D-Link
Building Networks for People

Межсетевой экран D-Link

Руководство пользователя

DFL-210/ 800/1600/ 2500
DFL-260/ 860/1660/ 2560(G)

Версия 2.27.01

NETWORK SECURITY SOLUTION http://www.dlink.com

NETDEFEND

Руководство пользователя

DFL-210/260/800/860/1600/1660/2500/2560/2560G NetDefendOS Версия 2.27.01

D-Link Corporation
No. 289, Синху, Нейху, Тайбэй, Тайвань
http://www.DLink.com

Опубликовано 2010-02-26

Руководство пользователя
DFL-210/260/800/860/1600/1660/2500/2560/2560G
NetDefendOS Версия 2.27.01

Опубликовано 2010-02-26

Уведомление об авторском праве

Отказ от прав

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления. Компания D-Link не дает никаких заверений или гарантий в отношении содержания настоящего документа и отказывается от любых косвенных гарантий, касающихся товарного качества или пригодности товаров к использованию по назначению. Компания D-Link оставляет за собой право пересмотреть данный документ и периодически вносить изменения в содержание документа без предварительного уведомления лица или сторон об изменениях.

Ограничение ответственности

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ D-LINK ИЛИ ЕЕ ПОСТАВЩИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА УБЫТКИ ЛЮБОГО ХАРАКТЕРА (НАПРИМЕР, УЩЕРБ ОТ ПОТЕРИ ПРИБЫЛИ, ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОСТАНОВКИ РАБОТЫ, ПОТЕРИ СОХРАНЕННЫХ ДАННЫХ ИЛИ ЛЮБЫЕ ДРУГИЕ КОММЕРЧЕСКИЕ УБЫТКИ ИЛИ ПОТЕРИ), ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ПРИМЕНЕНИЯ ИЛИ НЕПРАВИЛЬНОГО ИСПОЛЬЗОВАНИЯ ПРОДУКТА D-LINK ИЛИ НЕИСПРАВНОСТИ ПРОДУКТА, ДАЖЕ ЕСЛИ КОМПАНИЯ D-LINK БЫЛА ПРОИНФОРМИРОВАНА О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ. КРОМЕ ТОГО, КОМПАНИЯ D-LINK НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ, ЕСЛИ ТРЕТЬЯ СТОРОНА ПРЕДЪЯВЛЯЕТ ТРЕБОВАНИЯ КЛИЕНТУ ИЗ-ЗА ПОТЕРЬ ИЛИ ПОВРЕЖДЕНИЙ. КОМПАНИЯ D-LINK НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА УЩЕРБ, ПРЕВЫШАЮЩИЙ СУММУ, ПОЛУЧЕННУЮ КОМПАНИЕЙ ОТ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ ПРОДУКТА.

Содержание

Предисловие

Целевая аудитория

Данное Руководство пользователя предназначено преимущественно для администраторов сети, отвечающих за настройку и управление межсетевых экранов D-Link с операционной системой NetDefendOS. При разработке данного руководства предполагалось, что пользователь уже обладает базовыми знаниями в области сетевых технологий и обеспечения безопасности сети.

Структура документа и обозначения

Текст документа разбит на главы и разделы. Нумерация разделов приводится в оглавлении выше.

Текст, который используется непосредственно в интерфейсе пользователя, выделяется **жирным шрифтом**. *Курсивом* могут выделяться термины, которые появляются в тексте впервые. Также курсив используется при необходимости подчеркнуть некоторые моменты.

Когда результат взаимодействия с консолью показан в тексте не в примере, он приводится в виде текста с серым фоном.

Когда в тексте встречается ссылка на Web-адрес, нажатие на нее откроет данный URL в браузере в новом окне (однако, в некоторых системах это не допускается).
Например: *http://www.dlink.com*.

Снимки экрана

В этом руководстве представлено минимальное количество снимков экрана. Это сделано преднамеренно, поскольку в данном руководстве, прежде всего, описывается операционная система NetDefendOS, а администраторы могут выбрать нужный интерфейс управления. Поэтому было решено, что руководство будет менее загромождено и удобно для чтения, если оно будет ориентировано на то, как функционирует ОС NetDefendOS, а не будет включать большое количество иллюстраций, показывающих, как используются различные интерфейсы. Приводимые примеры большей частью представляют текстовые описания использования интерфейса управления.

Примеры

Примеры в тексте идут под заголовком **Пример** и изображаются на сером фоне, как показано ниже. Это может быть пример, касающийся использования Интерфейса командной строки CLI и/или Web-интерфейса. (в Руководстве по использованию *Интерфейса командной строки CLI* NetDefendOS приводится список всех команд CLI.)

Пример 1. Нотация примера

Здесь приводится общая информация о данном примере, иногда с поясняющими изображениями.

CLI

Пример, касающийся Интерфейса командной строки, появится здесь. Сначала будет идти командное приглашение, а затем сама команда:

```
gw-world:/> somecommand someparameter=somevalue
```

Web-интерфейс

Действия, выполняемые для данного примера в Web-интерфейсе, отображаются здесь. Они также отображаются в виде нумерованного списка в левой колонке интерфейса или в открываемом контекстном меню за информацией о данных, которые необходимо ввести:

1. Зайдите **X > Item Y > Item Z**

2. Введите:
•**DataItem1:** datavalue1
•**DataItem2:** datavalue2

Важная информация

Текст, на который читателю следует обратить особое внимание, выделяется курсивом и обозначается специальными символами в левой части страницы. Ниже приводится информация о встречающихся в тексте руководства значках:

Примечание
Указывает информацию, которая дополняет предыдущий текст и на которую следует обратить внимание.

Совет
Таким символом обозначается информация, которая не является критичной, но является полезной в определенных ситуациях.

Внимание
Указывает на ситуации, когда читатель должен быть внимателен с выполняемыми действиями, поскольку при несоблюдении определенных условий могут возникнуть нежелательные последствия.

Важно
Этим символом обозначается важная информация, которую пользователю необходимо прочитать и понять.

Предупреждение
Это важная информация для пользователей, поскольку они должны быть предупреждены, что могут возникнуть серьезные ситуации, если будут или не будут предприняты определенные действия.

Торговые марки

Все названия торговых марок, указанных в настоящем документе, являются собственностью их владельцев.

Windows, *Windows XP*, *Windows Vista* и *Windows 7* являются зарегистрированными товарными знаками или товарными знаками Microsoft Corporation в США и / или других странах.

Глава 1. Обзор NetDefendOS

В данной главе представлены основные функции системы NetDefendOS.

- Функции
- Архитектура NetDefendOS
- Управление потоком пакетов на основе механизма состояний (State Engine) системы NetDefendOS

1.1. Функции

Операционная система D-Link NetDefendOS является основным программным обеспечением, которое используется для управления межсетевыми экранами D-Link с расширенным функционалом.

NetDefendOS как сетевая операционная система

Разработанная как *сетевая операционная система*, NetDefendOS обеспечивает широкую полосу пропускания с высокой надежностью и малым шагом изменения полосы. В отличие от продуктов, использующих стандартную операционную систему, например, Unix или Microsoft Windows, NetDefendOS обеспечивает бесшовную интеграцию всех подсистем, подробный контроль над всеми функциями и снижение риска атак.

Объекты NetDefendOS

С точки зрения администратора, концептуальный подход NetDefendOS позволяет визуализировать операции посредством ряда логических блоков или объектов, которые позволяют настраивать устройство почти бесконечным числом образов. Маленький шаг управления позволяет администратору установить нужные настройки в различных сетях.

Основные функции

NetDefendOS – сетевая операционная система с расширенным функционалом. Ниже представлены основные функции продукта:

IP Routing

NetDefendOS обеспечивает различные опции IP-маршрутизации, включая статическую маршрутизацию, динамическую маршрутизацию, а также возможности маршрутизации multicast. Кроме того, NetDefendOS поддерживает такие функции, как Virtual LAN, мониторинг маршрутов, Proxy ARP и Transparency. Более подробная информация приведена в *Главе 4,Маршрутизация.*

Firewalling Policies

NetDefendOS предоставляет проверку пакетов SPI для широкого набора протоколов, включая TCP, UDP и ICMP.
Администратор может задать подробные политики межсетевого экрана на основе источника/назначения сети/интерфейса, протокола, портов, атрибутов пользователя (user credentials), времени дня и т.д. *Раздел 3.5, «IP-правила»*, описывает установку политик, позволяющих определить, какой трафик будет разрешен или запрещен NetDefendOS.

Address Translation

В целях обеспечения функционала, а также безопасности, NetDefendOS поддерживает трансляцию адресов на основе политик. Поддерживается как динамическая трансляция адресов (NAT), так и статическая трансляция адресов (SAT), что обеспечивает работу в различных типах сетей. Эта функция описывается в *Главе 7, «Преобразование адресов».*

VPN

NetDefendOS поддерживает различные варианты реализации Virtual Private Network (VPN). NetDefendOS поддерживает VPN на основе протоколов IPsec, L2TP и PPTP и может работать как сервер или клиент для всех типов VPN и позволяет индивидуальные политики безопасности для каждого VPN-туннеля. Подробные описания будут представлены в *Главе 9, VPN,* которая включает шаги установке, *Раздел 9.2, «Быстрый запуск VPN»*.

TLS Termination

NetDefendOS поддерживает TLS Termination, что позволяет межсетевым экранам D-Link работать в качестве конечной точки для клиентов Web-браузера HTTP (эта функция иногда называется *SSL termination*). Более подробная информация представлена в *Разделе 6.2.9, «TLS ALG»*.

Anti-Virus Scanning

NetDefendOS оснащена встроенным антивирусом.
Трафик, передаваемый через Межсетевой экран D-Link, может подвергаться детальному сканированию на вирусы, и узлы, рассылающие вирусы, могут быть занесены в черный список и заблокированы. Более подробная информация по этой функции приведена в *Разделе 6.4, «Антивирусное сканирование»*.

Примечание
Функция IDP доступна на всех моделях D-Link NetDefend в качестве абонентской услуги. Некоторые модели поддерживают стандартную упрощенную подсистему IDP.

Intrusion Detection and Prevention

Для предотвращения атак уровня приложений против уязвимостей в сервисах и приложениях NetDefendOS предоставляет защиту от вторжений *Intrusion Detection and Prevention (IDP)*.
IDP engine работает на основе политик и позволяет выполнять высокопроизводительное сканирование и обнаружение атак и выполнять блокировку и опционально вносить в черный список атакующие хосты. Более подробная информация о возможностях IDP NetDefendOS находятся в *Разделе 6.5, «Обнаружение и предотвращение вторжений (IDP)»*

Примечание
Функция IDP доступна на всех моделях D-Link NetDefend в качестве абонентской услуги. Некоторые модели поддерживают стандартную упрощенную подсистему IDP.

Web Content Filtering

NetDefendOS предлагает различные механизмы фильтрации Web-содержимого, не соответствующего политике использования Web. Web-содержимое может блокироваться на основе категории, несоответствующие объекты могут быть удалены, а Web-сайты могут быть добавлены в белый или черный список в нескольких политиках. Более подробная информация по фильтрации приводится в *Разделе 6.3, «Фильтрация Web-содержимого»*.

Примечание
Функция Dynamic WCF доступна только на некоторых моделях D-Link NetDefend.

Traffic Management

NetDefendOS обеспечивает удобные возможности для управления трафиком с помощью таких функций, как *Формирование трафика* (Traffic Shaping), *Правила порогов* (Threshold Rules) (только для некоторых моделей) и *Балансировка нагрузки сервера* (Server Load Balancing).
Traffic Shaping обеспечивает ограничение и распределение полосы пропускания; Threshold Rules обеспечивает спецификацию порогов для отправки сообщений об авариях и/или ограничения сетевого трафика; Server Load Balancing позволяет устройству с NetDefendOS распределять нагрузку в сети между несколькими хостами. Эти функции подробно обсуждаются в *Главе 10, Управление трафиком*.

Примечание
Функция Threshold Rules доступна только на некоторых моделях D-Link NetDefend.

Operations and Maintenance

Управление NetDefendOS осуществляется через Web-интерфейс или Интерфейс командной строки (CLI). NetDefendOS также предоставляет возможности подробного наблюдения за событиями и регистрацией, а также поддержку мониторинга через SNMP. Более подробная информация по данному вопросу приводится в *Главе 2, Управление и обслуживание*.

ZoneDefense

NetDefendOS может использоваться для управления коммутаторами D-Link с помощью функции ZoneDefense. Эта опция позволяет NetDefendOS изолировать участки сети, которые содержат источник нежелательного сетевого трафика.

Примечание
Функция NetDefendOS ZoneDefense доступна только на некоторых моделях D-Link NetDefend.

Документация NetDefendOS

Прочитав внимательно документацию, пользователь сможет получить максимум от продукта NetDefendOS. В дополнение к данному документу необходимо ознакомиться с другими руководствами:

• *Руководство по Интерфейсу командной строки CLI*, которое содержит информацию по всем командам NetDefendOS CLI.

• *Руководство по записям Журнала NetDefendOS* содержит подробности по всем сообщениям журнала NetDefendOS.

Все эти документы образуют важнейшую информацию по работе с ОС NetDefendOS.

1.2. Архитектура NetDefendOS

1.2.1. Архитектура на основе состояний

Архитектура NetDefendOS использует соединения на основе состояний. В основном, стандартные IP-маршрутизаторы или коммутаторы изучают пакеты и затем выполняют перенаправление на основе информации, содержащейся в заголовках пакетов. При этом пакеты перенаправляются без

контекста, что устраняет любую возможность определения и анализа комплексных протоколов и применения соответствующих политик безопасности.

Технология Stateful Inspection

Система NetDefendOS использует технологию *Stateful inspection*, осуществляющую проверку и перенаправление трафика на основе соединения. NetDefendOS определяет новое установленное соединение и сохраняет небольшую информацию или *state* в таблице *state table* для определения времени существования данного соединения. Таким образом, NetDefendOS предоставляет возможность определить контекст сетевого трафика, который позволяет выполнить тщательное сканирование трафика, управление полосой пропускания и множество других функций.

Технология Stateful inspection обеспечивает высокую производительность, повышая пропускную способность совместно с дополнительным преимуществом гибкого масштабирования. Подсистема NetDefendOS, выполняющая *stateful inspection*, иногда употребляется в документации как NetDefendOS *state-engine*.

1.2.2. Структурные элементы NetDefendOS

Основными структурными элементами в NetDefendOS являются интерфейсы, логические объекты и различные типы правил (или комплект правил).

Интерфейсы

Интерфейсы являются «входом» для исходящего и входящего трафика, проходящего через межсетевой экран NetDefend. При отсутствии интерфейсов система NetDefendOS не имеет возможности получать или отправлять данные.

NetDefendOS поддерживает следующие типы интерфейсов:

- **Физические интерфейсы** – относятся к актуальным физическим Ethernet-портам.
- **Под-интерфейсы (sub-interfaces)** – включают интерфейсы VLAN и PPPoE.
- **Интерфейсы туннелирования** – используются для отправки и получения данных через VPN-туннели.

Симметричные интерфейсы

Дизайн интерфейса NetDefendOS симметричен, это означает, что интерфейсы устройства нефиксированные и являются «незащищенными снаружи» или «защищенными внутри» в топологии сети и определяются только администратором.

Логические объекты

Логические объекты - это предварительно определенные элементы, используемые в наборах правил. Адресная книга, например, содержит назначенные объекты, представляющие хост и сетевые адреса.

Другим примером логических объектов являются сервисы, предоставляющие определенные комбинации протоколов и портов. Помимо этого, важную роль играют объекты Application Layer Gateway (ALG), которые используются для определения дополнительных параметров в определенных протоколах, таких как HTTP, FTP, SMTP и H.323.

Наборы правил NetDefendOS

В конечном итоге, правила, определенные администратором в различные *комплекты правил* (rule sets) используются для фактического применения политик безопасности NetDefendOS. Основополагающим комплектом правил являются *IP-правила* (IP Rules), которые используются, чтобы определить политику IP-фильтрации уровня 3, а также для переадресации и балансировки нагрузки сервера. Правила формирования трафика (Traffic Shaping Rules) определяют политику управления полосой пропускания, правила IDP обеспечивают защиту сети от вторжений и т.д.

1.2.3. Поток пакетов

Данный раздел описывает прохождение пакетов, полученных и отправленных системой NetDefendOS. Следующее описание является упрощенным и не может быть применимо ко всем сценариям, тем не менее, основные принципы являются действенными при использовании NetDefendOS.

1. Ethernet-фрейм получен на одном из Ethernet-интерфейсов системы. Выполняется проверка основного Ethernet-фрейма и, если фрейм не является допустимым, пакет будет отброшен.

2. Пакет ассоциируется с интерфейсом источника. Интерфейс источника определяется следующим образом:

   - Если Ethernet-фрейм содержит идентификатор VLAN ID (Virtual LAN identifier), (идентификатор виртуальной локальной сети), система сравнивает конфигурацию VLAN-интерфейса с соответствующим VLAN ID. В случае определения соответствия VLAN-интерфейс становится интерфейсом источника пакета. Если соответствия не обнаружено, пакет будет отброшен, а событие зарегистрировано в журнале.
   - Если Ethernet-фрейм содержит PPP-данные, система выполняет его проверку на соответствие с PPPoE-интерфейсом. Если соответствие обнаружено, интерфейс становится интерфейсом источника пакета. В противном случае пакет отбрасывается, а событие регистрируется в журнале.
   - Если ничего из вышеперечисленного не выполняется, то интерфейс получения (тот Ethernet-интерфейс, на который поступил Ethernet-фрейм) становится интерфейсом источника пакета.

3. IP-датаграмма из пакета передается на проверочное устройство NetDefendOS, которое выполняет проверку пакета на исправность, включая проверку контрольной суммы, флагов протокола, длины пакета и т.д. Если выявлена ошибка, пакет отбрасывается, а событие регистрируется в журнале.

4. NetDefendOS выполняет поиск существующего соединения, сопоставляя параметры входящего пакета, включая интерфейс источника, IP-адреса источника и назначения и IP-протокол.

   Если соответствие не обнаружено, начинается процесс установки соединения, который включает шаги, начиная с данного пункта до пункта *9*. Если соответствие обнаружено, процесс перенаправления продолжается с шага *10*.

5. *Правила доступа* (Access Rules) определяют, разрешен ли IP-адрес источника нового соединения на интерфейсе получения. Если соответствующего правила не обнаружено, в таблице маршрутизации выполняется *поиск обратного маршрута* (reverse route lookup).

   Другими словами, по умолчанию, интерфейс будет принимать только IP-адрес источника, который принадлежит сети данного интерфейса. *Поиск обратного маршрута* (reverse lookup) выполняется в таблице маршрутизации для того, чтобы подтвердить, что существует маршрут для использования того же интерфейса, если сеть является сетью назначения.

   Если поиск правила доступа или обратный поиск маршрута определяют, что IP источника неверный, в таком случае пакет отбрасывается и событие регистрируется в журнале.

6. Поиск маршрута выполняется в соответствующей таблице маршрутизации. Интерфейс назначения для соединения уже определен.

7. Определяются IP-правила, которым соответствуют параметры данного пакета. Используются

следующие параметры:

- Интерфейсы источника и назначения
- Сеть источника и назначения
- IP-протокол (например, TCP, UDP, ICMP)
- TCP/UDP-порты
- Типы ICMP-пакетов
- Время действия правила по расписанию

Если соответствие не обнаружено, пакет отбрасывается.

Если обнаружено правило, соответствующее новому соединению, параметр правила *Action* определяет действия системы NetDefendOS по отношению к соединению. Если определено действие *Drop* (Отклонить), пакет отбрасывается, а событие регистрируется в журнале.

Если определено действие *Allow* (Разрешить), пакет проходит через систему. Соответствующее состояние будет добавлено в таблицу соединений для соответствия с последующими пакетами, принадлежащих тому же соединению. Помимо этого, объект службы, с которым связан один или несколько IP-протоколов с соответствующими им номерами портов может быть связан с объектом Application Layer Gateway (ALG). Эти данные используются для того, чтобы система NetDefendOS управляла соответствующими приложениями для обеспечения обмена информацией.

В конечном итоге, новое соединение, созданное согласно настройкам правил, будет зарегистрировано в журнал.

Примечание: Дополнительные действия

Существует ряд дополнительных действий, например, переадресация и балансировка нагрузки сервера. При этом основная концепция запрета и разрешения трафика остается той же.

8. Правила обнаружения и предотвращения вторжений (Intrusion Detection and Prevention (IDP) Rules) оцениваются по аналогии с IP-правилами. Если выявлено соответствие, данные регистрируются. Таким образом, система NetDefendOS будет осведомлена о выполнении сканирования всех пакетов, относящихся к этому соединению.
9. Анализируется Формирование трафика (Traffic Shaping) и Правило ограничения порога (Threshold Limit rule). Если обнаружено соответствие, соответствующая информация регистрируется. Таким образом, выполняется управление трафиком.
10. При наличии информации система NetDefendOS решает, какое действие применить к входящему пакету:

    - При наличии данных ALG и выполнения IDP-сканирования данные пакета анализируются подсистемой псевдосборки TCP, которая в свою очередь использует различные ALG, механизмы сканирования содержимого на 7 уровне и т.д., для дальнейшего анализа или изменения трафика.
    - Если содержимое пакета зашифровано (с помощью протокола IPsec, PPTP/L2TP или другого типа протокола туннелирования), выполняется проверка списков интерфейсов на соответствие. Если обнаружено соответствие, пакет расшифровывается и данные (незашифрованный текст) пересылаются обратно в NetDefendOS, но уже с интерфейсом источника, который соответствует интерфейсу туннелирования. Другими словами, процесс продолжается с шага 3, указанного выше.
    - При наличии информации об управлении трафиком, пакет может быть определен в очередь или выполняются действия согласно настройкам по управлению трафиком.

11. В конечном итоге, пакет будет перенаправлен на интерфейс назначения в соответствии с его состоянием. Если интерфейс назначения является интерфейсом туннелирования или физическим под-интерфейсом, может выполняться дополнительная обработка данных, например, шифрование или инкапсуляция. В следующем разделе представлены диаграммы, иллюстрирующие поток

пакетов, проходящих через систему NetDefendOS.

1.3. Управление потоком пакетов на основе механизма состояний (State Engine) системы NetDefendOS

Представленные диаграммы отображают краткую информацию о потоке пакетов, проходящем через межсетевой экран с поддержкой NetDefendOS. В данном разделе рассматриваются три диаграммы, каждая из которых является продолжением следующей. Нет необходимости в тщательном разборе данных диаграмм, тем не менее, они могут быть полезны при настройке NetDefendOS в различных ситуациях.

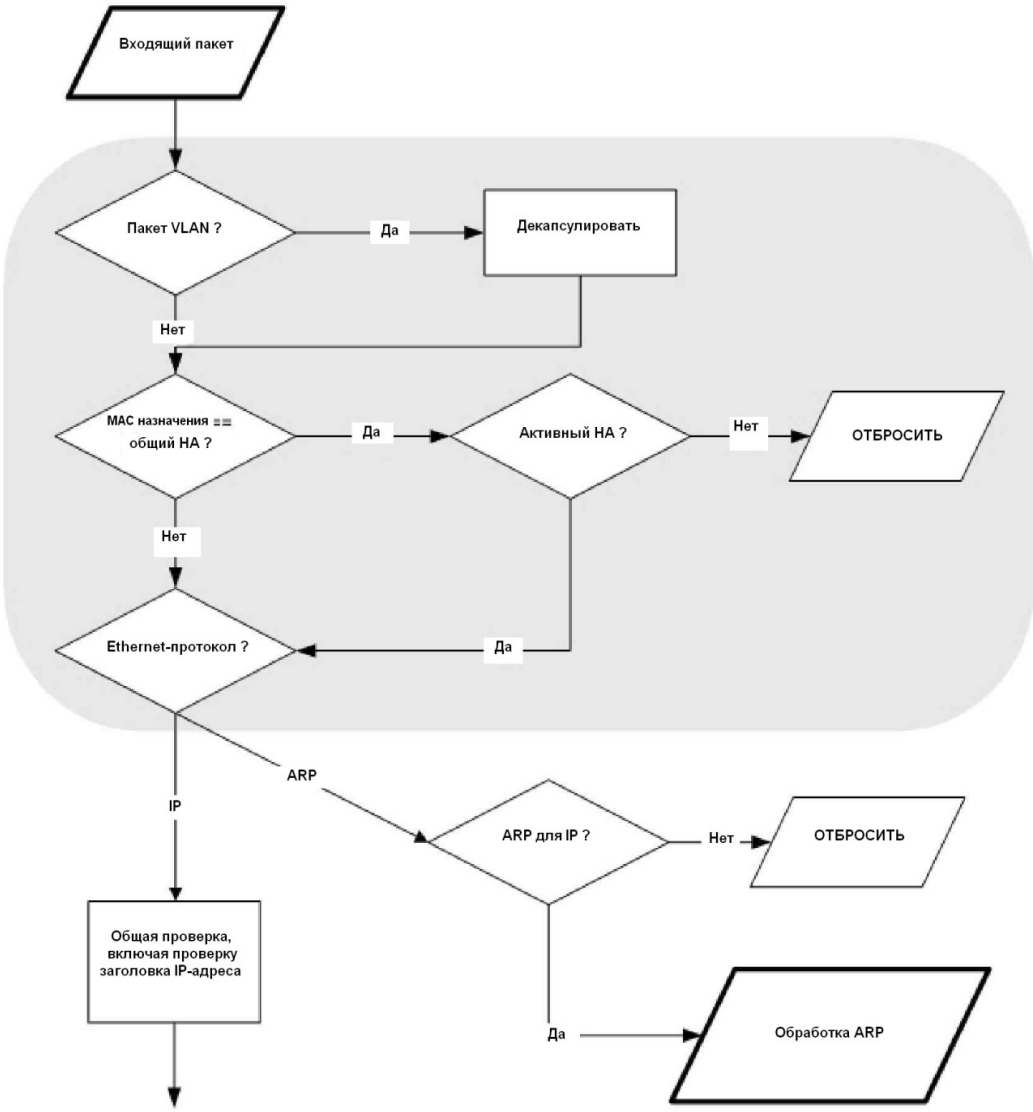


Рис. 1.1. Схематичное изображение потока пакетов. Часть I

Продолжение схемы на следующей странице.

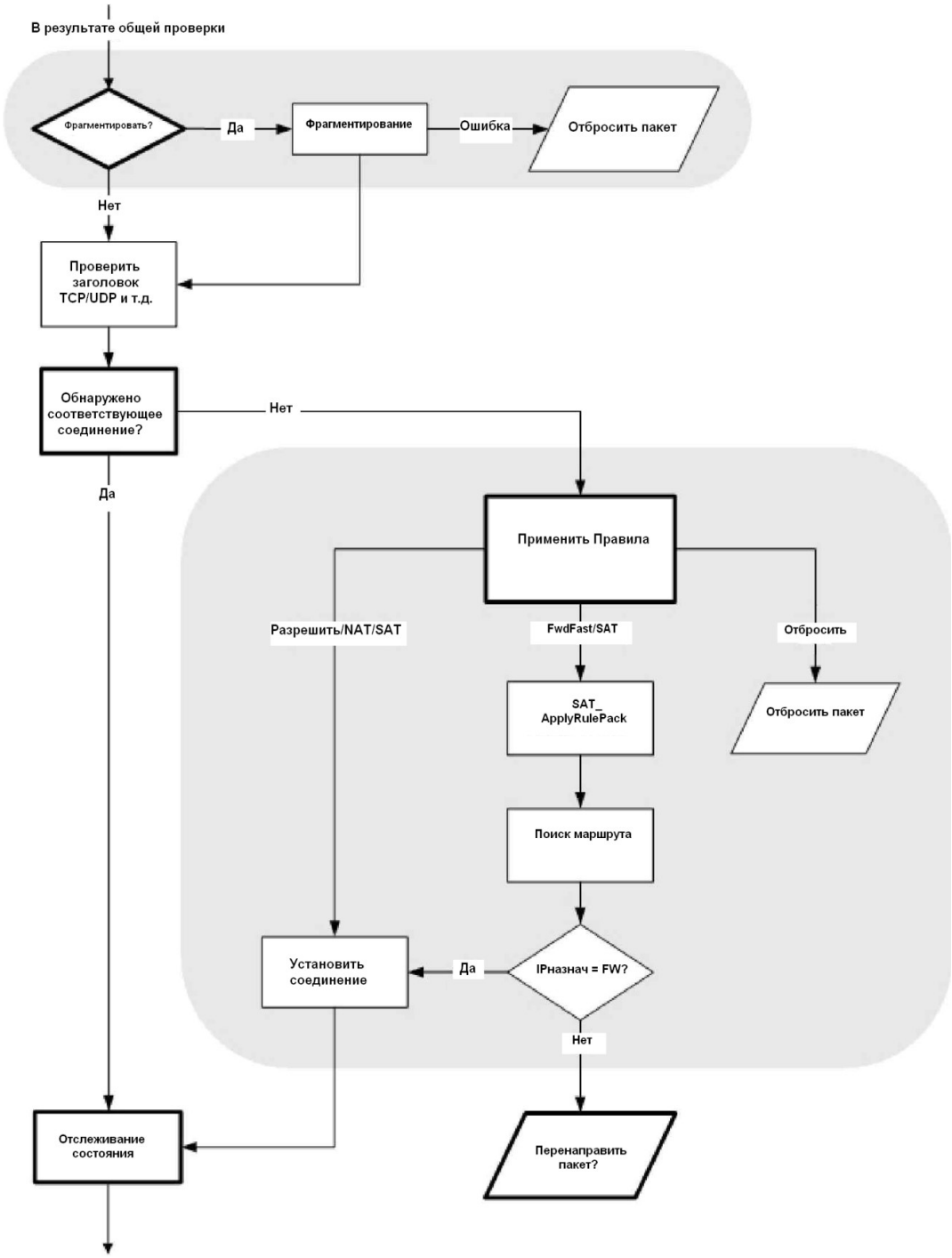


Рис. 1.2. Схематичное изображение потока пакетов. Часть II

Продолжение схемы на следующей странице.

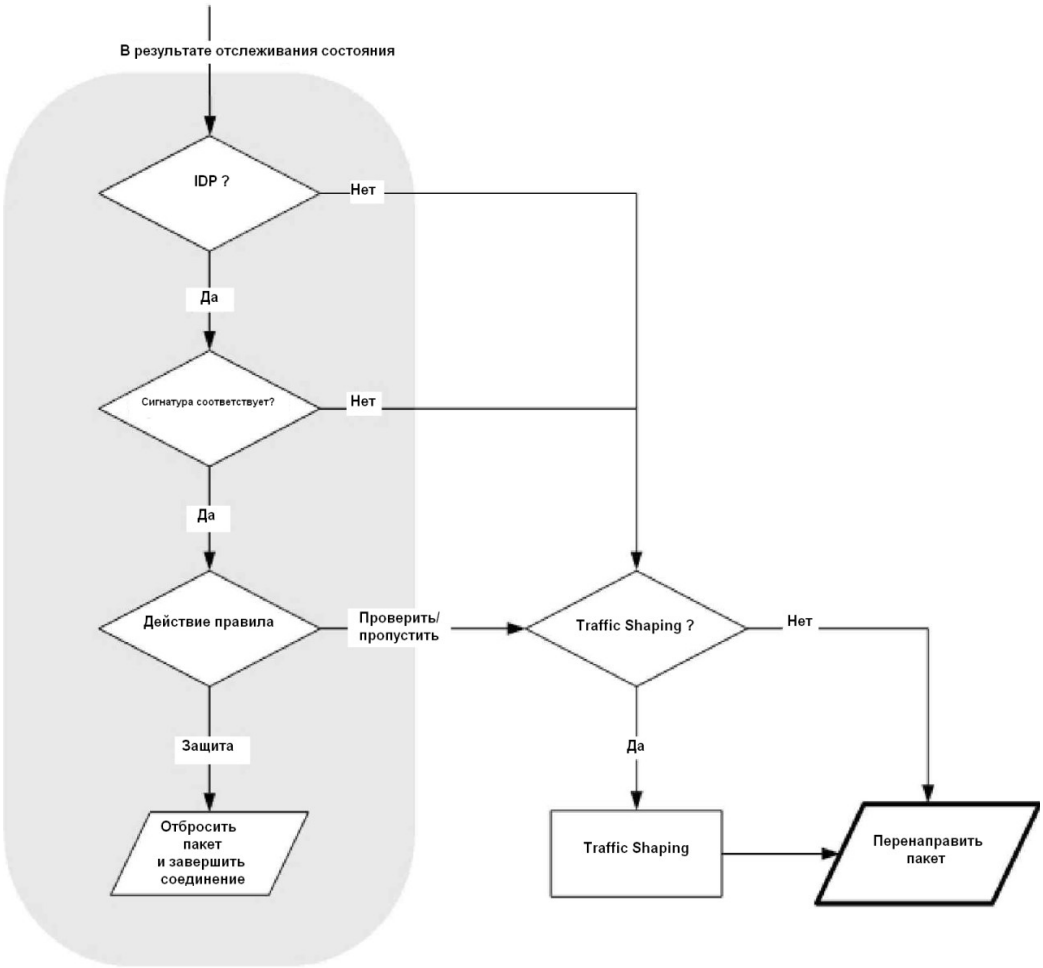


Рис. 1.3. Схематичное изображение потока пакетов. Часть III

Применяемые правила

На рисунке ниже представлена детальная логическая схема функции *Применить Правила* Рисунка 1.2, «Схематичное изображение потока пакетов Часть I», изображенного выше.

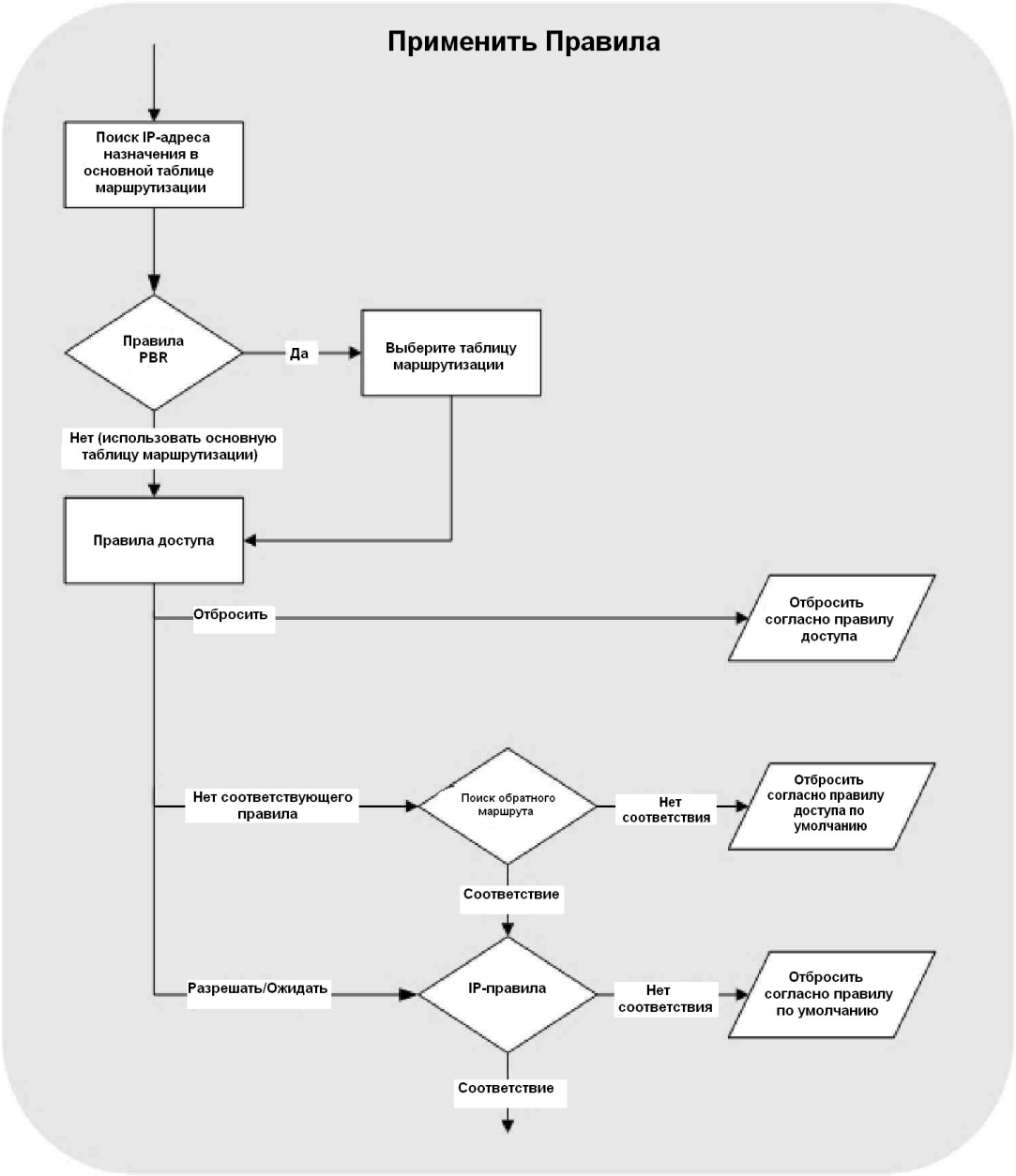


Рис. 1.4. Детальная логическая схема Применить Правила

Глава 2. Управление и обслуживание

В данной главе рассматриваются аспекты, связанные с управлением, операциями и обслуживанием NetDefendOS.

• Управление NetDefendOS

• События и Регистрация

• RADIUS Accounting

• Обзор аппаратного обеспечения

• SNMP Monitoring

• Команда pcapdump

• Обслуживание

2.1. Управление NetDefendOS

2.1.1. Обзор

Система NetDefendOS разработана для обеспечения высокой производительности и надежной работоспособности. Система предоставляет не только расширенный набор функций, но и дает администратору возможность полного управления каждой деталью системы. Это означает, что продукт подходит для применения в самых сложных условиях.

Для корректного использования системы, необходимо хорошо ориентироваться в настройках NetDefendOS. По этой причине в данном разделе представлена подробная настройка подсистемы, а также описание работы с различными интерфейсами управления.

Интерфейсы управления

NetDefendOS предоставляет следующие интерфейсы управления:

Web-интерфейс — Система NetDefendOS поддерживает встроенный дружественный пользователю Web-интерфейс (также известный как *Web-интерфейс пользователя* или *WebUI*). Данный интерфейс графического управления доступен через стандартный Web-браузер (рекомендуется Microsoft Internet Explorer или Firefox). Браузер подключается к одному из Ethernet-интерфейсов оборудования с помощью протокола *HTTP* или *HTTPS* и система NetDefendOS выступает в роли Web-сервера, позволяя использовать Web-страницы в качестве интерфейса управления.

Данная функция подробно представлена в *Разделе 2.1.3, «Web-интерфейс»*.

Интерфейс командной строки CLI — Интерфейс командной строки CLI, доступный локально через серийный консольный порт или удаленно с помощью протокола Secure Shell (SSH), обеспечивает управление всеми параметрами в NetDefendOS.

Данная функция подробно описана в *Разделе 2.1.4, «CLI»*.

Secure Copy — *Secure Copy* (SCP) – широко распространенный протокол коммуникации, используемый для передачи данных. NetDefendOS не предоставляет определенного SCP-клиента, однако, существует широкий выбор SCP-клиентов, доступных для всех платформ

рабочих станций. SCP является дополнением к CLI и обеспечивает защиту файлов, передаваемых между рабочей станцией администратора и межсетевым экраном NetDefend. Различные файлы, используемые системой NetDefendOS, могут быть скачаны и загружены с помощью SCP.

Данная функция подробно описана в *Разделе 2.1.6, «Secure Copy»*.

Меню загрузки консоли Перед запуском системы NetDefendOS, консоль, подключенная непосредственно к RS232-порту межсетевого экрана NetDefend, может использоваться для выполнения основных настроек через меню загрузки. Данное меню вводится нажатием любой клавиши консоли с момента включения питания до запуска NetDefendOS. В меню загрузки доступен *Загрузчик программного обеспечения*.

Данная функция подробно описана в *Разделе 2.1.6, «Меню загрузки консоли»*.

Примечание: Рекомендуемые браузеры

Бразузеры, рекомендуемые для использования с WebUI: Microsoft Internet Explorer (версия 7 и выше), Firefox (версия 3.0 и выше) и Netscape (версия 8 и выше). Также можно использовать другие браузеры.

Политики удаленного управления

Доступ к интерфейсам удаленного управления может быть организован с помощью политики удаленного управления, таким образом, администратор может ограничить доступ к управлению на основе сети источника, интерфейса источника, имени пользователя и пароля. В определенной сети доступ к Web-интерфейсу может быть разрешен пользователям с административными правами, в то же время разрешен удаленный доступ к интерфейсу командной строки CLI при подключении по IPsec-туннелю.

По умолчанию, доступ к Web-интерфейсу открыт пользователям в сети при подключении через LAN-интерфейс межсетевого экрана D-Link (при наличии более одного LAN-интерфейса, **LAN1** является интерфейсом по умолчанию).

2.1.2. Учетная запись по умолчанию «Administrator»

По умолчанию, NetDefendOS поддерживает локальную базу данных, AdminUsers, которая содержит предварительно определенную учетную запись admin. Имя пользователя и пароль данной учетной записи – admin. Учетная запись обладает правами записи/чтения в системе NetDefendOS.

Важно:

В целях безопасности, после подключения к межсетевому экрану NetDefend, рекомендуется как можно скорее изменить пароль по умолчанию учетной записи.

Создание дополнительных учетных записей

Если требуется, можно создать дополнительные учетные записи. Учетные записи могут

принадлежать группе пользователей **Администратор**, в таком случае, они обладают административными правами чтения/записи, или же группе пользователей **Аудитор**, при этом они обладают только правами чтения.

Несколько учетных записей администратора

Система NetDefendOS запрещает регистрацию более одной учетной записи администратора. Если одна учетная запись уже создана, регистрация второй учетной записи или более будет разрешена, но при этом предоставляются права только аудита. Другими словами, зарегистрированная вторая учетная запись или более будет обладать только правами чтения настроек без возможности их изменения.

2.1.3. Web-интерфейс

Система NetDefendOS предоставляет интуитивный *Web-интерфейс* (WebUI) для возможности управления системой через Ethernet-интерфейс, используя стандартный Web-браузер. При этом администраторы получают возможность удаленного управления из любой точки частной сети или Интернет, используя стандартный компьютер без специально установленного программного обеспечения.

Назначение IP-адреса по умолчанию

Новому межсетевому экрану D-Link NetDefend с заводскими настройками по умолчанию система NetDefendOS автоматически назначает внутренний IP-адрес по умолчанию на интерфейсе LAN1 (или интерфейс LAN на моделях с одним локальным интерфейсом). IP-адрес, назначаемый интерфейсу управления, зависит от модели межсетевого экрана NetDefend:

- Для моделей межсетевых экранов NetDefend DFL-210, 260, 800, 860, 1600 и 2500, IP-адрес интерфейса управления, назначаемый по умолчанию - *192.168.1.1*.

- Для моделей межсетевых экранов NetDefend DFL-1660, 2560 и 2560G, IP-адрес интерфейса управления, назначаемый по умолчанию - *192.168.10.1*.

Установка IP-адресов на рабочей станции

Назначаемый интерфейс межсетевого экрана NetDefend и интерфейс рабочей станции должны быть в одной и той же сети для успешной коммуникации между ними, таким образом, интерфейсу подключения рабочей станции вручную назначаются следующие значения статического IP-адреса:

- **IP-адрес:** *192.168.1.30*
- **Маска подсети:** *255.255.255.0*
- **Основной шлюз:** *192.168.1.1*

Регистрация в Web-интерфейсе

Для получения доступа к Web-интерфейсу, используя заводские настройки по умолчанию, запустите Web-браузер на рабочей станции (рекомендуется последняя версия Internet Explorer или Firefox) и введите адрес *192.168.1.1*.

При выполнении первоначального подключения к NetDefendOS, администратор **должен** использовать https:// так как в адресной строке браузера используется URL-протокол (другими словами, https://192.168.1.1). Использование протокола HTTPS обеспечивает защиту коммуникации с NetDefendOS.

При успешной установке соединения с NetDefendOS, появится диалоговое окно аутентификации

пользователя, изображенное ниже и отображаемое затем в окне браузера.

Введите имя пользователя и пароль, затем нажмите кнопку **Login**. Имя пользователя по умолчанию – ***admin,*** пароль по умолчанию – ***admin.*** Если учетные данные пользователя корректные, выполняется переход на главную страницу Web-интерфейса.

Первоначальная регистрация в Web-интерфейсе и Мастер установки

При выполнении первоначальной регистрации, имя пользователя по умолчанию и пароль - ***admin***.

После успешной регистрации интерфейс пользователя отображается в окне браузера. Если изменения в настройках не были загружены на межсетевой экран NetDefend, запуск Мастера установки NetDefendOS произойдет автоматически и пользователь сможет выполнить все необходимые шаги по установке публичного доступа к сети Интернет.

Важно: Отключение блокировки всплывающих окон

Блокирование всплывающих окон должно быть отключено в Web-браузере для обеспечения запуска Мастера установки ***NetDefendOS Setup Wizard*** *с момента его появления во всплывающем окне.*

Поддержка нескольких языков

Диалоговое окно регистрации в Web-интерфейсе предоставляет на выбор язык интерфейса (помимо английского). Поддержка языка осуществляется за счет комплекта отдельных файлов источника. Эти файлы можно загрузить с Web-сайта D-Link.

Возможны случаи, когда обновленная система NetDefendOS содержит функции, где отсутствует законченный вариант перевода на выбранный язык из-за ограничений по времени. В этом случае, в качестве временного решения используется английский язык.

Интерфейс Web-браузера

Слева в Web-интерфейсе представлено древовидное меню, обеспечивающее навигацию по различным объектам NetDefendOS. Центральная часть Web-интерфейса отображает информацию об этих модулях. Информация о текущем статусе выполнения представлена по умолчанию.

Для получения информации об имени пользователя и пароле по умолчанию обратитесь в *Раздел 2.1.2, «Учетная запись по умолчанию Administrator»*.

Примечание: Доступ к удаленному управлению

Доступ к Web-интерфейсу регулируется настраиваемой политикой удаленного управления. По умолчанию, система разрешает доступ к Web-интерфейсу только из внутренней сети.

Вид интерфейса

Главная страница Web-интерфейса состоит из трех основных разделов:

A.*Строка меню* Строка меню, расположенная в верхней части Web-интерфейса, содержит кнопки и выпадающее меню, используемые для выполнения задач настроек, а также для использования различных инструментов и просмотра страниц статуса.

- ***Home*** – Возврат на главную страницу Web-интерфейса
- ***Настройка***
  - ***Save and Actvate*** – Сохранение и активация настроек
  - ***Discard changes*** – Отмена изменений в настройках, выполненных во время текущей сессии
  - ***View Changes*** – Список изменений в настройках с момента последнего сохранения.
- ***Tools*** –Инструменты, необходимые для обслуживания системы.
- ***Status*** – Страницы различного статуса, используемые для диагностики системы.

- ***Maintenance (Обслуживание)***

  - ***Update Center –*** Обновление сигнатур антивируса и определения вторжений вручную или по расписанию.

  - ***License –*** Подробный просмотр лицензии и ввод кода активации.

  - ***Backup –*** Создание резервной копии настроек на локальном компьютере или восстановление предварительно загруженной резервной копии.

  - ***Reset –*** Перезапуск межсетевого экрана или сброс к заводским настройкам по умолчанию.

  - ***Upgrade –*** Обновление программного обеспечения межсетевого экрана.

  - ***Technical support –*** Предоставляет опцию для загрузки файла с межсетевого экрана, который может быть изучен локально или отправлен специалисту технической поддержки для помощи в исследовании проблемы. Это является крайне важным, так как автоматически предоставленная информация содержит множество деталей, которые требуются при поиске и устранении неисправностей.

Б. ***Навигатор*** Навигатор, расположенный в левой части Web-интерфейса, содержит настройки системы, отображенные в виде древовидного меню. Меню состоит из разделов, каждый из которых соответствует основным структурным блокам настроек. Меню может быть расширено при добавлении дополнительных разделов.

В. ***Главное окно*** Главное окно содержит настройки и детали статуса в соответствии с разделом, выбранном в навигаторе или строке меню.

Управление доступом к Web-интерфейсу

По умолчанию, доступ к Web-интерфейсу открыт только из внутренней сети. Если необходимо включить доступ из других сегментов сети, можно сделать это, изменив политику удаленного управления.

Пример 2.1. Включение удаленного управления через HTTPS

CLI

```
gw-world:/> add RemoteManagement RemoteMgmtHTTP https
                      Network=all-nets Interface=any
                      LocalUserDatabase=AdminUsers HTTPS=Yes
```

Web-интерфейс

1. Зайдите **System > Remote Management > Add > HTTP/HTTPS Management**

2. Введите **Name (Имя)** для политики удаленного управления HTTP/HTTPS, например, *https*

3. Установите флажок **HTTPS**

4. Выберите следующее из списков выпадающего меню:

• **User Database:** AdminUsers
• **Interface:** any
• **Network:** all-nets

5. Нажмите **OK**

Внимание: Не подвергайте интерфейс управления риску

Пример выше предоставлен исключительно в информационных целях. Никогда не передавайте скриншоты интерфейса пользователям в сети Интернет.

Выход из Web-интерфейса

После завершения работы необходимо выйти из Web-интерфейса, чтобы предотвратить доступ других пользователей к рабочей станции для получения неавторизованного доступа к системе. Выход из системы осуществляется при нажатии кнопки **Logout** справа в строке меню.

Совет: Корректная маршрутизация при управлении трафиком

Если при соединении через VPN-туннели возникла проблема, проверьте главную таблицу маршрутизации и найдите маршрут all-nets к VPN-туннелю. При управлении трафиком может использоваться этот маршрут.

Если для интерфейса управления не установлено определенного маршрута, в таком случае, весь трафик, идущий от NetDefendOS, будет автоматически маршрутизирован в VPN-туннель. В таком случае администратору следует добавить маршрут для обеспечения сетевого управления.

2.1.4. Интерфейс командной строки CLI

Система NetDefendOS предоставляет *интерфейс командной строки (CLI)* администраторам, которые предпочитают или которым требуется использование командной строки или более тщательное управление системными настройками. Интерфейс командной строки CLI доступен локально через серийный консольный порт (соединение с которым описывается ниже) или удаленно через Ethernet-интерфейс с использованием протокола *Secure Shell* (SSH) клиента SSH.

CLI предоставляет комплексный набор команд, обеспечивающих отображение и изменение информации по настройкам, а также отображение данных работы системы и выполнение задач обслуживания системы.

В данном разделе представлена краткая информация по использованию интерфейса командной строки CLI. Для получения информации обо всех командах CLI, см. *Руководство по интерфейсу командной строки CLI.*

Наиболее часто используемые команды CLI:

- *add* – Добавление объекта, например, IP-адреса или правила в настройки NetDefendOS.
- *set* – Установка какого-либо свойства объекта в качестве значения. Например, может использоваться для настройки интерфейса источника в IP-правиле.
- *show* – Отображение текущих категорий или значений объекта.
- *delete* – Удаление определенного объекта.

Структура команд CLI

Как правило, команды CLI обычно начинаются со структуры: <*command*> <*object_type*> <*object_name*>. Например, для отображения IP-адреса объекта *my_address*, используется команда:

```
gw-world:/> show Address IP4Address my_address
```

Вторая часть команды определяет *тип объекта* (object type) и необходима для идентификации категории объекта, к которой относится имя объекта (принимая во внимание то, что одно и то же имя может существовать в двух разных категориях).

Примечание: Категория и контекст

*Термин **категория** иногда упоминается в качестве **контекста** объекта.*

Команда *add* может также содержать *свойства объекта* (object properties). Для добавления нового объекта IP4Address с IP-адресом *10.49.02.01* используется команда:

```
gw-world:/> add IP4Address my_address Address=10.49.02.01
```

Tuny объекта может дополнительно предшествовать *категория* объекта. Группы *категории* совместно с набором *типов* используются с функцией *tab completion ,* которая описывается ниже.

Совет: Получение справки

*При наборе команды CLI `gw-world:/>` **`help help`** отображается информация о команде Справка.*

История команд CLI

Навигация по списку использованных команд в CLI-интерфейсе выполняется с помощью клавиш «стрелка вниз» и «стрелка вверх» (аналогично консоли в большинстве версий Microsoft Windows™). Например, нажатие клавиши «стрелка вверх» вызовет появление последней выполненной команды в текущей строке CLI. После появления команды, доступно ее повторное выполнение в первоначальной форме или измененной перед выполнением.

Функция Tab Completion

Достаточно сложно запомнить все команды и их опции. Система NetDefendOS предоставляет функцию, которая называется *tab completion*. Нажатие клавиши tab вызовет автоматическое завершение текущей части команды. Если завершение невозможно, в таком случае, нажатие клавиши tab приведет к автоматическому отображению доступных опций возможной команды.

Функция Tab Completion для данных

Польза функции tab completion заключается в возможности автоматического заполнения параметров данных текущими значениями в командной строке. Это выполняется путем набора символа ".", за которым следует нажатие клавиши tab после символа "=". Например, при наборе незаконченной команды:

```
set Address IP4Address lan_ip Address=
```

В данный момент при вводе " " с последующим нажатием клавиши tab, NetDefendOS отображает текущее значение параметра *Address*. Если данным значением является, например, *10.6.58.10,* автоматически получаем следующую строку незавершенной команды:

```
set Address IP4Address lan_ip Address=10.6.58.10
```

Система NetDefendOS автоматически вставляет текущее значение *10.6.58.10,* которое может быть легко изменено с помощью клавиши возврата на одну позицию или клавиши со стрелкой назад перед завершением команды.

Таким же образом, символ "<" перед tab может использоваться для автоматического заполнения значений параметров по умолчанию, если значение еще не было установлено. Например:

```
add LogReceiverSyslog example Address=example_ip LogSeverity=< (tab)
```

Заполнение значения по умолчанию для *LogSeverity*:

```
add LogReceiverSyslog example Address=example_ip LogSeverity=Emergency
```

Тем не менее, если в качестве альтернативы используется символ ".", получаем следующее:

```
add LogReceiverSyslog example Address=example_ip LogSeverity=. (tab)
```

Список всех возможных значений:

```
add         LogReceiverSyslog         example         Address=example_ip
 LogSeverity=Emergency,Alert,Critical,Error,Warning,Notice,Info
```

Впоследствии данный список может быть изменен с помощью клавиши со стрелкой назад и клавиши возврата на одну позицию.

Категории объектов

Ранее упоминалось, что объекты группируются по *muny*, например, *IP4Address*. Типы группируются по *категориям*. Тип *IP4Address* принадлежит категории *Address*. В основном, категории применяются функцией tab completion при поиске типа объекта, который необходимо использовать.

При вводе команды, например, *add* и нажатии клавиши tab, NetDefendOS отображает доступные категории. После выбора категории и повторного нажатия клавиши tab, будут отображены все типы объектов для данной категории. Использование категорий является для пользователя простым способом определения типа объекта и управляемого количества опций, отображаемых после нажатия tab.

Не все типы объектов принадлежат категориям. Тип объекта *UserAuthRule* является типом без категории и будет появляться в списке категорий после нажатия tab в начале команды.

В некоторых случаях категория рассматривается в качестве *контекста*.

Выбор категории объектов

Для некоторых категорий сначала необходимо выбрать члена данной категории с помощью команды cc (Изменить категорию) прежде чем отдельные объекты могут быть обработаны. Это касается, например, маршрутов. Если существует более одной таблицы маршрутизации, при добавлении или управлении маршрутом, прежде всего, необходимо использовать команду cc для идентификации именно той таблицы маршрутизации, которая требуется.

Предположим, что в таблицу маршрутизации необходимо добавить маршрут *main*. Первой командой будет:

```
gw-world:/> cc RoutingTable main

gw-world:/main>
```

Обратите внимание, что строка команды изменяется для указания текущей категории. Теперь можно

добавить маршрут:

```
gw-world:/> add Route Name=new_route1 Interface=lan Network=lannet
```

Для отмены категории используется команда *cc*:

```
gw-world:/main>

cc gw-world:/>
```

В категориях, которым перед обработкой объекта требуется предварительная команда *cc*, содержится символ «/», следующий за именами категорий, отображаемых при помощи команды *show*. Например, *RoutingTable/*.

Определение нескольких значений параметров

Иногда параметру команды требуется несколько значений. Например, некоторые команды используют параметр *AccountingServers,* и для данного параметра может быть определено более одного значения. При определении нескольких значений следует разделить их запятой «,». Например, если необходимо определить три сервера *server1*, *server2*, *server3,* назначение параметра в команде будет следующим:

```
AccountingServers=server1,server2,server3
```

Вставки в списки правил

Порядок правил, определенный в списках, например, набор IP-правил, является крайне важным. С помощью команды *add*, используемой CLI, по умолчанию добавляется новое правило в конце списка. Если размещение на определенной позиции является критичным, команда *add* может включить параметр *Index=* в качестве опции. Вставка на первую позицию в списке определена с помощью параметра *Index=1* в команде *add*, на вторую позицию – с помощью параметра *Index=2* и т.д.

Ссылка на объект по имени

Назначение имен некоторым объектам является дополнительным и выполняется с помощью параметра *Name=* в команде *add*. У объекта, такого как Правило порога, всегда есть значение *Index,* которое указывает на положение в списке правил, но которому дополнительно может быть присвоено имя. Следующее действие может быть выполнено либо по ссылке на его индекс, то есть его позицию в списке, либо, в качестве альтернативы, использовать назначенное имя.

В *Руководство по интерфейсу командной строки* отображен список опций, доступных для каждого объекта NetDefendOS, включая опции *Name=* и *Index=*.

Использование уникальных имен

Для удобства и ясности рекомендуется назначать имя всем объектам, таким образом, оно может использоваться для привязки, когда это требуется. Привязка по имени особенно полезна при написании сценариев CLI. Для получения подробной информации о сценариях, обратитесь в *Раздел 2.1.5, «Сценарии CLI»*.

CLI обеспечивает назначение уникальных имен в пределах типа объекта. По причинам совместимости с более ранними выпусками NetDefendOS существует исключение, связанное с IP-правилами, у которых могут быть двойные имена, тем не менее, рекомендуется избегать этого. Если дублированное имя IP-правила используется в двух IP-правилах, в таком случае только значение *Index* может однозначно определить каждое IP-правило в последующих командах CLI. Ссылка на IP-правило с дублированным именем окажется безуспешной и приведет к сообщению об ошибке.

Использование имен хоста в CLI

Для некоторых команд CLI, IP-адреса определяются как текстовое имя хоста вместо объекта IP4Address или IP-адреса, например, *192.168.1.10.* При этом перед именем хоста должен стоять префикс из букв *dns:* указывающий на то, что необходимо использовать DNS для поиска IP-адреса по имени хоста. Например, имя хоста *host.company.com* будет определено в CLI как *dns:host.company.com*.

Параметры, где могут употребляться URN с CLI:

- *Remote Endpoint (Удаленная конечная точка)* для IPsec, L2TP и PPTP-туннелей.
- *Хост* для LDAP-серверов.

Если требуется выполнить поиск с помощью DNS, необходимо настроить в системе NetDefendOS хотя бы один публичный DNS-сервер для преобразования имен хостов в IP-адреса.

Доступ к серийной консоли CLI

Порт серийной консоли – это локальный порт RS-232 межсетевого экрана NetDefend, обеспечивающий прямой доступ к интерфейсу командной строки NetDefendOS CLI при подключении к компьютеру или терминалу ввода/вывода. Для того чтобы определить, где находится серийный порт на устройстве D-Link, обратитесь к Руководству по быстрому запуску.

Для использования консольного порта необходимо следующее оборудование:

- Терминал или компьютер с серийным портом и возможностью эмулирования терминала (например, использование программного обеспечения *Hyper Terminal*, входящее в некоторые версии Microsoft Windows). Серийный консольный порт использует следующие настройки по умолчанию: *Скорость: 9600 бит/с, Четность: без проверки четности, Биты данных: 8 бит и Стоповые биты:1 стоп-бит*.

- Кабель RS-232 с соответствующими коннекторами. В комплект поставки входит кабель RS-232 null-modem.

Для подключения терминала к консольному порту, выполните следующие шаги:

1. Установите протокол терминала, как указано выше.
2. Подключите один из коннекторов кабеля RS-232 непосредственно к консольному порту устройства.
3. Подключите другой конец коннектора кабеля к терминалу или серийному коннектору компьютера, на котором установлено коммуникационное программное обеспечение.
4. Нажмите на терминале кнопку *enter*. На экране терминала должно появиться приглашение для регистрации (login prompt) в системе NetDefendOS.

Доступ к CLI по протоколу SSH (Secure Shell)

Протокол SSH (Secure Shell) используется для доступа к CLI с удаленного хоста в сети. Протокол SSH используется в первую очередь для обеспечения безопасности коммуникации незащищенных сетей, а также строгой аутентификации и целостности данных. SSH-клиенты доступны для большинства платформ.

Система NetDefendOS поддерживает версии 1, 1.5 и 2 SSH-протокола. Доступ по SSH-протоколу выполняется с помощью политики удаленного управления в NetDefendOS, и по умолчанию отключен.

Пример 2.2. Включение удаленного доступа по SSH-протоколу

Этот пример демонстрирует включение удаленного доступа по SSH-протоколу и сети lannet через интерфейс lan с помощью добавления правила в политику удаленного управления.

CLI

```
gw-world:/> add RemoteManagement RemoteMgmtSSH ssh Network=lannet
                                Interface=lan LocalUserDatabase=AdminUsers
```

Web-интерфейс

1. Зайдите **System > Remote Management > Add > Secure Shell Management**

2. Введите **Name (Имя)** для политики удаленного управления по SSH-протоколу, например, *ssh_policy*

3. Выберите следующее из списков выпадающего меню:

- **User Database:** AdminUsers
- **Interface:** lan
- **Network:** lannet

4. Нажмите **OK**

Регистрация в CLI

При доступе к интерфейсу командной строки CLI, установленном на NetDefendOS через серийную консоль или SSH-клиент, администратору необходимо зарегистрироваться в системе, прежде чем выполнить любую команду CLI. Данный шаг аутентификации необходим для обеспечения доступа к системе только доверенных пользователей, а также предоставления информации о пользователе для ведения контроля.

При удаленном доступе к интерфейсу командной строки CLI по SSH-протоколу, NetDefendOS отобразит инструкции по регистрации. Введите имя пользователя и нажмите клавишу *Enter*, далее введите пароль и снова нажмите *Enter*.

После успешной регистрации появится команда CLI:

```
gw-world:/>
```

Если ранее было установлено сообщение-приветствие, оно появится непосредственно после регистрации. В целях обеспечения безопасности рекомендуется отключить или анонимизировать приветственное сообщение CLI.

Изменение пароля пользователя *admin*

После первоначального запуска рекомендуется как можно скорее изменить пароль по умолчанию *admin* на любой другой. Пароль пользователя может быть любой комбинацией символов и не может содержать более 256 символов в длину. Рекомендуется использовать только печатные символы.

Для изменения пароля, например, *my-password,* используются следующие команды CLI. Прежде всего, необходимо изменить текущую категорию на *LocalUserDatabase* под названием *AdminUsers* (существует по умолчанию):

```
gw-world:/> cc LocalUserDatabase AdminUsers
```

В категории *AdminUsers* можно изменить пароль пользователя *admin:*

```
gw-world:/AdminUsers> set User admin Password="my-password"
```

В конечном итоге текущая категория возвращается на верхний уровень:

```
gw-world:/AdminUsers> cc
```

Примечание: Отдельный консольный пароль

Пароль, установленный для защиты прямого доступа к серийной консоли, - это отдельный пароль, который не следует путать с паролями учетных записей пользователей. Консольный пароль описан в Разделе 2.1.7 «Меню загрузки консоли».

Изменение CLI Prompt

CLI prompt по умолчанию:

```
gw-world:/>
```

где *Device* – это номер модели межсетевого экрана NetDefend. Он может быть создан пользователем, например, *my-prompt:/>,* с помощью команды CLI:

```
gw-world:/> set device name="my-prompt"
```

Руководство по интерфейсу командной строки CLI использует командную строку

gw-world:/>.

Совет:

Если значение командной строки изменено, эта строка также появляется в качестве нового имени устройства в самой верхней строке древовидного меню WebUI.

Активация и применение изменений

Если в текущих настройках с помощью CLI выполнены какие-либо изменения, данные изменения не будут загружены на NetDefendOS, пока не будет выполнена команда:

```
gw-world:/> activate
```

Непосредственно за командой *activate*, для применения изменений должна быть выполнена команда:

```
gw-world:/> commit
```

Если в течение 30 секунд (время по умолчанию) не выполнена команда *commit,* выполненные изменения автоматически отменяются, и происходит восстановление прежних настроек.

Проверка целостности настроек

После изменения настроек и перед выполнением команд *activate* и *commit,* можно выполнить проверку на наличие каких-либо проблем в настройках с помощью команды:

```
gw-world:/> show -errors
```

Система NetDefendOS просканирует настройки на проверку их активации и отобразит список проблем. Одна из возможных проблем, которая может быть обнаружена таким способом, – ссылка на IP-объект в Адресной книге, несуществующий в восстановленной резервной копии настроек.

Выход из CLI

После завершения работы в интерфейсе командной строки CLI, рекомендуется выйти из системы во избежание неавторизованного доступа к системе. Выход осуществляется с помощью команды *exit* или *logout*.

Настройка доступа для удаленного управления через интерфейс

Возможно, потребуется настроить доступ для удаленного управления через CLI. Доступ осуществляется через Ethernet-интерфейс *if2* с IP-адресом *10.8.1.34*.

Во-первых, устанавливаем значения объектов IP-адресов для *if2,* который уже существует в адресной книге NetDefendOS, начиная с IP-интерфейса:

```
gw-world:/> set Address IP4Address if2_ip Address=10.8.1.34
```

Следует установить подходящее значение IP-адреса сети для интерфейса:

```
gw-world:/> set Address IP4Address if2_net Address=10.8.1.0/24
```

В данном примере используются локальные IP-адреса, но вместо них могут также использоваться публичные IP-адреса.

Далее создайте объект удаленного HTTP-управления, в данном примере – *HTTP_if2*:

```
gw-world:/> add RemoteManagement RemoteMgmtHTTP HTTP_if2
                Interface=if2 Network=all-nets
                LocalUserDatabase=AdminUsers
                AccessLevel=Admin HTTP=Yes
```

Если активировать и применить новые настройки, станет доступным удаленное управление через IP-адрес *10.8.1.34* при использовании Web-браузера. Если требуется доступ к SSH-управлению, следует добавить объект *RemoteMgmtSSH*.

Учитывая вышеупомянутые команды, можно предположить, что существует маршрут *all-nets* к шлюзу провайдера Интернет-услуг. Другими словами, межсетевому экрану NetDefend открыт доступ в Интернет.

Сессии, управляемые с помощью *sessionmanager*

Интерфейс командной строки CLI предоставляет команду *sessionmanager* для самостоятельного управления сессиями. Команда используется для управления всеми типами сессий управления, включая:

- Сессии CLI по протоколу Secure Shell (SSH).
- Любая сессия CLI через интерфейс серийной консоли.
- Сессии по протоколу Secure Copy (SCP).
- Сессии Web-интерфейса по протоколу HTTP или HTTPS.

Команда без каких-либо опций предоставляет краткую информацию о текущих открытых сессиях:

```
gw-world:/> sessionmanager

Session Manager status
----------------------
Active connections          :       3
Maximum allowed connections :      64
Local idle session timeout  :     900
NetCon idle session timeout :     600
```

Для просмотра списка всех сессий используйте опцию *-list*. Ниже отображены типичные выходные данные локальной сессии:

```
gw-world:/> sessionmanager -list

User     Database          IP         Type    Mode     Access
-------- ---------------- ---------  ------- -------  --------
local    (none)           0.0.0.0    local   console  admin
```

Если пользователь обладает правами администратора, можно завершить любую сессию с помощью опции *-disconnect* команды *sessionmanager*.

Опции команды *sessionmanager* полностью представлены в *Руководстве по интерфейсу командной строки CLI.*

2.1.5. Сценарии CLI

Для простоты хранения и выполнения команд CLI администратором, NetDefendOS поддерживает функцию *CLI scripting*. *CLI script* – это предварительно определенная последовательность команд CLI, которые можно выполнить после их сохранения в файл и последующей загрузки файла на межсетевой экран NetDefend.

Выполните следующие шаги для создания CLI script:

1. Создайте текстовый файл с текстовым редактором, содержащим последовательный список команд, по одной на строку.

2. Для этих файлов D-Link рекомендует использовать расширение *.sgs* (S*ecurity* G*ateway* S*cript*). Имя файла, включая расширение, не должно содержать более 16 символов.

3. Загрузите файл на межсетевой экран NetDefend, используя Secure Copy (SCP). Файлы-сценарии должны храниться в папке *scripts*. Загрузка SCP подробно описана в Разделе 2.1.6, «Протокол Secure Copy».

4. Используйте команду CLI *script -execute* для запуска файла.

Команда CLI *script* – это инструмент, используемый для управления и применения сценариев. Полный синтаксис команды описан в *Руководстве по интерфейсу командной строки CLI,* а определенные примеры использования подробно представлены в последующих разделах. См. также *Раздел 2.1.4* «CLI» настоящего руководства.

Только четыре команды разрешены к использованию в сценариях:

add

set

delete

cc

Если в сценарии появляется любая другая команда, она игнорируется во время выполнения, при этом генерируется сообщение с предупреждением. Например, команда *ping* будет проигнорирована.

Выполнение сценариев

Как упоминалось выше, с помощью команды *script -execute* запускается назначенный файл сценария, предварительно загруженный на межсетевой экран. Например, для запуска файла сценария *my_script.sgs,* который был предварительно загружен, используется следующая команда CLI:

```
gw-world:/> script -execute -name=my_script.sgs
```

Переменные сценария

Файл сценария может содержать любое количество *переменных сценария*, которые выглядят следующим образом:

$1, *$2*, *$3*, *$4 $n*

Значения, используемые как имена переменных, определены в списке в конце командной строки *script -execute*. Число *n* в имени переменной указывает на положение значения переменной в списке. Первым идет значение *$1,* затем *$2* и т.д.

Примечание: Символ $0 является зарезервированным

Помните, что имя первой переменной $1. Переменная $0 является зарезервированной и перед выполнением всегда заменяется именем файла сценария.

Например, при выполнении сценария my_script.sgs все встречающиеся в нем ссылки $1 заменяются на IP адрес 126.12.11.01, а строка, содержащая адрес If1, подставляется в случае употребления $2.

Файл *my_script.sgs* содержит одну командную строку CLI:

```
add IP4Address If1_ip Address=$1 Comments=$2
```

Для запуска файла сценария после загрузки используется команда CLI:

```
> script -execute -name=my_script.sgs 126.12.11.01 "If1 address"
```

При запуске файла сценария замена переменной означает, что файл будет следующим:

```
add IP4Address If1_ip Address=126.12.11.01 Comments="If1 address"
```

Подтверждение сценария и порядок команд

По умолчанию, сценарии CLI не подтверждены. Это означает, что написание порядка сценариев не будет иметь значения. В начале сценария может быть ссылка на объект конфигурации, которая создается только в конце сценария. Несмотря на то, что это кажется нелогичным, это выполняется для улучшения читаемости сценариев. В случае, когда необходимо что-либо создать прежде, чем будет упомянута ссылка на этот объект, это может привести к запутанному и бессвязному файлу сценария; в файлах сценария с большим объемом предпочтительнее группировать аналогичные команды CLI.

Обработка ошибок

Если в существующем файле сценария встречается ошибка, по умолчанию, сценарий будет завершен. Завершение может быть прервано с помощью опции *-force.* Для запуска файла сценария *my_script2.sgs* таким способом, используется команда CLI:

```
gw-world:/> script -execute -name=my_script2.sgs -force
```

Если используется опция *-force,* выполнение сценария продолжается даже в том случае, если ошибки возвращены командой в файл сценария.

Выходные данные сценария

Все выходные данные выполненного сценария появятся в консоли CLI. Обычно эти выходные данные состоят из любых сообщений об ошибках, которые произошли во время выполнения. Для просмотра подтверждения выполнения каждой команды, используется опция *-verbose*:

```
gw-world:/> script -execute -name=my_script2.sgs -verbose
```

Сохранение сценариев

При загрузке файла сценария на межсетевой экран NetDefend, сначала он хранится только в памяти RAM. При перезапуске NetDefendOS все загруженные сценарии будут потеряны из энергозависимой памяти, и для их запуска потребуется повторная загрузка. Для хранения сценариев между перезапусками следует переместить их в энергонезависимую память NetDefendOS с помощью команды *script -store.*

Для перемещения примера *my_script.sgs* в энергонезависимую память используется команда:

```
gw-world:/> script -store -name=my_script.sgs
```

В качестве альтернативного варианта, все сценарии могут быть перемещены в энергонезависимую память с помощью команды:

```
gw-world:/> script -store -all
```

Удаление сценариев

Для того чтобы удалить сохраненный сценарий, используется команда *script –remove*.
Для того чтобы удалить файл сценария *my_script.sgs,* используется команда:

```
gw-world:/> script -remove   -name=my_script.sgs
```

Составление списков сценариев

Сам по себе *сценарий* является командой без каких-либо параметров, в нем отображен список всех

сценариев, доступных в настоящее время, и указан размер каждого сценария, а также тип памяти, в которой хранится сценарий (на хранение в энергонезависимой памяти указывает слово «*Disk*» в колонке *Memory).*

```
gw-world:/> script

Name            Storage       Size (bytes)
--------------  ------------  --------------
my_script.sgs   RAM           8
my_script2.sgs  Disk          10
```

Для создания списка содержимого определенного загруженного файла сценария, например, *my_script.sgs,* используется команда:

```
gw-world:/> script -show -name=my_script.sgs
```

Автоматическое создание сценариев

Когда необходимо скопировать одни и те же объекты конфигурации на несколько межсетевых экранов NetDefend, следует создать файл сценария, который создает необходимые объекты и затем загрузить и запустить один и тот же сценарий на каждом устройстве.

Если в NetDefendOS существуют объекты для копирования, запуск команды *script -create* обеспечивает автоматическое создание требуемого файла сценария. Данный файл сценария впоследствии может быть загружен на локальную рабочую станцию управления, а затем скачен и активирован на других межсетевых экранах NetDefend для дублирования объектов.

Например, требуется создать один и тот же набор объектов **IP4Address** на нескольких межсетевых экранах NetDefend, который уже существует на одном устройстве. Администратор подключается к одному устройству с помощью CLI и выполняет команду:

```
gw-world:/> script -create Address IP4Address -name new_script.sgs
```

При этом создается файл сценария с именем *new_script_sgs*, которое содержит все команды CLI, необходимые для создания всех объектов **IP4Address** в настройках устройства. Содержание созданного файла может быть, например, следующим:

```
add IP4Address If1_ip Address=10.6.60.10
add IP4Address If1_net Address=10.6.60.0/24
add IP4Address If1_br Address=10.6.60.255
add    IP4Address    If1_dns1    Address=141.1.1.1
             "
             "
             "
```

Файл *new_script_sgs* может быть впоследствии загружен с помощью SCP на локальную рабочую станцию управления и затем скачен и активирован на других межсетевых экранах NetDefend. В конечном результате, у всех устройств в адресных книгах будут находиться одни и те же объекты **IP4Address.**

Имя файла, созданного с помощью опции *-create* не может содержать более 16 символов в длину (включая расширение) с расширением *.sgs*.

Совет: Составление списков команд в консоли

Для внесения в список созданных команд CLI в консоли вместо сохранения их в файл, выключите опцию ***-name=*** *в команде* ***script -create****.*

Некоторые разновидности конфигурации, зависящие от аппаратного обеспечения, не могут содержать сценарий, созданный с использованием опции *-create.* Характерный тип узла CLI в команде *script -create* один из следующих:

COMPortDevice

Ethernet

EthernetDevice

Device

Если используется один из этих типов узлов, в таком случае система NetDefendOS отправляет сообщение об ошибке *script file empty*.

Комментарии к файлам сценария

Любая строка в файле сценария, которая начинается с символа *#,* рассматривается как комментарий. Например:

```
# The following line defines the If1 IP address

add IP4Address If1_ip Address=10.6.60.10
```

Сценарии, управляющие другими сценариями

Один сценарий может управлять другим. Например, сценарий *my_script.sgs* может содержать строку:

```
"
"
script -execute -name my_script2.sgs
"
"
```

Система NetDefendOS позволяет файлу сценария *my_script2.sgs* выполнить другой файл сценария и т.д. Максимальное количество вложенных сценариев – 5.

2.1.6. Протокол Secure Copy

Для скачивания или загрузки файлов на межсетевой экран или с него, может использоваться протокол *secure copy* (SCP). Протокол SCP основан на протоколе SSH и множестве свободно доступных SCP-клиентов, существующих практически для всех платформ. Примеры командной строки, представленные ниже, основаны на общем формате команд для SCP-клиента.

Формат команды SCP

Синтаксис команды SCP является простым для большинства клиентов на основе консоли. Основная команда, используемая здесь, *scp*, за которой следует источник и назначение для передачи файлов.

Скачивание выполняется с помощью команды:

```
>   scp <local_filename> <destination_firewall>
```

Загрузка выполняется по команде:

```
>   scp <source_firewall> <local_filename>
```

Адреса источника и назначения межсетевого экрана NetDefend представлены в виде:

<*user_name*>@<*firewall_ip_address*>:<*filepath*>.

Например: *admin@10.62.11.10:config.bak*.

<*user_name*> – это имя пользователя NetDefendOS в группе администраторов.

Примечание: Примеры SCP не отображают запрос пароля

SCP запросит пароль пользователя после командной строки, но этот запрос не отображен в представленных здесь примерах.

Следующая таблица суммирует операции, которые могут быть выполнены между SCP-клиентом и NetDefendOS:

Тип файла	Возможность скачивания	Возможность загрузки
Создание резервной копии настроек (config.bak)	Да (также через Web-интерфейс)	Да (также через Web-интерфейс)
Создание резервной копии системы (full.bak)	Да (также через Web-интерфейс)	Да (также через Web-интерфейс)
Обновление ПО	Да	Нет
Сертификаты	Да	Нет
Публичные SSH-ключи	Да	Нет
Файлы Web auth banner	Да	Да
Файлы Web content filter banner	Да	Да

Структурирование файлов в NetDefendOS

NetDefendOS поддерживает 2-х уровневую структуру каталога, которая состоит из верхнего уровня *root* и нескольких подкаталогов. Тем не менее, эти «каталоги» такие как *sshlclientkey* должны рассматриваться как *типы объектов*. Все файлы, хранящиеся в корневом каталоге NetDefendOS, также как и типы объектов, должны быть отображены с помощью команды CLI *ls*.

Итоговые данные отображены ниже:

```
gw-world:/> ls

HTTPALGBanners/

HTTPAuthBanners/

certificate/

config.bak

full.bak

script/

sshclientkey/
```

За исключением отдельных файлов, типы объектов в списке:

- *HTTPALGBanners/* - Файлы баннера для HTML-аутентификации пользователя. Скачивание файлов описано далее в *Разделе 6.3.4.4, «Настройка HTML-страниц».*
- *HTTPAuthBanner/* - Файлы баннера для динамической фильтрации HTML-содержимого ALG. Скачивание этих файлов описано далее в *Разделе 6.3.4.4, «Настройка HTML-страниц»*.
- *certificate/* - Тип объекта для всех цифровых сертификатов.
- *script/* - Тип объекта для сценариев CLI. Сценарии описаны далее в *Разделе 2.1.5, «Сценарии CLI»*.
- *sshclientkey/* - Тип объекта ключа SSH-клиента.

Примеры скачивания и загрузки

В некоторых случаях файл находится в корневой папке NetDefendOS. В эту категорию входят лицензионные файлы (*license.lic*), резервные копии настроек (*config.bak*) и полная резервная копия системы (*full.bak*). При скачивании эти файлы содержат уникальный идентифицирующий заголовок. Система NetDefendOS проверяет данный заголовок и обеспечивает хранение файла только в корневой папке (все файлы не содержат заголовок).

Если имя пользователя *admin1* и IP-адрес межсетевого экрана*10.5.62.11,* в таком случае, для

скачивания резервной копии конфигурационного файла используется команда SCP:

```
> scp config.bak admin1@10.5.62.11:
```

Для загрузки резервной копии конфигурационного файла в текущую локальную папку, используется команда:

```
> scp admin1@10.5.62.11:config.bak ./
```

Для скачивания файла в корневую папку под определенным типом, используемая команда немного отличается. Если файл сценария CLI *my_script.sgs*, для скачивания используется команда:

```
> scp my_script.sgs admin1@10.5.62.11:script/
```

Если тот же файл сценария CLI *my_script.sgs* хранится на межсетевом экране, для загрузки используется команда:

```
> scp admin1@10.5.62.11:script/my_script.sgs ./
```

Активация скаченных файлов

Как и все измененные настройки, скаченные файлы SCP активируются только после выполнения команд CLI *activate*, а затем команды *commit* для применения изменений.

Скаченные файлы обновленного программного обеспечения (в формате.*upg*) или полная резервная копия системы (*full.bak*) являются исключениями. Оба из этих типов файлов приводят к автоматической перезагрузке системы. Другим исключением являются скаченные файлы для сценариев, не влияющие на конфигурацию.

2.1.7. Меню перезагрузки консоли

Загрузчик NetDefendOS – это основное программное обеспечение для управления системой NetDefendOS, при этом интерфейс администратора называется *меню* перезагрузки *консоли* (также известный как *меню перезагрузки*). В данном разделе рассматриваются опции меню перезагрузки.

Доступ к меню перезагрузки консоли

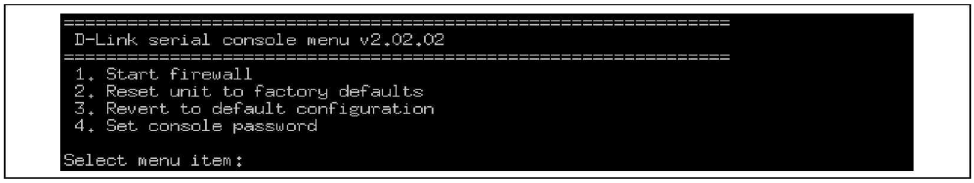
Меню перезагрузки доступно только через консоль устройства, подключенного непосредственно к серийному консольному порту межсетевого экрана NetDefend. Доступ осуществляется через консоль после включения межсетевого экрана NetDefend и запуска системы NetDefendOS.

После включения межсетевого экрана NetDefend запуск системы NetDefendOS произойдет через 3 секунды, в то же время появится сообщение *Press any key to abort and load boot menu (Нажмите любую кнопку для прерывания или загрузки меню перезагрузки),* отображенное ниже:

При нажатии любой консольной клавиши в течение 3 секунд, происходит остановка запуска системы NetDefendOS и отображается *меню перезагрузки консоли*.

Опции меню первоначальной загрузки без установки пароля

При первоначальном запуске системы NetDefendOS без установки консольного пароля для доступа к консоли, отображается полный набор опций загрузки меню, как показано ниже:



Следующие опции доступны в меню загрузки:

1. **Start firewall (Запуск межсетевого экрана)** Обеспечивает запуск программного обеспечения NetDefendOS на межсетевом экране NetDefend.

2. **Reset unit to factory defaults (Сброс устройства к заводским настройкам по умолчанию)**

   Опция обеспечивает сброс устройства к заводским настройкам по умолчанию. При выборе данной опции происходит следующее:

   - Риск безопасности консоли в случае отсутствия пароля консоли.
   - Восстановление по умолчанию выполняемых файлов совместно с настройками по умолчанию.

3. **Восстановление настроек по умолчанию**

   В данном случае выполняется восстановление только первоначальных настроек, файла с настройками по умолчанию NetDefendOS. Это не повлияет на остальные опции, например, безопасность консоли.

4. **Установка консольного пароля**
   Установка пароля для доступа к консоли. Пока пароль не установлен, любой пользователь может использовать консоль, таким образом, рекомендуется установить пароль как можно скорее. После установки пароля, консоль выполнит запрос пароля прежде, чем будет разрешен доступ к меню загрузки или интерфейсу командной строки (CLI).

Ниже представлены опции, появляющиеся после прерывания загрузки NetDefendOS при нажатии кнопки, в случае, если установлен консольный пароль.

Если выбрать опцию **Start firewall,** продолжится прерванный запуск системы NetDefendOS. При выборе опции **Login,** следует ввести консольный пароль, а также полностью меню загрузки, описанное выше.

Удаление консольного пароля

Однажды установленный пароль можно удалить, выбрав опцию *Set console password* в меню загрузки, оставив поле пароля незаполненным и нажав кнопку *Enter* для запроса.

Консольный пароль только для консоли

Установка пароля для консоли не связана с комбинацией имя пользователя/пароль, используемой

для доступа администратора через Web-браузер.

2.1.8. Расширенные настройки управления

В разделе Web-интерфейса **Удаленное управление** представлено несколько расширенных настроек:

SSH Before Rules

Включить SSH-трафик на межсетевом экране вне зависимости от настроенных IP-правил.

По умолчанию: *Включено*

WebUI Before Rules

Включить HTTP(S)-трафик на межсетевом экране вне зависимости от настроенных IP-правил.

По умолчанию: *Включено*

Таймаут при отсутствии активности локальной консоли

Количество секунд неактивности до автоматического выхода из системы пользователя локальной консоли.

По умолчанию: *900*

Таймаут ожидания подтверждения

Определяет количество секунд ожидания администратором регистрации прежде, чем вернуться к предыдущим настройкам.

По умолчанию: *30*

WebUI HTTP port

Определяет HTTP-порт для Web-интерфейса.

По умолчанию: *80*

WebUI HTTPS port

Определяет HTTP(S)-порт для Web-интерфейса.

По умолчанию: *443*

Сертификат для HTTPS

Определяет, какой сертификат используется для HTTPS-трафика. Поддерживаются только сертификаты RSA .

По умолчанию: *HTTPS*

2.1.9. Работа с настройками

Объекты конфигурации

Система конфигурации состоит из *Объектов конфигурации*, где каждый объект представляет конфигурируемый элемент любого вида. Примеры объектов конфигурации – записи в таблице маршрутизации, записи адресной книги, описание сервиса, IP-правила и т.д. Каждый объект конфигурации обладает набором свойств, которые составляют значения объекта.

Типы объектов

У объекта конфигурации четко определенный тип. Тип определяет свойства, доступные для объекта конфигурации, а также ограничения этих свойств. Например, тип *IP4Address* используется для всех объектов конфигурации, представляющих IPv4-адрес.

Структурирование объектов

В Web-интерфейсе объекты конфигурации систематизированы по принципу древовидной структуры на основе типа объекта.

В интерфейсе командной строки CLI, аналогичные типы объектов конфигурации группируются в *категорию*. Эти категории отличаются от структуры, используемой в Web-интерфейсе для обеспечения быстрого доступа к объектам конфигурации в CLI. Например, типы IP4Address, IP4Group и EthernetAddress группируются в категорию под названием *Address*, так как все они представляют различные адреса. Следовательно, объекты Ethernet и VLAN группируются в категорию *Interface*, так как они являются объектами интерфейса. В действительности, категории не влияют на системную конфигурацию; они являются всего лишь средствами, упрощающими администрирование.

Следующие примеры отображают способы управления объектами.

Пример 2.3. Внесение объектов конфигурации в список
Для выяснения того, какие объекты конфигурации существуют, можно восстановить список объектов. Этот пример отображает, как внести в список все объекты сервиса.

CLI

```
gw-world:/> show Service
```

Web-интерфейс

1. Зайдите **Objects > Services**

2. Отобразится Web-страница со списком всех сервисов, который содержит следующие основные элементы:

• **Add Button** - При нажатии появляется выпадающее меню. Меню отображает список всех типов объектов конфигурации, которые можно добавить.

• **Header** – Строка заголовка отображает названия колонок в списке. Небольшая стрелка рядом с каждым названием может использоваться для упорядочивания списка в соответствии с колонками.

• **Rows** – Каждая строка в списке соответствует одному объекту конфигурации. В основном, каждая строка начинается с имени объекта (если есть), за ним следуют значения колонок в списке.

Можно выбрать строку в списке, нажав на нее в месте, где нет гиперссылки. Фоновый цвет строки станет темно-синим. При нажатии на строку правой кнопкой мыши появляется меню, в котором можно выбрать изменение или удаление объекта, а также изменение порядка объектов.

Пример 2.4. Отображение объекта конфигурации

Самой простой операцией с объектом конфигурации является отображение его содержимого, другими словами, значения параметров объекта. Данный пример демонстрирует, как отобразить содержимое объекта конфигурации, представляющего сервис *telnet*.

CLI

```
gw-world:/> show Service ServiceTCPUDP telnet

         Property  Value
----------------  -------
             Name: telnet
 DestinationPorts: 23
             Type: TCP
      SourcePorts: 0-65535
         SYNRelay: No
   PassICMPReturn: No
              ALG: (none)
      MaxSessions: 1000
         Comments: Telnet
```

Колонка Property отображает список названий всех параметров в TCP/UDP сервисах, а колонка Value содержит значения соответствующих параметров.

Web-интерфейс

1. Зайдите **Objects > Services**

2. Нажмите на гиперссылку **telnet** в списке

3. Будет загружена Web-страница, отображающая сервис telnet

Примечание

При доступе к объекту через интерфейс командной строки CLI, можно пропустить имя категории и использовать только имя типа. Например, команда CLI в вышеуказанном примере может быть упрощена до:

```
gw-world:/> show ServiceTCPUDP telnet
```

Пример 2.5. Изменение объекта конфигурации

При необходимости изменить режим работы NetDefendOS, скорее всего, потребуется изменить один или несколько объектов конфигурации. Данный пример демонстрирует, как задать комментарий в поле *Comments* сервиса *telnet*.

CLI

```
gw-world:/> set Service ServiceTCPUDP telnet
                        Comments="Modified Comment"
```

Повторное отображение объекта для подтверждения значения нового параметра:

```
gw-world:/> show Service ServiceTCPUDP telnet Property  Value

         Property Value
---------------- -------
            Name: telnet
DestinationPorts: 23
            Type: TCP
     SourcePorts: 0-65535
        SYNRelay: No
  PassICMPReturn: No
             ALG: (none)
     MaxSessions: 1000
        Comments: Modified Comment
```

Web-интерфейс

1. Зайдите **Objects > Services**

2. Нажмите на гиперссылку **telnet** в списке

3. В поле **Comments** введите новый комментарий

4. Нажмите **OK** для подтверждения того, что в списке обновлен комментарий

Важно: Необходимо активировать измененные настройки

Изменения на объекте конфигурации не применяются до момента активации новых настроек NetDefendOS.

Пример 2.6. Добавление объекта конфигурации

Данный пример отображает, как добавить новый объект *IP4Address*, создав здесь IP-адрес *192.168.10.10*, для адресной книги.

CLI

```
gw-world:/> add Address IP4Address myhost Address=192.168.10.10
```

Отобразить новый объект:

```
gw-world:/> show Address IP4Address myhost

             Property Value
-------------------- -------------
                Name: myhost
             Address: 192.168.10.10
      UserAuthGroups: (none)
NoDefinedCredentials: No
            Comments: (none)
```

Web-интерфейс

1. Зайдите **Objects > Address Book**

2. Нажмите кнопку **Add**

3. В появившемся выпадающем меню выберите **IP-адрес**

4. В текстовом окне **Name** введите *myhost*

5. В текстовом окне **IP Address** введите 192.168.10.10

6. Нажмите **OK**

7. Подтвердите, что новый объект IP4 address добавлен в список

Пример 2.7. Удаление объекта конфигурации

Данный пример отображает, как удалить недавно добавленный объект IP4Address.

CLI

```
gw-world:/> delete Address IP4Address myhost
```

Web-интерфейс

1. Перейти в **Objects > Address Book**

2. Правой кнопкой мыши нажмите на строку, содержащую объект **myhost**

3. В появившемся выпадающем меню выберите **Delete**

Объект для удаления будет выделен зачеркнутым шрифтом.

Пример 2.8. Отмена удаления объекта конфигурации

Удаленный объект может быть восстановлен до момента активации и подтверждения настроек. Данный пример демонстрирует, как восстановить объект IP4Address, удаление которого показано в вышестоящем примере.

CLI

```
gw-world:/> undelete Address IP4Address myhost
```

Web-интерфейс

1. Зайдите **Objects > Address Book**

2. Правой кнопкой мыши нажмите на строку, содержащую объект **myhost**

3. В появившемся выпадающем меню выберите **Undo Delete**

Список измененных объектов

Возможно, после изменений нескольких объектов конфигурации, потребуется просмотреть список объектов, которые были изменены, добавлены и удалены с момента последнего подтверждения.

Пример 2.9. Список измененных объектов

Пример демонстрирует, как составить список измененных объектов конфигурации.

CLI

```
gw-world:/> show -changes
  Type           Object
  -------------  ------
- IP4Address     myhost
* ServiceTCPUDP  telnet
```

Символ «+» в начале строки указывает на то, что объект был добавлен. Символ «*» указывает на то, что объект был изменен. Символ «-» указывает на то, что объект отмечен для удаления.

Web-интерфейс

1. Зайдите **Configuration > View Changes** в строке меню

Появится список изменений

Активация и подтверждение настроек

После выполнения изменений в настройках необходимо выполнить активацию изменений, которые могут повлиять на работу системы. Во время активации выполняется проверка новых настроек, система NetDefendOS устанавливает в исходное положение подсистемы, на которые повлияли данные новых настроек.

Важно: Подтверждение изменений IPsec

Администратору следует знать, что при подтверждении любых изменений, которые могут повлиять на настройки туннелей IPsec, произойдет потеря соединений через туннели и потребуется их повторная установка.

После подтверждения новых настроек, система NetDefendOS выжидает некоторый период времени (30 секунд по умолчанию), в течение которого должно быть восстановлено соединение с администратором. Как указано ранее, если настройки активированы через CLI с помощью команды *activate*, далее следует выполнить команду *commit*. Если потерянное соединение не может быть восстановлено или команда *commit* не была выполнена, в таком случае, система NetDefendOS возвращается к использованию предыдущих настроек. Это отказоустойчивый механизм и, помимо прочего, с его помощью можно предотвратить блокировку удаленных администраторов.

Пример 2.10. Активация и подтверждение настроек

Данный пример демонстрирует, как активировать и подтвердить новые настройки.

CLI

```
gw-world:/> activate
```

Система подтвердит правильность новых настроек и введет их в эксплуатацию. Появится командная строка:

```
gw-world:/> commit
```

С этого момента зафиксированы изменения в новых настройках.

Web-интерфейс

1. Зайдите **Configuration > Save and Activate** в строке меню

2. Нажмите **OK** для подтверждения

Спустя 10 секунд Web-браузер автоматически попытается установить соединение через Web-интерфейс. Если соединение успешно установлено, система NetDefendOS воспримет это как подтверждение того, что удаленное управление по-прежнему работает. Далее новые настройки будут автоматически подтверждены.

Примечание: Необходимо подтвердить изменения

Перед сохранением изменений необходимо выполнить подтверждение настроек.
Если подтверждение не выполнено, изменения не сохраняются.

2.2.События и ведение журнала

2.2.1. Обзор

Ведение журнала и анализ функционирования системы является основной функцией NetDefendOS. Ведение журнала включает не только мониторинг статуса и работоспособности системы, но и проверку использования сети, что помогает при поиске и устранении неисправностей.

Генерирование сообщений для записи в Журнал

Система NetDefendOS определяет большое количество *сообщений для записи в Журнал событий,* сгенерированных в результате соответствующих системных событий. Например, установка и разрыв соединений, прием поврежденных пакетов, а также отклонение трафика в соответствии с политиками фильтрации.

Во всех случаях генерирования сообщения о событии, оно может быть отфильтровано и отправлено всем настроенным *Получателям события* (Event Receivers). Администратор может сконфигурировать несколько получателей события, у каждого из которых будет настраиваемый фильтр событий.

2.2.2. Сообщения для записи в Журнал

Типы событий

Система NetDefendOS определяет несколько сотен событий, после которых генерируются сообщения для записи в Журнал. События разделяются на высокоуровневые, настраиваемые пользователем, и низкоуровневые, например, системные события, выполняемые в обязательном порядке.

Событие *conn_open* event является типичным высокоуровневым событием, приводящим к генерированию сообщения при установке нового соединения, принимая во внимание то, что правило политики безопасности предусматривает генерирование сообщения о событии для данного соединения.

Примером низкоуровневого события является событие *startup_normal,* приводящее к генерированию сообщения сразу после запуска системы.

Формат сообщений

Все сообщения о событиях имеют общий формат, с атрибутами, включающими категорию, важность события и рекомендуемые действия. Использование данных параметров упрощает фильтрацию сообщений, либо в пределах NetDefendOS перед отправкой получателю события, либо как часть анализа после записи в Журнале и сохранения сообщения на внешнем сервере журнала.

Список всех сообщений о событиях находится в *Руководстве по записям Журнала NetDefendOS*. В данном руководстве описаны вид сообщений о событиях, значение уровня важности и различные доступные параметры.

Важность события

Важность каждого события определена заранее и является, в порядке важности, одной из:

Emergency (Аварийная ситуация)
Alert (Предупреждение об опасности)
Critical (Критическая ситуация)
Error (Ошибка)
Warning (Предупреждение)
Notice (Уведомление)
Info (Информация)
Debug (Отладка)

По умолчанию, NetDefendOS отправляет все сообщения уровня **Info (Информация)** и выше на настроенные серверы журнала. Категория **Debug (Отладка)** предназначена только для поиска и устранения неисправностей и должна быть включена, если она требуется при решении проблемы. Все сообщения для Журнала перечислены в *Руководстве по записям Журнала NetDefendOS*.

2.2.3. Log Receivers

Для того чтобы разместить и зарегистрировать сообщения о событиях в Журнале, необходимо назначить одного или более получателя события, определяющего *какие события* необходимо зафиксировать и *Журнал*, в который будет занесено уведомление о таких событиях.

NetDefendOS рассылает сообщения о событиях получателям различных типов, для этого необходимо создать объект *Log Receiver*:

- **MemoryLogReceiver**

  Система NetDefendOS поддерживает встроенный механизм ведения Журнала, известный как *MemLog*. В Журнале сохраняются все сообщения о событиях, а также доступен просмотр сообщений непосредственно через Web-интерфейс.

  Функция включена по умолчанию, но может быть отключена.

- **Syslog Receiver**

  Syslog – это стандарт регистрации событий, происходящих на сетевых устройствах. Если на серверах системного Журнала уже зарегистрированы события с других сетевых устройств, использование системного Журнала с сообщениями NetDefendOS может упростить общее управление.

  Данный тип получателя рассмотрен ниже в Разделе 2.2.5, «Запись сообщений в Syslog».

2.2.4. Запись сообщений в MemoryLogReceiver

MemoryLogReceiver (также известный как Memlog) – это дополнительная функция, которая позволяет записывать события непосредственно в память межсетевого экрана NetDefend вместо отправки сообщений на внешний сервер. Просмотр сообщений доступен через стандартный интерфейс пользователя.

Память журнала Memlog ограничена, ее размер предварительно определен и зафиксирован, т.к. ресурсы аппаратного обеспечения ограничены. При заполнении выделенного объема памяти старые сообщения удаляются, чтобы освободить место для новых входящих сообщений. Это означает, что Memlog вмещает ограниченное количество сообщений с момента последней инициализации системы и при заполнении буфера данные сообщения будут последними. Это означает, что при создании системой NetDefendOS большого количества сообщений в системах, с большим количеством VPN-туннелей, информация, хранящаяся в Memlog, становится менее значимой, так как она собрана за ограниченный период времени.

Отключение записи сообщений в память межсетевого экрана

В системе NetDefendOS объект *MemoryLogReceiver* существует по умолчанию. Если данный получатель не требуется, его можно удалить и данный тип записи событий будет отключен.

2.2.5. Запись сообщений в Syslog

Обзор

Syslog – это стандартизированный протокол отправки сообщений о происходящих в системе событиях, хотя стандартного формата для самих сообщений не существует. Формат, используемый NetDefendOS, хорошо подходит для автоматизированной обработки, фильтрации и поиска.

Хотя точный формат каждой записи зависит от работы получателя системного журнала, большинство сообщений похожи. Способ чтения журналов зависит от работы получателя системного журнала. На серверах UNIX демоны системного журнала обычно построчно записываются в текстовые файлы.

Формат сообщений

Большинство получателей системного журнала размещают в начале каждой записи отметку времени и IP-адрес компьютера, с которого отправлены данные:

```
Feb 5 2000 09:45:23 firewall.ourcompany.com
```

Данные сопровождаются текстом, выбранным отправителем:

```
Feb 5 2000 09:45:23 firewall.ourcompany.com EFW: DROP:
```

Последующий текст зависит от произошедшего события.

Для упрощения автоматизированной обработки всех сообщений, NetDefendOS записывает все данные в виде отдельной строчки текста. Все данные, следующие за исходным текстом, представлены в формате *имя=значение*. Благодаря этому автоматические фильтры легко находят необходимые значения без предположений, что часть данных находится в определенном месте записи в журнале.

Поля Prio и Severity

*Поле **Prio=** в сообщениях системного журнала содержит ту же информацию, что и поле **Severity** в сообщениях регистрирующего устройства D-Link. Тем не менее, порядок нумерации обратный.*

Пример 2.11. Включение записи событий в системный журнал

Для того чтобы включить запись всех событий с важностью более или равной Notice (Уведомление) на сервере системного журнала с IP-адресом 195.11.22.55, выполните шаги, указанные ниже:

CLI

```
gw-world:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Web-интерфейс

1. Зайдите **System > Log and Event Receivers > Add > Syslog Receiver**
2. Определите подходящее имя для ресивера события, например, *my_syslog*
3. Введите *195.11.22.55* в качестве **IP-адреса**
4. Выберите соответствующую функцию из списка **Facility** – имя функции, как правило, используется как параметр фильтра для большинства процессов-демонов системного журнала.
5. Нажмите **OK**

С этого момента система будет вносить в журнал все события с важностью более или равной Notice (Уведомление) на сервере системного журнала с IP-адресом *195.11.22.55*.

Примечание: Настройка сервера системного журнала

Сервер системного журнала может быть настроен на получение сообщений от NetDefendOS. Пожалуйста, обратитесь к документации по программному обеспечению сервера системного журнала, чтобы корректно выполнить настройки.

2.2.6. Сообщения SNMP Traps

SNMP-протокол

Протокол *Simple Network Management Protocol* (SNMP) используется для обмена информацией между Системой Управления Сетью (NMS) и управляемым устройством. SNMP определяет 3 типа

сообщений: команда *Read* для NMS, чтобы проверить управляемое устройство, команда *Write* для изменения статуса управляемого устройства и команда *Trap*, используемая управляемыми устройствами для неодновременной отправки сообщений об изменениях в NMS.

Сообщения SNMP Traps в NetDefendOS

Система NetDefendOS расширяет принцип реализации SNMP Trap, отправляя *любое* сообщение о событии как сообщение trap. Это означает, что администратор может настроить SNMP-уведомления о событиях, которые считаются важными для работы сети.

Компания D-Link предоставляет файл *DFLNNN-TRAP.MIB* (где *NNN* – номер модели межсетевого экрана), который определяет объекты SNMP и типы данных, используемые для описания уведомления SNMP Trap, полученного от NetDefendOS.

Примечание

Для каждой модели межсетевого экрана NetDefend существуют различные MIB-файлы. Убедитесь, что используется корректный файл.

Для каждой модели межсетевых экранов NetDefend существует один базовый объект с именем *DLNNNosGenericTrap*, используемый для всех сообщений traps (где *NNN* - номер модели). Данный объект содержит следующие параметры:

- *System* – Система, генерирующая сообщение trap
- *Severity* – Важность сообщения
- *Category* – Какая подсистема NetDefendOS сообщает о проблеме
- *ID* – Уникальный идентификатор в пределах категории
- *Description* – Короткое текстовое описание
- *Action* – Действие, предпринятое системой NetDefendOS

Эта информация может содержаться в перекрестной ссылке в *Руководстве по записям Журнала*.

Примечание: Стандартные сообщения SNMP Trap

NetDefendOS отправляет сообщения SNMP Traps на основе стандарта SNMPv2c, определенного RFC1901, RFC1905 и RFC1906.

Пример 2.12. Отправка сообщений типа SNMP Traps получателю SNMP (SNMP Trap Receiver)

Для того чтобы включить отправку сообщений SNMP traps для всех событий с важностью более или равной Alert (Предупреждение об опасности) получателю SNMP сообщений (SNMP trap receiver) с IP-адресом 195.11.22.55, выполните шаги, указанные ниже:

CLI

```
gw-world:/> add LogReceiver EventReceiverSNMP2c my_snmp
IPAddress=195.11.22.55
```

Web-интерфейс

1. Зайдите **Log & Event Receivers > Add > SNMP2cEventReceiver**

2. Определите имя для получателя события, например, *my_snmp*

3. Введите 195.11.22.55 в качестве **IP-адреса**

4. Введите SNMP **Community String**, если требуется

5. Нажмите **OK**

С этого момента система будет отправлять сообщения SNMP traps для всех событий с важностью более или равной Alert (Предупреждение об опасности) получателю SNMP сообщений (SNMP trap receiver) с IP-адресом 195.11.22.55.

2.2.7. Расширенные настройки журнала

Администратору доступны следующие расширенные настройки журналирования:

Настройка Send Limit

С помощью данной настройки можно ограничить количество пакетов в секунду, отправляемых системой NetDefendOS. Данная величина не должна быть слишком низкой или слишком высокой, так как это может привести к тому, что важные события не будут зарегистрированы.

Если установлено слишком большое значение и NetDefendOS отправляет сообщение на сервер, Log Receiver которого не активен, это может привести к повреждениям. Сервер отправит ответное сообщение *ICMP Unreachable (ICMP недоступен),* что может привести к отправке системой NetDefendOS другого сообщения, которое, в свою очередь, приведет к еще одному ответному сообщению *ICMP Unreachable (ICMP недоступен)* и т.д. Ограничивая количество сообщений, отправляемых в секунду системой NetDefendOS, администратор может избежать нерационального использования полосы пропускания.

По умолчанию: *3600* (в час)

Интервал между повторяющимися уведомлениями

Интервал в секундах между уведомлениями при использовании продолжительного уведомления. Минимум 0, Максимум 10 000.

По умолчанию: *60* (одна минута)

2.3. Сервер учета RADIUS Accounting

2.3.1. Обзор

В пределах сети с большим количеством пользователей наиболее выгодно использовать один центральный сервер или группу серверов, содержащих информацию об учетной записи пользователя и ответственных за аутентификацию и задачи авторизации. Центральная база данных, принадлежащая указанному серверу (-ам), содержит данные обо всех пользователях, а также подробную информацию о подключениях, что значительно упрощает работу администратора. Протокол RADIUS (*Remote Authentication Dial-in User Service)* – это протокол AAA (*Authentication, Authorization и Accounting)*, широко используемый системой NetDefendOS для выполнения вышеперечисленных функций.

Архитектура сервера RADIUS

Протокол RADIUS основан на архитектуре клиент/сервер. Межсетевой экран NetDefend действует

как клиент сервера RADIUS, создавая и отправляя запросы на определенные серверы. В терминологии RADIUS межсетевой экран действует в качестве *Network Access Server* (NAS).

Для аутентификации пользователя сервер RADIUS получает запросы, подтверждает информацию о пользователе, сверяясь с базой данных, и отправляет клиенту ответ «принять» или «отклонить». В соответствии с RFC2866 протокол RADIUS обеспечивает управление доставкой информации об учетных данных и это является стандартом для системы NetDefendOS (для получения более подробной информации об использовании сервера RADIUS для аутентификации NetDefendOS, см. *Раздел 8.2, «Настройка аутентификации»*).

2.3.2. Сообщения сервера RADIUS Accounting

Во время сессий на сервере RADIUS выполняется обновление и хранение статистики, например, количества отправленных или полученных байт, количество отправленных и полученных пакетов. В случае закрытия соединения с аутентифицированным пользователем выполняется обновление статистики.

Если сессия нового клиента начинается с установления нового соединения с помощью межсетевого экрана NetDefend, NetDefendOS отправляет сообщение *AccountingRequest* **START** на назначенный сервер RADIUS, для записи о начале новой сессии. Информация об учетной записи пользователя также доставляется на сервер RADIUS. Сервер отправляет системе NetDefendOS сообщение *AccountingResponse*, подтверждая, что сообщение было получено.

В случае если аутентификация пользователя больше не выполняется, например, при выходе пользователя из системы или истечении времени сессии, система NetDefendOS отправляет сообщение *AccountingRequest* **STOP,** содержащее статистику соответствующей сессии. Информация, содержащаяся в этой статистике, является конфигурируемой пользователем. Подробное содержимое сообщений **START** и **STOP** представлено ниже:

Параметры сообщения START

Параметры сообщения **START,** отправленного системой NetDefendOS, являются следующими:

- **Type** – Отмечает данный запрос AccountingRequest как оповещение о начале обслуживания (START).
- **ID** – Уникальный идентификатор для включения соответствия AccountingRequest с Acct-Status-Type, установка на STOP.
- **User Name** – Имя аутентифицированного пользователя.
- **NAS IP Address –** IP-адрес межсетевого экрана NetDefend.
- **NAS Port –** NAS-порт, на котором аутентифицирован пользователь (физический порт, не являющийся ни TCP-портом, ни UDP-портом).
- **User IP Address** – IP-адрес аутентифицированного пользователя. Отправляется только в случае определения на сервере аутентификации.
- **How Authenticated** – Способ аутентификации пользователя. Установлено либо *RADIUS,* если пользователь аутентифицирован через сервер RADIUS, либо *LOCAL,* если пользователь аутентифицирован через локальную базу данных пользователя.
- **Delay Time** – Время задержки (в секундах) с момента отправки пакета AccountingRequest и получения подтверждения аутентификации. Это значение можно вычесть из времени прибытия пакета на сервер, чтобы выяснить приблизительное время события, по причине которого сгенерировано данное сообщение AccountingRequest. Помните, что при этом не отображаются сетевые задержки. При первой попытке значение параметра – 0.

• **Timestamp** – Количество секунд с 1-ого января, 1970 года. Используется для установки отметки о времени отправки пакета из NetDefendOS.

Параметры сообщения STOP

Параметры сообщения **STOP,** отправленного системой NetDefendOS:

• **Type** - Отмечает данный запрос AccountingRequest как оповещение о завершении обслуживания (STOP).

• **ID** - Уникальный идентификатор для соответствия предварительно отправленного пакета AccountingRequest с Acct-Status-Type, установка на START.

• **User Name** – Имя аутентифицированного пользователя.

• **NAS IP Address** – IP-адрес межсетевого экрана NetDefend.

• **NAS Port** – NAS-порт, на котором аутентифицирован пользователь (это физический порт, не являющийся ни TCP, ни UDP-портом).

• **User IP Address** – IP-адрес аутентифицированного пользователя. Отправляется только в случае определения сервера аутентификации.

• **Input Bytes** – Количество байтов, полученных пользователем. (*)

• **Output Bytes** – Количество байтов, отправленных пользователем. (*)

• **Input Packets** – Количество пакетов, полученных пользователем. (*)

• **Output Packets** – Количество пакетов, отправленных пользователем. (*)

• **Session Time** – Длительность сессии в секундах. (*)

• **Termination Cause** – Причина завершения сессии.

• **How Authenticated** – Способ аутентификации пользователя. Установлено либо *RADIUS,* если пользователь аутентифицирован через сервер RADIUS, либо *LOCAL,* если пользователь аутентифицирован через локальную базу данных пользователя.

• **Delay Time** – См. комментарии выше.

• **Timestamp** – Количество секунд с 1 января 1970 года. Используется для установки отметки о времени отправки пакета с межсетевого экрана NetDefend.

Помимо этого, могут быть отправлены еще два параметра:

• **Input Gigawords** – Данный параметр возвращает значение счетчика входящих байт.

• **Output Gigawords** – Данный параметр возвращает значение счетчика исходящих байт.

Совет: Значение символа «звездочка» (*) после записи в списке

Символ «звездочка» (*) после записи в вышеуказанном списке свидетельствует о том, что отправка параметра является дополнительной и настраиваемой.

2.3.3. Промежуточные сообщения (Interim Accounting Messages)

Помимо сообщений **START** и **STOP** система NetDefendOS может периодически дополнительно отправлять *промежуточные сообщения (Interim Accounting Messages)* для обновления текущего статуса пользователя на сервере учета. Сообщение *Interim Accounting Message* можно рассмотреть как краткую текущую характеристику сетевых ресурсов, используемых аутентифицированным пользователем до заданного уровня. Благодаря данной функции сервер RADIUS может вести учет количества байт и пакетов, отправленных и полученных пользователем до момента отправки последнего сообщения.

Сообщение *Interim Accounting Message* содержит текущие значения статистики для аутентифицированного пользователя. Сообщение содержит почти те же параметры, что и сообщение AccountingRequest Stop, за исключением атрибута *Acct-Terminate-Cause* (так как пользователь еще не завершил сеанс).

Частота отправки сообщений *Interim Accounting Messages* может быть определена на сервере аутентификации или в NetDefendOS. Переключение на настройку в NetDefendOS отменит настройку на сервере учета.

2.3.4. Активация RADIUS Accounting

Для активации RADIUS accounting необходимо выполнить следующие шаги:

- Необходимо определить сервер RADIUS accounting.
- Объект аутентификации пользователя должен иметь правило, связанное с определением сервера RADIUS.

Необходимо отметить некоторые важные моменты активации:

- Сервер учета RADIUS Accounting не функционирует, если на соединение распространяется правило *FwdFast,* находящееся в наборе IP-правил.
- Нет необходимости в том, чтобы один и тот же сервер RADIUS управлял и аутентификацией, и учетными записями; один сервер является ответственным за аутентификацию, в то время как другой – за учетные записи.

В NetDefendOS можно настроить несколько серверов RADIUS для работы с событием, если основной сервер недоступен.

2.3.5. Безопасность RADIUS Accounting

Общий секретный ключ обеспечивает защиту коммуникации между NetDefendOS и любым сервером учета RADIUS accounting. Этот ключ никогда не пересылается через сеть и 16-байтное значение длины Кода аутентификации (*Authenticator code*) вычисляется с помощью MD5 хэш-функции, которое используется для аутентификации учетных записей.

Общий секретный ключ является чувствительным к регистру, может содержать до 100 символов, следует вводить один и тот же ключ для NetDefendOS и для сервера RADIUS.

Сообщения отправляются по UDP-протоколу, номер порта по умолчанию 1813 и является конфигурируемым пользователем.

2.3.6. Сервер учета RADIUS Accounting и высокая отказоустойчивость

В отказоустойчивом кластере учетная информация записях синхронизирована между активным и пассивным межсетевыми экранами NetDefend. Это означает, что учетная информация, автоматически обновляется на обоих узлах кластера при потере соединения. Активное устройство использует два определенных учетных события для синхронизации с пассивным устройством:

Каждый раз при получении ответа с учетного сервера, уведомление о начале соединения, **AccountingStart**, отправляется на неактивный узел в отказоустойчивом кластере. Это определяет необходимость хранения учетной информации для определенного аутентифицированного пользователя.

Трудности с синхронизацией учетной информации могут возникнуть в случае, если на активном устройстве прошел аутентификацию пользователь, сессия которого отключается по таймауту до начала синхронизации на пассивном устройстве. Для того чтобы решить эту проблему, во время таймаута на пассивное устройство отправляется уведомление о событии **AccountingUpdate,** содержащее последние учетные данные для соединений.

2.3.7. Операции с не отвечающими серверами

Проблема возникает в случае, если сервер RADIUS не отвечает на пакет *AccountingRequest* **START,** отправленный клиентом. Система NetDefendOS повторно отправляет запрос после количества секунд, определенного пользователем. Это означает, что у пользователя по-прежнему сохранен доступ в то время как система NetDefendOS пытается связаться с сервером учета.

Только после трех неудачных попыток системы NetDefendOS связаться с сервером, можно сделать вывод, что сервер недоступен. Администратор может использовать расширенную настройку **Allow on error** для того, чтобы принять соответствующие меры. Если настройка включена, то сессия аутентифицированного пользователя не будет прервана. Если настройка выключена, любой пользователь будет автоматически выведен из системы, даже если он уже аутентифицирован.

2.3.8. Выключение системы и отчетность

В случае если по каким-либо причинам клиенту не удалось отправить пакет RADIUS *AccountingRequest* **STOP,** сервер никогда не сможет обновить статистику пользователя, однако, сессия при этом остается активной. Следует не допускать таких ситуаций.

Если администратор межсетевого экрана NetDefend выполняет команду выключения в то время, когда аутентифицированные пользователи остаются в режиме онлайн, возможно, что пакет *AccountingRequest* **STOP** никогда не будет отправлен. Во избежание этой ситуации расширенная настройка **Logout at shutdown** позволяет администратору указать, что до начала выключения система NetDefendOS должна отправить сообщение **STOP** любому аутентифицированному пользователю на любой настроенный сервер RADIUS.

2.3.9. Ограничения NAT

Модуль аутентификации пользователя в системе NetDefendOS основан на IP-адресе пользователя. Если у пользователей одинаковые IP-адреса, могут возникнуть проблемы.

Проблема может возникнуть, если, например, несколько пользователей позади одной и той же сети используют NAT, чтобы разрешить сетевой доступ через один внешний IP-адрес. Это означает, что как только пользователь прошел аутентификацию, можно предположить, что трафик, проходящий через NAT (с указанием IP-адреса), является исходящим от аутентифицированного пользователя, даже если он идет от других пользователей в той же сети. По этой причине NetDefendOS RADIUS Accounting начнет собирать статистику для всех пользователей в сети, даже если присутствует только один пользователь вместо нескольких.

2.3.10. Расширенные настройки сервера RADIUS

Доступны следующие расширенные настройки сервера RADIUS:

Allow on error

Если при отправке учетных данных уже аутентифицированного пользователя сервер не отвечает, необходимо включить эту настройку для продолжения регистрации пользователя.

Выключение настройки приведет к тому, что пользователь будет выведен из системы, если сервер RADIUS недоступен, даже в случае предварительной аутентификации пользователя.

По умолчанию: *Включено*

Logout at shutdown (Выход из системы при выключении системы)

При выключении межсетевого экрана NetDefend администратором, система NetDefendOS не выполняет отключение, пока на любой сконфигурированный сервер RADIUS не будут отправлены сообщения **STOP**.

Если данная опция отключена, NetDefendOS выполнит выключение даже при наличии сессий, не завершенных корректно. Это может привести к тому, что сервер RADIUS предположит, что пользователи по-прежнему находятся в системе даже при завершенных сессиях.

По умолчанию: *Отключено*

Maximum Radius Contexts

Максимальное количество контекста, разрешенное на сервере RADIUS. Это относится к использованию учетных записей и аутентификации на сервере RADIUS.

По умолчанию: *1024*

Пример 2.13. Настройка сервера учета RADIUS Accounting

Данный пример демонстрирует настройку локального сервера RADIUS, известного как *radius-accounting* с IP-адресом *123.04.03.01* с использованием порта 1813.

Web-интерфейс

1. Зайдите **User Authentication > Accounting Servers > Add > Radius Server**
2. Введите:
• **Name:** radius-accounting
• **IP Address:** 123.04.03.01
• **Port:** 1813
• **Retry Timeout:** 2
• **Shared Secret:** *введите пароль*
• **Confirm Secret:** *повторно введите пароль*
• **Routing Table:** main

3. Нажмите **OK**

2.4. Мониторинг аппаратного обеспечения

Работоспособность

Некоторые модели аппаратного обеспечения D-Link позволяют администратору с помощью командной строки CLI выполнить запрос текущего значения различных параметров аппаратного обеспечения, например, текущую внутреннюю температуру межсетевого экрана. Эта функция называется *Мониторинг аппаратного обеспечения*.

Модели D-Link NetDefend, поддерживающие мониторинг устройств: DFL-1600, 1660, 2500, 2560 и 2560G.

Настройка и мониторинг устройства могут быть выполнены как с помощью командной строки CLI, так и через Web-интерфейс.

Включение мониторинга аппаратного обеспечения

Раздел **System > Hardware Monitoring** в Web-интерфейсе обеспечивает администратору следующие настройки для включения мониторинга устройства:

Включить датчики

Включить/Отключить мониторинг аппаратного обеспечения.

По умолчанию: *Выключено*

Интервал опроса (Poll Interval)

Интервал опроса – это промежуток времени в миллисекундах между опросами аппаратного обеспечения.

Минимальное значение: *100*

Максимальное значение: *10000*

По умолчанию: *500*

Использование команды *hwm* CLI

Для получения списка текущих значений всех доступных счетчиков, может использоваться команда:

```
gw-world:/> hwm -all
```

Команда может быть сокращена до:

```
gw-world:/> hwm -a
```

Ниже отображены типичные выходные данные для двух температурных датчиков:

```
gw-world:/> hwm -a
Name Current value (unit)
-------------- --------------------
```

```
SYS Temp = 44.000 (C) (x)
CPU Temp = 41.500 (C) (x)
```

Примечание: Значение "(x)"

"(x)" в конце строки указывает на то, что датчик включен. Опция *-verbose* отображает текущие значения и настроенные диапазоны:

```
gw-world:/> hwm -a -v
2 sensors available
Poll interval time = 500ms
Name [type][number] = low_limit] current_value [high_limit (unit)
---------------------------------------------------------------
SYS Temp [TEMP ][ 0] = 44.000] 45.000 [ 0.000 (C)
CPU Temp [TEMP ][ 1] = 42.000] 42.500 [ 0.000 (C)
Time to probe sensors: 2.980000e-05 seconds
```

Каждый физический параметр, отображенный в списке слева, сопровождается минимальным и максимальным диапазоном, в котором он должен работать. Если после опроса значение превышает данный диапазон, система NetDefendOS создает дополнительное сообщение и отправляет его в журнал сервера.

Примечание: Различные устройства поддерживают различные датчики и диапазоны

Каждая модель аппаратного обеспечения поддерживает различные датчики и различный рабочий диапазон. Выходные данные и их значения, указанные выше, представлены в качестве примера.

Настройка минимального и максимального диапазонов

Минимальные и максимальные значения, указанные в выходных данных команды *hwm* установлены в Web-интерфейсе при переходе в **System > Hardware Monitoring > Add** и выборе параметра для мониторинга. Далее можно указать необходимый рабочий диапазон.

Датчик идентифицируется в Web-интерфейсе путем определения уникальной комбинации следующих параметров:

- **Тип**

Это *тип* датчика, отображенный в вышеуказанных выходных данных CLI и представленный в Web-интерфейсе как список вариантов. Например, *Temp*.

- **Датчик**

Это *Номер* датчика, указанный выше в выходных данных CLI. Например, номер *SYS Temp – 0*.

- **Имя**

Это *Имя* датчика, отображенное в вышеуказанных выходных данных. Например, *SYS Temp*.

- **Enabled**

С помощью этой настройки можно включить или отключить индивидуальный счетчик. Если счетчик включен, в строке выходных данных появляется символ "*(x)*".

2.5. Мониторинг SNMP

Обзор

Simple Network Management Protocol (SNMP) – это стандартный протокол для управления сетевыми устройствами. Соответствующий SNMP-клиент может подключиться к сетевому устройству, которое поддерживает SNMP-протокол для запросов и управления.

Система NetDefendOS поддерживает версию 1 и версию 2 SNMP-протокола. Подключение к устройствам, поддерживающим NetDefendOS, может быть выполнено любым SNMP-клиентом. Тем не менее, в целях безопасности разрешены операции только с запросами. Главным образом, NetDefendOS поддерживает следующие операции с SNMP-запросами, посылаемыми клиентом:

- Операция *GET REQUEST*
- Операция *GET NEXT REQUEST*
- Операция *GET BULK REQUEST* (только SNMP Версия 2c)

NetDefendOS MIB

Management Information Base (MIB) – это база данных, как правило, в виде файла, определяющая параметры на сетевом устройстве, которые SNMP-клиент может запросить или изменить. Файл MIB для устройства, работающего под управлением системы NetDefendOS, входит в стандартный пакет NetDefendOS как файл с именем *DFLNNN-TRAP.MIB* (где *NNN* – номер модели межсетевого экрана), который должен быть перенесен на жесткий диск рабочей станции с настроенным SNMP-клиентом. При запуске клиента открыт доступ к файлу MIB, который может содержать информацию о значениях, запрашиваемых на устройстве NetDefendOS.

Определение SNMP-доступа

SNMP-доступ определяется через объект NetDefendOS *Remote* со значением SNMP *Mode*. Объекту Remote требуется:

- **Interface –** Интерфейс NetDefendOS, на который приходят SNMP-запросы.
- **Network** – IP-адрес или сеть, откуда приходят SNMP-запросы.
- **Community** – Строка community, которая предоставляет пароль для доступа.

Строка Community

Строка *Community String* обеспечивает защиту SNMP версий 1 и 2c и является тем же, что и пароль для SNMP-доступа. Следует создавать **строку Community String, которую трудно подобрать,** и которая создана тем же способом, что и любой другой пароль, с использованием комбинаций цифр и букв верхнего и нижнего регистра.

Включение IP-правила для SNMP

С помощью расширенной настройки **SNMP Before Rules** в разделе **RemoteAdmin** можно контролировать, выполняется ли проверка доступа по SNMP в соответствии с набором IP-правил. Настройка по умолчанию отключена, рекомендуется всегда включать данную настройку.

Результатом включения настройки будет добавление невидимого правила **Allow** в набор IP-правил, который автоматически разрешает доступ на порту 161 из сети и на интерфейсе, определенном для

SNMP-доступа. Порт 161 обычно используется для SNMP и на этом порту система NetDefendOS ожидает SNMP-трафик.

Шифрование удаленного доступа

Следует отметить, что доступ по протоколу SNMP версий 1 или 2c access означает, что строка community будет отправлена как читаемый текст. При работе удаленного клиента в публичной сети Internet это является небезопасным. Поэтому желательно иметь удаленный доступ через зашифрованный туннель VPN или аналогичное защищенное средство коммуникации.

Предотвращение перегрузок SNMP

Расширенная настройка **SNMP Request Limit** ограничивает количество разрешенных SNMP-запросов в секунду. Таким образом, можно предотвратить атаки, приводящие к перегрузке.

Пример 2.14. Включение мониторинга SNMP

Данный пример включает доступ по протоколу SNMP через внутренний интерфейс **lan** из сети **mgmt-net**, с использованием командной строки *Mg1RQqR*. (Так как клиент управления находится во внутренней сети, нет необходимости создавать VPN-туннель.)

CLI

```
gw-world:/> add RemoteManagement RemoteMgmtSNMP my_snmp Interface=lan
Network=mgmt-net SNMPGetCommunity=Mg1RQqR
```

Если необходимо включить **SNMPBeforeRules** (отключено по умолчанию), используется команда:

```
gw-world:/> set Settings RemoteMgmtSettings SNMPBeforeRules=Yes
```

Web-интерфейс

1. Зайдите **System > Remote Management > Add > SNMP management**

2. Для **Remote access type** введите:

• **Name:** соответствующее имя
• **Community:** Mg1RQqR

3. Для **Access Filter** введите:

• **Interface:** lan
• **Network:** mgmt-net

4. Нажмите **OK**

Если требуется включить **SNMPBeforeRules** (отключено по умолчанию), необходимая настройка находится в **System > Remote Management > Advanced Settings**.

2.5.1. Расширенные настройки SNMP

Следующие расширенные настройки SNMP находятся в разделе **Удаленное управление** в WebUI.

SNMP Before RulesLimit

Включить SNMP-трафик независимо от настроенных IP-правил.

По умолчанию: *Включено*

Ограничение SNMP-запросов

Существует определенное максимальное количество запросов SNMP, которое будет обрабатываться каждую секунду системой NetDefendOS. Если количество SNMP-запросов превышает этот показатель, то система NetDefendOS будет игнорировать лишние запросы.

По умолчанию: *100*

System Contact

Контактное лицо для управляемого узла.

По умолчанию: *N/A*

System Name

Имя управляемого узла.

По умолчанию: *N/A*

System Location

Физическое расположение узла.

По умолчанию: *N/A*

Описание интерфейса (SNMP)

Данные, отображаемые в SNMP MIB-II ifDescr variables.

По умолчанию: *Name*

Интерфейс Alias

Данные, отображаемые в SNMP ifMIB ifAlias variables.

По умолчанию: *Hardware*

2.6. Команда pcapdump

Важным инструментом диагностики является проверка пакетов, проходящих через интерфейсы межсетевого экрана NetDefend. С этой целью система NetDefendOS поддерживает команду *pcapdump*, которая не только позволяет выполнить проверку потоков пакетов, проходящих через интерфейсы, но также фильтрацию этих потоков в соответствии с определенными критериями.

Пакеты, отфильтрованные с помощью команды *pcapdump,* могут быть сохранены в файл с расширением *.cap,* который фактически является стандартным форматом файла для библиотеки *libpcap* при захвате пакетов.

Полный синтаксис команды *pcapdump* представлен в *Руководстве по интерфейсу командной строки CLI*.

Пример

Примером использования *pcapdump* является следующая последовательность:

```
gw-world:/> pcapdump -size 1024 -start int
gw-world:/> pcapdump -stop int
gw-world:/> pcapdump -show
gw-world:/> pcapdump -write int -filename=cap_int.cap
gw-world:/> pcapdump –cleanup
```

При просмотре строк можно сделать вывод, что:

1. Запись начинается для интерфейса *int* с использованием размера буфера 1024 Кбайт.

```
gw-world:/> pcapdump -size 1024 -start int
```

2. Запись прекращается для интерфейса *int*.

```
gw-world:/> pcapdump -stop int
```

3. Исходящий дамп отображается в консоли в суммарной форме.

```
gw-world:/> pcapdump -show
```

4. Та же информация записана в полной форме в файле с названием *cap_int.cap*.

```
gw-world:/> pcapdump -write int -filename=cap_int.cap
```

С этой точки зрения, файл *cap_int.cap* должен быть загружен на рабочую станцию управления для дальнейшего анализа.

5. Выполняется окончательная очистка и освобождение объема занятой памяти.

```
gw-world:/> pcapdump -cleanup
```

Повторное использование файлов сбора данных

Так как единственным способом удаления файлов с межсетевого экрана NetDefend является удаление через серийную консоль, рекомендуется всегда использовать одно и то же имя файла при использовании опции pcapdump -*write.* Каждая новая запись будет зарегистрирована поверх старой.

Работа с несколькими интерфейсами

С помощью команды *pcapdump* можно выполнять несколько операций одновременно. Описание данной функции представлено в следующих пунктах:

1. Вся информация после выполнения всех операций переходит в один и тот же буфер памяти.

Команда может быть выполнена несколько раз с указанием различных интерфейсов. В таком случае поток пакетов для различных операций будет собран в различных разделах отчета.

Если требуется детальная информация о потоке пакетов между интерфейсами, следует выполнить команду *pcapdump* с указанием интерфейсов, представляющих интерес.

2. Если интерфейс не указан, в таком случае, сбор данных и информации выполняется на всех интерфейсах.

3. Если интерфейс не указан, с помощью опции -*stop* сбор данных прекращается на всех интерфейсах.

4. Команда *pcapdump* не выполняет повторный сбор данных на одном и том же интерфейсе при дублировании команды.

Диалоговое окно Filter Expressions

Просмотр всех пакетов, проходящих через определенный интерфейс, дает избыток полезной информации. Для того чтобы сфокусироваться на определенных типах трафика команда *pcapdump* поддерживает опцию добавления выражений в строку описания фильтра в одной из следующих форм:

-*eth*=<*macaddr*> - Фильтрация по MAC-адресу источника или назначения.

-*ethsrc*=<*macaddr*> - Фильтрация по MAC-адресу источника.

-*ethdest*=<*macaddr*> - Фильтрация по MAC-адресу назначения

-*ip*=<*ipaddr*> - Фильтрация по IP-адресу источника или назначения.

-*ipsrc*=<*ipaddr*> - Фильтрация по IP-адресу источника.

-*ipdest*=<*ipaddr*> - Фильтрация по IP-адресу назначения.

-*port*=<*portnum*> - Фильтрация по номеру порта источника или назначения.

-*srcport*=<*portnum*> - Фильтрация по номеру порта источника.

-*destport*=<*portnum*> - Фильтрация по номеру порта назначения.

-*proto*=<*id*> - Фильтрация по протоколу, где идентификатор представляет собой десятичное значение.

-<*protocolname*> - Вместо номера протокола, может быть определено только имя протокола как -*tcp*, -*udp* или -*icmp*.

Загрузка выходного файла

Как показано в одном из вышестоящих примеров, с помощью опции -*write* команды *pcapdump* можно сохранить информацию о буферизованном пакете в файл на межсетевом экране NetDefend.

Данные выходные файлы находятся в корневой папке NetDefendOS и имя файла определено в командной строке *pcapdump,* как правило, с расширением *.cap*. Имена выходных файлов должны соответствовать некоторым правилам, которые описаны ниже. Файлы могут быть загружены на локальную рабочую станцию с помощью Secure Copy (SCP) (см. Раздел 2.1.6, «Протокол Secure Copy»). Список всех файлов, хранящихся в корневой папке NetDefendOS можно просмотреть, выполнив команду *ls* CLI.

С помощью опции *–cleanup* можно удалить все файлы, сохраненные с помощью команды *pcapdump* (а также с помощью ранее используемых команд), таким образом, следует выполнять очистку только после завершения загрузки файла.

Примечание: NetDefendOS ведет учет сохраненных файлов

NetDefendOS ведет учет файлов, созданных *с помощью команды* ***pcapdump.*** *Это выполняется даже при перезагрузке системы, так как опция очистки the* ***-cleanup*** *может удалить все файлы из памяти межсетевого экрана.*

Ограничения для имени файла вывода

Имя файла, используемое для исходящего дампа pcap, должно соответствовать следующим правилам:

- Имя файла (без расширения) не должно превышать 8 символов в длину.
- Расширение имени файла не должно превышать 3 символа в длину.
- Имя файла и расширение могут содержать только символы A-Z, 0-9, "-" и "_".

Совместное использование фильтров

Возможно совместное использование нескольких фильтров в целях дальнейшей детализации пакетов, представляющих интерес. Например, если требуется проверка пакетов, адресованных на определенный порт назначения по определенному IP-адресу назначения.

Совместимость с приложением Wireshark

Программа с открытым исходным кодом *Wireshark* (ранее известная как *Ethereal*) используется для анализа захваченных пакетов. Приложение Wireshark использует библиотеку *Pcap*.

Для получения более подробной информации о программе Wireshark, посетите сайт http://www.wireshark.org.

2.7. Обслуживание

2.7.1. Механизм автоматического обновления

Некоторые функции безопасности системы NetDefendOS задействуют внешние серверы для автоматического обновления и фильтрации содержимого. Системе определения и предотвращения вторжений и антивирусным программам требуется доступ к обновленным базам данных сигнатур для обеспечения защиты от угроз.

Для упрощения функции автоматического обновления D-Link поддерживает международную инфраструктуру серверов, предоставляющих сервисы обновления для межсетевых экранов NetDefend. Для обеспечения доступности и короткого времени отклика система NetDefendOS использует механизм автоматического выбора наиболее подходящего сервера для выполнения обновлений.

Для получения более подробной информации об этих функциях обратитесь к следующим разделам:

- *Раздел 6.5, «Определение и Предотвращение вторжений»*
- *Раздел 6.4, «Антивирусное сканирование»*
- *Раздел 6.3, «Фильтрация Web-содержимого»*

2.7.2. Резервное копирование настроек

Администратор обладает возможностями зафиксировать состояние системы NetDefendOS на определенный момент и восстановить его, если это необходимо. Фиксирование может быть двух типов:

- *Резервная копия настроек*, которая не содержит установленную версию NetDefendOS. Функция является полезной, если версия NetDefendOS не изменяется.
- *Резервная копия системы*, которая является полной резервной копией и настроек, и установленного программного обеспечения NetDefendOS. Функция является полезной, если

необходимо изменение настроек и обновление версии NetDefendOS.

Можно создать резервные копии файлов, загрузив файлы непосредственно с межсетевого экрана NetDefend, используя SCP (Secure Copy) или WebUI. Невозможно выполнить загрузку через интерфейс командной строки CLI.

Прерывание операции

Резервные копии могут быть созданы в любое время без вмешательства в режим работы NetDefendOS. После восстановления резервной копии необходимо выполнить команду **Activate** для активации восстановленной конфигурации/системы.

Восстановление и активация резервной копии только с настройками не помешает работоспособности системы. Восстановление целой системы потребует повторной инициализации системы NetDefendOS, с потерей всех существующих соединений. В зависимости от типа аппаратного обеспечения завершение инициализации может занять несколько секунд, в течение этого времени эксплуатация невозможна.

Резервное копирование и восстановление с помощью SCP

В корневой папке NetDefendOS находятся два файла:

- *config.bak* – Резервная копия текущих настроек.
- *full.bak* – Резервная копия целой системы.

SCP может использоваться для загрузки любого из этих файлов. После завершения загрузки имя файла видоизменяется, так как к нему добавляется дата. Например, *full.bak* может преобразоваться в *full-20081121.bak* , отображая зафиксированное состояние 21 ноября, 2008 года.

Для восстановления резервной копии файла администратору следует загрузить файл на межсетевой экран NetDefend. Нет необходимости изменять имя файла, оно может хранить дату с момента прочтения системой NetDefendOS заголовка в файле для определения файла.

Резервное копирование и восстановление настроек с помощью Web-интерфейса

В качестве альтернативы использования SCP, администратор может создать резервную копию файлов или восстановить конфигурационный файл или целую систему непосредственно через Web-интерфейс. Пример ниже демонстрирует выполнение данного действия.

Пример 2.15. Создание резервной копии целой системы

Данный пример демонстрирует создание резервной копии целой системы, 12 декабря 2008 года.

Web-интерфейс

1. Зайдите **Maintenance > Backup**

2. Появится диалоговое окно *Backup*

3. Нажмите кнопку **Backup configuration**

4. Появится диалоговое окно для работы с файлами – выберите папку для созданного файла

5. Начнется загрузка файла резервной копии

Та же опция из меню *обслуживание* может использоваться для восстановления предварительно созданной резервной копии.

Примечание: Резервные копии не содержат всей информации

Резервные копии содержат только статическую информацию из настроек NetDefendOS. Динамическая информация, например, база данных аренды DHCP-сервера или базы данных Антивирус/IDP, не будет скопирована.

2.7.3. Сброс к заводским настройкам по умолчанию

Сброс к заводским настройкам по умолчанию выполняется для возврата к первоначальным настройкам межсетевого экрана NetDefend. При выполнении сброса настроек все данные, такие, как база данных провайдера и антивирусная база данных, будут утеряны и должны быть повторно загружены.

Пример 2.16. Сброс устройства к заводским настройкам по умолчанию

CLI

```
gw-world:/> reset -unit
```

Web-интерфейс

1. Зайдите **Maintenance (Обслуживание) > Reset (Сброс к настройкам по умолчанию)**

2. Выберите **Restore the entire unit to factory defaults (Восстановить заводские настройки по умолчанию),** затем подтвердите действие и подождите завершения восстановления.

Важно: Все обновления будут утеряны после сброса к заводским настройкам

*Следует помнить, что после **сброса к заводским настройкам** все выполненные обновления NetDefendOS будут утеряны.*

Процедура сброса настроек межсетевых экранов NetDefend DFL-210, 260, 800 и 860 к заводским настройкам по умолчанию

Для сброса настроек межсетевых экранов NetDefend DFL-210/260/800/860 к настройкам по умолчанию, в течение 10-15 секунд при включенном питании устройства удерживайте кнопку reset, расположенную на задней панели устройства. Затем отпустите кнопку, после чего продолжится загрузка и запуск устройства с восстановленными заводскими настройками по умолчанию.

IP-адрес, назначенный LAN-интерфейсу - *192.168.1.1*.

Процедура сброса настроек межсетевых экранов NetDefend DFL-1600, 1660, 2500, 2560 и 2560G к заводским настройкам по умолчанию

Для сброса настроек межсетевых экранов DFL-1600/1660/2500/2560/2560G нажмите любую клавишу на клавиатуре после появления на дисплее сообщения *Press keypad to Enter Setup.* Затем выберите опцию *Reset firewall* и подтвердите действие, выбрав *Yes*. Подождите завершения процесса сброса к заводским настройкам, после чего произойдет запуск устройства с восстановленными заводскими настройками по умолчанию.

Для моделей DFL-1600 и DFL-2500 интерфейсу *LAN1* будет назначен IP-адрес *192.168.1.1*. По умолчанию IP-адрес интерфейса управления для моделей DFL-1660, DFL-2560 и DFL-2560G - *192.168.10.1*.

Настройка IP-адреса по умолчанию для интерфейса управления по умолчанию представлена в Разделе 2.1.3, «Web-интерфейс».

Предупреждение: НЕ прерывайте сброс к настройкам по умолчанию

Если процесс сброса к заводским настройкам по умолчанию прерван до своего завершения, работоспособность межсетевого экрана NetDefend может быть нарушена, при этом полностью теряются все сохраненные данные пользователя.

Процедуры, выполняемые в конце срока эксплуатации

Опция сброса к заводским настройкам по умолчанию должна использоваться как часть процедуры в конце срока эксплуатации, когда завершается срок службы межсетевого экрана NetDefend, и устройство больше не будет использоваться. В качестве части процедуры при выводе из эксплуатации, сброс к заводским настройкам всегда должен выполняться для удаления конфиденциальной информации, например, VPN-настроек.

В качестве мер предосторожности в конце срока эксплуатации продукта рекомендуется уничтожение носителя памяти межсетевого экрана NetDefend, засвидетельствованное

соответствующим провайдером, предоставляющим вывоз и утилизацию отходов.

Глава 3.Основные принципы

Эта глава посвящена основным принципам логических объектов, которые присутствуют в конфигурации NetDefendOS. Эти объекты включают такие элементы, как IP-правила и IP-адреса. Некоторые из них существуют по умолчанию, а некоторые должны быть определены администратором.

Кроме того, в этой главе рассматриваются различные виды интерфейсов, и объясняется, как создаются администратором политики безопасности.

• Адресная книга

• Сервисы

• Интерфейсы

• ARP

• Наборы IP-правил

• Расписания

• Сертификаты

• Дата и время

• DNS

3.1. Адресная книга

3.1.1. Обзор

Адресная книга системы NetDefendOS содержит именованные объекты, представляющие различные типы IP-адресов, включая как отдельные IP-адреса, сети, так и диапазоны IP-адресов.

Использование объектов адресной книги имеет три важных преимущества:

- При использовании символьных имен повышается уровень понимания.
- Применение имен адресных объектов вместо ввода числовых адресов уменьшает количество ошибок.
- Определив IP-адрес объекта только один раз в адресной книге и ссылки на этот определение, при изменении определения автоматически изменяются все ссылки на него.

3.1.2. IP-адреса

Объекты *IP-адреса* применяются для обозначения символьных имен для различных типов адресов. В зависимости от того, как определен адрес, объект IP-адрес может представлять любой уникальный IP-адрес (определенный хост), сеть или диапазон IP-адресов.

Кроме того, объект IP-адрес может использоваться для определения учетных данных, используемых в пользовательской аутентификации. Более подробная информация приведена в *Главе 8, Аутентификация пользователя*.

В следующем перечне указываются различные типы адресов, которые поддерживаются объектом *IP-адрес*, а также форматы, с помощью которых представляются эти адреса:

Хост	Каждый хост представляется своим уникальным IP-адресом. Например: *192.168.0.14*
IP-сеть	IP-сеть представлена с использованием форм бесклассовой внутридоменной маршрутизации - *Classless Inter Domain Routing* (CIDR). CIDR использует наклонную черту вправо и числа (0-32), для префиксного обозначения размера сети. Эти обозначения также называют *маской подсети*. /24 соответствует сети класса C с 256 адресами (маска подсети 255.255.255.0), /27 соответствует сети с 32 адресами (маска подсети 255.255.255.224) и так далее. Числа 0-32 соответствуют числу двоичных единиц в маске подсети. Например: 192.168.0.0/24.
Диапазон IP-адресов	Диапазон IP-адресов представляется в форме a.b.c.d - e.f.g.h. Следует отметить, что диапазон не ограничен маской подсети. Он может включать любой промежуток IP-адресов. Например, 192.168.0.10-192.168.0.15 представляет шесть узлов в последовательном порядке.

Пример 3.1. Добавление IP-хоста

В этом примере рассматривается добавление IP-хоста *www_srv1 с* IP-адресом *192.168.10.16* в адресную книгу:

CLI

```
gw-world:/> add Address IP4Address www_srv1 Address=192.168.10.16
```

Web-интерфейс

1. Перейти к **Objects > Address Book > Add > IP address**
2. Указать подходящее имя для IP-хоста, в данном случае *wwww_srv1*
3. Ввести в строку **IP Address** *192.168.10.16*
4. Нажать кнопку **OK**

Пример 3.2. Добавление IP-сети

В этом примере рассматривается добавление IP-сети с именем *wwwsrvnet* и адресом *192.168.10.0/24* в адресную книгу:

CLI

```
gw-world:/> add Address IP4Address wwwsrvnet Address=192.168.10.0/24
```

Web-интерфейс

1. Перейти к **Objects > Address Book > Add > IP address**

2. Указать подходящее имя для IP-сети, например *wwwsrvnet*

3. Ввести *192.168.10.0/24* как IP-адрес

4. Нажать кнопку **OK**

Пример 3.3. Добавление IP-диапазона

В этом примере рассматривается добавление диапазона IP-адресов от *192.168.10.16* до *192.168.10.21* и имени для этого диапазона *wwwservers*:

CLI

```
gw-world:/> add Address IP4Address wwwservers
               Address=192.168.10.16-192.168.10.21
```

Web-интерфейс

1. Перейти к **Objects > Address Book > Add > IP address**

2. Указать необходимое имя для IP-диапазона, например *wwwservers*.

3. Ввести *192.168.10.16-192.168.10.21* как IP-адрес

4. Нажать кнопку **OK**

Пример 3.4. Удаление адресного объекта

Чтобы удалить объект с именем wwwsrv1 в адресной книге, выполните следующие действия:

CLI

```
gw-world:/> delete Address IP4Address www_srv1
```

Web-интерфейс

1. Перейти к **Objects > Address Book**

2. Выделить адресный объект *www_srv1*

3. Выбрать **Delete** в меню

4. Нажать кнопку **OK**

Удаление используемых IP-объектов

Если будет удален IP-объект, который еще используется другим объектом, то NetDefendOS не допустит применения конфигурации и выдаст предупреждающее сообщение. Другими словами, будет казаться, что объект успешно удален, но NetDefendOS не позволит сохранить конфигурацию в межсетевом экране NetDefend.

3.1.3. Ethernet-адреса

Объекты *Ethernet-адреса* используются для определения символьных имен для Ethernet-адресов (также известных как MAC-адреса). Они удобны, например, при заполнении ARP-таблиц со статическими ARP-данными, или для других частей конфигурации, где символьное имя предпочтительнее числовых Ethernet-адресов.

При определении Ethernet-адреса должен использоваться формат *aa-bb-cc-dd-ee-ff*. Ethernet-адреса

также отображаются в этом формате.

Пример 3.5. Добавление Ethernet-адреса

В следующем примере рассматривается добавление объекта Ethernet-адрес с именем *wwwsrv1_mac с числовым* MAC-адресом *08-a3-67-bc-2e-f2*.

CLI

```
gw-world:/> add Address EthernetAddress wwwsrv1_mac
                        Address=08-a3-67-bc-2e-f2
```

Web-интерфейс

1. Перейти к **Objects > Address Book > Add > Ethernet Address**

2. Определить подходящее имя для объекта Ethernet-адреса, например *wwwsrv1_mac*

3. Ввести 08-a3-67-bc-2e-f2 как MAC-адрес

4. Нажать кнопку **OK**

3.1.4. Address Groups (Адресные группы)

Создание групп для упрощения конфигураций

Адресные объекты могут быть сгруппированы для упрощения конфигураций. Рассмотрим несколько публичных серверов, которые должны быть доступны из Интернета. Серверы используют неравномерно расположенные IP-адреса и, следовательно, на них нельзя ссылаться как на единственный IP-диапазон. Следовательно, объекты с индивидуальным IP-адресом должны быть созданы для каждого сервера.

Вместо затрат на создание и поддержание отдельных политик фильтрации разрешенного для каждого сервера трафика, может быть создана *Адресная Группа (Address Groups)*, например *web-серверы,* с узлами web-серверов в качестве членов группы. Теперь для данной группы может использоваться единственная политика, тем самым существенно уменьшая объем административной работы.

Группы, содержащие различные подгруппы

Объекты адресных групп могут содержать неограниченное число подгрупп. Объекты IP-хосты могут быть сгруппированы по IP-диапазонам, IP-сетям и т.д. Все адреса всех членов группы будут объединены системой NetDefendOS.

Например, если группа содержит следующие два диапазона IP-адресов:

- *192.168.0.10 - 192.168.0.15*
- *192.168.0.14 - 192.168.0.19*

Результатом объединения этих двух диапазонов будет единый диапазон адресов, содержащий *192.168.0.10 - 192.168.0.19*.

3.1.5. Автоматически генерируемые адресные объекты

Для упрощения конфигурации при первоначальном запуске система NetDefendOS автоматически создает некоторое число адресных объектов, и эти объекты используются в различных частях начальной конфигурации.

Следующие адресные объекты генерируются автоматически:

Адреса интерфейса

Для каждого Ethernet-интерфейса в системе заранее определены два объекта IP-адресов; один из них для IP-адреса физического интерфейса и второй объект, представляющий локальную сеть для этого интерфейса.

Интерфейс объектов IP-адресов прописывается как *<interface-name>_ip,* а интерфейс объектов сети: *<interface-name>_net*. Пример: для интерфейса lan эти объекты соответственно будут называться *lan_ip* и *lannet*

Шлюз по умолчанию (Default Gateway)

Объект IP-адрес с именем *wan_gw* генерируется автоматически и представляется встроенным шлюзом системы. В основном объект wan_gw используется таблицей маршрутизации, но также может использоваться подсистемой DHCP-клиент для хранения загруженной с DHCP-сервера информации об адресах шлюза. Если адрес шлюза по умолчанию был предоставлен на этапе установки, то объект wan_gw будет содержать этот адрес. В противном случае, объект останется незаполненным (другими словами IP-адрес будет *0.0.0.0/0*)

all-nets (все сети)

Все сети объекта IP-адрес инициализируется IP-адресом *0.0.0.0/0*, который представляет все возможные IP-адреса. Объект *все сети* широко используется в конфигурации NetDefendOS и поэтому важно понять его значение

3.1.6. Address Book Folders (Папки адресной книги)

Для упорядочивания и сортировки данных в адресной книге можно создавать папки адресной книги, которые подобны папкам файловой системы компьютера. При создании папке присваивается имя, и она может использоваться для хранения всех IP-адресов, принадлежащих одной группе.

Использование папок упрощает работу администратора, делая более удобным распределение данных по адресной книге и нет необходимости указывать специальные свойства папок. NetDefendOS доступны все записи, как если бы они были в большой таблице объектов IP-адресов.

Понятие папки используется системой NetDefendOS и в других областях, таких как наборы IP-правил, где связанные IP-правила группируются вместе в созданную администратором папку.

3.2. Сервисы

3.2.1. Обзор

Объект **Сервис** ссылается на определенный IP-протокол с соответствующими параметрами. Определение сервиса обычно базируется на одном из основных транспортных протоколов, таких как TCP или UDP, который связан с определенными номерами портов источника и/или приемника. Например, сервис *HTTP* определяется как использующий TCP-протокол с соответствующим портом назначения 80 и любым портом источника.

Однако, объекты Сервис не ограничиваются только TCP или UDP-протоколами. Они могут использоваться для заключения в себя ICMP-сообщений, а также для определяемого пользователем IP-протокола.

Пассивный сервис

Сервисы являются пассивными объектами в том смысле, что они не могут самостоятельно выполнять действия в конфигурации. Вместо этого сервисные объекты должны быть связаны с политиками безопасности, определяемыми различными наборами правил системы NetDefendOS, и действовать как фильтр, предназначенными для применения этих правил к определенному типу трафика.

Например, IP-правило в наборе IP-правил системы NetDefendOS сервисный объект связан с фильтрацией параметра, определяющего разрешить или запретить определенный тип трафика, проходящий через межсетевой экран NetDefend. Включение в IP-правило является наиболее важной часть использования сервисных объектов, они также как и ALG стали ассоциироваться с IP-правилами, поскольку ALG связывается с сервисом, а не непосредственно с IP-правилом.

Для получения более подробной информации о том, как сервисные объекты используются с IP-правилами *см. пункт 3.5, “Наборы IP-правил”*.

Стандартные сервисы

Большое число сервисных объектов заранее задано в системе NetDefendOS. К ним относятся распространенные сервисы, такие как HTTP, FTP, Telnet и SSH.

Стандартные сервисы можно использовать и изменять подобно обычным определенным пользователем сервисам. Однако, рекомендуется не изменять стандартные сервисы, вместо этого следует создавать пользовательские сервисы с нужными характеристиками.

Для получения более подробной информации о создании пользовательских сервисов *см. пункт 3.2.2, “Создание пользовательских сервисов”*.

Пример 3.6. Список доступных сервисов

Для получения списка доступных сервисов необходимо:

CLI

```
gw-world:/> show Service
```

Результат будет представлен следующим примерным списком с сервисами, сгруппированными по типу с сервисными группами вначале::

```
ServiceGroup
Name Comments
------------ --------------------------------------------------
all_services All ICMP, TCP and UDP services
all_tcpudp All TCP and UDP services
ipsec-suite The IPsec+IKE suite
l2tp-ipsec L2TP using IPsec for encryption and authentication
l2tp-raw L2TP control and transport, unencrypted
pptp-suite PPTP control and transport
ServiceICMP
Name Comments
------------ --------------------------------------------------
all_icmp All ICMP services
```

""

Web-интерфейс

1. Перейти к **Objects > Services**

Пример 3.7. Просмотр определенного сервиса

CLI

```
gw-world:/> show Service ServiceTCPUDP echo
```

Результат будет представлен следующим примерным списком:

```
Property Value
---------------- ----------------
Name: echo
DestinationPorts: 7
Type: TCPUDP (TCP/UDP)
SourcePorts: 0-65535
PassICMPReturn: No
ALG: (none)
MaxSessions: 1000
Comments: Echo service
```

Web-интерфейс

1. Перейти к **Objects > Services**

2. Выбрать в таблице конкретный сервисный объект

3. Будет выведен список всех сервисов

3.2.2. Создание пользовательских сервисов

Если список стандартных сервисных объектов системы NetDefendOS не соответствует требованиям для определенного трафика, то может быть создан новый сервис. В данном разделе не только объясняется, как создаются новые сервисы, но и рассказывается о свойствах стандартных сервисов.

Тип созданного сервиса может быть одним из следующих:

- **TCP/UDP-сервис** – Сервис, базирующийся на UDP или TCP-протоколе, или и том и другом. Данный тип сервиса рассматривается в этой главе далее.
- **ICMP-сервис** – Сервис, основанный на ICMP-протоколе. Данный тип сервиса рассматривается в *Разделе 3.2.3, "ICMP-сервисы"*.
- **IP Protocol-сервис** – Сервис, основанный на определенном пользователем протоколе. Данный тип сервиса рассматривается в *Разделе 3.2.4, "Клиентский сервис IP-протокола "*.
- **Группа сервисов** – Группа сервисов, состоящая из несколько сервисов. Данный тип сервиса рассматривается в *Разделе3.2.5, "Сервис-группа"*.

Теперь более подробно рассмотрим более TCP/UDP-сервисы.

Сервисы, основанные на TCP и UDP

Большинство приложений используют TCP и/или UDP в качестве транспортных протоколов для передачи данных по IP-сетям.

Протокол управления передачей - *Transmission Control Protocol* (TCP) – ориентированный на соединение протокол, включающий в себя механизм передачи данных точка-точка (point-to-point). TCP-протокол используется в большинстве приложений, в которых важна безошибочная передача данных, к таким можно отнести HTTP, FTP и SMTP.

UDP-ориентированные приложения

Для приложений, где скорость передачи данных играет главную роль, например, при потоковом аудио и видео, предпочтительнее использовать протокол пользовательских датаграмм - *User Datagram Protocol* (UDP). UDP - протокол, не ориентированный на соединение, обеспечивает минимальную передачу при восстановлении ошибок и значительно более низкую нагрузку, по сравнению с TCP-протоколом. Из-за более низких расходов UDP используется для некоторых непотоковых сервисов и в тех случаях, когда в самих приложениях содержатся какие-либо механизмы исправления ошибок.

Определение TCP и UDP-сервисов

Для определения TCP или UDP-протокол является основным для системы NetDefendOS, используется объект TCP/UDP-сервис. Помимо уникального имени, описывающего сервис, объект содержит информацию о протоколе (TCP, UDP или оба протокола) и применяемых для сервиса портах источника и назначения.

Определение номеров порта

Номера портов определены всеми типами сервисов и полезно знать, как они могут быть зафиксированы в пользовательских интерфейсах. Они могут быть определены для порта источника и/или порта назначения следующими способами:

Единственный порт

Для многих сервисов достаточно одного порта назначения. Например, HTTP обычно использует порт назначения 80. SMTP-протокол использует порт 25 и так далее. Для таких типов сервисов единственный номер порта просто указывается в определении сервиса как одно число.

Диапазоны портов

Некоторые сервисы используют диапазоны портов назначения. Например, NetBIOS-протокол, применяющийся в Microsoft Windows™, использует диапазон от 137 до 139.

Для определения диапазона портов в объекте TCP/UDP-сервис используется формат *mmm-nnn*. Обозначение *137-139* означает, что в этот диапазон входят *137*, *138* и *139* порты.

Множественный доступ к порту и диапазоны портов

Множественные диапазоны портов или индивидуальные порты можно вводить, разделяя их запятыми, что позволяет охватывать широкий диапазон портов с использованием только одного объекта TCP/UDP-сервис.

Например, все сети Microsoft Windows можно охватить, используя определение порта *135-139,445*. HTTP и HTTPS можно покрыть, указав порты назначения *80,443*.

Совет: Указание портов источника

Обычно большинство сервисов по умолчанию использует значения диапазона портов источника 0-65535 (соответствующее всем доступным портам источника).

Для некоторых приложений эффективнее определить порт источника, если он всегда находиться в ограниченном диапазоне значений. Рекомендуемый подход: определять как можно более узкий диапазон портов.

Другие свойства сервиса

Помимо основного протокола и информации о портах, у объектов TCP/UDP-сервис есть также несколько других свойств:

- **SYN Flood Protection** (защита от атак SYN Flood)

  Опция SYN Flood Protection разрешает сервису, основанному на TCP настраивать защиту от атак *SYN Flood*. Эта опция поддерживается только *TCP/IP-сервисами*.

  Более подробная информация о том, как работает эта функция, приведена в *Разделе 6.6.8, «Атака TCP SYN Flood»*.

- **Pass ICMP Errors** (прием ICMP-сообщений об ошибках)

  При попытке открыть TCP-соединение приложением пользователя, расположенного за межсетевым экраном NetDefend, и если удаленный сервер недоступен, то в ответ возвращается ICMP-сообщение об ошибке. Такие сообщения интерпретируются системой NetDefendOS как новое соединение и отклоняются, если IP-правилами не прописано другое.

  Опция **Pass returned ICMP error messages from destination** (возвращение ICMP-сообщений от получателя) разрешает таким ICMP-сообщениям автоматически передаваться обратно в запрашивающее приложение. В некоторых случаях лучше пропускать ICMP-сообщения. Например, если ICMP-сообщение *quench* направлено на уменьшение скорости потока трафика. С другой стороны, отклонение ICMP-сообщений увеличивает безопасность, предотвращая их использование в качестве способа атаки.

- **ALG**

  TCP/UDP-сервис может быть связан со шлюзом прикладного уровня - *Application Layer Gateway* (ALG), что обеспечит более детальную проверку определенных протоколов. Этот метод заключается в связи ALG с IP-правилами. Первоначально ALG связывается с сервисом, после чего сервис связывается с IP-правилами.

  Более подробная информация об этой теме представлена в *Разделе 6.2, "ALG"*.

- **Max Sessions** (Максимальное количество сессий)

  К одному из важных параметров относят *Max Sessions*. Этот параметр выделяет заданные по умолчанию значения при соединении сервиса с ALG. В зависимости от ALG это заданное по умолчанию значение меняется. Если, например, значение по умолчанию равно 100, то это означает, что для всех интерфейсов этого сервиса возможно только 100 соединений.

  Для сервисов, связывающих, например, HTTP и ALG значение по умолчанию часто может быть очень низким, если велико количество соединений, проходящих через межсетевой экран NetDefend.

Определение объекта *all_services*

При установке правил фильтрации сервиса возможно использование объекта, называемого *all_services,* ссылающегося на все протоколы. Однако применять этот объект не рекомендуется, определение более конкретных сервисов обеспечивает лучшую безопасность. Если, например, требуется фильтровать только протоколы типа TCP, UDP и ICMP, то можно использовать объект *all_tcpudpicmp*.

Совет: Сервис http-all не включает в себя DNS-протокол

Необходимый для web-серфинга DNS-протокол входит в состав сервиса ***dns-all,*** *который можно добавить в группу сервиса* ***http-all*** *и связать IP-правилами.*

Ограничение сервисов по минимально необходимым параметрам

При выборе сервисных объектов следует создавать политики, такие как IP-правила, протоколы, входящие в этот объект необходимы только для достижения трафика к фильтру. Использование объекта *all_services* может быть удобным, но исключаются преимущества безопасности, которые может обеспечить более конкретный сервисный объект.

Лучшей стратегией является сужение фильтра сервиса в политике безопасности таким образом, чтобы пропускались только те протоколы, которые действительно необходимы. Часто в качестве первоначального для общего трафика выбирается сервисный объект *all_tcpudpicmp,* но даже он разрешает больше протоколов, чем обычно необходимо; в дальнейшем администратор может сузить диапазон разрешаемых протоколов.

Пример 3.8. Создание пользовательского TCP/UDP-сервиса

В этом примере показывается добавление TCP/UDP-сервиса, применяя порт назначения 3306, который используется MySQL:

CLI

```
gw-world:/> add Service ServiceTCPUDP MySQL
            DestinationPorts=3306 Type=TCP
```

Web-интерфейс

1. Перейти к **Objects > Services > Add > TCP/UDP service**

2. Указать подходящее имя для сервиса, например *MySQL*

3. Ввести:

   - **Type:** TCP
   - **Source:** 0-65535
   - **Destination:** 3306

4. Нажать кнопку **OK**

3.2.3. ICMP-сервисы

Другим типом создаваемых пользовательских сервисов является *ICMP-сервис*.

Протокол управления сообщениями в сети - *Internet Control Message Protocol* (ICMP) – протокол,

интегрированный с IP для отчета об ошибках и передачи управляющей информации. Например, функция *ICMP Ping* используется для тестирования Интернет-соединений.

Типы и коды ICMP

ICMP-сообщения доставляются в IP-пакетах и содержат тип сообщения (*Message Type)*, который определяет формат ICMP-сообщения и код (*Code),* который используется для дальнейшего определения сообщения. Например, тип сообщения *Destination Unreachable (Невозможно определить получателя)* использует параметр кода, указывающий точную причину ошибки.

Либо все типы ICMP-сообщений (существует 256 типов) могут быть приняты сервисом, либо возможна фильтрация типов.

Определение кодов

Если тип выбран, то коды для данного типа могут быть указаны тем же способом, которым определены номера портов. Например, если выбран тип *Destination Unreachable* со списком кодов, разграниченных запятой *0,1,2,3,* то фильтр будет: *Network unreachable (сеть недоступна)*, *Host unreachable (хост недоступен)*, *Protocol unreachable (протокол недоступен)* и *Port unreachable (порт недоступен).*

Когда тип сообщения выбран, но значения кода не приведены, то все коды для этого типа являются предполагаемыми.

Типы ICMP-сообщений

Тип выбираемого сообщения может быть следующим:

Echo Request — Для проверки подключения в точку назначения отправляется команда PING.

Destination Unreachable — Источник сообщил, что проблема произошла при доставке пакета. Для этого типа предусмотрены следующие коды:

- Code 0: Net Unreachable (Сеть недоступна)
- Code 1: Host Unreachable (Хост недоступен)
- Code 2: Protocol Unreachable (Протокол недоступен)
- Code 3: Port Unreachable (Порт недоступен)
- Code 4: Cannot Fragment (Фрагментирование невозможно)
- Code 5: Source Route Failed (выбран неудачный маршрут)

Redirect — Источник сообщил, что существует наиболее оптимальный маршрут для конкретного пакета. Предусмотрены следующие коды:

- Code 0: Redirect datagrams for the network (Переадресация датаграмм для сети)
- Code 1: Redirect datagrams for the host (Переадресация датаграмм для хоста)
- Code 2: Redirect datagrams for the Type of Service and the network (Переадресация датаграмм для типа сервиса и сети)
- Code 3: Redirect datagrams for the Type of Service and

	the host (Переадресация датаграмм для типа сервиса и хоста)
Parameter Problem	Идентифицирует неправильный параметр в датаграмме.
Echo Reply	Ответ узла назначения, которое отправляется в результате эхо-запроса (Echo Request).
Source Quenching	В результате быстрой отправки сообщений источником происходит переполнение буфера узла назначения.
Time Exceeded	Пакет был отброшен, так как время доставки было превышено.

3.2.4. Пользовательский сервис IP-протокола

Сервисы, которые работают над IP и выполняет функции на транспортном уровне или уровне приложений могут быть однозначно идентифицированы *номерами IP-протокола*. IP-протокол может передавать данные для ряда других различных протоколов. Каждый из этих протоколов идентифицируется уникальным номером IP-протокола, определяемым в IP-заголовке. Например, ICMP, IGMP и EGP имеют номера протокола 1, 2 и 8 соответственно.

Как и описанные ранее диапазоны портов TCP/UDP, диапазон адресов IP-протокола может использоваться при указании нескольких приложений для одного сервиса. Например, определения диапазона *1-4,7* будет соответствовать протокола*м ICMP*, *IGMP*, *GGP*, *IP-in-IP* и *CBT*.

Адреса IP-протокола

В настоящее время назначенные адреса IP-протокола и ссылки публикуются уполномоченным органом по цифровым адресам - *Internet Assigned Numbers Authority* (IANA):

http://www.iana.org/assignments/protocol-numbers

Пример 3.9. Добавление сервиса IP-протокола

В этом примере рассматривается добавление сервиса IP-протокола с помощью протокола VRRP (Virtual Router Redundancy Protocol).

CLI

```
gw-world:/> add Service ServiceIPProto VRRP IPProto=112
```

Web-интерфейс

1. Перейти к **Objects > Services > Add > IP protocol service**
2. Указать подходящее имя для сервиса, например *VRRP*
3. Ввести *112 в поле* **IP Protocol**
4. При необходимости ввести *Virtual Router Redundancy Protocol* в поле **Comments**
5. Нажать кнопку **OK**

3.2.5. Service Groups (Сервисные группы)

Как видно из названия, сервисные группы – это объект системы NetDefendOS, состоящий из нескольких сервисов. Несмотря на то, что концепция группы проста, она может быть очень полезна при создании политик безопасности, так как группа может быть использована вместо отдельного сервиса.

Преимущество групп

Например, группа может быть необходима для набора IP-правил, идентичных друг другу за исключением сервисного параметра. Определяя сервисную группу, которая содержит все объекты сервиса, каждый с индивидуальными правилами, можно заменить их на одно IP-правило, которое используется группой.

Предположим, что требуется создать сервисную группу с именем *email-services,* состоящую из трех сервисных объектов для *SMTP*, *POP3* и *IMAP*. Теперь требуется определить только одно IP-правило, которое будет использоваться этой группой сервисов для того, чтобы разрешить прохождение всего трафика, связанного с email.

Группы могут содержать различные подгруппы

После того как группа определена, она может содержать отдельные сервисы или сервисные группы. Эту способность групп внутри групп следует использовать достаточно осторожно, так как она увеличивает сложность конфигурации и приводит к уменьшению способности поиска неисправностей.

3.2.6. Custom Service Timeouts (Тайм-ауты пользовательского сервиса)

У любого сервиса может быть пользовательский набор тайм-аутов. Тайм-ауты также можно устанавливать глобально в NetDefendOS, но обычно для изменений этих значений используют пользовательские сервисы.

Ниже приведены настройки тайм-аутов, которые могут быть созданы пользователем:

- **Initial Timeout**

  Время, допустимое для открытия нового соединения

- **Establish (Idle) Timeout**

  Если соединение неактивно в течение этого времени, то оно считается закрытым и удаляется из таблицы состояния системы NetDefendOS. В настройках по умолчанию для TCP/UDP-соединений это время составляет 3 дня.

- **Closing Timeout**

  Время, предоставляемое на закрытие соединения.

Администратору необходимо выбрать приемлемые значения для каждого конкретного протокола. Они могут зависеть, например, от ожидания ответной реакции серверов, к которым подключаются пользователи.

3.3. Интерфейсы

3.3.1. Обзор

Интерфейс является важным логическим блоком в системе NetDefendOS. Весь передаваемый сетевой трафик возникает или прекращается в межсетевом экране NetDefend при помощи одного или нескольких интерфейсов.

Интерфейсы источника и назначения

Интерфейс может рассматриваться как дверь, через которую сетевой трафик проходит в систему NetDefendOS или выходит из нее. Интерфейс системы NetDefendOS выполнят одну из двух функций:

- **Интерфейс источника**

  Когда трафик поступает через интерфейс, он упоминается в NetDefendOS как интерфейс источника (также известный как принимающий или входящий интерфейс).

- **Интерфейс назначения**

  При передаче трафика, после проверки политиками безопасности системы NetDefendOS, интерфейс, используемый для отправки трафика, упоминается в NetDefendOS как интерфейс назначения (также известный как интерфейс отправки).

Весь трафик, проходящий через систему NetDefendOS, имеет как интерфейс источника, так и интерфейс назначения. Как будет объяснено позже, специальный логический интерфейс *core* используется, когда система NetDefendOS сама является источником или назначением для трафика.

Типы интерфейсов

Система NetDefendOS поддерживает несколько типов интерфейсов, которые можно разделить на следующие 4 основные группы:

- **Ethernet-интерфейсы**

  Каждый Ethernet-интерфейс представляет физический Ethernet-порт устройства на основе NetDefendOS. Весь сетевой трафик, который возникает или входит в межсетевой экран, будет проходить через один из физических интерфейсов.

  В настоящее время NetDefendOS поддерживает только один тип физического интерфейса - *Ethernet*. Более подробная информация об Ethernet-интерфейсах приведена в *Разделе 3.3.2, «Ethernet-интерфейсы»*.

- **Под-интерфейсы**

  Для передачи данных некоторым интерфейсам требуется привязка к основному физическому интерфейсу. Эта группа интерфейсов называется физические под-интерфейсы - *Physical Sub-Interfaces*.

  NetDefendOS поддерживает два типа физических под-интерфейсов:

  - Интерфейсы *Virtual LAN* (VLAN) определяются стандартом IEEE 802.1Q. При маршрутизации IP-пакетов через Virtual LAN-интерфейс, они инкапсулируются в VLAN-тэговые Ethernet-кадры. Более подробная информация о VLAN-интерфейсе приведена в *Разделе 3.3.3., «VLAN»*.
  - Интерфейсы *PPPoE* (PPP-over-Ethernet) для подключения к PPPoE-серверам. Более подробная информация об этом разделе приведена в *Разделе 3.3.4, «PPPoE»*.

- **Туннельные интерфейсы**

  Туннельные интерфейсы используются, когда сетевой трафик передается по туннелю между системой и другим конечным устройством туннеля в сети, прежде чем он маршрутизируется в пункт назначения. VPN-туннели часто используются для реализации виртуальных частных сетей (VPN), которые могут обеспечить безопасное соединение между двумя межсетевыми экранами. При выполнении туннелирования к туннелируемому трафику добавляется дополнительный заголовок. Кроме того, в зависимости от типа туннельного интерфейса к сетевому трафику могут быть применены различные преобразования. Например, при маршрутизации трафика через IPsec-интерфейс, полезная информация обычно кодируется для достижения конфиденциальности.

  NetDefendOS поддерживает следующие типы туннельных интерфейсов:

  i. *IPsec-интерфейсы* используются в качестве конечных точек для VPN IPsec-туннелей. Более подробная информация приведена в *Разделе 9.3, "Компоненты IPsec"*.

  ii. *PPTP/L2TP-интерфейсы* используются в качестве конечных точек для PPTP /L2TP-туннелей. Более подробная информация приведена в *Разделе 9.5, «PPTP/L2TP»*.

  iii. *GRE-интерфейсы* используются для установления GRE-туннелей. Более подробная информация приведена в *Разделе 3.3.5, "GRE-туннели"*

Все интерфейсы логически эквивалентны

Каждому интерфейсу в системе NetDefendOS присваивается уникальное имя, с помощью которого интерфейс можно идентифицировать и выбрать его для использования с другими объектами конфигурации NetDefendOS. Некоторые типы интерфейсов, такие как физические Ethernet-интерфейсы, уже снабжены системой NetDefendOS соответствующими названиями по умолчанию, которые при необходимости можно изменять. Новые интерфейсы, определенные администратором, всегда будут требовать определенное пользователем имя, которое будет указано.

Предупреждение

При удалении определения интерфейса из конфигураций NetDefendOS необходимо сначала удалить или изменить какие-либо ссылки на этот интерфейс. Например, правила в наборе IP-правил, относящиеся к этому интерфейсу, должны быть удалены или изменены.

Интерфейсы *any* и *core*

Кроме того, система NetDefendOS обеспечена двумя специальными логическими интерфейсами, которые называются **any** и **core**. Значения каждого из них:

- **any** представляет все возможные интерфейсы, включая интерфейс **core**.

- **core** указывает на то, что система NetDefendOS сама будет контролировать движение трафика с этого интерфейса и в этот интерфейс. Примером использования core является случай, когда межсетевой экран NetDefend работает как сервер PPTP или Д2Е3 или отвечает на ICMP-запросы "Ping". При указании интерфейса назначения маршрута такого, как **core**, системе NetDefendOS будет известно, что она сама является конечной точкой назначения трафика.

Отключение интерфейса

Если нужно отключить интерфейс, чтобы через него не мог проходить никакой трафик, то используют следующую команду консоли:

```
gw-world:/> set Interface Ethernet <interface-name> -disable
```

Где <*interface-name*> - интерфейса, который должен быть отключен.

Для переподключения интерфейса используется команда:

```
gw-world:/> set Interface Ethernet <interface-name> -enable
```

3.3.2. Ethernet-интерфейсы

Ethernet-стандарт IEEE 802.3 позволяет связывать различные устройства с произвольно выбранными точками или «портами» с помощью физического транспортного механизма, такого как коаксиальный кабель. Используя CSMA/CD-протокол, каждое подключенное через Ethernet устройство «слушает» сеть и передает данные на другое подключенное устройство, когда сеть не занята. Если два устройства одновременно передают данные, алгоритмы позволяют им повторно пересылать данные в разное время.

Ethernet-фреймы (Ethernet Frames)

Устройства в широковещательной рассылке посылают данные, такие как Ethernet-фреймы, другие устройства «слушают» сеть и определяют, кому направлен любой из этих фреймов. Фрейм представляет собой последовательность бит, которые определяют отправляющее и принимающее устройства, а также полезную информацию вместе с битами для проверки ошибок. По мере развития технологии (Ethernet, Fast Ethernet и Gigabit Ethernet) времени на обработку каждого фрейма затрачивается все меньше, тем самым обеспечивается более высокая скорость передачи данных.

Физические Ethernet-интерфейсы

Каждый логический Ethernet-интерфейс системы NetDefendOS соответствует физическому Ethernet-порту в системе. Количество портов, скорость соединения и метод реализации портов зависят от аппаратной модели.

Примечание: Дополнительные коммутируемые порты

Некоторые системы используют интегрированный коммутатор второго уровня для обеспечения дополнительными физическими Ethernet-портами. Такие дополнительные порты рассматриваются системой NetDefendOS как отдельный интерфейс.

Параметры Ethernet-интерфейса

Ниже приведены различные параметры, которые могут быть установлены для Ethernet интерфейса:

- **Interface Name**

Имена Ethernet-интерфейсов заранее определены системой и отображаются именами физических портов; Ethernet-интерфейс системы с wan-портом будет называться *wan* и так далее.

Для наглядности имена Ethernet-интерфейсов могут быть изменены. Например, если интерфейс с именем *dmz* подключен к беспроводной локальной сети, для удобства имя интерфейса можно изменить на *radio*. Для защиты и поиска неисправностей рекомендуется отметить соответствующий физический порт с новым именем.

Примечание: Перечисление интерфейсов

*Процесс запуска будет перебирать все доступные Ethernet-интерфейсы. Каждому интерфейсу будут присвоены имена типа **lanN**, **wanN** и **dmz**, где N – номер интерфейса в том случае если в межсетевом экране NetDefend их несколько. В большинстве примеров данного приложения для LAN-трафика используется **lan**, а для WAN-трафика **wan**. Если в межсетевом экране NetDefend нет таких интерфейсов, то следует изменить ссылки с именами выбранных интерфейсов.*

- **IP Address**

Каждый Ethernet-интерфейс должен иметь IP-адрес интерфейса - Interface IP Address, который может быть статическим, либо адресом, указанным DHCP. IP-адрес интерфейса используется в качестве основного адреса для соединения с системой через определенный Ethernet-интерфейс.

Для определения IP-адресов Ethernet-интерфейсов в системе NetDefendOS, как правило, используется объекты *IP4 Address*. Такие объекты обычно автоматически генерируются системой. Более подробная информация приведена в *Разделе 3.1.5, «Автоматически генерируемые адресные объекты»*.

Совет: Задание множественных IP-адресов (multiple IP addresses) на интерфейсе

С помощью механизма ARP Publish для Ethernet-интерфейса можно указать множественные IP-адреса. (Более подробная информация приведена в Разделе 3.4, "ARP").

- **Network**

В дополнение к IP-адресу интерфейса для Ethernet-интерфейса также указывается сетевой адрес. Сетевой адрес обеспечивает систему NetDefendOS информацией о том, какие IP-адреса непосредственно доступны через интерфейс. Другими словами, те IP-адреса, которые находятся в одной подсети с этим интерфейсом. В связанной с интерфейсом таблице маршрутизации NetDefendOS автоматически создаст направленный маршрут к указанной сети через текущий интерфейс.

- **Default Gateway**

Дополнительно для Ethernet-интерфейса может быть определен адрес шлюза по умолчанию. Обычно это адрес маршрутизатора, который часто выступает в качестве шлюза для Интернета.

Как правило, для шлюза по умолчанию в таблице маршрутизации требуется только один маршрут по умолчанию *all-nets* (*все-сети)*.

- **Enable DHCP Client**

В систему NetDefendOS включена опция DHCP-клиент для динамического назначения информации об адресе подключенного DHCP-сервера. Эта опция часто используется для получения информации о внешнем IP-адресе от DHCP-сервера провайдера, используемая для общественного доступа в Интернет.

С помощью DHCP можно получить информацию об IP-адресе интерфейса, локальной сети, к которой относится данный интерфейс, и шлюза по умолчанию.

Все адреса, полученные от DHCP-сервера, присваиваются соответствующим объектам *IP4Address*. Таким образом, динамически назначенные адреса, так же как и статические, могут использоваться во всей конфигурации. По умолчанию используются те же объекты, информация о которых представлена в *Разделе 3.1.5, «Автоматическая генерация адресных объектов»*.

По умолчанию на Ethernet-интерфейсах опция DHCP-клиент отключена. Если интерфейс используется для подключения к публичной сети Интернет с помощью фиксированных IP-адресов провайдера, то DHCP не используется.

Адреса DNS-сервера, полученные через DHCP на интерфейс с именем *<interface-name>,* будут назначены адресным объектам системы NetDefendOS с именами *<interface-name>_dns1* и *<interface_name>_dns2*.

Примечание: При включенной опции DHCP IP-адрес шлюза не может быть удален

Если опция DHCP активирована для данного Ethernet-интерфейса, то любой IP-адрес шлюза, который определен для этого интерфейса, не может быть удален. Для удаления адреса шлюза необходимо сначала отключить опцию DHCP.

Если опция DHCP активирована, то на интерфейсе можно настроить определенные дополнительные настройки:

i. Возможность запроса предпочтительного IP-адреса.

ii. Возможность запроса предпочтительного времени аренды (lease time).

iii. Возможность отправления статических маршрутов от DHCP-сервера.

iv. Предотвращение коллизий IP-адресов в статических маршрутах.

v. Предотвращение сетевых коллизий в статических маршрутах.

vi. Определение разрешенного IP-адреса на период аренды DHCP.

vii. Определение диапазона адресов на DHCP-сервере, для которых будет установлен период аренды.

- **DHCP Hostname**

Иногда DHCP-серверу может потребоваться параметр *hostname,* отправляемый к DHCP-клиенту.

- **Enable Transparent Mode**

Рекомендуемым способом активации прозрачный режим (Transparent Mode) является способ добавления коммутаторов, описанный в *Разделе 4.7, "Прозрачный режим (Transparent Mode)*". Альтернативный метод заключается в активации прозрачного режима данной опцией непосредственно на интерфейсе.

Когда эта опция активирована, коммутируемые маршруты по умолчанию автоматически добавляются в таблицу маршрутизации для интерфейса, а любые некоммутируемые маршруты автоматически удаляются.

- **Hardware Settings**

Иногда необходимо изменить аппаратные настройки для интерфейса. Доступные параметры:

i. Может быть установлена скорость соединения. Предпочтительнее использовать *Auto*.

ii. Может быть установлен MAC-адрес, если он должен отличаться от MAC-адреса встроенного в аппаратное обеспечение. Для некоторых соединений через Интернет-провайдеров требуется установка этого параметра.

- **Virtual Routing**

Для реализации виртуальной маршрутизации (virtual routing), где маршруты, связанные с различными интерфейсами, хранятся в отдельной таблице маршрутизации, можно выбрать следующие параметры:

i. Обозначить интерфейс во всех таблицах маршрутизации. Эта опция активируется по умолчанию и означает, что трафик, поступающий на интерфейс, будет маршрутизироваться согласно таблице маршрутизации *main*. Маршруты для интерфейса IP будут добавлены во все таблицы маршрутизации.

ii. В качестве альтернативы предыдущей маршрут для этого интерфейса можно добавить только в конкретную таблицу маршрутизации. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации.

- **Automatic Route Creation**

Маршруты могут добавляться к интерфейсу автоматически. Добавление маршрутов может быть двух типов:

i. Добавление маршрута к этому интерфейсу для заданной сети. Используется по умолчанию.

ii. Добавление к этому интерфейсу маршрута по умолчанию, используя заданный шлюз по умолчании. Используется по умолчанию.

- **MTU**

Определяет максимальный размер пакета в байтах, который может отправляться на данный интерфейс. По умолчанию интерфейс использует максимальный размер.

- **High Availability**

Существует два параметра, специфических для кластеров высокой отказоустойчивости:

1. Для данного интерфейса может быть определен приватный IP-адрес.

2. Дополнительная опция, отключающая отправление тактовых импульсов HA-кластеров из этого интерфейса.

- **Quality of Service**

Опция предназначена для копирования последовательности выполнения IP DSCP в поле приоритета VLAN для любого VLAN-пакета. По умолчанию опция выключена.

Изменение IP-адресов Ethernet-интерфейса

Изменить IP-адрес интерфейса можно одним из двух методов:

- Изменить IP-адрес непосредственно на интерфейсе. Например, при изменении IP адреса **lan**-интерфейса на *10.1.1.2* необходимо использовать команду консоли:

```
gw-world:/> set Interface Ethernet lan IP=10.1.1.2
```

Ниже объясняется, почему изменять IP-адрес данным способом не рекомендуется.

- Объекту *ip_lan* адресной книги системы NetDefendOS должен быть назначен новый адрес, так как он часто используется другими объектами системы NetDefendOS, такими как IP-правила. Команда CLI следующая:

```
gw-world:/> set Address ip_lan Address=10.1.1.2
```

Эта операция может осуществляться через Web-интерфейс.

Краткое изложение команд CLI, используемых в Ethernet-интерфейсе приведено в *Разделе 3.3.2.1, «Использование CLI-команд в Ethernet-интерфейсе»”*.

3.3.2.1. Полезные CLI-команды для Ethernet-интерфейса

В этом разделе приведены CLI-команды, наиболее часто используемые для проверки и управления Ethernet-интерфейсами в системе NetDefendOS.

Ethernet-интерфейсы можно просмотреть через Web-интерфейс, но для некоторых операций необходимо использовать CLI-команды:

Для вывода текущего интерфейса с назначенным IP-адресом *wan_ip*:

```
gw-world:/> show Address IP4Address InterfaceAddresses/wan_ip

Property              Value
--------------------- --------------------------
Name:                 wan_ip
Address:              0.0.0.0
UserAuthGroups:       <empty>
NoDefinedCredentials:  No
Comments:             IP address of interface wan
```

Для вывода текущего интерфейса сети *wan_net*:

```
gw-world:/> show Address IP4Address InterfaceAddresses/wan_net

Property              Value
--------------------- ------------------------
Name:                 wan_net
Address:              0.0.0.0/0
UserAuthGroups:       <empty>
NoDefinedCredentials: No
Comments:             Network on interface wan
```

Для вывода текущего интерфейса шлюза wan_gw:

```
gw-world:/> show Address IP4Address InterfaceAddresses/wan_gw

Property              Value
--------------------- --------------------------------
Name:                 wan_gw
Address:              0.0.0.0
UserAuthGroups:       <empty>
NoDefinedCredentials: No
Comments:             Default gateway for interface wan
```

Для завершения команды в конце командной строки можно использовать клавишу Tab:

```
gw-world:/>   show   Address   IP4Address   InterfaceAddresses/wan_<tab>

[<Category>] [<Type> [<Identifier>]]:

InterfaceAddresses/wan_br   InterfaceAddresses/wan_gw
InterfaceAddresses/wan_dns1 InterfaceAddresses/wan_ip
InterfaceAddresses/wan_dns2 InterfaceAddresses/wan_net
```

Здесь клавиша Tab используется для завершения команды в конце командной строки

```
gw-world:/> set Address IP4Address<tab>

[<Category>] <Type> [<Identifier>]:

dnsserver1_ip InterfaceAddresses/wan_br timesyncsrv1_ip
InterfaceAddresses/aux_ip  InterfaceAddresses/wan_dns1
InterfaceAddresses/aux_net InterfaceAddresses/wan_dns2
InterfaceAddresses/dmz_ip  InterfaceAddresses/wan_gw
InterfaceAddresses/dmz_net InterfaceAddresses/wan_ip
InterfaceAddresses/lan_ip  InterfaceAddresses/wan_net
InterfaceAddresses/lan_net                                    Server
```

CLI используется для определения адреса интерфейса:

```
gw-world:/> set Address IP4Address
            InterfaceAddresses/wan_ip                 Address=172.16.5.1

Modified IP4Address InterfaceAddresses/wan_ip.
```

CLI можно использовать для активации DHCP на интерфейсе:

```
gw-world:/> set Interface Ethernet wan DHCPEnabled=yes

Modified Ethernet wan.
```

Некоторые настройки параметров интерфейса доступны только через соответствующий набор CLI-команд. Это применяется, если заменяется оборудование D-Link и нужно изменить настройки сетевой карты или если необходимо настроить интерфейсы, при запуске системы NetDefendOS на оборудовании другой компании. Например, для вывода информации о Ethernet-портах используется команда:

```
gw-world:/> show EthernetDevice
```

Эта команда выводит информацию обо всех определенных Ethernet-интерфейсах. В этот список также включаются интерфейсы, удаленные до активации. Удаленные интерфейсы будут обозначаться символом "-" перед именем. Восстановление удаленного интерфейса в списке можно осуществить с помощью команды *undelete*:

```
gw-world:/> undelete EthernetDevice <interface>
```

Следующая команда также может быть использована для вывода информации об интерфейсе:

```
gw-world:/> show Ethernet Interface
```

Для управления Ethernet-интерфейсом может использоваться команда *set.* Например, для включения интерфейса *lan* используется команда:

```
gw-world:/> set EthernetDevice lan -enable
```

Для установки драйверов на карту Ethernet-интерфейса используется команда:

```
gw-world:/> set EthernetDevice lan EthernetDriver=<driver>
                        PCIBus=<X> PCISlot=<Y> PCIPort=<Z>
```

Например, если имя драйвера - *IXP4NPEEthernetDriver* для шины, разъема, порта с комбинацией 0, 0, 2 на wan-интерфейсе, команда *set* будет выглядеть:

```
gw-world:/> set EthernetDevice lan
                        EthernetDriver=IXP4NPEEthernetDriver
                        PCIBus=0 PCISlot=0 PCIPort=2
```

Полный список опций CLI-команд приведен в руководстве *CLI Reference Guide*.

3.3.3. VLAN

Обзор

Виртуальная локальная сеть (Virtual LAN, VLAN), поддерживаемая системой NetDefendOS позволяет определять один или несколько VLAN-интерфейсов, которые связаны с конкретным физическим интерфейсом. VLAN-интерфейсы рассматриваются как логические интерфейсы NetDefendOS и могут обрабатываться как и другие интерфейсы в системе NetDefendOS с помощью наборов правил и таблиц маршрутизации.

VLAN применяется в нескольких случаях. Обычное применение – когда один Ethernet-интерфейс представлен как несколько интерфейсов. Это означает, что число физических Ethernet-портов на межсетевых экранах NetDefend не ограничивается числом соединений внешних сетей.

Другим типичным случаем применения VLAN является группировка отдельных пользователей таким образом, чтобы трафик, принадлежащий различным группам, был полностью отделен от других виртуальных локальных сетей. Трафик может проходить только между различными VLAN-сетями, находящимися под управлением NetDefendOS и фильтроваться с помощью политик безопасности, описываемых наборами правил системы NetDefendOS.

Ниже более подробно объясняется о том, что конфигурация VLAN системы NetDefendOS включает в себя комбинацию *VLAN-каналов* от межсетевых экранов NetDefend до коммутаторов, на интерфейсах которых порты настроены на основе VLAN. Любой физический интерфейс межсетевого экрана может одновременно пропускать как не- VLAN-трафик, так и VLAN-трафик для одного или нескольких VLAN.

Механизм работы VLAN

NetDefendOS полностью поддерживает стандарт IEEE 802.1Q. В этом стандарте определяется, как функционирует VLAN, добавляя к заголовку Ethernet-кадра виртуальный идентификатор локальной сети (VLAN ID), который является частью трафика VLAN-сети.

VLAN ID – это число от 0 до 4095, используемое для идентификации конкретной виртуальной локальной сети, которой принадлежит каждый фрейм. С применением такого механизма Ethernet-фреймы могут принадлежать разным виртуальным локальным сетям и при этом совместно использовать один физический интерфейс.

В основе обработки системой NetDefendOS VLAN-тэговых Ethernet-фреймов на физическом интерфейсе лежат следующие принципы:

- Etnernet-фреймы, полученные системой NetDefendOS от физического интерфейса проверяются на наличие VLAN ID. Если VLAN ID найден и для этого интерфейса определен соответствующий VLAN-интерфейс, NetDefendOS будет использовать этот VLAN-интерфейс в качестве логического интерфейса источника для дальнейшей обработки набором правил.

- Если в Ethernet-фрейме, полученном на интерфейс, нет VLAN ID, то источником фрейма считается физический интерфейс, а не VLAN.

- Если на физический интерфейс принимается VLAN-тэгированный трафик и в конфигурации системы NetDefendOS для этого интерфейса не определен VLAN с соответствующим VLAN ID, то этот трафик отклоняется NetDefendOS и генерируется сообщение журнала *unknown_vlanid.*

- Для одного физического интерфейса NetDefendOS VLAN ID должен быть уникальным, Но тот же самый VLAN ID может использоваться на нескольких физических интерфейсах. Другими словами, один и тот же VLAN может охватывать многие физические интерфейсы.

- Нет необходимости ориентировать физический интерфейс на виртуальные локальные сети, так как он может передавать как VLAN, так и не VLAN-трафик.

Физическое VLAN- соединение с VLAN

На рисунке показаны соединения типичного сценария VLAN системы NetDefendOS.

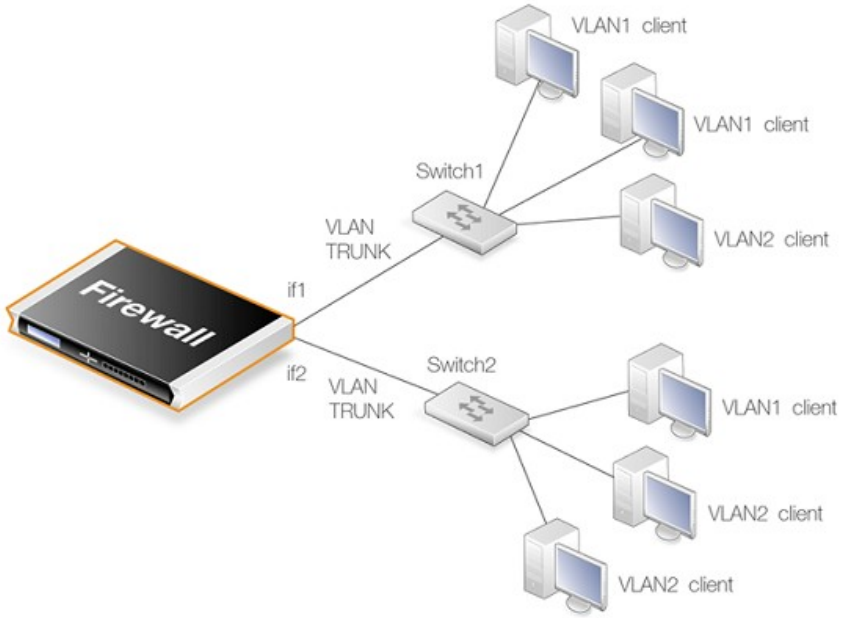


Рис. 3.1. VLAN-соединение

В системе NetDefendOS различают следующие физические соединения VLAN:

- Большинство VLAN-сетей, настроенных на физический интерфейс межсетевого экрана NetDefend, соединяются непосредственно с коммутатором. Эта соединение работает как VLAN-канал. Используемый коммутатор должен поддерживать порт на основе VLAN. Это означает, что каждый порт коммутатора можно настроить с идентификатором ID VLAN-сети или VLAN-сетью, с которой связан порт. Порт коммутатора, который соединяется с межсетевым экраном, должен быть настроен на прием VLAN ID, которые будут проходить через канал.

  На рис.3.1. соединение между коммутаторами *Switch1* и *Switch2* интерфейсов *if1* и *if2* осуществляется по VLAN-каналам.

- Другие порты коммутатора, которые соединяются с пользователями VLAN, настраиваются с индивидуальными VLAN ID. Любое устройство, подключенное к одному из этих портов, автоматически становится частью VLAN, настроенной на этот порт. В коммутаторах Cisco данная конфигурация называется *Static-access VLAN*.

  На рис 3.1. один интерфейс коммутатора *Switch2* настроен для *VLAN1,* а два других предназначены для *VLAN2*.

  Если потребуется, коммутатор также может передать трафик из канала межсетевого экрана в другой канал.

- Несколько интерфейсов на межсетевом экране могут передавать трафик из VLAN-канала, они будут подключаться к отдельным коммутаторам. Несколько каналов могут быть настроены для

передачи трафика с одинаковым VLAN ID.

Примечание: Стандарт 802.1ad не поддерживается

NetDefendOS не поддерживает стандарт IEEE 802.1ad (provider bridges), который позволяет работать VLAN-сети внутри другой VLAN-сети.

Лицензионные ограничения

Число VLAN-интерфейсов, определенных в NetDefendOS, ограничивается параметрами лицензионного соглашения. Различным моделям аппаратного обеспечения соответствуют различные лицензии и разное ограничение на VLAN-сети.

Краткие сведения по установке VLAN

Ниже приведены основные шаги по настройке VLAN-интерфейса:

1. Создать имя VLAN-интерфейса.
2. Выбрать физический интерфейс для VLAN.
3. Создать **VLAN ID**, уникальный на физическом интерфейсе.
4. Дополнительно можно определить IP-адрес для VLAN.
5. Дополнительно можно определить широковещательный IP-адрес для VLAN.
6. Создать требуемые для VLAN маршруты для VLAN в соответствующих таблицах маршрутизации.
7. Создать правила в наборе IP-правил, разрешающие прохождение трафика через VLAN-интерфейс.

Важно понимать, что администратор обращается к VLAN-интерфейсу, как к физическому интерфейсу, которому требуется соответствующие IP-правила и существование маршрутов в конфигурации NetDefendOS для того, чтобы через нее проходил трафик. Например, если нет IP-правила для определенного VLAN-интерфейса в качестве интерфейса источника, позволяющего проходить трафику, то пакеты, поступающие на этот интерфейс, будут отклонены.

Расширенные настройки VLAN

Существует единственная расширенная настройка для VLAN:

Unknown VLAN Tags

Что делать с пакетами, отмеченными с неизвестным идентификатором ID.

По умолчанию: *DropLog*

Пример 3.10. Определение VLAN

В данном простом примере рассматривается определение виртуальной локальной сети *VLAN10 с* идентификатором ID VLAN *10*. Предполагается, что IP-адрес VLAN уже определен в адресную книгу как объект *vlan10_ip.*

CLI

```
gw-world:/> add Interface VLAN VLAN10 Ethernet=lan
Network=all-nets VLANID=10
```

Web-интерфейс

1. Перейти к **Interfaces > VLAN > Add > VLAN**

2. Ввести:

- **Name**: ввести имя, например *VLAN10*
- **Interface:** lan
- **VLAN ID:** 10
- **IP Address**: vlan10_ip
- **Network:** all-nets

4.Нажать кнопку **OK**

3.3.4. PPPoE

Протокол передачи кадров PPP через Интернет - Point-to-Point Protocol over Ethernet (PPPoE) – туннелирующий протокол, используемый для подключения нескольких пользователей Ethernet-сети к Интернету через общий интерфейс, такой как одна DSL-линия, беспроводное устройство или кабельный модем. Общее соединение делится между всеми пользователями Ethernet, контроль доступа может осуществляться на основе каждого пользователя.

Для подключения к широковещательным сервисам Интернет-провайдеры (Internet server providers (ISPs)) часто требуют от пользователей использование PPPoE-протокола. При использовании PPPoE Интернет-провайдер может:

- Осуществлять безопасность и контроль доступа, используя имя пользователя/пароль для аутентификации
- Трассировка IP-адресов конкретных пользователей
- Автоматического распределения IP-адресов для пользователей ПК (аналогично DHCP). IP-адрес может резервироваться из расчета на группу пользователей.

Протокол PPP

Протокол точка-точка - Point-to-Point Protocol (PPP) – протокол, предназначенный для соединения двух компьютеров, использующих одинаковый интерфейс, например в случае соединения персонального компьютера через коммутируемую телефонную линию с Интернет-провайдером.

С точки зрения многоуровневой модели OSI, PPP сопровождается механизмом инкапсуляции второго уровня, позволяющим прохождение пакета любого протокола через IP-сети. PPP использует

протокол управления связью - Link Control Protocol (LCP), для создания соединений, настроек и тестирования. После инициализации LCP-протокола один или несколько протоколов управления сетью - Network Control Protocols (NCPs) – могут использоваться при передаче трафика для определенного набора протоколов, таким образом, несколько протоколов могут взаимодействовать на одной линии, например, оба протокола – IP и IPX – могут совместно использовать PPP-соединение.

PPP-аутентификация (PPP Authentication)

PPP-аутентификация не является обязательным свойством в PPP-протоколе. Аутентификацию протоколов поддерживают: протокол аутентификации по паролю - *Password Authentication Protocol* (PAP), протокол аутентификации по запросу при установлении соединения - *Challenge Handshake Authentication Protocol* (CHAP) и *Microsoft CHAP* (версии 1 и 2). При использовании аутентификации хотя бы один из пользователей должен идентифицировать себя до того, как параметры протокола сетевого уровня согласовываются с помощью протокола NCP. Во время совместной работы LCP и NCP могут договориться об использовании дополнительных типов кодирования.

Конфигурация PPPoE-клиента

PPPoE-протокол позволяет PPP работать через Ethernet, межсетевой экран, требующий использовать один из обычных Ethernet-интерфейсов, запускается через PPPoE.

Каждый PPPoE-туннель интерпретируется как логический интерфейс системы NetDefendOS, с некоторой маршрутизацией и возможностью настройки как у обычных интерфейсов и с IP-правилами, применяемыми ко всему трафику. Для сетевого трафика, входящего на межсетевой экран через PPPoE-туннель, в качестве интерфейса источника (Source Interface) является интерфейс PPPoE-туннеля. Для исходящего трафика интерфейс PPPoE-туннеля будет интерфейсом назначения (Destination Interface).

Как с любым интерфейсом, несколько маршрутов определяются так, что система NetDefendOS знает, на какой IP-адрес должен быть принят трафик и куда следует отправлять трафик через PPPoE-туннель. PPPoE-клиент можно настроить на использование имени сервиса, с помощью которого можно отличать данный сервер от остальных серверов в Ethernet-сети.

Информация об IP-адресе

Технология PPPoE использует автоматическое назначение IP-адреса (подобно DHCP). Система NetDefendOS, получив информацию об IP-адресе от Интернет-провайдера, сохраняет ее в сетевом объекте и использует в качестве IP-адреса интерфейса.

Аутентификация пользователя

Если Интернет-провайдеру требуется пользовательская аутентификация в автоматической рассылке на PPPoE-сервер системы NetDefendOS можно установить имя пользователя и пароль.

Предоставление канала по требованию (Dial-on-demand)

Если включена функция *dial-on-demand* , PPPoE-соединение произойдет только при наличии трафика на PPPoE-интерфейсе. Существует возможность настройки реакции межсетевого экрана на активность на интерфейсе либо на входящий трафик, либо на исходящий, либо на тот и другой. Кроме того, существует возможность настройки времени ожидания, по истечении которого если не будет передачи данных, то туннель будет разъединен.

Ненумерованные PPPoE (Unnumbered PPPoE)

Когда NetDefendOS действует как PPPoE-клиент, по умолчанию устанавливается *unnumbered PPPoE*. Дополнительно данную опцию можно активировать в настройках для использования PPPoE-сессий.

Unnumbered PPPoE обычно используется, если провайдер распределяет пользователям заранее установленные IP-адреса. Эти IP-адреса вводятся пользователем в компьютере вручную. Интернет-

провайдер не назначает IP-адрес PPPoE-клиенту на момент соединения.

При последующем выборе функции *unnumbered PPPoE* следует учитывать спецификацию уникального IP-адреса, используемого в качестве адреса интерфейса PPPoE-клиента. При использовании таких адресов должны достигаться следующие цели:

- Определенный IP-адрес отправляется к PPPoE-серверу как «preferred IP» (предпочитаемый IP). Если *unnumbered PPPoE* не задан принудительно, сервер может не принять «preferred IP» и назначить другой IP-адрес PPPoE-клиенту.

  Если выбрана опция к принудительному назначению *unnumbered PPPoE*, то клиент (т.е. NetDefendOS) не буде принимать назначение другого IP-адреса на сервере.

- Определенный или назначенный PPPoE-сервером IP-адрес, когда *unnumbered PPPoE* не задан принудительно, принимается в качестве IP-адреса интерфейса PPPoE-клиента. ОН будет использоваться как локальный IP-адрес для трафика исходящего из интерфейса, когда трафик возникает или находится за NAT на межсетевом экране NetDefend.

Примечание: В состав PPPoE включен сетевой протокол Discovery protocol

Для обеспечения соединения точка-точка через Ethernet для каждого PPP-сеанса необходимо установить Ethernet-адрес удаленного пользователя и уникальный сеансовый идентификатор, данную функцию выполняет discovery protocol.

PPPoE не может использоваться с HA

По причинам, связанным со способами разделения IP-адресов в кластерах высокой отказоустойчивости NetDefendOS, PPPoE работает не корректно. PPPoE нельзя настраивать с HA.

Пример 3.11. Настройка PPPoE-клиента

Данный пример показывает, как настроить PPPoE-клиента на *wan*-интерфейсе с трафиком, маршрутизируемым через PPPoE.

CLI

```
gw-world:/> add Interface PPPoETunnel PPPoEClient
EthernetInterface=wan Network=all-nets
Username=exampleuser Password=examplepw
```

Web-интерфейс

1. Перейти к **Interfaces > PPPoE > Add > PPPoE Tunnel**

2. Ввести:

   - **Name:** PPPoEClient
   - **Physical Interface:** wan
   - **Remote Network:** all-nets (т.к. весь трафик направляется в туннель)
   - **Service Name:** Имя сервиса, предусмотренное провайдером
   - **Username:** Имя пользователя, предоставленное провайдером
   - **Password:** Пароль, предоставленный провайдером
   - **Confirm Password:** Проверка пароля
   - В поле **Authentication** определяется, какой используется протокол аутентификации (по умолчанию будет использоваться встроенный протокол)
   - Отключить опцию **Enable dial-on-demand**
   - В поле **Advanced**, если включена опция **Add route for remote network**, будет добавлен новый маршрут для интерфейса

3. Нажать кнопку **OK**

3.3.5. GRE-туннели

Обзор

Протокол общей инкапсуляции маршрутов - *Generic Router Encapsulation* (GRE) - простой инкапсулирующий протокол, который используется при необходимости туннелирования трафика через сети и/или через сетевые устройства. GRE не предоставляет функций безопасности и его использование вызывает крайне низкие расходы.

Использование GRE

GRE обычно применяют в методах, использующихся для объединения двух сетей вместе через третью сеть, такую как Интернет. Объединенные сети связываются с общим протоколом, который туннелируется, использует GRE, промежуточную сеть. Примерами использования GRE являются:

- Обход сетевого оборудования, которое блокирует определенный протокол.
- Туннелирование IPv6- трафика через IPv4-сеть.
- Когда поток UDP-данных является многоадресным и его необходимо передать через сетевое устройство, не поддерживающего многоадресную передачу. GRE допускает туннелирование через сетевое устройство.

Производительность и безопасность GRE-туннелей

Для связи GRE-туннелю не использует кодирование и поэтому сам по себе безопасным не является. Безопасность должен обеспечивать протокол, прокладывающий туннель. Из-за отсутствия шифрования, преимущество GRE заключается в высокой производительности, появляющейся из-за низкой степени обработки трафика.

Отсутствие шифрования может быть приемлемым в тех случаях, когда туннелирование осуществляется через внутреннюю сеть, не имеющую выхода в публичную.

Настройка GRE-туннелей

Подобно другим туннелям системы NetDefendOS, таким как, IPSec-туннели, GRE-туннели рассматриваются как логические интерфейсы системы NetDefendOS, с такой же фильтрацией, управлением скоростью обработки трафика и свойствами конфигурации как в стандартных интерфейсах. Параметры GRE:

- **IP Address (IP-адрес)** – IP-адрес внутри туннеля со стороны локальной сети. Он не может быть пустым и должен принимать определенные значения.

  Указанный IP-адрес будет использоваться для следующих целей:

  i. К данному конечному узлу туннеля могут быть отправлены ICMP PING.

  ii. Сообщения журнала, связанные с туннелем будут генерироваться с этим IP-адресом как с источником

  iii. Если используется NAT, то не будет необходимости настраивать для IP-источника IP-правило, которое обрабатывается NAT, на трафик проходящий через туннель.

- **Remote Network (Удаленная сеть)** – Удаленная сеть, соединение с которой происходит по GRE-туннелю.

- **Remote Endpoint (Удаленная конечная точка)** – IP-адрес удаленного устройства, соединение с которым происходит по туннелю.

- **Use Session Key (Использование сессионного ключа)** – Уникальный номер, который можно дополнительно указать для туннеля. Этот параметр позволяет использовать несколько GRE-туннелей между двумя конечными точками. Значение ключа сессии применяется для того, чтобы различать эти туннели.

- **Additional Encapsulation Checksum (Дополнительная контрольная сумма инкапсуляции)** - GRE-протокол позволяет реализацию дополнительной контрольной суммы как в самом IPv4-протоколе, так и над ним, что обеспечивает дополнительную проверку целостности данных.

Расширенные (**Advanced**) настройки для GRE-интерфейса:

- **Automatically add route for remote network (Автоматическое добавление маршрута для удаленной сети)** – Эта опция, как правило, проверяет таблицу маршрутизации для того, чтобы она автоматически обновлялась. В качестве альтернативы существует возможность создания требуемого маршрута вручную.

- **Address to use as source IP (Адрес, используемый как источник IP)** – Эта опция позволяет задать определенный IP-адрес в качестве IP интерфейса источника для GRE-туннеля. При установке туннеля требуется инициация данного IP-адреса вместо IP-адреса интерфейса, на самом деле устанавливающего туннель.

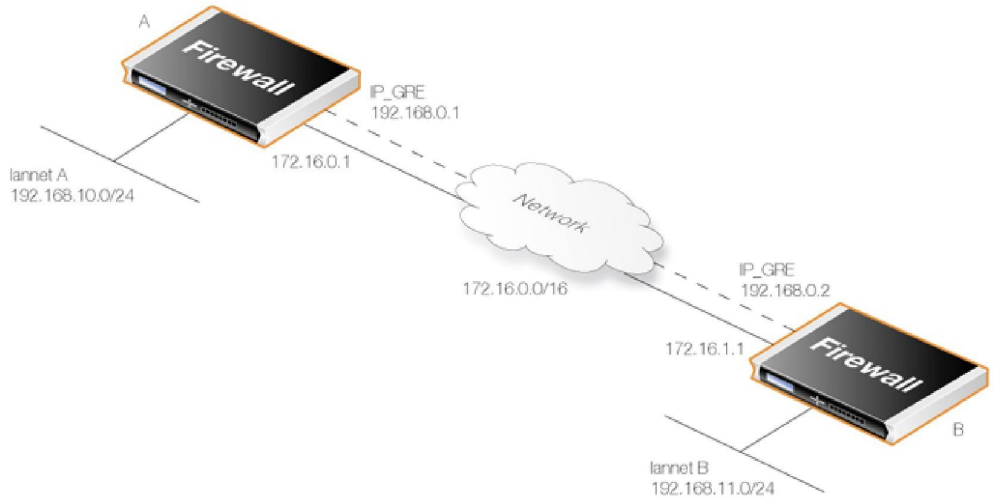
Эта опция применяется, например, если используются публикации ARP и туннель устанавливается с ARP-опубликованными IP-адресами.

GRE и наборы IP-правил

Установленный GRE-туннель еще не означает, что входящий и исходящий из него трафик проверен. Напротив, сетевой трафик, исходящий из GRE-туннеля будет передан системе NetDefendOS для анализа набором IP-правил. Именем интерфейса источника сетевого трафика будет имя связанного с ним туннеля.

То же самое выполняется и для трафика противоположного направления, то есть входящего в GRE-туннель. Кроме того, должен быть определен маршрут (**Route**), для того чтобы система NetDefendOS знала, какие IP-адреса должны быть приняты или отправлены через туннель.

Пример GRE-сценария



На рисунке, приведенном выше, изображен стандартный GRE-сценарий, в котором два межсетевых экрана NetDefend **A** и **B** должны связаться друг с другом через промежуточную внутреннюю сеть *172.16.0.0./16*.

Любой проходящий между **A** и **B** трафик туннелируется через промежуточную сеть, используя GRE-туннель и, поскольку сеть является внутренней, а не публичной, кодирование не требуется.

Настройка для межсетевого экрана NetDefend *"A"*

Предположим, что сеть *192.168.10.0/24* – это **lannet,** организованная на **lan-**интерфейсе, шаги для установки NetDefendOS на межсетевом экране **A** следующие:

1. Настроить в адресной книге следующие IP-объекты:
   - **remote_net_B:** 192.168.11.0/24
   - **remote_gw:** 172.16.1.1
   - **ip_GRE:** 192.168.0.1
2. Создать объект GRE-туннеля с именем **GRE_to_B** со следующими параметрами:
   - **IP Address:** ip_GRE
   - **Remote Network:** remote_net_B
   - **Remote Endpoint:** remote_gw
   - **Use Session Key:** 1
   - **Additional Encapsulation Checksum:** Enabled

3. Определить маршрут в таблице маршрутизации *main*, которая направляет весь трафик на **remote_net_B** по **GRE_to_B** GRE-интерфейса. В этом действии нет необходимости, если включена опция **Add route for remote network** в таблице **Advanced**, так как она добавляет маршрут автоматически.

4. Создать следующие правила в наборе IP-правил, позволяющие трафику проходить через туннель:

Имя	Действие	Интерфейс	Сеть	Интерфейс	Сеть	Сервис

(Name)	(Action)	источника (Src Int)	источника (Src Net)	назначения (Dest Int)	назначения (Dest Net)	(Service)
To_B	Allow	lan	lannet	GRE_to_B	remote_net_B	All
From_B	Allow	GRE_to_B	remote_net_B	lan	lannet	All

Настройка для межсетевого экрана NetDefend *"B"*

Предположим, что сеть *192.168.11.0/24* - это **lannet,** организованная на **lan-**интерфейсе, шаги для установки NetDefendOS на межсетевом экране **B** следующие:

1. Настроить в адресной книге следующие IP-объекты:
   - **remote_net_A:** 192.168.10.0/24
   - **remote_gw:** 172.16.0.1
   - **ip_GRE:** 192.168.0.2
2. Создать объект GRE-туннеля с именем **GRE_to_ A** со следующими параметрами:
   - **IP Address:** ip_GRE
   - **Remote Network:** remote_net_A
   - **Remote Endpoint:** remote_gw
   - **Use Session Key:** 1
   - **Additional Encapulation Checksum:** Enabled
3. Определить маршрут в основной таблице маршрутизации, которая направляет весь трафик на **remote_net_ A** по **GRE_to_ A** GRE-интерфейса. В этом действии нет необходимости, если включена опция **Add route for remote network** в таблице **Advanced**, так как она добавляет маршрут автоматически.
4. Создать следующие правила в наборе IP-правил, позволяющие трафику проходить через туннель:

Имя (Name)	Действие (Action)	Интерфейс источника (Src Int)	Сеть источника (Src Net)	Интерфейс назначения (Dest Int)	Сеть назначения (Dest Net)	Сервис (Service)
To_A	Allow	lan	lannet	GRE_to_A	remote_net_A	All
From_A	Allow	GRE_to_A	remote_net_A	lan	lannet	All

Проверка статуса GRE-туннеля

Статус IPsec-туннелей может быть либо активным, либо неактивным. Это не применяется для GRE-туннелей в системе NetDefendOS. Статус GRE-туннеля может быть активным, если он существует в конфигурации.

Однако можно проверить, что происходит с GRE-туннелем. Например, если туннель называется gre_interface, то можно использовать CLI-команду *ifstat*:

```
gw-world:/> ifstat gre_interface
```

Выполнение этой команды покажет, что происходит с туннелем, а параметры команды *ifstat* могут обеспечить различные детали.

3.3.6. Interface Groups (Группы интерфейсов)

Любой набор интерфейсов системы NetDefendOS может быть объединен в одну группу. После чего эти интерфейсы будут действовать как отдельный сконфигурированный объект системы NetDefendOS, который может быть использован в создании политик безопасности в пределах одной группы. Когда группа используется, например, как интерфейс источника в IP-правиле, любой из интерфейсов в группе может обеспечить соответствие правилу.

Группа может состоять из обычных Ethernet-интерфейсов или из интерфейсов других типов, таких как VLAN-интерфейсы или VPN-туннели. Кроме того, членам группы не требуется быть одного типа. Группа может состоять, например, из комбинации 2 Ethernet-интерфейсов и 4 VLAN-интерфейсов.

Пример 3.12. Создание группы интерфейсов

CLI

```
gw-world:/> add Interface InterfaceGroup examplegroup
                          Members=exampleif1,exampleif2
```

Web-интерфейс

1. Перейти к **Interfaces > Interface Groups > Add > InterfaceGroup**

2. Ввести следующую информацию для определения группы:

   - **Name:** имя группы будет использоваться позже
   - **Security/Transport Equivalent**: Если эта опция включена, то группа интерфейсов может использоваться в качестве интерфейса назначения в правилах, где соединениям возможно потребуется перемещение между интерфейсами.
   - **Interfaces:** Выбор интерфейсов в группу

3. Нажать кнопку **OK**

3.4. ARP

3.4.1. Обзор

Протокол определения адресов - *Address Resolution Protocol* (ARP) позволяет преобразовывать адрес протокола сетевого уровня (уровень 3 архитектуры OSI) в физический адрес канального уровня (уровень 2 архитектуры OSI). В сети передачи данных используется для преобразования IP-адреса в соответствующий ему Ethernet-адрес. ARP действует на 2 уровне архитектуры OSI – канальном, он инкапсулируется в Ethernet-заголовки для передачи.

Совет: Уровни OSI

*Информация об **архитектуре OSI** приведена в **приложении D**.*

IP-адресация через Ethernet

Хост в Ethernet-сети может связаться с другим хостом, только если известен Ethernet-адрес (MAC-адрес) этого хоста. Протоколы более высоких уровней, такие как IP-протокол, используют IP-адреса, которые существенно отличаются от физических адресов низших уровней, таких как MAC-адрес. ARP применяется для получения Ethernet MAC-адреса хоста с использованием его IP-адреса.

При необходимости получения IP-адреса из соответствующего Ethernet-адреса хост отправляет пакет с ARP-запросом. Пакет с ARP-запросом содержит MAC-адрес источника, IP-адрес источника и IP-адрес получателя. Каждый хост в локальной сети получает этот пакет. Хост с указанным IP-адресом назначения посылает пакет с ARP-ответом со своим MAC-адресом первому хосту.

3.4.2. ARP-кэш (ARP Cache) системы NetDefendOS

ARP-кэш сетевых устройств, таких как коммутаторы и межсетевые экраны, является важным компонентом в реализации ARP. ARP-кэш состоит из динамической таблицы, в которой хранятся соответствия между IP и Ethernet-адресами.

Система NetDefendOS использует ARP-кэш также как другие сетевые устройства. При запуске системы ARP-кэш не заполнен и заполняется записями по мере поступления трафика.

Типичное содержание минимальной таблицы ARP-кэша выглядит примерно следующим образом:

Тип (Type)	IP-адрес (IP Address)	Ethernet-адрес (Ethernet address)	Expires
Dynamic	192.168.0.10	08:00:10:0f:bc:a5	45
Dynamic	193.13.66.77	0a:46:42:4f:ac:65	136
Publish	10.5.16.3	4a:32:12:6c:89:a4	-

Разъяснение записей таблицы:

- Первая запись в этом ARP-кэше – динамическая ARP-запись, которая говорит о том, что IP-адрес *192.168.0.10* соответствует Ethernet-адресу *08:00:10:0f:bc:a5*.
- Вторая запись в таблице динамически отображает преобразование IP-адреса *193.13.66.77* к Ethernet-адресу *0a:46:42:4f:ac:65*.
- Третья запись является статической ARP-записью, связанной с преобразованием IP-адреса *10.5.16.3* к Ethernet-адресу *4a:32:12:6c:89:a4*.

Столбец *Expires*

В третьем столбце таблицы величина *Expires* используется для обозначения времени пребывания конкретной записи в ARP-кэше.

В первой строке, например, эта величина равна *45*, то есть запись будет признана недействительной и будет удалена из ARP-кэша через 45 секунд. Если трафик направляется к IP-адресу *192.168.0.10* по истечении этого срока, то система NetDefendOS отправляет новый ARP-запрос.

По умолчанию для динамической записи это время составляет 900 секунд (15 минут), но его можно изменить с помощью опции **ARP Expire**.

Расширенная опция **ARP Expire Unknown** определяет, как долго система NetDefendOS будет хранить ошибочные адреса. Это ограничение необходимо для того, чтобы предотвратить непрерывные запросы системы NetDefendOS. Значение по умолчанию для этого параметра составляет 3 секунды.

Пример 3.13. Отображение ARP-кэша

Содержимое ARP-кэша можно отобразить, используя CLI.

CLI

```
gw-world:/> arp -show
ARP cache of iface lan

Dynamic 10.4.0.1 = 1000:0000:4009 Expire=196
Dynamic            10.4.0.165            =            0002:a529:1f65            Expire=506
```

Очистка ARP-кэша (*flushing*)

Если при изменении аппаратного обеспечения IP-адрес хоста не изменился, то наиболее вероятно, что будет использоваться новый MAC-адрес. Если в системе NetDefendOS присутствуют старые ARP-записи для этого хоста в его ARP-кэше, то эти записи станут недействительными в связи с изменением MAC-адреса и данные, отправленные к данному хосту, не достигнут назначения.

После истечения срока действия ARP, NetDefendOS узнает новый MAC-адрес хоста, но иногда может возникнуть необходимость принудительного обновления. Саамы простой способ заключается в очистке ARP-кэша (*flushing*). При очистке все динамические ARP записи удаляются из кэша, что принуждает NetDefendOS посылать новые ARP-запросы для обнаружения соответствия MAC/IP-адресов для подключенных хостов.

Очистку можно осуществить, используя CLI-команду *arp-flush*:

Пример 3.14. Очистка ARP-кэша

В этом примере рассматривается, как очистить ARP-кэш через командную строку.

CLI

```
gw-world:/> arp –flush
ARP cache of all interfaces flushed.
```

Размер ARP-кэша

По умолчанию ARP-кэш может содержать 4096 записей одновременно. Этого достаточно для большинства сценариев, но в редких случаях, например, когда несколько очень больших LAN-сетей непосредственно подключены к межсетевому экрану, в этом случае может потребоваться настройка этой величины. Размер ARP-кэша можно изменять с помощью расширенной опции *ARP Cache Size*.

Для быстрого поиска записей в ARP-кэше используются хэш-таблицы. Для достижения максимальной эффективности хэш-таблица должна быть в два раза больше количества записей с индексами, так если самая крупная непосредственно подключенная LAN-сеть, содержит 500 IP-адресов, размер хэш-таблицы должен быть не менее 1000. Администратор может изменять опцию *ARP Hash Size* в расширенных настройках ARP, по умолчанию значение этого параметра составляет 512.

Опция **ARP Hash Size VLAN** подобна опции **ARP Hash Size,** но влияет на размер хэша для VLAN-интерфейсов. Значение по умолчанию 64.

3.4.3. Создание ARP-объектов

Для изменения метода системы NetDefendOS, обрабатывающего ARP на интерфейсе, администратор может создать в системе NetDefendOS ARP-объекты, каждый из которых имеет следующие параметры:

Mode	Тип ARP-объекта. Может быть одним из: • Static – Создание фиксированного отображения в локальном ARP-кэше. • Publish – публикация IP-адреса на определенном MAC-адресе (или на этом интерфейсе). • XPublish – публикация IP-адреса на определенном MAC-адресе и “неправда” о MAC-адресе, отправляющем Ethernet-фрейм, содержащий ARP-ответ.
Interface	Локальный физический интерфейс для ARP-объекта.
IP Address	IP-адрес для MAC/IP-преобразования.
MAC Address	MAC-адрес для MAC/IP-преобразования.

Три ARP-режима *Static*, *Publish* и *XPublish* будут рассмотрены ниже.

Режим Static

Статический (*Static*) ARP-объект добавляет определенное отображение MAC/IP-адреса в ARP-кэш системы NetDefendOS.

Наиболее часто статические ARP-объекты применяются в таких ситуациях, когда некоторые внешние сетевые устройства не корректно отвечают ARP-запросы и отправляют неправильный MAC-адрес. Такие проблемы характерны для некоторых сетевых устройств, таких как беспроводные модемы.

Статические ARP-объекты могут также использоваться для фиксации IP-адреса к определенному MAC-адресу в целях повышения безопасности или для того, чтобы избежать отказа в обслуживании при наличии в сети незаконных пользователей. Однако, такая защита действует только на пакеты, посылаемые на данный IP-адрес, и не распространяется на пакеты, отправляемые с данного адреса.

Пример 3.15. Определение статических ARP-записей

В данном примере рассматривается создание статического соответствия между IP-адресом 192.168.10.15 и Ethernet-адресом *4b:86:f6:c5:a2:14* на lan-интерфейсе:

CLI

```
gw-world:/> add ARP Interface=lan IP=192.168.10.15 Mode=Static
                          MACAddress=4b-86-f6-c5-a2-14
```

Web-интерфейс

1. Перейти к **Interfaces > ARP > Add > ARP**

2. Выбрать из следующих выпадающих списков:

   • **Mode:** Static

   • **Interface:** lan

3. Ввести следующее:

   • **IP Address:** 192.168.10.15

   • **MAC:** 4b-86-f6-c5-a2-14

4. Нажать кнопку **OK**

Опубликованные ARP-объекты

При необходимости, вместо MAC-адресов интерфейсов, система NetDefendOS поддерживает публикацию (*publishing)* IP-адресов на определенном интерфейсе вместе с конкретным MAC-адресом. NetDefendOS будет отправлять ARP-ответы на любые ARP-запросы, получаемые на интерфейс, связанный с опубликованными IP-адресами.

Публикацию ARP-адресов можно осуществлять по ряду причин:

- Для создания представления о том, что на интерфейсе системы NetDefendOS используется несколько IP-адресов.

  Этот бывает полезно, если несколько отдельных IP-диапазонов распределяются на единственной LAN-сети. В каждом IP-диапазоне хосты могут использовать шлюз в собственном диапазоне в том случае, когда эти адреса шлюза опубликованы на соответствующем интерфейсе NetDefendOS.

- Другой способ использования – публикация множественных адресов на внешнем интерфейсе, что позволяет системе NetDefendOS преобразовывать статический адрес трафика во множественные адреса и далее отправлять их к внутреннему серверу с приватными IP-адресами.

- Менее распространенной причиной является помощь соседнему сетевому устройству в случае отправки ARP в некорректной форме.

Режимы публикации

Различают два режима публикации, доступные при публикации пары MAC/IP-адресов:

- **Publish**
- **XPublish**

И в том, и в другом случаях определяются IP-адрес и связанный с ним MAC-адрес. Если MAC-адрес не определен (все нули), то используется MAC-адрес физического интерфейса отправки.

Отличие Publish от XPublish заключается в следующем: при отправке ARP-запроса в ответ система NetDefendOS получает два MAC-адреса в Ethernet-фрейме:

1. В Ethernet-фрейме MAC-адрес Ethernet-интерфейса, отправляющего ответ,.
2. MAC-адрес в ARP-ответе, который содержится внутри этого фрейма. Как правило, но не обязательно, он такой же как (**1**) MAC-адреса источника в Ethernet-фрейме.

На рисунке, приведенном ниже, показан Ethernet-фрейм, содержащий ARP-запрос:

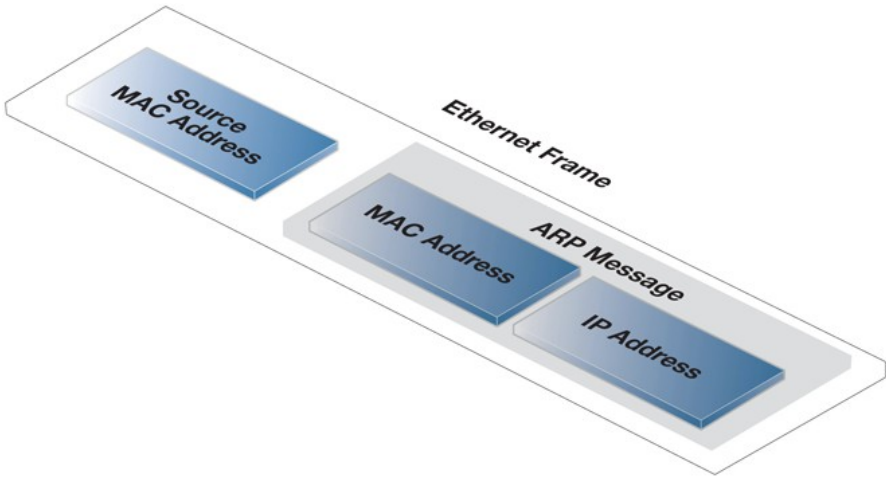


Рисунок 3.2. ARP-ответ в Ethernet-фрейме

Режим *Publish* использует реальный MAC-адрес интерфейса отправления для адреса (**1**) в Ethernet-фрейме.

Иногда некоторому сетевому оборудованию в ответе требуются оба MAC-адреса (**1** и **2**), которые будут совпадать. В этом случае используется режим *XPublish*, так как он изменяет оба MAC-адреса в ответе, содержащем опубликованный MAC-адрес. Другими словами, *XPublish* "лжет" об источнике адреса в ARP-ответе.

Если опубликованный MAC-адрес совпадает с MAC-адресом физического интерфейса результат работы *Publish* и *XPublish* будет одинаковый.

Публикация всех сети

При использовании ARP-записей, IP-адреса могут быть опубликованы только по одному. Тем не менее, администратор может использовать альтернативный метод Proxy ARP в системе NetDefendOS для обработки публикации всей сети (см. *Раздел 4.2.6, "Proxy ARP"*).

3.4.4. Использование расширенных настроек ARP

В этом разделе представлены некоторые расширенные настройки, связанные с ARP. В большинстве случаев эти настройки не следует менять, но в некоторых устройствах изменения могут быть необходимы.

Многоадресная (Multicast) и широковещательная (Broadcast) рассылки

ARP-запросы и ARP-ответы, содержащие адреса многоадресной или широковещательной рассылок, как правило, не корректны, за исключением некоторой балансировки нагрузки и избыточности устройств, которые используются на физическом уровне адресов многоадресной рассылки.

По умолчанию система NetDefendOS отклоняет и регистрирует такие ARP-запросы и ARP-ответы. Однако, эти настройки могут быть изменены с помощью расширенных опций **ARP Multicast** и **ARP Broadcast**.

Незапрашиваемые (Unsolicited) ARP-ответы

Вполне возможно, что хост, подключенный к сети, отправляет ARP-ответы системе NetDefendOS даже если не вызывались соответствующие ARP-запросы. Такие ответы называют незапрашиваемыми ARP-ответами.

Согласно спецификации ARP, получатель должен принимать эти типы ARP-ответов. Но, поскольку данная процедура уменьшает безопасность локального соединения, по умолчанию NetDefendOS регистрирует и отклоняет эти ответы.

Эти установки можно изменить с помощью расширенных настроек **Unsolicited ARP Replies**.

ARP-запросы

В спецификации ARP предусмотрено обновление ARP-кэша данными из ARP-запросов, полученными от других хостов. Но, поскольку данная процедура уменьшает безопасность локального соединения, система NetDefendOS, как правило, не позволяет этого.

Для того чтобы поведение системы соответствовало спецификации RFC 826, администратор может изменить настройку **ARP Requests**. Даже если состояние опции – *Drop* (то есть пакеты отброшены без сохранения), система NetDefendOS уведомит о получении запроса при соответствии его другим правилам.

Изменения в ARP-кэше

В системе NetDefendOS предусмотрена опция для управления изменениями ARP-кэша.

Получаемые ARP-запросы или ARP-ответы могут изменить существующую запись в ARP-кэше. При выполнении данной опции уменьшается безопасность локального соединения. Но отсутствие данной опции может вызвать проблемы в случае, например, при замене сетевого адаптера, поскольку система NetDefendOS не будет принимать новый адрес, до тех пор, пока не истечет время предыдущей записи.

Расширенная настройка **Static ARP Changes** может изменить данный режим работы. По умолчанию система NetDefendOS позволяет изменениям вступать в силу и регистрирует их.

Похожая проблема возникает при появлении конфликта между статическими записями в ARP-кэше и информацией в ARP-запросах или ARP-ответах. Таких ситуаций не должно быть и изменение настройки **Static ARP Changes** позволяют администратору определить, следует ли регистрировать такие ситуации.

Отправитель с IP-адресом 0.0.0.0

Систему NetDefendOS можно настроить для обработки ARP-запросов, полученных с IP-адреса *0.0.0.0*. Отправитель с таким IP-адресом никогда не получит ответа, но сетевые устройства иногда задают ARP-вопрос отправителю с «не определенным» ("unspecified") IP-адресом. Как правило, такие ARP-ответы отклоняются и регистрируются, но поведение системы изменить с помощью опции **ARP Query No Sender**.

Соответствие Ethernet-адресов

По умолчанию система NetDefendOS будет требовать, чтобы адрес отправителя на Ethernet-уровне соответствовал Ethernet-адресу, сообщаемому в ARP-данных. Если это условие не выполняется, ответ будет отклонен и зарегистрирован в журнале. Поведение системы можно изменить с помощью опции **ARP Match Ethernet Sender**.

3.4.5. Краткое описание расширенных настроек

В ARP доступны следующие расширенные настройки:

ARP Match Ethernet Sender

Определяется, если система NetDefendOS потребует согласовать адрес отправителя на Ethernet-уровне с физическим адресом, сообщаемым в ARP-данных.

По умолчанию: *DropLog*

ARP Query No Sender

Обрабатывает ARP-запросы от отправителя с IP-адресом *0.0.0.0*. Отправитель с таким IP-адресом никогда не получит ответа, но сетевые устройства иногда задают ARP-вопрос отправителю с «не определенным» ("unspecified") IP-адресом.

По умолчанию: *DropLog*

ARP Sender IP

Определяется, если IP-адрес отправителя должен согласовываться с правилами в разделе доступа (Access section).

По умолчанию: *Validate*

Unsolicited ARP Replies

Определяет, как NetDefendOS будет обрабатывать ARP-ответы, которые она не запрашивала. В соответствии с ARP-спецификацией получатель должен принимать такие ответы. Но, поскольку данная процедура уменьшает безопасность локального соединения, по умолчанию она отключена.

По умолчанию: *DropLog*

ARP Requests

Определяет, будет ли система NetDefendOS автоматически добавлять данные из ARP-запросов в ее ARP-таблицы. Согласно спецификации ARP это свойство должно быть выполнено, но поскольку данная процедура уменьшает безопасность локального соединения, по умолчанию она отключена. Даже если опция **ARPRequests** установлена в положение "Drop", которое означает, что пакет отклоняется без сохранения, система NetDefendOS будет отвечать на этот пакет, при соответствии его другим правилам.

По умолчанию: *Drop*

ARP Changes

Определяет, что будет делать NetDefendOS с ситуациями, когда получение ARP-запроса или ARP-ответа приводит к изменению существующей записи в ARP-таблице. При выполнении данной опции уменьшается безопасность локального соединения. Однако выключение данной опции может вызвать проблемы в случае, например, при замене сетевого адаптера, поскольку система NetDefendOS не будет принимать новый адрес, до тех пор, пока не истечет время предыдущей записи.

По умолчанию: *AcceptLog*

Static ARP Changes

Определяет, как система NetDefendOS будет обрабатывать ситуации, когда получение ARP-запроса или ARP-ответа приводит к изменению существующей записи в ARP-таблице. Такой случай

маловероятен, но эта опция позволяет определить, следует ли регистрировать такие ситуации.

По умолчанию: *DropLog*

ARP Expire

Определяется время хранения обычной динамической записи в ARP-таблице до удаления этой записи из таблицы.

По умолчанию: *900 seconds (15 minutes)*

ARP Expire Unknown

Определяет в секундах, как долго система NetDefendOS будет хранить ошибочные адреса. Это делается для того, чтобы NetDefendOS не получала постоянно запросы с таких адресов.

По умолчанию: *3*

ARP Multicast

Определяет, как система NetDefendOS решает вопросы, связанные с ARP-запросами и ARP-ответами, в состоянии которых указано, что они являются адресами с многоадресной рассылкой. Такие сообщения, как правило, не корректны, за исключением некоторой балансировки нагрузки и избыточности устройств, которые используют физический уровень адресов многоадресной рассылки.

По умолчанию: *DropLog*

ARP Broadcast

Определяет, как система NetDefendOS решает вопросы, возникающие с ARP-запросами и ARP-ответами, в состоянии которых указано, что они являются адресами с многоадресной рассылкой. Такие сообщения, как правило, не корректны.

По умолчанию: *DropLog*

ARP cache size

Максимальное количество записей в ARP-кэше.

По умолчанию: *4096*

ARP Hash Size

Хэш используется для быстрого поиска данных в таблице. Для достижения максимальной эффективности хэш должен быть в два раза больше таблицы с индексами. Если самая крупная непосредственно подключенная LAN-сеть, содержит 500 IP-адресов, размер хэш-таблицы должен быть не менее 1000.

По умолчанию: *512*

ARP Hash Size VLAN

Хеширование используется для быстрого поиска записей в таблице. Для достижения максимальной эффективности размер хеша должен быть в два раза больше таблицы с индексами, поэтому если самая крупная непосредственно подключенная VLAN-сеть, содержит 500 IP-адресов, размер хеш-таблицы должен быть не менее 1000.

По умолчанию: *64*

ARP IP Collision

Определяет поведение системы при получении ARP-запроса от получателя, IP-адрес которого противоречит одному из уже используемых на принимающем интерфейсе. Возможны следующие состояния: Drop или Notify.

По умолчанию: *Drop*

3.5. Наборы IP-правил

3.5.1. Политики безопасности (Security Policies)

Перед детальным рассмотрением наборов IP-правил в данном руководстве сначала рассматривается общая концепция политик безопасности, к которым принадлежат устанавливаемые наборы IP-правил.

Характеристики политики безопасности

Политики безопасности системы NetDefendOS настраиваются администратором для регулирования метода, в соответствии с которым трафик может проходить через межсетевой экран NetDefend. Такие политики описываются содержанием различных наборов правил системы NetDefendOS. Набора правил разделяются общими методами, с указанными критериями фильтрации, определяющими тип трафика, к которым они будут применяться. Возможные критерии фильтрации состоят из:

Source Interface	**Интерфейс** или **группа интерфейсов** межсетевого экрана NetDefend, на который приходит пакет. Им также может быть VPN-туннель.
Source Network	Сеть, содержащая IP-адрес источника пакета. Сетью источника может быть IP-объект системы NetDefendOS, который может определяться единственным IP-адресом или диапазоном адресов.
Destination Interface	**Интерфейс** или **группа интерфейсов** межсетевого экрана NetDefend, с которого отправляется пакет. Им также может быть VPN-туннель.
Destination Network	Сеть, которой принадлежит IP-адрес назначения пакета. Сетью назначения может быть IP-объект системы NetDefendOS, который может определяться единственным IP-адресом или диапазоном адресов.
Service	Тип протокола, к которому принадлежит пакет. Сервисные объекты определяют тип протокола/порта. Например, **HTTP** и **ICMP**. Сервисные объекты также определяют любой ALG, который будет применяться к трафику. Системой NetDefendOS предоставляет большое число встроенных сервисных объектов, но у администратора также существует возможность создания клиентских сервисов. Существующие сервисные объекты можно объединять в сервисные группы. Более подробная информация об этой теме приведена в

Разделе 3.2. "Сервисы".

Наборы правил политики безопасности системы NetDefendOS

Основные наборы правил системы NetDefendOS, которые определяют политики безопасности NetDefendOS и используют параметры фильтрации, описанные выше (сети/интерфейсы/сервис) включают в себя:

- **IP-правила**

  Определяют, какой трафик может проходить через межсетевой экран NetDefend, а также определяет, требуется ли трафику преобразование адреса. IP-правила описаны ниже.

- **Pipe-правила**

  Определяют, какой трафик активирует формирование трафика, более подробная информация приведена в *Разделе 10.1, "Формирование трафика"*.

- **Правила маршрутизации на основе правил**

  Определяют таблицы маршрутизации, используемой для трафика. Более подробная информация приведена в *Разделе 4.3, "Маршрутизация на основе правил (Policy-based Routing)"*.

- **Правила аутентификации**

  Определяют, какой трафик активизирует аутентификацию (сеть источника/только интерфейс), более подробная информация приведена в Главе 8, «Пользовательская аутентификация».

IP-правила и заданный по умолчанию набор IP-правил *main*

Наборы IP-правил – наиболее важная часть среди наборов правил политик безопасности. Они определяют функции фильтрации пакетов системы NetDefendOS, решающие что пропускать или не пропускать через межсетевой экран NetDefend и, если это необходимо, преобразовывать адреса подобно функции NAT. По умолчанию в системе NetDefendOS всегда существует один набор IP-правил, который называется *main*.

Существуют два возможных способа передачи трафика через межсетевой экран NetDefend:

- Отклоняется весь трафик, кроме разрешенного.
- Или пропускается весь трафик, кроме запрещенного.

Для обеспечения лучшей безопасности в системе NetDefendOS применяется первый метод. Это означает, что при первой установке и запуске в системе NetDefendOS не определены IP-правила в наборе IP-правил *main* и весь трафик отклоняется. Для прохождения любого трафика через межсетевой экран NetDefend (включая разрешение NetDefendOS реагировать на запросы ICMP *Ping)* администратором должны быть определены некоторые IP-правила.

Каждое IP-правило, которое добавляется администратором, будет определяться следующими критериями фильтрации:

- От какого интерфейса, к какому будет передаваться трафик.
- От какой сети, к какой будет передаваться трафик.
- Какой задействован вид протокола (*сервиса*).
- Какое действие правила будет выбрано, когда найденное соответствие инициирует фильтр.

Определение интерфейса Any или сети

При определении критериев фильтрации в любом из наборов правил, указанных выше можно воспользоваться следующими опциями:

- Для сети источника или назначения опция all-nets эквивалентна IP-адресам 0.0.0.0/0, то есть приемлем любой IP-адрес.
- Для интерфейса источника или назначения может использоваться опция any, при использовании которой система NetDefendOS не определяет интерфейсы входящего и исходящего трафика.
- Интерфейс core можно назначить как интерфейс назначения. Это означает, что система NetDefendOS будет реагировать на трафик типа ICMP Ping, предназначенный для самого межсетевого экрана NetDefend.

Создание правила Drop All

Трафик, не соответствующий ни одному правилу в наборе IP-правил, отклоняется системой NetDefendOS по умолчанию. Для регистрации трафика в журнал (регистрацию активизировать) рекомендуется использовать четкое правило с установленным действием - *Drop* - для источника/назначения сетей/интерфейсов. Такое правило часто упоминается как правило *drop all*.

Потоку трафика требуется IP-правило и маршрут

Как было сказано выше, при запуске NetDefendOS в первый раз IP-правила по умолчанию отклоняют весь трафик и для прохождения трафика необходимо добавить хотя бы одно правило. Фактически в системе NetDefendOS должны быть представлены два компонента:

- В таблице маршрутизации системы NetDefendOS должен существовать маршрут, определяющий на какой интерфейс отправить пакеты, чтобы они достигли места назначения.
- Для поиска интерфейса, на который отправлен пакет, также должен существовать второй маршрут.
- IP-правило в наборе IP-правил системы NetDefendOS, определяющее политику безопасности, которая позволяет пропускать пакеты с интерфейса и сети источника через межсетевой экран NetDefend на интерфейс, определенный маршрутом.

Если используется IP-правило *Allow*, то по умолчанию это двунаправленное движение.

Важен порядок выполнения этих шагов. Сначала для определения последующего интерфейса происходит поиск маршрута, затем NetDefendOS ищет IP-правило, которое позволяет трафику проходить через этот интерфейс. Если такие правила не существуют, то трафик отклоняется.

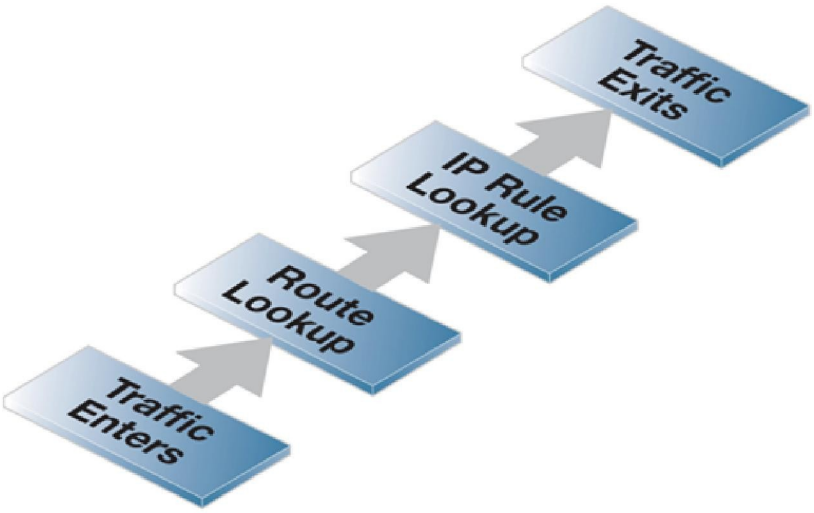


Рисунок 3.3. Упрощенное изображение потока трафика через систему NetDefendOS

Данное изображение потока трафика является упрощенным описанием, более подробная информация приведена в Разделе 1.3, «NetDefendOS State Engine Packet Flow».

Например, прежде чем начать поиск маршрута система NetDefendOS проверяет сеть источника полученного трафика на наличие соответствующего интерфейса. Это делается путем выполнения системой NetDefendOS механизма обратного поиска маршрута (*reverse route lookup*), то есть таблицы маршрутизации ищутся для маршрута, который указывает, что сеть должна быть найдена на данном интерфейсе.

При двунаправленном соединении должен логически существовать второй маршрут и с ним должна быть связанна пара маршрутов (по одному для каждого направления).

3.5.2. Сравнение IP-правил

При создании через межсетевой экран NetDefend нового соединения, например TCP/IP-соединения, сравнение IP-правил происходит сверху вниз до обнаружения правила, соответствующего параметрам нового соединения. Затем выполняется действие ***Action***.

Если действие разрешающее, то происходит создание нового соединения. Система NetDefendOS добавляет информацию о состоянии нового соединения во внутреннюю таблицу состояний, которая позволяет осуществить мониторинг открытых и активных соединений, проходящих через межсетевой экран NetDefend. Если соединение соответствует правилам *Drop* или *Reject*, то оно отклоняется.

Совет: Правила в неправильном порядке иногда вызывают проблемы

Важно помнить, что принцип поиска IP-правил в системе NetDefendOS – сверху вниз, до первого подходящего правила.

Если IP-правило игнорируется, следует проверить список правил, идущих выше, возможно оно не срабатывает в первую очередь.

Stateful Inspection

После первоначального сравнения с правилами, открывающими соединение, последующим пакетам, связанным с этим соединением, не требуется индивидуальное сравнение с набором правил. Вместо этого высокоэффективный алгоритм поиска в таблице состояний определяет принадлежность каждого пакета к установленному соединению.

Такой подход получил название *stateful inspection (проверка состояний с учетом состояния протокола),* его можно применять не только для протоколов, использующих информацию о состояниях (TCP), но и для протоколов, не использующих информацию о состояниях, «псевдо-соединениях», таких как UDP и ICMP. Этот подход означает, что сравнение на соответствие наборам IP-правил осуществляется только на этапе открытия соединения. Размер наборов IP-правил не оказывает большого влияния на общую пропускную способность.

Первый принцип соответствия

Если несколько правил соответствуют некоторым параметрам, то соединение будет обрабатываться в соответствии с тем правилом, которое при сканировании было найдено раньше остальных в списке наборов правил.

Исключения составляют правила SAT, поскольку они зависят от коммутирования со вторым правилом. После того как найдено соответствие с правилом SAT, поиск продолжается до нахождения соответствующего второго правила. Более подробная информация по этой теме приведена в Разделе 7.4, «SAT».

Несоответствующий правилам трафик

Входящие пакеты, не соответствующие ни одному правилу и не имеющие уже открытые соединения, отображаемые в таблице состояний, будут автоматически подвергаться действию *Drop*. Для контроля несоответствующего трафика рекомендуется в качестве конечного правила в наборе правил создать явное правило **DropAll** с действием *Drop*, сетью источника/назначения *all-nets* и интерфейсом источника/назначения *all***.** Данное правило позволяет регистрировать трафик, не соответствующий ни одному IP-правилу.

3.5.3. Действия IP-правил

Правило состоит из двух частей: параметров фильтрации и действий, которые следует предпринимать после фильтрации. Как описано выше, параметры любого правила NetDefendOS, а также IP-правил являются следующими:

- Интерфейс источника (Source Interface)
- Сеть источника (Source Network)
- Интерфейс назначения (Destination Interface)
- Сеть назначения (Destination Network)
- Сервис (Service)

Когда IP-правило активировано, может произойти одно из следующих действий (*Action*):

Allow Пакеты пропускаются дальше. Как правило, применяется к только что открытому соединению, в «таблицу состояний» производится запись о тома, что соединение открыто. Остальные пакеты данного соединения будут подвергаться проверке "Stateful engine" системы NetDefendOS.

FwdFast Пусть, например, пакет проходит через межсетевой экран NetDefend без установки его состояния в таблицу состояний. Это означает, что процесс *stateful inspection* не осуществляется, что менее безопасно, чем правила *Allow* или *NAT*. Время обработки пакета медленнее, чем при использовании правила *Allow*, поскольку каждый пакет проверяется всем набором правил.

NAT Подобно правилу *Allow,* но с использованием динамической трасляции адресов (более подробная информация приведена в Разделе 7.2, «NAT»).

SAT Уведомляет NetDefendOS о выполнении статического преобразования адреса. Правило SAT всегда требует получения разрешения о прохождении трафика от правил *Allow*, *NAT* или *FwdFast* (более подробная информация о преобразовании адресов приведена в *Разделе 7.4, "SAT"*).

Drop Уведомляет NetDefendOS о том, что пакет необходимо отклонить. Это более строгая версия правила **Reject**, так как при этом отправителю не посылается ответ. Очень часто это правило предпочтительнее, так как потенциальные злоумышленники не знают о том, что случилось с их пакетом.

Reject Данное действие работает примерно так же, как правило *Drop*, при этом

возвращается сообщение *TCP RST* или *ICMP Unreachable*, информирующее компьютер отправителя о том, что его пакет был отклонен. Данное правило является более “мягкой” формой IP-правила Drop.

Правило *Reject* полезно применять в приложениях, где исходящий трафик отклоняется только после наступления тайм-аута, если пришло уведомление об отказе, то трафик отклоняется, не дожидаясь тайм-аута.

Двунаправленные соединения (Bi-directional Connections)

Распространенной ошибкой при настройке IP-правил является создание двух правил, для определения прохождения трафика в одном и другом направлениях. Фактически почти все типы IP-правил поддерживают двунаправленный поток трафика при установке соединения. **Сеть источника** и **интерфейс источника** в правилах – это источник первоначальных запросов при создании соединения. Если соединение разрешено и установлено, то трафик может проходить в обоих направлениях.

Не поддерживает двунаправленный поток правило *FwdFast*. При использовании этого правила трафик не пройдет в обратном направлении. Если необходим двунаправленный поток, то требуется создать два правила *FwdFast* для каждого направления. Так же следует поступить в случае использования правила *FwdFast* совместно с правилом SAT.

Использование правила *Reject*

В некоторых случаях вместо правила *Drop* рекомендуется использовать правило *Reject,* так как требуется уведомление об отклонении пакета. Примером такой ситуации может служить ответ на запрос IDENT протокола идентификации пользователя. Некоторые приложения ждут наступления тайм-аута при использовании правила *Drop*, в случае использования правила *Reject* можно избежать таких задержек при обработке.

3.5.4. Редактирование записей набора IP-правил

После добавления различных правил в набор правил их можно отредактировать в Web-интерфейсе, щелкнув правой кнопкой мыши по этой строке.

Появится контекстное меню со следующими параметрами:

Edit

Позволяет изменить содержание правила.

Delete

Позволяет безвозвратно удалить правило из набора правил.

Disable/Enable

Позволяет отключить правило, не удаляя его из набора правил. Пока правило отключено, оно не влияет на прохождение трафика и выделяется серым цветом в пользовательском интерфейсе. Правило можно активировать в любое время.

Move options

Последний пункт контекстного меню позволяет перемещать правила на различные позиции в наборе IP-правил, следовательно, изменяя его

приоритет.

3.5.5. Папки наборов IP-правил

Для упорядочивания и сортировки большого числа записей в наборах IP-правил существует возможность создания папок IP-правил. Такая структура напоминает папки в файловой системе компьютера. При создании папке задается имя, и она может использоваться для хранения всех IP-правил, принадлежащих одной группе.

Использование папок упрощает работу администратора, делая более удобным распределение данных по адресной книге и нет необходимости указывать специальные свойства, принадлежащие записям, в разных папках. NetDefendOS доступны все записи, как будто они находятся в одном наборе IP-правил.

NetDefendOS использует концепцию папки в адресной книге, где связанные между собой объекты IP-адреса группируются вместе в созданную администратором папку.

Пример 3.16. Добавление IP-правила *Allow*

В этом примере рассматривается создание простого правила *Allow,* разрешающего открытие HTTP-соединения через *lannet-сеть* на *lan-интерфейсе* к любой сети *(all-nets)* на *wan-интерфейсе*.

CLI

Во-первых, нужно изменить текущую категорию на набор IP-правил *main*:
```
gw-world:/> cc IPRuleSet main
```

Теперь создать IP-правило:

```
gw-world:/main> add IPRule Action=Allow Service=http
SourceInterface=lan SourceNetwork=lannet
DestinationInterface=wan
DestinationNetwork=all-nets
Name=lan_http
```

Вернуться на исходный уровень:

```
gw-world:/main> cc
```

Изменения конфигурации должны быть сохранены при помощи активации следующей команды *commit*.

Web-интерфейс

1. Перейти к **Rules > IP Rules > Add > IPRule**

2. Указать подходящее имя для правила, например *LAN_HTTP*

3. Ввести:

- **Name:** Подходящее имя для правила. Например, *lan_http*
- **Action:** Allow
- **Service:** http
- **Source Interface:** lan
- **Source Network:** lannet
- **Destination Interface:** wan
- **Destination Network:** all-nets

4. Нажать кнопку **OK**

3.5.6. Метод Configuration Object Groups (Конфигурация групп объектов)

Концепция папок может использоваться для организации групп объектов системы NetDefendOS в связанную структуру. Такая структура напоминает организацию папок в файловой системе компьютера. Более подробная информация о папках, связанных с адресной книгой рассмотрена в *Разделе 3.1.6, "Папки адресной книги (Address Book Folders)"*. Папки также можно использовать при организации IP-правил.

В качестве альтернативы папкам для организации разных типов списков объектов системы NetDefendOS применяется метод *configuration object groups*. Группы объектов объединяют конфигурацию объектов, указанных в заголовке текста, с целью организации их вывода в графическом пользовательском интерфейсе. В отличие от папок, они не требуют открытия папки для отдельных объектов, для того, чтобы стать видимыми. Вместо этого все объекты уже видимы и отображаются способом, который указывает на то, как они сгруппированы.

В большинстве случаев группы могут использоваться там, где объекты системы NetDefendOS отображаются в виде таблиц, где каждая строка таблицы является экземпляром объекта. Наиболее часто группы используются для организации IP-адресов в адресной книге системы NetDefendOS и, в частности, для организации правил в наборах IP-правил, представленных в этом разделе.

Совет: Группы объектов помогают документировать конфигурации

Группы объектов рекомендуемый способ документирования содержания конфигураций системы NetDefendOS.

Такой способ может быть полезен для тех, кто видит эту конфигурацию впервые, например, сотрудники технической поддержки. В связи с определенным аспектом функционирования системы NetDefendOS в наборе, содержащем сотни IP-правил, быстрая идентификация этих правил может быть затруднена.

Группы объектов и CLI

Функция отображения метода групп объектов означает, что они не имеют отношения к интерфейсу командной строки (command line interface, CLI). Невозможно определять или другим образом изменять группы объектов через CLI, они не будут отображаться на экране при выводе в CLI. Любое редактирование группы должно выполняться через Web-интерфейс, как это описано ниже.

Простой пример

В качестве примера рассмотрен набор IP-правил *main*, который содержит только два правила, разрешающих web-серфинг во внутренней сети и третье правило *Drop-all* задерживающее любой другой трафик и регистрирующее это событие в журнале:

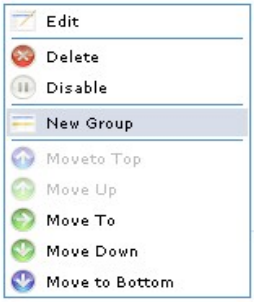
#	Name	Action
1	lan-to-internet-http	NAT
2	lan-to-internet-dns	NAT
3	drop-all	Drop

Примечание

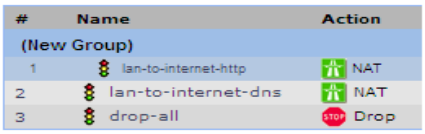
На рисунке, приведенном в этом примере, показаны только первые несколько столбцов свойств объекта.

Создадим группу объектов для двух IP-правил для Web-серфинга. Нужно выполнить следующие шаги:

- Щелчком правой кнопки мыши выбрать в новой группе первый объект.
- Из контекстного меню выбрать опцию **New Group**.



- Группа создана со строкой заголовка и IP-правилом, которое является единственным элементом группы. По умолчанию используется заголовок *"(new Group)"*.



У всей группы по умолчанию также определен цвет и отступ элементов группы. За объектами внутри группы сохраняется некоторый индекс – номер, показывающий его позицию в таблице. На индекс не влияет состав группы. Заголовок группы не содержит числовую последовательность, только текстовые символы.

Редактирование свойств группы

Изменить свойства группы можно щелкнув правой кнопкой мыши по заголовку группы и выбрав из контекстного меню опцию **Edit**.

Появится диалог редактирования *Group*, разрешающий две функции:

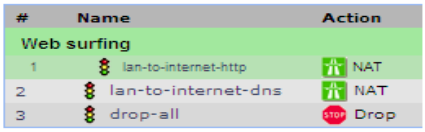
- **Specify the Title**

  В заголовке группы может быть любой требуемый текст, помимо свободных строк группа может содержать новые строки. От имени группы не требуется уникальности, так как оно используется только в качестве метки.

- **Change the Display Color**

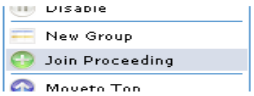
Цвет для группы может выбираться из 16 цветов, заранее заданных в палитре или вводится как шестнадцатеричное RGB-значение. Кроме того, когда введено шестнадцатеричное значение, полный спектрум цветовой палитры позволяет выбирать любой цвет щелчком мыши.

В данном примере имя группы изменяется на *Web surfing*, а цвет группы изменяется на зеленый. Результаты изменения проиллюстрированы ниже:

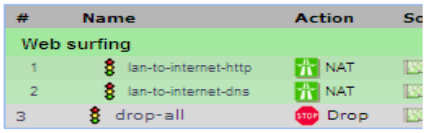


Добавление дополнительных объектов

Новая группа всегда содержит только один объект. В данном примере рассматривается добавление в группу нескольких объектов. Добавить объект в данную группу можно с помощью вызова контекстного меню (щелчком правой клавиши мыши по следующей после группы позиции) и выбрав опцию **Join Preceding**.



Результат выполнения действий, описанных выше, для второго IP-правила из примера приведен ниже:



При добавлении любого объекта в группу обязательно следует сначала выбрать следующую после группы позицию и выбрать опцию **Join Preceding**.

Добавление предшествующих объектов (Preceding Object)

Если объект предшествует группе или находиться в любой другой позиции, но не следует прямо за группой, то необходимо предпринять следующие шаги:

i. Щелчком по правой кнопке мыши вызвать контекстное меню и выбрать опцию **Move to**.

ii. Ввести номер позиции, следующей за заданной группой.

iii. После перемещения объекта на новую позицию, снова вызвать контекстное меню и выбрать опцию **Join Preceding**.

Перемещение объектов группы

Как только объект, например, IP-правило, помещается в группу, операции по перемещению происходят в группе. Например, при нажатии правой кнопкой мыши на объект группы и выборе опции **Move to Top** объект перемещается в верхнюю позицию группы, не путать с опцией по перемещению всей группы.

Перемещение групп

В некоторых случаях группы можно перемещать как индивидуальные объекты. При нажатии правой кнопкой мыши на заголовок группы открывается контекстное меню, содержащее опции по перемещению целой группы. Например, опция **Move to Top** перемещает группу в верхнюю позицию относительно других таблиц.

Отклонение группы

Если по объекту в группе щелкнуть правой кнопкой мыши, то откроется контекстное меню, включающее опцию **Leave Group**. При выборе данной опции объект из группы удаляется и перемещается в позицию, следующую после группы.

Удаление группы

При щелчке правой кнопкой мыши по заголовку группы открывается контекстное меню, включающее опцию **Ungroup**. Данная опция удаляет группу, но объекты группы сохраняются. Заголовок группы теряется, а у отдельных элементов группы отсутствуют отступы, и цвет меняется на соответствующий не сгруппированным элементам. Индивидуальный номер позиции объекта в таблице отсутствует.

Группы и папки

Важно понимать разницу между двумя методами соединения объектов: с использованием папок и с использованием групп.

Каждый из методов может использовать объекты группы, но структура папок подобна организации папок в системе компьютерных файлов. При этом папка может быть частью группы. В группы объединяют основные связанные объекты, в папке нет этого типа. С другой стороны возможно использование групп внутри папок.

Какой именно метод использовать для упорядочивания объектов в системы NetDefendOS решает администратор.

3.6. Расписания (Schedules)

В некоторых сценариях бывает полезным контролировать не только активацию функции, но и ее функциональные возможности, когда они уже используются.

Например, в IT-политике предприятия может оговариваться, что web-трафик от конкретного отдела будет проходить только в течение рабочего времени. Другим примером может служить аутентификация с использованием определенного VPN-туннеля, которая допускается только по будням до полудня.

Объекты Schedule (расписание)

Адресам системы NetDefendOS требуется предоставить объекты Schedule (часто называемые просто Schedules – расписания), которые могут выбираться и использоваться с различными типами политик безопасности для выполнения управлением на основе времени.

Несколько временных диапазонов

Объект Schedule предоставляет возможность вводить несколько временных диапазонов для каждого дня недели. Кроме того, можно указать период запуска и остановки, что будет накладывать дополнительные ограничения на расписание. Например, в расписании можно определить: понедельник 08:30 - 10:40, вторник 11:30 - 14:00, пятница 14:30 - 17:00.

Параметры расписания

Каждый объект Schedule состоит из следующих параметров:

Name	Имя расписания. Используется в отображении пользовательского интерфейса и в качестве ссылки на расписание от других объектов.
Scheduled Times	Это время, в течение каждой недели, когда применяется график. Время округляется до ближайшего часа. Расписание активно или неактивно в течение каждого часа каждый день недели.
Start Date	Если используется эта опция, то после истечения данного времени объект *Schedule* становится активным.
End Date	Если используется эта опция, то после истечения данного времени объект *Schedule* становится неактивным.
Comment	Любое описание, которое должно быть связано с объектом.

Функциональное назначение расписаний не ограничивается IP-правилами, но действуют для большинства видов политик, включая правила формирования трафика (Traffic Shaping), правила обнаружения и предотвращения вторжений (Intrusion Detection/Prevention, IDP) и правила виртуальной маршрутизации. Другими словами, объект Schedule является очень мощным компонентом, позволяющим детально регулировать активные или неактивные функции в системы NetDefendOS.

Важно: Установка системных даты и времени

Так как расписания зависят от системных даты и времени, то очень важно правильно их установить. Системные дата и время также важны для некоторых других функций, таких как сертификационное использование в VPN-туннелях.

Предпочтительно, чтобы была включена синхронизация времени для того, чтобы обеспечивать включение и отключение запланированных политик в нужное время. Более подробная информация приведена в Разделе 3.8, "Дата и Время".

Пример 3.17. Настройка политики по расписанию

В этом примере создается объект Schedule, предназначенный для рабочих часов в будние дни и связанный с IP-правилом, разрешающим прохождение HTTP-трафика.

CLI

```
gw-world:/> add ScheduleProfile OfficeHours
Mon=8-17 Tue=8-17 Wed=8-17 Thu=8-17 Fri=8-17
```

Теперь создаем IP-правило, которое использует этот трафик. Во-первых, нужно изменить текущую категорию на набор IP-правил *main*:

```
gw-world:/> cc IPRuleSet main
```

Теперь создаем IP-правило:

```
gw-world:/main> add IPRule Action=NAT Service=http
                SourceInterface=lan SourceNetwork=lannet
                DestinationInterface=any
                DestinationNetwork=all-nets
                Schedule=OfficeHours name=AllowHTTP
```

Возвращаемся на исходный уровень:

```
gw-world:/main> cc
```

Изменения конфигурации должны быть сохранены при помощи активации следующей команды *commit*.

Web-интерфейс

1. Перейти к **Objects > Schedules > Add > Schedule**
2. Ввести:
   - **Name:** OfficeHours
3. Выбрать в таблице: 08-17, с Понедельника по Пятницу
4. Нажать кнопку **OK**

1. Перейти к **Rules > IP Rules > Add > IPRule**
2. Ввести:
   - **Name:** AllowHTTP
3. Выбрать из выпадающих списков следующее:
   - **Action:** NAT
   - **Service:** http
   - **Schedule:** OfficeHours
   - **SourceInterface:** lan
   - **SourceNetwork** lannet
   - **DestinationInterface:** any
   - **DestinationNetwork:** all-nets
4. Нажать кнопку **OK**

3.7. Сертификаты

3.7.1. Обзор

X.509

Система NetDefendOS поддерживает цифровые сертификаты, соответствующие стандарту ITU-T X.509. Они включают в себя использование иерархии сертификатов X.509 с шифрованием с открытым ключом для достижения распространения ключа и организации аутентификации. В этом руководстве под словом «сертификат» понимается сертификат X.509.

Сертификат является цифровым подтверждением личности. Он ссылается на идентичность открытого ключа для того, чтобы установить подлинность владельца открытого ключа. Выполняя эту функцию, сертификат препятствуют перехвату передающихся данных вредоносной третьей стороной, предъявляющей фальшивый ключ и ID пользователя предполагаемому получателю.

Сертификаты с VPN-туннелями

В системе NetDefendOS сертификаты в основном используются вместе с VPN-туннелями. Самый простой и быстрый способ для обеспечения безопасности между конечными точками туннеля – использование Pre-shared-ключей (PSKs). По мере развития VPN-сетей использование PSKs становится все более сложным. Сертификаты предназначены для обеспечения безопасности в

крупных сетях.

Компоненты сертификата

Сертификат состоит из следующих частей:

- Публичный ключ: идентификатор пользователя, такой как имя и ID пользователя.
- Цифровые сигнатуры: сообщение, в котором говорится о том, что информация, заключенная в сертификате подтверждена центром сертификации (Certificate Authority).

Исходя из сказанного выше, сертификат – это публичный ключ с идентификацией, в сочетании со штампом утверждения участником его подлинности.

Центр сертификации

Центр сертификации (Certificate authority, CA) является достоверной организацией, которая выдает сертификаты другим субъектам. CA выдает всем сертификатам цифровую подпись. Подлинная сигнатура CA в сертификате удостоверяет личность держателя сертификата, и гарантирует, что сертификат не был изменен какой-либо третьей стороной.

CA отвечает за корректность информации в каждом сертификате. Это делается для того, чтобы убедиться в соответствии идентификатора сертификата и идентификатора владельца сертификата.

CA также может выдавать сертификаты другим CA, что приводит к древовидной иерархии сертификатов. CA самого верхнего уровня называется *корневым*. В этой иерархии каждый CA подписывается центром сертификации, находящимся непосредственно над ним, за исключением корневого CA, который обычно сам себя подписывает.

Маршрут сертификата ссылается на маршрут от одного сертификата к другому. При проверке надежности пользовательского сертификата для установления подлинности должен быть рассмотрен весь путь от пользовательского сертификата до достоверного корневого сертификата.

Сертификат CA подобен любому другому сертификату, за исключением того, что он разрешает подписывать соответствующим приватным ключом другие сертификаты. Если приватный ключ центра спецификации скомпрометирован, то все CA, включая каждый сертификат, подписанный этим CA, также считаются скомпрометированными.

Время действия (Validity Time)

Сертификат действует ограниченное время. Каждый сертификат содержит промежуток времени, в течение которого он считается действительным. После истечения данного периода сертификат не может использоваться и должен быть выдан новый сертификат.

Важно

При использовании сертификатов необходимо убедиться, что дата и время NetDefendOS установлены правильно.

Список отозванных сертификатов (Certificate Revocation List)

Certificate Revocation List (CRL) содержит список всех сертификатов, которые были отозваны до истечения срока их использования. Обычно они хранятся на внешнем сервере, который доступен для

определения действительности сертификата. Такая возможность проверки пользовательского сертификата является основной причиной, по которой безопасность сертификата упрощает администрирование больших групп пользователей.

CRL публикуются на серверах для того, чтобы все пользовательские сертификаты могли получить к ним доступ, используя либо LDAP, либо HTTP-протоколы. Отзыв сертификата может произойти по нескольким причинам. Одна из причин заключается в том, что ключи сертификата были в некотором роде скомпрометированы или возможно, что владелец сертификата потерял права, удостоверяющие использование этого сертификата по причине, например, ухода из компании. Независимо от причины CRL-сервер может быть обновлен при изменении в одном или нескольких сертификатах.

Часто сертификаты содержат поле CRL Distribution Point (CDP), которое определяет позицию, с которой будет загружаться CRL. Иногда сертификаты не содержат эту область. В таких случаях позиция CRL должна быть настроена вручную.

Цент сертификации обычно обновляет свой список CRL через определенный интервал. Длина этого интервала зависит от конфигурации CA, обычно он располагается в промежутке от часа до нескольких дней.

Надежность сертификатов (Trusting Certificates)

При использовании сертификатов система NetDefendOS доверяет любому пользователю, чей сертификат подписан данным CA. До принятия сертификата, для проверки его подлинности применяются следующие шаги:

- Построение маршрута сертификата до надежного корневого CA.
- Проверка сигнатур всех сертификатов в данном маршруте.
- Вызов CRL для каждого сертификата, подтверждающий, что ни один из сертификатов не был

отозван.

Идентификационный список

В дополнение к проверке сигнатур сертификатов система NetDefendOS также использует идентификационный список. Идентификационный список – это список всех удаленных идентификаторов, которым разрешен доступ через конкретный VPN-туннель, при условии, что успешно прошла процедура подтверждения подлинности сертификатов, описанная выше.

Повторное использование корневых сертификатов (Reusing Root Certificates)

В системе NetDefendOS корневые сертификаты следует рассматривать в качестве глобальных объектов, которые могут повторно использоваться между VPN-туннелями. Несмотря на то, что корневой сертификат связан с одним VPN-туннелем в системе NetDefendOS, он может повторно использоваться с любым количеством других различных VPN-туннелей.

3.7.2. Сертификаты в системе NetDefendOS

Сертификаты могут быть загружены в систему NetDefendOS для использования в IKE/IPsec-аутентификации, Webauth и других. Различают два типа сертификатов, которые могут быть загружены: самоподписанные (self-signed) сертификаты и удаленные (remote) сертификаты, принадлежащие удаленным узлам или CA-серверу. Самоподписанные сертификаты могут генерироваться с использованием одной из свободных доступных утилит.

Пример 3.18. Загрузка сертификата

Сертификат может быть либо самоподписанным, либо принадлежать к удаленному узлу или CA-серверу.

Web-интерфейс

1. Перейти к **Objects > Authentication Objects > Add > Certificate**
2. Указать подходящее имя для сертификата
3. Выбрать один из следующих пунктов:
    - **Upload self-signed X.509 Certificate**
    - **Upload a remote certificate**
4. Нажать кнопку **OK** и следовать инструкциям

Пример 3.19. Объединение сертификатов с IPsec-туннелями

Соединим импортируемый сертификат с IPsec-туннелем.

Web-интерфейс

1. Перейти к **Interfaces > IPsec**
2. Появятся свойства IPsec-туннеля
3. Выбрать вкладку **Authentication**
4. Выбрать опцию **X509 Certificate**
5. Выбрать корректные сертификаты **Gateway** и **Root**
6. Нажать кнопку **OK**

3.7.3. Запросы CA сертификатов (CA Certificate Requests)

Для запроса сертификатов с CA-сервера или CA-компании лучшим методом является отправка запроса CA-сертификата *CA Certificate Request,* который содержит запрос на сертификат в заранее определенном формате.

Создание запроса Windows CA-серверу (Windows CA Server) вручную

В настоящее время Web-интерфейс (WebUI) системы NetDefendOS не поддерживает создание запросов на сертификаты, которые отправляются на CA–сервер для генерации файлов с расширениями *.cer* и *.key*, необходимых NetDefendOS.

Требуемые для Windows CA-сервера файлы можно создать вручную, с помощью следующих этапов:

- Создание *gateway certificate* на Windows CA-сервере и экспортирование его как файл в формате *.pfx*.
- Конвертирование *.pfx* файла в формат *.pem*.
- Извлечение соответствующих частей из *.pem* файла для формирования требуемых файлов с расширениями *.cer* и *.key*.

Подробное описание вышеперечисленных этапов:

1. Создание *gateway certificate* на Windows CA-сервере и экспортирование его в файл формата *.pfx* на диск локальной рабочей станции, под управлением NetDefendOS.

2. Конвертирование локального *.pfx* файла в формат *.pem*, с помощью утилиты *OpenSSL,* вызываемой через командную строку:

```
> openssl pkcs12 -in gateway.pfx -out gateway.pem -nodes
```

В приведенном примере командной строки предполагается, что файл, экспортируемый с CA-сервера, называется *gateway.pfx* и его следует отнести к той же локальной директории, что и исполняемая программа OpenSSL.

Исходный файл *gateway.pfx* содержит 3 сертификата: корневой CA-сертификат, персональный сертификат и сертификат с частным ключом. Файл *gateway.pem* теперь содержит их в формате, который может быть вырезан и вставлен в текстовый редактор.

Примечание

OpenSSL в данном случае используется не как обычно в роли утилиты соединения, а в качестве утилиты преобразования.

3. Создать с помощью текстового редактора (например, Блокнот Windows) два пустых текстовых файла. Задать файлам те же имена, но использовать расширения *.cer* и *.key* соответственно. Например, могут быть имена *gateway.cer* и *gateway.key* might.

4. Запустить текстовый редактор, открыть загруженный *.pem* файл и найти строку, начинающуюся следующим образом

```
-----BEGIN RSA PRIVATE KEY -----
```

3. Выделить и скопировать в буфер обмена все, что находится под этой линией до следующей линии включительно:

```
END RSA PRIVATE KEY ---
```

6. Вставить скопированный текст в файл с расширением *.key* и сохранить его.

7. Вернуться в файл с расширением .pem найти строку, которая начинается следующим образом:

```
BEGIN CERTIFICATE ---
```

и скопировать в буфер обмена все, что находится под этой линией до следующей линии включительно:

```
END CERTIFICATE ---
```

8. Вставить скопированный текст в файл с расширением *.cer* и сохранить его.

Сохранить файлы *.key* и *.cer* и файлы готовы для загрузки в систему NetDefendOS.

3.8. Дата (Date) и время (Time)

3.8.1. Обзор

Корректная установка даты и времени важны для правильной работы системы NetDefendOS. Политики по расписанию, авто-обновления IDP и баз данных антивируса, а также других функций продукта требуется точно установленное системное время.

Кроме того, сообщения журнала отмечаются временной меткой для того, чтобы указать, когда произошло определенное событие. Кроме отсчета рабочих часов, время должно быть правильно синхронизировано с другими устройствами в сети.

Протоколы синхронизации времени

NetDefendOS поддерживает опциональное использование протоколов синхронизации времени для автоматической регулировки системных часов через ответы на запросы, отправляемые через публичную сеть Интернет, на специальный внешние серверы, которые называют сервера времени (*Time* Servers).

3.8.2. Установка даты и времени

Текущие дата и время

Администратор может установить дату и время вручную, это рекомендуется при первоначальном запуске новой системы NetDefendOS.

Пример 3.20. Настройка текущих даты и времени

Для настройки текущих даты и времени следует выполнить следующие шаги:

CLI

```
gw-world:/> time -set YYYY-mm-DD HH:MM:SS
```

Где YYYY-mm-DD HH:MM:SS - новые дата (год, месяц и день) и время. Следует обратить внимание на то, что сначала идет год, месяц, а затем день. Например, нужно установить 9:25 утра, 27 Апреля 2008 года:

```
gw-world:/> time -set 2008-04-27 09:25:00
```

Web-интерфейс

1. Перейти к **System > Date and Time**
2. Нажать **Set Date and Time**
3. С помощью выпадающего меню установить год, месяц, день и время
4. Нажать кнопку **OK**

Примечание: Повторная настройка не требуется

Новые дата и время загрузятся сразу после их установки. Реконфигурация или перезагрузка системы не требуется.

Часовые пояса (Time Zones)

Мир разделен на часовые пояса, городом со средним временем по Гринвичу (Greenwich Mean Time (GMT)) считается Лондон, где проходит нулевой меридиан, принимаемый в качестве основного часового пояса. Все остальные часовые пояса расположены к востоку и западу от нулевого меридиана и в зависимости от этого к GMT прибавляется или отнимается определенное целое число часов. Все объекты, расположенные в данном часовом поясе, будут иметь одно местное время, смещенное от GMT на целое число.

Установка часового пояса в системе NetDefendOS происходит, исходя из физического расположения межсетевого экрана NetDefend.

Пример 3.21. Установка часового пояса

Для изменения временной зоны системы NetDefend на один час предпринимаются следующие шаги:

CLI

```
gw-world:/> set DateTime Timezone=GMTplus1
```

Web-интерфейс

1. Перейти к **System > Date and Time**
2. Выбрать **(GMT+01:00)** в выпадающем списке **Timezone**
3. Нажать кнопку **OK**

Переход на летнее время (Daylight Saving Time)

Многие регионы переходят на летнее время (***Daylight*** *Saving Time,* DST), т.е. часы переводятся на летний период. Проблемой является то, что переход на летнее время в каждой стране, а иногда и в одной стране, осуществляется по разным правилам. По этой причине система NetDefendOS не может автоматически переходить на летнее время. Данная информация вводится вручную, при условии, что будет использоваться переход на летнее время.

Существует два параметра, определяющих переход на летнее время: DST-период и DST-смещение. DST-период отвечает за начало и окончание летнего времени. DST-смещение определяет на какое

количество часов смещено летнее время.

Пример 3.22. Активация DST

Для активации DST требуется выполнить действия, описанные ниже:

CLI

```
gw-world:/> set DateTime DSTEnabled=Yes
```

Web-интерфейс

1. Перейти к **System/Date and Time**

2. Включить **Enable daylight saving time**

3. **OK**

3.8.3. Серверы времени (Time Servers)

Аппаратные часы, которые используются в системе NetDefendOS, иногда могут отставать или спешить после определенного периода. Такое поведение является обычным для большинства сетевого и компьютерного оборудования, решается с помощью серверов времени.

Система NetDefendOS способна автоматически настраивать часы, в соответствии с данными, полученными от одного или нескольких серверов времени, которые предоставляют очень точное время. В NetDefendOS рекомендуется использовать серверы времени, поскольку это позволяет синхронизировать время с другими сетевыми устройствами.

Протоколы синхронизации времени (Time Synchronization Protocols)

Протоколы синхронизации времени - Time Synchronization Protocols – стандартизированный метод для получения информации с внешних серверов времени. Система NetDefendOS поддерживает следующие типы протоколов синхронизации времени:

- **SNTP**

Определяется стандартом RFC 2030, простой сетевой протокол синхронизации времени – простая реализация NTP (RFC 1305). NetDefendOS использует данный протокол для запросов к NTP-серверам.

- **UDP/TIME**

Протокол времени - Time Protocol (UDP/TIME) – более ранний метод, обеспечивающий синхронизацию времени через Интернет. Протокол обеспечивает получение машинно-читаемых даты и времени. Сервер возвращает значение времени в течение секунды.

Большинство публичных временных серверов работают с NTP или SNTP-протоколами.

Конфигурация серверов времени (Configuring Time Servers)

В конфигурацию могут быть занесены три сервера времени для отправления запросов. При использовании более чем одного сервера для синхронизации времени можно избежать ситуации недоступности одного из серверов. Система NetDefendOS анализирует информацию, полученную со всех доступных серверов, и на основе этого вычисляет среднее время. Для вывода всех доступных серверов времени можно воспользоваться функцией Интернет-поиска.

Важно: В системе NetDefendOS должны быть настроены DNS-серверы

Для работы с URL-протоколом сервера времени следует убедиться, что в системе NetDefendOS правильно настроен хотя бы один DNS-сервер. (для получения более подробной информации см. Пункт 3.9, «DNS»). Но данная функция не нужна при использовании IP-адресов.

Пример 3.23. Активация синхронизации времени с помощью SNTP

В данном примере рассматривается соединение с NTP-серверами Шведской национальной лаборатории времени и частоты (Swedish National Laboratory for Time and Frequency) с помощью SNTP-протокола. URL NTP-сервера: *ntp1.sp.se* и *ntp2.sp.se*.

CLI

```
gw-world:/> set DateTime TimeSynchronization=custom
TimeSyncServer1=dns:ntp1.sp.se
TimeSyncServer2=dns:ntp2.sp.se
TimeSyncInterval=86400
```

Web-интерфейс

1. Выбрать пункт меню **System > Date and Time**

2. Проверить включена ли функция **Enable time synchronization**

3. Ввести:
   - **Time Server Type:** SNTP
   - **Primary Time Server:** dns:ntp1.sp.se
   - **Secondary Time Server:** dns:ntp2.sp.se

4. **OK**

URL-протокол временного сервера должен иметь префикс *dns* (для определения работы DNS-сервера). Система NetDefendOS также должна определить DNS-сервер.

Примечание

*Если при использовании CLI в поле **TimeSyncInterval** не установлено значение интервала синхронизации, то по умолчанию оно будет равно 86400секунд*

Пример 3.24. Установка синхронизации времени вручную

Синхронизация времени может быть установлена через CLI. Выполнение этой операции рассмотрено ниже:

CLI

```
gw-world:/> time -sync
Attempting to synchronize system time...

Server time: 2008-02-27 12:21:52 (UTC+00:00)
Local time: 2008-02-27 12:24:30 (UTC+00:00) (diff: 158)

Local time successfully changed to server time.
```

Максимальное время установки (Maximum Time Adjustment)

Чтобы избежать ситуации, возникающей при синхронизации времени с неисправным сервером можно установить величину максимального времени установки (*Maximum Adjustment)* (в секундах). Если разница между текущим временем системы NetDefendOS и временем, полученным с сервера, будет больше заданной максимальной величины, то данные, полученные с сервера, будут отклонены. Например, значение максимального времени установки равно 60 секунд и текущее время системы NetDefendOS составляет 16:42:35. Если время, полученное с сервера: 16:43:38, то разница составляет 63 секунды, что превышает максимальную величину, т.е. время не будет обновлено.

Пример 3.25. Изменение величины максимального времени установки

Интерфейс командной строки

```
gw-world:/> set DateTime TimeSyncMaxAdjust=40000
```

Web-интерфейс

1. Выбрать пункт меню **System > Date and Time**

2. В поле **Maximum time drift that a server is allowed to adjust** ввести максимальное значение времени установки в секундах.

3. **OK**

Значение максимального времени установки можно отключить, это можно сделать при ручной синхронизации. Например, если опция синхронизации времени только что включена и различие между серверным временем и текущим больше максимального времени установки. Тогда можно вручную установить синхронизацию, игнорируя параметр максимального времени.

Пример 3.26. Принудительная синхронизация времени

В данном примере рассматривается синхронизация времени с отменой функции максимального времени установки.

CLI

```
gw-world:/> time -sync –force
```

Интервалы синхронизации

При необходимости можно изменять значение между каждой попыткой синхронизации. По умолчанию эта величина равна 86,400 секунд (1 день).

Серверы времени D-Link

При работе с системой NetDefendOS для синхронизации межсетевого времени рекомендуется использовать серверы времени D-Link, путь к которым прописан в опциях системы. Серверы D-Link связываются с NetDefendOS с помощью SNTP-протокола.

Когда опция D-Link Server включена, синхронизация осуществляется автоматически.

Пример 3.27. Включение функции D-Link NTP Server

CLI

```
gw-world:/> set DateTime TimeSynchronization=D-Link
```

Web-интерфейс

1. Выбрать пункт меню **System > Date and Time**

2. Выделить кнопку **D-Link TimeSync Server**

3.**OK**

Следует помнить, что для работы с URL сервера времени D-Link необходимо правильно настроить DNS.

3.8.4. Краткое описание настроек Даты и Времени

Ниже приведено краткое описание настроек для даты и времени:

Time Zone

Отклонение часовых поясов в минутах.

По умолчанию: 0

DST-Offset

Переход на дневное время в минутах

По умолчанию: *0*

DST Start Date

DST-начало месяца и дня, формат: MM-DD.

По умолчанию: *none*

DST End Date

DST-окончание месяца и дня, формат: MM-DD.

По умолчанию: *none*

Time Sync Server Type

Тип сервера, используемого для синхронизации времени, UDPTime или SNTP (Simple Network Time Protocol).

По умолчанию: *SNTP*

Primary Time Server

Имя DNS-хоста или IP-адреса временного сервера 1.

По умолчанию: *None*

Secondary Time Server

Имя DNS-хоста или IP-адреса временного сервера 2.

По умолчанию: *None*

teriary Time Server

Имя DNS-хоста или IP-адрес временного сервера3.

По умолчанию: *None*

Interval between synchronization

Промежуток времени между каждой повторной синхронизацией.

По умолчанию: *86400*

Max time drift

Максимальное время смещения (в секундах), разрешенное для корректировки.

По умолчанию: 600

Group interval

Интервал, согласно которому группируются ответы сервера.

По умолчанию: *10*

3.9. DNS

Обзор

При использовании DNS-сервера можно задать доменное имя - *Fully Qualified Domain Name* (FQDN) – вместо соответствующего IP-адреса. FQDN – уникальные текстовые доменные имена, которые определяют позицию узла в иерархии DNS-деревьев. При использовании одного и того же FQDN IP-адрес может меняться.

Унифицированный указатель ресурсов - *Uniform Resource Locator* (URL) отличается от FQDN тем, что содержит протокол доступа наряду с FQDN. Например, для доступа к web-страницам можно определить протокол: *http//:*.

FQDN используется в системе NetDefendOS при неизвестных IP-адресах или для использования DNS-имен вместо статических IP-адресов.

DNS в системе NetDefendOS

Для выполнения DNS в системе NetDefendOS предусмотрена встроенная опция DNS-клиент, которую можно настраивать на использование трех DNS-серверов: *Primary Server (первый сервер)*, *Secondary Server (второй сервер)* и *Tertiary Server (третий сервер)*. Для функционирования DNS необходимо настроить хотя бы primary server. Рекомендуется настраивать первый и второй серверы для непрерывной работы при отказе первичного сервера.

Методы, необходимые для работы DNS

Настройка хотя бы одного DNS-сервера необходима для функционирования следующих модулей системы NetDefendOS:

- Автоматическая синхронизация времени (Automatic time synchronization).
- Доступ к authority server для получения CA сертификатов.
- UTM-характеристики для доступа к внешним сервисам, таким как anti-virus и IDP.

Пример 3.28. Настройки DNS-серверов

В этом примере рассматриваются настройки DNS-клиента для использования primary и secondary DNS-серверов при помощи IP-адресов 10.0.0.1 и 10.0.0.2 соответственно.

CLI

```
gw-world:/> set DNS DNSServer1=10.0.0.1 DNSServer2=10.0.0.2
```

Web-интерфейс

1. Выбрать пункт меню **System > DNS**

2. Ввести:

   - **Primary Server:** 10.0.0.1
   - **Secondary Server:** 10.0.0.2

3. **OK**

Динамический DNS (Dynamic DNS)

DNS-характеристики системы NetDefendOS позволяют информировать DNS-серверы при изменении IP-адреса межсетевого экрана NetDefend. Данные характеристики ссылаются на *Dynamic DNS* и используются при изменении внешних IP-адресов межсетевых экранов NetDefend.

Dynamic DNS может применяться в VPN-сценариях, где обе конечные точки используют динамические IP-адреса. Если динамический адрес использует только одна конечная точка туннеля, то метод системы NetDefendOS VPN *keep alive* позволяет решить эту проблему.

В пункте меню **System > Misc. Clients** WebUI определено несколько динамических DNS-сервисов. *HTTP* Poster-клиент – сгенерированный динамический DNS-клиент, который позволяет определить 3 различных URL и значение поля *Delay in seconds until all URLs are refetched* (по умолчанию 604800 секунд или 7 дней).

По окончании каждого временного интервала *HTTP Poster* будет отправлять HTTP *GET*- запрос для определения URL.

Запросы не посылаются автоматически при изменении настроек системы NetDefendOS, но есть одно исключение – изменение настроек из-за получения нового локального IP-адреса интерфейса, который соединяется с DNS-сервером.

Различие между *HTTP Poster* и определенных DNS-серверов в WebUI заключается в использовании любых URL. Сервисы, с определенными именами облегчают возможность формирования правильного URL, необходимого для этого сервиса. Например, URL-адрес http:// для *dyndns.org* может быть определен следующим образом:

```
myuid:mypwd@members.dyndns.org/nic/update?hostname=mydns.dyndns.org
```

Приведенный выше пример можно представить с использованием *HTTP Poster* или URL может быть автоматически отформатирован системой NetDefendOS с использованием опций *DynDNS* и ввода информации, требуемой для *dyndns.org*.

Для поиска неисправностей в соединении NetDefendOS и серверов можно использовать команду CLI *httpposter*.

Примечание: Высокий уровень запросов сервера может вызвать проблемы

Динамические DNS-сервисы отрицательно реагируют на повторяющиеся через короткие промежутки времени попытки ввода и могут заблокировать IP-адреса, с которых запросы посылаются очень часто.

HTTP Poster можно использовать и для других целей. Характеристики системы NetDefendOS позволяют генерировать любые HTTP *GET*-запросы.

Глава 4. Маршрутизация

Эта глава посвящена настройкам IP-маршрутизации в системе NetDefendOS.

- Обзор
- Статическая маршрутизация
- Маршрутизация на основе правил (PBR)
- Балансировка нагрузки маршрута
- OSPF
- Многоадресная маршрутизация
- Прозрачный режим

4.1. Обзор

IP-маршрутизация – одна из основных функций системы NetDefendOS. При прохождении через межсетевой экран NetDefend любой IP-пакет проверяется, по крайней мере, один раз, и в зависимости от результатов данной проверки система решает, как реагировать на этот пакет.

Системой NetDefendOS поддерживаются следующие типы механизмов маршрутизации:

- Статическая маршрутизация
- Динамическая маршрутизация

Системой NetDefendOS поддерживается дополнительная функция *route monitoring* (мониторинг маршрутов), предназначенная для контроля актуальности и обеспечения возможности резервирования выбранных маршрутов.

4.2. Статическая маршрутизация (Static Routing)

Статическая маршрутизация – основная и наиболее распространенная форма маршрутизации. Термин «статическая» означает, что записи в таблицу маршрутизации добавляются вручную и поэтому постоянны (статичны).

Из-за такого ручного подхода статическая маршрутизация чаще всего применяется в малых сетях, где установлены фиксированные IP-адреса и небольшое количество связанных подсетей. Для больших сетей, где применятся сложная топология построения, запись в таблицы маршрутизации вручную затруднительна и отнимает много времени. В таких случаях используется динамическая маршрутизация.

Более подробная информация о динамической маршрутизации системы NetDefendOS приведена в *Разделе 4.5, «OSPF»*. Следует обратить внимание на то, что при настройке динамической маршрутизации необходимо знать основы статической маршрутизации.

4.2.1. Принципы маршрутизации

Механизм IP-маршрутизации применяется в TCP/IP-сетях для передачи IP-пакетов от их источника к получателю через промежуточные сетевые устройства – маршрутизаторы, которые выполняют задачу маршрутизации пакетов.

Таблицы маршрутизации (одна или более) каждого маршрутизатора содержат список маршрутов, в соответствии с которыми пакеты передаются получателям.

Составляющие маршрута

Параметры, определяющие маршрут:

- **Интерфейс (Interface)**

  Интерфейс, отправляющий пакет в сеть назначения. Другими словами, интерфейс, с которым связан диапазон IP-адресов сети назначения (непосредственно или через маршрутизатор).

  Интерфейс может быть физическим интерфейсом межсетевого экрана или VPN-туннелем (система NetDefendOS обрабатывает VPN-туннели аналогично физическим интерфейсам).

- **Сеть (Network)**

  Сеть назначения – диапазон IP-адресов получателей. Выбранный маршрут – маршрут из таблицы маршрутизации с одним из IP-адресов, находящихся в заданном диапазоне. Если таких маршрутов несколько, то выбирается тот маршрут, диапазон IP-адресов которого наименьший.

  Сеть назначения *all-nets* (все сети) обычно используют как маршрут по умолчанию в сетях публичного доступа в Интернет через ISP.

- **Шлюз (Gateway)**

  IP-адрес следующего маршрутизатора на пути назначения – это IP-адрес шлюза. Шлюз – необязательная часть маршрута, может не использоваться в случае, если интерфейс межсетевого экрана NetDefend непосредственно подключен к сети назначения.

  Если, к примеру, рассматривать маршрут, прописанный для сетей публичного доступа в Интернет через ISP с использованием публичных IP-адресов, то шлюз должен быть определен.

- **Локальный IP-адрес (Local IP address)**

  Этот параметр обычно не определяют. Если этот параметр определен, то система NetDefendOS отвечает на ARP-запросы этого адреса.

  Локальный IP-адрес и шлюз взаимно исключают друг друга, одновременно определить можно только один из них.

- **Метрика (Metric)**

  Метрика назначается маршрутизатору и применяется для сравнения весов маршрутов. Если два маршрута эквивалентны, но имеют различные метрические значения, то выбирается маршрут с минимальным значением.

  Метрика также используется при резервировании маршрутов (*Route Failover)* и при балансировке нагрузки маршрута *(Route Load Balancing*).

  Более подробная информация приведена в *Разделе 4.4.* «*Балансировка нагрузки маршрута»*.

Сценарий типичной маршрутизации

На рисунке проиллюстрирован сценарий работы межсетевого экрана NetDefend.

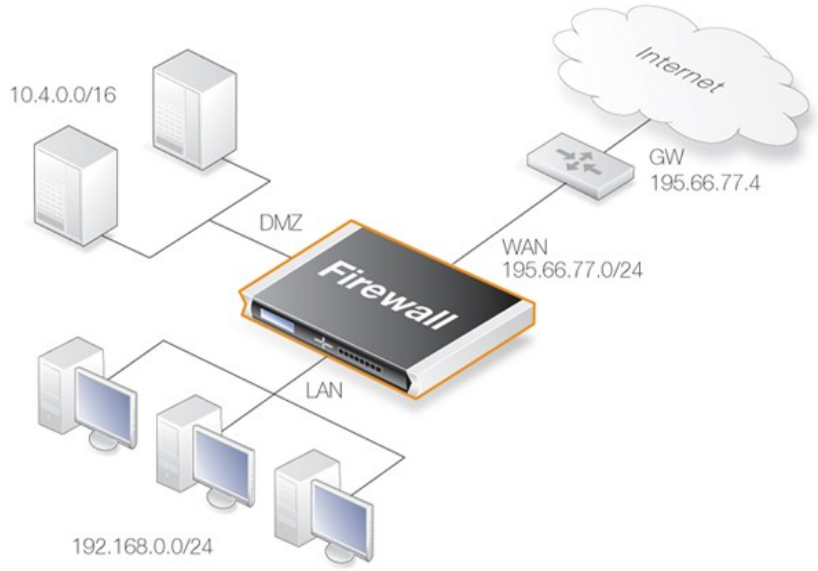


Рисунок 4.1 Сценарий типичной маршрутизации

На рисунке изображены: LAN-интерфейс, связанный с сетью *192.168.0.0/24*, DMZ-интерфейс, связанный с сетью *10.4.0.0/16*, WAN-интерфейс *195.66.77.0/24* и ISP-шлюз *195.66.77.4* с публичным доступом в Интернет.

Таблица маршрутизации для рассмотренного примера приведена ниже.

№ маршрута (Route #)	**Интерфейс (Interface)**	**Сеть назначения (Destination)**	**Шлюз (Gateway)**
1	lan	192.168.0.0/24	
2	dmz	10.4.0.0/16	
3	wan	195.66.77.0/24	
4	wan	all-nets	195.66.77.4

В таблице хранится следующая информация:

- **Маршрут №1 (Route #1)**

  Все пакеты, направляемые к хостам сети *192.168.0.0/24*, отправляются на LAN-интерфейс. Поскольку для этого маршрута не определен никакой шлюз, хост, расположенный в сегменте данной сети, принимает информацию непосредственно с LAN-интерфейса.

- **Маршрут №2 (Route #2)**

  Все пакеты, направляемые к хостам сети *10.4.0.0/16*, отправляются на DMZ-интерфейс. Для этого маршрута шлюз также не определен.

- **Маршрут №3 (Route #3)**

  Все пакеты, направляемые к хостам сети *195.66.77.0/24*, отправляются на WAN-интерфейс. Шлюз для доступа к хостам не требуется.

- **Маршрут №4 (Route #4)**

  Любые пакеты, направляемые к хосту (сеть *all-nets* соответствует всем хостам), отправляются на WAN-интерфейс и шлюз с IP-адресом *195.66.77.4*. Шлюз будет обращаться к таблице маршрутизации для выяснения дальнейшего маршрута пакета.

  Маршрут с назначением *all-nets* называется *Default Route* (маршрут по умолчанию),

так как все пакеты, маршрут которых не определен, соответствуют данному маршруту. Такой маршрут обычно определяет интерфейс, связанный с Интернетом.

Важной особенностью при оценке таблицы маршрутизации является распределение маршрутов. Чаще всего в начале списка маршрутов таблиц маршрутизации указываются конкретные маршруты. Другими словами, если найдены два эквивалентных маршрута, то больший приоритет будет иметь наиболее точно определенный маршрут.

В рассмотренном выше примере пакет с адресом *192.168.0.4* теоретически будет соответствовать как первому, так и последнему маршруту, при этом первый маршрут определен конкретнее и пакет будет отправлен согласно данному маршруту.

Параметры локального IP-адреса (Local IP Address Parameter)

Очень важна корректная настройка параметров локального IP-адреса.

Как правило, физический LAN-интерфейс связан с единственной сетью, и интерфейс и сеть находятся в одной подсети. Можно сказать, что сеть связана с физическим интерфейсом и клиенты данной сети могут автоматически связываться с межсетевым экраном NetDefend посредством ARP-запросов. Поскольку клиенты и интерфейс системы NetDefendOS относятся к одной сети, ARP функционирует нормально.

Вторую сеть можно добавить к этому интерфейсу через коммутатор, но у нового диапазона сети будет отсутствовать соответствующий IP-адрес физического интерфейса, т.е. эта сеть не связана с физическим интерфейсом. Клиенты второй сети не смогут связаться с межсетевым экраном NetDefend, так как межсетевой экран не будет отвечать на ARP-запросы из другой подсети.

Для решения этой проблемы в систему NetDefendOS следует добавить новый маршрут со следующими параметрами:

- **Интерфейс:** интерфейс, к которому подключена вторая сеть.
- **Сеть:** диапазон IP-адресов второй сети.
- **Локальный IP-адрес:** адрес в пределах диапазона IP-адресов второй сети.

В клиентских настройках в качестве шлюза по умолчанию *(Default Gateway)* должен быть установлен выбранный **Локальный IP-адрес**, после чего клиенты смогут связаться с интерфейсом межсетевого экрана.

При добавлении маршрута с локальным IP-адресом система NetDefendOS будет функционировать как шлюз с этим IP-адресом, отправлять ARP-запросы и отвечать на них.

Данная особенность продемонстрирована на рисунке, приведенном ниже. Сеть *10.1.1.0/24* связана с физическим интерфейсом с адресом *10.1.1.1*. При подключении второй сети *10.2.2.0/24* к интерфейсу через коммутатор IP-адрес интерфейса не будет принадлежать данной сети.

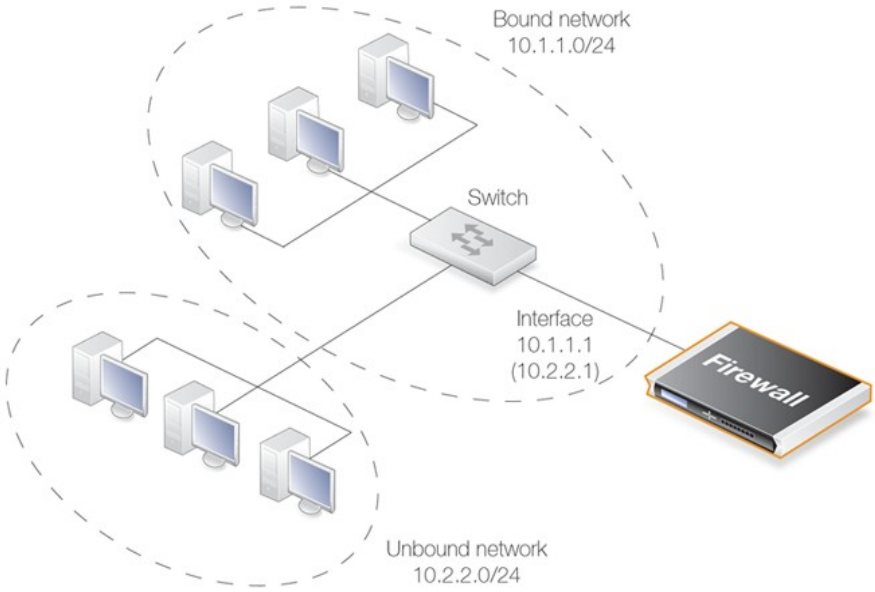


Рисунок 4.2. Применение локального IP-адреса и несвязанной сети

Интерфейс будет отвечать на ARP-запросы от сети *10.2.2.0/24* при добавлении в систему NetDefendOS маршрута для второй сети с локальным IP-адресом *10.2.2.1*. Для соединения с межсетевым экраном NetDefend клиенты второй сети должны указать адрес шлюза по умолчанию – *10.2.2.1*.

Данный метод используется в тех случаях, когда к интерфейсу необходимо добавить дополнительную сеть. С точки зрения безопасности данный метод может предоставлять угрозу, так как различные сети будут соединены друг с другом через коммутатор, который не управляет трафиком, проходящим между сетями.

При маршрутизации используется два связанных маршрута

Любой трафик в системе NetDefendOS должен проходить по двум связанным маршрутам. Кроме того, маршрут должен быть определен как для сети назначения, так и для сети источника.

Если маршрут определил сеть источника, то говорят, что сеть источника найдена на определенном интерфейсе. При открытии нового соединения система NetDefendOS выполняет проверку, известную как «обратный поиск маршрута» *(reverse route lookup*). Маршрут сети источника не используется для обработки маршрутизации, но исходная сеть должна быть найдена на интерфейсе источника. Если в результате проверки исходная сеть не найдена, то система NetDefendOS выводит сообщение об ошибке *Default Access Rule*.

В том числе трафик, предназначенный для интерфейса *Core* (непосредственно для системы NetDefendOS), такой как ICMP ping-запросы, проходит проверку правилом на наличие двух маршрутов. В этом случае интерфейс одного из маршрутов определяется как *Core*.

4.2.2. Статическая маршрутизация

В данном разделе рассматривается механизм осуществления маршрутизации в системе NetDefendOS и настройки статической маршрутизации.

Система NetDefendOS позволяет работать с несколькими таблицами маршрутизации. По умолчанию определена таблица маршрутизации **main.** Кроме этого, администратор может создать дополнительные таблицы маршрутизации для описания альтернативных маршрутов.

Такие определенные пользователем таблицы носят название Policy Based Routing – маршрутизации

на основе правил (PBR), то есть администратор может создавать IP-правила, в соответствии с которыми будет проходить трафик. (Более подробная информация о PBR приведена в *Разделе 4.3, «Маршрутизация на основе правил (PBR)»*).

Механизм поиска маршрута (Route Lookup)

Одна из причин высокой скорости отправления пакетов в системе NetDefendOS – механизм поиска маршрута, который несколько отличается от механизмов поиска в маршрутизаторах других производителей. В других моделях IP-пакеты отправляются без анализа их содержания, таблицы маршрутизации просматриваются для каждого пакета, полученного маршрутизатором. В системе NetDefendOS процесс поиска маршрутов объединен с механизмом Stateful inspection, который анализирует состояние пакета.

При поступлении IP-пакета на любой интерфейс начинают анализироваться таблицы маршрутизации, и выясняется наличие уже установленного соединения для определенного пакета. При наличии такого соединения в таблице маршрутизации появляется запись о данном маршруте и механизм поиска для данного пакета уже не требуется. Такой метод более эффективен, чем обычный механизм поиска маршрута.

Если установленное соединение не найдено, то таблицы маршрутизации снова анализируются. Важной особенностью является то, что поиск маршрутов осуществляется прежде применения к пакету правил (например, IP-правил), то есть к моменту применения правил системе NetDefendOS уже известен интерфейс назначения, и она решает пропустить соединение или прервать его. Такой метод позволяет политикам безопасности осуществлять более детальный контроль.

Описание маршрутов в системе NetDefendOS

В отличие от других систем в NetDefendOS достаточно легко описывать маршруты.

В других моделях вместо интерфейса таблицы маршрутизации определяется его IP-адрес. Пример таблицы маршрутизации рабочей станции с системой Microsoft Windows XP приведен ниже:

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 13 d4 51 8d dd ...... Intel(R) PRO/1000 CT Network
0x20004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
```

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface Metric
          0.0.0.0          0.0.0.0  192.168.0.1 192.168.0.10     20
         10.0.0.0        255.0.0.0   10.4.2.143   10.4.2.143      1
       10.4.2.143  255.255.255.255    127.0.0.1    127.0.0.1     50
   10.255.255.255  255.255.255.255   10.4.2.143   10.4.2.143     50
     85.11.194.33  255.255.255.255  192.168.0.1 192.168.0.10     20
        127.0.0.0        255.0.0.0    127.0.0.1    127.0.0.1      1
      192.168.0.0    255.255.255.0 192.168.0.10 192.168.0.10     20
     192.168.0.10  255.255.255.255    127.0.0.1    127.0.0.1     20
    192.168.0.255  255.255.255.255 192.168.0.10 192.168.0.10     20
        224.0.0.0        240.0.0.0   10.4.2.143   10.4.2.143     50
        224.0.0.0        240.0.0.0 192.168.0.10 192.168.0.10     20
  255.255.255.255  255.255.255.255   10.4.2.143   10.4.2.143      1
  255.255.255.255  255.255.255.255 192.168.0.10 192.168.0.10      1
Default Gateway:       192.168.0.1
===========================================================================
Persistent Routes:
None
```

Та же таблица маршрутизации в системе NetDefendOS:

```
Flags Network            Iface    Gateway         Local IP  Metric
----- ------------------ -------- --------------- --------- ------
      192.168.0.0/24     lan                                 20
      10.0.0.0/8         wan                                 1
      0.0.0.0/0          wan      192.168.0.1                20
```

Преимущества определения маршрутов в системе NetDefendOS

Метод определения маршрутов в системе NetDefendOS более легок для чтения и доступен для понимания маршрутов.

Еще одно преимущество заключается в том, что администратор может непосредственно определить шлюз для конкретного маршрута, учитывая следующее:

- Часть маршрутов уже определена, включая маршрут по умолчанию с IP-адресом шлюза.
- Вне зависимости от того существует ли отдельный маршрут с IP-адресом шлюза, трафик перенаправляется между интерфейсами.

Определение сложных подсетей

Преимущество такого определения маршрутов в системе NetDefendOS заключается в том, что администратор может выявить маршруты, маски которых не совпадают с общепринятыми масками подсети.

Например, точно определены следующие диапазоны IP-адресов для маршрутов: *192.168.0.5 – 192.168.0.17* и *192.168.0.18 – 192.168.0.254*, что позволяет применять маршрутизацию системы NetDefendOS в сетях со сложной топологией.

Отображение таблиц маршрутизации

Следует отметить, что в процессе работы маршруты в таблицах маршрутизации, настроенных администратором, могут добавляться, удаляться и изменяться, что отображается в таблицах маршрутизации.

Изменение записей в таблице маршрутизации может происходить по некоторым причинам. Например, если была запущена динамическая маршрутизация с OSPF, то записи в таблицы маршрутизации будут обновляться новыми маршрутами, полученными от других маршрутизаторов OSPF-сети. На содержание таблиц маршрутизации могут повлиять и недоступные маршруты.

Пример 4.1. Отображение таблицы маршрутизации *main*

В данном примере рассказывается, как отобразить содержимое таблицы маршрутизации *main*.

Интерфейс командной строки (Command-Line)

Выбор конфигурируемой таблицы маршрутизации:

```
gw-world:/> cc RoutingTable main

gw-world:/main> show

Route
# Interface Network Gateway Local IP
- --------- -------- ------------- --------
1 wan all-nets 213.124.165.1 (none)
2 lan lannet (none) (none)
3 wan wannet (none) (none)
```

Для вывода на экран списка активных таблиц маршрутизации необходимо ввести:

```
gw-world:/> routes

Flags Network Iface Gateway Local IP Metric

----- ------------------ ------- --------------- -------- ------
192.168.0.0/24 lan 0
213.124.165.0/24 wan 0
0.0.0.0/0 wan 213.124.165.1 0
```

Web-интерфейс

Выбор конфигурируемой таблицы маршрутизации:

1. Перейти на вкладку **Routing** > **Routing Tables**

2. Выбрать таблицу маршрутизации *main*

В главном окне появится список сформированных маршрутов

Для вывода списка активных таблиц маршрутизации необходимо выбрать **Routes** из выпадающего меню **Status**, после чего в главном окне появится список активных таблиц маршрутизации.

Совет: При использовании CLI-интерфейса может потребоваться команда cc

При использовании CLI, в приведенном выше примере, до начала управления конкретными маршрутами необходимо было выбрать название определенных таблиц маршрутизации с помощью команды cc (change category или change context). Эта команда применяется в случае использования нескольких групп объектов.

Статические маршруты, заданные по умолчанию (Default Static Routes) автоматически добавляются для каждого интерфейса

При первом запуске межсетевого экрана система NetDefendOS автоматически добавит маршрут в главную таблицу маршрутизации *main* для каждого физического интерфейса. Такие маршруты по умолчанию определяют IP-адрес объекта в адресной книге, для прохождения соответствующего трафика этим объектам необходимо изменить IP-адреса.

Примечание: По умолчанию метрика маршрутов равна 100

Метрика маршрутов для физических интерфейсов, созданных автоматически, всегда равна 100.

Автоматически созданные маршруты **нельзя удалять вручную** из таблицы маршрутизации. Вместо этого в свойствах интерфейса следует отключить опцию **Automatically add a route for this interface using the given network** (автоматическое добавление маршрута для этого интерфейса, использующего данную сеть). После отключения этой опции маршрут, созданный автоматически, будет удален.

Маршрут *all-nets* (все сети)

Маршрут *all-nets* — наиболее важный маршрут, который обычно предназначается для публичного доступа в Интернет через ISP. При использовании установщика системы NetDefendOS *setup wizard* этот маршрут добавляется автоматически.

Эта опция также определяется для любого физического интерфейса, который используется для соединения с Интернетом. В Web-интерфейсе *all-nets* добавляется в расширенных настройках Ethernet-интерфейса с помощью опции **Automatically add a default route for this interface using the**

given default gateway (автоматическое добавление заданного по умолчанию маршрута для этого интерфейса, использующего данный шлюз по умолчанию).

При включении этой опции маршрут *all-nets* автоматически добавляется в таблицу маршрутизации *main* данного интерфейса.

Маршруты *Core* (*Core* Routes)

Система NetDefendOS автоматически добавляет в таблицу маршрутизации маршруты *Core.*Эти маршруты предназначены непосредственно для системы и служат для определения движения трафика. Существует маршрут, который обязательно добавляется в каждый интерфейс системы. Другими словами, для LAN и WAN-интерфейсов с адресами *192.168.0.10* и *193.55.66.77* соответственно назначаются следующие маршруты:

№ маршрута (Route #)	Интерфейс (Interface)	Сеть назначения (Destination)	Шлюз (Gateway)
1	core	192.168.0.10	
2	core	193.55.66.77	

При получении системой IP-пакета, чей адрес назначения – один из IP-интерфейсов, он направляется на интерфейс core, то есть обрабатывается непосредственно системой NetDefendOS.

Помимо этого создается маршрут для всех адресов многоадресной рассылки:

№ маршрута (Route #)	Интерфейс (Interface)	Сеть назначения (Destination)	Шлюз (Gateway)
1	core	224.0.0.0/4	

Для того чтобы маршруты Core отображались в таблице маршрутизации, следует включить соответствующую опцию.

Пример 4.2. Отображение маршрутов *Core*

В данном примере рассказывается, как отобразить маршруты Core в активной таблице маршрутизации.

CLI

```
gw-world:/> routes –all

Flags Network Iface Gateway Local IP Metric
----- ----------------- ---------- ------------- -------- ------
127.0.0.1 core (Shared IP) 0
192.168.0.1 core (Iface IP) 0
213.124.165.181 core (Iface IP) 0
127.0.3.1 core (Iface IP) 0
127.0.4.1 core (Iface IP) 0
192.168.0.0/24 lan 0
213.124.165.0/24 wan 0
224.0.0.0/4 core (Iface IP) 0
0.0.0.0/0 wan 213.124.165.1 0
```

Web-интерфейс

1. Выбрать **Routes** из выпадающего меню **Status**

2. Установить флажок в поле **Show all routes** и нажать кнопку **Apply**

3. В главном окне появится список активных таблиц маршрутизации, включающих маршруты core.

Совет: Команды для маршрутов

Более подробная информация о CLI-командах для маршрутов

приведена в Руководстве по командной строке (CLI Reference Guide).

4.2.3. Резервирование маршрутов (Route Failover)

Обзор

Часто межсетевые экраны NetDefend устанавливаются в сетях, где необходима их постоянная готовность к работе. Например, на предприятии, сфера деятельности которого сильно зависит от Интернета, доступ к которому предоставляет только один провайдер.

Поэтому довольно часто используют так называемый резервный доступ к Интернету через второго провайдера. Интернет-провайдеры используют различные маршруты, чтобы избежать отказа соединения.

Для таких ситуаций в системе NetDefendOS предусмотрена возможность переключения маршрутов при отказе (*Route Failover)*: в случае отказа одного из маршрутов трафик автоматически начинает передаваться по другому запасному маршруту. Система NetDefendOS выявляет неудачные маршруты, используя при этом функцию мониторинга маршрутов *Route Monitoring,* и перенаправляет трафик на запасной маршрут.

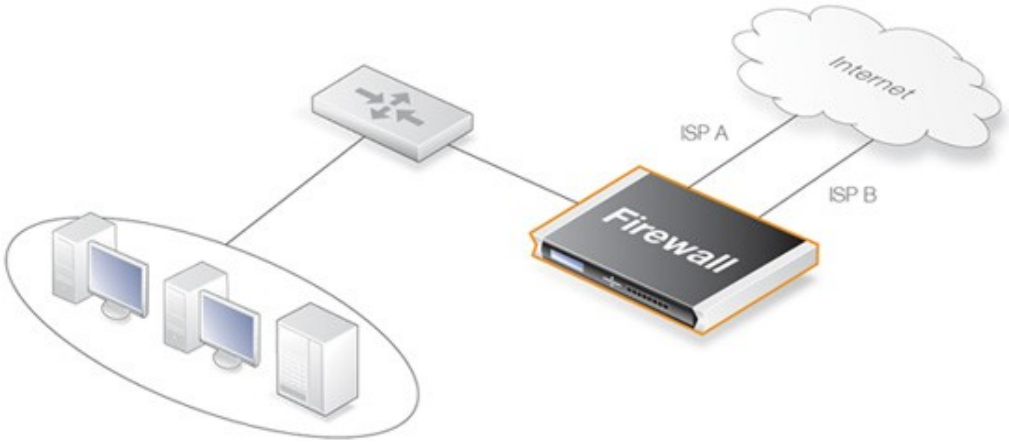


Рисунок 4.3. Сценарий применения свойства Route Failover для доступа через ISP

Настройки Route Failover

При установке Route Failover необходимо активизировать функцию *Route Monitoring.* В сценарии с основным и резервным маршрутами в основной маршрут добавляется *Route Monitoring*, в резервном маршруте это не указывается (если не требуется переключения при отказе). Когда функция *Route Monitoring* для маршрута включена, нужно выбрать один из следующих методов контроля:

Interface Link Status	Система NetDefendOS контролирует состояние подключения интерфейса, определенного для маршрута. Маршрут считается активным, пока существует физическое подключение интерфейса. Этот метод обеспечивает самый быстрый анализ маршрута, так как сразу обнаруживаются любые изменения состояния соединений.
Gateway Monitoring	При мониторинге шлюза как следующего сегмента маршрута, его доступность определяется при помощи ARP-запросов. До тех пор, пока шлюз отвечает на эти запросы, маршрут функционирует нормально.

Мониторинг автоматически добавляемых маршрутов

Следует заметить, что функцию *Route Monitoring* нельзя применять для автоматически созданных маршрутов, так как им присвоен специальный статус, и обращение к ним происходит по-другому. К таким маршрутам относятся маршруты для физических интерфейсов, автоматически созданные при запуске системы NetDefendOS.

Если требуется включить *Route Monitoring* для таких маршрутов, то их необходимо сначала удалить, а затем добавить вручную как новые маршруты.

Установка метрики маршрута (Route Metric)

При определении маршрута администратору необходимо установить метрику (*metric*) маршрута. Метрика – это целое положительное число, которое указывает на приоритет маршрута. При наличии двух маршрутов для одного и того же интерфейса назначения система NetDefendOS выберет маршрут с минимальным значением метрики (если два маршрута полностью эквивалентны, то из таблицы маршрутизации выбирается маршрут, расположенный выше другого).

Метрика основного маршрута всегда должна быть ниже, чем метрика резервного маршрута.

Несколько резервных маршрутов

При необходимости можно определить несколько резервных маршрутов. Например, для одного основного маршрута можно определить два резервных маршрута, при этом метрики каждого из этих маршрутов должны отличаться друг от друга. Например: “10” – для основного маршрута, “20” – для первого резервного и “30” – для второго резервного маршрутов. В таблице маршрутизации следует настраивать мониторинг только первых двух маршрутов.

Процесс переключения маршрутов (Failover Processing)

При определении отказавшего маршрута система NetDefendOS отмечает его как недоступный и переключает трафик на резервный маршрут. Для уже установленного соединения выполняется поиск маршрута и находится следующий необходимый маршрут, который используется в дальнейшем. Для нового соединения при поиске маршрутов игнорируются недоступные и ищутся следующие необходимые маршруты.

В таблице маршрутизации, приведенной ниже, определяются два маршрута, заданных по умолчанию, с одинаковыми интерфейсами назначения *all-nets*, но с различными шлюзами. Основному маршруту присвоено минимальное значение метрики и включена функция мониторинга маршрута *Route Monitoring*. Для второго маршрута включение данной функции необязательно.

№ маршрута (Route #)	**Интерфейс (Interface)**	**Сеть назначения (Destination)**	**Шлюз (Gateway)**	**Метрическая величина (Metric)**	**Мониторинг (Monitoring)**
1	wan	all-nets	195.66.77.1	10	On
2	wan	all-nets	193.54.68.1	20	Off

При установлении нового соединения хоста с Интернетом поиск завершается при нахождении маршрута с минимальной метрикой. В случае отказа основного WAN-маршрута система NetDefendOS фиксирует его как недоступный. После этого выполняется новый поиск маршрута и выбирается второй резервный маршрут.

Восстановление работоспособности маршрутов

Система NetDefendOS продолжает проверять состояние маршрута, даже если он недоступен. Если маршрут снова доступен, существующее соединение автоматически переходит на этот маршрут.

Объединение интерфейсов маршрута в группу

С помощью функции мониторинга маршрутов следует проверить, не приведет ли к отказу других маршрутов изменение интерфейса маршрутизации и предпринять, при необходимости, действия, которые будут гарантировать, что политики и открытые соединения будут корректно работать.

Пример одной из конфигураций:

Существует IP-правило, задающее действие NAT для всего HTTP-трафика, проходящего в Интернет через WAN-интерфейс:

Действие (Action)	Интерфейс источника (Src Iface)	Сеть источника (Src Net)	Интерфейс назначения (Dest Iface)	Сеть назначения (Dest Net)	Параметры (Parameters)
NAT	lan	lannet	wan	all-nets	http

Следовательно, в таблице маршрутизации содержится следующий заданный по умолчанию маршрут:

Интерфейс (Interface)	Сеть назначения (Destination)	Шлюз (Gateway)	Метрическая величина (Metric)	Мониторинг (Monitoring)
wan	all-nets	195.66.77.1	10	Off

Резервный маршрут создается для DSL-соединения и для него также включена функция *Route Monitoring*. Соответствующая запись в таблице маршрутизации примет вид:

№ маршрута (Route #)	Интерфейс (Interface)	Сеть назначения (Destination)	Шлюз (Gateway)	Метрическая величина (Metric)	Мониторинг (Monitoring)
1	wan	all-nets	195.66.77.1	10	On
2	Dsl	all-nets	193.54.68.1	20	Off

Следует отметить, что функция *Route Monitoring* включена только для первого маршрута.

Система будет работать по этому сценарию до тех пор, пока основной WAN-маршрут доступен. В случае отказа первого WAN-маршрута будет использоваться второй, резервный маршрут.

Однако, если происходит отказ маршрута, то для маршрута заданного по умолчанию следует использовать DSL-интерфейс. При установлении HTTP-соединения из локальной сети, поиск маршрутов будет заканчиваться DSL-интерфейсом назначения. Соединение будет отклонено, поскольку в IP-правиле, задающем действие NAT, указан WAN-интерфейс назначения.

Кроме того, любые открытые Интернет-соединения, соответствующие правилу NAT также будут отклонены в результате изменения интерфейса.

Для решения такой проблемы все возможные интерфейсы назначения должны быть сгруппированы в группу интерфейсов, для которой необходимо включить флаг **Security/Transport Equivalent.** После политики безопасности будут рассматривать данную группу как отдельный интерфейс назначения. Более подробная информация о группах приведена в *Разделе 3.3.6, «Interface Groups».*

Генерирование Gratuitous ARP-запросов

По умолчанию система NetDefendOS генерирует Gratuitous ARP-запросы для осуществления контроля над состоянием маршрута. Данные запросы предназначены для уведомления систем окружения об изменении маршрута. Этот режим работы может регулироваться настройками **Gratuitous ARP on Fail.**

4.2.4. Мониторинг хостов (Host Monitoring) при резервировании маршрутов

Обзор

Дополнительная функция системы NetDefendOS *Host Monitoring* обеспечивает гибкий и легко конфигурируемый способ контроля надежности маршрута. Данный метод позволяет системе

опрашивать один или несколько внешних хостов и на основе ответов принимать решение о доступности конкретного маршрута.

Преимущества функции *Host Monitoring*:

- В сложных сетевых топологиях необходима более тщательная проверка доступности внешних хостов. Контроль соединения локального коммутатора не может обнаружить проблему в другой части внутренней сети.

- Функция *Host Monitoring* может применяться для упрощения установки приемлемого уровня качества обслуживания (*Quality of Service*) Интернета (по времени отклика). В случае превышения времени отклика для существующего маршрута желательно инициировать процесс переключения маршрутов, соединение с Интернетом при этом не прерывается.

Включение Host Monitoring

В свойствах маршрута можно активировать функцию мониторинга хостов (*Host Monitoring)*, позволяющую контролировать состояние маршрута путем опроса нескольких хостов. Мониторинг нескольких хостов обеспечивает более высокую сетевую надежность в локальной сети по сравнению с мониторингом одного хоста, который может выключиться в любой момент.

При работе с *Host Monitoring* для маршрута задают два числовых параметра:

Grace Period	Период времени после запуска или реконфигурации межсетевого экрана NetDefend, в течение которого система NetDefendOS будет ожидать запуска Route Monitoring. Данное ожидание позволяет инициализировать все сетевые соединения межсетевого экрана.
Minimum Number of Hosts Available	Минимальное количество хостов, которое должно быть доступно, чтобы маршрут не был признан отказавшим.

Параметры хостов

У каждого хоста, для которого определена функция *Host Monitoring*, должны быть указаны следующие параметры:

- **Method**

  Хост запрашивает один из следующих методов:

  - *ICMP* – ICMP-запрос “ping”. Для данного метода должен быть определен IP-адрес.

  - *TCP* – TCP-соединение для хоста устанавливается и разъединяется. Для данного метода должен быть определен IP-адрес и порт.

  - *HTTP* – запросы HTTP-сервера с использованием URL. Должны быть определены URL-адрес и строковая переменная типа string, которая содержит начало или полный текст корректного ответа Web-сервера. Даже если такая величина не определена, любой ответ сервера будет считаться корректным.

- **IP Address**

  IP-адрес хоста при использовании методов ICMP или TCP.

- **Port Number**

  Номер порта для запросов при использовании метода TCP.

- **Interval**

Интервал (в миллисекундах) между попытками запросов. По умолчанию устанавливается 10000, минимальное значение 100 мс.

- **Sample**

  Число попыток запросов, используемое в качестве величины для вычисления процента потерь (*Percentage Loss)* и средней задержки (*Average Latency)*. Не может быть меньше 1.

- **Maximum Failed Poll Attempts**

  Максимальное допустимое количество неудачных опросов. Если это число превышено, то хост считается недоступным.

- **Max Average Latency**

  Максимальное среднее время ожидания (в миллисекундах) между запросом и ответом. Если этот порог превышен, то хост считается недоступным. Величина *Average Latency* вычисляется как среднее время ответов хоста. Если ответ на запрос не получен, то среднее время не вычисляется.

Опция обязательной доступности хоста (Reachability Required)

Reachability Required – опция, которая может быть включена для хоста. При выборе данной опции для того, чтобы маршрут функционировал, хост должен определиться как доступный. Если хост, отмеченный, как обязательно доступный, не отвечает, несмотря на то, что другие хосты доступны, маршрут считается отказавшим.

Если группа хостов выбрана для мониторинга, то для нескольких из них можно включить опцию **Reachability Required.** При определении системой NetDefendOS недоступности одного из таких хостов, маршрут считается отказавшим.

Параметры HTTP

Если метод мониторинга – HTTP, то можно указать следующие параметры:

- **Request URL**

  Запрашиваемый URL

- **Expected Response**

  Ожидаемый ответ от Web-сервера.

Анализ ожидаемого ответа обеспечивает возможность тестирования не только доступности хоста, но и работоспособности Web-сервера. Если, например, в ответе Web-сервера для определенной базы данных указывается текст “Database OK”, то отсутствие такого отчета указывает на то, что сервер работает, а приложение базы данных - нет.

Проблема, возникающая в том случае, если не определен ни один маршрут

При подключении к Интернет-провайдеру всегда должен быть определен маршрут внешней сети. Этот маршрут определяет, на каком интерфейсе может быть найдена сеть, существующая между межсетевым экраном NetDefend и провайдером. Если в системе к шлюзу Интернет-провайдера определен только маршрут по умолчанию (сеть назначения *all-nets)*, то в зависимости от используемого оборудования, механизм мониторинга маршрутов может функционировать не так, как ожидается.

Такая проблема возникает достаточно редко, причина ее появления – игнорирование ARP-запросов на неактивных маршрутах.

4.2.5. Расширенные настройки Route Failover

Для свойства *Route Failover* в системе NetDefendOS предусмотрены следующие расширенные настройки*:*

Iface poll interval

Время (в миллисекундах) после отправки запросов, по истечении которого интерфейс признается недоступным.

По умолчанию: *500*

ARP poll interval

Время (в миллисекундах) поиска хостов (ARP-lookup). Для некоторых маршрутов может не применяться.

По умолчанию: *1000*

Ping poll interval

Время (в миллисекундах) между отправкой к хосту Ping-запросов.

По умолчанию: *1000*

Grace time

Временной диапазон (в секундах) между первоначальным запуском или запуском после реконфигурации и началом мониторинга.

По умолчанию: *30*

Consecutive fails

Число последовательных неудачных запросов, необходимых для того, чтобы маршрут считался недоступным.

По умолчанию: *5*

Consecutive success

Число последовательных удачных запросов, необходимых для того, чтобы маршрут считался доступным.

По умолчанию: *5*

Gratuitous ARP on fail

Отправление Gratuitous ARP-запросов в режиме высокой отказоустойчивости (High Availability, HA) для уведомления хостов об изменениях на Ethernet-интерфейсе и изменениях IP-адресов.

По умолчанию: *Включена*

4.2.6. Proxy ARP

Обзор

Как уже было сказано в *разделе 3.4*, «*ARP*», ARP применяется для преобразования IP-адреса, используемого хостом Ethernet-сети, в MAC-адрес этого хоста.

Но иногда Ethernet-сеть может быть разделена на две части маршрутизирующим устройством, например межсетевым экраном NetDefend. В данном случае сама система NetDefendOS может отвечать на ARP-запросы, отправляя их в сеть, расположенную с другой стороны межсетевого экрана NetDefend, такой метод называется *Proxy ARP*.

Обычно метод *Proxy ARP* применяется при разделении Ethernet-сети на отдельные части таким образом, чтобы была возможность управления трафиком. В системе NetDefendOS для обеспечения безопасности трафика, проходящего между частями сети, используются наборы IP-правил.

Пример

Типичным примером является разделение сети на две подсети с установкой межсетевого экрана NetDefend между ними.

Хост **A** одной подсети может отправлять другой подсети **B** ARP-запросы для выяснения соответствия между MAC-адресом и IP-адресом. При включенной функции *Proxy ARP* система NetDefendOS отвечает на этот запрос – отправляет MAC-адрес вместо хоста **B**. После получения ответа хост **A** отправляет данные непосредственно системе NetDefendOS, которая в свою очередь перенаправляет их хосту **B**. В процессе прохождения трафика система NetDefendOS проверяет его на соответствие наборам IP-правил.

Настройка Proxy ARP

При настройке *Proxy ARP* в таблице маршрутизации определяются операции для маршрута. Пример: сеть, состоящая из двух подсетей *net_1* и *net_2*.

Сеть *net_1* связана с интерфейсом *if1*, сеть *net_2* связана с интерфейсом *if2*. *Route_1* – маршрут в системе NetDefendOS, описывающий, что сеть *net_1* подключена к интерфейсу *if1*.

Для маршрута *route_1* можно использовать *Proxy ARP* для сети *net_1* и интерфейса *if2*. После этого любой ARP-запрос хоста из сети *net_2,* связанной с *if2,* будет получать ответ от системы NetDefendOS при поиске IP-адреса в сети *net_1*. Другими словами, система NetDefendOS будет ссылаться на то, что адрес из сети *net_1* якобы найден на интерфейсе *if2*, и сама обеспечит прохождение трафика к *net_1*.

Таким же образом, включив Proxy ARP, можно опубликовать сеть *net_2* на интерфейсе *if1* для зеркалирования маршрутов.

№ маршрута (Route #)	**Сеть (Network)**	**Интерфейс (Interface)**	**Публикация Proxy ARP (Proxy ARP Published)**
1	net_1	if1	if2
2	net_2	if2	if1

В рассмотренном выше примере имеется возможность прозрачного обмена данными между хостами, при этом сети физически разделены. Пара маршрутов является зеркальным отображением друг друга и в таком типе соединения необязательно использовать *Proxy ARP*.

Следует учитывать, что если хост отправляет ARP-запрос IP-адреса, находящегося вне локальной сети, то этот запрос будет отправлен к шлюзу, настроенному для этого хоста. Пример такого соединения проиллюстрирован на следующем рисунке:

Рисунок 4.4. Пример Proxy ARP

Альтернатива Proxy ARP – прозрачный режим (Transparent Mode)

Прозрачный режим – еще один метод разделения Ethernet-сети на подсети. Настройка прозрачного режима не вызывает никакой сложности – достаточно просто определить соответствующие коммутируемые маршруты. Более подробная информация о коммутируемых маршрутах приведена в *Разделе 4.7, «Прозрачный режим (Transparent Mode)»*.

Proxy ARP и кластеры высокой отказоустойчивости (High Availability Clusters)

Коммутируемые маршруты не используются в HA-кластерах, то есть в этом случае нельзя применять прозрачный режим; нормально функционирует с HA-кластерами метод *Proxy ARP*.

Примечание: не все интерфейсы могут использовать Proxy ARP

Proxy ARP можно настроить только для VLAN и Ethernet-интерфейсов. Другими типами интерфейсов системы NetDefendOS Proxy ARP не поддерживается.

Маршруты, добавляемые автоматически

Следует заметить, что *Proxy ARP* нельзя применять для автоматически созданных маршрутов, так как им присвоен специальный статус, и их обработка происходит по-другому. К таким маршрутам относятся маршруты для физических интерфейсов, автоматически создаваемые при запуске системы NetDefendOS.

Если требуется включить функцию *Proxy ARP* для таких маршрутов, то их необходимо сначала удалить, а затем добавить вручную, как новые маршруты.

4.3. Маршрутизация на основе правил (PBR)

4.3.1. Обзор

Маршрутизация на основе правил (*PBR*, *Policy-Based Routing*) – дополнение к стандартной маршрутизации, описанной выше. PBR предоставляет администраторам гибкие возможности для определения правил маршрутизации на основе различных критериев, используя при этом альтернативные таблицы маршрутизации.

Стандартная маршрутизация отправляет пакеты согласно информации об IP-адресе получателя, полученной из статических или динамических протоколов маршрутизации. Например, при использовании OSPF, маршрут для пакета выбирается из SPF-расчета наименьшей длины пути. В PBR маршруты для трафика можно выбирать, исходя из определенных параметров трафика.

PBR может быть следующих типов:

Source based routing	Таблицы маршрутизации выбираются на основе источника трафика. При использовании более одного Интернет-провайдера, PBR может направлять трафик разных пользователей по различным маршрутам. Например, трафик из одного диапазона адресов может передаваться через одного ISP, в то время как трафик из другого диапазона адресов передается через второго ISP.
Service-based Routing	Таблицы маршрутизации выбираются на основе сервисов. PBR может маршрутизировать конкретный протокол, например HTTP, через proxy-службы, такие, как Web-кэш. Определенные сервисы также могут маршрутизироваться через выбранное Интернет-подключение.
User based Routing	Таблицы маршрутизации выбираются на основе идентификатора пользователя или группы, к которой он принадлежит. Данный метод удобно использовать в распределенной корпоративной сети, объеденной с помощью арендованных ISP-каналов.

В системе NetDefendOS маршрутизация на основе правил базируется на следующих понятиях:

- В дополнение к основной таблице маршрутизации **main**, заданной по умолчанию, пользователь может определить несколько альтернативных таблиц маршрутизации.
- Правила PBR применяются при выборе конкретной таблицы маршрутизации для соответствующего типа трафика.

4.3.2. PBR-таблицы

В системе NetDefendOS альтернативные таблицы маршрутизации содержат информацию, схожую с информацией из таблицы **main**, за исключением дополнительного параметра *Ordering*, определяющего приоритет просмотра таблиц маршрутизации относительно таблицы **main**. Более подробная информация приведена в *Разделе 4.3.5, «Параметры Ordering»*

4.3.3. Правила PBR

С помощью правил из набора правил PBR можно выбирать необходимые таблицы маршрутизации. Правила PBR могут применяться для определенных типов сервисов (например, HTTP), в сочетании с интерфейсом источника/назначения и сетью источника/назначения.

При просмотре наборов правил применяется первое подходящее правило.

4.3.4. Выбор таблицы маршрутизации

Когда система получает пакет, относящийся к новому соединению, то для выбора таблицы маршрутизации выполняются следующие шаги:

1. Прежде чем применять правила маршрутизации, с помощью основной таблицы маршрутизации определяется интерфейс назначения. Поэтому важно, чтобы в таблице main

был хотя бы маршрут по умолчанию (*all-nets)*, который будет использован в случае, если более подходящий маршрут не будет найден.

2. На данном этапе, осуществляется поиск правил, соответствующих заданным параметрам: интерфейс и сеть источника/назначения и выбранный протокол/сервис. Если соответствующее правило найдено, то используется определенная таблица маршрутизации. Если соответствующее правило не найдено, то используется таблица *main*.

3. Как только выбрана необходимая таблица маршрутизации, осуществляется проверка фактической принадлежности IP-адреса источника принимающему интерфейсу. Ищется соответствие с правилами доступа (Access Rules) (более подробная информация приведена в *Разделе 6.1, «Access Rules»).* Если правила доступа или соответствие с ними не найдено, то в выбранной таблице маршрутизации осуществляется обратный поиск, а в качестве параметра используется IP-адрес источника. В случае, если соответствие не найдено, в журнале *Log* генерируется сообщение об ошибке **Default access rule**.

4. На данном этапе в выбранной таблице маршрутизации осуществляется поиск маршрута, по которому пакет будет отправлен на интерфейс назначения. На результаты поиска влияет параметр *Ordering*, описываемый в следующем разделе. Для реализации виртуальной системы следует использовать опцию *Only*.

5. С этого момента соединение обрабатывается обычным набором IP-правил. Если в проверке участвует правило SAT, то выполняется преобразование адреса. Решение о том, какой маршрут использовать принимается до преобразования адресов, но фактический поиск маршрута выполняется с уже преобразованным адресом. Следует обратить внимание на то, что первоначальный поиск маршрута для определения интерфейса назначения осуществляется с еще не преобразованным адресом.

6. Если проверка IP-правилами прошла успешно, то в таблице состояний системы NetDefendOS открывается новое соединение и пакет передается через это соединение.

4.3.5. Параметры Ordering (Ordering parameter)

Если для нового соединения выбрана альтернативная таблица маршрутизации, то связанный с этой таблицей параметр *Ordering* определяет, как информация из альтернативной и основной (main) таблиц используется для поиска маршрута. Существуют три возможные опции:

1. **Default** – по умолчанию маршрут ищется сначала в основной таблице маршрутизации **main**. Если соответствующий маршрут не найден или найден маршрут с сетью назначения *all-nets* (*0.0.0.0/0*), то осуществляется поиск в альтернативной таблице. Если соответствующий маршрут в альтернативной таблице не найден, то будет использоваться маршрут по умолчанию из таблицы **main**.

2. **First** – в этом случае поиск маршрута осуществляется сначала в альтернативной таблице маршрутизации. Если соответствующий маршрут не найден, то поиск осуществляется в таблице **main**. Если в альтернативной таблице маршрутизации найден маршрут с сетью назначения *all-nets* (*0.0.0.0/0*), то он выбирается, как подходящий.

3. **Only** – при выборе данной опции все таблицы маршрутизации, за исключением альтернативной, игнорируются. В данном случае администратору следует выделить каждому приложению по отдельной таблице маршрутизации, с определенным набором интерфейсов. Данную опцию следует выбирать при создании виртуальных систем, так как в одной таблице маршрутизации можно определить набор интерфейсов.

Первые две опции можно считать, как объединение альтернативной таблицы с таблицей **main** и назначать только один маршрут, если в обеих таблицах найдено соответствие.

Важно: Маршрут all-nets обязательно должен присутствовать в таблице main

Отсутствие маршрутов с интерфейсом all-nets, заданных по умолчанию в таблице маршрутизации main – распространенная ошибка при использовании PBR.

Если соответствующий маршрут не найден и при этом отсутствует маршрут all-nets, то соединение будет отклонено (drop).

Пример 4.3. Создание таблицы маршрутизации на основе правил (Policy-based Routing Table)

В данном примере рассмотрено создание таблицы маршрутизации под названием *TestPBRTable*

Web-интерфейс

1. Выбрать **Routing > Routing Tables > Add > Routing Table**

2. Ввести:

- **Name**: *TestPBRTable*
- Выбрать один из следующих параметров **Ordering**:
  - **First** – изначально поиск ведется в таблице *TestPBRTable*. Если соответствующие маршруты не найдены, то поиск осуществляется в таблице *main*.
  - **Default** – изначально поиск ведется в таблице *main*. Если единственный соответствующий маршрут – маршрут, заданный по умолчанию (*all-nets*), то поиск осуществляется в таблице маршрутизации *TestPBRTable*. Если маршрут не найден, то поиск считается неудачным.
  - **Only** – поиск ведется только в таблице *TestPBRTable*. Даже если соответствующие маршруты не найдены, поиск в таблице *main* не осуществляется.

3. Если функция **Remove Interface IP Routes**, то созданные по умолчанию маршруты для интерфейса *core* удаляются.

4. Нажать кнопку **OK**

Пример 4.4. Создание маршрута

После определения таблицы *TestPBRTable,* в нее следует добавить маршруты.

Web-интерфейс

1. Выбрать **Routing > Routing Tables > TestPBRTable > Add > Route**

2. Ввести:

- **Interface**: Интерфейс отправки пакетов
- **Network**: Сеть назначения
- **Gateway**: Шлюз для отправки пакетов по данному маршруту
- **Local IP Address**: Определенный IP-адрес будет автоматически опубликован на соответствующем интерфейсе. Данный IP-адрес также будет использоваться в качестве адреса отправителя в ARP-запросах. Если IP-адрес не задан, то используется IP-адрес интерфейса межсетевого экрана.
- **Metric**: определенная метрика маршрута (Чаще всего применяется при резервировании каналов).

3. Нажать кнопку **OK**

Пример 4.5. Конфигурация PBR

В данном примере рассмотрен сценарий с несколькими ISP, при котором обычно используют PBR. Предполагается следующее:

- Каждый ISP предоставляет IP-сеть из принадлежащего ему диапазона. Пример: сценарий с двумя ISP, с сетью 10.10.10.0/24, предоставляемой провайдером *A* и 20.20.20.0/24 – провайдером *B*. ISP-шлюзы: 10.10.10.1 и 20.20.20.1 соответственно.

- Все адреса данного сценария публичные.

- Межсетевым экраном NetDefend используется по одному шлюзу в подсетях, предоставленных провайдерами.

В сети, независимой от провайдера, пользователю присваивается уникальный IP-адрес, обслуживаемый одним из провайдеров. У серверов с публичным доступом будет два IP-адреса, по одному от каждого провайдера. Этот параметр не влияет на настройки политик маршрутизации.

Следует обратить внимание на то, что для некоторых организаций Интернет-соединение, предоставляемое несколькими ISP, лучше осуществлять через BGP-протокол, где не требуется информация об IP-диапазонах или политиках маршрутизации. Но в некоторых случаях этот метод не применим, тогда возникает потребность в PBR.

В примере таблица маршрутизации main установлена для ISP A и добавлена вторая таблица маршрутизации *r2*, которая использует шлюз, заданный по умолчанию ISP B.

Интерфейс (Interface)	**Сеть (Network)**	**Шлюз (Gateway)**	**ProxyARP**
lan1	10.10.10.0/24		wan1
lan1	20.20.20.0/24		wan2
wan1	10.10.10.1/32		lan1
wan2	20.20.20.1/32		lan1
wan1	all-nets	10.10.10.1	

Таблица PBR с именем *r2*:

Интерфейс (Interface)	**Сеть (Network)**	**Шлюз (Gateway)**
wan2	all-nets	20.20.20.1

Значение параметра *Ordering* таблицы *r2* – *Default*, то есть к данной таблице маршрутизации будут обращаться в том случае, если в главной таблице будет найден только маршрут, заданный по умолчанию (*all-nets*).

Политики PBR:

Интерфейс источника (Source Interface)	**Диапазон источника (Source Range)**	**Интерфейс назначения (Destination Interface)**	**Диапазон назначения (Destination Range)**	**Выбранный сервис (Selected/ Service)**	**Прямая VR-таблица (Forward VR table)**	**Обратная VR-таблица (Return VR table)**
lan1	10.10.10.0/24	wan2	all-nets	ALL	r2	r2
wan2	all-nets	lan1	20.20.20.0/24	ALL	r2	r2

Настройки сценария:

Web-интерфейс:

1. Добавить маршрут, найденный в списке маршрутов в главную таблицу маршрутизации *main*, как было показано ранее.

2. Создать таблицу маршрутизации *r2* и установить Ordering-параметр в *Default*.

3. Добавить маршрут в таблицу маршрутизации *r2*, как было показано ранее.

4. На основании списка политик добавить две VR-политики, как было показано ранее.

   - Выбрать **Routing > Routing Rules > Add > Routing Rule**

   - Заполнить параметры правила, как было показано ранее.

   - Аналогично добавить второе правило.

Примечание

Правила в рассмотренном выше примере добавляются как для входящих, так и для исходящих соединений.

4.4. Функция Route Load Balancing

Обзор

В системе NetDefendOS предусмотрена функция, предназначенная для балансировки нагрузки – Route Load Balancing (RLB). При использовании этой функции появляется возможность распределения трафика.

Данная функция предназначена для следующих целей:

- Балансировка трафика между интерфейсами, управляемыми на основе политик.
- Балансировка трафика при одновременном подключении к Интернет через двух и более провайдеров.
- Для балансировки трафика, проходящего через VPN-туннели, установленные на разных физических интерфейсах.

Включение RLB

Функция RLB активизируется на основе таблицы маршрутизации путем создания объекта *RLB Instance*, в котором определены два параметра: таблица маршрутизации и RLB-алгоритм. С таблицей маршрутизации может быть связан только один объект *Instance*.

Для объекта *RLB Instance* должен быть определен один из следующих алгоритмов:

- **Round Robin**

  Циклический перебор подходящих маршрутов.

- **Destination**

  Данный алгоритм схож с алгоритмом Round Robin, за исключением того, что трафик, адресованный одному и тому же IP-адресу назначения, использует один и тот же маршрут.

- **Spillover**

  Если в течение заданного интервала времени трафик через определенный интерфейс превышает установленный порог, то используется следующий маршрут.

Отключение RLB

При удалении объекта *Instance* функция RLB для заданной таблицы маршрутизации отключается.

Этапы активации RLB

RLB для конкретной таблицы маршрутизации настраивается через объект *Instance*. После настройки алгоритм работы функции будет следующий:

1. В таблице маршрутизации осуществляется поиск маршрута; совпадающие маршруты собираются в список. Маршруты из списка должны охватывать одинаковый диапазон IP-адресов.

2. Если найден только один соответствующий маршрут, то используется именно этот маршрут и балансировка не производится.

3. Если найдено несколько маршрутов, то для выбора одного из них применяется RLB. Возможны следующие алгоритмы выбора в объекте *RLB Instance*:

   - **Round Robin**

     Маршруты один за другим выбираются из списка подходящих маршрутов. Если метрика всех маршрутов совпадает, то маршруты выбираются равномерно, если метрика маршрутов разная, то маршруты с меньшей метрикой выбираются чаще, пропорционально разнице весов маршрутов.

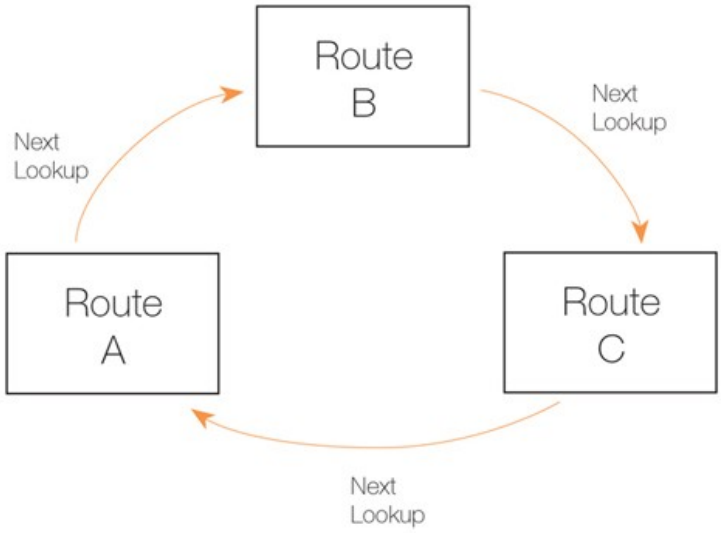


Рисунок 4.5. RLB-алгоритм Round Robin

   - **Destination**

     Данный алгоритм схож с алгоритмом Round Robin, за исключением того, что трафик, адресованный одному и тому же IP-адресу назначения, направляется через один и тот же маршрут. При использовании такого алгоритма, в случае установки нескольких соединений с конкретным сервером IP-адрес источника будет один и тот же.

   - **Spillover**

     Данный алгоритм отличается от алгоритмов, описанных выше. При использовании этого алгоритма, трафик направляется через первый подходящий маршрут. Смена маршрута происходит, когда в течение заданного интервала времени (параметр *Hold Timer)*, трафик через определенный интерфейс превышает установленный порог (параметр *Spillover Limits)*. С этого момента для пересылки трафика используется следующий маршрут, выбираемый из списка подходящих.

     Величины *Spillover Limits* и *Hold Timer* (по умолчанию 30 секунд) для интерфейса устанавливаются в настройках RLB *Algorithm Settings*.

     Когда объем проходящего через интерфейс трафика находится ниже величины *Spillover Limits* в течение интервала *Hold Timer,* трафик начинает пересылаться через соответствующий интерфейс по первоначальному маршруту.

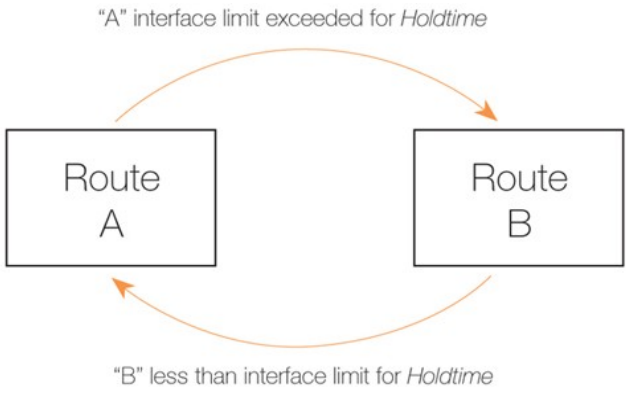


Рисунок 4.6. RLB-алгоритм Spillover

Для входящего и исходящего трафика устанавливается своя величина *Spillover Limits*. Как правило, используется только один из этих параметров. Даже если будут определены оба параметра, для инициирования процедуры смены маршрута достаточно превышения одной из величин *Spillover Limit* на период *Hold Timer*. Для удобства использвания *Spillover Limit* может измеряться в Кбит/с, Мбит/с, Гбит/с.

Использование метрик маршрута с алгоритмом Round Robin

Каждому конкретному маршруту назначена метрика, значение которой по умолчанию равно нулю. При использовании алгоритмов *Round Robin* и *Destination* можно устанавливать разное значение метрик, для того, чтобы сместить приоритет маршрутов в сторону маршрутов с меньшей метрикой. Маршруты с минимальным значением метрики будут выбираться чаще, чем маршруты с более высоким значением.

Если в сценарии с двумя ISP требуется, чтобы большая часть трафика проходила через один из ISP, то следует включить RLB и установить меньшую метрику для маршрута основного ISP, и более высокое значение метрики для маршрута второго ISP, нагрузка будет балансироваться пропорционально разнице метрик первого и второго маршрутов.

Использование метрик маршрута с алгоритмом Spillover

При использовании алгоритма *Spillover* должно быть учтено следующее:

- **Для каждого маршрута обязательно должно быть установлено значение метрики**

  В этом случае система NetDefendOS всегда выбирает маршрут с самым низким значением метрики. Алгоритм не предназначен для работы с одинаковыми метриками маршрутов, поэтому администратору следует устанавливать различные значения данных величин для всех маршрутов, к которым применяется алгоритм *Spillover*.

  Метрика определяет порядок, в соответствии с которым выбирается новый маршрут, после того как для текущего маршрута превышено допустимое значение передаваемого трафика.

- **Несколько альтернативных маршрутов**

  Как только установленный порог *Spillover Setting* для нового маршрута данного интерфейса также будет превышен, выбирается следующий маршрут с более высокой метрикой, и так далее. Когда объем трафика, проходящего через один из интерфейсов с меньшей метрикой, будет находиться ниже величины *Spillover Limits* в течение интервала *Hold Timer*, произойдет возврат к предыдущему выбранному маршруту.

- **При отсутствии альтернативного маршрута смена маршрута не происходит**

  Если на всех альтернативных маршрутах достигнуты пороговые значения *Spillover Limit*, то

маршрут не изменяется.

IP-диапазоны соответствующих маршрутов должны быть одинаковы

Как было рассмотрено выше, IP-адреса соответствующих маршрутов, выбранных RLB из таблицы маршрутизации, должны принадлежать одному диапазону, в противном случае балансировка между маршрутами не производится.

Например, если один маршрут принадлежит диапазону *10.4.16.0/24*, а второй – *10.4.16.0/16*, то балансировка между этими маршрутами не производится, так как диапазоны IP-адресов не совпадают.

Следует также учитывать, что механизм Route Lookup выбирает маршрут с минимальным диапазоном IP-адресов. В рассмотренном выше примере может быть выбран *10.4.16.0/24*, так как этот диапазон содержит меньше IP-адресов, чем диапазон *10.4.16.0/16* и оба диапазона содержат IP-адреса из *10.4.16.0/16*.

Сброс параметров RLB (RLB Reset)

RLB-алгоритмы устанавливаются в первоначальное состояние в двух случаях:

- Изменение конфигурации системы NetDefendOS.
- Переключение на резервное устройство при работе в режиме высокой отказоустойчивости.

При возникновении таких ситуаций выбранный маршрут возвратится к состоянию на момент начала работы алгоритма.

Ограничения RLB (RLB Limitations)

Следует отметить, что выбор альтернативных маршрутов происходит после завершения поиска маршрутов. Такой выбор зависит от использующегося для найденных маршрутов алгоритма и от текущего состояния этого алгоритма.

При работе у RLB-алгоритма нет информации о количестве переданного трафика между производимыми поисками маршрутов. Цель RLB-алгоритма состоит в распределении трафика между существующими альтернативными маршрутами, при условии, что каждый поиск маршрута будет связан с некоторым соединением, передающим какой-то предполагаемый объем трафика.

Сценарий RLB

На рисунке 4.7 приведен типичный пример применения RLB. Группа пользователей, объединенных в сеть через LAN-интерфейс межсетевого экрана NetDefend, получает доступ в Интернет.

Доступ в Интернет предоставляют два провайдера, шлюзы которых, GW1 и GW2, связаны через интерфейсы межсетевого экрана WAN1 и WAN2. RLB используется для балансировки соединений между этими ISP.

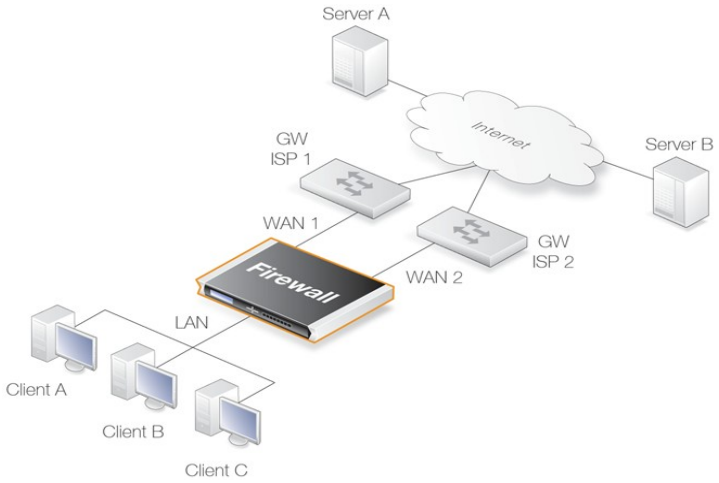


Рисунок 4.7 Сценарий балансировки Route Load Balancing

Следует определить маршруты к ISP в таблице маршрутизации *main*:

№ маршрута (Route №)	Интерфейс (Interface)	Назначение (Destination)	Шлюз (Gateway)	Метрика (Metric)
1	WAN1	all-nets	GW1	100
2	WAN2	all-nets	GW2	100

Поскольку в этом примере не используется алгоритм *Spillover* значение метрики, используемое для маршрутов, как правило, одинаковое, например 100.

При использовании RLB-алгоритма *Destination*, для клиентов, подключающихся к определенному серверу, используется один и тот же маршрут и один IP-адрес источника. Если применяется NAT, то IP-адресом будет адрес **WAN1** или **WAN2**.

Для передачи любого трафика, кроме маршрутов, необходимо задать разрешающие IP-правила. Указанные ниже правила разрешают прохождение трафика от любого ISP и определяют действие NAT для трафика, использующего внешние IP-адреса интерфейсов **WAN1** и **WAN2**.

№ правила (Rule №)	Действие (Action)	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
1	NAT	lan	lannet	WAN1	all-nets	All
1	NAT	lan	lannet	WAN2	all-nets	All

В вышеупомянутых IP-правилах используется сервис *All*, но предпочтительней указывать конкретный сервис или группу сервисов.

Пример 4.6. Настройка RLB

В данном примере рассматриваются детали настройки RLB. IP-адреса объектов адресной книги определены заранее.

IP-объекты WAN1 и WAN2 представляют интерфейсы, через которые производится соединение с двумя ISP, IP-объекты GW1 и GW2 представляют собой IP-адреса шлюзов маршрутизаторов ISP.

Шаг 1. Определение маршрутов в главной таблице маршрутизации *main*.

Шаг 2. Создание RLB-объекта *Instance*.

Созданный RLB-объект Instance использует алгоритм *Destination*, который фиксирует IP-адрес источника для конкретного сервера, вследствие чего сервер видит всегда один и тот же IP-адрес источника (WAN1 или WAN2).

CLI

gw-world:/> **add RouteBalancingInstance main Algorithm=Destination**

Web-интерфейс

1. Выбрать **Routing > Route Load Balancing > Instances > Add > Route Balancing Instance**

2. В открывшемся диалоге route balancing instance ввести:

- **Routing Table**: main
- **Algorithm**: Destination
- Нажать кнопку **OK**

Шаг 3. Создание IP-правил, разрешающих прохождение трафика.

В завершении, к набору IP-правил необходимо добавить IP-правила, разрешающие прохождение трафика. В данном примере не указаны подробные шаги создания IP-правил, поскольку они описываются в рассмотренных выше примерах.

RLB и VPN

При совместном использовании RLB и VPN возникает ряд проблем.

Проблема возникает при использовании RLB для балансировки трафика между двумя IPSec-туннелями, так как в этом случае удаленные точки (*Remote Endpoint*) для любого из этих туннелей должны быть различны. Для решения этой проблемы следует предпринять следующие шаги:

- Воспользоваться услугами двух ISP, через один туннель соединяться с первым ISP, через другой – со вторым. В этом случае RLB будет нормально функционировать с двумя туннелями.

  Чтобы функционировал второй туннель необходимо в таблицу маршрутизации **main** добавить уникальный маршрут хоста, указывающий на интерфейс и шлюз второго ISP.

  Такое решение обеспечивает избыточность в случае разрыва одного из ISP-соединений.

- Использовать VPN, в котором один из туннелей является IPSec-туннелем, а второй туннель организован на основе другого протокола.

  Если, например, оба туннеля должны быть с IPSec-соединениями, возможна инкапсуляция IPSec в GRE-туннель (другими словами IPSec-туннель помещается в GRE-туннель). GRE – простой туннелирующий протокол без шифрования, включающий в себя минимум затрат. Более подробная информация о GRE-туннелях приведена в *Разделе 3.3.5 «GRE-туннели».*

4.4. OSPF

Применяемый в системе NetDefendOS метод динамической маршрутизации (*Dynamic Routing*) построен на основе OSPF-архитектуры.

В данном разделе рассматривается понятие динамической маршрутизации и возможность ее применения, осуществление динамической маршрутизации на основе протокола OSPF и настройка простой OSPF-сети.

4.5.1. Динамическая маршрутизация (Dynamic Routing)

Прежде чем начать рассматривать OSPF следует понять, что такое динамическая маршрутизация, и какие типы динамической маршрутизации реализуют с использованием OSPF. Ниже приведены основные понятия динамической маршрутизации и OSPF.

Отличия от статической маршрутизации

При использовании динамической маршрутизации, в отличие от статической, маршрутизирующие сетевые устройства, такие как межсетевые экраны NetDefend, могут автоматически адаптироваться к изменениям топологии сети.

В динамической маршрутизации используются первоначальные сведения о непосредственно подключенных сетях, и постоянно поступает информация о других маршрутизаторах и связанных с ними сетях. Все поступающие данные о маршрутах обрабатываются и наиболее подходящие для локальных и удаленных соединений маршруты добавляются в локальные таблицы маршрутизации.

Динамическая маршрутизация реагирует на динамическое обновление маршрутов, но ее недостатком является более высокая восприимчивость к определенным проблемам, таким как петли маршрутизации. В основе механизма динамической маршрутизации обычно используют один из следующих алгоритмов:

- Вектора расстояний (*Distance Vector, DV*)
- Состояния канала (*Link State, LS*)

От типа используемого алгоритма зависит, как маршрутизатор принимает решение о выборе оптимального маршрута и передает обновленную информацию другим маршрутизаторам. Подробнее об этих алгоритмах рассказано ниже.

Алгоритм вектора расстояний (Distance Vector, DV)

Алгоритм вектора расстояний – алгоритм распределенной маршрутизации, который вычисляет наилучший среди альтернативных путей.

Каждый маршрутизатор в сети вычисляет «стоимость» подключенных к нему соединений и передает информация о них только соседним маршрутизаторам. Каждый маршрутизатор определяет путь с наименьшей «стоимостью» до сети назначения, с помощью итерационных вычислений, также используя информацию, полученную от соседних маршрутизаторов.

RIP-протокол – DV-алгоритм, применяемый для информационного обмена между маршрутизаторами, работающий посредством регулярной посылки сообщений которые содержат обновления и отражают изменения маршрутов в таблицах маршрутизации. Выбор пути основан на вычислении длины этого пути, которая равна количеству промежуточных пересылок (хопов).

После обновления своей таблицы маршрутизации, маршрутизатор незамедлительно начинает передачу всей своей таблицы маршрутизации соседним маршрутизаторам, информируя их об изменениях.

Алгоритм маршрутизации по состоянию канала (Link State, LS)

В отличие от DV-алгоритмов LS-алгоритмы допускают хранение таблиц маршрутизации, отражая тем самым топологию сети.

Каждый маршрутизатор пересылает связанные с ним соединения и стоимость этих соединений всем остальным маршрутизаторам в сети. При получении маршрутизатором таких сообщений запускается LS-алгоритм, который вычисляет свой собственный набор путей, имеющих наименьшую стоимость. Информация о любом изменении состояния соединения рассылается каждому маршрутизатору в сети, после чего, все маршрутизаторы содержат одинаковую информацию в таблицах маршрутизации и согласованные представления о состоянии сети.

Преимущества LS-алгоритмов

Так как информация о состоянии соединений распространена по всей сети, то LS-алгоритмы, например, используемые в OSPF, обеспечивают масштабируемость и позволяют выполнять более детальные настройки. Смена состояния соединения приводит к отправке другим маршрутизаторам только изменившейся информации, что обеспечивает быструю сходимость и меньшую вероятность возникновения петель маршрутизации. В отличие от RIP, который не хранит данные об адресации

подсетей, OSPF может функционировать в иерархических сетях.

Решение OSPF

Open Shortest Path First (OSPF) – широко используемый протокол, основанный на LS-алгоритме. Динамическая маршрутизация в системе NetDefendOS осуществляется с использованием OSPF-протокола.

Примечание: OSPF-протокол поддерживается не всеми моделями D-Link

OSPF-алгоритм поддерживается следующими моделями D-Link NetDefend: DFL-800, 860, 1600, 1660 2500, 2560 и 2560G.

Модели DFL-210 и 260 не поддерживают OSPF.

OSPF позволяет маршрутизатору идентифицировать другие маршрутизаторы и подсети, непосредственно с ним связанные, и только после этого передает информацию к остальным маршрутизаторам. Каждый маршрутизатор использует получаемую информацию и добавляет изученные OSPF маршруты в таблицу маршрутизации.

С такими расширенными данными каждый OSPF-маршрутизатор сможет получить информацию о сетях и маршрутизаторах, через которые проходят маршруты к заданному IP-адресу назначения, и определить наилучший из них. При использовании OSPF маршрутизатор отправляет другим маршрутизаторам не все записи таблицы маршрутизации, а только обновленные и измененные данные о маршрутах.

OSPF использует разные критерии (метрики) для выбора маршрута, включая хопы, полосу пропускания, загрузку и задержку. За счет правильного выбора подходящих метрик OSPF обеспечивает высокий уровень контроля над процессом маршрутизации.

Простой сценарий использования OSPF

Простая топология сети, проиллюстрированная ниже, наглядно демонстрирует применение OSPF. Два межсетевых экрана **A** и **B** связаны межу собой и сконфигурированы в некоторой OSPF-области (объяснение термина *область* (*area*) будет дано позже).

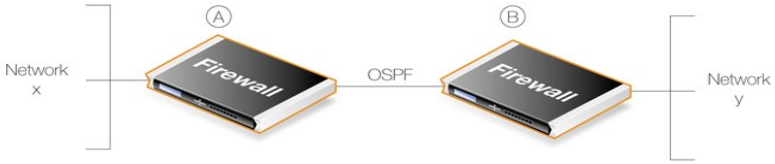


Рисунок 4.8. Простой сценарий использования OSPF

При использовании OSPF межсетевой экран A «знает», что для достижения сети Y, трафик необходимо отправить межсетевому экрану B. OSPF предоставляет возможность межсетевому экрану B обмениваться информацией с A, необходимость в ручном добавлении записей в таблицу маршрутизации отпадает.

Таким же образом межсетевой экран **B** автоматически узнает, что сеть **X** связана с межсетевым экраном **A**.

При использовании OSPF, обмен информацией о маршрутизации полностью автоматизирован.

OSPF обеспечивает резервирование маршрута (Route Redundancy)

Если в рассмотренный выше сценарий добавить третий межсетевой экран NetDefend **C,** то все межсетевые экраны будут знать о сетях, связанных с другими экранами. Такая ситуация проиллюстрирована на следующем рисунке.

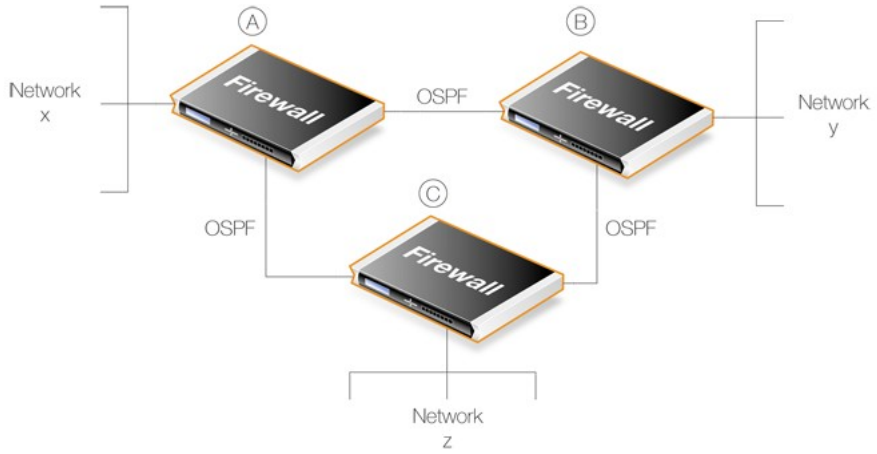


Рисунок 4.9. OSPF обеспечивает избыточность маршрута

Кроме того, в этом случае появляется избыточность между любыми двумя межсетевыми экранами. Например, если соединение между A и C утеряно, то OSPF незамедлительно информирует эти межсетевые экраны о наличии альтернативного маршрута через межсетевой экран B.

Трафик из сети X, предназначенный для сети Z будет автоматически направляться через межсетевой экран B.

На каждом межсетевом экране должны быть прописаны только маршруты для сетей, непосредственно с ним связанных. OSPF автоматически добавляет информацию о маршрутах сетей, связанных с другими межсетевыми экранами, даже если трафик до конкретного узла сети должен пройти через несколько транзитных маршрутизаторов.

Совет: Кольцевая топология всегда предусматривает альтернативные маршруты

При проектировании топологии сети, реализовывающей OSPF, установка межсетевых экранов NetDefend в кольцо означает, что у любого межсетевого экрана всегда есть два маршрута к другому межсетевому экрану. Если некоторое соединение через межсетевой экран отсутствует, то всегда существует альтернативный маршрут

Метрики маршрутизации (Metric Routing)

При описании динамической маршрутизации и метода OSPF полезно обратить внимание на метрики маршрутизации (*Metric Routing*).

Метрики маршрутизации – критерии, по которым алгоритм маршрутизации, вычисляет наилучшей маршрут к сети назначения. Протокол маршрутизации полагается на одну или несколько метрик для оценки имеющихся маршрутов и определения оптимального пути. Основные используемые метрические величины:

Path Length	Суммарная стоимость всех пересылок в маршруте. Обычно для этой метрики используется величина (“hop count”) – число маршрутизирующих устройств, через которые проходит пакет при пересылке от источника к назначению.
Item Bandwidth	Пропускная способность пути, измеряемая в Мбит/с.
Load	Загруженность маршрутизатора, оценивается коэффициентом, учитывающим доступную полосу пропускания и загруженность CPU.
Delay	Время, затраченное на пересылку пакета от источника к получателю. Время задержки зависит от различных факторов, включая полосу пропускания, загрузку и длину пути.

4.5.2. Концепции OSPF

Обзор

Open Shortest Path First (OSPF) – протокол маршрутизации, разработанный комиссией IETF *(Internet Engineering Task Force)* для IP-сетей. Выполнение NetDefend OSPF основано на стандарте RFC 2328, обратно совместимым с RFC 1583.

Примечание: OSPF-протокол поддерживается не всеми моделями D-Link

OSPF-алгоритм поддерживается следующими моделями D-Link NetDefend: DFL-800, 860, 1600, 1660 2500, 2560 и 2560G.

Модели DFL-210 и 260 не поддерживают OSPF.

Протокол OSPF осуществляет маршрутизацию IP-пакетов, основываясь только на IP-адресе назначения, который содержится в заголовке IP-пакета. IP-пакеты маршрутизируются «как есть», другими словами, когда пакеты проходят через автономную систему *Autonomous System (AS*), к ним не добавляется никаких дополнительных заголовков протоколов.

Автономная система (Autonomous System, AS)

Под термином «*Autonomous System*» понимается отдельная сеть или группа сетей с единственной, четко определенной политикой маршрутизации, контролируемая общим администратором. Политика маршрутизации определяет верхний уровень древовидной разветвленной структуры, описывающей различные компоненты OSPF.

В системе NetDefendOS *AS* соответствует объекту *OSPF Router*, который определяется первым при настройке *OSPF*. В большинстве сценариев требуется определить только один OSPF *Router* на каждом межсетевом экране NetDefend OSPF-сети. Объект OSPF *Router* системы NetDefendOS рассмотрен в Разделе *4.5.3.1, "OSPF Router Process"*.

OSPF – это динамический протокол маршрутизации, который достаточно быстро обнаруживает изменения топологии сети в автономной системе (например, в случае отказа интерфейса маршрутизатора) и выбирает новые маршруты к сетям назначения без образования петель.

Link-State-маршрутизация (Link-state Routing, LS)

OSPF – это форма *LS-маршрутизации*, которая отправляет *LS-оповещения* (*Link-State Advertisement, LSA*) всем остальным маршрутизаторам, относящимся в той же автономной системе. Каждый маршрутизатор управляет *LS-базой данных,* в которой хранится топология автономной системы. Используя эту базу данных, маршрутизатор строит дерево оптимальных маршрутов к другим маршрутизаторам, где корень дерева – он сам. Самый короткий путь в дереве соответствует оптимальному маршруту к каждой сети назначения в автономной системе.

Аутентификация

Если требуется, то весь обмен информацией в OSPF-протоколе может быть аутентифицирован. Это означает, что только после корректной аутентификации, маршрутизаторы могут присоединиться к AS. В системе NetDefendOS могут использоваться различные схемы аутентификации, например пароль или MD5-дайджест.

В системе NetDefendOS можно определять методы аутентификации для каждой автономной системы.

Область OSPF Area

Область *OSPF Area* состоит из сгруппированных вместе внутри автономной системы сетей и хостов. Маршрутизаторы, находящиеся внутри этой области называются *внутренними маршрутизаторами (internal router)*. Все интерфейсы внутренних маршрутизаторов непосредственно связаны с сетями, находящимися внутри этой зоны.

Топология области скрыта от остальной части автономной системы AS. Такое скрытие информации уменьшает количество служебного трафика между маршрутизаторами. Помимо этого, маршрутизация в пределах одной зоны, определяется только топологией этой зоны, что обеспечивает защиту области от неоптимальных маршрутов. Можно сказать, что область – обобщение понятия разделенной на IP-подсети сети.

В системе NetDefendOS области определяются объектами *OSPF Area* и добавляются в автономную систему AS, которая определяется объектом *OSPF Router*. В одной автономной системе может быть определено несколько областей, то есть к одному объекту *OSPF Router* можно добавить несколько объектов *OSPF Area*. В большинстве случаев одного объекта достаточно, и он должен быть определен на каждом межсетевом экране, который является частью OSPF-сети.

Более подробная информация приведена в *Разделе 4.5.3.2, "Объект OSPF Area"*.

Компоненты области OSPF Area

Краткие характеристики таких OSPF-компонентов приведены ниже.

ABR	*Граничные маршрутизаторы области* (*Area Border Router*) – маршрутизаторы, интерфейсы которых связаны с несколькими областями. В них хранятся отдельные базы данных топологий для каждой области, с которой они связаны.

ASBR — *Граничные маршрутизаторы автономной системы* (*Autonomous System Boundary Routers*) – маршрутизаторы, обменивающиеся информацией о маршрутизации с маршрутизаторами других автономных систем. Они отправляют анонсы изученных маршрутов к внешним сетям внутри автономной системы.

Backbone Area — В любых OSPF-сетях обязательно должна быть определена *магистральная область(Backbone Area)*, которая является OSPF-областью с идентификатором ID равным 0. Это область, к которой должны подключатся остальные связанные области. Магистраль обеспечивает распределение информации о маршрутизации между связанными областями. Если область не связана непосредственно с магистралью, то необходимо добавить виртуальное соединение.

Разработка OSPF-сети должна начинаться с создания магистральной области.

Stub Area — *Тупиковыми (Stub)* называются области, через/в которые не поступают внешние оповещения автономной системы. Когда область настроена в качестве тупиковой, маршрутизатор автоматически оповещает о маршруте по умолчанию для того, чтобы маршрутизаторы в тупиковой области могли отправлять данные в сети, находящиеся за пределами их области.

Transit Area — *Транзитная область* используется для передачи трафика из области не соединенной непосредственно с магистральной областью.

Маршрутизатор Designated Router (DR)

В каждой широковещательной OSPF-сети существует один выделенный маршрутизатор *Designated Router (DR)* и один резервный выделенный маршрутизатор *Backup Designated Router (BDR)*. Для выбора DR и BDR, каждый маршрутизатор отправляет OSPF-сообщения *Hello* со своим приоритетом. Если в сети уже сеть DR, то он не меняется независимо от приоритета других маршрутизаторов.

В системе NetDefendOS DR и BDR назначаются автоматически.

Соседние маршрутизаторы

Маршрутизаторы, находящиеся в одной области считаются соседними. Соседние маршрутизаторы выбираются путем обмена сообщениями *Hello*, которые периодически отправляются на каждый интерфейс с помощью многоадресной IP-рассылки. Маршрутизаторы считаются соседними с того момента, как они попали в список “соседей” в сообщении *Hello*. Таким образом, гарантируется двусторонний обмен данными.

Ниже приведены возможные состояния соседних маршрутизаторов (*Neighbor State*).

Down — Начальное состояние соседних маршрутизаторов.

Init — Если сообщение *Hello* от “соседа” получено, но у межсетевого экрана нет ID этого маршрутизатора.

Как только соседний маршрутизатор получит сообщение *Hello*, он узнает ID отправившего его маршрутизатора и укажет его в своем сообщении *Hello*, после этого состояние изменится на *2-Way*.

2-Way — Соединение между маршрутизатором и “соседом” является двунаправленным (bi-directional).

На OSPF-интерфейсах *Point-to-Point* и *Point-to-Multipoint* состояние

	изменится на *Full*. На широковещательных интерфейсах состояние *Full* будет только у соединений между DR/DBR и их соседями, в остальных случаях – *2-way*.
ExStart	Подготовка к построению связей между “соседями”.
Exchange	Маршрутизаторы обмениваются информацией из LS-базы данных.
Loading	Маршрутизаторы обмениваются *LS-оповещениями*.
Full	Нормальное состояние смежности между маршрутизатором и DR/BDR, когда их LS-базы данных считаются синхронизированным.

Агрегации (Aggregates)

OSPF-агрегирование используется для объединения группы маршрутизаторов с общими адресами в одну запись в таблице маршрутизации, что позволяет минимизировать таблицу маршрутизации.

Более подробная информация приведена в *Разделе 4.5.3.5, “Объект OSPF Aggregate”*.

Виртуальные каналы

Виртуальные каналы применяются в случае:

A. Подключения области, не имеющей прямого соединения с магистралью к магистрали.

B. Объединение областей (areas) магистрали, когда магистраль разделена на несколько частей.

Оба случая рассмотрены ниже.

A. *Подключения к магистрали области, не имеющей с ней прямого соединения*

Магистральная область *Backbone Area* должна быть центром для всех остальных областей. В редких случаях нет возможности подключить некоторую область непосредственно к магистральной области, для подключения используются *виртуальные каналы* (*Virtual Link*), которые предоставляют логическое соединение между областью и магистралью.

Виртуальный канал устанавливается между двумя *граничными маршрутизаторами области* (ABR), один из которых подключен к магистральной области. В приведенном ниже примере два маршрутизатора соединены с одной областью (Area 1), но только один из них, *fw1* физически связан с магистральной областью.

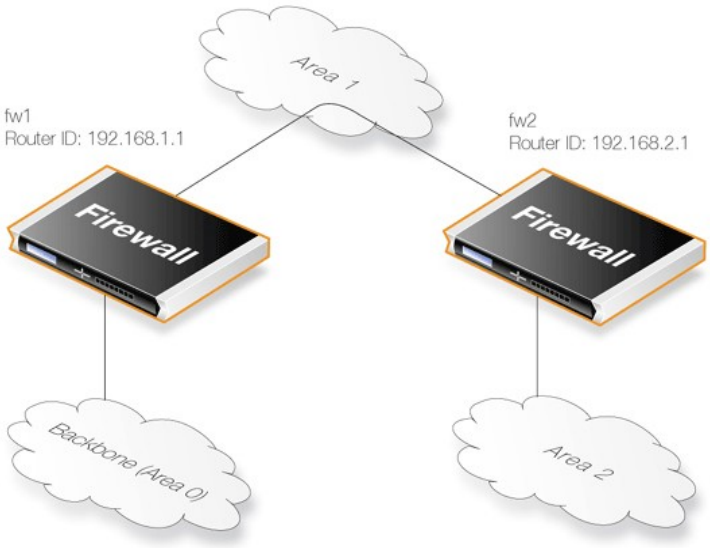


Рисунок 4.10. Соединение зон виртуальным каналом

В примере *виртуальный канал* настроен между *fw1* и *fw2* в *Area1*, которая используется как транспортная область. При такой конфигурации требуется только настройка *ID маршрутизатора* (*Router ID*). Как показано на рисунке требуется настроить виртуальный канал от *fw2* к *fw1* с ID маршрутизатора 192.168.1.1 и наоборот. Эти виртуальные каналы следует настраивать в области *Area1*.

B. *Объединение распределенной (разделенной на несколько частей) магистрали*

OSPF позволяет использовать виртуальный канал для объединения разделенной магистральной зоны. Виртуальный канал должен быть настроен между двумя отдельными ABR, лежащими на границе каждой из частей магистрали и объединенными общей зоной.

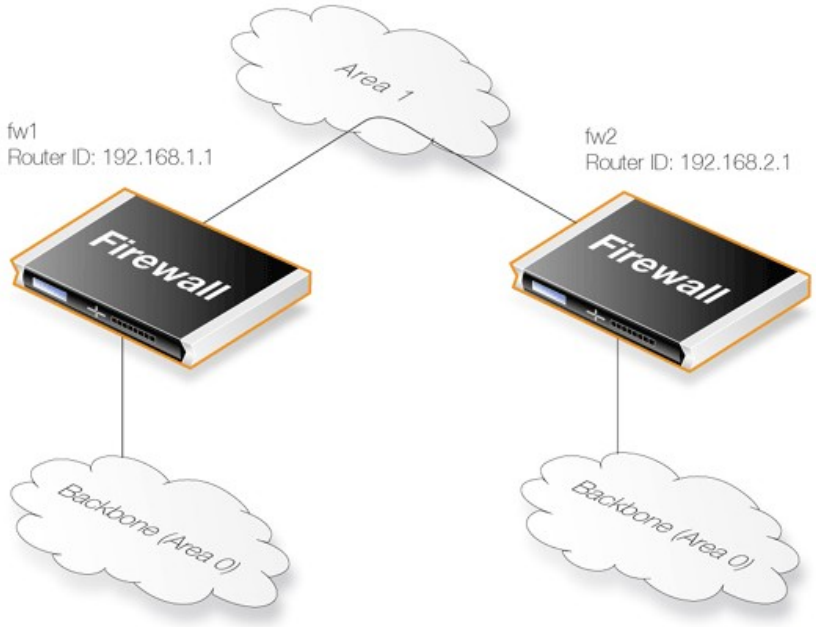


Рисунок 4.11. Виртуальные каналы, объединяющие разделенную магистраль

Виртуальный канал настроен между *fw1* и *fw2* в *Area1*, которая используется как транзитная область. При такой конфигурации требуется только настройка *ID маршрутизатора* (*Router ID*). Как уже было сказано, требуется настроить виртуальный канал от *fw2* к *fw1* с ID маршрутизатора *192.168.1.1* и наоборот. Эти виртуальные каналы следует настраивать в области *Area1*.

Более подробная информация приведена в *Разделе 4.5.3.6, "Виртуальные каналы OSPF"*.

OSPF в режиме высокой отказоустойчивости

Существуют некоторые ограничения в поддержке режима HA для OSPF:

На активном и резервном устройствах HA-кластера будут запущены раздельные процессы обработки, резервное устройство гарантирует, что будет иметь низший приоритет при выборе маршрутов. Управляющий (master) и подчиненный (slave) маршрутизаторы в HA-группе не могут обмениваться информацией о маршрутах непосредственно между собой и им не разрешено становиться DR или BDR в широковещательных сетях. Данные ограничения достигаются за счет принудительной установки приоритета маршрутизатора в 0.

Для того чтобы OSPF в режиме HA функционировал корректно, межсетевому экрану NetDefend требуется иметь широковещательный интерфейс, по крайней мере, с одним соседним маршрутизатором в каждой из областей, к которым подключен межсетевой экран. По сути, резервному межсетевому экрану требуется "сосед" для получения базы данных состояний соединений.

Следует также отметить, что невозможно поместить HA-группу в широковещательную сеть, если в ней нет других соседних маршрутизаторов (так как они не смогут синхронизировать базы данных состояний соединений из-за маршрутизатора с приоритетом 0). Тем не менее, в зависимости от поставленной задачи, можно установить между ними соединение точка-точка (point-to-point). Особое внимание должно быть уделено настройке виртуального канала к межсетевому экрану в HA-кластере. При настройке соединения между конечным хостом и межсетевым экраном в HA-кластере должно быть установлено 3 отдельных соединения: к маршрутизаторам с идентификаторами, соответствующими управляющему межсетевому экрану, подчиненному межсетевому экрану и общему идентификатору кластера.

Использование OSPF в системе NetDefendOS

При использовании OSPF в системе NetDefendOS возможен следующий сценарий: два или более межсетевых экрана связаны друг с другом некоторым способом. OSPF позволяет любому из этих межсетевых экранов выбирать корректный маршрут для передачи трафика в сеть назначения, находящуюся за другим межсетевым экраном, если таблице статической маршрутизации межсетевого экрана нет маршрута к этой сети.

Ключевой аспект установки OSPF заключается в том, что при соединении межсетевые экраны обмениваются информацией из своих таблиц маршрутизации таким образом, чтобы трафик, входящий на интерфейс межсетевого экрана мог автоматически маршрутизироваться к требуемому интерфейсу на том шлюзе, через который проходит рабочий маршрут к сети назначения.

Другим не менее важным аспектом является то, что межсетевые экраны контролируют состояние соединений друг с другом и маршрутизируемый трафик в случае необходимости может быть отправлен по альтернативному маршруту. Поэтому топология сети устойчива к ошибкам. Если связь между двумя межсетевыми экранами прервалась, то будет использоваться альтернативный маршрут.

4.5.3. Компоненты OSPF

В данном разделе рассматриваются объекты системы NetDefendOS, необходимые для настройки OSPF-маршрутизации. При определении этих объектов создается OSPF-сеть. Объекты должны быть определены на каждом межсетевом экране NetDefend, который является частью OSPF-сети и должны описывать ту же сеть.

Иллюстрация связей между OSPF-объектами системы NetDefendOS приведена ниже.

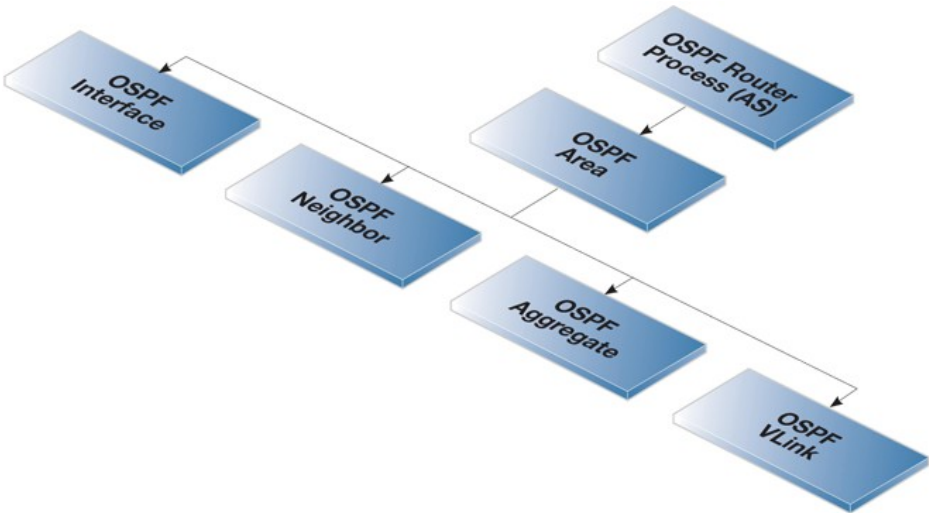


Рисунок 4.12. OSPF-объекты системы NetDefendOS

4.5.3.1. Объект OSPF Router Process

Объект *Автономная Система* (*Autonomous System)* является высшим уровнем OSPF-сети. Аналогичный объект *Router Process* необходимо определить на каждом межсетевом экране OSPF-сети.

Основные параметры

Name	Определенное символьное имя автономной системы OSPF.
Router ID	Определенный IP-адрес, который используется для идентификации маршрутизатора в автономной системе. Если Router ID не указан, то межсетевой экран вычисляет ID, принимая за основу максимальный IP-адрес интерфейса, входящего в автономную систему OSPF.
Private Router ID	Применяется в HA-кластере, как ID конкретного межсетевого экрана, а не HA-кластера в целом.

Примечание

При запуске OSPF в HA-кластере управляющему и подчиненному маршрутизаторам требуется задать разные Private Router ID, кроме того должен быть задан общий идентификатор кластера.

Reference Bandwidth	Базовая полоса пропускания используется при вычислении стоимости (*cost*) маршрута, проходящего через определенный интерфейс. Если вместо метрики в качестве стоимости на OSPF-интерфейсе используется полоса пропускания (*bandwidth*), то стоимость вычисляются по следующей формуле: ***Cost = reference bandwidth/bandwidth***
RFC 1583 Compatibility	Эта опция используется в случаях, когда в окружении межсетевого экрана NetDefend присутствуют маршрутизаторы, поддерживающие только RFC 1583.

Отладка (Debug)

Отладчик протокола предоставляет инструмент выявления неисправностей, регистрируя определенную информацию OSPF-протокола в журнале.

- **Off** – Ничего не регистрируется.
- **Low** – Регистрируются все действия.
- **Medium** – Регистрируются те же действия, что и Low, но более детально.
- **High** – Самая детальная регистрация.

Примечание

*При использовании установки **High** межсетевой экран регистрирует большое количество информации, даже если он подключен к небольшой автономной системе. Может потребоваться изменение параметра **Log Send Per Sec Limit** в расширенных настройках.*

Аутентификация (Authentification)

OSPF поддерживает следующие методы аутентификации:

No (null) authentification	Для обмена информацией в OSPF-протоколе не требуется аутентификация
Passphrase	Для аутентификации при обмене в OSPF-протоколе требуется простой пароль.
MD5 Digest	MD5-аутентификация содержит идентификатор ключа (key ID) и 128-битный ключ. Определенный ключ используется для создания 128-бит MD5-хэша. Это не означает, что OSPF-пакеты шифруются. Если OSPF-трафик необходимо зашифровать, то его требуется отправлять через VPN. Например, используя IPSec. Более подробная информация об отправке OSPF-пакетов через IPSec приведена в *Разделе 4.5.5, "Установка OSPF"*.

Важно: Параметры аутентификации должны быть одинаковыми на всех маршрутизаторах.

Если для OSPF-аутентификации используется пароль или MD5, то этот же пароль или ключ аутентификации должен быть установлен на всех OSPF-маршрутизаторах автономной системы.

Другими словами, на всех межсетевых экранах NetDefend должен быть одинаковый метод аутентификации.

Расширенные настройки

Настройки времени

SPF Hold Time	Минимальное время (в секундах) между двумя SPF-вычислениями. По умолчанию – 10 секунд. Значение 0 означает отсутствие задержки.
SPF Delay Time	Промежуток времени, между получением данных об изменении топологии сети и началом SPF-вычисления. По умолчанию – 5 секунд. Значение 0 означает отсутствие задержки. Следует учитывать, что SPF-вычисления могут отнимать ресурсы CPU, их не следует часто запускать в больших сетях.
LSA Group Pacing	Интервал времени (в секундах), в течение которого OSPF LSA собираются в группу и обновляются. Одновременная обработка сгруппированных LSA эффективнее, чем каждого LSA в отдельности.
Routes Hold Time	Таймаут (в секундах), в течение которого таблица маршрутизации не будет изменяться после реконфигурации OSPF-записей или активации механизма HA.

Настройки памяти

Memory Max Usage	Максимальный объем (в килобайтах) оперативной памяти, который разрешено использовать автономной системе OSPF, если параметр не задан, то используется 1 % от объема установленной памяти. Величина 0 означает, что автономной системе OSPF разрешено

использовать всю доступную оперативную память межсетевого экрана.

4.5.3.2. Объект OSPF Area

Автономная система разделена на меньшие части, называемые *областями* (*Area),* данный раздел объясняет, как настраиваются области. Область включает в себя OSPF-интерфейсы, соседние маршрутизаторы, агрегации (aggregates) и виртуальные каналы.

OSPF Area – потомок объекта *OSPF Router Process*, в одном объекте *Router Process* может быть определено несколько областей. В самых простых сценариях организации сети достаточно определить одну область. Как и *Router Process*, соответствующий объект *OSPF Area* должен быть определен на всех межсетевых экранах NetDefend OSPF-сети.

Основные параметры

Name	Имя OSPF-области.
ID	Идентификатор области. Если определено значение 0.0.0.0, то это магистральная область. Может быть определена только одна магистральная область, которая является центральной частью автономной системы. Информация о маршрутизации, которой обмениваются различные области, всегда передается через магистральную зону.
Is stub area	Данный параметр следует включать, когда область является тупиковой.
Become Default Router	Можно настроить межсетевой экран как маршрутизатор по умолчанию, с заданной метрикой для тупиковой области.

Фильтр импорта (Import Filter)

Данный фильтр используется для выбора информации, которая может быть импортирована в автономную систему OSPF из каких-либо внешних источников (например, основной таблицы маршрутизации или таблицы маршрутизации на основе правил) или внутри OSPF-области.

External	Определяются адреса сети, которые разрешено импортировать в OSPF-область от внешних устройств маршрутизации.
Interarea	Определяются адреса сети, которые разрешено импортировать от других маршрутизаторов внутри OSPF-области.

4.5.3.3. Объект OSPF Interface

В данном разделе описываются параметры настройки объекта *OSPF-интерфейс*. OSPF-интерфейс является потомком OSPF-области. В отличие от областей, OSPF-интерфейсы каждого межсетевого экрана NetDefend OSPF-сети отличаются друг от друга. Цель объекта *OSPF-интерфейс* – описать конкретный интерфейс, который будет частью OSPF-сети.

Примечание: В OSPF-интерфейсах могут использоваться разные типы интерфейсов.

Следует обратить внимание на то, что OSPF-интерфейс не всегда соответствует физическому интерфейсу. С OSPF-интерфейсом могут быть связаны другие типы

интерфейсов, например VLAN.

Примечание: В OSPF-интерфейсах могут использоваться разные типы интерфейсов.

Следует обратить внимание на то, что OSPF-интерфейс не всегда соответствует физическому интерфейсу. С OSPF-интерфейсом могут быть связаны другие типы интерфейсов, например VLAN.

Основные параметры

Interface — Определяет, какой интерфейс на межсетевом экране будет использоваться для данного OSPF-интерфейса.

Network — Определяет адрес сети для данного OSPF-интерфейса.

Interface Type — Тип интерфейса может быть:

- **Auto** – Межсетевой экран пытается автоматически определить тип интерфейса. Может использоваться для физических интерфейсов.
- **Broadcast** – широковещательный тип интерфейса, со стандартными для 2 уровня OSI широковещательными/многоадресными возможностями. Типичный пример широковещательной/многоадресной сети – обычный физический Ethernet-интерфейс.

  При использовании широковещания OSPF отправляет OSPF-пакеты *Hello* на IP-адрес многоадресной рассылки *224.0.0.5*. Все OSPF-маршрутизаторы в сети будут видеть эти пакеты. По этой причине для поиска «соседних маршрутизаторов» никаких настроек в объекте *OSPF Neighbor* не требуется.
- **Point-to-Point** – используется для прямых соединений между двумя маршрутизаторами (другими словами, двумя межсетевыми экранами). Типичный пример – VPN-туннель, который используется для передачи OSPF трафика между двумя межсетевыми экранами. Адрес второго маршрутизатора (соседа) настраивается путем создания объекта *OSPF Neighbor*.

  Более подробная информация о применении VPN-туннелей приведена в *Разделе 4.5.5, "Установка OSPF"*.
- **Point-to-Multipoint** – тип интерфейса Point-to-Multipoint является совокупностью сетей Point-to-Point, где используется несколько маршрутизаторов, у которых нет широковещательных/многоадресных возможностей 2 уровня модели OSI.

Metric — Определяет метрику для данного OSPF-интерфейса. Метрика отражает "стоимость", отправки пакетов через этот интерфейс. Данная мера стоимости обратно пропорциональна полосе пропускания интерфейса.

Bandwidth — Если метрика не указана, то вместо нее можно определить полосу пропускания. Если значение полосы пропускания известно, то его можно использовать вместо метрики.

Аутентификация (Authentification)

Обмен информацией в OSPF-протоколе может быть аутентифицирован при помощи пароля или криптографического MD5-хэширования.

Если включена опция **Use Default for Router Process**, то используется значения, указанные в свойствах объекта *Router Process*. Если данная опция не активна, то доступны следующие варианты:

- **No authentication**.
- **Passphrase**.
- **MD5 Digest**.

Расширенные настройки

Hello Interval	Определяет время (в секундах) между отправкой *Hello*-пакетов на интерфейс.
Router Dead Interval	Если по истечении данного интервала времени от соседнего маршрутизатора не получены *Hello*-пакеты, то предполагается, что маршрутизатор вышел из строя.
RXMT Interval	Время (в секундах) между повторными отправками LSA соседним маршрутизаторам на данном интерфейсе.
InfTrans Delay	Определяет предположительную задержку передачи для данного интерфейса. Эта величина показывает максимальное время, которое требуется для отправки LSA-пакета через маршрутизатор.
Wait Interval	Время (в секундах) между включением интерфейса и выборами DR и BDR. Данная величина должна быть выше, чем в Hello Interval.
Router Priority	Приоритет маршрутизатора, чем выше эта величина, тем больше шансов у маршрутизатора стать DR или BDR. Если эта величина равна 0, то маршрутизатор не может участвовать в выборах DR/BDR.

Примечание:

В HA-кластере приоритет маршрутизатора всегда равен 0 и он никогда не может использоваться как DR или BDR.

Иногда возникает необходимость добавить сеть в объект *OSPF Routing Process,* когда на интерфейсе, связанном с этой сетью, не запущен OSPF. Это можно сделать с помощью опции: **No OSPF router connected to this interface (“Passive”)**.

Этот путь является альтернативой использованию политик динамической маршрутизации для импорта статических маршрутов в *OSPF Routing Process*.

Если включена опция **Ignore received OSPF MTU restrictions**, то несоответствия размеров MTU на интерфейсах соседних маршрутизаторов будут игнорироваться.

4.5.3.4. Объект OSPF Neighbor

В некоторых ситуациях на межсетевом экране требуется явно определять соседний OSPF-маршрутизатор, например, когда маршрутизаторы связаны не через физические интерфейсы.

Наиболее часто такая ситуация возникает при использовании VPN-туннеля для соединения двух “соседей”, в этом случае требуется указать системе NetDefendOS то, что OSPF-соединение следует направлять через туннель. Более подробная информация об использовании VPN с IPSec-туннелями приведена в *Разделе 4.5.5, “Установка OSPF”*.

Объекты системы NetDefendOS *OSPF Neighbor* создаются в *OSPF Area*, каждый объект обладает

следующими свойствами:

Interface	Определяет OSPF-интерфейс, к которому подключен соседний маршрутизатор.
IP Address	IP-адрес соседнего маршрутизатора – IP-адрес интерфейса соседнего OSPF-маршрутизатора, соединенного с данным маршрутизатором. Для VPN-туннеля данный IP-адрес – адрес, к которому устанавливается туннель.
Metric	Определяет метрику маршрута к этому «соседу».

4.5.3.5. Объект OSPF Aggregate

OSPF-агрегирования используются для объединения группы маршрутов с общими адресами в одну запись в таблице маршрутизации. Если опция «*Отправка Анонсов*» (Advertise) активна, то агрегация позволяет уменьшить размер таблицы маршрутизации межсетевого экрана, если опция не активна, то сети будут скрытыми.
Объект системы NetDefendOS *OSPF Aggregate* создается в пределах *OSPF Area*, каждый объект обладает следующими свойствами:

Network	Сеть, состоящая из объединяемых маршрутизаторов.
Advertise	Показывает, будут ли отправляться анонсы данного объединения.

В большинстве случаев, при использовании простых конфигураций OSPF, объект *OSPF Aggregate* не требуется.

4.5.3.6. Объект OSPF VLink

Все области OSPF AS должны быть непосредственно соединены с магистральной зоной (область с ID *0*). Иногда такое соединение невозможно, в таких случаях для подключения к магистральной зоне через не магистральную применяются *виртуальные каналы* (*Virtual Link, VLink*).

Объект системы NetDefendOS *OSPF VLink* создается в пределах *OSPF Area*, каждый объект обладает следующими свойствами:

Основные параметры:

Name	Символьное имя виртуального канала.
Neighbor Router ID	Идентификатор маршрутизатора с другой стороны виртуального канала.

Аутентификация

Use Default For AS	Использует настраиваемое значение из настроек автономной системы.

Примечание: Соединение разделенной на несколько частей (распределенной) магистрали

Если магистральная область разделена на несколько частей, то для ее объединения используется виртуальный канал.

В большинстве случаев, при использовании простых конфигураций OSPF, объект *OSPF VLink* не требуется.

4.5.4 Правила динамической маршрутизации (Dynamic Routing Rule)

В данном разделе рассмотрены правила динамической маршрутизации, определяющие, какие маршруты могут быть экспортированы в автономную систему AS из локальных таблиц маршрутизации, а какие – могут быть импортированы в локальные таблицы маршрутизации из автономной системы.

4.5.4.1. Обзор

Заключительный шаг настройки OSPF – создание правил динамической маршрутизации

Заключительным шагом после создания OSPF-структуры всегда является создание *правил динамической маршрутизации* на каждом межсетевом экране NetDefend, которые позволяют добавлять в локальные таблицы маршрутизации информацию о маршрутизации, получаемую автономной системой OSPF от удаленных межсетевых экранов.

В данном разделе правила динамической маршрутизации рассматриваются в контексте OSPF, но они могут использоваться и в других случаях.

Причины использования правил динамической маршрутизации

В среде динамической маршрутизации важна возможность регулирования степени участия маршрутизаторов в маршрутизации трафика. Нельзя принимать всю или доверять всей получаемой информации о маршрутизации. Важно не опубликовывать часть своей базы данных маршрутизации для других маршрутизаторов.

По этой причине для контроля передаваемой информации о маршрутизации используются *правила динамической маршрутизации.*

Эти правила фильтруют статически настроенные и изученные OSPF маршруты в соответствии с такими параметрами, как источник происхождения маршрута, сеть назначения, метрика и т.п. С маршрутами, подпадающими под правила могут выполняться такие действия, как экспорт в одну из таблиц маршрутизации или в OSPF-процессы.

Использование с OSPF

В OSPF правила динамической маршрутизации используются для достижения следующих результатов:

- Разрешение импорта маршрутов из OSPF AS в локальную таблицу маршрутизации.
- Разрешение экспорта маршрутов из локальной таблицы маршрутизации в OSPF AS.
- Разрешение экспорта маршрутов из одной OSPF SA в другую.

Примечание

Последнее очень редко используется, за исключением случаев объединения нескольких асинхронных систем в очень больших сетях.

OSPF требуется, по крайней мере, правило импорта (Import Rule)

По умолчанию система NetDefendOS не импортирует и не экспортирует никакие маршруты. Поэтому для функционирования OSPF необходимо определить, по крайней мере, одно правило динамической маршрутизации – *правило импорта*.

Правило импорта определяет локальный объект *OSPF Router Process*, что позволяет импортировать

внешние маршруты, изученные OSPF AS в локальные таблицы маршрутизации.

Определение фильтра

Правила динамической маршрутизации позволяют определить фильтр, который определяет импортируемые маршруты, основываясь на сети назначения. В большинстве случаев, параметр **Or is within** определяется как *all-nets* и фильтр не применяется.

Когда используют правила экспорта (Export Rule)

Хотя правило импорта необходимо для импорта маршрутов из OSPF AS, для экспорта маршрутов предусмотрен другой механизм. Экспорт маршрутов к сетям, являющимся частью объекта OSPF-интерфейс, осуществляется автоматически.

Единственное исключение для маршрутов на интерфейсах, для которых определен шлюз, то есть если сеть назначения не связана напрямую с физическим интерфейсом и передача информации к сети назначения осуществляется через промежуточный маршрутизатор. Маршрут *all-nets*, используемый для доступа в Интернет через ISP, является примером такого маршрута.

В таких случаях для экспорта маршрута правило экспорта динамической маршрутизации должно быть явно определено.

Объекты правил динамической маршрутизации

Связь между объектами правил динамической маршрутизации в системе NetDefendOS проиллюстрирована ниже.

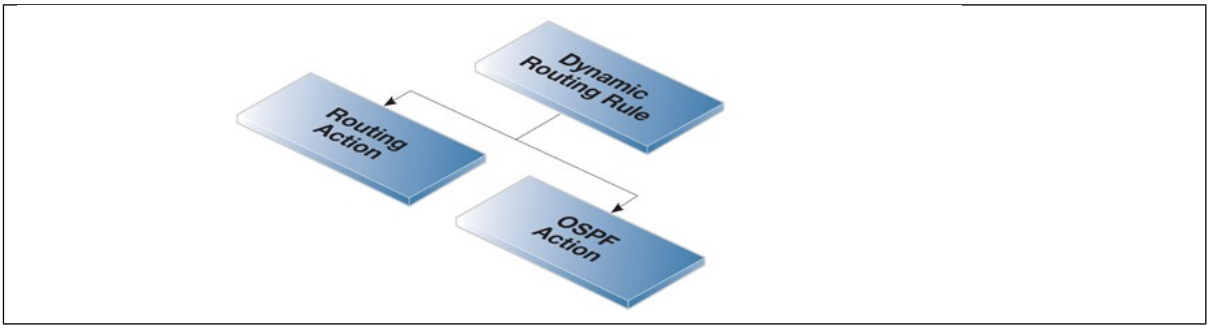


Рисунок 4.13. Объекты правил динамической маршрутизации

4.5.4.2. Объект *Dynamic Routing Rule* (Правила динамической маршрутизации)

Этот объект определяет правило динамической маршрутизации:

Основные параметры

Name	Определяет символьное имя правила.
From OSPF AS	Определяет, из какой OSPF AS (то есть из OSPF Router Process) должен быть импортирован маршрут в другую OSPF AS или в какую либо таблицу маршрутизации.
From Routing Table	Определяет, из какой таблицы маршрутизации должен быть импортирован маршрут в OSPF AS или скопирован в другую таблицу маршрутизации.
Destination Interface	Определяет, должно ли правило соответствовать определенному интерфейсу назначения.

Сеть назначения

Exactly Matches	Определяет, должна ли сеть назначения точно соответствовать определенной сети.
Or is within	Определяет, должна ли сеть находиться в пределах данной сети.

Другие параметры

Next Hop	Определяет адрес следующей пересылки (адрес следующего маршрутизатора) при срабатывании этого правила.
Metric	Определяет диапазон, в который должна попадать метрика маршрутизаторов.
Router ID	Определяет фильтрацию по идентификатору *Router ID*.
OSPF Route Type	Определяет фильтрацию по *типу OSPF-маршрутизатора*.
OSPF Tag	Определяет диапазон, допустимых значений для метки (tag) маршрутов.

4.5.4.3. Объект OSPF Action

Параметры, определяемые в OSPF-действии:

Основные параметры

Export to Process	Определяет, в какую OSPF AS должны импортироваться изменения маршрута
Forward	Если необходимо, то определяется IP, через который нужно маршрутизировать.
Tag	Определяет метку (tag) для данного маршрута, который может использоваться другими маршрутизаторами для фильтрации.
Route Type	Определяет тип внешнего маршрута, *1* – соответствует первому типу (*type1) OSPF-маршрута*. 2 – соответствует второму типу (*Type 2).* Если выбран второй тип, то стоимость внешней части маршрута будет определяющей при выборе маршрута.
OffsetMetric	Метрика импортируемого маршрута увеличивается на эту величину.
Limit Metric To	Ограничивает минимальное и максимальное значение метрики. Если значение метрики маршрута меньше, либо больше указанных границ, то ей присваивается соответствующее границе значение.

4.5.4.4. Объект Routing Action

Данный объект используются для управления и экспорта изменений в одну или несколько локальных таблиц маршрутизации.

Destination	Определяет, в какую таблицу маршрутизации автономной системы OSPF AS импортировать изменения маршрута.

Offset Metric	Метрика увеличивается на заданное значение.
Offset Metric Type 2	На заданное значение увеличивается метрика маршрута с типом *Type2*.
Limit Metric To	Ограничивает минимальное и максимальное значение метрики. Если значение метрики маршрута меньше, либо больше указанных границ, то ей присваивается соответствующее границе значение.
Static Route Override	Позволяет замещать статические маршруты.
Default Route Override	Позволяет замещать маршрут, заданный по умолчанию.

4.5.5. Настройка OSPF

Настройка OSPF может показаться сложной из-за большого количества параметров и их вариантов настройки. Но в большинстве случаев применяется простое OSPF-решение, использующее минимум объектов системы NetDefendOS с понятными настройками.

Ниже рассматривается сценарий с двумя межсетевыми экранами NetDefend, описанный ранее.

В данном примере объединены два межсетевых экрана NetDefend с OSPF, таким образом, что они могут совместно использовать маршруты из их таблиц маршрутизации. Оба межсетевых экрана будут находиться внутри определенной OSPF-области, которая является частью одной автономной системы OSPF AS. Более подробная информация об этих OSPF-концепциях рассмотрена в предыдущем разделе.

Ниже приведены шаги по установке в системе NetDefendOS на одном из межсетевых экранов.

1. ***Создание объекта OSPF Router***

В системе NetDefendOS создается объект *OSPF Router Process*, который будет представлять автономную систему OSPF AS (верхний уровень OSPF-иерархии). Объекту следует дать определенное имя. В поле Router ID можно ничего не указывать, в этом случае он будет назначен системой NetDefendOS автоматически.

2. ***Добавление объекта OSPF Area к объекту OSPF Router***

В пределах объекта *OSPF Router Process,* созданного на предыдущем этапе, следует добавить новый объект *OSPF Area*, задать его имя, задать 0.0.0.0 для идентификатора *Area ID*.

В автономной системе может быть несколько областей, но в большинстве случаев необходима только одна. ID 0.0.0.0 определяет эту область как магистральную, составляющую центральную часть автономной системы.

3. ***Добавление к OSPF Area объекта OSPF Interface***

В пределах *OSPF Area*, созданной на предыдущем этапе, следует добавить новый объект *OSPF Interface* для каждого физического интерфейса из этой области.

В объекте *OSPF Interface* требуется определить следующие параметры:

- **Interface** – физический интерфейс из данной OSPF-области.
- **Network** – сеть, связанная с интерфейсом из данной области.

  Этот параметр не обязателен, если он не задан, то будет использоваться сеть, назначенная для заданного физического интерфейса. Например, при использовании *lan*-интерфейса, сетью по умолчанию будет *lannet*.

- **Interface Type** – обычно используют значение для *Auto* и корректный тип интерфейса определяется автоматически.

- Расширенная опция **No OSPF routers connected to this interface** должна быть включена, если физический интерфейс не соединяется непосредственно с другим OSPF-маршрутизатором (другими словами, с межсетевым экраном NetDefend, работающим в качестве OSPF-маршрутизатора). Например, интерфейс может быть соединен только с клиентской сетью, в этом случае эта опция должна быть включена.

  Опция должна быть отключена, если физический интерфейс связан с другим межсетевым экраном, который настроен как OSPF-маршрутизатор. В данном примере, для физического интерфейса, соединенного с другим межсетевым экраном эта опция отключена.

4. ***Добавление правила динамической маршрутизации***

После этого для развертывания OSPF-сети следует определить правило динамической маршрутизации. Шаги по определению правил динамической маршрутизации:

I. Добавить объект *Dynamic Routing Policy Rule*. Данное правило должно быть правилом импорта, с активной опцией **From OSPF Process** и выбранным ранее определенным объектом *OSPF Router Process*. После этого появится возможность импорта всех маршрутов из автономной системы OSPF AS.

   Кроме того, в поле дополнительного фильтра **Or is within** необходимо указать параметр *all-nets*. Можно использовать более точный фильтр для сети назначения, в данном случае – это все сети.

II. В только что добавленном объекте *Dynamic Routing Policy Rule* следует создать объект *Routing Action* и добавить таблицу, которая будет получать информацию о маршрутизации от OSPF маршрутизации, в список выбранных таблиц *Selected*.

   Обычно это таблица маршрутизации *main*.

Нет необходимости в создании правила динамической маршрутизации для экспорта локальной таблицы маршрутизации в автономную систему, так как для объектов *OSPF Interface* экспорт осуществляется автоматически.

Исключение составляют ситуации, когда маршрут проходит через шлюз (другими словами, промежуточный маршрутизатор). В таких случаях правило экспорта должно быть явно определено. Наиболее часто такие ситуации возникают при прохождении **all-nets** через маршрутизатор интернет-провайдера для доступа в Интернет. Более подробная информация приведена ниже.

5. ***Добавление правила динамической маршрутизации для маршрута all-nets***

Иногда для маршрута *all-nets* необходимо дополнительно определить правило динамической маршрутизации, например, в случае соединения межсетевого экрана с ISP. Шаги по определению таких правил:

I. Добавить объект *Dynamic Routing Policy Rule* Данное правило должно быть правилом *экспорта*, с активной опцией **From Routing Table** и таблицей маршрутизации *main*, помещенной в список **Selected**.

   Кроме того, в поле дополнительного фильтра **Or is within** необходимо указать параметр *all-nets*.

II. В пределах только что добавленного объекта *Dynamic Routing Policy Rule* следует добавить объект *OSPF Action*. В настройках **Export to Process** данного объекта нужно выбрать объект *OSPF Router Process*, который представляет автономную систему OSPF AS.

6. ***Повторить все шаги для другого межсетевого экрана***

Повторить шаги 1 – 5 для второго межсетевого экрана NetDefend автономной OSPF-системы. Объекты *OSPF Router* и *OSPF Area* на этих межсетевых экранах будут одинаковыми. Объекты *OSPF Interface* будут отличаться в зависимости от интерфейсов и сетей, входящих в OSPF систему.
Если в одной OSPF-области будут находиться более двух межсетевых экранов, то остальные межсетевые экраны настраиваются аналогично.

Обмен информацией по OSPF-маршрутизации начинается автоматически

Когда новые настройки созданы и применены, OSPF запустится автоматически и начнет обмениваться информацией о маршрутизации. Поскольку OSPF динамическая и распределенная система, не имеет значения, в каком порядке была осуществлена настройка отдельных межсетевых экранов.

Когда установлено физическое соединение между интерфейсами двух различных межсетевых экранов и на этих интерфейсах настроены объекты *Router Process,* OSPF начинает обмен информацией о маршрутизации.

Проверка работоспособности OSPF

Теперь можно проверить работоспособность OSPF и то, как идет обмен информацией о маршрутизации.

Проверку можно осуществить, добавив запись в таблицу маршрутизации через CLI или Web-интерфейс. И в том и в другом случаях импортированные в таблицу маршрутизации маршруты OSPF будет буквой «O» слева от описания маршрута. Например, при использовании команды *routes* на экран будет выведена следующая запись:

```
gw-world:/> routes

Flags         Network             Iface       Gateway           Local IP    Metric
-----         -------------------- ----------- ------------------ ---------- ------
              192.168.1.0/24      lan                                       0
              172.16.0.0/16       wan                                       0
o             192.168.2.0/24      wan         172.16.2.1                    1
```

В данном случае маршрут для 192.168.2.0/24 был импортирован через OSPF и сеть может быть найдена на wan-интерфейсе со шлюзом 172.16.2.1. Шлюзом здесь является межсетевой экран NetDefend, через который передается трафик. Этот межсетевой экран может быть как соединен, так и не соединен с сетью назначения, но OSPF определил, что это оптимальный маршрут.

Передача OSPF-трафика через туннель

В некоторых случаях соединение между двумя межсетевыми экранами NetDefened, сконфигурированное с помощью объекта *OSPF-Router* может оказаться небезопасным, например, Интернет.

В таких ситуациях можно настроить VPN-туннель между двумя межсетевыми экранами и указать OSPF, чтобы протокол использовал этот туннель для обмена OSPF-информацией. Ниже рассмотрен пример, когда протокол IPSec использован для организации VPN-туннеля.

Для такой установки, кроме стандартных шагов настройки OSPF (которые приведены выше) следует выполнить следующие шаги:

1. Установка IPSec-туннеля

Сначала следует обычным способом установить IPSec-туннель между двумя межсетевыми экранами **A** и **B**. Более подробная информация по установке IPSec приведена в *Разделе 9.2, "Быстрая установка IPSec"*.

При настойке OSPF этот IPSec-туннель интерпретируется как любой другой интерфейс системы.

2. Выбор произвольной внутренней IP-сети

Для каждого межсетевого экрана требуется выбрать произвольную IP-сеть с внутренними IP-адресами. Например, для межсетевого экрана A – *192.168.55.0/24*.

Эта сеть используется только при настройке OSPF и никогда не будет связана с реальной физической сетью.

3. Определение OSPF-интерфейса для туннеля

В системе NetDefendOS необходимо определить объект *OSPF Interface*, в котором в качестве параметра **Interface** выступает IPSec-туннель. В параметре **Type** необходимо указать значение *point-to-point*, в параметре **Network** – выбрать сеть, в нашем примере *192.168.55.0/24*.

Объект *OSPF Interface* сообщает системе NetDefendOS о том, что любое относящееся к OSPF соединение, к узлам сети *192.168.55.0/24* должно быть отправлено через IPSec-туннель.

4. Определение объекта OSPF Neighbor

Далее следует явно указать OSPF, как найти соседний OSPF-маршрутизатор, для чего следует определить в системе NetDefendOS объект *OSPF Neighbor*. Данный объект состоит из объединения IPSec-туннеля (который рассматривается как интерфейс) и IP-адреса маршрутизатора с другой стороны туннеля.

Для IP-адреса маршрутизатора используется любой уникальный IP-адрес сети *192.168.55.0/24*. Например, *192.168.55.1*.

После установки OSPF будет обращаться к объекту *OSPF Neighbor* и пытаться посылать сообщения к IP-адресу *192.168.55.1*. Объект *OSPF Interface*, определенный на предыдущем шаге, сообщает системе NetDefendOS о том, что трафик, направленный OSPF к данному IP-адресу должен быть передан через IPSec-туннель.

5. Установка локального IP для конечной точки туннеля.

В заключение установки в параметрах межсетевого экрана **A** требуется изменить следующие параметры, отвечающие за установку IPSec-туннеля с межсетевым экраном **B**:

I. В свойствах IPSec-туннеля, в параметре **Local Network** необходимо установить значение *all-nets*. Такая настройка работает как фильтр, позволяющий пропускать в туннель весь трафик.

II. В свойствах IPSec, касающихся маршрутизации следует включить опцию **Specify address manually** (выбрать адрес вручную) и ввести IP-адрес, например, *192.168.55.1*. Эта настройка устанавливает IP конечной точки туннеля, в данном случае *192.168.55.1*, и любой OSPF-трафик будет отправляться на межсетевой экран **A** этим IP-адресом источника.

Результатом выполнения этих настроек будет являться маршрут к интерфейсу “core” для OSPF-трафика, получаемого от межсетевого экрана **A**. Другими словами, данный трафик предназначается непосредственно для системы NetDefendOS.

6. Повторение указанных шагов для другого межсетевого экрана

Указанные выше настройки позволяют OSPF-трафику протекать от межсетевого экрана **A** к межсетевому экрану **B**. Все шаги должны быть повторены для межсетевого экрана **B**, использующего тот же IPSec-туннель, единственное отличие – другая произвольная внутренняя IP-сеть для установки OSPF.

Совет: Через туннель может передаваться не только OSPF-трафик

Через VPN-туннель помимо OSPF-трафика могут передаваться и другие типы трафика. В данном случае нет требований для выделения туннеля для передачи только OSPF-трафика.

4.5.6. Пример OSPF

В данном разделе рассматриваются команды интерфейса для осуществления сценария описанного в *Разделе 4.5.5, "Настройки OSPF"*. Сценарий VPN IPSec не рассматривается.

Пример 4.7. Создание объекта OSPF Router Process

На первом межсетевом экране из OSPF AS создается объект *OSPF Router Process*.

Web-интерфейс

1. Перейти на вкладку **Routing > OSPF > Add > OSPF Routing Process**
2. Определить имя для объекта, например *as_0*
3. **OK**

Эти действия необходимо повторить для всех межсетевых экранов NetDefend, входящих в OSPF AS.

Пример 4.8. Добавление OSPF Area

Теперь к объекту *OSPF Router Process as_0* следует добавить объект *OSPF Area*, которая будет являться магистральной зоной с ID *0.0.0.0*.

Web-интерфейс

1. Перейти на вкладку **Routing > OSPF**
2. Выбрать процесс маршрутизации *as_0*
3. Выбрать **Add > OSPF Area**
4. Задать для зоны свойства:
   - Ввести соответствующее имя. Например, *area_0*
   - Определить **Area ID** как 0.0.0.0.
5. **OK**

Эти действия необходимо повторить для всех межсетевых экранов NetDefend, входящих в OSPF AS.

Пример 4.9. Добавление объекта OSPF Interface

Добавить для каждого физического интерфейса из OSPF-области *area_0* объект *OSPF Interface*.

Web-интерфейс

1. Перейти на вкладку **Routing > OSPF > as_0 > area_0 > OSPF Interfaces**
2. Выбрать **Add > OSPF Interface**
3. Выбрать **Interface**. Например, *lan*
4. **OK**

При выборе только значения параметра **Interface** значения в поле **Network** устанавливается сеть, связанная с этим интерфейсом. В данном случае *lannet*.

Эти действия необходимо повторить для всех интерфейсов входящих в OSPF-область, на данном межсетевом экране NetDefend, а затем для всех остальных межсетевых экранов, входящих в OSPF AS.

Пример 4.10. Импорт маршрутов из OSPF AS в таблицу маршрутизации main

Web-интерфейс

1. Прейти: **Routing > Dynamic Routing Rules > Add > Dynamic Routing Policy Rule**

2. Определить имя для правила, например *ImportOSPFRoutes*.

3. Выбрать **From OSPF Process**

4. Переместить *as0* из **Available** в **Selected**

5. Выбрать **all-nets** в опциях фильтра **…Or is within**

6. **OK**

Затем создать действие, которое и будет импортировать маршруты в таблицу маршрутизации. Выберите таблицу маршрутизации, в которую будут добавляться маршруты, в данном случае *main*.
Web-интерфейс

1. Прейти: **Routing > Dynamic Routing Rules**

2. Выбрать созданный объект *ImportOSPFRoutes.*

3. Прейти: **OSPF Routing Action > Add > DynamicRountingRuleAddRoute**

4. Переместить таблицу маршрутизации *main* из **Available** в **Selected**

5. **OK**

Пример 4.11. Экспорт маршрутов, заданных по умолчанию в автономную систему OSPF

В данном примере рассмотрен экспорт маршрута *all-nets*, заданного по умолчанию из таблицы маршрутизации *main* в OSPF AS с именем *as_0*. Этот экспорт должен быть явно определен, поскольку маршрут *all-nets* не экспортируется по умолчанию.

Во-первых, необходимо добавить новое *правило динамической маршрутизации*.

Web-интерфейс

1. Перейти: **Routing > Dynamic Routing Rules > Add > Dynamic routing policy rule**

2. Задать имя правила, например *ExportAllNets*

3. Выбрать опцию **From Routing Table**

4. Переместить таблицу маршрутизации *main* в список **Selected**

5. Выбрать **all-nets** в фильтре **…Or is within**

6. **OK**

Далее следует создать объект *OSPF Action*, который экспортирует отфильтрованную таблицу в выбранную OSPF AS.

Web-интерфейс

1. Перейти: **Routing > Dynamic Routing Rules**

2. Выбрать только что созданное правило *ExportAllNets*

3. Перейти: **OSPF Actions > Add > DynamicRoutingRuleExportOSPF**

4. Для **Export to process** выбрать *as_0*

5. **OK**

4.6. Многоадресная маршрутизация (Multicast Routing)

4.6.1. Обзор

Проблема многоадресной рассылки

Некоторым типам Интернет-взаимодействий, например конференции и видео, для отправки пакета нескольким получателям требуется отдельный хост. Поставленная цель может быть достигнута путем дублирования пакета к различным IP-адресам назначения или широковещательной рассылкой пакета через Интернет. Эти решения неэффективны, так как требуют много ресурсов для отправки или создают слишком много сетевого трафика. Приемлемое решение должно быть масштабируемо для большого числа получателей.

Многоадресная маршрутизация

Многоадресная маршрутизация решает указанную выше проблему непосредственно через сетевые маршрутизаторы, которые дублируют и пересылают пакеты по оптимальным маршрутам всем членам группы.

IETF-стандарты для многоадресной маршрутизации содержат следующее:

- Для многоадресного трафика зарезервированы IP-адреса класса D. Каждый IP-адрес с многоадресной рассылкой представляет некоторую группу получателей.
- Протокол управления группами Интернета (Internet Group Membership Protocol, IGMP) позволяет получателю сообщать сети о принадлежности к определенной группе многоадресной рассылки.
- Многоадресная рассылка, не зависящая от протокола (Protocol Independent Multicast, PIM) – группа протоколов маршрутизации, созданных для нахождения оптимального пути передачи пакетов многоадресной рассылки.

Основные принципы

Функционирование многоадресной маршрутизации построено на принципе присоединения получателей к группе многоадресной рассылки при помощи IGMP-протокола. После этого протокол маршрутизации PIM сможет дублировать и отправлять пакеты всем членам такой группы, создавая, таким образом, дерево распределения (*distribution tree*) потока пакетов. Вместо того, чтобы получать новую сетевую информацию PIM использует информацию маршрутизации от существующих протоколов, например OSPF, для выбора оптимального пути.

Передача по обратному пути (Reverse Path Forwarding)

Ключевым механизмом многоадресной маршрутизации является передача по обратному пути (*Reverse Path Forwarding*). При одноадресной передаче трафика маршрут связан только с получателем пакета. В случае многоадресной рассылки маршрутизатору требуется знать источник пакетов, так как пути пересылки пакета к клиенту, напрямую не связаны с источником пакетов. Данный подход применяется для предотвращения образования петель в дереве распределения.

Маршрутизация на корректный интерфейс

По умолчанию пакет многоадресной рассылки маршрутизируется на интерфейс **core** системы NetDefendOS (то есть непосредственно к NetDefendOS). Для того чтобы перенаправлять пакеты на требуемый интерфейс, в набор IP-правил добавляются правила *SAT Multiplex*. Данная операция демонстрируется на нижеописанных примерах.

Примечание: Функция многоадресной обработки (multicast handling) должна быть установлена в одно из двух состояний On или Auto.

Для корректного функционирования многоадресной рассылки на Ethernet-интерфейсе любого межсетевого экрана NetDefend, функция многоадресной обработки (multicast handling) должна быть установлена в одно из двух состояний On или Auto. Более подробная информация об Ethernet-интерфейсах приведена в Разделе 3.3.2, «Ethernet-интерфейсы».

4.6.2. Многоадресная рассылка (Multicast Forwarding) с использованием мультиплексных правил SAT Multiplex (SAT Multiplex Rules)

Правило SAT Multiplex используется для дублирования и передачи пакетов через более одного интерфейса. В системе NetDefendOS данный метод обеспечивает многоадресную рассылку, где пакет отправляется через несколько интерфейсов.

Следует обратить внимание, что это правило имеет более высокий приоритет, чем стандартные таблицы маршрутизации; пакеты, которые необходимо дублировать, должны быть направлены на интерфейс **core**.

Многоадресный IP-диапазон 224.0.0.0/4 всегда маршрутизируется к интерфейсу **core,** вручную добавлять этот маршрут в таблицу маршрутизации не требуется. На каждом выбранном отправляющем интерфейсе можно настроить SAT для преобразования адреса назначения. Поле **Interface** на вкладке **Interface/Net Tuple** может остаться пустым, если указано значение в поле **IPAddress**. В этом случае отправляющий интерфейс будет определен через поиск маршрута к указанному IP-адресу.

Правило SAT Multiplex может работать в двух режимах:

- Используя IGMP

  В соответствии с мультиплексным правилом, прежде чем пакеты многоадресной рассылки будут переданы через указанные интерфейсы к хостам, с которых должен прийти IGMP-запрос. По умолчанию система NetDefendOS работает в этом режиме.

- Не используя IGMP

  Трафик передается через определенный интерфейс без использования IGMP-запросов.

Примечание: Необходимо включить правило Allow или NAT

*Так как под мультиплексным правилом подразумевается правило **SAT**, то помимо него в должно быть определено одно из правил **Allow** или **NAT**.*

4.6.2.1. Многоадресная пересылка без преобразования адреса (Multicast Forwarding - No Address Translation)

В сценарии описывается настройка многоадресной пересылки с использованием IGMP. Источник *192.168.10.1* генерирует многоадресные потоки 239.192.10.0/24:1234, которые из исходного wan-интерфейса должны быть переданы через интерфейсы *if1*, *if2* и *if3*. Потоки должны передаваться только в случае отправления хостом запросов через IGMP-протокол.

В приведенном ниже примере рассмотрена часть конфигурации, относящаяся к многоадресной рассылке. Информация о настройке IGMP приведена в *Разделе 4.6.3.1, «Конфигурация IGMP-правил без преобразования адреса».*

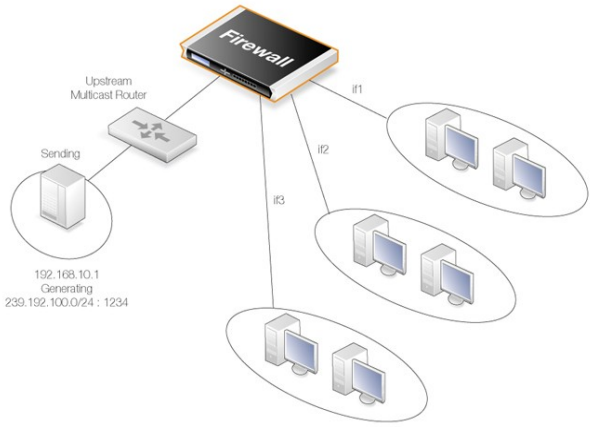


Рисунок 4.14. Многоадресная пересылка без преобразования адреса

Примечание: Кроме правил SAT Multiplex необходимо настраивать правила Allow.

*К соответствующему правилу **SAT Multiplex** необходимо добавлять соответствующее правило **Allow**.*

*В качестве соответствующего правила может использоваться правило **NAT** для преобразования адреса источника (рассмотрено ниже), правила **FwdFast** и **SAT** в данном случае применять нельзя.*

Пример 4.12. Пересылка трафика многоадресной рассылки с использованием SAT Multiplex-правил

В данном примере рассматривается создание Multiplex-правила, пересылающего трафик, адресованный многоадресным группам 239.192.10.0/24:1234 на интерфейсы if1, if2 и if3. У всех групп один отправитель 192.168.10.1, расположенный за wan-интерфейсом.

Данный трафик должен пересылаться на интерфейсы, если он был запрошен с помощью протокола IGMP клиентами, находящимися за этими интерфейсами. Для настройки пересылки трафика многоадресной рассылки требуется выполнить следующие шаги (IGMP настраивается отдельно):

Web-интерфейс:

A. Создание службы *multicast_service* для многоадресной рассылки:

1. Перейти на вкладку **Objects > Services > Add > TCP/UDP**

2. Ввести:

- **Name**: multicast_service
- **Type**: UDP
- **Destination**: 1234

B. Создание IP-правила:

1. Перейти на вкладку **Rules > IP Rules > Add > IP Rule**

2. Во вкладке **General** ввести:

- **Name**: название правила, например Multicast_Multiplex
- **Action**: Multiplex SAT
- **Service**: multicast_service

3. Во вкладке **Address Filter** ввести:

- **Source Interface:** wan

- **Source Network:** 192.168.10.1
- **Destination Interface:** core
- **Destination Network:** 239.192.10.0/24

4. Выделить таблицу **Multiplex SAT** и добавить выходные интерфейсы *if1, if1* и *if3.* Для каждого интерфейса поле **IP Address** следует оставить пустым, поскольку преобразование адресов назначения не требуется.

5. Установить флажок в поле **forwarded using IGMP**

6. **OK**

Создание мультиплексных правил через CLI

Для создания мультиплексных правил через CLI требуются некоторые дополнительные пояснения. Прежде всего, следует выбрать текущую категорию, для рассматриваемого примера – *IPRuleset*.

```
Gw-world:/> cc IPRuleset main
```

CLI-команда для создания мультиплексного правила:

```
gw-world:/main> add IPRule SourceNetwork=<srcnet> SourceInterface=<srcif>
DestinationInterface=<srcif> DestinationNetwork=<destnet> Action=MultiplexSAT Service=<service>
MultiplexArgument={outif1;ip1},{outif2;ip2},{outif3;ip3}...
```

Два значения *{outif;ip}* это комбинация выходного интерфейса и, если требуется трансляция адресов, IP- адреса.
Например, если требуется пересылка на интерфейсы *if2* и *if3* для группы многоадресной рассылки 239.192.100.50, то команда для создания правила будет следующей:

```
gw-world:/main> add IPRule SourceNetwork=<srcnet> SourceInterface=<if1>
DestinationInterface=core DestinationNetwork=239.192.100.50
Action=MultiplexSAT Service=<service>
MultiplexArgument={if2;},{if3;}
```

Поскольку многоадресная группа *239.192.100.50*, то интерфейс назначения будет **core**. Преобразование адреса не используется, но если оно требуется, например, для интерфейса *if2,* то последний параметр команды будет следующий:

```
MultiplexArgument = {if2; <new_ip_address>}, {if3;}
```

4.6.2.2. Многоадресная пересылка с преобразованием адреса (Multicast Forwarding - Address Translation Scenario)

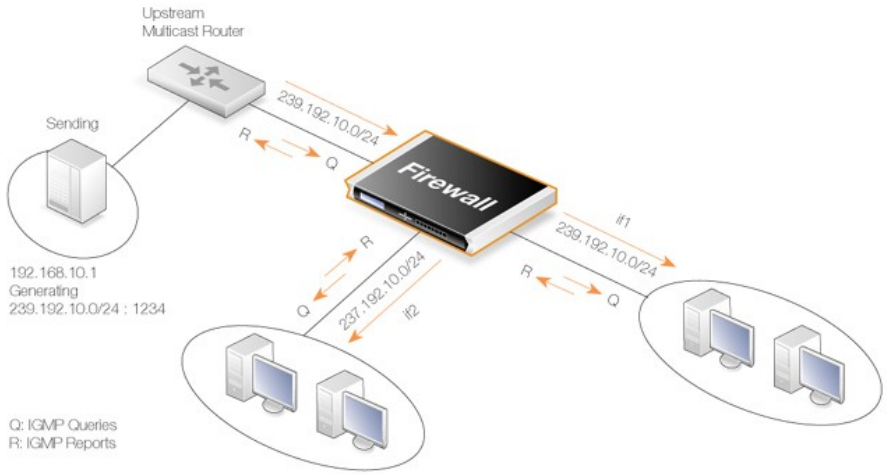


Рисунок 4.15 Многоадресная пересылка с преобразованием адресов

Данный сценарий основан на предыдущем, но в данном случае адрес группы многоадресной рассылки преобразуется. Когда многоадресный поток *239.192.10.0/24* передается через интерфейс *if2*, адрес группы должен преобразовываться в *237.192.10.0/24*.

Преобразование адреса не требуется при передаче через интерфейс *if1*.

Совет

*Как уже было отмечено, к соответствующему правилу **SAT Multiplex** необходимо добавить правило **Allow**.*

Пример 4.13. Многоадресная пересылка с преобразованием адреса

Должно быть настроено следующее SAT Multiplex-правило в соответствии с приведенным выше сценарием.

Web-интерфейс

А. Создание пользовательской службы *multicast_service* для многоадресной рассылки:

1. Перейти на вкладку **Objects > Services > Add > TCP/UDP**

2. Ввести:

- **Name**: multicast_service
- **Type**: UDP
- **Destination**: 1234

Б. Создание IP-правила:

1. Перейти на вкладку **Rules > IP Rules > Add > IP Rule**

2. На вкладке **General** ввести:

- **Name**: название правила, например Multicast_Multiplex
- **Action**: Multiplex SAT
- **Service**: multicast_service

3. В **Address Filter** ввести:

- **Source Interface:** wan
- **Source Network:** 192.168.10.1

- **Destination Interface:** core
- **Destination Network:** 239.192.10.0/24

4. Выбрать вкладку **Multiplex SAT.**

5. Добавить интерфейс **if1**, оставив поле **IPAddress** пустым

6. Добавить интерфейс **if2**, в поле **IPAdress** ввести 237.192.10.0

7. Установить флажок в поле **Forwarded using IGMP**

8. **OK**

Примечание: Для трансляции адреса источника, необходимо заменить Allow на NAT.

*Если требуется трансляции адреса источника, необходимо заменить правило **Allow**, расположенное после правила **SAT Multiplex** на правило **NAT**.*

4.6.3. Настройка IGMP

IGMP-сообщения между хостами и маршрутизаторами делятся на две категории:

- **IGMP-отчеты (IGMP Reports)**

  Сообщения отправляются от хостов к маршрутизатору, в том случае если хост хочет присоединиться к новой группе многоадресной рассылки или нужно изменить текущие подписки на группы.

- **IGMP-запрос (IGMP Queries)**

  Запросы – IGMP-сообщения, отправляемые от маршрутизатора к хостам для того, чтобы не остановить рассылку, которую какой либо хост хочет получать.

Обычно оба типа правил используются для нормального функционирования IGMP, но существуют два исключения:

1. Если источник многоадресной рассылки расположен в сети, непосредственно связанной с маршрутизатором, то правило для IGMP-запросов (query rule) не требуется.

2. Если на соседнем маршрутизаторе передача потока многоадресной рассылки на межсетевой экран NetDefend настроена статически, то IGMP-запросы также не требуются.

Система NetDefendOS поддерживает два режима работы IGMP:

- **Режим Snoop (Snoop Mode)**

- **Режим Proxy (Proxy Mode)**

Работа этих режимов проиллюстрирована на следующих рисунках:

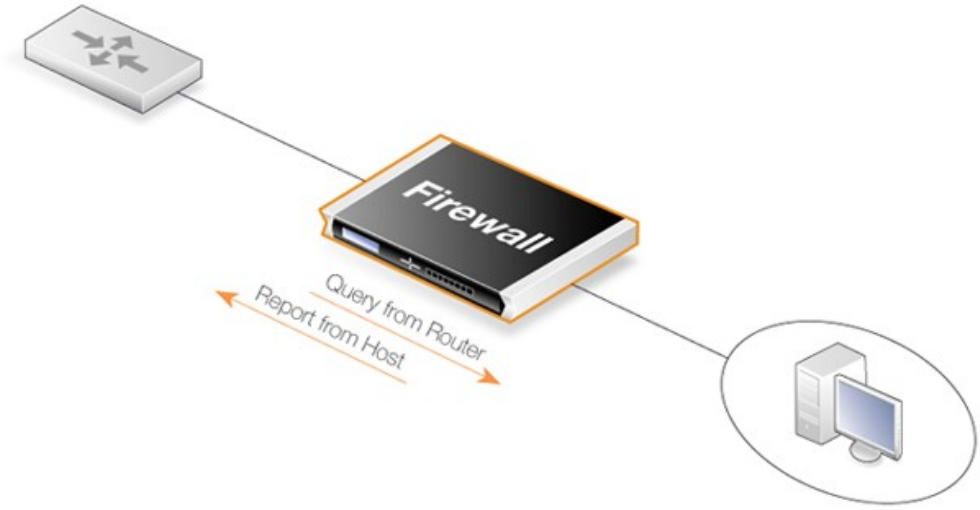


Рисунок 4.16. Работа в режиме Snoop

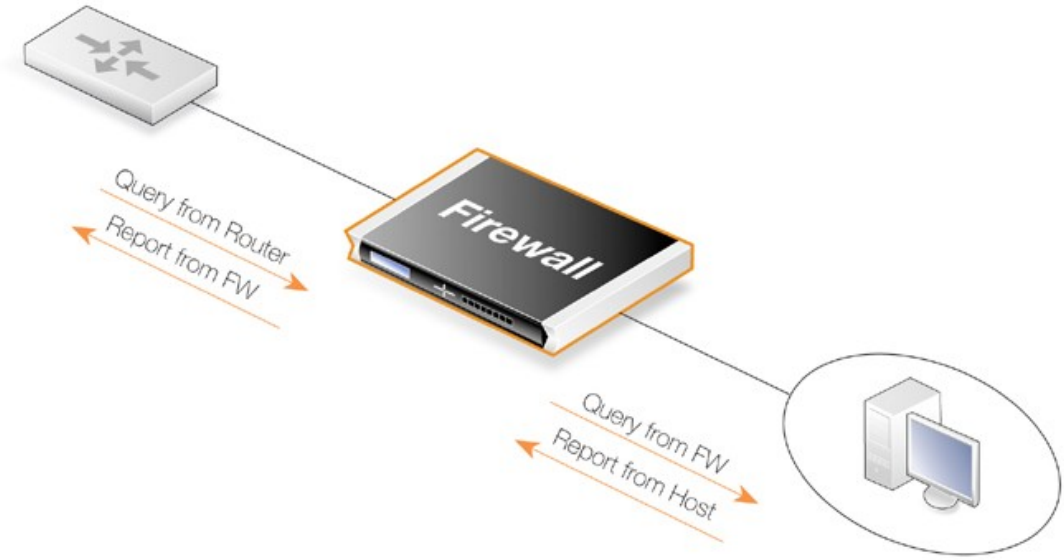


Рисунок 4.17. Работа в режиме Proxy

В режиме *Snoop* межсетевой экран NetDefend работает в прозрачном режиме между хостом и IGMP-маршрутизатором и не посылает никаких IGMP-запросов. Он только пересылает IGMP-запросы и IGMP-отчеты между другими хостами и маршрутизаторами.

В режиме *Proxy*, с точки зрения пользователей, межсетевой экран работает в качестве IGMP-маршрутизатора и активно отправляет запросы. С точки зрения вышестоящего маршрутизатора, межсетевой экран будет работать в качестве обычного хоста, осуществляя подписку на группы многоадресной рассылки от имени пользователей.

4.6.3.1. Настройка IGMP-правил без преобразования адресов

В данном примере показаны необходимые настройки IGMP соответствии с рассмотренным выше сценарием многоадресной рассылки без преобразования адреса. Маршрутизатору требуется работать в качестве хоста по отношению к вышестоящим маршрутизаторам, IGMP в этом случае следует настраивать в режиме *Proxy*.

Пример 4.14. IGMP без преобразования адресов

Данный пример требует наличия группы интерфейсов с именем *IfGrpClients*, включающую в себя интерфейсы *if1*, *if2* и *if3*. IP-адрес вышестоящего IGMP-маршрутизатора – хранится в объекте с именем *UpstreamRouterIP*.

Требуется два правила. Одно – правило отчета (report rule), которое позволяет клиентам, находящимся за интерфейсами *if1*, *if2* и *if3* присоединяться к группам многоадресной рассылки с IP-адресами из диапазона *239.192.10.0/24*. Второе правило – правило запроса (query rule), которое позволяет вышестоящему маршрутизатору запрашивать требуемые хостам за межсетевым экраном группы с многоадресной рассылкой.

Для создания этих правил необходимо:

Web-интерфейс

А. Создание первого IGMP-правила:

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:**Подходящее имя для правила, например *Reports*
- **Type:** Report
- **Action:** Proxy
- **Output:** wan (это ретранслирующий интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: IfGrpClients
- **Source Network**: if1net, if2net, if3net
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

Б. Создание второго IGMP-правила

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:** Подходящее имя для правила, например *Queries*
- **Type:** Query
- **Action:** Proxy
- **Output:** IfGrpClients (это ретранслирующий интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: wan
- **Source Network**: UpstreamRouterIp
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

4.6.3.2. Настройка IGMP-правил с преобразованием адресов

В следующем примере показана настройка IGMP правил для работы сценария многоадресной рассылки с преобразованием адреса, описанного в *разделе 4.6.2.2*. В данном случае необходимо два правила для IGMP-отчетов, по одному на каждый клиентский интерфейс. Для интерфейса *if1* не требуется преобразование адреса, а для интерфейса *if2* производится преобразование многоадресной группы к виду *237.192.10.0/24*. Помимо этого требуется два правила для IGMP-запросов, одно для преобразованного адреса и интерфейса *if2*, другое для исходного адреса и интерфейса *if1*.

Ниже приведены примеры для пар правил IGMP-отчетов и IGMP-запросов. IP-адрес вышестоящего IGMP-маршрутизатора – хранится в объекте с именем *UpstreamRouterIP*.

Пример 4.15. Настройка if1

Для создания правил report и query для *if1* без преобразования адресов требуется выполнить следующие шаги:

Web-интерфейс

А. Создание первого IGMP-правила:

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:** Определенное имя правила, например *Reports_if1*
- **Type:** Report
- **Action:** Proxy
- **Output:** wan (это ретранслирующий интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: if1
- **Source Network**: if1net
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

Б. Создание второго IGMP-правила

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:** Определенное имя правила, например *Queries_if1*
- **Type:** Query
- **Action:** Proxy
- **Output:** if1 (это ретранслирующий интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: wan
- **Source Network**: UpstreamRouterIp
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

Пример 4.16. Настройка if2 с преобразованием адресов группы многоадресной рассылки

Для создания правил report и query для *if2* с преобразованием адресов группы многоадресной рассылки требуется выполнить приведенные ниже шаги. Следует обратить внимание на то, что адреса группы преобразуются, поэтому IGMP-отчеты включают в себя преобразованные IP-адреса, а запросы содержат оригинальные IP-адреса.

Web-интерфейс

А. Создание первого IGMP-правила:

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:** Определенное имя правила, например *Reports_if2*
- **Type:** Report
- **Action:** Proxy
- **Output:** wan (это ретранслирующий интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: if2
- **Source Network**: if2net
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

Б. Создание второго IGMP-правила

1. Перейти на вкладку **Routing > IGMP > IGMP Rules > Add > IGMP Rule**

2. На вкладке **General** ввести:

- **Name:** Определенное имя правила, например *Queries_if2*
- **Type:** Query
- **Action:** Proxy
- **Output:** if2 (это промежуточный интерфейс)

3. В **Address Filter** ввести:

- **Source Interface**: wan
- **Source Network**: UpstreamRouterIp
- **Destination Interface**: core
- **Destination Network**: auto
- **Multicast Source**: 192.168.10.1
- **Multicast Destination**: 239.192.10.0/24

4. **OK**

Совет: Расширенные настройки IGMP

Часть расширенных настроек IGMP являются глобальными и применяются даже к тем интерфейсам, на которых явно не выполнялись настройки IGMP.

4.6.4. Расширенные настройки IGMP

Auto Add Multicast Core Route (Автоматическое добавление маршрута к core для многоадресных рассылок)

Данная настройка автоматически добавляет маршруты к core во все таблицы маршрутизации для многоадресного IP-диапазона *224.0.0.0/4*. Если опция отключена, то пакеты многоадресной рассылки могут передаваться с использованием маршрута по умолчанию.

По умолчанию: *Включена*

IGMP Before Rules (IGMP поверх правил)
Для IGMP-трафика применяются наборы IGMP-правил, стандартные наборы IP-правил при этом не используются.

По умолчанию: *Включена*

IGMP React To Own Queries (Реакция IGMP на собственные запросы)

Межсетевой экран должен всегда отвечать IGMP сообщениями участия в группе, даже если запрос отправлен самим межсетевым экраном. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *Отключена*

IGMP Lowest Compatible Version (Минимальная поддерживаемая версия IGMP)

IGMP-сообщения с версией ниже данной будут регистрироваться в журнале и игнорироваться. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *IGMPv3*

IGMP Router Version (Версия IGMP-маршрутизатора)

Версия протокола IGMP, которая будет использоваться как глобальная настройка на интерфейсах, где нет собственных настроек IGMP. Группа запрашивающих IGMP маршрутизаторов должна

использовать одну и ту же версию IGMP в пределах одной сети. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: IGMPv3

IGMP Last Member Query Interval (Интервал ожидания последнего участника IGMP-группы)

Максимальное время (в миллисекундах), в течение которого хост должен отправить ответ группе или группе и источнику на соответствующий запрос. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *5,000*

IGMP Max Total Requests (Максимальное общее количество IGMP-запросов)

Максимальное общее количество IGMP-сообщений, обрабатываемых в каждую секунду.

По умолчанию: *1000*

IGMP Max Interface Requests (Максимальное количество IGMP-запросов к интерфейсу)

Максимальное число запросов к интерфейсу в секунду. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *100*

IGMP Query Interval (Интервал запросов IGMP)

Интервал (в миллисекундах) между *общими запросами* (General Queries), отправляемыми устройствам, для обновления состояния IGMP-таблиц. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: 125,000

IGMP Query Response Interval (Интервал ответов IGMP)

Максимальное время (в миллисекундах), в течение которого хост должен отправить ответ на соответствующий запрос. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: 10,000

IGMP Robustness Variable (Переменная, влияющая на устойчивость к потерям пакетов IGMP)

Величина, позволяющая подстраиваться под ожидаемые потери IGMP пакетов в сети. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *2*

IGMP Startup Query Count

Межсетевой экран при запуске отправляет *общие запросы IGMP(General Queries)* в количестве равном значению, заданному в *Startup Query Count* с интервалом заданным в *IGMPStartupQueryInterval*. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *2*

IGMP Startup Query Interval

Интервал между о*бщими запросами* (в миллисекундах), отправляемыми на этапе запуска Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.

По умолчанию: *30,000*

IGMP Unsolicated Report Interval

Время (в миллисекундах) между повторениями начального сообщения хоста о присоединении к группе. Глобальная настройка, не перекрывающая IGMP-настройки конкретного интерфейса.
По умолчанию: *1,000*

4.7. Прозрачный режим (Transparent Mode)

4.7.1. Обзор

Использование прозрачного режима

Прозрачный режим системы NetDefendOS позволяет размещать межсетевой экран NetDefend в любой точке сети без изменения ее конфигураций и без уведомления пользователей о работе межсетевого экрана. В прозрачном режиме доступны все функции мониторинга и управления трафиком, проходящим через межсетевой экран. Система NetDefendOS может разрешать или запрещать доступ к различным службам (например, HTTP) и прохождение данных в определенных направлениях. До тех пор, пока пользователи обращаются к разрешенным сервисам, они могут не знать об установленном межсетевом экране NetDefend.

При использовании межсетевых экранов NetDefend, работающих в прозрачном режиме, значительно увеличивается безопасность передачи данных по сетям, а вмешательство в работу существующих пользователей и хостов - минимально.

Коммутируемые маршруты

Прозрачный режим позволяет вместо стандартных маршрутов определять в таблицах маршрутизации коммутируемые маршруты. Обычно в таких маршрутах указывается, что сеть *all-nets* находится за выбранным интерфейсом. При подключении к Ethernet-сети NetDefendOS, в отличие от некоммутируемых маршрутов, обменивается ARP-сообщениями для определения и хранения интерфейсов, за которыми находятся IP адреса хостов.

Иногда в коммутируемых маршрутах вместо *all-nets* можно указывать диапазон сети, это применяется в том случае, если сеть разделена между двумя интерфейсами и администратор не знает, за каким интерфейсом находятся конкретные пользователи.

Сценарий применения прозрачного режима

Ниже приведены примеры использования прозрачного режима:

- **Обеспечение безопасности между пользователями**

  Предприятиям может потребоваться ограничить доступ одних отделов к вычислительным ресурсам других отделов. Финансовому отделу может потребоваться доступ к ограниченным наборам служб (например, HTTP) коммерческого отдела, в то же время коммерческому отделу может потребоваться доступ к определенным сервисам финансового отдела. Устанавливая один межсетевой экран NetDefend между физическими сетями двух отделов, можно обеспечить прозрачный, но контролируемый доступ к ресурсам этих отделов.

- **Управление доступом в Интернет**

  В организации, где разрешено прохождение трафика между Интернетом и определенным диапазоном публичных IP-адресов внутренней сети, прозрачный режим позволяет определить, каким службам и в каком направлении разрешен доступ для этого диапазона IP-адресов. Например, в такой ситуации с данного диапазона IP-адресов можно разрешить исходящие соединения только для службы HTTP. Более подробная информация о применении межсетевого экрана в таких случаях приведена в *Разделе 4.7.2, «Предоставление доступа в Интернет».*

Сравнение с режимом маршрутизации (Routing Mode)

Межсетевой экран NetDefend может работать в двух режимах: режим маршрутизации, использующий некоммутируемые маршруты и прозрачный режим, использующий коммутируемые маршруты.

При использовании некоммутируемых маршрутов межсетевой экран NetDefend работает как

маршрутизатор и использует маршрутизацию на 3 уровне модели OSI. Если межсетевой экран размещен в сети впервые или если изменилась топология сети, то конфигурация маршрутизации должна быть проверена на совместимость таблицы маршрутизации с новой топологией. Новая настройка IP-параметров может потребоваться для уже существующих маршрутизаторов и защищенных серверов. Коммутируемые маршруты следует применять при необходимости всестороннего контроля над маршрутизацией.

При использовании коммутируемых маршрутов межсетевой экран NetDefend работает в прозрачном режиме как коммутатор 2 уровня модели OSI, в котором происходит проверка IP-пакетов и их передача к нужному интерфейсу без изменения информации об интерфейсах источника или назначения на IP или Ethernet-уровне. Это достигается за счет того, что система NetDefendOS сохраняет MAC-адреса хостов и позволяет физическим Ethernet-подсетям, расположенным по разные стороны межсетевого экрана, функционировать как единой логической IP-сети (См. *Приложение D, Краткий обзор уровней модели OSI*).

Преимущества прозрачного режима:

- Пользователь может перемещаться с одного интерфейса на другой без изменения своего IP-адреса (предполагается, что фиксированные IP-адреса закреплены за пользователями сети) и получать доступ к тем же сервисам, что и прежде (например, HTTP, FTP), не изменяя маршруты.

- Один и тот же диапазон IP-адресов может использоваться на нескольких интерфейсах.

Примечание: Объединение прозрачного режима и режима маршрутизации

Межсетевой экран NetDefend может работать сразу в двух режимах: прозрачном и режиме маршрутизации. Коммутируемые маршруты можно определить одновременно с некоммутируемыми, но на разных интерфейсах. Каждый интерфейс может работать в одном из двух режимов.

Также возможен гибридный вариант, когда используется трансляция сетевых адресов и часть трафика проходит в прозрачном режиме.

Как работает прозрачный режим

При использовании прозрачного режима система NetDefendOS позволяет ARP-транзакциям проходить через межсетевой экран NetDefend, и на основании этого ARP-трафика определяет связь между IP-адресами, физическими адресами и интерфейсами. NetDefendOS сохраняет информацию об этих адресах для дальнейшей передачи IP-пакетов. Обмен ARP-транзакций происходит прозрачно и обменивающиеся стороны не видят межсетевой экран NetDefend.

При установке нового соединения хост определяет физический адрес назначения путем отправки ARP-запроса. Система NetDefendOS перехватывает этот запрос, и передает ARP-запрос на все остальные интерфейсы, для которых созданы коммутируемые маршруты. Если в течение настраиваемого интервала времени, система NetDefendOS получает ARP-ответ от интерфейса назначения, то, используя сохраненную запись о состоянии ARP-транзакции, ARP-ответ передается интерфейсу, через который она была запрошена.

Во время ARP-транзакции, система NetDefendOS изучает информацию об адресе источника, информация о котором записывается в две таблицы: Content Addressable Memory (CAM, контекстно-адресуемая память) и КЭШ 3 уровня. В таблице CAM хранятся MAC-адреса, доступные для данного интерфейса, а в КЭШ 3 уровня заносится соответствие между IP-адресами и MAC-адресами. КЭШ 3 уровня применяется только для IP-трафика, записи КЭШа хранятся как запись об одном хосте в таблице маршрутизации.

Для каждого IP-пакета, проходящего через межсетевой экран NetDefend, осуществляется поиск маршрута. Если маршрут пакета соответствует коммутируемому маршруту или записи КЭШа 3 уровня в таблице маршрутизации, то система NetDefendOS знает, что должна обрабатывать пакет в прозрачном режиме. Если в маршруте доступны интерфейс назначения и MAC-адрес, то система NetDefendOS получает необходимую информацию для дальнейшей передачи пакета. Если маршрут

соответствует **коммутируемому маршруту** и информация об интерфейсе назначения отсутствует, межсетевой экран будет сам инициировать поиск адресата назначения в сети.

Поиск системой NetDefendOS осуществляется посредством отправки ARP и ICMP-запросов (ping), которая с точки зрения узла назначения, действует как отправитель оригинального IP-пакета на интерфейсах, указанных в **коммутируемом маршруте**. Если получен ARP-ответ, то система NetDefendOS обновляет CAM-таблицу и КЭШ 3 уровня и отправляет пакет к узлу назначения.

При переполнении CAM-таблицы или КЭШа 3 уровня происходит частичная автоматическая очистка таблиц и КЭШа. Используя механизм поиска на основе ARP и ICMP-запросов, NetDefendOS может повторно обнаружить узлы, записи о которых были стерты из КЭШа.

Включение функции Transparent Mode (Прозрачный режим)

Для активации в системе NetDefendOS прозрачного режима требуется выполнить следующие действия:

1. Следует собрать в одну группу интерфейсов все интерфейсы, для которых необходимо включить прозрачный режим. Если необходимо, чтобы хосты могли свободно переходить с одного интерфейса на другой, то для интерфейсов, входящих в группу должна быть включена опция **Security transport equivalent.**

2. На данном этапе в соответствующей таблице маршрутизации уже создан коммутируемый маршрут, связанный с данной группой интерфейсов. Любые некоммутируемые маршруты для интерфейсов этой группы должны быть удалены из таблицы маршрутизации.

   Для параметра **Network** коммутируемого маршрута следует определить значение *all-nets* или в качестве альтернативы указать значение сети или диапазона IP-адресов, которые будут прозрачно работать между интерфейсами (более подробное описание приведено ниже).

3. Создание соответствующих IP-правил в наборах IP-правил, позволяющих трафику проходить между интерфейсами, работающими в прозрачном режиме.

   Если на прохождение трафика в прозрачном режиме не нужно накладывать никаких ограничений, то следует указать только одно правило. Для обеспечения безопасности рекомендуется использовать более строгий набор IP-правил.

Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**	**Сервис (Service)**
Allow	any	all-nets	any	all-nets	all

Ограничение параметра *Network*

Система NetDefendOS анализирует ARP-трафик, непрерывно добавляет *single host routes (маршруты к отдельным хостам)* в таблицу маршрутизации и определяет интерфейс IP-адресов. Название говорит само за себя: создается отдельный маршрут для каждого IP-адреса. Рекомендуется задавать разные имена для маршрутов. Количество этих маршрутов может возрастать, соединяя все большее количество хостов.

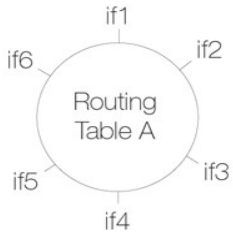
Основное преимущество указания конкретного диапазона адресов в параметре *Network* заключается в следующем: при задании определенной сети или диапазона IP-адресов вместо значения *all-nets* количество автоматически создаваемых маршрутов значительно уменьшается. Маршрут для каждого хоста будет создаваться, только если его адрес находится в пределах указанного диапазона IP-адресов или сети. Сокращение количества добавленных маршрутов уменьшит время поиска маршрутов.

Определение сети или диапазона адресов возможно только в том случае если администратору знакома топология сети.

Нескольких объединенных между собой коммутируемых маршрутов

Шаги по установки, приведенные выше, описывают размещение всех интерфейсов в одну группу интерфейсов, которая связана с единственным коммутируемым маршрутом. Если не объединять интерфейсы в группу, то для каждого из них следует задать коммутируемый маршрут. Конечный результат будет таким же. Все коммутируемые маршруты, созданные в одной таблице маршрутизации, будут объединены системой NetDefendOS. Независимо от того, как интерфейсы связаны с коммутируемыми маршрутами (в группе или каждый в отдельности) между ними будет существовать прозрачный обмен.

Например, если для интерфейсов с *if1* по *if6* присутствуют коммутируемые маршруты в таблице маршрутизации **A,** то в результате получим связи, которые проиллюстрированы ниже.



Если все интерфейсы связаны с одной и той же таблицей маршрутизации, то объединение коммутируемых маршрутов возможно только способом, показанным на рисунке.

Создание отдельных сетей, работающих в прозрачном режиме

Ниже приведены две таблицы маршрутизации **A** и **B**, коммутируемые маршруты для интерфейсов *if1, if2* и *if3*, описаны в таблице маршрутизации **A,** коммутируемые маршруты для интерфейсов *if4, if5* и *if6*, описаны в таблице маршрутизации **B**.

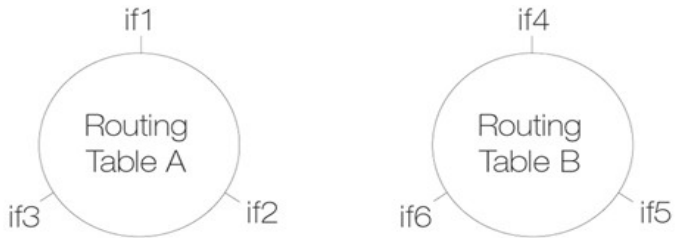


Диаграмма иллюстрирует, как коммутируемые маршруты одной таблицы маршрутизации полностью отделены от коммутируемых маршрутов второй таблицы маршрутизации. Другими словами, при использовании разных таблиц маршрутизации можно создавать две изолированных сети, которые работают в прозрачном режиме.

Таблицы маршрутизации выбираются на основе параметра *Routing Table Membership* для каждого интерфейса. Для отдельных сетей, работающих в прозрачном режиме, следует повторно установить параметры *Routing Table MemberShip.*

По умолчанию для всех интерфейсов значение параметра *Routing Table MemberShip* установлено как *все таблицы маршрутизации*. По умолчанию всегда существует одна главная таблица маршрутизации (**main**), и когда создана дополнительная таблица маршрутизации, в параметре *MemberShip* может быть указана созданная таблица маршрутизации.

Прозрачный режим при использовании VLAN

Описанная выше техника применения нескольких таблиц маршрутизации может быть использована при настройке прозрачного режима для всех хостов и пользователей в сети VLAN. Чтобы ограничить ARP-запросы к тому интерфейсу, на котором определена VLAN-сеть, для каждого идентификатора VLAN ID определяется отдельная таблица маршрутизации, в которой должны быть указаны коммутируемые маршруты соответствующие VLAN-интерфейсам.

Например, на двух физических интерфейсах *if1* и *if2* определена VLAN-сеть *vlan5*. Для каждого из этих интерфейсов определены коммутируемые маршруты, и они работают в прозрачном режиме. На

данных физических интерфейсах определены VLAN-интерфейсы *vlan5_if1* и *vlan5_if2* с одинаковым тегом VLAN ID.

Для работы VLAN-сети в прозрачном режиме следует создать таблицу маршрутизации с параметром *Ordering* равным *only*, которая будет содержать только 2 коммутируемых маршрута:

Network	**Interface**
all-nets	vlan5_if1
all-nets	vlan5_if2

Вместо отдельных записей в данной таблице маршрутизации можно использовать один маршрут для группы интерфейсов.

Для корректной работы в эту таблицу маршрутизации не следует включать другие некоммутируемые маршруты, так трафику, проходящему по этим маршрутам, будет добавляться некорректный тег VLAN ID.

На последнем этапе для данной таблицы маршрутизации определяется *PBR-правило*.

Включение прозрачного режима непосредственно на интерфейсах

Рекомендуемый способ включения прозрачного режима работы описан выше, но существует возможность включения прозрачного режима непосредственно на интерфейсе. В этом случае коммутируемые маршруты по умолчанию добавляются в таблицу маршрутизации для интерфейса, а некоммутируемые маршруты автоматически удаляются. Примеры использования данного метода рассмотрены ниже.

Высокая отказоустойчивость и прозрачный режим

Коммутируемые маршруты не могут быть использованы в режиме высокой отказоустойчивости, поэтому прозрачный режим не может использоваться в кластерах с высокой отказоустойчивостью (*High Availability Clusters, HA*).

При использовании режима высокой отказоустойчивости для того, чтобы разделить две сети, вместо коммутируемых маршрутов следует использовать *Proxy ARP*, более подробная информация о методе *Proxy ARP* приведена в *Разделе 4.2.6, «Proxy ARP»*. Основные недостатки метода *Proxy ARP*: если пользователь подключается к другому интерфейсу системы NetDefendOS, необходимо изменять его IP-адрес и для *Proxy ARP* необходимо настраивать вручную соответствующие сетевые маршруты.

Прозрачный режим и DHCP

В большинстве сценариев использования прозрачного режима используются заранее известные фиксированные IP-адреса пользователей и протокол DHCP (динамического распределения адресов) не используется. Основное преимущество прозрачного режима заключается в том, что независимо от местонахождения пользователя система NetDefendOS определяет его IP-адрес через ARP-запросы и направляет трафик по заданным маршрутам.

Тем не менее, DHCP-сервер можно использовать при установке прозрачного режима для распределения IP-адресов пользователей. При Интернет-соединении распределять публичные IP-адреса может DHCP-сервер провайдера. В этом случае система NetDefendOS **ДОЛЖНА** быть настроена как пересылатель *DHCP запросов (DHCP Relayer)*, передающий DHCP-трафик между пользователями и DHCP-сервером.

4.7.2. Настройка доступа в Интернет

Один из наиболее часто задаваемых вопросов при установке прозрачного режима: как правильно настроить доступ к Интернету? Ниже проиллюстрирован типичный сценарий получения доступа к Интернету пользователей IP-сети *lannet* через шлюз Интернет-провайдера с адресом *gw_ip*.

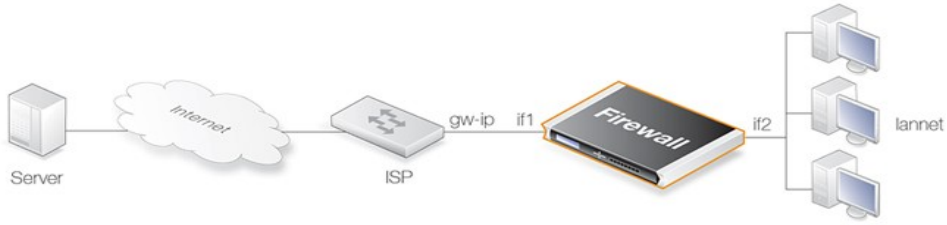


Рисунок 4.18 Доступ в Интернет при непрозрачном режиме работы

Некоммутируемые маршруты для доступа в Интернет приведены ниже:

Тип маршрута (Route type)	**Интерфейс (Interface)**	**Сеть назначения (Destination)**	**Шлюз (Gateway)**
Non-switch	If1	all-nets	gw-ip

На следующем рисунке рассматривается, как настроить соединение между Ethernet-сетью, где расположен шлюз провайдера (*pn1*) и внутренней физической Ethernet-сетью (*pn2*) с использованием коммутируемых маршрутов (межсетевой экран NetDefend работает в прозрачном режиме). Обе Ethernet сети рассматриваются как одна логическая IP-сеть в прозрачном режиме с общим диапазоном адресов (192.168.10.0/24).

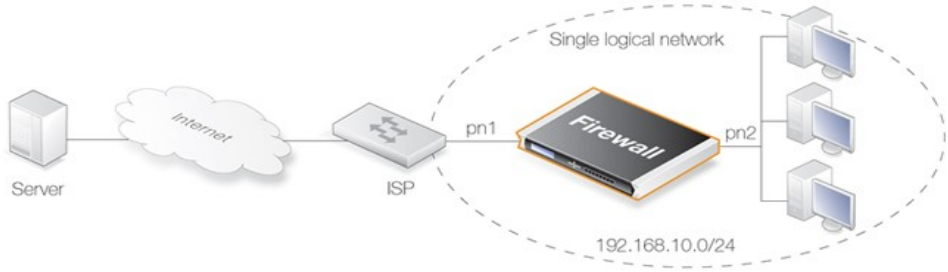


Рисунок 4.19 Доступ в Интернет в прозрачном режиме работы

В этом случае все «стандартные» некоммутируемые маршруты к *all-nets* из таблицы маршрутизации должны быть заменены коммутируемыми маршрутами *all-nets* (невыполнение этого действия – наиболее распространенная ошибка в процессе установки). Коммутируемые маршруты пропускают трафик локальных пользователей Ethernet-сети *pn2* к шлюзу провайдера.

На локальных компьютерах следует указать в настройках Интернет-шлюза адрес шлюза провайдера. В непрозрачном режиме в качестве адреса Интернет-шлюза указывался IP-адрес межсетевого экрана NetDefend, в прозрачном режиме работы шлюз провайдера и пользователи находится в одной логической IP-сети, поэтому в настройках Интернет-шлюза указывается *gw_ip*.

Системе NetDefendOS так же может требоваться Доступ в Интернет

Для работы таких механизмов как DNS-запросы (DNS lookup), фильтрация Web содержимого (Web Content Filtering) или обновление антивируса и IDP, системе NetDefendOS необходим доступ в Интернет. Чтобы получить такой доступ для каждого IP-адреса интерфейса, подключенного к Интернет-провайдеру, в таблице маршрутизации следует указать индивидуальные «стандартные» некоммутируемые маршруты со шлюзом соответствующим IP-адресу шлюза провайдера. Если системе NetDefendOS для работы требуются IP-адреса *85.12.184.39* и *194.142.215.15*, то таблица маршрутизации для рассмотренного выше примера будет выглядеть следующим образом:

Тип маршрута (Route type)	**Интерфейс (Interface)**	**Сеть назначения (Destination)**	**Шлюз (Gateway)**
Switch	if1	all-nets	
Switch	if2	all-nets	
Non-switch	if1	85.12.184.39	gw-ip
Non-switch	if1	194.142.215.15	gw-ip

К набору IP-правил следует добавить соответствующие правила, позволяющие получать доступ в Интернет через межсетевой экран NetDefend.

Объединение IP-адресов в группы

Вместо того чтобы работать с набором отдельных IP-адресов, часто удобно объединить эти адреса в группу и использовать имя этой группы при создании маршрута. В рассмотренном выше примере IP-адреса *85.12.184.39* и *194.142.215.15* можно объединить в отдельную группу.

Применение NAT

Если межсетевой экран NetDefend функционирует в прозрачном режиме, то есть ведет себя как коммутатор 2 уровня, то трансляция сетевых адресов (NAT) должна быть запрещена, так как она выполняется на более высоком уровне модели OSI.

Следствием этого является то, что для доступа пользователей в Интернет они должны использовать публичные IP-адреса.

Если необходимо использовать NAT, например для того, чтобы скрыть схему внутренней IP-адресации сети, то его можно реализовать на другом устройстве, например другом межсетевом экране, расположив его на границе собственной сети *192.168.10.0/24* и Интернета. В этом случае внутренние IP-адреса могут использоваться пользователями Ethernet-сети *pn2*.

4.7.3 Примеры использования прозрачного режима

Сценарий 1

Межсетевой экран в прозрачном режиме устанавливается между маршрутизатором, через который осуществляется доступ в Интернет и внутренней сетью. Маршрутизатор в данном случае используется для Интернет-соединения через один публичный IP-адрес. Внутренняя сеть, расположенная за NAT межсетевого экрана, использует пространство адресов *10.0.0.0/24*. Пользователям из внутренней сети разрешен доступ в Интернет через HTTP-протокол.

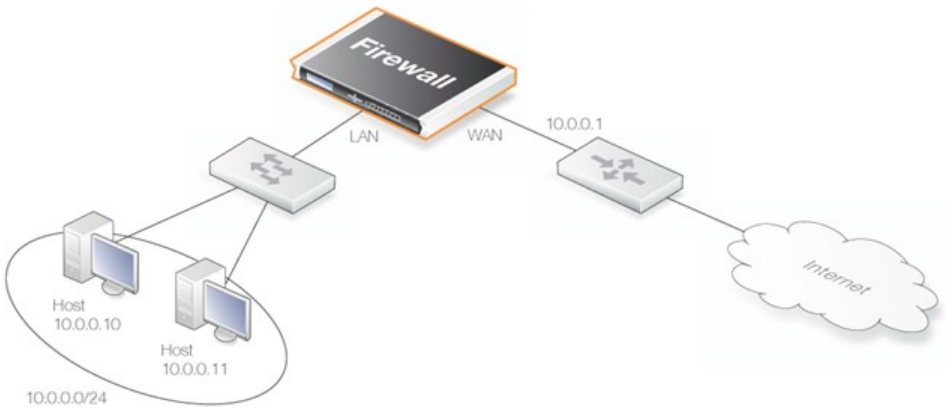


Рисунок 4.20 1 Сценарий прозрачного режима

Пример 4.17. Настройка прозрачного режима для сценария 1

Web-интерфейс

Настройка интерфейсов:

1. Перейти на вкладку **Interfaces > Ethernet > Edit (wan)**

2. Ввести:

- **IP Address**: 10.0.0.1
- **Network**: 10.0.0.0/24
- **Default Gateway**: 10.0.0.1
- **Transparent Mode**: Enable

3. **OK**

4. Перейти на вкладку **Interfaces > Ethernet > Edit (lan)**

5. Ввести:

- **IP Address**: 10.0.0.2
- **Network**: 10.0.0.0/24
- **Transparent Mode**: Enable

6. OK

Настройка правил:

1. Перейти на вкладку **Rules > IP Rules > Add > IPRule**

2. Ввести:

- **Name**: HTTPAllow
- **Action**: Allow
- **Service**: http
- **Source Interface**: lan
- **Destination Interface**: any
- **Source Network**: 10.0.0.0/24
- **Destination Network**: all-nets (0.0.0.0/0)

3. **OK**

Сценарий 2

В данном сценарии межсетевой экран NetDefend в прозрачном режиме отделяет сервера от остальных узлов для внутренней сети, за счет их подключения к разным интерфейсам.

Все хосты, подключенные к LAN и DMZ (lan-интерфейс и dmz-интерфейс) получают адреса из адресного пространства *10.1.0.0/16*. Поскольку в данном случае используется прозрачный режим, то для серверов может использоваться любой IP-адрес и при этом не нужно уведомлять хосты о том, к какому интерфейсу подключен требуемый ресурс. Хосты внутренней сети могут связываться с HTTP-сервером на DMZ-интерфейсе, который, в свою очередь, доступен из Интернет. Обмен данными через межсетевой экран NetDefend между DMZ и LAN прозрачен, но трафик контролируется набором IP-правил.

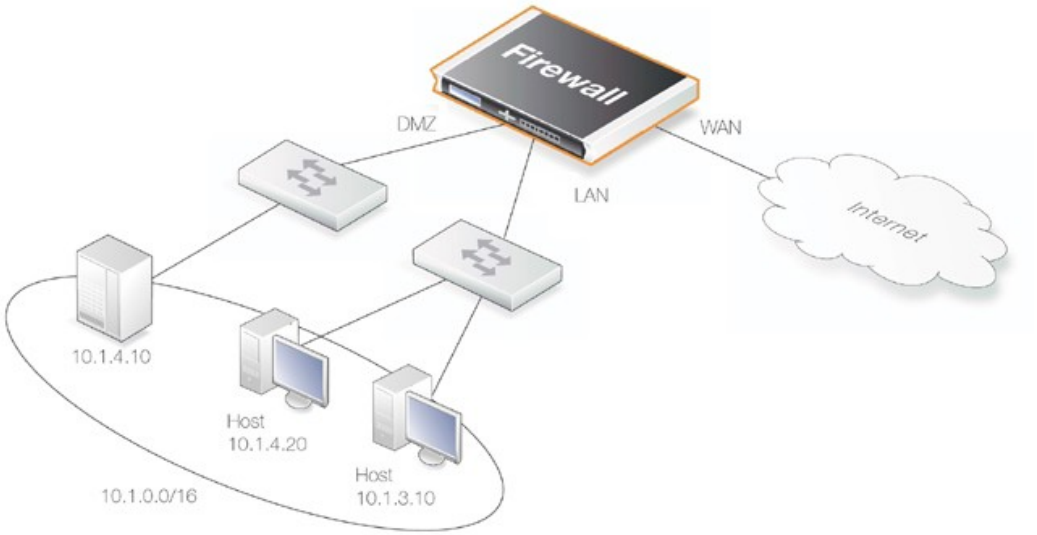


Рисунок 4.21 2 сценарий прозрачного режима

Пример 4.18. Настройка прозрачного режима для сценария 2

Настройка коммутируемого маршрута через LAN и DMZ-интерфейсы для диапазона 10.1.0.0/16 (предполагается, что WAN-интерфейс уже настроен)

Web-интерфейс

Настройка интерфейсов:

1. Перейти на вкладку **Interfaces > Ethernet > Edit (lan)**

2. Ввести:

- **IP Address**: 10.1.0.1
- **Network**: 10.1.0.0/16
- **Transparent Mode**: Disable
- **Add route for interface network**: Disable

3. **OK**

4. Перейти на вкладку **Interfaces > Ethernet > Edit (dmz)**

5. Ввести:

- **IP Address**: 10.1.0.2
- **Network:** 10.1.0.0/16
- **Transparent Mode**: Disable
- **Add route for interface network**: Disable

6. **OK**

Настройки группы интерфейсов:

1. Перейти на вкладку **Interfaces > Interface Groups > Add > InterfaceGroup**

2. Ввести:

- **Name**: TransparentGroup
- **Security/Transport Equivalent**: Disable

- **Interfaces**: Выбрать lan и dmz

3. **OK**

Настройки маршрутизации:

1. Перейти на вкладку **Routing > Main Routing Table > Add > SwitchRoute**

2. Ввести:

- **Switched Interfaces**: TransparentGroup
- **Network**: 10.1.0.0/16
- **Metric**: 0

3. **OK**

Настройки правил:

1. Перейти на вкладку **Rules > IP Rules > Add > IPRule**

2. Ввести:

- **Name**: HTTP-LAN-to-DMZ
- **Action**: Allow
- **Service**: http
- **Source Interface**: lan
- **Destination Interface**: dmz
- **Source Network**: 10.1.0.0/16
- **Destination Network**: 10.1.4.10

3. **OK**

4. Перейти на вкладку **Rules > IP Rules > Add > IPRule**

5. Ввести:

- **Name**: HTTP-WAN-to-DMZ
- **Action**: SAT
- **Service**: http
- **Source Interface**: wan
- **Destination Interface**: dmz
- **Source Network**: all-nets
- **Destination Network**: wan_ip
- **Translate**: Select Destination IP
- **New IP Address**: 10.1.4.10

6. **OK**

7. Перейти на вкладку **Rules > IP Rules > Add > IPRule**

8. Ввести:

- **Name**: HTTP-WAN-to-DMZ
- **Action**: Allow

- **Service**: http
- **Source Interface**: wan
- **Destination Interface**: dmz
- **Source Network**: all-nets
- **Destination Network**: wan_ip

9. **OK**

4.7.4. Поддержка Spanning Tree BPDU

Система NetDefendOS поддерживает пересылку *BPDU-фреймов* (*Bridge Protocol Data Unit*), через межсетевой экран NetDefend. Используя протокол STP (Spanning Tree Protocol) BPDU-фреймы передают сообщения между коммутаторами 2 уровня в сети. STP позволяет коммутаторам «понимать» топологию сети, препятствуя возникновению петель при коммутации пакетов.

На рисунке, представленном ниже, проиллюстрирована следующая ситуация: BPDU-сообщения появятся только в том случае, если администратор включит функцию управления STP-протоколом на коммутаторе. Между подсетями установлен межсетевой экран, работающий в прозрачном режиме. Коммутаторы, расположенные по обе стороны межсетевого экрана, должны взаимодействовать между собой, для этого система NetDefendOS должна пересылать BPDU-сообщения для того, чтобы можно было избежать петель.

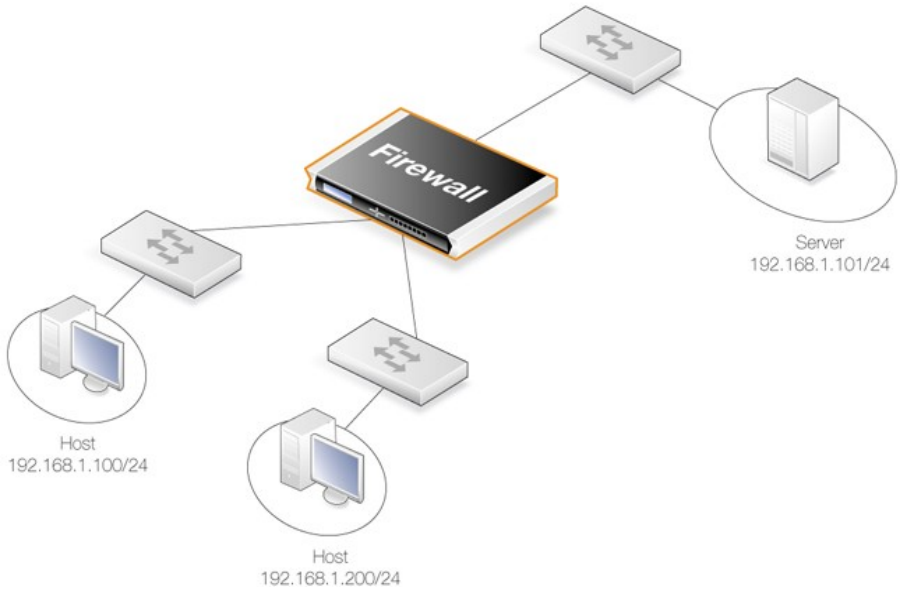


Рисунок 4.22. Пример сценария BPDU-передачи

Реализация опции BPDU-Relaying

При BPDU-передаче системой NetDefendOS будут пропускаться только STP-сообщения следующих типов:

- Normal Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

- Cisco proprietary PVST+ Protocol (Per VLAN Spanning Tree Plus).

Система NetDefendOS проверяет содержание BPDU-сообщений на принадлежность к одному из вышеперечисленных типов. Если соответствие не найдено, фрейм отбрасывается.

Включение/выключение BPDU-Relaying

По умолчанию опция **BPDU-Relaying** отключена, ее состояние можно изменить в расширенных настройках **Relay Spanning-tree BPDU.** Через эти настройки также можно настроить запись информации о BPDU-сообщениях в журнал. Когда данная опция включена, все входящие STP, RSTP и MSTP BPDU-сообщения передаются на все работающие в прозрачном режиме интерфейсы, кроме исходного в пределах одной таблицы маршрутизации.

4.7.5 Расширенные настройки прозрачного режима

CAM To L3 Cache Dest Learning

Эта опция включается, если межсетевой экран должен узнавать положение узлов назначения путем объединения информации об адресе назначения и информации, содержащейся в CAM-таблице.

По умолчанию: *Включена*

Decrement TTL

При включенной опции межсетевой экран уменьшает TTL пакета, каждый раз, когда пакет проходит через межсетевой экран, работающий в прозрачном режиме.

По умолчанию: *Отключена*

Dynamic CAM Size

Данная опция может отключаться, если необходимо вручную настроить размер CAM-таблицы. Обычно используют динамическое значение этой величины.

По умолчанию: *Динамический*

CAM Size

Если опция Dynamic CAM Size выключена, то можно вручную ограничить число записей в каждой CAM-таблице.

По умолчанию: *8192*

Dynamic L3C Size

Размер КЭШа 3 уровня изменяется динамически.

По умолчанию: *Включена*

L3 Cache Size

Данная опция может использоваться при ручной настройке размера КЭШа 3 уровня. Предпочтительнее включать опцию Dynamic L3C Size.

По умолчанию: *Динамический*

Transparency ATS Expire

Определяет время (в секундах) существования записи в таблице ARP-транзакций (ARP Transaction State, ATS) оставшегося без ответа ARP-запроса. Допустимые значения: 1-60 секунд.

По умолчанию: *3 секунды*

Transparency ATS Size

Определяет максимальное количество ARP-записей в таблице транзакций (ATS). Допустимые значения: 128-65536 записей.

По умолчанию: *4096*

Примечание: Скорость оптимальной обработки ATS

При использовании опций Transparency ATS Expire и Transparency ATS Size можно оптимизировать скорость обработки ATS под конкретные сетевые окружения.

Null Enet Sender

Определяет последовательность действий при получении пакета, значение MAC-адреса отправителя в Ethernet-заголовке которого равно нулю (00:00:00:00:00:00). Возможны следующие варианты:

- *Drop* – Отклонение пакетов
- *DropLog* – Отклонение пакетов с регистрацией события

По умолчанию: *DropLog*

Broadcast Enet Sender

Определяет последовательность действий при получении пакета, значение MAC-адреса отправителя в Ethernet-заголовке равно широковещательному Ethernet-адресу (FF:FF:FF:FF:FF:FF). Возможны следующие варианты:

- *Accept* – Принятие пакета
- *AcceptLog* – Принятие пакета с регистрацией события
- *Rewrite* – Перезапись MAC-адреса адресом передающего интерфейса
- *RewriteLog* – Перезапись MAC-адреса адресом передающего интерфейса с регистрацией события
- *Drop* – Отклонение пакета
- *DropLog* – Отклонение пакета с регистрацией события

По умолчанию: *DropLog*

Multicast Enet Sender

Определяет последовательность действий при получении пакета, значение MAC-адреса отправителя в Ethernet-заголовке равно Ethernet-адресу с многоадресной рассылкой. Возможны следующие варианты:

- *Accept* – Принятие пакета
- *AcceptLog* – Принятие пакета с регистрацией события
- *Rewrite* – Перезапись MAC-адреса адресом передающего интерфейса

- *RewriteLog* – Перезапись MAC-адреса адресом передающего интерфейса с регистрацией события

- *Drop* – Отклонение пакета

- *DropLog* – Отклонение пакета с регистрацией события

По умолчанию: *DropLog*

Relay Spanning-tree BPDUs

Если значение опции – **Ignore**, то все входящие STP, RSTP и MSTP BPDU-сообщения будут передаваться на все, работающие в прозрачном режиме интерфейсы, кроме исходного в пределах одной таблицы маршрутизации.
Возможны следующие варианты:

- *Ignore* – Пересылка пакетов без регистрации

- *Log* – Передача пакетов с регистрацией события

- *Drop* – Отклонение пакетов

- *DropLog* – Отклонение пакетов с регистрацией события

По умолчанию: *Drop*

Relay MPLS

Если значение опции – **Ignore**, то все входящие MPLS-пакеты пересылаются в прозрачном режиме. Возможны следующие варианты:

- *Ignore* – Пересылка пакетов без регистрации

- *Log* – Передача пакетов с регистрацией события

- *Drop* – Отклонение пакетов

- *DropLog* – Отклонение пакетов с регистрацией события

По умолчанию: *Drop*

Глава 5. Сервисы DHCP

В данной главе представлено описание DHCP-сервисов в операционной системе NetDefendOS.

- Обзор
- DHCP-серверы
- Использование функции DHCP Relay
- Пулы IP-адресов

5.1. Обзор

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это протокол, позволяющий сетевым администраторам автоматически назначать IP-адреса компьютерам сети.

Назначение IP-адресов

DHCP-сервер выполняет функции назначения IP-адресов DHCP-клиентам. Эти адреса выбираются из предопределенного пула IP-адресов, который управляется сервером DHCP. Когда DHCP-сервер получает запрос от DHCP-клиента, то сервер отсылает в ответ параметры конфигурации (например, IP-адрес, MAC-адрес, имя домена, период аренды IP-адреса) в одноадресном сообщении.

Период аренды адреса DHCP

В отличие от статического распределения адресов, при котором каждый клиент имеет постоянный IP-адрес, при динамическом распределении адресов каждый клиент получает адрес от DHCP-сервера на определенный период времени. В течение периода аренды клиенту разрешено сохранять выданный адрес, и ему гарантировано отсутствие коллизий с другими клиентами.

Истечение периода аренды

Перед тем, как период аренды IP-адреса истечет, клиенту необходимо ее пролонгировать, чтобы продолжать использовать назначенный ему IP-адрес. Клиент вправе в любое время отказаться от использования выданного ему IP-адреса, завершить аренду и освободить IP-адрес.

Период аренды устанавливается администратором в настройках DHCP-сервера.

5.2. DHCP-серверы

DHCP-серверы распределяют IP-адреса из определенного пула IP-адресов и управляют ими. В системе NetDefendOS DHCP-серверы не ограничены использованием одного диапазона IP-адресов, а могут обслуживать любой диапазон IP-адресов, который может быть определен как объект «IP-адрес» в системе NetDefendOS.

Множественные DHCP-серверы

В NetDefendOS администратор имеет возможность настроить один или несколько логических DHCP-серверов. Распределение запросов DHCP-клиентов разным DHCP-серверам зависит от двух параметров.

- **Интерфейс**

Каждый интерфейс в системе NetDefendOS может иметь, по крайней мере, один логический одиночный DHCP-сервер. Другими словами, NetDefendOS может предоставить DHCP-клиентам IP-адреса из разных диапазонов в зависимости от интерфейса клиента.

- **IP-адрес ретранслятора (Relayer IP)**

IP-адрес ретранслятора, передаваемый в IP-пакете, также используется для определения подходящего сервера. Значение по умолчанию *all-nets (все сети)* делает все IP-адреса допустимыми, и тогда выбор DHCP-сервера зависит только от интерфейса. Другие значения данного параметра описаны ниже.

Выбор сервера из списка

Список DHCP-серверов формируется по мере занесения в него новых строк, т.е. сервер, определенный последним, попадет в вершину списка. Когда в системе NetDefendOS выбирается DHCP-сервер для обслуживания запроса клиента, поиск по списку осуществляется сверху вниз. Выбор падает на верхний по списку сервер, соответствующий комбинации параметров (интерфейс и IP-адрес устройства, выполняющего функцию DHCP Relay). Если совпадений в списке не найдено, запрос игнорируется.

Порядок DHCP-серверов в списке можно изменить через один из интерфейсов пользователя.

Фильтрация по IP-адресу ретранслятора

Как указано выше, выбор DHCP-сервера из списка обусловлен совпадением обоих параметров – интерфейса и IP-адреса ретранслятора. Каждый DNS-сервер должен иметь определенное значение фильтра по IP-адресу ретранслятора. Возможны следующие варианты значений:

- **all-nets** (все сети)

all-nets (*0.0.0.0/0*) является значением по умолчанию. При установленном значении *all-nets* обслуживаются все DHCP-запросы, в независимости от того, поступили они от клиентов локальной сети или через DHCP Relayer.

- **Значение *0.0.0.0***

Фильтр *0.0.0.0* будет пропускать DHCP-запросы, приходящие только от клиентов локальной сети. Запросы, пересылаемые DHCP Relayer, будут игнорироваться.

- **Определенный IP-адрес**

Указывается IP-адрес DHCP-ретранслятора (DHCP Relayer), которому разрешено перенаправлять запросы. Запросы от локальных клиентов или других DHCP-ретрансляторов будут игнорироваться.

Опции DHCP-сервера

Для DHCP-сервера можно задать следующие параметры:

Основные параметры

Name (Имя)	Символьное имя сервера. Используется как ссылка на интерфейс или как ссылка в сообщениях для записи в Журнал событий.
Interface Filter (Фильтр по интерфейсу)	Интерфейс источника, на котором система NetDefendOS будет ожидать получения DHCP-запросов. Это может быть как один интерфейс, так и группа интерфейсов (Interface group).
IP Address Pool (Пул IP-адресов)	Диапазон IP-адресов (группа или сеть), который используется DHCP-сервером в качестве пула IP-адресов при их распределении.
Netmask (Маска подсети)	Маска подсети, которая будет рассылаться DHCP-

клиентам.

Необязательные параметры

Default GW (Основной шлюз)	Здесь определяется IP-адрес устройства, выполняющего функции основного шлюза, который передается клиенту (маршрутизатор, к которому подключается клиент)
Domain (Имя домена)	Имя домена, используемое DNS для определения IP-адреса. Например, *domain.com*.
Lease Time (Время аренды)	Время предоставленной DHCP-аренды в секундах. По истечении данного периода DHCP-клиент должен возобновить аренду.
Primary/Secondary DNS (Первичный/Вторичный DNS-серверы)	IP-адрес первичного и вторичного DNS-серверов.
Primary/Secondary NBNS/WINS (Первичный/Вторичный NBNS/WINS-серверы)	IP-адреса WINS-серверов среды Microsoft, которые используют NBNS-серверы для установления соответствий между IP-адресами и именами в NetBIOS.
Next Server (Последующий сервер)	Определяет IP-адрес сервера загрузки по сети. Обычно это TFTP-сервер.

Расширенные настройки DHCP-сервера

Ко всем DHCP-серверам применимы два следующих параметра расширенных настроек.

- **Auto Save Policy** (Автосохранение)

Сохранение базы данных арендованных IP-адресов на диск. Имеет следующие значения:

1. ***Never*** – Никогда не сохранять базу данных IP-адресов.

2. ***ReconfShut*** – Сохранять базу данных IP-адресов после изменения конфигурации или закрытии.

3. ***ReconfShutTimer*** – Сохранять базу данных IP-адресов после изменения конфигурации, закрытии и также через определенный период времени. Период времени между автоматическими сохранениями определяется параметром *Lease Store Interval*.

- **Lease Store Interval** (Интервал между автосохранениями)

Количество секунд между процедурами автосохранения базы данных арендованных IP-адресов на диск. Значение по умолчанию – 86400 секунд.

Пример 5.1. Настройка DHCP-сервера

В этом примере демонстрируется настройка DHCP-сервера с именем *DHCPServer1*, который распределяет IP-адреса из пула с именем *DHCPRange1* и управляет ими.

Подразумевается, что пул IP-адресов для DHCP-сервера уже создан.

CLI

```
gw-world:/> add DHCPServer DHCPServer1 Interface=lan
IPAddressPool=DHCPRange1 Netmask=255.255.255.0
```

Web-интерфейс

1. Зайдите **System > DHCP > DHCP Servers >Add > DHCPServer**

2. Затем введите:

• **Name:** DHCPServer1

• **Interface Filter:** lan

• **IP Address Pool:** DHCPRange1

• **Netmask:** 255.255.255.0

3. Нажмите **OK**

Пример 5.2. Проверка статуса DHCP-сервера

CLI

Чтобы видеть статус всех серверов:

```
gw-world:/> dhcpserver
```

Чтобы вывести список всех используемых IP-адресов:

```
gw-world:/> dhcpserver -show
```

Отображение таблицы сопоставления IP-адресов и MAC-адресов

Чтобы вывести таблицу сопоставления IP-адресов и MAC-адресов, являющуюся результатом распределения DHCP-аренды, используется следующая команда (в примере использования команды показан типичный вывод данных):

```
gw-world:/> dhcpserver -show -mappings
```

DHCP-таблица сопоставления IP-адресов и MAC-адресов:

```
Client IP       Client MAC              Mode
--------------- -----------------       -------------
10.4.13.240     00-1e-0b-a0-c6-5f       ACTIVE(STATIC)
10.4.13.241     00-0c-29-04-f8-3c       ACTIVE(STATIC)
10.4.13.242     00-1e-0b-aa-ae-11       ACTIVE(STATIC)
10.4.13.243     00-1c-c4-36-6c-c4       INACTIVE(STATIC)
10.4.13.244     00-00-00-00-02-14       INACTIVE(STATIC)
10.4.13.254     00-00-00-00-02-54       INACTIVE(STATIC)
10.4.13.1       00-12-79-3b-dd-45       ACTIVE
10.4.13.2       00-12-79-c4-06-e7       ACTIVE
10.4.13.3       *00-a0-f8-23-45-a3      ACTIVE
10.4.13.4       *00-0e-7f-4b-e2-29      ACTIVE
```

Знак сноски «*» перед MAC-адресом означает, что DHCP-сервер определяет клиента не по его MAC-адресу, а по идентификатору (*Client Identifier*), переданному клиентом.

Совет: Сохранение базы данных арендованных IP-адресов

База данных арендованных IP-адресов по умолчанию сохраняется системой NetDefendOS между перезагрузками. В разделе “Расширенные настройки DHCP-сервера” можно

установить необходимый интервал сохранения базы данных.

Дополнительные настройки сервера

DHCP-сервер с операционной системой NetDefendOS может иметь два дополнительных набора объектов, связанных с ним:

- Хосты со статическими IP-адресами (Static Hosts).
- Специальные опции (Custom Options).

На рисунке ниже показана связь между этими объектами.

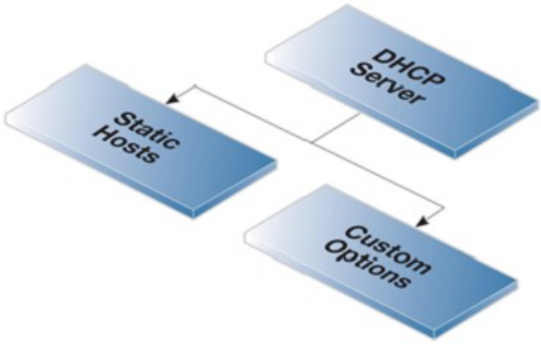


Рис. 5.1. Объекты DHCP-сервера

В следующих разделах данного руководства дополнительные настройки DHCP-сервера будут рассмотрены более детально.

5.2.1 Статические DHCP-хосты

При необходимости установления фиксированной связи между клиентом и определенным IP-адресом, система NetDefendOS позволяет это сделать с помощью назначения данного IP-адреса MAC-адресу клиента. Другими словами, позволяет создать хост со статическим IP-адресом.

Параметры хоста со статическим IP-адресом

Для одиночного DHCP-сервера можно создать много таких назначений и каждое будет иметь следующие параметры:

Host (хост)	IP-адрес, который будет выдан клиенту
MAC Address (MAC-адрес)	MAC-адрес клиента. Может использоваться как сам MAC-адрес, так и, в качестве альтернативы, идентификатор *Client Identified.*
Client Identified (Идентификатор клиента)	Для идентификации клиента может использоваться как его MAC-адрес, так и идентификатор, который клиент, в этом случае, отправляет в своем DHCP-запросе. В параметре *Client Identified* содержится значение данного идентификатора и его формат передачи (шестнадцатеричный или ASCII формат).

Пример 5.3. Назначение статического DHCP-хоста

В этом примере демонстрируется назначение соответствия IP-адреса *192.168.1.1* MAC-адресу *00-90-12-13-14-15.* Подразумевается, что DHCP-сервер с именем *DHCPServer1* уже определен.

CLI

1. Во-первых, измените категорию на *DHCPServer1*:

gw-world:/> **cc DHCPServer DHCPServer1**

2. Добавьте статическое DHCP-назначение:

gw-world:/> **add DHCPServerPoolStaticHost Host=192.168.1.1 MACAddress=00-90-12-13-14-15**

3. Можно просмотреть список всех установленных DHCP-назначений с их индексами:

gw-world:/> **show**

```
# Comments
- -------
+ 1 (none)
```

4. Отдельные статические DHCP-назначения можно просмотреть по их индексу:

```
gw-world:/> show DHCPServerPoolStaticHost 1

Property            Value
-----------         -----------------
Index:              1
Host:               192.168.1.1
MACAddress:         00-90-12-13-14-15
Comments:           (none)
```

5. В дальнейшем, статическое DHCP-назначение можно изменить с текущего IP-адреса на *192.168.1.12* при помощи следующей команды:

gw-world:/> **set DHCPServerPoolStaticHost 1 Host=192.168.1.12 MACAddress=00-90-12-13-14-15**

Web-интерфейс

1. Зайдите **System > DHCP > DHCP Servers > DHCPServer1 > Static Hosts > Add > Static Host Entry**

2. Затем введите:

• **Host:** 192.168.1.1

• **MAC:** 00-90-12-13-14-15

3. Нажмите **OK**

5.2.2 Специальные опции

Заполнение раздела специальных опций DHCP-сервера при его определении позволяет администратору в сообщениях, содержащих детали аренды, также отправлять дополнительную информацию для DHCP-клиентов.

В качестве примера могут служить те коммутаторы, которым требуется IP-адрес TFTP-сервера, для передачи дополнительной информации.

Параметры специальных опций

В разделе специальных опций могут быть определены следующие параметры:

Code (Код) Код, определяющий тип данных, пересылаемых клиенту. Существует значительный список возможных кодов.

Type (Тип) Описывает тип данных, которые будут отправлены. Например, если определен тип *String,* то в качестве данных будет отправлена символьная строка.

Data (Данные) Та информация, которая будет передана в сообщении, содержащем детали аренды. Это может быть одно значение или список значений, разделенных запятыми.

Содержание данных определено параметрами *Code* (Код) и *Type* (Тип). Например, если значение кода – *66* (имя TFTP-сервера), тогда *Type* может быть определен как *String,* и значением строки данных *Data* будет имя сайта, такое как *tftp.mycompany.com.*

Существует много специальных опций одиночного DHCP-сервера. Они описаны в стандарте:

RFC 2132 – DHCP Options and BOOTP Vendor *Extensions*

Коды вводятся в соответствии со значениями, определенными в RFC 2132. Данные, соответствующие определенному коду, первоначально определяются в системе NetDefendOS как *Type (Тип)* связанный с *Data (Данные).*

5.3. DHCP Relaying

Проблема DHCP

По протоколу DHCP компьютер-клиент, отправляет запросы DHCP-серверам, чтобы с помощью широковещательной рассылки определить их местоположение. Однако такие сообщения обычно распространяются только в локальных сетях. Это означает, что DHCP-сервер и клиент всегда должны находиться в одной и той же физической сети. Для сетевой топологии, подобной сети Интернет, это означает наличие в каждой сети своего DHCP-сервера. Эта проблема решается с помощью DHCP Relayer.

Решение проблемы с помощью DHCP Relayer

DHCP Relayer занимает место DHCP-сервера в локальной сети и выполняет роль связи между клиентом и удаленным DHCP-сервером. Он перехватывает запросы от клиентов и передает их DHCP-серверу. DHCP-сервер затем отвечает ретранслятору, который переадресовывает ответ обратно клиенту. Чтобы выполнять функции ретрансляции DHCP Relayer использует протокол TCP/IP *Bootstrap Protocol* (BOOTP). Поэтому DHCP Relayer иногда ассоциируют с агентом пересылки BOOTP (*BOOTP relay agent*).

IP-адрес источника ретранслирующего DHCP-трафик

Для интерфейса ретранслирующего DHCP-трафик в NetDefendOS возможно использование либо в качестве источника, на котором NetDefendOS будет ожидать переадресованный трафик, либо в качестве интерфейса назначения, на котором NetDefendOS будет передавать переадресованный запрос.

Хотя все интерфейсы в системе NetDefendOS являются *центрально направленными* (т.е. существует маршрут по умолчанию, по которому IP-адреса интерфейсов передаются в *Core* – интерфейс обработки правил), для ретранслированных DHCP-запросов такая трассировка не применяется. Напротив, интерфейс является интерфейсом источника, а не *core*.

Пример 5.4. Настройка DHCP Relayer

Этот пример демонстрирует получение IP-адресов клиентами системы NetDefendOS на интерфейсе VLAN от DHCP-сервера. Подразумевается, что в конфигурации межсетевого экрана NetDefend присутствуют VLAN-интерфейсы *vlan1* и *vlan2* с функцией DHCP Relay, и IP-адрес DHCP-сервера определен в адресной книге системы NetDefendOS как *ip-dhcp*. Когда в системе NetDefendOS завершается процесс получения IP-адреса по DHCP, для клиента добавляется еще один маршрут.

CLI

1. Добавьте VLAN интерфейсы *vlan1* и *vlan2* к группе интерфейсов с именем *ipgrp-dhcp:*

gw-world:/> **add Interface InterfaceGroup ipgrp-dhcp**
Members=vlan1,vlan2

2. Добавьте DHCP Relayer с именем *vlan-to-dhcpserver*:

gw-world:/> **add DHCPRelay vlan-to-dhcpserver Action=Relay**
TargetDHCPServer=ip-dhcp
SourceInterface=ipgrp-dhcp
AddRoute=Yes
ProxyARPInterfaces=ipgrp-dhcp

Web-интерфейс

Добавление VLAN интерфейсов *vlan1* и *vlan2* к группе интерфейсов с именем *ipgrp-dhcp:*

1. Зайдите **Interface > Interface Groups > Add > InterfaceGroup**

2. Затем введите

• **Name: ipgrp-dhcp**

• **Interfaces:** выберите vlan1 и vlan2 из списка **Available (Доступные)** и поместите их в список **Selected** (Выбранные).

3. Нажмите **OK**

Добавление DHCP Relayer с именем *vlan-to-dhcpserver*

1. Зайдите **System > DHCP > Add > DHCP Relay**

2. Затем введите

• **Name:** vlan-to-dhcpserver

• **Action:** Relay

• **Source Interface:** ipgrp-dhcp

• **DHCP Server to relay to:** ip-dhcp

• **Allowed IP offers from server:** all-nets

3. Во вкладке **Add Route (Добавить маршрут)** проверить **Add dynamic routes for this relayed DHCP lease (Добавить динамический маршрут для ретрансляции DHCP-аренды)**

4. Нажмите **OK**

5.3.1. Расширенные настройки DHCP Relay

Доступны следующие расширенные настройки функции DHCP Relay:

Max Transactions

Максимальное количество транзакций одновременно

Значение по умолчанию: *32*

Transaction Timeout

Время выполнения DHCP-транзакции

Значение по умолчанию: *10 секунд*

Max PPM

Количество DHCP-пакетов, которое может отправить клиент системы NetDefendOS DHCP-серверу в течение одной минуты.

Значение по умолчанию: *500 пакетов*

Max Hops

Количество сетевых сегментов пути передачи запроса от DHCP-клиента к DHCP-серверу.

Значение по умолчанию: *5*

Max lease Time

Максимальный период аренды, разрешенный в системе NetDefendOS. Если DHCP-сервер имеет более длительный период аренды, то он будет сокращен до указанного значения.

Значение по умолчанию: *10000 секунд*

Max Auto Routes

Количество активных ретрансляций одновременно.

Значение по умолчанию: *256*

Auto Save Policy

Режим сохранения списка аренды IP-адресов на диск. Возможные значения: *Disabled*, *ReconfShut* или *ReconfShutTimer*.

Значение по умолчанию: *ReconfShut*

Auto Save Interval

Периодичность (в секундах) сохранения списка аренды IP-адресов на диск, в случае если *DHCPServer_SaveRelayPolicy* установлено в режим *ReconfShutTimer*

Значение по умолчанию: *86400*

5.4. Пулы IP-адресов

Обзор

Пул IP-адресов предназначен для организации доступа различных подсистем к кэшу распределенных IP-адресов. Формирование пула IP-адресов происходит в процессе совместного функционирования DHCP-клиентов (каждому клиенту соответствует IP-адрес). Пул IP-адресов может использоваться более чем одним DHCP-сервером, как внешним, так и локальным, но обязательно определенным в системе NetDefendOS. Может быть настроено несколько пулов IP-адресов с разными идентификационными именами.

Внешний DHCP-сервер может быть определен:

- как одиночный DHCP-сервер на определенном интерфейсе;
- как один из многих со своим списком уникальных IP-адресов.

Пулы IP-адресов с Config Mode

Основное использование пулов IP-адресов происходит с *IKE Config Mode,* которое используется как свойство для распределения IP-адресов удаленным клиентам, подключающимся по IPsec-туннелям. Более полную информацию можно найти в *разделе 9.4.3, Roaming Clients (Клиенты, находящиеся в роуминге)*.

Базовые настройки пулов IP-адресов

Доступными базовыми настройками пулов IP-адресов являются:

DHCP Server behind interface (DHCP-сервер на интерфейсе) — Указывает, что пул IP-адресов следует использовать DHCP-серверам на определенном интерфейсе.

Specify DHCP Server Address (IP-адрес DHCP-сервера) — Определяет IP-адрес(а) DHCP-сервера(-ов) в порядке возрастания предпочтения в использовании. Эта функция альтернативна предыдущей.

Использование здесь loopback-адреса 127.0.0.1 означает, что DHCP-сервер – это сама система NetDefendOS.

Server filter (Фильтр серверов) — Опция, предназначенная для определения того, какие серверы необходимо использовать. Если параметр не определен, то может использоваться любой DHCP-сервер на соответствующем интерфейсе. Если фильтр содержит несколько адресов (диапазонов адресов), то они указываются в порядке приоритетного использования.

Client IP filter (Фильтр IP-адресов клиентов) — Опция используется, чтобы определить, возможно ли использование предложенного IP-адреса в этом пуле. В большинстве случаев по умолчанию параметр устанавливается в значение **all-nets** (все сети), чтобы все адреса были допустимыми. Или диапазоны допустимых IP-адресов могут быть определены.

Фильтр по IP-адресам используется в ситуации, когда есть вероятность ответа DHCP-сервера на недопустимый IP-адрес.

Расширенные настройки пулов IP-адресов

Расширенные настройки пулов IP-адресов доступные для конфигурирования:

Routing Table (Таблица маршрутизации) — Таблица маршрутизации используется для просмотра информации при определении интерфейса назначения для настраиваемых DHCP-серверов.

Receive Interface (Интерфейс приема пакетов) — Это интерфейс приема пакетов условного виртуального DHCP-сервера. Этот параметр используется для моделирования интерфейса приема пакетов, в случае, когда пул содержит IP-адреса внутренних DHCP-серверов. Параметр необходим, т.к. в критерии фильтрации DHCP-серверов включен параметр **Receive Interface.**

Внутренний DHCP-сервер не может принимать запросы от пула IP-адресов подсистем на каком-либо интерфейсе, т.к. и сервер, и пул являются внутренними по отношению к системе NetDefendOS. Параметр Receive Interface позволяет представить запросы из пула, как бы пришедшими на определенный интерфейс, чтобы ответ поступил с соответствующего DHCP-сервера.

MAC Range (Диапазон MAC- — Это диапазон MAC-адресов, который будет

адресов)	использован для создания условных DHCP-клиентов. Используется в случаях, когда DHCP-сервер (-ы) отображают клиентов по MAC-адресам. Когда DHCP-сервер продолжает выдавать один и тот же IP-адрес каждому клиенту, это свидетельствует о необходимости указания диапазона MAC-адресов.
Prefetch leases (Предварительная аренда)	Определяет количество IP-адресов, которые необходимо предварительно зарезервировать для аренды. Предварительное резервирование увеличивает быстродействие системы, т.к. после запроса время на получение IP-адреса не требуется (если зарезервированные IP-адреса уже есть).
Maximum free (Резерв свободных IP-адресов)	Максимальное количество свободных IP-адресов в резерве. Данное количество должно быть равно или превышать количество предварительно зарезервированных адресов. Пул IP-адресов начнет освобождать IP-адреса (возвращать их обратно DHCP-серверу) когда количество свободных клиентов превысит это значение.
Maximum clients (Емкость пула IP-адресов)	Опция, используемая для определения максимального количества клиентов (IP-адресов) разрешенных в данном пуле IP-адресов.
Sender IP (IP-адрес источника)	IP-адрес источника, который используется при обмене информацией с DHCP-сервером.

Выделение памяти для предварительного резервирования IP-адресов

Как было указано выше, функция *Prefetched Leases* (Предварительная аренда) определяет размер кэш-памяти для распределения IP-адресов, который управляется системой NetDefendOS. Эта кэш-память обеспечивает быстрое распределение IP-адресов и может увеличить общее быстродействие системы. Однако следует обратить внимание на то, что, общее количество предварительно резервируемых IP-адресов запрашивается при загрузке системы, и если число слишком велико, то это может снизить быстродействие системы на начальном этапе.

Так как распределение IP-адресов в предварительно зарезервированном кэше уже назначено, то DHCP-серверы производят запросы так, как если бы кэш был все время полон. Следовательно, администратор должен принять решение об оптимальном начальном размере предварительно зарезервированной кэш-памяти.

Команда интерфейса CLI *ippools* используется для просмотра текущего статуса пула IP-адресов. Наиболее простое представление данной команды следующее:

```
gw-world:/> ippool -show
```

Данная команда позволяет отобразить все настроенные пулы IP-адресов вместе с их статусом. Данные о статусе разделены на четыре части:

- **Zombies** (IP-адреса «зомби») – количество распределенных, но неактивных IP-адресов.
- **In progress** (Распределяемые в данный момент) – количество IP-адресов, находящиеся в процессе распределения.
- **Free maintained in pool** (Свободные IP-адреса в пуле) – количество IP-адресов, доступных для распределения.
- **Used by subsystems** (Используются подсистемами) – количество распределенных активных IP-адресов.

Другие опции команды *ippool* позволяют администратору изменять размер пула IP-адресов, освобождать IP-адреса из пула. Полный список опций данной команды можно найти в руководстве по

применению интерфейса CLI.

Пример 5.5. Создание пула IP-адресов

Этот пример демонстрирует создание объекта «пул IP-адресов», который используется DHCP-сервером с IP-адресом *28.10.14.1* и имеет 10 IP-адресов предварительно зарезервированных для аренды. Подразумевается, что данный IP-адрес уже определен в адресной книге как IP-объект с именем *ippool_dhcp*.

CLI

1. Добавьте VLAN интерфейсы *vlan1* и *vlan2* к группе интерфейсов с именем *ipgrp-dhcp:*

```
gw-world:/> add IPPool ip_pool_1 DHCPServerType=ServerIP
ServerIP=ippool_dhcp PrefetchLeases=10
```

Web-интерфейс

1. Зайдите **Objects > IP Pools > Add > IP Pool**

2. Затем введите **Name:** ip_pool_1

3. Выберите **Specify DHCP Server Address**

4. Добавьте *ippool_dhcp* к списку **Selected**

5. Выберите закладку **Advanced**

6. Присвойте **Prefetched Leases** значение 10

7. Нажмите **OK**

Глава 6. Механизмы безопасности

В данной главе рассматриваются функции безопасности NetDefendOS.

- Правила доступа
- ALG
- Фильтрация Web-содержимого
- Антивирусное сканирование
- Обнаружение и предотвращение вторжений
- Предотвращение атак Denial-of-Service (Отказ в обслуживании)
- «Черный список» хостов и сетей

6.1. Правила доступа

6.1.1. Обзор

Одной из основных функций NetDefendOS является разрешение доступа к защищенным ресурсам информации только авторизованным пользователям. Система NetDefendOS поддерживает управление доступом на основе набора IP-правил, в котором диапазон защищенных LAN-адресов рассматривается как доверенные хосты, при этом поток трафика с ненадежных ресурсов на доверенные хосты ограничивается.

Перед проверкой нового соединения на соответствие набору IP-правил, система NetDefendOS выполняет проверку источника соединения на соответствие *Правилам доступа*. Правила доступа могут использоваться для того, чтобы определить источник трафика на указанном интерфейсе, а также для автоматической блокировки пакетов с определенных источников. Правила доступа обеспечивают эффективную и направленную фильтрацию новых попыток соединения.

Правило доступа по умолчанию

Если администратор не может четко указать какие-либо Правила доступа, используется *Правило доступа по умолчанию*.

Данное правило доступа по умолчанию не является действующим, но на его основе осуществляется проверка входящего трафика с выполнением *обратного поиска (reverse lookup)* в таблицах маршрутизации NetDefendOS. Данный поиск выполняется для подтверждения того, что входящий трафик идет от источника, который, как указано в таблицах маршрутизации, доступен через интерфейс, на который приходит трафик. В случае сбоя обратного поиска, произойдет потеря соединения и генерирование журнального сообщения об отбрасывании пакетов правилом *Default Access Rule*.

Если при выполнении поиска и устранения неисправностей произошла потеря соединения, администратору необходимо просмотреть сообщения *Default Access Rule* в журналах. Решением проблемы является создание маршрута для интерфейса входящего соединения, таким образом, сеть назначения маршрута та же или в диапазон адресов сети входит IP-адрес входящего соединения.

Правила доступа пользователя (опционально)

Для большинства настроек достаточно использовать Правило доступа по умолчанию, администратору не нужно устанавливать другие правила. С помощью Правила доступа по умолчанию можно, например, реализовать защиту от атак IP spoofing, которая подробно описана в следующем разделе. Если Правила доступа четко обозначены, но новое соединение не соответствует какому-либо из этих правил, то по-прежнему используется Правило доступа по умолчанию.

Рекомендуется выполнять первоначальную настройку NetDefendOS без указания каких-либо Правил доступа и добавлять их только в том случае, если требуется тщательная проверка новых соединений.

6.1.2. IP Spoofing

Злоумышленник фальсифицирует IP-адрес пакетов, идущих с доверенного хоста, с целью обмана системы безопасности межсетевого экрана. Такая атака известна как *Spoofing*.

IP spoofing – одна из наиболее распространенных атак spoofing. Злоумышленники используют IP-адреса доверенных хостов, чтобы «обойти» фильтрацию. В заголовке IP-пакета указывается адрес источника пакета, измененный злоумышленником и используемый как адрес локального хоста. Межсетевой экран воспринимает пакет как пришедший с доверенного источника. Хотя источник пакета не может отреагировать корректно, возникает потенциальная угроза перегрузки сети и создания условий для атак *Denial of Service* (DoS).

Межсетевой экран с поддержкой VPN обеспечивает защиту от атак spoofing, но в случае, когда VPN не подходит, используются Правила доступа, которые обеспечивают защиту от атак spoofing за счет дополнительного фильтра, используемого для проверки адреса источника. С помощью Правила доступа можно подтвердить, что пакеты, пришедшие на соответствующий интерфейс, не имеют адреса источника, связанного с сетью другого интерфейса. Другими словами:

- Любой входящий трафик с IP-адреса источника, принадлежащего локальному доверенному хосту, БЛОКИРУЕТСЯ.
- Любой исходящий трафик с IP-адреса источника, принадлежащего внешней неизвестной сети, БЛОКИРУЕТСЯ.

Правило первого пункта не позволяет посторонним лицам использовать адрес локального хоста в качестве адреса источника. Правило, указанное во втором пункте, защищает любой локальный хост от атак spoof.

6.1.3. Настройки правила доступа

Настройка правила доступа аналогична настройке правил остальных типов. Конфигурация содержит **Filtering Fields,** а также **Action (Действие),** которое необходимо предпринять. При наличии соответствия активируется правило, и система NetDefendOS выполняет определенное действие.

Filtering Fields

Filtering Fields, используемые для запуска правила:

- **Interface**: Интерфейс, на который приходит пакет.
- **Network**: Диапазон IP-адресов, которому должен принадлежать адрес отправителя.

Actions (Действия) правила доступа

Действия, которые необходимо указать:

- **Drop**: Отклонить пакеты, соответствующие определенным полям.
- **Accept**: Принять пакеты, соответствующие определенным полям, для дальнейшей проверки набором правил.
- **Expect:** Если адрес отправителя пакета соответствует **Network (Сеть),** указанной данным правилом**,** интерфейс, на который приходит пакет, сравнивается с указанным интерфейсом. При соответствии интерфейсов, пакет принимается способом, указанным выше для действия **Accept.** Если интефейсы не совпадают, пакет отбрасывается, как указано в действии **Drop.**

Примечание: Включение ведения журнала

Для регистрации данных действий можно включить ведение журнала.

Выключение сообщений *Default Access Rule*

Если по некоторым причинам какой-либо источник продолжает генерировать сообщения об отбрасывании пакетов правилом *Default Access Rule,* то для того, чтобы выключить эту функцию необходимо указать Правило доступа для этого источника с действием **Drop** (**Отклонить**).

Решение проблем, связанных с Правилом доступа

Следует отметить, что Правила доступа являются основным фильтром трафика до момента его рассмотрения любыми другими модулями NetDefendOS. Иногда именно по этой причине возникают проблемы, например, при настройке VPN-туннелей. При выполнении поиска и устранения неисправностей рекомендуется проверять Правила доступа, так как правила могут помешать работе какой-либо другой функции, например, настройке VPN-туннелей.

Пример 6.1. Настройка Правила доступа

Необходимо указать правило, запрещающее пакетам с адреса источника, находящегося не в пределах сети lan, приходить на lan-интерфейс.

Интерфейс командной строки

```
gw-world:/> add Access Name=lan_Access Interface=lan
                       Network=lannet Action=Expect
```

Web-интерфейс

1. Зайдите **Interface > Interface Groups > Add > InterfaceGroup**
2. Выберите **Access Rule** в меню **Add menu**
3. Введите:
   - **Name:** lan_Access
   - **Action:** Expect
   - **Interface:** lan
   - **Network:** lannet
4. Нажмите **OK**

6.2. ALG

6.2.1. Обзор

Для выполнения фильтрации пакетов нижнего уровня, с помощью которой выполняется проверка только заголовков пакетов, относящихся к протоколам IP, TCP, UDP и ICMP, межсетевые экраны NetDefend применяют *Application Layer Gateways* (ALGs), обеспечивающие фильтрацию на более высоком уровне в модели OSI, на уровне *приложений*.

Объект ALG действует как посредник для получения доступа к широко используемым Интернет-приложениям за пределами защищенной сети, например, Web-доступ, передача файлов и мультимедиа. Шлюз прикладного уровня (ALG) обеспечивает более высокий уровень безопасности по сравнению с функцией фильтрации пакетов, так как он способен выполнять тщательную проверку трафика по определенному протоколу, а также проверку на самых верхних уровнях стека

TCP/IP.

В системе NetDefendOS следующие протоколы требуют ALGs:

- HTTP
- FTP
- TFTP
- SMTP
- POP3
- SIP
- H.323
- TLS

Реализация ALG

Система начинает использовать новый объект ALG сразу после его назначения администратором, во-первых, по ассоциации с объектом *Service (Служба)*, а затем по ассоциации данной службы с IP-правилом в наборе IP-правил системы NetDefendOS.

Рис. 6.1 ALG

Максимальное количество сессий

Служба шлюза прикладного уровня ALG поддерживает настраиваемый параметр *Max Sessions (Макс. кол-во сессий),* значение по умолчанию варьируется в зависимости от типа ALG. Например, значение по умолчанию для HTTP ALG – *1000,* это максимальное количество соединений, разрешенное на всех интерфейсах для HTTP-сервиса. Далее указан полный список максимального количества сессий по умолчанию:

- HTTP ALG - *1000* сессий
- FTP ALG - *200* сессий

- TFTP ALG - *200* сессий
- SMTP ALG - *200* сессий
- POP3 ALG - *200* сессий
- H.323 ALG - *100* сессий
- SIP ALG - *200* сессий

Совет: Значение максимального количества сессий HTTP может быть небольшим

При наличии большого количества клиентов, подключенных через межсетевой экран NetDefend, значение максимального количества сессий HTTP по умолчанию может быть небольшим, в таких условиях рекомендуется установить более высокое значение.

6.2.2. HTTP ALG

Протокол HTTP *(HyperText Transfer Protocol)* - это первичный протокол, используемый *World Wide Web* (WWW). HTTP является протоколом прикладного уровня на основе архитектуры запрос/ответ. Это протокол передачи без установления соединения, не использующий информацию о состоянии. Клиент, например Web-браузер, отправляет запрос на установку TCP/IP-соединения на известный порт (как правило, порт 80) удаленного сервера. Сервер отправляет ответ в виде строки, а затем собственное сообщение. Этим сообщением может быть, например, HTML-файл в Web-браузере, компонент ActiveX, работающий на клиенте, или уведомление об ошибке.

HTTP-протокол обладает рядом особенностей, так как существует большое количество различных Web-сайтов и типов файлов, которые можно загрузить, используя протокол.

Функции HTTP ALG

HTTP ALG – это расширенная подсистема в NetDefendOS, состоящая из опций, описанных ниже:

- **Фильтрация статического содержимого (Static Content Filtering)** – Функция на основе «*черных и белых списков*», в которые занесены определенные URL-адреса.

  1. «***Черный список*» *URL-адресов***

     Некоторые URL-адреса могут быть внесены в «черный список», таким образом, доступ к ним будет заблокирован. При указании URL-адресов можно использовать описанный ниже метод подстановки (Wildcarding).

  2. «***Белый список» URL-адресов***

     В отличие от «черного списка», «белый список» разрешает доступ к определенным URL-адресам. При указании URL-адресов можно использовать описанный ниже метод подстановки (Wildcarding).

     Следует отметить, что URL-адреса, находящиеся в «белом списке», не могут быть внесены в «черный», а также не могут быть проигнорированы при фильтрации Web-содержимого.

     Включенная функция «Антивирусное сканирование» всегда используется для проверки HTTP-трафика, даже если URL-адреса источника трафика находятся в «белом списке».

  Данные функции подробно описаны в Разделе 6.3.3, «Фильтрация статического содержимого».

- **Фильтрация динамического содержимого (Dynamic Content Filtering)** – Доступ к определенным URL-адресам может быть разрешен или заблокирован в соответствии с политиками для определенных типов Web-содержимого. Доступ к новостным сайтам может быть разрешен, в то время как доступ к игровым сайтам можно заблокировать.

  Данная функция подробно описана в Разделе 6.3.4, «Фильтрация динамического Web-

содержимого».

- **Антивирусное сканирование (Anti-Virus Scanning)** – Содержимое файлов, загружаемых по протоколу HTTP, может быть просканировано на наличие вирусов. Подозрительные файлы могут быть удалены или зарегистрированы в журнале.

  Данная функция является характерной для ALGs и подробно описана в *Разделе 6.4, «Антивирусное сканирование»*.

- **Подтверждение целостности файлов (Verify File Integrity)** – Данная функция предназначена для проверки типа загруженного файла. Существуют две отдельные дополнительные функции для проверки типа файла: **Verify MIME type** и **Allow/Block Selected Types,** которые описаны ниже:

  1. **Verify MIME type**

     Данная функция предназначена для проверки соответствия типа загружаемого файла содержимому (термин *тип файла* также известен как *расширение файла*).

     Все расширения, проверенные данным способом системой NetDefendOS, отображены в списке *Приложения C, «Типы файлов MIME, проходящих проверку».* Если опция включена, любой файл не прошедший проверку MIME, другими словами, если тип файл не соответствует его содержимому, будет удален системой NetDefendOS в целях обеспечения безопасности.

  2. **Allow/Block Selected Types**

     Данная опция действует независимо от проверки MIME, описанной выше, и основана на расширениях файлов, определенных предварительно и отображенных в списке *Приложения C, «Типы файлов MIME, проходящих проверку».* Включенная функция работает либо в режиме *Block Selected (Заблокировать выбранное),* либо в режиме *Allow Selected (Разрешить выбранное).* В этих режимах выполняются следующие функции:

     i. Block Selected (Заблокировать выбранное)

     Файлы с расширением, указанным в списке, при загрузке будут проигнорированы. Система NetDefendOS просматривает содержимое файла (способом, аналогичным проверке MIME) для подтверждения соответствия, чтобы переименованный файл не мог получить «обходной» доступ.

     Если, например, файлы с расширением *.exe* заблокированы, а в файле с расширением *.jpg* (который не заблокирован) находятся данные с расширением *.exe,* данный файл также будет заблокирован. Если включена блокировка, но в списке ничего не отмечено, блокировка не выполняется.

     ii. Allow Selected (Разрешить выбранное)

     Только файлы с отмеченным расширением будут разрешены для загрузки, файлы с другим расширением будут проигнорированы. Как и в случае блокировки, выполняется проверка содержимого файла. Если, например, файлы с расширением *.jpg* разрешены к загрузке, а в файле с расширением *.jpg* находятся данные с расширением *.exe,* данный файл также не будет загружен. Если опция включена, но в списке ничего не отмечено, ни один файл не будет загружен.

     Дополнительно указанные расширения файлов, которые не включены в список по умолчанию, могут быть добавлены в список Allow/Block, тем не менее, содержимое таких файлов не подлежит проверке, так как расширение рассматривается как соответствующее содержимому файла.

Примечание: Сходства с остальными функциями NetDefendOS

*Опции **Verify MIME type** и **Allow/Block Selected Types** работают по тому же принципу для FTP, POP3 и SMTP ALGs.*

- **Download File Size Limit** – Ограничение размеров любого загружаемого файла может быть определено дополнительно (данная опция доступна только для загрузок через HTTP и SMTP ALG).

Порядок фильтрации HTTP

Фильтрация HTTP выполняется в следующем порядке, аналогичный порядок используется для SMTP ALG:

1. «Белый список».
2. «Черный список».
3. Фильтрация Web-содержимого (если включено).
4. Антивирусное сканирование (если включено).

Как описывалось выше, если URL-адрес находится в «белом списке», он не будет заблокирован, даже если он также находится в «черном списке». Функция «Антивирусное сканирование», если она включена, применяется даже в том случае, если URL-адрес находится в «белом списке».

Функция «Фильтрация Web-содержимого», если она включена, по-прежнему применяется к URL-адресам из «белого списка», но вместо блокировки, отмеченные URL-адреса только регистрируются. Включенная функция «Антивирусное сканирование» применяется даже в том случае, если URL-адрес находится в «белом списке».

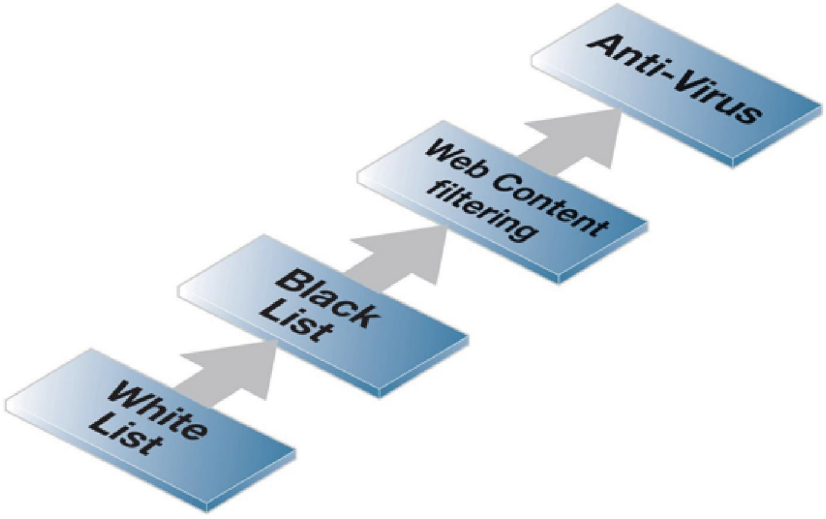


Рис. 6.2. Порядок обработки HTTP ALG

Использование метода Wildcards (Подстановка) в «белом списке» и «черном списке»

В записях, внесенных в «белый список» и «черный список», может использоваться *метод подстановки (wildcarding)* для того, чтобы одна запись была равноценна большому количеству URL-адресов. Символ подстановки «*» используется для отображения какой-либо последовательности символов.

Например, запись **.some_domain.com* заблокирует все страницы, URL-адреса которых заканчиваются на *some_domain.com*.

Если необходимо разрешить доступ на определенную страницу, это можно сделать, добавив в «белый список» запись в виде *my_page.my_company.com,* закрыть доступ на эту страницу с помощью

«черного списка» будет невозможно, так как «белый список» является более приоритетным.

Реализация HTTP ALG

Как указывалось во введении, объект HTTP вводится в использование по связи с объектом службы, а затем по связи объекта службы с правилом в наборе IP-правил. Некоторые предварительно определенные HTTP-сервисы могут использоваться с ALG. Например, для этой цели мог быть выбран сервис **http**. До тех пор пока сервис связан с IP-правилом, ALG будет применяться к трафику, разрешенному этим IP-правилом.

Сервис **https** (который также входит в сервис **http-all)** не может использоваться с HTTP ALG, так как HTTPS-трафик зашифрован.

6.2.3. FTP ALG

File Transfer Protocol (FTP) – это протокол на основе TCP/IP, используемый для обмена файлами между клиентом и сервером. Клиент запускает соединение, подключаясь к FTP-серверу. Как правило, клиент аутентифицирует себя, предоставляя логин и пароль. После получения доступа, сервер предоставляет клиенту список файлов/папок, доступных для загрузки/скачивания (в зависимости от прав доступа). FTP ALG используется для управления FTP-соединениями через межсетевой экран NetDefend.

FTP-соединения

FTP-протокол использует два канала связи: канал для передачи команд и канал для передачи данных. При открытии FTP-сессии, FTP-клиент устанавливает TCP-соединение (канал управления) с портом 21 (по умолчанию) на сервере FTP. Дальнейшее зависит от того, какой режим FTP будет выбран.

Режимы FTP-соединений

FTP работает в двух режимах: *активном* и *пассивном*. Режимы определяют роль сервера при открытии каналов для обмена данными между клиентом и сервером.

- ***Активный режим***

  В активном режиме FTP-клиент отправляет команду на FTP-сервер, указывая IP-адрес и порт, к которому следует подключиться. FTP-сервер устанавливает канал для передачи данных обратно к FTP-клиенту, используя полученную информацию.

- ***Пассивный режим***

  В пассивном режиме FTP-клиент открывает соединение с FTP-сервером для передачи команд. Для FTP-клиентов рекомендуется режим по умолчанию, хотя некоторые рекомендации могут быть противоположными.

Вопросы безопасности FTP

Активный и *пассивный* режимы FTP являются небезопасными для межсетевых экранов NetDefend.

Рассмотрим сценарий, когда FTP-клиент во внутренней сети подключается через межсетевой экран к FTP-серверу в сети Интернет. Далее следует добавить IP-правило, чтобы разрешить прохождение пакетов от FTP-клиента на порт 21 FTP-сервера.

При использовании активного режима система NetDefendOS не осведомлена, что FTP-сервер установит новое соединение обратно к FTP-клиенту. Поэтому запрос на входящее соединение для установки канала обмена данными будет отклонен. Так как номер порта, используемый для канала передачи данных, является динамическим, единственное решение в данной ситуации – разрешить трафик со всех портов FTP-сервера на все порты FTP-клиента, но это небезопасно.

При использовании пассивного режима межсетевому экрану не нужно разрешать соединения с FTP-сервера. С другой стороны, система NetDefendOS по-прежнему остается неосведомленной о том, какой порт FTP-клиент попытается использовать для установки канала передачи данных. Это означает, что необходимо разрешить трафик со всех портов FTP-клиента на все порты FTP-сервера. Хотя это и не так опасно как при использовании активного режима, потенциальная угроза безопасности все же существует. Более того, не все FTP-клиенты поддерживают пассивный режим.

NetDefendOS ALG

Система FTP ALG NetDefendOS касается вопросов безопасности при восстановлении канала TCP-потока для передачи FTP-команд и проверке его содержимого. При этом система NetDefendOS осведомлена о том, какой порт открыт для канала передачи данных. Кроме того, FTP ALG также предоставляет набор функций для фильтрации определенных команд управления и обеспечения защиты от переполнения буфера.

Hybrid Mode (Смешанный режим)

Важной функцией FTP ALG NetDefendOS является способность выполнять немедленное автоматическое переключение между активным и пассивным режимами, таким образом, режимы FTP-соединения могут комбинироваться. Такой тип использования FTP ALG иногда называется *смешанным режимом (hybrid mode).*

Преимущества смешанного режима следующие:

- FTP-клиент может использовать пассивный режим, рекомендованный всем клиентам.
- FTP-сервер может использовать активный режим, являющийся более безопасным для серверов.
- При открытии FTP-сессии межсетевой экран NetDefend автоматически получит прозрачный пассивный канал передачи данных от FTP-клиента и активный канал передачи данных от сервера, и корректно объединит их.

Использование смешанного режима приведет к тому, что и FTP-клиент, и FTP-сервер будут работать в наиболее безопасном режиме. Преобразование режимов также работает наоборот, то есть FTP-клиент использует активный режим, а FTP-сервер – пассивный. На рисунке ниже представлен типичный сценарий смешанного режима.

Рис. 6.3. Смешанный режим FTP ALG

Примечание: Автоматическое переключение между режимами

Нет необходимости включать Смешанный режим (Hybrid mode). Переключение между режимами происходит автоматически.

Опции ограничения соединения

FTP ALG поддерживает две функции по ограничению использования режимов FTP-клиентом и FTP-сервером:

- **Allow the client to use active mode (Разрешить клиенту использовать активный режим)**

  Если данная функция включена, FTP-клиентам разрешается использовать как активный, так и пассивный режим передачи данных. Если FTP-серверу требуется активный режим, NetDefendOS FTP ALG выполнит автоматическое переключение на активный режим.

  Для данной функции определен диапазон портов клиента, используемых для передачи данных. Серверу будет разрешено подключиться к любому из портов, если клиент использует активный режим. Диапазон по умолчанию *1024-65535*.

- **Allow the server to use passive mode (Разрешить серверу использовать пассивный режим)**

  Если данная функция включена, FTP-серверу разрешается использовать как пассивный, так и активный режим передачи данных. Если функция выключена, сервер не сможет использовать пассивный режим. Система NetDefendOS выполнит автоматическое переключение, если клиенты используют пассивный режим.

  Для данной функции определен диапазон портов сервера, используемых для передачи данных. Клиенту будет разрешено подключиться к любому из портов, если сервер использует пассивный режим. Диапазон по умолчанию *1024-65535*.

С помощью данных функций можно определить, требуется ли смешанный режим для завершения соединения. Например, если клиент подключается в пассивном режиме, который не разрешено использовать серверу, то автоматически используется смешанный режим, и FTP ALG выполняет переключение между двумя режимами.

Предварительно определенные FTP ALGs

Система NetDefendOS предоставляет 4 предварительно определенных FTP ALG, каждый с различной комбинацией ограничения режимов, описанных выше.

- ***ftp-inbound*** – Клиенты могут использовать любой режим, но серверы не могут использовать пассивный режим.
- ***ftp-outbound*** – Клиенты не могут использовать активный режим, а серверы могут использовать любой.
- ***ftp-passthrough*** – И клиент, и сервер могут использовать любой режим.
- ***ftp-internal*** – Клиент не может использовать активный режим, а сервер не может использовать пассивный.

Ограничение команды FTP ALG

Протокол FTP содержит набор стандартных команд, передаваемых между сервером и клиентом. Если NetDefendOS FTP ALG обнаруживает команду, которую он не может распознать, то команда блокируется. Необходимо снять данную блокировку, используя следующие опции:

- Разрешить неизвестные FTP-команды

В данном случае неизвестными являются команды, которые ALG не рассматривает как входящие в стандартный набор.

- Разрешить клиенту отправку команды *SITE EXEC* на FTP-сервер.
- Разрешить команду *RESUME*, даже если сканирование содержимого вызвало завершение соединения.

Примечание: Некоторые команды никогда не будут разрешены

Некоторые команды, например, инструкции по шифрованию, никогда не будут разрешены. Шифрование будет означать, что канал для передачи FTP-команд станет недоступным для проверки ALG, и будет невозможно открыть каналы для передачи динамических данных.

Ограничения для канала управления

FTP ALG также определяет следующий ряд ограничений для канала управления FTP, которые могут повысить уровень безопасности FTP-соединений:

- **Maximum line length in control channel (Максимальная длина строки в канале управления)**

При генерировании большого количества команд осуществляется атака на сервер, которая может привести к переполнению буфера. Данное ограничение устраняет потенциальную угрозу. Значение по умолчанию – *256*.

Если на сервере используется слишком большое название папки или файла, то, возможно, потребуется увеличить данное значение.

- **Maximum number of commands per second (Максимальное количество команд в секунду)**

Для предотвращения автоматизированных атак на FTP-сервер, используется ограничение частоты команд. Ограничение по умолчанию – *20* команд в секунду.

- **Allow 8-bit strings in control channel (Разрешить использование 8-битных строк в канале управления)**

С помощью данной опции можно разрешить использование 8-битных символов в канале управления. Разрешение использования 8-битных символов включает поддержку расширений, содержащих международные символы. Например, диакритические символы или символы с умлаутом.

Проверка расширения файла

FTP ALG предлагает тот же метод проверки расширения файла, что и HTTP ALG. Проверка включает две отдельные функции:

- **MIME Type Verification**

Если данная функция включена, система NetDefendOS выполняет проверку соответствия расширения загружаемого файла его содержимому. Если соответствия не обнаружено, загружаемый файл будет отброшен.

- **Allow/Block Selected Types**

Если выбран режим блокировки, файлы с определенным расширением будут отброшены при загрузке. Если выбран режим разрешения, только файлы с определенным расширением будут загружены.

Система NetDefendOS также выполняет проверку, чтобы убедиться, что расширение файла соответствует его содержимому. Новые расширения файлов могут быть добавлены в список предварительно указанных расширений.

Две описанные выше опции, используемые для проверки типа файла, являются теми же, что и в HTTP ALG. Данные опции подробно описаны в Разделе 6.2.2, «The HTTP ALG».

Антивирусное сканирование

Антивирусная подсистема может быть включена для выполнения сканирования всех FTP-загрузок для выявления вредоносного кода. Подозрительные файлы могут быть отброшены или просто зарегистрированы в журнале.

Данная функция является общей для ALGs и подробно описана в *Разделе 6.4, «Антивирусное сканирование».*

FTP ALG и ZoneDefense

Используемая совместно с FTP ALG, технология ZoneDefense обеспечивает защиту внутренней сети от вирусов, распространяемых серверами и хостами. Существует два сценария защиты:

- A. Блокировка клиентов, зараженных вирусами.
- B. Блокировка серверов, зараженных вирусами.

A. Блокировка клиентов, зараженных вирусами.

Администратор устанавливает сетевой диапазон, в который входят адреса локальных хостов. Если локальный клиент пытается загрузить зараженный вирусом файл на сервер FTP, NetDefendOS обращает внимание на то, что клиент относится к локальной сети и поэтому загрузит инструкции по блокировке на локальные коммутаторы. Хост будет заблокирован и не сможет причинить вреда.

Примечание: ZoneDefense не блокирует серверы, зараженные вирусом

Если клиент загружает с удаленного FTP-сервера в сети Интернет зараженный файл, ZoneDefense не будет блокировать сервер, так как он находится вне установленного сетевого диапазона. Тем не менее, вирус будет заблокирован межсетевым экраном NetDefend.

B. Блокировка серверов, зараженных вирусом

В зависимости от политики компании, администратор может заблокировать зараженный FTP-сервер, чтобы предотвратить заражение локальных компьютеров и серверов. В этом случае администратор устанавливает адрес сервера в пределах сетевого диапазона для его блокировки. Клиент не сможет загрузить зараженный файл, так как сервер изолирован от сети.

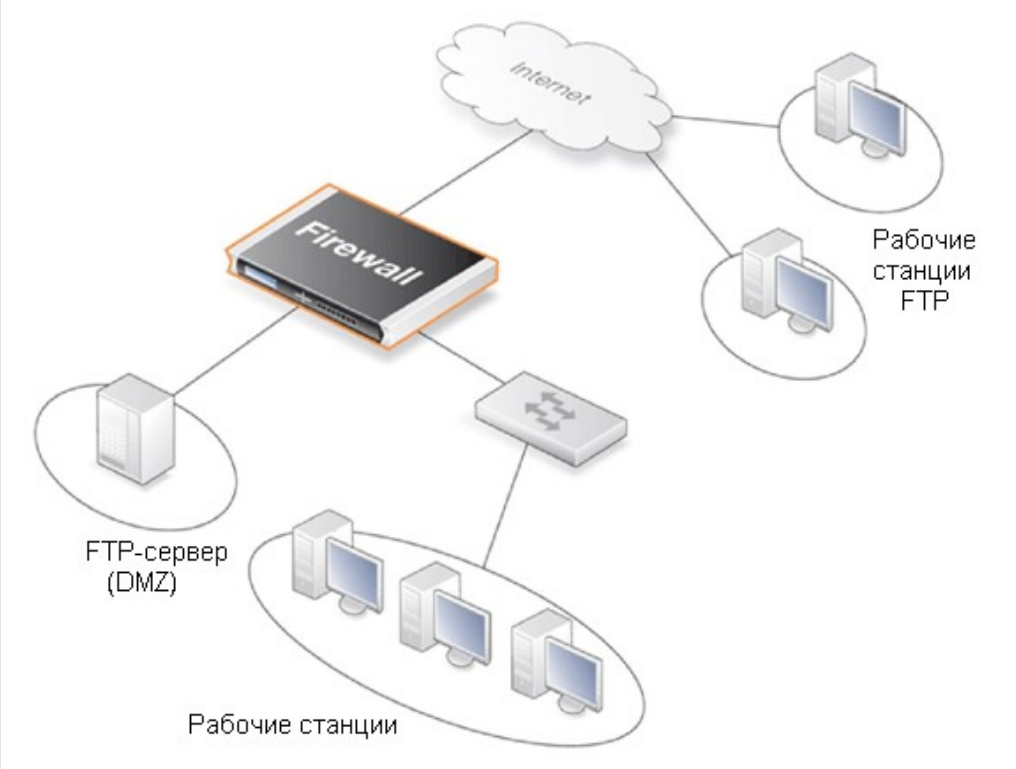
Выполните следующие шаги для установки ZoneDefense с FTP ALG:

- Выполните настройку ZoneDefense для коммутаторов в разделе **ZoneDefense** Web-интерфейса.
- Включите функцию антивирусного сканирования в FTP ALG.
- В настройках Антивируса ALG выберите сеть для защиты с помощью технологии ZoneDefense при обнаружении вируса.

Для получения более подробной информации, пожалуйста, обратитесь к Главе 12, ZoneDefense.

Пример 6.2. Защита FTP-сервера с помощью ALG

Как показано на рисунке ниже, FTP-сервер подключен к межсетевому экрану NetDefend в зоне DMZ с приватными IP-адресами:



В данном случае назначаются следующие ограничения FTP ALG.

• Включить FTP ALG опцию **Allow client to use active mode**, таким образом, клиенты могут использовать как активный, так и пассивный режимы.

• Выключить FTP ALG опцию **Allow server to use passive mode.** Это обеспечивает серверу более высокий уровень безопасности, так как сервер не будет получать данные в пассивном режиме. FTP ALG выполнит переключение при подключении клиента, использующего пассивный режим.

Настройка выполняется следующим образом:

Web-интерфейс

A. Определите ALG:

1. Зайдите **Objects > ALG > Add > FTP ALG**

2. Введите **Name:** ftp-inbound

3. Выберите поле **Allow client to use active mode**

4. Отмените выбор поля **Allow server to use passive mode**

5. Нажмите **OK**

Б. Определите Service:

1. Зайдите **Objects > Services > Add > TCP/UDP Service**

2. Введите следующее:

• **Name:** ftp-inbound-service

• **Type:** выберите TCP из списка

• **Destination:** 21 (порт FTP-сервера)

• **ALG:** выберите *ftp-inbound*, созданное выше

3. Нажмите **OK**

В. Определите правило, чтобы разрешить соединение с публичным IP-адресом на порту 21 и перенаправьте на внутренний FTP-сервер:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** SAT-ftp-inbound

• **Action:** SAT

• **Service:** ftp-inbound-service

3. Для **Address Filter** введите:

• **Source Interface:** любой

• **Destination Interface:** core

• **Source Network:** all-nets

• **Destination Network:** wan_ip

4. Для **SAT** выберите **Translate the Destination IP Address**

5. Введите **To: New IP Address:** ftp-internal (предположительно, данный внутренний IP-адрес для FTP-сервера был определен в объекте «Адресная книга»)

6. **New Port:** 21

7. Нажмите **OK**

Г. Необходимо «натировать» трафик с внутреннего интерфейса через один публичный IP-адрес:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** NAT-ftp

• **Action:** NAT

• **Service:** ftp-inbound-service

3. Для **Address Filter** введите:

• **Source Interface:** dmz

• **Destination Interface:** core

• **Source Network:** dmznet

• **Destination Network:** wan_ip

4. Для **NAT** выберите **Use Interface Address**

5. Нажмите **OK**

Д. Разрешение входящих соединений (SAT требует соответствующее правило *Allow*):

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** Allow-ftp

• **Action:** Allow

• **Service:** ftp-inbound-service

3. Для **Address Filter** введите:

• **Source Interface:** любой

• **Destination Interface:** core

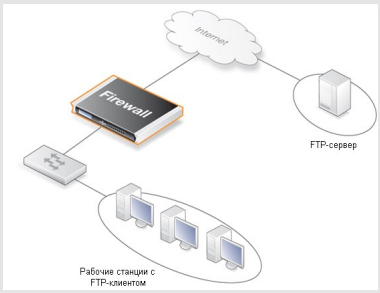
• **Source Network:** all-nets

• **Destination Network:** wan_ip

4. Нажмите **OK**

Пример 6.3. Защита FTP-клиентов

На рисунке, отображенном ниже, межсетевой экран NetDefend обеспечивает защиту рабочей станции, которая будет подключена к FTP-серверам в сети Интернет.



В данном случае будут установлены следующие ограничения FTP ALG.

• Выключите опцию FTP ALG **Allow client to use active mode,** таким образом, клиенты могут использовать только пассивный режим. Это обеспечивает клиенту более высокий уровень безопасности.

• Включите опцию FTP ALG **Allow server to use passive mode.** Опция позволит клиентам подключаться к FTP-серверам, которые поддерживают активный и пассивный режимы в сети Интернет.

Настройка выполняется следующим образом:

Web-интерфейс

A. Создайте FTP ALG
1. Перейдите **Objects > ALG > Add > FTP ALG**
2. Введите **Name:** ftp-outbound
3. Отмените выбор поля **Allow client to use active mode**
4. Выберите поле **Allow server to use passive mode**
5. Нажмите **OK**
Б. Создайте Службу
1. Зайдите **Objects > Services > Add > TCP/UDP Service**
2. Введите:
• **Name:** ftp-outbound-service
• **Type:** выберите TCP из выпадающего списка
• **Destination:** 21 (порт ftp-сервера)
• **ALG:** ftp-outbound
3. Нажмите **OK**
В. Создайте IP-правила
Необходимо создать IP-правила, разрешающие прохождение FTP-трафика, правила будут варьироваться в

зависимости от того, какой IP-адрес используется: приватный или публичный.
i. Использование публичных IP-адресов
Если используются публичные IP-адреса, убедитесь в том, что отсутствуют правила, запрещающие или разрешающие один и тот же тип портов/трафика. Применяемая здесь служба - *ftp-outbound-service*, которая должна использовать предварительно определенный ALG *ftp-outbound*, описанный ранее.

1. Зайдите **Rules > IP Rules > Add > IPRule**
2. Введите:
• **Name:** Allow-ftp-outbound
• **Action:** Разрешить
• **Service:** ftp-outbound-service

3. Для **Address Filter** введите:
• **Source Interface:** lan
• **Destination Interface:** wan
• **Source Network:** lannet
• **Destination Network:** all-nets

4. Нажмите **OK**
ii. Использование приватных IP-адресов
Если межсетевой экран использует приватные IP-адреса и один внешний публичный IP-адрес, необходимо добавить следующее правило *NAT:*
1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:
• **Name:** NAT-ftp-outbound
• **Action:** NAT
• **Service:** ftp-outbound-service

3. Для **Address Filter** введите:
• **Source Interface:** lan
• **Destination Interface:** wan
• **Source Network:** lannet
• **Destination Network:** all-nets

4. Выберите **Use Interface Address**

5. Нажмите **OK**

Настройка пассивного режима FTP-сервера

Как правило, FTP-сервер, находящийся позади межсетевого экрана NetDefend, находится под защитой и система NetDefendOS использует правила SAT-*Allow* для того, чтобы подключиться с внешних клиентов, подключенных в свою очередь к публичной сети Интернет. Если разрешен *Пассивный* режим FTP-сервера и клиент подключается с этим режимом, то FTP-сервер должен сообщить клиенту IP-адрес и порт, на котором можно установить соединение для передачи данных.

Как правило, этот IP-адрес определяется вручную администратором в программном обеспечении FTP-сервера и также необходимо определить внешний IP-адрес интерфейса на межсетевом экране, который подключается к сети Интернет. Тем не менее, это неправильно, если используется FTP ALG.

В качестве альтернативы при настройке FTP-сервера следует указать локальный, внутренний IP-адрес FTP-сервера.

6.2.4. TFTP ALG

Trivial File Transfer Protocol (TFTP) – это упрощенная версия FTP-протокол с ограниченными возможностями, основное предназначение которой – обеспечить клиенту скачивание или загрузку файлов с хоста. Передача данных TFTP основана на UDP-протоколе и поэтому поддерживает собственные протоколы передачи и управления сессией, которые подразделяются на уровни UDP.

Протокол TFTP широко используется в сетях предприятий для обновления программного обеспечения и резервного копирования настроек сетевых устройств. По существу протокол TFTP

небезопасен и часто используется только во внутренних сетях. NetDefendOS ALG снабжает TFTP дополнительным уровнем безопасности, устанавливая ограничения по его использованию.

Основные опции TFTP

Allow/Disallow Read — Можно отключить функцию TFTP **GET**, таким образом, файлы не могут быть загружены клиентом TFTP. Значение по умолчанию – *Allow* (Разрешить).

Allow/Disallow Write — Можно отключить функцию TFTP **PUT**, таким образом, TFTP-клиент не сможет использовать право записи. Значение по умолчанию – *Allow* (Разрешить).

Remove Request Option — Функция определяет, следует ли удалять опции из запроса. По умолчанию – False, что означает «не удалять».

Allow Unknown Options — Если данная опция выключена, то любая опция в запросе, за исключением запроса размера блока, периода неактивности и размера файла, блокируется. Настройка отключена по умолчанию.

TFTP-запросы

Пока описанная выше функция **Remove Request** установлена в значении *false* (функции не удаляются), то могут быть выполнены следующие настройки функции запроса:

Maximum Blocksize — Можно определить максимальный размер блока. Разрешенный диапазон от 0 до 65,464 байт. Значение по умолчанию –65,464 байт.

Maximum File Size — Можно определить максимальный размер передаваемого файла. По умолчанию разрешенное значение 999,999 Кбайт.

Block Directory Traversal — Данная опция может запретить Directory Traversal с помощью использования имен файлов, содержащих «..».

Разрешение таймаутов запроса

NetDefendOS TFTP ALG блокирует повторный TFTP-запрос идущий с одного и того же IP-адреса источника и порта в течение установленного периода времени. Основная причина этого в том, что некоторые TFTP-клиенты могут отправлять запросы с одного и того же порта источника без установки соответствующего таймаута.

6.2.5. SMTP ALG

Simple Mail Transfer Protocol (SMTP) – это протокол, используемый для передачи электронной почты в сети Интернет. Как правило, локальный SMTP-сервер будет расположен в зоне DMZ, таким образом, почта, отправленная удаленными SMTP-серверами, пройдет через межсетевой экран для достижения локального сервера (эта настройка проиллюстрирована далее в Разделе 6.2.5.1, «Фильтрация спама DNSBL»). Локальные пользователи будут использовать программное обеспечение клиента email для того, чтобы получить электронную почту с локального SMTP-сервера.

Протокол SMTP также используется при отправке клиентами электронной почты, SMTP ALG может использоваться для мониторига SMTP-трафика между клиентами и серверами.

Функции SMTP ALG

Основные функции SMTP ALG:

Email rate limiting

Можно назначить максимально допустимую скорость передачи email сообщений. Данный показатель рассчитывается на основе IP-адреса источника, другими словами, это не общий показатель, представляющий интерес, а показатель, зависящий от определенного источника email.
Данная функция является очень полезной, так как обеспечивает защиту от клиентов или серверов, зараженных вирусом, отправляющих большое количество вредоносных сообщений.

Email size limiting

Можно назначить максимально допустимый размер email сообщений. С помощью данной функции можно подсчитать общее количество байт для одного сообщения, к которому относятся: размер заголовка, размер содержимого, размер любого вложения после шифрования. Следует иметь в виду, что размер сообщения email, например, с вложением в 100 Кбайт, будет больше, чем сообщение без вложения размером 100 Кбайт. Размер переданного сообщения может быть 120 Кбайт или более, т.к. автоматическая кодировка вложения может существенно увеличить его размер. Поэтому при установке данного ограничения администратор должен указать размер выше ожидаемого.

Email address blacklisting

Можно внести в «черный список» адреса отправителя или получателя электронной почты для того, чтобы заблокировать сообщения с данными адресами. «Черный список» применяется после «белого списка», таким образом, если адрес соответствует записи в «белом списке», проверка на наличие его в «черном списке» не выполняется.

Email address whitelisting

Можно внести в «белый список» адреса отправителя или получателя электронной почты для того, чтобы разрешить прохождение через ALG независимо от того, занесен ли адрес в «черный список» или письмо отмечено как «спам».

Verify MIME type

Можно проверить содержание прикрепленного файла на соответствие с указанным расширением. Список всех типов файлов, проверенных данным способом, можно найти в Приложении C, Проверенные типы файлов MIME. Та же опция доступна в HTTP ALG, подробное описание ее работы представлено в Разделе 6.2.2, «HTTP ALG».

Block/Allow filetype

Предварительно определенные расширения файлов из списка могут быть заблокированы или разрешены как вложения, в список могут быть добавлены новые расширения файлов. Та же опция доступна в HTTP ALG, подробное описание ее работы представлено в Разделе 6.2.2, «HTTP ALG».

Anti-Virus scanning

Антивирусная подсистема NetDefendOS может выполнить сканирование вложения email для выявления вредоносного кода. Подозрительные файлы могут быть

удалены или просто занесены в журнал. Эта функция является общей для ряда ALGs и подробно описана в Разделе 6.4, «Антивирусное сканирование».

Порядок SMTP-фильтрации

SMTP-фильтрация выполняется в порядке, аналогичном порядку выполняемому HTTP ALG за исключением добавления фильтрации спама:

1. «Белый список».
2. «Черный список».
3. Фильтрация спама (если включено).
4. Антивирусное сканирование (если включено).

Как описано выше, если адрес находится в «белом списке», он не будет заблокирован, даже если он также находится в «черном списке». Фильтрация спама (если функция включена) применяется к адресам из «белого списка», но пакеты с адресами email, отмеченными как «Спам», не будут отклонены, а только зарегистрированы. Антивирусное сканирование (если функция включена) применяется даже в тех случаях, если адрес email находится в «белом списке».

Обратите внимание, что адрес либо получателя, либо отправителя электронной почты может стать основой для блокировки на одном из двух первых этапов фильтрации.

Рис. 6.4. Порядок обработки SMTP ALG

Использование метода подстановки (Wildcards) в «белом списке» и «черном списке»

В записях, сделанных в белых и черных списках можно использовать метод подстановки *(wildcarding)* для того, чтобы иметь одну запись вместо большого количества потенциальных адресов электронной почты. Подстановочный символ «*» можно использовать для представления любой последовательности символов.

Например, запись адреса **@some_domain.com* может использоваться для определения всех возможных адресов электронной почты для *some_domain.com.*

Если, например, подстановка (wildcarding) используется в «черном списке» для блокировки всех адресов для определенной компании под именем my_company, то в черный список следует добавить запись *@my_company.com.

Если необходимо разрешить передачу сообщений только для одного отдела под именем my_department в my_company, то в «белый список» добавляется запись в виде my_department@my_company.com.

Расширенный SMTP и его расширения

Расширенный SMTP-протокол (ESMTP) описан в RFC 1869 и дополняет расширениями стандартный протокол SMTP.

Когда SMTP-клиент открывает сессию с SMPT-сервером, используя ESMTP, сначала клиент отправляет команду *EHLO*. Если сервер поддерживает ESMTP, он ответит списком расширений, которые поддерживает. Эти расширения определены различными RFC. Например, RFC 2920 определяет расширение SMTP *Pipelining.* Другое общее расширение *Chunking,* определенное в спецификации RFC 3030.

NetDefendOS SMTP ALG не поддерживает все расширения ESMTP, включая *Pipelining* и *Chunking.* Поэтому ALG удаляет любые неподдерживаемые расширения из списка поддерживаемых расширений, который SMTP-сервер возвращает клиенту, находящегося позади межсетевого экрана NetDefend. Когда расширение удалено, генерируется сообщение со следующим текстом:

```
unsupported_extension
capability_removed
```

Параметр "*capa=*" в сообщении указывает, какое расширение ALG удалил из ответа сервера. Например, этот параметр может появиться в сообщении как:

```
capa=PIPELINING
```

Для того чтобы указать, что расширение *pipelining* было удалено из ответа SMTP-сервера на команду клиента *EHLO.*

Несмотря на то, что расширения ESMTP могут быть удалены шлюзом прикладного уровня ALG и будут сгенерированы соответствующие сообщения, **это не означает, что какие-либо сообщения будут отброшены**. Передача сообщения будет происходить как обычно, но без использования неподдерживаемых расширений, удаленных шлюзом прикладного уровня ALG.

SMTP ALG и ZoneDefense

SMTP используется как клиентами, которым необходимо отправить электронную почту, так и почтовыми серверами, которые передают сообщения на другие почтовые серверы. Совместное использование ZoneDefense и SMTP ALG обеспечивает блокировку локальных клиентов, которые занимаются распространением вирусов, прикрепляя их к исходящим сообщениям.

Не рекомендуется использовать технологию ZoneDefense для блокировки сообщений, передаваемых на SMTP-сервер, так как при этом будут заблокированы все входящие сообщения с заблокированного почтового сервера. Например, если удаленный пользователь отправляет сообщение, зараженное вирусом, используя широко известную почтовую службу, блокировка отправляющего сервера с помощью ZoneDefense заблокирует все последующие сообщения от той же службы, отправленные любому локальному получателю. Поэтому рекомендуется использовать технологию ZoneDefense совместно с SMTP ALG для блокировки локальных клиентов email.

Для того чтобы выполнить блокировку, администратор устанавливает сетевой диапазон ZoneDefense, содержащий всех локальных SMTP-клиентов.

Совет: Отмена блокировки может быть настроена вручную

Можно вручную настроить отмену блокровки некоторых хостов и серверов путем добавления их в список ***ZoneDefense Exclude****.*

При попытке клиента отправить сообщение, зараженное вирусом, вирус будет заблокирован и ZoneDefense изолирует хост.

Выполните следующие шаги по установке ZoneDefense с SMTP ALG:

- Выполните настройку ZoneDefense для коммутаторов согласно инструкциям в разделе ZoneDefense Web-интерфейса.
- Включите функцию антивирусного сканирования в FTP ALG.
- В настройках Антивируса ALG выберите сеть для защиты с помощью технологии ZoneDefense при обнаружении вируса.

Для получения более подробной информации обратитесь к Главе 12, ZoneDefense.

6.2.5.1. Фильтрация спама при помощи DNSBL

Нежелательные сообщения, часто упоминаемые как «спам», стали причиной раздражения пользователей, а также проблемой безопасности в сети Интернет. Нежелательные сообщения, разосланные в огромных количествах группами лиц, известных как «спамеры», могут расходовать ресурсы, содержать вредоносные программы, а также пытаться направить пользователя на Web-страницы, использующие уязвимые места браузера.

Неотъемлемой частью NetDefendOS SMTP ALG является модуль *фильтрации спама*, обеспечивающий фильтрацию входящих сообщений на основании источника. Это может существенно снизить нагрузку на почтовые ящики пользователей, находящихся за межсетевым экраном NetDefend. NetDefendOS предлагает два способа обработки спама:

• Отбрасывание сообщений с большой вероятностью содержания спама. Разрешение на прохождение сообщений email с небольшой вероятностью содержания спама.

- Разрешение прохождения сообщений email с небольшой вероятностью содержания спама.

Использование NetDefendOS

SMTP-протокол предназначен для обмена сообщениями email между серверами. Система NetDefendOS применяет фильтрацию спама для сообщений, проходящих через межсетевой экран с удаленного SMTP-сервера на локальный SMTP-сервер (с которого позднее локальные клиенты загрузят сообщения электронной почты). Как правило, локальный защищенный SMTP-сервер будет установлен в зоне DMZ и между сервером-отправителем и локальным, сервером-получателем, будет только один сегмент.

Ряд доверенных организаций поддерживает общедоступную базу данных IP-адресов SMTP-серверов, рассылающих спам, запрос на которые может быть выполнен через Интернет. Эти списки известны как базы данных *DNS Black List* (DNSBL), эту информацию можно получить с помощью стандартизированного метода запросов, поддерживаемого системой NetDefendOS. На рисунке ниже показаны все используемые компоненты:

При настройке функции фильтрации спама, IP-адрес сервера-отправителя сообщения может быть отправлен на один или более DNSBL-серверов, для поиска IP-адреса в спам базах DNSBL (для этого NetDefendOS проверяет заголовки IP-пакета). Сервер отправляет ответ, что IP-адрес либо *не находится в списке*, либо *внесен в список.* В последнем случае, когда IP-адрес находится в списке,

DSNBL-сервер указывает на то, что возможно сообщение электронной почты является спамом и, как правило, также предоставляет информацию, известную как запись *TXT*, представляющую собой текстовое пояснение к списку.

Рис. 6.5. Фильтрация спама с помощью DNSBL

Администратор может настроить NetDefendOS SMTP ALG для обращения к нескольким DNSBL-серверам в целях составления мнения об адресе источника сообщения email. Когда приходит новое сообщение, серверы опрашиваются для выявления вероятности того, является ли сообщение спамом, основанной на адресе источника. Администратор NetDefendOS назначает весовое значение больше нуля для каждого настроенного сервера, таким образом, взвешенная сумма (weighted sum) может быть вычислена на основе всех ответов. Администратор может настроить одно из следующих действий, основанных на вычисленной сумме:

1. **Dropped** (**Отбрасывание пакетов**)
   Если сумма больше или равна предварительно определенному значению *Drop threshold,* то сообщение рассматривается как спам и будет отброшено или отправлено в специальный почтовый ящик.
   Если сообщение отклонено, то администратор отправляет сообщение об ошибке на SMTP-сервер отправитель (это сообщение об ошибке аналогично используемому с «черным списком»).

2. **Flagged as SPAM (**Отметка «Спам»)
   Если сумма больше или равна предварительно определенному значению *SPAM threshold,* то сообщение рассматривается как возможный спам и будет перенаправлено получателю с уведомляющим вложенным текстом.

Пример вычисления значения порога

Предположим, что настроено три DNSBL-сервера: *dnsbl1*, *dnsbl2* и *dnsbl3*. Им назначаются весовые значения **3**, **2** и **2** соответственно. Установленное значение порога спама – **5**.

Если *dnsbl1* и *dnsbl2* считают, что сообщение является спамом, а *dnsbl3* так не считает, в результате получаем итоговую сумму **3+2+0=5.** Так как итоговая сумма **5** равна (или больше) значению порога, то сообщение email рассматривается как спам.

Если установленное значение *Drop threshold* – **7**, то всем трем DNSBL-серверам необходимо ответить, чтобы на основании вычисленной суммы (**3+2+2=7**) отбросить сообщение.

Альтернативные действия для отброшенного спама

Если вычисленная сумма больше или равна значению *Drop threshold,* то сообщение не будет перенаправлено назначенному получателю. Вместо этого, администратор может выбрать один из двух альтернативных вариантов для отброшенных сообщений:

- Можно указать определенный адрес электронной почты для всех отброшенных сообщений. Если это выполнено, то любые сообщения *TXT,* отправленные DNSBL-серверами (описано ниже), которые идентифицировали сообщение как спам, могут быть добавлены системой NetDefendOS в заголовок перенаправленного сообщения.

- Если нет адреса получателя отброшенных сообщений, то они удаляются системой NetDefendOS. Администратор может указать, что сообщение об ошибке отправлено обратно на адрес отправителя наряду с *TXT* сообщениями от DNSBL-серверов, определивших, что сообщение является спамом.

Маркировка спама

Если сообщения электронной почты рассматриваются как возможный спам, поскольку рассчитывается сумма выше порога спама, но ниже порога Drop, то тема (*Subject*) сообщения меняется, прибавляется префикс и сообщение пересылается предполагаемому получателю. Текст маркированного сообщения определяется администратором, но может и отсутствовать (хотя это не рекомендуется).

Например, первоначальная тема сообщения:

```
Buy this stock today!
```

Если текст маркировки обозначен как «***** SPAM ***»,** то получим следующую измененную тему сообщения:

```
*** SPAM *** Buy this stock today!
```

Получатель электронной почты будет видеть данный текст в теме входящих сообщений. Далее пользователь может принять решение о создании собственных фильтров на локальном клиенте для обработки таких маркированных сообщений, например, перемещения их в отдельную папку.

Добавление информации X-SPAM

Если сообщение электронной почты является спамом и определен адрес, куда пересылаются отброшенные сообщения, то администратор может применить к сообщению опцию *Add TXT Records (Добавить TXT записи)*. *TXT запись* – это информация, отправленная сервером DNSBL, если сервер считает отправителя источником спама. Данная информация может быть вставлена в заголовок сообщения с помощью *X-SPAM,* прежде чем сообщение будет отправлено. Поля X-SPAM:

- **X-Spam-Flag** – всегда значение *Yes*.

- **X-Spam-Checker-Version** – версия NetDefendOS как маркировка сообщения.

- **X-Spam-Status** – всегда значение *DNSBL*.

- **X-Spam-Report** – список DNSBL-серверов, отмечающих сообщения как спам.

- **X-Spam-TXT-Records** – список записей TXT, отправленных DNSBL-серверами, идентифицирующими сообщения как спам.
- **X-Spam_Sender-IP** – IP-адрес, используемый отправителем сообщения.

Данные поля могут быть отнесены к правилам фильтрации, установленным администратором в программном обеспечении почтового сервера.

Учет для вышедших из строя DNSBL серверов

Если запрос, отправленный на DNSBL-сервер, не был обработан в течение выделенного для него таймаута, то система NetDefendOS будет считать, что не удалось выполнить запрос, и весовое значение, указанное для этого сервера автоматически вычитается из обоих порогов спама и отбрасывания, чтобы подсчитать итоговую сумму для данного сообщения.

Если достаточное количество DNSBL-серверов не отвечает, то вычитание может привести к отрицательному значению порогов. Так как подсчет итоговой суммы всегда дает значение нуля или больше (серверы не могут иметь отрицательного весового значения), то при отрицательном значении порогов спама и отбрасывания будет разрешено прохождение всех сообщений.

Если DNSBL-сервер не отвечает в течение заданного времени, генерируется сообщение для регистрации в журнале. Это выполняется только один раз при последовательных ошибках ответов одного сервера во избежание ненужного повторения сообщения.

Проверка сообщения отправителя

Как часть модуля Антиспам, существует опция проверки несоответствия адреса «От кого» в команде SMTP-протокола с адресом «От кого» заголовка сообщения. Спамеры могут умышленно сделать их различными для того, чтобы сообщение прошло фильтрацию, таким образом, данная функция обеспечивает дополнительную проверку целостности сообщения.

Ведение журнала

Существует три типа ведения журнала, выполняемого модулем фильтрации спама:

- Регистрация отброшенных сообщений, маркированных как спам – Эти сообщения содержат адрес источника и IP, а также взвешенную сумму и информацию о том, какие DNSBL-серверы участвовали.

- DNSBL-серверы не отвечают – Регистрируются таймауты запросов, отправленные на DNSBL-серверы.

- Все указанные DNBSL-серверы перестали отвечать – Это событие высокого уровня важности, так как при этом будет разрешено прохождение всех сообщений.

Краткая информация по настройке

Для того чтобы выполнить настройку фильтрацию спама с помощью DNSBL в SMTP ALG, выполните следующие шаги:

- Определите, какие DNSBL-серверы будут использоваться. Сервер может быть один или их может быть несколько. Несколько серверов могут действовать в качестве дублеров друг друга, а также для подтверждения статуса отправителя.

- Определите *весовое значение* для каждого сервера, который определит важность значения во время принятия решения, является ли сообщение спамом, при расчете взвешенной суммы.

- Определите пороги для спама. Если взвешенная сумма больше или равна значению порога, то сообщение рассматривается как спам. Определены два порога:

  i. *Порог Spam* – Порог для сообщений, маркированных как спам.

  ii. *Порог Drop* – Порог для отбрасывания сообщений.

  Значение *Порога Spam* должно быть меньше значения *Порога Drop*. Если значения порогов одинаковые применяется только *Порог Drop*.

- Определите текстовую маркировку в качестве префикса в поле Тема сообщения, рассматриваемого как спам.

- Дополнительно определите адрес email, на который будут отправляться все отброшенные сообщения (или, в качестве альтернативы, просто отброшены). Также дополнительно укажите,

что *TXT* сообщения отправленные DNSBL-серверами, давшими сбой, вставлены в заголовок таких сообщений.

Кэширование адресов для повышения производительности

Для ускорения обработки система NetDefendOS поддерживает локальный кэш наиболее часто просматриваемых адресов отправителей. Если кэш переполняется, то удаляется самая старая запись, чтобы освободить место для новой. Существует два параметра, которые можно указать для кэширования адресов:

- **Размер кэша**

  Количество записей, которые могут содержаться в кэше. Если установлено значение ноль, кэш не используется. По мере увеличения размера кэша увеличивается объем памяти NetDefendOS, необходимый для фильтрации спама.

- **Таймаут кэша**

  Таймаут определяет время действия любого адреса при сохранении в кэше. После истечения этого периода времени, на DNSBL-сервер должен быть отправлен новый запрос адреса отправителя для кэширования.

  Значение по умолчанию – 600 секунд.

Кэш очищается при запуске или изменении настроек.

Записи для подсистемы DNSBL:

- Количество проверенных сообщений.
- Количество сообщений, маркированных как спам.
- Количество отброшенных сообщений.

Записи для каждого DNSBL-сервера:

- Количество положительных ответов (если сообщение является спамом) от каждого настроенного

DNSBL-сервера.

- Количество запросов, отправленных на каждый настроенный DNSBL-сервер.
- Количество неудачных запросов (без ответов) для каждого настроенного DNSBL-сервера.

Команда CLI *dnsbl*

С помощью команды CLI **dnsbl** осуществляется управление и мониторинг работы модуля фильтрации спама. Сама по себе команда **dnsbl** отображает статус всех шлюзов ALG. Если имя объекта SMTP ALG, на котором включена фильтрация спама с помощью SMTP, *my_smtp_alg*, то получим следующую выходную информацию:

```
gw-world:/> dnsbl
DNSBL Contexts:
Name                      Status    Spam     Drop     Accept
------------------------ -------- -------- -------- --------
my_smtp_alg               active    156      65       34299
```

```
alt_smtp_alg              inactive   0       0          0
```

С помощью опции *-show* можно просмотреть краткую сводку по фильтрации спама, выполненную определенным шлюзом ALG. Ниже представлен пример проверки работоспособности объекта *my_smtp_alg,* хотя в данном случае объект ALG еще не обработал ни одного сообщения.

```
gw-world:/>              dnsbl              my_smtp_alg              -show

Drop Threshold :   20
Spam Threshold :   10
Use TXT records :  yes
IP Cache disabled
Configured BlackLists : 4
Disabled BlackLists :   0
Current Sessions :      0
Statistics:
Total number of mails checked :  0
Number of mails dropped :        0
Number of mails spam tagged :    0
Number of mails accepted :       0

BlackList Status Value Total Matches Failed
------------------------ -------- ----- -------- -------- --------
zen.spamhaus.org          active    25     0          0         0
cbl.abuseat.org           active    20     0          0         0
dnsbl.sorbs.net           active    5      0          0         0
asdf.egrhb.net            active    5      0          0         0
```

Для проверки статистики определенного DNSBL-сервера используется следующая команда.

```
gw-world:/>     dnsbl     smtp_test     zen.spamhaus.org     -show

BlackList:          zen.spamhaus.org
Status :            active
Weight value :      25
Number of mails checked :                  56
Number of matches in list :                3
Number of failed checks (times disabled) : 0
```

Для того чтобы очистить кэш **dnsbl** объекта *my_smtp_alg* и сбросить все счетчики статистики, используется следующая команда:

```
gw-world:/> dnsbl my_smtp_alg -clean
```

Совет: DNSBL-серверы

Список DNSBL-серверов находится здесь:
http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists.

6.2.6. POP3 ALG

POP3 – это протокол передачи сообщений, который отличается от SMTP-протокола тем, что передает сообщение напрямую от сервера на программное обеспечение клиента, используемого пользователем.

Функции POP3 ALG

Основные функции POP3 ALG:

Block clients from sending USER and PASS command — Блокировка соединений между клиентом и сервером, отправляющим имя пользователя/пароль в виде текста, который можно легко прочитать (некоторые серверы могут поддерживать только этот метод).

Hide User — Данная функция предупреждает POP3-сервер, что имя пользователя не существует. Это позволяет пользователям подбирать различные имена, пока не будет найдено корректное имя.

Allow Unknown Commands — Можно разрешить или запретить нестандартные команды POP3, не распознанные объектом ALG.

Fail Mode — Можно разрешить или запретить прохождение файлов с нарушенной целостностью, обнаруженных при сканировании.

Verify MIME type — Можно выполнить проверку содержимого прикрепленного файла на соответствие указанному расширению. Список всех проверенных расширений находится в *Приложении C, Типы файлов MIME, проходящих проверку*. Та же самая функция доступна в HTTP ALG, а ее подробное описание представлено в Разделе 6.2.2, «HTTP ALG»

Block/Allow type — Предварительно определенные расширения файлов могут быть дополнительно заблокированы или разрешены, а новые расширения могут быть добавлены в список. Та же опция также доступна в HTTP ALG, а ее подробное описание представлено в Разделе 6.2.2, «The HTTP ALG».

Anti-Virus Scanning — Подсистема антивирусного сканирования NetDefendOS может дополнительно просканировать вложения электронной почты для обнаружения вредоносного кода. Подозрительные файлы могут быть отброшены или просто зарегистрированы. Данная функция является общей для объектов ALG и подробно описана в *Разделе 6.4, «Антивирусное сканирование»*

6.2.7. PPTP ALG

Причины использования PPTP ALG

PPTP ALG применяется для решения проблем, связанных с использованием PPTP-туннелей через NAT.

Допустим, в защищенной внутренней сети позади межсетевого экрана NetDefend присутствуют два клиента, **A** и **B**. Межсетевой экран подключен к внешней сети Интернет и определенное NAT-правило разрешает прохождение трафика от клиентов в Интернет. Поэтому кажется, что оба клиента используют один и тот же IP-адрес для соединения с серверами в Интернет.

Клиент **A** устанавливает PPTP-туннель для соединения с внешним хостом **C** в сети Интернет. Конечными точками туннеля являются клиент и внешний сервер. Благодаря IP-правилу NAT устанавливается соединение через внешний IP-адрес на межсетевом экране.

Это первое соединение будет успешным, но, когда второй клиент **B** попытается также подключиться к тому же серверу **C** с тем же IP-адресом конечной точки, первое соединение клиента **A** будет потеряно. Причина в том, что оба клиента пытаются установить PPTP-туннель через один и тот же внешний IP-адрес к одной и той же конечной точке.

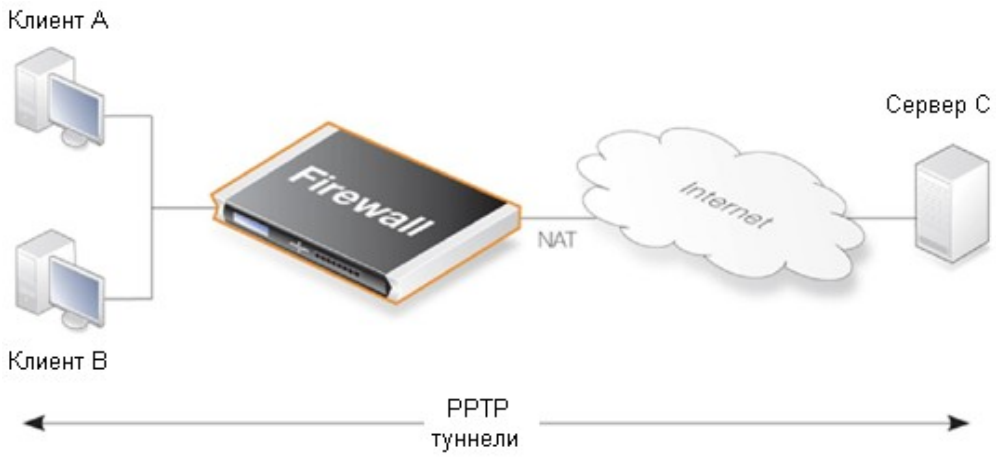


Рис. 6.6. Использование PPTP ALG

PPTP ALG решает эту проблему. С помощью ALG трафик от всех клиентов может быть мультиплексирован через один PPTP-туннель между межсетевым экраном и сервером.

Настройка PPTP ALG

Настройка PPTP ALG похожа на настройку других типов ALG. Объект ALG должен быть связан с соответствующей службой, а служба с IP-правилом. Последовательность шагов по настройке является следующей:

- Определите новый объект PPTP ALG с соответствующим названием, например *pptp_alg*. Полный список функций для ALG представлен в конце данного раздела.
- Свяжите новый объект ALG с соответствующим объектом *Служба*. Для этих целей может использоваться предварительно определенная служба под названием *pptp-ctl*.

  В качестве альтернативного варианта можно определить новый объект службы, например, *pptp_service*. Служба должна поддерживать следующие параметры:

  i. Выберите **Type** (протокол) – *TCP*.

  ii. По умолчанию диапазон портов источника **(Source)** – *0-65535*.

  iii. Установите порт назначения **(Destination)** – *1723*.

  iv. Выберите **ALG,** который будет объектом PPTP ALG**,** определенном в первом шаге. В этом случае, он будет носить название *pptp_alg*.
- Свяжите этот объект службы с IP-правилом NAT, которое позволяет прохождение трафика от клиентов на удаленную конечную точку PPTP-туннеля. Возможно, это правило, натирующее трафик с сетью назначения *all-nets*.

  Представленное ниже IP-правило отображает связь объекта службы *pptp_service* с типичным правилом NAT. Клиенты, являющиеся локальными конечными точками PPTP-туннелей, расположены позади межсетевого экрана в сети *lannet*, который подключен к интерфейсу *lan*. Доступ в Интернет открыт через интерфейс *wan*, который является интерфейсом назначения, с *all-nets* в качестве сети назначения.

Действие	**Интерфейс источника**	**Сеть источника**	**Интерфейс назначения**	**Сеть назначения**	**Служба**
NAT	lan	lannet	wan	all-nets	pptp_service

Настройки PPTP ALG

Для PPTP ALG доступны следующие настройки:

Name	Подробное имя ALG.
Echo timeout	Таймаут простоя для сообщений Echo в PPTP-туннеле.
Idle timeout	Таймаут простоя для сообщений трафика пользователя в PPTP-туннеле.

В большинстве случаев необходимо определить только имя, а все остальные настройки можно оставить по умолчанию.

6.2.8. SIP ALG

Session Initiation Protocol (SIP) – это протокол на основе ASCII (UTF-8), используемый для установки сессий между клиентами в IP-сети. Протокол использует архитектуру «запрос-ответ», также как и протоколы HTTP и SMTP. Сессия, которую устанавливает протокол SIP, может состоять из телефонного звонка Voice-Over-IP (VoIP) или это может быть совместная мультимедиа-конференция. Использование SIP с VoIP означает, что телефония может стать IP-приложением, которое может быть интегрировано в другие сервисы.

Протокол SIP не знает подробностей содержания сессии и несет ответственность только за ее инициацию, завершение и изменение. Как правило, сессии, установленные SIP, используются для передачи потокового аудио и видео в сети Интернет с использованием протокола RTP / RTCP (основан на UDP), но они могут также включать трафик на основе TCP-протокола. RTP / RTCP-сессии могут также включать трафик TCP или TLS в рамках одной и той же сессии.

SIP определен в IETF RFC 3261 и является одним из протоколов, лежащих в основе VoIP. SIP -протокол аналогичен протоколу H.323, но цель его создания заключалась в том, чтобы сделать этот протокол более масштабным, чем H.323. (Для получения подробной информации о VoIP см. также раздел 6.2.9 ", H.323 ALG".)

Примечание: Функция Формирование трафика (Traffic shaping) не работает с SIP ALG

Любые соединения трафика, активирующие IP-правило со служебным объектом, который использует SIP ALG, не могут быть подвержены воздействию функции Формирование трафика (Traffic shaping).

Компоненты SIP

Следующие компоненты являются блоками установки SIP-коммуникации:

User Agents Это конечные точки или *клиенты*, которые участвуют в коммуникации «клиент-клиент». Как правило, это рабочая станция или устройство, используемое в IP-телефонии. Термин «клиент» будет использоваться на протяжении всего этого раздела для описания *user agent* (агент пользователя).

Proxy Servers Proxy-серверы действуют как маршрутизаторы в SIP-протоколе, выступая как в роли клиента, так и сервера при получении запросов от клиентов. Proxy-серверы пересылают запросы в текущее местоположение клиента, а также выполняют аутентификацию и авторизацию для доступа к службам. Они также обеспечивают маршрутизацию вызова.

Proxy часто расположен на внешней, незащищенной стороне межсетевого

экрана NetDefend, но также может находиться и в других местах. Все эти сценарии поддерживаются системой NetDefendOS.

Registrars Сервер, который обрабатывает запросы SIP *REGISTER,* носит особое название – Registrar. Сервер Registrar выполняет задачи размещения хоста, в местах, где доступен другой клиент.

Registrar и Proxy-сервер являются логическими объектами и по сути могут находятся на одном физическом сервере.

SIP-протокол для передачи медиа

В сессиях SIP используются следующие протоколы: session makes use of a number of protocols. These are:

SDP *Session Description Protocol* (RFC4566), используемый для инициализации медиа-сессии.

RTP *Real-time Transport Protocol* (RFC3550), используемый для передачи аудио и видео-потоков с помощью UDP-протокола.

RTCP *Real-time Control Protocol* (RFC3550), используемый совместно с RTP-протоколом, для обеспечения управления потоком данных.

Установка NetDefendOS SIP

При настройке системы NetDefendOS для управления SIP-сессиями выполните следующие шаги:

- Определите один объект *Служба* для SIP-коммуникации.
- Определите объект *SIP ALG*, который связан с объектом *Служба*.
- Определите соответствующие IP-правила для SIP-коммуникаций, которые используют определенный объект *Служба*.

Функции SIP ALG

Для объекта SIP ALG можно настроить следующие функции:

Maximum Sessions per ID Количество одновременных сессий, в которых может учавствовать один клиент. Значение по умолчанию – *5*.

Maximum Registration Time Максимальный период времени регистрации с помощью SIP Registrar. Значение по умолчанию – *3600* секунд.

SIP Signal Timeout Максимальный период времени, разрешенный для SIP-сессий. Значение по умолчанию – *43200* секунд.

Data Channel Timeout Максимальный период времени, разрешенный при отсутствии трафика SIP-сессии. Значение по умолчанию – 120 секунд.

Allow Media Bypass Если эта опция включена, то такие данные, как RTP / RTCP связи, могут передаваться непосредственно между двумя клиентами без участия межсетевого экрана NetDefend. Это произойдет только в том случае, если два клиента находились позади одного интерфейса и принадлежат одной и той же сети. Значение по умолчанию *Disabled (Выключено)*.

Функция SIP Proxy *Record-Route*

Для того чтобы понять, как настроить сценарии SIP в системе NetDefendOS, сначала необходимо выяснить как действует функция SIP proxy *Record-Route.* SIP proxy поддерживают либо включенную, либо выключенную функцию Record-Route. Если функция включена, proxy-сервер известен как *Stateful proxy*. Если функция выключена, то proxy-сервер сообщает, что будет посредником для всех SIP сигналов между двумя клиентами.

При установке SIP-сессии, клиент отправляет сообщение *INVITE* на внешний SIP proxy-сервер. SIP proxy передает это сообщение на удаленный proxy-сервер, ответственный за контактную информацию об удаленном клиенте. Затем удаленный proxy передает сообщение *INVITE* вызываемому клиенту. После того, как два клиента изучили IP-адреса друг друга, они могут общаться непосредственно друг с другом и остальные сообщения SIP могут «обойти» proxy-сервер. Это облегчает масштабирование, так как proxies используются только для первоначального обмена SIP-сообщениями.

Недостаток удаления proxy-серверов из сессии в том, что IP-правила NetDefendOS должны разрешать прохождение всех SIP-сообщений через межсетевой экран NetDefend, и если сеть источника сообщений не известна, то появляется большое количество потенциально опасных соединений, разрешенных набором IP-правил. Эта проблема не возникает, если на локальном proxy-сервере включена функция Record-Route. В этом режиме все SIP-сообщения будут исходить только от proxy-сервера.

Различные правила, необходимые, если функция Record-Route включена или выключена, находятся в двух списках наборах IP-правил, представленных ниже в подробном описании Сценарий 1 Защита локальных клиентов – Proxy, расположенные в сети Internet.

IP-правила для медиа-данных

При рассмотрении потоков SIP-данных выделяют два различных типа обмена данными:

- SIP-сессия, установленная между двумя клиентами до начала обмена *медиа-данными*.
- Обмен *медиа-данными*, например, зашифрованные речевые данные, которые являются основой для телефонных VoIP-звонков.

В настройках SIP, описанных ниже, необходимо указать IP-правила, используемые для выше представленного первого пункта, протокол обмена SIP используется для коммуникации по схеме «клиент–клиент». Нет необходимости в указании IP-правил или других объектов для обработки второго указанного выше пункта, обмена медиа-данными. SIP ALG автоматически создает соединения (иногда называемые SIP *pinholes*), необходимые для прохождения потока данных через межсетевой экран NetDefend.

Совет

Убедитесь в отсутствии предыдущих правил в наборе IP-правил, запрещающих или разрешающих тот же самый тип трафика.

Сценарии использования SIP

Система NetDefendOS поддерживает различные варианты использования SIP. Следующие три сценария охватывают практически все возможные типы использования:

- **Сценарий 1**
  Защита локальных клиентов – Proxy-сервер расположен в Интернет

  SIP-сессия между клиентом на локальной, защищенной стороне межсетевого экрана NetDefend и клиентом, который находится на внешней, незащищенной стороне. SIP proxy расположен на внешней, незащищенной стороне межсетевого экрана NetDefend. Как правило, передача данных

реализуется через публичную сеть Интернет с клиентами на внутренней, защищенной стороне, зарегистрированными proxy-серверами на публичной, незащищенной стороне.

- **Сценарий 2**
  Защита proxy и локальных клиентов – Proxy-сервер находится в той же сети, что и клиенты

  SIP-сессия между клиентом на локальной, защищенной стороне межсетевого экрана NetDefend и клиентом, который находится на внешней, незащищенной стороне. SIP Proxy расположен на локальной, защищенной стороне межсетевого экрана NetDefend и может управлять регистрацией с обоих клиентов, расположенных в одной и той же локальной сети, а также с клиентов на внешней, незащищенной стороне. Передача данных выполняется в публичной сети Интернет или между клиентами в локальной сети.

- **Сценарий 3**
  Защита proxy-сервера и локальных клиентов – Proxy-сервер подключен к интерфейсу DMZ

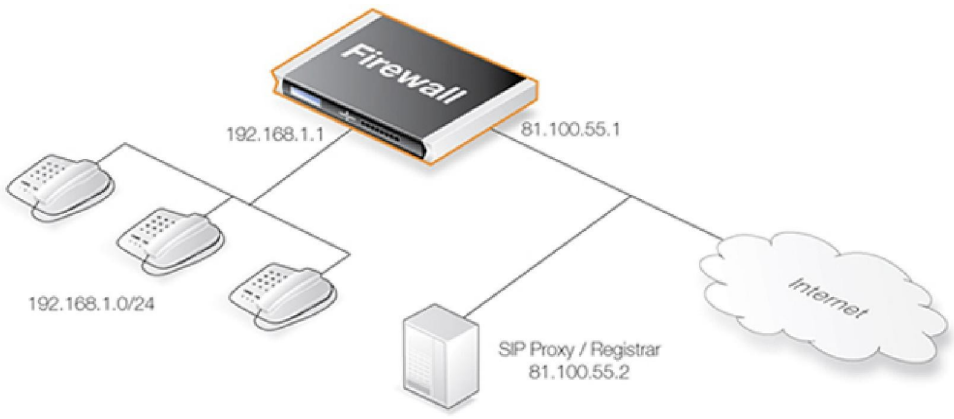
  SIP-сессия между клиентом на локальной, защищенной стороне межсетевого экрана NetDefend и клиентом, который находится на внешней, незащищенной стороне. SIP Proxy подключен к интерфейсу DMZ и физически отделен от сети локального клиента, а также от сети удаленного клиента и сети proxy-сервера.

Все выше перечисленные сценарии также используются в ситуации, когда два клиента, участвующие в сессии, находятся в одной и той же сети.

Рассмотрим подробно каждый из сценариев.

Сценарий 1
Защита локальных клиентов – Proxy-сервер расположен в сети Интернет

В сценарии предполагается, что офис с пользователями VoIP находятся в частной внутренней сети, где топология сети будет скрыта с помощью NAT. Это проиллюстрировано ниже.



SIP proxy в приведенной выше диаграмме может быть расположен удаленно в сети Интернет. Функция **Record-Route** должна быть включена для того чтобы весь SIP-трафик, отправленный или полученный клиентами офиса, мог быть отправлен через SIP Proxy. Это рекомендуемая функция, так как она сводит атаки к минимуму, разрешая прохождение в локальную сеть только SIP сигнализации с SIP Proxy-сервера.

Данный сценарий выполняется двумя способами:

- С применением NAT для скрытия топологии сети.
- Без применения NAT, таким образом, топология сети открыта.

Примечание: Нет необходимости в настройке NAT traversal

Нет необходимости в настройке NAT Traversal для клиентов SIP и SIP Proxies. Например, не должен использоваться протокол ***Simple Traversal of UDP through NATs*** *(STUN). NetDefendOS SIP ALG решает все вопросы, связанные с NAT traversal в SIP.*

Для данного сценария выполните следующие шаги по установке:

1. Определите объект *SIP ALG*, используя функции, описанные выше.
2. Определите объект *Служба*, который связан с объектом SIP ALG. В службе должны поддерживаться следующие параметры:

- **Порт назначения** – *5060* (по умолчанию сигнальный порт SIP).
- **Тип** – *TCP/UDP*.

3. Укажите два правила в наборе IP-правил:

- NAT-правило для трафика, исходящего от клиентов во внутренней сети на сервер SIP Proxy расположенный во внешней сети. SIP ALG будет следить за передачей всех адресов, необходимых для правила *NAT*. Данная передача будет происходить как на IP-уровне, так и на уровне приложений. Ни клиенты, ни proxy-серверы не должны быть осведомлены, что локальные пользователи натируются.
- Правило *Allow* для SIP-трафика, входящего с SIP proxy-сервера на IP межсетевого экрана NetDefend. Данное правило использует **core** (другими словами, NetDefendOS) в качестве интерфейса назначения. Причина этого связана с правилом *NAT*, указанным выше. При получении входящего вызова, NetDefendOS будет автоматически определять локального получателя, выполнять передачу адреса и перенаправлять SIP-сообщения получателю.

Нет необходимости в правиле *SAT* для передачи входящих SIP-сообщений, так как ALG автоматически перенаправит входящие SIP-запросы необходимому внутреннему пользователю. Если SIP-клиент позади натирующего межсетевого экрана NetDefend регистрируется с внешним SIP proxy-сервером, NetDefendOS отправляет свой собственный IP-адрес в качестве контактной информации на SIP proxy-сервер. Система NetDefendOS регистрирует контактную информацию о локальном клиенте и использует ее для перенаправления входящих вызовов пользователю. ALG следит за необходимой передачей адреса.

4. Убедитесь в том, что клиенты корректно настроены. SIP Proxy-сервер играет ключевую роль в определении текущего расположения другого клиента, участвующего в сессии. IP-адрес proxy-сервера не определяется в ALG. Вместо этого его местонахождение либо введено непосредственно на программное обеспечение клиента, либо клиент обладает возможностью получить IP-адрес proxy-сервера автоматически, например, через DHCP.

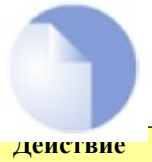
Примечание: Нет необходимости в настройке NAT

traversal

*Нет необходимости в настройке **NAT Traversal** для клиентов SIP и SIP Proxies. Например, не должен использоваться протокол **Simple Traversal of UDP through NATs** (STUN). NetDefendOS SIP ALG решает все вопросы, связанные с NAT traversal в SIP.*

IP-правила с включенной функцией Record-Route отображены ниже, изменения, применяемые при использовании NAT отображены в круглых скобках «*(..)*».

Действие (Action)	**Интерфейс источника**	**Сеть источника**	**Интерфейс назначения**	**Сеть назначения**
Allow (или NAT)	lan	lannet	wan	ip_proxy
Allow	wan	ip_proxy	lan (или core)	lannet (или wan_ip)



IP-правила без включенной функции Record-Route отображены ниже, изменения, применяемые при использовании NAT снова отображены в круглых скобках «*(..)*».

Действие (Action)	**Интерфейс источника**	**Сеть источника**	**Интерфейс назначения**	**Сеть назначения**
Allow (или NAT)	lan	lannet	wan	<All possible IPs>
Allow	wan	<All possible IPs>	lan (или core)	lannet (or ipwan)

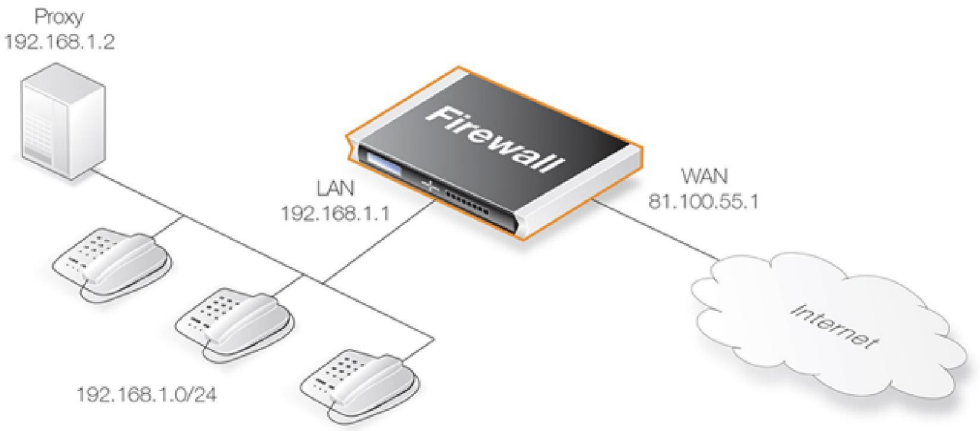
Преимущества использования функции *Record-Route* очевидны, так как сеть назначения для исходящего трафика и сеть источника для входящего трафика содержат все возможные IP-адреса.

Примечание: Объект Служба для IP-правил

*В данном разделе, таблицы со списками IP-правил, отображенными выше, пропускают объект **Служба**, связанный с правилом. Тот же пользовательский объект Служба используется для всех сценариев SIP.*

Сценарий 2
Защита proxy-серверов и локальных клиентов – Proxy-сервер находится в той же сети, что и клиенты

Основной целью данного сценария является защита локальных клиентов, а также SIP proxy-сервера. Proxy-сервер расположен в той же локальной сети, что и клиенты, с сигнализацией SIP потоком медиа-данных, проходящем через два интерфейса. Данный сценарий проиллюстрирован ниже.



Данный сценарий выполняется двумя способами:

- С применением NAT для скрытия топологии сети.
- Без применения NAT, таким образом, топология сети открыта.

Решение A – Использование NAT

В этом случае, proxy-сервер и локальные клиенты скрыты позади IP-адреса межсетевого экрана NetDefend. Выполните следующие шаги по установке:

1. Определите один объект SIP ALG, используя опции, описанные выше.
2. Определите объект *Служба*, связанный с объектом SIP ALG. Служба должна поддерживать:
   - **Порт назначения -** *5060* (по умолчанию сигнальный порт SIP)
   - **Тип -** *TCP/UDP*
3. Укажите 3 правила в наборе IP-правил:
   - *NAT*-правило для трафика, отправленного с локального прокси-сервера и клиентов во внутренней сети удаленным клиентам, находящимся, например, в сети Интернет. SIP ALG следит за передачей всех адресов, требуемой правилом *NAT*. Данная передача выполняется как на IP-уровне, так и на уровне приложений. Ни клиенты, ни proxy-серверы не должны быть осведомлены, что локальные пользователи натируются.
   - Если на SIP proxy-сервере включена функция *Record-Route*, сеть *источника* правила *NAT* может содержать только SIP proxy-сервер, и не может содержать локальных клиентов.
   - Правило *SAT* для перенаправления входящего SIP-трафика на приватный IP-адрес натированного локального proxy-сервера. Данное правило использует **core** в качестве интерфейса назначения (другими словами, NetDefendOS), так как входящий трафик будет отправлен на приватный IP-адрес SIP proxy-сервера.
   - Правило *Allow*, которое соответствует тому же типу трафика, что и правило *SAT* указанное в предыдущем пункте.

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundFrom ProxyUsers	NAT	lan	lannet	wan	all-nets
InboundTo ProxyAndClients	SAT SETDEST ip_proxy	wan	(ip_proxy)	core	wan_ip
InboundTo	Allow	wan	all-nets	core	wan_ip

ProxyAndClients					

Если функция *Record-Route* включена, то *Сеть назначения* для исходящего трафика от пользователей proxy-сервера может быть ограничена в правилах выше с помощью «*ip_proxy*».

При получении входящего вызова, SIP ALG придерживается правила *SAT* и перенаправит запрос SIP на proxy-сервер. Proxy-сервер, в свою очередь, перенаправит запрос конечному клиенту.

Если функция *Record-Route* выключена на proxy-сервере, в зависимости от статуса SIP-сессии, SIP ALG может перенаправить входящие SIP-сообщения непосредственно клиенту с игнорированием SIP proxy-сервера. Это происходит автоматически без дополнительных настроек.

Решение B – Без использования NAT

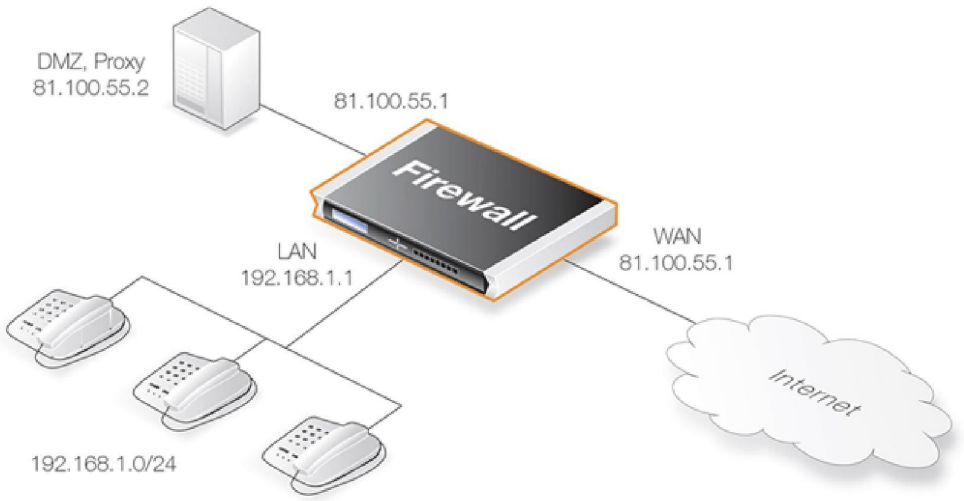
Если NAT не используется, правило *NAT* для исходящего трафика заменяется правилом *Allow*. Правило *SAT* для исходящего трафика и правила *Allow* заменяются одним правилом *Allow*.

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundFrom Proxy&Clients	Allow	lan	lannet (ip_proxy)	wan	all-nets
InboundTo Proxy&Clients	Allow	wan	all-nets	lan	lannet (ip_proxy)

Если функция *Record-Route* включена, то сети в правилах указанных выше могут быть дополнительно ограничены с помощью «*(ip_proxy)*» как указано в таблице.

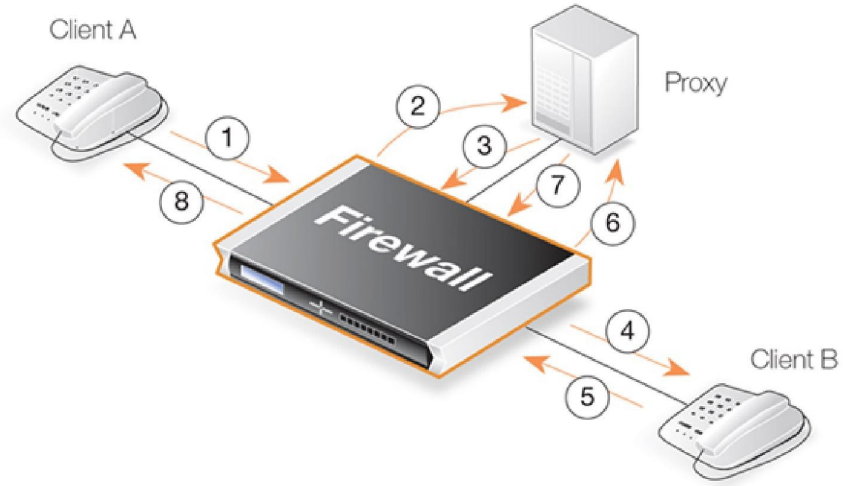
Сценарий 3
Защита proxy-сервера и локальных клиентов – Proxy-сервер подключен к интерфейсу DMZ

Данный сценарий аналогичен предыдущему, за исключением расположения локального SIP proxy-сервера. Сервер работает на отдельном интерфейсе и подключен к локальной сети. Эта установка увеличивает уровень безопасности, так как передача данных по протоколу SIP не осуществляется напрямую между удаленной конечной точкой и локальным, защищенным клиентом.



В данном сценарии уровень сложности выше, так как поток SIP-сообщений проходит через три

интерфейса: интерфейс, получающий звонок от инициатора соединения, DMZ интерфейс, взаимодействующий с proxy-сервером и интерфейс назначения, взаимодействующий с терминатором звонка. Первоначальный обмен сообщениями представлен на рисунке ниже:



Обмен сообщениями выглядит следующим образом:

- **1,2** – Запрос *INVITE* отправляется на локальный proxy-сервер, находящийся в зоне DMZ.
- **3,4** – proxy-сервер отправляет сообщения SIP по адресу назначения в сети Интернет.
- **5,6** – Удаленный клиент или proxy-сервер отвечает локальному proxy-серверу.
- **7,8** – Локальный proxy-сервер пересылает ответ локальному клиенту.

Сценарий может быть выполнен с установкой, скрывающей топологию с зоной DMZ (представленное ниже **Решение A**), а также с установкой без использования NAT (представленное ниже **Решение B**).

Решение A - Использование NAT

Для данного типа установки следует учитывать следующее:

- IP-адрес SIP proxy-сервера должен быть глобально маршрутизируемым. Межсетевой экран NetDefend не поддерживает скрытие proxy-сервера в зоне DMZ.
- IP-адрес интерфейса DMZ должен быть глобально маршрутизируемым. Этот адрес может быть тем же, что и используемый на внешнем интерфейсе.

Выполните следующие шаги по установке:

1. Определите один объект SIP ALG, используя опции, представленные выше.
2. Определите объект *Служба*, связанный с объектом SIP ALG. У службы должны быть:

- **Порт назначения** – *5060* (по умолчанию сигнальный порт SIP)
- **Тип** – *TCP/UDP*

3. Укажите 4 правила в наборе IP-правил:

- Правило *NAT* для исходящего трафика, направленного от клиентов, находящихся во внутренней сети, на proxy-сервер, подключенный к интерфейсу DMZ. SIP ALG следит за трансляцией всех адресов по правилу *NAT*. Данная передача выполняется как на IP-уровне, так и на уровне приложений.

Примечание

Контактным адресом клиентов, зарегистрированных на proxy-сервере в зоне DMZ, будет IP-адрес DMZ-интерфейса.

• Правило *Allow* для исходящего трафика, отправленного от proxy-сервера, находящегося позади DMZ-интерфейса, удаленным клиентам в сети Интернет.

• Правило *Allow* для входящего SIP-трафика, направленного от SIP proxy-сервера, находящегося позади DMZ-интерфейса, на IP-адрес межсетевого экрана NetDefend. Данное правило использует интерфейс **core** в качестве интерфейса назначения.

Причиной этого является правило *NAT*, указанное выше. При получении входящего вызова, NetDefendOS автоматически определяет локального получателя, выполняет передачу адреса и перенаправляет SIP-сообщения получателю. Это выполняется на основе статуса внутреннего SIP ALG.

• Правило *Allow* для входящего трафика, направленного, например, из сети Интернет, на proxy-сервер, находящийся позади DMZ.

4. Если на proxy-сервере **выключена** функция *Record-Route,* необходимо разрешить прямой обмен сообщениями между клиентами с игнорированием proxy-сервера. При отключенной функции *Record-Route* требуются два следующих дополнительных правила:

• Правило *NAT* для исходящего трафика, направленного от клиентов, находящихся во внутренней сети, к внешним клиентам и proxy-серверам, например, в сети Интернет. SIP ALG следит за преобразованием всех адресов в соответствии с правилом *NAT*. Преобразование выполняется как на IP-уровне, так и на уровне приложений.

• Правило *Allow* для входящего SIP-трафика, направленного, например, из сети Интернет на IP-адрес DMZ-интерфейса. Необходимо добавить это правило, так как локальные клиенты будут натированы с использованием IP-адреса DMZ-интерфейса, когда они регистрируются с proxy-сервером, расположенным в зоне DMZ.

Данное правило использует интерфейс **core** в качестве интерфейса назначения. При получении входящего вызова, система NetDefendOS использует регистрационную информацию локального получателя для автоматического определения этого получателя, выполнения преобразования адреса и перенаправления SIP-сообщений получателю. Это выполняется на основе внутреннего статуса SIP ALG.

При включенной функции *Record-Route* требуются следующие IP-правила:

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundToProxy	NAT	lan	lannet	dmz	ip_proxy
OutboundFromProxy	Allow	dmz	ip_proxy	wan	all-nets
InboundFromProxy	Allow	dmz	ip_proxy	core	dmz_ip
InboundToProxy	Allow	wan	all-nets	dmz	ip_proxy

Если функция *Record-Route* выключена, необходимо добавить следующие IP-правила:

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundBypassProxy	NAT	lan	lannet	wan	all-nets
InboundBypassProxy	Allow	wan	all-nets	core	ipdmz

Решение B – Без использования NAT

Выполните следующие шаги по установке:

1. Определите один объект SIP ALG, используя опции, описанные выше.
2. Определите объект *Служба*, связанный с объектом SIP ALG. У объекта службы должны быть:
   - **Порт назначения -** *5060* (по умолчанию сигнальный порт SIP)
   - **Тип** - *TCP/UDP*
3. Укажите 4 правила в наборе IP-правил:
   - Правило *Allow* для исходящего трафика, направленного от клиентов во внутренней сети на proxy-сервер, подключенный к DMZ-интерфейсу.
   - Правило *Allow* для исходящего трафика, направленного от proxy-сервера, находящегося позади DMZ-интерфейса, удаленным клиентам в сети Интернет.
   - Правило *Allow* для входящего SIP-трафика от SIP proxy-сервера позади DMZ-интерфейса клиентам в локальной, защищенной сети.
   - Правило *Allow* для входящего SIP-трафика от клиентов и proxy-серверов в сети Интернет на proxy-сервер позади DMZ-интерфейса.
4. Еси на proxy-сервере выключена функция *Record-Route*, необходимо разрешить прямой обмен SIP-сообщениями между клиентами без игнорирования proxy-сервера. При отключенной функции *Record-Route* требуются два следующих дополнительных правила:
   - Правило *Allow* для исходящего трафика от клиентов в локальной сети внешним клиентам и proxy-серверам в сети Интернет.
   - Правило *Allow* для входящего SIP-трафика из сети Интернет клиентам в локальной сети.

При включенной функции *Record-Route* требуются следующие IP-правила:

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundToProxy	Allow	lan	lannet	dmz	ip_proxy
OutboundFromProxy	Allow	dmz	ip_proxy	lan	lannet
InboundFromProxy	Allow	dmz	ip_proxy	core	dmz_ip
InboundToProxy	Allow	wan	all-nets	dmz	ip_proxy

Если функция *Record-Route* выключена, то необходимо добавить следующие IP-правила:

	Действие (Action)	**Интерфейс источника (Src Interface)**	**Сеть источника (Src Network)**	**Интерфейс назначения (Dest Interface)**	**Сеть назначения (Dest Network)**
OutboundBypassProxy	Allow	lan	lannet	wan	all-nets
InboundBypassProxy	Allow	wan	all-nets	lan	lannet

6.2.9. H.323 ALG

Стандарт H.323 – это набор протоколов, разработанный Международным Союзом Телекоммуникаций (International Telecommunication Union, ITU) для организации видеоконференций

в IP-сетях. Стандарт H.323 используется для передачи аудио, видеоданных в режиме реального времени в сетях, действующих на основе механизма передачи пакетов, например, сети Интернет. H.323 определяет компоненты, протоколы и операции для передачи мультимедиа, включая IP-телефонию и voice-over-IP (VoIP).

Компоненты H.323

H.323 состоит из 4-х основных компонентов:

Терминалы (Terminals)	Устройства, используемые для передачи аудио и видео, такие как телефоны, средства проведения видеоконференций, например, программа "NetMeeting".
Шлюзы (Gateways)	Предназначены для организации соединения между сетями H.323 и другими сетями, например, Телефонной Сетью Общего Пользования (PSTN), обеспечивая передачу данных по протоколам и преобразование потоков медиа-данных. Для установки соединения между двумя терминалами H.323 шлюз не требуется.
Привратники (Gatekeepers)	Привратник – это компонент в системе H.323, который используется для адресации, авторизации и аутентификации терминалов и шлюзов. Привратник также поддерживает функции управления полосой пропускания, учетными данными, составлением счетов и балансом загрузки. Привратник может разрешить звонки непосредственно между конечными точками или может маршрутизировать сигнализацию вызова через себя для того, чтобы выполнить такие функции как Follow-me/find-me, Forward on busy и т.д. Это требуется при наличии более одного терминала H.323 позади натирующего устройства только с одним публичным IP-адресом.
Серверы многосторонней конференции (Multipoint Control Units)	Серверы многосторонней конференции (MCUs) обеспечивают связь трех или более H.323 терминалов. Всем терминалам H.323, участвующим в конференции, необходимо установить соединение с сервером многосторонней конференции. Сервер многосторонней конференции управляет звонками, ресурсами, видео и аудио-кодеками, используемыми при совершении звонка.

Протоколы H.323

Для реализации H.323 используются различные протоколы:

H.225 RAS signalling and Call Control (Setup) signalling	Используется для сигналов вызова. Также используется для установления соединения между двумя конечными точками H.323. Данный канал сигнала вызова открывается между двумя конечными точками H.323 или между конечной точкой H.323 и привратником. Для организации передачи данных между двумя конечными точками H.323, используется TCP-порт 1720. При подключении к привратнику используется UDP-порт 1719 (RAS-сообщения H.225).
H.245 Media Control and Transport	Обеспечивает управление мультимедийными сессиями, установленными между двумя конечными точками H.323.

	Наиболее важная задача заключается в согласовании открытия и закрытия логических каналов. Логическим каналом может быть, например, канал, используемый для передачи аудио. Во время согласования каналы, используемые для передачи видео и данных по протоколу T.120 также называются логическими каналами.
T.120	Набор протоколов приложений и коммуникации. В зависимости от типа продукта H.323, T.120 может использоваться для совместного применения приложений, передачи файлов, а также для функций, обеспечивающий проведение конференций, например, функция White board (Электронная доска).

Функции H.323 ALG

H.323 ALG представляет собой шлюз уровня приложения, который позволяет устройствам H.323, таким как телефоны H.323 и приложения, выполнять и принимать вызовы между друг другом при подключении через приватные сети, защищенные межсетевыми экранами NetDefend.

Стандарт H.323 не был предназначен для работы с NAT, так как IP-адреса и порты отправляются в полезную нагрузку сообщений H.323. H.323 ALG переадресовывает и передает сообщения H.323, чтобы убедиться, что они будут направлены на корректный адрес назначения и им будет разрешено проходить через межсетевой экран NetDefend.

H.323 ALG поддерживает следующие функции:

• H.323 ALG поддерживает версию 5 спецификации H.323. Данная спецификация основана на H.225.0 v5 и H.245 v10.

• Помимо голосовых и видео-вызовов, H.323 ALG поддерживает обмен приложениями по протоколу T.120. Для передачи данных протокол T.120 использует TCP, а для передачи голоса и видео – UDP.

• Для поддержки привратников ALG осуществляет мониторинг RAS-трафика между конечными точками H.323 и привратником для того, чтобы корректно настроить прохождение вызовов через межсетевой экран NetDefend.

• Поддержка правил *NAT* и *SAT* позволяет клиентам и привратникам использовать приватные IP-адреса в сети позади межсетевого экрана NetDefend.

Настройка H.323 ALG

Конфигурация стандарта H.323 ALG может быть изменена в соответствии с различными вариантами использования. Настраиваемыми функциями являются:

• **Allow TCP Data Channels** – Данная функция обеспечивает согласование каналов передачи данных по протоколу TCP. Каналы передачи данных используются, например, протоколом T.120.

• **Number of TCP Data Channels** – Можно указать количество каналов для передачи данных по протоколу TCP.

• **Address Translation** – Можно указать **Network (Сеть)** для натированного трафика, разрешенного для передачи. **External IP (Внешний IP)** для **Network** – это IP-адрес, для которого применяется NAT. Если для внешнего IP-адреса установлено значение *Auto,* то выполняет автоматический поиск внешнего IP-адреса с помощью «route lookup».

• **Translate Logical Channel Addresses** – Как правило, эта функция всегда настроена. Если функция выключена, то передача адреса не будет выполняться по адресам логических каналов и администратору необходимо быть уверенным в IP-адресах и маршрутах, используемых в

определенном сценарии.

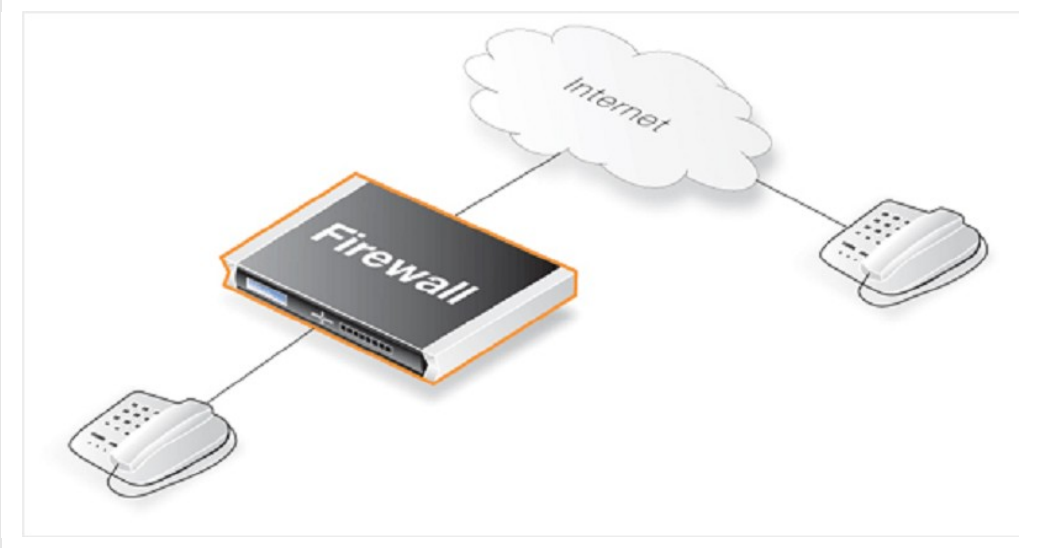
• **Gatekeeper Registration Lifetime** – Можно контролировать срок действия регистрации привратника для того, чтобы клиенты выполняли повторную регистрацию в течение определенного времени. Чем короче срок действия, тем чаще клиенты выполняют регистрацию привратника, тем самым снижая вероятность проблем, если сеть становится недоступной, и клиент думает, что все еще зарегистрирован.

Ниже представлены некоторые сетевые сценарии, в которых применяется H.323 ALG. Для каждого сценария представлен пример настройки ALG и правил. В сценариях используются три службы:

- Привратник (UDP ALL > 1719)
- H323 (H.323 ALG, TCP ALL > 1720)
- H323-привратник (H.323 ALG, UDP > 1719)

Пример 6.4. Защита телефонов позади межсетевых экранов NetDefend

В первом сценарии телефон H.323 подключен к межсетевому экрану NetDefend в сети (lannet) с публичными IP-адресами. Для того чтобы выполнить вызов с этого телефона на другой H.323 телефон в сети Интернет, а также разрешить H.323 телефонам в сети Интернет выполнять вызовы на этот телефон, необходимо настроить правила. В набор правил необходимо добавить следующие правила, убедитесь в отсутствии правил, запрещающих или разрешающих правил тот же тип трафика / портов.



Web-интерфейс

Правило для исходящих вызовов

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323AllowOut

• **Action:** Allow

• **Service:** H323

• **Source Interface:** lan

• **Destination Interface:** any

• **Source Network:** lannet

• **Destination Network:** 0.0.0.0/0 (all-nets)

• **Comment:** Allow outgoing calls

3. Нажмите **OK**

Правило для входящих вызовов:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323AllowOut

• **Action:** Allow

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** lan

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** lannet

• **Comment:** Allow incoming calls

3. Нажмите **OK**

Пример 6.5. H.323 с приватными IP-адресами

В этом сценарии телефон H.323 подключен к межсетевому экрану NetDefend в сети с приватными IP-адресами. Для того чтобы выполнить вызов с этого телефона на другой H.323 телефон в сети Интернет, а также разрешить H.323 телефонам в сети Интернет выполнять вызовы на этот телефон, необходимо настроить правила. В набор правил необходимо добавить следующие правила, убедитесь в отсутствии правил, запрещающих или разрешающих тот же тип трафика / портов. Так как в примере используются приватные IP-адреса, входящий трафик должен быть изменен с помощью SAT, как показано в примере ниже. Объект ip-телефон должен быть внутренним ip-телефоном H.323.

Web-интерфейс

Правило для исходящих вызовов

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323Out

• **Action:** NAT

• **Service:** H323

• **Source Interface:** lan

• **Destination Interface:** any

• **Source Network:** lannet

• **Destination Network:** 0.0.0.0/0 (all-nets)

• **Comment:** Allow outgoing calls

3. Нажмите **OK**

Правило для входящих вызовов:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** SAT

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

• **Comment:** Allow incoming calls to H.323 phone at ip-phone

3. Для **SAT** введите **Translate Destination IP Address**: To New IP Address: ip-phone (IP-адрес телефона)

4. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

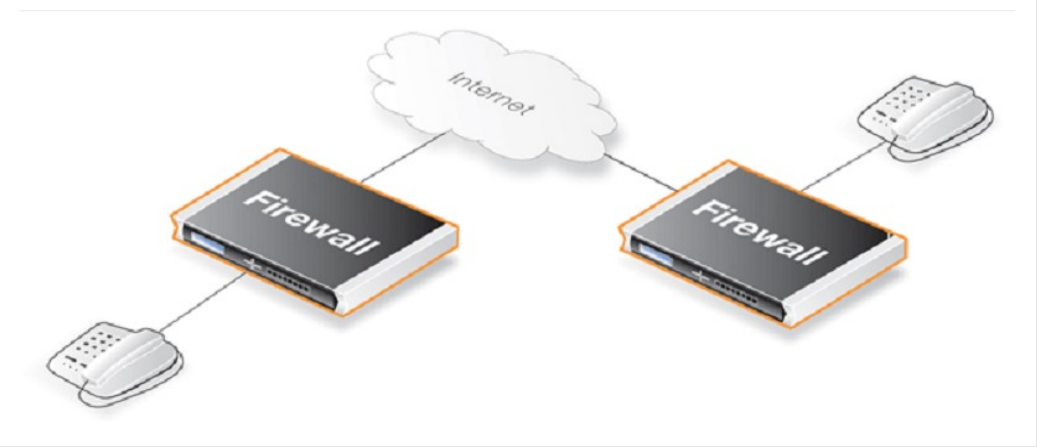
• **Comment:** Allow incoming calls to H.323 phone at ip-phone

3. Нажмите **OK**

Для того чтобы выполнить вызов на телефон позади межсетевого экрана NetDefend, необходимо послать вызов на внешний IP-адрес межсетевого экрана. Если позади межсетевого экрана NetDefend находится несколько телефонов H.323 ALG, то на каждом телефоне необходимо настроить правило *SAT*. Это означает, что используется несколько внешних адресов. Тем не менее, предпочтительнее использовать привратник H.323 по сценарию «H.323 with Gatekeeper», так как при этом требуется только один внешний адрес.

Пример 6.6. Два телефона позади различных межсетевых экранов

В этом сценарии участвуют два телефона H.323, каждый из которых подключен к межсетевому экрану NetDefend в сети с публичными IP-адресами. Для того чтобы осуществить вызов на эти телефоны в сети Интернет, необходимо добавить следующие правила на обоих межсетевых экранах. Убедитесь в отсутствии правил, запрещающих или разрешающих правил тот же тип трафика / портов.



Web-интерфейс

Правило для исходящих вызовов

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323AllowOut

• **Action:** Allow

• **Service:** H323

• **Source Interface:** lan

• **Destination Interface:** any

• **Source Network:** lannet

• **Destination Network:** 0.0.0.0/0 (all-nets)

• **Comment:** Allow outgoing calls

3. Нажмите **OK**

Правило для входящих вызовов:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323AllowIn

• **Action:** Allow

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** lan

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** lannet

• **Comment:** Allow incoming calls

3. Нажмите **OK**

Пример 6.7. Использование приватных IP-адресов

В этом сценарии участвуют два телефона H.323, каждый из которых подключен к межсетевому экрану NetDefend в сети с приватными IP-адресами. Для того чтобы позвонить на эти телефоны в сети Интернет, необходимо добавить следующие правила на межсетевом экране. Убедитесь в отсутствии правил, запрещающих или разрешающих правил тот же тип трафика / портов. Так как в примере используются приватные IP-адреса телефонов, входящий трафик необходимо изменить с помощью SAT, как в примере ниже. Объект ip-телефон должен быть внутренним ip-телефоном H.323.

Web-интерфейс

Правило для исходящих вызовов

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323Out

• **Action:** NAT

• **Service:** H323

• **Source Interface:** lan

• **Destination Interface:** any

• **Source Network:** lannet

• **Destination Network:** 0.0.0.0/0 (all-nets)

• **Comment:** Allow outgoing calls

3. Нажмите **OK**

Правило для входящих вызовов:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** SAT

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

• **Comment:** Allow incoming calls to H.323 phone at ip-phone

3. Для **SAT** введите **Translate Destination IP Address**: To New IP Address: ip-phone (IP-адрес телефона)

4. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

• **Comment:** Allow incoming calls to H.323 phone at ip-phone

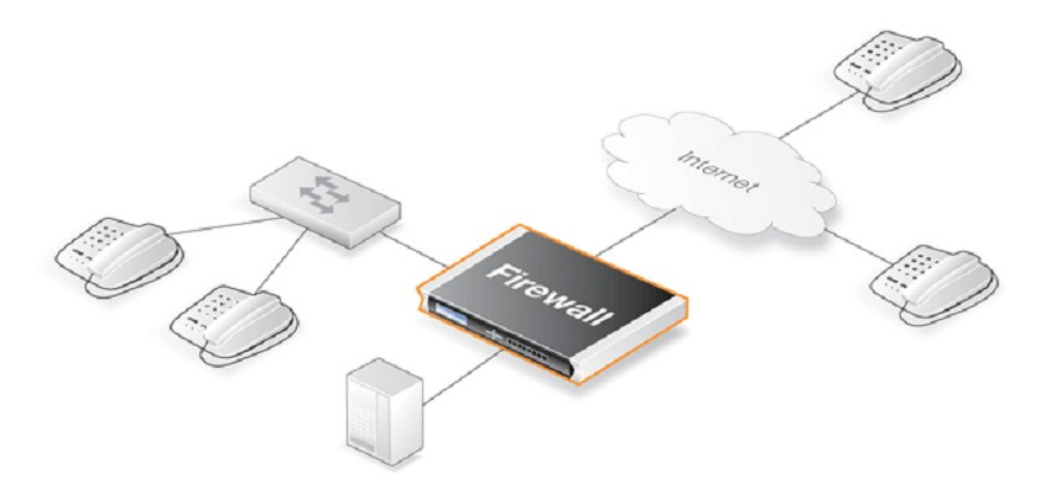
3. Нажмите **OK**

Для того чтобы выполнить вызов на телефон позади межсетевого экрана NetDefend, необходимо послать вызов на внешний IP-адрес межсетевого экрана. Если позади межсетевого экрана NetDefend находится несколько телефонов H.323 ALG, то на каждом телефоне необходимо настроить правило *SAT*. Это означает, что используется несколько внешних адресов. Тем не менее, предпочтительнее использовать привратник H.323 по сценарию «H.323 with Gatekeeper», так как при этом требуется только один внешний адрес.

Пример 6.8. H.323 привратник

В данном сценарии H.323 привратник помещается в зону DMZ межсетевого экрана NetDefend. Необходимо настроить правило на межсетевом экране, разрешающее прохождение трафика между приватной сетью, в которой телефоны H.323 подключены к внутренней сети и к привратнику в DMZ. У привратника приватный адрес.

Необходимо добавить следующие правила на обоих межсетевых экранах. Убедитесь в отсутствии правил, запрещающих или разрешающих правил тот же тип трафика / портов.



Web-интерфейс

Правило для исходящих вызовов

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** SAT

• **Service:** H323-Gatekeeper

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (external IP of the firewall)

• **Comment:** SAT rule for incoming communication with the Gatekeeper located at ip-gatekeeper

3. Для **SAT** введите **Translate Destination IP Address**: To New IP Address: ip-gatekeeper (IP-адрес привратника).

4. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

• **Comment:** Allow incoming communication with the Gatekeeper

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** dmz

• **Source Network:** lannet

• **Destination Network:** ip-gatekeeper (IP address of the gatekeeper)

• **Comment:** Allow incoming communication with the Gatekeeper

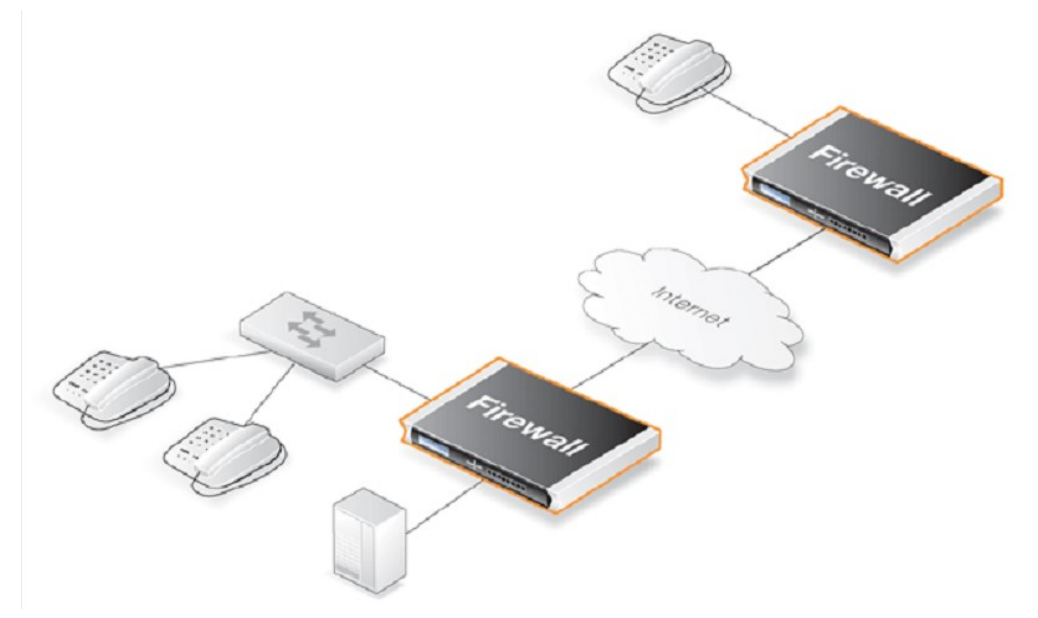
3. Нажмите **OK**

Примечание: Для исходящих вызовов не требуется определенное правило

Нет необходимости указывать определенное правило для исходящих вызовов. Система NetDefendOS выполняет мониторинг соединения между «внешними» телефонами и привратником, чтобы быть уверенным в том, что можно сделать звонок с внутренних телефонов на внешние телефоны, которые зарегистрированы с привратником.

Пример 6.9.

Этот сценарий аналогичен сценарию 3, с той разницей, что межсетевой экран NetDefend обеспечивает защиту "внешних" телефонов. Межсетевой экран NetDefend с привратником, подключенный к DMZ, должен быть настроен также как в сценарии 3. Другой межсетевой экран NetDefend должен быть настроен в соответствии с инструкциями, указанными ниже. Необходимо добавить следующие правила на межсетевом экране. Убедитесь в отсутствии правил, запрещающих или разрешающих правил тот же тип трафика / портов.



Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323Out

• **Action:** NAT

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** any

• **Source Network:** lannet

• **Destination Network:** 0.0.0.0/0 (all-nets)

• **Comment:** Allow outgoing communication with a gatekeeper

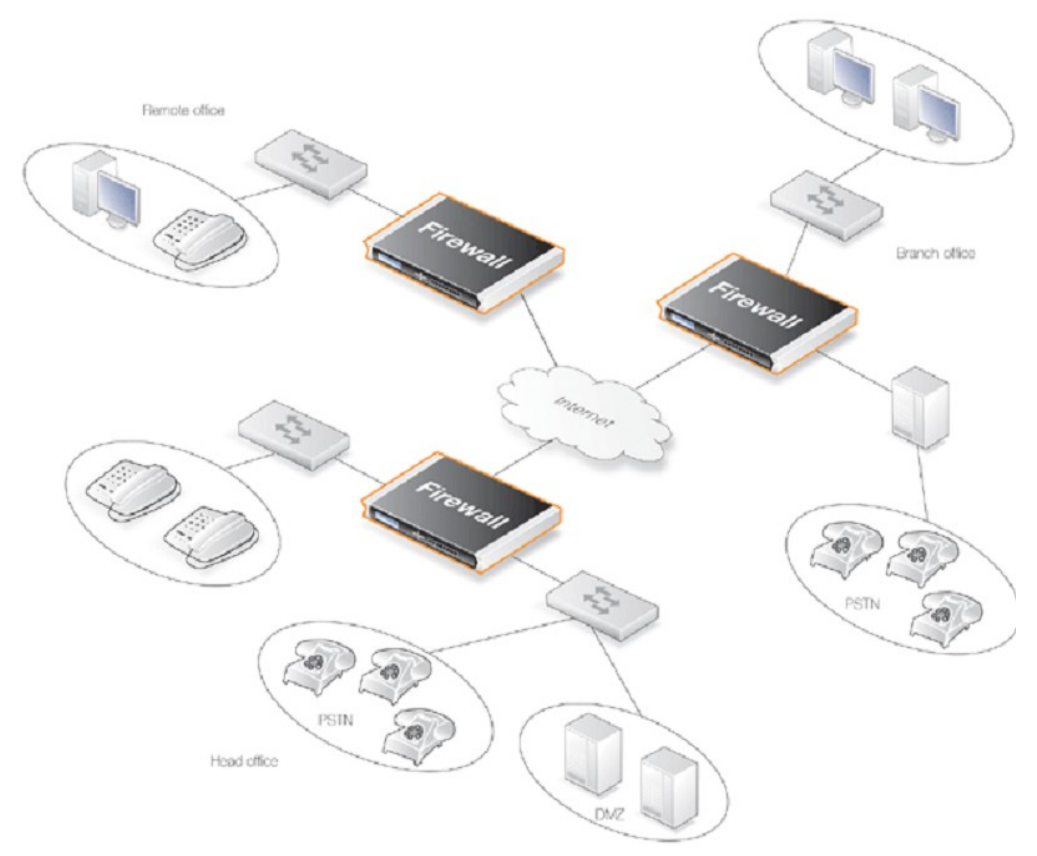
3. Нажмите **OK**

Примечание: Для исходящих вызовов не требуется определенное правило

Нет необходимости указывать определенное правило для исходящих вызовов. Система NetDefendOS выполняет мониторинг соединения между «внешними» телефонами и привратником, чтобы быть уверенным в том, что можно сделать звонок с внутренних телефонов на внешние телефоны, которые зарегистрированы привратником.

Пример 6.10. Использование H.323 ALG в корпоративных сетях

Этот сценарий является примером более сложной сети, которая отображает применение H.323 ALG в корпоративной среде. В главном офисе привратник H.323 в зоне DMZ может управлять всеми клиентами H.323, находящимися в главном офисе, филиалах и удаленных офисах. Это позволит целой корпорации использовать сеть для передачи голоса и совместного использования приложений. Предполагается, что VPN-туннели настроены корректно, и что все офисы используют диапазоны приватных IP-адресов в своих локальных сетях. Все "внешние" вызовы осуществляются через существующую телефонную сеть с использованием шлюза (IP-шлюз), подключенного к обычной телефонной сети.



Привратник H.323 расположен в главном офисе в зоне DMZ межсетевого экрана NetDefend. Этот межсетевой экран настроен следующим образом:

Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** LanToGK

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** dmz

• **Source Network:** lannet

• **Destination Network:** ip-gatekeeper

• **Comment:** Allow H.323 entities on lannet to connect to the Gatekeeper

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** LanToGK

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** dmz

• **Source Network:** lannet

• **Destination Network:** ip-gateway

• **Comment:** Allow H.323 entities on lannet to call phones connected to the H.323 Gateway on the DMZ

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** GWToLan

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** dmz

• **Destination Interface:** lan

• **Source Network:** ip-gateway

• **Destination Network:** lannet

• **Comment:** Allow communication from the Gateway to H.323 phones on lannet

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** BranchToGW

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** vpn-branch

• **Destination Interface:** dmz

• **Source Network:** branch-net

• **Destination Network:** ip-gatekeeper, ip-gateway

• **Comment:** Allow communication with the Gatekeeper on DMZ from the Branch network

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** BranchToGW

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** vpn-remote

• **Destination Interface:** dmz

• **Source Network:** remote-net

• **Destination Network:** ip-gatekeeper

• **Comment:** Allow communication with the Gatekeeper on DMZ from the Remotenetwork

3. Нажмите **OK**

Пример 6.11. H.323 для удаленных офисов

Если H.323 телефоны и приложения в филиалах и удаленных офисах настроены на использование привратника H.323 в главном офисе, межсетевые экраны NetDefend в удаленных офисах и филиалах должны быть настроены следующим образом: (это правило должно быть добавлено как на межсетевом экране филиала, так и на межсетевом экране удаленного офиса).

Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** ToGK

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** vpn-hq

• **Source Network:** lannet

• **Destination Network:** hq-net

• **Comment:** Allow communication with the Gatekeeper connected to the Head Office DMZ

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** any

• **Destination Interface:** core

• **Source Network:** 0.0.0.0/0 (all-nets)

• **Destination Network:** wan_ip (внешний IP-адрес межсетевого экрана)

• **Comment:** Allow incoming communication with the Gatekeeper

3. Нажмите **OK**

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** H323In

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** lan

• **Destination Interface:** dmz

• **Source Network:** lannet

• **Destination Network:** ip-gatekeeper (IP address of the gatekeeper)

• **Comment:** Allow incoming communication with the Gatekeeper

3. Нажмите **OK**

Пример 6.12. Разрешение регистрации H.323 шлюза привратником

H.323 привратник межсетевого экрана NetDefend, находящегося в филиале, подключен к DMZ. Для того чтобы разрешить шлюзу зарегистрироваться привратником H.323 в главном офисе, необходимо настроить следующее правило:

Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите:

• **Name:** GWToGK

• **Action:** Allow

• **Service:** H323-Gatekeeper

• **Source Interface:** dmz

• **Destination Interface:** vpn-hq

• **Source Network:** ip-branchgw

• **Destination Network:** hq-net

• **Comment:** Allow the Gateway to communicate with the Gatekeeper connected to the Head Office

3. Нажмите **OK**

Примечание: Для исходящих вызовов не требуется определенное правило

Нет необходимости указывать определенное правило для исходящих вызовов. Система NetDefendOS выполняет мониторинг соединения между «внешними» телефонами и привратником, чтобы быть уверенным в том, что можно сделать звонок с внутренних телефонов на внешние телефоны, которые зарегистрированы привратником.

6.2.10. TLS ALG

Обзор

Протокол *TLS (Transport Layer Security)* - это протокол, обеспечивающий защищенную передачу данных в публичной сети Интернет между двумя конечными точками путем шифрования, а также за счет аутентификации конечной точки.

Как правило, в сценарии TLS клиент/сервер перед началом установки зашифрованного соединения выполняется только аутентификация сервера. TLS часто применяется в случае, когда Web-браузер подключается к серверу, использующему TLS, например, когда клиенту требуется онлайн-доступ к

банковским услугам. Иногда это носит название HTTPS-соединение и часто обозначается значком замка, появляющимся в навигационной панели браузера.

TLS представляет собой удобное и простое решение для безопасного доступа клиентов к серверам и позволяет избежать сложностей, связанных с другими решениями VPN, например, использование IPsec. Большинство Web-браузеров поддерживают TLS и поэтому пользователи могут легко получить защищенный доступ к серверу без дополнительного программного обеспечения.

Связь с SSL

TLS является преемником протокола *Secure Sockets Layer* (SSL), но содержит небольшие отличия. Таким образом, в большинстве случаев протоколы TLS и SSL можно рассматривать как эквиваленты. Применительно к TLS ALG можно сказать, что межсетевой экран NetDefend обеспечивает *SSL терминацию (SSL termination)*, так как он действует в качестве конечной точки SSL.

Что касается поддерживаемых стандартов SSL и TLS, NetDefendOS обеспечивает терминацию для SSL 3.0, а также для TLS 1.0, в соответствии с директивой RFC 2246, определяющей поддержку TLS 1.0 (если на стороне сервера NetDefendOS поддерживается директива RFC 2246).

TLS на основе сертификатов

Протокол безопасности TLS основан на использовании цифровых сертификатов, которые присутствуют на стороне сервера и отправляются клиентам в начале сессии TLS с целью идентификации сервера, а затем используются как основа шифрования. На сервере могут использоваться доверенные сертификаты (Certificate Authority (CA)), в этом случае Web-браузер клиента будет автоматически определять срок действия сертификата.

Самозаверяющие сертификаты могут использоваться на сервере вместо сертификатов CA. В таком случае, Web-браузер клиента будет уведомлять пользователя о том, что подлинность сертификата не установлена и пользователю придется настроить браузер на принятие сертификата и продолжить.

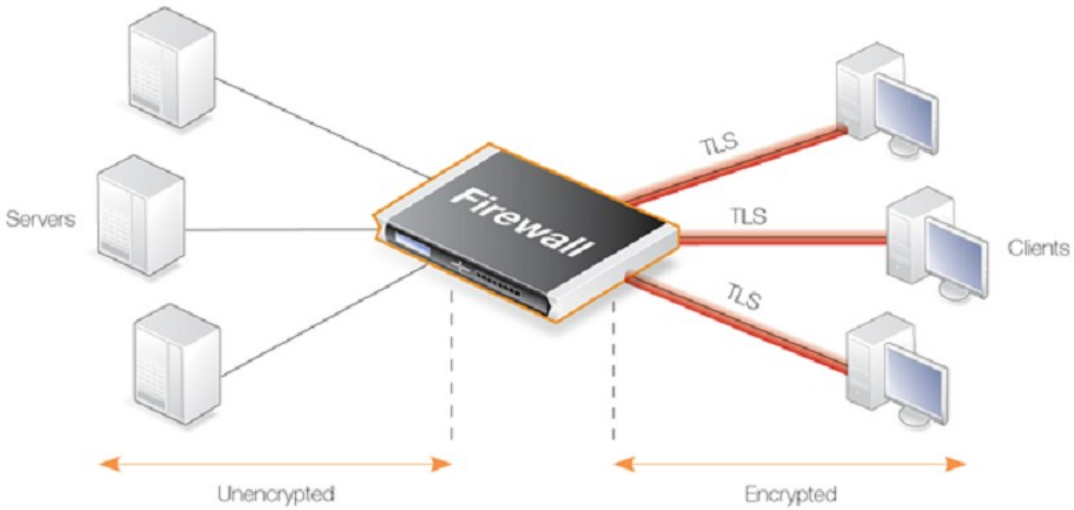


Рис. 6.7 TLS Терминация

Преимущества использования системы NetDefendOS для TLS терминации

Протокол TLS может быть реализован непосредственно на сервере, к которому подключаются клиенты, однако, если серверы находятся под защитой позади межсетевого экрана NetDefend, то система NetDefendOS может взять на себя роль конечной точки TLS. Далее система NetDefendOS выполняет TLS аутентификацию и шифрование отправленных/полученных данных, а также

передачу незашифрованных данных, отправленных на сервер или полученных с сервера. Преимущества этого подхода следующие:

• Поддержка TLS может быть централизована в межсетевом экране NetDefend вместо установки на отдельных серверах.

• Можно централизованно управлять сертификатами на межсетевом экране NetDefend, а не на отдельных серверах. Нет необходимости в том, чтобы уникальные сертификаты (или один «wildcard certificate») присутствовали на каждом сервере.

• Дополнительная обработка шифрования / дешифрования, необходимая TLS, может быть выполнена на межсетевом экране NetDefend. Эту обработку иногда называют *SSL acceleration*. Любые полученные преимущества обработки могут изменяться и будут зависеть от возможностей обработки, поддерживаемых серверами и межсетевым экраном NetDefend.

• Расшифрованный TLS-трафик может быть объектом для других функций NetDefendOS, таких как traffic shaping или поиск потенциальных угроз для сервера с помощью IDP-сканирования.

• Протокол TLS может быть объединен с функцией балансировки нагрузки сервера (server load balancing) системы NetDefendOS для обеспечения передачи трафика между серверами.

Включение TLS

Для того чтобы включить протокол TLS в NetDefendOS выполните следующие шаги:

1. Загрузите в NetDefendOS корневые сертификаты и сертификаты хоста для их использования TLS-протоколом.

2. Определите новый объект TLS ALG, соответствующие корневые сертификаты и сертификаты хоста. Если сертификат самозаверяющий, то корневой сертификат и сертификат хоста должны быть одинаковыми.

3. Создайте новый объект *Служба* на основе TCP-протокола.

4. Далее необходимо связать объект TLS ALG с недавно созданным объектом Служба.

5. Создайте IP-правило *NAT* или *Allow* для целевого трафика и свяжите объект службы с ним.

6. Дополнительно можно создать правило *SAT*, чтобы изменить порт назначения для незашифрованного трафика. В качестве альтернативы для балансировки нагрузки можно использовать правило *SLB_SAT* (порт назначения также может быть изменен с помощью пользовательского объекта службы).

URL-адреса, рассылаемые серверами

Следует отметить, что использование NetDefendOS для терминации TLS не изменит URL-адреса Web-страниц, рассылаемые серверами, которые находятся позади межсетевого экрана NetDefend.

Это означает, что если клиент подключается к Web-серверу, который находится позади межсетевого экрана NetDefend, используя протокол https://, то любые Web-страницы, переданные обратно, содержащие абсолютные URL-адреса, включающие протокол http:// (возможно, для ссылки на другие страницы того же сайта), не будут иметь этих URL-адресов, так как они преобразованы системой NetDefendOS в https://. Для решения этого вопроса серверы должны использовать относительные URL-адреса, а не абсолютные

Шифровка, поддерживаемая NetDefendOS TLS

NetDefendOS TLS поддерживает следующие наборы шифров:

1. TLS_RSA_WITH_RC4_128_SHA.

2. TLS_RSA_WITH_RC4_128_MD5.

3. TLS_RSA_EXPORT_WITH_RC4_56_SHA (размер сертифицированного ключа до 1024 бит).

4. TLS_RSA_EXPORT_WITH_RC4_40_MD5 (размер сертифицированного ключа до 1024 бит).

5. TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (размер сертифицированного ключа до 1024 бит).

6. TLS_RSA_WITH_NULL_MD5.

7. TLS_RSA_WITH_NULL_SHA.

Ограничения NetDefendOS TLS

Как указано выше, NetDefendOS TLS обеспечивает поддержку терминации только со стороны сервера. Также следует отметить следующие ограничения:

- Отсутствие поддержки аутентификации клиента (межсетевой экран NetDefend аутентифицирует подлинность клиента).

- Отсутствие поддержки пересогласования

- Отправка сообщений обмена ключами не поддерживается, это означает, что ключ в сертификате должен быть достаточно слабым, чтобы использовать экспорт шифров.

- Используемая системой NetDefendOS цепочка сертификатов может содержать не более 2 сертификатов.

6.3. Фильтрация Web-содержимого

6.3.1. Обзор

Web-трафик является одним из крупнейших источников нарушения безопасности и неправомерного использования сети Интернет. Просмотр Web-страниц может стать причиной угрозы безопасности сети. Производительность и пропускная способность Интернет-каналов также может быть нарушена.

Механизмы фильтрации

С помощью HTTP ALG система NetDefendOS применяет следующие механизмы фильтрации сомнительного Web-содержимого:

- Функция Active Content Handling может использоваться для фильтрации Web-страниц с содержимым, рассматриваемым администратором как потенциальная угроза, например, объекты ActiveX и Java Applets.

- С помощью функции Static Content Filtering (Фильтрация статического содержимого) можно вручную классифицировать Web-сайты на разрешенные и запрещенные. Эта функция также

известна как «белый/черный список» URL-адресов.

• Dynamic Content Filtering (Фильтрация динамического содержимого) – это эффективная функция, позволяющая администратору разрешать или блокировать доступ к Web-сайтам в зависимости от категории их классификации, выполненной службой автоматической классификации. Фильтрация динамического содержимого требует минимум усилий администратора и обеспечивает высокую точность.

Примечание: Включение WCF

Фильтрация всего Web-содержимого включается через HTTP ALG, подробное описание данной функции представлено в Разделе 6.2.2. «HTTP ALG».

6.3.2.Обработка активного содержимого

Web-содержимое может содержать вредоносный код, предназначенный для нанесения вреда рабочей станции или сети. Как правило, такой код встроен в различные типы объектов или файлы, которые встроены в Web-страницы.

Система NetDefendOS поддерживает возможность удаления следующих типов объектов из содержимого Web-страниц:

- Объекты ActiveX (включая Flash)
- Java applets
- Код Javascript/VBScript
- Cookies
- Некорректное отображение символов при использовании кодировки UTF-8 (некорректное отображение URL-адресов может использоваться для атаки на Web-серверы)

Типы объектов, которые следует удалить, могут быть выбраны индивидуально путем настройки соответствующего HTTP Application Layer Gateway.

Предупреждение: Последствия удаления объектов

Перед удалением любых типов объектов из Web-содержимого следует проявлять особое внимание. Многие Web-сайты используют Javascript и другие типы кодов на стороне клиента, и в большинстве случаев код не является вредоносным. Типичными примерами этого являются scripting, используемые для реализации выпадающих меню, а также скрытия и отображения элементов на Web-страницах. В лучшем случае, удаление таких законных кодов может стать причиной повреждений Web-сайта, а в худшем - полное прекращение работы браузера. По этой причине функция Active Content Handling должна быть использована только при четко выясненных последствиях удаления объектов.

Пример 6.13. Выключение ActiveX и Java applets

В данном примере демонстрируется, как настроить HTTP Application Layer Gateway на выключение ActiveX и Java applets. В примере используется объект content_filtering ALG и предполагается выполнение пользователем одного из предыдущих примеров.

CLI

```
gw-world:/> set ALG ALG_HTTP content_filtering
                        RemoveActiveX=Yes RemoveApplets=Yes
```

Web-интерфейс

1. Зайдите **Objects > ALG**
2. В таблице нажмите на объект HTTP ALG, content_filtering
3. Выберите управление **Strip ActiveX objects (включая flash)**
4. Выберите управление **Strip Java applets**
5. Нажмите **OK**

6.3.3. Фильтрация статического содержимого

С помощью HTTP ALG система NetDefendOS может блокировать или разрешать доступ к определенным Web-страницам на основе списков URL-адресов, которые носят название «черные/белые списки». Этот тип фильтрации также известен как *Static Content Filtering*. Функции фильтрации статического содержимого является отличным инструментом и помогает принимать решения относительно того, разрешить или заблокировать доступ.

Порядок фильтрации статического и динамического содержимого

Функция фильтрации статического содержимого выполняется перед функцией фильтрации динамического содержимого (описана ниже), предоставляющей возможность вручную вносить исключения в процессе автоматической классификации динамического содержимого. В случае, когда товары приобретаются в определенном магазине on-line, с помощью функции фильтрации динамического содержимого можно заблокировать доступ на подобные сайты путем внесения в категорию блокировки «Покупка товаров». При добавлении URL-адреса сайта магазина в «белый список» HTTP Application Layer Gateway, доступ к сайту с данным URL-адресом всегда разрешен, превосходя функцию фильтрации динамического содержимого.

Метод подстановки (Wildcarding)

И черный, и белый списки URL-адресов поддерживают метод подстановки URL-адреса для обеспечения наибольшей гибкости использования. Этот метод также применим к имени пути в URL-адресе хоста, что означает, что фильтрацией можно управлять на уровне файлов и папок.

Ниже приведены корректные и некорректные примеры использования URL-адресов в «черном списке»:

.example.com/	Корректно. Блокировка всех хостов в домене example.com и всех Web-страниц, используемых этими хостами.
www.example.com/*	Корректно. Блокировка Web-сайтов www.example.com и всех Web-страниц.
***/*.gif**	Корректно. Блокировка всех файлов с расширением .gif.
www.example.com	Некорректно. Блокировка только первого запроса доступа на Web-сайт. Доступ, например на www.example.com/index.html, не будет заблокирован.
example.com/	Некорректно. Блокировка доступа на www.myexample.com, так как будет запрещен доступ на все сайты, имя которых заканчивается на example.com.

Примечание: Добавление хостов и сетей в «черный список» является отдельным действием

Фильтрация Web-содержимого на основе «черного списка» URL-адресов является отдельным действием, представленным в Разделе

6.7, «Черный список хостов и сетей».

Пример 6.14. Настройка «черного/белого списков»

Этот пример отображает использование функции фильтрации статического содержимого, с помощью которой система NetDefendOS может блокировать или разрешать доступ на определенные Web-страницы на основе «черных и белых списков».

В этой небольшом сценарии пользователям запрещена загрузка .exe-файлов. Тем не менее, Web-сайт D-Link предоставляет необходимые программные файлы, которые должны быть разрешены для загрузки.

CLI

Начните с добавления HTTP ALG для фильтрации HTTP-трафика:

```
gw-world:/> add ALG ALG_HTTP content_filtering
```

Затем создайте HTTP ALG URL для настройки “черного списка»:

```
gw-world:/> cc ALG ALG_HTTP content_filtering

gw-world:/content_filtering> add ALG_HTTP_URL
                         URL=*/*.exe
                         Action=Blacklist
```

В довершение ко всему, создайте «белый список»:

```
gw-world:/content_filtering> add ALG_HTTP_URL
                         URL=www.D-Link.com/*.exe
                         Action=Blacklist
```

Web-интерфейс

Начните с добавления HTTP ALG для фильтрации HTTP-трафика:

1. Зайдите **Objects > ALG > Add > HTTP ALG**

2. Введите подходящее имя для ALG, например, *content_filtering*

3. Нажмите **OK**

Затем создайте HTTP ALG URL для настройки «черного списка»:

1. Зайдите **Objects > ALG**

2. В таблице выберите недавно созданный HTTP ALG для просмотра его свойств

3. Нажмите вкладку HTTP URL

4. Нажмите **Add** и выберите в меню HTTP ALG URL

5. Выберите **Blacklist** как **Action**

6. Введите ***/*.exe** в текстовом поле URL

7. Нажмите **OK**

В довершение ко всему создайте «белый список»:

1. Зайдите **Objects > ALG**

2. В таблице выберите недавно созданный HTTP ALG для просмотра его свойств

3. Нажмите вкладку HTTP URL

4. Нажмите **Add** и выберите в меню HTTP ALG URL

5. Выберите **Whitelist** как **Action**

6. В текстовом поле URL введите www.D-Link.com/*.exe

7. Нажмите **OK**

Продолжайте добавление «черных/белых списков», пока фильтр отвечает требованиям.

6.3.4. Фильтрация динамического Web-содержимого

6.3.4.1.Обзор

В рамках HTTP ALG, NetDefendOS поддерживает функцию фильтрации динамического Web-содержимого (WCF), что позволяет администратору разрешать или блокировать доступ на Web-страницы на основе содержания данных Web-страниц.

Базы данных функции Dynamic WFC

Функция Dynamic WCF системы NetDefendOS позволяет автоматически блокировать Web-страницы, поэтому нет необходимости предварительно вручную указывать заблокированные или разрешенные URL-адреса. Вместо этого, D-Link поддерживает глобальную инфраструктуру баз данных, содержащих огромное количество URL-адресов Web-сайтов, которые уже классифицированы и сгруппированы в различные категории, такие как покупка товаров, новости, спорт, информация, предназначенная только для взрослых и т.д.

Базы данных URL-адресов обновляются практически ежечасно, при этом самые старые, недействительные URL-адреса удаляются. Объем URL-адресов в базах данных носит глобальный характер, охватывая Web-сайты на различных языках, и размещается на серверах, расположенных в различных странах.

Примечание: Функция Dynamic WCF доступна только на некоторых моделях межсетевых экранов NetDefend

Функция Dynamic WCF доступна только на следующих моделях межсетевых экранов NetDefend: DFL-260, 860, 1660, 2560 и 2560G.

WCF Processing Flow

Когда пользователь с помощью Web-браузера запрашивает доступ к Web-сайту, система NetDefendOS отправляет запрос в базу данных Dynamic WCF с целью выяснения категории запрашиваемого сайта. Далее доступ к сайту может быть разрешен или запрещен на основе его категории.

Если доступ запрещен, пользователь получает Web-страницу, уведомляющую, что запрашиваемый сайт заблокирован. Для ускорения поиска система NetDefendOS использует локальную кэш-память, в которой хранятся недавно запрошенные URL-адреса. Кэширование может быть очень эффективно, так как данный пользователь сообщества, такого, как группа студентов, часто просматривает ограниченный круг Web-сайтов.

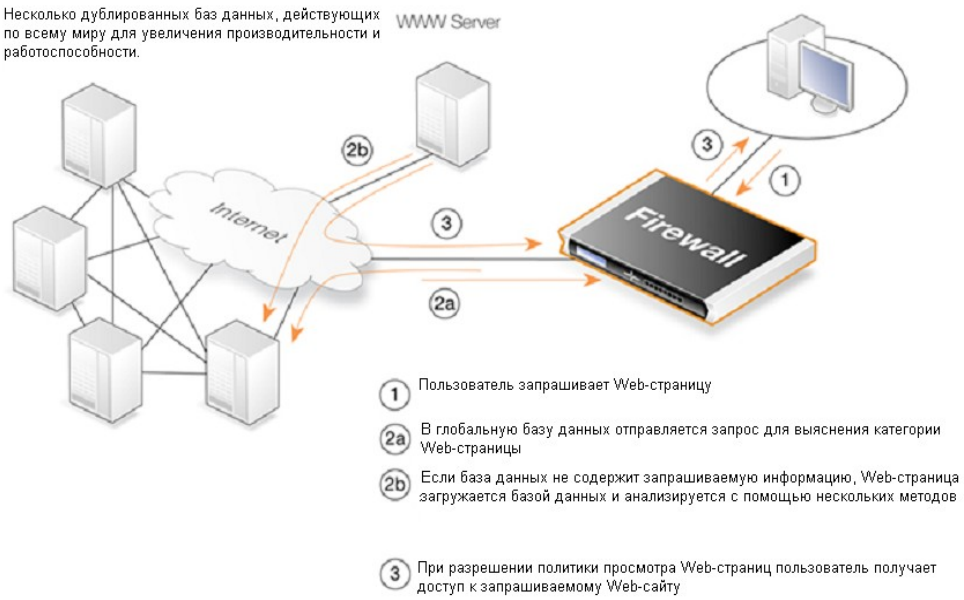


Рис. 6.8 Фильтрация динамического содержимого

Если URL-адреса запрашиваемой Web-страницы нет в базах данных, то содержимое Web-страницы по URL-адресу будет автоматически загружено в центральное хранилище данных D-Link и автоматически анализируется с помощью комбинации программных методов. После отнесения к определенной категории, URL размещается в глобальных базах данных, и NetDefendOS получает категорию для URL-адреса. Функция Dynamic WCF требует минимальных усилий администратора.

Примечание: Новые URL-адреса предоставляются анонимно

Новые, не распределенные по категориям, URL-адреса предоставляются анонимно и запись об их источнике отсутствует.

Классификация Web-страниц, а не сайтов

Функция динамической фильтрации классифицирует Web-страницы, а не сайты. Другими словами, Web-сайт может содержать определенные страницы, которые следует заблокировать, не блокируя весь сайт. Система NetDefendOS обеспечивает блокировку отдельной страницы, таким образом, пользователи могут получить доступ к остальным незаблокированным страницам Web-сайтов.

Функция WFC и «белый список»

Если какой-либо URL-адрес находится в «белом списке», то он будет «обходить» подсистему WCF. К URL-адресу не будет применена классификация, и доступ будет всегда разрешен. Это выполняется, если URL-адрес точно соответствует записи в «белом списке» или если он соответствует записи, которая использует подстановочные знаки.

6.3.4.2. Настройка WCF

Активация

Фильтрация динамического содержимого – это функция, для активации которой требуется

отдельная подписка на услугу. Это является дополнительным в стандартной лицензии NetDefendOS.

После оформления подписки должен быть определен объект HTTP Application Layer Gateway (ALG). Данный объект связан с объектом службы, а объект службы связан с правилом из набора IP-правил, определяющим какой трафик необходимо отфильтровать. Это дает возможность создания политик фильтрации на основе параметров фильтрации, используемых правилами в наборе IP-правил.

Совет: Использование расписания

Если необходимо, чтобы политика фильтрации содержимого менялась в зависимости от времени суток, используйте объект Расписание в соответствующем IP-правиле. Для получения более подробной информации, пожалуйста, см. Раздел 3.6, «Расписания».

Setting Fail Mode

Настройка HTTP ALG fail mode выполняется тем же способом, что и для других ALG, и применяется к WCF так же, как к таким функциям, как антивирусное сканирование. Режим fail mode определяет, почему не работает функция фильтрации динамического содержимого и, как правило, это происходит по причине того, что система NetDefendOS не может получить доступ к внешним базам данных для выполнения поиска URL-адреса. Можно установить одно из двух значений для режима fail mode:

- **Deny** – Доступ к сайтам по указанным URL-адресам будет запрещен, если доступ к внешней базе данных, выполняющей их проверку, заблокирован. Пользователь получит Web-страницу, уведомляющую, что доступ заблокирован.

- **Allow** – Если внешняя база данных WCF недоступна, доступ к сайтам по указанным URL-адресам будет разрешен, даже если бы они размещались в базе данных как запрещенные.

Пример 6.15. Включение фильтрации динамического Web-содержимого

Этот пример отображает настройку политики фильтрации динамического содержимого для HTTP-трафика, идущего с **intnet** в **all-nets**. Политика будет настроена на блокировку всех поисковых сайтов, в данном примере предполагается, что система использует одно правило *NAT* для HTTP-трафика, идущего с **intnet** в **all-nets**.

CLI

Сначала создайте объект HTTP Application Layer Gateway (ALG):

```
gw-world:/> add ALG ALG_HTTP content_filtering
                      WebContentFilteringMode=Enabled
                      FilteringCategories=SEARCH_SITES
```

Затем создайте объект службы, использующий новый HTTP ALG:

```
gw-world:/> add ServiceTCPUDP http_content_filtering Type=TCP
                     DestinationPorts=80
                     ALG=content_filtering
```

В довершение ко всему измените правило NAT для использования нового сервиса. Предполагаемое правило будет называться **NATHttp**:

```
gw-world:/> set IPRule NATHttp Service=http_content_filtering
```

Web-интерфейс

Сначала создайте объект HTTP Application Layer Gateway (ALG):

1. Зайдите **Objects > ALG > Add > HTTP ALG**

2. Укажите подходящее имя для ALG, например, *content_filtering*

3. Нажмите вкладку **Web Content Filtering**

4. Выберите **Enabled** в списке **Mode**

5. В списке **Blocked Categories**, выберите **Search Sites** и нажмите кнопку **>>**.

6. Нажмите **OK**

Затем создайте объект службы, использующий новый HTTP ALG:

1. Зайдите **Local Objects > Services > Add > TCP/UDP service**

2. Укажите подходящее имя для Службы, например, *http_content_filtering*

3. Выберите **TCP** в выпадающем меню **Type**

4. Введите **80** в текстовом поле **Destination Port**

5. Выберите HTTP ALG, только что созданный в списке **ALG**

6. Нажмите **OK**

В довершение ко всему измените правило NAT для использования нового сервиса:

1. Зайдите **Rules > IP Rules**

2. Выберите правило *NAT* для обработки HTTP-трафика

3. Нажмите вкладку **Service**

4. Выберите новый сервис *http_content_filtering*, в предварительно определенном списке **Service**

5. Нажмите **OK**

С этого момента функция фильтрации динамического содержимого включена для всего Web-трафика, идущего с *lannet* в *all-nets*.

Проверка функциональности выполняется с помощью следующих шагов:

1. На рабочей станции в сети *lannet* запустите стандартный Web-браузер.

2. Попытайтесь перейти в поисковую систему. Например, *www.google.com*.

3. Если все настройки выполнены корректно, появится Web-страница, информирующая пользователя о том, что запрашиваемый сайт заблокирован.

Режим Аудит

В режиме аудита система классифицирует и регистрирует все просмотры Web-страниц в соответствии с политикой фильтрации содержимого, но доступ на Web-сайты будет по-прежнему открыт пользователям. Это означает, что функция фильтрации содержимого может использоваться для выяснения того, доступ на Web-сайты каких категорий открыт пользователям и как часто.

Запуск режима аудита на определенный период времени поможет выяснить, какие Web-страницы наиболее часто посещают различные группы пользователей, а также потенциальные результаты включения функции WCF.

Поэтапное внедрение блокировки

Внезапная блокировка Web-сайтов может вызвать разногласия. Поэтому рекомендуется поэтапный ввод блокировки определенных категорий. Это дает пользователям время привыкнуть к блокировке

и поможет избежать неблагоприятных моментов, когда сразу блокируется много сайтов. Поэтапное внедрение блокировки также поможет проанализировать, выполняются ли цели блокировки.

Пример 6.16. Включение режима Audit

Данный пример основан на том же сценарии, что и предыдущий пример, но с включенным режимом аудит.

CLI

Сначала создайте объект HTTP Application Layer Gateway (ALG):

```
gw-world:/> add ALG ALG_HTTP content_filtering
                        WebContentFilteringMode=Audit
                        FilteringCategories=SEARCH_SITES
```

Web-интерфейс

Сначала создайте объект HTTP Application Layer Gateway (ALG):

1. Зайдите **Objects > ALG > Add > HTTP ALG**

2. Укажите подходящее имя для ALG, например, *content_filtering*

3. Нажмите вкладку **Web Content Filtering**

4. Выберите **Audit** в списке **Mode**

5. В списке **Blocked Categories** выберите **Search Sites** и нажмите кнопку **>>**

6. Нажмите **OK**

Шаги по созданию объекта службы, используя новый объект HTTP ALG, и изменение правила NAT для использования новой службы подробно описаны в предыдущем примере.

Функция Allowing Override

В некоторых случаях, функция фильтрации активного содержимого может препятствовать выполнению полезных задач. Рассмотрим пример: биржевой аналитик, который играет на бирже в режиме онлайн. Возможно, в повседневной работе ему потребуется просмотреть Web-сайты для проведения оценки компаний. Если корпоративная политика блокирует подобные Web-сайты, он не сможет выполнять свою работу.

По этой причине, система NetDefendOS поддерживает функцию под названием *Allow Override*. Если эта функция включена, компонент фильтрации содержимого предупреждает пользователя, что он собирается зайти на Web-сайт, доступ к которому ограничен в соответствии с корпоративной политикой, и что посещение Web-сайта будет зарегистрировано. Эта страница известна как *restricted site notice*. Далее пользователь может либо зайти на Web-сайт, либо прервать запрос.

При включении этой функции, только пользователям, у которых есть уважительная причина, будет разрешено посещать нежелательные сайты.

Предупреждение: Overriding the restriction of a site

Если пользователь отменяет страницу «Restricted site notice», он может просматривать все страницы без повторного появления уведомлений об ограниченном доступе на сайт. Тем не менее, пользователь по-прежнему регистрируется. Если в течение 5 минут пользователь неактивен, то при его дальнейшей попытке получить доступ на сайт, уведомление появится снова.

Изменение классификации заблокированных сайтов

Так как классификация неизвестных сайтов выполняется автоматически, всегда есть небольшой

риск, что некоторые сайты будут неправильно классифицированы. Система NetDefendOS поддерживает механизм, позволяющий пользователям выполнить вручную новую классификацию сайтов.

Данный механизм может быть включен на уровне HTTP-ALG, что означает, что можно выбрать включение данной функции для всех пользователей или только для выбранной группы пользователей.

Если включено изменение классификации и доступ к запрашиваемому Web-сайту заблокирован, Web-сайт будет содержать выпадающий список, содержащий все имеющиеся категории. Если пользователь считает, что запрашиваемый Web-сайт неправильно классифицирован, то он может выбрать более подходящую категорию из выпадающего списка.

URL-адрес запрашиваемого Web-сайта, а также предлагаемые категории будут отправлены в центральное хранилище данных D-Link для проверки вручную. Это проверка может привести к изменениям в классификации Web-сайта, либо в соответствии с предлагаемой категорией, либо с категорией, которая считается корректной.

Пример 6.17. Изменение классификации заблокированных сайтов

В данном примере демонстрируется, как можно выполнить переклассификацию Web-сайтов, если пользователь считает, что классификация неверная. Данный механизм включается на основе уровня HTTP ALG.

CLI

Сначала создайте объект HTTP Application Layer Gateway (ALG):

```
gw-world:/> add ALG ALG_HTTP content_filtering
                      WebContentFilteringMode=Enable
                      FilteringCategories=SEARCH_SITES
                      AllowReclassification=Yes
```

Далее продолжите настройку объекта службы и изменение правила NAT, как это было выполнено в предыдущих примерах.

Web-интерфейс

Сначала создайте объект HTTP Application Layer Gateway (ALG):

1. Зайдите **Objects > ALG > Add > HTTP ALG**

2. Укажите подходящее имя для ALG, например, *content_filtering*

3. Нажмите вкладку Web Content Filtering

4. Выберите **Enabled** в списке **Mode**

5. В списке **Blocked Categories** выберите **Search Sites** и нажмите кнопку **>>**

6. Check the **Allow Reclassification** control

7. Нажмите **OK**

Далее продолжите настройку объекта службы и изменение правила NAT, как это было выполнено в предыдущих примерах.

С этого момента активирована функция фильтрации динамического содержимого для всего Web-трафика, идущего из сети lannet в **all-nets** и пользователь способен выполнить переклассификацию заблокированных сайтов. Проверка функциональности выполняется с помощью следующих шагов:

1. На рабочей станции в сети *lannet* запустите стандартный Web-браузер.

2. Попытайтесь перейти в поисковую систему. Например, *www.google.com*.

3.Если все настройки выполнены корректно, появится Web-страница, отображающая выпадающий список со всеми доступными категориями.

4. С этого момента пользователь способен выбрать более подходящую категорию и предложить переклассификацию.

6.3.4.3. Категории фильтрации содержимого

В данном разделе представлен список всех категорий, используемый функцией фильтрации динамического содержимого, и подробное описание каждой категории.

Категория 1: Только для взрослых

Web-сайт может быть отнесен к категории «Только для взрослых», если он содержит описание или изображения эротического и сексуального характера, например, порнографию. Исключение составляют Web-сайты, содержащие информацию, касающуюся половой сферы и сексопатологии, которые могут быть отнесены к категории сайтов «Здоровье» (21). Примеры:

- www.naughtychix.com
- www.fullonxxx.com

Категория 2: Новости

Web-сайт может быть отнесен к категории «Новости», если он содержит информацию о последних событиях, касающихся населенного пункта пользователя (например, административного центра, города и страны), включая новости культуры и прогноз погоды. Как правило, содержимое такого сайта включает в себя выпуски новостей в режиме реального времени, а также журналы новостей промышленности и торговли. Сайт не содержит информацию о финансовых котировках, относящуюся к категории сайтов «Инвестирование» (11), или о спорте, имеющую отношение к категории «Спорт» (16). Примеры:

- www.newsunlimited.com
- www.dailyscoop.com

Категория 3: Поиск работы

Web-сайт может быть отнесен к категории «Поиск работы», если его содержимое включает в себя услуги по поиску или предоставлению вакансий в режиме реального времени. Помимо этого, сайт содержит информацию о составлении и размещении резюме и собеседовании, а также о подборе персонала и услугах по обучению. Примеры:

- www.allthejobs.com
- www.yourcareer.com

Категория 4: Азартные игры

Web-сайт может быть отнесен к категории азартных игр, если его содержание включает в себя рекламу, поощрение или услуги по принятию участия в азартных играх любого типа, на деньги или других. Помимо этого, сайт содержит информацию об играх в режиме реального времени, букмекерских конторах и лотереях. К этой категории не относятся сайты с наиболее распространенными или компьютерными играми, такие сайты входят в категорию «Игры» (10). Примеры:

• www.blackjackspot.com
• www.pickapony.net

Категория 5: Путешествия/Туризм

Web-сайт может быть отнесен к категории «Путешествия/Туризм», если он содержит информацию, связанную с туристической деятельностью, включая отдых и развлечения, а также услуги по бронированию билетов. Примеры:

• www.flythere.nu
• www.reallycheaptix.com.au

Категория 6: Покупка товаров

Web-сайт может быть отнесен к категории «Покупка товаров», если он содержит любую форму рекламы товаров или услуг, которые можно обменять на деньги, а также услуги для выполнения этой операции в режиме реального времени. К данной категории относятся сайты, занимающиеся продвижением товаров на рынке, продажей каталогов и услугами в сфере торговли. Примеры:

- www.megamall.com
- www.buy-alcohol.se

Категория 8: Чат

Web-сайт может быть отнесен к категории «Развлечения», если он содержит любой тип развлечений, не относящихся к какой-либо другой категории. Например, сайты с музыкой, кино, хобби, фан-клубами. Помимо этого, сайт содержит персональные Web-страницы, предоставленные провайдерами. Следующие категории более точно охватывают различные типы развлечений: «Только для взрослых» (1), «Азартные игры» (4), «Чат» (8), «Игры» (10), «Спорт» (16), «Клубы и сообщества» (22) и «Музыка для скачивания» (23). Примеры:

- www.celebnews.com
- www.hollywoodlatest.com

Категория 8: Чат

Web-сайт может быть отнесен к категории «Чат», если его посетители общаются меду собой в режиме реального времени. Помимо этого, сайт содержит доску объявлений, форумы в режиме онлайн, а также URL-адреса для загрузки программного обеспечения чата. Примеры:

- www.thetalkroom.com
- www.yazoo.com

Категория 9: Сайты знакомств

Web-сайт может быть отнесен к категории «Сайты знакомств», если он предоставляет услуги по размещению личных объявлений, организации романтических встреч, знакомства и брака (например, «невеста по почте»/ «замуж за иностранца») и служба сопровождения. Примеры:

- www.adultmatefinder.com
- www.marriagenow.com

Категория 10: Игры

Web-сайт может быть отнесен к категории «Игры», если он содержит наиболее распространенные или компьютерные игры, а также услуги для загрузки программного обеспечения, связанного с играми на компьютере, или участия в играх в режиме реального времени. Примеры:

- www.gamesunlimited.com
- www.gameplace.com

Категория 11: Инвестирование

Web-сайт может быть отнесен к категории «Инвестирование», если он содержит информацию и услуги, касающиеся персональных инвестиций. Сайты в данной категории включают такое содержимое как брокерские услуги, информацию о ценных бумагах, форумы управления денежными средствами, или котировки акций. К данной категории не относятся сайты с электронными банковскими услугами, эти сайты относятся к категории «Электронные банковские операции» (12). Примеры:

- www.loadsofmoney.com.au
- www.putsandcalls.com

Категория 12: Электронные банковские операции

Web-сайт может быть отнесен к категории «Электронные банковские операции», если он содержит информацию и услуги, касающиеся электронных банковских операций. К данной категории не относятся сайты, связанные с инвестированием, эти сайты относятся к категории «Инвестирование» (11). Примеры:

- www.nateast.co.uk
- www.borganfanley.com

Категория 13: Преступления/Терроризм

Web-сайт может быть отнесен к категории «Преступления/Терроризм», если он содержит описание или инструкции, касающиеся преступных или террористических действий. Примеры:

- www. beatthecrook.com.

Категория 14: Персональные убеждения/Секты

Web-сайт может быть отнесен к категории «Персональные убеждения/Секты», если он содержит описание, изображение или указания, касающиеся религиозных взглядов. Примеры:

- www.paganfed.demon.co.uk
- www.cultdeadcrow.com

Категория 15: Политика

Web-сайт может быть отнесен к категории «Политика», если он содержит информацию и мнения политического характера, информацию для избирателей, а также группы политических дискуссий. Примеры:

- www.democrats.org.au
- www.political.com

Категория 16: Спорт

Web-сайт может быть отнесен к категории «Спорт», если он содержит информацию или указания, связанные с оздоровительными или профессиональными видами спорта, включая обзоры на тему спортивных событий и результаты спортивных соревнований. Примеры:

- www.sportstoday.com.
- www.soccerball.com

Категория 17: Сайты www-Email

Web-сайт может быть отнесен к категории «Сайты www-Email», если он предоставляет услуги электронной почты на основе Web в режиме реального времени. Примеры:

- www.coldmail.com.
- www.yazoo.com

Категория 18: Насилие / Нежелательные действия

Web-сайт может быть отнесен к категории «Насилие / Нежелательные действия», если он содержит информацию насильственного характера. Информация включает распространение, описание или изображение актов насилия, а также сайты с подобным содержанием, которые могут не относиться ни к одной категории. Примеры:

- www.itstinks.com.
- www.ratemywaste.com

Категория 19: Вредоносные сайты

Web-сайт может быть отнесен к категории «Вредоносные сайты», если его содержимое может причинить вред компьютеру или компьютерной среде, включая расход полосы пропускания. К данной категории также относятся URL-адреса фишинг-сайтов, предназначенных для получения доступа идентификационных данных пользователя. Примеры:

- hastalavista.baby.nu

Категория 20: Поисковые системы

Web-сайт может быть отнесен к категории «Поисковые системы», если он предоставляет возможность поиска информации в Интернет в режиме онлайн. Примеры:

- www. zoogle.com
- www. yazoo.com

Категория 21: Здоровье

Web-сайт может быть отнесен к категории «Здоровье», если он содержит информацию и услуги, связанные со здоровьем, включая половую сферу и сексопатологию, а также сведения относительно лечебных учреждений и хирургии. Помимо этого, сюда также относятся группы поддержки и медицинские журналы. Примеры:

- www. thehealthzone.com
- www. safedrugs.com

Категория 22: Клубы и сообщества

Web-сайт может быть отнесен к категории «Клубы и сообщества», если он содержит информацию или услуги, касающиеся различных клубов и сообществ. К данной категории относятся Web-сайты с информацией об ассоциациях и конференциях. Примеры:

- www. sierra.org
- www. walkingclub.org

Категория 23: Музыка для загрузки

Web-сайт может быть отнесен к категории «Музыка для загрузки», если он предоставляет услуги по скачиванию, загрузке и совместного использования музыки в режиме реального времени, а также передачу аудиоданных по каналам с высокой пропускной способностью. Примеры:

- www.onlymp3s.com
- www. mp3space.com

Категория 24: Бизнес

Web-сайт может быть отнесен к категории «Бизнес», если его содержимое связано с повседневным бизнесом или корректной работоспособностью Интернет, например, обновления Web-браузера. Посещение сайтов, относящихся к данной категории, в большинстве случаев является безрезультативным.

Категория 25: Сайты, заблокированные правительственным учреждением

В данную категорию входят URL-адреса сайтов, указанные правительственным учреждением, которые считаются неподходящими для просмотра широкой аудиторией. Примеры:

- www.verynastystuff.com
- www.unpleasantvids.com

Категория 26: Образование

Web-сайт, отнесенный к категории «Воспитание», может быть также отнесен к другой категории, сайт содержит информацию и услуги в сфере образования, предоставляемые учебными заведениями. Примеры:

- highschoolessays.org
- www.learn-at-home.com

Категория 27: Реклама

Web-сайт может быть отнесен к категории «Реклама», если он содержит информацию или услуги, связанные с рекламированием. Примеры:

- www. admessages.com
- www. tripleclick.com

Категория 28: Наркотические вещества/Алкоголь

Web-сайт может быть отнесен к категории «Наркотические вещества/Алкоголь», если он содержит информацию или услуги, касающиеся наркотических веществ или алкоголя. Некоторые URL-адреса, относящиеся к данной категории, могут быть также отнесены к категории «Здоровье».

Примеры:

- www.the-cocktail-guide.com
- www. stiffdrinks.com

Категория 29: Компьютеры/IT

Web-сайт может быть отнесен к категории «Компьютеры/IT», если он содержит информацию или услуги, связанные с вычислительной техникой. Примеры:

- www.purplehat.com
- www.gnu.org

Категория 30: Нижнее белье/купальники/топ-модели

Web-сайт может быть отнесен к категории «Нижнее белье/купальники/топ-модели», если он содержит информацию или изображения купальников, нижнего белья и широко известных топ-моделей. Примеры:

- www.vickys-secre.com
- sportspictured.cnn.com/features/2002/swimsuit

Категория 31: Спам

Web-сайт может быть отнесен к категории «Спам», если он содержит сообщения спам массовой рассылки. Примеры:

- kaqsovdij.gjibhgk.info
- www. pleaseupdateyourdetails.com

Категория 32: Неклассифицированные сайты

К данной категории относятся неклассифицированные сайты и сайты, не вошедшие ни в одну категорию. Блокировка сайтов, относящихся к этой категории, может привести к блокировке безвредных URL-адресов.

6.3.4.4. Настройка HTML-страниц

Фильтрация динамического Web-содержимого использует набор HTML-файлов для того, чтобы уведомить пользователя о том, что он пытается получить доступ на заблокированный сайт. Эти Web-страницы, называемые иногда HTTP banner files, хранятся в NetDefendOS, но могут быть настроены, если требуется. WebUI предоставляет простой способ загрузки, изменения и скачивания этих файлов. Доступны следующие файлы:

CompressionForbidden
ContentForbidden
URLForbidden
RestrictedSiteNotice
ReclassifyURL

Для выполнения настройки сначала необходимо создать новый объект **ALG Banner Files**. Этот новый объект автоматически содержит копии всех файлов в объекте *по умолчанию* ALG Banner Files. Далее эти новые файлы могут быть изменены и загружены обратно в NetDefendOS. Первоначальный объект *Default* не может быть изменен. В следующем примере продемонстрированы необходимые шаги.

Пример 6.18. Отправка сообщений SNMP Traps на SNMP Trap Receiver

В данном примере продемонстрировано, как изменить содержимое страницы *URL forbidden* HTML:

Web-интерфейс

1. Зайдите **Objects > HTTP Banner files > Add > ALG Banner Files**

2. Введите имя, такое как *new_forbidden* и нажмите OK

3. Появится диалоговое окно для нового набора ALG banner files

4. Нажмите вкладку **Edit & Preview**

5. Выберите *URLForbidde*n из списка **Page**

6. Теперь измените источник HTML, который появляется в текстовом поле для страницы Forbidden URL page

7. Используйте **Preview** для проверки макета, если требуется

8. Нажмите **Save,** чтобы сохранить изменения

9. Нажмите **OK**, чтобы выйти

10. Зайдите **User Authentication > User Authentication Rules**

11. Выберите соответствующий HTML ALG и нажмите вкладку **Agent Options**

12. Установите функцию *new_forbidden* для функции **HTTP Banners**

13. Нажмите **OK**

14. Зайдите **Configuration > Save & Activate** для активации нового файла

15. Нажмите **Save**, а затем **OK**

С этого момента система отправляет сообщения SNMP traps для всех событий с важностью более или равной уровню **Alert** на SNMP trap receiver с IP-адресом 195.11.22.55.

Совет: Сохранение изменений

*В примере выше можно изменить более одного HTML-файла во время сессии, однако, необходимо нажать кнопку **Save** для сохранения любых изменений, прежде чем вносить изменения в другом файле.*

Загрузка по протоколу SCP

Можно загрузить новые файлы HTTP Banner files с помощью SCP. Для этого выполните следующие шаги:

1. Так как SCP не может использоваться для загрузки первоначального HTML по умолчанию, сначала следует скопировать код источника с WebUI и вставить в текст файла, который затем будет изменен с помощью соответствующего редактора.

2. Новый объект **ALG Banner Files** должен существовать, который загружает измененный файл (-ы). Если объект называется *mytxt*, то команда CLI создаст объект в виде:

```
gw-world:/> add HTTPALGBanners mytxt
```

Создается объект, который содержит копии всех файлов баннеров фильтрации содержимого по умолчанию.

3. Далее измененный файл загружается с помощью SCP. Файл загружается на объект *HTTPALGBanner* и объект *mytxt* с именем параметра *URLForbidden*. Если измененный локальный файл *URLForbidden* называется *my.html*, то использование клиента Open SSH SCP команда загрузки будет следующей:

```
scp myhtml admin@10.5.62.11:HTTPAuthBanners/mytxt/URLForbidden
```

Использование SCP-клиентов подробно описано в *Разделе 2.1.6., «Secure Copy».*

4. С помощью CLI соответствующий HTTP ALG должен быть установлен на использование *mytxt* banner files.Если ALG называется *my http alg*, используется следующая команда:

```
set ALG_HTTP my_http_alg HTTPBanners=mytxt
```

5. Как правило, для активации изменений на межсетевом экране NetDefend необходимо использовать команду *activate,* за которой следует команда CLI *commit.*

Параметры HTML-страницы

HTML-страницы содержат ряд следующих доступных параметров:

• **%URL%** - Запрашиваемый URL-адрес

• **%IPADDR%** - Просматриваемый IP-адрес

• **%REASON%** - Причина отказа в доступе

6.4 Антивирусное сканирование

6.4.1. Обзор

Антивирусный модуль NetDefendOS обеспечивает защиту от вредоносного кода, переносимого загрузочными файлами. Файлы могут быть загружены как часть Web-страницы в передаче HTTP, в загрузке FTP, или, возможно, в виде вложений в электронную почту, доставленных через SMTP. Вредоносный код в таких загрузках предназначен для различных целей, начиная от программ раздражающего воздействия до более злонамеренных действий, например, получение паролей, номеров кредитных карт и другой конфиденциальной информации. Термин «Вирус» может быть использован как общее описание для всех видов вредоносного кода, переносимого файлами.

Объединение с клиентом антивирусного сканирования

В отличие от функции обнаружения и предотвращения вторжений (IDP), которая в основном применяется при нападении на серверы, антивирусное сканирование сконцентрировано на загрузках, выполняемых клиентами. Антивирус NetDefendOS разработан как дополнение к стандартному антивирусному сканированию, которое обычно выполняется локально специализированным программным обеспечением, установленным на клиентских компьютерах. Функция IDP не предназначена для полноценной замены локального сканирования, а скорее является дополнительной функцией для повышения безопасности. Самое главное, она может выступать в качестве резервной функции, когда локальному клиенту не доступно антивирусное сканирование.

Активация через ALG

Антивирус NetDefendOS активируется на основе ALG. Активация доступна для загрузки файлов, связанных со следующими ALG и включается непосредственно в ALG:

• HTTP ALG
• FTP ALG
• POP3 ALG
• SMTP ALG

Примечание: Не все модели NetDefendOS оснащены антивирусом

Функция антивирусного сканирования доступна только на следующих моделях межсетевых экранов NetDefend: DFL-260, 860, 1660, 2560 и 2560G.

6.4.2. Реализация

Потоковая передача

Так как потоковая передача файлов выполняется через межсетевой экран NetDefend, система NetDefendOS будет сканировать потоковые данные на наличие вирусов, если антивирусный модуль включен. Так как файлы являются потоковыми и не были полностью прочитаны в памяти, требуется минимальный объем памяти, и влияние на общую пропускную способность будет минимальным.

Сопоставление с образцом

Процесс проверки основан на сопоставлении с базой данных известных вирусов и с высокой степенью достоверности помогает определить процесс загрузки вируса для пользователя, находящегося позади межсетевого экрана NetDefend. Как только в содержании файла обнаружен вирус, загрузка может быть прекращена до своего завершения.

Типы просканированных файлов загрузки

Как описано выше, антивирусное сканирование активируется на основе ALG и может просканировать файлы загрузки, связанные с HTTP, FTP, SMTP и POP3 ALG. В частности:

• Любой тип несжатого файла, передаваемого через ALGs, может быть просканирован.

• Если файл загрузки был сжат, файлы ZIP и GZIP могут быть просканированы.

Администратор обладает возможностью отклонить определенные файлы, а также возможностью указать ограничение размера сканируемых файлов. Если размер не указан, то по умолчанию максимальный размер файлов не ограничен.

Одновременное сканирование

Не существует фиксированного ограничения, какое количество антивирусных сканирований может быть одновременно выполнено на одном межсетевом экране NetDefend. Тем не менее, в доступный объем памяти можно установить ограничение количества одновременных сканирований.

Protocol Specific behavior

Так как антивирусное сканирование выполняется через шлюз уровня приложений (ALG), в NetDefendOS реализованы определенные функции конкретного протокола. С FTP, например, сканирование выполняется с двойным управлением и передача данных осуществляется по открытым каналам, также можно отправить запрос через управляющее соединение на прекращение загрузки, если обнаружен вирус.

Связь с IDP

Часто возникает вопрос относительно порядка антивирусного сканирования в отношении IPD сканирования. Фактически концепция порядка не является актуальной, так как два процесса сканирования могут произойти одновременно и работать на разных уровнях протокола.

Если функция IDP включена, выполняется сканирование всех пакетов, указанных определенным

правилом IDP, без принятия во внимание протоколов более высокого уровня, таких как HTTP, которые генерируют потоки пакетов. Тем не менее, Антивирус осведомлен о протоколе высокого уровня и только просматривает данные, участвующие в передаче файлов. Антивирусное сканирование является функцией, и поэтому логически принадлежит ALG, в то время как IDP не принадлежит.

6.4.3. Активация антивирусного сканирования

Связь с ALG

Активация антивирусного сканирования достигается за счет ALG, связанного с целевым протоколом. При включении опции антивирусного сканирования объект ALG должен уже существовать. Как всегда ALG должен быть связан с соответствующим объектом сервиса протокола для сканирования. Далее объект сервиса ассоциируется с правилом в наборе IP-правил, которое определяет источник и назначение трафика, к которому применяется ALG.

Создание антивирусных политик

Поскольку IP-правила из набора являются средствами, с помощью которых выполняется функция Антивирус, реализация функции выполняется *на основе политики*. IP-правила могут определить, что ALG и связанное с ним антивирусное сканирование может применяться к трафику, проходящему в данном направлении и между определенными IP-адресами источника и назначения и/или сетями. Расписание может также применяться для поиска вирусов, таким образом, оно используется только в определенное время.

6.4.4. База данных сигнатур

SafeStream

Антивирусное сканирование выполняется системой NetDefendOS D-Link с помощью баз данных сигнатур вирусов SafeStream. База данных SafeStream создана и поддерживается лабораторией Касперского – компанией, которая является мировым лидером в области обнаружения вирусов. База данных обеспечивает защиту от всех известных вирусов, включая троянские программы, «червей», «backdoor» и другие. База данных также тщательно протестирована для устранения ошибочных срабатываний.

Обновление базы данных

База данных SafeStream обновляется ежедневно с добавлением сигнатур новых вирусов. Старые сигнатуры редко удаляются, но вместо этого они заменяются более общими сигнатурами, которые охватывают несколько вирусов. Поэтому локальная копия NetDefendOS базы данных SafeStream должна регулярно обновляться, и этот сервис обновления включен как часть подписки на Антивирус D-Link.

6.4.5. Подписка на сервис Антивирус D-Link

Функция Антивирус D-Link приобретается как дополнительный компонент к лицензии D-Link в виде возобновляемой подписки. Подписка на Антивирус включает регулярные обновления базы данных Касперского SafeStream в течение периода подписки с добавлением последних вирусных угроз.

6.4.6. Функции Антивируса

При настройке антивирусного сканирования в ALG, можно установить следующие параметры:

1. Основные функции

Режим — Режим должен быть одним из них:
i. **Disabled** – Функция Антивирус выключена.
ii. **Audit** – Сканирование активировано, но единственным действием является ведение журнала.
iii. **Protect** – Функция Антивирус активирована. Подозрительные файлы будут удалены или занесены в журнал.

Fail mode behavior — Если по какой-либо по причине не удается выполнить проверку на наличие вирусов, то передача данных может быть прекращена или разрешена, при этом событие регистрируется в журнале. Если установлено значение *Allow* (Разрешить), то ситуация в условиях, когда вирусные базы не доступны или текущая лицензия не действительна, не приведет к удалению файлов. Вместо этого, передача файлов будет разрешена, а также будет сгенерировано сообщение для записи в журнал, указывающее на то, что произошел сбой.

2. Функция Scan Exclude

Если требуется, можно отменить сканирование файлов с определенным расширением. Данное действие может увеличить общую пропускную способность, если расширение файла является одним из видов, которые обычно встречаются в определенном сценарии, например, загрузка файлов через HTTP.

NetDefendOS выполняет проверку MIME всех расширений файлов, перечисленных в *Приложении C, Типы файлов MIME, проходящих проверку*, чтобы установить корректное расширение файла и затем посмотреть, находится ли это расширение в списке исключенных. Если расширение файла не может быть установлено на основе его содержания (а это может случиться с расширениями файлов, не указанными в *Приложении C, Типы файлов MIME, проходящих проверку*), то расширение в имени файла используется при проверке списка исключений.

3. Ограничение степени сжатия

При сканировании сжатых файлов, NetDefendOS должна применять распаковку для проверки содержимого файла. Некоторые типы данных могут привести к очень высокой степени сжатия, где сжатый файл является малой частью от первоначального размера несжатого файла. Это означает, что сравнительно небольшое вложение сжатого файла, возможно, нуждается в распаковке. Большой по объему файл может значительно израсходовать ресурсы NetDefendOS и заметно снизить пропускную способность.

Для предотвращения подобной ситуации, администратор должен указать предел степени сжатия (*Compression Ratio*). Если предел степени сжатия определен как **10**, то это будет означать, что если несжатый файл в 10 раз больше, чем сжатый, следует предпринять указанное действие. Действие может быть одним из следующих:

• **Allow** – Разрешить передачу файла без проверки на наличие вирусов

• **Scan** – Сканировать файл на наличие вирусов

• **Drop** – Отбросить файл

Во всех трех перечисленных выше случаях событие заносится в журнал.

Проверка файлов на соответствие типам MIME

Опции ALG **File Integrity** могут быть использованы совместно с антивирусным сканированием для того, чтобы проверить, соответствует ли содержание файла типу MIME.

MIME-тип определяет расширение файла. Например, можно определить расширение файла как *.gif* и, следовательно, файл должен содержать данные этого типа. Некоторые вирусы могут пытаться скрыться внутри файлов, используя ложное расширение. Файл может быть рассмотрен как файл *.gif*, но содержимое файла не будет соответствовать данным этого типа, так как он заражен вирусом.

Включение этой функции рекомендуется для того, чтобы предотвратить прохождение вируса. Типы MIME перечислены в *Приложении C, Типы файлов MIME, проходящих проверку*.

Настройка корректного системного времени

Очень важно установить правильное системное время в системе NetDefendOS, если функция автоматического обновления в антивирусном модуле работает корректно. Неправильное время может означать, что автоматическое обновление отключено.

Команда консоли

```
gw-world:/> updatecenter -status
```

отобразит текущий статус функции автоматического обновления. Это также может быть выполнено через Web-интерфейс.

Обновление в отказоустойчивых кластерах

Обновление антивирусных баз данных для межсетевых экранов NetDefend в отказоустойчивом кластере выполняется автоматически. В кластере всегда есть *активное* и *пассивное* устройства. Только активное устройство в кластере будет выполнять регулярную проверку новых обновлений базы данных. Если доступно обновление, последовательность событий будет выглядеть следующим образом:

1. Активное устройство определяет, есть ли новые обновления и необходимые файлы.

2. Активное устройство выполняет автоматическое изменение настроек для обновления своей базы данных.

3. Это изменение настроек приведет к переходу на другой ресурс, таким образом, пассивное устройство становится активным.
4. После завершения обновления, вновь активное устройство также загружает файлы для обновления и выполняет изменение настроек.

5. Данное вторичное изменение настроек приведет к повторному переходу на другой ресурс, таким образом, пассивное устройство снова становится активным.

Антивирус и ZoneDefense

ZoneDefense является функцией, изолирующей зараженные хосты и серверы в локальной сети. В то время как функция антивирусного сканирования следит за блокировкой входящих инфицированных файлового зараженные файлы, ZoneDefense может использоваться для перехвата вирусов, переданных с инфицированного локального хоста на другие локальные хосты. При обнаружении вируса, система NetDefendOS загружает инструкции блокировки на локальные коммутационные устройства и дает указание блокировать весь трафик с зараженного хоста или сервера.

Так как блокировка ZoneDefense является ограниченным ресурсом, у администратора есть возможность настроить, какие хосты и серверы следует заблокировать при обнаружении вируса.

Например: локальный клиент загружает зараженный файл с удаленного сервера FTP в сети Интернет. NetDefendOS обнаруживает это и останавливает передачу файлов. На данный момент, система NetDefendOS предотвратила проникновение зараженного файла во внутреннюю сеть. Следовательно, нет необходимости использовать блокировку удаленного FTP-сервера на локальных

коммутаторах, так как NetDefendOS уже заблокировала вирус. Блокировка IP-адреса сервера будет бесполезной тратой записей блокировок на коммутаторе.

Для того чтобы система NetDefendOS знала, какие хосты и серверы необходимо блокировать, администратор указывает сетевой диапазон для блокировки с помощью технологии ZoneDefense. Все хосты и серверы в пределах этого диапазона будут заблокированы.

Управление функцией осуществляется через конфигурацию Антивирус в ALG. В зависимости от используемого протокола, существуют различные сценарии того, как эта функция может быть применена.

Для получения дополнительной информации см. *Глава 12, ZoneDefense*.

Пример 6.19. Активация антивирусного сканирования

Данный пример отображает настройку политики антивирусного сканирования HTTP-трафика, идущего с **lannet** в **all-nets**. Предположительно, правило NAT уже определено в наборе IP-правил для натирования данного трафика.

CLI

Сначала создайте объект HTTP Application Layer Gateway (ALG) с включенной функцией антивирусного сканирования:

```
gw-world:/> set ALG ALG_HTTP anti_virus Antivirus=Protect
```

Далее создайте объект службы с помощью нового HTTP ALG:

```
gw-world:/> add ServiceTCPUDP http_anti_virus Type=TCP
                        DestinationPorts=80
                        ALG=anti_virus
```

В довершение ко всему измените правило *NAT* для использования новой службы:

```
gw-world:/> set IPRule NATHttp Service=http_anti_virus
```

Web-интерфейс

A. Сначала создайте объект HTTP ALG:

1. Зайдите **Objects > ALG > Add > HTTP ALG**

2. Определите подходящее имя для ALG, например, *anti_virus*

3. Нажмите вкладку **Antivirus**

4. Выберите **Protect** в выпадающем списке **Mode**

5. Нажмите **OK**

B. Далее создайте объект Служба с помощью нового HTTP ALG:

1. Зайдите **Local Objects > Services > Add > TCP/UDP service**

2. Определите подходящее имя для объекта Служба, например, http_anti_virus

3. Выберите **TCP** в выпадающем списке **Type**

4. Введите **80** в текстовом поле **Destination Port**

5. Выберите недавно созданный HTTP ALG в выпадающем списке **ALG**

6. Нажмите **OK**

C. В довершение ко всему измените правило *NAT* (в данном примере **NATHttp**) для использования новой службы:

1. Зайдите **Rules > IP Rules**

2. Выберите правило NAT для управления трафиком между **lannet** и **all-nets**

3. Нажмите вкладку **Service**

4. Выберите новый сервис, http_anti_virus, в прелварительно определенном выпадающем списке **Service**

5. Нажмите **OK**

С этого момента функция антивирусного сканирования активирована для всего Web-трафика между **lannet** и **all-nets**.

6.5. Обнаружение и предотвращение вторжений

6.5.1. Обзор

Определение вторжений

Уязвимые серверы могут стать жертвами таких атак как «черви», «трояны» и «backdoor», которые могут получить контроль над сервером. Общий термин, используемый для описания таких атак на сервер – *intrusions* (вторжения).

Обнаружение вторжений

Вторжения отличаются от вирусов тем, что вирус, как правило, содержится в одном файле, загружаемым в систему клиента. Вторжение представляет собой вредоносные Интернет-данные, целью которых является «обойти» механизмы безопасности сервера. Вторжения не являются редкостью и могут постоянно изменяться, так как они автоматически генерируются атакующим. NetDefendOS IDP обеспечивает защиту от этих угроз.

Обнаружение и предотвращение вторжений (IDP) является подсистемой NetDefendOS, которая предназначена для защиты от попыток вторжения. Система действует путем мониторинга сетевого трафика, проходящего через межсетевой экран NetDefend, поиска шаблонов, указывающих на попытку вторжения. После обнаружения вторжения, NetDefendOS IDP выполняет шаги по нейтрализации как вторжения, так и его источника.

Проблемы IDP

Для поддержки эффективности и надежности системы IDP, необходимо рассмотреть следующие вопросы:

1. Какие типы трафика следует подвергать анализу?

2. Что следует искать в таком трафике?

3. Какое действие необходимо предпринять при обнаружении вторжения?

Компоненты NetDefendOS IDP

NetDefendOS IDP решает выше перечисленные вопросы с помощью следующих механизмов:

1. **IDP-правила,** устанавливаемые администратором для того, чтобы определить какой трафик необходимо сканировать.

2. **Pattern Matching,** применяемый системой NetDefendOS IDP к трафику, который соответствует IDP-правилу и проходит через межсетевой экран.

3. Если система NetDefendOS IDP обнаруживает вторжение, выполняется **Действие**, указанное для запуска IDP-правила.

IDP-правила, Pattern Matching и Действия IDP-правила описаны в следующих разделах.

6.5.2. Система IDP и устройства D-Link

Maintenance и Advanced IDP

Компания D-Link предоставляет два типа IDP:

• Maintenance IDP

Maintenance IDP является основой системы IDP и включено в стандартную комплектацию NetDefend DFL-210, 800, 1600 и 2500.

Maintenance IDP является упрощенной IDP, что дает базовую защиту от атак и поддерживает возможность расширения до более высокого уровня и более комплексного *Advanced IDP*, представленного далее.

IDP не входит в стандартную комплектацию DFL-260, 860, 1660, 2560 и 2560G; для этих моделей межсетевых экранов необходимо приобрести подписку на *Advanced IDP*.

• Advanced IDP

Advanced IDP является расширенной системой IDP на основе подписки с более широким кругом баз данных сигнатур для оборудования с высокими требованиями. Стандартной является подписка сроком на 12 месяцев, обеспечивающая автоматическое обновление базы данных сигнатур IDP.

Эта опция IDP доступна для всех моделей D-Link NetDefend, включая те, в стандартную комплектацию которых не входит *Maintenance IDP*.

Maintenance IDP можно рассматривать, как ограниченную подсистему *Advanced IDP* и в следующих разделах описано, как действует *Advanced IDP*.

Подписка на услугу D-Link *Advanced IDP*

Advanced IDP приобретается как дополнительный компонент к базовой лицензии NetDefendOS. Подписка означает, что база данных сигнатур IDP может быть загружена на NetDefendOS, а также, что база данных регулярно обновляется по мере появления новых угроз.

Рис. 6.9. Обновление базы данных IDP

Новая, обновленная база данных сигнатур автоматически загружается системой NetDefendOS в течение указанного интервала времени. Это выполняется с помощью HTTP-соединения с сетью сервера D-Link, который предоставляет последние обновления базы данных сигнатур. Если существует новая версия базы данных сигнатур сервера, она будет загружена, заменив старую версию.

Термины *IDP, IPS* и *IDS*

Термины *Intrusion Detection and Prevention (IDP), Intrusion Prevention System (IDP)* и *Intrusion Detection System (IDS)* взаимозаменяют друг друга в документации D-Link. Все они относятся к функции IDP.

Настройка корректного системного времени

Очень важно установить правильное системное время в системе NetDefendOS, если функция автоматического обновления в антивирусном модуле работает корректно. Неправильное время может означать, что автоматическое обновление отключено.

Команда консоли

```
> updatecenter -status
```

отображает текущий статус функции автоматического обновления. Это также может быть выполнено через Web-интерфейс.

Обновление в отказоустойчивых кластерах

Обновление баз данных IDP для межсетевых экранов NetDefend в отказоустойчивом кластере выполняется автоматически. В кластере всегда есть *активное* и *пассивное* устройства. Только активное устройство в кластере будет выполнять регулярную проверку новых обновлений базы данных. Если доступно обновление, последовательность событий будет выглядеть следующим образом:

1. Активное устройство определяет, есть ли новые обновления и необходимые файлы.

2. Активное устройство выполняет автоматическое изменение настроек для обновления своей базы данных.

3. Это изменение настроек приведет к переходу на другой ресурс, таким образом, пассивное устройство становится активным.

4. После завершения обновления, вновь активное устройство также загружает файлы для обновления и выполняет изменение настроек.

5. Данное вторичное изменение настроек приведет к повторному переходу на другой ресурс, таким образом, пассивное устройство снова становится активным.

Эти шаги приведут к тому, что на обоих межсетевых экранах в кластере будут обновлены базы данных с первоначальным распределением активной и пассивной роли. Для получения более подробной информации об отказоусточивых кластерах см. *Глава 11, Высокая отказоустойчивость*.

6.5.3. IDP-правила

Компоненты правила

Правило IDP определяет, какой тип трафика необходимо анализировать. Правило IDP аналогично IP-правилу. Правила IDP структурированы так же как другие политики безопасности в системе NetDefendOS, например, IP-правила. Правило IDP определяет указанную комбинацию адреса/интерфесы источника/назначения, а также связано с объектом Service, определяющим какие протоколы для сканирования использовать. Расписание может быть также связано с правилом IDP. Самое главное, правило IDP определяет какое **Действие** предпринять при обнаружении вторжения.

Нормализация HTTP

В каждом IDP-правиле есть раздел с настройками для *нормализации HTTP*. Это позволяет администратору выбирать действия, которые необходимо предпринять, при обнаружении несоответствия в URI во входящих HTTP-запросах. Некоторые атаки на серверы основаны на создании унифицированных индикаторов ресурсов (URI), которые могут использовать уязвимые места серверов.

IDP может определить следующее:

• **Некорректная кодировка UTF8**

Поиск любых неправильных символов UTF8 в URI.

• **Некорректный шестнадцатеричный код шифрования**

Корректной является шестнадцатеричная последовательность, где присутствует знак процента, за которым следуют два шестнадцатеричных значения, представляющих один байт данных. Некорректная шестнадцатеричная последовательность – это последовательность, в которой присутствует знак процента, за которым следует то, что не является корректным шестнадцатеричным значением.

• **Двойное шифрование**

Выполняется поиск любой шестнадцатеричной последовательности, которая сама является закодированной с использованием других управляющих шестнадцатеричных последовательностей. Примером может быть первоначальная последовательность *%2526*, где *25%* далее может быть расшифровано HTTP-сервером как '%', в результате получится последовательность '%26'. Конечная расшифровка '*&*'.

Первоначальная обработка пакетов

Порядок первоначальной обработки пакетов с помощью IDP является следующим:

1. Пакет приходит на межсетевой экран и NetDefendOS выполняет стандартную проверку. Если пакет является частью нового соединения, то он проверяется на соответствие IP-правилу из набора, прежде чем перейти на модуль IDP. Если пакет является частью существующего соединения, он переходит непосредственно в систему IDP. Если пакет не является частью существующего соединения или отвергается IP-правилом из набора, то он будет отброшен.

2. Информация об адресе источника и назначения пакета сравнивается с набором правил IDP, определенных администратором. Если найдено совпадение, то пакет передается на следующий уровень обработки IDP, «сопоставление с образцом», описанный в шаге ниже. Если совпадения не обнаружено, то пакет принимается, и система IDP не предпринимает дальнейших мер, хотя в наборе IP-правил определены такие действия как преобразование адреса и регистрация.

Проверка отброшенных пакетов

Функция существует в NetDefendOS IDP для обнаружения вторжений, проверяются даже те пакеты, которые были отклонены набором IP-правил при проверке новых соединений, а также пакеты, которые не являются частью существующего соединения. Это дает администратору межсетевого экрана возможность обнаружения любого вторжения. Следует применять данную функцию с осторожностью, так как при обработке всех пакетов нагрузка будет достаточно высокой.

6.5.4. Предотвращение атак Insertion/Evasion

Обзор

При определении IP-правила администратор может включить или отключить опцию **Protect against Insertion/Evasion attack**. *Insertion/Evasion Attack* – это вид атаки, которая направлена на «обход» механизмов IDP. При этом используется тот факт, что в передаче данных TCP / IP, поток данных часто должен быть собран из небольших фрагментов данных, так как отдельные части либо приходят в неправильном порядке, либо некоторым образом фрагментированы. *Insertions* или *Evasions* предназначены для использования в процессе сборки.

Атаки Insertion

Атака Insertion состоит из вставки данных в поток, таким образом, подсистема IDP принимает полученную в результате последовательность пакетов данных, но данная последовательность будет отвергнута целевым приложением. Это приведет к образованию двух различных потоков данных.

В качестве примера, рассмотрим поток данных, разбитый на 4 пакета: p1, p2, p3 и p4. Злоумышленник может сначала отправить пакеты p1 и p4 целевому приложению. Они будут удерживаться и подсистемой IDP, и приложением, до прихода пакетов p2 и p3, таким образом, будет выполнена сборка. В настоящее время злоумышленник намеренно отправляет два пакета, p2 и p3, которые будут отклонены приложением, но приняты системой IDP. Система IDP в состоянии выполнить полную сборку пакетов и полагает, что это полный поток данных. Злоумышленник отправляет еще два пакета, p2 и p3, которые будут приняты приложением, способным выполнить завершение сборки, но в результате получаются различные потоки данных, который видит подсистема IDP.

Атаки Evasion

У атаки Evasion такой же конечный результат, что и у атаки Insertion, также образуются два различных потока данных: один, который виден подсистеме IDP, и другой, который виден целевому приложению, но в данном случае результат достигается обратным путем, который заключается в отправке пакетов данных, отклоненных подсистемой IDP, но принятых целевым приложением.

Обнаружение

Если атака Insertion/Evasion обнаружена с помощью включенной функции Insertion/Evasion Protect,

NetDefendOS автоматически корректирует поток данных, удаляя посторонние данные, связанные с атакой.

События Insertion/Evasion для записи в журнал

Подсистема Insertion/Evasion Attack в NetDefendOS может генерировать два типа сообщений для записи в журнал:

• Сообщение **Attack Detected**, указывающее на то, что атака была обнаружена и предотвращена.

• Сообщение **Unable to Detect,** уведомляющее о том, что система NetDefendOS не смогла выявить потенциальную атаку при сборке потока TCP / IP, хотя подобная атака могла присутствовать. Эта ситуация вызвана редкими и сложными образцами данных в потоке.

Рекомендуемые настройки

По умолчанию, защита от атак Insertion/Evasion включена для всех IDP-правил и это рекомендуемая настройка для большинства конфигураций. Существует две мотивации для отключения опции:

• **Increasing throughput** (Увеличение пропускной способности) - Если необходима высокая пропускная способность, следует выключить функцию, так как это обеспечит небольшое снижение скорости обработки.

• **Excessive False Positives** (Чрезмерное количество ложных срабатываний) - Если наблюдается большое количество ложных срабатываний функции Insertion/Evasion, то целесообразно выключить функцию во время выяснения причин ложных срабатываний.

6.5.5. Соответствие шаблону IDP

Сигнатуры

Для корректной идентификации атак система IDP использует профиль показателей, или *шаблон*, связанный с различными типами атак. Эти предварительно определенные шаблоны, также известные как *сигнатуры*, хранятся в локальной базе данных NetDefendOS и используются модулем IDP при анализе трафика. Каждой сигнатуре IDP назначается уникальный номер.

Рассмотрим следующий простой пример атаки, содержащий обмен данными с FTP-сервером. Неавторизованный пользователь может попытаться получить файл паролей «passwd» от FTP-сервера с помощью команды FTP **RETR passwd**. Сигнатура, выполняющая поиск тектовых строк ASCII RETR и passwd, обнаружит в данном случае соответствие, указывающее на возможную атаку. В данном примере найден шаблон в виде простого текста, но соответствие шаблону выполняется тем же способом на исключительно двоичных данных.

Диагностика неизвестных угроз

Злоумышленники, осуществляющие новые вторжения, часто повторно используют старый код. Это означает, что новые атаки могут появиться очень быстро. Чтобы противостоять этому, D-Link IDP использует подход, при котором модуль сканирует все многократно используемые компоненты, выявляя соответствие шаблону стандартных блоков, а не целого кода. Таким образом, можно защититься от «известных», новых, недавно реализованных, «неизвестных» угроз, сформированных с повторным использованием компонентов программного обеспечения.

Advisory

Advisory – это пояснительное текстовое описание сигнатуры. Прочитав текстовое описание сигнатуры, администратор выяснит, какую атаку или вирус поможет обнаружить данная сигнатура. В связи с изменением характера базы данных сигнатур, текстовые описания не содержатся в документации D-Link, но доступны на Web-сайте D-Link:

http://security.dlink.com.tw

Описания можно найти, выбрав функцию «NetDefend IDS» в меню « NetDefend Live».

Типы сигнатур IDP

IDP предлагает три типа сигнатур, которые предоставляют различные уровни достоверности в отношении угроз:

• **Intrusion Protection Signatures (IPS)** – Данный тип сигнатур обладает высокой точностью, и соответствие в большинстве случае указывает на угрозу. Рекомендуется действие Protect. Эти сигнатуры могут обнаружить административные действия и сканеры безопасности.

• **Intrusion Detection Signatures (IDS)** – У данного типа сигнатур меньше точности, чем у IPS, и они могут дать ложные положительные результаты, таким образом, перед тем как использовать действие **Protect** рекомендуется применить действие **Audit**.

• **Policy Signatures** - Этот тип сигнатур обнаруживает различные типы трафика приложений. Они могут использоваться для блокировки некоторых приложений, таких как совместное использование приложений и мгновенный обмен сообщениями.

6.5.6. Группы сигнатур IDP

Использование групп

Как правило, существует несколько линий атак для определенного протокола, и одновременное обнаружение всех атак во время анализа сетевого трафика является оптимальным для пользователя. Для этого, сигнатуры, связанные с определенным протоколом, сгруппированы вместе. Например, все сигнатуры, которые относятся к FTP-протоколу, образуют группу. Лучше указать группу, которая относится к определенному трафику, чем рассматривать отдельные сигнатуры. Для повышения качества функционирования, система NetDefendOS должна выполнять поиск, используя минимальное количество сигнатур.

Определение групп сигнатур

Группы сигнатур IDP подразделяются на три уровня иерархической структуры. Сигнатура *Type* находится на верхнем уровне, на втором уровне – *Category* и на третьем уровне – *Sub-Category*. Группа сигнатур под названием **POLICY_DB_MSSQL** отображает принцип, где **Policy** это *Type*, **DB** – *Category* и **MSSQL** – это *Sub-Category*. Эти 3 компонента сигнатур представлены ниже:

1. Тип группы сигнатур

Тип группы – это одно из значений *IDS*, *IPS* или *Policy*. Эти типы представлены выше.

2. Категория группы сигнатур

Второй уровень описывает тип приложения или протокола. Примеры:

• BACKUP
• DB
• DNS
• FTP
• HTTP

3. Подкатегория группы сигнатур Signature Group Sub-Category

Третий уровень определяет цель группы и часто указывает приложение, например, MSSQL. Подкатегория может не потребоваться, если для указания группы достаточно *Type* и *Category*, например, **APP_ITUNES**.

Списки групп IDP

Список групп IDP находится в *Приложении B*, *Группы сигнатур IDP*. В списке отображены имена групп, состоящие из *Category*, за которой следуют *Sub-Category*, *Type* может быть любым из IDS, IPS или POLICY.

Обработка с помощью нескольких действий

Для любого правила IDP можно указать несколько действий и тип действия, такой как **Protect**, который можно повторить несколько раз. У каждого действия будет одна или несколько сигнатур или групп, связанных с ним. Поиск соответствующей сигнатуры выполняется сверху вниз.

Метод подстановки (Wildcarding) в сигнатурах IDP

Для выбора более одной группы сигнатур IDP можно использовать метод подстановки (Wildcarding). Символ «?» используется как подстановочный знак в имени группы. В качестве альтернативы можно использовать символ «*» для замены набора символов любой длины в имени группы.

Предупреждение: Используйте минимальное количество сигнатур IDP

Не используйте всю базу данных сигнатур и избегайте использования сигнатур и групп сигнатур без необходимости. Используйте только те сигнатуры или группы, которые применяются к типу трафика, которому необходимо обеспечить защиту. Например, использование IDP-групп IDS_WEB, IPS_WEB*, IDS_HTTP* и * IPS_HTTP* будет подходящим для защиты HTTP-сервера.*

Использование слишком большого количества сигнатур во время сканирования может повысить нагрузку на аппаратное обеспечение межсетевого экрана, что негативно повлияет на пропускную способность.

6.5.7. Действия IDP

Функция Действие

После выявления вторжения, необходимо предпринять Действие, связанное с правилом IDP. Администратор может связать одну из трех функций Действие с IDP-правилом:

• **Ignore** – Не выполнять никаких действий, если обнаружено вторжение, и оставить соединение открытым.
• **Audit** – Оставить соединение открытым, но зарегистрировать событие.
• **Protect** – Отклонить соединение и зарегистрировать событие (с дополнительной функцией внесения в "черный список" источник соединения или переключение на ZoneDefense, как описано ниже).

«Черный список» IDP

Функция **Protect** содержит опцию добавления в "черный список" отдельных хостов или сети, активировавших правило IDP. Это означает, что весь последующий трафик, идущий с источника, который находится в "черном списке", будет автоматически отклонен системой NetDefendOS. Для получения более подробной информации о функциях «черного списка» см. *Раздел 6.7, «Черный список хостов и сетей»*.

ZoneDefense IDP

Действие **Protect** содержит опцию деактивации отдельного коммутатора D-Link, активировавшего правило IDP, с помощью функции ZoneDefense. Для получения более подробной информации о функциях ZoneDefense, см. *Главу 12, ZoneDefense*.

6.5.8. SMTP Log Receiver для событий IDP

Для того чтобы получать уведомления по электронной почте о событиях IDP, необходимо настроить SMTP Log receiver. Это сообщение электронной почты будет содержать обзор событий IDP, которые произошли в период времени, установленный пользователем.

После того, как произошло событие IDP, NetDefendOS ожидает несколько секунд (**Hold Time)** прежде, чем отправить уведомление по электронной почте. Тем не менее, сообщение будет отправлено только в том случае, если число событий, произошедших в этот период времени, равно или больее, чем значение **Log Threshold**. После отправки уведомления, NetDefendOS ожидает несколько секунд (**Minimum Repeat Time)** прежде, чем отправить новое сообщение.

IP-адрес SMTP Log Receivers

При определении SMTP log receiver, необходимо указать IP-адрес получателя. Имя домена, такое как *dns: smtp.domain.com* не может использоваться.

Пример 6.20. Настройка SMTP Log Receiver

В данном примере Правило IDP настроено с SMTP Log Receiver. Если происходит событие IDP, срабатывает Правило. Как минимум одно новое событие происходит в течение периода Hold Time, который длится 120 секунд, таким образом, достигнув уровня порога журнала (произошло не менее 2). В результате по электронной почте будет отправлено уведомление, содержащее краткую информацию о событиях IDP. После этого может произойти еще несколько событий IDP, но для предотвращения "наводнения" почтового сервера, перед отправкой новых сообщений NetDefendOS ожидает 600 секунд (10 минут). Предполагается, что SMTP-сервер настроен в адресной книге с именем **smpt-сервер**.

CLI

Добавление SMTP log receiver:

```
gw-world:/> add LogReceiver LogReceiverSMTP smt4IDP IPAddress=smtp-server
            Receiver1=youremail@yourcompany.com
```

Правила IDP:

```
gw-world:/> cc IDPRule examplerule

gw-world:/examplerule> set IDPRuleAction 1 LogEnabled=Yes
```

Web-интерфейс

Добавление SMTP log receiver:

1. Зайдите **System > Log and Event Receivers > Add > SMTP Event Receiver**

2. Введите:

- **Name:** smtp4IDP
- **SMTP Server:** smtp-server
- **Server Port:** 25
- Определите альтернативные адреса email (до 3)
- **Sender:** hostmaster
- **Subject:** Log event from NetDefendOS
- **Minimum Repeat Delay:** 600
- **Hold Time:** 120
- **Log Threshold:** 2
- Нажмите **OK**

Правила IDP:

1. Зайдите **IDP > IDP Rules**

2. Выберите правило и нажмите **Edit**

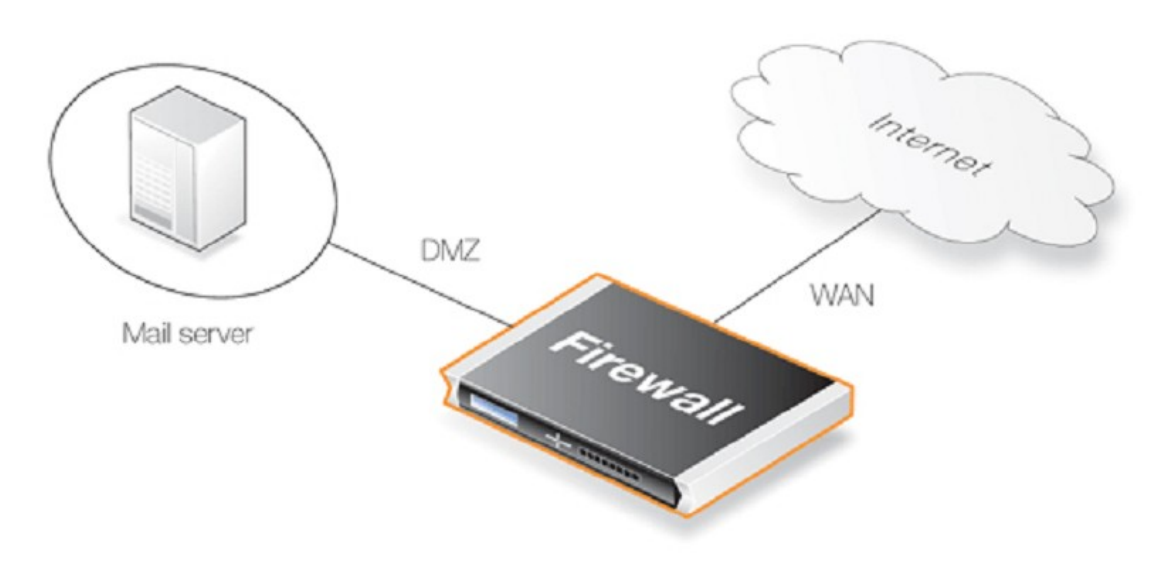
3. Выберите действие, которое необходимо зарегистрировать и нажмите **Edit**

4. Выберите **Enable logging** во вкладке **Log Settings**

5. Нажмите **OK**

Пример 6.21. Настройка IDP для почтового сервера

Данный пример подробно описывает шаги по установке IDP в простом сценарии, в котором почтовый сервер находится в сети Интернет в зоне DMZ с публичным IP-адресом. Соединение с публичной сетью Интернет можно установить через WAN-интерфейс межсетевого экрана, как показано на рисунке ниже.



Будет создано правило IDP под названием IDPMailSrvRule, и Service для использования сервиса SMTP. Интерфейс источника и Сеть источника определяют, откуда исходит трафик, в данном примере, из внешней сети. Интерфейс назначения и Сеть назначения определяют, куда направлен трафик, в данном случае, на почтовый сервер. Поэтому следут установить Сеть назначения на объекте, определяющем почтовый сервер.

CLI

Добавление правила IDP:

```
gw-world:/> add IDPRule Service=smtp SourceInterface=wan
            SourceNetwork=wannet
            DestinationInterface=dmz
            DestinationNetwork=ip_mailserver
            Name=IDPMailSrvRule
```

Определение действия правила:

```
gw-world:/> cc IDPRule IDPMailSrvRule

gw-world:/IDPMailSrvRule> add IDPRuleAction Action=Protect
                          IDPServity=All Signatures=IPS_MAIL_SMTP
```

Web-интерфейс

Добавление правила IDP:

Данное правило IDP называется *IDPMailSrvRule* и применяется к сервису SMPT. Интерфейс источника и Сеть источника определяют, откуда исходит трафик, в данном примере, из внешней сети. Интерфейс назначения и Сеть назначения определяют, куда направлен трафик, в данном случае, на почтовый сервер. Поэтому следут

установить Сеть назначения на объекте, определяющем почтовый сервер.
1. Зайдите **IDP > IDP Rules > Add > IDP Rule**

2. Введите:

• **Name:** IDPMailSrvRule
• **Service:** smtp
• Также проверьте отброшенные пакеты: весь трафик, соответствующий данному правилу, должен быть просканирован (это также означает, что трафик, что основной набор правил будет отброшен), необходимо установить флажок в поле **Protect against insertion/evasion attacks**.
• **Source Interface:** wan
• **Source Network:** wannet
• **Destination Interface:** dmz
• **Destination Network:** ip_mailserver
• Нажмите **OK**

Определите действие:

Определено действие, указывающее какие сигнатуры IDP использовать при соответствии сканируемых данных правилу, а также действия NetDefendOS, если обнаружено возможное вторжение. В этом примере, попытки вторжения будут причиной отклонения соединения, таким образом, установлено Действие Protect. Для функции Сигнатуры установлено значение IPS_MAIL_SMTP, чтобы использовать сигнатуры, которые описывают атаки из внешней сети, основанные на SMTP-протоколе.

1. Выберите вкладку **Rule Action** для правила IDP

2. Введите:

• **Action**: Protect
• **Signatures**: IPS_MAIL_SMTP
• Click **OK**

Если необходимо зарегистрировать попытки вторжения, это можно выполнить, нажав "Rule Actions" при создании правила IDP и включении регистрации. Для Severity следуте установить значение All, чтобы обпеспечить совпадение всех SMTP-атак.

Таким образом, произойдет следующее: если трафик идет из внешней сети на почтовый сервер, функция IDP будет активирована. Если трафик соответствует любой из сигнатур в группе сигнатур IPS_MAIL_SMTP, соединение будет отброшено, таким образом, осуществляется защита почтового сервера..

6.6. Предотвращение атак Denial-of-Service

6.6.1. Обзор

Используя сеть Интернет, предприятия приобретают новые возможности для бизнеса и роста. Сеть предприятия и сетевые приложения являются критически важными для бизнеса. Благодаря сети Интернет компания может не только значительно увеличить число своих клиентов, но и предоставить им ускоренное и эффективное обслуживание. В то же время, использование публичной IP-сети дает компаниям возможность сократить расходы, связанные с инфраструктурой.

К сожалению, те же преимущества, которые Интернет приносит бизнесу, также представляют интерес для хакеров, которые используют ту же общественную инфраструктуру для своих атак. Инструменты атак доступны в сети Интернет и работа по развитию применения этих инструментов часто разделена между группами начинающих хакеров — иногда называемых «хакеры-дилетанты» - по всему миру, обеспечивая круглосуточное ежедневное развитие методов атак. Многие новейшие методы атак используют распределенную топологию сети Интернет для запуска атак Отказ в обслуживании (DoS), в результате чего парализована работа Web-серверов, которые больше не могут отвечать на санкционированные запросы на соединение.

Атака DoS является одной из самых опасных сетевых атак. Появляясь совершенно неожиданно, атака DoS приводит к таким серьезным последствиям как полный отказ работы сервера, неактивные Интернет-соединения и перегрузка систем, критически важных для бизнеса.

Этот раздел рассматривает использование межсетевых экранов NetDefend для защиты организаций

от атак DoS.

6.6.2. Механизмы атак DoS

Существуют различные виды атак DoS, но можно выделить три основных типа:

• Потребление вычислительных ресурсов, таких как пропускная способность, пространство памяти на диске, или время CPU.

• Потеря информации о конфигурации, например, информации о маршрутизации.

• Повреждение физических компонентов сети.

Одним из наиболее часто используемых методов является исчерпание вычислительных ресурсов, т.е. атаки DoS приводят к остановке работы сети из-за большого количества бессмысленных или сформированных в неправильном формате запросов (flood) и «связыванию» ресурсов, используемых для запуска приложений, критически важных для бизнеса. В некоторых случаях используются уязвимые места в операционных системах Unix и Windows для намеренного разрушения системы, в то время как в других случаях большое количество внешне надежных пакетов отправляется на сайты в целях перегрузки и повреждения.

Некоторые из наиболее часто используемых атак DoS:

• Ping of Death / атаки Jolt
• «Fragmentation overlap» (Перекрытие фрагментов): Teardrop / Bonk / Boink / Nestea
• Land и LaTierra
• WinNuke
• Атаки с эффектом усиления: Smurf, Papasmurf, Fraggle
• TCP SYN Flood
• Jolt2

6.6.3. Атаки Ping of Death и Jolt Attacks

«Ping of Death» является одной из самых ранних атак уровня 3/4. Один из простейших способов выполнить эту атаку - запустить «ping-1 65 510 1.2.3.4» на Windows 95, где 1.2.3.4 - это IP-адрес компьютера-жертвы. «Jolt» – это просто специально написанная программа для создания пакетов в операционной системе, чьи команды ping отказываются генерировать пакеты с завышенными размерами.

Инициирующим фактором является то, что из-за последнего фрагмента общий размер пакета превышает 65535 байт, что является максимальным числом значений, которые могут быть представлены 16-битным целым числом. Когда значение превышено, оно возвращается к небольшому числу.

Система NetDefendOS не допустит фрагментацию, приводящую к тому, что общий размер пакета превышает 65535 байт. Помимо этого, существуют настраиваемые пределы размеров IP-пакета в разделе «Расширенные Настройки».

Атаки Ping of Death и Jolt регистрируются в журналах NetDefendOS «Ping of Death» как отброшенные пакеты с указанием на правило «LogOversizedPackets». IP-адрес отправителя может быть подделан.

6.6.4. Атаки Fragmentation overlap: *Teardrop, Bonk, Boink и Nestea*

Teardrop - это атака перекрытия фрагментов. Множество IP-стеков показали неустойчивую работу (чрезмерное истощение ресурсов или сбои), подвергнувшись перекрытию фрагментов.

NetDefendOS обеспечивает защиту от атак перекрытия фрагментации. Перекрывающимся фрагментам не разрешено проходить через систему.

Teardrop и похожие атаки регистрируются в журналах NetDefendOS как отброшенные пакеты с указанием на правило «IllegalFrags». IP-адрес отправителя может быть подделан.

6.6.5. Атаки *Land* и *LaTierra*

Атаки Land и LaTierra работают, отправляя пакет компьютеру-жертве и заставляя его отвечать самому себе, что, в свою очередь, генерирует еще один ответ самому себе, и т.д. Это вызовет либо остановку работы компьютера, либо повреждение.

Атака осуществляется за счет использования IP-адреса компьютера-жертвы в поле Source и Destination.

NetDefendOS обеспечивает защиту от атаки Land, применяя защиту от IP-спуфинга ко всем пакетам. В настройках по умолчанию, NetDefendOS будет просто сравнивать входящие пакеты с содержанием таблицы маршрутизации; если пакет приходит на интерфейс, который отличается от интерфейса, ожидаемого системой, пакет будет отброшен.

Атаки Land и LaTierra регистрируются в журналах NetDefendOS как отброшенные пакеты с указанием на правило «AutoAccess» по умолчанию, или, если в настройках содержатся Правила доступа пользователя, с указанием на правило Правило доступа, отбросившее пакет. В данном случае IP-адрес отправителя не представляет интереса, так как он совпадает с IP-адресом получателя.

6.6.6. Атака *WinNuke*

Принцип действия атаки WinNuke заключается в подключении к TCP-службе, которая не умеет обрабатывать «out-of-band» данные (TCP сегменты с набором битов URG), но все же принимает их. Это обычно зацикливает службу, что приводит к потреблению всех ресурсов процессора.

Одной из таких служб была NetBIOS через службу TCP/IP на WINDOWS-машинах, которая и дала имя данной сетевой атаке.

NetDefendOS обеспечивает защиту двумя способами:

• Благодаря использованию политики для входящего трафика количество атак значительно сокращается. Только открытые и публичные службы могут стать жертвами атак.

• Удаление по умолчанию битов URG из всех сегментов TCP, проходящих через систему (настраивается через **Advanced Settings> TCP> TCPUrg**).

Как правило, атаки WinNuke регистрируются в журналах NetDefendOS как отброшенные пакеты с указанием на правило, запрещающим попытку соединения. Для соединений, разрешенных в системе, появляется запись категории «TCP» или «DROP» (в зависимости от настройки TCPUrg), с именем правила «TCPUrg». IP-адрес отправителя может быть не поддельным; «троекратное рукопожатие» должно быть полностью выполнено до момента отправки сегментов «out-of-band».

6.6.7. Атаки с эффектом усиления: *Smurf, Papasmurf, Fraggle*

Эта категория атак использует некорректно настроенные сети, которые усиливают поток пакетов и отправляют его на конечный узел. Целью является чрезмерное использование полосы пропускания,

потребление всего потенциала Интернет-соединения жертвы. Атакующий с широкой полосой пропускания может не использовать эффект усиления для того, чтобы полностью занять всю полосу пропускания жертвы. Тем не менее, эти атаки позволяют атакующим с меньшей полосой пропускания, чем у жертвы, использовать усиление, чтобы занять полосу пропускания жертвы.

• «Smurf» и «Papasmurf» отправляют echo-пакеты ICMP по адресу широковещательной рассылки открытых сетей с несколькими компьютерами, выдавая IP-адрес источника за адрес жертвы. Далее все компьютеры в открытой сети «отвечают» жертве.

• «Fraggle» базируется на «Smurf», но использует echo-пакеты UDP и отправляет их на порт 7. В основном, атака «Fraggle» получает меньше факторов усиления, так как служба echo активирована у небольшого количества хостов в сети Интернет.

Атаки Smurf регистрируются в журналах NetDefendOS как множество отброшенных пакетов ICMP Echo Reply. Для перегрузки сетей используется поддельный IP-адрес. Также атаки Fraggle отображаются в журналах NetDefendOS как большое количество отброшенных пакетов (или разрешенных пакетов в зависимости от политики). Для перегрузки сетей используется поддельный IP-адрес.

В настройках по умолчанию, NetDefendOS отбрасывает пакеты, отправленные по адресу широковещательной рассылки усиливающей сети (настраивается через **Advanced Settings > IP > DirectedBroadcasts**). С точки зрения политики для входящего трафика, любая незащищенная сеть может также стать усиливающией.

Защита на стороне компьютера-жертвы

Smurf и похожие атаки являются атаками, расходующими ресурсы, так как они используют потенциал Интернет-соединения. В общем случае, межсетевой экран представляет собой «узкое место» в сети и не может обеспечить достаточную защиту против этого типа атак. Когда пакеты доходят до межсетевого экрана, ущерб уже нанесен.

Тем не менее, система NetDefendOS может помочь в снятии нагрузки с внутренних серверов, делая их доступными для внутренней службы, или, возможно, службы через вторичное Интернет-соединение, которое не является целью атаки.

• Типы flood-атак *Smurf* и *Papasmurf* будут рассматриваться как ответы ICMP Echo на стороне жертвы. Пока используются правила *FwdFast*, таким пакетам не будет разрешено инициировать новые соединения, независимо от того, существуют ли правила, разрешающие прохождение пакетов.

• Пакеты *Fraggle* могут прийти на любой UDP-порт назначения, который является мишенью атакующего. В этой ситуации может помочь увеличение ограничений в наборе правил.

Встроенная функция *Traffic Shaping* также помогает справляться с некоторыми flood-атаками на защищенные серверы.

6.6.8. Атаки *TCP SYN Flood*

Принцип работы атак *TCP SYN Flood* заключается в отправке большого количества пакетов TCP SYN на указанный порт и игнорировании пакетов SYN ACK, отправленных в ответ. Это позволит ограничить локальные ресурсы TCP-стека на Web-сервере жертвы, таким образом, что он не сможет ответить на большое количество пакетов SYN, пока не истечет определенный таймаут существующих полуоткрытых соединений.

Система NetDefendOS обеспечивает защиту от flood-атак TCP SYN, если опция *SYN Flood Protection* активирована в объекте службы, связанным с правилом в наборе IP-правил. Опция также иногда упоминается как *SYN Relay*.

Защита от flood-атак включается автоматически в предварительно определенных службах **http-in, https-in, smtp-in** и **ssh-in**. Если новый пользовательский объект службы определяется администратором, то опция защиты от flood-атак может быть включена или отключена по желанию.

Механизм защиты от атак SYN Flood

Принцип механизма защиты от атак SYN Flood заключается в выполнения 3-кратного подтверждения установления соединения с клиентом. В системе NetDefendOS могут происходить перегрузки по причине использования новейших средств обработки ресурсов и отсутствия ограничений, как правило, расположенных в других операционных системах. В то время как у других операционных систем могут возникнуть проблемы с 5 полуоткрытыми соединениями, не получившими подтверждение от клиента, NetDefendOS может заполнить всю таблицу состояний, прежде чем что-то произойдет. Когда таблица состояний заполнена, старые неподтвержденные соединения будут отброшены, чтобы освободить место для новых соединений.

Обнаружение SYN Floods

Атаки TCP SYN flood регистрируются в журналах NetDefendOS как большое количество новых соединений (или отброшенных пакетов, если атака направлена на закрытый порт). IP-адрес отправителя может быть подделан.

ALG автоматически обеспечивает защиту от flood-атак

Следует отметить, что нет необходимости включать функцию защиты от атак SYN Flood на объекте службы, с которым связан ALG. ALG автоматически обеспечивает защиту от атак SYN flood.

6.6.9. Атака *Jolt2*

Принцип работы атаки Jolt2 заключается в отправке непрерывного потока одинаковых фрагментов компьютеру-жертве. Поток из нескольких сотен пакетов в секунду останавливает работу уязвимых компьютеров до прекращения потока.

NetDefendOS обеспечивает комплексную защиту от данной атаки. Обычно первый фрагмент ставится в очередь, ожидая прихода ранних фрагментов, таким образом, фрагменты передаются по порядку, но в данном случае этого не произойдет, так как не пройдет даже первый фрагмент. Следующие фрагменты будут отброшены, так как они идентичны первому фрагменту.

Если выбранное злоумышленником значение смещения фрагмента больше, чем ограничения, налагаемые настройкой **Advanced Settings>LengthLim** в NetDefendOS, пакеты будут немедленно отброшены. Атаки Jolt2 могут быть зарегистрированы в журналах NetDefendOS. Если злоумышленник выбирает слишком большое значение смещения фрагмента для атаки, это будет зарегистрировано в журналах NetDefendOS как отброшенные пакеты с указанием на правило «LogOversizedPackets». Если значение смещения фрагмента достаточно низкое, регистрации в журнале не будет. IP-адрес Отправителя может быть подделан.

6.6.10. Атаки Distributed DoS (DDoS)

Наиболее сложной DoS-атакой является атака *Distributed Denial of Service*. Хакеры используют сотни или тысячи компьютеров по всей сети Интернет, устанавливая на них программное обеспечение DDoS и управляя всеми этими компьютерами для осуществления скоординированных атак на сайты-жертвы. Как правило, эти атаки расходуют полосу пропускания, обрабатывающую способность маршрутизатора, или ресурсы сетевого стека, нарушая сетевые соединения с жертвой.

Хотя последние атаки DDoS были выполнены как в частных, так и в публичных сетях, хакеры, как правило, часто предпочитают корпоративные сети из-за их открытого, распределенного характера. Инструменты, используемые для запуска DDoS-атак, включают Trin00, TribeFlood Network (TFN), TFN2K и Stacheldraht.

6.7. «Черный список» хостов и сетей

Обзор

NetDefendOS предоставляет «черный список» адресов хоста или IP-адресов сети, который используется для обеспечения защиты.

Некоторые подсистемы NetDefendOS поддерживают возможность дополнительно занести в «черный список» хост или сеть при определенных условиях. Это следующие подсистемы:

• Обнаружение и предотвращение вторжений (IDP)

• Правила порога (доступно только на некоторых моделях межсетевых экранов NetDefend – для получения более подробной информации см. *Раздел 10.3, «Правила порога»*)

Функции «черного списка»

Можно включить функцию автоматического занесения в «черный список» хоста или сети в IDP и в правилах порога, указав действие **Protect** при срабатывании правила. Существует три функции «черного списка»:

Time to Block Host/Network in Seconds	Хост или сеть, которые являются источником трафика, остаются в «черном списке» в течение указанного времени, а затем удаляются. Если тот же источник инициирует другую запись в «черном списке», то в таком случае будет восстановлено первоначальное время блокировки, «истинное значение» (другими словами, не «накопленное»).
Block only this Service	По умолчанию «черный список» блокирует все сервисы для запуска хоста.
Exempt already established connections from Blacklisting	Если существуют установленные соединения с тем же источником, что и новая запись в «черном списке», то они не будут удалены, если данная опция настроена.

IP-адреса или сети добавляются в список, далее трафик с этих источников блокируется на указанный период времени.

Примечание: Повторный запуск не повлияет на «черный список»

Содержимое «черного списка» не будет утеряно при отключении межсетевого экрана NetDefend и его перезапуске.

«Белый список»

Для того чтобы Интернет-трафик, поступающий из надежных источников, таких как рабочие станции управления, не попал в «черный список» ни при каких обстоятельствах, система NetDefendOS также поддерживает «*белый список*». Любой IP-адрес объекта может быть добавлен в этот «белый список».

Совет: Важные IP-адреса следует заносить в «белый список»

Рекомендуется добавить межсетевой экран NetDefend в «белый список», а также IP-адрес или сеть рабочей станции управления, так как их занесение в «черный список» может иметь серьезные последствия для

сетевых операций.

Важно также знать, что хотя использование «белого списка» предотвращает занесение в «черный список» определенных источников, это не мешает механизмам NetDefendOS (например, Правила порога) отбрасывать или отклонять соединения с этого источника. «Белый список» предотвращает добавление источника в «черный список», если это действие определено правилом.

Для получения более подробной информации см. *Раздел 6.5.7, «Действия IDP»*, *Раздел 10.3.8, «Правило Черного списка»* и *Раздел 10.3, «Правила порога».*

Примечание: Фильтрация содержимого в «черном списке» является отдельным действием

Фильтрация содержимого в «черном списке» - это отдельное действие, при котором используется отдельный логический список (см. Раздел 6.3, «Фильтрация Web-содержимого»).

Команда CLI *blacklist*

Команда *blacklist* может быть использована для просмотра, а также для управления текущим содержимым «черного списка» и «белого списка». Текущий «черный список» можно просмотреть с помощью команды:

```
gw-world:/> blacklist -show -black
```

Данная команда *blacklist* может использоваться для удаления хоста из «черного списка» с помощью опции -*unblock*.

Глава 7. Преобразование адресов

В данной главе представлено описание возможностей механизма преобразования адресов операционной системы NetDefendOS.

7.1. Обзор

Возможность системы NetDefendOS присваивать другие IP-адреса пакетам, проходящим через межсетевой экран NetDefend, называется *преобразованием (трансляцией) IP-адресов*.

Наличие возможности преобразования одного IP-адреса в другой дает ряд преимуществ. Наиболее важными из них являются следующие два.

- В защищенной сети могут использоваться хосты с приватными IP-адресами, которые имеют доступ в Интернет. Также возможна ситуация, когда к серверам с приватными IP-адресами можно обращаться из сети Интернет.
- Усложняя топологию защищенной сети, таким образом, повышаем ее защиту от несанкционированного доступа. Механизм трансляции адресов скрывает IP-адреса внутренних компьютеров, значительно усложняя получение доступа к ним извне.

Типы преобразования адресов

Система NetDefendOS поддерживает два типа преобразования адресов:

- Dynamic Network Address Translation (NAT) – динамическое преобразование сетевых адресов;
- Static Address Translation (SAT) – статическое преобразование адресов.

Оба типа преобразования адресов основаны на *правилах* NetDefendOS. Правила применяются к определенному типу трафика и зависят от источника/назначения сети/интерфейса, а также типа протокола. Для конфигурирования механизма преобразования адресов в системе NetDefendOS используются два типа IP-правил: NAT-правила и SAT-правила.

В этом разделе приводится описание и примеры конфигурирования NAT- и SAT-правил.

7.2. NAT

Динамическое преобразование сетевых адресов (NAT) обеспечивает механизм преобразования исходного IP-адреса источника в другой адрес. У исходящих пакетов изменяются IP-адреса источников. IP-адреса входящих пакетов, направленных по адресу этого источника, снова преобразуются в исходные IP-адреса.

Существует два важных преимущества механизма NAT:

- IP-адреса частных клиентов и хостов «спрятаны» за IP-адресом межсетевого экрана;

- Только межсетевому экрану требуется публичный IP-адрес. Хостам и сетям за межсетевым экраном могут быть назначены приватные IP-адреса, но они имеют доступ к публичной сети Интернет через публичный IP-адрес.

NAT обеспечивает преобразование IP-адресов типа «много в один»

Механизм NAT обеспечивает преобразование IP-адресов «много в один». Это значит, что каждое NAT-правило из набора IP-правил будет выполнять преобразование нескольких IP-адресов источника в один IP-адрес источника.

Чтобы обработать данные о состоянии сессии, для каждого соединения, установленного с динамически преобразованного адреса, используется уникальная комбинация из номера порта и IP-адреса отправителя. Помимо IP-адреса источника, система NetDefendOS также осуществляет автоматическое преобразование номера порта источника. Т.е. для того, чтобы установить соединение, IP-адреса нескольких источников преобразуются в один IP-адрес, и соединения различаются только по уникальному номеру порта каждого соединения.

Следующая схема иллюстрирует концепцию NAT.

Рис. 7.1. NAT-преобразование IP-адресов

На рисунке представлены три соединения с IP-адресов *A*, *B* и *C*, которые преобразованы с помощью NAT в один IP-адрес источника *N*. Начальные номера портов изменены.

При установлении очередного NAT-соединения, система NetDefendOS случайным образом определяет следующий свободный номер порта источника. Механизм случайного назначения портов способствует повышению уровня безопасности.

Ограничение количества соединений

Количество одновременных NAT-соединений не может превышать 64 500. При этом каждое соединение «состоит» из уникальной пары IP-адресов. Здесь под «парой IP-адресов» подразумевается соединение, установленное между IP-адресом на каком-либо интерфейсе системы NetDefendOS и IP-адресом некоторого внешнего хоста. Но если два разных IP-адреса внешнего хоста подключены с использованием одного и того же NAT-адреса межсетевого экрана, то они составляют две разные уникальные IP-пары. Поэтому количество в 64 500 одновременных соединений не является верхним пределом для всего межсетевого экрана NetDefend.

Совет: Ограничения количества соединений можно избежать, используя NAT-пулы.

Для всех сценариев за исключением чрезмерных, максимально возможное количество соединений, приходящееся на уникальную IP-пару, является достаточным. Однако если необходимо увеличить количество одновременных NAT-соединений межсетевого экрана NetDefend и определенного хоста с внешним IP-адресом, используется такое свойство системы NetDefendOS, как ***NAT-пулы.*** *Данное свойство позволяет автоматически задействовать дополнительные IP-адреса межсетевого экрана.*

Более детальная информация по данной теме представлена в разделе 7.3. «NAT-

пулы».

IP-адрес источника, используемый в NAT

В системе NetDefendOS существует три способа определения IP-адреса источника, который будет использован в NAT:

- **Использование IP-адреса интерфейса**

  Когда устанавливается новое соединение, для него по таблице маршрутизации назначается выходной интерфейс. И когда система NetDefendOS выполняет преобразование адресов, IP-адрес принятого интерфейса используется в качестве нового IP-адреса источника. Этот способ определения IP-адреса используется как способ по умолчанию.

- **Назначение определенного IP-адреса**

  В качестве нового IP-адреса источника может быть назначен определенный IP-адрес. Для этого необходимо, чтобы этот IP-адрес опубликовывался в ARP на выходном интерфейсе, т.к. в противном случае, обратный трафик не будет получен межсетевым экраном NetDefend. Этот метод используется, когда IP-адрес источника должен отличаться от адреса интерфейса источника. С использованием этого метода, например, Интернет-провайдер с помощью механизма NAT может выдавать разные IP-адреса разным клиентам.

- **Использование IP-адреса из NAT-пула**

  В качестве IP-адреса источника может использоваться *NAT-пул* – диапазон IP-адресов, определенный администратором сети. В этом случае в качестве IP-адреса NAT будет приниматься очередной доступный IP-адрес из пула. Причем NAT-пулов может существовать несколько. А также один NAT-пул может быть использоваться в более чем одном *NAT-правиле*. Более подробно эта тема освещена далее в *разделе 7.3. «NAT-пулы»*.

Применение NAT-преобразования

Следующий пример демонстрирует практическое применение механизма NAT в процессе установления нового соединения.

1. Отправитель *192.168.1.5* посылает пакет с динамически назначенного порта 1038 серверу *195.55.66.77* на порт 80.

```
192.168.1.5:1038 => 195.55.66.77:80
```

2. В этом примере используется параметр Use Interface Address, поэтому считаем *195.11.22.33* адресом интерфейса. Порт источника случайным выбором преобразован в определенный свободный порт межсетевого экрана NetDefend с номером больше 1024. В данном примере допускаем, что выбран порт 32789. Тогда пакет отправлен в свой адрес назначения.

```
195.11.22.33:32789 => 195.55.66.77:80
```

3. Сервер-получатель обрабатывает пакет и отправляет ответ.

```
195.55.66.77:80 => 195.11.22.33:32789
```

4. Система NetDefendOS получает пакет и сравнивает его со своим перечнем открытых соединений. Когда соответствующее соединение найдено, система восстанавливает исходный адрес и пересылает пакет.

```
195.55.66.77:80 => 192.168.1.5:1038
```

5. Источник-отправитель получает ответ.

Последовательность этих событий демонстрируется на следующей схеме:

Рис. 7.2. Пример функционирования механизма NAT

Пример 7.1. Добавление *NAT*-правила

В данном примере демонстрируется добавление *NAT*-правила, по которому осуществляется преобразование адресов для всего HTTP-трафика внутренней сети.

CLI

Во-первых, сделайте текущей категорией основной набор IP-правил *main:*

```
gw-world:/> cc IPRuleSet main
```

Затем, создайте IP-правило:

```
gw-world:/> add IPRule Action=NAT Service=http
                       SourceInterface=lan
                       SourceNetwork=lannet
                       DestinationInterface=any
                       DestinationNetwork=all-nets
                       Name=NAT_HTTP
                       NATAction=UseInterfaceAddress
```

Вернитесь на верхний уровень:

```
gw-world:/> cc
```

Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Задайте правилу соответствующее имя, например, *NAT_HTTP*

3. Затем введите:

- **Action:** NAT
- **Service:** http
- **Source Interface:** lan
- **Source Network:** lannet
- **Destination Interface:** any
- **Destination Network:** all-nets

4. Удостоверьтесь, что на вкладке **NAT** выбрана опция **Use Interface Address**

5. Нажмите **OK**

Протоколы совместимые с NAT

Механизм динамического преобразования адресов способен работать с протоколами TCP, UDP и ICMP, обеспечивая высокий уровень функциональности, поскольку уникальность соединения в этих трех протоколах определяется данными, которые могут быть скорректированы. Для других протоколов IP-уровня, уникальность соединения определяется по адресу отправителя, адресу назначения и номерам протоколов.

Таким образом:

- компьютер локальной сети может обмениваться информацией с несколькими внешними серверами, используя один и тот же IP-протокол;
- компьютер локальной сети может обмениваться информацией с несколькими внешними серверами, используя разные IP-протоколы;
- несколько компьютеров локальной сети могут обмениваться информацией с несколькими внешними серверами, используя один и тот же IP-протокол;
- несколько компьютеров локальной сети могут обмениваться информацией с одним и тем же сервером, используя разные IP-протоколы;
- несколько компьютеров локальной сети *не* могут обмениваться информацией с одним и тем же внешним сервером, используя один и тот же IP-протокол.

Примечание: Ограничения применимы только к протоколам IP-уровня

Эти ограничения применяются только к протоколам IP-уровня, таким как OSPF и L2TP. Исключение составляют протоколы TCP, UDP и ICMP. Ограничения не распространяются на протоколы telnet, FTP, HTTP и SMTP, использующие в качестве транспорта TCP и UDP.

Система NetDefendOS может менять информацию о номере порта в заголовках TCP и UDP, делая каждое соединение уникальным, т.к. адреса источников таких соединений преобразованы в один IP-адрес.

Некоторые протоколы могут некорректно работать при преобразовании адресов независимо от транспорта.

Сохранение анонимности Интернет-трафика с NAT

Одним из полезных свойств NAT в NetDefendOS является обеспечение провайдерами анонимизации доступа к публичной части сети Интернет. Анонимность трафика от клиента к серверу достигается тем, что публичный IP-адрес клиента не представлен ни в запросах на доступ к серверу, ни в одноранговом трафике.

Далее следует типичный пример, в котором межсетевой экран NetDefend выступает в роли PPTP-сервера и терминирует PPTP-туннель для PPTP-клиентов. Клиенты, которые хотят сохранить анонимность, обмениваются информацией с локальным Интернет-провайдером, используя PPTP. Трафик направляется к анонимному провайдеру услуг, где установлен межсетевой экран NetDefend, который, в качестве PPTP-сервера, терминирует для клиента PPTP-туннель. Данная структура представлена на следующей схеме.

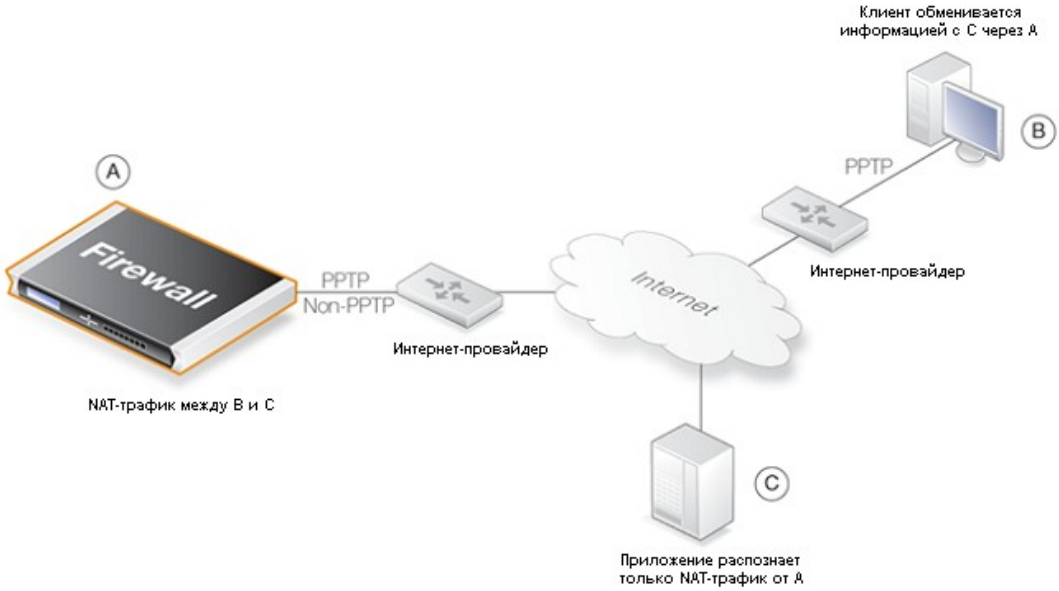


Рис. 7.3. Анонимность с NAT.

В наборе IP-правил системы NetDefendOS прописаны NAT-правила. Входящий трафик от клиента с помощью NAT направляется обратно в Интернет. Обмен информацией с клиентом происходит по PPTP-протоколу. PPTP-туннель от клиента терминируется на межсетевом экране. Когда трафик от межсетевого экрана направляется обратно в Интернет, он уже не инкапсулируется в протокол PPTP.

В тот момент, когда приложение, например, Web-сервер получает запросы от клиента, адрес источника этих запросов меняется с IP-адреса клиента на внешний IP-адрес провайдера услуг. Приложение отсылает свои ответы обратно на межсетевой экран, который передает трафик клиенту через PPTP-туннель. Исходный IP-адрес клиента в трафике не виден, т.к. он передается после терминации PPTP-туннеля в NetDefendOS.

Обычно весь трафик проходит через один физический интерфейс, и этот интерфейс имеет единый публичный IP-адрес. Если в наличии несколько публичных IP-адресов, можно использовать несколько интерфейсов.

За счет обеспечения анонимности трафика появляются незначительные накладные расходы, связанные с обработкой данных, но если для данного процесса задействованы значительные ресурсы аппаратных средств это не вызывает проблем.

Если вместо PPTP-соединений используется протокол L2TP, применяются аналогичные методы. Более подробно эти протоколы рассматриваются далее в *Разделе 9.5.4, «PPTP/L2TP-Клиенты»*.

7.3. NAT-пулы

Обзор

Преобразование сетевых адресов (Network Address Translation, NAT) дает возможность нескольким внешним клиентам и хостам с уникальными частными внутренними IP-адресами обмениваться информацией с удаленными хостами через один внешний публичный IP-адрес (данный вопрос подробно освещается в *Разделе 7.2., «NAT»*). Если в наличии несколько публичных внешних IP-адресов, то используется объект *«NAT-пул»*, чтобы при установлении новых подключений назначать им публичные IP-адреса из пула.

NAT-пулы обычно применяются, если требуется создать много уникальных подключений используя один порт. Менеджер портов в системе NetDefendOS может поддерживать до 65 000 соединений с уникальной комбинацией из IP-адреса источника и IP-адреса назначения. Большое количество портов может потребоваться, если многие внутренние клиенты используют, например, программные средства по совместному использованию файлов. Аналогичные требования могут возникнуть в

ситуации, когда множество клиентов одновременно имеет доступ в Интернет через прокси-сервер. Проблема с ограниченным количеством портов решается с помощью выделения дополнительных внешних IP-адресов для выхода в Интернет и использования NAT-пулов для распределения новых подключений через эти IP-адреса.

Типы NAT-пулов

Существует три типа NAT-пулов, каждый из которых производит распределение новых подключений разными способами:

- **Stateful** (Фиксирующий состояние)
- **Stateless** (Нефиксирующий состояние)
- **Fixed** (Фиксированный)

Эти типы NAT-пулов подробно рассматриваются далее.

NAT-пулы типа *Stateful*

Когда выбран тип NAT-пула *Stateful*, система NetDefendOS назначает вновь созданному подключению тот внешний IP-адрес, через который в настоящий момент осуществляется наименьшее количество соединений, полагая, что данный адрес является менее загруженным. Записи обо всех таких соединениях хранятся в памяти NetDefendOS. Все последующие соединения с тем же внутренним клиентом/хостом будут использовать тот же внешний IP-адрес.

Преимуществом данного подхода является обеспечение сбалансированной нагрузки нескольких внешних каналов связи Интернет-провайдера по количеству соединений и гарантия того, что информация от внешнего хоста всегда вернется обратно на IP-адрес отправителя, что важно в таких протоколах как HTTP, где применяются cookies-файлы. Неудобством является использование дополнительных ресурсов памяти, требующихся системе NetDefendOS для отслеживания соединения в таблице состояний, а также незначительные накладные расходы по обработке данных в процессе установления нового соединения.

Для того чтобы таблица состояний не содержала записей по неактивным процессам передачи информации, можно установить время активного состояния соединения (**State Keepalive**) – время неактивности подключения в секундах, по истечении которого, запись об этом подключении будет удалена из таблицы состояний. По прошествии данного периода система NetDefendOS определит, что исходящих соединений от данного ассоциированного внутреннего хоста создаваться больше не будет. В случае если запись о состоянии подключения из таблицы удалена, то последующие подключения данного хоста будут заноситься в новую запись таблицы и могут распределяться между другими внешними IP-адресами из NAT-пула.

Т.к. таблица состояний расходует ресурсы памяти, существует возможность ограничить ее размер, используя параметр *Max States* объекта «NAT-пул». Таблица состояний формируется не сразу, она увеличивается в размере по мере необходимости. Одна запись в таблице состояний отображает все соединения одного хоста за межсетевым экраном NetDefend, независимо от того, к какому внешнему хосту данное соединение относится. Если размер таблицы состояний достиг значения параметра *Max States*, в таблице перезаписывается то состояние, у которого самое длительное время неактивности. Если все состояния из таблицы активны, тогда новое соединение игнорируется. Исходя из практики, значение параметра *Max States* должно быть не менее количества локальных хостов или клиентов имеющих доступ к сети Интернет.

В каждом NAT-пуле есть только одна таблица соответствий, поэтому, если один NAT-пул несколько раз используется в разных IP-правилах NAT, то они будут совместно использовать одну и ту же таблицу состояний.

NAT-пулы типа *Stateless*

Если выбран тип NAT-пула *Stateless*, это означает, что таблица состояний не формируется, а внешний IP-адрес, выбираемый для каждого нового подключения, это тот IP-адрес через который осуществляется наименьшее количество соединений. Т.е. два разных подключения от одного внутреннего хоста к одному и тому же внешнему хосту могут использовать два разных внешних IP-адреса.

Преимуществом NAT-пула с типом *Stateless* является то, что он обеспечивает эффективное

распределение новых соединений между внешними IP-адресами без лишних затрат памяти на формирование таблицы состояний. Помимо этого, время на обработку данных при установлении каждого нового соединения сокращается. К недостаткам способа относится то, что он не подходит для подключений, требующих наличия постоянного внешнего IP-адреса.

NAT-пулы типа *Fixed*

Если выбран тип NAT-пула *Fixed*, это означает, что каждый внутренний клиент или хост поставлен в соответствие одному из внешних IP-адресов с помощью алгоритма хеширования. Хотя администратор не имеет возможности контролировать, какое из внешних подключений будет использоваться, такой подход гарантирует, что определенный внутренний клиент или хост всегда будет обмениваться информацией через один и тот же внешний IP-адрес.

Преимуществом типа *Fixed* является то, что он не требует ресурсов памяти на создание таблицы состояний и обеспечивает очень высокую скорость обработки данных при установлении нового соединения. Хотя точное распределение нагрузки не является частью данного подхода, распределение нагрузки через внешние подключения должно выполняться для обеспечения случайного характера алгоритма распределения.

Использование IP-пулов

При назначении внешних IP-адресов в NAT-пул не обязательно прописывать их вручную. Можно выбрать объект «IP-пул» системы NetDefendOS. IP-пулы получают наборы IP-адресов автоматически через DHCP-сервер и могут также автоматически добавлять внешние IP-адреса в NAT-пулы. Получить дополнительную информацию по данному вопросу можно в *Разделе 5.4, «IP-пулы»*.

Использование механизма Proxy ARP

Внешний маршрутизатор посылает ARP-запросы межсетевому экрану NetDefend, чтобы на основе ARP-ответов системы NetDefendOS принять решение о выборе внешних IP-адресов из NAT-пула. Таким образом, корректное формирование таблицы маршрутизации внешнего маршрутизатора зависит непосредственно от механизма Proxy ARP.

В разделе настроек NAT-пулов администратор должен определить, какие интерфейсы будут использоваться NAT-пулами по умолчанию. Это дает возможность подключить механизм Proxy ARP для NAT-пула на всех интерфейсах, но может привести к ситуации, когда прописываются маршруты к тем интерфейсам, на которые не должны доставляться пакеты. Поэтому рекомендуется, чтобы интерфейс или интерфейсы, используемые для Proxy ARP механизма NAT-пула, были точно определены.

Использование NAT-пулов

NAT-пулы используются в сочетании со стандартными IP-правилами NAT. В диалоговом окне определения NAT-правила присутствует возможность выбора NAT-пула, который должен использоваться вместе с правилом. С установления этой связи начинается функционирование NAT-пула.

Пример 7.2. Использование NAT-пулов

В данном примере демонстрируется создание NAT-пула с диапазоном внешних IP-адресов *10.6.13.10 – 10.16.13.15*, который затем используется в IP-правиле *NAT* для HTTP-трафика на **WAN**-интерфейсе.

Web-интерфейс

А. Во-первых, необходимо создать в адресной книге новый объект диапазона адресов:

1. Зайдите **Objects > Address Book > Add > IP address**

2. Задайте IP-диапазону соответствующее имя, например, *nat_pool_range*

3. Введите диапазон *10.6.13.10 – 10.16.13.15* в поле **IP Address** (возможен формат представления подсети, такой как 10.6.13.0/24 – IP-адреса 0 и 255 автоматически исключаются из диапазона).

4. Нажмите **OK**

Б. Затем создайте объект «NAT-пул» типа *Stateful* с именем *stateful_natpool*:

1. Зайдите **Objects > NAT Pools > Add > NAT Pool**

2. Затем введите:

- **Name:** stateful_natpool
- **Pool type:** stateful
- **IP Range:** nat_pool_range

3. Выберите вкладку **Proxy ARP** и добавьте **WAN**-интерфейс.

4. Нажмите **OK**

B. Теперь определите NAT-правило в наборе IP-правил:

1. Зайдите **Rules > IP Rules > Add > IP Rule**

2. В разделе **General** введите:

- **Name:** введите подходящее имя, такое как *nat_pool_rule*
- **Action**: NAT

3. В разделе **Address filter** введите:

- **Source Interface:** int
- **Source Network:** int-net
- **Destination Interface:** wan
- **Destination Network:** all-nets
- **Service:** HTTP

4. Перейдите на вкладку **NAT**:

- Проверьте опцию **Use NAT Pool**
- Выберите **stateful_natpool** из выпадающего списка

5. Нажмите **OK**

7.4. SAT

Система NetDefendOS может преобразовывать целые диапазоны IP-адресов и/или портов. Эти преобразования заключаются в установлении соответствия адреса или порта с определенным адресом или портом в новом диапазоне, причем при переназначении адресов и портов предшествующего диапазона им в соответствие ставится не один и тот же адрес/порт. Выполнение этих функций в системе NetDefendOS носит название *статического преобразования адресов* (Static Address Translation, SAT).

Примечание: Port forwarding (Перенаправление портов)

*Некоторые производители сетевого оборудования используют термин «**port forwarding**» ссылаясь на SAT. Оба термина подразумевают выполнение одинаковых функций.*

SAT требует несколько IP-правил

В отличие от механизма NAT, SAT требует определения не одного IP-правила, а нескольких. SAT-правило, которое добавляется первоначально, определяет только трансляцию адреса, но система

NetDefendOS не завершает выбор правил на нахождении подходящего SAT-правила. Система продолжает искать соответствующее *«Allow»*, *NAT*- или *FwdFast*-правило. Только когда оно найдено, первое SAT-правило может быть выполнено.

Первое SAT-правило определяет только механизм преобразования адресов. Второе, связанное правило, например, правило с действием «*Allow*», создается, чтобы фактически разрешить прохождение трафика через межсетевой экран.

Во втором правиле должен отображаться IP-адрес назначения до его преобразования

При создании IP-правил для SAT важно помнить о том, что, например, правило с действием «Allow» должно разрешать доступ с IP-адресом назначения до его преобразования. Распространенной ошибкой является создание «Allow» правила, которое разрешает доступ с адресом, уже преобразованным SAT-правилом.

Таким образом, если SAT-правило транслирует адрес назначения с *1.1.1.1* на *2.2.2.2*, то затем второе связанное правило должно разрешать прохождение трафика на адрес назначения *1.1.1.1*, а не на *2.2.2.2*.

Только после обработки второго правила дается разрешение на прохождение трафика. Система NetDefendOS производит подбор маршрута для переназначенного адреса, чтобы принять решение о том с какого интерфейса должны отправляться пакеты.

7.4.1. Преобразование IP-адресов «один к одному»

Самой простейшей формой использования SAT является преобразование одного IP-адреса. Чаще всего такая ситуация встречается когда внешним пользователям предоставляют возможность получать доступ к защищенному серверу в зоне DMZ с приватным IP-адресом.

Роль зоны DMZ

В этом разделе руководства пользователя целесообразно рассмотреть концепцию и роль компьютерной сети известной как *демилитаризованная зона (Demilitarized Zone, DMZ).*

При наличии зоны DMZ администратор может размещать в ней ресурсы, которые будут доступны непроверенным клиентам, обычно осуществляющим доступ к серверам через Интернет. Подобные серверы максимально подвержены угрозе внешних атак и угрозе несанкционированного доступа к зашифрованным материалам.

Выделяя такие серверы в зону DMZ, мы отделяем их от наиболее восприимчивых к атакам локальных внутренних сетей, и это позволяет системе NetDefendOS лучше контролировать поток данных между зоной DMZ и внутренними сетями и быстрее ликвидировать повреждения системы безопасности, которые могут возникать на DMZ-серверах.

На рисунке 7.4. представлена схема построения типичной компьютерной сети с межсетевым экраном NetDefend, посредством которого происходит обмен информацией между серверами в зоне DMZ, локальными клиентами из сети *LAN* и Интернет.

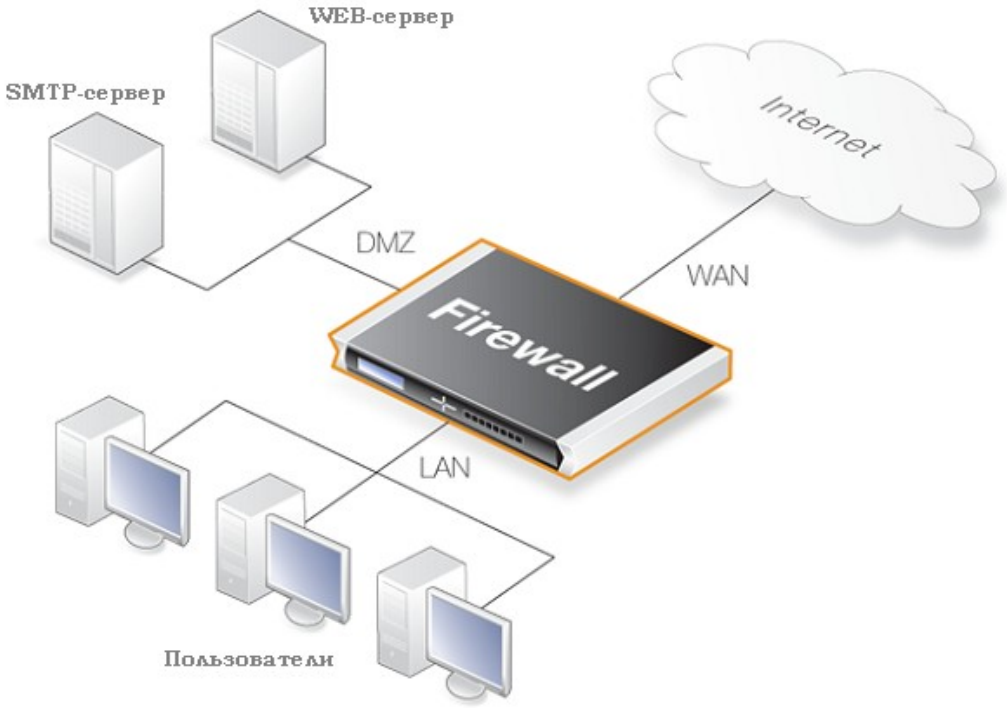


Рисунок 7.4. Роль зоны DMZ.

Примечание: Любой порт может стать портом DMZ

Во всех моделях устройств серии NetDefend компании D-link предусмотрен специальный Ethernet-порт, маркированный аббревиатурой «DMZ» и предназначенный специально для создания DMZ-зоны. Несмотря на это, данный порт можно использовать для других целей, так же как и любой другой Ethernet-порт можно использовать для создания зоны DMZ.

Пример 7.3. Разрешение трафика на защищенный WEB-сервер в зоне DMZ

В данном примере демонстрируется создание SAT-политики, которая будет перенаправлять и разрешать доступ соединениям из сети Интернет к WEB-серверу, размещенному в зоне DMZ. Межсетевой экран NetDefend подключен к Интернет через WAN-интерфейс с адресным объектом *wan_ip*, определенным как IP-адрес *195.55.66.77*. IP-адрес WEB-сервера – *10.10.10.5*. Он доступен через DMZ-интерфейс.

CLI

Во-первых, сделайте текущей категорией основной набор IP-правил *main:*

gw-world:/> **cc IPRuleSet main**

Затем, создайте IP-правило SAT:

```
gw-world:/> add IPRule Action=SAT Service=http
                       SourceInterface=any
                       SourceNetwork=all-nets
                       DestinationInterface=core
                       DestinationNetwork=wan_ip
                       SATTranslate=DestinationIP
                       SATTranslateToIP=10.10.10.5
                       Name=SAT_HTTP_To_DMZ
```

Затем создайте соответствующее правило с действием «*Allow*»

```
gw-world:/main> add IPRule action=Allow Service=http
                       SourceInterface=any
                       SourceNetwork=all-nets
                       DestinationInterface=core
                       DestinationNetwork=wan_ip
                       Name=Allow_HTTP_To_DMZ
```

Web-интерфейс

Во-первых, необходимо создать SAT-правило:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Задайте SAT-правилу соответствующее имя, например, *SAT_HTTP_To_DMZ*

3. Затем введите:

- **Action**: SAT
- **Service**: http
- **Source Interface**: any
- **Source Network**: all-nets
- **Destination Interface**: core
- **Destination Network**: wan_ip

4. Удостоверьтесь, что на вкладке **SAT** выбрана опция **Destination IP Address**.

5. В поле **New IP Address** введите *10.10.10.5*.

6. Нажмите **OK**

Затем создайте соответствующее правило с действием «*Allow*»

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Задайте правилу соответствующее имя, например, *Allow_HTTP_To_DMZ*:

3. Затем введите:

- **Action**: Allow

• **Service**: http

• **Source Interface**: any

• **Source Network**: all-nets

• **Destination Interface**: core

• **Destination Network**: wan_ip

4. На вкладке **Service** выберите в списке **Predefined** значение **http**:

5. Нажмите **OK**

В результате выполнения примера 7.3. создается набор правил, в котором присутствуют два правила:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST 10.10.10.5 80
2	Allow	any	all-nets	core	wan_ip	http

Эти два правила позволяют получить доступ к WEB-серверу через внешний IP-адрес межсетевого экрана NetDefend. Правило 1 устанавливает, что преобразование адреса может произойти только, если соединение было разрешено, а правило 2 – разрешает данное соединение.

Разумеется, также потребуется правило, которое позволяет внутренним компьютерам динамически получать преобразованные адреса для доступа в Интернет. В данном примере будем использовать следующее NAT-правило, которое позволяет любому компьютеру внутренней сети получать доступ к сети Интернет:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
3	NAT	lan	lannet	any	all-nets	All

А что не так с этим набором правил?

Если преобразование адреса выполняется не только по причине функциональности, но и с целью усиления безопасности, то последней цели мы не достигаем, т.к. очевидно, что созданный набор правил делает IP-адреса внутренних компьютеров видимыми для компьютеров зоны DMZ. Согласно правилу 2, в момент, когда внутренние компьютеры будут подключаться к WAN-порту 80 с именем wan_ip, им будет позволено продолжить соединение, т.к. исходя из правила – это подходящее направление для передачи информации. С точки зрения безопасности, для компьютеров внутренней сети машины из зоны DMZ ничем не отличаются от других серверов, подключенных к сети Интернет; им также нельзя «доверять», что и служит основной причиной их размещения в зоне DMZ.

Существует два выхода из данной ситуации:

1. Можно изменить правило 2 так, чтобы оно было применимо только к трафику извне.

2. Можно поменять местами правила 2 и 3, чтобы для внутреннего трафика NAT-правило выполнялось перед выполнением правила *Allow*.

Какой из предложенных вариантов лучше? Для данной конфигурации – это не имеет значения. Оба решения одинаково хороши в действии.

Но, предположим, что мы используем другой интерфейс *ext2* межсетевого экрана NetDefend и подключаем его к другой сети, возможно к сети соседней компании для более быстрого обмена информацией между серверами.

Если будет выбрано решение 1, набор правил должен выглядеть так:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST 10.10.10.5 80
2	Allow	wan	all-nets	core	wan_ip	http
3	Allow	ext2	ext2net	core	wan_ip	http
4	NAT	lan	lannet	any	all-nets	All

Для каждого интерфейса увеличивается количество правил, позволяющих обмен информацией с WEB-сервером.

Порядок исполнения правил не так важен, и это может помочь избежать ошибок.

Если выбор падает на решение 2, набор правил должен выглядеть так:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST 10.10.10.5 80
2	NAT	lan	lannet	any	all-nets	All
3	Allow	any	all-nets	core	wan_ip	http

Здесь не требуется увеличивать количество правил, но только в случае если все интерфейсы являются проверенными и через них можно обмениваться информацией с WEB-сервером. При добавлении же непроверенного интерфейса, через который нельзя обмениваться информацией с WEB-сервером, перед правилом, предоставляющим доступ всем машинам к WEB-серверу, необходимо разместить разделяющее Drop-правило.

Принятие решения о выборе того или иного способа действия зависит от обстоятельств в каждом конкретном случае.

Пример 7.4. Разрешение трафика на WEB-сервер внутренней сети

В данном примере рассматривается WEB-сервер с приватным IP-адресом, размещенный во внутренней сети. С точки зрения безопасности такое размещение является неверным, т.к. WEB-серверы слишком уязвимы для атак и, следовательно, должны размещаться в зоне DMZ. Однако этот пример демонстрируется, т.к. такая схема достаточно проста в использовании.

Для того чтобы внешние пользователи имели доступ к WEB-серверу, они должны иметь возможность устанавливать соединение с помощью публичных адресов. В данном примере происходит преобразование 80 порта внешнего IP-адреса межсетевого экрана NetDefend в 80 порт WEB-сервера:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST wwwsrv 80
2	Allow	any	all-nets	core	wan_ip	http

Эти два правила позволяют получить доступ к WEB-серверу через внешний IP-адрес межсетевого экрана NetDefend. Правило 1 устанавливает, что преобразование адреса может произойти только, если соединение было разрешено, а правило 2 – разрешает данное соединение.

Также потребуется правило, которое позволяет внутренним компьютерам динамически получать преобразованные адреса для доступа в Интернет. В данном примере используется правило, которое позволяет любому компьютеру внутренней сети анонимно получать доступ к сети Интернет через NAT:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
3	NAT	lan	lannet	any	all-nets	All

Недостаток этого набора правил заключается в том, что он не будет работать для трафика внутренней сети.

Чтобы проиллюстрировать, как это может произойти, будем использовать следующие IP-адреса:

• *wan_ip* (195.55.66.77) – публичный IP-адрес

• *lan_ip* (10.0.0.1) – приватный внутренний IP-адрес межсетевого экрана NetDefend

• *wwwsrv* (10.0.0.2) – приватный IP-адрес WEB-сервера

• *PC1* (10.0.0.3) – приватный IP-адрес компьютера

Согласно правилам будут выполняться действия в следующем порядке:

• Компьютер *PC1* отсылает пакет на *wan_ip*, чтобы выйти на сайт *www.ourcompany.com*:

10.0.0.3:1038 => 195.55.66.77:80

• Система NetDefendOS преобразует адрес в соответствии с правилом 1 и пересылает пакет в соответствии с правилом 2:

10.0.0.3:1038 => 10.0.0.2:80

• WEB-сервер *wwwsrv* обрабатывает пакет и отсылает ответ:

10.0.0.2:80 => 10.0.0.3:1038

Этот ответ направляется на компьютер *PC1,* минуя межсетевой экран, что служит причиной возникновения проблем.

Компьютер *PC1* ожидает ответа с *195.55.66.77:80*, а не с *10.0.0.2:80*. Неподходящий ответ отбрасывается, а компьютер *PC1* продолжает ожидать ответа, который не придет с *195.55.66.77:80.*

Разрешить проблемную ситуацию можно, незначительно изменяя набор правил, как это было описано выше в примере 7.3, причем, в данном случае можно выбрать любой из двух предложенных способов, например, способ 2.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST wwwsrv 80
2	NAT	lan	lannet	any	all-nets	All
3	Allow	any	all-nets	core	wan_ip	http

• Компьютер *PC1* отсылает пакет на адрес *wan_ip*, чтобы выйти на сайт *www.ourcompany.com*:

10.0.0.3:1038 => 195.55.66.77:80

• Система NetDefendOS статически преобразует адрес в соответствии с правилом 1 и динамически в соответствии с правилом 2:

10.0.0.1:32789 => 10.0.0.2:80

• WEB-сервер *wwwsrv* обрабатывает пакет и отсылает ответ:

10.0.0.2:80 => 10.0.0.1:32789

• Ответ достигает цели и оба преобразованных адреса возвращаются в исходное состояние.

195.55.66.77:80 => 10.0.0.3:1038

В этом случае ответ поступает на компьютер *PC1* с соответствующего адреса.

Другим способом решения данной проблемы является предоставление внутренним клиентам возможности соединяться напрямую с адресом 10.0.0.2. Это полностью поможет избежать проблем связанных с трансляцией адресов, однако, это не всегда практично.

7.4.2. Преобразование IP-адресов «много ко многим»

Одно SAT-правило можно использовать при преобразовании целого диапазона IP-адресов. В этом случае результатом преобразования будет замена первого исходного IP-адреса на первый IP-адрес из списка преобразования и т.п.

Например, политикой SAT определяется, что соединения с сетью 194.1.2.16/29 должны транслироваться на сеть 192.168.0.50. Далее представлена таблица с результатом преобразования адресов, которое последует:

Исходный адрес	Адрес после трансляции
194.1.2.16	192.168.0.50
194.1.2.17	192.168.0.51
194.1.2.18	192.168.0.52

194.1.2.19	192.168.0.53
194.1.2.20	192.168.0.54
194.1.2.21	192.168.0.55
194.1.2.22	192.168.0.56
194.1.2.23	192.168.0.57

Другими словами:

- При попытке соединения с *194.1.2.16* произойдет соединение с *192.168.0.50*.
- При попытке соединения с *194.1.2.22* произойдет соединение с *192.168.0.56*.

Этот способ может использоваться в ситуации, когда необходимо иметь доступ к одному из нескольких защищенных серверов, размещенных в зоне DMZ, через уникальный публичный IP-адрес.

Пример 7.5. Трансляция трафика на несколько защищенных WEB-серверов

В данном примере демонстрируется создание SAT-политики, которая будет перенаправлять и разрешать доступ соединениям из сети Интернет к пяти WEB-серверам, размещенным в зоне DMZ. Межсетевой экран NetDefend подключен к сети Интернет через WAN-интерфейс, используются публичные IP-адреса из диапазона от 10.10.10.5 до 10.10.10.9, они доступны через DMZ-интерфейс.

Чтобы выполнить задание, необходимо сделать следующее:

• Определить объект, содержащий публичные IP-адреса.

• Определить еще один объект на основе IP-адресов WEB-сервера.

• Опубликовать публичные IP-адреса на WAN-интерфейсе, используя механизм публикации ARP.

• Создать SAT-правило, по которому будет выполняться преобразование.

• Создать правило с действием «*Allow*», разрешающее входящие HTTP-соединения.

CLI

Создайте адресный объект, содержащий публичные IP-адреса:

```
gw-world:/> add Address IP4Address wwwsrv_pub
                    Address=195.55.66.77-195.55.66.81
```

Затем, создайте еще один адресный объект на основе IP-адресов WEB-сервера:

```
gw-world:/> add Address IP4Address wwwsrv_priv_base
                    Address=10.10.10.5
```

Опубликуйте публичные IP-адреса на WAN-интерфейсе, используя механизм публикации ARP. Один элемент ARP необходим для каждого IP-адреса:

```
gw-world:/main> add ARP Interface=wan IP=195.55.66.77 mode=Publish
```

Повторить процедуру для каждого из пяти публичных IP-адресов.

Сделайте текущей категорией основной набор IP-правил *main:*

```
gw-world:/> cc IPRuleSet main
```

Создайте SAT-правило для трансляции:

```
gw-world:/> add IPRule Action=SAT Service=http
                    SourceInterface=any
                    SourceNetwork=all-nets
                    DestinationInterface=wan
                    DestinationNetwork=wwwsrv_pub
                    SATTranslateToIP=wwwsrv_priv_base
                    SATTranslate=DestinationIP
```

Создайте соответствующее правило с действием «*Allow*»

```
gw-world:/> add IPRule Action=Allow Service=http
                    SourceInterface=any
                    SourceNetwork=all-nets
                    DestinationInterface=wan
                    DestinationNetwork=wwwsrv_pub
```

Web-интерфейс

Создайте адресный объект, содержащий публичные IP-адреса:

1. Зайдите **Objects > Address Book > Add > IP address**

2. Задайте объекту соответствующее имя, например, *wwwsrv_pub*

3. В поле **IP Address** введите *195.55.66.77 – 195.55.66.77.81*

4. Нажмите **OK**

Затем, создайте еще один адресный объект на основе IP-адресов WEB-сервера:

1. Зайдите **Objects > Address Book > Add > IP address**

2. Задайте объекту соответствующее имя, например, *wwwsrv_priv_base*

3. В поле **IP Address** введите *10.10.10.5*

4. Нажмите **OK**

Опубликуйте публичные IP-адреса на WAN-интерфейсе, используя механизм публикации ARP. Один элемент ARP необходим для каждого IP-адреса:

1. Зайдите **Interfaces > ARP > Add > ARP**

2. Затем введите:

- **Mode**: Publish
- **Interface**: wan
- **IP Address**: 195.55.66.77

3. Нажмите **OK** и повторите предыдущие действия для каждого из 5 публичных IP-адресов.

Создайте SAT-правило для трансляции:

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Определите для правила соответствующее имя, например, *SAT_HTTP_To_DMZ*

3. Затем введите:

Action: SAT

Servce: http

Source Interface: any

Source Network: all-nets

Destination Interface: wan

Destination Network: wwwsrv_pub

4. Перейдите на вкладку **SAT**

5. Удостоверьтесь, что выбрана опция **Destination IP Address**

6. В выпадающем списке **New IP Address** выберите *wwwsrv_priv*

7. Нажмите **OK**

Создайте соответствующее правило с действием «*Allow*»

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Задайте правилу соответствующее имя, например, *Allow_HTTP_To_DMZ*:

3. Затем введите:

- **Action**: Allow
- **Service**: http
- **Source Interface**: any
- **Source Network**: all-nets
- **Destination Interface**: wan
- **Destination Network**: wwwsrv_pub

4. Нажмите **OK**

7.4.3. Соответствие «много к одному»

Система NetDefendOS может преобразовывать диапазоны и/или группы IP-адресов в один IP-адрес.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	wan	194.1.2.16 – 194.1.2.20, 194.1.2.30	http SETDEST all-to-one 192.168.0.50 80

По этому правилу производится преобразование типа «много к одному» всех адресов из диапазона 194.1.2.16 – 194.1.2.20 и 194.1.2.30 в IP-адрес 192.168.0.50.

- При обращении по адресу *194.1.2.16* порт 80 соединение произойдет с адресом *192.168.0.50*.
- При обращении по адресу *194.1.2.30* порт 80 соединение произойдет с адресом *192.168.0.50*.

Примечание:

В случае если адресом назначения являются все сети (all-nets), всегда производится трансляция типа «много к одному».

7.4.4. Трансляция «порт-адрес»

Трансляция «порт-адрес» (Port Address Translation, PAT) используется, чтобы изменять адрес источника или адрес назначения на уровне портов.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	wan	wwwsrv_pub	TCP 80-85 SETDEST 192.168.0.50 1000

По такому правилу производится преобразование типа «один к одному» всех портов из диапазона 80 – 85 в диапазон 1080 – 1085.

• При обращении к публичному адресу WEB-сервера порт 80 соединение произойдет с публичным адресом WEB-сервера порт 1080.

• При обращении к публичному адресу WEB-сервера порт 84 соединение произойдет с публичным адресом WEB-сервера порт 1084.

Примечание: Для трансляции порт-адрес требуется объект «Custom Service»

Чтобы создать SAT-правило, которое позволяет производить трансляцию «порт-адрес», в правиле должен использоваться объект «Custom Service».

7.4.5. Протоколы совместимые с SAT

Обычно механизм статического преобразования адресов совместим со всеми протоколами, которые позволяют выполнение трансляции адресов. Однако существуют протоколы, которые могут быть транслированы только в специальных случаях, а также протоколы, которые вообще не могут быть транслированы.

Протоколы, которые нельзя транслировать при использовании SAT, чаще всего также несовместимы с NAT. Это может происходить по следующим причинам.

• В протоколах, требующих шифрования невозможно чередование адресов. Это относится ко многим VPN-протоколам.

• IP-адреса прописываются в протоколах на уровнях TCP и UDP, и необходимо, чтобы на IP-уровне, адреса отображались также как и в данных на других уровнях. Примерами являются FTP и Logon на домене NT через NetBIOS.

• Если некоторая группа приложений пытается установить новые динамические соединения с адресами, видимыми этой группе, то это можно исправить сменой приложения или изменением настроек межсетевого экрана.

Не существует определенного списка протоколов, которые могут или не могут быть работать с механизмом преобразования адресов. Общепринято, что VPN-протоколы, а также протоколы, по которым в дополнение к начальному соединению возможно создание дополнительных соединений, не совместимы с механизмом преобразования адресов.

7.4.6. Множественное соответствие SAT-правил

Система NetDefendOS не завершает выбор правил на нахождении подходящего SAT-правила, а продолжает искать соответствующее *«Allow»*, *NAT*- или *FwdFast*-правило. Только когда оно найдено, система NetDefendOS может выполнить статическое преобразование адресов.

Будет выполняться SAT-правило, соответствующее своему адресу, найденное первым. На одном и том же соединении одновременно может действовать два SAT-правила, если одно из них транслирует адрес отправителя, а второе транслирует адрес получателя.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wwwsrv_pub	TCP 80-85 SETDEST 192.168.0.50 1080
2	SAT	lan	lannet	all-nets	Standard	SETSRC pubnet

Оба правила, представленные выше, могут одновременно исполняться для одного соединения. В этом случае адреса внутренних источников буду преобразовываться в адреса из сети «*pubnet*» с типом преобразования «один к одному». Помимо этого, при попытке установления соединения с публичным адресом WEB-сервера – адрес назначения преобразуется в его приватный адрес.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	lan	lannet	wwwsrv_pub	TCP 80-85	SETDEST intrasrv 1080
2	SAT	any	all-nets	wwwsrv_pub	TCP 80-85	SETDEST wwwsrv-priv 1080

В последнем наборе правил оба правила определяют трансляцию адреса назначения, и только одно из них будет выполняться. При попытке внутреннего соединения с публичным адресом WEB-сервера, данный запрос будет перенаправлен на сервер внутренней сети. При других обращениях к публичному адресу WEB-сервера, запросы будут перенаправляться на приватный адрес публично доступного WEB-сервера.

Следует еще раз напомнить, что для того чтобы все представленные выше правила были выполнены, требуется наличие соответствующих правил с действием «*Allow*».

7.4.7. SAT-правила и FwdFast-правила

Статическое преобразование адресов можно использовать совместно с FwdFast-правилами, однако обратный трафик должен быть точно передан и транслирован.

Следующие правила служат примером выполнения статического преобразования адресов с использованием FwdFast-правил в отношении WEB-сервера, размещенного во внутренней сети.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST wwwsrv 80
2	SAT	lan	wwwsrv	any	all-nets	80 -> All SETSRC wan_ip 80
3	FwdFast	any	all-nets	core	wan_ip	http
4	FwdFast	lan	wwwsrv	any	all-nets	80 -> All

К данному набору правил необходимо добавить NAT-правило, чтобы разрешить всем соединениям внутренней сети доступ в Интернет.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	NAT	lan	lannet	any	all-nets	All

Последовательность выполнения представленных правил такова:

• Внешний трафик к *wan_ip:80* соответствует правилам 1 и 3 и будет перенаправлен на *wwwsrv*. Первый пункт выполняется правильно.

• Обратный трафик с *wwwsrv*:80 соответствует правилам 2 и 4, и его адрес источника будет преобразован в *wan_ip:80*. Второй пункт выполняется правильно.

• Внутренний трафик к *wan_ip:80* соответствует правилам 1 и 3 и будет перенаправлен на *wwwsrv*. Третий пункт выполняется почти правильно. Пакеты поступят на *wwwsrv*, но обратный трафик от *wwwsrv*:80 к компьютерам внутренней сети будет направлен напрямую. Такой механизм не будет работать корректно, т.к. пакеты будут интерпретированы как поступившие с несоответствующего адреса.

Поменяем последовательность выполнения правил, поставив NAT-правило между SAT-правилами и FwdFast-правилами.

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST wwwsrv 80
2	SAT	lan	wwwsrv	any	all-nets	80 -> All SETSRC wan_ip 80
3	NAT	lan	lannet	any	all-nets	All
4	FwdFast	any	all-nets	core	wan_ip	http
5	FwdFast	lan	wwwsrv	any	all-nets	80 -> All

Посмотрим, что изменится.

• Внешний трафик к *wan_ip:80* соответствует правилам 1 и 3 и будет перенаправлен на *wwwsrv*. Первый пункт выполняется правильно.

• Обратный трафик с *wwwsrv*:80 соответствует правилам 2 и 3, поэтому ответы будут динамически транслироваться. Вследствие этого порт источника изменится на совершенно другой порт, который не будет работать.

Изменить сложившуюся ситуацию можно с помощью следующего набора правил:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Параметры
1	SAT	any	all-nets	core	wan_ip	http SETDEST wwwsrv 80
2	SAT	lan	wwwsrv	any	all-nets	80 -> All SETSRC wan_ip 80
3	FwdFast	lan	wwwsrv	any	all-nets	80 -> All
4	NAT	lan	lannet	any	all-nets	All
5	FwdFast	lan	wwwsrv	any	all-nets	80 -> All

• Внешний трафик к *wan_ip:80* соответствует правилам 1 и 5 и будет перенаправлен на *wwwsrv*.

• Обратный трафик с *wwwsrv*:80 соответствует правилам 2 и 3.

• Внутренний трафик к *wan_ip:80* соответствует правилам 1 и 4 и будет перенаправлен на *wwwsrv*. Адресом отправителя будет внутренний IP-адрес межсетевого экрана NetDefend, что гарантирует прохождение обратного трафика через межсетевой экран NetDefend.

• Обратный трафик автоматически обрабатывается механизмом контроля состояния протокола (Stateful Inspection) межсетевого экрана NetDefend.

Глава 8. Аутентификация пользователя

В данной главе представлено описание процесса аутентификации пользователя в операционной системе NetDefendOS.

- Обзор
- Настройка аутентификации
- Настройка HTML-страниц

8.1. Обзор

Обычно когда пользователи подключаются к защищенным ресурсам через межсетевой экран NetDefend, прежде чем им будет разрешен доступ, они должны пройти процесс аутентификации.

В данной главе рассматривается описание процесса настройки аутентификации в системе NetDefend, и первоначально будут рассмотрены общие понятия, связанные с аутентификацией пользователя.

Подтверждение идентичности

Целью аутентификации является подтверждение идентичности пользователя, на основании которой администратор сети может разрешить или запретить ему доступ к ресурсам. Существуют следующие типы подтверждений.

А. «Личность пользователя»: по уникальным для каждого человека определяющим признакам, например, по отпечаткам пальцев.

Б. «Наличие чего-либо у пользователя»: например, смарт-карты, сертификата X.507, открытого или закрытого ключа.

В. «Знание пользователем чего-либо»: например, пароля.

Способ (А) может потребовать наличия специализированного оборудования, например, такого как биометрический считыватель.

Способы (Б) и (В) являются наиболее распространенными способами идентификации в сфере сетевой безопасности. Однако и они имеют недостатки: ключи могут быть перехвачены, смарт-карты – украдены, пароли – разгаданы или пользователь может просто рассказать кому-то свой пароль. Методы (Б) и (В) можно комбинировать, например, перед началом использования, смарт-карта может требовать ввода пароля или PIN-кода.

Использование комбинации из имени пользователя и пароля

В текущей главе описывается процесс аутентификации пользователя, при котором для получения доступа к ресурсам пользователь вручную вводит комбинацию из учетного имени пользователя и пароля. Примером может служить получение доступа к сети Интернет клиентами внутренней сети через межсетевой экран NetDefend по протоколу HTTP.

При таком типе аутентификации комбинация из имени пользователя и пароля становится объектом атак различных программных средств, цель которых подобрать или разгадать комбинацию, поэтому пароль должен быть правильно выбран.

Пароль должен:

- состоять из 8 символов, которые не повторяются;
- содержать символы в произвольном порядке (порядок символов, редко встречающийся во фразах);
- содержать прописные и строчные буквы;
- содержать цифры и специальные символы.

Также чтобы пароль оставался надежным следует:

- нигде не записывать пароль;
- никому не сообщать пароль;
- регулярно менять пароль, например, каждые три месяца.

8.2. Настройка аутентификации

8.2.1. Краткий обзор процесса настройки

Последовательность настройки аутентификации пользователя (*User Authentication*) в операционной системе NetDefendOS следующая:

- Создать источник аутентификации (*Authentication Source*), который представляет собой базу данных, содержащую комбинации имен пользователей и их паролей. Источником аутентификации может быть:
    1. Локальная база данных пользователей, являющаяся внутренней по отношению к системе NetDefendOS.
    2. Сервер RADIUS, являющийся внешним по отношению к системе NetDefendOS.
    3. Сервер LDAP, также являющийся внешним по отношению к системе NetDefendOS.
- Создать правило аутентификации (*Authentication Rule*), определяющее, какой трафик, проходящий через межсетевой экран должен проходить аутентификацию и какая запись базы аутентификации должна при этом использоваться. Более подробная информация дана в *разделе 8.2.5 «Правила аутентификации»*.
- При необходимости, определить IP-объект для IP-адресов клиентов, которые будут проходить аутентификацию. IP-объект может быть напрямую связан с правилом аутентификации в качестве *originator IP* или может быть связан с группой аутентификации (*Authentication Group*).

- Создать IP-правила, разрешающие аутентификацию, а также предоставляющие клиентам, принадлежащим IP-объекту, доступ к ресурсам.

В следующих разделах упомянутые этапы настройки аутентификации пользователя буду рассматриваться более подробно:

- *Раздел 8.2.2. «Локальная база данных пользователей».*
- *Раздел 8.2.3. «Внешние серверы RADIUS».*
- *Раздел 8.2.4. «Внешние серверы LDAP».*
- *Раздел 8.2.5. «Правила аутентификации».*

8.2.2. Локальная база данных пользователей

Локальная база данных пользователей – это встроенный системный реестр NetDefendOS, который содержит параметры авторизованных пользователей и групп пользователей. Имена пользователей и пароли могут вноситься в эту базу через WEB-интерфейс или интерфейс командной строки. Для упрощения процесса администрирования пользователи с одинаковыми правами объединены в группы.

Принадлежность к группе

Каждый пользователь в локальной базе данных пользователей может по выбору быть определен в качестве члена одной из групп аутентификации. Эти группы не являются предопределенными (за исключением групп *administrators* и *auditors*, которые будут описаны далее), их определяет администратор в виде списка текстовых строк. Определять названия групп следует с учетом регистра клавиатуры. Группы аутентификации не прописываются в правилах аутентификации, но связаны с IP-объектами, которые используются наборе IP-правил.

Использование групп с IP-правилами

При определении сети источника (*Source Network*) для IP-правила может использоваться IP-объект, определенный пользователем и связанный с группой аутентификации. Таким образом, IP-правило затем будет применяться только к зарегистрированным клиентам, которые принадлежат связанной группе сети источника.

Целью является ограничение возможности доступа отдельной группы пользователей к определенным сетям с помощью IP-правил, которые применяются только к членам данной группы. Чтобы получить доступ к ресурсу, должно быть создано IP-правило разрешающее доступ, а клиент должен быть членом группы сети источника, связанной с этим правилом.

Предоставление прав администратора

Когда пользователь определен, он может быть добавлен к двум группам с правами администратора, определенным по умолчанию:

- **Группа *administrators***

  Члены этой группы могут регистрироваться в системе NetDefendOS через WEB-интерфейс, удаленный интерфейс командной строки и имеют права изменения конфигурации системы NetDefendOS.

- **Группа *auditors***

  Члены этой группы имеют схожие права с группой *administrators*, за исключением того, что *auditors* могут только просматривать конфигурацию системы, но не изменять ее.

Конфигурация PPTP/L2TP

Если клиент подключается к межсетевому экрану NetDefend по PPTP/L2TP, то для пользователя, внесенного в локальную базу системы NetDefendOS, должны быть определены следующие три опции:

- **Статический IP-адрес клиента (Static Client IP Address)**

  Это IP-адрес, который должен быть у клиента для прохождения аутентификации. Если адрес не определен, пользователь может иметь любой IP-адрес. Эта опция предоставляет дополнительную степень защиты пользователям с фиксированными IP-адресами.

- **Подсеть пользователя (Network behind user)**

  Если для пользователя определена подсеть, то при его подключении, в главную таблицу маршрутизации *main* системы NetDefendOS автоматически добавляется маршрут. Существование этого маршрута означает, что любой трафик, предназначенный для этой сети, будет направляться через PPTP/L2TP туннель пользователя.

  По окончании соединения пользователя система автоматически удаляет маршрут.

Внимание: Эту опцию надо использовать с осторожностью

Администратор должен тщательно продумать возможные последствия использования этой опции. Например, значение опции ***all-nets (все сети)*** *направит весь Интернет трафик через туннель данного пользователя.*

- **Метрика для маршрутов сетей (Metric for Networks)**

  Если опция **Подсеть пользователя (Network behind user)** определена, то для маршрутов, автоматически добавляемых системой NetDefendOS, используется метрика. Если существует два маршрута к одной и той же сети, то с помощью метрики выбирается тот из них, который будет использоваться.

Примечание: Другие источники аутентификации не имеют PPTP/L2TP опций.

Спецификация открытого ключа SSH

Для PPTP/L2TP-клиентов использование ключа при аутентификации является альтернативой использования комбинации «имя пользователя/пароль». Закрытый ключ может быть определен для пользователя из локальной базы данных при выборе предварительно загруженного объекта *SSH Client Key* системы NetDefendOS. Для подтверждения личности пользователя при его подключении происходит автоматическая проверка используемых им ключей. После подтверждения нет необходимости вводить имя пользователя и пароль.

Чтобы использовать это свойство, релевантные объекты *SSH Client Key* или нерелевантные объекты должны быть определены в системе NetDefendOS отдельно. Ключи пользователей являются типами объектов аутентификации (*Authentication Objects*) WEB-интерфейса. При определении требуется загрузка файла открытого ключа для создания пары ключу, который используется клиентом.

8.2.3. Внешние серверы RADIUS

Причины использования внешних серверов

При сложной топологии сети с большим объемом работы для администратора предпочтительным является наличие центральной базы аутентификации на выделенном сервере. Когда в сети более одного межсетевого экрана и тысячи пользователей, оперирование отдельными базами аутентификации на каждом устройстве становится проблематичным. В этом случае внешний сервер аутентификации, отвечая на запросы системы NetDefendOS, может выполнять функции подтверждения комбинаций «имя пользователя/пароль». Для того чтобы обеспечить такую возможность система NetDefendOS поддерживает протокол RADIUS (*Remote Authentication Dial-in User Service*).

Использование RADIUS в системе NetDefendOS

Система NetDefendOS может выступать в роли клиента RADIUS, отсылая учетные записи пользователей с параметрами доступа в RADIUS-сообщениях, предназначенных RADIUS-серверу. Сервер обрабатывает запросы и отправляет ответные RADIUS-сообщения с разрешением или запретом доступа для пользователей. В системе NetDefendOS можно определить один или несколько внешних серверов.

Безопасность с RADIUS

Для обеспечения безопасности часто устанавливается секретный ключ (*shared secret*) для совместного использования RADIUS-клиентом и RADIUS-сервером. Ключ активирует шифрование сообщений, пересылаемых от RADIUS-клиента к серверу, и имеет вид достаточно длинной текстовой строки. Строка может содержать до 100 символов и должна вводиться с учетом регистра клавиатуры.

RADIUS использует PPP для передачи запросов с именем пользователя и паролем от клиента к RADIUS-серверу, а также использует схемы аутентификации PPP, такие как PAP и CHAP. RADIUS-сообщения посылаются в виде UDP-сообщений через порт UDP *1812*.

Поддержка групп пользователей

RADIUS-аутентификация поддерживает перечень групп пользователей. Пользователь может также быть определен в группе *administrators* или группе *auditors*.

8.2.4. Внешние серверы LDAP

Серверы LDAP (Lightweight Directory Access Protocol – облегчённый протокол доступа к каталогам) могут использоваться системой NetDefendOS в качестве источника аутентификации. В такой реализации межсетевой экран NetDefend выполняет функции клиента по отношению к одному или нескольким LDAP-серверам. Конфигурируется несколько альтернативных серверов, на случай, если некоторые серверы будут недоступны.

Настройка LDAP-аутентификации

Существует два этапа настройки аутентификации пользователя с помощью LDAP-серверов.

- Определение одного или нескольких LDAP-серверов для аутентификации пользователя в системе NetDefendOS.
- Указание одного или нескольких этих LDAP-серверов в правиле аутентификации пользователя.

  Если LDAP-серверов несколько, в правиле аутентификации они указываются списком. То, в каком порядке серверы указаны в списке, определяет последовательность обращения к ним.

  Первый сервер из списка имеет наивысший приоритет и будет использоваться первым. Если аутентификация не выполнена или сервер недоступен, то будет использоваться второй сервер из списка и так далее.

Вопросы, касающиеся LDAP

Настройка LDAP-аутентификации бывает не такой простой как, например, настройка RADIUS. Параметры, используемые при определении LDAP-сервера в системе NetDefendOS, имеют большое значение. Ряд вопросов требует особого внимания:

- LDAP-серверы отличаются по реализации. Система NetDefendOS предоставляет возможность разных вариантов конфигурации LDAP-серверов, и некоторые опции в различных конфигурациях могут меняться в зависимости от программного обеспечения сервера.
- Аутентификация PPTP- или L2TP-клиентов может требовать внесения некоторых изменений в настройки LDAP-сервера. Этот вопрос будет рассмотрен далее.

Microsoft Active Directory в качестве LDAP-сервера

Служба Active Directory от компании Microsoft может конфигурироваться в системе NetDefendOS как LDAP-сервер. В настройке LDAP-сервера системы NetDefendOS имеется опция, которая имеет значение для Active Directory – атрибут «имя» (*Name Attribute*). Данной опции следует установить значение *SAMAccountName*.

Определение LDAP-сервера

В системе NetDefendOS могут быть определены один или несколько объектов «LDAP-сервер». Эти объекты содержат информацию для системы NetDefendOS о том, какие LDAP-серверы доступны, и как к ним получить доступ.

Иногда бывает не так просто определить LDAP-сервер в системе NetDefendOS, т.к. некоторое программное обеспечение для LDAP-серверов не всегда точно соответствует техническим условиям LDAP. LDAP-администратор может внести изменения в схему (*schema*) LDAP-сервера так, чтобы изменилось имя LDAP-атрибута (*attribute*).

LDAP-атрибуты

Некоторые значения, используемые при определении LDAP, являются атрибутами. А именно:

- атрибут «Имя» (**Name**);
- атрибут «Принадлежность» (**Membership**);
- атрибут «Пароль» (**Password**).

LDAP-атрибут (**LDAP attribute**) – это пара значений, состоящая из имени атрибута (в данном руководстве будем называть его идентификатором) и значения атрибута. В качестве примера можно привести атрибут «имя пользователя», который представляет собой пару значений и состоит из идентификатора «имя пользователя» и значения «Смит».

Эти атрибуты могут использоваться по-разному, и их значение для LDAP-сервера обычно определяется схемой базы данных сервера. Схема базы данных может меняться администратором с целью внесения изменений в атрибуты.

Общие настройки

Для конфигурирования каждого сервера используются следующие общие настройки.

- **Имя (Name)**

  Имя, присвоенное объекту «сервер» для ссылок на него в системе NetDefendOS. Например, в системе NetDefendOS могут быть определены правила, ссылающиеся на это имя.

  Это значение не имеет ничего общего с атрибутом «имя», о котором будет сказано далее. Это значение используется системой NetDefendOS, а не LDAP-сервером.

- **IP-адрес (IP Address)**

  IP-адрес LDAP-сервера.

- **Порт (Port)**

  Номер порта LDAP-сервера, на котором сервер принимает запросы клиентов, отправленные с использованием TCP/IP.

  По умолчанию порт *389*.

- **Тайм-аут (Timeout)**

  Время в секундах, которое дается на попытку аутентификации пользователя LDAP-сервером. Если через указанное время от сервера не приходит ответ на запрос, сервер считается недоступным.

  Тайм-аут по умолчанию составляет 5 секунд.

- **Атрибут «имя» (Name Attribute)**

  Атрибут «имя» – это идентификатор поля данных LDAP-сервера содержащий имя пользователя. Значением по умолчанию в системе NetDefendOS является *uid*, который является корректным для большинства серверов на базе UNIX.

  При использовании Microsoft Active Directory, атрибуту «имя» должно быть присвоено

значение *SAMAccountName* (вводится без учета регистра клавиатуры). При просмотре информации о пользователе в Active Directory, значение имени пользователя при входе в систему определяется в поле *SAMAccountName* на вкладке *Account*.

Примечание: База данных LDAP-сервера устанавливает соответствующее значение идентификатора

Определение пары значений атрибута и схемы базы данных LDAP-сервера устанавливает соответствующее значение идентификатора.

- **Поиск принадлежности к группе (Retrieve Group Membership)**

  Эта опция определяет, должны ли группы, к которым принадлежит пользователь быть определены с LDAP-сервера. Имя группы часто используется при предоставлении пользователю доступа к какому-либо сервису после удачной регистрации.

  Если опция поиска принадлежности к группе активирована, то также должен быть установлен атрибут «принадлежность».

- **Атрибут «принадлежность» (Membership Attribute)**

  Атрибут «принадлежность» определяет, в какую группу входит пользователь. Принадлежность к группе в данном случае аналогична принадлежности пользователя к одной из групп с правами администратора (группа *administrators* и группа *revisors*) базы данных системы NetDefendOS. Этот атрибут также является парой значений, определенной схемой базы данных сервера. Значением идентификатора данного атрибута по умолчанию является *MemberOf.*

  В службе каталогов Microsoft Active Directory группы, к которым принадлежит пользователь, можно просмотреть на вкладке *MemberOf*, которая содержит информацию о пользователе.

- **Использование доменного имени (Use Domain Name)**

  Некоторым серверам для осуществления успешной аутентификации требуется к имени пользователя добавлять доменное имя. Доменное имя – это имя узла, в качестве которого выступает LDAP-сервер, например, *myldapserver*. У параметра *Use Domain Name* могут быть следующие варианты значений:

  а) *None* – при таком значении параметра имя пользователя никак не меняется. Например, *testuser*.

  б) *Username Prefix* – при таком значении параметра во время аутентификации доменное имя ставится перед именем пользователя. Например, *myldapserver/testuser*.

  в) *Username Postfix* – при таком значении параметра во время аутентификации после имени пользователя добавляется символ «@» и доменное имя. Например, *testuser@myldapserver*.

  Если выбрано значение параметра отличное от *None,* доменное имя должно быть определено.

  Разные LDAP-серверы могут обрабатывать доменное имя по-разному, это зависит от технических требований определенного сервера. В большинстве версий Windows Active Directory следует использовать вариант *Postfix*.

- **Таблица маршрутизации (Routing Table)**

  Это таблица маршрутизации системы NetDefendOS, в которой выполняется поиск соответствующего маршрута по IP-адресу сервера. Таблицей маршрутизации по умолчанию является главная таблица маршрутизации *main*.

Настройки базы данных

Существуют следующие настройки базы данных.

- **Базовый объект (Base Object)**

Определяет, откуда должен начинаться поиск учетной записи пользователя в дереве сервера LDAP.

Список пользователей, определенных в базе данных LDAP-сервера, организован в виде дерева. Базовым объектом определяется положение релевантных пользователей в данной структуре. Определение базового объекта ускоряет поиск по LDAP-дереву, т.к. просматриваются только пользователи, который находятся под базовым объектом.

Важно: Базовый объект должен быть правильно определен

Если базовый объект определен неверно, то пользователь не будет найден и аутентифицирован, если они не являются частью структуры дерева под базовым объектом. Рекомендуется изначально определять базовый объект как маршрут дерева.

Базовый объект определяется как обычный разделенный набор доменов *domainComponent (DC)*. Если полное доменное имя *myldapserver.local.eu.com* и он является базовым объектом, то он определяется как:

```
DC=myldapserver,DC=local,DC=eu,DC=com
```

Поиск имени пользователя будет начинаться в корне дерева *myldapserver.*

- **Учетная запись администратора (Administrator Account)**

  LDAP-серверу требуется, чтобы пользователь, устанавливающий соединение, для осуществления поиска обладал правами администратора. Учетная запись администратора определяет имя администратора в системе. Имя администратора в системе может быть затребовано сервером в специальном формате также как доменное имя (см. ранее Использование доменного имени).

- **Пароль/Подтверждение пароля (Password/Confirm Password)**

  Пароль для учетной записи администратора, о которой говорилось выше.

- **Доменное имя (Domain Name)**

  Доменное имя используется при форматировании имен пользователей. Domain Name – это первая часть полного доменного имени. В примерах, представленных выше, в качестве доменного имени выступало имя *myldapserver*. Полное доменное имя представляет собой текстовые данные, разделенные точками, например, *myldapserver.local.eu.com.*

  Эта опция доступна, только если тип сервера (*Server Type*) НЕ установлен в значение *Other*.

  Доменное имя можно не определять, кроме случаев, когда он требуется LDAP-серверу во время выполнения BIND-запроса.

Дополнительные настройки

Существует одна дополнительная настройка:

- **Атрибут «пароль» (Password Attribute)**

  В идентификаторе атрибута «пароль» на LDAP-сервере содержится пароль пользователя. Идентификатором по умолчанию является *userPassword*.

  Значение этой опции можно не заполнять, кроме случаев, когда LDAP-сервер используется для аутентификации пользователей, подключающихся через PPP с CHAP, MS-CHAPv1 или MS-CHAPv2.

  Когда атрибут «пароль» заполнен, он содержит идентификатор поля данных в базе данных сервера LDAP, содержащего пароль пользователя в виде текста. Администратор LDAP-сервера должен точно знать, что это поле действительно содержит пароль. Далее об этом будет рассказано более подробно.

Аутентификация с помощью BIND-запроса

Аутентификация LDAP-сервера автоматически конфигурируется для работы с использованием LDAP-аутентификации по BIND-запросу (*Bind Request Authentication*). Аутентификация проходит успешно, в случае если соединение с LDAP-сервером установлено, а идентификация отдельных клиентов в данном случае не имеет значения.

При аутентификации по BIND-запросу не должно возникать перенаправлений с LDAP-сервера. Если они появляются, то LDAP-сервер воспринимается как недоступный.

Ответы LDAP-сервера

Когда система NetDefendOS посылает запрос LDAP-серверу на аутентификацию пользователя, возможны следующие варианты:

- Сервер отвечает положительно, и аутентификация пользователя проходит успешно.

  Если клиенты используют PPP с CHAP, MS-CHAPv1 или MS-CHAPv2, то это частный случай, когда аутентификация фактически производится системой NetDefendOS (более подробно об этом будет сказано далее).

- Сервер отвечает отрицательно, и пользователь не проходит аутентификацию.

- Сервер не отвечает за время тайм-аута, выделенного на ответ серверу. Если определен только один сервер, то процесс аутентификации завершается. Если для правила аутентификации пользователя определены альтернативные серверы, то запросы отсылаются к ним.

Имя пользователя в сочетании с доменным именем

В процессе аутентификации пользователя при вводе комбинации из учетного имени и пароля некоторым LDAP-серверам требуется доменное имя, чтобы присоединить его к имени пользователя. Если домен – **mydomain.com**, то имя пользователя **myuser** будет определено как myuser@mydomain.com. Для некоторых LDAP-серверов возможны варианты **myuser@domain**, **mydomain.com\myuser** или **mydomain\myuser**. Формат записи полностью зависит от настроек сервера и того, какой формат ему требуется.

Мониторинг статистики в режиме реального времени

Статистика следующих параметров доступа пользователя к LDAP-серверу в процессе аутентификации доступна в режиме реального времени:

- количество аутентификаций в секунду;
- общее количество запросов на аутентификацию;
- общее количество успешных запросов на аутентификацию;
- общее количество неудачных запросов на аутентификацию;
- общее количество введенных недопустимых имен пользователя;
- общее количество введенных недопустимых паролей.

Команды CLI для LDAP-аутентификации

CLI-объекты, соответствующие LDAP-серверам и используемые для аутентификации, называются *LDAPDatabase*-объектами (LDAP-серверы, используемые для поиска сертификатов, называются LDAPServer-объектами в CLI).

Специальный LDAP-сервер, определенный в системе NetDefendOS для аутентификации, можно просмотреть с помощью команды:

```
gw-world:/> show LDAPDatabase <object_name>
```

Все содержимое базы данных можно вывести на экран с помощью команды:

```
gw-world:/> show LDAPDatabase
```

LDAP-аутентификация и PPP

Когда PPP-клиент пытается получить доступ через PPTP или L2TP и LDAP-аутентификация должна производиться с CHAP, MS-CHAPv1 или MS-CHAPv2 шифрованием, то такая ситуация требует тщательного рассмотрения. Далее рассматриваются два случая: (А) стандартная PPP-аутентификации и (Б) PPP-аутентификация с шифрованием.

А. Стандартная LDAP-аутентификация

Ниже представлена схема стандартной LDAP-аутентификации для Webauth, XAuth, или PPP с поддержкой PAP для повышения безопасности авторизации. Аутентификационный BIND-запрос имени пользователя и пароля отправляется LDAP-серверу, который выполняет аутентификацию и отправляет обратно BIND-ответ с результатом.

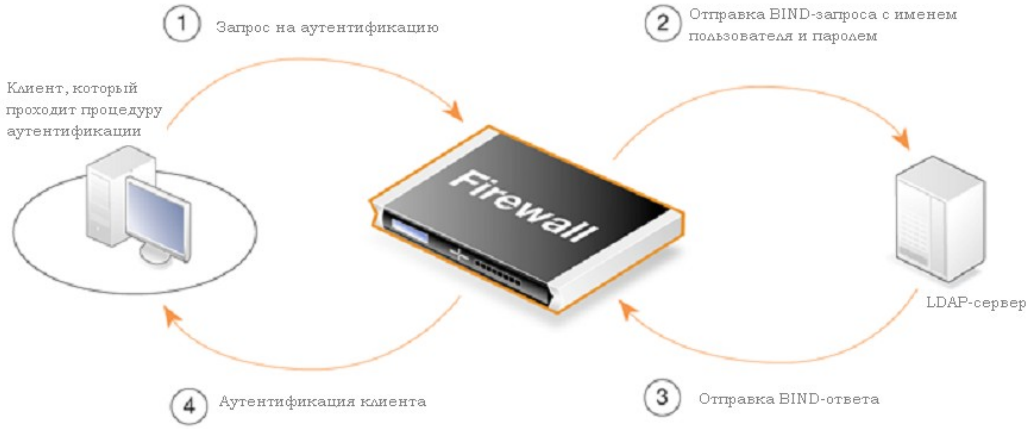


Рисунок 8.1. Стандартная LDAP-аутентификация.

Если принадлежность к группе определяется после того, как LDAP-серверу отправлен запрос на поиск принадлежности к группе и получен ответ с запрашиваемым значением, процесс аутентификации будет отличаться.

Б. PPP-аутентификация с CHAP, MS-CHAPv1 или MS-CHAPv2 шифрованием

Если для аутентификации используется PPP с CHAP, MS-CHAPv1 или MS-CHAPv2, то клиент отправляет системе NetDefendOS хэш пароля пользователя. Система не может просто переслать хэш LDAP-серверу, т.к. сервер его не «поймет». Система NetDefendOS может получить пароль в виде текста от LDAP-сервера, создать хэш и сравнить созданный хэш с хэшем от клиента. Если они совпадают, аутентификация происходит успешно. В этом случае решение об исходе аутентификации зависит не от LDAP-сервера, а от системы NetDefendOS.

Для получения пароля от LDAP-сервера требуется следующее:

- Атрибут «пароль» должен быть задан при определении сервера в NetDefendOS. Это идентификатор поля LDAP-сервера, из которого берется пароль при ответе.

  Этот идентификатор должен отличаться от атрибута «пароль» установленного по умолчанию

(на большинстве LDAP-серверов паролем по умолчанию является *userPassword*). Рекомендуется использовать поле *description* в базе данных LDAP.

- Прежде чем сервер занесет в поле базы данных атрибут «пароль» с установленным идентификатором, LDAP-администратор должен проверить, что там действительно находится пароль в текстовом виде. Пароли хранятся на LDAP-сервере в формате зашифрованного хэша, и автоматическое выполнение этих операций не предусмотрено. Это выполняется администратором вручную по мере добавления новых пользователей или изменения текущих паролей пользователей.

  Несомненно, это требует некоторых усилий администратора, но если оставить пароли незашифрованными в текстовом формате на LDAP-сервере, то впоследствии решение вопросов безопасности заставит приложить не меньше усилий. Это одна из тех причин, по которым LDAP не подходит для PPP-аутентификации с CHAP, MS-CHAPv1 или MS-CHAPv2 шифрованием.

Когда система NetDefendOS получает хэш пароля от клиента, она инициирует поисковый запрос (*Search Request*) LDAP-серверу. Сервер отправляет ответ на поисковый запрос (Search Response), содержащий пароль пользователя и данные о принадлежности пользователя к какой-либо группе. После этого система NetDefendOS может сравнить два хэша. Рисунок 8.2 иллюстрирует это процесс.

Рисунок 8.2. LDAP для PPP с CHAP, MS-CHAPv1 или MS-CHAPv2

Важно: Канал связи с LDAP-сервером должен быть защищен

Поскольку LDAP-сервер пересылает пароли системе NetDefendOS в формате простого текста, то канал связи между межсетевым экраном NetDefend и сервером должен быть защищенным. Если канал, по которому передаются данные, не является локальным, необходимо использовать VPN-канал.

Доступ к самому LDAP-серверу также должен быть ограничен, так как пароли в нем хранятся в формате простого текста.

8.2.5. Правила аутентификации

Правило аутентификации (*Authentication Rule*) должно определяться, когда клиент устанавливает соединение через межсетевой экран NetDefend и у него запрашиваются учетное имя пользователя и пароль.

Настройка правил аутентификации аналогична настройке других политик безопасности системы NetDefendOS. В них также указывается трафик, который должен подчиняться этому правилу. Правила аутентификации отличаются от других политик тем, что сеть или интерфейс назначения

определенного соединения не так важны в этом случае как с сеть или интерфейс источника.

Параметры правила аутентификации

Правила аутентификации имеют следующие параметры:

- **Агент аутентификации (Authentication Agent)**

  Тип трафика, проходящего аутентификацию. Возможны следующие варианты:

  а) HTTP

  HTTP WEB-соединения проходят аутентификацию через предопределенную или специальную WEB-страницу (подробное объяснение для HTTP представлено ниже).

  б) HTTPS

  HTTPS WEB-соединения проходят аутентификацию через предопределенную или специальную WEB-страницу (подробное объяснение для HTTP представлено ниже).

  в) XAUTH

  Это метод IKE-аутентификации, который используется как часть процесса создания VPN-туннеля с IPsec.

  XAuth является расширением обычного IKE-обмена, а также является дополнением к стандартной безопасности IPsec. Клиенты, получающие доступ к VPN, должны пройти регистрацию в системе, введя имя пользователя и пароль.

  Следует отметить, что интерфейс не указывается в правиле аутентификации XAuth, т.к. одно правило с XAuth в качестве агента используется для всех IPsec-туннелей. Однако такой подход предполагает использование единственного источника аутентификации для всех туннелей.

  г) PPP

  Используется только для L2TP- или PPTP-аутентификации.

- **Источник аутентификации (Authentication Source)**

  Определяет тип аутентификации в зависимости от параметров:

  а) ***LDAP*** – поиск пользователей осуществляется во внешней базе данных LDAP-сервера.

  б) ***RADIUS*** – для поиска используется внешний сервер RADIUS.

  в) ***Disallow*** – при таком значении параметра все соединения, которые подпадают под действие этого правила, будут отклоняться. Эти соединения не продут аутентификацию.

  Наиболее предпочтительно размещать *Disallow*-правила в конце набора правил аутентификации.

  г) ***Local*** – для поиска пользователей используется локальная база данных, определенная в системе NetDefendOS.

  д) ***Allow*** – при таком значении параметра все соединения, которые подпадают под действие этого правила, будут разрешены и аутентифицированы. Поиск по базе данных аутентификации не производится.

- **Интерфейс (Interface)**

  Интерфейс источника соединений, проходящих аутентификацию. Должен быть определен.

- **Originator IP**

  IP-адрес или сеть источника, откуда устанавливаются новые соединения. Для XAuth и PPP – это originator IP туннеля.

- **Terminator IP**

  Терминирует IP-адрес, на который устанавливаются новые соединения. Определяется в случае, если агентом аутентификации является PPP.

Временные ограничения соединений

В правиле аутентификации могут определяться временные ограничения для сеанса пользователя.

- **Время простоя (Idle Timeout)**

  Время простоя, после которого соединение будет автоматически прервано (по умолчанию 1800 секунд).

- **Время сеанса (Session Timeout)**

  Максимальное время существования соединения (значение по умолчанию не определяется).

Если используется сервер аутентификации, то можно активировать опцию **Use timeouts received from the authentication server (Использовать тайм-ауты сервера аутентификации)** и получать эти значения с сервера.

Многократная регистрация

В правиле аутентификации можно определить, как обрабатывать многократную регистрацию (*multiple logins*), т.е. когда несколько пользователей с разных IP-адресов источников пытаются войти в систему под одним и тем же именем пользователя. Можно предусмотреть следующие способы обработки:

- Разрешить многократную регистрацию с тем, чтобы несколько клиентов могли использовать одну и ту же комбинацию из имени пользователя и пароля.
- Для одного имени пользователя разрешить только однократный вход в систему.
- Разрешить однократный вход в систему для одного имени пользователя и завершать сеанс пользователя с совпадающим именем в системе, если к тому времени, когда второй пользователь с таким же именем входит в систему, время простоя первого достигло установленного.

8.2.6. Процесс аутентификации

При аутентификации с ручным вводом имени пользователя и пароля в системе NetDefendOS происходят следующие процессы.

1. Пользователь устанавливает новое соединение с межсетевым экраном NetDefend.
2. Система NetDefendOS определяет появление нового соединения с пользователем на некотором интерфейсе и ищет в наборе правил аутентификации соответствующее правило для трафика с этого интерфейса, приходящего из этой сети и одного из следующих типов:
   - HTTP-трафик;
   - HTTPS-трафик;
   - Трафик IPsec-туннеля;
   - Трафик L2TP-туннеля;
   - Трафик PPTP-туннеля.
3. Если соответствующее правило не найдено, то соединение разрешается (в случае если это установлено набором правил), и на этом процесс аутентификации завершается.
4. На основании настроек первого правила аутентификации, которое удовлетворяет условиям, система NetDefendOS выводит запрос на авторизацию пользователя.
5. Пользователь отвечает вводом идентификационной информации, которая обычно состоит из комбинации учетного имени пользователя и пароля.

6. Система NetDefendOS подтверждает правильность информации с помощью источника аутентификации, прописанного в правиле аутентификации. Это может быть локальная база данных системы NetDefendOS, внешняя база данных сервера RADIUS или внешний LDAP-сервер.

7. Система NetDefendOS разрешает дальнейшее прохождение трафика через соединение, т.к. процесс аутентификации прошел успешно и запрашиваемый сервис разрешен правилом из набора IP-правил. Объект «сеть источника», записанный в правиле, может иметь либо активированную опцию **No Defined Credentials (Отсутствие определенной учетной записи)**, либо сеть источника может быть связана с группой и пользователем, являющимся членом этой группы.

8. Если в правиле определено допустимое время простоя соединения, то в случае если соединение с аутентифицированным пользователем не активно в течение установленного периода, оно будет автоматически прервано.

Все пакеты с IP-адреса, не прошедшего аутентификацию, отбрасываются.

8.2.7. Пример использования группы аутентификации

Чтобы проиллюстрировать использование групп аутентификации возьмем группу пользователей, которые регистрируются из сети *192.168.1.0/24* подключенной на *lan* интерфейсе. Требуется ограничить доступ к сети с именем *important_net* на *int* интерфейсе, разрешив доступ к ней только одной группе проверенных (*trusted*) пользователей. В то же время группе других пользователей, которые не пользуются доверием (*untrusted*), разрешить доступ к другой сети с именем regular_net на *dmz* интерфейсе.

Для выполнения задания в качестве источника аутентификации будем использовать внутреннюю базу данных, куда внесем пользователей с соответствующими именами, паролями и специальной строкой для группового параметра (**Group**). Часть пользователей отнесем к группе *trusted*, часть – к группе *untrusted.*

Определяем два IP-объекта для одной сети *192.168.1.0/24*. Первый IP-объект назовем *untrusted_net*. Он имеет значение параметра группировки *untrusted*. Другому IP-объекту присвоим имя trusted_net и значение параметра группировки *trusted*.

Последним этапом будет определение набора IP-правил, так как это показано ниже:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
1	Allow	lan	trusted_net	int	important_net	All
2	Allow	lan	untrusted_net	dmz	regular_net	All

Если группе пользователей *trusted* необходимо предоставить доступ к сети *regular_net*, то следует добавить третье правило:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
1	Allow	lan	trusted_net	int	important_net	All
2	Allow	lan	trusted_net	dmz	regular_net	All
3	Allow	int	untrusted_net	dmz	regular_net	All

8.2.8. HTTP-аутентификация

Если пользователи обмениваются информацией через WEB-браузер, используя протокол HTTP, то аутентификация может быть выполнена с помощью HTML-страниц. Этот способ аутентификации называют *WebAuth*.

Изменение порта управления WebUI

HTTP-аутентификация некорректно работает при одновременном запуске с сервисом удаленного управления WebUI, который также использует TCP-порт 80. Чтобы избежать коллизий, номер порта для WebUI должен быть изменен до конфигурирования аутентификации. Сделать это можно, если перейти на вкладку **Remote Management > advanced settings** на WebUI и изменить настройку порта **WebUI HTTP Port**. Вместо 80 порта здесь можно использовать порт 81.

Опции агента

Для HTTP- и HTTPS-аутентификации в правилах аутентификации существует набор опций, которые называются опциями агента (**Agent Options**). Среди них:

- **Тип регистрации (Login Type).**

  а) **FORM** – пользователь заполняет поля данных на специальной HTML-странице для аутентификации, и информация отсылается NetDefendOS с помощью функции POST.

  б) **BASICAUTH** – при этом типе регистрации браузеру отправляется сообщение «**401 – Authentication Required**», которое вызывает встроенный диалог с запросом имени пользователя и пароля. Дополнительно в диалоге браузера может быть определена строка **Realm String**.

  Тип регистрации **FORM** более предпочтителен, чем **BASICAUTH**, потому что в некоторых случаях браузер может сохранять регистрационные данные в кэше.

- Если **агент** определяется для *HTTPS*, то корневой сертификат и сертификат хоста выбираются из списка сертификатов, загруженных в систему NetDefendOS.

Настройка IP-правил

HTTP-аутентификация не может осуществляться, пока правило, разрешающее аутентификацию, не будет добавлено в набор IP-правил. Рассмотрим пример, в котором несколько клиентов локальной сети *lannet* пытается получить доступ к сети Интернет через WAN-интерфейс. Тогда набор IP-правил должен быть следующим:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
1	Allow	lan	lannet	core	lan_ip	http-all
2	NAT	lan	trusted_users	wan	all-nets	http-all
3	NAT	lan	lannet	wan	all-nets	dns-all

Первое правило разрешает процесс аутентификации и подразумевает, что клиент пытается получить доступ к IP-адресу *lan_ip*, который является IP-адресом интерфейса межсетевого экрана NetDefend, на котором подключена локальная сеть.

Второе правило разрешает доступ к ресурсам, но *lannet* нельзя использовать в качестве сети источника, т.к. тогда правило будет распространяться на любого неаутентифицированного клиента из этой сети. В качестве сети источника здесь можно использовать IP-объект *trusted_users*, определенный администратором и который представляет собой ту же сеть *lannet*, либо с дополнительно активированной опцией аутентификации **No Defined Credentials,** либо связанную с группой аутентификации (группа, связанная с пользователями).

Третье правило разрешает DNS-поиск URL-адресов.

Принудительная регистрация пользователей

Если использовать указанный выше набор IP-правил, то пакеты всех неаутентифицированных пользователей, которые пытаются получить доступ ко всем IP-адресам кроме *lan_ip*, будут отбрасываться, т.к. эти запросы не соответствуют текущим правилам. Чтобы пользователи обязательно перешли на страницу аутентификации необходимо добавить SAT-правило и связанное с ним *Allow*-правило. Набор правил теперь должен выглядеть так:

#	Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
1	Allow	lan	lannet	core	lan_ip	http-all
2	NAT	lan	trusted_users	wan	all-nets	http-all
3	NAT	lan	lannet	wan	all-nets	dns-all
4	SAT	lan	lannet	wan	all-nets all-to-one 127.0.0.1	http-all
5	Allow	lan	lannet	wan	all-nets	http-all

Под SAT-правило подпадают все неаутентифицированные запросы, и поэтому в правиле устанавливается маршрутизация all-to-one, согласно которой все запросы направляются на адрес *127.0.0.1*, соответствующий интерфейсу *core*.

Пример 8.1. Создание группы аутентификации пользователей

В данном примере рассматривается аутентификация объекта адресной книги, в котором используется группа пользователей «users» для аутентификации пользователей в «lannet». В примере демонстрируется настройка группы пользователей в базе данных системы NetDefendOS.

Web-интерфейс

Шаг А

1. Зайдите **User Authentication > Local User Databases > Add > LocalUserDatabase**

2. Затем введите:

- **Name:** lannet_auth_users
- **Comments:** папка для "lannet" группы аутентификации пользователей – "users"

3. Нажмите **OK**

Шаг Б

1. Зайдите **lannet_auth_users > Add > User**

2. Затем введите:

- **Username:** введите учетное имя пользователя, например, *user1*
- **Password:** введите пароль пользователя
- **Confirm Password:** повторите пароль
- **Groups:** один пользователь может быть определен более чем в одной группе. Введите названия групп (в данном случае через запятую). Для этого примера это будет группа *users*.

3. Нажмите **OK**

4. Повторить **шаг Б**, чтобы добавить всех пользователей *lannet*, которые являются членами группы *users*, в папку *lannet_auth_users*.

Пример 8.2. Настройка аутентификации пользователя для доступа к WEB

В данном примере рассматривается настройка HTTP-аутентификации пользователя для группы пользователей *users* в подсети *lannet*. В соответствии с IP-правилом пользователи, которые входят в группу *users,* могут просматривать WEB-страницы после успешной аутентификации.

В данном примере подразумевается, что *lannet*, *users*, *lan_ip*, папка локальной базы данных пользователей *lannet_auth_users* и адрес объекта аутентификации *lannet_users* уже определены.

Web-интерфейс

А. Определение IP-правила для разрешения аутентификации

1. Зайдите **Rules > IP Rules > Add > IP rule**

2. Затем введите:

- **Name:** http2fw
- **Action:** Allow
- **Service:** HTTP
- **Source Interface:** lan
- **Source Network:** lannet
- **Destination Interface:** core
- **Destination Network:** lan_ip

3. Нажмите **OK**

Б. Определение правила аутентификации

1. Зайдите **User Authentication > User Authentication Rules > Add > User Authentication Rule**

2. Затем введите:

- **Name:** HTTPLogin
- **Agent:** HTTP
- **Authentication Source:** Local
- **Interface:** lan
- **Originator IP:** lannet

3. В пункте **Local User DB** выберите *lannet_auth_users*

4. В пункте **Login Type** выберите *HTMLForm*

5. Нажмите **OK**

В. Определение IP-правила, которое разрешает аутентифицированным пользователям просматривать WEB-страницы.

1. Зайдите **Rules > IP Rules > Add> IP rule**

2. Затем введите:

- **Name:** Allow_http_auth
- **Action:** NAT
- **Service:** HTTP
- **Source Interface:** lan
- **Source Network:** lannet_users
- **Destination Interface:** any
- **Destination Network:** all-nets

3. Нажмите **OK**

Пример 8.3. Настройка сервера RADIUS

В данном примере демонстрируется типичная настройка сервера RADIUS.

Web-интерфейс

1. Зайдите **User Authentication > External User Databases> Add > External User Database**

2. Затем введите:

а) **Name:** введите имя сервера, например, *ex-users*

б) **Type:** выберите RADIUS

в) **IP Address:** введите IP-адрес сервера или введите символьное имя сервера, если он определен в адресной книге (**Address Book**)

г) **Port:** 1812 (по умолчанию сервис RADIUS использует UDP-порт 1812)

д) **Retry Timeout:** 2 (В данном случае система NetDefendOS посылает повторные запросы на аутентификацию серверу через каждые 2 секунды, если по прошествии установленного времени, ответ не получен. Максимально возможно три повторения.)

е) **Shared Secret:** ввести текстовую строку с базовым шифрованием для сообщений RADIUS

ж) **Confirm Secret:** для подтверждения повторить строку с базовым шифрованием для сообщений RADIUS

3. Нажмите **OK**

8.3. Настройка HTML-страниц

В процессе аутентификации пользователя используется набор HTML-файлов для представления информации пользователю. Доступны следующие варианты процесса HTTP-аутентификации:

- При попытке пользователя открыть WEB-страницу в браузере происходит перенаправление на страницу регистрации *FormLogin*. После успешной регистрации пользователя происходит обратное перенаправление на первоначально запрашиваемую страницу.
- После успешной регистрации пользователя происходит перенаправление на определенную страницу.
- После успешной регистрации пользователя происходит перенаправление на страницу

LoginSuccess, а затем – на первоначально запрашиваемую страницу.

Файлы HTTP-баннеров

Файлы для WEB-страниц или HTTP-баннеров (*HTTP banner files*) хранятся в NetDefendOS и по умолчанию появляются при загрузке. Их можно настроить либо непосредственно через WEB-интерфейс, либо с помощью загрузки и повторной выгрузки через SCP-клиент так, чтобы они при инсталляции выполняли определенные задачи.

Файлы, доступные для редактирования:
FormLogin
LoginSuccess
LoginFailure
LoginAlreadyDone
LoginChallenge
LoginChallengeTimeout
LoginSuccess
LoginSuccessBasicAuth
LoginFailure
FileNotFound

Редактирование файлов баннера

WebUI обеспечивает простой способ загружать и редактировать файлы баннера, а затем выгружать отредактированные HTML обратно в NetDefendOS. Далее представлено описание этого процесса, который аналогичен процедуре, описанной в *разделе 6.3.4.4. «Настройка HTML-страниц».*

Чтобы выполнить настройку, сначала необходимо создать новый объект **Auth Banner Files** с новым именем. Этот новый объект автоматически будет содержать копии всех файлов объекта Auth Banner Files по умолчанию. Созданный файл можно отредактировать и выгрузить обратно в NetDefendOS. Исходный объект по умолчанию редактировать нельзя. В примере, приведенном далее, приводятся этапы настройки.

Параметры HTML-страницы

HTLM-страницы могут содержать некоторое количество параметров, используемых там, где это необходимо. Доступными параметрами являются:

- %URL% – запрашиваемый URL;
- %IPADDR% – IP-адрес с которого начался просмотр страниц;
- %REASON% – причина отказа в доступе;
- %REDIRURL% – ULR WEB-страницы для перенаправления.

Параметр %REDIRURL%

Параметр %REDIRURL% присутствует на определенных баннерах WEB-страниц. Перед тем, как появляется окно регистрации для неаутентифицированного пользователя, запрашивается URL, на который необходимо перенаправить пользователя после успешной аутентификации.

Так как параметр %REDIRURL% выполняет только эту внутреннюю задачу, он должен присутствовать не на WEB-страницах, а на странице *FormLogin*, в том случае если она используется.

Пример 8.4. Редактирование фильтра по содержимому файлов HTTP-баннера

В данном примере демонстрируется, как изменить содержимое URL запрещенной HTML-страницы.

Web-интерфейс

1. Зайдите **Objects > HTTP Banner files > Add > Auth Banner Files**

2. Введите: имя, например, *new_forbidden* и нажмите **OK**

3. Появится диалог для нового набора файлов ALG-баннера.

4. Выберите щелчком мыши вкладку **Edit & Preview tab**

5. В списке **Page** выберите *FormLogin*

6. Теперь измените HTML-код, который появляется в текстовом поле для страницы с запрещенным URL

7. При необходимости используйте **Preview**, чтобы просмотреть изменения

8. Нажмите **Save** для сохранения внесенных изменений

9. Нажмите **OK**, чтобы выйти из режима редактирования

10. Зайдите **Objects > ALG** и выберите соответствующий HTML ALG

11. В пункте **HTML Banner** выберите *new_forbidden*

12. Нажмите **OK**

13. Зайдите **Configuration > Save & Activate**, чтобы активировать новый файл

Важно: Необходимо сохранять изменения, внесенные в HTML-файл

*В примере, который представлен выше, возможно редактировать более одного HTML-файла за сеанс. Поэтому прежде чем начинать редактировать другой файл, любое изменение необходимо сохранять с помощью кнопки **Save**.*

Выгрузка с SCP

Существует возможность выгружать новые файлы HTTP-баннера с помощью SCP. Последовательность выполнения следующая:

1. Так как SCP нельзя использовать для загрузки исходных HTML по умолчанию, код источника необходимо первоначально скопировать из WebUI и вставить в локальный текстовый файл, который затем можно изменять с помощью подходящей программы-редактора.

2. Новый объект **Auth Banner Files**, в который будут выгружаться измененные файлы, уже должен быть создан. С помощью следующей CLI-команды можно создать такой объект с именем *ua_html*:

```
gw-world:/> add HTTPAuthBanners ua_html
```

   Так создается объект, содержащий копию всех файлов баннера аутентификации пользователя, которые имеются по умолчанию.

3. Измененный файл выгружается с помощью SCP. Он выгружается в объект *ua_html* с типом объекта *HTTPAuthBanner* и именем свойства *FormLogin*. Если редактируемый локальный файл *Formlogon* с именем *my.html* использует клиента Open SSH SCP, команда для выгрузки будет следующей:

```
pscp my.html admin@10.5.62.11:HTTPAuthBanners/ua_html/FormLogin
```

   Использование SCP-клиентов было описано в *разделе 2.1.6 «Протокол Secure Copy»*.

4. Необходимо создать релевантное правило аутентификации пользователя для *ua_html*. Если имя правила *my_auth_rule*, то с использованием командной строки его можно создать так:

```
set UserAuthRule my_auth_rule HTTPBanners=ua_html
```

5. Сразу после CLI-команды *activate* должна применяться команда *commit*, чтобы активировать изменения, внесенные в настройки межсетевого экрана NetDefend.

Глава 9. VPN

В данной главе представлено описание функциональных возможностей *Virtual Private Network (VPN)* системы NetDefendOS.

- Обзор
- Быстрый запуск VPN
- Компоненты IPsec
- Туннели IPsec
- PPTP/L2TP
- Сервер клиентского доступа (CA)
- Поиск и устранение неисправностей VPN

9.1. Обзор

9.1.1. Использование VPN

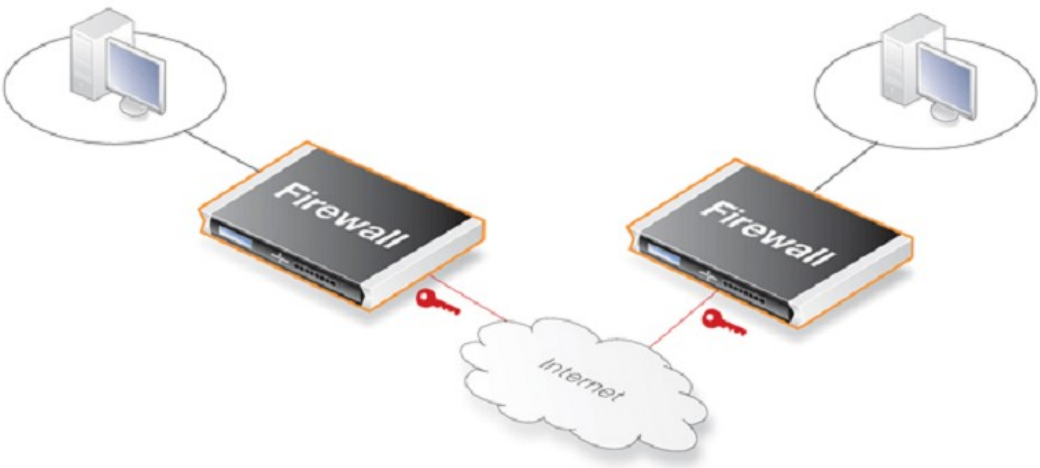
Сеть Интернет все чаще используется для установки соединения между компьютерами, так как она предоставляет пользователям эффективный и недорогой способ обмена информацией. Поэтому основным требованием к данным, передаваемым в сети Интернет определенному пользователю без участия третьей стороны, является возможность чтения и изменения.

Не менее важно, чтобы получатель был уверен в том, что никто не фальсифицировал данные, другими словами, не произошла замена информации другой. Виртуальные частные сети (VPN) обеспечивают удовлетворение данной потребности, благодаря организации защищенного и экономически эффективного соединения между двумя взаимодействующими компьютерами, таким образом, осуществляя защищенную передачу данных.

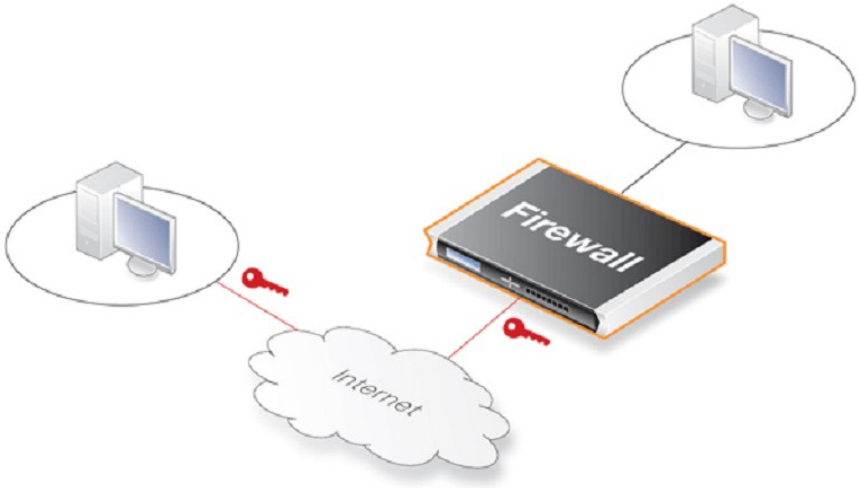
VPN обеспечивает установку *туннеля* между двумя устройствами, известными как *конечные точки туннеля*. Таким образом, все данные находятся под защитой. Механизм, обеспечивающий безопасность туннеля, называется *шифрование*.

Существует два основных сценария использования VPN:

4. **LAN to LAN connection** – Применяется, если требуется соединить две внутренние сети через Интернет. В данном случае, каждая сеть защищена отдельным межсетевым экраном NetDefend и между ними установлен VPN-туннель.



5. **Client to LAN connection** – Применяется, если необходимо подключить несколько удаленных клиентов к внутренней сети через Интернет. В этом случае внутренняя сеть защищена межсетевым экраном NetDefend, к которому подключается клиент, и между ними установлен VPN-туннель.



9.1.2. VPN-шифрование

Шифрование VPN-трафика выполняется с помощью криптографии. Понятие «криптография» включает три следующих преимущества:

Конфиденциальность	Помимо указанных получателей, никто не может получить сообщение и понять его содержание. Шифрование обеспечивает конфиденциальность передаваемой информации.
Аутентификация и целостность	Получатель уверен в том, что сообщение отправлено указанным отправителем, и данные не были изменены во время передачи. Это выполняется за счет аутентификации, и часто реализуется с помощью криптографического ключа хеширования.
Предотвращение отказа	Получатель уверен в том, что данные были отправлены указанным отправителем; отправитель не сможет позже отрицать отправку данных. Как правило, предотвращение отказа является побочным эффектом аутентификации.

Как правило, VPN касается только конфиденциальности и аутентификации. Управление Предотвращением отказа не доступно на сетевом уровне, однако, оно выполняется на самом высоком уровне – уровне передачи.

9.1.3. Организация VPN

Как правило, целью злоумышленника, атакующего VPN-соединение, не является взлом VPN-шифрования, так как это требует огромных усилий. Вместо этого атакующие просматривают VPN-трафик для обнаружения уязвимостей на другом конце соединения. Как правило, мобильные

клиенты и филиалы офисов являются более привлекательной целью, чем основная корпоративная сеть. Захват мобильных клиентов и филиалов упрощает проникновение в корпоративную сеть.

При разработке VPN существует много вопросов, которые не всегда очевидны и требуют решения. К ним относятся:

- Защита мобильных и домашних компьютеров;
- VPN-доступ только к необходимым сервисам, так как мобильные компьютеры являются уязвимыми;
- Создание DMZ для сервисов, совместно используемых другими компаниями с помощью VPN;
- Настройка политик VPN-доступа для различных групп пользователей;
- Создание политик распространения ключей.

Обеспечение безопасности конечной точки

Распространенным заблуждением является то, что с точки зрения безопасности VPN-соединения подобны внутренней сети и могут быть установлены напрямую без принятия дальнейших предупредительных мер по обеспечению защиты. Важно помнить, что хотя VPN-соединение само по себе уже является защищенным, общий уровень безопасности соответствует уровню защиты конечных точек туннеля.

В настоящее время увеличивается количество пользователей, которые, находясь в частых деловых поездках, подключаются напрямую со своих ноутбуков к сети компании через VPN. Тем не менее, сам ноутбук часто не защищен. Другими словами, злоумышленник может получить доступ к защищенной сети через незащищенный ноутбук и уже открытое VPN соединение.

Помещение в зону DMZ

Не следует рассматривать VPN-соединение как неотъемлемую часть защищенной сети. Межсетевой экран должен быть помещен в зону DMZ или за пределами межсетевого экрана, посвященному выполнению этой задачи. Выполнив это, администратор может ограничить VPN-доступ к определенным сервисам и быть уверенным в том, что данные сервисы надежно защищены от злоумышленников.

9.1.4. Распределение ключей

Схемы распределения ключей лучше разработать заранее. Необходимо рассмотреть ряд следующих вопросов:

- Каким образом распространять ключи? Электронная почта не является подходящим решением. Передача информации по телефону будет достаточно надежной.
- Какое количество различных ключей необходимо использовать? Один ключ на пользователя? Один ключ на группу пользователей? Один ключ на соединение LAN-to-LAN? Один ключ на всех пользователей и один ключ для всех соединений LAN-to-LAN? Возможно, лучше использовать больше ключей, чем необходимо на данный момент, таким образом, будет проще настроить доступ пользователю (группе) в будущем.
- Что происходит, если работник, обладающий ключом, увольняется из компании? Если несколько пользователей используют один и тот же ключ, его необходимо изменить.
- Как хранить ключ, если он не установлен непосредственно в память сетевого устройства, например, межсетевого экрана с поддержкой VPN? На дискете? В виде парольной фразы, которую

необходимо запомнить? На смарт-карте? Если используется физический носитель, то как это будет работать?

-

9.1.5. TLS в качестве альтернативы VPN

Если защищенный доступ клиентов к Web-серверам организован с использованием HTTP, то использование межсетевого экрана NetDefend для терминации TLS предлагает альтернативный «облегченный» подход, выполняемый быстро и просто. Для получения более подробной информации см. *Раздел 6.2.10, «TLS ALG»*.

9.2. Быстрый запуск VPN

Обзор

В последних разделах главы представлена подробная информация о компонентах VPN. Для согласования этих последних разделов с общей тематикой главы, данный раздел содержит краткую информацию по быстрому запуску, необходимую для пошаговой установки VPN.

Далее указаны шаги по настройке VPN для большинства сценариев:

- IPsec LAN to LAN с общими ключами;
- IPsec LAN to LAN с сертификатами;
- Удаленные IPsec клиенты с общими ключами;
- Удаленные IPsec клиенты с сертификатами;
- Удаленные L2TP клиенты с общими ключами;
- Удаленные L2TP клиенты с сертификатами;
- Удаленные PPTP- клиенты.

Общие требования по установке туннеля

Перед рассмотрением каждого из сценариев отдельно, полезно суммировать общие требования NetDefendOS при настройке любого VPN-туннеля вне зависимости от его типа.

- **Укажите туннель**

  Прежде всего, необходимо указать туннель. NetDefendOS поддерживает различные типы туннелей, например, *IPsec Tunnel*.

- **Укажите маршрут**

  Прежде чем любой трафик сможет проходить через туннель, необходимо указать *маршрут* в *таблице маршрутизации* NetDefendOS. Благодаря данному маршруту NetDefendOS узнает, какую сеть можно найти в противоположной точке туннеля, таким образом, система будет знать, какой трафик отправлять в туннель.

  В большинстве случаев этот маршрут создается автоматически при указании туннеля, что можно уточнить путем проверки таблиц маршрутизации.

  Если маршрут определен вручную, туннель обрабатывается как физический интерфейс в свойствах маршрута. Другими словами, маршрут «сообщает» системе NetDefendOS, что на другом конце туннеля обнаружена определенная сеть.

- **Укажите IP-правило, разрешающее прохождение VPN-трафика**

  Необходимо указать IP-правило, разрешающее прохождение трафика между сетью и туннелем. Как и в случае с указанием маршрута, туннель обрабатывается как физический интерфейс, если указано IP-правило.

  IP-правила не создаются автоматически после указания туннеля, и если они не существуют, трафик не сможет проходить через туннель и будет отклонен.

В следующих разделах подробно рассматривается подробная установка VPN по каждому из сценариев, представленных выше.

9.2.1. Создание IPsec-туннелей LAN to LAN с использованием общих ключей

1. Создайте объект **Pre-shared Key** (**Общий ключ**).

2. Если предложенные списки алгоритмов по умолчанию не содержат набора алгоритмов, которые являются подходящими для конечной точки туннеля, дополнительно создайте новый объект **IKE Algorithms** и/или объект **IPsec Algorithms**. Это будет зависеть от возможностей устройства на другом конце VPN-туннеля.

3. В **Address Book (Адресная книга**) создайте IP-объекты для:

- Удаленный VPN-шлюз, адрес которого – это IP-адрес сетевого устройства на другом конце туннеля (назовем этот объект *remote_gw*).

- Удаленная сеть, расположенная за удаленным VPN-шлюзом (назовем этот объект *remote_net*).

- Локальная сеть позади межсетевого экрана NetDefend, используемая для обмена данными через туннель. Предположим, что предварительно определенный адрес – *lannet* и сеть подключена к интерфейсу *lan* NetDefendOS.

4. Создайте объект **IPsec Tunnel** (назовем этот объект *ipsec_tunnel*). Определите следующие параметры туннеля:

- Установите *lannet* для **Local Network**.

- Установите *remote_net* для **Remote Network**.

- Установите *remote_gw* для **Remote Endpoint**.
- Установите *Tunnel* для **Encapsulation mode**.
- Для **Authentication** выберите объект **Pre-shared Key** (**Общий ключ**), определенный выше в шаге (1).

В последующих шагах объект **IPsec Tunnel** обрабатывается так же, как любой объект *Interface* NetDefendOS.

5. Укажите два IP-правила в наборе IP-правил для туннеля:

- Правило *Allow* для исходящего трафика, у которого есть предварительно определенный объект *ipsec_tunnel* в качестве **Destination Interface**. Сеть назначения (**Destination Network**) правила – это удаленная сеть *remote_net*.
- Правило *Allow* для входящего трафика, у которого есть предварительно определенный объект *ipsec_tunnel* в качестве **Source Interface**. Сеть источника (**Source Network**) – это удаленная сеть *remote_net*.

Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
Allow	lan	lannet	ipsec_tunnel	remote_net	All

Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
Allow	ipsec_tunnel	remote_net	lan	lannet	All

В данных правилах используется сервис *All*, однако это может быть предварительно определенный сервис.

6. Укажите новый **Маршрут (Route)** NetDefendOS, который определяет, что VPN туннель ipsec_tunnel – это Интерфейс, используемый для ограничения маршрутизации пакетов для удаленной сети на другом конце туннеля.

Интерфейс	Сеть	Шлюз
ipsec_tunnel	remote_net	<empty>

9.2.2. Создание IPsec-туннелей LAN to LAN с использованием сертификатов

Как правило, безопасность LAN to LAN обеспечивается за счет общих ключей, но иногда вместо них необходимо использовать сертификаты X.509. В таких случаях используются сертификаты, выданные центром сертификатов (*Certificate Authority,* CA), взятые с внутреннего сервера CA или предоставленные коммерческим поставщиком сертификатов.

Создание туннеля LAN to LAN с использованием сертификатов выполняется с помощью тех же шагов, что и в предыдущем разделе, описывающем использование общего ключа. Различие заключается в том, что в данном случае для аутентификации общие ключи заменены на сертификаты.

Для аутентификации туннеля LAN to LAN требуются два сертификата, выданных CA (два для каждой конечной точки, корневой сертификат и сертификат для шлюза).

Для установки выполняются следующие шаги:

1. Откройте Web-интерфейс управления межсетевого экрана NetDefend в одной точке туннеля.

2. В **Authentication Objects (Объекты аутентификации)** добавьте *Root Certificate* и *Host Certificate*. Для корневого сертификата добавляются два компонента: файл сертификата и файл приватного ключа. Для сертификата шлюза требуется добавить только файл сертификата.

3. Создайте объект **IPsec Tunnel** так же, как и в разделе с использованием общих ключей, но укажите использование сертификатов в **Authentication**. Выполните это с помощью следующих шагов:

а. Включите опцию **X.509 Certificate**.

б. Добавьте **Root Certificate**.

в. Выберите **Gateway Certificate**.

4. Откройте Web-интерфейс управления межсетевого экрана NetDefend в противоположной точке туннеля и повторите вышеуказанные шаги с другим набором сертификатов.

Примечание: Системные дата и время должны быть корректно настроены

Следует установить корректное время и дату в NetDefendOS, так как у сертификатов ограниченный срок действия.

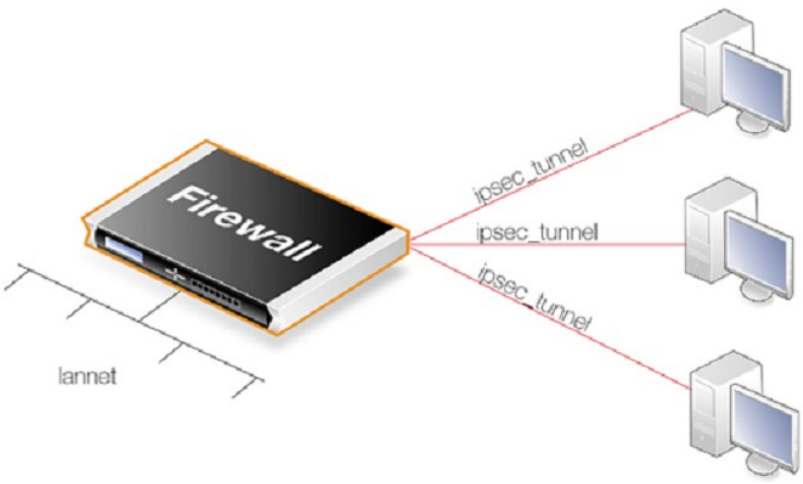
Также необходимо просмотреть указанный ниже *Раздел 9.6, «Доступ к серверу CA»*, в котором представлены принципы проверки подлинности сертификатов.

Самозаверяющие сертификаты вместо сертификатов, подписанных CA, могут использоваться для туннелей LAN to LAN, но Web-интерфейс и другие интерфейсы не поддерживают функцию их генерирования. Вместо этого, сертификаты должны быть сгенерированы другой утилитой и отправлены в NetDefendOS. Это означает, что сертификаты не являются действительно самозаверяющими, так как они генерируются вне управления NetDefendOS и следует помнить, что нет гарантии, что их приватный ключ является уникальным. Тем не менее, пользователю обеспечен соответствующий уровень безопасности.

Требуются два самозаверяющих сертификата, используемые в каждой точке туннеля следующим образом: один сертификат используется в качестве *корневого сертификата* в одной точке, называемой **Сторона А,** и в качестве *сертификата узла* в противоположной точке, называемой **Сторона Б**. Второй сертификат используется противоположным образом: в качестве *сертификата узла* на **Стороне А** и в качестве *корневого сертификата* на **Стороне Б.**

Нет необходимости рассматривать сервер CA при работе с самозаверяющими сертификатами, так как поиск сервера CA не выполняется.

9.2.3. Подключение удаленных клиентов к IPsec-туннелю с использованием общих ключей



В данном разделе представлена подробная информация о подключении удаленных клиентов через IPsec туннель с использованием общих ключей. Существует два типа удаленных клиентов:

А. IP-адреса клиентов уже назначены.

Б. IP-адреса клиентов неизвестны и должны быть выданы системой NetDefendOS при подключении клиентов.

А. IP-адреса уже назначены

IP-адреса могут быть известны заранее и предварительно назначены удаленным клиентам перед их подключением. IP-адрес вводится вручную.

1. Настройка аутентификации пользователя. Аутентификация пользователя *XAuth* не требуется удаленным клиентам IPsec, однако, это рекомендуемая функция (для упрощения первоначальной настройки можно пропустить данный шаг). Источник аутентификации может быть одним из следующих:

- Встроенная база данных пользователей (**Local User DB)**.
- Внешний сервер аутентификации.

В данном разделе выполняется настройка внутренней базы данных пользователя. Позднее можно заменить на внешний сервер.

Аутентификация пользователя с помощью внутренней базы данных осуществляется следующим образом:

- Укажите объект **Local User DB** (назовем его *TrustedUsers*).
- Добавьте пользователей в объект *TrustedUsers*. Необходима, как минимум, комбинация имени пользователя и пароля.

Можно указать строку пользователя **Group,** если необходимо ограничить доступ группы к определенным сетям источника. Также можно указать **Group** (с той же текстовой строкой) в разделе **Authentication** IP-объекта. Если IP-объект используется далее как **Source Network** правила в наборе IP-правил, данное правило будет применяться только к пользователю, если строка **Group** соответствует строке **Group** IP-объекта.

Примечание

*Строка **Group** не имеет значения в Правилах Аутентификации (**Authentication Rules**).*

- Создайте новое правило аутентификации пользователя **(User Authentication Rule)** с источником аутентификации **(Authentication Source)**, установленным со значением *TrustedUsers*. Остальные параметры для правила:

Agent	Auth Source	Src Network	Interface	Client Source IP
XAUTH	Local	all-nets	any	all-nets (0.0.0.0/0)

2. У объекта **IPsec Tunnel** *ipsec_tunnel* должны быть следующие параметры:

- Установите значение *lannet* для **Local Network.**
- Установите значение *all-nets* для **Remote Network**.
- Установите значение *all-nets* для **Remote Endpoint**.
- Установите значение *Tunnel* для **Encapsulation mode**.
- Укажите списки выбора алгоритмов IPsec и IKE, соответствующие возможностям клиентов.

- Нельзя предварительно указать маршруты, поэтому для объекта туннеля необходимо включить опцию **Динамически добавить маршрут в удаленную сеть после установки туннеля (Dynamically add route to the remote network when tunnel established)**. Если *all-nets* – это сеть назначения, необходимо отключить опцию *Добавить маршрут в удаленную сеть (Add route for remote network)*.

Примечание

Нет необходимости включать опцию динамического добавления маршрутов в сценарии установки туннеля LAN to LAN.

- Включите опцию **Require IKE XAuth user authentication for inbound IPsec tunnels**. При этом выполняется поиск соответствия правилу XAUTH в правилах аутентификации.

3. Набор IP-правил должен содержать одно правило:

Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
Allow	ipsec_tunnel	all-nets	lan	lannet	All

Так как правило *Allow* разрешает установку соединения, разрешен двунаправленный поток трафика, поэтому в данном случае используется только одно правило. Вместо *all-nets*, используемого выше, может использоваться более защищенный IP-объект, который указывает точный диапазон предварительно назначенных IP-адресов.

Б. IP-адреса выдаются системой NetDefendOS

Если IP-адреса клиента неизвестны, то они могут быть назначены системой NetDefendOS. Для этого необходимо выполнить следующее:

1. Если в качестве пула доступных адресов используется определенный диапазон IP-адресов, то:

- Создайте объект **Config Mode Pool** (только один, связанный с установкой NetDefendOS) и укажите диапазон адресов.

- Включите опцию **IKE Config Mode** в объекте **IPsec Tunnel –** *ipsec_tunnel*.

2. Если IP-адреса клиента получены через DHCP:

- Создайте объект **IP Pool** и укажите используемый DHCP-сервер. DHCP-сервер может быть указан в виде IP-адреса или, в качестве альтернативы, быть доступным на определенном интерфейсе. Если используется внутренний DHCP-сервер, то укажите адрес loopback *127.0.0.1* в качестве IP-адреса DHCP-сервера.

- Создайте объект **Config Mode Pool** (только один, связанный с установкой NetDefendOS) и свяжите его с объектом IP Pool, указанным в предыдущем шаге.

- Включите опцию **IKE Config Mode** в объекте **IPsec Tunnel –** *ipsec_tunnel*.

Настройка IPsec-клиентов

Оба варианта **(А)** и **(Б)**, представленные выше, требуют корректной настройки IPsec-клиента. Для настройки клиента требуется следующее (также как и в случае с использованием общих ключей):

- Укажите URL или IP-адрес межсетевого экрана NetDefend. Клиенту необходимо определить местоположение конечной точки туннеля.

- Укажите общий ключ, используемый для IPsec security.

- Укажите поддерживаемые системой NetDefendOS алгоритмы IPsec, которые будут использоваться в дальнейшем.

- Укажите, будет ли использовать клиент режим настройки.

Существует множество различных ПО IPsec, доступных у поставщиков, и данное руководство

пользователя не сконцентрировано на определенном ПО. Сетевой администратор должен использовать клиента, наиболее выгодного экономически и удовлетворяющего потребности.

9.2.4. Подключение удаленных клиентов к IPsec-туннелю с использованием сертификатов

Если при работе с удаленными IPsec-клиентами вместо общих ключей используются сертификаты, то в таком случае нет необходимости использовать объект **Pre-shared Key,** и различия в настройке будут следующими:

1. Загрузите *Корневой сертификат* и *Сертификат шлюза* в NetDefendOS. Необходимо загрузить два компонента корневого сертификата: файл сертификата и файл приватного ключа. Для сертификата шлюза необходимо добавить только файл сертификата.

2. При настройке объекта **IPsec Tunnel** определите сертификаты для использования в **Authentication**. Для этого выполните следующее:

а. Включите опцию **X.509 Certificate.**

б. Выберите **Gateway Certificate** (**Сертификат шлюза**).

в. Добавьте **Root Certificate** (**Корневой сертификат**).

3. Необходимо корректно настроить программное обеспечение IPsec с использованием сертификатов и удаленных IP-адресов. Как указано выше, программное обеспечение доступно у поставщиков и в данном руководстве не обсуждается какой-либо определенный клиент.

Шаг по настройке аутентификации пользователя является опциональным, так как представляет собой дополнительный уровень безопасности сертификатов.

Примечание: Системные дата и время должны быть корректно установлены

Следует установить корректное время и дату в NetDefendOS, так как у сертификатов ограниченный срок действия.

Также необходимо просмотреть *Раздел 9.6, «Доступ к серверу CA»*, в котором описывается проверка подлинности сертификатов.

9.2.5. Подключение клиентов к L2TP-туннелю с использованием общих ключей

L2TP, встроенный в Microsoft Windows, популярен среди VPN-клиентов удаленного доступа. Как правило, L2TP инкапсулируется в IPsec, обеспечивая шифрование при работе IPsec в режиме *transport mode* вместо *tunnel mode.* Для настройки L2TP over IPsec необходимы следующие шаги:

1. Создайте IP-объект (назовем его *l2tp_pool*), с указанием диапазона назначаемых клиенту IP-адресов. Диапазон может быть двух типов:

- Диапазон взят из внутренней сети, к которой подключены клиенты. Если диапазон внутренней сети – 192.168.0.0/24, то можно использовать адреса в диапазоне 192.168.0.10 – 192.168.0.20. Опасность заключается в случайном использовании IP-адреса во внутренней сети и его назначении клиенту.

- Используйте новый диапазон адресов, полностью отличающийся от диапазона любой внутренней сети, чтобы исключить возможность использования адреса во внутренней сети.

2. Укажите два других IP-объекта:

- *ip_ext* – внешний публичный IP-адрес для подключения клиентов (предположим, что это IP-адрес интерфейса *ext*).

- *ip_int* – внутренний IP-адрес интерфейса для подключения внутренней сети (назовем этот интерфейс *int*).

3. Укажите совместно используемый ключ (**Pre-shared Key**) для IPsec-туннеля.

4. Укажите объект *IPsec Tunnel* (назовем этот объект *ipsec_tunnel*) со следующими параметрами:

- Для **Local Network** (Локальная сеть) укажите значение *ip_ext* (укажите *all-nets*, если NetDefendOS находится позади устройства, преобразующего адреса с помощью NAT).
- Для **Remote Network** (Удаленная сеть) укажите значение *all-nets*.
- Для **Remote Endpoint** (Удаленная конечная точка) укажите значение *none*.
- Для **Authentication** (Аутентификация) выберите объект **Pre-shared Key**, заданный в первом шаге.
- Для **Encapsulation Mode** (Режим шифрования) укажите значение *Transport*.
- Укажите списки выбора алгоритмов IPsec и IKE.
- Включите опцию **Динамически добавить маршрут в удаленную сеть после установки туннеля (Dynamically add route to the remote network when tunnel established).**
- Если для сети назначения указано значение *all-nets*, как в данном случае, необходимо выключить опцию **Добавить маршрут для удаленной сети (Add route for remote network)**. Данная настройка включена по умолчанию.

5. Укажите PPTP/L2TP-сервер (назовем этот объект *l2tp_tunnel*) со следующими параметрами:

- Для **Inner IP Address** укажите значение *ip_int*.
- Для **Tunnel Protocol** укажите значение *L2TP*.
- Для **Outer Interface Filter** укажите значение *ipsec_tunnel*.
- Для **Outer Server IP** укажите значение *ip_ext*.
- Выберите **Microsoft Point-to-Point Encryption**. Поскольку используется шифрование IPsec, может быть установлено только значение *None*, в противном случае, двойное шифрование снизит пропускную способность.
- Для **IP Pool** (Пул IP-адресов) укажите значение *l2tp_pool*.
- Включите Proxy ARP на интерфейсе *int*, к которому подключена внутренняя сеть.
- Добавьте интерфейс в определенную таблицу маршрутизации, таким образом, маршруты автоматически добавляются в таблицу. Как правило, выбирается таблица *main*.

6. Для аутентификации пользователя:

- Укажите объект **Local User DB** (назовем его *TrustedUsers*).
- Добавьте отдельных пользователей в *TrustedUsers*. Необходима, как минимум, комбинация имени пользователя и пароля.

  Можно указать строку **Group,** подробная информация об этом представлена в аналогичном шаге в вышеуказанном разделе *IPsec Roaming Clients*.

- Укажите Правило аутентификации пользователя:

Agent	Auth Source	Src Network	Interface	Client Source IP
PPP	Local	all-nets	l2tp_tunnel	all-nets (0.0.0.0/0)

7. Для того чтобы разрешить прохождение трафика по L2TP-туннелю, необходимо указать следующие правила в наборе IP-правил:

Действие	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения	Сервис
Allow	l2tp_tunnel	l2tp_pool	any	int_net	All

NAT	ipsec_tunnel	l2tp_pool	ext	all-nets	All

Второе правило позволяет клиентам просматривать Web-страницы через интерфейс *ext* на межсетевом экране NetDefend. Клиенту будет назначен приватный внутренний IP-адрес, который необходимо преобразовать с помощью NAT в случае, если через межсетевой экран будет установлено соединение с Интернет.

8. Настройка клиента. В ОС Windows XP для запуска *Мастера установки нового соединения* необходимо выбрать опцию Создать новое соединение (**Create new connection)** в Сетевые соединения (**Network Connections)**. Для того чтобы войти в Мастер установки, необходимо ввести следующую информацию: URL-адрес межсетевого экрана или, в качестве альтернативы, его IP-адрес *ip_ext.*

Далее выберите **Сеть (Network)** > **Свойства (Properties)**. В открывшемся диалоговом окне выберите L2TP-туннель и Свойства (**Properties)**. В новом диалоговом окне выберите вкладку **Networking** и **Force to L2TP**. Далее вернитесь в свойства L2TP-туннеля, выберите вкладку Безопасность (**Security)** и нажмите кнопку Настройки IPsec (**IPsec Settings)**. Далее введите совместно используемый ключ.

9.2.6. Подключение клиентов к L2TP-туннелю с использованием сертификатов

Если вместо общих ключей L2TP-клиенты используют сертификаты, то различия в настройке будут следующими:

1. Необходимо установить корректную дату и время NetDefendOS, так как срок действия сертификатов ограничен.

2. Загрузите *Сертификат шлюза* и *Корневой сертификат* в NetDefendOS.

3. При настройке объекта **IPsec Tunnel**, укажите сертификаты, используемые в **Аутентификации**. Это выполняется следующим образом:

а. Включите опцию **X.509 Certificate**.

б. Выберите **Gateway Certificate**.

в. Добавьте **Root Certificate**.

4. При использовании L2TP-клиента Windows XP, перед установкой соединения с помощью **Мастера установки нового соединения**, необходимо загрузить в Windows соответствующие сертификаты.

Шаг по настройке аутентификации пользователя является дополнительным.

Пожалуйста, ознакомьтесь с *Разделом 9.6, «Доступ к серверу CA»*, в котором представлены важные аспекты проверки сертификатов.

9.2.7. Подключение клиентов к PPTP-туннелю

Установка PPTP значительно проще, чем установка L2TP, так как вместо IPsec используется собственное, менее эффективное шифрование.

Основным недостатком является невозможность установки соединений NAT PPTP через туннель, таким образом, несколько клиентов могут использовать только одно соединение с межсетевым экраном NetDefend. Если выполняется преобразование адресов с помощью NAT, соединение будет успешно установлено только для первого клиента.

Для установки PPTP выполняются следующие шаги:

1. В адресной книге (**Address Book**) укажите следующие IP-объекты:

- *pptp_pool* – диапазон внутренних IP-адресов, назначаемых из внутренней сети.
- *int_net* – внутренняя сеть, из которой назначаются адреса.

- *ip_int* – внутренний IP-адрес интерфейса, подключенного к внутренней сети. Предположим, что это интерфейс *int*.

- *ip_ext* – внешний публичный адрес, к которому подключаются клиенты (предположим, что это адрес интерфейса *ext*).

2. Укажите объект **PPTP/L2TP** (назовем его *pptp_tunnel*) со следующими параметрами:

- Для **Inner IP Address** укажите *ip_net.*

- Для **Tunnel Protocol** укажите *PPTP*.

- Для **Outer Interface Filter** укажите *ext*.

- Для **Outer server IP** укажите *ip_ext*.

- Для **Microsoft Point-to-Point Encryption** рекомендуется выключить все опции за исключением опции *128-битного* шифрования.

- Для **IP Pool** укажите *pptp_pool*.

- Включите Proxy ARP на интерфейсе *int*.

- Так же как в случае с использованием L2TP включите автоматическое добавление новых маршрутов в *основную* таблицу маршрутизации.

3. Укажите правило аутентификации пользователя, почти идентичное L2TP:

Agent	Auth Source	Src Network	Interface	Client Source IP
PPP	Local	all-nets	pptp_tunnel	all-nets (0.0.0.0/0)

4. Укажите IP-правила в наборе IP-правил:

Action	Src Interface	Src Network	Dest Interface	Dest Network	Service
Allow	pptp_tunnel	pptp_pool	any	int_net	All
NAT	pptp_tunnel	pptp_pool	ext	all-nets	All

Как указывалось для L2TP, правило *NAT* обеспечивает клиентам доступ в публичную сеть Интернет через межсетевой экран NetDefend.

5. Настройка клиента. Для Windows XP данная процедура аналогична настройке, описанной для L2TP, но без ввода общего ключа.

9.3. Компоненты IPsec

В данном разделе представлены стандарты IPsec и различные компоненты, методы и алгоритмы, используемые в VPN на основе IPsec.

9.3.1. Обзор

Internet Protocol Security (IPsec) – это набор протоколов, определенных организацией IETF (Internet Engineering Task Force) и обеспечивающих защищенную передачу данных на сетевом уровне. VPN на основе IPsec состоит из двух частей:

- Протокол IKE (Internet Key Exchange)

- Протоколы IPsec (AH/ESP/оба)

Первая часть, IKE, это фаза начального согласования, во время которой между двумя конечными точками VPN идут переговоры по поводу того, какие методы будут использоваться для обеспечения безопасности основного IP-трафика. Более того, IKE используется для управления соединениями,

определяя набор безопасных ассоциаций (Security Associations, SA) для каждого соединения. Ассоциации SA являются однонаправленными, поэтому, как правило, для каждого IPsec-соединения существует как минимум две ассоциации.

Вторая часть – передача IP-данных с помощью методов шифрования и аутентификации, утвержденных в согласовании IKE. Выполняется с помощью нескольких методов; с использованием IPsec-протоколов ESP, AH или комбинации из двух протоколов.

Поток событий состоит из следующих стадий:

- IKE согласовывает способ защиты IKE
- IKE согласовывает способ защиты IPsec
- IPsec отправляет данные в VPN

В следующих разделах представлено подробное описание каждой из данных стадий.

9.3.2. Протокол IKE (Internet Key Exchange)

Данный раздел описывает протокол IKE (Internet Key Exchange), а также используемые параметры.

Данные передаются напрямую, единственное, что требуется – алгоритмы шифрования и аутентификации, а также ключи. Протокол IKE (Internet Key Exchange), используемый в качестве метода распределения «ключей сессии», также предоставляет конечным точкам VPN возможность согласовать способ защиты данных.

У протокола IKE три основные задачи:

- Предоставить конечным точкам средства, позволяющие им аутентифицировать друг друга.
- Установить новые IPsec-соединения (создать пары SA)
- Управлять существующими соединениями

Безопасные ассоциации (SA)

Протокол IKE отслеживает соединения, назначая набор безопасных ассоциаций (SA) для каждого соединения. SA описывает все параметры, связанные с определенным соединением, например, используемый IPsec-протокол (ESP/AH/оба), а также ключи сессии, используемых для шифрования/дешифрования и/или аутентификации/проверки передаваемых данных.

Безопасная ассоциация SA является однонаправленной и используется для потока трафика, идущего только в одном направлении. Поэтому для двунаправленного трафика, характерного для VPN, требуется более одной безопасной ассоциации на соединение. В большинстве случаев, при использовании одного ESP или AH, для каждого соединения создаются две SA, одна описывает входящий трафик, а другая – исходящий. В случае, когда используются ESP и AH, будет создано четыре ассоциации SA.

Согласование IKE

Процесс согласования параметров сессии состоит из определенного количества фаз и режимов. Подробная информация представлена в разделах ниже.

Поток событий суммируется следующим образом:

IKE Phase-1
- Согласование защиты IKE

IKE Phase-2
- Согласование защиты IPsec
- Получение новых ключей сессии при обмене ключами в фазе-1, используемых в аутентификации и шифровании потока VPN-данных.

Срок действия IKE и IPsec

Оба соединения IKE и IPsec имеют ограниченный срок действия, измеряемый в единицах времени (секунды) и объема данных (килобайты). Данный срок действия предотвращает длительное использование соединения, что является выгодным с точки зрения криптоанализа.

Срок действия IPsec должен быть короче, чем срок действия IKE. Разница во времени между двумя сроками действия должна быть, как минимум, 5 минут. Это позволяет IPsec-соединению повторно получить ключ, благодаря выполнению другой фазы согласования – фазы-2. Нет необходимости выполнять согласование другой фазы-1 пока не истечет срок действия IKE.

IKE Algorithm Proposals

Список предложенных IKE алгоритмов предоставляет различные способы защиты потока данных с помощью IPsec. VPN-устройство, инициирующее IPsec-соединение, отправляет список поддерживаемых комбинаций алгоритмов, обеспечивающих защиту соединения, устройству в противоположной точке соединения, чтобы выяснить, какой из алгоритмов является подходящим.

Отвечающее VPN-устройство, получившее список поддерживаемых алгоритмов, выбирает комбинацию алгоритмов, наиболее подходящую политикам безопасности, и отправляет ответ с указанием выбранного алгоритма. Если подходящий алгоритм не найден, устройство отправляет ответ, сообщая, что в списке нет подходящего алгоритма, и, возможно, также предоставляет текстовое объяснение в целях диагностики.

Это согласование, осуществляемое при поиске взаимовыгодного алгоритма, выполняется не только для обнаружения наилучшего способа защиты IPsec-соединения, но также в целях обеспечения безопасности самого согласования IKE.

Список предлагаемых алгоритмов содержит не только подходящие комбинации алгоритмов для шифрования и аутентификации данных, но также другие параметры, связанные с IKE. Подробная информация о согласовании IKE и других параметрах IKE представлена далее.

IKE Phase-1 - IKE Security Negotiation

Согласование IKE состоит из двух фаз. Фаза 1 используется для взаимной аутентификации двух межсетевых экранов VPN или VPN-клиентов, подтверждая, что у удаленного устройства соответствующий общий ключ.

Защита согласования IKE выполняется, как описывается в предыдущем разделе, когда инициатор отправляет список предложений отвечающему устройству. После отправки и получения списка, попытаемся аутентифицировать противоположную точку VPN-соединения. Техника, известная как *Алгоритм обмена ключами Диффи-Хеллмана* позволяет двум узлам получить совместно используемый ключ и ключи для шифрования.

Аутентификация выполняется с помощью общих ключей, сертификатов или публичных ключей, используемых для шифрования. На данный момент применение общих ключей – это наиболее широко используемый метод аутентификации. NetDefendOS VPN-модуль поддерживает PSK и сертификаты.

IKE Phase-2 - IPsec Security Negotiation

В фазе 2 выполняется другое согласование с детализацией параметров для IPsec-соединения.

Во время фазы 2 также будут получены новые ключи в результате обмена Диффи-Хеллмана, используемые для защиты потока данных VPN.

Если используется *PFS* (Perfect Forwarding Secrecy), для каждого согласования фазы 2 выполняется новый обмен Диффи-Хеллмана. Поскольку это согласование требует больше времени, оно гарантирует, что никакие ключи не будут зависеть от любых ранее использованных ключей; никакие ключи не будут извлекаться из начального ключа. Это сделано для того, чтобы в случае рассекречивания некоторых ключей, не создавались зависимые ключи.

После завершения фазы 2 VPN-соединение установлено и готово к работе.

Параметры IKE

В процессе согласования используется ряд параметров.

Ниже приведена краткая информация о параметрах, необходимых для настройки VPN-соединения. Рекомендуется изучить данную информацию перед настройкой конечных точек VPN, так как

согласование всех параметров является крайне важным для обеих точек доступа.

При наличии двух межсетевых экранов в качестве конечных точек VPN, процесс согласования значительно упрощен, так как параметры настройки NetDefendOS будут такими же, что и на другом узле. Тем не менее, этот процесс может быть затруднен, если для установки VPN-туннеля используется оборудование различных производителей.

Endpoint Identification

Local ID – это идентификатор, используемый для идентификации конечной точки VPN-туннеля. Вместе с общими ключами это уникальная часть данных, идентифицирующая конечную точку.

Аутентификация с совместно используемым ключом основана на алгоритме Диффи-Хеллмана.

Local and Remote Networks/Hosts

Существуют подсети или узлы, между которыми передаются защищенные данные. В соединении LAN-to-LAN это сетевые адреса соответствующих сетей LAN.

Если используются удаленные клиенты, для удаленной сети будет установлено значение *all-nets*, означающее, что клиент может подключиться из любой точки.

Tunnel / Transport Mode

IPsec может использоваться в двух режимах *tunnel* или *transport*.

Режим *tunnel* указывает на то, что трафик стуннелирован на удаленное устройство, которое дешифрует/аутентифицирует данные, извлеченные из туннеля и отправленные в точку конечного назначения.

В режиме *transport*, трафик не будет стуннелирован и, следовательно, не будет проходить через VPN-туннели. Режим применяется для защиты данных, передаваемых от VPN-клиента непосредственно на межсетевой экран NetDefend, например, для защищенной удаленной настройки.

Как правило, в большинстве случаев установлено значение «tunnel».

Remote Endpoint

Удаленная конечная точка доступа (иногда – *удаленный шлюз*) – это устройство, выполняющее дешифрование/аутентификацию VPN и передающее незашифрованные данные в точку конечного назначения. В данном поле также можно установить значение *None*, после чего межсетевой экран NetDefend рассматривает удаленный адрес как удаленную конечную точку. Это особенно полезно при удаленном доступе, если IP-адреса удаленных VPN-клиентов не указаны предварительно. Настройка "none" позволит любому IP-адресу, соответствующему "remote network" адресу удаленной подсети, оговоренному выше, открыть VPN-соединение, при условии, что они могут проходить проверку подлинности должным образом.

Можно указать URL-адрес удаленной конечной точки, например, *vpn.company.com*. В таком случае необходимо использовать префикс *dns:*. Следовательно, URL-адрес будет выглядеть следующим образом *dns:vpn.company.com*.

Удаленная конечная точка не используется в режиме Transport.

Main/Aggressive Mode

У согласования IKE два режима работы: Main и Aggressive.

Различие между двумя режимами заключается в том, что в режиме Aggressive передается больше информации в меньшем количестве пакетов, с преимуществом более быстрой установки соединения и эффективной передачи.

При использовании режима Aggressive, некоторые параметры

настройки, такие как группы Диффи-Хеллман и PFS, не могут быть согласованы, что подчеркивает важность наличия «совместимых» настроек в обеих точках.

IPsec Protocols

Протоколы IPsec, используемые для обработки данных. На выбор доступны два протокола AH (Authentication Header) и ESP (Encapsulating Security Payload).

Протокол ESP обеспечивает шифрование, аутентификацию или обе функции вместе. Тем не менее, не рекомендуется использовать только шифрование, так как при этом значительно снижается уровень безопасности.

Помните, что протокол AH обеспечивает только аутентификацию. Отличие от ESP заключается только в том, что AH также аутентифицирует части внешнего IP-заголовка, например, адреса источника или назначения, подтверждая то, что пакет пришел с адреса, указанного в заголовке.

Примечание

Система NetDefendOS не поддерживает AH.

IKE Encryption

Указывает алгоритм шифрования, используемый в согласовании IKE и, в зависимости от алгоритма, размер используемого ключа шифрования.

Алгоритм, поддерживаемые NetDefendOS IPsec:

- DES

Алгоритм DES включен только для обеспечения совместимости с другими, более ранними реализациями VPN. Следует избегать использования DES в случаях, когда это возможно, так как это один из первоначальных алгоритмов, который является менее эффективным.

IKE Authentication

Определяет алгоритмы аутентификации, используемые в фазе согласования IKE.

Алгоритмы, поддерживаемые NetDefendOS IPsec:

- SHA1
- MD5

IKE DH Group

Указывает группу Diffi-Hellmann, используемую для обмена IKE. Доступные группы DH рассматриваются ниже.

IKE Lifetime

Продолжительность IKE-соединения.

Продолжительность соединения определена в единицах времени (секунды) и объема данных (килобайтах). Каждый раз по истечении продолжительности соединения, выполняется новая фаза-1. Если в течение последнего соединения не выполнялась передача данных, новое соединение не будет установлено до момента использования VPN-соединения. Данное значение должно быть больше, чем время продолжительности IPsec SA.

PFS

При отключении функции *PFS* (Perfect Forwarding Secrecy) во время обмена ключами при согласовании IKE на фазе-1 создаются данные

для начального ключа. Далее, в фазе-2 согласования IKE, из этих данных будут извлечены ключи для шифрования и аутентификации. Благодаря функции PFS в процессе повторного получения ключа будут создаваться новые данные для ключей. Если один ключ будет взломан, невозможно получить другой ключ, используя данную информацию.

Функция PFS используется в двух режимах: PFS on keys, обмен ключами будет выполняться для каждого согласования на фазе-2. При использовании режима PFS on identities, данные для идентификации также защищены, каждый раз при удалении фазы-1 SA согласование на фазе-2 будет прекращено, обеспечивая, таким образом, не более одного согласования на фазе-2, зашифрованного с помощью одного и того же ключа.

В целом функция PFS не требуется, так как взлом ключей для аутентификации или шифрования маловероятен.

PFS DH Group — Группа Диффи-Хеллман, используемая с PFS. Доступные группы DH рассматриваются ниже.

IPsec DH Group — Группа Диффи-Хеллман, используемая для соединения IPsec. Доступные группы DH рассматриваются ниже в разделе *Группы Диффи-Хеллман.*

IPsec Encryption — Алгоритм шифрования, используемый для защиты трафика IPsec.

При использовании AH или в случае использования ESP без кодирования, шифрование IPsec не требуется.

Алгоритм, поддерживаемый VPN межсетевого экрана NetDefend:

- DES

IPsec Authentication — Алгоритм аутентификации, используемый для защиты трафика.

При использовании ESP без аутентификации, данная функция не требуется, однако, не рекомендуется использовать ESP без аутентификации.

Алгоритмы, используемые межсетевым экраном NetDefend:

- SHA1
- MD5

IPsec Lifetime — Продолжительность VPN-соединения определена в единицах времени (секунды) и объема данных (килобайтах). Каждый раз при превышении этих значений выполняется повторная выдача ключей, с предоставлением новых ключей для аутентификации и шифрования IPsec. Если в течение последнего повторной выдачи ключа не использовалось VPN-соединение, соединение будет завершено и повторно установлено при необходимости.

Необходимо установить значение ниже, чем значение параметра IKE lifetime.

Группы Диффи-Хеллман

Диффи-Хеллман (Diffie-Hellman, DH) – это криптографический протокол, позволяющий двум сторонам, не имеющим информации друг о друге, задать общий секретный ключ через незащищенный канал соединения с помощью обмена незашифрованным текстом. В случае если обмен может просматриваться третьей стороной, алгоритм Диффи-Хеллмана значительно усложняет определение общего секретного ключа и расшифровку данных.

Алгоритм *Диффи-Хеллман* используется для назначения общих секретных ключей для IKE, IPsec и PFS.

Группа Diffie-Hellman указывает на степень безопасности, используемую для обмена DH. Чем больше количество групп, тем выше безопасность, а также расходы, связанные с обработкой. Система NetDefendOS поддерживает следующие группы DH:

- DH группа 1 (768-бит)
- DH группа 2 (1024-бит)
- DH группа 5 (1536-бит)

Все эти группы НА доступны для использования с IKE, IPsec и PFS.

9.3.3. Аутентификация IKE

Обмен ключами вручную

Наиболее простым способом настройки VPN является метод *manual keying* (обмен ключами вручную). В данном методе IKE не используется; настройка ключей для аутентификации и шифрования, а также некоторых других параметров выполняется непосредственно на противоположных узлах VPN-туннеля.

Примечание

NetDefendOS не поддерживает функцию обмена ключами вручную.

Преимущества функции обмена ключами вручную

Обмен ключами вручную является довольно простым и, соответственно, функционально совместимым процессом. В настоящее время в IKE существует множество проблем совместимости. Обмен ключами вручную «обходит» IKE и устанавливает собственные IPsec SA.

Недостатки функции обмена ключами вручную

Обмен ключами вручную является методом, который применялся до введения в использование протокола IKE и поэтому не содержащит некоторые функции IKE. Следовательно, этот метод имеет ряд ограничений, таких, как необходимость всегда использовать один и тот же ключ для аутентификации/шифрования и отсутствие служб анти-повтора (anti-replay services). Также нет способа проверки подлинности удаленного узла / межсетевого экрана.

Данный тип соединения также уязвим для так называемых «атак повтора» (replay attacks), другими словами, злоумышленники, у которых есть доступ к зашифрованному трафику, могут записывать некоторые пакеты, хранить их и отправлять по месту назначения позже. У конечной точки назначения VPN не будет никакой возможности сообщить, была ли выполнена повторная передача пакета или нет. Использование IKE устраняет эту уязвимость.

PSK

При применении *PSK* (Pre-shared Key) конечные точки VPN совместно используют секретный ключ. Эта услуга, предоставляемая IKE, и, следовательно, содержащая все преимущества IKE, что обеспечивает больше возможностей, чем обмен ключами вручную.

Преимущества PSK

Использование общего ключа имеет ряд преимуществ по сравнению с функцией обмена ключами вручную. Например, аутентификация пользователя, для которой используются общие ключи. Функция также включает в себя все преимущества использования IKE. Вместо использования фиксированного набора ключей шифрования, сеансовые ключи используются в течение ограниченного периода времени, после которого применяется новый набор сеансовых ключей.

Недостатки PSK

Единственное, что необходимо учитывать при использовании ключей PSK – это их распределение. Каким образом ключи PSK распределяются между удаленными VPN-клиентами и межсетевыми экранами? Это важный вопрос, так как безопасность системы PSK основана на секретности ключей. Если один ключ PSK взломан, необходимо изменить настройки для использования новый ключей.

Сертификаты

У каждого межсетевого экрана VPN есть собственный сертификат и один (или более) доверенный корневой сертификат.

Аутентификация основана на том, что:

- У каждой конечной точки есть приватный ключ, соответствующий публичному ключу в сертификате и доступный только для данной конечной точки.
- Сертификат, подписанный кем-либо, является доверенным для удаленной конечной точки.

Преимущества сертификатов

Основным преимуществом сертификатов является универсальность. Например, можно управлять несколькими VPN-клиентами без одного и того же ключа, настроенного на каждом из них, что часто требуется при использовании общих ключей и удаленных клиентов. Вместо этого, если клиент взломан, сертификат клиента может быть объявлен недействительным. Нет необходимости в повторной настройке каждого клиента.

Недостатки сертификатов

Основным недостатком сертификатов является комплексность. Аутентификация на основе сертификата может использоваться как часть крупной инфраструктуры публичного ключа, что делает всех VPN-клиентов и межсетевые экраны зависимыми от третьей стороны. Другими словами, существует множество аспектов, которые необходимо настроить, но вероятность проблем при этом крайне высока.

9.3.4. Протоколы IPsec (ESP/AH)

IPsec-протоколы используются для защиты трафика, проходящего через VPN. Актуальные протоколы и ключи, используемые с этими протоколами, согласуются с помощью протокола IKE.

Существует два протокола, связанных с IPsec: AH и ESP. Данные протоколы рассматриваются ниже.

AH (Authentication Header)

AH – это протокол, используемый для аутентификации потока данных.

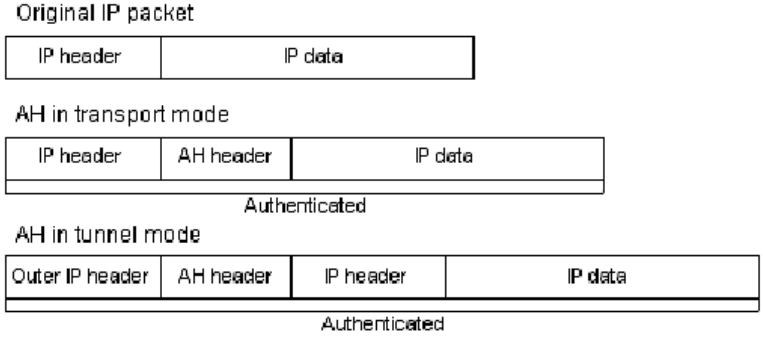


Рис. 9.1 Протокол AH

Протокол AH использует криптографическую хэш-функцию для создания MAC из данных в IP-

пакете. Далее выполняется передача данного MAC вместе с пакетом, позволяя удаленной конечной точке проверять целостность первоначального IP-пакета, чтобы убедиться в том, что данные не были подделаны при передаче в сети Интернет. Помимо данных IP-пакета, протокол AH также аутентифицирует части IP-заголовка.

Протокол AH вставляет заголовок AH после первоначального IP-заголовка. В режиме Tunnel заголовок AH вставляется после внешнего заголовка, но перед первоначальным, внутренним IP-заголовком.

ESP (Encapsulating Security Payload)

Протокол ESP вставляет заголовок ESP после первоначального IP-заголовка, в режиме Tunnel, заголовок ESP вставляется после внешнего заголовка, но перед первоначальным, внутренним IP-заголовком.

Все данные после заголовка ESP шифруются и/или аутентифицируются. Отличие от AH заключается в том, что ESP обеспечивает шифрование IP-пакета. Отличие фазы аутентификации состоит в том, что ESP только аутентифицирует данные после заголовка ESP; таким образом, внешний IP-заголовок остается незащищенным.

Протокол ESP используется как для шифрования, так и для аутентификации IP-пакета, а также только для шифрования или аутентификации.

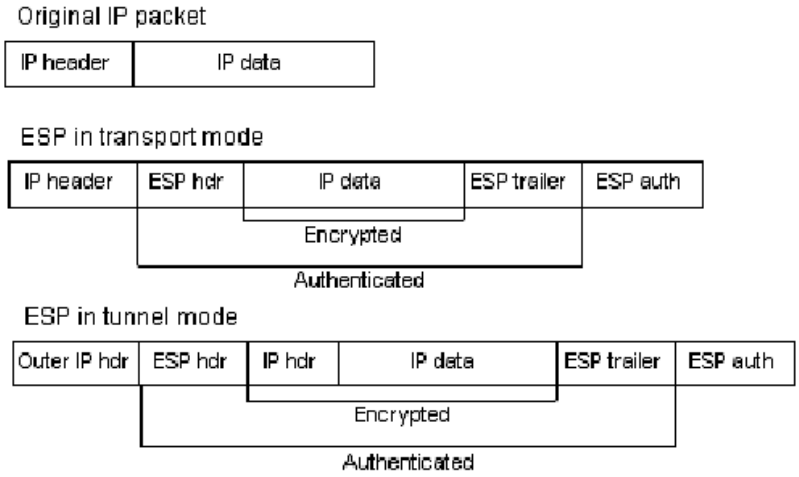


Рис. 9.2 Протокол ESP

9.3.5. NAT Traversal

У протоколов IKE и IPsec возникают сложности при работе NAT. Оба протокола не разработаны для работы с NAT и по этой причине используется протокол «NAT traversal». NAT traversal является дополнением к протоколам IKE и IPsec и позволяет им функционировать при преобразовании адресов с помощью технологии NAT. Система NetDefendOS поддерживает стандарт RFC3947 для NAT-Traversal с IKE.

NAT traversal разделяется на две части:

- Дополнения к протоколу IKE, позволяющие узлам IPsec сообщать друг другу о том, что они поддерживают NAT traversal и определенные версии. Система NetDefendOS поддерживает стандарт RFC3947 для NAT-Traversal с IKE.

- Изменения инкапсуляции ESP. При использовании NAT traversal ESP инкапсулируется в UDP, обеспечивающий более гибкое преобразование адресов с помощью технологии NAT.

Ниже представлено подробное описание изменений, примененных по отношению к протоколам IKE и IPsec.

NAT traversal используется только в том случае, если оба противоположных узла поддерживают данную функцию. С этой целью VPN-клиент с поддержкой NAT traversal отправляет специальный «vendor ID» для того, чтобы сообщить противоположному узлу, что поддерживает NAT traversal, а также указывает поддерживаемые версии проекта.

Использование NAT

Для определения NAT оба узла IPsec отправляют хэш собственных IP-адресов вместе с UDP-портом источника, используемым в согласованиях IKE. Эта информация используется для того, чтобы узнать, использует ли каждый узел тот же IP-адрес и порт источника, известные другим узлам. Если адрес и порт источника не изменены, то трафик не будет преобразован с помощью NAT и, соответственно, нет необходимости использовать NAT traversal. Если адрес и/или порт источника изменен, то трафик преобразован с помощью NAT.

Изменение портов

Если узлам IPsec необходимо использовать NAT traversal, согласование IKE перемещается с UDP-порта 500 на порт 4500. Это является необходимым, так как некоторые устройства NAT обрабатывают UDP-пакет на порту 500 в отличие от пакетов UDP, пытаясь решить проблему с IKE. Проблема заключается в том, что данная специальная обработка IKE-пакетов может нарушить согласование IKE, которое по этой причине переходит на другой порт.

Инкапсуляция UDP

Другая проблема, решаемая с помощью NAT traversal, связана с тем, что ESP-протокол является IP-протоколом. Нет информации о порте, как в TCP и UDP, что делает невозможным наличие более одного «натированного» клиента, подключенного к одному и тому же удаленному шлюзу в одно и то же время. По этой причине ESP-пакеты инкапсулируются в UDP. Трафик ESP-UDP отправляется на порт 4500, тот же порт использует IKE при применении NAT traversal. После смены порта, все последующие соединения IKE выполняются через порт 4500. Также периодически отправляются пакеты Keep-alive для поддержки NAT-отображения.

Настройка NAT Traversal

Большинство функций NAT traversal полностью автоматические, для инициации межсетевого экрана не требуется специальная настройка. Тем не менее, для отвечающих межсетевых экранов необходимо отметить два пункта:

- На отвечающих межсетевых экранах поле *Remote Endpoint* (Удаленная конечная точка) используется в качестве фильтра для IP-адреса источника полученных IKE-пакетов. Необходимо разрешить преобразование IP-адреса инициатора с помощью технологии NAT.

- При использовании общих ключей с несколькими туннелями, подключенными к одному удаленному межсетевому экрану, которые были преобразованы с помощью NAT в один и тот же адрес, важно убедиться в том, что *Local ID* является уникальным для каждого туннеля. Local ID может быть одним из:

    - **Auto** – в качестве локального идентификатора используется IP-адрес интерфейса исходящего трафика. Это рекомендуемая настройка, за исключением случаев, когда у двух межсетевых экранов один и тот же внешний IP-адрес.

    - **IP** – IP-адрес можно ввести вручную

    - **DNS** – DNS-адрес можно ввести вручную

    - **Email** – Email можно ввести вручную

9.3.6. Списки выбора алгоритмов (Algorithm Proposal Lists)

Для установки параметров VPN-соединения необходимо выполнить согласование. В результате согласований устанавливаются *security associations* (SA) IKE и IPsec. *Список выбора (proposal list)* является стартовой точкой согласования. Каждая запись в списке определяет параметры для алгоритма, поддерживаемого устройством конечной точки VPN-туннеля (в данном руководстве также будет использоваться сокращенный термин *tunnel endpoint*). Первоначальное согласование проводится для того, чтобы договориться о наборе алгоритмов, поддерживаемых устройствами на противоположных точках туннеля.

Существует два типа списков: IKE и IPsec. Списки IKE используются во время фазы-1 IKE (IKE Security Negotiation), а списки IPsec используются во время фазы-2 IKE (IPsec Security Negotiation).

Несколько списков выбора алгоритмов определены по умолчанию для различных сценариев VPN, также можно добавить списки, определенные пользователем.

По умолчанию определены два списка алгоритмов IKE и два списка IPsec:

- **High**

Состоит из ограниченного набора алгоритмов для повышения безопасности. Полный список: *MD5, SHA1*.

- **Medium**

Состоит из расширенного набора алгоритмов. Полный список: *MD5, SHA1*.

Пример 9.1. Использование списков выбора алгоритма

В данном примере рассматривается процесс создания и применения списка возможных алгоритмов IPSec для использования в VPN-туннеле. Предлагаемый алгоритм шифрования - DES. Необходимо использовать обе хэш-функции SHA1 и MD5, чтобы проверить, был ли изменен пакет во время передачи. Помните, что в данном примере не показано, как добавить определенный объект IPsec tunnel, который также будет использоваться в другом примере.

CLI

Сначала создайте список алгоритмов IPsec:

```
gw-world:/> add IPsecAlgorithms esp-l2tptunnel
                      DESEnabled=Yes DES3Enabled=Yes
                      SHA1Enabled=Yes MD5Enabled=Yes
```

Далее, примените список алгоритмов на выбор к туннелю IPsec:

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel
                      IPsecAlgorithms=esp-l2tptunnel
```

Web-интерфейс

Сначала создайте список алгоритмов IPsec:

1. Зайдите **Objects > VPN Objects > IPsec Algorithms > Add > IPsec Algorithms**

2. Введите имя списка, например, *esp-l2tptunnel*

3. Далее отметьте следующее:

   - **DES**
   - **SHA1**
   - **MD5**

4. Нажмите **OK**

Далее примените список алгоритмов на выбор к туннелю IPsec:

1. Зайдите **Interfaces > IPsec**

2. Выберите туннель IPsec

3. Выберите недавно созданный **esp-l2tptunnel** в настройках **IPsec Algorithms**

4. Нажмите **OK**

9.3.7. Общие ключи

Общие ключи используются для аутентификации VPN-туннелей. Ключи – это секретная информация, совместно используемая сторонами перед началом передачи данных. Для обмена данными обе стороны подтверждают, что им известен секретный ключ. Безопасность общего ключа зависит от «качества» парольной фразы. Парольные фразы это широко используемые слова, которые являются крайне уязвимыми для прямых атак.

Общие ключи генерируются автоматически через Web-интерфейс, а также через интерфейс командной строки CLI с помощью команды *pskgen* (данная команда подробно описана в *Руководстве по интерфейсу командной строки CLI*).

Остерегайтесь ключей, содержащих символы, не входящие в кодировку ASCII!

Если ключ PSK указан в виде парольной фразы и не в шестнадцатеричном значении, различные кодировки на разных платформах могут привести к проблеме с символами, не входящими в кодировку ASCII. Windows, например, кодирует общие ключи, содержащие символы, не входящие в кодировку ASCII, в кодировке UTF-16, в то время как система NetDefendOS использует кодировку UTF-8. Даже если они кажутся одинаковыми на противоположных точках туннеля, будет несоответствие, которое может привести к проблеме при настройке L2TP-клиента Windows, который подключен к системе NetDefendOS.

Пример 9.2. Использование общего ключа

В данном примере рассматривается процесс создания общего ключа и его применения к VPN-туннелю. Так как обыкновенные слова и фразы являются уязвимыми для прямых атак, не следует использовать их в качестве секретных ключей. В данном случае, общий ключ выбирается с помощью случайного выбора сгенерированного шестнадцатеричного ключа. Помните, что в данном примере не рассматривается способ добавления определенного объекта IPsec-туннеля.

CLI

Сначала создайте общий ключ. Для автоматической генерации ключа 64-бит (ключ по умолчанию) используйте:

```
gw-world:/> pskgen MyPSK
```

Для того чтобы создать более длинный, защищенный 512-битный ключ, используйте команду:

```
gw-world:/> pskgen MyPSK -size=512
```

Либо в качестве альтернативы, чтобы добавить общий ключ вручную, используйте:

```
gw-world:/> add PSK MyPSK Type=HEX PSKHex=<enter the key here>
```

Далее примените общий ключ к IPsec-туннелю:

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel PSK=MyPSK
```

Web-интерфейс

Сначала создайте общий ключ:

1. Зайдите **Objects > Authentication Objects > Add > Pre-shared key**

2. Введите имя общего ключа, например, *MyPSK*

3. Выберите **Hexadecimal Key (Шестнадцатеричный ключ)** и нажмите **Generate Random Key (Создать ключ методом случайного выбора)** для того, чтобы создать ключ в текстовом поле **Passphrase (Парольная фраза).**

4. Нажмите **OK**

Далее примените общий ключ к туннелю IPsec:

1. Зайдите **Interfaces > IPsec**

2. Выберите объект туннеля IPsec

3. Во вкладке **Authentication** выберите **Pre-shared Key** и выберите **MyPSK**

4. Нажмите **OK**

9.3.8. Списки идентификации

Если для аутентификации IPsec-туннелей используются сертификаты, межсетевой экран NetDefend принимает все удаленные устройства или VPN-клиентов, способных представить сертификат, подписанный любой из доверенных организаций CA (Certificate Authorities). Это может стать потенциальной проблемой, в особенности при использовании удаленных клиентов.

Типичный сценарий

Рассмотрим сценарий, когда выездные сотрудники получают доступ к внутренним корпоративным сетям с помощью VPN-клиентов. Организация управляет собственной доверенной организацией CA, и сотрудникам выдаются сертификаты. Различные группы сотрудников получают доступ к различным частям внутренней сети. Например, торговым агентам необходим доступ к серверам с системами подачи заказов, а техническим инженерам - доступ к базам с техническими данными.

Проблема

Так как IP-адреса VPN-клиентов выездных сотрудников не известны заранее, входящие VPN-соединения от клиентов не могут дифференцироваться. Это означает, что межсетевой экран не способен контролировать доступ к различным частям внутренних сетей.

Списки идентификаторов

Использование Списков идентификаторов представляет собой решение этой проблемы. Список идентификаторов содержит один или более идентификаторов (ID), где каждый идентификатор соответствует предметному полю в сертификате. Списки идентификаторов могут, таким образом, использоваться для регулирования того, какие сертификаты с доступом использовать и с какими IPsec-туннелями.

Пример 9.3. Использование списка идентификаторов

В данном примере рассматривается процесс создания списка идентификаторов и его применения к VPN-туннелю. Данный список идентификаторов содержит один идентификатор с именем DN (distinguished name) - отличительное имя, используемое в качестве первичного идентификатора. Помните, что в данном примере не рассматривается способ добавления определенного объекта IPsec-туннеля.

CLI

Сначала создайте Список идентификаторов:

```
gw-world:/> add IDList MyIDList
```

Далее создайте ID:

```
gw-world:/> cc IDList MyIDList

gw-world:/> add ID JohnDoe Type=DistinguishedName
                CommonName="John Doe"
                OrganizationName=D-Link
                OrganizationalUnit=Support
                Country=Sweden
                EmailAddress=john.doe@D-Link.com


gw-world:/> cc
```

В заключение примените список идентификаторов к IPsec-туннелю:

```
gw-world:/> set Interface IPsecTunnel MyIPsecTunnel
                      AuthMethod=Certificate IDList=MyIDList
                      RootCertificates=AdminCert
                      GatewayCertificate=AdminCert
```

Web-интерфейс

Сначала создайте список идентификаторов:

1. Зайдите **Objects > VPN Objects > ID List > Add > ID List**

2. Введите имя списка, например, *MyIDList*

3. Нажмите **OK**

Далее создайте ID:

1. Зайдите **Objects > VPN Objects > IKE ID List > Add > ID List**

2. Выберите **MyIDList**

3. Введите имя идентификатора, например, *JohnDoe*

4. Выберите **Distinguished name** в настройках **Type**

5. Далее введите:

• **Common Name:** John Doe

• **Organization Name:** D-Link

• **Organizational Unit:** Support

• **Country:** Sweden

• **Email Address:** john.doe@D-Link.com

6. Нажмите **OK**

В заключение примените список идентификаторов к туннелю IPsec:

1. Зайдите **Interfaces > IPsec**

2. Выберите необходимый объект туннеля IPsec

3. Во вкладке **Authentication** выберите **X.509 Certificate**

4. Выберите подходящий сертификат в управлении **Root Certificate(s)** и **Gateway Certificate**

5. Выберите **MyIDList** в **Identification List**

6. Нажмите **OK**

9.4. IPsec-туннели

Данный раздел содержит подробную информацию об IPsec-туннелях в NetDefendOS, их определении, функциях и использовании.

9.4.1. Обзор

IPsec-туннель определяет конечную точку зашифрованного туннеля. Каждый IPsec-туннель рассматривается в качестве физического интерфейса NetDefendOS, с одной и той же фильтрацией, формированием трафика и возможностями настройки в качестве стандартных интерфейсов.

Удаленная установка туннелей

Если другой межсетевой экран NetDefend или другой соответствующий сетевой продукт IPsec (также известный как *удаленная конечная точка*) попытается установить IPsec VPN-туннель к локальному межсетевому экрану, будет проверен список IPsec-туннелей, указанных в настоящее время в настройках NetDefendOS. Если найден соответствующий туннель, этот туннель будет открыт. Далее выполняются ассоциируемые согласования IKE и IPsec, в результате будет установлен туннель к удаленной конечной точке.

Локальная установка туннелей

В качестве альтернативы пользователь в защищенной локальной сети может попытаться получить доступ к источнику, который расположен в конечной точке IPsec-туннеля. В таком случае система NetDefendOS видит, что маршрут для IP-адреса источника проходит через определенный IPsec-туннель и установка туннеля выполняется с локального межсетевого экрана NetDefend.

IP-правила для управления зашифрованным трафиком

Необходимо помнить, что установка IPsec-туннеля НЕ гарантирует того, что весь трафик, проходящий через туннель, является доверенным. Наоборот, зашифрованный сетевой трафик будет проверен с помощью набора IP-правил. При выполнении этой проверки интерфейс источника трафика будет ассоциируемым IPsec-туннелем, так как туннели обрабатываются как интерфейсы в NetDefendOS.

Помимо этого, возможно потребуется указать Правило Маршрута или Доступа для удаленных клиентов, чтобы NetDefendOS смогла принять определенные IP-адреса источника из IPsec-туннеля.

Обратный трафик (Returning Traffic)

Для сетевого трафика, идущего в обратном направлении, в IPsec-туннель, выполняется обратный процесс. Сначала расшифрованный трафик оценивается набором правил. Если правило и маршрут совпадают, NetDefendOS пытается найти установленный IPsec-туннель, соответствующий критерию. Если туннель не найден, NetDefendOS попытается установить новый туннель к удаленной конечной точке, с помощью соответствующего указания IPSec-туннеля.

Для ограничения IPsec-трафика не требуются IP-правила

Вместе с IPsec-туннелями администратор, как правило, указывает IPsec-правила, которые позволяют незашифрованному трафику проходить через туннель (туннель обрабатывается как интерфейс NetDefendOS). Тем не менее, нет необходимости указывать IP-правила, разрешающие прохождение пакетов IPsec-трафика.

Пакеты IKE и ESP по умолчанию касаются внутреннего *IPsec engine* системы NetDefendOS и набор IP-правил не требуется.

Данные действия можно изменить в разделе **Расширенные настройки IPsec** на странице **IPsec Before Rules**. Примером причины выполнения данного изменения может быть большое количество попыток соединений IPsec, идущих с определенного IP-адреса или группы адресов. Это может снизить производительность NetDefendOS IPsec engine и привести к потере трафика с IP-правилом. Другими словами, можно использовать IP-правила для управления трафиком, связанным с туннелем.

Обнаружение недействующего узла (Dead Peer Detection)

Для IPsec-туннеля можно включить дополнительную функцию *DPD* (Dead Peer Detection). Функция DPD используется для контроля работоспособности туннеля с помощью отслеживания трафика, идущего с узла в противоположную точку туннеля. Если в течение определенного промежутка времени (указанного с помощью настройки **DPD Metric**) не получено сообщение, то система NetDefendOS отправляет сообщения *DPD-R-U-THERE* на узел, чтобы определить, доступен ли он и остается ли действующим.

Если узел не отвечает на эти сообщения в течение определенного периода времени (указанного с

помощью настройки **DPD Expire Time**), то узел считается недействующим и соединение разрывается. Система NetDefendOS пытается автоматически повторно установить туннель после определенного периода времени (указанного с помощью настройки **DPD Keep Time**).

Расширенные настройки DPD описаны в *Разделе 9.4.6, «Расширенные настройки IPsec»*. Для IPsec-туннелей NetDefendOS функция DPD включена по умолчанию. Отключение функции не приведет к выключению возможности ответить на сообщение *DPD-R-U-THERE* с другого узла.

Keep-alive

Функция IPsec *Keep-alive* обеспечивает сохранение туннеля в любое время, даже если передача данных не выполняется. Это выполняется с помощью непрерывной отправки запросов ICMP *Ping* через туннель. Если нет ответов на запросы ping, то соединение разрывается и выполняется попытка автоматической повторной установки туннеля. Данная функция является полезной только для туннелей LAN to LAN.

Дополнительно можно указать IP-адрес источника и/или назначения. Рекомендуется указать IP-адрес назначения хоста, который способен отвечать на сообщения ICMP. Если IP-адрес назначения не указан, система NetDefendOS будет использовать первый IP-адрес в удаленной сети.

Необходимо использовать функцию keep-alive, если можно установить туннель LAN to LAN с непостоянным трафиком только с одной стороны, но необходимо сохранить его для хостов на другом узле. Если узел, установивший туннель, использует функцию keep-alive для сохранения туннеля, любые хосты на противоположной стороне могут использовать туннель, даже если другой узел не может установить туннель в случае необходимости.

Различия между DPD и Keep-alive

DPD и Keep-alive выполняют практически одну и ту же функцию, определяющую, сохранен ли IPsec-туннель и осуществляющую повторную установку туннеля. Тем не менее, существуют различия:

- Функция Keep-alive используется только для IPsec-туннелей LAN to LAN. Не используется с удаленными клиентами.
- С помощью функции Keep-alive можно значительно быстрее определить, что соединение нарушено, и выполнить повторную установку соединения.

Нет необходимости в одновременном включении функций Keep-alive и DPD для туннеля LAN to LAN, так как, если отправлены запросы keep-alive pings, запуск функции DPD не произойдет.

Быстрый запуск IPsec-туннеля

Данный раздел содержит подробные сведения об IPsec-туннелях. Информация о быстром запуске шагов по установке для этих протоколов в типичных сценариях находится в следующих разделах:

- *Раздел 9.2.1, «Создание IPsec-туннелей LAN to LAN с использованием общих ключей».*
- *Раздел 9.2.2, «Создание IPsec-туннелей LAN to LAN с использованием сертификатов».*
- *Раздел 9.2.3, «Подключение удаленных клиентов к IPsec-туннелю с использованием общих ключей».*
- *Раздел 9.2.4, «Подключение удаленных клиентов к IPsec-туннелю с использованием сертификатов».*

Помимо раздела о быстром запуске, более подробная информация об установке туннеля представлена ниже.

9.4.2. Установка туннелей LAN to LAN с использованием общих ключей

VPN обеспечивает географически разделенным локальным вычислительным сетям (LAN)

защищенный обмен данными в сети Интернет. В корпоративном контексте это означает, что пользователи LAN в географически разделенных участках могут обмениваться информацией на безопасном уровне, что сопоставимо с обменом данными через выделенное, приватное соединение.

Защита соединения выполняется за счет использования IPsec туннелирования, с туннелем от VPN-шлюза в одном месте до VPN-шлюза в другом. Поэтому межсетевой экран NetDefend является установщиком VPN, и в то же время выполняет наблюдение за трафиком, проходящим через туннель. Этот раздел касается установки туннелей LAN to LAN, созданных с помощью общего ключа (PSK).

Шаги, необходимые для установки туннелей LAN to LAN с использованием общих ключей:

- Настройка **VPN tunnel properties,** включая общий ключ.
- Настройка **VPN tunnel properties.**
- Настройка **Route** в *главной (main)* таблице маршрутизации (или другой альтернативной таблице).
- Настройка **Rules** (двустороннему туннелю требуется 2 правила).

9.4.3. Удаленные клиенты

Сотрудник, который находится в командировке и которому требуется доступ к центральному корпоративному серверу с ноутбука из различных мест, является типичным примером удаленного клиента. Помимо необходимости защищенного VPN-доступа, другой основной вопрос заключается в том, что IP-адрес удаленного мобильного пользователя часто не известен заранее. Для управления неизвестным IP-адресом система NetDefendOS может динамически добавить маршруты в таблицу маршрутизации во время установки туннелей.

Неизвестные IP-адреса

Если IP-адрес клиента не известен заранее, то межсетевому экрану NetDefend необходимо динамически создать маршрут в таблице маршрутизации при подключении каждого клиента. Ниже отображается пример такой ситуации и динамическая маршрутизация внутри IPSec-туннеля.

Если клиентам разрешен удаленный доступ из любой точки, независимо от их IP-адреса, то для **Remote Network** необходимо установить значение **all-nets** (IP address: 0.0.0.0/0), что позволит всем существующим IPv4-адресам подключаться через туннель.

Как правило, при установке VPN-туннелей для удаленных клиентов, нет необходимости добавлять или изменять список предлагаемых алгоритмов, предварительно указанных в NetDefendOS.

Туннели на основе PSK

Следующий пример отображает установку туннеля с использованием PSK.

Пример 9.4. Установка VPN-туннеля с использованием PSK для удаленных клиентов

В данном примере рассматривается настройка IPsec-туннеля в главном офисе, где находится межсетевой экран NetDefend. Настройка выполняется для удаленных клиентов, подключенных к сети главного офиса, которым необходим удаленный доступ. Для сети главного офиса используется диапазон 10.0.1.0/24 с внешним IP-адресом межсетевого экрана wan_ip.

Web-интерфейс

A. Создайте общий ключ для аутентификации IPsec:

1. Зайдите **Objects > Authentication Objects > Add > Pre-Shared Key**

2. Далее введите:

• **Name**: Введите имя ключа, например, SecretKey

• **Shared Secret**: Введите секретную парольную фразу

• **Confirm Secret**: Введите повторно секретную парольную фразу

3. Нажмите **OK**

Б. Создайте IPsec-туннель:

1. Зайдите **Interfaces > IPsec > Add > IPsec Tunnel**

2. Далее введите:

• **Name**: RoamingIPsecTunnel

• **Local Network**: 10.0.1.0/24 (это локальная сеть, к которой будут подключены удаленные клиенты)

• **Remote Network**: all-nets

• **Remote Endpoint**: (None)

• **Encapsulation Mode**: Tunnel

3. Для Алгоритмов (Algorithms) введите:

• **IKE Algorithms**: Medium или High

• **IPsec Algorithms**: Medium или High

4. Для Аутентификации (Authentication) введите:

• **Pre-Shared Key**: Выберите общий ключ, сгенерированный ранее

5. На вкладке **Routing**:

• Включите опцию: **Dynamically add route to the remote network when a tunnel is established**.

6. Нажмите **OK**

В. В заключение укажите набор IP-правил, разрешающих прохождение трафика через туннель.

Туннели на основе самоподписанных сертификатов

Следующий пример отображает установку туннеля с использованием сертификата.

Пример 9.5. Установка VPN-туннеля с использованием самоподписанного сертификата для удаленных клиентов

В данном примере рассматривается настройка IPsec-туннеля в главном офисе, где находится межсетевой экран NetDefend. Настройка выполняется для удаленных клиентов, подключенных к сети главного офиса, которым необходим удаленный доступ. Для сети главного офиса используется диапазон 10.0.1.0/24 с внешним IP-адресом межсетевого экрана IP wan_ip.

Web-интерфейс

А. Создайте самоподписанный сертификат для аутентификации IPsec:

Создание самоподписанного сертификата выполняется через Web-интерфейс с помощью соответствующего программного обеспечения. Сертификат должен быть в формате PEM (Privacy Enhanced Mail).

Б. Загрузите все самоподписанные сертификаты клиента:

1. Зайдите **Objects > Authentication Objects > Add > Certificate**

2. Введите подходящее имя для объекта Сертификат

3. Выберите опцию **X.509 Certificate**

4. Нажмите **OK**

В. Создайте список идентификаторов:

1. Зайдите **Objects > VPN Objects > ID List > Add > ID List**

2. Введите подходящее **имя**, например, *sales*

3. Нажмите **OK**

4. Зайдите **Objects > VPN Objects > ID List > Sales > Add > ID**

5. Введите **имя** клиента

6. Выберите **Email** в качестве **Type**

7. В поле **Email address**, введите адрес электронной почты, выбранный при создании сертификата

8. Создайте новый идентификатор для каждого клиента, которому необходимо предоставить права доступа в соответствии с вышеуказанными инструкциями.

Г. Настройте IPsec-туннель:

1. Зайдите **Interfaces > IPsec > Add > IPsec Tunnel**

2. Далее введите:

• **Name**: RoamingIPsecTunnel

• **Local Network**: 10.0.1.0/24 (это локальная сеть, к которой будут подключены удаленные пользователи).

• **Remote Network**: all-nets

• **Remote Endpoint**: (None)

• **Encapsulation Mode**: Tunnel

3. Для Алгоритмов (Algorithms) введите:

• **IKE Algorithms**: Medium или High

• **IPsec Algorithms**: Medium или High

4. Для Аутентификации (Authentication) введите:

• Выберите **X.509 Certificate** в качестве метода аутентификации

• **Root Certificate(s)**: Выберите все сертификаты клиентов и добавьте их в список **Selected**

• **Gateway Certificate**: Выберите недавно созданный сертификат межсетевого экрана

• **Identification List**: Выберите список идентификаторов, которые необходимо ассоциировать с VPN-туннелем. В данном случае, это **sales**

5. На вкладке **Routing**:

• Включите опцию **Dynamically add route to the remote network when a tunnel is established**.

6. Нажмите **OK**

Д. В заключение укажите набор IP-правил, разрешающих прохождение трафика через туннель.

Туннели на основе сертификатов сервера CA

Настройка туннелей клиента с использованием сертификата, выпущенного CA, идентична настройке с использованием самоподписанных сертификатов, с различием в паре шагов.

За получение соответствующего сертификата ответственен администратор. Некоторые системы, например, сервер Windows 2000, поддерживают встроенный доступ к серверу CA (на сервере Windows 2000 он находится в **Certificate Services**). Для получения подробной информации о сертификатах, выпущенных на сервере CA, см. *Раздел 3.7, «Сертификаты»*.

Пример 9.6. Установка VPN-туннеля с использованием сертификата сервера CA для удаленных клиентов

В данном примере рассматривается настройка IPsec-туннеля в главном офисе, где находится межсетевой экран NetDefend. Настройка выполняется для удаленных клиентов, подключенных к сети главного офиса, которым необходим удаленный доступ. Для сети главного офиса используется диапазон 10.0.1.0/24 с внешним IP-адресом межсетевого экрана IP wan_ip.

Web-интерфейс

А. Загрузите все сертификаты клиентов:

1. Зайдите **Objects > Authentication Objects > Add > Certificate**

2. Введите подходящее имя для объекта Сертификат

3. Выберите опцию **X.509 Certificate**

4. Нажмите **OK**

Б. Создайте список идентификаторов:

1. Зайдите **Objects > VPN Objects > ID List > Add > ID List**

2. Введите описательное **имя**, например, *sales*

3. Нажмите **OK**

4. Зайдите **Objects > VPN Objects > ID List > Sales > Add > ID**

5. Введите **имя** клиента

6. Выберите **Email** в качестве **Type**

7. В поле **Email address**, введите адрес электронной почты, выбранный при создании сертификата на клиенте

8. Создайте новый идентификатор для каждого клиента, которому необходимо предоставить права доступа в соответствии с вышеуказанными инструкциями.

В. Настройте IPsec-туннель:

1. Зайдите **Interfaces > IPsec > Add > IPsec Tunnel**

2. Далее введите:

• **Name**: RoamingIPsecTunnel

• **Local Network**: 10.0.1.0/24 (это локальная сеть, к которой будут подключены удаленные пользователи).

• **Remote Network**: all-nets

• **Remote Endpoint**: (None)

• **Encapsulation Mode**: Tunnel

3. Для Алгоритмов (Algorithms) введите:

• **IKE Algorithms**: Medium или High

• **IPsec Algorithms**: Medium или High

4. Для Аутентификации (Authentication) введите:

• Выберите **X.509 Certificate** в качестве метода аутентификации

• **Root Certificate(s)**: Выберите корневые сертификаты сервера CA, импортированные ранее, и добавьте их в список **Selected**

• **Gateway Certificate**: Выберите недавно созданный сертификат межсетевого экрана

• **Identification List**: Выберите список идентификаторов, которые необходимо ассоциировать с VPN-туннелем. В данном случае, это **sales**

5. На вкладке **Routing**:

• Включите опцию **Dynamically add route to the remote network when a tunnel is established**.

6. Нажмите **OK**

Г. В заключение укажите набор IP-правил, разрешающих трафику проходить через туннель.

Режим настройки (Config Mode)

Режим настройки *IKE Configuration Mode* (Config Mode) – это расширение IKE, позволяющее системе NetDefendOS предоставлять удаленным клиентам информацию о настройках LAN. Используется для динамической настройки IPsec-клиентов с IP-адресами и соответствующими масками и для обмена другой информацией, связанной с DHCP. IP-адрес, назначенный клиенту, может быть в диапазоне предварительно указанных статических IP-адресов, определенных для режима настройки, а также может быть назначен DHCP-серверами, связанными с объектом *IP Pool*.

Пул IP-адресов – это кэш IP-адресов, собранных с DHCP-серверов. Аренда этих адресов продлевается автоматически после истечения указанного срока. Пулы IP-адресов управляют дополнительной информацией, такой как DNS и WINS / NBNS, так же как и обычный DHCP-сервер. (Для получения подробной информации о пулах см. *Раздел 5.4, «Пулы IP-адресов»*.)

Определение объекта Config Mode

В настоящее время в системе NetDefendOS можно определить только один объект Config Mode, который будет называться *Config Mode Pool*. Параметры ключа, связанного с объектом, следующие:

Use Predefined IP Pool Object	Объект Пул IP-адресов, предоставляющий IP-адреса.
Use a Static Pool	В качестве альтернативы пула IP-адресов используется набор статических IP-адресов.
DNS	IP-адрес DNS, используемый для URL (уже предоставленный пулом IP-адресов).
NBNS/WINS	IP-адрес для NBNS/WINS (уже предоставленный пулом IP-адресов).
DHCP	Инструктирует узел об отправке любых внешних DHCP-запросов на данный адрес.
Subnets	Список подсетей, к которым у клиента есть доступ.

Пример 9.7. Настройка Config Mode

В данном примере объект *Config Mode Pool* ассоциируется с уже заданным объектом *IP Pool*, который называется *ip_pool1*.

Web-интерфейс

1. Зайдите **Objects > VPN Objects > IKE Config Mode Pool**
2. Появится Web-страница со свойствами объекта Config Mode
3. Выберите **Use a predefined IPPool object**
4. Выберите объект *ip_pool1* из раскрывающегося меню **IP Pool**
5. Нажмите **OK**

После указания объекта Config Mode, включите Config Mode для применения к IPsec-туннелю.

Пример 9.8. Использование Config Mode с IPsec-туннелями

Принимая во внимание предварительно указанный туннель, названный *vpn_tunnel1*, данный пример отображает, как включить Config Mode для данного туннеля.

Web-интерфейс

- Зайдите **Interfaces > IPsec**
- Выберите туннель *vpn_tunnel1* для изменения
- Выберите **IKE Config Mode** в раскрывающемся списке
- Нажмите **OK**

Проверка IP-адреса

Система NetDefendOS всегда проверяет, совпадает ли IP-адрес источника каждого пакета внутри IPsec-туннеля с IP-адресом, назначенным IPsec-клиенту с IKE Config Mode. Если обнаружено несоответствие, пакет отбрасывается, и генерируется сообщение с уровнем важности Предупреждение (**Warning**). Это сообщение содержит два IP-адреса, а также идентификатор клиента.

Помимо этого, если не удалось выполнить проверку, несоответствующие SA могут быть автоматически удалены. Это выполняется с помощью включения расширенной настройки IPsecDeleteSAOnIPValidationFailure. По умолчанию для данной настройки установлено значение *Выключено*.

9.4.4. CRL, полученные от альтернативного LDAP-сервера

Как правило, корневой сертификат включает IP-адрес или имя узла Центра сертификации для взаимодействия, если необходимо загрузить сертификаты или CRL на межсетевой экран NetDefend. Для этих загрузок используется протокол *LDAP* (Lightweight Directory Access Protocol).

Тем не менее, в некоторых случаях эта информация отсутствует или администратор использует другой LDAP-сервер. Для того чтобы вручную указать альтернативные LDAP-серверы используйте раздел с настройками LDAP.

Пример 9.9. Настройка LDAP-сервера

В данном примере рассматривается установка LDAP-сервера вручную.

CLI

```
gw-world:/> add LDAPServer Host=192.168.101.146 Username=myusername
                        Password=mypassword Port=389
```

Web-интерфейс

1. Зайдите **Objects > VPN Objects > LDAP > Add > LDAP Server**

2. Далее введите:

• **IP Address**: 192.168.101.146

• **Username**: myusername

• **Password**: mypassword

• **Confirm Password**: mypassword

• **Port**: 389

3. Нажмите **OK**

9.4.5. Поиск и устранение неисправностей с помощью *ikesnoop*

Согласование VPN-туннеля

При настройке IPsec-туннелей могут возникнуть проблемы, например, не удается выполнить первоначальное согласование, так как устройства на противоположных сторонах VPN-туннеля не могут договориться о том, какие протоколы и методы шифрования использовать. Команда консоли *ikesnoop* с функцией *verbose* является инструментом, используемым для выявления причины проблемы, отображая детали согласования.

Использование *ikesnoop*

Команда ikesnoop вводится через консоль CLI или напрямую через консоль RS232.

Для запуска проверки используется следующая команда:

```
gw-world:/> ikesnoop -on -verbose
```

моаЭто означает, что исходящий ikesnoop будет отправлен в консоль для каждого IKE-согласования VPN-туннеля. Исходящие данные можно ограничить до одного IP-адреса, например, IP-адрес -10.1.1.10, используется следующая команда:

```
gw-world:/> ikesnoop -on 10.1.1.10 -verbose
```

ралИспользуемый IP-адрес – это IP-адрес удаленной конечной точки VPN-туннеля (либо IP-адрес удаленной конечной точки, либо IP-клиента). Для выключения функции мониторинга используется следующая команда:

```
gw-world:/> ikesnoop -off
```

ppp

Исходящие данные опции *verbose* могут оказаться сложными для восприятия администратора, который видит их в первый раз. Ниже представлены некоторые типичные исходящие данные *ikesnoop* с объясняющей аннотацией. Согласование туннеля выполняется на основе общих ключей. В данном разделе не обсуждается согласование на основе сертификатов, но используются те же принципы, что и в согласовании туннелей на основе общих ключей.

Подробная информация об опциях команды *ikesnoop* содержится в *Руководстве по интерфейсу командной строки CLI*.

Клиент и сервер

Две стороны, участвующие в процессе согласования туннеля, называются в данном разделе *клиент* и *сервер*. В данном контексте слово *«клиент»* обозначает устройство, которое является *инициатором* согласования, а *сервер* – это устройство, которое является *ответчиком*.

Шаг 1. Клиент инициирует обмен, отправляя список поддерживаемых алгоритмов

Исходящие данные функции *verbose* отображают список алгоритмов на выбор, которые клиент сначала отправляет на сервер. В списке отображаются поддерживаемые протоколы и методы шифрования. Основное назначение списка алгоритмов заключается в том, чтобы клиент обнаружил соответствующий набор протоколов/методов, поддерживаемых сервером. Сервер проверяет список и пытается найти комбинацию протоколов/методов, отправленных клиентом, который их поддерживает. Этот процесс является одним из основных в обмене IKE.

```
IkeSnoop: Received IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0

Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x00000000
Message ID    : 0x00000000
Packet length : 324 bytes
# payloads    : 8
Payloads:
  SA (Security Association)
    Payload data length : 152 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID               : ISAKMP
          SPI Size                  : 0
          Transform 1/4
            Transform ID            : IKE
            Encryption algorithm    : DES-cbc
            Hash algorithm          : MD5
            Authentication method   : Pre-Shared Key
            Group description       : MODP 1024
            Life type               : Seconds
            Life duration           : 43200
```

```
            Life type               : Kilobytes
            Life duration           : 50000
          Transform 2/4
            Transform ID            : IKE
            Encryption algorithm    : DES-cbc
            Hash algorithm          : SHA
            Authentication method   : Pre-Shared Key
            Group description       : MODP 1024
            Life type               : Seconds
            Life duration           : 43200
            Life type               : Kilobytes
            Life duration           : 50000
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 8f 9c c9 4e 01 24 8e cd f1 47 59 4c 28 4b 21 3b
     Description : SSH Communications Security QuickSec 2.1.0
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 27 ba b5 dc 01 ea 07 60 ea 4e 31 90 ac 27 c0 d0
     Description : draft-stenberg-ipsec-nat-traversal-01
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 61 05 c4 22 e7 68 47 e4 3f 96 84 80 12 92 ae cd
     Description : draft-stenberg-ipsec-nat-traversal-02
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 44 85 15 2d 18 b6 bb cd 0b e8 a8 46 95 79 dd cc
     Description : draft-ietf-ipsec-nat-t-ike-00
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
     Payload data length : 16 bytes
     Vendor ID   : 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     Description : draft-ietf-ipsec-nat-t-ike-03
```

Объяснение значений

Exchange type: Режим Main или Aggressive
Cookies: Случайное число для идентификации согласования
Encryption algorithm: Шифрование
Key length: Длина ключа
Hash algorithm: Хэш-алгоритм
Authentication method: Общий ключ или сертификат
Group description: Группа Diffie Hellman (DH)
Life type: Секунды или килобайты
Life duration: Количество секунд или килобайт
VID: Производитель программного обеспечения IPsec и поддерживаемые стандарты. Например, NAT-T

Шаг 2. Сервер отвечает клиенту

Типичный ответ сервера представлен ниже. Ответ может содержать предложение, идентичное одному из списка выше. Если сервер не обнаружил соответствие, то появляется сообщение «No proposal chosen» («Ничего не выбрано»), установка туннеля не выполняется и выходные данные команды *ikesnoop* остаются на этом уровне.

```
IkeSnoop: Sending IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0

Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
```

```
Message ID    : 0x00000000
Packet length : 224 bytes
# payloads    : 8
Payloads:
  SA (Security Association)
    Payload data length : 52 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID               : ISAKMP
          SPI Size                  : 0
          Transform 1/1
            Transform ID            : IKE
            Encryption algorithm    : DES
            Key length              : 56
            Hash algorithm          : MD5
            Authentication method   : Pre-Shared Key
            Group description       : MODP 1024
            Life type               : Seconds
            Life duration           : 43200
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 8f 9c c9 4e 01 24 8e cd f1 47 59 4c 28 4b 21 3b
    Description : SSH Communications Security QuickSec 2.1.0
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 27 ba b5 dc 01 ea 07 60 ea 4e 31 90 ac 27 c0 d0
    Description : draft-stenberg-ipsec-nat-traversal-01
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 61 05 c4 22 e7 68 47 e4 3f 96 84 80 12 92 ae cd
    Description : draft-stenberg-ipsec-nat-traversal-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 44 85 15 2d 18 b6 bb cd 0b e8 a8 46 95 79 dd cc
    Description : draft-ietf-ipsec-nat-t-ike-00
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
    Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
    Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID   : 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
    Description : draft-ietf-ipsec-nat-t-ike-03
```

Шаг 3. Клиент начинает обмен ключами

Сервер принимает предложение на этом уровне, и клиент начинает обмен ключами. Помимо этого, используются механизмы обнаружения NAT detection payloads, чтобы выяснить, используется ли NAT.

```
IkeSnoop: Received IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0

Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 220 bytes
# payloads    : 4
Payloads:
  KE (Key Exchange)
    Payload data length : 128 bytes
  NONCE (Nonce)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
```

Шаг 4. Сервер отправляет данные об обмене ключами

Сервер отправляет данные об обмене ключами обратно клиенту.

```
IkeSnoop: Sending IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0

Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 220 bytes
# payloads    : 4
Payloads:
  KE (Key Exchange)
    Payload data length : 128 bytes
  NONCE (Nonce)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
```

Шаг 5. Клиент отправляет идентификатор

Инициатор отправляет идентификатор, который, как правило, представляет собой IP-адрес или *Альтернативное имя субъекта*, если используются сертификаты.

```
IkeSnoop: Received IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0

Flags         : E(encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 72 bytes
# payloads    : 3
Payloads:
  ID (Identification)
    Payload data length : 8 bytes
    ID : ipv4(any:0,[0..3]=192.168.0.10)
  HASH (Hash)
    Payload data length : 16 bytes
  N (Notification)
    Payload data length : 8 bytes
    Protocol ID  : ISAKMP
    Notification : Initial contact
```

Объяснение значений

Flags: E означает encryption (шифрование) (используется только этот флаг).
ID: Идентификатор клиента

Поле *Notification* предоставлено в качестве *Initial Contact*, чтобы идентифицировать, что ключ не является повторно выданным.

Шаг 6. Сервер отправляет идентификатор в качестве ответа

Сервер отправляет свой идентификатор.

```
IkeSnoop: Sending IKE packet from 192.168.0.10:500 Exchange type :
       Identity Protection (main mode) ISAKMP Version : 1.0
```

```
Flags         : E(encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 60 bytes
# payloads    : 2
Payloads:
 ID (Identification)
   Payload data length : 8 bytes
   ID : ipv4(any:0,[0..3]=192.168.0.20)
 HASH (Hash)
   Payload data length : 16 bytes
```

Шаг 7. Клиент отправляет Список поддерживаемых алгоритмов IPsec

Клиент отправляет список поддерживаемых алгоритмов IPsec серверу. Список также содержит узел/сети, разрешенные в туннеле.

```
IkeSnoop: Received IKE packet from 192.168.0.10:500 Exchange type :
       Quick mode ISAKMP Version : 1.0

Flags         : E(encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 264 bytes
# payloads    : 5
Payloads:
 HASH (Hash)
   Payload data length : 16 bytes
 SA (Security Association)
   Payload data length : 164 bytes
   DOI : 1 (IPsec DOI)
     Proposal 1/1
       Protocol 1/1
         Protocol ID
         Protocol ID               : ESP
         SPI Size                  : 4
           SPI Value               : 0x4c83cad2
         Transform 1/4
           Transform ID            : DES
           Key length              : 128
           Authentication algorithm : HMAC-MD5
           SA life type            : Seconds
           SA life duration        : 21600
           SA life type            : Kilobytes
           SA life duration        : 50000
           Encapsulation mode      : Tunnel
 NONCE (Nonce)
   Payload data length : 16 bytes
 ID (Identification)
   Payload data length : 8 bytes
   ID : ipv4(any:0,[0..3]=10.4.2.6)
 ID (Identification)
   Payload data length : 12 bytes
   ID : ipv4_subnet(any:0,[0..7]=10.4.0.0/16)
```

Объяснение значений

Transform ID: Шифрование
Key length: Длина ключа шифрования
Authentication algorithm: HMAC (Хэш)
Group description: PFS и группа PFS
SA life type: Секунды или килобайты
SA life duration: Количество секунд или килобайт
Encapsulation mode: может использоваться transport, tunnel или UDP tunnel (NAT-T)
ID: ipv4(любой:0,[0..3]=10.4.2.6)

Здесь первый идентификатор – идентификатор локальной сети туннеля с точки зрения клиента, а второй идентификатор – идентификатор удаленной сети. Если есть какая-либо сетевая маска, как правило, SA на сеть и в противном случае – SA на узел.

Шаг 8. Клиент отправляет Список поддерживаемых алгоритмов

Сервер отправляет ответ в виде соответствующий IPsec-протокол из списка, отправленного клиентом. Как указано в шаге 2 выше, если сервер не обнаружил соответствия, то появляется сообщение «No proposal chosen», установка туннеля не выполняется и выходные данные команды *ikesnoop* остаются на этом уровне.

```
IkeSnoop: Sending IKE packet from 192.168.0.10:500 Exchange type :
       Quick mode ISAKMP Version : 1.0

Flags         : E(encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 156 bytes
# payloads    : 5
Payloads:
 HASH (Hash)
 Payload data length : 16 bytes
 SA (Security Association)
   Payload data length : 56 bytes
   DOI : 1 (IPsec DOI)
     Proposal 1/1
      Protocol 1/1
        Protocol ID               : ESP
        SPI Size                  : 4
          SPI Value               : 0xafba2d15
        Transform 1/1
          Transform ID             : DES
          Key length               : 128
          Authentication algorithm : HMAC-MD5
          SA life type             : Seconds
          SA life duration         : 21600
          SA life type             : Kilobytes
          SA life duration         : 50000
          Encapsulation mode       : Tunnel
 NONCE (Nonce)
   Payload data length : 16 bytes
 ID (Identification)
   Payload data length : 8 bytes
   ID : ipv4(any:0,[0..3]=10.4.2.6)
 ID (Identification)
   Payload data length : 12 bytes
   ID : ipv4_subnet(any:0,[0..7]=10.4.0.0/16)
```

Шаг 9. Клиент подтверждает установку туннеля

Данным последним сообщением является сообщение от клиента, информирующее, что туннель установлен и работает. Все обмены между клиентом/сервером прошли успешно.

```
IkeSnoop: Received IKE packet from 192.168.0.10:500 Exchange type :
       Quick mode ISAKMP Version : 1.0
Flags         : E(encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 48 bytes
# payloads    : 1
Payloads:
 HASH (Hash)
   Payload data length : 16 bytes
```

9.4.6. Расширенные настройки IPsec

Для настройки IPsec-туннелей доступны следующие настройки.

IPsec Max Rules

С помощью данной настройки можно указать количество IP-правил для подключения к IPsec-

туннелям. По умолчанию это приблизительно 4 лицензированных **IPsecMaxTunnels** и системная память, выделенная для этого при запуске. При уменьшении количества правил, требования к памяти также уменьшаются, однако, не рекомендуется вносить данное изменение.

Сброс правил **IPsec Max Rules** происходит автоматически до 4 **IPsec Max Tunnels**, если последнее изменено. Это происходит с момента изменения **IPsec Max Rules** вручную, таким образом, последующие изменения **IPsec Max Tunnels** не приведут к автоматическому изменению в **IPsec Max Rules**.

По умолчанию: *4 лицензированных IPsec Max Tunnels*

IPsec Max Tunnels

С помощью данной настройки можно указать количество разрешенных IPsec-туннелей. Первоначально данное значение извлекается из максимального количества туннелей, разрешенных лицензией. NetDefendOS использует настройку, чтобы выделить память для IPsec. Если для IPsec необходимо выделить меньше памяти, то можно уменьшить значение в данной настройке. Значение не должно превышать ограничение лицензии.

Предупреждающее сообщение, регистрируемое в журнале, генерируется автоматически при достижении 90% значения данной настройки.

По умолчанию: *Ограничение определено лицензией*

IKE Send Initial Contact

С помощью данной настройки IKE отправляет сообщение-уведомление «Initial contact». Данное сообщение будет отправлено на каждую удаленную конечную точку при открытии с ней соединения и отсутствия предварительно указанной IPsec SA.

По умолчанию: *Включено*

IKE Send CRLs

С помощью данной настройки можно отправлять списки CRL (Certificate Revocation Lists) как часть обмена IKE. Как правило, следует установить ENABLE, за исключением тех случаев, когда удаленный узел не принимает полезные нагрузки CRL.

Помните, что для применения данной настройки необходим перезапуск.

По умолчанию: *Включено*

IPsec Before Rules

Передача трафика IKE и IPsec (ESP/AH), отправленного напрямую в NetDefendOS, на компьютер IPsec без выполнения проверки в соответствии с набором правил.

По умолчанию: *Включено*

IKE CRL Validity Time

CRL содержит поле «next update», позволяющее установить дату и время, когда новый CRL будет доступен для загрузки с CA. Время между обновлениями CRL может быть различным, от нескольких часов и более, в зависимости от настройки CA. Большинство программного обеспечения CA позволяет администратору выдавать новые CRL в любое время, таким образом, даже если поле «next update» информирует, что новый CRL доступен только через 12 часов, возможно уже существует CRL для загрузки.

Данная настройка ограничивает время действия CRL. Новый CRL загружается по истечении времени

IKECRLVailityTime или когда наступает время «next update», вне зависимости от того, что произойдет раньше.

По умолчанию: *86400* секунд

IKE Max CA Path

После проверки сигнатуры сертификата пользователя, система NetDefendOS выполняет поиск поля *issuer name* в сертификате пользователя для того, чтобы найти CA, который подписал сертификат. Сертификат CA, в свою очередь, может быть подписан другим центром организацией CA, который подписан другим CA, и т.д. Каждый сертификат будет проверен, пока не будет найден сертификат с пометкой «доверенный» (trusted) или пока не будет установлено, что ни один из сертификатов не является доверенным.

Если в данном случае обнаружено больше сертификатов, чем определено настройкой, сертификат пользователя будет рассматриваться как недействующий.

По умолчанию: *15*

IPsec Cert Cache Max Certs

Максимальное количество сертификатов/CRL, допустимых во внутреннем кэше сертификатов. Когда кэш полон, записи будут удалены в соответствии с алгоритмом LRU (Least Recently Used).

По умолчанию: *1024*

IPsec Gateway Name Cache Time

Максимальное количество сертификатов/CRL, допустимых во внутреннем кэше сертификатов. Когда кэш полон, записи будут удалены в соответствии с алгоритмом LRU (Least Recently Used).

По умолчанию: *1024*

DPD Metric

Количество времени в десятках секунд, указывающее на срок действия (доступность) узла с момента получения последнего сообщения IKE. Это означает, что DPD-сообщения для проверки срока действия узла будут отправлены в течение этого времени, хотя никаких пакетов от узла не было получено.

Другими словами, количество времени (в десятках секунд) отсутствия трафика в туннеле или любой другой признак работоспособности прежде, чем узел будет считаться недействующим. Если необходим запуск DPD, но присутствуют другие признаки работоспособности (например, IKE пакеты с противоположной точки туннеля) в течение заданного интервала времени, сообщения *DPD-R-U-TAM* не будут отправлены.

По умолчанию: *3* (другими словами, 3 x 10 = 30 секунд)

DPD Keep Time

Количество времени в десятках секунд, указывающее на то, что узел является недействующим после его обнаружения системой NetDefendOS. Если узел является недействующим, система NetDefendOS не пытается повторно установить туннель или отправить DPD-сообщения на узел. Тем не менее, узел не будет считаться недействующим после получения от него пакета.

Другими словами, это количество времени в десятках секунд, в течение которого SA будет оставаться в недействующем кэше после удаления. SA помещается в недействующий кэш, если противоположная сторона туннеля не ответила на сообщения *DPD-RU-THERE* для *DPD Expire Time* x

10 секунд, а также нет других признаков работоспособности. Когда SA помещается в недействующий кэш, NetDefendOS не будет пытаться повторно установить туннель. Если получен трафик, связанный с SA в недействующем кэше, SA будет удален из недействующего кэша. DPD не сработает, если SA уже сохранен в недействующем кэше.

Данная настройка используется только с IKEv1.

По умолчанию: *2* (другими словами, 2 x 10 = 20 секунд)

DPD Expired Time

Количество времени в секундах, в течение которого на узел будут отправлены DPD-сообщения. Если узел не отвечает на сообщения в течение этого времени, он считается недействующим.

Другими словами, это количество времени в секундах, в течение которого отправляются сообщения *DPD-R-U-THERE*. Если противоположная точка туннеля не отправила ответ на любое сообщение, она считается недействующей (недоступной). SA помещается в недействующий кэш.

Настройка используется только с IKEv1.

По умолчанию: *15 секунд*

9.5. PPTP/L2TP

Доступ клиента, использующего модемное соединение (dial-up), возможно, с неизвестным IP-адресом, к защищенным сетям через VPN создает ряд определенных проблем. Оба протокола PPTP и L2TP предоставляют два различных способа получения удаленного VPN-доступа. Относительно данного сценария наиболее часто используется способность NetDefendOS выступать в качестве PPTP или L2TP-сервера, два раздела ниже содержат информацию об этой функции. Третий раздел посвящен способности системы NetDefendOS действовать в качестве PPTP или L2TP-клиента.

Быстрый запуск PPTP/L2TP

В данном разделе представлена подробная информация о протоколах L2TP и PPTP. Список шагов по быстрому запуску этих протоколов можно найти в следующих разделах:

Раздел 9.2.5, «Подключение клиентов к L2TP- туннелю с использованием общих ключей»

Раздел 9.2.6, «Подключение клиентов к L2TP-туннелю с использованием сертификатов»

Раздел 9.2.7, «Подключение клиентов к PPTP-туннелю»

9.5.1 PPTP-серверы

Обзор

PPTP-протокол (Point to Point Tunneling Protocol) разработан Форумом PPTP – союзом компаний, включая Microsoft. Это протокол уровня 2 OSI «data-link» (см. *Приложение Г, «Основы построения OSI»*) и расширенный *PPP*-протокол (Point to Point Protocol), используемый для коммутируемого доступа в Интернет (dial-up). Это один из первых протоколов, разработанных для предоставления VPN-доступа к удаленным серверам по сети dial-up, который широко используется в настоящее время.

Использование

PPTP-протокол используется в контексте VPN для туннелирования различных протоколов в сети

Интернет. Туннелирование выполняется за счет инкапсуляции PPP-пакетов с помощью *Generic Routing Encapsulation* (GRE - IP-протокол 47). Сначала клиент устанавливает соединение с провайдером обычным способом с помощью PPP-протокола и далее устанавливает TCP/IP-соединение через Интернет к межсетевому экрану NetDefend, который действует в качестве PPTP-сервера (используется TCP-порт 1723). Провайдер не осведомлен о VPN, так как туннель идет от PPTP-сервера к клиенту. Стандарт PPTP не определяет способ шифрования данных. Как правило, шифрование выполняется с помощью стандарта *Microsoft Point-to-Point Encryption* (MPPE).

Применение

PPTP-протокол является удобным и простым в использовании решением, обеспечивающим доступ клиентам. PPTP-протоколу не требуется инфраструктура сертификата, находящегося в L2TP, но вместо этого используется последовательность имя пользователя /пароль для установки доверия между клиентом и сервером. Уровень безопасности, предлагаемый не на основе сертификата, возможно, является единственным недостатком PPTP. Так как PPTP-протокол не использует IPsec, PPTP-соединения могут быть преобразованы с помощью технологии NAT и NAT traversal не требуется. Компания Microsoft включает PPTP в состав своих операционных систем, начиная с Windows 95 и, следовательно, существует большое количество клиентов с уже установленным программным обеспечением.

Поиск и устранение неисправностей PPTP

Основной проблемой при настройке PPTP-протокола является то, что маршрутизатор и/или коммутатор в сети блокирует TCP-порт 1723 и/или IP-протокол 47 перед установкой PPTP-соединения с межсетевым экраном NetDefend. При проверке журнала можно выявить проблему, появится сообщение следующего вида:

```
Error PPP lcp_negotiation_stalled ppp_terminated
```

Пример 9.10. Настройка PPTP-сервера

В данном примере рассматривается процесс настройки сетевого PPTP-сервера. Предполагается, что в адресной книге уже созданы некоторые объекты адресов.

Пользователю необходимо определить IP-адрес интерфейса PPTP-сервера, внешний IP-адрес (который необходимо прослушивать PPTP-серверу) и пул IP-адресов, который будет использовать PPTP-сервер для назначения IP-адресов клиентам.

CLI

```
gw-world:/> add Interface L2TPServer MyPPTPServer
                        ServerIP=lan_ip Interface=any
                        IP=wan_ip IPPool=pp2p_Pool
                        TunnelProtocol=PPTP
                        AllowedRoutes=all-nets
```

Web-интерфейс

1. Зайдите **Interfaces > PPTP/L2TP Servers > Add > PPTP/L2TP Server**

2. Введите имя PPTP-сервера, например, *MyPPTPServer*

3. Далее введите:

• **Inner IP Address:** lan_ip

• **Tunnel Protocol:** PPTP

• **Outer Interface Filter:** any

• **Outer Server IP:** wan_ip

4. На вкладке **PPP Parameters** выберите **pptp_Pool** в настройках **IP Pool**

5. На вкладке **Add Route**, выберите **all_nets** из **Allowed Networks**

6. Нажмите **OK**

Функция **Use User Authentication Rules** (Использовать Правила аутентификации пользователя) включена по умолчанию. Для аутентификации пользователей с использованием PPTP-туннеля необходимо настроить правила аутентификации, которые не представлены в данном примере.

9.5.2. L2TP-серверы

L2TP-протокол (Layer 2 Tunneling Protocol) – это открытый стандарт IETF, решающий множество проблем PPTP. Он представляет собой комбинацию *L2F-протокола* (Layer 2 Forwarding) и PPTP-протокола, с использованием наиболее полезных функций обоих протоколов. Так как стандарт L2TP не выполняет шифрование, эту функцию, как правило, выполняет IETF, известный как L2TP/IPsec, в котором L2TP-пакеты инкапсулируются по протоколу IPsec.

Клиент обменивается данными с *LAC* (Local Access Concentrator) и LAC обменивается информацией через Интернет с *LNS-сервером* (L2TP Network Server). Межсетевой экран действует в качестве LNS-сервера. LAC туннелирует данные, например, PPP, используя IPsec в сети Интернет. В большинстве случаев клиент действует в качестве LAC.

L2TP-протокол основан на сертификате, благодаря чему он упрощает управление большим количеством клиентов и обеспечивает более высокий уровень безопасности, чем PPTP-протокол. При использовании L2TP, в отличие от PPTP, можно организовать несколько виртуальных сетей через один туннель. Так как протокол L2TP основан на IPsec, ему требуется NAT traversal (NAT-T) на стороне LNS.

Пример 9.11. Настройка L2TP-сервера

В данном примере рассматривается процесс настройки L2TP-сервера. Предполагается, что уже созданы некоторые объекты IP-адресов. Пользователю необходимо указать IP-адрес интерфейса L2TP-сервера, внешний IP-адрес (который необходимо прослушивать L2TP-серверу) и пул IP-адресов, который будет использовать L2TP-сервер для назначения IP-адресов клиентам.

CLI

```
gw-world:/> add Interface L2TPServer MyL2TPServer ServerIP=ip_l2tp
                        Interface=any IP=wan_ip
                        IPPool=L2TP_Pool TunnelProtocol=L2TP
                        AllowedRoutes=all-nets
```

Web-интерфейс

1. Зайдите **Interfaces > L2TP Servers > Add > L2TPServer**

2. Введите имя L2TP-сервера, например, *MyL2TPServer*

3. Далее введите:

• **Inner IP Address:** ip_l2tp

• **Tunnel Protocol:** L2TP

• **Outer Interface Filter:** any

• **Outer Server IP:** wan_ip

4. На вкладке **PPP Parameters** выберите **L2TP_Pool** в настройках **IP Pool**

5. На вкладке **Add Route** tab, выберите **all_nets** из **Allowed Networks**

6. Нажмите **OK**

Функция **Use User Authentication Rules** (Использовать Правила аутентификации пользователя) включена по умолчанию. Для аутентификации пользователей при использовании PPTP необходимо указать правила

аутентификации, которые не представлены в данном примере.

Пример 9.12. Настройка L2TP over IPsec

В данном примере рассматривается процесс настройки L2TP-туннеля на основе IPsec-шифрования, а также основы настройки VPN. Перед запуском необходимо указать некоторые объекты адресов, например, адрес, назначаемый L2TP-клиентам. Требуются списки с предлагаемыми вариантами и общий ключ PSK. В данном случае используются объекты, созданные в предыдущих примерах.

Для аутентификации пользователей при использовании L2TP-туннелей применяется локальная база данных пользователя.

А. Начните с подготовки локальной базы данных пользователя:

CLI

```
gw-world:/> add LocalUserDatabase UserDB

gw-world:/> cc LocalUserDatabase UserDB

gw-world:/> add User testuser Password=mypassword
```

Web-интерфейс

1. Зайдите **User Authentication > Local User Databases > Add > Local User Database**

2. Введите имя базы данных пользователя, например, *UserDB*

3. Зайдите **User Authentication > Local User Databases > UserDB > Add > User**

4. Далее введите:

• **Username:** testuser

• **Password:** mypassword

• **Confirm Password:** mypassword

5. Нажмите **OK**

Далее выполняется установка IPsec-туннеля, который позднее будет использоваться в разделе L2TP. Так как мы намерены использовать L2TP, у локальной сети тот же IP-адрес, что и у L2TP-туннеля, wan_ip. Более того, для IPsec- необходимо настроить динамическое добавление маршрутов в удаленную сеть после установки туннеля.

Б. Продолжение установки IPsec-туннеля

CLI

```
gw-world:/> add Interface IPsecTunnel l2tp_ipsec LocalNetwork=wan_ip
                      RemoteNetwork=all-nets IKEAlgorithms=Medium
                      IPsecAlgorithms=esp-l2tptunnel
                      PSK=MyPSK EncapsulationMode=Transport
                      DHCPOverIPsec=Yes AddRouteToRemoteNet=Yes
                      IPsecLifeTimeKilobytes=250000
                      IPsecLifeTimeSeconds=3600
```

Web-интерфейс

1. Зайдите **Interfaces > IPsec > Add > IPsec Tunnel**

2. Введите имя IPsec-туннеля, например, *l2tp_ipsec*

3. Далее введите:

   а. **Local Network:** wan_ip

   б. **Remote Network:** all-nets

   в. **Remote Endpoint:** none

г. **Encapsulation Mode:** Transport

д. **IKE Algorithms:** High

е. **IPsec Algorithms:** esp-l2tptunnel

4. Введите *3600* в настройке **IPsec Life Time seconds**

5. Введите 250000 в настройке **IPsec Life Time kilobytes**

6. На вкладке **Authentication**, выберите **Pre-shared Key**

7. Выберите **MyPSK** в настройке **Pre-shared Key**

8. На вкладке **Routing**, отметьте следующее:

• **Allow DHCP over IPsec from single-host clients**

• **Dynamically add route to the remote network when a tunnel is established**

9. Нажмите **OK**

Далее выполняется установка L2TP-сервера. Внутренний IP-адрес должен относиться к сети, из которой клиентам были назначены IP-адреса, lan_ip. Внешний интерфейс - это интерфейс, на котором L2TP-сервер будет принимать соединения, l2tp_ipsec. Также для IP, используемых L2TP-клиентами, необходимо настроить ProxyARP.

В. Установка L2TP-туннеля

CLI

```
gw-world:/> add Interface L2TPServer l2tp_tunnel IP=lan_ip
                      Interface=l2tp_ipsec ServerIP=wan_ip
                      IPPool=l2tp_pool TunnelProtocol=L2TP
                      AllowedRoutes=all-nets
                      ProxyARPInterfaces=lan
```

Web-интерфейс

1. Зайдите **Interfaces > L2TP Servers > Add > L2TPServer**

2. Введите имя L2TP-туннеля, например, *l2tp_ipsec*

3. Далее введите:

• **Inner IP Address:** lan_ip

• **Tunnel Protocol:** L2TP

• **Outer Interface Filter:** l2tp_ipsec

• **Server IP:** wan_ip

4. На вкладке **PPP Parameters** отметьте **Use User Authentication Rules**

5. Выберите **l2tp_pool** в настройке **IP Pool**

6. На вкладке **Add Route** выберите **all-nets** в **Allowed Networks**

7. На вкладке **Add Route** выберите **all-nets** в **Allowed Networks**

8. Нажмите **OK**

Для аутентификации пользователей при использовании L2TP-туннеля необходимо настроить правило аутентификации.

Г. Установка L2TP-туннеля

CLI

```
gw-world:/> add Interface L2TPServer l2tp_tunnel IP=lan_ip
                      Interface=l2tp_ipsec ServerIP=wan_ip
                      IPPool=l2tp_pool TunnelProtocol=L2TP
                      AllowedRoutes=all-nets
                      ProxyARPInterfaces=lan
```

Web-интерфейс

1. Зайдите **User Authentication > User Authentication Rules > Add > UserAuthRule**

2. Введите имя правила, например, *L2TP_Auth*

3. Далее введите:

• **Agent:** PPP

• **Authentication Source:** Local

• **Interface:** l2tp_tunnel

• **Originator IP:** all-nets

• **Terminator IP:** wan_ip

4. На вкладке **Authentication Options** введите *UserDB* в качестве **Local User DB**

5. Нажмите **OK**

После выполнения основных действий остается добавить правила. Для того чтобы разрешить прохождение трафика из туннеля, необходимо добавить два правила.

Д. В завершение добавьте правила:

CLI

Сначала измените текущую категорию на *main* (основной) набор IP-правил:

```
gw-world:/> cc IPRuleSet main
```

Далее добавьте IP-правила:

```
gw-world:/> add IPRule action=Allow Service=all_services
                    SourceInterface=l2tp_tunnel
                    SourceNetwork=l2tp_pool
                    DestinationInterface=any
                    DestinationNetwork=all-nets
                    name=AllowL2TP

gw-world:/> add IPRule action=NAT Service=all_services
                    SourceInterface=l2tp_tunnel
                    SourceNetwork=l2tp_pool
                    DestinationInterface=any
                    DestinationNetwork=all-nets
                    name=NATL2TP
```

Web-интерфейс

1. Зайдите **Rules > IP Rules > Add > IPRule**

2. Введите имя правила, например, *AllowL2TP*

3. Далее введите:

• **Action:** Allow

• **Service:** all_services

• **Source Interface:** l2tp_tunnel

• **Source Network:** l2tp_pool

• **Destination Interface:** any

• **Destination Network:** all-nets

4. Нажмите **OK**

5. Зайдите **Rules > IP Rules > Add > IPRule**

6. Введите имя правила, например, *NATL2TP*

7. Далее введите:

• **Action:** NAT

• **Service:** all_services

• **Source Interface:** l2tp_tunnel

• **Source Network:** l2tp_pool

• **Destination Interface:** any

• **Destination Network:** all-nets

8. Нажмите **OK**

9.5.3. Расширенные настройки L2TP/PPTP-сервера

Администратору доступны следующие расширенные настройки L2TP/PPTP-сервера:

L2TP Before Rules

С помощью данной настройки выполняется передача L2TP-трафика, отправленного на межсетевой экран NetDefend, непосредственно на L2TP-сервер, не сверяясь с набором правил.

По умолчанию: *Включено*

PPTP Before Rules

Передача PPTP-трафика, отправленного на межсетевой экран NetDefend, непосредственно на PPTP-сервер, не сверяясь с набором правил.

Default: *Включено*

Max PPP Resends

Максимальное число попыток повторной передачи PPP.

По умолчанию: *10*

9.5.4. L2TP/PPTP-клиенты

Описание протоколов PPTP и L2TP представлено в предыдущем разделе. Помимо способности действовать в качестве PPTP или L2TP-сервера, NetDefendOS также предоставляет возможность действовать как PPTP или L2TP-клиент. Это может быть полезно, если в качестве VPN-протокола вместо IPsec используются PPTP или L2TP. Один межсетевой экран NetDefend может действовать в качестве клиента и подключаться к другому устройству, которое действует в качестве сервера.

Настройка клиента

У PPTP и L2TP общий подход к настройке клиента с помощью следующих настроек:

Основные параметры

- **Name** – Имя клиента
- **Interface Type** – Определяет тип клиента: PPTP или L2TP

- **Remote Endpoint** – IP-адрес удаленной конечной точки. Если указан URL, префикс *dns:* должен стоять перед ним.

Имена назначаемых адресов

При подключении через PPTP и L2TP назначаются динамические IP-адреса с использованием *PPP LCP*-протокола. Полученная системой NetDefendOS информация хранится в символичных именах узла/сети. Для этого используются следующие настройки:

- **Inner IP Address** – Имя узла, используемое для хранения назначенного IP-адреса. Если данный сетевой объект существует и не имеет значение 0.0.0.0, то PPTP/L2TP-клиент попытается получить его с PPTP/L2TP-сервера как предпочтительный IP-адрес.

- **Automatically pick name** – Если данная опция включена, то система NetDefendOS создает имя узла на основе имени PPTP/L2TP-интерфейса, например, *ip_PPTPTunnel1*.

- **Primary/Secondary DNS Name –** Указывает DNS-серверы из списка предварительно указанных сетевых объектов.

Примечание: Маршрут по умолчанию при использовании протоколов PPTP/L2TP

PPTP/L2TP-сервер не предоставляет такую информацию, как шлюз или адреса широковещательной рассылки, так как не используется с PPTP/L2TP-туннелями. При использовании PPTP/L2TP маршрут по умолчанию, как правило, направлен напрямую через PPTP/L2TP-туннель без определенного шлюза.

Аутентификация

- **Username** – Имя пользователя, используемое для данного PPTP/L2TP-интерфейса
- **Password** – Пароль для интерфейса
- **Authentication** – Укажите, какой протокол использовать для аутентификации.
- **MPPE** – Укажите уровень шифрования с использованием протоколов *MPPE* (Microsoft Point-to-Point Encryption).

Если включена функция **Dial On Demand**, то PPTP/L2TP-туннель не будет установлен, пока трафик не отправлен на интерфейс. Параметры для опции:

- **Activity Sense –** С помощью данного параметра можно запустить функцию Dial-on-demand для **Send** или **Recv,** или для обоих.
- **Idle Timeout** – Время неактивности (в секундах) перед разъединением.

Использование PPTP-клиента

Использование функции PPTP-клиента отображено в сценарии ниже.

В данном случае представлено количество клиентов, преобразованных с помощью технологии NAT через межсетевой экран NetDefendOS перед подключением к PPTP-серверу на противоположной точке межсетевого экрана NetDefend. Если в качестве PPTP-клиента действует более одного клиента, который пытается подключиться к PPTP-серверу, то сервер не будет действовать по причине использования технологии NAT.

Существует только один способ преобразования с помощью NAT нескольких PPTP-клиентов – межсетевой экран действует в качестве PPTP-клиента при подключении к PPTP-серверу. Подведем итоги по настройке:

- PPTP-туннель установлен между системой NetDefendOS и сервером.

- Маршрут добавлен в таблицу маршрутизации в NetDefendOS, которая определяет, что трафик для сервера должен быть смаршрутизирован через PPTP-туннель.

Д

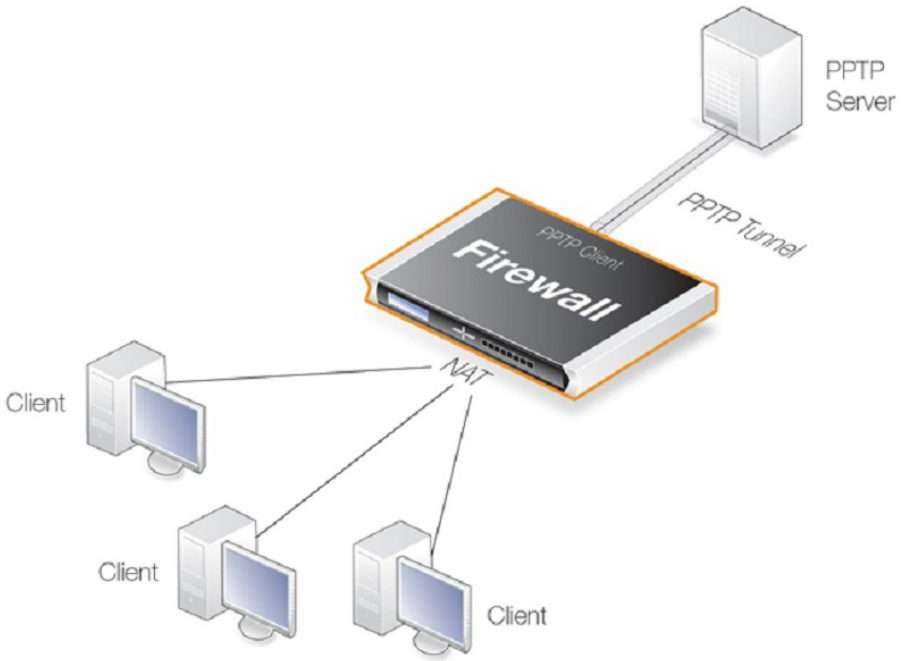


Рис. 9.3. Использование PPTP-клиента

9.6. Доступ к серверу CA

Описание

При использовании сертификатов две противоположных точки VPN-туннеля обмениваются своими сертификатами во время согласования установки туннеля, и каждая из них может попытаться проверить полученный сертификат с помощью доступа к *серверу CA*. Сертификат содержит URL (*CRL Distribution Point*), который определяет проверку сервера CA, и доступ к серверу осуществляется с использованием запроса HTTP *GET* с ответом HTTP. (Более корректно назвать этот URL-адрес FQDN - *Fully Qualified Domain Name*.)

Типы серверов CA

Существует два типа серверов CA:

- Коммерческий сервер CA, управляемый одной из коммерческих компаний, выпускающих сертификаты. Доступны в сети Интернет и их FQDN также доступны через DNS-сервер.

- Приватный сервер CA, управляемый той же организацией, которая устанавливает VPN-туннели. IP-адрес приватного сервера неизвестен публичной DNS-системе до тех пор, пока не будет зарегистрирован. Адрес также не будет известен внутренней сети до тех пор, пока не будет зарегистрирован на внутреннем DNS-сервере.

Принципы доступа

Для успешного доступа к серверу CA необходимо учитывать следующее:

- Каждая сторона VPN-туннеля может отправлять запрос проверки на сервер CA.

- Для отправки запроса проверки сертификата сначала необходимо преобразовать FQDN сертификата сервера CA в IP-адрес. Возможны следующие сценарии:

1. Сервер CA – это приватный сервер позади межсетевого экрана NetDefend, туннели установлены через Интернет, но к тем клиентам, которые не будут пытаться проверить сертификат, отправленный системой NetDefendOS.

В этом случае необходимо зарегистрировать IP-адрес приватного сервера на приватном DNS-сервере, таким образом, FQDN может быть преобразован. Данный приватный DNS-сервер также необходимо настроить в системе NetDefendOS таким образом, чтобы можно было определить его местоположение, когда система NetDefendOS отправит запрос на проверку.

2. Сервер CA – это приватный сервер с туннелями, установленными через сеть Интернет и клиентами, которые попытаются проверить сертификат, полученный от NetDefendOS. В этом случае необходимо выполнить следующее:

а. Необходимо настроить приватный DNS-сервер таким образом, чтобы NetDefendOS могла определить местоположение приватного сервера CA для проверки сертификата от клиентов.

б. Необходимо зарегистрировать в публичной DNS-системе внешний IP-адрес межсетевого экрана NetDefend таким образом, чтобы FQDN сервера CA в сертификатах, отправленных клиентам, могло быть преобразовано. Например, NetDefendOS может отправить сертификат клиенту с именем *ca.company.com*, которое необходимо преобразовать в публичный внешний IP-адрес межсетевого экрана NetDefend через публичную DNS-систему.

Следует выполнить те же шаги, если противоположную сторону туннеля представляет межсетевой экран вместо нескольких клиентов.

3. Сервер CA – это коммерческий сервер в публичной сети Интернет. В данном, простейшем случае, публичные DNS-серверы преобразовывают FQDN. Единственное требование заключается в том, чтобы у NetDefendOS был хотя бы один публичный адрес DNS-сервера, настроенный на преобразование FQDN в полученном сертификате.

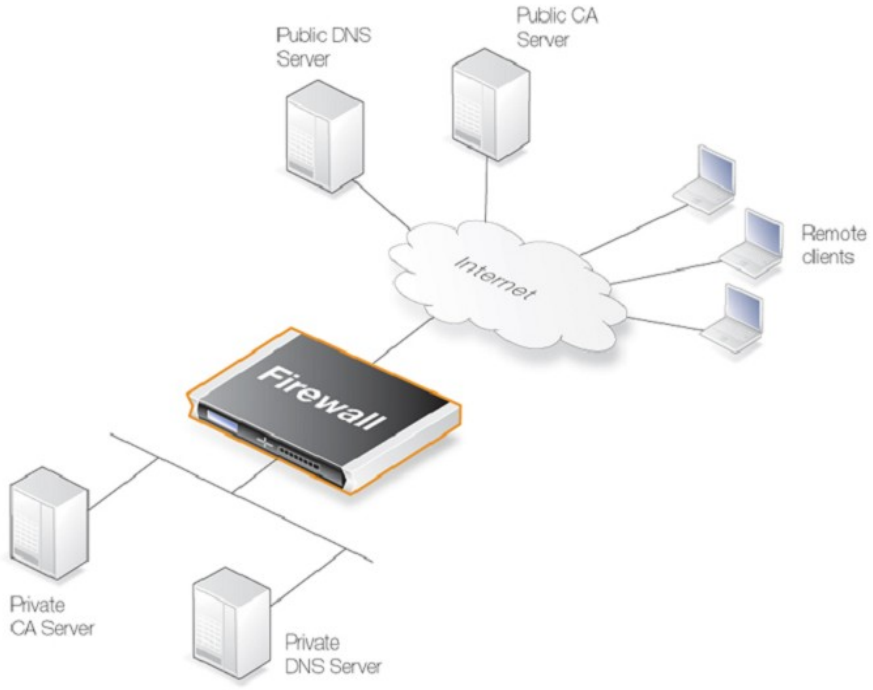


Рис. 9.4. Компоненты проверки сертификата

Доступ клиентов к серверу CA

В VPN-туннеле с удаленными клиентами, подключенными к межсетевому экрану NetDefend, программному обеспечению VPN-клиента может потребоваться доступ к серверу CA. Не каждому программному обеспечению VPN-клиента необходим этот доступ. В клиентах Microsoft, прежде всего, Vista, не отправляются запросы на сервер CA. В Microsoft Vista проверка выполняется по

умолчанию с возможностью отключения. Остальные клиенты (не Microsoft) отличаются в работе, но большинство из них попытаются проверить сертификат.

Расположение приватных серверов CA

Наиболее простым решением по размещению приватного сервера CA является его расположение на незащищенной стороне межсетевого экрана NetDefend. Тем не менее, с точки зрения безопасности это не рекомендуется. Лучше разместить сервер на внутренней стороне (или, если возможно, в зоне DMZ) под управлением NetDefendOS.

Как объяснялось ранее, адрес приватного сервера CA должен быть преобразован через публичные DNS-серверы для запросов проверки сертификата, идущих через сеть Интернет. Если запросы идут только от межсетевого экрана NetDefendOS и сервер CA находится на внутренней стороне межсетевого экрана, то IP-адрес внутреннего DNS-сервера должен быть задан в системе NetDefendOS, таким образом, эти запросы могут быть удовлетворены.

Выключение

Как было представлено в разделе «Поиск и устранение неисправностей» идентификация проблем с сервером CA может быть выполнена с помощью выключения требования проверки сертификата. Попытки доступа системы NetDefendOS к серверам CA можно выключить с помощью опции **Disable CRLs** для объектов сертификатов. Это означает, что проверка будет выключена и доступ к серверу заблокирован.

9.7. Поиск и устранение проблем VPN

В данном разделе рассматривается поиск и устранение общих проблем VPN.

9.7.1. Поиск и устранение проблем

Для всех типов VPN можно выполнить поиск и устранение неисправностей:

- Проверьте корректность IP-адресов
- Проверьте корректность ввода общих ключей и имен пользователей/паролей
- Используйте ICMP *Ping* для подтверждения активности туннеля. Для удаленных клиентов наиболее эффективным способом является Pinging. С помощью команды ping выполняется проверка внутреннего IP-адреса локального сетевого интерфейса на межсетевом экране NetDefend (в LAN to LAN команда ping может быть выполнена в любом направлении). Если NetDefendOS отвечает на запрос ping, то необходимо добавить следующее правило в набор IP-правил:

Action	Src Interface	Src Network	Dest Interface	Dest Network	Service
Allow	vpn_tunnel	all-nets	core	all-nets	ICMP

- Убедитесь, что другой **IPsec Tunnel** не препятствует корректному. Система NetDefendOS сканирует список туннелей сверху вниз, и туннель в верхней части списка с установленным значением *all-nets* для **Remote Network** и *none* для **Remote Endpoint** может препятствовать достижению корректного туннеля. Признаком этого является сообщение *Incorrect Pre-shared Key*.
- Попытайтесь избежать дублирования IP-адресов между удаленной сетью, к которой у клиента есть доступ, и внутренней сетью, которой принадлежит удаленный клиент.

Если удаленный клиент временно становится частью сети, например, Wi-Fi в аэропорту, клиент получает IP-адрес от DHCP-сервера в сети Wi-Fi. Если IP-адрес также принадлежит сети позади межсетевого экрана, то Windows по-прежнему считает, что IP-адрес принадлежит локальной сети клиента. По этой причине вместо удаленной сети пакеты маршрутизируются в локальную сеть.

Решением данной проблемы дублирования локального/удаленного IP-адреса является создание нового маршрута в таблице маршрутизации клиента Windows.

- Если при аутентификации удаленного пользователя не требуется имя пользователя/пароль, то убедитесь в том, что включены следующие расширенные настройки:
    - *IPsec Before Rules* для удаленных IPsec-клиентов
    - *L2TP Before Rules* для удаленных L2TP-клиентов
    - *PPTP Before Rules* для удаленных PPTP-клиентов

Данные настройки должны быть включены по умолчанию, благодаря этому трафик аутентификации между NetDefendOS и клиентом может «обходить» набор IP-правил. Если соответствующая настройка не включена, то необходимо добавить правило в набор IP-правил, чтобы разрешить прохождение трафика аутентификации между удаленными клиентами и системой NetDefendOS. Данное правило будет иметь интерфейс назначения **core.**

- Если удаленная конечная точка указана как URL, убедитесь, что префикс *dns:* предшествует строке URL. Например, если удаленная точка указана в виде *vpn.company.com,* то необходимо указать ее как *dns:vpn.company.com*.

9.7.2. Поиск и устранение проблем при использовании сертификатов

Если в решении VPN использовались сертификаты, то причины потенциальных проблем могут быть следующие:

- Проверьте корректность используемых сертификатов.
- Убедитесь, что у файлов *.cer* и *.key* одно и то же имя файла. Например, *my_cert.key* и *my_cert.cer*.
- Убедитесь, что срок действия сертификата не истек. У сертификатов есть определенный срок действия, по истечении которого они становятся недействительными, после чего требуются новые сертификаты.
- Убедитесь, что дата и время NetDefendOS установлены корректно. Если системные дата и время некорректные, то может показаться, что срок действия сертификатов уже истек, хотя в действительности он продолжается.
- Возможны проблемы, связанные с часовым поясом. Часовой пояс, установленный для межсетевого экрана NetDefend, может не совпадать с часовым поясом для сервера CA и, возможно, сертификат недействителен в локальной зоне.
- Отключите проверку списка отозванных сертификатов (Certificate Revocation List, CRL), чтобы выяснить, есть ли проблемы с доступом на сервер CA. Подробная информация о сервере CA содержится в *Разделе 9.6, «Доступ к серверу CA»*.

9.7.3. Команды поиска и устранения проблемы в IPsec

Для диагностики IPsec-туннелей используются следующие команды:

Команда *ipsecstat*

Команда *ipsecstat* используется для отображения корректной установки IPsec-туннелей. Ниже представлен пример выходных данных:

```
gw-world:/> ipsecstat

--- IPsec SAs:

Displaying one line per SA-bundle

IPsec Tunnel   Local           Net Remote     Net Remote GW
------------   --------------   ------------   -------------
L2TP_IPSec     214.237.225.43   84.13.193.179  84.13.193.179
IPsec_Tun1     192.168.0.0/24   172.16.1.0/24  82.242.91.203
```

Для проверки первой фазы согласования IKE настройки туннеля используется следующая команда:

```
gw-world:/> ipsecstat -ike
```

Для получения подробной информации об установке туннеля используется следующая команда:

```
gw-world:/> ipsecstat -u -v
```

у.

Предупреждение: Будьте осторожны при использовании опции -num=all

Если существует большое количество туннелей, то избегайте использования опции -num=all, так как это приведет к большому количеству выходных данных.

Например, при большом количестве туннелей избегайте использования команды:

```
gw-world:/> ipsecstat -num=all
```

оо *Также избегайте использования команды:*

```
gw-world:/> ipsectunnels -num=all
```

В таких условиях рекомендуется использование опции с небольшим значением, например, ***-num=10****.*

Команда *ikesnoop*

При настройке IPsec часто возникает следующая проблема: алгоритмы из списка на выбор не


```
gw-world:/> ikesnoop -on -verbose
```

подходят устройству в противоположной точке туннеля. Команда *ikesnoop* является полезной для диагностики списков алгоритмов с отображением деталей согласования во время установки туннеля. Команда выглядит следующим образом:

KlКоманда ICMP *ping* может быть отправлена на межсетевой экран NetDefend с удаленной точки туннеля. Это приведет к отображению выходных данных *ikesnoop* о согласовании установки туннеля к консоли и списка несовместимых алгоритмов.

Если существует несколько туннелей или нескольких клиентов на один туннель, то выходных данных опции *verbose* может быть слишком много. Поэтому лучше указать, что выходные данные идут с одного туннеля, указав IP-адрес конечной точки туннеля (это либо IP-адрес удаленной конечной точки, либо IP-адрес клиента). Команда принимает следующий вид:

```
gw-world:/> ikesnoop -on <ip-address> -verbose
```

чить *Ikesnoop* можно отключить с помощью следующей команды:

```
gw-world:/> ikesnoop -off
```

Для получения подробной информации обратитесь в *Раздел 9.4.5, «Поиск и устранение проблем с помощью команды ikesnoop».*

9.7.4. Сбой интерфейса управления VPN

Если после создания VPN-туннеля интерфейс управления больше не работает, то, вероятно, проблема в трафике управления, направленном обратно через VPN-туннель вместо корректного интерфейса.

Проблема возникает в случае добавления в таблицу маршрутизации маршрута, направляющего трафик для **all-nets** через VPN-туннель. Если после создания VPN-туннеля интерфейс управления недоступен, администратору необходимо добавить определенный маршрут, направляющий трафик интерфейса управления с межсетевого экрана NetDefend обратно в подсеть управления.

После указания VPN-туннеля в таблицу маршрутизации будет автоматически добавлен маршрут **all-nets,** таким образом, администратору необходимо всегда указывать определенный маршрут для корректной маршрутизации.

9.7.5. Сообщения об ошибках

Данный раздел подробно описывает сообщения об ошибках, которые могут появиться при создании VPN-туннелей:

1. ***Could not find acceptable proposal / no proposal chosen.***
2. ***Incorrect pre-shared key.***
3. ***Ike_invalid_payload, Ike_invalid_cookie.***
4. ***Payload_Malformed.***
5. ***No public key found.***

1. *Could not find acceptable proposal / no proposal chosen*

Это наиболее распространенное сообщение об ошибке, связанное с IPsec. Сообщение означает, что в зависимости от того, на какой стороне инициирована установка туннеля, согласования на фазе IKE или IPSec не выполнены, так как не удалось обнаружить соответствующее предложение, подходящее для обеих сторон.

При поиске и устранении неисправностей можно использовать данное сообщение, так как причин для его отправки может быть несколько, в зависимости от того, где было выполнено согласование.

- **Если не удалось выполнить согласование в течение фазы-1 – IKE**

Список IKE proposal не соответствует. Убедитесь, что список IKE proposal соответствует списку удаленной стороны. Желательно использовать команду *ikesnoop verbose* и создать туннель для инициации туннеля с удаленной стороны. Далее пользователь может просмотреть, какие предложения отправляет удаленная сторона, и сравнить результаты с собственным списком IKE proposal. Для прохождения фазы-1 необходимо ОДНО соответствие. Помните, что сроки действия крайне важны, так как они будут указаны в разделе признаков проблем. Примечание: В новых версиях невозможно установить срок действия в килобайтах (КБ) для фазы IKE, только в секундах.

- **Если не удалось выполнить согласование в течение фазы-2 – IPsec**

Список предложений IPsec не соответствует. Убедитесь, что список предлагаемых значений IPsec соответствует списку удаленной стороны. Можно использовать описанную выше консольную команду *ikesnoop,* когда удаленная сторона инициирует туннель, и сравнить с собственным списком. Дополнительным в фазе IPsec является то, что здесь происходит согласование сетей, таким образом, даже если список IPsec proposal кажется соответствующим, проблема может заключаться в несоответствии сетей. Локальная сеть (-и) на стороне пользователя должна быть Удаленной сетью в противоположной стороне и наоборот. Помните, что несколько сетей генерируют несколько SA IPsec, одну SA на сеть (или хост, при использовании данной опции). Важно указать размер сети, который должен быть одинаковым на обеих сторонах, так как он будет упоминаться позднее в разделе признаков проблем.

Также на вкладке IKE IPsec-туннеля существуют некоторые настройки, которые можно отнести к проблеме «No proposal chosen». Например режим Main или Aggressive, группа DH (для фазы IKE) и PFS (для фазы IPsec).

2. *Incorrect pre-shared key*

Проблема с общим ключом на любой стороне может привести к сбою согласования туннеля. Возможно, это наименее сложная проблема из всех, так как в данном случае причина только одна – некорректный общий ключ. Убедитесь, что используется один и тот же общий ключ (парольная фраза или шестнадцатеричный ключ), корректно добавленный в обеих точках туннеля.

Другой причиной для обнаружения системой NetDefendOS некорректного общего ключа может быть запуск некорректного туннеля во время согласований туннеля. Система NetDefendOS обрабатывает IPsec-туннели в списке сверху вниз и первоначально туннели сопоставляются с удаленным шлюзом. Например, удаленный туннель использует *all-nets,* как и удаленный шлюз. Этот туннель будет установлен прежде, чем выбранный Вами туннель, если в списке туннелей он стоит выше.

Например, рассмотрим следующие IPsec-туннели:

Name	Local Network	Remote Network	Remote Gateway
VPN-1	lannet	office1net	office1gw
VPN-2	lannet	office2net	office2gw
L2TP	ip_wan	all-nets	all-nets
VPN-3	lannet	office3net	office3gw

Так как *L2TP-туннель* в вышеуказанной таблице выше туннеля *VPN-3*, он будет установлен раньше *VPN-3* из-за удаленного шлюза *all-nets* (*all-nets* соответствует любой сети). Так как два туннеля используют различные общие ключи, пользователь получит сообщение об ошибке *«Incorrect pre-shared key»*.

Проблема решается благодаря изменению нумерации в списке и перестановки *VPN-3* выше *L2TP*. Далее шлюз *office3gw* будет соответствовать корректным образом и система NetDefendOS выберет туннель *VPN-3*.

3. *Ike_invalid_payload, Ike_invalid_cookie*

В данном случае компьютер с поддержкой IPsec в NetDefendOS получает пакет IPsec IKE, но не может сопоставить его с существующим IKE.

Если VPN-туннель установлен только на одной стороне, это может привести к сообщению об ошибке в тот момент, когда трафик приходит из туннеля, который не существует. Например, по некоторым причинам соединение было нарушено на стороне инициатора, но терминатор по-прежнему наблюдает активное соединения. Далее терминатор отправляет пакеты по туннелю, но когда они

приходят к инициатору, он отбрасывает их, так как соответствующий туннель не обнаружен.

Для решения проблемы просто удалите туннель со стороны, которая считает его по-прежнему активным. Рекомендуется выяснить, почему на одной стороне нарушено соединение. Возможно, *DPD* и/или *Keep-Alive* используются только на одной стороне. Другой возможной причиной может быть то, что даже при получении пакета *DELETE*, туннель не был удален.

4. *Payload_Malformed*

Данная проблема аналогична проблеме *Incorrect pre-shared key*, описанной выше. Возможная причина заключается в том, что на любой стороне используется ключ PSK неверного типа (парольная фраза или шестнадцатеричный ключ).

Убедитесь в том, что на обеих сторонах IPsec-туннеля используется один и тот же тип ключа. Если на одной стороне используется шестнадцатеричный ключ, а на другой парольная фраза, скорее всего, будет отправлено сообщение об ошибке.

5. No public key found

Это часто отправляемое сообщение при работе с VPN-туннелями и использовании сертификатов для аутентификации.

Устранение данной проблемы может оказаться сложным, так как причины ее возникновения различны. Также важно помнить, что при работе с сертификатами необходимо совместно использовать журналы *ikesnoop* и обычные журналы, так как *ikesnoop* не предоставляет информации о сертификатах, а стандартные журналы могут содержать важную информацию о причине проблемы. Прежде чем заняться устранением проблемы рекомендуется установить туннель на основе PSK, далее проверить, успешно ли прошла установка, а затем перейти к использованию Сертификатов (если тип конфигурации разрешает это).

Возможны следующие причины проблемы:

- Сертификат на любой стороне не подписан одним и тем же сервером CA.
- Срок действия сертификата истек или еще не вступил в силу. Последнее может произойти из-за некорректного времени, установленного либо на сервере CA, либо на межсетевом экране NetDefend, или по причине того, что они находятся в разных часовых поясах.
- У межсетевого экрана NetDefend нет доступа к *Списку отозванных сертификатов* (Certificate Revocation List, CRL) на сервере CA, чтобы проверить подлинность сертификата. Убедитесь в корректности пути CRL в свойствах сертификата. (Можно отключить функцию CRL). Также убедитесь, что в NetDefendOS настроен DNS-клиент для корректного преобразования пути к CRL.

Примечание: L2TP и Microsoft Vista

С помощью L2TP система Microsoft Vista по умолчанию пытается загрузить список CRL, в то время как система Microsoft XP этого не выполняет. В операционной системе Vista можно выключить данную опцию.

- Если существует несколько похожих или удаленных туннелей и для их различения используются списки идентификаторов, возможной причиной будет то, что ни один из списков идентификаторов не соответствует свойствам сертификатов подключенного пользователя. Вероятно, пользователь является неавторизованным или свойства сертификата неверные, помимо этого, возможно необходимо обновить списки идентификаторов.
- При использовании L2TP-протокола сертификат клиента помещается в хранилище неверных сертификатов на клиенте Windows. При подключении клиента используется неверный сертификат.

9.7.6. Особые признаки

Существует два особых признака:

1. ***Только одна сторона может инициировать установку туннеля.***

2. ***Невозможно установить туннель, и команда* ikesnoop *сообщает о проблеме config mode XAuth, даже если XAuth не используется.***

1. Только одна сторона может инициировать установку туннеля

Причиной данной проблемы является несоответствие размера в локальной или удаленной сети и/или настройки срока действия в предлагаемом списке (-ax).

Для поиска и устранения данной проблемы необходимо проверить настройки для локальной сети, удаленной сети, списка IKE proposal и списка IPsec на обеих сторонах для идентификации несоответствия.

Например, предположим, что в каждой точке туннеля установлены следующие IPsec-настройки:

- **Сторона А**

Локальная сеть = 192.168.10.0/24

Удаленная сеть = 10.10.10.0/24

- **Сторона Б**

Локальная сеть = 10.10.10.0/24

Удаленная сеть = 192.168.10.0/16

В данном сценарии указанный диапазон адресов удаленной сети на **стороне Б** больше, чем на **стороне А**. Это означает, что только **сторона А** может успешно инициировать установку туннеля к **стороне Б**, так как размер ее сети меньше. Когда **сторона Б** пытается установить туннель, **сторона А** отклоняет эту попытку, так как размер сети больше, чем указано. Причина заключается в том, что сети с меньшим размером являются более защищенными. Это также относится к сроку действия в списках *proposal*.

2. Невозможно настроить по запросу конфигурации. Поддельное сообщение XAuth

Основная причина отправки этого сообщения – «No proposal chosen». Это происходит в случае неподходящего размера локальной или удаленной сети. Так как система NetDefendOS определила, что проблема заключается в размере сети, она предпримет последнюю попытку получить корректные настройки, отправив запрос на конфигурирование.

С помощью *ikesnoop*, когда обе стороны инициируют туннель, можно легко сравнить, находятся ли обе стороны в фазе-2. С помощью этой информации можно определить проблемы в сети. Возможно, причина в несоответствии размера сети или в полном отсутствии соответствия.

Глава 10. Управление трафиком

Данная глава содержит информацию об управлении трафиком в системе NetDefendOS.

- Traffic Shaping
- IDP Traffic Shaping
- Правила порога
- Сервер балансировки нагрузки

10.1. Traffic Shaping

10.1.1. Обзор

QoS и TCP/IP

Недостатком TCP/IP является отсутствие функции *Quality of Service* (QoS). QoS гарантирует и ограничивает полосу пропускания для определенных служб и пользователей. Такие решения, как архитектура *дифференцированного обслуживания – Differentiated Services* (Diffserv), были разработаны для решения проблемы QoS в крупных сетях благодаря использованию информации в заголовках пакетов для предоставления сетевым устройствам информации QoS.

Поддержка Diffserv в NetDefendOS

NetDefendOS поддерживает архитектуру Diffserv следующими способами:

- NetDefendOS отправляет 6 битов, образующих *точку кода дифференцированного обслуживания* (Differentiated Services Code Point (DSCP) Diffserv), копируя эти биты из потока данных внутри VPN-туннеля в инкапсулированные пакеты.
- Как будет описано далее, подсистема Traffic shaping NetDefendOS может использовать DSCP-биты как основу для приоритезации трафика, проходящего через межсетевой экран NetDefend.

Важно знать, что функция Traffic shaping в NetDefendOS не добавляет новую информацию Diffserv в пакеты во время их прохождения через межсетевой экран NetDefend. *Приоритеты* Traffic shaping NetDefendOS, описанные далее, действуют только в рамках системы NetDefendOS и не замещают информацию Diffserv, добавляемую в пакеты.

Применение Traffic Shaping

Тем не менее, такие архитектуры как Diffserv не применяются, если приложения сами предоставляют информацию QoS. В большинстве сетей приложения и пользователи не назначают приоритет собственному трафику. Если ситуация не зависит от пользователей, то сетевое оборудование само должно принимать решения относительно приоритетов и распределения полосы пропускания.

NetDefendOS обеспечивает управление QoS, позволяя администратору применять ограничения и гарантии к сетевому трафику, проходящему через межсетевой экран NetDefend. Этот подход часто именуется *traffic shaping* и идеально подходит для управления полосой пропускания в локальной сети, а также для управления трафиком в «узких» местах, которые могут образоваться в крупных сетях. Traffic shaping применяется к любому типу трафика, включая проходящий через VPN-туннели.

Средства Traffic Shaping

Traffic shaping действует путем сравнения и постановки IP-пакетов в очередь в соответствии со значением настраиваемых параметров. Используются следующие средства:

- Применение ограничений полосы пропускания и постановка в очередь пакетов, превышающих установленные ограничения. Позже, при снижении запросов на полосу пропускания, выполняется отправка данных пакетов.

- Отбрасывание пакетов, если буфер пакетов переполнен. Отбрасываемые пакеты выбираются из тех, которые вызвали перегрузку канала связи.

- Приоритезация трафика в соответствии с решениями администратора. Если количество трафика с более высоким приоритетом увеличивается, в то время как канал связи перегружен, трафик с более низким приоритетом можно временно ограничить, чтобы освободить место для трафика с более высоким приоритетом.

- Гарантия полосы пропускания. Как правило, это выполняется за счет обработки определенного количества трафика (гарантированного количества) в качестве высокоприоритетного. Трафик, превышающий гарантированное значение, приобретает такой же приоритет, как и любой другой трафик, конкурируя с неприоритетным трафиком.

Как правило, Traffic shaping не выполняет постановку в очередь огромного количества данных с последующей отсортировкой приоритетного трафика для его отправки перед неприоритетным. Вместо этого, определяется количество приоритетного трафика и неприоритетный трафик ограничивается динамически таким образом, чтобы не препятствовать прохождению приоритетного трафика.

Примечание: Traffic shaping не работает с SIP ALG

Любое соединение, запускающие IP-правило вместе с объектом службы, который использует SIP ALG, не может быть объектом для traffic shaping.

10.1.2. Traffic Shaping в NetDefendOS

NetDefendOS предоставляет расширенные возможности Traffic shaping для пакетов, проходящих через межсетевой экран NetDefend. Различные ограничения скорости и гарантии трафика могут быть созданы в качестве политик на основе протокола, источника и назначения трафика, аналогично способу создания политик безопасности на основе IP-правил.

Существует два основных компонента Traffic shaping в NetDefendOS:

- **Каналы** (Pipes)

- **Правила каналов** (Pipe Rules)

Каналы (Pipes)

Канал является основным объектом для Traffic shaping и представляет собой концептуальный канал, через который проходит поток данных. Существуют различные характеристики канала, определяющие способ обработки проходящего трафика. Количество необходимых каналов определяет администратор. По умолчанию не задан ни один канал.

Простота использования каналов заключается в том, что ни тип, ни направление проходящего трафика не имеют для каналов значения. Каналы определяют количество данных, проходящих через них, и далее применяют ограничения, заданные администратором, либо в совокупности, либо для *Приоритетов* и / или *Групп* (подробная информация об этих понятиях представлена в *Разделе 10.1.6*, *«Приоритеты»*).

Система NetDefendOS способна обрабатывать сотни каналов одновременно, но в действительности в большинстве сценариев используется только несколько каналов. Вполне возможно, что десятки каналов могут потребоваться в сценарии, в котором для отдельных протоколов используются отдельные каналы. Большое количество каналов может потребоваться в сценарии провайдера

Интернет-услуг, в котором для каждого клиента выделен канал.

Правила каналов (Pipe Rules)

Одно или несколько *Правил канала* составляют *набор Правил канала* NetDefendOS, которые определяют, какой трафик будет проходить через каналы.

Каждое правило канала назначается, как и другие политики безопасности NetDefendOS: указывается интерфейс/сеть источника/назначения, а также службы, к которой применяется правило. После того как набор IP-правил разрешает новое соединение, выполняется проверка набора правил канала на соответствие правилам канала.

Правила канала проверяются так же, как IP-правила, сверху вниз (с первого по последнее) в наборе правил. Первое соответствующее правило, если таковое имеется, решает, является ли соединение объектом для Traffic shaping. Помните, что любое соединение, которое не попадает под правило канала, не является объектом для Traffic shaping и потенциально может использовать любую необходимую пропускную способность.

Примечание: По умолчанию не определено ни одного правила канала

Первоначально набор правил для правил канала не содержит ни одного правила по умолчанию. Для активации Traffic shaping необходимо создать хотя бы одно правило.

Правила каналов (Pipe Rules)

После указания правила также указываются используемые с этим правилом каналы, которые помещаются в один или два следующих списка правил канала:

- **Прямая цепочка (Forward Chain)**

Канал или каналы, которые будут использоваться для трафика, исходящего от межсетевого экрана NetDefend. Можно указать один канал, несколько каналов или ни одного.

- **Обратная цепочка (Return Chain)**

Канал или каналы, которые будут использоваться для входящего трафика с межсетевого экрана NetDefend. Можно указать один канал, несколько каналов или ни одного.

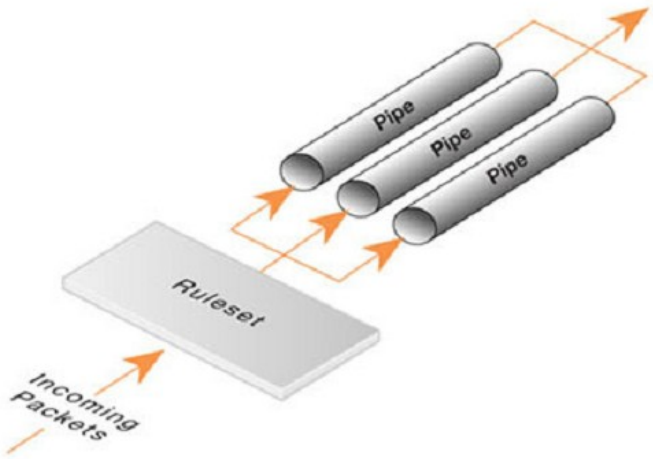


Рис. 10.1. Правила канала определяют использование канала

Используемые каналы указаны в *списке каналов*. Если указан только один канал, то это канал, чьи характеристики применяются к трафику. Если указаны несколько каналов, то они формируют цепочку каналов, через которые пройдет трафик. Максимальное количество каналов в цепочке – 8.

Исключение трафика из обработки подсистемой Traffic Shaping

Если в списке правил не указано ни одного канала, то трафик, соответствующий правилу, не будет проходить через какой-либо канал. Это также означает, что инициирующий трафик не будет обработан любыми другими соответствующими правилами каналов, которые возможно находятся в наборе правил.

Это обеспечивает исключение определенного трафика из обработки подсистемой Traffic shaping. Такие правила не являются необходимыми, но если они находятся в начале набора правил каналов, они могут предотвратить Traffic Shaping последующими правилами.

Каналы не работают с IP-правилами *FwdFast*

Важно знать, что Traffic shaping не будет работать с трафиком, который проходит в результате запуска IP-правила *FwdFast* из набора IP-правил NetDefendOS.

Причина заключается в том, что Traffic shaping выполняется с помощью *механизма состояний (state engine)* NetDefendOS, который является подсистемой, отвечающей за отслеживание соединений. IP-правила *FwdFast* не направляют соединение в подсистему механизма состояний. Вместо этого пакеты не рассматриваются как часть соединения и индивидуально перенаправляются в точку назначения, обходя механизм состояний.

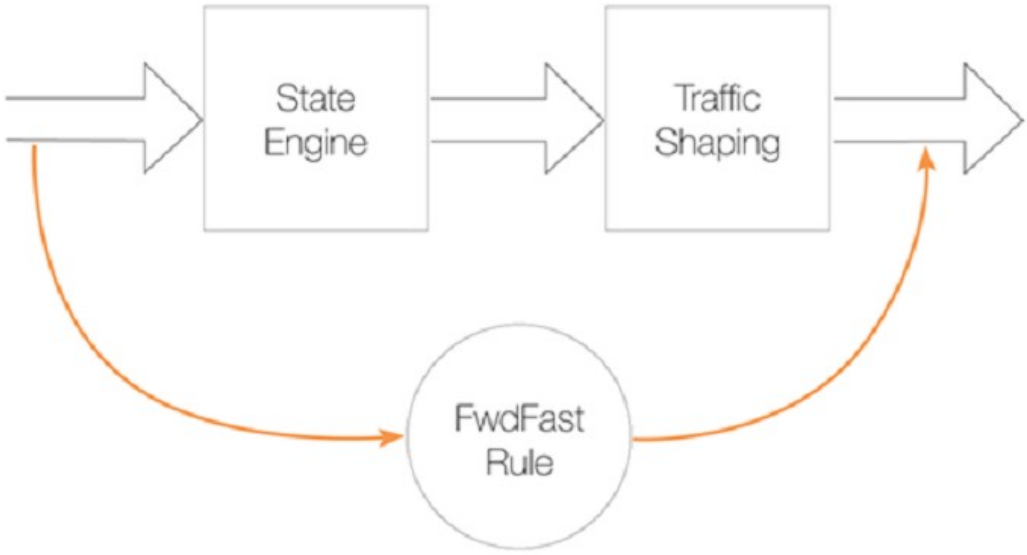


Рис. 10.2. Правила *FwdFast* обходят Traffic Shaping

10.1.3. Простое ограничение полосы пропускания

Самый простой способ использования каналов – это ограничение полосы пропускания, при этом не требуется специальная планировка. В следующем примере ограничение полосы пропускания применяется только для входящего трафика. Именно в данном направлении чаще всего возникают проблемы с Интернет-соединением.

Пример 10.1. Применение простого ограничения полосы пропускания

Начните с создания простого канала, который ограничивает весь проходящий через него трафик до 2 Мбит/с, независимо от типа трафика.

CLI

```
gw-world:/> add Pipe std-in LimitKbpsTotal=2000
```

Web-интерфейс

1. Зайдите **Traffic Management > Traffic Shaping > Pipes > Add > Pipe**

2. Укажите подходящее имя канала, например, *std-in*

3. Введите значение *2000* в текстовом поле **Total** на вкладке **Pipe Limits**

4. Нажмите **OK**

Трафик должен проходить через канал, и это выполняется за счет использования канала в Правиле канала.

Мы будем использовать созданный выше канал для ограничения входящего трафика. Это ограничение применяется к пакетам трафика, а не к соединениям. При выполнении Traffic shaping нас интересует направление, в котором перемещаются данные, а не компьютер, инициировавший соединение.

Создаем простое правило, разрешающее прохождение любого исходящего трафика. Добавляем созданный канал в *обратную цепочку* (return chain*)*. Это означает, что пакеты, идущие в *обратном направлении* данного соединения (outside-in), должны проходить через канал *std-in*.

CLI

```
gw-world:/> add PipeRule ReturnChain=std-in SourceInterface=lan
            SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=all_services name=Outbound
```

Web-интерфейс

1. Зайдите **Traffic Management > Traffic Shaping > Pipes > Add > Pipe Rule**

2. Укажите подходящее имя канала, например, *outbound*

3. Далее введите:

• **Service:** all_services

• **Source Interface:** lan

• **Source Network:** lannet

• **Destination Interface:** wan

• **Destination Network:** all-nets

4. На вкладке **Traffic Shaping** выберите *std-in* в настройках для **Return Chain**

5. Нажмите **OK**

Данная настройка ограничивает весь входящий трафик (Интернет) до 2 Мбит/с. Не применяются ни свойства, ни динамическая балансировка.

10.1.4. Ограничение полосы пропускания в обоих направлениях

Использование одного канала для обоих направлений

Направление трафика, проходящего через один канал, не имеет значения, так как учитывается только величина общей пропускной способности. Система NetDefendOS разрешает использование одного и того же канала для входящего и исходящего трафика, но при этом не будет точного разделения ограничений канала между двумя направлениями.

В предыдущем примере полоса пропускания ограничена только для входящего направления. В большинстве случаев это направление заполняется в первую очередь. Но что делать, если необходимо ограничить исходящий трафик таким же образом?

Помещение **std-in** в прямую цепочку (forward chain) не принесет результата, так как возможно нам потребуется получить ограничение до 2 Мбит/с для исходящего трафика отдельно от ограничения до 2 Мбит/с для входящего. Если помимо исходящего трафика (2 Мбит/с) через канал проходит входящий трафик (2 Мбит/с), то общий поток трафика составит 4 Мбит/с. Так как ограничение канала составляет 2 Мбит/с фактическая величина потока будет близка к значению в 1 Мбит/с в каждом направлении.

Увеличение общего ограничения до 4 Мбит/с не решит проблему, так как одиночному каналу будет неизвестно, что имеются в виду ограничения 2 Мбит/с для входящего и 2 Мбит/с для исходящего трафика. В результате может быть 3 Мбит/с исходящего и 1 Мбит/с входящего трафика, так как это также составляет 4 Мбит/с.

Использование двух отдельных каналов

Для управления полосой пропускания в обоих направлениях рекомендуется использовать два отдельных канала: один для входящего, а другой для исходящего трафика. В данном сценарии в целях достижения оптимального результата для каждого канала установлено ограничение 2 Мбит/с. Следующий пример описывает данную настройку.

Пример 10.2. Ограничение полосы пропускания в обоих направлениях

Создайте второй канал для исходящего трафика:

CLI

```
gw-world:/> add Pipe std-out LimitKbpsTotal=2000
```

Web-интерфейс

1. Зайдите **Traffic Management > Traffic Shaping > Pipes > Add > Pipe**

2. Укажите подходящее имя канала, например, *std-out*

3. Введите значение *2000* в текстовом поле **Total**

4. Нажмите **OK**

После создания канала для управления исходящей полосой пропускания, добавьте его в прямую цепочку каналов правила, созданного в предыдущем примере:

CLI

```
gw-world:/> set PipeRule Outbound ForwardChain=std-out
```

Web-интерфейс

1. Зайдите **Traffic Management > Traffic Shaping > Pipes > Add > Pipe Rules**

2. Правой кнопкой мыши нажмите на правило канала, созданное в предыдущем примере, и выберите **Edit**

3. На вкладке **Traffic Shaping** выберите *std-out* в списке **Forward Chain**

4. Нажмите **OK**

В результате все подключения будут ограничены до 2 Мбит/с в каждом направлении.

10.1.5. Создание дифференцированных ограничений с помощью цепочек

В предыдущих примерах выполнялось ограничение трафика для всех исходящих соединений. Что делать, если необходимо ограничить навигацию по Web-страницам больше, чем остальной трафик? Предположим, что ширина общей полосы пропускания – 250 кбит/с, из которых 125 кбит/с выделены для трафика, расходуемого на просмотр Web-страниц.

Некорректное решение задачи

Можно установить два канала для просмотра Web-страниц для входящего и исходящего трафика. Как правило, ограничение исходящего трафика не требуется, так как в большинстве случаев, навигация по Web-страницам обычно состоит из коротких исходящих запросов, отправленных на сервер и следующих за ними длинных входящих ответов.

Поэтому сначала для входящего трафика создается канал **surf-in** с ограничением в 125 кбит/с. Далее задается новое Правило канала для просмотра Web-страниц, которое использует канал **surf-in** и помещается перед правилом, направляющим остальной трафик в канал **std-in**. Таким образом, трафик, расходуемый на просмотр Web-страниц, проходит через канал **surf-in**, а остальной трафик будет обработан правилом и каналом, созданными ранее.

К сожалению, это не приведет к желаемому результату в виде выделения максимального ограничения в 125 кбит/с, как части общего ограничения 250 кбит/с. Входящий трафик проходит через один из двух каналов: один допускает 250 кбит/с, а другой – 125 кбит/с, создавая итоговую величину в 375 кбит/с для входящего трафика, но данное значение превышает ограничение в 250 Кбит/с.

Корректное решение задачи

Для решения задачи создайте *цепочку*, состоящую из канала **surf-in** и канала **std-in**, в правиле канала для трафика, расходуемого на просмотр Web-страниц. Входящий трафик сначала проходит через канал **surf-in** и получает максимальное ограничение до 125 кбит/с. Далее трафик проходит через канал **std-in** вместе с остальным входящим трафиком, для которого используется общее ограничение в 250 кбит/с.

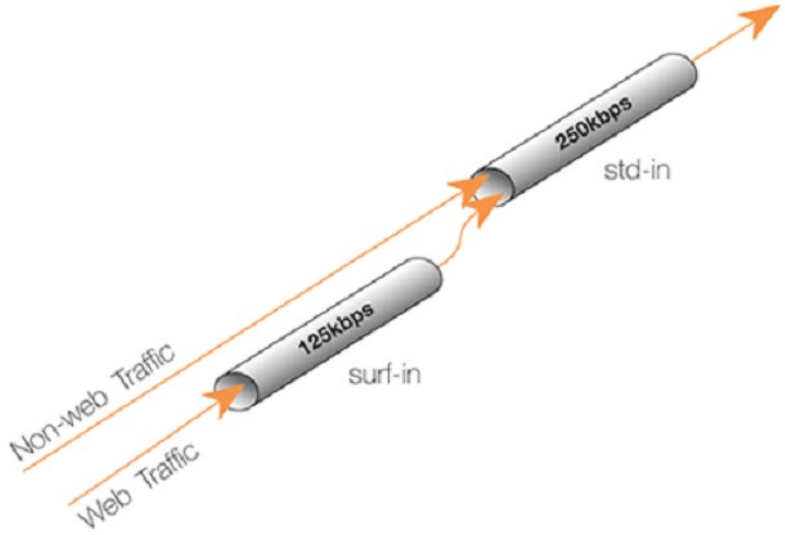


Рис. 10.3. Дифференцированные ограничения с использованием цепочек

Если при просмотре Web-страниц используется ограничение в 125 кбит/с полностью, эти 125 кбит/с займут половину канала **std-in**, оставшиеся 125 кбит/с будут использоваться для остального трафика. Если просмотр Web-страниц не выполняется, то все 250 кбит/с, доступные для канала **std-in**, могут использоваться для другого трафика.

Это не обеспечивает гарантируемую полосу пропускания для просмотра Web-страниц, но устанавливает ограничение до 125 кбит/с и гарантирует полосу пропускания 125 кбит/с для всего остального трафика. Для просмотра Web-страниц в процессе конкуренции за полосу пропускания в 125 кбит/с применяются стандартные правила: трафик будет проходить на общих основаниях в порядке поступления наравне с другими типами трафика. Это может означать и 125 кбит/с, но также и более низкую скорость, если канал соединения занят.

Установка каналов таким способом накладывает ограничения только на максимальные значения для некоторых типов трафика и не предоставляет приоритетов для различных типов конкурирующего трафика.

10.1.6. Приоритеты

Приоритет по умолчанию – ноль

Все пакеты, которые проходят через каналы Traffic shaping NetDefendOS, обладают *Приоритетом* (Precedence). В примерах, используемых до данного момента, приоритеты не были четко указаны и, таким образом, у всех пакетов был один и тот же приоритет по умолчанию – 0.

8 возможных уровней приоритетов

Существует восемь приоритетов, пронумерованных от 0 до 7. Приоритет 0 – это наименее значимый приоритет (низший), а 7 – наиболее значимый приоритет (наивысший). Приоритет рассматривается как отдельная очередь трафика; трафик с приоритетом 2 будет отправлен раньше трафика с приоритетом 0, а трафик с приоритетом 4 перед трафиком с приоритетом 2.

Рис. 10.4. Восемь приоритетов каналов

Значение приоритета является относительным

Значение приоритета основано на том, что он либо выше, либо ниже, чем другой приоритет, и не зависит от его числового значения. Например, если в сценарии Traffic shaping используются два приоритета, то выбор приоритетов со значениями 4 и 6 вместо 0 и 3 не повлияет на конечный результат.

Назначение приоритета трафику

Способ назначения приоритета трафику указан в правиле канала и выполняется с помощью одного из трех методов:

- **Использование приоритета первого канала**

  Каждый канал обладает *приоритетом по умолчанию,* и пакетам присваивается приоритет по умолчанию первого канала, через который они проходят.

- **Использование фиксированного приоритета**

  Сработавшее правило канала назначает фиксированный приоритет.

- **Использование DSCP-битов**

  Приоритет назначается из DSCP-битов пакета. DSCP является элементом архитектуры Diffserv, где биты *Type of Service* (ToS) включены в заголовок IP-пакета.

Назначение приоритетов в пределах каналов

После установки канала можно указать значения *приоритета по умолчанию* (Default Precedence)*, минимального приоритета* (Minimum Precedence) и *максимального приоритета* (Maximum Precedence)*.* Приоритеты по умолчанию:

- **Минимальный приоритет: 0**
- **Приоритет по умолчанию: 0**
- **Максимальный приоритет: 7**

Как описывалось выше, *Приоритет по умолчанию* – это приоритет, назначаемый пакету, в случае, если приоритет не назначен правилом канала.

Минимальный и максимальный приоритеты определяют диапазон приоритетов, который будет обработан каналом. Если пакет приходит с уже назначенным приоритетом ниже минимального, то его приоритет меняется на минимальный. Таким же образом, если приходит пакет с уже назначенным приоритетом выше максимального, его приоритет меняется на максимальный.

Для каждого канала можно дополнительно указать отдельные ограничения полосы пропускания для каждого уровня приоритета. Эти ограничения могут быть указаны в килобитах в секунду и/или пакетах в секунду (если указаны оба, то будет использоваться ограничение, первым достигшее своего предела).

Совет: Указание полосы пропускания

*Помните, что при указании полосы пропускания сетевого трафика, приставка **Kilo** означает **1000**, а НЕ 1024. Например, **3 Kbps** означает **3000** битов в секунду.*

*Таким же образом, приставка **Mega** означает один миллион в контексте полосы пропускания.*

Ограничения приоритета являются Гарантиями

Ограничение приоритета является как ограничением, так и гарантией. Величина полосы пропускания, указанная для приоритета, также гарантирует, что данная полоса пропускания будет доступна за счет урезания полосы пропускания с наименьшим приоритетом. Если указанное

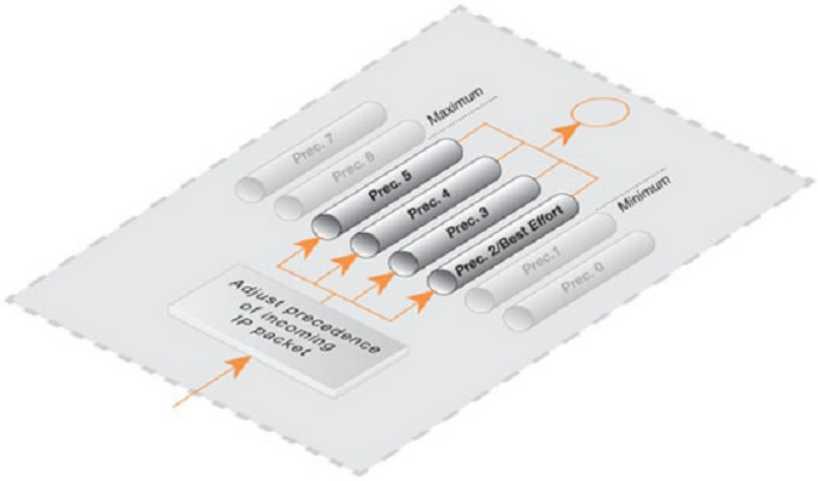
значение полосы пропускания превышено, трафик получает наименьший приоритет. Подробная информация о значении наименьшего приоритета представлена далее.

Наименьший приоритет (*Best Effort*)

Минимальный (наименьший) приоритет имеет особое значение: он действует как *Приоритет негарантированной доставки (Best Effort)*. Все пакеты с данным приоритетом обрабатываются по в порядке поступления.

Пакеты с приоритетом выше, чем приоритет негарантированной доставки, превысившие ограничение для своего приоритета, автоматически получают наименьший приоритет (best effort) и обрабатываются так же как остальные пакеты с наименьшим приоритетом.

На рисунке ниже значение наименьшего приоритета – 2, а



максимального – 6. Приоритет 2 является приоритетом негарантированной доставки (best effort).

Рис. 10.5. Минимальный и максимальный приоритет канала

Ограничения наименьшего приоритета

Как правило, нет необходимости в указании ограничения для наименьшего приоритета (best effort), так как этот приоритет использует любую свободную часть полосы пропускания, не используемую наивысшими приоритетами. Тем не менее, можно указать ограничение, если необходимо ограничить полосу пропускания, используемую для наименьшего приоритета. Это может потребоваться в случае, если определенный тип трафик всегда получает наименьший приоритет, но ему необходимо ограничить использование полосы пропускания.

Приоритеты применяются только при заполнении канала

Использование приоритета не является эффективным, пока не достигнуто общее ограничение, указанное для канала. Это происходит потому, что пока не достигнуто ограничение канала (заполнение канала), между приоритетами нет конкуренции.

При заполнении канала система NetDefendOS приоритезирует трафик согласно приоритету: пакеты с высоким приоритетом, которые не превышают ограничение данного приоритета, отправляются перед пакетами с более низким приоритетом. Пакеты с низким приоритетом до момента отправки помещаются в буфер. Если буферного пространства недостаточно, пакеты отбрасываются.

Если общее ограничение канала не указано, то это равнозначно утверждению, что канал имеет неограниченную пропускную способность и, следовательно, никогда не может быть заполнен, таким образом, использование приоритетов не имеет смысла.

Применение приоритетов

Продолжая использовать предыдущий пример с Traffic shaping, добавим требование, что трафик SSH и Telnet должен иметь более высокий приоритет по сравнению с остальным трафиком. Для этого добавим Правило канала специально для SSH и Telnet и установим в правиле более высокий приоритет – например, 2. В данном новом правиле мы указываем каналы, используемые для остального трафика.

Результатом данного действия является то, что правило SSH и Telnet назначает более высокий приоритет пакетам, связанным с данными службами, и отправка этих пакетов выполняется через тот же канал, что и остальной трафик. Канал гарантирует, что при превышении ограничения полосы пропускания, указанного в настройках канала, пакеты с более высоким приоритетом будут отправлены в первую очередь. Пакеты с более низким приоритетом будут помещены в буфер и отправлены, если используемое значение пропускной способности меньше, чем максимальная величина, указанная для канала. Процесс буферизации иногда приводит к эффекту обратного давления («throttling back»), так как он уменьшает скорость потока.

Необходимость гарантий

Проблема может возникнуть в случае, если приоритезируемый трафик представляет собой непрерывный поток данных, например, аудио в режиме реального времени, приводящее к непрерывному использованию всей доступной полосы пропускания и длительному времени ожидания в очереди других служб, таких как просмотр Web-страниц, DNS или FTP. Таким образом, требуется средство для обеспечения выделения некоторой части полосы пропускания для менее приоритетного трафика, и это выполняется с помощью *гарантированной полосы пропускания* (Bandwidth Guarantees).

Использование приоритетов в качестве гарантий

Указание ограничения для приоритета также гарантирует минимальное количество полосы пропускания для данного приоритета. Трафик, проходящий через канал, получит гарантию, указанную для приоритета, за счет урезания трафика с более низким приоритетом.

Для изменения способа приоритезации трафика SSH и Telnet из предыдущего примера так, чтобы гарантировать ему 96 кбит/с, необходимо в канале *std-in* установить ограничение для приоритета равное 96 кбит/с.

Это не означает, что входящий трафик SSH и Telnet ограничен до 96 кбит/с. Ограничения приоритетов более высоких, чем приоритет негарантированной доставки всего лишь ограничивают количество проходящего трафика с конкретным приоритетом.

Если приходящий трафик с приоритетом 2 превышает 96 кбит/с, то приоритет той части трафика, которая превышает данное ограничение, понижается до приоритета негарантированной доставки (best effort). Весь трафик с приоритетом негарантированной доставки (best effort) будет отправлен в порядке поступления.

Дифференцированные гарантии

Проблема возникает, если необходимо предоставить определенную гарантию в 32 кбит/с трафику Telnet и определенную гарантию в 64 кбит/с трафику SSH. Можно было бы задать ограничение в 32

кбит/с для приоритета 2, 64 кбит/с для приоритета 4 и затем пустить различные типы трафика с заданными каждому из них приоритетами. Тем не менее, при таком подходе существует две очевидные проблемы:

- Какой трафик наиболее важен? Этот вопрос не является существенным, но приобретает значение по мере увеличения комплексности сценария Traffic shaping.

- Количество приоритетов ограничено. Возможно, данного количества будет недостаточно во всех случаях, даже если исключить проблему «Какой трафик наиболее важен?».

Решение заключается в создании двух новых каналов: один для трафика Telnet и другой для трафика SSH, подобно тому, как ранее был создан канал «surf».

Сначала удалите ограничение в 96 кбит/с в канале **std-in**, затем создайте два новых канала: **ssh-in** и **telnet-in**. Для обоих каналов укажите приоритет 2 в качестве приоритета по умолчанию, и, соответственно, задайте ограничения для приоритета 2 в 32 и 64 кбит/с.

Далее, разделите предварительно указанное правило, отвечавшее за диапазон портов 22-23 на два отдельных правила для каждого порта 22 и 23 соответственно:

Оставьте в качестве прямой цепочки для обоих правил только канал **std-out**. Для упрощения данного примера мы рассматриваем только входящий трафик, в этом направлении заполнение канала наиболее вероятно в условиях, ориентированных на клиента.

В качестве обратной цепочки в правиле для порта 22 укажите канал **ssh-in** и следующий за ним канал **std-in**. В качестве обратной цепочки в правиле для порта 23 укажите канал **telnet-in** и следующий за ним канал **std-in**.

В качестве значения приоритета в обоих правилах выберете **Use defaults from first pipe**; для обоих каналов **ssh-in** и **telnet-in** приоритетом по умолчанию является приоритет 2.

Использование данного подхода является более рациональным решением, чем указание приоритета 2 в наборе правил, при этом можно легко изменить приоритет всего трафика SSH и Telnet, поменяв приоритет по умолчанию каналов **ssh-in** и **telnet-in**.

Помните, что мы не задали общее ограничение для каналов **ssh-in** и **telnet-in**. В этом нет необходимости, так как общее ограничение будет осуществлено с помощью канала **std-in**, расположенного в конце соответствующих цепочек.

Каналы **ssh-in** и **telnet-in** действуют в качестве «приоритетных фильтров» (priority filter): благодаря им через канал **std-in** будет проходить только зарезервированное количество трафика с приоритетом 2 (64 и 32 кбит/с соответственно). Остальная часть трафика SSH и Telnet, превысившего свои гарантии, пройдет через канал **std-in** с приоритетом 0, который является приоритетом негарантированной доставки для каналов **std-in** и **ssh-in**.

Примечание: Порядок обратной цепочки имеет значение

*В данном случае порядок указания каналов в обратной цепочки крайне важен. Если поставить канал **std-in** перед **ssh-in** и **telnet-in**, то трафик будет пропущен через канал std-in с наименьшим приоритетом и, следовательно, будет конкурировать за 250 кбит/с доступной полосы пропускания с остальным трафиком.*

10.1.7. Группы каналов

Система NetDefendOS обеспечивает дополнительный уровень управления каналами благодаря возможности разделить полосу пропускания канала между отдельными пользователями в рамках *группы* и применить для каждого пользователя ограничение и гарантию.

Можно выделить отдельных пользователей в соответствии с одним из следующих пунктов:

- IP-адрес источника (Source IP)

- IP-адрес назначения (Destination IP)
- Сеть источника (Source Network)
- Сеть назначения (Destination Network)
- Порт источника (Source Port) (подразумевает IP-адрес)
- Порт назначения (Destination Port) (подразумевает IP-адрес)
- Интерфейс источника (Source Interface)
- Интерфейс назначения (Destination Interface)

Данная функция активируется с помощью включения в канале опции *Grouping*. При этом отдельные пользователи получают возможность установить ограничение и/или гарантию, указанные для них в канале. Например, если создание групп выполняется по IP-адресу источника, то каждый *пользователь* соответствует одному уникальному IP-адресу источника.

Создание групп по порту подразумевает IP-адрес

Если выбрано создание групп по порту, то это также задействует IP-адрес. Например, порт 1024 компьютера А отличается от порта 1024 компьютера Б. В данном случае имеет место комбинация порта и IP-адреса, которые идентифицируют отдельного пользователя в группе.

При создании групп по сети требуется размер сети

Если выполняется создание групп по сети источника или назначения, то необходимо указать размер сети. Другими словами для сети в NetDefendOS необходимо указать маску подсети.

Указание групповых ограничений

После выбора метода создания группы необходимо указать **Групповые ограничения (Group Limits)**. Данные ограничения могут состоять из одного или двух следующих элементов:

- **Общее значение ограничения группы**

  Данное значение указывает ограничение для каждого пользователя в рамках создаваемой группы. Например, если создание группы выполняется по IP-адресу источника, и общее ограничение – 100 кбит/с, то это означает, что ни один IP-адрес не сможет получить более 100 Кбит/с полосы пропускания.

- **Гарантии групповых приоритетов**

  В качестве дополнения или альтернативы общему групповому ограничению можно задать определенные значения отдельным приоритетам. Эти значения в действительности являются *гарантиями* (не ограничениями) для каждого пользователя группы. Например, приоритет 3 может иметь значение 50 кбит/с, это означает, что каждому отдельному пользователю (другими словами, каждому IP-адресу источника, если выбрано создание группы именно по этому признаку) с этим приоритетом будет гарантировано 50 кбит/с за счет урезания трафика с более низким приоритетом.

  Приоритеты для каждого пользователя необходимо назначить с помощью различных правил каналов, которые срабатывают на отдельных пользователей. Например, если группа создается по IP-адресу источника, то различные правила каналов будут срабатывать на различные IP-адреса и отправлять трафик в один и тот же канал с заданным приоритетом.

  При некоторых обстоятельствах потенциальная сумма значений приоритетов может стать больше, чем пропускная способность канала, таким образом, при использовании данных гарантий важно указать величину общего ограничения канала.

Одновременное использование общего ограничения группы и приоритетов

Можно одновременно использовать групповые приоритеты и общее групповое значение. Это

означает, что:

- Пользователи в группе сначала разделяются правилами канала по приоритетам.
- Затем к пользователям применяются гарантии, указанные для их приоритета.
- Весь суммарный поток трафика подвергается общему групповому ограничению.

На рисунке ниже представлен поток трафика, который был распределен в группы по IP-адресу источника.

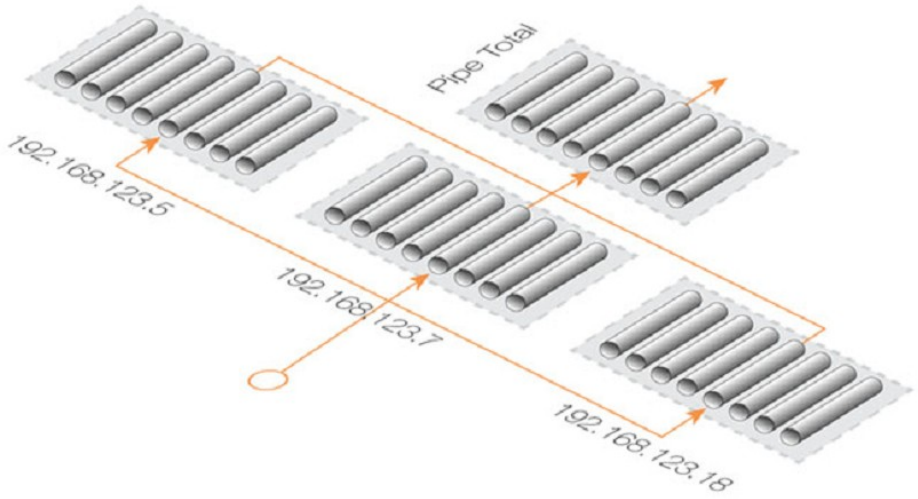


Рис. 10.6. Трафик, сгруппированный по IP-адресу

Другой пример использования групп

Рассмотрим другую ситуацию, в которой общее ограничение полосы пропускания канала составляет 400 бит/с. Если необходимо разделить эту полосу пропускания среди нескольких IP-адресов назначения таким образом, чтобы на отдельный IP-адрес приходилось не более 100 кбит/с полосы пропускания, необходимо выполнить следующие шаги:

- Задать обычным способом ограничение канала – 400 кбит/с.
- Установить в канале опцию **Grouping** в значении *Destination IP*.
- На вкладке **Group Limits** задать общее групповое значение канала – 100 кбит/с.

Теперь полоса пропускания распределяется по принципу живой очереди, однако, ни один IP-адрес назначения не сможет получить более 100 кбит/с. Независимо от количества подключений общая ширина полосы пропускания все же не сможет превысить ограничение для канала в 400 кбит/с.

Сочетание значений ограничений приоритетов каналов и групп

Предположим, что опция создания группы включена с помощью выбора одной из переменных, такой как IP-адрес источника и некоторые значения приоритетов были указаны на вкладке **Group Limits**. Как эти значения сочетаются со значениями, указанными для соответствующих приоритетов на вкладке **Pipe Limits**?

В данном случае значение приоритета на вкладке **Group Limits** является гарантией, а значение для того же приоритета на вкладке **Pipe Limits** является ограничением. Например, если трафик группируется по IP-адресу источника, и на вкладке **Group Limits** для приоритета 5 задано значение 5 Кбит/с, а на вкладке **Pipe Limits** приоритету 5 присвоено значение 20 Кбит/с, то после подключения четвертого уникального IP-адреса источника (4 x 5 = 20 Кбит/с) будет достигнуто ограничение

приоритета, и далее гарантии не будут предоставляться.

Динамическая балансировка

Вместо указания общего группового ограничения можно включить опцию *Dynamic Balancing*. Это обеспечивает одинаковое разделение полосы пропускания между всеми адресами независимо от их количества. Данное действие выполняется для ограничения канала.

Если при включенной опции динамической балансировки также задано общее групповое ограничение 100 бит/с, то это все равно означает, что ни один пользователь не сможет получить больше данной величины полосы пропускания.

Приоритеты и динамическая балансировка

Как отмечалось ранее, помимо указания общего ограничения группы можно указать ограничения для каждого приоритета в рамках группы. Если в групповых ограничениях для приоритета 2 мы указываем значение 30 кбит/с, то это означает, что пользователям с назначенным приоритетом 2 по правилу канала будет гарантировано 30 бит/с, независимо от количества пользователей, использующих канал. Так же как в случае обычных приоритетов канала, трафик, превысивший 30 кбит/с для пользователей с приоритетом 2, будет понижен до значения приоритета негарантированной доставки.

Продолжая предыдущий пример, мы можем установить ограничение на величину гарантированной полосы пропускания, которую получит каждый пользователь для входящего SSH-трафика. Это помешает одному пользователю занять всю доступную высокоприоритетную полосу пропускания.

Сначала мы создадим группу пользователей канала **ssh-in** таким образом, что ограничения будут применяться к каждому пользователю внутренней сети. Так как пакеты являются входящими, в качестве параметра для создания группы в настройках канала **ssh-in** мы выбираем опцию *Destination IP*.

Далее указываем ограничения для каждого пользователя, установив для приоритета 2 ограничение в 16 кбит/с на пользователя. Это означает, что каждый пользователь гарантированно получит не более 16 кбит/с для своего SSH-трафика. Если необходимо также можно ограничить общую ширину полосы пропускания группы для каждого пользователя, указав какое-либо значение, например, 40 Кбит/с.

Если более 5 пользователей одновременно используют SSH, возникнет проблема, так как 5 раз по 16 кбит/с – больше, чем 64 кбит/с. Общее ограничение канала продолжает действовать, и каждый пользователь будет конкурировать за доступную для приоритета 2 полосу пропускания таким же образом, как они конкурируют за полосу пропускания самого низкого приоритета. Некоторые пользователи по-прежнему получат свои 16 кбит/с, а некоторые нет.

Для улучшения ситуации можно включить динамическую балансировку, обеспечив каждому из 5 пользователей одинаковое количество полосы пропускания. Когда 5-ый пользователь начинает генерировать SSH-трафик, балансировка снизит пользовательское ограничение до 13 кбит/с (64 кбит/с, разделенные между 5 пользователями).

Динамическая балансировка выполняется в пределах каждого приоритета отдельно. Это означает, что если на всех пользователей выделено определенное, но небольшое количество трафика с высоким приоритетом и более широкая полоса пропускания для трафика негарантированной доставки (best-effort), все пользователи получат равные доли как высокоприоритетного графика, так и трафика негарантированной доставки.

10.1.8. Рекомендации по Traffic shaping

О важности ограничения канала

Функция Traffic shaping эффективна только в том случае, когда канал NetDefendOS *заполнен*. Другими словами, через канал проходит количество трафика, разрешенное значением общего ограничения. Если для канала установлено общее ограничение в 500 кбит/с, но в текущий момент времени по нему проходит 400 кбит/с трафика с низким приоритетом и 90 кбит/с высокоприоритетного трафика, то остается 10 кбит/с полосы пропускания, поэтому нет необходимости урезать какой-либо из типов трафика. Поэтому важно указать общее ограничение

для канала, таким образом, каналу известна пропускная способность и механизм приоритетов полностью зависит от него.

Ограничения каналов для VPN

Функция Traffic shaping измеряет количество трафика внутри VPN-туннелей. Используются незашифрованные данные без указания дополнительных данных какого-либо протокола, таким образом, трафик будет меньше по объему, чем фактический VPN-трафик. VPN-протоколы, например, IPsec, могут добавить значительный объем к исходным данным, и по этой причине рекомендуется установить ограничение для каналов для VPN-трафика примерно на 20% ниже доступной ширины полосы пропускания.

Особенность группового ограничения

Особым случаем является ситуация, когда общее ограничение канала не указано, и вместо этого используется групповое ограничение. Ограничение полосы пропускания назначается на каждого пользователя сети, например, в случае, если пользователи должны получать фиксированную долю от общей полосы пропускания. Провайдер услуг Интернет может использовать этот подход для ограничения полосы пропускания отдельного пользователя с помощью выбора опции «Destination IP» при создании группы. Информация о моменте заполнения канала не является важной, так как на каждого пользователя наложено ограничение. Если были задействованы приоритеты, то будет использоваться максимум канала.

Значения ограничений не должны превышать значения доступной полосы пропускания

Если заданное ограничение канала выше, чем доступная полоса пропускания, каналу не будет известно, что скорость соединения достигла своих физических возможностей. Если физический предел полосы пропускания 500 кбит/с, но в качестве общего ограничения канала указано 600 кбит/с, канал будет полагать, что он не заполнен и поэтому не будет урезать низкоприоритетный трафик.

Значения ограничений должны быть немного ниже значения доступной полосы пропускания

Ограничения каналов должны быть немного ниже ширины полосы пропускания сети. Рекомендуемым значением ограничения канала является 95% от общего физического ограничения. Необходимость этой разницы уменьшается по мере увеличения полосы пропускания, так как 5% представляют собой все более увеличивающуюся долю общей ширины полосы пропускания.

Причина понижения значения ограничения канала связана с методами обработки трафика системой NetDefendOS. Для исходящих соединений, когда пакеты отправляются межсетевым экраном NetDefend, всегда существует возможность, что NetDefendOS может немного перегрузить соединение, так как программные модули, вовлеченные в решение задачи по отправке пакетов, работают с некоторыми задержками, фактически отправляемых из буферов.

При входящих соединениях требуется меньше контроля над входящими пакетами и пакетами, которые должны быть обработаны подсистемой Traffic shaping и поэтому более важно задать ограничения канала немного ниже существующего ограничения соединения, учитывая время, необходимое системе NetDefendOS для адаптации к изменяющимся условиям.

Атаки на полосу пропускания

Traffic shaping не защищает от входящих атак, расходующих ресурсы, например, атаки DoS или другие flood-атаки. NetDefendOS препятствует тому, чтобы эти посторонние пакеты достигли хостов за межсетевым экраном NetDefend, но не может защитить соединение от перегрузки, если действуют flood-атаки.

Отслеживание утечек

Намереваясь применить защиту и Traffic shaping в самом «узком месте» сети, убедитесь, что весь трафик, проходящий через «узкое место», также проходит через определенные каналы NetDefendOS.

Если трафик проходит через Интернет-подключение, неизвестное каналам, то они не смогут определить, когда Интернет-соединение достигло своего максимума.

Проблемы, возникающие по причине утечек, аналогичны проблемам, описанным выше. Трафик, проходящий в обход каналов, попадает на участок полосы пропускания, находящийся вне

административного контроля, но будет оставаться частью текущего соединения.

Решение проблем

Для лучшего понимания того, что происходит при заданных установках, используется консольная команда:

```
gw-world:/> pipe -u <pipename>
```

Данная команда также используется для отображения списка текущих активных пользователей в каждом канале.

10.1.9. Краткая информация по Traffic shaping

Подсистема Traffic shaping NetDefendOS предоставляет набор инструментов для управления и приоритезации сетевых пакетов. Следующие пункты являются общими принципами работы данного механизма:

- Необходимо выбрать трафик, обрабатываемый с помощью *правил канала* (Pipe Rules).
- Правила канала отправляют трафик через *каналы* (Pipes).
- Канал может иметь ограничение, определяющее максимальное количество разрешенного трафика.
- Канал может определить, что он *заполнен*, только если указано его ограничение.
- Одиночный канал должен обрабатывать трафик только в одном направлении (хотя допустимы двунаправленные каналы).
- Каналы могут быть объединены в цепочки, таким образом, трафик из одного канала переходит в другой.
- Определенные типы трафика в канале получают *приоритет*.
- Приоритетам может быть присвоено максимальное ограничение, которое также является гарантией. Трафик, превысивший это ограничение, будет отправлен с минимальным приоритетом, который также называется *приоритетом негарантированной доставки* (Best Effort).
- Все пакеты с приоритетом негарантированной доставки (best effort) обрабатываются в порядке живой очереди.
- В пределах канала трафик может быть разделен с использованием настройки *группы* (Group). Например, по IP-адресу источника. Каждый пользователь в группе (например, каждый IP-адрес источника) может получить максимальное ограничение и приоритеты, группе могут быть заданы ограничение/гарантия.
- Нет необходимости задавать ограничение канала, если указано максимальное ограничение для участников группы.
- *Динамическая балансировка* может использоваться для указания того, что все пользователи в группе получают одинаковое количество полосы пропускания.

10.1.10. Дополнительные примеры использования каналов

Данный раздел рассматривает некоторые дополнительные сценарии и использование Traffic shaping для решения отдельных проблем.

Основной сценарий

В первом сценарии рассматривается настройка, изображенная на рисунке ниже, где входящий и исходящий трафик ограничен до 1 мегабита в секунду.

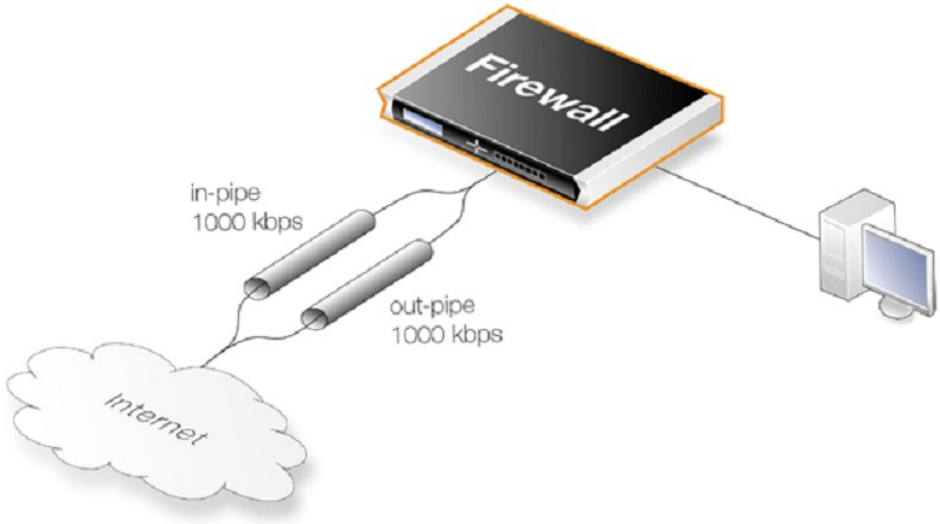


Рис. 10.7. Основной сценарий Traffic Shaping

В данном случае причина использования 2 различных каналов заключается в том, что они в большей степени соответствуют физическим характеристикам пропускной способности соединения. Это наиболее применимо к асинхронным соединениям, например, ADSL.

Сначала необходимо создать 2 канала *in-pipe* и *out-pipe* со следующими параметрами:

Pipe Name	Min Prec	Def Prec	Max Prec	Grouping	Net size	Pipe limit
in-pipe	0	0	7	PerDestIP	24	1000kb
out-pipe	0	0	7	PerSrcIP	24	1000kb

Для обоих каналов необходимо включить функцию **динамической балансировки**. Вместо *PerDestIP* и *PerSrcIP* можно использовать *PerDestNet* и *PerSrcNet* при наличии нескольких сетей.

Следующим шагом является создание Правила канала, которое направит трафик в созданные каналы.

Rule Name	Forward Pipes	Return Pipes	Source Interface	Source Network	Destination Interface	Destination Network	Service
all_1mbps	out-pipe	in-pipe	lan	lannet	wan	all-nets	all

Правило направит весь трафик в каналы, присвоив ему уровень приоритета по умолчанию, и каналы ограничат общий трафик до 1 Мбит/с. Наличие включенной функции **динамической балансировки** означает, что заданная пропускная способность будет равномерно распределена между всеми пользователями.

Использование нескольких приоритетов

Усложним предыдущий пример, назначив приоритеты различным типам Интернет-трафика, идущего из главного офиса.

Предположим, что имеем симметричный 2/2 Мбит/с канал доступа к Интернет. Распределим приоритеты и потребление трафика следующим образом:

- **Приоритет 6** – VoIP (500 кбит/с)
- **Приоритет 4** – Citrix (250 кбит/с)
- **Приоритет 2** – Остальной трафик (1000 кбит/с)
- **Приоритет 0** – Web и остаточный трафик с других уровней

Для реализации этой схемы мы можем использовать *in-pipe* и *out-pipe*. Сначала вводим *ограничения канала* (Pipe Limits) для каждого канала. Эти ограничения основаны на списке выше:

- **Приоритет 6** – *500*
- **Приоритет 4** – 250
- **Приоритет 2** – 1000

Далее создаем *Правила каналов*:

Rule Name	Forward Pipes	Return Pipes	Source Interface	Source Network	Dest Interface	Dest Network	Selected Service	Precedence
web_surf	out-pipe	in-pipe	lan	lannet	wan	all-nets	http_all	0
voip	out-pipe	in-pipe	lan	lannet	wan	all-nets	H323	6
citrix	out-pipe	in-pipe	lan	lannet	wan	all-nets	citrix	4
other	out-pipe	in-pipe	lan	lannet	wan	all-nets	All	2

Данные правила обрабатываются сверху вниз и с их помощью каждой указанной *Службе* будет присвоен свой приоритет. Возможно, сначала потребуется создать особые пользовательские службы, чтобы идентифицировать отдельные типы трафика. Служба *all* перехватывает любой трафик, который идет в обход вышеуказанных правил, поскольку важно, чтобы ни один тип трафика не обходил набор правил каналов, в противном случае используемые каналы не будут работать.

Объединение каналов в цепочки

Предположим, что необходимо ограничить пропускную способность приоритета 2 (остальной трафик) до 1000 кбит/с, таким образом, чтобы значение приоритета не понижалось до 0. Это выполняется с помощью *объединения каналов в цепочки*, для чего мы создаем новые каналы *in-other* и *out-other* и для них обоих задаем *ограничение канала* (Pipe Limit) со значением 1000. Далее модифицируем правило каналов для остального трафика следующим образом:

Rule Name	Forward Pipes	Return Pipes	Source Interface	Source Network	Dest Interface	Dest Network	Selected Service	Precedence
other	out-other out-pipe	in-other in-pipe	lan	lannet	wan	all-nets	All	2

Обратите внимание на то, что каналы *in-other* и *out-other* стоят первыми в цепочке каналов в обоих направлениях. Причина этого заключается в необходимости ограничить трафик до того, как он попадет в каналы *in-pipe* и *out-pipe* и начнет конкурировать с трафиком VoIP, Citrix и трафиком, расходуемым на просмотр страниц.

Сценарий VPN

В вышеуказанных случаях Traffic shaping выполняется внутри одного межсетевого экрана NetDefend. Как правило, VPN используется для обмена информацией между главным офисом и филиалами, в данном случае каналы могут управлять потоком трафика в обоих направлениях. VPN – это туннель, который является интерфейсом назначения и источника для правил канала.

Важным моментом, который уже обсуждался ранее, является то, что при задании общего ограничения канала необходимо учесть величину дополнительных данных, используемых VPN-протоколом. Как правило, целесообразно установить общее ограничение канала в 1700 кбит/с для VPN-туннеля с общей физической пропускной способностью соединения в 2 Мбит/с.

Также важно помнить о необходимости направления в канал всего трафика, который не является VPN, использующим одно и то же физическое соединение.

Для решения проблемы дополнительных данных VPN используется *объединение каналов в цепочку*. Для трафика VPN-туннеля устанавливается допустимое ограничение на эти дополнительные данные, а трафик, который не является VPN-трафиком направляется в канал, ширина которого соответствует скорости физического соединения.

Для этого сначала необходимо создать отдельные каналы для исходящего и входящего трафика. VoIP-трафик будет отправлен через VPN-туннель с высоким приоритетом. Весь остальной трафик будет отправлен с *приоритетом негарантированной доставки* (best effort). Предположим снова, что имеем симметричное соединение 2/2 Мбит/с.

Необходимые каналы:

- **vpn-in**
  - *Приоритет 6*: VoIP (500 кбит/с)
  - *Приоритет 0*: Best Effort

  Total: 1700
- **vpn-out**
  - *Приоритет 6*: VoIP 500 кбит/с
  - *Приоритет 0*: Best Effort

  Total: 1700
- **in-pipe**
  - *Приоритет 6*: VoIP 500 кбит/с

  Total: 2000
- **out-pipe**
  - *Приоритет 6*: VoIP 500 кбит/с

  Total: 2000

Для направления трафика в корректные каналы с необходимыми уровнями приоритетов требуются следующие правила:

Rule Name	Forward Pipes	Return Pipes	Src Int	Source Network	Dest Int	Destination Network	Selected Service	Precedence
vpn_voip_out	vpn-out out-pipe	vpn-in in-pipe	lan	lannet	vpn	vpn_remote_net	H323	6
vpn_out	vpn-out out-pipe	vpn-in in-pipe	lan	lannet	vpn	vpn_remote_net	All	0
vpn_voip_in	vpn-in in-pipe	vpn-out out-pipe	vpn	vpn_remote_net	lan	lannet	H323	6
vpn_in	vpn-in in-pipe	vpn-out out-pipe	vpn	vpn_remote_net	lan	lannet	All	0
out	out-pipe	in-pipe	lan	lannet	wan	all-nets	All	0
in	in-pipe	out-pipe	wan	all-nets	lan	lannet	All	0

Благодаря данной настройке на весь VPN-трафик накладывается ограничение до 1700 кбит/с, на общий трафик ограничение до 2000 кбит/с и VoIP-соединение с удаленной сетью гарантированно получает 500 кбит/с от пропускной способности, все что выше этих 500 кбит/с будет понижено до приоритета негарантированной доставки.

Использование SAT с каналами

Если используется SAT, например, для Web- или FTP-сервера, необходимо направить трафик в каналы, в противном случае он обойдет Traffic shaping и тем самым нарушит запланированную систему QoS. Помимо этого, инициация соединения с сервером выполняется с внешней стороны, поэтому направление каналов необходимо изменить в обратную сторону: прямым каналом будет канал *in-pipe,* а обратным – *out-pipe.*

Простым решением является помещение правила «catch-all-inbound», отвечающего за обработку всего входящего трафика, ниже основного правила каналов. Тем не менее, чтобы избежать помещения в каналы трафика, исходящего из внутренней сети и направленного к внешним IP-адресам, в качестве интерфейса источника должен быть указан внешний интерфейс (wan). Поэтому последнее правило должно выглядеть следующим образом:

Rule Name	Forward Pipes	Return Pipes	Source Interface	Source Network	Dest Interface	Dest Network	Selected Service	Precedence
all-in	in-pipe	out-pipe	wan	all-nets	core	all-nets	All	0

Примечание: SAT и IP-адреса из ARP-таблицы

Если SAT использует IP-адреса, принудительно прописанные в ARP-таблице, то в качестве интерфейса назначения должен быть указан интерфейс ***wan.***

Д

10.2. Traffic Shaping на основе IDP

10.2.1. Обзор

Назначением функции Traffic Shaping на основе IDP является управление трафиком, основанное на информации, поступающей от подсистемы *обнаружения и предотвращения вторжений* (Intrusion Detection and Prevention, IDP) NetDefendOS (за дополнительной информацией см. *Раздел 6.5, «Обнаружение и предотвращение вторжений»*).

Проблема использования полосы пропускания

Основной задачей Traffic Shaping на основе IDP является решение проблем в управлении трафиком, связанных с ресурсоемкими приложениями. Типичным примером этого является трафик, генерируемый приложениями, работающими по протоколам peer-to-peer (P2P), например, такими как *Bit Torrent* и *Direct Connect*.

Перегрузки трафика, создаваемые P2P-соединениями, могут негативно повлиять на качество обслуживания остальных пользователей сети. Поэтому провайдеру или администратору корпоративной сети необходимо контролировать полосу пропускания, занимаемой этими приложениями, и Traffic Shaping на основе IDP предоставляет такую возможность.

Объединение IDP и Traffic Shaping

Одной из проблем, связанных с управлением такого типа трафика как P2P, является возможность отличить его от другого трафика. Сигнатурные базы NetDefendOS уже предоставляют высокоэффективные средства для выполнения такого опознавания, а в качестве дополнения к этому NetDefendOS также предоставляет возможность применить принудительное урезание полосы пропускания с помощью подсистемы Traffic shaping NetDefendOS после того, как целевой трафик опознан.

Traffic Shaping на основе IDP – это комбинация двух функций, где потоки трафика, идентифицированные подсистемой IDP, автоматически направляются в заданные каналы подсистемы Traffic shaping для управления данными потоками.

10.2.2. Настройка Traffic Shaping на основе IDP

Для установки Traffic Shaping на основе IDP выполните следующие шаги:

1. **Укажите IDP-правило, которое будет реагировать на целевой трафик.**

Выбранная IDP-сигнатура определяет, какой трафик будет целевым, и имя сигнатуры, как правило, содержит слово «*POLICY*», которое указывает на связь с определенными типами приложений.

2. **В качестве действия для правила выберите опцию *Pipe*.**

Указывает на то, что к соединению, на которое реагирует правило, и к последующим зависимым соединениям будет применена функция Traffic Shaping на основе IDP.

3. **Укажите в правиле значение ширины полосы пропускания.**

Это величина общей полосы пропускания, которая будет доступна для целевого трафика. Данное количественное значение трафика является суммой потоков, проходящих через соединение, вызвавшее срабатывание правила, и любых зависимых соединений независимо от направления потока.

Соединения, открытые до срабатывания IDP, не будут подвержены ограничению.

4. **Введите временной интервал в секундах (дополнительно).**

Это период времени после срабатывания правила, в течение которого Traffic shaping применяется ко всем открытым зависимым соединениям.

Как правило, передача данных по P2P-протоколу начинается с предварительного соединения для передачи контрольной информации, за которым следует несколько соединений с передачей данных на другие хосты.

Именно это предварительное соединение определяется IDP, а *временной интервал* определяет предположительный период, в течение которого будут открыты другие соединения, которые необходимо подвергнуть действию Traffic shaping. Соединения, открытые после истечения *временного интервала*, больше не подвергаются действию Traffic shaping.

Временной интервал равный 0 означает, что под действие Traffic shaping попадает только трафик, проходящий через предварительное соединение, вызвавшее срабатывание правила. Любые другие зависимые соединения, которые не вызывают срабатывания IDP-правила не будут подвергаться Traffic shaping.

5. **Укажите диапазон *сети* (дополнительно)**

Если *временной интервал* больше 0, можно задать целевую *сеть*. Этот диапазон IP-адресов разрешает администратору более точно определить последующие соединения, ассоциируемые с применяемым IDP-правилом, которые будут подвергнуты действию Traffic shaping. Для того чтобы попасть под действие Traffic shaping, хотя бы одна из сторон зависимого соединения должна находиться в заданном диапазоне IP-адресов.

10.2.3. Обработка потока

Рассмотрим следующие этапы, происходящие при обработке, для того, чтобы лучше понять, как применяется Traffic Shaping на основе IDP:

1. Открыто новое соединение между двумя хостами через межсетевой экран NetDefend, и начинается прохождение трафика. Система NetDefendOS фиксирует IP-адрес источника и назначения.

2. Трафик запускает IDP-правило. В качестве действия в IDP-правиле выбрано «*Pipe*», таким образом, трафик данного соединения теперь является объектом Traffic Shaping относительно трафика канала, полоса пропускания которого задана в IDP-правиле.

3. Далее устанавливается новое соединение, которое не запускает правило IDP, но у которого тот же IP-адрес назначения и источника, что и у соединения, запустившего правило. Если адрес источника или назначения является участником диапазона IP-адресов, заданного в поле *Network*, то трафик направляется в канал, в котором выполняется Traffic shaping первичного соединения, включившего правило.

   Если значение *Network* не указано, то данное новое соединение будет также направлено в канал с трафиком соединения, запустившего правило, что адреса источника и назначения одинаковые.

10.2.4. Важность указания сети

Каждая сторона может запустить IDP

Прочитав вышеуказанное описание обработки потока, можно убедиться в важности указания сети. Подсистема IDP не может знать, какая из сторон запустила правило. Иногда инициатором является клиент, а иногда отвечающий сервер. Если прохождение трафика с обеих сторон становится затруднительным, возможно, причина в непреднамеренном воздействии Traffic shaping на соединения, которые не должны подвергаться обработке.

Непреднамеренное воздействие

Рассмотрим ситуацию, когда клиент А подключается к хосту Х по P2P-протоколу и запускает IDP ID-правило, в котором в качестве действия задано *Pipe*, таким образом, данное соединение становится объектом для Traffic shaping. Теперь, если другой клиент Б также подключается к хосту Х, но по HTTP-протоколу, правило IDP не запускается, и соединение не должно быть подвергнуто действию Traffic shaping наряду с соединением клиента А на основании того, что вовлечен хост Х.

Исключение хостов

Для того чтобы избежать непреднамеренного воздействия, мы указываем IP-адреса клиента А и клиента Б в диапазоне поля *Network*, а IP-адрес хоста Х не указываем. При этом система NetDefendOS проинформирована о том, что хост Х не является причиной для принятия решения о включении новых соединений, не отвечающих непосредственно за срабатывание IDP-правила, в Traffic shaping.

Возможно, указание адреса клиента Б в сетевом диапазоне может показаться нелогичным, но это выполняется на предположении, что клиент Б является пользователем, чей трафик также может быть подвержен действию Traffic shaping, если он участвует в передаче данных по P2P.

Если сеть не задана, то любое соединение с участием либо клиента А, либо хоста Х будет объектом для Traffic shaping, что, возможно, окажется нежелательным.

10.2.5. Сценарий P2P

Схема, представленная ниже, отображает типичный сценарий с использованием передачи данных по P2P-протоколу. Последовательность событий выглядит следующим образом:

- Клиент с IP-адресом *192.168.1.15* инициирует передачу файлов по P2P-протоколу через соединение (1) с сервером Tracking server с адресом *81.150.0.10*.

- Данное соединение запускает IDP-правило NetDefendOS, связанное с сигнатурой IDP, целевыми объектами для которой являются P2P-приложения.

- Действие *Pipe* в правиле создает канал Traffic shaping с заданной пропускной способностью, и соединение направляется в этот канал.

- Последующее зависимое соединение (2) с файл-хостом 92.92.92.92 выполняется в пределах временного интервала IDP-правила, поэтому трафик данного соединения направлен в канал и подвергается действию Traffic shaping.

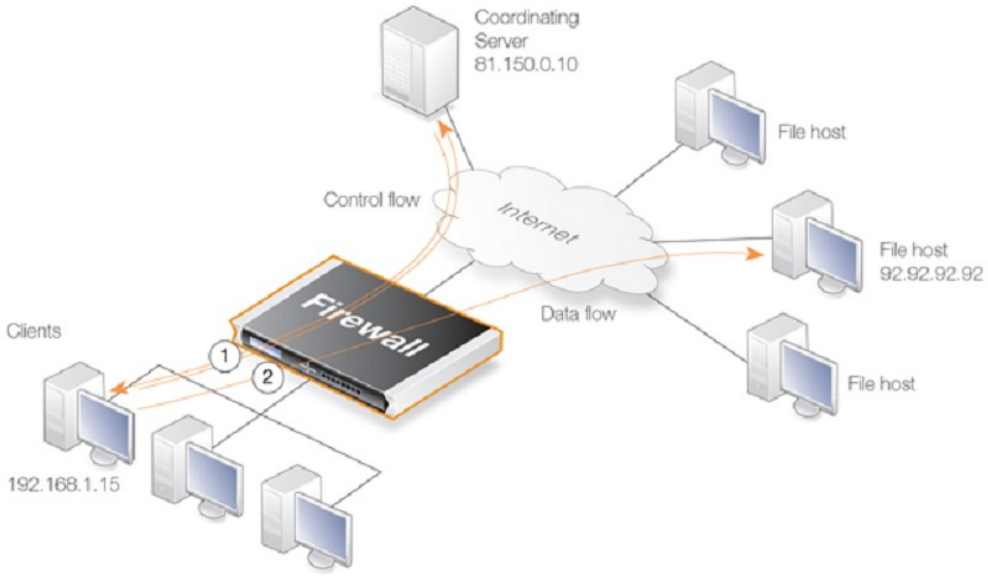


Рис. 10.8. Traffic shaping на основе IDP в сценарии P2P

10.2.6. Обзор объектов Traffic Shaping

Обзор хостов

Traffic shaping на основе IDP поддерживает специальную команду CLI, которая называется *idppipes,*и с помощью которой можно осуществлять наблюдение и управление хостами, являющимися в данный момент объектами для Traffic shaping .

Для отображения всех хостов, подвергающихся действию Traffic shaping посредством IDP, используется следующая команда:

```
gw-world:/> idppipes -show

Host         kbps Tmout
------------ ---- ----
192.168.1.1   100   58
```

Хост, в данном случае с IP-адресом 192.168.1.1, может быть удален из обработки Traffic shaping с помощью команды:

```
gw-world:/> idppipes -unpipe -host=192.168.1.1
```

Полное описание команды *idppipes* находится в отдельном *Руководстве по интерфейсу командной строки CLI*.

Обзор каналов

Traffic Shaping на основе IDP использует стандартные каналы NetDefendOS, которые создаются автоматически. Эти каналы всегда получают наивысший приоритет и для Traffic Shaping используют особенности *групповой* настройки.

Тем не менее, созданные каналы не видны администратору при просмотре текущих заданных объектов Traffic Shaping через Web-интерфейс, но их обзор и управление можно выполнить с

помощью команды CLI *pipes*. Например, для отображения всех текущих указанных каналов используется следующая команда CLI:

```
gw-world:/> pipes -show
```

Каналы Traffic Shaping на основе IDP можно определить по характерной системе наименований, речь о которой пойдет ниже.

Система наименований каналов

Система NetDefendOS автоматически назначает имена каналам, создаваемых для Traffic Shaping посредством IDP, используя шаблон *IDPPipe_<bandwidth>* для каналов с исходящим (прямым) трафиком и *IDPPipe_<bandwidth>R* для каналов с входящим (обратным) трафиком. Если происходит дублирование имени, то в конце имени канала прибавляется цифровое окончание.

Например, первые каналы, созданные с ограничением 1000 кбит/с будут называться *IDPPipe_1000* для исходящего трафика и *IDPPipe_1000R* для входящего трафика. Дубликаты с таким же ограничением полосы пропускания получают имена *IDPPipe_1000_(2)* и *IDPPipe_1000R_(2)*. Если появится еще один набор дубликатов, в конце имени используется окончание *(3)*.

Совместно используемые каналы

Количество запусков IDP-правила не равно количеству созданных каналов. Для каждой заданной величины ширины полосы пропускания создается два канала: один для исходящего (прямого) трафика, а другой для входящего (обратного). Несколько хостов используют один и тот же канал каждого направления, трафик во входящем канале сгруппирован с использованием опции «Per Source IP», а трафик во входящем канале сгруппирован с помощью опции «Per Destination IP».

10.2.7. Гарантирование полосы пропускания вместо ограничения

При необходимости Traffic Shaping на основе IDP в отношении определенных приложений может использоваться для действия, противоположного ограничению полосы пропускания.

Если администратору необходимо гарантировать полосу пропускания, например, 10 Мегабит, для приложения, то можно настроить IDP-правило для срабатывания на данное приложение с последующим действием Pipe с заданным значением требуемой полосы пропускания. В этом случае автоматически созданные каналы Traffic shaping по умолчанию получают наивысший приоритет, и поэтому полоса пропускания будет гарантированной.

10.2.8. Ведение журнала

Traffic Shaping на основе IDP создает сообщения для записи в журнал в связи со следующими событиями:

- Если запущено IDP-правило с действием Pipe, при этом хост или клиент указаны в диапазоне *Network*
- Если подсистема добавляет хост, будущие соединения которого будут заблокированы.
- После истечения временного интервала, в течение которого в канал направлялись новые зависимые соединения, созданное сообщение журнала указывает, что новые соединения с хостом или от него далее не будут направляться в канал.

Также существуют и другие сообщения, которые указывают на специфические ситуации. Информация обо всех вариантах сообщений содержится в *Руководстве по журналу*.

10.3. Правила порога

10.3.1. Обзор

Основной целью применения *Правил порога* является обнаружение аварийного соединения, а также указание действий, которые необходимо предпринять. Например, причиной аварийного соединения активности может быть внутренний хост, зараженный вирусом, который отправляет на внешние IP-адреса повторяющиеся запросы на соединения. Также причиной аварийного соединения может быть внутренний источник, пытающийся установить большое количество соединений. (Термин «соединение» в данном контексте относится ко всем типам соединений, включая TCP, UDP или ICMP, отслеживаемых механизмом состояний NetDefendOS).

Примечание: Не все модели NetDefend поддерживают Правила порога

Правила порога поддерживают только модели DFL-800, 860, 1600, 1660, 2500, 2560 и 2560G.

Политики порога

Правило порога, как и другая политика NetDefendOS, представляет собой комбинацию сеть/интерфейс источника/назначения и может быть указана для правила и типа службы, например, HTTP. У каждого правила есть связанные с ним **Действия**, одно или более, которые определяют методы обработки различных условий порога.

Правило порога поддерживает следующие, связанные с ним параметры:

- **Action (Действие)**

  Это ответ правила при превышении ограничения. Можно выбрать либо опцию **Audit,** либо **Protect**.

- **Group by (Группировать по)**

  Правило создания группы по следующему признаку: **Host** или **Network**.

- **Threshold (Порог)**

  Числовое ограничение, при превышении которого выполняется запуск действия.

- **Threshold Type (Тип порога)**

  Можно указать правило либо для ограничения количества соединений в секунду, либо для ограничения общего количества одновременных соединений.

Данные параметры описаны ниже.

10.3.2. Ограничение скорости соединения/общего количества соединений

Ограничение скорости соединения

Ограничение скорости соединения позволяет администратору ограничить количество новых соединений в секунду, открытых для межсетевых экранов NetDefend.

Ограничение общего количества соединений

Ограничение общего количества соединений позволяет администратору ограничить общее количество соединений, открытых для межсетевых экранов NetDefend.

Эта функция особенно полезна, если из-за большого количества соединений, установленных P2P-пользователями, требуются пулы NAT.

10.3.3. Создание групп

Существует два типа создания групп:

- **Host Based** (На основе хоста) – Порог применяется к отдельным соединениям, установленным с различных IP-адресов.
- **Network Based** (На основе сети) – Порог применяется ко всем соединениям в соответствии с правилами.

10.3.4. Действия правила

При запуске Правила порога возможен один из следующих ответов:

- **Audit** – Оставляет соединение неактивным, но регистрирует событие.
- **Protect** – Отбрасывает установленное соединение.

Ведение журнала предпочтительнее в случае, если время запуска невозможно указать заранее. Для данного порога можно выполнить несколько действий *Audit,* в то время как для более высокого значения порога выполняется действие *Protect*.

10.3.5. Запуск нескольких действий

При запуске правила система NetDefendOS выполняет Действия связанные с правилом в зависимости от произошедших условий. Если необходимо выполнить более одного Действия, то эти Действия применяются в порядке их появления в интерфейсе пользователя.

Если несколько Действий, у которых одинаковая комбинация **Type** и **Grouping** (определения данных терминов указаны выше) запущены одновременно, будет зарегистрировано только Действие с самым высоким значением порога.

10.3.6. Соединения, освобожденные от проверки

Следует отметить, что с помощью некоторых расширенных настроек, известных как настройки *Before Rules*, можно освободить некоторые типы соединений для удаленного управления от проверки набором IP-правил NetDefendOS, если они включены. С помощью данных настроек *Before Rules*

можно исключить соединения из Правил порога, если они включены.

10.3.7. Правила порога и ZoneDefense

Правила порога используются в функции D-Link ZoneDefense для блокировки источника большого количества соединений с внутренних хостов. За подробной информацией обратитесь к *Главе 12, ZoneDefense*.

10.3.8. «Черный» список правил порога

Если используется опция *Protect,* можно назначить Правила порога таким образом, чтобы источник, запустивший правило, автоматически добавлялся в *«Черный» список* IP-адресов или сетей. Если одновременно запущено несколько Действий *Protect* с включенной функцией «черного» списка, система NetDefendOS выполняет только первое Действие, запустившее «черный» список.

Действие на основе хоста с включенной функцией «черного» списка занесет при запуске в «черный» список один хост. Действие на основе сети с включенной функцией «черного» списка занесет в «черный» список сеть источника, связанного с правилом. Если Правило порога связано со службой, то можно заблокировать только эту службу.

После включения функции «черный» список, администратор может либо завершить уже существующие соединения с источника, не зараженного вирусом, либо, в качестве альтернативы, выбрать соединения, отброшенные системой NetDefendOS.

Помимо этого, можно установить количество времени (в секундах) для помещения источника в «черный» список.

Эта функция подробно описана в *Разделе 6.7, «Хосты и сети в «черном» списке»*.

10.4. Балансировка нагрузки сервера

10.4.1. Обзор

Функция *SLB* (Server Load Balancing) позволяет администратору рассылать запросы приложений клиента большому количеству серверов, используя IP-правила с *Действием SLB_SAT*.

SLB - это мощный инструмент, который может улучшить следующие аспекты сетевых приложений:

- Производительность
- Масштабирование
- Надежность
- Удобство администрирования

Основным преимуществом SLB является распределение нагрузки между несколькими серверами, что значительно улучшает не только производительность приложений, но и масштабирование с помощью кластера серверов (иногда именуемого *server farm*), который может обрабатывать гораздо большее количество запросов, чем один сервер.

Примечание: Не все модели NetDefend поддерживают SLB

Функция SLB доступна только на моделях DFL-800, 860, 1600, 1660, 2500,

2560 и 2560G.

Иллюстрация ниже отображает типичный сценарий SLB, с наличием Интернет-доступа внешних клиентов к приложениям внутреннего сервера.

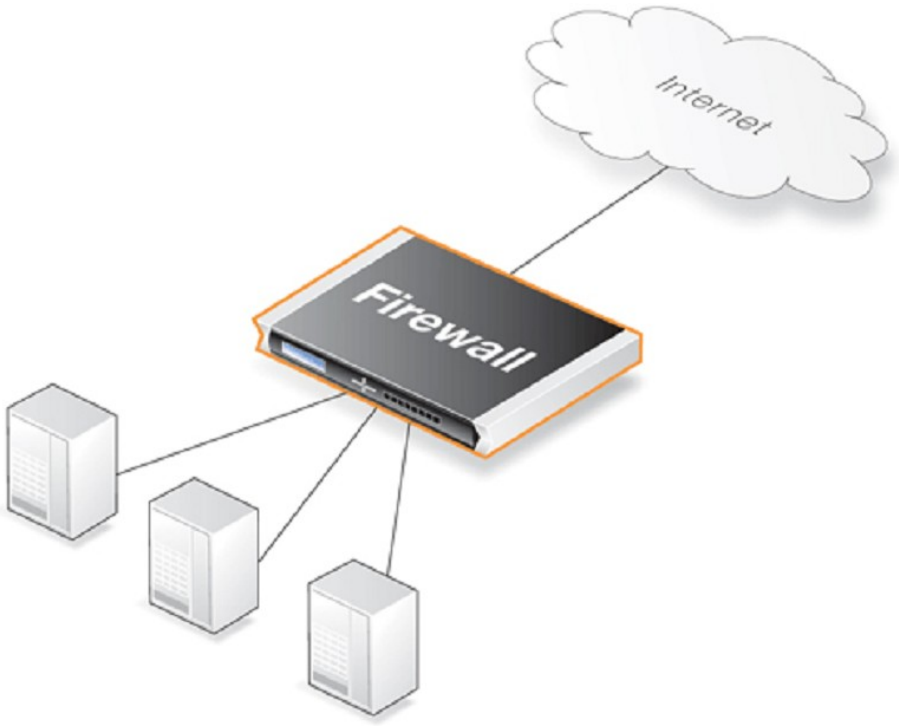


Рис. 10.9. Настройка балансировки нагрузки сервера

Дополнительные преимущества SLB

Помимо повышения производительности и масштабирования SLB предоставляет и другие преимущества:

- SLB увеличивает надежность сетевых приложений благодаря активному мониторингу серверов, между которыми распределена нагрузка. NetDefendOS SLB может определить момент сбоя или перегрузки сервера и больше не отправлять запросы на это сервер до тех пор, пока он не будет восстановлен или снизится нагрузка.

- SLB позволяет сетевым администраторам выполнять различные задачи на серверах или приложениях без влияния на службы. Можно перезапустить, обновить, удалить или заменить индивидуальные серверы и добавить или удалить новые серверы или приложения без влияния на серверы, оставшиеся в кластере или снижения работоспособности приложений.

- Комбинация из сетевого мониторинга и распределенной между серверами общей нагрузки также обеспечивает дополнительный уровень защиты от атак *DoS* (Denial Of Service).

Принципы распределения SLB

При распределении SLB следует помнить о следующем:

- Между какими серверами распределяется нагрузка

- Какой алгоритм SLB используется

- Будет ли использоваться привязка (stickiness)
- Какой метод мониторинга будет использоваться

Каждый из этих пунктов подробно описан в следующем разделе.

Идентификация серверов

Первым важным шагом при распределении SLB является идентификация серверов, между которыми распределяется нагрузка. Это может быть кластер серверов, также называемый *server farm*, представляющий собой группу серверов, настроенных как один «виртуальный сервер». Необходимо указать серверы, которые обрабатываются SLB как один виртуальный сервер.

10.4.2. Алгоритмы распределения SLB

Существует несколько способов распределения нагрузки между серверами. NetDefendOS SLB поддерживает два следующих алгоритма для распределения нагрузки:

Round-robin

Алгоритм распределяет новые входящие соединения между серверами в списке на основе поочередности. Для первого соединения алгоритм выбирает сервер методом случайного отбора и назначает ему соединение. Для последовательных соединений алгоритм перенаправляет нагрузку на серверы по порядку. Несмотря на возможности каждого сервера и другие аспекты, например, количество существующих соединений на сервере или время его ответа, последовательные соединения отправляются на все доступные серверы по очереди.

Данный алгоритм гарантирует, что все серверы получат одинаковое количество запросов, поэтому он является наиболее подходящим для кластеров серверов, где все серверы обладают одинаковыми возможностями и обрабатывают почти одинаковое количество запросов.

Connection-rate

Данный алгоритм рассматривает количество запросов, которое каждый сервер получает в течение определенного промежутка времени. Данный период времени известен как «*Window Time*». SLB отправляет следующий запрос на сервер, который получил наименьшее количество запросов в течение последнего периода времени «*Window Time*» (в секундах).

«*Window Time*» – это настройка, которую администратор может изменить. Значение по умолчанию – *10* секунд.

10.4.3. Привязка соединения к определенному адресу (Stickiness)

В некоторых сценариях, например, SSL-соединения, очень важно, чтобы для последовательных соединений использовался один и тот же сервер. Это выполняется за счет опции привязки соединения к определенному адресу *(Stickiness)*, которая может использоваться как с алгоритмом round-robin, так и с алгоритмом connection-rate. Опции «Stickiness» выглядят следующим образом:

Per-state Distribution

Данный режим используется по умолчанию и означает, что опция «Stickiness» не применяется. Каждое новое соединение не зависит от остальных соединений, даже если установлено с одного и того же IP-адреса или сети. По этой причине последующие соединения, установленные одним и тем же клиентом, могут передаваться на различные серверы.

	Данный режим не подходит для применения, если необходимо использовать один и тот же сервер для последовательных соединений, установленных одним и тем же клиентом. В таком случае необходимо использовать опцию «Stickiness».
IP Address Stickiness (Привязка к IP-адресу)	При использовании данного режима последовательные соединения, установленные определенным клиентом, будет отправлены на один и тот же сервер. Это особенно важно для служб на основе TLS и SSL, например, HTTPS, которым требуется повторное соединение с одним и тем же хостом.
Network Stickiness (Привязка к сети)	Данный режим аналогичен режиму IP stickiness за исключением того, что привязка может ассоциироваться с сетью вместо одного IP-адреса. Для сети в качестве параметра указан ее размер. Например, если для размера сети указано значение *24* (по умолчанию), то предположительно IP-адрес *10.01.01.02* будет относиться к сети *10.01.01.00/24*, к которой и будет применяться привязка.

Параметры привязки

Если включена опция «Привязка соединения к IP-адресу» (IP stickiness) или «Привязка к сети» (Network stickiness), то необходимо указать следующие параметры:

- **Idle Timeout (Таймаут простоя)**

После установки соединения, IP-адрес источника фиксируется в таблице. Каждый IP-адрес ассоциируется с определенным *слотом*. После создания запись действительна только в течение определенного количества секунд *(Idle Timeout)*. После установки нового соединения, в таблице выполняется поиск такого же IP-адреса источника, при этом значение таймаута для записи не будет превышено. После того, как найден соответствующий адрес, привязка обеспечивает отправку нового соединения на тот же сервер, на который были отправлены предыдущие соединения с одного и того же IP-адреса источника.

По умолчанию для данной настройки указано значение *10* секунд.

- **Макс. кол-во слотов (Max Slots)**

Данный параметр определяет максимальное количество слотов в таблице привязки. Если таблица заполнена, то самая старая запись будет удалена для того, чтобы освободить место для новой записи, даже если она все еще действительна (т.е. не превышено значение *Idle Timeout*).

Последствием переполнения таблицы может быть потеря привязки для любых отброшенных IP-адресов источника. По этой причине администратор должен указать значение параметра *Max Slots* в соответствии с предполагаемым количеством соединений, которые потребуют привязки.

По умолчанию для данной настройки указано значение *2048* слотов.

- **Размер сети** (**Net Size)**

Если применение привязки является важным, ресурсы для хранения и обработки данных требуют соответствия индивидуальным IP-адресам. При выборе опции *«Привязка к сети»* (Network Stickiness) количество данных запросов сокращается.

При выборе опции *«Привязка к сети»* (Network Stickiness) параметр *Net Size* определяет размер сети, которая должна ассоциироваться с IP-адресом источника новых соединений. Поиск в таблице привязки выполняется для того, чтобы выяснить, принадлежит ли IP-адрес источника той же сети, что и предыдущее соединение, уже зафиксированное в таблице. Если IP-адреса принадлежат одной сети, то будет выполнена привязка к одному и тому же серверу.

По умолчанию для данной настройки указано значение *24*.

10.4.4. Алгоритмы SLB и привязка (Stickiness)

Данный раздел описывает взаимодействие привязки и алгоритмов SLB.

В проиллюстрированном ниже примере межсетевой экран NetDefend является ответственным за балансировку соединений трех клиентов с различными адресами и двух серверов. Функция привязки (Stickiness) включена.

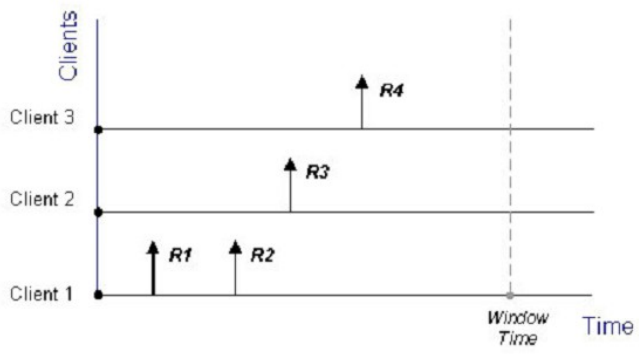


Рис.10.10. Соединения, установленные тремя клиентами

При использовании алгоритма «Round-robin», запросы *R1* и *R2*, приходящие от *Клиента 1*, назначаются одному серверу в соответствии с привязкой, назовем его *Сервер 1*. Следующий запрос *R3* от *Клиента 2* будет смаршрутизирован на *Сервер 2*. Запрос *R4* от *Клиента* 3 будет отправлен *Серверу 1*.

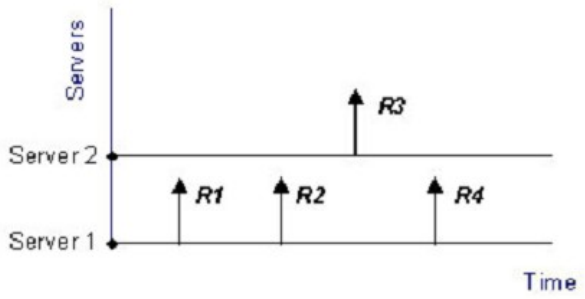


Рис. 10.11. Привязка (Stickiness) и алгоритм Round-Robin

При использовании алгоритма connection-rate, *R1* и *R2* будут отправлены на один и тот же сервер, в соответствии с привязкой, но последующие запросы *R3* и *R4* будут смаршрутизированы на другой сервер, так как количество новых соединений на каждом сервере в пределах периода времени «Window Time» ограничено.

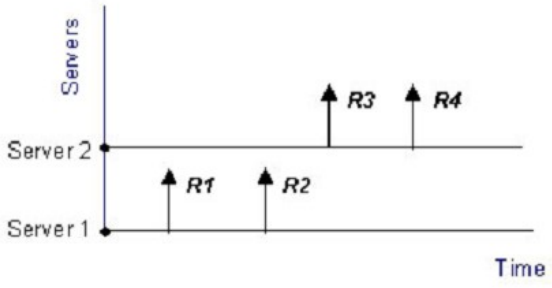


Рис. 10.12. Привязка (Stickiness) и алгоритм Connection-rate

Независимо от того, какой алгоритм выбран, если сервер отключен, трафик будет отправлен на другие серверы. После возвращения сервера в режим «онлайн», он автоматически помещается в кластер серверов и снова начинает получать запросы.

10.4.5. Мониторинг состояния сервера

SLB использует *Мониторинг состояния сервера*, обеспечивающий непрерывную проверку состояния серверов. SLB поддерживает мониторинг различных уровней OSI для проверки состояния каждого сервера. Независимо от того, какой алгоритм используется, если произошел сбой сервера, установка новых соединений не будет выполняться до тех пор, пока сервер не восстановится.

Функция балансировки нагрузки сервера D-Link обеспечивает следующие режимы мониторинга:

ICMP Ping	Работает на 3-ем уровне OSI. SLB отправляет запрос ping на IP-адрес каждого отдельного сервера в кластере. Команда ping используется для выявления неисправных серверов.
TCP Connection	Работает на 4-ом уровне OSI. SLB пытается подключиться к определенному порту каждого сервера. Например, если Web-службы запущены на порту 80, SLB отправит запрос TCP SYN на этот порт. Если SLB не получает TCP SYN/ACK обратно, то порт 80 будет отмечен как недействующий. SLB идентифицирует следующее: *no response, normal response* или *closed port response*.

10.4.6. Настройка правил *SLB_SAT*

Ключевым компонентом в настройке SLB являются IP-правила с действием *SLB_SAT*. Для настройки данных правил необходимо выполнить следующие шаги:

1. Укажите IP-адрес для каждого сервера, для которого включен SLB.
2. Укажите группу IP-адресов, которая включает все данные индивидуальные объекты.
3. Укажите правило *SLB_SAT* в наборе IP-правил, которое относится к данной группе IP-адресов и в котором указаны все остальные параметры SLB.
4. Укажите следующее правило, которое дублирует интерфейс/сеть источника/назначения правила *SLB_SAT*, которое разрешает прохождение трафика. Это должно быть одно правило или комбинация правил, использующих следующие действия:
   - Allow
   - NAT

Примечание: Правила FwdFast не должны использоваться с SLB

Для нормального функционирования SLB требует, чтобы механизм state engine NetDefendOS отслеживал соединения. Не следует использовать IP-правила FwdFast с SLB, так как пакеты, которые перенаправляются этими правилами, находятся под управлением state engine.

В таблице ниже представлены правила для каждого типичного сценария с набором Web-серверов позади межсетевого экрана NetDefend, для которого выполняется балансировка нагрузки. Правило *Allow* обеспечивает внешним клиентам доступ к Web-серверам.

Имя правила	Тип правила	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения
WEB_SLB	SLB_SAT	any	all-nets	core	ip_ext
WEB_SLB_ALW	Allow	any	all-nets	core	ip_ext

Если в одной и той же сети существуют клиенты, которым также необходим доступ к Web-серверам, то необходимо использовать правило *NAT*:

Имя правила	Тип правила	Интерфейс источника	Сеть источника	Интерфейс назначения	Сеть назначения
WEB_SLB	SLB_SAT	any	all-nets	core	ip_ext
WEB_SLB_NAT	NAT	lan	lannet	core	ip_ext
WEB_SLB_ALW	Allow	any	all-nets	core	ip_ext

Помните, что в качестве интерфейса назначения указано **core**. Основным преимуществом правила *Allow* является то, что Web-серверы могут внести в журнал точный IP-адрес, с которого выполняются внешние запросы. При использовании правила *NAT* Web-серверы будут видеть только IP-адрес межсетевого экрана NetDefend.

Пример 10.3. Настройка SLB

В данном примере рассматривается балансировка нагрузки между двумя Web-серверами HTTP, которые расположены позади межсетевого экрана NetDefend. IP-адреса данных Web-серверов: 192.168.1.10 и 192.168.1.11, соответственно. Для мониторинга, метода распределения и привязки (stickiness) используются значения SLB по умолчанию.

Правило *NAT* используется вместе с правилом *SLB_SAT* таким образом, чтобы клиенты позади межсетевого экрана могли получить доступ к Web-серверам. Правило *Allow* обеспечивает доступ внешним клиентам.

Web-интерфейс

А. Создайте Объект для каждого Web-сервера:

1. Зайдите **Objects > Address Book > Add > IP Address**

2. Далее введите подходящее имя, например, *server1*

3. Введите **IP-адрес**, *192.168.1.10*

4. Нажмите **OK**

5. Повторите все указанные шаги снова, чтобы создать объект *server2* с IP-адресом *192.168.1.11*

Б. Создайте Группу, содержащую два Web-сервера:

1. Зайдите **Objects > Address Book > Add > IP4 Group**

2. Далее введите подходящее имя, например, *server_group*

3. Добавьте в группу *server1* и *server2*

4. Нажмите **OK**

В. Укажите IP-правило **SLB_SAT**:

1. Зайдите **Rules > IP Rule Sets > main > Add > IP Rule**

2. Далее введите:

• **Name**: Web_SLB

• **Action**: SLB_SAT

• **Service**: HTTP

• **Source Interface**: any

• **Source Network:** all-nets

• **Destination Interface:** core

• **Destination Network:** ip_ext

3. Выберите вкладку **SAT SLB**

4. В **Server Addresses** добавьте *server_group* в **Selected**

5. Нажмите **OK**

Г. Укажите соответствующее IP-правило **NAT** для внутренних клиентов:

1. Зайдите **Rules > IP Rule Sets > main > Add > IP Rule**

2. Далее введите:

• **Name**: Web_SLB_NAT

• **Action**: NAT

• **Service**: HTTP

• **Source Interface**: lan

• **Source Network:** lannet

• **Destination Interface:** core

• **Destination Network:** ip_ext

3. Нажмите **OK**

Д. Укажите IP-правило *Allow* для внешних клиентов:

1. Зайдите **Rules > IP Rule Sets > main > Add > IP Rule**

2. Далее введите:

• **Name**: Web_SLB_ALW

• **Action**: Allow

• **Service**: HTTP

• **Source Interface**: any

• **Source Network:** all-nets

• **Destination Interface:** core

• **Destination Network:** ip_ext

3. Нажмите **OK**

Глава 11. Режим высокой доступности

В данной главе представлено описание настройки параметров режима высокой доступности межсетевых экранов NetDefend.

- Обзор
- Механизмы реализации режима высокой доступности
- Настройка HA-кластера
- Особенности при работе с HA-кластером
- Обновление HA-кластера
- Расширенные настройки HA-кластера

11.1. Обзор

HA-кластеры

Операционная система NetDefendOS позволяет межсетевым экранам NetDefend обеспечивать высокий уровень отказоустойчивости. Отказоустойчивость системы достигается за счет использования двух межсетевых экранов NetDefend: главного устройства (*master*) и подчиненного резервного устройства (*slave*). Главный и подчиненный межсетевые экраны взаимосвязаны и составляют логический HA-кластер. Когда одно из устройств кластера активно, второе находится в режиме ожидания, т.е. неактивно.

Изначально, slave-устройство в кластере является неактивным и только отслеживает действия главного устройства. Если же подчиненное устройство обнаруживает, что master-устройство перестает функционировать, то выполняется обработка ситуации отказа, т.е. slave-устройство становится активным и принимает на себя функции обработки всего трафика. Даже если затем master-устройство снова становится работоспособным, slave-устройство продолжает работать, а master-устройство теперь отслеживает его действия, чтобы при сбое принять выполнение функций на себя. Такую схему работы называют активно-пассивной (*active-passive*) реализацией режима высокой доступности системы.

Примечание: Возможность создания отказоустойчивых кластеров поддерживаются не всеми моделями межсетевых экранов NetDefend.

Возможность создания отказоустойчивых кластеров поддерживаются моделями межсетевых экранов D-Link NetDefend DFL-1600/1660/2500/2560/2560G.

Разница между понятиями «master-устройство» и «активное устройство»

Следует обратить внимание на то, что master-устройство отказоустойчивого кластера не всегда является активным устройством.

Активным устройством кластера в определенный момент времени является тот межсетевой экран NetDefend, который в это время фактически обрабатывает весь трафик. Slave-устройство может являться активным устройством, если произошло восстановление системы после сбоя и master-устройство не функционирует.

Взаимосвязь узлов кластера

В кластере master- и slave-устройства должны быть синхронизированы через интерфейс, называемый в операционной системе NetDefendOS интерфейсом синхронизации (*sync* interface). Интерфейсом

синхронизации является одним из стандартных интерфейсов между master-устройством и slave-устройством и имеет вид перекрестного кабеля.

Для связи между устройствами кластера операционная система NetDefendOS через интерфейс синхронизации и другие интерфейсы периодически отправляет специальные пакеты, называемые пакетами обнаружения (*heartbeats*). Эти пакеты позволяют устройствам отслеживать состояние друг друга. Пакеты обнаружения периодически отправляются в обоих направлениях, и таким образом, неактивное устройство имеет информацию о состоянии активного устройства и наоборот.

Более подробно механизм обмена пакетами обнаружения будет рассмотрен в *разделе 11.2 «Механизмы реализации режима высокой доступности»*.

Управление кластерами

Один HA-кластер, состоящий из двух межсетевых экранов NetDefend, управляется как единый блок с уникальным именем, которое отображается в интерфейсе управления как имя единого логического межсетевого экрана NetDefend. Операции по администрированию, например, такие как изменение набора IP-правил, будут выполняться как обычно, причем вносимые изменения будут автоматически применяться к конфигурациям обоих устройств: как главного, так и второстепенного.

Распределение нагрузки

HA-кластер D-Link не обеспечивает распределение нагрузки между параллельными устройствами, т.к. только одно устройство является в определенный момент времени активным, в то время как второе устройство находится в режиме ожидания. Два межсетевых экрана NetDefend (master и slave) составляют единый отказоустойчивый кластер. Неактивное устройство выполняет только копирование состояния активного устройства и принимает на себя функции обработки трафика в случае его отказа.

Дублирование оборудования

Отказоустойчивый кластер D-Link функционирует при условии наличия двух межсетевых экранов NetDefend. Программное обеспечение межсетевых экранов разных производителей значительно отличается, и не существует согласованных методов обмена информацией об их текущем состоянии.

Для создания отказоустойчивого кластера настоятельно рекомендуется использовать межсетевые экраны NetDefend с одинаковой конфигурацией. Также устройства должны иметь идентичные права, позволяющие им выполнение одинаковых действий, в том числе работу в HA-кластере.

Увеличение количества избыточного оборудования

Создание HA-кластера повышает отказоустойчивость только в одной точке сети. Маршрутизаторы, коммутаторы и точки подключения к сети Интернет остаются потенциально уязвимыми, и их дублирование также целесообразно.

11.2. Механизмы реализации режима высокой доступности

В этом разделе более подробно рассматриваются механизмы, операционной системы NetDefend реализующие режим высокой доступности системы.

Основные принципы

Отказоустойчивый кластер D-Link представляет собой избыточную аппаратную систему с синхронизацией состояния. Данные о состоянии активного устройства, например, такие как таблица подключений и другая необходимая информация, непрерывно копируются резервным устройством через интерфейс синхронизации. В момент, когда происходит обработка ситуации отказа основного устройства, дублирующее устройство имеет информацию о том, какие подключения являются сейчас активными, а после незначительной задержки на время восстановления системы передача трафика продолжается.

Резервная система фиксирует сбой основной системы в момент, когда не получает достаточного количества пакетов обнаружения кластера (*Cluster Heartbeats*). Пакеты обнаружения передаются как

через интерфейс синхронизации, так и через другие интерфейсы.

Частота отправки пакетов обнаружения

Операционная система NetDefendOS активного устройства отправляет 5 пакетов обнаружения в секунду, и если три пакета будут пропущены (т.е. через 0,6 секунд), инициируется восстановление системы. Отправка пакетов обнаружения через все интерфейсы позволяет неактивному устройству получать полную информацию о состоянии активного устройства. Даже если намеренно отключить интерфейс синхронизации, механизм восстановления системы не будет запущен, если неактивное устройство получает достаточно пакетов обнаружения через другие интерфейсы, например, через коммутатор, который подключен к двум межсетевым экранам. Однако по интерфейсу синхронизации передается вдвое больше пакетов обнаружения, чем через обыкновенные интерфейсы.

Пакеты обнаружения посылаются не чаще, чем через указанный промежуток времени, так как и в процессе нормального функционирования устройства могут возникать аналогичные задержки. Например, открытие файла может вызвать задержку достаточно длительную для того, чтобы резервная неактивная система перешла в активное состояние, даже если основная система остается активной.

Отключение отправки пакетов обнаружения через интерфейсы

При необходимости администратор может вручную отключить отправку пакетов обнаружения через любой интерфейс. Но выполнять это действие **не** рекомендуется, т.к. чем меньше действующих интерфейсов передают пакеты обнаружения, тем больше риск того, что недостаточное количество полученных пакетов будет неправильно отображать состояние системы.

Эта рекомендация не относится к отключенным интерфейсам. Необходимо отключать передачу пакетов обнаружения через неиспользуемый интерфейс. Операционная система NetDefendOS будет продолжать отправлять пакеты обнаружения через неработающий интерфейс и это может создать искаженное представление о состоянии системы, т.к. отправленные пакеты будут постоянно теряться. Результатом может стать ошибочный запуск восстановления системы после «сбоя».

Характеристики пакетов обнаружения

Пакеты обнаружения имеют следующие характеристики:

- IP-адресом источника является IP-адрес интерфейса межсетевого экрана, отправляющего пакет.
- IP-адресом назначения является широковещательный адрес интерфейса межсетевого экрана, отправляющего пакет.
- Время жизни (TTL) IP-пакета всегда должно быть равным 255. Если операционная система NetDefendOS получает пакет обнаружения кластера с другим значением TTL, предполагается, что данный пакет прошел через маршрутизатор. Такой пакет обнаружения считается недостоверным.
- Пакет обнаружения – это UDP-пакет, отправленный с порта 999 на порт 999.
- MAC-адрес назначения – это Ethernet-адрес групповой рассылки, соответствующий совместно используемому аппаратному адресу. Например, *11-00-00-C1-4A-nn*. Для обеспечения безопасности помимо обычных одноадресных пакетов используются групповые рассылки канального уровня. Использование одноадресных пакетов будет означать, что нарушитель из локальной сети смог перенаправить пакеты обнаружения от коммутаторов так, чтобы они не поступали на неактивное устройство.

Время обработки ситуации отказа

Обычно время обработки ситуации отказа составляет около одной секунды, и в это время может произойти небольшое увеличение количества потерянных пакетов. Для протокола TCP время обработки ситуации отказа составляет время стандартной паузы для повторной передачи пакета. TCP повторно передает потерянные пакеты в течение короткого промежутка времени, а далее продолжается обмен пакетами в стандартном режиме. Протокол UDP не предусматривает повторной передачи, т.к. является протоколом, не гарантирующим доставку пакета.

Совместно используемые IP-адреса и протокол ARP

Для Master-устройства и slave-устройства установлен один совместно используемый IP-адрес. ARP-запросы на получение совместно используемого IP-адреса или любого другого IP-адреса публикуются через раздел конфигурации ARP или через Proxy ARP и обрабатываются активной системой.

Аппаратный адрес совместно используемого IP-адреса и других опубликованных адресов не связан с реальными аппаратными адресами интерфейсов. Напротив, MAC-адрес задается операционной системой NetDefendOS в виде *10-00-00-C1-4A-nn*, где *nn* – это комбинация из идентификатора кластера (Cluster ID), задаваемого в разделе «Расширенные настройки» (Advanced Settings) и аппаратной шины / слота / порта данного интерфейса. Идентификатор кластера должен быть уникальным для каждого кластера сети.

Т.к. совместно используемый IP-адрес всегда имеет один аппаратный адрес, то при возникновении сбоя не возникнет задержек во время обновления ARP-кэша устройствами, находящимися в одной локальной сети с кластером.

Когда одно из устройств кластера обнаруживает, что второе устройство не функционирует, оно начинает широковещательную рассылку Gratuitous ARP-запросов на все интерфейсы, используя совместно используемый аппаратный адрес в качестве отправителя. Это позволяет коммутаторам в течение миллисекунд переопределить, куда отправлять пакеты, предназначенные для совместно используемого адреса. Определить, что произошел сбой в работе активного устройства можно только по задержке, возникающей из-за восстановления системы.

Для того чтобы коммутаторы всегда имели правильный совместно используемый аппаратный адрес для отправки по нему пакетов, периодически производится широковещательная рассылка ARP-запросов.

Процесс обновления антивирусных и IDP-баз в отказоустойчивом кластере

Если кластер с операционной системой NetDefendOS имеет антивирусную подсистему или подсистему обнаружения и предотвращения вторжений (IDP), то периодически будет возникать необходимость обновления баз вирусных сигнатур. Такие обновления подразумевают загрузки с внешних баз D-Link, а также требуют внесения изменений в конфигурацию для активации содержимого новых баз.

Обновление базы данных подразумевает следующую последовательность операций в HA-кластере:

6. На активное устройство (master) загружаются файлы новой базы данных с серверов D-Link. Загрузка производится через совместно используемый IP-адрес кластера.

7. С активного устройства (master) файлы новой базы данных отправляются второму неактивному устройству.

8. Для активации файлов новой базы данных на неактивном устройстве (slave) изменяется конфигурация.

9. Затем на активном устройстве (master) изменяется конфигурация для активации файлов новой базы данных путем инициации восстановления системы и переключения на slave-устройство.

10. После того, как изменение конфигурации master-устройства завершено, происходит обратное переключение, и master-устройство снова становится активным.

Разрыв *sync*-соединения

В HA-кластере может произойти разрыв *sync*-соединения между master- и slave-устройствами, и в результате неактивное устройство не будет получать пакетов обнаружения и обновляемых данных о состоянии активного устройства.

Следствием возникновения такого сбоя будет ситуация, когда оба устройства кластера будут продолжать функционировать без синхронизации друг с другом. Другими словами, неактивное устройство уже не будет иметь корректную копию состояния активного устройства. Но обработка ситуации отказа не произойдет, т.к. неактивное устройство определит разрыв *sync*-соединения.

В результате сбоя *sync*-интерфейса активное устройство генерирует системные сообщения *hasync_connection_failed_timeout*. Однако следует заметить, что такое же системное сообщение также генерируется в случае, когда неактивное устройство не функционирует, например, в процессе обновления ПО.

Возникновение сбоя *sync*-интерфейса определяется после сравнения результатов выполнения определенных команд командной строки для каждого устройства. Разницу в количестве соединений можно установить с помощью *stats*-команд. Если используются большое количество IPsec-туннелей, то можно применять команду *ipsecglobalstat -verbose*. Значительные различия в значениях IPsec SA, IKE SA, активных пользователей и в статистике пула IP-адресов будут означать сбой синхронизации. Если *sync*-интерфейс корректно функционирует, то также могут возникать некоторые различия в статистике устройств кластера, но их будет значительно меньше по сравнению с ситуацией сбоя.

Если сбой в работе sync-интерфейса произошел, то даже после замены соединяющего кабеля, восстановление синхронизации между активным и неактивным устройством **не** произойдет автоматически. Несинхронизированное неактивное устройство необходимо перезапустить. И далее:

- Во время перезапуска неактивное устройство отправит активному устройству сообщение, о своей готовности к работе, запрашивая полную информацию о состоянии активного устройства.
- Активное устройство отправит неактивному устройству копию основных параметров своего текущего состояния.
- Тогда неактивное устройство будет синхронизировано, и при возникновении системного сбоя восстановление системы будет выполнено корректно.

Примечание: Для возобновления синхронизации требуется перезапуск неактивного устройства.

Только во время перезапуска неактивного устройства ему отправляется полная информация о состоянии активного устройства. Поэтому для возобновления синхронизации требуется перезагрузка неактивного устройства.

11.3. Настройка HA-кластера

В данном разделе описывается процесс пошаговой настройки HA-кластера.

11.3.1. Настройка аппаратного обеспечения HA-кластера

Пошаговая настройка аппаратного обеспечения HA-кластера:

1. Для создания HA-кластера необходимо два аппаратно идентичных межсетевых экрана NetDefend. Это могут быть два новых устройства, либо к имеющемуся устройству может быть дополнительно приобретено еще одно.

На аппаратном уровне master- и slave-устройства не обязательно должны быть полностью идентичными, однако, желательно, чтобы использовалось оборудование с одинаковой производительностью, чтобы избежать изменения производительности после восстановления системы.

2. Создание физических подключений:

- Подключите соответствующие интерфейсы master- и slave-устройств через отдельные коммутаторы или отдельные широковещательные домены. Важно отделить трафик каждой пары интерфейсов от других пар.
- Подключите *sync*-интерфейсы. Это можно сделать непосредственно с помощью перекрестного кабеля или через отдельный коммутатор (или широковещательный домен).

3. Определите совместно используемый IP-адрес для каждого интерфейса кластера. Некоторые

интерфейсы могут иметь совместно используемые адреса только тогда, когда другие интерфейсы также могут иметь уникальные индивидуальные IP-адреса для каждого интерфейса, определенного в объекте *IP4 HA Address*. Совместно используемые и индивидуальные адреса используются следующим образом:

- Индивидуальные адреса, определенные для интерфейса в объекте *IP4 HA Address* позволяют осуществлять удаленное управление через данный интерфейс. Такие IP-адреса могут отвечать на запросы команды ping по протоколу ICMP, если это разрешено IP-правилами (по умолчанию, ICMP-запросы набором IP-правил отбрасываются).

  Если любое из устройств кластера не функционирует, индивидуальный IP-адрес этого устройства будет недоступен. Индивидуальные IP-адреса обычно являются внутренними. Но при необходимости удаленного управления устройством через Интернет, в качестве индивидуального IP-адреса должен выступать внешний адрес.

  Если для интерфейса не определен индивидуальный адрес через объект *IP4 HA Address*, то ему должен быть назначен адрес локального узла (*localhost*) по умолчанию, который является IP-адресом из подсети *127.0.0.0/8*.

  На ARP-запросы по индивидуальным IP-адресам, определенным в объектах *IP4 HA Address*, отвечает межсетевой экран, обладающий данным адресом, используя при этом обычный аппаратный адрес как с обычными IP-узлами.

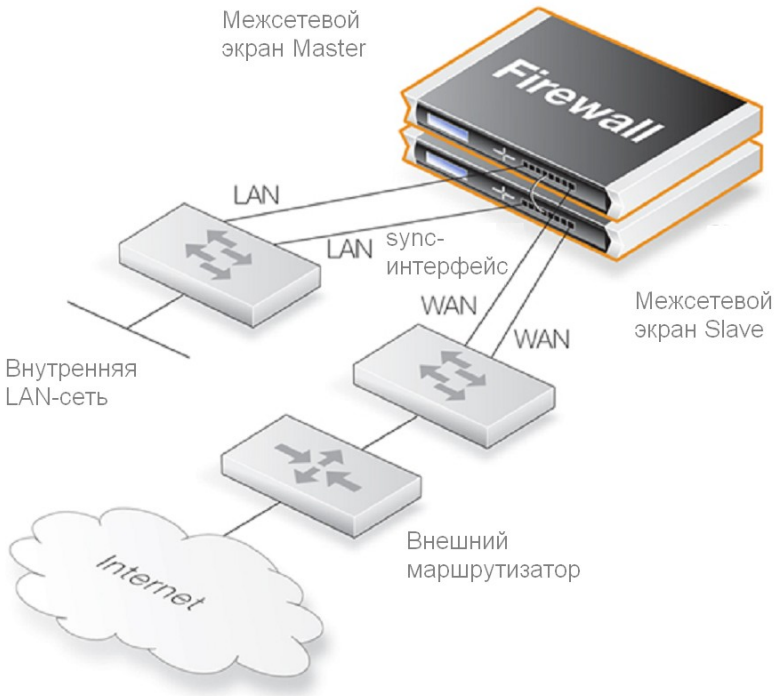
- Единый совместно используемый IP-адрес используется для маршрутизации, а также является адресом, используемым при процедуре динамического преобразования адресов, кроме случаев, когда в конфигурации определен другой адрес.

Примечание: Управление через совместно используемый IP-адрес невозможно.

Совместно используемый IP-адрес не может использоваться для удаленного управления и мониторинга. Например, при использовании SSH для удаленного управления межсетевыми экранами NetDefend, составляющими один HA-кластер, необходимо использовать индивидуальные IP-адреса интерфейсов каждого из межсетевых экранов. IP-адреса определены в объектах IP4 HA Address, упомянутых ранее.

Типичная схема подключения HA-кластера

На рисунке ниже изображена схема типичного подключения HA-кластера в сети. Все интерфейсы master-устройства обычно повторяют соответствующие интерфейсы slave-устройства и подключены к одним и тем же сетям. Это реализовано с помощью подключения одинаковых интерфейсов master- и slave-устройств через отдельный коммутатор (или широковещательный домен) к другим сегментам сети.



На приведенной схеме, LAN-интерфейс master-устройства и LAN-интерфейс slave-устройства подключаются к одному и тому же коммутатору, который затем подключен к внутренней сети. Аналогично WAN-интерфейс master-устройства и WAN-интерфейс slave-устройства подключаются к коммутатору, который подключен к внешней сети Интернет.

Примечание: на рисунке представлено sync-подключение, организованное с помощью перекрестного кабеля.

На рисунке представлено подключение, организованное с помощью перекрестного кабеля, между sync-интерфейсами устройств кластера. Такое подключение также может быть организовано через коммутатор или широковещательный домен.

11.3.2. Ручная настройка HA-кластера в операционной системе NetDefendOS

Для того чтобы вручную настроить HA-кластер, необходимо выполнить следующие действия:

1. Подключиться к master-устройству через WEB-интерфейс.
2. Перейти **System > High Availability**.
3. Установить флажок в пункте **Enable High Availability**.
4. Присвоить значение идентификатору кластера в поле **Cluster ID**. Значение идентификатора должно быть уникальным для каждого кластера.
5. Выбрать sync-интерфейс в поле **Sync Interface**.
6. Установить тип узла *Master*.
7. Перейти **Objects > Address Book** и создать объект **IP4 HA Address** для каждой пары интерфейсов. Каждая пара должна содержать IP-адреса интерфейсов master-устройства и slave-устройства.

   Создание объекта обязательно для пары интерфейсов, используемых для удаленного управления, и необязательно для других интерфейсов (в этом случае необходимо использовать адрес локального узла (*localhost*) по умолчанию, который является IP-

адресом из подсети *127.0.0.0/8*).

8. Перейти **Interfaces > Ethernet** и для каждого интерфейса в списке ввести в поле **IP Address** совместно используемый IP-адрес для этого интерфейса.

   Также для каждого интерфейса необходимо выбрать вкладку **Advanced** и установить в поле **High Availability**, **Private IP Address** имя объекта IP4 HA Address, созданного заранее для этого интерфейса (операционная система NetDefendOS автоматически выберет соответствующий определенный в объекте адрес от master-устройства и slave-устройства).

Примечание: IP-адреса могут быть внешними IP-адресами.

В данном контексте термин «внутренний IP-адрес» не является корректным. IP-адрес, используемый в объекте IP4 HA Address может являться внешним адресом, если существует необходимость осуществлять внешние управление устройством через сеть Интернет.

9. Сохранить и активировать новую конфигурацию с помощью **Save and activate**.

10. Повторить указанные выше действия для второго межсетевого экрана NetDefend, выбирая тип узла *Slave*.

Внесение изменений в конфигурацию HA-кластера

Конфигурация двух межсетевых экранов NetDefend должна быть одинаковой. Конфигурация двух устройств кластера будет автоматически синхронизироваться. Чтобы изменить что-либо в конфигурации кластера необходимо подключиться либо к master-устройству, либо к slave-устройству, изменить настройки, затем сохранить и активировать изменения. Внесенные изменения будут применены к обоим устройствам.

11.3.3. Проверка функций HA-кластера

Для того чтобы удостовериться в том, что кластер функционирует корректно, первоначально необходимо применить команду *ha* к каждому устройству кластера. Пример выполнения команды (для master-устройства):

```
gw-world:/> ha

This device is an HA MASTER
This device is currently ACTIVE (will forward traffic)
HA cluster peer is ALIVE
```

Далее используйте команду *stat* для того чтобы удостовериться, что master-устройство и slave-устройство имеют равное количество подключений. Пример выполнения команды:

```
Connections 2726 out of 128000
```

В данном примере меньшее из двух чисел, расположенное слева, указывает текущее количество подключений. А большее правое число – максимальное количество разрешенных подключений.

Следующие пункты также важны при настройке кластера:

- Если текущий кластер является не первым кластером в сети, то идентификатор кластера *Cluster ID* необходимо изменить так, чтобы он был уникальным (значение по умолчанию 0). Идентификатор кластера определяет уникальный MAC-адрес кластера.

- Рекомендуется активировать параметр расширенных настроек *Use Unique Share MAC* для того чтобы каждому интерфейсу был присвоен свой MAC-адрес. Если этот праметр не активирован, то интерфейсы будут совместно использовать один MAC-адрес и это может помешать работе сторонних коммутаторов.

- Удостоверьтесь, что параметр расширенных настроек *High Buffers* установлен в значение *automatic* для обоих устройств кластера. Эта настройка определяет распределение памяти

операционной системой NetDefendOS для обработки увеличивающегося количества подключений. Для применения внесенных изменений в данном пункте настроек необходима перезагрузка устройства.

Если кластер имеет очень большое количество (например, десятки тысяч) одновременных подключений, то возможно потребуется установить большое значение данного параметра вместо *automatic*. Большое значение параметра *High Buffers* подходит для ситуаций с большим количеством подключений, но имеет недостаток в виде снижения пропускной способности.

11.3.4. Опция Unique Shared Mac Addresses

Для настройки режима высокой доступности, в операционной системе NetDefendOS предусмотрена опция расширенных настроек *Use Unique Shared MAC Address*. По умолчанию эта опция активирована и для большинства конфигураций ее не следует отключать.

Активирование опции Unique Shared MAC Address

Результатом активации данной опции будет то, что единый уникальный MAC-адрес будет использоваться для каждой пары соответствующих аппаратных интерфейсов. Таким образом, интерфейс *lan1* master-устройства будет иметь такой же MAC-адрес, что и интерфейс *lan1* slave-устройства.

Трудности в диагностике

HA-кластер будет функционировать, даже если данная опция отключена, но могут возникнуть проблемы, т.к. только в некоторых видах коммутаторов, применяется совместно используемая ARP-таблица. Проблемы такого характера трудно диагностируемы. Следовательно, рекомендуется, чтобы эта опция была активирована постоянно.

При использовании отличающегося оборудования

Если HA-кластер создается с использованием отличающегося оборудования, опция Unique Shared MAC Address должна быть отключена. Для правильного функционирования уникальные совместно используемые MAC-адреса не должны применяться.

11.4. Особенности при работе с HA-кластером

При управлении и настройке HA-кластера следует обращать внимание на следующие особенности:

Каждый интерфейс кластера должен иметь IP-адрес

Для каждого интерфейса обоих устройств кластера должен быть определен допустимый внутренний адресный объект IP4. Для этой цели может использоваться предопределенный IP-объект *local host*. Необходимость в назначении адреса остается, даже если интерфейс отключен.

SNMP

SNMP-статистика не является совместной для master-устройства и slave-устройства. SNMP-менеджеры не имеют возможности обработки ситуации отказа. Каждый межсетевой экран в кластере учитывается отдельно.

Использование индивидуальных IP-адресов

Уникальные индивидуальные IP-адреса master-устройства и slave-устройства не могут безопасно использоваться для чего-либо кроме управления. При их использовании, например, в качестве IP-адреса источника в соединениях динамически преобразуемых с помощью NAT или для служб публикаций, могут возникать проблемы, т.к. IP-адреса перестанут быть уникальными, когда межсетевой экран, к которому они относятся, начнет функционировать.

IP-адрес *0.0.0.0* не может быть совместно используемым

Необходимо избегать назначения IP-адреса *0.0.0.0* в качестве совместно используемого IP-адреса. При использовании IP-адреса *0.0.0.0* в качестве совместно используемого IP-адреса произойдет переход операционной системы NetDefend в режим блокировки (Lockdown Mode).

Поврежденные интерфейсы

Повреждения интерфейсов невозможно определить, кроме случаев, когда повреждения касаются функционирования операционной системы NetDefendOS. Это означает, что обработка ситуации отказа не будет инициироваться в случае, если активное устройство все еще способно отправить пакет обнаружения неактивному устройству через любой из своих интерфейсов, даже если один или несколько интерфейсов будут несправны.

Изменение идентификатора кластера

Изменение идентификатора кластера в рабочей сети не рекомендуется по двум причинам. Во-первых, это приведет к изменению аппаратного адреса для совместно используемых IP-адресов, что повлечет проблемы для всех устройств, присоединенных к внутренней LAN-сети, т.к. они хранят в ARP-кэше старый аппаратный адрес до истечения его срока действия. Такие устройства будут вынуждены очистить ARP-кэш.

Во-вторых, это разорвет соединение между межсетевыми экранами кластера на то время, пока они используют разные конфигурации. Возникнет ситуация, при которой оба устройства кластера будут активными одновременно.

Неверные контрольные суммы в пакетах обнаружения

Пакеты обнаружения кластера намеренно отправляются с ошибочными контрольными суммами. Это делается для того, чтобы их было невозможно передавать дальше по маршруту. Некоторые маршрутизаторы могут указывать эти ошибочные контрольные суммы в своих системных сообщениях.

Использование протокола OSPF

Если для определения метрики маршрутов применяется протокол OSPF, кластер **не может** использоваться в качестве выделенного маршрутизатора (*designated router*).

Если протокол OSPF должен применяться, тогда должен быть доступен другой выделенный маршрутизатор в той же OSPF-области (*OSPF area*), где находится кластер. Целесообразно иметь второй резервный выделенный маршрутизатор, который будет предоставлять данные о метриках OSPF, в случае если основной выделенный маршрутизатор выйдет из строя.

PPPoE-туннели и DHCP-клиенты

По причинам, связанным с применением совместно используемых IP-адресов в HA-кластере, не следует организовывать PPPoE-туннели и производить настройку DHCP-клиентов в HA-кластере.

11.5. Обновление HA-кластера

Версии операционной системы NetDefendOS на master-устройстве и slave-устройстве одного HA-кластера должны совпадать. Когда новая версия NetDefendOS становится доступной, ее необходимо установить на оба устройства кластера, и обновление должно производиться на каждом устройстве в отдельности.

Основным принципом процесса обновления кластера является то, что установка нового ПО на неактивное устройство не повлияет на работу кластера, а только на некоторое время сделает неактивное устройство недоступным.

Общая последовательность шагов следующая:

- Определить, какое из двух устройств является в данный момент неактивным, и установить обновление на него в первую очередь.
- Когда неактивное устройство снова будет синхронизировано с активным устройством, инициировать ситуацию сбоя, чтобы неактивное устройство перешло в состояние активного.
- Обновить второе устройство, которое теперь является неактивным. После повторной синхронизации оба устройства будут использовать обновленную версию операционной системы NetDefend.

Вышеперечисленные действия далее будут рассмотрены более подробно.

А. Определить, какое из двух устройств кластера является в данный момент неактивным

Неактивное на данный момент устройство следует обновлять первым, поэтому его необходимо определить. Для этого подключитесь к консоли командной строки одного из устройств кластера и запустите команду *ha*. Пример выполнения команды для активного устройства приведен ниже:

```
gw-world:/> ha

This device is a HA SLAVE
This device is currently ACTIVE (will forward traffic)
This device has been active: 430697 sec
HA cluster peer is ALIVE
```

Slave-устройство является активным на данный момент. Таким образом, master-устройство сейчас является неактивным.

Б. Установить обновленную версию ПО на неактивное устройство

Когда неактивное устройство кластера определено, необходимо установить на него новую версию операционной системы NetDefend. Это производится так же, как если бы устройство не входило в кластер. Например, для установки обновления можно использовать WEB-интерфейс.

Важно: Удостоверьтесь, что неактивное устройство имеет статус ALIVE

Прежде чем переходить к выполнению следующего шага, удостоверьтесь в том, что после завершения обновления неактивное устройство правильно функционирует и синхронизировано с активным.

*Для этого запустите на неактивном устройстве CLI-команду **ha**. Результат выполнения команды должен содержать текущий статус устройства – ALIVE.*

```
gw-world:/> ha

This device is a HA SLAVE
This device is currently INACTIVE (won't forward traffic)
This device has been inactive: 2 sec
HA cluster peer is ALIVE
```

В. Инициируйте ситуацию сбоя

Теперь необходимо подключиться к активному устройству (которое все еще продолжает использовать старую версию NetDefendOS) через консоль командной строки и запустить на выполнение команду *ha -deactivate*. Это вызовет смену активного устройства. Активное в данный момент устройство станет неактивным, а неактивное – активным.

```
gw-world:/> ha -deactivate

HA Was: ACTIVE
HA going INACTIVE...
```

Для подтверждения того, что процедура обработки сбоя завершена успешно, следует еще раз запустить команду *ha*, и теперь в тексте результата выполнения программы должно присутствовать «**INACTIVE**» и «**is ALIVE**».

Г. Обновите устройство, ставшее теперь неактивным

Когда процедура обработки сбоя завершена, следует установить на устройство, ставшее теперь неактивным, новую версию операционной системы NetDefend. Установка обновления производится также как это указано в пункте Б, т.е. так же, как если бы устройство не входило в кластер.

Д. Дождитесь выполнения повторной синхронизации

Когда обновление ПО второго устройства будет завершено, оба устройства кластера автоматически произведут повторную синхронизацию, и кластер продолжит работу. Роли активного и неактивного устройств сохранятся.

Если необходимо сделать активное устройство неактивным, а неактивное – активным, то следует использовать CLI-команду *ha -active*.

11.6. Расширенные настройки HA-кластера

Следующие параметры расширенных настроек операционной системы NetDefendOS используются для режима высокой доступности:

Sync Buffer Size

Показывает, объем данных (в Кбайт), который необходимо поместить в буфер в процессе ожидания уведомления от второго устройства кластера.

По умолчанию: *1024*

Sync Packet Max Burst

Максимальное количество пакетов синхронизации состояния, отправляемых одновременно.

По умолчанию: *20*

Initial Silence

Период времени (в секундах) сразу после запуска устройства или после изменения его конфигурации, в течение которого устройство не будет отправлять пакеты обнаружения. Когда активное устройство HA-кластера обнаруживает, что неактивное устройство стало недоступным, оно все равно продолжает посылать данные синхронизации в обычном режиме в течение одной минуты, ожидая, что за это время неактивное устройство может снова стать доступным. После того как минута истекла, чтобы излишне не загружать сеть, данные синхронизации передаются только после периодов молчания. Длительность периодов определяется данной настройкой.

По умолчанию: *5*

Use Unique Shared Mac

Для каждого интерфейса применяется уникальный совместно используемый MAC-адрес. Более подробное описание параметра приведено в *разделе 11.3.4 «Опция Unique Shared Mac Addresses»*.

По умолчанию: *активировано*

Deactivate Before Reconf

Если данный параметр активирован, то активный узел при сбое переходит в неактивное состояние, прежде чем изменение конфигурации вступит в силу. В противном случае неактивный узел должен определять, что активный не функционирует и перейти в активное состояние. Активирование данного параметра сокращает период, в течение которого ни один из узлов не является активным во время применения конфигурации.

По умолчанию: *активировано*

Reconf Failover Time

Количество секунд неактивности перед процедурой обработки сбоя при изменении конфигурации HA-кластера. Значение по умолчанию 0 означает мгновенное изменение конфигурации.

По умолчанию: *0*

Глава 12. ZoneDefense

Эта глава посвящена методу D-Link ZoneDefense.

- Обзор
- Коммутаторы ZoneDefense
- Функционирование ZoneDefense

12.1. Обзор

Управляемые коммутаторы ZoneDefense

Функция ZoneDefense позволяет межсетевому экрану NetDefend работать с коммутаторами локальных сетей. Данная функция позволяет изолировать инфицированные компьютеры сети и предотвратить распространение ими вредоносного трафика.

Заражение хоста в сети вирусами или другой формой вредоносного ПО может выражаться в его аномальном поведении, характеризующимся большим числом новых соединений, открываемых к внешним хостам.

Применение порогов

При установке в ZoneDefense *пороговых правил* (*Threshold Rules*) хосты или сети, которые превышают определенный порог соединений, динамически блокируются. Настройки *Threshold Rules* базируются на количестве новых соединений, произведенных за секунду или на общем количестве созданных соединений.

Соединения могут быть созданы единственным хостом или всеми хостами в пределах выбранного диапазона IP-адресов CIDR (в диапазоне IP-адресов указывается комбинация IP-адреса и относящейся к нему маски).

Загрузка ACL

Если система NetDefendOS обнаружит, что хост или сеть достигли определенного порога, то она загружает ACL-правила (Access Control List) для соответствующего коммутатора, которые блокируют весь трафик для хоста или сети, поведение которых не соответствует норме. Такие хосты и сети остаются заблокированными до тех пор, пока администратор вручную их не разблокирует при помощи Web-интерфейса или CLI.

Примечание: ZoneDefense поддерживают не все модели NetDefend

Функцию ZoneDefense поддерживают только следующие модели D-Link: DFL-800, 860, 1600, 1660, 2500,2560, 2560G.

12.2. Коммутаторы ZoneDefense

Информацию о каждом коммутаторе, который должен работать с межсетевым экраном, необходимо вводить вручную при конфигурировании межсетевого экрана. Информация, необходимая для работы с коммутатором, содержит:

- IP-адрес интерфейса управления коммутатора

- Тип коммутатора
- Строка SNMP community (с доступом *write*)

На настоящий момент функцию ZoneDefense поддерживают следующие модели коммутаторов:

- DES-3226S (Версии R4.02-B26 и выше)
- DES-3250TG (Версии R3.00-B09 и выше)
- DES-3326S (Версии R4.01-B39 и выше)
- DES-3350SR (Версии R3.02-B12 и выше)
- DES-3526 R3.x (Только версия R3.06-B20)
- DES-3526 R4.x (Версии R4.01-B19 и выше)
- DES-3550 R3.x (Только версия R3.05-B38)
- DES-3550 R4.x (Версии R4.01-B19 и выше)
- Серия DES-3800 (Версии R2.00-B13 и выше)
- Серия DGS-3200 (Версии R1.10-B06 и выше)
- DGS-3324SR/Sri (Версии R4.30-B11 и выше)
- Серия DGS-3400 R1.x (Только версия R1.00-B35)
- Серия DGS-3400 R2.x (Версии R2.00-B52 и выше)
- DXS-3326GSR (Версии R4.30-B11 и выше)
- DXS-3350SR (Версии R4.30-B11 и выше)
- DHS-3618 (Версии R1.00-B03 и выше)
- DHS-3626 (Версии R1.00-B03 и выше)

Совет: Версия программного обеспечения коммутатора должна быть самой последней

Прежде чем активировать функцию ZoneDefence следует убедиться в том, что минимальные системные требования соответствуют запросам.

12.3. Функционирование ZoneDefense

12.3.1. SNMP

Простой протокол сетевого управления (Simple Network Management Protocol, SNMP) – протокол прикладного уровня для комплексного управления сетями. SNMP позволяет управляющему и управляемому сетевым устройствам связываться друг с другом.

SNMP-управление

Типичное управляющее устройство (менеджер), например межсетевой экран NetDefend, использует SNMP-протокол для контроля и управления сетевыми устройствами в управляемой среде. Менеджер может запрашивать у контролируемых устройств статистику с помощью *строки SNMP Community* (*SNMP Community String*). Такая строка (последовательность символов) схожа с идентификатором пользователя или паролем и позволяет получить доступ к информации из таблицы состояния устройства. Если тип данной строки – *write*, то менеджер может изменить состояние устройства.

Управляемые устройства

Управляемые устройства (агенты) должны быть SNMP-совместимыми. Коммутаторы D-Link являются SNMP-агентами, они хранят данные о состоянии в базе данных MIB (Management Information Base) и обеспечивают информацией управляющее устройство после получения SNMP-запроса.

12.3.2. Пороговые правила (Threshold Rules)

Пороговое правило инициирует механизм ZoneDefense для блокировки определенных узлов или сети, если превышен указанный порог соединений, который может быть двух типов:

- **Connection Rate Limit** – ограничение количества новых соединений за секунду к межсетевому экрану.
- **Total Connections Limit** – ограничение общего количества соединений к межсетевому экрану.

Параметры пороговых правил схожи с параметрами IP-правил и определяют тип трафика, к которому обращается пороговое правило.

У каждого порогового правила выделяют следующие параметры:

- Интерфейс источника и сеть источника
- Интерфейс назначения и сеть назначения
- Сервис
- Тип порога: для хоста и/или сети

При прохождении трафика, соответствующего вышеупомянутым критериям и превышающего порог для данного хоста/сети, срабатывает механизм ZoneDefense, который будет препятствовать обращению хоста/сети к коммутатору. Все блокировки из-за превышения порога основаны на IP-адресе хоста или сети на коммутаторе. Если порог в сети превышается, то в этой сети блокируется хост, превысивший данный порог.

Более подробная информация об определении и функционировании пороговых правил приведена в *Разделе 10.3 “Пороговые правила”*.

12.3.3. Ручная блокировка и создание списка Exclude (Exclude Lists)

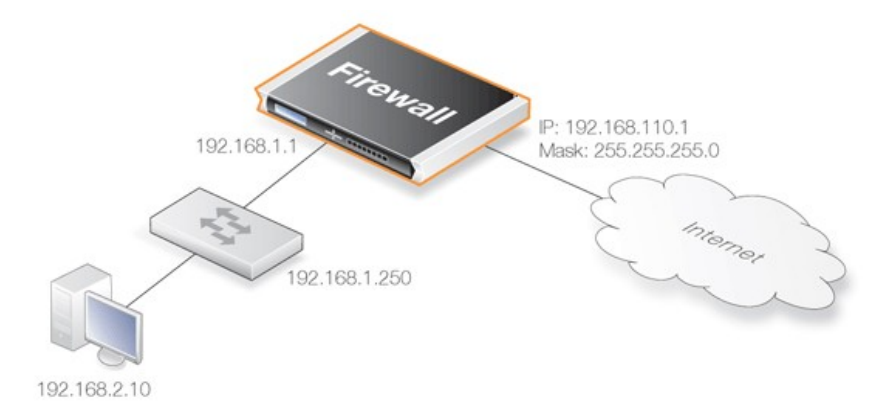
В дополнение к пороговым правилам можно вручную определить хосты и сети, которые необходимо заблокировать или исключить. Заблокированные вручную хосты или сети могут блокироваться по умолчанию или на основе расписания. Существует возможность определения протоколов, которые должны быть заблокированы.

Для предотвращения блокировки хостов в случае превышения ими порога следует создать *список Exclude*. Желательно в этот список включать IP-адрес интерфейса межсетевого экрана или MAC-адрес коммутатора ZoneDefense, что предотвращает межсетевой экран от случайной блокировки.

Пример 12.1. Простой сценарий ZoneDefense

В данном примере рассмотрены шаги, необходимые для установки ZoneDefense. Предполагается, что все интерфейсы межсетевого экрана уже настроены.

Для HTTP установлен порог 10 соединений в секунду. Если количество соединений превышает этот порог, межсетевой экран блокирует доступ к коммутатору определенного хоста (например, в сети с диапазоном 192.168.2.0/24).



В данном случае используется модель коммутатора D-Link DES-3226S с адресом управляющего интерфейса 192.168.1.250, соединяющегося с адресом интерфейса межсетевого экрана 192.168.1.1. Интерфейс межсетевого экрана добавляется в список Exclude, для предотвращения случайной блокировки.

Web-интерфейс

Добавить новый коммутатор в раздел ZoneDefense:

1. Перейти на вкладку **ZoneDefense > Switches > Add > ZoneDefense switch**

2. Ввести:

- **Name**: switch1
- **Switch model**: DES-3226S
- **IP Address**: 192.168.1.250

3. Для **SNMP Community** ввести строку *Write Community String*, определенную для коммутатора.

4. Запустить **Check Switch** для проверки соединений межсетевого экрана с коммутатором и корректность строки SNMP Community.

5. **OK**

Добавить управляющий интерфейс коммутатора в список Exclude:

1. Перейти на вкладку **ZoneDefense > Exclude list**

2. Для выбранного в поле **Addresses** имени объекта вставить адрес 192.168.1.1 из списка **Available** в список **Selected**.

3. **OK**

Настройка порога, равного 10 соединениям в секунду, для HTTP:

1. Перейти на вкладку **Traffic Management** > **Threshold Rules** > **Add** > **Threshold Rule**

2. Для **Threshold Rule** ввести:

- **Name**: HTTP-Threshold

- **Service**: http

3. Для **Address Filter** ввести:

- **Source Interface**: Управляющий интерфейс межсетевого экрана
- **Destination Interface**: any
- **Source Network**: 192.168.2.0/24 (или имя объекта)
- **Destination Network**: all-nets

4. **OK**

Определение порога, типа порога и действий, в случае превышения порога:

1. Перейти на вкладку **Add > Threshold Action**

2. Настройки для **Threshold Action**:

- **Action**: Protect
- **Group By**: Host-based
- **Threshold**: 10
- Установить единицу измерения пороговой величины: **Connection/Second**
- Установить флажок в поле **Use ZoneDefense**
- Нажмите **OK**

12.3.4. ZoneDefense и сканирование антивирусом

ZoneDefense может использоваться в связке со встроенным антивирусом системы NetDefendOS, которая сначала идентифицирует источник вредоносного ПО, а затем блокирует его, действуя совместно с коммутатором, сконфигурированным для работы с механизмом ZoneDefense. Эта функция активируется через следующие ALG:

- **HTTP** – ZoneDefense может заблокировать HTTP-сервер, если он является источником вредоносного ПО.
- **FTP** – ZoneDefense может заблокировать локального FTP-клиента при загрузке им вредоносного ПО.
- **SMTP** – ZoneDefense может заблокировать локального SMTP-клиента при отправке им вредоносного ПО через e-mail.

12.3.5. Ограничения

В зависимости от модели коммутатора процесс работы ZoneDefense может различаться. Первое отличие заключается в разном времени ожидания между запуском блокирующего правила и моментом фактического блокирования соответствующего трафика коммутатором. Всем моделям коммутаторов необходим небольшой интервал времени ожидания для осуществления блокирования после запуска правила. Для некоторых моделей эта величина не превышает секунды, в то время как другим коммутаторам может потребоваться несколько минут.

Второе отличие заключается в максимальном количестве правил, поддерживаемых различными коммутаторами. Некоторые модели коммутаторов поддерживают только 50 правил, другие – до 800 правил (обычно для того, чтобы заблокировать хост или сеть необходимо одно правило на порт коммутатора). Когда этот предел будет достигнут, хосты или сети перестанут блокироваться.

Важно: Очистка записей в наборе ACL-правил коммутатора

ZoneDefense использует диапазон в наборе ACL-правил коммутатора. Чтобы избежать конфликтов в правилах и гарантировать межсетевому экрану доступ к управлению, перед установкой ZoneDefense администраторам рекомендуется очищать записи в наборе ACL-правил коммутатора.

Глава 13. Дополнительные настройки

Данная глава содержит информацию о дополнительных настройках для системы NetDefendOS, которые не были описаны в предыдущих главах. Для получения дополнительной информации о данных настройках зайдите в меню Web-интерфейса **System > Advanced Settings**.

Настройки разделяются на следующие категории:

Примечание: Активация измененных настроек

Для вступления новых измененных настроек NetDefendOS в действие необходимо их активировать.

- Настройки IP-уровня
- Настройки TCP-уровня
- Настройки ICMP-уровня
- Настройки состояний
- Настройки таймаута соединения
- Настройки ограничения размеров
- Настройки фрагментации
- Настройки сборки фрагментов в локальной сети
- Остальные настройки

13.1. Настройки IP-уровня

Log Checksum Errors

Данная настройка используется для регистрации в журналах IP-пакетов, содержащих неверное значение контрольной суммы. Как правило, это происходит из-за повреждения пакета при передаче в сети. Все сетевые устройства, как маршрутизаторы, так и рабочие станции, отбрасывают IP-пакеты, содержащие неверные контрольные суммы. Вероятность атак на основе неверного значения контрольной суммы маловероятна.

По умолчанию: *Включено*

Log non IP4

Данная настройка используется для регистрации в журналах IP-пакетов, которые не являются пакетами версии 4. Система NetDefendOS принимает только IP-пакеты версии 4; все остальные пакеты будут отброшены.

По умолчанию: *Включено*

Log Received TTL 0

Данная настройка используется для регистрации в журналах полученных IP-пакетов со значением TTL (Time To Live), равным 0. Ни при каких обстоятельствах сетевое устройство не должно отправлять пакеты со значением TTL – 0.

По умолчанию: *Включено*

Block 0000 Src

Настройка используется для блокировки пакетов с адресом 0.0.0.0 в качестве адреса источника.

По умолчанию: *Отбросить*

Block 0 Net

Настройка используется для блокировки пакетов с числом 0.* в качестве адреса источника.

По умолчанию: *DropLog*

Block 127 Net

Настройка используется для блокировки пакетов с числом 127.* в качестве адреса источника.

По умолчанию: *DropLog*

Block Multicast Src

Настройка используется для блокировки пакетов с IP-адресом многоадресной рассылки в диапазоне от 224.0.0.0 до 255.255.255.255.

По умолчанию: *DropLog*

TTL Min

Минимальное значение TTL, разрешенное при получении.

По умолчанию: *3*

TTL on Low

С помощью данной настройки указывается действие, выполняемое по отношению к пакету, значение TTL которого ниже установленного значения TTLMin.

По умолчанию: *DropLog*

Multicast TTL on Low

С помощью данной настройки можно указать действие, выполняемое по отношению к пакету, значение TTL которого ниже установленного значения Multicast TTLMin.

По умолчанию: *DropLog*

Default TTL

С помощью данной настройки можно указать значение TTL NetDefendOS, используемое при генерировании пакетов. Как правило, диапазон данных значений – от 64 до 255.

По умолчанию: *255*

Layer Size Consistency

Настройка используется для проверки того, что информация о размере в каждом «слое» (Ethernet, IP, TCP, UDP, ICMP) соответствует содержанию других слоев.

По умолчанию: *ValidateLogBad*

SecuRemoteUDP Compatibility

Данная настройка позволяет содержать более 8 байт в поле UDP IP-данных. Checkpoint SecuRemote нарушает NAT-T.

По умолчанию: *Выключено*

IP Option Sizes

Проверяет размер опций IP-заголовка. Данные опции представляют собой небольшие блоки информации, которые можно добавить в конце каждого заголовка IP-адреса. Данная функция проверяет размер широко известных опций и гарантирует отсутствие опций, превышающих ограничение, заданное IP-заголовком.

По умолчанию: *ValidateLogBad*

IP Option Source/Return

Указывает, разрешена ли опция маршрутизации от источника. Эти опции позволяют отправителю управлять маршрутом пакета, проходящим через маршрутизатор или межсетевой экран. Таким образом, существует огромный риск безопасности. Система NetDefendOS никогда не руководствуется маршрутами от источников, определенными данными опциями, независимо от данной настройки.

По умолчанию: *DropLog*

IP Options Timestamps

Благодаря опции Метка времени (Time stamp) каждый маршрутизатор и межсетевой экран информирован о времени перенаправления пакета. Данные опции не применяются при стандартном трафике. Метки времени также могут использоваться для «записи» маршрута пакета, принятого от отправителя в конечной точке назначения. Система NetDefendOS никогда не выполняет ввод информации для этих опций, независимо от данной настройки.

По умолчанию: *DropLog*

IP router alert option

Используется для управления IP-пакетами, содержащими уведомление об опасности.

По умолчанию: *ValidateLogBad*

IP Options Other

Все остальные опции, кроме перечисленных выше.

По умолчанию: *DropLog*

Directed Broadcasts

С помощью данной настройки система NetDefendOS может перенаправить пакеты, направленные по адресу широковещательной рассылки в непосредственно подключенной сети. Данная функция выполняется за счет добавления каналов в раздел Правила. Эта форма проверки быстрее, чем записи в разделе Правила, так как является более специализированной.

По умолчанию: *DropLog*

IP Reserved Flag

С помощью данной настройки можно указать действия системы NetDefendOS, если в «зарезервированных» полях IP-заголовков существуют данные. В обычных обстоятельствах данные поля содержат 0. Используется для опознавания удаленной ОС (Fingerprinting).

По умолчанию: *DropLog*

Strip DontFragment

Используется для снятия флага «Не фрагментировать» для пакетов, размер которых равен или меньше значения, определенного данной настройкой.

По умолчанию: *65535 байт*

Multicast Mismatch

Задает действие, которое необходимо выполнить, если адреса Ethernet и IP multicast не совпадают.

По умолчанию: *DropLog*

Min Broadcast TTL

Минимальное значение Time-To-Live IP broadcast, разрешенное при получении.

По умолчанию: *1*

Low Broadcast TTL Action

Задает действие, которое необходимо выполнить при слишком низком значении TTL broadcast.

По умолчанию: *DropLog*

13.2. Настройки TCP-уровня

TCP Option Sizes

Используется для проверки размера TCP-опций. Данная функция действует таким же образом, что и *IPOptionSizes*, описанная выше.

По умолчанию: *ValidateLogBad*

TCP MSS Min

Задает минимальный разрешенный размер TCP MSS. Пакеты, содержащие значение размера MSS ниже данного значения, обрабатываются в соответствии со следующей настройкой.

По умолчанию: *100 байт*

TCP MSS on Low

Задает действие, которое необходимо выполнить по отношению к пакетам, если значение MSS ниже указанного значения *TCPMSSMin*. Слишком низкие значения могут вызвать проблемы в стеках TCP.

По умолчанию: *DropLog*

TCP MSS Max

Задает максимальный разрешенный размер TCP MSS. Пакеты, содержащие значение размера MSS выше данного значения, обрабатываются в соответствии со следующей настройкой.

По умолчанию: *1460 байт*

TCP MSS VPN Max

Как и в случае с *TCPMSSMax*, определен максимальный разрешенный размер TCP сегмента. Однако, данная настройка контролирует MSS только в VPN-соединениях. Таким образом, NetDefendOS может сократить размер сегмента, используемый TCP во всех VPN-соединениях. При этом сокращается фрагментация TCP в VPN-соединении даже в случаях, когда хосты не выполняют обнаружение MTU.

По умолчанию: *1400 байт*

TCP MSS On High

Задает действие, которое необходимо выполнить по отношению к пакетам, если значение MSS превышает указанное значение *TCPMSSMax*. Слишком высокие значения могут вызвать проблемы в плохо организованной сети или привести к слишком большому количеству фрагментированных пакетов, что может негативно повлиять на производительность.

По умолчанию: *Adjust*

TCP MSS Log Level

Определяет момент записи в журнале при слишком большом значении TCP MSS, если это не было выполнено опцией *TCPMSSOnHigh*.

По умолчанию: *7000 байт*

TCP Auto Clamping

Автоматически сжимает значение TCP MSS в соответствии с MTU задействованных интерфейсов, помимо TCPMSSMax.

По умолчанию: *Включено*

TCP Zero Unused ACK

С помощью данной настройки система NetDefendOS может установить значение 0 в поле Sequence Number и Acknowledgment Number в TCP-пакетах, если оно не используется. Некоторые операционные системы отображают таким способом информацию о порядковом номере, что значительно упрощает захват установленных соединений злоумышленниками.

По умолчанию: *Включено*

TCP Zero Unused URG

Снимает указатели URG со всех пакетов.

По умолчанию: *Включено*

TCP Option WSOPT

Опция Window-Scaling применяется для увеличения размера окна, используемого протоколом TCP, таким образом, данная опция используется для увеличения количества информации, которое можно отправить, пока отправитель ожидает ACK. Опция используется для опознавания удаленной ОС (Fingerprinting). WSOPT находит широкое применение в современных сетях.

По умолчанию: *ValidateLogBad*

TCP Option SACK

Опция Selective Acknowledgement (SACK) TCP используется для установки битов ACK отдельных пакетов вместо целой серии пакетов, что может повысить производительность соединений, в которых происходит потеря пакетов. Опция используется для опознавания удаленной ОС (Fingerprinting). SACK находит широкое применение в современных сетях.

По умолчанию: *ValidateLogBad*

TCP Option TSOPT

Опция Time Stamp (Метка времени). Как указывает метод PAWS (Protect Against Wrapped Sequence numbers), TSOPT используется для предотвращения «превышения» максимального значения порядкового номера (32-битовое число) без уведомления получателя.

Как правило, это не вызывает проблем. С помощью TSOPT некоторые стеки TCP оптимизируют соединение, измеряя время, потраченное на передачу пакета. Данная информация может значительно ускорить повторную отправку. Опция используется для опознавания удаленной ОС (Fingerprinting). TSOPT находит широкое применение в современных сетях.

По умолчанию: *ValidateLogBad*

TCP Option ALTCHKREQ

Опция запроса альтернативной контрольной суммы. Первоначально данная опция предназначалась для помощи в выборе наиболее точной контрольной суммы в TCP. Тем не менее, современные системы не поддерживают данную опцию.

По умолчанию: *StripLog*

TCP Option ALTCHKDATA

Данная опция используется для передачи альтернативных контрольных сумм при разрешении ALTCHKREQ. Как правило, не встречается в современных сетях.

По умолчанию: *StripLog*

TCP Option Con Timeout

С помощью данной опции система NetDefendOS управляет счетчиком соединений.

По умолчанию: *StripLogBad*

TCP Option Other

Все остальные TCP-опции. Как правило, не встречаются в современных сетях.

По умолчанию: *StripLog*

TCP SYN/URG

Задает способ обработки системой NetDefendOS TCP-пакетов с установленными флагами SYN (синхронизировать) и URG (срочные данные). Установленный флаг SYN указывает на установку нового соединения, а флаг URG указывает на то, что пакет содержит данные, требующие срочного внимания. Не рекомендуется устанавливать два этих флага в одном пакете, так как они используются для поврежденных компьютеров в плохо организованной сети.

По умолчанию: *DropLog*

TCP SYN/PSH

Задает способ обработки системой NetDefendOS TCP-пакетов с установленными флагами SYN и PSH (push). Флаг PSH указывает на то, что получатель должен немедленно отправить информацию в пакете приложению назначения на компьютере.

Не рекомендуется устанавливать два этих флага в одно и то же время, так как это может вызвать сбой в плохо организованной сети. Тем не менее, некоторые системы Apple MAC используют TCP нестандартным способом и отправляют SYN-пакеты с установленным флагом PSH. По этой причине система NetDefendOS, как правило, снимает флаг PSH и разрешает прохождение пакета, несмотря на то, что такие пакеты должны быть отброшены.

По умолчанию: *StripSilent*

TCP SYN/RST

Флаг TCP RST вместе с SYN, как правило, некорректный (strip=strip RST).

По умолчанию: *DropLog*

TCP SYN/FIN

Флажок TCP FIN вместе с SYN, как правило, некорректный (strip=strip FIN).

По умолчанию: *DropLog*

TCP FIN/URG

Задает способ обработки системой NetDefendOS TCP-пакетов с установленными флагами FIN (завершить соединение) и URG. Как правило, не применяется, так как пользователь не выполняет одновременно завершения соединения и отправку важных данных. Данная комбинация флагов может привести к сбоям в плохо организованной сети, также используется для опознавания удаленной ОС (Fingerprinting).

По умолчанию: *DropLog*

TCP URG

Задает способ обработки системой NetDefendOS TCP-пакетов с установленным флагом URG, не

принимая во внимание остальные флаги. Некоторые TCP-стеки и приложения неправильно работают с флагами Urgent, что в худшем случае может привести к прекращению работы. Помните, что некоторые программы, такие как FTP и MS SQL Server, почти всегда используют флаг URG.

По умолчанию: *StripLog*

TCPE ECN

Задает способ обработки системой NetDefendOS TCP-пакетов с установленными флагами Xmas и Ymas. В основном, данные флаги используются для опознавания удаленной ОС (Fingerprinting).

Следует отметить, что развивающийся стандарт *Explicit Congestion Notification* также использует эти флаги, но поскольку данный стандарт поддерживает лишь небольшое количество операционных систем, следует снять флаги.

По умолчанию: *StripLog*

TCP Reserved Field

Задает способ обработки системой NetDefendOS информации, представленной в зарезервированном поле в заголовке TCP, как правило, это 0. Это поле отличается от флагов Xmas и Ymas. Используется для опознавания удаленной ОС (Fingerprinting).

По умолчанию: *DropLog*

TCP NULL

Задает способ обработки системой NetDefendOS TCP-пакетов без установленных флагов SYN, ACK, FIN или RST. Согласно стандарту TCP такие пакеты являются недействительными и используются для опознавания удаленной ОС (Fingerprinting), а также сканерами скрытых портов, так как некоторые межсетевые экраны не способны их обнаружить.

По умолчанию: *DropLog*

TCP Sequence Numbers

Перед перенаправлением TCP-пакета значение поля Sequence number TCP-пакета будет сравниваться с окном получателя.

Проверка поля Sequence number TCP-пакета возможна только в соединениях, отслеживаемых механизмом state-engine (не для пакетов, перенаправленных с помощью правила *FwdFast*).

Возможные значения:

Ignore – Не выполнять проверку. Указывает на то, что проверка поля Sequence number выключена.
ValidateSilent – Выполнить проверку и продолжить.
ValidateLogBad – Выполнить проверку и продолжить, при возникновении проблемы зарегистрировать запись в журнале.
ValidateReopen – Выполнить проверку попытки восстановления стандартного соединения; выполнить проверку и продолжить.
ValidateReopenLog – Выполнить проверку попытки восстановления стандартного соединения; выполнить проверку, при возникновении проблемы зарегистрировать запись в журнале.
ReopenValidate – Не выполнять проверку попытки восстановления соединения; выполнить проверку и продолжить.
ReopenValidLog – Не выполнять проверку попытки восстановления соединения; выполнить проверку, при возникновении проблемы зарегистрировать запись в журнале.
По умолчанию: *ValidateLogBad*

Примечания к настройке *TCPSequenceNumbers*

Значение по умолчанию *ValidateLogBad* (или *ValidateSilent*) разрешает попытки повторно установить TCP-соединение, это означает, что попытки восстановления соединения с применением ранее используемого поля Sequence number будут отклонены.

ValidateReopen и *ValidReopenLog* являются особыми настройками, обеспечивающими действия по умолчанию в предыдущих версиях NetDefendOS, где разрешены попытки повторной установки соединения только с использованием поля Sequence number внутри текущего (или последнего) окна TCP. При этом существует больше ограничений, чем при использовании *ValidateLogBad/ValidateSilent*, и некоторые корректные попытки повторной установки TCP-соединений будут заблокированы. Это приведет к значительному сокращению трафика, потраченного на просмотр Web-страниц (короткие, но завершенные запросы от небольшого количества клиентов с интервалом в несколько секунд), в то время как трафик TCP не будет затронут.

Тем не менее, не рекомендуется использовать *ValidateReopen* или *ValidateReopenLog*, так как можно достичь тот же результат за счет запрета повторной установки TCP-соединения. Данные настройки существуют, главным образом, для обратной совместимости.

ReopenValidate и *ReopenValidLog* имеют меньше ограничений, чем *ValidateLogBad* или *ValidateSilent*. Некоторые клиенты и/или операционные системы могут использовать случайно выбранное поле Sequence number при восстановлении предыдущего TCP-соединения (как правило, из соображений безопасности), при использовании данных настроек возможна некорректная работа соединения. Скорее всего, будет затронут трафик, потраченный на просмотр Web-страниц, и данное воздействие будет происходить в произвольном порядке. Использование данных значений вместо значения по умолчанию полностью отключит проверку поля Sequence number при повторной установке TCP-соединения. После установки соединения возобновляется обычная проверка поля Sequence number TCP-пакета.

Allow TCP Reopen

Позволяет клиентам восстановить завершенные TCP-соединения.

По умолчанию: *Выключено*

13.3. Настройки ICMP-уровня

ICMP Sends Per Sec Limit

Задает максимальное количество ICMP-сообщений в секунду, генерируемых системой NetDefendOS, включая ответы на запрос ping, сообщения Destination unreachable (точка назначения недоступна), а также пакеты TCP RST. Другими словами, данная настройка ограничивает количество Отказов в секунду, которые генерируются правилами Отказа (Reject rules) в разделе Правила.

По умолчанию: *500*

Silently Drop State ICMPErrors

С помощью данной настройки система NetDefendOS может отбрасывать ICMP-пакеты с ошибками в отслеживаемых открытых соединениях. Если пакеты с ошибками не будут отброшены, они проходят дальше и подвергаются обработке согласно набору правил.

По умолчанию: *Включено*

13.4. Настройки состояний

Connection Replace

С помощью данной настройки можно добавить новые соединения в список соединений NetDefendOS с заменой старых записей, если нет свободного пространства.

По умолчанию: *ReplaceLog*

Log Open Fails

В некоторых случаях, когда правило разрешает прохождение пакета, впоследствии механизм Stateful Inspection может решить, что пакет не может открыть новое соединение. Например, ситуация, когда для TCP-пакета, прохождение которого было разрешено правилами и который не является частью установленного соединения, не установлен флаг SYN. Такие пакеты не могут открывать новые соединения. Помимо этого, ICMP-сообщения, за исключением ICMP ECHO (Ping), также никогда не смогут открыть новые соединения. С помощью данной настройки NetDefendOS может регистрировать такие пакеты.

По умолчанию: *Включено*

Log Reverse Opens

С помощью данной настройки система NetDefendOS регистрирует в Журнале запись о пакетах, которые пытаются открыть новое соединение через уже открытое соединение. Функция применяется только к TCP-пакетам с установленным флагом SYN и пакетам ICMP ECHO. При использовании других протоколов, например, UDP, невозможно определить, пытается ли удаленный узел открыть новое соединение.

По умолчанию: *Включено*

Log State Violations

С помощью данной настройки система NetDefendOS регистрирует пакеты, которые нарушают предполагаемую диаграмму коммутации соединения, например, получение пакетов TCP FIN в ответ на пакеты TCP SYN.

По умолчанию: *Включено*

Log Connections

Данная настройка используется для регистрации соединений системой NetDefendOS:

- *NoLog* – Не регистрирует ни одного соединения, таким образом, не имеет значения, включена ли регистрация для правила *Allow* или для правила *NAT* в наборе IP-правил; они не будут зарегистрированы. Тем не менее, правила *FwdFast, Drop и Reject* будут зарегистрированы, как указано в настройках раздела Правила.

- *Log* – Регистрирует соединения в краткой форме; предоставляет короткое описание соединения, разрешенное правилом, и любого применяемого правила *SAT*. После закрытия соединений, они также будут зарегистрированы.

- *LogOC* – Действует так же, как и *Log*, но включает два пакета, которые открывают и закрывают соединение. Если соединение закрыто по истечении таймаута, закрывающие пакеты не будут зарегистрированы.

- *LogOCAll* – Регистрирует все пакеты, задействованные в открытии и закрытии соединения. При использовании TCP регистрирует все пакеты с установленными флагами SYN, FIN или RST.

- *LogAll* – Регистрирует все пакеты.

По умолчанию: *Log*

Log Connection Usage

При использовании данной настройки создается сообщение для каждого пакета, проходящего через соединение, установленное в state-engine NetDefendOS. Трафик, назначением которого является межсетевой экран, например, трафик управления NetDefendOS, не является объектом для данной настройки.

Сообщение, регистрируемое в Журнале, содержит информацию о порте, службе, IP-адресе и интерфейсе источника/назначения. Следует включить данную настройку исключительно в целях диагностики и проверки, так как это приведет к генерированию большого количества сообщений и может значительно снизить работоспособность.

По умолчанию: *Выключено*

Dynamic Max Connections

С помощью данной настройки динамически назначается максимальное количество соединений.

По умолчанию: *Включено*

Max Connections

Данная настройка применяется, если указанная выше опция **Dynamic Max Connections** выключена. С помощью данной настройки можно указать максимальное количество одновременно открытых соединений, поддерживаемых системой NetDefendOS. Каждое соединение занимает около 150 байт RAM. Если настройка динамическая, NetDefendOS попытается использовать столько соединений, сколько разрешено устройством.

По умолчанию: *8192*

13.5. Настройки таймаута соединений

С помощью настроек данного раздела можно указать количество времени простоя соединения, т.е. периода времени, когда не выполняется отправка данных, перед автоматическим закрытием соединения. Пожалуйста, помните, что для каждого соединения указываются два значения таймаута, по одному для каждого направления. Соединение будет закрыто, если любое из двух значений достигнет 0.

TCP SYN Idle Lifetime

Задает время простоя (в секундах) не полностью установленного TCP-соединения перед его закрытием.

По умолчанию: *60*

TCP Idle Lifetime

Задает время простоя (в секундах) полностью установленного TCP-соединения перед его закрытием. Соединение считается полностью установленным, если пакеты с неустановленными флагами SYN прошли в обоих направлениях соединения.

По умолчанию: *262144*

TCP FIN Idle Lifetime

Задает время простоя (в секундах) TCP-соединения перед его непосредственным закрытием. Соединения переходят в это состояние, когда пакет с установленным флагом FIN проходит в любом направлении.

По умолчанию: *80*

UDP Idle Lifetime

Задает время простоя (в секундах) UDP-соединения перед его закрытием. Как правило, данное значение таймаута низкое, так как UDP не поддерживает способы уведомления о скором закрытии соединения.

По умолчанию: *130*

UDP Bidirectional Keep-alive

Данная настройка позволяет обеим сторонам поддерживать действующее UDP-соединение. По умолчанию, соединение считается действующим (без простоя) при каждой отправке данных стороной, открывшей соединение. Соединения, которые не получают данные от стороны, открывшей соединение, будут закрыты по этой причине в течение времени действия UDP, даже если одна сторона продолжает передачу данных.

По умолчанию: *Выключено*

Ping Idle Lifetime

Задает время простоя (в секундах) для Ping (ICMP ECHO) перед закрытием.

По умолчанию: *8*

IGMP Idle Lifetime

Время действия (в секундах) для IGMP-соединения.

По умолчанию: *12*

Other Idle Lifetime

Задает время простоя (в секундах) для соединения, использующего неизвестный протокол.

По умолчанию: *130*

13.6. Настройки ограничения размеров

Данный раздел содержит информацию об ограничении размеров, накладываемом на протоколы IP-уровня, такие как TCP, UDP и ICMP.

Значения, указанные здесь, касаются IP-данных, содержащихся в пакетах. При использовании Ethernet, один пакет может содержать до 1480 байт IP-данных без фрагментации. Помимо этого, существует 20 байт заголовка IP-адреса и 14 байт заголовка Ethernet, что соответствует максимальному количеству данных, передаваемых в сети Ethernet – 1514 байт.

Max TCP Length

Задает максимальный размер TCP-пакета, включая заголовок. Как правило, данное значение связано с количеством IP-данных, которые можно собрать в нефрагментированный пакет, так как TCP, как правило, выбирает перед отправкой сегменты максимального размера. Тем не менее, возможно потребуется увеличить данное значение на 20-50 байт в некоторых нетипичных VPN-системах.

По умолчанию: *1480*

Max UDP Length

Задает максимальный размер UDP-пакета, включая заголовок (в байтах). Возможно, потребуется увеличить данное значение, так как множество приложений, действующих в режиме реального времени, используют фрагментированные UDP-пакеты большого размера. Если такие протоколы не используются, ограничение размера, налагаемое на UDP-пакеты, может быть снижено до 1480 байт.

По умолчанию: *60000*

Max ICMP Length

Задает максимальный размер ICMP-пакета (в байтах). Размер ICMP-сообщений с ошибками никогда не должен превышать 600 байт, хотя размер пакетов Ping может быть больше, если требуется. Данное значение может быть снижено до 1000 байт, если нет необходимости использовать пакеты Ping большого размера.

По умолчанию: *10000*

Max GRE Length

Задает максимальный размер GRE-пакета (в байтах). Протокол GRE (Generic Routing Encapsulation) используется в различных целях, включая передачу данных по протоколу PPTP (Point to Point Tunneling Protocol). В качестве данного значения должен быть указан размер самого большого пакета, которому разрешено проходить через VPN-соединения, не принимая во внимание первоначальный протокол, прибавив приблизительно 50 байт.

По умолчанию: *2000*

Max ESP Length

Задает максимальный размер (в байтах) ESP-пакета. ESP (Encapsulation Security Payload) используется в IPsec для шифрования данных. В качестве данного значения должен быть указан размер самого большого пакета, которому разрешено проходить через VPN-соединения, не принимая во внимание первоначальный протокол, прибавив приблизительно 50 байт.

По умолчанию: *2000*

Max AH Length

Задает максимальный размер AH-пакета (в байтах). AH (Authentication Header) используется в IPsec для аутентификации. В качестве данного значения должен быть указан размер самого большого пакета, которому разрешено проходить через VPN-соединения, не принимая во внимание первоначальный протокол, прибавив приблизительно 50 байт.

По умолчанию: *2000*

Max SKIP Length

Задает максимальный размер SKIP-пакета (в байтах).

По умолчанию: *2000*

Max OSPF Length

Задает максимальный размер OSPF-пакета (в байтах). OSPF – это протокол маршрутизации, используемый главным образом в крупных сетях LAN.

По умолчанию: *1480*

Max IPIP/FWZ Length

Задает максимальный размер IP-in-IP пакета (в байтах). IP-in-IP используется в VPN соединениях межсетевыми экранами Checkpoint Firewall-1 в случае, если IPsec не используется. В качестве данного значения должен быть указан размер самого большого пакета, которому разрешено проходить через VPN-соединения, не принимая во внимание первоначальный протокол, прибавив приблизительно 50 байт.

По умолчанию: *2000*

Max IPsec IPComp Length

Задает максимальный размер IPComp-пакета (в байтах).

По умолчанию: *2000*

Max L2TP Length

Задает максимальный размер пакета, передаваемого по протоколу туннелирования уровня 2 (в байтах).

По умолчанию: *2000*

Max Other Length

Задает максимальный размер пакетов (в байтах), передаваемых по протоколам, не указанным выше.

По умолчанию: *1480*

Log Oversized Packets

С помощью данной настройки NetDefendOS будет регистрировать пакеты, размер которых превышен.

По умолчанию: *Включено*

13.7. Настройки фрагментации

По IP-протоколу можно передавать до 65536 байт данных. Тем не менее, большинство сетей, например, Ethernet, не поддерживают передачу таких больших пакетов. Данные фрагментируются на отдельные пакеты, предназначенные для отправки, у каждого из которых есть собственный IP-заголовок и информация, которая поможет получателю корректно собрать все фрагменты в первоначальный пакет.

Тем не менее, множество IP-стеков не способны обрабатывать пакеты, которые были неправильно фрагментированы, и этим могут воспользоваться злоумышленники. Система NetDefendOS обеспечивает защиту подобных атак с помощью нескольких способов.

Pseudo Reass Max Concurrent

Максимальное количество одновременных сборок фрагментов. Для того чтобы отбросить все фрагментированные пакеты, установите значение 0 для PseudoReass_MaxConcurrent.

По умолчанию: *1024*

Illegal Fragments

Задает способ обработки неправильно собранных фрагментов. Термин «неправильно собранные» относится к перекрывающимся фрагментам, дублированным фрагментам с различными данными, к фрагментам с неправильными размерами и т. д. Используются следующие настройки:

- *Drop* – Отбрасывает неразрешенный фрагмент, не регистрируя запись в журнале. В памяти сохраняется информация, что собираемый пакет является «подозрительным», что может использоваться в дальнейшем.

- *DropLog* – Отбрасывает и регистрирует неразрешенный фрагмент. В памяти сохраняется информация, что собираемый пакет является «подозрительным», что может использоваться в дальнейшем.

- *DropPacket* – Отбрасывает неразрешенный фрагмент и все предварительно сохраненные фрагменты. Запрещает дальнейшее прохождение фрагментов этого пакета в течение периода ReassIllegalLinger (в секундах).

- *DropLogPacket* – Действует так же, как и опция *DropPacket,* но с регистрацией события.

- *DropLogAll* – Действует так же, как и опция *DropLogPacket*, но регистрирует фрагменты, принадлежащие пакету, который приходит в течение периода ReassIllegalLinger (в секундах).

Два фактора влияют на выбор следующих действий: отбросить индивидуальные фрагменты или запретить прохождение целого пакета:

- В целях безопасности лучше отбрасывать целый пакет.

- Если в результате получения неразрешенного фрагмента, Вы выберите действие «отбросить целый пакет», злоумышленники смогут прервать обмен данными, отправив неразрешенные фрагменты во время сборки пакета, и заблокируют, таким образом, почти все соединения.

- По умолчанию: *DropLog – отбрасывает отдельные фрагменты, при этом в памяти сохраняется информация о том, что собираемый пакет является «подозрительным».*

Duplicated Fragment Data

Если один и тот же фрагмент приходит несколько раз, это может означать, что либо он был дублирован, либо, что злоумышленник пытается нарушить сборку пакета. Для того чтобы

определить причину, система NetDefendOS сравнивает компоненты данных фрагмента. Сравнение фрагментов осуществляется по 2 - 512 случайным образом выбранным частям фрагмента, выбираются четыре байта из каждой части в качестве образца. Чем больше количество образцов для сравнения, тем выше вероятность обнаружения несовпадающих дубликатов. Однако, большое количество сравнений может привести к увеличению загрузки CPU.

По умолчанию: *Check8 – сравнивает 8 случайным образом выбранным частей фрагмента, всего 32 байта.*

Failed Fragment Reassembly

Сборка пакета может быть прервана по одной из следующих причин:

- Некоторые фрагменты не пришли в течение времени, указанного в настройках ReassTimeout или ReassTimeLimit. Это может означать, что один или более фрагментов были потеряны во время передачи в сети Интернет, что случается довольно часто.

- Система NetDefendOS была вынуждена прервать сборку пакета, так как были получены новые фрагментированные пакеты, и система временно израсходовала ресурсы. В подобных ситуациях предыдущая сборка будет отменена или будет зафиксирован «сбой сборки».

- Злоумышленник попытался отправить некорректно фрагментированный пакет.

В обычных обстоятельствах нет необходимости регистрировать часто происходящие сбои. Тем не менее, регистрация сбоев с наличием «подозрительных» фрагментов может оказаться полезной. Подобные сбои случаются, если, например, для настройки IllegalFrags установлено значение Drop, а не DropPacket.

Для FragReassemblyFail доступны следующие настройки:

- *NoLog* – Запись о прекращении сборки не регистрируется в журнале.

- *LogSuspect* – Регистрирует неудачную сборку только в случае обнаружения «подозрительных» фрагментов.

- *LogSuspectSubseq* – Действует так же, как *LogSuspect*, но с регистрацией последующих фрагментов пакета по мере их получения.

- *LogAll* – Регистрирует все неудавшиеся попытки сборки пакета.

- LogAllSubseq – Действует так же, как *LogAll*, но с регистрацией последующих фрагментов пакета по мере их получения.

По умолчанию: *LogSuspectSubseq*

Dropped Fragments

Если пакет был отброшен в соответствии с настройками в разделе Правила, возможно, отдельные фрагменты этого пакета будут зарегистрированы. С помощью настройки DroppedFrags можно указать действия системы NetDefendOS. Настройки для этого правила будут следующими:

- *NoLog* – Регистрация не выполняется (помимо отмены регистрации, указанной в наборе правил).

- *LogSuspect* – Регистрирует неудачную сборку, только в случае обнаружения «подозрительных» фрагментов.

- *LogAll* – Всегда регистрирует отдельные отброшенные фрагменты.

По умолчанию: *LogSuspect*

Duplicate Fragments

Если один и тот же фрагмент приходит несколько раз, это может означать, что либо он был дублирован в какой-либо точке своего маршрута, либо, что злоумышленник пытается нарушить сборку пакета. С помощью настройки DuplicateFrags можно зарегистрировать в Журнале такой фрагмент. Помните, что с помощью DuplicateFragData также можно зарегистрировать фрагменты, если данные, содержащиеся в них, не совпадают. Возможные настройки будут следующими:

- *NoLog* – В обычных обстоятельствах регистрация не выполняется.
- *LogSuspect* – Регистрирует дублированные фрагменты, если при сборке были обнаружены «подозрительные» фрагменты.
- *LogAll* – Всегда регистрирует дублированные фрагменты.

По умолчанию: *LogSuspect*

Fragmented ICMP

За исключением ICMP ECHO (Ping), ICMP-сообщения не должны быть фрагментированы, так как они содержат такой маленький объем данных, что фрагментация не требуется. С помощью настройки FragmentedICMP можно указать действие, которое необходимо предпринять, когда NetDefendOS получает фрагментированные ICMP-сообщения, которые не являются ни ICMP ECHO, ни ECHOREPLY.

По умолчанию: *DropLog*

Minimum Fragment Length

С помощью данной настройки можно указать минимальный размер фрагмента пакета в байтах, за исключением конечного фрагмента.

Хотя получение слишком большого количества фрагментов минимального размера может вызвать проблемы в сети, невозможно установить слишком высокое ограничение. В редких случаях отправители создают фрагменты небольшого размера. Тем не менее, пользователь может отправить фрагменты размером 1480 байт и во время прохождения через маршрутизатор или VPN-туннель к получателю значение MTU снижается до 1440 байт. В результате будут созданы фрагменты размером 1440 байт и одинаковое число фрагментов размером 40 байт. Так как это может привести к потенциальным проблемам, настройки NetDefendOS по умолчанию разрешают прохождение фрагментов минимального размера, 8 байт. Для внутреннего использования, когда все размеры известны, данное значение может быть увеличено до 200 байт и более.

По умолчанию: *8*

Reassembly Timeout

Попытка сборки будет прервана, если в течение Таймаута при сборке (в секундах) не пришли последующие фрагменты.

По умолчанию: *65*

Max Reassembly Time Limit

Попытка сборки будет прервана в течение периода Reassembly Time Limit после первого полученного фрагмента.

По умолчанию: *90*

Reassembly Done Limit

После сборки пакета система NetDefendOS может сохранить в памяти сборку для данного количества

секунд, чтобы предотвратить приход следующих фрагментов, например, старых дублированных фрагментов.

По умолчанию: *20*

Reassembly Illegal Limit

После того, как целый пакет отмечен как разрешенный, система NetDefendOS может сохранить это в памяти для данного количества секунд, чтобы предотвратить приход следующих фрагментов данного пакета.

По умолчанию: *60*

13.8. Настройки сборки фрагментов в локальной сети

Max Concurrent

Максимальное количество одновременных сборок в локальной сети.

По умолчанию: *256*

Max Size

Максимальный размер пакета, собранного в локальной сети.

По умолчанию: *1000*

Large Buffers

Количество буферов сборки с большой емкостью (более 2K) в локальной сети.

По умолчанию: *32*

13.9. Остальные настройки

UDP Source Port 0

Настройка используется для обработки UDP-пакетов с портом источника 0.

По умолчанию: *DropLog*

Port 0

Настройка используется для обработки TCP/UDP-пакетов с портом назначения 0 и TCP-пакетов с портом источника 0.

По умолчанию: *DropLog*

Watchdog Time

Количество секунд без ответа перед запуском таймера Watchdog.

По умолчанию: *180*

Flood Reboot Time

Система NetDefendOS автоматически перезагружается, если буферы заполнены в течение длительногого времени. С помощью данной настройки можно указать количество этого времени.

По умолчанию: *3600*

Max Connections

При сборке пакета все IP-фрагменты комплектуются в IP-датаграммы и, если используется TCP, выполняется реорганизация сегментов для их обработки в правильном порядке и также, чтобы отслеживать потенциально перекрывающиеся сегменты и информировать другие подсистемы о подобных перекрытиях.

С помощью данной настройки можно указать максимальное количество соединений. Данное количество выражается в процентах от общего числа разрешенных соединений. Минимум 1, Максимум 100.

По умолчанию: *80*

Max Memory

С помощью данной настройки можно указать количество памяти, выделяемое системой сборки на обработку пакетов. Данное количество выражается в процентах от общего количества доступной памяти. Минимум 1, Максимум 100.

По умолчанию: *3*

Max Pipe Users

С помощью данной настройки можно указать максимальное количество пользователей канала. Так как отслеживание выполняется только на 20-ой секунде, то количество пользователей канала, как правило, не соответствует количеству существующих пользователей или отслеживаемых соединений с сохранением состояния. Если каналы не установлены, количество пользователей не указывается, независимо от данной настройки. Для получения более подробной информации о каналах и пользователях, см. *Раздел 10.1, «Traffic Shaping»*.

По умолчанию: *512*

Приложение A. Подписка на обновления

Обзор

Для работы антивирусной (AV) защиты, обнаружения и предотвращения вторжений (IDP) и динамической фильтрации Web-содержимого требуются базы данных D-Link, которые содержат подробную информацию о новейших вирусах, угрозах и классификации URL. Данные базы данных постоянно обновляются и для того, чтобы получить доступ к последним обновлениям, необходимо получить Подписку на обновления от D-Link. Это выполняется следующим образом:

- Подписка приобретается у одного из поставщиков D-Link.
- После приобретения Вы получает уникальный код активации, идентифицирующий Вас как пользователя услуги.
- Зайдите в **Обслуживание > Лицензия** в Web-интерфейсе межсетевого экрана NetDefend и введите код активации. Система NetDefendOS идентифицирует код, и услуга обновления будет активирована (выполняя данное действие, убедитесь в наличии доступа к сети Интернет).

Совет: Руководство регистрации доступно для загрузки

Пошаговое «Руководство регистрации» содержит подробную информацию о регистрации и услуге обновления и доступно для загрузки на web-сайте D-Link.

Продление подписки

В web-интерфейсе зайдите в **Обслуживание > Лицензия** для того, чтобы проверить, какие службы обновления активированы и когда заканчивается срок подписки.

Важно: Своевременное продление подписки

Продлите подписку до завершения срока действия! Не откладывайте это на последний момент.

Отслеживание обновлений базы данных

Для настройки автоматического обновления базы данных зайдите в меню Web-интерфейса **Maintenance > Update**. Также можно проверить время и статус последней попытки обновления.

В том же меню Web-интерфейса можно настроить обновление вручную выбрав **Update now**, чтобы загрузить последние сигнатуры в базу данных.

Консольные команды для управления базами данных

Управление базами данных IDP и Антивируса (AV) осуществляется с помощью ряда консольных команд.

Обновление баз данных

Обновление базы данных IDP можно выполнить в любое время с помощью следующей команды:

```
gw-world:/> updatecenter -update IDP
```

Обновление базы данных антивируса выполняется таким же образом с помощью команды:

```
gw-world:/> updatecenter -update Antivirus
```

Запрос статуса обновления

Для получения статуса обновления базы данных IDP используйте команду:

```
gw-world:/> updatecenter -status IDP
```

Для получения статуса обновления базы данных AV используйте команду:

```
gw-world:/> updatecenter -status Antivirus
```

Запрос статуса сервера

Для получения статуса сервера используйте команду:

```
gw-world:/> updatecenter -servers
```

Удаление локальных баз данных

Удаление баз данных или перезагрузка является решением некоторых технических проблем, возникающих при работе функции IDP или антивируса. Для удаления базы данных IDP используется команда:

```
gw-world:/> removedb IDP
```

Для удаления антивирусной базы данных используется команда:

```
gw-world:/> removedb Antivirus
```

После удаления следует перезапустить систему и выполнить обновление базы данных. Также

удаление базы данных рекомендуется в случае, когда IDP или антивирус долгое время не используются.

Примечание: Обновление базы данных может вызвать паузу в процессе обработки

После загрузки для оптимизации обновления антивирусной базы данных требуется несколько секунд. Это приведет к остановке работы межсетевого экрана. Поэтому для времени обновления следует выбирать часы низкого потребления трафика, например, утро. Удаление базы данных также может привести к остановке работы.

Приложение Б. Группы сигнатур IDP

Для выполнения сканирования IDP на выбор доступны следующие группы сигнатур. Эти группы доступны только для Расширенного сервиса IDP D-Link. Для каждой группы существует три *Tuna* **IDS**, **IPS** и **Policy**. Для получения подробной информации обратитесь к *Разделу 6.5, «Обнаружение и предотвращение вторжений»*.

Имя группы	**Тип вторжения**
APP_AMANDA	Amanda, популярное ПО для резервного копирования
APP_ETHEREAL	Ethereal
APP_ITUNES	Медиаплеер Apple iTunes
APP_REALPLAYER	Медиаплеер RealNetworks
APP_REALSERVER	Медиаплеер RealServer RealNetworks
APP_WINAMP	WinAMP
APP_WMP	Медиаплеер MS Windows
AUTHENTICATION_GENERAL	Аутентификация
AUTHENTICATION_KERBEROS	Kerberos
AUTHENTICATION_XTACACS	XTACACS
BACKUP_ARKEIA	Решение для резервного копирования
BACKUP_BRIGHTSTOR	Решения для резервного копирования, созданные CA
BACKUP_GENERAL	Решения для резервного копирования
BACKUP_NETVAULT	Решение для резервного копирования
BACKUP_VERITAS	Решения для резервного копирования
BOT_GENERAL	Программы-роботы, включая боты, управляемые IRC-каналами
BROWSER_FIREFOX	Mozilla Firefox
BROWSER_GENERAL	Основные атаки на web-браузеры/клиенты
BROWSER_IE	Microsoft IE
BROWSER_MOZILLA	Браузер Mozilla
COMPONENT_ENCODER	Шифраторы как часть атаки
COMPONENT_INFECTION	Вирус как часть атаки
COMPONENT_SHELLCODE	Шелл-код как часть атак
DB_GENERAL	Системы базы данных
DB_MSSQL	Сервер MS SQL
DB_MYSQL	MySQL DBMS
DB_ORACLE	Oracle DBMS
DB_SYBASE	Сервер Sybase
DCOM_GENERAL	MS DCOM
DHCP_CLIENT	DHCP-клиент
DHCP_GENERAL	DHCP-протокол
DHCP_SERVER	DHCP-сервер
DNS_EXPLOIT	DNS-атаки
DNS_GENERAL	Система доменных имен
DNS_OVERFLOW	Атака на переполнение длины DNS запроса
DNS_QUERY	Атаки, связанные с запросом
ECHO_GENERAL	Принцип работы Echo протокола
ECHO_OVERFLOW	Переполнение буфера Echo

FINGER_BACKDOOR	Finger backdoor
FINGER_GENERAL	Принцип работы протокола Finger
FINGER_OVERFLOW	Переполнение буфера в реализации протокола Finger
FS_AFS	Файловая система AFS (Andrew File System)
FTP_DIRNAME	Атака Directory name attack
FTP_FORMATSTRING	Атака Format string attack
FTP_GENERAL	FTP-протокол и использование
FTP_LOGIN	Атака с целью определения логина
FTP_OVERFLOW	Переполнение буфера FTP
GAME_BOMBERCLONE	Игра Bomberclone
GAME_GENERAL	Generic game servers/clients
GAME_UNREAL	Игровой сервер UnReal
HTTP_APACHE	Apache httpd
HTTP_BADBLUE	Web-сервер Badblue
HTTP_CGI	HTTP CGI
HTTP_CISCO	Встроенный Web сервер Cisco
HTTP_GENERAL	Основные операции HTTP
HTTP_MICROSOFTIIS	HTTP атаки, специфичные для Web сервера MS IIS
HTTP_OVERFLOWS	Переполнение буфера для HTTP-серверов
HTTP_TOMCAT	Tomcat JSP
ICMP_GENERAL	Принцип работы ICMP-протокола
IGMP_GENERAL	IGMP
IMAP_GENERAL	Принцип работы IMAP-протокола
IM_AOL	AOL IM
IM_GENERAL	Реализация обмена мгновенными сообщениями
IM_MSN	MSN Messenger
IM_YAHOO	Yahoo Messenger
IP_GENERAL	Принцип работы IP-протокола
IP_OVERFLOW	Переполнение буфера в реализации протокола IP
IRC_GENERAL	Internet Relay Chat
LDAP_GENERAL	Основные LDAP клиенты/серверы
LDAP_OPENLDAP	Открыть LDAP
LICENSE_CA-LICENSE	Лицензия для программного обеспечения CA
LICENSE_GENERAL	Менеджер лицензии
MALWARE_GENERAL	Вредоносные атаки
METASPLOIT_FRAME	Атака с помощью metasploit frame
METASPLOIT_GENERAL	Атака Metasploit general attack
MISC_GENERAL	Основная атака
MSDTC_GENERAL	MS DTC
MSHELP_GENERAL	Справка Microsoft Windows
NETWARE_GENERAL	Основной протокол NetWare
NFS_FORMAT	Форматировать
NFS_GENERAL	Принцип работы NFS-протокола
NNTP_GENERAL	Принцип работы NNTP-протокола
OS_SPECIFIC-AIX	AIX specific
OS_SPECIFIC-GENERAL	OS general
OS_SPECIFIC-HPUX	HP-UX related
OS_SPECIFIC-LINUX	Linux specific
OS_SPECIFIC-SCO	SCO specific
OS_SPECIFIC-SOLARIS	Solaris specific
OS_SPECIFIC-WINDOWS	Windows specific
P2P_EMULE	Инструмент eMule P2P
P2P_GENERAL	Основные инструменты P2P
P2P_GNUTELLA	Инструмент Gnutella P2P
PACKINGTOOLS_GENERAL	Атака General packing tools
PBX_GENERAL	PBX
POP3_DOS	Denial of Service для POP
POP3_GENERAL	Post Office Protocol v3
POP3_LOGIN-ATTACKS	Атака с целью определения логина и пароля
POP3_OVERFLOW	Переполнение сервера POP3

POP3_REQUEST-ERRORS	Ошибка запроса
PORTMAPPER_GENERAL	PortMapper
PRINT_GENERAL	LP printing server: LPR LPD
PRINT_OVERFLOW	Переполнение буфера в реализации протокола IP или LPR/LPD
REMOTEACCESS_GOTOMYPC	Перейти в Мой компьютер
REMOTEACCESS_PCANYWHERE	PcAnywhere
REMOTEACCESS_RADMIN	Удаленный администратор
REMOTEACCESS_VNC-CLIENT	Атаки на VNC-клиентов
REMOTEACCESS_VNC-SERVER	Атаки на VNC-серверы
REMOTEACCESS_WIN-TERMINAL	Windows terminal/Удаленный рабочий стол
RLOGIN_GENERAL	RLogin протокол и использование
RLOGIN_LOGIN-ATTACK	Атаки с целью определения логина
ROUTER_CISCO	Атаки на маршрутизатор Cisco
ROUTER_GENERAL	Атаки на маршрутизатор
ROUTING_BGP	Протокол BGP
RPC_GENERAL	Принцип работы RFC-протокола
RPC_JAVA-RMI	Java RMI
RSYNC_GENERAL	Rsync
SCANNER_GENERAL	Сканеры
SCANNER_NESSUS	Сканер Nessus
SECURITY_GENERAL	Антивирусные решения
SECURITY_ISS	ПО для обеспечения безопасности
SECURITY_MCAFEE	McAfee
SECURITY_NAV	Решение Symantec AV
SMB_ERROR	Ошибка SMB
SMB_EXPLOIT	SMB Exploit
SMB_GENERAL	Атаки SMB
SMB_NETBIOS	Атаки NetBIOS
SMB_WORMS	Черви SMB
SMTP_COMMAND-ATTACK	SMTP command attack
SMTP_DOS	Denial of Service для SMTP
SMTP_GENERAL	Принцип работы SMTP-протокола
SMTP_OVERFLOW	Переполнение буфера SMTP
SMTP_SPAM	СПАМ
SNMP_ENCODING	SNMP шифрование
SNMP_GENERAL	Принцип работы SNMP-протокола
SOCKS_GENERAL	Принцип работы SOCKS-протокола
SSH_GENERAL	Принцип работы SSH-протокола
SSH_LOGIN-ATTACK	Атаки с целью определения логина и пароля
SSH_OPENSSH	Сервер OpenSSH
SSL_GENERAL	Принцип работы SSL-протокола
TCP_GENERAL	Принцип работы TCP-протокола
TCP_PPTP	Point-to-Point Tunneling Protocol
TELNET_GENERAL	Принцип работы Telnet протокола
TELNET_OVERFLOW	Telnet buffer overflow attack
TFTP_DIR_NAME	Directory Name attack
TFTP_GENERAL	Принцип работы TFTP-протокола
TFTP_OPERATION	Атака, нарушающая работоспособность
TFTP_OVERFLOW	Атака на переполнение буфера TFTP
TFTP_REPLY	TFTP Reply attack
TFTP_REQUEST	TFTP request attack
TROJAN_GENERAL	Троян
UDP_GENERAL	UDP
UDP_POPUP	Всплывающее окно для MS Windows
UPNP_GENERAL	UPNP
VERSION_CVS	CVS
VERSION_SVN	Свободная централизованная система управления версиями
VIRUS_GENERAL	Вирус

VOIP_GENERAL	Принцип работы VoIP-протокола
VOIP_SIP	Принцип работы SIP-протокола
WEB_CF-FILE-INCLUSION	Вложение файлов Coldfusion
WEB_FILE-INCLUSION	Вложение файлов
WEB_GENERAL	Web application attacks
WEB_JSP-FILE-INCLUSION	Вложение файлов JSP
WEB_PACKAGES	Пакеты популярных Web-приложений
WEB_PHP-XML-RPC	PHP XML RPC
WEB_SQL-INJECTION	Внедрение SQL-кода
WEB_XSS	Cross-Site-Scripting
WINS_GENERAL	Служба MS WINS
WORM_GENERAL	Черви
X_GENERAL	Generic X applications

Приложение B. Типы файлов MIME, проходящих проверку

Некоторые шлюзы прикладного уровня NetDefendOS (ALG) поддерживают дополнительную возможность подтверждения, что содержимое загруженного файла соответствует типу, указанному в его имени. Это следующие ALG:

- HTTP ALG
- FTP ALG
- POP3 ALG
- SMTP ALG

ALG, представленные выше, могут разрешить или заблокировать некоторые загруженные файлы с расширениями, указанными в списке ниже.

Для получения подробной информации обратитесь к *Разделу 6.2.2, «HTTP ALG»*.

Расширение файла	**Приложение**
3ds	3d Studio
3gp	Файл мультимедиа 3GPP
aac	Файл MPEG-2 Advanced Audio Coding
ab	Файл Applix Builder
ace	Сжатый файл архиватора ACE
ad3	Сжатый голосовой файл 3-bit
ag	Applix Graphic
aiff, aif	Файл Audio Interchange
am	Applix SHELF Macro
arc	Архивный файл
alz	Сжатый файл ALZip
avi	Файл Audio Video Interleave
arj	Сжатый архив
ark	Сжатый архив QuArk
arq	Сжатый архив
as	Таблица Applix
asf	Advanced Streaming Format
avr	Audio Visual Research
aw	Applix Word
bh	Blackhole
bmp	Растровая графика Windows OS/2
box	Почтовый ящик
bsa	Сжатый архив BSARC
bz, bz2	Сжатый файл Bzip UNIX
cab	Файл Cabinet (Microsoft архив инсталяции)
cdr	Файл векторной графики Corel
cgm	Графический компьютерный метафайл
chz	Архивный файл ChArc
class	Java byte code
cmf	Аудиофайл Creative
core/coredump	Unix core dump
cpl	Расширение панели управления
dbm	База данных
dcx	Файл растровой графики
deb	Пакет Debian Linux
djvu	Файл DjVu
dll	Динамически связанная библиотека

dpa	Архивный файл DPA
dvi	Документ в формате dvi
eet	Архивный файл EET
egg	Allegro datafile
elc	Исходный код eMacs Lisp битовой компиляции
emd	Модуль ABT EMD
esp	Архивный файл в формате Encapsulated PostScript
exe	Исполняемый файл для Windows
fgf	Free Graphics Format
flac	Free Lossless Audio Codec
flc	Анимированное изображение FLIC
fli	Анимация FLIC
flv	Macromedia Flash Video
gdbm	База данных
gif	Изображение в формате GIF
gzip, gz, tgz	Архивный файл в формате gzip
hap	Архивный файл HAP
hpk	Архивный файл HPack
hqx	Архивный файл Macintosh BinHex 4
icc	Профиль ICC, Kodak Color Management System
icm	Файл профиля образа набора цветов
ico	Иконка
imf	Аудиофайл Imago Orpheus module
Inf	Информация для установки
it	Музыкальный модуль Impulse Tracker
java	Исходный код Java
jar	Архивный файл Java JAR
jng	Видеоформат JNG
jpg, jpeg, jpe, jff, jfif, jif	Файл JPEG
jrc	Архивный файл Jrchive
jsw	Just System Word Processor Ichitaro
kdelnk	Файл KDE link
lha	Архивный файл LHA
lim	Архивный файл LIM
lisp	Архивный файл LISP
lzh	Архивный файл LZH
md	Архивный файл MDCD
mdb	База данных Microsoft Access
mid,midi	Файл Musical Instrument Digital Interface (MIDI)
mmf	Yamaha SMAF Synthetic Music Mobile Application
mng	Сетевая графика Multi-image Network Graphic
mod	Модуль Ultratracker
mp3	Аудиофайл MP3 MPEG Layer III
mp4	Видеофайл MPEG-4
mpg,mpeg	Видеофайл MPEG 1 System Stream
mpv	Видеофайл MPEG-1
Microsoft files	Файлы Microsoft
msa	Архивный файл Atari MSA
niff, nif	Файл Navy Interchange
noa	Nancy Video CODEC
nsf	Аудиофайл NES
obj, o	Объектный файл Windows, linux
ocx	Файл связи и внедрения объектов
ogg	Аудиофайл Ogg Vorbis
out	Исполняемый файл Linux
pac	Архивный файл CrossePAC
pbf	Файл компактной растровой графики
pbm	Файл компактной растровой графики
pdf	Файл Adobe Acrobat
pe	Файл Portable Executable

pfb	Шрифт (двоичный)
pgm	Графика в оттенках серой шкалы
pkg	SysV R4 PKG Datastreams
pll	Архивный файл PAKLeo
pma	Архивный файл PMarc
png	Файл Portable (Public) Network Graphic
ppm	Компактная пиксельная графика PBM
ps	Файл PostScript
psa	Архивный файл PSA
psd	Файл графики Photoshop
qt, mov, moov	Видеофайл Quicktime
qxd	Файл Quark Xpress
ra, ram	Файл RealMedia
rar	Архив RAR
rbs	Аудиофайл (песня) Rebirth
riff, rif	Растровый рисунок Fractal Painter
sar	Архивный файл SAR
sbi	Файл инструмента Sound Blaster
sc	Электронная таблица sc
sgi	Графический файл Silicon Graphics IRIS
sid	Аудиофайл Commodore 64 (C64) SID
sit	Архивный файл Stuffit
sky	Архивный файл SKY
snd, au	Аудиофайл AU (Sun/NeXT)
so	Файл библиотеки общего пользования UNIX
sof	Архивный файл ReSOF
sqw	Архивный файл SQWEZ
sqz	Архивный файл Squeeze It
stm	Файл модуля Scream Tracker 2
svg	Файл Scalable Vector Graphics
svr4	SysV R4 PKG Datastreams
swf	Файл Macromedia Flash
tar	Архивный файл в формате tar
tfm	TeX font metric
tiff, tif	Файл Tagged Image
tnef	Transport Neutral Encapsulation
torrent	Файл BitTorrent Metainfo
ttf	TrueType Font
txw	Аудиофайл Yamaha TX Wave
ufa	Архивный файл UFA
vcf	Файл Vcard
viv	Файл VivoActive Player Streaming Video
wav	Аудиофайл в формате WAV
wk	Файл Lotus 1-2-3
wmv	Файл Windows Media
wrl, vrml	Файл Plain Text VRML
xcf	Файл GIMP
xm	Расширенный модуль Fasttracker 2
xml	Файл XML
xmcd	Файл базы данных xmcd для kscd
xpm	BMC Software Patrol UNIX Icon
yc	Архивный файл YAC
zif	Файл ZIF
zip	Архивный файл ZIP
zoo	Архивный файл zoo
zpk	Архивный файл ZPack
z	Архивный файл compress

Приложение Г. Структура модели OSI

Обзор

OSI (Open Systems Interconnection) – модель для создания сетевых коммуникаций. В модели OSI сетевые функции распределены между семью уровнями. Модель OSI описывает структуру передачи данных от одного приложения другому.

Данные в процессе передачи проходят от одного уровня к другому: начиная с прикладного уровня на первом компьютере, дальнейшего преобразования до физического уровня, передачи на второй компьютер и последующей трасформации до самого верхнего уровня уже на нем. Каждому уровню соответствует определенный набор протоколов, таким образом, работа с приложением может быть поделена между уровнями и реализована отдельно на каждом из уровней. Модель необходима для понимания работы многих функций NetDefendOS, таких как ARP, Сервисы и ALG.

Номер уровня	Предназначение
Уровень 7	Прикладной
Уровень 6	Представления
Уровень 5	Сеансовый
Уровень 4	Транспортный
Уровень 3	Сетевой
Уровень 2	Канальный
Уровень 1	Физический

7 уровней модели OSI

Функции уровней

Различные уровни выполняют следующие функции:

Уровень 7 - Прикладной уровень	Обеспечивает взаимодействие пользовательских приложений с сетью. Протоколы: HTTP, FTP, TFTP. DNS, SMTP, Telnet, SNMP и т.п. На этом уровне работает ALG.
Уровень 6 – Представительский уровень	Преобразовывает данные в универсальный распознаваемый формат.
Уровень 5 – Сеансовый уровень	Устанавливает, поддерживает и завершает сессии в сети. Протоколы: NetBIOS, RPC и т.п.
Уровень 4 – Транспортный уровень	Обеспечивает передачу данных и коррекцию ошибок. Протоколы: TCP, UDP и т.п.
Уровень 3 – Сетевой уровень	Адресация и маршрутизация. Протоколы: IP, OSPF, ICMP, IGMP и т.п.
Уровень 2 – Канальный уровень	Упаковывает данные в стандартные фреймы для передачи через физический уровень и обеспечивает проверку/коррекцию ошибок. Протоколы: Ethernet, PPP и т.п. На этом уровне работает ARP.
Уровень 1 – Физический уровень	Предназначен непосредственно для передачи данных.