D-Link

Межсетевой экран с поддержкой VPN

Межсетевой экран с поддержкой VPN для сетей предприятий

D-Link DFL-900 - аппаратный межсетевой экран с поддержкой VPN, который является экономически эффективным решением проблемы безопасности, обеспечивая полноценную защиту сети, высокую производительность и надежность. Данный межсетевой экран/маршрутизатор VPN является идеальной системой по обеспечению безопасности сетей уровня предприятия, предлагая надежную защиту от внешних вторжений, поддержку VPN (Virtual Private Network) и простоту управление.

Защита межсетевым экраном

Межсетевой экран DFL-900 предоставляет широкий спектр функций защиты от внешних атак и обеспечения безопасности, которые включают аутентификацию пользователей, настройку политики безопасности и Virtual Server Mapping. DFL-900 обеспечивает NAT трансляцию IP-адресов внутренней частной сети в IP-адреса общедоступной сети.

Проверка содержимого пакетов

В качестве одной из функций межсетевого экрана, DFL-900 обеспечивает фильтрацию потенциально опасных кодов, встроенных в Web-страницы, удаляя объекты ActiveX, Java, JavaScript и другие потенциальные угрозы.

Надежная защита от атак хакеров

Межсетевой экран DFL-900 защищает сеть от атак Denial of Service (DoS) и обеспечивает стабильность работы сети посредством анализа содержимого пакетов (Stateful Packet Inspection, SPI). Устройство может обнаруживать атаки хакеров и отбрасывать вредоносные пакеты, предотвращая их проникновение в сеть.

DFL-900 защищает сеть от таких атак как SYN Flood, Ping of Death, Spoof, Tear Drop, ICMP Flood, UDP Flood и т.д. Его можно настроить на протоколирование этих атак, определение IP-адреса источника атаки и посылку предупреждений об атаках в виде отчета по электронной почте. Помимо этого можно задать правила ограничения потока данных с указанных IP-адресов.

VPN туннели между сетями и удаленными мобильными пользователями

DFL-900 поддерживает функции VPN, включая IPSec и безопасность ESP в режиме туннеля. DFL-900 имеет встроенную поддержку VPN, что позволяет создавать множество туннелей IPSec для удаленных офисов. Реализация IPSec в DFL-900 использует надежное шифрование DES, 3DES, AES и управление ключами Automated Key Management согласно спецификации IKE/ISAKMP. Туннель VPN может быть активирован от DFL-900 к удаленному офису или мобильному пользователю для надежной передачи потока данных с использованием шифрования triple DES. Это позволяет пользователям конфиденциально получать доступ и передавать важную информацию. Множество туннелей VPN может быть легко создано без необходимости определения правил протокола обмена ключами (Internet Key Exchange - IKE).

Управление доступом

Доступ для управления к DFL-900 может быть настроен как из внутренней защищенной сети, так и из внешней сети Интернет. DFL-900 содержит внутреннюю базу данных для аутентификации пользователей обращающихся к различным сервисам. Для организации к ним общественного доступа DFL-900 устанавливает связь между внешними IP-адресами и информационными серверами внутренней сети. Помимо этого, используя систему задания шаблонов URL, можно ограничить доступ к определенным Web-сайтам.

Планирование политик безопасности

Политики межсетевой защиты могут применяться в соответствии с расписанием, составленным для различных дней/недель/месяцев и для однократного или периодического использования.

Аппаратное ускорение

DFL-900 использует специально разработанные микросхемы ASIC для выполнения шифрования и дешифрования VPN, что разгружает центральный процессор.

1 DMZ порт, 1 защищенный порт LAN

DFL-900 имеет один 10/100BASE-TX порт LAN с автоопределением режима работы для подключения внутренней сети офиса и выделенный порт DMZ, позволяющий организовать доступ к почтовому, Web или FTP серверу компании непосредственно из Интернет. Функция DMZ очень полезна, т.к. снижает трафик от сервера во внутренней сети и защищает ее компьютеры от атак из Интернет, скрывая их за межсетевым экраном.

Управление

DFL-900 имеет удобный Web-интерфейс управления. Для соединения с управляющим терминалом во внутренней корпоративной сети или в удаленном офисе используется безопасное соединение SSL. Помимо этого, для локального управления DFL-900 можно использовать последовательный порт RS-232.

Основные характеристики

- *Защита межсетевым экраном с фильтрацией содержимого пакетов*
- *Функция VPN с шифрованием данных/аутентификацией IPSec, VPN туннели и поддержка VPN pass-through*
- *Быстрое аппаратное шифрование и дешифрование VPN*
- *До 100 VPN туннелей, 10 000 параллельных сессий, 1000 настраиваемых правил, 256 расписаний их применения*
- *3 порта 10/100BASE-TX: 1 WAN, 1 LAN, 1 выделенный DMZ*
- *Безопасное управление системой через VPN туннель на интерфейсе*
- *Управление полосой пропускания для сеанса связи в VPN туннеле*
- *Аутентификация пользователей/управление доступом*
- *Расписание применения политик безопасности/ «родительский контроль» и блокирование URL/доменов*
- *Web-интерфейс управления и удаленное управление через Web-браузер*
- *Обновление ПО через браузер*

DFL-900

Технические характеристики

Производительность и возможности

Параллельные сессии
300 000 макс.

Открытие новых сессий за секунду
4 000 макс.

Пропускная способность межсетевого экрана
100 Мбит/с

Пропускная способность при шифровании 3DES
60 Мбит/с

Количество политик безопасности
1 000 макс.

Расписаний применения политик безопасности
256 макс.

Количество VPN туннелей
1 000 макс.

Аппаратура

Интерфейсы
3 10/100BASE-TX порта (1 LAN, 1 WAN, 1 DMZ)

SDRAM
256 МБ

FLASH память
32 МБайт

Консольный порт
DB-9 RS-232 (асинхронный последовательный DTE)

Индикаторы диагностики
- На устройство: Power
- На порт Ethernet: Speed 100 Mbps, 10 Mbps, Link/Act

Программное обеспечение

Режимы работы
- Режим Transparent *
- Режим NAT/Route

Stateful Packet Inspection (SPI)
- IP-адрес и номер порта
- Счетчик пакетов и байтов
- Номер последовательности и подтверждения
- Временной штамп
- История изменения нагрузки
- Динамическое связывание

Denial of Service (DOS) атаки
- IP Source Routing
- IP Spoofing
- SYN Flooding
- ICMP Flood
- UDP Flood
- LAND Attack
- Address sweep attack
- Tear drop attack
- Winnuke attack
- Port scan attack
- Ping of death

Network Address Translation (NAT) (на порт)
- PAT
- NAT через IPSec

Проверка содержимого пакетов
- Динамическая фильтрация URL
- Блокирование HTTP URL: по ключевому слову/полному URL *
- Проверка содержимого HTTP: блокирование URL, объектов Java, JavaScript, ActiveX, Cookie

Межсетевой экран с поддержкой VPN

- Proxy для приложений: POP3, SMTP, FTP
- Назначение IP-адреса: статическое, клиент PPPoE для порта WAN, клиент DHCP для порта WAN, сервер DHCP для порта LAN, DHCP relay

IDS (Intrusion Detection System)
- Модель NIDS
- Определение домена атаки
- Уведомление об атаке (через электронную почту)
- Протоколирование и отчет

Virtual Private Network (VPN)
- VPN туннель между офисами
- VPN туннель между офисом и клиентом

Управление ключами VPN
- ISAKMP/Oakley (IKE) *
- SKIP *

Шифрование данных VPN
- DES (56-бит)
- 3DES (128-бит)
- AES *
- PKI (X.509) *

Протоколы VPN туннелирования
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol
- IPSec

Аутентификация VPN IPSec
- MD5
- SHA-1
- Запросы сертификата PKI (PKCS 7 и PKCS 10) *
- Automated certificated enrollment (SCEP) *
- Online certificate status protocol (OCSP) *

Аутентификация пользователей через межсетевой экран и VPN
- Встроенная (внутренняя) база данных (до 1500 пользователей) *
- Клиент RADIUS *
- Клиент RSA SecureID *
- Клиент LDAP *
- Аутентификация через сервер RADIUS *
- Аутентификация XAUTH VPN *
- Аутентификация на основе Web

Управление полосой пропускания
- Выделение гарантированной полосы пропускания
- Выделение максимальной полосы пропускания
- Загрузка полосы пропускания по приоритету
- Обработка кода типа сервиса DiffServ *

Протоколы маршрутизации
- RIP-1, RIP-2
- OSPF *

Сетевые протоколы
- TCP/IP
- UDP
- ARP
- ICMP

Управление
- SNMP v1, v2
- HTTP
- Клиент TFTP
- Telnet
- Интерфейс командной строки (CLI) *
- Защищенная командная оболочка (SSH v1.5) *

Протоколирование и мониторинг
- Графическое отображение накопленной статистики *
- Протоколирование фильтрации: регистрация отклоненных внутренних и внешних запросов на соединение
- Протоколирование сеансов связи: регистрация создания и разрыва соединения

DFL-900

Технические характеристики

Межсетевой экран с поддержкой VPN

- Предупреждения/уведомления при обнаружении атак: запись информации о внешней атаке
- Протоколирование аутентификации пользователей: регистрация момента аутентификации пользователя через межсетевой экран
- Протоколирование доступа через Web
- Таблица DHCP
- Протоколирование системы
- Протоколирование ошибок
- Протоколирование электронной почты
- Мониторинг VPN туннелей
- Протоколирование событий и система предупреждений

** Функции будут доступны в следующей версии ПО*

Физические параметры

Питание
Переменный ток 90 - 264 В, 50/60 Гц, внутренний универсальный источник питания

Потребляемая мощность
100 Вт

Размеры
425 x 257 x 44 мм (только устройство),
для установки в 19-дюймовую стойку, высота 1 U

Рабочая температура
0° до 50° C

Температура хранения
-25° до 55° C

Рабочая влажность
От 5% до 95% без образования конденсата

Сертификаты EMI
- FCC Class A
- CE Class A

Безопасность
CSA International

Информация для заказа

Широкополосный межсетевой экран/VPN маршрутизатор

DFL-900	1 10/100BASE-TX порт WAN, 1 10/100BASE-TX порт внутренней LAN, 1 10/100BASE-TX порт DMZ

129626, Москва, Графский пер., 14, 6 этаж
Тел./Факс +7 (095) 744-0099,
E-mail:mail@dlink.ru,
Web: www.dlink.ru