



— DFL-600

Межсетевой экран с поддержкой VPN

Интегрированное решение обеспечения безопасности для сетей SOHO

D-Link DFL-600 легко развертываемый, аппаратный межсетевой экран с поддержкой VPN, разработанный для сетей малых предприятий, рабочих групп и отделов, требующих наилучшего соотношения цена/производительность. Это устройство является мощным решением по обеспечению безопасности, которое предоставляет интегрированные функции NAT, межсетевого экрана, защиту от атак DoS и поддержку VPN. Внутри компактного, легко размещающегося корпуса, межсетевой экран VPN DFL-600 имеет 1 порт WAN, 4 порта LAN, которые исключают необходимость в использовании внешнего концентратора или коммутатора и порт DMZ для поддержки локальных почтовых, Web и FTP серверов. Благодаря интуитивно понятному Web-интерфейсу управления и простоте процесса, мастер установки D-Link позволит пользователям выполнить настройку устройства за несколько минут.

Многофункциональное устройство обеспечения безопасности

DFL-600 является эффективным межсетевым экраном с поддержкой VPN для малого и среднего бизнеса, т.к. обеспечивает поддержку технологии Stateful Packet Inspection (SPI), обнаружения и блокировки вторгающихся пакетов, VPN, физического порта DMZ, multiple-mapped Ips и множества виртуальных серверов, т.е. всего, что обычно можно найти в межсетевых экранах уровня предприятия. DFL-600 легко подключает ваш офис к кабельному или DSL модему, через порт 10/100BASE-TX WAN.

Надежная защита от атак хакеров

DFL-600 имеет расширенные функции обеспечения безопасности, которые обычно отсутствуют в резидентных шлюзах. Он защищает сеть от атак Denial of Service (DoS) и обеспечивает стабильность работы сети посредством анализа содержимого пакетов (Stateful Packet Inspection). Устройство может обнаруживать атаки хакеров и отбрасывать вторгающиеся пакеты, предотвращая их проникновение в сеть.

DFL-600 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, с которого велась атака и посылку предупреждений об атаках в виде отчета по электронной почте, также можно задать правила ограничения потока данных с указанных IP адресов.

Поддержка высокопроизводительных VPN туннелей на основе IPSec

DFL-600 имеет встроенную поддержку VPN, что позволяет создавать множество туннелей IPSec для удаленных офисов. Реализация IPSec в DFL-600 использует шифрование DES, 3DES и управление ключами Automated Key Management согласно спецификации IKE/ISAKMP. Туннель VPN может быть активирован с DFL-600 к удаленному офису для целостной передачи потока данных между двух точек для мобильных пользователей использующих шифрование triple DES. Это позволяет пользователям конфиденциально получать доступ и передавать важную информацию. Множество туннелей VPN могут быть легко созданы без необходимости определения правил протокола обмена ключами (Internet Key Exchange - IKE).

Списки управления доступом (ACL)

Блокирование URL - это одна из основных функций, поддерживаемых DFL-600. Она позволяет ограничивать доступ к нежелательным ресурсам Интернет. Лог-файлы Интернет трафика, предупреждения об атаках из Интернет и уведомления об использовании ресурсов Интернет сохраняются и могут быть отправлены в виде отчета по электронной почте.

DFL-600 поддерживает аутентификацию Radius. Таким образом, можно использовать существующий сервер Radius и информацию о пользователях. Он также поддерживает аутентификацию на основе сертификатов X.509, используя набор PKIX-совместимых сертификатов и стандартов проверки полномочий (*).

(*Функция X.509 будет доступна в следующей версии ПО.

Уведомление по электронной почте

Сетевые администраторы могут задать набор почтовых адресов (e-mail) для получения предупреждающих сообщений от DFL-600. При обнаружении попытки вторжения, DFL-600 запротоколирует ее и отправит предупреждающее сообщение на адрес электронной почты. Администратор может проверить лог-файл на маршрутизаторе, чтобы выяснить, что произошло.

1 DMZ порт, 3 порта коммутатора Fast Ethernet

DFL-600 имеет 3 10/100BASE-TX порта LAN с автоопределением, которые подключаются к внутренней сети офиса и выделенный порт DMZ, позволяющий организовать доступ к почтовому, Web или FTP серверу компании непосредственно из Интернет. На DFL-600 можно создать дополнительный порт DMZ, назначив любой из 3-х портов LAN портом DMZ. Функция DMZ очень полезна, т.к. уменьшает количество трафика от сервера во внутренней сети и защищает ее компьютеры от атак из Интернет, скрывая их за межсетевым экраном.

Простота установки

DFL-600 имеет удобный Web- интерфейс управления с защитой паролем, доступ к которому можно получить с любого компьютера с браузером. Более того, правила работы с входящим и выходящим потоком данных межсетевого экрана наряду с другими параметрами конфигурации устройства полностью задаются средствами Web - интерфейса.

DFL-600

Технические характеристики

Межсетевой экран с поддержкой VPN

Характеристики

- 3 10/100BASE-TX LAN порта, 1 10/100BASE-TX DMZ порт
- 1 10/100BASE-TX WAN порт
- Поддержка VPN туннелей на основе PPTP, L2TP, IPSec
- Поддержка PPTP, L2TP, IPSec VPN pass throughput
- Поддержка Stateful Packet Inspection (SPI)
- Блокировка атак Denial of Service (DoS)
- Network Address Translation (NAT)/Network Address Port Translation (NAPT)

Аппаратура

Порт WAN

- 10/100BASE-TX порт
- Поддержка автосогласования NWay

Порты LAN

- 3 10/100BASE-TX LAN порта
- 1 10/100BASE-TX DMZ порт
- Авто MDI/MDIX, автосогласование NWay для всех портов

Кнопка сброса

Сброс установок к настройкам по умолчанию

Память

- SDRAM: 32Мбайт
- Flash: 8Мбайт

Безопасность VPN

Поддержка VPN

- L2TP/PPTP/IPSec tunneling
- L2TP/PPTP/IPSec pass-through

Алгоритмы хеширования

- ESP-MD5/AH-MD5
- RSP-SHA1/AH-SHA1

Алгоритмы шифрования

- DES/3DES
- AES *

* Функция AES будет доступна в следующей версии ПО.

Управление ключами

- Вручную
- Internet Key Exchange (IKE)
- Internet Security Association и Key Management Protocol (ISAKMP)

Механизмы аутентификации/PKI *

- Поддержка аутентификации RADIUS (RADIUS клиент)
- Поддержка аутентификации на основе сертификатов X.509
- X.509 Public Key Infrastructure Certificate и CRL Profile (RFC 2489)
- X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)
- X.509 Certificate Request Message Format (RFC 2511)
- X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) (RFC 2560)
- Certificate Management Messages over CMS (RFC 2797)

* Функция аутентификации будет доступна в следующей версии ПО.

Маршрутизация

Функции и протоколы

- Статическая маршрутизация
- Динамическая маршрутизация *
- RIP-1, RIP-2 *
- IP Multicast *
- UDP, TCP, ICMP, ARP

* Динамическая маршрутизация (RIP-1, RIP-2, IP multicast) будет доступна в следующей версии ПО.

Функции межсетевого экрана

- На основе Интернет-шлюза
- NAT/NAPT

- Поддержка NAT Application Level Gateway (ALG)
- DHCP сервер/клиент и «родительский контроль»
- Поддержка маршрутизации PPPoE
- Universal Plug and Play (UPnP)
- Фильтрация содержимого, блокировка URL/доменов
- Поддержка виртуального сервера
- Web-интерфейс управления
- Поддержка протокола SYSlog

NAT ALG

- Стек протокола H.323
- File Transfer Protocol (FTP)
- Session Initiation Protocol (SIP) *
- Session Description Protocol (SDP)
- Real-Time Transport Protocol (RTP)
- Internet Relay Chat (IRC)
- Multiple Gaming Protocol
- NetMeeting 3/ 2.0 Video/Audio receive/send
- ICQ: Chat and File Send

* Функция SIP будет доступна в следующей версии ПО.

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)

- SYN Flooding
- TCP Hijacking
- LAND Attack
- WinNuke/OOBNuke
- Christmas Tree SYN/FIN (Jackal)
- SYN / FIN (zero-sized DNS zone payload)
- BackOffice (UDP 31337)
- NetBus
- Smurf
- Tear Drop
- ICMP Flooding
- Trojan Horse
- UDP Flooding
- UDP Scan
- ARP Attack

Блокировка пользователей

(Default blocking port number for each server)

- NNTP сервер -- TCP Порт(ы): 119
- SMTP сервер -- TCP Порт(ы) - 25
- POP3 сервер -- TCP Порт(ы): 110, 995
- Quake 3 сервер -- UDP Порт(ы): 27960
- IMAP сервер -- TCP Порт(ы): 143, 220, 585, 993
- FTP сервер (только активный режим) -- TCP Порт(ы): 20, 21
- SSH сервер -- TCP Порт(ы): 22
- Telnet сервер
- HTTP сервер

Настройка и управление

- IP управление
- DHCP сервер/клиент
- PPPoE для DSL
- UPnP *

* Функция UPnP будет доступна в следующей версии ПО.

Система

- Системные лог-файлы
- Резервное копирование ПО
- Уведомление по E-mail *
- Удаленное управление через порт WAN
- Simple Network Time Protocol (SNTP)

* Функция будет доступна в следующей версии ПО

DFL-600

Технические характеристики

Межсетевой экран с поддержкой VPN

Интерфейсы конфигурирования

- Web—интерфейс управления (через web браузер)
- Обновление ПО через Web

Индикаторы диагностики

- Power (на устройство)
- Link/Act (порт WAN)
- Link/Act (на внутренний порт LAN)

Физические параметры

Размер

234 (W) x 161 (D) x 35 (H) мм

Вес

500 г.

Питание

- 5В переменного тока 2.5А
- Через внешний адаптер питания

Рабочая температура

0° до 45° C

Температура хранения

-25° до 55° C

Влажность хранения

От 10% до 90% без образования конденсата

Рабочая влажность

От 10% до 95% без образования конденсата

Сертификаты EMI

- FCC Class B
- CE Class B
- C-Tick Class B

Safety

CSA International

Информация для заказа

Межсетевой экран с поддержкой VPN

DFL-600

1 порт RJ-45 10/100BASE-TX (WAN для подключения к Интернет)
1 порт RJ-45 10/100BASE-TX (для сети DMZ)
3 порта встроенного коммутатора RJ-45 10/100BASE-TX (для внутренней сети)

D-Link®

129626, Москва, Графский пер., 14, 6 этаж
тел/факс 7 (095) 744-00-99
www.dlink.ru