NETDEFEND

Встроенный межсетевой экран / VPN
- Защита встроенным межсетевым экраном
- Безопасность виртуальных частных сетей VPN
- Управление полосой пропускания с небольшим шагом
- 802.1Q VLAN Tagging и на основе портов VLAN
- Активная защита с помощью механизма Zone-Defense

Расширенные функции межсетевого экрана
- Stateful Packet Inspection (SPI)
- Обнаружение / отбрасывание злонамеренных пакетов
- Балансировка нагрузки серверов
- Маршрутизация на основе политик

Unified Threat Management (UTM)
- Система предотвращения вторжений (IPS)
- Антивирусная (AV) защита
- Фильтрация Web-содержимого
- Годовая подписка на обновление*

Виртуальная частная сеть (VPN)
- IPSec NAT traversal
- VPN Hub and Spoke
- IPSec, PPTP, L2TP
- Шифрование DES, 3DES, AES, Twofish, Blowfish, CAST-128
- Автоматизированное управление ключами через IKE/ISAKMP
- Согласование режимов работы (Aggressive/Main/Quick)

Расширенные сетевые сервисы
- DHCP-сервер/клиент/relay
- IGMP v3
- H.323 NAT Traversal
- Обеспечение надлежащего уровня безопасности для ALG
- Протокол динамической маршрутизации OSPF
- Аутентификация на основе Web

Оптимизация производительности
- Аппаратное ускорение UTM
- Несколько WAN-интерфейсов для обеспечения отказоустойчивости

ICSA labs CERTIFIED IPSEC-ENHANCED
VPNC CERTIFIED AES Interop
ICSA labs CERTIFIED FIREWALL-CORPORATE
VPNC CERTIFIED Basic Interop

** Только для DFL-1660/2560/2560G*

Серия межсетевых экранов NetDefend UTM

По мере того, как бизнес-процессы становятся все более зависимыми от сетевой инфраструктуры, капиталовложения, вложенные в решения по безопасности становятся все более значимыми. D-Link представляет ряд мощных решений для защиты сетей предприятий от разнообразных угроз. Межсетевые экраны NetDefend UTM предлагают всестороннюю защиту от вирусных атак, от несанкционированного доступа и нежелательного контента, а также расширенные возможности управления, мониторинга и обслуживания безопасной сети.

Межсетевой экран уровня Enterprise
Межсетевые экраны NetDefend UTM обеспечивают законченное решение для управления, мониторинга и обслуживания безопасной сети. Среди функций управления: удаленное управление, политики управления полосой пропускания, блокировка по URL/ключевым словам, политики доступа и SNMP. Также поддерживаются такие функции сетевого мониторинга, как уведомление по e-mail, системный журнал, проверка устойчивости и статистика в реальном времени.

Unified Threat Management (UTM)
Межсетевые экраны NetDefend UTM оснащены системой обнаружения и предотвращения, антивирусом и фильтрацией Web-содержимого для проверки и защиты содержимого на 7 уровне. Используемый в данных устройствах аппаратный ускоритель увеличивает производительность IPS и AV, управляющей базы поиска в Web, содержащей миллионы URL для фильтрации Web-содержимого (WCF). Сервисы обновления IPS, антивируса и базы данных URL защищают офисную сеть от вторжений, червей, вредоносных кодов и удовлетворяют потребностям бизнеса по управлению доступом сотрудников к Интернет.

Производительность VPN
Для оптимальной настройки VPN межсетевые экраны NetDefend UTM поддерживают встроенный VPN-клиент и сервер, что позволяет работать практически с любой политикой VPN и осуществлять подключение филиалов к головному офису по безопасной сети. Пользователи, работающие на дому, также могут безопасно подключиться к сети для доступа к внутренним данным компании и получения электронной почты. Межсетевые экраны NetDefend UTM поддерживают аппаратные VPN engines для поддержки и управления широким диапазоном сетей VPN. Эти устройства поддерживают протоколы IPSec, PPTP и L2TP в режиме Клиент/Сервер и осуществляют обработку проходящего через них трафика. Расширенные опции настройки VPN включают: шифрование DES, управление ключами IKE/ISAKMP или вручную, согласование режимов Quick/Main/Aggressive и поддержка аутентификации VPN, используя внешний RADIUS-сервер или базу данных пользователей.

Сервисы UTM
Для обеспечения эффективной защиты от угроз из Интернет необходимо, чтобы все три базы данных, используемых межсетевых экранов NetDefend UTM, поддерживались в актуальном состоянии. В связи с этим D-Link предлагает дополнительную подписку на обновление сигнатур для каждого из сервисы NetDefend Firewall UTM: IPS, антивирус и WCF. Это позволяет обеспечить точность и актуальность баз данных NetDefend UTM.

Мощная система предотвращения атак (IPS)
Межсетевые экраны NetDefend UTM используют уникальную технологию IPS – компонентные сигнатуры, которые позволяют распознавать и обеспечивать защиту, как против известных, так и против неизвестных атак. В результате данные устройства помогают при атаках (реальных или потенциальных) значительно снизить влияние на такие важные аспекты, как полезная нагрузка, закрытая информация, а также предотвратить распространение инфекций и компьютерные вторжения. База данных IPS включает информацию о глобальных атак и вторжениях, собранную на публичных сайтах (например, National Vulnerability Database и Bugtrax). Межсетевые экраны NetDefend UTM обеспечивают высокую эффективность сигнатур IPS, постоянно создавая и оптимизируя сигнатуры NetDefend через D-Link Auto-Signature Sensor System. Эти сигнатуры обеспечивают высокую точность обнаружения при минимальном количестве ошибочных срабатываний.

Потоковое сканирование вирусов
Межсетевые экраны NetDefend UTM позволяют сканировать файлы любого размера, используя технологию потокового сканирования. Данный метод сканирования увеличивает производительность проверки, сокращая так называемые «узкие места» в сети. Эти межсетевые экраны используют сигнатуры вирусов от известных надежных антивирусных компаний, например, Kaspersky Labs, при этом существует возможность обновления сигнатур. В результате вирусы и вредоносные программы могут быть эффективно заблокированы до того, как они достигнут настольных или мобильных устройств.

Фильтрация Web-содержимого
Фильтрация Web-содержимого помогает администраторам осуществлять мониторинг, управление и контроль использования сотрудниками предоставленного им доступа к Интернет. Межсетевые экраны NetDefend UTM поддерживают несколько серверов глобальных индексов с миллионами URL и информацией в реальном времени о Web-сайтах, что позволяет увеличить производительность и обеспечить максимальную доступность сервиса. В этих межсетевых экранах используются политики с множеством параметров, а также белые и черные списки, что позволяет запретить или разрешить доступ в заданное время к Web-сайтам для любой комбинации пользователей, интерфейсов и IP-сетей. Эти устройства также позволяют обходить потенциально опасные объекты, включая Java-апплеты, Java-скрипты/VBS-скрипты, объекты ActiveX и cookies, активно обрабатывая содержимое Интернет.

Серия межсетевых экранов NetDefend UTM

DFL-260E
- Производительность межсетевого экрана: 150 Мбит/с
- Производительность VPN: 45 Мбит/с (3DES/AES)
- 1 порт 10/100/1000 Ethernet WAN
- 5 портов 10/100/1000 Ethernet LAN
- 1 порт 10/100/1000 Ethernet DMZ

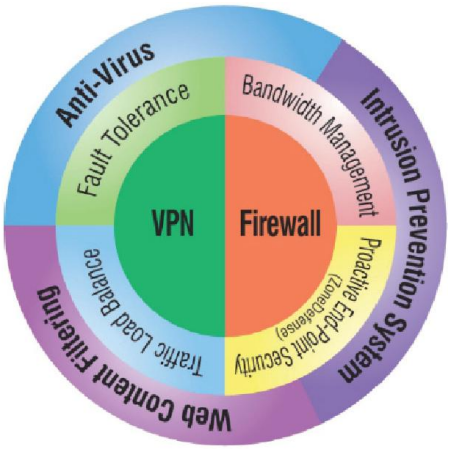
DFL-860E
- Производительность межсетевого экрана: 200 Мбит/с
- Производительность VPN: 60 Мбит/с (3DES/AES)
- 2 порта 10/100/1000 Ethernet WAN
- 8 портов 10/100/1000 Ethernet LAN
- 1 порт 10/100/1000 Ethernet DMZ

DFL-1660
- Производительность межсетевого экрана: 1.2 Гбит/с
- Производительность VPN: 350 Мбит/с (3DES/AES)
- 6 настраиваемых портов Gigabit Ethernet

DFL-2560(G)
- Производительность межсетевого экрана: 2 Гбит/с
- Производительность VPN: 1 Гбит/с (3DES/AES)
- 10 настраиваемых портов Gigabit Ethernet
- 4 порта SFP (DFL-2560G)

Подписка на сервисы NetDefend UTM[1]
Стандартная подписка NetDefend UTM (Unified Threat Management) рассчитана на 12 месяцев*, начиная со дня активации или продления сервиса. Рекомендуется регулярно продлевать подписку на сервисы NetDefend UTM. Сервисы NetDefend UTM доступны по подписке на сайте центра безопасности NetDefend D-Link: http://security.dlink.com.tw

**Срок подписки зависит от региона.*



VPN Engine
Аппаратное шифрование и аутентификация данных для IPSec, PPTP и L2TP в режиме Клиент/Сервер позволяет организовать быструю и безопасную обработку VPN-трафика.

Профессиональная система предотвращения вторжений (IPS)
Автоматическое обновление базы данных сигнатур IPS и защита сети от атак zero-day.

Антивирусная (AV) проверка в реальном времени
Для межсетевых экранов ZoneDefense UTM сканирование осуществляется по наиболее полной и актуальной базе данных антивирусных сигнатур, используя технологию потокового сканирования, что позволяет наиболее эффективно защищать сеть от вирусов.

Быстрая и эффективная фильтрация web-содержимого
Несколько серверов глобальных индексов, политики с множеством параметров, чёрные списки и активная обработка содержимого – всё это улучшает производительность и эффективность контроля доступа в Интернет.

Аппаратный ускоритель для Unified Threat Management
Встроенный аппаратный ускоритель позволяет межсетевому экрану осуществлять IPS и антивирусное сканирование одновременно, не ухудшая производительность межсетевого экрана.

Резервирование канала WAN
2 WAN-порта поддерживают распределение нагрузки, а также функцию fail-over, обеспечивая доступность Интернет и требуемую полосу пропускания.

Доступность дополнительного сервиса по обновлению сигнатур в течение года
Дополнительные сервисы подписки на сигнатуры IPS, AV, фильтрации Web-содержимого приобретаются сразу для всего межсетевого экрана, и их цена не зависит от количества пользователей, что делает данные сигнатуры очень доступными по цене.

Активная сетевая безопасность с D-Link ZoneDefense**
Благодаря применению механизма Zone-Defense при работе с коммутаторами серии xStack D-Link, инфицированные рабочие станции автоматически блокируются и не имеют возможности распространять по внутренней сети злонамеренный трафик.

dlink green™

Сертификат D-Link Green
Сертифицированные D-Link Green DFL-1660 и DFL-2560(G) имеют встроенный источник питания 80 PLUS, который предлагает увеличенную надежность, обусловленную большей эффективностью, и обеспечивает сокращение затрат, благодаря длинному сроку службы оборудования. Кроме того, источник питания 80 PLUS уменьшает загрязнение окружающей среды благодаря уменьшенному энергопотреблению и снижению температуры во избежание затрат на вентиляцию. DFL-260E и DFL-860E автоматически сохраняют энергию посредством определения длины кабеля и статуса соединения. При определении длины кабеля, подключенного к порту, величина питания, используемая для порта может регулироваться насколько это необходимо. DFL-260E/860E также может определить используется ли порт, тогда как подключенный компьютер отключен или порт не используется, тогда питание автоматически уменьшается для этого порта вплоть до значительного снижения питания.

Сертифицированные устройства соответствуют директивам RoHS (Ограничение содержания вредных веществ) и WEEE (Отходы электрического и электронного оборудования). Директивы RoHS ограничивают использование определенных опасных материалов во время производства, в то время как WEEE следует стандартам переработки отходов и повторному использованию. Все это делает межсетевые экраны D-Link Green продуктами, наименее загрязняющими окружающую среду.

[1]На устройство предоставляется пробная бесплатная подписка (trial) на 90 дней.
**Срок подписки зависит от региона и приобретается отдельно.*
***Только для DFL-860E, DFL-1660 и DFL-2560(G)*

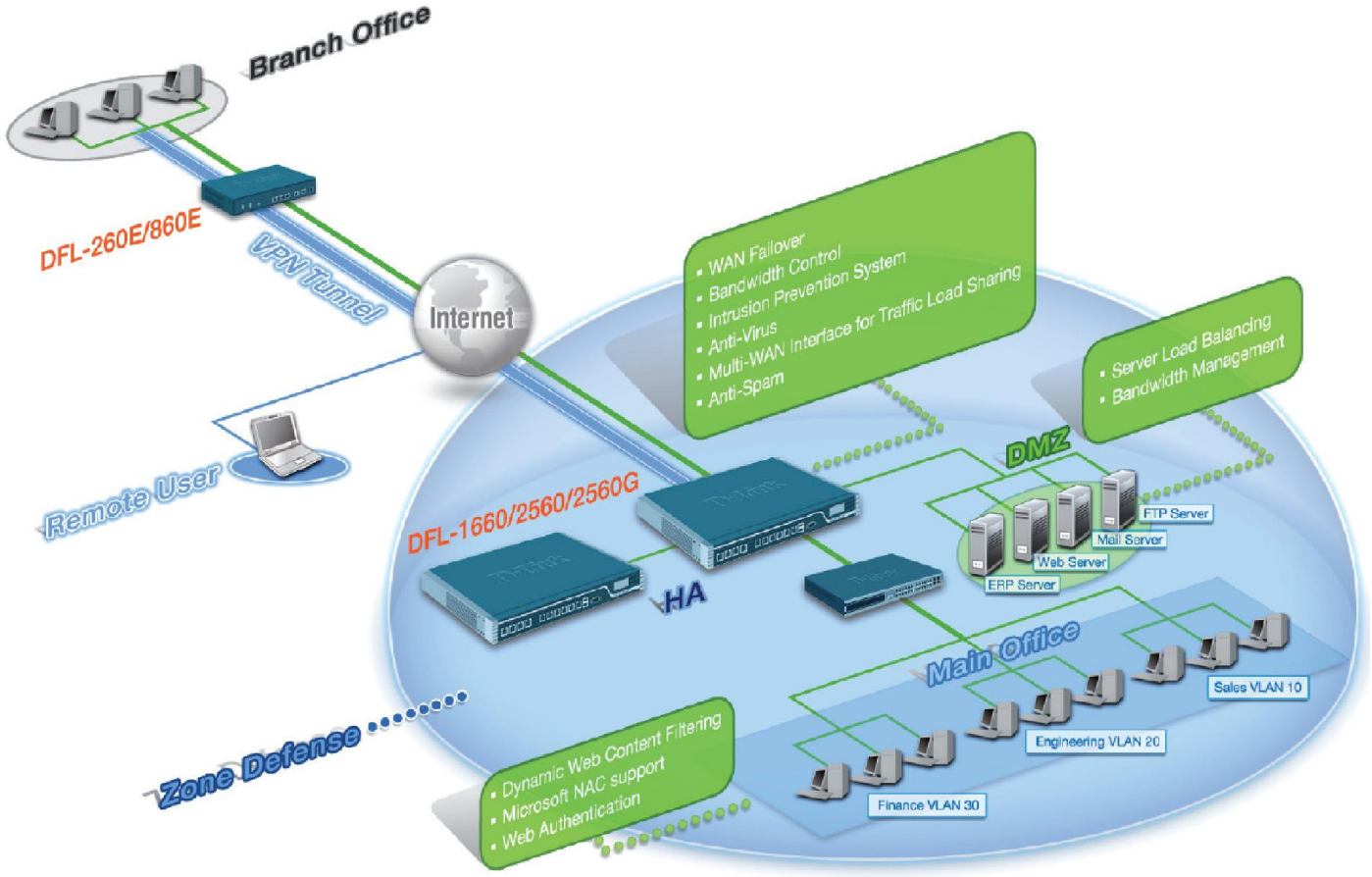
Технические характеристики		DFL-260E	DFL-860E	DFL-1660	DFL-2560(G)
					
Интерфейсы	Ethernet	• 1 порт 10/100/1000 Ethernet WAN • 1 порт 10/100/1000 Ethernet DMZ (настраиваемый) • 5 портов 10/100/1000 Ethernet LAN • USB: 2 USB порта (зарезервировано) • Console: RJ-45	• 2 порта 10/100/1000 Ethernet WAN • 1 порт 10/100/1000 Ethernet DMZ • (настраиваемый) • 8 портов 10/100/1000 Ethernet LAN • USB: 2 USB порта (зарезервировано) • Console: RJ-45	• 6 настраиваемых портов Gigabit Ethernet • USB: 2 USB порта (зарезервировано) • Console: 1 DB-9 RS 232	• 10 настраиваемых портов Gigabit Ethernet • USB: 2 USB порта (зарезервировано) • Console: 1 DB-9 RS 232
	SPF	-	-	-	4 порта SFP (только DFL-2560G)[7]
Производительность системы	Производительность межсетевого экрана[2]	150 Мбит/с	200 Мбит/с	1.2 Гбит/с	2 Гбит/с
	Производительность VPN[3]	45 Мбит/с	60 Мбит/с	350 Мбит/с	1 Гбит/с
	Производительность IPS[4]	60 Мбит/с	80 Мбит/с	400 Мбит/с	600 Мбит/с
	Производительность антивируса [4]	35 Мбит/с	50 Мбит/с	225 Мбит/с	450 Мбит/с
	Количество параллельных сессий	25,000[5]	40,000[5]	600,000	1,500,000
	Количество новых сессий (в секунду)	2,000	4,000	15,000	20,000
	Политики	500	1,000	4,000	6,000
Межсетевой экран	Прозрачный режим	v	v	v	v
	NAT, PAT	v	v	v	v
	Протокол динамической маршрутизации	-		OSFP	
	H.323 NAT Traversal	v	v	v	v
	Политики по расписанию	v	v	v	v
	Application Layer Gateway	v	v	v	v
	Активная сетевая безопасность	v	v	v	v
Сетевые функции	DHCP сервер/клиент	v	v	v	v
	DHCP Relay	v	v	v	v
	Маршрутизация на основе политик	v	v	v	v
	IEEE 802.1q VLAN	8	16	1024	2048
	VLAN на основе портов			v	
	IP Multicast			IGMP v3	
Виртуальные частные сети (VPN)	Шифрование (DES/3DES/AES/Twofish/ Blowfish / CAST-128)	v	v	v	v
	Выделенные VPN-туннели	100	200[5]	2,500	5,000
	Сервер PPTP/L2TP	v	v	v	v
	Hub and Spoke	v	v	v	v
	IPSec NAT Travesal	v	v	v	v
	SSL VPN			Функция будет доступна в будущем	

Технические характеристики		DFL-260E	DFL-860E	DFL-1660	DFL-2560(G)
					
Балансировка нагрузки	Балансировка исходящего трафика	v	v	v	v
	Балансировка нагрузки сервера	-	v	v	v
	Алгоритм балансировки нагрузки серверов	Round-robin, Weight-based Round-robin, Destination-based, Spill-over			
	Перенаправление трафика при обрыве канала (fail-over)	v	v	v	v
Управление полосой пропускания	Traffic Shaping на основе политик	v	v	v	v
	Гарантированная полоса пропускания	v	v	v	v
	Максимальная полоса пропускания	v	v	v	v
	Полоса пропускания на основе приоритета	v	v	v	v
	Динамическое распределение полосы пропускания	v	v	v	v
High Availability (HA)	Резервирование канала WAN	v	v	v	v
	Режим Active/Passive	-	-	v	v
	Обнаружение отказа устройства	-	-	v	v
	Определение обрыва канала	-	-	v	v
	Синхронизация сессий FW/VPN	-	-	v	v
Intrusion Detection & Prevention System (IDP/IPS)	Автоматическое обновление шаблонов	v	v	v	v
	Защита от атак DoS, DDoS	v	v	v	v
	Предупреждение об атаках по электронной почте	v	v	v	v
	Расширенная подписка IDP/IPS	Приобретается отдельно			
	Черный список по IP (пороговая величина или IDP/IPS)	-	v	v	v
Фильтрация содержимого	Тип HTTP	Белый / черный список URL			
	Тип скриптов	Java Cookie, ActiveX, VB			
	Тип e-mail	Белый / черный список e-mail			
	Внешняя база данных фильтрации содержимого	v	v	v	v
Антивирусная защита	Антивирусное сканирование в реальном времени	v	v	v	v
	Неограниченный размер файла	v	v	v	v
	Сканирование VPN-туннелей	v	v	v	v
	Поддержка сжатых файлов	v	v	v	v
	Поставщик сигнатур	Kaspersky			
	Количество антивирусных сигнатур	4000*	4000*	12000*	12000*
	Автоматическое обновление шаблонов	v	v	v	v

Технические характеристики		DFL-260E	DFL-860E	DFL-1660	DFL-2560(G)
					
Физические параметры и условия эксплуатации	Питание	Внутренний источник питания		Внутренний источник питания	Внутренний источник питания 80 PLUS
	Потребляемая мощность	18.6 Вт переменного тока/ 16.13 Вт постоянного тока	22.8 Вт переменного тока / 18.95 Вт постоянного тока	N/A	
	Размеры	280 x 180 x 44 мм Установка в стойку 11"	330 x 180 x 44 мм Установка в стойку 13"	440 x 400 x 44 мм Установка в стойку 19"	
	Вес	1.59 кг	1.623 кг	6.1 кг	6.2 кг
	Рабочая температура	От 0º до 40ºC			
	Температура хранения	От -20º до 70ºC			
	Рабочая влажность	От 5% до 95%, без образования конденсата			
	EMI	FCC Class A CE Class A C-Tick VCCI			
	Safety	UL LVD (EN60950-1)	LVD (EN60950-1)	cUL, CB	
	MTBF	186,614 ч	140,532 ч	400,000 ч	310,000 ч

** Используются сигнатуры для актуальных вирусов распространяющихся в момент действия подписки.*
[1] Фактическая производительность может изменяться в зависимости от сетевых условий и активности сервисов.
[2] Максимальная производительность межсетевого экрана основана на RFC2544.
[3] Пропускная способность VPN измерялась с использованием UDP трафика и размере пакета 1420, согласно RFC 2544
[4] Тест производительности IPS и антивируса основан на протоколе HTTP с вложением файла 1 Мб, запущенным на IXIA IxLoad. Тест сделан со множеством потоков через несколько пар портов.
[5] Производительность определена на основе прошивки 2.27.00 и выше
[6] Доступно, если DMZ порт настроен как WAN порт
[7] Совместим с модулями SFP-трансиверов D-Link: DEM-310GT, DEM-311GT, DEM-312GT2, DEM-314GT, DEM-315GT, DEM-330T, DEM-330R, DEM-331T, DEM-331R, DGS-712

Обеспечение сетевой безопасности с помощью межсетевых экранов NetDefend™ UTM



ACN 052 202 838

Версия 02 (Октябрь 2010)