D-Link®

Product Highlights

Increased Security

Integrated Firewall/VPN and UTM provides protection from viruses, intrusions and harmful content.

Reduced Cost of Ownership

Subscription service per firewall rather than per user reduces licensing cost and simplifies management.

Easily Manage and Control Internet Usage

Fast, efficient web content filtering helps administrators monitor and control employee Internet usage.

DFL-260E/860E/1660/2560/2560G

NetDefend™ UTM Firewall Series

Features

Integrated Firewall/VPN

- Powerful Firewall Engine
- Virtual Private Network (VPN) Security
- Granular Bandwidth Management
- 802.1Q VLAN Tagging and Port-based VLAN
- D-Link End-to-End Security Solution (E2ES) Integration with ZoneDefense[9]
- High Availability[11]

Advanced Functions

- Stateful Packet Inspection (SPI)
- Detect/Drop Intruding Packets
- Server Load Balancing
- Policy-based Routing

Unified Threat Management

- Optional Service Subscriptions
  - Intrusion Prevention System (IPS)
  - Antivirus (AV) Protection
  - Web Content Filtering (WCF)

Virtual Private Network (VPN)

- IPSec NAT Traversal
- VPN Hub and Spoke
- IPSec, PPTP, L2TP
- DES, 3DES, AES, Twofish, Blowfish,CAST-128 Encryption

The D-Link® NetDefend™ Unified Threat Management (UTM) firewalls provide a powerful security solution to protect business networks from a wide variety of threats. UTM Firewalls offer a comprehensive defense against virus attacks, unauthorized intrusions, and harmful content, successfully enhancing fundamental capabilities for managing, monitoring, and maintaining a healthy network.

Unified Threat Management

NetDefend UTM Firewalls integrate intrusion detection and prevention, gateway antivirus, and content filtering for superior Layer 7 content inspection protection. The real-time update service keeps the IPS information, antivirus signatures, and URL databases current. Combined, these enhancements help to protect office networks from application exploits, network worms, malicious code attacks, and provide everything a business needs to safely manage employee Internet access.

Powerful VPN Performance

NetDefend UTM Firewalls offer an integrated VPN Client and Server allowing remote offices or trusted partner to securely connect to a head office. Mobile users working remotely from home or on the road can also safely connect to the office network to access company data and e-mail. NetDefend UTM Firewalls incorporate hardware-based VPN engines to support and manage a large number of VPN configurations.

- Automated Key Management via IKE/ISAKMP
- Aggressive/Main/Quick Negotiation
- Multiple WAN Interfaces for Traffic Load Sharing[6]

Enhanced Network Services

- DHCP Server/Client/Relay
- IGMP V3
- H.323 NAT Traversal
- Robust Application Security ALGs
- OSPF Dynamic Routing Protocol[9]
- Run-Time Web-Based Authentication

DFL-260E

- Firewall Throughput: 150 Mbps
- VPN Performance: 45 Mbps (3DES/AES)
- 1 10/100/1000 Ethernet WAN Port
- 5 Switched 10/100/1000 Ethernet LAN Ports
- 1 10/100/1000 Ethernet DMZ Port

DFL-860E

- Firewall Throughput: 200 Mbps
- VPN Performance: 60 Mbps (3DES/AES)
- 2 10/100/1000 Ethernet WAN Ports
- 8 Switched 10/100/1000 Ethernet LAN Ports
- 1 10/100/1000 Ethernet DMZ Port

DFL-1660

- Firewall Throughput: 1.2 Gbps
- VPN Performance: 350 Mbps (3DES/AES)
- 6 Configurable Gigabit Ethernet Ports

DFL-2560(G)

- Firewall Throughput: 2 Gbps
- VPN Performance: 1 Gbps (3DES/AES)
- 10 Configurable Gigabit Ethernet Ports
- 4 SFP Ports (DFL-2560G)

Advanced VPN configuration options include:

- DES/3DES/AES/Twofish/Blowfish/CAST-128 encryption
- Manual or IKE/ISAKMP key management
- Quick/Main/Aggressive Negotiation modes
- VPN Authentication support using Radius server or user database

Enterprise-Class Firewall Security

NetDefend UTM Firewalls provide a complete set of advanced security features to manage, monitor, and maintain a healthy and secure network. Network management features include:

- Remote Management and Access Policies
- Bandwidth Control Policies
- URL Blacklists and Whitelists

UTM Services

Maintaining an effective defense against the various threats originating from the Internet requires that all three databases used by the NetDefend UTM Firewalls are kept up-to-date. In order to provide a continuous defense, D-Link offers optional UTM Service subscriptions which include updates for each defense:

- Intrusion Prevention Systems (IPS)
- Antivirus Protection (AV)
- Web Content Filtering (WCF).

NetDefend UTM Subscriptions ensure that each of the firewall's service databases are complete and effective.

Robust Intrusion Prevention[10]

The NetDefend UTM Firewalls employ component-based signatures, a unique IPS technology which recognizes and protects against all varieties of known and unknown attacks. This system can address all critical aspects of an attack or potential attack including payload, NOP sled, infection, and exploits. The IPS database includes attack information and data from a global attack sensor-grid and exploits collected from public sites such as the National Vulnerability Database and Bugtrax. The NetDefend UTM Firewalls constantly create and optimize NetDefend signatures via the D-Link Auto-Signature Sensor System without overloading existing security appliances. These signatures ensure a high ratio of detection accuracy and a low ratio of false positives.

Stream-based Virus Scanning[10]

The NetDefend UTM Firewalls examine files of any size, using a stream-based virus scanning technology which eliminates the need to cache incoming files. This zero-cache scanning method not only increases inspection performance but also reduces network bottlenecks. NetDefend UTM firewalls use virus signatures from Kaspersky Labs to provide systems with reliable and accurate antivirus protection, as well as prompt signature updates. Consequently, viruses and malware can be effectively blocked before they reach desktops or mobile devices.

Fast, Efficient Web Content Filtering[10]

Web Content Filtering helps administrators monitor, manage, and control employee Internet usage. The NetDefend UTM Firewalls implement multiple global index servers with millions of URLs and real-time website data to enhance performance capacity and maximize service availability. These firewalls use granular policies and explicit blacklists and whitelists to control access to certain types of websites for any combination of users, interfaces, and IP networks. The firewall can actively handle Internet content by stripping potential malicious objects, such as Java Applets, JavaScripts/VBScripts, ActiveX objects, and cookies.

NetDefend UTM Subscription

The standard NetDefend UTM Subscription provides your firewall with UTM service updates for 12 months starting from the day you activate or extend your service.2 The NetDefend UTM Subscription can be renewed regularly to provide your firewalls with the most up-to-date security service available from D-Link.

NetDefend Center: http://security.dlink.com.tw

Powerful VPN Engine

Hardware-based data encryption and authentication for IPSec, PPTP, L2TP, and SSL in Client/Server mode enable fast and safe handling of VPN traffic.[1]

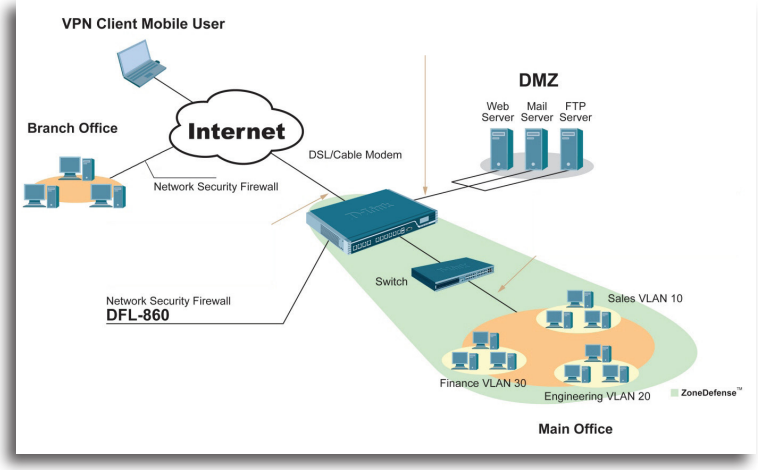
Professional Intrusion Prevention System (IPS)

Automatic updates from a comprehensive IPS signature database focus on attack payloads to protect the network against zero-day attacks.

Real-Time Antivirus Inspection (AV)

The antivirus engine scans using the most complete, most up-to-date antivirus signature database. Streaming-based pattern matching provides effective protection against viruses.

Secure Network Implementation Using NetDefend™ UTM Firewalls



Licensed for Unlimited Users

Optional subscription services for IPS, Antivirus Scanning, and Web Content Filtering are priced per firewall rather than per user, thus reducing the total cost of ownership for licensing.

WAN Link Load-Balancing and Fault-Tolerance

Multiple WAN ports support traffic load balancing and failover, thus guaranteeing Internet availability and bandwidth.

D-Link End-to-End Security (E2ES) Solutions[9]

The ZoneDefense mechanism, operating in conjunction with D-Link xStack switches, automatically quarantines infected workstations and prevents them from flooding the internal network with malicious traffic.

D-Link Green Certified

The D-Link Green certified DFL-1660 and DFL-2560(G) are built with an 80 PLUS internal power supply. 80 PLUS certified power supplies offer increased reliability due to greater efficiency, and provide a reduced cost of ownership through longer equipment life. Additionally, 80 PLUS power supplies help prevent pollution by limiting energy consumption, and run at a lower temperature reducing cooling costs.

The DFL-260E and DFL-860E save energy automatically through cable length and link status detection. By detecting the length of cables connected to a port, the amount of power used for the port can be adjusted, only using as much as is needed. The DFL-260E/860E also detect if a port is not in use, and can automatically reduce the power used for that port, cutting energy used for it by a substantial amount.

D-Link Green certified devices comply with RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) directives. RoHS directives restrict the use of specific hazardous materials during manufacturing, while WEEE implements standards for proper recycling and disposal. Together, these considerations make D-Link Green firewall products the environmentally responsible choice.

D-Link®

DFL-260E/860E/1660/2560/2560G NetDefend UTM Firewall Series

Technical Specifications

	DFL-260E	DFL-860E	DFL-1660	DFL-2560(G)
				
Ethernet Ports	• 1 10/100/1000 DMZ port (configurable) • 1 10/100/1000 WAN port • 5 Switched 10/100/1000 LAN ports	• 1 10/100/1000 DMZ port (configurable) • 2 10/100/1000 WAN port • 8 Switched 10/100/1000 LAN ports	• 6 configurable 10/100/1000 ports	• 10 configurable 10/100/1000 ports
SFP				• 4 SFP ports (DFL-2560G ONLY)[7]
USB	• 2 USB ports (reserved)			
Console	• RS-232		• DB-9 RS-232	
System Performance[1]				
Firewall Throughput[2]	• 150Mbps	• 200Mbps	• 1.2Gbps	• 2Gbps
VPN Throughput[3]	• 45Mbps	• 60Mbps	• 350Mbps	• 1Gbps
IPS Throughput[4]	• 60Mbps	• 80Mbps	• 400Mbps	• 600Mbps
Antivirus Throughput[4]	• 35Mbps	• 50Mbps	• 225Mbps	• 450Mbps
Concurrent Sessions	• 25,000	• 40,000	• 600,000	• 1,500,000
New Sessions (per second)	• 2,000	• 4,000	• 15,000	• 20,000
Policies	• 500	• 1,000	• 4,000	• 6,000
Firewall System	• Transparent Mode • NAT, PAT	• H.323 NAT Traversal	• Time-Scheduled Policies	• Application Lyer Gateway
Dynamic Routing Protocol		• OSPF		
Proactive End-Point Security		• ZoneDefense		
Networking	• DHCP Server/Client	• DHCP Relay	• Policy-Based Routing	• Port-based VLAN
IEEE 802.1q VLAN	• 8	• 16	• 1024	• 2048
IP Multicast	• IGMP v3			
Virtual Private Network (VPN)	• Encryption Methods (DES/3DES/AES/Twofish/Blowfish/CAST-128)	• PPTP/L2TP Server • SSL VPN	• Hub and Spoke	• IPSec NAT Traversal
Dedicated VPN Tunnels	• 100	• 300[5]	• 2,500	• 5,000
Traffic Load Balancing	• Outbound Load Balancing • Traffic Redirect at Fail-over	• Outbound Load Balancing • Traffic Redirect at Fail-over • Server Load Balancing		
Outbound Load Balance Algorithems	• Round-robin, Weight-based Round-robin, Destination-based, Spill-over			

Bandwidth Management	• Policy-Based Traffic Shaping	• Guaranteed Bandwidth • Dynamic Bandwidth Balancing	• Maximum Bandwidth	• Priority Bandwidth
High Availability	• WAN Fail-Over		• WAN Fail-Over • Active-Passive Mode • Device Failure Detection	• Link Failure Detection • FW/VPN Session SYN
Intrusion Detection & Prevention System (IDP/IPS)	• Automatic Pattern Update • DoS, DDoS Protection • Attack Alarm via E-mail • Advanced IDP/IPS Subscription	• Automatic Pattern Update • DoS, DDoS Protection • Attack Alarm via E-mail • Advanced IDP/IPS Subscription • IP Blacklist by Threshold or IDP/IPS		
Content Filtering	• HTTP Type: URL Blacklist/Whitelist • Script Type: Java, Cookie, ActiveX, VB		• Email Type: E-mail Blacklist/Whitelist • External Database Content Filtering	
Antivirus	• Real Time AV Scanning • Unlimited File Size • Scans VPN Tunnels		• Supports Compressed Files • Automatic Pattern Update • Signature Licensor: Kaspersky	
Physical & Environmental				
Power Supply	• Internal Power Supply		• 80 PLUS Internal Power Supply	
Dimensions	• 11.02" x 7.08" x 1.73" (280 x 180 x 44mm) • 11" Racket Mount	• 12.99" x 7.08" x 1.73" (330 x 180 x 44mm) • 13" Rack-Mount	• 17.32" x 15.75" x 1.73" (440 x 400 x 44mm) • 19" Standard Rack-Mount	
Operating Temperature	• 32°F to 104°F (0° to 40°C)			
Storage Temperature	• -40°F to 158°F(-20° to 70°C)			
Operating Humidity	• 5% to 95% non-condensing			
EMI	• FCC Class A	• CE Class A	• C-Tick	• VCCI
Safety	• UL LVD (EN60950-1)	• LVD (EN60950-1)	• cUL, CB	
MTBF	• 186,614 Hours	• 140,532 Hours	• 400,000 Hours	• 310,000 Hours
Warranty				
Warranty	• Limited Lifetime			
Ordering Information				

Part Number	*Description*
DFL-260E-NB	NetDefend Network Security UTM Firewall, 1 Gigabit WAN, 1 Gigabit DMZ, 5T LAN (90-Day IPS Subscription)
DFL-260-IPS-12	NetDefend IPS 1-Year Subscription for DFL-260/DFL-260E
DFL-260-AV-12	NetDefend AV 1-Year Subscription for DFL-260/DFL-260E
DFL-260-WCF-12	NetDefend WCF 1-Year Subscription for DFL-260/DFL-260E
DFL-860E-NB	NetDefend Network Security UTM Firewall, 2 Gigabit WAN, 1 Gigabit DMZ, 8 Gigabit LAN (90-Day IPS Subscription)
DFL-860-WCF-12	NetDefend WCF 1-Year Subscription for DFL-860/DFL-860E
DFL-860-IPS-12	NetDefend IPS 1-Year Subscription for DFL-860/DFL-860E
DFL-860-AV-12	NetDefend AV 1-Year Subscription for DFL-860/DFL-860E

Ordering Information	
Part Number	*Description*
DFL-1600	NetDefend Network Security Firewall, 6 User-Configurable Gigabit Ports (90-Day IPS Subscription)
DFL-1660-AV-12	NetDefend AV 1-Year Subscription for DFL-1660
DFL-1660-IPS-12	NetDefend IPS 1-Year Subscription for DFL-1660
DFL-1660-WCF-12	NetDefend WCF 1-Year Subscription for DFL-1660
DFL-1660-NB	NetDefend Network UTM Firewall, IU, 6GbE, 90 day IPS/AV/WCF
DFL-1600-AV-12	NetDefend AV 1-Year Subscription for DFL-1600
DFL-1600-IPS-12	NetDefend IPS 1-Year Subscription for DFL-1600
DFL-1600-WCF-12	NetDefend WCF 1-Year Subscription for DFL-1600
DFL-2560-NB	NetDefend Network UTM Firewall, IU, 10GbE, 90 day IPS/AV/WCF
DFL-2560G-NB	NetDefend Network UTM Firewall, IU, 6GbE, 4SFP, 90 day IPS/AV/WCF
DFL-2560-AV-12	NetDefend AV 1-Year Subscription for DFL-2560/2560G
DFL-2560-IPS-12	NetDefend IPS 1-Year Subscription for DFL-2560/2560G
DFL-2560-WCF-12	NetDefend WCF 1-Year Subscription for DFL-2560/2560G

[1] Actual performance may vary depending on network conditions and activated services.
[2] The maximum Firewall plaintext throughput is based on RFC2544 testing methodologies.
[3] VPN throughput is measured using UDP traffic at 1420 byte packet size adhering to RFC 2544.
[4] IPS and Anti-Virus performance test is based on HTTP protocol with a 1Mb file attachment run on the IXIA IxLoad. Testing is done with multiple flows through multiple port pairs.
[5] Performance based on firmware 2.27.00 and above
[6] Available when DMZ port is configured as WAN port
[7] Compatible with D-Link SFP module transceivers: DEM-310GT, DEM-311GT, DEM-312GT2, DEM-314GT, DEM-315GT, DGS-712
[8] Sold seperatley
[9] For DFL-860E, DFL-1660, and DFL-2560(G) only
[10] With optional subscription services
[11] For DFL-1660 and DFL-2560(G) only

Updated 12/7/11

DFL-260E DFL-860E DFL-1660 DFL-2560 DFL-2560G

For more information

U.S.A. | 17595 Mt. Herrmann Street | Fountain Valley, CA 92708 | 800.326.1688 | dlink.com **Canada** | 2525 Meadowvale Blvd | Mississauga, ON L5N 5S2 | 800.361.5265 | dlink.ca

NETDEFEND dlinkgreen D-Link® Building Networks for People