NETDEFEND

INTEGRATED FIREWALL/VPN

- Powerful Firewall Engine
- Virtual Private Network (VPN) Security
- Granular Bandwidth Management
- 802.1Q VLAN Tagging
- D-Link End-to-End Security Solution (E2ES) Integration with ZoneDefense

ADVANCED FUNCTIONS

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

UNIFIED THREAT MANAGEMENT

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

VIRTUAL PRIVATE NETWORK (VPN)

- IPSec NAT Traversal
- VPN Hub and Spoke
- IPSec, PPTP, L2TP
- DES, 3DES, AES, Twofish, Blowfish, CAST-128 Encryption
- Automated Key Management via IKE/ISAKMP
- Aggressive/Main/Quick Negotiation

ENHANCED NETWORK SERVICES

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

NetDefend UTM Firewall Series

Today's continuously shifting security environment presents a challenge for small/home office networks with limited IT capabilities. Fortunately, 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.

Enterprise-Class Firewall Security

NetDefend UTM Firewalls provide complete advanced security features to manage, monitor, and maintain a healthy and secure network. Network management features include: Remote Management, Bandwidth Control Policies, URL Black/White Lists, Access Policies and SNMP. For network monitoring, these firewalls support e-mail alerts, system logs, consistency checks and real-time statistics.

Unified Threat Management

NetDefend UTM Firewalls integrate an intrusion detection and prevention system, gateway antivirus, and content filtering for superior Layer 7 content inspection protection. An acceleration engine increases throughput, while the real-time update service keeps the IPS information, antivirus signatures, and URL databases current. Combined, these enhancements help to protect the office network 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. This allows remote offices to securely connect to a head office or a trusted partner network. Mobile users working from home or remote locations can also safely connect to the office network to access company data and e-mail. NetDefend UTM Firewalls have hardware-based VPN engines to support and manage a large number of VPN configurations. They support IPSec, PPTP, and L2TP protocols in Client/Server mode and can handle pass-through traffic as well. Advanced VPN configuration options include: DES/3DES/AES/Twofish/Blowfish/CAST-128 encryption, Manual or IKE/ISAKMP key management, Quick/Main/Aggressive Negotiation modes, and VPN authentication support using either an external RADIUS server or a large user database.

ICSA labs CERTIFIED IPSEC-ENHANCED

VPNC CERTIFIED AES Interop

ICSA labs CERTIFIED FIREWALL-CORPORATE

VPNC CERTIFIED Basic Interop

PERFORMANCE OPTIMIZATION

- UTM Acceleration Engine
- Multiple WAN Interfaces for Traffic Load Sharing

DFL-260

- Firewall Throughput: 80Mbps
- VPN Performance: 25Mbps (3DES/AES)
- 1 10/100 Ethernet WAN Ports
- 4 10/100 Ethernet LAN Ports
- 1 10/100 Ethernet DMZ Port

DFL-860

- Firewall Throughput: 150Mbps
- VPN Performance: 50Mbps (3DES/AES)
- 2 10/100 Ethernet WAN Ports
- 7 10/100 Ethernet LAN Ports
- 1 10/100 Ethernet DMZ Port

DFL-1660

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

DFL-2560(G)

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

NetDefend UTM Firewall Series

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 robust defense, D-Link offers optional NetDefend Firewall UTM Service subscriptions which include updates for each aspect of defense: Intrusion Prevention Systems (IPS), Antivirus and Web Content Filtering (WCF). NetDefend UTM Subscriptions ensure that each of the firewall's service databases are complete and effective.

Robust Intrusion Prevention

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. In terms of signature coverage, 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

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. Consequentially, viruses and malware can be effectively blocked before they reach the network's desktops or mobile devices.

Web Content Filtering

Web Content Filtering helps administrators monitor, manage, and control employee usage of and access to the Internet. 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 highly granular policies and explicit black/white lists 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.

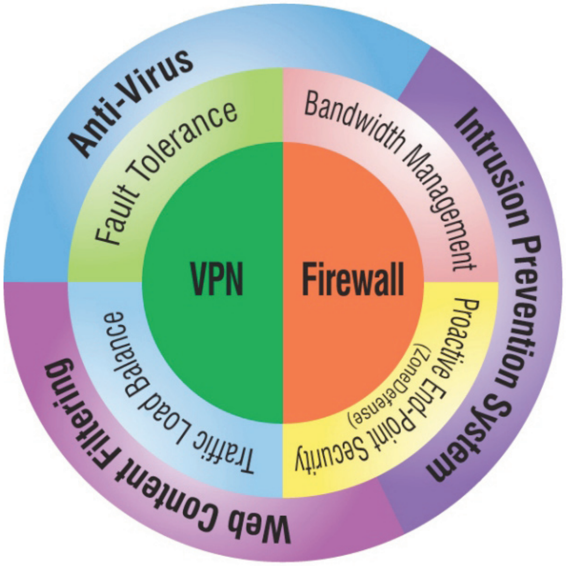
NetDefend UTM Subscription

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. 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

*Actual service package may vary depending on region.

NetDefend UTM Firewall Series



Powerful VPN Engine

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

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 the effective protection against viruses.

Fast, Efficient Web Content Filtering

Multiple index server implementation, highly granular policies, black lists and active content handling enhance performance and effectiveness of web surfing control.

Acceleration Engine for Unified Threat Management

A powerful processor allows the firewall to carry out IPS and Antivirus scanning simultaneously without performance degradation.

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) Solution*

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.

*For DFL-860, DFL-1660, and DFL-2560(G) only

D-Link Green Certified

The DFL-1660 and DFL-2560(G) have attained D-Link Green Certification. These firewalls 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 to prevent pollution by limiting energy consumption, and run at a lower temperature to reduce cooling costs.

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.

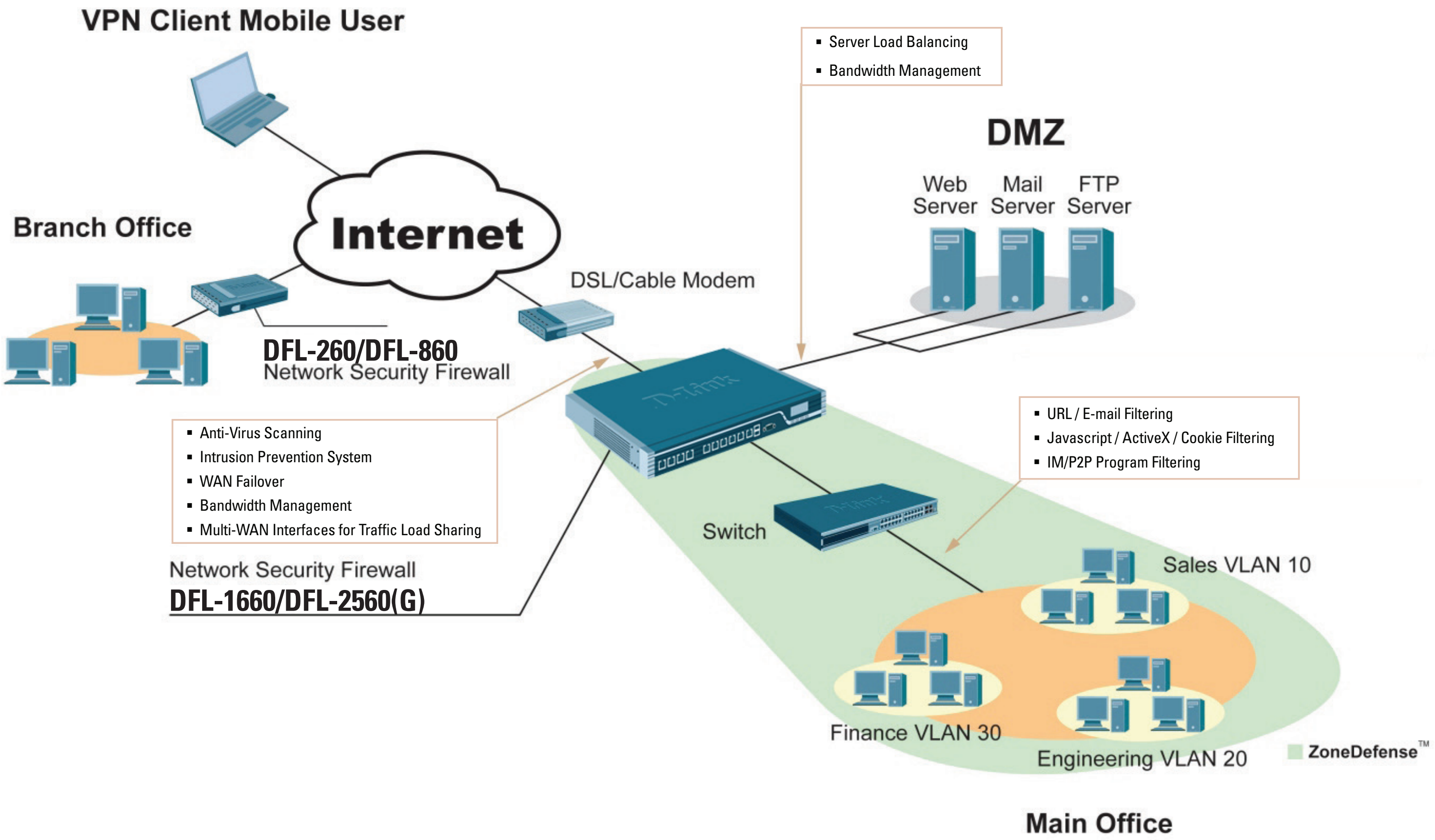
Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Interfaces	Ethernet	1 10/100 WAN Port 1 10/100 DMZ Port 4 10/100 LAN Ports	2 10/100 WAN Ports 1 10/100 DMZ Port 7 10/100 LAN Ports	6 Configurable Gigabit Ports	10 Configurable Gigabit Ports
	SFP	–	–	–	4 SFP Ports (DFL-2560G only)[7]
	USB	–	–	2 USB Ports (reserved)	2 USB Ports (reserved)
	Console	1 DB-9 RS-232	1 DB-9 RS-232	1 DB-9 RS-232	1 DB-9 RS-232
System Performance[1]	Firewall Throughput[2]	80Mbps	150Mbps	1.2Gbps	2Gbps
	VPN Throughput[3]	25Mbps	45Mbps	350Mbps	1Gbps
	IPS Throughput[4]	20Mbps	40Mbps	400Mbps	600Mbps
	Antivirus Throughput[4]	10Mbps	20Mbps	225Mbps	450Mbps
	Concurrent Sessions	10,000[5]	20,000[5]	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	✓	✓	✓	✓
	Dynamic Routing Protocol	–	OSPF		
	H.323 NAT Traversal	✓	✓	✓	✓
	Time-Scheduled Policies	✓	✓	✓	✓
	Application Layer Gateway	✓	✓	✓	✓
	Proactive End-Point Security	–	ZoneDefense		
Networking	DHCP Server/Client	✓	✓	✓	✓
	DHCP Relay	✓	✓	✓	✓
	Policy-Based Routing	✓	✓	✓	✓
	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)	✓	✓	✓	✓
	Dedicated VPN Tunnels	100	200[5]	2,500	5,000
	PPTP/L2TP Server	✓	✓	✓	✓
	Hub and Spoke	✓	✓	✓	✓
	IPSec NAT Traversal	✓	✓	✓	✓

Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Traffic Load Balancing	Outbound Load Balancing	✓	✓	✓	✓
	Server Load Balancing	–	✓	✓	✓
	Outbound Load Balance Algorithms	Round-robin, Weight-based Round-robin, Destination-based, Spill-over			
	Traffic Redirect at Fail-Over	✓	✓	✓	✓
Bandwidth Management	Policy-Based Traffic Shaping	✓	✓	✓	✓
	Guaranteed Bandwidth	✓	✓	✓	✓
	Maximum Bandwidth	✓	✓	✓	✓
	Priority Bandwidth	✓	✓	✓	✓
	Dynamic Bandwidth Balancing	✓	✓	✓	✓
High Availability (HA)	WAN Fail-Over	✓[6]	✓	✓	✓
	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	✓	✓	✓	✓
	IP Blacklist by Threshold or IDP/IPS	–	✓	✓	✓
Content Filtering	HTTP Type	URL Blacklist/Whitelist			
	Script Type	Java, Cookie, ActiveX, VB			
	E-mail Type	E-mail Blacklist/Whitelist			
	External Database Content Filtering	✓	✓	✓	✓

Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Antivirus	Real Time AV Scanning	✓	✓	✓	✓
	Unlimited File Size	✓	✓	✓	✓
	Scans VPN Tunnels	✓	✓	✓	✓
	Supports Compressed Files	✓	✓	✓	✓
	Signature Licensor	Kaspersky			
	Automatic Pattern Update	✓	✓	✓	✓
Physical & Environmental	Power Suppy	External Power Adapter		80 PLUS Internal Power Supply	
	Dimensions	235 x 162 x 36 mm Desktop Size	280 x 214 x 44 mm Desktop Size	440 x 400 x 44 mm 19” Standard Rack-Mount	
	Operating Temperature	0° to 40° C			
	Storage Temperature	-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

[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 2.26.00 and above
[6] Available when DMZ port is configured as WAN port
[7] Compatible with D-Link SFP module transceivers: DEM-330T, DEM-330R, DEM-331T, DEM-331R, DEM-310GT, DEM-311GT, DEM-312GT2, DEM-314GT, DEM-315GT, and DGS-712

Secure Network Implementation Using NetDefend™ UTM Firewalls



- Server Load Balancing
- Bandwidth Management

- Anti-Virus Scanning
- Intrusion Prevention System
- WAN Failover
- Bandwidth Management
- Multi-WAN Interfaces for Traffic Load Sharing

- URL / E-mail Filtering
- Javascript / ActiveX / Cookie Filtering
- IM/P2P Program Filtering

ACN 052 202 838

D-Link Corporation
No. 289 Xinhu 3rd Road, Neihu, Taipei 114, Taiwan
Specifications are subject to change without notice.
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.
©2009 D-Link Corporation. All rights reserved.
Release 03 (November 2009)