NETDEFEND

Integrated Firewall/VPN

- Powerful Firewall Engine featuring an intuitive redesigned Web GUI
- Virtual Private Network (VPN) Security
- Granular Bandwidth Management
- 802.1Q VLAN Tagging and Port-Based VLAN
- D-Link End-to-End Security Solutions (E2ES) Integration with ZoneDefense

Advanced Functions

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

Unified Threat Management

- Intrusion Prevention System (IPS)
- Antivirus (AV) Protection
- Web Content Filtering (WCF) in HTTPS
- Optional Service Subscriptions
- SafeSearch Enforcement
- Application Control

Virtual Private Network

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

ICSA labs CERTIFIED IPSEC - ENHANCED

ICSA labs CERTIFIED FIREWALL - CORPORATE

IPv6 READY

VPNC CERTIFIED AES Interop

VPNC CERTIFIED Basic Interop

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 a complete set of advanced security features to manage, monitor, and maintain a healthy and secure network. Network management features include: Remote Management, Bandwidth Control Policies, URL Blacklists and Whitelists, 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 office networks from application exploits, network worms, malicious code attacks, and provide everything a business needs to safely manage employee Internet access.

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

Application Control

Application control further enhances security by only allowing certain types of network traffic for predefined applications. NetDefend UTM Firewalls use application control to help accurately shape network traffic by either giving priority or applying control policies to effectively manage network utilization. Using packet inspection and a database of application signatures based on the application's network usage patterns, NetDefend UTM Firewalls give complete control over the content that is delivered to end users.

User Identity Awareness

Working with a Windows Domain controller, User Identity Awareness provides easy user authentication and tracking of network users. It provides a deeper insight to network administrators, helping to uniquely identify users by matching them with their network traffic. This gives network administrators a better understanding of what the needs of the network are, and allow for easier identification of usage, potential problems, security concerns and so forth. Network control with User Identity Awareness is more streamlined and efficient, allowing for the creation of identity-based policies and giving administrators instant updates for unintended usage of network resources.

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 remotely 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, L2TP, and SSL protocols in Client/Server mode and can handle pass-through traffic as well.[1] 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.

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

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

NetDefend UTM Firewall Series

Enhanced Network Services

- L2TPv3 Server / Client
- DHCP Server/Client/Relay
- IGMP V3
- H.323 NAT Traversal
- Robust Application Security for ALGs
- OSPF Dynamic Routing Protocol
- Run-Time Web-Based Authentication

Performance Optimization

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

DFL-260E

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

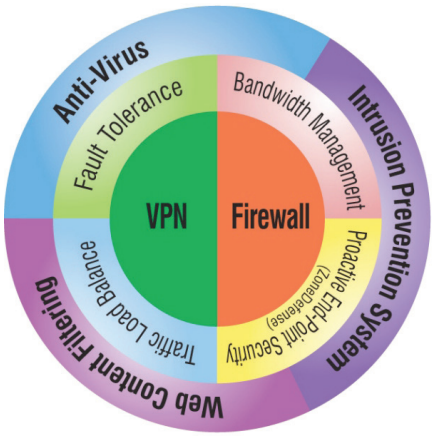
DFL-2560(G)

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

[1] Only Server mode available for SSL VPN.
[2] Actual service subscription options may vary depending on region.
[3] For DFL-860E, DFL-1660, and DFL-2560(G) only

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.

Web Content Filtering
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 in both regular HTTP and secured HTTPS by stripping potential malicious objects, such as Java Applets, JavaScripts/VBScripts, ActiveX objects, and cookies. Integration of SafeSearch Enforcement also ensures that results from search engine providers are provided without malicious content.

NetDefend UTM Subscription
The standard NetDefend UTM Subscription provides your firewall with UTM service updates for 12, 24, or 36 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

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.

Acceleration Engine for Unified Threat Management

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

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 [3]
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 to reduce cooling costs.

dlink green™

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 can also detect if a port is not in use, such as when a connected computer is shut down or if nothing is connected to the port, 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.

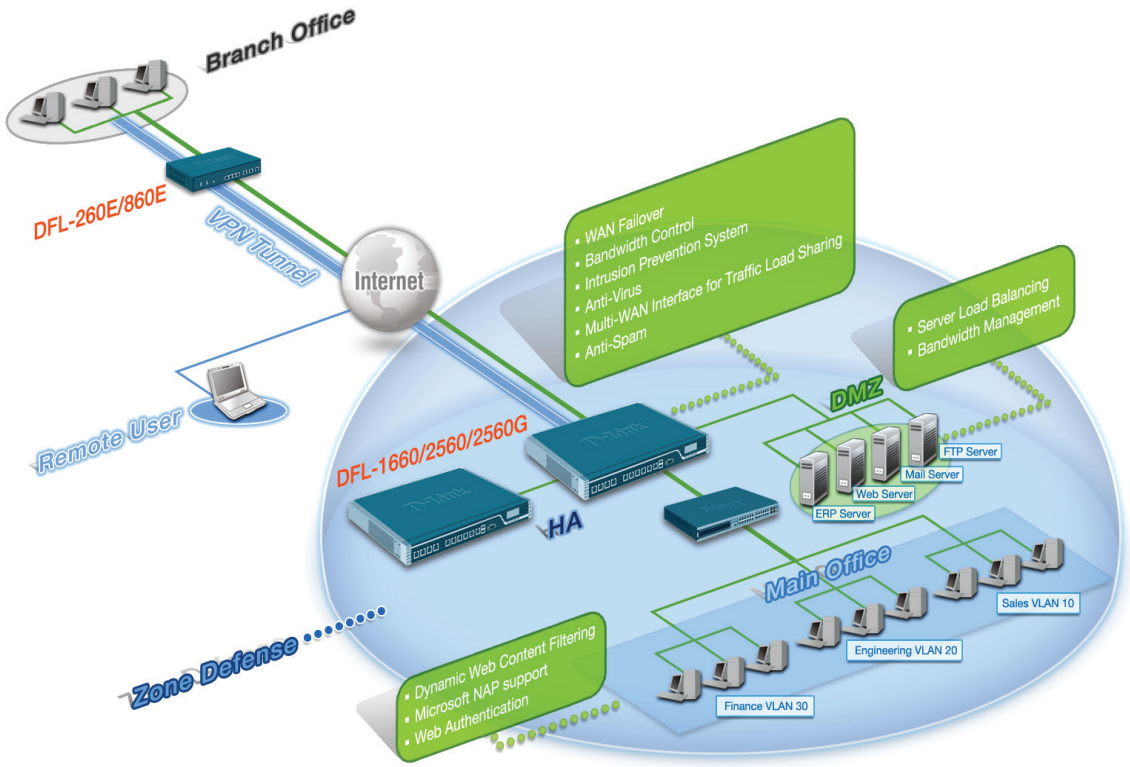
Technical Specifications		DFL-260E	DFL-860E	DFL-1660	DFL-2560(G)
					
Interfaces	Ethernet	1 10/100/1000 WAN port 1 10/100/1000 DMZ port (configurable) 5 10/100/1000 LAN ports	2 10/100/1000 WAN ports 1 10/100/1000 DMZ port (configurable) 8 10/100/1000 LAN ports	6 configurable 10/100/1000 ports	10 configurable 10/100/1000 ports
	SFP	–	–	–	4 SFP ports (DFL-2560G only) [4]
	USB	2 USB ports (reserved)	2 USB ports (reserved)	2 USB ports (reserved)	2 USB ports (reserved)
	Console	RJ-45	RJ-45	1 DB-9 RS-232	1 DB-9 RS-232
System Performance [5]	Firewall Throughput [6]	150 Mbps	200 Mbps	1.2 Gbps	2 Gbps
	VPN Throughput [7]	45 Mbps	60 Mbps	350 Mbps	1 Gbps
	IPS Throughput [8]	60 Mbps	80 Mbps	400 Mbps	600 Mbps
	Antivirus Throughput [8]	35 Mbps	50 Mbps	225 Mbps	450 Mbps
	Concurrent Sessions	25,000 [9]	40,000 [9]	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
	Port-based VLAN	✓			
	IP Multicast	IGMP v3			
Virtual Private Network (VPN)	Encryption Methods (DES/ 3DES/ AES/ Twofish/ Blowfish/ CAST-128)	✓	✓	✓	✓
	Dedicated VPN Tunnels	100	200 [9]	2,500	5,000
	PPTP/L2TP Server	✓	✓	✓	✓
	Hub and Spoke	✓	✓	✓	✓
	IPSec NAT Traversal	✓	✓	✓	✓
	SSL VPN	✓	✓	✓	✓

Technical Specifications		DFL-260E	DFL-860E	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 Failover	✓	✓	✓	✓
Bandwidth Management	Policy-Based Traffic Shaping	✓	✓	✓	✓
	Guaranteed Bandwidth	✓	✓	✓	✓
	Maximum Bandwidth	✓	✓	✓	✓
	Priority Bandwidth	✓	✓	✓	✓
	Dynamic Bandwidth Balancing	✓	✓	✓	✓
High Availability (HA)	WAN Fail-Over	✓ [10]	✓	✓	✓
	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/HTTPS Type	URL Blacklist/Whitelist			
	Script Type	Java, Cookie, ActiveX, VB			
	E-mail Type	E-mail Blacklist/Whitelist			
	External Database Content Filtering	✓	✓	✓	✓
	SafeSearch Enforcement	✓	✓	✓	✓
Application Control	Recognize over 1,000 Applications	✓	✓	✓	✓
	Bandwidth Management, Policy Control, and Prioritization	✓	✓	✓	✓
	Scheduling, and Rule-Based Control	✓	✓	✓	✓

Technical Specifications		DFL-260E	DFL-860E	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 Supply**	Internal Power Supply		80 PLUS Internal Power Supply	
	Max. Power Consumption	18.6 watts	22.8 watts	66.8 watts	103 watts
	Dimensions	280 x 180 x 44 mm 11" Rack-Mount	330 x 180 x 44 mm 13" Rack-Mount	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

[4] Compatible with D-Link SFP module transceivers: DEM-310GT, DEM-311GT, DEM-312GT2, DEM-314GT, DEM-315GT, DEM-330T, DEM-330R, DEM-331T, DEM-331R, DGS-712
[5] Actual performance may vary depending on network conditions and activated services.
[6] The maximum firewall plaintext throughput is based on RFC2544 testing methodologies.
[7] VPN throughput is measured using UDP traffic at 1420 byte packet size adhering to RFC 2544.
[8] 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.
[9] Performance based on firmware 2.27.00 and above
[10] Available when DMZ port is configured as WAN port

Secure Network Implementation Using NetDefend™ UTM Firewalls



ACN 052 202 838

D-Link Corporation
No. 289 Xinhu 3rd Road, Neihu, Taipei 114, Taiwan
Specifications are subject to change without notice.

Release 04 (June 2014)