Powerful Unified Threat Management (UTM) Firewalls for Small Businesses

- Integrated Firewall/VPN Appliance
- Intrusion Prevention System (IPS)
- Anti-Virus (AV) Protection
- Web Content Filtering (WCF)
- Proactive End-Point Security With D-Link ZoneDefense [3]
- Powerful Hardware Accelerator & VPN Performance

FEATURES

Integrated Firewall/VPN Appliance
- Powerful Firewall Engine
- Virtual Private Network (VPN) Security
- Granular Bandwidth Management
- 802.1Q VLAN Tagging
- Proactive End-Point Security With D-Link ZoneDefense [3]

Advanced Firewall Functions
- Stateful Packet Inspection (SPI)
- Detect/Drop Intruding Packets
- Server Load Balancing
- Policy-Based Routing
- Robust Application Security for ALGs

Unified Threat Management
- Intrusion Prevention System (IPS)
- Anti-Virus (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

Performance Optimization
- Hardware-Based UTM Acceleration
- Multiple WAN Interfaces for Traffic Load Sharing [1]

Enhanced Network Services
- DHCP Server/Client/Relay
- IGMP V3 [2]
- H.323 NAT Traversal
- SIP ALG [2]
- OSPF Dynamic Routing Protocol [3]
- Run-Time Web-Based Authentication

[1] Available on DFL-260 when DMZ port is configured as WAN2
[2] Available in future firmware upgrade
[3] Available on DFL-860

D-Link, the world's leading provider of total network solutions for SOHO and SMB, with products ranging from broadband modems/routers to managed Ethernet/Gigabit switches, wireless LAN, surveillance IP cameras and network storage, introduces a series of high-performance NetDefend UTM firewalls designed to answer businesses' need for complete network integration across different product lines. The D-Link DFL-260 and DFL-860 NetDefend Unified Threat Management (UTM) firewalls are powerful security solution designed to protect the small to mid-sized offices from a wide variety of network threats. These firewalls provide integrated remote routing, Network Address Translation (NAT), Virtual Private Network (VPN), proactive network security, Intrusion Prevention System (IPS), Web Content Filtering (WCF), Anti-Virus (AV) Protection, traffic load balancing and bandwidth management, all in one compact desktop chassis that can be easily integrated to existing network.

Enterprise-Class Firewall Security
The DFL-260 and DFL-860 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/Keyword Blocking, Access Policies and SNMP. For network monitoring, these firewalls support e-mail alerts, system log, consistency checks and real-time statistics.

Powerful VPN Performance
For optimal VPN configuration, the DFL-260 and DFL-860 have an integrated VPN Client and Server to support almost any required VPN policy. This allows a remote office to securely connect to a head office or a trusted partner network, while mobile users working from home or at other places can also safely connect to the office network to access company data and access e-mail. The DFL-260 and DFL-860 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.

Unified Threat Management
The DFL-260 and DFL-860 integrate an Intrusion Detection and Prevention System (IDP/IPS), gateway Anti-Virus (AV) and Content Filtering/Web URL Filtering for superior Layer 7 content inspection protection. They use a hardware accelerator approach to increase IPS and AV throughput, and a web surfing control database containing millions of URLs for Web Content Filtering (WCF). IPS, Anti-Virus and URL database real-time update services protect the office network from application exploits, network worms, malicious code attacks, and provide everything a business needs to manage employee Internet access behavior.

D-Link
Building Networks for People

NETDEFEND™

2 UTM Firewalls

For 2 Different Business Sizes

DFL-260 FOR SOHO

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

DFL-860 FOR SMALL BUSINESS

- Firewall Throughput: 150Mbps
- VPN Performance: 60Mbps (3DES/AES)
- 2 Ethernet WAN Ports, 7 Ethernet LAN Ports, 1 Ethernet DMZ Port

* DMZ port is user-configurable

UTM Services

Maintaining an effective defense against the various threats originating from the Internet requires that all three databases used by the DFL-260 and DFL-860 are kept up-to-date. In order to provide a robust defense, D-Link offers optional NetDefend Firewall UTM Services subscriptions which include distinct NetDefend service updates for each aspect of defenses: IPS, Anti-Virus and WCF. NetDefend UTM Subscription ensure that each of the firewall' s service databases is always accurate and current.

Robust Intrusion Prevention

The DFL-260 and DFL-860 adopt a unique IPS technology - component-based signatures, which are built to recognize and protect against all varieties of known and unknown attacks, and which 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 DFL-260 and DFL-860 delivers high quality IPS signatures by constantly creating and optimizing 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 the lowest ratio of false positives.

Stream-Based Virus Scanning

The DFL-260 and DFL-860 scan files of any sizes, using the stream-based virus scanning technology that does away with caching of incoming files. This scanning method increases inspection performance while eliminating network bottlenecks. The firewalls use virus signatures from the known, respected antivirus company Kaspersky Labs to provide users with reliable and accurate antivirus signatures, as well as prompt signature updates. Viruses and malware consequently can be effectively blocked before they reach the network's desktops or mobile devices.

Web Content Filtering

Web Content Filtering helps MIS monitor, manage, and control employee usage of and access to the Internet. The DFL-260 and DFL-680 implement multiple global index servers with millions of URL and real-time website information to enhance performance capacity and maximize service availability. These firewalls use highly granular policies and explicit black lists/white lists to allow or disallow where and when access to certain types of websites for any combination of users, interfaces and IP networks. They can strip potential malicious objects, such as Java applets, JavaScripts/VBScripts, ActiveX objects and cookies to actively handle the Internet content.

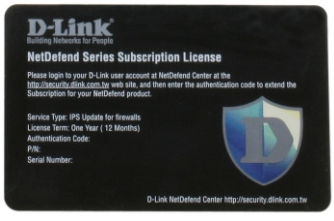
Hardware Accelerator

Equipped with hardware accelerators, the DFL-260 and DFL-860 can carry out IPS, Anti-Virus scanning functions simultaneously without degrading firewall and VPN performance. These powerful accelerators allow these firewalls to perform with a much higher throughput than other antivirus-capable UTM firewalls on the market.

NetDefend UTM Subscription

The standard NetDefend UTM (Unified Threat Management) Subscription provides your security appliances with UTM services for 12 months starting from the day you activate or extend your service. Your NetDefend UTM Subscription can be renewed regularly to provide your security devices with important updates and your network with the most up-to-date security service available from D-Link.

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



Integrated VPN/Firewall Functions

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

Professional Intrusion Prevention System (IPS)
Automatic update from comprehensive IPS signature database and focus on attack payload protect network against zero-day attacks.

Real-Time Anti-Virus Inspection (AV)
Powerful AV acceleration engine scans most complete, most up-to-date Anti-Virus signature database using streaming-based pattern matching for most effective protection against Internet virus.

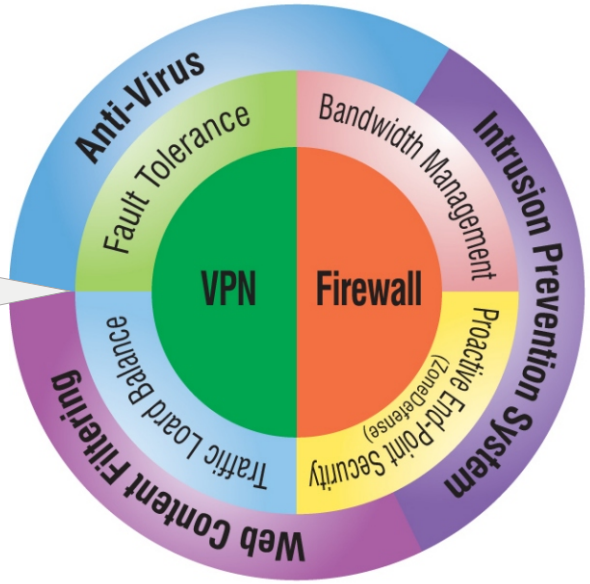
Fast, Efficient Web Content Filtering
Multiple index server implementation, highly granular policies, black lists and active content handling enhance performance and effectiveness of web surfing control.

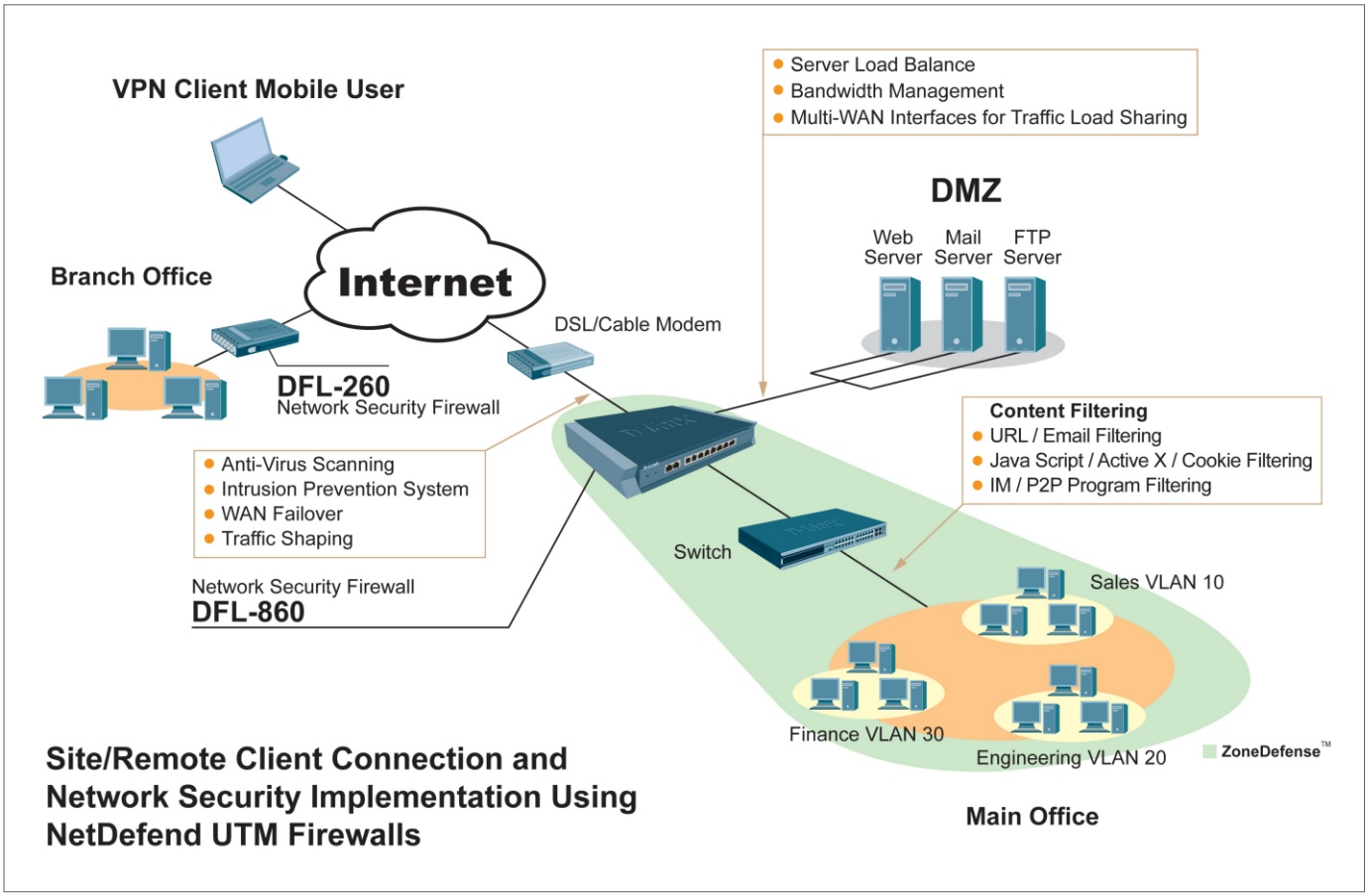
Hardware Accelerator for Unified Threat Management
Built-in hardware accelerator allows firewall to carry out IPS, Anti-Virus scanning simultaneously with no performance degradation.

All-Year-Round Database Update
Optional subscription services for IPS, AV scanning and Web Content Filtering are priced per firewall instead of per user, dispensing need for large total cost of ownership for licensing.

Guaranteed WAN Links
2 WAN ports supporting traffic load sharing, and fail-over guarantee Internet availability and bandwidth.

Proactive End-Point Security with D-Link ZoneDefense
ZoneDefense mechanism operating with D-Link xStack switches automatically quarantines infected workstations and prevents them from flooding internal network with malicious traffic.





Site/Remote Client Connection and Network Security Implementation Using NetDefend UTM Firewalls

D-Link®
Building Networks for People

NETDEFEND™

Specification Chart		DFL-260	DFL-860
			
Interfaces	Multiple User-Configurable Ports	1 Ethernet WAN Port 1 Ethernet DMZ Port [2] 4 Ethernet LAN Ports	2 Ethernet WAN Ports 1 Ethernet DMZ Port [2] 7 Ethernet LAN Ports
System Performance [3]	Firewall Throughput	80Mbps	150Mbps
	VPN Throughput	25Mbps	60Mbps
	Concurrent Sessions	12,000	25,000
	Policies	500	1,000
Firewall System	Transparent Mode	√	√
	NAT, PAT	√	√
	Dynamic Routing Protocol	-	OSPF
	H.323 NAT Traversal	√	√
	Time-Scheduled Policies	√	√
	Application Layer Gateway (ALG)	√	√
	Proactive End-Point Security	-	ZoneDefense
Networking	DHCP Server/Client	√	√
	DHCP Relay	√	√
	Policy-Based Routing	√	√
	IEEE 802.1q VLAN	8	16
	IP Multicast [1]	IGMP v3	IGMP v3
Virtual Private Network (VPN)	Encryption Methods (DES/3DES/AES/Twofish/Blowfish/CAST-128)	√	√
	Dedicated VPN Tunnels	100	300
	PPTP/L2TP Server	√	√
	Hub and Spoke	√	√
	IPSec NAT Traversal	√	√
Traffic Load Balancing	Outbound Load Balancing [1]	√	√
	Server Load Balancing	-	√
	Load Balance Algorithms	2 Types	3 Types
	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	√ [4]	√
Intrusion Detection & Prevention System (IDP/IPS)	Automatic Pattern Update	√	√
	DoS, DDoS Protection	√	√
	Attack Alarm via Email	√	√
	Advanced IDP/IPS Subscription	√	√
	IP Blacklist by Threshold or IDP/IPS	-	√
Content Filtering	HTTP Type [6]	URL, Keyword	URL, Keyword
	Script Type	Java, Cookie, ActiveX, VB	Java, Cookie, ActiveX, VB
	Email Type [5]	Blacklist, Keyword	Blacklist, Keyword
	External Database Content Filtering	√	√
Anti-Virus	Real Time AV Scanning	√	√
	Unlimited File Size	√	√
	Scans VPN Tunnels	√	√
	Supported Compression File	√	√
	Signature Licensor	Kaspersky	Kaspersky
	Automatic Pattern Update	√	√

Physical & Environmental	DFL-260	DFL-860
Power Input	External Power Adapter	External Power Adapter
Dimensions	235 x 162 x 36 mm Desktop Size	280 x 214 x 44 mm Desktop Size
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	FCC Class B CE Class B C-Tick
Safety	UL LVD (EN60950-1)	LVD (EN60950-1)
MTBF	21,571 Hours	36,879 Hours

[1] *Available in future firmware upgrade*
[2] *DMZ port is user-configurable*
[3] *Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services*
[4] *Available when DMZ port is configured as WAN port*
[5] *For SMTP protocol only*
[6] *For HTTP protocol only*

LISTED ITE E141136 66F9
ACN 052 202 838

Rev. 02 (Jun. 2007)