NETDEFEND

INTEGRATED FUNCTIONS

- Powerful Firewall Engine
- D-Link End-to-End Security Solution (E2ES) Integration
- Content Filtering/Intrusion Detection & Prevention
- User Authentication
- Instant Message/P2P Blocking
- Denial of Service (DoS) Protection
- Virtual Private Network (VPN) Security
- Bandwidth Management

CONTENT FILTERING

- URL/E-Mail Address Filtering
- Java Script/Active X/Cookie Filtering
- IM/P2P Program Filtering

FAULT TOLERANCE

- WAN Traffic Fail-Over
- Active/Passive Modes for High Availability[1]

BANDWIDTH MANAGEMENT

- WAN Traffic Bandwidth Management
- Multi-WAN Interfaces for Traffic Load Sharing/Load
- Balancing
- Dynamic Bandwidth Balancing

HARDWARE

- Powerful Firewall Engines
- Multiple User-Configurable Ports
- High-Speed Gigabit Interfaces[1]

SETUP & MANAGEMENT

- Installation Wizard for Quick Setup
- Easy Web-Based Configuration/ Management
- Command Line Interface (CLI)
- Logging and Real-Time Monitoring

[1] For DFL-1600 and DFL-2500 only

[2] For DFL-800, DFL-1600, and DFL-2500 only

[3] Component-based signature database is available through advanced IPS subscription

NetDefend Firewall Series

D-Link NetDefend firewalls offer the next-generation of high-performance, business-class network security solutions, addressing growing concerns over network security, hacker attacks, virus threats, and increasing privacy demands. NetDefend firewalls provide businesses with the assurance of a dedicated network security solution.

D-Link's NetDefend Firewall Series packs an impressive set of features including high-speed processors, extensive signature databases, and the power to handle up to a million concurrent sessions. Enclosed in an industrial chassis, these firewalls include multiple user-configurable interfaces, including high-speed Gigabit ports[1] for flexible, scalable and bottleneck-free network deployment.

NetDefend makes use of component-based signatures[3] which are built to recognize and protect against all varieties of known and unknown attacks. The IPS system can address all critical aspects of an attack or potential attack including the payload, NOP sled, infection, and any 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 D-Link constantly updates its Auto-Signature Sensor System in order to deliver high-quality, optimized, IPS signatures. Without overloading existing security appliances, these signatures ensure a high ratio of detection accuracy and the lowest ratio of false positives[3].

D-Link NetDefend firewalls can be remotely managed via a web-based interface or through a dedicated VPN connection. They include flexible features to monitor and maintain a healthy and secure network, such as e-mail alerts, system log and real-time statistics.

To minimize the impact of any event on an entire network, D-Link NetDefend firewalls include a special feature called ZoneDefense - a mechanism that operates seamlessly with D-Link xStack switches to perform proactive network security[2]. ZoneDefense automatically quarantines infected computers and prevents them from flooding the network with malicious traffic.

ICSA labs CERTIFIED IPSEC - ENHANCED

VPNC CERTIFIED AES Interop

ICSA labs CERTIFIED FIREWALL - CORPORATE

VPNC CERTIFIED Basic Interop

DFL-210 FOR SOHO
- Firewall Throughput: 80Mbps
- VPN Performance: 25Mbps (3DES/AES)
- 1 Ethernet WAN Ports
- 4 Ethernet LAN Ports
- 1 User-Configurable Ethernet DMZ Port

DFL-800 FOR SMALL BUSINESS
- Firewall Throughput: 150Mbps
- VPN Performance: 50Mbps (3DES/AES)
- 2 Ethernet WAN Ports
- 7 Ethernet LAN Ports
- 1 User-Configurable Ethernet DMZ Port

DFL-1600 FOR MEDIUM BUSINESS
- Firewall Throughput: 320Mbps
- VPN Performance: 120Mbps (3DES/AES)
- 6 User-Configurable Gigabit Ports

DFL-2500 FOR ENTERPRISE
- Firewall Throughput: 600Mbps
- VPN Performance: 235Mbs (3DES/AES)
- 8 User-Configurable Gigabit Ports

NetDefend Firewall Series

Fault Tolerance

NetDefendOS features Route Failover capability. Whenever a route failure is detected, traffic can automatically failover to an alternate route.

Content Filtering

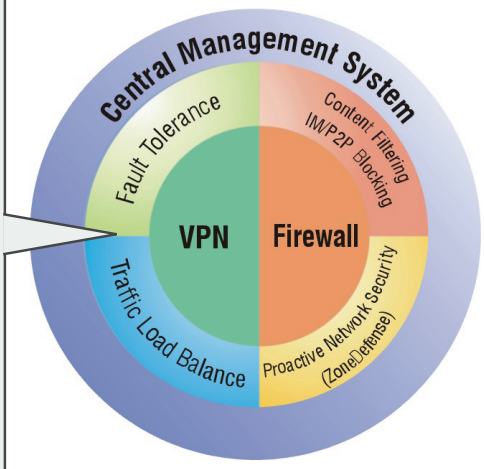
NetDefend firewalls protect users from dangerous and undesirable content on the web. Filters can also block IM/P2P programs to increase the efficiency and utilization of your network

Traffic Load Balancing

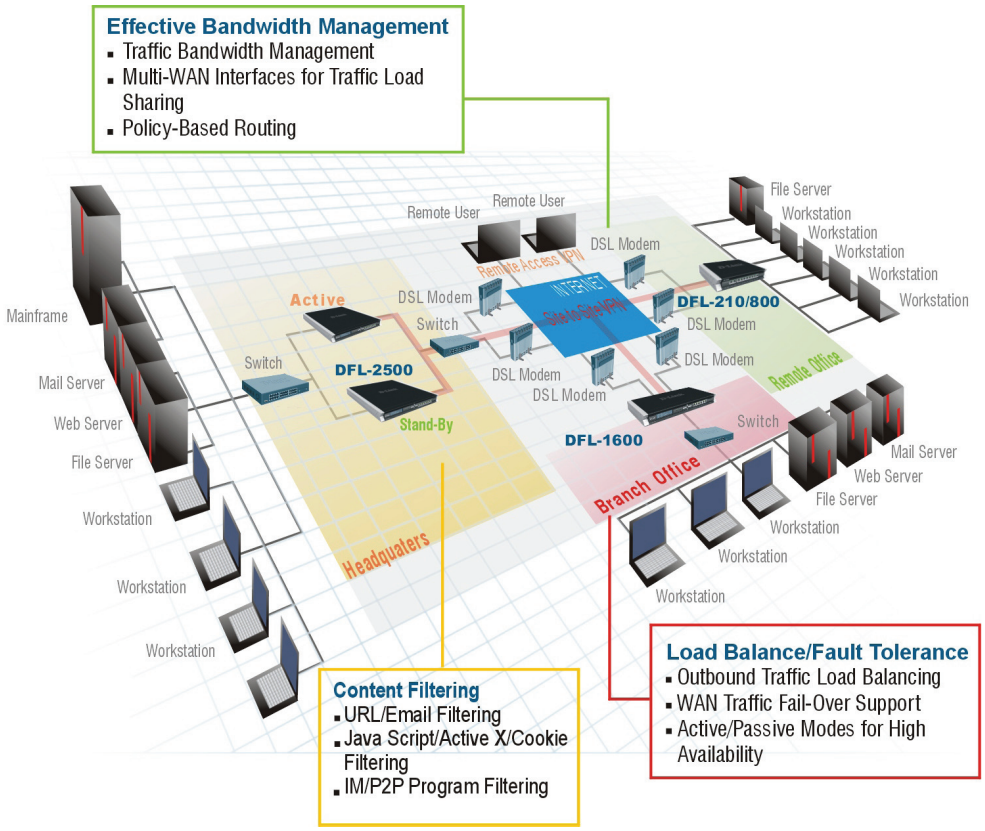
Keep your network running smoothly by balancing traffic using dual firewalls.

D-Link E2ES Solution

NetDefend firewalls feature ZoneDefense, a mechanism that operates seamlessly with your D-Link LAN switches to perform proactive network security. Whenever network virus or worm attacks are detected by the Firewall, ZoneDefense triggers and notifies D-Link Switches automatically. The infected hosts are the immediately disconnected to stop further infection among internal hosts.



Secure Network Implementation Using NetDefend™ Firewalls



NetDefend Firewall Series

Software Features

Firewall System
- Proprietary firewall system kernel, providing more security than open source-based firewalls
- Stateful Packet Inspection
- ZoneDefense with seamless integration with D-Link xStack series switches[2]
- Content filtering, Intrusion Detection & Prevention
- Time-scheduled policy-based routing and bandwidth management

Virtual Private Network (VPN)
- DES/3DES/AES/Twofish/Blowfish/CAST-128 encryption
- IKE v2 and X.509 v3 authentication
- VPN keep alive/Hub and Spoke

Traffic/Device Fault Tolerance
- WAN interface fail-over[3]
- Active/passive modes for High Availability[1]

Routing and IP Assignment
- IP alias
- DHCP Server/Client/Relay/over IPSec
- OSPF dynamic routing protocol[2]
- HTTP, FTP, SMTP, H.323, SIP Application Layer Gateway
- IEEE 802.1q tag-based VLAN

User Authentication
- Local database, external database with RADIUS/LDAP/Microsoft IAS
- Run-time user authentication
- Multiple authentication servers simultaneous operation

Bandwidth Management
- Guaranteed/Maximum/Priority bandwidth control
- Outbound traffic load balancing
- Policy-based bandwidth management
- Dynamic Bandwidth Balancing

Logging and Reporting
- Device management via HTTP, HTTPS and SSH
- SNMP v1, v2c and SNMP traps
- Real-time system monitoring and event log/alert
- Built-in LCM module for sample configuration[1]

Unified Threat Management
- Intrusion Prevention System (IPS)
- Web Content Filtering (WCF)[5]
- Antivirus (AV) protection[4]
- Optional service subscriptions[4]

[1] Available on DFL-1600 and DFL-2500 only

[2] Available on DFL-800, DFL-1600 and DFL-2500

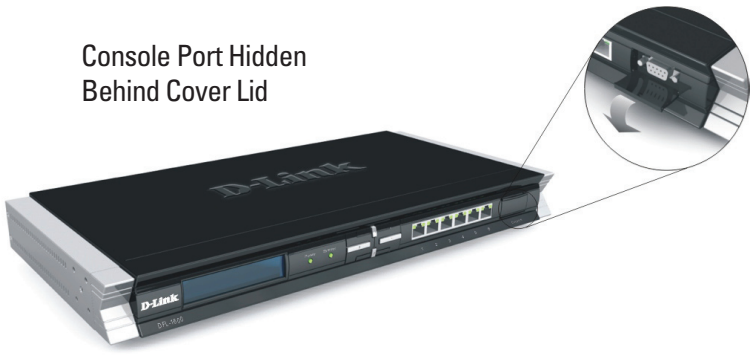
[3] Available on DFL-210 when DMZ ports configured as WAN port

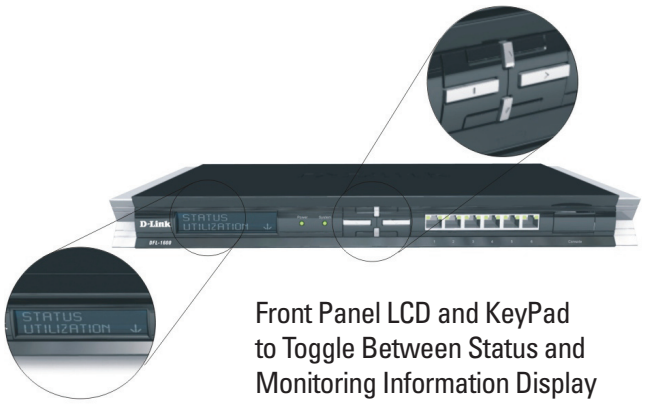
[4] Available on DFL-210 and DFL-800 with firmware 2.26.00 and above

[5] Dynamic Web Content Filtering available on DFL-210 and DFL-800 with firmware 2.26.00 and above

Hardware Features

Console Port Hidden Behind Cover Lid





Front Panel LCD and KeyPad to Toggle Between Status and Monitoring Information Display

Technical Specifications		DFL-210	DFL-800	DFL-1600	DFL-2500
Interfaces	Multiple User-Configurable Ports	1 Ethernet WAN Port 1 Ethernet DMZ Port [1] 4 Ethernet LAN Ports	2 Ethernet WAN Ports 1 Ethernet DMZ Port [1] 7 Ethernet LAN Ports	6 User-Configurable Gigabit Ports	8 User-Configurable Gigabit Ports
System Performance [2]	Firewall Throughput[5]	80Mbps	150Mbps	320Mbps	600Mbps
	VPN Throughput[6]	25Mbps	45Mbps	120Mbps	300Mbps
	IPS Throughput[7]	20Mbps	40Mbps	150Mbps	400Mbps
	Antivirus Throughput[7]	10Mbps[4]	20Mbps[4]	—	—
	Concurrent Sessions	10,000[4]	20,000[4]	400,000	1,000,000
	New Sessions (per second)	2,000	4,000	10,000	15,000
	Policies	500	1,000	2,500	4,000
Firewall System	Transparent Mode	✓	✓	✓	✓
	NAT, PAT	✓	✓	✓	✓
	Dynamic Routing Protocol	–	OSPF		
	H.323 NAT Traversal	✓	✓	✓	✓
	Time-Scheduled Policies	✓	✓	✓	✓
	Application Layer Gateway (ALG)	✓	✓	✓	✓
	Proactive Network Security	–	ZoneDefense		
Networking	DHCP Server/Client	✓	✓	✓	✓
	DHCP Relay	✓	✓	✓	✓
	Policy-Based Routing	✓	✓	✓	✓
	IEEE 802.1q VLAN	8	16	128	1024
	IP Multicast	IGMP v3			
Virtual Private Network (VPN)	Encryption Methods (DES/ 3DES/ AES/ Twofish/ Blowfish/ CAST-128)	✓	✓	✓	✓
	Dedicated VPN Tunnels	100	200[4]	1,200	2,500
	PPTP/L2TP Server	✓	✓	✓	✓
	Hub and Spoke	✓	✓	✓	✓
	IPSec NAT Traversal	✓	✓	✓	✓

Technical Specifications		DFL-210	DFL-800	DFL-1600	DFL-2500
System Management	Console Interface	RS-232			
	Web-Based User Interface	HTTP, HTTPS			
	Command Line/SSH	✓	✓	✓	✓
	Firmware Upgrade	✓	✓	✓	✓
	Config. Backup/ Restore	✓	✓	✓	✓
User Authentication	Built-in Database	✓	✓	✓	✓
	RADIUS	✓	✓	✓	✓
	LDAP	Microsoft AD 2003/2008 OpenLDAP 2.2.26			
	Microsoft IAS	✓	✓	✓	✓
	XAUTH for IPSec Authentication	✓	✓	✓	✓
Logging and Monitoring	Internal Log	✓	✓	✓	✓
	External Log	Syslog Server			
	E-mail Notification	✓	✓	✓	✓
	Event Log and Alarm	✓	✓	✓	✓
	SNMP	SNMP v1/v2c, SNMP traps			
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	✓	✓	✓	✓

Technical Specifications		DFL-210	DFL-800	DFL-1600	DFL-2500
High Availability (HA)	WAN Fail-Over	✓[3]	✓	✓	✓
	Active/Passive Modes	–	–	✓	✓
	Device Failure Detection	–	–	✓	✓
	Link Failure Detection	–	–	✓	✓
	FW/VPN Session Sync.	–	–	✓	✓
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 IPS/IDP	–	✓	✓	✓
Content Filtering	HTTP Type	URL Blacklist/Whitelist			
	Script Type	Java, Cookie, ActiveX, VB			
	E-mail Type	E-mail Blacklist/Whitelist			
	External Database Content Filtering	✓[4]	✓[4]	—	—
Antivirus	Real Time AV Scanning	✓[4]	✓[4]	—	—
	Unlimited File Size	✓[4]	✓[4]	—	—
	Scans VPN Tunnels	✓[4]	✓[4]	—	—
	Supports Compressed Files	✓[4]	✓[4]	—	—
	Signature Licensor	Kaspersky[4]		—	—
	Automatic Patter Update	✓[4]	✓[4]	—	—

Technical Specifications	DFL-210	DFL-800	DFL-1600	DFL-2500
Physical & Environmental — Power Supply	External Power Adapter		Internal Universal Power Supply	Internal Universal Power Supply
Dimensions	235 x 162 x 36 mm Desktop Size	280 x 214 x 44 mm Desktop Size	440 x 254 x 44 mm 19-inch Standard Rack-Mount Width, 1U Height	440 x 454 x 44 mm 19-inch Standard Rack-Mount Width, 1U Height
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)		
MTBF	186,614 Hours	140,532 Hours	71,965 Hours	101,819 Hours

[1] DMZ port is user-configurable
[2] Actual performance may vary depending on network conditions and activated services
[3] Available when DMZ port is configured as WAN port
[4] Supported from firmware 2.26.00 and above
Performance based on firmware 2.26.00 and above
[5] The maximum firewall plaintext through is based on RFC2544 testing methodologies
[6] VPN throughput is measured using UDP traffic at 1420 byte packet size adhering to RFC 2544
[7] IPS and Anti-Virus performance test is based on HTTP protocol with 1Mb file attachment run on IXIA Ixload. Testing is done with multiple flows through multiple port pairs

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 17 (November 2009)