D-Link®
Building Networks for People

Product Highlights

Comprehensive UTM Firewall Solution

Provides a versatile, integrated firewall solution to secure you network, with anti-spam, anti-virus, web content filtering, and application control features

ZoneDefense End-to-End Security (E2ES)

D-Link's proactive ZoneDefense End-to-End Security platform quarantines compromised workstations on the network and prevents malicious traffic flooding

Complete VPN Feature

With support for a wide range of security protocols, secure remote communication is easily configured and maintained in virtually any environment

DFL-870

NetDefend UTM Firewall

Features

Integrated Firewall

- Multiple WAN ports for WAN failover and outbound load balancing
- Link aggregation on LAN ports
- IEEE 802.1Q VLAN
- Granular bandwidth management
- D-Link pro-active ZoneDefense™ End-to-End Security (E2ES) solution

Unified Threat Management (UTM)

- Intrusion Detection & Prevention System (IDPS)
- Anti-virus protection
- Web Content Filtering (WCF) in HTTP/HTTPS
- Application control
- Email security

Virtual Private Network (VPN)

- Supports IPSec, PPTP, L2TP, SSL, GRE protocols
- Redundant VPN gateway
- Hub-and-spoke VPN support

Advanced Functions

- User authentication through:
  - Captive portal
  - User Identity Awareness
- Active/passive High Availability (HA)

The D-Link DFL-870 NetDefend UTM Firewall is a next generation Unified Threat Management (UTM) firewall which provides a powerful security solution to protect business networks from a wide range of threats. The DFL-870 offers a comprehensive defense against virus attacks, unauthorized intrusions, and flooding of harmful traffic, for successfully managing, monitoring, and maintaining a healthy network.

Enterprise-Class Security and Performance

The DFL-870 provides a complete set of advanced security features to secure, manage, and monitor your network. These features include remote management, bandwidth control policies, URL blacklists and whitelists, access policies, and SNMP support. The DFL-870 furthermore supports email alerts, system logging, consistency checking, and real-time statistics gathering that keeps you up-to-date on the status of the network. Additionally, multiple WAN ports support traffic load balancing and failover, thus guaranteeing Internet availability and bandwidth.

Unified Threat Management

The D-Link DFL-870 integrates an intrusion detection and prevention system, gateway anti-virus, content filtering, and application control for superior Layer 7 content inspection. An acceleration engine increases throughput, while the real-time update service keeps the IDPS information, anti-virus signature, URL and application 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. D-Link offers optional, cost-efficient, per-device NetDefend Firewall UTM Service subscriptions that ensure that each of the firewall's service databases remain current[1].

Robust Intrusion Prevention

The DFL-870 employs component-based signatures, a unique Intrusion Detection and Prevention System (IDPS) technology which recognizes and protects against all varieties of known and unknown attacks. This can address all critical aspects of an attack or potential attack including payload, NOP sled, infection, and exploits. In terms of signature coverage, the IDPS 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-870 constantly creates and optimizes NetDefend signatures via the D-Link Auto-Signature Sensor System without overloading existing security appliances. These signatures ensure high detection accuracy and a minimal amount of false positives. Automatic updates from a comprehensive IDPS signature database focus on attack payloads to protect the network against zero-day attacks.

Web Content Filtering

Web Content Filtering (WCF) helps administrators monitor, manage, and control employee Internet usage. The DFL-870 implements multiple global index servers with millions of URLs and real-time website data to enhance performance capacity and maximize service availability. The firewall uses 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 connections by stripping potential malicious objects, such as Java, JavaScript, and VBScript applets, ActiveX objects, and cookies. Integration of SafeSearch Enforcement[2] also ensures that results from search engine providers are provided without malicious content.

Application Control

Application control enhances security by only allowing certain types of network traffic for predefined applications. The DFL-870 uses 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, the DFL-870 gives complete control over the content that is delivered to end users.

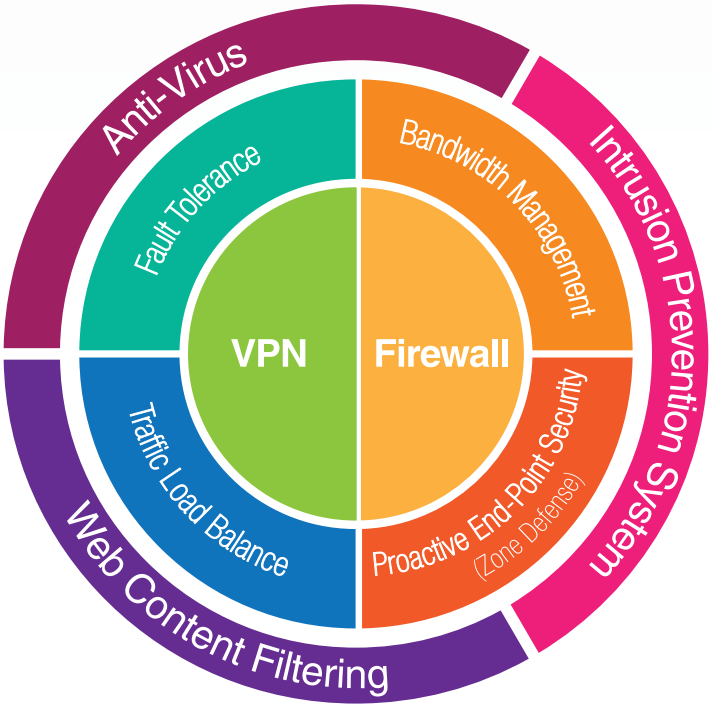
Powerful VPN Performance

The DFL-870 NetDefend UTM Firewall offers an integrated VPN client and server which support IPSec, PPTP, L2TP, and SSL protocols[3]. This allows remote offices to securely connect to a head office or a trusted partner network. With hardware-based VPN engines, it supports and manages a large number of VPN configurations. It supports IPSec, PPTP, L2TP, and SSL[3] protocols in client/server mode and can handle pass-through traffic as well.

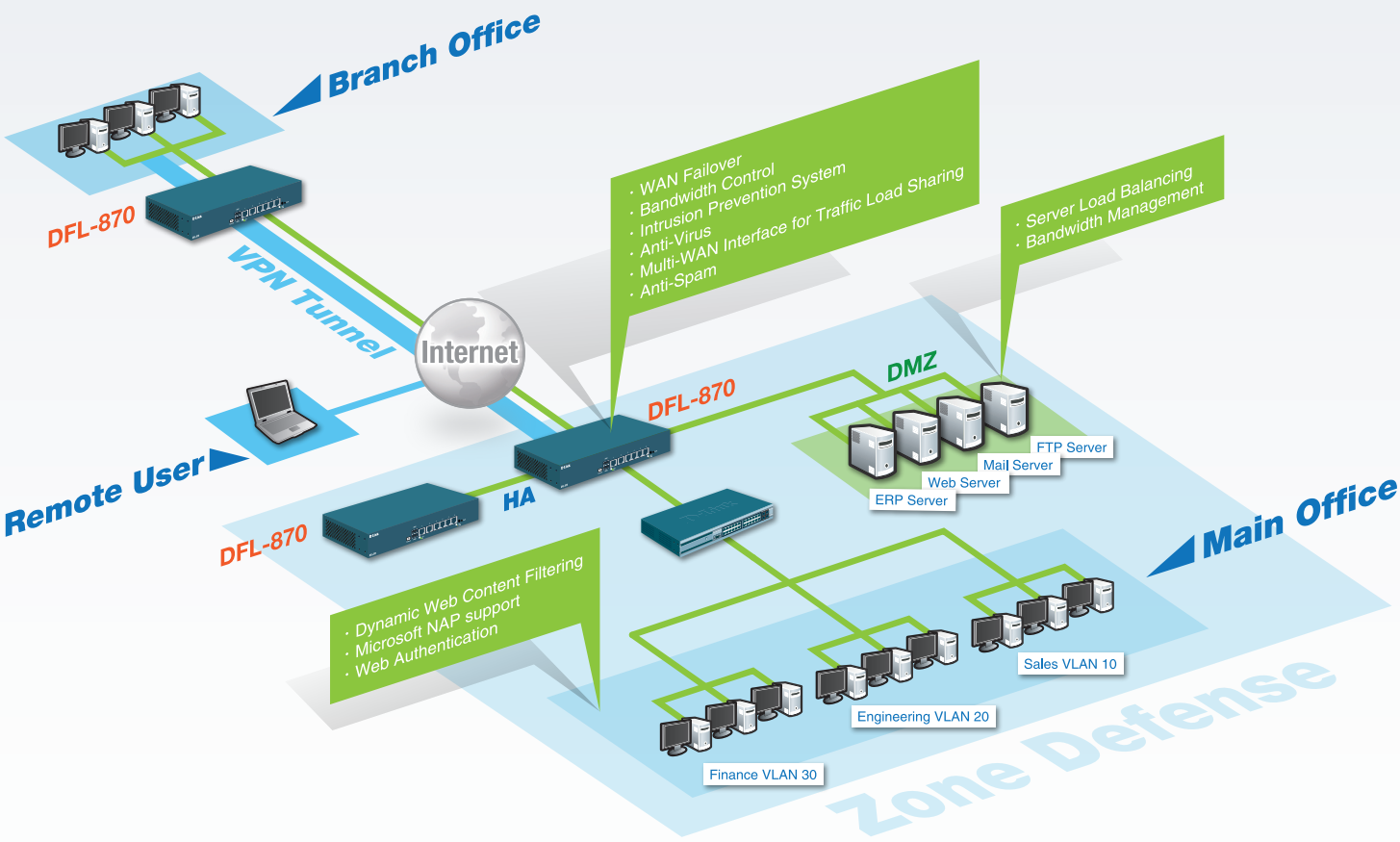
Stream-based Virus Scanning

The DFL-870's stream-based virus scanning examines files of any size while eliminating the need to cache incoming files first. This zero-cache scanning method not only increases inspection performance, but also reduces network bottlenecks. Kaspersky Labs virus signatures to provide reliable and accurate anti-virus and malware protection, as well as prompt signature updates.

Segmented Overview of the DFL-870's Dedicated Features



Secure Enterprise Network Implementation Using the DFL-870



Technical Specifications

Interface		
Ports	• 6 x configurable 10/100/1000BASE-T ports • 2 x USB 2.0 ports (reserved for future use)	• 1 x Mini-USB console port
Performance[4]		
Firewall Throughput[5]	• 4 Gbps	
VPN Throughput[6]	• 1 Gbps	
IPS Throughput[7]	• 450 Mbps	
Anti-virus Throughput[7]	• 600 Mbps	
Application Control Throughput[7]	• 700 Mbps	
Concurrent Sessions	• 500,000	
New Sessions per Second	• 45,000	
Supported Number of Policies	• 2,000	
Physical		
Power Supply	• 100 ~ 240 V AC, internal AC power supply	
Maximum Power Consumption	• 20 W	
Dimensions (W x D x H)	• 278 x 183 x 44 mm (10.95 x 7.20 x 1.73 inch)	
Weight	• 1.7 kg (3.75 lbs)	
Temperature	• Operating: 0 to 40 ˚C (32 to 104 ˚F)	• Storage: -20 to 70 ˚C (-4 to 158 ˚F)
Operating Humidity	• 5% to 95% RH, non-condensing	
MTFB	• 374,681 hours	
EMI	• FCC Class A • VCCI	• CE Class A
Safety	• LVD (EN60950-1)	

D-Link
Building Networks for People

DFL-870 NetDefend UTM Firewall

Software		

Firewall System	• NAT/PAT
	• Dynamic Routing Protocol
	  • OSFPv2
	• Application layer gateway
	  • HTTP
	  • FTP
	  • H.323
	  • POP3
	  • SMTP
	  • SIP
	  • TFTP
	  • TLS 1.0 (RFC2246)
		• Transparent mode
		• H.323 NAT Traversal
		• Time-scheduled policies
		• ZoneDefend proactive endpoint security
		• User Authentication
		  • Local user database
		  • RADIUS
		  • Microsoft AD
		  • LDAP

Networking	• DHCP server/client • DHCP relay • IGMPv3 IP multicasting • IPv6 support	• Policy-based Routing • IEEE 802.1Q VLAN • Link aggregation
Traffic Load Balancing	• Outbound load balancing • Failover traffic redirection	• Server load balancing
Bandwidth Management	• Guaranteed bandwidth • Priority bandwidth • Time-scheduled traffic shaping • Dynamic bandwidth balancing	• Maximum bandwidth • Policy-based traffic shaping • VPN tunnel bandwidth management • IDP traffic shaping
High Availability (HA)	• WAN failover • Device failure detection • FW/VPN session synchronisation	• Active/passive mode • Link failure detection

Virtual Private Network (VPN)	• 200 tunnels
	• Encryption methods:
	  • DES
	  • 3DES
	  • AES
	  • Blowfish
	  • Twofish
	  • CAST-128
		• IKE/IKEv2
		• Redundant IPSec VPN gateway
		• Hub-and-spoke
		• IPSec NAT traversal
		• Dead Peer Detection (DPD)
		• PPTP/L2TP server/client
		• SSL VPN[3]
		• GRE

Intrusion Detection & Prevention System (IDPS)	• 12, 24, 36 months service subscription • Automatic pattern updating • DoS/DDoS attack protection	• Email-based intrusion notification • IP blacklisting based on threshold or IDP/IPS • Advanced IDP/IPS subscription

Content Filtering	• 12, 24, 36 months service subscription
	• Web URL blacklisting/whitelisting:
	  • HTTP
	  • HTTPS
	• Customize forbidden web page
	• Maximum file size protection
	• SafeSearch Enforcement[2]
		• Filtering based on script types:
		  • Java applets
		  • JavaScript
		  • VBScript
		  • Cookies
		  • ActiveX

Anti-Virus	• Real-time scanning
	• Virus scanning for protocols:
	  • HTTP
	  • FTP
	  • SMTP
	  • POP3
	  • IMAP
		• Stream-based scanning
		• Anti-virus over VPN
		• ZIP/GZIP compressed file scanning up to 10 levels
		• Signature licensing
		  • Kaspersky

Application Control	• 12, 24, 36 months service subscription • Supports 1,000+ recognized applications • Schedule and rule-based control	• Application bandwidth management, policy control, and prioritization

Email Security	• Supported protocols:
	  • SMTP
	  • POP3
	  • IMAP
	• File type whitelisting/blacklisting
		• Email address filtering
		  • Sender/receiver blacklist
		  • Exempt list
		• File extension and MIME type verification
		• Anti-spam

DFL-870 NetDefend UTM Firewall

System Management	• Install Wizard • Command line interface (CLI) • SNMP (v1/v2c) • Email notifications	• Web-based user interface (HTTP/HTTPS) • Secure Shell (SSH) • Syslog • Real-time performance monitoring

Ordering Information

Part Number	*Description*
DFL-870	NetDefend UTM Firewall

[1] Service subscription options may vary depending on the region.
[2] The SafeSearch Enforcement only supports Google, Bing, and Yahoo search engines.
[3] Only server mode is available for SSL VPN.
[4] Actual performance may very depending on network conditions and services activated on the firewall.
[5] Firewall throughput was measured using UDP traffic with a 1,518 bytes packet size, conforming with RFC2544.
[6] VPN Throughput was measured using UDP traffic with a 1,420 bytes packet size, conforming with RFC2544.
[7] IPS and anti-virus performance is based on FTP protocol with a 1 GB file attachment run on IXIA IxLoad. Testing was done with multiple flows through multiple port pairs.

Updated October 7, 2016

D-Link®
Building Networks for People