

DFL-300

Hardware-Based VPN Router / FireWall

Hardware -Based Firewall Designed for the Small Office Environment

The D-Link DFL-300 Office Firewall is a hardware-based firewall designed for the small office environment. The DFL-300 Office Firewall provides an economical solution for providing small offices with dependable firewall protection against malicious attacks from hackers on the Internet. The DFL-300 provides a web-based interface for easy setup and configuration but is also designed with more advanced security features than typically found in residential gateways. The DFL-300 defends networks against damaging Denial of Service (DoS) attacks and offers network reliability through Stateful Packet Inspection (SPI). It can detect hacker attacks and disallow intruding packets from entering the office network.

Additionally, the DFL-300 is equipped with embedded VPN support that can create multiple IPSec tunnels to remote offices. IPSec on the DFL-300 uses strong encryption with DES, 3DES, and Automated Key Management via IKE/ISAKMP. A VPN tunnel can be activated from the DFL-300 to a remote office for a secured traffic flow between the two locations for mobile users using triple DES Encryption. This offers users a way to confidentially access and transfer sensitive information. Multiple VPN tunnels may be easily created without the need to setup IKE (Internet Key Exchange) policies.

The DFL-300 can support an unlimited number of network clients without the cost of additional licensing fees for the clients. URL blocking is part of the basic feature offered by DFL-300 and provides the benefit of limiting access to undesirable Internet sites. Logs of real-time Internet traffic, alarms of Internet attacks, and notice of web-browsing activities are logged and can be reported through e-mail notification.

The DFL-300 is a cost-effective firewall solution for small and medium-sized businesses because it features SPI (Stateful Packet Inspection), Detect/Drop intruding packets (DoS and Hacker attacks), embedded VPN, DMZ port, multiple-mapped IPs, multiple virtual servers, and server load balancing, typically found on more expensive firewalls.

The DFL-300 includes with three auto-sensing 10Base-T, 100Base-TX, RJ-45 ports. The Internal LAN port connects to the office network and the External WAN port connects to a broadband modem such as Cable or DSL. The DFL-300 Office Firewall also offers a DMZ (Demilitarized Zone) port which allows DMZ computers to be accessed from the Internet. This particular feature is useful because it alleviates congested server traffic from entering the Internal network. Web, Mail, and FTP Servers can take advantage of the DMZ port.

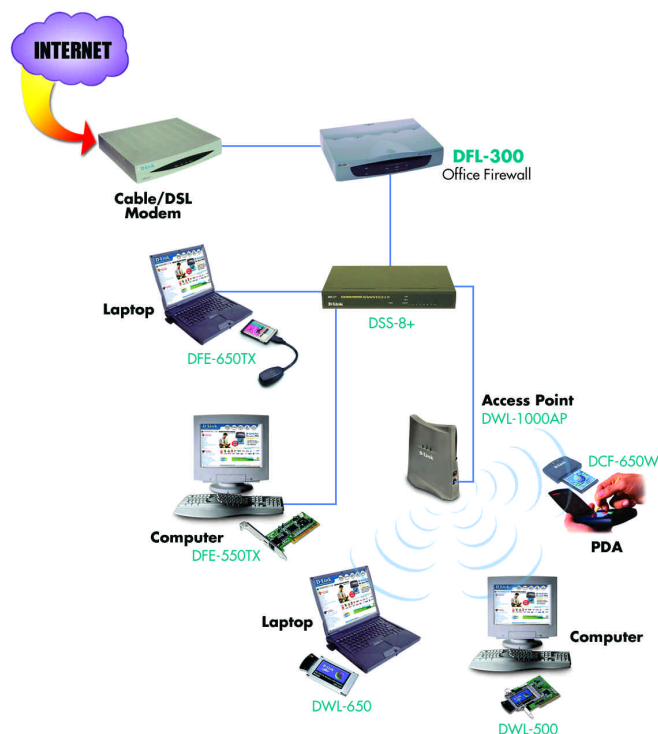
The web-based management offered by the DFL-300 provides an easy-to-use interface and is password-protected but still easily accessible through



The D-Link DFL-300 Office Firewall is a hardware-based firewall designed for the small office environment.

any Internet browser. Thus, incoming and outgoing policies for firewall traffic, as well as, setup configuration are easily accomplished through the web-based interface.

The DFL-300 Office Firewall detects SYN, Ping of Death, Spoof, Tear Drop, ICMP Flood, UDP Flood, and other attacks against the local network and can be set up to log and send the attack report notification to a specified e-mail address. The DFL-300 can be configured to log all these attacks, locate the source IP address generating the attack, and establish the policy to restrict incoming traffic from that specific IP address source.



The DFL-300 Office Firewall provides an economical solution for providing small offices with dependable firewall protection against malicious attacks from hackers on the Internet.

DFL-300

Office Firewall

Technical Specifications	
Features & Benefits	<ul style="list-style-type: none">● Easy-to-Install, Easy-to-Use● VPN: IPSec, Triple-DES, DES, Automated Key Management via IKE/ISAKMP, MD5, SHA-1● Unlimited Users (No Additional License Required)● Multiple IPSec VPN tunnels (No License Re● Remote and local administration through a Web-based Configuration● Three auto-sensing 10/100 Base-TX Ethernet Ports (External, Internal, & DMZ)● Real-time monitoring provides traffic detail viewable via Web Browser● 100Mbps performance with simultaneous advanced firewall rules● Standard Support: ARP, TCP/IP, FTP, DNS, SMTP, UDP, ICMP, DHCP, HTTP, RIP1, RIP2, IKE, IPSec
Hardware Description	<ul style="list-style-type: none">● Processor: NS Geode GX1 300 MHz Low-Power CPU on-board● Chipset: NS CS5530A● 256K Ward Licensed BIOS● 32MB SDRAM● 16MB Flash Memory● Universal Power Adapter: Output 5V, 3A● Operating Temperature: 0°C ~ 60°C● Humidity: 5% ~ 95% RH, non-condensing● 8 LED's (6 Networking Connection, 1 Power-on, 1 Status)● One 10/100Mbps LAN/Internal port● One 10/100Mbps WAN/external port● One 10/100Mbps DMZ port● Factory Reset Button● Dimensions (l*h*w): 8.7in x 6.57in x 1.1in
Software Functions	<ul style="list-style-type: none">● Web-Based Management● Support DMZ Port● Firewall Reset Setting● Software Update (via Browser)● Detect Hackers, DoS Attacks● Ping and Web GUI /Enable or Disable● Synchronize System Clock with Client● NAT/PAT (IP Sharing)● SPI (Stateful Packet Inspection)● Detect DoS (SYN/UDP/ICMP) Attacks● Drop intruding packets● E-mail Alert Notification● Built-in PPPoE Client● DHCP Client/Server● DHCP Management● Address Book / Address Group Book Setting● Service Book / Service Group Book Setting● Pre-defined Service / Custom Service Group● Support Group Setting● Static Route● Fixed IP Assigned by DHCP Server● Support Policies● External to Internal Access Control● External to DMZ Access Control● Internal to DMZ Access Control● Support Server Load Balancing● Support VPN (IPSec)● Support Schedule of Access Control● Multiple Mapped IP (Software DMZ Host)● Multiple Virtual Server● Traffic/Event Log● Log Report/Mail● Traffic/Event Alarm● Statistics● LAN/WAN Browser Management● DNS Proxy● Status Report● ARP Table● DHCP Client log
Warranty	One Year Limited Warranty