D-Link
Building Networks for People

Network Security Firewall for Enterprise

DFL-1100

NetDefend

- High Performance IPSec VPN Support
- Policy Based Firewall Functionality
- Content Filtering
- Bandwidth Management
- Intuitive Web-Based Management Interface
- 3 Year Warranty

Network Security Firewall

VPNC CERTIFIED Basic Interop

Hardware Firewall

HIGH Performance

FREE TECH SUPPORT

D-Link's DFL-1100 is an easy-to-deploy, high-capacity firewall designed for large Enterprises that require superior price/performance.

This firewall is a powerful security solution that features fault tolerance and high availability, providing integrated NAT, Firewall, Content Filtering, IDS protection, bandwidth management as well as VPN support. Other features include WAN link support, a trusted LAN port, a DMZ port to support local e-mail and web servers, and a backup port to connect to another firewall.

The DFL-1100 features enterprise-grade firewall functions, including SPI, detect/drop intruding packets, embedded VPN, a physical DMZ port, multiple-mapped IPs and multiple virtual servers. The DFL-1100 connects your office to a broadband modem such as cable or DSL through an external 10/100BASE-TX WAN port.

The DFL-1100 provides complete firewall functions, including the NAT mode, PAT (Port Address Translation) mode, Transparent mode, Routing mode and SPI. It also supports customized policy and virtual server configuration. Administrators can easily manage the network through graphical statistics in a logging/monitoring system.

Because the DFL-1100 is equipped with embedded VPN support, this allows you to create multiple IPSec tunnels to remote sites/clients. IPSec on the DFL-1100 uses strong encryption with DES, 3DES, AES and Automated Key Management via IKE/ISAKMP. A VPN tunnel can be activated from the DFL-1100 to a remote site or a mobile user for secured traffic flow 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 URL blocking function 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. Radius authentication is also supported, so you can make use of your existing Radius Server and user information.

DFL-1100 provides advanced features including Content filtering, IDS (Intrusion Detection System), Bandwidth Management for complete solution protection to users's network. Content Filtering lets you filter/protect your network with customized policy. Bandwidth management guarantees bandwidth for different services. The DFL-1100 protects your network from attacks. It can be configured to log all attacks, locate the source IP address generating the attack, send the attack report notification to a specified e-mail address and establish policies to restrict incoming traffic from specific IP address sources. Network administrators can set e-mail addresses to receive alert message from the DFL-1100. When intrusion events are detected, the DFL-1100 will log them and send alert e-mail, and the administrator can check the log file on the router to find out what happened.

The DFL-1100 can operate with up to 200,000 concurrent sessions, providing up to 1,000 VPN tunnels for up to 1,000 mobile telecommuters needing secure remote connections to the company network. In addition, this firewall also provides fault tolerance through redundancy backup with another firewall through a backup port, providing continuous firewall protection for mission-critical applications.

The DFL-1100 includes a LAN port that connects to your internal office network, a backup port that connects to another firewall, and a physical DMZ (Demilitarized Zone) port that can connect your Web, mail or FTP servers for access from the Internet. DMZ alleviates

Network Security Firewall

Technical Specs

Firewall Mode of Operation
- NAT (Network Address Translation)
- PAT (Port Address Translation)
- Route mode
- Virtual IP
- Policy-based NAT

VPN Security
- IPSec Server/Client, PPTP Server/Client, L2TP Server/Client
- IPSec/PPTP/L2TP pass through
- Authentication transform: MD5 and SHA-1
- Encryption transform: Null, DES, 3DES and AES
- Key management: manual and IKE
- Keying mode: Pre-Shared Key
- Key exchange: DH1, DH2 and DH5
- Negotiation mode: Quick, Main & Aggressive mode
- Remote access VPN
- Policy-Based firewall and session protection
- Keep-Alives on tunnel free configurable
- Hub-n-Spoke

Firewall Security
- NAT
- Stateful Packet Inspection (SPI)/ Denial of Service (DOS)
- Packet filter
- Content filter
- Custom Protocol Filters
- Custom ICMP Filter
- Microsoft Active Directory Integration (via MS IAS)

Administration
- Multiple administrators
- Root Admin, Admin & Read Only user levels
- Software upgrades and configuration changes
- Trust host

Bandwidth Management
- Guaranteed bandwidth
- Maximum bandwidth
- Priority-bandwidth utilisation
- DiffServ stamp
- Class-based policies
- Application-specific traffic class
- Policy-based traffic shaping
- Subnet-specific traffic class

Network Service
- DHCP Server/Client
- DHCP Relay
- DHCP over IPSec
- PPPoE for xDSL
- PPTP for xDSL
- BigPond Cable
- H.323 Application layer gateway
- SIP Application layer gateway
- FTP application layer gateway
- DNS resolving remote gateway

System
- System log
- Firmware backup
- E-mail alerts
- Filtering activity
- Web access log
- Internet Access Monitor
- Remote Management from WAN
- SNTP and SNMP
- SDI service (Ericsson Solution)
- Http & Consistency checks

Firewall & VPN User Authentication
- RADIUS (external) database
- Built-in database: 1500 users

IDS
- NIDS pattern
- DDoS and DoS detected
- Mac address bind with IP
- On-line pattern update
- Attack alarm (via E-mail)
- Log and report

Hardware
- CPU: x86 300MHz high performance processor
- DRAM: 256 Mbytes SDRAM
- Flash memory: 64 Mbytes
- Factory reset button
- VPN accelerator for higher performance

Device Ports
- WAN: 10/100BASE-TX port
- LAN: 10/100BASE-TX port
- DMZ: 10/100BASE-TX port
- Sync: 10/100BASE-TX port
- Console port: serial COM port

Performance & Throughput
- Firewall: 250 Mbps or higher
- 3DES: 34 Mbps or higher
- AES: 84 Mbps or higher
- Concurrent sessions: 200,000 max.
- VPN tunnels: 1000 max.

Diagnostic LEDs
- Power & Status
- WAN
- LAN
- DMZ
- Backup

Power Supply
- Internal universal power supply

Dimensions
- 29.5 x 44 x 4.4 cm

Weight
- 3.8 kg (device only)

Environmental

Operating
- 0 to 60 deg C
- 5% – 95% non-condensing

Storage
- -20 to 70 deg C
- 5% – 95% non-condensing

Emissions (EMI)
- FCC Class A, CE Class A, C-Tick

Safety
- UL, TUV/GS, LVD (EN60950)

Package Content

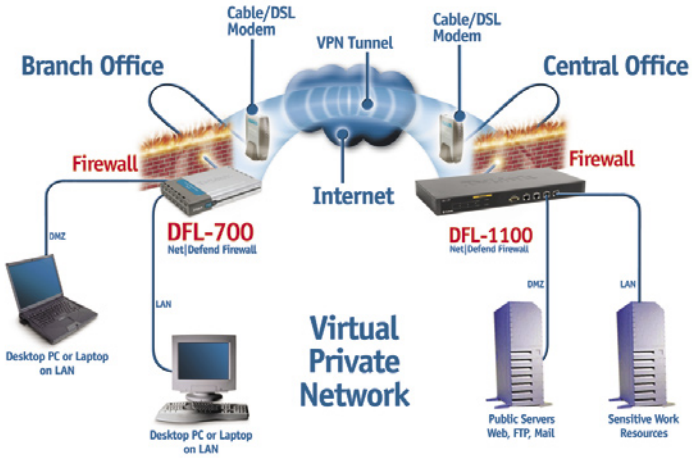
DFL-1100 Network Security Firewall
- Quick Installation Guide
- Installation CD
- CAT5 straight-through Cable
- RS232 Cable

Warranty Details

- 3 Years from date of purchase
  (return to D-Link Australia Office)

Ordering Information

- DFL-1100
(Network Security Firewall)



D-Link Australia Pty. Ltd. 1 Giffnock Avenue North Ryde NSW 2113 Phone: +61-(0)2-8899-1800
www.dlink.com.au *www.dlink.co.nz*

N856 N856

D-Link® Building Networks for People