D-Link®
Building Networks for People

DFL-M510

FEATURES

IM/P2P Application Management

- Supports Most IM/P2P Applications
- Blocks Viruses over IM/SPIM
- Prevents Misuse of IM/P2P Applications

Bandwidth Management

- Controls File Transfer/Streaming Media Over HTTP
- Controls Personal Mail
- Controls Web Usage
- QoS Bandwidth Management

Malicious Traffic Prevention

- Blocks Spyware, Network Worms, Trojans and Illegal Agents
- Identifies Victims
- Protects Against DoS/DDoS
- Zone-Defense Mechanism[1]

Traffic Monitoring/Report

- Monitors Traffic Real Time
- Provides Multi-layer TOP N Reports

Hardware

- Hardware-Based Layer 7 Payload Inspection
- Hardware Bypass to Maximize Network Uptime
- 1 Ethernet WAN Port
- 1 Ethernet LAN Port
- Front Panel LCD/Key Pad to Display Status/Monitoring Information

Product Data Sheet

NetDefend
Information Security Gateway

The NetDefend family of Firewall/VPN Security Appliances is D-Link's answer for hardware-based network security. The D-Link DFL-M510 NetDefend Information Security Gateway is a revolutionary security device designed to protect your network from the emerging security risks.

The DFL-M510 is an essential resource for business facing threats posed by an increasing use of instant messaging (IM) and peer-to-peer (P2P) applications. Without effective management and control mechanisms in place, these applications are vulnerable to a wide variety of security risks including viruses and worms, leakage of confidential information, corporate and regulatory compliance violations, and even identity theft.

The DFL-M510 can help address these threats by identifying unmanaged, unauthorized IM and P2P activity on your network. Effectively control and manage information flows from your company to the outside world. The DFL-M510 will not only let you control and manage IM and P2P applications, but also file transfers, e-mail and streaming media applications.

IM/P2P and Bandwidth Management

The DFL-M510 allows you to better manage your employees' network activities and prevent possible misuse of IM and P2P applications. Implementation can be based on company policies and operation is both automatic and transparent. Eliminate excessive use of precious network bandwidth and prevent against possible leaks of company secrets through unauthorized and unmanaged communication.

Malicious Traffic Prevention

Hackers and scammers are becoming more sophisticated in their approach to vulnerable networks, distributing not just viruses and malicious agents, but putting together blended attacks, increasing perimeter security for other scam methods, multiplying mutations of initial attacks and migrating new threats. The DFL-M510 Information Security Gateway can prevent these threats by blocking illegal agents attempting to hide amongst normal network traffic, eliminating harmful programs, identifying victims and providing a Zone Defense Mechanism(1) to quarantine infected computers. You can detect and drop traffic with health concerns, including Trojan, illegal agents and Network Worms, based on policy rules applied to specific groups, hosts, IP addresses and subnets.

Seamless Integration

The DFL-M510 integrates easily with industry-standard network infrastructures and works exceptionally well when used in tandem with a D-Link NetDefend VPN Firewall. Deployed between your company's internal network and the network firewall, the DFL-M510 can be installed in in-line mode without causing any change to your current network architecture. It implements a hardware bypass function that avoids single points of failure and maximizes network connection in the event of a hardware crash.

With the DFL-M510, leverage your existing investments by adding anti-virus and anti-IM spam, identity authentication and management, session logging and archiving, as well as detection and usage reporting. Improve office productivity, reduce potential legal liability, and enhance your company's overall network security with the D-Link DFL-M510 NetDefend Information Security Gateway.

NetDefend

DFL-M510

Information Security Gateway

Specifications

Real Transparent Mode Implementation
- Easy Installation with No Change to Existing Network Architecture
- Interoperability with third-party network devices

Hardware-Based Layer 7 Payload Inspection
High-Performance Processing via ASIC Content Processing Chip

Granular Management by Hosts, IPs, Groups and Subnets
- Transparent Control of IM, P2P, File Transfers, Streaming Media, Personal Mail
- Discreet Control of Internet Activities Through Application of Policy-Based Actions on Hosts, Groups, IP Addresses, Subnets

Transparent Blocking of Trojan, Spyware, Illegal Agents, and Network Worms
Prevention of Malicious Traffic Spreading on the Network

Victim Identification
Isolation of Trouble Spots for Troubleshooting

Hardware Bypass
No Single Points of Failure, Maximized Network Connection in Case of Hardware Crash

Log/Analysis Report
Easily Readable Reports Printable in HTML Formats

DOS/DDOS Protection, Stealth Mode
- Protection from Various Kinds of DOS/DDOS Attacks
- No Response to ICMP Packets in Stealth Mode

IM/P2P Management
- Control/management of IM applications
- Control/management of P2P applications
- Policy setting by IP, host name, group or subnet

Layer 7 Applications Management
- Control/Management of Mile Transfers
- Control/Management of Streaming Media
- Control/Management of Web Applications
- Control/Management of Email for Personal Use
- User-Defined Application Control

Health Checking
- Detection/Blocking of Malicious Programs such as Spyware, SoftEther, Network Worms
- Victim Identification in Intranet
- D-Link Zone Defense Mechanism[1] to Prevent Malicious Programs from Spreading on Network when Used in Conjunction with Certain D-Link Mananged Switches

Real-Time Monitor and Report
- Real-time Traffic Monitoring
- Multi-Layer TOP N Reports

Installation/Setup
- Plug-and-play Installation with No Change to Existing Network
- Transparent In-line mode, Seamless Integration with Other Network Devices
- Java Web-Based Setup Wizard
- Hardware Bypass Mechanism to Maximize Network Connectivity
- Stealth Mode for Interface

Performance
- 4,000 Concurrent TCP sessions
- Up to 150 Concurrent Users
- Up to 22Mbps Throughput (All Functions Enabled)
- Up to 80Mbps Throughput (Bypass Mode)

Power Input
Internal Universal Power Supply

Dimensions
- Standard 19-Inch Rackmount, 1U Height
- 17.3” x 9.8” x 1.75”

Operating Temperature
32°F to 140°F

Storage Temperature
-4°F to 158°F

Safety
- UL/CUL
- LVD (EN60950)

EMI
- FCC Class A
- CE Class A
- C-Tick

Operating Humidity
5% to 95% (non-condensing)

Warranty
1-Year

[1] Future firmware upgrade.

D-Link®
Building Networks for People