D-Link
Building Networks for People

DFL-M510

Information Security Gateway

Sicheres Netzwerk gegen auftretende Risiken

- Kontrollieren und verwalten Sie Instant Message- und Peer-to-Peer-Anwendungen
- Behalten Sie die Kontrolle über die Bandbreite für Streaming Media, Dateiübertragung und Internet-Nutzung
- Erkennen und blockieren Sie Spyware, Trojanern, Softether und Netzwerkwürmern
- Verhindern Sie die Ausbreitung von bösartiger Software im Netzwerk

Das D-Link NetDefend DFL-M510 Information Security Gatewy (ISG) ist ein völliger neuer Gerätetyp, der für den Schutz Ihres Netzwerks vor auftretenden Risiken entwickelt wurde. Die Bedrohung aus dem Internet durch die steigende Nutzung von Instant Message (IM)- und Peer-to-Peer (P2P)-Anwendungen wächst. Ohne effektives Management und Kontrollmechanismen ist Ihr Netzwerk durch eine Vielzahl verschiedener Bedrohungen, wie z.B. Viren und Würmern, Verlust von vertraulichen Informationen, Verletzung von Firmen- und anderen Vorschriften, gefährdet

Das NetDefend Information Security Gateway (ISG) hilft Ihnen gegen diese Bedrohungen vorzugehen und unkontrollierten, nicht genehmigten IM- und P2P-Gebrauch in Ihrem Netzwerk zu erkennen. So können Sie effektiv den Informationsfluss zwischen Ihrer Firma und dem „Rest der Welt" kontrollieren und verwalten. Sie kontrollieren und verwalten Instant Message- und Peer-to-Peer-Anwendungen, Datenüber-tragungen, Email und Streaming Media im Internet.

IM/P2P und Bandbreiten-Management

Das NetDefend Information Security Gateway (ISG) unterstützt Sie beim Management der Internetaktivitäten Ihrer Angestellten und verhindert den möglichen Missbrauch von IM- und P2P-Anwendungen. Die Durchführung kann auf Firmenregeln basieren. Der Ablauf ist sowohl automatisch als auch transparent. Dadurch werden fühlbare Vorteile erreicht, auch bei der sinnvollen Ausnutzung der wertvollen Bandbreite im Netzwerk und beim Schutz vor möglichen Lecks durch den unkontrollierten, nicht genehmigten Einsatz von IM und Email.

Verhinderung von „bösartigem" Datenverkehr

Hacker und Betrüger werden immer ausgebuffter in ihren Versuchen in verwundbare Netzwerke einzudringen. Dabei verteilen sie nicht nur Viren und bösartige Software, sondern sie vermengen auch Angriffe, erhöhen den Schutzumfang gegen andere Methoden, verfielfältigen Mutationen des ursprünglichen Angriffs und erzeugen neue Bedrohungen. Das D-Link NetDefend Information Security Gateway kann solche Bedrohungen durch die Blockade von unbekannten Software-Agenten, die sich im normalen Datenverkehr verbergen, verhindern, dabei werden gefährliche Programme eliminiert, Opfer aufgespürt und ein Zone-Defense-Mechanismus* zur Quarantäne von infizierten Rechner eingesetzt. Datenverkehr mit bedenklichem Inhalt wird erkannt und auf Basis von Regeln für bestimmte Gruppen, Hostnamen, IP-Adressen und/oder Subnetze unterdrückt, darin eingeschlossen sind Trojaner, illegale Agenten und Netzwerkwürmer.

Nahtlose Integration

Das NetDefend Information Security Gatewy (ISG) lässt sich problemlos in eine Netzwerk-Infrastruktur nach Industriestandard integrieren. Die Kompatibilität mit Geräten anderer Hersteller bietet ein Maximum an Flexibilität und Kontrolle. Das ISG wird zwischen Ihrem Firmennetzwerk und einer Firewall ein-gesetzt. Es kann im In-Line-Modus ohne weitere Änderungen an der bestehenden Netzwerk-Architektur eingerichtet werden. Es verfügt über ein hardwareseitige Bypass-Funktion, die einzelne Fehler-quellen (Single Points of Failure) umgeht und die Netzwerk-verbindung für den Fall eines Hardware-Ausfalls maximiert.

Mit der hardware-basierten Nutzlastüberwachung (Layer 7) bietet dieses Gerät ein schnelle Verarbeitung für die Netzwerksicherheit. Sie können ihre getätigten Investitionen verbessern, indem Sie Antivirus und Anti-IM-Spam, Authentifizierung und Benutzer-management, Logen und Archivieren von Session, sowie Erkennung und Nutzungsauswertung hinzufügen. All dies hilft Ihnen dabei, die Produktivität zu erhöhen, die mögliche Haftung zu verringern, die Nutzung der IT-Ressourcen zu optimieren und die Sicherheit im ganzen Netzwerk zu erweitern.

Merkmale

Verwaltung von IM- und P2P-Anwendungen
- Unterstützt die meisten IM-Anwendungen, P2P-Anwendungen und IM-Aktionen
- Blockiert Viren über IM und SPIM
- Verhindert den Missbrauch von IM- und P2P-Anwendungen
- Schützt vor Informationslecks

Bandbreiten-Management
- Kontrolle von Dateiübertragungen per http
- Kontrolle von Streaming Media per http
- Kontrolle von privaten Emails
- Kontrolle der Internet-Nutzung
- Bandbreiten-Management (QoS)

Verhinderung von „bösartigem" Datenverkehr
- Identifiziert/vernichtet Viren und Schadprogramme
- Erkennt befallene/infizierte Computer
- Zone-Defense Mechanismus* für Quarantäne von befallenen Computern und Schutz vor der Ausbreitung von Schadprogrammen

Überwachung des Datenverkehrs/Berichte
- Überwachung des Datenverkehrs in Echtzeit
- Mehrschichtige TOP N-Berichte

Hardware
- Hardware-basierte Nutzlastüberwachung
- Hardware-Bypass für maximale Betriebszeit
- 1 Ethernet-WAN-Port, 1 Ethernet-LAN-Port
- Anzeige/Tasten für Status und Überwachung

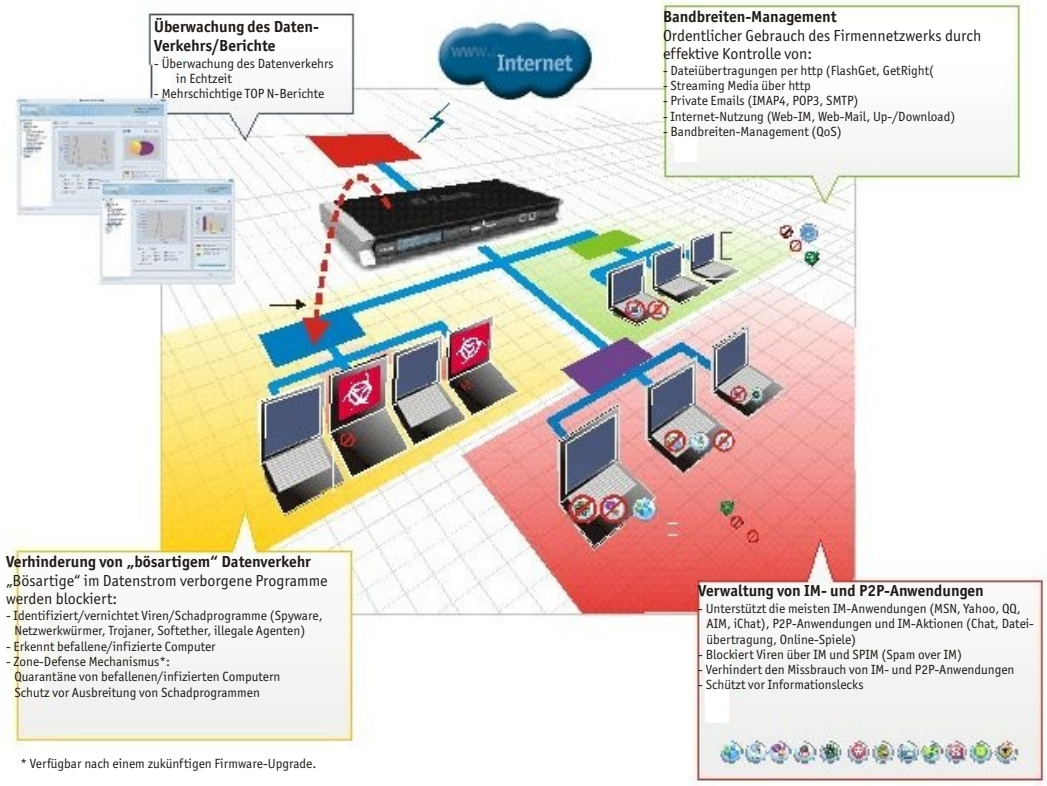
*Verfügbar nach einem zukünftigen Firmware-Upgrade.

D NETDEFEND

NETDEFEND

Vorderseite: LCD und Tasten zur Umschaltung zwischen Status- und Monitoring-Anzeige.

Die Konsolen-Schnittstelle ist hinter einer Klappe verborgen.



* Verfügbar nach einem zukünftigen Firmware-Upgrade.

DFL-M510

Information Security Gateway

NetDefend

Funktionen und Vorteile

Real Transparent Mode Implementation
- Einfache Installation ohne Änderung an der bestehenden Architektur
- Interoperabilität mit Netzwerkgeräten anderer Hersteller

Granulares Management für Gruppen, Hostnamen, IP-Adressen und Subnetze
- durchlässige Kontrolle von IM, P2P, Streaming Media, Datenübertragung und privaten Mails
- Diskrete Kontrolle der Internet-Aktivitäten, basierend auf Regeln für Gruppen, Hostnamen, IP-Adressen und Subnetzen

Durchlässiges Blockieren von Trojanern, Spyware, illegalen Agenten (Softether) und Netzwerkwürmern
- Verhindert die Ausbreitung von Schädlingen im Netzwerk

Identifizierung der Opfer
- Isoliert Problemstellen zum Troubleshooting

Hardware-basierter Bypass
- Keine Einzelausfälle
- Maximale Netzwerk-Konnektivität im Falle eines Hardware-Ausfalls

Logs/Analysen
- Leicht lesbare Berichte im HTML-Format ausdruckbar

Hardware-basierte Nutzlastüberwachung (Layer 7)
- Schnellste Verarbeitung durch ASIC Content-Processing-Chip

DOS/DDOS, Stealth-Modus
- Schutz vor verschiedenen Arten von DOS/DDOS-Angriffen
- Keine Antwort auf ICMP-Pakete im Stealth-Modus

Zusammenfassung der Hauptfunktionen

IM-/P2P-Management
- Kontrolle/Management von:
  - IM-Anwendungen
  - P2P-Anwendungen
- Regeln basierend auf Gruppen, Host-Namen, IP-Adresse oder Subnetzen

Anwendungsmanagement (Layer 7)
- Kontrolle/Management von:
  - Dateiübertragungen
  - Streaming Media
  - Web-Anwendungen
  - privaten Emails
- Benutzerdefinierte Kontrolle von Anwendungen

Verhinderung von „bösartigem" Datenverkehr
- Erkennung/Blockade von Schadprogrammen, wie Spyware, Softether, Netzwerkwürmen
- Identifizierung der befallenen Rechner
- D-Link Zone-Defense-Mechanismus* schützt vor der Ausverbreitung von Schadprogrammen im Netzwerk

Überwachung des Datenverkehrs/Berichte
- Überwachung des Datenverkehrs in Echtzeit
- Mehrschichtige TOP N-Berichte

* Nach einem zukünftigen Firmware-Upgrade verfügbar.

Installation und Einrichtung
- Plug-and-play-Installation ohne Änderungen am Netzwerk
- Transparent in-line mode, nahtlose Integration mit Netzwerkgeräten anderer Hersteller
- Java-basierter Einrichtungsassistent
- Hardware-basierter Bypass für maximale Netzwerk-Konnektivität
- Stealth-Modus für Schnittstellen

Technische Daten

Stromversorgung
- Internes Netzteil

Abmessungen
- 440 x 250 x 44 mm,
- 1HE, 19-Inch-Standard für Rack

Relative Luftfeuchtigkeit
- 5% bis 95% nicht kondensierend

Betriebstemperatur: 0° bis 60°C

Lagertemperatur: -20° bis 70°

Emission (EMV)
- FCC Class A
- CE Class A
- C-Tick

Sicherheit
- UL/CUL
- LVD (En60950)

Bestellinformationen

DFL-M510

Februar 2007