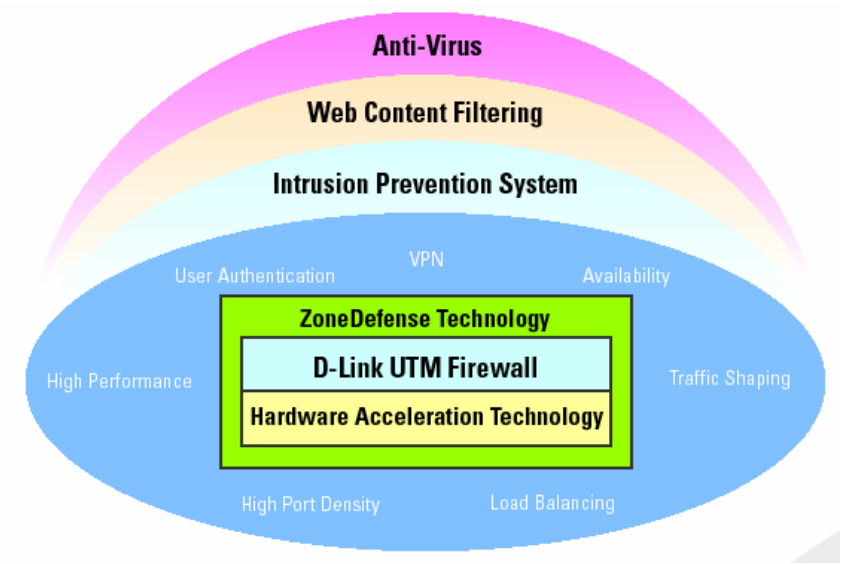
Merkmale

- Echtzeit AntiVirus Gateway Inspection (AV)
- Professionelles Intrusion Prevention System (IPS)
- Automatische Signaturen-Updates
- Zero Day Schutz vor Angriffen
- Web Surfing Management (WCF)
- Geringe Lizenzgebühren durch Wartungskosten je Firewall nicht je Nutzer

NetDefend Firewall UTM Dienste

Unified Threat Management (UTM)

D-Link's NetDefend UTM Firewalls (DFL-260/860) verfügen über ein Intrusion Prevention System (IPS), Gateway Anti-Virus (AV) sowie Web Content Filtering und bieten so einen umfassenden Schutz durch Layer 7 Überprüfung der Inhalte. D-Link's Firewalls nutzen ferner einen Hardware-Accelerator um den IPS und AV Durchsatz zu erhöhen, sowie eine Datenbank mit Millionen von URLs zur Überwachung der Internetnutzung via WCF. Echtzeit-Updates für IPS, AV sowie die URL Datenbank schützen Ihr Netzwerk vor Spionage-Anwendungen, Würmern, und schädlichen Codes, und bieten Ihnen ferner eine Vielzahl von Möglichkeiten zur Überwachung der Internetnutzung Ihrer Mitarbeiter. Um einen sichern Schutz vor Angriffen aus dem Internet zu bieten müssen alle drei vom DFL-260 und DFL-860 unterstützen Datenbanken auf dem aktuellsten Stand gehalten werden. Um eben diesen beständigen Schutz zu gewährleisten, bietet D-Link optionale NetDefend Firewall UTM Dienst Abos, die ausgewählte NetDefend Service Updates für alle Sicherheitsaspekte beinhalten: IPS, Anti-Virus und WCF. NetDefend UTM Abos stellen sicher, dass die Firewall Datenbanken aktuell und auf dem neuesten Stand sind.



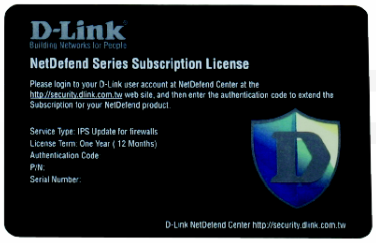
NetDefend Intrusion Prevention System (IPS) Abo

D-Link's IPS Dienste nutzen eine einzigartige Technologie – komponenten-basierte Signaturen erkennen und schützen vor einer Vielzahl von bekannten und unbekannten Angriffen und gehen ferner auf alle kritischen Aspekte eines potenziellen oder tatsächlichen Angriffs wie beispielsweise Payload, NOP sled, Infektion und Exploits ein. Für eine exakte und umfassende Erfassung der Signaturen beinhaltet die IPS

NetDefend Firewall UTM Services

Merkmale

- Fokus auf angreifende Lasten
- IM und P2P Management
- Zero Day Schutz vor Angriffen
- Automatische Signaturen-Updates
- Umfassende IP Signaturen-Datenbank
- Vollständige IPS Signaturen Warnungen



Datenbank Angriff-Informationen aus einem globalen Sensor-Grid, zusammengestellt aus öffentlichen Seiten wie beispielsweise der National Vulnerability Database und Bugtrax.
D-Link legt großen Wert auf qualitativ hochwertige IPS Signaturen und optimieret deshalb die NetDefend Signaturen laufend über das D-Link Auto-Signature Sensor System. Ohne bestehende Sicherheits-Anwendungen zu überfordern, gewährleisten diese Signaturen eine hohe Zahl an Entdeckungen bei einer sehr geringen Zahl an Fehlerzahl.

My D-Link

My D-Link ist eine Plattform zur Registrierung und Verwaltung und allen D-Link Kunden zugänglich. Um IPS Updates vom NetDefend Center auf My D-Link zu erhalten müssen D-Link Kunden Ihre Firewall hier registrieren. Der Status der registrierten Produkte unter Angabe von Produktname, MAC Adresse, Seriennummer, Registrierungsdatum, und Ablaufdatum des IPS Dienstes kann hier angezeigt werden. Auf diese Weise können Kunden spielend den Überblick über Ihre registrierten Firewalls behalten.

NetDefend Live

Zusätzlich bieten wir unseren Kunden über das NetDefend Center einen 'NetDefend Live' Service an. Die NetDefend Live Plattform stellt Informationen über etwaige Sicherheitslücken, sowie ähnliche Hinweise oder Warnungen bereit. Erkennt das D-Link Sicherheits-Center neue Exploits oder veröffentlicht es neue Signaturen, werden die entsprechenden Sicherheitshinweise zeitgleich aktualisiert. Diese Updates erfolgen 24 Std. am Tag, 7 Tage die Woche und 365 Tage im Jahr. Ziel von NetDefend Live ist es, unseren Kunden ein besseres Verständnis neuer Signaturen und Schwächen zu vermitteln. Die IT Abteilung hingegen kann auf NetDefend Live zurückgreifen um Gefahren und Schwächen im Unternehmen aufzuspüren ehe diese ausgenutzt werden. Mit der NetDefend Firewall als ersten Schutzwall, und D-Link NetDefend Live, als nachgelagertem Schutz, ermöglicht es D-Link seinen Kunden drohenden Gefahren zu begegnen, noch bevor sie dem Unternehmen schaden.

Merkmale und Funktionen

- **Augenmerk auf Attack payload und nicht Angreifern oder IP Adressen**

Die IPS Scan Engine umfasst eine tiefgreifende Layer 2 bis Layer 7 Überprüfung des Datenverkehrs, und schützt so sowohl vor positiven als auch negativen Fehlerkennungen und bietet so einen exakten Schutz vor einer Vielzahl von Gefahren innerhalb eines Netzwerks.

- **IM und P2P Management**

D-Link's IPS Dienst bietet Signaturen zur Verwaltung von Instant Messaging (IM) und Peer-to-Peer (P2P) Programmen, um so eine Überwachung der IM oder P2P Anwendungen in Ihrem Netzwerk zu ermöglichen.

- **Zero Day Schutz vor Angriffen**

IPS erkennt Abwandlungen von Angriffen oder schädlichen Codes, und kann so die Verbreitung dieser Bedrohung auch ohne Erstellung unnötiger Signaturen verhindern und dabei dennoch Zero Day Schutz bieten.

- **Automatische Signaturen-Updates**

Alle IPS Signaturen werden laufend und automatisch über die weltweiten D-Link Update-Server aktualisiert. Dieser Service hält Ihre Signaturen-Datenbank so aktuell wie möglich.

- **Umfassende IPS Signaturen Datenbank**

Schützen Sie Ihr Netzwerk gegen Netzwerkangriffen mit über 1800 Signaturen sowie der Überprüfung der Protokolle auf Unregelmäßigkeiten.

- **Umfassende IPS Signaturen-Hinweise**

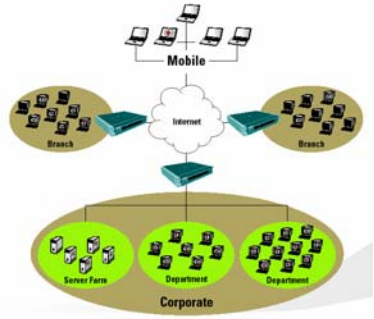
NetDefend Firewall UTM Services

Vollständige IPS Protokolle unter Angabe einer Kennung der Schwachstelle, Schweregrad, Beschreibung des Angriffs, sowie Wiederherstellungsmöglichkeiten erlauben es der IT Abteilung schnell von Angriffen zu erfahren und auf diese zu reagieren.

NetDefend Firewall UTM Services

Merkmale

- Aktuellster Schutz
- Hochleistungs-AV-Engine
- Streaming-basierte Musterzuordnung
- Schnelle Reaktionszeiten
- Umfassende Signaturen-Datenbank
- Vollständige AntiViren Warnungen



NetDefend Anti-Virus (AV) Abo

Mittels einer stream-basierten Viren-Scan Technologie überprüfen die NetDefend UTM Firewalls Dateien jeder Größe, ganz ohne Cachen. Diese Methode erhöht die Leistung während der Überprüfung und beseitigt gleichzeitig Engpässe im Netzwerk. Die Firewalls bedienen sich Virensignaturen des bekannten und renommierten Antiviren-Unternehmens Kaspersky Labs um Anwendern sowohl zuverlässige und exakte Virensignaturen, als auch aktuelle Signaturenupdates zu liefern. Durch die Nutzung der integrierten Hochleistungs-AV Engine und der stream-basierten Viren-Scan Technologie können die NetDefend UTM Firewalls Viren und schädliche Software konsequent und effektiv blockieren noch bevor sie Computer oder mobile Geräte im Netzwerk erreichen. Die NetDefend Firewalls ermöglichen die Einrichtung eines sicheren Netzwerkes für jede Unternehmensgröße.

Merkmale und Funktionen

- **Aktuellster Schutz**

Kaspersky Labs, Marktführer im Bereich AV Signaturen, reagiert umgehend auf die gefährlichsten Viren, Trojaner, Würmer und Spionageprogramme. D-Link's Firewall AV Schutz verlässt sich deshalb auf Kaspersky Labs.

- **Optimierte Leistung**

D-Link's AntiVirus Lösung verfügt über eine integrierte Hochleistungs-AV-Engine die es den D-Link's UTM Firewalls ermöglicht einen sehr weitaus höheren Durchsatz zu erreichen als andere am Markt verfügbare Antivirus-fähige UTM Firewalls.

- **Streaming-basierte Musterzuordnung**

Die streaming-basierte Scan-Engine überprüft alle Lasten und ordnet je Paket Signaturen zu. Der dateibasierte AV-Schutz hat keinerlei Schwierigkeiten mit der Größe der Dateien, da die D-Link Firewalls nicht die ganze Datei zur Überprüfung abspeichern.

- **Schnelle Reaktionszeiten**

Alle Virensignaturen werden stündlich aktualisiert und weltweit von D-Link Servern bereitgestellt. Die Herausgabe von Notfall-Viren-Signaturen schützt auch vor den neuesten und gefährlichsten Virenvarianten.

- **Umfassende Signaturen-Datenbank**

NetDefend's proaktive Signaturen-Datenbank umfasst etwa 2000 Signaturen wie z.B. alle Wild List Gefahren sowie tausende bekannte OS Exploits und Schwachstellen verschiedener Anwendungen und schützt Ihre Systeme so vor Würmern, Trojanern oder Spionageprogrammen.

- **Vollständige AntiViren Signaturen Hinweise**

Völlständige AntiViren Protokolle unter Angabe von Ausstellungsdatum, Verhalten und technischen Details ermöglichen es Mitarbeitern der IT Abteilung schnell von Angriffen zu erfahren und auf diese zu reagieren.

NetDefend Web Content Filtering (WCF) Abo

Merkmale

- Enorme Kosteneinspar-potenziale
- Globale Index-Server
- Hohe Integrität mit anderen D-Link Security Gateway Subsystemen
- Statische weiße und schwarze Listen
- Active Content Handling
- Kostengünstiges Web Content Filtering

Die Überwachung der Internetnutzung gewinnt für Unternehmen jeder Größe zunehmend an Bedeutung. D-Link's Web Content Filtering (WCF) Service verschärft die Zugangskontrolle und Verwaltungsregelungen Ihres Unternehmens insbesondere im Hinblick auf die Zuweisung von Internetressourcen. Web Content Filtering unterstützt IT Abteilung dabei, das Internet-Nutzungsverhalten sowie den Mitarbeiter-Zugriff zu verwalten, zu überwachen und zu kontrollieren. Auf diese Weise gewinnt die Unternehmensleitung an Kontrolle und die teilweise knappen Internetressourcen können unternehmensbezogen und Kosten-orientiert eingesetzt werden.

Enorme Kosteneinsparpotenziale durch:

- **Reduzierung der Arbeitszeit** durch das Verhindern unangemessener Internetnutzung
- **Reduzierung der Internetkosten** und Bandbreiteneinsparungen durch die Einschränkung und Überwachung privater Internetnutzung, und somit Verbesserung der Netzwerkreaktionszeiten
- **Reduzierung der rechtlichen Angreifbarkeit** am Arbeitsplatz und Haftbarkeit (z.B. Sexuelle Belästigung, Kinderpornographie und die negativen Schlagzeilen die diese Vorfälle mit sich bringen)
- **Reduzierung der Kosten zur Wiederherstellung des Systems nach Angriffen** da viel weniger schädliche Inhalte in das Netzwerk eindringen können.

Merkmale und Funktionen

- **Globale Index-Server**

Globale Index-Server halten Datenbanken mit Millionen URLs bereit und sammeln Echtzeit-Informationen über die neuesten Webseiten so dass diese stets auf dem aktuellen Stand gehalten werden können. Weltweit verbessern eine Vielzahl von Servern die Leistung und optimieren die Verfügbarkeit des Dienstes wo auch immer eine D-Link Firewall eingesetzt wird.

- **Optimierte Leistung**

D-Link implementiert eine Vielzahl von Index-Servern um so die Leistungskapazitäten und Verfügbarkeit des Dienstes zu verbessern. Kategorien der Webseiten auf die zuletzt zugegriffen wurde werden lokal in jeder UTM Firewall gecacht um so die Leistung bei nachfolgenden Anfragen zu verbessern.

- **Hohe Integrität mit anderen D-Link Security Gateway Subsystemen**

D-Link ermöglicht es Ihnen extreme genaue Regelungen über die Erlaubnis oder Verwehrung des Zugriffs auf bestimmte Webseiten zu formulieren. Für verschiedene Nutzer, Schnittstellen und IP Netzwerke können verschiedene Regelungen formuliert und angewendet werden.

- **Statische weiße und schwarze Listen**

Definieren Sie Webseiten die ausdrücklich erlaubt oder geblockt werden ganz unabhängig von Ihrer Klassifizierung. NetDefend UTM Firewalls verfügen über 32 verschiedene Klassifikationen und erlauben es Netzwerkadministratoren so, dass Internetnutzungsverhalten zu überwachen.

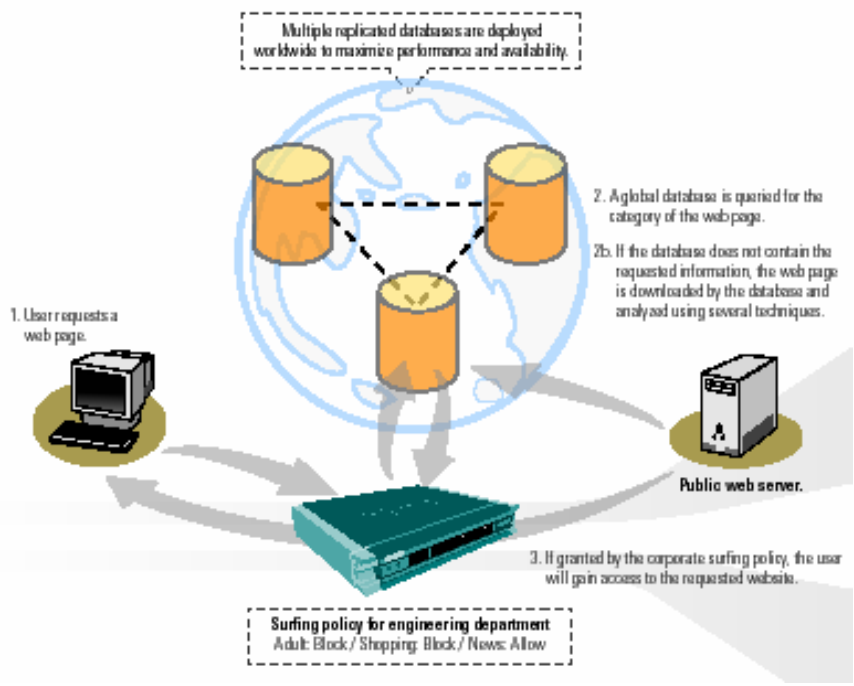
- **Active Content Handling**

Auf diese Weise können potenziell gefährliche Objekte, wie Java applets, JavaSkripts/VBSkripts, ActiveX Objekte und Cookies entfernt werden um Inhalte aus

dem Internet zu verwalten.

- **Kostengünstiges Web Content Filtering**

D-Link's WCF Service wird je Firewall und nicht je Nutzer abgerechnet, so dass bei großen Unternehmen keine enormen Lizenzgebühren entstehen um die Internetnutzung Ihrer Mitarbeiter zu verwalten. Ein einziges Abo kann so das Internetnutzungsverhalten des gesamten Unternehmens überwachen und verwalten.



August 2007