D-Link®

Product Highlights

Intrusion Prevention System
Detects and prevents known and unknown attacks/exploits/vulnerabilities, preventing outbreaks and keeping your network safe.

Gateway Anti Virus Protection
Detects and blocks malicious files at the gateway providing a 1st line of defense for your network.

Web Content Filtering
Blocks access to websites by category allowing you to restrict inappropriate content in the workplace and keep your staff more productive.

NetDefend Firewall UTM Services

Features

• Professional Intrusion Prevention System (IPS)
• Automatic Signature Update
• Zero Day Attack Protection
• Real-Time AntiVirus Gateway Inspection (AV)
• Web Content Filtering (WCF)
• Low Cost Licensing, using Per-Firewall Service Maintenance

Unified Threat Management

D-Link NetDefend UTM firewalls integrate an Intrusion Prevention System (IPS), gateway AntiVirus (AV), and Web Content Filtering (WCF) for superior layer 7 content inspection protection. The real-time update service keeps the IPS information, antivirus signatures, and URL databases current. Combined, these enhancements help to protect office networks from application exploits, network worms, malicious code attacks, and provide everything a business needs to safely manage employee Internet access. Maintaining an effective defense against the various threats originating from the Internet requires that all three databases used by the UTM firewall are kept up-to-date. In order to provide a robust defense, D-Link offers NetDefend Firewall UTM Services which include distinct NetDefend service updates for each aspect of your defenses: IPS, AV, and WCF. NetDefend Firewall UTM Services ensure that each of your UTM firewall’s service databases is always accurate and current. In addition to other fundamental wireless security features including WEP, WPA Personal/Enterprise, WPA2 Personal/Enterprise, and MAC Authentication to determine the identity of wireless devices, the HTTP Authentication feature allows you to block clients from accessing the network until the clients verify their identities. This double-layer authentication and authorization provides a robust security fence to also protect against attacks from within the network.
My D-Link
My D-Link provides a registration and management platform for all D-Link customers. D-Link customers need to register their firewall to initiate the IPS update service from the NetDefend Center’s My D-Link Portal. The current status of all registered products will be presented, including model names, MAC addresses, serial numbers, registration dates, and IPS service expiration dates, making it easy for customers to maintain all of their D-Link firewalls.

NetDefend Live
The NetDefend Center includes a ‘NetDefend Live’ service for our customers. NetDefend Live is a platform for providing information about potential security breaches and associated advisories. When D-Link Security Center discovers new exploits and releases new signatures, associated security advisories will be simultaneously updated, 24x7x365. The main purpose of NetDefend Live is to help our customers know more about new signatures and vulnerabilities. IT staff can use NetDefend Live as reference to uproot threats and patch vulnerabilities within the enterprise before they are exploited. With NetDefend firewalls as the first line of defense and NetDefend Live as the second, D-Link helps customers to counteract emerging network threats promptly, before they have an impact on business operations.

NetDefend Intrusion Prevention System (IPS) Subscription
D-Link’s IPS service adopts a unique technology, component-based signatures, which are built to recognize and protect against all varieties of known and unknown attacks, and which address all critical aspects of an attack or potential attack including payload, NOP sled, infection, and exploits. In terms of signature coverage, the IPS database includes attack information and data from a global attack sensor-grid and exploits collected from public sites such as the National Vulnerability Database and Bugtrax.

D-Link is committed to delivering high quality IPS signatures by constantly creating and optimizing NetDefend signatures via the D-Link Auto-Signature Sensor System. Without overloading existing security appliances, D-Link IPS signatures ensure a high ratio of detection accuracy and the lowest ratio of false positives.
Focus on Attack Payload, not Attackers or IP Addresses
The IPS scan engine is an in-depth inspection of data from Layer 2 to Layer 7 protecting against both false positives and false negatives and preventing various types of network-based threats with a high degree of accuracy.

Zero Day Attack Protection
IPS captures variations of attacks and stealthy malicious traffic to prevent outbreaks of these threats without creating unnecessary new signatures, while still protecting against Zero-Day attacks.

Continuous Automatic Signature Updates
All IPS signatures are continuously updated automatically and made available through D-Link update servers worldwide. The service keeps your IPS signature database as current as possible.

Comprehensive IPS Signature Database
Protect the system against network attacks using over 17,000 signatures as well as protocol anomaly inspection.

Complete IPS Signature Advisory
Complete IPS logs with vulnerability ID numbers, severity levels, attack descriptions, and recovery solutions enable IT personnel to know about and respond quickly to network attacks.

NetDefend Anti-Virus (AV) Subscription
NetDefend UTM firewalls implement stream-based virus scanning technology without first caching incoming files, thus increasing inspection performance and easing network bottleneck nightmares while enabling powerful virus defense capabilities.

D-Link's firewalls use virus signatures from Kaspersky Labs, a reputable name in Antivirus, to provide our customers with prompt signature updates and reliable, accurate antivirus signatures.

Using a stream-based virus scanning technology, NetDefend UTM firewalls block viruses and malware before they ever reach the desktops or mobile device on your network. NetDefend firewalls create a safer network environment for companies of all sizes, from SMBs to enterprises.

Up-to-date Protection
D-Link firewall AV defenses rely on Kasperky Labs. Kaspersky Labs is the market leader in AV signature creation, providing the fastest response to the most dangerous viruses, Trojans, worms, and spyware programs.

Streaming-based Pattern Matching
A streaming-based scan engine inspects all payloads and matches the signature packet-by-packet. File-based AV protection will never encounter a file-size limitation since D-Link firewalls do not need to store whole files in memory for inspection purposes.

Fast Response Time
All AntiVirus signatures are updated hourly and made available through D-Link update servers worldwide. Emergency signature releases protect against the latest, most virulent virus variations.

Comprehensive AntiVirus Signature Database
NetDefend's proactive signature database protects each system against network worms, Trojans, and spyware with signatures covering all Wild List threats and thousands of well-known OS exploits and application vulnerabilities.

Complete AntiVirus Signature Advisory
Complete antivirus logs with issue dates, behavior and technical details allow IT personnel to become aware of and immediately respond to virus threats and infections.
NetDefend Firewall UTM Services

NetDefend Web Content Filtering (WCF) Subscription

Web surfing control is becoming a critical concern for businesses of all sizes. D-Link’s Web Content Filtering (WCF) service enforces access protection and management policy for Internet usage. NetDefend Web Content Filtering helps IT staff monitor, manage, and control employee usage of and access to the Internet. It puts Management back in control, enabling a more business-orientated and cost effective use of Internet resources.

Organizations experience significant cost savings through:

1) A reduction in wasted staff time by reducing inappropriate web surfing.
2) Reduced Internet access costs and bandwidth savings by limiting and controlling non-business related uses, thus improving network response.
3) Reducing legal exposure to workplace conflicts and liabilities (e.g. sexual harassment cases or pornography and the adverse publicity that such incidents can generate).
4) Reduced costs in recovering from attacks as much less inappropriate content will even be allowed to enter the network.

Global Index Servers

Global index servers maintain databases of millions of URLs and collect real-time website information in order to keep the data as current as possible. Multiple servers worldwide enhance performance and maximize service availability wherever a NetDefend firewall is installed.

Performance Optimized

D-Link implements multiple index servers to enhance performance capacity and maximize service availability. Categories of recently visited websites are cached locally in each UTM firewall to maximize performance for subsequent requests.

Tight Integration with other D-Link Security Gateway Subsystems

D-Link allows you to define highly-granular policies for allowing or disallowing where and when access to certain types of websites is permitted, and different policies can be applied to any combination of users, interfaces, and IP networks.

Static White and Black Lists

Define websites that will be explicitly allowed or blocked, independent of their classification. There are 32 default classification groups in NetDefend UTM firewalls to allow network administrators to control Internet usage.

Active Content Handling

The WCF capabilities of D-Link UTM firewalls can strip potential malicious objects, such as Java applets, JavaScripts / VBScripts, ActiveX objects and cookies, all of which are popular methods for hacker attacks.

Cost-Effective Web Content Filtering

D-Link’s WCF service is priced per firewall instead of per user, so an enterprise-level organization does not need to contemplate a large TCO for licensing in order to manage the surfing privileges of all employees. One subscription can provide web surfing control for an entire organization.
NetDefend Firewall UTM Services

D-Link UTM firewalls are shipped with a 90 day Intrusion Prevention System (IPS), AntiVirus (AV), and Web Content Filtering (WCF) subscription - free of charge. Upon expiration of these free subscription services, you can extend your subscriptions by purchasing NetDefend UTM subscriptions for specific services. Contact your D-Link reseller for details.

**Subscription Service Ordering Information:**

<table>
<thead>
<tr>
<th>Product Number</th>
<th>Product Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFL-260-IPS-12</td>
<td>12-month IPS update service for DFL-260/DFL-260E firewalls</td>
</tr>
<tr>
<td>DFL-260-AV-12</td>
<td>12-month Anti-Virus update service for DFL-260/DFL-260E firewalls</td>
</tr>
<tr>
<td>DFL-260-WCF-12</td>
<td>12-month Web Content Filtering service for DFL-260/DFL-260E firewalls</td>
</tr>
<tr>
<td>DFL-860-IPS-12</td>
<td>12-month IPS update service for DFL-860/DFL-860E firewalls</td>
</tr>
<tr>
<td>DFL-860-AV-12</td>
<td>12-month Anti-Virus update service for DFL-860/DFL-860E firewalls</td>
</tr>
<tr>
<td>DFL-860-WCF-12</td>
<td>12-month Web Content Filtering service for DFL-860/DFL-860E firewalls</td>
</tr>
<tr>
<td>DFL-1660-IPS-12</td>
<td>12-month IPS update service for DFL-1660 firewall</td>
</tr>
<tr>
<td>DFL-1660-AV-12</td>
<td>12-month Anti-Virus update service for DFL-1660 firewall</td>
</tr>
<tr>
<td>DFL-1660-WCF-12</td>
<td>12-month Web Content Filtering service for DFL-1660 firewall</td>
</tr>
<tr>
<td>DFL-2560-IPS-12</td>
<td>12-month IPS update service for DFL-2560/2560G firewalls</td>
</tr>
<tr>
<td>DFL-2560-AV-12</td>
<td>12-month Anti-Virus update service for DFL-2560/2560G firewalls</td>
</tr>
<tr>
<td>DFL-2560-WCF-12</td>
<td>12-month Web Content Filtering service for DFL-2560/2560G firewalls</td>
</tr>
</tbody>
</table>