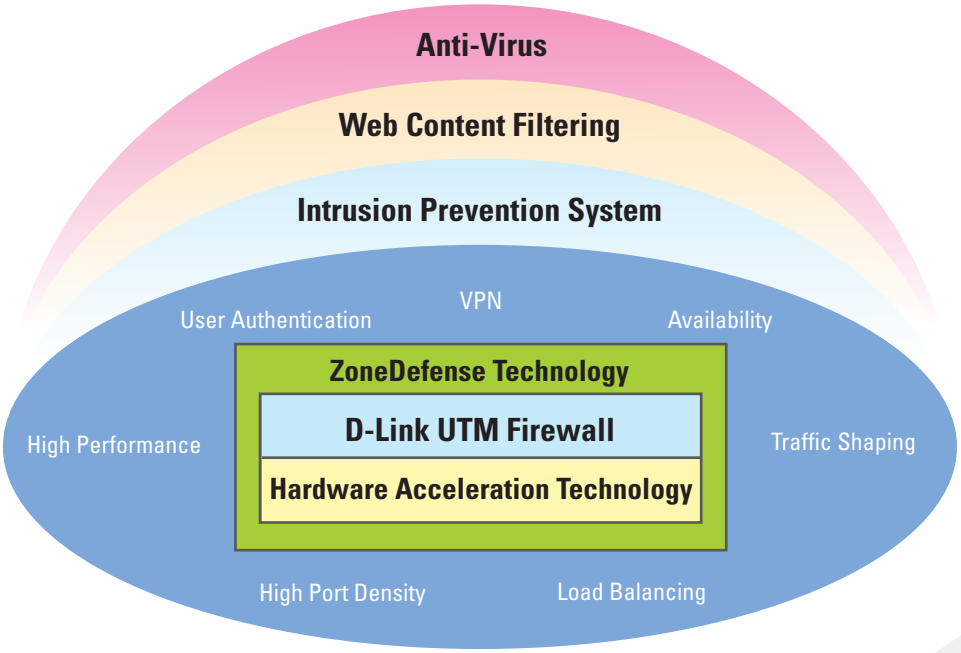
NetDefend Firewall UTM Services

Unified Threat Management –

D-Link NetDefend UTM firewalls (DFL-260/860) integrate an Intrusion Prevention System (IPS), gateway AntiVirus (AV), and Web Content Filtering (WCF) for superior Layer 7 content inspection protection. D-Link firewalls also use a hardware accelerator approach to increase IPS and AV throughput, and a web surfing control database containing millions of URLs for WCF. IPS, AntiVirus and URL database real-time update services protect your enterprise network from application exploits, network worms, malicious code attacks, and provide everything you need to manage employee Internet access behavior. 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, AntiVirus, and WCF. NetDefend Firewall UTM Services ensure that each of your UTM firewall's service databases is always accurate and current.



Each Device Features:

- Real-Time AntiVirus Gateway Inspection (AV)
- Professional Intrusion Prevention System (IPS)
- Automatic Signature Update
- Zero Day Attack Protection
- Web Surfing Management (WCF)
- Low Cost Licensing Using Per-Firewall Service Maintenance

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 deliver 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.

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 receive IPS update service from the NetDefend Center's My D-Link. The current status of all registered products will be presented, including Model Names, MAC addresses, Serial Numbers, Registration dates, and IPS Service Expiration dates. Customers can easily maintain all firewalls registered under My D-Link.

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. This update frequency is provided on a 7x24x365 basis. The main purpose of NetDefend Live is to help our customers know more about new signatures and vulnerabilities. MIS departments 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.

Features and Benefits

- **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.

- **IM and P2P Management**

D-Link's IPS service provides signatures to manage Instant Messaging (IM) and Peer-to-Peer (P2P) applications, so that you control what IM and P2P applications are blocked or allowed in your network.

- **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**

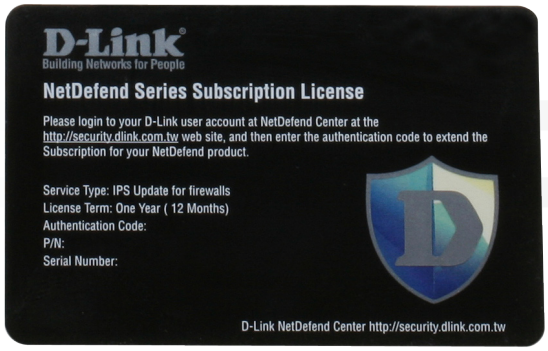
All IPS signatures are continuously updated automatically and made available through D-Link update servers worldwide. The service keeps your IPS signature database as current as possible at the outside of new threats.

- **Comprehensive IPS Signature Database**

Protect the system against network attacks using over 1,800 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 MIS personnel to know about and respond quickly to network attacks.



NetDefend AntiVirus (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 the known, respected antivirus company Kaspersky Labs to provide our customers with prompt signature updates and reliable, accurate antivirus signatures.

Using a built-in extreme-performance AV acceleration engine together with stream-based virus scanning technology, NetDefend UTM firewalls block viruses and malware before they ever reach your network's desktops or mobile devices. NetDefend firewalls create a safer network environment for companies of all sizes, from SMBs to enterprises.

Features and Benefits

- **Up-to-date Protection**

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

- **Performance Optimized**

D-Link's AntiVirus solution has a built-in extreme-performance AV acceleration engine that allows D-Link's UTM firewalls to perform with a much higher throughput than other antivirus-capable UTM firewalls on the market.

- **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**

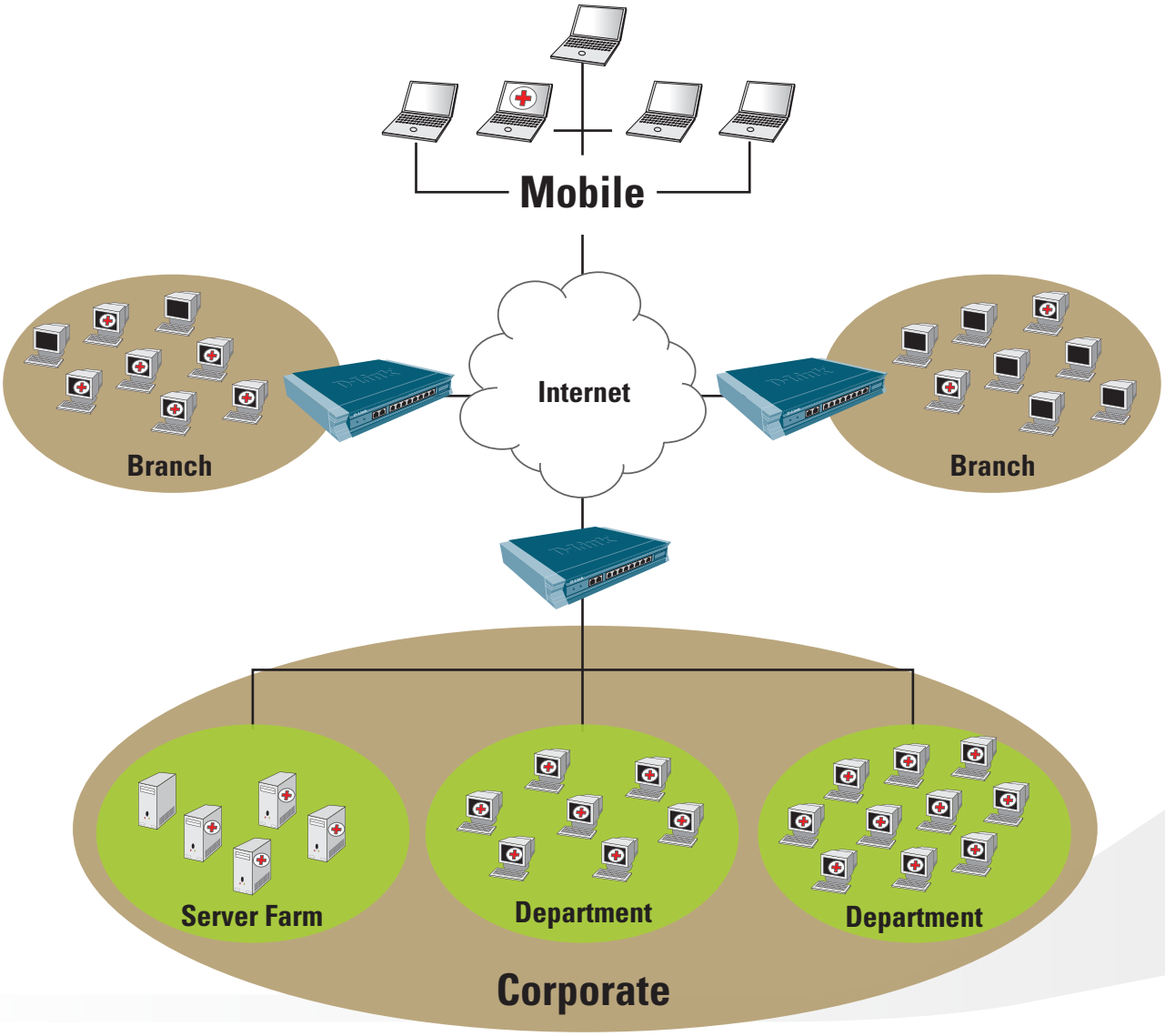
All AntiVirus signatures are updated hourly and made available through D-Link update servers worldwide, and emergency signature releases protect against the latest, most virulent virus variations.

- **Comprehensive AntiVirus Signature Database**

NetDefend's proactive signature database protects each system against network worms, Trojans, and spyware with over 2,000 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 enable MIS personnel to know about and then respond immediately to virus threats and infections.



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 in terms of Internet resource allocation for your organization.

NetDefend Web Content Filtering helps MIS 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 sometimes scarce Internet resources.

Organizations gain 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 child 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.

Features and Benefits

- **Global Index Servers**

Global index servers maintain databases of millions of URLs and collect real-time website information about the latest sites 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.