

# Firewall Security for SMB Networks

White Paper  
November, 2008

## Abstract

Every year billions of dollars and tens of thousands of productive hours are lost to network security breaches and malicious attacks. One of the critical lines of defense against such attacks is the firewall. Firewalls protect your business assets, intellectual property and sensitive information from outside attackers, malicious software, and intentional or unintentional internal security breaches. A firewall is a security system that protects computing resources from outside intrusions, online attackers, internal threats (inside the company network), and viruses, worms, and Trojan horses. More specifically, a firewall is a hardware or software device designed to permit, deny, encrypt, decrypt or proxy computer traffic between different security domains based upon a set of rules or policies. This white paper describes evolving firewall requirements, the technologies involved, and some specific D-Link® firewall solutions.

## Why Firewalls Are Important

Firewalls establish levels of trust to regulate the flow of digital traffic between computer networks. For example, the Internet is a low-trust zone, while an internal network is considered high trust. Intermediate trust zones – like those situated between the Internet and a trusted internal network – are often termed “perimeter networks.”

Generally, firewalls prevent the following:

- Attacks and intrusions – like hackers attempting to improperly access information resources from inside or outside the organization.
- Internet threats – like viruses, spyware and other types of malware. (For example, a user downloads a file or opens an email attachment from the Internet and introduces a threat to the network.)
- Security breaches – like incidents where boundaries are breached between switches and servers, between different departments, or between a Wi-Fi access point and the regular wired LAN. (For example, a user accesses data from a department they are not authorized to access.)

A comprehensive approach to security should consider complete firewall protection for both perimeter (e.g. LAN to WAN) and internal networks.

## How Firewalls Work – Summary

Firewalls manage access and trust between IT resources by comparing corporate policies about user network access rights to the connection information that transpires during individual access attempts. A firewall will not grant access to network resources unless the policies and connection information conform. This is the essential mechanism that prevents break-ins, inadvertent access and infiltration of malicious files.

There are a number of locations where firewalls traditionally reside. These include:

- Network perimeter, where the data center connects to the WAN and/or Internet.
- Between LAN switch ports and dedicated application servers (like email or financial/sales application servers)
- Between wired and wireless LANs (access points)
- Between departments, to police group policy and access rights
- Between a branch office and a WAN
- As software in laptops, smart phones or other devices used by mobile workers

## Firewall Vulnerabilities and New Security Demands

As computing demands increase and more people use networked resources to complete their work, shop for goods and services, and

entertain themselves, firewalls become much more critical. Mobile computing, virtual offices and remote access demands require that people connect into office resources from computers and devices outside the hardened network, for example. Venues include café hotspots, home offices, branch locations, customer sites and other similar locations.

Business computing resources connect to partner computers for collaboration, and many companies now use Web-based applications and eBusiness applications outside of their network. Some Web applications require access to sensitive data on the LAN, as well. The result is a hybrid internal/external application. Wireless LANs are also untrusted. Without the proper security measures in place, they can be penetrated and used as channels into the larger business network.

Regulatory mandates like Sarbanes-Oxley, Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard, require strict security auditing and tracking capabilities.

All these factors are driving the need for more robust, feature-rich firewalls.

## Firewall Technology

There are three distinct categories of firewalls:

1. Packet filter
2. Stateful Packet Inspection (SPI)
3. Application layer (or proxy-based firewall)

### Packet Filtering

Packet filters examine each header of every packet that moves across their domain. As a network layer (Layer 3) technology, they function efficiently yet fundamentally they have no concept of state. In other words, they treat each packet in isolation. This means a packet filter firewall cannot tell if a given packet is part of a trusted connection or a new, rogue connection. As a result, these kinds of older firewalls are subject to spoofing attacks and other exploits. Newer firewalls, like those described below, are connection-aware or state-aware. They allow network administrators to examine network traffic more closely.

### Stateful Packet Inspection (SPI)

Stateful firewalls maintain a data table of open connections. They intelligently associate new connection requests with existing legitimate connections by parsing this table. Only packets matching a known connection state are allowed by the firewall. All others are rejected. Effectively, SPI accepts incoming packets only if the packets were expected in response to a request that originated from the internal network, thus the “state”.

### Application Filtering

Application filtering takes SPI a step further. While SPI determines what type of protocol is being sent over each port, application-level filters examine what the protocol is being used for. The application filter can tell the difference between peer-to-peer file sharing and standard HTTP traffic, for example. A SPI firewall treats all HTTP traffic equally and cannot make this distinction.

Application filtering firewalls typically maintain multiple application proxies on a single firewall. Since these proxies sit between the client and server, the two end points never communicate directly. As a result, suspicious data can be dropped without incident. Also, since application filters are application-aware, they can handle complex teleconferencing and VoIP protocols like H.323.

## Typical Firewall Functions

### DMZ - (DeMilitarized Zone)

Firewalls establish a middle ground between trusted internal networks and untrusted external networks such as the Internet. Companies usually place their Web, email and authentication/policy servers in the DMZ. The area acts as a subnet between firewalls and systems. DMZs are also referred to as “perimeter networks.”

### Port Forwarding

This is the function that allows parties outside the corporate network to contact a user inside. A port is opened on the firewall to allow for a specific type of communication. A port opened for VoIP, for example, creates an easy two-way channel for calls initiated by someone inside or outside the network.

### Port Triggering

This is the function that opens specific ports based on specific trigger conditions. For example, predetermined ports might send inbound traffic to specific incoming ports when a client on the local network makes an outgoing connection to a predetermined port on a server. Security is enhanced because incoming ports are not open all the time. They are opened only when a program is actively using the trigger port. This is useful on NAT-enabled routers that provide services that require a static host (or unchanged network address). NAT is discussed in more detail below. This function is disadvantageous in that only one client at a time is allowed to use a particular service on a particular port.

### Virtual Private Network (VPN)

Most firewalls support VPN functionality, which encrypts data in transit to prevent theft, misuse or unauthorized access.

## Extended or Advanced Network Security Features

### Network Address Translation (NAT)

Many firewalls now feature Network Address Translation (NAT) to

hide addresses of protected resources from malicious intervention. This functionality establishes a “private address range,” which hides the true address of protected hosts. The feature is technically not considered a “firewall,” however it’s now quite common. NAT was originally developed to address the limited number of IPv4 routable addresses and reduce the costs associated with obtaining public addresses for every computer in a network.

### NAT Traversal

In certain situations some effects of the NAT function can be undesirable, however. NATs often block certain types of traffic that users and businesses want to utilize. For example, VoIP networks, P2P file sharing, and online services for video game consoles (like the Xbox 360’s Xbox Live or PS3’s PlayStation Network) require clients to act like servers. Since requests cannot be correlated to the proper internal host, this poses a problem for users behind NAT devices. The NAT device has no way of determining which internal host incoming packets should be routed to.

NAT traversal is the solution. This is the general term for various techniques that establish and maintain network connections that traverse NAT gateways. The problem is that most NAT techniques bypass enterprise security policies and break end-to-end transparency. Ideally, NAT traversal would cooperate with NAT and firewalls, allowing traversal while still enforcing enterprise security policies. Two IETF standards are addressing this issue - Realm-Specific IP (RSIP) and Middlebox Communications (MIDCOM).

## Other Technologies Associated with Network Security and Firewalls

### Unified Threat Management (UTM)

UTM describes a category of security devices that integrate multiple security features into a single appliance. They typically combine firewall, gateway, anti-virus, anti-malware, anti-spam, and intrusion detection and prevention capabilities into a single platform.

### Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

IPSs provide another layer of internal network security by detecting and blocking malicious traffic and suspicious traffic patterns. Firewalls are commonly offered in combination with IPSs.

### Access Control List (ACL)

An ACL is basically a table or data file that determines whether a user is granted access to a specific computer, network or application resource. It also contains information about what kinds of rights and privileges the user has with respect to the resource (e.g. read, write, execute, delete). An ACL for a network is similar to a firewall in that the data table specifies lists of ports and services available on a specific host. By assisting a switch in deciding whether to forward or filter packets, the list controls access to and from the network.

## D-Link Solutions

### ZoneDefense™

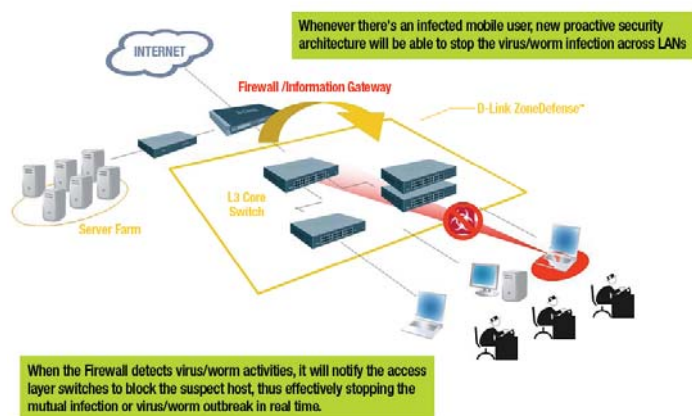
ZoneDefense by D-Link enables D-Link's NetDefend™ firewalls to integrate with D-Link's xStack® switches to construct a network security architecture that can effectively block any malicious host upon detection. Whenever a NetDefend firewall detects any abnormal network activity, ZoneDefense triggers immediately to disconnect the infected host from the network, not only stopping it at the firewall, but also at the very edge of the network. ZoneDefense is the technology to integrate the central NetDefend firewall and xStack switch at the edge.

ZoneDefense provides SMBs with a proactive network security that integrates network security appliance to automatically detect the network traffic. If the packet flow of a user computer triggers the conditions for ZoneDefense, a ZoneDefense command will immediately and automatically be sent to the specified network switch to block the network connection of the user computer instantaneously. For SMBs, this means ZoneDefense can greatly reduce the damages and losses caused by attacks from viruses and hackers, as well as effectively enhance network performance. For network administrators, this solution provides an easy and time-saving approach to locating infected computers. Once the computers are located, there is no need to manually issue system commands on network devices.

ZoneDefense, a sound solution with proactive security mechanism from D-link, is a true solution for SMBs to realize their defense-in-depth strategy. By collaborating D-Link NetDefend firewalls and xStack switches, your SMB network is secured at the edge against all varieties of network threats.

### Proactive Security Architecture

D-Link NetDefend firewalls along with D-Link xStack switches coordinate security policies between LANs, to create an effective ZoneDefense.



The diagram shows the benefits of ZoneDefense.

### D-Link DFL-1600 Rackmount VPN Firewall

The DFL-1600 is a powerful security solution that provides integrated Network Address Translation (NAT), SPI Firewall, advanced content filtering features, IDS protection, bandwidth management, OSPF routing as well as Virtual Private Network (VPN) support. The DFL-1600 includes 6 configurable gigabit Ethernet ports that can be used for LAN, WAN, or DMZ. The DFL-1600 scales up to 400,000 connections and supports 1200 VPN tunnels.

### D-Link DFL-800 Desktop VPN Firewall

The DFL-800 is a powerful security solution that provides integrated Network Address Translation (NAT), SPI Firewall, advanced content filtering features, IDS protection, bandwidth management, OSPF routing as well as Virtual Private Network (VPN) support. The DFL-800 hardware includes seven trusted LAN ports, dual-WAN ports for load balancing, and a user-configurable DMZ port to support local servers. The DFL-800 can manage up to 25,000 connections and up to 300 VPN tunnels.

### D-Link DFL-210 Network Security Firewall

The NetDefend family of Firewall/VPN Security Appliances is D-Link's answer for hardware-based network security. The new D-Link Network Security Firewall (DFL-210) is an easy-to-deploy VPN and firewall solution designed specifically for the Small Office / Home Office (SOHO) market that demands superior performance and security.

The DFL-210 is a powerful security solution that provides integrated Network Address Translation (NAT), SPI Firewall, advanced content filtering features, IDS protection, bandwidth management, as well as Virtual Private Network (VPN) support. The DFL-210 hardware includes four trusted LAN ports, a WAN port, and a user-configurable DMZ port to support local servers such as e-mail, Web, and FTP. The DMZ port can also be reconfigured as a WAN fail-over port. All of these features conveniently fit into a desktop chassis that can be easily integrated into your network.

To provide enterprise-class network security, the DFL-210 has several flexible firewall features to manage, monitor, and maintain a healthy and secure network. Network management features include: Remote Management, Bandwidth Control Policies, URL/Keyword Blocking, Access Policies, and SNMP. For network monitoring, the DFL-210 supports e-mail alerts, system log, consistency checks, and real-time statistics. These features along with a firmware backup function provide and maintain maximum network performance and security.