SonicWALL TZ 180 TotalSecure Administrator's Guide

Introduction

SonicWALL TZ 180 TotalSecure is included in SonicWALL's unified threat management solution that integrates Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service into an intelligent, real-time network security solution. This provides a comprehensive, yet layered approach to securing your network.

Document Scope

This document contains the following subsections:

What is TotalSecure?

SonicWALL® TotalSecure removes the complexity associated with choosing between a host of point products and add-on services by integrating everything you need in a convenient and affordable package. These all-in-one solutions combine a high-performance deep packet inspection firewall and dynamic security services to keep your network safe from viruses, spyware, worms, Trojans and more. Even before new threats are identified, TotalSecure solutions are automatically updated with signatures that stop attacks before they can enter your network, ensuring you have around-the-clock protection.

SonicWALL TotalSecure is included in SonicWALL's unified threat management solution that integrates Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service into an intelligent, real-time network security solution. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion

Prevention Service delivers unified threat management directly on the SonicWALL security appliance gateway.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interval enable administrators to configure a custom set of detection or prevention policies tailored to their specific network environment. Network administrators can create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.

Every SonicWALL TotalSecure solution includes the following:

- SonicWALL deep packet inspection network security appliance (wired and wireless options)
- Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service subscription (1 year)
- Content Filtering Service subscription – Standard Edition on TZ Series and Premium Edition on PRO Series (1 year)
- Dynamic Support 24x7 subscription (1 year)
- ViewPoint reporting software

Benefits of TotalSecure

Upgrading to SonicOS TZ 180 TotalSecure provides a variety of network security advantages:

- A **complete network security solution** integrates everything you need for comprehensive protection from threats such as viruses, spyware, worms, Trojans, adware, keyloggers, malicious mobile code (MMC) and other dangerous applications.
- A configurable, **high performance deep packet inspection firewall** delivers protection for key Internet services such as Web, e-mail, file transfer, Windows services and DNS.
- **Gateway anti-virus, anti-spyware and intrusion prevention** provides real-time security against the latest viruses, spyware, software vulnerabilities and other malicious code.
- **Content filtering** reduces liability concerns and increases employee productivity by providing the ability to manage access to objectionable or even illegal online content.
- **Dynamic Support 24x7** protects your business and your SonicWALL investment through crucial firmware updates and upgrades, the finest technical support, timely hardware replacement and access to electronic self-help tools.
- **ViewPoint reporting software** provides easy-to-use Web-based reporting that delivers instant insight into the health of your network through dynamic real-time and historical reports.

SonicWALL Gateway Anti-Virus

This section provides an overview to the SonicWALL Gateway Anti-Virus. This section contains the following subsections:

GAV Overview

SonicWALL Gateway Anti-Virus (SonicWALL GAV) is part of the SonicWALL Gateway Anti-Virus/Intrusion Prevention Service solution that provides unified threat management. The integration of gateway anti-virus and intrusion prevention delivers intelligent, real-time network security protection against sophisticated application layer and content-based attacks. Utilizing a configurable, high-performance deep packet inspection architecture, SonicWALL Gateway Anti-Virus/Intrusion Prevention Service secures the network from the core to the perimeter against a comprehensive array of dynamic threats including viruses, worms, Trojans, and software vulnerabilities, such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.

How Does GAV Work?

SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

Benefits

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

SonicWALL Gateway Anti-Virus/Intrusion Prevention Features

The Gateway Anti-Virus/Intrusion Prevention features are described below:

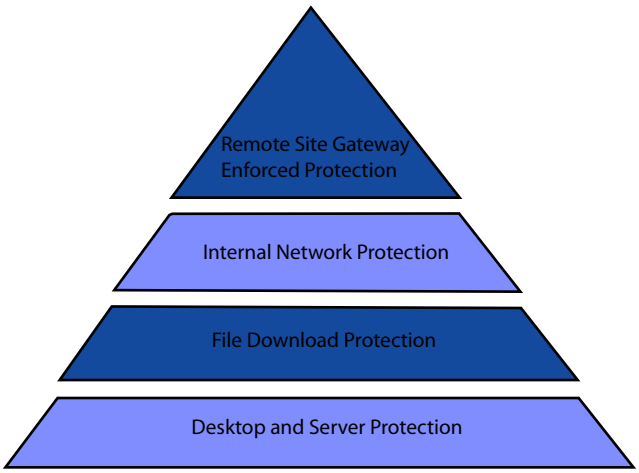
- **Integrated Deep Packet Inspection Technology** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service features a configurable, high-performance deep packet inspection architecture that uses parallel searching algorithms up through the application layer to deliver increased application layer, Web and e-mail attack prevention. Parallel processing reduces the performance impact on the firewall and maximizes available memory for exceptional throughput on SonicWALL integrated security gateways.
- **Real-Time Anti-Virus Gateway Scanning** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service delivers intelligent file-based virus and malicious code prevention by scanning in real-time for decompressed and compressed files containing viruses, Trojans, worms and other Internet threats over the corporate network.
- **Powerful Intrusion Prevention** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides complete protection from a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.
- **Ultimate Scalability and Performance** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service utilizes a per packet scanning engine, making SonicWALL's solution unique in its ability to handle unlimited file size and virtually unlimited concurrent downloads, offering ultimate scalability and performance for today's networked environment.
- **Day Zero Protection** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service ensures incredibly fast time-to-protection by employing a dynamically-updated database of signatures created by a combination of SonicWALL's SonicAlert Team, third-party virus analysts and developers, and open source databases of known threats.
- **Extensive Virus Signature List** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service utilizes an extensive database of thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, worms, Tojans, application exploits, and malicious applications.
- **Distributed Enforcement Architecture** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service utilizes a distributed enforcement architecture to deliver automated signature updates, providing real-time protection from emerging threats and lowering total cost of ownership.
- **Inter-zone Protection** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides application layer attack protection against malicious code and other threats originating from the Internet or from internal sources. Administrators have the ability to enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones for added security (Requires SonicOS Enhanced).
- **Advanced File Decompression Technology** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses, Trojans, worms and malware. Supported compression formats include: ZIP, Deflate and GZIP.
- **File-Based Scanning Protocol Support** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service delivers protection for high threat viruses and malware by inspecting the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NETBIOS, instant messaging and peer-to-peer applications, and dozens

of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

- **Application Control** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides the ability to prevent instant messaging and peer-to-peer file sharing programs from operating through the firewall, closing a potential back door that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service allows network administrators to create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.
- **Granular Management** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides an intuitive user interface and granular policy tools, allowing network administrators to configure a custom set of detection or prevention policies for their specific network environment and reduce the number of false policies while identifying immediate threats.
- **Logging and Reporting** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrators to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System.

SonicWALL GAV Multi-Layered Approach

SonicWALL GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, network systems, and at remote sites. SonicWALL GAV monitors files as they come into the network and enforces anti-virus policies at the gateway to ensure all users have the latest updates.



Remote Site Protection

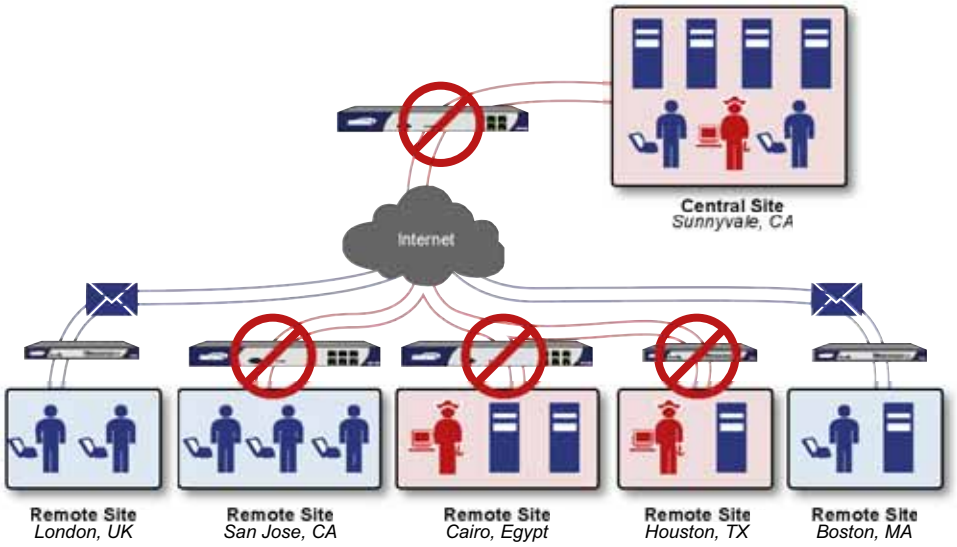
To protect the internal network, perform the following steps:

Step 1 Users send typical e-mail and files between remote sites and the corporate office.

Step 2 SonicWALL GAV scans and analyzes files and e-mail messages on the SonicWALL security appliance.

Step 3 Viruses are found and blocked before infecting remote desktop.

Step 4 Virus is logged and alert is sent to administrator.



Internal Network Protection

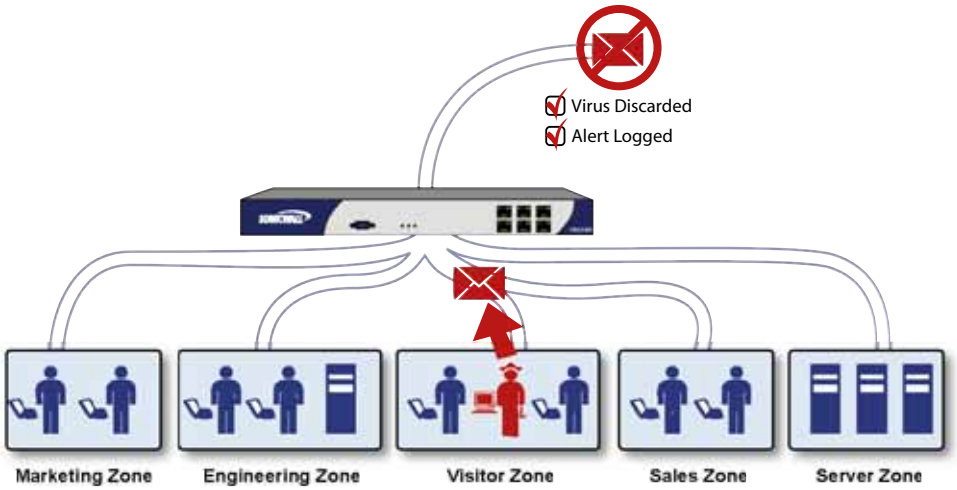
The process for Internal Network Protection is demonstrated in the steps and diagram below:

Step 1 Internal user contracts a virus and releases it internally.

Step 2 All files are scanned at the gateway before being received by other network users.

Step 3 If virus is found, file is discarded.

Step 4 Virus is logged and alert is sent to administrator.



HTTP File Downloads

The process for HTTP File Downloads is described in the steps and diagram below:

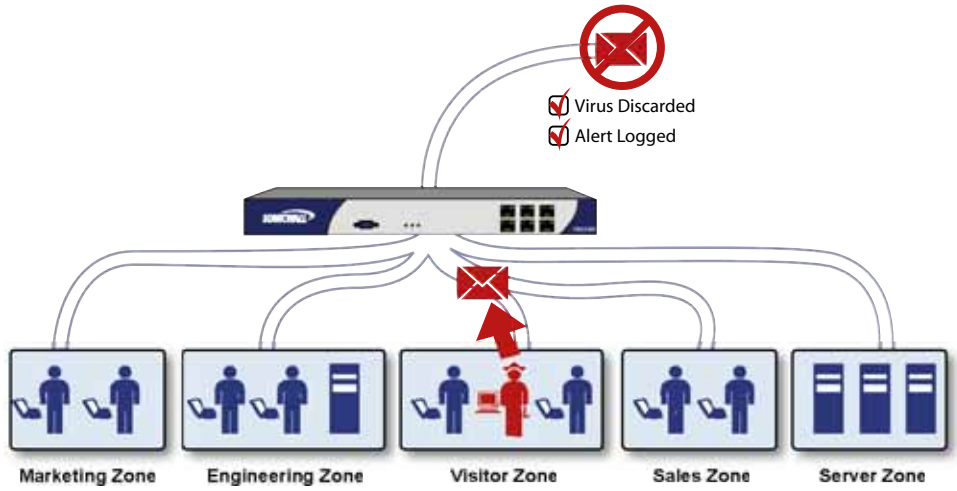
Step 1 Client makes a request to download a file from the Web.

Step 2 File is downloaded through the Internet.

Step 3 File is analyzed through the SonicWALL GAV engine for malicious code and viruses

Step 4 If virus found, file discarded.

Step 5 Virus is logged and alert sent to administrator.



Server Protection

The process for Server Protection is described in the steps below:

Step 1 Outside user sends an incoming e-mail.

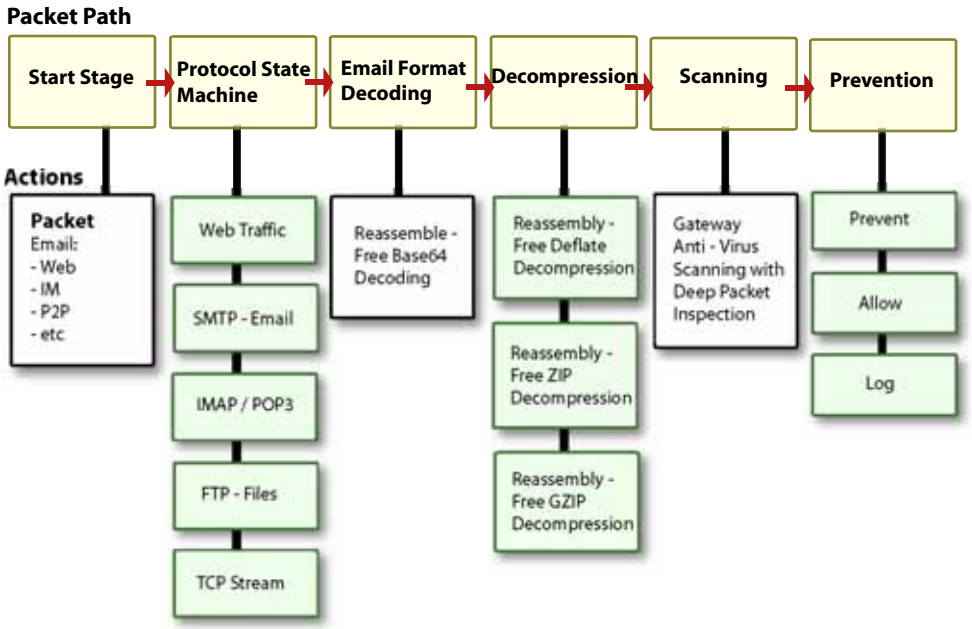
Step 2 E-mail is analyzed through the SonicWALL GAV engine for malicious code and viruses before received by e-mail server.

Step 3 If virus found, threat prevented.

Step 4 E-mail is returned to sender, virus is logged, and alert sent to administrator.

SonicWALL GAV Architecture

SonicWALL GAV is based on SonicWALL's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWALL security appliance. SonicWALL GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The SonicWALL GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWALL's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWALL GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on SonicWALL's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWALL GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWALL GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

Stream Concurrency Limitations by SonicWALL Security Appliance

Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Stream-concurrency are platform dependent as follows:

Platform	GAV-Disabled Connections Cache Size	GAV-Enabled Connections Cache Size (Concurrent File Downloads)	Concurrent Compressed File Downloads with GAV	GAV Signatures
TZ 150 Series	2,048	2,048	100	4,500
TZ 170 Series	6,144	6,144	100	4,500
PRO 1260	6,144	6,144	100	4,500
PRO 2040	32,768	16,384	300	25,000
PRO 3060	131,072	65,536	1,000	25,000
PRO 4060	524,288	131,072	1,500	25,000
PRO 5060	750,000	393,216	3,000	25,000

Disabling the SonicWALL GAV/IPS Engine

In the unlikely event that SonicWALL Gateway Anti-Virus/Intrusion Prevention Service is not enabled on your SonicWALL security appliance, the SonicWALL GAV/IPS engine itself can be disabled, and the resources can be reallocated to the SPI connection cache.

To disable the SonicWALL GAV/IPS engine, perform the following steps:

Step 1 Select the **Firewall > Advanced** page.

Step 2 Select the **Disable Gateway AV and IPS Engine (increases maximum SPI connections)** checkbox. This presents an alert informing you that the SonicWALL security appliance must be rebooted for the change to take effect.

Step 3 Restart your SonicWALL security appliance.

Protocol Handling

SonicWALL GAV functionality supports the following protocols: HTTP, SMTP, IMAP, POP3, FTP and the scanning of generic TCP streams for viruses.

If malicious traffic is detected, appropriate actions are taken based on the protocol. For generic TCP streams, the traffic is dropped and the connection is reset. If so configured, an encrypted and hashed message explaining the action is sent to the user's Global Security Client (requires version 2.0 or higher) and to the user's 'Security Action Notification Applet', and displayed to the user if either application is active. Application level awareness of the type of protocol that was transporting the violation allows for very specific actions to be taken to gracefully handle the rejection of the payload:

Note 8-bit encoding is handled natively for all email based protocols (SMTP, POP3, and IMAP) since no decoding is required for each encoding scheme.

SMTP

Capabilities: base64 decoding, zip (including archives) and gzip decompression.

Prevention Mechanism: The message which contains the virus is removed from the head of the sent queue, thus preventing it from being resent, via 552 SMTP response and the connection is terminated.

POP3

Capabilities: base64 decoding, zip (including archives) and gzip decompression.

Prevention Mechanism: The message which contains the virus is removed from the POP3 server via 'DELE' command and the connection is terminated. Continuation of message downloads following termination requires the user to re-initiate the download process on their POP3 client in order to download the rest of the messages from the POP3 server.

Note: POP3 client behavior varies from one client to the next. SonicWALL GAV attempts to determine the type of POP3 client being used, and to compensate for behavioral differences. In rare cases, some clients may require special GAV settings - these settings have been made available in the /diag.html page.

- **Disable Gateway AV POP3 Auto Deletion** - When a POP3 client is identified as Outlook Express, DELE (delete) message sequencing is tailored to Outlook Express' behavior. This setting can resolve problems caused by misidentification that are encountered during the deletion of virus-infected emails.
- **Disable Gateway AV POP3 UIDL Rewriting** - Certain Netscape POP3 clients have difficulty with the UIDL (unique ID listing - RFC1939) command. When a POP3 client is recognized as Netscape, UIDL messages are suppressed, which is allowable because they are optional. This setting can resolve problems caused by misidentification that are encountered during the message retrieval process.

IMAP

Capabilities: base64 decoding, zip (including archives) and gzip decompression.

Prevention Mechanism: The connection is terminated, preventing the user from downloading the mail containing the violation. The user must manually mark the mail deleted and purge it from the server.

HTTP

Capabilities: zip (including archives), gzip and deflate decompression. Deflate decompression method is not supported when HTTP response is Chunk Encoded. All HTTP traffic is inspected, not just TCP port 80. Suppresses the use of HTTP Byte-Range requests to prevent the sectional retrieval and reassembly of potentially malicious content.

Note Suppression of HTTP Byte-Range requests may inhibit the use of certain download accelerator programs that attempt to retrieve files as multiple simultaneous requests.

Prevention Mechanism: The connection is terminated, preventing the user from receiving the malicious payload.

FTP

Capabilities: zip (including archives) and gzip decompression. FTP stateful code follows data port negotiations, allowing FTP data to be inspected across any operating TCP port. Suppresses the use of the FTP 'REST' (restart) request to prevent the sectional retrieval and reassembly of potentially malicious content. "The suppression of the 'REST' request can be overridden from the /diag.html page with the option 'Enable FTP 'REST' requests with Gateway AV'.

Prevention Mechanism: The connection is terminated, preventing the user from receiving the malicious payload.

IM, P2P and Proprietary Protocols

Capabilities: zip (including archives) and gzip decompression.

Prevention Mechanism: The connection is terminated, preventing the user from receiving the malicious payload.

SonicWALL Intrusion Prevention Service

This section provides an overview to the SonicWALL Intrusion Prevention Service. This section contains the following subsections:

- IPS Overview
- How Does IPS Work?
- What is a Zone?
- Benefits

IPS Overview

SonicWALL Intrusion Prevention Service is part of the SonicWALL Gateway Anti-Virus/Intrusion Prevention Service solution that provides protection against real-time for viruses, worms, Trojans, and malicious code using a patent-pending scanning engine. SonicWALL's unique solution features a high-performance deep packet inspection architecture. It is a zone-based security service that enables easy and secure managemet. When you activate SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus is also activated. SonicWALL IPS is managed directly from the SonicWALL security appliance.

How Does IPS Work?

SonicWALL Intrusion Prevention Service (SonicWALL IPS) utilizes a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. IPS is set up using the SonicWALL network zones concept.

What is a Zone?

A Zone is a logical grouping of one or more interfaces and/or VLANs designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Network security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

Benefits

The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Alternatively, SonicWALL Global Management System (SonicWALL GMS) provides global management capabilities that enabled administrators to manage SonicWALL IPS across multiple SonicWALL security appliances from a central location. SonicWALL GMS and SonicWALL ViewPoint solutions allow administrators to create detailed reports based on attack source, destination and type of intrusion, such as "Top Intrusions," "Destinations Over Time" and "Intrusions Over Time."

Note Please visit <http://www.sonicwall.com> for more information on SonicWALL GMS and SonicWALL ViewPoint.

Note Refer to the SonicWALL Gateway Anti-Virus Administrator's Guide for information you need to successfully activate, configure, and administer SonicWALL Gateway Anti-Virus on a SonicWALL security appliance, located on the SonicWALL Web site: <http://www.sonicwall.com/services/documentation.html>.

SonicWALL Anti-Spyware

SonicWALL Anti-Spyware is included within the SonicWALL Gateway Anti-Virus (GAV), Anti-Spyware and Intrusion Prevention Service (IPS) unified threat management solution. SonicWALL GAV, Anti-Spyware and IPS delivers a comprehensive, real-time gateway security solution for your entire network.

This section provides an overview to the SonicWALL Anti-spyware. This section contains the following subsections:

The Spyware Threat

Spyware is software that utilizes a computer's Internet access without the host's knowledge or permission. Spyware can gather information about browsing habits, data entered into online forms, and keystrokes.

Computers are infected with Spyware applications from a variety of sources:

- Downloaded programs such as P2P applications, freeware, screensavers, utilities, download managers, demo software, and video games.
- Trojans delivered through e-mail, downloaded from an FTP site, or installed with freeware.
- Banner ads

The impact of spyware for users includes the following threats:

- Identity theft
- Stolen proprietary data
- Invasion of privacy
- Degraded computer performance
- Excessive bandwidth use resulting in a network slowdown

SonicWALL Anti-Spyware Security Service

The SonicWALL Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWALL Anti-Spyware works with other anti-spyware programs, such as applications that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

Benefits

SonicWALL Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the SonicWALL Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected

clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the SonicWALL security appliance identifies that traffic and resets the connection.

The SonicWALL Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.

Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.

SonicWALL Content Filtering Service - Premium

This section provides an overview to the SonicWALL Content Filtering Service. This section contains the following subsections:

CFS Overview

SonicWALL Content Filtering Services Premium (CFS Premium) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. CFS Premium provides network administrators with greater control by automatically and transparently enforcing acceptable use policies.

SonicWALL CFS Premium gives administrators the flexibility to enforce content filtering on Zones as well as custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students.

How Does CFS Premium Work?

SonicWALL CFS Premium utilizes a dynamic database of millions of URLs, IP addresses and domains to block 56 categories of objectionable, inappropriate or unproductive Web content. At the core of CFS Premium is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

Benefits

With SonicWALL CFS Premium, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. CFS Premium automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL CFS Premium can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliances can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

SonicWALL Deep Packet Inspection

This section provides an overview to the SonicWALL Intrusion Prevention Service (DPI). This section contains the following subsections:

DPI Overview

Deep Packet Inspection (DPI) looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

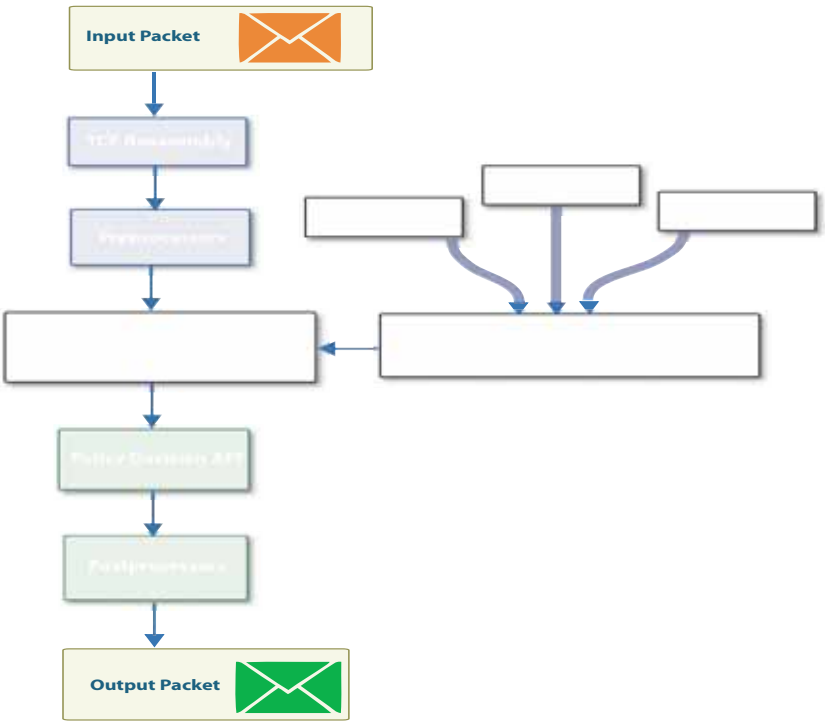
How Does DPI Work?

Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

Benefits

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

Figure 1 Deep Packet Inspection Flow Diagram



The following steps describe how the SonicWALL Deep Packet Inspection Architecture functions:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or reset a TCP connection.
5. SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

SonicWALL Security Dashboard

This section provides an introduction to the Security Dashboard feature. This section contains the following subsections:

- Security Dashboard Overview
- What is Security Dashboard?
- How Does the Security Dashboard Work?
- Benefits

Security Dashboard Overview

The SonicWALL Security Dashboard provides reports of the latest threat protection data from a single SonicWALL appliance and aggregated threat protection data from SonicWALL security appliances deployed globally. The SonicWALL Security Dashboard displays automatically upon successful authentication to a SonicWALL security appliance running SonicOS 3.8 firmware or later, and can be viewed at any time by navigating to the **System > Security Dashboard** menu in the left-hand menu. Reports in the Security Dashboard include:

- Viruses Blocked by SonicWALL Network
- Intrusions Prevented by SonicWALL Network
- Spyware Blocked by SonicWALL Network
- Multimedia (IM/P2P) Detected/Blocked by SonicWALL Network

Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, SonicWALL Security Dashboard reports can be transformed into a PDF file format with the click of a button. Figure 2 provides the default view of the SonicWALL Security Dashboard.

Figure 2 SonicWALL Security Dashboard

What is Security Dashboard?

The TotalSecure provides the latest threat protection information to keep you informed about potential threats being blocked by SonicWALL security appliances. When you activate SonicWALL's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the SonicWALL Security Dashboard. SonicWALL's security services include ongoing new signature updates to protect against the latest virus and spyware attacks.

How Does the Security Dashboard Work?

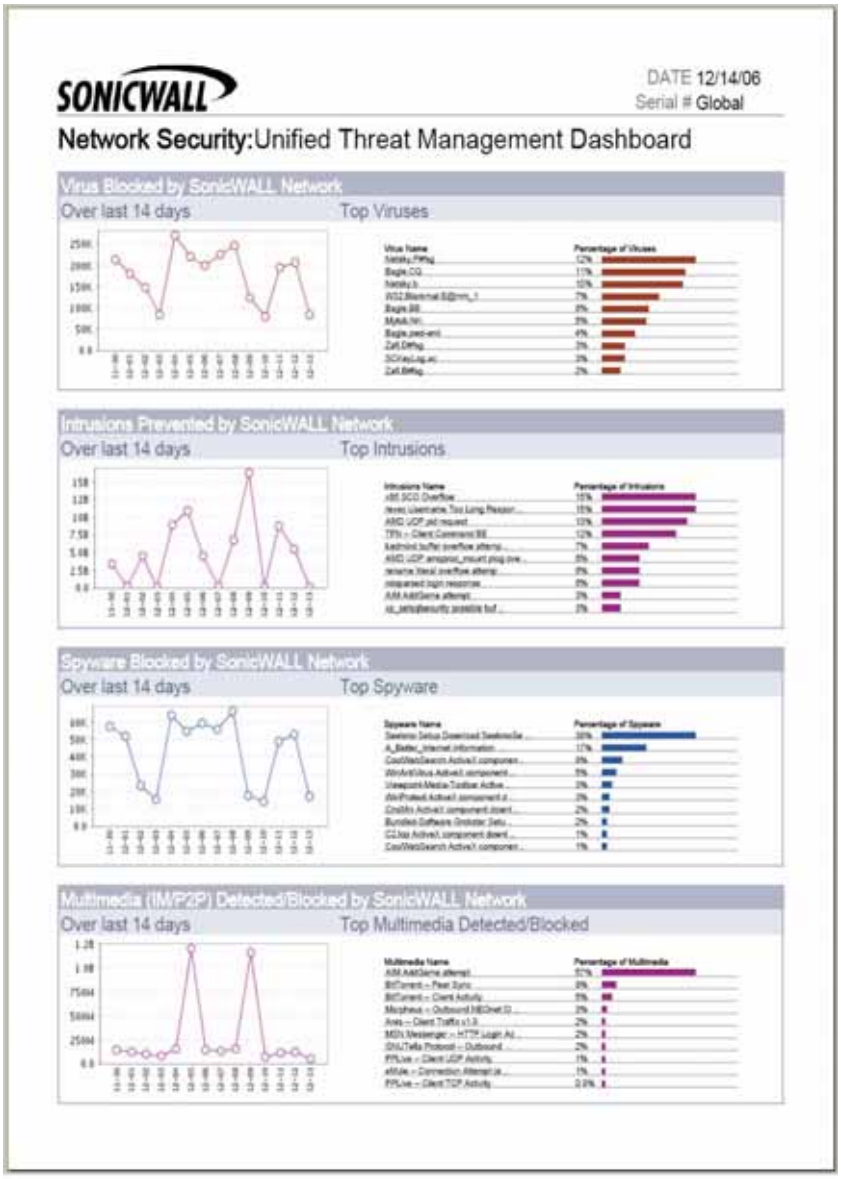
The SonicWALL Security Dashboard provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your SonicWALL security appliance is displayed. At the global level, the SonicWALL Security Dashboard is updated hourly from the SonicWALL backend server with aggregated threat protection data from globally-deployed SonicWALL security appliances. Data provided by the SonicWALL backend server is cached locally for reliable delivery.

Note The SonicWALL security appliance must have Internet connectivity to receive the latest threat protection statistics from the SonicWALL backend server, which reports aggregated data from globally deployed SonicWALL security appliances. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

Benefits

The Security Dashboard provides insight into threats over time, and can be configured to display data from multiple time periods. The SonicWALL Security Dashboard can be viewed easily in the **System > Security Dashboard** page of the SonicWALL appliance management interface, or as a custom generated PDF file. Figure 3 provides a PDF report view of the SonicWALL Security Dashboard.

Figure 3 SonicWALL Security Dashboard PDF Report



Registering Your Appliance on MySonicWALL

While the SonicWALL TZ 180 TotalSecure includes licenses for the Intrusion Prevention services, you must activate these services by following the steps within the sections listed below.

This section provides an overview to the SonicWALL Intrusion Prevention Service. This section contains the following subsections:

- Creating a mySonicWALL.com Account
- Registering Your SonicWALL Security Appliance

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and free. Simply complete an online registration form in the SonicWALL security appliance management interface.

Note: If you already have a mysonicWALL.com account, go to "" on page 18.

1. Log into the SonicWALL security appliance management interface.
2. On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**.

3. In the **mySonicWALL.com Login** page, click the **here** link in **If you do not have a mySonicWALL account, please click here to create one**.

4. In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (*****) are required fields.
5. Remember your username and password to access your mySonicWALL.com account.
6. Click **Submit** after completing the **MySonicWALL Account** form.
7. When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

Congratulations. Your mySonicWALL.com account is activated.

Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.

Note: mySonicWALL.com registration information is not sold or shared with any other company.

Registering Your SonicWALL Security Appliance

1. Log into the SonicWALL security appliance management interface.
2. If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
3. On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
4. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit.**
5. The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
   - **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
   - **Network Anti Virus** - Provides desktop and server anti-virus protection with software running on each computer.
   - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
   - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.

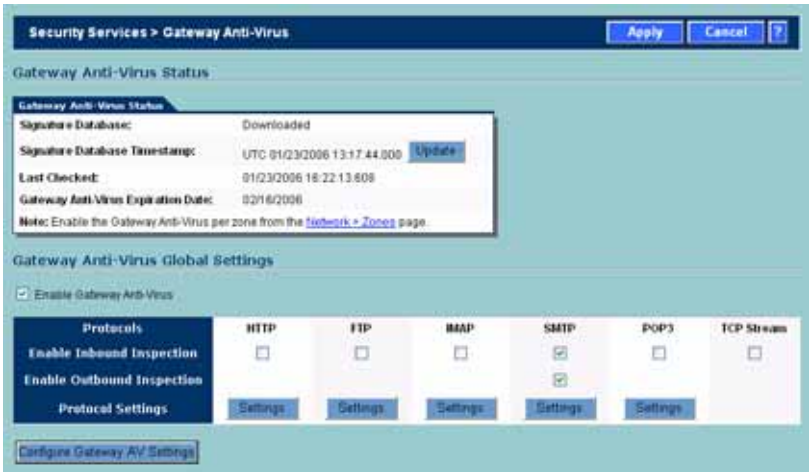
   Click **Continue** on each page.
6. At the top of the **Product Survey** page, Enter a "friendly name" for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
7. Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
8. Click **Submit**.
9. When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

TotalSecure Configuration Task List

This section contains the following sections:

Setting Up SonicWALL GAV Protection

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring SonicWALL GAV on your SonicWALL security appliance.



Enabling SonicWALL GAV

You must select **Enable Gateway Anti-Virus** check box in the **Gateway Anti-Virus Global Settings** section to enable SonicWALL GAV on your SonicWALL security appliance. If your SonicWALL security appliance is running SonicOS Standard 3.0, you must also specify the interfaces you want to apply SonicWALL GAV protection. If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you must specify the Zones you want SonicWALL GAV protection on the **Network > Zones** page.

Applying SonicWALL GAV Protection on Interfaces

If your SonicWALL security appliance is running SonicOS Standard 3.0, you also need to specify the interface that you want enabled for SonicWALL GAV protection. Depending on the SonicWALL security appliance model you are using, you can choose the **WAN**, **LAN**, **DMZ**, **OPT** or **WLAN** port. After selecting the interface(s), click **Apply**.It is recommended you select the WAN and LAN interfaces.

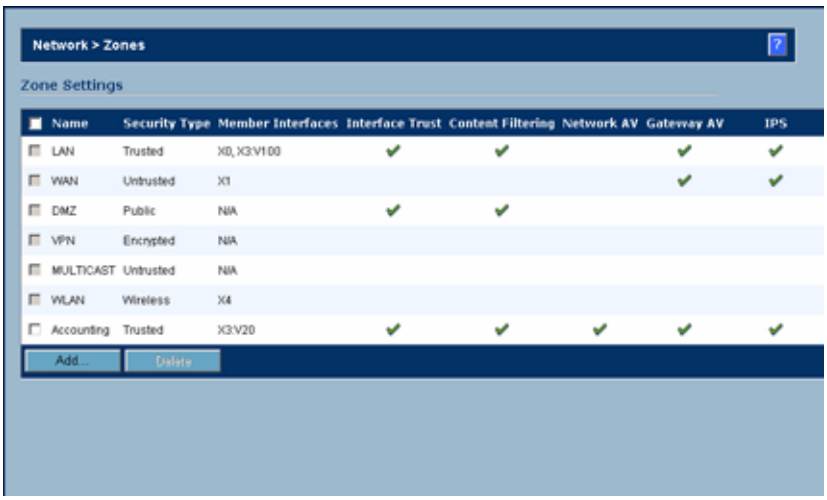
If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you apply SonicWALL GAV to Zones on the **Network > Zones** page.

Note: Refer to "Applying SonicWALL GAV Protection on Zones (SonicOS Enhanced 3.0)" on page 26 for instructions on applying SonicWALL GAV protection to zones.

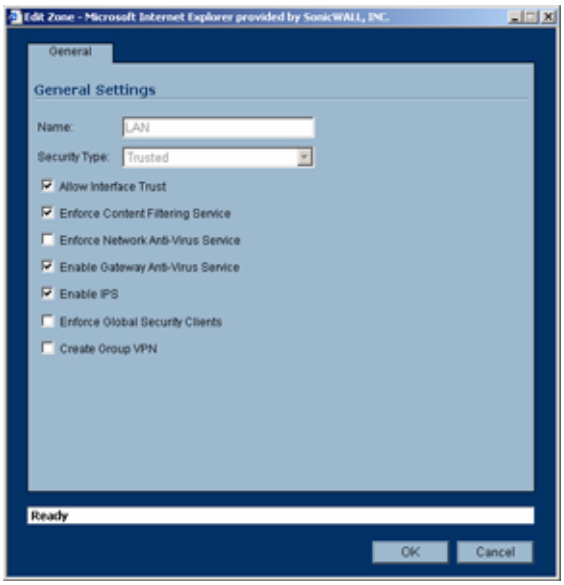
Applying SonicWALL GAV Protection on Zones (SonicOS Enhanced 3.0)

If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you can enforce SonicWALL GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic.

Step 1 In the SonicWALL security appliance management interface, select **Network > Zones** or from the **Gateway Anti-Virus Status** section, on the **Security Services > Gateway Anti-Virus** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.



Step 2 In the **Configure** column in the **Zone Settings** table, click the edit icon . The **Edit Zone** window is displayed.



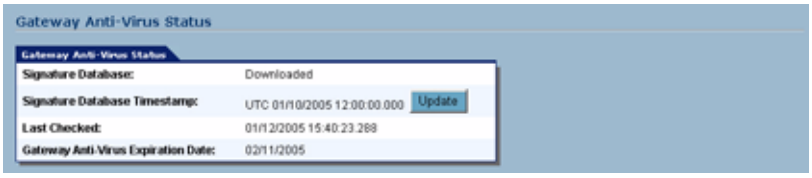
Step 3 Click the **Enable Gateway Anti-Virus Service** checkbox. A checkmark appears. To disable Gateway
Anti-Virus Service, uncheck the box.

Step 4 Click **OK**.

Note You also enable SonicWALL GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

Viewing SonicWALL GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWALL signature servers were last checked for the most current database version. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.



The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWALL GAV signature database, not the last update to your SonicWALL security appliance.
- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWALL GAV service expires. If your SonicWALL GAV subscription expires, the SonicWALL IPS inspection is stopped and the SonicWALL GAV configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL GAV license to the previously configured state.

If your SonicWALL security appliance you are running SonicOS Standard 3.0 and no interfaces are specified in the **Gateway Anti-Virus Global Settings** section, the message: **Warning: No interfaces have Gateway Anti-Virus enabled** is displayed in the **Gateway Anti-Virus Status** section. You must check the **Enable Gateway Anti-Virus on Interface** and specify the interface(s) you want to apply anti-virus scanning.

If your SonicWALL security appliance you are using SonicOS Enhanced 3.0, the **Gateway Anti-Virus Status** section displays **Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWALL GAV on Zones.

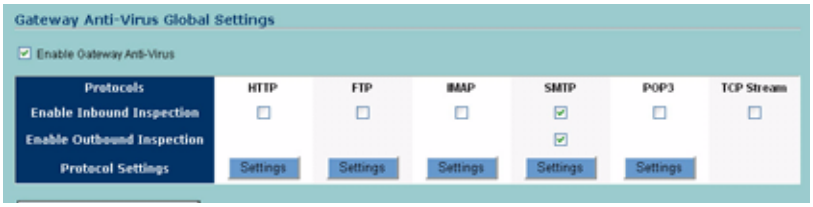
Note: Refer to "Applying SonicWALL GAV Protection on Zones (SonicOS Enhanced 3.0)" on page 26 for instructions on applying SonicWALL GAV protection to zones.

Updating SonicWALL GAV Signatures

By default, the SonicWALL security appliance running SonicWALL GAV automatically checks the SonicWALL signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWALL GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWALL GAV signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

Specifying Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows SonicWALL GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

Note: Refer to "Protocol Handling" on page 9 for detailed descriptions of how SonicWALL GAV handles protocol traffic.

Enabling Inbound Inspection

Within the context of SonicWALL GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to any Zone.
- Non-SMTP traffic from a Public Zone destined to an Untrusted Zone.
- SMTP traffic initiating from a non-Trusted Zone destined to a Trusted, Wireless, Encrypted, or Public Zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to a Trusted, Wireless, or Encrypted Zone.

The **Enable Inbound Inspection** protocol traffic handling represented as a table:

SMTP Traffic					
From / To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✗	✗
Encrypted	✓	✓	✓	✗	✗
Wireless	✓	✓	✓	✗	✗
Public	✓	✓	✓	✓	✓
Untrusted	✓	✓	✓	✓	✓

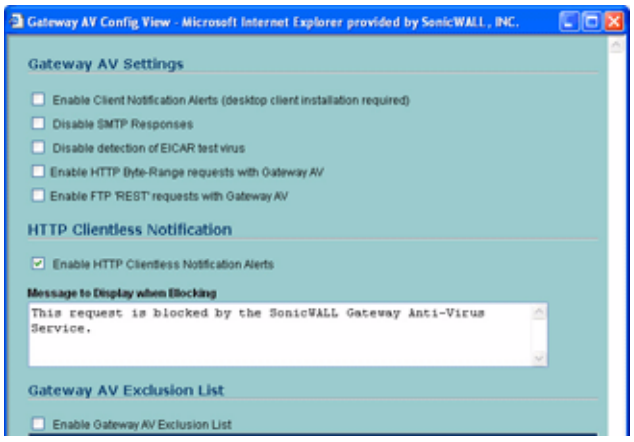
All Other Traffic					
From / To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✓	✓
Encrypted	✓	✓	✓	✓	✓
Wireless	✓	✓	✓	✓	✓
Public					✓
Untrusted					

Enabling Outbound SMTP Inspection

The **Enable Outbound Inspection** feature is available for SMTP traffic, such as for a mail server that might be hosted on the DMZ. Enabling outbound inspection for SMTP scans mail that is delivered to the internally hosted SMTP server for viruses.

Configuring Client Alerts and an Exclusion List

Clicking the **Configure Gateway AV Settings** button in the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Config View** window, which allows you to configure client notification alerts and create a SonicWALL GAV exclusion list.



Configuring Client Alerts

If you want clients on your network to receive notifications on their desktop when a HTTP file download is blocked by GAV, check the **Enable Client Notification Alerts (desktop client installation is required)** box. You must install the client software included on the Resource CD for your SonicWALL security appliance for the client to receive these notifications from SonicWALL GAV.

If you want to suppress the sending of e-mail messages (SMTP) to clients from SonicWALL GAV when a virus is detected in an e-mail or attachment, check the **Disable SMTP Responses** box.

Configuring a SonicWALL GAV Exclusion List

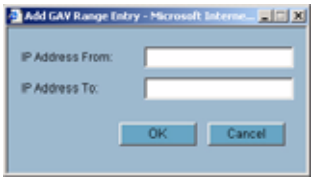
Any IP addresses listed in the exclusion list bypass virus scanning on their traffic.The **Gateway AV Exclusion List** section provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWALL GAV scanning.

Caution Use caution when specifying exclusions to SonicWALL GAV protection.

To add an IP address range for exclusion, perform the following steps:

Step 1 Click the **Enable Gateway AV Exclusion List** checkbox to enable the exclusion list.

Step 2 Click the **Add** button. The **Add GAV Range Entry** window is displayed.

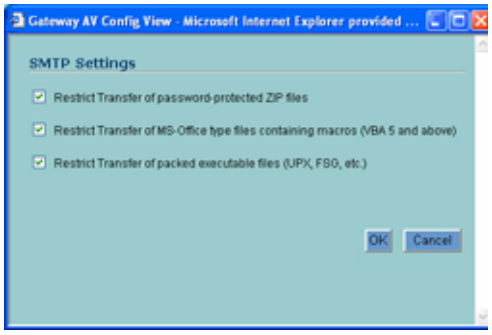


Step 3 Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. You IP address range appears in the **Gateway AV Exclusion List** table. Click the edit icon in the **Configure** column to change an entry or click the trashcan icon to delete an entry.

Step 4 Click **OK** to exit the **Gateway AV Config View** window.

Restricting File Transfers

The restrict transfer settings listed under the **Configure Gateway AV Settings** button in the **Gateway Anti-Virus Global Settings** section, if enabled, prevent files with specific attributes from being transferred.



The restrict transfer settings include:

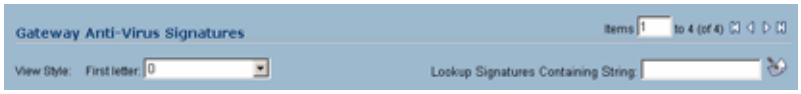
- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWALL Gateway
  Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with SonicWALL GAV signature updates.

Viewing SonicWALL GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWALL GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWALL GAV signature database downloaded to your SonicWALL security appliance.

Note: Signature entries in the database change over time in response to new threats.

Displaying Signatures



You can display the signatures in a variety of views using the **View Style** menu.

- **Use Search String** - Allows you to display signatures containing a specified string entered in the Lookup Signatures **Containing String** field.
- **All Signatures** - Displays all the signatures in the table, 50 to a page.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A-Z** - Displays signature names beginning with the letter you select from menu.

Navigating the Gateway Anti-Virus Signatures Table

The SonicWALL GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you're displaying the first page of a signature table, the entry might be **Items** 1 to 50 (of 58). Use the navigation buttons to navigate the table.Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the Lookup Signatures Containing String field, then clicking the edit (Notepad) icon.

Setting Up SonicWALL Intrusion Prevention Service Protection

Activating the SonicWALL Intrusion Prevention Service license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

1. Enable SonicWALL Intrusion Prevention Service
2. Specify the Priority attack Groups
3. Apply SonicWALL Intrusion Prevention Service Protection to Zones

Note: For complete instructions on setting up SonicWALL Intrusion Prevention Service, refer to the SonicWALL Intrusion Prevention Service Administrator's Guide available on the SonicWALL documentation Web site <http://www.sonicwall.com/us/3396.html>.

Selecting **Threat Protection > Intrusion Prevention** displays the configuration settings for SonicWALL IPS on your SonicWALL security appliance.

The **Intrusion Prevention Service** page is divided into three sections:

- **IPS Status** - displays status information on the state of the signature database, your SonicWALL IPS license, and other information.
- **IPS Global Settings** - provides the key settings for enabling SonicWALL IPS on your SonicWALL security appliance, specifying global SonicWALL IPS protection based on three classes of attacks, and other configuration options.
- **IPS Policies** - allows you to view SonicWALL IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

After activating your Intrusion Prevention Service license, you must enable and configure SonicWALL IPS on the SonicWALL management interface to before intrusion prevention policies are applied to your network traffic.

Enabling SonicWALL IPS

SonicWALL IPS must be globally enabled on your SonicWALL security appliance by checking the **Enable IPS** check box in the **IPS Global Settings** section. A checkmark in the **Enable IPS** check box turns on the service on your SonicWALL security appliance.

To disable IPS, uncheck the **Enable IPS** check box. This will prevent blocking of traffic that matches the IPS signatures. However, some signatures belong to Application Filter category sets as well as other types of category sets such as GAV, IPS, Anti-Spyware, or Web Filters. If Application Filtering is enabled, these signatures are blocked by the Application Filter process even when you configure the other filters to allow them.

Caution Checking the **Enable IPS** check box does not automatically start SonicWALL IPS protection. You must also update the **IPS Global Settings** section.You must specify a **Prevent All** action in the **Signature Groups** table to activate Intrusion Prevention on the SonicWALL security appliance, and specify the interface or zones you want to protect.

Specifying Global Attack Level Protection

SonicWALL IPS allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous and disruptive attacks. For more detailed information on configuring global signature groups, refer to “Configuring Global Signature Groups” in the *SonicWALL Intrusion Prevention Service Administrator’s Guide* available on the SonicWALL Resource CD or at<http://www.sonicwall.com/us/3396.html>

Fine-tuning the IPS

To really take advantage of the SonicWALL IPS, it is sometimes necessary to fine-tune the behavior of certain IPS Categories and/or IPS Signatures.

Since all network are not alike, it can be quite difficult to *exactly* tell what IPS Categories or IPS Signatures should be *Prevented* or *Detected*.

However, what can be done is to create a *Baseline Setup* where as much hostile traffic as possible is Prevented and Detected regardless of what traffic may flow in an individual network.

Refer to the descriptions in this document for instructions on how to change the behavior of a certain IPS Category and/or IPS Signature.

A Baseline Setup can be accomplished in two different ways. The outcome is basically the same, but involves somewhat different steps, both depends heavily on logging of the correct

Enable IPS Logging

To view IPS-related events in the log, ensure that the correct log categories are enabled.

The more categories enabled while fine-tuning, the better, although the logs fill fast. Always make sure the categories *Intrusion Prevention* and *Security Services* are enabled.

The Brute-force Baseline Setup

The Brute-force Baseline setup is quite brutal and will in most cases break valid traffic flowing in the network.

- Use the **IPS Global Setting** to enable the option *Detect All* for ***all three*** IPS Signature Groups.

- Use the **IPS Global Setting** to enable the option *Prevent All* for ***all three*** IPS Signature Groups.

Now all three IPS *Signature Groups* [*High, Medium resp. Low Priority*] will be Prevented, which will Prevent quite a lot flowing in the network, for example:

- MSN Messenger, Yahoo Messenger, AIM, IRC and other Instant Messaging application will not work as will not any Peer-to-Peer applications.
- A Terminal Service client will not be able to connect.
- The VoIP Skype-application will not be able to connect
- Zone Transfers will be Prevented

After these settings are implemented, the network administrator must keep a very close eye on the logs of the SonicWALL appliance for some time and there possibly could be some enraged users for a brief period of time.

As soon as traffic is Prevented by the IPS, a log-entry will be written to the logs. Depending whether the prevented traffic is valid or not, the network administrator has the option to disable the Prevention of that particular IPS-event, *directly from the log viewer.*

If the user tries to log in to a blocked site, an error message will appear.

Setting Up SonicWALL Anti-Spyware Protection

The SonicWALL Anti-Spyware license provided on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Anti-Spyware to begin protecting your network, you need to perform the following steps:

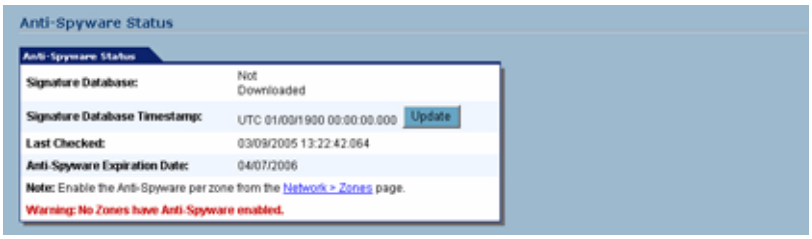
1. Enable SonicWALL Anti-Spyware
2. Specify Spyware Danger Level Protection
3. Apply SonicWALL Anti-Spyware Protection to Zones

Note: For complete instructions on setting up SonicWALL Anti-Spyware Service, refer to the SonicWALL Anti-Spyware Service Administrator's Guide available on the SonicWALL Web site <http://www.sonicwall.com/us/3396.html>

Once you configure these basic anti-spyware protection settings, you can perform additional configuration options to tailor SonicWALL Spyware protection for your network environment.

Selecting **Threat Protection > Anti-Spyware** displays the configuration settings for SonicWALL Anti-Spyware on your SonicWALL security appliance. The **Anti-Spyware** page is divided into three sections:

- **Anti-Spyware Status** - displays status information on the state of the signature database, your SonicWALL Anti-Spyware license, and other information.

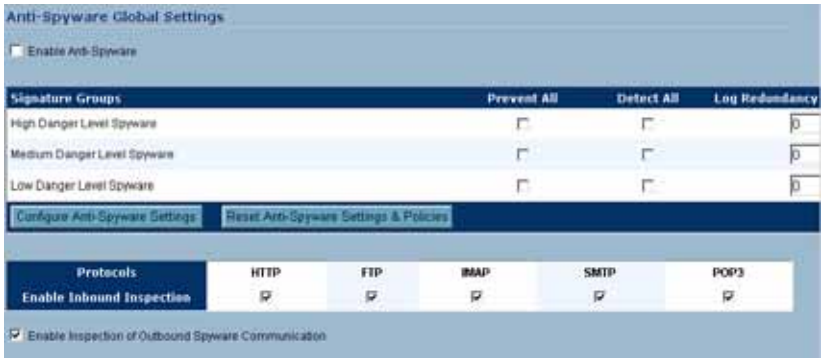


- **Anti-Spyware Global Settings** - provides the key settings for enabling SonicWALL Anti-Spyware on your SonicWALL security appliance, specifying global SonicWALL Anti-Spyware protection based on three classes of spyware, and other configuration options.
- **Anti-Spyware Policies** - allows you to view SonicWALL Anti-Spyware signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

Caution You must enable and configure SonicWALL Anti-Spyware on the SonicWALL management interface before anti-spyware policies are applied to your network traffic.

Enabling SonicWALL Anti-Spyware

SonicWALL Anti-Spyware must be globally enabled on your SonicWALL security appliance. Select the the **Enable Anti-Spyware** check box (a checkmark is displayed), and then click **Apply**.



Checking the **Enable Anti-Spyware** check box does not automatically start SonicWALL Anti-Spyware protection. You must also specify a **Prevent All** action in the **Signature Groups** table to activate Anti-Spyware on the SonicWALL security appliance, and then specify the zones you want to protect on the **Network > Zones** page. You can also select **Detect All** for spyware event logging and alerting.

To disable Anti-Spyware, uncheck the **Enable Anti-Spyware** check box. This will prevent blocking of traffic that matches the Anti-Spyware signatures. However, some signatures belong to Application Filter category sets as well as other types of category sets such as GAV, IPS, Anti-Spyware, or Web Filters. If Application Filtering is enabled, these signatures are blocked by the Application Filter process even when you configure the other filters to allow them.

Specifying Spyware Danger Level Protection

SonicWALL Anti-Spyware allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Danger Level Spyware**, **Medium Danger Level Spyware** and **Low Danger Level Spyware**.

Selecting the **Prevent All** and **Detect All** check boxes for **High Danger Level Spyware** and **Medium Danger Level Spyware** in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous spyware.

Caution SonicWALL recommends enabling Prevent All for **High Danger Level Spyware** and **Medium Danger Level Spyware** signature groups to provide anti-spyware protection against the most damaging and disruptive spyware applications. You can also enable **Detect All** for spyware logging and alerting.

SonicWALL Anti-Spyware also allows you to configure anti-spyware policies at the category and signature level to provide flexible granularity for tailoring SonicWALL Anti-Spyware protection based on your network environment requirements. If you're running SonicOS Enhanced, you can apply these custom SonicWALL Anti-Spyware policies to Address Objects, Address Groups, and User Groups, as well as create enforcement schedules. For more information, refer to the *SonicWALL Anti-Spyware Administrator's Guide* available on the SonicWALL Web site: <*http://www.sonicwall.com/us/3396.html*>

Setting Up CFS Premium

To activate SonicWALL CFS Premium, perform the following steps:

Step 1 Click the **SonicWALL Content Filtering Subscription** link. The **mySonicWALL.com Login** page is displayed.

Step 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.

Step 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS Premium subscription is activated on your SonicWALL.

Glossary

- **Capabilities**: base64 decoding, zip (including archives) and gzip decompression.

- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Distributed Enforcement Architecture** - SonicWALL's unified threat management technology that delivers automated signature updates that provide real-time protection from current and emerging threats
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traff
- **Stateful Packet Inspection** - examines the contents of individual packets at all layers of the OSI model, from network layer to application layer.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Snort** - an open source network intrusion detection system. SonicWALL IPS includes open-source Snort signatures, as well as signatures from other signature databases, and SonicWALL created signatures. SonicWALL does not use the Snort engine.
- **Prevention Mechanism**: The message which contains the virus is removed from the head of the sent queue, thus preventing it from being resent, via 552 SMTP response and the connection is terminated.

Related Documentation

SonicWALL user guides and reference documents are available at the SonicWALL Technical Documentation Online Library:

http://www.sonicwall.com/us/Support.html

For basic and advanced deployment examples, refer to SonicOS Guides and SonicWALL TechNotes available on the Web site.

See the following documents for more information:

- SonicWALL CFS Premium Administrator's Guide
- SonicWALL Gateway Anti-Virus 2.0 Administrator's Guide
- SonicWALL Intrusion Prevention Service 2.0 Administrator's Guide
- SonicWALL Anti-Spyware Administrator's Guide
- SonicOS Standard 3.8 Administrator's Guide
- SonicOS Enhanced 3.8 Administrator's Guide
- SonicWALL TZ 180 Getting Started Guide
- SonicWALL TZ 180 Wireless Getting Started Guide
- SonicWALL Intrusion Prevention Service Primer
- NAT over VPN with Sonic OS Enhanced
- Blocking Skype with SonicWALL Unified Threat Management Appliances

Solution Document Version History

Version Number	Date	Notes
1	6/11/2007	This document was created.
2	6/12/2007	Formatting changes, Updated Illustrations, Reference Links, All other related information.