SonicWALL Anti-Spyware
Administrator's Guide
# Table of Contents

Preface ................................................................................................................. 1  
Copyright Notice ................................................................................................. 1  
Trademarks ......................................................................................................... 1  
Limited Warranty ................................................................................................. 1  

## About this Guide

Guide Conventions ............................................................................................... 3  
Icons Used in this Guide ..................................................................................... 4  
SonicWALL Technical Support ........................................................................... 4  
  North America Telephone Support ................................................................... 4  
  International Telephone Support ....................................................................... 4  

## Deploying SonicWALL Anti-Spyware

SonicWALL Anti-Spyware Overview .................................................................... 6  
The Spyware Threat ............................................................................................. 6  
SonicWALL Anti-Spyware Security Service ......................................................... 6  
SonicWALL’s Unified Threat Management Solution ............................................ 7  
SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Security Services .................................................. 7  
How SonicWALL’s Deep Packet Inspection Architecture Works .................... 9  
Inbound and Outbound Protection ..................................................................... 11  
Disabling the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Engine ......................................................... 11  

## Activating the SonicWALL Anti-Spyware License

Creating a mySonicWALL.com Account ............................................................. 13  
Registering Your SonicWALL Security Appliance ............................................. 14  
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License ................................. 15  
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service on mySonicWALL.com ............... 17  
Activating FREE TRIALS .................................................................................. 17  

## Setting Up SonicWALL Anti-Spyware Protection

Enabling SonicWALL Anti-Spyware ...................................................................... 19  
Specifying Spyware Danger Level Protection ................................................... 19  
Applying SonicWALL Anti-Spyware Protection to Zones for SonicOS Enhanced .............................................................................. 20  
Applying SonicWALL Anti-Spyware Protection on Interfaces for SonicOS Standard .......................................................................... 20  
Understanding SonicWALL Anti-Spyware Status Information ....................... 21  
Updating SonicWALL Anti-Spyware Signatures ............................................... 21  

## Configuring Global, Category, and Signature Level Policies

............................................................................................................................... 22
Preface

Copyright Notice

© 2005 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.


Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.
DISCLAIMER OF LIABILITY. SONICWALL’S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.
About this Guide

Welcome to the SonicWALL Anti-Spyware Service Administrator’s Guide. This manual provides the information you need to successfully activate, configure, and administer SonicWALL Anti-Spyware Service on a SonicWALL security appliance running SonicOS Standard 3.1 (or higher) or SonicOS Enhanced 3.1 (or higher). The intended audience for this guide is users that are familiar with the basic features, functions, and operating characteristics of SonicWALL security appliances.

**Note:** This guide assumes your SonicWALL security appliance is operational with Internet connectivity. If your SonicWALL security appliance is not setup, refer to the Getting Started Guide for your SonicWALL security appliance available on the SonicWALL Web site: <http://www.sonicwall.com/support/documentation.html>

SonicWALL Anti-Spyware is part of the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service unified threat management solution that provides comprehensive protection against spyware, viruses, worms, Trojans, and software vulnerabilities.

**Note:** Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL Web site: <http://www.sonicwall.com/support/documentation.html>

Guide Conventions

Conventions used in this guide are as follows:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Highlights items on the SonicWALL Management Interface you can select, or keywords you need to enter to complete a configuration.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Highlights an argument or parameter value to enter into a field. For example, “type 192.168.168.168 in the IP Address field.”</td>
</tr>
<tr>
<td><strong>Top Level Menu Button &gt; Submenu Item</strong></td>
<td>Indicates a multiple step in the SonicWALL security appliance’s management interface menu choice. For example, <strong>Security Services &gt; Anti-Spyware</strong> means select the <strong>Security Services</strong> top-level menu item, then select the <strong>Anti-Spyware</strong> submenu item to display the <strong>Anti-Spyware</strong> page in the SonicWALL management interface.</td>
</tr>
</tbody>
</table>
Icons Used in this Guide
The graphical icons used in this guide refer to noteworthy information, and include a symbol for quick identification:

⚠️ **Alert!** Important information that cautions features affecting firewall performance or security features.

💡 **Tip!** Useful recommendation about features and configurations of SonicWALL Anti-Spyware or your SonicWALL security appliance.

📝 **Note:** Callout important information on a feature that requires special attention or reference to other related resources.

**SonicWALL Technical Support**
For timely resolution of technical support questions, visit <http://www.sonicwall.com/support/index.html>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL Telephone support, see the telephone numbers listed below:

**North America Telephone Support**
U.S./Canada - 888.777.1476

**International Telephone Support**
- **Australia** - +1.800.35.1642
- **Austria** - + 43(0)820.400.105
- **EMEA** - +31(0)411.617.810
- **France** - + 33(0)1.4933.7414
- **Germany** - + 49(0)1805.0800.22
- **Hong Kong** - + 1.800.93.0997
- **India** - + 1.600.44.9255
- **Italy** - +39.02.7541.9803
- **Japan** - + 81(0)3.5460.5356
- **New Zealand** - + 0800.446489
- **Singapore** - + 800.110.1441
- **Spain** - + 34(0)9137.53035
- **Switzerland** - +41.1.308.3.977
- **UK** - +44(0)1344.668.484

📝 **Note:** Visit <http://www.sonicwall.com/services/contact.html> for the latest Technical Support telephone numbers.
Deploying SonicWALL Anti-Spyware

SonicWALL Anti-Spyware is designed to provide comprehensive protection with minimal configuration as well as provide more advanced granularity features for tailoring intrusion prevention based on your network requirements. The following sections provide the key information you need to successfully activate, configure, and administer SonicWALL IPS on a SonicWALL security appliance running SonicOS Standard 3.1 (or higher) or SonicOS Enhanced 3.1 (or higher):

Table 1: SonicWALL Anti-Spyware Deployment Procedures

<table>
<thead>
<tr>
<th>Document Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“SonicWALL Anti-Spyware Overview” on page 6</td>
<td>Presents an overview of SonicWALL Anti-Spyware capabilities and how it works as part of SonicWALL’s Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service unified threat management solution</td>
</tr>
<tr>
<td>“Activating the SonicWALL Anti-Spyware License” on page 12</td>
<td>Provides instructions for activating the SonicWALL Anti-Spyware license on your SonicWALL security appliance as part of the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service license. If you already have SonicWALL IPS activated on your SonicWALL security appliance, skip this section.</td>
</tr>
<tr>
<td>“Setting Up SonicWALL Anti-Spyware Protection” on page 18</td>
<td>Provides procedures to set up SonicWALL Anti-Spyware to enable anti-spyware protection against the most dangerous and disruptive spyware applications on your network.</td>
</tr>
<tr>
<td>“Configuring Global, Category, and Signature Level Policies” on page 22</td>
<td>Provides instructions for configuring anti-spyware protection at the global, signature category, and individual signature level to provide flexible granularity for tailoring SonicWALL Anti-Spyware protection based on your network environment.</td>
</tr>
<tr>
<td>“Configuring Client Alerts and Exclusions” on page 29</td>
<td>Provides procedures to configure client alerts when SonicWALL Anti-Spyware blocks traffic and specifying IP addresses for exclusion from SonicWALL Anti-Spyware protection.</td>
</tr>
<tr>
<td>“Specifying Protocol Inspections” on page 30</td>
<td>Describes the protocol handling capabilities of SonicWALL Anti-Spyware for detecting and responding to spyware traffic on supported protocols (HTTP, FTP, IMAP, SMTP and POP3). Includes instructions for specifying protocols, as well as configuring filtering for outbound spyware communications.</td>
</tr>
</tbody>
</table>

Note: This guide assumes your SonicWALL security appliance is operational with Internet connectivity. If your SonicWALL security appliance not setup, refer to the Getting Started Guide for your SonicWALL security appliance available the SonicWALL Web site: <http://www.sonicwall.com/support/documentation.html>
SonicWALL Anti-Spyware Overview

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.

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 program, such as programs 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.

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’s Unified Threat Management Solution

Utilizing SonicWALL’s configurable, high-performance Deep Packet Inspection architecture, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service secures the network from the core to the perimeter against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, and remote exploitation of software vulnerabilities, such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code. Because new threats emerge daily and are often unpredictable, the deep packet inspection architecture is constantly updated to deliver the highest protection against an ever-changing threat landscape.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service inspects e-mail, Web traffic, file transfers, a multitude of stream-based protocols, as well as instant messaging and peer-to-peer applications. Because files containing malicious code, viruses and worms can be compressed and therefore inaccessible to conventional solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis. Supported compression formats include ZIP, Deflate, GZIP and packed executables. As an added layer of security, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection not only against external threats, but also against those originating inside the network.

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 interface 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.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service running on multiple SonicWALL security appliances can be managed by SonicWALL Global Management System (SonicWALL GMS) from a central location. SonicWALL ViewPoint solutions allow administrator’s to create detailed reports of network activities.

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Security Services

- **Integrated Deep Packet Inspection Technology** - features a configurable, high-performance Deep Packet Inspection architecture that uses parallel searching algorithms up through the application layer to deliver complete application layer, Web and e-mail attack prevention. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Spyware Protection** - prevents malicious spyware from infecting networks by blocking spyware installations at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- **Real-Time AV Gateway Scanning** - 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** - delivers 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.
- **Scalability and Performance** - utilizes a per packet scanning engine, allowing the SonicWALL unified threat management solution to handle unlimited file size and virtually unlimited concurrent downloads.
- **Day Zero Protection** - ensures fast time-to-protection by employing a dynamically updated database of signatures created by a combination of SonicWALL’s SonicAlert Team and third-party sources.
• **Extensive Signature List** - utilizes an extensive database of thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, spyware, worms, Trojans, application exploits, and malicious applications.

• **Distributed Enforcement Architecture** - 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** - 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** - 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** - 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** - 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** - 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** - 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** - 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.
How SonicWALL’s Deep Packet Inspection Architecture Works

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service is built on SonicWALL’s Deep Packet Inspection technology that enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. SonicWALL’s Deep Packet Inspection Engine version 2.0 enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

SonicWALL DEEP PACKET INSPECTION ARCHITECTURE

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 could even 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.

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

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 could even 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.

If TCP packets arrive out of order, the SonicWALL IPS engine reorders them before inspection. However, SonicWALL’s IPS framework supports complete signature matching across the TCP fragments without having to perform complete reassembly. SonicWALL’s unique reassembly-free matching solution dramatically reduces CPU and memory resource requirements.

SonicWALL’s Deep Packet Inspection architecture incorporates detection and prevention capabilities. Detection finds anomalies in the traffic and alerts the administrator. Prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.
Deep Packet Inspection 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 SonicWALL security appliance to detect and log intrusions that pass through it, 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.

Because of the feature enhancements in the Deep Packet Inspection Engine version 2.0 (DPIv2.0), platform dependent concurrency limitations for TCP stream processing are as follows:

<table>
<thead>
<tr>
<th>Platform</th>
<th>SonicWALL GAV/Anti-Spyware/IPS-Disabled Connection Cache Size</th>
<th>SonicWALL GAV/Anti-Spyware/IPS-Enabled Connection Cache Size</th>
<th>SonicWALL IPS Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>TZ 150 Series</td>
<td>2,048</td>
<td>2,048</td>
<td>4,500</td>
</tr>
<tr>
<td>TZ 170 Series</td>
<td>6,144</td>
<td>6,144</td>
<td>4,500</td>
</tr>
<tr>
<td>PRO 1260</td>
<td>6,144</td>
<td>6,144</td>
<td>4,500</td>
</tr>
<tr>
<td>PRO 2040</td>
<td>32,768</td>
<td>16,384</td>
<td>25,000</td>
</tr>
<tr>
<td>PRO 3060</td>
<td>131,072</td>
<td>65,536</td>
<td>25,000</td>
</tr>
<tr>
<td>PRO 4060</td>
<td>524,288</td>
<td>131,072</td>
<td>25,000</td>
</tr>
<tr>
<td>PRO 5060</td>
<td>750,000</td>
<td>393,216</td>
<td>25,000</td>
</tr>
</tbody>
</table>

Only TCP traffic is bound by stream concurrency; UDP traffic is continually inspected in a connectionless packet-by-packet basis up to the connection cache limit. If the TCP concurrency limit is reached, all traffic will continue to be inspected, but the state machine with neither reorder over-limit fragments, nor will it span over-limit packets for signature matching.
Inbound and Outbound Protection

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Service are applied to both inbound and outbound traffic, because signatures are written directionally. That is, the direction of the attack is considered when applying protection on a SonicWALL security appliance.

For example, the Sasser worm. SonicWALL signatures were written to examine different stages and directions of this complex attack. One signature looked for a NetBIOS buffer overflow attack that uses the common NetBIOS ports as an exploit. This SonicWALL signature is applied inbound between zones (SonicOS Enhanced) and interfaces (SonicOS Standard) from the Internet, effectively stopping the proliferation of the exploit from the external network. After the initial exploit, the Sasser worm attempts to download the main part of its program through an FTP session out to the Internet.

Another SonicWALL signature automatically prevents Sasser from establishing an outbound FTP session to the Internet, and it may be applied to each zone or interface.

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service does not require you to understand what signatures are applied in what directions. You simply select predefined groups based on the severity of the attacks or the danger level of the spyware.

Disabling the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Engine

In the unlikely event that SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service are not enabled on your SonicWALL security appliance, you can disable the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service engine to reallocate resources to the SPI (Security Parameter Index) connection cache.

To disable the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service engine:

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

2. Select the **Disable Anti-Spyware, Gateway AV and IPS Engine (increases maximum SPI connections)** checkbox. An alert is displayed informing you that the SonicWALL security appliance must be rebooted for the change to take effect.

3. Restart your SonicWALL security appliance.
Activating the SonicWALL Anti-Spyware License

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the Security Services > Anti-Spyware page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

SonicWALL Anti-Spyware is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, so you use a single parent License Key to activate all three services on your SonicWALL security appliance. You activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service parent license for SonicWALL Intrusion Prevention Service first from the Security Services > Intrusion Prevention page. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicOS Standard 3.1 or SonicOS Enhanced 3.1.** Your SonicWALL security appliance must be running SonicOS Standard 3.1 or SonicOS Enhanced 3.1 for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. If you do not have SonicOS 3.1 installed on your SonicWALL security appliance, refer to the SonicOS Standard or Enhanced Administrator's Guide available on the SonicWALL Web site <http://www.sonicwall.com/support/documentation.html> for SonicOS upgrade instructions.

- **mySonicWALL.com account.** A mySonicWALL.com account allows you to manage your SonicWALL products. You need to register your SonicWALL security appliance to activate SonicWALL security services. Creating a mySonicWALL.com is fast, simple, and FREE. Simply complete an online registration form directly from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser.

- **Registered SonicWALL Security Appliance with Active Internet Connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface. Once your SonicWALL security appliance is registered, you can activate your SonicWALL security service using an activation key. If your SonicWALL security appliance is registered and running SonicOS Standard/Enhanced 3.1, and you have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation Key, proceed to “Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License” on page 15.

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada). After purchasing the license, you are provided with an Activation Key. You use this Activation Key to activate the service on your SonicWALL security appliance.

---

**Tip!** If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Virus, and SonicWALL Intrusion Prevention Service separately from the Security Services > Gateway Anti-Virus, Security Services > Anti-Spyware, and Security Services > Intrusion Prevention pages in the management interface.
Creating a mySonicWALL.com Account

To create a mySonicWALL.com account:

1. Log into the SonicWALL security appliance management interface.

2. If the **System > Status** page is not displayed 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 in **Your SonicWALL is not registered. Click here to Register your SonicWALL**.

4. 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**.

5. 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.

   **Note:** *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.
Registering Your SonicWALL Security Appliance

You need to register your SonicWALL security appliance to activate SonicWALL security services. If your SonicWALL security appliance is not registered, the Security Services section on the System > Status page displays the message: Your SonicWALL is not registered. Click here to Register your SonicWALL.

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.
   - **Anti-Spyware** - protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts outbound spyware communications.

   Click Continue on each page.

   **Note:** Clicking on the Continue button does not activate the FREE TRIAL versions of these SonicWALL Security Services. You must activate these free trials from the System > Licenses 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.
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License

Since SonicWALL Anti-Spyware is part of SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

⚠️ **Alert!** After activating your SonicWALL Anti-Spyware license, you must enable and configure SonicWALL Anti-Spyware on the SonicWALL management interface before anti-spyware policies are applied to your network traffic.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account.

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

1. On the Security Services > Intrusion Prevention page, click the SonicWALL Intrusion Prevention Service Subscription link. The mySonicWALL.com Login page is displayed.

2. Enter your mySonicWALL.com account username and password in the User Name and Password fields, then click Submit. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the System > Licenses page appears.

3. Click Activate or Renew in the Manage Service column in the Manage Services Online table.
4. Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

5. Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

6. Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

7. Click on the SonicWALL Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

8. Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service on mySonicWALL.com

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on your mySonicWALL.com account <https://www.mysonicwall.com>, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the Synchronize button on the Security Services > Summary page to immediately update your SonicWALL security appliance.

Activating FREE TRIALs

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the System > Licenses page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. Security Services > Gateway Anti-Virus).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

1. Click the FREE TRIAL link on the Security Services > Gateway Anti-Virus, Security Services > Anti-Spyware, or Security Services > Intrusion Prevention page. The mySonicWALL.com Login page is displayed.

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

3. Click Try in the FREE TRIAL column in the Manage Services Online table. The service is enabled on your security appliance.
Setting Up SonicWALL Anti-Spyware Protection

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

1. Enable SonicWALL Anti-Spyware on your SonicWALL security appliance
2. Specify Global Spyware Danger Level Protection
3. Apply SonicWALL Anti-Spyware Protection to Interfaces or Zones

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

Selecting **Security Services > 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 product or manufacturer.

**Alert!** *After activating your SonicWALL Anti-Spyware license, 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 Enable Anti-Spyware check box (a checkmark is displayed), and then click Apply.

Alert! Checking the Enable Anti-Spyware check box does not automatically start SonicWALL Anti-Spyware protection. You must also select a Prevent All action in the Signature Groups table to activate anti-spyware prevention at the global level on the SonicWALL security appliance, and then specify the interfaces or zones you want to protect. You can also select Detect All for spyware event logging and alerting.

Specifying Spyware Danger Level Protection

SonicWALL Anti-Spyware allows you to globally manage your network protection against spyware 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 and disruptive spyware. You can also enable Detect All for spyware logging and alerting.

Tip! 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 or intrusive 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. Refer to “Configuring Global, Category, and Signature Level Policies” on page 22 for more information.
Applying SonicWALL Anti-Spyware Protection to Zones for SonicOS Enhanced

If your SonicWALL security appliance is running SonicOS Enhanced, you apply SonicWALL Anti-Spyware to Zones on the Network > Zones page to enforce SonicWALL Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL Anti-Spyware on the LAN zone enforces SonicWALL Anti-Spyware on all incoming and outgoing LAN traffic.

To enable SonicWALL Anti-Spyware policies on a zone:

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

2. In the Configure column in the Zone Settings table, click the edit icon for the zone you want to apply SonicWALL Anti-Spyware. The Edit Zone window is displayed.

3. Click the Enable Anti-Spyware Service checkbox. A checkmark appears. To disable SonicWALL Anti-Spyware Service, uncheck the box.

4. Click OK.

You also enable SonicWALL Anti-Spyware 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.

Applying SonicWALL Anti-Spyware Protection on Interfaces for SonicOS Standard

If your SonicWALL security appliance is running SonicOS Standard, you also need to specify the interface that you want to enable SonicWALL Anti-Spyware 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.
Understanding SonicWALL Anti-Spyware Status Information

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

<table>
<thead>
<tr>
<th>Anti-Spyware Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signature Database</strong>: Not Downloaded</td>
</tr>
<tr>
<td><strong>Signature Database Timestamp</strong>: UTC 01/01/00 00:00:00:00</td>
</tr>
<tr>
<td><strong>Last Checked</strong>: 03/01/00 13:22:42,64</td>
</tr>
<tr>
<td><strong>Anti-Spyware Expiration Date</strong>: 01/01/2006</td>
</tr>
</tbody>
</table>

- **Signature Database** - indicates the signature database has been downloaded to the SonicWALL security appliance.
- **Signature Database Timestamp** - displays the date and time the signature database was last updated. The **Signature Database Timestamp** is a timestamp for updates to the SonicWALL Anti-Spyware signature database not the last update to the SonicWALL security appliance.
- **Last Checked** - displays the last time the SonicWALL security appliance checked for signature updates.
- **Anti-Spyware Expiration Date** - displays your SonicWALL Anti-Spyware license expiration date. If your SonicWALL Anti-Spyware subscription expires, the SonicWALL Anti-Spyware inspection is stopped and the SonicWALL Anti-Spyware configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL Anti-Spyware license to the previously configured state.

If your SonicWALL security appliance is running SonicOS Standard, you may see the message **Warning: No Interfaces have Anti-Spyware enabled**, if you have not enabled SonicWALL Anti-Spyware protection to any interfaces. You enable SonicWALL Anti-Spyware on the SonicWALL interfaces in the **Anti-Spyware Global Settings** section.

If your SonicWALL security appliance is running SonicOS Enhanced, the following message is displayed in the **Anti-Spyware Status** section: **Note: Enable the Anti-Spyware per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying Anti-Spyware policies on Zones. If no Anti-Spyware policies have been applied to any Zones, a warning message is displayed at the bottom of the **Anti-Spyware Status** section: **Warning: No Zones have Anti-Spyware enabled**.

**Updating SonicWALL Anti-Spyware Signatures**

By default, the SonicWALL security appliance running SonicWALL Anti-Spyware automatically checks the SonicWALL signature servers once an hour.

You can force a check of the SonicWALL Anti-Spyware signatures database for updates at any time by clicking the **Update** button located in the **Anti-Spyware Status** section.

SonicWALL Anti-Spyware 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.

**Note**: Clicking the **Update** button checks the SonicWALL signature servers and updates all Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service signatures.
Configuring Global, Category, and Signature Level Policies

SonicWALL Anti-Spyware allows you to override global and category spyware prevention and detection levels to provide flexible granularity for tailoring SonicWALL Anti-Spyware protection based on your network environment requirements.

- **Global** - SonicWALL Anti-Spyware protection includes global **High Danger Level Spyware**, **Medium Danger Level Spyware**, and **Low Danger Level Spyware** signature groups available in the **Signature Groups** table. These global signature groups organize signatures within these classes to provide an easy-to-deploy and comprehensive intrusion prevention solution. Refer to “Configuring Global Signature Groups” on page 22 for instructions on configuring global signature groups.

- **Category** - SonicWALL Anti-Spyware organizes signatures into categories based on spyware product or manufacturer categories. These categories include signatures with high, medium, and low danger levels. You configure these categories to override the global prevention and/or detection settings. Refer to “Configuring Category Policies” on page 26 for instructions on configuring signature categories.

- **Signature** - SonicWALL Anti-Spyware provides maximum granularity by allowing you to override SonicWALL Anti-Spyware category prevention and detection settings for individual signatures. Refer to “Configuring Signature Policies” on page 27 for instructions on configuring signatures.

You can display all the categories and signatures in the **Anti-Spyware Policies** table. The number of category and signature entries in the **Anti-Spyware Policies** table change as new signatures are added to the SonicWALL Anti-Spyware signature database.

---

**Note:** You cannot add custom signatures to the SonicWALL Anti-Spyware database or modify existing signatures.

---

Configuring Global Signature Groups

SonicWALL Anti-Spyware allows you to globally prevent and/or detect attacks based on the following attack levels listed in the **Signature Groups** table:

- **High Danger Level Spyware** - These spyware applications are the most dangerous to your network, such as keyloggers or porn dialers, or may contain security vulnerabilities. Removal may be extremely difficult or impossible.

- **Medium Danger Level Spyware** - These spyware applications can cause disruption to your network, such as increased network traffic that slows down performance. Removal may be extremely difficult.

- **Low Danger Level Spyware** - These spyware applications are characterized by less intrusive activity and are not an immediate threat. They may profile users and usually are simple to remove.

---

**Tip!** SonicWALL recommends enabling Prevent All for **High Danger Level Spyware** and **Medium Danger Level Spyware** to provide network protection against the most damaging spyware.

SonicWALL Anti-Spyware provides two methods for managing global spyware threats: detection (Detect All) and prevention (Prevent All). You must specify a Prevent All action in the **Signature Groups** table for anti-spyware to occur on a global level on the SonicWALL security appliance.

When Prevent All is enabled for a signature group in the **Signature Groups** table, the SonicWALL security appliance automatically drops and resets the connection, to prevent the traffic from reaching its destination.
When **Detect All** is enabled for a signature group in the **Signature Groups** table, the SonicWALL security appliance logs and alerts any traffic that matches any signature in the group, but does not take any action against the traffic. The connection proceeds to its intended destination. You view the SonicWALL log on the **Log > View** page as well as configure how alerts are handled by the SonicWALL security appliance in the **Log > Automation** page.

**Alert!** Be careful when selecting only **Detect All**. Selecting only **Detect All** logs and alerts on traffic that matches any signature in the group, but does not take any action against the traffic. The traffic proceeds to its intended destination.

When **Detect All** and **Protect All** are both enabled for a signature group in the **Signature Groups** table, the SonicWALL logs and alerts on traffic that matches any signature in the group, and automatically drops and resets the connection to prevent the traffic from reaching its destination.

**Log Redundancy Filter**

The **Log Redundancy Filter (seconds)** field allows you to define the time in seconds that the same attack is logged as a single entry in the SonicWALL log. Various spyware communications are often rapidly repeated, which can quickly fill up a log if each attack is logged. The default 60 seconds entry for **Low Priority Attacks** in the **Log Redundancy Filter (seconds)** field is recommended because the relatively high volume of these types of signature triggers. You can view and manage the SonicWALL log events by clicking on the **Log** button in the Management Interface. The **Log > View** page displays the log contents.

**Tip!** For the more critical **High Danger Level Spyware** and **Medium Danger Level Spyware** applications, it is recommended you use the default 0 setting to deal with the threat immediately.

**Resetting SonicWALL Anti-Spyware Configuration to Default Settings**

Clicking the **Reset Anti-Spyware Settings and Policies** button resets all the SonicWALL Anti-Spyware settings to the default global settings. It removes all custom SonicWALL Anti-Spyware signature settings you created in the **Edit Anti-Spyware Category** and **Edit Anti-Spyware Signature** windows as well as reset global **Prevent All** and **Detect All** settings and **Log Redundancy Filter (seconds)** settings in the **Signature Group** table.
Managing Category and Signature Policies

The Anti-Spyware Policies section allows you to view and manage how SonicWALL Anti-Spyware handles signatures by category groups or on a signature by signature basis. Categories are signatures grouped together by product or manufacturer, and they are listed in the View Style menu.

Displaying Categories and Signatures

You can display the signatures in a variety of views using the View Style menu. This menu allows you to specify the categories or signatures to display in the Anti-Spyware Policies table. You can select All Signatures, or by the first number or letter in the spyware name.

Selecting All Signatures from the menu displays all of the signatures by category. The Anti-Spyware Policies table displays all the categories and their signatures. The category headers divide the signature entries. These headers display Global in the Prevent and Detect columns, indicating the global settings you defined in the Anti-Spyware Global Settings section.
Anti-Spyware Policies Table

The Anti-Spyware Policies table displays the following information about each signature entry:

- **Product** - Displays the spyware name or manufacturer.
- **Name** - Displays the name of the spyware as a link. Clicking the name link displays the SonicAlert information about the spyware.
- **ID** - The SonicWALL database ID number of signature.
- **Detect** - A check mark in this column indicates detection is enabled. A green check mark ✔ appears in the Detect column any time you make a change from the global or category detection settings.
- **Prevent** - A check mark in this column indicates prevention is enabled. A green check mark ✔ appears in the Detect column any time you make a change from the global or category prevention settings.
- **Danger Level** - Defines the attack signature as **Low**, **Medium**, or **High** as defined for the Signature Groups table.
- **Configure** - Clicking the edit icon in the Configure column of the category header displays the Edit Anti-Spyware Category window. Clicking the edit icon in the Configure column for an individual signature displays the Edit Anti-Spyware Signature window. These windows allow you to define a different action from the global settings for the specific category or signature.

Displaying Spyware Information

In the Anti-Spyware Policies table, clicking on the spyware name link in Name column, displays a SonicALERT page that provides detailed information about the spyware.

Navigating the Anti-Spyware Policies Table

The **Items** field displays the table number of the first category or signature. If you are displaying the first page of a table, the entry might be **Items** 1 to 50 (of 58). You can enter a number in the **Items** field to go directly to a specific entry or use the navigation buttons to navigate the table.

![Items](1.png)

The SonicWALL Anti-Spyware signatures are displayed fifty to a page in the Anti-Spyware Policies table.

---

**Note:** You can change the default 50 entries per page table display on the System > Administration page in the Web Management Settings section.

Searching the Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking **Search** icon.

Sorting Category or Signature Entries

Clicking on the Anti-Spyware Policies table headings (Name, ID, Prevent, Detect, or Danger Level) sorts the table entries according to the heading. An up arrow by the column header name indicates the entries are sorted descending order. A down arrow by the column header name indicates the entries are sorted in ascending order.
Configuring Category Policies

You can choose to override the global prevention and detection settings on a category-by-category basis. The global Prevent All and Detect All settings, which include High Danger Level Spyware, Medium Danger Level Spyware, and Low Danger Level Spyware are configured in the Anti-Spyware Global Settings section. Categories can include any combination Danger Levels as defined in the Signature Groups table.

The available signature categories are listed in the View Style menu in the Anti-Spyware Policies section. Configuring the prevent and detect behaviors on a category basis affects all the signatures in the category, regardless of the global attack priority settings (Low, Medium, or High)

Overriding Global Prevent and Detect Settings by Category in SonicOS Standard

1. Select All categories or an individual category from the Category menu.
2. If you select All categories, click on the edit icon in the Configure column for the category you want to change. The Edit Anti-Spyware Category window is displayed.
3. If you select an individual category, click on the edit icon to the right of the Category menu. The Edit Anti-Spyware Category window is displayed.
4. If you want to change the Global Setting for Prevention, select Enable or Disable from the Prevention menu.
5. If you want to change the Global Setting for Detection, select Enable or Disable from the Detection menu.
6. If you want to change the Global Settings for both detection and prevention, select Enable or Disable from the Detection and Prevention menu.
7. If you want to change the Log Redundancy Filter setting from the default global setting, uncheck the Use Category Settings box for Log Redundancy Filter (seconds) and enter a time value in seconds.
8. Click OK to save your changes.

Tip! If you select All signatures from the Category menu, all the categories and their signatures are displayed in the Anti-Spyware Policies table, allowing you to configure both the category and signatures within the category.

Overriding Global Prevent and Detect Settings by Category in SonicOS Enhanced

1. Select All categories or an individual category from the Category menu.
2. If you select All Categories, click on the edit icon in the Configure column for the category you want to change. The Edit Anti-Spyware Category window is displayed.
3. If you select an individual category, click on the edit icon to the right of the Category menu. The Edit Anti-Spyware Category window is displayed.
4. If you want to change the Global Setting for Prevention, select Enable or Disable from the Prevention menu.
5. If you want to change the Global Setting for Detection, select Enable or Disable from the Detection menu.
6. If you want to change the Global Settings for both detection and prevention, select Enable or Disable from the Detection and Prevention menu.
7. The following settings allow you to select specific users/groups, IP address ranges, and schedule objects to be included or excluded from this SonicWALL Anti-Spyware category:

   **Included Users/Groups** - select the Users/Groups you want included in this SonicWALL Anti-Spyware category. The default is **All**.

   **Excluded Users/Groups** - select the Users/Groups you want excluded from this SonicWALL Anti-Spyware category. The default **None**.

   **Included IP Address Range** - select the IP address range you want excluded from this SonicWALL Anti-Spyware category. The default **All**.

   **Excluded IP Address Range** - select the IP address range you want excluded from this SonicWALL Anti-Spyware category. The default **None**.

   **Schedule** - select the scheduled time you want for the activation of this SonicWALL Anti-Spyware category. The default **Always on**.

8. If you want to change the Log Redundancy Filter setting from the default global setting, uncheck the **Use Category Settings** box for **Log Redundancy Filter (seconds)** and enter a time value in seconds.

9. Click **OK** to save your changes.

---

**Tip!**
If you select **All signatures** from the **Category** menu, all the categories and their signatures are displayed in the **Anti-Spyware Policies** table, allowing you to configure both the category and signatures within the category.

---

**Resetting SonicWALL Anti-Spyware Configuration to Default**
You can remove all custom category and signature settings you created as well as reset global **Prevent All** and **Detect All** settings and **Log Redundancy Filter (seconds)** settings by clicking the **Reset Anti-Spyware Settings & Policies** button in the **Anti-Spyware Global Settings** section.

**Configuring Signature Policies**
Selecting **All signatures** from the **Category** menu displays all of the signatures organized within categories. The **All signatures** option displays every signature in the Anti-Spyware database.

If global **Prevent All** and **Detect All** settings are in effect for the category, **Global** is displayed in the **Prevent** and **Detect** columns for the category and all of its signatures.

Selecting a specific signature category, displays the signatures in that category.

---

**Note:** You cannot import your own customized signatures into SonicWALL Anti-Spyware or delete a signature entry.

**Alert!** Use caution when overriding global **High Danger Level Spyware** and **Medium Danger Level Spyware** signature behaviors because you can create vulnerabilities. If you make changes and want to restore the default global signature settings, click the **Reset Anti-Spyware Settings & Policies** button to restore the default settings.
Overriding Category Detect and Prevent Settings for a Signature in SonicOS Standard

To override category detect and prevent attributes for signatures, perform these steps:

1. In the Anti-Spyware Policies table, display the signature you want to change, click the edit icon in the Configure column for the entry to display the Edit Anti-Spyware Signature window.
2. If you want to change the Category Setting for Prevention, select Enable or Disable from the Prevention menu.
3. If you want to change the Category Setting for Detection, select Enable or Disable from the Detection menu.
4. If you want to change the Category Setting for both detection and prevention, select Enable or Disable from the Detection and Prevention menu.
5. If you want to change the Log Redundancy Filter setting from the Category setting, uncheck the Use Category Settings box for Log Redundancy Filter (seconds) and enter a time value in seconds.
6. Click OK to save your changes.

Overriding Category Detect and Prevent Settings for a Signature in SonicOS Enhanced

To override category detect and prevent attributes for signatures, perform these steps:

1. In the Anti-Spyware Policies table, display the signature you want to change, click the edit icon in the Configure column for the entry to display the Edit Anti-Spyware window.
2. If you want to change the Category Setting for Prevention, select Enable or Disable from the Prevention menu.
3. If you want to change the Category Setting for Detection, select Enable or Disable from the Detection menu.
4. If you want to change the Category Setting for both detection and prevention, select Enable or Disable from the Detection and Prevention menu.
5. The following settings allow you to select specific users/groups, IP address ranges, and schedule objects to be included or excluded from this SonicWALL Anti-Spyware signature:
   - Included Users/Groups - select the Users/Groups you want included in this SonicWALL Anti-Spyware signature. The default is All.
   - Excluded Users/Groups - select the Users/Groups you want excluded from this SonicWALL Anti-Spyware signature. The default None.
   - Included IP Address Range - select the IP address range you want excluded from this SonicWALL Anti-Spyware signature. The default All.
   - Excluded IP Address Range - select the IP address range you want excluded from this SonicWALL Anti-Spyware signature. The default None.
   - Schedule - select the scheduled time you want for the activation of this SonicWALL Anti-Spyware signature. The default Always on.
6. If you want to change the Log Redundancy Filter setting from the Category setting, uncheck the Use Category Settings box for Log Redundancy Filter (seconds) and enter a time value in seconds.
7. Click OK to save your changes.

Resetting SonicWALL Anti-Spyware Settings to Default

You can removes all custom category and signature settings you created as well as reset global Prevent All and Detect All settings and Log Redundancy Filter (seconds) settings by clicking the Reset Anti-Spyware Settings & Policies button in the Anti-Spyware Global Settings section.
Alert! Use caution when changing the global settings for individual spyware signatures because they override the global settings, which may result in creating exposure.

Configuring Client Alerts and Exclusions

Clicking the Configure Anti-Spyware Settings button in the Anti-Spyware Global Settings section displays the Anti-Spyware Config View window, which allows you to configure SonicWALL Anti-Spyware client notification settings and exclusion list.

Configuring Client Alerts

If you want clients on your network to receive notifications on their desktop when spyware content is blocked by SonicWALL Anti-Spyware, check the Enable Client Notification Alerts (desktop client installation is required) box.

Note: You must install the client software to receive these notifications from SonicWALL Anti-Spyware. This client software will be available in the near future.

If you want to suppress the sending of e-mail messages (SMTP) to clients from SonicWALL Anti-Spyware when a spyware is detected in an e-mail or attachment, check the Disable SMTP Responses box.
Configuring an Exclusion List

If you want to specify IP addresses to exclude from intrusion detection and prevention, you can create a SonicWALL Anti-Spyware exclusion list in the Anti-Spyware Config View window:

1. Click Configure Anti-Spyware Settings in the Anti-Spyware Global Settings section. The Anti-Spyware Config View window
2. In the Anti-Spyware Exclusion List section, click the Enable Anti-Spyware Exclusion List checkbox to enable the exclusion list.
3. Click the Add button. The Add Anti-Spyware Range Entry window is displayed.

4. Enter the IP address range in the IP Address Form and IP Address To fields, then click OK. You IP address range appears in the Anti-Spyware Exclusion List table. Click the edit icon in the Configure column to change an entry or click the delete (Trashcan) icon to delete an entry.
5. Click OK to exit the Anti-Spyware Config View window.

Specifying Protocol Inspections

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

If configured in the Anti-Spyware Config View window, an encrypted message explaining the action is sent to the user's Global Security Client (requires version 2.0 or higher).

By default, SonicWALL Anti-Spyware inspects all inbound HTTP, FTP, IMAP, SMTP and POP3 traffic. If malicious traffic is detected, appropriate actions are taken based on the protocol. SonicWALL Anti-Spyware also inspects outbound spyware communication through these protocols. The protocol filtering setting are located in the Anti-Spyware Global Settings section below the Signature Groups table.

How SonicWALL Anti-Spyware Handles Protocol Inspections and Actions

The following describes the protocol handling capabilities of SonicWALL Anti-Spyware for the supported protocols:

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

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.

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.

- **Disable Anti-Spyware 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 e-mails.
- **Disable Anti-Spyware 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.

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

Within the context of SonicWALL Anti-Spyware, 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:

<table>
<thead>
<tr>
<th>From</th>
<th>Trusted</th>
<th>Encrypted</th>
<th>Wireless</th>
<th>Public</th>
<th>Untrusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Encrypted</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wireless</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Untrusted</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Enabling Inspection of Outbound Spyware Communication

The Enable Inspection of Outbound Spyware Communication feature is available for scanning outbound traffic for spyware communication.

Note: See the Administrator’s Guide for your SonicWALL security appliance for more information on managing the SonicWALL security appliance’s log located on the SonicWALL Web site <http://www.sonicwall.com/support/documentation.html>.
Applying SonicWALL Anti-Spyware Protection to Encrypted VPN Traffic

You can enforce Anti-Spyware policies on traffic coming in to your networks from VPN tunnels at the point of entry for the unencrypted data from the VPN tunnel. SonicWALL Anti-Spyware cannot perform inspection on any encrypted traffic that is in transit through the SonicWALL security appliance. However, the SonicWALL security appliance can perform SonicWALL Anti-Spyware inspection on any VPN tunnel that terminates directly on the SonicWALL security appliance. SonicWALL Anti-Spyware can inspect traffic as it goes into the tunnel and/or when the traffic comes out of the tunnel. For example, if the VPN tunnel terminates and begins on the LAN, SonicWALL Anti-Spyware can inspect the traffic before and/or after it enters the VPN tunnel.

For SonicOS Standard, you must enable **Apply NAT and Firewall Rules** in the VPN Policy window’s **Advanced** tab for each VPN policy in order for SonicWALL Anti-Spyware inspection to happen on a VPN tunnel that terminates directly on the SonicWALL security appliance.

**Note:** Refer to the [SonicOS Standard or Enhanced Administrator’s Guide](http://www.sonicwall.com/support/documentation.html) for instructions on configuring VPN policies, located on the SonicWALL Web site.

Logging SonicWALL Anti-Spyware Events

If you selected **Detect All** for any of the signature groups in the **Signature Groups** table on the **Security Services > Anti-Spyware** page, any log entries associated with the signature group is displayed on the **Log > View** page.

**Note:** Refer to the [SonicOS Log Events Reference Guide](http://www.sonicwall.com/support/documentation.html) for a complete listing of SonicWALL Anti-Spyware generated log events located on the SonicWALL Web site.
Index

A
activating a free trial of SonicWALL Anti-Spyware 17
activating the license
  activation key 15
  creating a mysonicwall.com account 13
  procedures overview 12
  registering the SonicWALL security appliance 14
  SonicOS requirements 12
anti-spyware policies table 25
anti-spyware protection for encrypted VPN traffic 33

C
client alerts 29
configuring anti-spyware policies 22
  global signature groups 22

D
deep packet inspection 9
deploying SonicWALL Anti-Spyware
  procedures overview 5
detect all 23
disabling the GAV, Anti-Spyware and IPS engine 11
displaying spyware information 25

E
enabling inbound inspection 29
  exclusion list 29

H
high danger level spyware 22
how deep packet inspection works 9

I
inbound and outbound traffic protection 11

L
log redundancy filter 23
logging anti-spyware events 33
low danger level spyware 22

M
managing category and signature policies 24
medium danger level spyware 22

N
navigating the anti-spyware policies table 25

O
outbound spyware communication 32
overriding category policies by signatures 27
overriding global policies by category 26

P
prevent all 22
protocol inspections 29

R
resetting to defaults 23

S
searching signature database 25
setting up anti-spyware protection 18
  applying to SonicOS Enhanced zones 20
  applying to SonicOS Standard interfaces 20
  enabling 19
  specifying danger level protection 19
SonicWALL Anti-Spyware
  overview 6
  protects against 6
  use with other anti-spyware programs 6
SonicWALL Anti-Spyware spyware threats 6
SonicWALL Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service 7

T
Technical Support 4

U
unified threat management 7


