# Table of Contents

Preface ............................................................................................................. 1  
Copyright Notice ............................................................................................ 1  
Trademarks....................................................................................................... 1  
Limited Warranty ............................................................................................. 1  
About this Guide ................................................................................................. 3  
Guide Conventions ........................................................................................... 3  
Icons Used in this Guide .................................................................................. 3  
SonicWALL Technical Support ......................................................................... 4  
North America Telephone Support .................................................................. 4  
International Telephone Support ..................................................................... 4  
SonicWALL Intrusion Prevention Service Overview ..................................... 5  
SonicWALL Gateway Anti-Virus/Intrusion Prevention Service Features ..... 6  
What’s New in SonicWALL IPS 2.0 ................................................................. 7  
SonicWALL’s Deep Packet Inspection Technology ....................................... 7  
Disabling the SonicWALL GAV/IPS Engine ............................................... 8  
How SonicWALL’s Deep Packet Inspection Architecture Works ............ 9  
Inbound and Outbound Protection ................................................................. 10  
Deploying SonicWALL IPS ............................................................................. 10  
Activating SonicWALL IPS ............................................................................ 11  
Creating a mySonicWALL.com Account ..................................................... 12  
Registering Your SonicWALL Security Appliance ....................................... 13  
Activating SonicWALL IPS with an Activation Key .................................... 14  
Activating the SonicWALL IPS FREE TRIAL ............................................ 14  
Setting Up SonicWALL IPS Protection ............................................................ 15  
Enabling SonicWALL IPS .............................................................................. 16  
Specifying Global Attack Level Protection ............................................... 16  
Applying SonicWALL IPS Protection on Interfaces (SonicOS Standard) .... 16  
Applying SonicWALL IPS Protection on Zones (SonicOS Enhanced 3.0) .... 17  
Viewing SonicWALL IPS Status Information ............................................. 18  
Updating SonicWALL IPS Signatures ............................................................. 19  
Configuring Global, Category, and Signature Level Policies ................. 19  
Configuring Global Signature Groups ......................................................... 19  
Log Redundancy Filter .................................................................................. 20  
Resetting SonicWALL IPS Configuration to Default Settings ............... 20
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 Intrusion Prevention Service 2.0 Administrator’s Guide. This manual provides the information you need to successfully activate, configure, and administer SonicWALL Intrusion Prevention Service (SonicWALL IPS) on a SonicWALL security appliance running SonicOS Standard 3.0 (or higher) or SonicOS Enhanced 3.0 (or higher). The audience for this guide is administrators that are familiar with the 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 located on the SonicWALL Web site: <http://www.sonicwall.com/services/documentation.html>.

SonicWALL Intrusion Prevention Service is part of the SonicWALL Gateway Anti-Virus/Intrusion Prevention Service solution that provides comprehensive protection against viruses, worms, Trojans, and software vulnerabilities. When you activate SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus is also activated.


Guide Conventions

Conventions used in this guide are as follows:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Highlights items you can select on the SonicWALL Management Interface.</td>
</tr>
<tr>
<td>Italic</td>
<td>Highlights a value to enter into a field. For example, “type 192.168.168.168 in the IP Address field.”</td>
</tr>
<tr>
<td>Top Level Menu Button&gt;Submenu Item</td>
<td>Indicates a multiple step Management Interface menu choice. For example, Security Services &gt; Intrusion Prevention means select Security Services, then select Intrusion Prevention.</td>
</tr>
</tbody>
</table>

Icons Used in this Guide

These special messages refer to noteworthy information, and include a symbol for quick identification:

Alert! Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL Intrusion Prevention Service or security appliance.

Tip! Useful information about security features and configurations on your SonicWALL Intrusion Prevention Service or security appliance.
Note: Important information on a feature that requires callout for special attention or reference to other related resources.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/services/support.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 or +1 408.752.7819

**International Telephone Support**
- Australia - + 1800.35.1642
- 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 - + 8026556828
- 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: Please visit <http://www.sonicwall.com/services/contact.html> for the latest technical support telephone numbers.
SonicWALL Intrusion Prevention Service Overview

SonicWALL Intrusion Prevention Service is part of the SonicWALL Gateway Anti-Virus/Intrusion Prevention Service solution that provides comprehensive 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. When you activate SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus is also activated. SonicWALL IPS is managed directly from the SonicWALL security appliance.

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers 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.

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 administrator’s 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 Gateway Anti-Virus/Intrusion Prevention Service Features

- **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 Signature Database** - 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.

**What’s New in SonicWALL IPS 2.0**

• **IP Fragmentation** - Provides the ability to either disallow IP fragments, or to reassemble fragments for full application layer inspection.

• **Checksum Validation** - Provides the ability to detect and prevent invalid IP, ICMP, TCP, and UDP checksums.

• **Global IP Exclusion List** - Provides the ability to configure a range of IP addresses whose traffic will be excluded from SonicWALL IPS evaluation.

• **Log Redundancy Granularity** - Allows per-category and per-signature log redundancy filter settings.

• **Dynamic Categorization** - Enables signatures to be automatically grouped and displayed by expanded category views. Category maintenance is performed through automated signature updates.

• **Category and Signature User and Group Controls** - Signatures and category policies can be applied at the user or group level, overriding global settings (SonicOS Enhanced Only).

• **Category and Signature Scheduling** - The application of signatures and category policies can be controlled using schedule objects (SonicOS Enhanced Only).

• **Category and Signature Addressing** - The ability to explicitly include or exclude an Address Object from a signature or a category (SonicOS Enhanced Only).

**SonicWALL’s Deep Packet Inspection Technology**

Deep Packet Inspection 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.

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

### Disabling the SonicWALL GAV/IPS Engine

In the unlikely event that 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:

1. Select the **Firewall > Advanced** page.
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.
3. Restart your SonicWALL security appliance.
How SonicWALL’s Deep Packet Inspection Architecture Works

SonicWALL’s 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 Engine version 2.0 enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

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.
Inbound and Outbound Protection

SonicWALL IPS is applied to both inbound and outbound traffic because signatures are written directionally. That is the direction of the attack is considered when applying SonicWALL IPS protection on a SonicWALL security appliance. For example, The Sasser attack has SonicWALL signatures written to protect networks against this known threat. One signature looks for a NetBIOS buffer flow attack that uses the common NetBIOS ports as an exploit. This SonicWALL Sasser signature is automatically applied inbound between zones (SonicOS Enhanced) and interfaces (SonicOS Standard) from the Internet, effectively stopping the proliferation of the exploit. 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 Sasser signature automatically prevents an outbound FTP Sasser session to the Internet, which is applied to each zone or interface.

SonicWALL IPS doesn’t require you to understand what signatures are applied in what directions. You simply specify the Prevent All global settings for High Priority Attacks, Medium Priority Attacks, and/or Low Priority Attacks in the SonicWALL management interface.

Deploying SonicWALL IPS

SonicWALL IPS 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 3.0 (or higher) or SonicOS Enhanced 3.0 (or higher):

- “Activating SonicWALL IPS” on page 11 - provides instructions for activating the SonicWALL IPS license on your SonicWALL security appliance via the management interface. If you already have SonicWALL IPS activated on your SonicWALL security appliance, skip this section.
- “Setting Up SonicWALL IPS Protection” on page 15 - provides instructions for essential configuration of SonicWALL IPS to protect your network against the most dangerous and disruptive attacks.

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

- “Configuring Global, Category, and Signature Level Policies” on page 19 - provides instructions for configuring intrusion prevention at the global, signature category, and individual signature level to provide flexible granularity for tailoring SonicWALL IPS protection based on your network environment.
- “Managing Category and Signature Policies” on page 21 - provides configuration options for error checking of traffic, and specifying IP addresses for exclusion from intrusion detection and prevention.

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 located on he SonicWALL Web site: <http://www.sonicwall.com/services/documentation.html>.
Activating SonicWALL IPS

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

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

- **SonicWALL Gateway Anti-Virus/Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus/Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form 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.

- **SonicOS Standard 3.0 or SonicOS Enhanced 3.0.** Your SonicWALL security appliance must be running SonicOS Standard 3.0 or SonicOS Enhanced 3.0 for SonicWALL Gateway Anti-Virus/Intrusion Prevention Service.

**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 IPS.

**Note:** Refer to the SonicWALL Gateway Anti-Virus Administrator’s Guide for the information you need to successfully activate, configure, and administer SonicWALL Gateway Anti-Virus on a SonicWALL security appliance.

If you activated SonicWALL IPS at <https://www.mysonicwall.com>, SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the Synchronize button on the Security Services > Summary page to update 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.

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.

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.
Activating SonicWALL IPS with an Activation Key

If you have an Activation Key for your SonicWALL IPS, follow these steps to activate the SonicWALL IPS license on your SonicWALL security appliance:

1. Click the SonicWALL IPS Subscription link on the 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. The System > Licenses page is displayed. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the System > Licenses page appears after you click the SonicWALL IPS Subscription link.

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 IPS subscription is activated on your SonicWALL security appliance.

If you activated the SonicWALL IPS subscription on mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the Synchronize button on the Security Services > Summary page to update your SonicWALL security appliance.

Activating the SonicWALL IPS FREE TRIAL

To try a FREE TRIAL of SonicWALL IPS, follow these steps:

1. Click the FREE TRIAL 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. 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 FREE TRIAL link.

3. Click FREE TRIAL in the Manage Service column in the Manage Services Online table. Your SonicWALL IPS trial subscription is activated on your SonicWALL security appliance.

⚠️ Alert! 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.
Setting Up SonicWALL IPS Protection

There are three steps to setting up SonicWALL IPS to begin protecting your network:

1. Enable SonicWALL IPS on your SonicWALL security appliance.
2. Specify global Prevent All actions in the Signature Groups table to activate intrusion prevention filtering against High and Medium level attacks.
3. Choose the interfaces (SonicOS Standard 3.0) or zones (SonicOS Enhanced 3.0) you want to apply SonicWALL IPS protection.

Selecting Security Services > 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.

**Alert!** 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.

⚠️ Alert! Checking the Enable IPS check box does not automatically start SonicWALL IPS protection. You must also n 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” on page 19.

⚠️ Alert! Leaving the High Priority Attacks, Medium Priority Attacks, and Low Priority Attacks signature groups with no Prevent All action checked means no intrusion prevention is occurring on the SonicWALL security appliance.

SonicWALL IPS allows you to tailor these global SonicWALL IPS signature group prevention and detection settings for categories or individual signatures. Refer to “Configuring Global, Category, and Signature Level Policies” on page 19 for more information.

Applying SonicWALL IPS Protection on Interfaces (SonicOS Standard)

If your SonicWALL security appliance is running SonicOS Standard 3.0, you also need to specify the interface that you want to enable SonicWALL IPS 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.
Applying SonicWALL IPS Protection on Zones (SonicOS Enhanced 3.0)

If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you apply SonicWALL IPS to Zones on the Network > Zones page to enforce SonicWALL IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL IPS on the LAN zone enforces SonicWALL IPS on all incoming and outgoing LAN traffic.

In the IPS Status section of the Security Services > Intrusion Prevention Service page, click the Network > Zones link to access the Network > Zones page. You apply SonicWALL IPS to a zone listed on the Network > Zones page.

To enable SonicWALL on a zone, perform these steps:

1. In the SonicWALL security appliance management interface, select Network > Zones or from the IPS Status section, on the Security Services > Intrusion Prevention 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 IPS. The Edit Zone window is displayed.

3. Click the Enable IPS checkbox. A checkmark appears. To disable SonicWALL IPS, uncheck the box.

4. Click OK.
You also enable SonicWALL IPS 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.

Refer to “SonicWALL IPS Logging” on page 30 for instructions on applying Intrusion Prevention Service protection to zones.

Viewing SonicWALL IPS Status Information

The IPS 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 database version. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.

- **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 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.
- **IPS Service Expiration Date** - displays your SonicWALL IPS expiration date. If your SonicWALL IPS subscription expires, the SonicWALL IPS inspection is stopped and the SonicWALL IPS configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL IPS license to the previously configured state.

If your SonicWALL security appliance is running SonicOS Standard, the message **Warning: No Interfaces have IPS enabled.** You enable SonicWALL IPS on the SonicWALL interfaces in the IPS Settings section.

If your SonicWALL security appliance is running SonicOS Enhanced 3.0, at the bottom of the IPS Status section the following message is displayed **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 Gateway Anti-Virus on Zones.
Updating SonicWALL IPS Signatures

By default, the SonicWALL security appliance running SonicWALL IPS 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 IPS database at any time by clicking the Update button located in the IPS Status section.

SonicWALL IPS 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.

Configuring Global, Category, and Signature Level Policies

SonicWALL IPS allows you to configure intrusion prevention at the global, signature category, and individual signature level to provide flexible granularity for tailoring SonicWALL IPS protection based on your network environment.

You can create a tailored protection plan to manage your network protection against attacks using a multi-layer approach that provides you with the flexibility to adjust the level of protection based on your network environment.

- **Global** - You can configure global SonicWALL IPS protection by configuring **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**. 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 19 for instructions on configuring global signature groups.

- **Category** - SonicWALL IPS also organizes signatures based on attack categories. These signature categories are listed in the Category menu in the IPS Policies section. These categories include such attack categories as DDOS, DNS, IM, MULTIMEDIA, SMTP, WEB-ATTACKS, and others. These categories include signatures with high, medium, and low attack priorities organized by the type of attack. You configure these categories to change the global prevention and/or detection settings. Refer to “Configuring Category Policies” on page 23 for instructions on configuring signature categories.

- **Signature** - SonicWALL IPS provides maximum granularity by allowing you to change the global and/or category prevention and detection settings for individual signatures in the IPS Policies section. Refer to “Configuring Signature Policies” on page 25 for instructions on configuring signatures.

Categories and signatures are defined by the SonicWALL IPS database change based on new signature updates in response to new forms of attacks. You can display all the categories and signatures and in the IPS Policies table.

---

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

Configuring Global Signature Groups

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

- **High Priority Attacks** - These attacks are the most dangerous to your network. They can take down your entire network or disable servers, such as various Backdoor, DDoS, and DOS attacks.
- **Medium Priority Attacks** - These attacks can cause disruption to your network, such as increased network traffic that slows down performance. For example, various DNS, FTP, and Telnet attacks.
- **Low Priority Attacks** - These attacks are characterized more as informational events, such as various Scan, RPC, and SMTP attacks.
Tip! It’s recommended you enable **Prevent All** for **High Priority Attacks** and **Medium Priority Attacks** to provide network protection against the most damaging attacks.

SonicWALL IPS provides two methods for managing global attack threats: detection (**Detect All**) and prevention (**Prevent All**). You must specify a **Prevent All** action in the **Signature Groups** table for intrusion prevention to occur on the SonicWALL security appliance.

If **Prevent All** is enabled for a signature group in the **IPS Settings** table, the SonicWALL security appliance automatically drops and resets the connection, to prevent the traffic to reach its destination.

If **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 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.

If **Detect All** and **Protect All** are both enabled for a signature group in the **Signature Groups** table, the SonicWALL logs and alerts any traffic that matches any signature in the group, as well as automatically drop and reset the connection, to prevent the traffic to reach 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 attacks 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 Priority** and **Medium Priority** attacks, it is recommended you use the default 0 setting to deal with the threat immediately.

Resetting SonicWALL IPS Configuration to Default Settings

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

The **IPS Policies** section of the **Security Services > Intrusion Prevention** page allows you to view and manage how SonicWALL IPS handles signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack, and they are listed in the **Category** menu.

All the entries listed in the **IPS Policies** table are from the SonicWALL IPS signature database downloaded to your SonicWALL security appliance. Categories and signatures are dynamically updated by the SonicWALL Intrusion Prevention Service. Categories and signatures dynamically change over time in response to new threats.

### Displaying Categories and Signatures

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

![IPS Policies Table](image)

The **Category** menu allows you to specify the categories or signatures to display in the **IPS Policies** table.

Selecting **All categories** from the **Category** menu displays all of the signatures by category. The **IPS Policies** table displays all the categories with **Global** displayed in the **Prevent** and **Detect** columns, indicating the global settings you defined in the **IPS Global Settings** section.

The **Priority** menu allows you to specify **All** the signatures associated with the category, or display only signatures that fall within the **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks** signature groups.
**IPS Policies Table**

The **IPS Policies** table displays the following information about each signature entry:

- **Name** - The name of the attack signature.
- **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.
- **Priority** - Defines the attack signature as **Low**, **Medium**, or **High** as defined for the **Signature Groups** table.
- **Configure** - Clicking the edit 🖊 icon in this column displays the **Edit IPS Signature** window, which allows you to define a different action from the global settings for the specific signature.

**Navigating the IPS Policies Table**

The **Items** field displays the table number of the first category or signature. If you are viewing 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.

The SonicWALL IPS signatures are displayed fifty to a page in the **IPS 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 the signature ID number on the **Lookup Signature ID** field, then clicking the edit (Notepad) icon.

The **Edit IPS Signature** window is displayed with the signature information.

**Sorting Category or Signature Entries**

Clicking on the **IPS Policies** table headings (**Name**, **ID**, **Prevent**, **Detect**, or **Priority**) 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 Priority Attacks, Medium Priority Attacks, and Low Priority Attacks are configured in the IPS Global Settings section. Categories can include any combination priority attacks as defined in the Signature Groups table.

The available signature categories are listed in the Category menu in the IPS 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 attack priority)

Overriding Global Prevent and Detect Settings by Category (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 IPS 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 IPS 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 IPS Policies table, allowing you to configure both the category and signatures within the category.
If you override any global settings for a category, a green check mark appears in the Prevent and/or Detect columns of the IPS Policies table.

Overriding Global Prevent and Detect Settings by Category (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 IPS 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 IPS 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 IPS category:
Included Users/Groups - select the Users/Groups you want included in this SonicWALL IPS category. The default is **All**.

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

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

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

Schedule - select the scheduled time you want for the activation of this SonicWALL IPS 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 **IPS Policies** table, allowing you to configure both the category and signatures within the category.

---

**Resetting SonicWALL IPS 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 IPS Settings & Policies** button in the **IPS 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 Intrusion Prevention Service 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.

---

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>ID</th>
<th>Prevent Global</th>
<th>Detect Global</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTACK-RESPONSES</td>
<td>403 Forbidden</td>
<td>7</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Command Completed</td>
<td>2</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Command/Exit</td>
<td>3</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Deception/Listing</td>
<td>1</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>file copied ok</td>
<td>4</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Indexed/hidden Response</td>
<td>6</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Invalid URL</td>
<td>5</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>Microsoft/active banner</td>
<td>14</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>oracle one factor Install</td>
<td>8</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>reexecute malware.bin</td>
<td>13</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>successful gobble w5f exploit (COMBLED)</td>
<td>11</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTACK-RESPONSES</td>
<td>successful gobble w5f exploit (uncompressed)</td>
<td>12</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Selecting a specific signature category, such as **BACKDOOR**, **DDOS**, or **WEB-ATTACKS** displays the signatures in that category.

![IPS Policies Table](image1)

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

**Alert!** Use caution when overriding global **High Priority Attacks** and **Medium Priority Attack** signature behaviors because you can create vulnerabilities. If you make changes and want to restore the default global signature settings, click the **Reset IPS Configuration to Default**.

**Overriding Category Detect and Prevent Settings for a Signature (SonicOS Standard)**

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

1. In the **IPS Policies** table, display the signature you want to change, click the edit icon in the **Configure** column for the entry to display the **Edit IPS 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**  
(SonicOS Enhanced)

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

1. In the **IPS Policies** table, display the signature you want to change, click the edit icon in the **Configure** column for the entry to display the **Edit IPS 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. The following settings allow you to select specific users/groups, IP address ranges, and schedule objects to be included or excluded from this SonicWALL IPS signature:
   - **Included Users/Groups** - select the Users/Groups you want included in this SonicWALL IPS signature. The default is **All**.
   - **Excluded Users/Groups** - select the Users/Groups you want excluded from this SonicWALL IPS signature. The default **None**.
   - **Included IP Address Range** - select the IP address range you want excluded from this SonicWALL IPS signature. The default **All**.
   - **Excluded IP Address Range** - select the IP address range you want excluded from this SonicWALL IPS signature. The default **None**.
   - **Schedule** - select the scheduled time you want for the activation of this SonicWALL IPS 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.
Displaying Information about the Vulnerability

In the Edit IPS Signature window, clicking on the here link in Note: Click here for comprehensive information regarding this vulnerability, displays a SonicALERT page that provides detailed information about the attack.

Resetting SonicWALL IPS Configuration 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 IPS Settings & Policies button in the IPS Settings section.

Alert! Use caution when changing the global settings for individual attack signatures because they override the global settings, which may result in creating vulnerabilities.
Configuring Network Services and an Exclusion List

Clicking the **Configure IPS Settings** button in the **IPS Global Settings** section displays the **IPS Config View** window, which allows you to configure SonicWALL IPS network services and exclusions list.

### Configuring Network Services

The **IPS Network Services** section allows you to configure SonicWALL IPS to prevent (**Prevent Invalid Checksum**) and detect (**Detect Invalid Checksum**) invalid IP, ICMP, TCP, and UDP checksums.

- **Prevent Invalid Checksum**
  - If **Prevent Invalid Checksum** is enabled, the SonicWALL security appliance automatically drops and resets the connection, to prevent the traffic to reach its destination.

- **Detect Invalid Checksum**
  - If **Detect Invalid Checksum** is enabled, the SonicWALL security appliance logs and alerts any traffic, 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.
  - If **Detect Invalid Checksum** and **Prevent Invalid Checksum** are both enabled, the SonicWALL logs and alerts any traffic, as well as automatically drop and reset the connection, to prevent the traffic to reach its destination.

- Check **Enable IP Reassembly** to reassemble fragments for full application layer inspection.

When you select **Detect Invalid Checksum**, the Low Priority Attack Log Redundancy setting is used for logging.

### Configuring an Exclusion List

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

1. Click **Configure IPS Settings** in the **IPS Global Settings** section.
2. In the **IPS Exclusion List** section, click the **Enable IPS Exclusion List** checkbox to enable the exclusion list.
3. Click the **Add** button. The **Add IPS 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 **IPS 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 **IPS Config View** window.

### SonicWALL IPS Logging

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

Clicking on the **IPS Detection Alert** or **IPS Prevention Alert** link in the **Message** column of the Log displays the **Edit IPS Signature** window, allowing you to customize the **Detection** and **Prevention** settings.

---

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

---

**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.

---

### Managing False Positives

A false positive is a traffic pattern that is falsely identified as an attack traffic pattern. You can control false positives in SonicWALL IPS using a variety of methods.

- Click on the log message link for the signature in the **Log > View** page, which displays the **Edit IPS Signature** window. You can then disable the signature detection and/or enable prevention.
- Disable **Detect All** for the **Low Priority Attacks** signature group.
- Search the signature database by entering the signature ID number on the **Lookup Signature ID** field, then clicking the **edit** (Notepad) icon. The **Edit IPS Signature** window is displayed with the signature information. You can then disable the signature detection and/or enable prevention.
SonicWALL IPS Inspection of VPN/Encrypted Traffic

You can enforce intrusion prevention on traffic coming in to your networks from VPN tunnels at the point of entry for the unencrypted data from the VPN tunnel. SonicWALL IPS cannot perform inspection on any encrypted traffic that is in transit through the SonicWALL security appliance. However, the SonicWALL security appliance can perform SonicWALL IPS inspection on any VPN tunnel that terminates directly on the SonicWALL security appliance. SonicWALL IPS 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 IPS 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 IPS inspection to happen on a VPN tunnel that terminates directly on the SonicWALL security appliance.

---

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

---

Glossary

- **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.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.
- **Stateful Packet Inspection** - examines the contents of individual packets at all layers of the OSI model, from network layer to application layer.
Index

A
activating an IPS license 14
activating IPS free trial 14
activating SonicWALL IPS overview 11

C
concurrency capabilities 8
PRO 1260 8
PRO 2040 8
PRO 3060 8
PRO 4060 8
PRO 5060 8
TZ 150 Series 8
TZ 170 Series 8
configuring category settings 23
configuring global, category, and signature policies
global signature groups 19
overview 19
configuring log event alerts 20
configuring signature policies 25
creating a mysonicwall.com account 12

D
deep packet inspection technology 7
deploying SonicWALL IPS 10
disabling the GAV/IPS engine 8
Distributed Enforcement Architecture (DEA) 5

E
Edit IPS Signature window 22
Edit Zone window 17
enabling Gateway Anti-Virus on zones (SonicOS Enhanced) 17

F
false positives
managing 30

G
Gateway Anti-Virus
intrusion prevention 6
GAV/IPS features
application control 6
deep packet inspection 6
Distributed Enforcement Architecture 6
file based scanning protocol support 6
file decompression technology 6
graular management 7
inter-zone scanning 6
logging and reporting 7
real-time scanning 6
glossary 31
deep packet inspection 31
Distributed Enforcement Architecture 31
false positive 31
intrusion detection 31
intrusion prevention 31
signature 31
stateful packet inspection 31

H
how SonicWALL’s deep packet inspection architecture works 9

I
inbound and outbound protection 10
inspection of VPN/encrypted traffic 31
Intrusion Prevention Service
overview 5
IP reassembly 29
IPS 2.0 features 7
category and signature addressing 7
category and signature scheduling 7
category and signature user/group controls 7
checksum validation 7
dynamic categorization 7
global IP exclusion list 7
IP fragmentation reassembly 7
log redundancy granularity 7
IPS detection and prevention configuration options 16
IPS exclusion list 29
IPS features 6
IPS network services 29
detect invalid checksum 29
prevent invalid checksum 29
IPS running on SonicOS Standard 3

L
Log Redundancy Filter 20
logging 30

M
managing category and signature policies 21
displaying 21
IPS Policies table 21
navigating the IPS Policies table 22
signature ID lookup 22
signature information 22
sorting entries 22
managing false positives 30

O
overriding category policies for signatures
SonicOS Enhanced 27
SonicOS Standard 26
overriding global settings by category
SonicOS Enhanced 24
overriding global settings by category
SonicOS Standard 23
overriding prevent and detect settings for signatures 27
registering the SonicWALL security appliance 13
resetting IPS signature overrides to defaults 25, 28
resetting IPS to default settings 20

searching the signature database by ID 22
setting up SonicWALL IPS protection 15
applying IPS on zones
  (SonicOS Enhanced) 17
applying IPS protection to interfaces
  (SonicOS Standard 3.0) 16
enabling 16
specifying global attack level protection 16
signature groups
  Detect All setting 20
  high priority attacks 19
  low priority attacks 19
  medium priority attacks 19

Prevent All setting 20
SonicALERT information 28
SonicWALL Gateway Anti-Virus/Intrusion
Prevention Service overview 5
SonicWALL Global Management System 5
SonicWALL Intrusion Prevention Service 5
SonicWALL ViewPoint 5
status information 18
  last checked 18
  service expiration date 18
  signature database 18
  signature database timestamp 18

updating signatures 19
updating signatures manually 19

viewing log events 20
VPN and encrypted traffic 31