

SonicWALL Intrusion Prevention Service (IPS)

Prepared by SonicWALL, Inc.
4/27/2004

Announcement Overview

SonicWALL announces its new Intrusion Prevention Service (IPS). Available on SonicWALL TZ 170 and PRO Series appliances, SonicWALL Intrusion Prevention Service integrates an ultra-high performance deep packet inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. A scalable solution supporting virtually any network size, SonicWALL IPS allows intrusion prevention to be enforced not only between each network zone and the Internet, but also between internal network zones for added security.

SonicWALL Intrusion Prevention Service provides:

Integrated Deep Packet Inspection Technology. SonicWALL Intrusion Prevention Service features a configurable, ultra-high performance deep packet inspection engine that uses parallel searching algorithms up through the application layer to deliver increased attack prevention capabilities over those supplied by traditional stateful packet inspection firewalls.

Inter-zone Intrusion Prevention. Inter-zone Intrusion Prevention allows administrators to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones.

Extensive Signature List. SonicWALL Intrusion Prevention Service utilizes an extensive database of over 1,700 attack and vulnerability signatures written to detect and prevent intrusions, worms, application exploits, and the use of peer-to-peer and instant messaging applications.

Dynamically Updated Signature Database. SonicWALL Intrusion Prevention Service includes an extensive database with automated signature updates delivered through SonicWALL's distributed enforcement architecture, providing protection from emerging threats and lowering total cost of ownership.

Scalable Solution. SonicWALL Intrusion Prevention Service is a scalable solution for SonicWALL TZ 170 and PRO Series appliances that secures small, medium and large networks with complete protection from application exploits, worms and malicious traffic.

Application Control. SonicWALL Intrusion Prevention Service provides the ability to monitor and manage the use of instant messaging and peer-to-peer file sharing programs, closing a potential backdoor that can be used to compromise the network while improving employee productivity and conserving bandwidth.

Simplified Deployment and Management. SonicWALL 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 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 Intrusion Prevention Service offers comprehensive logging of all intrusion attempts with the option 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.



Eligible Appliances:

SonicWALL Intrusion Prevention Service is available on SonicWALL TZ 170 and PRO Series Internet Security appliances running SonicOS 2.2 or higher.

SonicWALL Intrusion Prevention Service SKU information is as follows:

Product	SonicWALL SKU	Subscription Length
SonicWALL Intrusion Prevention Service Basic for TZ 170 10 Node	01-SSC-5750	1 Year
SonicWALL Intrusion Prevention Service for TZ 170	01-SSC-5751	1 Year
SonicWALL Intrusion Prevention Service for PRO 2040	01-SSC-5757	1 Year
SonicWALL Intrusion Prevention Service for PRO 3060	01-SSC-5758	1 Year
SonicWALL Intrusion Prevention Service for PRO 4060	01-SSC-5759	1 Year

To purchase SonicWALL Intrusion Prevention Service, contact a SonicWALL-certified reseller. To find a reseller in your area, please visit <http://www.sonicwall.com/howtobuy/index.html> or call SonicWALL at +1 888-557-6642 or +1 408-745-9600.

SonicWALL IPS Sales Q&A Section:

Q: On which SonicWALL platforms is SonicWALL Intrusion Prevention Service available?

A: SonicWALL Intrusion Prevention Service is available on SonicWALL TZ 170 and PRO Series (PRO 2040/3060/4060) Internet Security platforms running SonicOS 2.2 or higher. When activated, SonicWALL IPS requires 10-15MB of RAM (depending on platform), and initially 500KB of flash space.

Q: There are two versions of SonicWALL IPS for the TZ 170. What is the difference?

A: SonicWALL offers two versions of our Intrusion Prevention Service for SonicWALL TZ 170 appliances: SonicWALL Intrusion Prevention Service for TZ 170 and SonicWALL Intrusion Prevention Service Basic for TZ 170. Designed for small offices, the "Basic" version does not provide application level signature support for servers. Otherwise the two versions are the same.

Q: How do I activate my SonicWALL Intrusion Prevention Service subscription?

A: Upon purchasing a SonicWALL Intrusion Prevention Service subscription, you will receive an upgrade manual with instructions for activating the product. There is an installation guide with a single activation code sticker. Follow the installation guide instructions to activate your SonicWALL Intrusion Prevention Service subscription.

Q: How do I manage my SonicWALL Intrusion Prevention Service subscription?

A: Security administrators can manage the intrusion prevention policy and signature database directly on the SonicWALL appliance. Alternatively, SonicWALL Global Management System provides global management capabilities that enable administrators to manage the intrusion prevention policy and signature database for multiple SonicWALL appliances from a central location and push those policies to all remote appliances.

Q: Can I create reports?

A: Yes. SonicWALL's award-winning Global Management System and ViewPoint solutions each include an "Intrusion Prevention" tab that allow security administrators to create detailed reports based on attack source, destination and type of Intrusion such as "Top Intrusions," "Destinations Over Time," "Intrusions Over Time" and more.

Q: Where can I find more information on the SonicWALL Intrusion Prevention Service?

Additional information on the SonicWALL Intrusion Prevention Service is available at <http://www.sonicwall.com/products/ips.html>.

Q: What form of support is included with my SonicWALL Intrusion Prevention Service subscription?

▶ SONICWALL OVERVIEW / FAQ :

A: Support for SonicWALL's Intrusion Prevention Service is tied to the support contract of the SonicWALL appliance with which it is associated. Signature updates are included in the first year once the service has been activated. Ongoing signature updates after the first year require a yearly SonicWALL Intrusion Prevention Service subscription.

Q: Does SonicWALL offer a free trial of the Intrusion Prevention Service?

A: Yes. SonicWALL IPS will be licensed as a service through the distributed enforcement architecture (DEA) Licensing Framework. SonicWALL IPS will have a Free Trial as well as a regular subscription. There will be an expiration date and a signature timestamp indicating how up to date the signatures should be. Also, SonicWALL IPS will have a signature download URL that will be set by the DEA Licensing Server and a configurable hostname so that signatures could be served from a dedicated server.

SonicWALL IPS Technical Q&A Section:

What exactly is "deep packet inspection"?

Deep packet inspection is a technology which allows a SonicWALL device to classify passing traffic based on rules that not only include information about layer 3 and layer 4 contents of the packet, but also include information that describes the contents of the packet's payload – including the application data (for example, an FTP session, or a HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log various intrusions that pass through the SonicWALL device, as well as prevent (i.e., drop packet, reset TCP connection) them. SonicWALL's deep packet inspection also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

Deep Packet Inspection technology enables the SonicWALL device to investigate further into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture (DEA). 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, an HTTP request may be URL encoded and thus the request is
4. URL decoded in order to perform correct pattern matching on the payload.
5. 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.
6. 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.

IN which firmware versions is SonicWALL IPS included?

SonicWALL IPS can be licensed and installed on any SonicWALL device capable of running SonicOS 2.2 Standard or SonicOS 2.2 Enhanced and newer. SonicWALL IPS is not supported on older SonicWALL devices or firmware versions.

How is SonicWALL IPS licensed?

SonicWALL IPS is licensed as a service through the DEA Licensing Framework. Any IPS-capable device has the option for a free 30-day trial, as well as an annual subscription. SonicWALL IPS has an expiration date and a signature timestamp indicating how up-to-date the signatures are.

What is the difference between IPS "Detection" vs. IPS "Prevention"?

When the Detection setting is "Enabled" for a group (or a signature), the SonicWALL will log and alert any traffic that matches that signature, but will not take any action against the traffic, and the connection will proceed to its intended destination. When the Prevention setting is "Enabled" for a group (or signature), the SonicWALL will



▶ SONICWALL OVERVIEW / FAQ :

actively drop and reset the connection, and prevent the connection from reaching its intended destination. In simpler terms, Detection tells you something is wrong, but Prevention actually goes and does something about it.

When should I enable Detection vs. Prevention?

This decision is entirely up to the network administrator – since using the Prevention setting will actively drop and reset a connection, this may be seen as too heavy-handed for some companies, and they may wish to use Detection only. You will need to experiment with the settings for each group and signature to find a balance between security and accessibility that serves the needs of your network best.

Does IPS use Snort?

SonicWALL IPS includes the open-source Snort signatures, as well as other signature databases, and signatures created in-house, but does not use the Snort engine. SonicWALL IPS was developed entirely by SonicWALL and does not include any external third-party IDP/IPS technology.

Is SonicWALL IPS incompatible with any feature or service on my SonicWALL device?

No. SonicWALL Intrusion Prevention Service will not impact or prevent any feature or service on the SonicWALL device from functioning correctly – it simply will inspect all inbound traffic for the interface or zone on which it's activated.

How do I enable SonicWALL IPS on my SonicWALL appliance?

Depending on whether your SonicWALL is running SonicOS Enhanced 2.2 (or higher) or SonicOS Standard 2.2 (or higher), you can apply intrusion prevention protection to selected Interfaces or zones. When you enable IPS on an Interface or zone, SonicWALL IPS operates on traffic bi-directionally (ingress and egress).

If your SonicWALL is running SonicOS Standard, the 'Security Services>Intrusion Prevention' page allows you to enable IPS on the available interfaces listed in 'Select Interfaces' to enable IPS on, which is located below the 'Signature Groups' table.

If your SonicWALL is running SonicOS Enhanced with multiple interfaces, SonicWALL IPS allows you to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones. For example, enabling IPS on the LAN zone enforces intrusion prevention on all incoming and outgoing LAN traffic.

Can I activate SonicWALL IPS on every single interface/zone?

Yes. If you wish, you can activate SonicWALL IPS to inspect traffic on all interfaces/zones. There is no extra performance impact when doing so, either.

What are the differences between the Priority Levels in SonicWALL IPS?

SonicWALL IPS allows you to enable/disable detection or prevention based on the priority level of the attack through 'High', 'Medium' or 'Low' predefined priority groups, as well as instant messaging (IM) and peer-to-peer (P2P) applications. You can manage your risk by selecting these specific signature groups:

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.

IM (Instant Messaging) Applications - These signatures protect your network from the vulnerabilities of Instant Messaging applications, such as ICQ, MSN, IRC, AIM, Yahoo, and QQ.

P2P (Peer-to-Peer) Applications - These signatures protect your network from the vulnerabilities of P2P applications, such as Gnutella, Fastrack, Kazaa, Morpheus, and eDonkey.

How many IPS "categories" are there?

As noted above, there are five signature groups, and 43 IPS categories spread across those groups. The categories group together similar types of attacks and exploits into manageable sections, rather than freely listing the 1,700+ signatures.



How many signatures are in the SonicWALL IPS database?

In the current SonicWALL IPS database snapshot (as of 4/20/04), there are over 1,700+ signatures, but this number increases as attacks are classified and added to the signature database each day.

Does SonicWALL IPS do TCP reassembly?

Yes. If TCP packets arrive out of order, the SonicWALL IPS engine will reassemble them before inspection. However, SonicWALL's IPS framework supports complete signature matching across the TCP fragments without having to perform complete reassembly. Reassembly-free signature matching gives SonicWALL's IPS framework a unique competitive advantage, since competing solutions have far greater CPU and memory resource requirements. As a comparison, SonicWALL's solution may consume anywhere between 10MB – 15MB of RAM (depending on the # of TCP connections).

At existing memory requirements, 60,000 TCP connections are supported with full bi-directional inspection across fragmented TCP streams (unlimited, i.e., up to the limit of the firewall, number of TCP connections without support for fragmented TCP streams). In other words, after 60,000 TCP stream fragmentation will not be handled, but TCP streams will still be examined. An Unlimited number of UDP sessions are supported (i.e., up to the limit on the firewall).

Can SonicWALL IPS inspect application data running on non-standard ports?

In the current version of SonicWALL IPS, it cannot, with the exception of some of the P2P/IM applications, which have multiple signatures.

How fast are the SonicWALL IPS signature updates?

By default, a SonicWALL appliance running IPS will check SonicWALL's IPS signature servers once per hour. SonicWALL's IPS solution allows system administrators to choose an option to prevent all high priority intrusions. When this option is selected, SonicWALL's firewall will automatically decide which signatures should be treated with preventive measures. There will not be any need for an administrator to constantly check how up to date the signatures are and try to pick the attacks he needs to prevent. Since SonicWALL's firewall will become up to date with the latest signature file within one hour of a new intrusion being announced by SonicWALL, a "Zero Administration" IPS solution is an extremely attractive option for SonicWALL's customers.

Each version of the SonicWALL IPS signature database has a different timestamp (IPS_TIMESTAMP). Using SonicWALL's DEA Licensing framework, the SonicWALL appliance polls the DEA Server once per hour for the information about the Intrusion Prevention Service with one of the pieces of that information being IPS_TIMESTAMP. When a new IPS signature database is available, the DEA database is updated with the new timestamp, and as firewall polls DEA Server, new IPS_TIMESTAMP becomes known to the firewall and it is an indication to the firewall to download the newly available IPS signature database. Along with the new IPS timestamp, the DEA Server also sends signature download URL to the firewall, which tells the firewall the location of the signature database. Successful updates will display as "Downloaded" in the SonicWALL's internal management GUI, at the top of the 'Security Services > Intrusion Prevention Services' page.

I don't want to wait – can I make the SonicWALL update its IPS signatures immediately?

Yes, there are two ways to do this: either reboot the SonicWALL, or go to the SonicWALL's 'Security Services > Summary' page and click on the 'Synchronize' button. Both actions will cause the SonicWALL appliance to immediately poll the IPS signature servers and update to the most recent IPS signature database.

The SonicWALL signature database timestamp is old and won't update no matter what I do – why?

It may be that the signature database has not been updated since that date listed; while the SonicWALL device checks hourly for new IPS signature database updates, it does not necessarily mean that the SonicWALL device will receive a new one each time.

Are the SonicWALL IPS signature updates secured?

SonicWALL IPS signature download is completely secure, as the SonicWALL appliance, in its signature database request, has to first authenticate itself with a pre-shared secret, created during DEA Licensing registration of the SonicWALL appliance. In addition, the request is transported through HTTPS, along with full server certificate verification.



What does Log Redundancy Filter on the SonicWALL IPS configuration screen do?

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. For the more critical High Priority and Medium Priority attacks as well as IM and P2P vulnerability signatures, it's recommended you use the default 0 setting to deal with the threat immediately.

I don't know what signatures are enabled or disabled anymore – can I just reset the IPS policy completely and start over?

Yes – on the 'Security Services > Intrusion Prevention Service' page, you will find a button labeled 'Reset IPS Configuration to Default'. Clicking on this button will reset the status of every signature in all categories to default settings.

What happens when the SonicWALL IPS license expires?

If the SonicWALL appliance's IPS signature expires, it will immediately stop inspecting traffic and the configuration page for SonicWALL IPS will disappear.

What happens when you renew the license after letting the SonicWALL IPS policy expire?

The SonicWALL retains any previously configured IPS settings, even if the IPS subscription has expired, so if the subscription is renewed after letting it lapse, all previous settings will return and will not be lost.

What is the performance hit when IPS is running?

Activating SonicWALL IPS will incur a 15-20% performance hit on the SonicWALL device's throughput, regardless of how many zones/interfaces are performing inspection, or how many categories are active.

Can SonicWALL IPS inspect VPN or encrypted traffic?

The SonicWALL can perform inspection on any VPN tunnels that terminate directly on the SonicWALL device itself – traffic will be inspected as it goes into the tunnel before and/or when it comes out of the tunnel. Please note that when using SonicOS Enhanced, you cannot enforce IPS on the VPN zone itself, but you can enforce intrusion prevention on traffic coming into your networks from VPN tunnels at the point of entry for the unencrypted data from the VPN tunnel. If a VPN tunnel terminates at the LAN zone, enabling IPS on the LAN zone enforces intrusion prevention as the data is unencrypted before entering the LAN zone. The SonicWALL appliance cannot perform decryption on any in-transit encrypted traffic -- for example, a client VPN session that originated behind the SonicWALL device that terminates somewhere else.

I'm using SonicWALL IPS and I got a false positive – can I shut that signature off?

Yes, there are two ways to do this. The simplest way is to click on the log message for that signature, which will bring up a GUI control to enable or disable the signature. The second is to note the signature ID number in question, and using the signature ID search function on the 'Security Services > Intrusion Prevention Service' page, pull up the GUI control for that signature to enable or disable the signature.

I can't shut some of the signatures off – why?

All SonicWALL appliances contain a number of older signatures that are part of the firmware, and are not part of the SonicWALL IPS signature database. These signatures, for older attacks such as 'NetBus' or 'Ripper', will lead to a description page in the SonicWALL if clicked, and not to the IPS signature configuration screen. These older signatures cannot currently be deactivated.

Can I write or import my own Intrusion Prevention Service signatures?

No. At present, it's not possible to create or import customized IPS signatures into the SonicWALL appliance. This capability may be supported in a future release.

