SonicWALL

Intrusion Prevention Service

# SonicWALL Intrusion Prevention Service

- *Utilizes a configurable, ultra-high performance deep packet inspection engine to deliver maximum network protection*
- *Provides a dynamically updated database of over 1,700 attack and vulnerability signatures*
- *Prevents known buffer overflow vulnerabilities in software, as well as various worms, Trojans, and backdoor exploits*
- *Manages the use of instant messaging and peer-to-peer applications to mitigate risk and legal liability while improving productivity*
- *Protects networks not only from attacks originating outside the network (WAN), but also from internal attacks targeting network segments (LANs)*

**SONICWALL DEEP PACKET INSPECTION ARCHITECTURE**

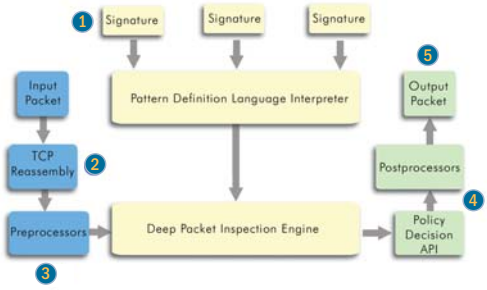


**Figure 1)**

1) Signatures can be written to detect and prevent known and unknown protocols, applications and exploits.

2) TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.

3) Preprocessing involves normalization of the packet's payload.

4) Postprocessors perform actions that simply pass the packet without modification, drop a packet or even reset a TCP connection.

5) SonicWALL's Deep Packet Inspection architecture supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order).

Every day, hackers become more sophisticated in their attempts to breach corporate networks. Over the past few years, attacks such as Nimda, Code Red, SQL Slammer and MS Blaster targeted application vulnerabilities and infected computers worldwide. More recently, hackers have exploited peer-to-peer and instant messaging applications to propagate their attacks. As these attacks become more dynamic and malicious in nature, businesses need to stay one step ahead by employing a firewall with the most robust detection and prevention solution available.

The SonicWALL® Intrusion Prevention Service (IPS) is a high-speed, scalable solution delivering complete protection from application exploits and malicious traffic targeting all points of the network. Featuring a configurable, ultra-high performance deep packet inspection engine and a dynamically updated database with over 1,700 attack and vulnerability signatures, SonicWALL IPS protects against known buffer overflow vulnerabilities in software, as well as various worms, Trojans, application exploits and the use of instant messaging and peer-to-peer applications. The extensible signature language used in the deep packet inspection engine provides a proactive defense against newly discovered application vulnerabilities.

While many attacks originate outside the network, the threat of internal attack is just as real. Protecting confidential information from unauthorized access across company departments is critical. SonicWALL IPS manages this risk by providing network administrators with the tools to enforce intrusion prevention not only between each network zone and the Internet, but also between departments located on different internal network zones (See Figure 3). SonicWALL IPS prevents another potential source or vulnerability by allowing administrators to monitor and manage the use of instant messaging and peer-to-peer file sharing applications, closing a potential backdoor that could be used to compromise the network.

The vast signature database in SonicWALL IPS can be tailored to meet the needs of both large and small network environments. Per-signature configuration flexibility, combined with the option to configure a custom set of detection or prevention policies by network zone, reduces the number of false positives often found in other intrusion prevention solutions.

SonicWALL IPS provides comprehensive logging of all intrusion attempts with the option to filter logs based on priority level, enabling administrators to highlight high-priority attacks. SonicWALL ViewPoint® and Global Management System both offer granular reporting based on attack source, destination and type of intrusion for greater insight into malicious activities targeting any point on the network.

With its powerful performance, leading-edge features and extensive management capabilities, SonicWALL's Intrusion Prevention Service delivers the network protection today's businesses require and the low total cost of ownership they expect.

SONICWALL

# SonicWALL Intrusion Prevention Service

## SONICWALL INTRUSION PREVENTION SERVICE (IPS) FEATURES AND BENEFITS

**Integrated Deep Packet Inspection Technology.** SonicWALL IPS 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. Parallel processing reduces the performance impact on the firewall and maximizes available memory for exceptional throughput on SonicWALL appliances.

**Inter-zone Intrusion Prevention.** SonicWALL IPS provides an additional layer of protection against malicious threats by allowing administrators to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones.

**Extensive Signature List.** SonicWALL IPS 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. SonicWALL continually adds signatures to the IPS database to protect networks from newly discovered exploits.

**Dynamically-updated Signature Database.** SonicWALL IPS 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 IPS 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 IPS provides network administrators with the ability to monitor and manage the use of instant messaging and peer-to-peer file sharing programs, closing a potential backdoor that could be used to compromise the network while improving employee productivity and conserving bandwidth.

**Simplified Deployment and Management.** SonicWALL IPS 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 IPS 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 positives while identifying immediate threats.

**Logging and Reporting.** SonicWALL IPS 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.

## SONICWALL INTRUSION PREVENTION

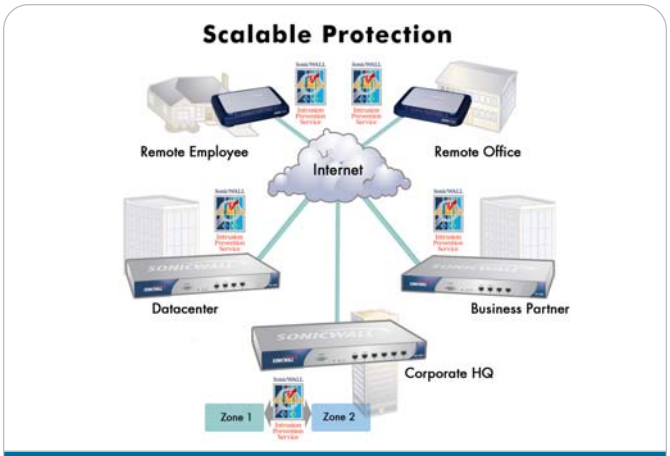


Figure 2) SonicWALL's Intrusion Prevention Service is a scalable solution for SonicWALL TZ 170 and PRO Series appliances securing all Internet and VPN connections into your network with complete protection from application exploits, worms and malicious traffic.


Figure 3) SonicWALL's Intrusion Prevention Service provides an additional layer of protection against malicious threats by allowing administrators to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones.

## SONICWALL INTRUSION PREVENTION SERVICE MINIMUM SYSTEM REQUIREMENTS

SonicWALL TZ 170 or PRO Series Internet security appliance running SonicOS 2.2 or higher

## SONICWALL INTRUSION PREVENTION SERVICE PART NUMBERS

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

*For more information on SonicWALL Intrusion Prevention Service and our complete line of security services, please visit our Web site at http://www.sonicwall.com/products/vpnsoft.html.*


*SonicWALL's ICSA-certified Internet security appliances consistently receive awards from industry-leading publications.*

**SonicWALL, Inc.**
1143 Borregas Avenue
Sunnyvale, CA 94089-1306
T: +1 408.745.9600
F: +1 408.745.9300
www.sonicwall.com



SONICWALL