Intrusion Prevention

Advanced threat protection for blocking cyber attacks

Today's cybercriminals are developing new and increasingly sophisticated attacks to find a way into your network. They are also creating specialized exploits to take advantage of new vulnerabilities sometimes even before software vendors have an opportunity to release a patch so delays in patching these zero-day vulnerabilities provides attackers a dangerous window of opportunity. In order to combat these evolving threats, systems administrators need a robust network security solution that protects the network 24 hours a day, 365 days a year.

The SonicWall Intrusion Prevention System (IPS) Service provides network protection around the clock — including the critical periods between regularly scheduled updates. SonicWall's award-winning IPS Service is activated as a license on SonicWall TZ, Network Security Appliance (NSA) and SuperMassive Series appliances, and integrates a high- performance, deep packet inspection architecture with dynamically updated countermeasures for complete protection from application exploits and other malicious traffic. The IPS Service is scalable to support virtually any size organization. It also provides enforcement between each network zone and the internet, and between internal zones for added security.

In addition, the IPS Service is powered by an industry-leading threat research team with extensive experience in vulnerability analysis and countermeasure creation. The team gathers threat intelligence from over one million connected sensors around the world, so SonicWall IPS subscribers benefit from a nimble and fast response to new attacks, regular security updates and out-of-band updates when necessary.

Features

Bi-directional, full stack inspection — Provides inbound and outbound inspection of critical application traffic. Includes protection for a wide variety of attacks, such as SQL injection, cross-site scripting, remote code execution, shell code payloads and remote procedure calls.

Robust protocols inspection — Spans a wide variety of protocols, including TCP, ICMP, DNS, HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, SIP, H.323, RTP, SNMP, MySQL, MS-SQL, RPC, NetBIOS, SMB and SMB2.

Context aware monitoring engine — Features full traffic visibility on end users, applications, sources, destinations, threat types, content and devices.

Full network traffic inspection — Inspects all ports, protocols and IP addresses, and includes support for IPv6 traffic and SSL-encrypted traffic (this requires SSL Inspection Service).

Robust, sophisticated traffic normalization — Provides advanced resistance to evasion, including IP packet fragmentation, TCP stream segmentation, RPC fragmentation, SMB/NetBIOS, Payload Encoding, FTP, TCP Split Handshake and layered combinations.

Benefits:

- Highly rated, comprehensive threat protection
- Provides complete and continuously updated security
- Simplified deployment and management of security across a distributed network
- Customized to fit your security needs with granular management
- Scalable to secure any size network

Microsoft Active Protections Program

SonicWall has a partnership Microsoft to receive advance notification of new threats through MAPP. This enables our threat research team to respond quickly to regular and out-of-band security advisories.

System requirements

IPS is available with the following SonicWall firewalls:

- TZ 105 / TZ 105W
- TZ 205 / TZ 205W
- TZ 215 / TZ 215W
- NSA 220 / NSA 220W
- NSA 250M / NSA 250MW
- NSA 2600
- NSA 3600
- NSA 4600
- NSA 5600
- NSA 6600
- SuperMassive 9200
- SuperMassive 9400
- SuperMassive 9600
- SuperMassive 9800
- SuperMassive E10200
- SuperMassive E10400
- SuperMassive E10800

Compression algorithm inspection — Supports on-the-fly inspections for numerous algorithms, including Deflate, Zip, gzip, LZH, gz, tar, tar.gz, tar.Z, tar. bz2 and Base64 encoding.

Anomaly-based protection — Provides numerous forms of security, including malformed packets, protocol fuzzing, IP spoofing, MAC spoofing, RFC 793 / RFC 1122 violations, port scanning, URL obfuscation, HTML obfuscation, multicast snooping and DNS tunneling.

Denial of service threshold and heuristic protection — Includes Ping of Death, Teardrop, Bonk, Sub-Seven, Nestea, Smurf, SYN/RST/FIN Flood, WinNuke, LAND.c, ICMP Flood, UDP Flood, LOIC, Christmas Tree and Backscatter.

Clean VPN™ — Inspects all incoming and outgoing VPN traffic for attacks and blocks malicious traffic.

Zone-based protection — Flexible, object-based policy engine enables quick and easy rule creation for specific systems, users, groups, hosts or networks.

Application traffic analytics — Offers comprehensive logging with filtering options, on-box reporting and administrator notification capabilities. Includes customized intrusion prevention templates for off-box IPFix exporting for long-term analytics reporting.

Application control — Provides the ability to monitor and manage over 4,500 applications including instant messaging and peer-to-peer file sharing programs, closing a potential back door that can be used to compromise the network, while improving employee productivity and conserving bandwidth.

Administrator-defined regular expression monitoring — Prevents data leakage by enabling transmission control and blocking of sensitive data such as credit card and social security numbers, or specific file attachments to personal web mail services and corporate SMTP or POP3 email.

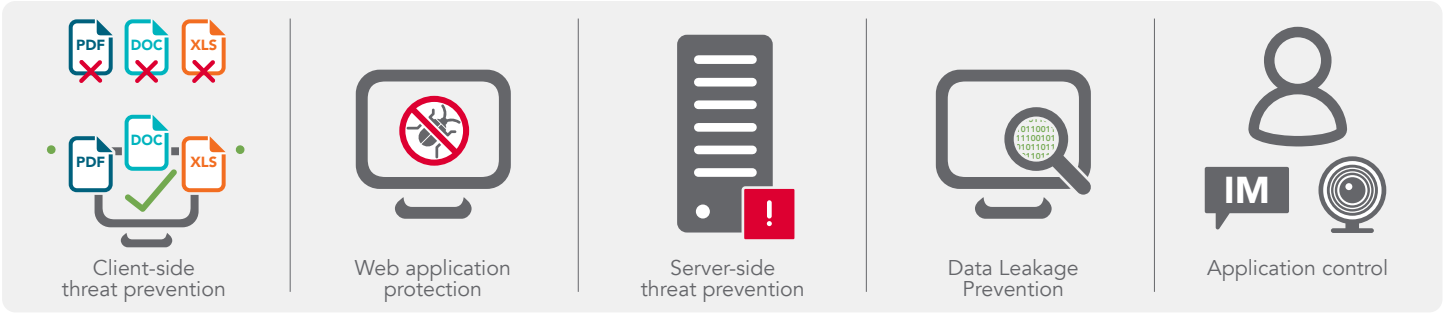
About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

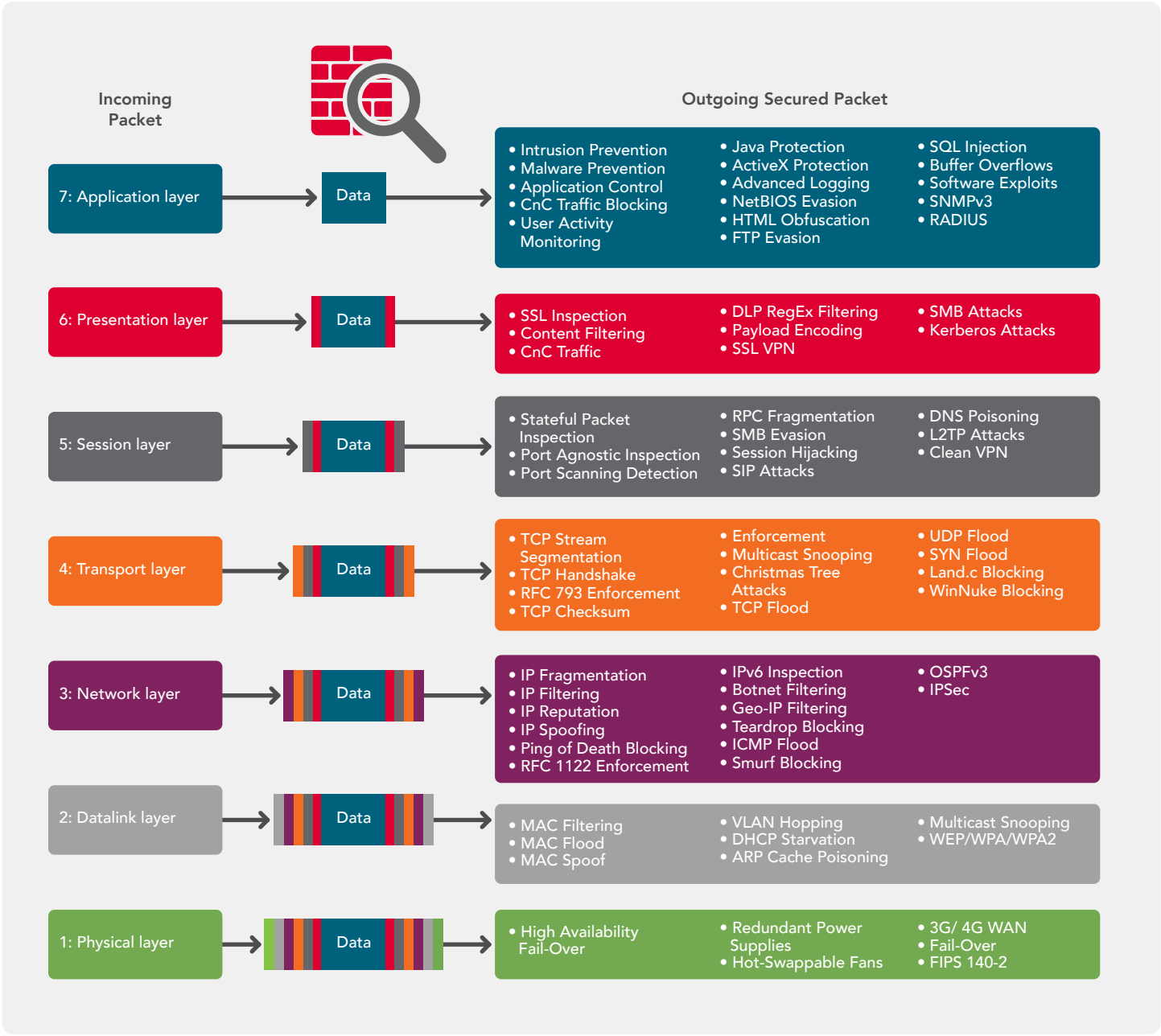
NSS LABS RECOMMENDED

In 2013, SonicWall earned a 'Recommend' rating from NSS Labs in Next-Generation Firewall and Intrusion Prevention System group testing.

SONICWALL™



The SonicWall Intrusion Prevention Service protects against a wide array of attack types.



The SonicWall Intrusion Prevention system utilizes a patented reassembly-free deep packet inspection engine for full stack protection.

SONICWALL™

SonicWall appliance	Intrusion prevision throughput	Maximum inspected connections	New connections per second
TZ 105 / TZ 105W	60 Mbps	8,000	1,000
TZ 205 / TZ 205W	80 Mbps	12,000	1,500
TZ 215 / TZ 215W	110 Mbps	32,000	1,800
NSA 220 / NSA 220W	195 Mbps	32,000	2,200
NSA 250M / NSA 250MW	250 Mbps	64,000	3,000
NSA 2600	700 Mbps	125,000	15,000
NSA 3600	1.1 Gbps	175,000	20,000
NSA 4600	2.0 Gbps	200,000	40,000
NSA 5600	3.0 Gbps	375,000	60,000
NSA 6600	4.5 Gbps	500,000	90,000
SuperMassive 9200	5.0 Gbps	1,000,000	100,000
SuperMassive 9400	8.0 Gbps	1,000,000	130,000
SuperMassive 9600	9.7 Gbps	1,250,000	130,000
SuperMassive 9800	20 Gbps	2,500,000	280,000
SuperMassive E10200	7.5 Gbps	2,500,000	160,000
SuperMassive E10400	15 Gbps	5,000,000	320,000
SuperMassive E10800	30 Gbps	10,000,000	640,000

	Gateway Anti Malware, IPS and AppControl	Comprehensive Gateway Security Suite	Total Secure Bundle
Intrusion Prevention	Yes	Yes	Yes
Malware Prevention	Yes	Yes	Yes
Application Control*	Yes	Yes	Yes
Content Filtering		Yes	Yes
24x7 Technical Support		Yes	Yes
NGFW Hardware Appliance			Yes

Intrusion Prevention is also available for the following SonicWall Next Generation and Unified Threat Management Firewalls:

- TZ 100
- TZ 200
- TZ 210
- NSA 240
- NSA 2400
- NSA 2400MX
- NSA 3500
- NSA 4500
- NSA 5000
- NSA E5500
- NSA E6500
- NSA E7500
- NSA E8500
- NSA E8510

	Gateway Anti Malware, IPS and App Control (1-year)	Gateway Anti Malware, IPS and App Control (2-year)	Gateway Anti Malware, IPS and App Control (3-year)	Comprehensive Gateway Suite Services (1-year)	Comprehensive Gateway Suite Services (2-year)	Comprehensive Gateway Suite Services (3-year)
TZ 105 / TZ 105W	01-SSC-4844	01-SSC-4845	01-SSC-4846	01-SSC-4877	01-SSC-4878	01-SSC-4879
TZ 205 / TZ 205W	01-SSC-4799	01-SSC-4800	01-SSC-4801	01-SSC-4838	01-SSC-4839	01-SSC-4840
TZ 215 / TZ 215W	01-SSC-4757	01-SSC-4758	01-SSC-4759	01-SSC-4793	01-SSC-4794	01-SSC-4795
NSA 220 / NSA 220W	01-SSC-4612	01-SSC-4613	01-SSC-4614	01-SSC-4648	01-SSC-4649	01-SSC-4650
NSA 250M / NSA 250MW	01-SSC-4570	01-SSC-4571	01-SSC-457	01-SSC-4606	01-SSC-4607	01-SSC-4608
NSA 2600	01-SSC-4459	01-SSC-4460	01-SSC-4461	01-SSC-4453	01-SSC-4454	01-SSC-4455
NSA 3600	01-SSC-4435	01-SSC-4436	01-SSC-4437	01-SSC-4429	01-SSC-4430	01-SSC-4431
NSA 4600	01-SSC-4411	01-SSC-4412	01-SSC-4413	01-SSC-4405	01-SSC-4406	01-SSC-4407
NSA 5600	01-SSC-4240	01-SSC-4241	01-SSC-4242	01-SSC-4234	01-SSC-4235	01-SSC-4236
NSA 6600	01-SSC-4216	01-SSC-4217	01-SSC-4218	01-SSC-4210	01-SSC-4211	01-SSC-4212
SuperMassive 9200	01-SSC-4202	01-SSC-4203	01-SSC-4204	01-SSC-4172	01-SSC-4173	01-SSC-4174
SuperMassive 9400	01-SSC-4166	01-SSC-4167	01-SSC-4168	01-SSC-4136	01-SSC-4137	01-SSC-4138
SuperMassive 9600	01-SSC-4130	01-SSC-4131	01-SSC-4132	01-SSC-4100	01-SSC-4101	01-SSC-4102
SuperMassive 9800	01-SSC-0839	01-SSC-0840	01-SSC-0841	01-SSC-0809	01-SSC-0810	01-SSC-0811
SuperMassive E10200	01-SSC-9527	01-SSC-9528	01-SSC-9529	01-SSC-9533	01-SSC-9534	01-SSC-9535
SuperMassive E10400	01-SSC-9545	01-SSC-9546	01-SSC-9547	01-SSC-9551	01-SSC-9552	01-SSC-9553
SuperMassive E10800	01-SSC-9563	01-SSC-9564	01-SSC-9565	01-SSC-9569	01-SSC-9570	01-SSC-9571

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

DataSheet-IPS-US-KS-24989-D120

SONICWALL™