TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Ata de Registro de Preços Nº 62/2020

Pregão Eletrônico nº 74/2020	**Processo SEI nº 0012283-09.2020.6.18.8000**

O TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, inscrito no CNPJ/MF sob o n° 05.957.363/0001-33, situado no endereço Praça Des. Edgar Nogueira, S/N - Centro Cívico - Bairro Cabral - CEP 64000-920 - Teresina (PI), neste ato representado por seu Presidente, em exercício, Des. ERIVAN JOSÉ DA SILVA LOPES, inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda sob o nº 284.095.583-00, com fundamento na Lei n° 8.666/93 e no Decreto n° 7.892/2013, emite a presente Ata de Registro de Preços com o objetivo de formalizar o Registro de Preços **para aquisição de Solução de Firewall UTM/VPN**, em decorrência das propostas apresentadas no Pregão Eletrônico n° 000074/2020 e em conformidade com os Anexos do Edital do referido Pregão Eletrônico.

1. Os dados relativos ao licitante vencedor e aos itens registrados estão especificados nos quadros a seguir:

1.1. Dados referentes ao licitante vencedor:

Empresa:	**CNPJ:**
NOVA SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E NETWORKING EIRELI	10.685.932/0001-79
Endereço:	**Telefone/ Fax:**
SCS Quadra 04 Bloco A Lote 219/237 1º Andar Parte O, Ed. Vera Cruz, CEP: 70.304-913, Brasília - DF	(61) 99411-7460
	E-mail:
	administrativo@grupoinovva.com.br
Representante legal:	**CPF:**
Marli Teresinha Erbe	393.391.060-91

1.2. Dados relativos aos itens registrados, em conformidade com as especificações constantes nos Anexos do Edital licitatório:

Item	**Especificação**	**Quantidade estimada de aquisição**	**Valor unitário (R$)**	**Valor Total (R$)**
1	Atualização da Solução de Firewall tipo concentrador com atualização dos equipamentos existentes para, no mínimo, o SonicWall NSA 5650, com serviço de suporte 24X7 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: NSA 5650 PN: 01-SSC-1939 / 01-SSC-3217 / 01-SSC-3678	2	R$ 295.000,00	R$ 590.000,00
2	Atualização da Solução de Firewall tipo pequeno porte com atualização dos equipamentos existentes para, no mínimo, o SonicWall SOHO 250 W, com serviço de suporte 8x5 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: SOHO 250W PN: 02-SSC-1865 / 02-SSC-1760	51	R$ 5.700,00	R$ 290.700,00
3	Atualização da Solução de Firewall tipo pequeno porte com atualização dos equipamentos existentes para, no mínimo, o SonicWall SOHO 250 W, com serviço de suporte 8x5 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: SOHO 250W PN: 02-SSC-1865 / 02-SSC-1760	17	R$ 5.700,00	R$ 96.900,00
4	Licença SonicWall Global Management System para até 70 nós por 03 anos Referências: a) 01 Licença 01-SSC-3311; b) 02 Licenças 01-SSC-7664; c) 01 Licença 01-SSC-3301; d) 02 Licenças 01-SSC-6532; e) 02 Licenças 01-SSC-6536. Fabricante: SonicWall / Modelo: GMS PN: 01-SSC-3311 / 01-SSC-7664 / 01-SSC-3301 / 01-SSC-6532 / 01-SSC-6536	1	R$ 175.000,00	R$ 175.000,00
			TOTAL (R$)	**1.152.600,00**

2. A presente Ata de Registro de Preços terá vigência de 12 (doze) meses, a contar da data de sua publicação.

3. A existência de preços registrados não obriga o TRE-PI a efetuar as aquisições, facultando-se a realização de licitação específica para as aquisições pretendidas. Nesse caso, o beneficiário do registro de preços terá preferência de fornecimento, em igualdade de condições.

4. As quantidades constantes do Anexo I do edital licitatório são estimativas máximas para eventual fornecimento, durante o prazo de vigência da Ata de Registro de Preços.

4.1. As aquisições ocorrerão em conformidade com as necessidades e conveniências do TREPI, facultada a aquisição parcial, total ou mesmo a não aquisição dos materiais licitados.

5. O licitante vencedor deverá atender às solicitações de fornecimento dos produtos, entregando-os em perfeitas condições de uso e armazenamento, no prazo máximo estipulado na Ordem de Fornecimento, a contar do recebimento da respectiva Ordem de Fornecimento e Nota de Empenho, conforme especificado no Termo de Referência.

5.1. O licitante vencedor será responsável pela confirmação do local e horário de entrega dos materiais mediante contato telefônico com a Seção de Almoxarifado e Patrimônio, pelo telefone (86) 2107-9811.

5.2. O licitante deverá atender aos pedidos formalizados durante a vigência da Ata de Registro de Preços, ainda que a entrega seja prevista para data posterior a sua vigência.

6. O eventual fornecimento, objeto da presente Ata de Registro de Preços, obedecerá ao estipulado neste instrumento, bem como às disposições do Pregão Eletrônico nº 74/2020, além das disposições constantes da proposta apresentada pelo licitante vencedor, que independentemente de transcrição, fazem parte integrante e complementar deste documento, no que não o contrarie.

7. O licitante vencedor tem obrigação de manter, durante toda a vigência da Ata de Registro de Preços, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

E, por estarem justos e contratados, foi lavrado o presente instrumento no Sistema Eletrônico de Informações que, após lido e achado conforme vai assinado pelas partes.

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Des**.** ERIVAN JOSÉ DA SILVA LOPES
Presidente

NOVA SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E NETWORKING EIRELI
Marli Teresinha Erbe
Representante legal

ANEXO

LOCAL DE ENTREGA

Item	ÓRGÃO	Quantidade	local de entrega
1	TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ	1	Pça. Des. Edgar Nogueira, S/N, Bairro Cabral, Teresina-PI, CEP:

Item	ÓRGÃO	Quantidade	local de entrega
			64.000-920
1	INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA – MT CAMPUS JUINA - **ÓRGÃO PARTICIPANTE DA LICITAÇÃO**	1	Linha J, Quadra 8, Setor Chácara, Caixa Postal 255, Juina, Mato Grosso. CEP: 78.320-000
2	TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ	51	Pça. Des. Edgar Nogueira, S/N, Bairro Cabral, Teresina-PI, CEP: 64.000-920
3	TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ	17	Pça. Des. Edgar Nogueira, S/N, Bairro Cabral, Teresina-PI, CEP: 64.000-920
4	TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ	1	Pça. Des. Edgar Nogueira, S/N, Bairro Cabral, Teresina-PI, CEP: 64.000-920

Documento assinado eletronicamente por **MARLI TERESINHA ERBE**, **Usuário Externo**, em 27/11/2020, às 15:31, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Corregedor Regional Eleitoral**, em 28/11/2020, às 16:23, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br /sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1134550** e o código CRC **30C7A7C5**.

PROPOSTA DE PREÇOS

UASG: 070006
PREGÃO ELETRÔNICO nº 74/2020

Nome da empresa:	**Nova Serviços de Tecnologia da Informação e Networking EIRELI**				
CNPJ nº:	**10.685.932/0001-79**				
Endereço:	**SCS Quadra 04 Bloco A Lote 219/237 1º Andar Parte O, Ed. Vera Cruz**				
CEP: **70.304-913**	Cidade: **Brasília**	UF: **DF**	Telefone: **99411-7460**		
Fax:	e-mail: administrativo@grupoinovva.com.br				
Banco **Sicoob (756)**	Conta Corrente: **115241-6**	Agência: **4001 – Brasília – DF**			

ITEM	ESPECIFICAÇÕES	UNIDADE	QTDE	PREÇO (R$)	
				UNITÁRIO	TOTAL
1	Atualização da Solução de Firewall tipo concentrador com atualização dos equipamentos existentes para, no mínimo, o SonicWall NSA 5650, com serviço de suporte 24X7 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: NSA 5650 PN: 01-SSC-1939 / 01-SSC-3217 / 01-SSC-3678	Unidade	2 (1 para TRE-PI + 1 para IFMT)	R$ 295.000,00	R$ 590.000,00
2	Atualização da Solução de Firewall tipo pequeno porte com atualização dos equipamentos existentes para, no mínimo, o SonicWall SOHO 250 W, com serviço de suporte 8x5 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: SOHO 250W PN: 02-SSC-1865 / 02-SSC-1760	Unidade	51	R$ 5.700,00	R$ 290.700,00
3	Atualização da Solução de Firewall tipo pequeno porte com atualização dos equipamentos existentes para, no mínimo, o SonicWall SOHO 250 W, com serviço de suporte 8x5 cobertos pela Garantia de 60 meses Fabricante: SonicWall / Modelo: SOHO 250W PN: 02-SSC-1865 / 02-SSC-1760	Unidade	17	R$ 5.700,00	R$ 96.900,00
4	Licença SonicWall Global Management System para até 70 nós por 03 anos Referências: a) 01 Licença 01-SSC-3311; b) 02 Licenças 01-SSC-7664; c) 01 Licença 01-SSC-3301; d) 02 Licenças 01-SSC-6532; e) 02 Licenças 01-SSC-6536. Fabricante: SonicWall / Modelo: GMS PN: 01-SSC-3311 / 01-SSC-7664 / 01-SSC-3301 / 01-SSC-6532 / 01-SSC-6536	Unidade	1	R$ 175.000,00	R$ 175.000,00
	TOTAL GERAL DA PROPOSTA				**R$ 1.152.600,00**

MARLI TERESINHA ERBE:39339106091

Assinado de forma digital por MARLI TERESINHA ERBE:39339106091
Dados: 2020.11.25 10:08:15 -03'00'

Importa a presente proposta no valor total de **R$ 1.152.600,00 (um milhão, cento e cinquenta e dois mil e seiscentos reais)**

Prazo de validade da proposta: **90 (noventa) dias**;

Prazo de entrega dos materiais: **Conforme especificações do Termo de Referência**;

- **Declaramos que todos os impostos, taxas, fretes, seguros, bem como quaisquer outras despesas, diretas e indiretas, estão inclusas na proposta**

Declaramos, também, que concordamos com todas as condições estabelecidas no Edital e seus respectivos Anexos.

Declaramos, ainda, que todos os equipamentos serão entregues embalados em caixas, conforme enviado pela fábrica e têm prazo de validade indefinido, devendo evitar ser armazenados ao relento ou expostos a água e luz solar direta.

Brasília, 25 de novembro de 2020.

MARLI TERESINHA ERBE:39339106091

Assinado de forma digital por MARLI TERESINHA ERBE:39339106091
Dados: 2020.11.25 10:07:35 -03'00'

Marli Teresinha Erbe

CPF 393.391.060-91
Sócia Proprietária
administrativo@grupoinovva.com.br
(61) 9 9411-7460

SonicWall Network Security appliance (NSa) series

Industry-validated security effectiveness and performance for mid-sized networks, distributed enterprises and data centers

The SonicWall Network Security appliance (NSa) series provides organizations that range in scale from mid-sized networks to distributed enterprises and data centers with advanced threat prevention in a high-performance security platform. Utilizing innovative deep learning technologies in the SonicWall Capture Cloud Platform, the NSa series delivers the automated real-time breach detection and prevention organizations need.

Cutting-edge threat prevention with superior performance

Today's network threats are highly evasive and increasingly difficult to identify using traditional methods of detection. Staying ahead of sophisticated attacks requires a more modern approach that heavily leverages security intelligence in the cloud. Without that cloud intelligence, gateway security solutions can't keep pace with today's complex threats. NSa series next-generation firewalls (NGFWs) integrate two advanced security technologies to deliver cutting-edge threat prevention that keeps your network one step ahead. Enhancing SonicWall's multi-engine Capture Advanced Threat Protection (ATP) service is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, SonicWall's patented* single-pass Reassembly-Free Deep Packet Inspection (RFDPI) engine examines every byte of every packet, inspecting both inbound and outbound traffic on the firewall. By leveraging the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, anti-malware and web/URL filtering, the NSa series blocks even the most insidious threats at the gateway.

Further, SonicWall firewalls provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. The firewall looks deep inside every packet (the header and data) searching for protocol non-compliance, threats, zero-days, intrusions, and even defined criteria. The deep packet inspection engine detects and prevents hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.

When organizations activate deep packet inspection functions such as IPS, anti-virus, anti-spyware, TLS/SSL decryption/inspection and others on their firewalls,

Benefits:

- Superior threat prevention and performance
- Patent-pending real-time deep memory inspection technology
- Patented reassembly-free deep packet inspection technology
- On-box and cloud-based threat prevention
- TLS/SSL decryption and inspection
- Industry-validated security effectiveness
- Multi-core hardware architecture
- Dedicated Capture Labs threat research team

Network control and flexibility

- Secure SD-WAN
- Powerful SonicOS operating system
- Application intelligence and control
- Network segmentation with VLANs
- High-speed wireless security

Easy deployment, setup and ongoing management

- Zero-Touch Deployment
- Cloud-based and on-premises centralized management
- Scalable line of firewalls
- Low total cost of ownership

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723 network performance often slows down, sometimes dramatically. NSa series firewalls, however, feature a multi-core hardware architecture that utilizes specialized security microprocessors. Combined with our RTDMI and RFDPI engines, this unique design eliminates the performance degradation networks experience with other firewalls.

Network control and flexibility

At the core of the NSa series is SonicOS, SonicWall's feature-rich operating system. SonicOS provides organizations with the network control and flexibility they require through application intelligence and control, real-time visualization, an intrusion prevention system (IPS) featuring sophisticated anti-evasion technology, high-speed virtual private networking (VPN) and other robust security features.

Using application intelligence and control, network administrators can identify and categorize productive applications from those that are unproductive or potentially dangerous, and control that traffic through powerful application-level policies on both a per-user and a per-group basis (along with schedules and exception lists). Business-critical applications can be prioritized and allocated more bandwidth while non-essential applications are bandwidth-limited. Real-time monitoring and visualization provides a graphical representation of applications, users and bandwidth usage for granular insight into traffic across the network.

For distributed organizations requiring advanced flexibility in their network design, the SD-WAN technology in SonicOS is a perfect complement to NSa firewalls deployed at the headquarters or at remote and branch sites. Instead of relying on more expensive legacy technologies such as MPLS and T1, organizations using SD-WAN can choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance.

Built into every NSa series firewall is a wireless access controller that enables organizations to extend the network perimeter securely through the use of wireless technology. Together, SonicWall firewalls and SonicWave 802.11ac Wave 2 wireless access points create a wireless network security solution that combines industry-leading next-generation firewall technology with high-speed wireless for enterprise-class network security and performance across the wireless network.

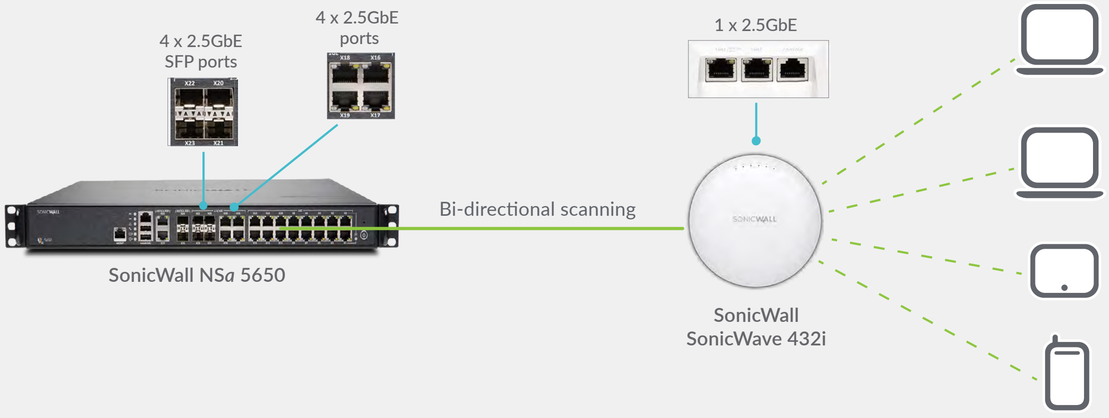
Easy deployment, setup and ongoing management

Like all SonicWall firewalls, the NSa series tightly integrates key security, connectivity and flexibility technologies into a single, comprehensive solution. This includes SonicWave wireless access points and the SonicWall WAN Acceleration (WXA) series, both of which are automatically detected and provisioned by the managing NSa firewall. Consolidating multiple capabilities eliminates the need to purchase and install point products that don't always work well together. This reduces the effort it takes to deploy the solution into the network and configure it, saving both time and money.

Cloud-based centralized management, reporting, licensing and analytics are handled through the SonicWall Capture Security Center. A key component of the Capture Security Center is Zero-Touch Deployment. This cloud-based feature simplifies and speeds the deployment and provisioning of SonicWall firewalls at remote and branch office locations. Together, the simplified deployment and setup along with the ease of management enable organizations to lower their total cost of ownership and realize a high return on investment.

Secure, High-speed Wireless

Combine an NSa series next-generation firewall with a SonicWall SonicWave 802.11ac Wave 2 wireless access point to create a high-speed wireless network security solution. NSa series firewalls and SonicWave access points both feature 2.5 GbE ports that enable multi-gigabit wireless throughput offered in Wave 2 wireless technology. The firewall scans all wireless traffic coming into and going out of the network using deep packet inspection technology and then removes harmful threats such as malware and intrusions, even over encrypted connections. Additional security and control capabilities such as content filtering, application control and intelligence and Capture Advanced Threat Protection can be run on the wireless network to provide added layers of protection.

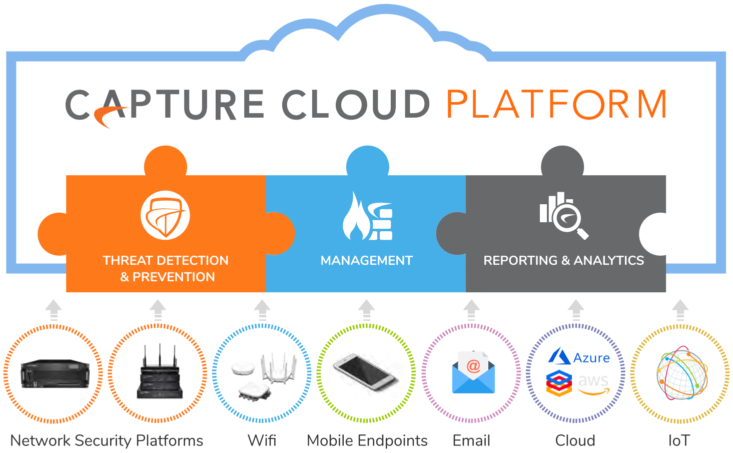


Capture Cloud Platform

SonicWall's Capture Cloud Platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. The platform consolidates threat intelligence gathered from multiple sources including our award-winning multi-engine network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe.

If data coming into the network is found to contain previously-unseen malicious code, SonicWall's dedicated, in-house Capture Labs threat research team develops signatures that are stored in the Capture Cloud Platform database and deployed to customer firewalls for up-to-date protection. New updates take effect immediately without reboots or interruptions. The signatures resident on the appliance protect against wide classes of attacks, covering tens of thousands of individual threats. In addition to the countermeasures on the appliance, NSa firewalls also have continuous access to the Capture Cloud Platform database which extends the onboard signature intelligence with tens of millions of signatures.

In addition to providing threat prevention, the Capture Cloud Platform offers single pane of glass management and administrators can easily create both real-time and historical reports on network activity.



Advanced threat protection

At the center of SonicWall's automated, real-time breach prevention are two advanced malware detection technologies; Capture Advanced Threat Protection™ (Capture ATP) and Capture Security appliance™ (CSa).

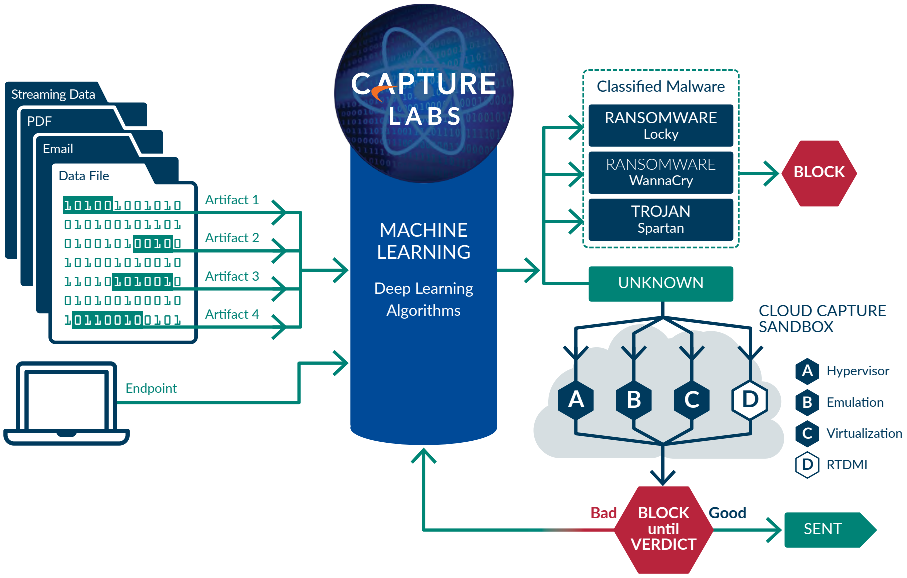
Capture ATP is a cloud-based multi-engine sandbox platform, which includes Real-Time Deep Memory Inspection™ (RTDMI), virtualized sandboxing, full system emulation and hypervisor level analysis technology. CSa is an on-premises device that features RTDMI, which utilizes memory-based static and dynamic techniques for fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day threats in a variety of SonicWall solutions such as next-generation firewalls.

Suspicious files are sent to either solution where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined.

In the case of Capture ATP, when files are identified as malicious, they are blocked, and a hash is immediately created within the Capture ATP database for all customers to leverage to block follow-on attacks. These signatures are eventually sent to firewalls to create static defenses. Results generated by CSa are not shared outside your organization for privacy and compliance reasons.

These services analyze a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

For complete endpoint protection, the SonicWall Capture Client combines next-generation antivirus technology with SonicWall's cloud-based multi-engine sandbox with optional integration with SonicWall firewalls.

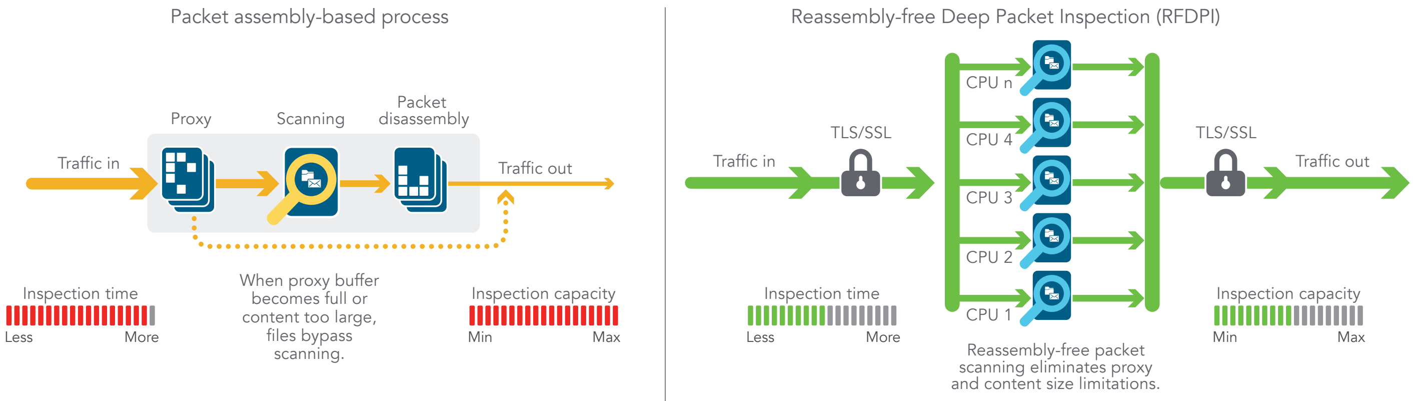


Reassembly-Free Deep Packet Inspection engine

The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. This proprietary engine relies on streaming traffic payload inspection to detect threats at Layers 3-7, and takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including TLS/SSL decryption, it is analyzed against a single, proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken.

In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.


Packet assembly-based process
Proxy
Scanning
Packet disassembly
Traffic in
Traffic out
Inspection time
Less
More
When proxy buffer becomes full or content too large, files bypass scanning.
Inspection capacity
Min
Max
Reassembly-free Deep Packet Inspection (RFDPI)
Traffic in
TLS/SSL
CPU n
CPU 4
CPU 3
CPU 2
CPU 1
TLS/SSL
Traffic out
Inspection time
Less
More
Reassembly-free packet scanning eliminates proxy and content size limitations.
Inspection capacity
Min
Max

Competitive proxy-based architecture

SonicWall stream-based architecture

Centralized management and reporting

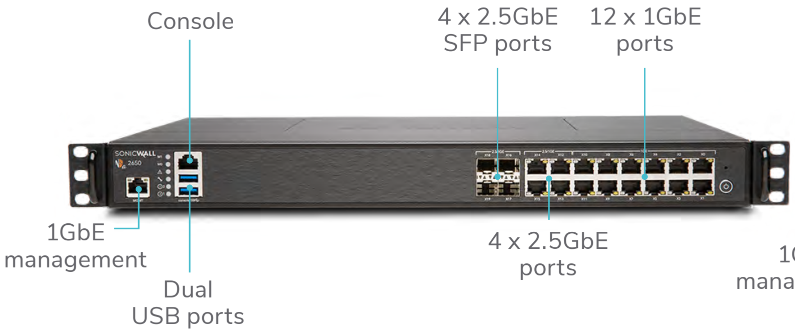
For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, SonicWall provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access points and Dell N-Series and X-Series switches through a correlated and auditable workstream process. Enterprises can easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities, and govern all operational aspects of the security infrastructure, including centralized policy management and enforcement; real-time event monitoring; user activities; application identifications; flow analytics and forensics; compliance and audit reporting; and more. In addition, enterprises meet the firewall's change management requirements through workflow automation which provides the agility and confidence to deploy the right firewall policies at the right time and in conformance with compliance regulations. Available on premises as SonicWall Global Management System and in the cloud as Capture Security Center, SonicWall management and reporting solutions provide a coherent way to manage network security by business processes and service levels, dramatically simplifying lifecycle management of your overall security environments compared to managing on a device-by-device basis.

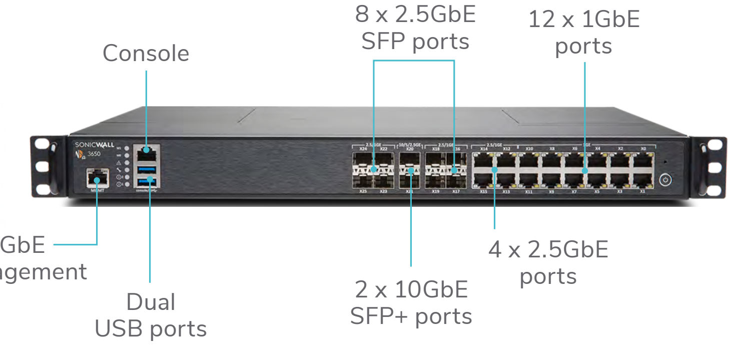
NSa 2650

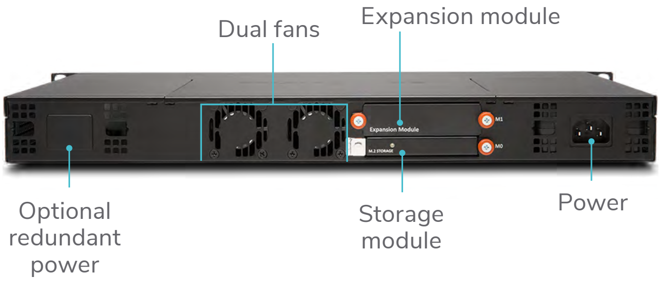
The NSa 2650 delivers high-speed threat prevention over thousands of encrypted and even more unencrypted connections to mid-sized organizations and distributed enterprises.

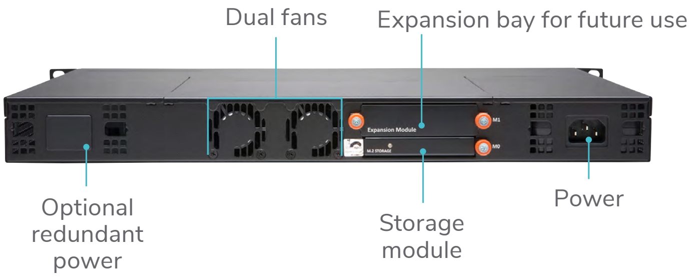
NSa 3650

The SonicWall NSa 3650 is ideal for branch office and small- to medium-sized corporate environments concerned about throughput capacity and performance.









Firewall	NSa 2650
Firewall throughput	3.0 Gbps
IPS throughput	1.4 Gbps
Anti-malware throughput	1.3 Gbps
Threat Prevention throughput	1.5 Gbps
Maximum connections	1,000,000
New connections/sec	14,000/sec
Storage module	16 GB

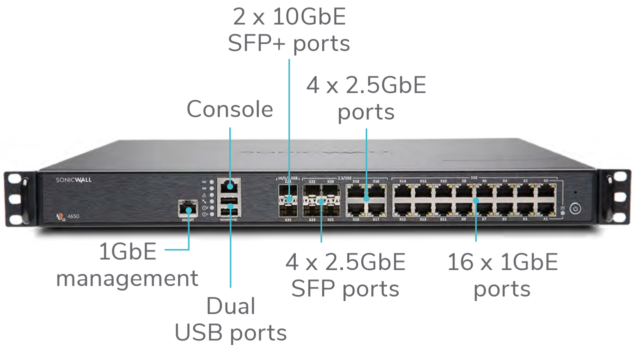
Description	SKU
NSa 2650 firewall only	01-SSC-1936
NSa 2650 TotalSecure Advanced (1-year)	01-SSC-1988

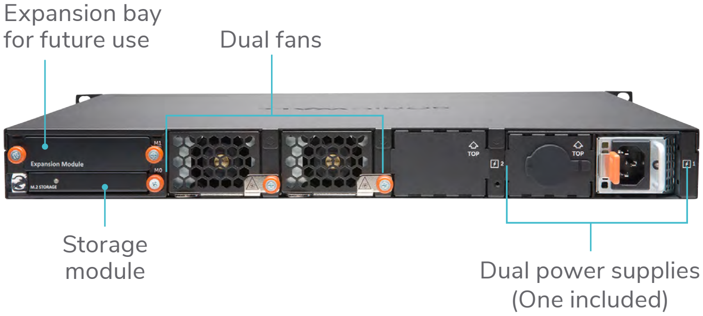
Firewall	NSa 3650
Firewall throughput	3.75 Gbps
IPS throughput	1.8 Gbps
Anti-malware throughput	1.5 Gbps
Threat Prevention throughput	1.75 Gbps
Maximum connections	2,000,000
New connections/sec	14,000/sec
Storage module	32 GB

Description	SKU
NSa 3650 firewall only	01-SSC-1937
NSa 3650 TotalSecure Advanced (1-year)	01-SSC-4081

NSa 4650

The SonicWall NSa 4650 secures growing medium-sized organizations and branch office locations with enterprise-class features and uncompromising performance.



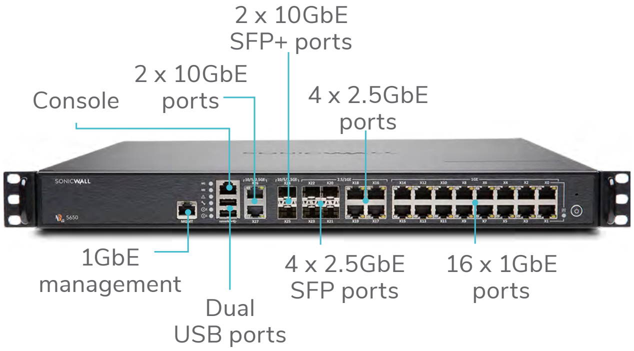

Expansion bay for future use
Dual fans
Storage module
Dual power supplies (One included)

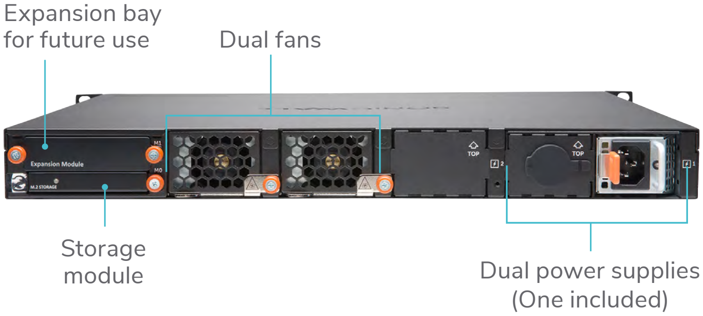
Firewall	NSa 4650
Firewall throughput	6.0 Gbps
IPS throughput	2.3 Gbps
Anti-malware throughput	2.45 Gbps
Threat Prevention throughput	2.5 Gbps
Maximum connections	3,000,000
New connections/sec	40,000/sec
Storage module	32 GB

Description	SKU
NSa 4650 firewall only	01-SSC-1938
NSa 4650 TotalSecure Advanced (1-year)	01-SSC-4094

NSa 5650

The SonicWall NSa 5650 is ideal for distributed, branch office and corporate environments needing significant throughput and high port density.



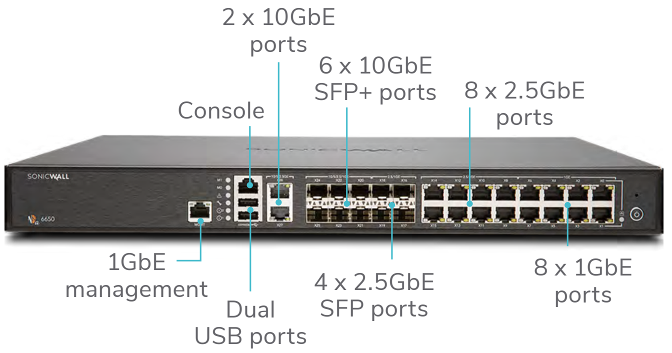

Expansion bay for future use
Dual fans
Storage module
Dual power supplies (One included)

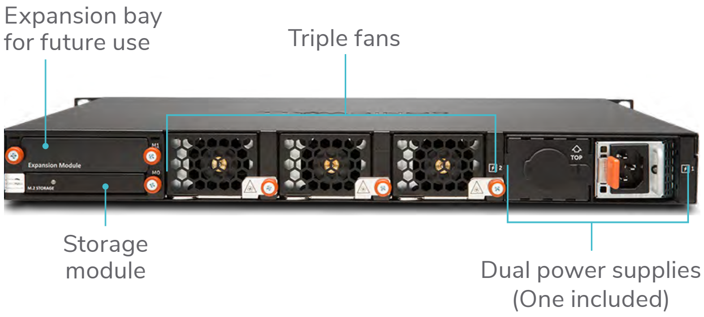
Firewall	NSa 5650
Firewall throughput	6.25 Gbps
IPS throughput	3.4 Gbps
Anti-malware throughput	2.8 Gbps
Threat Prevention throughput	3.4 Gbps
Maximum connections	4,000,000
New connections/sec	40,000/sec
Storage module	64 GB

Description	SKU
NSa 5650 firewall only	01-SSC-1939
NSa 5650 TotalSecure Advanced (1-year)	01-SSC-4342

NSa 6650

The SonicWall NSa 6650 is ideal for large distributed and corporate central site sites requiring high throughput capacity and performance.



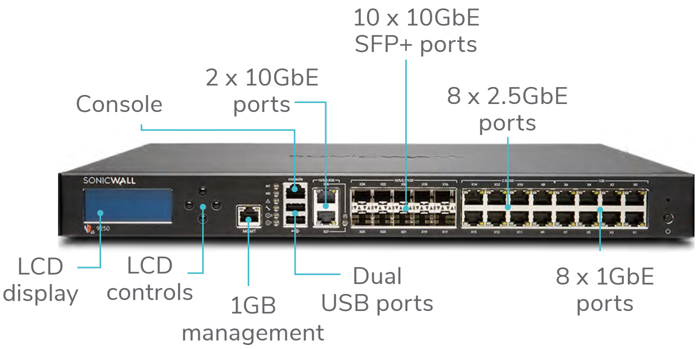

Expansion bay for future use
Triple fans
Storage module
Dual power supplies (One included)

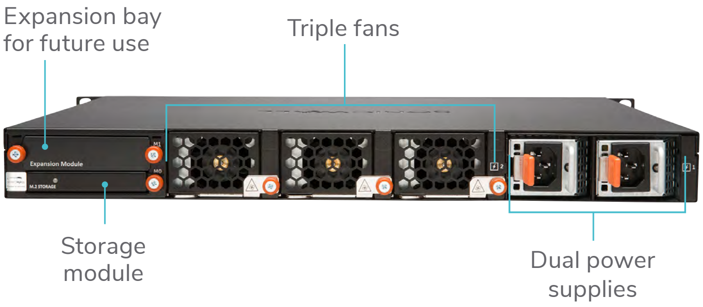
Firewall	NSa 6650
Firewall throughput	12.0 Gbps
IPS throughput	6.0 Gbps
Anti-malware throughput	5.4 Gbps
Threat Prevention throughput	5.5 Gbps
Maximum connections	5,000,000
New connections/sec	90,000/sec
Storage module	64 GB

Description	SKU
NSa 6650 firewall only	01-SSC-1940
NSa 6650 TotalSecure Advanced (1-year)	01-SSC-2209

NSa 9250/9450/9650

The SonicWall NSa 9250/9450/9650 provide distributed enterprises and data centers with scalable, deep security at multi-gigabit speeds.





Firewall	NSa 9250	NSa 9450	NSa 9650
Firewall throughput	12.0 Gbps	17.1 Gbps	17.1 Gbps
IPS throughput	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware throughput	6.5 Gbps	8.0 Gbps	8.5 Gbps
Threat Prevention throughput	6.5 Gbps	9.0 Gbps	9.4 Gbps
Maximum connections	7,500,000	10,000,000	12,500,000
New connections/sec	90,000/sec	130,000/sec	130,000/sec
Storage modules	1 TB, 128 GB	1 TB, 128 GB	1 TB, 256 GB

Description	SKU	SKU	SKU
NSa firewall only	01-SSC-1941	01-SSC-1942	01-SSC-1943
NSa TotalSecure Advanced (1-year)	01-SSC-2854	01-SSC-4358	01-SSC-3475

Features

RFDPI ENGINE

Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

Feature	Description
Secure SD-WAN	An alternative to more expensive technologies such as MPLS, Secure SD-WAN enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using using readily-available, low-cost public internet services.
REST APIs	Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
High availability/clustering	The NSa series supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI and Active/Active clustering high availability modes. Active/Active DPI offloads the deep packet inspection load to cores on the passive appliance to boost throughput.
DDoS/DoS attack protection	SYN flood protection provides a defense against DoS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DoS/DDoS through UDP/ICMP flood protection and connection rate limiting.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With SonicOS, the hardware will support filtering and wire mode implementations.
Flexible deployment options	The NSa series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.
Single and cascaded Dell N-Series and X-Series switch management	Manage security settings of additional ports, including Portshield, HA, PoE and PoE+, under a single pane of glass using the firewall management dashboard for Dell's N-Series and X-Series network switch.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.

MANAGEMENT AND REPORTING

Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

VIRTUAL PRIVATE NETWORKING (VPN)

Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the NSa series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.

Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

CONTENT/CONTEXT AWARENESS

Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching. Provides the ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.

Breach prevention subscription services

CAPTURE ADVANCED THREAT PROTECTION

Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Real-Time Deep Memory Inspection (RTDMI)	This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type and size analysis	Supports analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture ATP subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Capture Client	Capture Client is a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic. It leverages layered protection technologies, comprehensive reporting and endpoint protection enforcement.

CAPTURE SECURITY APPLIANCE (CSa)

Feature	Description
Compliance-centered malware detection	Analyze suspicious files in your own environment without sending files or results to a third-party cloud.
Built-in integrations	CSa supports out of the box integrations with other security solutions (firewalls and email security) from SonicWall.
Near real-time protection	SonicWall's patented RTDMI technology helps detect malware quickly, even for previously unknown malware, that CSa can enable the block until verdict capability on SonicWall next-generation firewalls.
Deployment	CSa can be configured on a private network directly connected to a singular edge firewall or be reachable over the Internet directly or using VPN by branch firewalls.

ENCRYPTED THREAT PREVENTION

Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic. Included with security subscriptions for all NSa series models.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.

INTRUSION PREVENTION

Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.

Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

THREAT PREVENTION

Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
Capture Cloud malware protection	A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

APPLICATION INTELLIGENCE AND CONTROL

Feature	Description
Application control	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity.
Custom application identification	Control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
Granular control	Control applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

CONTENT FILTERING

Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced Content Filtering Client	Extend policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.

ENFORCED ANTIVIRUS AND ANTI-SPYWARE

Feature	Description
Multi-layered protection	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of antivirus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

SonicOS feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6
- Biometric authentication for remote access
- DNS proxy
- REST APIs

TLS/SSL/SSH decryption and inspection[1]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- TLS/SSL control
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[1]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

Intrusion prevention[1]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[1]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application identification[1]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

HTTP/HTTPS Web content filtering[1]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Networking

- Secure SD-WAN
- PortShield
- Jumbo frames
- Enhanced logging
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DNS security
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire/virtual wire mode, tap mode
- 3G/4G WAN failover
- Asymmetric routing
- Common Access Card (CAC) support

Wireless

- WIDS/WIPS
- RF spectrum analysis
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- Auto-channel selection
- Floor plan view/Topology view
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Guest cyclic quota
- LHM guest portal

VoIP

- Granular QoS control
- Bandwidth management
- SIP and H.323 transformations per access rule
- H.323 gatekeeper and SIP proxy support

Management and monitoring

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2/v3
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat Security Analytics Platform
- SonicWall access point management
- Dell N-Series and X-Series switch management including cascaded switches

Local storage

- Logs
- Reports
- Firmware backups

[1] *Requires added subscription*

NSa series system specifications

Firewall general	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Operating system	SonicOS 6.5.4			
Interfaces	4 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 8 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*			
Built-in storage (SSD)	16 GB	32 GB	32 GB	64 GB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs			
SSO users	40,000	50,000	60,000	70,000
Maximum access points supported	48	96	128	192
Logging	Analyzer, Local Log, Syslog			

Firewall/VPN Performance	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Firewall inspection throughput[1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
Threat Prevention throughput[2]	1.5 Gbps	1.75 Gbps	2.5 Gbps	3.4 Gbps
Application inspection throughput[2]	1.85 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS throughput[2]	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
Anti-malware inspection throughput[2]	1.3 Gbps	1.5 Gbps	2.45 Gbps	2.8 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL)[2]	300 Mbps	320 Mbps	675 Mbps	800 Mbps
VPN throughput[3]	1.45 Gbps	1.5 Gbps	3.0 Gbps	3.5 Gbps
Connections per second	14,000/sec	14,000/sec	40,000/sec	40,000/sec
Maximum connections (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
Maximum connections (DPI)	500,000	750,000	1,000,000	1,500,000
Default/Maximum Connections (DPI SSL)	100,000/60,000	100,000/40,000	175,000/145,000	175,000/125,000

VPN	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Site-to-site tunnels	1,000	3,000	4,000	6,000
IPSec VPN clients (max)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			

Networking	NSa 2650	NSa 3650	NSa 4650	NSa 5650
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode			
VLAN interfaces	256	256	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications (in progress)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC			
High availability[5]	Active/Passive with State Sync	Active/Passive with State Sync Active/Active Clustering		Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering

Hardware	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Power supply	Dual, redundant 120W (one included)		Dual, redundant 350W (one included)	
Fans	Dual, Fixed		Dual, Removable	
Input power	100-240 VAC, 50-60 Hz			
Maximum power consumption (W)	37.2	46	93.6	103.6
MTBF @25°C in hours	162,231	156,681	154,529	153,243
MTBF @25°C in years	18.5	17.9	17.6	17.5
Form factor	1U Rack Mountable			
Dimensions	16.9 x 12.8 x 1.8 in (43 x 32.5 x 4.5 cm)		16.9 x 16.3 x 1.8 in (43 x 41.5 x 4.5 cm)	
Weight	11.5 lb (5.2 kg)	11.7 lb (5.3 kg)	15.2 lb (6.9 kg)	15.2 lb (6.9 kg)
WEEE weight	12.1 lb (5.5 kg)	12.3 lb (5.6 kg)	19.6 lb (8.9 kg)	19.6 lb (8.9 kg)
Shipping weight	17.0 lb (7.7 kg)	17.2 lb (7.8 kg)	24.9 lb (11.3 kg)	24.9 lb (11.3 kg)
Major regulatory	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL			
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	10-90% non-condensing			

NSa series system specifications con't

Firewall general	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Operating system	SonicOS 6.5.4			
Interfaces	6 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*			
Built-in storage (SSD)	64 GB	1TB, 128 GB	1TB, 128 GB	1TB, 256 GB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs	CLI, SSH, Web UI, GMS, REST APIs		
SSO users	70,000	80,000	90,000	100,000
Maximum access points supported	192	192	192	192
Logging	Analyzer, Local Log, Syslog, IPFIX, NetFlow			

Firewall/VPN Performance	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Firewall inspection throughput[1]	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
Threat Prevention throughput[2]	5.5 Gbps	6.5 Gbps	9.0 Gbps	9.4 Gbps
Application inspection throughput[2]	6.0 Gbps	7.8 Gbps	10.8 Gbps	11.5 Gbps
IPS throughput[2]	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware inspection throughput[2]	5.4 Gbps	6.5 Gbps	8.0 Gbps	8.5 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL)[2]	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
VPN throughput[3]	6.0 Gbps	6.75 Gbps	10.0 Gbps	10.0 Gbps
Connections per second	90,000/sec	90,000/sec	130,000/sec	130,000/sec
Maximum connections (SPI)	5,000,000	7,500,000	10,000,000	12,500,000
Maximum connections (DPI)	2,000,000	3,000,000	4,000,000	5,000,000
Default/Maximum Connections (DPI SSL)	250,000/170,000	250,000/170,000	450,000/290,000	550,000/320,000

VPN	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Site-to-site tunnels	8,000	12,000	12,000	12,000
IPSec VPN clients (max)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			

Networking	NSa 6650	NSa 9250	NSa 9450	NSa 9650
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode			
VLAN interfaces	512			
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications (in progress)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC			
High availability[5]	Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering			

Hardware	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Power supply	Dual, redundant 350W (one included)	Dual, redundant, 350W		
Fans	Triple, Removable			
Input power	100-240 VAC, 50-60 Hz			
Maximum power consumption (W)	144.3	86.7	90.9	113.1
MTBF @25°C in hours	157,193	139,783	134,900	116,477
MTBF @25°C in years	17.9	15.96	15.4	13.3
Form factor	1U Rack Mountable			
Dimensions	16.9 x 16.3 x 1.8 in (43 x 41.5 x 4.5 cm)			
Weight	17.9 lb (8.1 kg)	17.9 lb (8.1 kg)		
WEEE weight	22.5 lb (10.2 kg)	22.5 lb (10.2 kg)		
Shipping weight	27.8 lb (12.6 kg)	27.8 lb (12.6 kg)		
Major regulatory	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI			
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	10-90% non-condensing			

[1] *Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.*

[2] *Threat Prevention/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. DPI SSL performance measured on HTTPS traffic with IPS enabled.*

[3] *VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.*

[4] *For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 3,000 except for NSa 9250 and above.*

[5] *Active/Active Clustering and Active/Active DPI with State Sync require purchase of Expanded License except for NSa 9250 and above.*

**Future use. All specifications, features and availability are subject to change.*

NSa series ordering information

NSa 2650	SKU
NSa 2650 TotalSecure Advanced Edition (1-year)	01-SSC-1988
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 2650 (1-year)	01-SSC-1783
Capture Advanced Threat Protection for NSa 2650 (1-year)	01-SSC-1935
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 2650 (1-year)	01-SSC-1976
24x7 Support for NSa 2650 (1-year)	01-SSC-1541
Content Filtering Service for NSa 2650 (1-year)	01-SSC-1970
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 2650 (1-year)	01-SSC-2001

NSa 3650	SKU
NSa 3650 TotalSecure Advanced Edition (1-year)	01-SSC-4081
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 3650 (1-year)	01-SSC-3451
Capture Advanced Threat Protection for NSa 3650 (1-year)	01-SSC-3457
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 3650 (1-year)	01-SSC-3632
24x7 Support for NSa 3650 (1-year)	01-SSC-3439
Content Filtering Service for NSa 3650 (1-year)	01-SSC-3469
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 3650 (1-year)	01-SSC-4030

NSa 4650	SKU
NSa 4650 TotalSecure Advanced Edition (1-year)	01-SSC-4094
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 4650 (1-year)	01-SSC-3493
Capture Advanced Threat Protection for NSa 4650 (1-year)	01-SSC-3499
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 4650 (1-year)	01-SSC-3589
24x7 Support for NSa 4650 (1-year)	01-SSC-3487
Content Filtering Service for NSa 4650 (1-year)	01-SSC-3583
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 4650 (1-year)	01-SSC-4062

NSa 5650	SKU
NSa 5650 TotalSecure Advanced Edition (1-year)	01-SSC-4342
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 5650 (1-year)	01-SSC-3674
Capture Advanced Threat Protection for NSa 5650 (1-year)	01-SSC-3680
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 5650 (1-year)	01-SSC-3698
24x7 Support for NSa 5650 (1-year)	01-SSC-3660
Content Filtering Service for NSa 5650 (1-year)	01-SSC-3692
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 5650 (1-year)	01-SSC-4068

NSa 6650	SKU
NSa 6650 TotalSecure Advanced Edition (1-year)	01-SSC-2209
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 6650 (1-year)	01-SSC-8761
Capture Advanced Threat Protection for NSa 6650 (1-year)	01-SSC-8930
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 6650 (1-year)	01-SSC-8979
24x7 Support for NSa 6650 (1-year)	01-SSC-8663
Content Filtering Service for NSa 6650 (1-year)	01-SSC-8972
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 6650 (1-year)	01-SSC-9131

NSa 9250	SKU
NSa 9250 TotalSecure Advanced Edition (1-year)	01-SSC-2854
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 9250 (1-year)	01-SSC-0038
Capture Advanced Threat Protection for NSa 9250 (1-year)	01-SSC-0121
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9250 (1-year)	01-SSC-0343
24x7 Support for NSa 9250 (1-year)	01-SSC-0032
Content Filtering Service for NSa 9250 (1-year)	01-SSC-0331
Capture Client	Based on user count

NSa series ordering information con't

NSa 9450	SKU
NSa 9450 TotalSecure Advanced Edition (1-year)	01-SSC-4358
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 9450 (1-year)	01-SSC-0414
Capture Advanced Threat Protection for NSa 9450 (1-year)	01-SSC-0855
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9450 (1-year)	01-SSC-1196
24x7 Support for NSa 9450 0 (1-year)	01-SSC-0407
Content Filtering Service for NSa 9450 (1-year)	01-SSC-1158
Capture Client	Based on user count

NSa 9650	SKU
NSa 9650 TotalSecure Advanced Edition (1-year)	01-SSC-3475
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, 24x7 Support for NSa 9650 (1-year)	01-SSC-2036
Capture Advanced Threat Protection for NSa 9650 (1-year)	01-SSC-2042
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9650 (1-year)	01-SSC-2142
24x7 Support for NSa 9650 0 (1-year)	01-SSC-1989
Content Filtering Service for NSa 9650 (1-year)	01-SSC-2136
Capture Client	Based on user count

Modules and accessories*	SKU
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinax Cable	01-SSC-9787
10GBASE SFP+ 3M Twinax Cable	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791

**Please consult with your local SonicWall reseller for a complete list of supported SFP and SFP+ modules*

SonicWall NSa/NSv Firewall Bundle

The following NSa series firewalls are eligible to receive a one-year license to the corresponding NSv Virtual Appliance TotalSecure Subscription* at no additional cost.

Eligible NSa Firewall	Corresponding NSv Firewall
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

** NSv Virtual Appliance TotalSecure Subscription includes NSv virtual firewall, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Firewall Service, Content Filtering Service and 24x7 Support.*

Regulatory model numbers:

NSa 2650 - 1RK38-0C8
NSa 3650 - 1RK38-0C7
NSa 4650 - 1RK39-0C9
NSa 5650 - 1RK39-0CA
NSa 6650 - 1RK39-0CB
NSa 9250 - 1RK39-0CC
NSa 9450 - 1RK39-0CD
NSa 9650 - 1RK39-0CE

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com

The Gartner Peer Insights Customers' Choice logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice distinctions are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here, and are not intended in any way to represent the views of Gartner or its affiliates.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

SonicOS Platform

The SonicOS architecture is at the core of every SonicWall physical and virtual firewall including the TZ, NSa, NSv and SuperMassive Series. SonicOS leverages our patented*, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) and patent-pending Real-Time Deep Memory Inspection™ (RTDMI) technologies to deliver industry-validated high security effectiveness, SD-WAN, real-time visualization, high-speed virtual private networking (VPN) and other robust security features.

Firewall features

REASSEMBLY-FREE DEEP PACKET INSPECTION (RFDPI) ENGINE

Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

FIREWALL AND NETWORKING

Feature	Description
Secure SD-WAN	An alternative to more expensive technologies such as MPLS, Secure SD-WAN enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public internet services.
REST API	Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
High availability/clustering	Supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI2 and Active/Active clustering high availability modes.2 Active/Active DPI offloads the deep packet inspection load to passive appliance to boost throughput.
DDoS/DoS attack protection	SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The firewall can be deployed in wire, network tap NAT or Layer 2 bridge2 modes.

FIREWALL AND NETWORKING (CONTINUED)

Feature	Description
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. Policy-based routing Creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.
Single and cascaded Dell N-Series and X-Series switch management2	Manage security settings of additional ports, including Portshield, HA, PoE and PoE+, under a single pane of glass using the firewall management dashboard for Dell's N-Series and X-Series network switches.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credential from social networking service such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.
Multi-domain authentication	Provides a simple and fast way to administer security polices across all network domains. Manage individual policy to a single domain or group of domains.

MANAGEMENT AND REPORTING

Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Analytics or other tools that support IPFIX and NetFlow with extensions.

VIRTUAL PRIVATE NETWORKING (VPN)

Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

CONTENT/CONTEXT AWARENESS

Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression matching and filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

Breach prevention subscription services

CAPTURE ADVANCED THREAT PROTECTION[1]

Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK plus multiple operating systems including Windows, Android, Mac OS and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWALL Capture subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Capture Client	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and rollback to a previous uninfected state.

ENCRYPTED THREAT PREVENTION

Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden inside of encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.

INTRUSION PREVENTION[1]

Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols as they attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

THREAT PREVENTION[1]

Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
Capture Cloud malware protection	A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbond threats.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP. Decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

APPLICATION INTELLIGENCE AND CONTROL[1]

Feature	Description
Application control	Controls applications, or individual application features that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures. This increases network security and enhances network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network.
Application bandwidth management	Application bandwidth management granularly allocates and regulates available bandwidth for critical applications (or application categories), while inhibiting nonessential application traffic.
Granular control	Controls applications (or specific components of an application) based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

CONTENT FILTERING[1]

Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced content filtering client	Extends policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Blocks content using any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.
Local CFS Responder	Local CFS Responder can be deployed as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V. This provides deployment flexibility option (Light weight VM) of CFS ratings database in various customer network use cases that require a dedicated on premise solution that speeds up CFS ratings request and response times, supports large number of allowed/blocked URL list (+100K), and adds up to 1000 SonicWall firewalls for CFS rating lookups.

ENFORCED ANTI-VIRUS AND ANTI-SPYWARE[1]

Feature	Description
Multi-layered protection	Utilizes the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block viruses entering the network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

[1] *Requires added subscription*
[2] *Not supported NSv firewall series*

SonicOS feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- REST APIs

TLS/SSL/SSH decryption and inspection[2]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[2]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated & manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

Intrusion prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[2]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application identification[2]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

HTTP/HTTPS Web content filtering[2]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Secure SD-WAN
- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (RIP/OSPF/BGP)

Networking

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NSa 2650 and above)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller1
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation[1] (static and dynamic)
- Port redundancy[1]
- A/P high availability with state sync
- A/A clustering1
- Inbound/outbound load balancing
- L2 bridge,1 wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover[1]
- Asymmetric routing
- Common Access Card (CAC) support

VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

[1] *Not supported on NSv Series firewalls*
[2] *Requires added subscription.*

SonicOS feature summary (continued)

Management and monitoring

- Web GUI
- Command-line interface (CLI)
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen[1]
- Dell N-Series and X-Series switch management including cascaded switches[1]

Wireless[1]

- SonicWave AP cloud management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Guest cyclic quota
- LHM guest portal

Integrated Wireless (TZ Series only)

- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards
- Wireless intrusion detection and prevention
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

SONICWALL GLOBAL MANAGEMENT SYSTEM

Comprehensive security management, monitoring, reporting and analytics

Info Security Products Guide
2017
GLOBAL EXCELLENCE
GOLD
★★★★★

A winning security management strategy demands deep understanding of the security environment to promote better policy coordination and decisions. Not having an enterprise-wide view of the full security construct often leaves organizations at risk to preventable cyber-attacks and compliance violations. Using numerous tools running on different platforms and reporting data in different formats make security analytics and reporting operationally inefficient. This further impairs the organization's ability to quickly recognize and respond to security risks. Organizations must establish a systematic approach to governing the network security environment to overcome these challenges.

SonicWall Global Management System (GMS) solves these challenges. GMS integrates management and monitoring, analytics, forensics and audit reporting. This forms the foundation of a security governance, compliance and risk management strategy. The feature-rich GMS platform gives distributed enterprises, service providers and other organizations a fluid, holistic approach to unifying all operational aspects of their security environment. With GMS, security teams can easily manage SonicWall firewall, wireless access point, email security and secure mobile access solutions, as well as third-party network switch solutions. This is all done via a controlled and auditable work-stream process to keep networks sharp, safe and compliant. GMS includes centralized policy management and enforcement, real-time event monitoring, granular data analytics and reporting, audit trails, and more, under a unified management platform.

Benefits:

- Establishes a unified security governance, compliance and risk management security program
- Adopts a coherent and auditable approach to security orchestration, forensics, analytics and reporting
- Reduces risk and provide a fast response to security events
- Provides an enterprise-wide view of the security ecosystem
- Automates workflows and assures security operation compliance
- Operationalize firewalls at remote and branch offices in four easy steps with Zero-Touch Deployment
- Provisions, manages and monitors SD-WAN deployment, connectivity and performance centrally
- Reports on HIPAA, SOX, and PCI for internal and external auditors
- Deploys fast and easy with software, virtual appliance or cloud deployment options — all at a low cost

GOVERNS CENTRALLY

- Establish an easy path to comprehensive security management, analytic reporting and compliance to unify your network security defense program
- Automate and correlate workflows to form a fully coordinated security governance, compliance and risk management strategy

COMPLIANCE

- Helps make regulatory bodies and auditors happy with automatic PCI, HIPAA and SOX security reports
- Customize any combination of security auditable data to help you move towards specific compliance regulations

RISK MANAGEMENT

- Move fast and drive collaboration, communication and knowledge across the shared security framework
- Make informed security policy decisions based on time-critical and consolidated threat information for higher level of security efficiency

GMS provides a holistic approach to security governance, compliance and risk management

Workflow Automation

Employing native workflow automation, GMS helps security operations conform to firewall policy change management and auditing requirements of various regulatory laws such as PCI, HIPPA and GDPR. It enables policy changes by applying a series of rigorous procedures for configuring, comparing, validating, reviewing and approving firewall policies prior to deployment. The approval groups are flexible to comply with varying authorization and audit procedures from different types of organizations. Workflow automation programmatically deploys sanctioned security policies to improve operational efficiency, mitigate risks and eliminate errors.

> GMS provides a holistic approach to security governance, compliance and risk management.

1. CONFIGURE AND COMPARE

GMS configures policy **change orders** and **color-codes** differences for clear comparisons

2. VALIDATE

GMS performs an integrity **validation of the policy's** logic

3. REVIEW & APPROVE

GMS emails reviewers and logs a **(dis)approval audit trail** of the policy

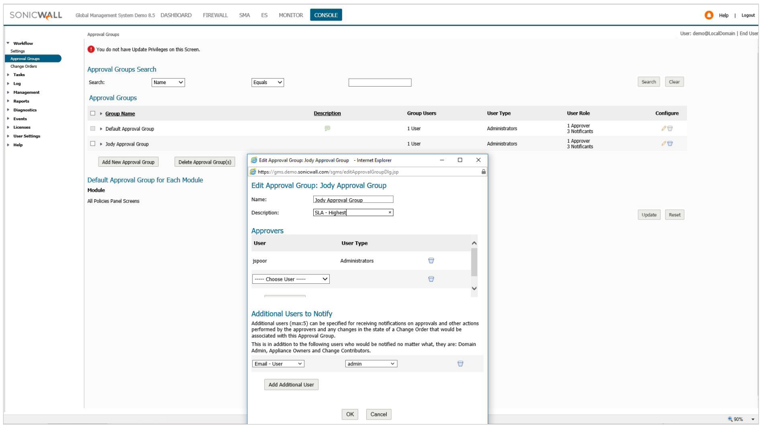
4. DEPLOY

GMS deploys the policy changes immediately or **on a schedule**

5. AUDIT

The change logs enable accurate policy **auditing** and precise **compliance** data

GMS Workflow Automation: Five steps to error-free policy management



Approval Groups

User: demo@LocalDomain | End User

You do not have Update Privileges on this Screen.

Approval Groups Search

Search: Name Equals

Approval Groups

Group Name	Description	Group Users	User Type	User Role	Configure
Default Approval Group		1 User	Administrators	1 Approver 3 Notificants	
Jody Approval Group		1 User	Administrators	1 Approver 3 Notificants	

Default Approval Group for Each Module

Module

All Policies Panel Screens

Edit Approval Group: Jody Approval Group - Internet Explorer

https://gms.demo.sonicwall.com/sgms/editApprovalGroupDlg.jsp

Edit Approval Group: Jody Approval Group

Name: Jody Approval Group

Description: SLA - Highest

Approvers

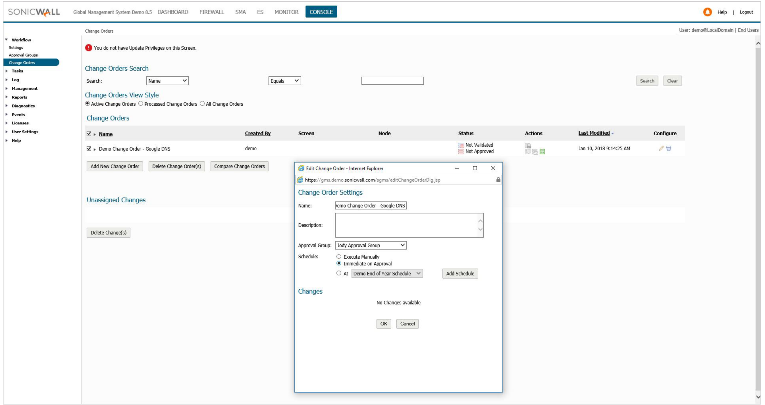
User	User Type
jspoor	Administrators
----- Choose User -----	

Additional Users to Notify

Additional users (max:5) can be specified for receiving notifications on approvals and other actions performed by the approvers and any changes in the state of a Change Order that would be associated with this Approval Group.

This is in addition to the following users who would be notified no matter what, they are: Domain Admin, Appliance Owners and Change Contributors.

Email - User admin



Change Orders

User: demo@LocalDomain | End Users

You do not have Update Privileges on this Screen.

Change Orders Search

Search: Name Equals

Change Orders View Style

● Active Change Orders ○ Processed Change Orders ○ All Change Orders

Change Orders

Name	Created By	Screen	Node	Status	Actions	Last Modified	Configure
☑ Demo Change Order - Google DNS	demo			Not Validated Not Approved		Jan 10, 2018 9:14:25 AM	

Unassigned Changes

Edit Change Order - Internet Explorer

https://gms.demo.sonicwall.com/sgms/editChangeOrderDlg.jsp

Change Order Settings

Name: emo Change Order - Google DNS

Description:

Approval Group: Jody Approval Group

Schedule: ○ Execute Manually ● Immediate on Approval ○ At Demo End of Year Schedule

Changes

No Changes available

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

Zero-Touch Deployment

Integrated into GMS is the Zero-Touch Deployment service, which simplifies and speeds the provisioning process for SonicWall firewalls at remote and branch office locations. The process requires minimal user intervention and is fully automated to operationalize firewalls at scale in four easy deployment steps. This significantly reduces the time, cost and complexity associated with installation and configuration, while security and connectivity occur instantly and automatically.

STEP 1 **REGISTER THE FIREWALL**

Registers the new firewall in MySonicWall using its assigned serial number and authentication code.

STEP 2 **CONNECT THE FIREWALL**

Connects the firewall to the network using the ethernet cable that came with the unit.

STEP 3 **POWER UP THE FIREWALL**

Power up the firewall after connecting the power cable and plugging it into a standard wall outlet. Units are automatically assigned a WAN IP using DHCP server. Once connectivity is established, the unit is automatically discovered, authenticated, and added to Capture Security Center with all licensed and configurations synchronized with MySonicWall and License Manager.

STEP 4 **MANAGE THE FIREWALL**

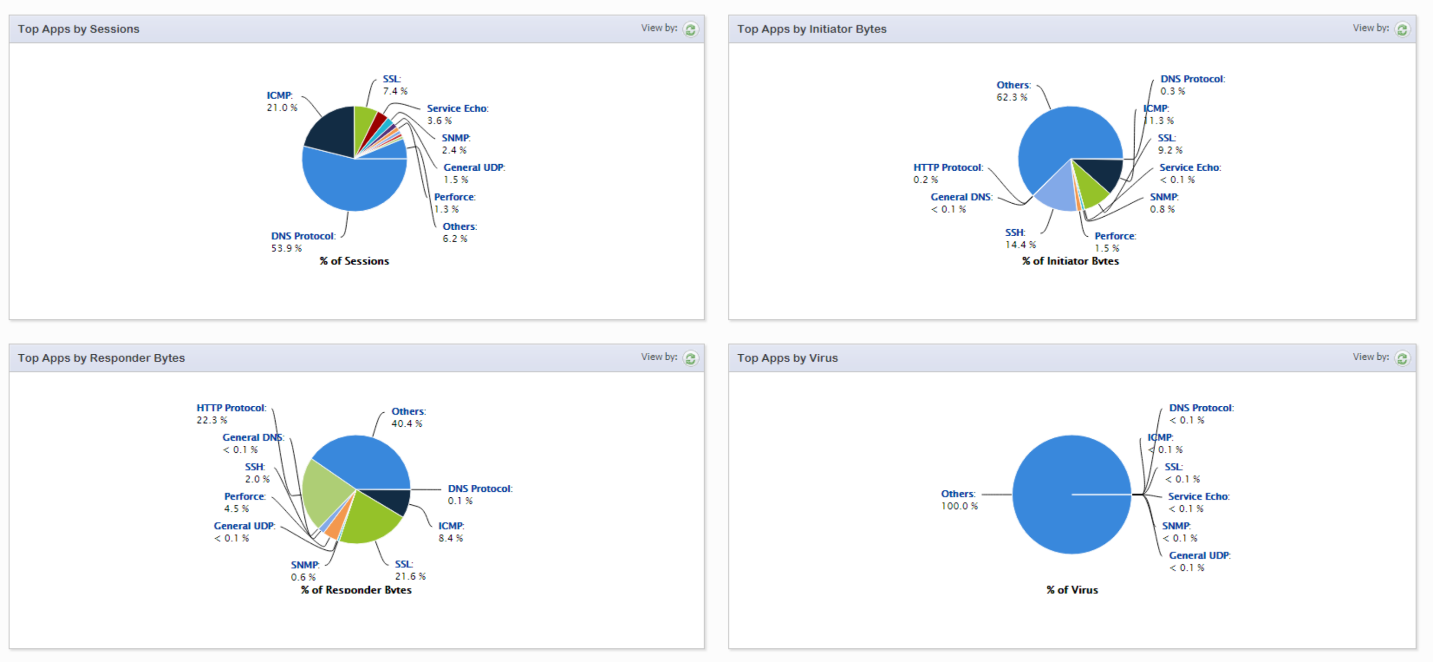
The unit is now operational and managed via the Capture Security Center cloud-based central management console such as firmware upgrades, security patching, and group level configuration changes.

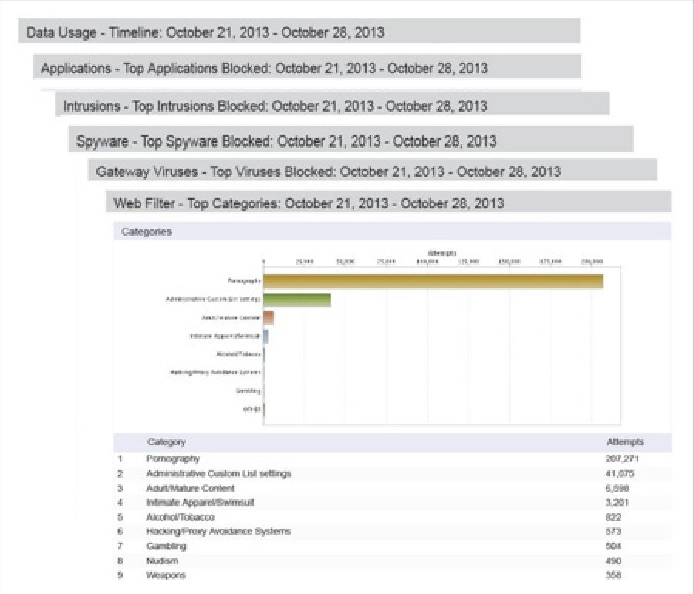
Zero-Touch Deployment: Operationalize firewall in four easy steps

Reporting

GMS offers over 140 pre-defined reports as well as the flexibility to create custom reports using any combination of auditable data to acquire various use case outcomes. These outcomes include big-picture and detailed awareness of network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and even post-mortem analysis. Every report is designed, with the collective input from many years of SonicWall customer and partner collaborations. This provides the deep granularity, scope and knowledge of syslog and IPFIX/NetFlow data needed to track, measure and run an effective network and security operation.

Intuitive graphical reports simplify managed appliance monitoring. Administrators can easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. They can also export reports to a Microsoft® Excel® spreadsheet, portable document format (PDF) file or directly to a printer for regular business review.




Data Usage - Timeline: October 21, 2013 - October 28, 2013

Applications - Top Applications Blocked: October 21, 2013 - October 28, 2013

Intrusions - Top Intrusions Blocked: October 21, 2013 - October 28, 2013

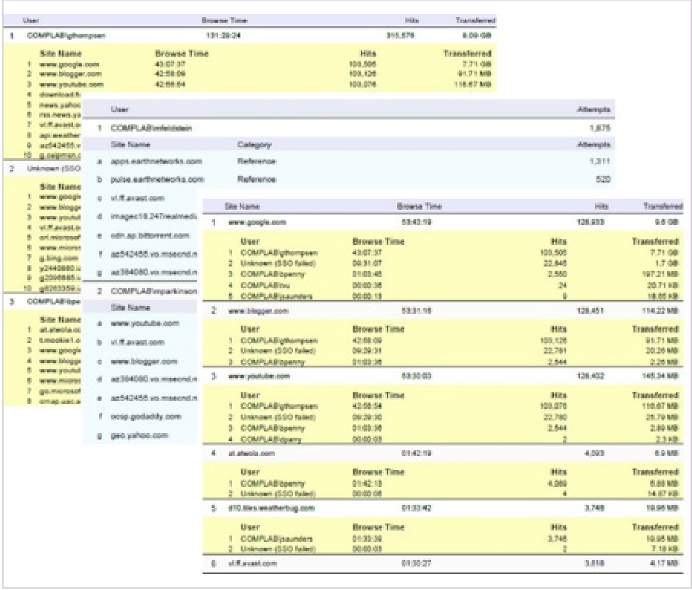
Spyware - Top Spyware Blocked: October 21, 2013 - October 28, 2013

Gateway Viruses - Top Viruses Blocked: October 21, 2013 - October 28, 2013

Web Filter - Top Categories: October 21, 2013 - October 28, 2013

Categories

	Category	Attempts
1	Pornography	207,271
2	Administrative Custom List settings	41,075
3	Adult/Mature Content	6,598
4	Intimate Apparel/Swimsuit	3,201
5	Alcohol/Tobacco	822
6	Hacking/Proxy Avoidance Systems	573
7	Gambling	504
8	Nudism	490
9	Weapons	358


	User	Browse Time	Hits	Transferred
1	COMPLAB\gthompson	131:29:24	315,578	8.09 GB

	Site Name	Browse Time	Hits	Transferred
1	www.google.com	43:07:37	103,506	7.71 GB
2	www.blogger.com	42:58:09	103,126	91.71 MB
3	www.youtube.com	42:58:54	103,076	116.67 MB
4	download.fi			
5	news.yahoo			
6	rss.news.ya			
7	vl.ff.avast.o			
8	api.weather			
9	az542455.v			
10	g.ceipmsn.c			

2 Unknown (SSO

	Site Name
1	www.googl
2	www.blogge
3	www.youtul
4	vl.ff.avast.o
5	crl.microsof
6	www.micros
7	g.bing.com
8	y2440880.u
9	g2006885.u
10	g8263359.u

3 COMPLAB\bpe

	Site Name
1	at.atwola.co
2	t.mookie1.c
3	www.google
4	www.blogge
5	www.youtul
6	www.micros
7	go.microsof
8	cmap.uac.a

	User		Attempts
1	COMPLAB\mfeldstein		1,875
	Site Name	Category	Attempts
a	apps.earthnetworks.com	Reference	1,311
b	pulse.earthnetworks.com	Reference	520
c	vl.ff.avast.com		
d	imagec18.247realmedi		
e	cdn.ap.bittorrent.com		
f	az542455.vo.msecnd.n		
g	az384080.vo.msecnd.n		
2	COMPLAB\mparkinson		
	Site Name		
a	www.youtube.com		
b	vl.ff.avast.com		
c	www.blogger.com		
d	az384080.vo.msecnd.n		
e	az542455.vo.msecnd.n		
f	ocsp.godaddy.com		
g	geo.yahoo.com		

	Site Name	Browse Time	Hits	Transferred
1	www.google.com	53:43:19	128,933	9.8 GB
	User	Browse Time	Hits	Transferred
1	COMPLAB\gthompson	43:07:37	103,506	7.71 GB
2	Unknown (SSO failed)	09:31:07	22,845	1.7 GB
3	COMPLAB\bpenny	01:03:45	2,550	197.21 MB
4	COMPLAB\tvu	00:00:36	24	20.71 KB
5	COMPLAB\jsaunders	00:00:13	9	18.65 KB
2	www.blogger.com	53:31:18	128,451	114.22 MB
	User	Browse Time	Hits	Transferred
1	COMPLAB\gthompson	42:58:09	103,126	91.71 MB
2	Unknown (SSO failed)	09:29:31	22,781	20.26 MB
3	COMPLAB\bpenny	01:03:36	2,544	2.26 MB
3	www.youtube.com	53:30:03	128,402	145.34 MB
	User	Browse Time	Hits	Transferred
1	COMPLAB\gthompson	42:58:54	103,076	116.67 MB
2	Unknown (SSO failed)	09:29:30	22,780	25.79 MB
3	COMPLAB\bpenny	01:03:36	2,544	2.89 MB
4	COMPLAB\dperry	00:00:03	2	2.3 KB
4	at.atwola.com	01:42:19	4,093	6.9 MB
	User	Browse Time	Hits	Transferred
1	COMPLAB\bpenny	01:42:13	4,089	6.88 MB
2	Unknown (SSO failed)	00:00:06	4	14.87 KB
5	d10.tiles.weatherbug.com	01:33:42	3,748	19.96 MB
	User	Browse Time	Hits	Transferred
1	COMPLAB\jsaunders	01:33:39	3,746	19.95 MB
2	Unknown (SSO failed)	00:00:03	2	7.18 KB
6	vl.ff.avast.com	01:30:27	3,618	4.17 MB

Security management and monitoring features	
Feature	Description
Centralized security and network management	Helps administrators deploy, manage and monitor a distributed network security environment.
Federate policy configuration	Easily sets policies for thousands of SonicWall firewalls, wireless access points, email security, secure remote access devices and switches from a central location.
Change Order Management and Work Flow	Assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment. The approval groups are user-configurable for adherence to company security policy. All policy changes are logged in an auditable form that ensures the firewall complies with regulatory requirements. All granular details of any changes made are historically preserved to help with compliance, audit trailing, and troubleshooting.
Zero-Touch Deployment	Simplifies and speeds the deployment and provisioning of SonicWall firewalls remotely using the cloud. Automatically pushes policies; performs firmware upgrades; and synchronizes licenses.
SD-WAN Provisioning	Centrally provision, manage and monitor SD-WAN deployment and connectivity with ease across a distributed enterprise environment.
Sophisticated VPN deployment and configuration	Simplifies the enablement of VPN connectivity, and consolidates thousands of security policies.
Offline management	Enables scheduling of configurations and firmware updates on managed appliances to minimize service disruptions.
Streamlined license management	Simplifies appliance management via a unified console, as well as the management of security and support license subscriptions.
Universal dashboard	Features customizable widgets, geographic maps and user-centric reporting.
Active-device monitoring and alerting	Provides real-time alerts with integrated monitoring capabilities, and facilitates troubleshooting efforts, thus allowing administrators to take preventative action and deliver immediate remediation.
SNMP support	Provides powerful, real-time traps for all Transmission Control Protocol/Internet Protocol (TCP/IP) and SNMP-enabled devices and applications, greatly enhancing troubleshooting efforts to pinpoint and respond to critical network events.
Application Visualization and Intelligence	Shows historic and real-time reports of what applications are being used, and by which users. Reports are completely customizable using intuitive filtering and drill-down capabilities.
Rich integration options	Provides application programming interface (API) for web services, command line interface (CLI) support for the majority of functions, and SNMP trap support for both service providers and enterprises.
Dell Networking X-Series switch management	Dell X-Series switches can now be managed easily within TZ, NSA and SuperMassive series firewalls to offer single-pane-of-glass management of the entire network security infrastructure.
Closed Network Support	Deploy GMS in closed environments, such as highly protected government networks. All license keysets and signature files from SonicWall backend services are packaged, encrypted and securely transferred to the local file system, where GMS can access, upload and then push required updates to all managed security appliances.

Security reporting and analytics	
Feature	Description
Botnet Report	Includes four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User.
Geo IP Report	Contains information on blocked traffic that is based on the traffic's country of origin or destination. Includes four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User

Security reporting and analytics (continued)

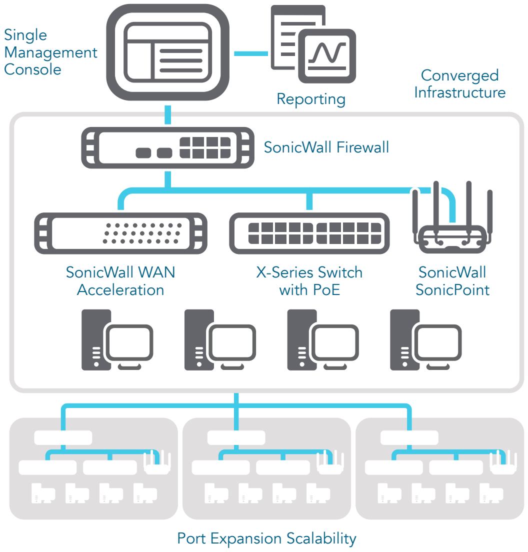
Feature	Description
MAC Address Report	Shows the Media Access Control (MAC) address on the report page. Includes device-specific information (Initiator MAC and Responder MAC) in five report types: • Data Usage > Initiators • Data Usage > Responders • Data Usage > Details • User Activity > Details • Web Activity > Initiators
Capture ATP Report	Shows detail threat behavior information to respond to a threat or infection.
HIPPA, PCI and SOX reports	Includes pre-defined PCI, HIPAA and SOX report templates to satisfy security compliance audits.
Rogue Wireless Access Point Reporting	Shows all wireless devices in use as well as rogue behavior from ad-hoc or peer-to-peer networking between hosts and accidental associations for users connecting to neighboring rogue networks.
Flow analytics and reports	Provides a flow reporting agent for application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring. Offers administrators an effective and efficient interface to visually monitor their network in real-time, providing the ability to identify applications and websites with high bandwidth demands, view application usage per user and anticipate attacks and threats encountered by the network. • A Real-Time Viewer with drag and drop customization • A Real-Time Report screen with one-click filtering • A Top Flows Dashboard with one-click View By buttons • A Flow Reports screen with five additional flow attribute tabs • A Flow Analytics screen with powerful correlation and pivoting features • A Session Viewer for deep drill-downs of individual sessions and packets.
Intelligent reporting and activity visualization	Provides comprehensive management and graphical reports for SonicWall firewalls, email security and secure mobile access devices. Enables greater insight into usage trends and security events while delivering a cohesive branding for service providers.
Centralized logging	Offers a central location for consolidating security events and logs for thousands of appliances, providing a single point to conduct network forensics.
Real-time and historic next-generation syslog reporting	Through a revolutionary enhancement in architecture, streamlines the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages. Also provides the ability to drill down into data and customize reports extensively.
Universal scheduled reports	Schedules reports that are automatically created and mailed out across multiple appliances of various types to authorized recipients.
Application traffic analytics	Provides organizations with powerful insight into application traffic, bandwidth utilization and security threats, while providing powerful troubleshooting and forensics capabilities.

Authentication security

Feature	Description
Account lockout	Account lockout policy disables a GMS user account if incorrect passwords are entered after a specified number of allowed attempts during a given period. This helps prevent attackers from guessing users' passwords and reducing the chance of successful attacks gaining unauthorized access to protected assets and data on the network.
Password Complexity	The password complexity policy sets the minimum guidelines considered important for a strong password to log in and access the GMS system.
Admin access to specific address range	Customers will be able to control admin access to specific IP address ranges.

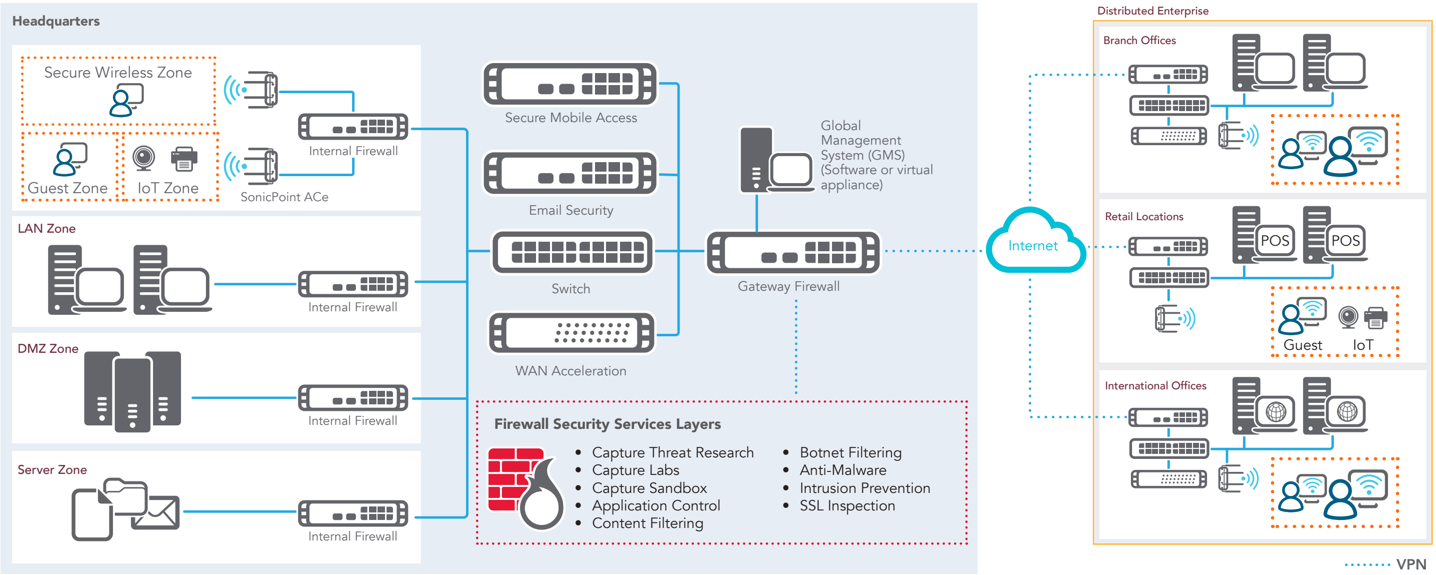
Scalable distributed architecture

GMS is an on-premises solution, deployable as a software or a virtual appliance. At the core of GMS is a distributed architecture that facilitates limitless system availability and scalability. A single instance of GMS can add visibility and control over thousands of your network security devices under its management, regardless of location. At the customer-facing level, its highly interactive universal dashboards, loaded with real-time monitoring, reporting, and analytics data, help guide smart security policy decisions, and drive collaboration, communication and knowledge across the shared security framework. With an enterprise-wide view of the security environment and real-time security intelligence reaching the right people in the organization, accurate security policies and controls actions can be made towards attaining a stronger adaptive security posture.



SonicWall Global Management System (GMS)

On-premise GMS provides a complete and scalable security management, analytic and reporting platform for distributed enterprises and data centers.



On-Premise SonicWall Global Management System Environments

Feature summary

Reporting

- Comprehensive Set of Graphical Reports
- Compliance Reporting
- Customizable Reporting with Drill Down Capabilities
- Centralized Logging
- Multi-threat Reporting
- User-centric Reporting
- Application Usage Reporting
- Granular Services Reporting
- New Attack Intelligence
- Bandwidth and Services Report per Interface
- Reporting for SonicWall Firewall Appliances
- Reporting for SonicWall SRA SSL VPN Appliances
- Universal Scheduled Reports
- Next-generation Syslog and IPFIX Reporting
- Flexible and Granular Near Real-Time Reporting
- Per User Bandwidth Reporting
- Client VPN Activity Reporting
- Detailed Summary of Services over VPN Report
- Rogue Wireless Access Point Reporting SRA SMB Web Application Firewall (WAF) Reporting

Management

- Ubiquitous Access
- Alerts and Notifications
- Diagnostic Tools
- Multiple Concurrent User Sessions
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of Email Security Policies
- Management of Secure Remote Access/SSL VPN Policies
- Management of Value Added Security Services
- Define Policy Templates at the Group Level
- Policy Replication from Device to a Group of Devices
- Policy Replication from Group Level to a Single Device
- Redundancy and High Availability
- Provisioning Management
- Scalable and Distributed Architecture
- Dynamic Management Views
- Unified License Manager
- Command Line Interface (CLI)
- Web Services Application Programming Interface (API)
- Role Based Management (Users, Groups)
- Universal Dashboard
- Backup of preference files for firewall appliances
- SD-WAN
- Zero-Touch Deployment
- Closed network support
- Firewall Sandwich support

Monitoring

IPFIX Data Flows in Real time

SNMP Support

Active Device Monitoring and Alerting

SNMP Relay Management

VPN and Firewall Status Monitoring

Live Syslog Monitoring and Alerting

Authentication Security

Account lockout

Password Complexity

Admin access to specific address range

Minimum system requirements

Below are the minimum requirements for SonicWall GMS with respect to the operating systems, databases, drivers, hardware and SonicWall-supported appliances:

Operating system[1]

- Windows Server 2016
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Standard 64-bit (English and Japanese language versions)
- Windows Server 2012 R2 Datacenter

Hardware requirements

- Use the GMS Capacity Calculator to determine the hardware requirements for your deployment.

Virtual appliance requirements

- **Hypervisor:** ESXi 6.5, 6.0 or 5.5
- Use the GMS Capacity Calculator to determine the hardware requirements for your deployment.

VMware Hardware Compatibility Guide:
www.vmware.com/resources/compatibility/search.php

Supported databases

- **External databases:** Microsoft SQL Server 2012 and 2014
- **Bundled with the GMS application:** MySQL

Internet browsers

- Microsoft® Internet Explorer 11.0 or higher (do not use compatibility mode)
- Mozilla Firefox 37.0 or higher
- Google Chrome 42.0 or higher Safari (latest version)

Supported SonicWall appliances managed by GMS

- **SonicWall Network Security Appliances:** SuperMassive E10000 and 9000 Series, E-Class NSA, NS*a* Series, and TZ Series appliances®
- **SonicWall Network Security Virtual Appliances:** NS*v* Series
- **SonicWall Secure Mobile Access (SMA) appliances:** SMA Series and E-Class SRA
- SonicWall Email Security appliances
- All TCP/IP and SNMP-enabled devices and applications for active monitoring

Global Management System (GMS) ordering information

Product	SKU
SONICWALL GMS 5 NODE SOFTWARE LICENSE	01-SSC-3311
SONICWALL GMS 10 NODE SOFTWARE LICENSE	01-SSC-7662
SONICWALL GMS 25 NODE SOFTWARE LICENSE	01-SSC-3350
SONICWALL GMS 1 NODE SOFTWARE UPGRADE	01-SSC-7664
SONICWALL GMS 5 NODE SOFTWARE UPGRADE	01-SSC-3301
SONICWALL GMS 10 NODE SOFTWARE UPGRADE	01-SSC-3303
SONICWALL GMS 25 NODE SOFTWARE UPGRADE	01-SSC-3304
SONICWALL GMS 100 NODE SOFTWARE UPGRADE	01-SSC-3306
SONICWALL GMS 250 NODE SOFTWARE UPGRADE	01-SSC-0424
SONICWALL GMS 1000 NODE SOFTWARE UPGRADE	01-SSC-7675
SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW	01-SSC-6524
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1 NODE (1 YR)	01-SSC-6514
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 5 NODE (1 YR)	01-SSC-3334
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 10 NODE (1 YR)	01-SSC-3336
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 25 NODE (1 YR)	01-SSC-3337
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 100 NODE (1 YR)	01-SSC-3338
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 250 NODE (1 YR)	01-SSC-6524
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1000 NODE (1 YR)	01-SSC-6514
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 25 NODE (1 YR)	01-SSC-3334
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 100 NODE (1 YR)	01-SSC-3336
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 250 NODE (1 YR)	01-SSC-3337
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1000 NODE (1 YR)	01-SSC-3338

About Us

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit **www.sonicwall.com** or follow us on Twitter, LinkedIn, Facebook and Instagram.

SONICWALL

SonicWall TZ series

Integrated threat prevention and SD-Branch platform for small/medium organizations and distributed enterprises

The SonicWall TZ series enables small to mid-size organizations and distributed enterprises realize the benefits of an integrated security solution that checks all the boxes. Combining high-speed threat prevention and software-defined wide area networking (SD-WAN) technology with an extensive range of networking and wireless features plus simplified deployment and centralized management, the TZ series provides a unified security solution at a low total cost of ownership.

Flexible, integrated security solution

The foundation of the TZ series is SonicOS, SonicWall's feature-rich operating system. Firewalls supporting the latest SonicOS 7.0 OS, features new modern-look UI/UX, advanced security, networking and simplified policy management capabilities.

SonicOS further includes a powerful set of capabilities that provides organizations with the flexibility to tune these Unified Threat Management (UTM) firewalls to their specific network requirements. For example, creating a secure high-speed wireless network is simplified through a built-in wireless controller which supports IEEE 802.11 standards or by adding our SonicWave 802.11ac Wave 2 access points. To reduce the cost and complexity of connecting high-speed wireless access points and other Power over Ethernet (PoE)-enabled devices such as IP cameras, phones and printers, the TZ300P, TZ600P and TZ570P provide PoE/PoE+ power.

Distributed retail businesses and campus environments can take advantage of the many tools in SonicOS to gain even greater benefits. Branch locations are able to exchange information securely with the central office using virtual private networking (VPN). Creating virtual LANs (VLANs) enables segmentation of the network into separate corporate and customer groups with rules that determine the level of communication with devices on other VLANs. SD-WAN offers a secure alternative to costly MPLS circuits while delivering consistent application performance and availability. Deploying TZ firewalls to remote locations is easy using Zero-Touch Deployment which enables provisioning of the firewall remotely through the cloud.

Superior threat prevention and performance

Our vision for securing networks in today's continually-evolving cyber threat landscape is automated, real-time threat detection and prevention. Through a combination of cloud-based and on-box technologies we deliver protection to our firewalls that's been validated by independent third-party testing for its extremely high security effectiveness. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multi-engine sandbox for analysis. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine detects and blocks malware

Benefits:

Flexible, integrated security solution

- Multi-gigabit interfaces in a desktop form factor
- Secure SD-Branch with SD-WAN
- Powerful SonicOS 7.0 operating system
- High-speed 802.11ac Wave 2 wireless
- Power over Ethernet (PoE/PoE+)
- 5G/4G/LTE support
- Built-in and expandable storage
- Redundant power

Superior threat prevention and performance

- Patent-pending real-time deep memory inspection technology
- Patented reassembly-free deep packet inspection technology
- TLS 1.3 support
- Industry-validated security effectiveness

Easy deployment, setup and ongoing management

- Zero-Touch Deployment
- Cloud-based and on-premises centralized management
- SonicExpress App onboarding

and zero-day threats by inspecting directly in memory. RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, our patented single-pass Reassembly-Free Deep Packet Inspection (RFDPI) engine examines every byte of every packet, inspecting both inbound and outbound traffic directly on the firewall. By leveraging Capture ATP with RTDMI technology in the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, anti-malware and web/ URL filtering, TZ series firewalls stop malware, ransomware and other threats at the gateway. For mobile devices used outside the firewall perimeter, SonicWall Capture Client provides an added layer of protection by applying advanced threat protection techniques such as machine learning and system rollback. Capture Client also leverages the deep inspection of encrypted TLS traffic (DPI-SSL) on TZ series firewalls by installing and managing trusted TLS certificates.

The continued growth in the use of encryption to secure web sessions means it is imperative firewalls are able to scan encrypted traffic for threats. TZ series firewalls provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. The firewall searches for protocol non-compliance, threats, zero-days, intrusions, and even defined criteria by looking deep inside every packet. The deep packet inspection engine detects and prevents hidden attacks that leverage cryptography. It also blocks encrypted malware downloads, ceases the spread of infections and thwarts command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.

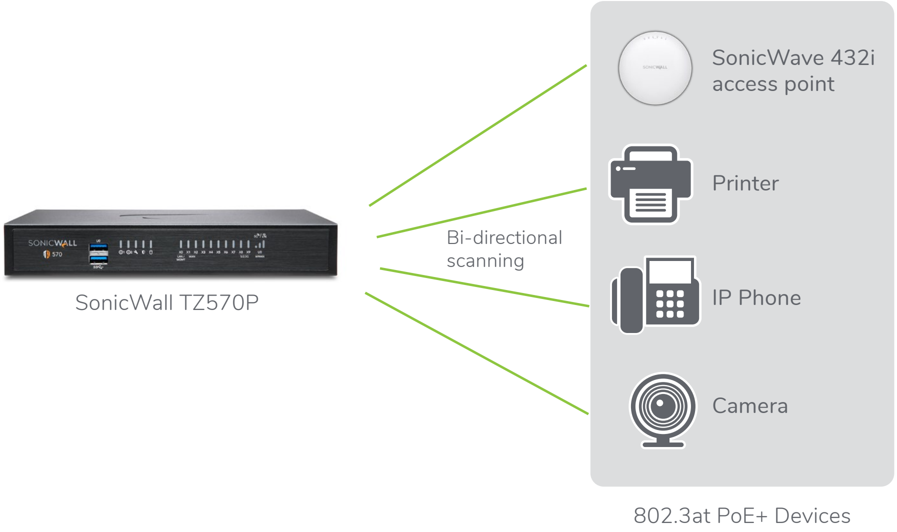
TZ670 and TZ570 provides TLS 1.3 support, which offers several changes that improves performance and security, while eliminating complexities.

Easy deployment, setup and ongoing management

SonicWall makes it easy to configure and manage TZ series firewalls and SonicWave 802.11ac Wave 2 access points no matter where you deploy them. Centralized management, reporting, licensing and analytics are handled through our cloud-based Capture Security Center which offers the ultimate in visibility, agility and capacity to centrally govern the entire SonicWall security ecosystem from a single pane of glass.

A key component of the Capture Security Center is Zero-Touch Deployment. This cloud-based feature simplifies and speeds the deployment and provisioning of SonicWall firewalls at remote and branch office locations. The process requires minimal user intervention, and is fully automated to operationalize firewalls at scale in just a few steps. This significantly reduces the time, cost and complexity associated with installation and configuration, while security and connectivity occurs instantly and automatically. Together, the simplified deployment and setup along with the ease of management enable organizations to lower their total cost of ownership and realize a high return on investment.

* 802.11ac currently not available on SOHO/SOHO 250 models; SOHO/SOHO 250 models support 802.11a/b/g/n



Integrated Security and Power for Your PoE-enabled Devices

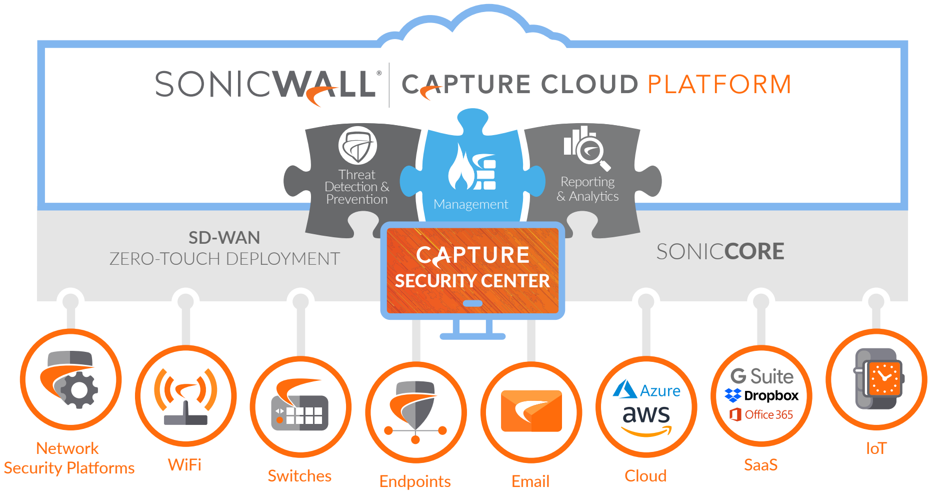
Provide power to your PoE-enabled devices without the cost and complexity of a Power over Ethernet switch or injector. TZ300P, TZ600P and TZ570P firewalls integrate IEEE 802.3at technology to power PoE and PoE+ devices such as wireless access points, cameras, IP phones and more. The firewall scans all traffic coming from and going to each device using deep packet inspection technology and then removes harmful threats such as malware and intrusions, even over encrypted connections.

Capture Cloud Platform

SonicWall's Capture Cloud Platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. The platform consolidates threat intelligence gathered from multiple sources including our award-winning multi-engine network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe.

If data coming into the network is found to contain previously-unseen malicious code, SonicWall's dedicated, in-house Capture Labs threat research team develops signatures that are stored in the Capture Cloud Platform database and deployed to customer firewalls for up-to-date protection. New updates take effect immediately without reboots or interruptions. The signatures resident on the appliance protect against wide classes of attacks, covering tens of thousands of individual threats. In addition to the countermeasures on the appliance, TZ firewalls also have continuous access to the Capture Cloud Platform database which extends the onboard signature intelligence with tens of millions of signatures.

In addition to providing threat prevention, the Capture Cloud Platform offers single pane of glass management and administrators can easily create both real-time and historical reports on network activity.



Advanced threat protection

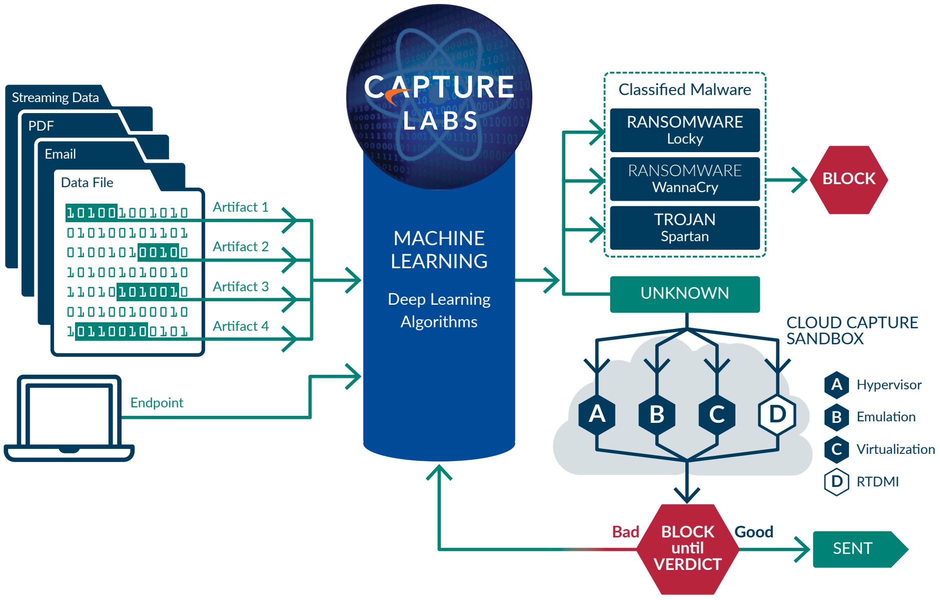
At the center of SonicWall's automated, real-time breach prevention are two advanced malware detection technologies; Capture Advanced Threat Protection™ (Capture ATP) and Capture Security appliance™ (CSa).

Capture ATP is a cloud-based multi-engine sandbox platform, which includes Real-Time Deep Memory Inspection™ (RTDMI), virtualized sandboxing, full system emulation and hypervisor level analysis technology. CSa is an on-premises device that features RTDMI, which utilizes memory-based static and dynamic techniques for fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day threats in a variety of SonicWall solutions such as next-generation firewalls.

Suspicious files are sent to either solution where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined. In the case of Capture ATP, when files are identified as malicious, they are blocked, and a hash is immediately created within the Capture ATP database for all customers to leverage to block follow-on attacks. These signatures are eventually sent to firewalls to create static defenses. Results generated by CSa are not shared outside your organization for privacy and compliance reasons.

These services analyze a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

For complete endpoint protection, the SonicWall Capture Client combines next-generation antivirus technology with SonicWall's cloud-based multi-engine sandbox with optional integration with SonicWall firewalls.

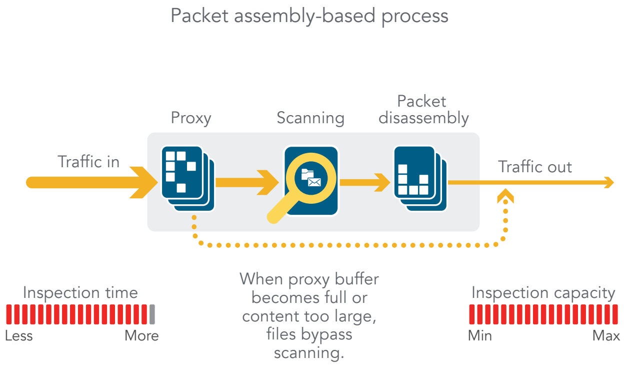


Reassembly-Free Deep Packet Inspection engine

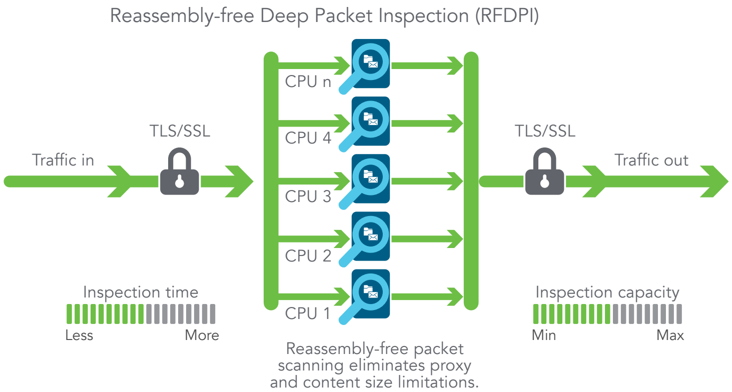
The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. This proprietary engine relies on streaming traffic payload inspection to detect threats at Layers 3-7, and takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including TLS/SSL decryption, it is analyzed against a single, proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken.

In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.


Packet assembly-based process
Proxy
Scanning
Packet disassembly
Traffic in
Traffic out
Inspection time
Less
More
When proxy buffer becomes full or content too large, files bypass scanning.
Inspection capacity
Min
Max

Competitive proxy-based architecture


Reassembly-free Deep Packet Inspection (RFDPI)
Traffic in
TLS/SSL
CPU n
CPU 4
CPU 3
CPU 2
CPU 1
TLS/SSL
Traffic out
Inspection time
Less
More
Reassembly-free packet scanning eliminates proxy and content size limitations.
Inspection capacity
Min
Max

SonicWall stream-based architecture

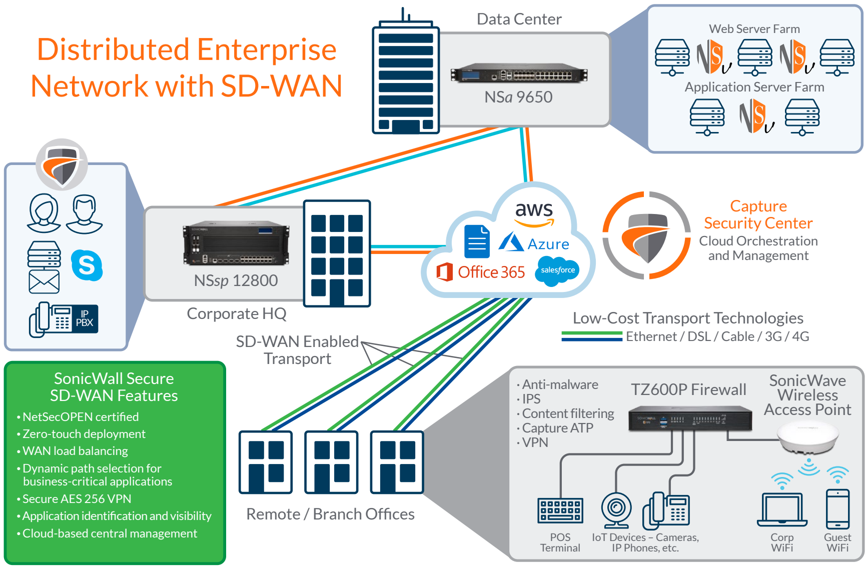
Centralized management and reporting

For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, SonicWall provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access points and Dell N-Series and X-Series switches through a correlated and auditable workstream process. Enterprises can easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities, and govern all operational aspects of the security infrastructure, including centralized policy management and enforcement; real-time event monitoring; user activities; application identifications; flow analytics and forensics; compliance and audit reporting; and more. In addition, enterprises meet the firewall's change management requirements through workflow automation which provides the agility and confidence to deploy the right firewall policies at the right time and in conformance with compliance regulations. Available on premises as SonicWall Global Management System and in the cloud as Capture Security Center, SonicWall management and reporting solutions provide a coherent way to manage network security by business processes and service levels, dramatically simplifying lifecycle management of your overall security environments compared to managing on a device-by-device basis.

Distributed networks

Because of their flexibility, TZ series firewalls are ideally suited for both distributed enterprise and single site deployments. In distributed networks like those found in retail organizations, each site has its own TZ firewall which connects to the Internet often through a local provider using a DSL, cable or 3G/4G connection. In addition to Internet access, each firewall utilizes an Ethernet connection to transport packets between remote sites and the central headquarters. Web services and SaaS applications such as Office 365, Salesforce and others are served up from the data center. Through mesh VPN technology, IT administrators can create a hub and spoke configuration for the safe transport of data between all locations.

Distributed Enterprise Network with SD-WAN



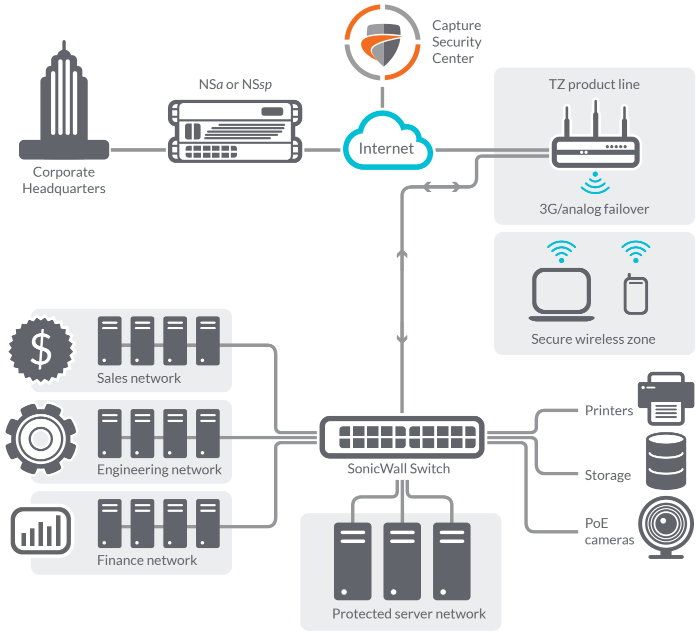
SonicWall Secure SD-WAN Features

- NetSecOPEN certified
- Zero-touch deployment
- WAN load balancing
- Dynamic path selection for business-critical applications
- Secure AES 256 VPN
- Application identification and visibility
- Cloud-based central management

The SD-WAN technology in SonicOS is a perfect complement to TZ firewalls deployed at remote and branch sites. Instead of relying on more expensive legacy technologies such as MPLS and T1, organizations using SD-WAN can choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance.

Capture Security Center

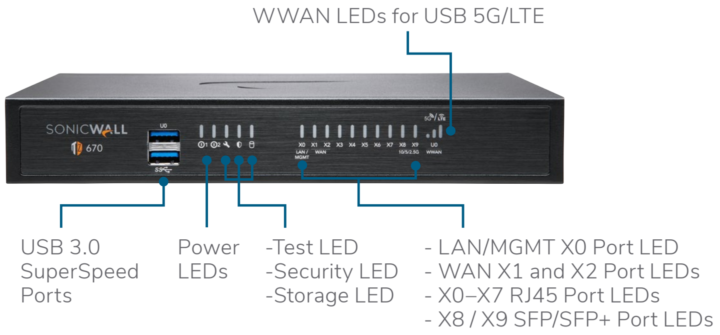
Tying the distributed network together is SonicWall's cloud-based Capture Security Center (CSC) which centralizes deployment, ongoing management and real-time analytics of the TZ firewalls. A key feature of CSC is Zero-Touch Deployment. Configuring and deploying firewalls across multiple sites is time-consuming and requires on-site personnel. However Zero-Touch Deployment removes these challenges by simplifying and speeding the deployment and provisioning of SonicWall firewalls remotely through the cloud. Similarly, CSC eases ongoing management by providing cloud-based single-pane-of-glass management for SonicWall devices on the network. For complete situational awareness of the network security environment, SonicWall Analytics offers a single-pane view into all activity occurring inside the network. Organizations gain a deeper understanding of application usage and performance while reducing the possibility of Shadow IT.

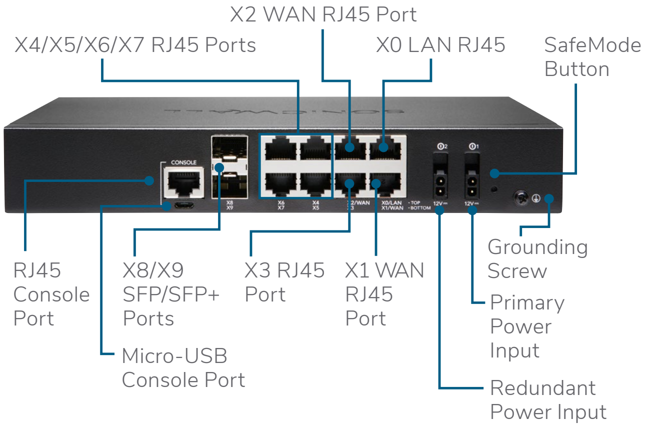


Part of CSC, SonicWall Network Security Manager (NSM), a multi-tenant centralized firewall manager, allows you to centrally manage all firewall operations error-free by adhering to auditable workflows. Its native analytic engine gives single-pane visibility and lets you monitor and uncover threats by unifying and correlating logs across all firewalls. NSM also helps you stay compliant as it provides full audit trail of every configuration changes and granular reporting. NSM scales to any size organization managing networks with up to thousands of firewall devices deployed across many locations.

SonicWall TZ670 series

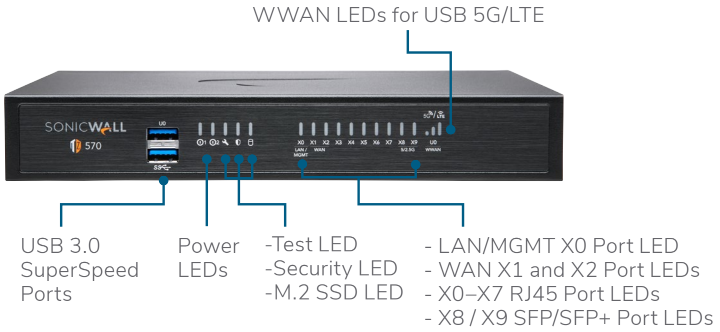
Designed for mid-sized organizations and distributed enterprise with SD-Branch locations, the TZ670 delivers industry-validated security effectiveness with best-in-class price-performance.

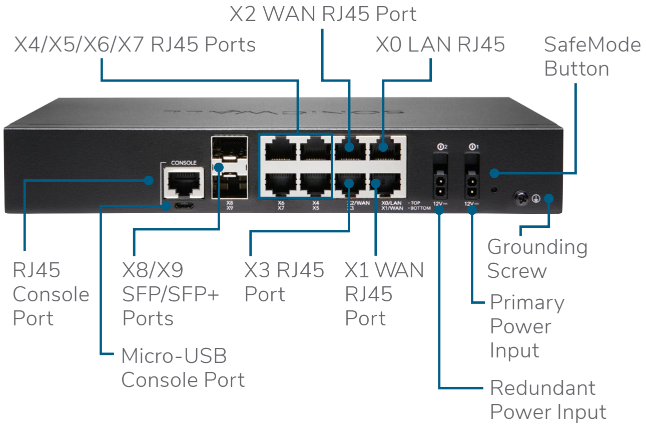




SonicWall TZ570 series

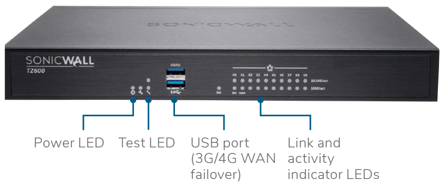
Designed for small to mid-sized organizations and distributed enterprise with SD-Branch locations, the TZ570 series deliver industry-validated security effectiveness with best-in-class price-performance.

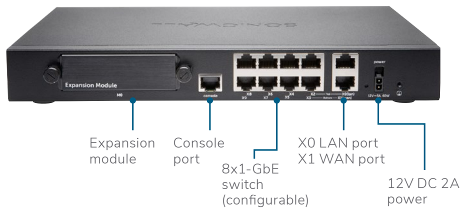


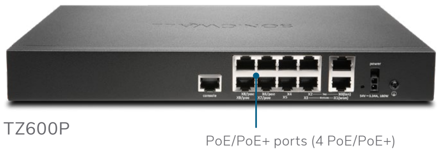


SonicWall TZ600 series

For emerging enterprises, retail and branch offices looking for security, performance and options such as 802.3at PoE+ support at a value price, the SonicWall TZ600 secures networks with enterprise-class features and uncompromising performance.

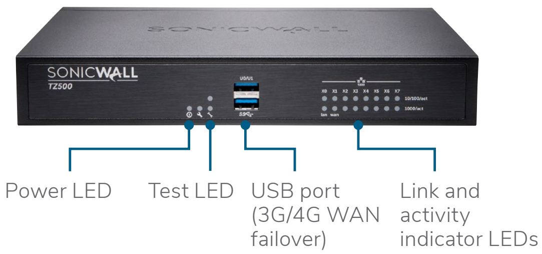

Power LED
Test LED
USB port (3G/4G WAN failover)
Link and activity indicator LEDs

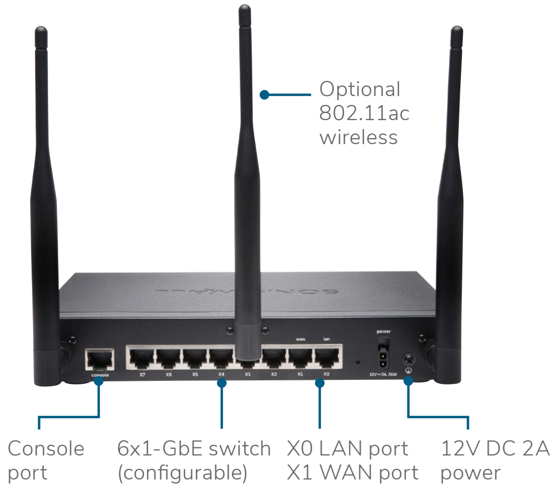



TZ600P

SonicWall TZ500 series

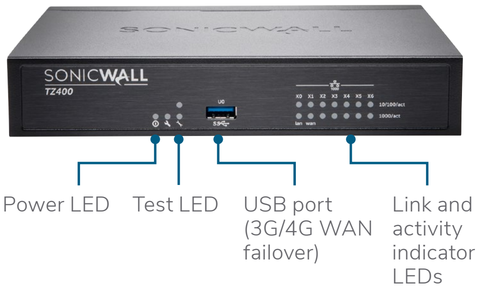
For growing branch offices and SMBs, the SonicWall TZ500 series delivers highly effective, no-compromise protection with network productivity and optional integrated 802.11ac dual-band wireless.

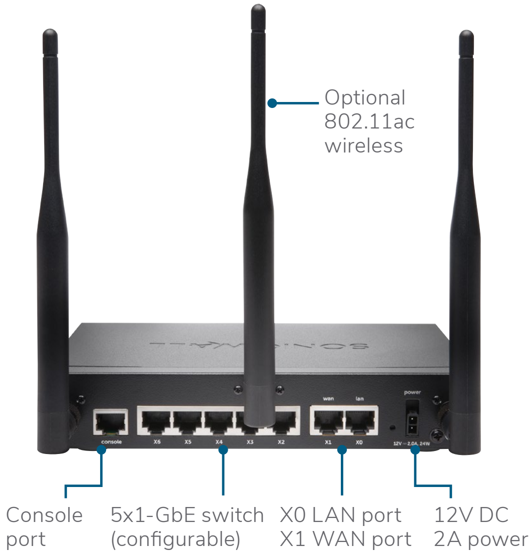

Power LED
Test LED
USB port (3G/4G WAN failover)
Link and activity indicator LEDs



SonicWall TZ400 series

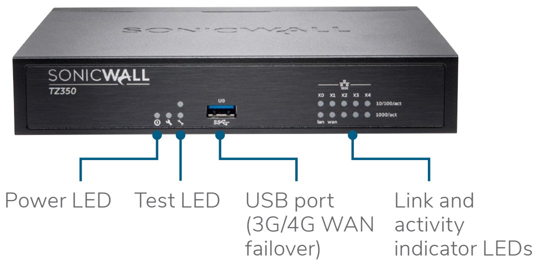
For small business, retail and branch office locations, the SonicWall TZ400 series delivers enterprise-grade protection. Flexible wireless deployment is available with optional 802.11ac dual-band wireless integrated into the firewall.


Power LED
Test LED
USB port (3G/4G WAN failover)
Link and activity indicator LEDs

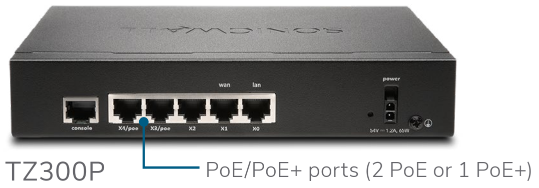


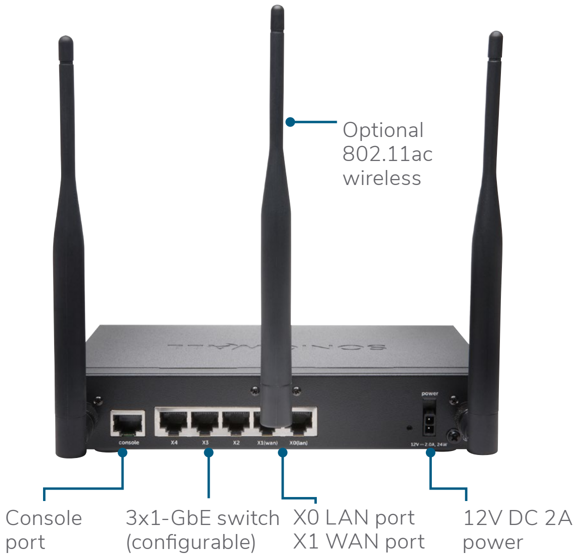
SonicWall TZ350/TZ300 series

The SonicWall TZ300 and TZ350 series offer an all-in-one solution that protects networks from advanced attacks. Unlike consumer grade products, these UTM firewalls combine high-speed intrusion prevention, anti-malware and content/URL filtering plus broad secure mobile access support for laptops, smartphones and tablets along with optional integrated 802.11ac wireless. In addition, the TZ300 offers optional 802.3at PoE+ to power PoE-enabled devices.



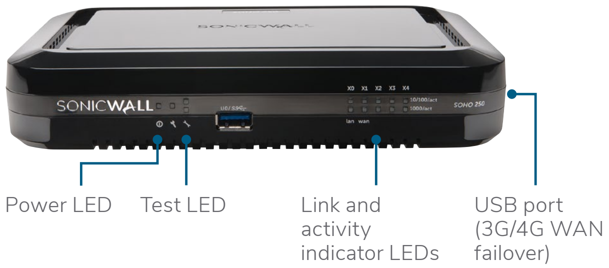
Power LED
Test LED
USB port (3G/4G WAN failover)
Link and activity indicator LEDs



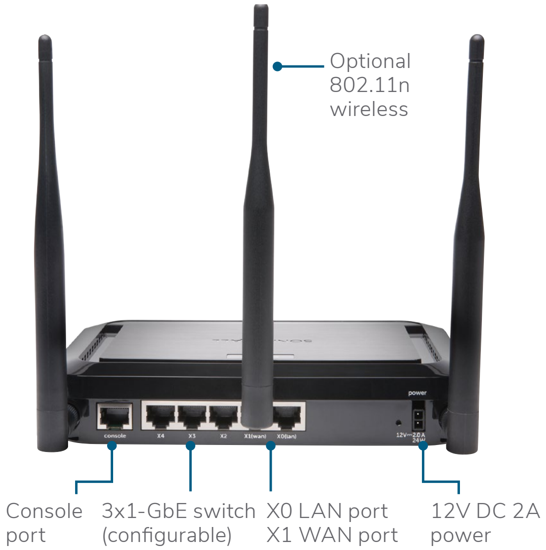


SonicWall SOHO 250/SOHO series

For wired and wireless small and home office environments, the SonicWall SOHO 250 and SOHO series deliver the same business-class protection large organizations require at a more affordable price point. Add optional 802.11n wireless to provide employees, customers and guests with secure wireless connectivity.



Power LED
Test LED
Link and activity indicator LEDs
USB port (3G/4G WAN failover)



Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

SonicOS 7.0 feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- Full API support
- SonicWall Switch integration
- SD-WAN scalability
- SD-WAN Usability Wizard[1]
- SonicCoreX and SonicOS containerization[1]
- Connections scalability (SPI, DPI, DPI SSL)

Enhanced dashboard[1]

- Enhanced device view
- Top traffic and user summary
- Insights to threats
- Notification center

TLS/SSL/SSH decryption and inspection

- TLS 1.3 with enhanced security[1]
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Enhancements for DPI-SSL with CFS
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[2]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

Intrusion prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[2]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application identification[2]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

HTTP/HTTPS Web content filtering[2]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Secure SD-WAN
- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Networking

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NSa 2650 and above)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- A/P high availability with state sync
- Inbound/outbound load balancing
- High availability - Active/Standby with state sync
- L2 bridge, wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing
- Common Access Card (CAC) support

VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

Management, monitoring and support

- Capture Security Appliance (CSa) support
- Capture Threat Assessment (CTA) v2.0
  - New design or template
  - Industry and global average comparison
- New UI/UX, Intuitive feature layout[1]
  - Dashboard
  - Device information, application, threats
  - Topology view
  - Simplified policy creation and management
- Policy/Objects usage statistics[1]
  - Used vs Un-used
  - Active vs Inactive
- Global search for static data
- Storage support[1]
- Internal and external storage management[1]
- WWAN USB card support (5G/LTE/4G/3G)
- Network Security Manager (NSM) support
- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- CSC Simple Reporting[1]
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualization
- IPv4 and IPv6 management
- CD management screen
- Dell N-Series and X-Series switch management including cascaded switches

Debugging and diagnostics

- Enhanced packet monitoring
- SSH terminal on UI

Wireless

- SonicWave AP cloud management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- RF enhancements and improvements
- Guest cyclic quota

Integrated Wireless Models

- 802.11ac Wave 2 wireless (TZ570W)
- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards
- Wireless intrusion detection and prevention
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

[1] New feature, available on SonicOS 7.0
[2] Requires added subscription

SonicWall TZ Series system specifications — SOHO, SOHO 250, TZ300 and TZ350

FIREWALL GENERAL	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Operating system	SonicOS			
Interfaces	5x1GbE, 1 USB, 1 Console		5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console
Power over Ethernet (PoE) support	—	—	TZ300P - 2 ports (2 PoE or 1 PoE+)	—
Expansion	USB			
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs			
Single Sign-On (SSO) Users	250	350	500	500
VLAN interfaces	25			
Access points supported (maximum)	2	4	8	8
FIREWALL/VPN PERFORMANCE	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Firewall inspection throughput[1]	300 Mbps	600 Mbps	750 Mbps	1.0 Gbps
Threat Prevention throughput[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Application inspection throughput[2]	—	275 Mbps	375 Mbps	600 Mbps
IPS throughput[2]	200 Mbps	250 Mbps	300 Mbps	400 Mbps
Anti-malware inspection throughput[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	30 Mbps	50 Mbps	60 Mbps	65 Mbps
IPSec VPN throughput[3]	150 Mbps	200 Mbps	300 Mbps	430 Mbps
Connections per second	1,800	3,000	5,000	6,000
Maximum connections (SPI)	10,000	50,000	100,000	100,000
Maximum connections (DPI)	10,000	50,000	90,000	90,000
Maximum connections (DPI SSL)	250	25,000	25,000	25,000
VPN	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Site-to-site VPN tunnels	10	10	10	15
IPSec VPN clients (maximum)	1 (5)	1 (5)	1 (10)	2 (10)
SSL VPN licenses (maximum)	1 (10)	1 (25)	1 (50)	1 (75)
Virtual assist bundled (maximum)	—	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP[4]			
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN			
Global VPN client platforms supported	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10			
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)			
SECURITY SERVICES	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL			
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists			
Comprehensive Anti-Spam Service	Supported			
Application Visualization	No	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes
NETWORKING	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay			
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode			
Routing protocols[4]	BGP[4], OSPF, RIPv1/v2, static routes, policy-based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)			

SonicWall TZ series specifications cont'd — SOHO, SOHO 250, TZ300 and TZ350

NETWORKING CONT'D	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database		LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)	
Local user database	150			
VoIP	Full H.323v1-5, SIP			
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications[5]	FIPS 140-2 (with Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)			
Common Access Card (CAC)	Supported			
High availability	No		Active/standby	
HARDWARE	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Form factor	Desktop			
Power supply	24W external		24W external 65W external (TZ300P only)	24W external
Maximum power consumption (W)	6.4 / 11.3	6.9 / 11.3	6.9 / 12.0	6.9 / 12.0
Input power	100 to 240 VAC, 50-60 Hz, 1 A			
Total heat dissipation	21.8 / 38.7 BTU	23.5 / 38.7 BTU	23.5 / 40.9 BTU	23.5 / 40.9 BTU
Dimensions	3.6 x 14.1 x 19 cm 1.42 x 5.55 x 7.48 in		3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 in	3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 in
Weight	0.34 kg / 0.75 lbs 0.48 kg / 1.06 lbs		0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs
WEEE weight	0.80 kg / 1.76 lbs 0.94 kg / 2.07 lbs		1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs
Shipping weight	1.20 kg / 2.64 lbs 1.34 kg / 2.95 lbs		1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs
MTBF (in years)	58.9/56.1 (wireless)	56.1	56.1	56.1
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	5-95% non-condensing			
REGULATORY	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL		FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL	
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH		FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	
INTEGRATED WIRELESS	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Standards	802.11 a/b/g/n		802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	
Frequency bands[6]	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz		802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz	

SonicWall TZ series system specifications cont'd — SOHO, SOHO 250, TZ300 and TZ350

INTEGRATED WIRELESS	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64;		802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64	
Transmit output power	Based on the regulatory domain specified by the system administrator			
Transmit power control	Supported			
Data rates supported	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel		802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel	
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)		802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	

**Future use*

[1] *Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.*

[2] *Threat Prevention/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. DPI SSL performance measured on HTTPS traffic with IPS enabled.*

[3] *VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.*

[4] *BGP is available only on SonicWall TZ350, TZ400, TZ500 and TZ600.*

[5] *Pending FIPS and ICSA approval on SOHO 250 and TZ350*

[6] *All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access point products*

SonicWall TZ series system specifications — TZ400, TZ500 and TZ600

FIREWALL GENERAL	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Operating system	SonicOS		
Interfaces	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Power over Ethernet (PoE) support	—	—	TZ600P - 4 ports (4 PoE or 4 PoE+)
Expansion	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs		
Single Sign-On (SSO) Users	500	500	500
VLAN interfaces	50	50	50
Access points supported (maximum)	16	16	24
FIREWALL/VPN PERFORMANCE	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Firewall inspection throughput[1]	1.3 Gbps	1.4 Gbps	1.9 Gbps
Threat Prevention throughput[2]	600 Mbps	700 Mbps	800 Mbps
Application inspection throughput[2]	1.2 Gbps	1.3 Gbps	1.8 Gbps
IPS throughput[2]	900 Mbps	1.0 Gbps	1.2 Gbps
Anti-malware inspection throughput[2]	600 Mbps	700 Mbps	800 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	180 Mbps	225 Mbps	300 Mbps
IPSec VPN throughput[3]	900 Mbps	1.0 Gbps	1.1 Gbps
Connections per second	6,000	8,000	12,000
Maximum connections (SPI)	150,000	150,000	150,000
Maximum connections (DPI)	125,000	125,000	125,000
Maximum connections (DPI SSL)	25,000	25,000	25,000
VPN	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Site-to-site VPN tunnels	20	25	50
IPSec VPN clients (maximum)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	2 (100)	2 (150)	2 (200)
Virtual assist bundled (maximum)	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography		
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v		
Route-based VPN	RIP, OSPF, BGP		
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN		
Global VPN client platforms supported	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10		
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE		
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)		
SECURITY SERVICES	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL		
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists		
Comprehensive Anti-Spam Service	Supported		
Application Visualization	Yes	Yes	Yes
Application Control	Yes	Yes	Yes
Capture Advanced Threat Protection	Yes	Yes	Yes
NETWORKING	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay		
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode		
Routing protocols[4]	BGP[4], OSPF, RIPv1/v2, static routes, policy-based routing		
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)		

SonicWall TZ series system specifications cont'd — TZ400, TZ500 and TZ600

NETWORKING	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)		
Local user database	150	250	
VoIP	Full H.323v1-5, SIP		
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications	FIPS 140-2 (with Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)		
Common Access Card (CAC)	Supported		
High availability	Active/standby	Active/Standby with stateful synchronization	

HARDWARE	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Form factor	Desktop		
Power supply	24W external	36W external	60W external 180W external (TZ600P only)
Maximum power consumption (W)	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100-240 VAC, 50-60 Hz, 1 A		
Total heat dissipation	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 in	3.5 x 15 x 22.5 cm 1.38 x 5.91 x 8.86 in	3.5 x 18 x 28 cm 1.38 x 7.09 x 11.02 in
Weight	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.92 kg / 2.03 lbs 1.05 kg / 2.31 lbs	1.47 kg / 3.24 lbs
WEEE weight	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.34 kg / 2.95 lbs 1.48 kg / 3.26 lbs	1.89 kg /4.16 lbs
Shipping weight	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.93 kg / 4.25 lbs 2.07 kg / 4.56 lbs	2.48 kg / 5.47 lbs
MTBF (in years)	54.0	40.8	18.4
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)		
Humidity	5-95% non-condensing		

REGULATORY	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/ GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/ GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/ MSIP, ANATEL	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/ TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/ TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	—

SonicWall TZ series system specifications cont'd — TZ400, TZ500 and TZ600

INTEGRATED WIRELESS	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Standards	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS		—
Frequency bands[5]	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 5.180-5.825 GHz		—
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64		—
Transmit output power	Based on the regulatory domain specified by the system administrator		—
Transmit power control	Supported		—
Data rates supported	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel		—
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)		—

SonicWall TZ series specifications — TZ570 and TZ670

FIREWALL GENERAL	TZ570 SERIES	TZ670 SERIES
Operating system	SonicOS 7.0	
Interfaces	8x1GbE, 2x5GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Console
Power over Ethernet (PoE) support	TZ570P (5 PoE or 3PoE+)	—
Expansion	Storage Expansion Slot (Up to 256GB)	Storage Expansion Slot (Up to 256GB) (32GB included)
Management	Network Security Manager, CLI, SSH, Web UI, GMS, REST APIs	
Single Sign-On (SSO) Users	2,500	2,500
VLAN interfaces	256	256
Access points supported (maximum)	32	32
FIREWALL/VPN PERFORMANCE	TZ570 SERIES	TZ670 SERIES
Firewall inspection throughput[1]	4.00 Gbps	5.00 Gbps
Threat Prevention throughput[2]	2.00 Gbps	2.50 Gbps
Application inspection throughput[2]	2.5 Gbps	3.0 Gbps
IPS throughput[2]	2.5 Gbps	3.0 Gbps
Anti-malware inspection throughput[2]	2.00 Gbps	2.50 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	750 Mbps	800 Mbps
IPSec VPN throughput[3]	1.80 Gbps	2.10 Gbps
Connections per second	16,000	25,000
Maximum connections (SPI)	1,250,000	1,500,000
Maximum connections (DPI)	400,000	500,000
Maximum connections (DPI SSL)	30,000	30,000
VPN	TZ570 SERIES	TZ670 SERIES
Site-to-site VPN tunnels	200	250
IPSec VPN clients (maximum)	10 (500)	10 (500)
SSL VPN licenses (maximum)	2 (200)	2 (250)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography	
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v	
Route-based VPN	RIP, OSPF, BGP	
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN	
Global VPN client platforms supported	Microsoft® Windows 10	
NetExtender	Microsoft® Windows 10, Linux	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10	
SECURITY SERVICES	TZ570 SERIES	TZ670 SERIES
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL	
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists	
Comprehensive Anti-Spam Service	Yes	
Application Visualization	Yes	
Application Control	Yes	
Capture Advanced Threat Protection	Yes	
DNS Security	Yes	

SonicWall TZ series specifications cont'd — TZ570 and TZ670

NETWORKING	TZ570 SERIES	TZ670 SERIES
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay	
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode	
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing	
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)	
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)	
Local user database	250	
VoIP	Full H.323v1-5, SIP	
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE a802.3	
Certifications pending	FIPS 140-2 (with Suite B) Level 2, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)	

HARDWARE	TZ570 SERIES	TZ670 SERIES
Form Factor	Desktop[5]	
Power supply	60W external 180W external (TZ570P only)	60W external
Maximum power consumption (W)	13.1	13.1
Input Voltage & Frequency	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz
Total heat dissipation	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.5 x 15 x 22.5 (cm) 1.38 x 5.91 x 8.85 in	3.5 x 15 x 22.5 (cm) 1.38 x 5.91 x 8.85 in
Weight	0.97 kg / 2.14 lbs	0.97 kg / 2.14 lbs
WEEE weight	1.42 kg / 3.13 lbs	1.42 kg / 3.13 lbs
Shipping weight	1.93 kg / 4.25 lbs	1.93 kg / 4.25 lbs
MTBF @25°C in years	26.1	43.9
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)	
Humidity	5-95% non-condensing	

REGULATORY	TZ570 SERIES	TZ670 SERIES
Major regulatory compliance (wired models - TZ670, TZ570)	FCC Class B, FCC , ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL/cUL, TUV/GS, CB, Mexico DGN notice by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Class B, FCC , ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL/cUL, TUV/GS, CB, Mexico DGN notice by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL
Major regulatory compliance (wireless models - TZ570W)	FCC Class B, FCC P15C, FCC P15E, ICES Class B, ISED/IC, CE (RED, RoHS), C-Tick, VCCI Class B, Japan Wireless, UL/cUL, TUV/GS, CB, Mexico DGN notice by UL, WEEE, REACH, BSMI, NCC (TW) KCC/MSIP, SRRC, ANATEL	—
Major regulatory compliance (PoE models - TZ570P)	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico DGN notice by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	—

SonicWall TZ series specifications cont'd — TZ570 and TZ670

INTEGRATED WIRELESS	TZ570 SERIES	TZ670 SERIES
Standards	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	—
Frequency bands[5]	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 5.180-5.825 GHz	—
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64	—
Transmit output power	Based on the regulatory domain specified by the system administrator	—
Transmit power control	Supported	—
Data rates supported	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel	—
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	—

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

[2] Threat Prevention/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. DPI SSL performance measured on HTTPS traffic with IPS enabled.

[3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.

[4] For rack mount, separate rack mount kit available.

[5] All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access point products.

SonicWall TZ Series ordering information

Product	SKU
SOHO 250 with 1-year TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC with 1-year TotalSecure Advanced Edition	02-SSC-1824
TZ300 with 1-year TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1703
TZ300P with 1-year TotalSecure Advanced Edition	02-SSC-0602
TZ350 with 1-year TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC with 1-year TotalSecure Advanced Edition	02-SSC-1851
TZ400 with 1-year TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1706
TZ500 with 1-year TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1709
TZ570 with 1-year TotalSecure Essential Edition	02-SSC-5651
TZ570W with 1-year TotalSecure Essential Edition	02-SSC-5649
TZ570P with 1-year TotalSecure Essential Edition	02-SSC-5653
TZ600 with 1-year TotalSecure Advanced Edition	01-SSC-1711
TZ600P with 1-year TotalSecure Advanced Edition	02-SSC-0600
TZ670 with 1-year TotalSecure Essential Edition	02-SSC-5640
High availability options (each unit must be the same model)	
TZ500 High Availability	01-SSC-0439
TZ570 High Availability	02-SSC-5694
TZ570P High Availability	02-SSC-5655
TZ600 High Availability	01-SSC-0220
TZ670 High Availability	02-SSC-5654

Services	SKU
For SonicWall SOHO 250 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	02-SSC-1726
Capture Advanced Threat Protection for SOHO 250 (1-year)	02-SSC-1732
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-1750
Content Filtering Service (1-year)	02-SSC-1744
Comprehensive Anti-Spam Service (1-year)	02-SSC-1823
24x7 Support (1-year)	02-SSC-1720
For SonicWall TZ300 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1430
Capture Advanced Threat Protection for TZ300 (1-year)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0602
Content Filtering Service (1-year)	01-SSC-0608
Comprehensive Anti-Spam Service (1-year)	01-SSC-0632
24x7 Support (1-year)	01-SSC-0620
For SonicWall TZ350 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	02-SSC-1773
Capture Advanced Threat Protection for TZ350 (1-year)	02-SSC-1779
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-1797
Content Filtering Service (1-year)	02-SSC-1791
Comprehensive Anti-Spam Service (1-year)	02-SSC-1809
24x7 Support (1-year)	02-SSC-1767

SonicWall TZ Series ordering information

For SonicWall TZ400 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1440
Capture Advanced Threat Protection for TZ400 (1-year)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0534
Content Filtering Service (1-year)	01-SSC-0540
Comprehensive Anti-Spam Service (1-year)	01-SSC-0561
24x7 Support (1-year)	01-SSC-0552
For SonicWall TZ500 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1450
Capture Advanced Threat Protection for TZ500 (1-year)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0458
Content Filtering Service (1-year)	01-SSC-0464
Comprehensive Anti-Spam Service (1-year)	01-SSC-0482
24x7 Support (1-year)	01-SSC-0476
For SonicWall TZ600 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1460
Capture Advanced Threat Protection for TZ600 (1-year)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0228
Content Filtering Service (1-year)	01-SSC-0234
Comprehensive Anti-Spam Service (1-year)	01-SSC-0252
24x7 Support (1-year)	01-SSC-0246
For SonicWall TZ670 Series	
Essential Protection Service Suite - Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1-year)	02-SSC-5053
Capture Advanced Threat Protection for TZ670 (1-year)	02-SSC-5035
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-5059
Content Filtering Service (1-year)	02-SSC-5047
Comprehensive Anti-Spam Service (1-year)	02-SSC-5041
24x7 Support (1-year)	02-SSC-5029
For SonicWall TZ570 Series (TZ570)	
Essential Protection Service Suite - Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1-year)	02-SSC-5137
Capture Advanced Threat Protection for TZ570 (1-year)	02-SSC-5083
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-5155
Content Filtering Service (1-year)	02-SSC-5119
Comprehensive Anti-Spam Service (1-year)	02-SSC-5101
24x7 Support (1-year)	02-SSC-5065
For SonicWall TZ570 Series (TZ570W)	
Essential Protection Service Suite - Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1-year)	02-SSC-5149
Capture Advanced Threat Protection for TZ570W (1-year)	02-SSC-5095
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-5167
Content Filtering Service (1-year)	02-SSC-5131
Comprehensive Anti-Spam Service (1-year)	02-SSC-5113
24x7 Support (1-year)	02-SSC-5077
For SonicWall TZ570 Series (TZ570P)	
Essential Protection Service Suite - Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1-year)	02-SSC-5143
Capture Advanced Threat Protection for TZ570P (1-year)	02-SSC-5089
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-5161
Content Filtering Service (1-year)	02-SSC-5125
Comprehensive Anti-Spam Service (1-year)	02-SSC-5107
24x7 Support (1-year)	02-SSC-5071

Accessories	SKU
TZ670/570 Series	
SonicWall TZ670/570 Series FRU Power Supply	02-SSC-3078
SonicWall TZ670/570 Series Rack Mount Kit	02-SSC-3112
SonicWall 32GB Storage Module for TZ670/570 Series	02-SSC-3114
SonicWall 64GB Storage Module for TZ670/570 Series	02-SSC-3115
SonicWall 128GB Storage Module for TZ670/570 Series	02-SSC-3116
SonicWall 256GB Storage Module for TZ670/570 Series	02-SSC-3117
SonicWall Micro USB Console Cable for TZ670/570 Series	02-SSC-5173
TZ600/500/400/350/300, SOHO 250 Series	
SonicWall TZ600 Rack Mount Kit	01-SSC-0225
SonicWall TZ600 Series FRU Power Supply	01-SSC-0280
SonicWall TZ500 Series Rack Mount Kit	01-SSC-0438
SonicWall TZ500 Series FRU Power Supply	01-SSC-0437
SonicWall TZ400 Series Rack Mount Kit	01-SSC-0525
SonicWall TZ350, TZ300 Series Rack Mount Kit	01-SSC-0742
SonicWall TZ400, TZ350, TZ300, SOHO 250, SOHO Series FRU Power Supply	01-SSC-0709
SonicWall TZ300 PoE FRU Power Supply	02-SSC-0613
SonicWall SFP/SFP+ Modules	
10GB-SR SFP+ Short Reach Fiber Module Multi-Mode No Cable	01-SSC-9785
10GB-LR SFP+ Long Reach Fiber Module Single-Mode No Cable	01-SSC-9786
10GB SFP+ Copper with 1M Twinax Cable	01-SSC-9787
10GB SFP+ Copper with 3M Twinax Cable	01-SSC-9788
1GB-SX SFP Short Haul Fiber Module Multi-Mode No Cable	01-SSC-9789
1GB-LX SFP Long Haul Fiber Module Single-Mode No Cable	01-SSC-9790
1GB-RJ45 SFP Copper Module No Cable	01-SSC-9791
SonicWall SFP+ 10GBASE-T Transceiver Copper RJ45 Module	02-SSC-1874

Regulatory model numbers

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/TZ300P	APL28-0B4/APL28-0B5/APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3
TZ670	APL62-0F7
TZ570/ TZ570W/ TZ570P	APL62-0F7/APL62-0F8/APL63-0F9

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

The Gartner Peer Insights Customers' Choice logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice distinctions are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here, and are not intended in any way to represent the views of Gartner or its affiliates.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

• NETWORK SECURITY ADMINISTRATOR •

SONICWALL NETWORK SECURITY ADMINISTRATOR (SNSA) TECHNICAL GUIDE

SonicWall Network Security Administrator Course Description

SonicWall offers an extensive technical training curriculum for network administrators, security experts and SonicWall partners who need to enhance their knowledge and maximize their investment in SonicWall products and security applications.

The SonicWall Network Security Administrator (SNSA) training curriculum is designed to teach students specific SonicWall network security technology. The course will provide students with the skills to successfully implement and configure SonicWall firewall appliances and security services. SonicWall recommends this course for networking professionals responsible for the daily operation of one or more security appliances.

Once you have completed the **SonicWall Network Security Administrator course**, you are eligible to take the **SonicWall Network Security Administrator exam**.

Course Overview:

- Two days of instructor-led classroom training — 80 percent hands-on labs and 20 percent lecture
- Six hours of online learning pre-requisite modules
- Based on the recently released SonicOS 6.5 firmware

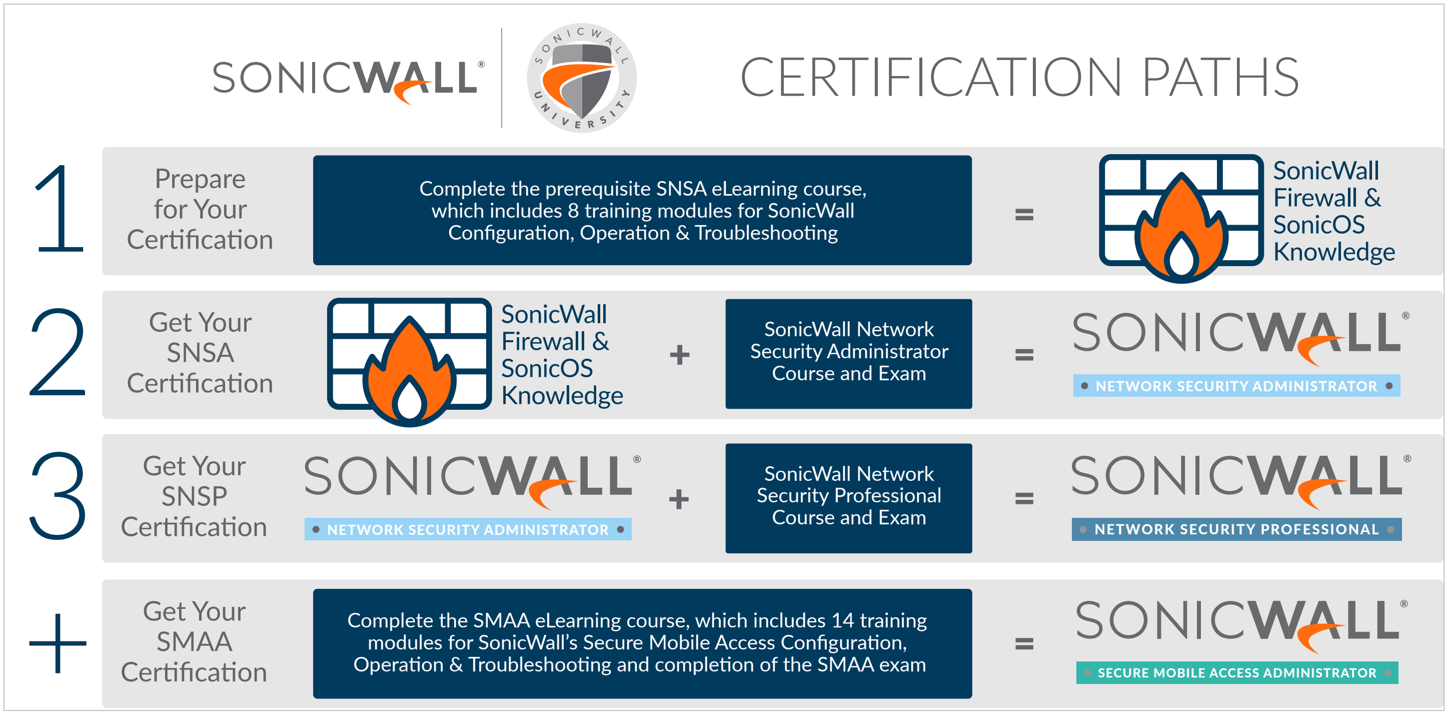
NEW! How can you register for the SonicWall Network Security Administrator Course (SNSA)?

To register for a SonicWall instructor-led training course:

1. Go to SonicWall University and log in to your account. Select the SecureFirst login if you are a SecureFirst partner. If you are not a SecureFirst partner, select the MySonicWall login. If you do not have a MySonicWall account, follow the instructions to create one.
2. Go to the **Events** link and click on **ATP Schedules** to find a class that meets your needs.
3. Click on the Course Name link, which will redirect you to the **Agenda and Details** page for the specific class.
4. If you would like to enroll in this class, click on the **Class Schedule** button.
5. This will take you to the Authorized Training Partner's website.
6. If a local class is not available, go to the **Events** link and click on **Authorized Training Partners** to find a local training partner.
7. The new SonicWall Network Security Administrator e-learning content is available through SonicWall University.
8. To access the content in SonicWall University, the Authorized Training Partner will provide you with activation keys for each course.

To access the SNSA certification exam:

1. Log in to your SonicWall University account.
2. The SNSA Exam page requires an activation key to enable the exam.
3. Enter the key provided by your instructor into the **Enter Course Key** field to activate the exam.
4. If you did not pass the exam, you can purchase an additional attempt test key from the exam page in SonicWall University
5. The **SNSA** exam is a proctored exam. If you take and pass the exam, you will receive a notification within 48 hours with the final status of your exam.
6. Because this is a proctored exam, you will be required to take the exam on a single-monitor computer. Additional resources are not allowed.



SONICWALL | SONICWALL UNIVERSITY CERTIFICATION PATHS

1 Prepare for Your Certification: Complete the prerequisite SNSA eLearning course, which includes 8 training modules for SonicWall Configuration, Operation & Troubleshooting = SonicWall Firewall & SonicOS Knowledge

2 Get Your SNSA Certification: SonicWall Firewall & SonicOS Knowledge + SonicWall Network Security Administrator Course and Exam = SONICWALL NETWORK SECURITY ADMINISTRATOR

3 Get Your SNSP Certification: SONICWALL NETWORK SECURITY ADMINISTRATOR + SonicWall Network Security Professional Course and Exam = SONICWALL NETWORK SECURITY PROFESSIONAL

+ Get Your SMAA Certification: Complete the SMAA eLearning course, which includes 14 training modules for SonicWall's Secure Mobile Access Configuration, Operation & Troubleshooting and completion of the SMAA exam = SONICWALL SECURE MOBILE ACCESS ADMINISTRATOR

For more information, visit training.SonicWall or email trainingsupport@sonicwall.com

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
SECRETARIA DE ADMINISTRAÇÃO, ORÇAMENTO E FINANÇAS
COORDENADORIA DE MATERIAL E PATRIMÔNIO

EXTRATO DE PREÇOS REGISTRADOS

Procedimento Licitatório nº 74/2020- Pregão Eletrônico - Sistema de Registro de Preços (SEI nº 0012283-09.2020.6.18.8000).
Ata nº 62/2020: CONTRATADA: NOVA SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E NETWORKING EIRELI (CNPJ: 10.685.932/0001-79): ITEM 1- Atualização da Solução de Firewall tipo concentrador, QUANT: 2 unidades, valor unitário: R$ 295.000,00 (duzentos e noventa e cinco mil reais); ITEM 2 -Atualização da Solução de Firewall tipo pequeno porte, QUANT: 51 unidades, valor unitário: R$ 5.700,00 (cinco mil e setecentos reais); ITEM 3 - Atualização da Solução de Firewall tipo pequeno porte, QUANT: 17 unidades, valor unitário: R$ 5.700,00 (cinco mil e setecentos reais); ITEM 4 - Licença SonicWall Global Management System para até 70 nós por 03 anos , QUANT: 1 unidade, valor unitário: R$ 175.000,00 (cento e setenta e cinco mil reais).

Procedimento Licitatório nº 79/2020- Pregão Eletrônico - Sistema de Registro de Preços (SEI nº 0020101-12.2020.6.18.8000).
Ata nº 63/2020: CONTRATADA: ALMEIDA REPRESENTAÇÕES E COMÉRCIO DE MATERIAL ESCOLAR E ALIMENTOS LTDA (CNPJ: 02.488.226/0001-09). ITEM 3 - ADOÇANTE LÍQUIDO, QUANT: 250 frascos, valor unitário: R$ 11,50 (onze reais e cinquenta centavos); ITEM 5 - COPO DESCARTÁVEL PARA ÁGUA , QUANT: 6.000 centos, valor unitário:R$ 4,05 (quatro reais e cinco centavos); ITEM 6 - COPO DESCARTÁVEL PARA CAFÉ , QUANT: 1.000 centos, valor unitário: R$ 1,95 (um real e noventa e cinco centavos).

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

1) Processo Administrativo Eletrônico/Protocolo nº 9931/2020; 2) Espécie: Inexigibilidade de Licitação; 3) Objeto: Contratação de assinatura anual de WEB para gestão tributária; 4) Favorecido: OPEN TREINAMENTOS EMPRESARIAIS E EDITORA LTDA. - EPP, CNPJ: 09.094.300/0001-51; 5) Fundamento Legal: Art. 25, caput, da Lei n.º 8.666/1993; 6) Valor: R$ 7.188,00; 7) Autorização: em 11/11/2020, por Yvette Bezerra Guerreira Maia, Diretora-Geral do TRE/RN (fl. 30). RATIFICAÇÃO: em 27/11/2020, pelo Desembargador Gilson Barbosa, Presidente do TRE/RN (fl. 37).

AVISO DE SUSPENSÃO
PREGÃO Nº 90/2020

Comunicamos a suspensão da licitação supracitada, publicada no D.O.U em 20/11/2020 . Objeto: Pregão Eletrônico - Contratação de serviços de cobertura securitária (seguro contra acidentes pessoais) para estagiários e servidores voluntários do Tribunal Regional Eleitoral do Rio Grande do Norte.

MANOEL NAZARENO FERNANDES FILHO
Pregoeiro

(SIDEC - 30/11/2020) 070008-00001-2020NE111111

TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 79/2020 - UASG 70017

Nº Processo: 202000000323436. Objeto: Aquisição de material de elétrica e lógica. Total de Itens Licitados: 31. Edital: 01/12/2020 das 08h00 às 17h59. Endereço: Av. Presidente Wilson, 194 - 1º Andar, Centro - Rio de Janeiro/RJ ou https://www.gov.br/compras/edital/70017-5-00079-2020. Entrega das Propostas: a partir de 01/12/2020 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 14/12/2020 às 11h00 no site www.gov.br/compras.

REJANE LOPES DE OLIVEIRA
Pregoeira

(SIASGnet - 30/11/2020) 70017-00001-2020NE000001

DIRETORIA-GERAL
ASSESSORIA JURÍDICA

EXTRATO DE TERMO ADITIVO

PROCESSO SEI Nº 2020.0.000045958-3. Quarto Termo Aditivo ao Contrato nº 81/2016, de prestação de serviços de suporte técnico mensal de gerenciamento de som, para aplicação nas sessões plenárias do TRE/RJ. CONTRATADA: KENTA INFORMÁTICA S/A, CNPJ: 01.276.330/0001-77. FUND. LEGAL: Lei nº 8.666/93, com redação da Lei nº 8.883/94. OBJETO: Prorrogação contratual para o período de 05/12/20 a 04/12/21. VALOR PARA 2020: R$5.482,13, conforme nota de empenho 1709, de 19/11/20. VALOR PARA 2021: R$ 70.424,36. ELEMENTO: 3390.40. PROGRAMA: Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral.

AVISOS DE HOMOLOGAÇÃO
PREGÃO ELETRÔNICO Nº 71/2020

Processo SEI nº 2020.0.000031317-1.

A Sra. Diretora-Geral torna pública a homologação da licitação mediante Pregão Eletrônico nº 71/2020, destinado à aquisição de material de marcenaria, tendo como vencedora a empresa V R M REPRESENTACAO COMERCIAL - EIRELI, para os itens 1, 2 e lote 2, nos valores de R$2.475,00, R$ 3.840,00 e R$ 4.005,10, respectivamente; e a empresa JLA COMERCIO DE MADEIRAS E PALLETS EIRELI, para o lote 1, no valor de R$4.508,00.

PREGÃO ELETRÔNICO Nº 72/2020

Processo SEI nº 2020.0.000009984-6.

A Sra. Diretora-Geral torna pública a homologação da licitação mediante Pregão Eletrônico nº 72/2020, destinado à contratação de empresa para prestação de serviço de higienização de acervo bibliográfico, tendo como vencedora dos item único, a empresa TEMPO REAL PRODUÇÃO E COMUNICAÇÃO LTDA, no valor de R$10.448,38.

ADRIANA FREITAS BRANDÃO CORREIA
Diretora-Geral

AVISO DE PENALIDADE

O Tribunal Regional Eleitoral do Rio de Janeiro resolve aplicar a CARTONAGEM PERIMETRAL INDÚSTRIA E COMÉRCIO EIRELI, CNPJ nº 09.161.208/0001-67, a penalidade de impedimento de contratar e licitar com a União, pelo prazo de 3 (três) meses, a contar desta publicação.

A penalidade é resultado das irregularidades apuradas no processo administrativo nº 2020.0.000049914-3.

ADRIANA FREITAS BRANDÃO CORREIA
Diretora-Geral

TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA

EXTRATO DE TERMO ADITIVO

Espécie: 4º T.A. ao Contrato TRE-RO 22/2018, de 30/11/20. Contratada: EACE ENGENHEIROS ASSOCIADOS CONSULTORES EM ENGENHARIA LTDA, CNPJ 15.110.739/0001-23. Objeto: I) Prorrogar o prazo de vigência por mais 180 dias corridos, a contar de 05/12/2020, sem ônus para o Contratante; e II) Prorrogar o prazo de execução por mais 180 dias corridos, a contar de 21/09/2020, sem ônus para o Contratante. Fundamentação: Art. 57, I, § 1º, V, da Lei nº 8.666/93, e na CLÁUSULA 4ª, Subcláusula 3ª, do Contrato. Autorização DECISÃO 126/GABDG, de 25/11/20. Signatários: Desembargador MARCOS ALAOR DINIZ GRANGEIA, Presidente do TRE-RO, e, pela Contratada, LUIS MIGUEL GOMES DE OLIVEIRA. Processo 0001552-45.2017.6.22.8000.

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

EXTRATO DE TERMO ADITIVO

Contratada: Litoral Engenharia e Construções EIRELI. CNPJ da Contratada: 026.051.611/0001-52. Objeto: Termo Aditivo n. 155/2020, referente ao Contrato n. 023/2020, cujo objeto é a manutenção da fachada do Edifício Sede do TRESC (altera a Cláusula Nona - Do acompanhamento e da fiscalização da execução do contrato). Fundamento legal: Lei n. 8.666/1993. Data da assinatura: 26/11/2020. Pregão nº 8/2020.

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO

RESULTADO DE JULGAMENTO
PREGÃO Nº 93/2020

Objeto: fornecimento de estabilizadores de voltagem O pregoeiro do TRE torna público o resultado da licitação em epígrafe. Sagrou-se vencedora a licitante ITEC INFORMÁTICA E TECNOLOGIA LTDA. E TECNOLOGIA LTDA. EPP para o item único. São Paulo, 27 de novembro de 2020 Ricardo Mendonça Falcão Pregoeiro do TRE-SP

ANA CAROLINA DA SILVA ROCHA
Equipe de apoio

(SIDEC - 30/11/2020) 070018-00001-2020NE000061

RESULTADO DE JULGAMENTO
PREGÃO Nº 99/2020

Objeto: registro de preço para aquisição de cartuchos de toner para impressora laser Samsung modelos SL-M4020ND e MLT-3710 O pregoeiro do TRE torna público o resultado da licitação em epígrafe. Sagraram-se vencedoras as licitantes REPREMIG REPRESENTAÇÃO E COMÉRCIO DE MINAS GERAIS para o item 01 e A H DA S MORAES-EPP para o item 02. São Paulo, 26 de novembro de 2020 Ricardo Mendonça Falcão Pregoeiro do TRE-SP

ANA CAROLINA DA SILVA ROCHA
Equipe de apoio

(SIDEC - 30/11/2020) 070018-00001-2020NE000061

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 106/2020 - UASG 70018

Nº Processo: 080803-33.2019. Objeto: Aquisição de nobreaks.. Total de Itens Licitados: 1. Edital: 01/12/2020 das 08h00 às 12h00 e das 13h00 às 17h00. Endereço: Rua Francisca Miquelina, 123, Bela Vista - São Paulo/SP ou https://www.gov.br/compras/edital/70018-5-00106-2020. Entrega das Propostas: a partir de 01/12/2020 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 14/12/2020 às 13h00 no site www.gov.br/compras. Informações Gerais: .

WALDIR SEBASTIAO DE NUEVO CAMPOS JUNIOR
Presidente do Tribunal Regional Eleitoral de São Paulo

(SIASGnet - 25/11/2020) 70018-00001-2020NE000169

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS
SECRETARIA-GERAL DA CORREGEDORIA
VARAS COM JURISDIÇÃO EM TODO O TERRITÓRIO DO DISTRITO FEDERAL
VARA DA INFÂNCIA E DA JUVENTUDE DO DISTRITO FEDERAL

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 15/2020 - UASG 100009

Nº Processo: 15/2020. Objeto: O objeto da presente licitação é a aquisição de automóveis novos, 0 km, para transporte institucional da Vara da Infância e da Juventude do Distrito Federal - VIJDF, nos termos do Edital e dos anexos.. Total de Itens Licitados: 2. Edital: 01/12/2020 das 08h00 às 11h59 e das 12h00 às 17h59. Endereço: Sgan Q. 909 - Bl."c" - Setor de Contabilidade, Asa Norte - BRASÍLIA/DF ou https://www.gov.br/compras/edital/100009-5-00015-2020. Entrega das Propostas: a partir de 01/12/2020 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 11/12/2020 às 09h00 no site www.gov.br/compras. Informações Gerais: .

FRANCISCO DEMONTIE CORREIA CUNHA
Pregoeiro

(SIASGnet - 30/11/2020) 100009-00001-2020NE000002

TRIBUNAL REGIONAL DO TRABALHO DA 1ª REGIÃO

EXTRATO DE TERMO ADITIVO

Contratada: IBS ADMINISTRAÇÃO DE SERVIÇOS E LOCAÇÃO DE MÃO DE OBRA EIRELI; a) Espécie: 5º TA ao contrato de empreitada por preço global para prestação de serviço de empreitada por preço global para prestação de serviço de recepção nas dependências do TRT/RJ (Proc. 5429-44.2016.5.01.1000); b) fund. legal: art. 65, inciso II, alínea "d" c/c art. 78, inciso XIV, Lei nº 8.666/93; c) objeto: convalidação da revisão contratual decorrente da ampliação do período de suspensão da execução do contrato até 02/11/2020, por necessidade de se manter as medidas de enfrentamento da propagação do novo coronavírus (COVID-19) tratadas no 4º Termo Aditivo; d) valor: R$ 21.894,25; e) vigência: os efeitos serão produzidos nos períodos indicados na cláusula segunda, passando o término do período de suspensão da execução contratual para 02/11/2020, encerrando-se o prazo de vigência em 17/09/2022; f) assinam em 26/11/2020 o Sr. Luis Felipe Carrapatoso Peralta da Silva, pelo Contratante, e o Sr. Isaac Bastos Sias, pela Contratada.