

# SonicWall Product Lines

## Table of Contents

SonicWall Network Security services platform (NSsp) 12000 series	2
SonicWall Network Security appliance (NSa) series	3
SonicWall TZ series	5
SonicWall Capture Client	7
SonicWall WAN Acceleration (WXA) series	8
SonicWall Network Security virtual (NSv) series	9
SonicWall Web Application Firewall (WAF) series	11
SonicWall SonicWave series	12
SonicWall SonicWave series POE Injector	13
SonicWall SonicPoint series	14
SonicWall SonicPoint series PoE Injector	15
SonicWall Secure Mobile Access (SMA)	16
SonicWall Email Security	19
SonicWall Hosted Email Security	21
SonicWall Cloud App Security	22
SonicWall Capture Security Center	24
SonicWall Global Management System (GMS)	26
SonicWall Analyzer	27

### 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](http://www.sonicwall.com/PES).

## NSsp series system specifications

Firewall General	NSsp 12400	NSsp 12800
Operating system	SonicOS 6.5.1.8	
Security processing cores	128	256
Interfaces	4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE Management, 1 Console	4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE Management, 1 Console
Built-in storage	2 x 480 GB	
Management	CLI, SSH, Web UI, GMS, REST APIs	
SSO users	110,000	110,000
Maximum access points supported	128	128
Logging	Analyzer, Local Log, Syslog, IPFIX, NetFlow	
Firewall/VPN Performance	NSsp 12400	NSsp 12800
Firewall inspection throughput <sup>1</sup>	58.4 Gbps	120.3 Gbps
Threat Prevention throughput <sup>2</sup>	33.5 Gbps	67.5 Gbps
Application inspection throughput <sup>2</sup>	45.5 Gbps	91.0 Gbps
IPS throughput <sup>2</sup>	36.8 Gbps	73.0 Gbps
Anti-malware inspection throughput <sup>2</sup>	33.5 Gbps	67.5 Gbps
IMIX throughput	14.8 Gbps	29.0 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL) <sup>2</sup>	8.1 Gbps	17.6 Gbps
VPN throughput <sup>3</sup>	24.5 Gbps	47.0 Gbps
Connections per second	430,000/sec	860,000/sec
Maximum connections (SPI)	40,000,000	80,000,000
Maximum connections (DPI)	16,000,000	32,000,000
Maximum connections (DPI SSL)	1,300,000	2,600,000
VPN	NSsp 12400	NSsp 12800
Site-to-site VPN tunnels	25,000	25,000
IPSec VPN clients (max)	2,000 (10,000)	2,000 (10,000)
SSL VPN NetExtender clients (max)	2 (3,000)	2 (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	NSsp 12400	NSsp 12800
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	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, 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	Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering	
Hardware	NSsp 12400	NSsp 12800
Power supply	Dual, Redundant, 1,200W	
Fans	Dual, Removable	
Input power	100-240 VAC, 50-60 Hz	
Maximum power consumption (W)	679	965
MTBF @25°C in hours	113,114	91,118
MTBF @25°C in years	12.9	10.4
Form factor	4U Rack Mountable	
Dimensions	24.0 x 16.9 x 7.1 in (61 x 43 x 18 cm)	
Weight	59.3 lb (26.9 kg)	67.2 lb (30.5 kg)
WEEE weight	67.7 lb (30.7 kg)	75.6 lb (34.3 kg)
Shipping weight	83.1 lb (37.7 kg)	91.1 lb (41.3 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	10-95% non-condensing	

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

<sup>2</sup> Full DPI/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.

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

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

## NSa series system specifications

Firewall general	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Operating system	SonicOS 6.5.3			
Security processing cores	4	4	10	10
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	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 <sup>1</sup>	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
Threat Prevention throughput <sup>2</sup>	1.25 Gbps	1.75 Gbps	2.5 Gbps	3.4 Gbps
Application inspection throughput <sup>2</sup>	1.4 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS throughput <sup>2</sup>	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
Anti-malware inspection throughput <sup>2</sup>	1.3 Gbps	1.5 Gbps	2.45 Gbps	2.8 Gbps
IMIX throughput	700 Mbps	900 Mbps	1.3 Gbps	1.45 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL) <sup>2</sup>	250 Mbps	320 Mbps	675 Mbps	800 Mbps
VPN throughput <sup>3</sup>	1.3 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
Maximum connections (DPI SSL)	18,000	24,000	30,000	37,000
Default connections (DPI/DPI SSL) <sup>4</sup>	500,000/12,000	625,000/15,000	750,000/18,000	1,000,000/19,000
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 <sup>5</sup>	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, 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			

## NSa series system specifications cont'

Firewall general	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Operating system	SonicOS 6.5.3			
Security processing cores	24	24	32	32
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	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 <sup>1</sup>	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
Threat Prevention throughput <sup>2</sup>	5.5 Gbps	6.5 Gbps	9.0 Gbps	9.4 Gbps
Application inspection throughput <sup>2</sup>	6.0 Gbps	7.8 Gbps	10.8 Gbps	11.5 Gbps
IPS throughput <sup>2</sup>	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware inspection throughput <sup>2</sup>	5.4 Gbps	6.5 Gbps	8.0 Gbps	8.5 Gbps
IMIX throughput	2.65 Gbps	2.65 Gbps	4.1 Gbps	4.1 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL) <sup>3</sup>	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
VPN throughput <sup>3</sup>	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
Maximum connections (DPI SSL)	100,000	100,000	200,000	300,000
Default connections (DPI/DPI SSL) <sup>4</sup>	1,500,000/45,000	2,000,000/48,000	3,000,000/134,000	4,000,000/210,000
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 <sup>5</sup>	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			

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

<sup>2</sup> 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.

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

<sup>4</sup> For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 3,000 except for NSa 9250 and above.

<sup>5</sup> 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.

## SonicWall TZ series

Hardware overview	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600 series
Operating system	SonicOS				
Security processing cores	2	2	4	4	4
Interfaces	5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Power over Ethernet (PoE) support	-	TZ300P - 2 ports (2 PoE or 1 PoE+)	-	-	TZ600P - 4 ports (4 PoE or 4 PoE+)
Expansion	USB	USB	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs				
Single Sign-On (SSO) Users	250	500	500	500	500
VLAN interfaces	25	25	50	50	50
Access points supported (maximum)	2	8	16	16	24
Firewall/VPN performance	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600 series
Firewall inspection throughput <sup>1</sup>	300 Mbps	750 Mbps	1.3 Gbps	1.4 Gbps	1.5 Gbps
Threat Prevention throughput <sup>2</sup>	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Application inspection throughput <sup>2</sup>	-	300 Mbps	900 Mbps	1.0 Gbps	1.1 Gbps
IPS throughput <sup>2</sup>	100 Mbps	300 Mbps	900 Mbps	1.0 Gbps	1.1 Gbps
Anti-malware inspection throughput <sup>2</sup>	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX throughput	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL) <sup>2</sup>	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN throughput <sup>3</sup>	100 Mbps	300 Mbps	900 Mbps	1.0 Gbps	1.1 Gbps
Connections per second	1,800	5,000	6,000	8,000	12,000
Maximum connections (SPI)	10,000	50,000	100,000	125,000	150,000
Maximum connections (DPI)	10,000	50,000	90,000	100,000	125,000
Maximum connections (DPI SSL)	100	500	500	750	750
VPN	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600 series
Site-to-site VPN tunnels	10	10	20	25	50
IPSec VPN clients (maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual assist bundled (maximum)	-	1 (30-day trial)	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				
Certificate support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to- SonicWall VPN, SCEP				
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	TZ300 series	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	No	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes	Yes

## SonicWall TZ series con't

Networking	SOHO series	TZ300 series	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 <sup>4</sup>	BGP <sup>4</sup> , 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	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, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus				
Certifications pending	Common Criteria NDPP (Firewall and IPS)				
Common Access Card (CAC)	Supported				
High availability	No	Active/standby	Active/standby	Active/standby with stateful synchronization	Active/standby with stateful synchronization
Hardware	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Form factor	Desktop				
Power supply	24W external	24W external 65W external (TZ300P only)	24W external	36W external	60W external 180W external (TZ600P only)
Maximum power consumption (W)	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100 to 240 VAC, 50-60 Hz, 1 A				
Total heat dissipation	21.8 / 38.7 BTU	23.5 / 40.9 BTU	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.6x14.1x19cm	3.5x13.4x19cm	3.5x13.4x19cm	3.5x15x22.5cm	3.5x18x28cm
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	0.92 kg / 2.03 lbs 1.05 kg / 2.31 lbs	1.47 kg / 3.24 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	1.34 kg / 2.95 lbs 1.48 kg / 3.26 lbs	1.89 kg / 4.16 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	1.93 kg / 4.25 lbs 2.07 kg / 4.56 lbs	2.48 kg / 5.47 lbs
MTBF (in years)	58.9/56.1 (wireless)	56.1	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	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600 series
Regulatory model (wired)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
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	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	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	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	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
Regulatory model (wireless)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, 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 (R&TTE, EMC, LVD, 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 (R&TTE, EMC, LVD, 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 (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	-

## SonicWall TZ series con't

Integrated Wireless	SOHO series	TZ300, TZ400, TZ500 series	TZ600 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 <sup>5</sup>	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	-
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	Based on the regulatory domain specified by the system administrator	-
Transmit power control	Supported	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.

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

<sup>2</sup> 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.

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

<sup>4</sup> BGP is available only on SonicWall TZ400, TZ500 and TZ600.

<sup>5</sup> All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access points products (SonicPoints)

## SonicWall Capture Client

Antivirus feature	Capture Client Basic	Capture Client Advanced
Firewall enforcement	Yes	Yes
DPI-SSL certificate management	Yes	Yes
Continuous behavioral monitoring	Yes	Yes
Highly accurate determinations achieved through machine learning	Yes	Yes
Threat Visualization	No	Yes
Unique rollback capabilities	No	Yes
Capture Advanced Threat Protection (ATP) integration	No	Yes
Capture ATP verdict one-click look up	No	Yes
<b>System requirements</b>		
Windows operating system	Windows 7 and upwards	Windows 7 and upwards
Windows Servers	Windows Server 12 and Upwards	Windows Server 12 and Upwards
Mac OS/OSX	10.10 and upwards	10.10 and upwards
Minimum CPU processor	1 GHz dual-core CPU or better	1 GHz dual-core CPU or better
Minimum memory	1 GB RAM or higher if required by OS	1 GB RAM or higher if required by OS
Recommended memory	2 GB RAM	2 GB RAM
Minimum storage available	2 GB	2 GB

## SonicWall WAN Acceleration (WXA) series

	WXA 500 Software	WXA 5000 Virtual Appliance	WXA 6000 Software
Platform	Software <sup>5</sup>	Virtual appliance	Software <sup>5</sup>
Maximum users <sup>1</sup>	20	360	2,000
Maximum connections	100	1,800 <sup>3</sup>	10,000
Maximum web caching connections	100	1,800 <sup>3</sup>	10,000
Included/maximum concurrent WXA client licenses <sup>4</sup>	2/20	2/125	2/125
Byte caching		Yes	
TCP/file compression		Yes	
Management		Requires SonicOS 5.8.1 or later	
Clustering <sup>6</sup>	—	Yes	Yes
CIFS/SMB acceleration	Yes <sup>2</sup>		
Signed SMB support		Yes	
WFS/TCP visualization		Yes	
SNMP		Yes	
Syslog		Yes	
Operating system		Hardened SonicWall Linux OS	

	WXA 500 Software only	WXA 6000 Software only
Dell hardware	Dell Inspiron 3847, Dell XPS 8700	Dell PowerEdge R320 Server

WXA 5000 Virtual Appliance only		
Hypervisor	VMware ESX or ESXi version 5.0 or higher	Microsoft Windows Server 2012 or 2012 R2 with the Hyper-V role enabled
Virtual appliance requirements	<a href="#">SonicWall WXA release notes</a>	
VMware Hardware Compatibility Guide	<a href="http://vmware.com/resources/compatibility/search.php">vmware.com/resources/compatibility/search.php</a>	

<sup>1</sup>Maximum users may vary depending on the number of connections being generated per user.

<sup>2</sup>CIFS/SMB acceleration is available only when the WXA software image is installed on the supplied Dell hardware.

<sup>3</sup>The max number of connections is dependent on the hardware specifications and may vary depending on the hardware configuration. The specifications provided are the minimum requirements to run the WXA Virtual Appliance.

<sup>4</sup>NetExtender is required in order to use the WXA client software. Please refer to the WXA release notes for supported operating systems.

<sup>5</sup>The WXA 500 and 6000 software can be downloaded from [www.mysonicwall.com](http://www.mysonicwall.com) and requires specific Dell hardware in order to operate.

<sup>6</sup>Requires SonicOS 6.2 or higher.



## SonicWall Network Security virtual (NSv) series

Firewall General	NSv 10	NSv 25	NSv 50	NSv 100
Operating system	SonicOS <sup>1</sup>			
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5, Microsoft Hyper-V			
License Types	Perpetual, Non-perpetual	Perpetual	Perpetual, Non-perpetual	Perpetual
Max Supported vCPUs	2	2	2	2
Interface Count (ESXi)	8	8	8	8
Max Mgmt/DataPlane Cores	1/1	1/1	1/1	1/1
Min Memory <sup>2</sup>	4 GB	4 GB	4 GB	4 GB
Max Memory <sup>3</sup>	6 GB	6 GB	6 GB	6 GB
Supported IP/Nodes	10	25	50	100
Minimum Storage	60 GB			
SSO users	25	50	100	100
Logging	Analyzer, Local Log, Syslog			
High availability	Active/Passive			
Firewall/VPN Performance <sup>5</sup>	NSv 10	NSv 25	NSv 50	NSv 100
Firewall Inspection Throughput	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
Full DPI Throughput (GAV/GAS/IPS)	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Application Inspection Throughput	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
IPS Throughput	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
Anti-Malware Inspection Throughput	450 Mbps	550 Mbps	650 Mbps	750 Mbps
IMIX Throughput	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
TLS/SSL DPI Throughput	650 Mbps	750 Mbps	850 Mbps	950 Mbps
VPN Throughput	500 Mbps	550 Mbps	600 Mbps	650 Mbps
Connections per second	1,800	5,000	8,000	10,000
Maximum connections (SPI)	2,500	6,250	12,500	25,000
Maximum connections (DPI)	2,500	6,250	12,500	25,000
TLS/SSL DPI Connections	500	1,000	2,000	4,000
VPN	NSv 10	NSv 25	NSv 50	NSv 100
Site-to-Site VPN Tunnels	10	10	25	50
IPSec VPN clients	10	10	25	25
SSL VPN NetExtender Clients (Maximum)	2(10)	2(25)	2(25)	2(25)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			
Networking	NSv 10	NSv 25	NSv 50	NSv 100
IP address assignment	Static, DHCP, internal DHCP server, DHCP relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT			
VLAN Interfaces	25	25	50	50
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix			
VoIP	SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

## SonicWall Network Security virtual (NSv) series con't

Firewall General	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Operating system	SonicOS <sup>1</sup>				
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5, Microsoft Hyper-V				
License Types	Perpetual, Non-perpetual	Perpetual	Perpetual, Non-perpetual	Perpetual, Non-perpetual	Perpetual
Supported Public Cloud Platforms (Instance Type)	AWS (c5.large), Azure (Std D2 v2)	N/A	AWS (c5.xlarge), Azure (Std D3 v2)	AWS (c5.2xlarge), Azure (Std D4 v2)	AWS (c5.4xlarge), Azure (Std D5 v2)
Max Supported vCPUs	2	3	4	8	16
Interface Count (ESXi/AWS/Azure)	8/3/2	8/-/-	8/4/4	8/4/8	8/8/8
Max Mgmt/DataPlane Cores	1/1	1/2	1/3	1/7	1/15
Min Memory <sup>2</sup>	4 GB	6 GB	8 GB	10 GB	12 GB
Max Memory <sup>3</sup>	6 GB	8 GB	10 GB	14 GB	18 GB
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Minimum Storage	60 GB				
SSO users	500	5,000	10,000	15,000	20,000
Logging	Analyzer, Local Log, Syslog				
High availability	Active/Passive <sup>4</sup>				
Firewall/VPN Performance <sup>5</sup>	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Firewall Inspection Throughput	4.1 Gbps	5.9 Gbps	7.8 Gbps	13.9 Gbps	17.2 Gbps
Full DPI Throughput (GAV/GAS/IPS)	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.4 Gbps
Application Inspection Throughput	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.4 Gbps
IPS Throughput	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.7 Gbps
Anti-Malware Inspection Throughput	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.6 Gbps
IMIX Throughput	1.5 Gbps	2.3 Gbps	2.8 Gbps	4.2 Gbps	5.3 Gbps
TLS/SSL DPI Throughput	1.1 Gbps	1.2 Gbps	1.8 Gbps	3.4 Gbps	5.1 Gbps
VPN Throughput	750 Mbps	1.4 Gbps	1.9 Gbps	4.2 Gbps	8.4 Gbps
Connections per second	13,760	24,360	37,270	75,640	125,000
Maximum connections (SPI)	225,000	1M	1.5M	3M	4M
Maximum connections (DPI)	125,000	500,000	1.5M	2M	2.5M
TLS/SSL DPI Connections	8,000	12,000	20,000	30,000	50,000
VPN	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Site-to-Site VPN Tunnels	75	100	6000	10,000	25,000
IPSec VPN clients (Maximum)	50(1000)	50(1000)	2000(4000)	2000(6000)	2000(10,000)
SSL VPN NetExtender Clients (Maximum)	2(100)	2(100)	2(100)	2(100)	2(100)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v				
Route-based VPN	RIP, OSPF, BGP				
Networking	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
IP address assignment	Static, DHCP, internal DHCP server, DHCP relay				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT				
VLAN Interfaces	50	256	500	512	512
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p				
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix				
VoIP	SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

<sup>1</sup>Currently supporting SonicOS 6.5.0. SonicOS 6.5.2 support available end of calendar year.

<sup>2</sup>Memory with Jumbo frame disabled.

<sup>3</sup>Memory with Jumbo frame enabled. Additional memory is required for Jumbo frame enabled.

<sup>4</sup>High availability available on VMware ESXi platform and Microsoft Hyper-V.

<sup>5</sup>Published performance numbers are up to the specification and the actual performance may vary depending on underlying hardware, network conditions; firewall configuration and activated services. Performance and capacities may also vary based on underlying virtualization infrastructure, and we recommend additional testing within your environment to ensure your performance and capacity requirements are met. Performance metrics were observed using Intel Xeon W Processor (W-2195 2.3GHz, 4.3GHz Turbo, 24.75M Cache) running SonicOSv 6.5.0.2 with VMware vSphere 6.5.

Testing Methodologies:

Maximum performance based on RFC 2544 (for firewall).

Full DPI/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.

VPN throughput measured using UDP traffic at 1418 byte packet size adhering to RFC 2544. All specifications and features are subject to change.

## SonicWall Web Application Firewall (WAF) series

MODEL	WAF 200	WAF 400	WAF 800	WAF 1600
Supported Platform	VMware ESXi v6.5 Microsoft Hyper-V Manager 6.2 / 6.3 Amazon AWS Microsoft Azure			
WAF Tier	Tier 1	Tier 2	Tier 3	Tier 4
SSL Transactions/sec	6,000	12,000	24,000	48,000
SSL Throughput	500 Mbps	1 Gbps	2 Gbps	4 Gbps
Recommended vCPUs*	2	4	8	16
Recommended Memory	4 GB	8 GB	16 GB	32 GB
Recommended Storage	8 GB	8 GB	8 GB	8 GB
Recommended AWS Instance	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge
Recommended Azure Instance	Standard_F2s_v2	Standard_F4s_v2	Standard_F8s_v2	Standard_F16s_v2

\*This is based on typical enterprise-grade server systems. For more information, please see the Deployment Guides.

## SonicWall SonicWave series

Hardware Specifications	SonicWave 432e	SonicWave 432i	SonicWave 432o
Location	Indoor	Indoor	Outdoor
Dimensions	8.5 (D) x 2.0 (H) in 21.6 (D) x 5.1 (H) cm	8.5 (D) x 2.0 (H) in 21.6 (D) x 5.1 (H) cm	9.5 (W) x 9.3 (D) x 2.4 (H) in 24.1 (W) x 23.6 (D) x 6.1 (H) cm
Weight	1.1 kg / 2.5 lbs	1.0 kg / 2.2 lbs	2.2 kg / 4.9 lbs
WEEE weight	1.4 kg / 3.1 lbs	1.2 kg / 2.6 lbs	4.1 kg / 9.1 lbs
Shipping weight	1.7 kg / 3.8 lbs	1.5 kg / 3.3 lbs	4.7 kg / 10.4 lbs
PoE injector		802.3at	
Maximum power consumption (W)	18.8 W	18.8 W	21.2 W
Status indicators	Six (6) LED (WLAN/Link) (LAN/Link) Power, Test		
Antennas	4+4 (SMA 2.4 GHz + TNC 5 GHz)	8 fully internal	8 N-type dipole
Wired network ports	(1) 10/100/1000 auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE); (1) 100/1000/2.5 GbE auto-sensing RJ-45 for Ethernet; (1) RJ-45 console; (1) USB 2.0 (except 432o)		
Accessories included	Wall/ceiling mount kit		
Virtual access points	Up to 8 per access point		
Chassis	UL 1024 plenum rated		
Standards and compliance	SonicWave 432e	SonicWave 432i	SonicWave 432o
IEEE Standard	802.11a/b/g/n/ac Wave 2		
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA, TKIP, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w		
Regulatory	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE		
MIMO	MU-MIMO 4x4 (4 streams)		
Max/Recommended connected clients per radio	128/30	128/30	128/30
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union		
Environmental	SonicWave 432e	SonicWave 432i	SonicWave 432o
Temperature range	32 to 104°F, 0 to 40°C		-40 to 140°F, -40 to 60°C
Humidity	10 - 95%, non-condensing		
Radio specifications	SonicWave 432e/432i/432o		
Radios	Dual: 4x4 11n + 4x4 11ac MU-MIMO; Dedicated third scanning radio; Bluetooth Low Energy radio		
Frequency bands	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		
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 36-48/52-64 802.11ac: 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, 1040, 1170, 1300, 1560, 1733.4 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)		
Security	SonicWave 432e/432i/432o		
Data encryption	WPA2, IPsec*, 802.11i, WPA, 64/128/152-bit WEP, TKIP, AES, SSL VPN**		
Authentication	SonicWave 432e/432i/432o		
Authentication	RADIUS, Active Directory, single sign-on (SSO)		

\*When used with a SonicWall firewall

\*\*When used with SonicWall Secure Mobile Access Series appliance

## SonicWave Series PoE Injector

Hardware Specifications		SonicWave 432e/432i/432o
Number of ports	2: (1) Data In; (1) data and power out	
Dimensions	1.69 (H) x 3.46 (W) x 6.54 (L) in; (43 (H) x 87.9 (W) x 166 (L) mm	
Weight	0.91 lbs/(0.41 kg)	
WEEE weight	1.2 lbs/(0.54 kg)	
Shipping weight	1.28 lbs/(0.58 kg)	
Connectors	Shielded RJ-45, EIA 568A and 568B	
Status Indicators	LED indicator: Power On (yellow); Power supplied over Ethernet (green); Over current/short circuit (blinking green)	
Data rates	10/100/1000 Mbps/2.5 GbE	
Power over LAN output		SonicWave 432e/432i/432o
Pin assignment and polarity	4/5 (+), 7/8 (-)	
Output power voltage	-55 VDC	
Maximum output power	30 W	
Input power requirements		SonicWave 432e/432i/432o
AC input voltage	100 to 240 VAC	
AC frequency	50 to 60 Hz	
AC input current	1.5A at 100-240 VAC	
Standards and compliance		SonicWave 432e/432i/432o
Regulatory compliance	CE, EN 55022 Class B (Emissions), FCC Part 15 Class B, EN 55024 (Immunity), VCCI	
Safety	UL/CUL 60950-1, GS Mark per IEC 60950-1	
Environmental	RoHS, WEEE	
Environmental requirements		SonicWave 432e/432i/432o
Operating ambient temperature	14 to 113 °F, -10 to 40 °C	
Operating humidity	Maximum 90%, non-condensing	
Storage temperature	-4 to 158 °F, -20 to 70 °C	
Storage humidity	Maximum 95%, non-condensing	

## SonicWall SonicPoint Series

Hardware Specifications	SonicPoint ACe	SonicPoint ACi	SonicPoint N2
Location	Indoor	Indoor	Indoor
Dimensions	6.9 (D) x 1.5 (H) in 17.5 (D) x 3.8 (H) cm	6.9 (D) x 1.5 (H) in 17.5 (D) x 3.8 (H) cm	6.9 (D) x 1.5 (H) in 17.5 (D) x 3.8 (H) cm
Weight	0.53 kg / 1.2 lbs	0.48 kg / 1.1 lbs	0.53 kg / 1.2 lbs
WEEE weight	1.2 kg / 2.6 lbs	0.53 kg / 1.2 lbs	0.74 kg / 1.6 lbs
Shipping weight	1.74 kg / 3.8 lbs	0.79 kg / 1.8 lbs	1.1 kg / 2.4 lbs
PoE injector	802.3at		
Power supply	802.3at + AC Adapter (12 v)	802.3at PoE	802.3at PoE
Maximum power consumption (W)	15.2 W	15.6 W	13.7 W
Status indicators	Six (6) LED (WLAN/Link) (LAN/Link) Power, Test		
Antennas	3+3 (SMA 2.4 GHz + TNC 5 GHz)	6 fully internal	3+3 (SMA 2.4 GHz + TNC 5 GHz)
Wired network ports	(2) 10/100/1000 auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE); (1) RJ-45 console; (1) USB 2.0		
Accessories included	Wall/ceiling mount kit		
Virtual access points	Up to 8 per SonicPoint		
Chassis	UL 2043 plenum rated		
Standards and compliance	SonicPoint ACe	SonicPoint ACi	SonicPoint N2
IEEE Standard	802.11a/b/g/n/ac Wave 1	802.11a/b/g/n/ac Wave 1	802.11a/b/g/n
Compliance	IEEE 802.11i, IEEE 802.3e, IEEE 802.3i, IEEE 802.3at, WPA/WPA2, TKIP, AES		
Regulatory	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE, IEEE 802.11ac		
MIMO	SU-MIMO 3x3 (3 streams)		
Max/Recommended connected clients per radio	128/30	128/30	128/30
Certifications	WiFi, Dynamic Frequency Selection (DFS)		
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union		
Environmental	SonicPoint ACe/ACi/N2		
Temperature range	32 to 104°F, 0 to 40°C		
Humidity	10 - 95%, non-condensing		
Radio specifications	SonicPoint ACe	SonicPoint ACi	SonicPoint N2
Radios	Dual: 3x3 11n + 3x3 11ac		Dual: 3x3 11n + 3x3 11n
Frequency bands	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		
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 **802.11ac: 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)		

## SonicPoint Series con't

Security		SonicPoint ACe/ACi/N2
Data encryption		WPA2; IPSec, 802.11i, WPA; 64/128/152-bit WEP, TKIP, AES, SSL VPN*
Authentication		SonicPoint ACe/ACi/N2
Authentication		RADIUS, Active Directory, single sign-on (SSO)
Security		SonicPoint ACe/ACi/N2
Data encryption		WPA2; IPSec, 802.11i, WPA; 64/128/152-bit WEP, TKIP, AES, SSL VPN*
Authentication		SonicPoint ACe/ACi/N2
Authentication		RADIUS, Active Directory, single sign-on (SSO)

\*When used with SonicWall Secure Remote Access Series appliance

\*\*Available on SonicPoint ACe and SonicPoint ACi only

## SonicPoint Series PoE Injector

Hardware Specifications		SonicPoint ACe/ACi/N2
Number of ports		2: (1) Data In; (1) data and power out
Dimensions		1.22 (H) x 1.97 (W) x 6.30 (L) in; (31 (H) x 50 (W) x 160 (L) mm
Weight		0.5 lbs/(0.3 kg)
WEEE weight		0.85 lbs/(0.38 kg)
Shipping weight		0.87 lbs/(0.4 kg)
Connectors		Shielded RJ-45, EIA 568A and 568B
Status Indicators		System indicator: AC power (yellow); User indicator: channel power active (green)
Data rates		10/100/1000 Mbps
Power over LAN output		SonicPoint ACe/ACi/N2
Pin assignment and polarity		4/5 (+), 7/8 (-)
Output power voltage		-48 VDC
Maximum output power		30 W
Input power requirements		SonicPoint ACe/ACi/N2
AC input voltage		100 to 240 VAC
AC frequency		50 to 60 Hz
AC input current		0.8A at 100-240 VAC
Standards and compliance		SonicPoint ACe/ACi/N2
Regulatory compliance		CB, S Mark, RCM, ICES, cUL, CCC, CE, GS, BIS, PSE, MOM, EAC, KCC/MSIP, BSMI, UL, FCC
Electromagnetic emission and immunity		Class B emission level, EN 55022, CISPR 22, FCC Part 15
Safety		IEC/EN/UL 60950-1
Environmental		EU RoHS, China RoHS, EU WEEE, DOE Level VI, MEPS
Environmental requirements		SonicPoint ACe/ACi/N2
Operating ambient temperature		32 to 104 °F, 0 to 40 °C
Operating humidity		Maximum 90%, non-condensing
Storage temperature		-4 to 158 °F, -20 to 70 °C
Storage humidity		Maximum 95%, non-condensing

## SonicWall Secure Mobile Access (SMA)

### Appliance Specifications

Choose from a range purpose-built secure mobile access (SMA) appliances.  
Get flexible deployment options with virtual and physical appliances.



### Physical appliance specifications

Performance	SMA 200	SMA 400	SMA 6200	SMA 7200	SRA EX9000
Concurrent sessions/Users	Up to 50	Up to 250	Up to 2,000	Up to 10,000	Up to 20,000
SSL VPN Throughput* (at max CCU)	Up to 100 Mbps	Up to 368 Mbps	Up to 400 Mbps	Up to 3.75 Gbps	Up to 3.75 Gbps
Form factor	1U	1U	1U	1U	2U
Dimensions	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	27.0 x 18.9 x 3.4 in (68.6 x 48.2x 8.8 cm)
Appliance weight	11 lbs (5 kgs)	11 lbs (5 kgs)	16 lbs (7.3 kgs)	18.3 lbs (8.3 kgs)	49.1 lbs (22.3 kgs)
Encryption data acceleration (AES-NI)	NO	NO	YES	YES	YES
Dedicated management port	NO	NO	YES	YES	YES
SSL acceleration	NO	NO	YES	YES	YES
Storage	2GB (Flash Memory)	2GB (Flash Memory)	2 X 500 GB SATA	2 X 500 GB SATA	2 X 2TB SATA
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	6 (6-port 1GE)	8 (6-port 1GE + 2-port 10Gb SFP+)	12 (8-port 1GE + 4-port 10Gb SFP+)
Memory	2GB	4GB	8GB DDR3	16GB DDR3	32 GB DDR3
TPM chip	NO	NO	YES	YES	NO
Processor	2 cores	4 cores	4 cores	4 cores	2 X 4 cores
MTBF (@ 25°C or 77°F) in hours	61,815	60,151	200,064	233,892	129,489
Operations and Compliance	SMA 200	SMA 400	SMA 6200	SMA 7200	SRA EX9000
Power	Fixed power supply	Fixed power supply	Fixed power supply	Dual power supply, hot swappable	Dual power supply, hot swappable
Input rating	100-240VAC, 50-60MHz	100-240VAC, 50-60MHz	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A	100-240 VAC, 2.8.5 A
Power consumption	26.9 W	31.9 W	78 W	127 W	320 W
Total heat dissipation	92 BTU	109 BTU	266 BTU	432 BTU	1091 BTU
Environmental	WEEE, EU RoHS, China RoHS				
Non-operating shock	110 g, 2 msec				
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC				
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme				
Operating temperature	0°C to 40°C (32°F to 104° F)				
FIPS certification	NO	NO	FIPS 140-2 Level 2 with anti-tamper protection		

\* Throughput performance may vary based on deployment and connectivity. Published numbers are based on internal lab conditions

### Virtual appliance specifications

Specifications	SMA 500v (ESX/ESXI)	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper-V)
Concurrent sessions	Up to 250 users	Up to 5000	Up to 250
SSL-VPN throughput* (at max CCU)	Up to 186 Mbps	Up to 1.58 Gbps	Up to 1.2 Gbps
Allocated memory	2GB		8 GB
Processor	1 core		4 cores
SSL acceleration	NO		YES
Applied disk size	2GB	64 GB (default)	Admin Configurable
Operating system installed	Linux		Hardened Linux
Dedicated management port	NO		YES

\* Throughput performance may vary based on deployment and connectivity. Published numbers are based on internal lab conditions. SMA 8200v on Hyper-V scales up to 5000 concurrent sessions and provides up to 1.58 Gbps SSL-VPN throughput when running SMA OS 12.1 with Windows Server 2016



## Feature Summary (comparison by model)

Category	Feature	200	400	500v	6200	7200	9000	8200v
Throughput	Max concurrent user sessions	50	250	250	2,000	10,000	20,000	5,000
	Max SSL/TLS throughput	100 Mbps	368 Mbps	186 Mbps	400 Mbps	3.75 Gbps	3.75 Gbps	1.58 Gbps
Client access	Layer 3 tunnel	•	•	•	•	•	•	•
	Split-tunnel and redirect-all	•	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•	•
	Auto ESP encapsulation	-	-	-	•	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•	•
	Secure Network Detection	-	-	-	•	•	•	•
	File browser (CIFS/NFS)	•	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•	•
	VMware View	-	-	-	•	•	•	•
	On Demand tunnel	-	-	-	•	•	•	•
	Chrome/Firefox extensions	-	-	-	•	•	•	•
	CLI tunnel support	-	-	-	•	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	-	-	-	-
Mobile access	Connect Tunnel (Windows, Mac OSX, Linux)	-	-	-	•	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•	•
	Per app VPN	-	-	-	•	•	•	•
	App control enforcement	-	-	-	•	•	•	•
User portal	App ID validation	-	-	-	•	•	•	•
	Branding	•	•	•	•	•	•	•
	Customization	-	-	-	•	•	•	•
	Localization	•	•	•	•	•	•	•
	User defined bookmarks	•	•	•	•	•	•	•
	Custom URL support	•	•	•	•	•	•	•
Security	SaaS application support	-	-	-	•	•	•	•
	FIPS 140-2	-	-	-	•	•	•	-
	ICSA SSL-TLS	-	-	-	•	•	•	•
	Suite B ciphers	-	-	-	•	•	•	•
	Dynamic EPC interrogation	•	•	•	•	•	•	•
	Role Based Access Control (RBAC)	-	-	-	•	•	•	•
	Endpoint registration	•	•	•	•	•	•	•
	Secure File Share (Capture ATP)	•	•	•	•	•	•	•
	Endpoint quarantine	•	•	•	•	•	•	•
	OSCP CRL validation	-	-	-	•	•	•	•
	Cipher selection	-	-	-	•	•	•	•
	PKI and client certificates	•	•	•	•	•	•	•
	Geo IP filter	•	•	•	-	-	-	-
	Botnet filter	•	•	•	-	-	-	-
Forward proxy	•	•	•	•	•	•	•	
Authentication and identity services	Reverse proxy	•	•	•	•	•	•	•
	SAML 2.0	-	-	-	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•	•
	SAML Identity Provider (IdP)	-	-	-	•	•	•	•
	Biometric device support	•	•	•	•	•	•	•
	Face ID support for iOS	•	•	•	•	•	•	•
Two-factor authentication (2FA)	•	•	•	•	•	•	•	
Multi-factor authentication (MFA)	-	-	-	•	•	•	•	

## Feature Summary (comparison by model con't)

Category	Feature	200	400	500v	6200	7200	9000	8200v
Authentication and identity services con't	Chained authentication	-	-	-	•	•	•	•
	One Time Passcode (OTP)	•	•	•	•	•	•	•
	Common Access Card (CAC) support	-	-	-	•	•	•	•
	X.509 certificate support	•	•	•	•	•	•	•
	Captcha integration	-	-	-	•	•	•	•
	Remote password change	•	•	•	•	•	•	•
	Forms based SSO	•	•	•	•	•	•	•
	Federated SSO	-	-	-	•	•	•	•
Access control	Session persistence	-	-	-	•	•	•	•
	Auto logon	•	•	•	•	•	•	•
	Group AD	•	•	•	•	•	•	•
	LDAP attributes	•	•	•	•	•	•	•
Management	Geolocation policies	•	•	•	-	-	-	-
	Continual endpoint monitoring	•	•	•	•	•	•	•
	Management interface (ethernet)	-	-	-	•	•	•	•
	Management interface (console)	-	-	-	•	•	•	•
	HTTPS administration	•	•	•	•	•	•	•
	SSH administration	-	-	-	•	•	•	•
	SNMP MIBS	•	•	•	•	•	•	•
	Syslog and NTP	•	•	•	•	•	•	•
	Usage monitoring	•	•	•	•	•	•	•
	Configuration rollback	•	•	•	•	•	•	•
	Centralized management	-	-	-	•	•	•	•
	Centralized reporting	-	-	-	•	•	•	•
	Management REST APIs	-	-	-	•	•	•	•
	Authentication REST APIs	-	-	-	•	•	•	•
	RADIUS accounting	-	-	-	•	•	•	•
Networking	Scheduled tasks	-	-	-	•	•	•	•
	Centralized session licensing	-	-	-	•	•	•	•
	Event-driven auditing	-	-	-	•	•	•	•
	IPv6	•	•	•	•	•	•	•
	Global load balancing	-	-	-	•	•	•	•
	Server load balancing	•	•	•	-	-	-	-
	TCP state replication	•	•	•	•	•	•	•
	Cluster state failover	-	-	-	•	•	•	•
	Active/passive high availability	-	•	•	•	•	•	•
	Active/active high availability	-	-	-	•	•	•	•
Integration	Horizontal scalability	-	-	-	•	•	•	•
	Single or multiple FQDNs	-	-	-	•	•	•	•
	L3-7 smart tunnel proxy	•	•	•	•	•	•	•
	L7 application proxy	•	•	•	•	•	•	•
	2FA TOTP support	•	•	•	•	•	•	•
	EMM and MDM product support	-	-	-	•	•	•	•
Licensing options	SIEM product support	-	-	-	•	•	•	•
	TPAM password vault	-	-	-	•	•	•	•
	ESX hypervisor support	-	-	•	-	-	-	•
	Hyper-V hypervisor support	-	-	-	-	-	-	•
	Subscription based license	-	-	-	•	•	•	•
	Perpetual license with support	•	•	•	•	•	•	•
Virtual assist	Web Application Firewall (WAF)	•	•	•	-	-	-	-
	Spike licensing	•	•	•	•	•	•	•
	Tiered licensing	-	-	-	•	•	•	•
	Virtual assist	•	•	•	-	-	-	-

\* To learn more about VPN clients, visit: <https://www.sonicwall.com/en-us/products/remote-access/vpn-client>

## Features

	APPLIANCE, VIRTUAL APPLIANCE	WINDOWS SERVER®
<b>Advanced Total Secure subscription – Advanced protection bundle</b>		
Includes SonicWall Capture ATP advanced attachment and URL protection, in addition to the Total Secure subscription	Yes	Yes
<b>Total Secure subscription – Basic protection bundle</b>		
Includes email protection dynamic 24x7 subscription plus multi-layer anti-virus (McAfee and Cyren), malicious URL detection and compliance management subscription features	Yes	Yes
<b>Ransomware &amp; Zero-day protection – optional</b>		
SonicWall Capture ATP advanced attachment and URL protection add-on for Total Secure subscription	Yes	Yes
<b>Complete inbound and outbound email protection</b>		
Anti-spam effectiveness	Yes	Yes
Connection management with advanced IP reputation	Yes	Yes
Phishing detection, classification, blocking	Yes	Yes
Directory harvest, denial of service, NDR protection	Yes	Yes
Anti-spoofing with support for SPF, DKIM and DMARC	Yes	Yes
Policy rules for user, group, all	Yes	Yes
In memory message transfer agent (MTA) for enhanced throughput	Yes	Yes
Complete inbound and outbound protection in a single system	Yes	Yes
<b>Easy administration</b>		
Installation	< 1 hour	< 1 hour
Management per week	< 10 min	< 10 min
Automatic multi-LDAP sync for users, groups	Yes	Yes
Compatible with all SMTP email servers	Yes	Yes
SMTP Authentication support (SMTP AUTH)	Yes	Yes
Allow/deny end user controls	Yes	Yes
Customize, schedule and email 30+ reports	Yes	Yes
Judgment details	Yes	Yes
At-a-glance, customizable management dashboard	Yes	Yes
Rapid message search engine	Yes	Yes
Scalable split-mode architecture	Yes	Yes
Clustering and remote clustering	Yes	Yes
<b>Easy for end users</b>		
Single sign-on	Yes	Yes
Per user junk boxes, junk box summary actionable email	Yes	Yes
Per user anti-spam aggressiveness, block/allow lists	Yes	Yes
<b>Email protection subscription with dynamic support-required</b>		
SonicWall Cloud anti-virus, anti-spam, anti-phishing auto-updates every minute	Yes	Yes
24x7 support	Yes	Yes
RMA (appliance replacement)	Yes	Yes
Software/firmware updates	Yes	Yes
<b>Anti-virus subscription-optional</b>		
McAfee and Cyren Anti-virus	Yes	Yes
SonicWall TimeZero anti-virus	Yes	Yes
Zombie detection	Yes	Yes
<b>Compliance subscription-optional</b>		
Robust policy management,	Yes	Yes
Attachment scanning	Yes	Yes
Record ID matching	Yes	Yes
Dictionaries	Yes	Yes
Approval boxes/workflow	Yes	Yes
Email archiving	Yes	Yes
Compliance reporting	Yes	Yes
<b>Encryption subscription-optional</b>		
Compliance subscription capabilities plus policy-enforced email encryption and secure email exchange	Yes	Yes

## System Specifications

EMAIL SECURITY APPLIANCES	5000	7000	9000
Domains	Unrestricted		
Operating system	Hardened SonicWall Linux OS appliance		
Rackmount chassis	1RU	1RU	1RU
CPU(s)	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Hard drive	500 GB	1 TB	1 TB
Redundant disk array (RAID)	–	RAID 1	RAID 5
Hot swappable drives	No	Yes	Yes
Redundant power supply	No	No	Yes
SAFE Mode Flash	Yes	Yes	Yes
Dimensions	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 cm	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 cm	27.5 x 19.0 x 3.5 in 69.9 x 48.3 x 8.9 cm
Weight	16 lbs / 7.26 kg	16 lbs / 7.26 kg	50.0 lbs/ 22.7 kg
WEEE weight	16 lbs / 7.37 kg	16 lbs / 22.2 kg	48.9 lbs/ 22.2 kg
Power consumption (watts)	46	48	158
BTUs	155	162	537
MTBF @25C in hours	130,919	150,278	90,592
MTBF @25C in years	14.9	17.2	10.3
<b>Email Security Software</b>			
Domains	Unrestricted		
Operating system	Microsoft Hyper-V Server 2012 (64-bit) or higher Windows Server 2008 R2 or higher x64 bit only		
CPU	Intel or AMD 64-bit processor		
RAM	8 GB minimum configuration		
Hard drive	160 GB minimum configuration		
<b>Email Security Virtual Appliance</b>			
Hypervisor	ESXi™ and ESX™ (version 5.0 and newer)		
Operating system installed	8 GB (expandable)		
Allocated memory	4 GB		
Appliance disk size	160 GB (expandable)		
VMware hardware compatibility guide	<a href="http://www.vmware.com/resources/compatibility/search.php">http://www.vmware.com/resources/compatibility/search.php</a>		

## Features

<b>COMPLETE INBOUND AND OUTBOUND EMAIL PROTECTION</b>	
Capture ATP - advanced attachment and URL protection	Optional
Anti-spam effectiveness	Yes
Sender IP reputation	Yes
Directory harvest, denial of service, protection	Yes
Capture Labs reputation services	Yes
SonicWall Cloud Anti-Virus	Yes
Multi Anti-Virus	Yes
Malicious URL detection	Yes
Phishing detection, classification, blocking	Yes
Zombie detection, flood protection	Yes
Policy rules	Yes
<b>EASY ADMINISTRATION</b>	
Multi-tenant management	Yes
Office 365 and G suite support	Yes
Automated provisioning and setup	Yes
Reputation auto-updates	Yes
Anti-spam auto-updates	Yes
Automatic upgrades and maintenance	Yes
Anti-Virus signature auto-updates	Yes
Customize, schedule and email reports	Yes
Automatic LDAP Sync	Yes
Rapid message search engine	Yes
<b>EASY FOR END-USERS</b>	
SMTP Auth for inbound/outbound	Yes
Allow/deny all end user controls	Yes
Emergency Inbox	Optional
Per user junk boxes	Yes
Per user anti-spam aggressiveness	Yes
Per user allowed/blocked lists	Yes
Junk box summaries in 15 languages	Yes
Judgement details	Yes
<b>SYSTEM FEATURES</b>	
Compatible with all SMTP email servers	Yes
SMTP Authentication support (SMPT AUTH)	Yes
Unrestricted domains supported	Yes
Email Continuity	Optional
15 days of junk email retention	Yes
Email spooling up to 7 days	Yes
<b>COMPLIANCE POLICY AND MANAGEMENT</b>	
Attachment scanning	Yes
Record ID matching	Yes
Dictionaries	Yes
Approval boxes/workflow	Yes
Compliance reporting	Yes

Features con't

<b>EMAIL ENCRYPTION SERVICE FOR HOSTED EMAIL SECURITY - OPTIONAL</b>	
Policy-enforced secure email exchange	Yes
Works natively on mobile devices (no app required)	Yes
Outlook Send Secure add-on button	Yes
Quickly encrypts file attachments up to 100MB	Yes
Send messages directly to recipient with nothing for them to install	Yes
Message notification includes link to auto-provisioned recipient accounts	Yes
Replies are automatically decrypted into sender's inbox	Yes
Built in tracking of all messages and files sent, received, and opened	Yes
Rebrand encrypted email	Yes
Reporting and monitoring	Yes
500 MB per company	Yes
Industry-standard, compliance-grade encryption: AES 256, TLS	Yes
No keys to manage or lose	Yes
Portal localized in ten languages including English, French, Italian, German, Spanish, Japanese, Brazilian Portuguese, Simplified & Mandarin Chinese, and Korean	Yes
Outlook 2010/2013/2016 support	Yes
SSAE 16, SAS 70 Type II & Fedramp Certified Data Center	Yes
<b>SUPPORT AND SERVICES</b>	
24x7 email and phone support	Yes
Multiple data centers	Yes

### Features

Feature	Benefit
Real-Time Dashboard	Get real-time, visual representation of applications being used, traffic volume, user activity and location of use
App Discovery	Automate cloud application discovery by leveraging your SonicWall firewall log files to identify shadow IT activities on the network
App Risk Assessment	Make informed decisions to block/unblock applications based on the risk assessment
App Classification and Control	Classify applications into Sanctioned or Unsanctioned apps, and set policies to block risky applications

## SonicWall Capture Security Center

### Licensing and packaging

The cloud-based services of CSC Management, Reporting, Analytics and CAS are available in below packaging options. The minimum use requirement is each managed firewall must have an active AGSS or CGSS subscription.

#### 1. CSC Basic Management (Lite)

This version is best suited for Backup/Restore of firewall system or preferences, and for firmware upgrade. Any firewall with AGSS or CGSS subscription can have this basic management functionality activated to help administer firewalls.

#### 2. CSC Management

This paid subscription option activates full management capabilities including Workflow Automation and Zero-Touch Deployment features.

#### 3. CSC Management and Reporting

This license option is an ideal fit for larger institutions with many firewalls deployed in geographically dispersed locations that are under group-level or tenant-based management. These include mid-market organizations, distributed enterprises, public sector and educational organization with many districts and campuses, and managed service providers (MSPs).

In addition to full management capabilities, this subscription option provides full reporting features to perform periodic or on-demand security and network performance reviews and audits. This can be done using the on-screen interactive universal dashboard with live charts and tables, or off-screen with scheduled exported reports.

#### 4. CSC Analytics

This is a powerful add-on service to all Capture Security Center subscription options. Activating the service provides full access to the SonicWall Analytics and SonicWall Cloud App Security tools and services to conduct network forensic and threat hunting using comprehensive drill-down and pivoting capabilities.

	Features	CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Management	Backup/Restore – firewall system	Yes	Yes	Yes	Yes
	Backup/Restore – firewall preferences	Yes	Yes	Yes	Yes
	Firmware upgrade	From local file only	From local file only or MySonicWall	Yes	From local file only
	Task scheduling	–	Yes	Yes	–
	Group firewall management	–	Yes	Yes	–
	Inheritance – forward/reverse	–	Yes	Yes	–
	Zero touch deployment <sup>1</sup>	–	Yes	Yes	–
	Offline firewall signature downloads	–	Yes	Yes	–
	Workflow	–	Yes	Yes	–
	Pooled Licenses – Search, Sharing, Used Activation Code Inventory	–	Yes	Yes	–
Reporting (Netflow/ IPFIX based)	Schedule reports, Live monitor, Summary dashboards	–	–	Yes	Yes
	Download Reports: Applications, Threats, CFS, Users, Traffic, Source/Destination (1-year flow reporting)	–	–	Yes	Yes
Analytics (Netflow/ IPFIX based)	Network forensic and threat hunting using drill-down and pivots	–	–	–	Yes
	Cloud App Security	–	–	–	Yes
	30-day traffic data retention	–	–	–	Yes
Technical Support		Web Cases only	24x7 support	24x7 support	24x7 support

<sup>1</sup> Supported for SOHO-W with firmware 6.5.2+; TZ, NSA series and NSa 2650-6650 with firmware 6.5.1.1+. Not supported for SOHO or NSv series.



## SonicWall Capture Security Center con't

### Supported firewall models

Capture Security Center is available only to AGSS/CGSS customers with

SOHO-W, TZ Series, NSA Series, NSa 2650-6650, and NSv Series firewalls. For SuperMassive 9000 Series, NSa 9250 to 9650 and NSsp 12400 to 12800,

CSC Management subscription option is automatically activated as part of its corresponding AGSS subscription activation.

Capture Security Center			
	Management	Reporting	Analytics
Entry-level FW	SOHO-W, TZ Series, NSv 10-100	TZ Series, NSv 10-100	TZ Series, NSv 10-100
Mid-range FW	NSA Series, NSa 2650-6650, NSv 200-400	NSA Series, NSa 2650-6650, NSv 200-400	NSA Series, NSa 2650-6650, NSv 200-400
High-end FW	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600		

### Ordering information

Product	SKU
SonicWall Capture Security Center Management for TZ Series, SOHO-W, NSv 10 to 100 1Yr	01-SSC-3664
SonicWall Capture Security Center Management for TZ Series, SOHO-W, NSv 10 to 100 2Yr	01-SSC-9151
SonicWall Capture Security Center Management for TZ Series, SOHO-W, NSv 10 to 100 3Yr	01-SSC-9152
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3665
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9214
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9215
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 to 100 1Yr	01-SSC-3435
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 to 100 2Yr	01-SSC-9148
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 to 100 3Yr	01-SSC-9149
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3879
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9154
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9202
SonicWall Capture Security Center Analytics for TZ Series, NSv 10 to 100 1Yr	02-SSC-0171
SonicWall Capture Security Center Analytics for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	02-SSC-0391

### 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 Capture Security Center

- SonicWall Network Security Appliances: NSa 2600 to NSa 6650, and TZ Series appliances
- SonicWall Network Security Virtual Appliances: NSv 10 to NSv 400

- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)

## SonicWall Global Management System

### 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

---

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:

<http://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)

#### GMS gateway

---

SonicWall SuperMassive™ E10000 Series, SonicWall SuperMassive™ 9000 Series, E-Class Network Security Appliance (NSA), and NSA Series

#### Supported SonicWall appliances managed by GMS

---

SonicWall Network Security Appliances: SuperMassive E10000 and 9000 Series, E-Class NSA, NSa, NSA, and TZ Series appliances®

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

## SonicWall Analyzer

### Operating system

---

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  
Windows 10  
Windows 8.1 64-bit  
Windows 7 64-bit

### Hardware requirement for Analyzer server

---

Minimum Requirements: Single Core 3 GHz x86 Processor, 4 GB RAM, 100 GB HDD

### Internet browsers

---

Microsoft® Internet Explorer 11.0 or higher  
Mozilla Firefox 37.0 or higher  
Google Chrome 42.0 and above  
Safari (latest version)

### Virtual appliance

---

**Hypervisor:** VMware® ESXi 6.5, 6.0 and 5.5

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

**VMware Compatibility Guide:** [www.vmware.com/resources/compatibility/search.php](http://www.vmware.com/resources/compatibility/search.php)

### Supported SonicWall appliances

---

SonicWall Next-Generation Firewalls: SuperMassive™ Series, E-Class Network Security Appliance (NSA) Series, NSa series, NSA Series and TZ Series  
SonicWall Secure Mobile Access (SMA) appliances: SMA Series and E-Class SRA  
SonicWall Email Security appliances

### Supported SonicWall firmware

---

SonicWall SuperMassive E10000 Series: SonicOS 6.0 or higher  
SonicWall SuperMassive 9000 Series: SonicOS 6.1 or higher  
SonicWall NSa Series: SonicOS 6.5 or higher  
SonicWall E-Class NSA and NSA Series: SonicOS 5.0 or higher  
SonicWall TZ Series: SonicOS 5.0 or higher  
SonicWall SOHO Series: SonicOS 6.2.6 or higher  
SonicWall Secure Mobile Access Series: Firmware 10.7.2 or higher  
SonicWall SRA for SMB: Firmware 2.0 or higher  
SonicWall Aventail™ E-Class SRA: Firmware 9.0 or higher  
SonicWall Email Security: Firmware 7.2 or higher

© 2018 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

## 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](http://www.sonicwall.com) or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.  
1033 McCarthy Boulevard  
Milpitas, CA 95035

Refer to our website for additional information.  
**[www.sonicwall.com](http://www.sonicwall.com)**