SONICWALL

SonicWall TZ Series

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

With the SonicWall TZ series,
Small and medium-sized organizations and distributed enterprises enjoy the benefits of an integrated security solution that meets all their needs. Combining high-speed threat prevention capabilities and software-defined wide area network (SD-WAN) technology with a wide variety of wireless connectivity and networking capabilities for more simplified deployment and centralized management, The TZ series provides a unified security solution at a low total cost of ownership.

Flexible and integrated security solution

The TZ series is based on SonicOS, the SonicWall operating system, which offers a host of features. Firewalls compatible with the latest SonicOS 7.0 operating system incorporate a new modern-looking UI / UX, advanced security features, networking, and simplified policy management.

SonicOS also includes a powerful set of capabilities that provide organizations with the flexibility to tailor these Unified Threat Management (UTM) firewalls to their specific network requirements. For example, the integrated wireless controller, compliant with IEEE 802.11 standards, as well as the ability to add our own *access points* SonicWave 802.11ac Wave 2, simplify the creation of a high-speed wireless network. In order to reduce the cost and complexity of connecting *access points* high-speed wireless devices and other Power over Ethernet (PoE) technology devices such as IP cameras, telephones and printers, the TZ300P, TZ600P and TZ570P firewalls offer PoE / PoE + power.

Distributed retail companies and campus environments can use the many tools in SonicOS to further benefit. Branch offices can exchange information with the central office securely using virtual private networks (VPNs). The creation of virtual LANs (VLANs) allows segmenting the network into corporate and customer groups with rules that determine the level of communication with devices in other VLANs. SD-WAN offers a secure alternative to expensive MPLS circuits while providing consistent application performance and availability. Zero-Touch implementation, which allows the firewall to be provisioned remotely via the cloud, simplifies the installation of TZ firewalls in remote locations.

Superior performance and threat prevention

Our vision for network protection in today's ever-evolving cyber threat landscape is real-time, automated threat detection and prevention. Thanks to the combination of cloud-based and integrated technologies, our firewalls have robust protection validated by independent third-party testing and are characterized by an extremely high level of security effectiveness. Unknown threats are sent to SonicWall's Capture Advanced Threat Protection (ATP) cloud-based multi-engine sandbox for analysis. In addition, the patent-pending Memory Inspection technology

Advantage:

Flexible and integrated security solution

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

Threat prevention and superior quality performance

- Real-time memory deep inspection technology patent pending
- Patented deep packet inspection technology without reassembled
- TLS 1.3 support
- Industry Validated Security Effectiveness

Simple functions of deployment, configuration

and ongoing management

- Zero-Touch implementation
- Centralized management, based cloud and local
- Incorporation of the SonicExpress application

Real-time deep-dive (RTDMI ™) increases the effectiveness of Capture ATP. The RTDMI engine detects and blocks malware and zero-day threats through direct in-memory inspection. RTDMI technology is accurate, minimizes false positives, and identifies and mitigates sophisticated attacks in which malware weapons are exposed for less 100 nanoseconds. Combined with it, our proprietary one-step * reassembly-free Deep Packet Inspection (RFDPI) engine examines every byte in every packet and inspects incoming and outgoing traffic directly at the firewall. By using Capture ATP with RTDMI technology on the SonicWall Capture Cloud platform along with built-in capabilities such as intrusions, antimalware 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 utilizes deep inspection of TLS encrypted traffic (DPI-SSL) from TZ series firewalls by installing and managing trusted TLS certificates.

As encryption technologies are increasingly being used to protect web sessions, firewalls must be able to scan encrypted traffic for threats. TZ series firewalls provide complete protection by decrypting and inspecting encrypted connections using TLS / SSL and SSH, regardless of port or protocol. The firewall looks for protocol breaches, threats, zero-day attacks, intrusions and even defined criteria analyzing each packet in depth. This deep packet inspection engine detects and prevents stealth attacks that use cryptography. It also blocks encrypted malware downloads, stops the spread of infections, and thwarts command communications. and control and data exfiltration. The include and exclude rules provide full control allowing you to customize which traffic should be subjected to decryption and inspection according to specific corporate and / or legal requirements.

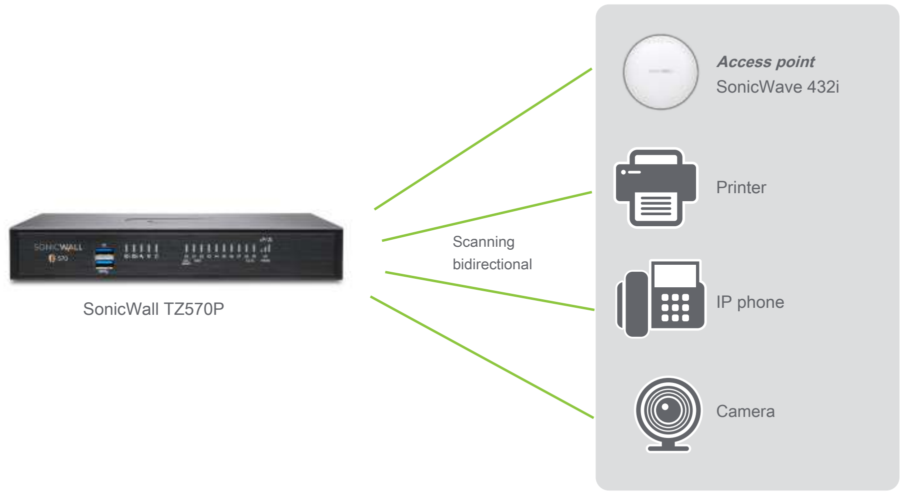
The TZ670 and TZ570 firewalls support TLS 1.3, which offers several changes that improve performance and security, while eliminating complexities.

Simple functions of deployment, configuration and ongoing management

SonicWall simplifies the configuration and management of TZ series firewalls and *access points* SonicWave 802.11ac Wave 2, regardless of where they are implemented. Management, reporting, licensing and analytics are centralized in our cloud-based Capture Security Center, which offers the highest level of visibility, agility, and the ability to control the entire SonicWall security ecosystem centrally from a single console .

A key component of the Capture Security Center is the Zero-Touch implementation. This cloud-based capability simplifies and accelerates the deployment and provisioning of SonicWall firewalls in remote locations and branch offices. The process requires minimal user intervention and fully automates 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 occur instantly and automatically. Simplified deployment and configuration, coupled with ease of management, enable organizations to lower the total cost of ownership and achieve a high return on investment.

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



802.3at PoE + Devices

Built-in security and power for your PoE-enabled devices

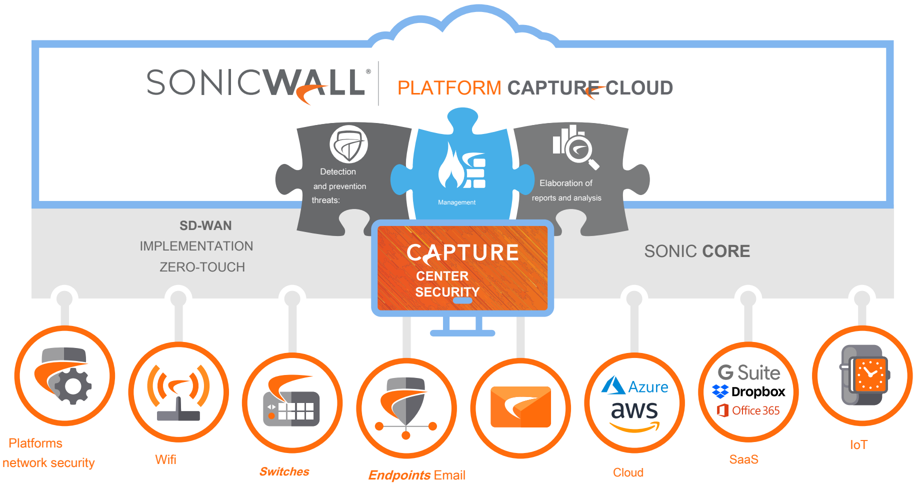
Power your PoE-enabled devices without the cost or complexity of a Power over Ethernet switch or injector. The TZ300P, TZ600P and TZ570P firewalls integrate IEEE 802.3at technology to power PoE and PoE + devices, such as wireless access points, cameras, IP phones, etc. The firewall scans all traffic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

Capture Cloud Platform

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

If data accessing the network is found to contain previously unseen malicious code, SonicWall Capture Labs' specialized internal threat research team develops definitions that are stored in the Capture Cloud platform database and they are deployed on client firewalls to provide up-to-date protection. New updates take effect immediately without the need to restart or interrupt the system. Device-resident definitions offer protection against a wide variety of attack types, covering tens of thousands of individual threats. In addition to the countermeasures built into the device, TZ firewalls also have continuous access to the Capture Cloud platform database, which includes tens of millions of definitions.

Along with threat prevention, the Capture Cloud platform also offers a single management console and enables administrators to easily create real-time and historical reports on network activity.



Threat protection advanced

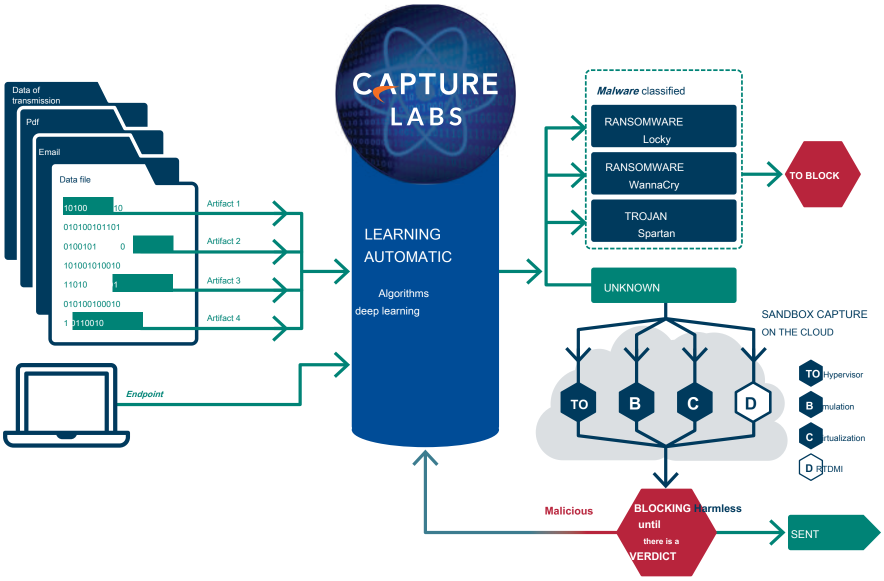
SonicWall's real-time, automated breach prevention is based on two advanced malware detection technologies: Capture Advanced Threat Protection ™ (Capture ATP) and Capture Security appliance ™ (CS *to).*

Capture ATP is a platform for *sandbox* cloud multi-engine, including Real-Time Deep Memory Inspection ™ (RTDMI), *sandboxing* virtualized, full system emulation and analytics technology at the hypervisor level. CS *to* It is a local device equipped with RTDMI, which uses memory-based dynamic and static techniques to obtain fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day attacks on various SonicWall solutions, such as next-generation firewalls.

Suspicious files are sent to one of these solutions, where they are analyzed using deep learning algorithms, with the possibility of retaining them in the *gateway* until a verdict is rendered. In the case of Capture ATP, files identified as malicious are locked and a file is immediately created. *hash* within the Capture ATP database so that all clients can take advantage of it to block subsequent attacks. These definitions are then sent to firewalls to create static defenses. For legal reasons and privacy, the results generated by CS *to* they are not shared outside of your organization.

These services scan a wide variety of operating systems and file types, including executable programs, DLLs, PDF files, MS Office documents, archives, JARs, and APKs.

In order to offer protection of *endpoints* complete, SonicWall Capture Client combines state-of-the-art antivirus technology with *sandbox* SonicWall cloud-based multi-engine with optional integration into SonicWall firewalls.

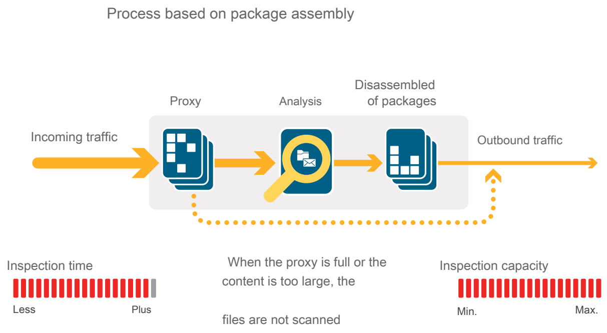


Deep packet inspection engine without reassembly

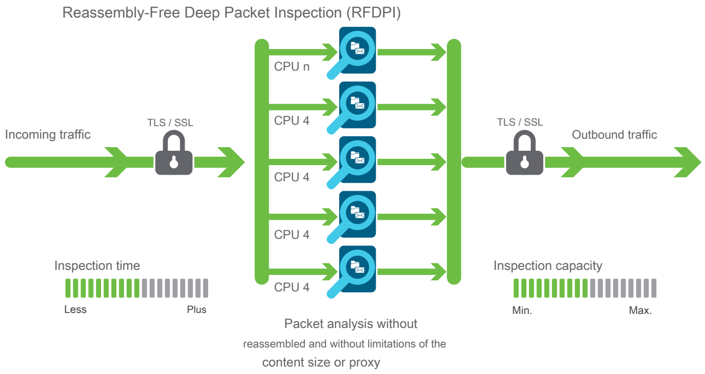
SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a low-latency, one-step inspection system that performs high-speed, stream-based, bi-directional traffic analysis without buffering or proxies to discover potential intrusion attempts or downloads of *malware* and to identify application traffic regardless of port and protocol. This patented engine is based on inspecting useful data from data traffic to detect threats at Layers 3-7 and subjects network flows to extensive and repeated normalization and decryption processes in order to neutralize advanced evasion techniques that seek to bypass detection engines and introduce malicious code into the network.

Once a packet undergoes the necessary pre-processing, including TLS / SSL decryption, it is analyzed with the help of a single proprietary in-memory representation of three definition databases: intrusion attacks, *malware* and applications. The connection status is constantly updated on the firewall and checked with these databases until an attack or other security event is identified, in which case a preset action is taken.

In most cases, the system ends the connection and creates logging and notification events. However, the motor can also be configured to perform only inspection or, in the case of application discovery, to provide Layer 7 bandwidth management services for the rest of the application flow as soon as an application is identified.



Competitive proxy-based architecture (competition)


Reassembly-Free Deep Packet Inspection (RFDPI)
Incoming traffic
TLS / SSL
CPU n
CPU 4
CPU 4
CPU 4
CPU 4
TLS / SSL
Outbound traffic
Inspection time
Less
Plus
Inspection capacity
Min.
Max.
Packet analysis without reassembled and without limitations of the content size or proxy

SonicWall flow-based architecture

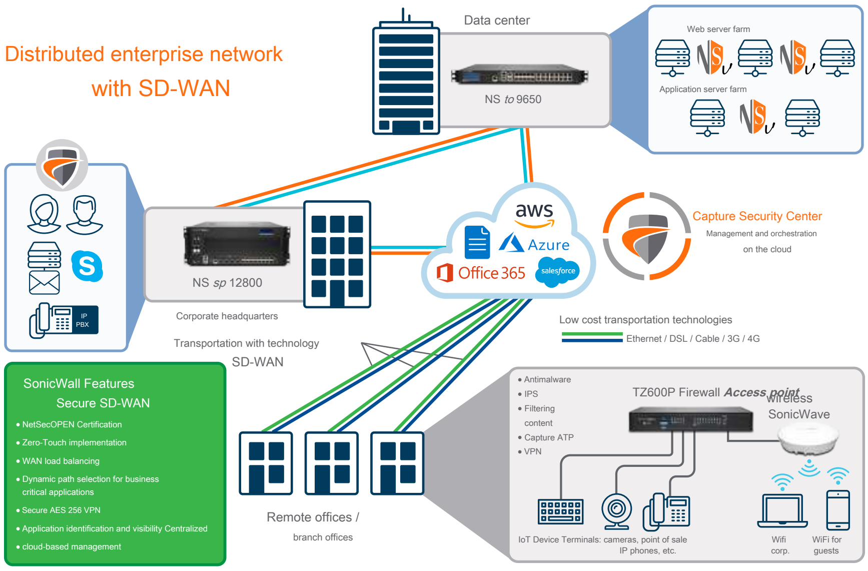
Centralized reporting and management

For highly who want to coordinate security, control, regulatory compliance, and their risk management strategy, SonicWall provides administrators with a unified, secure, and extensible platform to manage firewalls, *access points* wireless devices and Dell N series and X series switches using a process auditable and correlated workflow. Enterprises can easily consolidate the management of security devices, reduce administrative and troubleshooting complexities, and control all operational aspects of the security infrastructure, such as centralized management and enforcement of policies, monitoring of events in real-time, user activities, application identification, flow and forensic analysis, compliance and audit reports, among other functions. Additionally, companies are meeting firewall change management requirements by automating workflow, providing the agility and confidence needed to implement firewall policies. appropriate at the appropriate time and in accordance with current regulations. Available locally as the SonicWall Global Management System and in the cloud as the Capture Security Center, SonicWall's management and reporting solutions provide a consistent way to manage network security through business processes and service levels. In this way they dramatically simplify the life cycle management of their security environments, compared to device-by-device management.

Distributed networks

Because of their flexibility, the TZ series firewalls are ideal for both distributed enterprises and single-site deployments. In distributed networks, such as those of organizations

Retailers, each site has its own TZ firewall, which often connects to the Internet through a local provider using a DSL, cable or 3G / 4G connection. In addition to Internet access, each firewall uses an Ethernet connection to transport packets between remote sites and headquarters. From the data center, Web services and SaaS applications, such as Office 365, Salesforce, etc., are made available. Using mesh VPN technology, IT administrators can create a “hub and spoke” configuration for the secure transport of data between all locations.


Distributed enterprise network with SD-WAN

Data center
NS *to* 9650
Web server farm
Application server farm
IP PBX
NS *sp* 12800
Corporate headquarters
aws
Azure
Office 365
salesforce
Capture Security Center
Management and orchestration on the cloud
Transportation with technology SD-WAN
Low cost transportation technologies
Ethernet / DSL / Cable / 3G / 4G
SonicWall Features
Secure SD-WAN
• NetSecOPEN Certification
• Zero-Touch implementation
• WAN load balancing
• Dynamic path selection for business critical applications
• Secure AES 256 VPN
• Application identification and visibility Centralized
• cloud-based management
Remote offices /
branch offices
• Antimalware
• IPS
• Filtering content
• Capture ATP
• VPN
TZ600P Firewall *Access point*
wireless
SonicWave
IoT Device Terminals: cameras, point of sale IP phones, etc.
Wifi corp.
WiFi for guests

SonicOS SD-WAN technology is a perfect complement to

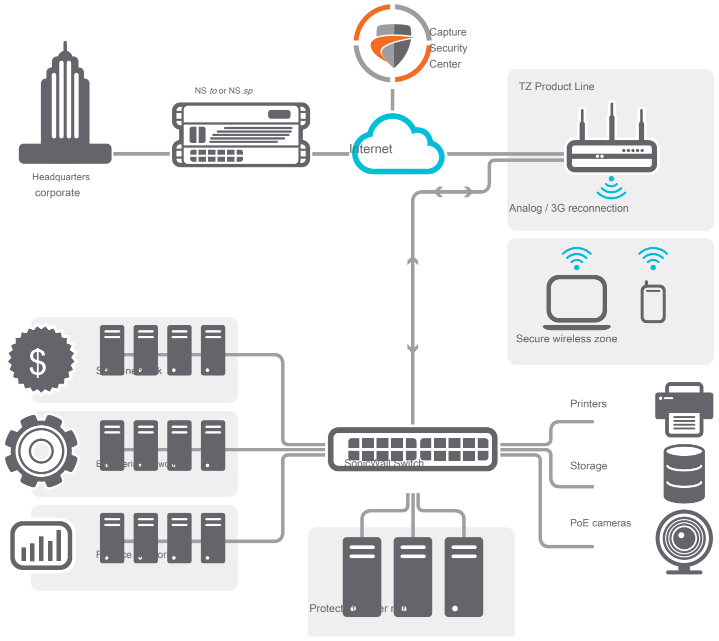
TZ firewalls deployed at remote sites and branch offices. Rather than relying on more expensive existing technologies such as MPLS

and T1, organizations that use

SD-WAN can choose cheaper public Internet services while still enjoying high application availability as well as predictable performance.

Capture Security Center

SonicWall's Capture Security Center (CSC) cloud-based security center acts as the nexus of the distributed network, centralizing the deployment, ongoing management, and real-time analysis of TZ firewalls. A key feature of the CSC is Zero-Touch Implementation. Setting up and deploying firewalls at multiple sites takes time and requires staff intervention *in situ.* Zero-Touch Deployment, however, eliminates these drawbacks by simplifying and speeding up the installation and provisioning of SonicWall firewalls remotely via the cloud. Similarly, CSC simplifies ongoing management by allowing SonicWall devices on the network to be managed through the cloud and from a single console. So that you can have a complete understanding of the state of the network security environment, SonicWall Analytics gives you a centralized view of all the activity that takes place on the network. In this way, organizations gain a deeper understanding of application usage and performance, while curbing shadow computing.

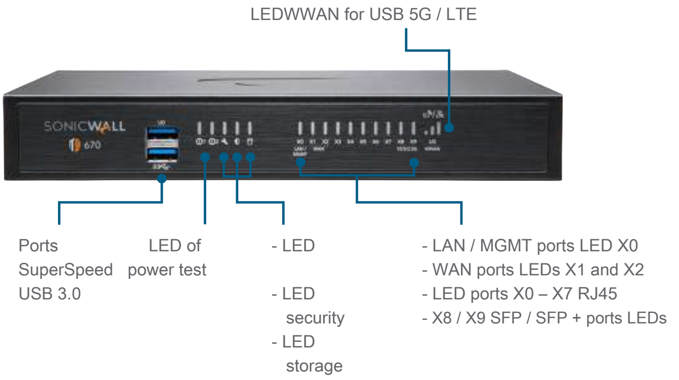


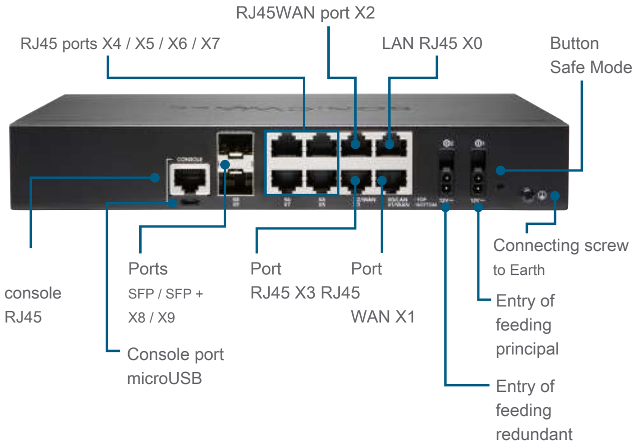
SonicWall Network Security Manager (NSM), part of CSC, is a centralized multi-tenant firewall manager that allows you to centrally manage all firewall operations without errors following auditable workflows. Its native analytical engine provides visibility in a single pane and allows you to monitor and detect threats

unifying and correlating records across all firewalls. NSM also helps you to be compliant at all times by providing a complete audit trail of every configuration change and detailed reports. NSM adapts to the management networks of organizations of all sizes with up to thousands of firewall appliances deployed in many locations.

SonicWall TZ670 Series

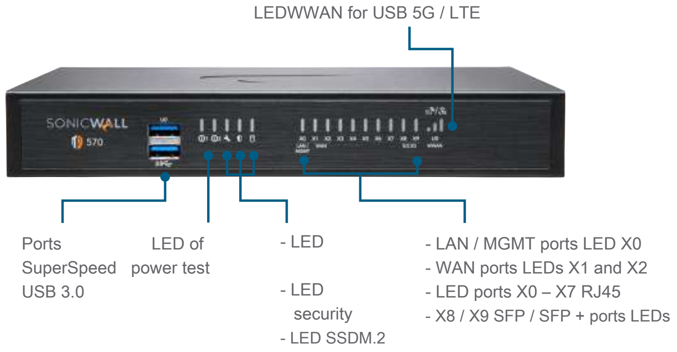
Designed for midsize organizations and distributed enterprises with SD-Branch sites, the TZ670 series provides robust industry-validated security with the best price-performance ratio in its class.

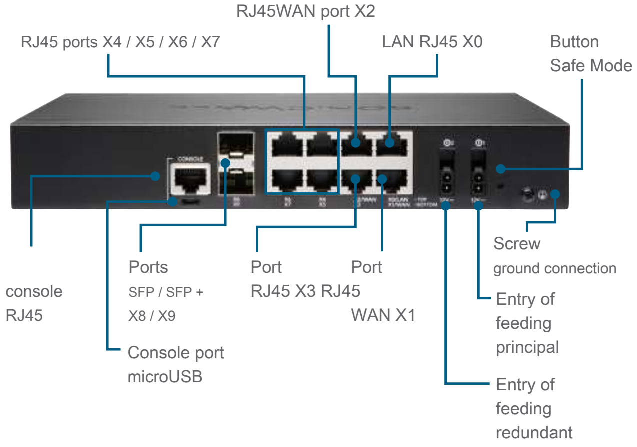




SonicWall TZ570 Series

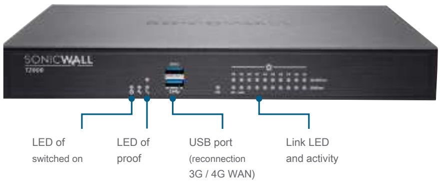
Designed for small to medium-sized organizations and distributed enterprises with SD-Branch sites, the TZ570 series provides robust industry-validated security at the best price-performance ratio in its class.

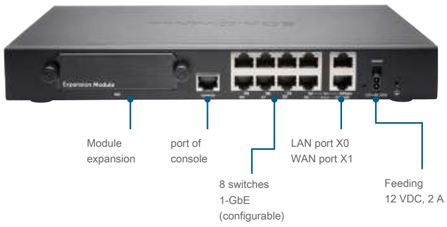


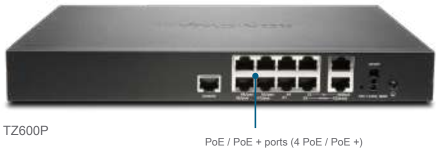


SonicWall TZ600 Series

For start-ups, retailers and branch offices that need security, performance and options like PoE + 802.3at with good value for money, the SonicWall TZ600 protects networks with enterprise-class features and unquestionable performance.

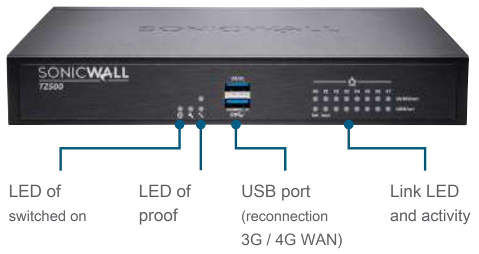


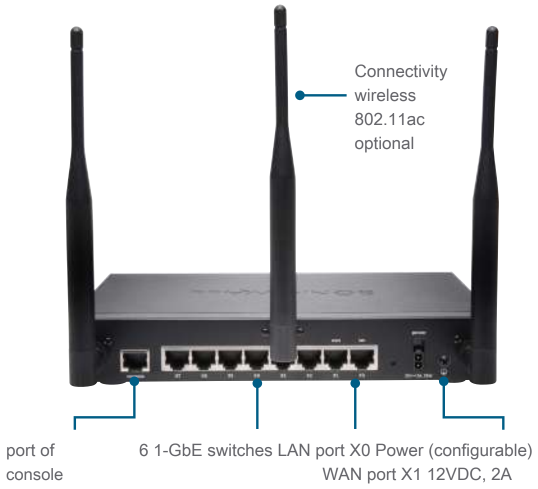




SonicWall TZ500 Series

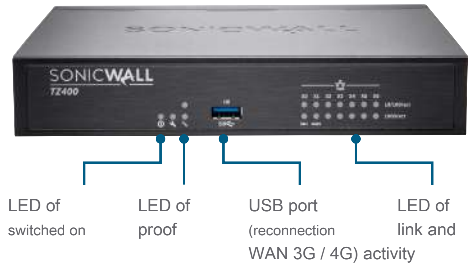
For growing SMBs and branch offices, the SonicWall TZ500 series provides highly effective and unbreakable protection with network productivity and optional integrated dual-band 802.11ac wireless connection.

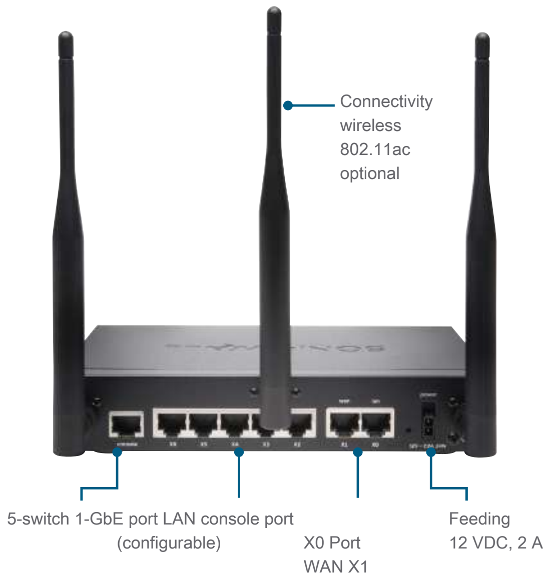




SonicWall TZ400 Series

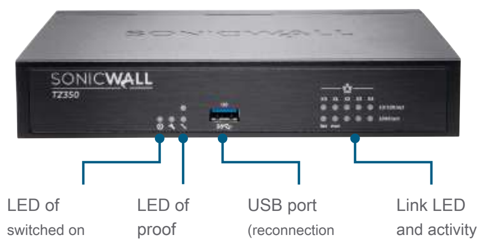
The SonicWall TZ400 series provides enterprise-class protection for small businesses, retail and branch offices. Flexible wireless deployment available with optional dual-band 802.11ac wireless connectivity built into the firewall.

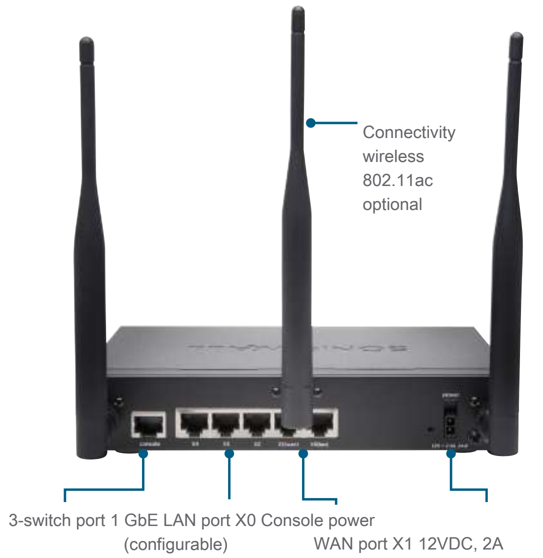




SonicWall TZ350 / TZ300 Series

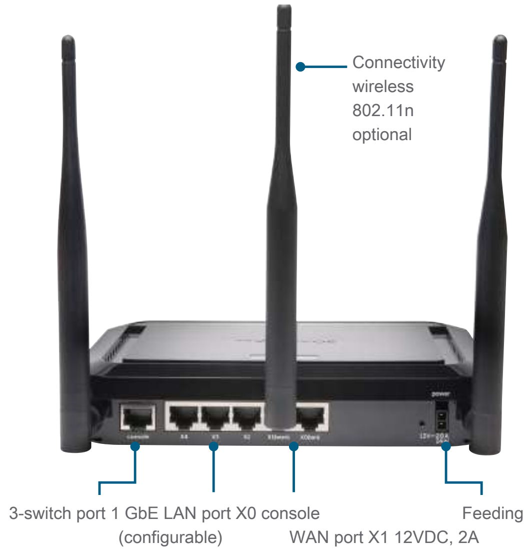
The SonicWall TZ300 and TZ350 series provide a comprehensive solution that protects networks against advanced attacks. Unlike consumer products, these UTM firewalls combine high-speed intrusion prevention, antimalware, and content / URL filtering, plus broad support for secure mobile access for laptops, smartphones, and tablets, along with technology optional integrated wireless 802.11ac. Additionally, the TZ300 series offers the option of 802.3at PoE + to power PoE devices.

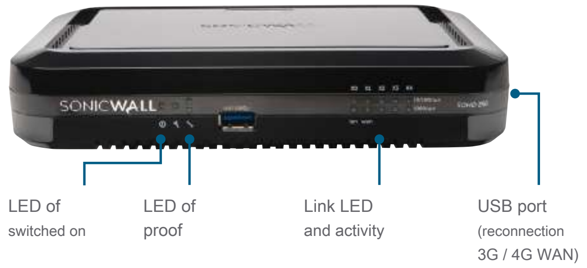




SonicWall SOHO 250 / SOHO Series

For wired and wireless environments in small home office environments, the SOHO 250 and SOHO series provide the same business-grade protection that large enterprises require at a much more affordable price. Add optional 802.11n wireless connectivity to provide employees, customers, and guests with secure wireless connectivity.





Services enabled by *partners*

Need help planning, deploying, or optimizing your SonicWall solution? The *partners* SonicWall Advanced Services are trained to provide you with first-class professional services. Learn more at www.sonicwall.com/PES.

Overview of SonicOS 7.0 Features

Firewall

- Dynamic packet inspection
- Deep packet inspection without reassembly
- Protection against DDoS attacks (UDP / ICMP / SYN floods)
- Support for IPv4 / IPv6
- Biometric authentication for remote access
- DNS proxy
- Full API compatibility
- Integration of *switch* by SonicWall
- SD-WAN scalability
- SD-WAN usability wizard [1]
- Containerization of SonicCoreX and SonicOS [1]
- Scalability of connections (SPI, DPI, DPI SSL)

Improved dashboard [1]

- Improved view of devices
- Summary of traffic and main users
- Threat information
- Notification center

Decryption and TLS / SSL / SSH inspection

- TLS 1.3 with enhanced security [1]
- Deep packet inspection for TLS / SSL / SSH
- Include / exclude objects, groups, or host names
- SSL control
- Improvements for DPI-SSL with CFS
- Granular SSL DPI controls by zone or standard

Capture Advanced Threat Protection [2]

- Real-time deep memory inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Analysis of a wide variety of file types
- Automatic and manual delivery
- Real-time threat intelligence updates
- Lock until there is a verdict
- Capture Client

Intrusion prevention [2]

- Analysis based on definitions
- Automatic updates of definitions
- Bidirectional inspection
- Capability for detailed IPS rules
- Application of GeoIP policies
- Filtering botnets with dynamic list
- Regular expression matching

Antimalware [2]

- Analysis of *malware* flow-based
- Gateway antivirus
- Antispyware gateway
- Bidirectional inspection
- Unlimited file size
- Database of *malware* on the cloud

Application identification [2]

- Application control
- Application bandwidth management
- Create custom application definitions
- Data leak prevention
- Application reports using NetFlow / IPFIX
- Comprehensive database of application definitions

Traffic visualization and analysis

- User activity
- Applications / bandwidth / threats
- Cloud-based analytics

HTTP / HTTPS2 web content filtering

- URL filtering
- Proxy bridging
- Keyword blocking
- Policy-based filtering (exclusion / inclusion)
- HTTP header insert
- Bandwidth management according to CFS classification categories
- Unified policy model with application control
- Content Filtering Client

VPN

- Secure SD-WAN
- VPN with automatic provisioning
- IPSec VPN for inter-site connectivity
- Remote access via SSL VPN and IPSec client
- *Gateway* Redundant VPN
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android, and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Networking

- PortShield
- Jumbo structures
- Discovery of MTU routes
- Improved protocolization
- VLAN trunk
- Port mirroring (NS *to* 2650 and above)
- QoS level 2
- 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 synchronization
- Inbound / outbound load balancing
- High Availability - Active / Standby with status synchronization
- L2 bridge, Wire / Virtual Wire mode, TAP mode, NAT mode
- Asymmetric routing
- Common Access Card (CAC) compatibility

Voip

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

Management, monitoring and compatibility

- Support for Capture Security Appliance (CS *to)*
- Capture Threat Assessment (CTA) v2.0
  - New design or template
  - Comparison of global and sector average
- New UI / UX, intuitive layout of functions [1]
  - Control Panel
  - Device, application, threat information
  - Topology view
  - Simplified policy creation and management
- Policy / object usage statistics [1]
  - Used vs. Not used
  - Active vs. Inactive
- Global statistical data search
- Storage assistance [1]
- External and external storage management [1]
- Compatible with USBWWAN cards (5G / LTE / 4G / 3G)
- Compatible with Network Security Manager (NSM)
- Web GUI
- Command line interface (CLI)
- Registration and provisioning *Zero-Touch*
- Simple CSC reporting [1]
- Compatible with the SonicExpress mobile app
- SNMPv2 / v3
- Centralized management and reporting with SonicWall Global Management System (GMS) [2]
- Protocolization
- NetFlow / IPFIX exports
- Cloud-based configuration backup
- BlueCoat Security Analysis Platform
- Viewing applications and bandwidth
- IPv4 and IPv6 management
- CD management screen
- Management of Dell N and Dell X series switches including cascaded switches

Debugging and diagnostics

- Improved packet monitoring
- SSH terminal in the user interface

Wireless connection

- AP SonicWave Cloud Management
- WIDS / WIPS
- Prevention of *access points* Not allowed
- Fast roaming (802.11k / r / v)
- 802.11s mesh networks
- Automatic channel selection
- RF spectrum analysis
- Plan view
- Topology view
- *Band steering (* band addressing)
- *Beamforming (* beam shaping)
- AirTime Fairness (connection fairness)
- Bluetooth low energy
- MiFi Extender
- RF enhancements
- Temporary access for guest users

Integrated wireless models

- 802.11ac Wave 2 Wireless Connectivity (TZ570W)
- Dual band (2.4 GHz and 5.0 GHz)
- Wireless standards 802.11 a / b / g / n / ac
- Wireless intrusion detection and prevention
- Wireless services for guest users
- Lightweight messaging at connection points
- Segmentation through *access points* virtual
- Captive portal
- ACL for the cloud

[1] *New feature available in SonicOS 7.0*

[2] *Requires additional subscription*

SonicWall TZ Series System Specifications: SOHO, SOHO 250, TZ300, and TZ350

GENERAL FIREWALL	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
OS	SonicOS			
Interfaces	5x1GbE, 1 USB, 1 Console		5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console
Supports Power over Ethernet (PoE)	-	-	TZ300P - 2 ports (2 PoE or 1 PoE +)	-
Expansion	USB			
Management	CLI, SSH, IUWeb, Capture Security Center, GMS, REST APIs 250			
Single sign-on (SSO) users VLAN interfaces		350	500	500
	25			
Access points admitted (maximum)	2	4	8	8
FIREWALL / VPN PERFORMANCE	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Firewall inspection performance[1]	300 Mbps	600 Mbps	750 Mbps	1.0 Gbps
Threat prevention performance[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Application inspection performance[2]	-	275 Mbps	375 Mbps	600 Mbps
IPS performance[2]	200 Mbps	250 Mbps	300 Mbps	400 Mbps
Antimalware inspection performance[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
TLS / SSL decryption and inspection performance (DPI SSL)[2]	30 Mbps	50 Mbps	60 Mbps	65 Mbps
IPSec VPN performance[3]	150 Mbps	200 Mbps	300 Mbps	430 Mbps
Connections per second	1,800	3,000	5,000	6,000
Maximum number of connections (SPI) Maximum	10,000	50,000	100,000	100,000
number of connections (DPI) Maximum number of	10,000	50,000	90,000	90,000
connections (DPI SSL)	250	25,000	25,000	25,000
VPN	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
VPN tunnels between sites IPSec VPN	10	10	10	fifteen
clients (maximum) SSL VPN licenses	fifteen)	fifteen)	1 (10)	2 (10)
(maximum)	1 (10)	1 (25)	1 (50)	1 (75)
Virtual Assist included (maximum)	-	1 (proof of 30 days)	1 (proof of 30 days)	1 (proof of 30 days)
Encryption / authentication	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, Crypto Suite B			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Routing-based VPN	RIP, OSPF, BGP4			
VPN features	Dead Peer Detection, DHCP over VPN, IPSec NAT Traversal, Redundant VPN gateway, routing-based VPN			
Supported Global VPN Client Platforms NetExtender	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			
	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	Manzana® 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, content and keyword analysis, comprehensive filtering based on file types such as ActiveX, Java, cookies for privacy, allow / deny lists			
Comprehensive antispam service	Compatible			
Viewing applications	No	Yes	Yes	Yes
App control	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes
NETWORKS	**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, maximum bandwidth, bandwidth guaranteed, DSCP marking, 802.1e (WMM)			

SonicWall TZ Series System Specifications: SOHO, SOHO 250, TZ300, and TZ350 (continued)

NETWORKS, CONTINUED	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 VoIP user database	150			
	H.323 v1-5 full, SIP			
Standards	TCP / IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP / IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications5	FIPS 140-2 (with Suite B) level 2, UC APL, VPNC, IPv6 (phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (firewall and IPS)			
Common Access Card (CAC) High availability	Compatible			
	No		Active / Standby	
HARDWARE	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Form factor	Desktop			
Power supply	24 W (external)		24 W (external) 65 W (external, only TZ300P)	24 W (external)
Maximum power consumption (W) Input	6.4 / 11.3	6.9 / 11.3	6.9 / 12.0	6.9 / 12.0
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 inches		3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 inch	3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 inch
Weight	0.34kg / 0.75lbs 0.48kg / 1.06lbs		0.73kg / 1.61lbs 0.84kg / 1.85lbs	0.73kg / 1.61lbs 0.84kg / 1.85lbs
WEEE weight	0.80 kg / 1.76 pounds 0.94kg / 2.07lbs		1.15 kg / 2.53 pounds 1.26kg / 2.78lbs	1.15 kg / 2.53 pounds 1.26kg / 2.78lbs
Shipping weight	1.20 kg / 2.64 pounds 1.34kg / 2.95lbs		1.37 kg / 3.02 pounds 1.48 kg / 3.26 pounds	1.37 kg / 3.02 pounds 1.48 kg / 3.26 pounds
MTBF (in years)	58.9 / 56.1 (wireless)	56.1	56.1	56.1
Environment (Operational / Storage)	0-40 ° C (32-105 ° F) / - 40 to 70 ° C (-40 to 158 ° F)			
Humidity	5-95%, non-condensing			
REGULATIONS	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Standards Compliance (Cable Models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV / GS, CB, Certificate of Compliance for Mexico 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, Certificate of Compliance for Mexico by UL, WEEE, REACH, KCC / MSIP, ANATEL	
Compliance with major regulations (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, Certificate of Compliance for Mexico 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, Certificate of Compliance for Mexico by UL, WEEE, REACH	
INTEGRATED WIRELESS CONNECTION	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: SOHO, SOHO 250, TZ300, and TZ350 (continued)

INTEGRATED WIRELESS CONNECTION	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Operational channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b / g: USA 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: USA 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): USA 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 Transmit Power Control	It is based on the regulatory scope specified by the system administrator			
Supported Transfer Rates	Compatible			
	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) / Spread Spectrum Direct Sequence (DSSS) 802.11n: Frequency Division Multiplexing orthogonal (OFDM)		802.11a: Orthogonal Frequency Division Multiplexing (OFDM) 802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM) / Spread Spectrum Direct Sequence (DSSS) 802.11n: Frequency Division Multiplexing Orthogonal (OFDM) 802.11ac: Frequency division multiplexing orthogonal (OFDM)	

** Future use.*

[1] *Test methods: 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 performance measured using the standard Spirent WebAvalanche HTTP performance test and Ixia testing tools. Multiple streams through multiple pairs of ports have been used for testing. Threat Prevention performance measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled.*

[3] *VPN performance measurement using UDP traffic with 1280-byte packets in accordance with RFC 2544. Specifications, capabilities, and availability are subject to change.*

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

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

[6] *All built-in wireless TZ models can support 2.4GHz or 5GHz bands. For dual band support, use the products from access points SonicWall wireless*

SonicWall TZ Series System Specifications: TZ400, TZ500, and TZ600

GENERAL FIREWALL	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
OS	SonicOS		
Interfaces	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 expansion slot
Supports Power over Ethernet (PoE)	-	-	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 500 APIs		
Single sign-on (SSO) users VLAN interfaces		500	500
	fifty	fifty	fifty
Access points admitted (maximum)	16	16	24
FIREWALL / VPN PERFORMANCE	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Firewall inspection performance[1]	1.3 Gbps	1.4 Gbps	1.9 Gbps
Threat prevention performance[2]	600 Mbps	700 Mbps	800 Mbps
Application inspection performance[2]	1.2 Gbps	1.3 Gbps	1.8 Gbps
IPS performance[2]	900 Mbps	1.0 Gbps	1.2 Gbps
Antimalware inspection performance[2]	600 Mbps	700 Mbps	800 Mbps
TLS / SSL decryption and inspection performance (DPI SSL)[2]	180 Mbps	225 Mbps	300 Mbps
IPSec VPN performance[3]	900 Mbps	1.0 Gbps	1.1 Gbps
Connections per second	6,000	8,000	12,000
Maximum number of connections (SPI) Maximum	150,000	150,000	150,000
number of connections (DPI) Maximum number of	125,000	125,000	125,000
connections (DPI SSL)	25,000	25,000	25,000
VPN	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
VPN tunnels between sites IPSec VPN	twenty	25	fifty
clients (maximum) SSL VPN licenses	2 (25)	2 (25)	2 (25)
(maximum) Virtual Assist included	2 (100)	2 (150)	2 (200)
(maximum) Encryption / authentication	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, Crypto Suite B		
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v		
Routing-based VPN	RIP, OSPF, BGP		
VPN features	Dead Peer Detection, DHCP over VPN, IPSec NAT Traversal, Redundant VPN gateway, routing-based VPN		
Supported Global VPN Client Platforms	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	Manzana® 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, content and keyword analysis, extensive filtering based on file types such as ActiveX, Java, cookies for privacy, allow / deny lists		
Comprehensive antispam service	Compatible		
Viewing applications	Yes	Yes	Yes
App control	Yes	Yes	Yes
Capture Advanced Threat Protection	Yes	Yes	Yes
NETWORKS	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
IP address assignment NAT modes	Static, (DHCP, PPPoE, L2TP and PPTP client), internal DHCP server, DHCP relay		
	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, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)		

SonicWall TZ Series System Specifications: TZ400, TZ500, and TZ600 (continued)

NETWORKS	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 VoIP user database	150	250	
	H.323 v1-5 full, 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, Common Criteria NDPP (firewall and IPS)		
Common Access Card (CAC)	Compatible		
High availability	Active / Standby	Active / Standby with status sync	
HARDWARE	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Form factor	Desktop		
Power supply	24 W (external)	36W (external)	60W (external) 180W (external) (TZ600P only)
Maximum power consumption (W) Input	9.2 / 13.8	13.4 / 17.7	16.1
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 inches	3.5 x 15 x 22.5 cm 1.38 x 5.91 x 8.86 inch	3.5 x 18 x 28 cm 1.38 x 7.09 x 11.02 inches
Weight	0.73kg / 1.61lbs 0.84kg / 1.85lbs	0.92kg / 2.03lbs 1.05kg / 2.31lbs	1.47 kg / 3.24 pounds
WEEE weight	1.15 kg / 2.53 pounds 1.26kg / 2.78lbs	1.34kg / 2.95lbs 1.48 kg / 3.26 pounds	1.89 kg / 4.16 pounds
Shipping weight	1.37 kg / 3.02 pounds 1.48 kg / 3.26 pounds	1.93kg / 4.25lbs 2.07 kg / 4.56 pounds	2.48kg / 5.47lbs
MTBF (in years)	54.0	40.8	18.4
Environment (Operational / Storage)	0-40 ° C (32-105 ° F) / - 40 to 70 ° C (-40 to 158 ° F)		
Humidity	5-95%, non-condensing		
REGULATIONS	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Compliance with the main regulations (cable models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV / GS, CB, Certificate of Compliance for Mexico 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, Certificate of Compliance for Mexico 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, Certificate of Compliance for Mexico by UL, WEEE, REACH, KCC / MSIP
Compliance with major regulations (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, certificate of compliance for Mexico 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, certificate of compliance for Mexico by UL, WEEE, REACH	-

SonicWall TZ Series System Specifications: TZ400, TZ500, and TZ600 (continued)

INTEGRATED WIRELESS CONNECTION	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		-
Operational 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): USA 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		-
Transmission output power	It is based on the specified regulatory scope by the system administrator		-
Transmission power control Supported transfer	Compatible		-
rates	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: Division Multiplexing Orthogonal Frequency Frequency (OFDM) 802.11ac: Division Multiplexing orthogonal frequencies (OFDM)		-

SonicWall TZ Series System Specifications: TZ500 and TZ670

GENERAL FIREWALL	TZ570 SERIES	TZ670 SERIES
OS	SonicOS 7.0	
Interfaces	8x1GbE, 2x5GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Console
Supports Power over Ethernet (PoE)	TZ570P (5 PoE or 3PoE +)	-
Expansion	Storage expansion slot (up to 256 GB)	Storage expansion slot (up to 256 GB) (32 GB included)
Management	Network Security Manager, CLI, SSH, IUWeb, GMS, REST APIs	
Single sign-on (SSO) users VLAN interfaces	2,500	2,500
	256	256
Access points admitted (maximum)	32	32
FIREWALL / VPN PERFORMANCE	TZ570 SERIES	TZ670 SERIES
Firewall inspection performance[1]	4.00 Gbps	5.00 Gbps
Threat prevention performance[2]	2.00 Gbps	2.50 Gbps
Application inspection performance[2]	2.5 Gbps	3.0 Gbps
IPS performance[2]	2.5 Gbps	3.0 Gbps
Antimalware inspection performance[2]	2.00 Gbps	2.50 Gbps
TLS / SSL decryption and inspection performance (DPI SSL)[2]	750 Mbps	800 Mbps
IPSec VPN performance[3]	1.80 Gbps	2.10 Gbps
Connections per second	16,000	25,000
Maximum number of connections (SPI) Maximum	1,250,000	1,500,000
number of connections (DPI) Maximum number of	400,000	500,000
connections (DPI SSL)	30,000	30,000
VPN	TZ570 SERIES	TZ670 SERIES
VPN tunnels between sites IPSec VPN	200	250
clients (maximum) SSL VPN licenses	10 (500)	10 (500)
(maximum) Encryption / authentication	2 (200)	2 (250)
	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, Crypto Suite B	
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v	
Routing-based VPN	RIP, OSPF, BGP	
VPN features	Dead Peer Detection, DHCP over VPN, IPSec NAT Traversal, redundant VPN gateway, routing-based VPN	
Supported Global VPN Client Platforms NetExtender	Microsoft® Windows 10	
	Microsoft® Windows 10, Linux	
Mobile Connect	Manzana® 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, content and keyword analysis, full filtering based on file types such as ActiveX, Java, cookies for privacy, allow / deny lists	
Comprehensive antispam service	Yes	
Viewing applications	Yes	
App control	Yes	
Capture Advanced Threat Protection DNS	Yes	
Security	Yes	

SonicWall TZ Series System Specifications: TZ500 and TZ670 (continued)

NETWORKS	TZ570 SERIES	TZ670 SERIES
IP address assignment NAT modes	Static, (DHCP, PPPoE, L2TP and PPTP client), internal DHCP server, DHCP relay	
	1: 1, 1: many, many: 1, many: many, Flexible NAT (overlapping IPs), PAT, transparent mode	
Routing protocols	BGP4, OSPF, RIPv1 / v2, static routes, policy-based routing	
QoS	Bandwidth priority, maximum 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 VoIP user database	250	
	H.323 v1-5 full, 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 Antivirus, 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) Input	13.1	13.1
voltage and frequency Total heat	100-240 VAC, 50-60 Hz,	100-240 VAC, 50-60 Hz,
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 inches	3.5 x 15 x 22.5 (cm) 1.38 x 5.91 x 8.85 inches
Weight	0.97kg / 2.14lbs	0.97kg / 2.14lbs
WEEE weight	1.42kg / 3.13lbs	1.42kg / 3.13lbs
Shipping weight	1.93kg / 4.25lbs	1.93kg / 4.25lbs
MTBF at 25 ºC in years	26.1	43.9
Environment (Operational / Storage)	0-40 ° C (32-105 ° F) / - 40 to 70 ° C (-40 to 158 ° F)	
Humidity	5-95%, non-condensing	
REGULATIONS	TZ570 SERIES	TZ670 SERIES
Compliance with major regulations (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, DGN notification for Mexico by UL, WEEE, REACH, BSMI , KCC / MSIP, ANATEL	FCC Class B, FCC, ICES Class B, CE (EMC, LVD, CB, RoHS), C-Tick, VCCI Class B, UL / cUL, TUV / GS, WEEE, DGN notification for Mexico by UL, REACH, BSMI, KCC / MSIP, ANATEL
Compliance with Major Regulations (Wired 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, DGN notification for Mexico by UL, WEEE, REACH, BSMI, NCC (TW) KCC / MSIP, SRRC, ANATEL	-
Compliance with major regulations (PoE models: TZ570P)	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL / cUL, TUV / GS, CB, DGN notification for Mexico by UL, WEEE, REACH, BSMI, KCC / MSIP, ANATEL	-

SonicWall TZ Series System Specifications: TZ500 and TZ670 (continued)

INTEGRATED WIRELESS CONNECTION	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	-
Operational 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); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): USA 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	-
Transmission output power Transmission	It is based on the specified regulatory scope by the system administrator	-
power control	Compatible	-
Supported transfer speeds	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: 802.11ac Orthogonal Frequency Division Multiplexing (OFDM): Orthogonal Frequency Division Multiplexing (OFDM)	-

[1] *Test methods: 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 performance measured using the standard Spirent WebAvalanche HTTP performance test and Ixia testing tools. Multiple streams through multiple pairs of ports have been used for testing. Threat Prevention performance measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled.*

[3] *VPN performance measurement using UDP traffic with 1280-byte packets in accordance with RFC 2544. Specifications, capabilities, and availability are subject to change.*

[4] *A separate rack mount kit is available.*

[5] *All built-in wireless TZ models can support 2.4GHz or 5GHz bands. For dual band support, use SonicWall 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 of TotalSecure Advanced Edition TZ300 with 1 year of	02-SSC-1824
TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC with 1 year of TotalSecure Advanced Edition TZ300P with 1 year	01-SSC-1703
of TotalSecure Advanced Edition TZ350 with 1 year of TotalSecure Advanced Edition	02-SSC-0602
	02-SSC-1843
TZ350 Wireless-AC with 1 year of TotalSecure Advanced Edition TZ400 with 1 year of	02-SSC-1851
TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC with 1 year of TotalSecure Advanced Edition TZ500 with 1 year of	01-SSC-1706
TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC with 1 year of TotalSecure Advanced Edition TZ570 with 1 year of	01-SSC-1709
TotalSecure Essential Edition	02-SSC-5651
TZ570W with 1 year of TotalSecure Essential Edition TZ570P with 1	02-SSC-5649
year of TotalSecure Essential Edition TZ600 with 1 year of	02-SSC-5653
TotalSecure Advanced Edition TZ600P with 1 year of TotalSecure	01-SSC-1711
Advanced Edition TZ670 with 1 year of TotalSecure Essential Edition	02-SSC-0600
	02-SSC-5640
High availability options (all drives must be the same model)	
TZ500 with high availability TZ570 with	01-SSC-0439
high availability TZ570P with high	02-SSC-5694
availability TZ600 with high availability	02-SSC-5655
TZ670 with high availability	01-SSC-0220
	02-SSC-5654

Services	SKU
For SonicWall SOHO 250 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention and 24x7 support (1 year) Capture Advanced Threat	02-SSC-1726
Protection for SOHO 250 (1 year)	02-SSC-1732
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-1750
	02-SSC-1744
Comprehensive antispam service (1 year) 24x7	02-SSC-1823
support (1 year)	02-SSC-1720
For SonicWall TZ300 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention and 24x7 Support (1 year) Capture Advanced Threat	01-SSC-1430
Protection for TZ300 (1 year)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	01-SSC-0602
	01-SSC-0608
Comprehensive antispam service (1 year) 24x7	01-SSC-0632
support (1 year)	01-SSC-0620
For SonicWall TZ350 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention and 24x7 Support (1 year) Capture Advanced Threat	02-SSC-1773
Protection for TZ350 (1 year)	02-SSC-1779
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-1797
	02-SSC-1791
Comprehensive antispam service (1 year) 24x7	02-SSC-1809
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) Capture Advanced Threat	01-SSC-1440
Protection for TZ400 (1 year)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	01-SSC-0534
	01-SSC-0540
Comprehensive antispam service (1 year) 24x7	01-SSC-0561
support (1 year)	01-SSC-0552
For SonicWall TZ500 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention and 24x7 Support (1 year) Capture Advanced Threat	01-SSC-1450
Protection for TZ500 (1 year)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	01-SSC-0458
	01-SSC-0464
Comprehensive antispam service (1 year) 24x7	01-SSC-0482
support (1 year)	01-SSC-0476
For SonicWall TZ600 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention and 24x7 Support (1 year) Capture Advanced Threat	01-SSC-1460
Protection for TZ600 (1 year)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	01-SSC-0228
	01-SSC-0234
Comprehensive antispam service (1 year) 24x7	01-SSC-0252
support (1 year)	01-SSC-0246
For SonicWall TZ670 series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1 year) Capture Advanced Threat Protection for TZ670 (1	02-SSC-5053
year)	02-SSC-5035
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-5059
	02-SSC-5047
Comprehensive antispam service (1 year) 24x7	02-SSC-5041
support (1 year)	02-SSC-5029
For SonicWall TZ570 (TZ570) series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1 year) Capture Advanced Threat Protection for TZ570 (1	02-SSC-5137
year)	02-SSC-5083
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-5155
	02-SSC-5119
Comprehensive antispam service (1 year) 24x7	02-SSC-5101
support (1 year)	02-SSC-5065
For SonicWall TZ570 (TZ570W) series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support (1 year) Capture Advanced Threat Protection for TZ570W	02-SSC-5149
(1 year)	02-SSC-5095
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-5167
	02-SSC-5131
Comprehensive antispam service (1 year) 24x7	02-SSC-5113
support (1 year)	02-SSC-5077
For SonicWall TZ570 (TZ570P) series	
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering, Antispam and 24x7 Support (1 year) Capture Advanced Threat Protection for TZ570P	02-SSC-5143
(1 year)	02-SSC-5089
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering Service (1 year)	02-SSC-5161
	02-SSC-5125
Comprehensive antispam service (1 year) 24x7	02-SSC-5107
support (1 year)	02-SSC-5071

accessories	SKU
TZ670 / 570 Series	
Power supply for SonicWall TZ670 / 570 series, FRU Rack mount kit for	02-SSC-3078
SonicWall TZ670 / 570 series	02-SSC-3112
32 GB SonicWall storage module for TZ670 / 570 series 64 GB SonicWall storage module for	02-SSC-3114
TZ670 / 570 series 128 GB SonicWall storage module for TZ670 / 570 series 256 GB SonicWall	02-SSC-3115
storage module for TZ670 series / 570 SonicWall microUSB console cable for TZ670 / 570	02-SSC-3116
series	02-SSC-3117
	02-SSC-5173
TZ600 / 500/400/350/300 Series, SOHO 250	
Rack mount kit for SonicWall TZ600	01-SSC-0225
Power supply for SonicWall TZ600 series, FRU Rack mount kit for	01-SSC-0280
SonicWall TZ500 series Power supply for SonicWall TZ500 series, FRU	01-SSC-0438
Rack mount kit for SonicWall TZ400 series	01-SSC-0437
	01-SSC-0525
Rack Mount Kit for SonicWall TZ350, TZ300 Series	01-SSC-0742
Power supply for SonicWall TZ400, TZ350, TZ300, SOHO 250, SOHO, FRU series PoE power supply for SonicWall	01-SSC-0709
TZ300, FRU	02-SSC-0613
SonicWall SFP / SFP + modules	
10GB-SR SFP + short-range fiber module multi-mode without cable Long-range fiber	01-SSC-9785
module 10GB-LR SFP + single-mode without cable 1 m Twinax cable 10GB SFP + copper	01-SSC-9786
	01-SSC-9787
Twinax 10GB SFP + Copper Cable 3m	01-SSC-9788
1GB-SX SFP + short-haul fiber multimode wireless module 1GB-LX SFP + single-mode	01-SSC-9789
long-haul fiber module without cable 1GB-RJ45 SFP copper module without cable	01-SSC-9790
	01-SSC-9791
Sonicwall 10GBASE-T Copper SFP + Transceiver with RJ45 Module	02-SSC-1874

Official model numbers:

SOHO / SOHOWireless	APL31-0B9 / APL41-0BA
SOHO 250 / SOHO 250 Wireless TZ300 /	APL41-0D6 / APL41-0BA
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 offers Unlimited Cybersecurity for the age of hyper-distributed computing and a workplace reality where everyone uses mobile, remote and insecure technology. By knowing the unknown, as well as providing real-time visibility and facilitating a revolutionary economy, SonicWall bridges the business gap in cybersecurity for businesses, governments and SMEs around the world. 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 customers based on their experiences, by the number of reviews published in Gartner Peer Insights and by the global rankings of a given vendor in the market, as described in greater detail herein, and are not intended in any way to represent the views of Gartner or its affiliates.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 (United States)
You will find more information on our website.
www.sonicwall.com

SONICWALL®