SONICWALL

SonicWall TZ series (Gen 6)

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

The generation 6 (Gen 6) SonicWall TZ series enables small to mid-size organizations and distributed enterprises realize the benefits of an integrated security solution that checks all the boxes. Combining high-speed threat prevention and software-defined wide area networking (SD-WAN) technology with an extensive range of networking and wireless features plus simplified deployment and centralized management, the Gen 6 TZ series provides a unified security solution at a low total cost of ownership.

Flexible, integrated security solution

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

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

Superior threat prevention and performance

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

Benefits:

Flexible, integrated security solution

- Secure SD-WAN
- Powerful SonicOS operating system
- High-speed 802.11ac wireless
- Power over Ethernet (PoE/PoE+)
- Network segmentation with VLANs

Superior threat prevention and performance

- Patent-pending real-time deep memory inspection technology
- Patented reassembly-free deep packet inspection technology
- On-box and cloud-based threat prevention
- TLS/SSL decryption and inspection
- Industry-validated security effectiveness
- Dedicated Capture Labs threat research team
- Endpoint security with Capture Client

Easy deployment, setup and ongoing management

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

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

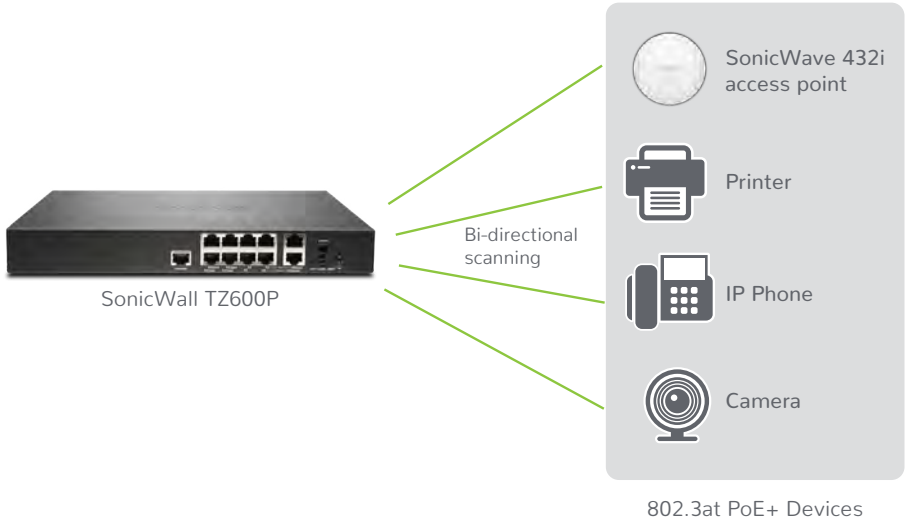
The continued growth in the use of encryption to secure web sessions means it is imperative firewalls are able to scan encrypted traffic for threats. TZ series firewalls provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port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

Easy deployment, setup and ongoing management

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

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

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



Integrated Security and Power for Your PoE-enabled Devices

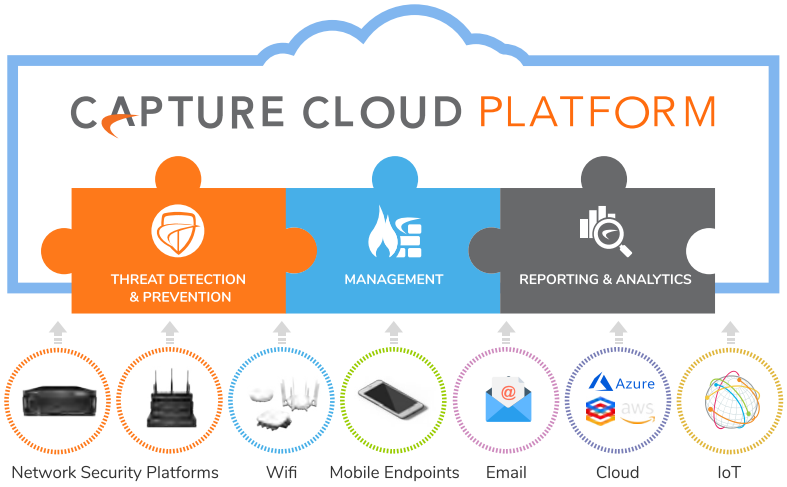
Provide power to your PoE-enabled devices without the cost and complexity of a Power over Ethernet switch or injector. TZ300P and TZ600P firewalls integrate IEEE 802.3at technology to power PoE and PoE+ devices such as wireless access points, cameras, IP phones and more. The firewall scans all traffic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

Capture Cloud Platform

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

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

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

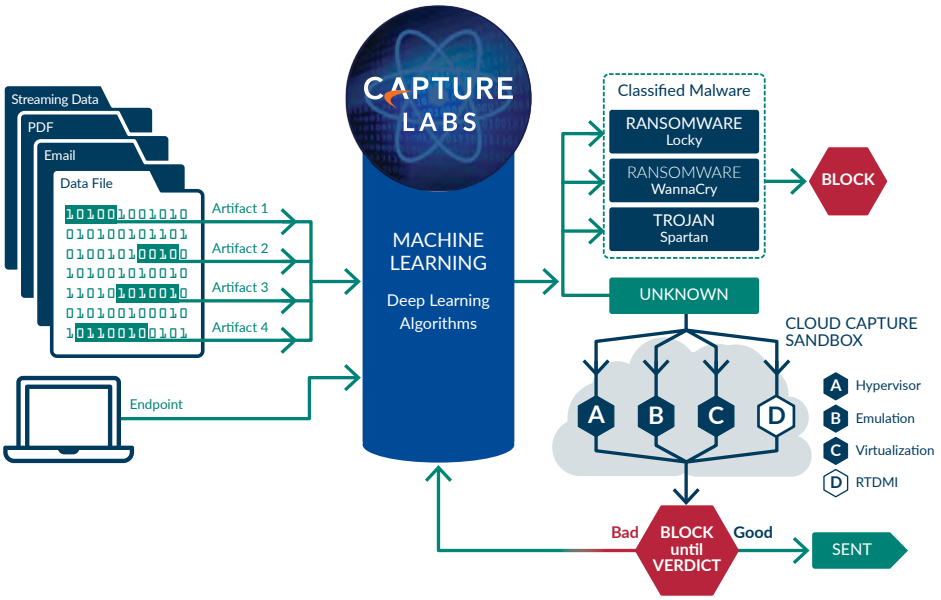


Advanced threat protection

At the center of SonicWall automated, real-time breach prevention is SonicWall Capture Advanced Threat Protection service, a cloud-based multi-engine sandbox that extends firewall threat protection to detect and prevent zero-day threats. Suspicious files are sent to the cloud where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined. The multi-engine sandbox platform, which includes Real-Time Deep Memory Inspection, virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior. When a file is identified as malicious, it is blocked and a hash is immediately created within Capture ATP. Soon after, a signature is sent to firewalls to prevent follow-on attacks.

The service analyzes a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

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



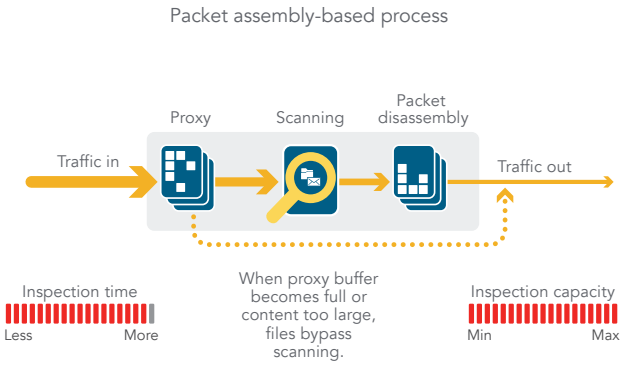
SONICWALL®

Reassembly-Free Deep Packet Inspection engine

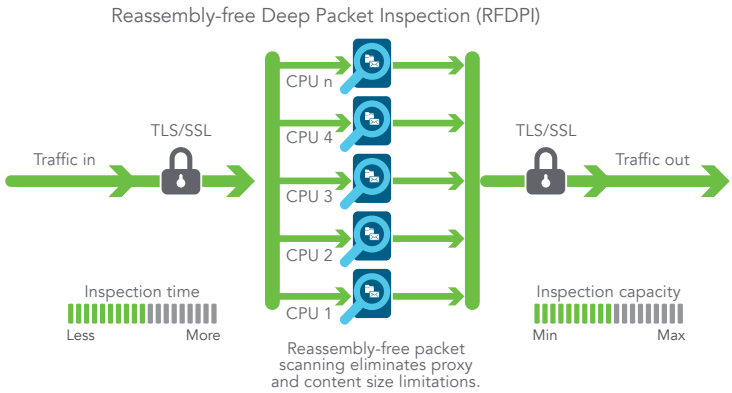
The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application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

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

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



Competitive proxy-based architecture



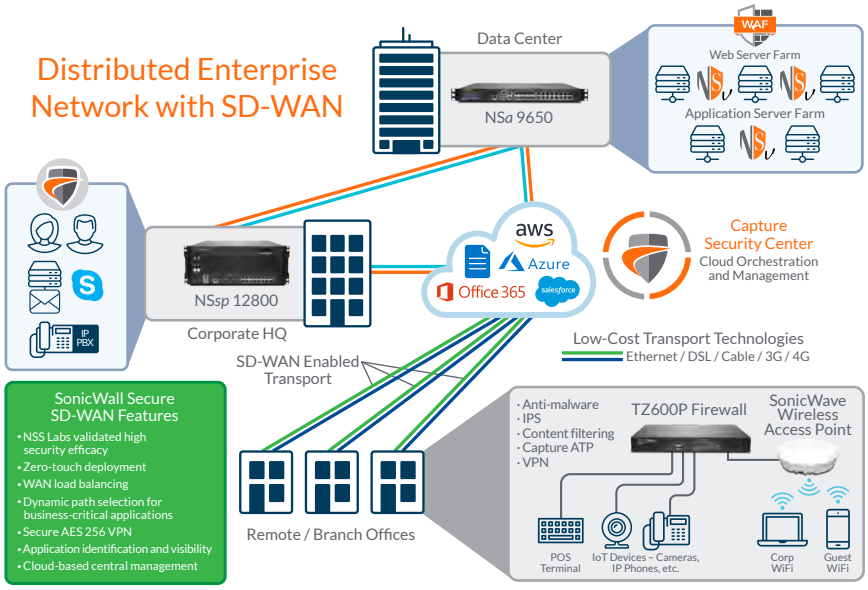
SonicWall stream-based architecture

Centralized management and reporting

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

Distributed networks

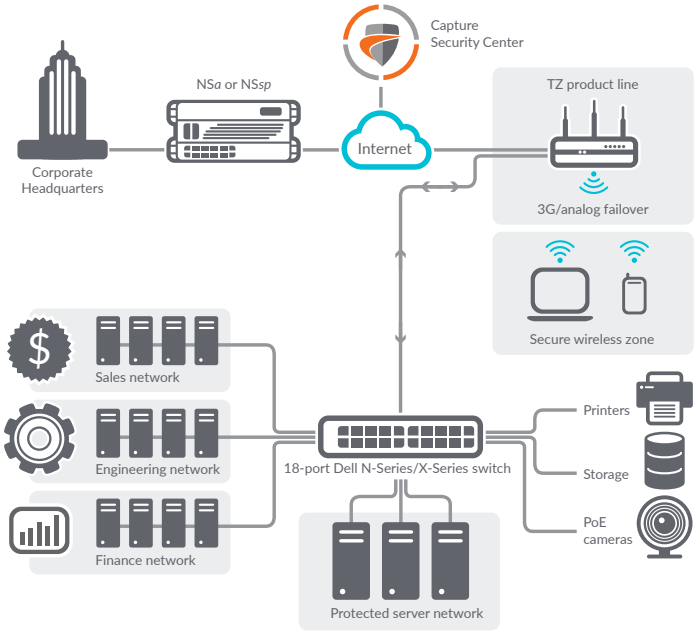
Because of their flexibility, TZ series firewalls are ideally suited for both distributed enterprise and single site deployments. In distributed networks like those found in retail organizations, each site has its own TZ firewall which connects to the Internet often through a local provider using a DSL,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



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

Capture Security Center

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



Single Sites

For single site deployments, having an integrated network security solution is highly beneficial. TZ series firewalls combine high security effectiveness with options such as built-in 802.11ac wireless and, in the case of the TZ300P and TZ600P, PoE/PoE+ support. The same security engine in our mid-range NSa series and high-end NSsp series is featured in TZ series firewall along with the broad feature set of SonicOS. Configuration and management is easy using the intuitive SonicOS UI. Organizations save valuable rack space due to the compact desktop form factor.

SonicWall TZ600 series

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

TZ600P

PoE/PoE+ ports (4 PoE/PoE+)

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

Expansion module | Console port | 8x1-GbE switch (configurable) | X0 LAN port X1 WAN port | 12V DC 2A power

SonicWall TZ500 series

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

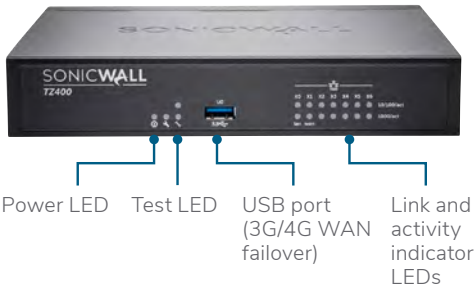
Optional 802.11ac wireless

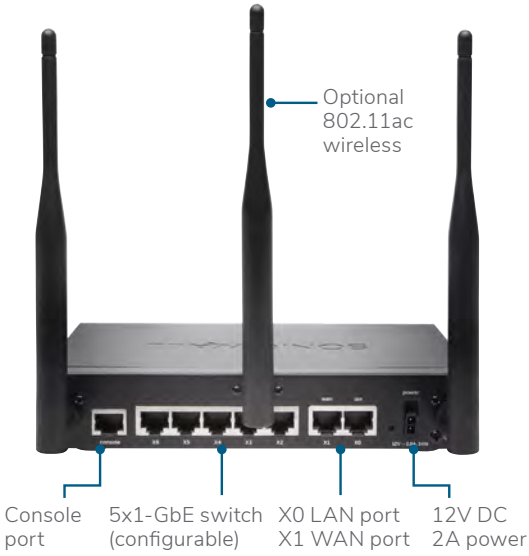
Power LED | Test LED | USB port (3G/4G WAN failover) | Link and activity indicator LEDs

Console port | 6x1-GbE switch (configurable) | X0 LAN port X1 WAN port | 12V DC 2A power

SonicWall TZ400 series

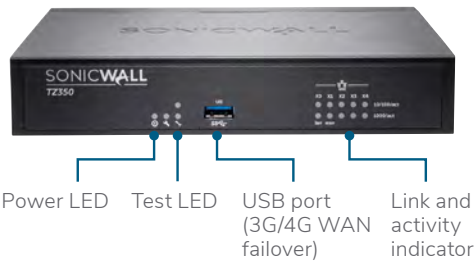
For small business, retail and branch office locations, the SonicWall TZ400 series delivers enterprise-grade protection. Flexible wireless deployment is available with optional 802.11ac dual-band wireless integrated into the firewall.

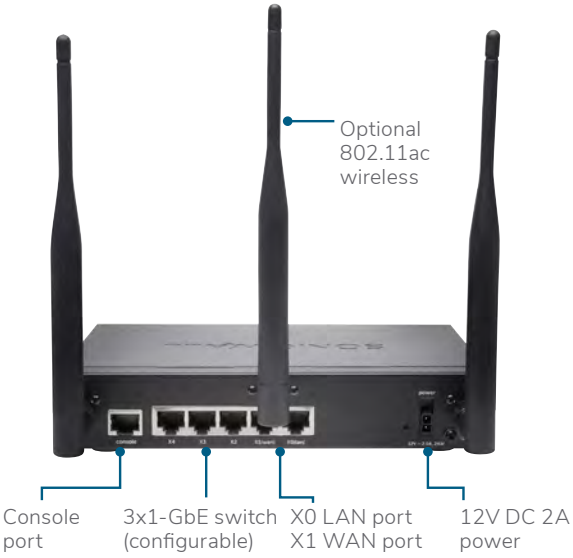




SonicWall TZ350/TZ300 series

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

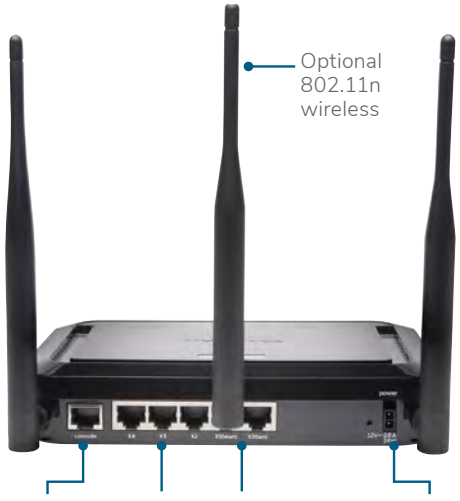




SonicWall SOHO 250/SOHO series

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

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



Partner Enabled Services

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

SonicOS feature summary

Firewall

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

SSL/SSH decryption and inspection[1]

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

Capture Advanced Threat Protection[1]

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

Intrusion prevention[1]

- Signature-based scanning
- Automatic signature updates
- Bidirectional inspection
- Granular IPS rule capability
- GeoIP/Botnet filtering[2]
- Regular expression matching

Anti-malware[1]

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

Application identification[1]

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

Traffic visualization and analytics

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

HTTP/HTTPS Web content filtering[1]

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

VPN

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

Networking

- Secure SD-WAN
- PortShield
- Enhanced logging
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- Asymmetric routing
- DHCP server
- NAT
- Bandwidth management
- High availability - Active/Standby with state sync[2]
- Inbound/outbound load balancing
- L2 bridge mode, NAT mode
- 3G/4G WAN failover
- Common Access Card (CAC) support

VoIP

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

Management and monitoring

- Web GUI
- Command line interface (CLI)
- SNMPv2/v3
- Centralized management and reporting with SonicWall GMS and Capture Security Center
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualization
- IPv4 and IPv6 management
- Dell N-Series and X-Series switch management including cascaded switches[2]

Integrated Wireless

- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards[2]
- WIDS/WIPS
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

[1] *Requires added subscription*
[2] *State sync high availability only on SonicWall TZ500 and SonicWall TZ600 models*

SonicWall TZ series system specifications

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

SonicWall TZ series specifications cont'd

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

SonicWall TZ series system specifications cont'd

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

*Future use

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

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

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

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

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

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

SonicWall TZ series system specifications cont'd

FIREWALL GENERAL	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Operating system		SonicOS	
Interfaces	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Power over Ethernet (PoE) support	—	—	TZ600P - 4 ports (4 PoE or 4 PoE+)
Expansion	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs		
Single Sign-On (SSO) Users	500	500	500
VLAN interfaces	50	50	50
Access points supported (maximum)	16	16	24
FIREWALL/VPN PERFORMANCE	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Firewall inspection throughput[1]	1.3 Gbps	1.4 Gbps	1.9 Gbps
Threat Prevention throughput[2]	600 Mbps	700 Mbps	800 Mbps
Application inspection throughput[2]	1.2 Gbps	1.3 Gbps	1.8 Gbps
IPS throughput[2]	900 Mbps	1.0 Gbps	1.2 Gbps
Anti-malware inspection throughput[2]	600 Mbps	700 Mbps	800 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	180 Mbps	225 Mbps	300 Mbps
IPSec VPN throughput[3]	900 Mbps	1.0 Gbps	1.1 Gbps
Connections per second	6,000	8,000	12,000
Maximum connections (SPI)	150,000	150,000	150,000
Maximum connections (DPI)	125,000	125,000	125,000
Maximum connections (DPI SSL)	25,000	25,000	25,000
VPN	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Site-to-site VPN tunnels	20	25	50
IPSec VPN clients (maximum)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	2 (100)	2 (150)	2 (200)
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	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL		
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists		
Comprehensive Anti-Spam Service	Supported		
Application Visualization	Yes	Yes	Yes
Application Control	Yes	Yes	Yes
Capture Advanced Threat Protection	Yes	Yes	Yes
NETWORKING	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay		
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode		
Routing protocols[4]	BGP[4], OSPF, RIPv1/v2, static routes, policy-based routing		
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)		

SONICWALL®

SonicWall TZ series system specifications cont'd

NETWORKING	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)		
Local user database	150	250	
VoIP	Full H.323v1-5, SIP		
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications	FIPS 140-2 (with Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus		
Common Access Card (CAC)	Supported		
High availability	Active/standby	Active/Standby with stateful synchronization	
HARDWARE	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Form factor	Desktop		
Power supply	24W external	36W external	60W external 180W external (TZ600P only)
Maximum power consumption (W)	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100-240 VAC, 50-60 Hz, 1 A		
Total heat dissipation	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.5 x 13.4 x 19 cm 1.38 x 5.28 x 7.48 in	3.5 x 15 x 22.5 cm 1.38 x 5.91 x 8.86 in	3.5 x 18 x 28 cm 1.38 x 7.09 x 11.02 in
Weight	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.92 kg / 2.03 lbs 1.05 kg / 2.31 lbs	1.47 kg / 3.24 lbs
WEEE weight	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.34 kg / 2.95 lbs 1.48 kg / 3.26 lbs	1.89 kg /4.16 lbs
Shipping weight	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.93 kg / 4.25 lbs 2.07 kg / 4.56 lbs	2.48 kg / 5.47 lbs
MTBF (in years)	54.0	40.8	18.4
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)		
Humidity	5-95% non-condensing		
REGULATORY	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP, ANATEL
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	—

SonicWall TZ series system specifications cont'd

INTEGRATED WIRELESS	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Standards	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS		—
Frequency bands[5]	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 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)		—

SonicWall TZ Series ordering information

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

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

SonicWall TZ Series ordering information

For SonicWall TZ400 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1440
Capture Advanced Threat Protection for TZ400 (1-year)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0534
Content Filtering Service (1-year)	01-SSC-0540
Comprehensive Anti-Spam Service (1-year)	01-SSC-0561
24x7 Support (1-year)	01-SSC-0552
For SonicWall TZ500 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1450
Capture Advanced Threat Protection for TZ500 (1-year)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0458
Content Filtering Service (1-year)	01-SSC-0464
Comprehensive Anti-Spam Service (1-year)	01-SSC-0482
24x7 Support (1-year)	01-SSC-0476
For SonicWall TZ600 Series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, and 24x7 Support (1-year)	01-SSC-1460
Capture Advanced Threat Protection for TZ600 (1-year)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	01-SSC-0228
Content Filtering Service (1-year)	01-SSC-0234
Comprehensive Anti-Spam Service (1-year)	01-SSC-0252
24x7 Support (1-year)	01-SSC-0246

Regulatory model numbers

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/ TZ300P	APL28-0B4/APL28-0B5/ APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 28 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

Datasheet-TZSeries-Gen6-COG-3366

SONICWALL®