SONICWALL™

SonicWall TZ series

Exceptional security and stellar performance at a disruptively low TCO

The SonicWall TZ series of Unified Threat Management (UTM) firewalls is ideally suited for any organization that requires enterprise-grade network protection.

SonicWall TZ series firewalls provide broad protection with advanced security services consisting of on-box and cloud-based anti-malware, anti-spyware, application control, intrusion prevention system (IPS), and URL filtering. To counter the trend of encrypted attacks, the TZ series has the processing power to inspect encrypted SSL/TLS connections against the latest threats. Combined with Dell X-Series switches, selected TZ series firewalls can directly manage the security of these additional ports.

Backed by the SonicWall Capture Threat Network, the SonicWall TZ series delivers continuous updates to maintain a strong network defense against cybercriminals. The SonicWall TZ series is able to scan every byte of every packet on all ports and protocols with almost zero latency and no file size limitations.

The SonicWall TZ series features Gigabit Ethernet ports, optional integrated 802.11ac wireless*, IPSec and SSL VPN, failover through integrated 3G/4G support, load balancing and network segmentation. The SonicWall TZ series UTM firewalls also provide fast, secure mobile access over Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X and Linux platforms.

The SonicWall Global Management System (GMS) enables centralized deployment and management of SonicWall TZ series firewalls from a single system.

Managed security for distributed environments

Schools, retail shops, remote sites, branch offices and distributed enterprises need a solution that integrates with their corporate firewall. SonicWall TZ series firewalls share the same code base—and same protection—as our flagship SuperMassive next-generation firewalls. This simplifies remote site management, as every administrator sees the same user interface (UI). GMS enables network administrators to configure, monitor and manage remote SonicWall firewalls through a single pane of glass. By adding high-speed, secure wireless, the SonicWall TZ series extends the protection perimeter to include customers and guests frequenting the retail site or remote office.

Benefits:

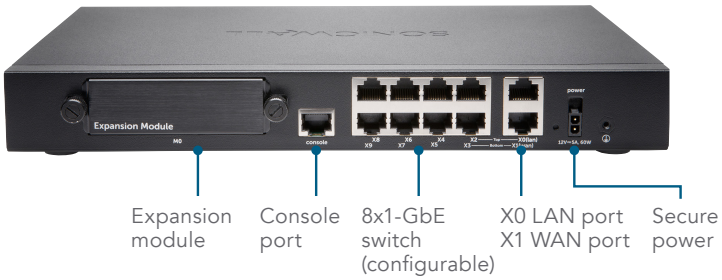
- Enterprise grade network protection
- Deep packet inspection of all traffic without restrictions on file size or protocol
- Secure 802.11ac wireless connectivity using integrated wireless controller or via external SonicPoint wireless access points
- SSL VPN mobile access for Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS and Linux devices
- Over 100 additional ports can be securely managed by the TZ console when deployed in combination with Dell X-Series switches

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

SonicWall TZ600 series

For emerging enterprises, retail and branch offices looking for security performance at a value price, the SonicWall TZ600 next-generation firewall secures networks with enterprise-class features and uncompromising performance.

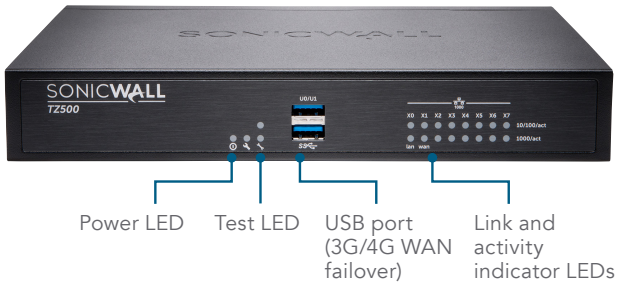
Specification	TZ600 series
Firewall throughput	1.5 Gbps
Full DPI throughput	500 Mbps
Anti-malware throughput	500 Mbps
IPS throughput	1.1 Gbps
IMIX throughput	900 Mbps
Max DPI connections	125,000
New connections/sec	12,000



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.

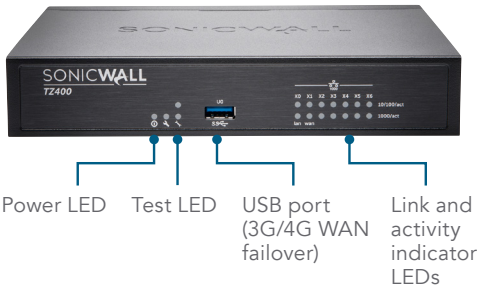
Specification	TZ500 series
Firewall throughput	1.4 Gbps
Full DPI throughput	400 Mbps
Anti-malware throughput	400 Mbps
IPS throughput	1.0 Gbps
IMIX throughput	700 Mbps
Max DPI connections	100,000
New connections/sec	8,000



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.

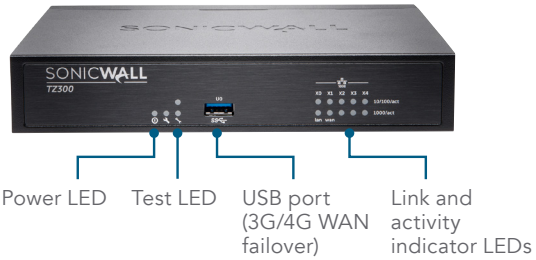
Specification	TZ400 series
Firewall throughput	1.3 Gbps
Full DPI throughput	300 Mbps
Anti-malware throughput	300 Mbps
IPS throughput	900 Mbps
IMIX throughput	500 Mbps
Max DPI connections	90,000
New connections/sec	6,000



SonicWall TZ300 series

The SonicWall TZ300 series offers an all-in-one solution that protects networks from attack. Unlike consumer grade products, the SonicWall TZ300 series firewall combines effective intrusion prevention, anti-malware and content/URL filtering with optional 802.11ac integrated wireless and broadest secure mobile platforms support for laptops, smartphones and tablets.

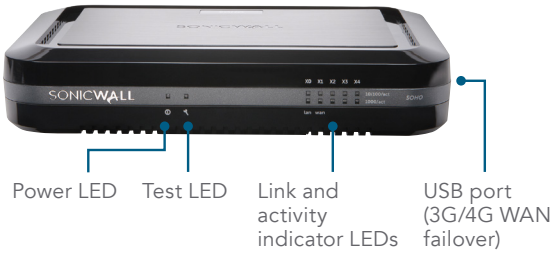
Specification	TZ300 series
Firewall throughput	750 Mbps
Full DPI throughput	100 Mbps
Anti-malware throughput	100 Mbps
IPS throughput	300 Mbps
IMIX throughput	200 Mbps
Max DPI connections	50,000
New connections/sec	5,000

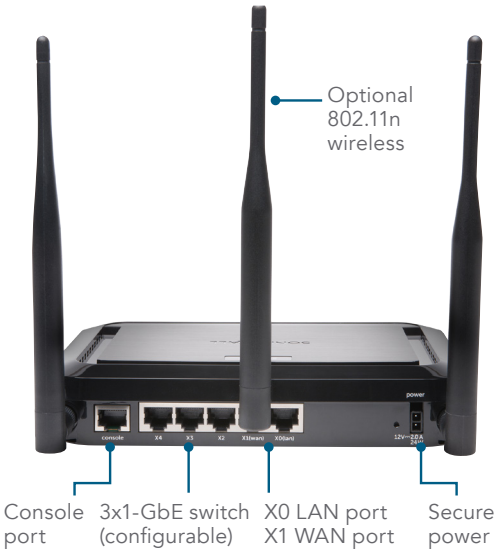


SonicWall SOHO series

For wired and wireless small and home office environments, the SonicWall SOHO series delivers the same business-class protection large organizations require at a more affordable price point.

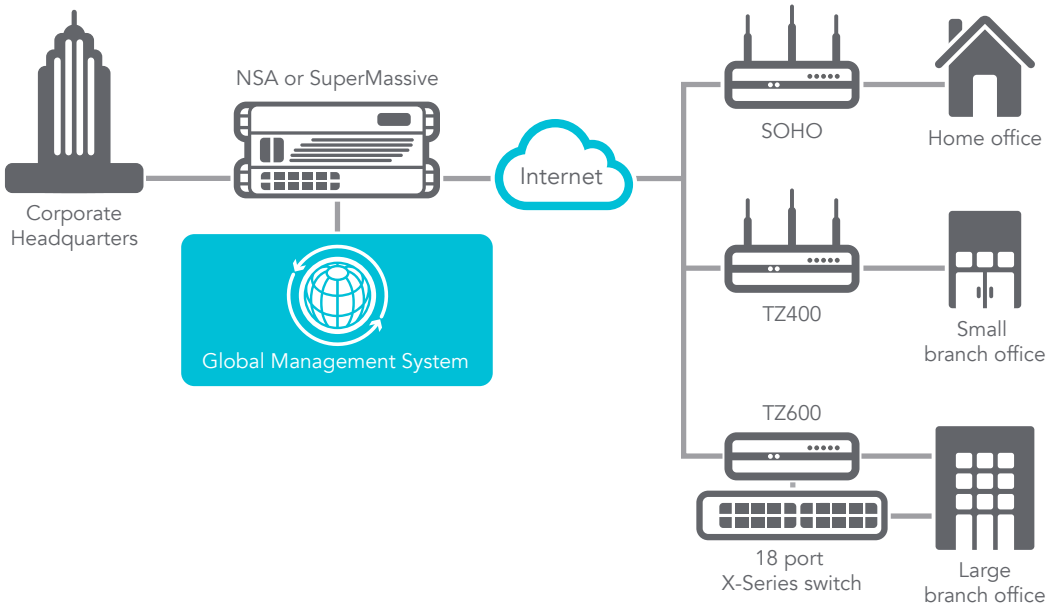
Specification	SOHO series
Firewall throughput	300 Mbps
Full DPI throughput	50 Mbps
Anti-malware throughput	50 Mbps
IPS throughput	100 Mbps
IMIX throughput	60 Mbps
Max DPI connections	10,000
New connections/sec	1,800





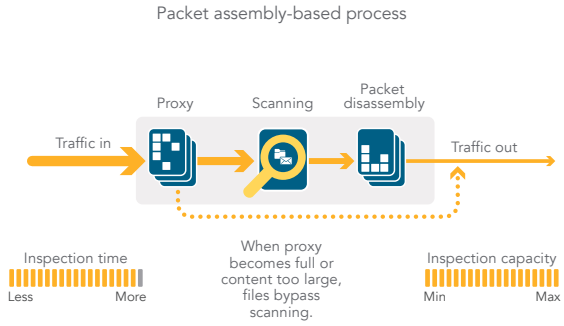
Extensible architecture for extreme scalability and performance

The Reassembly-Free Deep Packet Inspection (RFDPI) engine is designed from the ground up with an emphasis on providing security scanning at a high performance level, to match both the inherently parallel and ever-growing nature of network traffic. When combined with multi-core processor systems, this parallel-centric software architecture scales up perfectly to address the demands of deep packet inspection at high traffic loads. The SonicWall TZ Series platform relies on processors that, unlike x86, are optimized for packet, crypto and network processing while retaining flexibility and programmability in the field — a weak point for ASICs systems. This flexibility is essential when new code and behavior updates are necessary to protect against new attacks that require updated and more sophisticated detection techniques.

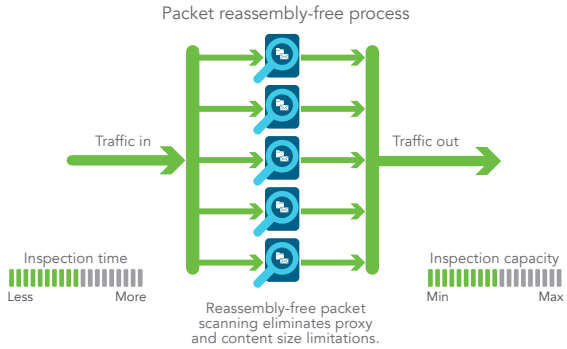


Reassembly-Free Deep Packet Inspection (RFDPI) engine

The RFDPI engine provides superior threat protection and application control without compromising performance. This patented engine inspects the traffic stream to detect threats at Layers 3-7. The RFDPI engine 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 preprocessing, including 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 another "match" event, at which point a pre-set action is taken. As malware is identified, the SonicWall firewall terminates the connection before any compromise can be achieved and properly logs the event. However, the engine can also be configured for inspection only or, in the 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.



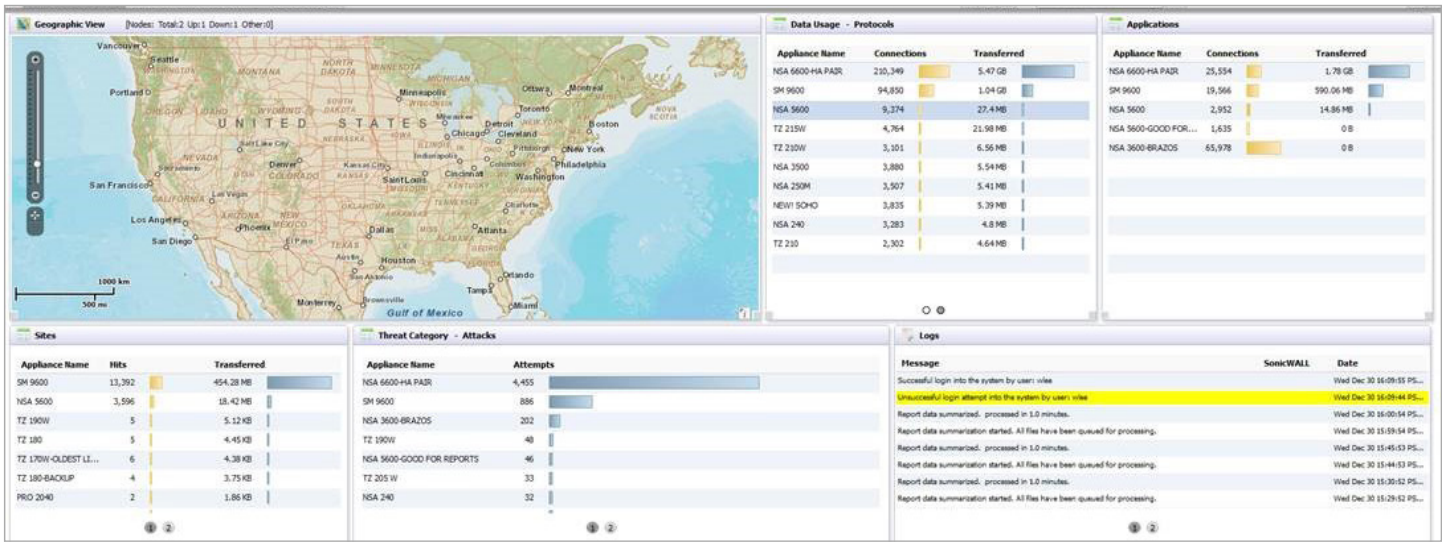
Competitive proxy-based architecture



SonicWall stream-based architecture

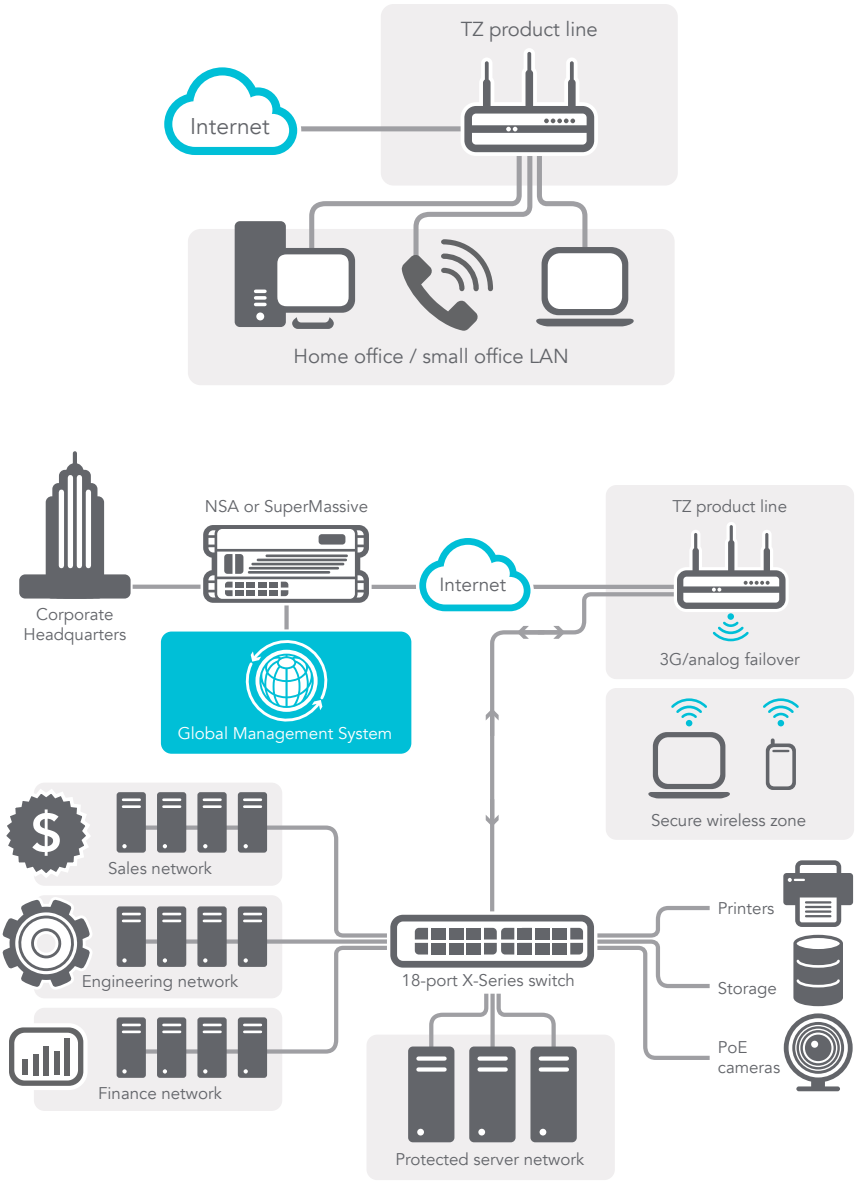
Global management and reporting

For larger, distributed enterprise deployments, the optional SonicWall Global Management System (GMS) provides administrators a unified, secure and extensible platform to manage SonicWall security appliances and Dell X-Series switches. It enables enterprises to easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities and governs all operational aspects of the security infrastructure including centralized policy management and enforcement, real-time event monitoring, analytics and reporting, and more. GMS also meets the firewall change management requirements of enterprises through a workflow automation feature. GMS provides a better way to manage network security by business processes and service levels that dramatically simplify the lifecycle management of your overall security environments rather than on a device-by-device basis.



Security and protection

The dedicated, in-house SonicWall Capture Labs threat research team works on researching and developing countermeasures to deploy to the firewalls in the field for up-to-date protection. The team leverages more than one million sensors across the globe for malware samples, and for telemetry feedback on the latest threat information, which in turn is fed into the intrusion prevention, anti-malware and application detection capabilities. SonicWall firewall customers with current subscriptions are provided continuously updated threat protection around the clock, with new updates taking effect immediately without reboots or interruptions. The signatures on the appliances protect against wide classes of attacks, covering up to tens of thousands of individual threats with a single signature. In addition to the countermeasures on the appliance, all SonicWall firewalls also have access to SonicWall CloudAV, which extends the onboard signature intelligence with more than 20 million signatures, and growing. This CloudAV database is accessed via a proprietary light-weight protocol by the firewall to augment the inspection done on the appliance. With Geo-IP and botnet filtering capabilities, SonicWall next-generation firewalls are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.



Application intelligence and control

Application intelligence informs administrators of application traffic traversing the network, so they can schedule application controls based on business priority, throttle unproductive applications and block potentially dangerous applications. Real-time visualization identifies traffic anomalies as they happen, enabling immediate countermeasures against potential inbound or outbound attacks or performance bottlenecks. SonicWall application traffic analytics provide granular insight into application traffic, bandwidth utilization and security threats, as well as powerful troubleshooting and forensics capabilities. Additionally, secure single sign-on (SSO) capabilities enhance the user experience, increase productivity and reduce support calls. Management of application intelligence and control is simplified by using an intuitive web-based interface.

Flexible and secure wireless

Available as an optional feature, high-speed 802.11ac wireless* combines with SonicWall next-generation firewall technology to create a wireless network security solution that delivers comprehensive protection for wired and wireless networks.

This enterprise-level wireless performance enables WiFi-ready devices to connect from greater distances and use bandwidth-intensive mobile apps, such as video and voice, in higher density environments without experiencing signal degradation.

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

SONICWALL™

Features

RFDPI engine	
Feature	Description
Reassembly-Free Deep Packet Inspection	This high-performance, proprietary and patented inspection engine performs stream based bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts, malware and identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware, and does not become a launch platform for attacks in case an infected machine is brought inside.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for deep packet inspection of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Deep Packet Inspection of Secure Socket Shell (DPI-SSH)	Detects and prevents advanced encrypted attacks that leverage SSH, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control communications and data exfiltration.
Capture Advanced Threat Protection	
Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Broad file type analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OSX and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Encrypted threat prevention	
Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in TLS/SSL encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.
Intrusion prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Capture Labs threat research team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.
Threat prevention	
Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV malware protection	A continuously updated database of over 20 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.

Threat prevention con't	
Feature	Description
SSL decryption and inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL encrypted traffic Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports.
Application intelligence and control	
Feature	Description
Application control	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over 3,500 application signatures, to increase network security and enhance network productivity.
Custom application identification	Control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
Granular control	Control applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.
Content filtering	
Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive with Content Filtering Service. Extend policy enforcement to block internet content for devices located outside the firewall perimeter with the Content Filtering Client.
Granular controls	Block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
YouTube for Schools	Enable teachers to choose from hundreds of thousands of free educational videos from YouTube EDU that are organized by subject and grade and align with common educational standards.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.
Enforced anti-virus and anti-spyware	
Feature	Description
Multi-layered protection	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the most recent version of anti-virus and anti-spyware signatures installed and active, eliminating the costs commonly associated with desktop anti-virus and anti-spyware management.
Automated deployment and installation option	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Always on, automatic virus protection	Frequent anti-virus and anti-spyware updates are delivered transparently to all desktops and file servers to improve end user productivity and decrease security management.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.
Firewall and networking	
Feature	Description
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DDoS/DoS attack protection	SYN Flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it provides the ability to protect against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The SonicWall TZ Series can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode and Network Tap modes.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With the latest SonicOS, the hardware will support filtering implementations.
Biometric authentication for remote access	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user's identity for network access.
Dell X-Series switch integration	Manage security settings of additional ports, including POE and POE+, under a single pane of glass using TZ series dashboard with X-Series switch (not available with the SOHO model)

Firewall and networking con't	
Feature	Description
High availability	SonicWall TZ500 and SonicWall TZ600 models support high availability with Active/Standby with state synchronization. SonicWall TZ300 and SonicWall TZ400 models support high availability without Active/Standby synchronization. There is no high availability on SonicWall SOHO models.
Threat API	Enables the firewall to receive any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Wireless Network Security	IEEE 802.11ac wireless technology can deliver up to 1.3 Gbps of wireless throughput with greater range and reliability. Available on SonicWall TZ600 through SonicWall TZ300 models. Optional 802.11 a/b/g/n is available on SonicWall SOHO models.
Management and reporting	
Feature	Description
Global Management System	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances and Dell X-Series switches through a single management console with an intuitive interface to reduce management costs and complexity.
Powerful, single device management	An intuitive, web-based interface allows quick and convenient configuration. Also, a comprehensive command line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall GMSFlow Server or other tools that support IPFIX and NetFlow with extensions.
Virtual Private Networking	
Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the SonicWall TZ Series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.
Content/context awareness	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix1/TerminalServices SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

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
- Threat API

SSL/SSH decryption and inspection[1]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control

Capture Advanced Threat Protection[1]

- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated & manual submission
- Real-time threat intelligence updates
- Auto-Block capability

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 visualization[2]
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- User activity tracking (SSO)
- Comprehensive application signature database

Web content filtering[1]

- URL filtering
- Anti-proxy technology
- Keyword blocking
- 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

- 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[3]
- 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
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualization
- IPv4 and IPv6 management
- Dell X-Series switch management including cascaded switches

Integrated Wireless

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

[1] Requires added subscription
[2] Not available on SOHO series
[3] State sync high availability only on SonicWall TZ500 and SonicWall TZ600 models

SONICWALL™

SonicWall TZ system specifications

Hardware overview	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Operating system	SonicOS				
Security processing cores	2	2	4	4	4
Interfaces	5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Expansion	USB	USB	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Single Sign-On (SSO) Users	250	500	500	500	500
VLAN interfaces	25	25	50	50	50
Access points supported (maximum)	2	8	16	16	24
Dell X-Series switch models supported	Not available	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Firewall/VPN performance	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Firewall inspection throughput[1]	300 Mbps	750 Mbps	1,300 Mbps	1,400 Mbps	1,500 Mbps
Full DPI throughput[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Application inspection throughput[2]	-	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
IPS throughput[2]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Anti-malware inspection throughput[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX throughput	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN throughput[3]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Connections per second	1,800	5,000	6,000	8,000	12,000
Maximum connections (SPI)	10,000	50,000	100,000	125,000	150,000
Maximum connections (DPI)	10,000	50,000	90,000	100,000	125,000
Maximum connections (DPI SSL)	100	500	500	750	750
VPN	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Site-to-site VPN tunnels	10	10	20	25	50
IPSec VPN clients (maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual assist bundled (maximum)	-	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14				
Route-based VPN	RIP, OSPF				
Certificate support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to- SonicWall VPN, SCEP				
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN				
Global VPN client platforms supported	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10				
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)				
Security services	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
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				
Enforced Client Anti-Virus and Anti-Spyware	McAfee®				
Comprehensive Anti-Spam Service	Supported				
Application Visualization	No	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes	Yes

SONICWALL™

SonicWall TZ series specifications con't

Networking	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
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)				
Authentication	LDAP (multiple domains), XAUTH/ RADIUS, SSO, Novell, internal user database	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix			
Local user database	150			250	
VoIP	Full H.323v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	FIPS 140-2 (with Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus				
Certifications pending	Common Criteria NDPP				
Common Access Card (CAC)	Supported				
High availability	No	Active/standby	Active/standby	Active/standby with stateful synchronization	Active/standby with stateful synchronization
Hardware	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Form factor	Desktop				
Power supply (W)	24W external	24W external	24W external	36W external	60W external
Maximum power consumption (W)	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100 to 240 VAC, 50-60 Hz, 1 A				
Total heat dissipation	21.8 / 38.7 BTU	23.5 / 40.9 BTU	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.6x14.1x19cm	3.5x13.4x19cm	3.5x13.4x19cm	3.5x15x22.5cm	3.5x18x28cm
Weight	0.34 kg / 0.75 lbs 0.48 kg / 1.06 lbs	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.92 kg / 2.03 lbs 1.05 kg / 2.31 lbs	1.47 kg / 3.24 lbs
WEEE weight	0.80 kg / 1.76 lbs 0.94 kg / 2.07 lbs	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.34 kg / 2.95 lbs 1.48 kg / 3.26 lbs	1.89 kg /4.16 lbs
Shipping weight	1.20 kg / 2.64 lbs 1.34 kg / 2.95 lbs	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.93 kg / 4.25 lbs 2.07 kg / 4.56 lbs	2.48 kg / 5.47 lbs
MTBF (years)	58.9/56.1 (wireless)	56.1	54.0	40.8	18.4
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)				
Humidity	5-95% non-condensing				
Regulatory	**SOHO series**	**TZ300 series**	**TZ400 series**	**TZ500 series**	**TZ600**
Regulatory model (wired)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, BSMI, KCC/MSIP	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/ GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP
Regulatory model (wireless)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	-

SonicWall TZ series specifications con't

Integrated Wireless	SOHO series	TZ300, TZ400, TZ500 series	TZ600
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[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;	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz	-
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64;	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64	-
Transmit output power	Based on the regulatory domain specified by the system administrator	Based on the regulatory domain specified by the system administrator	-
Transmit power control	Supported	Supported	-
Data rates supported	802.11a: 6, 9, 12, 18,24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15,30, 45, 60, 90, 120, 135, 150 Mbps per channel;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15,30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel	-
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	-

**Future use.*
[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] Full DPI/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.
[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 TZ400, TZ500 and TZ600.
[5] All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access points products (SonicPoints)

SonicWall TZ Series ordering information

Product	SKU
SonicWall SOHO with 1-year TotalSecure	01-SSC-0651
SonicWall SOHO Wireless-N with 1-year TotalSecure	01-SSC-0653
SonicWall TZ300 with 1-year TotalSecure Advanced Edition	01-SSC-1702
SonicWall TZ300 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1703
SonicWall TZ400 with 1-year TotalSecure Advanced Edition	01-SSC-1705
SonicWall TZ400 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1706
SonicWall TZ500 with 1-year TotalSecure Advanced Edition	01-SSC-1708
SonicWall TZ500 Wireless-AC with 1-year TotalSecure Advanced Edition	01-SSC-1709
SonicWall TZ600 with 1-year TotalSecure Advanced Edition	01-SSC-1711
High availability options (each unit must be the same model)	
SonicWall TZ500 High Availability	01-SSC-0439
SonicWall TZ600 High Availability	01-SSC-0220

SonicWall TZ Series ordering information con't

Services	SKU
For SonicWall SOHO Series	
Comprehensive Gateway Security Suite 1-year	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0670
Content Filtering Service 1-year	01-SSC-0676
Comprehensive Anti-Spam Service 1-year	01-SSC-0682
24x7 Support 1-year	01-SSC-0700
For SonicWall TZ300 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ300 (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 TZ400 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ400 (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, Content Filtering and 24x7 Support for TZ500 (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	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ600 (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

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

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

Datasheet-TZ Series-US-VG-MKTG658

SONICWALL™