

SonicWall TZ Series

Exceptional security and stellar performance at an incredibly low total cost of ownership

SonicWall Unified Threat Management (UTM) firewalls are ideal for any organization that needs enterprise-class network protection.

SonicWall TZ series firewalls offer comprehensive protection through advanced security services including integrated and cloud-based antimalware, antispyware, application control, IPS (Intrusion Prevention System), and URL filtering capabilities. In order to counter the trend of encrypted attacks, the processing power of the TZ series firewalls allows them to inspect encrypted SSL / TLS connections to deal with the latest threats. In combination with Dell X series switches, some TZ series firewalls can directly manage the security of these additional ports.

Powered by the SonicWall Capture Threat Network, the SonicWall TZ series provides continuous updates to maintain a robust network defense against cybercriminals. The SonicWall TZ series is capable of analyzing every byte of every packet on all ports and protocols with almost no latency and no limitations on file size.

The SonicWall TZ series includes Gigabit
Ethernet ports, connectivity
optional integrated 802.11ac wireless, * IPSec and
SSL VPN, reconnection via integrated 3G / 4G
support, balance

load and network segmentation. The SonicWall TZ series UTM firewalls also provide fast and secure mobile access using Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X, and Linux platforms.

The SonicWall Global Management System (GMS) enables you to centrally deploy and manage SonicWall TZ Series firewalls from a single system.

Managed security services for distributed environments

Schools,

Retail establishments, 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 the same protection - as our flagship
SuperMassive next-generation firewalls, simplifying
remote site management since all administrators see
the same user interface. With GMS, network
administrators can configure, monitor and manage
SonicWall firewalls remotely from a single console.
By incorporating high-speed and secure wireless
connectivity, the SonicWall TZ series products
extend the perimeter of protection to encompass
customers and guest users who frequent a particular
retail location or remote office.



Advantage:

- Enterprise-class network protection
- Deep packet inspection of all traffic with no protocol or file size restrictions
- Secure wireless connectivity 802.11ac via integrated wireless controller or via external SonicWall SonicPoint wireless access points
- Mobile SSL VPN access for Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS and Linux devices
- Implemented in combination with Dell X-series switches, TZ firewalls allow you to securely manage more than 100 additional ports through your console.

 $^{^{*}}$ 802.11ac is not currently available on SOHO models; SOHO models support 802.11a / b / g / n

SonicWall TZ600 Series

For startups, retailers, and branch offices looking for value for money security performance, the SonicWall TZ600 Next-Generation Firewall protects networks with enterprise-class features and uncompromising performance.

specs	TZ600 Series
Firewall performance	1.5 Gbps
Full DPI performance Anti-malware	500 Mbps
performance	500 Mbps
IPS performance	1.1 Gbps
IMIX performance	900 Mbps
Maximum DPI connections	125,000
New connections / s	12,000





SonicWall TZ500 Series

For growing SMBs and branch offices, the SonicWall TZ500 series provides highly effective protection without compromise with network productivity and an optional integrated dual-band 802.11ac wireless connection.

specs	TZ500 Series
Firewall performance	1.4 Gbps
Full DPI performance Anti-malware	400 Mbps
performance	400 Mbps
IPS performance	1.0 Gbps
IMIX performance	700 Mbps
Maximum DPI connections	100,000
New connections / s	8,000





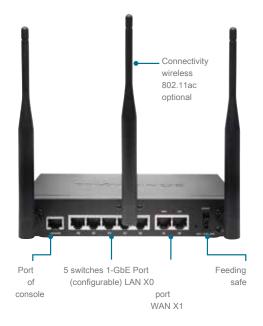


SonicWall TZ400 Series

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.

specs	TZ400 Series
Firewall performance	1.3 Gbps
Full DPI performance Anti-malware	300 Mbps
performance	300 Mbps
IPS performance	900 Mbps
IMIX performance	500 Mbps
Maximum DPI connections	90,000
New connections / s	6,000





SonicWall TZ300 Series

The SonicWall TZ300 series provides a comprehensive solution that protects networks against attacks. Unlike consumer products, the SonicWall TZ300 Series Firewall combines powerful intrusion prevention, antimalware, and content / URL filtering capabilities with an optional built-in 802.11ac wireless connection and the broadest support for secure mobile platforms from laptops, smartphones and tablets.

specs	TZ300 Series
Firewall performance	750 Mbps
Full DPI performance Anti-malware	100 Mbps
performance	100 Mbps
IPS performance	300 Mbps
IMIX performance	200 Mbps
Maximum DPI connections	50,000
New connections / s	5,000







SonicWall SOHO Series

For small office or home office wired and wireless environments, the SonicWall SOHO series provides the same enterprise-class protection that large enterprises require at a much more affordable price.

specs	SOHO series
Firewall performance	300 Mbps
Full DPI performance Anti-malware	50 Mbps
performance	50 Mbps
IPS performance	100 Mbps
IMIX performance	60 Mbps
Maximum DPI connections	10,000
New connections / s	1,800

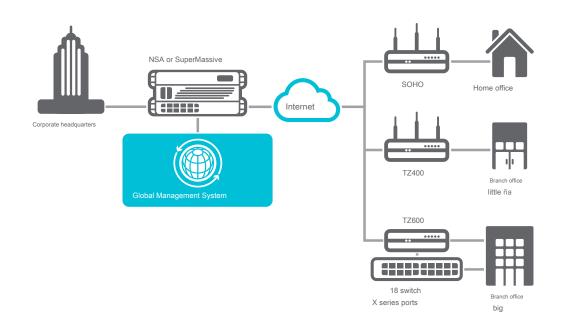




Scalable architecture for maximum performance and scalability

The Reassembly-Free Deep Packet Inspection (RFDPI) engine is designed from the ground up with the goal of providing high-performance security scanning to accommodate the parallel and growing nature of network traffic. When combined with multi-core processor systems, this parallel processing-centric software architecture seamlessly scales to meet the requirements

of deep packet inspection with high traffic loads. The SonicWall TZ platform is based on processors that, unlike x86, are optimized for packet, encryption and network processing, while preserving flexibility and on-site programming, a weak point in ASIC systems. This flexibility is essential when new code and behavior updates are required to provide protection against new attacks that require updated and more sophisticated detection techniques.





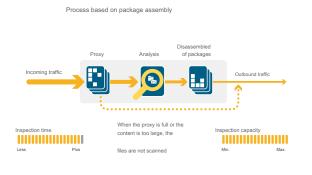
Reassembly-Free Deep Packet Inspection (RFDPI) engine

The RFDPI engine offers exceptional threat protection and application control without sacrificing performance. This patented engine inspects traffic flow for threats at levels 3-7. The RFDPI engine subjects network flows to extensive and repeated normalization and decryption processes to neutralize advanced evasion techniques that seek to circumvent threats. detection engines and introduce malicious code into the

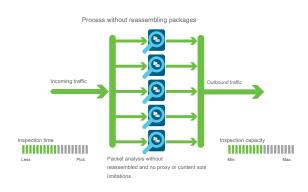
net. After the necessary preprocessing is applied to a packet, including SSL decryption, it is parsed against a single proprietary in-memory representation of three

definition databases: intrusion, malware and application attacks. The connection state is then updated to represent the position of the flow relative to those databases until an attack state or other event that is recognized as a threat is encountered. At that time, a predefined action takes place. When malware is identified, the SonicWall firewall terminates the connection earlier

damage and properly record the event. However, the engine can also be configured for inspection only or, in the case of application discovery, to offer Layer 7 bandwidth management services for the rest of the application flow as soon as the application has been identified.



Competitor architecture

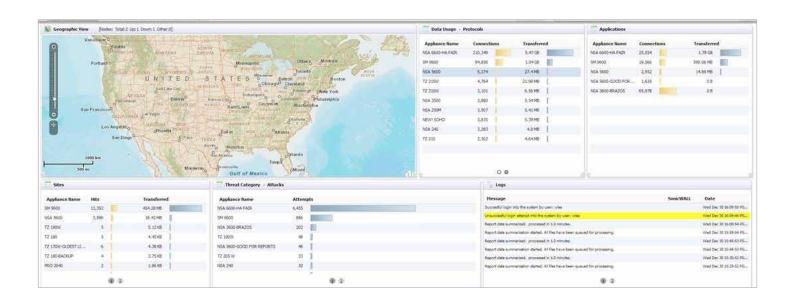


SonicWall architecture

Global reporting and management

For larger deployments in distributed enterprises, the SonicWall Global Management System (GMS) provides administrators with a unified, secure, and extensible platform to manage SonicWall security appliances and Dell X-series switches. This system enables companies to easily consolidate the management of security devices, reduce administrative and troubleshooting complexities, and control all operational aspects of the security infrastructure, such as

centralized policy management and enforcement, real-time event monitoring, analytics and reporting, and more. GMS also meets enterprise firewall change management requirements with a workflow automation capability. GMS provides a better way to manage network security using business processes and service levels that dramatically simplify lifecycle management of your overall security environments, rather than device-by-device.





Protection and security

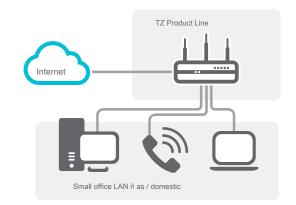
SonicWall Capture Labs' dedicated internal threat research team studies and develops countermeasures to apply to on-premises firewalls for up-to-date protection. With the help of more than a million sensors distributed around the world, they obtain malware samples and telemetric information on the latest threats, which in turn is transmitted to firewalls to support intrusion prevention, antimalware and detection functions. Applications. SonicWall firewall customers with current subscriptions enjoy continually updated threat protection 24/7. Plus, those updates are applied immediately without the need for reboots or interruptions. The definitions available on the devices protect against a wide range of attacks. In fact, each of them covers tens of thousands of individual threats. In addition to countermeasures

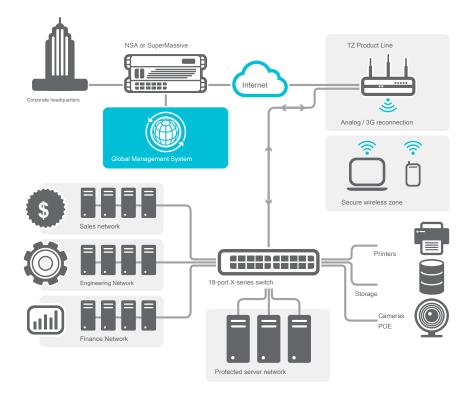
Available on the appliance, all SonicWall firewalls have access to SonicWall CloudAV, which expands the definition data built in with more than 20 million definitions, an ever-growing number. The firewall accesses the CloudAV database using a proprietary lightweight protocol in order to enforce the inspection performed on the device. With botnet and IP filtering capabilities based on geographic data, SonicWall next generation firewalls can block traffic from rogue domains or entire geographic regions to reduce the risk profile for the network.

Application intelligence and control

Application intelligence informs administrators of the application traffic traversing the network so that they can program application controls based on the

business priorities, restrict unproductive applications, and block potentially dangerous ones. Real-time visualization identifies traffic anomalies as they occur, allowing immediate countermeasures against





possible inbound or outbound attacks or performance bottlenecks. SonicWall application traffic analytics provide detailed information on application traffic, bandwidth usage, and security threats, as well as powerful troubleshooting and forensic analysis capabilities. Additionally, secure single sign-on (SSO) improves the user experience, increases productivity, and reduces help desk calls. Using an intuitive web-based interface simplifies application intelligence and control management.

Flexible and secure wireless connection

Available as an optional feature, high-speed 802.11ac wireless connectivity is combined with SonicWall's next-generation firewall technology to create a wireless network security solution that provides comprehensive protection for both wired and wireless networks.

With this enterprise-grade wireless performance, Wi-Fi ready devices can

connect farther away and use bandwidth-hungry mobile applications, such as voice and video, in higher density environments without reducing signal quality.



 $^{^{\}ast}$ 802.11ac is not currently available on SOHO models; SOHO models support 802.11a / b / g / n

Benefits

New Proposed impaction without reasonably This proprietely, high performance impaction engine performs too very flow-based terific analysis, without proxy or buffering, to discover introduce and impaction in stricts or application staff required by proxy or buffering, to discover introduce and an impaction or properties. Bufferform impaction The proxy or buffering and outgoing terific simultaneously for threats to prevent the redearch from being used for maleure data Durching part for stricts and an implicate and an implication compare or ratio. Bufferform and outgoing terific simultaneously actually to provide any policy and the properties of the p	DEDOL assiss		
Deep parket inspection without researchly If its proprietary, high orderinance inspection storps reprive the record for bodder analysis, without proving trustment and melement and inference and inf	RFDPI engine		
Situres and makes are and settlering spiritions malifer projections of provent the reference from being used for makesee distribution or becoming a backford profession of provent the reference from being used for makesee distribution or becoming a backford profession of the standard settlering and the province of the	Benefit	Description	
Single pass inequation The single-pass pass for data in Intended comparison returns. The single-pass pass of the	Deep packet inspection without reassembly	This proprietary, high-performance inspection engine performs two-way flow-based traffic analysis, without proxy or buffering, to discover intrusio attempts and malware and identify application traffic regardless of port.	
Industrial projection of entire in the call of the call from the call of the call production is a organ actile close. Industrial projection of instructions provided by provided and proposed inspection of simulations as entire without industrial projection of instructions are without instruction. Capture Affordat Triangl Projection Description Seption instruction and analysis is to behavior, providing comprise validity with medicinal activity. APPAs, as a web validity of the types Seption instruction of an analysis as to behavior, providing comprise validity in medicinal activity. APPAs, as a web validity of the types Seption instruction of an analysis as to behavior, providing comprise validity with medicinal activity. APPAs, as a web validity of the types Seption instruction instruction instruction of the types of	Bidirectional inspection	It scans incoming and outgoing traffic simultaneously for threats to prevent the network from being used for malware distribution or becoming a launching pad for attacks should an infected computer enter.	
without involved infollocing inhibitories or steem and file size. After, it can be applied to common protocole as well as rate TCP determin. Determine Advanced Throat Protocols Combar Advanced Throat Protocols The mills engine sandtow platform, including visualized samples and control communications and data selfination. Description The mills engine sandtow platform, including visualized samples and control communications and data selfination. Description The mills engine sandtow platform, including visualized samples and control (RII) years enualized, and hyperticon-level analysis technology, executes supplications calcularly executes supplications calcularly executes supplications calcularly executes supplications and analysis technology, executes supplied permitting visualized samples program (PEI, DLLS PDFs, MS Office documents, surfaves, APAS, and APAS, and analysis control of a wide variety of file types. Such as executable programs (PEI, DLLS PDFs, MS Office documents, surfaves, APAS, and APAS, and analysis can be supplied to the Somotival Capture subscription finewals and serie in the Gateway Mell Virus and IPS definition databases and CRIL. IP repaid on the surfave and IPS definition databases and common within 4th hours. Lock until there is a verificit. Description Description	Single pass inspection	The single-pass DPI architecture simultaneously scans traffic for malware and intrusion detection and for application identification, dramatically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.	
Counted Naturated Treated Protection Bereiff Description Control Control Protection Control	Flow-based inspection	Bufferless, proxy-free inspection technology provides very low-latency performance for deep packet inspection of simultaneous network streams without introducing limitations on stream and file size. Also, it can be applied to common protocols as well as raw TCP streams.	
Decorption The multi-engine sandbox platform, including withaltoral sandboxing, full system emulation, and hypoxisto-level analytics technology, executes supposes code and analytics to behavior, providing compiles visibility into malicious activity. Scarn a wide variety of file types Signor a wide variety of file types Signor a wide variety of file types Signor a wide variety of file types. When a malicious file is detected, a definition is immediately and evaluate to the Sciul/Val Capture subscription for the Capture of the Ca	Secure Socket Shell Deep Packet Inspection (DPI-SSH)	Detects and prevents advanced encrypted attacks using SSH, blocks encrypted malware downloads, stops the spread of infections, and thwarts command-and-control communications and data exfiltration.	
The multi-engine sandbooking Supports scanning of a wide variety of file types Supports scanning of a wide variety of file types, such as executable programs (PE), DLLs. PDF, and Sifes documents, archives, ARAs, and ARAS, and wide variety of file types, such as executable programs (PE), DLLs. PDF, and multi-browser environments. When a malicious file is defected, a definition is immediately made available to the Sonicival Capture subscription firewalls and sent to the Catenory ARA-Yma and IPO definition definitions and URIL, IP regulation delibbases and comains within 46 hours. Lock until there is a verificit The prevent potentially diargenous files from accessing the network, files sent to the cloud for analysis can be held at the gateway until a verificity in residency. Benefit Description Description Description Description SSH Desp Packet Inspection SSH Desp Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH turnels to prevent affacts using SSH. Interestion Description Description Description The spirity integrated intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits. But a covering a wide range of allacks and vulnerabilities. Pile protection based on countermeasures The Spirity integrated intrusion Prevention System (IPS) uses definitions and interest protection prevention to prevent the spirity integrated intrusion Prevention System (IPS) uses definitions and interest protection interrupting your service. Pile protection based or countermeasures The Spirity integrated intrusion Prevention System (IPS) uses definitions and interest prevent the spiral prevention to prevent the spiral prevention to prevent the spiral prevention to prevent the spiral prevention for prevent the spiral prevention of inte	Capture Advanced Threat Protection		
secules suspicious code and analyzes its behavior, providing complete visibility into nationous activity. Scan a wide variety of file types Supports scanning of a wide variety of file types, such as executable programs (PE), DLLs PDFs, MS Office documents, activities, AARs, and ARKs, as well as multiple operating systems, such as Windows, Android, Msc OS X, and multi-ADD office documents, activities, AARs, and ARKs, as well as multiple operating systems, such as Windows, Android, Msc OS X, and multi-ADD office occurrence environments. When a multicous this is detected, a definition is immediately made cannot activities and sent to the Calevoys And-Virtus and IPS definition disblasees and URIL. IP regulation disblasees and domains within 40 hours. In prevent potentially dangerous files from accessing the network, files sent to the double for analysis can be held at the gateway until a verificity in recipilate. Description Description Description Description Description and 11.5 / SSL inspection SSH Inspection SSH Inspection SSH Inspection SSH Desp Packet Inspection (DPI-SSH) decrypts and impocts the data passing through SSH tumoris to prevent attacks using SSH. The signify integrated intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and expolisi, thus covering a wide carrage of attacks and vulnerabilities. The SonroVall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering as a description in the spot, without requiring a restoor or interrupting your service. The SonroVall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering to the spot with a state of the filterior and covering as reduce or interrupting your service. Per postaction between zones It strangeries internal security by againming the network individual engines and inclination prevented in the spread of threating are abo	Benefit	Description	
APKs, as well as multiple operating systems, such as Windows, Androul, Mac OS X, and multi-browner environments. Quick definition implementation When a realization file is detected, a definition is immediately made available to the Sprint/Villous and PS definition databases and URL, IP reputation databases and somains within 48 hours. Lock until there is a verdict To prevent potentially dangerous files from accessing the network, files sent to the cloud for analysis can be held at the getereary until a verdict is rendered. Description Benefit Description Description and TLS / SSL inspection Description and TLS / SSL inspection SSH Deep Packet Inspection (DPI-SSH) decrypts and inspect threats helder in TLS encrypted traffic / SSL. Included with security subscriptions for all models expose SSH inspection. SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH. Intuition prevention The spirity integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerability and exploits, thus covering a wide range of latasts and vulnerabilities. Automatic updates of definitions The Scientific Agrature Latas Trivers the Security for better on the spot, without requiring a relator or interrupting pure service. It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent on the prevention to prevent on the local network and directed to IPs and domains identified as advised from botted attacks. The scription and blocking of command and control (CnC) Elected in block attacks and subspections for the spot, without requiring a relator or interrupting pure service. Protection based a nanomaly Identify and block attacks that subspections for botto on the local network and directed to IPs and domains identified as advised from botted attacks. Threat prevention Protect your revision from zero day etitacks with constant up	Multi-engine sandboxing		
Galeway Anti-Vins and IPS definition databases and URL. IP reputation databases and domains within 48 hours. Lock until there is a verdict To prevent potentially dangerous files from accessing the network, files sent to the cloud for analysis can be held at the gateway until a verdict is incidented. Description Description	Scan a wide variety of file types		
Benefit Description Benefit Description Description and TLS / SSL inspection Description and TLS / SSL inspection SSH inspection SSH project in inspect in the fig. without the need for proxies, for malware, infrusions, and data leaks, and enforce application, URL, a content control policies to protect against threats hidden in TLS-encrypted traffic / SSL. Included with security subscriptions for all models excess SOHO. For SOHO models, it is soid as a separate license. SSH inspection SSH projection SSH projection Description Description Thistory prevention Description The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities. Automatic updates of definitions The Schick/all Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. If sprotection between zones It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagations or known as of CnC points. Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bysess the IPS. Protection Protec	Quick definition implementation		
Benefit Description Description and TLS / SSL inspection SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH. Inspection SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH. Inspection Description The tightly integrated Infrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerability and exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SontcWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. It is transplanes internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Jenual Protection between transplants and protection individual exploits. Anti-evasion technology The Specific or protection individual exploits. Description Description Selection and blocking of command and control (CnC) and protection individual exploits. Jenual Protection between zones in the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Jenual Protection between zones in the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Jenual Protection between zones and treatms and control traffic originating from bots on the local	Lock until there is a verdict		
Decrypt and inspect SSL traffic on the fly, without the need for proxies, for malware, infrusions, and data leaks, and enforce application, URL, a content control policies to protect against threats hidden in TLS-encrypted traffic / SSL included with security subscriptions for all models excess SCHO, For SCHO models, it is sold as a separate license. SSH Inspection SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH. Intrusion prevention Benefit Description The tightly integrated intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. PS protection between zones It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Identifies and blocks command and control (CnC) Identifies and blocks command and control (SnC) Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Identify and block attacks that abuse protocols to try to bypass the IPS. Zero day protection Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Protect your network from zero-day attacks with constant updates against the latest ex	Encrypted Threat Prevention		
content control policies to protect against threats hidden in TLS-encrypted traffic / SSL. Included with security subscriptions for all models excessive SOHO. For SOHO models, it is sold as a separate license. SSH inspection SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH. Institution prevention Benefit Description The tightly integrated intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. IPS protection between zones It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) Identifies and blocks actuacks that abuse protocols to try to bypass the IPS. Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bypass the IPS. Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive from pronocology and provided to the protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques of updates and intrusion prevention and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threa	Benefit	Description	
Intrusion prevention Benefit Description The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. IPS protection between zones It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) activities from bortent attacks Identify and block attacks that abuse protocols to try to bypass the IPS. Protocol abuse / anomally Identify and block attacks that abuse protocols to try to bypass the IPS. Protocol abuse / anomally Identify and block attacks that abuse protocols to try to bypass the IPS. Protocol abuse / anomally Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. 24 hour security updates New threat updates are automatically transferred to frewalls with active security services, where they are immediately effective without the	Decryption and TLS / SSL inspection	content control policies to protect against threats hidden in TLS-encrypted traffic / SSL. Included with security subscriptions for all models e	
Benefit Description Protection based on countermeasures The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. IPS protection between zones It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as analyzer propagators or known as CnC points. Protecol abuse/ anomaly Identify and block attacks that abuse protecols to try to bypass the IPS. Zero day protection Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description Gateway antimalware REDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware inflies of unlimited length and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing REDPI technology with an broad threat coverage.	SSH inspection	SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH.	
Protection based on countermeasures The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilitiand exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bypass the IPS. Protoct your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Intrusion prevention		
and exploits, thus covering a wide range of attacks and vulnerabilities. Automatic updates of definitions The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC) Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagators or known as CnC points. Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bypass the IPS. Perotect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description Gateway antimalware RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams . CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Benefit	Description	
more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service. It strengthens internal security by segmenting the network into multiple security zones with intrusion prevent the spread of threats from one zone to another. Detection and blocking of command and control (CnC)	Protection based on countermeasures	The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits, thus covering a wide range of attacks and vulnerabilities.	
threats from one zone to another. Detection and blocking of command and control (CnC) activities from botnet attacks Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bypass the IPS. Zero day protection Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description Gateway antimalware RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams . CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage.	Automatic updates of definitions	The SonicWall Capture Labs Threat Research team investigates and implements IPS countermeasures, continually updating a long list covering more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service.	
activities from botnet attacks malware propagators or known as CnC points. Protocol abuse / anomaly Identify and block attacks that abuse protocols to try to bypass the IPS. Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams . CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	IPS protection between zones		
Zero day protection Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams . CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the			
individual exploits. Anti-evasion technology Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion technique at Layers 2-7. Threat prevention Benefit Description RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Protocol abuse / anomaly	Identify and block attacks that abuse protocols to try to bypass the IPS.	
Threat prevention Benefit Description RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Zero day protection		
Benefit Description RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. 24 hour security updates New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Anti-evasion technology	Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion techniques at Layers 2-7.	
RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Threat prevention		
and size on all TCP ports and streams. CloudAV antimalware protection SonicWall cloud servers have a database of more than 20 million threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. 24 hour security updates New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Benefit	Description	
capabilities of the integrated definition database, providing RFDPI technology with an broad threat coverage. 24 hour security updates New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the	Gateway antimalware	RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams.	
	CloudAV antimalware protection		
	24 hour security updates		



Tourishment Control Congression Despite one of St. Inspection (Congression) Despite ordered in proof Despite ordered in pr		
Perspitan and SIL risportion Control	Threat Prevention (cont.)	
personant III in and control protection in growth in section for every protection and makes an expension of the internal control protection and makes and ma	Benefit	Description
Elevelar porceased support Elevelar porce	Decryption and SSL inspection	application, URL and content control policies to provide protection against threats hidden in SSL-encrypted traffic. This feature is included with
Application intelligence and service Finediate ministrance and service Commission of the control of the contr	Bidirectional TCP Inspection (Raw)	
Control applications or individual applications, or individual application functions, identified by the RTDFI engine by maching against a growing database of more than 350 application report offencions, with the road of increasing interactives become and productive. Control applications for an engine of production of the private of productions of particulars and applications in your network.	Broad protocol support	
Costerol applications, or inflicional applications, control applications for inflicions, with the goal of increasing entends according an expension of productions, with the goal of increasing entends according an expension of applications according an expension of applications according and according entends according an expension of applications according and according entends according an expension of applications according and according entends. Application translation for greater certex of your related. Application translation for greater certex of your related. Application translation according according to a management of the according applications or categories according to a production according to a supplication and a range of accircin with complete scene identification via SSO directly. DLAP / AD / Terminal Services / Disk integration. Control filters Entering Protoco according to supplications and block accords to website that control unaccording to reproductive information or integree with Control applications and block according to the control of according to the protocol ac	Application intelligence and control	
Ceston application derinflication Control caption applications by creating derinform beased on specific parameters or patterns unique to an application in your network communications for agreed the control of your network control applications for the control of your network control applications for an application of the control applications or categories of applications, while limiting non-essential application halfs. Control applications for profit comprisement of an application of categories of applications, while limiting non-essential applications with communications. Control applications for a specific comprisement of an application of categories of applications, while limiting non-essential application in the control applications of a specification of the SSO through LIDAP / AD. (Terminal Services / Citiz Integration. Control filtering Entering Entering Description Entering control in and out Control filtering Citizent Control filtering Citizent Control filtering Citizent Entering control in an out Control filtering Citizent Control filtering Citizent Entering control in and out Control filtering Citizent Control filtering Citizent Entering control in and out Control filtering Citizent Entering control in and out Control filtering Citizent Entering control in an out Ent	Benefit	Description
Application bandwidth management Fine-ture and regulate available bendwidth for original applications, while limiting non-essential application traffic. Grandar control Cont	App control	
Central applications for specific components of an application) based on schedulies, user groups, exclusion lists, and a range of actions with complete user identification via SSO through LDAP / AO / Terminal Services / Climic Integration. Benefit Description Filtering content in and cut Entering scription in and cut Entering Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Service. Extend your policy enforcement to block internet content on devices outside the fervall permater with the Content Princing Services. Further of enducational services. Let teachers choose from hundreds of thousands of fee Yeal labe EDU educational violetics, organized by subject and course, and ballotred to common educational standards. Entering Description Entering Description Description Description Description Description Description Make sure that discription and destinate, such as the first layer of deforms at the permater, along with endpoint protection, to block viruses the permaters your network through ballotes. It shart drives, and other unproduced by systems. Automated application option Make sure that discription and destinates can adher unproduced by systems. United principles of the permaters of the services to improve end-user productivity and reduce exception from the course of the permaters to improve end-user productivity and reduce exception from the course of the permaters of desktops. Precuted ex	Custom application identification	
Content filtering Filtering content in and cut Enforce acceptable use policies and block access to websites that contain unacceptable or unproductive information or images with Content Filtering Center Filtering Center Filtering Center Filtering Center Filtering Center Secretary (Center Filtering Center) Book content using the prodefined collegories or any combination of categories. Filtering can be schoolated by time of day, for example during work or school hours, and applied to inclined users or groups. You Tube for educational centers Let leachers choose from hundreds of thousands of free You Tube EDU educational videos, organized by subject and course, and fabriced to common educational standards. Web carding Let leachers choose from hundreds of thousands of free You Tube EDU educational videos, againsteed by subject and course, and fabriced to common educational standards. Web carding Reflection of the Society of the Society of Society (Center) Enforced And-More and Anti-Soyowan Enforced And-More and Anti-Soyowan Enforced And-More and Anti-Soyowan Describtion Use firewall features, such as the first layer of defense at the parmeter, along with endpoint protection, to block viruses that peneturals your network through laptops, flash drives, and other unprotected systems. Automated application option Mee sum that all computers accessing the network have the latest version of the antivitus and antispoyeare definitions installed and activited. This eliminates the costs bytically associated with managing entirus and antispoyeare definitions installed and activited and septoyment option Anderhands and entipoyeare speciation of a full state of spyware programs on desktops and laptops before they are an anti-installation and deployment option. The convertil appears protection regards to end interess and allocks the installation of a full state of spyware programs on desktops and laptops before they are arranged regarding Protection against a consisting in the converting through the spyware prote	Application bandwidth management	Fine-tune and regulate available bandwidth for critical applications or categories of applications, while limiting non-essential application traffic.
Benefit Description Filtering content in and out Enforce acceptabilities and block access to websiles that contain unacceptable or unproductive information or images with Content Filtering Clients. Granular controls Enforce acceptabilities policies and block access to websiles that contain unacceptable or unproductive information or images with Content Filtering Clients. Granular controls Electroceptive Interior of Productive Interior of Content Filtering Clients. Vol Tube for educational centers Let teachers choose from hundreds of thousands of free YouTube EDU educational videos, organized by subject and course, and tailored to common educational standards. Web carding URL desplication are cached in the SonicWall freewark, reducing the response time for subsequent access to frequently visited siles to just a facilities of a second. Enforced Anti-Vitus and Anti-Signore Description Protection at various levels Description Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the code to provide signory associated with managing antivirus and antispyware profusions for decistages. Automated installation and deployment option The powerful applyware updates are delivered transparently to all desktops and file servers to improve end user productivity and reduce a covery transparent protection Automated installation and deployment and deploy	Granular control	
Enforce acceptable use policies and block access to websites that contain unacceptable or unproductive information or images with Content Filtering Service. Extend you public enforcement to block internation center or devices outside the firmwall perimeter with the Content Filtering Service. Extend you public enforcement to block internation centers or devices outside the firmwall perimeter with the Content standard controls Block content using the predictined categories or any contentation of categories. Filtering can be scheduled by time of day, for example during work or school outside. and explored to individual users or groups, and perimeter of the individual users or groups, and perimeter of the original users or groups. The perimeter is the content of the school of th	Content filtering	
Content Filtering Service. Extend your policy enforcement to block internet content on devices outside the firewall perimeter with the Content Filtering Client. Granular controls Bock content using the predefined calegories or any combination of calegories. Filtering can be scheduled by time of day, for example during work or school hours, and applied to individual users or groups. VouTube for educational centers Let seachers choose from hundreds of thousands of free YouTube EDU educational videos, organized by subject and course, and tailored to common deducational standards. Verb caching Let cash the control of the sea of the control of the caching the response time for subsequent access to frequently visited after to just a fraction of a second. Enforced Anti-Virus and Anti-Sipyssare Benefit Description Verb cotion at various levels Let forest features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through laptages, filtanh drives, and other unprotected systems. Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs byocally associated with managing arthrins and antispyware solutions for desktops. Automated installation and deployment option Antispyware protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce secontly management tasks. The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmitted automative data, helping to increase the security and performance of desktops. Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Syn flood protection agai	Benefit	Description
YouTube for educational centers Let teachers choose from hundreds of thousands of free YouTube EDU educational videos, organized by subject and course, and tailored to common educational standards. Web caching URL classifications are cached in the SonicWall firewall, reducing the response time for subsequent access to frequently visited sites to just a fraction of a second. Enforced Anti-Yrus and Anti-Styware Benefit Description Protection at various levels Use firewall features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through laptose, flash drives, and other unprotected systems. Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Makehine-be-machine deployment and installation of antivirus and antispyware clients occurs automatically across the network minimizing administrative overhead. Uninterrupted, automatic virus protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful apyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Frevail and disteromestion Frescall and disteromestion Practice inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. SyrV flood protection provides a defense against DOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Spost for IPv6 Integration of Delit X Series Switches Management	Filtering content in and out	Content Filtering Service. Extend your policy enforcement to block Internet content on devices outside the firewall perimeter with the
web caching Lett. classifications are cached in the SonicWall frewall, reducing the response time for subsequent access to frequently visited sites to just a fraction of a second. Enforced Anti-Xirus and Anti-Spyware Benefit Description Description Automated application option Wall frewall features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through papers, flesh drives, and other unprotected systems. Automated application option Makes sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware clients occurs automatically across the network, minimizing administrative overhead. Uninterrupted, automatic virus protection Frequent antivirus and antistryware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Frewall and introconcator Frewall and introconcator Syn flood protection against All network traffic is inspected, analyzed, and subject to frewall access policies. Syn flood protection against DOS / DOS attacks by using level 3 (GYN proxy) and level 2 (GYN) blacklisting technologies. It also offers protection against DOS / DOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. I	Granular controls	
Enforced Anti-Virus and Anti-Spyware Benefit Description Protection at various levels Description Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware solutions for desktops. Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware solutions for desktops. Automated installation and deployment option Automatic virus protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Firewall and interconnector Preval and interconnector Preval and interconnector Solos / DOS attacks Obscription All network traffic is inspected, analyzed, and subject to firewall access policies. Syn flood protection provides a defernse against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DOS attacks through UDP / ICMP flood protection rate limiting functions. Society IDS / IDS attacks through UDP / ICMP flood protection and connection rate limiting functions. Internet Protocol Version 6 (IPV6) is in the early stages of replacing IPV4. With the latest SonicOS operating system, the hardware will support inflering implementations. Integration of Delt X Series Switches Management of additional ports security settings, including POE and POE+, from a single conso	YouTube for educational centers	
Benefit Description Protection at various levels Use firewall features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through laptops, flash drives, and other unprotected systems. Automated application option Make sure that all computers accessing the network have the latest version of the artivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Administrative overhead. Uninterrupted, automatic virus protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Prevail and interconnection Benefit Description All network traffic is inspected, analyzed, and subject to firewall access policies. Dos/ DOS attacks Syn flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options Sonic/Wall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE	Web caching	
Protection at various levels Use firewall features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through laptops, flash drives, and other unprotected systems. Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware citents occurs automatically across the network, minimizing administrative overhead. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Frevall and interconnection Benefit Description Oynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to frewall access policies. SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Spoil Wall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Enforced Anti-Virus and Anti-Spyware	
Automated application option Make sure that all computers accessing the network have the latest version of the antivirus and antispyware definitions installed and activated. This eliminates the costs typically associated with managing antivirus and antispyware solutions for desktops. Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware clients occurs automatically across the network, minimizing administrative overhead. Uninterrupted, automatic virus protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Firewall and interconnection Benefit Description John Company of the protection against of the protection against of the protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall Tz series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a Tz series dashboard with an X	Benefit	Description
Automated installation and deployment option Machine-to-machine deployment and installation of antivirus and antispyware clients occurs automatically across the network, minimizing administrative overhead. Uninterrupted, automatic virus protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Firewall and interconnection Benefit Description Junatic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DOS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Protection at various levels	
Antispyware protection Frequent antivirus and antispyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Firevall and interconnection Benefit Description Joyamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Automated application option	
Security management tasks. Antispyware protection The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops. Firewall and interconnection Benefit Description Dynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DoS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDOS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Automated installation and deployment option	
Firewall and interconnection Benefit Description Dynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DDoS / DOS attacks Syn flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Uninterrupted, automatic virus protection	
Description Dynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DDoS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Antispyware protection	
Dynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DDoS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Firewall and interconnection	
Dynamic packet inspection Protection against All network traffic is inspected, analyzed, and subject to firewall access policies. DDoS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Benefit	Description
DDoS / DOS attacks SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also offers protection against DOS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions. Flexible deployment options SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes. Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X		
Support for IPv6 Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With the latest SonicOS operating system, the hardware will support filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X		SYN flood protection provides a defense against DOS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklisting technologies. It also
filtering implementations. Biometric authentication for remote access It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Flexible deployment options	SonicWall TZ series products can be implemented in traditional NAT mode and in Layer 2 Bridge, Wire Mode, and Network Tap modes.
authenticate the identity of the user so that they can access the network. Integration of Dell X Series Switches Management of additional ports security settings, including POE and POE +, from a single console using a TZ series dashboard with an X	Support for IPv6	
	Biometric authentication for remote access	
	Integration of Dell X Series Switches	



Firewall and Interconnect (cont.)		
Benefit	Description	
High availability	The SonicWall TZ500 and SonicWall TZ600 models offer support for active / standby high availability configurations with state synchronization. The SonicWall TZ300 and SonicWall TZ400 models support high availability configurations without active / standby synchronization. SonicWall SOHO models do not have high availability.	
Threat API	Allows the firewall to receive any proprietary intelligence information from original equipment manufacturers or third-party to combat advanced threats such as zero-day attacks, malicious internal users, compromised credentials, ransomware, and advanced persistent threats.	
Wireless network security	IEEE 802.11ac wireless technology is capable of delivering up to 1.3 Gb / s of wireless performance with increased range and reliability. Available on SonicWall models from the TZ300 series to the TZ600. 802.11 a / b / g / n connectivity is available as an option on SonicWall SOHO models.	
Management and reports		
Benefit	Description	
Global management system	SonicWall GMS monitors and configures multiple Dell SonicWall devices and X-series switches and reports on them through a single management console with an intuitive interface to reduce management costs and complexity.	
Powerful individual device management	An intuitive web-based interface enables quick and easy setup. In addition, it offers a comprehensive command-line interface and SNMPv2 / 3 support.	
IPFIX / Netflow reports of application flows	Export application traffic analysis and usage data using IPFIX or NetFlow protocols to monitor and report in real time and old data with tools such as SonicWall GMSFlow Server or other compatible with IPFIX and NetFlow with extensions.	
Virtual private networks		
Benefit	Description	
VPN with automatic provisioning	Simplify and minimize the complexity of distributed firewall deployments by automating the initial provisioning of the end-to-end VPN gateway between SonicWall firewalls, while the security and connectivity systems work instantly and automatically.	
IPSec VPN for inter-site connectivity	High-performance IPSec VPN enables the SonicWall TZ series to act as a VPN concentrator for thousands of other large sites, branch offices, or home offices.	
Remote access via SSL VPN or IPSec client	It enables the use of clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to e-mails, 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 automatic reconnection and recovery of all VPN sessions.	
Routing-based VPN	Dynamic routing over VPN links ensures uninterrupted service in the event of failure temporary VPN tunnel, as traffic between endpoints can easily be re-routed through alternate routes.	
Contextual / content recognition		
Benefit	Description	
Tracking user activity	Thanks to the seamless integration of SSO functions with AD / LDAP / Citrix1 / Terminal Services, in combination with the extensive information provided by the DPI, it is possible to identify users and their activities.	
GeoIP - Identification of traffic based on country	Identify and monitor network traffic to or from specified countries to provide protection against attacks from threats of known or suspected origin, or to investigate suspicious traffic originating from the network.	
DPI filtering of regular expressions	Prevents data leakage by identifying and controlling content that traverses the network through regular expression matching.	



SonicOS Capabilities Overview

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
- Threat API

Decryption and SSL / SSH inspection

- Deep Packet Inspection for TLS / SSL / SSH
- · Include / exclude objects, groups, or host names
- SSL control

Capture Advanced Threat Protection

- Cloud-based multi-engine analysis
- · Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Analysis of a wide variety of file types
- Automated and manual shipping
- Real-time threat intelligence updates
- Self-locking function

Intrusion prevention

- Analysis based on definitions
- Automatic updates of definitions
- Bidirectional inspection
- Capability for detailed IPS rules
- GeoIP / botnet filtering:
- Regular expression matching

Antimalware

- Stream-based malware analysis
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Bidirectional inspection
- Unlimited file size
- Malware database in the cloud

Application identification

- App control
- Viewing applications₂
- App Component Lock
- · Application bandwidth management
- Create custom application definitions
- · Data leak prevention
- Application reporting using NetFlow / IPFIX
- User Activity Tracking (SSO)
- · Complete database of application definitions

Web content filtering

- URL filtering
- Antiproxy technology
- Keyword blocking
- Bandwidth management according to CFS classification categories
- Unified Policy Model with Application Control
- · Content Filtering Client

VPN

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

Interconnection

- PortShield
- Improved protocolization
- 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 Synchronization.
- Inbound / outbound load balancing L2 bridge
- mode, NAT mode
- 3G / 4G WAN reconnection
- Common Access Card (CAC) support

Voip

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

Management and supervision

- Web GUI
- SNMPv2 / v3 Command Line Interface (CLI)
- .
- Centralized management and reporting with SonicWall GMS
- Protocolization
- NetFlow / IPFIX exports
- · Cloud-based configuration backup
- · Viewing applications and bandwidth
- IPv4 and IPv6 management
- Management of Dell X series switches, including cascade switches

Integrated wireless connection

- 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 services for guest users
- Lightweight messaging at endpoints
- Segmentation through virtual access points
- Captive portal
- ACL for cloud

Requires additional subscription



² Not available on SOHO series

High Availability with State Synchronization is only available on the SonicWall TZ500 and SonicWall TZ600 models

SonicWall TZ Series System Specifications

Hardware - Overview	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
os			SonicOS		
Security Processing Cores Interfaces	2	2	4	4	4
	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 slot expansion
Expansion	USB	USB	USB	2 USB	Expansion slot (rear), * 2 USB
Single sign-on (SSO) users VLAN interfaces	250	500	500	500	500
	25	25	fifty	fifty	fifty
Supported access points (maximum)	2	8	16	16	24
Supported Dell X-Series Switch Models	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 performance	300 Mbps	750 Mbps	1,300 Mbps	1,400 Mbps	1,500 Mbps
Full DPI performance 2	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Application inspection performance:	-	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
IPS performance ₂	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Anti-malware inspection performance ₂	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX performance	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
TLS / SSL decryption and inspection performance (DPI SSL):	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN performances	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 number of connections (DPI) Maximum	10,000	50,000	90,000	100,000	125,000
number of connections (DPI SSL)	100	500	500	750	750
VPN	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
VPN tunnels between sites IPSec VPN	10	10	twenty	25	fifty
clients (maximum) SSL VPN licenses	fifteen)	1 (10)	2 (25)	2 (25)	2 (25)
(maximum) Virtual Assist included	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
(maximum) Encryption / authentication	-	1 (30-day trial)	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	e Hellman Groups 1, 2, 5, 14		
Routing-based VPN Certificate			RIP, OSPF		
Support	Verisign, Thawte, Cy	bertrust, RSA Keon, Entrust, ar	nd Microsoft CA for VPN SonicV	Vall-SonicWall VPN, SCEP	
VPN features	Dead Peer Detection,	DHCP over VPN, IPSec NAT	Fraversal, redundant VPN gate routing	way, VPN based	
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 bits, Windows 10				
NetExtender	32/64-bit Microsoft Window	s Vista, Windows 7, 32/64-bit V 10.4+, Linu	Vindows 8.0, 32/64-bit Window x FC3 + / Ubuntu 7 + / OpenSUS		
Mobile Connect	Apple® iO	S, Mac OS X, Google® Android	™, Kindle Fire, Chrome, Wind	dows 8.1 (built-in)	
Security services	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Deep Packet Inspection Content Filtering		Gateway Anti-Virus, Anti	-Spyware, Intrusion Prevention	, DPI SSL	
Service (CFS) Services	HTTP URL, HTTPS IP,	HTTP URL, HTTPS IP, content and keyword analysis, full filtering based on file types such as ActiveX, Java, cookies for privacy, allow / deny lists			
Enforced Client Anti-Virus and Anti-Spyware	McAfee « and Kaspersky ~				
Comprehensive Anti-Spam Service	Supported				
					i contraction of the contraction
Viewing applications	No	Yes	Yes	Yes	Yes
Viewing applications App control	No Yes	Yes Yes	Yes Yes	Yes Yes	Yes Yes



SonicWall TZ Series System Specifications (cont.)

Interconnection	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
IP address assignment NAT modes	Sta	atic, (DHCP, PPPoE, L2TP an	d 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 OSPF, RIPv1 / v2, static routes, policy-based routing				
QoS	Bandwidth priority, maxim	um bandwidth, guaranteed ba	andwidth, DSCP marking, 802	.1e (WMM)	
Authentication	LDAP (multiple domains), XAUTH / RADIUS, SSO, Novell, base of user data internal	LDAP (multiple domains).	, XAUTH / RADIUS, SSO, No Terminal Se	vell, internal user database, rivices, Citrix	
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, L2	TP, PPTP, RADIUS, IEEE 802.3	
Certifications	FIPS 140-2 (with	Suite B) level 2, UC APL, VP	NC, IPv6 (phase 2), ICSA Netw	ork Firewall, ICSA Anti-virus	
Certifications pending			Common Criteria NDPP		
Common Access Card (CAC) High availability	No	Active / standby	Supported Active / standby	Active / standby with synchronization of State	Active / standby with state sync
Hardware	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Form factor			Desktop PC		
Power supply (W) Maximum power	24 W (external)	24 W (external)	24 W (external)	36 W (external)	60W (external)
consumption (W) Input power	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
		10	0 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	3.6 x 14.1 x 19 cm	3.5 x 13.4 x 19 cm	3.5 x 13.4 x 19 cm	3.5 x 15 x 22.5 cm	3.5 x 18 x 28 cm
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	0.92kg / 2.03lbs 1.05kg / 2.31lbs	1.47 kg / 3.24 pounds
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	1.34kg / 2.95lbs 1.48 kg / 3.26 pounds	1.89 kg / 4.16 pounds
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	1.93kg / 4.25lbs 2.07 kg / 4.56 pounds	2.48kg / 5.47lbs
MTBF (years)	58.9 / 56.1 (wireless)	56.1	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	SOHO series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Regulatory model (wired)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
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	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	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	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	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL, cUL, TUV / GS, CB, Certified compliance for Mexico by UL, WEEE, REACH, KCC / MSIP
Regulatory model (wired)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Compliance with the main regulatory rules (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	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,	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,	



SonicWall TZ Series System Specifications (cont.)

Wireless connection integrated	SOHO series	TZ300, TZ400 and 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 bandss	802.11a: 5180-5825 GHz; 802.11b / g: 2412-2472 GHz; 802.11n: 2412-2472 GHz, 5180-5825 GHz;	802.11a: 5180-5825 GHz; 802.11b / g: 2412-2472 GHz; 802.11n: 2412-2472 GHz, 5180-5825 GHz; 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz	-
Operational channels	802.11a: Canada and US 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b / g: 1-11, Europe 1-13, Japan 1-14 (14 only 802.11b); 802.11n (2.4 GHz); Canada and USA 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz); Canada and USA 36-48 / 149-165, Europe 36-48, Japan 36-48, Spain 36-48 / 52-64;	802.11a: Canada and US 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b / g: 1-11, Europe 1-13, Japan 1-14 (14 only 802.11b); 802.11n (2.4 GHz): Canada and US 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): Canada and USA 36-48 / 149- 165, Europe 36-48, Japan 36-48, Spain 36-48 / 52-64; 802.11ac: Canada and US 36-48 / 149-165, Europe 36-48, Japan 36-48, Spain 36-48 / 52-64	-
Transmission output power	It is based on the normative domain specified by the system administrator	It is based on the normative domain specified by the system administrator	-
Transmission power control	Supported	Supported	-
Speeds supported transfer	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mb / s per channel; 802.11b: 1, 2, 5.5, 11 Mb / s per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb / s 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 Mb / s per channel;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mb / s per channel; 802.11b: 1, 2.5, 11 Mb / s per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb / s 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 Mb / s 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 Mb / s per channel	-
Spectrum of the technology of modulation	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	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: Division multiplexing	-
	(OFDM)	orthogonal frequencies (OFDM)	

- . Full DPI / Gateway AV / 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.

 JVPN performance measurement based on UDP traffic with 1280-byte packets in accordance with RFC 2544. Specifications, capabilities, and availability are subject to change.
- BGP is only available on the SonicWall TZ400, TZ500, and TZ600.
- All integrated wireless TZ models can support 2.4GHz or 5GHz bands. For dual band support, use SonicWall wireless access point 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 of TotalSecure SonicWall	01-SSC-0653
TZ300 with 1 year of TotalSecure	01-SSC-0581
SonicWall TZ300 Wireless-AC with 1 year of TotalSecure SonicWall	01-SSC-0583
TZ400 with 1 year of TotalSecure	01-SSC-0514
SonicWall TZ400 Wireless-AC with 1 year of TotalSecure SonicWall	01-SSC-0516
TZ500 with 1 year of TotalSecure	01-SSC-0445
SonicWall TZ500 Wireless-AC with 1 year of TotalSecure SonicWall	01-SSC-0446
TZ600 with 1 year of TotalSecure	01-SSC-0219
High availability options (all drives must be the same model)	
SonicWall TZ500 with high availability	01-SSC-0439
SonicWall TZ600 with high availability	01-SSC-0220



Test methods: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

SonicWall TZ Series Ordering Information

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) Content Filtering	01-SSC-0670
Service (1 year)	01-SSC-0676
Comprehensive Anti-Spam Service (1 year) 24x7	01-SSC-0682
Support (1 year)	01-SSC-0700
For SonicWall TZ300 series	
Advanced Gateway Security Suite - Capture ATP, Threat Prevention,	01-SSC-1430
content filtering and 24x7 support for TZ300 (1 year)	
Capture Advanced Threat Protection for TZ300 (1 year)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 year) Content Filtering	01-SSC-0602
Service (1 year)	01-SSC-0608
Comprehensive Anti-Spam Service (1 year) 24x7	01-SSC-0632
Support (1 year)	01-SSC-0620
For SonicWall TZ400 series	
Advanced Gateway Security Suite - ATP Capture, 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) Content Filtering	01-SSC-0534
Service (1 year)	01-SSC-0540
Comprehensive Anti-Spam Service (1 year) 24x7	01-SSC-0561
Support (1 year)	01-SSC-0552
For SonicWall TZ500 series	
Advanced Gateway Security Suite - ATP Capture, 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) Content Filtering	01-SSC-0458
Service (1 year)	01-SSC-0464
Comprehensive Anti-Spam Service (1 year) 24x7	01-SSC-0482
Support (1 year)	01-SSC-0476
For SonicWall TZ600	
Advanced Gateway Security Suite - ATP Capture, 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) Content Filtering	01-SSC-0228
Service (1 year)	01-SSC-0234
Comprehensive Anti-Spam Service (1 year) 24x7	01-SSC-0252
Support (1 year)	01-SSC-0246

About us

SonicWall has been fighting the cybercrime industry for over 25 years, defending small, medium and large businesses around the world. Our combination of products and partners has enabled us to create a real-time cyber defense solution tailored to the specific needs of more than 500,000 global businesses in more than 150 countries, so you can fully focus on your business without having to worry about the threats.

registered trademarks are the property of their respective owners.

© 2017 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and / or its affiliates in the US and / or other countries. All other trademarks and

