SonicWALL TZ Series

Unified Threat Management

- Built on the proven security architecture of SonicOS, the TZ Series provides **highly effective anti-malware and intrusion prevention** to keep networks safe from sophisticated modern threats.

- **Highly secure SSL VPN remote access** is available natively for Apple iOS, Google Android, Windows, Mac OS and Linux based devices to unleash the potential of a mobile workforce.

- SonicWALL content and URL filtering **blocks multiple categories of objectionable web content** to enable high workplace productivity and reduce legal liability.

- Easy to comprehend and quick to deploy, the graphical user interface in the TZ Series **eliminates the choice between ease-of-use and power,** driving down total cost of ownership.

The SonicWALL® TZ Series is the most secure Unified Threat Management (UTM) firewall for small businesses, retail deployments, government organizations, remote sites and branch offices. Unlike consumer-grade products, the TZ Series delivers the most effective anti-malware, intrusion prevention, content/URL filtering and application control capabilities along with the broadest most secure mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enabling organizations to realize increased productivity gains. The TZ Series is the most secure, sophisticated and widely-deployed security platform on the market today.

Additionally, the SonicWALL Application Intelligence and Control capabilities in the TZ 215 ensures that bandwidth is available for business-critical applications while throttling or blocking unproductive applications. The TZ 215 also offers advanced application traffic analytics and reporting for deep insight into bandwidth utilization and security threats.

The TZ Series includes additional advanced networking features such as IPSec and SSL VPN, multiple ISP failover, load balancing, optional integrated 802.11n wireless and network segmentation, and also enables PCI compliance. The TZ Series is the only available UTM firewall that provides native VPN remote access client for Apple® iOS, Google® Android™, Windows, Mac OS and Linux. This unique client also supports Clean VPN™, which decontaminates threats from VPN traffic. Providing the most secure support for mobile platforms, only SonicWALL delivers full malware scanning of SSL encrypted traffic and application control for Android and iOS devices.

The new TZ Series is an elegant integration of multiple point products, combined into a single solution providing value while reducing complexity

About SonicWALL
Guided by its vision of Dynamic Security for the Global Network, SonicWALL develops advanced intelligent network security and data protection solutions that adapt as organizations and threats evolve. SonicWALL designs award-winning hardware, software and virtual-appliance solutions to detect and control applications and protect networks from intrusions and malware attacks. SonicWALL is trusted by small businesses and large enterprises worldwide. Since 1991, it has shipped over two million appliances through its global network of channel partners to keep tens of millions of business computer users safe and in control of their data.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL Architecture

The SonicWALL TZ 205 and TZ 215 feature dual-core Cavium CPUs, which process parallel data streams simultaneously, increasing overall protection and performance. Dual-core technology offers superior performance, scalability, and energy efficiency when compared with network security platforms based on general-purpose processors with separate security co-processors, or Application-Specific Integrated Circuits (ASIC), which can't keep up with evolving complex attacks in real time from both inside and outside the network perimeter. The advanced high performance dual-core architecture makes the TZ Series the fastest solution in its class, with performance levels of up to 500 Mbps of stateful throughput, 110 Mbps deep packet inspection throughput and 130 Mbps 3DES or AES VPN throughput.
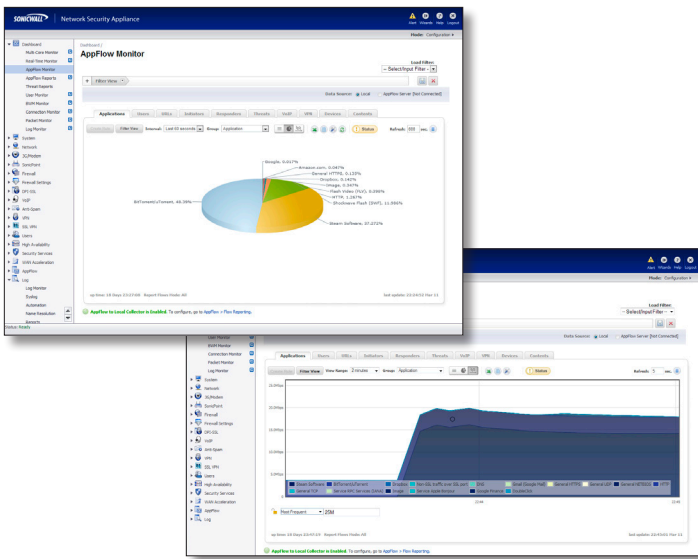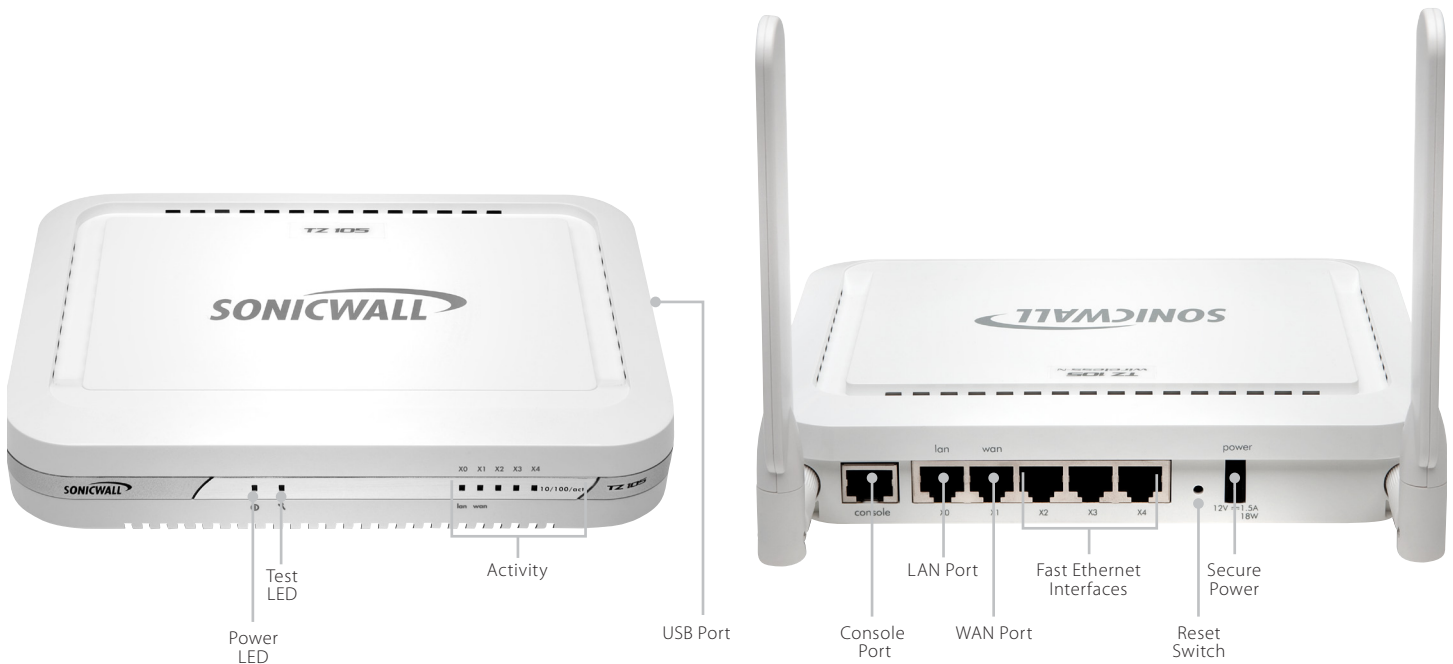
SonicOS Software

SonicWALL's patented Reassembly-Free Deep Packet Inspection® (RFDPI) technology enables simultaneous, multi-threat and application scanning and analysis of unlimited files sizes and connections at extremely high speeds. This single code base is at the core of every SonicWALL firewall, from the TZ 105 to the SonicWALL SuperMassive E10800. SuperMassive E10800 with SonicOS is the highest overall protection Next-Generation Firewall to earn the NSS Labs *Recommend* rating. RFDPI is tightly integrated into the firewall platform, streamlining management of granular firewall policies, directly via the firewall interface or via the SonicWALL Global Management System. Organizations can choose from an entire line of proven SonicWALL firewalls with SonicOS, which massively scale to meet the needs of the highest performance networks.

	TZ 105 Series	TZ 205 Series	TZ 215 Series
Firewall Overview			
Stateful Packet Inspection Firewall Throughput	200 Mbps	500 Mbps	500 Mbps
IPS Throughput	60 Mbps	80 Mbps	110 Mbps
GAV Throughput	40 Mbps	60 Mbps	70 Mbps
VPN Throughput	75 Mbps	100 Mbps	110 Mbps
Full DPI (UTM)	25 Mbps	40 Mbps	60 Mbps
Maximum UTM/DPI Connections	8,000	12,000	32,000
Unlimited File Size Protection	✔	✔	✔
Hardware			
Dual Core Processor		✔	✔
Gigabit Ethernet		✔	✔
802.11n Support	✔	✔	✔
Dual Band 802.11 a/b/g/n Support		✔	✔
Security Services			
Intrusion Protection*	✔	✔	✔
Gateway Anti-Virus, Anti-Spyware and Cloud AV*	✔	✔	✔
Content and URL Filtering (CFS)*	✔	✔	✔
Enforced Client Anti-Virus and Anti-Spyware*	✔	✔	✔
Application Intelligence and Control*			✔

*Available with Subscription Service

SonicWALL TZ 105   Home Office/Small Office

Test LED

Activity

Power LED

USB Port

LAN Port

Fast Ethernet Interfaces

Secure Power

Console Port

WAN Port

Reset Switch

The new SonicWALL TZ 105 is the most secure Unified Threat Management (UTM) firewall available for small offices, home offices and small retail deployments. Unlike consumer-grade products, the TZ 105 delivers the proven, most effective intrusion prevention, anti-malware and content/URL filtering, along with the broad mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enabling organizations to realize increased productivity gains without the increased cost.
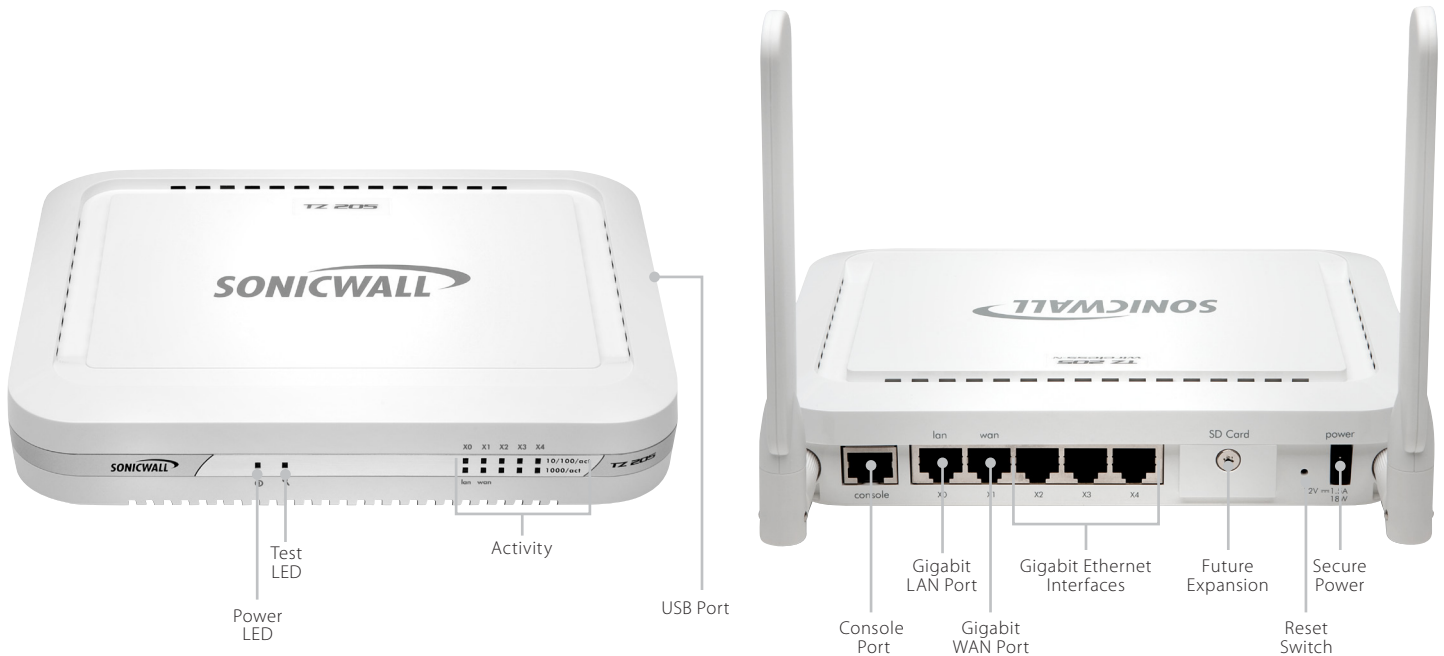
TZ 105

Internet

Home Office/Small Office LAN

Home/Work LAN
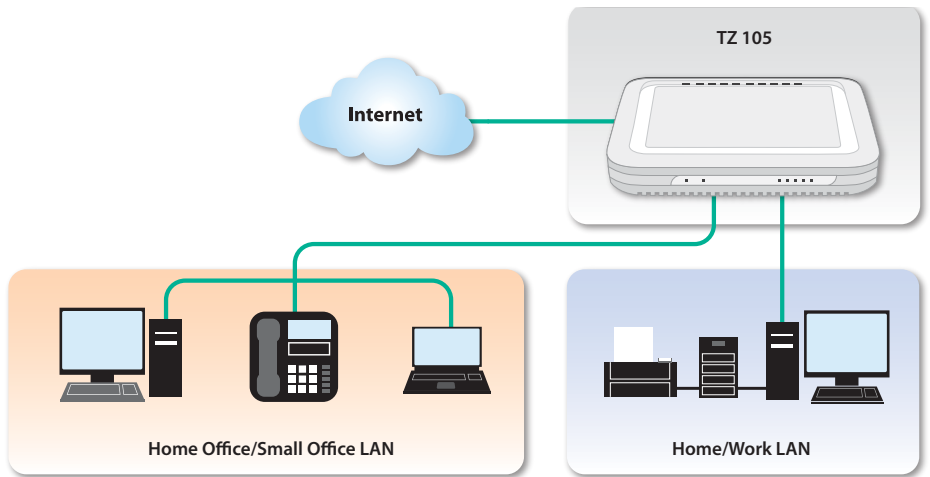
Hardware Description	SKU
TZ 105 TotalSecure 1-year	01-SSC-4906
TZ 105 Wireless-N TotalSecure 1-year	01-SSC-4908
TZ 105 Wireless-N TotalSecure International 1-year	01-SSC-4910

Service Description	SKU
Comprehensive Gateway Security Suite 1-year	01-SSC-4877
Gateway Anti-Virus and Intrusion Prevention Service 1-year	01-SSC-4844
Content/URL Filtering 1-year	01-SSC-4850
Comprehensive Anti-Spam Service 1-yea	01-SSC-4871
8x5 Support 1-year	01-SSC-4856
24x7 Support 1-year	01-SSC-4862

3

Test
LED

Activity

Power
LED

USB Port

Gigabit
LAN Port

Gigabit Ethernet
Interfaces

Future
Expansion

Secure
Power

Console
Port

Gigabit
WAN Port

Reset
Switch

Small businesses, retail deployments, government organizations, remote sites and branch offices can benefit from the powerful security and business-class performance of the new SonicWALL TZ 205. Unlike consumer grade products, this powerful Unified Threat Management (UTM) firewall combines the most effective intrusion prevention, anti-malware and content/URL filtering with the broadest, most secure mobile platform support for laptops, smartphones and tablets. By providing full deep packet inspection (DPI) at very high performance levels, it eliminates the tradeoff between comprehensive security and performance.

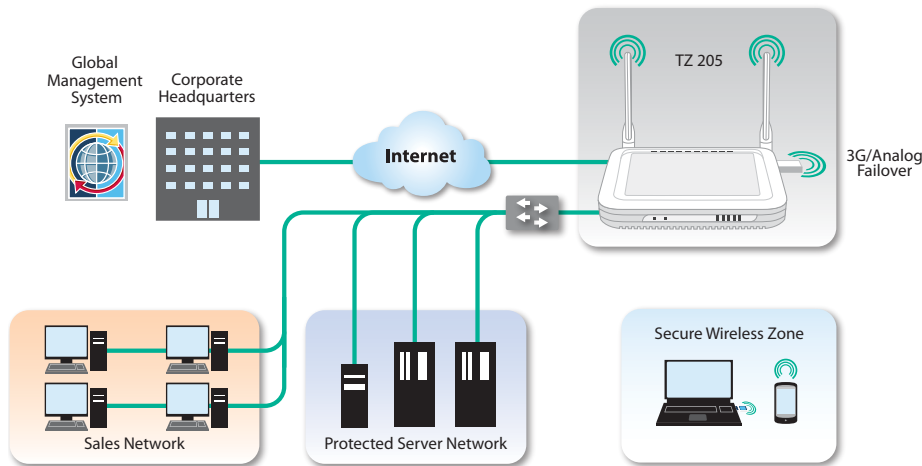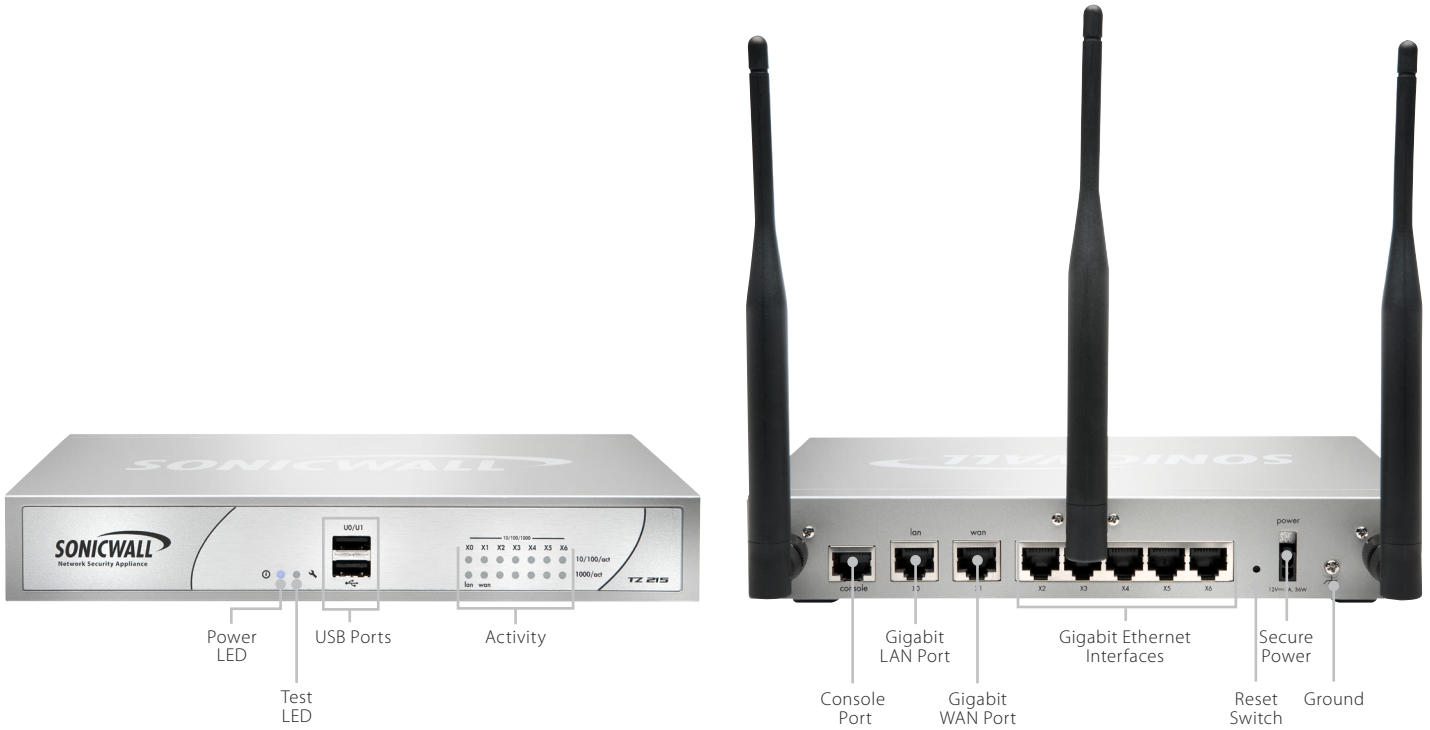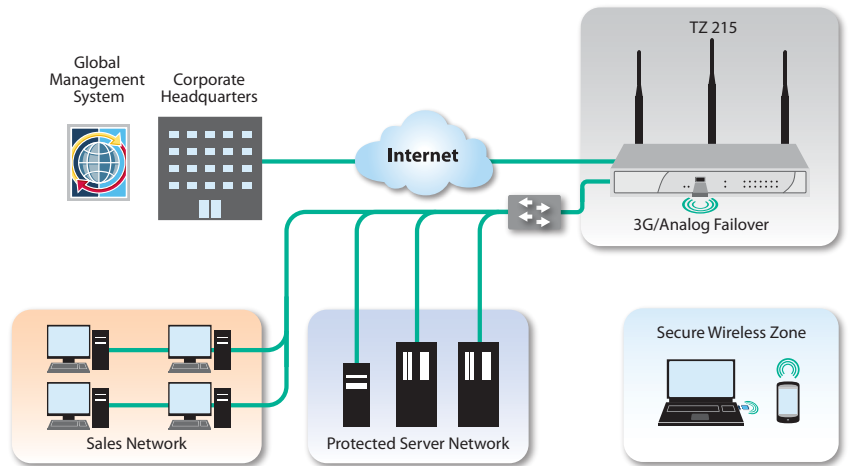| Hardware Description	SKU
TZ 205 Hardware: Wired	01-SSC-6945
TZ 205 Hardware: Wireless-N	01-SSC-6947
TZ 205 Hardware: Wireless-N International	01-SSC-4883
TZ 205 TotalSecure 1-year	01-SSC-4906
TZ 205 Wireless-N TotalSecure 1-year	01-SSC-4908
TZ 205 Wireless-N TotalSecure International 1-year	01-SSC-4910

Service Description	SKU
Comprehensive Gateway Security Suite 1-year	01-SSC-4838
Gateway Anti-Virus and Intrusion Prevention Service 1-year	01-SSC-4799
Content/URL Filtering 1-year	01-SSC-4805
Comprehensive Anti-Spam Service 1-year	01-SSC-4832
8x5 Support 1-year	01-SSC-4811
24x7 Support 1-year	01-SSC-4817

Power LED | USB Ports | Activity

Test LED

Console Port | Gigabit LAN Port | Gigabit WAN Port | Gigabit Ethernet Interfaces | Reset Switch | Secure Power | Ground

The new SonicWALL TZ 215 is the most secure, highest performance Unified Threat Management (UTM) firewall available for small businesses and branch offices. Designed for small businesses, distributed enterprises, branch offices and retail deployments, the TZ 215 integrates anti-malware, intrusion prevention, application control and URL filtering, driving down cost and complexity. It provides a dual-core architecture delivering full deep packet inspection (DPI) without diminishing network performance, thus eliminating bottlenecks that other products introduce, enabling businesses to realize increased productivity gains. The TZ 215 also provides application control to ensure bandwidth for critical applications, while throttling non-productive ones. Advanced networking features include multiple ISP failover and load balancing, optional dual-band secure wireless, IPSec VPN support, network segmentation and PCI compliance capabilities.

Hardware Description	SKU
TZ 215 Hardware: Wired	01-SSC-4976
TZ 215 Hardware: Wireless-N	01-SSC-4977
TZ 215 Hardware: Wireless-N International	01-SSC-4969
TZ 215 TotalSecure 1-year	01-SSC-4982
TZ 215 Wireless-N TotalSecure 1-year	01-SSC-4984
TZ 215 Wireless-N TotalSecure International 1-year	01-SSC-4986

Service Description	SKU
Comprehensive Gateway Security Suite 1-year	01-SSC-4793
Gateway Anti-Virus and Intrusion Prevention Service 1-year	01-SSC-4757
Content/URL Filtering 1-year	01-SSC-4763
Comprehensive Anti-Spam Service 1-year	01-SSC-4787
8x5 Support 1-year	01-SSC-4769
24x7 Support 1-year	01-SSC-4775

Features

Intrusion Prevention

Signature-based Scanning	Tightly integrated, signature-based intrusion prevention scans packet payloads for vulnerabilities and exploits that target critical internal systems.
Automatic Signature Updates	SonicWALL's Research Team continuously updates and deploys an extensive list of over 5,400 IPS signatures covering 52 attack categories. These signatures take immediate effect and do not require reboots or any other interruption in service.
Outbound Threat Prevention	The ability to inspect both inbound and outbound traffic ensures that the network will not unwittingly be used in Distributed Denial of Service attacks and will prevent any Command and Control Botnet communication.
Intra-Zone IPS Protection	Intrusion prevention can be deployed between internal security zones to protect sensitive servers and to prevent internal attacks.

VPN

IPSec VPN for Site-to-site Connectivity	High-performance IPSec VPN allows the firewall to connect remote branch offices to a central location.
SSL VPN or IPSec Client Remote Access	Utilize clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN Gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure by seamlessly re-routing traffic between endpoints through alternate routes.
Clean VPN	SonicWALL Clean VPN™ both secures the integrity of VPN access and decontaminates malicious threats before they can enter the corporate network.

Gateway Threat Prevention

Gateway Anti-Malware	SonicWALL's patented RFDPI engine scans all ports and protocols for viruses without file size or stream length limitation. SonicLabs Researchers constantly provide updated threat protection, providing faster response times and threat prevention.
Reassembly-Free Deep Packet (RFDPI)	Reassembly-Free Deep Packet Inspection keeps track of malware regardless of the order or inspection timing with which the packets arrive. This allows for extremely low latency while eliminating file and stream size limitations. This provides greater performance and security than outdated proxy designs which reassemble contents using sockets bolted to traditional anti-virus programs and are plagued with inefficiencies and the overhead of memory thrashing leading to high latency, low performance and size limitations.
Cloud Anti-Virus (AV)	Using the built-in RFDI engine, SonicWALL can leverage the power of the cloud to provide the most comprehensive set of anti-malware signatures available, while minimizing latency or delay. The SonicWALL Cloud Anti-Virus Service provides millions of additional malware signatures for inspection of executable files using the most up-to-date information available.
Bi-directional Inspection	RFDPI can be performed on both inbound and outbound connections to provide protection in all network traffic directions.
24x7 Signature Updates	SonicLabs Research Team team creates and updates signature databases that are propagated automatically to the firewalls in the field, with those signatures taking immediate effect without any reboot or service interruption required.

Firewall and Networking

Stateful Packet Inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DOS Attack Protection	SYN Flood protection provides defense against DOS attacks using both layer 3 SYN proxy and layer 2 SYN blacklisting technologies.
Flexible Deployment	Can be deployed in traditional NAT and Layer 2 Bridge modes.
Policy-based Routing	Create routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
High Availability	Supports Active/Passive failover to ensure increased reliability by protecting against hardware or software faults.
WAN Load Balancing	Load balance up to four WAN interfaces using Round Robin, Spillover or Percentage based methods.
WAN Acceleration	WAN Acceleration decreases latency and increases transfer speeds between remote sites for even higher network efficiency gains.

Features

VoIP

Advanced QoS	Guarantee critical communications with 802.1p and DSCP tagging and remapping of VoIP traffic on the network.
DPI of VoIP Traffic	Predefined signatures detect and block VoIP specific threats.
H.323 Gatekeeper and SIP Proxy Support	Block spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.

Management and Monitoring

Web GUI	An intuitive web-based interface allows quick and convenient configuration in addition to management through SonicWALL Global Management System (GMS®), or the CLI.
SNMP	SNMP provides the ability to protectively monitor and respond to threats and alerts.
Netflow/IPFIX	Export an extended set of data through IPFIX or NetFlow protocols for granular insight into application traffic, bandwidth utilization and security threats in addition to powerful troubleshooting and forensics capabilities. Compatible with SonicWALL Scrutinizer and third-party monitoring and reporting applications. (TZ 215 only)
Centralized Policy Management	With SonicWALL GMS, monitor, configure and report on multiple SonicWALL appliances from a single intuitive interface and customize your security environment to suit your individual policies.

Application Intelligence and Control

Application Control	Identify and control applications or individual components of an application based on RFDPI technology instead of relying on well-known ports and protocols.
Application Bandwidth Management	Allocate bandwidth to critical applications while throttling unproductive application traffic for an efficient and productive network.
Custom Application Identification	Create and configure custom application identification based on traffic parameters or on patterns unique to an application in its network communications.
Application Traffic Analytics	Provides organizations with granular insight into application traffic, bandwidth utilization and security in addition to powerful troubleshooting and forensics capabilities. (TZ 215 only)
Application Signature Database	A continuously expanding database of over 3,500 application signatures ensures that administrators are able to control the usage of all the latest applications on their network at a category or individual level.
User Activity Tracking	User identification is seamlessly integrated with Microsoft® Active Directory and other authentication systems enabling tracking and reporting of individual user identification.
GeoIP Country Traffic Identification	Identify and control network traffic going to or coming from specific countries. (TZ 215 only)

Firewall and Networking

Firewall
- Reassembly-Free Deep Packet Inspection
- Stateful Packet Inspection
- DOS Attack Protection
- TCP Reassembly
- Stealth Mode

Application Control
- Application Control
- Application Component Blocking
- Application Bandwidth Management
- Custom Application Signature Creation
- AppFlow Visualization
- Data Leakage Prevention
- IPFIX with Extensions Reporting
- User Activity Tracking
- GeoIP Country Traffic Identification
- Comprehensive Application Signature Database

Intrusion Prevention
- Signature-based Scanning
- Automatic Signature Updates
- Outbound Threat Prevention
- IPS Exclusion List
- Hyperlinked Log Messages
- Unified CFS and App Control with Bandwidth Throttling

Anti-Malware
- Stream-based Malware Scanning
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Cloud Anti-Virus Service

VoIP
- Advanced QoS
- Bandwidth Management
- DPI of VoIP Traffic
- Full Interoperability
- H.323 Gatekeeper and SIP Proxy Support

Networking
- Dynamic Routing
- Policy-based Routing
- Advanced NAT
- DHCP Server
- Bandwidth Management
- Link Aggregation
- Port Redundancy
- High Availability
- IPv6 Ready
- Load Balancing

Management and Monitoring
- Web GUI
- Command Line Interface
- SNMP
- Analyzer Reporting
- Scrutinizer Reporting
- GMS Policy Management and Reporting
- Logging
- Netflow/IPFIX
- App Visualization

- Centralized Policy Management
- Single Sign-On
- Terminal Service/Citrix Support

Security Services
- Intrusion Prevention Service
- Gateway Anti-Malware Service
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware Service – McAfee® or Kaspersky® options
- Application Intelligence, Control and Visualization Service

Specifications

Firewall	TZ 105 Series	TZ 205 Series	TZ 215 Series
SonicOS Version		SonicOS 5.8.1 and later	
Stateful Throughput[1]	200 Mbps	500 Mbps	500 Mbps
IPS Throughput[2]	60 Mbps	80 Mbps	110 Mbps
GAV Throughput[2]	40 Mbps	60 Mbps	70 Mbps
UTM Throughput[2]	25 Mbps	40 Mbps	60 Mbps
Maximum Connections[3]	8,000	12,000	48,000
Maximum UTM/DPI Connections	8,000	12,000	32,000
New Connections/Sec	1,000	1,500	1,800
Nodes Supported		Unrestricted	
Denial of Service Attack Protection		22 classes of DoS, DDoS and scanning attacks	
SonicPoints Supported	1	2	16

VPN			
3DES/AES Throughput[4]	75 Mbps	100 Mbps	130 Mbps
Site-to-Site VPN Tunnels	5	10	20
Bundled GVC Licenses (Maximum)	0 (5)	2 (10)	2 (25)
Bundled SSL VPN Licenses (Maximum)	1 (5)	1 (10)	2 (10)
Encryption/Authentication/DH Group		DES, 3DES, AES (128, 142, 256-bit), MD5, SHA-1/DH Group 1, 2, 5, 14	
Virtual Assist Bundled (Maximum)	—	1 (30-day trial)	2 (30-day trial)
Key Exchange		IKE, Manual Key, Certificates (X.509), L2TP over IPSec	
Certificate Support		Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWALL-to-SonicWALL VPN, SCEP	
VPN Features		Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN	
Global VPN Client Platforms Supported		Microsoft® Windows XP, Vista 32/64-bit, Windows 7 32/64-bit	
SSL VPN Platforms		Microsoft Windows XP/Vista 32/64-bit/Windows 7, Mac OSX 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE	
Mobile Connect Platform Supported		Apple® iOS 4.2 or higher, Google® Android™ 4.0 or higher	

Security Services			
Deep Packet Inspection Services		Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control (TZ 215 only)	
Content Filtering Service (CFS)		HTTP URL, HTTPS IP, keyword and content scanning, ActiveX, Java Applet, and cookie blocking bandwidth management on filtering categories, allow/forbid lists	
Enforced Client Anti-Virus and Anti-Spyware		McAfee® or Kaspersky®	
Comprehensive Anti-Spam Service[6]		Supported	
Application Intelligence and Control	Application Control		Application Traffic Visualization and Bandwidth Management

Networking			
IP Address Assignment		Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay	
NAT Modes		1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode	
VLANS	5, PortShield	10, PortShield	20, PortShield
DHCP		Internal server, relay	
Routing		OSPF, RIP v1/v2, static routes, policy-based routing, multicast	
Authentication		XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix	
Local User Database		150 users	
VoIP		Full H.323v1-5, SIP, gatekeeper support, outbound bandwidth management, VoIP over WLAN, deep inspection security, full interoperability with most VoIP gateway and communications devices	

System			
Zone Security		Yes	
Schedules		Yes	
Object-based/Group-based Management		Yes	
DDNS		Dynamic DNS providers include: dyndns.org, yi.org, no-ip.com and changeip.com	
Management and Monitoring		Local CLI, Web GUI (HTTP, HTTPS), SNMP v2; Global management with SonicWALL GMS	
Logging and Reporting		Analyzer, Scrutinizer, GMS, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX with Extensions, Real-time Visualization	
Hardware Failover	—	Active/Passive	Active/Passive
Anti-Spam		RBL support, Allowed/Blocked Lists, Optional SonicWALL Comprehensive Anti-Spam Service[6]	
Load Balancing		Yes, Outgoing and Incoming	
Standards		TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
WAN Acceleration Support[7]		Yes, with SonicWALL WXA Appliances	

Built-in Wireless LAN			
Standards	802.11b/g/n	802.11a/b/g/n (2x2)	802.11a/b/g/n (3x3)
Wireless Security Standards		(WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS)	
Virtual Access Points (VAPs)		Up to 8	
Antennas	Double, detachable, dual	Double, detachable, external	Triple, detachable, external
Radio Power–802.11b/802.11g/802.11n	18 dBm max/18 dBm @ 6Mbps, 15 dBm @ 54Mbps	15.5 dBm max/18 dBm max/17 dBM @ 6 Mbps, 13 dBM @ 54 Mbps	
Radio Power–802.11a/802.11b/802.11g/802.11n	—	15.5 dBm max/18 dBm max/17 dBM @ 6 Mbps, 13 dBM @ 54 Mbps	
Radio Power–802.11n (2.4GHz)/802.11n (5.0GHz)	19 dBm MCS 0, 12 dBm MCS 15	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15	
Radio Receive Sensitivity–802.11a/802.11b/802.11g	-90 dBm @ 11Mbps/-91 dBm @ 6 Mbps , -74 dBm @54 Mbps	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm @ 11Mbps/ -91 dBm @ 6Mbps, -74 dBm @ 54 Mbps	
Radio Receive Sensitivity–802.11n (2.4GHz)/802.11n (5.0GHz)	-89 dBm MCS 0, -70 dBm MCS 15	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15	

Hardware Built-in Wireless LAN			
Interfaces	(5) 10/100 Fast Ethernet, 1 USB, 1 Console	(5) 10/100/1000 Copper Gigabit, 1 USB, 1 Console	(7) 10/100/1000 Copper Gigabit, 2 USB, 1 Console
Processor	Single-Core	Dual-Core	Dual-Core
Flash Memory/RAM	32 MB/256 MB	32 MB/256 MB	32 MB/512 MB
3G Wireless/Modem[5]		Supported with approved adapters[5]	
USB Ports	1	1	2
Power Input		100 to 240 VAC, 50-60 Hz, 1 A	
Max Power Consumption	5.2W/7.0W	6.4W/10.5W	9.0W/12.0W
Total Heat Dissipation	17.8 BTU/23.7 BTU	21.9 BTU/35.8 BTU	30.6 BTU/41.4 BTU
Certifications		VPNC, ICSA Firewall 4.1	
Certifications Pending		EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2	
Form Factor and Dimensions	5.555 x 1.42 x 7.48 in (14.1 x 3.6 x 19 cm)	5.555 x 1.42 x 7.48 in (14.1 x 3.6 x 19 cm)	7.125 x 1.5 x 10.5 in (18.1 x 3.81 x 26.67 cm)
Weight	0.75 lbs/0.34 kg 0.84 lbs/0.38 kg	0.75 lbs/0.34 kg 0.84 lbs/0.38 kg	1.95 lbs/0.97 kg 2.15 lbs/0.97 kg
Major Regulatory Compliance		FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, NOM, UL, cUL, TUV/GS, CB, NOM, WEEE, RoHS	
Environment/Humidity		40-105° F, 0-40° C/ 5-95% non-condensing	
MTBF		28 years/15 years	

[1]Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. [2]UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. [3]Actual maximum connection counts are lower when DPI services are enabled. [4]VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. [5]3G card and modem are not included. See http://www.sonicwall.com/us/products/cardsupport.html for supported USB devices. [6]The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less. [7]With SonicWALL WXA Series Appliances.

ICSAlabs
CERTIFIED FIREWALL - CORPORATE

VPNC CERTIFIED

Available on the App Store

ANDROID APP ON Google play

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY   SECURE REMOTE ACCESS   WEB AND E-MAIL SECURITY   BACKUP AND RECOVERY   POLICY AND MANAGEMENT

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600   F +1 408.745.9300
www.sonicwall.com

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™