SONICWALL

SonicWall TZ670

The SonicWall TZ670 is the first desktop-form-factor next-generation firewall (NGFW) with 10 Gigabit Ethernet interfaces.

Designed for mid-sized organizations and distributed enterprise with SD-Branch locations, the TZ670 delivers industry-validated security effectiveness with best-in-class price-performance. TZ670 NGFWs address the growing trends in web encryption, connected devices and high-speed mobility by delivering a solution that meets the need for automated, real-time breach detection and prevention.

The TZ670 is highly scalable, with high port density of 10 ports. It features both in-built and an expandable storage of up to 256GB, that enables various features including logging, reporting, caching, firmware backup and more. An optional second power supply provides added redundancy in case of failure.

Deployment of TZ670 is further simplified by Zero-Touch Deployment, with the ability to simultaneously roll out these devices across multiple locations with minimal IT support. Built on next-gen hardware, it integrates firewalling and switching capabilities, plus provides single-pane-of-glass management for SonicWall Switches and SonicWave Access Points. It allows tight integration with Capture Client for seamless endpoint security.

SonicOS and Security Services

The SonicOS architecture is at the core of TZ NGFWs. TZ670 is powered by the feature rich SonicOS 7.0 operating system with new modern looking UX/UI, advanced security, networking and management capabilities. TZ670 features integrated SD-WAN, TLS 1.3 support, real-time visualization, high-speed virtual private networking (VPN) and other robust security features.

Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. As one of Capture ATP's engine, RTDMI detects and blocks malware and zero-day threats by inspecting directly in memory.

By leveraging Capture ATP with RTDMI technology, in addition to security services such as Reassembly-Free Deep Packet Inspection (RFDPI), Anti-virus and Anti-spyware Protection, intrusion prevention system, Application Intelligence and Control, Content Filtering Services, DPI-SSL, TZ series firewalls stop malware, ransomware and other advanced threats at the gateway. For more information, refer the SonicOS and Security Services Datasheet.

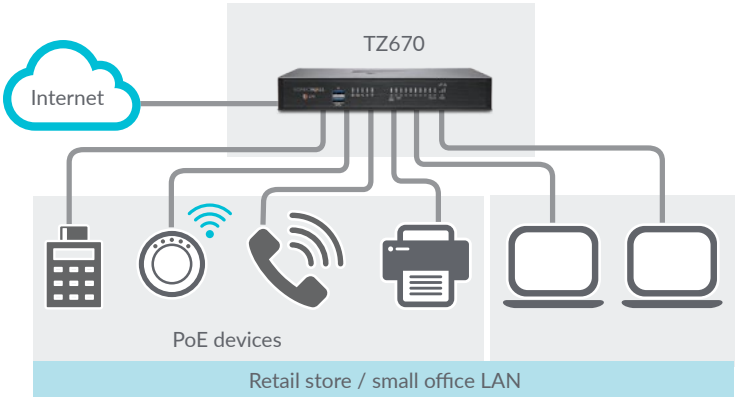
Highlights:

- 10 GbE interfaces in a desktop form factor
- SD-Branch ready
- Secure SD-WAN capability
- SonicExpress App onboarding
- Zero-Touch Deployment
- Single-pane-of-glass-management through cloud or firewall
- SonicWall Switch, SonicWave Access Point and Capture Client integration
- Built-in and expandable storage
- Redundant power
- High port density
- Cellular failover
- SonicOS 7.0
- TLS 1.3 support
- Groundbreaking performance
- High connection count
- Fast DPI performance
- Low TCO

Deployments

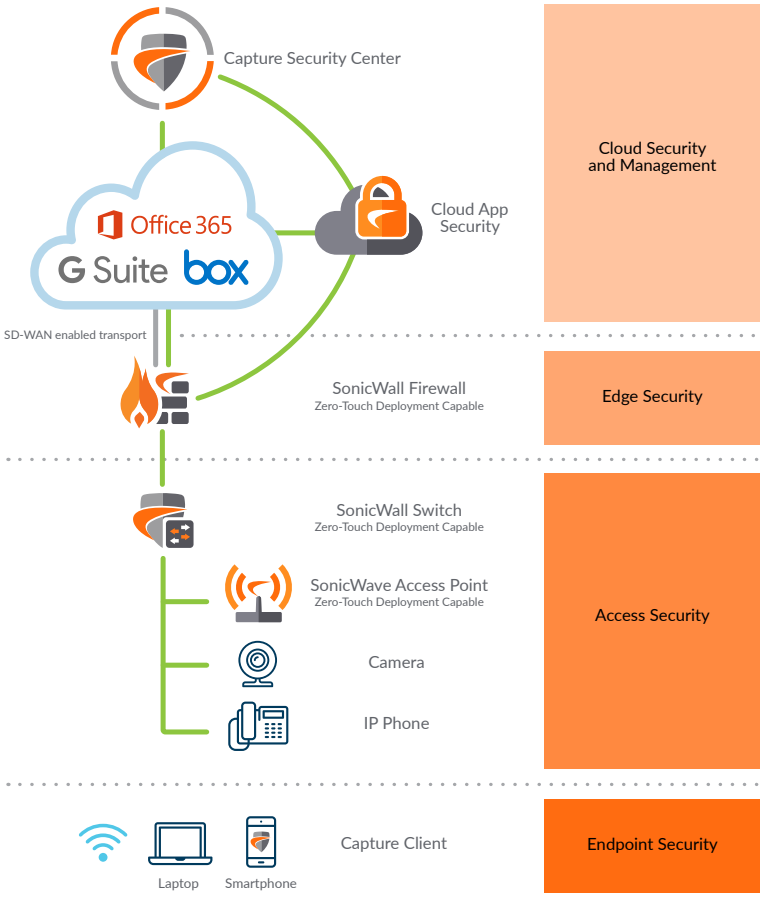
Small to Medium size Business

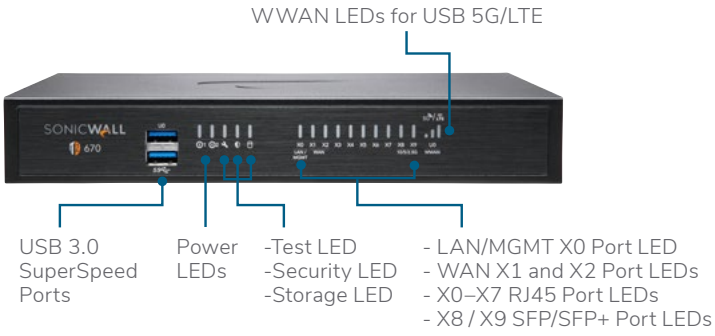
- Save space and money with an integrated gateway security solution with firewalling, switching and wireless capabilities
- Reduce complexity and get the business running without relying on IT personnel with easy onboarding using SonicExpress App and Zero-Touch Deployment, and easy management through a single pane of glass
- Attain business continuity by providing failover to cellular connectivity
- Protect network from attacks with a comprehensive security solution that incorporates VPN, IPS, CFS, AV and much more
- Leverage high port density to power on multiple PoE devices such as IP phones and IP cameras
- Boost employee productivity by blocking unauthorized access with traffic segmentation and access policies

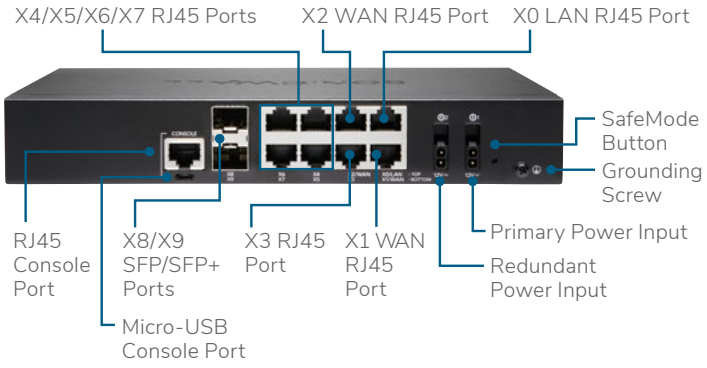


Distributed Enterprise with SD-Branches

- Enhance customer experience and adapt to the changing business needs by enabling next-gen branch connectivity with SD-Branch
- Drive business growth by investing in next-gen appliances with multi-gigabit and advanced security features, to future-proof against the changing network and security landscape
- Secure networks from the most advanced attacks with advanced security features and automatically block threats on decrypted traffic using protocols such as TLS 1.3
- Leverage end-to-end network security with seamless integration of SonicWave access points, SonicWall Switches and Capture Client
- Ensure seamless communication as stores talk to HQ via easy VPN connectivity which allows IT administrators to create a hub and spoke configuration for the safe transport of data between all locations
- Improve business efficiency, performance and reduce costs by leveraging TZ670's hardware and software enhancements, plus features such SD-WAN technology
- Scale quickly and effortlessly with SonicExpress App and Zero-Touch Deployment
- Ensure business continuity by providing failover to cellular connectivity
- Maintain compliance with security features, and leverage built-in and expandable storage to store logs for audit purposes







SonicWall TZ670 specifications

FIREWALL GENERAL	TZ670 SERIES
Operating system	SonicOS 7.0
Interfaces	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Console
Power over Ethernet (PoE) support	N/A
Expansion	Storage Expansion Slot (Up to 256GB, with 32 GB included)
Management	Network Security Manager, CLI, SSH, Web UI, GMS, REST APIs
Single Sign-On (SSO) Users	2,500
VLAN interfaces	256
Access points supported (maximum)	32
FIREWALL/VPN PERFORMANCE	**TZ670 SERIES**
Firewall inspection throughput[1]	5.00 Gbps
Threat prevention throughput[2]	2.50 Gbps
Application inspection throughput[2]	3.0 Gbps
IPS throughput[2]	3.0 Gbps
Anti-malware inspection throughput[2]	2.50 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	800 Mbps
IPSec VPN throughput[3]	2.10 Gbps
Connections per second	25,000
Maximum connections (SPI)	1,500,000
Maximum connections (DPI)	500,000
Maximum connections (DPI SSL)	30,000
VPN	**TZ670 SERIES**
Site-to-site VPN tunnels	250
IPSec VPN clients (maximum)	10 (500)
SSL VPN licenses (maximum)	2 (250)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v
Route-based VPN	RIP, OSPF, BGP
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN
Global VPN client platforms supported	Microsoft® Windows 10
NetExtender	Microsoft® Windows 10, Linux
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10
SECURITY SERVICES	**TZ670 SERIES**
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL

SonicWall TZ670 specifications, continued

Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists
Comprehensive Anti-Spam Service	Yes
Application Visualization	Yes
Application Control	Yes
Capture Advanced Threat Protection	Yes
DNS Security	Yes
NETWORKING	**TZ670 SERIES**
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)
Local user database	250
VoIP	Full H.323v1-5, SIP
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE a802.3
Certifications pending	FIPS 140-2 (with Suite B) Level 2, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)
HARDWARE	**TZ670 SERIES**
Form factor	Desktop[5]
Power supply	60W external
Maximum power consumption (W)	13.1
Input voltage & frequency	100-240 VAC, 50-60 Hz
Total heat dissipation	55.1 BTU
Dimensions	3.5 x 15 x 22.5 (cm) 1.38 x 5.91 x 8.85 in
Weight	0.97 kg / 2.14 lbs
WEEE weight	1.42 kg / 3.13 lbs
Shipping weight	1.93 kg / 4.25 lbs
MTBF @25°C in years	43.9
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)
Humidity	5-95% non-condensing
REGULATORY	**TZ670 SERIES**
Major regulatory compliance	FCC Class B, FCC , ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL/cUL, TUV/GS, CB, Mexico DGN notice by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL

[1] *Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.*
[2] *Threat Prevention/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled.*
[3] *VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.*
[4] *BGP is available only on SonicWall TZ400, TZ500 and TZ600.*
[5] *For rack mount, separate rack mount kit available.*

SonicOS 7.0 Feature Summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- Full API support
- SonicWall Switch integration
- SD-WAN scalability
- SD-WAN Usability Wizard[1]
- SonicCoreX and SonicOS containerization[1]
- Connections scalability (SPI, DPI, DPI SSL)

Enhanced dashboard[1]

- Enhanced device view
- Top traffic and user summary
- Insights to threats
- Notification center

TLS/SSL/SSH decryption and inspection

- TLS 1.3 with enhanced security[1]
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Enhancements for DPI-SSL with CFS
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[2]

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

Intrusion prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[2]

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

Application identification[2]

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

Traffic visualization and analytics

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

HTTP/HTTPS Web content filtering[2]

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

VPN

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

Networking

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NSa 2650 and above)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- A/P high availability with state sync
- Inbound/outbound load balancing
- High availability - Active/Standby with state sync
- L2 bridge, wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing
- Common Access Card (CAC) support

VoIP

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

Management, monitoring and support

- Capture Security Appliance (CSa) support
- Capture Threat Assessment (CTA) v2.0
  - New design or template
  - Industry and global average comparison
- New UI/UX, Intuitive feature layout[1]
  - Dashboard
  - Device information, application, threats
  - Topology view
  - Simplified policy creation and management
- Policy/Objects usage statistics[1]
  - Used vs Un-used
  - Active vs Inactive
- Global search for static data
- Storage support[1]
- Internal and external storage management[1]
- WWAN USB card support (5G/LTE/4G/3G)
- Network Security Manager (NSM) support
- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- CSC Simple Reporting[1]
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualization
- IPv4 and IPv6 management
- CD management screen
- Dell N-Series and X-Series switch management including cascaded switches

Debugging and diagnostics

- Enhanced packet monitoring
- SSH terminal on UI

Wireless

- SonicWave AP cloud management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- RF enhancements and improvements
- Guest cyclic quota

[1] *New feature, available on SonicOS 7.0*
[2] *Requires added subscription*