

SonicWall TZ Series (Gen 7)

Integrierte SD-Branch-Plattform für moderne KMUs und Filialen

Bei den Firewalls der neuesten SonicWall TZ Series handelt es sich um die ersten Next-Generation-Firewalls (NGFWs) mit Desktop-Formfaktor und 10- oder 5-Gigabit-Ethernet-Schnittstellen. Die Reihe zeichnet sich durch ein breites Spektrum an Produkten für die unterschiedlichsten Anwendungsfälle aus.

Für kleine und mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die siebte Generation (Gen 7) der TZ Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis. Diese NGFWs ermöglichen eine automatisierte, echtzeitbasierte Erkennung und Prävention von Sicherheitslücken und bieten so eine Antwort auf die wachsenden Trends in den Bereichen Webverschlüsselung, vernetzte Geräte und Highspeed-Mobilität.

HIGHLIGHTS

- 10-/5-/2,5-/1-GbE-Schnittstellen in einem kompakten Gehäuse (Desktop-Formfaktor)
- SD-Branch-Unterstützung
- Sichere SD-WAN-Funktionen
- SonicExpress-App-Onboarding
- Vollautomatische Implementierung
- Zentrale Verwaltung über Cloud oder Firewall
- SonicWall-Switch, SonicWave-Access-Point und Capture-Client-Integration
- Integrierter und erweiterbarer Speicher
- Redundante Stromversorgung
- Hohe Portdichte
- Mobilfunk-Failover
- SonicOS 7.0
- TLS-1.3-Unterstützung
- Bahnbrechende Performance
- Hohe Zahl von Verbindungen
- Schnelle DPI-Performance
- Niedrige Gesamtbetriebskosten



Überblick über die technischen Daten der TZ Series (Gen 7).

[Alle technischen Daten anzeigen »](#)

Max. Threat-Prevention-Durchsatz

2,5 GBit/s

Max. Anzahl von Verbindungen

1,5 Millionen

Ports

8 x 1-GbE, 2 x 2,5-/5-/10-GbE

Finden Sie die richtige SonicWall-Lösung für Ihr Unternehmen:

sonicwall.com/TZ

„Die TZ570 lässt sich spielend leicht onboarden, nutzen und verwalten. Sie punktet mit einem einfachen Wizard und klaren Menüs. Ich bin von SonicWall begeistert – sowohl die Produkte als auch der Support sind exzellent.“

– Gaurav Pandey, Head IT, Delhivery

[Case-Study lesen »](#)

Die Gen 7 TZ Series ist mit einer Portdichte von bis zu zehn Ports hochgradig skalierbar. Sie bietet sowohl einen integrierten als auch einen erweiterbaren Speicher von bis zu 256 GB, der verschiedene Features wie zum Beispiel Protokollierung, Reporting, Caching und Firmware-Backups ermöglicht. Eine optionale zweite Stromversorgung bei ausgewählten Modellen sorgt für zusätzliche Redundanz bei Ausfällen.

Durch die vollautomatische Implementierung lassen sich die Gen-7-TZ-Firewalls denkbar einfach und mit minimaler Unterstützung der IT an mehreren Standorten gleichzeitig bereitstellen. Die Serie baut auf Next-Gen-Hardware auf und integriert Firewall-, Switch- und Wireless-Funktionen. Außerdem erlaubt sie eine zentrale Verwaltung von SonicWall-Switches und SonicWave-Access-Points. Für eine nahtlose Endpoint-Security ist eine enge Integration mit Capture Client möglich.

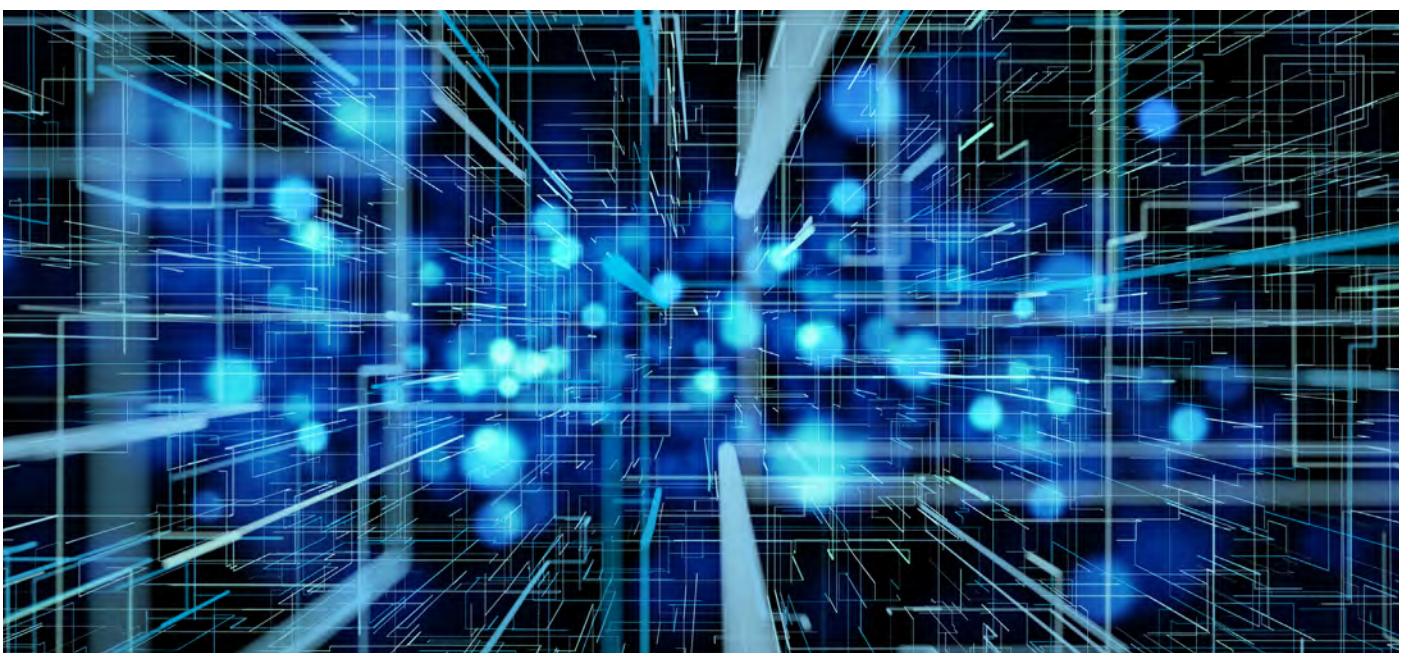
SonicOS und Sicherheitsservices

Die SonicOS-Architektur bildet das Herzstück der TZ-NGFWs. Die Gen-7-TZ-Firewalls basieren auf dem Betriebssystem [SonicOS 7.0](#), das viele Features wie eine neue moderne UX/UI sowie erweiterte Sicherheits-, Netzwerk- und Management-Funktionen umfasst. Daneben bieten die

Firewalls integriertes [SD-WAN](#), Unterstützung für TLS 1.3, Echtzeitvisualisierung, ultraschnelles Virtual Private Networking (VPN) und andere robuste Sicherheitsfeatures.

Verdächtige Dateien werden zur Analyse an die cloudbasierte SonicWall-Multi-Engine-Sandbox [Capture Advanced Threat Protection \(ATP\)](#) weitergeleitet. Wesentlicher Bestandteil von Capture ATP ist unsere patentierte [Real-Time Deep Memory Inspection \(RTDMI™\)](#)-Technologie. Als eine von mehreren Engines von Capture ATP führt die RTDMI-Engine die Überprüfung direkt im Arbeitsspeicher aus und ist so in der Lage, Malware und Zero-Day-Bedrohungen zu erkennen und zu blockieren.

Neben Sicherheitsservices wie [Reassembly-Free Deep Packet Inspection \(RFDPI\)](#), Viren- und Spyware-Schutz, einem Intrusion-Prevention-System, Application-Intelligence und Anwendungskontrolle, Content-Filtering-Services und DPI-SSL nutzen die Firewalls der TZ Series auch Capture ATP mit RTDMI-Technologie, um Malware, Ransomware und andere hoch entwickelte Bedrohungen am Gateway zu stoppen. Weitere Informationen finden Sie im Datenblatt [SonicOS und Sicherheitsservices](#).



Implementierungsoptionen

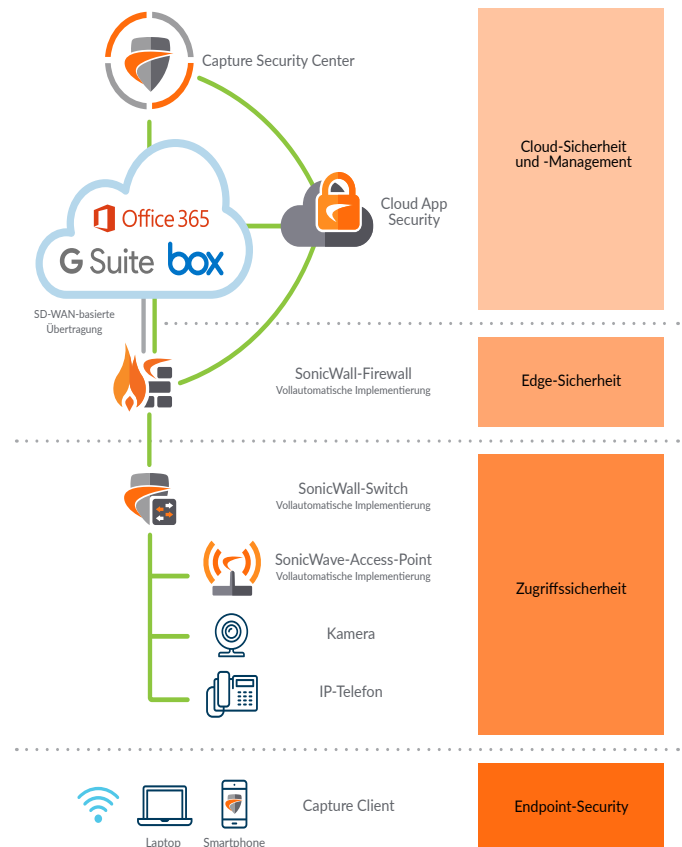
Kleine und mittlere Unternehmen

- Sparen Sie Platz und Geld mit einer integrierten Gateway-Sicherheitslösung mit Firewall-, Switch- und Wireless-Funktionen
- Vereinfachen Sie Ihre Prozesse und halten Sie Ihr Geschäft am Laufen, ohne auf die IT angewiesen zu sein – dank einfachem Onboarding mithilfe der SonicExpress-App und der vollautomatischen Implementierung sowie einer einfachen Verwaltung über eine einzige Konsole
- Stellen Sie die Business-Continuity dank Mobilfunk-Failover sicher
- Schützen Sie das Netzwerk vor Angriffen – mithilfe einer umfassenden Sicherheitslösung inklusive VPN, IPS, CFS, AV und noch viel mehr
- Nutzen Sie die hohe Portdichte der TZ570P für mehrere PoE-Geräte wie IP-Telefone und IP-Kameras
- Setzen Sie auf Traffic-Segmentierung und Zugriffsregeln, um den Zugriff auf unerlaubte Inhalte zu blockieren und so die Produktivität der Mitarbeiter zu verbessern



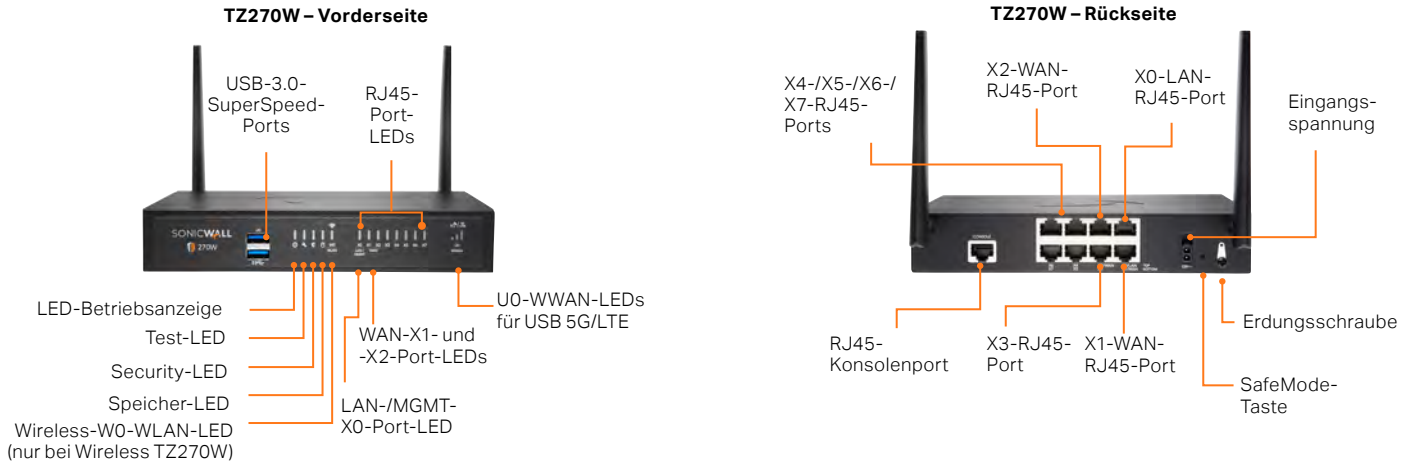
Verteiltes Unternehmen mit SD-Branches

- Nutzen Sie SD-Branch für einen reibungslosen Datenverkehr zwischen verschiedenen Standorten; so können Sie angemessen auf veränderte Geschäftsanforderungen reagieren und die Kundenerfahrung verbessern
- Investieren Sie in Next-Gen-Appliances mit Multi-Gigabit- und erweiterten Sicherheitsfeatures, um das Unternehmenswachstum voranzutreiben und eine zukunftssichere Lösung für die dynamische Netzwerk- und Sicherheitslandschaft zu schaffen
- Schützen Sie Netzwerke mithilfe erweiterter Sicherheitsfeatures vor den raffiniertesten Angriffen und blockieren Sie Bedrohungen im verschlüsselten Netzwerkverkehr automatisch mit Protokollen wie TLS 1.3
- Profitieren Sie von einer durchgängigen Netzwerksicherheit mit nahtloser Integration von SonicWave-Access-Points, SonicWall-Switches und Capture Client
- Stellen Sie eine unkomplizierte Kommunikation zwischen Zentrale und Filialen sicher; nutzen Sie dazu einfache VPN-Verbindungen, um eine Hub-and-Spoke-Konfiguration für die sichere Datenübertragung zwischen allen Standorten zu erstellen
- Optimieren Sie die betriebswirtschaftliche Effizienz und Performance und reduzieren Sie Kosten dank Verbesserungen an der Hardware und Software der Gen-7-TZ-Firewalls sowie Features wie SD-WAN-Technologie
- Profitieren Sie von einer schnellen und einfachen Skalierung mit der SonicExpress-App und der vollautomatischen Implementierung
- Stellen Sie die Business-Continuity durch ein Failover auf eine Mobilfunkverbindung sicher
- Halten Sie Compliance-Vorgaben mithilfe der Sicherheitsfeatures ein und nutzen Sie den integrierten und erweiterbaren Speicher, um Protokolle zu Audit-Zwecken aufzubewahren



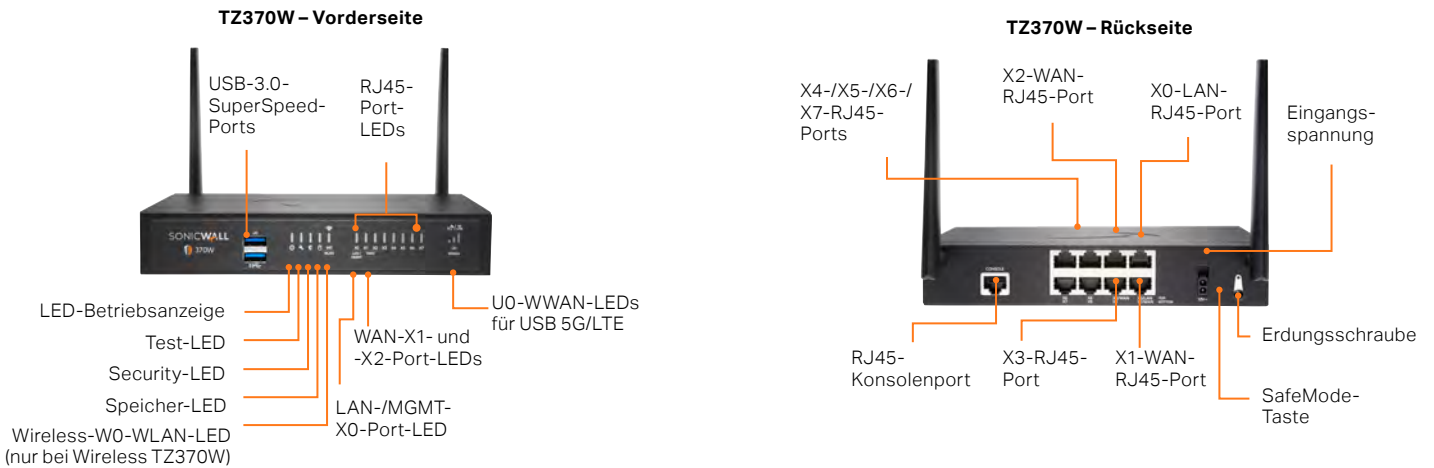
SonicWall TZ270 Series

Für Heimbüros und kleine Filialen konzipiert, bietet die TZ270 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.



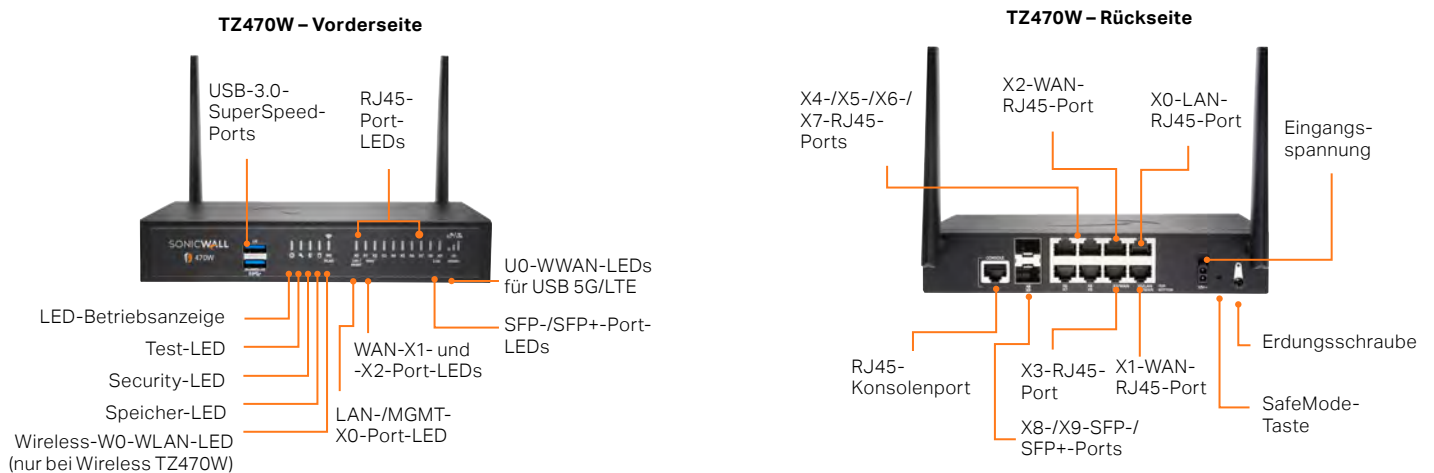
SonicWall TZ370 Series

Für kleine Organisationen und Filialen konzipiert, bietet die TZ370 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.



SonicWall TZ470 Series

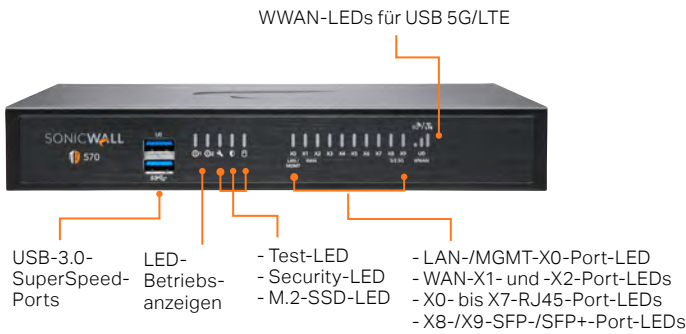
Für kleine Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ470 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.



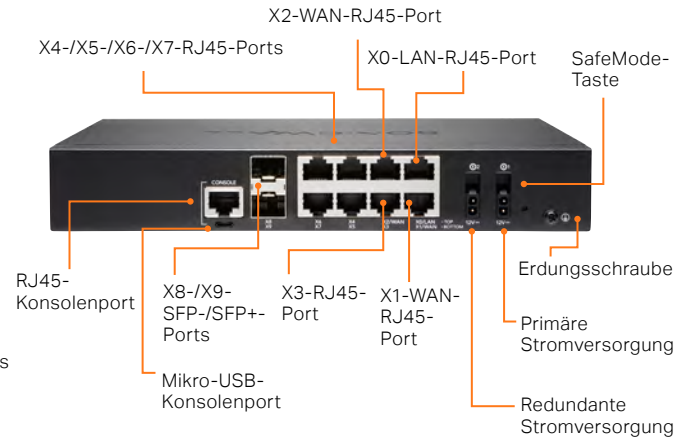
SonicWall TZ570 Series

Für kleine und mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ570 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ570W – Vorderseite



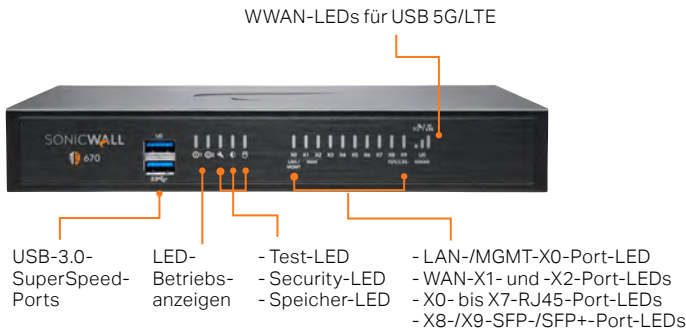
TZ570W – Rückseite



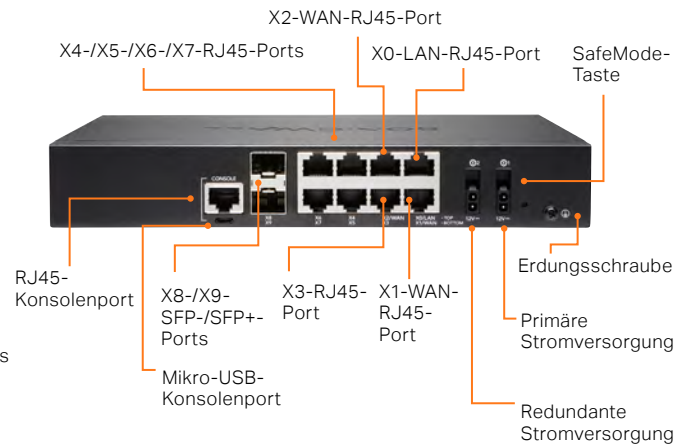
SonicWall TZ670 Series

Für mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ670 bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ670W – Vorderseite



TZ670W – Rückseite



SonicWall TZ Series (Gen 7) – technische Daten

Firewall allgemein	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Betriebssystem	SonicOS 7.0				
Schnittstellen	8 x 1-GbE, 2 USB 3.0, 1 Konsole	8 x 1-GbE, 2 USB 3.0, 1 Konsole	8 x 1-GbE, 2 x 2,5-G-SFP+, 2 USB 3.0, 1 Konsole	8 x 1-GbE, 2 x 5-G-SFP+, 2 USB 3.0, 1 Konsole	8 x 1-GbE, 2 x 10-G-SFP+, 2 USB 3.0, 1 Konsole
Wireless-Unterstützung	2 x 2 802.11ac Wave 2 (TZ270W)	2 x 2 802.11ac Wave 2 (TZ370W)	2 x 2 802.11ac Wave 2 (TZ470W)	2 x 2 802.11ac Wave 2 (TZ570W)	Nicht zutreffend
Power-over-Ethernet(PoE)-Unterstützung	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	5-PoE oder 3-PoE+ (TZ570P)	Nicht zutreffend
Erweiterungssteckplatz für Speicher (Unterseite)	Optional bis 256 GB				Optional bis 256 GB, 32 GB im Lieferumfang enthalten
Verwaltung	Network Security Manager, CLI, SSH, Web-UI, GMS, REST-APIs				
Redundante Stromversorgung	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Ja	Ja
Single-Sign-on(SSO)-Benutzer	1.000	1.000	2.500	2.500	2.500
VLAN-Schnittstellen	64	128	128	256	256
Unterstützte Access-Points (max.)	16	16	32	32	32
Firewall-/VPN-Performance	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Firewall-Inspection-Durchsatz ¹	2 GBit/s	3 GBit/s	3,5 GBit/s	4 GBit/s	5 GBit/s
Threat-Prevention-Durchsatz ²	750 MBit/s	1 GBit/s	1,5 GBit/s	2 GBit/s	2,5 GBit/s
Application-Inspection-Durchsatz ²	1 GBit/s	1,5 GBit/s	2 GBit/s	2,5 GBit/s	3 GBit/s
IPS-Durchsatz ²	1 GBit/s	1,5 GBit/s	2 GBit/s	2,5 GBit/s	3 GBit/s
Anti-Malware-Inspection-Durchsatz ²	750 MBit/s	1 GBit/s	1,5 GBit/s	2 GBit/s	2,5 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung (DPI-SSL) ²	300 MBit/s	500 Mbit/s	600 MBit/s	750 MBit/s	800 MBit/s
IPSec-VPN-Durchsatz ³	750 MBit/s	1,38 GBit/s	1,5 GBit/s	1,8 GBit/s	2,1 GBit/s
Verbindungen pro Sekunde	6.000	9.000	12.000	16.000	25.000
Max. Anzahl an Verbindungen (SPI)	750.000	900.000	1.000.000	1.250.000	1.500.000
Max. Anzahl von Verbindungen (DPI)	150.000	200.000	250.000	400.000	500.000
Max. Anzahl von Verbindungen (DPI-SSL)	25.000	30.000	35.000	50.000	75.000
VPN	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Site-to-Site-VPN-Tunnel	50	100	150	200	250
IPSec-VPN-Clients (max.)	5 (200)	5 (200)	5 (200)	10 (500)	10 (500)
SSL-VPN-Lizenzen (max.)	1 (50)	2 (100)	2 (150)	2 (200)	2 (250)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit) / MD5, SHA-1, Suite B Cryptography				
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v				
Routenbasiertes VPN	RIP, OSPF, BGP				
Unterstützte Zertifikate	Verisign, Thawte, Cybertrust, RSA Keon, Entrust und Microsoft CA für SonicWall-to-SonicWall-VPN, SCEP				
VPN-Funktionen	Dead-Peer-Detection, DHCP über VPN, IPSec-NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN				
Unterstützte globale VPN-Client-Plattformen	Microsoft® Windows 10				
NetExtender	Microsoft® Windows 10, Linux				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10				
Sicherheitservices	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Deep Packet Inspection-Services	Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention, DPI-SSL				
Content Filtering Service (CFS)	Prüfung nach HTTP-URL, HTTPS-IP, Schlüsselwörtern und Inhalt, umfassende Filterung anhand von Dateitypen wie ActiveX, Java, Cookies für Datenschutz, Freigabe- und Sperlisten				
Comprehensive Anti-Spam Service	Ja				
Anwendungsvisualisierung	Ja				
Anwendungskontrolle	Ja				
Capture Advanced Threat Protection	Ja				
Netzwerk	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
IP-Adresszuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus				
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)				
Authentifizierung	LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)				

Netzwerk	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Lokale Benutzerdatenbank	150	250	250	250	250
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Zertifikate	Gewährt: FIPS 140-2 Level 2 (mit Suite B), IPv6/USGv6, ICSCA Network Firewall, ICSCA Firewall Enterprise, ICSCA Network Anti-Virus / Anti-Malware Ausstehend: Common Criteria NDPP (mit VPN und IPS), DoDIN, CSfC				
Hochverfügbarkeit	Active/Standby mit Stateful-Synchronisierung				
Hardware	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Formfaktor	Desktop ⁴				
Stromversorgung	36 W (extern)	36 W (extern)	36 W (extern)	60 W (extern) (TZ570/570W), 180 W (extern) (nur TZ570P)	60 W (extern)
Maximaler Stromverbrauch (W)	16,84 (TZ270), 18,91 (TZ270W)	16,84 (TZ370), 18,91 (TZ370W)	19,95 (TZ470), 21,98 (TZ470W)	13,4 (TZ570), 15,3 (TZ570W), 108,75 (TZ570P)	13,1
Eingangsspannung	100–240 VAC, 50–60 Hz, 3 A	100–240 VAC, 50–60 Hz, 3 A	100–240 VAC, 50–60 Hz, 3 A	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Gesamtwärmeabgabe (BTU)	57,42 (TZ270), 64,48 (TZ270W)	57,42 (TZ370), 64,48 (TZ370W)	68,03 (TZ470), 74,95 (TZ470W)	44,7 (TZ570), 52,17 (TZ570W), 370,84 (TZ570P)	55,1
Abmessungen	3,5 x 13,5 x 19 cm	3,5 x 13,5 x 19 cm	3,5 x 13,5 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 15 x 22,5 cm
Gewicht	0,82 kg (TZ270), 0,85 kg (TZ270W)	0,82 kg (TZ370), 0,85 kg (TZ370W)	0,83 kg (TZ470), 0,87 kg (TZ470W)	0,97 kg (TZ570), 0,99 kg (TZ570W), 1,05 kg (TZ570P)	0,97 kg
WEEE-Gewicht	1,18 kg (TZ270), 1,24 kg (TZ270W)	1,18 kg (TZ370), 1,24 kg (TZ370W)	1,24 kg (TZ470), 1,27 kg (TZ470W)	1,42 kg (TZ570), 1,47 kg (TZ570W), 1,57 kg (TZ570P)	1,42 kg
Versandgewicht	1,41 kg (TZ270), 1,47 kg (TZ270W)	1,41 kg (TZ370), 1,47 kg (TZ370W)	1,43 kg (TZ470), 1,51 kg (TZ470W)	1,93 kg (TZ570), 1,98 kg (TZ570W), 2,08 kg (TZ570P)	1,93 kg
MTBF bei 25 °C in Jahren	51,1 (TZ270), 27,1 (TZ270W)	51,1 (TZ370), 27,1 (TZ370W)	46 (TZ470), 24,1 (TZ470W)	26,1 (TZ570), 23,3 (TZ570W), 31,7 (TZ570P)	43,9
Umgebungstemperatur (Betrieb/ Lagerung)	0 bis 40 °C / -40 bis 70 °C				
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend				
Richtlinien	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Einhaltung wichtiger gesetzlicher Vorschriften (kabelgebundene Modelle)	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, BSMI, KCC MSIP, ANATEL	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Klasse B, FCC, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL/ cUL, TÜVGS, CB, Mexiko DGN-Mitteilung nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Klasse B, FCC, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL/ cUL, TÜV/ GS, CB, Mexiko DGN-Mitteilung nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL
Einhaltung wichtiger gesetzlicher Vorschriften (Wireless-Modelle)	FCC Klasse B, FCC RF ICES Klasse B, IC RF CE (R&TTE, EMV, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, ANATEL	FCC Klasse B, FCC RF ICES Klasse B, IC RF CE (R&TTE, EMV, LVD, RoHS), RCM, VCCI Klasse B, MIC/ TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, ANATEL	FCC Klasse B, FCC RF ICES Klasse B, IC RF CE (R&TTE, EMV, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, ANATEL	FCC Klasse B, FCC P15C, FCC P15E, ICES Klasse B, ISED/ IC, CE (RED, RoHS), C-Tick, VCCI Klasse B, Japan Wireless, UL/cUL, TÜV/ GS, CB, Mexiko DGN-Mitteilung nach UL, WEEE, REACH, BSMI, NCC (TW) KCC/ MSIP, SRRC, ANATEL	Nicht zutreffend

Richtlinien	TZ270 SERIES	TZ370 SERIES	TZ470 SERIES	TZ570 SERIES	TZ670 SERIES
Einhaltung wichtiger gesetzlicher Vorschriften (PoE-Modelle)	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	FCC Klasse A, ICES Klasse A, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse A, UL/cUL, TÜV/GS, CB, Mexiko DGN-Mitteilung nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	Nicht zutreffend
Integrierte Wireless-Optionen⁵ (NUR TZ270W/370W/470W/570W)					
Standards	802.11a/b/g/n/ac Wave 2, WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS				
Frequenzbänder	802.11a: 5,180–5,825 GHz; 802.11b/g: 2,412–2,472 GHz; 802.11n: 2,412–2,472 GHz, 5,180–5,825 GHz; 802.11ac: 5,180–5,825 GHz				
Verwendete Kanäle	802.11a: USA und Kanada 12, Europa 11, Japan 4, Singapur 4, Taiwan 4; 802.11b/g: USA und Kanada 1–11, Europa 1–13, Japan 1–14 (Kanal 14 nur nach 802.11b-Standard); 802.11n (2,4 GHz): USA und Kanada 1–11, Europa 1–13, Japan 1–13; 802.11n (5 GHz): USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64; 802.11ac: USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64				
Sendeleistung	Basierend auf dem vom Systemadministrator angegebenen Geltungsbereich				
Steuerung der Sendeleistung	Ja				
Unterstützte Datenübertragungsraten	802.11a: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 802.11b: 1, 2, 5, 5 und 11 MBit/s pro Kanal; 802.11g: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 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 MBit/s pro Kanal; 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 und 866,7 MBit/s pro Kanal				
Modulationstechnologie/ Frequenzspreizung	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)				

1. Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren.
2. Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit Keysight-HTTP-Leistungstesttools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt. Der Threat-Prevention-Durchsatz wurde bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle mit Standard-Firewall-Einstellungen gemessen.
3. Messung des VPN-Durchsatzes bei UDP-Verkehr mit 1.418 Bytes pro Paket und AESGMAC16-256-Verschlüsselung gemäß RFC 2544. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.
4. Für eine Rackmontage ist ein separates Rackmount-Kit erhältlich.
5. Alle TZ-Modelle mit integrierten Wireless-Optionen unterstützen entweder das 2,4-GHz- oder 5-GHz-Band. Wenn Sie eine Dual-Band-Unterstützung wünschen, nutzen Sie bitte die Wireless-Access-Point-Produkte von SonicWall.

Modellnummern (Zulassung)

TZ270/270W	APL57-100/APL57-101
TZ370/370W	APL57-100/APL57-101
TZ470/470W	APL57-0F1/APL57-0F2
TZ570/TZ570W/TZ570P	APL62-0F7/APL62-0F8/APL63-0F9
TZ670	APL62-0F7

PARTNER ENABLED SERVICES

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Die SonicWall Advanced Services Partner unterstützen Sie mit erstklassigen Professional Services. Weitere Informationen:

www.sonicwall.com/PES

Die SonicOS-7.0-Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- Umfassende API-Unterstützung
- SonicWall-Switch-Integration
- SD-WAN-Skalierbarkeit
- SD-WAN-Usability-Assistent¹
- SonicCoreX- und SonicOS-Containerisierung¹
- Skalierbarkeit von Verbindungen (SPI, DPI, DPI-SSL)
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filterung mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Verbessertes Dashboard¹

- Optimierte Geräteansicht
- Überblick über den häufigsten Traffic und die häufigsten Nutzer
- Einblick in Bedrohungen
- Benachrichtigungszentrale

TLS-/SSL-/SSH-Entschlüsselung und -Prüfung

- TLS 1.3 mit verbesserter Sicherheit¹
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Verbesserungen für DPI-SSL mit CFS
- Granulare DPI-SSL-Steuerung nach Zone oder Regel

Capture Advanced Threat Protection²

- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention²

- Signaturbasierte Scans

Anti-Malware²

- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloudbasierte Malware-Datenbank

Anwendungsidentifizierung²

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellung benutzerdefinierter Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungs-signaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten²

- URL-Filterung
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Rating-Kategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN

- Sicheres SD-WAN
- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client

- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (OSPF, RIP, BGP)

Netzwerk

- PortShield
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung (NSa 2650 und höher)
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Hochverfügbarkeitsmodus A/P mit State-Sync
- Lastausgleich für ein- und ausgehenden Datenverkehr
- Hochverfügbarkeit – Active/Standby mit State-Sync
- L2-Bridge-, Wire-/Virtual-Wire-, Tap-, NAT-Modus
- Asymmetrisches Routing
- Unterstützung von Common Access Card (CAC)

VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Unterstützung

Verwaltung, Überwachung und Unterstützung

- Unterstützung von Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) V2.0
 - Neues Design oder Template
 - Vergleich mit Branchen- bzw. weltweitem Durchschnitt
- Neue UI/UX, intuitives Feature-Layout¹
 - Dashboard
 - Geräteinformationen, Anwendungen, Bedrohungen
 - Topology View
 - Vereinfachte Erstellung und Verwaltung von Richtlinien

- Nutzungsstatistiken zu Regeln/Objekten¹
 - Verwendet vs. nicht verwendet
 - Aktiv vs. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung¹
- Interne und externe Speicherverwaltung¹
- WWAN-USB-Kartenunterstützung (5G/LTE/4G/3G)
- Network Security Manager(NSM)-Unterstützung
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- Einfaches CSC-Reporting¹
- Unterstützung der mobilen SonicExpress-App
- SNMPv2/v3
- Zentrales Management und Reporting mit dem SonicWall Global Management System (GMS)²
- Protokollierung
- NetFlow-/IPFIX-Export

- Cloudbasiertes Konfigurationsbackup
- BlueCoat Security Analytics Platform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- CD-Bildschirm
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinandergeschalteten Switches

Fehlersuche und Diagnose

- Erweiterte Paketüberwachung
- SSH-Terminal auf der Benutzeroberfläche

Wireless

- SonicWave-AP-Cloud-Management
- WIDS/WIPS
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- 802.11s-Mesh-Networking
- Automatische Kanalauswahl
- Analyse des HF-Spektrums
- Floor Plan View

- Topology View
- Bandsteering
- Beamforming
- AirTime-Fairness
- Bluetooth Low Energy
- MiFi-Extender
- Verbesserte Funkfrequenzen
- Zyklische Quote für Gastbenutzer

Integrierte Wireless-Optionen (nur TZ270/370/470/570W)

- 802.11ac Wave 2 Wireless
- Dualband (2,4 GHz und 5 GHz)
- Wireless-Standards 802.11 a/b/g/n/ac
- Erkennung und Vermeidung von Wireless-Angriffen
- Wireless Guest Services
- Lightweight Hotspot Messaging
- Segmentierung mithilfe virtueller Access-Points
- Captive Portal
- Cloud-Zugriffssteuerungsliste

¹ Neues Feature, erhältlich für SonicOS 7.0

² Erfordert zusätzliches Abo

Erfahren Sie mehr über die SonicWall Gen 7 TZ Series

www.sonicwall.com/TZ

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

Weitere Informationen erhalten Sie auf unserer Website.

www.sonicwall.com

SONICWALL®

© 2022 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Haftung und keinerlei ausdrückliche, stillschweigende oder gesetzliche Gewährleistung für deren Produkte, einschließlich, aber nicht beschränkt auf die stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck und die Nichtverletzung von rechten Dritter, soweit sie nicht in den Bestimmungen der Lizenzvereinbarung für dieses Produkt niedergelegt sind. SonicWall und/oder dessen Tochtergesellschaften haften nicht für irgendwelche unmittelbaren, mittelbaren, strafrechtlichen, speziellen, zufälligen oder Folgeschäden (einschließlich, aber nicht beschränkt auf Schäden aus entgangenem Gewinn, Geschäftsunterbrechung oder Verlust von Information), die aus der Verwendung oder der Unmöglichkeit der Verwendung dieses Dokuments entstehen, selbst wenn SonicWall und/oder dessen Tochtergesellschaften auf die Möglichkeit solcher Schäden hingewiesen wurden. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.