Gartner
Peer Insights™

DATENBLATT

SonicWall TZ Series (Gen 8)

Integrierte SD-Branch-Plattform mit leistungsstarken Next-Gen-Firewalls für KMUs und Filialen

Speziell für kleine und mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, punkten die neuesten Modelle der SonicWall TZ Series mit einer erstklassigen Performance zu niedrigen Gesamtbetriebskosten.

Diese NGFWs mit Desktop-Formfaktor 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.



Technische Daten der TZ Series.

Alle technischen Daten anzeigen »

Max. Threat-Prevention-Durch-satz	Max. Verbindungen	Ports
Bis zu 3 GBit/s	Bis zu 1,5 Millionen	Bis zu 8 x 1-GbE, 2 x 10-/5-/2,5-G-SFP+

HIGHLIGHTS

- Bis zu 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
- Kompatibel mit SonicWall Unified Management
- Zentralisierte, einfachere Verwaltung über Network Security Manager (NSM)
- SonicWall-Switch, SonicWave-Access-Point und Capture-Client-Integration
- Integrierter und erweiterbarer Speicher
- Redundante Stromversorgung
- DNS-Sicherheit
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- Wi-Fi-6-Firewall-Management
- Integration der Netzwerkzugriffskontrolle mit Aruba ClearPass
- Hohe Portdichte
- Mobilfunk-Failover
- TLS-1.3-Unterstützung
- Bahnbrechende Performance
- Hohe Zahl von Verbindungen
- Schnelle DPI-Performance
- Niedrige Gesamtbetriebskosten
- Unterstützung für Cloud-Secure-Edge-Konnektor
- Integrierte Cybergarantie

Nur für Firewalls, die nach dem 1. November 2024 verkauft und registriert wurden.

sonicwall.com

SONICWALL®

Die Gen 8 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 512 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-8-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-8-TZ-Firewalls basieren auf dem Betriebssystem SonicOS 8, 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 RTDMI 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 TZ-Firewalls auch Capture ATP mit RTDMI-Technologie, um Malware, Ransomware und andere hoch entwickelte Bedrohungen am Gateway zu stoppen.

Die mit den Gen-8-NGFWs angebotenen Security-Suites verfügen über eine kostenlose integrierte Garantie von Cysurance in Höhe von bis zu 200.000 USD.[1]

Die neue Integration des Cloud-Secure-Edge-Konnektors ermöglicht einen sicheren Zugriff auf private Anwendungen, der sich zentral und unkompliziert verwalten lässt. Dieser Ansatz sorgt dafür, dass die Vertrauenswürdigkeit von Benutzern und Geräten mehrfach überprüft wird, bevor ein Zugriff auf bestimmte Anwendungen gewährt wird – unabhängig von Standort und Gerätetyp.

Weitere Informationen finden Sie unter **Gen-8-Architektur und -Services**.

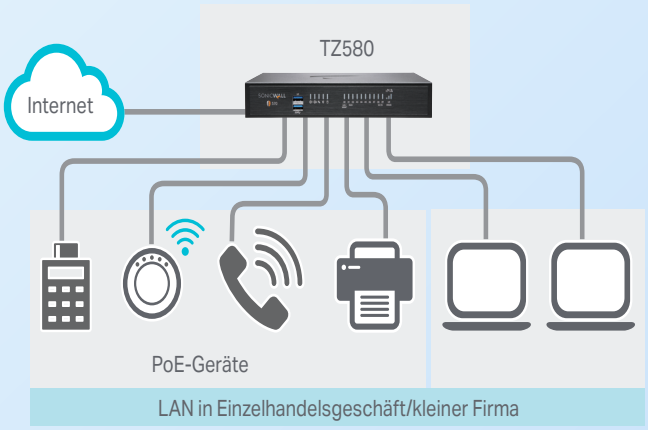
[1] Nur für Firewalls, die nach dem 1. November 2024 verkauft und registriert wurden.

SONICWALL®

Implementierungsoptionen

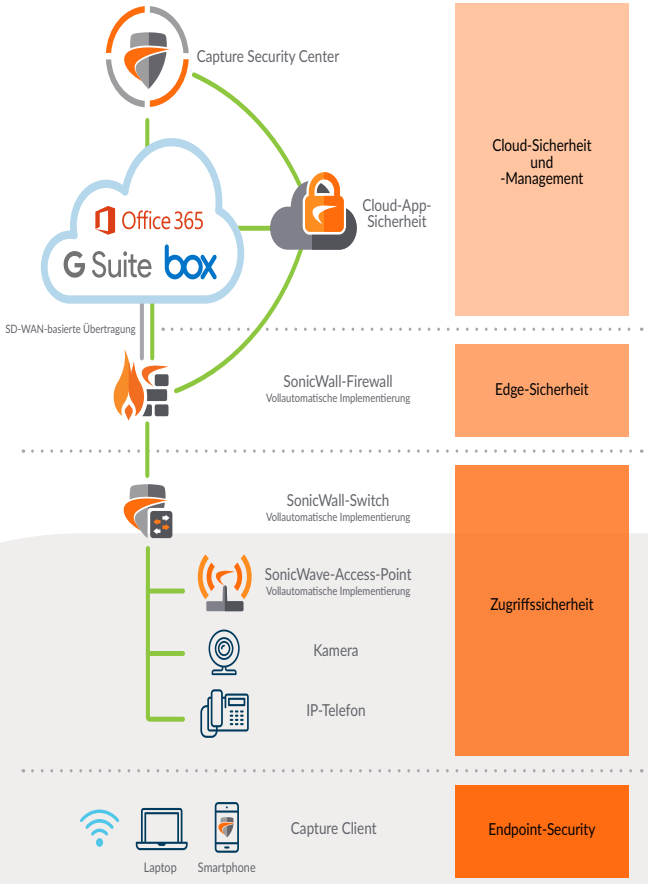
Kleine und mittlere Unternehmen

- Sparen Sie Platz und Geld mit einer integrierten Gateway-Security-Lösung mit Firewall-, Switching- 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 TZ580 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-8-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

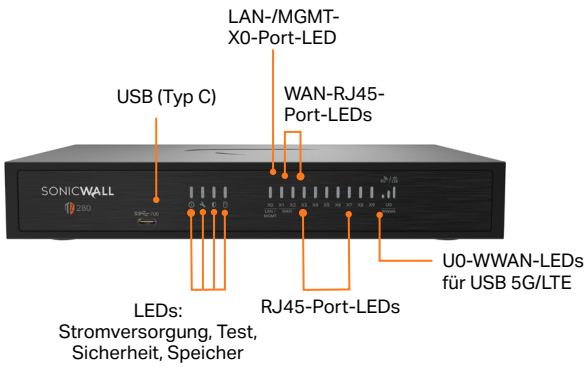


SONICWALL

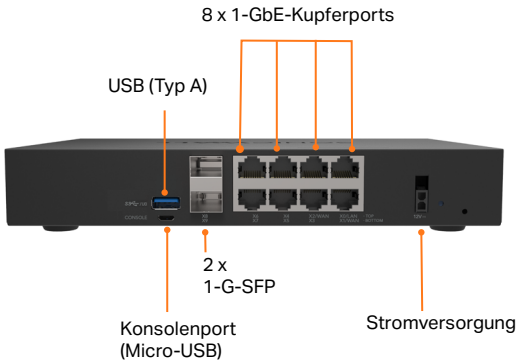
SonicWall TZ280

Für Homeoffices sowie kleine Büros und Filialen konzipiert, bietet die TZ280 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ280 – Vorderseite



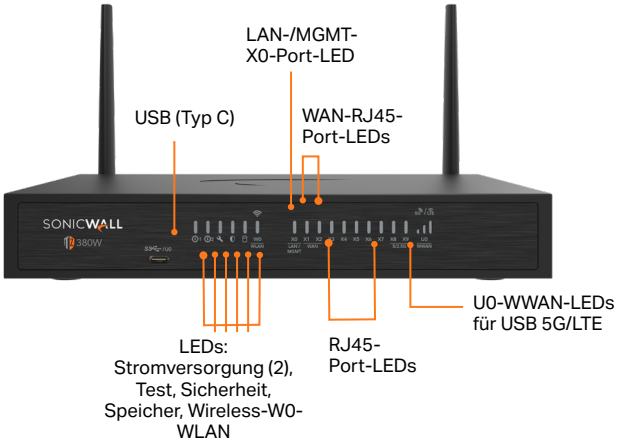
TZ280 – Rückseite



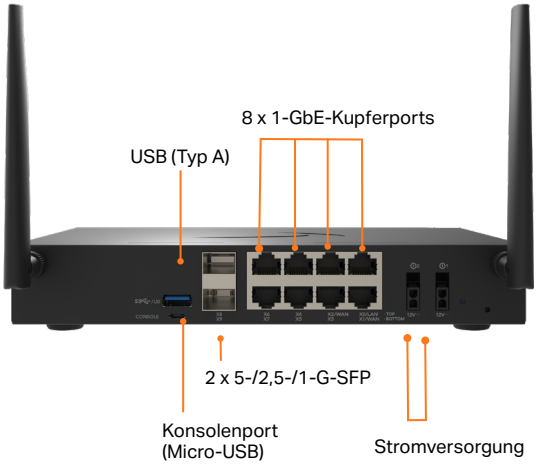
SonicWall TZ380 Series

Für kleine Organisationen und Filialen konzipiert, bietet die TZ380 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ380W – Vorderseite



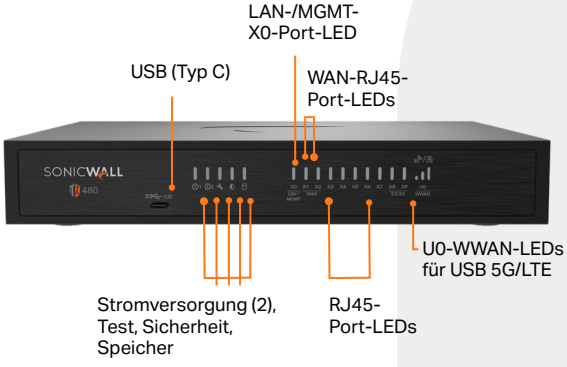
TZ380W – Rückseite



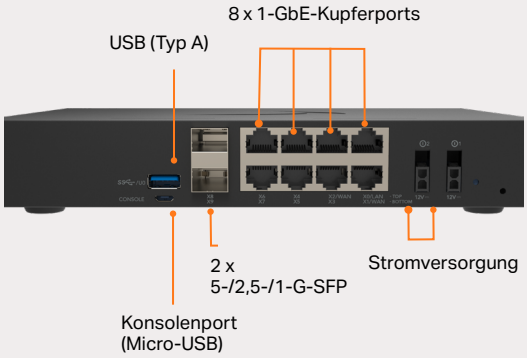
SonicWall TZ480 Series

Für kleine Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ480 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ480 – Vorderseite



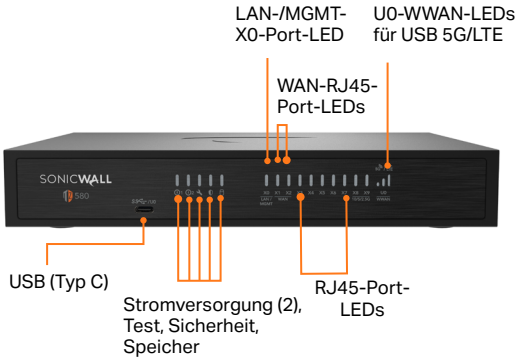
TZ480 – Rückseite



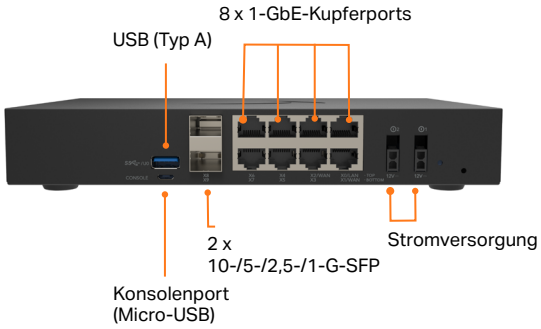
SonicWall TZ580 Series

Für kleine und mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ580 Series bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ580 – Vorderseite



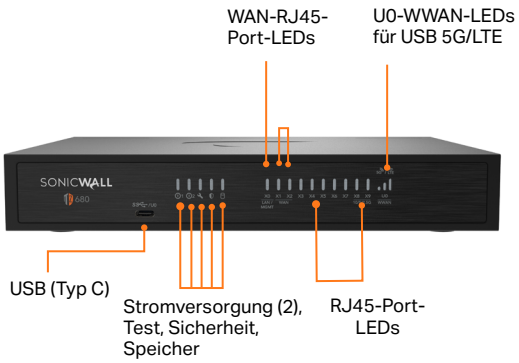
TZ580 – Rückseite



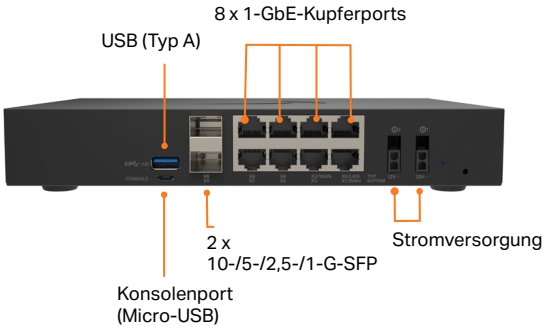
SonicWall TZ680 Series

Für mittlere Organisationen sowie dezentrale Unternehmen mit SD-Branch-Standorten konzipiert, bietet die TZ680 bewährte Sicherheit bei erstklassigem Preis-Leistungs-Verhältnis.

TZ680 – Vorderseite



TZ680 – Rückseite



SonicWall TZ Series (Gen 8) – technische Daten

Firewall allgemein	TZ280 Series	TZ380 Series	TZ480 Series	TZ580 Series	TZ680 Series
Betriebssystem	SonicOS 8				
Schnittstellen	8 x 1-GbE-Kupferports, 2 x 1-G-SFP, 1 Konsole (Micro-USB), 1 USB (Typ C)	8 x 1-GbE-Kupferports, 2 x 5-/2,5-/1-G-SFP, 1 Konsole (Micro-USB), 1 USB (Typ C)	8 x 1-GbE-Kupferports, 2 x 5-/2,5-/1-G-SFP, 1 Konsole (Micro-USB), 1 USB (Typ C)	8 x 1-GbE-Kupferports, 2 x 10-/5-/2,5-/1-G-SFP, 1 Konsole (Micro-USB), 1 USB (Typ C)	8 x 1-GbE-Kupferports, 2 x 10-/5-/2,5-/1-G-SFP, 1 Konsole (Micro-USB), 1 USB (Typ C)
Wireless-Unterstützung	Keine Angabe	2x2 802.11ax (TZ380W)	Keine Angabe	Keine Angabe	Keine Angabe
Speicher (Erweiterung)	(Optional: bis zu 512 GB)	(Optional: bis zu 512 GB)	(Optional: bis zu 512 GB)	(Optional: bis zu 512 GB)	(Optional: bis zu 512 GB)
Zentralisierte Verwaltung	Network Security Manager (NSM) 3.0 und höher, CLI, SSH, Web-UI, REST-APIs				
Logische VLAN- und Tunnel-Schnittstellen (max.)	64	128	128	256	256
SAML-Single-Sign-on(SSO)-Nutzer[1]	1.000	1.000	2.500	2.500	2.500
Unterstützte Access-Points (max.)	16	16	32	32	32
Firewall-/VPN-Performance					
Firewall-Inspection-Durchsatz[2]	2,5 GBit/s	3,5 GBit/s	4 GBit/s	4,5 GBit/s	5 GBit/s
Threat-Prevention-Durchsatz[3]	1 GBit/s	1,5 GBit/s	2 GBit/s	2,2 GBit/s	2,5 GBit/s
Application-Inspection-Durchsatz[3]	1,5 GBit/s	2,0 GBit/s	2,2 GBit/s	2,5 GBit/s	3 GBit/s
IPS-Durchsatz[3]	1,5 GBit/s	2,0 GBit/s	2,2 GBit/s	2,5 GBit/s	3 GBit/s
Anti-Malware-Inspection-Durchsatz[3]	1 GBit/s	2,0 GBit/s	2 GBit/s	2,2 GBit/s	2,5 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung[3]	430 MBit/s	600 MBit/s	650 MBit/s	750 MBit/s	800 MBit/s
IPsec-VPN-Durchsatz[4]	1,2 GBit/s	1,6 GBit/s	2 GBit/s	2,2 GBit/s	2,5 GBit/s
Verbindungen pro Sekunde	12.000	15.000	18.000	20.000	26.000
Max. Anzahl von Verbindungen (SPI)	1.000.000	1.100.000	1.200.000	1.400.000	1.600.000
Max. Anzahl von Verbindungen (DPI)	200.000	250.000	350.000	500.000	600.000
Max. Anzahl von Verbindungen (TLS)	35.000	40.000	50.000	60.000	75.000
VPN und ZTNA					
Site-to-Site-VPN-Tunnel	200	200	200	250	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	AES (128, 192, 256 Bit)/MD5, SHA-256, SHA-384, 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 und Windows 11				
NetExtender	Microsoft® Windows 10 und Windows 11, Linux				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™				
SonicWall Private Access auf Basis von Cloud Secure Edge[5]	Im „3 & Free"-Loyalty-Programm enthalten				
Sicherheitsservices					
Deep-Packet-Inspection-Services	Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention, TLS-Entschlüsselung				
Content Filtering Service (CFS)	Reputationsbasierte URL-Filterung, Prüfung nach HTTP-URL, HTTPS-IP, Schlüsselwörtern und Inhalt, umfassende Filterung anhand von Dateitypen wie ActiveX, Java, Cookies für Datenschutz, Freigabe- und Sperrlisten				
Comprehensive Anti-Spam Service	Ja	Ja	Ja	Ja	Ja
Anwendungsvisualisierung	Ja	Ja	Ja	Ja	Ja

SONICWALL®

Anwendungskontrolle	Ja	Ja	Ja	Ja	Ja
Capture Advanced Threat Protection	Ja	Ja	Ja	Ja	Ja
Erweiterte DNS-Filterung	Ja	Ja	Ja	Ja	Ja
Netzwerk					
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, TACACS+, SAML-SSO[1], Radius Accounting NTLM, interne Benutzerdatenbank, 2FA, Terminaldienste, Citrix, Common Access Card (CAC)				
Lokale Benutzerdatenbank	1.000	1.000	1.000	1.000	1.000
VoIP	Volle Unterstützung für H3230v1.5 SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Zertifikate	IPv6				
Hochverfügbarkeit	Active/Standby mit Stateful-Synchronisierung				
Hardware					
Formfaktor	Desktop				
Stromversorgung	12 V / 1,03 A	12 V / 1,14 A (TZ380) 12 V / 1,45 A (TZ380W)	12 V / 1,13 A	12 V / 1,34 A	12 V / 1,34 A
Maximaler Stromverbrauch (W)	12,36	13,77 (TZ380) 17,4 (TZ380W)	13,77	15,6	16,99
Eingangsleistung	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Redundante Stromversorgung	1 (Optional)	1 (Optional)	1 (Optional)	1 (Optional)	1 (Optional)
Gesamtwärmeabgabe (BTU)	42,43	46,95 (TZ380) 59,33 (TZ380W)	42,43	56,74	57,93
Abmessungen (in cm)	3,5 x 13 x 19 Versandmaße: 7,2 x 22,8 x 23	3,5 x 13 x 19 Versandmaße: 7,2 x 22,8 x 23	3,5 x 13 x 19 Versandmaße: 7. 2 x 22,8 x 23	3,5 x 13 x 19 Versandmaße: 7,2 x 22,8 x 23	3,5 x 13 x 19 Versandmaße: 7,2 x 22,8 x 23
Gewicht	0,82 kg	0,82 kg (TZ380) 0,85 kg (TZ380W)	0,82 kg	0,97 kg	0,97 kg
WEEE-Gewicht	1,18 kg	1,18 kg (TZ380) 1,24 kg (TZ380W)	1,18 kg	1,42 kg	1,42 kg
Versandgewicht	1,41 kg	1,41 kg (TZ380) 1,47 kg (TZ380W)	1,41 kg	1,93 kg	1,93 kg
MTBF bei 25 °C in Jahren	51,7	46,4 (TZ380) 24,9 (TZ380W)	52,8	30,7	29,9
Umgebungstemperatur (Betrieb/ Lagerung)	0 bis +40 °C / -40 bis +70 °C	0 bis +40 °C / -40 bis +70 °C	0 bis +40 °C / -40 bis +70 °C	0 bis +40 °C / -40 bis +70 °C	0 bis +40 °C / -40 bis +70 °C
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend
Integrierte Wireless-Optionen (nur TZ380W)					
Standards	802.11a/b/g/n/ac/ax, WPA, WPA2, WPA3, 802.11i, 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; 802.11ax; 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 (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				

SONICWALL

Unterstützte Datenübertragungsraten	802.11a: 6, 9, 12, 18, 24, 36, 48, 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, 54 MBit/s pro Kanal; 802.11n: 15, 30, 45, 60, 90, 120, 135, 150, 30, 60, 90, 120, 180, 240, 270, 300 MBit/s pro Kanal; 802.11ac: 32,5, 65, 97,5, 130, 195, 260, 292,5, 325, 390, 433,3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866,6 MBit/s pro Kanal; 802.11ax: 36, 72, 106, 144, 216, 288, 324, 360, 432, 480, 540, 600, 72, 144, 216, 288, 432, 576, 648, 720, 864, 960,1201 MBit/s pro Kanal				
Modulationstechnologie/ Frequenzspreizung	802.11a: Orthogonal Frequency Division Multiplexing (OFDM)/64QAM; 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/64QAM/Direct Sequence Spread Spectrum (DSSS); 802.11n:Orthogonal Frequency Division Multiplexing (OFDM)/64QAM; 802.11AC:Orthogonal Frequency Division Multiplexing (OFDM)/256QAM; 802.11ax: Orthogonal Frequency Division Multiplexing Access (OFDMA)/1024QAM				
Richtlinien					
Modellnummern (Zulassung)	APL70-11D	APL72-120 (TZ380), APL72-121 (TZ380W)	APL72-120	APL72-120	APL72-120
Erfüllt folgende Standards/Normen	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse B, KCC/ MSIP, BSMI, MTCTE/ TEC, CB	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal & Radio, VCCI Klasse B, KCC/ MSIP, BSMI, MTCTE/ TEC, CB	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse B, KCC/ MSIP, BSMI, MTCTE/ TEC, CB	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse B, KCC/MSIP, BSMI, MTCTE/TEC, CB	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse B, KCC/MSIP, BSMI, MTCTE/TEC, CB
Erfüllt folgende Standards/Normen (Wireless-Modelle)	Keine Angabe	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse B, KCC/MSIP, BSMI, NCC SRRC, MTCTE/TEC, CB	Keine Angabe	Keine Angabe	Keine Angabe
Erfüllt folgende Standards/Normen (PoE-Modelle)	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

[1] SAML-Single-Sign-on ist für das demnächst erscheinende SonicOS-8.1-Release verfügbar.

[2] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren.

[3] Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit Keysight-HTTP-Leistungstesttools nach Branchenstandard gemessen. Der Test-Durchsatz wurde bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen.

[4] Der VPN-Durchsatz wurde bei UDP-Verkehr mit 1.418 Bytes pro Paket und AESGMAC16-256-Verschlüsselung gemäß RFC 2544 gemessen. Änderungen von Spezifikationen, Funktionen und Verfügbarkeiten vorbehalten.

[5] Im 3-Jahres-Bundle inbegriffen.

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

SONICWALL

Die SonicOS-8-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
- Integration mit SonicWall-Wi-Fi-6-AP
- SD-WAN-Skalierbarkeit
- SD-WAN-Usability-Assistent
- Skalierbarkeit von Verbindungen (SPI, DPI, TLS)

Verbessertes Dashboard

- 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 Sicherheit
- 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 Protection[1]

- 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[1]
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client[1]

Intrusion-Prevention[1]

- Signaturbasierte Scans
- Integration der Netzwerkzugriffskontrolle mit Aruba ClearPass
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filterung mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[1]

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

Anwendungsidentifizierung[1]

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

Visualisierung und Analyse des Datenverkehrs

Benutzeraktivitäten

- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[1]

- URL-Filterung
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- DNS-Filterung
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Rating-Kategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN und ZTNA

- 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, Android
- Routenbasiertes VPN (OSPF, RIP, BGP)
- Secure Private Access auf Basis von Cloud Secure Edge

Netzwerk

- PortShield
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung (NS*a* 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-Layout
  - Dashboard

SONICWALL

- Geräteinformationen, Anwendungen, Bedrohungen
- Topology View
- Vereinfachte Erstellung und Verwaltung von Richtlinien

- Nutzungsstatistiken zu Regeln/Objekten
  - Verwendet vs. nicht verwendet
  - Aktiv vs. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung
- Interne und externe Speicherverwaltung
- WWAN-USB-Kartenunterstützung (5G/LTE/4G/3G)
- Unterstützung von Network Security Manager (NSM)
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- Einfaches CSC-Reporting
- Unterstützung der mobilen SonicExpress-App
- SNMP V2/V3
- 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- und -Firewall-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 TZ380W)

- 802.11ax
- 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] Erfordert zusätzliches Abo.

Erfahren Sie mehr über die SonicWall Gen 8 TZ Series

www.sonicwall.com/TZ

Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose 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
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

© 2023 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 Tochtergesellschaften von SonicWall Inc. übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.