

SCHEDA TECNICA

Serie SonicWall TZ (Gen 8)

Piattaforma SD-Branch integrata con firewall di nuova generazione ad alta efficacia per PMI e filiali

I firewall della nuova serie SonicWall TZ, progettati per le piccole e medie imprese e per aziende distribuite con sedi SD-Branch, offrono prestazioni eccellenti con un basso TCO.

Questi firewall di ultima generazione (NGFW) rispondono alle attuali tendenze in tema di crittografia web, dispositivi connessi e mobilità ad alta velocità, fornendo una soluzione che soddisfa le esigenze di rilevamento e prevenzione automatica delle violazioni in tempo reale.



La serie TZ in breve.

[Specifiche complete »](#)

Throughput di prevenzione minacce (max.)	Connessioni (max.)	Porte
Fino a 3 Gb/s	Fino a 1,5 milioni	Fino a 8x1GbE, 2x10/5/2,5G SFP+

CARATTERISTICHE PRINCIPALI

- Interfacce fino a 10/5/2,5/1 GbE nel formato desktop
- Compatibilità SD-Branch
- Funzionalità SD-WAN sicura
- Onboarding con la app SonicExpress
- Implementazione Zero Touch
- Predisposizione per SonicWall Unified Management
- Gestione centralizzata semplificata tramite Network Security Manager (NSM)
- Integrazione con switch SonicWall, access point SonicWave e Capture Client
- Memoria integrata ed espandibile
- Alimentazione ridondante
- Sicurezza DNS
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Gestione firewall Wi-Fi 6
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Alta densità di porte
- Failover cellulare
- Supporto per TLS 1.3
- Prestazioni innovative
- Elevato numero di connessioni
- Prestazioni DPI veloci
- Basso TCO
- Supporto per Cloud Secure Edge Connector
- Garanzia informatica integrata

Solo per i firewall venduti e registrati dopo il 1° novembre 2024.

I firewall della serie TZ di Generazione 8 (Gen 8) offrono un'elevata scalabilità e un alto numero di porte (fino a 10). La memoria integrata ed espandibile fino a 512 GB consente diverse funzioni tra cui registrazione di log, creazione di report, memorizzazione in cache, backup del firmware e molto altro. Un secondo alimentatore opzionale, disponibile per alcuni modelli, garantisce una maggiore ridondanza in caso di guasti.

L'installazione dei firewall TZ Gen 8 è ulteriormente semplificata dalla modalità Zero-Touch, che consente di installare contemporaneamente i firewall in più sedi con un intervento minimo del personale IT. I nuovi dispositivi, basati su hardware di nuova generazione e dotati di funzionalità firewall, switch e wireless, consentono di gestire da un unico pannello di controllo gli switch SonicWall e gli access point SonicWave. La stretta integrazione con Capture Client garantisce inoltre una protezione ottimale degli endpoint.

SonicOS e servizi di sicurezza

L'architettura SonicOS è l'elemento centrale dei firewall TZ di nuova generazione. I firewall TZ Gen 8 sono basati sul sistema operativo [SonicOS 8](#), dotato di una nuova e moderna interfaccia utente e di numerose funzionalità avanzate di sicurezza, gestione e connettività. La serie TZ Gen 8 integra funzionalità [SD-WAN](#), supporto TLS 1.3, visualizzazione in tempo reale, rete privata virtuale (VPN) ad alta velocità e altre potenti funzioni di sicurezza.

Le minacce sconosciute vengono inviate per l'analisi alla sandbox multi-engine [Capture Advanced Threat Protection \(ATP\)](#) basata su cloud di SonicWall. Capture ATP utilizza la nostra tecnologia brevettata [Real-Time Deep Memory Inspection \(RTDMI™\)](#). RTDMI, uno dei motori di Capture ATP, rileva e blocca il malware e le minacce zero-day mediante l'analisi diretta in memoria.

Grazie all'azione combinata di Capture ATP con tecnologia RTDMI e di servizi di sicurezza come [Reassembly-Free Deep Packet Inspection \(RFDPI\)](#), protezione antivirus e antispyware, sistema di prevenzione delle intrusioni, controllo e gestione delle applicazioni, servizi di filtraggio dei contenuti e ispezione DPI-SSL, i firewall della serie TZ bloccano malware, ransomware e altre minacce avanzate a livello del gateway.

Le suite di sicurezza offerte con i firewall Gen 8 di nuova generazione includono una garanzia informatica integrata di Cysurance fino a 200.000 dollari, senza costi aggiuntivi.¹

Le aziende possono utilizzare la nuova integrazione di Cloud Secure Edge Connector per fornire l'accesso sicuro alle proprie applicazioni private in modo semplice e centralizzato. Questo approccio garantisce che l'attendibilità dell'utente e del dispositivo venga ripetutamente verificata prima di concedere l'accesso ad applicazioni specifiche, indipendentemente dalla posizione e dal tipo di endpoint.

Per maggiori informazioni, consultare [l'architettura e i servizi della Generazione 8](#).

¹ Solo per i firewall venduti e registrati dopo il 1° novembre 2024.

Implementazioni

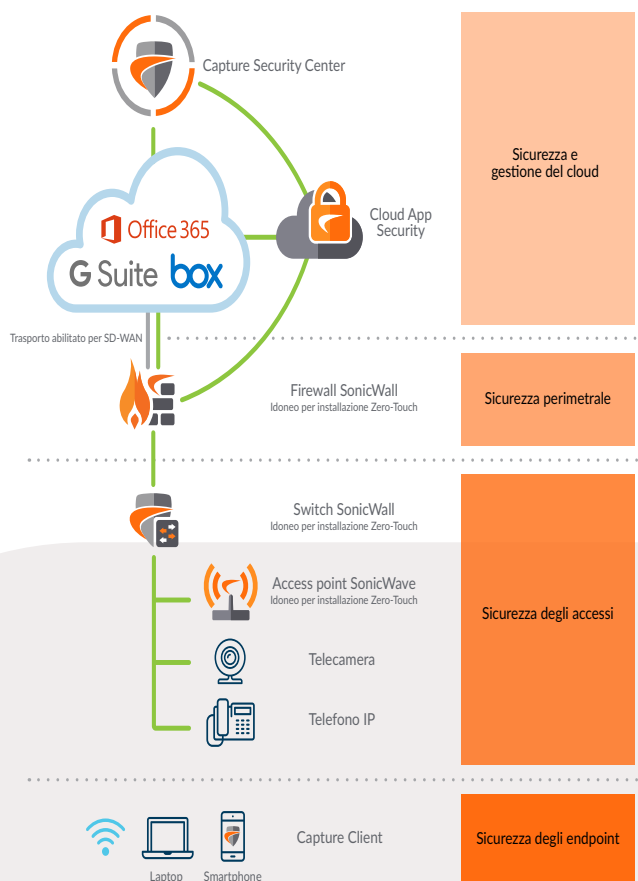
Piccole e medie imprese

- Risparmiare spazio e denaro con una soluzione di sicurezza integrata per gateway con funzionalità firewall, switch e wireless
- Ridurre la complessità e garantire l'operatività senza l'intervento di tecnici informatici, con facilità di presa in carico tramite l'app SonicExpress e la funzione di installazione Zero-Touch, oltre alla praticità della gestione da un unico pannello di controllo
- Raggiungere la continuità aziendale fornendo un failover per la connettività cellulare
- Proteggere la rete dagli attacchi con una soluzione di sicurezza completa che include VPN, IPS, CFS, antivirus e molto altro
- Sfruttare l'alta densità di porte per alimentare diversi dispositivi PoE, come telefoni IP e telecamere IP con TZ580
- Aumentare la produttività dei dipendenti bloccando l'accesso non autorizzato con policy di accesso e segmentazione del traffico



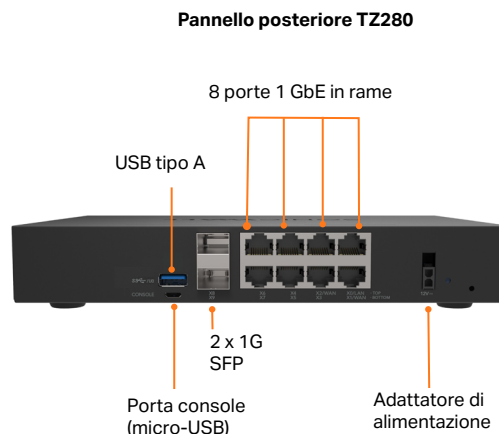
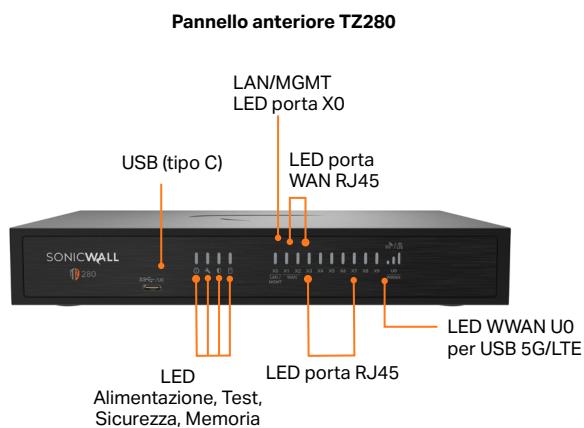
Aziende distribuite con SD-Branch

- Migliorare l'esperienza dei clienti e la capacità di adattamento alle mutevoli esigenze aziendali mediante la connettività per filiali di nuova generazione con SD-Branch
- Favorire la crescita aziendale investendo in dispositivi di nuova generazione dotati di funzionalità di sicurezza multi-gigabit avanzate, compatibili con le future trasformazioni delle reti e della sicurezza
- Proteggere le reti dagli attacchi più avanzati con funzioni di sicurezza avanzate e il blocco automatico delle minacce nel traffico decriptato tramite protocolli come TLS 1.3
- Sfruttare la sicurezza di rete end-to-end mediante l'integrazione trasparente di access point SonicWave, switch SonicWall e Capture Client
- Garantire una comunicazione efficace tra i punti vendita e la sede centrale attraverso una facile connettività VPN, per consentire ai responsabili IT di creare una configurazione hub-and-spoke per il trasferimento sicuro dei dati tra tutte le sedi
- Migliorare l'efficienza e le prestazioni aziendali e ridurre i costi grazie all'ottimizzazione hardware e software della serie TZ Gen 8, oltre a funzionalità come la tecnologia SD-WAN
- Scalare i dispositivi in modo semplice e rapido con la app SonicExpress e l'implementazione zero-touch
- Garantire la continuità aziendale fornendo un failover per la connettività cellulare
- Mantenere la conformità alle caratteristiche di sicurezza e utilizzare la memoria integrata e quella espandibile per archiviare i log a fini di verifica



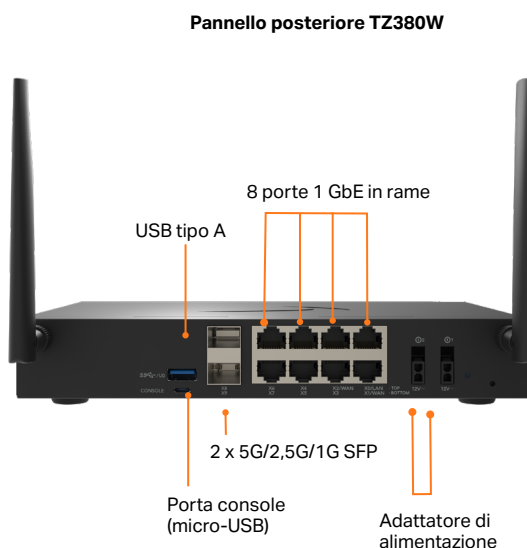
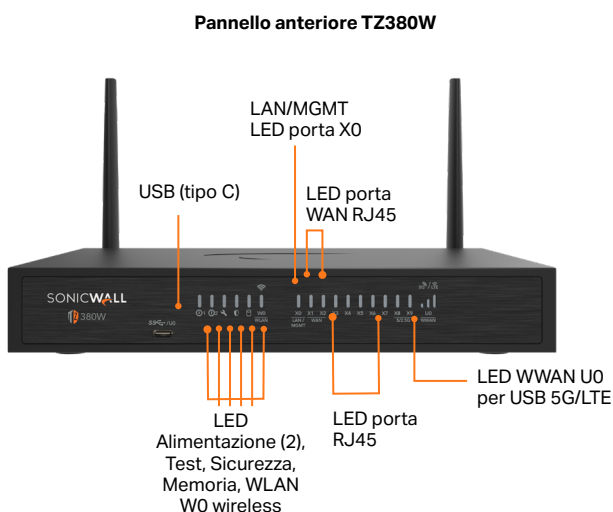
SonicWall TZ280

I firewall della serie TZ280, progettati per ambienti domestici, piccoli uffici e filiali snelle, si distinguono per la comprovata efficacia della sicurezza e l'eccellente rapporto qualità-prezzo.



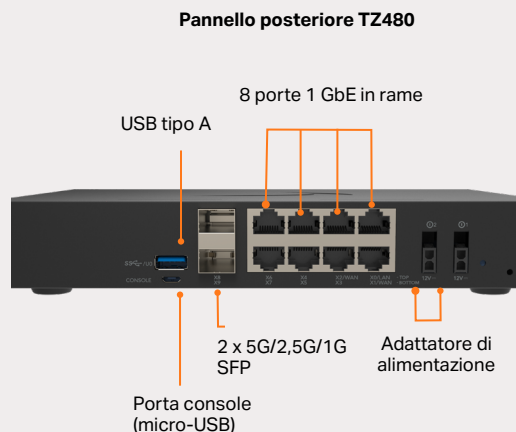
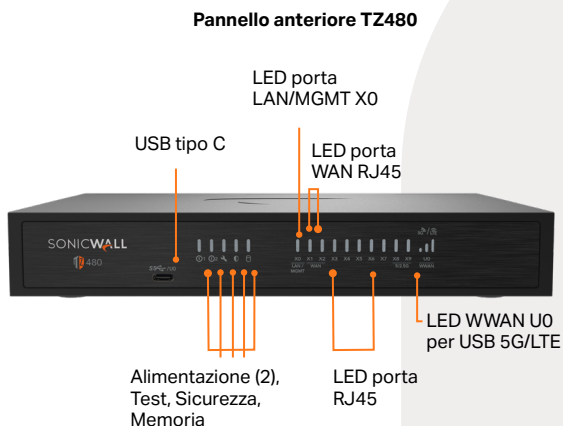
Serie SonicWall TZ380

I firewall della serie TZ380, progettati per piccole aziende e filiali snelle, si distinguono per la comprovata efficacia della sicurezza e l'eccellente rapporto qualità-prezzo.



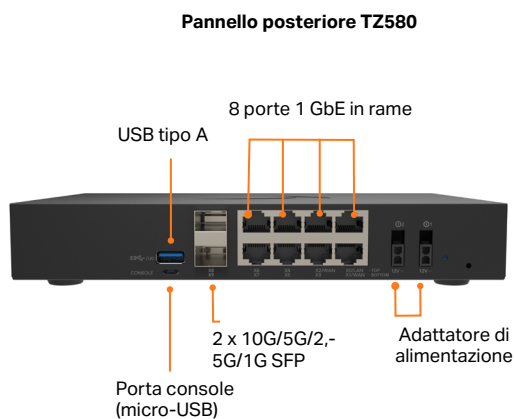
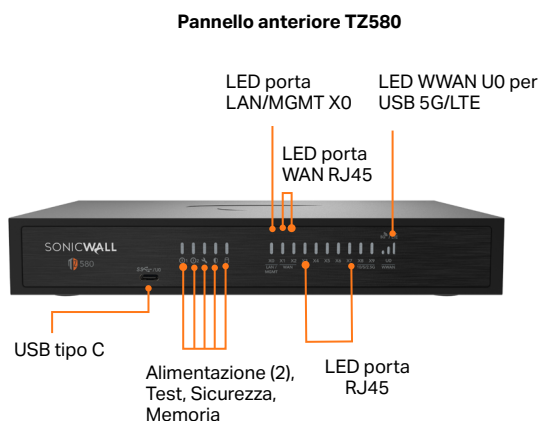
Serie SonicWall TZ480

I firewall della serie TZ480, progettati per piccole imprese e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e l'eccellente rapporto qualità-prezzo.



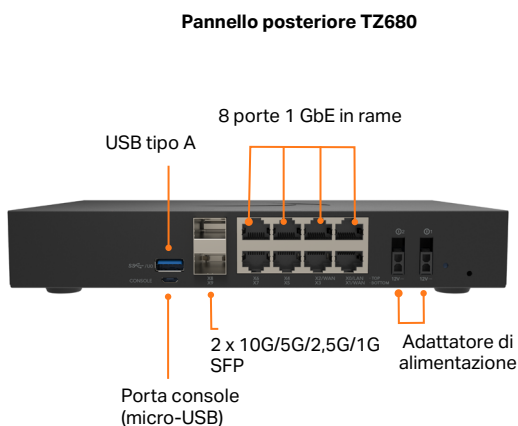
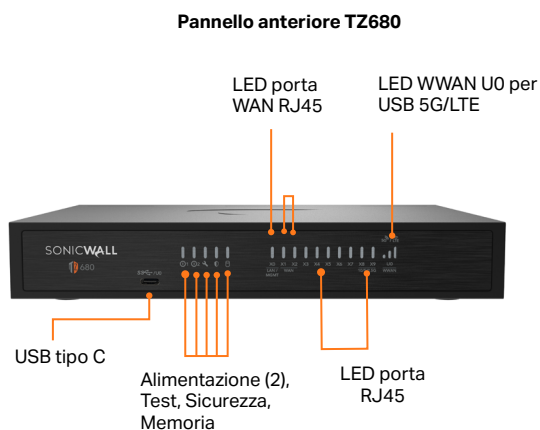
Serie SonicWall TZ580

I firewall della serie TZ580, progettati per PMI e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e l'eccellente rapporto qualità-prezzo.



Serie SonicWall TZ680

I firewall della serie TZ680, progettati per imprese di medie dimensioni e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e un eccellente rapporto qualità-prezzo.



Specifiche tecniche della serie SonicWall TZ (Gen 8)

Firewall in generale	Serie TZ280	Serie TZ380	Serie TZ480	Serie TZ580	Serie TZ680
Sistema operativo	SonicOS 8				
Interfacce	8 x 1GbE Cu, 2 x 1G SFP, 1 console (micro-USB), 1 USB (tipo C)	8 x 1GbE Cu, 2 x 5G/2,5G/1G SFP, 1 console (micro-USB), 1 USB (tipo C)	8 x 1GbE Cu, 2 x 5G/2,5G/1G SFP, 1 console (micro-USB), 1 USB (tipo C)	8 x 1GbE Cu, 2 x 10G/5G/2,5G/1G SFP, 1 console (micro-USB), 1 USB (tipo C)	8 x 1GbE Cu, 2 x 10G/5G/2,5G/1G SFP, 1 console (micro-USB), 1 USB (tipo C)
Supporto wireless	N/D	2x2 802.11ax (TZ380W)	N/D	N/D	N/D
Memoria / (espansione)	(Opzionale: fino a 512 Gb)	(Opzionale: fino a 512 Gb)	(Opzionale: fino a 512 Gb)	(Opzionale: fino a 512 Gb)	(Opzionale: fino a 512 Gb)
Gestione centralizzata	Network Security Manager (NSM) 3.0 e superiore, CLI, SSH, Web UI, API REST				
Interfacce VLAN logiche e tunnel (max.)	64	128	128	256	256
Utenti Single Sign-On (SSO) SAML ¹	1000	1000	2500	2500	2500
Punti di accesso supportati (max.)	16	16	32	32	32
Prestazioni firewall/VPN					
Throughput di ispezione firewall ²	2,5 Gb/s	3,5 Gb/s	4 Gb/s	4,5 Gb/s	5 Gb/s
Throughput di prevenzione delle minacce ³	1 Gb/s	1,5 Gb/s	2 Gb/s	2,2 Gb/s	2,5 Gb/s
Throughput di ispezione applicazioni ³	1,5 Gb/s	2,0 Gb/s	2,2 Gb/s	2,5 Gb/s	3 Gb/s
Throughput IPS ³	1,5 Gb/s	2,0 Gb/s	2,2 Gb/s	2,5 Gb/s	3 Gb/s
Throughput di ispezione anti-malware ³	1 Gb/s	2,0 Gb/s	2 Gb/s	2,2 Gb/s	2,5 Gb/s
Throughput ispezione e decrittografia TLS/SSL ³	430 Mb/s	600 Mb/s	650 Mb/s	750 Mb/s	800 Mb/s
Throughput VPN IPsec ⁴	1,2 Gb/s	1,6 Gb/s	2 Gb/s	2,2 Gb/s	2,5 Gb/s
Connessioni al secondo	12.000	15.000	18.000	20.000	26.000
Connessioni SPI (max.)	1.000.000	1.100.000	1.200.000	1.400.000	1.600.000
Connessioni DPI (max.)	200.000	250.000	350.000	500.000	600.000
Connessioni TLS (max.)	35.000	40.000	50.000	60.000	75.000
VPN e ZTNA					
Tunnel VPN site-to-site	200	200	200	250	250
Client VPN IPsec (max.)	5 (200)	5(200)	5(200)	10(500)	10(500)
Licenze VPN SSL (max.)	1 (50)	2(100)	2(150)	2(200)	2(250)
Autenticazione/crittografia	AES (128, 192, 256 bit)/MD5, SHA-256, SHA-384, crittografia Suite B				
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v				
VPN basata su route	RIP, OSPF, BGP				
Certificati supportati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWall a SonicWall, SCEP				
Caratteristiche VPN	Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, gateway VPN ridondante, VPN basata su routing				
Piattaforme client supportate per la VPN globale	Microsoft® Windows 10 e Windows 11				
NetExtender	Microsoft® Windows 10 e Windows 11, Linux				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™				
Accesso privato SonicWall basato su Cloud Secure Edge ⁵	Incluso nel programma di fidelizzazione 3&Free				
Servizi di sicurezza					
Servizi di ispezione Deep Packet	Antivirus gateway, antispysware, prevenzione delle intrusioni, decrittografia TLS				
Content Filtering Service (CFS)	Filtraggio degli URL basato sulla reputazione, scansione di URL HTTP, IP HTTPS, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, elenchi di siti consentiti/vietati				
Servizio anti-spam completo	Sì	Sì	Sì	Sì	Sì
Visualizzazione delle applicazioni	Sì	Sì	Sì	Sì	Sì

Controllo delle applicazioni	Sì	Sì	Sì	Sì	Sì
Capture Advanced Threat Protection	Sì	Sì	Sì	Sì	Sì
Filtraggio DNS avanzato	Sì	Sì	Sì	Sì	Sì
Connettività di rete					
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay				
Modalità NAT	1:1, 1:many, many:1, many:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente				
Protocolli di routing	BGP, OSPF, RIPv1/v2, route statici, routing basato su policy				
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1e (WMM)				
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, TACACS+, SSO SAML ¹ , accounting Radius, NTLM, database utenti interno, 2FA, servizi Terminal, Citrix, Common Access Card (CAC)				
Database utenti locale	1000	1000	1000	1000	1000
VoIP	H3230v1.5 SIP completo				
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certificazioni	IPv6				
Alta disponibilità	Attiva/Standby con sincronizzazione dello stato				
Hardware					
Fattore di forma	Desktop				
Alimentazione	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
Potenza max. assorbita (W)	12,36	13,77 (TZ380) 17,4 (TZ380W)	13,77	15,6	16,99
Tensione di esercizio	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
Alimentazione ridondante	1 (opzionale)	1 (opzionale)	1 (opzionale)	1 (opzionale)	1 (opzionale)
Dissipazione di calore totale (BTU)	42,43	46,95 (TZ380) 59,33 (TZ380W)	42,43	56,74	57,93
Dimensioni (unità: cm)	3,5x13x19 Confezione: 7,2x22,8x23	3,5 x 13 x 19 Confezione: 7,2 x 22,8 x 23	3,5 x 13 x 19 Confezione: 7,2 x 22,8 x 23	3,5 x 13 x 19 Confezione: 7,2 x 22,8 x 23	3,5 x 13 x 19 Confezione: 7,2 x 22,8 x 23
Peso	0,82 kg	0,82 kg (TZ380) 0,85 kg (TZ380W)	0,82 kg	0,97 kg	0,97 kg
Peso RAEE	1,18 kg	1,18 kg (TZ380) 1,24 kg (TZ380W)	1,18 kg	1,42 kg	1,42 kg
Peso con la confezione	1,41 kg	1,41 kg (TZ380) 1,47 kg (TZ380W)	1,41 kg	1,93 kg	1,93 kg
MTBF a 25 °C in anni	51,7	46,4 (TZ380) 24,9 (TZ380W)	52,8	30,7	29,9
Condizioni ambientali (in funzionamento/stoccaggio)	da 0 °C a +40 °C / da -40 °C a +70 °C	da 0 °C a +40 °C / da -40 °C a +70 °C	da 0 °C a +40 °C / da -40 °C a +70 °C	da 0 °C a +40 °C / da -40 °C a +70 °C	da 0 °C a +40 °C / da -40 °C a +70 °C
Umidità	5-95% senza condensa	5-95% senza condensa	5-95% senza condensa	5-95% senza condensa	5-95% senza condensa

Wireless integrato (solo TZ380W)

Standard	802.11a/b/g/n/ac/ax WPA,WPA2, WPA3, 802.11i, EAP-PEAP, EAP-TTLS
Bande di frequenza	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
Canali operativi	802.11a: USA e Canada 12, Europa 11, Giappone 4, Singapore 4, Taiwan 4; 802.11b/g: USA e Canada 1-11, Europa 1-13, Giappone 1-14 (14 solo 802.11b); 802.11n (2,4 GHz): USA e Canada 1-11, Europa 1-13, Giappone 1-13; 802.11n (5 GHz): USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64; 802.11ac: USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64
Potenza di trasmissione in uscita	In base al dominio normativo specificato dall'amministratore di sistema
TPC (Transmit Power Control)	Sì

Velocità di trasmissione dati supportate	802.11a: 6, 9,12,18, 24, 36, 48, 54 Mb/s per canale; 802.11b: 1, 2, 5,5, 11 Mb/s per canale; 802.11g: 6, 9,12,18, 24, 36, 48, 54 Mb/s per canale; 802.11n: 15,30,45,60,90,120,135,150,30,60,90,120,180,240,270,300 Mb/s per canale; 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 Mb/s per canale; 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 Mb/s per canale
Spettro tecnologia di modulazione	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

Normative

Numeri di modello normativi	APL70-11D	APL72-120 (TZ380) APL72-121 (TZ380W)	APL72-120	APL72-120	APL72-120
Principali normative di conformità	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe B, KCC/MSIP, BSMI, MTCTE/TEC, CB	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal & Radio, VCCI Classe B, KCC/MSIP, BSMI, MTCTE/TEC, CB	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe B, KCC/MSIP, BSMI, MTCTE/TEC, CB	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe B, KCC/MSIP, BSMI, MTCTE/TEC, CB	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe B, KCC/MSIP, BSMI, MTCTE/TEC, CB
Conformità normative principali (modelli wireless)	N/D	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe B, KCC/MSIP, BSMI, NCC SRRC, MTCTE/TEC, CB	N/D	N/D	N/D
Conformità alle principali normative (modelli PoE)	N/D	N/D	N/D	N/D	N/D

- ¹ Il Single Sign-On SAML è disponibile in SonicOS 8.1, che sarà rilasciato a breve.
- ² Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare a seconda delle condizioni di rete e dei servizi attivati.
- ³ Rilevazione throughput per prevenzione minacce/Gateway AV/antispysware/IPS tramite strumenti di test delle performance Keysight HTTP standard nel settore. Rilevazione throughput di prova con Gateway AV, Anti-Spyware, IPS e Application Control attivati
- ⁴ Throughput VPN rilevato con il traffico UDP mediante pacchetti da 1418 byte, crittografia AESGMAC16-256 in conformità a RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.
- ⁵ Incluso nel pacchetto di 3 anni

SERVIZI OFFERTI DAI PARTNER

Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partner sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni:

www.sonicwall.com/PES

Riepilogo delle funzioni di SonicOS 8

Firewall

- Ispezione Stateful Packet
- Ispezione Reassembly-Free Deep Packet
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- Supporto API completo
- Integrazione switch SonicWall
- Integrazione AP SonicWall Wi-Fi 6
- Scalabilità SD-WAN
- Procedura guidata di usabilità SD-WAN
- Scalabilità delle connessioni (SPI, DPI, TLS)

Dashboard ottimizzata

- Visualizzazione migliorata dei dispositivi
- Riepilogo traffico e utenti principali
- Informazioni sulle minacce
- Centro notifiche

Decrittazione e ispezione TLS/SSL/SSH

- TLS 1.3 con sicurezza migliorata
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- Miglioramenti per DPI-SSL con CFS
- Controlli DPI SSL granulari in base a zone o regole

Capture Advanced Threat Protection¹

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatizzato e manuale
- Informazioni sulle minacce con aggiornamenti in tempo reale¹
- Blocco fino al verdetto
- Capture Client¹

Prevenzione delle intrusioni¹

- Scansione basata sulle firme
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Identificazione tramite GeolP
- Filtraggio Botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware¹

- Scansione antimalware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware nel cloud

Identificazione delle applicazioni¹

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di perdite di dati
- Creazione di rapporti sulle applicazioni tramite NetFlow/IPFIX
- Database completo di firme delle applicazioni

Visualizzazione e analisi del traffico

Attività degli utenti

- Utilizzo applicazioni/larghezza di banda/minacce
- Analisi basate su cloud

Filtraggio dei contenuti Web HTTP/HTTPS¹

- Filtraggio URL
- Proxy avoidance
- Blocco in base a parole chiave
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Filtraggio DNS
- Filtraggio basato su policy (esclusione/inclusione)
- Inserimento intestazione HTTP
- Categorie di classificazione CFS per la gestione della larghezza di banda
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN e ZTNA

- Secure SD-WAN
- Provisioning automatico delle VPN
- VPN IPsec per una connettività Site-to-Site
- Accesso remoto tramite VPN SSL e client IPsec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Android
- VPN basata sul routing (OSPF, RIP, BGP)
- Accesso privato sicuro tramite Cloud Secure Edge

Connettività di rete

- PortShield
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (NSa 2650 e successivi)
- QoS livello 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Alta disponibilità A/P con sincronizzazione dello stato
- Bilanciamento del carico in ingresso/in uscita
- Alta disponibilità - Attiva/Standby con sincronizzazione dello stato
- Modalità Bridge (L2), Wire/Wire virtuale, Tap, NAT
- Routing asimmetrico
- Supporto CAC (Common Access Card)

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Gatekeeper H.323 e supporto per proxy SIP

Gestione, monitoraggio e supporto

- Supporto Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) v2.0
 - Progettazione o template di nuova concezione
 - Confronti con la media di settore e globale
- Nuova UI/UX, layout intuitivo delle funzioni
 - Dashboard

- Informazioni sui dispositivi, applicazioni, minacce
- Visualizzazione della topologia
- Definizione e gestione semplificate delle policy
- Statistiche d'uso per policy e oggetti
 - Utilizzato / non utilizzato
 - Attivo / non attivo
- Ricerca globale di dati statici
- Supporto memorizzazione
- Gestione memoria interna ed esterna
- Supporto scheda USB WWAN (5G/LTE/4G/3G)
- Supporto Network Security Manager (NSM)
- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning zero-touch
- Reportistica semplificata CSC
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Logging
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat

- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Schermata di gestione CD
- Gestione degli switch Dell serie N e X, compresi gli switch a cascata

Debugging e diagnostica

- Monitoraggio ottimizzato dei pacchetti
- Terminale SSH su interfaccia utente

Wireless

- Gestione firewall e AP SonicWave nel cloud
- WIDS/WIPS
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Connettività di rete 802.11s mesh
- Selezione automatica dei canali
- Analisi dello spettro RF
- Vista planimetrica
- Visualizzazione della topologia
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy

- MiFi extender
- Migliorie e potenziamenti RF
- Quota ciclica ospite

Wireless integrato (solo TZ380W)

- 802.11ax
- Dual band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac
- Rilevamento e prevenzione di intrusioni wireless
- Servizi wireless guest
- Lightweight hotspot messaging
- Segmentazione degli access point virtuali
- Captive portal
- ACL cloud

*Richiede la sottoscrizione aggiuntiva

Maggiori informazioni sulla serie SonicWall TZ Gen 8:

www.sonicwall.com/TZ

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e senza soluzione di continuità per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL®

© 2023 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari. Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. Salvo quanto specificato nei termini e nelle condizioni stabiliti nel contratto di licenza di questo prodotto, SonicWall e/o le sue affiliate non si assumono alcuna responsabilità ed escludono garanzie di qualsiasi tipo, esplicite, implicite o legali, in relazione ai propri prodotti, incluse, in via esemplificativa, qualsiasi garanzia implicita di commerciabilità, idoneità a scopi specifici o violazione di diritti altrui. SonicWall e/o le sue affiliate declinano ogni responsabilità per danni di qualunque tipo, siano essi diretti, indiretti, consequenziali, punitivi, speciali o incidentali (inclusi, senza limitazioni, danni per mancato guadagno, interruzioni dell'attività o perdite di dati) derivanti dall'utilizzo o dall'impossibilità di utilizzare il presente documento, anche nel caso in cui SonicWall e/o le sue affiliate siano state avvertite dell'eventualità di tali danni. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riservano il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.