SONICWALL

Serie SonicWall TZ

Prevenzione delle minacce e piattaforma SD-Branch integrata per PMI e aziende distribuite

La serie SonicWall TZ consente a PMI e aziende distribuite di sfruttare i vantaggi di una soluzione di sicurezza integrata che soddisfa ogni esigenza. Combinando la prevenzione delle minacce ad alta velocità e la tecnologia SD-WAN (Software-Defined Wide Area Networking) con un'ampia gamma di funzionalità di rete e wireless, oltre all'installazione semplificata e alla gestione centralizzata, la serie TZ offre una soluzione di sicurezza unificata a un basso costo di proprietà.

Soluzione di sicurezza flessibile e integrata

Alla base della serie TZ c'è SonicOS, il sistema operativo SonicWall ricco di funzioni. I firewall compatibili con l'ultima versione del sistema operativo SonicOS 7.0 si contraddistinguono per le nuove caratteristiche di interfaccia e interazione utente (UI/UX) di concezione moderna, la sicurezza avanzata e le funzioni di gestione semplificata delle politiche e delle reti.

Inoltre il sistema operativo Sonic presenta tutta una serie di potenti caratteristiche che consentono alle aziende di ottimizzare questi firewall UTM (Unified Threat Management) secondo requisiti di rete specifici. Ad esempio, la realizzazione di una rete wireless sicura ad alta velocità è semplificata dal controller wireless integrato, che supporta gli standard IEEE 802.11, con la possibilità di aggiungere i nostri access point SonicWave 802.11ac Wave 2. Per ridurre i costi e la complessità di connessione degli access point wireless ad alta velocità e di altri dispositivi con funzionalità Power over Ethernet (PoE) come telecamere, telefoni e stampanti IP, i modelli TZ300P, TZ600P e TZ570P sono dotati di alimentazione PoE/PoE+.

Le aziende della grande distribuzione e le istituzioni scolastiche distribuite possono usufruire dei numerosi strumenti del sistema operativo per ottenere vantaggi ancora maggiori. Le filiali possono scambiare informazioni con la sede centrale in completa sicurezza utilizzando una rete privata virtuale (VPN). La definizione di LAN virtuali (VLAN) consente di segmentare la rete in gruppi aziendali e di clienti separati con regole che stabiliscono il livello di comunicazione con i dispositivi di altre VLAN. L'SD-WAN costituisce un'alternativa sicura ai costosi circuiti MPLS, fornendo al tempo stesso prestazioni costanti e disponibilità delle applicazioni. L'installazione dei firewall TZ nelle sedi remote è particolarmente semplice grazie alla funzione Zero-Touch Deployment, che consente il provisioning dei firewall da remoto attraverso il cloud.

Prevenzione delle minacce e prestazioni di livello superiore

La nostra filosofia di protezione delle reti nell'attuale panorama delle minacce informatiche in continua evoluzione consiste nel rilevare e prevenire automaticamente le minacce in tempo reale. Grazie alla combinazione di tecnologie integrate basate sul cloud, i nostri firewall dispongono di una protezione la cui elevata efficacia è stata confermata da test indipendenti di terzi. Le minacce sconosciute vengono inviate alla sandbox multi-engine Capture Advanced Threat Protection (ATP) nel cloud per essere analizzate. Capture ATP si basa sulla nostra tecnologia Real-Time Deep Memory Inspection (RTDMI™) in attesa di brevetto. L'engine RTDMI rileva e blocca il malware e le minacce zero-day mediante analisi diretta in memoria. La tecnologia RTDMI di SonicWall è precisa, riduce al minimo i falsi positivi e identifica e attenua gli attacchi sofisticati in cui l'armamentario del malware resta

Vantaggi:

Soluzione di sicurezza flessibile e integrata

- Interfacce multi-gigabit in formato desktop
- Secure SD-Branch con SD-WAN
- Potente sistema operativo SonicOS 7.0
- Connettività wireless 802.11ac Wave 2 ad alta velocità
- Power over Ethernet (PoE/PoE+)
- Supporto 5G/4G/LTE
- Memoria integrata ed espandibile
- Alimentazione ridondante

Prevenzione delle minacce e prestazioni di livello superiore

- Tecnologia Real-Time Deep Memory Inspection in attesa di brevetto
- Tecnologia Reassembly-Free Deep Packet Inspection brevettata
- Supporto TLS 1.3
- Efficacia della sicurezza comprovata nel settore

Semplicità di installazione, configurazione e gestione

- Installazione zero-touch
- Gestione centralizzata basata sul cloud e interna
- Presa in carico delle applicazioni SonicExpress

esposto per meno di 100 nanosecondi. Viene inoltre utilizzato in combinazione il nostro engine RFDPI (Reassembly- Free Deep Packet Inspection) a singola fase brevettato per esaminare ogni byte di ogni pacchetto, ispezionando il traffico in entrata e in uscita direttamente sul firewall. Sfruttando Capture ATP con tecnologia RTDMI, integrati nella piattaforma SonicWall Capture Cloud, oltre a funzionalità on-box come prevenzione delle intrusioni, anti-malware e filtraggio Web/URL, i firewall della serie TZ bloccano il malware, il ransomware e altre minacce a livello del gateway. Per i dispositivi mobili utilizzati all'esterno del perimetro del firewall, SonicWall Capture Client fornisce un ulteriore livello di protezione applicando tecniche di protezione avanzate contro le minacce, come l'apprendimento automatico e il rollback di sistema. Inoltre consente l'ispezione approfondita del traffico TLS crittografato (SSL DPI) sui firewall della serie TZ mediante l'installazione e la gestione di certificati TLS affidabili.

Con il continuo aumento dell'uso della crittografia per proteggere le sessioni web, è indispensabile che i firewall siano in grado di esaminare il traffico crittografato alla ricerca di minacce. I firewall della serie TZ offrono una protezione completa attraverso la decrittazione e l'ispezione complete delle connessioni TLS/SSL ed SSH crittografate, indipendentemente dalla porta o dal protocollo utilizzati. Il firewall ricerca eventuali non conformità ai protocolli, minacce, zero-day, intrusioni e persino criteri definiti esaminando a fondo ogni singolo pacchetto. L'engine d'ispezione Deep Packet rileva e previene gli attacchi nascosti che sfruttano la crittografia. Inoltre blocca il download di malware crittografato, interrompe la diffusione di infezioni e impedisce comunicazioni di comando e controllo (C&C) e la sottrazione di dati. Le regole di inclusione e di esclusione consentono di stabilire quale traffico dev'essere sottoposto alla decrittazione e all'ispezione in base a requisiti di conformità specifici dell'azienda e/o legali.

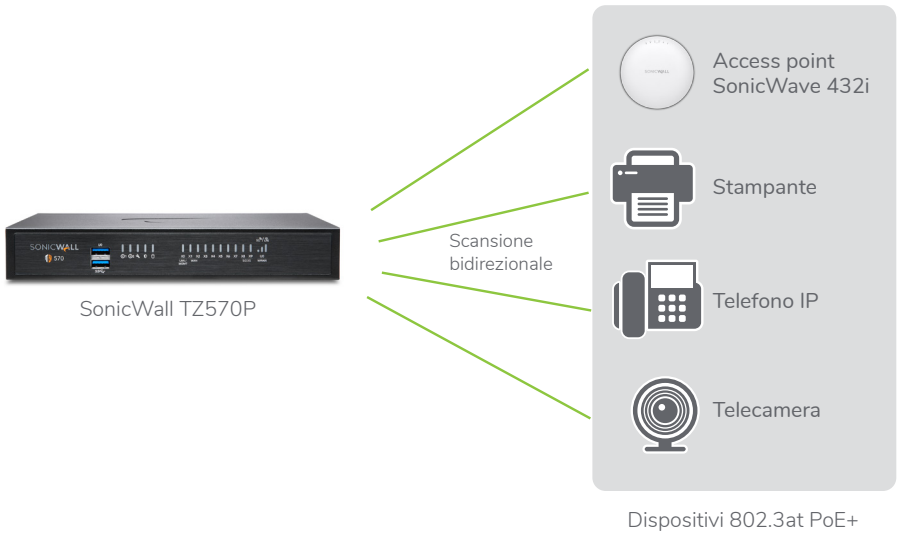
I modelli TZ670 e TZ570 sono compatibili con TLS 1.3, che prevede diversi cambiamenti che migliorano le prestazioni e la sicurezza, eliminando al tempo stesso le complessità.

Semplicità di installazione, configurazione e gestione

SonicWall semplifica la configurazione e la gestione dei firewall della serie TZ e degli access point SonicWave 802.11ac Wave 2, ovunque siano installati. La gestione centralizzata, la reportistica, le licenze e le analisi sono gestite dal nostro Capture Security Center basato sul cloud, che offre la massima visibilità, agilità e capacità di amministrare centralmente l'intero ecosistema di sicurezza SonicWall da un'unica consolle di controllo.

Una componente fondamentale del Capture Security Center è l'installazione zero-touch (Zero-Touch Deployment). Questa funzione, basata sul cloud, semplifica e velocizza l'installazione e il provisioning dei firewall SonicWall presso le sedi remote e le filiali aziendali. Il processo richiede un intervento minimo da parte dell'utente ed è completamente automatizzato per rendere operativi i firewall su vasta scala in pochi passaggi. Ciò riduce significativamente il tempo, i costi e la complessità associati all'installazione e alla configurazione, mentre la protezione e la connettività vengono applicate in modo immediato e automatico. Le procedure semplificate di installazione e di configurazione e la facilità di gestione consentono alle organizzazioni di ridurre il costo totale di proprietà e ottenere un elevato ritorno sull'investimento.

** 802.11ac non è attualmente disponibile per 250 modelli SOHO/SOHO, che supportano 802.11a/b/g/n*



Sicurezza e alimentazione integrate per i dispositivi PoE

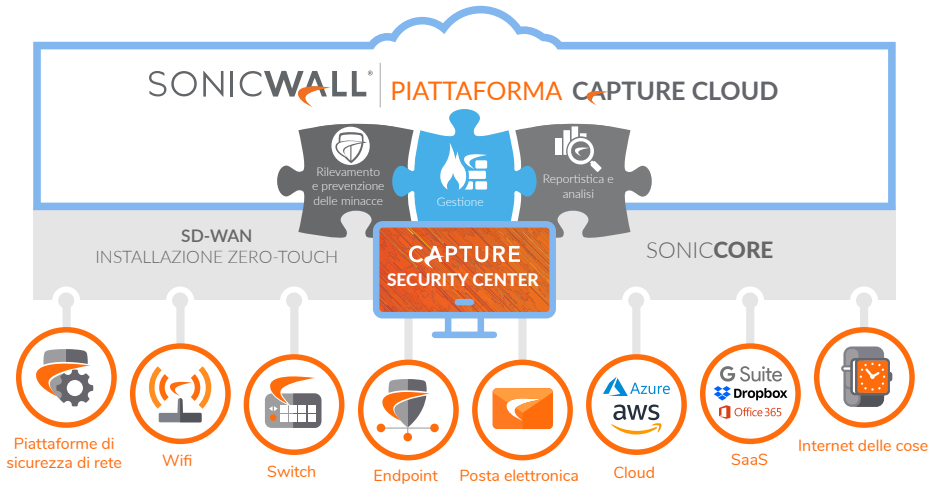
I dispositivi con funzionalità PoE possono essere alimentati senza il costo e la complessità di uno switch o un iniettore Power over Ethernet. I firewall TZ300P, TZ600P e TZ570P integrano la tecnologia IEEE 802.3at che consente di alimentare dispositivi PoE e PoE+ come access point wireless, telecamere, telefoni IP e molto altro. Il firewall scansiona tutto il traffico in entrata e in uscita da ogni dispositivo mediante la tecnologia Deep Packet Inspection, quindi elimina le minacce pericolose come malware e intrusioni, anche su connessioni crittografate.

Piattaforma Capture Cloud

La piattaforma Capture Cloud di SonicWall utilizza la prevenzione delle minacce basata sul cloud e la gestione della rete oltre a funzioni di reportistica e analisi per organizzazioni di qualsiasi dimensione. La piattaforma consolida le informazioni sulle minacce raccolte da molteplici fonti, tra cui il nostro premiato servizio sandbox di rete multi-engine Capture Advanced Threat Protection, e oltre 1 milione di sensori SonicWall situati in tutto il mondo.

Se i dati in arrivo nella rete contengono codice maligno precedentemente non rilevato, il team interno Capture Labs di SonicWall dedicato alla ricerca delle minacce sviluppa segnature che vengono archiviate nel database della piattaforma Capture Cloud e distribuite ai firewall dei clienti per aggiornare la protezione. I nuovi aggiornamenti vengono attivati immediatamente senza riavvii o interruzioni. Le segnature residenti nell'apparecchiatura forniscono protezione da numerose classi di attacchi, coprendo decine di migliaia di singole minacce. Oltre alle contromisure sull'apparecchiatura, i firewall TZ hanno anche accesso continuo al database della piattaforma Capture Cloud, che amplia le informazioni sulle segnature integrate con decine di milioni di segnature.

La piattaforma Capture Cloud fornisce la prevenzione delle minacce e offre un unico pannello di gestione da cui gli amministratori possono facilmente creare report in tempo reale e storici sull'attività di rete.



Protezione contro le minacce avanzate

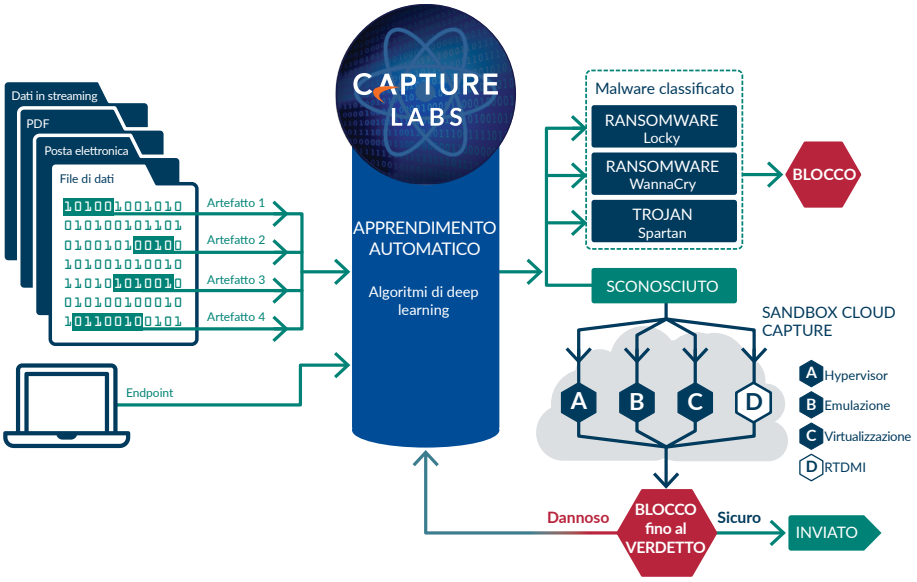
Al centro della prevenzione automatica delle violazioni in tempo reale vi sono due tecnologie di rilevamento del malware avanzate: Capture Advanced Threat Protection™ (Capture ATP) e Capture Security appliance™ (CSa).

Capture ATP è una piattaforma di sandbox multi-engine basata sul cloud, che comprende Real-Time Deep Memory Inspection™ (RTDMI), sandboxing virtualizzato, emulazione completa del sistema e tecnologia di analisi a livello di hypervisor. CSa è un dispositivo per installazione interna dotato di tecnologia RTDMI, che utilizza tecniche dinamiche e statiche basate sulla memoria per emettere verdetti definitivi e precisi. Entrambe le soluzioni ampliano la protezione contro le minacce avanzate al rilevamento e alla prevenzione degli attacchi zero-day in tutta una gamma di soluzioni SonicWall come i firewall di prossima generazione.

I file sospetti vengono inviati a una delle due soluzioni dove vengono analizzati utilizzando algoritmi di deep learning con la possibilità di trattenerli nel gateway fino a quando non viene stabilito un verdetto. Nel caso di Capture ATP, quando i file vengono identificati come nocivi vengono bloccati e viene immediatamente creato un hash nel database Capture ATP per tutti i clienti per beneficiare del blocco degli attacchi successivi. In ultima analisi queste segnature vengono inviate ai firewall per realizzare difese statiche. Per motivi di privacy ed esigenze di conformità i risultati prodotti da CSa non vengono diffusi fuori dall'organizzazione.

Questi servizi analizzano un'ampia gamma di sistemi operativi e tipologie di file, tra cui programmi eseguibili, DLL, PDF, documenti MS Office, archivi, JAR e APK.

Per una protezione completa degli endpoint, SonicWall Capture Client abbina la tecnologia antivirus di prossima generazione alla sandbox multi-engine basata sul cloud di SonicWall integrandola facoltativamente con firewall SonicWall.

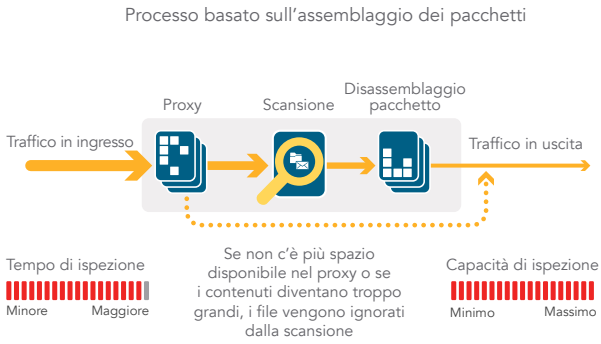


Engine Reassembly-Free Deep Packet Inspection

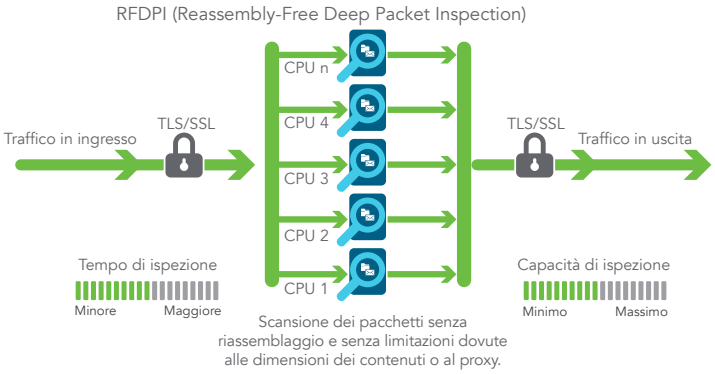
La tecnologia Reassembly-Free Deep Packet Inspection (RFDPI) di SonicWall è un sistema di ispezione a singolo passaggio e bassa latenza che esegue analisi ad alta velocità del traffico bidirezionale in base al flusso, senza proxy o buffering, per scoprire efficacemente i tentativi di intrusione e download di malware esaminando il traffico applicativo indipendentemente dalla porta e dal protocollo. Questo engine proprietario ispeziona i payload del traffico in transito per rilevare eventuali minacce ai livelli 3-7 ed esamina i flussi di rete, con procedure complesse e ripetute di normalizzazione e decrittazione, per sventare le tecniche di evasione avanzata che tentano di confondere i motori di rilevamento e introdurre codice dannoso nella rete.

Una volta superata la necessaria elaborazione preliminare, che comprende anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di tre database di segnature: attacchi intrusivi, malware e applicazioni. Lo stato di connessione viene quindi fatto progredire in modo che rappresenti la posizione del flusso riferita a questi database, finché non rileva uno stato di attacco o un altro evento "corrispondente".

Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. L'engine tuttavia può anche essere configurato per eseguire solo l'ispezione oppure, in caso di rilevamento delle applicazioni, per fornire servizi di gestione della larghezza di banda al livello 7 per il rimanente flusso dell'applicazione non appena quest'ultima viene identificata.



Architettura competitiva basata su proxy



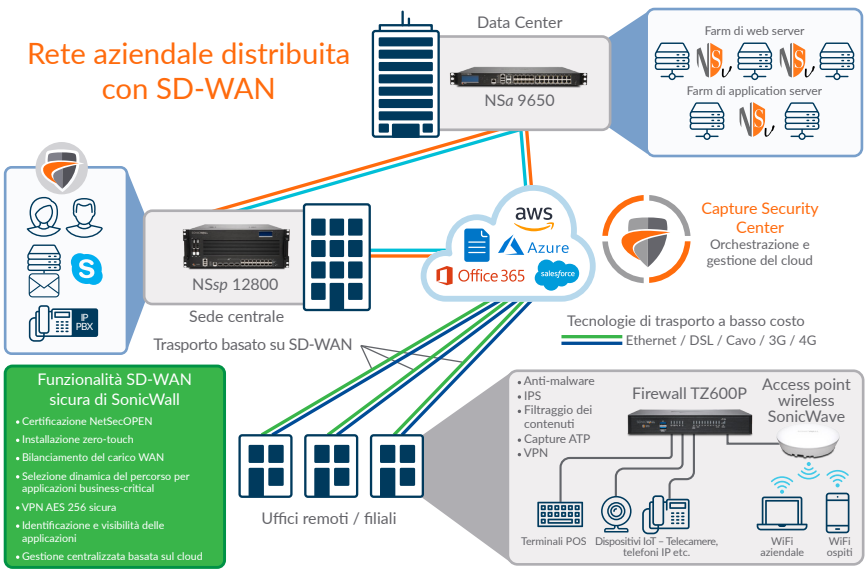
Architettura SonicWall basata sullo stream

Gestione e reportistica centralizzate

Per le organizzazioni ad elevata regolamentazione che desiderano creare una strategia coordinata di gestione della sicurezza, compliance e gestione del rischio, SonicWall offre agli amministratori una piattaforma unificata, sicura ed espandibile per gestire i firewall SonicWall, gli access point wireless e gli switch Dell delle serie N e X attraverso un processo di workstream correlato e verificabile. Le imprese possono consolidare facilmente la gestione delle apparecchiature di sicurezza, ridurre la complessità amministrativa e di risoluzione dei problemi e gestire tutti gli aspetti operativi dell'infrastruttura di sicurezza, compresa la gestione e l'applicazione centralizzata delle politiche, il monitoraggio degli eventi in tempo reale, le attività degli utenti, l'identificazione delle applicazioni, l'analisi investigativa e dei flussi, la conformità e la reportistica di verifica e altro ancora. Inoltre, le imprese soddisfano i requisiti di gestione delle modifiche del firewall attraverso l'automazione del flusso di lavoro, che fornisce l'agilità e la sicurezza necessarie per adottare le giuste politiche del firewall al momento giusto e in conformità con le normative di compliance. Le soluzioni di gestione e reportistica di SonicWall, disponibili in versione on-premise come SonicWall Global Management System e in cloud come Capture Security Center, offrono un metodo coerente per gestire la sicurezza della rete in base ai processi aziendali e ai livelli di servizio, semplificando notevolmente la gestione del ciclo di vita degli ambienti di sicurezza nel loro insieme rispetto alla gestione dispositivo per dispositivo.

Reti distribuite

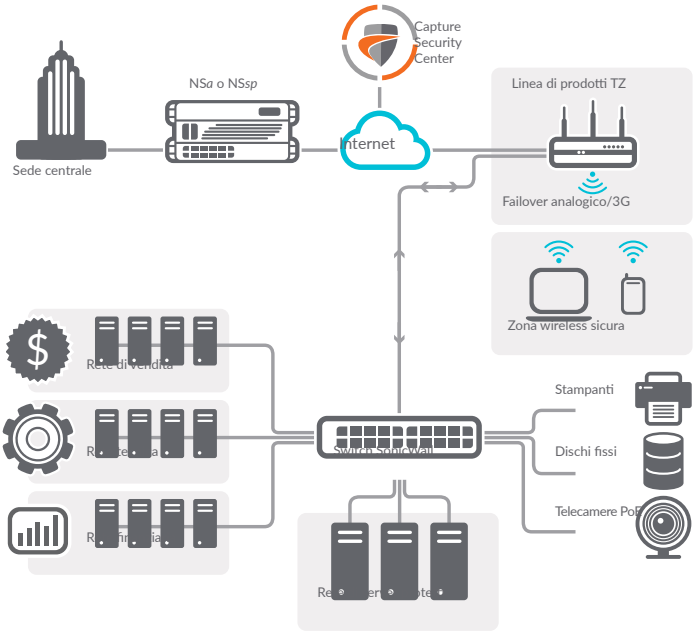
Grazie alla loro flessibilità, i firewall della serie TZ sono la scelta ideale sia per aziende distribuite, sia per installazioni in sedi singole. Nelle reti distribuite, come quelle delle imprese della grande distribuzione, ogni sede è dotata del proprio firewall TZ che in genere si collega a Internet tramite un provider locale utilizzando una connessione DSL, via cavo o 3G/4G. Oltre all'accesso Internet, ogni firewall utilizza una connessione Ethernet per trasportare i pacchetti tra le filiali e la sede centrale. I servizi web e le applicazioni SaaS come Office 365, Salesforce e altre sono forniti dal data center. Mediante la tecnologia mesh VPN, gli amministratori informatici possono creare una configurazione hub-and-spoke per il trasporto sicuro dei dati tra le varie sedi.



La tecnologia SD-WAN di SonicOS è il complemento ideale per i firewall TZ installati in sedi remote e filiali. Invece di affidarsi a tecnologie legacy più costose come MPLS e T1, le imprese che utilizzano la tecnologia SD-WAN possono scegliere servizi Internet pubblici a basso costo continuando ad ottenere un elevato livello di disponibilità delle applicazioni e prestazioni prevedibili.

Capture Security Center

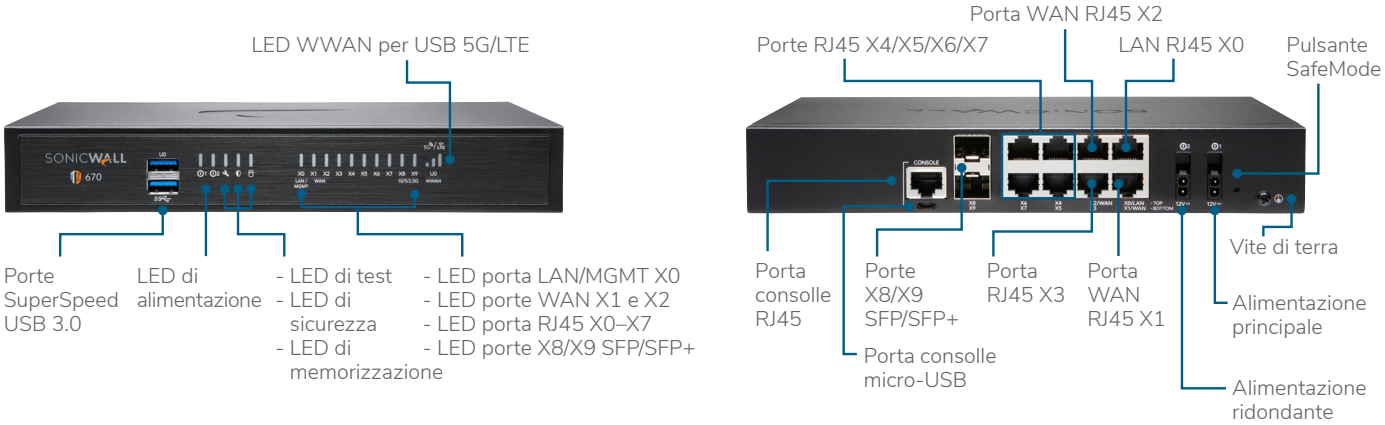
La rete distribuita viene coordinata tramite il Capture Security Center (CSC) basato sul cloud, che consente l'installazione, la gestione continua e l'analisi in tempo reale centralizzate dei firewall TZ. Una delle funzionalità fondamentali di CSC è la Zero-Touch Deployment. La configurazione e installazione dei firewall in più siti richiedono tempo e la presenza di personale in loco. L'installazione zero-touch elimina queste problematiche semplificando e velocizzando l'installazione e il provisioning dei firewall SonicWall da remoto attraverso il cloud. Inoltre CSC semplifica la gestione quotidiana grazie ad un'unica consolle di gestione basata sul cloud per tutti i dispositivi SonicWall collegati alla rete. Per garantire la consapevolezza situazionale dell'ambiente di sicurezza della rete, SonicWall Analytics offre una visione unificata di tutte le attività che si verificano all'interno della rete. Le aziende possono avere le idee più chiare sull'uso delle applicazioni e sulle prestazioni, riducendo la possibilità di Shadow IT.



SonicWall Network Security Manager (NSM), un gestore centralizzato di firewall multi-tenant che fa parte di CSC, consente di gestire centralmente tutte le operazioni dei firewall senza errori aderendo a flussi di lavoro verificabili. Il suo motore analitico nativo offre visibilità da un unico punto di controllo e consente di monitorare e individuare le minacce unificando e correlando i registri di tutti i firewall. NSM consente inoltre di rispettare le norme in quanto garantisce un audit trail completo di tutte le modifiche della configurazione e una reportistica granulare. NSM è adatto per le organizzazioni di qualsiasi dimensione che gestiscono reti con migliaia di dispositivi firewall distribuiti in diverse sedi.

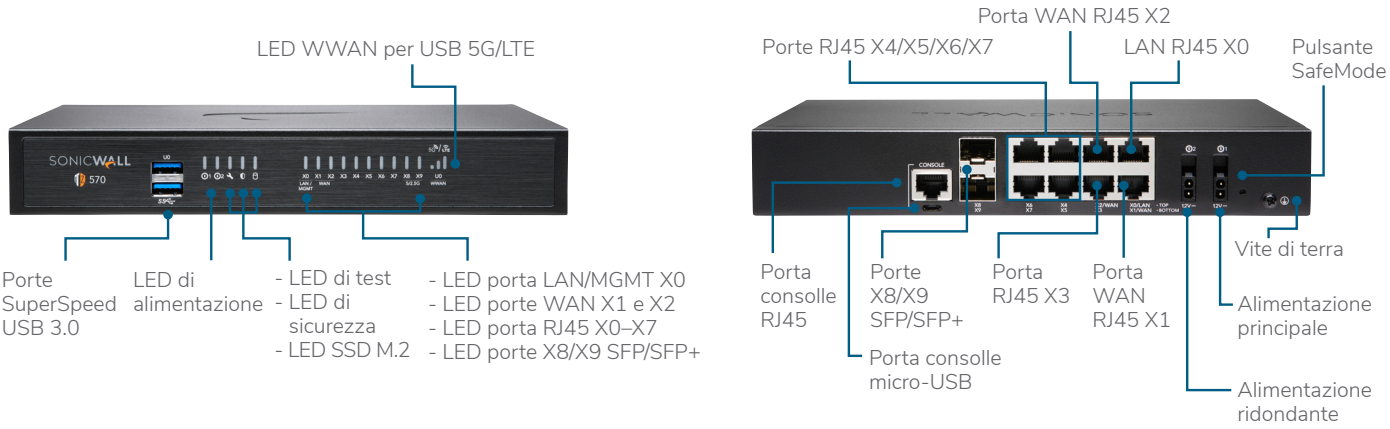
SonicWall serie TZ670

Progettato per le organizzazioni di media grandezza e le imprese distribuite con sedi SD-Branch, il firewall TZ670 si contraddistingue per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.



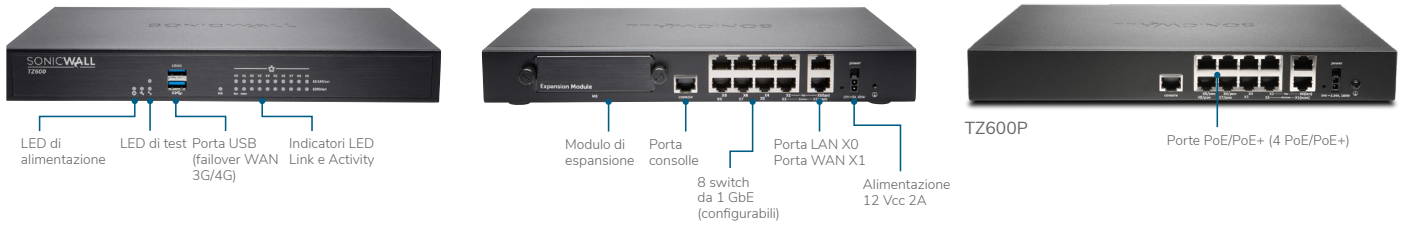
SonicWall serie TZ570

Progettati per le organizzazioni di piccola e media grandezza e le imprese distribuite con sedi SD-Branch, i firewall della serie TZ570 si contraddistinguono per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.



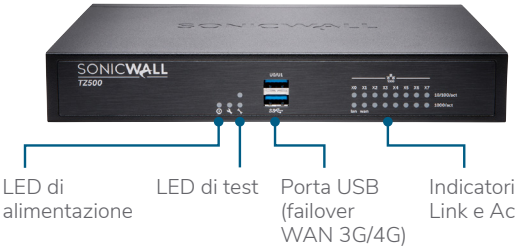
SonicWall serie TZ600

Per le imprese, i punti vendita e le filiali emergenti che necessitano di prestazioni elevate, sicurezza e opzioni come il supporto 802.3at PoE+ a un prezzo competitivo, SonicWall TZ600 offre la protezione delle reti con funzionalità di classe enterprise e prestazioni senza compromessi.



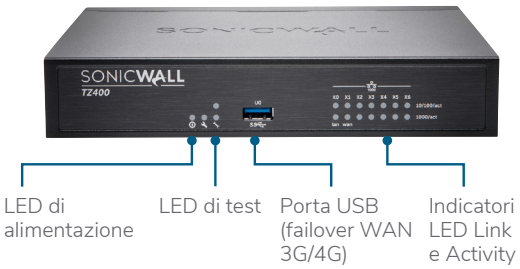
SonicWall serie TZ500

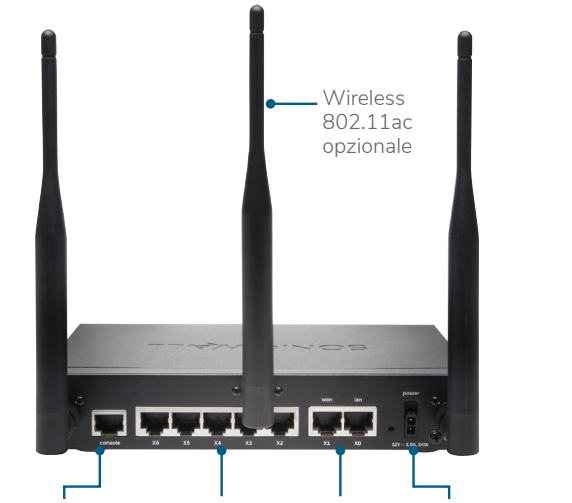
Per le PMI e le filiali in crescita, la serie TZ500 di SonicWall fornisce protezione altamente efficace e senza compromessi, con produttività di rete e connettività wireless integrata dual-band 802.11ac opzionale.



SonicWall serie TZ400

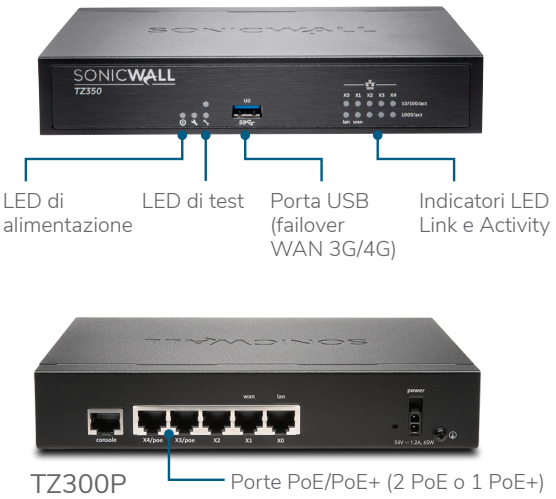
Per le piccole imprese, i punti vendita e le filiali, la serie TZ400 di SonicWall fornisce protezione di classe enterprise. L'installazione wireless flessibile è disponibile con connettività wireless 802.11ac dual-band integrata nel firewall.

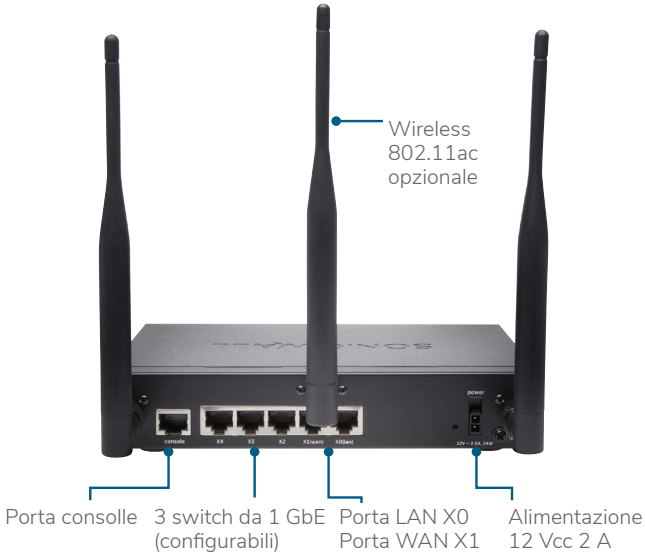




SonicWall serie TZ350/TZ300

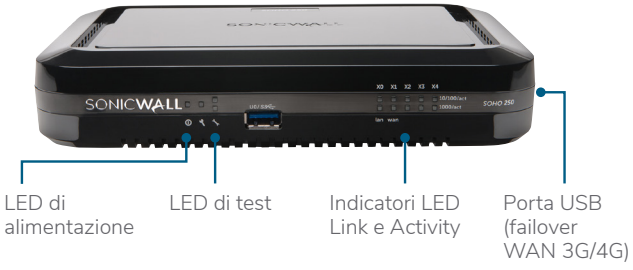
La serie TZ300 di SonicWall offre una soluzione all-in-one che protegge la rete dagli attacchi avanzati. Diversamente dai prodotti di largo consumo, questi firewall UTM abbinano la prevenzione ad alta velocità contro le intrusioni, la protezione anti-malware e il filtraggio dei contenuti e degli URL ad un supporto più ampio per l'accesso mobile per portatili, smartphone e tablet, oltre alla connessione wireless integrata opzionale 802.11ac. Inoltre, il modello TZ300 dispone come optional di 802.3at PoE+ per alimentare i dispositivi compatibili PoE.





SonicWall serie SOHO 250/SOHO

Per chi lavora da casa e per gli uffici di piccole dimensioni cablati o wireless i modelli delle serie SonicWall SOHO 250 e SOHO offrono lo stesso livello di protezione aziendale richiesto dalle grandi organizzazioni ad un prezzo molto più ragionevole. Grazie alla connessione wireless 802.11n opzionale, dipendenti, clienti ed ospiti potranno utilizzare una connettività wireless sicura.



Servizi attivati dai partner

Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni su www.sonicwall.com/PES.

Riepilogo delle funzioni di SonicOS 7.0

Firewall
- Ispezione Stateful Packet
- Reassembly-Free Deep Packet Inspection
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto di IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- Supporto API completo
- Integrazione switch SonicWall
- Modularità SD-WAN
- Procedura guidata utilizzabilità SD-WAN[1]
- Containerizzazione SonicCoreX e SonicOS[1]
- Modularità connessioni (SPI, DPI, SSL DPI)

Pannello di controllo migliorato[1]
- Visualizzazione migliorata dei dispositivi
- Sintesi del traffico e degli utenti principali
- Indicazioni sulle minacce
- Centro notifiche

Decrittazione e ispezione TLS/SSL/SSH
- TLS 1.3 con sicurezza migliorate[1]
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- Migliorie SSL DPI con CFS
- Controlli SSL DPI granulari in base a zone o regole

Capture Advanced Threat Protection[2]
- 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
- Intelligenza delle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[2]
- Scansione basata sulle segnature
- Aggiornamenti automatici delle segnature
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Applicazione GeoIP
- Filtraggio botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware[2]
- Scansione antimalware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware cloud

Identificazione delle applicazioni[2]
- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di segnature per applicazioni personalizzate
- Prevenzione della perdita di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di segnature delle applicazioni

Visualizzazione e analisi del traffico
- Attività degli utenti
- Utilizzo applicazioni/larghezza di banda/minacce
- Analisi basate sul cloud

Filtraggio dei contenuti HTTP/HTTPS Web[2]
- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Filtraggio basato sulle politiche (esclusione/inclusione)
- Inserimento intestazione HTTP
- Categorie di classificazione CFS per la gestione della larghezza di banda
- Modello di politica unificato con controllo delle applicazioni
- Content Filtering Client

VPN
- SD-WAN sicura
- Provisioning automatico delle VPN
- VPN IPSec per la connettività da sede a sede
- VPN SSL e accesso remoto da client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata sul routing (OSPF, RIP, BGP)

Connettività di rete
- PortShield
- Frame Jumbo
- Individuazione percorsi MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (NSa 2650 e successivi)
- QoS layer 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato sulle politiche (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Elevata disponibilità A/P con sincronizzazione statica
- Bilanciamento del carico in ingresso/in uscita
- Elevata disponibilità - Attivo/Standby con sincronizzazione statica
- Bridge L2, modalità wire/virtual wire, modalità tap, modalità NAT
- Routing asimmetrico
- Supporto CAC (Common Access Card)

VoIP
- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Supporto gatekeeper H.323 e 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, disposizione intuitiva delle funzioni[1]
  - Pannello di controllo
  - Informazioni sui dispositivi, applicazioni, minacce
  - Visualizzazione della topologia
  - Definizione e gestione semplificate delle politiche
- Statistiche d'uso delle politiche e degli oggetti[1]
  - Utilizzato vs. non utilizzato
  - Attivo vs. inattivo
- Ricerca globale dati statici
- Supporto di memorizzazione[1]
- Gestione della memoria interna ed esterna[1]
- 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[1]
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con SonicWall Global Management System (GMS)[2]
- Registrazione
- Esportazione per Netflow/IPFix
- Backup della configurazione basato sul 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 inclusi gli switch a cascata

Debugging e diagnostica
- Monitoraggio migliorato dei pacchetti
- Terminale SSH su interfaccia utente

Wireless
- Gestione AP SonicWave nel cloud
- WIDS/WIPS
- Prevenzione di rogue AP
- Fast roaming (802.11k/r/v)
- Connettività di rete 802.11s mesh
- Selezione automatica dei canali
- Analisi dello spettro di RF
- Visualizzazione in pianta
- Visualizzazione della topologia
- Band steering
- Beamforming
- AirTime Fairness
- Bluetooth Low Energy
- MiFi Extender
- Migliorie e potenziamento RF
- Quota ciclica ospite

Modelli wireless integrati
- Wireless 802.11ac Wave 2 (TZ570W)
- Dual-band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac
- Rilevamento e prevenzione delle intrusioni wireless
- Servizi wireless guest
- Messaggistica hotspot leggera
- Segmentazione degli access point virtuali
- Captive Portal
- ACL cloud

[1] *Nuova funzione, disponibile su SonicOS 7.0*
[2] *Richiede un abbonamento aggiuntivo*

SONICWALL®

Specifiche di sistema SonicWall serie TZ — SOHO, SOHO 250, TZ300 e TZ350

CARATTERISTICHE GENERALI DEI FIREWALL	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
Sistema operativo	SonicOS			
Interfacce	5 da 1 GbE, 1 USB, 1 consolle		5 da 1 GbE, 1 USB, 1 consolle	5 da 1 GbE, 1 USB, 1 consolle
Supporto PoE (Power over Ethernet)	—	—	TZ300P - 2 porte (2 PoE o 1 PoE+)	—
Espansione	USB			
Gestione	CLI, SSH, Web UI, Capture Security Center, GMS, API REST			
Utenti Single Sign-On (SSO)	250	350	500	500
Interfacce VLAN	25			
Access point supportati (max)	2	4	8	8
FIREWALL/PRESTAZIONI VPN	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Throughput di ispezione firewall[1]	300 Mbps	600 Mbps	750 Mbps	1,0 Gbps
Throughput di prevenzione delle minacce[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Throughput di ispezione applicazioni[2]	—	275 Mbps	375 Mbps	600 Mbps
Throughput IPS[2]	200 Mbps	250 Mbps	300 Mbps	400 Mbps
Throughput di ispezione anti-malware[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Throughput con decrittografia e ispezione (SSL DPI)[2]	30 Mbps	50 Mbps	60 Mbps	65 Mbps
Throughput con VPN IPSec[3]	150 Mbps	200 Mbps	300 Mbps	430 Mbps
Connessioni al secondo	1.800	3.000	5.000	6.000
Numero massimo di connessioni (SPI)	10.000	50.000	100.000	100.000
Numero massimo di connessioni (DPI)	10.000	50.000	90.000	90.000
Numero massimo di connessioni (SSL DPI)	250	25.000	25.000	25.000
VPN	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Tunnel VPN da sede a sede	10	10	10	15
Client VPN IPSec (max)	1 (5)	1 (5)	1 (10)	2 (10)
Licenze VPN SSL (max)	1 (10)	1 (25)	1 (50)	1 (75)
Virtual Assist in bundle (max)	—	1 (versione di prova di 30 giorni)	1 (versione di prova di 30 giorni)	1 (versione di prova di 30 giorni)
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basata su routing	RIP, OSPF, BGP[4]			
Caratteristiche VPN	Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing			
Piattaforme del client della VPN globale supportate	Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10			
NetExtender	Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/OpenSUSE			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato)			
SERVIZI DI SICUREZZA	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI			
Content Filtering Service (CFS)	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, liste di autorizzazione/blocco			
Servizio completo antispam	Supportato			
Visualizzazione delle applicazioni	No	Sì	Sì	Sì
Controllo delle applicazioni	Sì	Sì	Sì	Sì
Capture Advanced Threat Protection	No	Sì	Sì	Sì
CONNETTIVITÀ DI RETE	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
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[4]	BGP[4], OSPF, RIPv1/v2, static route, routing basato sulle politiche			
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1e (WMM)			

Specifiche di sistema SonicWall serie TZ - cont. — SOHO, SOHO 250, TZ300 e TZ350

CONNETTIVITÀ DI RETE - CONT.	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
Autenticazione	LDAP (domini multipli), XAUTH/ RADIUS, SSO, Novell, database utenti interno		LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)	
Database utenti locali	150			
VoIP	Full H.323v1-5, SIP			
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni[5]	FIPS 140-2 (con Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS)			
Common Access Card (CAC)	Supportato			
Elevata disponibilità	No		Active/Standby	
HARDWARE	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Fattore di forma	Desktop			
Alimentazione	24 W esterna		24 W esterna 65 W esterna (solo TZ300P)	24 W esterna
Potenza max assorbita (W)	6,4/11,3	6,9/11,3	6,9/12,0	6,9/12,0
Alimentazione in ingresso	100-240 Vca, 50-60 Hz, 1 A			
Dissipazione di calore totale	21,8/38,7 BTU	23,5/38,7 BTU	23,5/40,9 BTU	23,5/40,9 BTU
Dimensioni	3,6 x 14,1 x 19 cm		3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm
Peso	0,34 kg 0,48 kg		0,73 kg 0,84 kg	0,73 kg 0,84 kg
Peso RAEE	0,80 kg 0,94 kg		1,15 kg 1,26 kg	1,15 kg 1,26 kg
Peso con la confezione	1,20 kg 1,34 kg		1,37 kg 1,48 kg	1,37 kg 1,48 kg
MTBF (in anni)	58,9/56,1 (wireless)	56,1	56,1	56,1
Condizioni ambientali (in funzionamento/ stoccaggio)	0-40 °C / -40 - 70 °C			
Umidità	5-95%, non condensante			
NORMATIVE	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Conformità normative principali (modelli cablati)	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, KCC/MSIP, ANATEL		FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, KCC/MSIP, ANATEL	
Conformità normative principali (modelli wireless)	FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH		FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH	
WIRELESS INTEGRATO	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Standard	802.11 a/b/g/n		802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS)	
Bande di frequenza[6]	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		802.11a: 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: 2,412-2,472 GHz, 5,180-5,825 GHz	

Specifiche di sistema SonicWall serie TZ - cont. — SOHO, SOHO 250, TZ300 e TZ350

WIRELESS INTEGRATO	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
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 (solo 14-802.11b) 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		802.11a: 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 (solo 14-802.11b) 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 regolatore specificato dall'amministratore di sistema			
TPC (Transmit Power Control)	Supportato			
Velocità dati supportate	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 802.11b: 1, 2, 5,5, 11 Mbps per canale; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 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 Mbps per canale		802,11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 802,11b: 1, 2, 5,5, 11 Mbps per canale; 802,11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 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 Mbps per canale, 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, 866,7 Mbps per canale	
Spettro tecnologia di modulazione	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)		802.11a: 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)	

*Uso futuro

[1] *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.*

[2] *Rilevazione throughput per prevenzione minacce/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Il test viene eseguito con più flussi attraverso varie coppie di porte. Rilevazione throughput di prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati.*

[3] *Throughput VPN misurato mediante il traffico UDP con pacchetti di 1.280 byte in base al valore RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.*

[4] *BGP è disponibile solo su SonicWall TZ350, TZ400, TZ500 e TZ600.*

[5] *In attesa di approvazione FIPS e ICSA su SOHO 250 e TZ350*

[6] *Tutti i modelli TZ con wireless integrato possono supportare la banda a 2,4 GHz o 5 GHz. Per supporto dual-band utilizzare gli access point wireless SonicWall*

Specifiche di sistema SonicWall serie TZ — TZ400, TZ500 e TZ600

CARATTERISTICHE GENERALI DEI FIREWALL	SERIE TZ400	SERIE TZ500	SERIE TZ600
Sistema operativo		SonicOS	
Interfacce	7 da 1 GbE, 1 USB, 1 consolle	8 da 1 GbE, 2 USB, 1 consolle	10 da 1 GbE, 2 USB, 1 consolle, 1 slot di espansione
Supporto PoE (Power over Ethernet)	—	—	TZ600P - 4 porte (4 PoE o 4 PoE+)
Espansione	USB	2 USB	Slot di espansione (posteriore)*, 2 USB
Gestione		CLI, SSH, Web UI, Capture Security Center, GMS, API REST	
Utenti Single Sign-On (SSO)	500	500	500
Interfacce VLAN	50	50	50
Access point supportati (max)	16	16	24
FIREWALL/PRESTAZIONI VPN	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Throughput di ispezione firewall[1]	1,3 Gbps	1,4 Gbps	1,9 Gbps
Throughput di prevenzione delle minacce[2]	600 Mbps	700 Mbps	800 Mbps
Throughput di ispezione applicazioni[2]	1,2 Gbps	1,3 Gbps	1,8 Gbps
Throughput IPS[2]	900 Mbps	1,0 Gbps	1,2 Gbps
Throughput di ispezione anti-malware[2]	600 Mbps	700 Mbps	800 Mbps
Throughput con decrittografia e ispezione (SSL DPI)[2]	180 Mbps	225 Mbps	300 Mbps
Throughput con VPN IPSec[3]	900 Mbps	1,0 Gbps	1,1 Gbps
Connessioni al secondo	6.000	8.000	12.000
Numero massimo di connessioni (SPI)	150.000	150.000	150.000
Numero massimo di connessioni (DPI)	125.000	125.000	125.000
Numero massimo di connessioni (SSL DPI)	25.000	25.000	25.000
VPN	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Tunnel VPN da sede a sede	20	25	50
Client VPN IPSec (max)	2 (25)	2 (25)	2 (25)
Licenze VPN SSL (max)	2 (100)	2 (150)	2 (200)
Virtual Assist in bundle (max)	1 (versione di prova di 30 giorni)	1 (versione di prova di 30 giorni)	1 (versione di prova di 30 giorni)
Crittografia/autenticazione		DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B	
Scambio chiavi		Gruppi Diffie-Hellman 1, 2, 5, 14v	
VPN basata su routing		RIP, OSPF, BGP	
Caratteristiche VPN		Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing	
Piattaforme del client della VPN globale supportate		Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10	
NetExtender		Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/OpenSUSE	
Mobile Connect		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato)	
SERVIZI DI SICUREZZA	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Servizi Deep Packet Inspection		Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI	
Content Filtering Service (CFS)		Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, liste di autorizzazione/blocco	
Servizio completo antispam		Supportato	
Visualizzazione delle applicazioni	Sì	Sì	Sì
Controllo delle applicazioni	Sì	Sì	Sì
Capture Advanced Threat Protection	Sì	Sì	Sì
CONNETTIVITÀ DI RETE	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
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[4]		BGP[4], OSPF, RIPv1/v2, static route, routing basato sulle politiche	
Qualità del servizio (QoS)		Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p (WMM)	

Specifiche di sistema SonicWall serie TZ - cont. — TZ400, TZ500 e TZ600

CONNETTIVITÀ DI RETE	SERIE TZ400	SERIE TZ500	SERIE TZ600
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)		
Database utenti locali	150	250	
VoIP	Full H.323v1-5, SIP		
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certificazioni	FIPS 140-2 (con Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS)		
Common Access Card (CAC)	Supportato		
Elevata disponibilità	Active/Standby	Active/Standby con sincronizzazione dello stato	
HARDWARE	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Fattore di forma	Desktop		
Alimentazione	24 W esterna	36 W esterna	60 W esterna 180 W esterna (solo TZ600P)
Potenza max assorbita (W)	9,2/13,8	13,4/17,7	16,1
Alimentazione in ingresso	100-240 Vca, 50-60 Hz, 1 A		
Dissipazione di calore totale	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Dimensioni	3,5 x 13,4 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Peso	0,73 kg 0,84 kg	0,92 kg 1,05 kg	1,47 kg
Peso RAEE	1,15 kg 1,26 kg	1,34 kg 1,48 kg	1,89 kg
Peso con la confezione	1,37 kg 1,48 kg	1,93 kg 2,07 kg	2,48 kg
MTBF (in anni)	54,0	40,8	18,4
Condizioni ambientali (in funzionamento/stoccaggio)	0-40 °C / -40 - 70 °C		
Umidità	5-95%, non condensante		
NORMATIVE	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Conformità normative principali (modelli cablati)	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, KCC/MSIP, ANATEL	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, KCC/MSIP, ANATEL
Conformità normative principali (modelli wireless)	FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH	FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH	—

Specifiche di sistema SonicWall serie TZ - cont. — TZ400, TZ500 e TZ600

WIRELESS INTEGRATO	SERIE TZ400	SERIE TZ500	SERIE TZ600
Standard	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS)		—
Bande di frequenza[5]	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		—
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 (solo 14-802.11b) 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 regolatore specificato dall'amministratore di sistema		—
TPC (Transmit Power Control)	Supportato		—
Velocità dati supportate	802,11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 802,11b: 1, 2, 5,5, 11 Mbps per canale; 802,11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 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 Mbps per canale, 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, 866,7 Mbps per canale		—
Spettro tecnologia di modulazione	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)		—

Specifiche di sistema SonicWall serie TZ — TZ570 e TZ670

CARATTERISTICHE GENERALI DEI FIREWALL	SERIE TZ570	SERIE TZ670
Sistema operativo	SonicOS 7.0	
Interfacce	8 da 1 GbE, 2 da 5 GbE, 2 USB 3.0, 1 console	8 da 1 GbE, 2 da 10 GbE, 2 USB 3.0, 1 console
Supporto PoE (Power over Ethernet)	TZ570P (5 PoE o 3PoE+)	—
Espansione	Slot di espansione memoria (fino a 256 GB)	Slot di espansione memoria (fino a 256 GB) (compresi 32 GB)
Gestione	Network Security Manager, CLI, SSH, Web UI, GMS, API RET	
Utenti Single Sign-On (SSO)	2.500	2.500
Interfacce VLAN	256	256
Access point supportati (max)	32	32
FIREWALL/PRESTAZIONI VPN	**SERIE TZ570**	**SERIE TZ670**
Throughput di ispezione firewall[1]	4,00 Gbps	5,00 Gbps
Throughput di prevenzione delle minacce[2]	2,00 Gbps	2,50 Gbps
Throughput di ispezione applicazioni[2]	2,5 Gbps	3,0 Gbps
Throughput IPS[2]	2,5 Gbps	3,0 Gbps
Throughput di ispezione anti-malware[2]	2,00 Gbps	2,50 Gbps
Throughput con decrittografia e ispezione (SSL DPI)[2]	750 Mbps	800 Mbps
Throughput con VPN IPSec[3]	1,80 Gbps	2,10 Gbps
Connessioni al secondo	16.000	25.000
Numero massimo di connessioni (SPI)	1.250.000	1.500.000
Numero massimo di connessioni (DPI)	400.000	500.000
Numero massimo di connessioni (SSL DPI)	30.000	30.000
VPN	**SERIE TZ570**	**SERIE TZ670**
Tunnel VPN da sede a sede	200	250
Client VPN IPSec (max)	10 (500)	10 (500)
Licenze VPN SSL (max)	2 (200)	2 (250)
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B	
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v	
VPN basata su routing	RIP, OSPF, BGP	
Caratteristiche VPN	Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing	
Piattaforme del client della VPN globale supportate	Microsoft® Windows 10	
NetExtender	Microsoft® Windows 10, Linux	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10	
SERVIZI DI SICUREZZA	**SERIE TZ570**	**SERIE TZ670**
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI	
Content Filtering Service (CFS)	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, liste di autorizzazione/blocco	
Servizio completo antispam	Sì	
Visualizzazione delle applicazioni	Sì	
Controllo delle applicazioni	Sì	

Specifiche di sistema SonicWall serie TZ - cont. — TZ570 e TZ670

Capture Advanced Threat Protection	Sì	
Sicurezza DNS	Sì	
CONNETTIVITÀ DI RETE	**SERIE TZ570**	**SERIE TZ670**
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, static route, routing basato sulle politiche	
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p (WMM)	
Autenticazione	LDAP (domini multipli), XAUTH/ RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)	
Database utenti locali	250	
VoIP	Full H.323v1-5, SIP	
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE a802.3	
Certificazioni in corso	FIPS 140-2 (con Suite B) Level 2, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS)	
HARDWARE	**SERIE TZ570**	**SERIE TZ670**
Fattore di forma	Desktop[5]	
Alimentazione	60 W esterna 180 W esterna (solo TZ570P)	60 W esterna
Potenza max assorbita (W)	13,1	13,1
Tensione e frequenza d'ingresso	100-240 Vca, 50-60 Hz	100-240 Vca, 50-60 Hz
Dissipazione di calore totale	45,9/60,5 BTU	55,1 BTU
Dimensioni	3,5 x 15 x 22,5 (cm)	3,5 x 15 x 22,5 (cm)
Peso	0,97 kg	0,97 kg
Peso RAEE	1,42 kg	1,42 kg
Peso con la confezione	1,93 kg	1,93 kg
MTBF @25°C in anni	26,1	43,9
Condizioni ambientali (in funzionamento/ stoccaggio)	0-40 °C / -40 - 70 °C	
Umidità	5-95%, non condensante	
NORMATIVE	**SERIE TZ570**	**SERIE TZ670**
Conformità normative principali (modelli cablati - TZ670, TZ570)	FCC Classe B, FCC , ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL/cUL, TUV/GS, CB, avviso DGN UL (Messico), WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Classe B, FCC , ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL/ cUL, TUV/GS, CB, avviso DGN UL (Messico), WEEE, REACH, BSMI, KCC/MSIP, ANATEL
Conformità normative principali (modelli wireless - TZ570W)	FCC Classe B, FCC P15C, FCC P15E, ICES Classe B, ISED/IC, CE (RED, RoHS), C-Tick, VCCI Classe B, Wireless (Giappone), UL/ cUL, TUV/GS, CB, avviso DGN UL (Messico), WEEE, REACH, BSMI, NCC (TW) KCC/MSIP, SRRC, ANATEL	—
Conformità normative principali (modelli PoE - TZ570P)	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL/cUL, TUV/ GS, CB, avviso DGN UL (Messico), WEEE, REACH, BSMI, KCC/MSIP, ANATEL	—

Specifiche di sistema SonicWall serie TZ - cont. — TZ570 e TZ670

WIRELESS INTEGRATO	SERIE TZ570	SERIE TZ670
Standard	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS)	—
Bande di frequenza[5]	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	—
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 (solo 14-802.11b) 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 regolatore specificato dall'amministratore di sistema	—
TPC (Transmit Power Control)	Supportato	—
Velocità dati supportate	802,11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 802,11b: 1, 2, 5,5, 11 Mbps per canale; 802,11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per canale; 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 Mbps per canale, 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, 866,7 Mbps per canale	—
Spettro tecnologia di modulazione	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]*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.*
[2]*Rilevazione throughput per prevenzione minacce/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e strumenti di test Ixia. Il test viene eseguito con più flussi attraverso varie coppie di porte. Rilevazione throughput di prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati.*
[3]*Throughput VPN misurato mediante il traffico UDP con pacchetti di 1.280 byte in base al valore RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.*
[4]*Per installazione a rack, disponibile kit d'installazione a rack separato.*
[5]*Tutti i modelli TZ con wireless integrato possono supportare la banda a 2,4 GHz o 5 GHz. Per supporto dual-band utilizzare gli access point wireless SonicWall.*

Informazioni per ordinare SonicWall serie TZ

Prodotto	SKU
SOHO 250 con 1 anno di TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC con 1 anno di TotalSecure Advanced Edition	02-SSC-1824
TZ300 con 1 anno di TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC con 1 anno di TotalSecure Advanced Edition	01-SSC-1703
TZ300P con 1 anno di TotalSecure Advanced Edition	02-SSC-0602
TZ350 con 1 anno di TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC con 1 anno di TotalSecure Advanced Edition	02-SSC-1851
TZ400 con 1 anno di TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC con 1 anno di TotalSecure Advanced Edition	01-SSC-1706
TZ500 con 1 anno di TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC con 1 anno di TotalSecure Advanced Edition	01-SSC-1709
TZ570 con 1 anno di TotalSecure Essential Edition	02-SSC-5651
TZ570W con 1 anno di TotalSecure Essential Edition	02-SSC-5649
TZ570P con 1 anno di TotalSecure Essential Edition	02-SSC-5653
TZ600 con 1 anno di TotalSecure Advanced Edition	01-SSC-1711
TZ600P con 1 anno di TotalSecure Advanced Edition	02-SSC-0600
TZ670 con 1 anno di TotalSecure Essential Edition	02-SSC-5640
Opzioni ad elevata disponibilità (ogni unità deve essere dello stesso modello)	
TZ500 ad elevata disponibilità	01-SSC-0439
TZ570 ad elevata disponibilità	02-SSC-5694
TZ570P ad elevata disponibilità	02-SSC-5655
TZ600 ad elevata disponibilità	01-SSC-0220
TZ670 ad elevata disponibilità	02-SSC-5654

Servizi	SKU
Per SonicWall SERIE SOHO 250	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	02-SSC-1726
Capture Advanced Threat Protection per SOHO 250 (1 anno)	02-SSC-1732
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-1750
Servizio filtraggio contenuti (1 anno)	02-SSC-1744
Servizio completo antispam (1 anno)	02-SSC-1823
Assistenza 24x7 (1 anno)	02-SSC-1720
Per SonicWall serie TZ300	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	01-SSC-1430
Capture Advanced Threat Protection per TZ300 (1 anno)	01-SSC-1435
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	01-SSC-0602
Servizio filtraggio contenuti (1 anno)	01-SSC-0608
Servizio completo antispam (1 anno)	01-SSC-0632
Assistenza 24x7 (1 anno)	01-SSC-0620
Per SonicWall serie TZ350	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	02-SSC-1773
Capture Advanced Threat Protection per TZ350 (1 anno)	02-SSC-1779
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-1797
Servizio filtraggio contenuti (1 anno)	02-SSC-1791
Servizio completo antispam (1 anno)	02-SSC-1809
Assistenza 24x7 (1 anno)	02-SSC-1767

Informazioni per ordinare SonicWall serie TZ

Per SonicWall serie TZ400	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	01-SSC-1440
Capture Advanced Threat Protection per TZ400 (1 anno)	01-SSC-1445
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	01-SSC-0534
Servizio filtraggio contenuti (1 anno)	01-SSC-0540
Servizio completo antispam (1 anno)	01-SSC-0561
Assistenza 24x7 (1 anno)	01-SSC-0552
Per SonicWall serie TZ500	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	01-SSC-1450
Capture Advanced Threat Protection per TZ500 (1 anno)	01-SSC-1455
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	01-SSC-0458
Servizio filtraggio contenuti (1 anno)	01-SSC-0464
Servizio completo antispam (1 anno)	01-SSC-0482
Assistenza 24x7 (1 anno)	01-SSC-0476
Per SonicWall serie TZ600	
Advanced Gateway Security Suite – Capture ATP, prevenzione minacce e assistenza 24x7 (1 anno)	01-SSC-1460
Capture Advanced Threat Protection per TZ600 (1 anno)	01-SSC-1465
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	01-SSC-0228
Servizio filtraggio contenuti (1 anno)	01-SSC-0234
Servizio completo antispam (1 anno)	01-SSC-0252
Assistenza 24x7 (1 anno)	01-SSC-0246
Per SonicWall serie TZ670	
Essential Protection Service Suite - Capture ATP, prevenzione minacce, filtraggio contenuti, antispam e assistenza 24x7 (1 anno)	02-SSC-5053
Capture Advanced Threat Protection per TZ670 (1 anno)	02-SSC-5035
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-5059
Servizio filtraggio contenuti (1 anno)	02-SSC-5047
Servizio completo antispam (1 anno)	02-SSC-5041
Assistenza 24x7 (1 anno)	02-SSC-5029
Per SonicWall serie TZ570 (TZ570)	
Essential Protection Service Suite - Capture ATP, prevenzione minacce, filtraggio contenuti, antispam e assistenza 24x7 (1 anno)	02-SSC-5137
Capture Advanced Threat Protection per TZ570 (1 anno)	02-SSC-5083
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-5155
Servizio filtraggio contenuti (1 anno)	02-SSC-5119
Servizio completo antispam (1 anno)	02-SSC-5101
Assistenza 24x7 (1 anno)	02-SSC-5065
Per SonicWall serie TZ570 (TZ570W)	
Essential Protection Service Suite - Capture ATP, prevenzione minacce, filtraggio contenuti, antispam e assistenza 24x7 (1 anno)	02-SSC-5149
Capture Advanced Threat Protection per TZ570W (1 anno)	02-SSC-5095
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-5167
Servizio filtraggio contenuti (1 anno)	02-SSC-5131
Servizio completo antispam (1 anno)	02-SSC-5113
Assistenza 24x7 (1 anno)	02-SSC-5077
Per SonicWall serie TZ570 (TZ570P)	
Essential Protection Service Suite - Capture ATP, prevenzione minacce, filtraggio contenuti, antispam e assistenza 24x7 (1 anno)	02-SSC-5143
Capture Advanced Threat Protection per TZ570P (1 anno)	02-SSC-5089
Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno)	02-SSC-5161
Servizio filtraggio contenuti (1 anno)	02-SSC-5125
Servizio completo antispam (1 anno)	02-SSC-5107
Assistenza 24x7 (1 anno)	02-SSC-5071

Accessori	SKU
Serie TZ670/570	
Alimentatore FRU SonicWall serie TZ670/570	02-SSC-3078
Kit d'installazione a rack SonicWall serie TZ670/570	02-SSC-3112
Modulo di memoria SonicWall da 32 GB per serie TZ670/570	02-SSC-3114
Modulo di memoria SonicWall da 64 GB per serie TZ670/570	02-SSC-3115
Modulo di memoria SonicWall da 128 GB per serie TZ670/570	02-SSC-3116
Modulo di memoria SonicWall da 256 GB per serie TZ670/570	02-SSC-3117
Cavo consolle Micro USB SonicWall per serie TZ670/570	02-SSC-5173
TZ600/500/400/350/300, serie SOHO 250	
Kit d'installazione a rack SonicWall TZ600	01-SSC-0225
Alimentatore FRU SonicWall serie TZ600	01-SSC-0280
Kit d'installazione a rack SonicWall serie TZ500	01-SSC-0438
Alimentatore FRU SonicWall serie TZ500	01-SSC-0437
Kit d'installazione a rack SonicWall serie TZ400	01-SSC-0525
Kit d'installazione a rack SonicWall serie TZ350 e TZ300	01-SSC-0742
Alimentatore FRU SonicWall TZ400, TZ350, TZ300, SOHO 250, Serie SOHO	01-SSC-0709
Alimentatore FRU PoE SonicWall serie TZ300	02-SSC-0613
Moduli SonicWall SFP/SFP+	
Modulo fibra Short Reach multimodale 10 GB-SR SFP+ senza cavo	01-SSC-9785
Modulo fibra Long Reach unimodale 10 GB-LR SFP+ senza cavo	01-SSC-9786
Rame 10 GB SFP+ con cavo Twinax 1M	01-SSC-9787
Rame 10 GB SFP+ con cavo Twinax 3M	01-SSC-9788
Modulo fibra Short Haul multimodale 10 GB-SX SFP senza cavo	01-SSC-9789
Modulo fibra Long Haul unimodale 10 GB-LX SFP senza cavo	01-SSC-9790
Modulo rame 1 GB-RJ45 SFP senza cavo	01-SSC-9791
Modulo RJ45 rame ricetrasmettitore SonicWall SFP+ 10 GBASE-T	02-SSC-1874

Codici RMN

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/TZ300P	APL28-0B4/APL28-0B5/APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3
TZ670	APL62-0F7
TZ570/ TZ570W/ TZ570P	APL62-0F7/APL62-0F8/APL63-0F9

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune della cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com.

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

Datasheet-TZSeries-US-KJ-2126