Gartner peerinsights customers' choice 2018

SONICWALL

# Serie SonicWall TZ

**Prevenzione delle minacce e piattaforma SD-WAN 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'implementazione 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 funzionalità. SonicOS include una serie di potenti caratteristiche che offrono alle aziende la flessibilità per ottimizzare questi firewall UTM (Unified Threat Management) secondo i propri requisiti di rete specifici. Ad esempio, la creazione di una rete wireless sicura ad alta velocità è semplificata dal controller wireless integrato e dal supporto dello standard IEEE 802.11ac, con la possibilità di aggiungere i nostri access point SonicWave 802.11ac Wave 2. Per ridurre i costi e la complessità di connessione di punti di accesso wireless ad alta velocità e altri dispositivi con funzionalità Power over Ethernet (PoE) come telecamere, telefoni e stampanti IP, i modelli TZ300P e TZ600P offrono l'alimentazione PoE/PoE+.

Le imprese al dettaglio e gli ambienti aziendali distribuiti possono usufruire dei numerosi strumenti di SonicOS per ottenere vantaggi ancora maggiori. Le filiali remote possono scambiare informazioni con la sede centrale in completa sicurezza utilizzando una rete privata virtuale (VPN). La creazione di LAN virtuali (VLAN) permette 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 offre un'alternativa sicura ai costosi circuiti MPLS, fornendo al contempo prestazioni costanti e disponibilità delle applicazioni. L'installazione dei firewall TZ nelle sedi remote è particolarmente semplice grazie alla funzionalità Zero-Touch Deployment, che consente il provisioning dei firewall da remoto attraverso il cloud.

## Prevenzione delle minacce e prestazioni di livello superiore

La nostra visione per la protezione delle reti nell'attuale panorama di minacce informatiche in continua evoluzione consiste nel rilevare e prevenire automaticamente le minacce in tempo reale. Mediante una combinazione di tecnologie integrate e basate su cloud forniamo ai nostri firewall una protezione la cui elevata efficacia è stata confermata da test indipendenti di terzi. Le minacce sconosciute vengono inviate alla sandbox multi-engine in cloud Capture Advanced Threat Protection (ATP) di SonicWall 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 l'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 le armi del malware sono esposte per meno di 100 nanosecondi. Inoltre, il nostro engine RFDPI (Reassembly- Free Deep Packet Inspection) a singola fase brevettato viene utilizzato in combinazione per esaminare ogni byte di ogni pacchetto, ispezionando il traffico in entrata e in uscita direttamente

## Vantaggi:

### Soluzione di sicurezza flessibile e integrata

- SD-WAN sicura
- Potente sistema operativo SonicOS
- Connettività wireless 802.11ac ad alta velocità
- Power over Ethernet (PoE/PoE+)
- Segmentazione della rete tramite VLAN

### 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
- Prevenzione delle minacce integrata e basata su cloud
- Decrittazione e ispezione TLS/SSL
- Efficacia della sicurezza comprovata nel settore
- Team Capture Labs dedicato alla ricerca delle minacce
- Sicurezza degli endpoint con Capture Client

### Semplicità di installazione, configurazione e gestione

- Zero-Touch Deployment
- Gestione centralizzata basata su cloud e on-premise
- Linea scalabile di firewall
- Basso costo totale di proprietà

sul firewall. Sfruttando Capture ATP con la 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 di 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 (DPI-SSL) sui firewall della serie TZ mediante l'installazione e la gestione di certificati TLS affidabili.

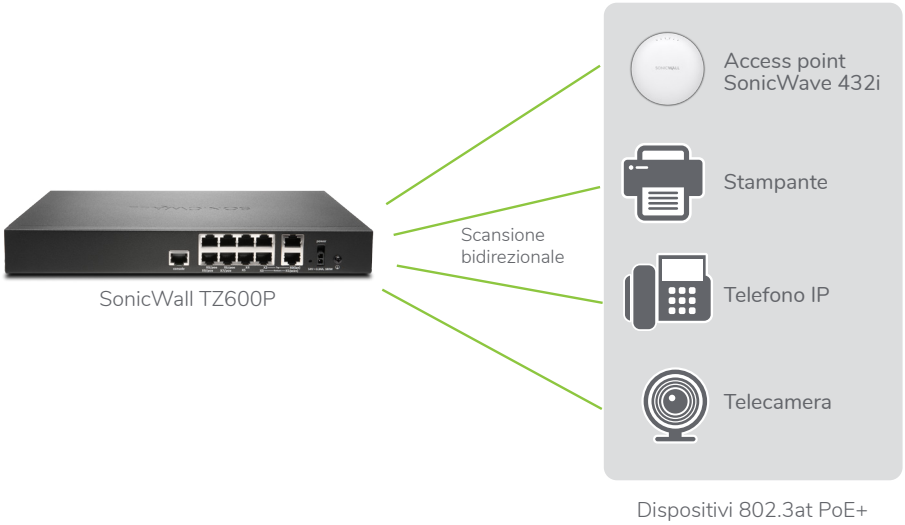
Con il continuo aumento dell'uso della crittografia per proteggere le sessioni web, è indispensabile che i firewall siano in grado di esaminare il traffico crittografato alla ricerca di minacce. I firewall della serie TZ offrono una protezione completa eseguendo la decrittazione ed ispezione complete delle connessioni TLS/SSL ed SSH crittografate, indipendentemente dalla porta o dal protocollo. 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 ed esclusione consentono di stabilire quale traffico deve essere sottoposto alla decrittazione e all'ispezione in base a requisiti di conformità specifici dell'azienda e/o legali.

## 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 su cloud, che offre la massima visibilità, agilità e capacità di amministrare centralmente l'intero ecosistema di sicurezza SonicWall da un'unica console di controllo.

Un componente fondamentale del Capture Security Center è Zero-Touch Deployment (installazione zero-touch). 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 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

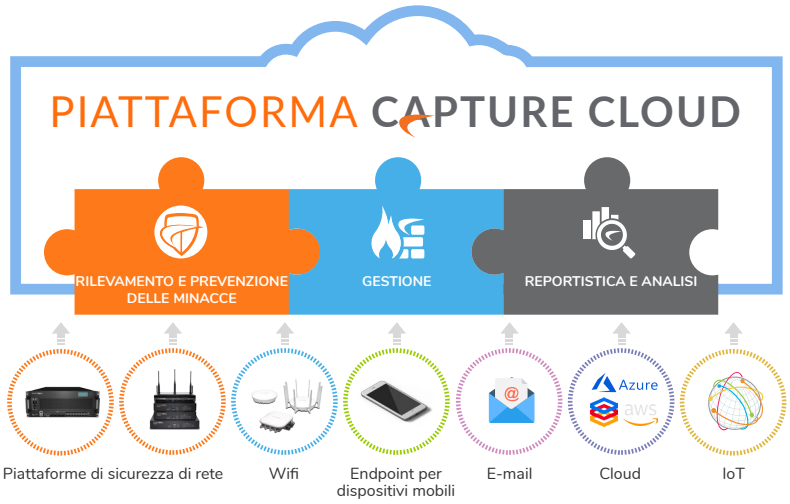
I dispositivi con funzionalità PoE possono essere alimentati senza il costo e la complessità di uno switch o un iniettore Power over Ethernet. I firewall TZ300P e TZ600P integrano la tecnologia IEEE 802.3at che consente di alimentare dispositivi PoE e PoE+ come punti di accesso wireless, telecamere, 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 offre la prevenzione delle minacce basata sul cloud e la gestione della rete oltre a funzionalità 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 firme 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 firme integrate con decine di milioni di firme.

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

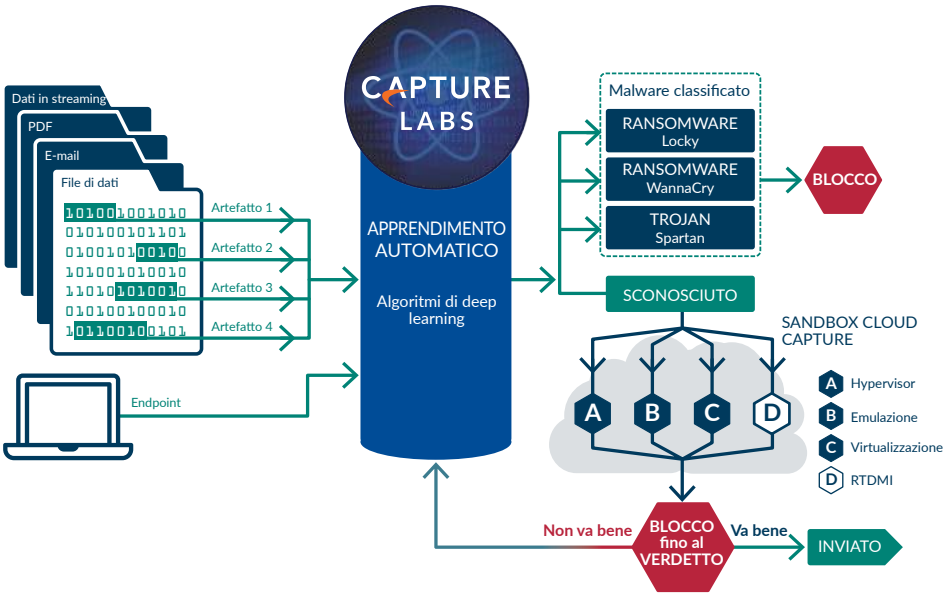



## Protezione contro le minacce avanzate

Al centro della prevenzione automatizzata delle violazioni in tempo reale di SonicWall si trova il servizio SonicWall Capture Advanced Threat Protection, una sandbox multi-engine basata su cloud che estende la protezione dalle minacce del firewall per rilevare e prevenire le minacce zero-day. I file sospetti vengono inviati al cloud dove vengono analizzati utilizzando algoritmi di deep learning con la possibilità di trattenerli al gateway fino a quando non viene emesso un verdetto. La piattaforma sandbox multi-engine, che include la tecnologia Real-Time Deep Memory Inspection, sandboxing virtualizzato, emulazione di sistema completa e tecnologia di analisi a livello hypervisor, esegue il codice sospetto e analizza il comportamento. Quando un file viene identificato come maligno, viene bloccato e viene creato immediatamente un hash all'interno di Capture ATP. Poco dopo, una firma viene inviata ai firewall per prevenire gli attacchi successivi.

Il servizio analizza 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 combina la tecnologia antivirus di nuova generazione con la sandbox multi-engine basata sul cloud di SonicWall.





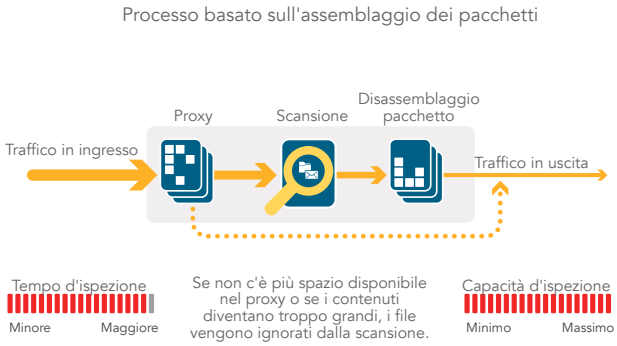

SONICWALL®

## Engine Reassembly-Free Deep Packet Inspection

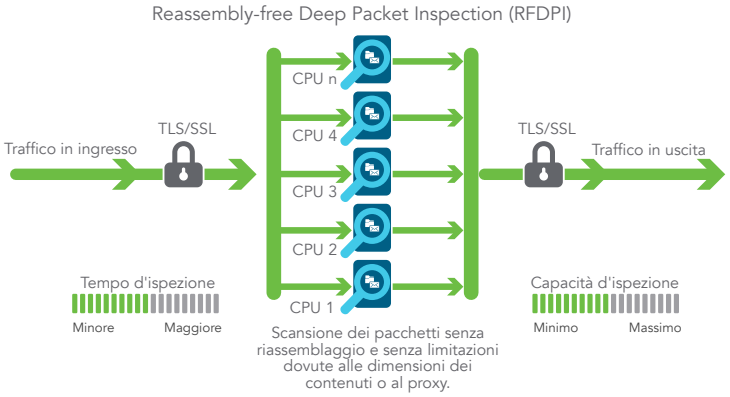
La tecnologia Reassembly-Free Deep Packet Inspection (RFDPI) di SonicWall è un sistema di ispezione a singolo passaggio e bassa latenza che esegue analisi ad alta velocità del traffico bidirezionale in base al flusso, senza proxy o buffering, per scoprire efficacemente i tentativi di intrusione e download 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 gli engine di rilevamento e introdurre codice dannoso nella rete.

Una volta superata la necessaria elaborazione preliminare, che include anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di tre database di firme: 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".

A questo punto viene intrapresa un'azione predefinita. Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. L'engine 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 viene identificata l'applicazione.




**Architettura competitiva basata su proxy**



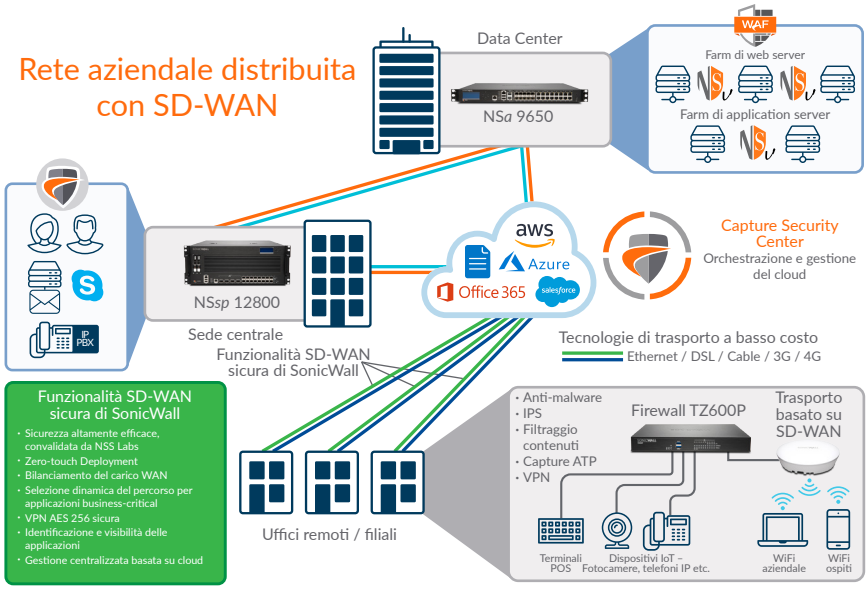

**Architettura SonicWall basata sullo stream**

## Gestione e reporting centralizzati

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 forense 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 implementare le giuste politiche del firewall al momento giusto e in conformità con le normative di compliance. Le soluzioni di gestione e reporting 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

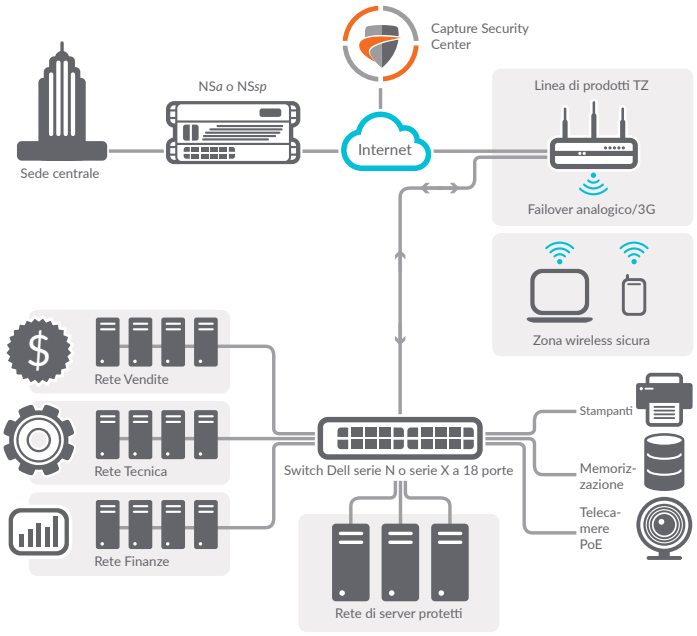
Grazie alla loro flessibilità, i firewall della serie TZ sono la scelta ideale sia per aziende distribuite, sia per implementazioni in sedi singole. Nelle reti distribuite, come quelle delle imprese della grande distribuzione, ogni sede è dotata del proprio firewall TZ che in genere si collega a Internet 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 su cloud di SonicWall, che centralizza l'implementazione, la gestione continua e l'analisi in tempo reale dei firewall TZ. Una delle funzionalità fondamentali di CSC è la Zero-Touch Deployment. La configurazione e l'implementazione 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'implementazione e il provisioning dei firewall SonicWall da remoto attraverso il cloud. Inoltre, CSC semplifica la gestione quotidiana fornendo un'unica console di gestione basata su 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 ottengono così una migliore comprensione dell'uso delle applicazioni e delle performance, riducendo la possibilità di shadow IT.




## Sedi singole

Per le implementazioni in sedi singole è particolarmente vantaggioso utilizzare una soluzione di sicurezza di rete integrata. I firewall della serie TZ abbinano un'elevata efficacia della sicurezza ad opzioni quali wireless 802.11ac integrato e, nel caso dei modelli TZ300P e TZ600P, supporto PoE/PoE+. Nei firewall della serie TZ è integrato lo stesso engine di sicurezza delle nostre serie NSa di fascia media ed NSsp di fascia alta, oltre all'ampio set di funzionalità di SonicOS. I processi di configurazione e gestione sono semplificati dall'intuitiva interfaccia utente di SonicOS. Le aziende possono inoltre risparmiare spazio su rack grazie al fattore di forma compatto.

## 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.

| Specifiche | Serie TZ600 |
|---|---|
| Throughput firewall | 1,9 Gb/s |
| Throughput prevenzione delle minacce | 800 Mb/s |
| Throughput antimalware | 800 Mb/s |
| Throughput IPS | 1,2 Gb/s |
| Numero massimo di connessioni | 150.000 |
| Nuove connessioni/sec | 12.000 |

TZ600P

Porte PoE/PoE+ (4 PoE/PoE+)


LED di alimentazione

LED di test

Porta USB (failover WAN 3G/4G)

Indicatori LED Link e Activity


Modulo di espansione

Porta console

8 switch da 1 GbE (configurabili)

Porta LAN X0
Porta WAN X1

Alimentazione 12 Vcc 2 A

## 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.

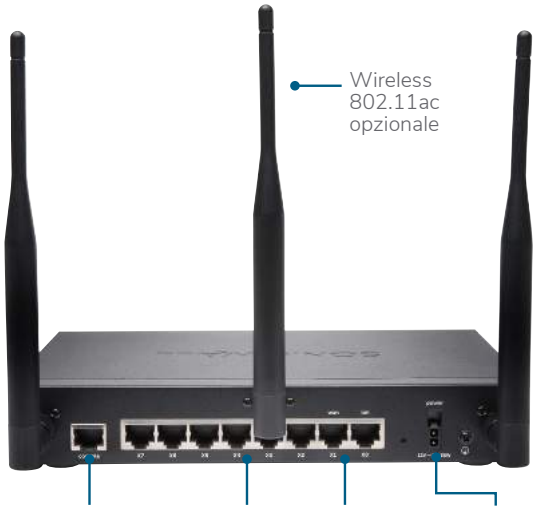
| Specifiche | TZ500 Series |
|---|---|
| Throughput firewall | 1,4 Gb/s |
| Throughput prevenzione delle minacce | 700 Mb/s |
| Throughput antimalware | 700 Mb/s |
| Throughput IPS | 1,0 Gb/s |
| Numero massimo di connessioni | 150.000 |
| Nuove connessioni/sec | 8.000 |


LED di alimentazione

LED di test

Porta USB (failover WAN 3G/4G)

Indicatori LED Link e Activity



Wireless 802.11ac opzionale

Porta console

6 switch da 1 GbE (configurabili)

Porta LAN X0
Porta WAN X1

Alimentazione 12 Vcc 2 A

## SonicWall serie TZ400

Per le piccole imprese, i negozi 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.

| Specifiche | TZ400 Series |
|---|---|
| Throughput firewall | 1,3 Gb/s |
| Throughput prevenzione delle minacce | 600 Mb/s |
| Throughput antimalware | 600 Mb/s |
| Throughput IPS | 900 Mb/s |
| Numero massimo di connessioni | 150.000 |
| Nuove connessioni/sec | 6.000 |


LED di alimentazione | LED di test | Porta USB (failover WAN 3G/4G) | Indicatori LED Link e Activity


Porta console | 5 switch da 1 GbE (configurabili) | Porta LAN X0 Porta WAN X1 | Alimentazione 12 Vcc 2 A

## SonicWall serie TZ350/TZ300

Le serie TZ300 e TZ350 di SonicWall offrono una soluzione all-in-one che protegge la rete dagli attacchi. 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.

| Specifiche | TZ350 Series | Serie TZ300 |
|---|---|---|
| Throughput firewall | 1,0 Gb/s | 750 Mb/s |
| Throughput prevenzione delle minacce | 335 Mb/s | 235 Mb/s |
| Throughput antimalware | 300 Mb/s | 200 Mb/s |
| Throughput IPS | 400 Mb/s | 300 Mb/s |
| Numero massimo di connessioni | 100.000 | 100.000 |
| Nuove connessioni/sec | 6.000 | 5.000 |


LED di alimentazione | LED di test | Porta USB (failover WAN 3G/4G) | Indicatori LED Link e Activity

TZ300P — Porte PoE/PoE+ (2 PoE o 1 PoE+)


Porta console | 3 switch da 1 GbE (configurabili) | Porta LAN X0 Porta WAN X1 | Alimentazione 12 Vcc 2 A

## 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.

| Specifiche | Serie SOHO 250 | Serie SOHO |
|---|---|---|
| Throughput firewall | 600 Mb/s | 300 Mb/s |
| Throughput prevenzione delle minacce | 200 Mb/s | 150 Mb/s |
| Throughput antimalware | 100 Mb/s | 50 Mb/s |
| Throughput IPS | 250 Mb/s | 100 Mb/s |
| Numero massimo di connessioni | 50.000 | 10.000 |
| Nuove connessioni/sec | 3.000 | 1.800 |


LED di alimentazione | LED di test | Indicatori LED Link e Activity | Porta USB (failover WAN 3G/4G)

Wireless 802.11n opzionale

Porta console | 3 switch da 1 GbE (configurabili) | Porta LAN X0 Porta WAN X1 | Alimentazione 12 Vcc 2 A

**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 sul sito www.sonicwall.com/PES.

## Caratteristiche

| ENGINE RFDPI | |
|---|---|
| **Funzionalità** | **Descrizione** |
| Reassembly-Free Deep Packet Inspection (RFDPI) | Si tratta di un engine di ispezione proprietario, brevettato e ad alte prestazioni, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni in qualsiasi porta. |
| Ispezione bidirezionale | Con la scansione contemporanea del traffico in ingresso e in uscita per il rilevamento delle minacce, questa opzione impedisce l'utilizzo della rete come vettore di malware e come piattaforma per sferrare attacchi qualora venga introdotto un computer infetto. |
| Ispezione basata sui flussi | La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni, sia a flussi TCP primari. |
| Architettura altamente parallela e scalabile | L'esclusivo engine RFDPI basato su architettura multi-core offre l'ispezione deep packet ad alta velocità e consente di creare nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse. |
| Ispezione single-pass | Un'architettura DPI a passaggio singolo consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura. |
| **FIREWALL E CONNETTIVITÀ DI RETE** | |
| **Funzionalità** | **Descrizione** |
| SD-WAN sicura | SD-WAN sicura è una valida alternativa a tecnologie più costose come MPLS, che permette alle imprese distribuite di creare, utilizzare e gestire reti sicure ad alte prestazioni negli uffici remoti per condividere dati, applicazioni e servizi utilizzando servizi Internet pubblici prontamente disponibili e a basso costo. |
| API REST | Consentono al firewall di ricevere e sfruttare tutti i feed di intelligence proprietari dei produttori di dispositivi originali e di terzi per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate. |
| Ispezione Stateful Packet | Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle politiche di accesso del firewall. |
| Alta disponibilità/clustering | I modelli SonicWall TZ500 e TZ600 supportano un'elevata disponibilità Active/Standby con sincronizzazione dello stato. I modelli SonicWall TZ300 e TZ400 supportano un'elevata disponibilità Active/Standby senza sincronizzazione dello stato. L'opzione di disponibilità elevata non è presente sui modelli SOHO di SonicWall. |
| Protezione da attacchi DDoS/DoS | La protezione da flood SYN offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DoS/DDoS attraverso la protezione da flood UDP/ICMP e la limitazione della velocità di connessione. |
| Supporto di IPv6 | Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con SonicOS, l'hardware supporta il filtraggio e le implementazioni in modalità Wire. |
| Opzioni di installazione flessibili | La serie TZ può essere installata nelle tradizionali modalità NAT, bridge Layer 2, Wire e Network Tap. |
| Bilanciamento del carico WAN | Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over. |
| Qualità del servizio (QoS) avanzata | Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete. |
| Gatekeeper H.323 e supporto per proxy SIP | Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP. |
| Gestione di switch N-Series e X-Series di Dell singoli e in cascata | Gestione delle impostazioni di sicurezza di porte aggiuntive, tra cui Portshield, HA, PoE e PoE+, attraverso un unico pannello di controllo utilizzando il dashboard di gestione del firewall per gli switch di rete serie N e serie X di Dell (non disponibile con il modello SOHO). |
| Autenticazione biometrica | Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete. |
| Autenticazione aperta e social login | Consente agli utenti ospiti di utilizzare le loro credenziali da servizi di social network come Facebook, Twitter o Google+ per accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through. |
| Sicurezza delle reti wireless | Disponibile come opzione integrata sui modelli SonicWall TZ300 fino a TZ500, la tecnologia wireless IEEE 802.11ac può fornire un throughput fino a 1,3 Gb/s con maggiore copertura e affidabilità. Connettività 802.11 a/b/g/n opzionale disponibile sui modelli SonicWall SOHO. |
| **GESTIONE E REPORTING** | |
| **Funzionalità** | **Descrizione** |
| Gestione basata sul cloud e on-premise | La configurazione e la gestione delle apparecchiature SonicWall sono disponibili via cloud attraverso il SonicWall Capture Security Center e in sede tramite il SonicWall Global Management System (GMS). |
| Gestione avanzata con un unico dispositivo | Configurazione comoda e veloce tramite l'interfaccia web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3. |
| Report sul flusso delle applicazioni con IPFIX/ NetFlow | Le analisi del traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti che supportano IPFIX e NetFlow con estensioni. |

| RETE PRIVATA VIRTUALE (VPN) | |
|---|---|
| Funzionalità | Descrizione |
| Provisioning automatico delle VPN | Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sito a sito tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività. |
| VPN IPSec per la connettività Site-to-Site | La rete VPN IPSec ad alte prestazioni consente di utilizzare la serie TZ come concentratore di VPN per migliaia di utenti privati, filiali o altri siti di grandi dimensioni. |
| Accesso remoto tramite VPN SSL o client IPSec | Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi e-mail, file, computer, siti intranet e applicazioni da un'ampia serie di piattaforme. |
| Gateway per la rete VPN ridondante | Se si utilizzano più WAN, è possibile configurare una VPN principale e una secondaria per assicurare failover e failback automatizzati e trasparenti per tutte le sessioni VPN. |
| VPN basato su routing | La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo al tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso route alternative. |
| SENSIBILITÀ AL CONTESTO/AL CONTENUTO | |
| Funzionalità | Descrizione |
| Tracciamento delle attività degli utenti | Le tecnologie AD/LDAP/Citrix1/Terminal Services 1 SSO integrate si combinano con le informazioni esaustive ricavate dall'ispezione DPI per consentire il tracciamento delle attività e l'identificazione degli utenti. |
| GeoIP per l'identificazione del traffico da determinati paesi | Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da determinati paesi. Lo scopo è proteggere dagli attacchi provenienti da origini note o sospette di attività pericolose o analizzare il traffico sospetto che ha origine nella rete. Consente di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP. Elimina il filtraggio non voluto degli indirizzi IP dovuto ad errata classificazione. |
| Filtro DPI con espressioni regolari | Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati. Consente di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP. |
| CAPTURE ADVANCED THREAT PROTECTION | |
| Funzionalità | Descrizione |
| Sandboxing multi-engine | La piattaforma sandbox multi-engine, che include emulazione completa del sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità completa sulle attività malevole. |
| Real-Time Deep Memory Inspection (RTDMI) | Questa tecnologia basata su cloud in attesa di brevetto rileva e blocca i malware che non evidenziano comportamenti dannosi e nascondono il loro armamentario tramite crittografia. Forzando il malware a scoprire il suo armamentario nella memoria, l'engine RTDMI rileva e blocca in anticipo le minacce generalizzate, quelle zero-day e i malware sconosciuti. |
| Blocco fino al verdetto | Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway finché non viene determinata la loro natura. |
| Analisi di un'ampia gamma di tipi e dimensioni di file | Supporta l'analisi di un'ampia gamma di tipi di file, sia individualmente, sia come gruppo, inclusi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, tra cui Windows, Android, Mac OS X e ambienti multi-browser. |
| Rapida distribuzione delle firme | Quando un file è identificato come dannoso, viene immediatamente distribuita una firma ai firewall con abbonamento a SonicWall Capture ATP, ai database delle firme per Gateway Anti-Virus e IPS, nonché ai database di URL, IP e reputazione dei domini nel giro di 48 ore. |
| Capture Client | Capture Client è una piattaforma client unificata che presenta numerose funzioni di protezione dell'end point, tra cui quella avanzata contro i malware e supporto per la visibilità del traffico crittografato. La piattaforma sfrutta tecnologie di protezione su più livelli, reporting completo e applicazione della protezione degli end point. |
| PREVENZIONE DELLE MINACCE CRITTOGRAFATE | |
| Funzionalità | Descrizione |
| Decrittazione e ispezione TLS/SSL | Esegue la decrittazione e l'ispezione del traffico crittografato TLS/SSL in tempo reale, senza proxy, di malware, intrusioni e fughe di dati, e applica politiche di controllo di applicazioni, URL e contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato. Opzione inclusa negli abbonamenti di sicurezza per tutti i modelli della serie TZ, tranne SOHO. Per quest'ultimo è venduta come licenza a parte. |
| Ispezione SSH | La Deep Packet Inspection di SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano SSH. |
| PREVENZIONE DELLE INTRUSIONI | |
| Funzionalità | Descrizione |
| Protezione basata su contromisure | Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le firme e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di vulnerabilità e attacchi. |
| Aggiornamenti automatici delle firme | Il team del SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti sono subito attivi senza la necessità di riavvii o interruzioni del servizio. |

| PREVENZIONE DELLE INTRUSIONI - CONTINUAZIONE | |
|---|---|
| Funzionalità | Descrizione |
| Protezione IPS interna alle zone | La segmentazione della rete in varie zone di sicurezza, protette dalle intrusioni, consente di potenziare la sicurezza interna poiché impedisce alle minacce di propagarsi oltre i confini di una zona. |
| Rilevamento e blocco di comando e controllo Botnet (CnC) | Questa opzione consente di individuare e bloccare il traffico di comando e controllo proveniente dai bot nella rete locale e diretto ai domini e agli indirizzi IP che sono stati identificati come fonte di propagazione di malware o punti CnC noti. |
| Anomalia/abuso di protocolli | Individua e blocca gli attacchi che sfruttano i protocolli noti per tentare di eludere il controllo IPS. |
| Protezione zero-day | Per proteggere la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit. |
| Tecnologia antievasione | La normalizzazione estesa dei flussi, la decodifica e altre tecniche assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate. |
| PREVENZIONE DELLE MINACCE | |
| Funzionalità | Descrizione |
| Antimalware a livello gateway | L'engine RFDPI sottopone a scansione tutto il traffico in ingresso, in uscita e interno alle zone in cerca di virus, trojan, keylogger e altri malware, interessando file di dimensioni e lunghezza illimitati in tutte le porte e in tutti i flussi TCP. |
| Protezione Capture Cloud contro il malware | Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte dell'engine RFDPI. |
| Aggiornamenti di sicurezza costanti | I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall sul campo con servizi di sicurezza attivi e sono subito attivi senza riavvii o interruzioni. |
| Ispezione bidirezionale dei TCP primari | L'engine RFDPI è in grado di scansionare flussi TCP primari in entrambe le direzioni su qualsiasi porta, bloccando gli attacchi che tentano di passare attraverso sistemi di sicurezza obsoleti, concepiti per proteggere solo poche porte note. |
| Ampio supporto di protocolli | Oltre a identificare i protocolli più comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri, che non inviano dati nel TCP primario, questa opzione consente di decodificare i payload in cerca di malware, anche se non sono eseguiti in porte standard note. |
| INTELLIGENCE E CONTROLLO DELLE APPLICAZIONI | |
| Funzionalità | Descrizione |
| Controllo delle applicazioni | Per potenziare la sicurezza e la produttività della rete vengono controllate le applicazioni, o singole funzionalità delle applicazioni, identificate dall'engine RFDPI utilizzando un database in continua espansione, contenente migliaia di firme di applicazioni. |
| Identificazione di applicazioni personalizzate | Controlla le applicazioni personalizzate generando firme basate su parametri specifici o su modelli di comunicazione in rete univoci per ogni applicazione, in modo da garantire un maggiore controllo sulla rete. |
| Gestione della larghezza di banda delle applicazioni | Il traffico delle applicazioni superflue viene bloccato, mentre la larghezza di banda disponibile viene regolamentata e allocata in modo granulare per le applicazioni o le categorie di applicazioni più importanti. |
| Controllo granulare | Consente di controllare le applicazioni o i componenti specifici di un'applicazione in base a pianificazioni, gruppi di utenti, elenchi di esclusione e una serie di attività con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/Terminal Services/Citrix. |
| FILTRAGGIO DEI CONTENUTI | |
| Funzionalità | Descrizione |
| Filtraggio dei contenuti interno/esterno | Mette in atto le politiche di utilizzo accettabili e blocca l'accesso a siti web HTTP/HTTPS contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service e Content Filtering Client. |
| Enforced Content Filtering Client | Estende l'applicazione delle politiche per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall. |
| Controlli granulari | L'uso di categorie predefinite o di una combinazione qualsiasi di categorie consente di bloccare determinati contenuti. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo, e applicato a gruppi o singoli utenti. |
| Cache Web | Le classificazioni degli URL sono memorizzate nella cache locale del firewall SonicWall, in modo che il tempo di risposta per l'accesso successivo ai siti web visitati con maggior frequenza sia inferiore a un secondo. |
| ANTIVIRUS E ANTISPYWARE APPLICATI | |
| Funzionalità | Descrizione |
| Protezione su più livelli | Utilizza le funzionalità del firewall come primo livello di difesa sul perimetro, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti. |
| Opzione di applicazione automatizzata | Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop. |
| Distribuzione e installazione automatizzate | La distribuzione e l'installazione macchina per macchina dei client antivirus e antispyware sono automatizzate sull'intera rete, riducendo al minimo l'impegno amministrativo. |
| Antivirus di nuova generazione | Capture Client utilizza un engine statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto. |
| Protezione antispyware | La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza analizzando e bloccando i programmi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili. |

## Riepilogo delle funzionalità di SonicOS

### 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
- API REST

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

### Capture Advanced Threat Protection[1,2]
- 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
- Intelligence sulle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

### Prevenzione delle intrusioni[1]
- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Filtraggio GeoIP/Botnet[2]
- Corrispondenza con espressioni regolari

### Anti-malware[1]
- 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[1]
- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di eventuali perdite di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database 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 HTTP/HTTPS Web[1]
- Filtraggio degli URL
- Tecnologia antiproxy
- 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
- Provisioning automatico delle VPN
- VPN IPSec per la connettività Site-to-Site
- 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
- SD-WAN sicura
- PortShield
- Registrazione avanzata
- QoS layer 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato sulle politiche (ToS/metrico ed ECMP)
- Routing asimmetrico
- Server DHCP
- NAT
- Gestione della larghezza di banda
- Alta disponibilità - Active/Standby con sincronizzazione di stato[3]
- Bilanciamento del carico in ingresso/in uscita
- Modalità Bridge (L2), NAT
- Failover WAN 3G/4G
- 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 e monitoraggio
- GUI Web
- CLI (Command Line Interface)
- SNMPv2/v3
- Gestione centralizzata e reportistica con SonicWall GMS e Capture Security Center
- Accesso
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Gestione di switch Dell delle serie N e X, anche in cascata[2]

### Wireless integrato
- Dual-band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac[2]
- WIDS/WIPS
- Servizi guest wireless
- Messaggistica hotspot leggera
- Segmentazione degli access point virtuali
- Captive portal
- ACL cloud

[1] *Richiede un abbonamento aggiuntivo*
[2] *Non disponibile su SOHO/SOHO Wireless*
[3] *Alta disponibilità con sincronizzazione dello stato disponibile solo sui modelli SonicWall TZ500 e SonicWall TZ600*

## Specifiche di sistema SonicWall serie TZ

| GENERALI FIREWALL | SERIE SOHO | SOHO SERIE 250 | SERIE TZ300 | SERIE TZ350 |
|---|---|---|---|---|
| Sistema operativo | SonicOS | | | |
| Interfacce | 5 da 1 GbE, 1 USB, 1 Console | | 5 da 1 GbE, 1 USB, 1 Console | 5 da 1 GbE, 1 USB, 1 Console |
| 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 | | | |
| Punti di accesso supportati (max) | 2 | 4 | 8 | 8 |
| **FIREWALL/PRESTAZIONI VPN** | **SERIE SOHO** | **SOHO SERIE 250** | **SERIE TZ300** | **SERIE TZ350** |
| Throughput con ispezione firewall[1] | 300 Mb/s | 600 Mb/s | 750 Mb/s | 1,0 Gb/s |
| Throughput con prevenzione delle minacce[2] | 150 Mb/s | 200 Mb/s | 235 Mb/s | 335 Mb/s |
| Throughput con ispezione applicazioni[2] | — | 275 Mb/s | 375 Mb/s | 600 Mb/s |
| Throughput con IPS[2] | 100 Mb/s | 250 Mb/s | 300 Mb/s | 400 Mb/s |
| Throughput con ispezione anti-malware[2] | 50 Mb/s | 100 Mb/s | 200 Mb/s | 300 Mb/s |
| Throughput con decrittografia e ispezione (SSL/DPI)[2] | 30 Mb/s | 40 Mb/s | 50 Mb/s | 65 Mb/s |
| Throughput con VPN IPSec[3] | 100 Mb/s | 200 Mb/s | 300 Mb/s | 430 Mb/s |
| 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** | **SOHO SERIE 250** | **SERIE TZ300** | **SERIE TZ350** |
| Tunnel VPN site-to-site | 10 | 10 | 10 | 15 |
| Client VPN IPSec (max) | 1 (5) | 1 (5) | 1 (10) | 1 (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) |
| Autenticazione/crittografia | DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B | | | |
| Key exchange | Gruppi Diffie-Hellman 1, 2, 5, 14v | | | |
| VPN basato su routing | 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 su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing | | | |
| Piattaforme del client della VPN globale supportate | Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 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 (Embedded) | | | |
| **SERVIZI DI SICUREZZA** | **SERIE SOHO** | **SOHO SERIE 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 | | | |
| Comprehensive Anti-Spam Service | 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** | **SOHO SERIE 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, 802.1p (WMM) | | | |

## Specifiche SonicWall serie TZ - continuazione

| NETWORKING - CONTINUAZIONE | SERIE SOHO | SOHO SERIE 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 locale | 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 | FIPS 140-2 (con Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus | | | |
| Certificazioni in corso | Common Criteria NDPP (Firewall e IPS) | | | |
| Common Access Card (CAC) | Supportato | | | |
| Alta disponibilità | No | | Active/Standby | |
| **HARDWARE** | **SERIE SOHO** | **SOHO SERIE 250** | **SERIE TZ300** | **SERIE TZ350** |
| Fattore di forma | Desktop | | | |
| Alimentazione | 24 W esterna | | 24 W esterna<br>65W esterna<br>(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<br>0,48 kg | | 0,73 kg<br>0,84 kg | 0,73 kg<br>0,84 kg |
| Peso RAEE | 0,80 kg<br>0,94 kg | | 1,15 kg<br>1,26 kg | 1,15 kg<br>1,26 kg |
| Peso con la confezione | 1,20 kg<br>1,34 kg | | 1,37 kg<br>1,48 kg | 1,37 kg<br>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** | **SOHO SERIE 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 | | 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 | |
| Conformità normative principali (modelli wireless) | FCC Classe B, FCC RF ICES Classe B, IC RF CE (R&TTE, EMC, LVD, 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 (R&TTE, EMC, LVD, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH | |
| **WIRELESS INTEGRATO** | **SERIE SOHO** | **SOHO SERIE 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[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 | | 802.11a: 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 - continuazione

| WIRELESS INTEGRATO | SERIE SOHO | SOHO SERIE 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 normativo specificato dall'amministratore di sistema | | | |
| Controllo potenza di trasmissione (TPC) | Supportato | | | |
| Velocità di trasmissione 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 TZ400, TZ500 e TZ600.*

[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*

## Specifiche di sistema SonicWall serie TZ - continuazione

| GENERALI FIREWALL | SERIE TZ400 | SERIE TZ500 | SERIE TZ600 |
|---|---|---|---|
| Sistema operativo | | SonicOS | |
| Interfacce | 7 da 1 GbE, 1 USB, 1 Console | 8 da 1 GbE, 2 USB, 1 Console | 10 da 1 GbE, 2 USB, 1 Console, 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 |
| Punti di accesso supportati (max) | 16 | 16 | 24 |
| **FIREWALL/PRESTAZIONI VPN** | **SERIE TZ400** | **SERIE TZ500** | **SERIE TZ600** |
| Throughput con ispezione firewall[1] | 1,3 Gb/s | 1,4 Gb/s | 1,9 Gb/s |
| Throughput con prevenzione delle minacce[2] | 600 Mb/s | 700 Mb/s | 800 Mb/s |
| Throughput con ispezione applicazioni[2] | 1,2 Gb/s | 1,3 Gb/s | 1,8 Gb/s |
| Throughput con IPS[2] | 900 Mb/s | 1,0 Gb/s | 1,2 Gb/s |
| Throughput con ispezione anti-malware[2] | 600 Mb/s | 700 Mb/s | 800 Mb/s |
| Throughput con decrittografia e ispezione (SSL/DPI)[2] | 150 Mb/s | 200 Mb/s | 300 Mb/s |
| Throughput con VPN IPSec[3] | 900 Mb/s | 1,0 Gb/s | 1,1 Gb/s |
| 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 site-to-site | 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) |
| Autenticazione/crittografia | | DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B | |
| Key exchange | | Gruppi Diffie-Hellman 1, 2, 5, 14v | |
| VPN basato su routing | | 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 su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing | |
| Piattaforme del client della VPN globale supportate | | Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 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 (Embedded) | |
| **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 | |
| Comprehensive Anti-Spam Service | | 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 - continuazione

| 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 locale | 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, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus | | |
| Certificazioni in corso | Common Criteria NDPP (Firewall e IPS) | | |
| Common Access Card (CAC) | Supportato | | |
| Alta disponibilità | Active/Standby | Active/Standby con sincronizzazione dello stato | |
| **HARDWARE** | **SERIE TZ400** | **SERIE TZ500** | **SERIE TZ600** |
| Fattore di forma | Desktop | | |
| Alimentazione | 24 W esterna | 36W esterna | 60W esterna<br>180W esterna<br>(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<br>0,84 kg | 0,92 kg<br>1,05 kg | 1,47 kg |
| Peso RAEE | 1,15 kg<br>1,26 kg | 1,34 kg<br>1,48 kg | 1,89 kg |
| Peso con la confezione | 1,37 kg<br>1,48 kg | 1,93 kg<br>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 | 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 | FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL, cUL, TÜV/ GS, CB, CoC UL (Messico), RAEE, REACH, KCC/MSIP |
| Conformità normative principali (modelli wireless) | FCC Classe B, FCC RF ICES Classe B, IC RF CE (R&TTE, EMC, LVD, 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 (R&TTE, EMC, LVD, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH | — |

## Specifiche di sistema SonicWall serie TZ - continuazione

| 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: 2,412 - 2,472 GHz, 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 (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 normativo specificato dall'amministratore di sistema | | — |
| Controllo potenza di trasmissione (TPC) | Supportato | | — |
| Velocità di trasmissione 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) | | — |

Informazioni per ordinare SonicWall serie TZ

| Prodotto | SKU |
|---|---|
| SOHO con 1 anno di TotalSecure | 01-SSC-0651 |
| SOHO Wireless-N con 1 anno di TotalSecure | 01-SSC-0653 |
| 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 |
| TZ600 con 1 anno di TotalSecure Advanced Edition | 01-SSC-1711 |
| TZ600P con 1 anno di TotalSecure Advanced Edition | 02-SSC-0600 |
| **Opzioni di alta disponibilità (ogni unità deve essere dello stesso modello)** | |
| TZ500 ad alta disponibilità | 01-SSC-0439 |
| TZ600 ad alta disponibilità | 01-SSC-0220 |

| Servizi | SKU |
|---|---|
| **Per SonicWall serie SOHO** | |
| Suite di sicurezza completa per gateway Security Suite - Prevenzione delle minacce, filtraggio dei contenuti e assistenza 24x7 (1 anno) | 01-SSC-0688 |
| Antivirus per gateway - prevenzione intrusioni e controllo applicazioni (1 anno) | 01-SSC-0670 |
| Servizio filtraggio contenuti (1 anno) | 01-SSC-0676 |
| Servizio completo antispam (1 anno) | 01-SSC-0682 |
| Assistenza 24x7 (1 anno) | 01-SSC-0700 |
| **Per SonicWall SOHO serie 250** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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 |

## Informazioni per ordinare SonicWall serie TZ

| | |
|---|---|
| **Per SonicWall TZ350 Series** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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 |
| **Per SonicWall TZ400 Series** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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** | |
| Suite di sicurezza avanzata per gateway - Capture ATP, prevenzione minacce, filtraggio contenuti 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 |

### 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 |

### SonicWall

SonicWall è attiva nel settore della lotta al cibercrimine da più di 27 anni a difesa delle PMI, delle imprese e degli enti pubblici in ogni parte del mondo. Grazie alla ricerca dei SonicWall Capture Lab, le nostre premiate soluzioni di rilevamento e prevenzione delle violazioni in tempo reale garantiscono più di un milione di reti con le email, le applicazioni e i dati relativi, in oltre 215 paesi e territori, consentendo alle organizzazioni di funzionare in modo più efficace e con meno timori per la sicurezza. Per ulteriori informazioni visitare www.sonicwall.com o seguirci su Twitter, LinkedIn, Facebook e Instagram.



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



Datasheet-TZ Series-US-VG-MKTG5144