SonicWall TZ Series

Sicurezza e prestazioni eccezionali a un TCO incredibilmente basso

I firewall UTM (Unified Threat Management) della serie SonicWall TZ sono ideali per tutte le aziende che necessitano di una protezione di rete di classe enterprise.

I firewall SonicWall TZ Series forniscono ampia protezione e servizi di sicurezza avanzata con tecnologie integrate basate su cloud come antimalware, antispyware, controllo delle applicazioni, sistema di prevenzione delle intrusioni (IPS) e filtraggio di contenuti/URL. Per contrastare gli attacchi crittografati, i firewall della serie TZ dispongono della potenza di elaborazione per ispezionare le connessioni SSL/TLS crittografate, proteggendo dalle minacce più recenti. In combinazione con gli switch serie X di Dell, alcuni modelli firewall della serie TZ possono gestire direttamente la sicurezza di queste porte aggiuntive.

Con il supporto della rete SonicWall Capture, i firewall SonicWall TZ Series forniscono aggiornamenti costanti, che garantiscono un'efficace protezione della rete contro i criminali informatici. Questi firewall sono in grado di analizzare ogni byte di ogni pacchetto su tutte le porte e i protocolli, con una latenza quasi nulla e nessun limite alle dimensioni dei file.

I firewall SonicWall TZ Series sono dotati di porte Gigabit Ethernet, connettività wireless integrata 802.11ac opzionale*, VPN IPSec e SSL, failover mediante supporto 3G/4G integrato, bilanciamento del carico e segmentazione della rete. I firewall UTM della linea SonicWall TZ Series, inoltre, forniscono un accesso mobile rapido e sicuro attraverso le piattaforme Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X e Linux.

Grazie a SonicWall Global Management System (GMS) i firewall SonicWall TZ Series possono essere installati e gestiti centralmente da un unico sistema.

Sicurezza gestita per gli ambienti distribuiti

Scuole, negozi, filiali, uffici remoti e aziende distribuite richiedono tutti una soluzione che si integri con il firewall aziendale. I firewall SonicWall TZ Series presentano la stessa base di codice e lo stesso livello di protezione dei firewall di nuova generazione SuperMassive, il prodotto di punta dell'azienda. Gestire i siti remoti non è mai stato così semplice, perché tutti gli amministratori possono utilizzare la stessa interfaccia utente. GMS consente agli amministratori di rete di configurare, monitorare e gestire in remoto i firewall SonicWall mediante un unico pannello. Grazie alla connettività wireless sicura ad alta velocità, la linea SonicWall TZ Series amplia il perimetro di protezione fino a includere i clienti e gli utenti guest che si trovano in un ufficio remoto o negozio.

Vantaggi:

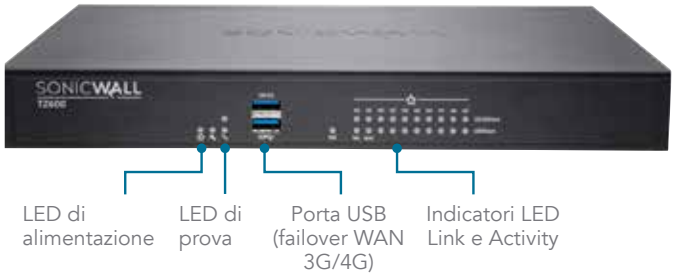
- Protezione di rete di classe enterprise
- Analisi DPI (Deep Packet Inspection) di tutto il traffico, senza limiti alle dimensioni dei file o protocolli
- Connettività wireless 802.11ac sicura mediante un controller wireless integrato o i punti di accesso wireless esterni SonicWall SonicPoint
- Accesso mobile a VPN SSL per dispositivi Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS e Linux
- In combinazione con gli switch Dell della serie X è possibile gestire in sicurezza più di 100 porte aggiuntive tramite la console TZ

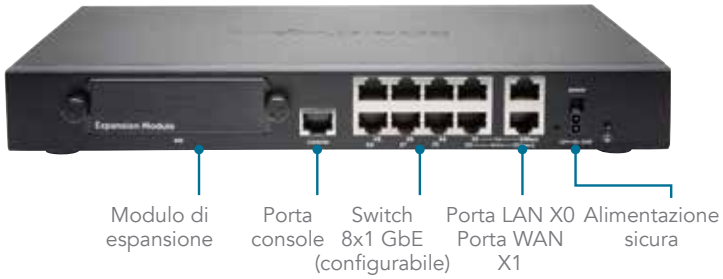
** 802.11ac non è attualmente disponibile per i modelli SOHO, che supportano 802.11a/b/g/n*

SonicWall TZ600 Series

Per le imprese, i negozi e le filiali emergenti che necessitano di prestazioni di sicurezza a un prezzo competitivo, il firewall SonicWall TZ600 di nuova generazione protegge le reti con funzionalità di classe enterprise e prestazioni senza compromessi.

Specifiche	TZ600 Series
Throughput firewall	1,5 Gb/s
Throughput DPI completo	500 Mb/s
Throughput antimalware	500 Mb/s
Throughput IPS	1,1 Gb/s
Throughput IMIX	900 Mb/s
Num. max. connessioni DPI	125.000
Nuove connessioni/sec	12.000





SonicWall TZ500 Series

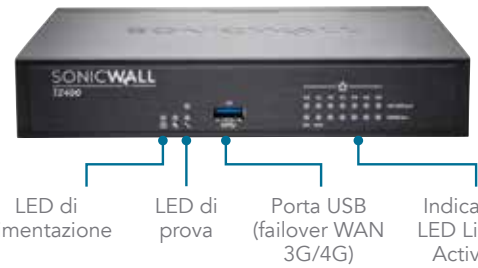
Per le PMI e le filiali in crescita, SonicWall TZ500 Series fornisce protezione altamente efficace e senza compromessi, con produttività di rete e connettività wireless integrata dual-band 802.11ac opzionale.

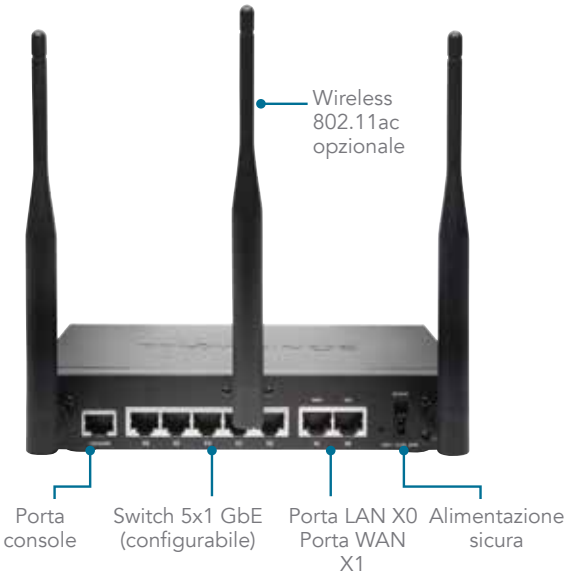
Specifiche	TZ500 Series
Throughput firewall	1,4 Gb/s
Throughput DPI completo	400 Mb/s
Throughput antimalware	400 Mb/s
Throughput IPS	1,0 Gb/s
Throughput IMIX	700 Mb/s
Num. max. connessioni DPI	100.000
Nuove connessioni/sec	8.000

SonicWall TZ400 Series

Per le piccole imprese, i negozi e le filiali, la linea SonicWall TZ400 Series 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 DPI completo	300 Mb/s
Throughput antimalware	300 Mb/s
Throughput IPS	900 Mb/s
Throughput IMIX	500 Mb/s
Num. max. connessioni DPI	90.000
Nuove connessioni/sec	6.000

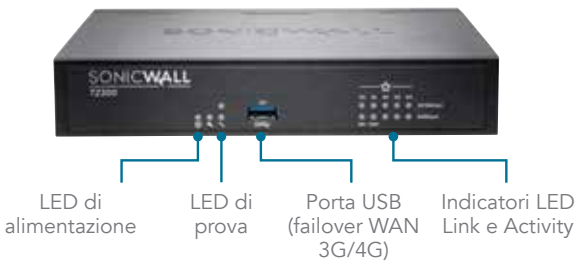


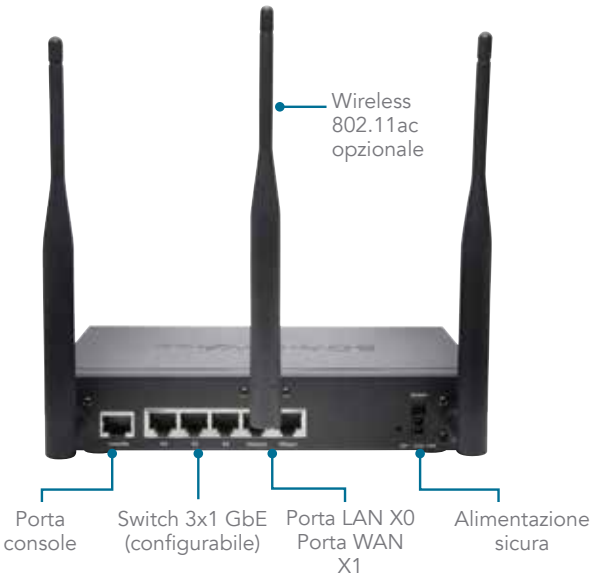


SonicWall TZ300 Series

La linea SonicWall TZ300 Series offre una soluzione all-in-one che protegge la rete dagli attacchi. Contrariamente ai prodotti per privati, il firewall SonicWall TZ300 Series combina prevenzione delle intrusioni, funzioni antimalware e filtraggio di contenuti/URL altamente efficaci con connettività wireless integrata 802.11ac opzionale e il supporto sicuro più ampio alle piattaforme mobili per notebook, smartphone e tablet.

Specifiche	TZ300 Series
Throughput firewall	750 Mb/s
Throughput DPI completo	100 Mb/s
Throughput antimalware	100 Mb/s
Throughput IPS	300 Mb/s
Throughput IMIX	200 Mb/s
Num. max. connessioni DPI	50.000
Nuove connessioni/sec	5.000

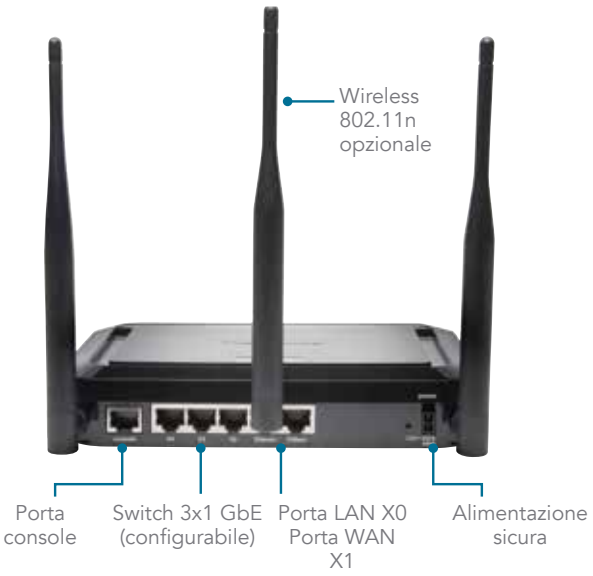




Serie SonicWall SOHO

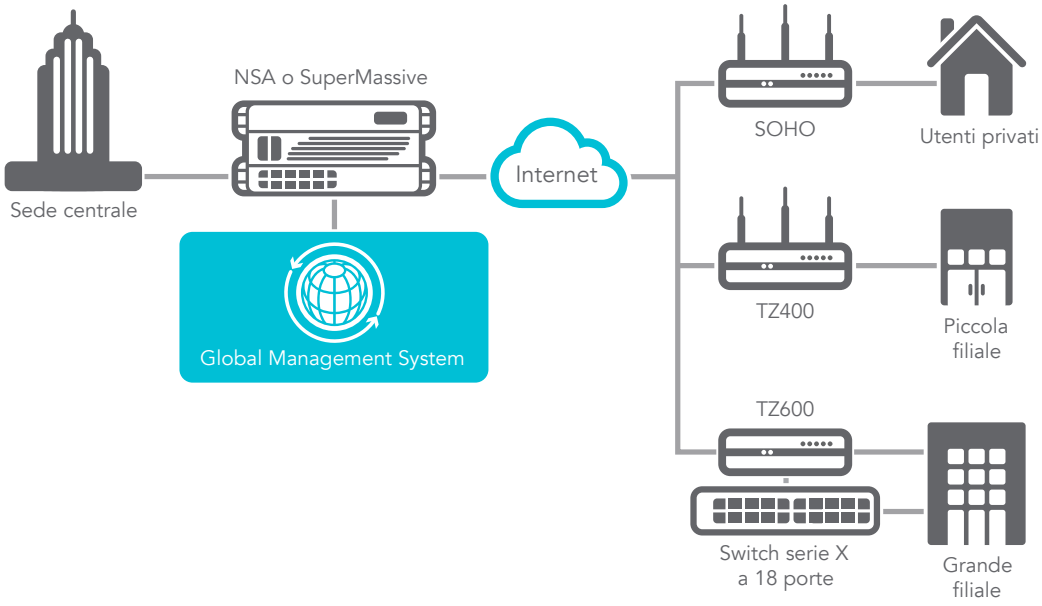
Per gli ambienti SOHO cablati e wireless, la serie SonicWall SOHO fornisce la stessa protezione di classe enterprise richiesta dalle grandi organizzazioni, ma a costi più accessibili.

Specifiche	Serie SOHO
Throughput firewall	300 Mb/s
Throughput DPI completo	50 Mb/s
Throughput antimalware	50 Mb/s
Throughput IPS	100 Mb/s
Throughput IMIX	60 Mb/s
Num. max. connessioni DPI	10.000
Nuove connessioni/sec	1.800



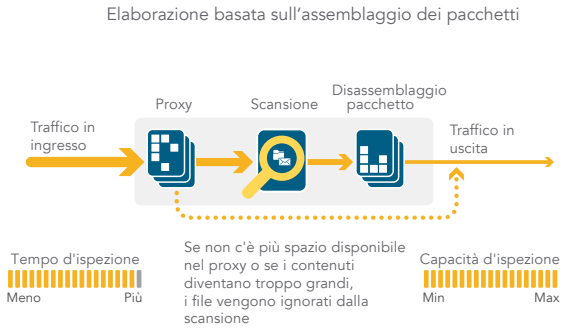
Architettura ampliabile per massime prestazioni e scalabilità

Durante la progettazione del motore Reassembly-Free Deep Packet Inspection (RFDPI) si è prestata particolare attenzione a garantire una scansione di sicurezza con prestazioni elevate, che fosse compatibile con l'espansione continua e il parallelismo intrinseco del traffico di rete. Se combinata con sistemi di processori multi-core, questa architettura software incentrata sui parallelismi è perfettamente scalabile per gestire i requisiti della tecnologia DPI in caso di carichi di traffico elevati. La piattaforma SonicWall TZ Series è basata su processori che, a differenza dei sistemi x86, sono ottimizzati per l'elaborazione di rete, crittografia e pacchetti, assicurando al tempo stesso flessibilità e possibilità di programmazione sul campo, un aspetto critico per i sistemi ASIC. Questa flessibilità è un fattore essenziale quando si tratta di aggiornare comportamenti e nuovi codici per difendersi da attacchi inediti, che richiedono tecniche di rilevamento più sofisticate e innovative.

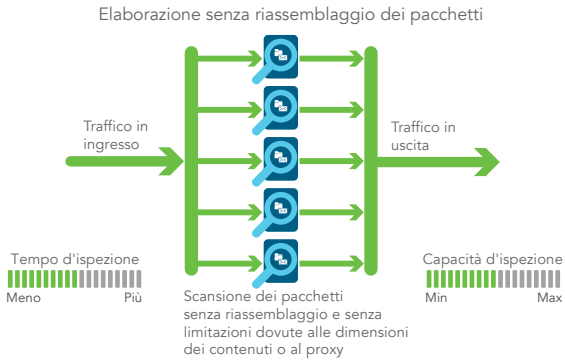


Motore Reassembly-Free Deep Packet Inspection (RFDPI)

Il motore RFDPI assicura un controllo delle applicazioni e una protezione dalle minacce di qualità superiore senza pregiudicare le prestazioni. Si tratta di un sistema brevettato che analizza il flusso di traffico per rilevare le minacce ai livelli da 3 a 7. I flussi di rete vengono individuati con procedure complesse e ripetute di normalizzazione e decrittografia, per sventare le tecniche di evasione avanzata che tentano di confondere i motori di rilevamento e introdurre codici dannosi nella rete. Dopo la fase obbligatoria di pre-elaborazione, che comprende la decrittografia SSL, ogni pacchetto viene confrontato con una rappresentazione nella memoria proprietaria di tre database di firme, corrispondenti ad applicazioni, malware e attacchi intrusivi. 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. Con l'identificazione del malware, il firewall SonicWall arresta la connessione prima che si possano verificare eventi negativi e registra correttamente l'evento. Il motore può comunque essere configurato solo per l'analisi oppure, se si tratta del rilevamento di applicazioni, per fornire servizi che gestiscano la larghezza di banda di livello 7 nel flusso restante non appena viene individuata l'applicazione.



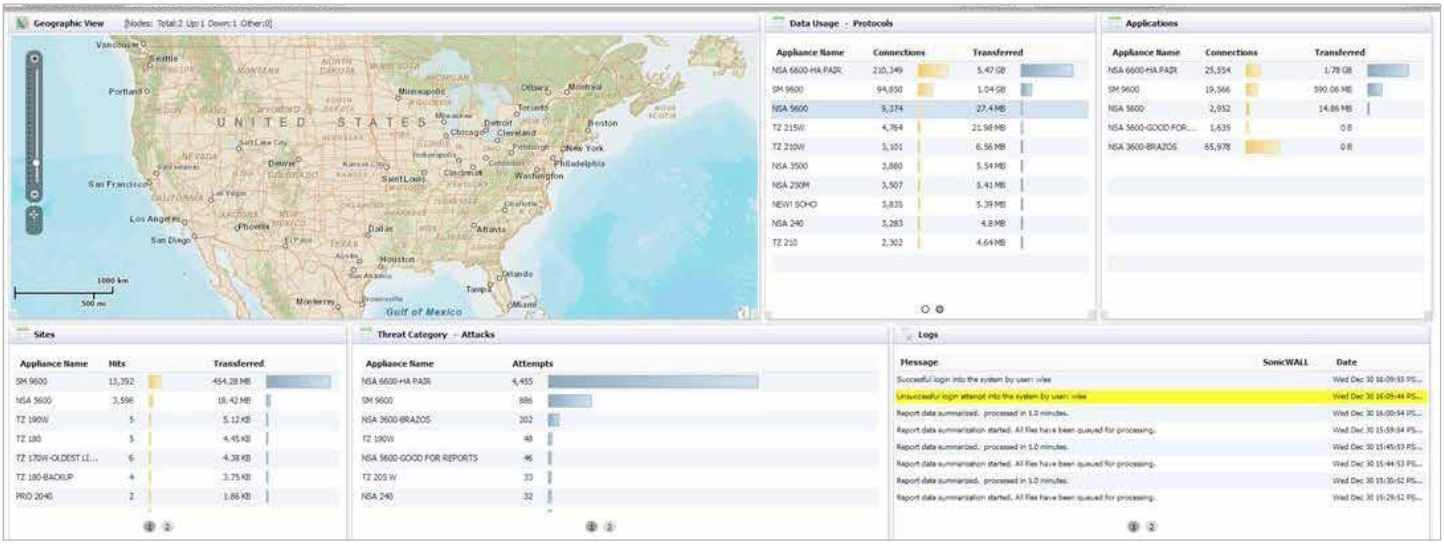
Architettura della concorrenza



Architettura SonicWall

Creazione di rapporti e gestione globale

Con la soluzione opzionale SonicWall Global Management System (GMS), gli amministratori delle imprese distribuite di grandi dimensioni hanno a disposizione una piattaforma unificata, sicura e ampliabile per gestire le appliance di sicurezza SonicWall e gli switch serie X di Dell. La soluzione semplifica il consolidamento gestionale delle appliance di sicurezza, mitiga le complessità relative all'amministrazione e alla risoluzione dei problemi e disciplina tutti gli aspetti operativi dell'infrastruttura di sicurezza: l'applicazione e la gestione centralizzate delle policy, il monitoraggio degli eventi in tempo reale, l'analisi, la creazione di rapporti e altro ancora. Inoltre, grazie a una funzionalità di automazione dei flussi di lavoro, il sistema GMS va incontro ai requisiti delle imprese per la gestione delle modifiche del firewall. La soluzione GMS rappresenta un metodo migliore per gestire la sicurezza di rete, poiché non agisce dispositivo per dispositivo, ma in base a livelli di servizio e processi aziendali che semplificano drasticamente la gestione del ciclo di vita complessivo dell'ambiente di lavoro.



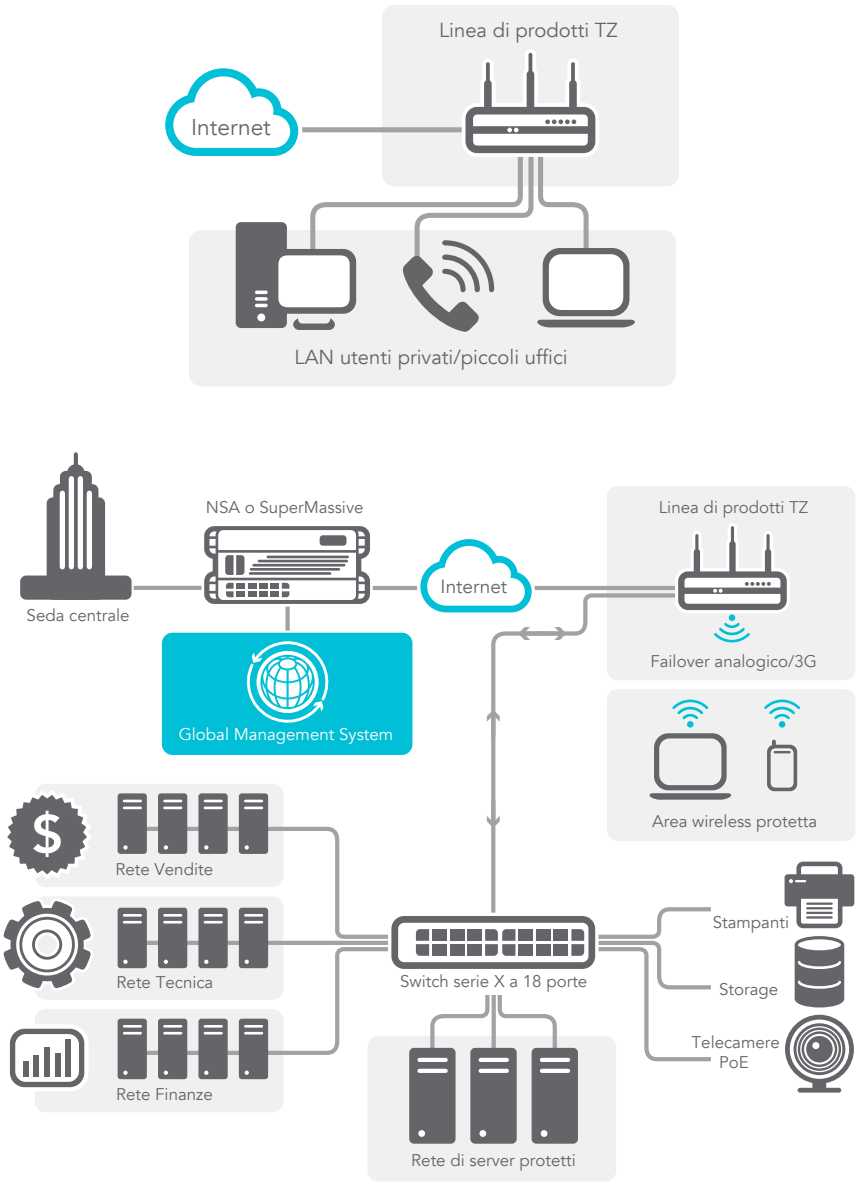
SONICWALL®

Sicurezza e protezione

Capture Labs, il team interno di SonicWall dedicato alla ricerca delle minacce, è costantemente impegnato a ricercare e sviluppare contromisure da implementare nei firewall in uso, in modo da mantenere aggiornata la protezione. Il team utilizza oltre un milione di sensori dislocati in tutto il mondo per raccogliere campioni di malware e dati telemetrici con informazioni sulle minacce più recenti. Questi dati servono a loro volta per le funzionalità di rilevamento delle applicazioni, antimalware e prevenzione delle intrusioni. Gli utenti dei firewall SonicWall con un abbonamento valido possono fare affidamento su una protezione sempre aggiornata 24 ore su 24, con nuovi aggiornamenti che vengono attivati senza riavvii o interruzioni. Le firme nelle appliance contrastano classi di attacchi molto ampie, che coprono fino a decine di migliaia di minacce con una sola firma. Oltre alle contromisure presenti nell'appliance, tutti i firewall SonicWall hanno accesso al servizio SonicWall CloudAV, che amplia le funzionalità di intelligence sulle firme integrate con oltre 20 milioni di firme, un valore che è in costante espansione. I firewall accedono al database del servizio CloudAV mediante un protocollo proprietario leggero, aumentando così la capacità d'ispezione dell'appliance. I firewall SonicWall di nuova generazione dispongono inoltre di funzionalità di geolocalizzazione IP e filtraggio di Botnet, che consentono di bloccare il traffico proveniente da domini pericolosi o da intere aree geografiche per ridurre il livello di rischio della rete.

Controllo e intelligence delle applicazioni

Il sistema di gestione delle applicazioni segnala agli amministratori il traffico delle applicazioni che attraversa la rete. Questo permette di pianificare opportuni controlli sulla base delle priorità aziendali, circoscrivere le applicazioni poco produttive e bloccare quelle potenzialmente pericolose. La visualizzazione in tempo reale individua subito le anomalie nel traffico, consentendo di adottare contromisure immediate contro potenziali attacchi in entrata o uscita o colli di bottiglia per le prestazioni. Oltre a fornire efficaci funzionalità forensi e di risoluzione dei problemi, l'analisi del traffico delle applicazioni offerta da SonicWall aiuta a comprendere più approfonditamente il traffico delle applicazioni, l'utilizzo della larghezza di banda e le minacce alla sicurezza. Le funzionalità SSO (Single Sign-On) aggiuntive offrono ulteriori vantaggi, tra cui una migliore esperienza per gli utenti, un aumento di produttività e la riduzione delle chiamate al supporto tecnico. Un'interfaccia Web intuitiva semplifica la gestione e il controllo dell'intelligence delle applicazioni.



Wireless flessibile e sicuro

La connettività wireless 802.11ac ad alta velocità, disponibile come funzionalità opzionale*, si combina alla tecnologia firewall SonicWall di ultima generazione per creare una soluzione di sicurezza di rete wireless che fornisce protezione completa per le reti cablate e wireless.

Le prestazioni wireless di classe enterprise consentono ai dispositivi abilitati al Wi-Fi di connettersi da distanze maggiori e di utilizzare app per dispositivi mobili a consumo intensivo di banda, come video e voce, in ambienti a densità più alta, senza degradazione del segnale.

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

Caratteristiche

Motore RFDPI	
Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection	Si tratta di un motore di ispezione proprietario, brevettato e ad alte prestazioni, che esegue analisi bidirezionali del traffico basate sui flussi senza l'uso di proxy o buffering. Lo scopo è individuare tentativi di intrusione, rilevare malware e individuare il traffico delle applicazioni in qualsiasi porta.
Ispezione bidirezionale	Con la scansione simultanea del traffico in entrata 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 single-pass	Un'architettura DPI single-pass consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, in modo da ridurre notevolmente la latenza dell'ispezione DPI e mettere in correlazione tutte le informazioni sulle minacce in un'unica architettura.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per l'ispezione DPI su flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata tanto a protocolli comuni, quanto a flussi TCP primari.
Deep Packet Inspection di Secure Socket Shell (DPI-SSH)	Identifica e previene attacchi crittografati avanzati che sfruttano il protocollo SSH, blocca il download di malware cifrato, arresta la diffusione di infezioni e impedisce comunicazioni di comando e controllo e la sottrazione di dati.
Capture Advanced Threat Protection	
Funzionalità	Descrizione
Sandbox multi-engine	La piattaforma sandbox multi-engine, che include la piena emulazione di sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità sulle attività malevole.
Analisi di un'ampia varietà di file	Supporta l'analisi di un'ampia gamma di tipi di file, tra cui programmi eseguibili (PE), DLL, documenti PDF e MS Office, archivi, JAR e APK, su diversi sistemi operativi come Windows, Android, Mac OSX e ambienti multi-browser.
Rapida installazione delle firme	Quando un file viene identificato come dannoso, una signature viene inviata immediatamente ai firewall con abbonamento al servizio SonicWall Capture, ai database con le firme per l'antivirus a livello gateway e l'ispezione IPS e ai database di reputazione degli URL, degli IP e dei domini entro 48 ore.
Blocco fino all'identificazione	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.
Prevenzione delle minacce crittografate	
Funzionalità	Descrizione
Ispezione e decrittografia TLS/SSL	Il traffico SSL viene immediatamente decrittografato e analizzato senza l'uso di proxy, per individuare malware, intrusioni e perdite di dati, e vengono applicate policy per il controllo di contenuti, URL e applicazioni che difendono dalle minacce nascoste nel traffico TLS/SSL crittografato. L'opzione è inclusa negli abbonamenti di sicurezza di tutti i modelli, tranne SOHO. Per quest'ultimo è venduta come licenza a parte.
Ispezione DPI-SSH	L'ispezione approfondita dei pacchetti del protocollo SSH (DPI-SSH) decripta e ispeziona i dati che attraversano i tunnel SSH, per prevenire attacchi basati su SSH.
Prevenzione delle intrusioni	
Funzionalità	Descrizione
Protezione basata sulle 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 di ricerca delle minacce del SonicWall Capture Labs 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.
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	Questa opzione individua e blocca gli attacchi che abusano dei protocolli per tentare di aggirare l'IPS.
Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura un aggiornamento costante 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 impediscono l'ingresso non rilevato delle minacce nella rete, grazie all'uso di tecniche di evasione nei livelli da 2 a 7.
Prevenzione delle minacce	
Funzionalità	Descrizione
Antimalware a livello gateway	Il motore 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 antimalware CloudAV	Nei server cloud di SonicWall è presente un database sempre aggiornato di oltre 20 milioni di firme sulle minacce, che viene consultato per potenziare le funzionalità del database di firme integrato e assicurare alle opzioni RFDPI una copertura estesa delle minacce.
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.

Prevenzione delle minacce (cont.)	
Funzionalità	Descrizione
Ispezione e decrittografia SSL	Il traffico SSL viene decrittografato e analizzato all'istante, senza l'uso di proxy, per individuare malware, intrusioni e perdite di dati, e vengono applicate policy per il controllo di contenuti, URL e applicazioni che difendono dalle minacce nascoste nel traffico SSL crittografato. L'opzione è inclusa negli abbonamenti di sicurezza di tutti i modelli, tranne SOHO. Per quest'ultimo è venduta come licenza a parte.
Ispezione bidirezionale dei TCP primari	La capacità di scansione bidirezionale dei flussi TCP primari, eseguita in tutte le porte dal motore RFDPI, previene gli attacchi che tentano di aggirare i sistemi di sicurezza obsoleti dove erano protette 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.
Controllo e intelligence delle applicazioni	
Funzionalità	Descrizione
Controllo delle applicazioni	Per potenziare la sicurezza e la produttività della rete, vengono controllate le applicazioni o le singole funzionalità che il motore RFDPI ha identificato a fronte di un database in crescita di oltre 3.500 firme di applicazioni.
Identificazione delle applicazioni personalizzate	Per verificare le applicazioni personalizzate e quindi acquisire maggiore controllo sulla rete, è possibile creare firme basate su schemi o parametri specifici, che risultano univoci per un'applicazione nelle relative comunicazioni di 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 più importanti.
Controllo granulare	Questa opzione 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/servizi Terminal/Citrix.
Filtraggio dei contenuti	
Funzionalità	Descrizione
Filtraggio dei contenuti interno/esterno	Con Content Filtering Service è possibile applicare le policy relative a un utilizzo accettabile e bloccare l'accesso ai siti Web che contengono informazioni o immagini inopportune o di ostacolo alla produttività. Con Content Filtering Client è inoltre possibile applicare policy che bloccano contenuti Internet specifici per i dispositivi 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.
YouTube per le scuole	I docenti possono scegliere tra centinaia di migliaia di video istruttivi messi a disposizione gratuitamente da YouTube EDU. I video sono organizzati per classe e argomento e sono conformi agli standard didattici più diffusi.
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	Le funzionalità del firewall sono utilizzate come primo livello di difesa presso il perimetro, insieme alla protezione degli endpoint che impedisce l'ingresso di virus nella rete attraverso notebook, unità USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Questa opzione verifica che in tutti i computer con accesso alla rete sia installata e attiva la versione più recente delle firme antivirus e antispyware. In questo modo si eliminano i costi normalmente legati alla gestione degli antivirus e degli antispyware sui computer desktop.
Opzione di installazione automatizzata	Per ridurre il carico amministrativo, l'installazione dei client per antivirus e antispyware avviene automaticamente, computer per computer, in tutta la rete.
Protezione automatica e sempre attiva contro i virus	Per migliorare la produttività degli utenti finali e ridurre le attività di gestione della sicurezza, gli aggiornamenti antivirus e antispyware più frequenti vengono distribuiti in modo trasparente a tutti i file server e i computer desktop.
Protezione antispyware	Grazie all'opzione di protezione avanzata contro gli spyware, è possibile eseguire scansioni e bloccare l'installazione di una serie completa di programmi spyware su desktop e notebook prima che vengano trasmessi dati riservati. Questo potenzia le prestazioni e la sicurezza dei computer desktop.
Firewall e connettività di rete	
Funzionalità	Descrizione
Stateful Packet Inspection	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle policy di accesso del firewall.
Protezione da attacchi DDoS/DoS	La protezione da flooding SYN offre una difesa dagli attacchi DOS che si basa su tecnologie di blacklist SYN di livello 2 e proxy SYN di livello 3. Inoltre tutela dagli attacchi DOS/DDoS mediante la protezione da flooding UDP/ICMP e la limitazione della frequenza di connessione.
Opzioni di installazione flessibili	La linea SonicWall TZ Series può essere installata nelle modalità NAT tradizionale, Layer 2 Bridge, Wire Mode e Network Tap.
Supporto di IPv6	Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con il più recente sistema SonicOS, l'hardware sarà in grado di supportare implementazioni di filtraggio.
Autenticazione biometrica per l'accesso remoto	Supporto dell'autenticazione per dispositivi mobili che non può essere facilmente condivisa o duplicata, come il riconoscimento delle impronte digitali, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Integrazione con switch della serie X	Gestione delle impostazioni di sicurezza delle porte aggiuntive, tra cui POE e POE+, da una singola interfaccia utilizzando il dashboard della serie TZ con gli switch serie X (non disponibile con il modello SOHO).

Firewall e connettività di rete (cont.)	
Funzionalità	Descrizione
Alta disponibilità	I modelli SonicWall TZ500 e SonicWall TZ600 supportano un'elevata disponibilità Active/Standby con sincronizzazione dello stato. I modelli SonicWall TZ300 e SonicWall TZ400 supportano un'elevata disponibilità Active/Standby senza sincronizzazione dello stato. L'opzione di disponibilità elevata non è presente sui modelli SonicWall SOHO.
API di gestione delle minacce	Consente al firewall di ricevere flussi di intelligence proprietari, OEM o di terze parti, per contrastare minacce zero-day, attacchi malicious insider, credenziali compromesse, ransomware e minacce persistenti avanzate.
Sicurezza delle reti wireless	La tecnologia wireless IEEE 802.11ac può fornire un throughput fino a 1,3 Gb/s, con maggiore copertura e affidabilità. Disponibile dai modelli SonicWall TZ600 ai modelli SonicWall TZ300. Connettività 802.11 a/b/g/n opzionale disponibile sui modelli SonicWall SOHO.
Gestione e creazione di rapporti	
Funzionalità	Descrizione
Global Management System (GMS)	Con SonicWall GMS è possibile monitorare varie appliance SonicWall e switch Dell della serie X, configurarle e creare rapporti mediante un'interfaccia intuitiva che riduce la complessità e i costi gestionali.
Gestione avanzata con un unico dispositivo	L'interfaccia Web intuitiva consente una configurazione comoda e veloce, integrando una CLI completa e il supporto per SNMPv2/3.
Creazione di rapporti sul flusso delle applicazioni IPFIX/NetFlow	Grazie ai protocolli IPFIX o NetFlow, le analisi sul traffico delle applicazioni e i dati di utilizzo possono essere impiegati per scopi di monitoraggio e per creare rapporti cronologici o in tempo reale con SonicWall GMSFlow Server o altri strumenti che supportano IPFIX e NetFlow.
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 site-to-site tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per una connettività Site-to-Site	La rete VPN IPSec ad alte prestazioni consente di utilizzare la soluzione SonicWall TZ Series come concentratore di VPN per migliaia di utenti privati, filiali o altri siti di grandi dimensioni.
VPN SSL o accesso remoto da 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 usano più WAN, è possibile configurare una VPN primaria e secondaria per un failover e un failback automatici di 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 SSO integrate si combinano con le informazioni esaustive ricavate da DPI per consentire il tracciamento delle attività e l'identificazione degli utenti.
GeoIP per l'identificazione del traffico da Paesi specifici	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da Paesi specifici. 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.
Filtro DPI con espressioni regolari	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza con espressioni regolari per impedire perdite di dati.

Riepilogo delle funzionalità di SonicOS

Firewall

- Stateful Packet Inspection
- 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 di gestione delle minacce

Ispezione e decrittografia SSL/SSH[1]

- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi host
- Controllo SSL

Capture Advanced Threat Protection[1]

- 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
- Capacità di blocco automatico

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
- Visualizzazione delle applicazioni[2]
- Blocco dei componenti delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di eventuali perdite di dati
- Creazione di rapporti sulle applicazioni tramite NetFlow/IPFIX
- Tracciamento delle attività degli utenti (SSO)
- Database completo di firme delle applicazioni

Filtraggio dei contenuti Web[1]

- Filtraggio degli URL
- Tecnologia antiproxy
- Blocco in base a parole chiave
- Categorie di classificazione CFS per la gestione della larghezza di banda
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Provisioning automatico delle VPN
- VPN IPSec per una 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

- PortShield
- Registrazione avanzata
- QoS Layer-2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato su policy (ToS/metrico ed ECMP)
- Routing asimmetrico
- Server DHCP
- NAT
- Gestione della larghezza di banda
- Alta disponibilità Active/Standby con sincronizzazione dello 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 e creazione di rapporti centralizzate con SonicWall GMS
- Logging
- Esportazione per Netflow/IPFix
- Backup della configurazione basato sul cloud
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Gestione di switch Dell serie X, anche in cascata

Wireless integrato

- Dual-band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac[2]
- Rilevamento e prevenzione delle intrusioni wireless
- Servizi guest wireless
- Messaggistica hotspot leggera
- Segmentazione dei punti di accesso virtuali
- Captive portal
- ACL cloud

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

SONICWALL®

Specifiche di sistema SonicWall TZ Series

Panoramica hardware	Serie SOHO	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Sistema operativo	SonicOS				
Core di elaborazione di sicurezza	2	2	4	4	4
Interfacce	5 da 1 GbE, 1 USB, 1 Console	5 da 1 GbE, 1 USB, 1 Console	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
Espansione	USB	USB	USB	2 USB	Slot di espansione (posteriore)*, 2 USB
Utenti Single Sign-On (SSO)	250	500	500	500	500
Interfacce VLAN	25	25	50	50	50
Punti di accesso supportati (max.)	2	8	16	16	24
Modelli di switch Dell serie X supportati	Non disponibile	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Firewall/prestazioni VPN	**Serie SOHO**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Throughput ispezione firewall[1]	300 Mb/s	750 Mb/s	1.300 Mb/s	1.400 Mb/s	1.500 Mb/s
Throughput Full DPI[2]	50 Mb/s	100 Mb/s	300 Mb/s	400 Mb/s	500 Mb/s
Throughput ispezione applicazioni[2]	-	300 Mb/s	900 Mb/s	1.000 Mb/s	1.100 Mb/s
Throughput IPS[2]	100 Mb/s	300 Mb/s	900 Mb/s	1.000 Mb/s	1.100 Mb/s
Throughput ispezione antimalware[2]	50 Mb/s	100 Mb/s	300 Mb/s	400 Mb/s	500 Mb/s
Throughput IMIX	60 Mb/s	200 Mb/s	500 Mb/s	700 Mb/s	900 Mb/s
Throughput decrittografia e ispezione TLS/SSL (SSL DPI)[2]	15 Mb/s	45 Mb/s	100 Mb/s	150 Mb/s	200 Mb/s
Throughput VPN IPSec[3]	100 Mb/s	300 Mb/s	900 Mb/s	1.000 Mb/s	1.100 Mb/s
Connessioni al secondo	1.800	5.000	6.000	8.000	12.000
Numero massimo di connessioni (SPI)	10.000	50.000	100.000	125.000	150.000
Numero massimo di connessioni (DPI)	10.000	50.000	90.000	100.000	125.000
Numero massimo di connessioni (SSL DPI)	100	500	500	750	750
VPN	**Serie SOHO**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Tunnel VPN site-to-site	10	10	20	25	50
Client VPN IPSec (massimo)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
Licenze VPN SSL (massimo)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual Assist in pacchetti (massimo)	-	1 (versione di prova di 30 giorni)	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	Diffie Hellman gruppi 1, 2, 5, 14				
VPN basato su routing	RIP, OSPF				
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 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 (integrato)				
Servizi di sicurezza	**Serie SOHO**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, scansione di parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, Cookie per la privacy, elenchi consenti/nega				
Antivirus e antispyware per client	McAfee® e Kaspersky™				
Comprehensive Anti-Spam Service	Supportato				
Visualizzazione delle applicazioni	No	Sì	Sì	Sì	Sì
Controllo delle applicazioni	Sì	Sì	Sì	Sì	Sì
Capture Advanced Threat Protection	No	Sì	Sì	Sì	Sì

SONICWALL®

Specifiche di sistema SonicWall TZ Series (cont.)

Connettività di rete	Serie SOHO	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Assegnazione indirizzo IP	Statico (client DHCP, PPPoE, L2TP e PPTP), server DHCP interno, DHCP relay				
Modalità NAT	1 a 1, 1 a molti, molti a 1, molti a molti, NAT flessibile (IPS sovrapposti), PAT, modalità trasparente				
Protocolli di routing[4]	BGP[4], OSPF, RIPv1/v2, routing statico, routing basato su policy				
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	LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, servizi Terminal, Citrix			
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				
Common Access Card (CAC)	Supportato				
Alta disponibilità	No	Active/Standby	Active/Standby	Active/Standby con sincronizzazione dello stato	Active/Standby con sincronizzazione dello stato
Hardware	**Serie SOHO**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Fattore di forma	Desktop				
Alimentazione (W)	24 W esterna	24 W esterna	24 W esterna	36 W esterna	60 W esterna
Potenza max. assorbita (W)	6,4/11,3	6,9/12,0	9,2/13,8	13,4/17,7	16,1
Alimentazione in ingresso	100-240 V CA, 50-60 Hz, 1 A				
Dissipazione di calore totale	21,8/38,7 BTU	23,5/40,9 BTU	31,3/47,1 BTU	45,9/60,5 BTU	55,1 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	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Peso	0,34 kg/0,75 lb 0,48 kg/1,06 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,92 kg/2,03 lb 1,05 kg/2,31 lb	1,47 kg/3,24 lb
Peso WEEE	0,80 kg/1,76 lb 0,94 kg/2,07 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,34 kg/2,95 lb 1,48 kg/3,26 lb	1,89 kg/4,16 lb
Peso con la confezione	1,20 kg/2,64 lb 1,34 kg/2,95 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,93 kg/4,25 lb 2,07 kg/4,56 lb	2,48 kg/5,47 lb
MTBF (anni)	58,9/56,1 (wireless)	56,1	54,0	40,8	18,4
Ambiente (operativo/storage)	0-40 °C (32-105 °F) / da -40 a 70 °C (da -40 a 158 °F)				
Umidità	5-95% senza condensa				
Normative	**Serie SOHO**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Modello normativo (cablato)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
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), WEEE, 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), WEEE, 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), WEEE, 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), WEEE, 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), WEEE, REACH, KCC/MSIP
Modello normativo (wireless)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
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), WEEE, 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), WEEE, 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), WEEE, 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), WEEE, REACH	-

SONICWALL®

Specifiche di sistema SonicWall TZ Series (cont.)

Wireless integrato	Serie SOHO	Serie TZ300, TZ400, TZ500	TZ600
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	-
Canali operativi	802.11a: USA e Canada 12, Europa 11, Giappone 4, Singapore 4, Taiwan 4; 802.11b/g: USA e Canada 1-11, Europa 1-13, Giappone 1-14 (14 solo 802.11b); 802.11n (2,4 GHz): USA e Canada 1-11, Europa 1-13, Giappone 1-13; 802.11n (5 GHz): USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64;	802.11a: USA e Canada 12, Europa 11, Giappone 4, Singapore 4, Taiwan 4; 802.11b/g: USA e Canada 1-11, Europa 1-13, Giappone 1-14 (14 solo 802.11b); 802.11n (2,4 GHz): USA e Canada 1-11, Europa 1-13, Giappone 1-13; 802.11n (5 GHz): USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64; 802.11ac: USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64	-
Potenza di trasmissione in uscita	In base al dominio normativo specificato dall'amministratore di sistema	In base al dominio normativo specificato dall'amministratore di sistema	-
Controllo potenza di trasmissione	Supportato	Supportato	-
Velocità di trasmissione dati supportate	802.11a: 6, 9, 12, 18,24, 36, 48, 54 Mb/s per canale; 802.11b: 1, 2, 5,5, 11 Mb/s per canale; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s per canale; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150 Mb/s per canale;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s per canale; 802.11b: 1, 2, 5,5, 11 Mb/s per canale; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s per canale; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150 Mb/s 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 Mb/s 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 in base al valore RFC 2544 (per firewall). Le prestazioni effettive possono variare a seconda delle condizioni di rete e dei servizi attivati.*

[2]*Throughput Full DPI/Gateway antivirus/antispyware/IPS misurato mediante il test di prestazioni standard Spirent WebAvalanche HTTP e gli strumenti di test Ixia. Il test viene eseguito con più flussi attraverso varie coppie di porte.*

[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 il supporto dual-band, utilizzare i prodotti SonicWall con punti di accesso wireless (SonicPoint)*

Informazioni per ordinare SonicWall TZ Series

Prodotto	SKU
SonicWall SOHO con 1 anno di TotalSecure	01-SSC-0651
SonicWall SOHO Wireless-N con 1 anno di TotalSecure	01-SSC-0653
SonicWall TZ300 con 1 anno di TotalSecure	01-SSC-0581
SonicWall TZ300 Wireless-AC con 1 anno di TotalSecure	01-SSC-0583
SonicWall TZ400 con 1 anno di TotalSecure	01-SSC-0514
SonicWall TZ400 Wireless-AC con 1 anno di TotalSecure	01-SSC-0516
SonicWall TZ500 con 1 anno di TotalSecure	01-SSC-0445
SonicWall TZ500 Wireless-AC con 1 anno di TotalSecure	01-SSC-0446
SonicWall TZ600 con 1 anno di TotalSecure	01-SSC-0219
Opzioni di alta disponibilità (ogni unità deve corrispondere allo stesso modello)	
SonicWall TZ500 ad alta disponibilità	01-SSC-0439
SonicWall TZ600 ad alta disponibilità	01-SSC-0220

Informazioni per ordinare SonicWall TZ Series

Servizi	SKU
Per SonicWall SOHO Series	
Comprehensive Gateway Security Suite (1 anno)	01-SSC-0688
Antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni (1 anno)	01-SSC-0670
Content Filtering Service (1 anno)	01-SSC-0676
Comprehensive Anti-Spam Service (1 anno)	01-SSC-0682
Supporto 24 ore su 24, 7 giorni su 7 (1 anno)	01-SSC-0700
Per SonicWall TZ300 Series	
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per TZ300 (1 anno)	01-SSC-1430
Capture Advanced Threat Protection per TZ300 (1 anno)	01-SSC-1435
Antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni (1 anno)	01-SSC-0602
Content Filtering Service (1 anno)	01-SSC-0608
Comprehensive Anti-Spam Service (1 anno)	01-SSC-0632
Supporto 24 ore su 24, 7 giorni su 7 (1 anno)	01-SSC-0620
Per SonicWall TZ400 Series	
Suite di sicurezza avanzata al gateway – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per TZ400 (1 anno)	01-SSC-1440
Capture Advanced Threat Protection per TZ400 (1 anno)	01-SSC-1445
Antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni (1 anno)	01-SSC-0534
Content Filtering Service (1 anno)	01-SSC-0540
Comprehensive Anti-Spam Service (1 anno)	01-SSC-0561
Supporto 24 ore su 24, 7 giorni su 7 (1 anno)	01-SSC-0552
Per SonicWall TZ500 Series	
Suite di sicurezza avanzata al gateway – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per TZ500 (1 anno)	01-SSC-1450
Capture Advanced Threat Protection per TZ500 (1 anno)	01-SSC-1455
Antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni (1 anno)	01-SSC-0458
Content Filtering Service (1 anno)	01-SSC-0464
Comprehensive Anti-Spam Service (1 anno)	01-SSC-0482
Supporto 24 ore su 24, 7 giorni su 7 (1 anno)	01-SSC-0476
Per SonicWall TZ600	
Suite di sicurezza avanzata al gateway – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per TZ600 (1 anno)	01-SSC-1460
Capture Advanced Threat Protection per TZ600 (1 anno)	01-SSC-1465
Antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni (1 anno)	01-SSC-0228
Content Filtering Service (1 anno)	01-SSC-0234
Comprehensive Anti-Spam Service (1 anno)	01-SSC-0252
Supporto 24 ore su 24, 7 giorni su 7 (1 anno)	01-SSC-0246

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG658

SONICWALL®