

Firewall di nuova generazione



Fascia alta: Serie NSp

I firewall sono progettati per grandi imprese distribuite, data center e MSSP e si contraddistinguono per la protezione ad alte prestazioni, l'alta densità di porte e throughput di ispezione firewall fino a 100 Gbps.



Fascia media: Serie NSA

Efficacia e prestazioni di sicurezza riconosciute dal mercato per reti di medie dimensioni, filiali e aziende distribuite.



Entry Level: Serie TZ

Prevenzione delle minacce e piattaforma SD-WAN integrate per chi lavora da casa e presso PMI e SD-Branch.



SOHO e Micro PMI: TZ80

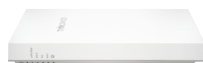
Protezione avanzata contro le minacce per piccoli uffici, home office, IoT e Micro PMI, con semplice gestione in cloud per implementazioni remote.

NSV

Virtuale: Serie NSv

Firewall virtuali con modalità di licenza flessibili per proteggere tutti i componenti critici delle infrastrutture cloud pubbliche e private.

I firewall SonicWall includono il filtraggio DNS e il filtraggio dei contenuti basato sulla reputazione per bloccare siti web e applicazioni dannose e consentono di impostare policy per la visualizzazione dei contenuti web utilizzando livelli di reputazione. L'ampia memoria per i file di audit, l'integrazione di Network Access Control (NAC) e gli aggiornamenti automatici aumentano la facilità d'uso.



Serie SonicWave

Sicurezza avanzata, prestazioni e scalabilità migliorate grazie al supporto Wi-Fi 6, gestione via cloud con SonicWall Wireless Network Manager o Network Security Manager.



Serie SMA

Accesso semplice, sicuro e basato su policy alle risorse di rete e in cloud.



SonicWall Switch

Garantisce una commutazione intelligente per la connettività sicura di nuova generazione per PMI e SD-Branch.



Protezione delle e-mail

Serie ESA

Una soluzione di protezione multilivello contro le minacce avanzate trasmesse per posta elettronica disponibile come apparecchiatura fisica, VM o SaaS in cloud.



Capture Security appliance (CSa)

Verifica dei file e prevenzione del malware on-premise.



Gestione, reportistica e analisi

SonicWall Unified Management

Network Security Manager

Wireless Network Manager

Visibilità unificata per la gestione centralizzata, la mitigazione dei rischi e l'applicazione delle policy. Report e informazioni dettagliate sul traffico e sulle minacce. Aggiornamenti, implementazioni e flussi di lavoro automatizzati.



Capture Client

Un client unificato semplice da implementare e basato su un doppio motore che offre difese stratificate, protezione e prevenzione delle minacce di classe enterprise, semplificando al contempo i silos di gestione. Protezione ottimale degli endpoint sia all'interno che all'esterno della rete locale.



Cloud Secure Edge

SonicWall Cloud Secure Edge (CSE), già Banyan Security, è una soluzione Security Service Edge (SSE) semplice da adottare che consente alla forza lavoro di accedere in sicurezza a qualsiasi risorsa da qualsiasi dispositivo. Offre un accesso Zero Trust semplice e sicuro a risorse private e internet per tutti i dipendenti e terze parti, indipendentemente dalla loro posizione di rete. A questo scopo, CSE combina le funzionalità di più appliance di rete tradizionali – VPN di accesso remoto, proxy web, firewall ecc. – in un'unica soluzione basata sul cloud, migliorando le posture di sicurezza e l'esperienza d'uso dell'intera forza lavoro.



Servizi di sicurezza gestiti

Un SOC presidiato 24x7x365 da tecnici esperti garantisce il monitoraggio e la risposta agli incidenti per l'intera superficie di attacco. Tutti i servizi sono disponibili senza quote minime o impegni a lungo termine.

Managed Detection and Response

protegge gli endpoint aggiungendo il monitoraggio di un SOC agli strumenti NGAV e EDR. SonicWall supporta diverse opzioni NGAV/EDR, tra cui Capture Client, Sentinel One e Windows Defender. Il servizio include controlli di configurazione bisettimanali e una Proof of Concept gratuita di 30 giorni.

Cloud Detection and Response

comprende due offerte: Cloud Threat Analytics offre il monitoraggio tramite SOC per molte applicazioni aziendali comuni basate sul cloud, come Microsoft 365, Salesforce e Slack. Cloud Email Security utilizza il machine learning per impedire che le e-mail di phishing raggiungano le caselle di posta degli utenti. Il monitoraggio a cura del SOC è disponibile per CES se acquistato insieme a Cloud Threat Analytics o come componente aggiuntivo.

Network Detection and Response

applica il monitoraggio del SOC ai log del firewall. NDR può essere applicato a qualsiasi firewall di qualsiasi produttore.



Servizi firewall di nuova generazione in abbonamento

Advanced Protection Security Suite

offre una protezione avanzata per la rete. Il pacchetto comprende i servizi essenziali più gestione cloud e reportistica e analisi basate sul cloud per 7 giorni.

Managed Protection Security Suite

include tutti i servizi di sicurezza della suite Advanced Protection più report e analisi estesi per 30 giorni e servizi di gestione dei firewall, tra cui monitoraggio e aggiornamenti del firmware.

Garanzia informatica integrata

Tutti i pacchetti delle suite di sicurezza includono una garanzia informatica integrata fino a 200.000 dollari. La garanzia consente di mitigare i costi in caso di violazioni della sicurezza e soddisfare i requisiti di conformità, offrendo una maggiore tranquillità.

SonicWall, Inc.

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

© 2025 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

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

La linea di prodotti in sintesi

sonicwall.com

