SCHEDA TECNICA

Suite di sicurezza e protezione SonicWall

Pacchetti semplificati per la gestione completa dei firewall e della sicurezza di rete

La sicurezza di rete è un argomento complesso da comprendere e ancor più da gestire. Per fortuna esiste una semplice soluzione per bloccare gli attacchi avanzati, valutare e mitigare i rischi e semplificare la gestione dei firewall.

SonicWall Advanced Protection Security Suite (APSS) e SonicWall Managed Protection Security Suite (MPSS) sono pacchetti semplificati di servizi di sicurezza completi, ideali per ogni esigenza aziendale.

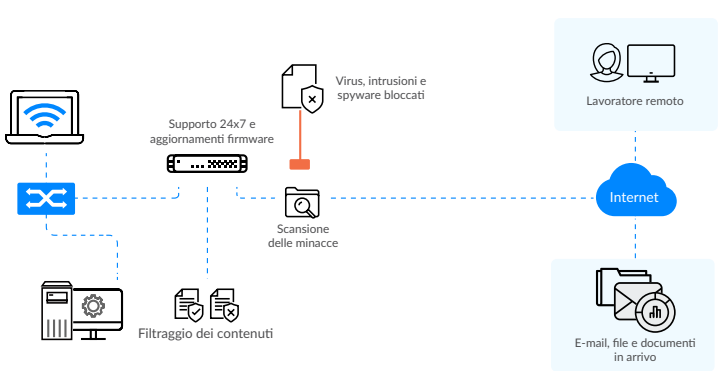
APSS include servizi di protezione contro le minacce avanzate, Capture ATP, gestione della rete basata sul cloud, report, analisi e supporto 24/7 per mantenere le aziende al sicuro e sempre un passo avanti rispetto alle minacce.

MPSS semplifica la gestione dei firewall, delegandola agli esperti di SonicWall. Oltre a tutti i servizi offerti in APSS, include il monitoraggio 24/7, la gestione della configurazione, aggiornamenti programmati del firmware e report dei controlli mensili di integrità che illustrano l'attività delle minacce e lo stato della protezione.

Entrambi i pacchetti includono la prima garanzia informatica per firewall del settore, che contribuisce a mitigare eventuali perdite finanziarie dovute a violazioni della sicurezza, offrendo alle aziende maggiore tranquillità.

VANTAGGI

- Soluzione di sicurezza semplice e completa
- Protezione anti-virus e anti-spyware al gateway
- Servizio anti-spam completo
- Tecnologia IPS all'avanguardia
- Controllo e intelligence delle applicazioni
- Filtraggio DNS
- Filtraggio dei contenuti
- Supporto 24/7 con aggiornamenti firmware e sostituzione dell'hardware
- Gestione, reportistica e analisi avanzate basate sul cloud
- Sandbox di rete multi-engine con la brevettata tecnologia Real-Time Deep Memory Inspection (RTDMI™) di SonicWall
- Servizi firewall gestiti opzionali
- Garanzia informatica integrata, senza costi aggiuntivi



sonicwall.com

SONICWALL®

Caratteristiche e vantaggi

I servizi di protezione dalle minacce proteggono la rete da virus, intrusioni, botnet, spyware, trojan, worm e altri attacchi dannosi. Appena vengono identificate nuove minacce, e spesso prima che i produttori di software rilascino le patch corrispondenti, i firewall SonicWall e il database Capture Cloud vengono automaticamente aggiornati con nuove firme per garantire una protezione efficace dalle minacce. In questi firewall è integrato il brevettato motore RTDMI™, che analizza il traffico alla ricerca di svariati tipi di applicazioni e protocolli e garantisce una protezione totale, 24 ore su 24, da attacchi interni ed esterni e da vulnerabilità delle applicazioni.

Network Security Manager (NSM), una soluzione di gestione centralizzata dei firewall basata su cloud, offre una gestione semplificata e scalabile delle attività dei firewall, tra cui l'amministrazione multi-tenant. Le funzionalità di **reportistica e analisi avanzate** forniscono visibilità da un unico pannello di gestione e consentono di monitorare e scoprire le minacce unificando e correlando i log di tutti i firewall.

Il servizio **Capture ATP** rivoluziona i sistemi di rilevamento delle minacce avanzate e il sandboxing con una soluzione multi-engine basata sul cloud che blocca gli attacchi sconosciuti e zero-day a livello del gateway. Capture ATP blocca gli attacchi zero-day prima che entrino nella rete e consente di realizzare una protezione avanzata contro le minacce in continua evoluzione e di analizzare un'ampia gamma di tipi di file.

La protezione **anti-virus al gateway** combina l'anti-malware basato sulla rete e un database nel cloud aggiornato dinamicamente con decine di milioni di firme malware. La protezione anti-spyware dinamica blocca l'installazione di spyware dannosi e interrompe le comunicazioni spyware esistenti.

La **tecnologia IPS all'avanguardia** protegge da worm, trojan, vulnerabilità software e altre intrusioni mediante l'analisi di tutto il traffico di rete per rilevare pattern dannosi o anomali, aumentando così l'affidabilità e le prestazioni della rete.

Application Intelligence and Control è un insieme di policy granulari specifiche per applicazione che consente agli amministratori di controllare e gestire gli applicativi (aziendali e non) tramite la classificazione delle applicazioni e l'utilizzo di policy.

Comprehensive Anti-Spam Service offre alle PMI un'efficacia anti-spam superiore al 99%, bloccando più dell'80% dello spam a livello del gateway grazie a tecniche anti-spam avanzate come il filtraggio Adversarial Bayesian™ e basato sul machine learning.

Content Filtering Services (CFS) consente di applicare policy sull'uso di Internet e di controllare l'accesso interno a contenuti web inappropriati, improduttivi e potenzialmente illegali grazie al filtraggio completo dei contenuti. **CFS 5.0** basato sulla reputazione fornisce un punteggio di reputazione che prevede il rischio per la sicurezza di un URL in 93 categorie web.

Il **filtraggio DNS** blocca i siti web o le applicazioni malevoli a livello DNS per filtrare i contenuti dannosi o inappropriati, senza attivare la decrittazione TLS per non influire sulle prestazioni.

Gli **access point** ad alta sicurezza di SonicWall possono essere gestiti via cloud mediante lo strumento SonicWall Wireless Network Manager (WNM) di SonicWall Unified Management o tramite i firewall SonicWall, garantendo una gestione semplice e un'integrazione fluida con i prodotti wireless di SonicWall.

Network Access Control (NAC) consente ai clienti SonicWall di controllare gli accessi alla rete grazie all'integrazione con Aruba ClearPass, fornendo funzioni di profilazione, autenticazione e autorizzazione complete e precise per i sistemi e i dispositivi che tentano di accedere alle risorse IT. SonicOS offre un'API RESTful che supporta Aruba ClearPass come NAC per l'integrazione con i Next-Generation Firewall di SonicWall. Questa architettura trasforma la sicurezza statica in una sicurezza contestuale per garantire una protezione più flessibile e avanzata.

Il **supporto 24/7** con aggiornamenti firmware e sostituzione dell'hardware protegge l'azienda e l'investimento nella tecnologia SonicWall. Il supporto include l'accesso al supporto tecnico per telefono e via web, 24 ore su 24, per ottenere assistenza in fase di configurazione e nella risoluzione dei problemi nonché sostituzione dell'hardware in caso di guasto.

Managed Protection Security Suite (MPSS) semplifica ulteriormente la gestione dei firewall, delegandola al team SonicWall. Il nostro personale monitora i firewall dei clienti e li informa in caso di interruzioni o modifiche locali, oltre a gestire per loro tutti gli aggiornamenti del firmware in base alle loro scadenze. MPSS include una garanzia informatica da 200.000 dollari.

La **garanzia Cysurance incorporata**, offerta insieme ai servizi di sicurezza per mitigare i costi in caso di violazioni della sicurezza, soddisfa i requisiti di conformità e garantisce maggiore tranquillità.

FUNZIONALITÀ	ADVANCED PROTECTION SECURITY SUITE	MANAGED PROTECTION SECURITY SUITE
Supporto 24/7	●	●
IPS	●	●
Controllo delle applicazioni	●	●
Servizio di filtraggio dei contenuti	●	●
Anti-virus al gateway	●	●
Sicurezza DNS con filtraggio DNS avanzato**	●	●
Integrazione di Network Access Control (NAC) con Aruba ClearPass	●	●
Integrazione Wi-Fi 6	●	●
Deep Packet TLS/SSL per la decrittazione e l'ispezione	●	●
Identificazione del traffico in base al paese (GeoIP)	●	●
Servizio botnet	●	●
Servizio anti-spam completo	●	●
Sandbox Capture ATP (statica, RTDMI, memoria, hypervisor, emulazione)	●	●
Gestione NSM (cloud)	●	●
Reportistica e analisi avanzate (cloud)***	7 giorni inclusi	30 giorni inclusi
Gestione della configurazione del firewall		●
Supporto strategico oltre l'orario di lavoro		●
Garanzia integrata****	Fino a $ 100.000	Fino a $ 200.000

** Il filtraggio DNS non è supportato sulle interfacce WireMode
*** Reportistica e analisi possono essere estese a 30, 90 o 365 giorni.
**** Solo per i firewall venduti e registrati dopo il 1° novembre 2024

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.

sonicwall.com

SONICWALL®