Suite di servizi di protezione SonicWall

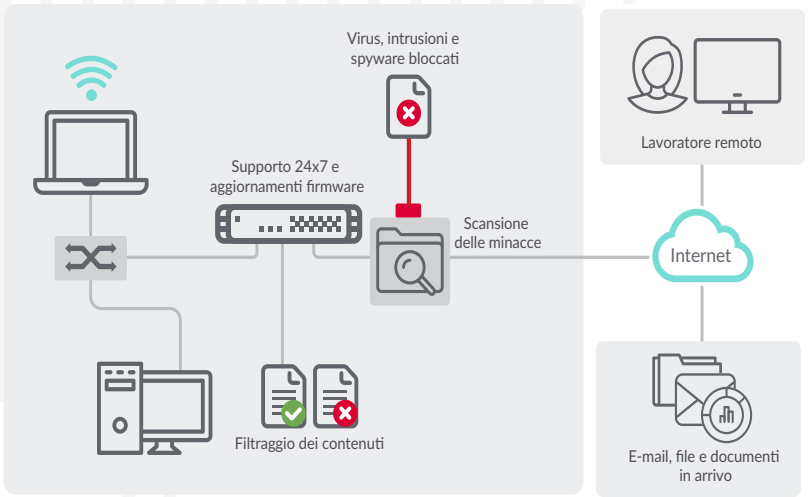
Gestione completa della sicurezza di rete e dei firewall in un unico pacchetto integrato

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 ha integrato un'ampia gamma di servizi di sicurezza di rete in alcuni convenienti pacchetti: Threat Protection Service Suite, Essential Protection Service Suite e Advanced Protection Service Suite.

VANTAGGI

- Soluzione di sicurezza completa per la rete
- Protezione anti-virus e anti-spyware al gateway con certificazione ICSA
- Gestione della sicurezza di rete basata su cloud
- Servizio anti-spam completo
- Tecnologia IPS all'avanguardia
- Controllo e intelligence delle applicazioni
- Sicurezza DNS
- Filtraggio dei contenuti
- Supporto 24x7 con aggiornamenti firmware e sostituzione dell'hardware
- Sandbox di rete multi-engine con la brevettata tecnologia Real-Time Deep Memory Inspection (RTDMI™) di SonicWall



ICSA labs CERTIFIED ENTERPRISE FIREWALL
ICSA labs CERTIFIED ANTI-VIRUS
ICSA labs CERTIFIED ADVANCED THREAT DEFENSE
ICSA labs CERTIFIED ANTI-MALWARE

SCHEDA TECNICA

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), un sistema centralizzato di gestione firewall multi-tenant basato su cloud, consente di gestire centralmente tutte le operazioni dei firewall senza errori applicando workflow verificabili. **Reporting e Analytics** offrono 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 soluzione di protezione **Gateway Anti-Virus** con certificazione ICSA 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.

Il servizio SonicWall **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 antispam 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. Il filtraggio 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 e in tal modo influire sulle prestazioni.

Gli **access point** altamente sicuri di SonicWall possono essere gestiti via cloud mediante SonicWall Wireless Network Manager (WNM) o tramite i firewall SonicWall, semplificando la gestione e l'integrazione senza soluzione di continuità con i prodotti wireless di SonicWall.

L'integrazione del **Network Access Control** (NAC) offre ai clienti SonicWall il controllo degli 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 firewall NGFW di SonicWall. Questa architettura trasforma la sicurezza statica in una sicurezza contestuale per garantire una protezione più flessibile e avanzata.

Il **supporto 24x7** 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.

FUNZIONALITÀ	THREAT PROTECTION SECURITY SUITE*	ESSENTIAL PROTECTION SECURITY SUITE	ADVANCED PROTECTION SECURITY SUITE
Supporto 24x7	Sì	Sì	Sì
IPS	Sì	Sì	Sì
Controllo delle applicazioni	Sì	Sì	Sì
Servizio di filtraggio dei contenuti	Sì	Sì	Sì
Gateway Anti-Virus	Sì	Sì	Sì
Sicurezza DNS di base	Sì	Sì	Sì
Filtraggio DNS	No	No	Sì
Integrazione del Network Access Control (NAC) con Aruba ClearPass	Sì	Sì	Sì
Integrazione Wi-Fi 6	Sì	Sì	Sì
Deep Packet Inspection per SSL	Sì	Sì	Sì
Aggiornamenti GeoIP	Sì	Sì	Sì
Servizio botnet	Sì	Sì	Sì
Servizio anti-spam completo	No	Sì	Sì
Capture ATP - Sandbox (statico, RTDMI, memoria, hypervisor, emulazione)	No	Sì	Sì
Gestione NSM (cloud)	No	No	Sì
Reporting NSM (cloud) - conservazione per 7 giorni	No	No	Sì

* Disponibile solo su TZ 270, 370 e 470

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e trasparenti per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

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

© 2022 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.