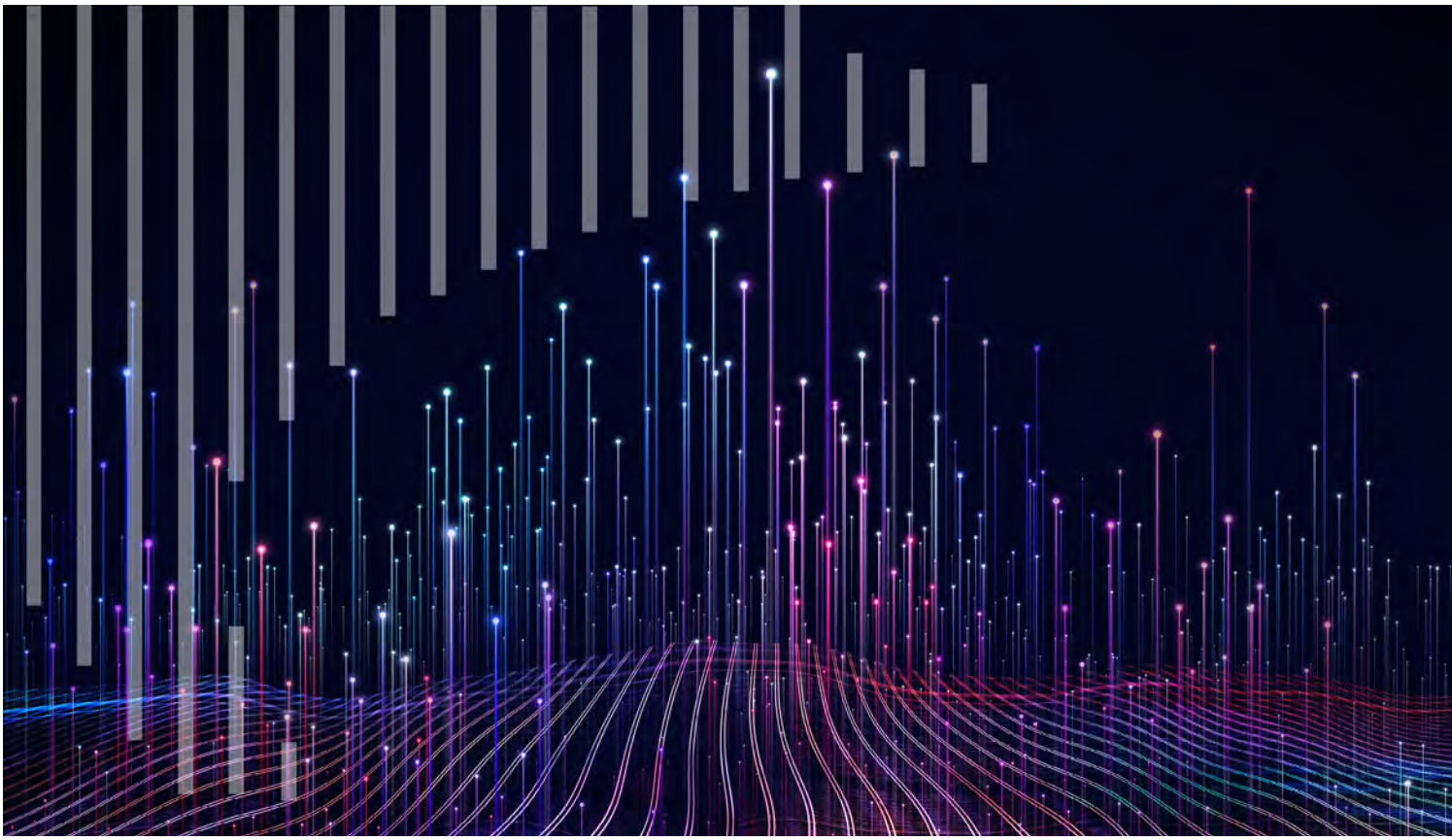
Linee di prodotti SonicWall

Giugno 2022



Introduzione

Per un'azienda è fondamentale proteggere il proprio cloud pubblico/privato, le applicazioni, gli utenti e i dati in maniera approfondita senza compromettere le prestazioni della rete. La piattaforma Capture Cloud di SonicWall integra i servizi di sicurezza, gestione, analisi e intelligence delle minacce in tempo reale della gamma di prodotti SonicWall dedicati alla protezione di reti, connessioni wireless, e-mail, dispositivi mobili, web e cloud. Questo approccio consente a piccole e medie imprese, grandi aziende, enti pubblici, punti vendita al dettaglio, istituti accademici, aziende sanitarie e service provider di usufruire del nostro ecosistema di sicurezza completo che sfrutta la potenza, l'agilità e la scalabilità del cloud.

La strategia e la visione del futuro della piattaforma Capture Cloud puntano all'innovazione e allo sviluppo continui di applicazioni di sicurezza as-a-service containerizzate che siano facili da programmare e da distribuire on-demand. La piattaforma è composta dai componenti e dalle funzionalità seguenti:

- Sicurezza di rete
- Sicurezza in LAN
- Sicurezza wireless
- Sicurezza degli endpoint
- Accelerazione WAN
- Servizi di sicurezza avanzati
- Sicurezza delle applicazioni cloud
- Accesso sicuro al cloud edge
- Accesso mobile sicuro
- Protezione delle e-mail
- Gestione, reportistica e analisi
- Servizi professionali e supporto Enterprise

La combinazione di queste caratteristiche fornisce una difesa informatica multilivello fondamentale, intelligence delle minacce, analisi, collaborazione e funzionalità comuni di gestione, reportistica e analisi che interagiscono in modo sincronizzato.

Sicurezza di rete

SonicWall è uno dei fornitori leader di firewall di nuova generazione (NGFW). Tutti i firewall NGFW di SonicWall sono basati sul firmware SonicOS o SonicOSX, che utilizza un'architettura hardware scalabile abbinata ai nostri motori Real-Time Deep Memory Inspection (RTDMI™) in attesa di brevetto e Reassembly-Free Deep Packet Inspection® (RFDPI) single-pass brevettato* a latenza ridotta per ispezionare tutto il traffico, indipendentemente dalla porta o dal protocollo.

I firewall NGFW di SonicWall analizzano ogni singolo byte di ogni pacchetto, pur mantenendo le prestazioni elevate e la bassa latenza richiesti dalle reti a carico di lavoro elevato. Diversamente dai prodotti della concorrenza, il motore RFDPI single-pass consente la scansione simultanea delle applicazioni alla ricerca di minacce e l'analisi di file di qualsiasi dimensione senza il riassemblaggio dei pacchetti. In questo modo, i firewall SonicWall di nuova generazione risultano altamente scalabili e consentono di estendere le funzioni di sicurezza avanzate a reti aziendali distribuite e in crescita e a data center.

I firewall SonicWall di nuova generazione offrono un'ampia gamma di potenti funzionalità, tra cui:

- Sandbox Capture ATP multi-engine basata sul cloud
- SD-WAN
- API REST
- Decrittazione e ispezione del traffico crittografato
- Servizio di prevenzione delle intrusioni (IPS)
- Protezione dal malware
- Controllo, intelligence e visualizzazione in tempo reale delle applicazioni
- Filtraggio di siti web/URL (filtro dei contenuti)
- VPN (Virtual Private Networking) tramite SSL o IPSec
- Sicurezza wireless
- Sicurezza per ambienti ibridi e multi-cloud
- Stateful failover/failback

Inoltre, i firewall SonicWall offrono una risposta rapida e protezione continua contro le minacce zero-day grazie ai dati forniti dal team di ricerca delle minacce Capture Labs. Questo team dedicato raccoglie, analizza ed esamina informazioni sulle minacce multivettoriali provenienti da svariate fonti di intelligence delle minacce, tra cui il Capture Threat Network di SonicWall che include oltre un milione di sensori in tutto il mondo.

Serie SonicWall Network Security services platform (NS*sp*)

La piattaforma firewall di nuova generazione della serie SonicWall NS*sp* è progettata per fornire scalabilità, affidabilità e sicurezza elevata a velocità multi-gigabit per reti di grandi dimensioni.

ICSA Labs ha testato i firewall SonicWall e rilevato che offrono un'eccellente efficacia della sicurezza, con un tasso di rilevamento del 100% e nessun falso positivo negli ultimi cinque trimestri consecutivi. I firewall SonicWall definiscono nuovi standard per il controllo delle applicazioni ad alte prestazioni e la prevenzione delle minacce in vari scenari d'implementazione, dalle piccole aziende a grandi data center, operatori e fornitori di servizi.

Ad esempio, il nostro firewall multi-istanza di fascia alta NS*sp* garantisce un elevato livello di qualità del servizio, offrendo la disponibilità e la connettività di rete senza interruzioni necessarie alle moderne imprese, agli enti pubblici, ai fornitori di servizi e alle università con infrastrutture a 100/40/10 Gb/s. Grazie alle innovative tecnologie di sicurezza basate sul deep learning della piattaforma SonicWall Capture Cloud, la serie NS*sp* offre una protezione efficace contro le minacce più avanzate senza rallentare le prestazioni.

Policy unificate con SonicOSX 7

La funzione di gestione unificata delle policy di SonicOSX 7 consente la gestione integrata delle policy di accesso e sicurezza per determinati firewall SonicWall di fascia alta della serie NS*sp* e per i firewall virtuali NS*v*.

La nuova interfaccia web è stata progettata con un approccio completamente diverso, che mette l'utente in primo piano e consente una configurazione più intuitiva di policy di sicurezza contestuali tramite avvisi impostabili e un utilizzo semplice e immediato.

L'interfaccia ha un design più accattivante rispetto alla versione classica. Attraverso una console di controllo sul firewall, l'interfaccia presenta all'utente informazioni sull'efficacia delle varie regole di sicurezza e consente di modificare le regole predefinite per gateway anti-virus, anti-spyware, filtraggio dei contenuti, prevenzione delle intrusioni, filtraggio degli IP in base alla posizione geografica e ispezione approfondita dei pacchetti del traffico crittografato con la massima trasparenza.

Con questa nuova interfaccia di gestione unificata delle policy, SonicWall semplifica e riduce il tempo necessario per controllare le variazioni del traffico dinamico, a tutto vantaggio della sicurezza generale.

*Brevetti USA 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Serie SonicWall Network Security appliance (NS*a*)

La serie Network Security appliance (NS*a*) di SonicWall è una delle linee di firewall di nuova generazione più sicure e performanti della sua categoria. Offre funzionalità di sicurezza di fascia alta senza compromettere le prestazioni, utilizzando la stessa architettura dei nostri firewall NGFW di punta della serie NS*sp*, sviluppati per le reti aziendali più complesse al mondo.

Basata su anni di ricerca e sviluppo, la serie NS*a* è appositamente concepita per le esigenze di aziende distribuite, imprese di medie dimensioni, filiali aziendali, campus universitari ed enti pubblici. La serie NS*a* combina una rivoluzionaria architettura multi-core con la tecnologia Real-Time Deep Memory Inspection (RTDMI) basata su cloud, un brevettato motore di prevenzione delle minacce ad altissima scalabilità. Questa combinazione offre livelli di protezione, prestazioni e scalabilità leader del settore, numerose connessioni simultanee, bassa latenza, nessun limite per le dimensioni dei file e un numero di connessioni al secondo maggiore rispetto ai principali produttori di firewall.

Serie SonicWall TZ

La serie TZ di SonicWall è composta da firewall UTM (Unified Threat Management) estremamente affidabili e sicuri, progettati per PMI, punti vendita al dettaglio, pubblica amministrazione e aziende distribuite con uffici remoti e filiali. A differenza dei prodotti di livello consumer, la serie TZ consolida potenti funzioni di protezione dal malware, prevenzione delle intrusioni, filtraggio di contenuti/URL e controllo delle applicazioni in reti cablate e wireless, nonché un ampio supporto di piattaforme mobili per notebook, smartphone e tablet. Fornisce inoltre la tecnologia DPI (Deep Packet Inspection) ad altissime prestazioni, eliminando i colli di bottiglia della rete causati da altri prodotti e consentendo alle aziende di migliorare la produttività.

Come tutti i firewall SonicWall, anche i firewall della serie TZ esaminano i file nella loro interezza, compresi quelli crittografati tramite TLS/SSL, per assicurare una protezione a tutto campo. La serie TZ offre inoltre funzionalità di controllo e intelligence delle applicazioni, analisi avanzata e report sul traffico delle applicazioni, IPsec (Internet Protocol Security) e VPN SSL, failover ISP multiplo, bilanciamento del carico e SD-WAN. L'alimentazione Power over Ethernet (PoE) e la connettività wireless 802.11ac ad alta velocità integrate opzionali consentono alle aziende di estendere i confini delle proprie reti in modo semplice e sicuro. In combinazione con gli switch SonicWall, i firewall della serie TZ offrono tutta la flessibilità necessaria per far crescere l'azienda grazie all'implementazione zero-touch, senza aggiungere complessità.

I firewall di nuova generazione della serie TZ sono i primi in formato desktop dotati di interfacce multi-gigabit (2,5/5/10 Gb), Secure SD-WAN, memoria integrata ed espandibile, supporto TLS 1.3 e predisposizione 5G, il tutto con eccellenti prestazioni. Ulteriori caratteristiche di questi dispositivi sono gli alimentatori ridondanti e il supporto per 802.11ac Wave 2. Progettati per aziende di medie dimensioni e imprese distribuite con sedi SD-Branch, i firewall di nuova generazione della serie TZ si distinguono per l'efficacia della sicurezza riconosciuta nel settore e per il miglior rapporto qualità-prezzo in assoluto.

Serie SonicWall Network Security virtual (NS*v*)

I firewall SonicWall della serie Network Security virtual (NS*v*) estendono la prevenzione e il rilevamento automatizzati delle violazioni ad ambienti ibridi e multi-cloud con versioni virtualizzate dei firewall SonicWall di nuova generazione. Dotati di strumenti e servizi di sicurezza equivalenti a quelli di un firewall SonicWall fisico, i firewall NSv proteggono in modo efficace gli ambienti virtuali e cloud da attacchi che implicano un uso illecito delle risorse, attacchi tra macchine virtuali o su canale laterale e tutte le comuni minacce ed exploit basati sulla rete.

I firewall NS*v* possono essere facilmente installati e configurati in un ambiente multi-tenant virtuale, in genere tra reti virtuali. Questi firewall applicano misure di controllo degli accessi per preservare la sicurezza dei dati e delle macchine virtuali e analizzano il traffico virtuale tra macchine e reti virtuali, garantendo una prevenzione automatica delle violazioni.

Grazie al supporto per implementazioni ad alta disponibilità (HA), la serie NS*v* soddisfa i requisiti di scalabilità e disponibilità dei software-defined data center (SDDC). Semplice installazione come appliance virtuale in piattaforme cloud private come VMWare ESXi, Linux KVM, Nutanix o Microsoft Hyper-V, oppure in ambienti cloud pubblici AWS o Microsoft Azure. I firewall della serie NS*v*, disponibili con i modelli di licenza flessibili BYOL e PAYG, offrono alle aziende tutte le caratteristiche di sicurezza di un firewall fisico combinate ai vantaggi operativi ed economici di una soluzione virtuale.

Alcuni modelli di firewall NS*v* sono dotati del sistema operativo SonicOSX con la funzione Unified Policy, che consente di controllare le modifiche del traffico dinamico in modo più semplice e rapido, garantendo un migliore livello di sicurezza generale.

Per maggiori informazioni sui prodotti firewall SonicWall: www.sonicwall.com/products/firewalls/

Capture Security appliance 1000 (CSa 1000)

Per rispettare le normative in materia di privacy, le aziende hanno bisogno di una piattaforma di analisi delle minacce a un prezzo accessibile e in grado di rilevare e bloccare il codice dannoso. SonicWall Capture Security appliance (CS*a*) è una soluzione di analisi dei file e rilevamento del malware on-premise con tecnologia Real-Time Deep Memory Inspection (RTDMI) di SonicWall. RTDMI consente alla soluzione CS*a* di rilevare più malware, in modo più veloce ed efficace. La sua bassa percentuale di falsi positivi migliora la sicurezza e l'esperienza d'uso per gli utenti finali.

CS*a* consente di analizzare il malware nascosto in svariate tipologie di file di varie dimensioni e ambienti operativi, garantendo un rilevamento completo delle minacce zero-day. Grazie all'ispezione in tempo reale basata sulla memoria, rileva e blocca gli attacchi su canale laterale. Inoltre, forzando il malware a rivelare la sua presenza in memoria, CS*a* blocca in modo proattivo minacce di massa, zero-day e sconosciute. CS*a* supporta le reti chiuse e può essere utilizzata con i più recenti firewall SonicWall di nuova generazione.

L'installazione di SonicWall CS*a* avviene in modo semplice e rapido: basta configurare la rete di base, la creazione di report e l'accesso ai dispositivi consentiti per iniziare a utilizzarla. CS*a* è progettata per essere raggiungibile tramite l'indirizzo IP e può quindi essere implementata ovunque, a condizione che sia raggiungibile dai dispositivi che dovranno inviare i file da analizzare. CS*a* può anche essere installata in reti chiuse o air gap.

Sicurezza in LAN

Gli switch SonicWall offrono la commutazione di rete ad alta velocità con prestazioni e facilità di gestione senza precedenti. Presentano un numero elevato di porte, alimentazione Power over Ethernet (PoE) opzionale e throughput a 1 o 10 gigabit. Ideali per le PMI e le reti SD-Branch (Software-Defined Branch), consentono alle aziende di qualsiasi dimensione di affrontare la trasformazione digitale e restare al passo con i cambiamenti nel mondo del networking e della sicurezza.

Gli switch SonicWall possono essere gestiti tramite i firewall SonicWall o la piattaforma Wireless Network Manager (WNM), che integra soluzioni di sicurezza cablate e wireless end-to-end garantendo una protezione unificata. Questo semplifica l'implementazione, la gestione e la risoluzione dei problemi ed elimina eventuali problemi con switch di terze parti. Gli switch SonicWall possono essere installati rapidamente in filiali distribuite utilizzando l'implementazione zero-touch.

Sicurezza wireless

L'innovativa soluzione SonicWall Wireless Network Security rende le reti wireless più sicure, semplici e convenienti. Gli access point wireless ad alte prestazioni della serie SonicWave 802.11ax sono facilmente gestibili tramite Wireless Network Manager.

Oltre agli access point wireless ad alta velocità e al pannello di controllo gestito in cloud, la soluzione di sicurezza wireless di SonicWall comprende Wi-Fi Planner, uno strumento avanzato di indagine dei siti che aiuta gli amministratori a pianificare e installare le reti Wi-Fi in modo efficace. La soluzione include anche l'app per dispositivi mobili SonicExpress, che semplifica l'inserimento e il monitoraggio degli access point fornendo agli amministratori informazioni in tempo reale sullo stato e la sicurezza della rete.

La nostra soluzione offre molto più di un semplice sistema di sicurezza wireless, proteggendo le reti wireless con le tecnologie RTDMI e RFDPI, e dispone di funzioni di sicurezza avanzate come sandboxing multi-engine, filtraggio dei contenuti e anti-virus cloud direttamente presso l'access point, senza dover ricorrere a un firewall. Consente inoltre di migliorare ulteriormente la sicurezza e le prestazioni della rete con funzioni come la prevenzione delle intrusioni, la decrittazione e ispezione TLS/SSL e il controllo delle applicazioni, garantendo prestazioni e protezione di livello aziendale.

Gli access point SonicWave supportano il fast roaming, che consente agli utenti di spostarsi agevolmente da un luogo all'altro senza perdere la connessione. L'ampia gamma di funzioni comprende captive portal, selezione automatica del canale, analisi dello spettro, air-time fairness, band steering e strumenti di analisi del segnale per il monitoraggio e la risoluzione di problemi.

SonicWall consente di ridurre il costo totale di proprietà (TCO), in quanto gli amministratori non devono più implementare e gestire separatamente una costosa soluzione ad hoc per la rete wireless in parallelo alla rete cablata esistente.

Sicurezza degli endpoint

La gestione e la sicurezza degli endpoint sono di fondamentale importanza nel contesto aziendale attuale. Con utenti che entrano ed escono dalla rete con i loro dispositivi e minacce crittografate in grado di raggiungere inosservate gli endpoint, occorre fare qualcosa per proteggere questi dispositivi. L'aumento dei ransomware e le vulnerabilità delle applicazioni hanno trasformato gli endpoint nel campo di battaglia delle odierne minacce.

Inoltre, gli amministratori faticano a mantenere visibilità e a gestire le proprie infrastrutture di sicurezza. Oltre a ciò devono garantire la sicurezza costante dei client e la disponibilità di funzioni di intelligence e reportistica pratiche e semplici da utilizzare.

I prodotti per la sicurezza degli endpoint sono presenti sul mercato da anni, ma gli amministratori hanno difficoltà a:

- mantenere aggiornati i prodotti per la sicurezza
- applicare le policy a livello globale
- creare report e monitorare lo stato dei tenant
- bloccare le minacce provenienti da canali crittografati
- capire gli avvisi e le procedure di risoluzione
- catalogare le applicazioni e le loro vulnerabilità
- bloccare minacce come il ransomware
- rilevare attacchi fileless e dispositivi USB infetti che aggirano le difese perimetrali

SonicWall Capture Client è una piattaforma client unificata con varie funzioni di sicurezza per gli endpoint. Questa soluzione offre un'esperienza di sicurezza unificata ai clienti SonicWall grazie alla console di gestione basata sul cloud e all'integrazione completa opzionale con i firewall SonicWall di nuova generazione. Grazie a funzionalità di applicazione dei criteri, SonicWall Capture Client può verificare che negli endpoint sia in esecuzione un software di sicurezza e/o sia incorporato un certificato SSL per l'ispezione del traffico crittografato. Per rendere l'ispezione del traffico SSL (DPI-SSL) più semplice e offrire un'esperienza migliore agli utenti finali, Capture Client consente agli amministratori di inviare i certificati SSL agli endpoint con maggiore facilità.

Capture Client dispone inoltre di un motore antivirus avanzato per bloccare il malware più evoluto, con un'opzione di rollback per ripristinare lo stato precedente l'infezione. Capture Client Advanced si integra con SonicWall Capture Advanced Threat Protection (ATP) per esaminare i file sospetti e bloccare gli attacchi prima che vengano attivati.

Gli amministratori possono ora catalogare tutte le applicazioni presenti su ciascun endpoint protetto da Capture Client, creando report sulle vulnerabilità note all'interno dell'ecosistema.

La dashboard unificata è stata progettata per visualizzare il numero di infezioni, le vulnerabilità presenti e la

versione di Capture Client installata in ogni tenant. Consente di vedere cosa e chi viene bloccato più frequentemente dal filtraggio dei contenuti e quali dispositivi sono online e operativi. Il sistema di policy globali consente agli amministratori di applicare un'unica policy di base per tutti i tenant. In questo modo è più semplice configurare nuovi tenant e creare protezioni contro le nuove minacce per tutti i tenant inclusi in questa policy.

SonicWall Capture Client include le seguenti funzionalità:

- Applicazione dei criteri di sicurezza
- Gestione dei certificati DPI-SSL
- Monitoraggio continuo del comportamento
- Determinazione accurata grazie al machine learning
- Tecniche multilivello basate su metodi euristici
- Intelligence delle vulnerabilità delle applicazioni
- Capacità di ripristino esclusive
- Integrazione con la sandbox di rete Capture Advanced Threat Protection
- Dashboard globale e policy globali con opzioni di ereditarietà
- Verifica dei file sospetti (con un semplice clic) a fronte del database di Capture ATP, che contiene informazioni su minacce accertate e presunte
- Filtraggio dei contenuti per applicare policy web e bloccare indirizzi IP, URL e domini dannosi su dispositivi fuori dalla rete
- Controllo dei dispositivi basato su policy per bloccare dispositivi di archiviazione potenzialmente infetti

Servizi di sicurezza avanzati

I servizi firewall SonicWall per la sicurezza di rete offrono una protezione avanzata e altamente efficace per aiutare le aziende di ogni dimensione a difendersi dalle minacce, ottenere un maggiore controllo della sicurezza, migliorare la produttività e ridurre i costi.

SonicWall propone tre pacchetti di abbonamento per i firewall della serie Gen 7: Threat Protection Services Suite, Essential Protection Services Suite e Advanced Protection Services Suite. Threat Protection Service Suite comprende i servizi di sicurezza di base necessari per garantire la protezione della rete dalle minacce, il tutto in un unico e conveniente pacchetto. Il pacchetto SonicWall Essential offre i servizi di sicurezza essenziali per proteggersi da minacce note e sconosciute, mentre la versione Advanced offre una protezione avanzata della rete con l'aggiunta di servizi di sicurezza essenziali per il cloud.

Threat Protection Services Suite, disponibile solo per le serie TZ270/370/470, comprende anti-virus sul gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio dei contenuti, ispezione profonda dei pacchetti del traffico TLS/SSL crittografato (DPI-SSL) e supporto 24x7.

Essential Protection Services Suite comprende Capture Advanced Threat Protection con tecnologia RTDMI, anti-virus sul gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio dei contenuti, servizio anti-spam completo, ispezione profonda dei pacchetti del traffico TLS/SSL crittografato (DPI-SSL) e supporto 24x7.

Advanced Protection Services Suite comprende Capture Advanced Threat Protection con tecnologia RTDMI, anti-virus sul gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio dei contenuti, servizio anti-spam completo, ispezione profonda dei pacchetti del traffico TLS/SSL crittografato (DPI-SSL), supporto 24x7, gestione cloud, reportistica basata sul cloud per 7 giorni e supporto Premier opzionale.

Analisi approfondita della memoria

SonicWall RTDMI (Real-Time Deep Memory Inspection), una tecnologia in attesa di brevetto, individua e blocca proattivamente il malware sconosciuto tramite l'ispezione approfondita della memoria in tempo reale. Ora disponibile con Capture Advanced Threat Protection (ATP), il servizio di sandboxing nel cloud di SonicWall, questo motore identifica e mitiga le attuali minacce anche più insidiose, tra cui i futuri exploit Meltdown.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Sicurezza delle applicazioni cloud

La soluzione SonicWall Cloud App Security protegge le più comuni applicazioni SaaS di posta elettronica, collaborazione e produttività come Office 365 email, SharePoint, OneDrive, G-Suite, Dropbox e Box. Offre protezione dalle minacce seguenti:

- Compromissione delle email aziendali (BEC)
- Prevenzione della perdita di dati (DLP)
- Acquisizione degli account (ATO)
- Malware avanzato e minacce zero-day in allegati dannosi e file di archivio
- Phishing mirato
- Tentativi di frode

Cloud App Security utilizza la profilazione e analisi avanzate del comportamento degli utenti, con oltre 300 indicatori di minaccia, per stabilire se gli account legittimi vengono sfruttati dai cybercriminali. La soluzione utilizza funzionalità di machine learning a AI per bloccare gli attacchi di impersonificazione e include la scansione retroattiva delle attività.

Per le applicazioni SaaS e di condivisione file come OneDrive, Cloud App Security applica i meccanismi multi-sandbox di SonicWall Capture ATP per rilevare malware mai visti prima. Effettua scansioni storiche in tempo reale di file e dati, residenti o in transito in un ambiente SaaS, a livello interno o da cloud a cloud. Inoltre, la funzionalità DLP della soluzione protegge i dati archiviati, limitando l'accesso alle sole applicazioni approvate e impedendo il caricamento di dati non autorizzati.

Trattandosi di un servizio SaaS, Cloud App Security è attivabile e operativa in pochi minuti. Grazie alla scalabilità illimitata, la soluzione consente ad aziende di qualsiasi dimensione di applicare immediatamente la protezione per gli utenti delle applicazioni SaaS, indipendentemente che si tratti di poche centinaia o di centinaia di migliaia di utenti distribuiti in tutto il mondo. Ogni applicazione SaaS dispone di un sistema di gestione delle policy separato, con regole e funzioni di attivazione specifiche. In questo modo è possibile assegnare policy specifiche ad ogni applicazione SaaS in base ai propri requisiti di sicurezza.

Cloud App Security non richiede l'installazione o la gestione di hardware e software, eliminando così le spese in conto capitale, le complessità d'installazione e i costi di manutenzione periodica associati a soluzioni alternative installate in loco.

Per maggiori informazioni su SonicWall Cloud App Security: www.sonicwall.com/cloud-security

Accesso sicuro al cloud edge

L'evoluzione della VPN tradizionale nella sicurezza Zero-Trust

Oggi i dipendenti desiderano la flessibilità di lavorare da qualsiasi luogo, mentre le aziende vogliono sfruttare le efficienze operative e i risparmi sui costi offerti dal cloud.

Ma le soluzioni VPN tradizionali non sono state create per questa nuova realtà. La loro installazione può richiedere giorni o addirittura settimane, inoltre occorre prevedere eventuali problemi di disponibilità e la difficoltà di programmare i tempi di fermo.

Ancor peggio, una VPN può creare backdoor per potenziali violazioni, perché consente a qualsiasi utente collegato l'accesso ad ampie sezioni della rete e un movimento laterale all'interno della sottorete.

Infine, una VPN induce una latenza aggiuntiva che peggiora l'esperienza degli utenti nel cloud, perché il traffico passa attraverso il concentratore VPN installato in sede anziché andare direttamente nel cloud.

Gartner prevede che entro il 2023 il 60% delle imprese eliminerà gradualmente la maggior parte delle reti private virtuali (VPN) ad accesso remoto per passare a soluzioni di accesso alla rete zero-trust (ZTNA).

La sicurezza di rete Zero-Trust protegge le risorse ad alto valore

Cloud Edge Secure Access di SonicWall è una soluzione ZTNA che risolve questi problemi, offrendo numerosi altri vantaggi. Cloud Edge Secure Access si basa su tre funzionalità essenziali:

- Accesso con privilegio minimo per proteggere le risorse aziendali
- Installazione rapida in modalità self-service
- Accesso diretto e affidabile al cloud da qualsiasi luogo

Essendo un servizio nativo per il cloud, offre un semplice servizio NaaS (Network-as-a-Service) per la connettività site-to-site e in cloud ibrido, con protezione Zero-Trust integrata e sicurezza basata sul privilegio minimo.

- Device Posture Check (DPC) concede l'accesso alla rete solo ai dispositivi autenticati e conformi
- Le policy di microsegmentazione software-defined prevengono la diffusione di violazioni
- Network Traffic Control (NTC) è un firewall-as-a-service (FwaaS) stateful che offre protezione basata su policy che definiscono chi può accedere a quali risorse e da dove

Le aziende possono così abilitare il lavoro da remoto, proteggendo allo stesso tempo le risorse aziendali ad alto valore.

Un servizio cloud-native configurabile in tutto il mondo in pochi minuti

SonicWall Cloud Edge è supportato da oltre 30 punti di presenza (PoP) globali.

Questo servizio globale consente ai responsabili IT di connettere una filiale e implementare il servizio in 15 minuti. Gli utenti finali possono installare il client SonicWall Cloud Edge ed essere operativi in soli 5 minuti.

L'infrastruttura è basata sull'architettura SDP (Software-Defined Perimeter), che separa il controller centralizzato dai gateway, che fungono da "garanti dell'affidabilità".

Mediante la distribuzione dei gateway SDP, Cloud Edge Secure Access può essere rapidamente ampliato, mantenendo prestazioni elevate e offrendo un'esperienza ottimale nel cloud.

Inoltre, la separazione delle funzioni rende Cloud Edge Secure Access inattaccabile da cyber minacce comuni come attacchi DDos, exploit Log4j, dirottamento su Wi-Fi pubblico, SYN flood e Slowloris.

Ulteriori vantaggi:

- Soluzione di sicurezza per imprese distribuite e forza lavoro remota
- Accesso sicuro istantaneo a siti fisici e risorse su cloud ibridi
- Scalabilità da decine a migliaia di utenti
- Accesso web senza client con qualsiasi dispositivo pubblico
- Crittografia WireGuard ad alte prestazioni
- Integrazione con Cloud Identity Provider e SIEM
- Integrazione con i moderni servizi SSO e MFA
- Integrazione SIEM
- Multi-tenancy per gli MSSP
- Network Traffic Control (NTC) consente la protezione a livello di firewall definendo chi (e da dove) può accedere a reti e servizi specifici.
- Device Posture Check (DPC) concede l'accesso alla rete solo ai dispositivi autenticati e conformi.
- Servizio disponibile negli USA, in Europa, Medio Oriente e Asia

Per maggiori informazioni su SonicWall Cloud Edge Secure Access: www.sonicwall.com/products/cloud-edge-secure-access

Accesso mobile sicuro

SonicWall Secure Mobile Access (SMA) è il gateway di accesso sicuro unificato

per le aziende che si trovano ad affrontare le sfide poste dalla mobilità, dallo smart working, dal BYOD e dalla migrazione nel cloud. La soluzione consente alle aziende di fornire l'accesso a risorse aziendali mission-critical in qualunque luogo e momento e su qualunque dispositivo. Il sistema di controllo granulare degli accessi di SMA, l'autorizzazione dei dispositivi in base al contesto, la VPN a livello di applicazione e l'autenticazione avanzata con Single Sign-on consentono alle aziende di adottare il BYOD (Bring Your Own Device) e la mobilità in un ambiente IT ibrido.

Inoltre, SMA riduce la superficie esposta alle minacce mediante funzionalità come Geo IP e Botnet Detection, Web Application Firewall e l'integrazione con la sandbox Capture ATP.

Mobilità e BYOD

Per le aziende che desiderano adottare il BYOD, la flessibilità sul lavoro o servizi di sviluppo offshore, SMA diventa il punto di implementazione centrale per tutti questi aspetti. SMA offre la migliore sicurezza nel settore per ridurre al minimo le minacce in superficie, rendendo più sicure le aziende grazie al supporto dei più recenti algoritmi di crittografia e cifrari. SMA di SonicWall consente agli amministratori di fornire un accesso mobile sicuro e privilegi basati sui ruoli in modo che gli utenti finali possano accedere in maniera semplice e veloce alle applicazioni, ai dati e alle risorse aziendali di cui hanno bisogno. Allo stesso tempo, le aziende possono definire criteri di BYOD sicuro per proteggere le proprie reti e i dati aziendali da accessi non autorizzati e dal malware.

Il passaggio al cloud

Per le aziende che si apprestano a compiere la migrazione verso il cloud, SMA offre un'infrastruttura Single Sign-on (SSO) che utilizza un unico portale Web per autenticare gli utenti in un ambiente IT ibrido. L'esperienza di accesso è fluida e coerente, indipendentemente dal fatto che la risorsa aziendale si trovi in sede, nel Web o in un cloud in hosting. Gli utenti non devono ricordarsi gli URL di ogni singola applicazione o conservare segnalibri dettagliati. Attraverso il portale di accesso centralizzato WorkPlace, gli utenti ricevono un URL per accedere a tutte le applicazioni fondamentali da un browser web standard. SMA fornisce l'autenticazione SSO federata sia per applicazioni SaaS in hosting nel cloud che utilizzano SAML 2.0 sia per applicazioni in hosting nel campus che utilizzano RADIUS o Kerberos. SMA si integra con diversi server di autenticazione, autorizzazione ed accounting e tecnologie di autenticazione multifattore (MFA) leader del settore per garantire una maggiore sicurezza. L'accesso SSO sicuro viene fornito solo ai dispositivi endpoint autorizzati dopo averne verificato l'integrità e la conformità.

Fornitori di servizi gestiti

SMA è una soluzione chiavi in mano che offre un elevato grado di continuità e scalabilità aziendale sia alle aziende con data center propri che ai provider di servizi gestiti. SMA di SonicWall è in grado di supportare fino a 20.000 connessioni simultanee su una singola appliance, con una scalabilità verticale fino a un milione di utenti tramite un clustering intelligente. Inoltre è possibile ridurre i costi con il clustering attivo/attivo ad alta disponibilità (Global High Availability) e con il bilanciatore di carico dinamico integrato (Global Traffic Optimizer), che permette di riallocare il traffico globale verso il data center più ottimizzato in tempo reale e in base alle esigenze degli utenti. SMA offre ai gestori di servizi una serie di strumenti per fornire un servizio senza tempi di inattività, permettendo loro di soddisfare accordi SLA (Service Level Agreement) anche molto stringenti.

Appliance SMA

SonicWall SMA può essere installato come dispositivo potenziato ad alte prestazioni o come appliance virtuale, sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. I dispositivi hardware sono basati su un'architettura multi-core ad elevate prestazioni che offre accelerazione SSL, throughput VPN e potenti proxy per garantire un accesso sicuro e affidabile. Per le organizzazioni regolamentate e federali, SMA è disponibile con certificazione FIPS 140-2 Level 2. Le appliance virtuali SMA offrono le stesse caratteristiche avanzate di accesso sicuro delle principali piattaforme virtuali e cloud come Hyper-V, VMWare ESX/ ESXi, KVM, AWS e Azure. Indipendentemente dalla soluzione adottata – dispositivo hardware, appliance virtuale o una combinazione di entrambi –, la serie SMA si adatta perfettamente all'infrastruttura IT esistente.

Web Application Firewall SMA

Il firewall WAF (Web Application Firewall) della serie SonicWall SMA100 consente di adottare una strategia di difesa approfondita aumentando la sicurezza perimetrale, in modo da proteggere le applicazioni web presenti in un ambiente cloud privato, pubblico o ibrido. Il firewall WAF della serie SMA100 protegge le applicazioni web, previene la divulgazione delle informazioni e accelera la distribuzione delle applicazioni, garantendo un bilanciamento del carico in funzione delle applicazioni, l'offloading SSL e un livello superiore di coinvolgimento ed esperienza digitale.

Ulteriori vantaggi:

- Protezione da vulnerabilità note e zero-day con patch virtuali e regole personalizzate
- Difesa dalle vulnerabilità e minacce più recenti individuate da OWASP, compresi l'iniezione SQL e lo scripting cross-site (XSS)

- Accesso Zero-Trust clientless tramite browser web per un comodo utilizzo con qualsiasi dispositivo pubblico.
- Stringenti requisiti di gestione delle sessioni e di autenticazione come OTP, 2FA e SSO
- Protezione dell'elevata disponibilità dei server da attacchi DoS/DDoS

Gestione e reportistica

SonicWall offre un'intuitiva piattaforma basata sul web che semplifica la gestione delle appliance e fornisce ampie funzionalità di reporting. La GUI di facile utilizzo agevola la gestione di più macchine. La gestione unificata delle policy consente di creare e monitorare facilmente le policy e le configurazioni di accesso. Con una singola policy è possibile gestire utenti, dispositivi, applicazioni, dati e reti. Le attività di routine possono essere pianificate e automatizzate, liberando i team addetti alla sicurezza dai compiti ripetitivi affinché si concentrino su attività di sicurezza strategiche, come la risposta agli incidenti.

I reparti informatici possono così fornire la migliore esperienza e l'accesso più sicuro possibile a seconda dello scenario d'uso. È possibile scegliere tra una gamma di soluzioni per l'accesso sicuro basato sul web completamente clientless per fornitori e contraenti terzi, oppure un più tradizionale accesso completo a tunnel VPN basato su client per i dirigenti. SonicWall SMA è la soluzione ideale sia per aziende che devono fornire un accesso sicuro e affidabile a pochi utenti da un singolo data center, sia per le imprese che necessitano di scalabilità fino a migliaia di utenti in data center distribuiti a livello globale.

Per maggiori informazioni sui prodotti SonicWall per la sicurezza dei dispositivi mobili: www.sonicwall.com/products/remote-access/

Protezione delle e-mail

L'e-mail è fondamentale per la comunicazione aziendale, ma è anche il principale vettore di attacco per minacce come ransomware, phishing, business email compromise (BEC), spoofing, spam e virus. Inoltre, in base alle normative vigenti, è responsabilità dell'azienda proteggere i dati riservati impedendo eventuali perdite di dati e assicurare lo scambio sicuro di e-mail contenenti informazioni riservate o dati sensibili dei clienti. Le organizzazioni di ogni dimensione, dalle PMI in crescita alle grandi aziende con ambienti distribuiti fino ai fornitori di servizi gestiti (MSP), necessitano di una soluzione a costi contenuti che garantisca la sicurezza e la crittografia delle e-mail e la scalabilità necessaria per aumentare agevolmente la capacità delle unità organizzative e dei domini delegando i processi di gestione.

Per gestire al meglio i costi e le risorse, sempre più aziende stanno adottando Microsoft Office 365 e Google G Suite. Poiché questi programmi offrono funzionalità di sicurezza predefinite, per combattere le minacce avanzate le aziende hanno bisogno di una soluzione di sicurezza e-mail di ultima generazione in grado di integrarsi perfettamente con Office 365 e G Suite per proteggerle dalle minacce sofisticate di oggi.

Appliance SonicWall Email Security

Semplice da configurare e gestire, SonicWall Email Security è scalabile da 10 fino a 100.000 caselle di posta a costi ridotti. Può essere installato come dispositivo hardware, come appliance

virtuale basata su risorse di calcolo condivise o come software, inclusa una versione ottimizzata per Microsoft Windows Server o Small Business Server. Le apparecchiature fisiche di SonicWall Email Security sono la scelta ideale per le aziende che necessitano di una soluzione dedicata in sede. La nostra soluzione multilivello offre protezione completa in entrata e in uscita. È disponibile un'ampia gamma di dispositivi hardware, ciascuno scalabile fino a 10.000 utenti. SonicWall Email Security è anche disponibile come appliance virtuale o come applicazione software, la soluzione ideale per le aziende che richiedono la flessibilità e l'agilità offerte dalla virtualizzazione. La soluzione può essere configurata per l'alta disponibilità in modalità split, per gestire distribuzioni su larga scala a livello centralizzato e con la massima affidabilità.

SonicWall Email Security utilizza tecnologie come machine learning, euristica, analisi della reputazione e del contenuto, protezione time-of-click degli URL e sandboxing per gli allegati e gli URL, garantendo la protezione completa dei messaggi e-mail in entrata e in uscita.

La soluzione include anche potenti standard di autenticazione delle e-mail per bloccare gli attacchi di spoofing e le frodi via e-mail, come ad esempio SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting and Conformance).

- Blocco delle minacce avanzate prima che raggiungano le caselle di posta
- Protezione da frodi via e-mail e attacchi di phishing mirati
- Sicurezza sempre aggiornata con l'intelligence delle minacce in tempo reale
- Protezione dei servizi e-mail su cloud (Office 365, G Suite)
- Prevenzione della perdita di dati delle e-mail e conformità
- Semplice gestione e reporting
- Opzioni di installazione flessibili

La soluzione Email Security è intuitiva, rapida e semplice da gestire. La gestione dello spam può essere delegata agli utenti finali, mantenendo comunque il controllo finale sull'applicazione della protezione. Inoltre, la sincronizzazione continua con più server LDAP consente di gestire facilmente gli account degli utenti e dei gruppi.

La soluzione offre anche una semplice integrazione con Office 365 e G Suite per proteggersi dalle minacce avanzate.

In ambienti distribuiti di grande estensione, il supporto multi-tenancy consente di delegare ad amministratori subordinati la gestione delle impostazioni su più unità organizzative (come divisioni aziendali o clienti MSP) all'interno di un'unica implementazione di Email Security.

Servizio SonicWall Hosted Email Security

I servizi in hosting, rapidi da implementare e semplici da gestire, proteggono le aziende da minacce basate sulla posta elettronica come ransomware, minacce zero-day, spear phishing e business email compromise (BEC) e soddisfano i requisiti normativi e di conformità delle e-mail. La nostra soluzione in hosting offre lo stesso livello di protezione avanzata delle e-mail e le stesse funzionalità delle appliance fisiche e virtuali. Le funzioni di continuità della posta elettronica garantiscono che i messaggi e-mail vengano sempre consegnati, senza impatti sulla produttività in caso di interruzioni pianificate o impreviste dei server di posta elettronica in azienda o di un provider di servizi cloud come Office 365 e G Suite.

SonicWall Hosted Email Security offre un'eccellente protezione basata su cloud contro le minacce in entrata e in uscita a fronte di un abbonamento mensile o annuale flessibile, a costi moderati e prevedibili. La soluzione riduce al minimo non solo i costi e il tempo di installazione iniziali, ma anche le spese amministrative correnti, il tutto senza compromettere la sicurezza.

SonicWall offre a MSP e VAR maggiori opportunità competitive e di guadagno, riducendo al tempo stesso i rischi, le spese generali e i costi ricorrenti. SonicWall Hosted Email Security include funzionalità adatte agli MSP quali multi-tenancy avanzata, gestione centralizzata di più sottoscrittori, integrazione con Office 365, opzioni

di acquisto flessibili e provisioning automatizzato.

Per maggiori informazioni sui prodotti SonicWall Email Security: www.sonicwall.com/en-us/products/secure-email.

Gestione, reportistica e analisi

SonicWall ritiene che un approccio connesso alla gestione della sicurezza sia fondamentale non solo come buona pratica di sicurezza preventiva, ma anche per creare le basi di una strategia unificata di governance della sicurezza, conformità e gestione del rischio. Le soluzioni di gestione, reportistica e analisi di SonicWall offrono alle aziende una piattaforma integrata, protetta e ampliabile per creare un sistema di difesa solido e uniforme e una strategia di risposta per le loro reti cablate, wireless e multi-cloud. Inoltre, adottando questa piattaforma comune, le aziende possono prendere decisioni sulla sicurezza basate su informazioni dettagliate e agire velocemente, favorendo la collaborazione, la comunicazione e il trasferimento di conoscenze all'interno dell'infrastruttura di sicurezza condivisa.

SonicWall Network Security Manager

SonicWall Network Security Manager (NSM) mette a disposizione delle aziende tutto ciò che serve per un sistema di gestione firewall unificato. Offre visibilità a livello dei tenant, controllo dei dispositivi in base a gruppi e scalabilità illimitata per configurare e gestire centralmente le attività di sicurezza della rete SonicWall.

Queste attività comprendono l'installazione e la gestione di tutti i dispositivi firewall, dei gruppi di dispositivi e dei tenant, l'orchestrazione e l'applicazione di configurazioni e policy di sicurezza coerenti in ambienti SD-Branch e SD-WAN nonché il monitoraggio generale da un pannello di controllo dinamico con report e analisi dettagliate. NSM consente di fare tutto questo da un'unica console nativa per il cloud, facile da utilizzare e accessibile da ogni luogo con qualsiasi dispositivo dotato di browser.

NSM offre ai fornitori di servizi un sistema di gestione multi-tenant completo e il controllo isolato di policy indipendenti per tutti i tenant gestiti. Questa separazione riguarda tutte le funzionalità gestionali di NSM, che determinano il funzionamento del firewall per ogni tenant. In questo modo è possibile strutturare ogni tenant con il proprio insieme di utenti, gruppi e ruoli per condurre la gestione del gruppo di dispositivi, delle policy e tutte le altre attività amministrative entro i limiti dell'account assegnato al tenant. Offre visibilità a livello dei tenant, controllo dei dispositivi in base a gruppi e scalabilità illimitata per configurare e gestire centralmente le attività di sicurezza della rete SonicWall.

SonicWall Analytics

SonicWall Analytics trasforma i dati in decisioni e le decisioni in azioni, per risolvere i problemi di sicurezza e impedire che si ripetano.

Questo potente servizio di analisi e monitoraggio del traffico offre una visione dettagliata di tutto ciò che accade all'interno dell'ambiente di sicurezza di rete. Il motore di analisi basato su intelligence aggrega, normalizza e contestualizza i dati di sicurezza, tra cui il traffico di rete e le attività degli utenti che attraversano il firewall e i Access Point wireless, offrendo agli amministratori una visione diretta e in tempo quasi reale delle minacce dirette alle loro reti e agli utenti.

Grazie ad analisi e report dettagliati, le aziende dispongono delle informazioni e della capacità di individuare e risolvere i problemi operativi e di sicurezza con maggiore efficienza. Le funzionalità di drill-down consentono ai responsabili della sicurezza di indagare, analizzare e adottare azioni basate sull'evidenza contro le attività e i comportamenti sospetti o rischiosi degli utenti, il tutto con maggiore

[1] NSM SaaS include funzioni di analisi e reportistica.
[2] NSM On-Prem richiede l'installazione di SonicWall Analytics On-Prem e una licenza separata per le funzionalità di analisi e reportistica.

visibilità, accuratezza e velocità. Inoltre possono dedicare il loro tempo e il loro impegno alla creazione di azioni di risposta e correzione rapide per i rischi di sicurezza rilevanti, anziché reagire ad ogni evento.

L'integrazione di Analytics nel processo aziendale aiuta anche a rendere operative le analisi mediante l'invio automatico di avvisi in tempo reale, l'orchestrazione delle policy e dei controlli di sicurezza in modo proattivo e automatizzato e il monitoraggio dei risultati per garantire la sicurezza.

SonicWall Wireless Network Manager

SonicWall Wireless Network Manager (WNM) integra a livello globale la gestione dei Access Point e degli switch SonicWave. Parte integrante dell'ecosistema SonicWall Capture Security Center, offre visibilità e gestione unificata per le reti cablate e wireless.

Basato sul cloud e facile da utilizzare, WNM semplifica l'accesso, il controllo e la risoluzione dei problemi attraverso un'unica dashboard di controllo. WNM consente agli amministratori di creare singole policy a livello di tenant e di inviarle in diverse sedi e zone, e offre funzionalità di drill-down sui dispositivi gestiti per ottenere dati granulari.

WNM è altamente scalabile e in grado di gestire da un semplice sito a reti aziendali globali con decine di migliaia di dispositivi gestiti.

Per garantire le prestazioni e la produttività, prima di implementare i Access Point è possibile eseguire un'analisi wireless del sito con il tool Wi-Fi Planner integrato in WNM, che aiuta a installare i Access Point in modo strategico per ottimizzare l'esperienza d'uso del Wi-Fi ed evitare costosi errori.

Gli access point SonicWave e gli switch SonicWall offrono l'implementazione zero-touch, che consente un caricamento automatico in pochi minuti con l'app SonicExpress per dispositivi mobili. Il provisioning è semplice e può essere eseguito da remoto, con un notevole risparmio di tempo e denaro.

Gli aggiornamenti automatici di sicurezza e del firmware mantengono sempre aggiornati i dispositivi gestiti. In caso di interruzione della connessione Internet, gli access point e gli switch possono continuare a funzionare senza WNM, garantendo la continuità dei servizi.

Per maggiori informazioni sui prodotti di gestione e reportistica di SonicWall: www.sonicwall.com/en-us/productsfirewalls/management-and-reporting.

Servizi professionali e supporto Enterprise

Ottenete di più dalla soluzione di sicurezza di rete SonicWall con tutto il supporto che serve, quando serve. Con il supporto Enterprise e i servizi professionali di SonicWall potete aumentare il valore della vostra soluzione nel tempo.

Servizi di supporto globali

Diverse opzioni di assistenza convenienti per mantenere la vostra azienda sempre operativa:

Supporto tecnico

- **8x5** – Dal lunedì al venerdì, dalle ore 8 alle ore 17, per ambienti non critici.
- **7x24** – Supporto 24 ore su 24, 7 giorni su 7, inclusi i fine settimana e i giorni festivi, per ambienti business-critical.

Supporto a valore aggiunto

- **Supporto Premier**: un Technical Account Manager (TAM) dedicato per gli ambienti aziendali. Il TAM opera come consulente di fiducia che collabora con il vostro personale per ridurre i tempi di inattività imprevisti e ottimizzare i processi IT, fornisce rapporti operativi per incrementare le efficienze ed è il vostro unico interlocutore, garantendo così un'esperienza di supporto coerente.
- **Dedicated Support Engineer (DSE)**: un tecnico di supporto dedicato per la vostra infrastruttura aziendale. Il DSE conosce e comprende il vostro ambiente, le vostre policy e gli obiettivi di IT, per offrirvi una rapida risoluzione tecnica appena serve assistenza.

Servizi professionali globali

Serve aiuto per stabilire qual è la soluzione di sicurezza migliore per la vostra azienda e per configurarla all'interno della vostra infrastruttura esistente? Lasciate che ce ne occupiamo noi. Con i Servizi Professionali Globali avrete un unico punto di contatto per tutte le vostre esigenze di implementazione e integrazione. Riceverete servizi creati su misura per il vostro ambiente aziendale e assistenza relativamente a:

- **Pianificazione:** determinazione e comprensione dei requisiti del vostro firewall.
- **Implementazione/installazione:** valutazione e implementazione della vostra soluzione.
- **Trasferimento di conoscenze:** uso, gestione e manutenzione del vostro dispositivo.
- **Migrazione:** riduzione dei tempi di fermo e garanzia di continuità dei servizi.

I servizi Enterprise di SonicWall sono disponibili per le linee di prodotti NS*sp*/NS*a*/TZ Series/SMA/Email Security/GMS.

Per maggiori informazioni: www.sonicwall.com/en-us/support

Conclusioni

Scoprite i prodotti per la sicurezza di SonicWall

L'integrazione di hardware, software e servizi garantisce la protezione migliore della categoria. Per maggiori informazioni, visitare il nostro sito www.sonicwall.com. Per conoscere le varie opzioni di acquisto e upgrade, consultare la pagina www.sonicwall.com/how-to-buy. E per provare direttamente le soluzioni SonicWall, visitare www.sonicwall.com/trials.

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla 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

Per chiarimenti sul potenziale utilizzo di questo materiale rivolgersi a:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com