SCHEDA TECNICA

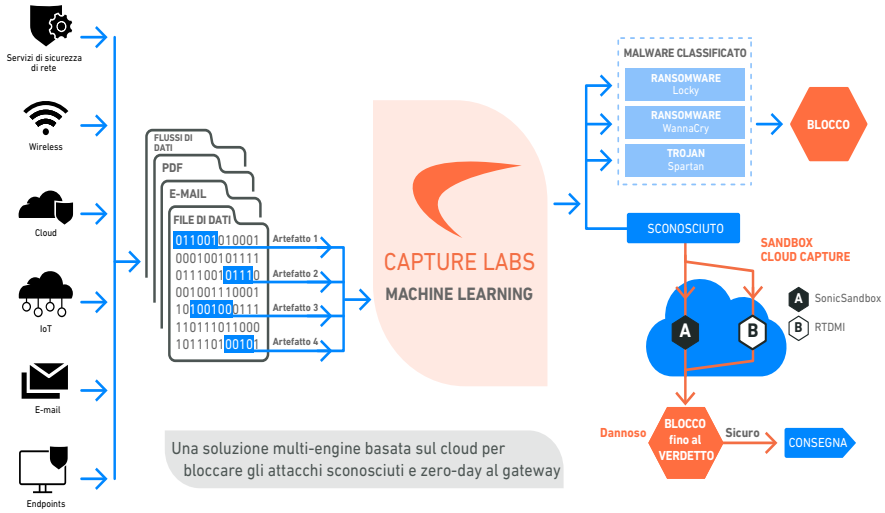
Gen 8: Architettura e sicurezza

Protezione contro le minacce avanzate per l'attuale panorama in continua evoluzione

La generazione 8 (Gen 8) di SonicWall risolve i problemi di sicurezza della rete per organizzazioni di ogni dimensione, dagli ambienti SOHO alle PMI fino alle aziende distribuite. Il cuore della serie di firewall Gen 8 è l'architettura SonicOS.

SonicOS 8 migliora ulteriormente le prestazioni, la coerenza e l'affidabilità della sicurezza di rete. Utilizza le nostre brevettate tecnologie Reassembly-Free Deep Packet Inspection® (RFDPI) single-pass a bassa latenza e Real-Time Deep Memory Inspection™ (RTDMI) per garantire un'elevata efficacia di sicurezza comprovata nel settore, SD-WAN, visualizzazione in tempo reale, rete privata virtuale (VPN) ad alta velocità e altre potenti funzioni di sicurezza.

La nostra filosofia di protezione delle reti nell'attuale panorama di minacce informatiche in continua evoluzione consiste nel rilevare e prevenire automaticamente le minacce in tempo reale. Grazie alla combinazione di tecnologie integrate basate sul cloud, i nostri firewall dispongono di una protezione la cui elevata efficacia è stata confermata da test indipendenti di terze parti. Le minacce sconosciute vengono inviate per l'analisi alla sandbox multi-engine Capture Advanced Threat Protection (ATP) basata su cloud di SonicWall. La sandbox Capture ATP è ulteriormente potenziata dalla nostra tecnologia RTDMI™. Il motore RTDMI rileva e blocca il malware e le minacce zero-day mediante l'analisi diretta in memoria. La tecnologia RTDMI di SonicWall è precisa, riduce al minimo i falsi positivi, identifica e attenua gli attacchi sofisticati in cui i meccanismi di attacco del malware restano esposti per meno di 100 nanosecondi.



Una soluzione multi-engine basata sul cloud per bloccare gli attacchi sconosciuti e zero-day al gateway

sonicwall.com

SONICWALL®

In combinazione con questa tecnologia, il nostro motore RFDPI esamina ogni byte di ogni pacchetto, ispezionando il traffico sia in entrata che in uscita direttamente sul firewall. Utilizzando Capture ATP con la tecnologia RTDMI, integrati nella piattaforma SonicWall Capture Cloud, oltre a funzionalità integrate come prevenzione delle intrusioni, anti-malware e filtraggio web/URL, i nostri firewall di ultima generazione bloccano il malware, il ransomware e altre minacce a livello del gateway.

SonicOS 8 offre caratteristiche di sicurezza avanzate, gestione semplificata delle policy e funzioni di connettività e gestione essenziali sia per imprese avanzate con SD-Branch di ultima generazione sia per le PMI. Il nuovo sistema operativo supporta inoltre Wi-Fi 6, sicurezza DNS avanzata, filtraggio dei contenuti basato sulla reputazione e l'integrazione con Network Access Control (NAC).

I firewall Gen 8 supportano le funzionalità Zero Trust Network Access (ZTNA). Questo approccio garantisce che l'attendibilità dell'utente e del dispositivo venga ripetutamente verificata prima di concedere l'accesso ad applicazioni specifiche, indipendentemente dalla posizione e dal tipo di endpoint.

Il piano di gestione dei firewall Gen 8 include SonicWall Unified Management, che offre una console unificata per gestire le soluzioni di cybersecurity di SonicWall. Creato su misura per MSP e MSSP, SonicWall Unified Management semplifica la gestione dello stack di sicurezza grazie a un unico pannello di controllo, che facilita e ottimizza le attività di sicurezza essenziali. La gestione dei firewall è inclusa nei firewall Gen 8 dotati di servizi di assistenza o pacchetti di sicurezza attivi.

Suite di sicurezza e opzioni di licenza

I firewall SonicWall di nuova generazione consentono alle aziende di soddisfare le proprie esigenze operative con licenze semplificate. Nella versione più recente, la Generazione 8 offre diverse opzioni per la formula Hardware Only[1] e per le suite di sicurezza con e senza servizi firewall gestiti[2]. Il modello di licenze semplificate offre una maggiore sicurezza ed efficienza operativa per le nostre piattaforme dedicate a PMI e aziende, senza la complessità di dover gestire più licenze. Inoltre, le suite di sicurezza SonicWall consentono alle aziende di ridurre i rischi di perdite finanziarie derivanti da violazioni della sicurezza grazie a una garanzia informatica integrata con copertura fino a 200.000 dollari.

SonicWall Advanced Protection Security Suite (APSS) offre servizi avanzati di sicurezza, reportistica e analisi per proteggere le reti e migliorare la visibilità e l'efficienza operativa. Questa opzione di licenza è ideale per le organizzazioni che non necessitano di servizi firewall gestiti.

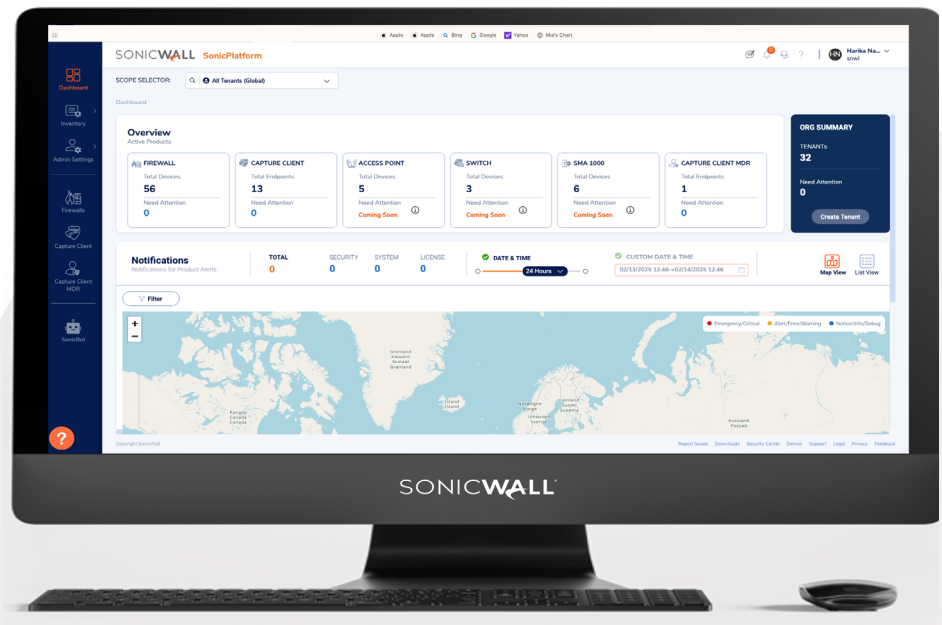
SonicWall Managed Protection Security Suite (MPSS) comprende servizi firewall gestiti, oltre a tutti i servizi offerti in APSS. Il nostro personale monitora i firewall dei clienti e li informa in caso di interruzioni o modifiche locali, oltre a gestire per loro tutti gli aggiornamenti del firmware in base alle loro scadenze.

[1] L'opzione Hardware Only non è disponibile per TZ80, che richiede una licenza basata su abbonamento.

[2] TZ80 per SOHO e IoT dispone di Secure Connect Lite, Secure Connect, Advanced Protection Security Suite e Managed Protection Security Suite. Per maggiori informazioni, consultare la scheda tecnica di TZ80.

Per maggiori informazioni, consultare le Suite di sicurezza.

Scopri di più



Dashboard migliorata

Dashboard migliorata

Funzionalità	Descrizione
Sicurezza DNS	Utilizza il DNS (Domain Name System) per bloccare siti web o applicazioni dannose e per filtrare contenuti malevoli o inappropriati.
Integrazione di Network Access Control (NAC)	Fornisce il controllo degli accessi alla rete ai clienti SonicWall grazie all'integrazione con Aruba ClearPass. Questa architettura trasforma la sicurezza statica in una sicurezza contestuale per garantire una protezione più flessibile e avanzata.
Supporto Wi-Fi 6	Integrazione e gestione degli access point SonicWave Wi-Fi 6.
Miglioramenti dello storage secondario	Supporto per acquisizione dei pacchetti, TSR e dati di correlazione delle minacce nello spazio di storage. Salvataggio dei log seguenti in memoria: log delle minacce, log di audit, flusso di applicazioni, pcap.
Registrazioni basate su token	Una stringa che sostituisce il nome utente e la password di MySonicWall nel file di bootstrap utilizzato per il processo di avvio di NS*v* per automatizzare le distribuzioni di massa con informazioni di configurazione e licenza di base.
Bootstrap di NS*v*	Semplificazione delle implementazioni NS*v* di massa; supporto di VMware, Hyper-V, AWS e Azure; semplificazione delle registrazioni dei prodotti con licenze basate su token; il file INIT include la configurazione di base per avviare l'istanza con una configurazione minima.
Dashboard migliorata	Dashboard con avvisi attivabili.
Vista ottimizzata dei dispositivi	Nella scheda Home dell'interfaccia utente sono disponibili la vista anteriore e posteriore dei dispositivi nonché statistiche sull'uso della memoria.
Utilizzo del sistema e della larghezza di banda in tempo reale	L'utente può visualizzare in tempo reale l'utilizzo delle risorse di sistema e della larghezza di banda nella rete.
Riepilogo della distribuzione del traffico	Utilizzo della distribuzione del traffico sul firewall dell'utente con aggiornamento in tempo reale delle applicazioni più utilizzate.
Riepilogo degli utenti principali	Riepilogo degli utenti principali in base alle sessioni consentite o bloccate, suddiviso per dati inviati e ricevuti.
Riepilogo delle minacce osservate	Riepilogo in tempo reale delle minacce osservate nella rete del cliente come virus, malware zero-day, spyware, vulnerabilità e applicazioni a rischio.
Riepilogo dei servizi	Stato in tempo reale dei servizi di sicurezza abilitati o disabilitati come IPS, GAV, Anti-Spyware, Capture ATP o DPI-SSL.
Informazioni sugli host infettati	Visualizzazione in tempo reale del numero totale di macchine host infettate nella rete.
Informazioni sugli attacchi critici	Visualizzazione in tempo reale del numero totale di attacchi critici nella rete.
Informazioni sul traffico crittografato	Visualizzazione in tempo reale del numero totale di traffico crittografato nella rete.
Riepilogo delle applicazioni principali	Visualizzazione delle principali applicazioni utilizzate nella rete con opzioni aggiuntive di ordinamento per sessioni, byte, blocchi di regole di accesso, virus, spyware e intrusioni.
Riepilogo degli indirizzi principali	Visualizzazione dei principali oggetti indirizzo utilizzati nella rete con opzioni aggiuntive di ordinamento per sessioni, byte, blocchi di regole di accesso, virus, spyware e intrusioni.
Riepilogo degli utenti principali	Visualizzazione dei principali utenti utilizzati nella rete con opzioni aggiuntive di ordinamento per sessioni, byte, blocchi di regole di accesso, virus, spyware e intrusioni.
Riepilogo delle valutazioni dei siti web principali	Visualizzazione delle valutazioni dei siti web principali per sessione.
Riepilogo delle statistiche dei paesi principali	Visualizzazione delle statistiche dei paesi principali ordinate per sessione, traffico eliminato, byte inviati o ricevuti.
Riepilogo delle minacce in tempo reale	Visualizzazione delle principali minacce con statistiche separate per virus, intrusioni, spyware e botnet per sessione.
Istantanea migliorata degli access point	Visualizzazione in tempo reale delle statistiche sullo stato degli access point nelle associazioni di rete e client
Velocità del traffico degli access point	Informazioni in tempo reale sull'utilizzo della larghezza di banda per ogni access point.
Report dei client Wi-Fi	Report in tempo reale sui client Wi-Fi in base a tipo di sistema operativo, frequenza ed elenco dei client principali.
Monitoraggio client Wi-Fi in tempo reale	Determina la macchina host, il tipo di sistema operativo, la frequenza, le informazioni sugli access point e il trasferimento dei dati.
Informazioni sui verdetti di Capture ATP	Visualizzazione dei verdetti forniti da Capture ATP per l'analisi dei file.
Informazioni su tipi di file	Visualizzazione del tipo di file in base al report di Capture ATP.
Informazioni sull'indirizzo di destinazione	Visualizzazione delle principali destinazioni utilizzate dai file dannosi.
Statistiche dell'analisi del malware	Visualizzazione di statistiche dettagliate sull'analisi dinamica e statica del malware per ogni file.
Analisi dell'origine degli attacchi zero-day basata sulla posizione	Visualizzazione dell'origine degli attacchi per paese.
Statistiche di Capture ATP	Visualizzazione di informazioni sul numero totale dei file inviati, di quelli analizzati dinamicamente, di quelli dannosi e sul tempo medio di elaborazione tramite Capture ATP.
Visualizzazione della topologia di rete	Visualizzazione degli host e degli access point connessi alla rete dell'utente in base al nome del dispositivo, all'indirizzo MAC e all'indirizzo IP
Gestione basata su API	La gestione del firewall è basata sulle API
Wizard SD-WAN	Procedura guidata per configurare automaticamente le policy SD-WAN sul firewall
Centro notifiche	Nuovo centro notifiche con riepilogo delle minacce, log degli eventi e avvisi del sistema.
Guida online migliorata	Guida online con collegamenti alla documentazione tecnica per ciascun modello.
Monitoraggio SD-WAN	Visualizza i dati prestazionali e le principali connessioni SD-WAN.
Utility di monitoraggio dei pacchetti ottimizzata	Il monitoraggio dei pacchetti migliorato include ora le regole di accesso, la regola NAT e informazioni di instradamento.
Configurazione del dispositivo di storage	Supporto per la configurazione dei moduli di archiviazione, compresi quelli estesi. Statistiche sull'utilizzo dei moduli.

Capture Threat Assessment	Supporta il nuovo modello di report con opzioni di personalizzazione come logo, nome e sezioni. Supporta l'analisi dei file e del malware. Statistiche aziendali con media di settore e media globale per ogni sezione. Modello Executive separato con raccomandazioni.
Download dei log di sistema	I log di sistema includono i registri della console, che possono essere scaricati dalla sezione diagnostica senza che l'utente debba collegare la macchina alla porta della console per acquisirli. Questo semplifica i metodi di debug e riduce i tempi di risoluzione delle anomalie.
Terminale SSH su interfaccia utente	Il terminale SSH è accessibile dall'interfaccia utente web.
Utility di verifica Grid	Questa utility consente di controllare la reputazione di un indirizzo IP a fini diagnostici.
Utility di debug	L'utente può abilitare la modalità di debug dallo stesso firmware ed eseguire i comandi di debug dal terminale SSH nell'interfaccia utente.
Strumenti di diagnosi del sistema	Supporto per ulteriori strumenti diagnostici come GDB, HTOP e Linux Perf Tool.
Panoramica della rete di switch	Visualizzazione degli switch SonicWall con vista fisica, vista tabulare e vista VLAN.
Uso della larghezza di banda per porta switch	Informazioni sulla larghezza di banda utilizzata per ogni porta degli switch SonicWall.
Stato WWAN	Visualizzazione dello stato del modem e della rete WWAN.

Funzionalità e servizi firewall

Motore Reassembly-Free Deep Packet Inspection (RFDPI)

Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un motore di ispezione proprietario, brevettato e di elevate prestazioni, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni su qualsiasi porta.
Ispezione bidirezionale	Con la scansione contemporanea del traffico in ingresso 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 basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni che a flussi TCP primari.
Architettura altamente parallela e scalabile	L'esclusivo motore RFDPI basato su architettura multi-core consente un'elevata velocità DPI e l'avvio di nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI single-pass consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.

Firewall e connettività di rete

Funzionalità	Descrizione
Secure SD-WAN	SD-WAN sicura è una valida alternativa a tecnologie più costose come MPLS che permette alle imprese distribuite di creare, utilizzare e gestire reti sicure ad alte prestazioni negli uffici remoti per condividere dati, applicazioni e servizi utilizzando servizi internet pubblici immediatamente disponibili e a basso costo.
API REST	Consentono al firewall di ricevere e sfruttare tutti i feed di intelligence proprietari dei produttori di dispositivi originali e di terze parti per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle policy di accesso del firewall.
Alta disponibilità	Supporta la modalità attiva/passiva (A/P) con sincronizzazione dello stato.
Protezione da attacchi DDoS/ DoS	La protezione da flood SYN offre una difesa contro gli attacchi DOS basata su tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge dagli attacchi DOS/DDoS mediante la protezione da flood UDP/ICMP e la limitazione della velocità di connessione.
Opzioni di installazione flessibili	Il firewall può essere utilizzato in modalità wire, network tap NAT o Layer 2 bridge[2].
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over. Il routing basato su policy crea percorsi basati sui protocolli per indirizzare il traffico verso una connessione WAN preferita, con possibilità di commutare su una WAN secondaria in caso di interruzione.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto gatekeeper H.323 e proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.
Integrazione degli switch SonicWall	Gli switch di SonicWall si integrano perfettamente con i firewall, fornendo gestione e visibilità della rete da un unico pannello di controllo
Gestione di switch Dell serie N e X singoli e in cascata	Gestione delle impostazioni di sicurezza di porte aggiuntive, tra cui Portshield, HA, PoE e PoE+, da un unico pannello di controllo utilizzando la dashboard di gestione del firewall per gli switch di rete delle serie N e X di Dell.

Autenticazione biometrica	Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Autenticazione aperta e social login	Consente agli utenti ospiti di utilizzare le loro credenziali da servizi di social network come Facebook, Twitter o Google+ per registrarsi e accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through.
Autenticazione multi-dominio	Offre un metodo semplice e veloce per amministrare le policy di sicurezza in tutti i domini di rete e gestire policy individuali per un singolo dominio o per un gruppo di domini.
Supporto API completo	Supporto API completo per ogni sezione dell'interfaccia utente del firewall.
Scalabilità SD-WAN	Interfacce tunnel scalabili per le imprese distribuite.

Gestione, reportistica e supporto

Funzionalità	Descrizione
Gestione basata sul cloud e on-premise	La configurazione e la gestione dei dispositivi SonicWall sono disponibili via cloud tramite SonicWall Network Security Manager (NSM) on-premise o in cloud, che è accessibile da SonicWall Unified Management.
Gestione avanzata con un unico dispositivo	Configurazione comoda e veloce tramite l'interfaccia web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3.
Report sul flusso delle applicazioni con IPFIX/NetFlow	Le analisi del traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Analytics o altri che supportano IPFIX e NetFlow con estensioni.
Rilevamento del malware basato sulla conformità	Analizza i file sospetti direttamente nel proprio ambiente senza inviare file o risultati a cloud di terze parti.

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 da sede a sede tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per una connettività Site-to-Site	La VPN IPSec ad alte prestazioni consente di utilizzare il firewall come concentratore di VPN per migliaia di altre sedi di grandi dimensioni, filiali o utenti privati.
Accesso remoto tramite VPN SSL o 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 utilizzano più WAN è possibile configurare una VPN principale e una secondaria per consentire il failover e il failback automatici senza soluzione di continuità di tutte le sessioni VPN.
VPN basata su route	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di interruzione temporanea del tunnel VPN, perché il traffico viene reinstradato senza interruzioni tra gli endpoint attraverso percorsi alternativi.

Zero Trust Network Access (ZTNA)

Funzionalità	Descrizione
Connettore per Secure Private Access (SPA)	Utilizza i firewall SonicWall esistenti e l'integrazione con Cloud Secure Edge per consentire l'accesso di rete Zero Trust alle applicazioni private ospitate dietro i firewall.

Sensibilità al contesto e al contenuto

Funzionalità	Descrizione
Tracciamento delle attività degli utenti	Le tecnologie AD/LDAP/Citrix/Terminal Services SSO integrate si combinano con le informazioni esaustive ottenute con l'ispezione DPI, per consentire il tracciamento delle attività e l'identificazione degli utenti.
GeoIP per l'identificazione del traffico da determinati paesi	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da determinati paesi. 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. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP, eliminando così il filtraggio indesiderato di indirizzi IP a causa di classificazioni errate.
Corrispondenza e filtraggio 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.

Servizi in abbonamento per la prevenzione delle violazioni

Capture Advanced Threat Protection[1]

Funzionalità	Descrizione
Sandbox multi-engine	La piattaforma sandbox multi-engine, che include l'emulazione completa del 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 dannose.
Real-Time Deep Memory Inspection (RTDMI™)	SonicWall RTDMI è un processo e una tecnologia brevettata, utilizzata da SonicWall Capture Cloud per identificare e mitigare anche le più insidiose minacce attuali, tra cui i futuri exploit di Meltdown. Questa tecnologia rileva e blocca anche i malware che non mostrano alcun comportamento dannoso e nascondono i propri strumenti di attacco attraverso la crittografia.
Blocco fino al verdetto	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.
Analisi di un'ampia varietà di tipi di file	Supporta l'analisi di un'ampia gamma di tipi di file, tra cui programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a diversi sistemi operativi come Windows, Android, Mac OS e ambienti multi-browser.
Distribuzione rapida delle firme	Quando un file viene identificato come dannoso, viene immediatamente distribuita una firma ai firewall con abbonamento al servizio SonicWall Capture, ai database con le firme per l'antivirus a livello gateway e l'ispezione IPS nonché ai database di reputazione degli URL, degli IP e dei domini.

Sicurezza degli endpoint

Funzionalità	Descrizione
Protezione degli endpoint	Capture Client applica la protezione contro le minacce avanzate basata sul comportamento, con tecnologia EDR di SentinelOne di ultima generazione. L'integrazione con Capture ATP garantisce una maggiore efficacia in termini di sicurezza, tempi di risposta più rapidi e un costo totale di proprietà inferiore.
Applicazione DPI-SSL	Applica i certificati DPI-SSL, con possibilità di eseguire l'ispezione approfondita dei pacchetti di traffico crittografato (DPI-SSL) sugli endpoint.
Applicazione agli endpoint	Gli utenti non protetti vengono indirizzati alla pagina di download di Capture Client prima di accedere a Internet da dietro un firewall.
Accesso Single Sign-On (SSO)	Consente di utilizzare le informazioni degli utenti dagli endpoint per le policy SSO.
Single Sign-On SAML[1]	Semplifica l'autenticazione consentendo l'accesso a più applicazioni tramite un set di credenziali[1]

Prevenzione delle minacce crittografate

Funzionalità	Descrizione
Decrittazione e ispezione TLS/SSL	Il traffico TLS/SSL crittografato viene decrittografato e analizzato in tempo reale senza l'uso di proxy per individuare malware, intrusioni e fughe di dati, e vengono applicate policy per il controllo di contenuti, URL e applicazioni che proteggono dalle minacce nascoste nel traffico crittografato. L'opzione è inclusa negli abbonamenti di sicurezza per tutti i modelli, tranne SOHO. Per quest'ultimo viene venduta come licenza a parte.
Ispezione SSH	L'ispezione approfondita dei pacchetti del protocollo SSH (DPI-SSH) decripta e ispeziona i dati che attraversano i tunnel SSH per prevenire gli attacchi basati su SSH.
Supporto TLS 1.3	Supporto per TLS 1.3 per migliorare la sicurezza generale sul firewall. Implementato in Firewall Management, SSL VPN e DPI.

Prevenzione delle intrusioni[2]

Funzionalità	Descrizione
Protezione basata su 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 SonicWall Threat Research 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)	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 e abuso di protocolli	Individua e blocca gli attacchi che abusano dei protocolli per tentare di eludere l'IPS.
Protezione zero-day	Protegge la rete dagli attacchi zero-day mediante aggiornamenti costanti 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 assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate.
Ampio elenco di firme IPS	Oltre 10.000 firme IPS associate alla protezione contro gli exploit che sfruttano le vulnerabilità del software.*

*Alcune firme associate alla protezione contro gli exploit che sfruttano le vulnerabilità del software si trovano nei servizi GAV e antispyware.

[1] Il Single Sign-On SAML è disponibile in SonicOS 8.1, che sarà rilasciato a breve.

Prevenzione delle minacce[2]

Funzionalità	Descrizione
Antimalware a livello del 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 Capture Cloud contro il malware	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte del motore RFDPI.
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.
Ispezione bidirezionale dei TCP primari	Il motore RFDPI esegue la scansione dei flussi TCP primari in entrambe le direzioni su tutte le porte per rilevare e prevenire le minacce in ingresso e in uscita.
Ampio supporto di protocolli	Identifica protocolli comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri che non inviano dati nel TCP grezzo. Decodifica i payload per l'ispezione del malware, anche se non utilizzano porte standard e ben note.

Controllo e intelligence delle applicazioni[2]

Funzionalità	Descrizione
Controllo delle applicazioni	Controlla le applicazioni o singole funzionalità rilevate dal motore RFDPI utilizzando un database in continua espansione, contenente migliaia di firme di applicazioni. Ciò aumenta la sicurezza della rete e ne migliora la produttività.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate creando firme basate su parametri specifici o pattern esclusivi delle singole applicazioni nelle comunicazioni di rete. Ciò consente di acquisire un maggiore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	Il traffico delle applicazioni superflue viene bloccato, mentre la larghezza di banda disponibile viene regolamentata e ripartita in modo granulare per le applicazioni (o le categorie di applicazioni) più importanti.
Controllo granulare	Controlla 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/Terminal Services/Citrix.

Filtraggio dei contenuti[2]

Funzionalità	Descrizione
Filtraggio dei contenuti basato sulla reputazione	Limita e controlla i contenuti web a cui un utente Internet è in grado di accedere. Il filtraggio dei contenuti basato sulla reputazione fornisce un punteggio di reputazione che prevede il rischio per la sicurezza di un URL.
Filtraggio dei contenuti interno/esterno	Applica policy di utilizzo accettabili e blocca l'accesso a siti web HTTP/HTTPS contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service e Content Filtering Client.
Content Filtering Client	Estende l'applicazione delle policy per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	Bloccano determinati contenuti utilizzando qualsiasi combinazione di categorie. 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.
Web caching	Le classificazioni degli URL vengono 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.
Local CFS Responder	Local CFS Responder può essere utilizzato come appliance virtuale in cloud privati basati su VMWare o Microsoft Hyper-V, offrendo l'opzione di installazione flessibile (Light weight VM) del database di classificazioni CFS in diversi casi di utilizzo della rete del cliente che richiedono una soluzione dedicata in sede in grado di velocizzare la richiesta di classificazioni CFS e i tempi di riposta, oltre a supportare un gran numero di elenchi di URL autorizzati/bloccati (oltre 100.000), supporta fino a 1000 firewall SonicWall per le ricerche di classificazioni CFS.

Antivirus e antispyware applicati[2]

Funzionalità	Descrizione
Protezione multilivello	Utilizza le funzioni del firewall come primo livello di difesa perimetrale, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop.
Distribuzione e installazione automatizzate	I client antivirus e antispyware vengono distribuiti e installati automaticamente macchina per macchina sull'intera rete, riducendo così l'impegno degli amministratori.
Protezione antispyware	La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza, analizzando e bloccando l'installazione di numerose tipologie di programmi spyware prima che questi possano sottrarre dati sensibili da computer fissi o portatili.

Sicurezza avanzata

Funzionalità	Descrizione
Visibilità della rete	Fornisce visibilità granulare della topologia di rete insieme a informazioni sull'host
Gestione via cloud	Gestione dei firewall via cloud tramite lo strumento Network Security Manager di SonicWall Unified Management

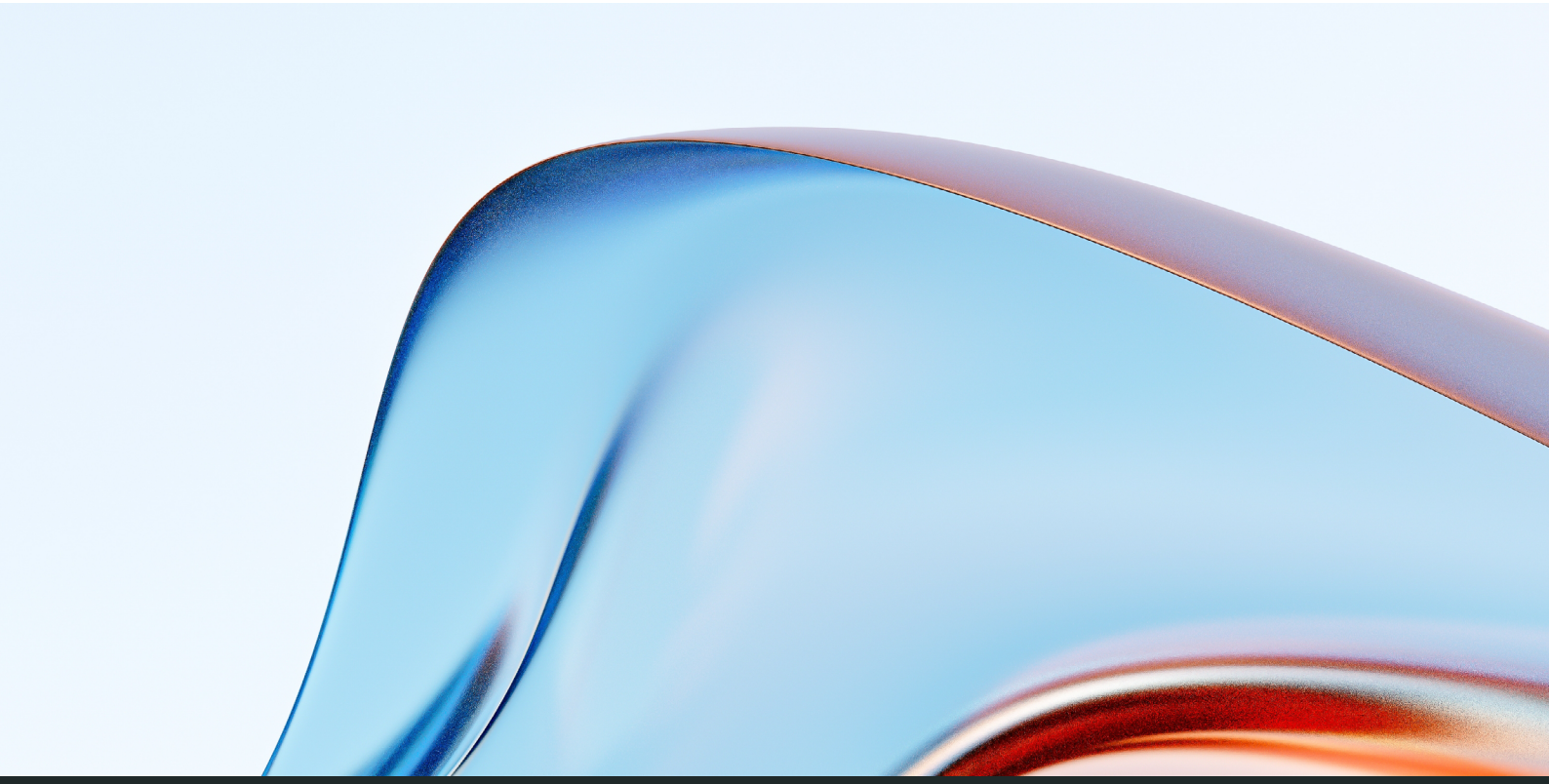
[2] Richiede un abbonamento aggiuntivo.

SONICWALL

SERVIZI OFFERTI DAI PARTNER

Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partner sono qualificati per fornire servizi professionali di altissimo livello.

Per maggiori informazioni:
www.sonicwall.com/PES



SonicWall, Inc.

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

sonicwall.com

SONICWALL®