Datasheet SonicOS 7.0 e servizi

L'architettura SonicOS è l'elemento centrale dei firewall fisici e di quelli virtuali di SonicWall, compresi i modelli delle serie TZ, NSa, NSv e NSsp. SonicOS utilizza le nostre tecnologie single-pass a bassa latenza Reassembly-Free Deep Packet Inspection® (RFDPI) (brevettata) e Real-Time Deep Memory Inspection™ (RTDMI) (per la quale è stata presentata domanda di brevetto) per offrire una sicurezza altamente efficace riconosciuta in campo industriale, SD-WAN, visualizzazione in tempo reale, rete privata virtuale (VPN) ad alta velocità e altre potenti funzioni di sicurezza.

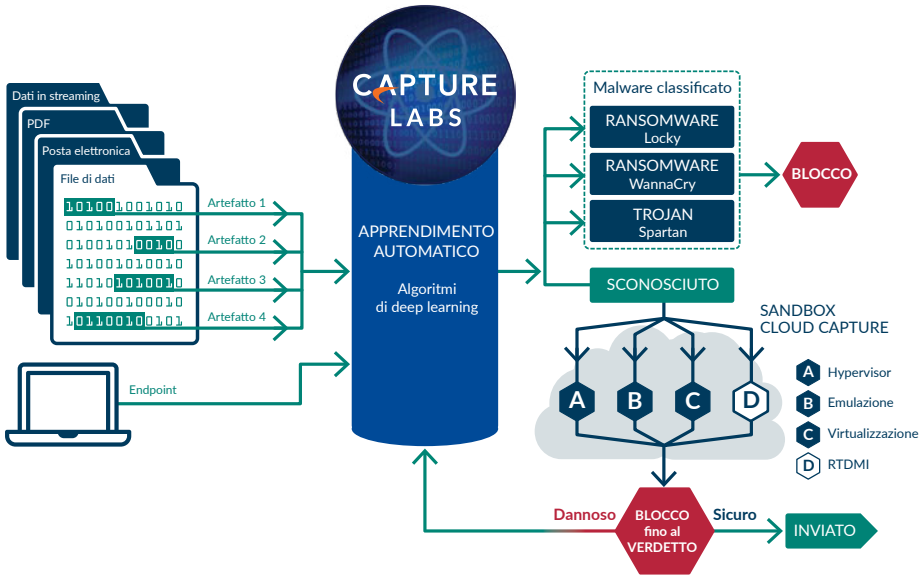
La nostra filosofia di protezione delle reti nell'attuale panorama delle minacce informatiche in continua evoluzione consiste nel rilevare e prevenire automaticamente le minacce in tempo reale. Grazie alla combinazione di tecnologie integrate basate sul cloud, i nostri firewall dispongono di una protezione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

In combinazione con questa tecnologia viene utilizzato il nostro engine RFDPI per esaminare ogni byte di ogni pacchetto, ispezionando il traffico in entrata e in uscita direttamente sul firewall. Sfruttando Capture ATP con tecnologia RTDMI, integrati nella piattaforma SonicWall Capture Cloud, oltre a funzionalità on-box come prevenzione delle intrusioni, anti-malware e filtraggio Web/URL, i nostri firewall di prossima generazione bloccano il malware, il ransomware e altre minacce a livello del gateway.

Con l'introduzione del nuovissimo sistema operativo (OS) SonicOS 7.0 le caratteristiche e le funzionalità del firewall di prossima generazione passano direttamente al livello successivo. Il nuovo sistema operativo integra SD-WAN, supporto TLS 1.3, visualizzazione in tempo reale, rete privata virtuale ad alta velocità (VPN) e altre potenti funzioni di sicurezza. Il sistema operativo SonicOS 7.0 - completamente nuovo - si caratterizza per la sicurezza avanzata, la gestione semplificata delle politiche e funzioni essenziali per il networking e la gestione, sia per le grandi imprese distribuite che utilizzano filiali SD-Branch di prossima generazione, sia per le PMI.

Pacchetti di servizi di sicurezza

I servizi di sicurezza di SonicWall trasformano il firewall in una soluzione di sicurezza completa. I servizi di sicurezza vengono proposti in tre pacchetti di abbonamento: Essential, Advanced e Premier. (i) SonicWall Essential Protection Service Suite fornisce tutti i servizi di sicurezza essenziali necessari per la protezione dalle minacce note e sconosciute. (ii) SonicWall Advanced Protection Service Suite offre una sicurezza avanzata per estendere la sicurezza della rete con servizi di sicurezza essenziali per il cloud. (iii) SonicWall Premier Protection Service Suite* offre una sicurezza totale con ulteriori servizi di sicurezza, visibilità cloud, analisi e servizi endpoint per una protezione estrema.



Disponibile prossimamente

FUNZIONE	ESSENTIAL	ADVANCED	PREMIER*
Antivirus per gateway - prevenzione intrusioni, controllo applicazioni	√	√	√
Servizio di filtraggio dei contenuti	√	√	√
Anti-spam	√	√	√
Supporto 24x7	√	√	√
Visibilità della rete	√	√	√
Sandboxing Capture ATP (Multi-Engine)	√	√	√
Tecnologia RTDMI	√	√	√
Sicurezza DNS di base	√	√	√
Gestione del cloud	!	√	√
Reportistica basata sul cloud – 7 giorni	!	√	√
Analisi avanzata del cloud – Report virtuali, 365 giorni	!	!	√
Sicurezza DNS avanzata	!	!	√
Strumento di controllo del sistema Firewall	X	X	√
Pacchetto iniziale Cloud App Security	X	X	√
Pacchetto iniziale Capture Client	X	X	√
Supporto Premier	X	!	!

√ *Parte del pacchetto*
! *Non disponibile in pacchetto, ma acquistabile separatamente*
X *Non supportato con il pacchetto*
* *Disponibile prossimamente*

Pannello di controllo migliorato

PANNELLO DI CONTROLLO MIGLIORATO	
Funzione	**Descrizione**
Pannello di controllo migliorato	Pannello di controllo con avvisi azionabili.
Visualizzazione migliorata del dispositivo con visualizzazione anteriore, posteriore e statistiche di archiviazione dell'hardware	L'utente può conoscere - dalla scheda home dell'interfaccia utente - lo stato in tempo reale del pannello anteriore, del pannello posteriore e delle statistiche di utilizzo del modulo di archiviazione. È come se l'operatore si trovasse fisicamente di fronte all'hardware.
Utilizzo in tempo reale del sistema e utilizzo della larghezza di banda	L'utente può visualizzare in tempo reale l'utilizzo da parte del sistema dell'elemento centrale e della larghezza di banda nella rete.
Sintesi della distribuzione del traffico	Utilizzo della distribuzione del traffico sul firewall dell'utente con aggiornamento in tempo reale dell'applicazione più utilizzata.
Riepilogo dei principali utenti	Riepilogo dei principali utenti in base alle sessioni autorizzate o bloccate 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.
Indicazioni sugli host infettati	Visualizzazione in tempo reale del numero totale di macchine host infettate nella rete.
Indicazioni sugli attacchi critici	Visualizzazione in tempo reale del numero totale di attacchi critici nella rete.
Indicazioni sul traffico crittografato	Visualizzazione in tempo reale del numero totale di traffico criptato nella rete.
Riepilogo delle principali applicazioni	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 dei principali indirizzi	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 dei principali utenti	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 principali valutazioni dei siti web	Visualizza le principali valutazioni dei siti web per sessione.
Riepilogo delle principali statistiche nazionali	Visualizzazione delle principali statistiche dei paesi per sessione, traffico perso, 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	Indica in tempo reale l'utilizzo della larghezza di banda da parte degli access point.
Reportistica Client WiFi	Fornisce in tempo reale report sui client Wi-Fi in base al tipo di sistema operativo, alla frequenza e alla tabella dei client principali

PANNELLO DI CONTROLLO AVANZATO (CONTINUA)	
Monitoraggio in tempo reale dei client Wifi	Individua la macchina host, il tipo di sistema operativo, la frequenza, le informazioni sugli access point e i trasferimenti di dati.
Indicazioni per acquisire i verdetti ATP	Visualizza i verdetti forniti per l'analisi dei file da parte di Capture ATP.
Indicazioni per i tipi di file	Mostra il tipo di file basato sui report Capture-ATP.
Indicazioni sull'indirizzo di destinazione	Visualizza le principali destinazioni utilizzate dai file dannosi.
Statistiche di analisi dei malware	Visualizza statistiche approfondite delle analisi del malware dinamico rispetto a quello statico per file.
Analisi dell'origine degli attacchi zero-day basata sull'ubicazione	Mostra l'origine degli attacchi per paese.
Statistiche Capture ATP	Visualizza informazioni sul totale dei file inviati, di quelli analizzati dinamicamente, di quelli nocivi e sul tempo medio di elaborazione tramite Capture ATP.
Visualizzazione della topologia di rete	Visualizza gli host, gli access point connessi alla rete dell'utente in base al nome del dispositivo, all'indirizzo mac e all'indirizzo IP
Gestione basata sulle API	La gestione del firewall è basata sulle API
Procedura guidata SDWAN	Procedura guidata per configurare automaticamente la politica SDWAN sul firewall
Centro notifiche	Nuovo centro notifiche con il riepilogo delle minacce, i registri eventi e gli allarmi di sistema.
Assistenza online migliorata	Assistenza online con collegamenti alla documentazione tecnica per tutti i modelli.
Monitoraggio SDWAN	Visualizza i dati prestazionali e le principali connessioni SD-WAN.
Utility Packet Monitor migliorata	Packet Monitor migliorato con l'inserimento delle regole di accesso, della regola NAT e delle informazioni sui percorsi.
Configurazione del dispositivo di memorizzazione	Supporto per la configurazione dei moduli di archiviazione, compresi quelli estesi. Statistiche sull'utilizzo dei moduli.
Capture Threat Assessment (CTA) 2.0	Il nuovo report CTA 2.0 supporta il nuovo modello di report con opzioni di personalizzazione come logo, nome e sezioni. Supporto per 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 registri di sistema	I registri di sistema comprendono quelli di consolle, che possono essere scaricati dalla sezione diagnostica senza che l'utente debba collegare la macchina alla porta della consolle per acquisirli. In questo modo si semplificano i metodi di debug e si riducono i tempi per la risoluzione delle anomalie.
Terminale SSH su interfaccia utente	Il terminale SSH è accessibile dall'interfaccia utente Web.
Utilità di verifica della tabella IP	Questa utility consente di controllare l'indirizzo IP sulla tabella degli IP a fini diagnostici.
Utilità di debug	L'utente può abilitare la modalità di debug dallo stesso firmware ed eseguire i comandi di debug dal terminale SSH dall'interfaccia utente.
Strumenti diagnostici di sistema	Supporto per strumenti diagnostici come GDB, HTOP e Linux Perf Tool.
Descrizione della rete degli switch	Visualizzazione degli switch SonicWall come vista fisica, vista tabulare e vista VLAN.
Larghezza di banda utilizzata dalle porte degli switch	Informazioni sulla larghezza di banda utilizzata dalle singole porte degli switch SonicWall.
Stato WWAN	Visualizzazione stato modem e rete WWAN.

Caratteristiche e servizi firewall

ENGINE REASSEMBLY-FREE DEEP PACKET INSPECTION (RFDPI)	
Funzione	**Descrizione**
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un engine di ispezione brevettato e di prestazioni elevate, 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, sia a flussi TCP primari.
Architettura altamente parallela e modulabile	L'esclusivo engine 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

Funzione	Descrizione
SD-WAN sicura	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 a prestazioni elevate 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 terzi 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 politiche di accesso del firewall.
Alta disponibilità e clustering	Supporta le modalità ad alta disponibilità Attivo/Passivo (A/P) con sincronizzazione statica, DPI[2] Attivo/Attivo (A/A) e clustering Attivo/Attivo. La modalità DPI Attivo/Attivo trasferisce il carico di lavoro dell'ispezione deep packet all'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flood SYN offre una difesa contro gli attacchi DOS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DOS/DDoS attraverso 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 sulle politiche crea percorsi basati sul protocollo per indirizzare il traffico a una connessione WAN preferita, con la possibilità di ripiegare 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 switch SonicWall	I primi switch SonicWall consentono un'integrazione senza soluzione di continuità con i firewall per la gestione da un unico pannello di controllo e la visibilità della rete
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 tramite i pannelli di gestione dei firewall per gli switch di rete serie Dell N e X.
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	Mette a disposizione un modo semplice e rapido per amministrare le politiche di sicurezza in tutti i domini di rete e la gestione delle singole politiche per un dominio o un gruppo di domini.
Supporto API completo	Supporto API completo per ogni sezione dell'interfaccia utente del firewall.
Modularità SDWAN	Interfacce tunnel modulari per le imprese distribuite.

GESTIONE, REPORTISTICA E SUPPORTO

Funzione	Descrizione
Gestione basata sul cloud e in sede	La configurazione e la gestione delle apparecchiature SonicWall sono disponibili via cloud attraverso il SonicWall Capture Security Center e in sede tramite il SonicWall Global Management System (GMS).
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 preparazione 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 il file con i risultati a cloud esterni.

RETE PRIVATA VIRTUALE (VPN)

Funzione	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 la connettività da sede a sede	La rete VPN IPSec di prestazioni elevate consente di utilizzare il firewall come concentratore di VPN per migliaia di utenti privati, filiali o altre sedi di grandi dimensioni.
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 di posta elettronica, file, computer, siti intranet e applicazioni da tutta una 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 per tutte le sessioni VPN.
VPN basata su routing	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo del tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso percorsi alternativi.
Match Object migliorato	Match Object supporta l'aggiunta di applicazioni con un'esperienza utente migliorata.
Oggetti basati su profili	Oggetti profilo per sicurezza degli endpoint, la gestione della larghezza di banda, la marcatura QoS, il filtraggio dei contenuti, l'opzione DHCP e VPN AWS.
Oggetti basati su azioni	Oggetti azione per azioni Application Rule e Content Filtering Rule Action.
Regole di accesso migliorate	Visualizzazione migliorata delle regole per un'esperienza utente intuitiva
Impostazioni tabella personalizzabili	Colonne personalizzabili e mobili secondo le regole di accesso, le regole NAT e le regole di routing.
Visualizzazione delle regole attive e inattive	Visualizza le regole abilitate e quelle disabilitate.
Visualizzazione regole utilizzate e non utilizzate	Visualizza le regole che vengono utilizzate attivamente e quelle che non vengono utilizzate.
Esportazione regole di accesso	Esporta tutte le regole di accesso in un file CSV.
Contatore in tempo reale sulle regole di accesso	Consente di acquisire statistiche in tempo reale sulle regole di accesso.
Diagramma delle regole	Visualizzazione grafica di una particolare regola di accesso, NAT e di routing che aiuta a trovare statistiche in tempo reale.
Profilo di sicurezza in una regola di accesso	Possibilità di aggiungere un profilo di sicurezza a una regola per consentire o bloccare DPI, DPI-SSL, Botnet e Geo-IP.
Regole di sicurezza dell'endpoint	Possibilità di aggiungere regole di sicurezza per la sicurezza degli endpoint usando Capture Client.

SENSIBILITÀ AL CONTESTO E AL CONTENUTO

Funzione	Descrizione
Tracciamento delle attività degli utenti	Le tecnologie AD/LDAP/Citrix1/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 associati a un indirizzo IP. Elimina il filtraggio non voluto degli indirizzi IP dovuto ad errata classificazione.
Corrispondenza e filtraggio regolare delle espressioni	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati.

Servizi in abbonamento per la prevenzione delle violazioni

CAPTURE ADVANCED THREAT PROTECTION[1]

Funzione	Descrizione
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che comprende 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 completa sulle attività dannose
Real-Time Deep Memory Inspection (RTDMI™)	RTDMI di SonicWall è una tecnologia e un processo per i quali è stata presentata domanda di brevetto, utilizzati dal Capture Cloud di SonicWall per identificare e ridurre anche le più insidiose minacce moderne, tra cui le future manifestazioni di Meltdown. La tecnologia rileva e blocca i malware che non evidenziano comportamenti dannosi e nascondono il loro armamentario tramite 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 file	Supporta l'analisi di un'ampia gamma di tipi di file, compresi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, tra cui Windows, Android, Mac e ambienti multi-browser.
Distribuzione rapida delle segnature	Quando un file viene identificato come dannoso, viene immediatamente distribuita una segnatura ai firewall con abbonamento a SonicWall Capture ATP, ai database delle segnature per Gateway Anti-Virus e IPS, nonché ai database di URL, IP e reputazione dei domini.
Capture Client	Capture Client utilizza un engine statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.

PREVENZIONE DELLE MINACCE CRITTOGRAFATE

Funzione	Descrizione
Decrittazione e ispezione TLS/SSL	Esegue la decrittazione e l'ispezione del traffico crittografato TLS/SSL in tempo reale, senza proxy, di malware, intrusioni e fughe di dati, e applica politiche di controllo di applicazioni, URL e contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato. Opzione compresa negli abbonamenti di sicurezza per tutti i modelli tranne SOHO. Per quest'ultimo viene venduta come licenza separata.
Ispezione SSH	La Deep Packet Inspection di SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano SSH.
Supporto TLS 1.3	Supporto per TLS 1.3 per migliorare la sicurezza generale sul firewall. Questo è implementato in Firewall Management, SSL VPN e DPI.

PREVENZIONE DELLE INTRUSIONI[1]

Funzione	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le segnature e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di attacchi e vulnerabilità.
Aggiornamenti automatici delle segnature	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)	Questa opzione 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 sfruttano i protocolli noti per tentare di eludere il controllo IPS.
Protezione zero-day	Protegge la rete dagli attacchi zero-day con 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.

PREVENZIONE DELLE MINACCE[1]

Funzione	Descrizione
Antimalware a livello del gateway	L'engine 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 illimitate 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 segnature delle minacce, viene consultato per ottimizzare le capacità del database di segnature integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte dell'engine 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	L'engine RFDPI esegue la scansione dei flussi TCP primari su qualsiasi porta e bidirezionalmente per rilevare e prevenire le minacce in entrata e in uscita.
Ampia compatibilità con i protocolli	Identifica protocolli comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri, che non inviano dati in TCP primari. Decodifica i payload per l'ispezione del malware, anche se non funzionano su porte standard e ben note.

INTELLIGENZA E CONTROLLO DELLE APPLICAZIONI[1]

Funzione	Descrizione
Controllo delle applicazioni	Controlla le applicazioni, o le singole funzioni delle stesse, identificate dall'engine RFDPI utilizzando un database in continua espansione, contenente migliaia di segnature di applicazioni. Ciò aumenta la sicurezza della rete e ne migliora la produttività.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate, definendo segnature basate su parametri specifici o pattern esclusivi delle singole applicazioni nelle comunicazioni di rete. Ciò consente un ulteriore controllo della 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 azioni con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/Terminal Services/Citrix.

FILTRAGGIO DEI CONTENUTI[1]	
Funzione	**Descrizione**
Filtraggio dei contenuti interno ed esterno	Attua le politiche 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.
Filtraggio contenuti applicato al client	Estende l'applicazione delle politiche per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	Bloccano i 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.
Cache Web	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.
Risponditore CFS locale	Il risponditore CFS locale può essere utilizzato come dispositivo virtuale in cloud privati basato su VMWare o Microsoft Hyper-V, mettendo a disposizione l'opzione di flessibilità di installazione (Light weight VM) del database di classificazioni CFS in diversi casi di utilizzo della rete dei clienti che richiede una soluzione interna dedicata che acceleri la richiesta di classificazioni CFS e i tempi di risposta, supporta un gran numero di URL consentiti e bloccati (oltre 100.000) e aggiunge fino a 1000 firewall SonicWall per i controlli di valutazione CFS.
ANTIVIRUS E ANTISPYWARE APPLICATI[1]	
Funzione	**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	La distribuzione e l'installazione macchina per macchina dei client antivirus e antispyware sono automatizzate sull'intera rete, il che riduce al minimo l'impegno amministrativo.
Antivirus di prossima generazione	Capture Client utilizza un engine statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
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	
Funzione	**Descrizione**
Sicurezza DNS avanzata	La sicurezza DNS offre TTD (tempo necessario per la rilevazione Time to Detect) migliore e TCO (Total Cost of Ownership, costo totale della proprietà) avanzato. La sicurezza DNS ispeziona i campi DNS per identificare domini dannosi e quindi bloccare la connessione in una fase molto precoce della stessa. SonicWall dispone di petabyte di dati sulle minacce che aiutano a classificare il dominio come dannoso, riducendo i falsi positivi.
Strumento di controllo del sistema Firewall	Identifica i rischi e migliora la conformità e la sicurezza. Disponibile sull'interfaccia utente del firewall, lo strumento Heath Check monitora costantemente in tempo reale le infrastrutture di sicurezza, i gateway, le tecnologie, le politiche e le impostazioni di configurazione.
Visibilità della rete	Fornisce visibilità granulare della topologia della rete insieme alle informazioni dell'host
Gestione del cloud	Gestisce i firewall via cloud tramite la funzione Network Security Manager di Capture Security Center
Reportistica basata sul cloud	Comprende sette giorni di reportistica basata sul cloud

[1] *Richiede un abbonamento aggiuntivo*

Servizi attivati dai partner

Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni su www.sonicwall.com/PES.

SonicWall

SonicWall fornisce soluzioni di cybersecurity illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com

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

Datasheet-SonicOSplatform-COG-2584