IL RISCHIO NASCOSTO DEI FIREWALL MODERNI

Scopri come evitare che il tuo firewall venga sfruttato dai cybercriminali durante un attacco

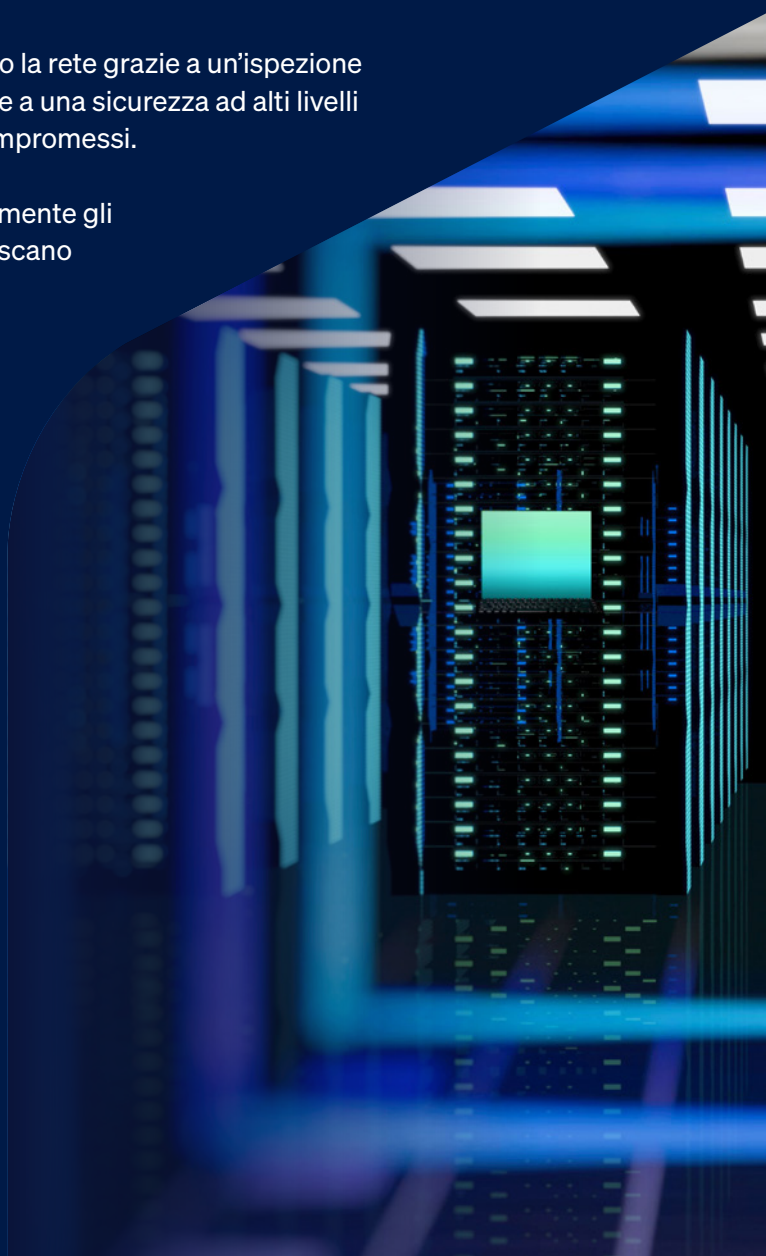
Riepilogo

I firewall di rete affrontano una quantità di attacchi mirati senza precedenti. Quasi ogni giorno i titoli di testa riportano notizie di exploit legati a nuove vulnerabilità dei firewall, rivelando una verità preoccupante: i firewall (ovvero gli stessi sistemi progettati per tutelare le reti) rappresentano un rischio significativo e sono diventati i bersagli principali di cybercriminali estremamente sofisticati[1]. Questi attacchi non sfruttano solo le vulnerabilità intrinseche del software del firewall, ma anche punti deboli fondamentali nell'approccio delle organizzazioni alla protezione della rete.

Questo white paper presenta un framework completo, basato su tre pilastri, per la moderna protezione della rete, pensato per affrontare le minacce prima, durante e dopo la loro esecuzione:

- **Protezione avanzata:** riduci proattivamente la tua superficie di attacco attraverso i principi dell'approccio Secure by Design, l'applicazione automatizzata delle patch, il controllo delle configurazioni e il controllo di accesso Zero Trust.
- **Protezione:** blocca le minacce prima che raggiungano la rete grazie a un'ispezione avanzata, al rilevamento delle minacce basato sull'IA e a una sicurezza ad alti livelli di performance, che non ti costringe a scendere a compromessi.
- **Rilevamento e risposta:** identifica e isola automaticamente gli active adversary che operano nella rete prima che riescano a portare a termine un attacco.

La maggior parte delle soluzioni di protezione della rete si concentra principalmente sulla sicurezza, lasciando vulnerabilità scoperte nell'infrastruttura della rete; inoltre, non include capacità adeguate di identificazione e risposta a un attacco in corso. Questo white paper offre ai professionisti della protezione della rete e ai team IT una roadmap pratica per implementare con efficacia tutti e tre i pilastri.



Il panorama attuale delle minacce

I firewall sono sotto assedio

I firewall di rete si collocano sulla linea di confine tra le reti interne attendibili e il mondo esterno, il quale è ostile per natura. Questa posizione privilegiata li rende bersagli di altissimo valore. I titoli dei giornali documentano un ritmo incessante di attacchi ai danni dei principali vendor di firewall, alcuni dei quali approfittano di vulnerabilità già note ma alle quali non sono state applicate patch negli ambienti di produzione; altri invece prendono di mira configurazioni predefinite non ottimali, o difetti di progettazione che creano punti deboli che possono essere sfruttati[2].

Frontier AI ha gettato ulteriore benzina sul fuoco per quanto riguarda gli attacchi informatici guidati dall'IA agentica. Il modello Claude Mythos di Anthropic ha individuato oltre 2.000 nuove vulnerabilità zero-day in poche settimane, preannunciando una svolta decisiva sia per gli hacker che per i team di sicurezza.

Mentre i titoli su Frontier AI si concentrano sulla capacità dell'IA di individuare vulnerabilità su larga scala, l'aspetto più rilevante riguarda il modo in cui l'IA riesce a ridurre i tempi di risposta, accorciando il lasso di tempo che intercorre tra l'individuazione di una vulnerabilità e l'impatto sulle attività aziendali. Permette agli autori degli attacchi di agire più rapidamente, su scala più ampia e con meno attrito rispetto al passato.

Le conseguenze si estendono ben oltre le singole organizzazioni. Quando i cybercriminali riescono a compromettere un firewall, non ottengono solo l'accesso diretto alla rete, ma potenzialmente anche le credenziali e l'accesso ai fornitori e ai clienti dell'organizzazione, entrando di fatto in possesso delle "chiavi del regno".

+ di 2.000

Numero di vulnerabilità zero-day scoperte da Mythos in appena sette settimane

I tre pilastri della protezione della rete

Una protezione della rete efficace richiede un approccio a 360 gradi, che affronti le minacce lungo il loro intero ciclo di vita: prima, durante e dopo la loro distribuzione. Questo genera tre pilastri di difesa distinti ma interconnessi:

PROTEZIONE AVANZATA

RIDUCI LA SUPERFICIE DI ATTACCO

Progetta, sviluppa e mantieni soluzioni per diminuire il rischio, ridurre l'esposizione e rafforzare la sicurezza della tua infrastruttura contro gli attacchi.

PROTEZIONE

BLOCCA GLI ATTACCHI PRIMA CHE RIESCANO A INFILTRARSI NELLA RETE

Implementa la migliore protezione possibile per identificare e impedire a cybercriminali ed exploit di infiltrarsi nella rete

RILEVAMENTO E RISPOSTA

BLOCCA GLI ATTACCHI ATTIVI SUL NASCERE

Utilizza funzionalità di rilevamento e risposta per identificare e isolare automaticamente un active adversary

Il divario critico

La maggior parte dei firewall di rete si concentra quasi esclusivamente sulla protezione in tempo reale, come il filtro del traffico, la prevenzione delle minacce e i sistemi di prevenzione delle intrusioni. Sebbene queste funzionalità siano essenziali, concentrarsi unicamente sull'ispezione del traffico in tempo reale lascia le organizzazioni esposte alle vulnerabilità.

I titoli dei giornali dimostrano che la maggior parte dei firewall e dei team IT non riesce a rafforzare la sicurezza del proprio ambiente in modo efficace, ovvero non è in grado di ridurre la superficie di attacco. I firewall rimangono vulnerabili, la "stanchezza da patch" è diffusa, i prodotti End-of-Life continuano a occupare posizioni privilegiate e le VPN di accesso remoto continuano a dominare nonostante le loro lacune di sicurezza. Nel frattempo, le funzionalità di rilevamento e risposta per fermare gli attacchi attivi prima che possano produrre un impatto sono spesso del tutto assenti nella maggior parte delle distribuzioni di firewall.

Per correggere questo squilibrio è necessaria una focalizzazione mirata sui pilastri trascurati, in particolar modo sulla protezione avanzata, che costituisce la base di un profilo di sicurezza effettivamente resiliente.

Protezione avanzata dell'infrastruttura di rete - Riduzione del rischio

La protezione avanzata consiste nel ridurre in modo proattivo la superficie di attacco, eliminando i punti deboli prima che i cybercriminali possano individuarli e sfruttarli.

Strategie essenziali di protezione avanzata

1. **Riduci al minimo l'esposizione:** controlla regolarmente i sistemi e le infrastrutture connessi a Internet e, di conseguenza, riduci il numero di potenziali punti di ingresso.

2. **Assicurati che i sistemi siano Secure by Design:** scegli prodotti realizzati considerando la sicurezza come principio fondamentale di progettazione.

3. **Controlla la configurazione e mantieni aggiornati software e firmware:** mantieni una corretta igiene della sicurezza attraverso un monitoraggio continuo.

4. **Elimina le identità compromesse come vettore di attacco:** Isola l'accesso e l'autenticazione. Implementa l'autenticazione multifattoriale (MFA) a livello universale e sostituisci la VPN con Zero Trust Network Access (ZTNA).

Riduci al minimo l'esposizione

Controlla regolarmente la tua infrastruttura di rete e valuta in quale fase del ciclo di vita si trova ogni componente. Se un componente si sta avvicinando all'End-of-Life, pianificane la sostituzione in modo proattivo. Il costo del rinnovo delle tecnologie obsolete è decisamente inferiore rispetto al potenziale impatto di un attacco ransomware che sfrutta sistemi non più supportati.

Questa è anche un'opportunità per semplificare e consolidare la tua infrastruttura di rete. Se utilizzi dispositivi separati per firewall, VPN, ZTNA, SD-WAN, DNS e filtro web, valuta la possibilità di riunire tutte queste funzionalità in un'unica piattaforma. Ridurre il numero di dispositivi e soluzioni nel tuo ambiente può diminuire la complessità, migliorare l'efficienza e rafforzare la resilienza complessiva.

È altrettanto importante mantenere aggiornata la tua infrastruttura. Gli aggiornamenti di firmware e software includono spesso patch di sicurezza critiche per vulnerabilità, che potrebbero essere sfruttate dagli autori degli attacchi. Sebbene applicarle possa richiedere del tempo, si tratta di un'attività decisamente meno destabilizzante rispetto a dover affrontare le conseguenze di un attacco ransomware.

Assicurati che i sistemi siano Secure by Design

Le aziende hanno bisogno di prodotti sicuri tanto quanto hanno bisogno di prodotti per la sicurezza.

Il settore della cybersecurity deve fare i conti con una verità fondamentale: le aziende hanno bisogno di prodotti sicuri tanto quanto hanno bisogno di prodotti per la sicurezza. Quando i cybercriminali prendono di mira gli strumenti creati per proteggere le organizzazioni, queste ultime hanno bisogno di prodotti di sicurezza che siano essi stessi sicuri. Le aziende devono premiare i vendor che dimostrano un impegno sincero nei confronti della sicurezza e della trasparenza, compresa la comunicazione chiara e tempestiva di eventuali violazioni: l'approccio corretto, anche quando è scomodo.

I principi chiave di Secure by Design includono:

- MFA è integrato in tutti i sistemi di default.
- Eliminazione di password e credenziali predefinite.
- Implementazione di patch di sicurezza automatizzate che riducono al minimo i disagi.
- Procedure di segnalazione delle vulnerabilità rapide e trasparenti.
- Controlli di sicurezza periodici e penetration test.
- Pratiche del ciclo di vita dello sviluppo sicure, integrate nell'ingegnerizzazione del prodotto.

Controllo della configurazione e aggiornamento costante dei sistemi

I firewall di rete sono complessi, il che li rende inclini a errori di configurazione e impostazioni rischiose, che possono creare punti di ingresso involontari per gli autori degli attacchi. La sfida consiste nel capire quali elementi sono configurati in modo errato e dove si trovano tali vulnerabilità. A volte il problema è evidente, ma più spesso le falle rimangono nascoste finché non vengono soggette a exploit. La maggior parte dei firewall non fornisce alcun tipo di informazione sulle impostazioni di configurazione che potrebbero comportare dei rischi. Scegline uno che lo faccia.

Lo stress da applicazione delle patch è una realtà, ma non è detto che debba per forza essere così. I tradizionali processi di applicazione delle patch implicano un notevole carico operativo. Le vulnerabilità di sicurezza possono essere individuate in qualsiasi momento e ora, grazie all'intelligenza artificiale, a un ritmo allarmante. La frequenza degli aggiornamenti richiesti può mettere a dura prova i team di amministrazione. Gran parte dei firewall promette "aggiornamenti automatici", ma in genere richiedono comunque che gli amministratori pianifichino tempi di inattività, installino il firmware e riavviino i dispositivi.

Le organizzazioni dovrebbero porsi una semplice domanda: perché l'applicazione delle patch non può essere davvero automatica? La risposta è che la maggior parte dei vendor non ha progettato il proprio software per supportare aggiornamenti di sicurezza in tempo reale e over-the-air. Tuttavia, i moderni approcci architetturali possono consentire l'uso di funzionalità di hotfix automatizzate in grado di:

- Applicare le patch di sicurezza automaticamente, senza l'intervento dell'amministratore.
- Non richiedere tempi di inattività dei sistemi o riavvii.
- Colmare il divario tra i rilasci principali del firmware.
- Ridurre il periodo di vulnerabilità, portandolo da diversi mesi a pochissime ore o giorni.

Gli errori di configurazione rappresentano un altro punto di ingresso comunemente sfruttato dai cybercriminali. Set di regole del firewall complesse, modifiche delle policy scarsamente documentate e scostamenti nella configurazione nel corso del tempo possono inavvertitamente lasciare aperti dei punti di ingresso che dovrebbero invece essere messi in sicurezza.

La sfida consiste nell'identificazione: come fanno gli amministratori a capire quali elementi non sono configurati correttamente? I firewall tradizionali non offrono alcuna visibilità sulla sicurezza della configurazione. Gli approcci moderni includono funzionalità di controllo dell'integrità automatiche in grado di:

- Controllare ininterrottamente la configurazione del firewall, confrontandola con best practice consolidate e parametri di riferimento di CIS.
- Fornire nella dashboard visibilità sui controlli superati e non superati.
- Assegnare un livello di gravità a ciascun elemento valutato.
- Consentire l'analisi dettagliata per regolare rapidamente le impostazioni o documentare eccezioni intenzionali.

Queste funzionalità offrono una visibilità di cui i firewall tradizionali sono privi, garantendo che il profilo di sicurezza rimanga ottimale anche a fronte dell'evoluzione delle configurazioni nel tempo.

Eliminazione delle identità compromesse come vettore di attacco

Il 67% degli incidenti analizzati da Sophos nel 2025 è iniziato con la compromissione di credenziali legittime[3], rendendo l'eliminazione degli attacchi basati sull'identità una priorità fondamentale per poter difendere i sistemi con una protezione avanzata. Questa realtà richiede l'adozione dei principi dell'approccio Zero Trust: Mai fidarsi di niente, meglio controllare tutto.

Le organizzazioni che si affidano ancora alle VPN di accesso remoto devono considerare come priorità assoluta la migrazione da queste soluzioni. ZTNA offre un'alternativa moderna alla VPN che rispetta i principi dell'approccio Zero Trust. Anziché concedere un accesso esteso alla rete, ZTNA fornisce accesso mirato ad applicazioni e risorse specifiche. Se un dispositivo viene compromesso, ZTNA può limitare o bloccare automaticamente l'accesso finché non viene ripristinata l'integrità del dispositivo.

Anche se un cybercriminale dovesse compromettere un dispositivo connesso tramite ZTNA, avrebbe accesso solo alle applicazioni specifiche a cui quell'utente è autorizzato ad accedere, non all'intera rete. Il perimetro di sicurezza si sposta proprio dove è richiesto: attorno alle applicazioni e ai dati critici.

67%

Percentuale di incidenti analizzati da Sophos nel 2025 che hanno avuto inizio con la compromissione di un'identità

ZTNA offre sei vantaggi chiave rispetto alla VPN:

1. **MFA obbligatoria:** l'autenticazione multifattoriale (MFA) è richiesta per tutti gli accessi, senza eccezioni, eliminando così il rischio che i cybercriminali sfruttino la compromissione delle credenziali e gli attacchi brute force come possibili vettori di attacco.

2. **Inclusione dell'integrità del dispositivo nelle policy di accesso:** la conformità e lo stato di integrità dei dispositivi vengono valutati continuamente nell'ambito delle decisioni relative all'accesso.

3. **Funziona ovunque:** ZTNA funziona altrettanto bene sia che gli utenti si trovino fisicamente all'interno della rete aziendale, sia che lavorino da remoto, garantendo una sicurezza uniforme, indipendentemente dalla loro posizione geografica.

4. **Connettività trasparente:** le moderne implementazioni ZTNA offrono connessioni trasparenti e affidabili, senza i problemi di connessione che spesso affliggono le VPN.

5. **Migliore visibilità:** le organizzazioni ottengono una visibilità chiara sulle risorse alle quali accedono gli utenti, il che permette di pianificare meglio la capacità e di gestire le licenze con più efficienza.

6. **Maggiore facilità di amministrazione:** con ZTNA, l'aggiunta e la rimozione di utenti, la distribuzione di nuove applicazioni e la gestione delle policy di accesso sono tutte operazioni decisamente più semplici rispetto a una VPN tradizionale.

Le strategie di protezione avanzata devono includere l'eliminazione delle VPN di accesso remoto e l'implementazione di un'architettura Zero Trust con l'applicazione universale della MFA.

Protezione - Blocco delle minacce a livello del gateway

Implementa una protezione completa per identificare e bloccare le minacce prima che raggiungano la rete. Questo pilastro include l'ispezione TLS avanzata, il rilevamento delle minacce zero-day basato sull'IA e l'analisi intelligente del traffico, che garantisce alti livelli di performance senza scendere a compromessi sulla sicurezza.

I moderni requisiti di protezione

- **Ispezione TLS 1.3 ad alta performance:** ormai, la maggior parte del traffico web è crittografata e gli autori degli attacchi nascondono sempre più frequentemente malware e traffico di comando e controllo all'interno di canali crittografati. I firewall devono eseguire la decrittografia e l'ispezione del traffico TLS in modo intelligente, applicando regole basate sulle policy che bilancino i requisiti di sicurezza con le esigenze di privacy e l'impatto sulla performance.

- **Accelerazione dell'hardware:** le operazioni di crittografia e l'ispezione del traffico richiedono un uso intensivo di risorse computazionali. Le moderne architetture firewall dovrebbero trasferire le applicazioni attendibili e le operazioni di crittografia su percorsi di accelerazione dell'hardware, liberando risorse per un'analisi approfondita del traffico non attendibile.

- **Protezione contro le minacce zero-day basata sull'IA:** il rilevamento basato sulle firme è ancora utile, ma da solo non basta contro le nuove minacce. L'analisi dei file statici basata sull'IA, abbinata al sandboxing dinamico in fase di esecuzione, permette di identificare e bloccare le minacce zero-day prima che raggiungano la rete. Queste sono minacce che sfuggirebbero completamente ai tradizionali sistemi basati sulle firme.

SIA le capacità di protezione CHE la performance devono migliorare col tempo, non peggiorare. I firewall basati su architetture programmabili possono ricevere potenziamenti sia sul fronte della protezione che della performance attraverso aggiornamenti del software, prolungando così il ciclo di vita effettivo degli investimenti hardware. A differenza dei firewall tradizionali, che tendono a rallentare man mano che vengono aggiunte nuove funzionalità di sicurezza, le architetture moderne mantengono o migliorano la performance grazie a un'ottimizzazione continua.

Rilevamento e risposta - Blocco degli attacchi attivi

Quando gli active adversary riescono a penetrare le difese, il rilevamento della loro presenza è immediato e la minaccia viene contenuta automaticamente. Network Detection and Response (NDR), unito al coordinamento tra i vari prodotti, è in grado di identificare e isolare i sistemi compromessi prima che i cybercriminali raggiungano i loro obiettivi.

Network Detection and Response (NDR)

Network Detection and Response utilizza l'intelligenza artificiale e l'analisi del comportamento per identificare gli active adversary già presenti nella rete. A differenza delle difese perimetrali che analizzano il traffico in entrata, NDR esamina i pattern del traffico interno della rete, alla ricerca di eventuali indicatori di compromissione:

- Movimenti laterali insoliti tra i sistemi.
- Comunicazioni di comando e controllo verso host esterni sospetti.
- Pattern di accesso ai dati anomali.
- Tentativi di privilege escalation.
- Attività di ricognizione volte ad analizzare le risorse interne.

NDR è sempre stata una funzionalità di classe Enterprise che richiedeva prodotti distinti e investimenti significativi. Le organizzazioni più lungimiranti stanno ora integrando funzionalità NDR direttamente nelle piattaforme firewall, il che rende questa capacità critica accessibile anche alle aziende di medie dimensioni.

Risposta automatica

Il rilevamento senza risposta si limita a informare gli amministratori che il sistema è stato compromesso. E spesso questo avviene troppo tardi per poter evitare danni. Le funzionalità di risposta automatizzata permettono di contenere il pericolo all'istante.

Quando viene rilevata una minaccia in qualsiasi punto dell'infrastruttura di sicurezza (che sia grazie al firewall, alla protezione endpoint o delle e-mail, oppure a un analista MDR) occorre una soluzione di sicurezza che coordini una risposta automatizzata su tutti i prodotti di sicurezza integrati. Una strategia simile può impedire a un dispositivo compromesso di comunicare con altri sistemi, bloccarne l'accesso alle applicazioni e ai dati, e impedirne i movimenti laterali.

Questa risposta automatica è particolarmente utile fuori dal normale orario di lavoro, ovvero quando ha inizio l'88% degli attacchi ransomware[4]. Considera lo "scenario del venerdì sera": un cybercriminale riesce a compromettere un dispositivo nella tarda serata di venerdì, quando il personale addetto alla sicurezza non è disponibile. Senza una risposta automatica, l'autore dell'attacco ha a disposizione l'intero fine settimana per spostarsi lateralmente, elevare i propri privilegi e distribuire il ransomware. L'organizzazione si accorge della violazione lunedì mattina, quando compaiono file crittografati e richieste di riscatto.

Con una risposta automatizzata e coordinata tra i vari prodotti, la prima intrusione attiva l'isolamento immediato. L'autore dell'attacco si ritrova intrappolato in un segmento di rete sottoposto a quarantena, incapace di avanzare o muoversi. Al loro rientro il lunedì mattina, i team di sicurezza troveranno un avviso attivo relativo a una minaccia già contenuta, invece di un vero e proprio attacco ransomware su larga scala.

88%

Percentuale di attacchi ransomware che ha inizio al di fuori del normale orario lavorativo

Sophos Firewall: una soluzione completa

Sebbene il framework a tre pilastri descritto qui rappresenti le best practice in materia di sicurezza, per implementarlo in modo efficace è necessario scegliere un'infrastruttura che supporti tutti e tre i pilastri.

Sophos Firewall si distingue come una delle poche soluzioni ad aver investito in modo significativo in tutti e tre gli ambiti, offrendo numerose funzionalità che gli acquirenti non troveranno altrove.

Monitoraggio dell'integrità del sistema

I team di sicurezza di Sophos monitorano costantemente tutti i sistemi distribuiti, alla ricerca di eventuali segni di attacco, accelerando i tempi di risposta e di remediation.

Controllo continuo dello stato di integrità

Identifica le configurazioni ad alto rischio confrontandole con i parametri di riferimento delle best practice, e fornisce indicazioni prioritarie per una risoluzione più rapida.

Hotfix automatici e aggiornamenti di sicurezza

Le patch di sicurezza possono essere inviate tramite push a Sophos Firewall over-the-air, e applicate automaticamente senza tempi di inattività.

Tutti gli aggiornamenti del firmware sono crittografati in modo sicuro e firmati per garantirne l'integrità e l'autenticità.

Sistemi dotati di protezione avanzata

Distribuzione sicura, fin dall'attivazione

MFA e gateway ZTNA integrati

Servizi e portali containerizzati e dotati di protezione avanzata

La protezione avanzata del kernel e del piano di controllo elimina intere categorie di vulnerabilità

Gestione remota sicura

L'accesso di gestione crittografato tramite Sophos Central elimina l'esposizione del firewall a rischi evitabili.

Per garantire la massima protezione, tutti i backup vengono archiviati in modo sicuro e sottoposti a doppia crittografia in Sophos Central.

Secure By Design

Sophos Firewall affronta il pilastro della protezione avanzata attraverso un approccio Secure by Design a 360 gradi, che elimina gli oneri solitamente associati al mantenere un'infrastruttura sicura.

Funzionalità automatica di hotfix: elimina lo stress da applicazione delle patch

L'esclusiva funzionalità di hotfix automatizzati di Sophos Firewall modifica radicalmente il periodo di esposizione alle vulnerabilità:

- Le patch di sicurezza vengono inviate automaticamente tramite push over-the-air, non appena Sophos le sviluppa e le verifica.
- Le patch vengono applicate senza alcun intervento da parte dell'amministratore.
- Non sono richiesti né tempi di inattività, né riavvii dei sistemi.
- Gli hotfix colmano il divario tra i principali rilasci del firmware, garantendo una protezione continua.

Questo vantaggio architetturale riduce il periodo di vulnerabilità, portandolo da diversi mesi a pochissime ore o giorni. Quando Sophos individua e corregge una vulnerabilità, tutti i clienti di Sophos Firewall vengono protetti immediatamente, senza dover aspettare che gli amministratori trovino spazio in agenda o pianifichino finestre di manutenzione.

Nessun altro dei principali vendor di firewall è in grado di offrire un'applicazione delle patch di sicurezza che sia davvero automatica e a zero tempi di inattività. Anche solo questa funzionalità rappresenta un miglioramento rivoluzionario per quanto riguarda il pilastro della protezione avanzata.

Controllo integrità: audit continuo della configurazione

La funzionalità Controllo integrità di Sophos Firewall offre una visibilità senza precedenti sulla configurazione:

- Verifica costantemente decine di impostazioni di configurazione dei firewall, confrontandole con parametri di riferimento di CIS e best practice di settore.
- Mostra i controlli superati e non superati, direttamente nella dashboard del Control Center.
- Assegna un livello di gravità a ogni elemento valutato (critico, alto, medio, basso).
- Consente l'analisi dettagliata per regolare rapidamente le impostazioni o documentare eccezioni intenzionali.
- Si aggiorna automaticamente, seguendo l'evoluzione delle best practice.

Questo monitoraggio proattivo delle configurazioni aiuta a mantenere un profilo di sicurezza ottimale, anche se le configurazioni cambiano nel tempo. Gli amministratori ricevono avvisi immediati sulle impostazioni potenzialmente rischiose prima che gli hacker possano individuarle e sfruttarle.

Monitoraggio remoto dell'integrità

Sophos è l'unico vendor capace di monitorare l'intera base installata dei propri Sophos Firewall. Grazie al sensore Linux integrato di Sophos Extended Detection and Response (XDR), siamo in grado di monitorare l'integrità del sistema, identificando ad esempio:

- Modifiche non autorizzate della configurazione.
- Attività di esportazione delle regole.
- Azioni di manomissione dei file.
- Tentativi di esecuzione di programmi dannosi.

Questo sensore integrato permette ai team di sicurezza di Sophos di monitorare proattivamente l'intera base installata dei clienti, alla ricerca di potenziali segni di attacco: un ulteriore livello di sicurezza che nessun altro vendor di firewall offre al momento. Quando viene rilevata una minaccia, Sophos è in grado di intervenire all'istante per aiutare i clienti a risolvere il problema, distribuendo allo stesso tempo hotfix automatici per proteggere tutti gli altri clienti.

Autenticazione multifattoriale integrata e Zero Trust Network Access

Sophos Firewall integra la MFA in tutti i punti di accesso amministrativo, e include un gateway ZTNA integrato, semplificando così l'adozione e la distribuzione di ZTNA e l'upgrade a questo nuovo sistema delle VPN di accesso remoto vulnerabili.

Massima protezione CON livelli superiori di performance

Mentre molti vendor offrono difese informatiche efficaci, Sophos Firewall garantisce un approccio diverso alla protezione, assicurando una sicurezza completa senza compromettere in alcun modo la performance, eliminando così il problema che spesso costringe le organizzazioni a disattivare funzionalità importanti.

Architettura Xstream FastPath

L'architettura Xstream programmabile di Sophos Firewall gestisce il traffico in modo intelligente, per garantire sia massima sicurezza che massimi livelli di performance**.** Questo approccio garantisce che l'attivazione di funzionalità di sicurezza complete (inclusi ispezione TLS, sandboxing e IPS) non comprometta in alcun modo la performance. Sophos Firewall integra anche una protezione zero-day basata sull'IA per identificare tempestivamente le minacce più recenti.

Miglioramenti continui della performance e della protezione

A differenza dei firewall tradizionali, che tendono a rallentare con l'aggiunta di nuove funzionalità di sicurezza, l'architettura programmabile di Sophos Firewall consente di migliorare sia la protezione, **sia** la performance con ogni aggiornamento del software. I clienti possono usufruire di ottimizzazioni continue degli hardware in cui hanno investito, senza che debbano acquistare nuovi dispositivi fisici: ottengono infatti una protezione e una performance che migliorano nel tempo, invece di peggiorare.

Rilevamento e risposta che non hanno rivali

La maggior parte dei firewall di rete non offre praticamente alcuna funzionalità di rilevamento e risposta. Una volta che un cybercriminale riesce a superare le difese perimetrali, i firewall tradizionali non hanno alcun meccanismo per individuare l'intrusione o avviare un'azione di risposta. Questa è una lacuna molto grave, che rende le organizzazioni vulnerabili agli attacchi più sofisticati.

Sophos Firewall si distingue per la sua capacità unica di offrire funzionalità automatizzate di rilevamento e risposta.

Network Detection and Response (NDR) integrata:

Network Detection and Response è sempre stata una funzionalità riservata alle grandi imprese, che richiedeva prodotti distinti e investimenti significativi. Sophos Firewall include NDR come funzionalità standard nella principale sottoscrizione di base.

Ciò permette alle organizzazioni di qualsiasi dimensione di poter adottare un sistema di rilevamento delle minacce di classe Enterprise, che garantisce che gli autori degli attacchi che riescono a superare le difese perimetrali possano essere identificati prima che possano raggiungere i loro obiettivi.

Synchronized Security: risposta automatizzata tra più prodotti

Il rilevamento senza risposta si limita a informare gli amministratori che il sistema è stato compromesso. E spesso questo avviene troppo tardi per poter evitare danni. La Synchronized Security di Sophos Firewall garantisce una risposta automatizzata e coordinata all'interno dell'intera infrastruttura di sicurezza.

Quando un prodotto Sophos (sia che si tratti del firewall, della protezione endpoint, delle e-mail o dell'area di lavoro, oppure di un analista MDR) rileva una minaccia, Synchronized Security esegue automaticamente le seguenti operazioni:

- Isola il dispositivo compromesso, impedendogli di comunicare con altri sistemi.
- Blocca l'accesso ad applicazioni e dati.
- Impedisce i movimenti laterali all'interno della rete.
- Contiene la minaccia finché i team di sicurezza non riescono a svolgere indagini e procedere con la remediation.

Lo "scenario del venerdì sera" mette in evidenza l'importanza critica della risposta automatizzata:

Senza risposta automatica: un cybercriminale riesce a compromettere un dispositivo nella tarda serata di venerdì, quando il personale addetto alla sicurezza non è disponibile. L'autore dell'attacco ha a disposizione l'intero fine settimana per spostarsi lateralmente, elevare i propri privilegi e distribuire il ransomware. L'organizzazione si accorge della violazione lunedì mattina, quando compaiono file crittografati e richieste di riscatto.

Con Synchronized Security: la violazione di sicurezza iniziale attiva immediatamente l'isolamento automatico. L'autore dell'attacco si ritrova intrappolato in un segmento di rete sottoposto a quarantena, incapace di avanzare. Al loro rientro il lunedì mattina, i team di sicurezza troveranno un avviso attivo relativo a una minaccia già contenuta, invece di un vero e proprio attacco ransomware su larga scala.

Questa capacità di risposta automatizzata è particolarmente importante per le aziende che non hanno Security Operations interne operative 24/7, ovvero proprio le aziende di medie dimensioni che i tradizionali vendor di soluzioni NDR hanno sempre trascurato.

Conclusione

I firewall di rete si trovano ad affrontare pressioni senza precedenti, con attacchi sempre più spietati. Le notizie che mettono in luce le vulnerabilità di diversi vendor importanti rivelano una verità scomoda: i sistemi progettati per difendere le reti sono diventati gli obiettivi primari di cybercriminali estremamente sofisticati.

Il framework a tre pilastri descritto in questo white paper (protezione avanzata, sicurezza, rilevamento e risposta) offre un approccio alla protezione della rete a 360 gradi, che affronta le minacce prima, durante e dopo che si verificano. Purtroppo, la maggior parte dei vendor di firewall si concentra quasi esclusivamente sulla protezione, lasciando lacune critiche nei pilastri di protezione avanzata e rilevamento e risposta.

Per implementare in modo efficace questo framework, occorre scegliere un'infrastruttura che investa in modo equilibrato in tutti e tre i pilastri. Le aziende devono valutare i vendor di firewall in base ai seguenti fattori:

- **Impegno Secure by Design**, un approccio sicuro fin dalla progettazione comprovato da fatti concreti, non solo da promesse.
- **Funzionalità di applicazione automatica delle patch** che eliminano i tempi di inattività e lo stress da implementazione delle patch.
- **Controllo della configurazione** in grado di offrire visibilità sul profilo di sicurezza.
- **Funzionalità Zero Trust integrate**, tra cui MFA e ZTNA.
- **Network Detection and Response** per identificare le minacce attive.
- **Capacità di risposta automatica** che isolino le minacce senza alcun intervento umano.

Il costo della sostituzione di un'infrastruttura obsoleta o inadeguata è nettamente inferiore a quello richiesto per riprendersi da un attacco ransomware che sfrutta vulnerabilità note. Il momento di agire è adesso, prima che sia la tua organizzazione a finire nelle news.

La sicurezza è una responsabilità condivisa. I vendor devono sviluppare prodotti sicuri. Le organizzazioni devono distribuirli correttamente, gestirli con cura e ritirarli dal servizio quando raggiungono l'End-of-Life. Se entrambe le parti adempiono alle loro responsabilità, si creerà un ecosistema decisamente più sicuro.

La domanda fondamentale che devi porti è: **il mio firewall riduce il rischio o lo aumenta?**

La risposta dipende dal fatto se la tua infrastruttura copre tutti e tre i pilastri della moderna protezione della rete, oppure se presenta lacune critiche che gli autori degli attacchi non vedono l'ora di sfruttare.

Il mio firewall riduce il rischio o lo aumenta?

1, 2, 3, 4 Active Adversary Report 2026 - Sophos.

SOPHOS

Per saperne di più su Sophos Firewall, visita **sophos.it/firewall**

Vendite per l'Italia
Tel: (+39) 02 94 75 98 00
E-mail: **sales@sophos.it**