STORMSHIELD

ARTICOLO DI OPINIONE

FIREWALL AZIENDALE: BACK TO BASICS

Stéphane Prevost
Product Marketing Manager, Stormshield

L'importanza di utilizzare un firewall nelle aziende non è più in discussione. Ma di fronte alle sofisticate minacce odierne, un firewall periferico non è più sufficiente. In un'era in cui tutto è in continua evoluzione, come integrare un firewall nell'architettura di rete? Come utilizzarlo al meglio?

Collocazione del firewall, segmentazione della rete, approccio Zero Trust, gestione e monitoraggio centralizzati: tutto quello che c'è da sapere sull'uso ottimale del firewall nell'architettura di rete.

COMPRENDERE LE ESIGENZE E IL PERIMETRO DA PROTEGGERE

Il firewall è uno dei pilastri della sicurezza perimetrale delle aziende. Storicamente concepito come un muro impenetrabile ai margini della rete, la sua funzione si è notevolmente sviluppata. In risposta all'evoluzione delle minacce e al fine di bloccare tutti i tentativi di spostamento laterale ad opera del malware, gli amministratori di sistema hanno dovuto rivedere l'uso dei firewall, aggiungendo nuovi livelli di protezione.

La giusta collocazione di un firewall nell'architettura di rete dipende dalle esigenze di sicurezza. Il firewall tradizionale ai margini della rete, pur essendo ancora una parte essenziale dell'arsenale di sicurezza, non è più sufficiente a fornire un buon livello di protezione. Infatti, l'evoluzione delle modalità lavorative (home office, lavoro da remoto, SaaS e altre infrastrutture cloud) e la sofisticazione delle minacce informatiche hanno costretto le aziende a estendere l'uso dei firewall. Oggi, è necessario fare un ulteriore passo avanti e distribuire i firewall in diverse parti del perimetro di sicurezza dell'azienda, che è però in continua evoluzione e composto da elementi eterogenei, sia interni che esterni.

Ma allora, **qual è la collocazione strategica di un firewall?** Ai margini di Internet, nel cuore della rete, nel cloud... le possibilità sono molteplici e variano a seconda degli obiettivi di sicurezza e della capacità dei firewall. In linea con il principio della difesa in profondità, è consigliabile installare almeno due firewall per creare una zona di sicurezza (DMZ, *demilitarized zone*). Una doppia barriera che offre un filtro aggiuntivo a livello di flussi (potenzialmente dannosi). L'obiettivo è creare diversi livelli di fiducia, da Internet alla LAN, fino ai data center e ad altri ambienti cloud.

E i firewall di nuova generazione (NGFW) possono portare la sicurezza dell'architettura di rete ancora più avanti, in particolare con la segmentazione della rete e l'approccio *Zero Trust*. Ecco come funziona.

L'IMPORTANZA DELLA SEGMENTAZIONE DELLA RETE E DELL'APPROCCIO *ZERO TRUST*

Perché è così importante segmentare le reti? Perché il modus operandi dei criminali informatici prevede una fase di ricognizione. Una volta compromesso e infiltrato un computer, scansionano le apparecchiature collegate alla rete preparandosi un eventuale attacco. Per evitare che progrediscano, è necessario applicare una rigorosa segmentazione sulla rete principale e sulle sottoreti. Dividendo il tutto in zone distinte, l'amministratore può applicare un controllo rigoroso sugli accessi e sui flussi.

La creazione di una DMZ, come già detto, è un «*caso particolare della segmentazione*», secondo Simon Dansette, Product Manager di Stormshield. «*Offre il vantaggio di poter compartimentare la rete per un'esigenza specifica, bloccando tutte le possibilità di spostamento laterale*». E, come sottolinea **Sébastien Viou,** Direttore di Cybersecurity e Product Management di Stormshield, «*l'interruzione del protocollo è un principio progettato per fermare tutti i flussi di rete, di trasporto e di applicazione per consentirne l'interpretazione e la riscrittura. In sostanza, deve essere impossibile eseguire il routing diretto tra i due firewall*». Il principio della doppia barriera non consiste quindi nell'impilare

diversi firewall «*pensando che il primo sopperisca alle vulnerabilità dell'altro*», ma piuttosto «*nel creare zone di fiducia e applicare regole di sicurezza coerenti durante il controllo degli scambi*». Negli ambienti industriali sensibili, questa segmentazione della rete consente di intraprendere diverse azioni. Da una parte, isola gli ambienti IT e OT, bloccando così il movimento laterale del ransomware che infetta un'infrastruttura IT e cerca di diffondersi negli ambienti di produzione. Dall'altra, la segmentazione può arrivare fino al cuore del sistema OT, il più vicino possibile alle macchine e ai PLC, con l'applicazione di un filtraggio granulare dei flussi, fino al comando inviato.

Per garantire la legittimità degli utenti e delle macchine che si connettono alle reti, le aziende possono anche adottare l'approccio ***Zero Trust,* che si basa sul principio che gli utenti e gli asset della rete non devono essere considerati affidabili di default, ma devono dimostrare la propria identità e legittimità ogni volta che richiedono l'accesso alle risorse**. L'architettura *Zero Trust Network Access* (ZTNA) include sia gli utenti che i dispositivi nell'autenticazione e nell'autorizzazione dell'accesso alla rete. L'accesso è quindi granulare e specifico per le esigenze dell'utente. «*In un'architettura Zero Trust, il firewall deve innanzitutto integrarsi con tecnologie di autenticazione forte per identificare l'utente. Ma deve anche verificare che la workstation da autenticare sia sana*», spiega Simon Dansette. È grazie a questa filosofia che i più recenti modelli di firewall consentono di applicare il controllo dell'accesso degli utenti, anziché filtrare esclusivamente sulla base dell'IP (come facevano i firewall tradizionali). Le regole di filtraggio del traffico possono quindi essere utilizzate per implementare politiche di sicurezza granulari e in tempo reale. Per Simon Dansette, «*oggi esistono interazioni tra le soluzioni di tipo EDR e i firewall per autorizzare un utente a connettersi. Sono questi meccanismi che consentono di portare avanti il processo di autenticazione.*» Il firewall di nuova generazione diventa quindi un elemento chiave dell'architettura Zero Trust.

Applicazione di regole specifiche o comuni, aggiornamento dei dispositivi, monitoraggio e supervisione, che siano fisici o virtualizzati: la proliferazione dei firewall nelle aziende costringe gli amministratori di sistema a ripensare la loro gestione, passando da una visione unitaria a una centralizzata. Uno strumento ormai indispensabile.

L'INDISPENSABILE GESTIONE CENTRALIZZATA DEI FIREWALL

Che si trovino ai margini o nel cuore di una rete, vicino alle apparecchiature industriali o ospitati nel cloud, il numero di firewall e la loro ubicazione si sono moltiplicati a tal punto che la loro gestione può risultare molto complessa. Distribuzione, configurazione, manutenzione, gestione delle patch... Secondo Simon Dansette, la gestione centralizzata consente di «*ridurre la complessità della gestione delle varie connessioni ai firewall e di ridurre i tempi di amministrazione della rete, e quindi i relativi costi*».

La gestione centralizzata semplifica anche il processo di conformità alla sicurezza,

garantendo che tutti i criteri di sicurezza siano applicati in modo uniforme a tutti i firewall della rete. Per gli MSSP e i rivenditori IT, questo è un vero vantaggio. Infatti, **la gestione centralizzata consente di gestire la configurazione di diversi firewall con un unico strumento e di amministrarli tutti da un'unica piattaforma**. Qualsiasi modifica può così essere apportata in modo rapido e semplice, garantendo sia la sicurezza dei clienti sia l'aumento della produttività dei team.

La centralizzazione della gestione dei log consente inoltre di visualizzare gli indicatori in un'unica interfaccia, facilitando il monitoraggio e la generazione di report. Se i log vengono raccolti, memorizzati e archiviati in un'unica piattaforma, l'amministratore di sistema può trovare e correggere più facilmente i problemi di configurazione. Secondo Simon Dansette, «*la centralizzazione fornisce una visione d'insieme che rende più facile analizzare dove si trova il problema e quindi andare a correggerlo sul firewall incriminato. Di conseguenza, la fase di risoluzione dei problemi è più semplice per gli amministratori di sistema e consente di risparmiare tempo nei momenti di maggiore stress*».

E domani? Risulta evidente che non sono solo i punti di protezione della rete a moltiplicarsi nelle aziende; anche i punti di protezione degli endpoint stanno seguendo la stessa tendenza. Tuttavia, la ricorrente constatazione del successo degli attacchi informatici dimostra la scarsa efficacia di questo approccio. Questo perché la proliferazione delle soluzioni di rilevamento genera eventi multipli e copiosi, con comportamenti difficili da interpretare e correlare per gli amministratori. Questa mancanza di visibilità limita la reattività e, nella pratica, si traduce in un livello di protezione inferiore. Proprio in risposta a questa situazione e al fine di offrire una gestione più completa, sono state sviluppate le soluzioni XDR (*eXtended Detection & Response*). La loro promessa è triplice: ridurre i rischi, correlare gli eventi segnalati dalle varie soluzioni di sicurezza informatica e migliorare la produttività operativa informatica delle organizzazioni.