FORTINET

Tenere gli hacker lontani dall'edge

Indice

Sintesi Esecutiva

Oggi gli utenti hanno bisogno di una rete che consenta di connettersi a qualunque risorsa da ogni luogo e dispositivo. Contestualmente, le reti dei data center e dei campus richiedono un'architettura IT ibrida, che si adatti a filiali di nuova generazione, reti multi-cloud private e pubbliche, lavoratori remoti e soluzioni Software-as-a-Service (SaaS) basate sul cloud. Di conseguenza, i team di sicurezza aziendali hanno il difficile compito di fornire una visibilità completa su un ambiente di rete in movimento e distribuito, al fine di proteggere e tracciare ogni utente e dispositivo che accede a dati, applicazioni e carichi di lavoro. Questo scenario offre ai criminali informatici ottime opportunità per infiltrarsi nelle reti dall'edge. E una volta dentro, non c'è più controllo.

Purtroppo, la maggior parte degli strumenti di sicurezza tradizionali, come i firewall, non sono stati progettati per questo tipo di problematiche. Sono nati come punti di controllo statici della rete, in tempi in cui i flussi di lavoro e i dati erano molto prevedibili. Ma quei giorni sono passati. Oggi serve una soluzione di hybrid mesh firewall (HMF) che integri i firewall di nuova generazione su tutte le reti e i fattori di forma, per consentire una gestione centralizzata e una risposta coordinata alle minacce. Questa soluzione deve proteggere gli asset e gli utenti ovunque, far convergere e unificare le soluzioni distribuite per ridurre le spese, semplificare la gestione e abilitare l'automazione, e infine scalare dinamicamente i servizi e la larghezza di banda per soddisfare i nuovi requisiti di business.

Nuovi problemi

Il data center, per quanto essenziale, ma non è più la locazione primaria in cui risiedono le applicazioni. Oggi le applicazioni possono essere distribuite ovunque. Considerato che una transazione o un flusso di lavoro può estendersi a più ambienti e applicazioni, la sua origine, la destinazione e il percorso dei dati possono cambiare più volte, rendendo impossibile tracciare e proteggere una transazione dall'inizio alla fine.

L'adozione del 5G ha creato difficoltà anche ai firewall tradizionali, soprattutto ora che il 95% di tutto il traffico è crittografato.[1] L'uso estensivo del traffico crittografato, in particolare dei tunnel SSL/TLS (Secure Sockets Layer/Transport Layer Security), serve per proteggere l'accesso remoto e le transazioni. Tuttavia, i criminali informatici utilizzano la crittografia anche per nascondere attività dannose, come il furto di dati e di segreti aziendali, oltre che per lanciare attacchi ransomware. La maggior parte dei firewall non è in grado di decifrare e ispezionare il traffico crittografato senza incidere fortemente sulle prestazioni e sull'esperienza dell'utente. Quindi, la maggior parte del traffico crittografato, soprattutto i dati che viaggiano ad alta velocità, non viene ispezionato.

Anche gli ambienti multi-cloud e la forza lavoro ibrida richiedono nuovi requisiti di sicurezza. Il cloud consente uno sviluppo agile delle applicazioni e funzionalità di scale-out/scale-up per soddisfare l'accesso crescente alle applicazioni da parte dei lavoratori remoti. Ma molte applicazioni business-critical devono ancora essere ospitate in un data center on-premise per ragioni di conformità o di privacy, e per la necessità di proteggere la proprietà intellettuale o i dati sensibili. E del resto la maggior parte dei firewall tradizionali non è in grado di supportare i casi d'uso dei data center ibridi, inclusi i modelli di interconnessione da utente a data center, da data center a cloud, da utente a cloud e da data center a data center.

Di conseguenza, le aziende finiscono per creare soluzioni alternative complesse per far funzionare insieme soluzioni diverse. Questo rende l'infrastruttura del data center sempre più complessa, dato che il numero di dispositivi, server, switch, router, firewall, bilanciatori di carico e altri componenti interconnessi tentano di fornire un flusso di dati continuo tra vari sistemi e applicazioni. Con l'aumento del numero di dispositivi e del volume di traffico dati cresce anche la complessità della rete, rendendo più difficile la gestione, il monitoraggio e la risoluzione dei problemi.

Il data center, per quanto essenziale, ma non è più la locazione primaria in cui risiedono le applicazioni. Oggi le applicazioni possono essere distribuite ovunque.

Nuove soluzioni

Per supportare e proteggere le architetture ibride è necessaria una visibilità unificata sull'intera rete distribuita. Bisogna quindi conoscere tutti gli utenti e i dispositivi della rete, nonché tutte le applicazioni e risorse a cui accedono. Inoltre, è necessario identificare i comportamenti anomali e le attività nocive ovunque si verifichino. Orchestrare in modo efficace tutte le risorse di sicurezza necessarie per una risposta tempestiva e coordinata è fondamentale per arrestare le minacce. E per supportare le attuali reti in espansione e i loro vari edge, molte aziende hanno iniziato ad adottare soluzioni diverse di secure access service edge (SASE), software-defined wide area network (SD-WAN) e zero-trust network access (ZTNA). Tutto ciò aumenta la complessità, limitando la visibilità, l'esperienza dell'utente e la capacità di rispondere efficacemente agli attacchi.

Oggi serve un nuovo approccio ai firewall di nuova generazione (NGFW) che integri queste funzioni e fornisca una sicurezza contestuale e coordinata a tutta la rete. Una soluzione HMF combina soluzioni on-premise e cloud-native con un componente di gestione unificato. Questa configurazione fornisce una protezione coordinata a diverse aree dell'enterprise IT, tra cui siti corporate, filiali, campus, data center, cloud pubblici e privati e lavoratori remoti. Grazie alla sua interoperabilità nativa, la soluzione HMF semplifica le operazioni, assicura la conformità, riduce la complessità e consente un'ampia automazione aumentando l'efficienza operativa. Il risultato non cambia se si dispone di firewall solo on-premise, solo nel cloud o un mix di entrambi. Il valore aggiunto risiede nella gestione centralizzata e unificata di tutte le implementazioni di firewall.

I casi d'uso infatti sono molto simili indipendentemente dal luogo in cui si implementa la sicurezza: un ambiente di campus o di data center, una rete multi-cloud, filiali o uffici domestici. Ciò che conta è suddividere la sicurezza in tre funzioni primarie: protezione, convergenza e scalabilità. Basandosi su questi tre concetti, è possibile implementare una strategia di sicurezza progettata per offrire un'esperienza utente integrata e una protezione allineata agli obiettivi aziendali.

Protezione

L'obiettivo principale è impedire a qualsiasi minaccia di entrare nella rete. Ma se ciò accade, il passo successivo è ridurre al minimo le interruzioni operative nel più breve tempo possibile. Un NGFW deve essere consapevole dell'intero ciclo di vita di un'applicazione, e dell'interoperabilità con gli strumenti per velocizzare l'accesso e l'utilizzo delle applicazioni. È quindi necessario un filtraggio web essenziale, aumentato dal riconoscimento avanzato delle immagini e dal filtraggio dei contenuti video, per assicurare un uso accettabile e la conformità.

Una soluzione NGFW deve anche fornire soluzioni di sicurezza avanzate per prevenire attacchi noti, zero-day e sconosciuti con un sistema integrato di prevenzione delle intrusioni (IPS) e anti-malware. Deve supportare feed costanti di informazioni sulle minacce condivisi da prodotti complementari come quelli per la sicurezza delle email e le sandbox, al fine di rilevare e prevenire le minacce più recenti.

Infine, deve interagire con altre soluzioni, come EDR (endpoint detection and response), firewall per applicazioni web (WAF) e altri sistemi di sicurezza.

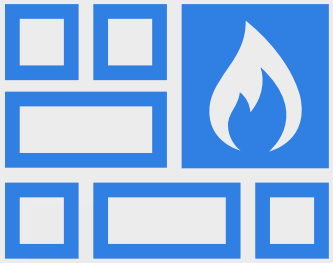
Questa combinazione di protezione nativa dalle minacce e di integrazione con altre tecnologie assicura una protezione efficace della rete contro tutte le minacce attuali ed emergenti.

Convergenza

Un NGFW deve fornire piena visibilità sugli attacchi sofisticati che si nascondono nei canali HTTPS sicuri per rubare dati e per caricare ransomware. Inoltre, deve integrare le funzioni essenziali di networking e sicurezza in una soluzione unificata - fornita direttamente da un NGFW on-premise o tramite un SASE fornito su cloud - che combini funzioni avanzate di routing e connettività con soluzioni di sicurezza dinamiche.

La soluzione deve anche identificare ogni utente, dispositivo o applicazione che richieda accesso e assegnarlo automaticamente al segmento di rete appropriato. Questo richiede servizi proxy integrati in modo nativo. Quando un dispositivo effettua la richiesta iniziale di accesso, il firewall deve cooperare con i client endpoint (per utenti e server) e con le soluzioni di controllo degli accessi di rete (per i dispositivi Internet-of-Things [IoT]/Industrial-Internet-of-Things [IIoT]). Inoltre, deve supportare l'autenticazione a più fattori per determinare il ruolo di un utente o dispositivo, collegarlo alle policy associate e concedere l'accesso solo all'applicazione o al segmento della rete utile per svolgere l'attività.

Nel caso delle applicazioni e dei flussi di lavoro che si spostano da un ambiente all'altro, un NGFW deve comprendere, implementare e applicare le stesse policy ovunque. Questo approccio coerente di orchestrazione e applicazione, con gestione da un'unica interfaccia, consente alla sicurezza di seguire le applicazioni, i flussi di lavoro e altre transazioni end-to-end.



Nel caso delle applicazioni e dei flussi di lavoro che si spostano da un ambiente all'altro, un NGFW deve comprendere, implementare e applicare le stesse policy ovunque.

Scalabilità

A prescindere dal luogo in cui si implementa un firewall, il requisito fondamentale è uno solo: deve essere veloce. E domani dovrà essere ancora più veloce. I data center di oggi generano ed elaborano enormi quantità di dati a velocità transazionali: big data per modellazione avanzata, dati a bassa latenza per transazioni finanziarie ad alta velocità o per iperprestazioni in ambienti multiutente di grandi dimensioni.

La velocità si riferisce alla rapidità con cui un firewall può ispezionare i dati e alla sua capacità di supportare l'automazione. Un NGFW deve proteggere efficacemente la rete da attacchi ad alta velocità con una sicurezza avanzata e coordinata, senza rallentamenti generati da lunghe operazioni di provisioning manuale. Le operazioni manuali rallentano i processi, mentre gli errori di configurazione possono essere a loro volta compromessi dal ransomware e da altri attacchi.

Il problema è che la maggior parte dei firewall tradizionali vanno già a pieno regime, quindi non possono scalare in linea con le nuove esigenze aziendali. Questo è normale visto che non sono stati progettati per le iperprestazioni. Il problema principale è che si basano su processori standard in un'epoca in cui tutto, dalle schede grafiche agli smartphone ai server cloud, funziona su chip personalizzati. La sicurezza è un'attività che richiede un forte uso del processore. Per poter scalare e soddisfare le esigenze prestazionali di oggi servono funzionalità firewall complete senza sacrificare le prestazioni o superare i limitati budget per l'IT e la sicurezza.

[1] “HTTPS encryption on the web,” Google Transparency Report, versione del 1 giugno 2023.

www.fortinet.com

novembre 9, 2023 12:17 AM

2170366-0-0-EN