I data center ibridi distribuiti richiedono più capacità NGFW

Sommario

Panoramica preliminare 3

I data center distribuiti espandono la superficie di attacco 4

Proteggere gli ambienti IT ibridi 6

Prestazioni per gestire i rischi 7

Resilienza e scalabilità 9

Automazione e orchestrazione 11

Scegliere una soluzione integrata con gli NGFW più efficaci 12

FORTINET

Panoramica preliminare

L'evoluzione dei moderni data center ha portato a una crescente distribuzione di applicazioni e dati su infrastrutture ibride. Se da un lato ciò migliora l'agilità per i flussi di lavoro business-critical, dall'altro amplia allo stesso tempo la superficie di attacco dell'organizzazione, oscurando la visibilità e ostacolando i controlli. I responsabili della gestione tecnica e operativa della rete richiedono una sicurezza integrata con funzionalità avanzate progettate per proteggere gli ambienti dei data center IT ibridi. In particolare, necessitano di un firewall NGFW che includa funzionalità di gestione dei rischi critici, scalabilità che estenda la protezione dei data center su tutte le parti dell'organizzazione, resilienza per garantire la Business Continuity, nonché funzionalità di automazione e orchestrazione per ridurre il carico di lavoro sul personale, accelerando al contempo i tempi di risposta.

I data center distribuiti espandono la superficie di attacco

Gli utenti aziendali hanno ora accesso ad applicazioni critiche da data center sempre più distribuiti che si estendono su un'infrastruttura IT ibrida. Usano flussi di lavoro e dati in ambienti locali, coubicazioni e cloud privati e pubblici, e questa ampia distribuzione di contenuti vulnerabili crea una superficie di attacco in continua espansione per le organizzazioni.

Per compensare questa crescente esposizione al rischio, molti responsabili della gestione tecnica e operativa della rete hanno provato ad aggiungere soluzioni di sicurezza monofunzionali per colmare le nuove lacune difensive e per coprire l'evoluzione dei requisiti di conformità normativa. Purtroppo, questo approccio frammentario non può affrontare l'intero spettro delle vulnerabilità attuali e future. Le probabilità di attacchi informatici o di disastri naturali che interrompono l'attività sono in aumento, così come il TCO e la complessità operativa della sicurezza per l'organizzazione.

Il costo totale medio dei tempi di inattività è di 67,2 milioni di dollari per azienda in due anni, compresi i danni alla fiducia e alla reputazione.[1]

Proteggere gli ambienti IT ibridi

Per affrontare l'espansione della superficie di attacco dei data center, i responsabili della gestione tecnica e operativa della rete devono prima integrare la sicurezza in tutte le parti dei loro ambienti IT ibridi. Necessitano inoltre di sicurezza tramite firewall NGFW che garantisca visibilità end-to-end, controlli delle policy e prevenzione delle intrusioni (IPS), insieme a funzionalità avanzate in grado di offrire:

- **Prestazioni.** La gestione dei rischi richiede una sicurezza in grado di tenere il passo con le reti ad alte prestazioni, insieme a funzionalità robuste che contribuiscano efficacemente a ridurre la superficie di attacco.
- **Resilienza e scalabilità.** Con l'espansione e la diversificazione degli ambienti IT ibridi, la sicurezza dei data center deve garantire scalabilità, resilienza e disponibilità per una Business Continuity affidabile. L'intera architettura di rete e di sicurezza deve essere in grado di resistere anche ai problemi causati da interruzioni di rete e disastri naturali.
- **Automazione e orchestrazione.** Un'architettura di sicurezza integrata consente di sfruttare appieno i vantaggi dell'automazione intelligente in tutta l'infrastruttura IT ibrida. Le risposte di sicurezza automatizzate e le funzioni di gestione accelerata riducono le finestre di esposizione al rischio, diminuendo al contempo il carico di lavoro sul personale, gli errori umani e le spese operative (OpEx).

Le principali preoccupazioni relative ai carichi di lavoro dei dati ibridi includono la sicurezza dei dati e la conformità normativa (71%), le prestazioni (62%) e la facilità di gestione (53%).[2]

Prestazioni per gestire i rischi

I firewall dei data center sono tipicamente distribuiti nella parte più veloce della rete. Pertanto, un'efficace soluzione NGFW distribuita in questi casi d'uso deve essere in grado di applicare una sicurezza L7 avanzata con un impatto minimo sulle prestazioni della rete. Per raggiungere questo obiettivo, la soluzione necessita di **processori di sicurezza dedicati** che consentano al firewall NGFW di eseguire le funzioni di sicurezza in modo affidabile senza creare un collo di bottiglia nella rete.

La protezione di un moderno data center distribuito richiede anche la visibilità di tutti gli elementi di sicurezza distribuiti in tutti i vari ambienti (locali, coubicazioni, cloud, ecc.), così come la visibilità degli utenti, delle applicazioni e dei dispositivi. Con oltre un terzo (34%) delle violazioni che proviene ora da fonti interne affidabili,[3] il controllo degli accessi alla rete interna diventa un imperativo. I responsabili della gestione tecnica e operativa della rete possono raggiungere questo obiettivo attraverso una **segmentazione della rete** scalabile e sufficientemente flessibile per adattarsi ai vari casi d'uso (inclusa l'attendibilità dinamica di utenti, dispositivi e applicazioni). Ma la segmentazione da sola non è in grado di fornire molte funzioni di sicurezza critiche per le minacce avanzate di oggi, compresa l'ispezione dei contenuti. Pertanto, una distribuzione NGFW per i data center deve essere in grado di adattarsi a varie tecniche di segmentazione, di comunicare con soluzioni di sicurezza di terze parti per condividere la threat intelligence, di ispezionare i contenuti e di proteggere dalle minacce in modo automatizzato.

Tenere il passo con il volume e la velocità delle minacce odierne richiede una soluzione di sicurezza che condivida l'intelligence in tempo reale attraverso un'architettura di sicurezza integrata. Allo stesso tempo, la soluzione deve applicare tecnologie di intelligenza artificiale (IA) per identificare le minacce sconosciute. La cosa più importante è che questo **sistema di rilevamento e prevenzione delle minacce basato sull'intelligenza artificiale** deve essere applicabile alle risorse digitali ovunque si trovino.

IL 77%

delle organizzazioni attualmente si affida in una certa misura a soluzioni di sicurezza monofunzionali non integrate.[4]

Resilienza e scalabilità

La natura in continua espansione dell'innovazione digitale ha un impatto diretto sulla sicurezza. Con la continua decentralizzazione dei carichi di lavoro dei data center attraverso un'infrastruttura IT ibrida, la sicurezza richiede **elasticità per potersi espandere in modo scalabile** con nuove applicazioni e carichi di lavoro crescenti, oltre le appliance tradizionali negli ambienti locali, nelle iterazioni di distribuzione su cloud e macchine virtuali (VM).

La sicurezza dei data center deve inoltre adattarsi alle esigenze di un traffico sempre più intenso, costituito da flussi di dati crittografati e non. Oltre il 72% del traffico di rete totale è ora costituito da dati crittografati, con un aumento di quasi il 20% rispetto all'anno precedente.[5] I maggiori volumi di traffico crittografato richiedono una visibilità avanzata tramite strumenti di ispezione del traffico HTTP e HTTPS.

I data center distribuiti sono particolarmente vulnerabili alle minacce che si spostano in modo nascosto nei flussi di dati crittografati. Per attenuare questi rischi è necessaria una soluzione di sicurezza con funzionalità avanzate di **ispezione della crittografia SSL (Secure Sockets Layer) e TLS (Transport Layer Security)**, nonché con integrazione di sandboxing e di esche/honeypot, per grandi quantità di traffico che si sposta tra gli utenti e i sistemi e all'interno dei sistemi, senza incidere sulle prestazioni delle applicazioni. Le funzionalità di ispezione devono supportare il protocollo più recente **TLS 1.3**.[6]

In termini di resilienza e disponibilità, la soluzione deve garantire il failover del sistema in tempo reale in caso di guasto di un componente. Il **clustering N+1 integrato** offre un'architettura completamente ridondante per eliminare ogni singolo punto di guasto. Inoltre, **test di convalida di terze parti** condotti da esperti del settore indipendenti contribuiscono a garantire l'affidabilità della soluzione in condizioni reali.

IL 60%

del traffico crittografato contiene malware;[7] il 28% delle violazioni è causato da malware.[8]

Automazione e orchestrazione

L'attuale carenza di competenze in materia di sicurezza informatica pone sotto forte pressione molte organizzazioni di sicurezza, che si ritrovano con personale insufficiente a gestire carichi di lavoro eccessivi. La riduzione della complessità operativa è la chiave che consente di limitare i costi OpEx e di liberare risorse tecniche addette alla sicurezza, che possono così concentrarsi maggiormente sui risultati aziendali e sull'attuazione di ottimizzazioni piuttosto che sulle attività manuali. A questo proposito, un firewall efficace per i data center dovrebbe includere funzionalità quali **flussi di lavoro ottimizzati** per semplificare la distribuzione e la gestione.

Un'architettura di sicurezza integrata offre una base per la condivisione dell'intelligence e risposte automatizzate che coordinano la sicurezza tra infrastrutture ibride. Una soluzione NGFW con supporto per **API aperte** offre vantaggi critici come l'automazione dei flussi di lavoro, l'orchestrazione e risposte di sicurezza sincronizzate per le applicazioni prive di patch e gli ambienti DevOps in continua evoluzione. La soluzione dovrebbe anche essere in grado di **applicare una logica di business che determina continuamente l'attendibilità di utenti, dispositivi e applicazioni** per aiutare ad automatizzare i processi di sicurezza (come il provisioning e il controllo degli accessi). Ciò riduce il carico di lavoro del personale e i costi OpEx, aumentando al contempo l'efficienza operativa e l'efficacia della sicurezza.

Le funzionalità NGFW che aiutano ad **automatizzare i processi di reporting e di controllo della conformità** possono anche aiutare i responsabili della gestione tecnica e operativa della rete a ridurre i carichi di lavoro, tenendo il passo con l'evoluzione delle normative governative e di settore, nonché con gli standard di sicurezza come quelli del NIST (National Institute of Standards and Technologies) e del CIS (Center for Internet Security).

Più della metà dei responsabili delle decisioni IT (54%) afferma che la capacità di trattenere talenti è parte del problema quando si decide di adottare un modello ibrido.[9]

Scegliere una soluzione integrata con gli NGFW più efficaci

Quando i data center diventano più distribuiti e si evolvono verso un approccio IT ibrido, si espande anche la superficie di attacco di un'organizzazione. E nonostante la richiesta di livelli sempre più elevati di prestazioni dei data center, i responsabili della gestione tecnica e operativa della rete non possono scendere a compromessi tra la sicurezza e la risposta alla domanda degli utenti. Di fronte ai rischi in aumento, alle crescenti possibilità di interruzioni della rete e ai sempre maggiori costi, le organizzazioni devono rivedere la sicurezza dei data center moderni.

Per garantire sia la sicurezza che le prestazioni, i responsabili della gestione tecnica e operativa della rete devono adottare un'architettura di sicurezza integrata basata su una soluzione NGFW robusta, che offra prestazioni, resilienza, scalabilità e automazione.

[1] Filip Truta, "Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation", Security Boulevard, 21 febbraio 2019.

[2] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model", TechRepublic, 15 novembre 2018.

[3] "2019 Data Breach Investigations Report", Verizon, aprile 2019.

[4] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[5] John Maddison, "Encrypted Traffic Reaches A New Threshold", Network Computing, 28 novembre 2018.

[6] Alex Samonte, "TLS 1.3: What This Means For You", Fortinet, 15 marzo 2019.

[7] Omar Yaacoubi, "The hidden threat in GDPR's encryption push", PrivSec Report, 8 gennaio 2019.

[8] "2019 Data Breach Investigations Report", Verizon, aprile 2019.

[9] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model", TechRepublic, 15 novembre 2018.

www.fortinet.com

472724-0-0-IT

aprile 24, 2020 3:14 PM

eb-advanced-ngfw-security