Akamai

WHITE PAPER

Segmentazione e microsegmentazione della rete negli ambienti aziendali moderni

Panoramica

L'idea della segmentazione per motivi di sicurezza non è una novità. Tradizionalmente, la maggior parte delle aziende ha utilizzato i firewall perimetrali, insieme alle VLAN e agli ACL per segmentare e proteggere la propria infrastruttura IT. Tuttavia, i tempi stanno cambiando. L'aumento della containerizzazione, delle reti definite dal software, dell'uso di infrastrutture pubbliche e multicloud e dell'espansione dei dispositivi connessi a Internet ha generato una nuova serie di problemi di sicurezza da affrontare, che necessitano di una soluzione appositamente creata per un ambiente IT eterogeneo con diverse caratteristiche. Inoltre, i ransomware e gli autori di minacce affiliati a stati-nazionali rappresentano ora un rischio per qualsiasi azienda e i criminali stanno diventando sempre più sofisticati mentre, allo stesso tempo, diventa sempre più difficile comprendere come ottenere visibilità nell'ambiente IT. Le tradizionali misure di sicurezza perimetrale, così come i firewall di nuova generazione basati sull'ispezione approfondita dei pacchetti o sul rilevamento basato sulle firme, faticano a tenere il passo con la quantità di traffico a cui è sottoposto oggi un data center aziendale. Esaminiamo come le tecniche di microsegmentazione appropriate siano la migliore tecnologia per affrontare le carenze di altri approcci alternativi alla segmentazione della rete.

> Poiché gli ambienti cloud ibridi sono diventati la norma, richiedono una serie specifica di requisiti che vanno ben oltre la tradizionale sicurezza perimetrale

I firewall tradizionali sono inadeguati per il traffico est-ovest

Quando tenta di segmentare gli ambienti IT, un'azienda potrebbe prendere principalmente in considerazione i dispositivi di sicurezza perimetrali tradizionali. Purtroppo questi dispositivi sono stati realizzati per monitorare il traffico che si sposta da nord a sud, da client a server. Questo include tutto il traffico che arriva al data center da qualsiasi fonte esterna. Più recentemente, la quantità di traffico all'interno del data center che si sposta da un server all'altro, solitamente definito traffico est-ovest, è aumentata in modo esponenziale. Ciò è in gran parte dovuto alla crescita della virtualizzazione e delle infrastrutture convergenti come hypervisor, VPC ed elaborazione basata su container.

Le misure di sicurezza perimetrali come i firewall tradizionali non fanno nulla per proteggere la vostra azienda dai dispositivi infetti o per impedire ai criminali di espandere il loro punto d'appoggio utilizzando il traffico est-ovest. Con l'aumento della crittografia TLS e la facilità con cui il traffico dannoso riesce a sfruttare le porte aperte di applicazioni legittime, molti attacchi riescono anche a eludere i firewall. Ciò vi impedisce di individuare le violazioni esistenti e di risolverle o evitarle. Significa anche che non è possibile limitare facilmente il tempo di permanenza degli autori di attacchi sulla rete. Più lungo è il tempo di permanenza, più catastrofica sarà la violazione. L'Active Adversary Playbook 2022 di Sophos ha rilevato che, rispetto al tempo di permanenza medio di 15 giorni, le piccole imprese e settori specifici hanno registrato tempi di permanenza medi molto più lunghi, fino a 34 giorni.[1] Più a lungo un criminale riesce a passare inosservato nella rete, più danni può causare.

È semplicemente impossibile utilizzare un numero sufficiente di firewall virtualizzati per proteggere migliaia di applicazioni o carichi di lavoro. Anche se fosse possibile creare una soluzione virtualizzata, sarebbe impossibile da gestire o controllare considerando gli odierni ambienti dinamici in continua evoluzione in cui lavoriamo. Nel caso di un cloud ibrido, ad esempio, i firewall tradizionali sono ancora più difficili da utilizzare, poiché devono funzionare in vari ambienti, tenere traccia dei carichi di lavoro su cloud diversi ed essere controllati da un unico punto. Per cercare di risolvere questi problemi, sono emersi diversi approcci di segmentazione della rete.

Tre approcci di segmentazione da considerare

Con la consapevolezza che i firewall, anche se virtualizzati, sono inadeguati a proteggere i data center del cloud ibrido, le aziende cercano di applicare la segmentazione all'interno dell'infrastruttura est-ovest in tre modi fondamentali. Come abbiamo descritto, senza una policy di segmentazione e misure di sicurezza efficaci, qualsiasi porta o server può consentire l'accesso per comunicare con altre porte o server. Ciò significa che, se il firewall di un server viene violato, un autore di attacchi può spostarsi facilmente su tutti gli altri server nella rete. Il modo più efficace per limitare la connettività tra i server è segmentare la rete. Esistono tre tipi fondamentali di segmentazione della rete, dove la microsegmentazione è la tecnologia che le aziende possono utilizzare per applicare policy e controlli sempre più granulari. Gli utenti possono combinare i tre tipi di policy di segmentazione elencati di seguito, creando policy più granulari per applicazioni critiche o rischiose.

Segmentazione dell'ambiente

Questo approccio separa tra loro ambienti diversi. In questo modo le aziende potrebbero, ad esempio, separare il ramo di sviluppo della propria azienda dall'ambiente di produzione. Questa è la prima fase cruciale di qualsiasi strategia di segmentazione, che può poi essere seguita da una creazione di policy più granulari.

Segmentazione delle applicazioni

Un ulteriormente livello di segmentazione, è "l'isolamento" delle applicazioni di alto valore, che separa ciascuna applicazione critica specifica dal resto della rete. Le migliori soluzioni di microsegmentazione consentiranno di controllare questo aspetto anche a livello di processo.

Segmentazione dei livelli

La forma più rigorosa di segmentazione avviene all'interno dell'applicazione stessa. Qui è possibile creare policy su come vengono gestite le comunicazioni tra livelli all'interno dello stesso cluster di applicazioni, controllando ad esempio il traffico tra server web, server delle applicazioni e server di database. Questo controllo può essere applicato anche a livello di processo, se desiderato.

Metodo di segmentazione della rete: segmentazione della rete tramite VLAN

La maggior parte delle aziende inizia utilizzando le VLAN. Queste reti locali virtuali consentono alle aziende di assegnare a ciascun segmento il proprio percorso di comunicazione, tramite un firewall o elenchi di controllo degli accessi (ACL) sul router stesso. Sebbene la VLAN sia una scelta comune per la segmentazione della rete, i problemi sottostanti sono molti. Esaminiamo più in profondità, facendo il punto sul motivo per cui le VLAN costituiscano una scelta inadeguata per soddisfare le odierne esigenze di sicurezza.

È facile capire perché molte aziende scelgono le VLAN come metodo di segmentazione. Tale metodo può essere attuato con l'architettura esistente, il che lo rende economico e semplice da implementare. Tuttavia, si tratta di un approccio di segmentazione molto rigido e complesso, che può risultare costoso da gestire e la cui implementazione implica problemi di downtime.

Per iniziare a utilizzare le VLAN, dovrete acquisire familiarità con i server e le dipendenze in ciascun segmento, quindi creare la configurazione desiderata per lo switch o gli switch di rete che state segmentando. Poiché questa operazione viene eseguita da tecnici di rete e spesso coinvolge più sedi, l'operazione può richiedere molti giorni e costi sproporzionati. Il traffico potrebbe essere interrotto o lento durante il periodo di configurazione.

In un'epoca in cui l'agilità è un importante vantaggio competitivo e forse anche un requisito indispensabile, i costi elevati e la lentezza dei cambiamenti hanno conseguenze disastrose per la redditività. Secondo Forbes, l'adattabilità è essenziale per la sopravvivenza: "Le interruzioni non sono una novità, ma la velocità, la complessità e la natura globale delle interruzioni raggiungono una scala mai vista prima. ... Non saranno le imprese più grandi o quelle finanziariamente più stabili a sopravvivere, ma quelle che riusciranno ad adattarsi al ritmo esponenzialmente accelerato del cambiamento".[2]

È importante riconoscere che le VLAN non sono state create pensando alla segmentazione. Inizialmente progettate per ridurre la congestione, utilizzarle per controllare le comunicazioni non è un modo intelligente di sfruttare la tecnologia esistente: per molti versi è un uso improprio. Considerando ciò, non sorprende che la segmentazione tramite VLAN presenti delle limitazioni.

- **Tecnologia cloud**: le VLAN e altre policy tradizionali di segmentazione della rete non possono essere estese al cloud. Se utilizzate firewall segmentati interni (ISFW) o ACL per controllare quali utenti possono accedere ai segmenti di rete, probabilmente dovrete ricorrere a una SDN (rete definita dal software) per il cloud, tramite provider di software di terze parti che utilizzano firewall o sottoreti virtualizzate.
- **Container**: la sicurezza resta un grande problema data la diffusa adozione dei container negli ambienti IT. Poiché ciascun container viene eseguito sullo stesso kernel, un exploit potrebbe mettere a rischio tutti i container. L'isolamento è una criticità costante che non può essere risolto con i consueti metodi di segmentazione della rete.
- **Restrizioni del protocollo**: il limite per le VLAN è di 4.096 segmenti, che limita la capacità di fornire un'adeguata segmentazione nei data center di grandi dimensioni. Gli approcci di segmentazione più granulari non presentano questa limitazione.

Dalla segmentazione della rete alla segmentazione delle applicazioni: introduzione dei controlli di livello 4

Molti di questi problemi sono stati migliorati adottando la segmentazione delle applicazioni utilizzando gruppi di sicurezza all'interno di ambienti cloud e firewall basati su hypervisor per ambienti virtualizzati locali. La segmentazione tradizionale delle applicazioni implementa i controlli di livello 4, consentendo di isolare tra loro i livelli di servizio, per garantire un confine sicuro a un'applicazione. Ogni livello è limitato al livello di accesso necessario per fornire tutte le funzionalità, e non di più. Vi è una chiara separazione tra i livelli di una singola applicazione e il rischio di una potenziale compromissione è ridotto al minimo.

Pensate ai possibili livelli disponibili in un'azienda standard, dai sistemi di bilanciamento del carico e database ai server applicativi all'interno/all'esterno della DMZ. Mantenere questi livelli separati consente di applicare a ciascun livello le proprie regole e funzionalità di sicurezza. La segmentazione delle applicazioni può consentire alle aziende di applicare i controlli appropriati per ciascun livello, limitando le informazioni e le comunicazioni sensibili e consentendo al tempo stesso un ampio accesso agli utenti ove necessario. Ad esempio, un'azienda può impedire del tutto a determinati database di comunicare con Internet o garantire che, se un criminale viola un semplice sistema di bilanciamento del carico, non possa sfruttarlo per accedere a informazioni più sensibili a livello di database.

Con l'aumento della granularità della soluzione, la segmentazione delle applicazioni consente a un'azienda di segmentare un intero cluster di applicazioni da altre aree dell'azienda. Come descritto, ciò riduce la superficie di attacco e la possibilità per gli aggressori di effettuare movimenti laterali da un livello all'altro.

I limiti dei controlli di livello 4

La segmentazione tradizionale delle applicazioni può non essere abbastanza profonda, il che ha un impatto diretto sulla visibilità. Al livello di rete, dove avviene il routing, i dati vengono spostati tra i sistemi, assegnando indirizzi IP e protocolli che descrivono in dettaglio il percorso dei segmenti di dati fino alla propria destinazione. La segmentazione delle applicazioni utilizza spesso i controlli di rete di livello 4, concentrandosi sul metodo di delivery dei dati. I segmenti di dati di maggiori dimensioni vengono suddivisi in segmenti o blocchi di dimensioni inferiori, pronti per essere ricongiunti a destinazione. Il controllo del flusso consente di accelerare o rallentare dinamicamente questo processo, laddove i dispositivi che inviano o ricevono le informazioni lo richiedano.

Nell'odierno panorama delle minacce, i controlli su questi livelli sono essenziali, ma in alcuni potrebbe essere necessario impostare policy a un livello ancora più granulare. Gli autori di attacchi hanno dimostrato di essere in grado di falsificare gli indirizzi IP e di utilizzare tecniche di sfruttamento delle porte consentite per violare una rete. Inoltre, la protezione di livello 4 non limita i movimenti laterali all'interno di un'applicazione o di un livello, lasciandovi con una possibile superficie di attacco più ampia di quanto desideriate.

Uno dei migliori esempi della necessità di controlli più granulari rispetto al semplice livello 4 è rappresentato dalle iniziative di conformità. Le tradizionali tecniche di segmentazione delle applicazioni hanno, in una certa misura, consentito alle aziende di soddisfare alcune normative di conformità specifiche, come mantenere CDE separato per PCI-DSS o proteggere le PHI per HIPAA. Tuttavia, sebbene in passato le tecniche di livello 4 siano state accettate come metodi efficaci per dimostrare la conformità, la realtà ha dimostrato che potrebbero non essere sufficienti. Secondo il Verizon 2022 Payment Security Report, solo il 43% delle aziende è "pienamente conforme".[3] E quel che è peggio, anche una conformità al 100% non garantisce la sicurezza al 100%. Sebbene i controlli di livello 4 possano soddisfare i requisiti di conformità, non riducono la superficie di attacco abbastanza da fare una differenza significativa per la sicurezza. Questo è indiscutibile. Gli autori di attacchi possono sfruttare una porta di livello 4 aperta tra due livelli con un processo separato (livello 7) e sottrarre tutto ciò che desiderano.

Segmentazione al buio: mancanza di visibilità nella segmentazione della rete e delle applicazioni

Come stanno scoprendo le aziende, anche se non c'è dubbio che la segmentazione delle applicazioni sia un passo nella giusta direzione, non è sufficiente a risolvere tutti i problemi inerenti a un approccio di segmentazione grossolana. Un'altra sfida che deve ancora essere affrontata è la visibilità. Disporre di una visibilità accurata e in tempo reale della vostra rete è essenziale in ogni fase del processo di segmentazione, un limite che presentano molti approcci alla segmentazione.

Prima di iniziare, vi consigliamo di visualizzare le dipendenze delle applicazioni in modo da poter elaborare regole di policy precise. Dopo aver implementato la segmentazione, dovrete avere le prove che la segmentazione funzioni come previsto, non solo per verificare che il vostro livello di sicurezza sia solido, ma anche per dimostrare la conformità normativa, ove necessario.

Senza una visibilità storica e in tempo reale, né voi potrete accedere alle informazioni richieste, né potranno farlo le parti interessate o gli organismi di regolamentazione di terze parti. La raccolta manuale di tali prove richiede tempo ed è costosa da gestire, inoltre esiste sempre la possibilità di errori generici ed errori di configurazione. Una soluzione di segmentazione che non è in grado di fornire questo tipo di visibilità è semplicemente insufficiente.

Microsegmentazione fino al livello 7: il livello dell'applicazione

Al contrario, la segmentazione a livello di applicazione (livello 7) è altamente efficace nel limitare il movimento laterale, anche all'interno di un cluster di applicazioni. Il livello 7 è il punto in cui i servizi di rete si integrano con il sistema operativo. Protocolli come HTTP, FTP, TFTP e SMTP sono tutti protocolli di livello 7. I miglioramenti più recenti nella tecnologia di microsegmentazione consentono di segmentare questo livello con una profondità notevolmente maggiore rispetto ad altre soluzioni, consentendo alla vostra azienda di visualizzare e controllare l'attività a livello 7 così come al tradizionale livello 4. In questo modo, anziché fare affidamento su indirizzi IP e porte, è possibile utilizzare processi e flussi specifici quando le aziende configurano le proprie policy. Ciò porta i vantaggi della segmentazione ben oltre un livello specifico o addirittura un cluster di applicazioni. Consente inoltre di individuare potenziali minacce anche con l'hash errato, anche quando l'autore di attacchi esegue il mirroring di un processo o un percorso autorizzato.

Per quanto riguarda la creazione di policy, la segmentazione al livello 7 implica regole o eccezioni per elenchi di elementi consentiti molto specifiche, in cui sono consentiti solo processi o flussi esatti e tutte le altre comunicazioni vengono bloccate per impostazione predefinita. Ciò può imporre l'isolamento dei dati tra i sistemi, ma consente comunque la comunicazione per i flussi di dati necessari o critici per l'azienda.

Le migliori soluzioni di microsegmentazione forniscono la visibilità di cui le aziende necessitano per acquisire flessibilità

Con agenti su ogni carico di lavoro (basati su hypervisor o VPC, container, server bare metal o persino sistemi IoT/OT), una soluzione di microsegmentazione olistica può fornire alla vostra azienda una mappa visiva completa dell'intera infrastruttura IT. Le soluzioni veramente intelligenti includono ambienti data center, cloud, multicloud e cloud ibrido e dispositivi remoti. Le tradizionali soluzioni di segmentazione delle applicazioni faticano a ottenere questa visibilità completa, solitamente perché utilizzano una combinazione di tecnologie incentrate sulla rete.

Una mappa visiva completa del vostro ambiente dovrebbe anche mostrarvi le policy di sicurezza applicate in tempo reale. I tecnici e professionisti della sicurezza dovrebbero essere in grado di visualizzare in tempo reale potenziali lacune da colmare nel vostro sistema di policy o quali policy aggiuntive devono implementare o creare appositamente.

Disporre di questa visibilità consente inoltre alla vostra azienda di prepararsi in anticipo per nuovi software o aggiornamenti ai sistemi esistenti, creando per tempo le regole per segmentare le applicazioni nuove o aggiornate, prima che siano pronte per l'implementazione. Una volta che gli aggiornamenti sono attivi, i team di sicurezza dispongono delle informazioni in tempo reale di cui necessitano per rilevare e risolvere attività di applicazioni anomale, garantendo che nessun rischio per la sicurezza passi inosservato o diventi un exploit attivo. A fatto compiuto, la vostra azienda disporrà degli strumenti contestuali per confrontare un incidente con i dati storici e comprendere l'ambiente esatto che ha consentito il verificarsi dell'anomalia. È possibile rendere le policy più rigorose, adattare la segmentazione e analizzare in modo dettagliato l'incidente per le normative di conformità o per ulteriori studi.

Utilizzo del modello Zero Trust

Un altro vantaggio aggiuntivo della microsegmentazione è la capacità di adottare il modello di sicurezza Zero Trust. Sebbene il concetto di Zero Trust sia stato coniato da Forrester già nel 2010, tecnologie come la microsegmentazione stanno contribuendo a trasformarlo in realtà, e ricercatori ed esperti di sicurezza continuano a pubblicizzarne i vantaggi in lungo e in largo.[4]

L'idea è semplice: nessun traffico o utente è considerato affidabile finché non viene dimostrato e approvato, sia che provenga da una fonte esterna che da una fonte interna, ogni volta che si verifica un tentativo di connessione. I tre principi fondamentali di Forrester del modello Zero Trust[5] sono tutti supportati da policy di microsegmentazione solide e granulari:

- Tutte le entità sono considerate non attendibili per impostazione predefinita
- Viene implementato un monitoraggio completo della sicurezza
- Viene applicato l'accesso basato sul privilegio minimo

Zero Trust si trova all'estremità opposta dello spettro rispetto al modello di sicurezza solo perimetrale, che considera l'azienda come un castello da difendere con un profondo fossato presumendo che tutto ciò che si trova all'interno sia autorizzato all'accesso. Poiché la maggior parte delle aziende non dispone più di una rete o di un data center autonomi, l'idea di un "castello" è obsoleta e una strategia basata su privilegi minimi come il modello Zero Trust è l'unico modo per garantire di poter sapere e controllare chi si trova all'interno in ogni dato momento.

Adattamento dell'azienda alle esigenze future con la microsegmentazione

La segmentazione della rete può certamente andare oltre la sicurezza perimetrale e la segmentazione dell'ambiente e delle applicazioni fino al livello 4 sono passaggi importanti nella reazione della vostra strategia di segmentazione. Tuttavia, con l'aumento della complessità degli ambienti IT, potreste scoprire di aver bisogno di una soluzione di segmentazione che offra ancora maggiore granularità con la segmentazione dei livelli e l'applicazione a livello di processo fino al livello 7 nelle fasi relative ad applicazioni e livelli.

Le aziende moderne hanno superato il modello di infrastruttura autonoma. Spesso si affidano a tecnologie come SDN nel cloud, in container o hypervisor bare metal. Funzionano in varie aree geografiche e data center fisici.

L'unico modo per proteggersi dalle minacce esterne e interne è utilizzare una soluzione che ispezioni e controlli tutto il traffico, sia da est a ovest che da nord a sud, e, per applicazioni cruciali o rischiose, offra maggiore visibilità rispetto al solo livello 4. La microsegmentazione fino al livello 7 a livello di applicazione o di livello offre la possibilità di ottenere una visibilità accurata dell'intero ambiente IT e consente di creare e applicare facilmente policy di sicurezza granulari che seguono il modello Zero Trust. Una buona soluzione di microsegmentazione non richiederà di scegliere tra sicurezza e flessibilità, quindi optate per una soluzione capace di offrire la strategia di sicurezza complessiva più solida alla vostra organizzazione.

Per ulteriori informazioni, visitate il sito akamai.com/guardicore.

1 Shier John. 2022. "Guida ai criminali attivi nel 2022". Sophos. 7 giugno

2 Gonda Rob. 2018. "L'adattabilità è la chiave per sopravvivere nell'epoca del darwinismo digitale". Forbes 24 maggio

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. Giugno 2022 "Le best practice per la microsegmentazione Zero Trust". Forrester. Aprile.

5 Holmes David e Jess Burn. Gen. 2022. "La definizione del modello Zero Trust moderno". Forrester. Aprile.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare ed evolvere la vostra strategia di sicurezza per favorire il modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS, offrendovi la sicurezza necessaria per concentrarvi costantemente sull'innovazione, sull'espansione e sulla trasformazione di tutto il possibile. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 05/23.