zscaler™

7 sintomi che il tuo firewall legacy non è adatto a supportare lo zero trust

E-book

Lo zero trust è sempre più adottato dalle aziende

Oggi, gli stakeholder della sicurezza IT sanno bene che lo zero trust è il modello di sicurezza giusto per le aziende digitali moderne. Le indagini mostrano che lo ZTNA è stato adottato o sarà adottato nel 78% dei programmi di sicurezza aziendali.[1] È ormai risaputo che concentrarsi direttamente sulla protezione degli utenti, dei dati e delle applicazioni, invece che sulla rete, è la chiave per proteggere le imprese di oggi, che sono basate sui dati e sul lavoro da remoto.

Decenni fa, quando le configurazioni di rete hub-and-spoke erano ancora soluzioni all'avanguardia, i firewall e le infrastrutture di rete costruite intorno a essi erano al passo con i tempi, promettenti ed efficaci. Rappresentavano la scelta tecnologica giusta per quell'epoca, offrivano un servizio affidabile e svolgevano bene il loro lavoro. Nell'era moderna del cloud computing, tuttavia, la loro presenza è un peso, e le configurazioni basate sull'architettura a castello e fossato sono totalmente incompatibili con il concetto di zero trust.

Ecco una guida diagnostica che illustra i sette sintomi che rivelano perché il firewall non è adatto al mondo moderno, che è fondato sulla sicurezza zero trust. La presenza di uno qualsiasi di questi 7 sintomi indica che l'organizzazione ha bisogno di una cura basata sulla sicurezza sul cloud.

1. Fonte: Cybersecurity Insiders, Zero Trust Adoption Report, 2019.

SINTOMO N. 1

Mancanza di visibilità quando si cerca di ispezionare il traffico su larga scala

Indipendentemente dalla loro forma, i firewall basati su dispositivi non sono in grado di ispezionare su larga scala il traffico criptato con SSL. Questo problema è sempre più critico, dato l'aumento di questo tipo di traffico a livello globale. Gli aggressori sono a conoscenza di questo aumento, e lo sfruttano per nascondervi all'interno un numero sempre maggiore di minacce avanzate.

Se il firewall soffre di questa condizione, ogni volta che cercherai di attivare l'ispezione SSL, noterai un calo delle prestazioni del 50% o superiore. Dovrai quindi eseguire l'aggiornamento a un firewall con una capacità superiore o aggiungere più apparecchi (o istanze firewall virtuali) al solo scopo di mantenere le prestazioni accettabili per gli utenti.

QUAL È LA CURA?

- Passare a un servizio fornito sul cloud, in grado di offrire le funzionalità dei firewall nativi del cloud, anziché cercare di sfruttare e scalare versioni di macchine virtuali (VM) di dispositivi fisici ormai obsoleti. Solo i servizi e le soluzioni che dispongono veramente di una base cloud sono scalabili illimitatamente e possono soddisfare le esigenze attuali di traffico.

2. Fonte: Agenzia dell'Unione europea per la cibersicurezza, Analisi del traffico criptato
3. Fonte: Zscaler, Indagine sui firewall di rete

SINTOMO N. 2

Inconsapevolezza del movimento laterale

I firewall sono stati progettati per proteggere il perimetro delle reti costruite sul modello a castello e fossato. L'idea consisteva nel fatto che, una volta che il firewall avesse preso la decisione di consentire o meno l'ingresso, tutto il traffico all'interno di tale perimetro avrebbe potuto essere ritenuto attendibile incondizionatamente. In queste architetture, la maggior parte degli utenti lavorava in sede, gran parte dell'infrastruttura era on-premise e la maggior parte delle applicazioni risiedeva all'interno del data center; questo scenario è radicalmente diverso al giorno d'oggi.

Attualmente, il 70% del traffico è interno alla rete, ovvero scorre tra i server e le applicazioni all'interno del cloud privato o del data center dell'azienda. Le difese perimetrali lasciano pochi mezzi, se non addirittura nessuno, per ispezionare o bloccare questo traffico; così, una volta entrati nella rete, gli aggressori possono agire liberamente.

Dopo aver ottenuto l'accesso a questo modello di rete, è molto semplice scoprire tutte le risorse a cui è connesso. L'utente ha bisogno unicamente di uno strumento di scansione open source per rilevare tutti gli indirizzi IP all'interno della rete. A questo punto, la distribuzione di ransomware o l'esfiltrazione di dati di valore sono operazioni molto facili, e non c'è nulla che un firewall possa fare per arrestarle.

Il 64%
degli amministratori della rete di oggi ritiene che i firewall siano inefficaci nel bloccare il movimento laterale.[4]

Il 57%
dei responsabili delle decisioni IT ritiene che i firewall non siano in grado di fermare gli attacchi ransomware.[4]

QUAL È LA CURA?

- Implementare un approccio ZTNA (Zero Trust Network Access), che consenta di stabilire connessioni solo dopo la verifica delle identità dei dispositivi, degli utenti, dello stato della sicurezza, e di applicare policy per ogni singola connessione, ogni volta. In questo modo è possibile stabilire connessioni dirette e sicure tra utenti e applicazioni, anziché instaurare connessioni non protette a una rete.

4. Fonte: Zscaler, Indagine sui firewall di rete

SINTOMO N. 3

Grave infiammazione delle policy

I team che si occupano di sicurezza cercano di ottenere un approccio zero trust all'interno delle architetture di rete tradizionali configurando delle policy volte a segmentare le reti in porzioni sempre più piccole. In teoria si tratta di una forma di microsegmentazione, ma in pratica queste policy sono ingestibili perché richiedono troppo impegno e lavoro amministrativo.

Per proteggere le applicazioni di oggi, le aziende devono distribuire un numero crescente di firewall virtuali su tutta la rete. Questo si traduce in una valanga di policy che richiedono configurazioni e riconfigurazioni infinite per riuscire a ottenere un risultato che assomigli lontanamente all'applicazione dello zero trust.

Come i loro predecessori fisici, i firewall virtuali non sono in grado di garantire scalabilità oltre una certa soglia, e prima o poi richiederanno migliaia, se non decine di migliaia di policy, che ne renderanno impossibile l'amministrazione.

QUAL È LA CURA?

Il segreto è separare le reti dal controllo degli accessi ad applicazioni e risorse. Lo ZTNA permette di concedere ai singoli utenti un accesso diretto e sicuro alle applicazioni, e non ai segmenti di rete. Ciò significa che gli utenti possono essere collegati direttamente alle applicazioni di cui hanno bisogno, mentre il traffico segue così il percorso più breve possibile, e gli amministratori e i team di sicurezza non devono più preoccuparsi dell'infrastruttura sottostante.

Si tratta di un approccio che non può essere implementato da un giorno all'altro, ma che, se adottato in modo attento, può semplificare la gestione dell'IT, della rete e della sicurezza, e offrire al contempo migliori prestazioni agli utenti finali.

SINTOMO N. 4

Il rischio che un'infezione si diffonda tra le risorse sul cloud pubblico

Sui loro marketplace di software online, i provider di servizi cloud pubblici offrono dei firewall virtuali che dovrebbero essere certificati per soddisfare le esigenze dei clienti. Spesso però questi firewall non sono altro che versioni virtuali di firewall basati su apparecchi fisici in esecuzione come istanze di VM sul cloud pubblico.

Se uno di questi firewall viene eseguito sul cloud, l'architettura di rete legacy viene praticamente estesa verso l'esterno, affinché includa le risorse cloud. In questo modo, gli aggressori che sono in grado di violare le difese basate sui firewall possono muoversi liberamente all'interno della rete estesa e far ottenere l'accesso alle risorse cloud a chiunque si trovi all'interno della rete.

Inoltre, la configurazione delle policy per gestire il traffico tra i carichi di lavoro sul cloud pubblico e nei cloud privati virtuali è caotica e complessa, e saranno necessarie delle istanze di firewall virtuali in ogni punto di uscita e di ingresso nell'architettura cloud. Se si pensa per un attimo all'interconnettività intrinseca del cloud, è facile comprendere perché questa configurazione risulta così problematica.

Inoltre, sarà necessario gestire un'infrastruttura di routing e di rete contorta al solo scopo di far funzionare questa architettura cloud insieme al resto della rete legacy.

Ricorda: i firewall non sono stati progettati per bloccare il movimento laterale.

QUAL È LA CURA?

- Investire in una piattaforma moderna, che agisca come punto di scambio tra i carichi di lavoro, indipendentemente dalla loro posizione. In questo modo, si impedisce agli aggressori di muoversi lateralmente per accedere alle risorse di rete, e si semplificano la gestione e la risoluzione dei problemi. Inoltre, questo approccio offre agli amministratori un controllo granulare e condizionale sugli accessi, che possono essere revocati se il contesto cambia.

SINTOMO N. 5

Dipendenza da policy troppo permissive

La trasformazione cloud sta cambiando il business in tutto il mondo, e le organizzazioni di tutti i settori stanno sfruttando l'agilità e la libertà di innovare offerte dal cloud.Se si è parte di un team IT o di sicurezza, è solo questione di tempo prima che ci si ritrovi a gestire un progetto di migrazione verso il cloud, se non lo si sta facendo già.

Il problema è che configurare delle architetture legacy basate su firewall per proteggere delle risorse cloud è un'operazione gravosa e complessa. Le policy proliferano, le complessità abbondano e a tutto ciò si aggiungono gli utenti che hanno bisogno di accedere alle applicazioni per essere produttivi. Qual è la soluzione?

Il 90% degli amministratori IT e della sicurezza ammette di aver applicato delle policy altamente permissive*, almeno temporaneamente, per accelerare i progetti e fornire agli utenti l'accesso richiesto. Nel corso del tempo, queste policy permissive si sommano e, alla fine, vengono ignorate o dimenticate, e aumentano il rischio di un'organizzazione di subire una violazione o un attacco ransomware devastante. Naturalmente, queste pratiche sono in diretta contraddizione con quelle dell'approccio fondato sullo zero trust e sull'accesso a privilegi minimi.

L'85%
delle organizzazioni adotterà una strategia cloud first entro il 2025.[5]

Il 95%
dei nuovi carichi di lavoro digitali oggi viene distribuito su piattaforme native del cloud.[5]

QUAL È LA CURA?

- Cercare una soluzione zero trust con base cloud semplice da implementare e da usare. Una piattaforma unificata zero trust, con un'unica console di gestione, sarà più facile da configurare e gestire, e offrirà al contempo una sicurezza più solida rispetto a un firewall perimetrale legacy.

5. Fonte: Gartner, "Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences"

SINTOMO N. 6

Esposizione alle potenziali infezioni provenienti da Internet

I firewall perimetrali sono stati progettati per agire da front-end della rete. Sono asset esposti a Internet per natura, che, in caso di violazione, consentono l'accesso diretto alle reti interne e alle risorse. Quindi, l'utilizzo di un firewall legacy come gateway per distribuire servizi VPN, mette intrinsecamente a rischio la rete.

La criticità di questi rischi è evidenziata da una serie di recenti violazioni andate a buon fine, condotte da aggressori che hanno sfruttato le vulnerabilità delle VPN tradizionali. L'attacco ransomware a Colonial Pipeline, il più grande attacco informatico reso noto pubblicamente contro delle infrastrutture critiche mai avvenuto negli Stati Uniti, si è verificato perché gli aggressori hanno "sfruttato una VPN legacy che non avrebbe dovuto essere in uso", secondo il CEO della società.[6]

Le VPN basate su firewall non consentono in alcun modo di implementare dei controlli di accesso granulari o di limitare gli utenti che possono connettersi a delle risorse specifiche. Quindi, affidandosi alle VPN si adotta un approccio fondato sul "tutto o niente", che estende la superficie di attacco della rete dal cloud fino ai router e alle reti wireless domestiche dei singoli dipendenti. Inoltre, più la rete si espande, più aumentano i potenziali danni e la velocità degli attacchi.

Le VPN basate su firewall non consentono in alcun modo di implementare dei controlli di accesso granulari o di limitare gli utenti che possono connettersi a delle risorse specifiche.

QUAL È LA CURA?

- Cercare un'alternativa alla VPN che consenta l'accesso sicuro alle applicazioni stabilendo connessioni one-to-one tra utenti e applicazioni su base dinamica e che prenda in considerazione identità e contesto. Queste soluzioni utilizzano connessioni inverse, dall'interno verso l'esterno, che rendono le app invisibili alla rete Internet pubblica, offrendo di conseguenza prestazioni migliori rispetto alle VPN e migliorando notevolmente la sicurezza.

6. Fonte: "Colonial Pipeline hack explained: Everything you need to know", TechTarget, aprile 2022.

SINTOMO N. 7

Congestione del traffico

L'impresa distribuita è ormai la nuova realtà del business e la maggior parte delle aziende sta adottando modelli di lavoro ibridi e da remoto per rimanere al passo con questa tendenza. Ma se si fa ancora affidamento su un'architettura di rete legacy basata sul modello a castello e fossato, e ci si ritrova a dover gestire un elevato numero di utenti da remoto, sarà necessario eseguire il backhauling di grandi quantità di traffico verso il data center aziendale, per consentirne l'ispezione da parte del firewall.

È superfluo scriverlo: questa architettura è complessa e adotta un approccio illogico. I firewall tradizionali e i set di soluzioni di sicurezza basati su dispositivi fisici sono dispendiosi in termini di tempo e complicati da gestire. Se si utilizzano linee MPLS in leasing, si pagherà un sovrapprezzo per via della complessa infrastruttura di routing, di switching e per la segmentazione del traffico. Questo è il motivo per cui sta crescendo l'interesse verso la SD-WAN (Software-Defined Wide Area Network), ma l'aggiunta di overlay di reti non fa che accrescere la complessità e i costi associati alla gestione dei firewall.

Se si effettua il backhauling del traffico, le prestazioni delle applicazioni e l'esperienza dell'utente finale ne risentono. Per non parlare della latenza, un problema annoso destinato a diventare ancora più gravoso, in quanto le organizzazioni si affidano sempre più pesantemente ad app di comunicazione che richiedono un'ampia larghezza di banda, come Zoom e Microsoft Teams.

QUAL È LA CURA?

- Con una soluzione zero trust con base cloud, i controlli di sicurezza si trovano dove si trovano anche gli utenti e le applicazioni: sul cloud. Una piattaforma zero trust applica le policy inline e all'edge, in modo che il traffico non debba compiere ulteriori hop; inoltre, poiché opera nel percorso dei dati, è in grado di monitorare ogni connessione e di individuare e risolvere automaticamente i problemi delle prestazioni.

LA CURA È LO ZERO TRUST

Perché Zscaler rappresenta la cura per la tua rete e la sua architettura

Zero Trust Exchange™ di Zscaler è una piattaforma nativa nel cloud creata appositamente per supportare lo zero trust. Zero Trust Exchange consente di stabilire connessioni dirette e sicure basate sul principio dell'accesso a privilegi minimi; inoltre, prima di consentire qualsiasi connessione, ispeziona i contenuti accuratamente e verifica i diritti di accesso in base all'identità e al contesto.

Il motore di policy basato su IA/ML di Zscaler, supportato dal security cloud più grande del mondo, apprende il contesto in base alle informazioni su utenti, dispositivi e applicazioni, e lo utilizza per prendere decisioni intelligenti sui livelli di accesso e sulle restrizioni, preservando così la sicurezza degli utenti e dei dati. Inoltre, Zero Trust Exchange agisce da broker per le connessioni one-to-one tra utenti e applicazioni, e garantisce che queste ultime siano invisibili a Internet, eliminando di conseguenza la superficie di attacco.

Il nostro approccio rende la sicurezza zero trust accessibile e semplice per i nostri clienti. Ecco perché i leader del settore e gli analisti esperti sono d'accordo nel considerare Zero Trust Exchange la piattaforma zero trust più evoluta e più facile da usare.

La distribuzione di Zero Trust Exchange è facile e veloce; inoltre, questa piattaforma offre una gamma completa di funzionalità integrate di sicurezza inline, che potenziano le sue funzioni principali di Security Service Edge (SSE).
Queste funzioni includono:

- **Firewall di nuova generazione**
- **Sandboxing avanzato sul cloud**
- **Secure Web Gateway (SWG)**
- **Prevenzione sulla perdita dei dati (DLP)**
- **CASB**
- **e molto altro**

Per maggiori informazioni, visita:
www.zscaler.it/products/zscaler-internet-access

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zero Trust Exchange di Zscaler protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata sull'SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it