WHITE PAPER

Oltre l'SD-WAN: la sicurezza Zero Trust e Internet come WAN aziendale

Perché SD-WAN, accesso sicuro e protezione dalle minacce vanno insieme

Akamai

Il futuro della rete WAN aziendale

Le reti WAN (Wide Area Network) esistono sin dagli anni '60, epoca degli albori della comunicazione tra computer. Continuano ad essere sviluppate e migliorate, con l'evolversi della tecnologia e della domanda di traffico. Per le aziende di oggi, le WAN sono un'infrastruttura che consente una rete unificata in qualunque posizione.

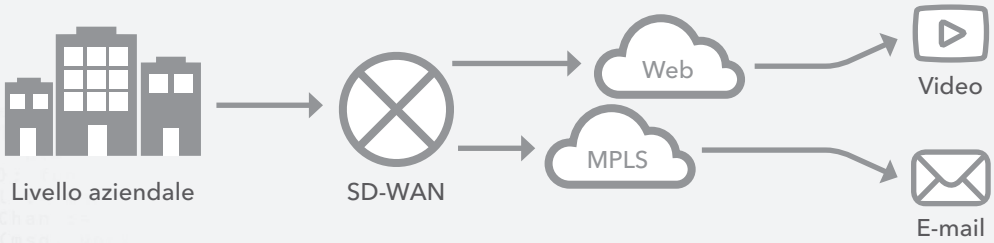
Tuttavia, questa sottostruttura critica non è priva di limitazioni. Le WAN spesso offrono una larghezza di banda bassa o insufficiente, causano problemi di performance di applicazioni specifiche, hanno un'affidabilità altalenante e potrebbero comportare rischi per la sicurezza della vostra azienda. Inoltre, le WAN vengono spesso realizzate su linee dedicate o fornite da provider di servizi la cui infrastruttura utilizza metodi di commutazione di circuito o di pacchetto, come ATM (Asynchronous Transfer Mode) e MPLS (Multiprotocol Label Switching), oltre all'Internet pubblico. Anche se quest'ultimo è in certa misura l'opzione meno costosa, è comunque molto costoso e non si presta a scalabilità.

La rete aziendale si sta trasformando

In risposta a queste sfide in termini di performance, sicurezza e costi, le aziende adottano SD-WAN (WAN definite da software), riducendo i costi e garantendo flessibilità.

A partire dall'innovazione delle tecnologie SDN (Software-Defined Networking) ed NFV (Network Function Virtualization) utilizzate in origine nei data center, i reparti IT hanno adottato rapidamente la tecnologia per le reti che garantivano le connessioni delle organizzazioni.

In altre parole, l'SD-WAN separa i dati e i piani di controllo della rete WAN. L'SD-WAN monitora le performance dell'insieme di connessioni dati WAN (MPLS, ATM e Internet) e seleziona la connessione più appropriata per ogni tipo di traffico, in base alle performance dei collegamenti attuali, al costo della connessione e alle esigenze dell'applicazione o del servizio.



SD-WAN in azione

Una SD-WAN potrebbe indirizzare le e-mail tramite MPLS, perché la latenza non è un grande problema e il costo per bit inviato è quello più basso. Per contro, l'SD-WAN potrebbe indirizzare il traffico delle videoconferenze tramite Internet per garantire performance ottimali e latenza minima, ma un costo per bit inviati maggiore.

Internet può diventare la nuova WAN aziendale?

Le SD-WAN possono essere certamente flessibili, efficienti e convenienti se utilizzano più servizi di trasporto, compreso l'Internet pubblico. Ma poiché non esistono garanzie sulle performance o accordi sul livello di servizio (SLA) per queste opzioni di trasporto, le SD-WAN utilizzano Internet esclusivamente per le applicazioni le cui performance non sono di primaria importanza.

Per migliorare l'uso di Internet allo scopo di offrire ulteriore traffico WAN aziendale in modo efficiente, conveniente e sicuro, ma anche in un modo che possa coesistere con le distribuzioni di SD-WAN correnti, dovrete adottare un approccio che elimini le limitazioni soggiacenti di Internet. Un modo per farlo è utilizzare una piattaforma edge per offrire applicazioni aziendali sicure, rapide e affidabili su Internet, senza esporle pubblicamente su Internet. Ciò vi consente di ottimizzare i vostri attuali investimenti nelle reti SD-WAN, riducendo i costi durante lo spostamento di altro traffico su Internet.

Effettuare il routing di una fetta maggiore di traffico aziendale su Internet ha semplicemente senso data la traiettoria delle moderne reti aziendali. L'aumento dei carichi di lavoro sul cloud, insieme a utenti mobili e dispositivi diversificati, implica che i workflow fanno un uso già ampio di Internet. E questa tendenza continua a diffondersi.

E se si potesse fare un ulteriore passo avanti, creando una WAN aziendale sicura, scalabile ed efficiente su Internet?

In questo articolo, parleremo dei processi di trasformazione della rete grazie all'SD-WAN e alla sicurezza Zero Trust, per far sì che la vostra organizzazione sia in grado di evolversi al di là dell'SD-WAN, adottando una rete aziendale interamente basata su Internet.

Una piattaforma edge vi consente di offrire applicazioni aziendali sicure, rapide e affidabili su Internet, senza esporle pubblicamente su Internet.

> *Entro la fine del 2023, più del 90% delle iniziative di aggiornamento dell'infrastruttura edge WAN si baseranno su piattaforme vCPE (virtualized Customer Premises Equipment) o software/appliance con WAN definite da software (SD-WAN), invece che sui router tradizionali (partendo da meno del 40% di oggi)".*
>
> *- Magic Quadrant di Gartner per l'infrastruttura edge WAN, ottobre 2018*

Il valore dell'SD-WAN

L'SD-WAN fornisce, in primo luogo, equilibrio dei collegamenti, configurazione automatica dei dispositivi e inserimento dei servizi di sicurezza di terze parti. Il valore di queste funzioni, ossia una user experience migliore, la riduzione dei costi dei collegamenti e dell'OpEx, può avere un impatto notevole. L'utilizzo è ben definito e il riscontro evidente.

Decine di fornitori offrono varie funzionalità per SD-WAN, ma è possibile generalizzarle ampiamente in tre categorie:

1. *Controllo flessibile dei collegamenti*
2. *Gestibilità*
3. *Inserimento dei servizi*

Controllo flessibile dei collegamenti

La prima funzionalità, il controllo flessibile dei collegamenti, è l'obiettivo principale dell'SD-WAN. Poiché il cloud è la destinazione principale di molte organizzazioni, trasmettere il traffico su una rete privata verso un data center, fungendo di fatto da punto di controllo centralizzato, non è pratico. L'SD-WAN risolve questa sfida utilizzando il controllo del traffico intelligente, che comprende la selezione dinamica dei percorsi. Inoltre, l'SD-WAN stabilisce breakout locali o Internet delle filiali, anche noti come DIA (Direct Internet Access), in grado di indirizzare il traffico sul cloud anziché tramite un data center. Pertanto, tutte le applicazioni legacy, come quelle vocali e video, sono progettate per collegamenti MPLS, mentre le applicazioni cloud e il traffico Internet vanno direttamente su Internet.

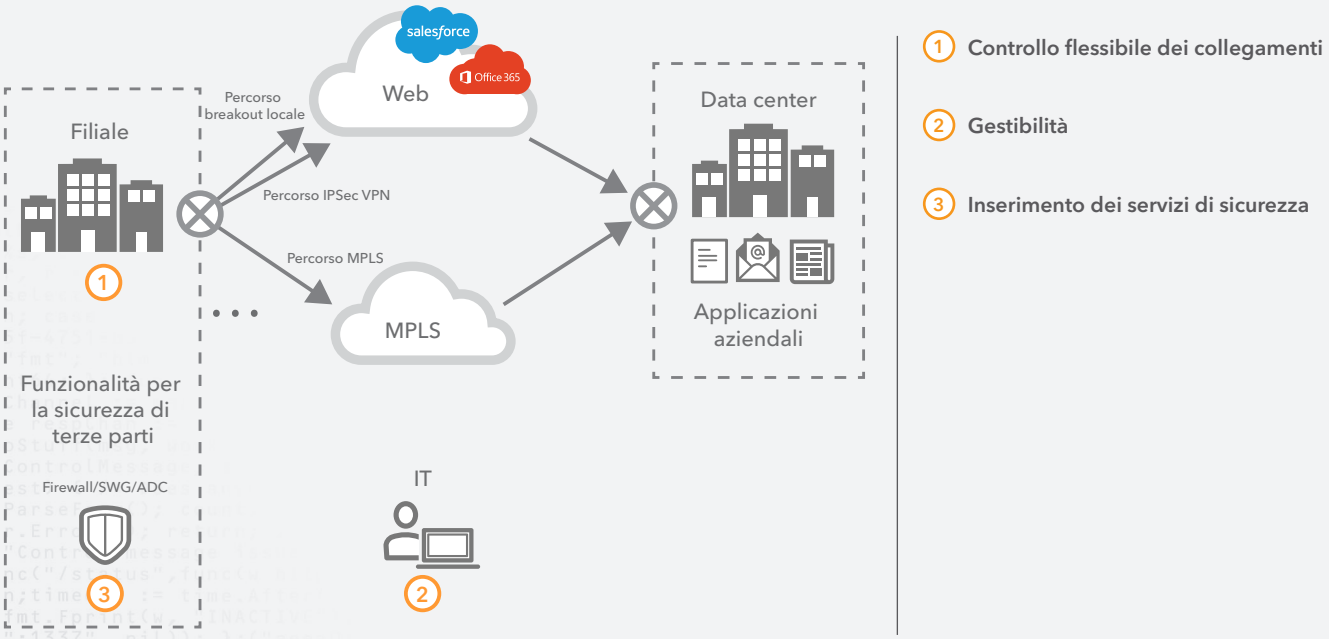
Gestibilità

I fornitori di SD-WAN possono anche offrire gestibilità, semplificando il funzionamento e la gestione dei dispositivi di rete. Sin dagli anni '90, le WAN aziendali sono state composte da dispositivi di rete come router e switch multilivello. Questi dispositivi sono stati gestiti per la gran parte in base al tipo di appliance. In altre parole, gli amministratori devono configurare e gestire da centinaia a migliaia di dispositivi singolarmente, monitorando lo stack software di ognuno di essi all'interno dell'organizzazione. Anche se i dispositivi scambiano in modo dinamico informazioni di routing o stabiliscono un'elevata disponibilità tramite protocolli di routing, l'impegno è enorme. Con l'SD-WAN, tutta la gestione dei dispositivi può essere portata a termine con un'unica console centralizzata.

Inserimento dei servizi

Infine, alcuni provider di SD-WAN si specializzano nell'inserimento dei servizi. Il requisito minimo per la WAN è la raggiungibilità dell'IP, ossia della connettività di rete di livello 3 nell'organizzazione. Tuttavia, con l'evolversi della rete, si sono evolute anche le funzioni di sicurezza: firewall, IPS (Intrusion Protection System, sistemi di protezione dalle intrusioni) e ADC (Application Delivery Controller), solo per nominarne alcune. In passato, era necessario un design di routing complesso per aggiungere queste funzionalità alla rete, in quanto i dispositivi che offrono questi servizi in genere non sono in grado di comunicare con protocolli di routing dinamici (Open Shortest Path First [OSPF], Border Gateway Protocol [BGP]), il che produce una complessa combinazione di ridistribuzione e routing statico. L'SD-WAN rende queste tecnologie, spesso fornite da terze parti, semplici da configurare e da gestire grazie a un portale unificato.

Il valore dell'SD-WAN per l'azienda

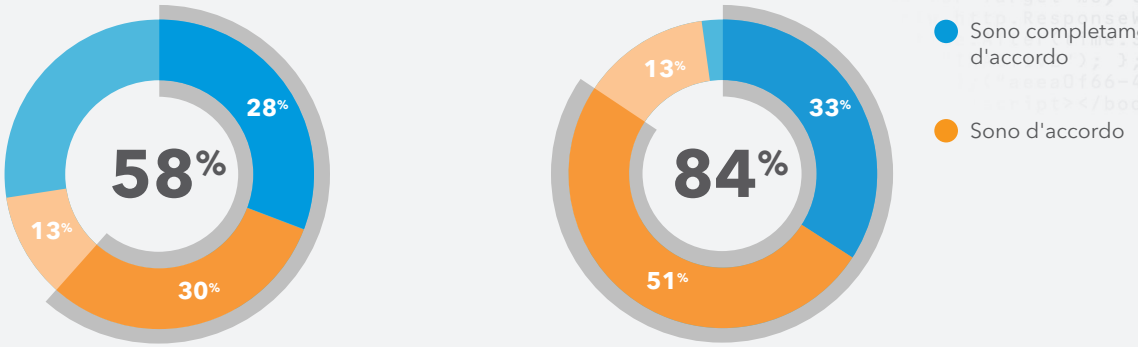


1. Controllo flessibile dei collegamenti
2. Gestibilità
3. Inserimento dei servizi di sicurezza

Un nuovo modello: la sicurezza Zero Trust

Una nuova architettura richiede nuovi metodi di sicurezza. Mentre le transazioni si spostano sul cloud e su Internet, le reti sono diventate ampiamente distribuite, creando ulteriori superfici di attacco. Le applicazioni, gli utenti, i dati e i dispositivi si stanno spostando al di fuori della tradizionale zona di controllo, dissolvendo quello che un tempo era l'affidabile perimetro aziendale. Pertanto, realizzare e applicare un modello di sicurezza che si basi su un perimetro aziendale non è più fattibile. Una strategia di difesa moderna deve essere adatta ai carichi di lavoro e alla forza lavoro distribuiti di oggi.

Fino a che punto siete/non siete d'accordo?



"Il perimetro di rete è indifendibile nell'ecosistema della tecnologia odierna di reti cloud distribuite e utenti mobili/remoti".

"La trasformazione digitale necessita di modifiche alle tradizionali strategie di sicurezza (perimetrali)".

Forrester Research, Realizzate la vostra strategia di sicurezza Zero Trust con la microsegmentazione (in inglese), settembre 2018

Un modello di sicurezza Zero Trust si basa sull'assunto che non esiste un "dentro" e che tutti gli utenti e tutti i dispositivi sono potenzialmente inaffidabili, senza distinzioni. Ogni richiesta di accesso necessita di autenticazione e autorizzazione. Applicazioni e dati vengono distribuiti solo dopo una verifica e, persino allora, su una base transitoria e con un ambito limitato. Questo sistema di sicurezza tratta tutte le applicazioni come interfacciate con Internet e considera la rete come compromessa e ostile. Inoltre, la visibilità è fondamentale; log completi e analisi comportamentali sono un elemento indispensabile.

Tra i principi fondamentali della sicurezza Zero Trust vi sono:

- *Garantire un accesso sicuro a tutte le risorse, a prescindere dalla posizione o dal modello di hosting*
- *Adottare una strategia che si basi sul principio dei "privilegi minimi" e del "rifiuto dell'accesso per impostazione predefinita", quando si abilita l'accesso alle applicazioni*
- *Ispezionare e registrare il traffico, sia per applicazioni da voi controllate che per quelle che non controllate, al fine di identificare attività dannose*

Esistono due componenti principali che supportano l'implementazione della sicurezza Zero Trust:

- *Proxy sensibile all'identità per un accesso sicuro alle applicazioni*
- *Secure Internet Gateway per proteggere gli utenti*

Proxy sensibile all'identità per un accesso sicuro alle applicazioni

Se gli utenti, i dati e le applicazioni si trovano sul cloud e il DIA abilitato dall'SD-WAN fornisce la connessione, perché non spostare anche la sicurezza e lo stack DMZ sul cloud? In questo modo, è possibile sfruttare un modello Zero Trust per garantire un accesso sicuro alle applicazioni che controllate, mitigando il rischio associato agli utenti che accedono alle applicazioni che non controllate.

Se attualmente optate per una semplice configurazione VPN per fornire accesso alle applicazioni aziendali, probabilmente consentite agli utenti connessi un accesso di livello IP alla vostra intera rete. Ma tutto questo è molto rischioso e va contro i principi fondamentali della sicurezza Zero Trust. Perché i dipendenti di un call center hanno l'autorizzazione ad accedere agli archivi dei codici sorgente? Perché un collaboratore che usa il vostro sistema di fatturazione ha il diritto di accedere ai terminali di elaborazione delle carte di credito? Dovrebbe essere concesso di accedere soltanto alle applicazioni necessarie per svolgere il proprio ruolo. La VPN tradizionale non consente questo accesso granulare, ma fa un affidamento continuato a un modello di rete hub and spoke.

Un'architettura IAP (proxy sensibile all'identità) consente di accedere alle applicazioni tramite un proxy basato su cloud. L'identità e l'autorizzazione avvengono sull'edge e si basano sui principi di privilegio minimo e previa identificazione, simili all'accesso tramite SDP (Software Defined Perimeter), ma utilizzano protocolli HTTPS standard a livello delle applicazioni (livello 7).

I due modi in cui funziona l'IAP

Si integra una CDN nelle transazioni tra vari paesi per migliorare la risposta dell'applicazione

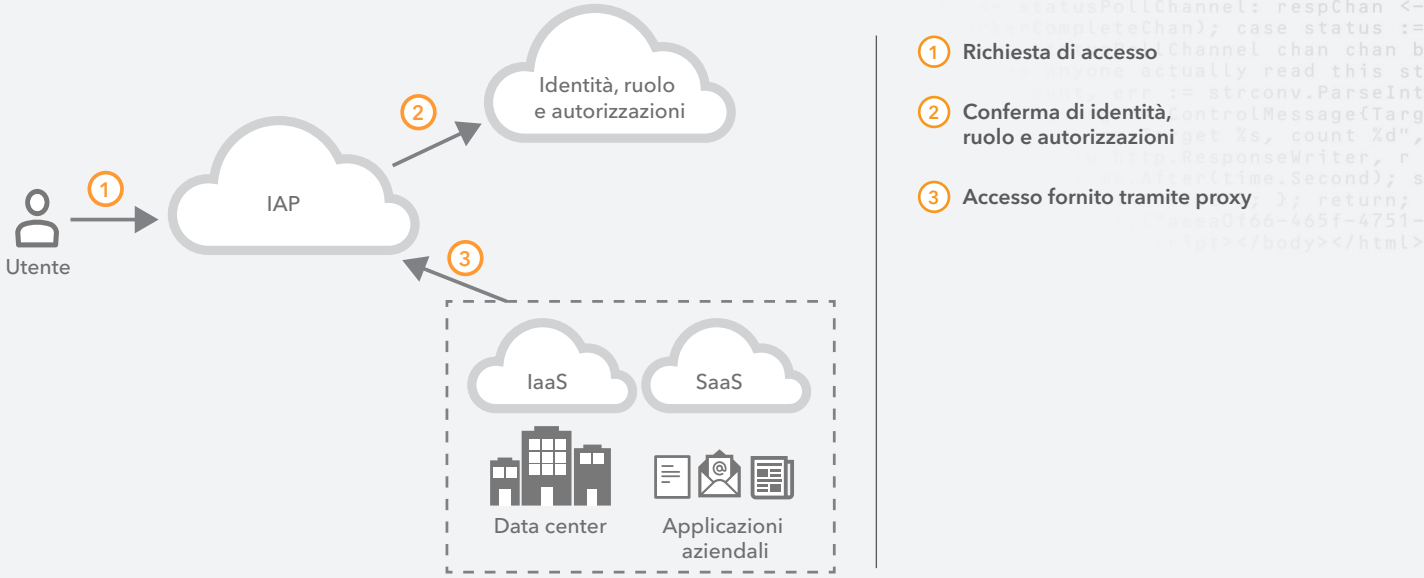
OPPURE

Si usa un WAF (Web Application Firewall) per proteggere i server web aziendali da vulnerabilità comuni, come SQL injection e Cross-Site Scripting.

Un componente chiave di un IAP è una fonte di identità che verifica l'attendibilità di utenti e dispositivi (autenticazione) e ciò a cui possono accedere (autorizzazione). Questa fonte di identità può basarsi su directory aziendali o provider di identità basati sul cloud. Anche prima di confermare l'identità di un utente, verificando la posizione di un dispositivo è possibile garantire che il dispositivo che sta tentando di ottenere l'accesso soddisfi determinati criteri di sicurezza, ad es. che abbia un certificato, disponga della versione più recente del sistema operativo, sia protetto da password o che su di esso sia installata e funzionante la soluzione di rilevamento degli endpoint e di risposta più appropriata.

Un notevole vantaggio dell'IAP rispetto ad altre tecnologie di accesso: non solo gli utenti vengono controllati, ma viene anche analizzato il traffico degli utenti ed è possibile rifiutare, esaminare e autorizzare le richieste delle singole applicazioni. Una volta terminata una transazione sul proxy, è possibile integrare ulteriori servizi, per consentire una migliore user experience e protezione delle applicazioni.

IAP (proxy sensibile all'identità)



L'IAP si basa anche su un controllo degli accessi a livello di applicazione, non sulle regole del firewall; le policy configurate possono riflettere l'intenzione di utenti e applicazioni, non solo di porte e IP. Proprio come l'SDP, questo approccio è in grado di rendere invisibili le applicazioni e altre risorse nel cloud o dietro il firewall e non si basa su client per le applicazioni web.

Mentre si utilizza sempre di più il cloud, ci si concentra ora sulla sfida posta dalla migrazione delle applicazioni aziendali. Molte organizzazioni si sforzano di sfruttare il cloud sia per applicazioni cloud native che per quelle tradizionali. Non solo l'IAP può essere utilizzato per autenticare gli utenti per applicazioni native SaaS, ma principalmente anche per "SaaSificare" le applicazioni legacy nel data center. Inoltre, un proxy facilita la migrazione sul cloud e l'ammodernamento delle applicazioni senza ricorrere a una strategia di rinnovamento totale. Di conseguenza, le imprese possono adottare un approccio metodico passo passo all'implementazione del modello Zero Trust, riducendo il debito tecnico associato ai controlli perimetrali legacy e alle VPN tradizionali.

Secure Internet Gateway per proteggere gli utenti

Un aspetto critico della transizione a un modello di sicurezza Zero Trust è garantire che gli utenti restino al sicuro mentre accedono alle applicazioni che non sono sotto il vostro controllo. Un vasto numero di minacce informatiche si nasconde dietro ogni clic su Internet. In passato, quando gli utenti erano legati a dispositivi di rete aziendale e gestiti, la protezione dai malware, dai ransomware e dal phishing era semplice come lanciare antivirus su endpoint, installando uno stack di appliance in un data center e trasmettendo il traffico per l'ispezione e il controllo.

Con utenti presenti in vari luoghi, Internet diventa la rete aziendale prescelta; un SIG basato sul cloud vi offre un collegamento sicuro, proteggendo gli utenti in modo proattivo, ovunque essi siano.

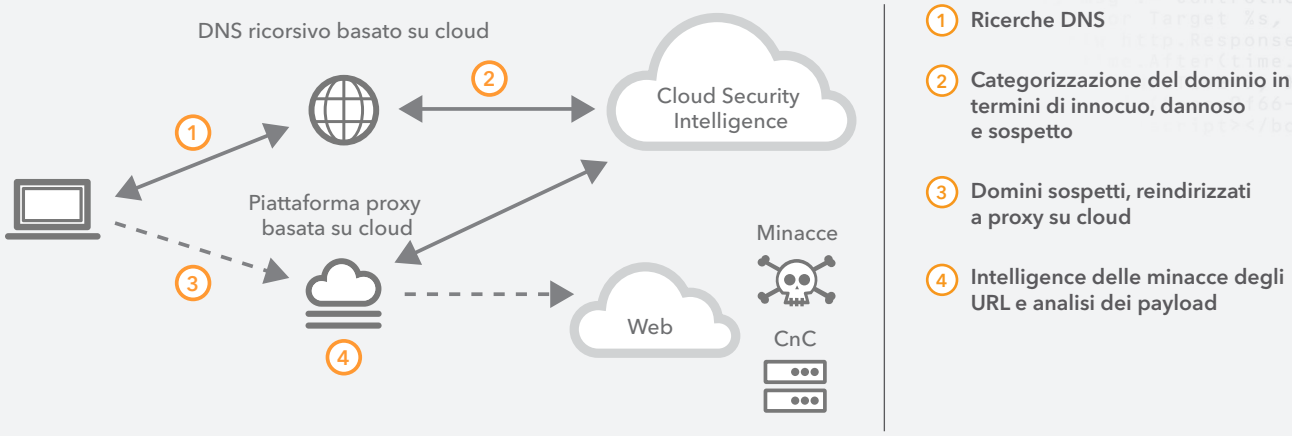
Ma gli utenti escono dagli edifici, i dispositivi non sono gestiti e Internet sta diventando la rete aziendale prescelta. La connettività DIA rende obsolete le soluzioni di controllo centrale e di sicurezza delle ispezioni. Un'alternativa è replicare lo stack di appliance di sicurezza in ogni breakout Internet. Tuttavia, per molte imprese, questo è un fallimento in partenza, sia dal punto di vista logistico che finanziario. E, forse cosa più importante, la complessità intrinseca di questo approccio introduce carenze di sicurezza, progettato in diretta opposizione alle best practice del modello Zero Trust.

Un metodo più semplice, più veloce e conveniente per proteggere il traffico DIA è usare un SIG (Secure Internet Gateway) basato sul cloud. Un SIG è un collegamento sicuro a Internet, che protegge gli utenti in modo proattivo da minacce avanzate, a prescindere dalla loro posizione, con un proxy del traffico rischioso, per finalità di controllo e ispezione. Ciò si ottiene esaminando ogni richiesta DNS, bloccando richieste a domini dannosi, consentendo alle richieste a domini sicuri di procedere normalmente e inoltrando le richieste a domini rischiosi a un proxy basato su cloud, per ulteriori indagini.

In quest'ultima fase, quando il proxy riceve una richiesta HTTPS, confronta l'URL richiesto con la knowledge base sull'intelligence sulle minacce basata sul cloud e blocca gli URL dannosi. Per tutti gli altri URL richiesti, categorizzati come rischiosi, il proxy invia i contenuti web per l'analisi dei payload in linea tramite più motori di analisi dei malware. Questi motori usano una serie di tecniche di rilevamento (con firma, senza firma e apprendimento automatico), per identificare e bloccare le minacce note e le minacce zero-day precedentemente sconosciute. Con una serie di metodi di rilevamento a disposizione, è possibile indirizzare un payload al motore (o ai motori) più adatto a seconda del tipo di contenuto, il che garantisce tassi di rilevamento ottimali e una bassa quantità di falsi positivi.

È importante notare che questo approccio è abbastanza diverso da quello adottato dalle appliance di sicurezza legacy, come gli SWG (Secure Web Gateway). Nello specifico, gli SWG eseguono il proxy di tutto il traffico Internet, analizzando quello buono e quello dannoso, il che può essere negativo specialmente per le pagine web complesse e i contenuti HTTPS più pesanti. Questo approccio deteriora le performance, introduce la latenza e aumenta il volume dei siti web e delle applicazioni danneggiati in seguito alla trasmissione proxy di tutto il traffico. Gli SWG spesso causano altri incidenti relativi alla sicurezza e falsi positivi, facendo aumentare le richieste di assistenza e monopolizzando le risorse IT.

Architettura SIG (Secure Internet Gateway)



Un proxy intelligente e selettivo può sfruttare la DNS come collegamento a Internet e primo livello di sicurezza. Consentendo di instradare il traffico sicuro direttamente su Internet, bloccando il traffico dannoso e inoltrando al proxy solo il traffico rischioso, questo approccio offre:

- *Sicurezza semplificata*
- *Latenza ridotta e migliori performance*
- *Minor numero di applicazioni e pagine web danneggiate*

Trasformazione della rete con meno rischi: implementare il modello Zero Trust in un ambiente SD-WAN

Molte organizzazioni che stanno effettuando la migrazione ad architetture basate su Internet danno all'SD-WAN il ruolo di abilitatore, per via del controllo dei collegamenti e della capacità di ridurre potenzialmente gli oneri finanziari relativi alla proprietà dell'MPLS. Possono utilizzare reti a banda larga o wireless per espandere o completare le connessioni MPLS, creando una WAN ibrida. Ma se utilizzano già il DIA, allora ha senso impiegare un modello di sicurezza con lo stesso approccio.

Man mano che viene utilizzata l'SD-WAN, le aziende devono evolvere la propria strategia di sicurezza da un sistema basato sul perimetro a un sistema basato su Zero Trust sull'edge. Allora oggi com'è la situazione e cosa succederà dopo?

In genere, le reti con l'SD-WAN sono presenti in tre scenari, a seconda della mentalità e della strategia a lungo termine dell'azienda:

1. *WAN privata tradizionale con breakout centralizzati; si sta prendendo in considerazione l'SD-WAN, ma non è stata ancora implementata*
2. *Implementazione ibrida della rete WAN privata tradizionale in siti esistenti e dell'SD-WAN in nuove filiali*
3. *Principalmente SD-WAN*

Un approccio di sicurezza Zero Trust può adattarsi bene a tutti questi scenari. Tuttavia, se l'azienda sta già implementando o pensando di implementare l'SD-WAN, potrebbe aver già adottato Internet come strumento di rete aziendale idoneo e, pertanto, è preparata per utilizzare una strategia di sicurezza Zero Trust per il proprio ambiente di rete aziendale.

Esaminiamo le architetture attuali per identificare come implementare un modello Zero Trust e poi spostarsi verso lo stato futuro desiderato.

Rete WAN privata tradizionale con breakout centralizzati

Se le motivazioni dietro la migrazione all'SD-WAN sono il costo, la flessibilità e l'agilità (vantaggi che un'architettura di rete basata su Internet è in grado di offrire), può avere senso ignorare del tutto l'SD-WAN e passare direttamente a un sistema Zero Trust. L'IAP consente un accesso basato su un modello Zero Trust alle applicazioni, a prescindere dalla posizione, mentre il SIG fornisce agli utenti un accesso a Internet sicuro, il tutto senza che le organizzazioni debbano realizzare stack di sicurezza in ogni breakout Internet.

Un punto da tenere a mente: se l'azienda supporta già servizi in tempo reale come il VoIP e le videoconferenze tramite un provider di servizi cloud Internet, si trova nella posizione ideale per adottare completamente un'architettura di rete e di accessi basata su Internet. Se questi servizi sono ancora posti principalmente in sede, potrebbe essere necessario conservare un certo livello di reti "private" tra i luoghi: private (ad es. basate su MPLS) o basate su SD-WAN.

Ibrida con WAN tradizionale ed SD-WAN

In questo scenario, le organizzazioni hanno già compiuto il primo passo verso un'architettura più efficiente, basata su Internet.

In questi ambienti, è importante capire in che modo viene gestito il traffico:

- *Gli utenti hanno un DIA da uffici in remoto oppure il collegamento Internet viene utilizzato solo per fare rete di nuovo sui siti principali?*
- *Dove si trovano le applicazioni principali degli utenti? Nella sede fisica, in un data center oppure sul cloud?*
- *Se viene usato il cloud, in che modo gli utenti si collegano a queste applicazioni? Viene fornito un DIA semplice da una filiale oppure viene trasmesso a un collegamento per la connessione diretta?*
- *Quanto è ampio l'uso di applicazioni SaaS?*
- *Per DIA a livello di filiale, quanto è completo lo stack di sicurezza in ogni sede?*

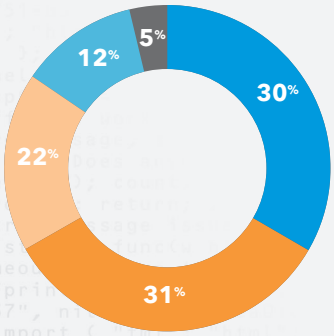
Le risposte, ovviamente, varieranno a seconda del trattamento del traffico degli utenti e, come tale, la migrazione di rete presenterà gradi di complessità variabili. Ma esistono due costanti: ci saranno un aumento nell'uso di Internet e il bisogno di passare da una sicurezza perimetrale a un modello Zero Trust.

Prendete, ad esempio, una situazione in cui ci sia una connettività DIA da un ufficio in remoto. Un SIG può permettersi una protezione aggiuntiva per lo stack di sicurezza centralizzato, nonché sostituire parte dello stack, riducendo la complessità e i costi.

Se gli utenti accedono ad applicazioni basate su cloud, un approccio basato su IAP potrebbe sia rafforzare l'approccio di sicurezza dell'organizzazione che migliorare la user experience. Potrebbe anche aumentare le performance delle applicazioni, consentendo un accesso diretto alle applicazioni su Internet con una CDN.

Potrete continuare a spostarvi dalla rete WAN tradizionale a un ambiente SD-WAN servendovi di un DIA per gli uffici in remoto e adottando i principi del modello di sicurezza Zero Trust.

Quali sono i vostri piani di business relativi all'uso della tecnologia di rete SD-WAN (WAN definita da software) oggi?



- Attualmente in uso
- Esecuzione di test entro il prossimo anno
- Adozione nei prossimi due anni
- Probabile uso, ma nessuna pianificazione
- Nessun probabile uso e nessuna pianificazione

Forrester Research, La trasformazione digitale svela i punti deboli delle reti distribuite dei negozi (in inglese), aprile 2018

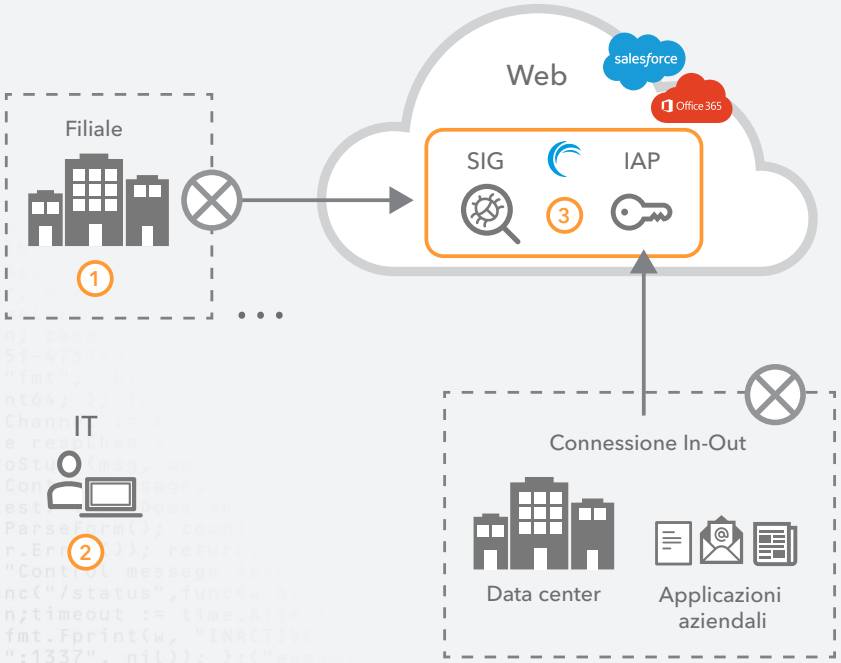
Principalmente SD-WAN

In questo stato, le organizzazioni probabilmente avranno rinunciato a una rete WAN privata tradizionale, utilizzando un routing intelligente tramite i collegamenti Internet tra i siti per la comunicazione tra i vari uffici, sfruttando appieno i vantaggi del DIA. Queste aziende si affidano già a un accesso a Internet per la maggior parte dei siti, per cui far evolvere la rete al di là dell'SD-WAN è la direzione più logica da prendere.

Il passaggio successivo? Iniziare a ridurre l'uso di collegamenti MPLS spostando le applicazioni su Internet, per offrire flessibilità ed efficienza dei costi. È possibile accedere alle applicazioni aziendali tramite IAP anche in un ambiente DIA. Se le applicazioni si trovano già in un ambiente cloud, non ha senso farvi accesso trasmettendo il traffico a un data center prima di creare una connessione in una posizione centralizzata (ad es. tramite una topologia per la connessione diretta).

Infine, questo ambiente è molto adatto a una connettività e a un accesso futuri basati su Internet. È possibile accedere a tutte le applicazioni aziendali tramite IAP, che si trovino in sede o sul cloud. Tramite il SIG è possibile proteggere tutto il traffico degli utenti. E, se i provider basati su Internet offrono comunicazioni in tempo reale, come quelle vocali e video, potrebbe essere possibile eliminare del tutto l'SD-WAN e persino la WAN aziendale. Ciò potrebbe ridurre i costi e le complessità, nonché migliorare la sicurezza tramite un modello di architettura Zero Trust.

Il valore di un'architettura basata su Internet con un modello di sicurezza Zero Trust



1. **Il più semplice accesso di rete**
   - Solo accesso a Internet
   - Nessun accesso out-in
2. **Gestibilità**
   - Singolo punto di gestione
   - Monitoraggio dei dispositivi
   - Monitoraggio degli utenti
3. **Maggiore controllo della sicurezza**
   - Prevenzione di attacchi zero-day
   - AAA centralizzata (Authentication, Authorization, Accounting)
   - Controllo del grado di sicurezza basato su client
   - Prevenzione di phishing, malware e CnC

Trasformare le attività aziendali

Le moderne realtà delle aziende aumentano l'esposizione in un ambiente già pieno di rischi e complessità. Un modello di rete regolato da transazioni hub and spoke su una WAN privata è obsoleto tanto quanto una difesa perimetrale per l'azienda; le architetture di rete e di sicurezza devono evolversi. Mentre l'SD-WAN attualmente consente alla rete aziendale di gestire in modo efficiente il traffico e spostare i carichi di lavoro sul cloud, questo modello di rete deve continuare a ripetersi. Internet è la rete WAN aziendale del prossimo futuro.

Akamai ritiene che l'uso dell'SD-WAN, combinato a servizi di sicurezza e accesso conformi al modello Zero Trust, sia il primo passo verso il passaggio a Internet come rete aziendale. Abbinate l'SD-WAN all'Akamai Intelligent Edge Platform, per poter applicare policy di accesso e di sicurezza universali e garantire agli utenti finali experience rapide e affidabili con le applicazioni su Internet.

Akamai può aiutarvi a controllare l'evoluzione della rete e del sistema di sicurezza. Contattate il vostro account team, per ulteriori informazioni sulla valutazione Zero Trust di Akamai: i nostri esperti di sicurezza vi daranno dei consigli concreti su come iniziare o continuare il vostro processo di trasformazione Zero Trust. In alternativa, visitate *3 semplici modi per iniziare a implementare il modello Zero Trust oggi stesso* per consultare le risorse necessarie ad avviare la vostra transizione.