FORTINET

WHITE PAPER

Approfondimento sugli ostacoli alla trasformazione della WAN

Sicurezza, prestazioni e TCO

Sintesi preliminare

I responsabili della gestione tecnica e operativa della rete stanno volgendo lo sguardo alle reti definite da software in una rete estesa (SD-WAN) per supportare l'afflusso di traffico e applicazioni determinato dalla trasformazione digitale (DX). Queste applicazioni migliorano la produttività del personale creando al contempo nuove opportunità di business, ma ridisegnano anche le esigenze aziendali di rete e sicurezza.

Molte organizzazioni stanno, pertanto, iniziando a ripensare la loro architettura WAN tradizionale. Come alternativa è emersa la SD-WAN, che però in molte implementazioni pone anche notevoli sfide, da una sicurezza inadeguata a un elevato costo totale di proprietà (TCO). L'approfondimento di queste problematiche è fondamentale per orientarsi nel mercato sempre più complesso delle tecnologie per le WAN.

Secondo IDC, il mercato delle SD-WAN registrerà un tasso di crescita annuo composto (CAGR) superiore al 40% entro il 2022.[1]

"La comparsa della tecnologia SD-WAN è stata una delle trasformazioni industriali più rapide alle quali abbiamo assistito nel corso degli anni. Le organizzazioni di tutte le dimensioni stanno modernizzando le loro WAN per offrire all'utente una migliore esperienza in un'ampia gamma di applicazioni cloud-enabled".[2]

– Rohit Mehra
VP, Network Infrastructure
IDC

Come la Digital Transformation sta influendo sulle reti aziendali

Sempre più numerose sono le organizzazioni che intraprendono iniziative di Digital Transformation (DX), dalla crescente adozione di video e Voice over IP (VoIP) per la collaborazione, la gestione di progetti e persino lo sviluppo aziendale, all'uso di DevOps per accelerare la distribuzione di nuove applicazioni web, passando per l'utilizzo di dispositivi IoT (Internet of Things) per la telemetria e la raccolta di dati.

Per la filiale o l'ufficio distaccato, tuttavia, queste iniziative DX presentano nuove sfide, e il responsabile della gestione tecnica e operativa della rete ha il compito di mantenere le prestazioni e la sicurezza della rete, dal campus del data center al perimetro della rete. Tuttavia, le WAN tradizionali non sono progettate per supportare il volume e la velocità del traffico che viene inoltrato verso filiali e uffici distaccati. In particolare, queste soluzioni WAN utilizzano una rete basata su MPLS (Multiprotocol Label Switching) che effettua il backhaul di tutto il traffico di rete attraverso il data center aziendale per il filtering e i controlli di sicurezza, un'architettura hub-and-spoke che può creare strozzamenti lungo il perimetro con conseguente rallentamento delle prestazioni per gli utenti finali.

Questo, però, non è l'unico problema delle soluzioni WAN tradizionali. Le connessioni MPLS sono costose, e il costo può aumentare velocemente in maniera esponenziale, soprattutto a causa del rapido aumento dei volumi di traffico di filiali e uffici distaccati.

Raccogliere le sfide della WAN tradizionale

In risposta, molte organizzazioni stanno optando per le SD-WAN sulla base del fatto che offrono migliori prestazioni di rete. Esistono tuttavia sul mercato varie soluzioni SD-WAN con diverse funzionalità e può risultare difficile stabilire quale di esse soddisfi effettivamente i requisiti del core business. Prima che un responsabile della gestione tecnica e operativa della rete proceda con la valutazione delle opzioni disponibili, è opportuno che analizzi le motivazioni che inducono a tale scelta e i differenti vantaggi e svantaggi delle varie SD-WAN.

Sicurezza inadeguata: mancanza di una protezione completa dalle minacce

Sebbene il throughput ne risenta quando una WAN instrada tutto il traffico attraverso il data center, le WAN basate su MPLS sono generalmente percepite come adeguatamente sicure. Al contrario, per molte soluzioni SD-WAN, la sicurezza avanzata non è integrata o, se inclusa, è insufficiente. In particolare, le funzionalità di sicurezza della maggior parte delle soluzioni SD-WAN non coprono la sicurezza avanzata nella sua interezza, dal livello 3 al livello 7, poiché mancano una tecnologia IPS (Intrusion Prevention System)

integrata, il web filtering, l'ispezione SSL (Secure Sockets Layer)/TLS (Transportation Layer Security) e altri tipi di protezione.

Per soddisfare tali requisiti di sicurezza nelle reti di filiali e uffici distaccati, i responsabili della gestione tecnica e operativa della rete devono abbinare alla SD-WAN appliance di sicurezza dedicate. Ciò comporta l'aggiunta almeno di un firewall in ogni punto, a volte più di uno (ad esempio, l'ispezione SSL/TLS non è disponibile in ogni firewall sul mercato). Questo crea però complessità, che aumenta il TCO, dalle spese in conto capitale (CapEx) per l'appliance aggiuntiva al tempo del personale (spese operative [OpEx]) impiegato per la gestione del firewall aggiuntivo e di altre appliance.

Anche tra le soluzioni SD-WAN che includono tecnologie più avanzate, esistono ancora lacune. Ad esempio, non tutte le soluzioni SD-WAN hanno opzioni di sicurezza che sono state accuratamente controllate da esperti terzi come NSS Labs. Questo confronto e questa analisi oggettivi delle soluzioni SD-WAN consentono ai responsabili della gestione tecnica e operativa della rete di determinare quali soluzioni SD-WAN soddisfano al meglio le esigenze di business reali.

Prestazioni: un compromesso con la sicurezza

La connettività diretta e il bilanciamento del carico delle soluzioni SD-WAN migliorano le prestazioni rispetto alla WAN tradizionale. Tuttavia, come nel caso della sicurezza, questo è un altro ambito in cui tutte le soluzioni SD-WAN non sono create allo stesso modo. In particolare, non tutte le soluzioni SD-WAN sono in grado di identificare e classificare il traffico delle applicazioni e attuare policy di routing a un livello molto capillare. Il risultato è che alcune applicazioni non possono essere rese prioritarie rispetto ad altre. Con questo unico modello di traffico per tutte le applicazioni, le applicazioni critiche, le chiamate VoIP e i video possono rallentare e ostacolare la produttività dell'utente finale.

Inoltre, nel sottoinsieme delle soluzioni SD-WAN con sicurezza integrata, alcune impostazioni di sicurezza possono degradare le prestazioni della rete. Ad esempio, l'attivazione di un'ispezione approfondita del traffico crittografato SSL/TLS può avere un impatto enorme sulle prestazioni di throughput. Tuttavia, per le organizzazioni che scelgono di lasciarla disattivata, il rischio aumenta: il 72% del traffico di rete è crittografato e il 60% degli attacchi utilizza la crittografia per nascondere il malware con crittografia SSL e TLS.[4]

Costi e risorse: il TCO rimane alto

L'incremento del volume e della velocità del traffico di rete proveniente da VoIP, video e applicazioni basate su SaaS è allarmante, e aumenta considerevolmente i costi della larghezza di banda della rete per molte organizzazioni. Considerando che i costi della connettività MPLS si stanno quadruplicando o quintuplicando, il risparmio in termini di costi di una SD-WAN che utilizza l'Internet pubblico è notevole.

Nondimeno, i responsabili della gestione tecnica e operativa della rete che distribuiscono soluzioni SD-WAN sono spesso sorpresi di scoprire un TCO molto più alto del previsto. In particolare, l'aggiunta di più appliance per funzionalità diverse aumenta le spese in conto capitale (CapEx) e il tempo necessario al personale per la loro gestione (OpEx). Il personale responsabile della rete deve monitorare e inserire manualmente le informazioni di registro per la gestione delle minacce, attività dispendiose in termini di tempo e molto inefficienti.

Inoltre, la necessità di distribuire più prodotti monofunzionali per ogni ufficio distaccato e filiale, dai router ai firewall passando per i gateway web di sicurezza e l'ottimizzazione della WAN, richiede molto tempo al personale per la gestione. Ogni prodotto ha

"Il 72% degli intervistati [sulla base di un'indagine di Gartner] ha confermato che la sicurezza era la sua principale preoccupazione parlando di WAN".[3]

Molte aziende che passano a una SD-WAN realizzano risparmi notevoli a livello di connettività a banda larga, più del 40% in alcuni casi.[5]

Il 72% del traffico di rete è crittografato, e oggi il 60% degli attacchi utilizza la crittografia.

Il costo totale di proprietà (TCO) delle soluzioni SD-WAN varia da $5 a $496 per megabit al secondo (Mbps). Le organizzazioni dovrebbero valutare attentamente il TCO a breve e lungo termine della soluzione SD-WAN che stanno prendendo in esame al fine di stabilire quale offre il maggior numero di funzionalità con il TCO più basso.[6]

protocolli e interfacce utente propri. Per ottenere visibilità e controllo centralizzato e dimostrare la conformità a vari regolamenti di settore, regolamenti di governo e standard di sicurezza, il personale responsabile della gestione tecnica e operativa della rete deve dedicare tempo manuale all'aggregazione e alla riconciliazione dei dati di ciascun ambito tecnologico specifico. A fronte di una carenza di competenze, questo dispendio di tempo può diventare alquanto costoso poiché i team responsabili della gestione tecnica e operativa della rete continuamente ricercano l'espansione per soddisfare questi requisiti.

Le inefficienze si accumulano nelle reti distribuite dove la gestione delle soluzioni di rete e sicurezza impone al personale di recarsi in loco. In particolare, quando le soluzioni SD-WAN non offrono né un'alternativa virtuale né funzionalità di distribuzione zero-touch, può accumularsi rapidamente un notevole dispendio di tempo per la distribuzione iniziale e la regolare manutenzione.

Conclusione: cosa cercare in una SD-WAN

Nel valutare le numerose soluzioni SD-WAN disponibili, i responsabili della gestione tecnica e operativa della rete devono porsi le seguenti domande su ogni soluzione individuata:

- Quali risultati reali sono stati documentati in test indipendenti di terzi come quelli condotti da NSS Labs?
- Come è stata valutata la soluzione nei rapporti di analisti terzi come i Magic Quadrants di Gartner?
- Supponendo che la soluzione integri la sicurezza, sono incluse funzionalità avanzate, ossia controlli di sicurezza dal livello 3 al livello 7: 1) IPS, 2) web filtering e 3) ispezione approfondita del traffico crittografato SSL/TLS?
- Supponendo che la soluzione abbia una funzionalità di ispezione SSL/TLS, quale impatto comporta sulle prestazioni se attivata?
- La soluzione riconosce le applicazioni e utilizza l'intelligence del percorso automatizzata e la prioritizzazione di applicazioni SaaS business-critical, chiamate VoIP e video? La soluzione si integra con elementi di sicurezza in tutta l'azienda e in diverse aree di sicurezza (ad esempio, posta, cloud, endpoint, ecc.) per una condivisione integrata e automatizzata della threat intelligence?

[1] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022", IDC, 7 agosto 2018.

[2] Ibid.

[3] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth", Gartner, 12 novembre 2018.

[4] John Maddison, "More Encrypted Traffic Than Ever", Fortinet Blog, 10 dicembre 2018; Omar Yaacoubi, "The hidden threat in GDPR's encryption push", PrivSec Report, 8 gennaio 2019.

[5] Paul Ruelas, "Catching the SD-WAN wave: the cost savings hype and MPLS misconceptions need more explanation", Network World, 18 aprile 2018.

[6] Thomas Skybakmoen, "SD-WAN Comparative Report", NSS Labs, 8 agosto 2018.

ottobre 24, 2019 4:08 p.

376872-0-1-IT

wp-understanding-the-obstacles-to-wan-transformation-A4