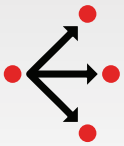
UN PUNTO DI VISTA DI FORTINET

È arrivato il momento di lasciare i router delle filiali alle spalle

4 grandi vantaggi di Secure SD-WAN.

Un numero sempre crescente di organizzazioni sta abbandonando i router delle filiali a favore di Secure SD-WAN per garantire la predisposizione al cloud e migliorare l'esperienza dell'utente. Le soluzioni Secure SD-WAN sono semplici da gestire; inoltre, semplificano le operazioni WAN complessive.

Le organizzazioni devono adottare soluzioni Secure SD-WAN per aiutare gli utenti delle filiali a sfruttare meglio le comunicazioni unificate e la collaborazione, utilizzare applicazioni SaaS critiche e accedere facilmente alle risorse archiviate nel cloud. Ecco i quattro principali vantaggi offerti da Secure SD-WAN rispetto alle architetture di routing delle filiali legacy:



Le soluzioni sicure SD-WAN sono facili da gestire e semplificano le operazioni WAN complessive.

1. Miglioramento dell'agilità delle applicazioni

I router operano in base a pacchetti. Di conseguenza, non sono in grado di fornire una visibilità approfondita delle applicazioni. Poiché la maggior parte delle organizzazioni ha investito in applicazioni e servizi cloud, non essendo in grado di identificare le applicazioni business-critical e di applicare protocolli per supportare le proprie esigenze di larghezza di banda e connettività, rischiano di peggiorare l'esperienza dell'utente.

Le soluzioni SD-WAN possono fare tutto quello che un router tradizionale può fare, ad esempio fornire routing avanzato e connettività WAN. Oltre alle funzioni di routing tradizionali, tuttavia, le soluzioni SD-WAN:

- Identificano e guidano le applicazioni utilizzando la selezione dinamica dei percorsi per una qualità dell'esperienza uniforme
- Possono identificare applicazioni e creare SLA per migliaia di applicazioni come O365, Salesforce.com e Unified Communications
- Sono in grado di aggiornare quotidianamente le applicazioni aziendali per garantire che vengano identificate con precisione e che seguano il percorso previsto

2. Scalabilità semplificata, con notevoli risparmi in termini di CAPEX e OPEX

Le velocità e i volumi delle connessioni MPLS sono predeterminati e costosi, il che significa che un improvviso aumento del traffico, come connessioni multiple di comunicazioni unificate ad alta velocità o la necessità di elaborare una grande quantità di dati, può influire su chiunque. Anche l'aggiunta di nuovi siti di router di filiali è un processo costoso e dispendioso in termini di tempo.

Le soluzioni SD-WAN, tuttavia, possono aiutare i clienti a migrare da MPLS a banda larga (DSL, 4G/5G, Ethernet) e realizzare un risparmio del 40% in termini di OPEX in molti casi. La SD-WAN consente alle organizzazioni di scalare in modo dinamico e sicuro fino a decine di migliaia di filiali, di interagire senza problemi con le infrastrutture fisiche e cloud esistenti e di fornire una risoluzione dei problemi remota per eliminare costosi interventi fisici da parte di tecnici specializzati. La Secure SD-WAN consolida inoltre tutta una gamma di prodotti specifici, compresi router, firewall e strumenti di ottimizzazione della WAN, in un unico prodotto, con un notevole risparmio in termini di CAPEX.

3. Gestione e orchestrazione semplificate

I router delle filiali sono spesso complessi da installare, aggiornare e gestire, anche quando si suppone che siano una soluzione "low-touch". La configurazione richiede competenza con l'interfaccia a riga di comando (CLI, Command Line Interface) di un router e, a causa della sua complessità, raramente può essere eseguita da chiunque si trovi sul posto in una filiale.

La gestione della Secure SD-WAN centralizzata garantisce che i nuovi servizi e le nuove policy siano focalizzati sull'applicazione e che le configurazioni di connettività e sicurezza e i cambiamenti delle policy possano essere propagati senza problemi in tutta la WAN estesa, eliminando la necessità di configurare o gestire ogni dispositivo o servizio singolarmente. La Secure SD-WAN centralizzata fornisce inoltre analisi approfondite che mostrano le prestazioni storiche e in tempo reale delle applicazioni, consentendo ai team di risolvere rapidamente i problemi e migliorare le principali metriche delle prestazioni, ad esempio il tempo di risposta medio.

4. Sicurezza e connettività di rete integrate

I router delle filiali non sono soluzioni di sicurezza e di rete completamente integrate con qualsiasi mezzo. Quando l'MPLS è integrato con lo split tunneling per consentire l'accesso diretto a Internet, i router delle filiali forniscono una gestione minima o nulla dei collegamenti o delle connessioni. Anche quando il traffico si interrompe o viene spostato in un percorso alternativo, non dispongono di un controllo proattivo eseguito nel giro di frazioni di secondo per evitare la caduta delle connessioni, e non hanno la capacità di attenuare i problemi di trasporto o di fornire funzionalità come il buffering dinamico delle instabilità. Non sono inoltre in grado di regolare attivamente il traffico prima che la congestione diventi un problema. Ancora peggio, poiché i router non sono dotati di una sicurezza efficace, queste connessioni non MPLS espongono l'organizzazione a ulteriori rischi.

Tuttavia, è importante notare che la maggior parte delle soluzioni SD-WAN non sono prive di problemi di sicurezza: uno dei requisiti critici per il successo della SD-WAN è la sicurezza completamente integrata. I Next-Generation Firewall (NGFW), i cui componenti chiave includono IPS, Web filtering, ispezione SSL e antimalware, sono un esempio di soluzione integrata. Senza una sicurezza completamente integrata, la SD-WAN diventa solo un altro canale con cui malware e criminali informatici possono per attaccare la rete.

Una vera piattaforma ha bisogno di strumenti appositamente progettati per interagire come un unico sistema, idealmente con ogni elemento eseguito nello stesso sistema operativo e gestito con una singola console di gestione. In questo modo, si garantisce che tutte le transazioni vengano visualizzate e ispezionate, e che le eventuali minacce o comportamenti anomali siano condivisi tra ogni soluzione per la massima protezione. Nell'ambito di un sistema integrato di questo tipo, le funzionalità di rete e di connettività di una SD-WAN non sono soltanto strettamente associate alle soluzioni di sicurezza installate sulla piattaforma. Sono la stessa cosa.

Considerazioni sui passaggi successivi

È essenziale non solo riconoscere la necessità di abbandonare la tradizionale strategia WAN basata su router, ma anche scegliere con attenzione una soluzione Secure SD-WAN progettata per fornire l'intero spettro di funzionalità e il più ampio numero possibile di casi d'uso. In questo modo, è possibile garantire che la distribuzione della nuova SD-WAN non solo soddisfi le esigenze dell'organizzazione di oggi, ma che possa anche adattarsi alle esigenze del futuro in rapida evoluzione.

FORTINET

www.fortinet.com

June 1, 2021 3:51 PM

Sheldon:Fortinet:2021-04-1006801-Updating-branding-SD-WAN-assets:pov-sdwan-branch-routers:Italian:pov-sdwan-branch-routers-IT

1006801-0-1-IT