

UN PUNTO DI VISTA DI FORTINET

La lista di controllo dei responsabili della SD-WAN

7 passaggi chiave per una distribuzione sicura e di successo di una SD-WAN



Anche se l'acronimo fa pensare a qualcosa di tecnico, i suoi effetti vanno ben oltre il Network Operations Center. Software-Defined Wide Area Network o SD-WAN è un acronimo che anche i top manager conoscono bene perché può aprire la strada per un'innovazione digitale di livello superiore. Purtroppo, offre anche ai criminali informatici nuove vie di accesso ai preziosi sistemi IT. Per evitare di trasformare un'idea promettente in una violazione dei dati, ecco 7 passaggi a cui la tua organizzazione deve attenersi.

1. Non agire completamente in autonomia

Due terzi dei progetti di trasformazione sono significativamente in ritardo o falliscono completamente a causa dei continui rifiuti da parte dei soggetti interessati interni, ha affermato McKinsey quasi un decennio fa¹. La tecnologia SD-WAN non fa eccezione, soprattutto perché sempre più persone accedono ad applicazioni SaaS come Office 365, Google Docs o Salesforce, per non parlare delle applicazioni di teleconferenza e delle piattaforme di trasferimento file come HighTail. Prima di interrompere un ecosistema di lavoro, assicurati di coinvolgere i giusti soggetti interessati e valuta periodicamente qualsiasi scelta di trasformazione alla luce di questi feedback.

2. Spiega chiaramente i motivi

L'innovazione digitale non è l'obiettivo finale, né lo è la SD-WAN. Entrambe sono strumenti a supporto della strategia aziendale, a sua volta supportata da obiettivi di business identificati. I progetti SD-WAN in cui vengono chiaramente comunicati fin da subito i motivi per cui deve essere distribuita hanno maggiori probabilità di successo. Spiega gli obiettivi strategici, come ad esempio definendo quale applicazione contribuisce maggiormente a favorire un determinato obiettivo di produttività oppure identificando i principali requisiti legali che possono essere interessati da una violazione dei dati. Questo approccio ha il pregio di mettere i piani aziendali al centro dell'implementazione della SD-WAN. I motivi garantiscono una visione in prospettiva e aumentano significativamente il livello di coinvolgimento.

Punti chiave

- La distribuzione di una SD-WAN deve essere stabilita dai responsabili dirigenziali. Anche se sembra un acronimo tecnico, il dominio richiede una certa attenzione da parte dei dirigenti, in quanto ha un impatto su domini chiave come l'assegnazione di priorità alle applicazioni e la strategia di sicurezza.
- Coinvolgi i soggetti interessati interni. Gran parte dei progetti di innovazione digitale falliscono, poiché vengono rifiutati dagli utenti interni che non sono stati considerati come figure di primo piano nel processo decisionale.
- Metti la sicurezza al centro di tutto. Nella fase di progettazione, ma anche nella fase di test, scegli una soluzione in cui lo stack di sicurezza e lo stack di rete interessano marginalmente le prestazioni complessive.
- Le fonti indipendenti sono sempre un punto di riferimento interessante. Documentati e approfitta di prospettive esterne e imparziali per scegliere una soluzione SD-WAN ampia, integrata e automatizzata.

3. Sfrutta tutti i vantaggi dell'automazione

Sebbene ogni soluzione SD-WAN supporti l'assegnazione di priorità alle applicazioni e le VPN, non tutte sono create allo stesso modo in termini di distribuzione zerotouch.

Nel momento in cui si inizia a propagare manualmente in catena o a modificare le regole durante la distribuzione della SD-WAN nelle sedi distaccate, si introducono inevitabilmente errori umani, ritardi e combinazioni imprevedibili di entrambi. Garantire che la tua soluzione SD-WAN consenta l'automazione della distribuzione ti consente di evitare ritardi e costi significativi.

4. Supervisiona le prestazioni con tutte le funzionalità di sicurezza attivate

Il test delle prestazioni è un'area in cui i dirigenti si affidano alle operazioni, che spesso delegano il compito a integratori o fornitori terzi. Non c'è nulla di sbagliato nel delegare ad altri, ad eccezione del fatto che le prestazioni possono variare enormemente una volta che le funzioni di sicurezza avanzate vengono attivate, un aspetto raramente notato nelle schede tecniche pubblicate. L'insistenza dei dirigenti sui test delle prestazioni, con particolare attenzione alle funzionalità di sicurezza, ha un forte impatto sul successo di qualsiasi progetto. Inoltre, motiva il team del progetto a integrare la sicurezza quando risponde alle esigenze specifiche di ogni sede dell'organizzazione.

5. Effettua test approfonditi prima di una distribuzione massiccia

Scegliere diverse sedi rappresentative e prendersi il tempo di eseguire un modello di verifica realistico sono in realtà due procedure che consentono di risparmiare tempo. Le SD-WAN sfruttano un'ampia gamma di opzioni di larghezza di banda (MPLS, dati mobili e accesso a Internet a banda larga) per soddisfare le esigenze di una vasta gamma di utenti che utilizzano una serie di applicazioni diverse. In questo contesto, è praticamente impossibile prevedere il comportamento di un ecosistema così complesso in un laboratorio. Un modello di verifica consente di valutare l'esperienza dell'utente finale dei diversi profili di utenti e di misurare le prestazioni tecniche e finanziarie in varie condizioni operative. Coinvolge anche i team locali, con un effetto positivo sull'accettazione complessiva del progetto SD-WAN.

1. Delivering large-scale IT projects on time, on budget, and on value, Mc Kinsey, ottobre 2012

FORTINET

www.fortinet.com

Copyright © 2021 Fortinet, Inc. Tutti i diritti riservati. Fortinet®, FortiGate®, FortiCare®, FortiGuard® e altri marchi sono marchi registrati di Fortinet, Inc. Anche altri nomi Fortinet qui citati possono essere marchi registrati e/o marchi di diritto comune di Fortinet. Tutti gli altri nomi di prodotti o società possono essere marchi registrati dei rispettivi proprietari. I dati riportati relativi a prestazioni e altre caratteristiche sono stati ottenuti con prove interne di laboratorio in condizioni ideali e, pertanto, le prestazioni effettive e altri risultati possono variare. Elementi variabili della rete, diversi ambienti di rete e altre condizioni possono influenzare i risultati delle prestazioni. Nulla di quanto qui contenuto rappresenta un impegno vincolante per Fortinet, e Fortinet esclude qualsiasi garanzia, esplicita o implicita, eccetto quelle previste da un contratto scritto, firmato da un rappresentante legale di Fortinet, che garantisce esplicitamente all'acquirente che le prestazioni del prodotto indicato saranno conformi a determinati dati esplicitamente indicati. In tal caso, solo gli specifici dati delle prestazioni esplicitamente identificati in tale contratto scritto saranno vincolanti per Fortinet. Per chiarezza, qualsiasi garanzia è limitata alle prestazioni ottenute nelle stesse condizioni ideali delle prove interne di laboratorio di Fortinet. Fortinet esclude in toto qualsiasi convenzione, rappresentanza e garanzia, esplicita o implicita, sulla base del presente documento. Fortinet si riserva il diritto di cambiare, modificare, trasferire o comunque revisionare questa pubblicazione senza alcun preavviso. La versione applicabile della presente pubblicazione è quella più recente.

6. Presta particolare attenzione alla visibilità

È impossibile controllare quello che non si riesce a vedere, e poiché le SD-WAN vengono utilizzate prevalentemente per migliorare la connettività delle sedi distaccate riducendo i costi, è importante adottare una soluzione SD-WAN che consenta di monitorare tali vantaggi. Anche se la tua soluzione prevede l'intervento di un MSSP (Managed Security Service Provider), chiedi di tenere d'occhio la rete tramite una dashboard di sola lettura. Tale visibilità ti consentirà di concentrarti su attività più strategiche, garantendo al contempo un monitoraggio continuo delle metriche che influiscono sulla produttività e sulla conformità giuridica.

7. Verifica le opinioni delle fonti neutrali

La combinazione delle funzioni di rete e di sicurezza in un'unica soluzione comporta l'integrazione di un numero molto elevato di tecnologie diverse. I fornitori sottolineeranno naturalmente le aree in cui sono più forti. Per ottenere una visione imparziale, è sempre importante fare riferimento a quello che gli utenti reali e le fonti indipendenti sperimentano quando si confrontano con la realtà di una distribuzione di SD-WAN. Fonti come NSS Labs, che conducono test approfonditi di terzi, sono sempre ricche di insegnamenti. In una categoria diversa, i Magic Quadrant di Gartner rappresentano da sempre una fonte interessante, da consultare prima di procedere con un investimento.

Conclusioni

Garantire una connettività onnipresente in presenza di sedi distaccate non è mai stato così importante. Le SD-WAN hanno già dimostrato di essere la tecnologia in grado di mantenere questa promessa, con risparmi sui costi e assegnazione di priorità alle applicazioni difficili da ignorare. Tuttavia, il lato della rete pura delle SD-WAN non è l'unico aspetto da considerare. Come in molte soluzioni con un intento trasformativo, rimandare la sicurezza a un secondo momento può comportare una grave esposizione ai rischi, l'insoddisfazione degli utenti e violazioni di dati. Prenditi il tempo necessario per riflettere su questi sette passaggi principali: in questo modo, eviterai tutti questi aspetti negativi, rafforzando anche il ruolo del CISO nel processo di innovazione digitale.