NOTA SINTETICA

Le vostre filiali sono vulnerabili ai ciberattacchi?

Perché l'aumentata esposizione, le risorse limitate e l'aumento dei costi rendono necessaria una soluzione sicura SD-Branch

Sommario

I metodi tradizionali di installazione e mantenimento dei sistemi di sicurezza presso le filiali sono divenuti inefficaci, troppo costosi e impossibili da gestire. Una soluzione SD-Branch può costituire l'asse portante della sicurezza illimitata negli ambienti aziendali distribuiti.

L'esplosione dei punti di esposizione

Nel 2019 i ricercatori delle minacce di SonicWall Capture Labs hanno registrato 9,9 miliardi di attacchi malware. Negli ultimi cinque anni i cibercriminali hanno puntato sulla quantità degli attacchi. L'obiettivo era semplice: lanciare una rete per poter catturare il maggior numero di prede. E di pari passo con l'evoluzione delle ciberdifese, gli attacchi sono diventati più mirati, con una percentuale maggiore di successi.

Inoltre, la situazione delle reti e della sicurezza sta conoscendo una trasformazione digitale, con la conseguente esplosione dei dispositivi mobili e dell'Internet delle cose. Per questo motivo le imprese tendono a basarsi su client mobili e sulla realizzazione di reti mobile-first. Un altro catalizzatore del cambiamento è costituito dal passaggio al cloud e dall'adozione di applicazioni per tale ambiente. Con applicazioni business-critical come MS Office che stanno passando al cloud e con le aziende che stanno utilizzando applicazioni cloud come Salesforce o Workday per le attività quotidiane, è diventato di fondamentale importanza garantirne la sicurezza. La trasformazione digitale traina la domanda di apparecchiature dalle prestazioni elevate in grado di tenere il passo dell'aumento della domanda di dati.

I costi in continua crescita della connettività

Per lo svolgimento delle attività quotidiane, gli uffici o le filiali mobile-first fanno ampiamente affidamento su applicazioni che richiedono molta ampiezza di banda. Può trattarsi di semplici funzioni come lo streaming di video o di altri contenuti, o di lavorare con Office 365. Di queste applicazioni che consumano molta ampiezza di banda, alcune possono essere business-critical, altre no. È essenziale segregare questo traffico in modo efficace, altrimenti i costi diventano proibitivi: s'immagini di dover effettuare il backhaul del traffico di tutte le filiali con costose connessioni MPLS alla sede centrale.

Per fortuna, i costi possono essere ridotti utilizzando accessi Internet economici per il traffico dei dati non critici, mentre quello dei dati critici può essere prioritizzato mediante meccanismi di selezione dinamica dei percorsi. Tuttavia, alcune di queste applicazioni, fondamentali per la gestione delle imprese distribuite e delle filiali, avrebbero bisogno di una connettività ridondante per garantire il funzionamento ininterrotto.

Un metodo per garantire la connettività ridondante per le filiali consiste nel disporre di una soluzione che consenta di utilizzare WAN ad elevata disponibilità e dalle prestazioni elevate con funzioni di bilanciamento del carico di rete. Ciò può essere ottenuto grazie alla tecnologia SD-WAN.

Utilizzando accessi a Internet a basso costo (banda larga, 3G/4G/LTE, fibra), le organizzazioni possono sostituire le costose tecnologie di connessione WAN come MPLS con SD-WAN con un valido rapporto costi-benefici. Tuttavia, poter disporre di tutto questo gestendo nel contempo le soluzioni di sicurezza dell'intera rete da un unico pannello di controllo spesso non risulta fattibile.

Alle prese con risorse sempre più limitate

Il costo della sicurezza convenzionale sta diventando sempre più proibitivo e la mancanza di personale qualificato sempre più grave. A causa delle limitazioni di bilancio e della scarsezza di personale non è semplicemente possibile mantenere il passo, il che ha provocato un vuoto a livello di cibersicurezza aziendale.

I prodotti multi-point rendono difficile per le filiali installare, configurare, gestire e risolvere le anomalie della soluzione. Disponendo di uno stack di sicurezza end-to-end è possibile unificare firewall, switch, access point, sicurezza cloud e client end-point per poter utilizzare una gestione a singolo pannello di controllo che amplifichi la visibilità e il controllo per i diversi prodotti. Questo stack di sicurezza end-to-end garantisce condizioni di sicurezza potenti ed unificate.

Cambiare il modo di mantenere le reti è fondamentale. È possibile restare al passo con la trasformazione digitale garantendo condizioni di sicurezza potenti, altrimenti le organizzazioni avranno difficoltà a gestire e a controllare il crescente numero di dispositivi in rete. Vi sarebbero minacce che non verrebbero identificate e le aziende sarebbero costrette ad adottare un approccio reattivo anziché proattivo.

Inoltre, l'installazione modulare potrebbe essere difficile senza tecnologie come l'installazione Zero-Touch. I tecnici dovrebbero recarsi presso le filiali per configurare manualmente i singoli dispositivi, il che contribuirebbe ad aumentare i costi generali e comporterebbe un maggiore dispendio di tempo per mettere in funzione le soluzioni presso le filiali, che in alcuni casi sono diffuse a livello globale.

Per finire, le filiali come le sedi centrali devono consentire un accesso wireless sicuro, che garantisca agli utenti un'esperienza superiore e di prestazioni elevate. Dal momento che le reti Wi-Fi sono dappertutto, i dipendenti e gli ospiti si aspettano prestazioni Wi-Fi affidabili e veloci.

Perché è necessaria una soluzione SD-Branch

Oggi, l'evoluzione della tecnologia presso le filiali è essenziale. Le filiali tradizionali non possono restare al passo con la crescente domanda proveniente dalla moltiplicazione dei dispositivi mobili e dell'Internet delle cose. Con la proliferazione dei dispositivi, la gestione e la sicurezza diventano problematiche, perché possono richiedere politiche diverse. Per questo diventa fondamentale poter disporre di una politica unificata per LAN e WAN da un unico pannello di controllo (SPOG).

Inoltre, la gestione SPOG può mettere a disposizione una notevole mole di dati analitici relativi all'intero ecosistema di sicurezza. Man mano che le imprese passano al cloud, la connettività WAN tra le filiali dev'essere concepita in modo intelligente per poter sfruttare i collegamenti Internet più convenienti rispetto alle costose connessioni MPLS, e per poter utilizzare l'installazione Zero-Touch.

Tutto ciò garantisce la flessibilità operativa, per cui le organizzazioni possono installare e mettere rapidamente in funzione dispositivi in modalità Zero-Touch, eliminando – o riducendo – il fabbisogno di personale informatico qualificato che si rechi presso le filiali per configurare e installare le soluzioni. Per garantire continuità, integrazione e modularità, le organizzazioni dovrebbero optare per una gestione SPOG razionale con i servizi di un unico fornitore.

Le soluzioni SD-Branch ampliano le SD-WAN per poter disporre del successivo livello di connettività e flessibilità. Le soluzioni SD-Branch trasformano la tecnologia SD-WAN in una soluzione su misura per l'installazione presso le filiali, dispongono di un maggior numero di funzioni e vanno oltre la gestione mediante connettività tra le sedi delle filiali. Le soluzioni SD-Branch comprendono SD-WAN, connettività di rete locale e sicurezza. Inoltre, l'installazione Zero-Touch e la gestione SPOG riducono il fabbisogno di personale informatico, il che abbatte ulteriormente i costi operativi.

Conclusioni

Le imprese distribuite sono alle prese con i problemi di sicurezza delle filiali dovuti all'incremento dei punti di esposizione, alle risorse limitate e all'aumento dei costi. Tutto ciò contribuisce ad aggravare le lacune della cibersicurezza aziendale.

Una soluzione efficace riunisce in sé la flessibilità di SD-Branch, la sicurezza end-to-end, la segmentazione di rete e la conformità. Ciò consente di adottare politiche unificate per l'intero ecosistema di rete, rendendo possibili controlli di sicurezza granulari per individuare gli odierni attacchi più nascosti e mai visti prima e impedire che gli stessi compromettano le reti.

SonicWall considera la tecnologia SD-Branch un asse portante della sicurezza illimitata per l'era iper-distribuita. La soluzione SD-Branch di SonicWall rende sicura la connettività e trasforma l'esperienza degli utenti delle filiali mettendo a loro disposizione una piattaforma integrata che consente di beneficiare della connettività più conveniente (SD-WAN), abilitare il BYOD, adottare applicazioni SaaS e collegarsi alla sede centrale e ad altre filiali. La soluzione integra SD-WAN, installazione Zero-Touch, gestione da un unico pannello di controllo, visibilità unificata e rilevamento delle minacce, firewall di prossima generazione, switch sicuri, access point wireless, sicurezza degli endpoint e sicurezza delle applicazioni cloud.

Ulteriori informazioni: leggere la nostra SonicWall SD-Branch Solution Brief.

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare il sito www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per ulteriori informazioni consultare il nostro sito web.
www.sonicwall.com

ExecutiveBrief-AreYourBranchSites-US-VG-1980