FORTINET

WHITE PAPER

Come realizzare reti cablate e wireless sicure

Le sfide più importanti e come risolverle

Sintesi preliminare

Il livello di accesso rappresenta la superficie di attacco più ampia della rete di un'impresa. Supporta infatti tutta la connettività di rete (sia tramite switch Ethernet cablati che tramite punti di accesso wireless) per il personale interno ed esterno e gli ospiti, oltre che i dispositivi Internet-of-Things (IoT). Visto il numero sempre crescente di dispositivi che si collegano alle reti ogni giorno, garantire la sicurezza di tale livello diventa un'esigenza critica. Considerato poi che il telelavoro è diventato il nuovo standard durante la pandemia da COVID-19 (e tale tendenza potrebbe confermarsi anche in futuro), una sicurezza adeguata per attenuare gli attacchi al livello di accesso non è mai stata così importante.[1]

L'upgrade della LAN di un campus non solo aggiorna un elemento trascurato della rete, ma può anche porre le basi per una gestione e una visibilità complete end-to-end.[3]

Problemi con l'infrastruttura di accesso esistente

Il perimetro della LAN rappresenta un obiettivo ampio e potenzialmente vulnerabile per i cybercriminali, soprattutto in un momento in cui le aziende di ogni settore dipendono dalla connettività di rete per sopravvivere. E gli attacchi sono in aumento. Ad esempio, nel primo trimestre del 2020 gli attacchi DDoS (Distributed Denial-of-Service) intesi a travolgere le connessioni di rete sono stati superiori del 542% rispetto al trimestre precedente (4° trimestre 2019).[2]

Alcune sfide specifiche che le organizzazioni IT devono affrontare nella gestione dei livelli di accesso includono:

- Mantenere sincronizzate diverse configurazioni
- Ottenere la visibilità di tutta la rete
- Gestire diversi livelli di accesso
- TCO (costo totale di proprietà) elevato

Per gestire meglio una rete sicura, le aziende cercano approcci integrati basati su piattaforme. Una soluzione in grado di combinare la gestione delle funzioni cablate, wireless e di sicurezza sta diventando sempre più comune poiché l'obiettivo dei gruppi IT è quello di ridurre i costi di esercizio. Ma non tutte le soluzioni di rete offrono la semplicità, le caratteristiche e le prestazioni necessarie.

La complessità crea sfide per le LAN

Man mano che le reti LAN tradizionali si espandono fisicamente per la crescita del business e l'aggiunta di utenti e dispositivi, la loro complessità aumenta. Di conseguenza, gli amministratori IT devono dedicare più tempo a tenere traccia di tutti i diversi movimenti. Con la distribuzione di filiali o succursali e l'aumento del numero di dipendenti che telelavorano, la situazione delle LAN sta diventando sempre più complicata e costosa a livello operativo.

Gestire la configurazione

- Nel caso di un grande campus, un minimo cambiamento può interferire con parti importanti della rete. Le organizzazioni devono garantire che ogni aggiunta, modifica e aggiornamento sia monitorabile e gestibile in modo che tutte le parti della rete rimangano sincronizzate e operative.
- Anche la distribuzione della rete in siti remoti presenta potenziali problemi di configurazione. L'installazione e la supervisione di uno standard comune in molte sedi remote e topologie di filiali diverse possono esaurire rapidamente le risorse IT.

Visibilità della rete

- Le reti dei campus cambiano costantemente per il continuo andirivieni dei dispositivi del personale interno ed esterno e degli ospiti. La tipica visibilità del perimetro della LAN può fornire dettagli sulla connessione del dispositivo, ma può sfuggire il contesto di livello superiore come, ad esempio, il livello di autenticazione dell'utente ed eventuali limiti di accesso alle risorse associati.

- I dispositivi IoT pongono una sfida particolare in termini di visibilità. Quando questi dispositivi compaiono in rete, l'IT è sotto pressione per autorizzare le applicazioni che rappresentano senza mettere a repentaglio la sicurezza generale della rete. In luoghi senza personale IT in loco, questo compito può essere ancora più difficile perché le uniche informazioni su un determinato dispositivo sono quelle fornite nell'interfaccia del livello di accesso.

TCO (costo totale di proprietà) elevato

- Le moderne reti LAN hanno cercato di risolvere i problemi di complessità aggiungendo licenze e/o abbonamenti aggiuntivi per rispondere alle varie esigenze del gruppo IT. Aggiungendo tutte queste caratteristiche, il costo complessivo della soluzione diventa doppio o addirittura triplo rispetto al costo delle sole apparecchiature di rete.
- Inoltre, più aumentano i sistemi e gli strumenti di overlay online per gestire e proteggere il perimetro della LAN, più i gruppi IT diventano oberati nel tentativo di capire e gestire tutte queste diverse interfacce di soluzioni scollegate.

Le LAN sono state trascurate dal punto di vista della sicurezza, per cui non hanno caratteristiche chiave come la crittografia, il controllo degli accessi e la visibilità capillare. I malintenzionati stanno scoprendo rapidamente che ora il punto debole è la LAN.[4]

Sicurezza

- Le reti LAN diventano sempre più complesse, e anche la sicurezza in tutti i punti di ingresso della rete per ogni tipo di utente autorizzato può diventare eccessivamente complicata. Molte organizzazioni aggiungono singoli prodotti di sicurezza puntuali per colmare le lacune una alla volta. Questo approccio complesso e disaggregato alla sicurezza può mettere a repentaglio l'intera organizzazione. Un solo errore di configurazione di una soluzione di sicurezza per la LAN può portare alla violazione di altre parti della rete.

Elementi da considerare nella valutazione di una soluzione

Nell'aggiornare una rete LAN cablata e wireless, sono varie le considerazioni che dovrebbero rientrare nel processo decisionale di un'organizzazione:

- ✓ **Struttura della topologia.** Quando si analizza come distribuire una LAN sicura, un aspetto fondamentale è la natura dei siti in cui la rete sarà distribuita. Si tratta di una serie di grandi campus o diverse piccole filiali? Sono previste formule di telelavoro per cui i dipendenti avranno bisogno della connettività? Molto spesso la soluzione è un ibrido di due o più requisiti operativi. Poiché ogni topologia ha le sue sfide e i suoi limiti, la soluzione scelta dovrà essere estensibile e scalabile in modo da poter aggiungere valore e offrire funzionalità appropriate a ogni scenario.
- ✓ **Dispositivi connessi.** Quali tipi di dispositivi si connetteranno alla rete? E chi sono i diversi utenti? Se anche ospiti e personale esterno avranno bisogno di accedere con propri dispositivi, occorrerà provvedere al mantenimento della sicurezza della LAN. Una buona soluzione per il perimetro della LAN dovrà offrire la possibilità di gestire tutti i tipi di dispositivi e utenti connessi, senza coinvolgere costantemente il personale IT. Le tecnologie di link aggregation rendono relativamente facile per gli architetti di rete stare al passo con la domanda crescente di larghezza di banda dei dispositivi finali.[6]
- ✓ **TCO basso.** Esistono soluzioni in grado di offrire tutte le caratteristiche appena descritte, ma i costi complessivi per la concessione di licenze, l'abilitazione e l'abbonamento a capacità à la carte possono aumentare. I decisori responsabili della rete devono tenere accuratamente traccia del numero di sistemi e soluzioni da acquistare per far sì che le funzionalità desiderate siano a disposizione dell'intera l'organizzazione, del numero di licenze eventualmente necessario e della necessità di abbonamenti ricorrenti per alcune caratteristiche fondamentali.

  Inoltre, il costo di proprietà va oltre l'investimento di capitale e gli abbonamenti. Anche il tempo dedicato dal personale alla distribuzione e alla manutenzione di una determinata soluzione può variare notevolmente. I decisori devono essere pronti a chiedersi quanto è complicata la soluzione da gestire? Funziona in modo semplice perché perfettamente integrata o richiede più prodotti che facciano da "collante" per il suo corretto funzionamento?
- ✓ **Sicurezza integrata.** Molte soluzioni LAN non integrano la sicurezza, per cui occorre adottare un approccio "bolt-on" alla sicurezza della rete a posteriori, che aggiunge sia costi che complessità. A volte accade invece che siano disponibili opzioni di sicurezza, ma non sono integrate con il perimetro della LAN, il che può creare "cuciture" nella rete in cui le configurazioni possono "sfilacciarsi" consentendo ai malintenzionati di insinuarsi. Le reti devono essere costruite e mantenute in un contesto di sicurezza per garantire la migliore protezione possibile, nonché un impatto minimo sulla gestione dell'infrastruttura LAN nel suo complesso.

L’accesso sicuro richiede una soluzione senza soluzione di continuità

Le reti LAN cablate e wireless possono costituire la spina dorsale di ogni azienda, ma rappresentano anche un notevole investimento di denaro e tempo per qualsiasi gruppo IT. Scegliere la soluzione giusta aiuta i team responsabili della sicurezza e dell’infrastruttura informatica a consentire l’attuazione delle iniziative aziendali e accompagnarle perfettamente.

Sono molti i fornitori di apparecchiature di rete oggi presenti sul mercato, e i VP dell’IT devono analizzare attentamente tutte le opzioni disponibili per trovare una soluzione che offra flessibilità di distribuzione a livello di accesso con sicurezza integrata per garantire la continuità delle operazioni.

[1] “In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns,” Help Net Security, 21 luglio 2020.

[2] Ibid.

[3] Andrew Froehlich, “A Network’s Weakest Link May be Different Than you Think,” Network Computing, 26 novembre 2019.

[4] Ibid.

[5] Ibid.

Copyright © 2020 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 garantisca 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.

febbraio 16, 2021 12:28 PM

762006-0-1-IT