Estendere la SD-WAN agli ambienti OT

Sfide e soluzioni

Sommario

Panoramica preliminare

La convergenza degli ambienti di tecnologia operativa (OT) con le soluzioni di tecnologia dell'informazione (IT) di livello enterprise sta creando molte capacità rivoluzionarie a livello di industria, produzione e infrastrutture critiche. La SD-WAN (Software-Defined Wide-Area Network) è una di queste. La SD-WAN può sostituire la WAN tradizionale in infrastrutture distribuite e remote con connessioni Internet più performanti e convenienti. Ma questo risparmio di prestazioni e costi comporta la perdita della sicurezza centralizzata della WAN tradizionale.

Affinché le organizzazioni basate su OT vulnerabili (e sempre più bersagliate) ottengano i vantaggi di una SD-WAN, una soluzione adottata deve prevedere una sicurezza robusta e integrata, progettata per le esigenze particolari di questi ambienti sensibili. Una soluzione firewall di nuova generazione (NGFW) che abbini il networking alla protezione OT-native rappresenta uno strumento ideale per questo tipo di distribuzioni.

Ricollegare le sedi remote

La WAN tradizionale si basa principalmente sulla costosa tecnologia MPLS (Multiprotocol Label Switching) o su collegamenti satellitari. Per mantenere il controllo e la visibilità centralizzati, il traffico viene reindirizzato verso un data center on-premises, il che può avere un impatto sulle prestazioni a causa di colli di bottiglia a livello di sicurezza.

La SD-WAN è diventata un modo diffuso per collegare le sedi remote delle aziende. La SD-WAN utilizza una serie di connessioni Internet come Long-Term Evolution (LTE), Digital Subscriber Line (DSL) o via cavo al posto della tecnologia MPLS/delle connessioni satellitari con notevole risparmio di costi. Per garantire le prestazioni dell'applicazione e l'esperienza dell'utente, la SD-WAN gestisce l'instradamento del traffico in base alle prestazioni (ad esempio, latenza, jitter) e ai costi di connettività per fornire una connessione affidabile e di alta qualità.

La diffusa adozione della SD-WAN nelle organizzazioni aziendali lascia intendere che gli ambienti OT saranno i prossimi, una volta individuate apparecchiature che soddisfino le esigenze degli ambienti OT, a iniziare da una SD-WAN robusta progettata per situazioni e ambienti industriali, produttivi e con infrastrutture critiche con condizioni ambientali difficili (ad esempio, piattaforme petrolifere, sottostazioni elettriche, linee di assemblaggio, trasporti marittimi).

Si prevede che il mercato mondiale delle SD-WAN crescerà del 168% di qui al 2024 superando i 3,2 miliardi di dollari.[1]

La SD-WAN per l'OT ha alcune esigenze particolari

La SD-WAN offre alle organizzazioni basate su OT gli stessi risparmi sui costi di connettività che offre alle aziende e può anche contribuire ad aumentare la produttività. L'accelerazione dei flussi di traffico e delle comunicazioni assicura che la produzione si svolga a un ritmo ottimale. La SD-WAN può inoltre ridurre la latenza rispetto alla connessione tramite firewall centrale del data center.[2]

La natura unica degli ambienti OT presenta tuttavia alcune esigenze particolari che non si possono ignorare nella scelta di una soluzione per questo tipo di infrastruttura. L'interruzione di un sistema OT può avere enormi ripercussioni sulla produttività, l'efficienza e persino sulla sicurezza. All'interno di un'infrastruttura critica (ad esempio, dighe idroelettriche, centrali nucleari, oleodotti e gasdotti), l'interruzione dei sistemi di controllo possono persino avere gravi conseguenze sulla vita umana e l'ambiente.

La SD-WAN risolve allo stesso tempo diverse sfide OT, tra cui rapida distribuzione, connettività veloce e gestione unificata per ridurre i costi di gestione dell'IT.[3]

Chi gestisce le operazioni OT si trova bloccato in una situazione di reattività nel tentativo di proteggere ambienti particolarmente sensibili.[4]

Una soluzione fisicamente robusta

Alcuni ambienti OT possono essere proibitivi per le normale apparecchiature IT a causa delle condizioni fisiche estreme (temperatura, umidità, vibrazioni, interferenze elettromagnetiche, spazi ristretti o fonti di alimentazione). Pertanto, le organizzazioni hanno bisogno di una soluzione SD-WAN che sia fisicamente robusta e progettata per funzionare in modo affidabile in qualsiasi condizione ambientale difficile.

Una soluzione capace

Una soluzione SD-WAN con capacità OT deve anche supportare l'installazione a lungo termine in luoghi remoti dove può non esserci personale IT a disposizione, come sottostazioni elettriche, navi o piattaforme petrolifere. La soluzione deve dunque offrire capacità di distribuzione zero-touch, nonché di monitoraggio e gestione a distanza. Un'altra capacità critica di da ricercare a livello di connettività è un modem LTE integrato per luoghi con copertura cellulare. Infine, le soluzioni devono anche soddisfare i requisiti di certificazione di specifici standard o regolamentazioni industriali.

Una soluzione sicura

Con la digitalizzazione, gli air gap che prima proteggevano gli ambienti OT stanno scomparendo e i sistemi OT sono sempre più spesso il bersaglio sia di attacchi rivolti a infrastrutture IT e poi riciclati che di exploit concepiti appositamente per gli ambienti OT.[5]

Le implicazioni a livello di sicurezza dell'accesso diretto alle risorse cloud e Internet possono potenzialmente avere un impatto ancora maggiore in un ambiente OT rispetto a quanto accade in una tipica distribuzione SD-WAN.[6]

Poiché la SD-WAN utilizza connessioni Internet dirette senza backhauling del traffico verso un data center per controlli di sicurezza centralizzati, queste connessioni devono essere protette da una marea crescente di attacchi opportunistici. E ciò richiede una sicurezza OT-native che non interrompa i sistemi di controllo sensibili, non riduca le prestazioni creando colli di bottiglia e non degradi la produttività degli utenti.

Sfortunatamente, la maggior parte delle soluzioni oggi sul mercato non offre alcuna protezione robusta integrata, per non parlare della sicurezza OT-native. La maggior parte dei prodotti tradizionali SD-WAN fornisce solo meccanismi per la determinazione dei percorsi di traffico. La sicurezza diventa un costosa riflessione successiva, un onere in termini di complessità e investimenti aggiuntivi di cui deve poi farsi carico l'organizzazione.

Un sondaggio del 2020 ha rivelato che il 90% delle organizzazioni ha subito almeno un'intrusione nel sistema OT nell'ultimo anno, e il 65% ne ha subite tre o più.[7]

Una soluzione combinata per la sicurezza e il networking

Per far fronte a tutte queste criticità, le organizzazioni hanno bisogno di una soluzione che abbini capacità di rete SD-WAN avanzate e sicurezza OT-native. Un NGFW con controllo del traffico SD-WAN avanzato e funzioni di sicurezza adeguate all'ambiente OT (ad esempio, protezione avanzata dalle minacce, ispezione delle applicazioni, prevenzione delle intrusioni [IPS], URL filtering, protezione botnet) è una soluzione ideale. Le organizzazioni basate su OT hanno bisogno di una sicurezza costruita ad hoc che risponda a tre requisiti essenziali:

- **Visibilità.** Le organizzazioni non possono proteggere parti della loro infrastruttura che non possono vedere. E la maggior parte (78%) delle organizzazioni ha una visibilità centralizzata dell'ambiente OT solo parziale.[8]
- **Controllo.** È necessario poter disporre della capacità di far rispettare le policy e adottare le azioni appropriate in base alle necessità, senza interrompere o spegnere i sistemi critici.
- **Consapevolezza.** Occorre monitorare costantemente la sicurezza per rilevare le anomalie. Tale attività comprende l'analisi continua dei comportamenti degli utenti e dei dispositivi (sapere cosa, dove, quando, chi e come) per fornire informazioni utili a intraprendere azioni a fronte di qualsiasi potenziale minaccia nota o ignota.

Un approccio basato su NGFW supporta la gestione centralizzata delle policy e dei controlli SD-WAN da un SOC (Security Operations Center). Le organizzazioni OT con distribuzioni remote e personale limitato possono operare in modo continuo sin dal momento della distribuzione. Il SOC può mantenere la visibilità di ogni singolo sito per monitorare i livelli di minaccia, segmentare le reti mantenendo separati gli ambienti OT e IT e mettere in quarantena i sistemi che risultano infetti al fine di limitare la propagazione del malware.

Ridurre costi e rischi

Per i settori che dipendono da sistemi di controllo OT, una soluzione SD-WAN sicura può fornire un ulteriore livello di protezione oltre a quello già eventualmente garantito da un gateway IT/OT. Una soluzione realmente integrata può non solo consentire di usufruire del risparmio di una WAN, ma anche offrire un unico approccio alla sicurezza informatica che riduce la complessità, estende la visibilità necessaria e il controllo in profondità della rete OT e impedisce di sfruttare le vulnerabilità dell'ambiente OT evitando costosi tempi di inattività produttiva.

La convergenza IT/OT può essere alla base delle sfide odierne in materia di sicurezza, ma è anche la chiave per una soluzione duratura che consenta di ottenere informazioni accurate e utilizzabili per agire. [9]

[1] "SD-WAN Market Expected to Increase 168 Percent by 2024," BBC Magazine, 8 luglio 2020.

[2] Joe Robertson, "What Manufacturing CISOs Need to Know About SD-WAN," LinkedIn, 20 dicembre 2019.

[3] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, 15 luglio 2020.

[4] "Independent Study Finds That Security Risks Are Slowing IT-OT Convergence," Fortinet/Forrester Consulting, 6 maggio 2020.

[5] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

[6] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, 15 luglio 2020.

[7] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[8] Ibid.

[9] "Securing Critical Operational Technology in Manufacturing," MAPI, 26 marzo 2020.

www.fortinet.com

829648-0-0-IT

febbraio 16, 2021 11:39 AM

eb-sdwan-ot-environments_IT