FORTINET

LIVRE BLANC

Concrétiser les promesses du SD-WAN pour les environnements OT

Synthèse

L'innovation digitale des technologies industrielles (ou OT pour operational technology) exige des connexions solides vers Internet et le cloud. Le SD-WAN (Software-defined wide-area networking) émerge en tant que solution potentielle pour remplacer les infrastructures WAN traditionnelles, peu performantes et coûteuses. Mais à l'heure d'une convergence entre IT et OT, les entreprises doivent pouvoir étendre leur visibilité sur l'ensemble de leur périmètre d'exploitation, environnements distants inclus. Et bien sûr, les fonctions de sécurité sophistiquées s'imposent pour se protéger de la vague d'attaques OT.

La convergence IT/OT fait émerger de nouvelles fonctionnalités et risques

Dans les secteurs industriels (production manufacturière, activités critiques, etc.), les systèmes OT opèrent leur convergence avec les technologies IT pour faire émerger de nouvelles fonctionnalités et concrétiser des gains de productivité. Mais cette convergence crée un besoin pour de nouveaux outils et solutions adaptés aux spécificités de l'OT.

La transformation digitale est un vecteur de complexité et d'exposition au risque pour les industriels. Les managers OT doivent bénéficier d'une vue holistique sur l'infrastructure réseau de leur entreprise. Une majorité (78%) des entreprises ne dispose aujourd'hui que d'une visibilité parcellaire sur leurs environnements OT.[1] Sans perspectives plus larges, toute partie invisible de l'infrastructure ne peut tout simplement pas être protégée.

En tant que résultat d'une convergence IT/OT généralisée, les systèmes OT ne sont plus cloisonnés, et donc plus sécurisés. Avec ces systèmes, toute menace dispose d'une passerelle pour accéder à des cibles OT de valeur et vulnérables. Les cybercriminels peuvent ainsi s'immiscer au sein d'environnements OT, pour ensuite se propager en interne. L'absence d'outils permettant d'identifier immédiatement les intrus contribue à alourdir les dommages potentiels. Pour un assaillant, il suffit souvent de quelques minutes pour compromettre un réseau OT. Pour autant, sur le terrain, l'identification d'un tel incident peut prendre jusqu'à plusieurs mois.[2]

Les entreprises exigent également de nouvelles infrastructures adaptées tant aux environnements IT que OT, dans l'optique de simplifier les opérations, la formation, le reporting, tout en assurant la maîtrise des coûts. L'utilisation d'outils distincts provenant d'éditeurs multiples favorise la complexité au sein de l'infrastructure, induit des investissements plus importants et rajoute de nouvelles tâches de déploiement, de gestion et de monitoring qui pèsent sur des équipes aux ressources limitées. Il en résulte des coûts d'exploitation plus importants.

Les connexions WAN traditionnelles induisent de nouveaux coûts

Les coûts sont une problématique récurrente pour de nombreuses entreprises industrielles, mais l'infrastructure WAN offre une opportunité d'économies. Le WAN traditionnel dépend essentiellement de liens coûteux MPLS ou par satellite. Pour des raisons de contrôle et de visibilité centralisée, le trafic est routé vers le data center sur site à des fins d'analyse de sécurité, ce qui peut peser sur les performances.

Le SD-WAN est devenu un moyen populaire interconnecter les sites distants d'entreprise. Le SD-WAN utilise des liens Internet publics (4G, ADSL, fibre, câble, etc.) pour remplacer les liens satellite/MPLS à un coût bien moindre. Pour assurer les performances applicatives et optimiser l'expérience utilisateur, le SD-WAN gère le routage du trafic sur la base des performances (latence, gigue) et des coûts de connectivité, contribuant ainsi à une connexion fiable et de qualité.

Nombre d'experts tablent sur une recrudescence des attaques sur les infrastructures critiques : des botnets qui conçoivent des attaques par DDoS sur les réseaux OT, des attaques sur des systèmes de production industrielle utilisant des services cloud, ainsi que des attaques sur la supply chain qui compromettent des éditeurs tiers en tant que tremplin pour accéder à des secteurs critiques cibles.[3]

Les besoins physiques spécifiques à l'OT

Les acteurs de l'OT opèrent dans différents environnements, et sur des sites de toutes tailles, de campus corporate étendus et tout confort à de petites installations opérationnelles sur des sites éloignés. Ces derniers peuvent parfois être plutôt hostiles pour des équipements IT classiques, compte tenu de conditions physiques extrêmes. Parmi ces sites :

- Postes électriques
- Plateforme de forage pétrolier
- Usines
- Installations hydroélectriques
- Entrepôts/centres de distribution
- Aéroports
- Ports

L'adoption généralisée du SD-WAN par les acteurs de l'OT implique de déployer un équipement SD-WAN conçu pour les infrastructures industrielles, de production ou critiques dont les conditions environnementales sont complexes, voire hostiles (forages pétroliers, stations électriques, lignes d'assemblage, fret maritime...).

Le SD-WAN répond à de nombreux défis OT, parmi lesquels un déploiement rapide, une connectivité accélérée vers les applications cloud et une gestion unifiée qui allège les charges de travail IT.[4] Le SD-WAN est donc un levier de productivité. Les utilisateurs sur site qui se connectent à un service cloud (Microsoft 365, Orcle Cloud ou AWS) au sein d'une architecture multi-cloud peuvent y accéder à partir de tout lieu. Ceci assure une latence plus faible et une meilleure expérience utilisateur par rapport à une connexion vers Internet via un pare-feu déployé au sein d'un data center centralisé.[5]

La question du SD-WAN et de la sécurité

Les impacts en matière de sécurité d'un accès direct aux ressources Cloud et Internet peuvent être plus lourds en milieu OT par rapport à un environnement SD-WAN plus classique.[6] Migrer d'un WAN traditionnel vers un SD-WAN est source de risque supplémentaire, puisque le trafic connecté à Internet n'est pas réacheminé vers un data center pour y appliquer des fonctions de sécurité centralisées. Cependant, la majorité des produits SD-WAN est basée sur des technologies de routage, conçues essentiellement pour identifier le meilleur chemin de connectivité pour le trafic. Et ces produits SD-WAN du marché n'offrent aucune sécurité intégrée.

Les vulnérabilités OT constituent une problématique majeure, compte tenu des multiples attaques qui ciblent ces environnements. La grande majorité (90%) des entreprises a subi au moins une intrusion sur leurs systèmes OT sur l'année écoulée. Et 65% d'entre elles en ont subi plus de trois.[7]

Les pannes ou disruptions OT résultant d'une attaque ont un impact majeur sur la productivité, l'efficacité et même la sécurité physique. Les attaques par malware sont désormais conçues pour cibler les vulnérabilités des systèmes de contrôle industriels, les systèmes SCADA et les systèmes de sécurité.[8] Les infrastructures critiques sont exposées au risque d'une attaque réussie qui pourrait impacter directement des vies humaines ou l'environnement.

Les réseaux industriels exigent une connectivité protégée et prioritisée pour contrôler les data centers et les applications Cloud. Les capteurs intelligents basés sur des protocoles de communication IIoT et IoT comme OPC UA (Open Platform Communications Unified Architecture), MQTT (Message Queuing Telemetry Transport) et HTTP doivent être sécurisés. L'acheminement via Internet d'indicateurs et d'informations de contrôle, du réseau de contrôle des processus vers le réseau IT corporate, est susceptible d'utiliser des protocoles vulnérables tels que Modbus, BACnet ou SafetyNET. Ces protocoles doivent être attribués à différents segments et inspectés, prioritisés et protégés. Un SD-WAN classique n'offre aucune de ces fonctions de sécurité.

Déploiement, management et monitoring à distance

Une autre problématique commune lorsqu'il s'agit d'adapter un SD-WAN à un environnement OT relève du besoin commun de déployer cette technologie sur des sites distants. Pas toujours simple lorsqu'on sait que ces sites ne disposent généralement d'équipe technique sur place.[9] Pour les sites distants, le SD-WAN doit bénéficier de règles de sécurité cohérentes qui protègent les systèmes sur site opérationnels.

De plus, le centre opérationnel de sécurité (SOC) d'une entreprise doit disposer d'une visibilité centralisée sur chaque site distant pour surveiller le niveau des menaces, gérer les passerelles entre les réseaux IT et OT et mettre en quarantaine les systèmes identifiés comme étant infectés, ceci afin de maîtriser toute propagation.

Les besoins physiques spécifiques à l'OT (suite)

De tels sites nécessitent des équipements IT et électroniques spécialisés, capables de fonctionner dans des conditions environnementales spécifiques à l'OT :

- Températures extrêmes
- Humidité
- Vibrations importantes et/ou constantes
- Interférences électromagnétiques
- Espaces réduits pour les équipements
- Différentes options en matière d'alimentation électrique (au-delà du 220V)
- Certifications réglementaires relatives à l'OT

Le marché mondial du SD devrait progresser de 168% jusqu'en 2024 et franchir la barre des $3,2 milliards.[10]

Les cybercriminels maximisent leurs opportunités en ciblant simultanément les vulnérabilités OT anciennes, mais aussi celles, nouvelles, qui émergent sur une surface d'attaque en expansion.[11]

Le besoin d'un SD-WAN fiable, sécurisé et économique pour l'OT

Alors que les cybercriminels (hacktivistes, assaillants opérant pour le compte d'états-nations ou groupuscules du crime organisé) cherchent de plus en plus à endommager les systèmes OT pour atteindre leurs propres objectifs, les entreprises doivent maximiser les avantages de la digitalisation tout en minimisant les nouveaux risques induits par ces technologies et leurs environnements sensibles.

Les gains de productivité et les économies sont essentiels pour toutes les entreprises. Mais les secteurs d'activité qui dépendent de l'OT ne peuvent se permettre de tenir ces objectifs au détriment de la sécurité de leurs activités et de leurs équipes. Le risque supplémentaire que les connexions directes à Internet font courir aux environnements OT nécessite un SD-WAN avec une sécurité intégrée, une visibilité centralisée et des fonctions de gestion à distance. De plus, pour apporter les avantages du SD-WAN aux environnements industriels modernes, il s'agit d'opter pour des solutions renforcées et adaptées aux conditions physiques austères et parfois hostiles des environnements OT.

[1] « 2020 State of Operational Technology and Cybersecurity Report, » Fortinet, 30 juin 2020.

[2] « 2019 Data Breach Investigations Report, » Verizon, avril 2019.

[3] Bruce Sussman, « 15 Cyber Threat Predictions for 2020, » SecureWorld, 12 décembre 2019.

[4] Nirav Shah, « SD-WAN: More Than A Retail Solution, » Network World, 15 juillet 2020.

[5] Joe Robertson, « What Manufacturing CISOs Need to Know About SD-WAN, » LinkedIn, 20 décembre, 2019.

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

[7] « 2020 State of Operational Technology and Cybersecurity Report, » Fortinet, 30 juin 2020.

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

[9] « SD-WAN Isn't Just for Retail, » Fortinet, 3 avril 2020.

[10] « SD-WAN Market Expected to Increase 168 Percent by 2024, » BBC Magazine, 8 juillet 2020.

[11] Derek Manky, « Operational Technology: Why Old Networks Need to Learn New Tricks, » Dark Reading, 31 décembre 2019.

mars 2, 2021 11:15 AM

839530-0-1-FR

wp-FA-the-promise-of-sdwan-A4_FR