FORTINET

Extending SD-WAN To OT Environments

Challenges and Solutions

Table of Contents

Executive Overview

The convergence of operational technology (OT) environments with enterprise-grade information technology (IT) solutions is offering many breakthrough capabilities across industrial businesses, manufacturing, and critical infrastructure. Software-defined wide-area networking (SD-WAN) is one such solution. SD-WAN can replace traditional WAN across distributed and remote deployment infrastructures with higher-performing and more affordable commodity internet connections. But this performance and cost savings comes at the cost of losing traditional WAN's centralized security.

For vulnerable (and increasingly targeted) OT-based organizations to gain the benefits of adopting SD-WAN, they need to look for a solution with robust, integrated security that's designed for the unique needs of these sensitive environments. A next-generation firewall (NGFW) solution that combines networking and OT-native protection offers an ideal tool for these sorts of deployments.

Reconnecting Remote Offices

Traditional WAN relies primarily on expensive multiprotocol label switching (MPLS) or satellite connections. To maintain centralized control and visibility, traffic is backhauled to an on-premises data center—which can impact performance due to security bottlenecks.

SD-WAN has become a popular way to connect remote locations for corporate enterprises. SD-WAN uses a variety of commodity internet connections such as Long-Term Evolution (LTE), digital subscriber line (DSL), or cable to replace MPLS/satellite links at significant cost savings. To ensure application performance and user experience, SD-WAN manages traffic routing based on performance (e.g., latency, jitter) and connectivity costs to deliver a reliable, high-quality connection.

Broad SD-WAN adoption in enterprise organizations suggests that OT environments will be next, once gear that meets the needs of OT environments exists. That starts with ruggedized SD-WAN equipment designed for industrial, manufacturing, and critical infrastructure environments—situations with demanding environmental conditions (e.g., oil rigs, electrical substations, assembly lines, maritime cargos).

The worldwide SD-WAN market is forecasted to grow 168% through 2024 and surpass $3.2 billion.[1]

SD-WAN for OT Has Some Unique Needs

SD-WAN offers the same connectivity cost savings to OT-based organizations that it does to enterprises. It can also help boost productivity. Accelerating traffic flows and communications ensures that production performs at an optimal pace. SD-WAN can also reduce latency versus connecting via a central data-center firewall.[2]

The unique nature of OT environments, however, presents some particular needs when selecting a solution for these types of infrastructures. Disruption to an OT system can have a huge impact on productivity, efficiency, and even safety. Within critical infrastructure (e.g., hydroelectric dams, nuclear power plants, oil and gas pipelines), control systems outages can even have repercussions that impact human lives and the environment.

SD-WAN solves several OT challenges at the same time, including rapid deployment, fast connectivity, and unified management to reduce IT overhead.[3]

Those who manage OT operations find themselves stuck in a reactive stance while trying to protect environments with uniquely sensitive requirements.[4]

A solution must be physically rugged

Some OT environments can be prohibitively harsh for normal IT gear due to extreme physical conditions (temperature, moisture, vibration, electromagnetic interference, limited space, or power sources). Therefore, organizations need an SD-WAN solution that is physically ruggedized and designed to reliably perform under all sorts of punishing environmental conditions.

A solution must be capable

An OT-capable SD-WAN solution must also support long-term installation in remote locations where there may not be any IT staff on hand—such as electrical substations, ships, or oil rig platforms. Therefore, the solution should offer zero-touch deployment capabilities as well as remote monitoring and management. Another critical connectivity capability to look for would be an integrated LTE modem for locations with cellular tower coverage. The solutions should also address certification requirements of specific industry standards or regulations.

A solution must be secure

As the air gaps that previously protected OT environments disappear with digitalization, OT systems are increasingly being barraged with both recycled IT-based attacks and purpose-built OT exploits.[5]

The security implications of direct access to cloud and internet resources can potentially have even greater impact in an OT environment than they would in a typical SD-WAN deployment.[6]

Because SD-WAN uses direct internet connections without backhauling traffic to a data center for centralized security checks, these connections need to be protected from a rising tide of opportunistic attacks. And this requires OT-native security that doesn't disrupt sensitive control systems, bottleneck performance, or degrade user productivity.

Unfortunately, most solutions on the market today do not offer any robust, built-in protections—let alone OT-native security. Most traditional SD-WAN products just provide mechanisms for determining traffic routes. Security becomes an expensive afterthought—an additional cost and complexity burden that must be taken on by the organization.

A 2020 survey revealed that 90% of organizations experienced at least one OT system intrusion in the past year—and 65% had three or more.[7]

A Combined Solution for Security and Networking

To address all of these critical needs, organizations need a combination of advanced SD-WAN networking capabilities and OT-native security. An NGFW that integrates advanced SD-WAN traffic control with OT-appropriate security features (e.g., advanced threat protection, application inspection, intrusion prevention [IPS], URL filtering, botnet protection) offers an ideal solution. OT-based organizations need purpose-built security that covers three essential needs:

- **Visibility.** Organizations cannot protect any part of their infrastructure that they cannot see. And a majority (78%) of organizations have only partial centralized visibility of their OT environments.[8]
- **Control.** The ability to enforce policies and take appropriate action as needed, without disrupting or shutting down critical systems.
- **Awareness.** Continuous security monitoring to detect anomalies. This includes ongoing analysis of user and device behaviors (learning what, where, when, who, and how) to provide actionable intelligence about any potential known or unknown threats.

An NGFW-based approach supports centralized management of SD-WAN policies and controls from a security operations center (SOC). Distributed OT organizations with remote deployments and limited staff can ensure continuously secure operations from the moment of deployment. The SOC can maintain visibility of each and every site to monitor threat levels, segment the networks to keep OT and IT separate, and quarantine systems found to be infected in order to limit malware propagation.

Reducing Costs—and Risks

For industries that depend on OT control systems, a secure SD-WAN solution can provide an extra level of protection beyond what may already exist in an IT/OT gateway. A truly integrated solution could not only provide WAN savings but also furnish a single cybersecurity approach that reduces complexity, extends needed visibility and control deep into the OT network, and prevents the exploitation of OT vulnerabilities that lead to costly production downtime.

IT/OT convergence may be the root of today's security challenges, but it is also the foundation for a durable solution in enabling delivery of accurate, actionable information. [9]

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

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

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

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

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

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

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

[8] Ibid.

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

www.fortinet.com

829648-0-0-EN

November 18, 2020 8:13 AM

eb-sdwan-ot-environments