Fortinet and Siemens Security Solutions

Industrial Switching Platform with Integrated FortiGate for Enhanced Security and Simplified Deployments

Executive Overview

Unlike Information Technology (IT) networks that are responsible for business and information systems, Operational Technology (OT) controls industrial equipment in manufacturing plants, power grids, water utilities, shipping lines, and more. Traditionally, OT and IT networks were separated by an air gap to keep OT environments safe from cyber-attacks. Recently, however, IT-based technologies such as sensors, Machine Learning (ML), and big data are being integrated with OT networks to create new efficiencies and competitive advantages. But this convergence with IT increases the risk of intrusion in OT networks. Security architectures must now include all the connected systems where an intrusion can occur—even deeply embedded OT controls in harsh environments. A joint solution from Fortinet and Siemens combines FortiGate Next-Generation Firewalls (NGFW) with RUGGEDCOM switching and routing platform from Siemens designed for these sorts of remote OT deployments.

Deploying reliable connectivity and security in harsh and frequently remote or substation environments has traditionally not been easy. Segmenting OT networks is one of the first steps for good cybersecurity hygiene. However, harsh environments have few options when it comes to deploying world-class firewalls. While rugged products do exist, assembling and deploying the various parts of the complete solution can create issues with connectivity, reliability, space, and even physical security.

Fortinet and RUGGEDCOM Benefits

This single-box joint solution for harsh environments simplifies:

- Space
- Power
- Deployment
- Connectivity
- Management

FORTINET Fabric-Ready

Siemens and Fortinet recently established a technology partnership to address the above challenges by integrating award-winning FortiGate NGFW technology into the proven and flexible RUGGEDCOM switching and routing platform. This solution provides a single, integrated appliance for OT network segmentation in harsh environmental conditions. It simplifies deployment of the solution to a single piece of hardware. Power, space, physical security, and connectivity issues and concerns are all resolved with the single box deployment model. Remote management further simplifies the deployment and ongoing management. Working together, Siemens and Fortinet are providing the connectivity and security needed by organizations with OT systems.

More than half of organizations with OT environments lack internal network segmentation.

Joint Solution Description

Leveraging the flexibility of the RUGGEDCOM platform, Siemens and Fortinet have enabled FortiGate-VM to run within the switch's virtual machine computing platform. This integrated solution provides for best-in-class protection for OT networks—including full firewall capabilities, malware blocking, application control, and Secure Sockets Layer (SSL)/Transport Layer Security (TLS)-inspection for encrypted traffic flowing through the switch. Using FortiGuard Labs threat research services and FortiGate Intrusion Prevention System (IPS) technology for discovering unknown threats, this integrated platform offers the ability to search traffic for the protocols and vulnerabilities specific to OT environments.

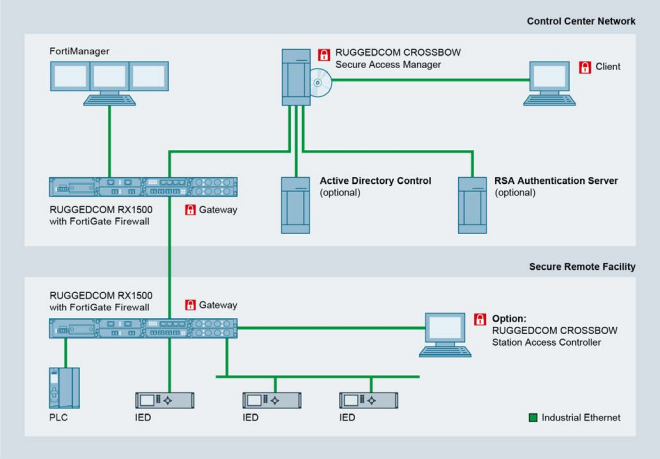

Figure 1: A remote location showing the single box, joint solution deployed at the edge of the network.

About 74% of OT organizations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.

FortiGate-VM

FortiGate-VM provides a full-featured FortiGate packaged as a virtual appliance. FortiGate-VM offers an ideal solution for monitoring and enforcing virtual traffic on leading virtualization, cloud, and Software Define Network (SDN) platforms. FortiGate-VM can be orchestrated in software-defined environments to provide agile and elastic network security services to virtual workloads. FortiGate-VM helps to mitigate blind spots by implementing critical security controls within virtual infrastructures. They enable rapidly provisioning of firewall, intrusion prevention, VPN, antivirus, and other consolidated security functions to virtual workloads.

Rugged, Resilient, and Reliable OT Controls

Regardless of the industry or environmental conditions, stable and resilient OT controls require integrated security to keep safe from advanced threats and running smoothly. The RUGGEDCOM security solution from Fortinet and Siemens combines best-of-breed virtual NGFW security capabilities with a proven platform for industrial switching and routing.

RUGGEDCOM Cybersecurity Solutions

The RUGGEDCOM RX1500 is a multi-service platform for Layer 2 and Layer 3 switch routing. With its field replaceable line modules, the RX1500 is designed and manufactured for harsh environments. The RUGGEDCOM Application Processing Engine (APE) is a utility-grade computing platform that allows for the Fortinet FortiGate to provide next generation firewall functionality within the multi-service platform form factor. As part of a Defense in Depth approach based upon IEC 62443 which includes the Siemens Secure Remote Access by CROSSBOW, Siemens and Fortinet joint enhanced cybersecurity solution helps to protect and secure OT environments.

FORTINET

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray