SOLUTION BRIEF

Securing OT with Network Microsegmentation

Executive Summary

Traditionally, Operational Technology (OT) networks have used Local Area Network (LAN) solutions, such as Virtual LAN (VLAN) on network switches, to segment flat networks and protect against lateral movement of malware throughout the network. While VLAN solutions can provide segmentation with a greater degree of flexibility, this level of segmentation is insufficient to secure these networks from advanced threats and lack visibility into application-level communication.

By implementing microsegmentation using Fortinet technologies, it is possible to implement a zero-trust security policy and to inspect all network traffic within a VLAN via a next-generation firewall (NGFW). This dramatically decreases the ability of malware to move laterally throughout the network. Microsegmentation provides OT networks with the security they need—without sacrificing network performance.

Introduction to ICS/OT Networks

The communications network within an industrial control system (ICS) realm is known as a process control network (PCN), also broadly referred to as an OT network. It enables communication between the various automation processes residing on discrete components of the ICS, including the programmable logic controller (PLC), remote terminal unit (RTU), distributed control system (DCS), and supervisory control and data acquisition (SCADA) system.

The PCN transmits instructions and data between control and measurement units and interconnects various components within an OT environment. PCNs are high-performance, robust, and deterministic LANs. A PCN must maintain constant availability, rapid response, robust error checking, and correction to ensure zero downtime and enable the deterministic, error-free, and continuous operations of an ICS.

To achieve the determinism and robustness requirements of an ICS, PCNs are often configured in flat network structures with little or no boundary limits between the different components of an ICS, as shown in Figure 1. This inherently flat network structure of the PCN makes it faster and easier to maintain.

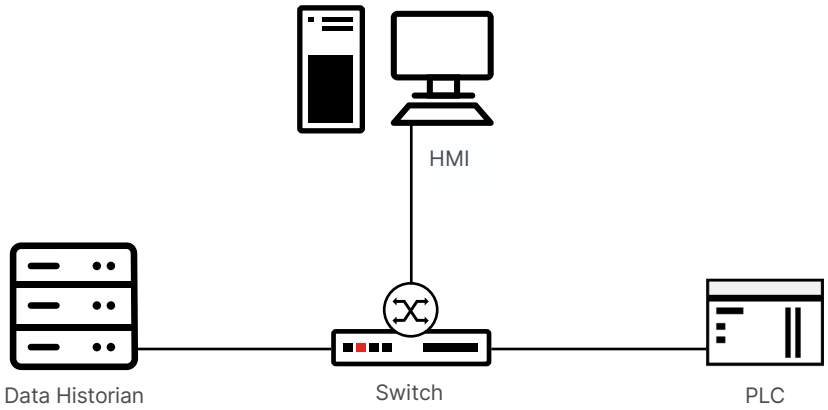

Figure 1: Example of a flat PCN topology

However, it also makes PCNs prone to numerous security threats, such as lateral movement of malware within the PCN and network floods. These threats can potentially disrupt the PCN communications and stall the entire ICS. Moreover, the flat network structure makes it difficult to integrate a PCN with other communication networks outside of the ICS boundary.

Traditionally, the automation industry has utilized LAN solutions, such as network bridges and gateways, to separate the various network components and restrict network broadcasts or floods within the PCN. The implementation of VLANs can add flexibility to this network segmentation process, allowing network separation regardless of physical layout of the network. However, VLANs alone do not address the security issues that could still cause significant damage to the PCN. Furthermore, the adoption of VLAN-based segmentation within PCNs is slow compared to enterprise networks.

Zones and Conduits in ICS/OT Networks

To address the security challenges within ICS/OT networks, the automation industry introduced the concept of zones and conduits to divide the PCN into multiple segments, isolating the various components in an ICS. Within an ICS, a zone groups logical or physical assets that share common security requirements and defines the security boundaries for information entering and leaving a zone. Conduits are introduced between different zones to control communication between zones and to implement security controls. Conduits act as control mechanisms (gatekeepers) between the different zone boundaries.

The zone and conduit model is introduced in International Society of Automation (ISA) and International Electrotechnical Commission IEC 62443-1-1 and IEC 62443-3-2. It provides detailed guidance on how to define zones and conduits. Furthermore, the Purdue Enterprise Reference Architecture (PERA) framework lays out the foundation for separating the various zones and conduits within an ICS into a hierarchical network architecture comprising multiple levels.

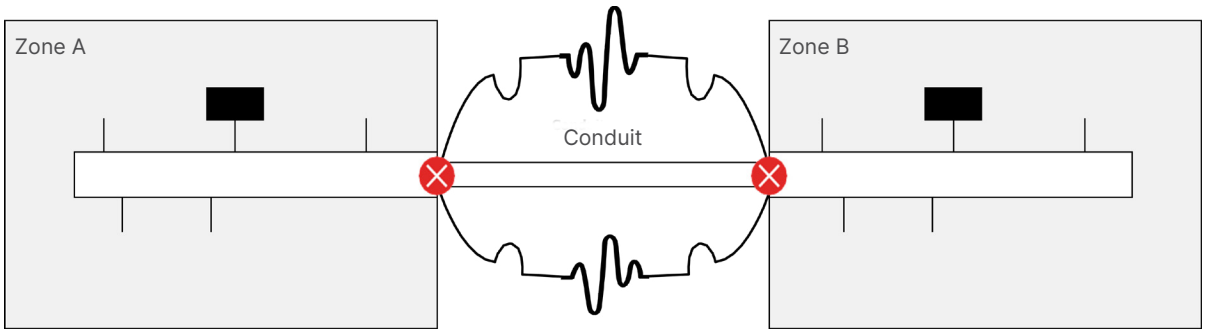

Figure 2: Concept of security zones and conduits

Industrial Disruption—OT, IIoT, IT, IoT, and Convergence

The evolution of Industry 4.0 and disruptive technologies, like the Internet of Things (IoT) and Industrial Internet of Things (IIoT), transformed ICS/OT networks into more converged networks. ICS/OT are no longer operating in an isolated environment, however, they are connected to enterprise IT networks and external networks to increase productivity, optimize resources, collect process analytics, and derive business decisions.

In a converged OT/IT infrastructure, communication is no longer based on proprietary network communication protocols or even standard ICS-specific communication protocols. Instead, the converged OT and IT networks rely on a combination of complex and open standard internet-enabled communication protocols that are inherently vulnerable to various attacks. This expands the network's attack surface and makes traditional security controls—such as VLANs—insufficient for ICS, especially as OT and IT networks converge.

Although defining zones and conduits, and separating networks into segments are essential steps for securing converged OT/IT networks, with just VLANs, it doesn't entirely the address network security challenges for a converged infrastructure that uses complex network protocols and applications. VLANs are not sufficient to prevent sophisticated network attacks in such infrastructures.

VLANs freely forward network packets to devices that are part of the same broadcast domain. Every packet that needs to travel beyond the broadcast domain boundary requires a network routing mechanism. Typically, the routing mechanism acts as a virtual or physical conduit and is sometimes used to implement security controls, such as network traffic inspection, to control communication between the two broadcast domains. While VLAN routing mechanisms offer some security benefits, they are insufficient in modern OT/IT converged infrastructures.

VLANs also fail to inspect the network communication within the same broadcast domain. Within a broadcast domain, the devices that are part of a VLAN can unrestrictedly communicate with one another without these communications being inspected or controlled. Private VLANs (PVLAN) can solve some of these challenges however, PVLANs are complex to implement and it also can't offer network traffic inspection.

In a typical ICS network deployment, there are dozens of components grouped together in a single VLAN, and these components can freely communicate with one another without going through a security mechanism or security conduit. This enables any anomalous network communication to move laterally within the PCN.

Once these networks are converged with other networks, usually outside the OT boundaries, it becomes critical to inspect each communication channel. Otherwise, attacks on the network could remain undetected due to complex network integrations. Moreover, the use of internet-enabled open communication protocols for exchanging information between the OT and IT networks introduces additional risk. Weakness in the communication protocol design and the availability of exploits can provide a vector to attack ICS/OT environments.

Network Microsegmentation for ICS/OT Networks

VLAN provides logical network segmentation flexibility. However, network microsegmentation provides more granular control over network traffic by further (micro)segmenting the VLAN and implementing security policies for each (micro)segment. These security policies can be tailored to different types of network traffic to limit network and application flows between various components of an ICS. With network microsegmentation, ICS owners can implement a zero-trust security model, ensuring that a particular PLC cannot communicate with another PLC unless explicitly permitted by the security policy, even when both PLCs are part of the same VLAN.

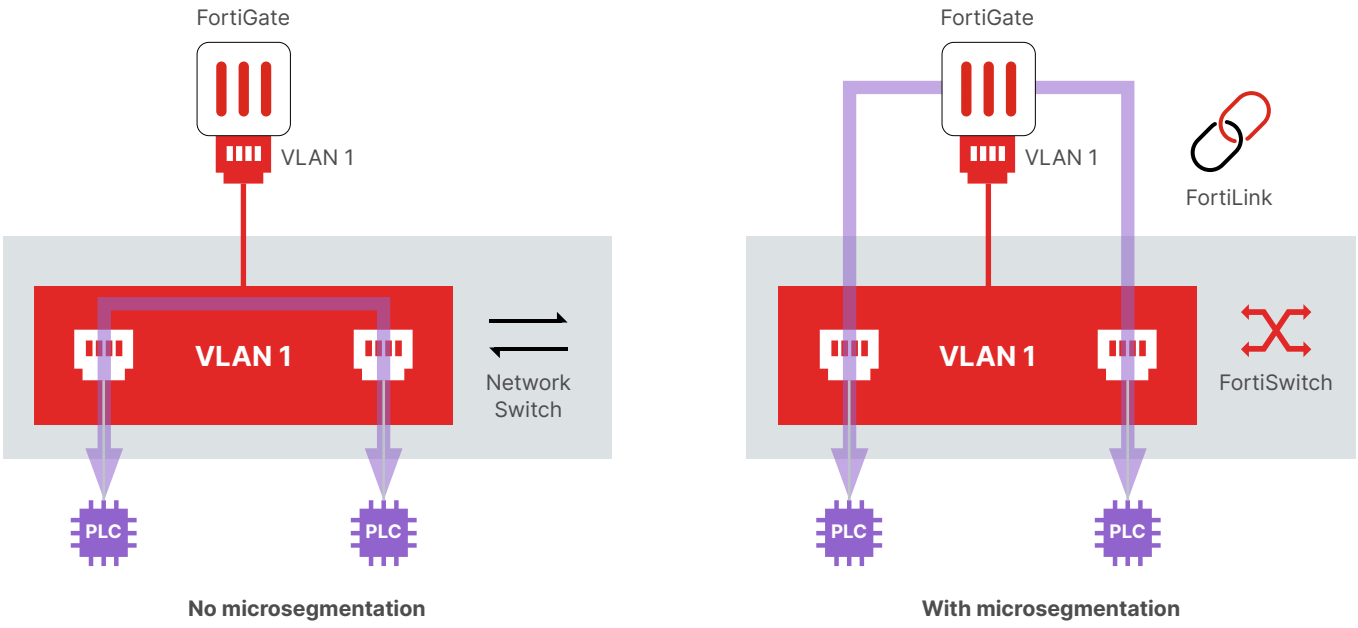

Figure 3: Normal VLAN routing vs. network microsegmentation using Fortinet FortiSwitch and FortiGate

In a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications.

FortiSwitch switches and FortiGate NGFWs offer an integrated approach for implementing network microsegmentation. This integrated solution expands VLAN capabilities from layer 2 network communication to layer 3 (routing) and layer 7 (application visibility), enabling network traffic inspection. The FortiSwitch works at layer 2, defining VLANs, and the FortiGate NGFW works at layer 3, securely routing all communications between VLANs and within the same VLAN. Further, at layer 7, the next-generation intrusion prevention (NGIPS) capabilities of FortiGate enable network traffic inspection using granular security policies, payload level visibility for the communication protocols, and policing of information passing between the network applications through the FortiGate.

The Fortinet integrated solution for microsegmenting the ICS networks provides numerous benefits to ICS/OT asset owners.

- **Host/device isolation.** Isolating each device within the ICS network provides granular control over network communication. Network traffic entering and exiting a device is forced to flow through the FortiGate NGFW, enabling security policy enforcement, traffic inspection, application control, and intrusion detection and prevention.
- **ICS protocol deep packet inspection (DPI).** The FortiGate NGFW provides support for DPI for over 50+ ICS/OT protocols with 1,800+ out-of-the-box application control signatures and 300+ vulnerability signatures.
- **Lateral movement prevention.** Isolation of each component of ICS makes it difficult for malware to spread laterally within the ICS network. All traffic within the ICS network is subject to inspection and policing.
- **High performance.** FortiGate NGFWs are powered by purpose-built security processing units (SPUs) that offer unmatched performance and low latency, which makes them an ideal choice for network traffic inspection within a microsegmented ICS network.
- **Seamless integration.** Logical and physical network connections remain unchanged.
- **Single-pane-of-glass management.** The entire solution is managed through an integrated management console, assisting ICS owners with security automation.

The Fortinet integrated solution for network microsegmentation also uses PERA guidance for solution deployment. The microsegmentation can be implemented at any level within the ICS/OT network if there is network connectivity between the various components of the ICS.

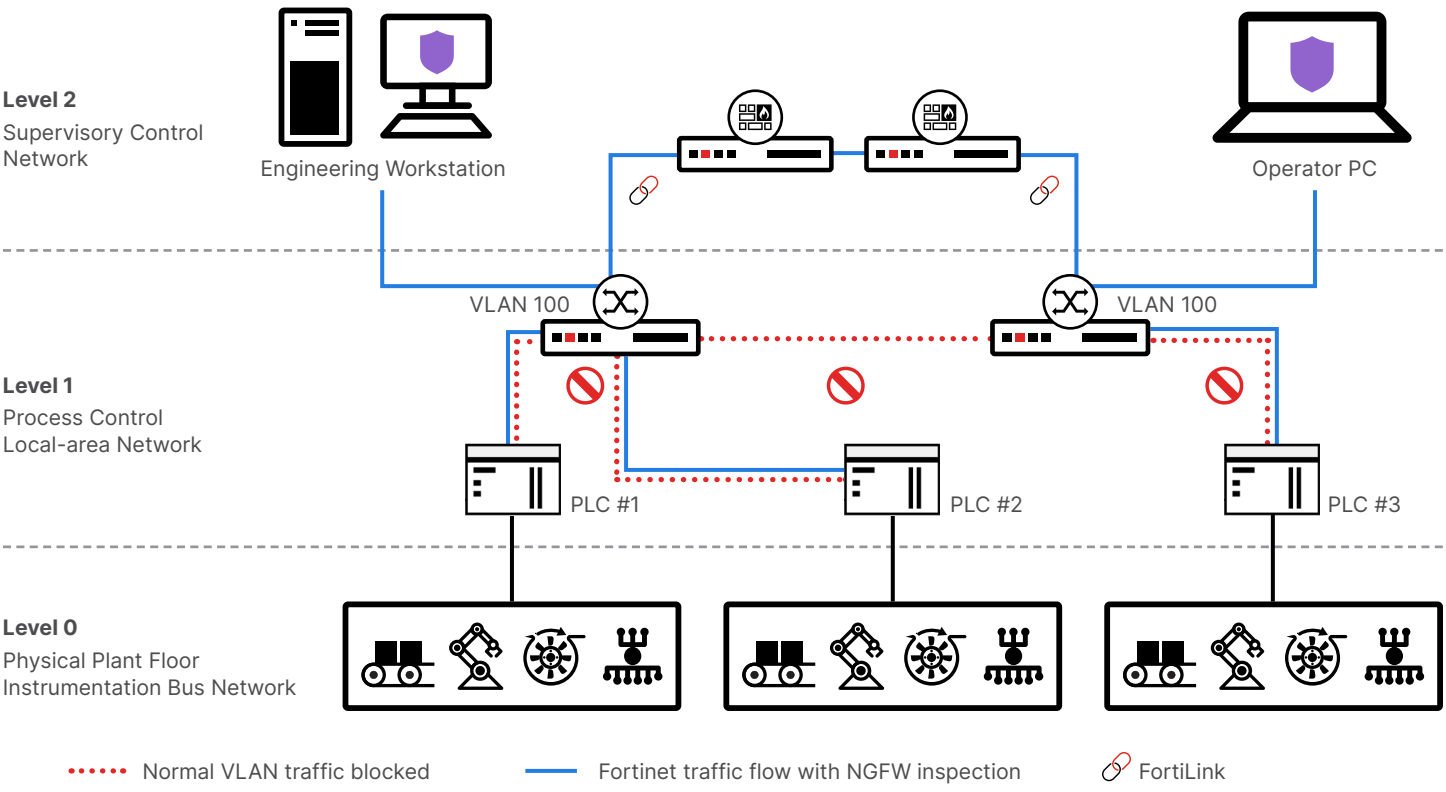

Figure 4: Sample PERA-based deployment architecture for network microsegmentation using integrated FortiSwitch and FortiGate

FortiSwitch for ICS/OT Networks

Fortinet FortiSwitch comes in both rugged and non-rugged hardware, and it supports layer 2 and layer 3 modes of operations. The FortiSwitch portfolio includes high-performance network switches suited for enterprise networks and data center applications as well as DIN-rail and rackmount ruggedized network switches suited for harsh industrial environments with specific features for ICS and OT networks and field applications.

ICS/OT Network Resiliency

While securing converged OT/IT networks and implementing network microsegmentation, consideration must be given to maintain resiliency within the ICS/OT networks that offer 24×7 non-stop critical services. Many ICS/OT networks need to provide up to 99.999% uptime, lightning fast and reliable recovery in case of failures, and an automated mechanism to avoid or minimize network outages.

In combination with network switches, typically, ICS networks follow ring network topology for interconnecting various elements of the ICS in the network. Ring network topology offers simplicity and reduces the total cost of ownership (TCO) in terms of network cabling and implementation. However, ring network topologies are also the most challenging ones in terms of network convergence and implementing network resiliency.

Traditional network convergence protocols such as Spanning Tree Protocol (STP) or its different variants, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Per-VLAN Spanning Tree Protocol (PVSTP) that offer network convergence and recovery times in seconds, are not suitable for implementing resilient and fault-tolerant ICS networks. To improve network availability, redundant ring networks are implemented within the ICS. Redundant ring networks improve the ICS network availability, however, further complicate the implementation of network recovery and convergence mechanisms using traditional network recovery protocols such as STP.

Thus, robust and fault-tolerant network redundancy protocols are required to minimize the recovery times and provide the PCN with the ability to recover and converge faster in case of full or partial network failure. There also needs to be a mechanism for the PCN to recover faster in case only a network node failure occurs in the ring network, instead of a full or partial network failure.

The international standard IEC 62439 specifies network protocols for implementing and maintaining high availability in the industrial and automation networks. The protocols specified in the IEC 62439 standard offer network recovery and convergence in milliseconds and are widely used in ICS/OT networks. Part of IEC 62439-2, is the Media Redundancy Protocol (MRP) that operates at layer 2 in ring networks, comprising up to 50 network switches and achieving deterministic convergence and network recovery times of up to 10 milliseconds. Although, normally 500 milliseconds or even 200 milliseconds are suitable for most of the ICS environments.

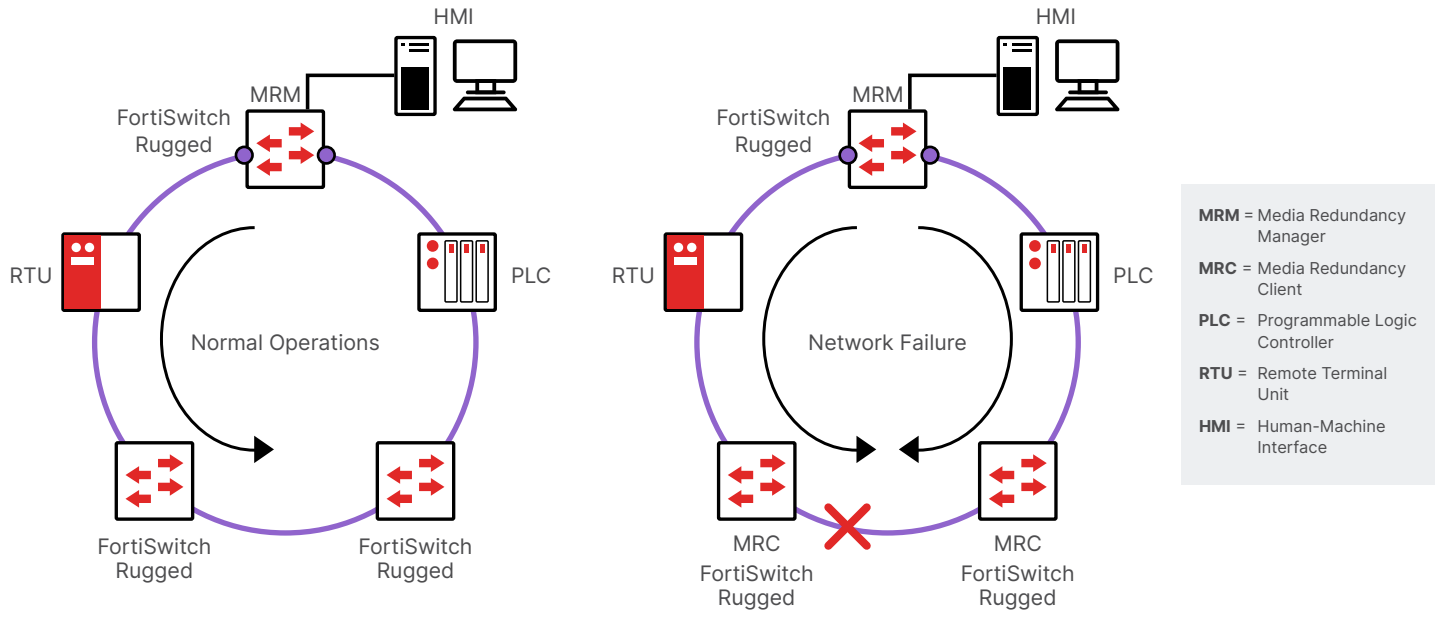

Figure 5: Media Redundancy Protocol (MRP) Ring-Based on FortiSwitch Rugged

An MRP-based network consists of network switches arranged in a redundant ring network topology with one (or more) network switches acting as master node and the rest of the network switches as client nodes. The network switches in the MRP-based ring network must use physical ports to form the ring, or a single port configured as a static trunk. The network switch ports participating in the MRP-based ring network are disabled if they operate with STP. Further details regarding the MRP can be found in the IEC 62439-2 standard.

To address the high-availability and resiliency requirements for ICS/OT networks, FortiSwitch Rugged Series switches support IEC 62439-2 MRP and MRP-based ring network implementation.[1]

ICS/OT Network Monitoring

ICS/OT network asset owners and operators often deploy passive industrial network anomaly detection solutions—also known as industrial intrusion detection systems (IDS)—that passively ingest PCN traffic, analyze it, and provide visibility for network assets and vulnerabilities. The industrial IDS solutions use "sensors" or "probes" that rely on network switches to capture the network traffic, which is then sent to the central server—also knowns as the console—for correlation, analysis, visualization, and reporting purposes.

The network switches connected to the industrial IDS sensors utilize mechanisms such as port-mirroring, switched port analyzer (SPAN), remote SPAN (RSPAN) to passively capture the live network traffic over a layer 2 network without affecting network communication. Typically, multiple industrial IDS sensors are required to capture network traffic from various network segments and as the number of sensors grow in the network, the network layout becomes complex and difficult to manage since the network links stretch across the entire network from each sensor to each network segment. Also, such implementation drastically increases the total cost of the passive network monitoring solution.

FortiSwitch supports SPAN and RSPAN technologies and Fortinet partner industrial IDS solutions like Nozomi Networks Guardian,[2] The Dragos Platform,[3] Claroty Continuous Threat Detection (CTD),[4] and more, can work cohesively with FortiSwitch in ICS/OT networks.

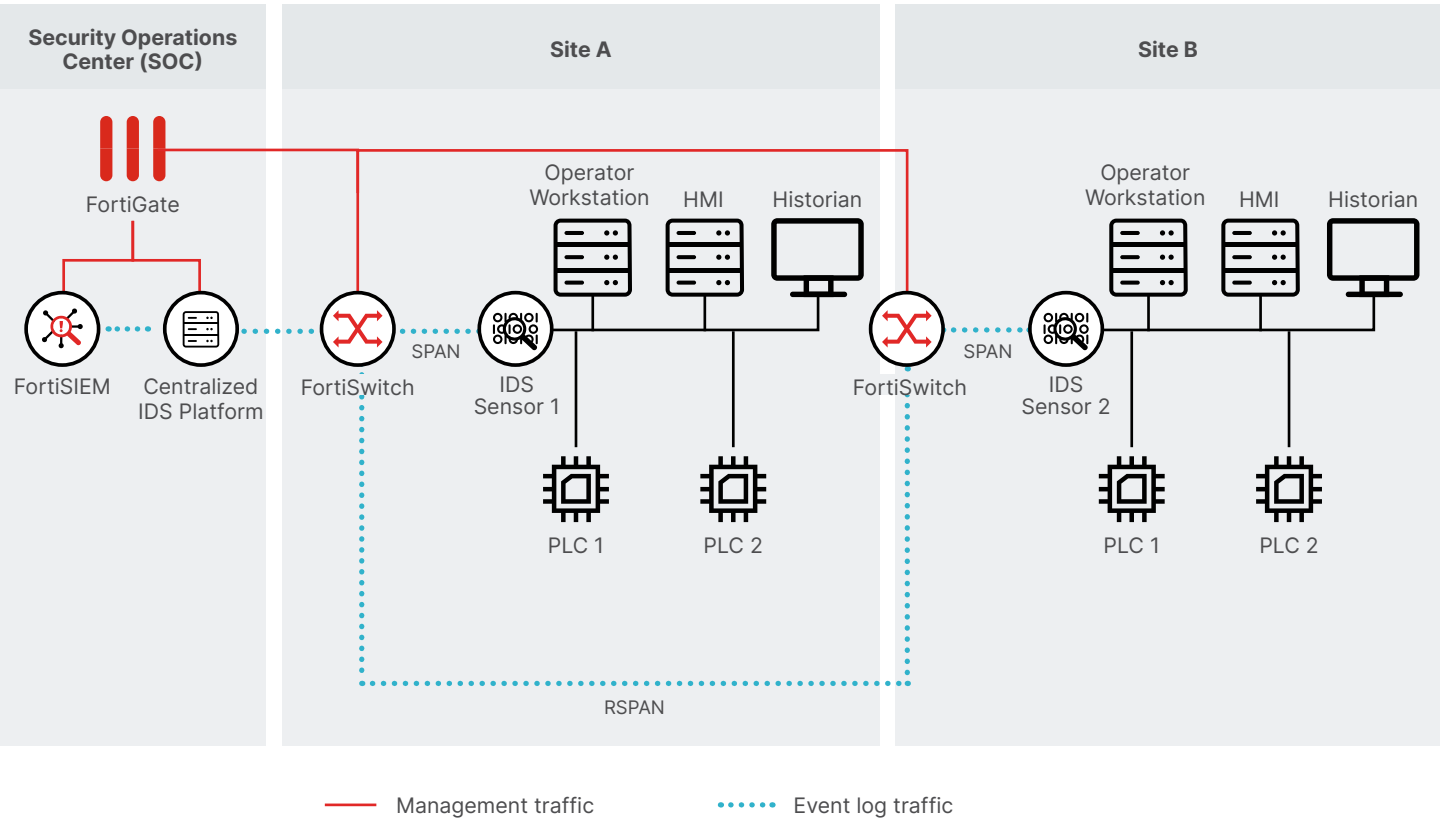

Figure 6: FortiSwitch with industrial IDS sensors showcasing SPAN and RSPAN implementation

To reduce the overall cost of implementing a passive network monitoring solution for ICS, Remote Switched Port Analyzer (RSPAN) and Virtual Extensible LAN (VXLAN) technologies can be used. RSPAN is a layer 2 technology that reduces the number of network capture points (also known as, network taps) and network cabling requirements by combining the network captures to a central network switch. Instead of running physical network cables to each network capture point, the central switch can remotely capture the network traffic within a LAN using RSPAN. On the other hand, VXLAN is a layer 3 technology that can help transport the network captures from various Layer 2 network segments directly to a single central industrial IDS sensor over the Layer 3 network. This eliminates the need for several network capture points and multiple industrial IDS sensors required for the purpose of capturing network traffic from several network segments. FortiGate NGFW supports VXLAN technology.

FortiLink Technology

FortiLink is a Fortinet propriety technology and protocol that allows a FortiGate NGFW to remotely manage single or multiple FortiSwitch units – also known as FortiSwitch in FortiLink mode. FortiLink defines the management interface and the remote management protocol between the FortiGate and FortiSwitch. FortiLink makes it possible to natively integrate FortiSwitch within a FortiGate NGFW UI and perform management and monitoring of network ports available on the FortiSwitch.

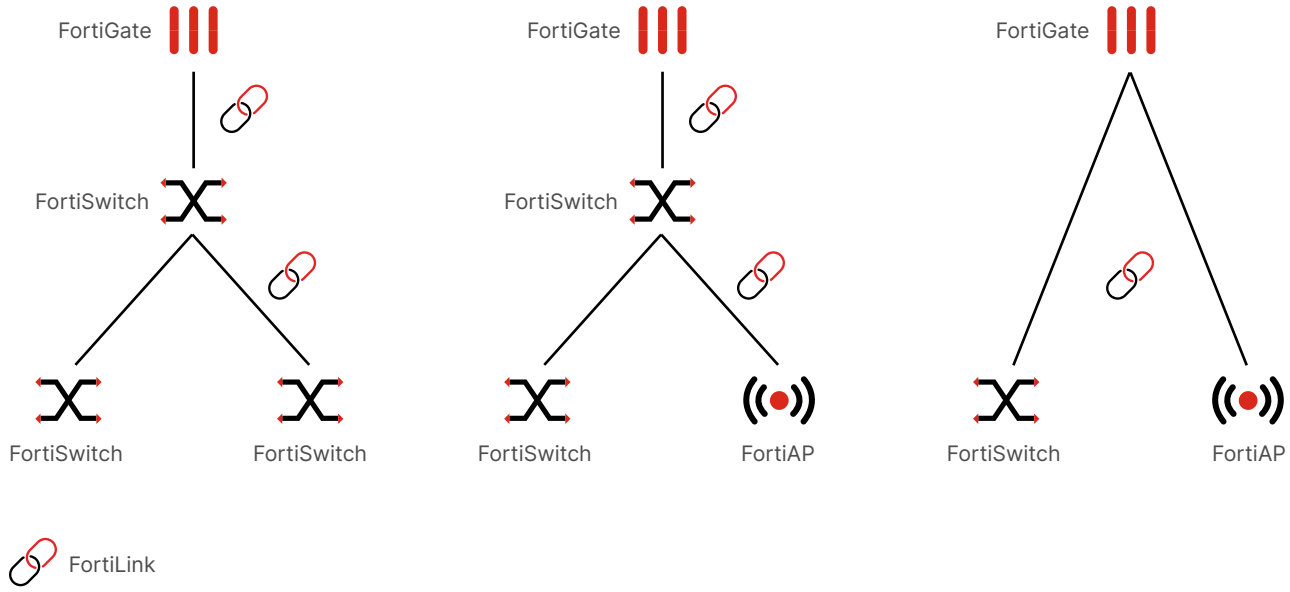

Figure 7: FortiSwitch integration with FortiGate using FortiLink

The native integration of FortiSwitch units within a FortiGate NGFW allows full visibility of network nodes and assets connected to the FortiSwitch. This allows ICS and OT engineers to pinpoint faults and issues in the network and efficiently troubleshoot them.

Centralized Management

FortiSwitch units support local as well as centralized management. While FortiManager—the centralized management platform for FortiGate NGFWs—can also centrally manage FortiSwitch units, the FortiSwitch Manager is a dedicated platform just for FortiSwitch centralized management, monitoring, and logging.

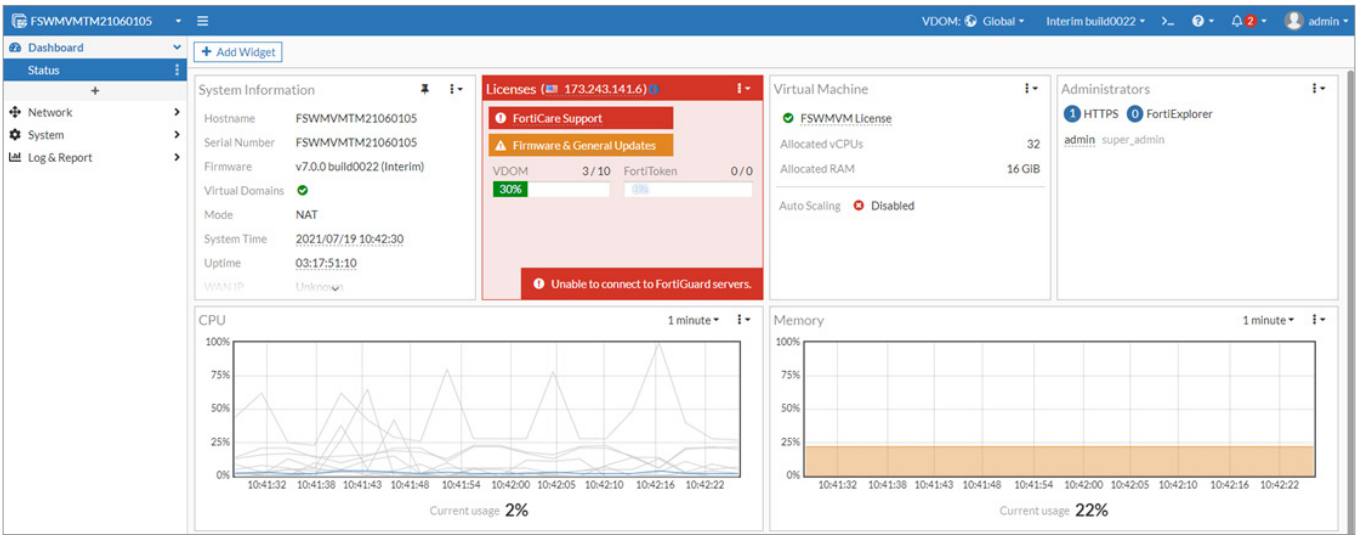

Figure 8: FortiSwitch Manager dashboard

FortiSwitch Manager is a virtual machine (VM)-based platform that can be deployed on-premises using a leading hypervisor platform, including Linux KVM, VMware ESXi, and Microsoft Hyper-V. The FortiSwitch Manager platform can manage single or multiple FortiSwitch units connected to it over a layer 3 network. The FortiSwitch Manager platform acts as the FortiLink Switch Controller.

Conclusion

ICS/OT networks are largely composed of long-life-cycle devices with unique operating requirements. They require an OT-specific approach to security.

Fortinet has demonstrated that it has a unique perspective on ICS/OT network security that enables Fortinet to combine insights with OT-specific threats tracked by FortiGuard Labs into OT-specific security threat reports and to develop solutions that uniquely meet the needs of OT environments.

VLAN-based microsegmentation enables ICS to control business risk while benefiting from a logically segmented network. The Fortinet Security Fabric is essential to tying these solutions together and providing the security team with full, centralized visibility and control over all their security infrastructure.

[1] Media Redundancy Protocol, Fortinet Document Library, accessed July 1, 2022.

[2] Fortinet and Nozomi Networks Comprehensive OT Security Solution, Fortinet, May 2021.

[3] FortiSIEM and the Dragos Platform Deliver Security Visibility, Fortinet, May 2021.

[4] Fortinet and Claroty Comprehensive ICS & SCADA Cybersecurity Solution, Fortinet, September 2021.

July 8, 2022 1:35 PM

1561914-0-0-EN