SOLUTION BRIEF

Securing OT Networks with Microsegmentation

Using Firewall Inspection on Local VLAN Traffic

Executive Overview

Traditionally, operational technology (OT) networks have used local-area network (LAN) solutions, such as virtual LAN (VLAN) on switches, to 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.

With Fortinet microsegmentation, it is possible to implement a zero-trust security policy and to scan all traffic within a VLAN using a next-generation firewall (NGFW), dramatically decreasing the ability of malware to move laterally throughout the network. Microsegmentation provides the OT network with the level of security that it needs without sacrificing network performance.

A VLAN operates at Layer 2 of the communications network and divides a single communications network into multiple virtual networks. This partitions a single broadcast domain into multiple smaller domains, improving network performance. VLANs also enable logical grouping of network elements that are physically dispersed within a communications network.

Introduction to ICS/OT Networks

The communications network within an industrial control system (ICS)/operational technology (OT) realm is known as a process control network (PCN). 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) systems.

The PCN transmits instructions and data between control and measurement units and interconnects various components within an ICS/OT environment. They 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.

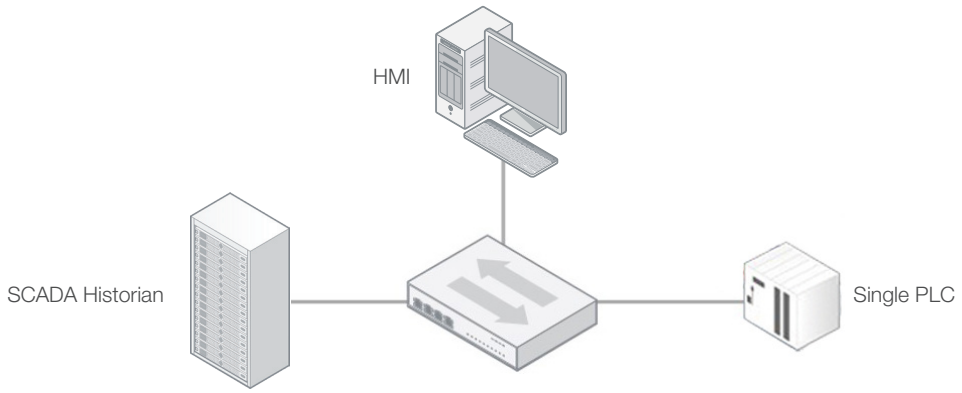

Figure 1: Example of flat PCN topology.

However, it also makes it 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 communications networks outside of the ICS boundary.

Traditionally, the automation industry has utilized LAN solutions, such as network bridges and gateways, to separate the various components and restrict network broadcasts or floods within the PCN. The implementation of VLANs can add flexibility to this segmentation process, allowing network separation regardless of physical layout. 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.

The Purdue Enterprise Reference Architecture, originally developed in the 1990s for computer integrated manufacturing, provides guidance to system integrators and owners on how to segment a large-scale system into multiple levels. This enables better control over integration of various components and subsystems. ISA-99 adopted this model for segmenting ICS into multiple levels and implementing security controls. ISA-99 later became an IEC standard, ISA/IEC 62443.

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 segment the PCN into multiple zones, 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)/International Electrotechnical Commission (IEC) 62443-1-1 and IEC 62443-3-2 and provides detailed guidance on how to define zones and conduits. Additionally, the Purdue Enterprise Reference Architecture (PERA) framework can be used to segment the various zones and conduits within an ICS into multiple levels.

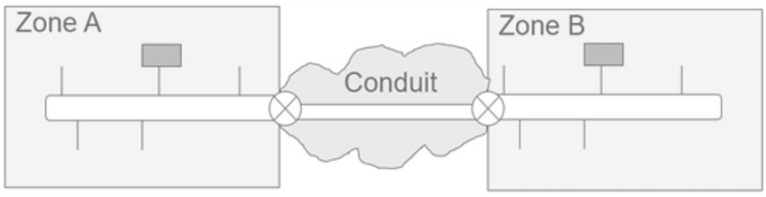

Figure 2: Concept of zones and conduits.

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 IoT (IIoT), transformed ICS/OT networks into more converged networks. ICS/OT are no longer operating in an isolated environment. Instead, they are connected to enterprise IT networks and the external internet and are being used to collect business intelligence and derive business decisions.

In a converged ICS/OT and IT infrastructure, communication is no longer based on proprietary network communication protocols or even simply ICS/OT-specific communication protocols. Instead, the converged ICS/OT and IT network relies on a combination of complex proprietary and open standard 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 segmenting networks into levels are essential for ICS/OT and IT convergence, it doesn't entirely address network security challenges within a converged infrastructure. VLANs are not sufficient to prevent sophisticated network attacks.

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 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 ICS/OT and IT converged infrastructure.

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.

In a typical ICS/OT 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 routing conduit. This enables any anomalous network communication to move laterally within the PCN.

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

The zero-trust network model, or zero-trust architecture, was created in 2010 by John Kindervag at Forrester Research Inc.[1] The zero-trust model states that all attempted connections to an organization's system should be verified before granting access, whether they come from inside or outside the organization's network.

The same zero-trust security concept is followed in ICS/OT infrastructure to whitelist the network communication between different ICS components.

Microsegmenting ICS/OT Networks

VLAN provides logical segmentation flexibility; however, microsegmentation provides more granular control over network traffic by further partitioning the VLAN and implementing security policies for each partition. Further, 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 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.

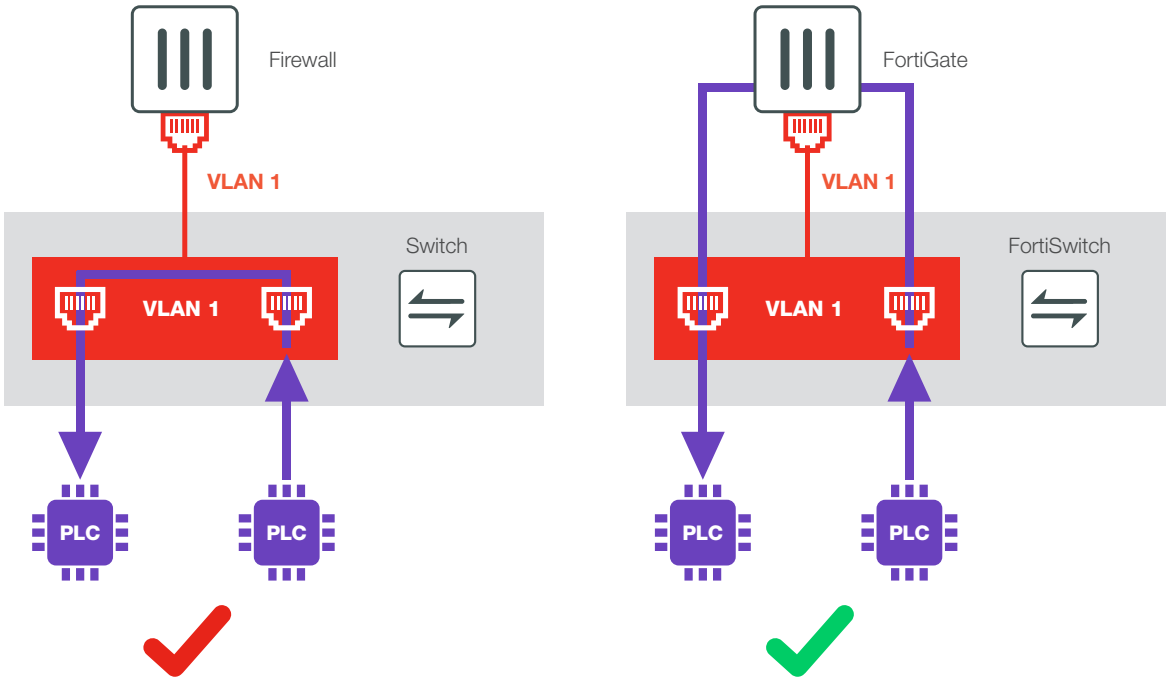

Figure 3: Normal VLAN routing vs. microsegmentation using Fortinet FortiSwitch and FortiGate.

Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation. This integrated solution expands VLAN capabilities from Layer 2 network communication to Layer 3 (routing) and Layer 7 (visibility), enabling network traffic inspection. The FortiSwitch acts at Layer 2, defining VLANs, and the FortiGate NGFW acts at Layer 3, routing all communications between VLANs and within the same VLAN. This enables network traffic inspection using granular security policies, and the NGFWs enable Layer 7 inspection for the network protocols and information passing through the firewall.

The FortiGate NGFW runs on Fortinet's proprietary operating system, FortiOS, which provides industry-leading network security features, such as DPI for ICS/OT protocols, support for ICS/OT specific network protocols, such as the Parallel Redundancy Protocol (PRP), advanced malware protection, an intrusion prevention system (IPS), and software-defined wide-area networking (SD-WAN) capabilities.

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

- **Host/device isolation**—Isolating each device within the ICS network provides granular control over the network communication. The 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 32 ICS/OT protocols with 1,500+ out-of-the-box application control 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 proven industry-leading, high-performance firewalls with the lowest latency,[2] making 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 microsegmentation also uses PERA guidance for solution deployment. The microsegmentation can be implemented at any level within the ICS/OT network as long as there is network connectivity between the various components of the ICS.

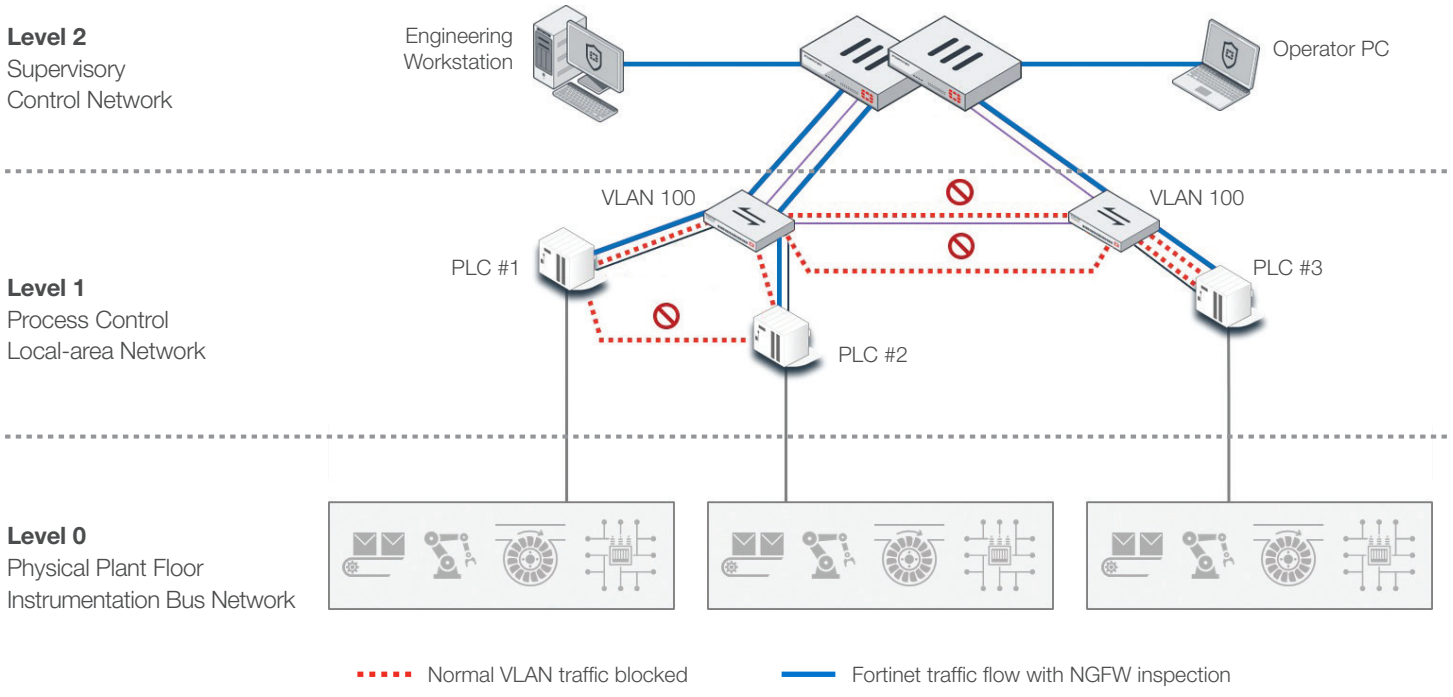

Figure 4: Sample Fortinet FortiSwitch and FortiGate microsegmentation PERA deployment architecture.

Conclusion

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

Fortinet has demonstrated that it has a unique perspective on ICS/OT network security. Fifteen years of partnering with OT organizations have provided Fortinet with the insight needed to publish the first-ever OT-specific security trends report.[3]

This same knowledge and experience enables Fortinet 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 of their security infrastructure.

[1] Mary K. Pratt, "What is Zero Trust? A model for more effective security," CSO, January 16, 2018.

[2] "Deterministic Communications for Secure High-speed Performance: Fortinet Protects Connections to Electronic Trading Platforms with the Industry's Lowest Latency and Jitter Rates," Fortinet, September 23, 2019.

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

Copyright © 2020 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.

March 7, 2020 12:05 AM

562135-0-0-EN

D:\Fortinet\Work\2020\March\030620\sb-secure-vlan-technology