SANS

Analyst Program

Product Overview

Effective Implementation of the NIST Cybersecurity Framework with Fortinet

Original Paper Written by **Don C. Weber**
Updated by **Jason Dely**

February 2020
Updated March 2023

FORTINET

Introduction: Challenges of Connected IT and ICS Networks

Implementing cybersecurity is never straightforward, and this is particularly the case for businesses that run industrial control systems (ICSes) and other operational technology (OT).

OT provides specialized functionality for specific tasks, and that specialized functionality does not conform to the common security practices for securing a corporate IT network. Security teams cannot force IT network policies, standards, and procedures onto the OT network's processes and technology. Instead, they must address the unique systems, devices, and protocols configured in the OT (or the operational dependencies related to the functional requirements of an ICS). Failing to do so will result in the IT security requirements being watered down, formally rejected, or simply ignored, which endangers the business's operations. OT networks are typically connected to the IT network, and increasingly they are linked to internet-connected resources such as cloud-based systems, all potential entry vectors for malware that could disrupt critical operations.

This paper reviews the NIST-based approach to implementing security for an ICS/OT, referencing the NIST Cybersecurity Framework[1] (CSF), the five cybersecurity Critical Controls from the SANS Institute that are most relevant to ICSes, and Fortinet Security Fabric[2] technologies. We also examine how to effectively support and implement the NIST CSF and explore how some of Fortinet's cybersecurity offerings can help an organization fulfill its ICS/OT security road map.

Origin of the NIST Cybersecurity Framework

Since implementation of the Energy Independence and Security Act of 2007 (EISA),[3] NIST has been directly assisting the utility industry with the development of standards for the interoperability and security of the U.S. smart grid. While this effort gave a strong security foundation to the energy sector, the standards could not be easily applied to other critical infrastructure and nonregulated sectors of the economy.

In some ways, sectors that must work under regulations that mandate the objectives that an organization's security program must achieve through the implementation of cybersecurity controls have an advantage. Such sectors have experienced—sometimes for decades—the process of translating words from standards, frameworks, and guidelines into practitioner-focused programs. Some mature standards bodies allow for standards improvements and enforcement capability to measure adherence.

Unregulated organizations, however, must formulate their own approach to cybersecurity. And they often run into a few challenges not always shared by their regulated counterparts. The first is the absence of clearly defined objectives to be supported by the security program. The others are a lack of experience and underfunding, which can preclude the security program's effective execution and maintenance.

The shortcomings of EISA were addressed in 2013, when President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[4] It tasked NIST with providing guidance for improving the security posture of all critical infrastructure sectors. The result was the NIST CSF, which proved to be flexible enough to improve security programs in the critical infrastructure sector and nonregulated sectors as well. For more specific background and guidance on implementation of the NIST CSF, please refer to the SANS paper "Security by Design: A Systems Road Map Approach."[5]

---

[1] Cybersecurity Framework, NIST, www.nist.gov/cyberframework

[2] Fortinet Security Fabric, www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html

[3] Energy Independence and Security Act of 2007, www.epa.gov/greeningepa/energy-independence-and-security-act-2007

[4] Executive Order—Improving Critical Infrastructure Cybersecurity, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] "Security by Design: A Systems Road Map Approach," SANS Institute, January 16, 2020, www.sans.org/reading-room/whitepapers/analyst/security-design-systems-road-map-approach-39370. (Registration required for access.)

Identifying Operational and Tactical Efforts

The NIST CSF has been used successfully by many organizations to shape their OT-specific security programs, and it has proved adaptable for their purposes. IT and OT personnel who are tasked with implementing the short- to mid-range tactical steps necessary to achieve the strategic security goals set for the ICS must also maintain the organization's core operational requirements. As for the organizations, they prefer to modify their existing ICS because that is less expensive than starting from scratch. They also prefer to minimize the modifications made to their ICS architecture and ICS operations, favoring exceptions and alternatives. A common goal is to implement needed security controls in a manner that is cost-effective and has no negative effect on the processes within the OT networks.

It is important that these business-driven implementation goals accommodate a program that a SANS whitepaper identified as "The Five ICS Cybersecurity Critical Controls."[6] (See Figure 1.)

ICS INCIDENT RESPONSE

Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control

SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

RISK-BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Figure 1: Five Critical Controls for ICS/OT Cybersecurity

As the whitepaper says, "Organizations should note, especially if they are part of critical infrastructure, that they have an obligation to ensure a safe operating environment for personnel and a duty to protect from harm the communities they operate in by ensuring appropriate investments in ICS cybersecurity."

Many of the NIST CSF controls focus on the preventive aspect of cybersecurity, but their IT-influenced aspects are challenging to implement and can lead to security exceptions or avoidances. There is inherent value in (and peer acceptance of) utilizing a framework such as the NIST CSF to guide resources and cybersecurity into ICS/OT environments. Some organizations spend years of focused effort on prevention and detection and minimal effort on response and recovery. Although readiness and availability of an ICS directly

[6] "The Five ICS Cybersecurity Critical Controls," SANS Institute, November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls (Registration required for access.)

influences a safe and reliable operation, resources and efforts must be, at minimum, equally applied to response and recovery activities of the ICS/OT cybersecurity program. "The Five ICS Cybersecurity Critical Controls" supplements the NIST CSF by helping to balance the heavily weighted preventative aspect of the framework.

To learn more about the NIST CSF and how your organization can best use it, consult the NIST CSF Quick Start Guide.[7]

NIST CSF Coverage with Fortinet Security Fabric

This section explores how the technologies included in the Fortinet Security Fabric could help drive a balanced implementation of the ICS security program across the five key functions (identify, protect, detect, respond, and recovery) outlined in the NIST CSF. The usual practice of the SANS Analyst Program is to manually test in a lab environment configured for normal operations each technology discussed in our papers to understand its stalwartness and shortcomings. However, ICS lab networks are too restrictive compared with an operational environment and cannot provide a realistic picture.

Fortinet Security Fabric Technologies

The Fortinet Security Fabric is an integration of network and cybersecurity products from Fortinet (see Table 1) and its vendor partners. Within the integration, FortiManager unifies the management and orchestration of Fortinet products, very nearly providing the proverbial single pane of glass. Another Fortinet product, FortiNAC, provides visibility, control, and automated response for everything that connects to the network because it can integrate with third-party devices. With integration being inherent in the Fortinet Security Fabric, control environments benefit because implementation has minimal impact on current operations.

Table 1. Fortinet Products and Descriptions

Fortinet Product	Product Description
FortiEDR	Delivers real-time automated endpoint protection with orchestrated incident response across IT and OT endpoints. The single integrated platform offers flexible deployment options and a predictable operating cost. FortiEDR provides real-time, proactive risk mitigation; endpoint security; pre-infection protection via a kernel-level, next-generation antivirus engine; post-infection protection; and forensics.
FortiClient FortiClient EMS	FortiClient is an endpoint agent that provides visibility and control of software and hardware inventory across the entire Fortinet Security Fabric, allowing organizations to discover, monitor, and assess endpoint risks in real time. It also provides secure remote access (VPN client). FortiClient, along with the FortiClient Enterprise Management Server (EMS), is an integral part of Fortinet's zero-trust network access (ZTNA) offering, and includes these ZTNA, secure access service edge (SASE), and endpoint protection (EPP) capabilities: • With ZTNA, remote users can access their corporate applications, with strict authentication and a verifiable endpoint security posture ensured before access is granted. • With SASE, remote users can securely connect to the corporate network following the same corporate security policies regardless of their location. SASE integrates seamlessly with ZTNA to deliver a transparent user experience while offering security protection from advanced threats for all endpoints. • With EPP, all endpoints gain vulnerability detection and protection, auto-patching for antivirus software, an application firewall, ransomware protection, and endpoint management.

[7] "Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide," NIST, https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

Fortinet Product	Product Description
FortiSwitch	FortiSwitch is a secure-access switch family that delivers outstanding performance, scalability, and manageability while allowing users with OT environments to extend networking and security across their network infrastructure. FortiSwitch seamlessly integrates with the Fortinet Security Fabric via FortiLink and can be managed by FortiCloud or FortiGate. The unified management of FortiSwitch via FortiGate offers complete visibility and control of users and devices in the network.
FortiAP	FortiAP is a series of Wi-Fi access points that can be managed by FortiCloud or FortiGate. These access points offer high throughput, optimal coverage, and enterprise-class 802.11ax services, and security and access control policy enforcement.
FortiExtender	Provides a bridge between local Ethernet LANs and wireless LTE/5G WAN connections. FortiExtender can support diverse wireless applications with a high level of backhaul redundancy using a single LTE/5G modem platform over redundant SIM cards attaching to different mobile networks. FortiExtender can be used as the LTE/5G backhaul of an on-premises FortiGate with maximum wireless LTE/5G signal strength. It can be centrally managed by FortiGate.
FortiGate	FortiGate is the flagship next-generation firewall and intrusion prevention system (NGFW/NGIPS) product family from Fortinet, delivering best-in-class security, high-speed networking, hardware-accelerated performance features using purpose-built security processors for NGFW/NGIPS, and built-in, market-leading SD-WAN. FortiGate comes in different form factors and sizes, including ruggedized appliances to withstand the harsh environmental conditions often facing industrial applications.
FortiToken	Enables two-factor authentication via a one-time password (OTP) application with push notifications or a hardware-based OTP token. FortiToken Mobile (FTM) and the hardware OTP tokens are fully integrated with FortiClient, secured by FortiGuard, and available for direct management and use within the FortiGate and FortiAuthenticator security products. The FortiGate, FortiToken, and FortiAuthenticator integrated solution is easy to implement, use, and manage for multifactor authentication.
FortiAuthenticator	FortiAuthenticator offers single sign-on and user authorization for the Fortinet secured enterprise network. It identifies users, queries access permissions from third-party systems, and forwards the access requests to FortiGate to implement identity-based security policies. FortiAuthenticator supports a wide array of methods and tools for authentication and authorization, such as Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI, and multifactor authentication.
FortiNAC	This network access control product enhances the Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against malicious access, extends access control to third-party devices, offers greater visibility for devices, supports dynamic network access control, and orchestrates automatic responses to a wide range of networking events.
FortiAnalyzer	FortiAnalyzer is a centralized log management, analytics, and reporting platform that provides customers with single-pane orchestration, automation, and response for simplified security operations, proactive identification, remediation of risks, and complete visibility of the entire attack surface. FortiAnalyzer can collect different types of logs and events from Fortinet products via Fortinet Security Fabric integration.
FortiManager	FortiManager provides automation-driven centralized management. It allows end users to centrally manage FortiGate, FortiSwitch, and FortiAP devices in their network with a centralized management platform.
FortiSIEM	FortiSIEM provides unified event correlation and risk management for multivendor implementations. It enables analytics from diverse information sources, including logs, performance metrics, SNMP traps, security alerts, and configuration changes. It feeds all the information into an event-based analytics engine and supports real-time searches, rules, dashboards, and ad hoc queries. FortiSIEM offers Purdue Model for ICS Security level classification for assets, logs, and event correlation, and it also supports MITRE ATT&CK® for ICS framework for log analysis. Integration with third-party OT security tools is supported out of the box.
FortiSOAR	FortiSOAR is a holistic security orchestration, automation, and response workbench that lets security operations center (SOC) teams efficiently respond to the ever-increasing influx of alerts, automate repetitive manual processes, and cope with their chronic shortage of resources. Its patented and customizable security operations platform provides automated playbooks and incident triaging and real-time remediation for enterprises to identify, defend, and counter attacks. FortiSOAR optimizes SOC team productivity by proving more than 3,000 actions and seamlessly integrating with over 300 security platforms. This results in faster responses, streamlined containment, and mitigation times reduced from hours to seconds. FortiSOAR includes ICS-specific capabilities, such as MITRE ATT&CK® for ICS framework for asset and event correlation, IT/OT asset inventory dashboards, compliance dashboards for OT specific cybersecurity regulations and frameworks, and more.

Fortinet Product	Product Description
FortiProxy	This secure web proxy protects employees against internet-borne attacks by incorporating multiple detection techniques, such as web filtering, DNS filtering, data loss prevention, antivirus protection, intrusion prevention, and advanced threat protection.
FortiWeb	A web application firewall (WAF) that secures cloud-based resources and DevOps environments by protecting against known and unknown threats, including sophisticated ones such as SQL injection, cross-site scripting, buffer overflows, and DDoS attacks.
FortiDeceptor	FortiDeceptor provides honeypot and deception technology to deceive, expose, and eliminate external and internal threats early in the attack kill chain, proactively blocking threats before any significant damage occurs. Integrated with FortiEDR and FortiGate, FortiDeceptor automates the blocking of attackers targeting IT and OT systems and devices by laying out a layer of decoys and lures designed to redirect attackers' focus while revealing their presence on the network.
FortiSandbox	FortiSandbox provides top-rated, AI-powered breach protection that integrates with the Fortinet Security Fabric platform to address both rapidly evolving and targeted threats, including ransomware and crypto-malware, across a broad digital attack surface. Designed specifically for OT, FortiSandbox automates zero-day advanced malware detection and response in order to detect threats targeting OT systems and protocols in real time.
FortiNDR	Next-generation, AI-driven breach protection technology to defend against various cyberthreats, including advanced persistent threats, through a trained Virtual Security Analyst™. The virtual analyst helps with identifying, classifying, and responding to threats, including well-camouflaged ones. Employing deep neural networks based on advanced AI and artificial neural networks, FortiNDR provides fast security investigation (less than one second) by harnessing deep-learning technologies that assist in an automated response to remediate different types of attacks.
FortiSASE	A cloud-delivered service, FortiSASE is an architecture that combines network, security, and WAN capabilities to provide endpoints (remote users, devices, and branches) with secure access to the internet, cloud resources, and the data center network. It uses network security technologies including firewall-as-a-service (FWaaS), secure web gateway (SWG), zero-trust network access (ZTNA), and cloud access security broker (CASB). It relies on WAN technologies including SD-WAN.
FortiGuard Security Services	FortiGuard Security Services are powered by FortiGuard Labs, a global threat research and response team that leverages machine learning (ML) and AI systems around the globe to collect real-time threat intelligence. FortiGuard Security Services are offered through subscription bundles and include several advanced threat protection services for enterprise networks, web, cloud, OT, etc. The Industrial Security Service and IoT Detection Service are among the FortiGuard subscription offerings. Industrial Security Service offers more than 2,000 IPS signatures for ICS/OT applications, as well as protocols that support deep packet inspection (DPI) and more than 500 IPS signatures for ICS-specific threat and vulnerability protection.
FortiCamera FortiRecorder	A suite of secure, network-based video surveillance cameras and recorders that bolster protection against cyber-physical attacks.

Network Segmentation and Isolation

The NIST CSF maps informative references to many well-known standards, including IEC 62443 (also known as ISA 62443). Most organizations have deployed their ICS networks following guidelines outlined by the IEC 62443 set of standards. One of the publications within the IEC 62443 provides guidance on how to segment an ICS into security zones and assign security levels (i.e., targeted amounts of security) based on a clear understanding of risk. More information on IEC 62443 can be found in the SANS whitepaper "Effective ICS Cybersecurity Using the IEC 62443 Standard."[8]

[8] "Effective ICS Cybersecurity Using the IEC 62443 Standard," SANS Institute, November 17, 2020, www.sans.org/white-papers/39960

Fortinet Network Management

In our testing, FortiManager enabled us to interact with Fortinet products designed to achieve the network segmentation and isolation detailed in the ICS410 Reference Architecture. (See the FortiManager load-in screen in Figure 2.)

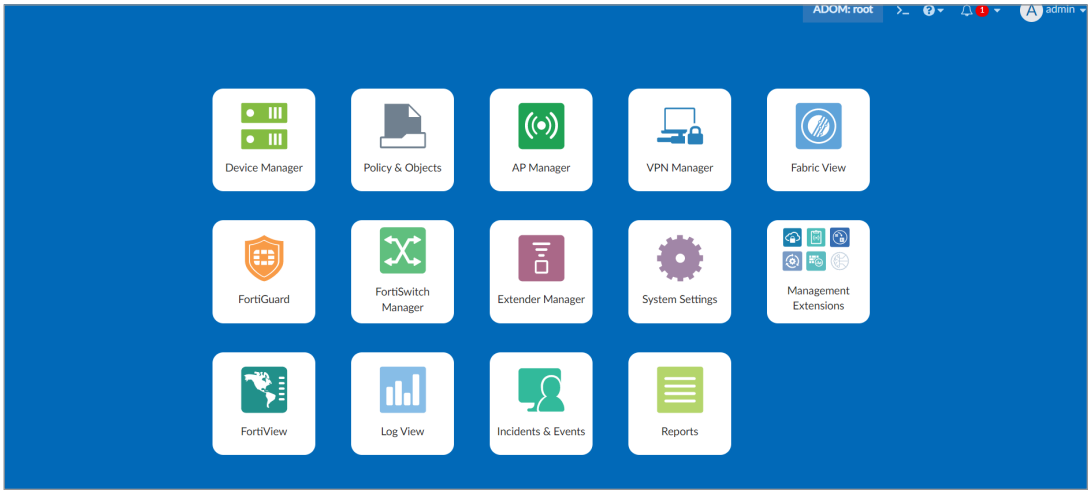

Figure 2. FortiManager Load-In Screen

Our attention was initially drawn to the FortiGate management icons to review how the solution helps with network segmentation and isolation. Policy & Objects and VPN Manager are necessary to control network segmentation and isolation. We assumed that managing the network configuration would work similarly to any firewall, and therefore, we focused on locating specific policy objects related to industrial control protocols.

Selecting the Policy & Object icon took us to the FortiGate management portal. From there, we located the management of industrial protocols by drilling into the Security Profiles and Application Control menu items in the left sidebar, as shown in Figure 3.

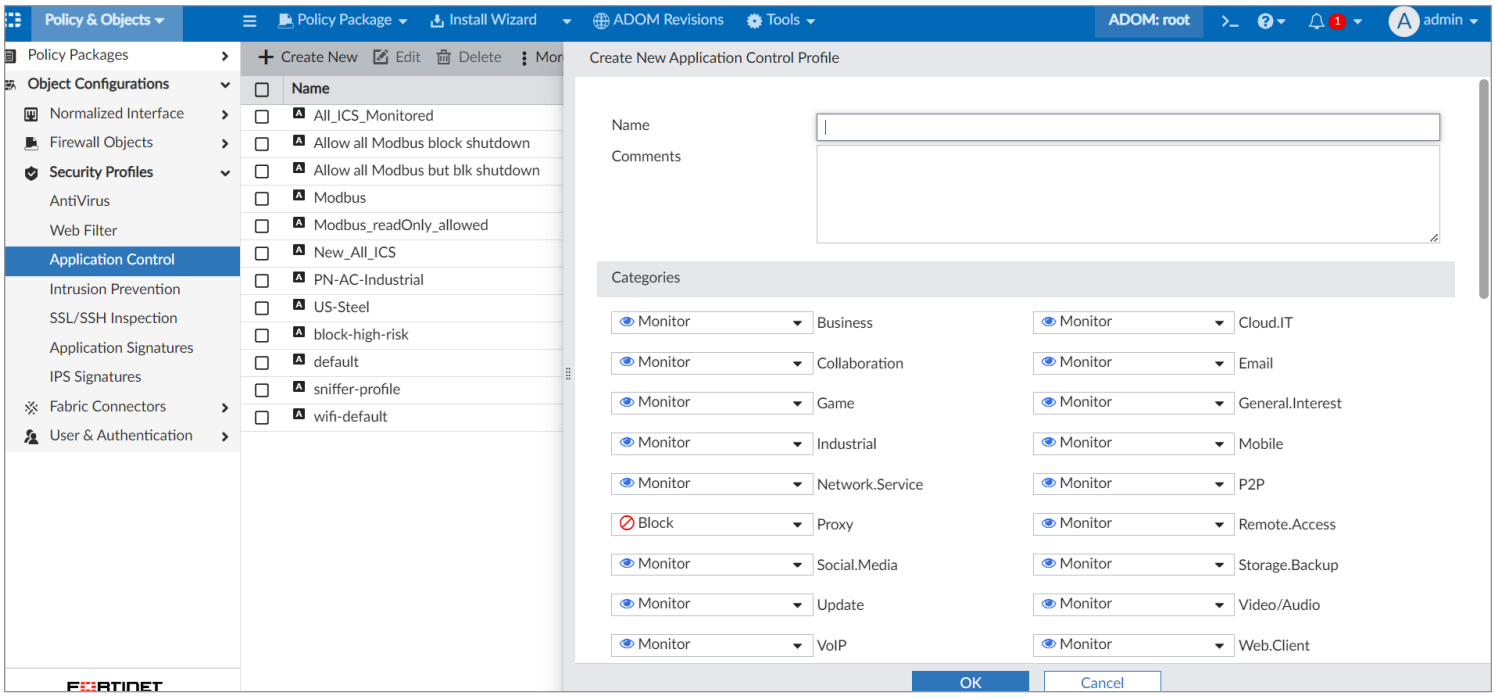

Figure 3. Accessing the Application Control Profile

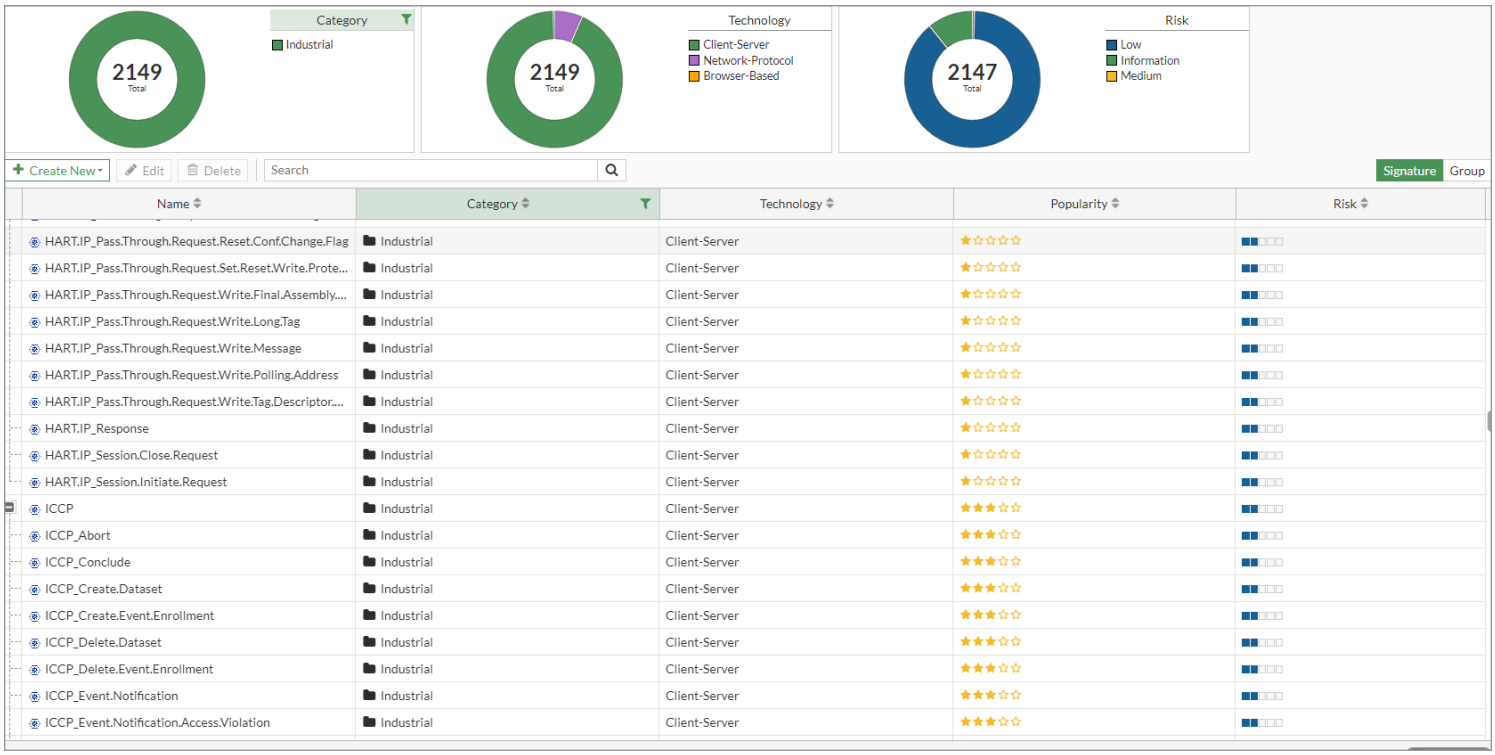

Figure 4. Industrial Control Signatures on FortiGate

A review of the industrial protocols shows that FortiGate provides capabilities for monitoring and controlling many protocols that will be implemented within a control network. These include, but are not limited to, Modbus, Ethernet/IP, Common Industrial Protocol (CIP), BACnet, Profinet, Open Platform Communications (OPC), Siemens protocols, Inter-Control Center Communications Protocol (ICCP), and HART. (See Figure 4.)

To see some of the capabilities, refer to Figure 5.

The capabilities provided allow for the management of specific protocol commands, such as HART and Modbus reading and writing activities, but this control is limited to communications between destinations rather than what happens across the protocol. Initial implementations within operational environments would likely restrict by protocol, while the capability to additionally restrict by functions and commands is necessary as organizations mature.

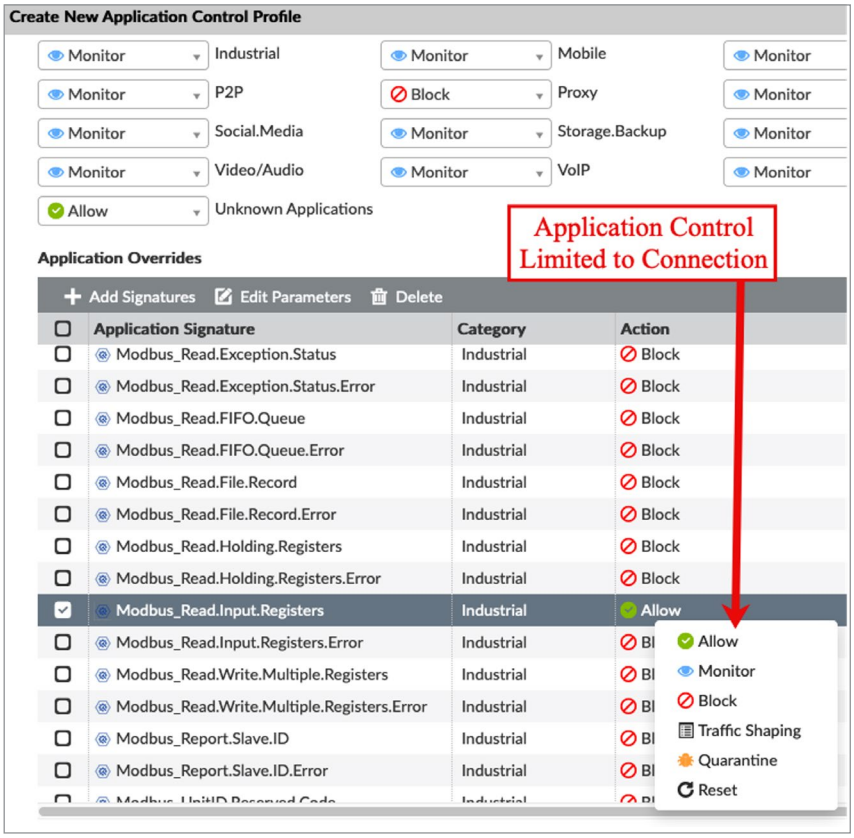

Figure 5. Industrial Application Control Limited to Connection

The log data provided by FortiManager's industrial protocol functionality should provide an organization with visibility into several key areas of concern for ICS personnel. Once implemented, network communication logs can be used to review device redundancy configurations, understand and validate failover functionality, and ensure there are no operational timing issues that occur during device failures. Thus, these industrial protocol-specific network communication logs could improve security while also adding value to the process being protected.

We looked at the VPN Manager functionality that is integrated with FortiManager. Such a tool is greatly needed to defend environments that have increased the amount of remote access they allow, especially because there has been a parallel increase in threat groups using remote-access pathways to gain access to ICS environments. The integrated VPN Manager application allows for the configuration of advanced VPN strategies and technologies, such as those found with SD-WAN, zero-trust access, and privileged access management. The VPN configuration capabilities, shown in Figure 6, provide configuration options to limit connectivity to specific assets within the control network.

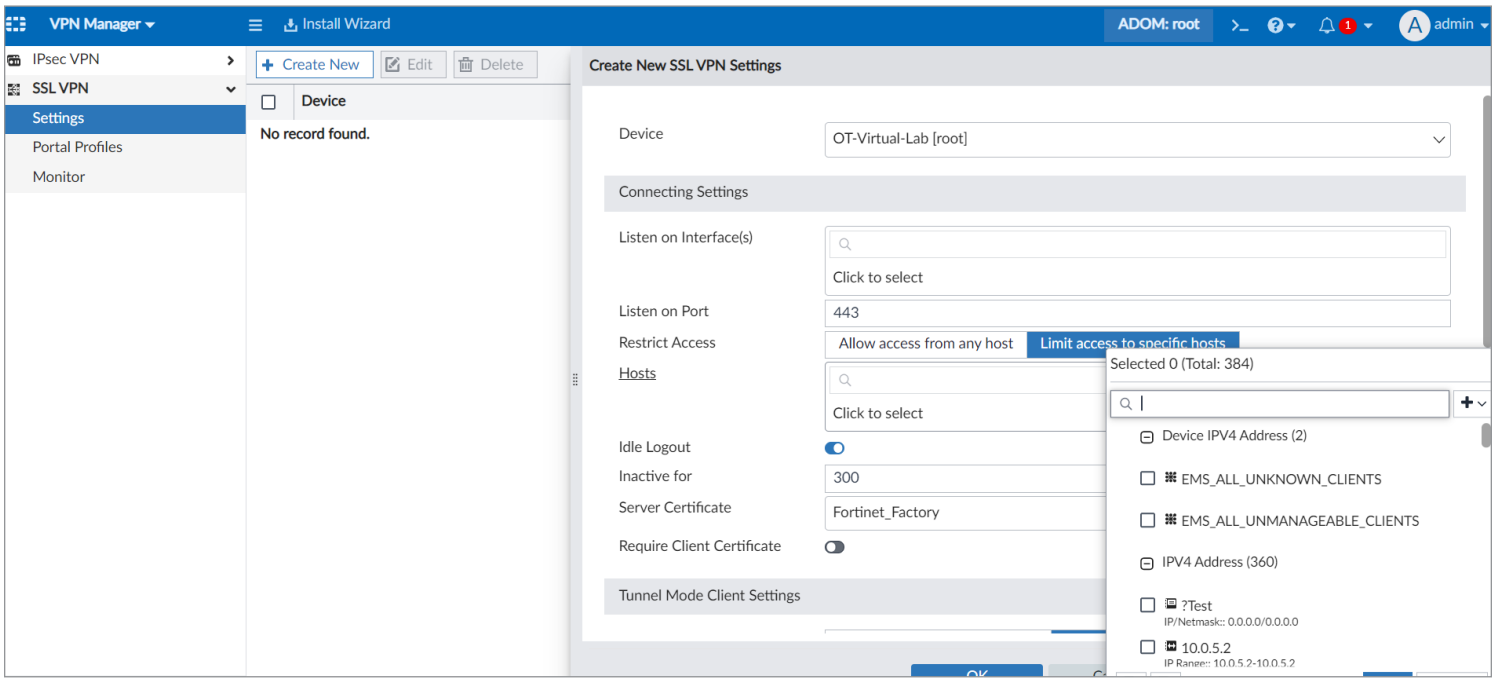

Figure 6. SSL VPN Configuration for Internal Assets

This capability is extremely useful when considering restrictions for remote vendor and integrator access to the control network. Although many advance remote access defense capabilities exist, they were not configured in our test environment and therefore not analyzed beyond these steps.

Access Control

Access control, the second consideration, is a challenging effort for many organizations. Mature control networks will have separate authentication and authorization servers, such as Microsoft Active Directory servers, for their corporate network and the control network. This situation is common for control networks associated with critical infrastructure. Businesses not related to critical infrastructure, however, may struggle with justifying the additional cost and expertise necessary to implement separate access control servers within the control network. Businesses that have deployed their control network access control with a trust relationship to the corporate network should immediately reconsider this configuration and separate these assets.

The FortiAuthenticator and FortiToken devices are two Fortinet technologies that could help in improving control network identity management. FortiAuthenticator integrates with FortiManager and could be beneficial by providing more granular control of users and assets within the control network and improving activity logging. Identity- and role-based policies are leveraged by several of the Fortinet products to limit and monitor user and asset activities within the control network.

The FortiToken device, which provides a two-factor authentication mechanism, is another useful appliance for the control network. Many organizations have deployed two-factor authentication products in their corporate environment that, due to network segmentation and isolation, cannot be used in the control network. Requirements for remote access and administrative access for vendors and integrators leave many organizations in a conundrum as to how to implement two-factor authentication for control network users. The FortiToken appliance integrates with FortiAuthenticator, although it does not directly integrate with FortiManager, and can easily provide an organization with a solution while also integrating with the rest of the Fortinet Security Fabric to provide two-factor authentication capabilities for security administration of the platform.

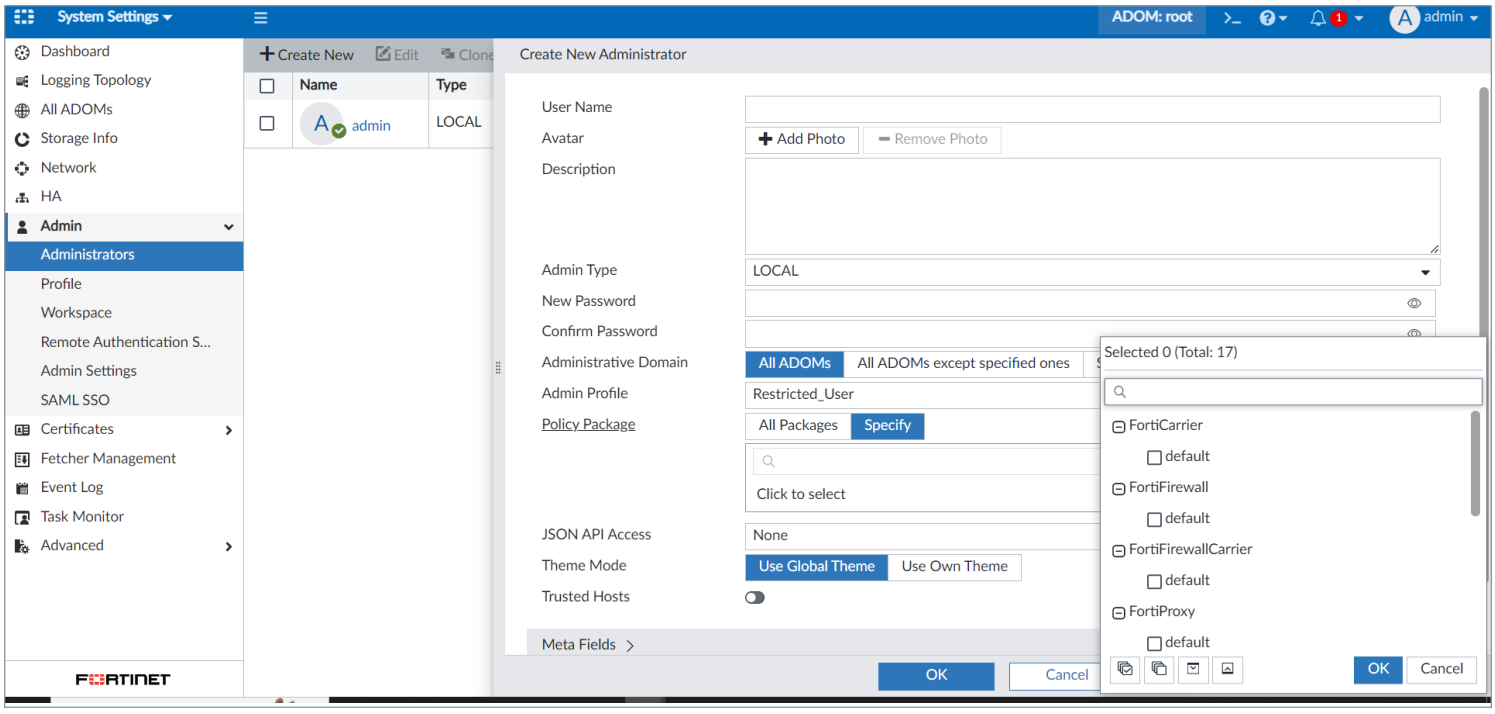

Figure 7. FortiManager Granular User Management

Although these technologies were not available in the test network, we took a look at the access control provided through FortiManager. Deploying many security controls within a network can result in complex and time-consuming user management. FortiManager provides the capability to granularly manage the roles and responsibilities (see Figure 7) for users accessing most of the Fortinet products.

Coupled with two-factor authentication, a central point of management for access control and role management of the security controls is an important feature, and the reduction in management overhead could prove useful.

Logging and Monitoring

Next, we turned our attention to how the Fortinet Security Fabric can help with the third consideration: logging and monitoring. Each ICS device and system produces, and provides vision into, the technology's local events. Understanding these events requires alerting on known unusual activity, correlating events, and reporting on specific activities for classes of assets.

FortiAnalyzer provides visibility into the events that occur across the Fortinet Security Fabric. This device integrates with FortiManager, and its capabilities can be accessed by selecting the FortiManager SOC/Log View, then Incidents & Events, and Reports icons (see Figure 7). The appliance can import syslog events from other devices, but its analyzing and reporting functionality is limited specifically to Fortinet products.

The Fortinet lab we accessed was not configured to provide any reportable details. However, the power of combining information from FortiGuard, FortiVPN, FortiNAC, and FortiAuthenticator cannot be dismissed. The integration of industrial protocols in the FortiGuard appliance provides the capability to generate reports involving these protocols (see Figure 8).

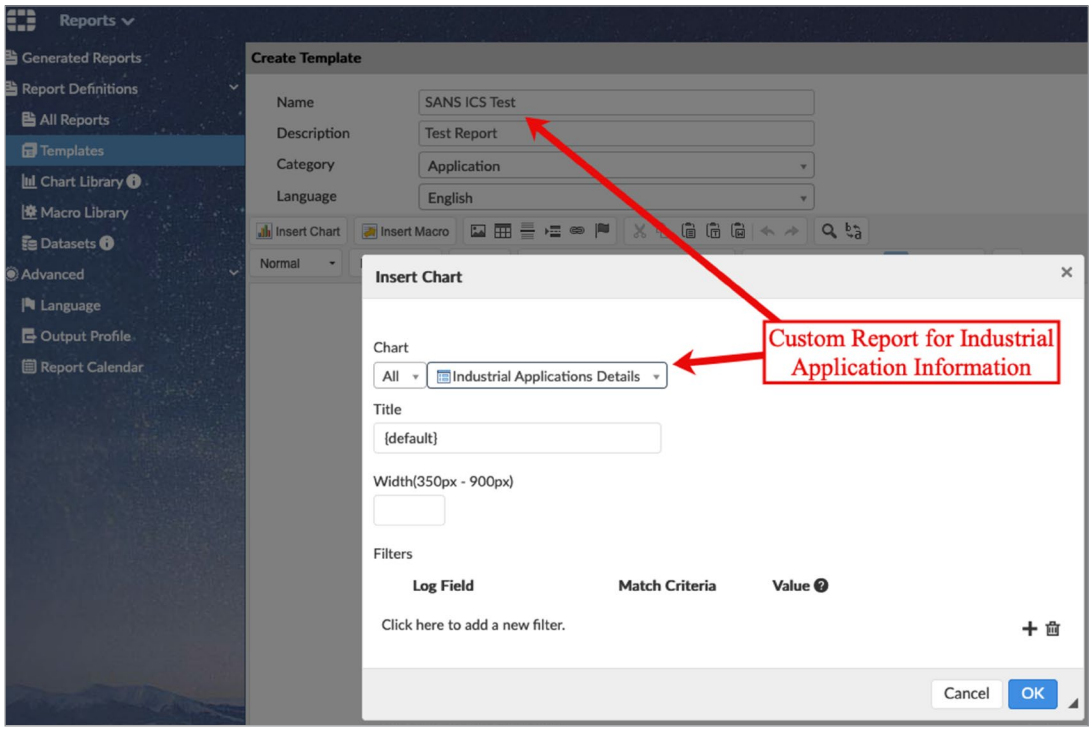

Figure 8. Generating Custom Reports in FortiAnalyzer

Understanding the common baseline of device communications and interactions gets an organization closer to generating a baseline of common behavior. This data is invaluable during event evaluations and incident response.

FortiSIEM is the primary central logging, correlation, and analysis portal of the Fortinet Security Fabric. This appliance receives logs from all configured OT devices, produces alerts on configured activity, and provides a portal for security operations center analysts. The aggregated data is correlated against MITRE ATT&CK® for ICS as well as threat feeds from third parties such as Dragos and Nozomi. Figure 9 shows the FortiSIEM portal interface.

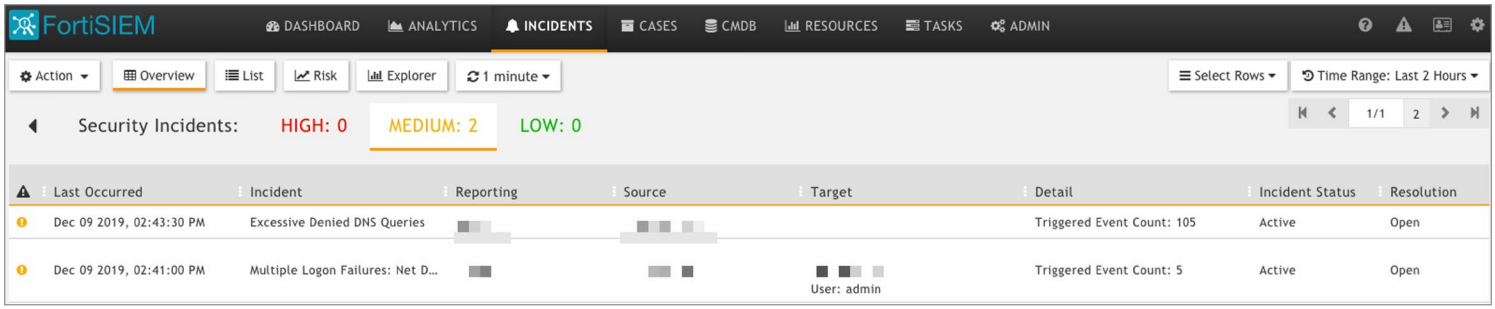

Figure 9. FortiSIEM Dashboard

The effectiveness of this interface in identifying events and managing workflow could not be determined without being deployed in an operational environment. Because the lab had limited implemented assets, the events stored in the FortiSIEM could not be analyzed. This situation limited the review of events, incidents, ticket analysis, and report generation. We attempted to create a new report related to industrial protocols such as Modbus and Profinet, but the report could not be generated without data from an active ICS network. Rules for default ports related to industrial protocols had not been configured in this FortiSIEM.

Asset Inventory

Asset inventory can be a challenge for many organizations. Collecting and maintaining this information is a huge drain on personnel. To help with hardware inventory, the Fortinet Security Fabric provides two capabilities that appear to help ease some of this effort. Hardware inventory can be accomplished through the integration of FortiNAC and FortiSIEM into the Fortinet Security Fabric. FortiNAC allows for the integration with an organization's networking devices, such as Cisco switches and routers. See Figure 10.

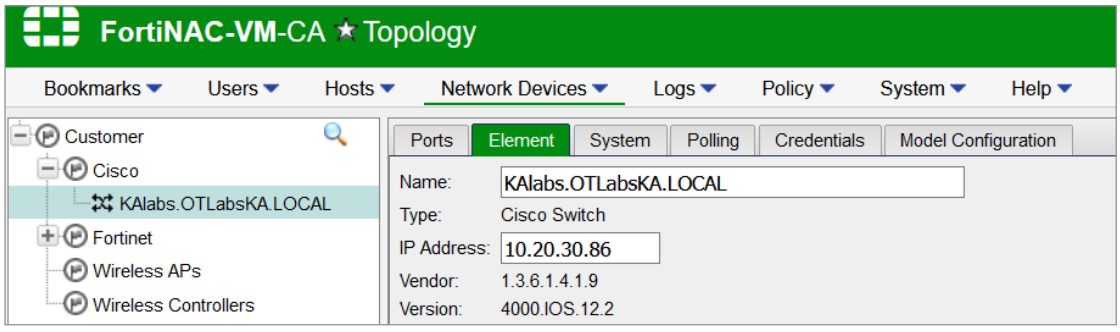

Figure 10. FortiNAC Integrated with Cisco Switch

This integration allows FortiNAC to observe and provide details about devices communicating across the ICS network. Figure 11 is an example of this information, which can be extracted in several formats including comma-separated values and Microsoft Excel. Periodic reports can be generated to gain an understanding of the assets communicating within the control network.

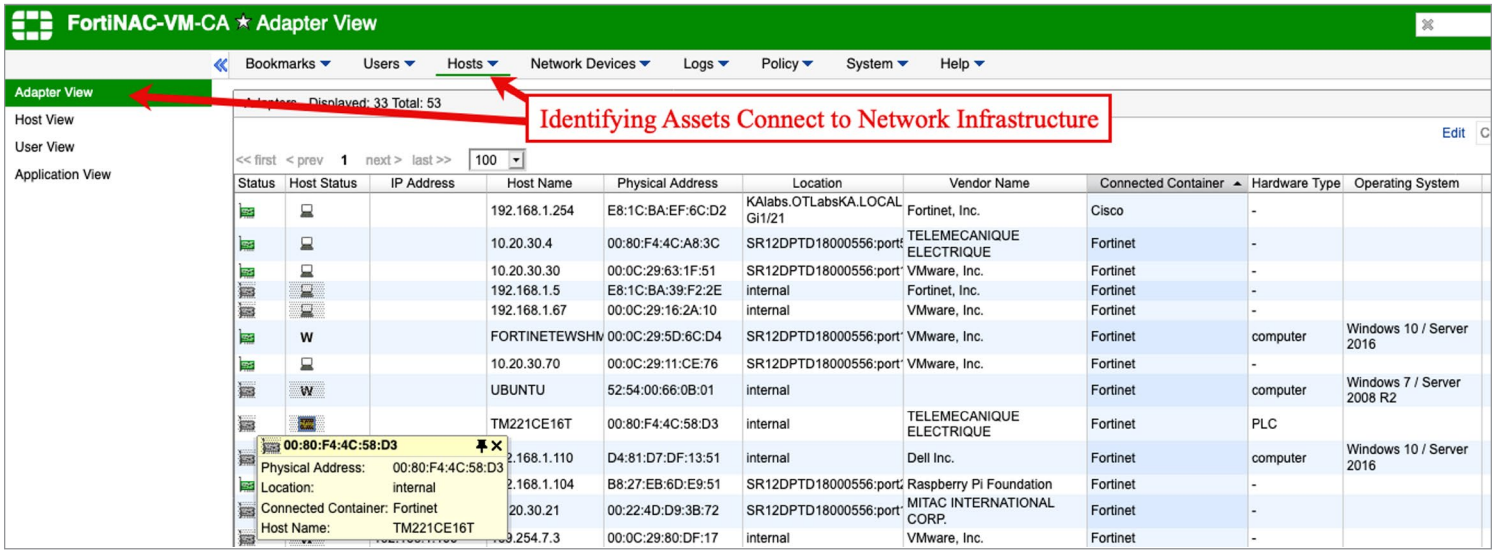

Figure 11. Asset Inventory Using FortiNAC

FortiSIEM includes an OT asset inventory capability that also maps to Purdue levels for reports and alerts as well as a configuration management database, shown in Figure 12, that tracks all assets logging in to the appliance.

The database is automatically updated and maintained with information from incoming events, allowing administrators to quickly understand these assets and where they are located and to generate reports for baselining normal activity. This information is extremely valuable for normal operations and critical during the investigation of security events and incident response.

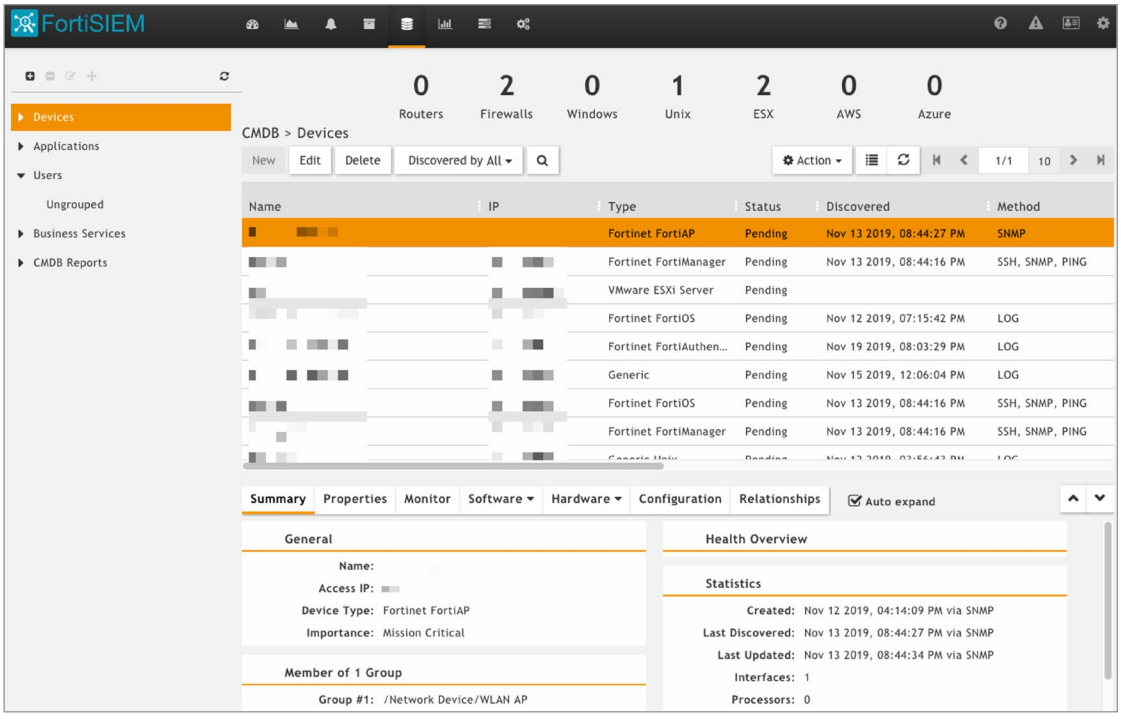

Figure 12. FortiSIEM's Configuration Management Database

In addition to hardware inventory, organizations need to do a software inventory. As a part of the Fortinet Security Fabric, software inventory can be accomplished through the deployment of FortiClients to servers and workstations with the control network. During this review, we were not able to review the effects that FortiClient has on server and workstation resources such as memory, CPU, and network usage. Therefore, organizations will want to review the effects of FortiClients with their vendors or integrators before deploying to an environment. Alternatively, deploying the FortiClient on engineer, operator, and programmer workstations may be easier. The cost to processing power on the system may be justified by the asset information provided through the FortiClient. This information includes software and hardware information about the workstation. Additionally, it provides valuable vulnerability information and connectivity with the FortiNAC device for additional administrative and security benefits.

Incident Response and Recovery

Incident response and recovery can be a confusing and stressful operation for any organization. Accurate information about system, network, and authentication events is critical during these periods. Correlating these events across the control network is equally important. Having a single management console that allows administrators to gather and analyze this information can be especially beneficial by reducing the steps to access the information.

The Fortinet Security Fabric lab provided for this analysis was not configured in a manner that provided actual data to understand its true value during an incident response effort. However, the integration of security controls, via FortiManager, and the data it correlates is promising and would be useful to analysts, incident responders, and managers. Once configured and integrated correctly, the information provided by the Fortinet Security Fabric technologies has the potential to significantly reduce the gaps between compromise and identification. These security controls will also provide valuable correlated information that will assist with the containment of a security incident and eventual recovery of the ICS environment.

The best path forward for any team to address security events within the ICS network is to conduct incident response tabletop scenarios. The Fortinet Security Fabric assets will provide the team with details about the control network to assist with scenario generation, data collection, and impact analysis. Teams with this type of data are more prepared than those that must manually acquire and correlate device logs.

Summary

The NIST CSF is designed to assist critical infrastructure operators in the development and implementation of a security program specifically for ICS environments. There is no reason that teams managing noncritical infrastructure cannot use the NIST CSF in the same manner. This approach ensures that the processes at the center of the ICS network are driving the requirements while the IT and ICS team members are being educated about these requirements. This communication and agreement about priorities are the keys to success.

New security policies are going to mean a change of procedures and, potentially, technologies. Because processes do not change often, the use of a tightly integrated, homogeneous security control environment makes a lot of sense. A tool such as FortiManager that so nearly approximates a single pane of glass for managing and monitoring many security controls can go a long way toward reducing time and effort. The overhead of account management provided by FortiAuthenticator should also reduce confusion and mistakes, compared with managing administrative and user access to each resource individually.

It is difficult to judge how each Fortinet product will function separately within an ICS network without actual data. But the demonstration the SANS review team had of the basic capabilities of the Fortinet Security Fabric did help us understand the integration's potential. The capabilities of FortiGate to monitor and manage, even at a high level, specific industrial protocols will help ICS teams implement effective enforcement boundaries between each Purdue level. The integration of FortiGate with FortiAuthenticator and the control network's Active Directory will provide the benefits of access control to the Fortinet Security Fabric and other ICS technologies. The FortiAnalyzer and FortiSIEM products will provide ICS teams with correlated system and network events generated within the ICS environment, which, in turn, will assist them with identifying and addressing security events and improve the response to security incidents. FortiNAC and FortiClient will help improve hardware and software asset management, a topic a majority of organizations struggle with the most.

The capabilities the Fortinet Security Fabric brings to the ICS networks and their supporting teams are impressive. Funding and deploying all of these technologies at the same time is unrealistic for most organizations. But with a planned security program, based on the security requirements directly associated with the organization's process, migration to a Fortinet Security Fabric-managed ICS infrastructure could be possible and help organizations protect these critical networks and technologies. For new processes, determine the information security requirements and work them into the factory and site acceptance testing (FAT and SAT) phases of the process's life cycle. This action will help identify and justify the deployment of these security controls and ensure that they have a positive impact on the process. Organizations securing active processes will need to use testing and cutover times to implement these products; this will provide ICS teams the necessary time to test and validate how the process's reliability and availability are affected by the implementation of the new technologies. Planned properly, these technologies should improve the security and functionality of the processes in which they are deployed.

Sponsor

SANS would like to thank this paper's sponsor:

FORTINET®