WHITE PAPER

Advanced Threat Protection for Industrial Control Systems and Operational Technology

FortiGuard Industrial Security Service Secures ICS and OT With Application Control and Virtual Patching

Executive Summary

As digital innovation initiatives dissolve the operational technology (OT) network boundaries, from IT networks (also known as the "air gap"), OT networks have become a target of a growing number of attacks. Application control and intrusion prevention (IPS) technologies that are integrated into every FortiGate Next-Generation Firewall (NGFW) can uniquely identify traffic from 55 different OT applications and protocols with more than 1,850 unique application control signatures to protect against advanced threats. In addition, IPS signatures can also virtually patch OT applications and protocols.

FortiGuard Labs leverages OT-specific knowledge and the analysis of billions of security events per day to generate threat intelligence and develop application control and IPS signatures. This combination of application control and OT-specific threat intelligence enables OT operators to define and enforce robust threat protection through application-specific firewall policies and virtual patching within their OT environments without causing any performance impacts.

Nine out of ten OT organizations experienced at least one system intrusion in the past year. Malware and phishing are the most common intrusions.[1]

Evolving Threat Landscape Compels Shift in OT Protection

Traditionally, the threat model of OT network security plans relied upon a physical disconnect between OT and IT networks. But increasingly, this model is fading away. Although digital transformation is a clear trend with business benefits, the process brings with it a number of security challenges.

OT operators now need visibility and control over how OT applications and protocols communicate with each other over the network. FortiGate NGFWs include built-in application control and IPS signatures that enable enforcement of application-specific firewall policies for OT network traffic. They also support virtual patching of any legacy devices that have been running in the network with potential security vulnerabilities—without the need for security fixes or software patches.

Why OT Needs Application Control

OT systems such as programmable logic controllers (PLCs), remote terminal units (RTUs), and human machine interfaces (HMIs) run specific protocols and associated applications that are not secure by design. Rather than using a zero-trust approach, most OT systems follow inherent trust and do not have any authentication and authorization built into their command-and-control frameworks. Because of this issue, ICS environments require a mechanism to limit inappropriate or risky operations from being blindly executed on target systems.

With application control configured in the ICS network, security teams can manage which specific operations are and are not allowed. This reduces the risk of ICS process disruptions from either a legitimate user making a mistake or a malicious threat actor launching an attack. A FortiGate NGFW provides the necessary level of protection by monitoring and filtering all traffic entering and exiting the ICS network.

Why OT Needs an Intrusion Prevention System (IPS)

Maintaining uptime of OT systems is so important to plant operations that most OT operators are willing to defer applying patches to critical ICS elements (e.g., PLCs, RTUs, HMIs). However, leaving these systems unpatched when known vulnerabilities exist can lead to an attacker targeting vulnerabilities that could compromise their safety, availability, and reliability. It's also common for manufacturers to stop providing security fixes on legacy OT systems once they are declared obsolete. Any unpatched legacy OT system creates a major security gap in the broader OT environment. Organizations need a compensating control to mitigate the risks of any known vulnerabilities in their OT environment.

An NGFW armed with OT-specific IPS signatures can provide a virtual patch to the environment so that unpatched systems can continue to operate within the OT network with minimized risk of exploitation. IPS signatures offer a virtual shield over the network. A security team can wait until the next scheduled outage to apply an underlying patch or continue to operate the vulnerable OT systems with a virtual patch in place in case no security fix is available for it.

The FortiGuard Industrial Security Service Provides Application Control and IPS Signatures for OT

The differences between IT and OT environments mean that industrial control systems often face different threats and require security monitoring tailored to their unique threat landscape. Years of experience securing OT environments and membership in the largest OT-specific partner ecosystem give Fortinet a deep understanding of these kinds of threats. FortiGuard Labs has developed OT-specific threat intelligence based on analysis of over 100 billion security events per day.[2]

The FortiGuard Industrial Security Service for FortiGate combines application control and IPS signatures that are developed specifically for OT. It provides the capability to detect and protect against network-level threats, while enabling extensive visibility into industrial applications.

The FortiGate IPS engine can identify over 55 different OT-specific network protocols (e.g., Modbus TCP, BACnet, OPC) with more than 1,850 unique application control signatures within these protocols for specific security policy rules that can be applied to the various OT systems communicating in the network. Combining these capabilities with the OT-specific threat intelligence from FortiGuard Labs enables OT operators to identify and monitor the types of traffic flowing in their networks and apply granular control over the usage of protocol functions and values restricting data flows within their environments. (Figure 1 shows the list of currently supported ICS/OT protocols.)

ADDP	FactoryTalk (View SE)	MOXA Modbus RTU →
Allen-Bradley PCCC	FL-net	MQTT
BACnet	GE SRTP (GE Fanuc)	MTConnect
CC-Link	HART-IP	Net C/X (Digi RealPort)
CIP	HL7	Niagara Fox
CN/IP (EIA/CEA-852)	IEC 60870-5-104 (IEC 104) →	OCPP
CoAP	IEC 60870-6 (TASE.2/ICCP)	OPC Classic (DA, HDA, AE)
DICOM	IEC 61850 MMS	OPC UA
DNP3 →	IEC 61850 R-GOOSE	IEC 62056 (DLMS/COSEM)
RealPort DNP3	IEC 61850 R-SV	OpenADR
ECHONET Lite	IEEE 1278.2 Distributed Interactive Simulation	OSIsoft PI System
ELCOM 90	IEEE C37.118 Synchrophasor	PROFINET
Emerson DeltaV	KNXnet/IP (EIBnet/IP)	RTPS
Ether-S-Bus	LonTalk/EIA-709.1	SafetyNet p
EtherCAT Automation Protocol (EAP)	Mitsubishi MELSEC	Siemens S7, S7Plus, LOGO
Ethernet Global Data (GE EGD)	Modbus TCP →	STANAG 4406
Ethernet Powerlink	Modbus Unity	STANAG 5066
EtherNet/IP	MOXA	TriStation
		Vedeer-Root

→ - Additional parameters supported for the signatures in the GUI (requires FortiOS v6.4 and above)

Figure 1: List of currently supported ICS/OT protocols with application control signatures.

Application Control and IPS in ICS Environments

Digital transformation initiatives take advantage of the productivity and efficiency gains made available by connecting OT environments so that industrial data can be analyzed to help minimize downtime and lost production. As IT and OT networks become increasingly connected, securing OT environments requires network segmentation.[3] Figure 2 (on the next page) shows a high-level deployment architecture with FortiGate NGFWs in a connected IT enterprise and OT infrastructure. The IT and OT networks are segmented into several zones using the FortiGate NGFWs.

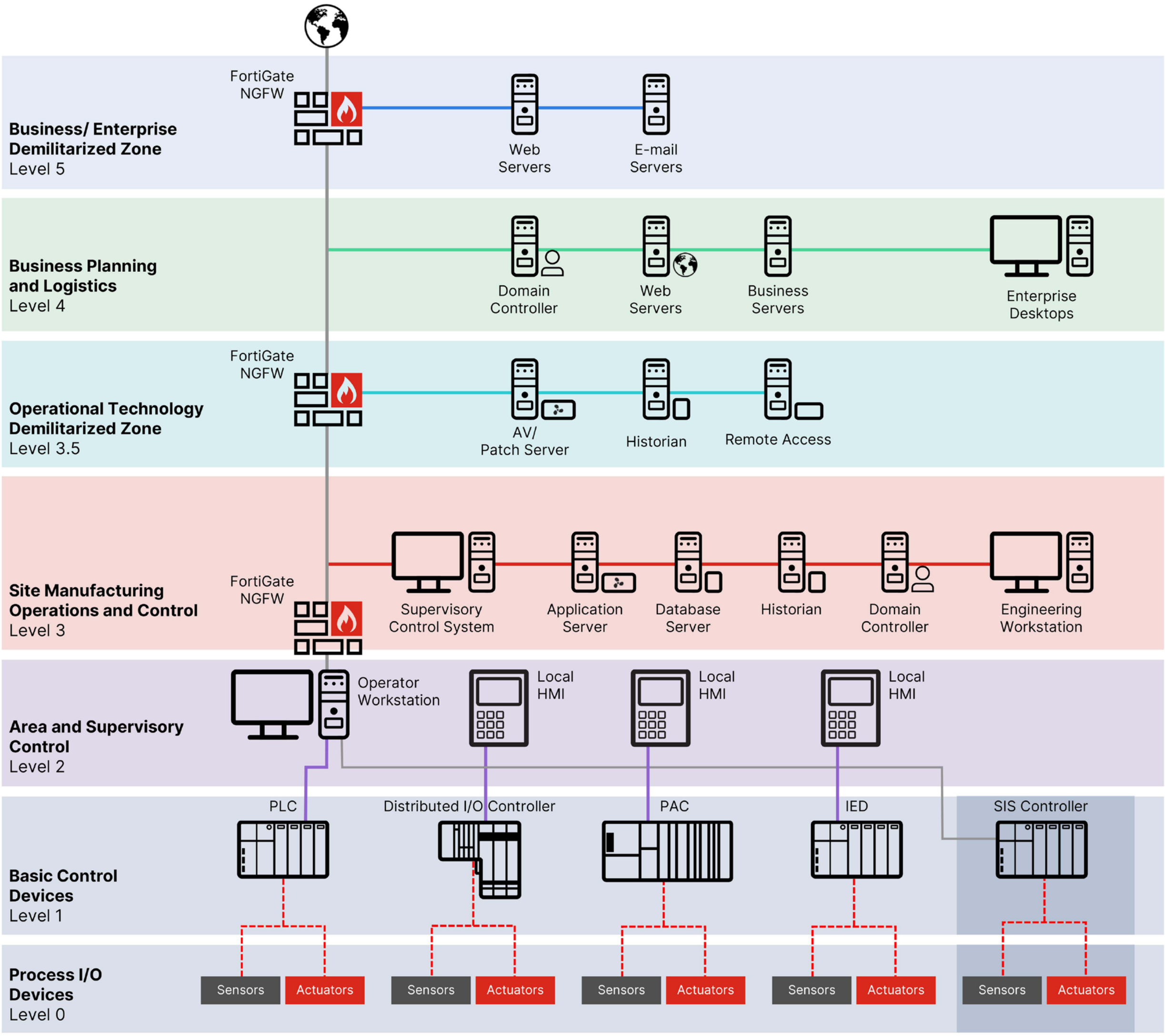


Figure 2: Interconnected IT enterprise and OT networks secured using FortiGate NGFWs.

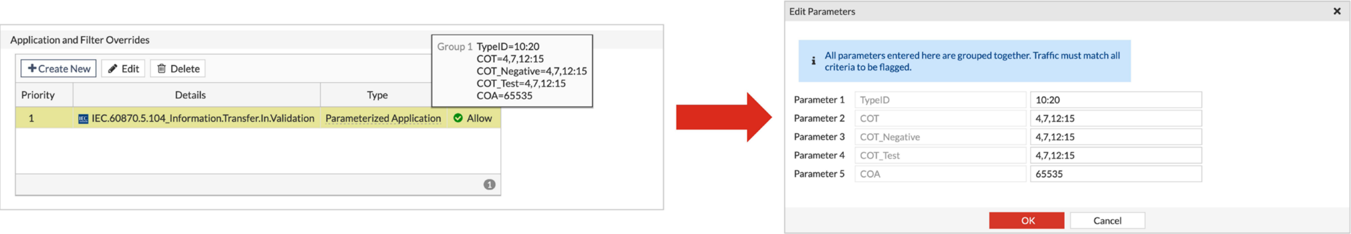
Communications between different zones within the OT network and to the organization's intranet, internet, and remote sites are monitored and secured by a FortiGate NGFW with virtual patching. Demilitarized zone (DMZ) networks provide secure connectivity to the services from lower to higher networks, including the internet. As part of its built-in IPS capabilities, the FortiGate NGFW comes with web filtering and antispam features for the internet-facing DMZ networks.

How application control signatures can reduce the attack surface for ICS and OT

Application control signatures perform deep packet inspection (DPI) for the protocol payload and offer the ability to identify protocol functions and values. The signatures can be configured within the FortiGate firewall policies to allow and deny certain protocol parameters traversing over a network communication channel. Some application control signatures can support matching multiple parameters within the FortiGate policy configuration, whereby a granular security policy can be defined to regulate and control network communication within the ICS network.[4]

Versions 6.4 and later of the FortiOS network operating system for FortiGate NGFWs offer GUI-based policy configuration to define multiple parameters for certain application control signatures (e.g., definition of values or value range for specific protocol functions in combination with AND/OR logic operations). Figure 3 (on the next 2 pages) shows matching multiple parameters within an application control signature with AND/OR logic operations.

Example 1: IEC 60870-5-104



Application and Filter Overrides

Priority	Details	Type	
1	IEC.60870.5.104_Information.Transfer.In.Validation	Parameterized Application	Allow

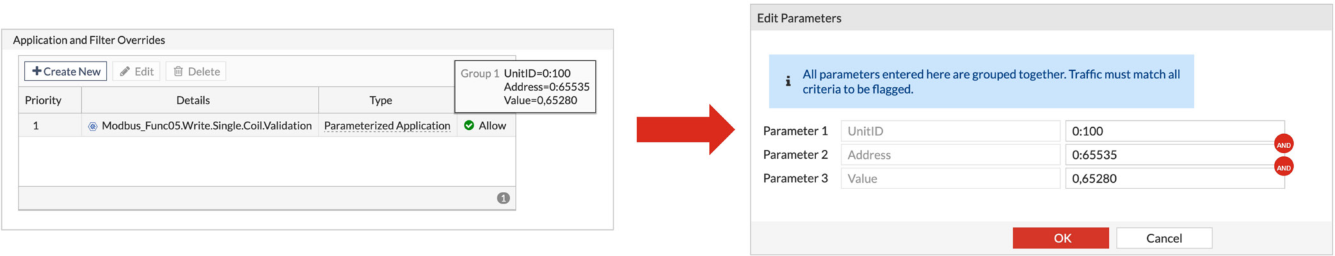
Group 1 TypeID=10:20
COT=4,7,12:15
COT_Negative=4,7,12:15
COT_Test=4,7,12:15
COA=65535

All parameters entered here are grouped together. Traffic must match all criteria to be flagged.

Parameter 1	TypeID	10:20
Parameter 2	COT	4,7,12:15
Parameter 3	COT_Negative	4,7,12:15
Parameter 4	COT_Test	4,7,12:15
Parameter 5	COA	65535

Example security policy configuration for IEC 60870-5-104 Application Control signature with Multiple Parameters

Example 2: And / Or logic operations



Application and Filter Overrides

Priority	Details	Type	
1	Modbus_Func05.Write.Single.Coil.Validation	Parameterized Application	Allow

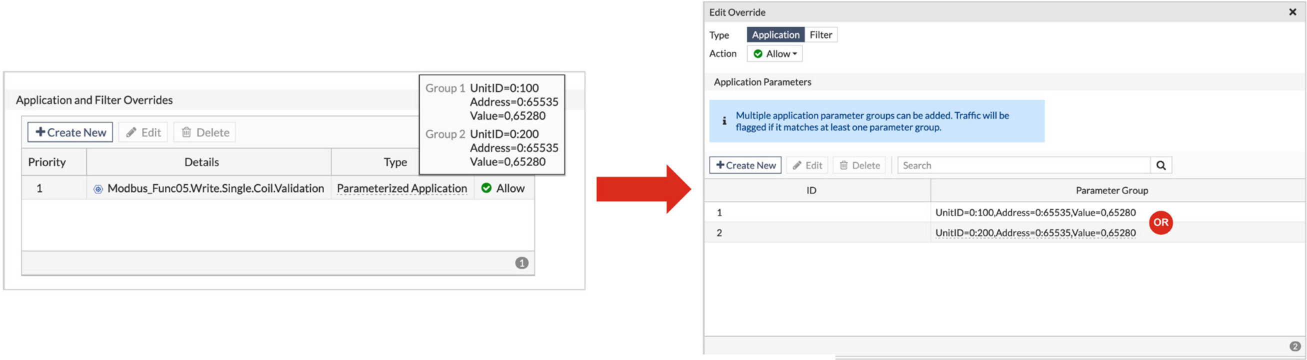
Group 1 UnitID=0:100
Address=0:65535
Value=0,65280

All parameters entered here are grouped together. Traffic must match all criteria to be flagged.

Parameter 1	UnitID	0:100
Parameter 2	Address	0:65535
Parameter 3	Value	0,65280

Example AND operation

Note: To be read as Parameter 1 AND Parameter 2 AND Parameter 3



Application and Filter Overrides

Priority	Details	Type	
1	Modbus_Func05.Write.Single.Coil.Validation	Parameterized Application	Allow

Group 1 UnitID=0:100
Address=0:65535
Value=0,65280
Group 2 UnitID=0:200
Address=0:65535
Value=0,65280

Application Parameters

Multiple application parameter groups can be added. Traffic will be flagged if it matches at least one parameter group.

ID	Parameter Group
1	UnitID=0:100,Address=0:65535,Value=0,65280
2	UnitID=0:200,Address=0:65535,Value=0,65280

Example OR operation

Note: To be read as Group1 OR Group 2 or ID 1 OR ID 2

Figure 3: Matching multiple parameters within an application control signature with AND/OR logic operations.

Figure 4 (below) provides an overview of how network traffic flows through the FortiGate IPS engine when application control signatures are configured for a specific protocol.

FortiGate NGFW With Application Control (AppCtrl)

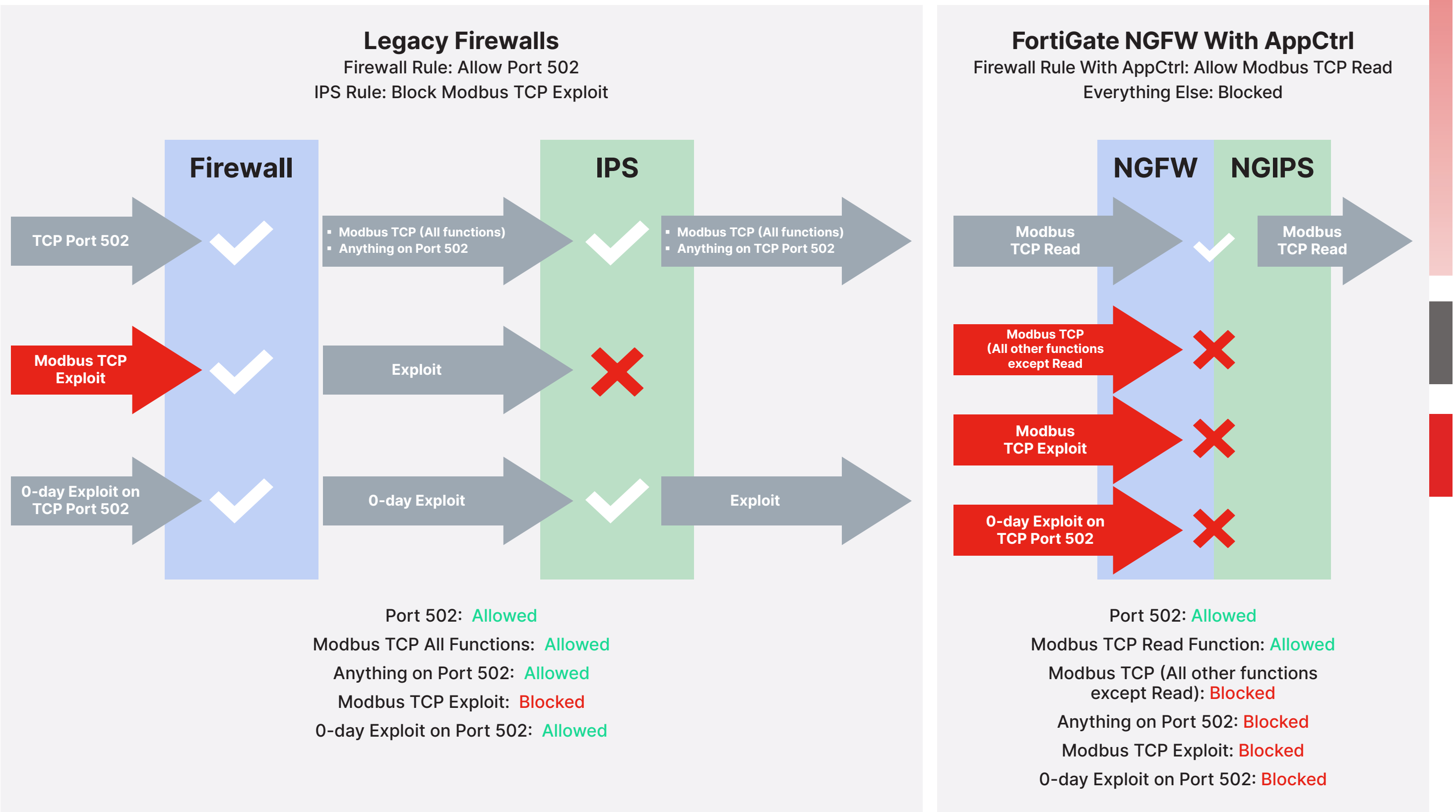

Legacy Firewalls
Firewall Rule: Allow Port 502
IPS Rule: Block Modbus TCP Exploit
Firewall
IPS
TCP Port 502
Modbus TCP (All functions)
Anything on Port 502
Modbus TCP (All functions)
Anything on TCP Port 502
Modbus TCP Exploit
Exploit
0-day Exploit on TCP Port 502
0-day Exploit
Exploit
Port 502: Allowed
Modbus TCP All Functions: Allowed
Anything on Port 502: Allowed
Modbus TCP Exploit: Blocked
0-day Exploit on Port 502: Allowed
FortiGate NGFW With AppCtrl
Firewall Rule With AppCtrl: Allow Modbus TCP Read
Everything Else: Blocked
NGFW
NGIPS
Modbus TCP Read
Modbus TCP Read
Modbus TCP (All other functions except Read)
Modbus TCP Exploit
0-day Exploit on TCP Port 502
Port 502: Allowed
Modbus TCP Read Function: Allowed
Modbus TCP (All other functions except Read): Blocked
Anything on Port 502: Blocked
Modbus TCP Exploit: Blocked
0-day Exploit on Port 502: Blocked

Figure 4: Network traffic flows through a FortiGate NGFW's IPS engine.

How IPS signatures can offer virtual patching for ICS and OT

Threat actors often probe ICS platforms in search of vulnerabilities. Should a vulnerability be discovered, an exploit code is created that leverages the vulnerability to stage an attack. If the exploit code traverses on to the target platform and executes successfully, it can compromise safety, availability, integrity, and confidentiality. IPS signatures are essentially predefined patterns that, when configured within the IPS policy, detect exploit codes in a network communication stream and block them from traversing on to the target platform. This ultimately prevents exploit code execution.

Applying security fixes or software patches in an ICS/OT environment can have many challenges, such as:

- Very slow patch cycles—there is no "patch Tuesday" concept in ICS/OT
- Vendor delays with releasing a patch—it requires a long process (development, testing, validation, and release)
- Customers cannot afford downtime—impossible to shut down the plant operations or issue system downtime
- Expansive ICS infrastructure—deployment of necessary patches could take years
- Complexities of the ICS/OT environment—multiple integrations and dependencies
- System or platform obsolescence—deploying patches could break the system, disrupt integration with other key OT components, or void support/warranty contracts

IPS signatures can protect legacy ICS platforms that do not have a software patch available from malicious exploits (see Figure 5). The FortiGuard Labs Industrial Security Service currently covers more than 495 ICS and OT specific IPS signatures for known vulnerabilities. Likewise, through its extensive alliance and partnership ecosystem, Fortinet works closely with industrial automation and control system vendors to develop IPS signatures for their ICS platforms that may have known vulnerabilities.

Custom signatures and the session helper capability within FortiOS

FortiOS also supports custom application control signatures. If a signature is not already part of the IPS database supplied by FortiGuard Labs, end-users with sufficient knowledge of FortiGuard IPS technology can create a custom application control signature and deploy it on the FortiGate NGFW.[5] Detailed instructions for creating custom application control signatures can be found in the *Custom IPS and Application Control Signature—Syntax Guide*.[6]

Some complex and legacy ICS/OT protocols may have special requirements due to the way the protocol is designed or functions. In such cases, FortiOS uses a session helper to process any network communication sessions that have special requirements. Session helpers function like proxies by getting information from the session and performing required support functions. For example, legacy Open Platform Communications (OPC) operations such as data access (DA), historical data access (HDA), and alarms and events (AE) work on dynamic network ports. These ports can pose challenges when defining security policies on a network firewall because they can vary from one session to the next. However, by using Fortinet's built-in session helper capabilities, end-users can efficiently manage dynamic network port allocation for the operation and secure it.[7]

Similarly, if a vulnerable ICS platform cannot be patched on time, FortiGuard Labs can develop an IPS signature that can be deployed on a FortiGate NGFW via virtual patching to secure the vulnerable platform from cyber threats in the interim. As an example, an IPS signature was developed for the Schneider Electric Triconex platform, which is vulnerable to Triton/Trisis malware.[8,9]

Virtual Patching or Vulnerability Shielding— acts as a **compensating security control against threats that have the potential to exploit known or unknown vulnerabilities.** Virtual patching works by implementing layers of security controls that **intercept and prevent an exploit from compromising the vulnerable assets** connected on the network(s).

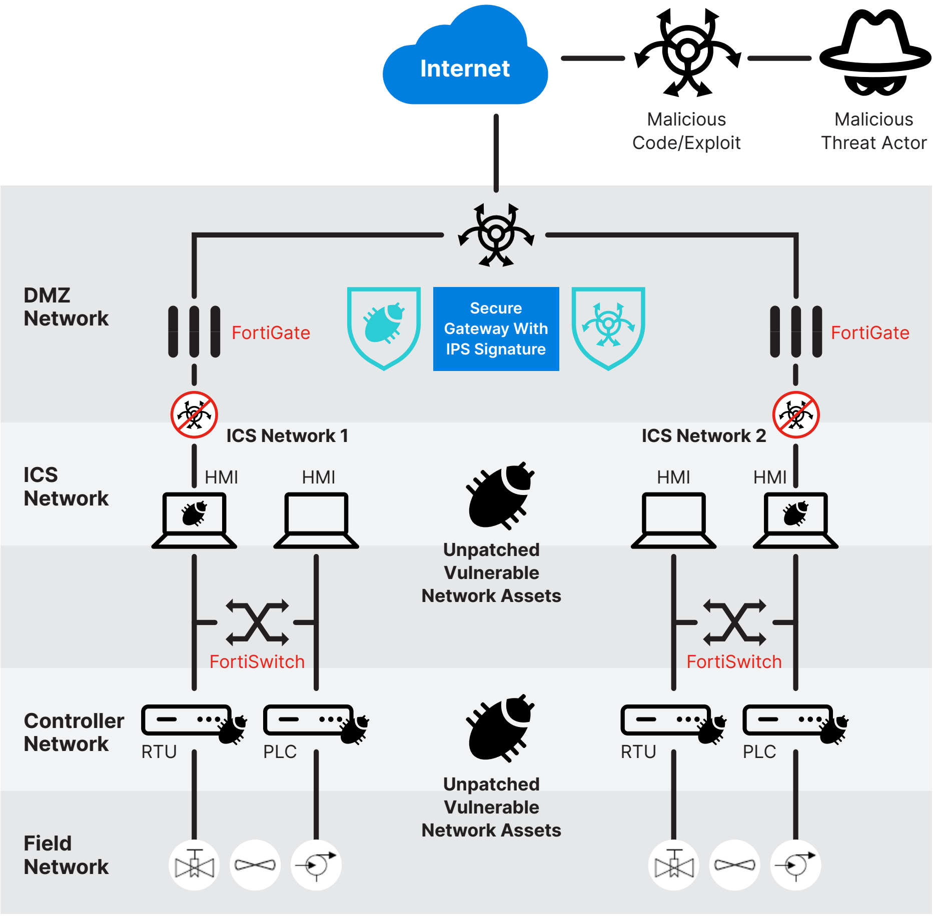


Figure 5: Virtual Patching or Vulnerability Shielding within an ICS environment.

An ICS Threat Mitigation Scenario

The ability to identify and filter network communications at the application level enables an organization to enforce granular firewall policies. Asset owners can protect against sophisticated threats without negatively impacting their operations or the productivity of an OT environment.

For example, as part of ICS operations, a data historian may need read access to several PLCs in order to collect and store operational data. However, the underlying ICS protocol that is used to make these requests for data acquisition could potentially be used by a threat actor to send malicious commands to the PLC. Because a network connection must be present between the data historian and the PLC to enable read access of data, simply blocking all traffic between the two systems is not a viable solution. However, filtering the transmissions between the two systems to differentiate between legitimate reads and malicious commands would require an understanding of the specific commands included in the underlying ICS protocol.

Application control can provide the appropriate level of filtering. A FortiGate NGFW can be configured to permit the data historian restricted access to the PLC. If a malicious threat actor compromises the data historian's access and attempts to send a command to the PLC, this malicious request would be identified and blocked by the FortiGate NGFW. The NGFW would then automatically generate an alert and transmit it via the logging mechanism to the security operations center (SOC), which could investigate the incident and take steps to enhance the security defenses if necessary.

FortiGate virtual patching capabilities can also protect vulnerable OT systems from exploitation. FortiGate NGFWs use the FortiGuard Industrial Security Service to receive updated signatures, even in isolated and air-gapped network environments. FortiGate can then detect and protect against attempted exploits of known OT vulnerabilities.

Conclusion

As the OT threat landscape expands and evolves, OT operators need granular visibility into the types of network traffic reaching their ICS. Application control and IPS signature capabilities are built into all FortiGate NGFWs. Adding the FortiGuard Labs Industrial Security Service further extends those capabilities to OT environments.

Protecting OT systems requires OT-specific security solutions. Network segmentation and microsegmentation, coupled with the advanced threat protection capabilities of FortiGate NGFWs, reduce an OT network's exposure to cyber threats while centralizing visibility and management of an organization's security architecture.

[1] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[2] "FortiGuard Security Services," Fortinet, November 6, 2021.

[3] "Securing OT Networks With Microsegmentation," Fortinet, August 27, 2021.

[4] "Matching multiple parameters on application control signatures," Fortinet Document Library, accessed January 31, 2022.

[5] "Creating IPS and application control signatures," Fortinet Document Library, accessed January 31, 2022.

[6] "Custom IPS and Application Control Signature—Syntax Guide," Fortinet, February 25, 2020.

[7] "Securing Open Platform Communications in OT Environments with FortiGate Next-generation Firewalls," Fortinet, July 16, 2021.

[8] "Triton.Malware.Backdoor," FortiGuard Labs, updated April 26, 2021.

[9] Kelly Jackson Higgins, "Triton/Trisis Attacks Another Victim," Dark Reading, April 11, 2019.

www.fortinet.com

April 15, 2022 11:23 PM

1430569-A-0-EN