DO NOT REPRINT
© FORTINET



OT Security Study Guide

for FortiOS 7.2

FORTINET®
Training Institute

DO NOT REPRINT
© FORTINET

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

11/15/2022

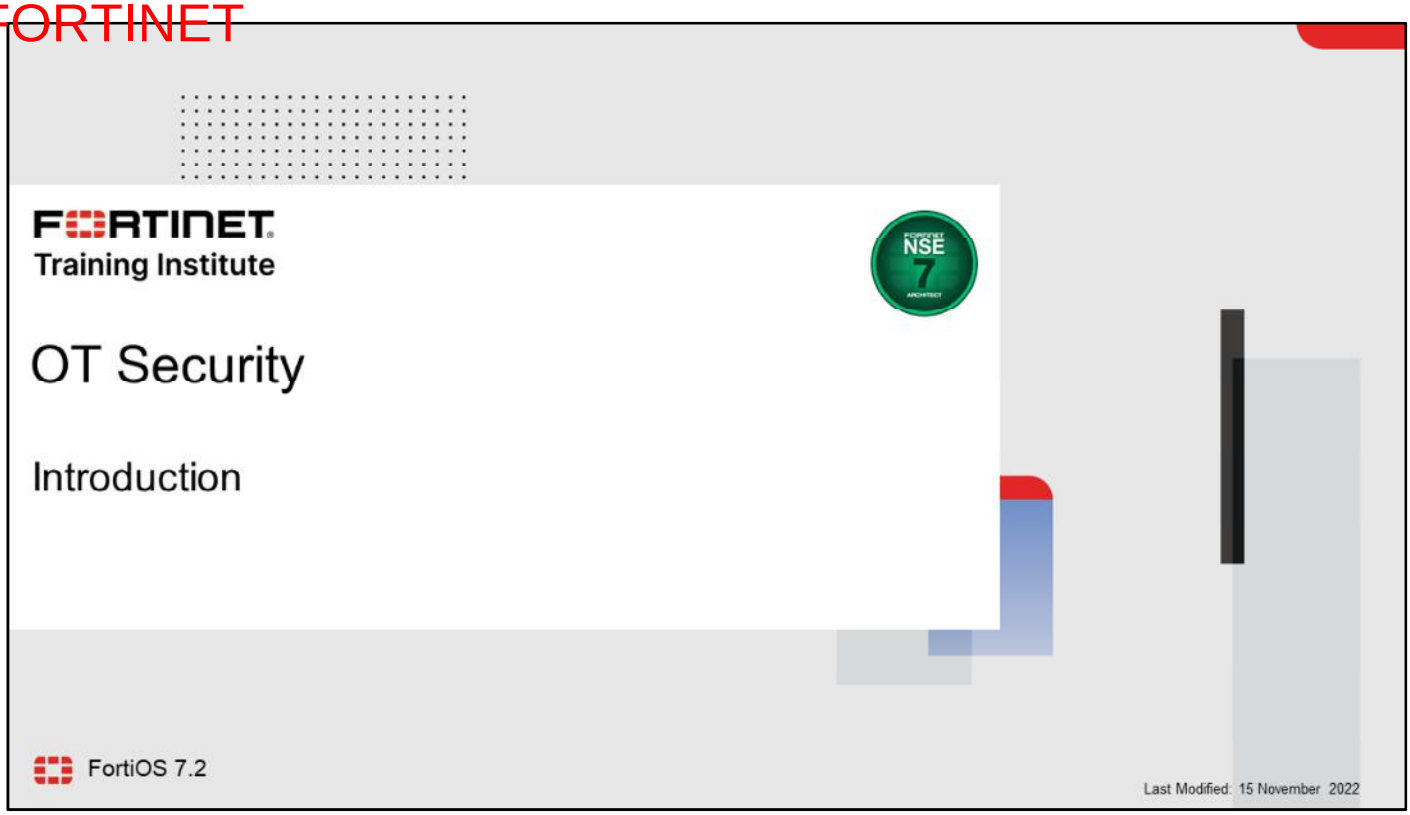
DO NOT REPRINT
© FORTINET

Brave-Dumps.com

TABLE OF CONTENTS

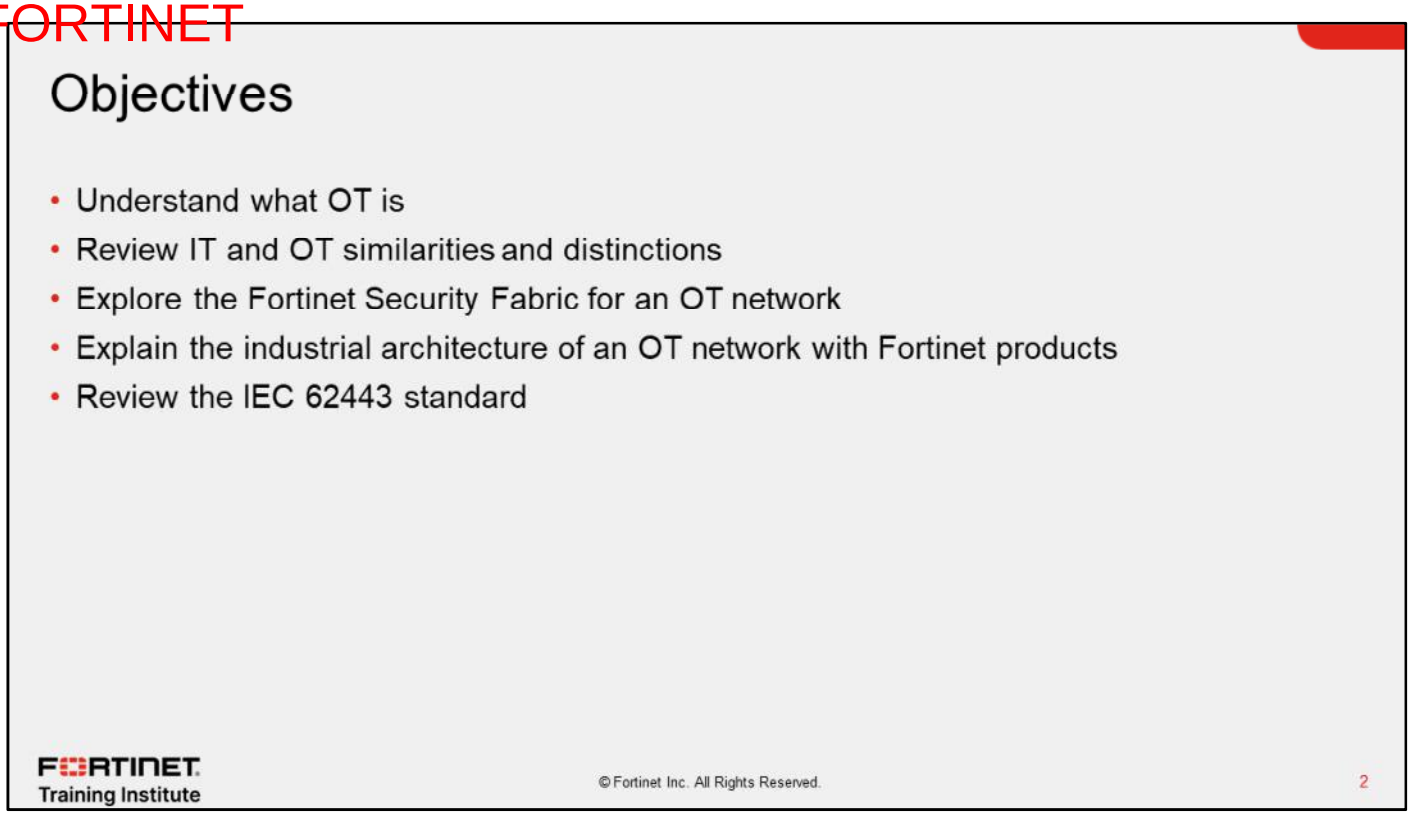
01 Introduction **4**
02 Asset Management **30**
03 Access Control **91**
04 Segmentation **128**
05 Protection **167**
06 Logging and Monitoring **205**
07 Risk Assessment **254**
Solution Slides **287**

DO NOT REPRINT
© FORTINET



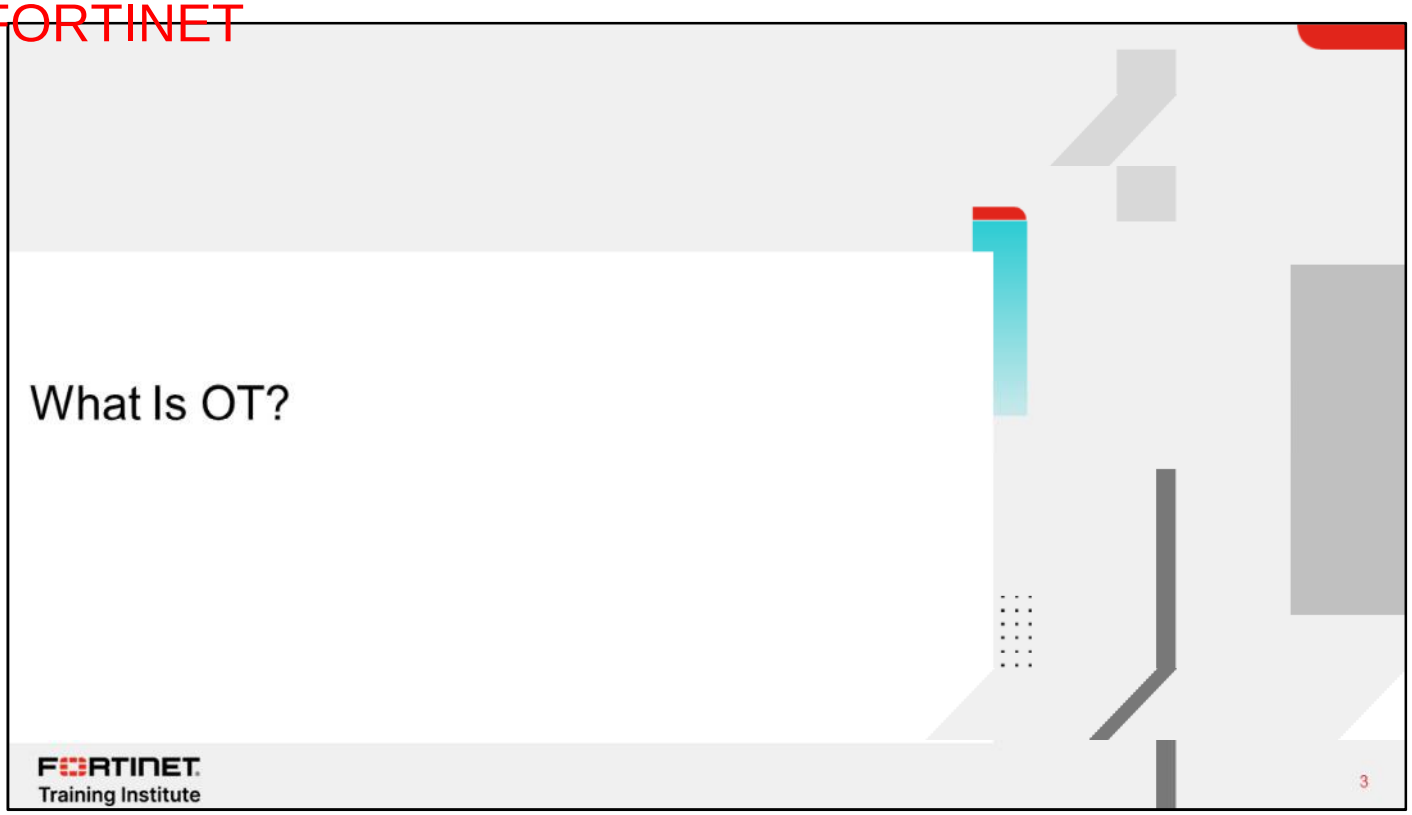
In this lesson, you will learn about operational technology (OT).

DO NOT REPRINT
© FORTINET



After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn what OT is.

DO NOT REPRINT
© FORTINET

What Is OT?

- OT is the use of hardware and software to monitor and control physical processes, devices, and infrastructure



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

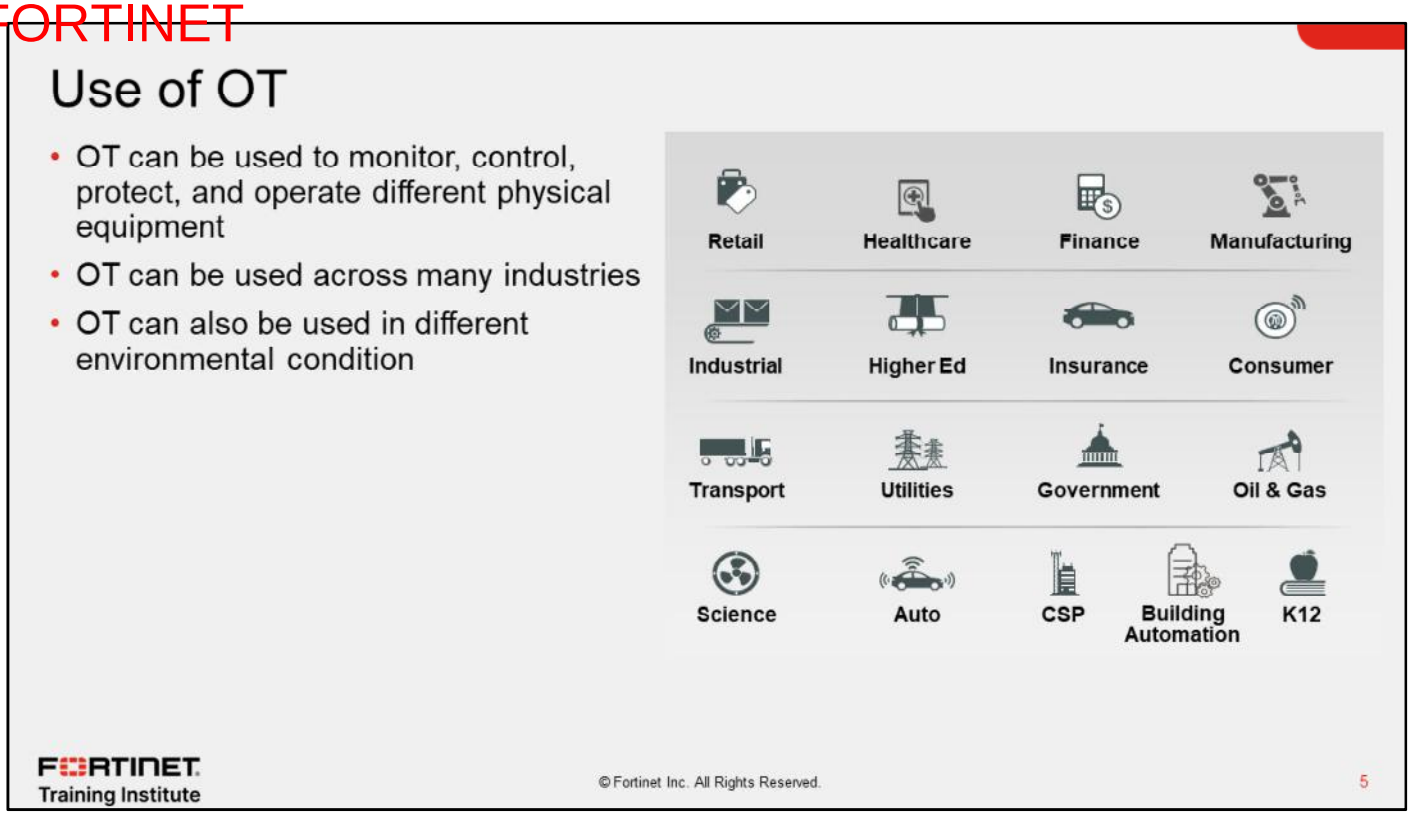
4

OT is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.

OT security can be defined as practices and technology used to protect people, assets, and information. OT security can also be used to initiate state changes to enterprise OT systems.

For example, a power utility uses OT to reduce costs and improve operating efficiency, monitoring, and control of power generation and distribution.

DO NOT REPRINT
© FORTINET

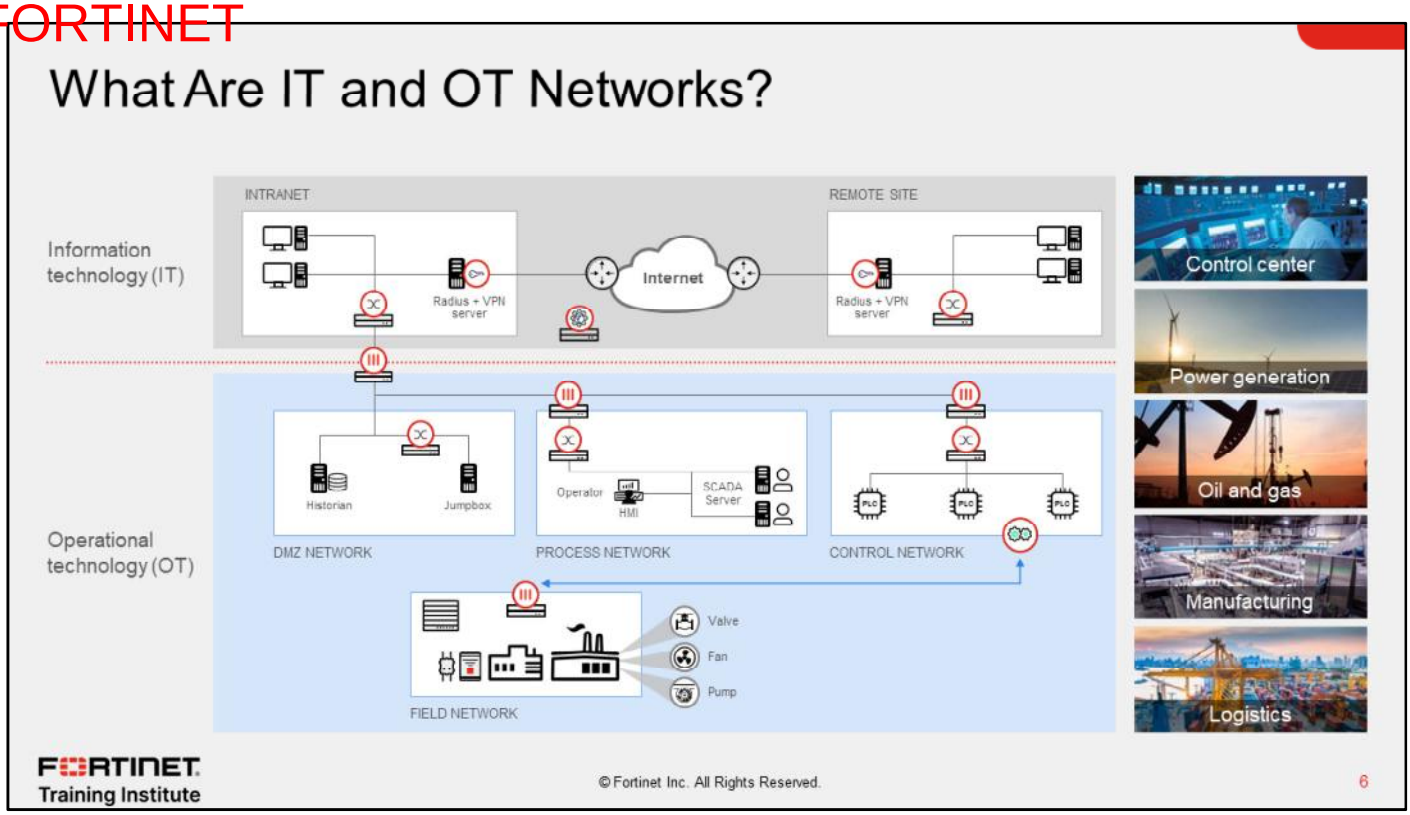


OT is used to monitor, control, protect, and operate different physical equipment.

OT is unique because it can be found across many industries, such as manufacturing, automotive, medical systems, military systems, power, refineries, pipelines, chemicals, water, and more.

OT can also be found operating in all types of environmental conditions, including the most harsh.

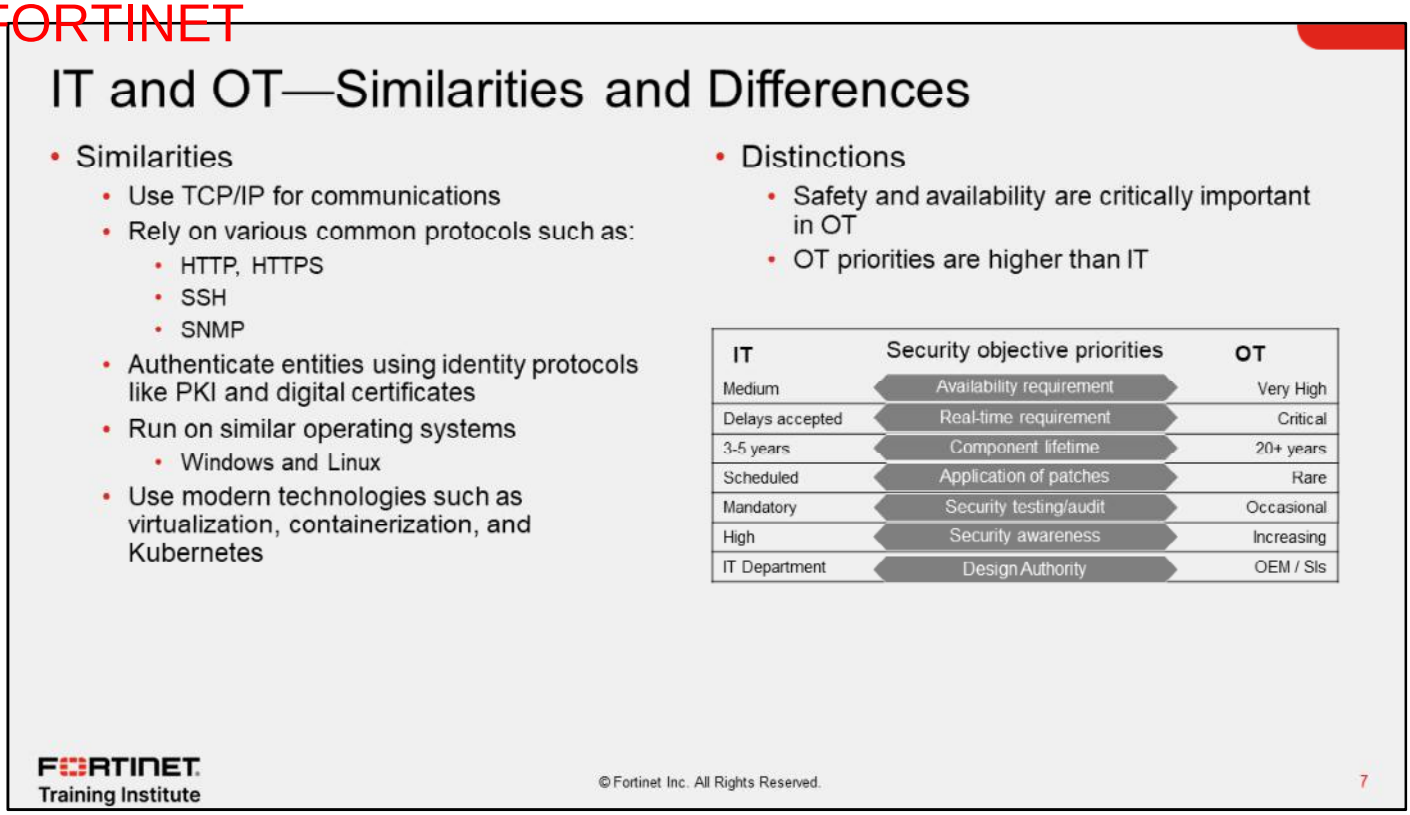
DO NOT REPRINT
© FORTINET



The slide shows a high-level enterprise view of an industrial plant. It could be a grid control center, a wind farm, an oil drilling rig, a food and beverage plant, or a maritime port. Fundamentally, all of these kinds of operational networks tend to have similar technologies and structures.

The two sections represent a simplified model of the IT side of a business and the OT side of a business. Each network consists of various subnetworks. In the IT section, you can see the intranet and remote connectivity to a remote site or branch. Below that, you see a DMZ network, segmenting the OT aspects from the IT aspects, the process network, the control network, and the field network.

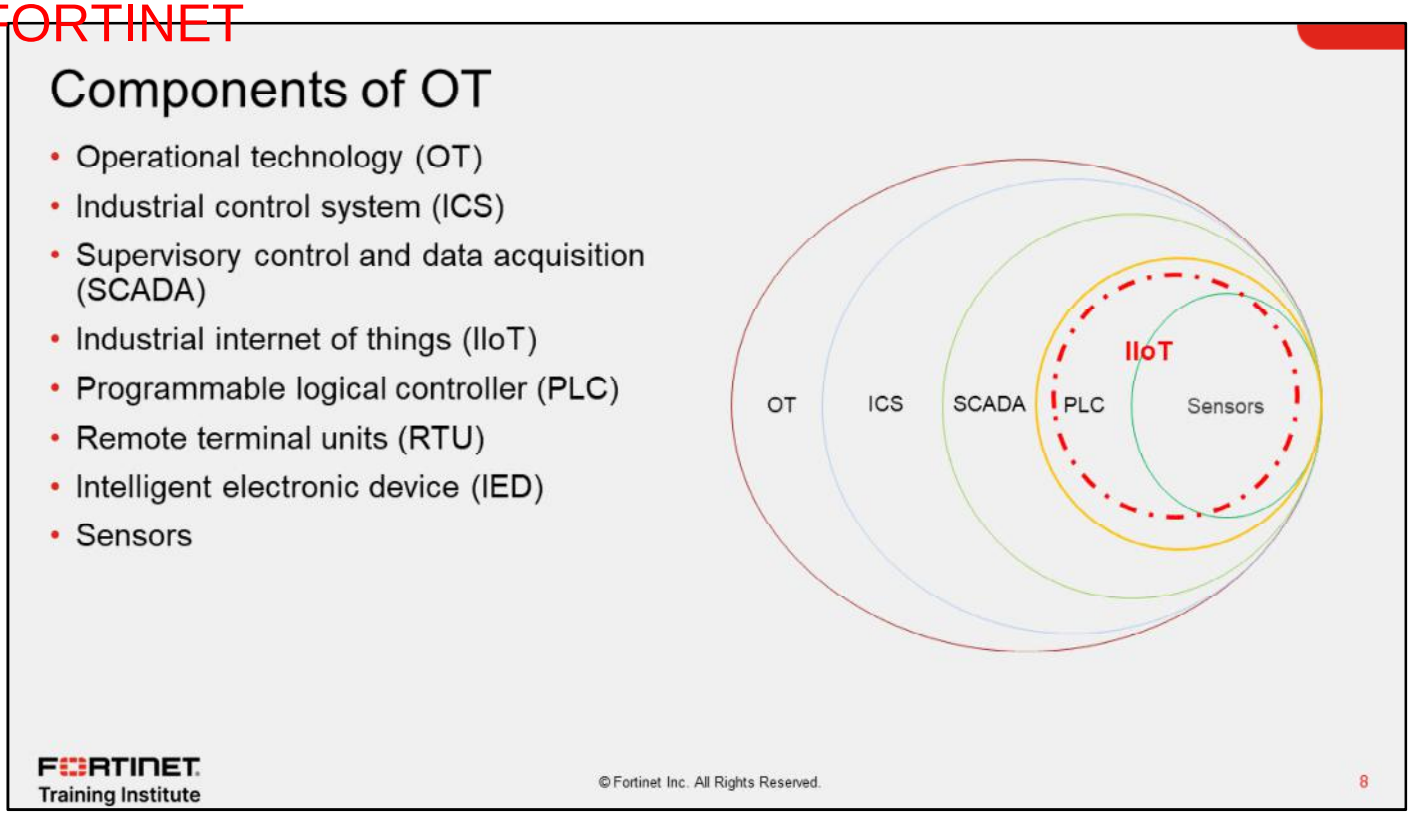
DO NOT REPRINT
© FORTINET



IT and OT share features, such as TCP and IP communications and other protocols that allow remote access to devices and monitoring resources. IT and OT also run similar operating systems, such as Windows and different Linux distributions.

For IT, security refers to the ability to ensure the confidentiality, integrity, and availability of systems and data. For OT, safety refers to the physical well-being of people, equipment, and the environment—preventing injury and damage to people and things.

DO NOT REPRINT
© FORTINET



The main components of OT are shown on this slide.

- ICS consists of systems that are used for monitoring and controlling industrial processes.
- SCADA systems collect data from various sensors at a factory, plant, or in other remote locations and sends this data to a central computer for control.
- PLCs connect the sensors and remote terminal units (RTUs) to the SCADA system. PLCs collect and pass data to and from the SCADA system in real time.
- IEDs issue commands to other power system equipment, such as circuit breaker and capacitor banks. It receives the data from sensors and other power equipment.

DO NOT REPRINT
© FORTINET

ICS

- Main component of OT
- Consists of systems that are used for monitoring and controlling industrial processes
- Controls SCADA and DCS



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

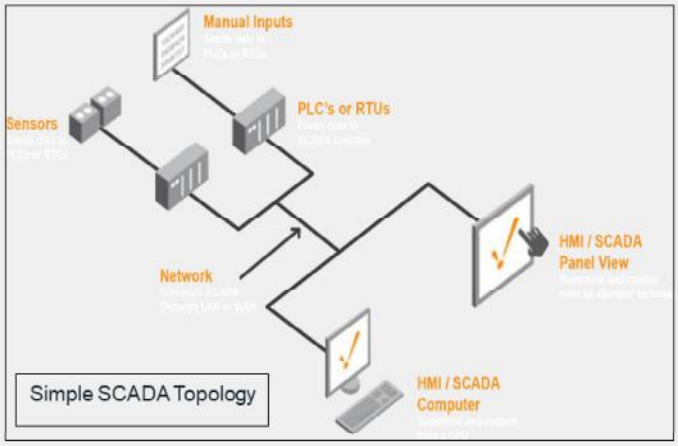
9

ICS are a main component of OT. ICS includes different types of devices, systems, controls, and networks that manage a variety of industrial processes. The most common are SCADA systems and distributed control systems (DCS).

DO NOT REPRINT
© FORTINET

SCADA

- Collects real-time data from various sensors
- Helps you visualize the OT environment



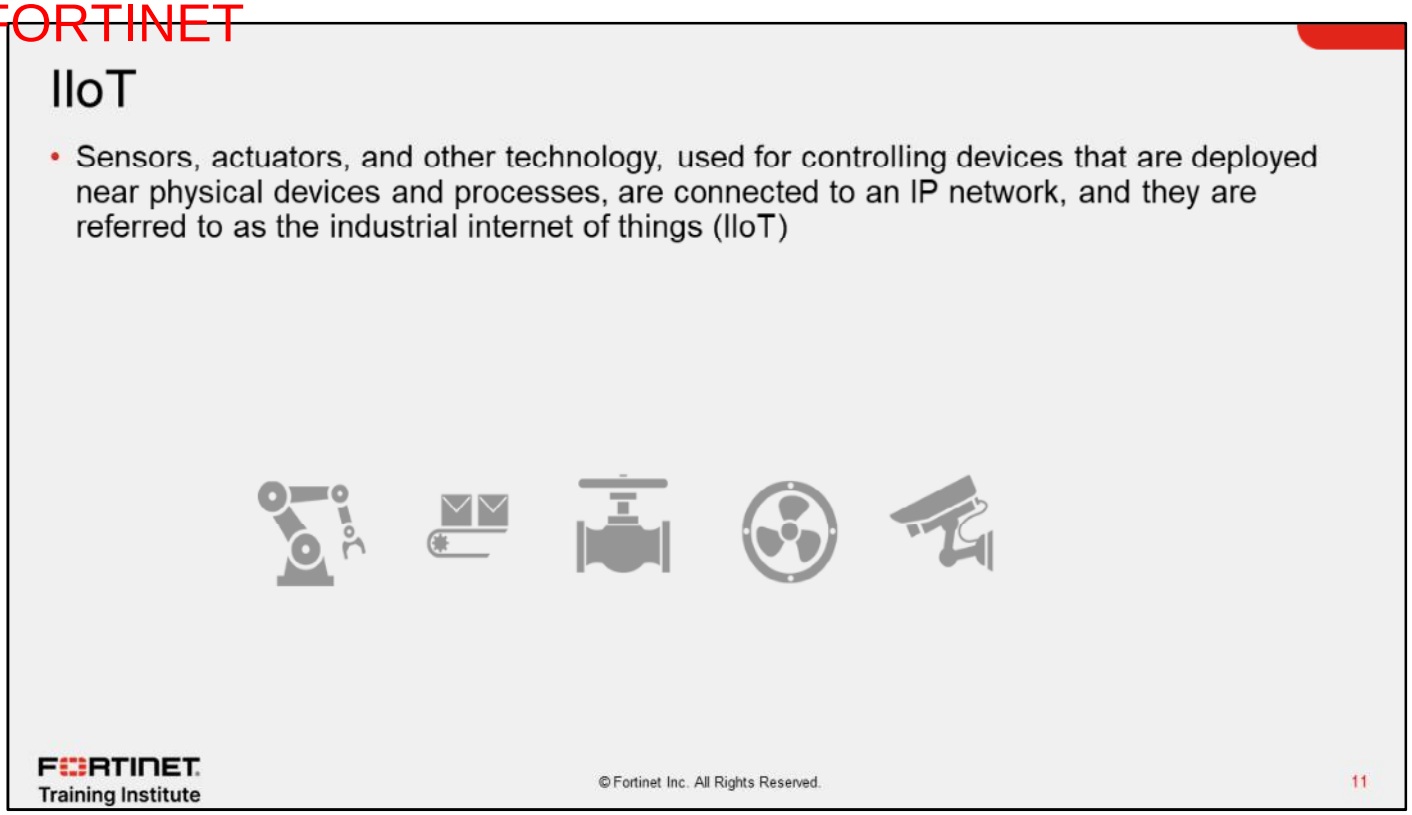
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

SCADA is a system that collects data in real time to assist with equipment control and monitoring conditions in an OT environment. It includes sensors, PLCs, RTUs, DCS, and so on. SCADA is an integral component of an OT system because it helps you to visualize and control the OT environment.

DO NOT REPRINT
© FORTINET



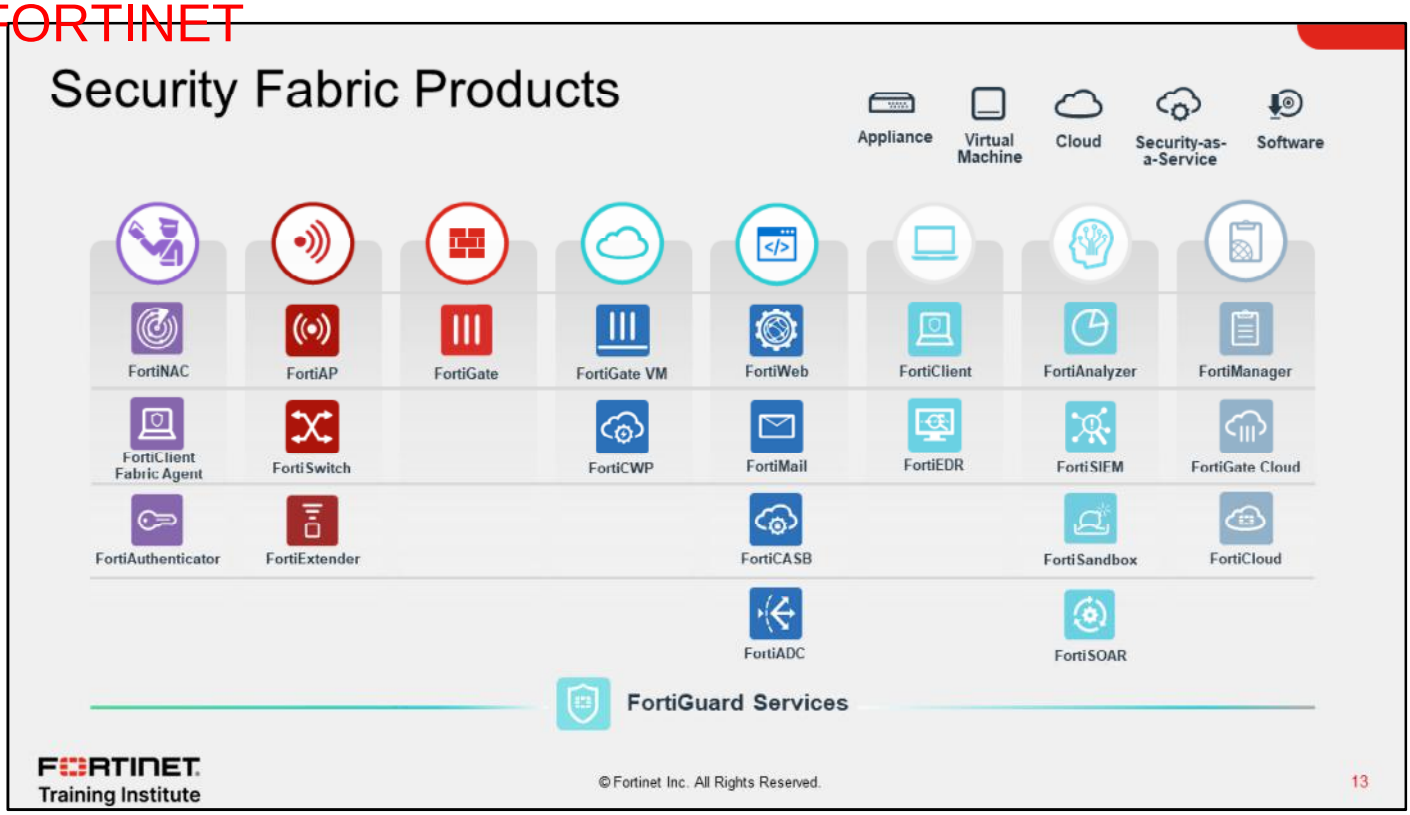
The smallest components of operational technology are a diverse array of sensors, monitors, actuators, and other technologies that are deployed on or near OT equipment. This equipment is pervasive and includes generators, pipelines, fans, programmable logic controllers (PLC), RPU, industrial robots, and so on. These sensors are examples of IIoT.

DO NOT REPRINT
© FORTINET



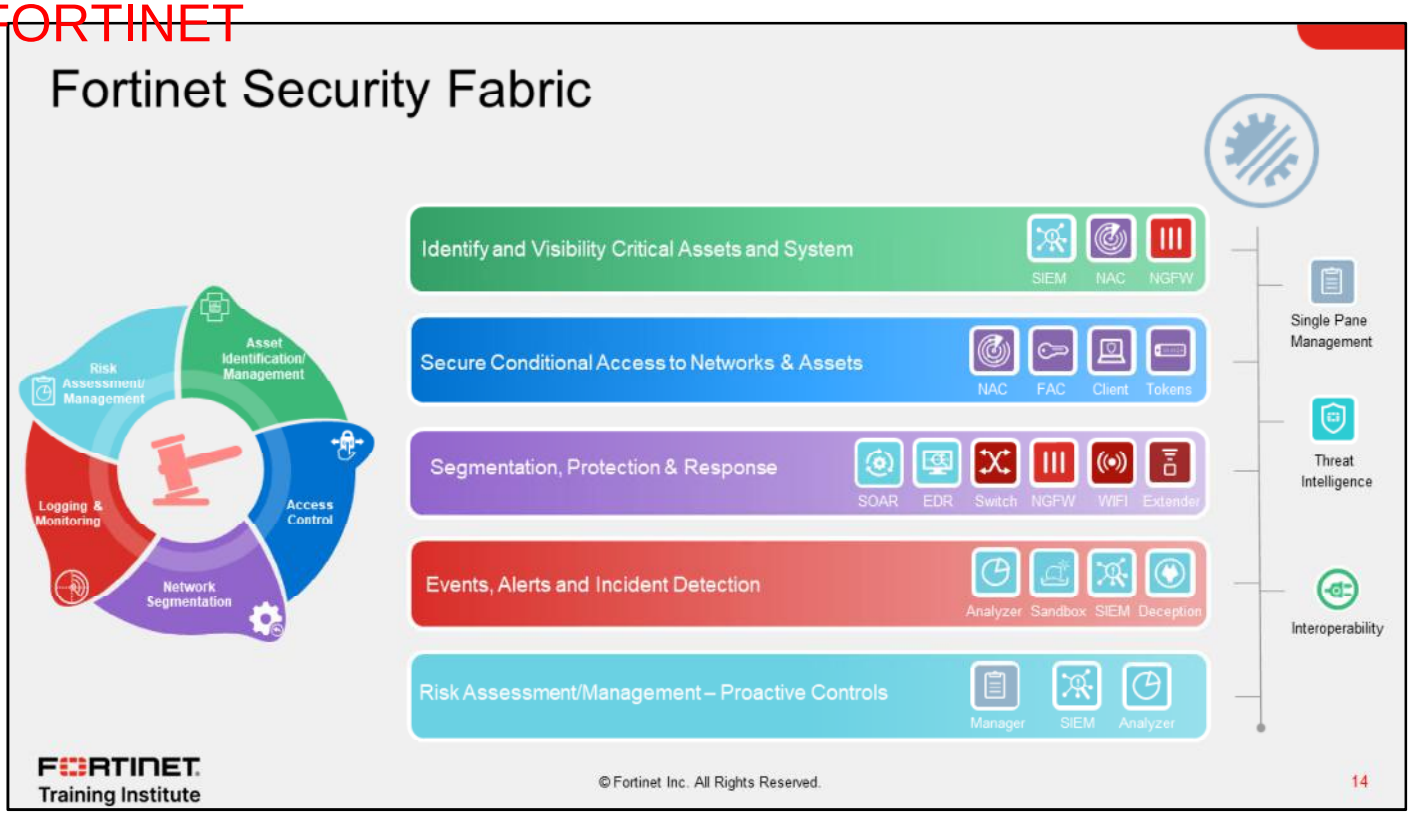
In this section, you will learn about Fortinet Security Fabric for an OT network.

DO NOT REPRINT
© FORTINET



All the products that can be integrated into the Fortinet Security Fabric are shown on this slide. All these products are supported by FortiGaurd services.

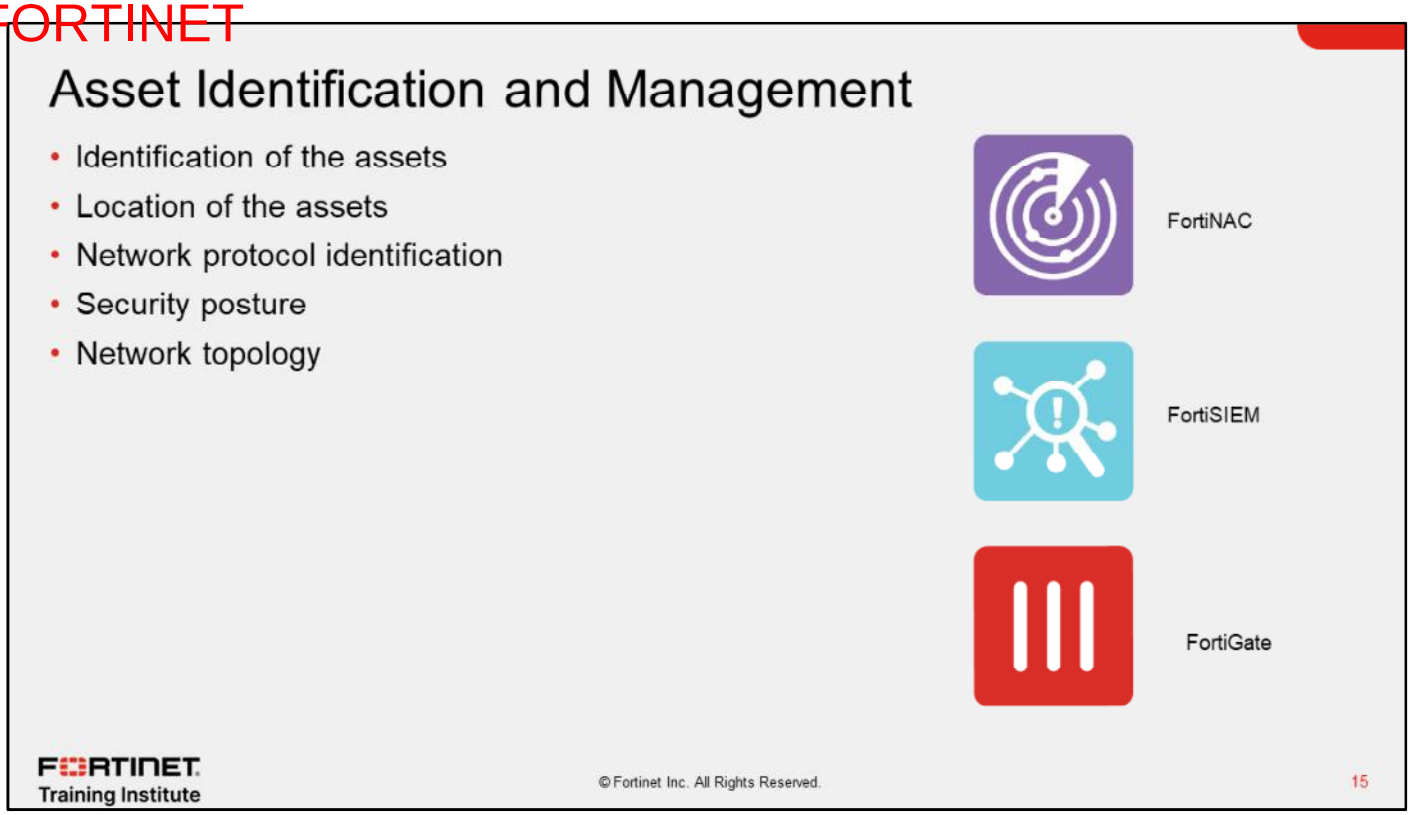
DO NOT REPRINT
© FORTINET



An OT framework represents core functions and consists of cybersecurity activities, desired results, and best practices that are common across the organization structure. This OT security framework mainly consists of the following five concurrent and continuous functions:

- Asset Identification/management
- Access control
- Network segmentation
- Logging and monitoring
- Risk management

DO NOT REPRINT
© FORTINET

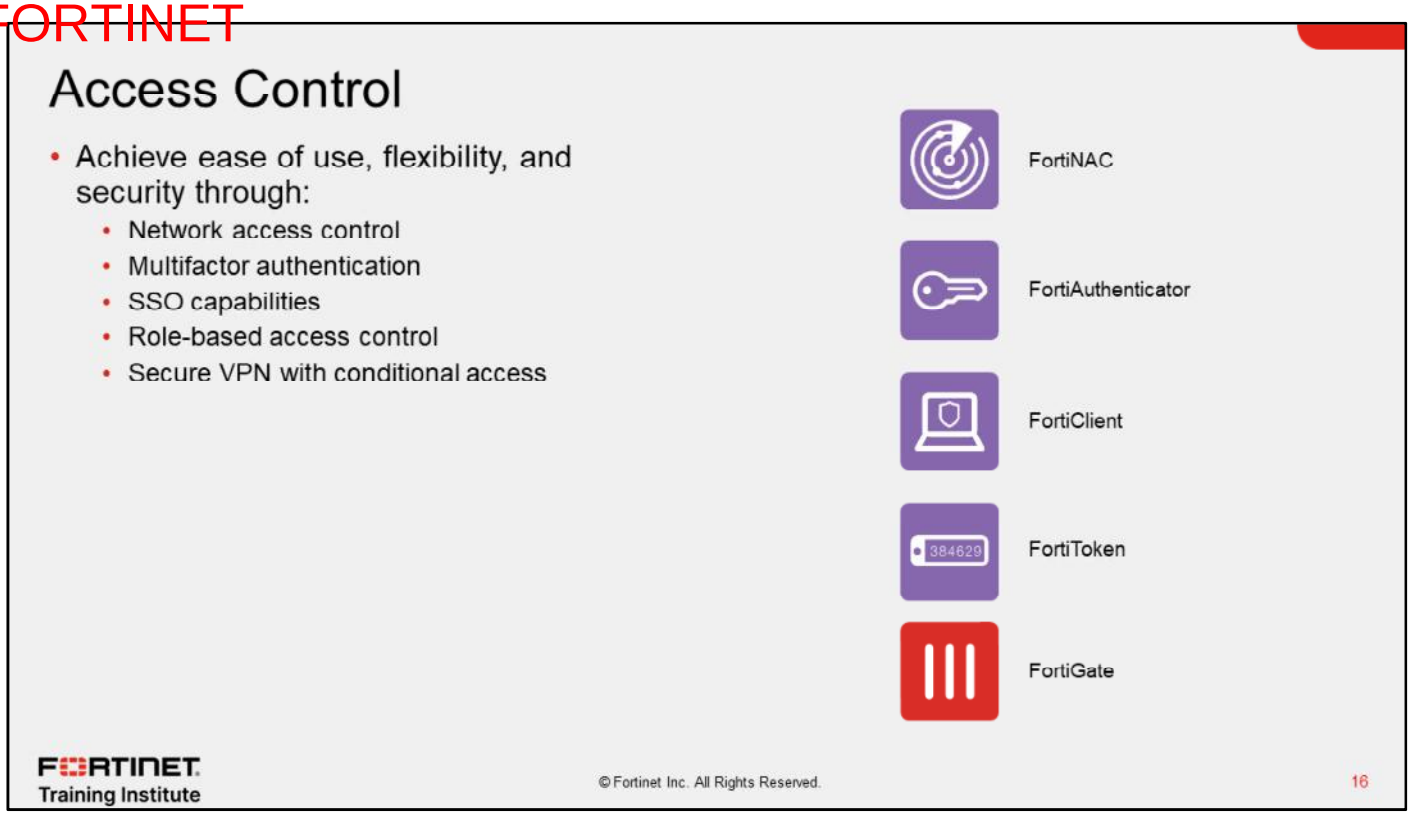


Assets identification and management includes the following activities for any ICS:

- The identification of assets and the creation of an asset inventory. Asset identification enables you to document all hardware and software that are on the OT network.
- The locating of all the critical assets. You can document the locations of all critical assets.
- The identification of which network protocols are being used by the critical assets. This is done through the use of tools.
- The creation of network topology. By gathering information through asset identification and management activities, you can create and accurate network topology.

NGFW, FortiNAC, and FortiSIEM can be used in an OT network to achieve all the objectives shown on the slide.

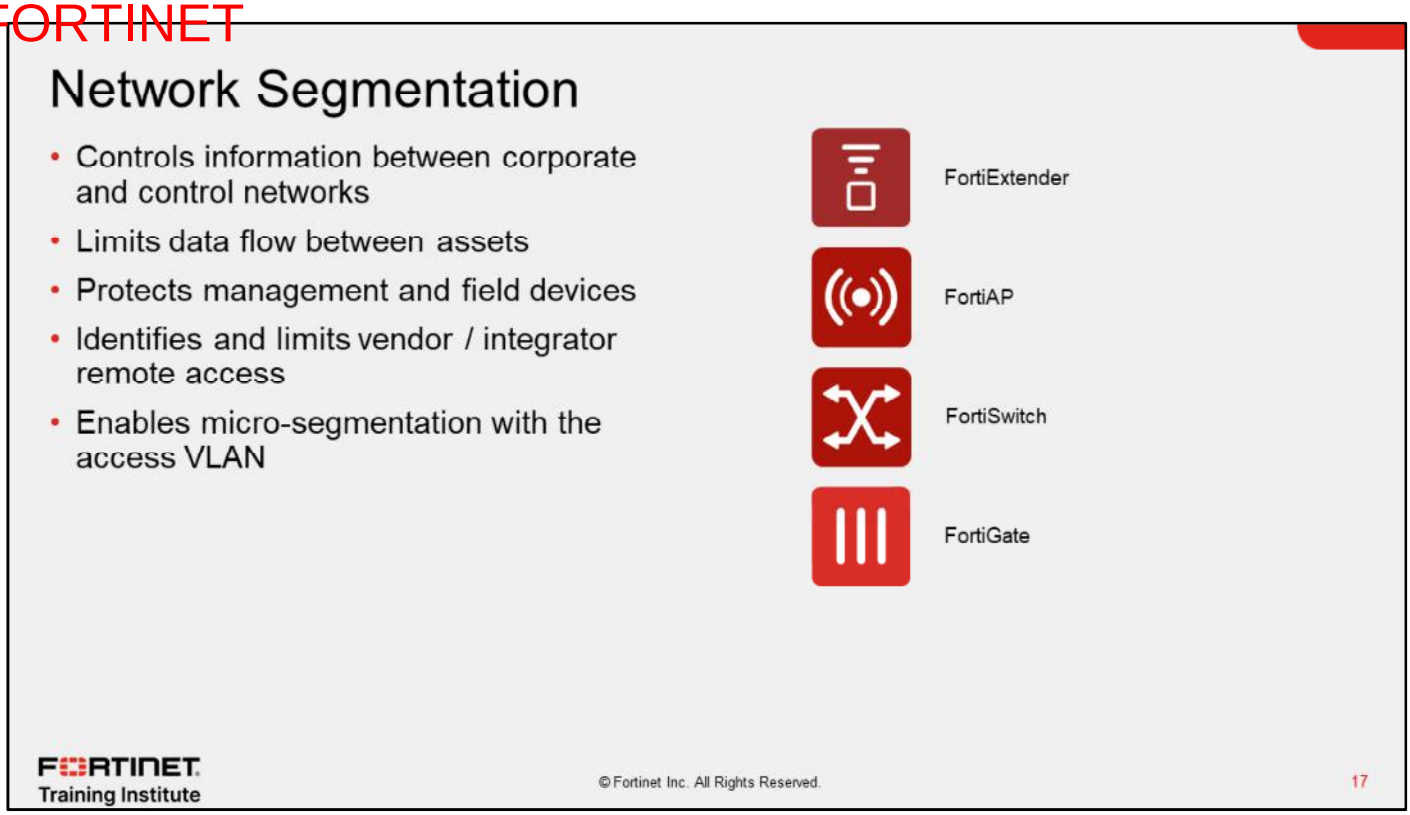
DO NOT REPRINT
© FORTINET



The main goal of access control in an OT environment is to access the assets easily and securely. You do not want to allow bad actors, vendors, or staff members access to all assets. You want to allow only *approved* operators to securely access the allowed applications. By implementing access control in an OT environment, you will provide operators to access approved applications easily, and most importantly, securely.

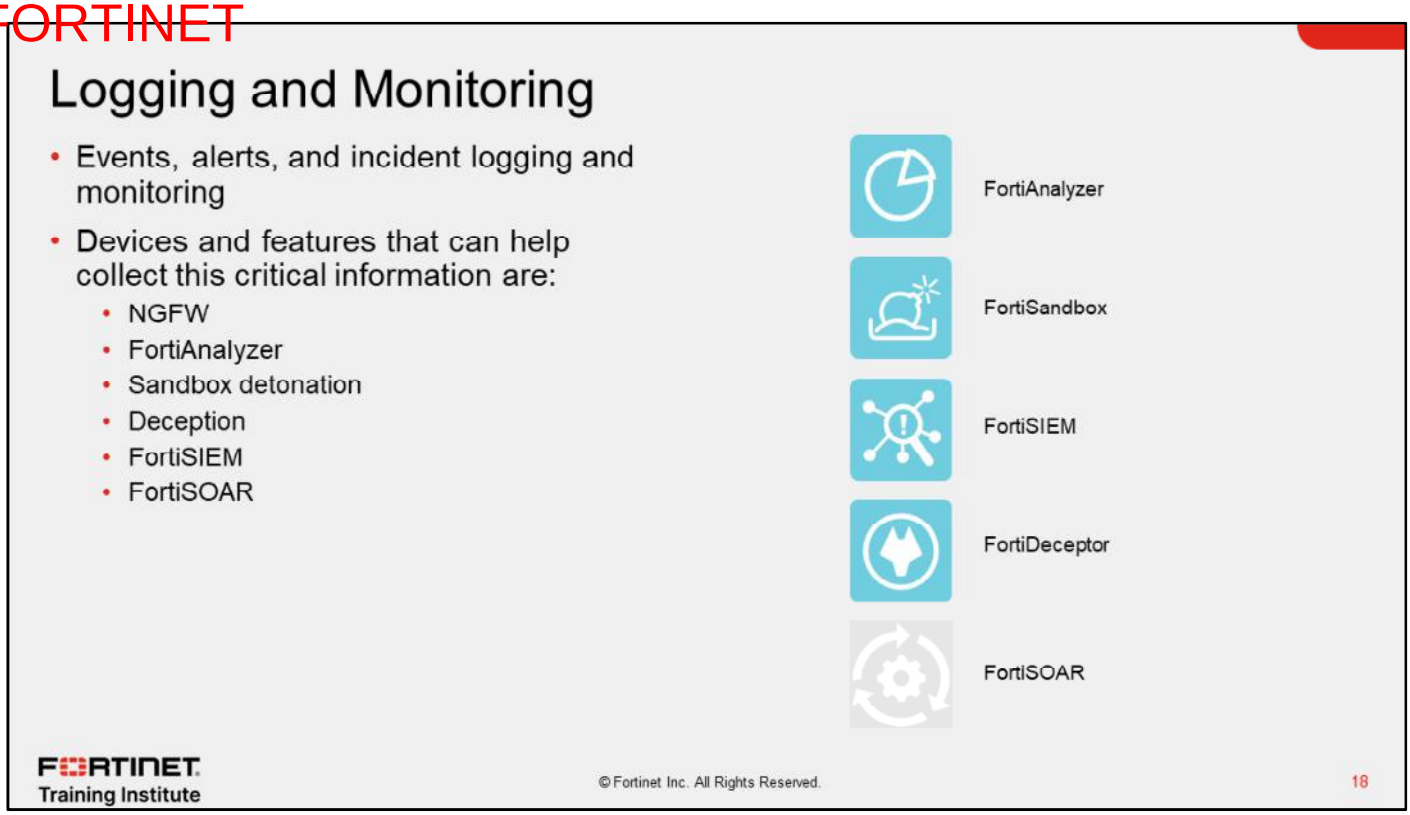
FortiAuthenticator, FortiNAC, and FortiClient, along with FortiToken, can help you achieve access control in your environment.

DO NOT REPRINT
© FORTINET



Segmentation can be achieved with enforcement boundaries or the establishment of zone and conduits aligned with your OT environment requirements. The most important boundary is the IT/OT boundary, because it will determine the OT secured perimeter accessible through a unique access point (AP). This AP is called the electronic access point (EAP) in the NERC-CIP standard, and it is a requirement. All inbound and outbound communication, including access from the corporate network, remote connectivity, or application residing in the cloud, should go through the EAP, making it the most critical part of your infrastructure.

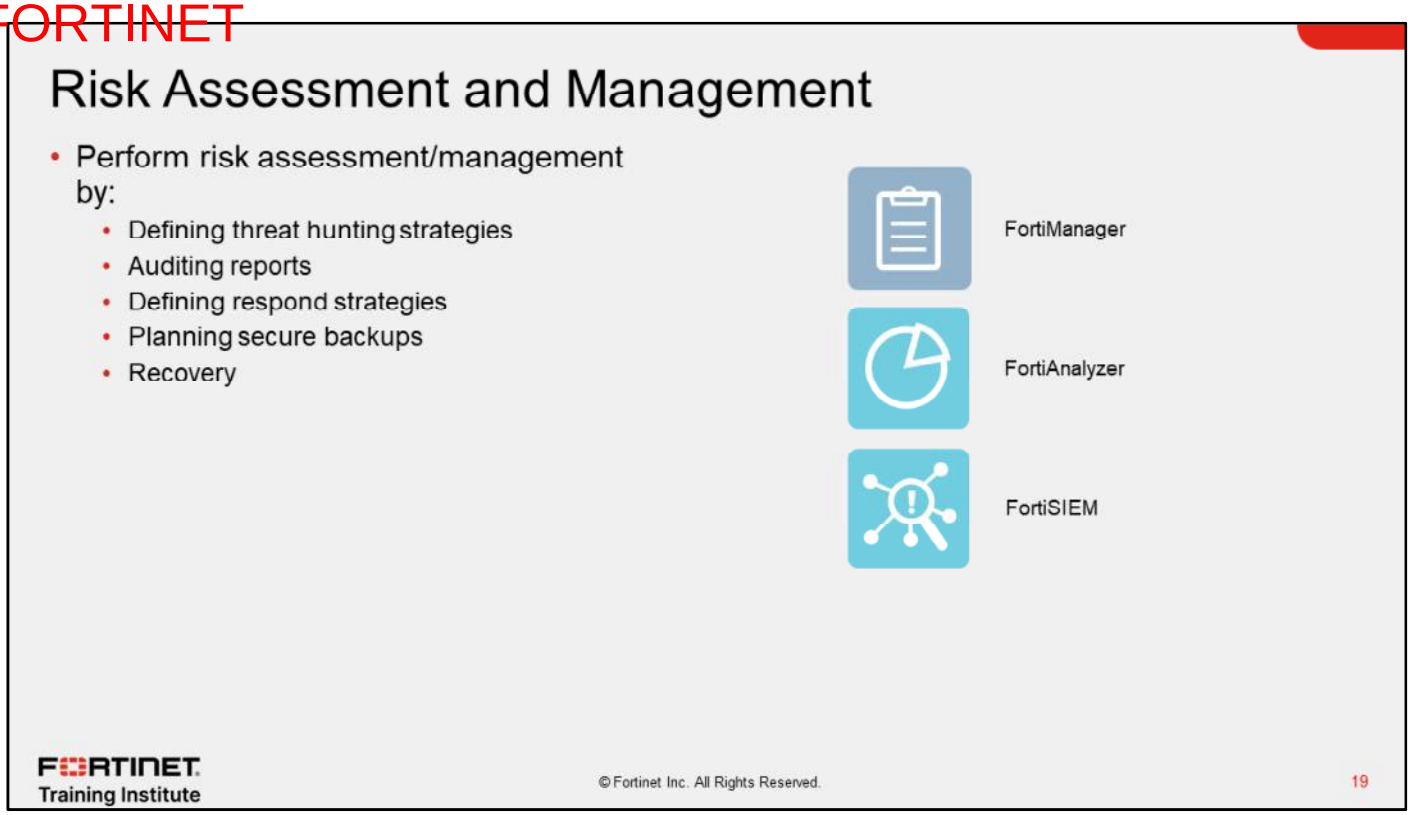
DO NOT REPRINT
© FORTINET



You need full log visibility in both the IT and OT environments. Logging and reporting is a crucial element in the framework because it helps auditors perform threat hunting and the spot possible threats to the OT network.

The advantages of the single-pane-of glass approach are key when reviewing an incident. Utilizing the Fortinet Security Fabric, operators and incident responders can link access logs, device information, and network traffic to provide a complete picture during post-incident forensics.

DO NOT REPRINT
© FORTINET



Planning a threat hunting strategy for any organization is a critical task. Auditors should be able to follow set of guidelines for threat hunting through reports and to respond to the threats in timely manner. FortiSOAR is a product that can be used to automate the repose to reported incident.

Risk management is also about evaluating what can go wrong before it happens. You need to consider how industrial control systems can be manipulated and what the physical, environmental, and financial consequences would be. This will drive the types of controls you will want to put in place.

FortiManager together with FortiAnalyzer can provide security rating for the Fortinet network security scope. It will provide rating against ICS guidelines, such as the NIST CSF or the CIS top 20 best practices.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the industrial architecture of an OT network with Fortinet Fabric devices.

DO NOT REPRINT
© FORTINET

ICS Standards and Frameworks



Key ICS policies, standards, guidelines, and frameworks	Type	Related institutions and agencies	Host countries	Scope	Applicable GEOs
NIS Directives	Policies	ENISA	EU (+ UKI)	OES & DSP (*) IT/OT	EU
ANSI - ISA/IEC 62443 (formerly ISA-99)	Standards	ISA,IEC, ANSI	International	Multi-Industry **OT**	Global
NIST CSF	Guidelines (Framework)	NIST	US	Multi-Industry IT/OT	Global
Critical Security Controls (CIS Top 20)	Guidelines	CIS	US	Multi-Industry **OT**	Global
NERC-CIP	Standards	FERC	US	Electricity IT/OT	US, Canada, Mexico
NIST 800-82	Guidelines	NIST	US	Multi-Industry **OT**	Global
PCI DSS	Standard	Card Companies	International	Payment Card IT	Global
GDPR	Policy	EU Parlement	EU	Multi-Industry IT	Global

FORTINET Training Institute

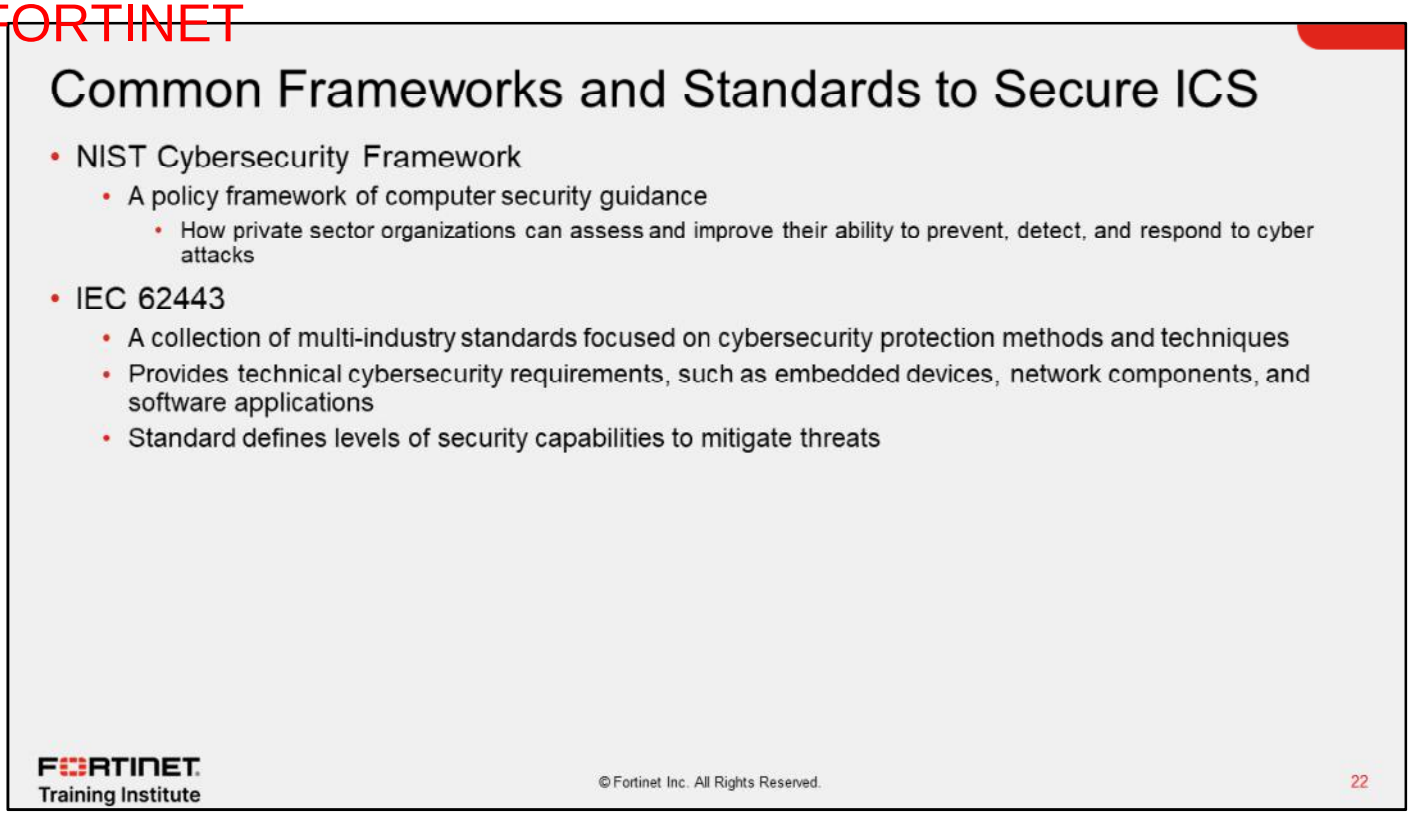
© Fortinet Inc. All Rights Reserved.

21

Asset owners, such as utilities or train operators, are regulated by bodies that can enforce compliance to several standards through policies and directives that are published by institutions, agencies, and regulators.

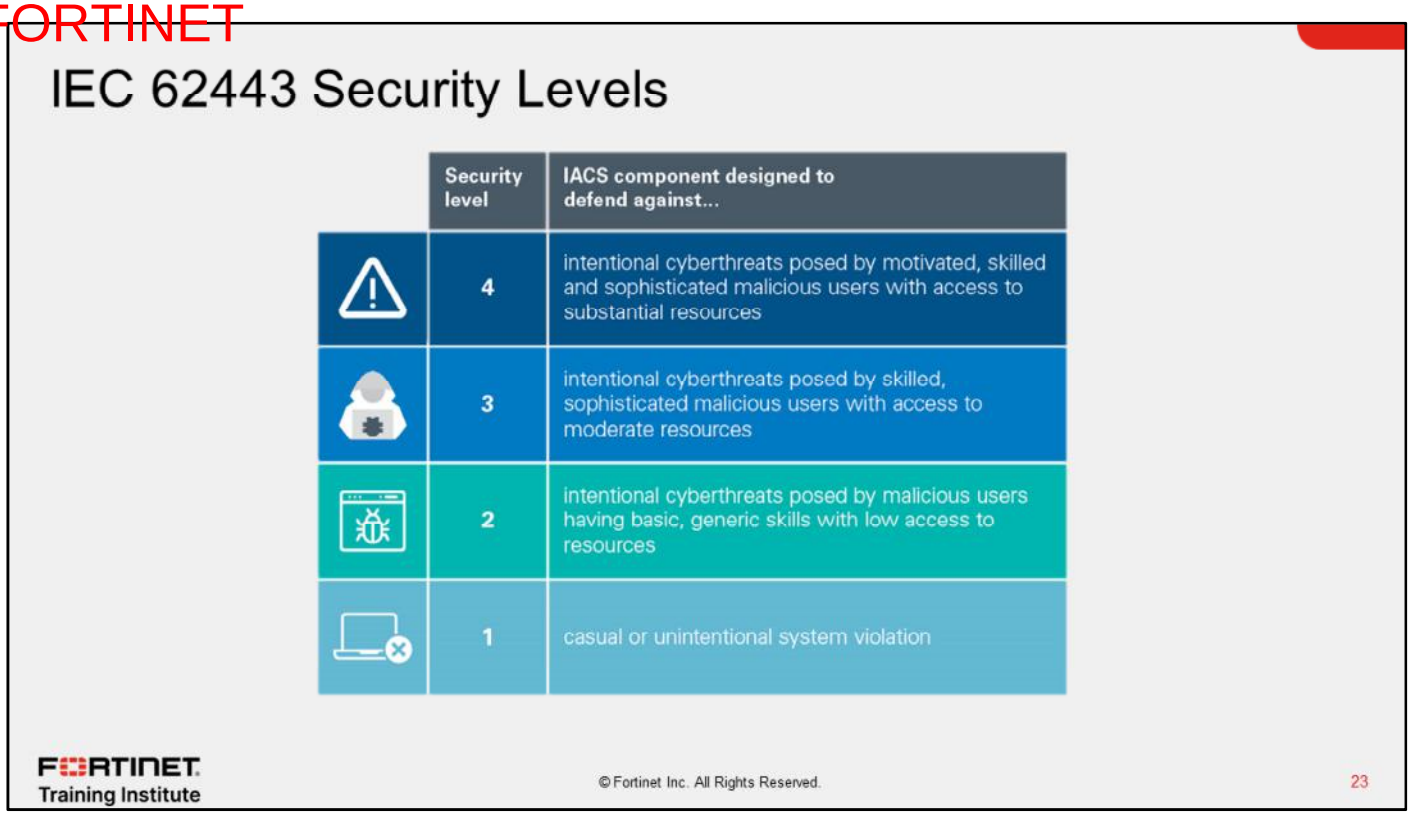
The table shows the most important standards and guidelines for ICS. All are critically important to know by name. The most important set of standards is the cybersecurity standard of multi-industry (IEC 62443). IEC 62443 is specific to OT security and is applicable across all industrial sectors. Fortinet built its reference architecture around it.

DO NOT REPRINT
© FORTINET



The NIST cybersecurity framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. The framework not only helps organizations understand their cybersecurity risks, such as threats, vulnerabilities and impacts, but also how to reduce these risks with customized measures.

DO NOT REPRINT
© FORTINET



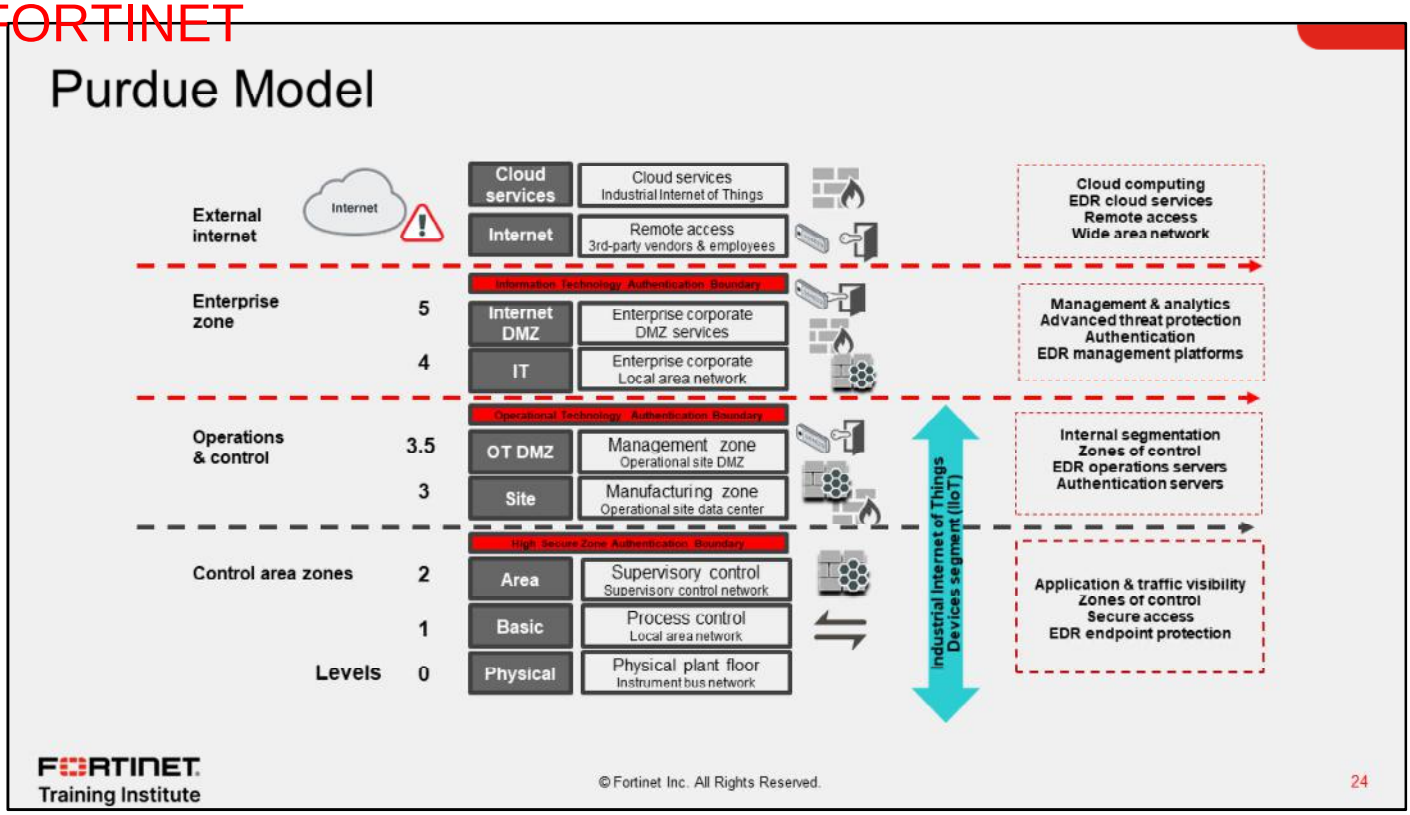
The IEC 62443 standard introduces the concept of security levels (SL) that can be applied to zones and conduits. The security level is defined by researching a particular device, and then determining what level of security it should have, depending on its place in the system. The security levels are classified into four distinct levels:

- Level 1: A casual exposure—unintentional operator error
- Level 2: An intentional attack with low resources
- Level 3: An intentional attack with moderate resources
- Level 4: An intentional attack with extensive resources

If you are up against a syndicate of cyber extortion with extensive resources and capabilities, then you should work toward security level 4.

After you define the security level target of a zone, you should determine whether the devices inside the zone can meet the corresponding security level. If they cannot, it is necessary to plan which countermeasures can help reach the SL target. These countermeasures can be technical (for example, a firewall), administrative (for example, policies and procedures), or physical (for example, locked doors).

DO NOT REPRINT
© FORTINET



OT has traditionally been segmented based on the Purdue Model. OT security has been mapped to the desired segmentation based on these operational needs: use, flexibility, availability of physical processes, and safety.

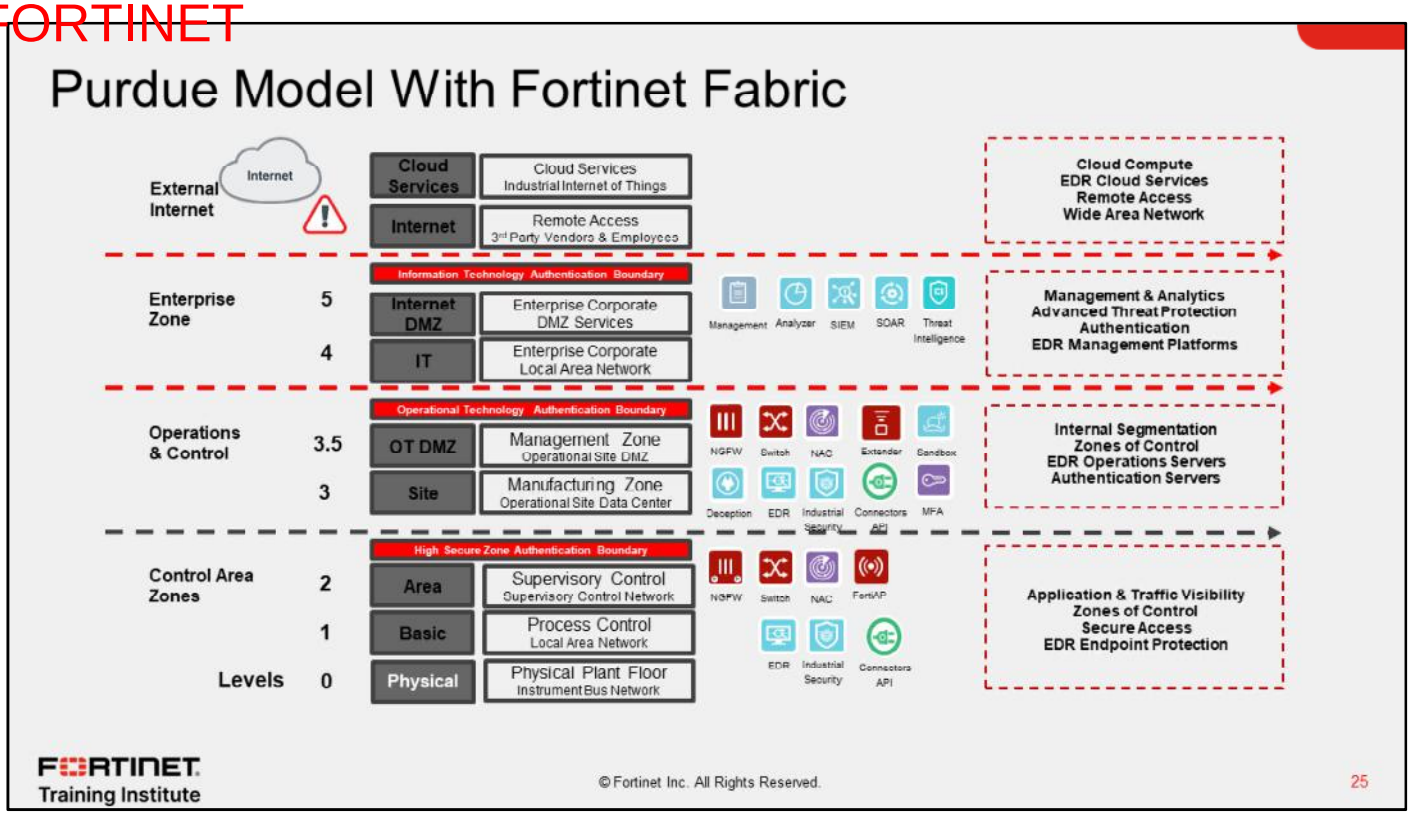
On the physical plant floor, all the critical physical assets are placed. These physical assets are equipped with sensors (IIoT).

The plant floor is broken up into control area zones, which consist of process automation elements, servers to control the process, PLCs, RTUs, and IEDs to execute the process. The control area zones are located away from the operations and control zone.

The operations and control zone consist of servers, engineering workstations, operator workstations, and a DMZ where you will find shared services, management and analytics, historians, and data shared between OT and IT.

The enterprise zone is where traditional IT resides and connects with the external internet.

DO NOT REPRINT
© FORTINET



In this slide, you can see how security can be applied to each segment of the Purdue model.

The control area zone has three levels. Level 0 will have IIoT devices. These devices need to be segmented from Level 1 and Level 2.

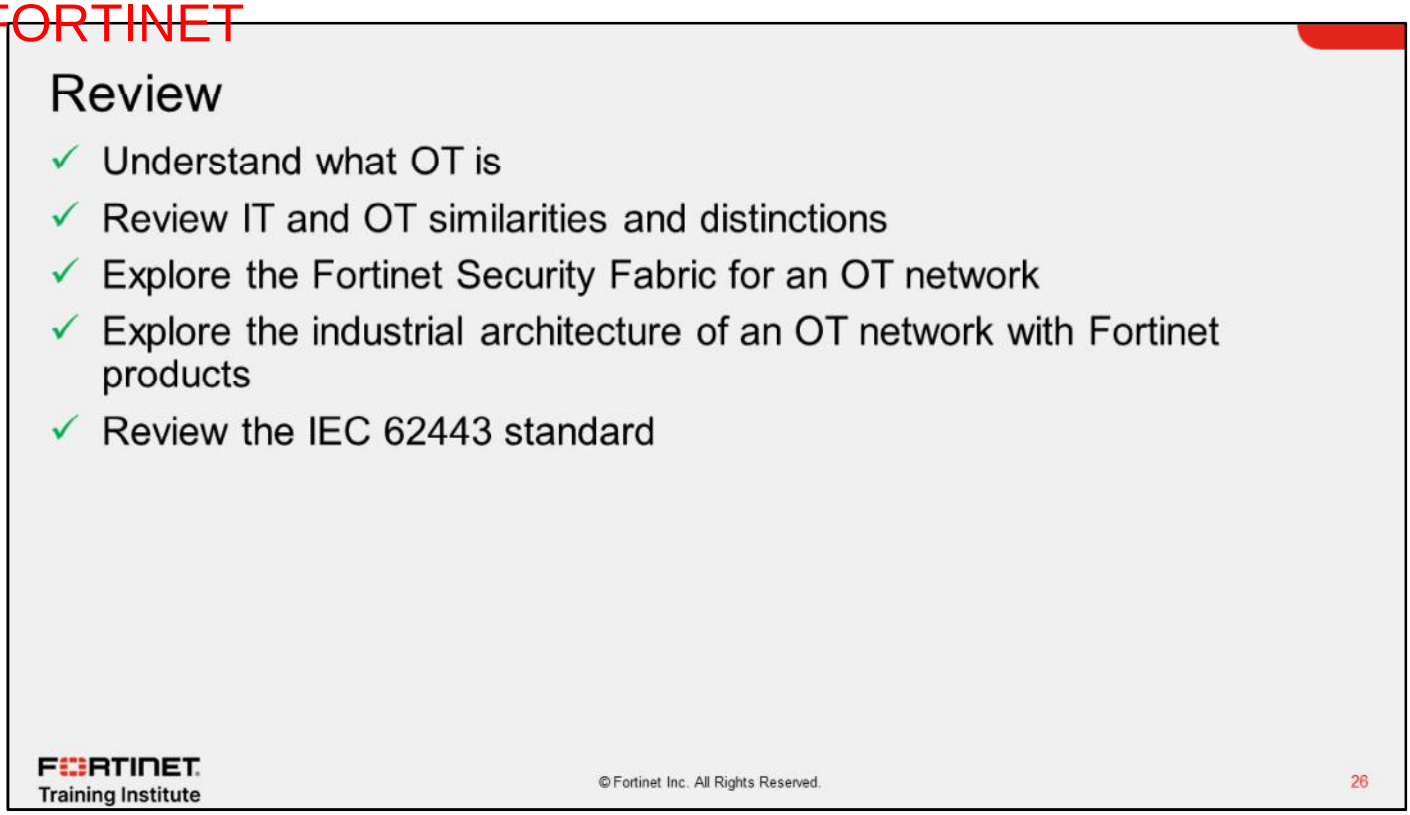
Level 1 usually has PLCs, RTUs, and IEDs connected to Ethernet switches. Visibility of these devices is essential, which can be accomplished with FortiGate, or FortiNAC, or both.

In Level 2, you will find the processes and programs that control the PLCs, RTUs, and IEDs found at Level 1. It is necessary to segment, or even microsegment these servers with firewall segmentation, along with policies that include application control and virtual patching. Additionally, FortiEDR can be deployed on these servers to ensure process availability and security directly on the servers.

Level 3 is manufacturing zone, and Level 3.5 is a management zone. In Level 3, you will find servers and workstations. Those servers are for authentication, engineering workstations, operator workstations, OT applications, and supply chain management applications. Level 3.5 includes servers for the management of operations. In these zones, next generation firewalls (NGFW), and switching are the base requirements of a solution. Authentication, two-factor authentication, and policy controls that include device, user, application, and protocols controls are a must.

As IT and OT converge, you must consider management and advanced threat protection at Level 4 and Level 5 of the Purdue Model. Advanced threat protection includes SIEM and SOAR, along with IOCs and threat intelligence.

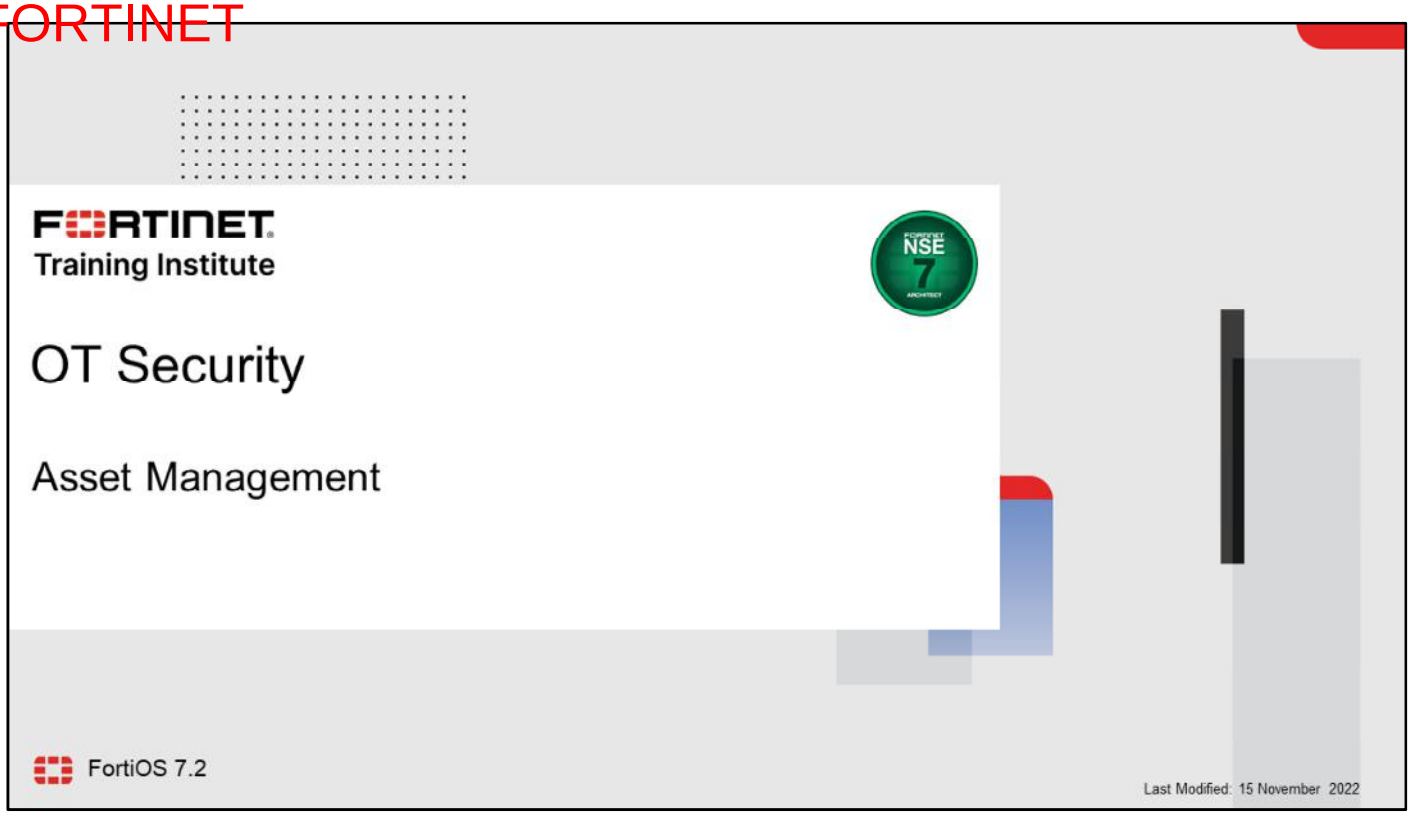
DO NOT REPRINT
© FORTINET



This slide shows the objectives that you covered in this lesson.

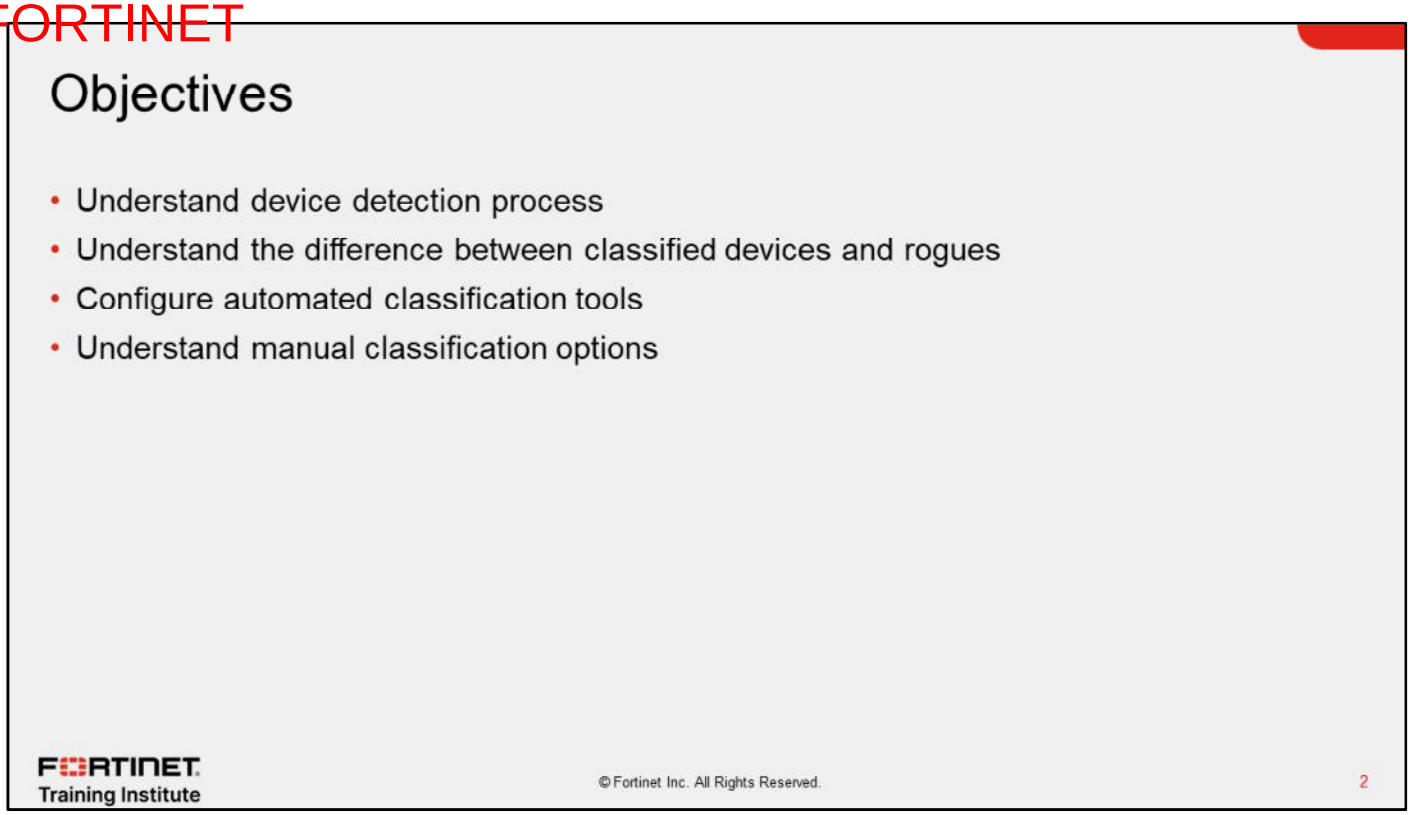
By mastering the objectives covered in this lesson, you learned about the basics of OT and the Fortinet Security Fabric for an OT network.

DO NOT REPRINT
© FORTINET



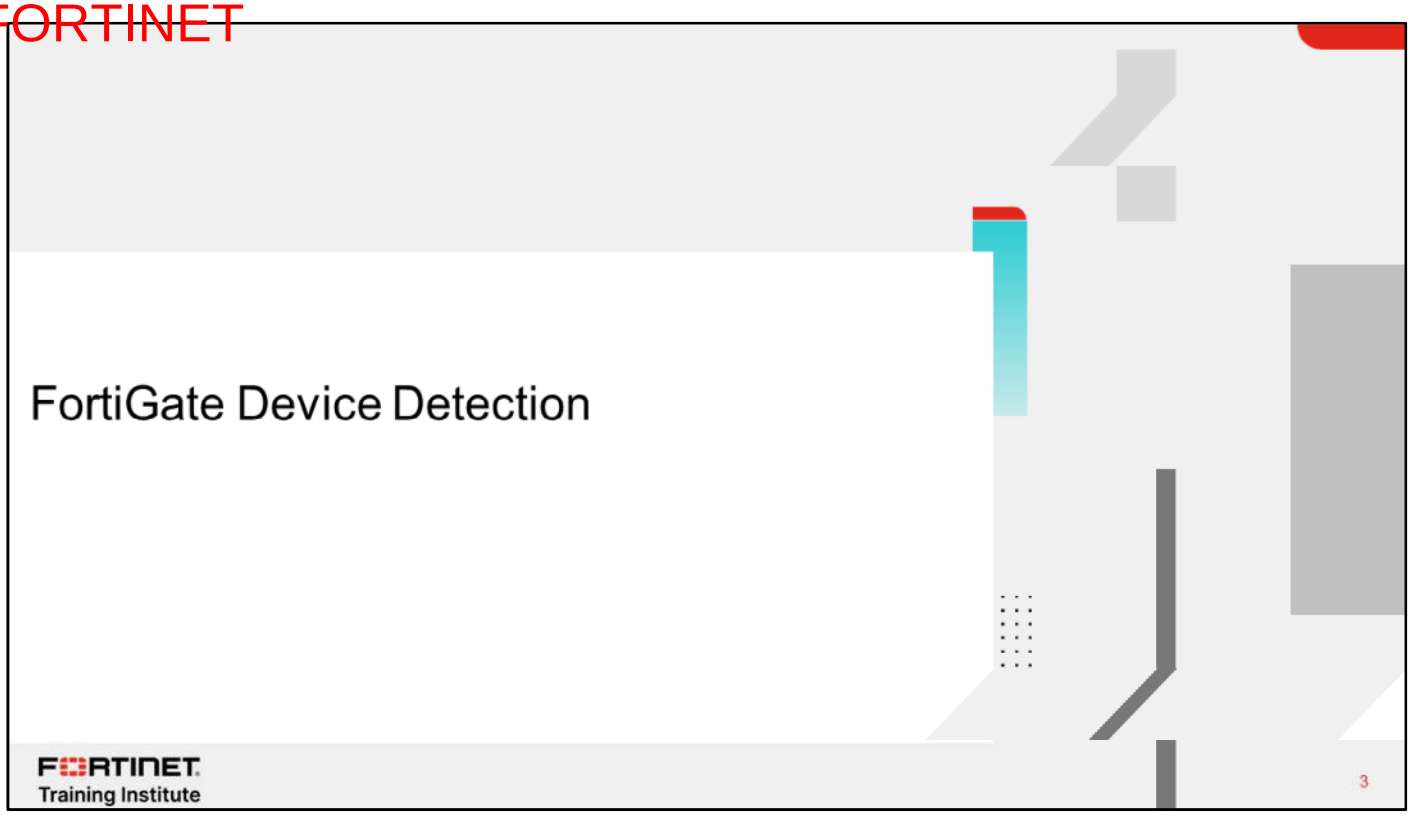
In this lesson, you will learn about asset management in the OT network.

DO NOT REPRINT
© FORTINET



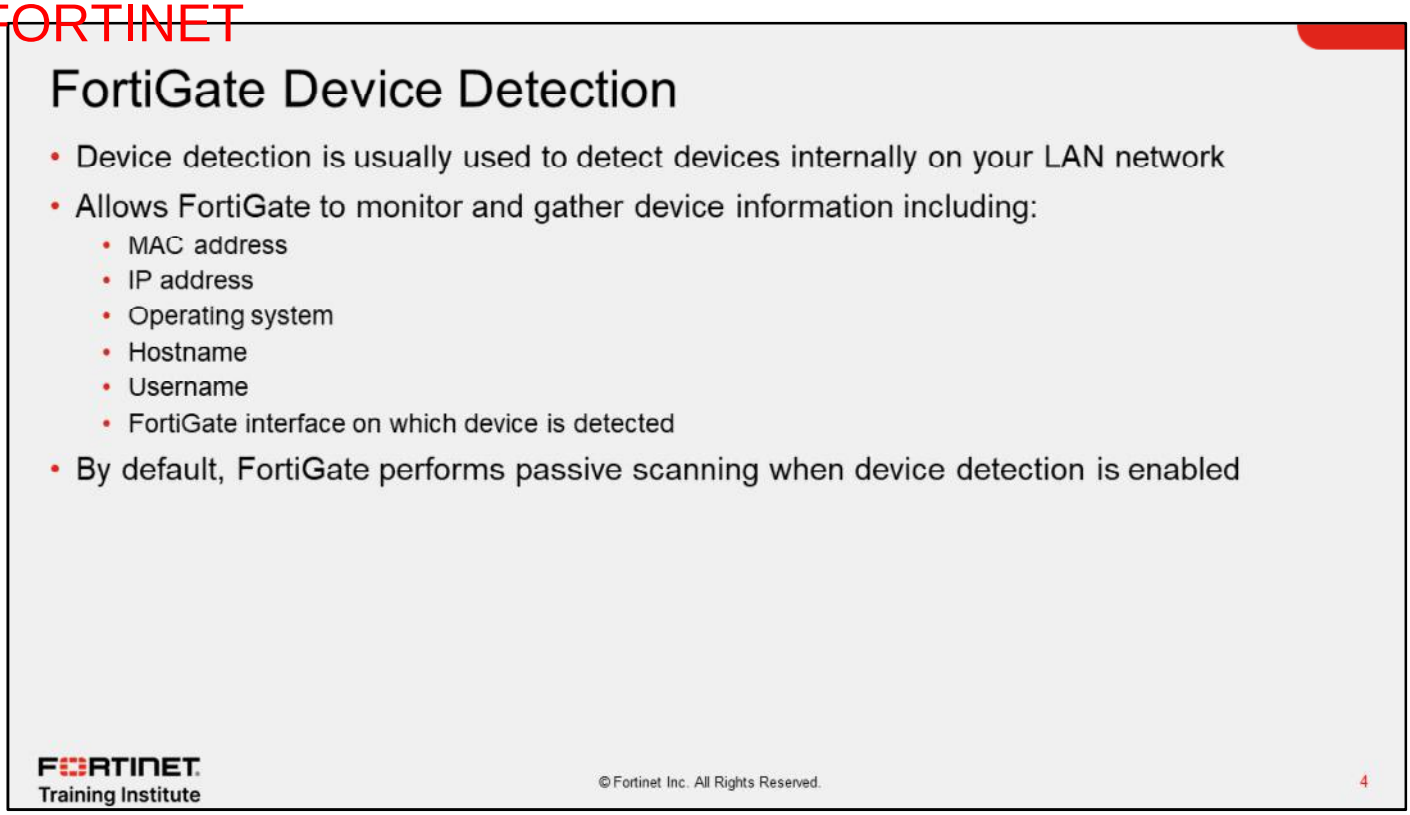
After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about different methods of device detection by FortiGate.

DO NOT REPRINT
© FORTINET



You can enable device detection separately on each interface on FortiGate. You would usually use device detection to detect devices internally on your LAN network. For this reason, device detection is not available when you select WAN as the interface role. After you enable device detection on an interface, local MAC address filtering is available and you can restrict or allow devices using a MAC address object in the firewall policy.

Device detection allows FortiGate to detect devices, and provides important information about them, such as MAC address, IP address, the FortiGate interface on which the device is detected, and so on.

DO NOT REPRINT
© FORTINET

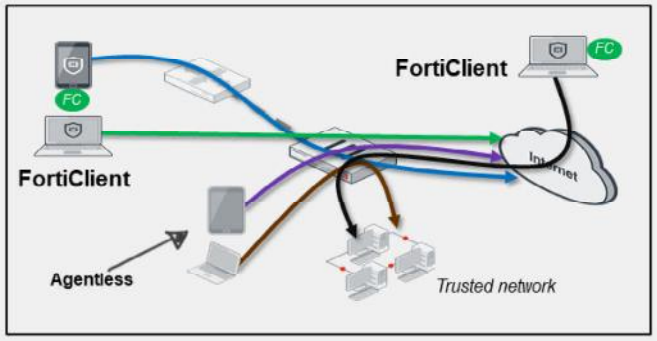
Device Identification–Agentless vs. Agent

Agentless

- Useful feature for the Security Fabric topology view
- Requires *direct* connectivity to FortiGate
- Detection methods:
  - HTTP user agent
  - TCP fingerprinting
  - MAC address vendor codes
  - DHCP
  - Microsoft Windows browser service (MWBS)
  - SIP user agent
  - Link Layer Discovery Protocol (LLDP)
  - Simple Service Discovery Protocol (SSDP)
  - QUIC
  - FortiOS-VM detection
    - FortiOS-VM vendor ID in IKE messages
    - FortiOS-VM vendor ID in FortiGuard web filter and spam filter requests

Agent (FortiClient)

- Location and infrastructure independent



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

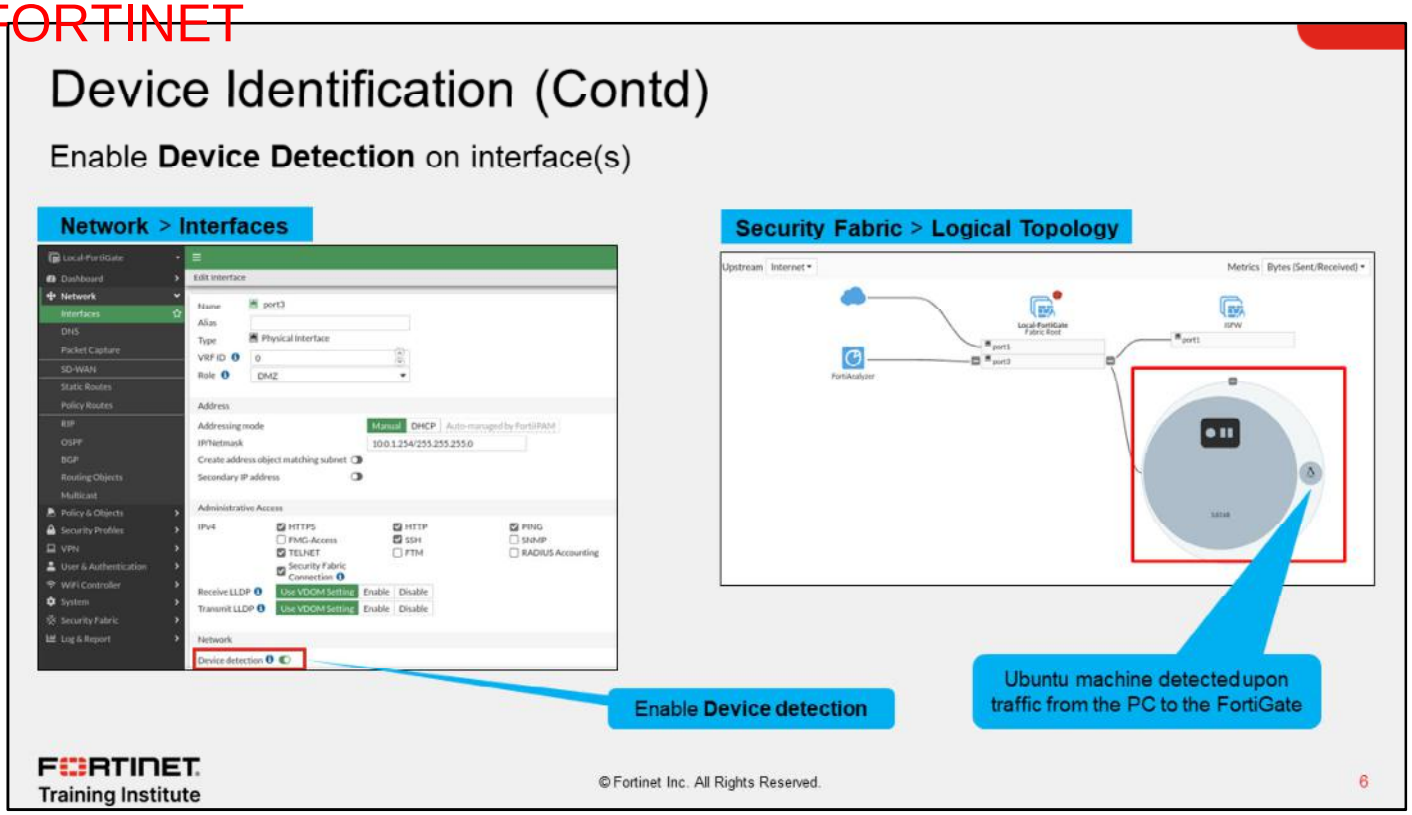
Device identification is an important component in the Security Fabric. FortiGate detects most of the third-party devices in your network and added into the topology view in the Security Fabric. There are two device identification techniques: with an agent and without an agent (agentless).

Agentless identification uses traffic from the device. Devices are indexed by their MAC address and there are various ways to identify devices, such as HTTP user-Agent header, TCP fingerprint, MAC address OUI, and FortiOS-VM detection methods, to name a few. Agentless device identification is only effective if FortiGate and the workstations are directly connected network segments, where traffic is sent directly to FortiGate, and there is no intermediate router or Layer 3 device between FortiGate and the workstations.

Note that FortiGate uses a *first come, first served* approach to determine the device identity. For example, if a device is detected by the HTTP user agent, FortiGate updates its device table with the detected MAC address and scanning stops as soon as the type has been determined for that MAC address.

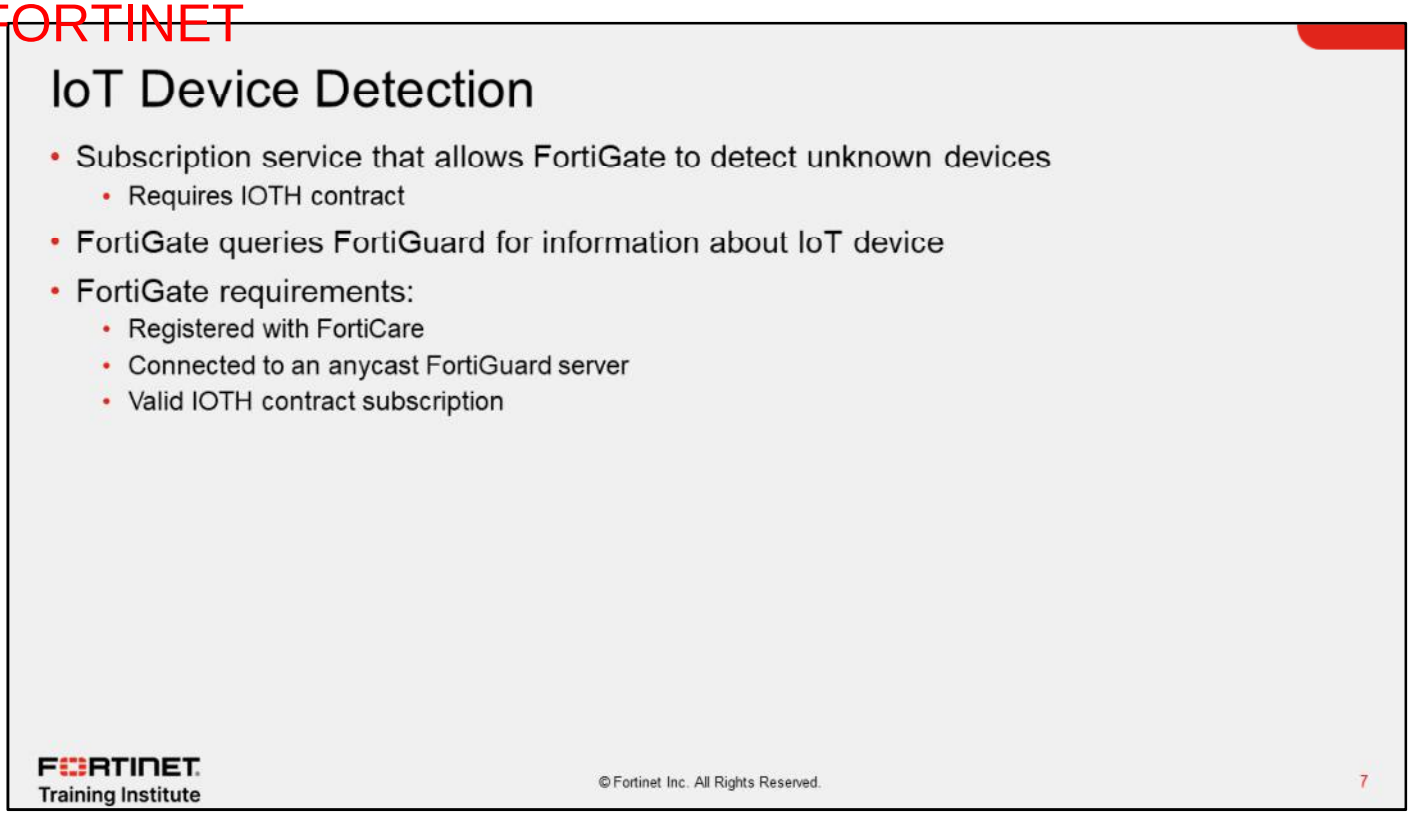
Agent-based device identification uses FortiClient. FortiClient sends information to FortiGate, and the device is tracked by its unique FortiClient user ID (UID).

DO NOT REPRINT
© FORTINET



By default, FortiGate uses device detection, which runs scans based on the arrival of traffic.

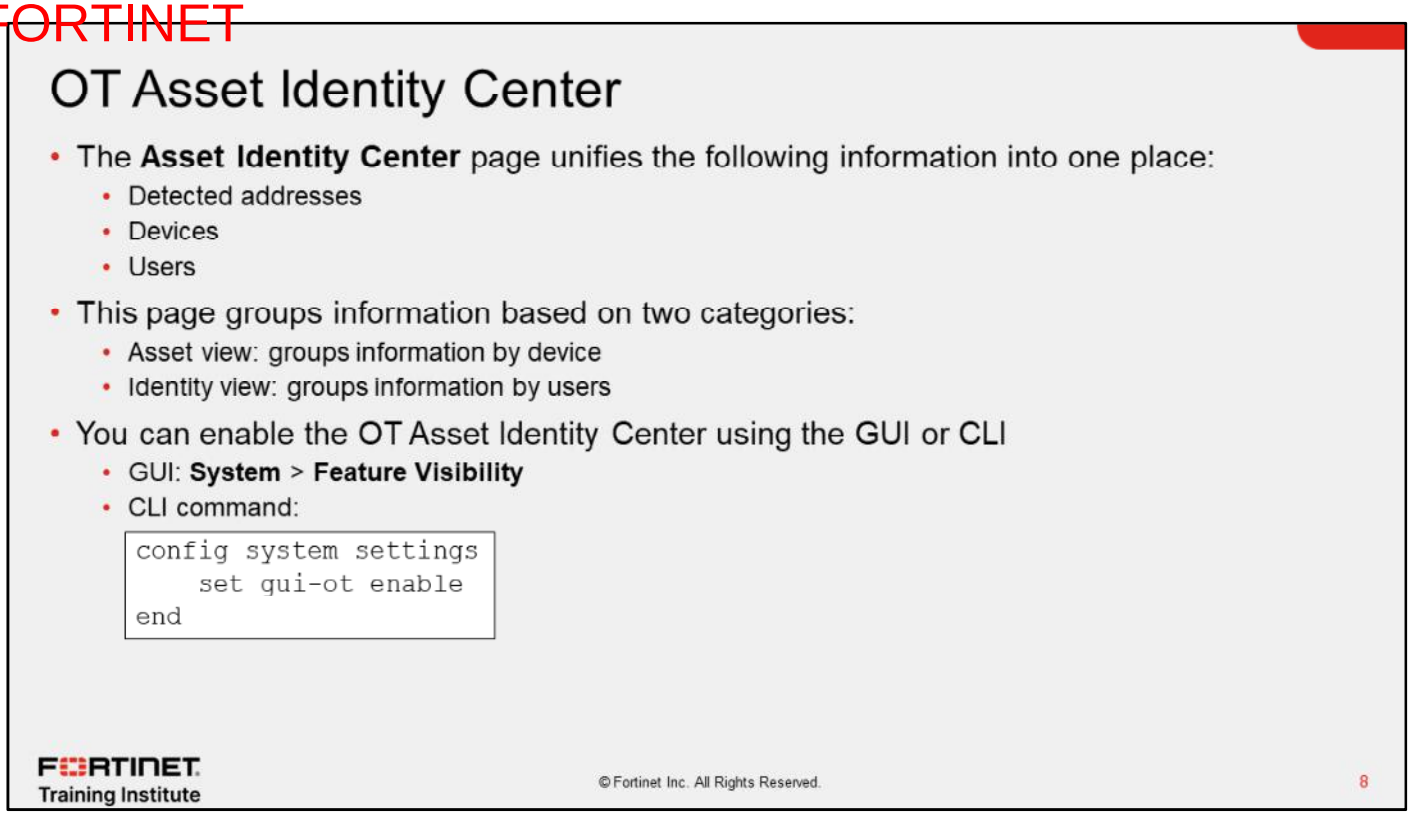
DO NOT REPRINT
© FORTINET



To detect IoT devices, FortiGate requires an internet of things (IOTH) contract. FortiGate uses the interface to detect device traffic flow. FortiGate will first try to detect the devices based on the information in the local device database (CIDB). If FortiGate is unable to detect the devices, then FortiGate queries the FortiGuard servers by sending the unknown device data to the FortiGuard servers and, in response, FortiGuard servers provide more information about the devices.

FortiGate must:
- Be registered with FortiCare
- Be connected to an anycast FortiGuard server
- Have a valid IOTH contract subscription

DO NOT REPRINT
© FORTINET



The **Asset Identity Center** page provides IT and OT information such as detected address, devices, and users. You can view the information in two different ways:

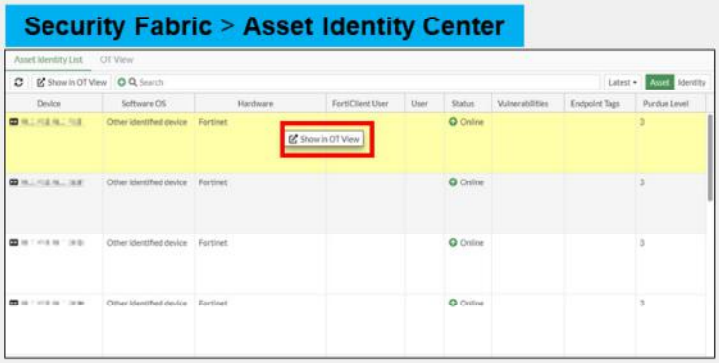
- Asset view—which groups the information by the device type
- Identity view—which groups the information by the users

The feature is not enabled by default. You can enable it in the **Feature Visibility** section of the GUI, or using the CLI command shown on this slide.

DO NOT REPRINT
© FORTINET

OT Asset Identity Center (Contd)

- The **Asset Identity Center** page displays an **Asset Identity List** tab and an **OT View** tab
- The **Purdue Level** column shows the current level of a device
  - The level of each device can change to a different Purdue level
- Right-click the device and then click **Show in OT View** to switch the display to **OT View**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

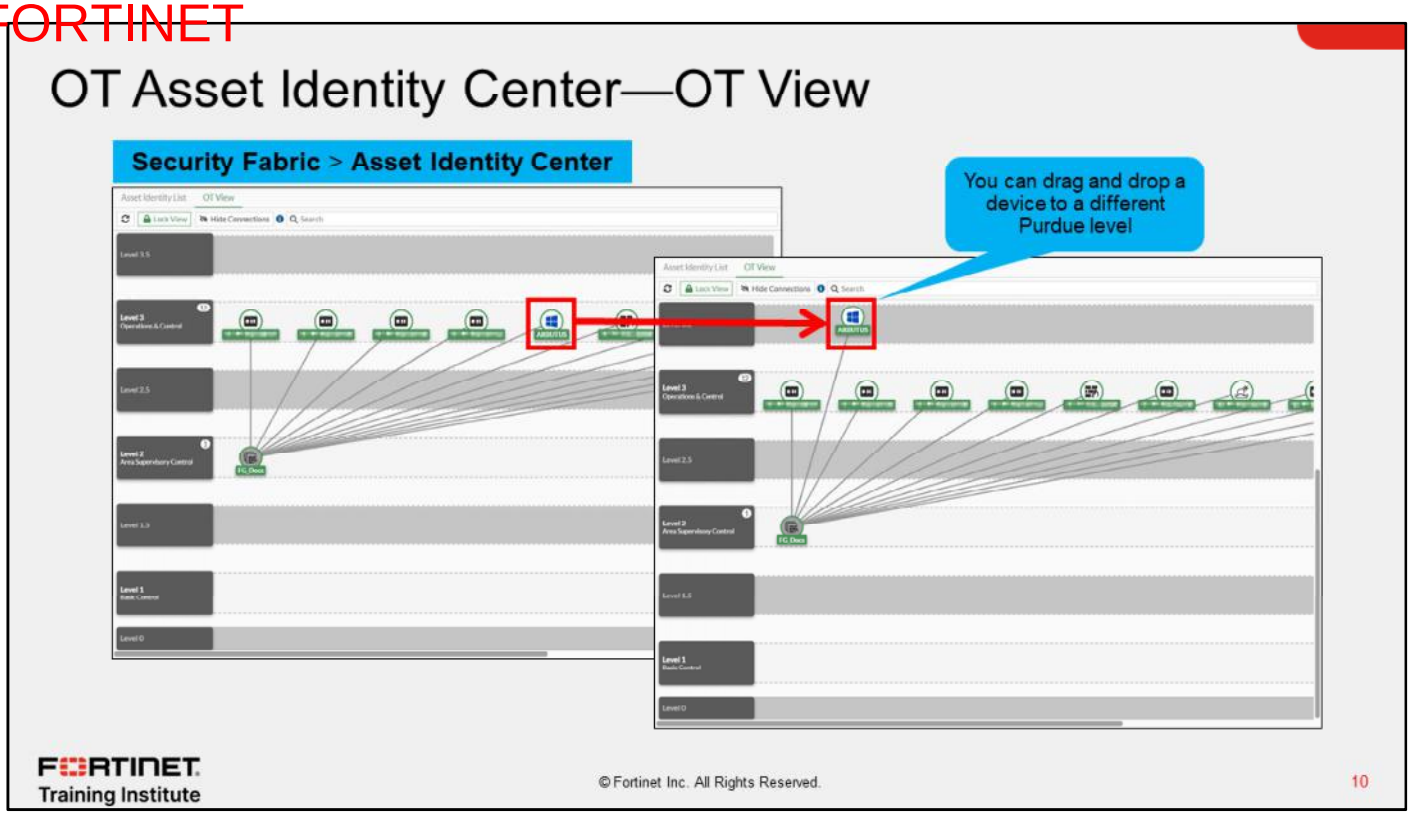
9

The two displays are **Asset Identity List** and **OT View**.

The **Asset Identity List** tab shows IT and OT devices and whether each is an asset or an identity. This tab also displays the current Purdue level for each device, which may change.

Select the **OT View** tab to display the devices in a Purdue diagram.

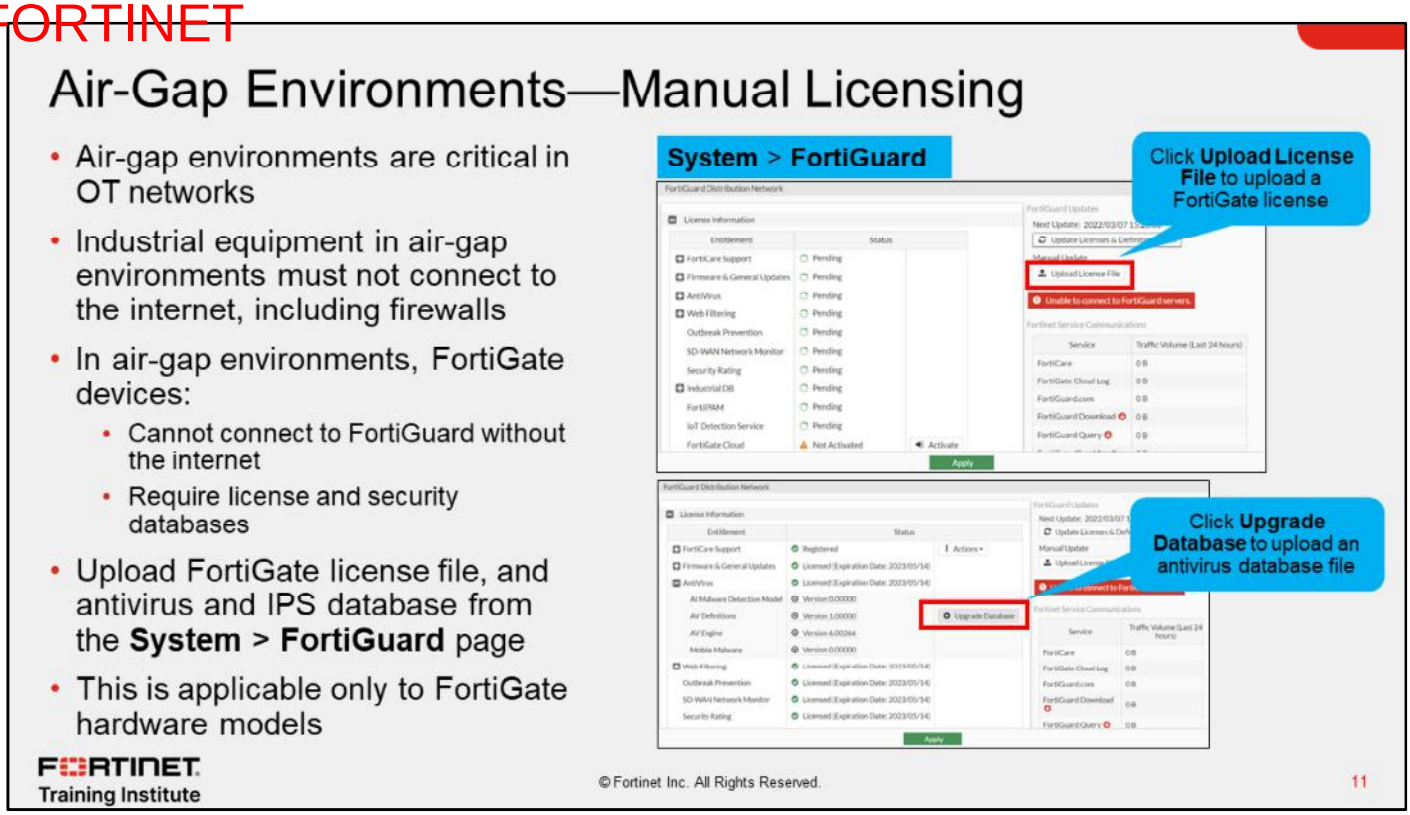
DO NOT REPRINT
© FORTINET



The **OT View** tab displays devices in a logical view, based on the Purdue level of each device. Each level is associated with the category that each device is classified.

You can drag and drop a device to a different Purdue level while preserving the logical links with other devices. By doing this, the current level of the device changes instantly on both the **OT View** tab and on the **Asset Identity List** tab.

DO NOT REPRINT
© FORTINET



FortiGate devices in any environment require an internet connection to obtain the required device license and security databases needed to protect these environments.

However, in air-gap environments, industrial equipment, including firewall devices, must not connect to the internet, because of the lack of an available external gateway.

You can manually upload a FortiGate device license as well as antivirus and IPS database files from the **System** > **FortiGuard** page. Note that this option is available on FortiGate hardware models.

DO NOT REPRINT
© FORTINET

IoT Device Detection—Signature Packages

- IoT devices include metadata when passing traffic
- FortiGate extracts metadata from the traffic generated by the IoT devices
  - It builds a table of IoT devices
  - The signature package version is important to update the table
- FortiGate uses the signature packages locally and does not pass information to network traffic



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

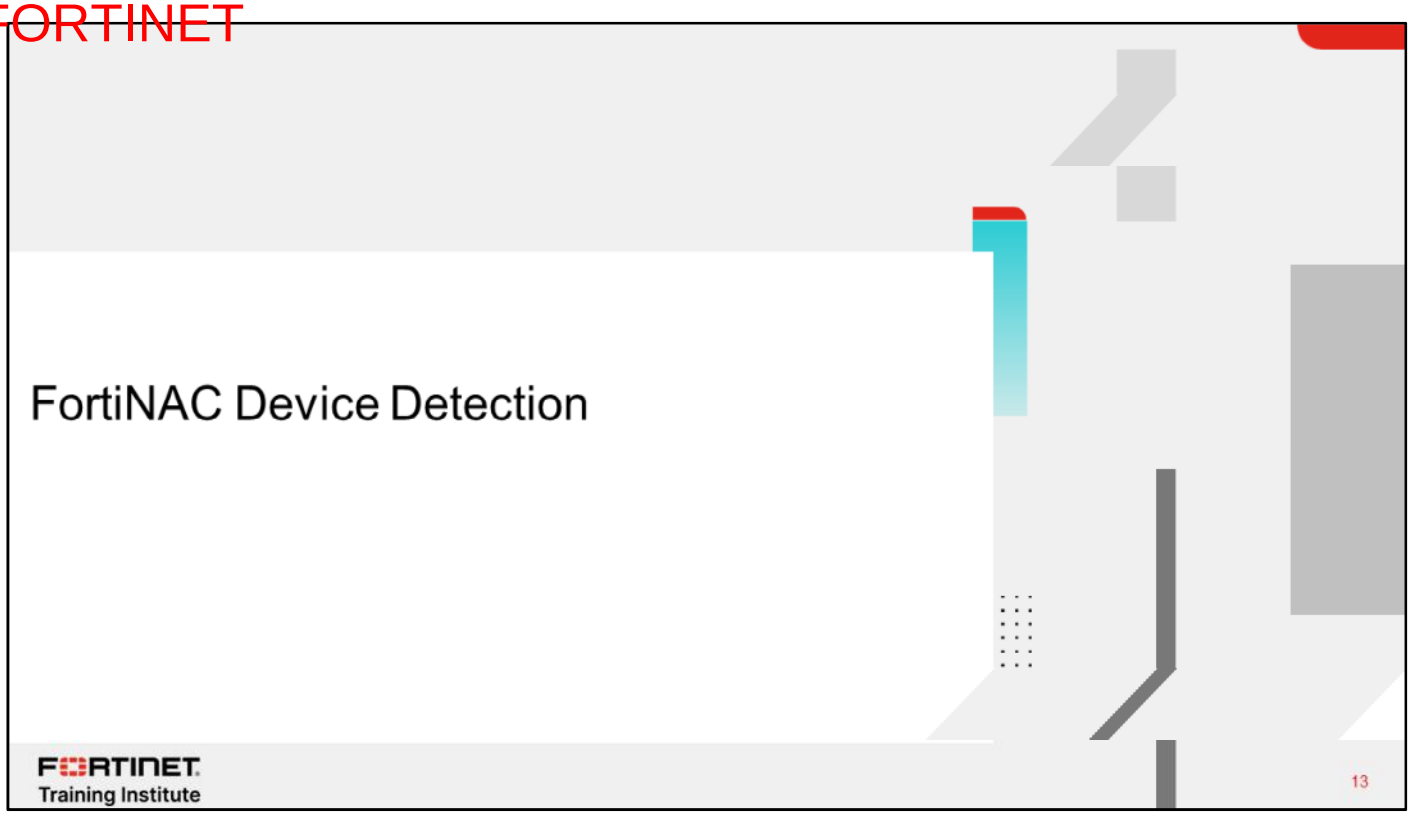
12

IoT devices generate data when sending traffic to the network. The data helps to identify more information about the device—for example, the operating system of the IoT device.

FortiGate uses IoT device detection to extract metadata using the traffic generated by the IoT devices, and maintains a list of devices locally. FortiGate cannot pass the information it collects to the network.

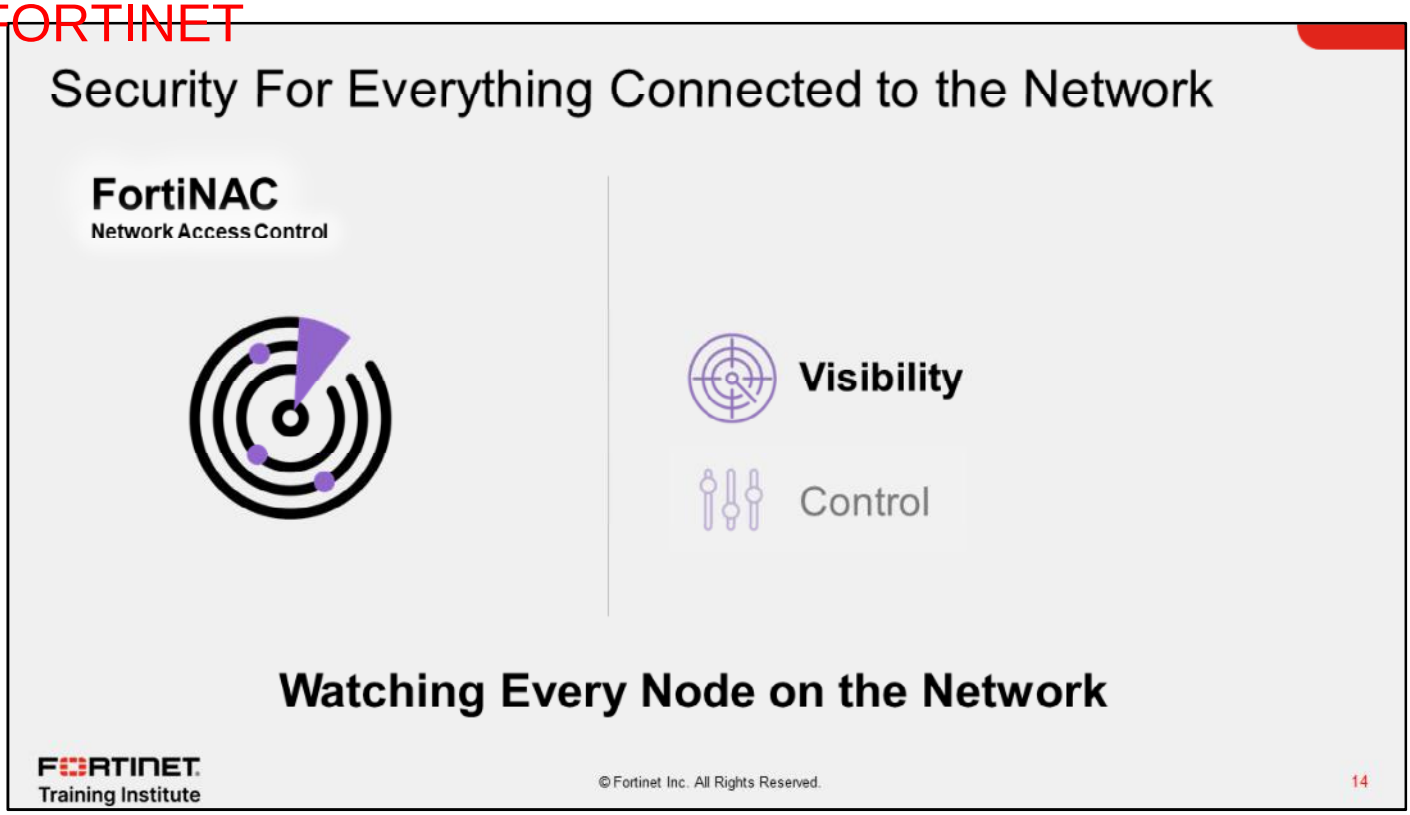
The IoT detection service is a license service and requires an internet connection to continue to receive updates for the signature packages from FortiGuard.

DO NOT REPRINT
© FORTINET



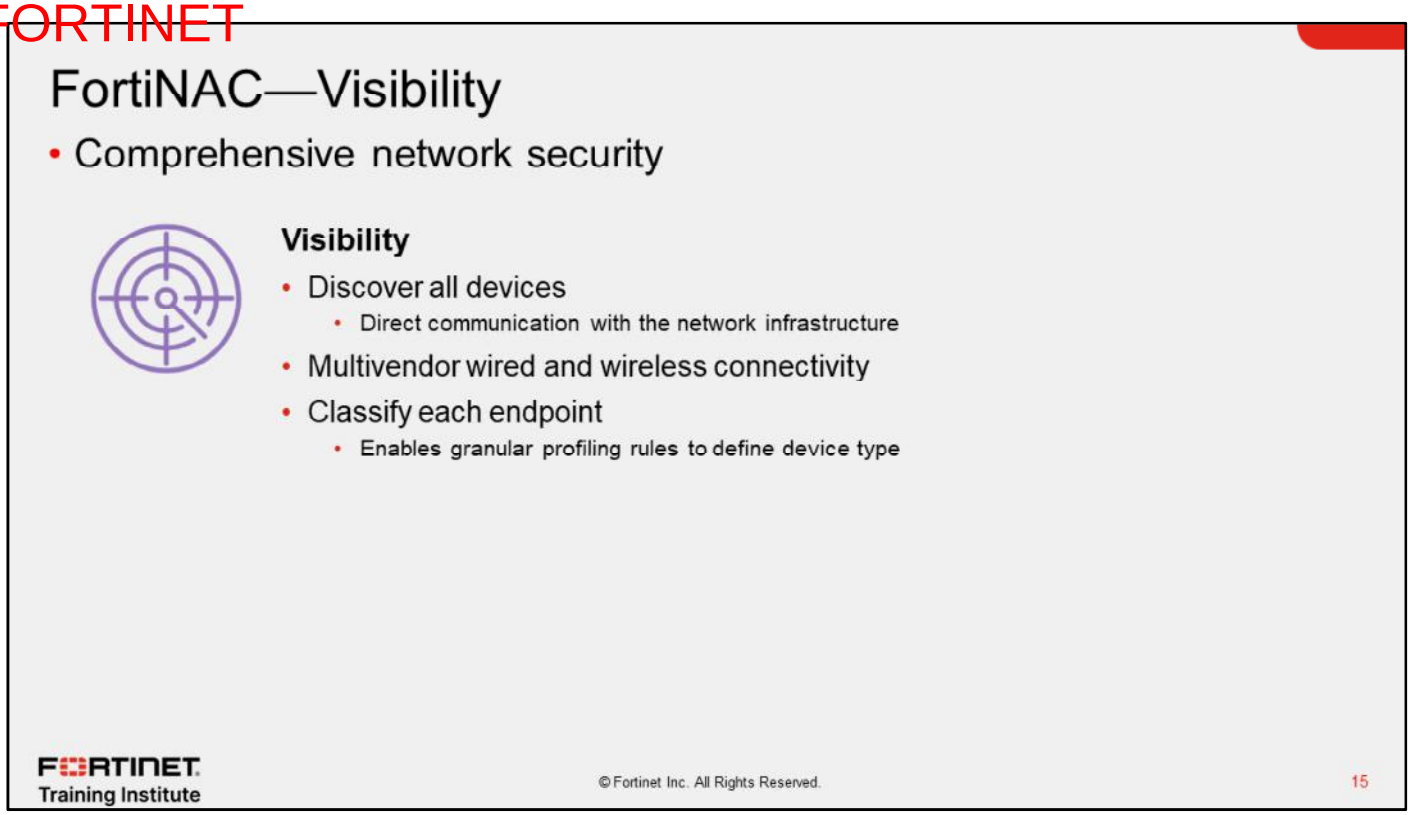
In this section, you will learn about different methods of device detection by FortiNAC.

DO NOT REPRINT
© FORTINET



In this course you will learn about two primary FortiNAC capabilities: visibility and control. This lesson focus on the visibility aspect, explaining how visibility is achieved and how devices become classified. The control capabilities are covered in another lesson.

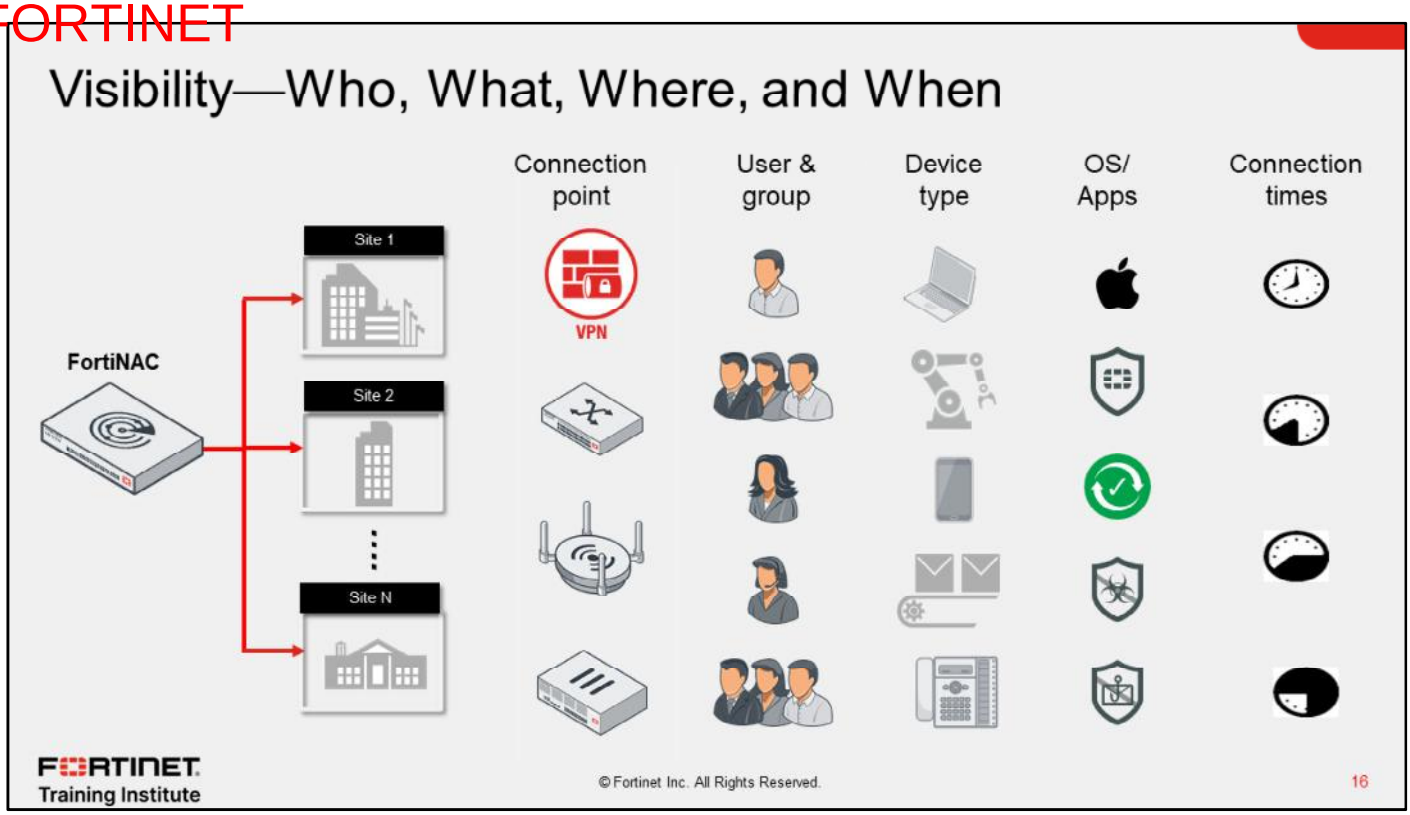
DO NOT REPRINT
© FORTINET



FortiNAC provides complete visibility of your network. This is achieved by communicating with the switches, access points, and firewalls to determine which end points are connected, and where they are connected.

Connected end points can then be classified using a variety of tools, most often the built-in device profiling tool. The device profiling tool leverages a large number of active and passive methods to accurately classify each end point.

DO NOT REPRINT
© FORTINET

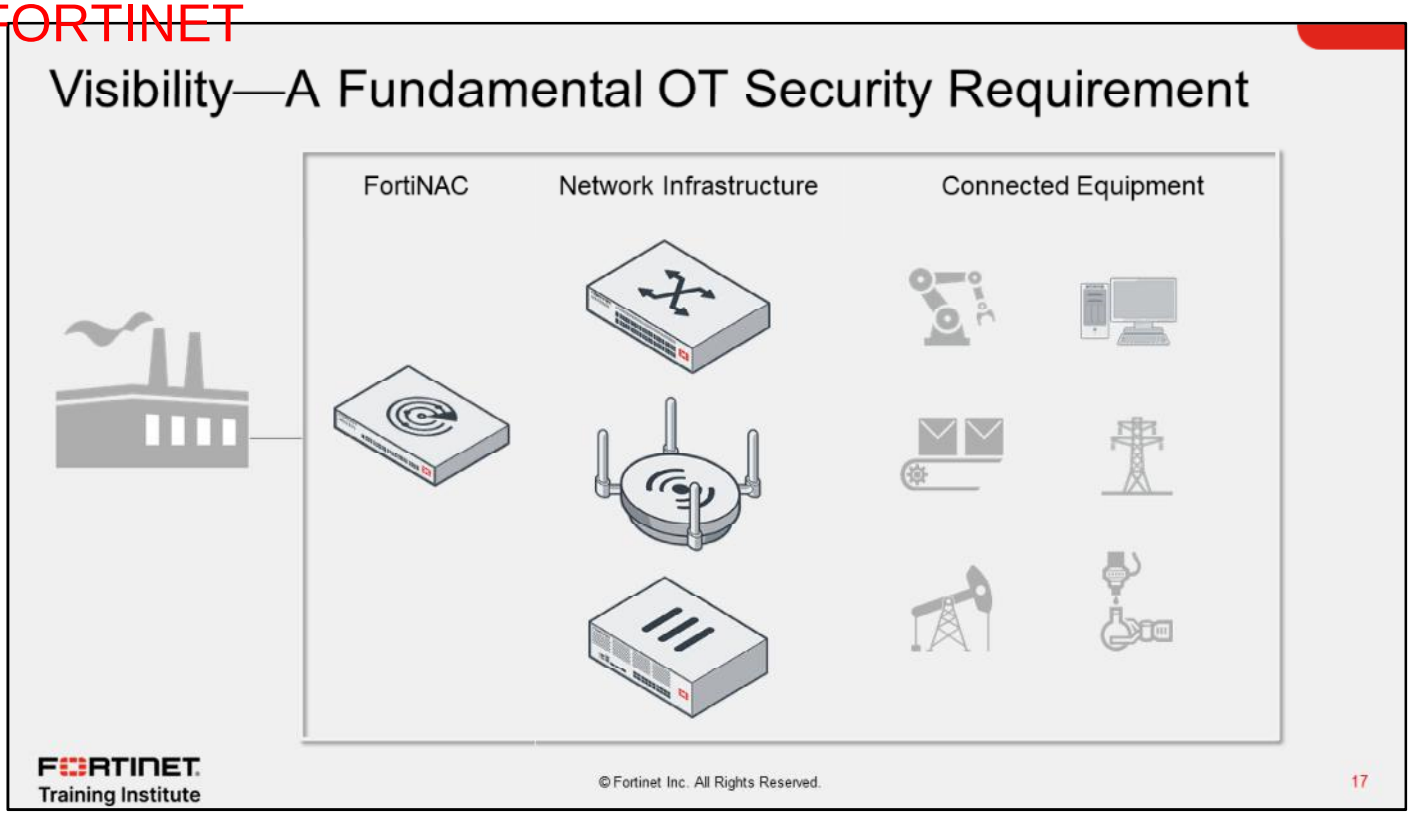


You can deploy FortiNAC as a physical device or as a virtual machine. To allow for streamlined deployments in high-security environments, you can license FortiNAC without internet access.

FortiNAC communicates with infrastructure devices, such as wireless controllers, autonomous APs, switches, routers, and others. Because these infrastructure devices are online, they can detect connected devices and connecting endpoints. They send this information back to FortiNAC, or FortiNAC gathers this information from them.

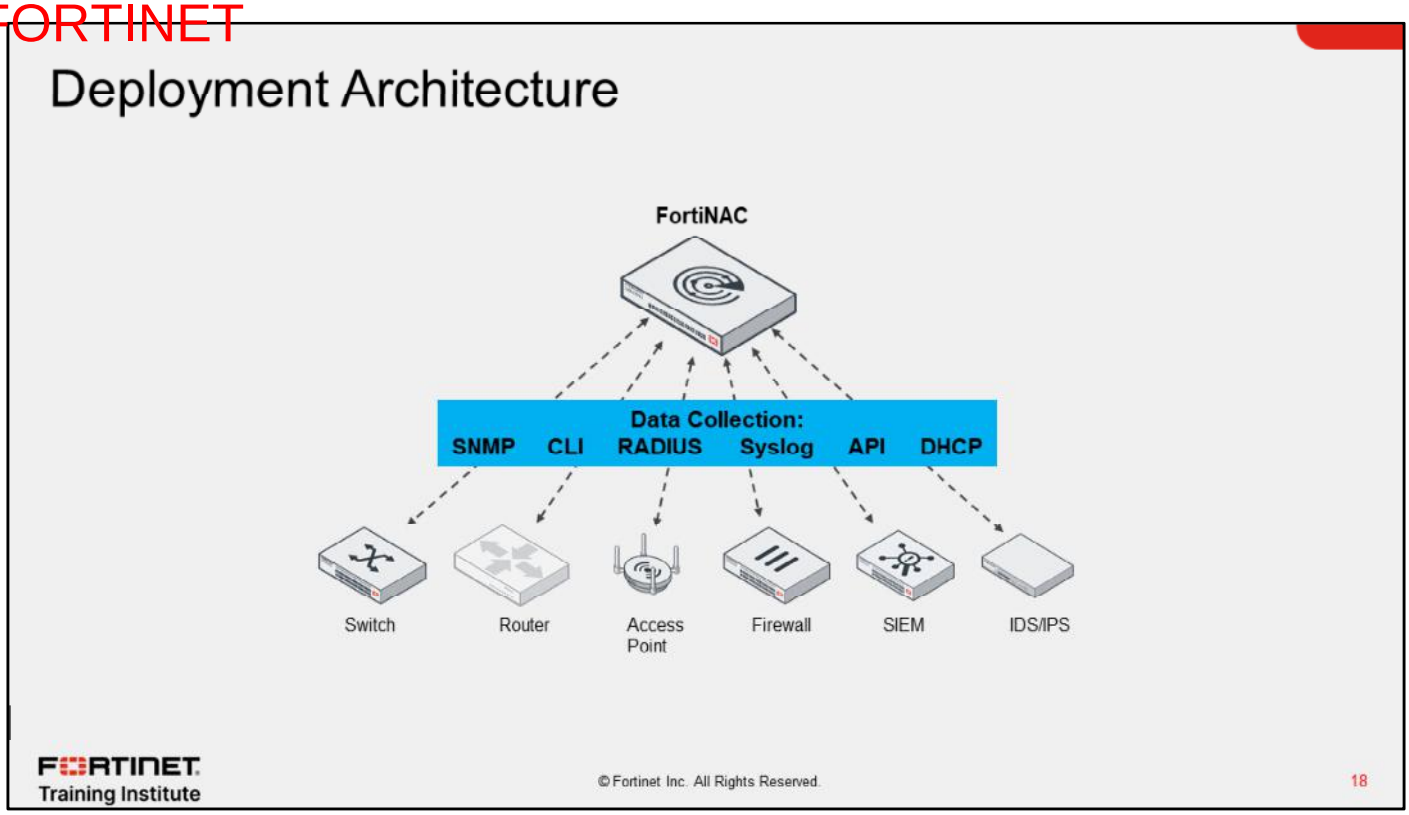
FortiNAC also gathers information passively by collecting information from sources like DHCP and RADIUS.

DO NOT REPRINT
© FORTINET



Visibility is a fundamental requirement for security. OT environments can consist of large numbers of specialized endpoints. For example, a manufacturing facility could use PLCs for the automation of robotics, conveyor belts, and other specialized machines for product assembly and movement, while the oil industry may use complex valve systems to manage pipelines. The identification and classification of these diverse assets must be complete and accurate in order to enforce secure access to the infrastructure. After classified assets can be granted access to appropriate resources, and unknown endpoints can be denied. To this end, FortiNAC communicates directly with infrastructure devices, such as wireless controllers, autonomous APs, switches, routers, firewalls, and others. Because these infrastructure devices are in line, they see all connected endpoints because they connect or disconnect form the infrastructure. They send this information back to FortiNAC, or FortiNAC gathers this information from them. FortiNAC will then understand, in real time, exactly what is connected to the infrastructure, and where it is connected. These capabilities allow FortiNAC to provide valuable visibility at all levels of an ICS architecture.

DO NOT REPRINT
© FORTINET

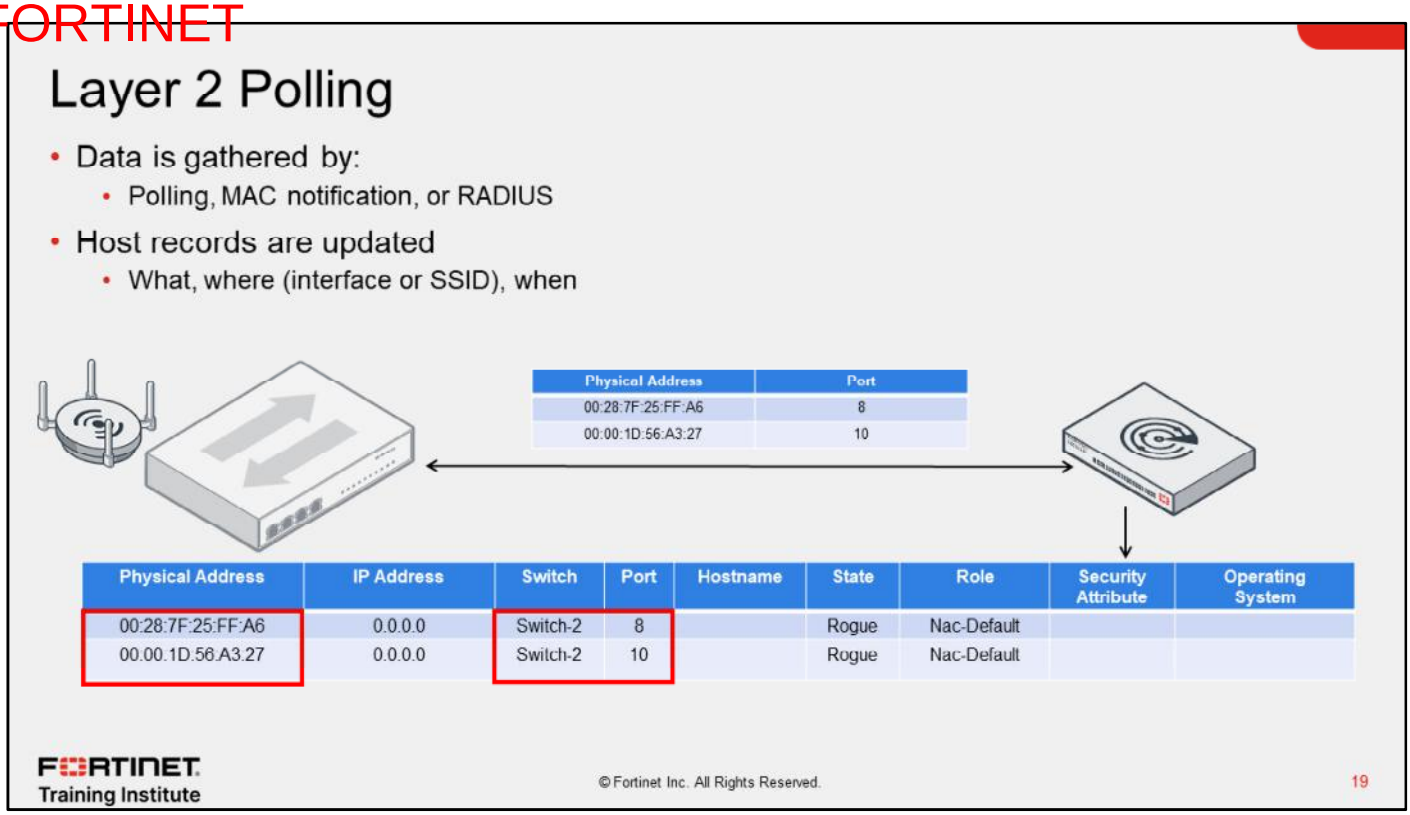


FortiNAC uses a variety of methods to communicate with and gather information from the infrastructure:

- FortiNAC uses SNMP to discover the infrastructure, complete data collection, and perform on going management.
- SSH or Telnet through the CLI is commonly used to complete tasks related to the infrastructure. For example, FortiNAC can use SSH to connect to a device and issue commands to gather visibility information or execute control functions.
- FortiNAC can also use RADIUS, across a wired or wireless connection, to gather visibility information and control access.
- FortiNAC uses Syslog to stay up to date on visibility details, such as hosts going off-line. Syslog can also provide security device integration, giving FortiNAC the ability to log and react, if configured to do so, when it receives a security alert.
- Depending on the vendor of the infrastructure device, FortiNAC may leverage available API capabilities to enhance visibility and enforce control.
- FortiNAC can use DHCP, typically through fingerprinting, to identify connected devices and gain enhanced visibility.

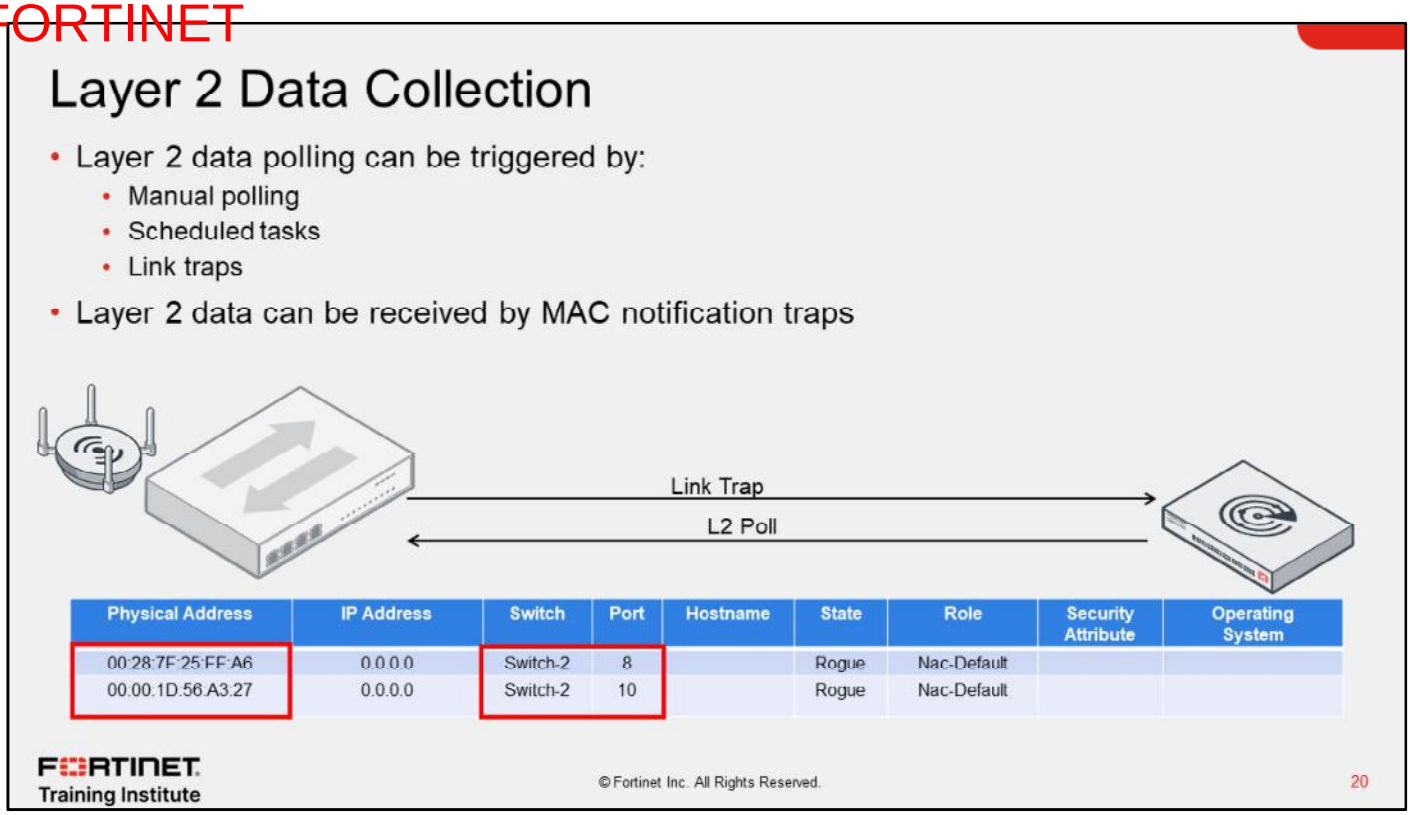
The communication methods that FortiNAC uses depend on the vender and model of the infrastructure device that FortiNAC is trying to integrate with. After FortiNAC knows the type of device it is communicating with, it determines and uses the appropriate methods and commands to gather information and maintain control.

DO NOT REPRINT
© FORTINET



Because each physical address is unique, FortiNAC can identify hosts as they connect to the network. FortiNAC uses the information that it gathers when it identifies a host to fill in the physical address and location information in the database.
The information is gathered through the polling of the infrastructure device acting as the point of connection for the endpoint, or through the receipt of a MAC notification trap or RADIUS request sent to FortiNAC from the device that an endpoint has connected to.
The physical address that was learned, the time it was learned, and where it was learned from, provide the beginnings of endpoint visibility in the form of what, where, and when information.

DO NOT REPRINT
© FORTINET



The three ways that Layer 2 polling is triggered are:

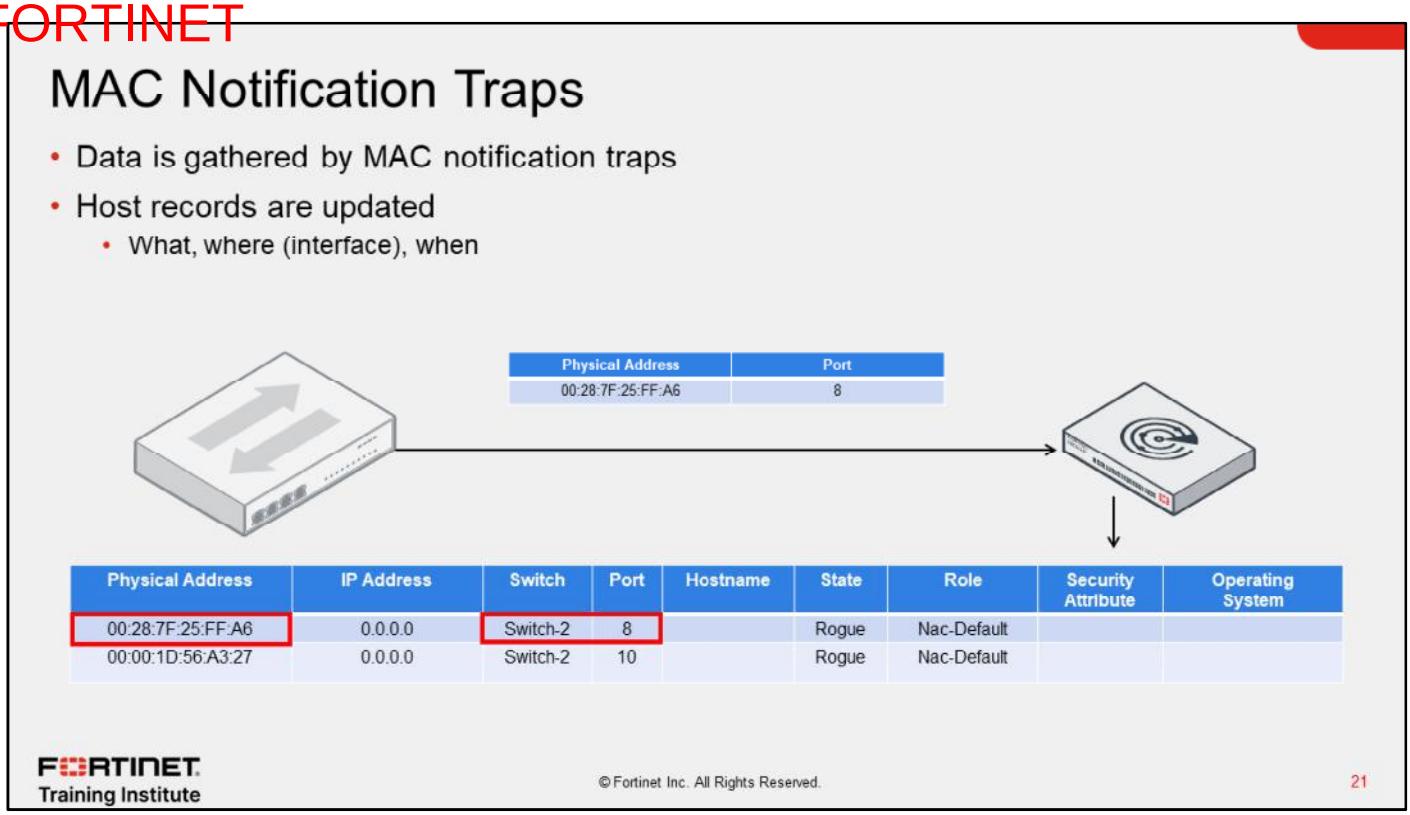
- Manual polling: Manual polling is initiated when an administrative user right-clicks the switch in the inventory view and selects **Poll for L2 (Hosts) info**, or clicks **Network** > **L2 Polling**.
- Scheduled: Layer 2 polling is scheduled in the **Networks** > **L2 Polling** view, which you select in the **Network Devices** drop-down list. You can change the default scheduled intervals.
- Link Traps: Link traps received from an edge device trigger FortiNAC to perform an Layer 2 poll to update its awareness of devices that are connected on that edge device. The traps that trigger the poll are: Linkup, Linkdown, WarmStart, and ColdStart. This trigger keeps FortiNAC up to date in real-time as devices connect to and disconnect from edge devices.

You can also collect Layer 2 data from MAC notification traps. When an edge device issues a MAC notification trap to FortiNAC, the notification contains the MAC address that was just learned or removed from the MAC address table of the edge device, as well as the port that MAC address was associated with. FortiNAC can then update its database with the new information.

MAC notification traps are the preferred method for learning and updating Layer 2 information and you should always use them when they are an option. Receiving and processing MAC notification traps is much less resource intensive than having to contact and query an edge device.

You should not configure link traps to be sent to FortiNAC on devices that have MAC notification traps configured. You should not configure MAC notification traps on interfaces that are uplinks.

DO NOT REPRINT
© FORTINET

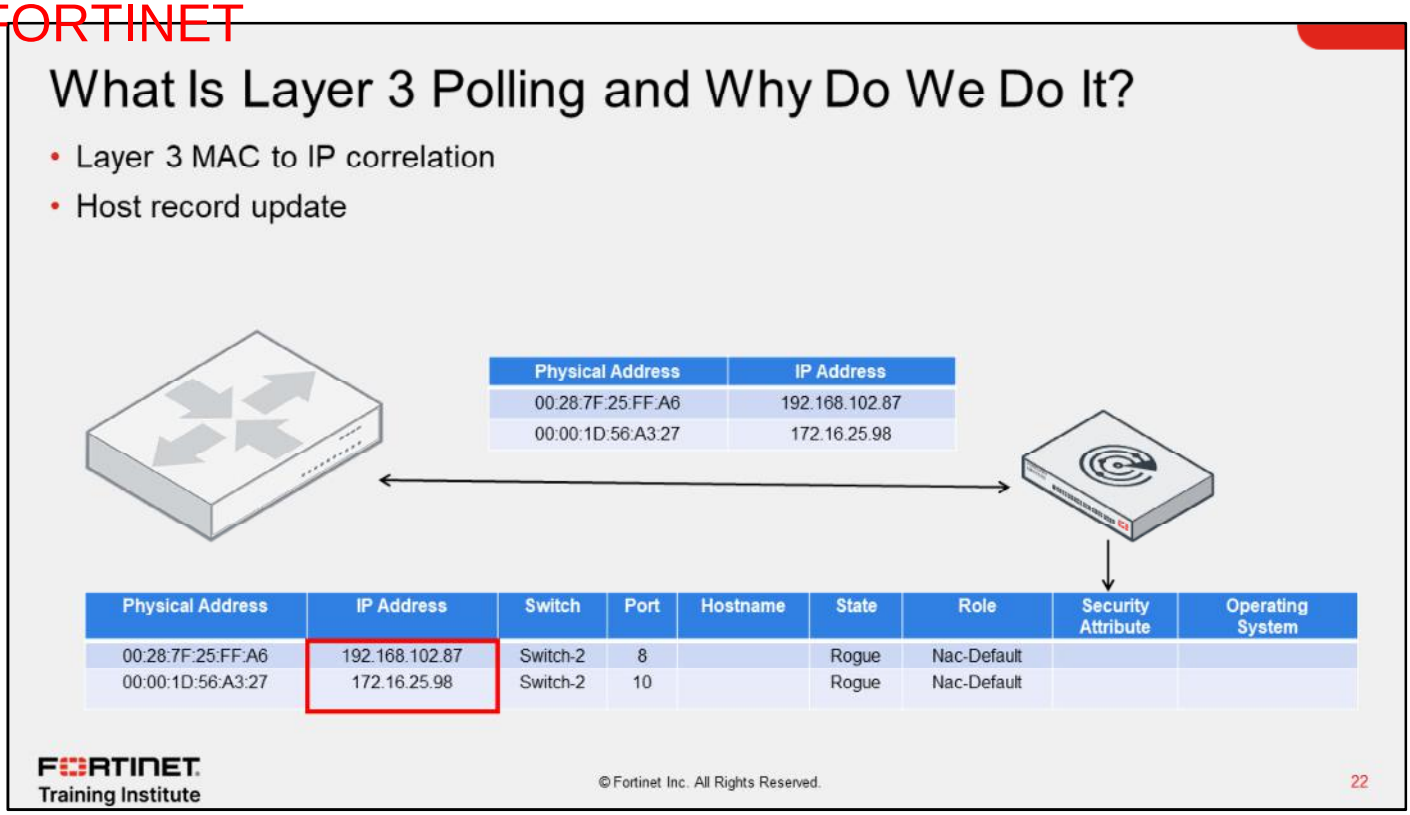


MAC notification traps offer, with specific vendors, an alternative and preferred method of Layer 2 data gathering. A MAC notification trap is generated by the infrastructure device when a new MAC address is learned or removed from its MAC address table.

There are a couple of reasons why MAC notification traps are preferred over link up and link down traps and why you should always use them whenever possible:

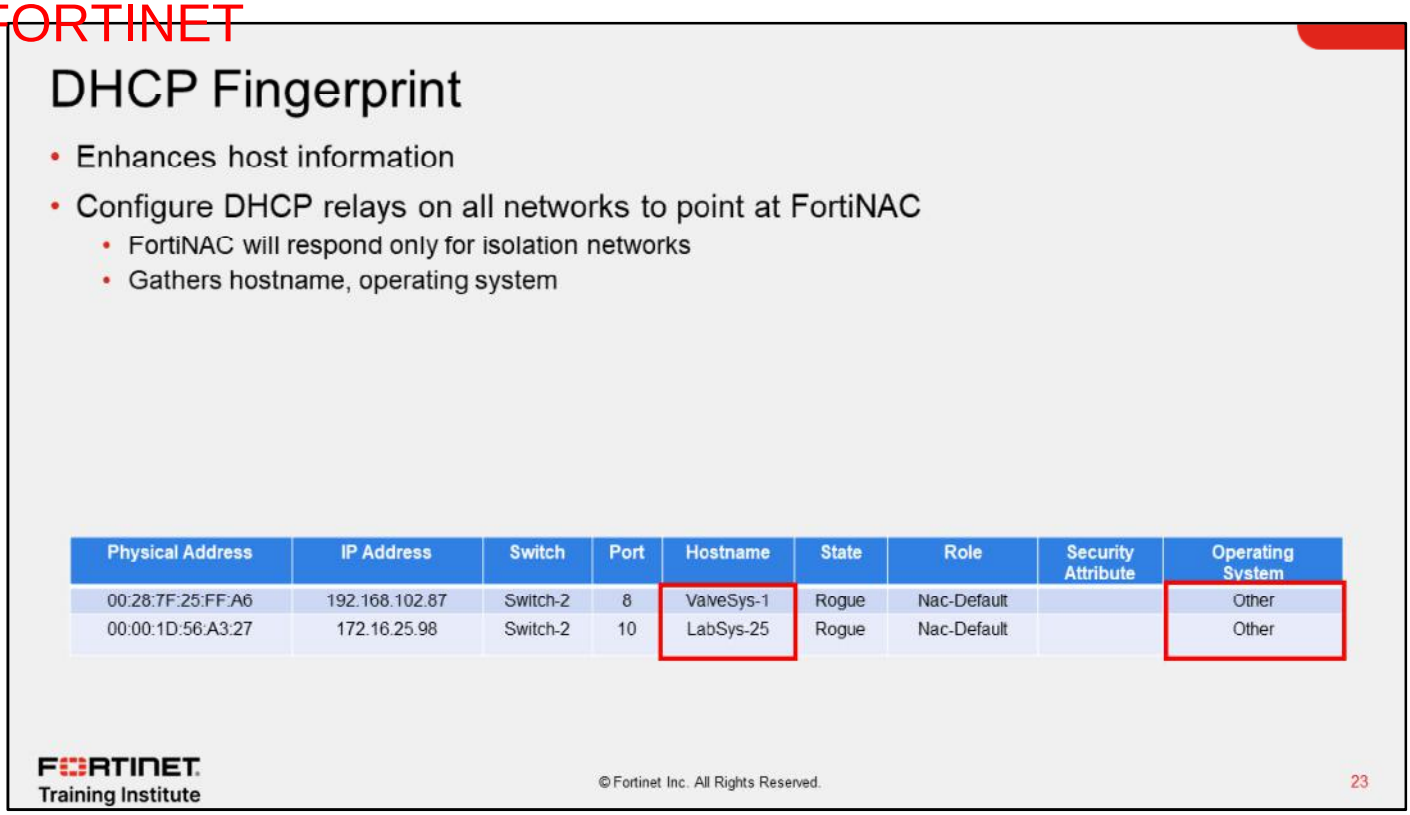
- First, FortiNAC no longer needs to establish a connection to the infrastructure device each time a link up or link down trap is received because the required information is included in the MAC notification trap. This makes database updates faster and demands fewer resources.
- Second, hosts and devices that connect through hubs or IP phones will be seen immediately, even if the device they connected to can't generate link up or link down traps.

DO NOT REPRINT
© FORTINET



Layer 3 IP address information is a critical piece of network visibility and is a necessary component for some FortiNAC capabilities. As devices are added or discovered, they are automatically added into the **L2 Wired Devices** or **L2 Wireless Devices** groups. These groups are nested as subgroups of the **L2 Network Devices** group. A default **L3 (IP --> MAC Devices)** group is created by FortiNAC, but it may not be automatically populated. You may add your Layer 3 devices to this group. The polling of devices in the Layer 3 device group is performed on a scheduled basis and the correlated IP address is added to the database record for the corresponding MAC address.

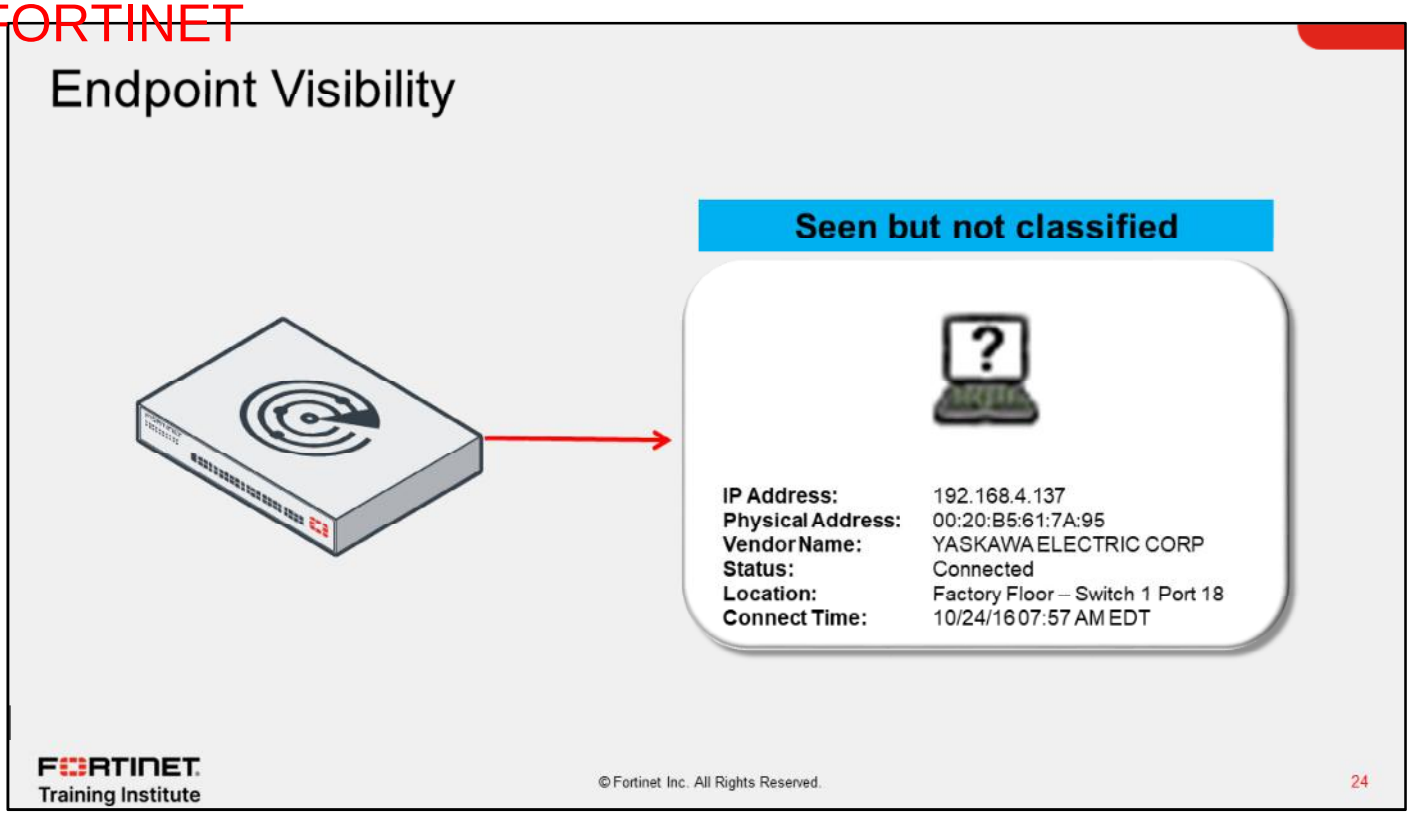
DO NOT REPRINT
© FORTINET



Configuring FortiNAC as an additional DHCP server using DHCP relays throughout an environment will result in FortiNAC receiving copies of DHCP discovery and request packets. FortiNAC will never respond to the packets forwarded to it from production networks because it should never have DHCP scopes configured on it for those networks. Once received, FortiNAC can parse the contents of each DHCP discovery or request and identify, based on parameters in the packet, the originating host's hostname and operating system. This information will be used to update and enhance the visibility information stored in the database.

This added visibility can also be used to generate notifications when hostnames or host operating systems change.

DO NOT REPRINT
© FORTINET



Endpoint visibility is the information gathered about endpoints connected or previously connected to the network. Endpoint visibility information usually includes all or some of following information:

- The MAC or physical address, which is gathered using Layer 2 polling or MAC notification traps
- The network or IP address, which is gathered using Layer 3 polling
- Its current or last location on the network, which is known through Layer 2 polling
- Connection status (connected or disconnected) and the connect and disconnect times, which is based on L2 polling
- The vendor name, which is based on the vendor OUI of the MAC address. (FortiNAC has a current list of vendor OUIs in the database.)
- The hostname and operating system, which is gathered from DHCP fingerprinting

Endpoint visibility and details do not define device trust. Trust is defined through the classification of each endpoint.

DO NOT REPRINT
© FORTINET

Rogue Devices

- Any device that has not been classified within FortiNAC
- Displayed as a PC with a question mark on the screen
- A host state enforced with the Forced Registration port group



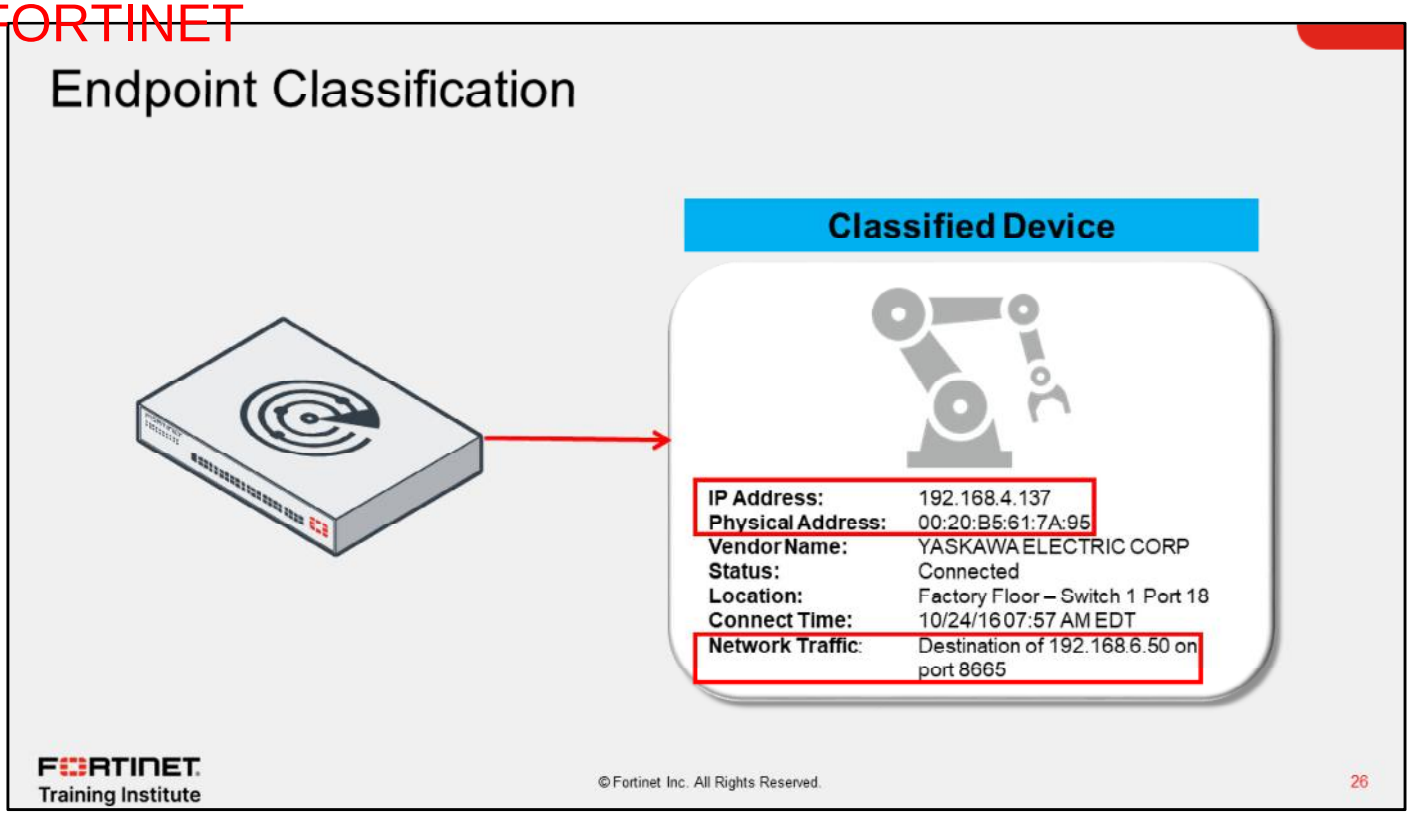
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

A rogue device is a physical address that has been seen on the network but has not been associated with an existing known device and is therefore considered unknown. On the GUI, FortiNAC represents a rogue device as a laptop image with a question mark on the screen. Rogue devices are often referred to as *unknown* or *untrusted* endpoints, they have not been classified. The default logical network called **Registration** is the method used to isolate rogue hosts at the point of connection when enforcement is enabled.

DO NOT REPRINT
© FORTINET



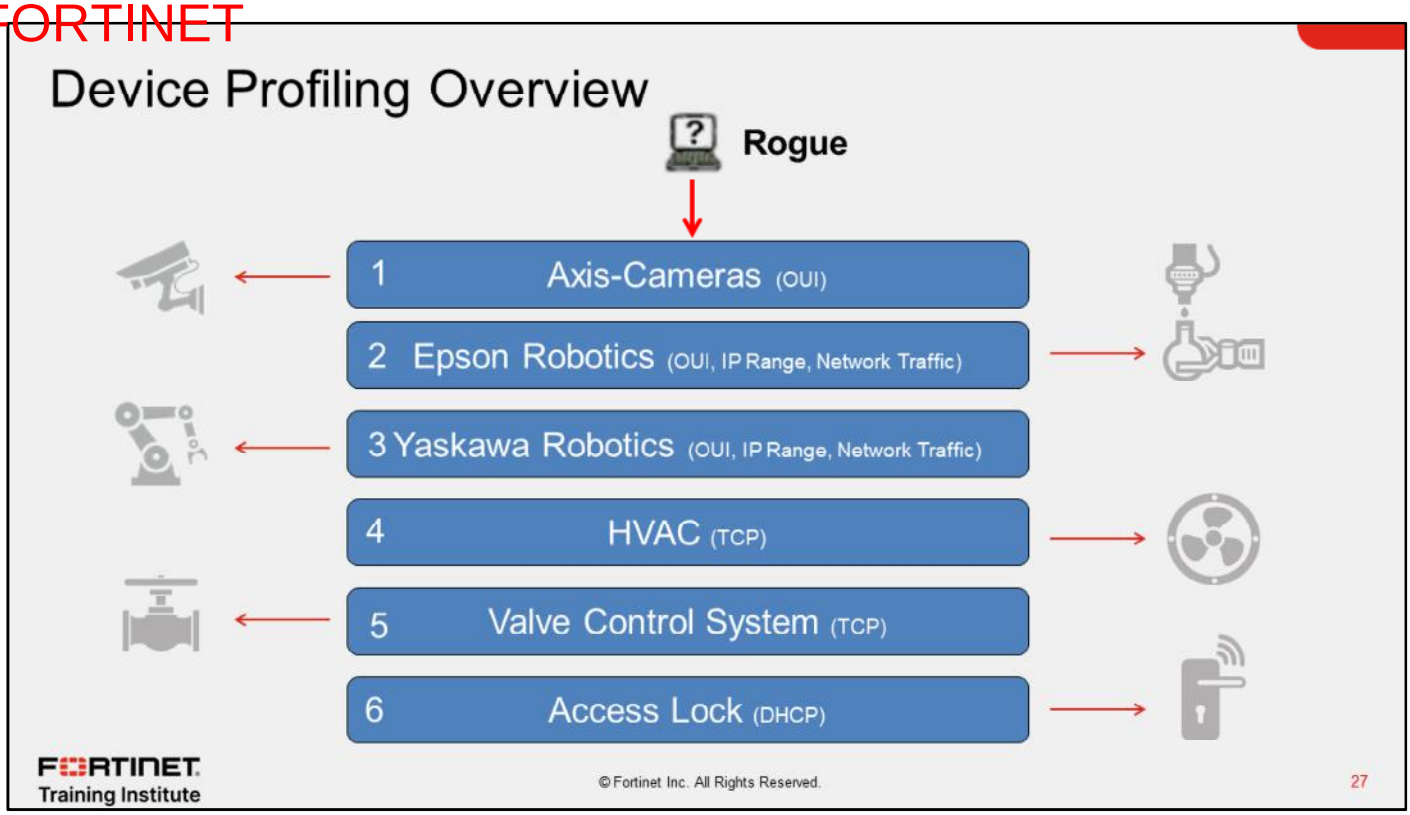
A foundation of visibility is created from the information that FortiNAC gathers from endpoints. Endpoints are a collection of elements: IP addresses, physical addresses, vendor names, statuses, and so on. However, having this information about endpoints does not classify them as trusted devices. One tool used to classify connected devices is the device profiling tool. The device profiling tool uses administratively created rules that identify what's connected to the network using one or more methods that identify the type of device. In the example shown on this slide, there is a rule called Yaskawa Robotics that uses OUI, IP address range and network traffic. This will identify devices as they connect to the network by validating the vendor OUI of the device, the IP address it has been assigned and what it is communicating with and the port used for that communication. This information can result in a change in classification from unknown rogue device to a trusted device, in this case, a Yaskawa robotics device.

You can create rules, as needed, for each different type of device that requires classification. An industrial device rule, for example, may use **Vendor OUI** and **Network Traffic**, which means FortiNAC first verifies the device OUI and then validates network traffic information, such as protocol, destination port, and destination IP. When FortiNAC evaluates the gathered information and compares it to a pre-set list in the database to determine if it is a match for the selected device type. You can also enter user-defined values to allow for detailed device-specific customizations.

You can use multiple methods for more robust rule creation.

Endpoints that are classified are also known as registered hosts, because they are now considered registered in the system and trusted.

DO NOT REPRINT
© FORTINET



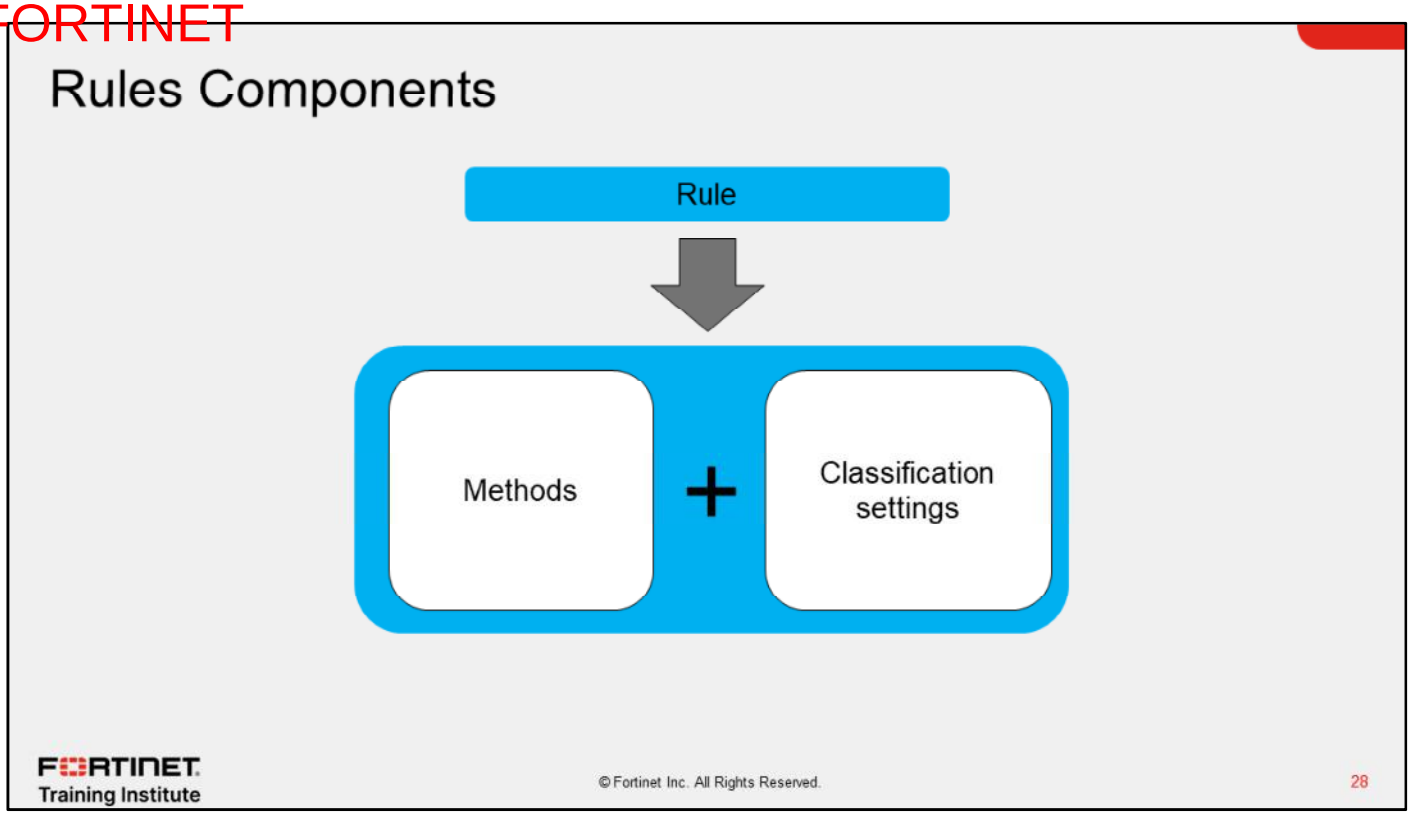
When a rogue device record is created, the device is evaluated against the enabled device profiling rules. FortiNAC evaluates a device against each rule until a fail, pass, or cannot evaluate result is reached.

The following is an example list of rules and the methods used to validate each rule. They are prioritized for efficient processing and specific identification:

- Rule 1, called Axis-Cameras, uses a single validation method: Vendor OUI
- Rule 2, called Epson Robotics, uses three methods: Vendor OUI, IP Range and Network Traffic
- Rule 3, called Yaskawa Robotics, also uses Vendor OUI, IP Range and Network Traffic
- Rule 4, called HVAC, uses a single method: TCP
- Rule 5, called Valve Control System, uses a single method: TCP
- Rule 6, called Access, uses a single method: DHCP fingerprint

Next, you will take a closer look at the components of a device profiling rule.

DO NOT REPRINT
© FORTINET

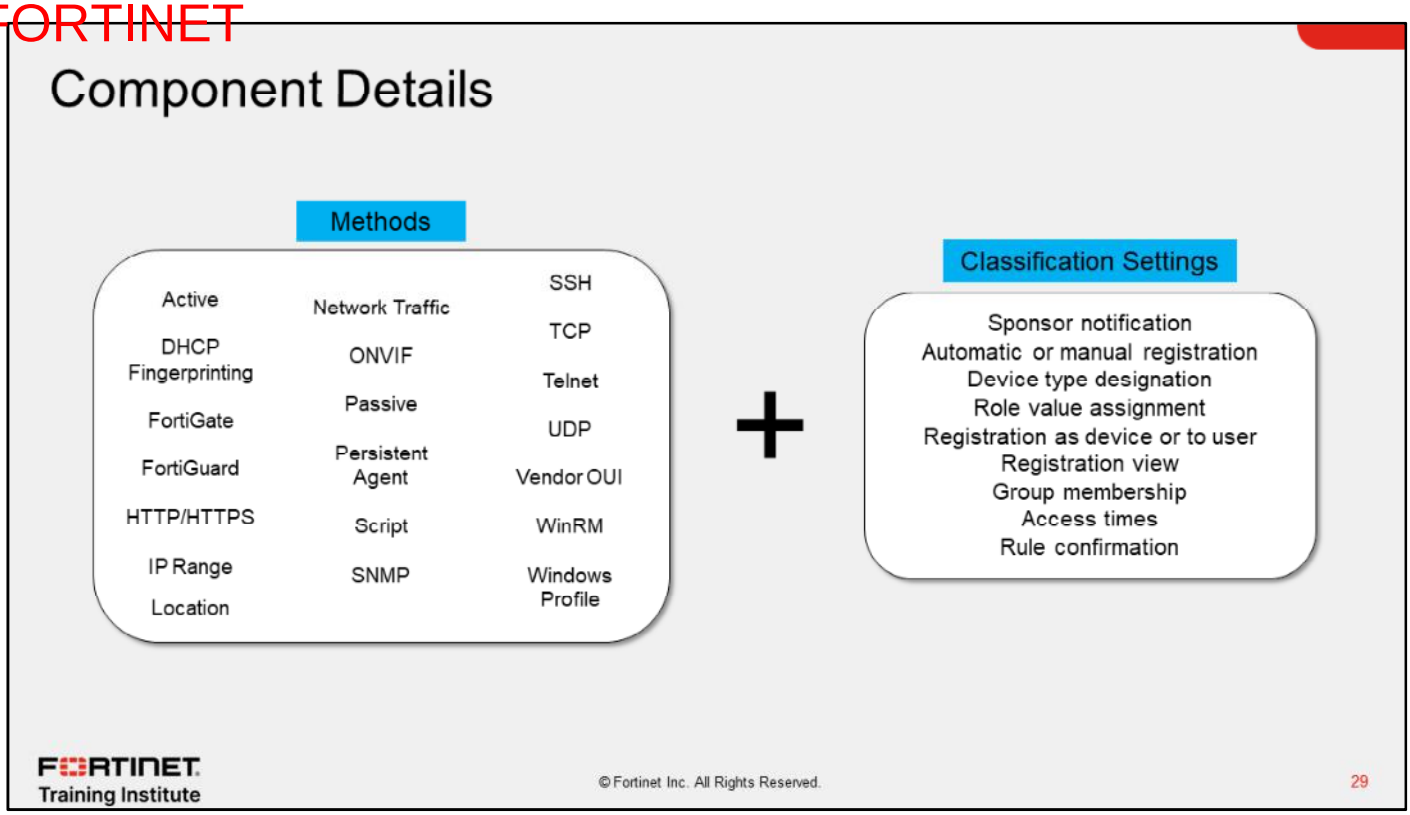


Device profiling rules are used to evaluate and classify rogue devices. You can configure profiling rules to automatically, manually, or through sponsorship, evaluate and classify unknown, untrusted devices as they are identified and created.

Device profiling leverages rules comprising classification settings and methods used for evaluation.

FortiNAC uses the rule methods to evaluate devices to test for a pass or fail result. If all selected methods result in a pass result, then FortiNAC applies the rule-defined classification settings of device type, grouping, and attribute values.

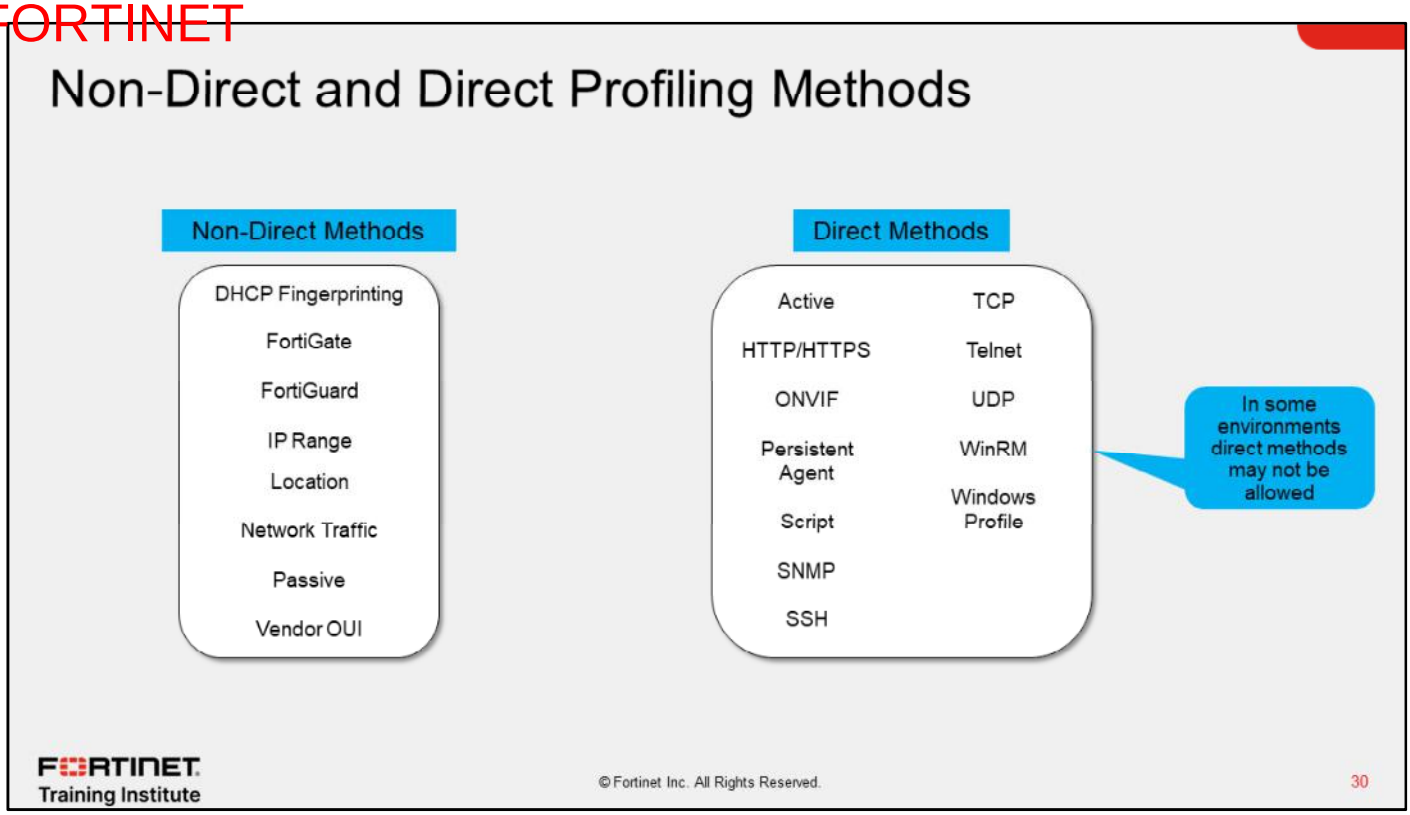
DO NOT REPRINT
© FORTINET



The methods shown on this slide are used to evaluate devices during profiling. If more than one method is selected, the selected methods are logically ANDED when determining if the rule is matched. Match criteria are configured for each method, as the methods are selected.

The classification settings define how FortiNAC will classify the connected device and how it will appear in the GUI. You can leverage the device type, role, and group membership for policy enforcement. You can use access availability settings to grant networks access during specific days and times, and the **Rule Confirmation** option to revalidate previously profiled devices.

DO NOT REPRINT
© FORTINET



In certain environments, direct engagement of endpoints during profiling may be unacceptable, and could even have a negative impact on performance. For this reason it is good to understand which methods do not require FortiNAC to interact with the device being profiled. The methods that *do not* directly interact with a device during profiling are:

- **DHCP Fingerprint**: Determined by DHCP discover or request information
- **FortiGate**: Leverages FortiGate session information, gathered from FortiGate
- **FortiGuard**: Based MAC address information gathered from the infrastructure and the FortiGuard IoT database
- **IP Range**: Determined based on IP address gathered from infrastructure
- **Location**: Based on point of connection learned from infrastructure
- **Network Traffic**: Gathered from infrastructure
- **Passive**: Based on traffic generated by the device being profiled
- **Vendor OUI**: Determined by MAC address gathered from infrastructure

All other methods will directly scan or directly interact with the device being profiled.

DO NOT REPRINT
© FORTINET



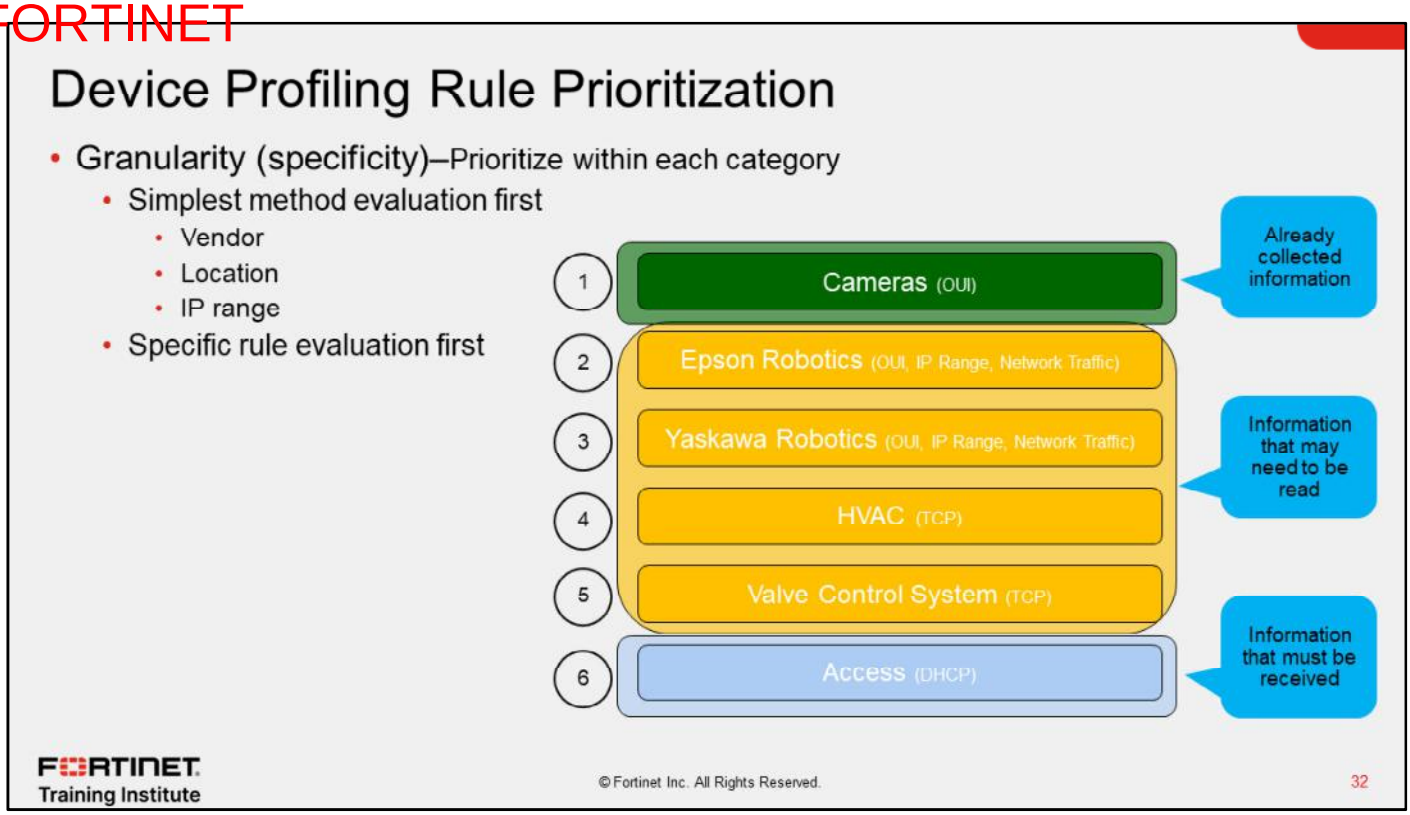
Efficient and specific ranking of the rules is important to avoid a cannot evaluate result.
FortiNAC evaluates a device against each rule until a pass, fail, or cannot evaluate (because of insufficient data) result is reached.

- A rule evaluation result of pass classifies the device as defined by the rule classification settings.
- A rule evaluation result of fail continues the device evaluation process with the next ranked rule.
- A rule evaluation result of cannot evaluate stops the device evaluation process. This occurs when a method within the rule requires data that is not available or able to be validated as current.

As a best practice, categorize rules fall into the three prioritized groups, which should, in most cases, follow these guidelines:

- Place rules with vendor OUI and/or location methods only in the Already Collected group.
- Place rules with one or more IP-based methods in the Needs to be Read group,
- Place any rules that use DHCP methods in the Must be Received group.

DO NOT REPRINT
© FORTINET

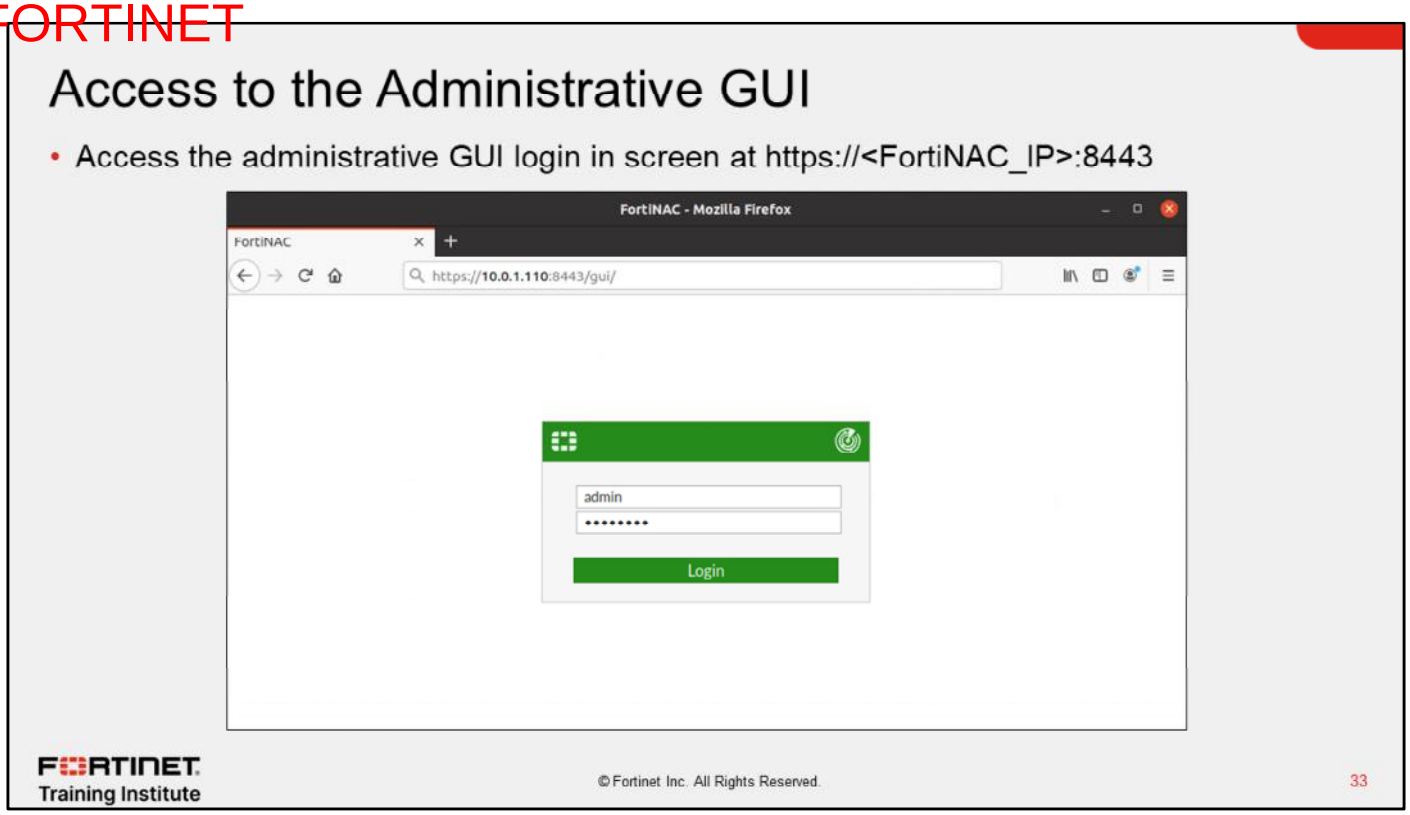


Within each group organize the rules based on granularity.

Here is the result of following those guidelines with these example rules:

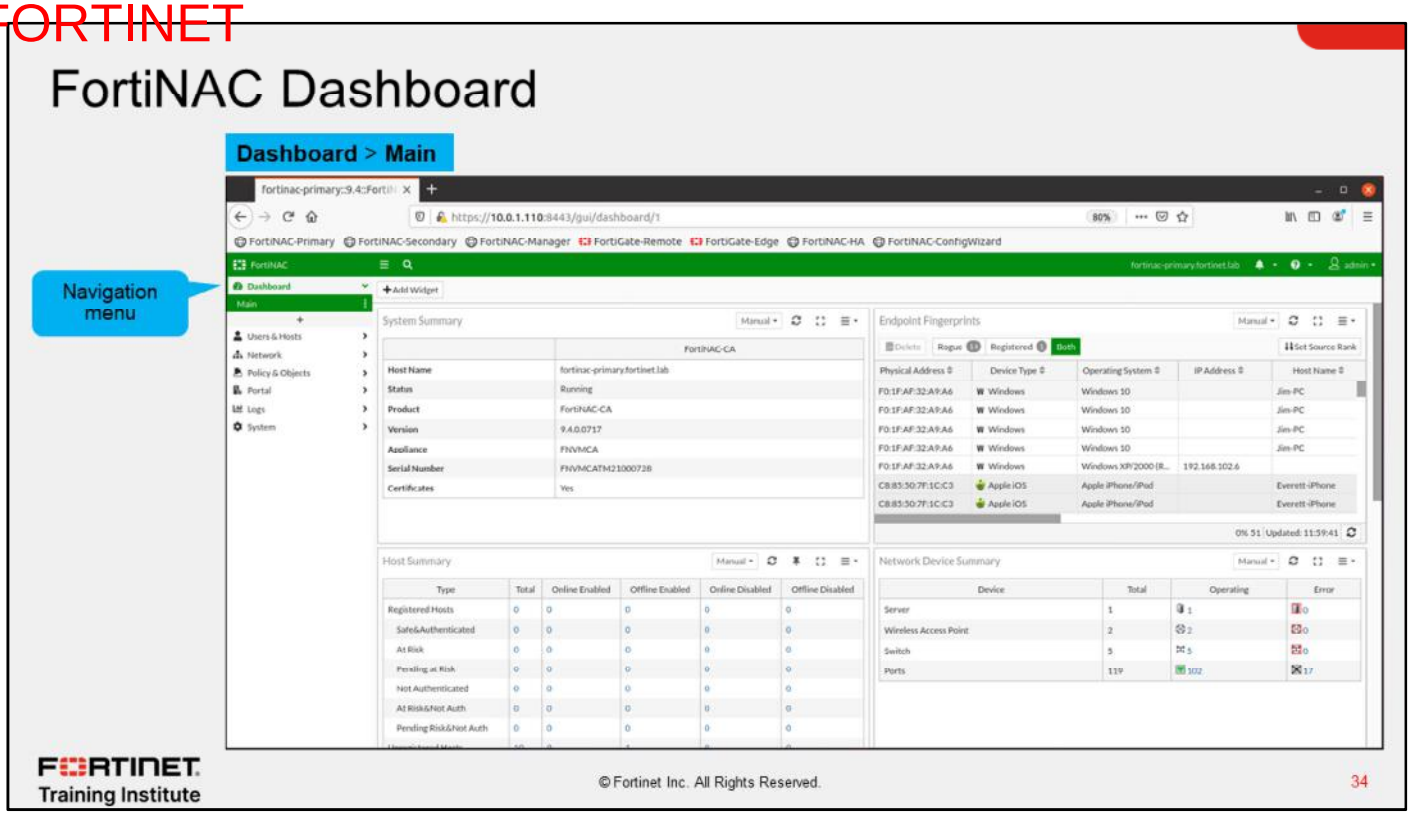
- Rule 1 OUI evaluation result is the simplest path to failure, resulting in the lowest overhead to validate.
- Rule 2 is the evaluation of IP range and network traffic that is done only if OUI matches. This prevents unnecessary processing of devices that don't have the correct vendor OUI.
- Rule 3 is configured using the same methods as rule two.
- Rule 4 and 5 evaluate open TCP ports, requiring active scanning of each device evaluated.
- Rule 6 is efficiently ordered because DHCP fingerprint receipt is not controlled by FortiNAC and could stop rule evaluation (cannot evaluate) if no fingerprint is received.

DO NOT REPRINT
© FORTINET



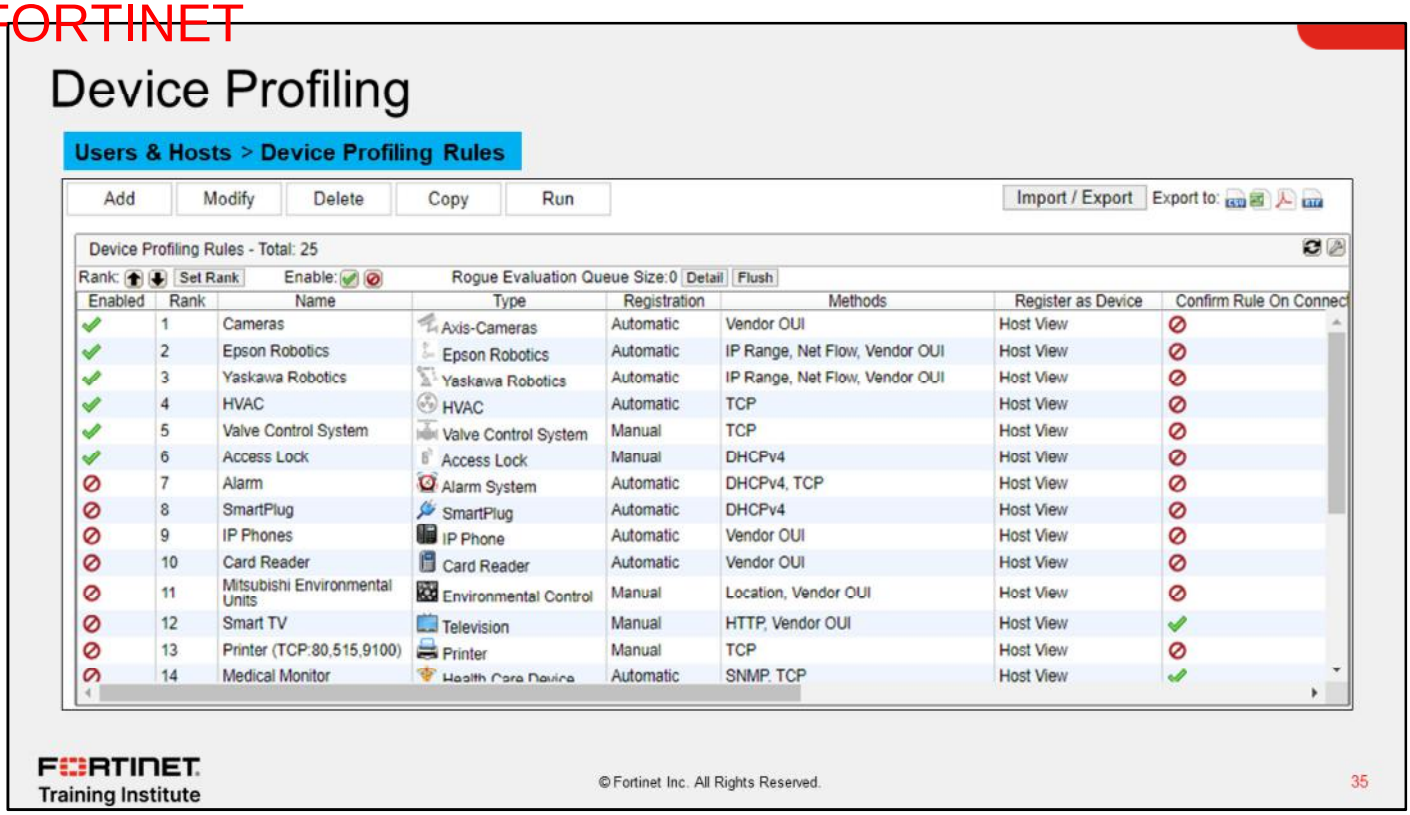
FortiNAC uses a simple browser-based administrative user interface to get username and password credentials. The credentials can be validated using a local administrative account or an LDAP or RADIUS server. FortiNAC administration access is handled by the device eth0 interface.

DO NOT REPRINT
© FORTINET



The main dashboard is the default landing page for an administrative user. The dashboard is made up of individually configurable panels for presentation of detailed FortiNAC information, including user details, device details, and alarm and event information. The navigation menu is located on the left side of the GUI.

DO NOT REPRINT
© FORTINET



You can access the **Device Profiling Rules** window by clicking **Users & Hosts** > **Device Profiling Rules**.

The **Device Profiling Rules** view displays the default set of rules provided. Use this window to modify the default rules or to create your own set of rules. Default rules vary depending on the version of the software and the firmware installed. Upgrading to a newer version of the software does not add or modify default rules.

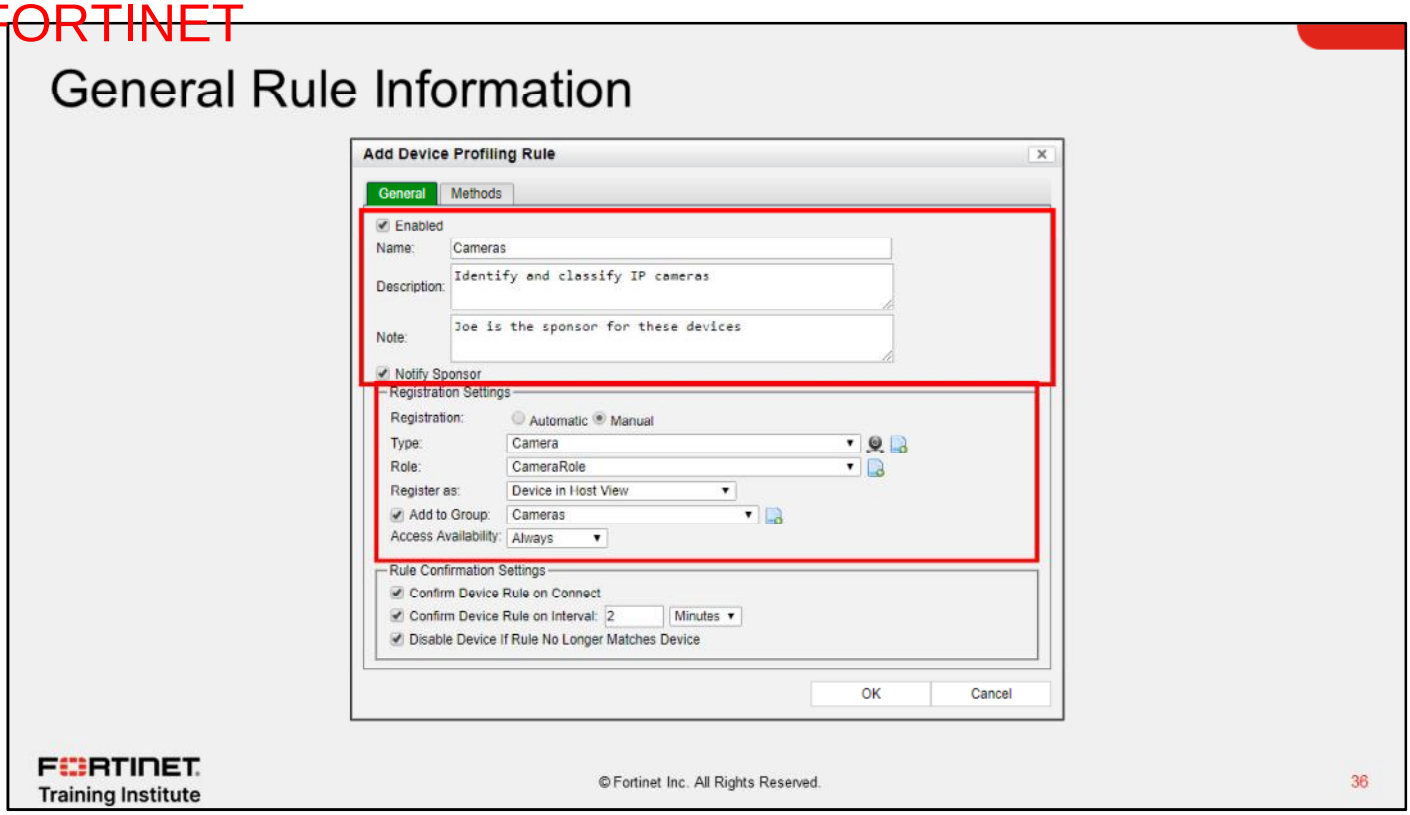
In multi-method rules, evaluate OUI, location, and IP range before any other methods. This is so that you can write profiling rules to target specific devices while excluding others.

Disabled rules are ignored when processing rogues. Device profiling rules are disabled by default and are set not to register devices. When you are ready to begin profiling, enable the rule or rules you want to use.

Notice that the rules are ranked, which you can modify, for the order in which the rules should be applied.

Run the rules to evaluate rogues that already exist in the database.

DO NOT REPRINT
© FORTINET

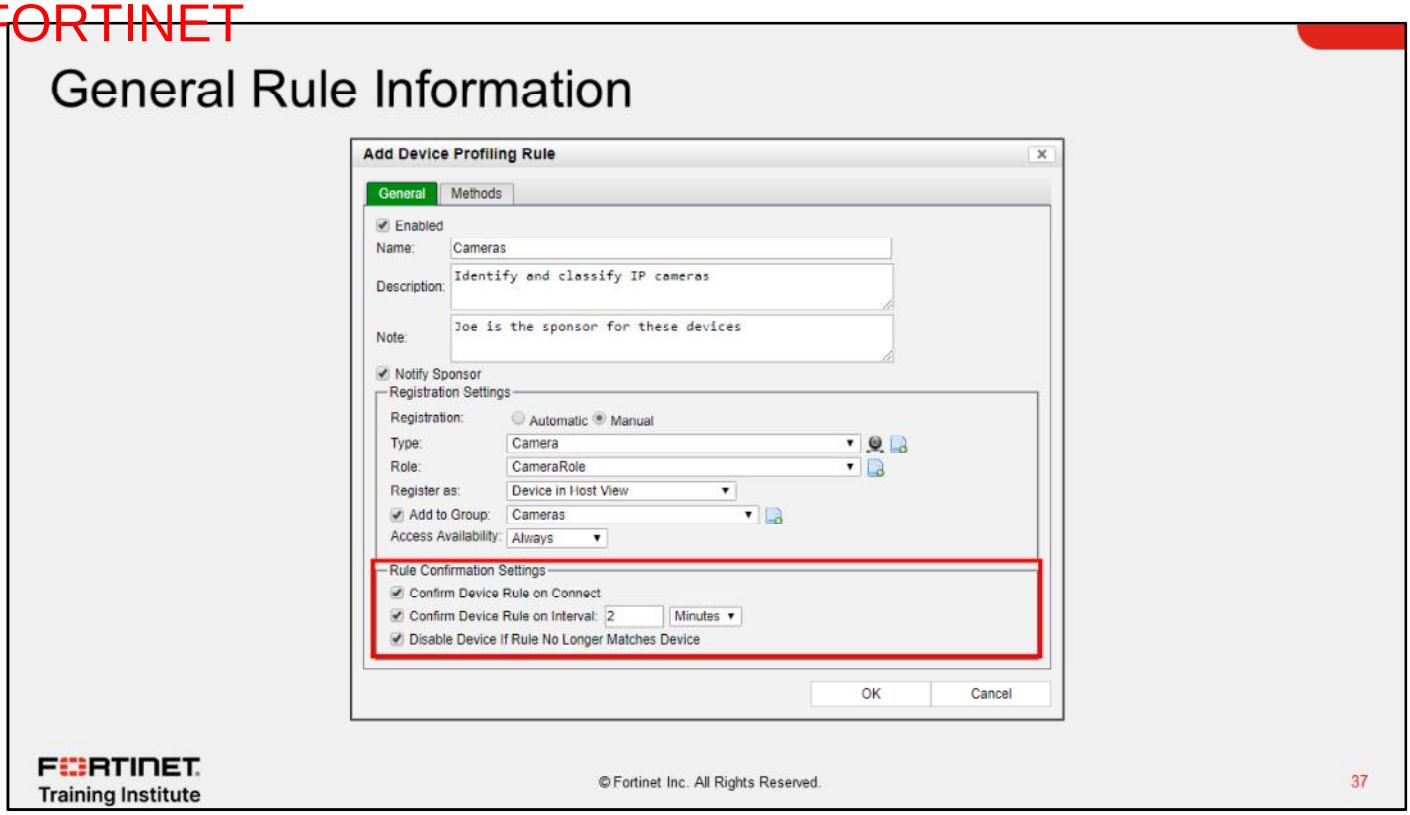


Creation of a device profiling rule begins with configuring the general settings that define the registration settings and rule confirmation settings, and other general attributes. At the top of the **Add Device Profiling Rule** window, there is an option to enable the rule. Only rules that are enabled will process rogues to see if they match. The rule needs a name and can also have an optional description. At the bottom of the selected area, there is an option to notify a sponsor. Any rule can be set up so that a sponsor is notified when a rule is matched. A sponsor is an administrative user. This can be configured on a rule-by-rule basis and is configured within an administrator profile.

The middle section is where you configure the registration settings. The very first option is to have the settings carried out automatically or as a manual process. If set to **Automatic**, FortiNAC will carry out all the following registration steps as soon as the rule is matched. If set to **Manual**, the rule is still matched, the device is profiled, however, the registration settings are not processed until a sponsor logs into the GUI and manually registers the device. The next setting to configure is the device type. There are many pre-existing device types. However, administrative users can also create their own types, which provides complete flexibility, regardless of the types of devices in any given environment. A role can be assigned to a device and this value could then be leveraged in a policy. For example, there could be a network access policy configured to provision devices with a role of camera to a particular network, depending on the point of connection. The **Register as** field is where you can define were the device is placed. The options are, in the host view, the topology view, or both. The most common option is the host view.

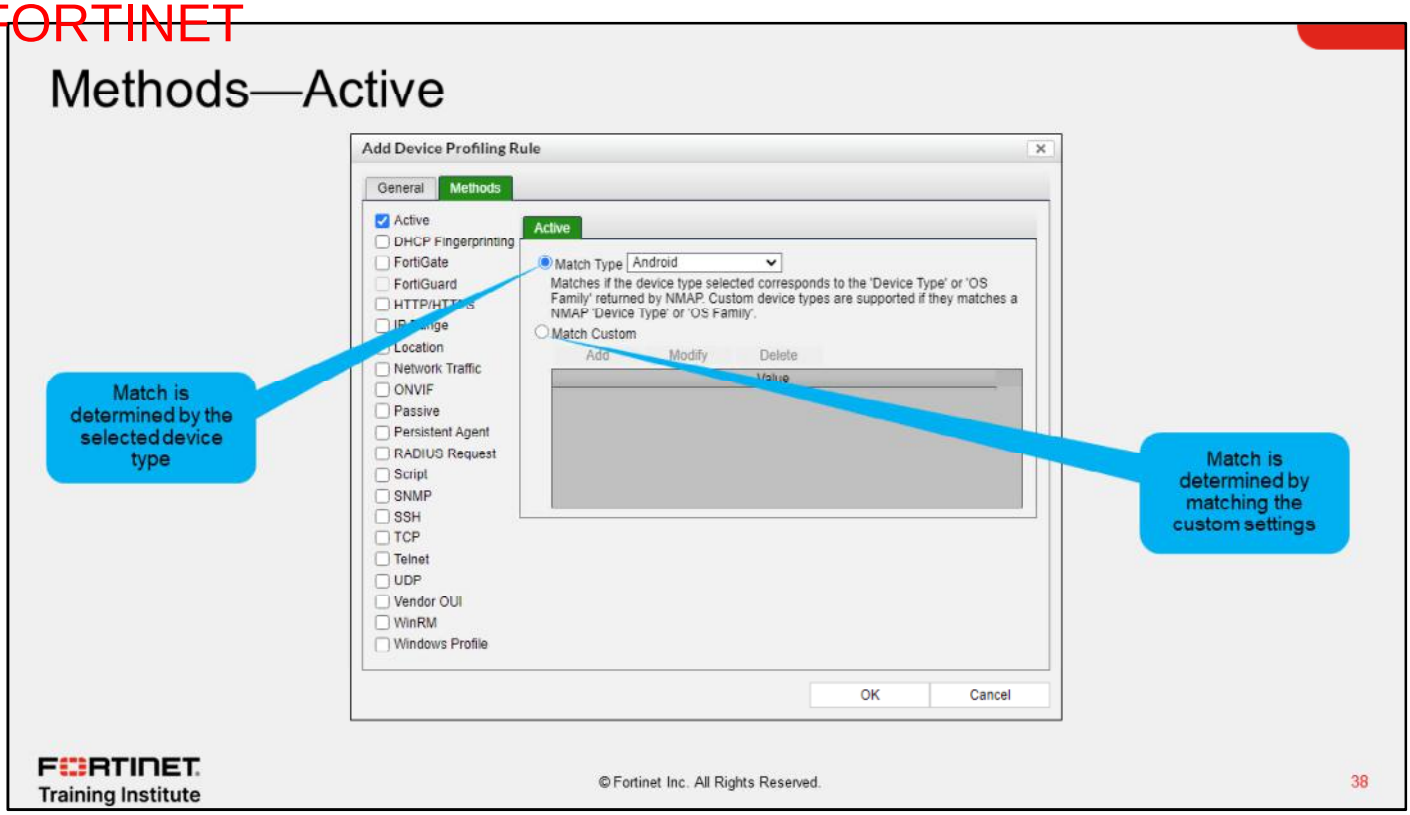
For devices that are in the host view, they can automatically be added to a host group. However, for devices that are in the topology view, you need to select a topology container. The **Access Availability** option lets the administrative user define specific days and times the profiled device is allowed on the network.

DO NOT REPRINT
© FORTINET



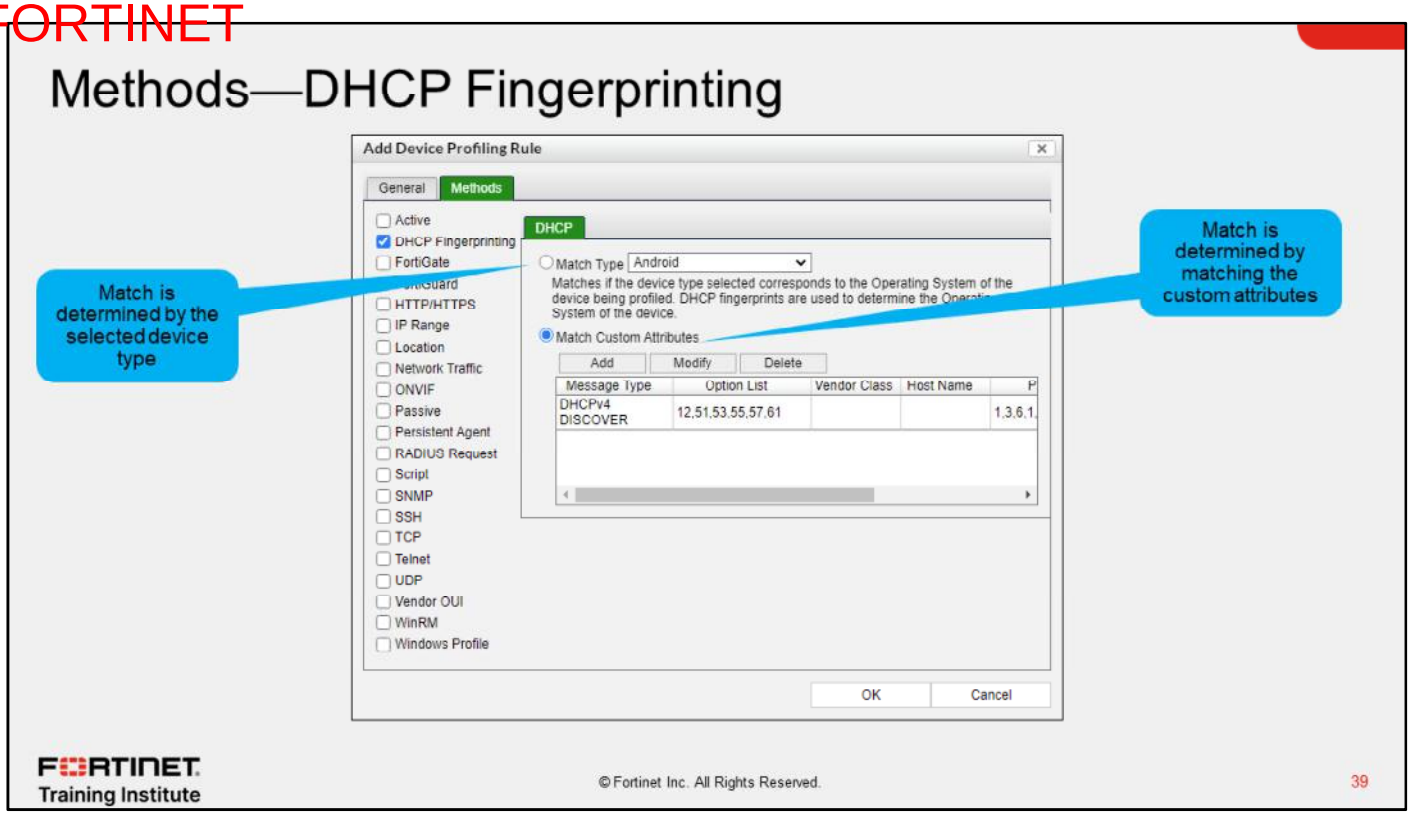
When a rogue device is processed by a rule and found to be a match, FortiNAC remembers the matching rule. Going forward, FortiNAC can be configured to revalidate that the device still matches the rule, each time the device connects to the network, and/or at a user-defined time interval. If the device fails to match the rule on revalidation, you can configure FortiNAC to automatically disables the device. This is a safeguard against impersonation of a previously-profiled endpoint.

DO NOT REPRINT
© FORTINET



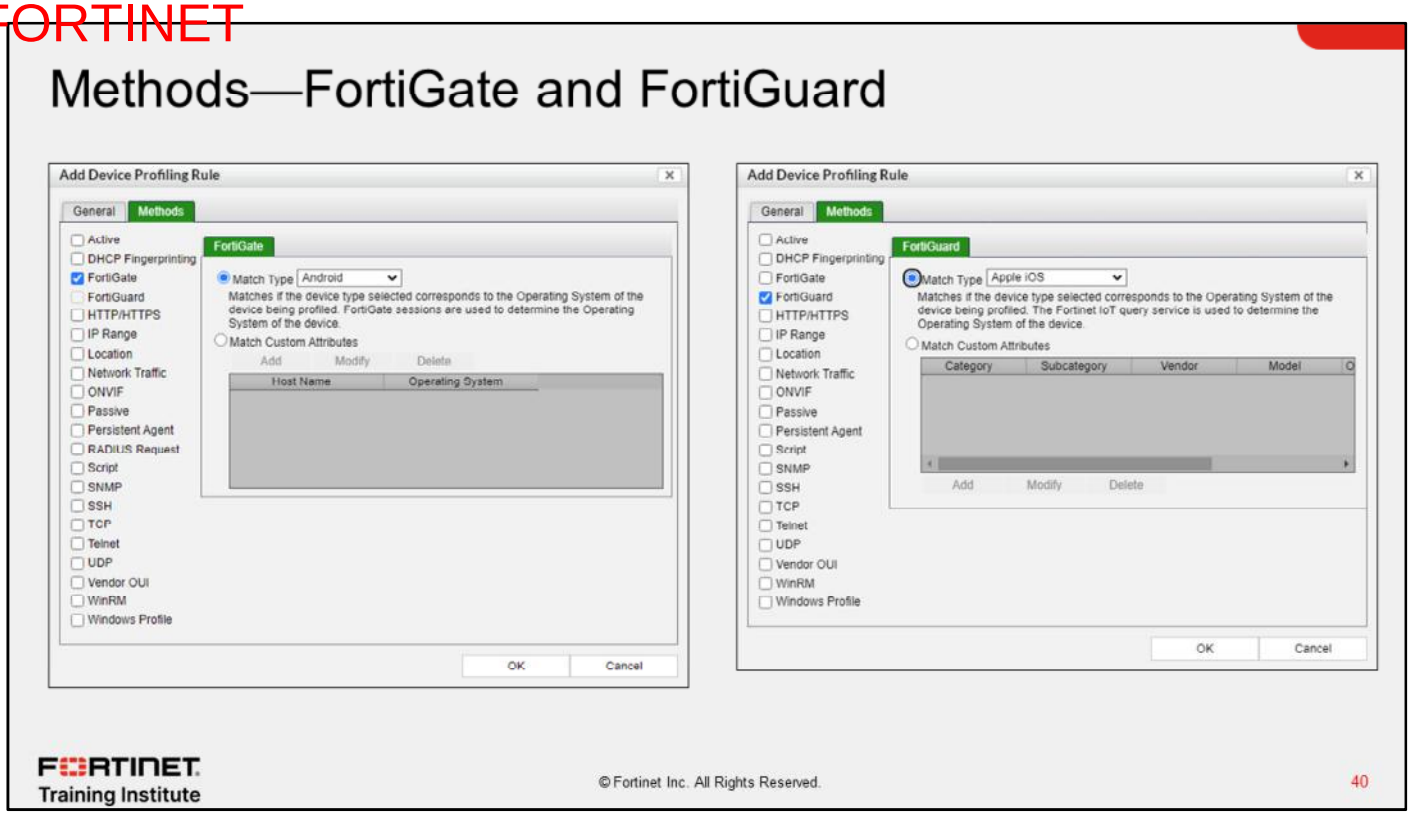
The active method is an NMAP scan of a connected host. A device database matches using the operating system detail information that is gathered during the NMAP scan. The second option is to match a custom value. You can use the key values that you find in the NMAP scan results instead of using the existing database entries. Therefore, you can use an exact string match or regular expression, which lets you customize the active method for almost any environment.

DO NOT REPRINT
© FORTINET



The DHCP fingerprinting method evaluates a DHCP packets received by the FortiNAC device. Similar to the NMAP scan, the FortiNAC device has a DHCP fingerprint database that contains a large list of fingerprints. These fingerprints are identified using option lists and parameters seen in the DHCP packets. When you use the **Match Custom Attributes** option, fields that are left blank are ignored. The custom attributes supported are: DHCP message type, option list, vendor class (DHCP option 60), host name (DHCP option 12), parameter list (DHCP option 55), and operating system.

DO NOT REPRINT
© FORTINET



The FortiGate method leverages firewall session information to determine a match. The **Match Type** option returns a pass for this method if the session information indicates a matching operating system. The **Match Custom Attributes** option uses the firewall session information and evaluats against defined host name or operating system values. The values can be an exact string match or a regular expression.

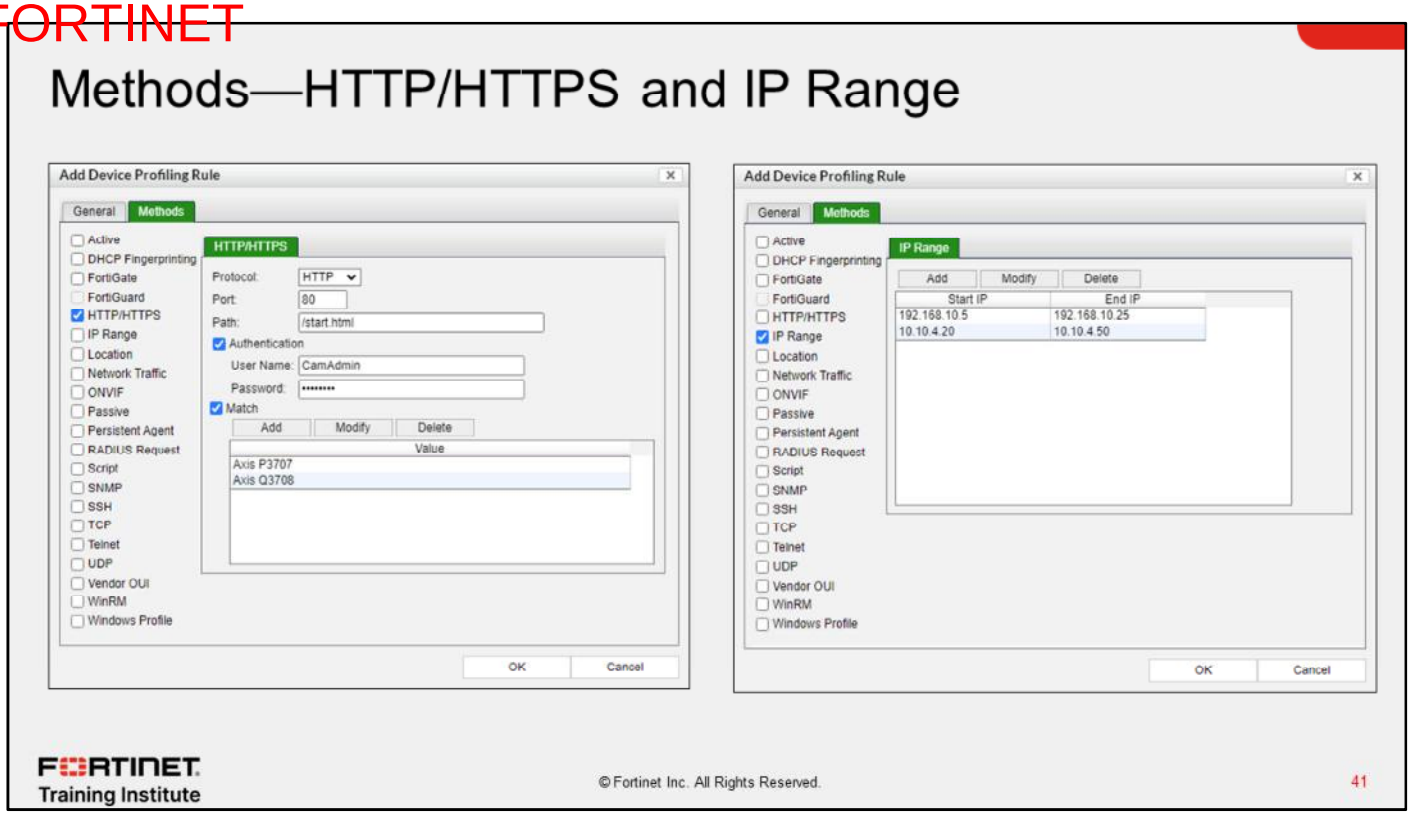
You must setup firewall session polling to use this method. Right-click FortiGate in the **Network** > **Inventory** view and select **Set Firewall Session Polling**.

The FortiGuard method uses the Fortinet IoT query service to determine the OS of the device. When you use the **Match Type** option, you will get a match if the device type selected corresponds to the operating system of the device being profiled. The **Match Custom Attributes** option can be used to match against one or more of the following attributes:

- Category
- Subcategory
- Vendor
- Model
- Operating System
- Sub Operating System

Note that a FortiCare support contract is required to enable the FortiGuard device profiling method; otherwise, the method will be grayed out.

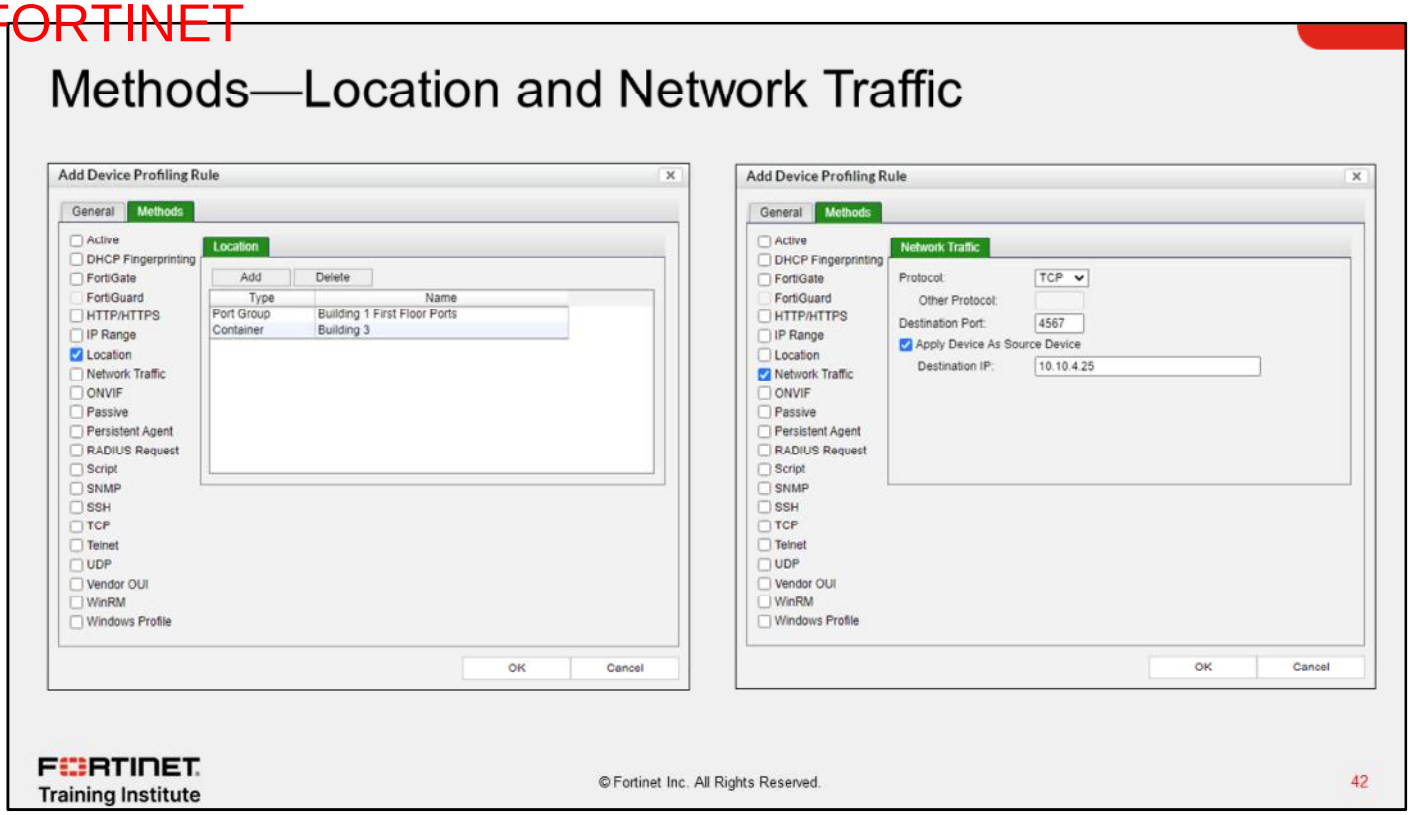
DO NOT REPRINT
© FORTINET



The HTTP/HTTPS method configures the FortiNAC device so that it attempts to open a connection with the device it is trying to profile on a particular port of your choosing, and using the selected protocol. Optionally, it can attempt to load a page and/or enter designated credentials. A matching value is specified and the page contents are parsed for those values. If multiple response values are entered, FortiNAC will attempt to match any of them.

The IP range method results in a match, if the IP address of a device falls within one of the ranges. You must specify at least one IP range. This method requires the FortiNAC device to know the current IP address of the device that is profiled, and will trigger an L3 (IP to MAC) poll to gather this information.

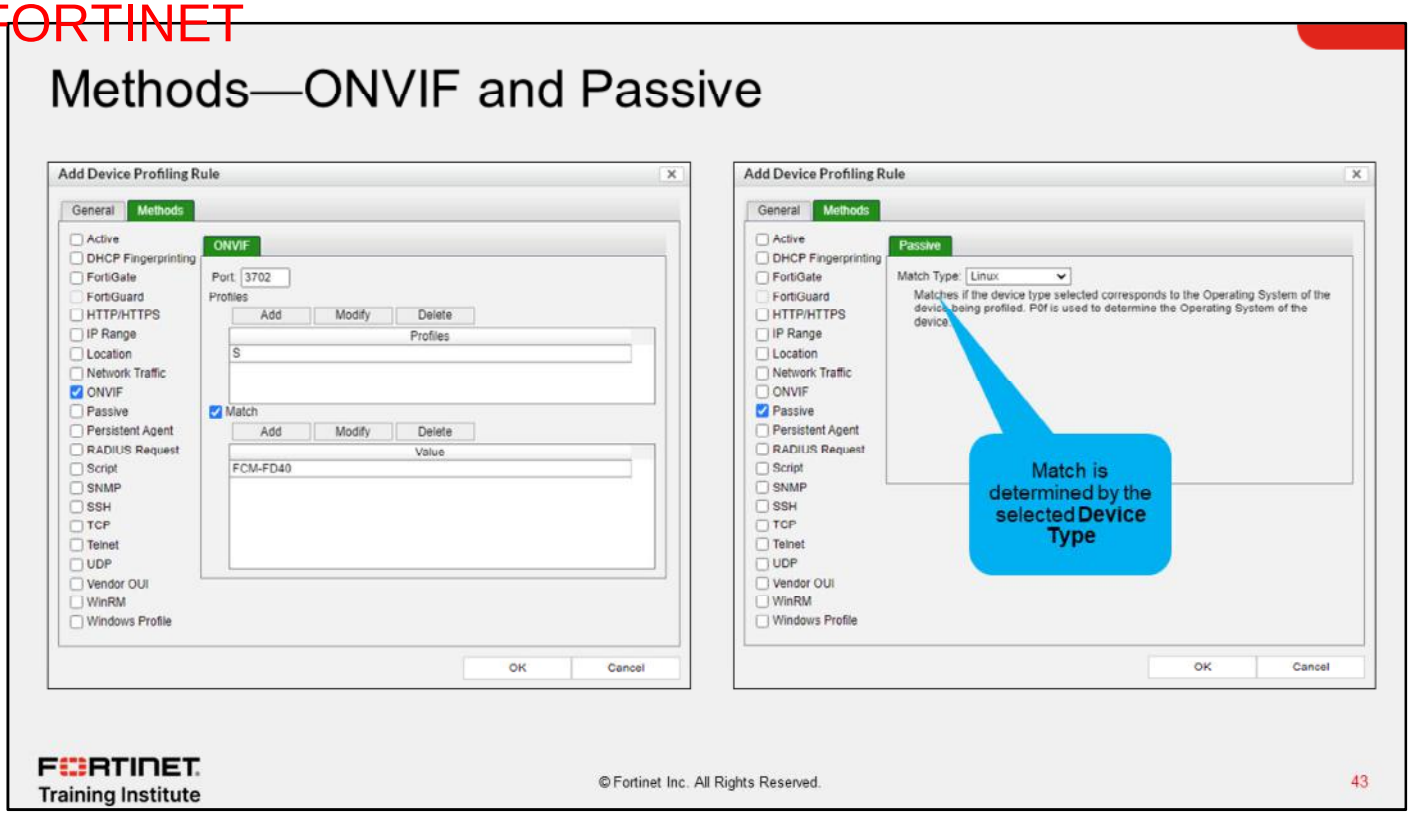
DO NOT REPRINT
© FORTINET



The location method finds a match if the device connects to the selected location on your network. The options are: anything within a container in the topology view, anything in a port group, or anything in a device group. In this example, if the endpoint being evaluated is connected to a port in the **Building 1 First Floor Ports** group or any port of any device in the **Building 3** container, then it will satisfy the location criteria.

The network traffic method evaluates network traffic generated or received by the device being profiled by protocol, destination port and destination IP address. Firewall session polling must be enabled to leverage this method. Firewall session polling is configured by right clicking on a device in the topology tree and selecting **Set Firewall Session Polling**.

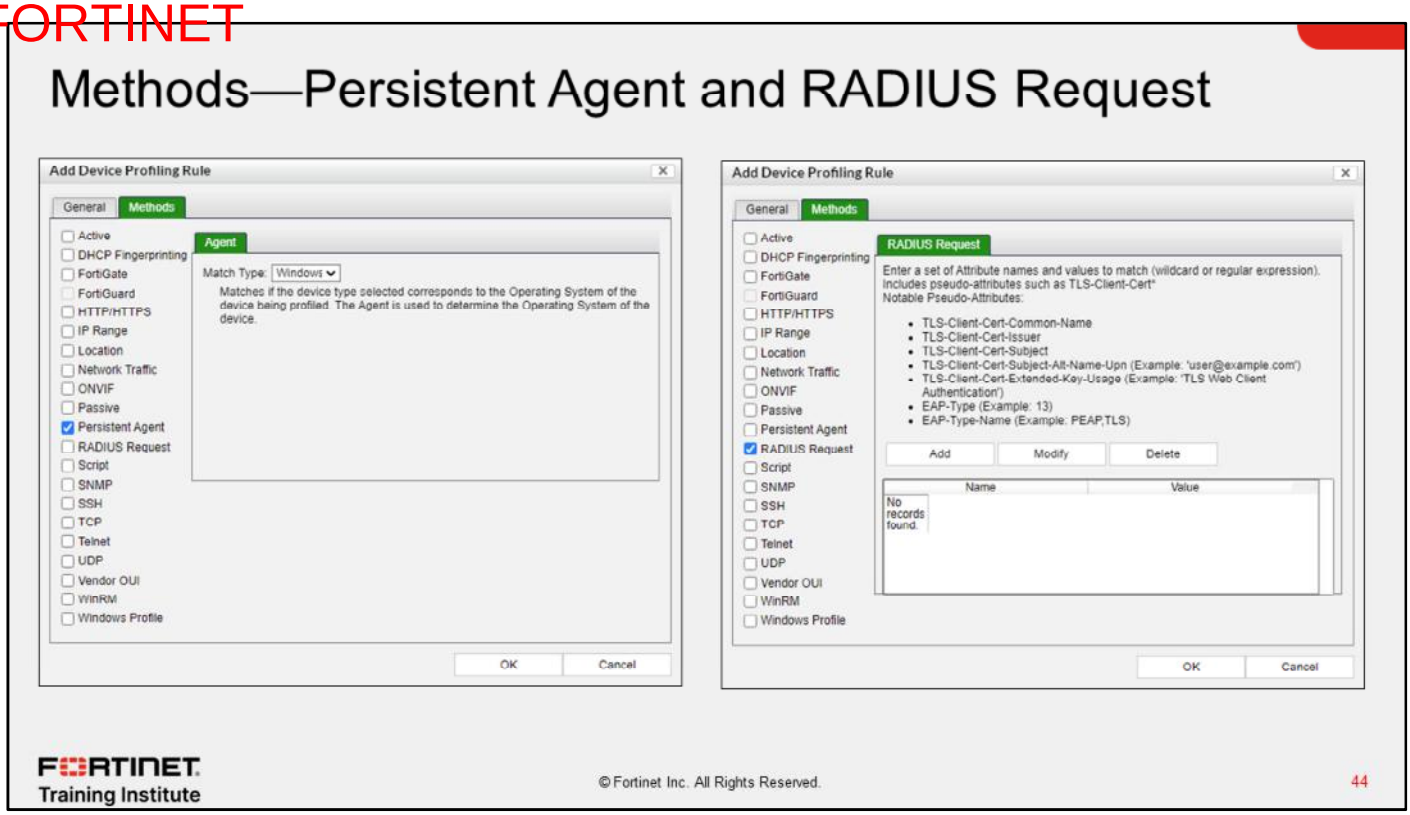
DO NOT REPRINT
© FORTINET



The ONVIF profiling method determines if a connected device supports one or more ONVIF profiles. Matching a defined string can profile devices with greater granularity. The example shown on this slide would match a FortiCamera FD40 because they support ONVIF profile S, and contained FCM-FD40 in the profile response.

The passive method uses p0f, which is a passive TCP/IP fingerprinting tool. It requires communication to take place between the FortiNAC device and the device being profiled. This determines the operating system of the endpoint by analyzing specific fields in the received packets. There is nothing to set on the **Methods** tab. This method uses the selected device type on the **General** tab to determine a match.

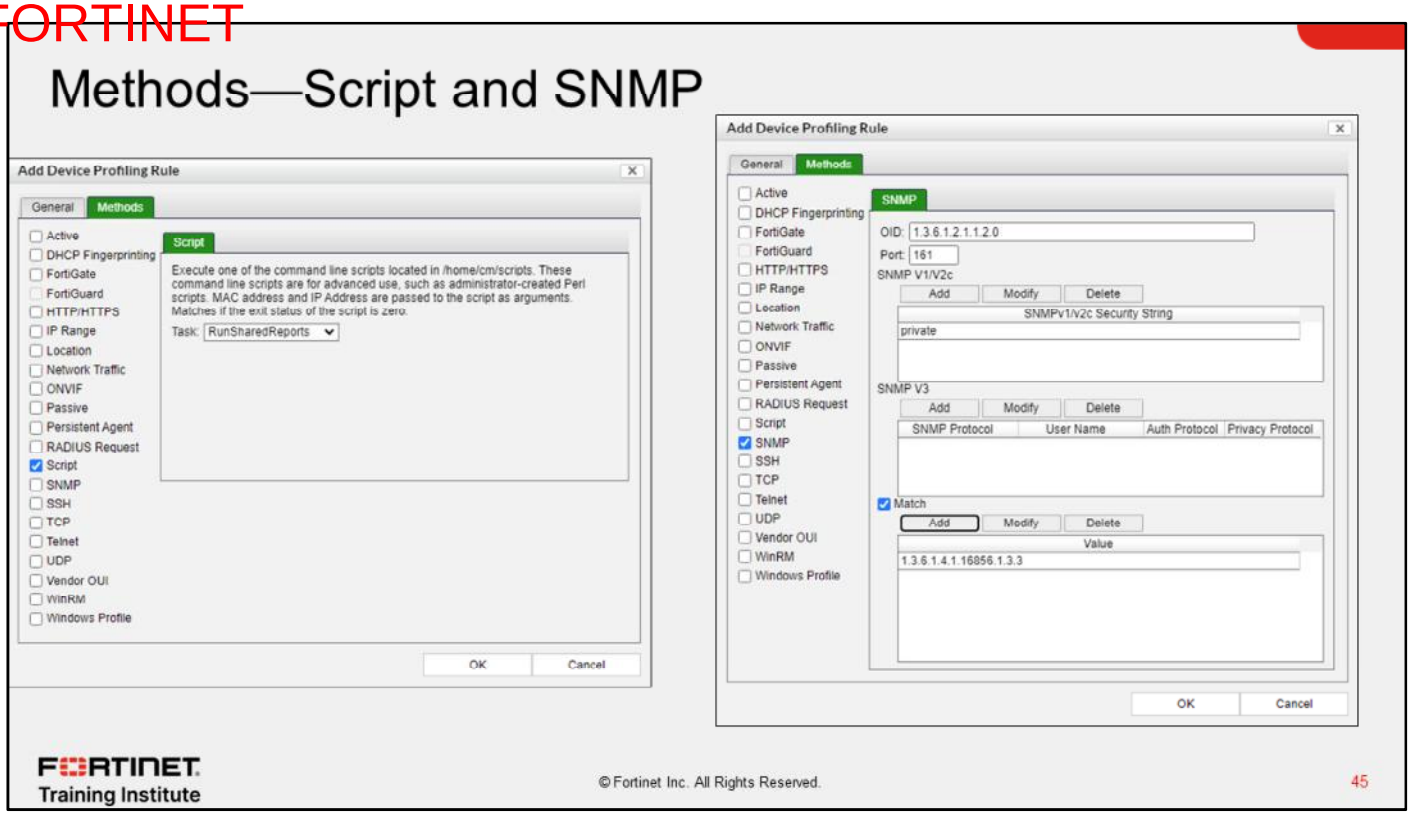
DO NOT REPRINT
© FORTINET



The persistent agent method matches if the device type that is selected in the **Match Type** drop-down list is the same as the operating system of the device being profiled, and if the device has an agent installed, such as the persistent agent or mobile agent. The agent is used to determine the operating system of the device. To register hosts running the persistent agent using this method, you must disable registration from the **Credential Configuration** page for persistent agents, located under the system settings. If you do not, the persistent agent may register the host before the device profiler has the opportunity to register it.

The RADIUS request method uses administratively defined attributes to evaluate fingerprints gathered from local RADIUS access requests. This can allow for profiling of devices after they are connected.

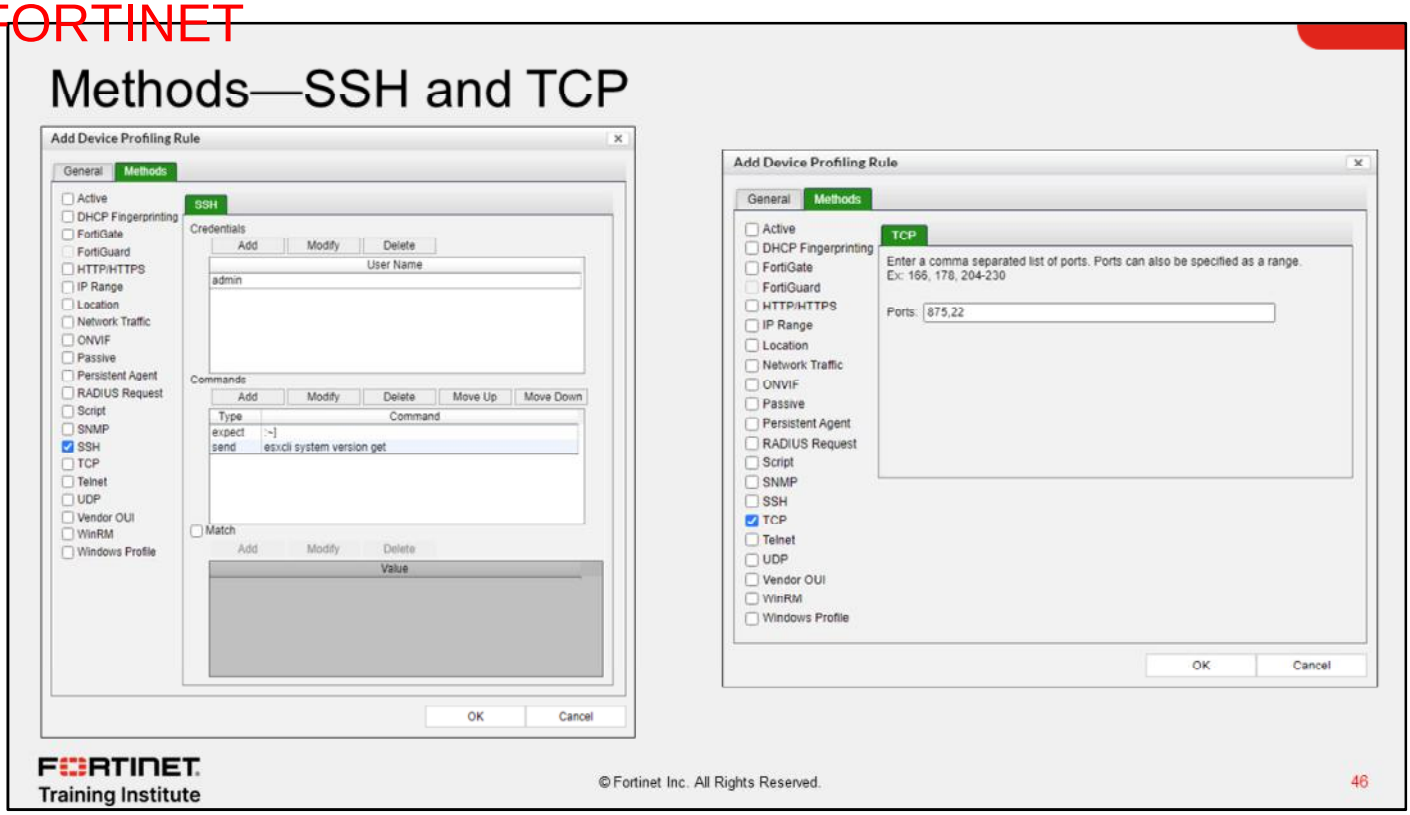
DO NOT REPRINT
© FORTINET



The script method with execute a command line script, such as a Perl script, located in the `/home/cm/scripts` directory and selected in the **Task** drop-down list. MAC address and IP address are passed to the script as arguments. Matches if the exit status of the script is zero.

The SNMP method matches if the device successfully responds to an SNMP GET request for the specified OID. SNMP security credentials are required. If there are multiple security credentials, each set of credentials will attempt to find a potential match. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.

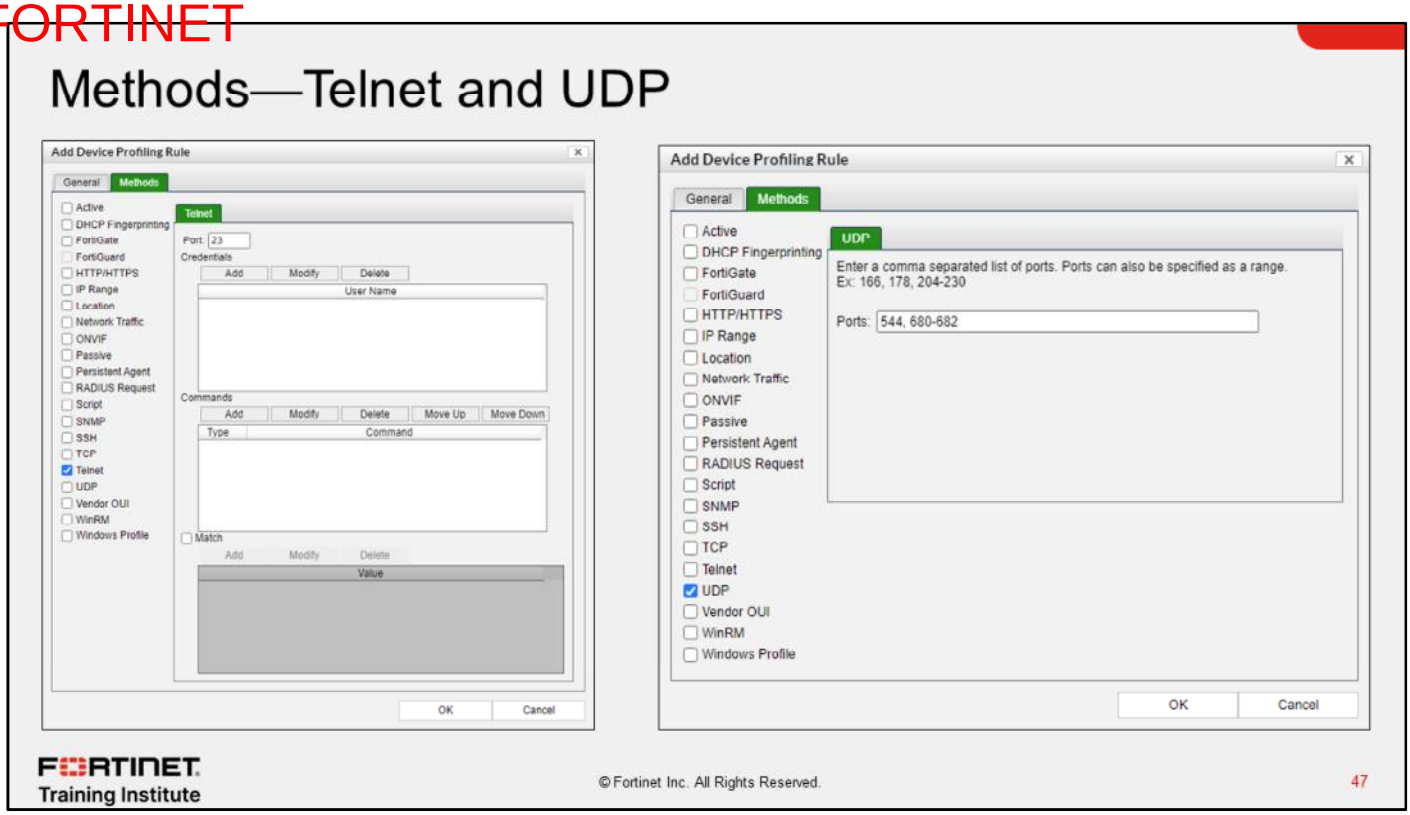
DO NOT REPRINT
© FORTINET



The SSH method attempts to open a client session with the endpoint. User name and password credentials are required. If there are multiple credentials, each set of credentials will attempt to find a potential match. The commands are used to automate interaction with the device. The command options are **expect** and **send**. **Expect** is used by the FortiNAC device to determine when the endpoint is ready for commands to send and is a regular expression string that matches the response from the device. The **send** command sends a string to the device. The **send** command has two optional keywords that you can use to pass the defined credentials, %USERNAME% and %PASSWORD%, as part of the user-defined command. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.

The TCP method matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports are entered, separated by commas, such as, `162, 175, 188`. A range of ports are entered using a hyphen, such as `204-215`. The FortiNAC device uses NMAP to perform the port scan.

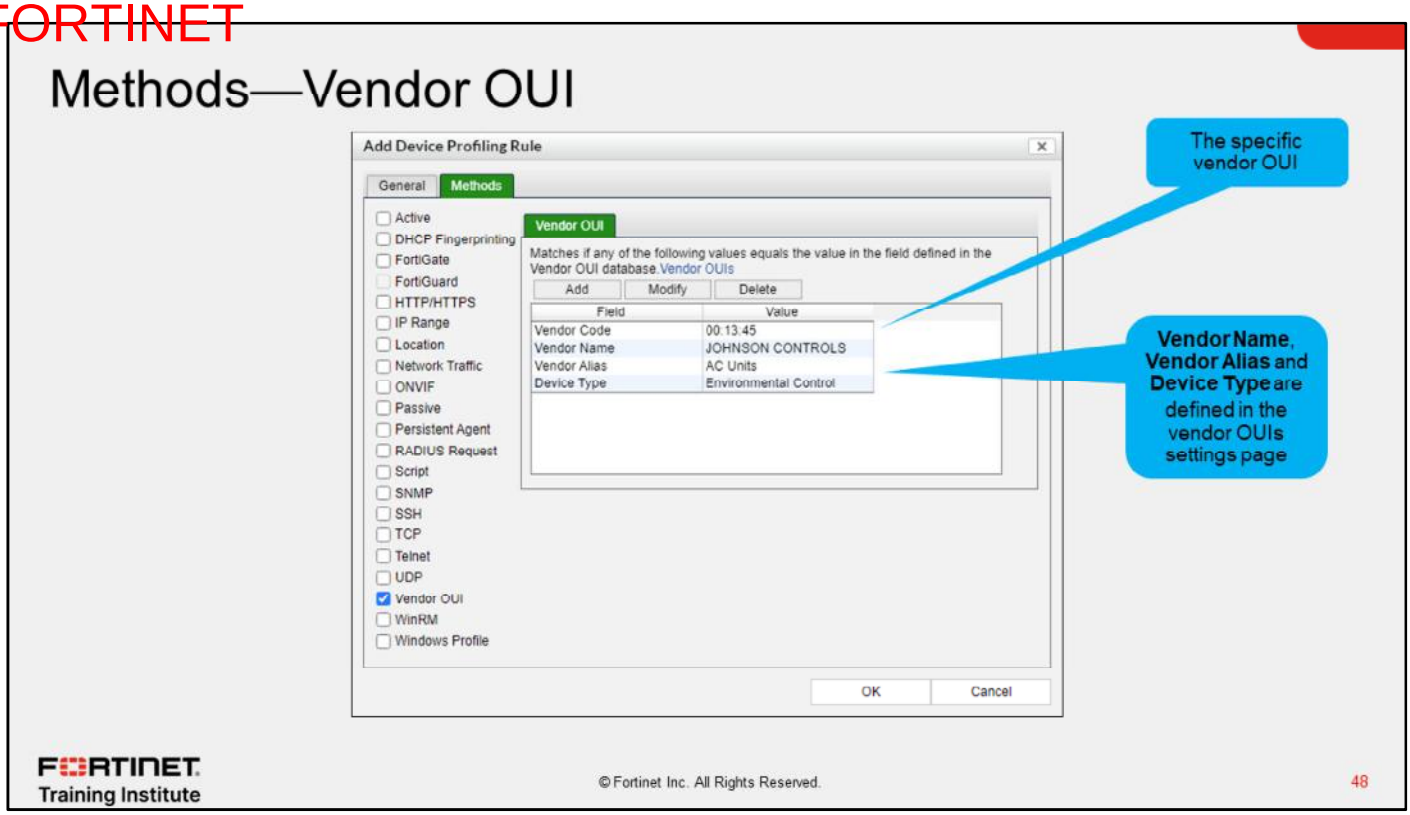
DO NOT REPRINT
© FORTINET



Similar to the SSH method, the Telnet method matches if the device successfully responds to a Telnet client session request. User name and password credentials are not required. If there are multiple credentials, each set of credentials will attempt to find a potential match. The commands are used to automate interaction with the device. The possible commands are **expect** and **send**. The **expect** command is a regular expression string that matches the response from the device. The **send** command sends a string to the device. The **send** command has two keywords %USERNAME% and %PASSWORD% for the username and password. There is an optional field to match the response string value. If multiple string values are entered, it will attempt to match any of them.

The UDP method works similar to the TCP method. The UDP method matches if the device provides a service on all of the specified ports. You must specify at least one port, but all specified ports must match. Multiple ports are entered separated by commas, such as, `162, 175, 188`. A range of ports are entered using a hyphen, such as `204-215`.

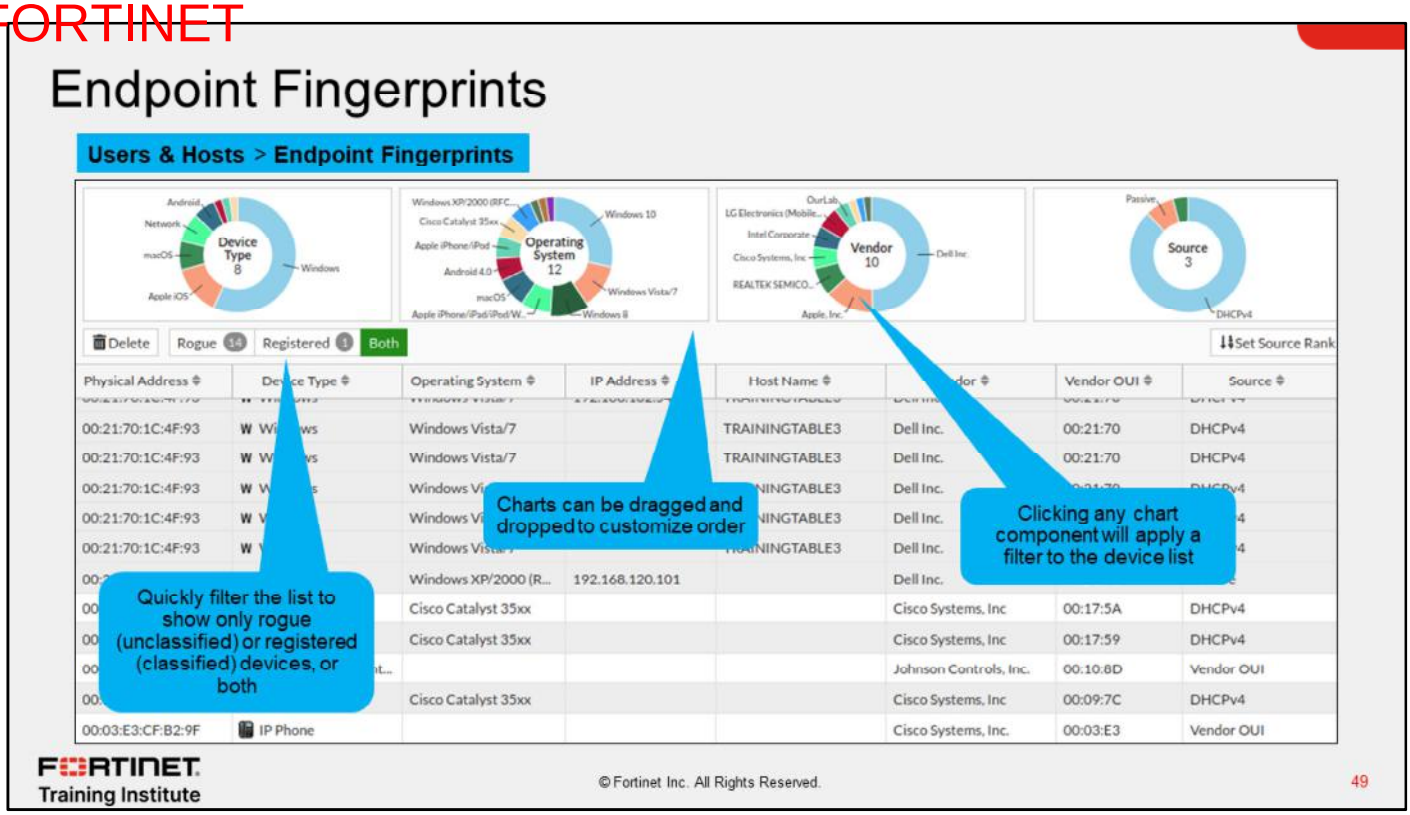
DO NOT REPRINT
© FORTINET



The vendor OUI method matches if the vendor OUI for the device corresponds to the OUI information selected for the method. At least one vendor option must be specified. If there are multiple entries, the device only has to match one entry to match this rule. Options include:
Vendor Code: A specific vendor OUI selected from the list in the FortiNAC database. To select the OUI, begin typing the first few characters. A list of matching OUIs is displayed in a drop-down list.
Vendor Name: A single vendor name selected from the list in the FortiNAC database. To select the name, begin typing the first few characters. A list of matching vendors appear in a drop-down list. You can use an asterisk as a wildcard at the beginning and/or end of a vendor name to match all variations of a name.
Vendor Alias: A vendor alias is an administratively-defined string that you can assign to one or more vendor OUIs, across multiple vendors. You can define the alias values in the **Vendor OUI** settings page, located in the **Identification** folder, which you can find in the system settings.
Device Type: Select a device type from the drop-down list provided. Includes items such as Alarm System or Card Reader. If this option is selected, the device type associated with the vendor OUI of the connecting device must match the device type for the OUI in the FortiNAC vendor database. You can see the device type in the vendor database, and override it in the vendor OUIs settings page, located in the **Identification** folder in the system settings.

Note that it is a best practice to use the vendor OUI method in conjunction with other methods to avoid undesired matches due to MAC address spoofing.

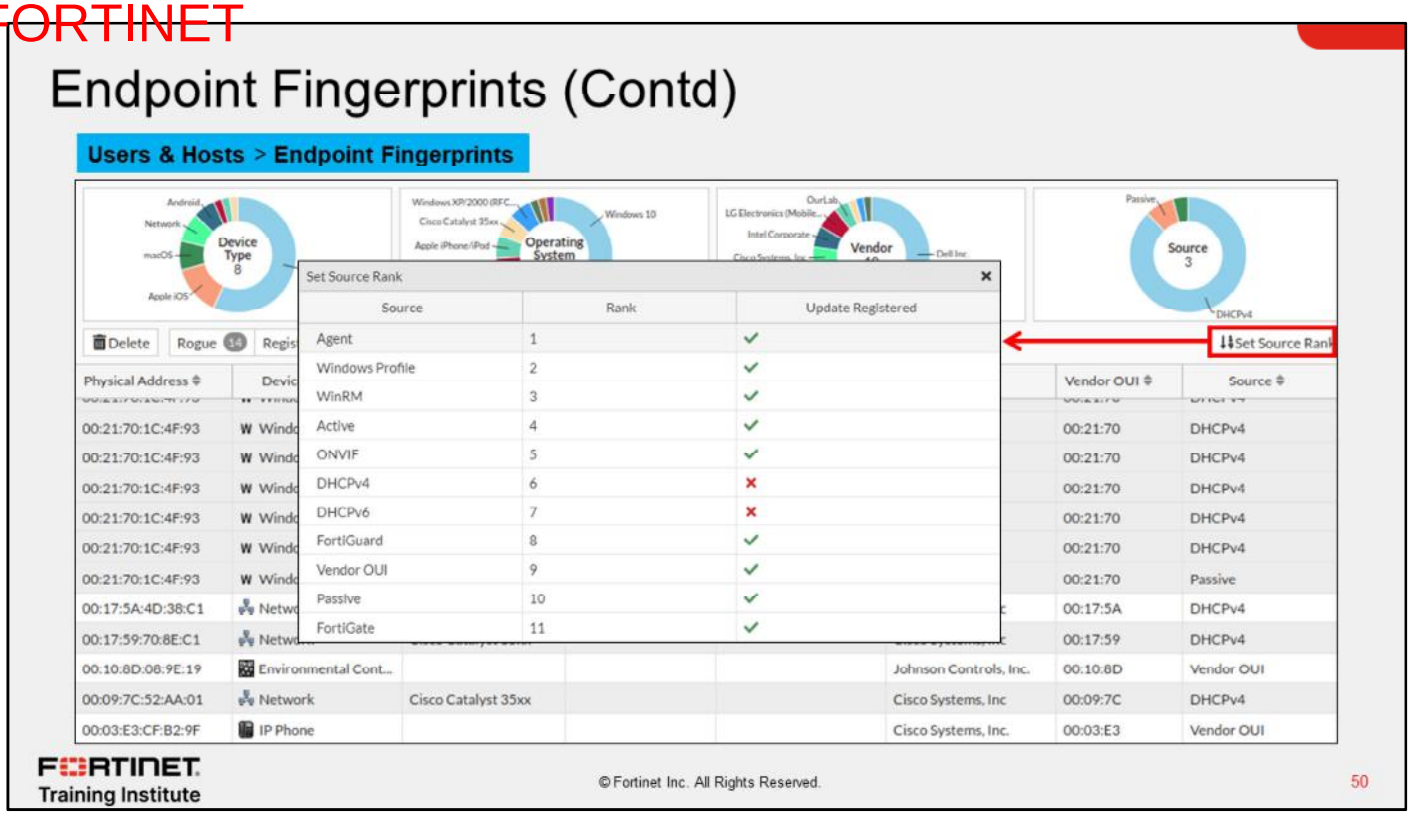
DO NOT REPRINT
© FORTINET



FortiNAC uses a list of sources to gather fingerprint information about all devices (rogue and registered) that are connected or have previously connected to the network. Charts across the top of the view break down the devices by device type, operating system, vendor and source. The graphs can be dragged and dropped to customize the order, and any component of a chart can be clicked on to apply a filter to the device list. Button at the top of the device list allow for filtering the list to display only rogue or registered devices, or both.

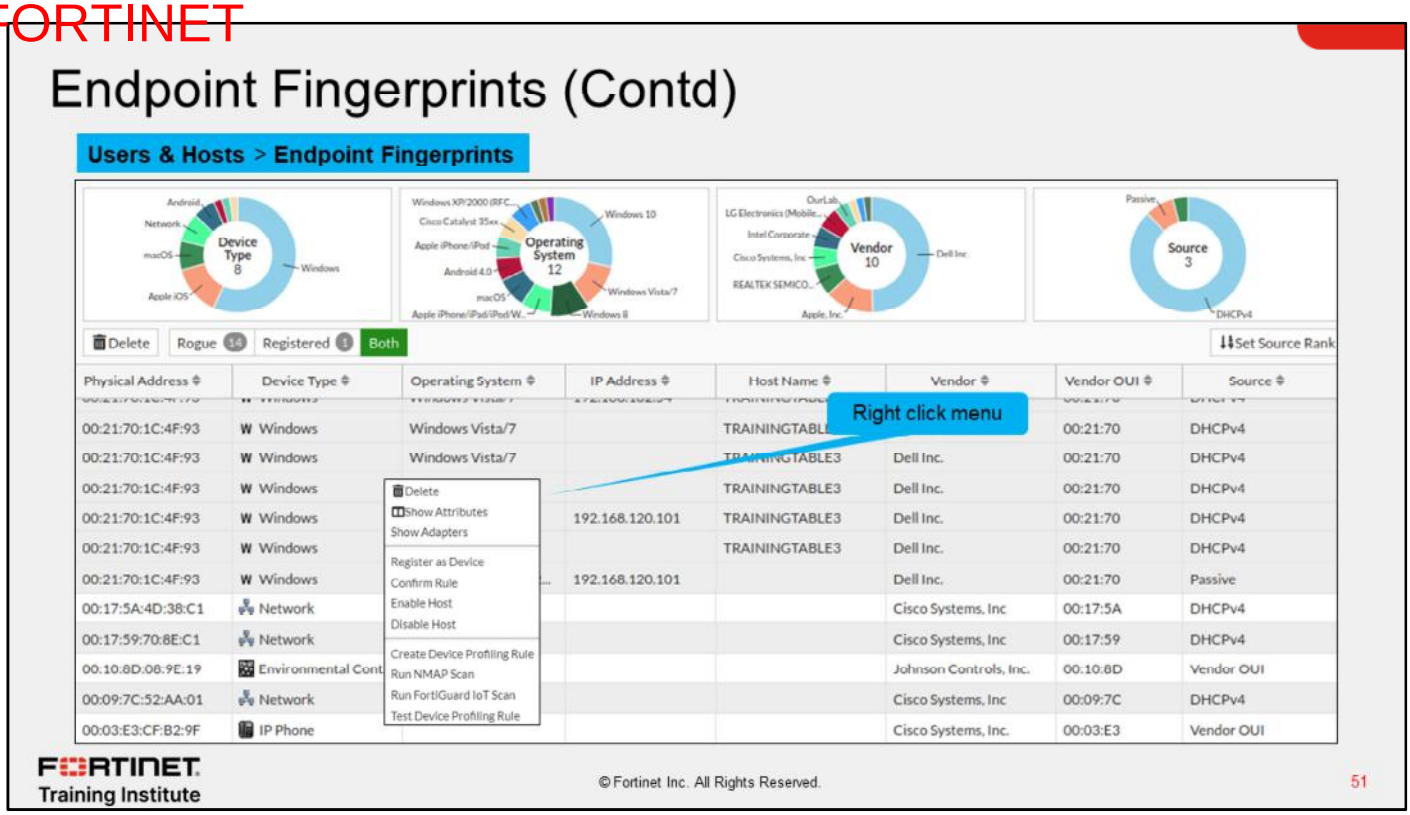
The same device may have several fingerprint entries in the list. This is because a new entry is made for each unique fingerprint. For example, a fingerprint may show a different set of DHCPv4 options or parameters from two DHCP discovery messages, or between DHCP discovery and request messages. The same host with multiple fingerprints identifying different operating systems is most likely a dual-boot host.

DO NOT REPRINT
© FORTINET



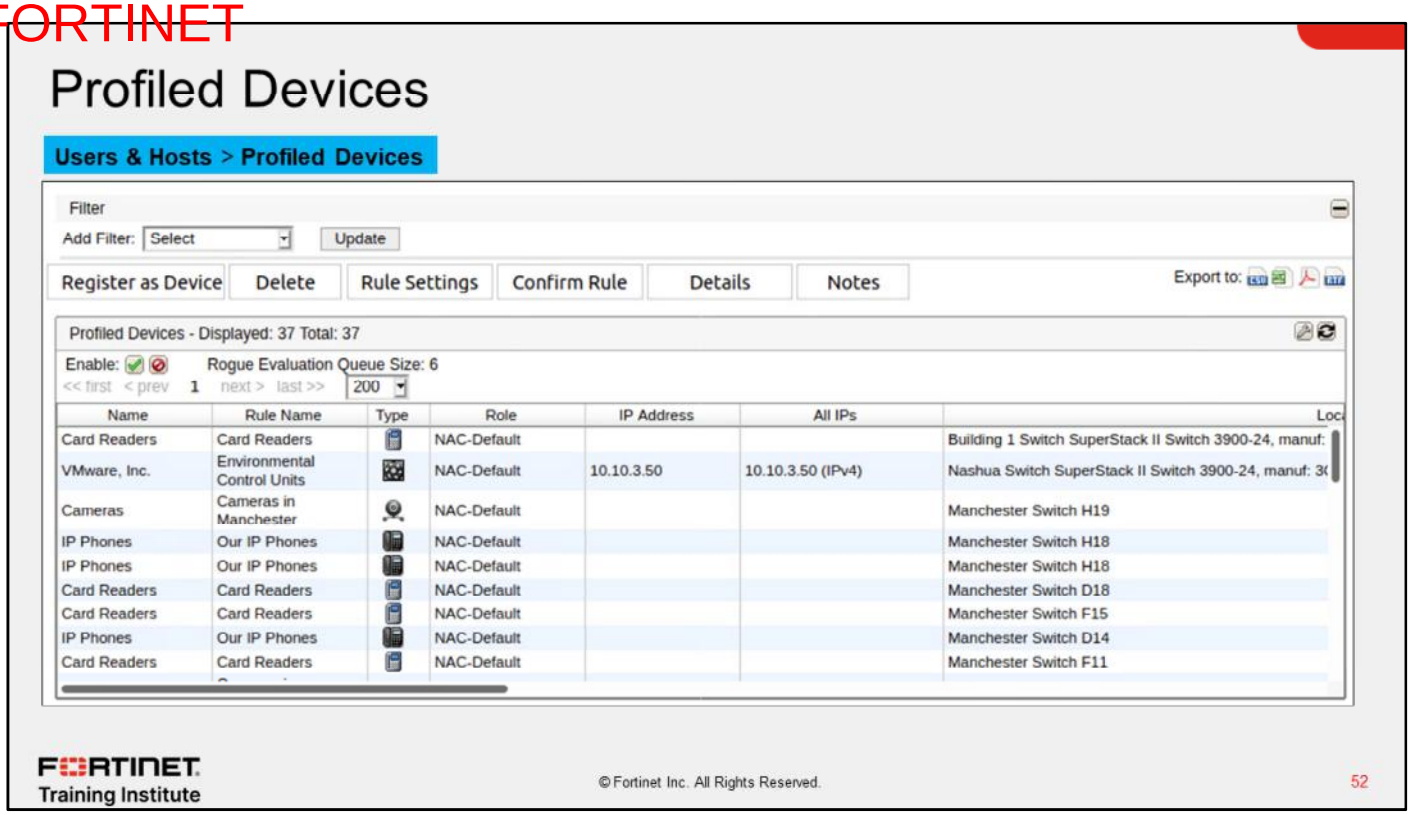
The set source rank list will display the sources of data collection used to gather the fingerprints. These sources can be ranked for situations where a device has conflicting data. For example, if the **Vendor OUI** source fingerprints it as one type of device and **Active** another, FortiNAC will represent it in the list as the device type associated with the higher ranked source.

DO NOT REPRINT
© FORTINET



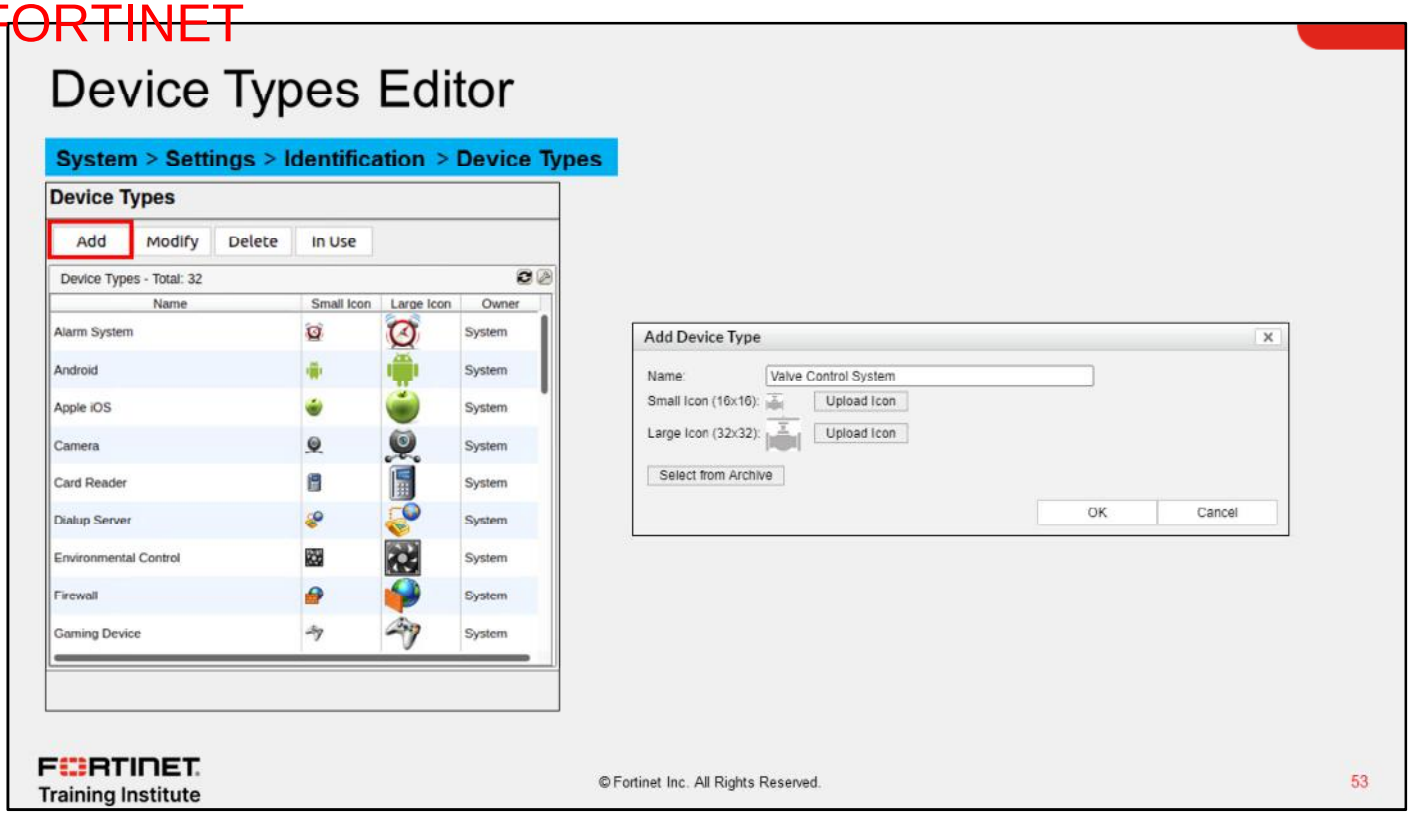
Right click options are available for any host in the list. The options are:
Delete: Deletes the selected fingerprint(s).
Show Attributes: Displays the fingerprint attributes information.
Show Adapters: Displays the adapter information associated with the device.
Register as Device: Registers the host as a device.
Confirm Rule: If the device has matched a device profiling rule it will be re-evaluated against that rule.
Enable Host: Enable the host if it has been disabled.
Disable Host: Disables the host.
Create Device Profiling Rule: Displays the **Add Device Profiling Rule** window with any methods known as a result of the fingerprint enabled and populated.
Run FortiGuard IoT Scan: Attempts to identify the device using FortiGuard.
Test Device Profiling Rule: Evaluates the device against an existing profiling rule.

DO NOT REPRINT
© FORTINET



When a device matches a profiling rule it appears in the **Users & Hosts** > **Profiled Devices** view. This view displays the device name, the profiling rule that was matched, the type of device it is or will be registered as, role assignment, IP address and physical address, location, and several other pieces information. If the rule was configured to automatically register the device there is nothing more you need to do. It appears as registered in the **Registered** column. If the rule was set for manual registration it also appears in the **Registered** column. However, an administrative user or sponsor needs to select the device in the **Profiled Devices** view, and click **Register as Device** to complete the process.

DO NOT REPRINT
© FORTINET

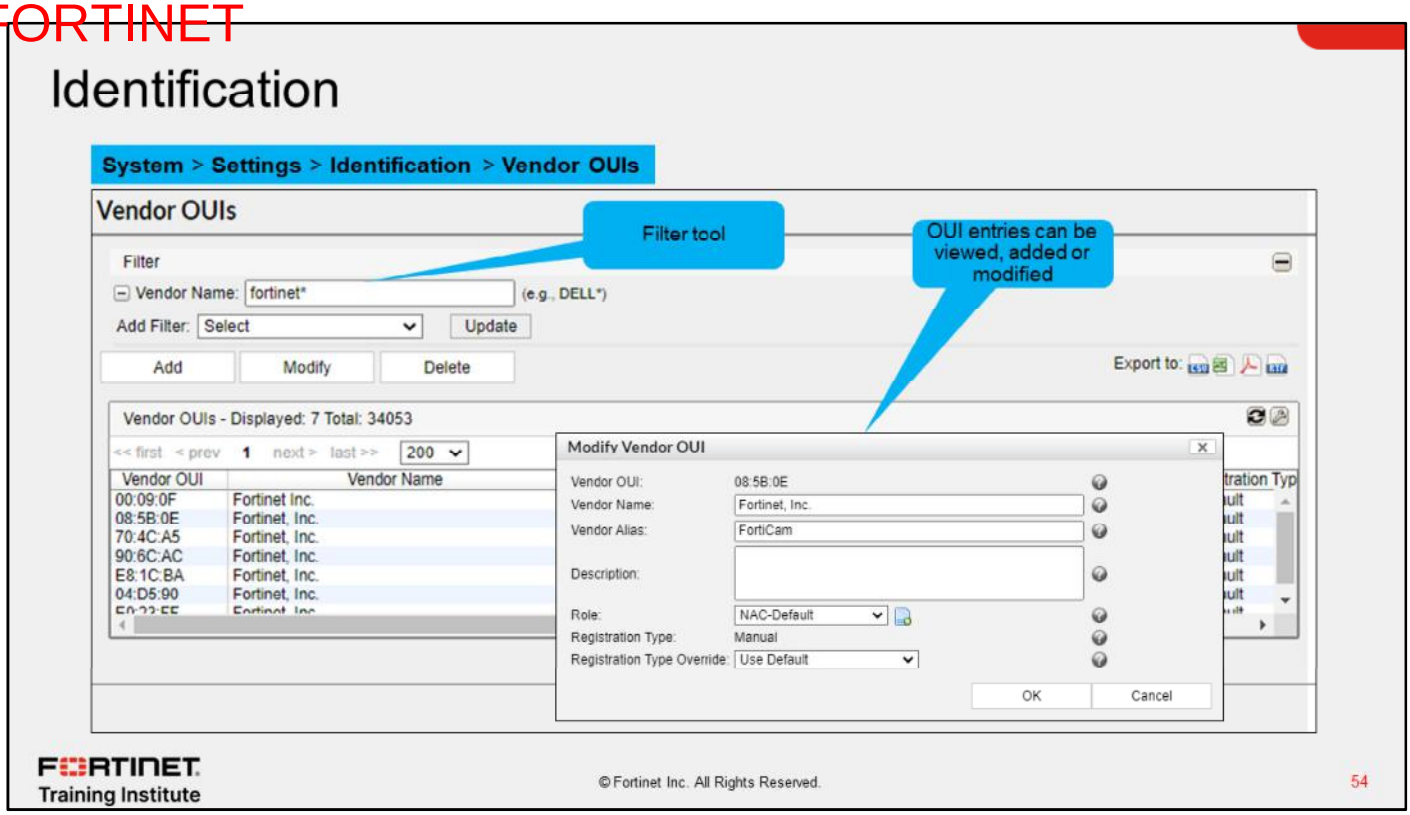


Access the **Device Types** editor by clicking **System** > **Settings** and expanding the **Identification** folder.

An important part of classifying devices is to accurately portray the many diverse endpoints that connect to an environment. Device type is commonly used for running inventory reports or creating security policies. There is a default set of pre-existing device types that you can use during the classification process. You can view the list from the **System Settings** menu, within the **Identification** folder use the device types editor to modify or create new device types. This helps you to customize device types to fit any environment.

To create a new device, click **Add**. Give the device type a name. Then upload icons of the appropriate size, or select a small and large icon pair from the archive list of almost 2,000 icon pairs. After you create a new device type, it appears in the list and works exactly like the default device types.

DO NOT REPRINT
© FORTINET

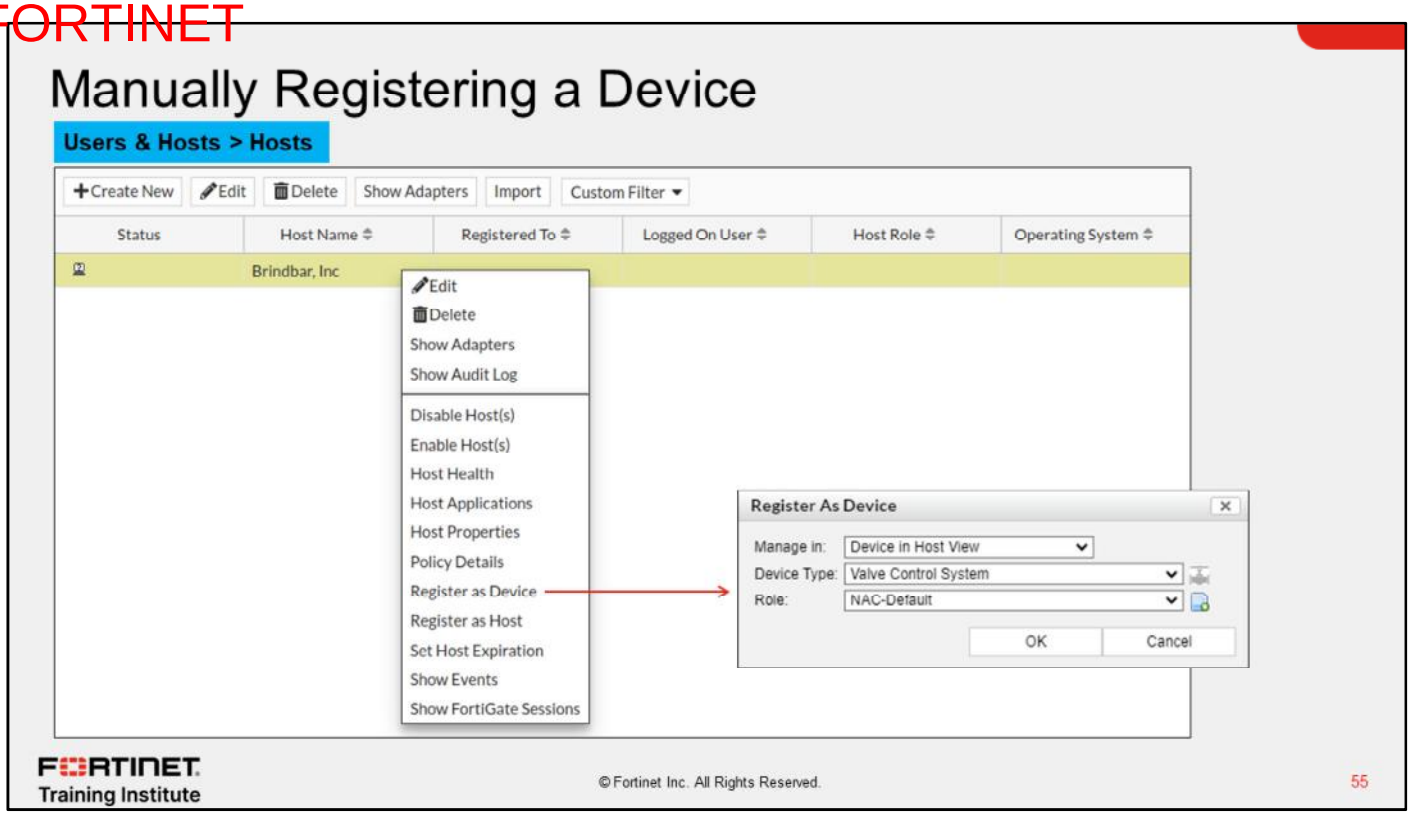


Access the vendor OUIs view by clicking **System** > **Settings** and expanding the **Identification** folder. From this view you can locate specific vendor OUIs using the filter, and you can modify specific attributes of the selected OUI. To configure an alias, select an entry and click **Modify**. You learned about alias attributes when you learned about device profiling configurations.

You can set the alias in the **Vendor Alias** field. You can also make configuration changes for default role assignment and registration type. The default role assignment is the value assigned if the device is registered using a portal page. The registration type is a default device type association and is used with the vendor OUI method of a device profiling rule. You can override the registration type when the type set by the FortiNAC device does not reflect what is seen in a specific environment.

Vendor OUI information is kept up to date by the auto-definition synchronizer scheduled task that exists in the scheduler tool.

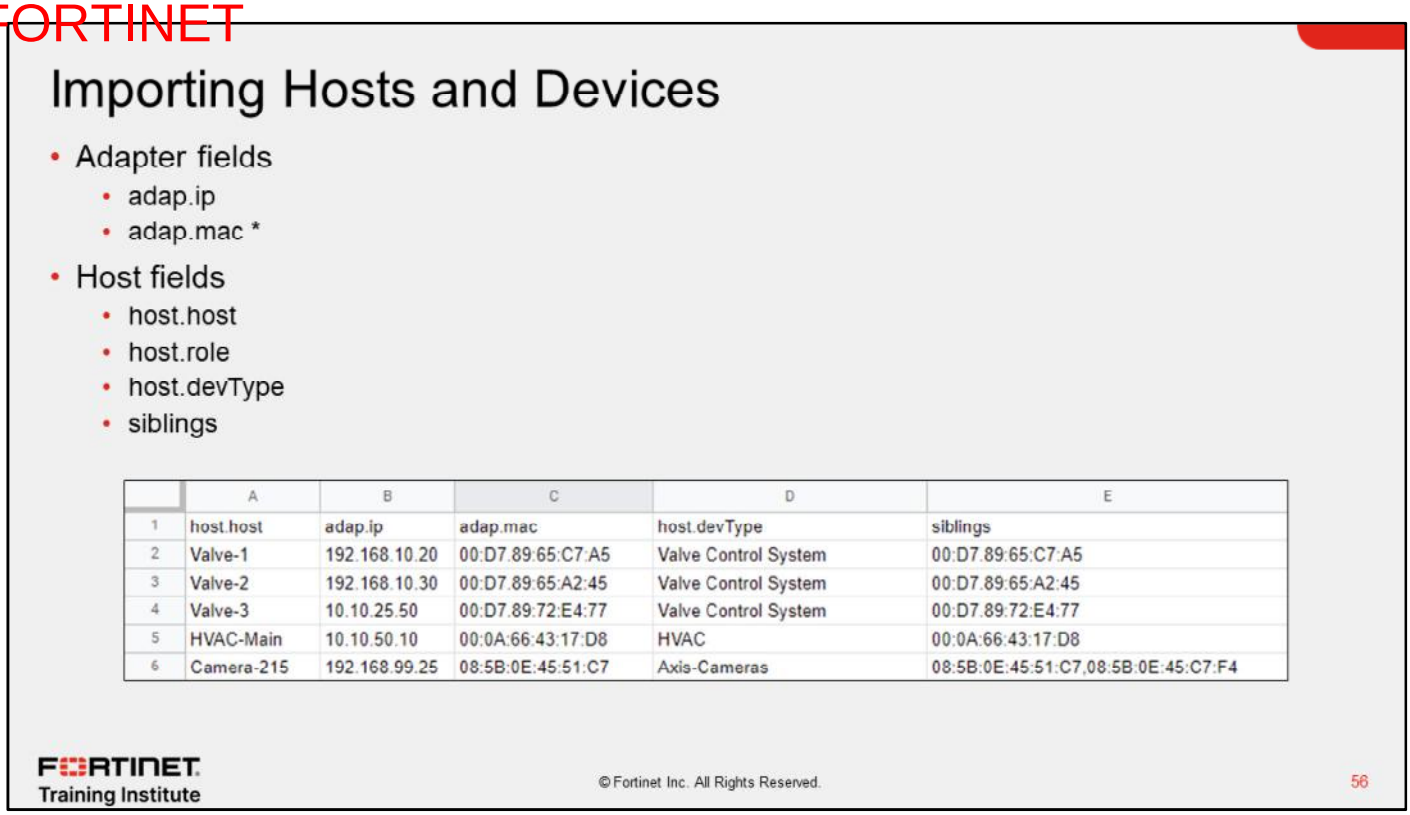
DO NOT REPRINT
© FORTINET



To register a host as a device, select the option from the right-click menu. The **Manage in** drop-down list helps the administrative user decide how the registered device is viewed and managed after registration.

- The **Device in Host View** option will model the device as a host, and it will appear and be managed in the host view.
- The **Device in Topology** view will display the host in the topology tree. Note that security policies are not applied to devices modeled using the **Device in Topology** option.
- The **Device in Host View and Topology** option will display the device in both locations.
- The **Device Type** drop-down list is used to manually assign the device type and will include all default and administratively created device types.

DO NOT REPRINT
© FORTINET



To import devices, create a comma separated value (CSV) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

You can mix the types of records you are importing in the same file, as long as you have all of the appropriate fields in the header row.

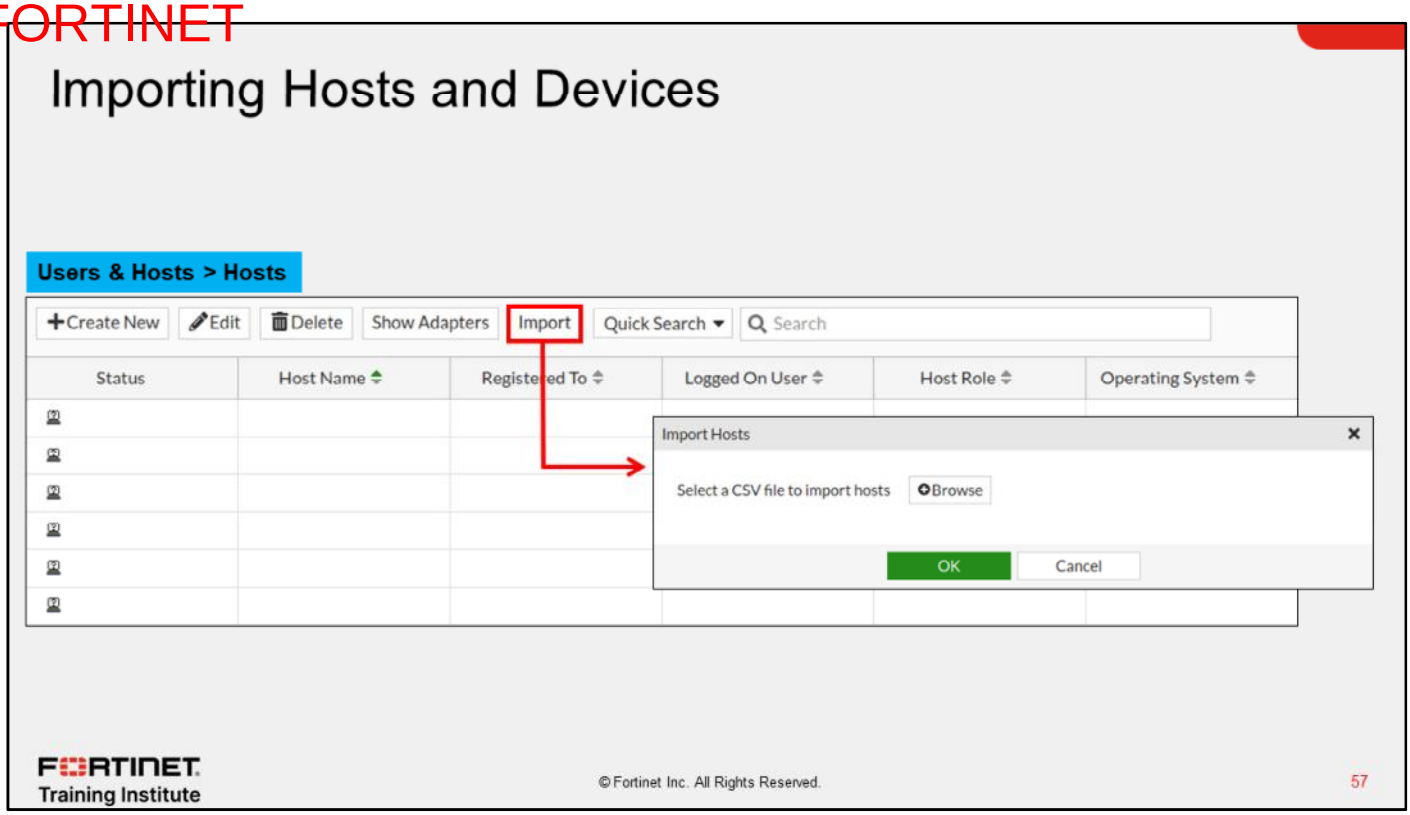
The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import hosts and their corresponding adapters, the header row could have the following columns:
adap.mac, **adap.ip**, **host.devType**, **host.host**, and **siblings**.

There are a couple required columns, depending on what is being imported.
For devices, the **adap.mac** column is required.

Note that fields are case sensitive, and if you import something that already exists in the database, the existing record is updated with the new data from the import.

The fields displayed on this slide are some of the most commonly used. A more complete list exists in the help.

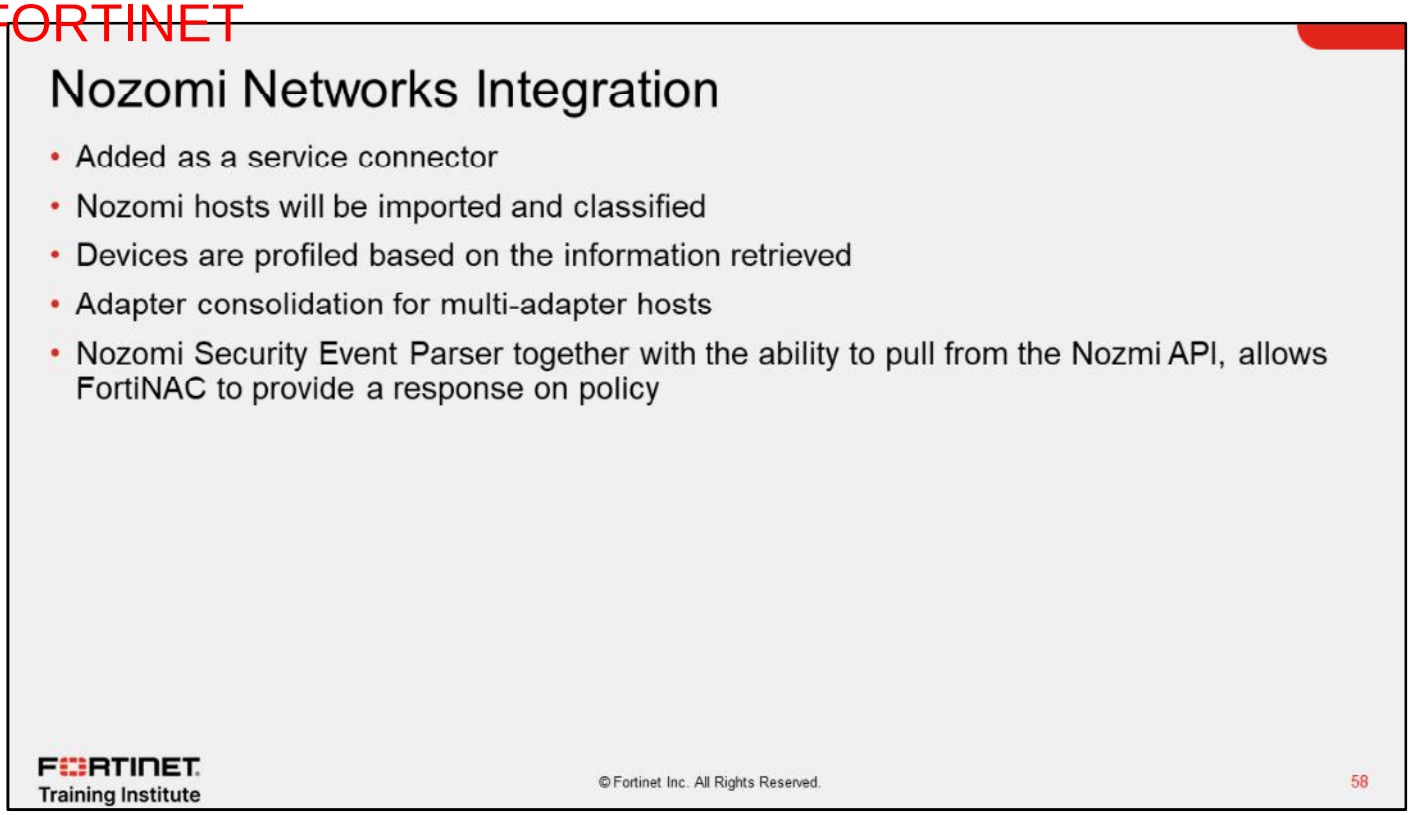
DO NOT REPRINT
© FORTINET



After you create a CSV file with all the required fields and entries, you can import it into the database from the **Users & Hosts** > **Hosts** view by clicking **Import** and then clicking **Browse**. Navigate to and choose the CSV file and click **OK**. The entries will appear in an **Import Results** window. Click **OK** to close the window. The imported records will now be searchable within the different visibility views.

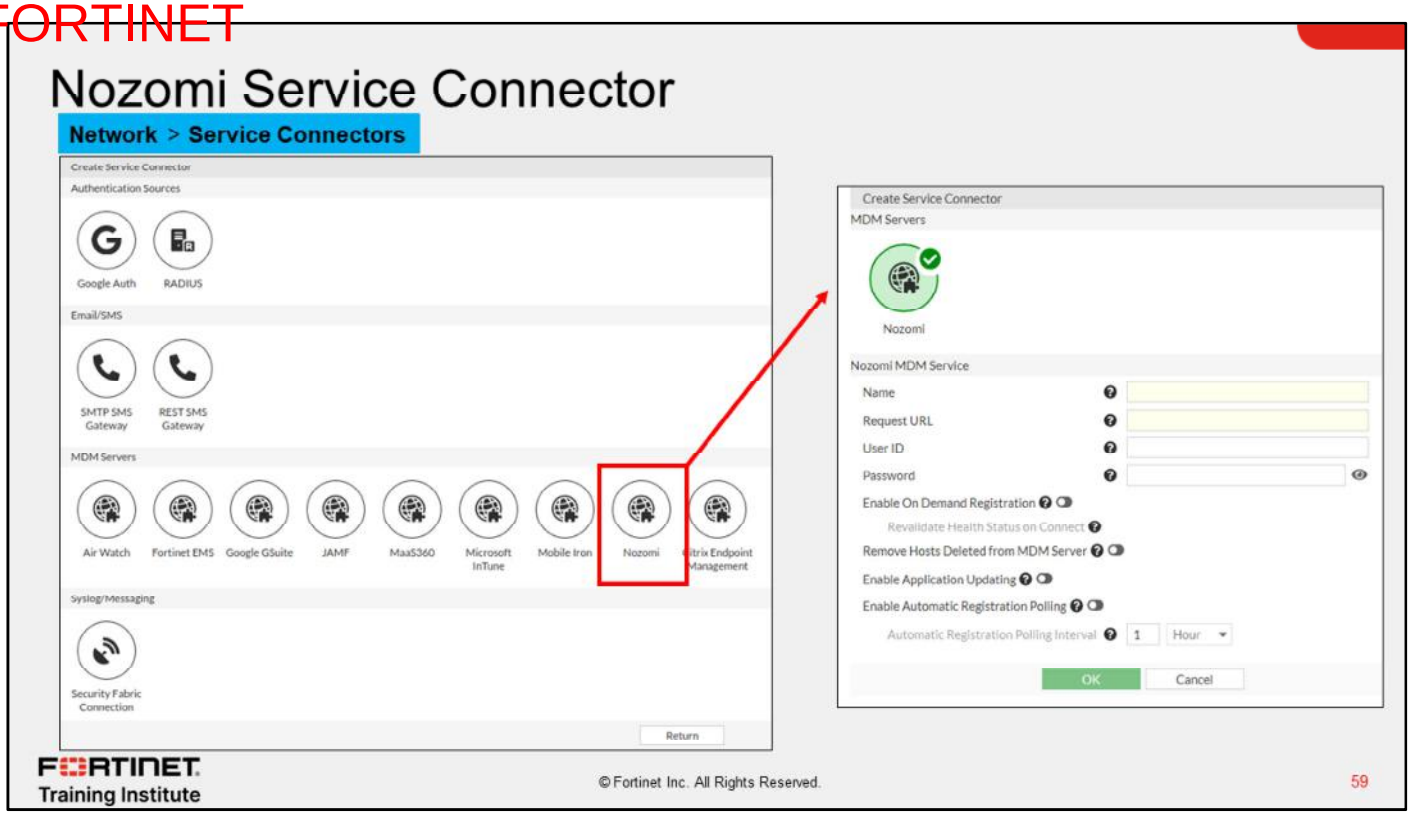
Note that the **Import** option is visible only after the **Legacy View Architecture** option is enabled under **System** > **Feature Visibility**.

DO NOT REPRINT
© FORTINET



FortiNAC provides out-of-the-box integration capabilities with Nozomi Networks device management, a tool designed for OT and IoT environments. Devices known to Nozomi can be imported and registered or classified automatically. The imported devices will be profiled based on information retrieved from the Nozomi product. Devices with multiple network adapters will have the devices consolidated under the single device in the FortiNAC. Automated responses to Nozomi events can be configured using the pre-existing event parser.

DO NOT REPRINT
© FORTINET

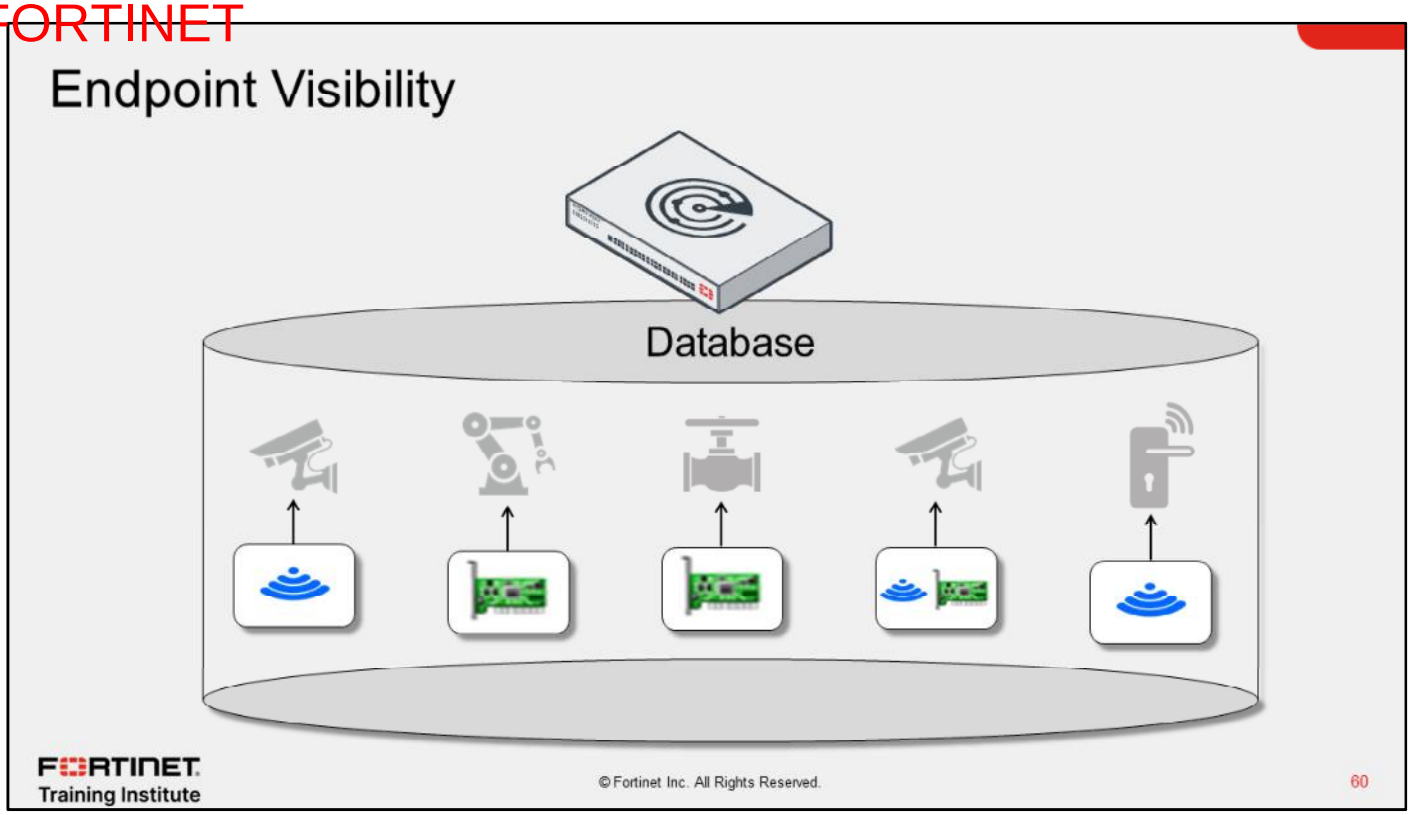


The Nozomi integration is performed from the **Network** > **Service Connectors** view. Click **Create New** to create a new integration. Select **Nozomi** from the **MDM Servers** list, name the integration, and fill in the appropriate communication parameters.

Use the appropriate behavioral options for the integration:

- **Enable On Demand Registration** triggers the FortiNAC to query the MDM whenever a host reaches the captive portal for onboarding. If the host is found in the MDM, it is registered using the data obtained from the MDM.
- **Revalidate Health Status on Connect** prompts FortiNAC to query the MDM for host compliance whenever hosts connect to the network. This is disabled by default, and can generate a lot of overhead for the MDM.
- **Remove Hosts Deleted from the MDM Server** prompts FortiNAC to remove hosts from its database, if they have been deleted from the MDM server.
- **Enable Application Updating** prompts FortiNAC to retrieve and store the application inventory for hosts that are in the FortiNAC database.
- **Enable Automatic Registration Polling** sets the time interval for MDM server polling by the FortiNAC.

DO NOT REPRINT
© FORTINET



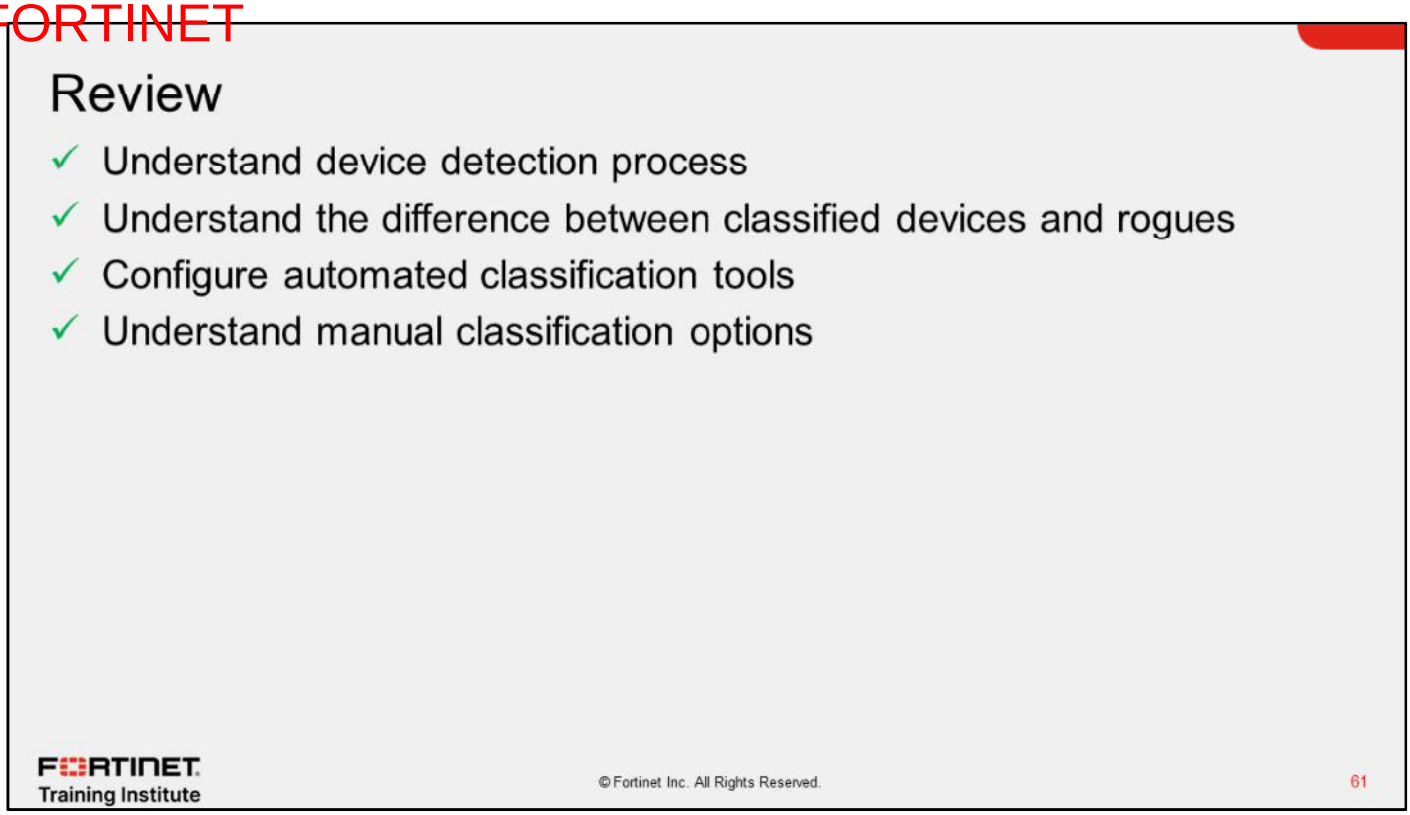
Network visibility is the first step to building a comprehensive network security solution that will profile and track all the endpoints accessing your network.

Host and adapter information is gathered from communication with the infrastructure, DHCP fingerprints and agent technology. Hosts will have associated adapters and a variety of host properties, such as hostname, operating system, and expiration dates. This host information makes up part of the What component of visibility.

Adapters are associated with hosts and contain a set of properties as well, such as physical address and IP address information. This adds additional information to the what component. Communication with the infrastructure adds where a particular adapter is connected and historic information is retained to track where it was connected in the past. This fills in the where and when information.

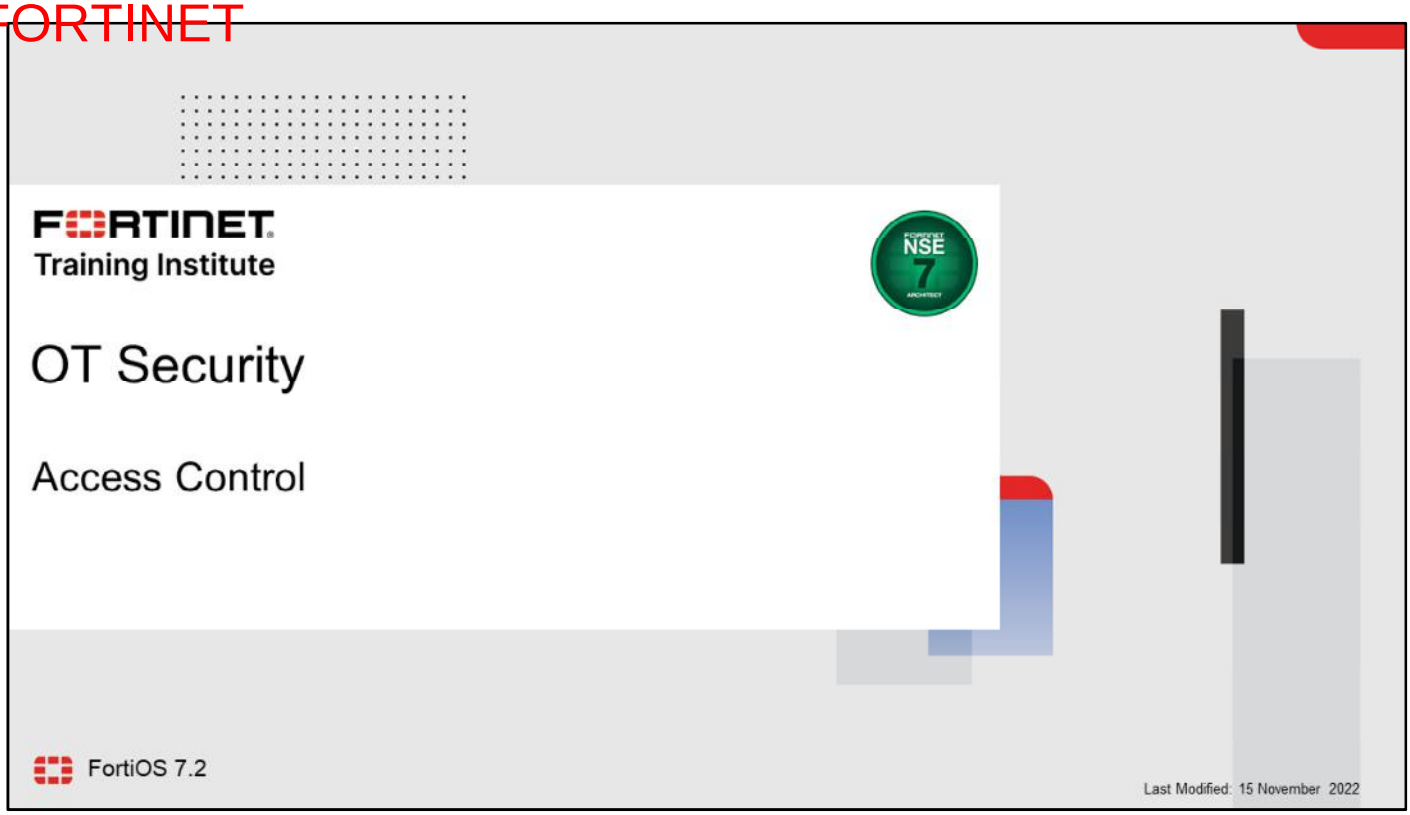
Endpoint devices represented in the database can have varying levels of attributes. An OT or IoT device, for example, may have nothing more than an adapter associated to it. It may have applications that communicate with control systems. It may have wired, wireless adapters, or both. These devices are most often displayed in the **Host View** with the visibility detail broken down into two categories: hosts (these are the devices), and associated adapters.

DO NOT REPRINT
© FORTINET



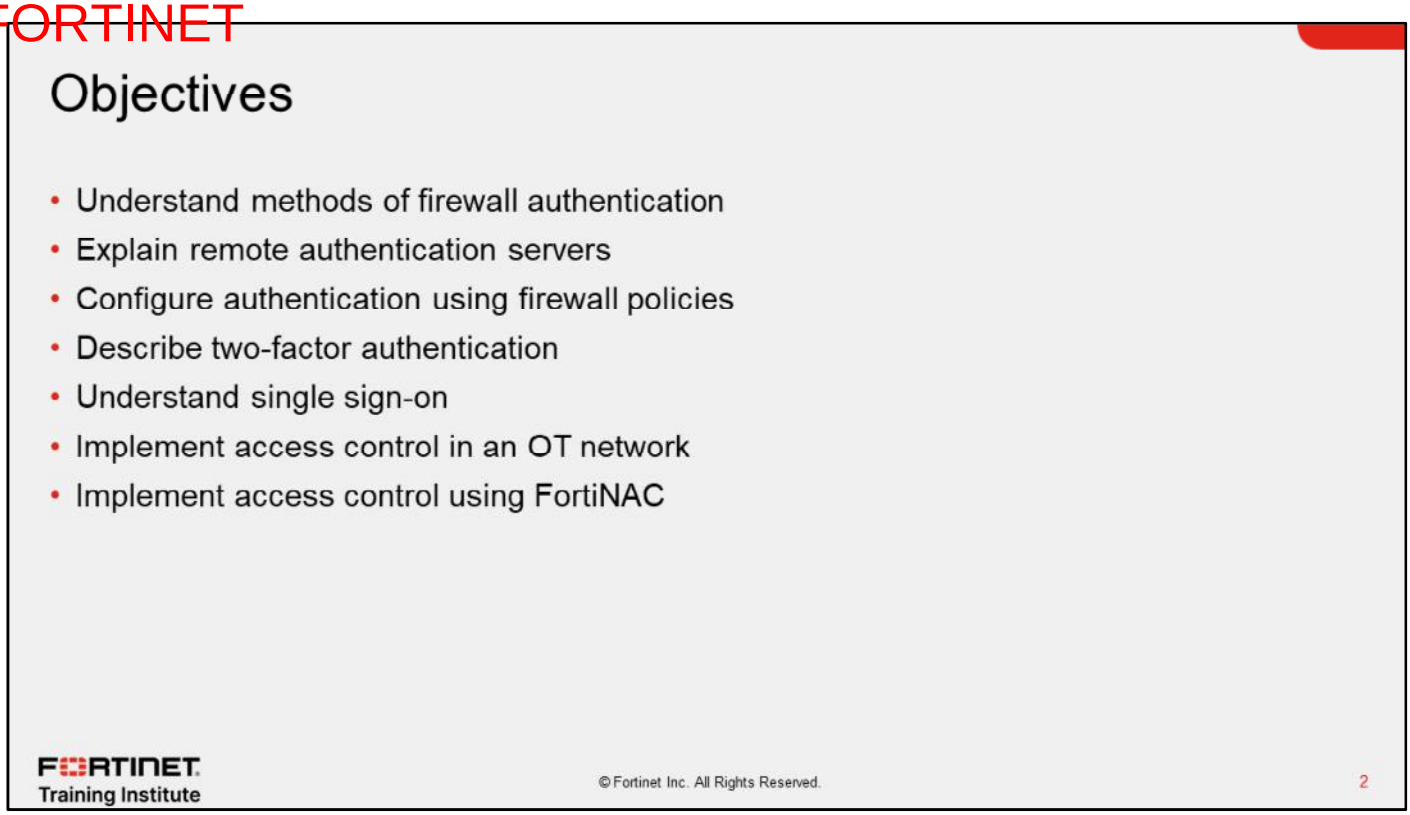
This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how perform asset management in an OT network.

DO NOT REPRINT
© FORTINET



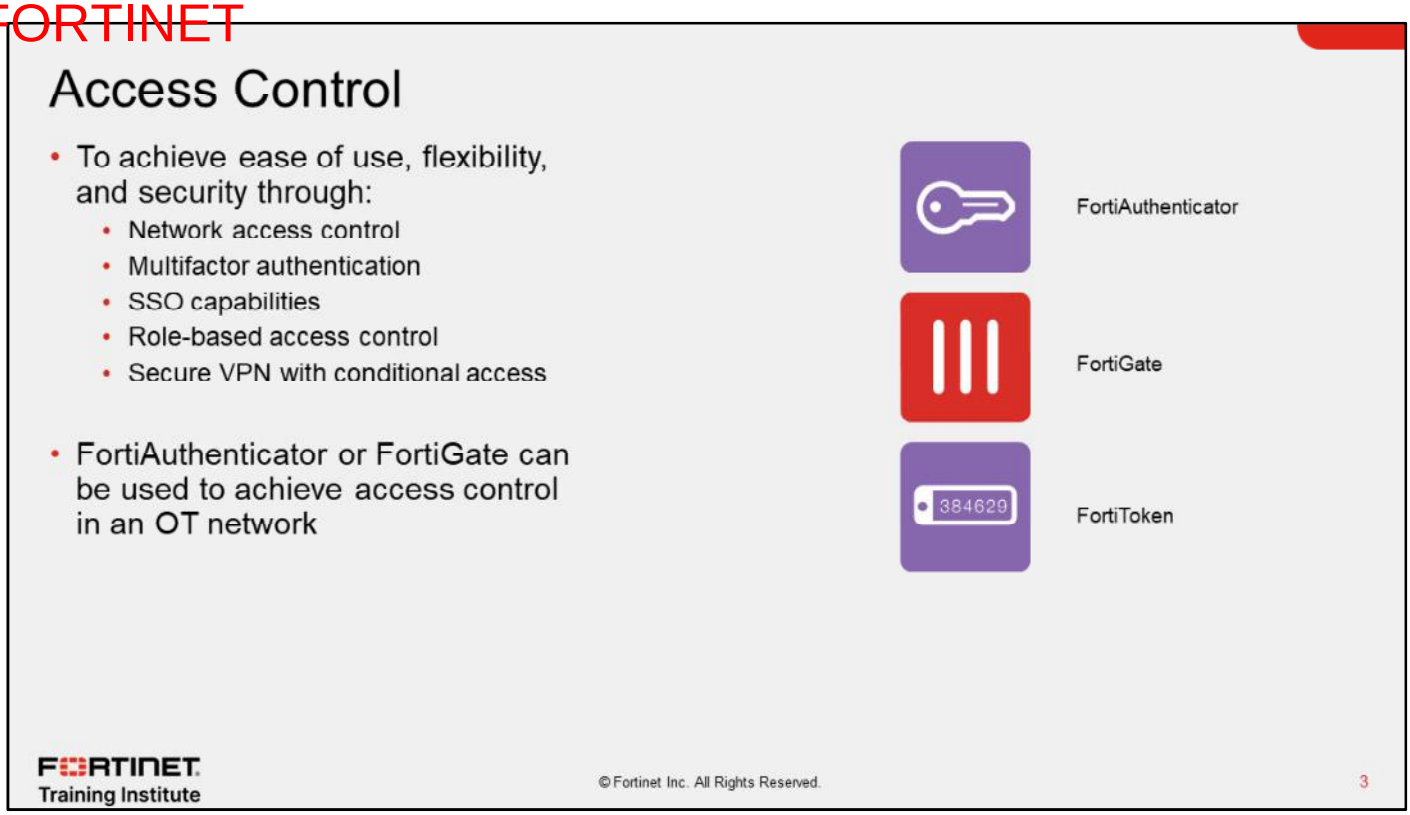
In this lesson, you will learn about access control methods in an OT network.

DO NOT REPRINT
© FORTINET



After completing this lesson, you should be able to achieve the objectives shown on this slide.

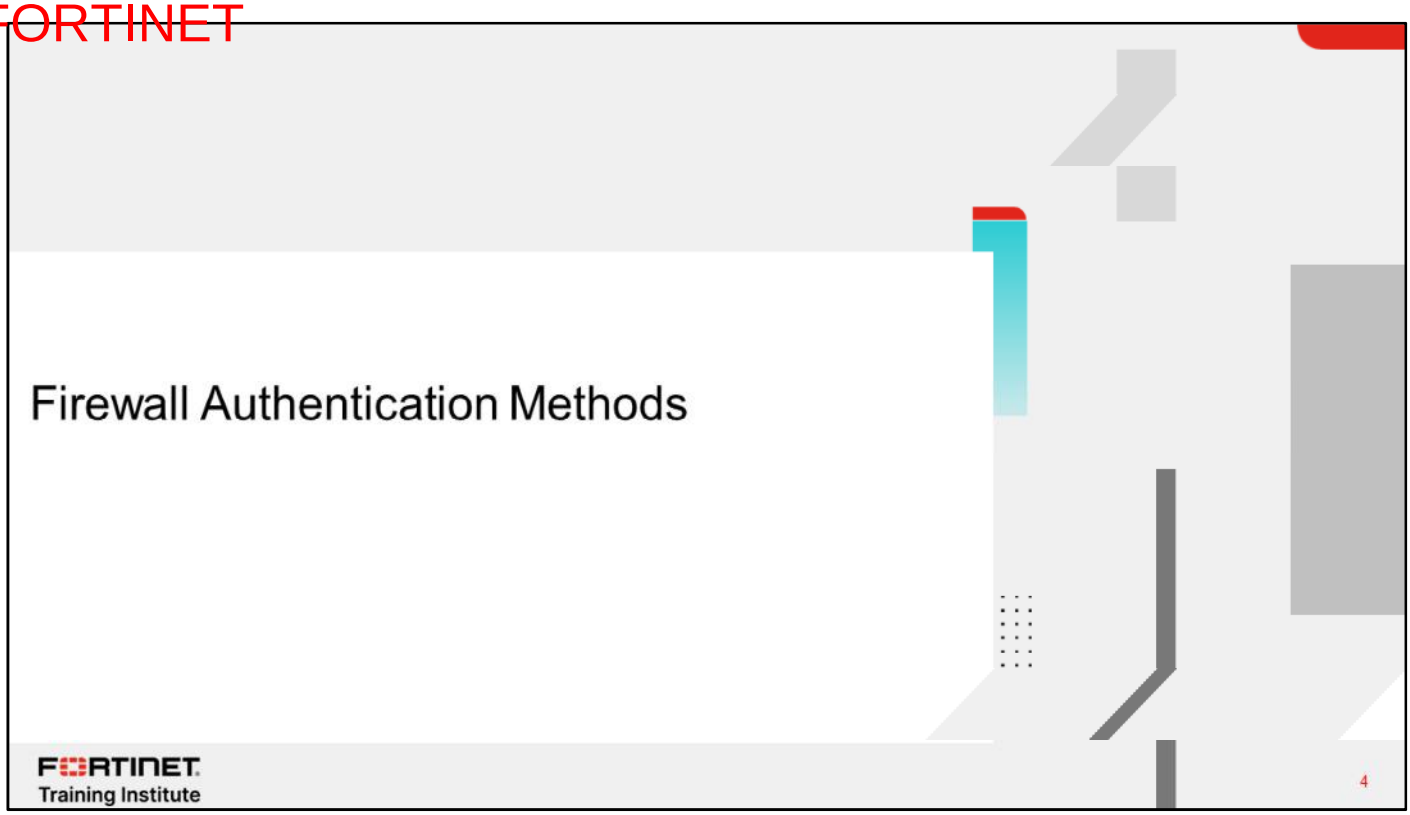
DO NOT REPRINT
© FORTINET



The main motive behind achieving access control in an OT environment is to access the assets easily and securely. By implementing access control in an OT environment you will provide operators access to their allowed applications easily, and most importantly, securely.

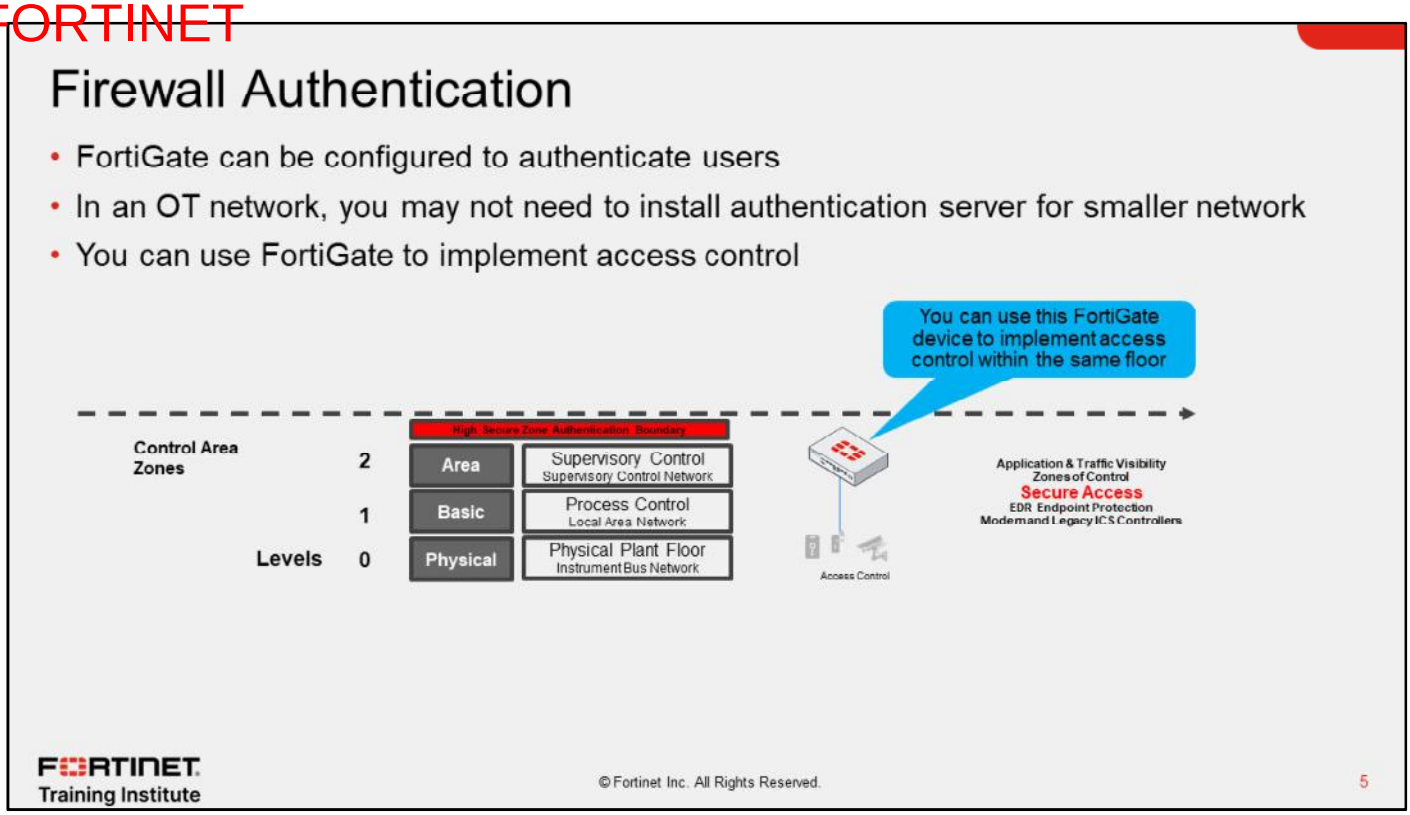
In this lesson, you will learn about different methods of authentication. These methods can be configured using FortiGate or FortiAuthenticator.

DO NOT REPRINT
© FORTINET



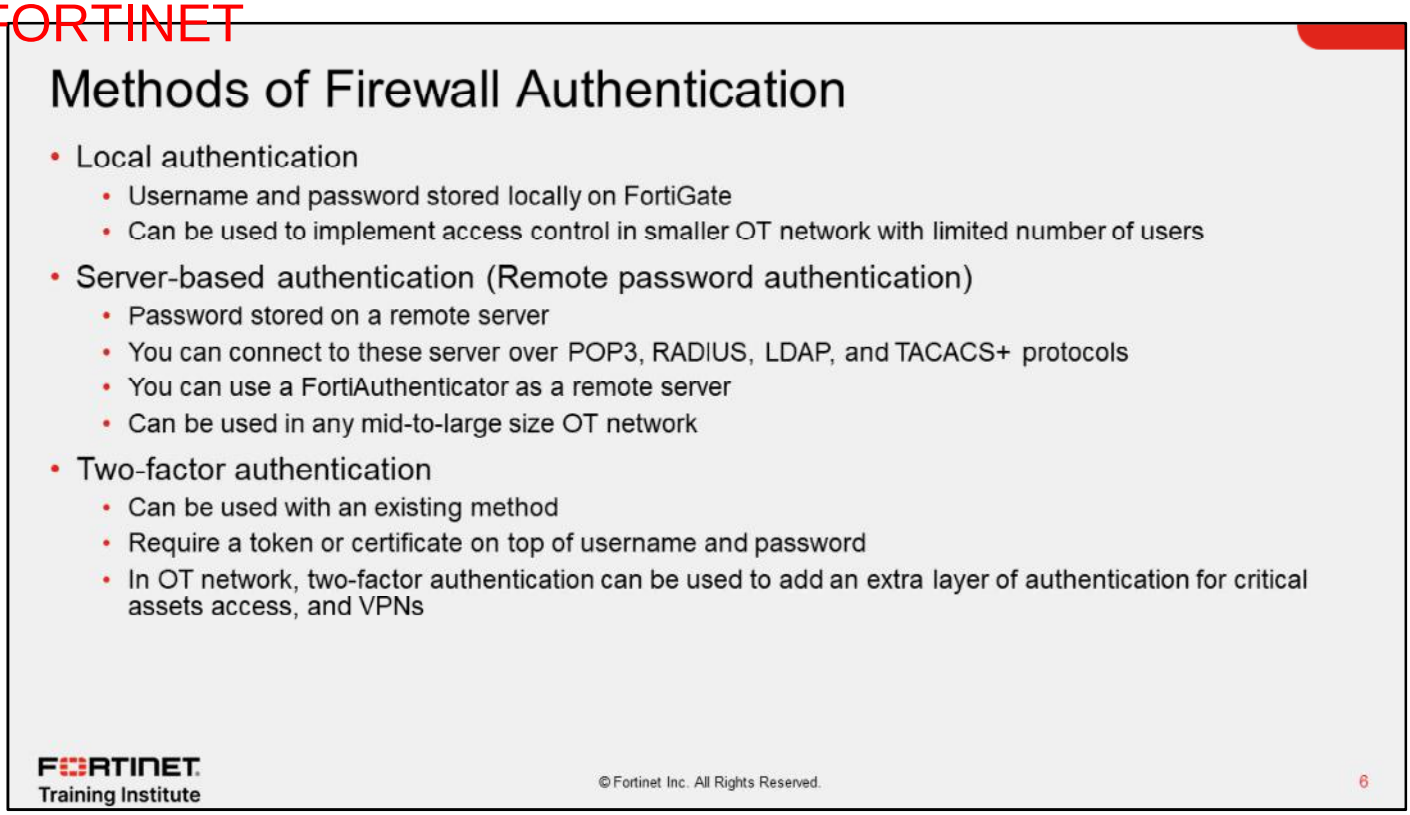
In this section, you will learn about different types of firewall authentication.

DO NOT REPRINT
© FORTINET



FortiGate can be used as a authentication server. You can create users profiles and use it for authentication on a FortiGate device. Not all OT networks are big enough that you need an external authentication server. You can use FortiGate to implement access control for OT networks.

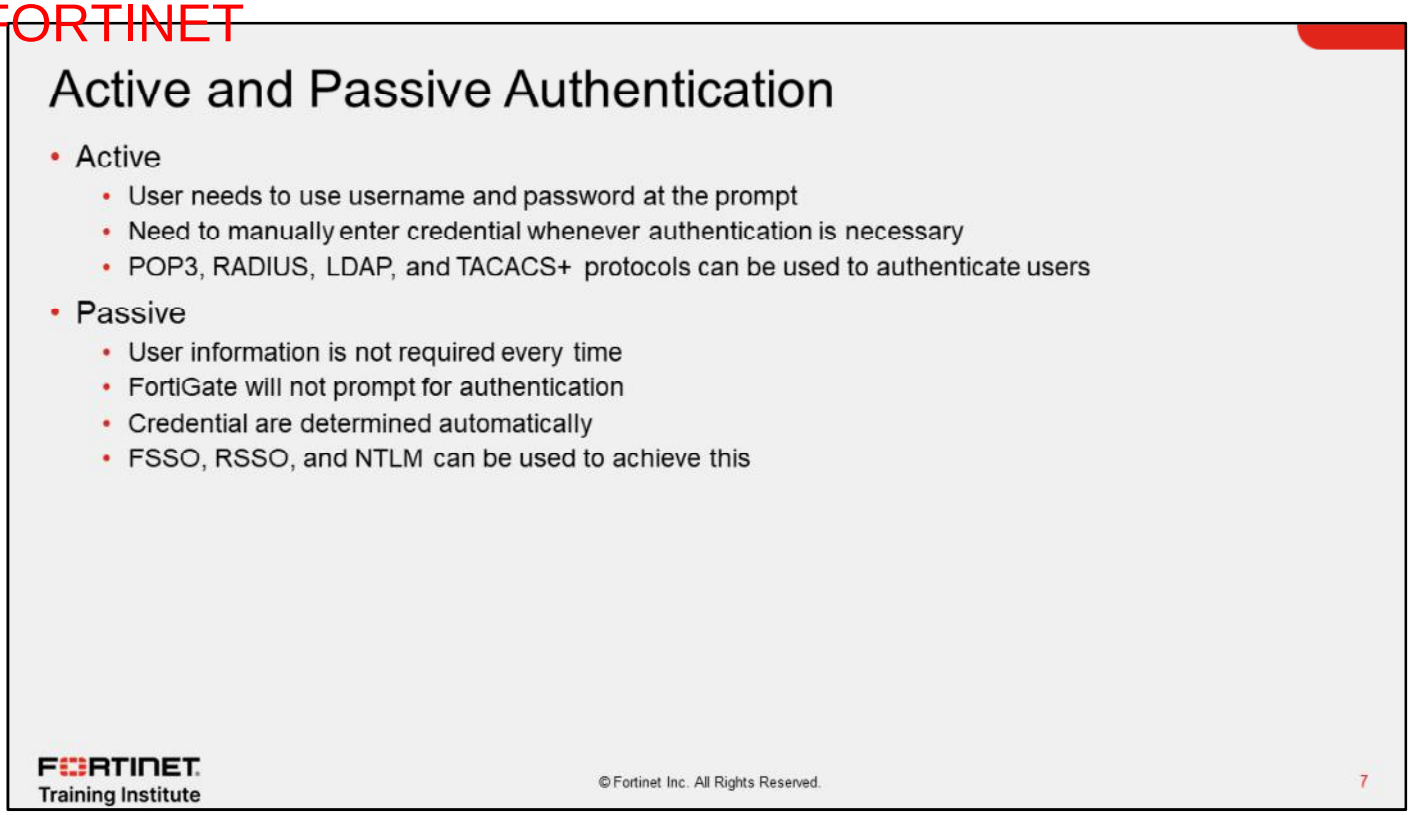
DO NOT REPRINT
© FORTINET



FortiGate offers the following authentication methods. These methods can also be configured on a FortiAuthenticator as well.

- Local authentication: In this method, you can configure and store a username and password on FortiGate. Local authentication can be used to implement access control in smaller OT networks with a limited number of users.
- Server-based: In this method, FortiGate relies on a remote server to authenticate users. You can use POP3, RADIUS, LDAP, and TACACS+ protocols to connect to the remote server. To save firewall resources, it is recommended to use an external authentication server or FortiAuthenticator.
- Two-factor: You can use this method to add an extra layer of authentication with a username and password. A token, or a certificate can be used for the two-factor authentication. In an OT network, two-factor authentication can be used to add an extra layer of authentication for critical assets access and VPNs.

DO NOT REPRINT
© FORTINET



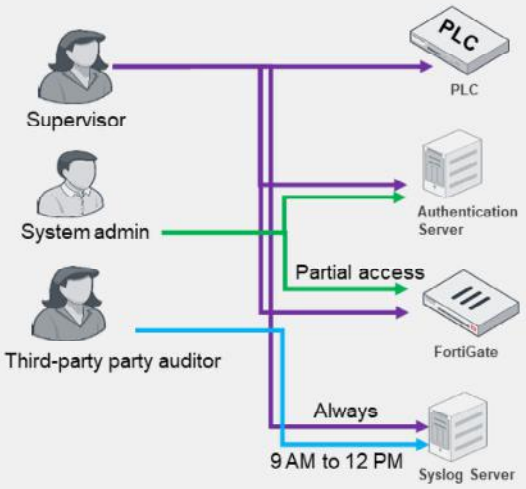
Local authentication, remote authentication, and two-factor authentication are called active authentication. Active authentication simply means users are required to enter their credentials every time before being granted access.

On the other hand, some users can be granted access transparently, because user information is determined without asking the user to enter their login credentials. This is known as passive authentication. Single sign-on is a passive authentication method.

DO NOT REPRINT
© FORTINET

Role-Based Authentication

- Assign device access based on role to restrict access for business critical devices and servers
- Create separate user groups for different roles and use them to allow access throughout the network
- Carefully create a list of devices and servers and determine an access list based on roles
- Third-party user access can be scheduled to allow access during a set time window



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

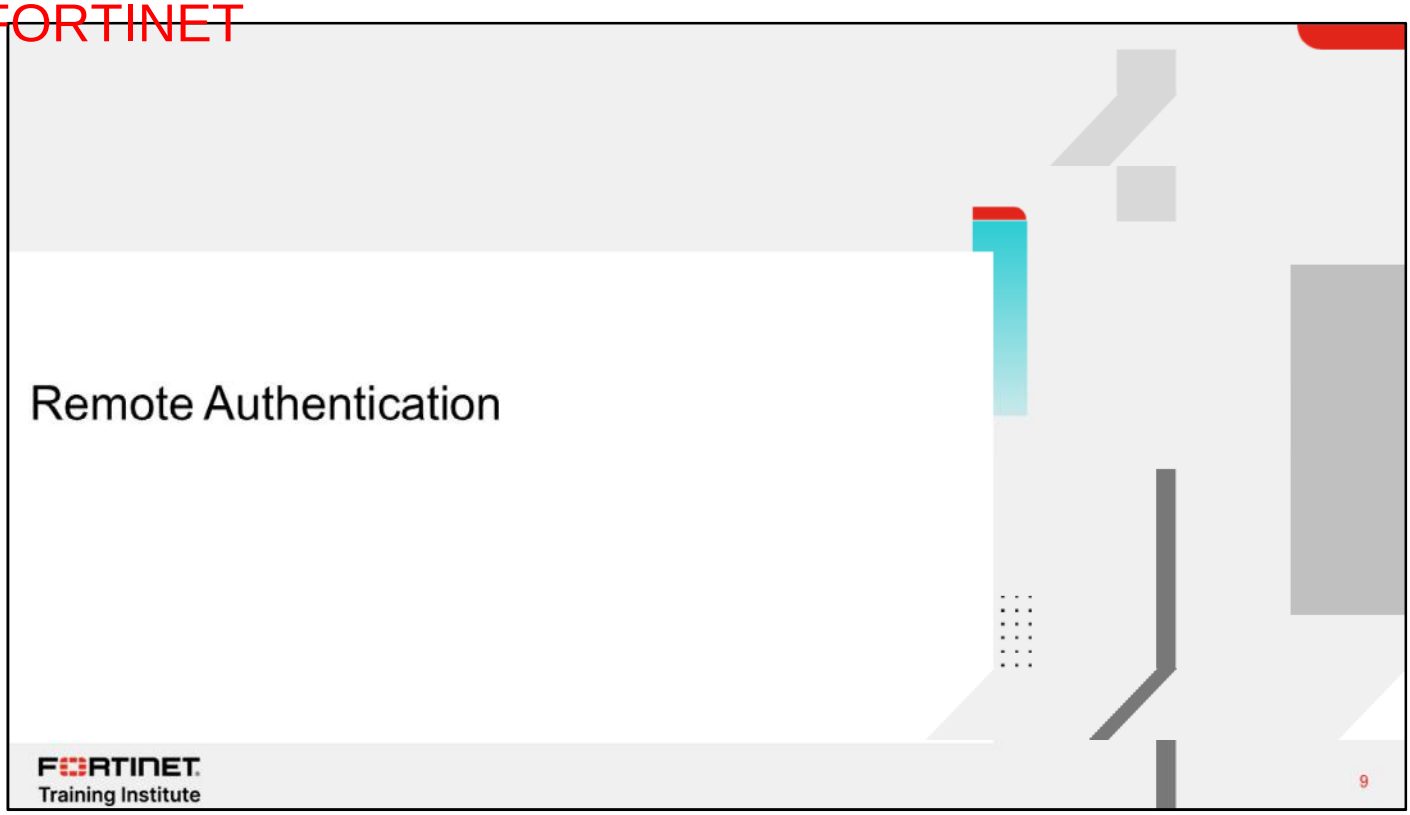
8

In an OT network, different users have different duties. Not all users require access to all devices. It is very critical, in an OT network, to come up with a strategy to assign different access for different roles to avoid any security risks.

Role-based authentication can be very helpful to achieve this. You can create different groups for different roles and assign them to allow, or restrict access to network devices and servers using the firewall policies. You can also use the firewall policies to restrict access to third-party users to restrict access for a time window to minimize any risk.

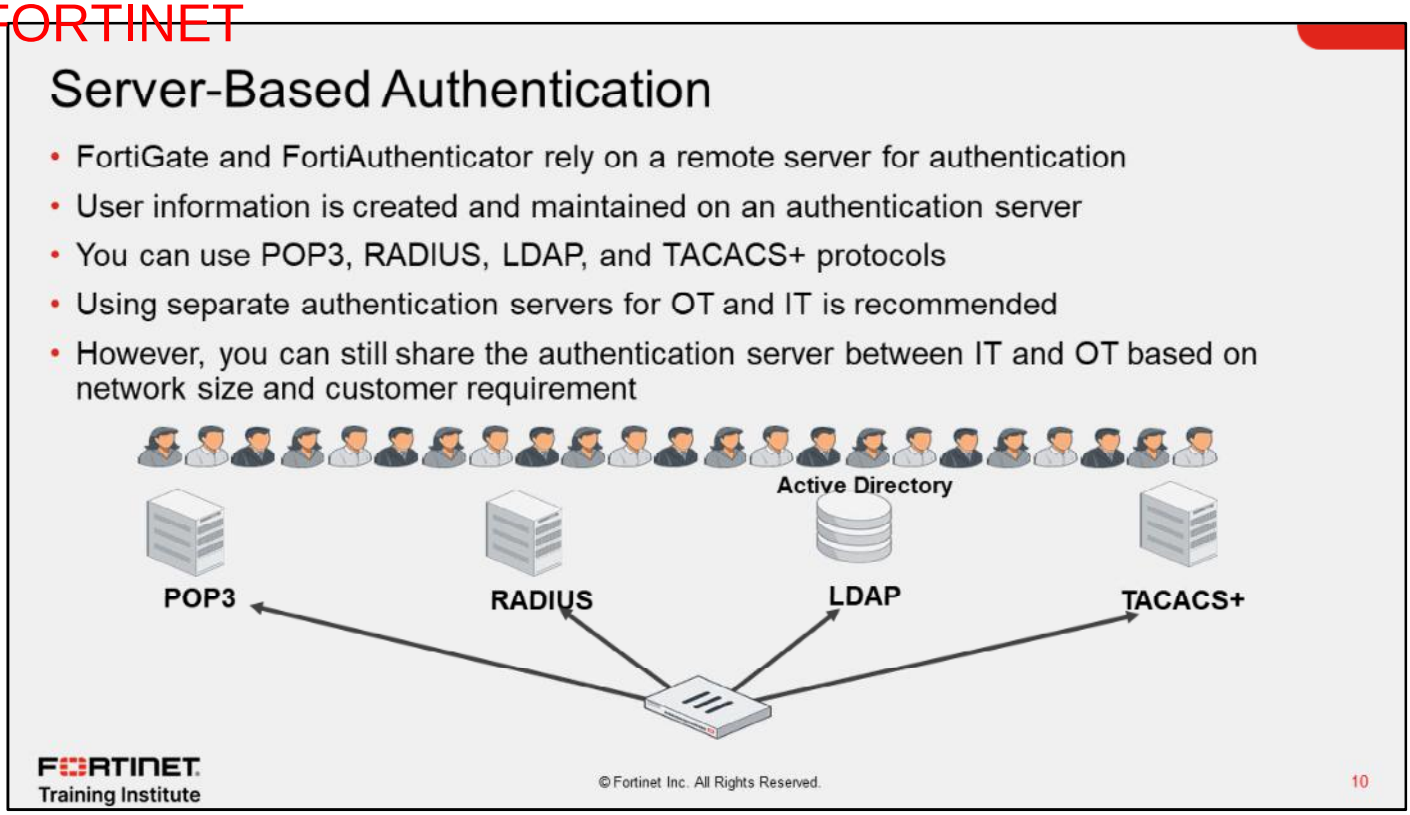
You can configure and maintain role-based user groups on FortiGate, FortiAuthenticator, or any remote authentication server.

DO NOT REPRINT
© FORTINET



In this section, you will learn about remote authentication.

DO NOT REPRINT
© FORTINET



In a larger OT network, it is difficult to create and manage local authentication with FortiGate devices. You need an external authentication server to centralize the user list. In this case, you can configure FortiGate with a remote authentication server or FortiAuthenticator to take care of the authentication. Using remote authentication you can create and maintain larger user list in a centralize location to save FortiGate recourses.

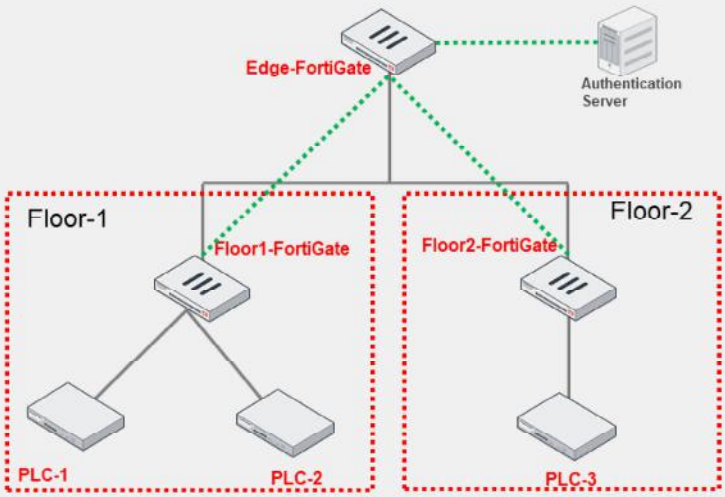
When you use a remote authentication server to authenticate users, FortiGate sends the user's entered credentials to the remote authentication server. The remote authentication server responds by indicating whether the credentials are valid or not. If valid, FortiGate consults its configuration to deal with the traffic. Note that it is the remote authentication server—not FortiGate—that evaluates the user credentials.

You should separate the authentication server between IT and OT. However, it can be shared based on customer network and requirements.

DO NOT REPRINT
© FORTINET

Securing the Remote Authentication Server

- You should keep the authentication server on separate interface or VLAN
- Make sure to allow only the authentication protocol to access the server
- Define source IP addresses to restrict access from select devices
- You can use FortiAuthenticator to pull user information from remote servers and use FortiAuthenticator as a remote server for all the Firewalls



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

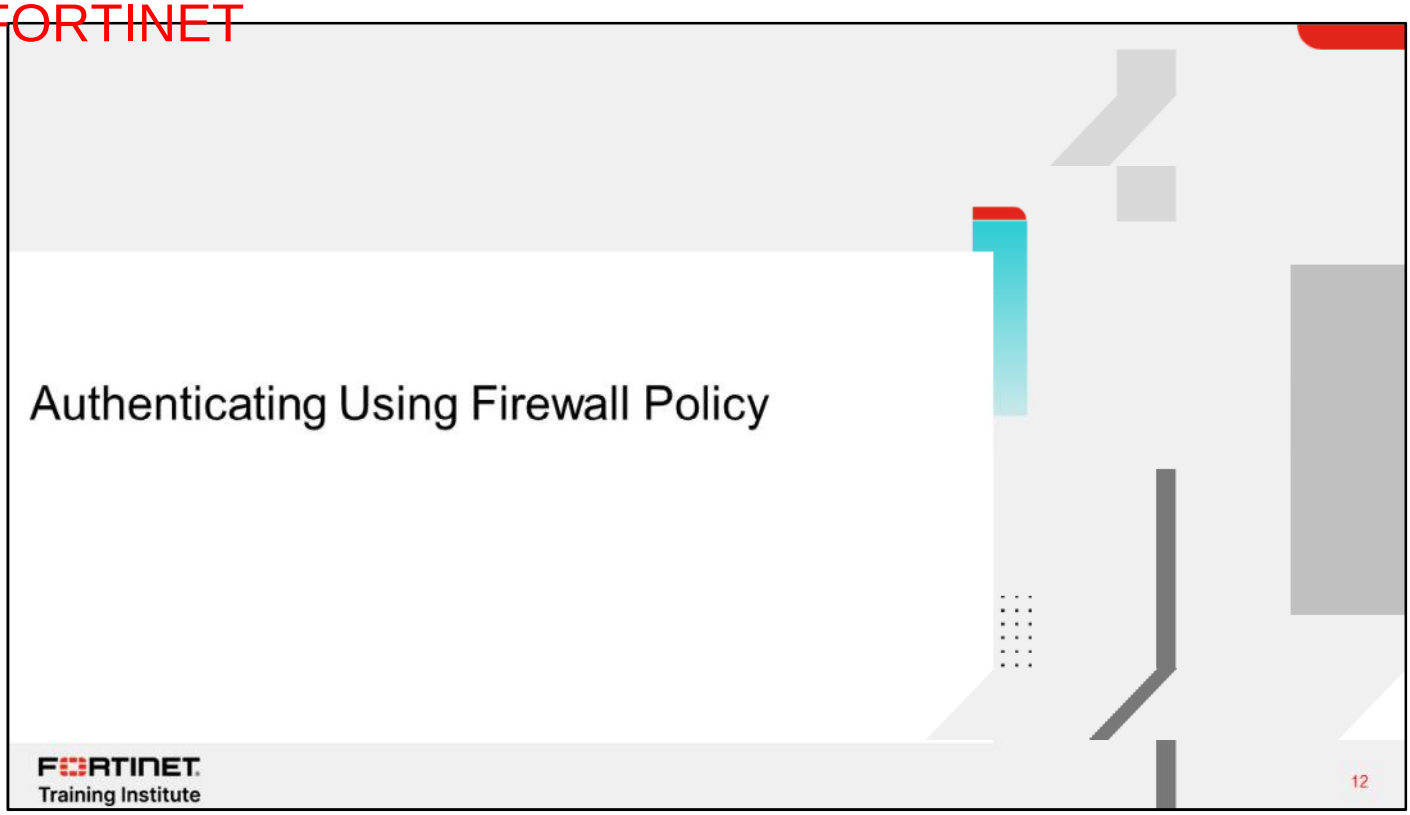
11

Using a remote authentication server requires you to secure the server from any threats and security risks. To secure the server you should do the following:

- Keep the authentication server behind the most restricted firewall
- Keep the authentication server on a separate interface or VLAN
- Create a policy that allows only authentication protocols to access the server
- Define source IP addresses in a policy to restrict access from select devices

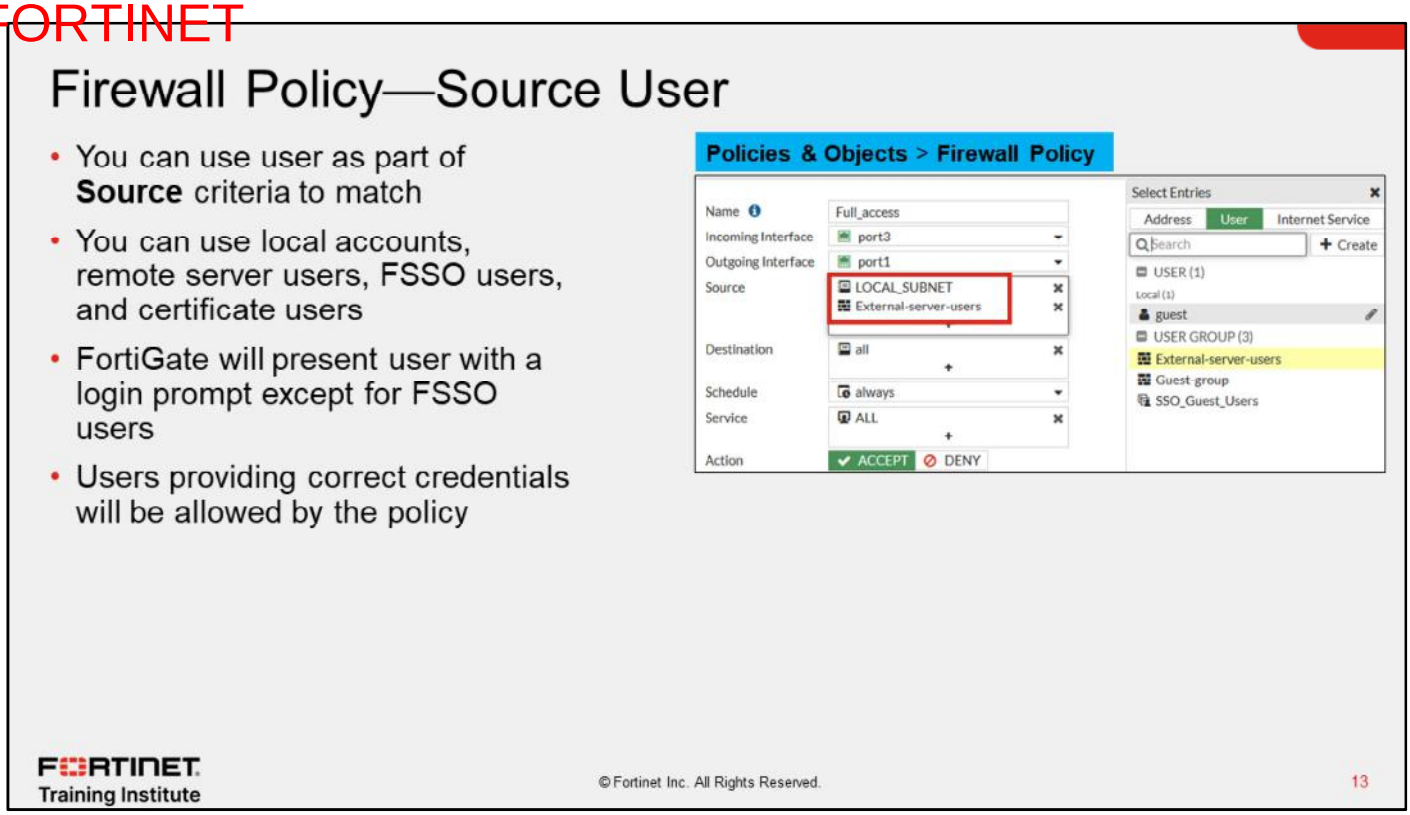
You can configure and use FortiAuthenticator as a remote server. You can configure and maintain user information, or pull information from remote server on FortiAuthenticator, and then use FortiAuthenticator as remote server on FortiGate.

DO NOT REPRINT
© FORTINET



In this section, you will learn about implementing authentication using firewall policy.

DO NOT REPRINT
© FORTINET



Whenever a user initiates traffic and the firewall receives the initial connection, FortiGate checks the firewall policies to determine whether to accept or deny the communication session. You can configure firewall policies to inspect different criteria to allow or deny traffic. One instruction is to check authentication. You can use the source of a firewall policy for this purpose. The source of a firewall policy must include the source address (IP address), but you can also include the user, and user group. In this way, any user, or user group that is included in the source definition for the firewall policy can successfully authenticate.

You can include local user accounts, remote server users and groups, PKI users, and FSSO users.

DO NOT REPRINT
© FORTINET

Mixed Firewall Policies

- Using authentication on a policy does not always force an active authentication prompt
- Three options:
  - Enable authentication on every policy that could match the traffic
  - Enforce authentication on demand option (CLI option only)
  - Enable a captive portal on the ingress interface for the traffic
- If login cannot be determined passively, then FortiGate uses active authentication
  - FortiGate will not prompt the user for login credentials when the user can be determined passively
  - By default, active authentication is intended to be used as a backup when passive authentication fails

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
port3 → port1 2									
1	Full_Access	Maintenance-users LOCAL_SUBNET	all	always	Web Access	ACCEPT	Enabled	no-inspection	UTM
2	Limited	LOCAL_SUBNET	all	always	Web Access	ACCEPT	Enabled	no-inspection	UTM

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

In the example shown on this slide, assuming active authentication is used, any initial traffic from LOCAL_SUBNET will not match policy sequence 1 (Full_Access). Policy ID 1 looks for both IP and user, and user group information (LOCAL_SUBNET and Maintenance-users respectively), and since the user has not yet authenticated, the user group aspect of the traffic does not match. Since the policy match is not complete, FortiGate continues its search down the sequence list, to see if there is a complete match.

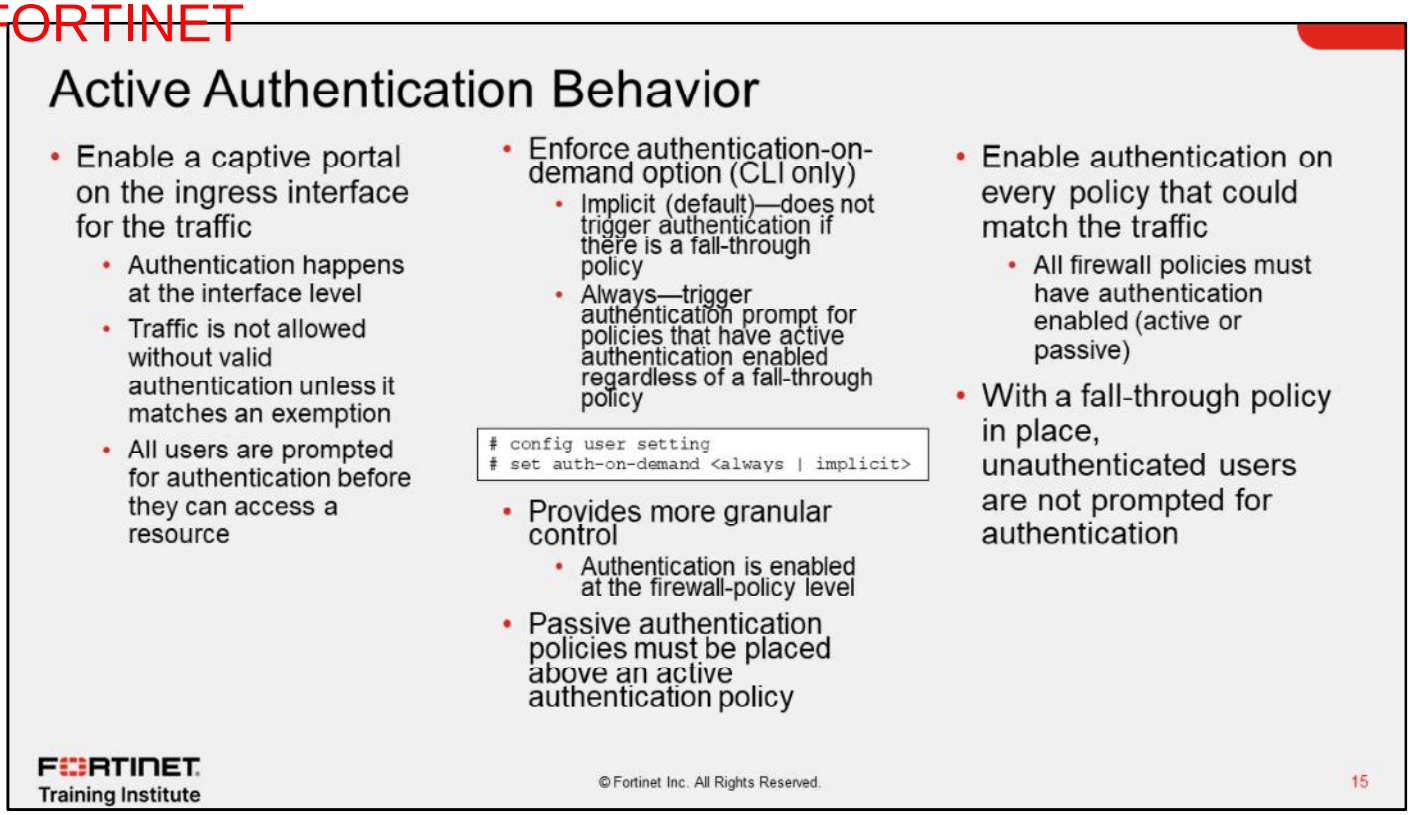
Next, FortiGate evaluates policy ID 2 to see if the traffic matches. It matches all criteria, so traffic is allowed with no need to authenticate.

When only active authentication is used, if all possible policies that could match the source IP have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol). In other words, if policy ID 2 also had authentication enabled, the users would receive login prompts.

If passive authentication is used and it can successfully obtain user details, then traffic from LOCAL_SUBNET with users that belong to Maintenance-users will apply to policy ID 1, even though policy ID 2 does not have authentication enabled.

If you are using both active and passive authentication, and a user's credentials can be determined through passive authentication, the user will never receive a login prompt, regardless of the order of any firewall policies. This is because there is no need for FortiGate to prompt the user for login credentials when it can determine who the user is passively. When active and passive authentication methods are combined, active authentication is intended to be used as a backup, to be used only when passive authentication fails.

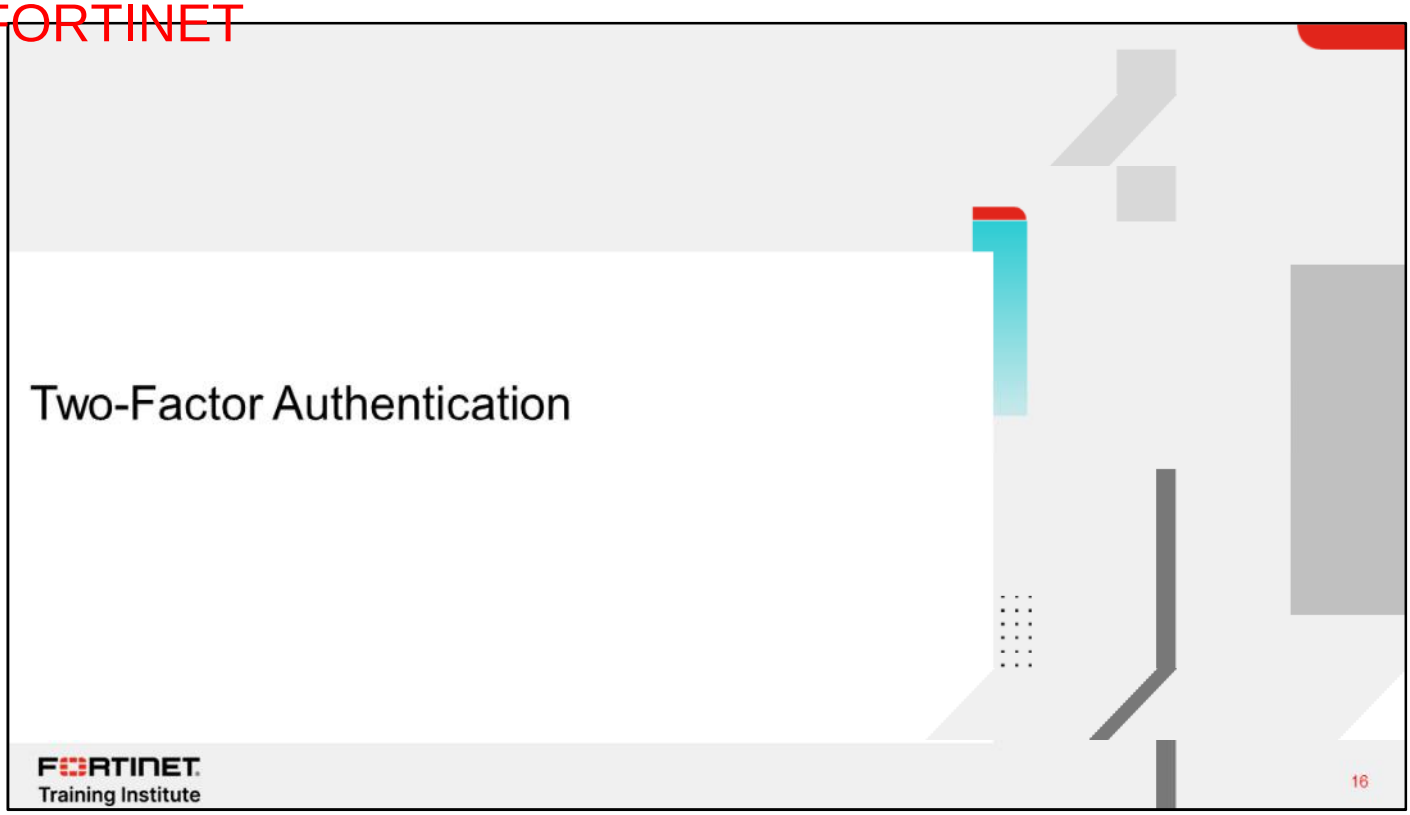
DO NOT REPRINT
© FORTINET



You can alter active authentication behavior in three different ways:

- If you configure an active authentication firewall policy followed by a fall-through policy that does not have authentication enabled, then all traffic uses the fall-through policy. This means that users are not required to authenticate. By default, all traffic passes through the catch-all policy without being authenticated. You can alter this behavior by enabling authentication on all firewall policies. When you enable authentication, all the systems must authenticate before traffic travels to the egress interface.
- Alternatively, on the CLI only, you can change the auth-on-demand option to `always`. This instructs FortiGate to trigger an authentication request if a firewall policy with active authentication is enabled. In this case, the traffic is not allowed until authentication is successful.
- To have all users connect to a specific interface, it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

DO NOT REPRINT
© FORTINET



In this section, you will learn about two-factor authentication.

DO NOT REPRINT
© FORTINET

One-Time Password Tokens

- Can be used as second factor authentication on top of the username and password
- Generates passwords that can only be used once
- Secured from reply attacks
- You can use the following methods for OTP:
  - Hardware tokens
  - Software tokens
  - FortiToken cloud
  - Email or SMS-based delivery
- Use in OT:
  - For critical servers and assets access
  - VPN access for remote users



FORTINET Training Institute

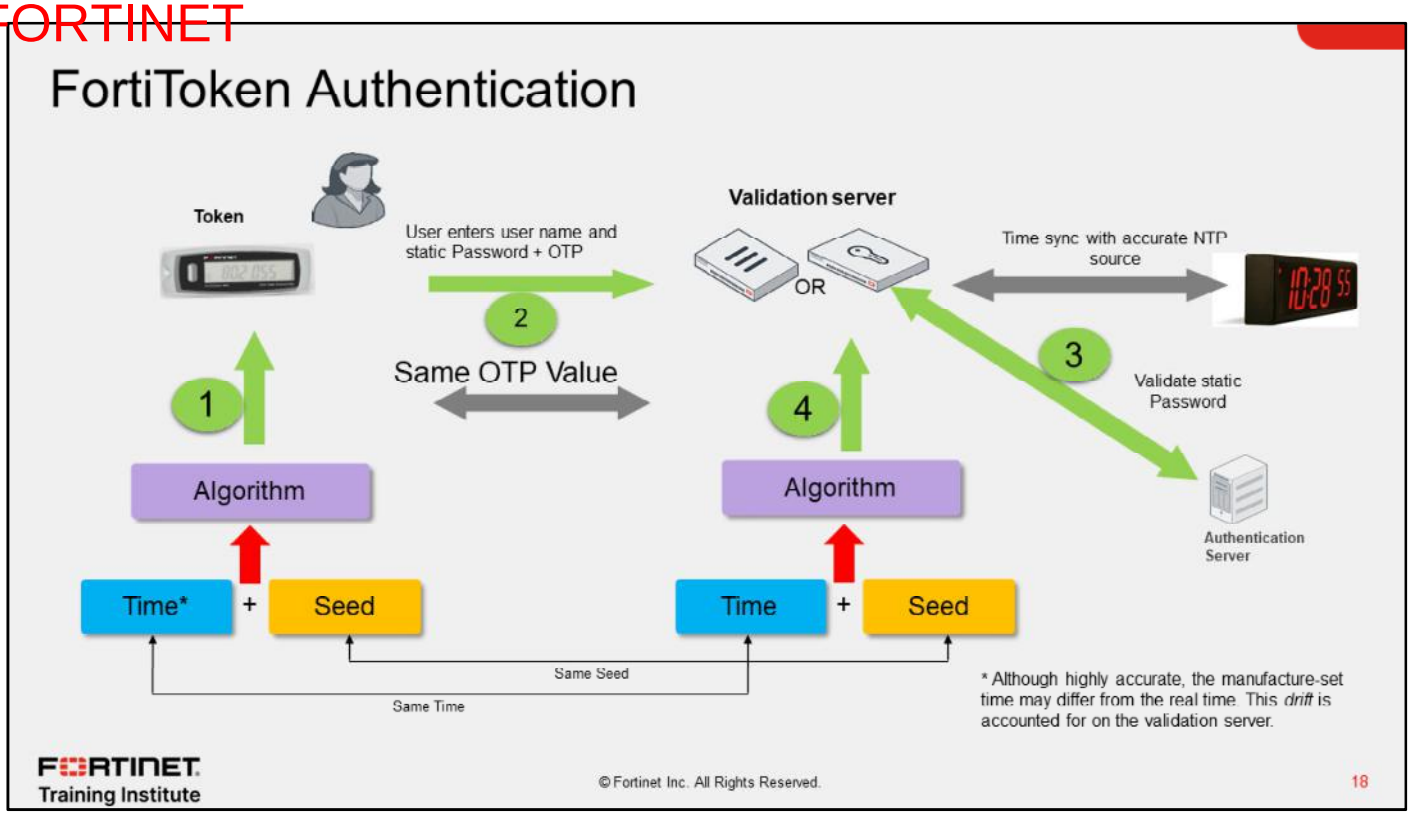
© Fortinet Inc. All Rights Reserved.

17

Two-factor authentication with the one-time password (OTP) method is to add an additional layer of authentication. OTP is not used as standalone solution, but to be used with an existing authentication method for username and password. OTP generates passwords that can only be used once, for a specific time period (usually 60 seconds). OTP is not vulnerable to reply attacks.

In an OT environment , you should use two-factor authentication for critical server and asset access, and for VPN access for the remote users.

DO NOT REPRINT
© FORTINET



Now you will review two-factor authentication workflow with tokens:

1. A token uses an algorithm to create OTP. This algorithm consists of a seed and the time. A single passcode is valid for only a short interval (usually 60 seconds) and then a new one generates. The cycle of generating passwords repeats over and over again.
2. A user is required to authenticate using credentials (username and password).
3. After the user provides the credentials, FortiGate validates the credentials based on the authentication method that is configured on FortiGate. After the credentials are verified, FortiGate asks the user to enter the second factor authentication; that is, OTP.
4. The validation server has the seed being used by the token. The validation server uses this seed and system time to generate OTP. Now, the validation server will match this OTP with the one it received from the user. If it's a match, the user will be successfully authenticated.

DO NOT REPRINT
© FORTINET

Two-Factor Authentication—FortiGate and FortiAuthenticator

- FortiGate (native FortiOS validation server):
  - Scope if specific to one instance of FortiGate device or an HA pair
  - Built-in validation server
  - Used for single FortiGate deployment of Firewall or VPN
  - Integrates with AD/LDAP directory
  - Supports all methods of OTP
- FortiAuthenticator (remote validation server):
  - For multiple FortiGate devices
  - Can be used for other applications and NAS devices
  - Supports RADIUS, LDAP, and REST API authentication methods
  - Includes a built-in LDAP server
  - Supports all methods of OTP





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

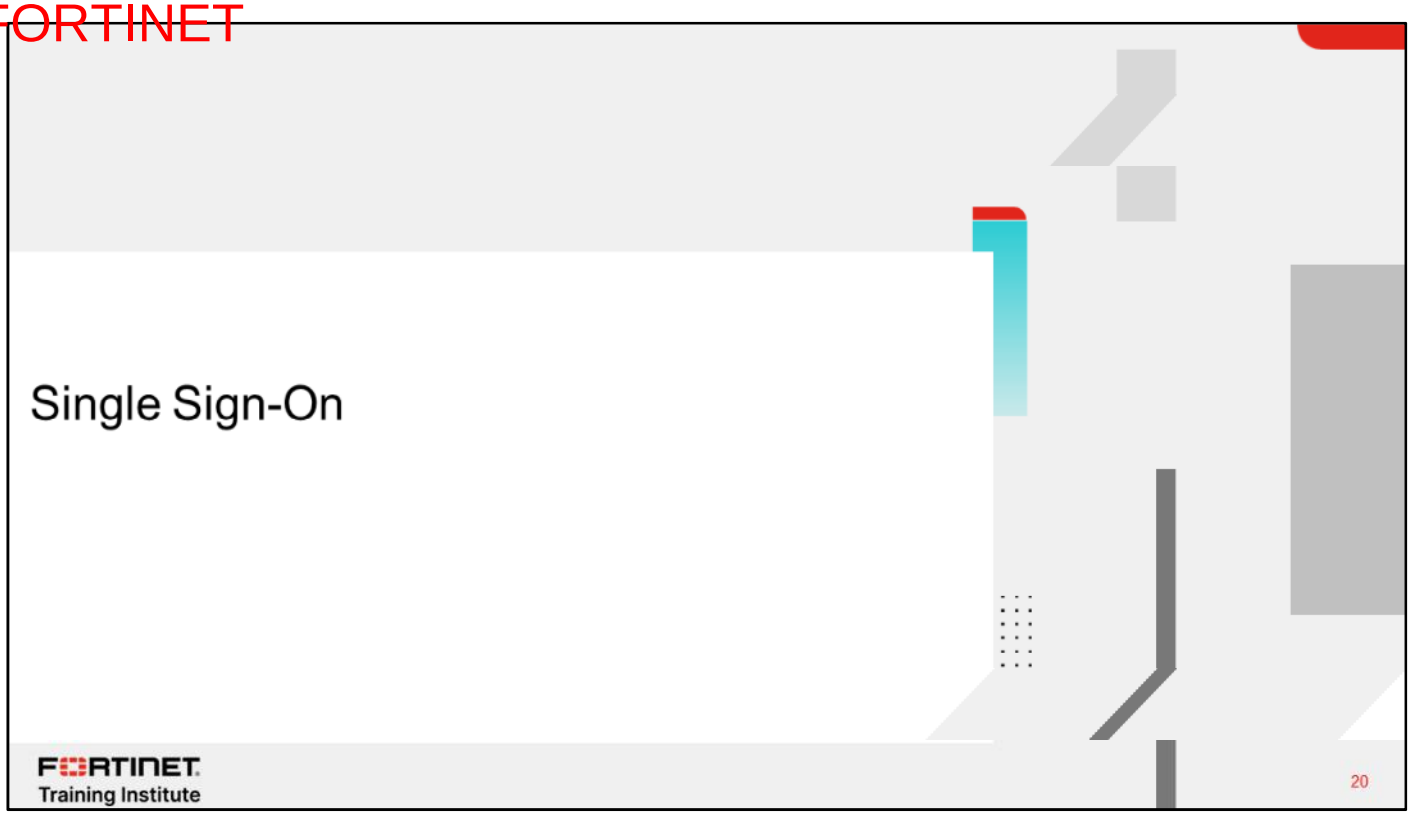
FortiGate and FortiAuthetnicator both offer all four methods for OTP. So, what are the key benefits of using FortiAuthetnicator for two-factor authentication?

With FortiGate, by design, the scope of two-factor authentication without FortiAuthenticator is specific and limited to one instance of FortiGate (or HA pairs). So, it works well only in cases where tokens are stored on only one FortiGate device.

FortiAuthenticator can support multiple FortiGate devices or other third-party vendor devices. With FortiAuthenticator, one FortiToken can be used to authenticate to multiple systems.

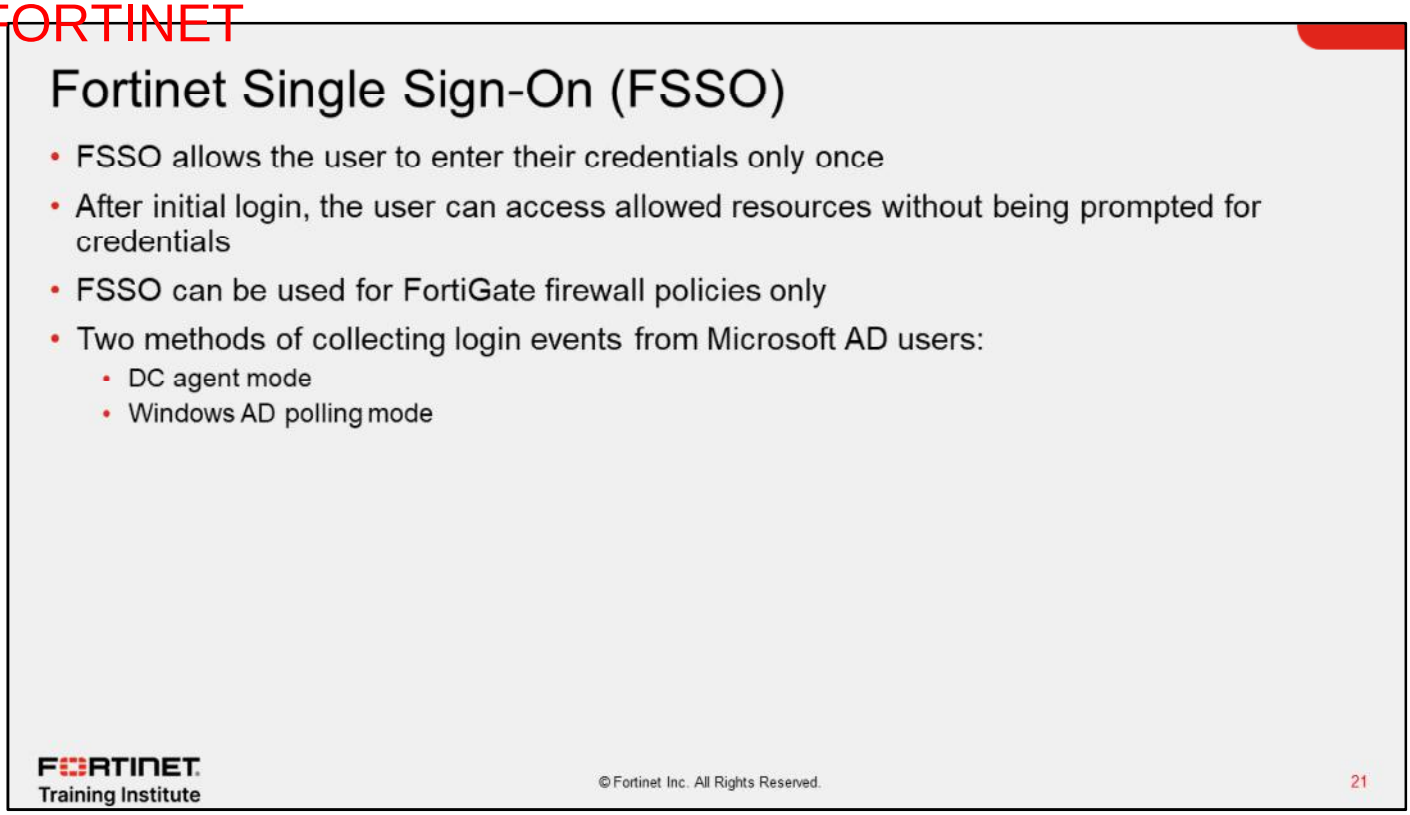
Other advantages are that FortiAuthenticator has a built-in LDAP server and an API for integrating authentication services within a corporate web site or application. It also supports wireless authentication through social channels, extends guest management capabilities, and delivers certificate management.

DO NOT REPRINT
© FORTINET



In this section, you will learn about single sign-on.

DO NOT REPRINT
© FORTINET

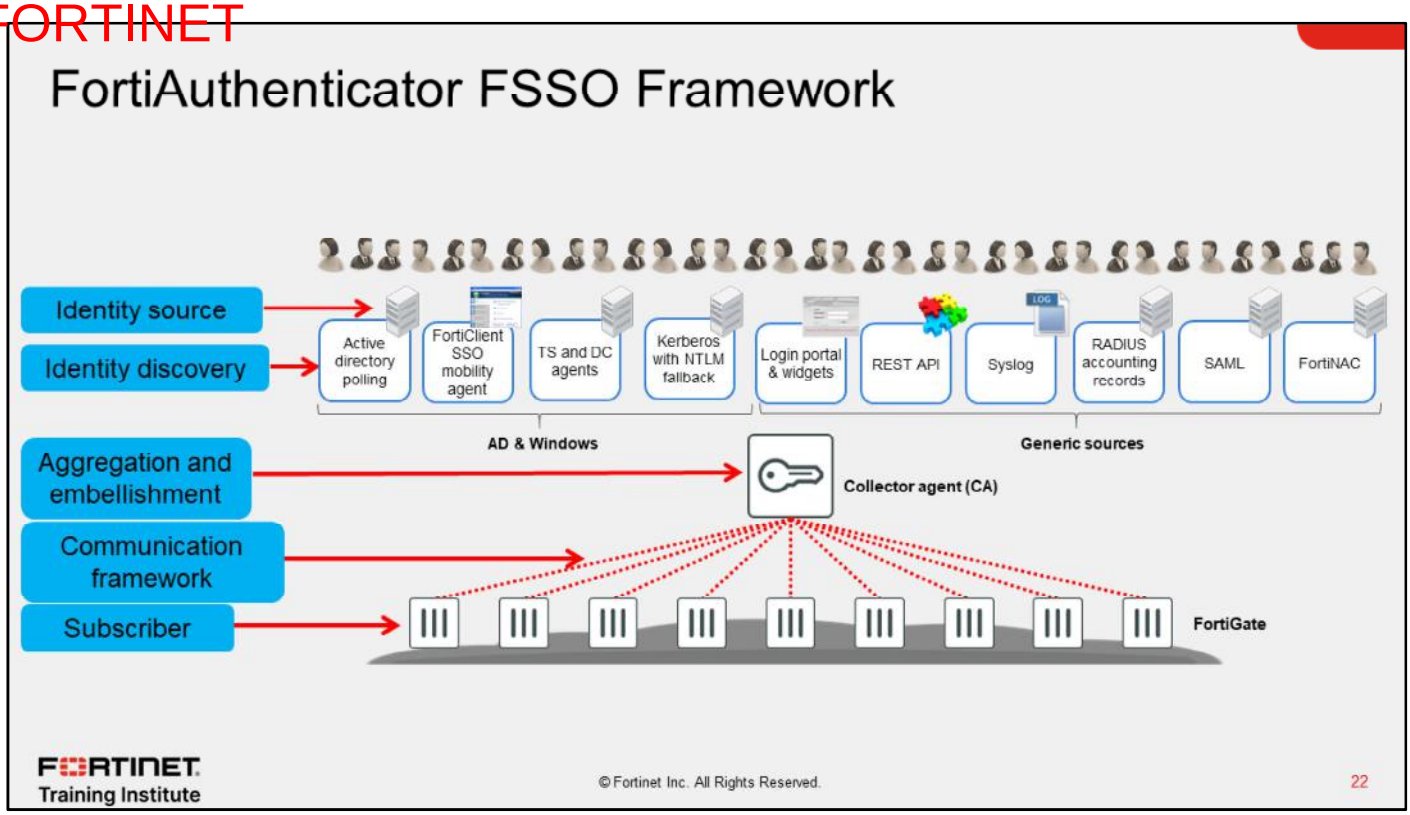


FSSO allows users, who have already authenticated to the network through another system, to be transparently identified. After initial login to any system on the network, users can access allowed resources without being prompted for credentials.

FSSO differs from the generic single sign-on (SSO) in that FSSO is a single sign-on into the FortiGate firewall policy only, as opposed to a single sign-on into any web or similar application.

FSSO is commonly used to transparently authenticate Microsoft AD users, but with FortiAuthenticator, it is not limited to that environment. FSSO can also transparently authenticate users in non-Microsoft environments by leveraging the Fortinet mobility agent, Syslog SSO, and SAML SSO.

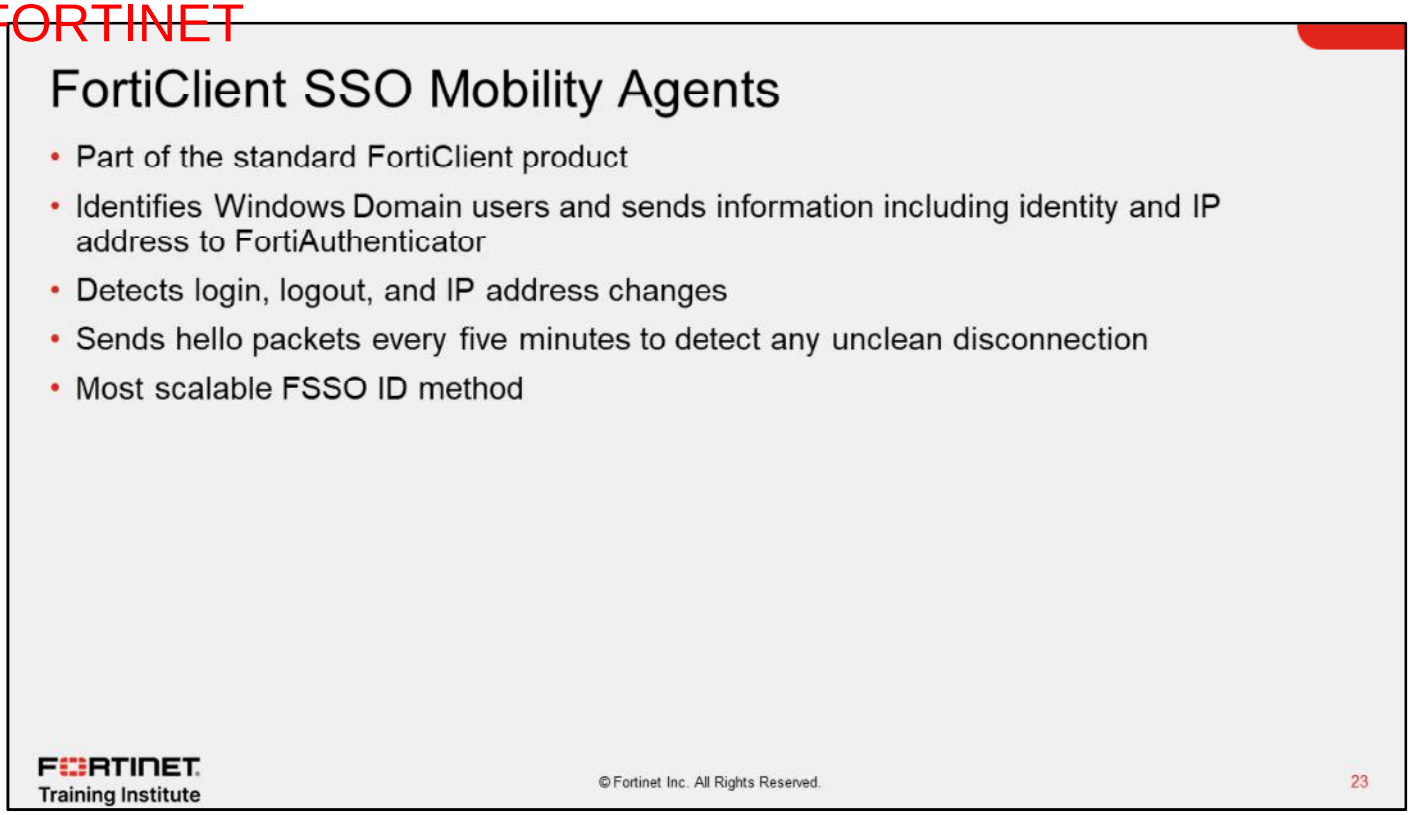
DO NOT REPRINT
© FORTINET



FortiAuthenticator FSSO framework can be divided into five layers:

- Identity source: This layer defines the method by which the user identity is ascertained.
- Identity discovery: In this layer, you can define which method to use to discover user identity and IP address.
- Aggregation and embellishment: Method to use for the collection of user identity and addition of any missing information, such as group, which is gathered from the external LDAP/AD.
- Communication framework: Defines which method to use to communicate authentication information with the subscribing devices.
- Subscriber: This layer is made of FortiGate devices which will receive authentication information to be used in firewall policies.

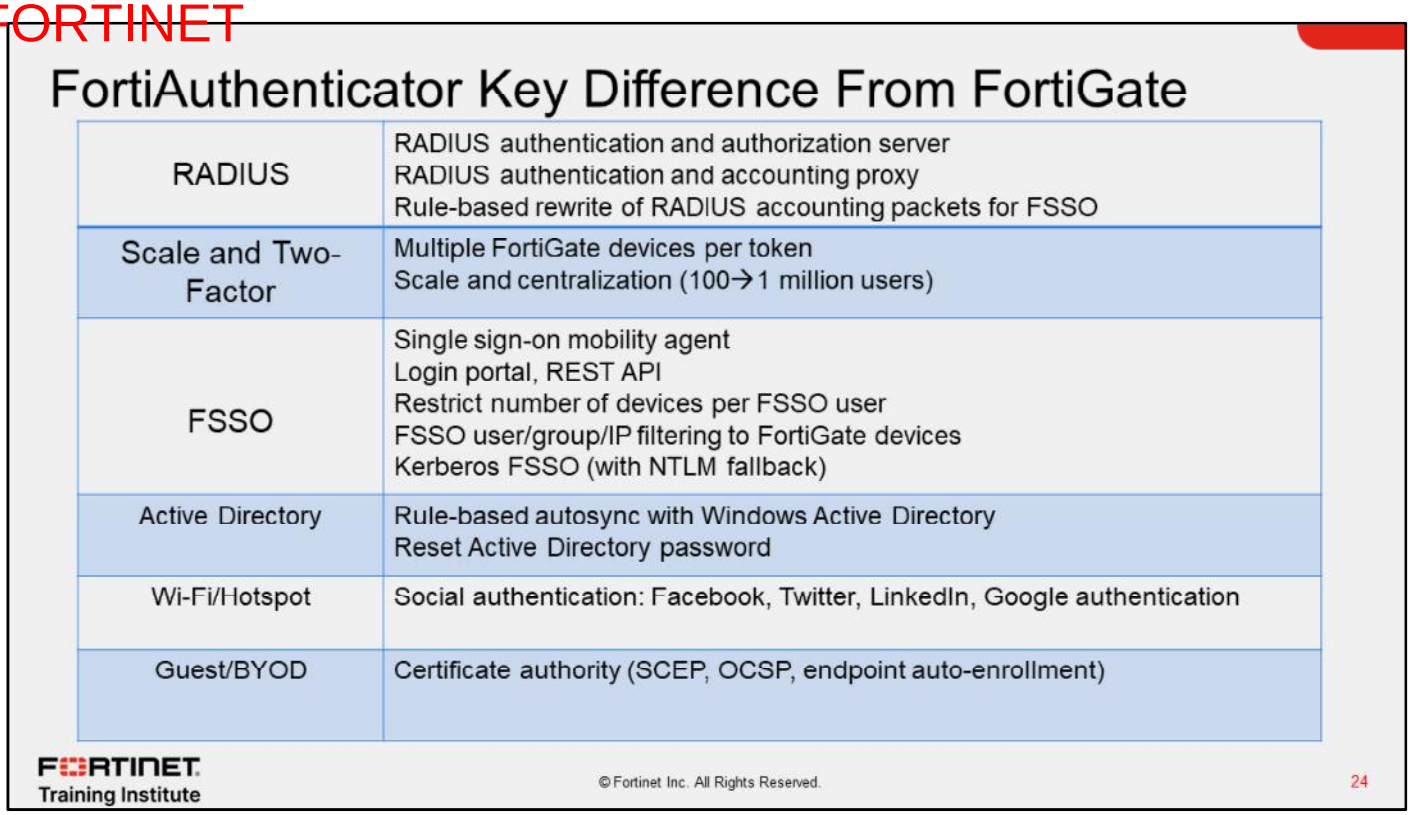
DO NOT REPRINT
© FORTINET



One of the most scalable FSSO ID methods that can be used to collect user information and IP addresses, the FortiClient SSO Mobility Agent is part of the standard FortiClient product installation.

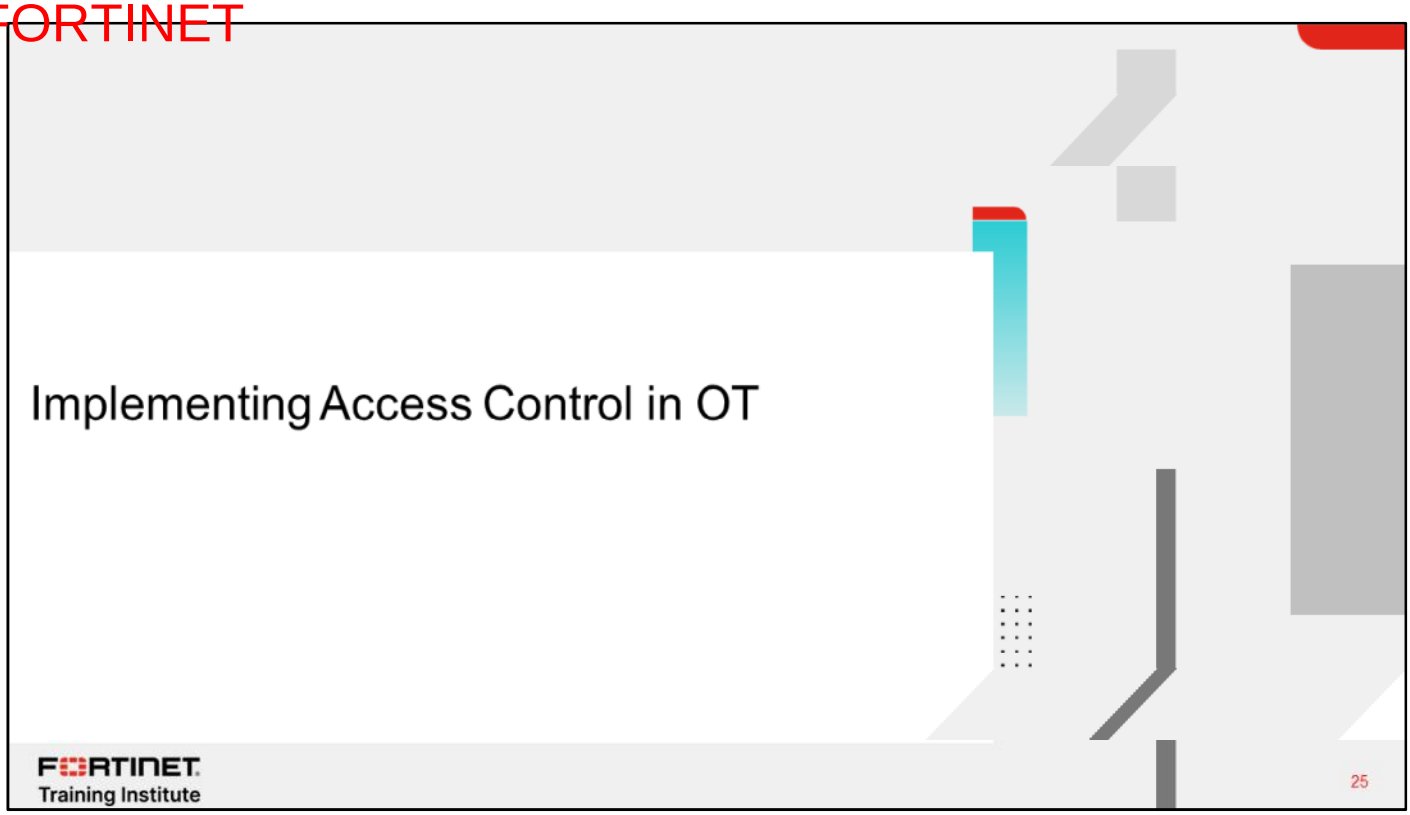
When installed, the SSO Mobility Agent identifies Windows Domain users transparently and communicates the user identity and IP address to FortiAuthenticator for use in FSSO. The agent also monitors the system for IP address changes, such as those caused by Wi-Fi roaming, and automatically updates FortiAuthenticator. When the user logs out or shuts down, the user is also logged out of FortiAuthenticator. In cases where an unclean disconnection is made (for example, power failure, hibernation, network failure), a heartbeat system is implemented so the user will be de-authenticated following a configurable number of heartbeat failures.

DO NOT REPRINT
© FORTINET



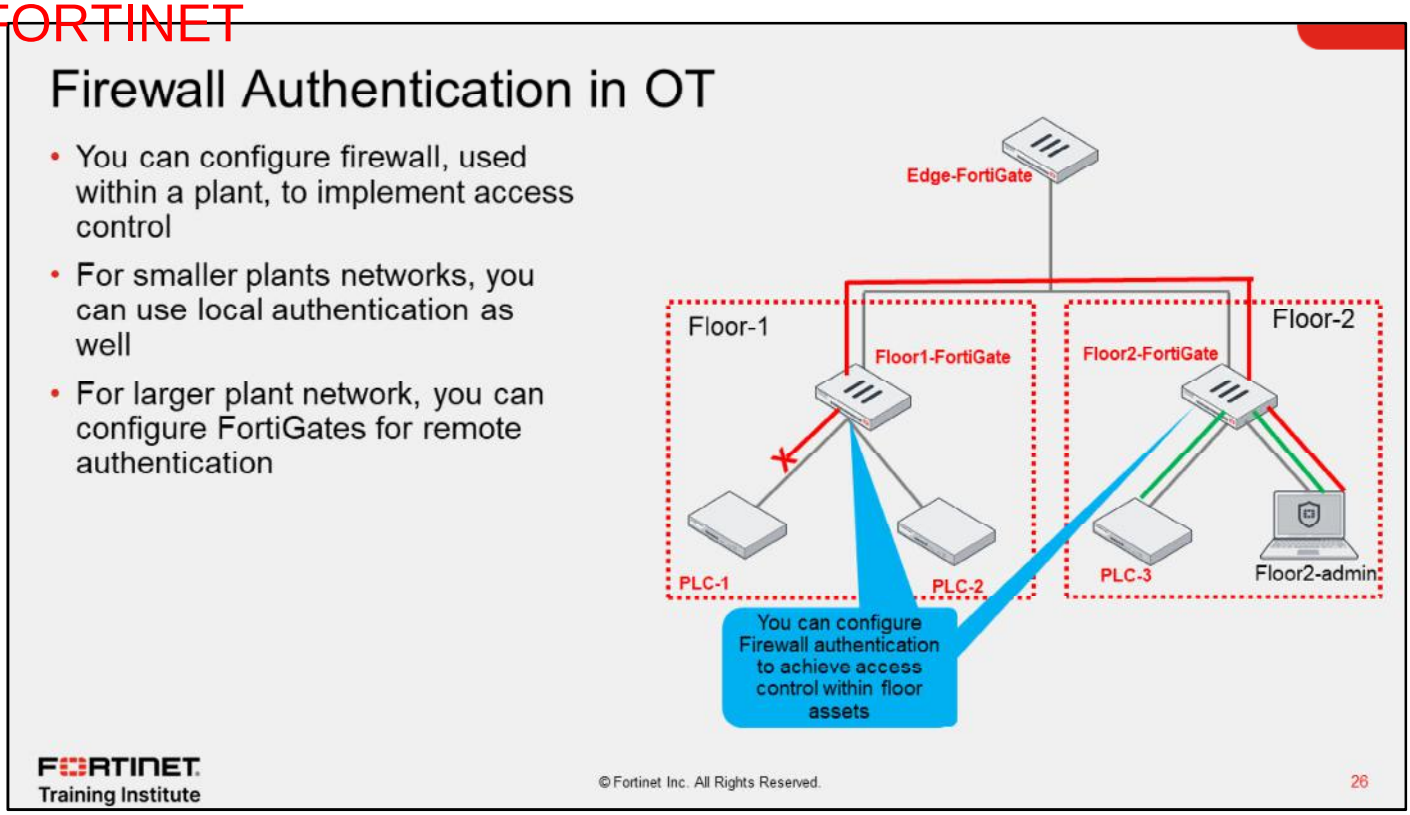
The slide shows some key advantages of FortiAuthenticator over FortiGate.

DO NOT REPRINT
© FORTINET



In this section, you will learn about implementing access control in an OT network.

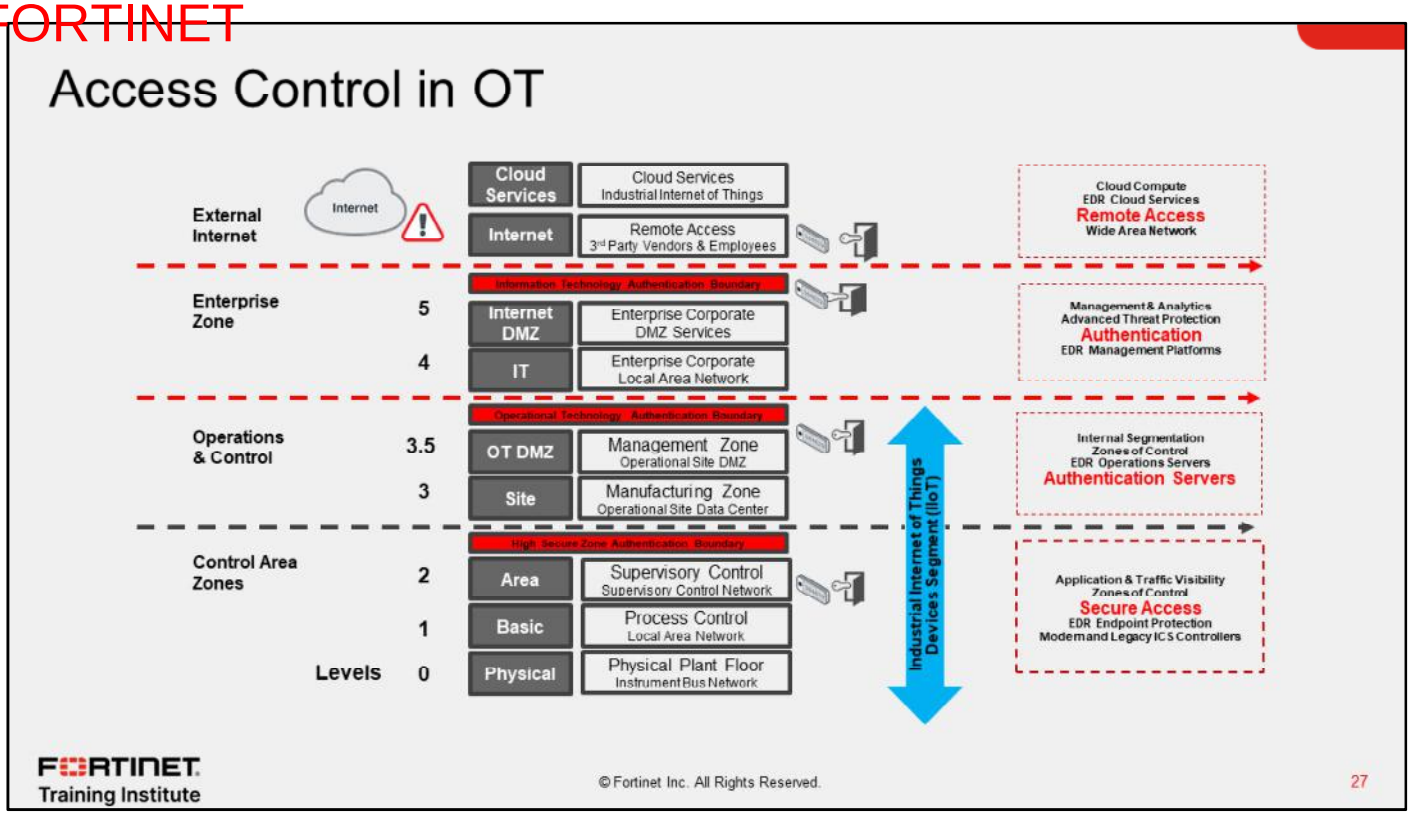
DO NOT REPRINT
© FORTINET



Achieving access control in OT is very important. When designing, the main question is, where to implement access control and which method. This depends on the various scenarios and customer requirements.

As shown in the example on the slide, with smaller floor networks, you can configure local authentication if the user list is small and can be manageable easily. Floor1-FortiGate and Floor2-FortiGate have been configured with the local users for the floor, allowing them access within the floor PLCs only. Floor2-admin has access to PLC-3 as because it is on the same floor. However, whenever Floor2-admin tries to access any device on Floor-1, Floor1-FortiGate will not allow the traffic because Floor2-admin is not part of the users allowed access to Floor-1.

DO NOT REPRINT
© FORTINET



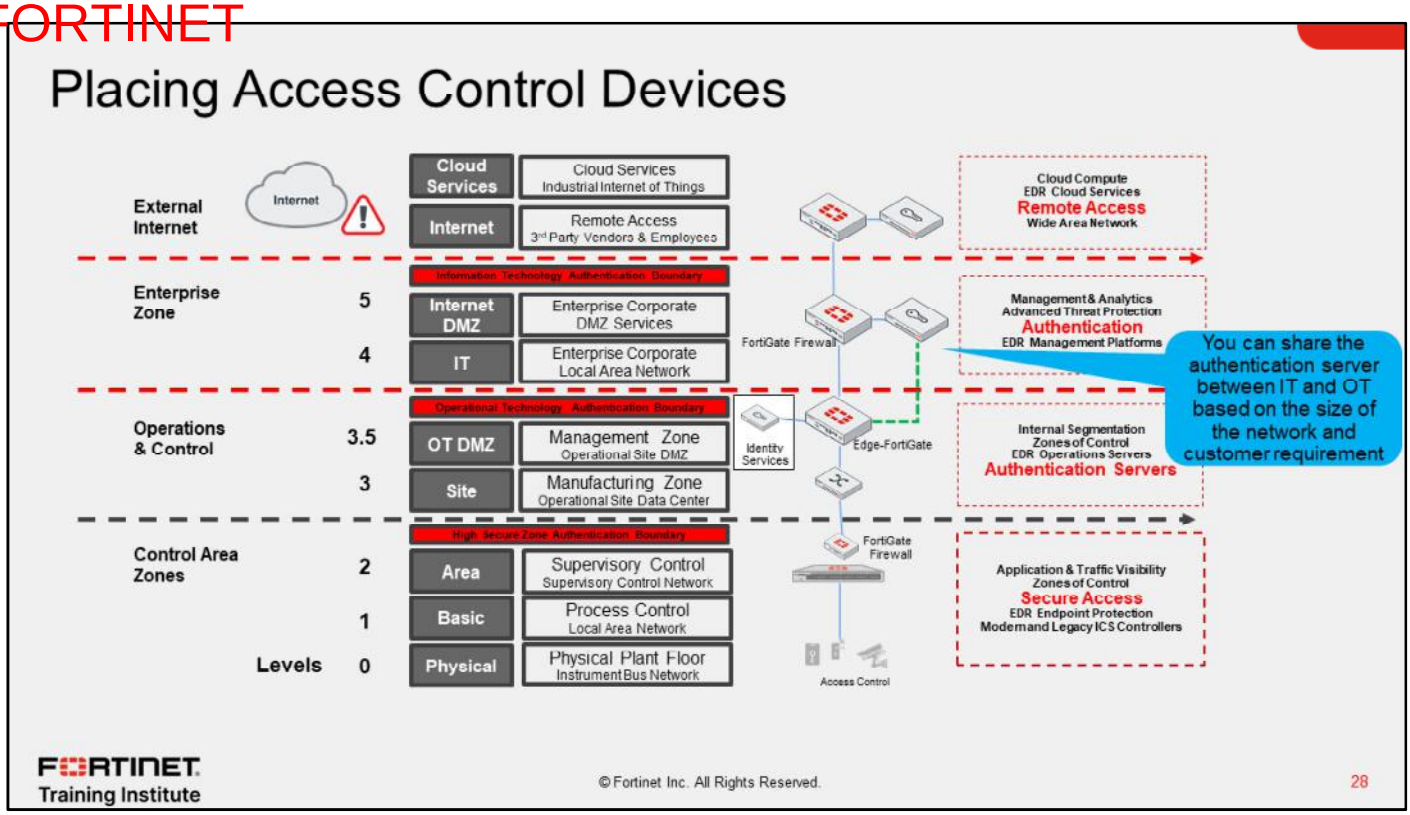
If you referenced the Purdue model, you can implement access control in every zone.

Starting from the control area zones, you can implement access control at Layer 2 to restrict and allow user within the zone.

In the operations & control zone, you can use authentication on the edge firewall. If you are using an authentication server for the OT network, this authentication server will be placed and secured under this zone. All the other devices below Level 3.5, configured with remote authentication, will be using this authentication server to authenticate users.

In enterprise zone, you can place authentication server for IT. As discussed previously, based on requirements, you can share this server with OT.

DO NOT REPRINT
© FORTINET



Now you will learn about deciding where to place FortiGate, FortiAuthenticator, and authentication servers.

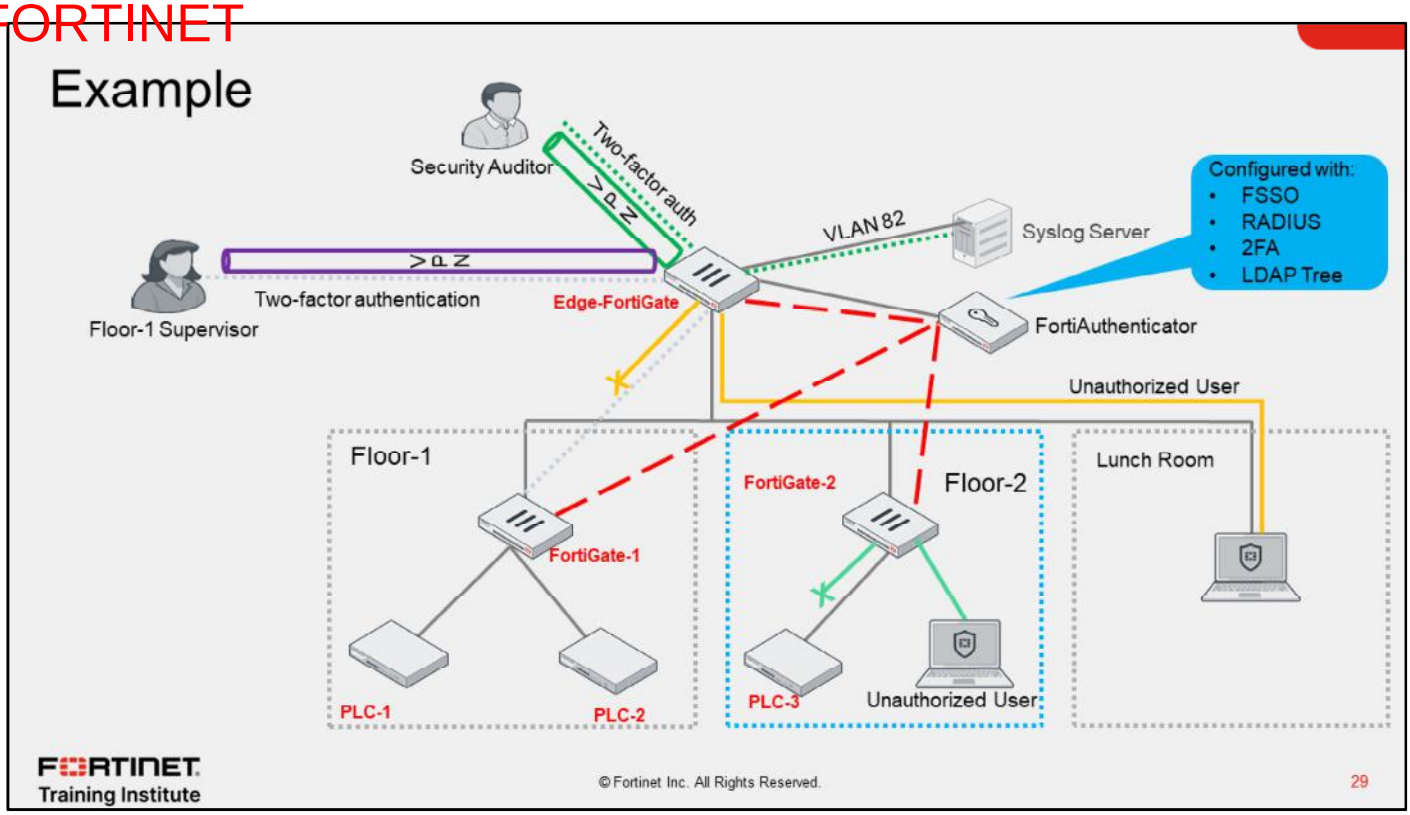
Start with the Control Area Zones. If you are using remote authentication, access control can be implemented if you are using a FortiGate device within the zone. If FortiGate is being used, you can configure FortiGate for remote authentication and use FortiGate to implement access control within the zone, floor, or plant. Using FortiGate here, you can restrict traffic for your critical assets, allowing access to authorized users only.

Now, if you are using FortiAuthenticator as a remote authentication server, FortiAuthenticator and any other authentication servers for OT need to be placed and secured behind a firewall. In the Purdue model, you can implement the authentication servers FortiAutheticator under the protection of the Edge-FortiGate. This FortiAuthenticator can be used as remote authentication server for the entire OT network. Make sure to secure this server by allowing only authentication protocols and restricted access by the authorized users only.

On the Edge-FortiGate, you can use two-factor authentication for remote users for VPN authentication. Also, you can use FSSO in the whole OT network and use it in the policy to implement access control.

In most of the cases, using a separate authentication server from OT is recommended. However, as shown on the slide, you can share the IT and OT authentication server, based on the requirements.

DO NOT REPRINT
© FORTINET

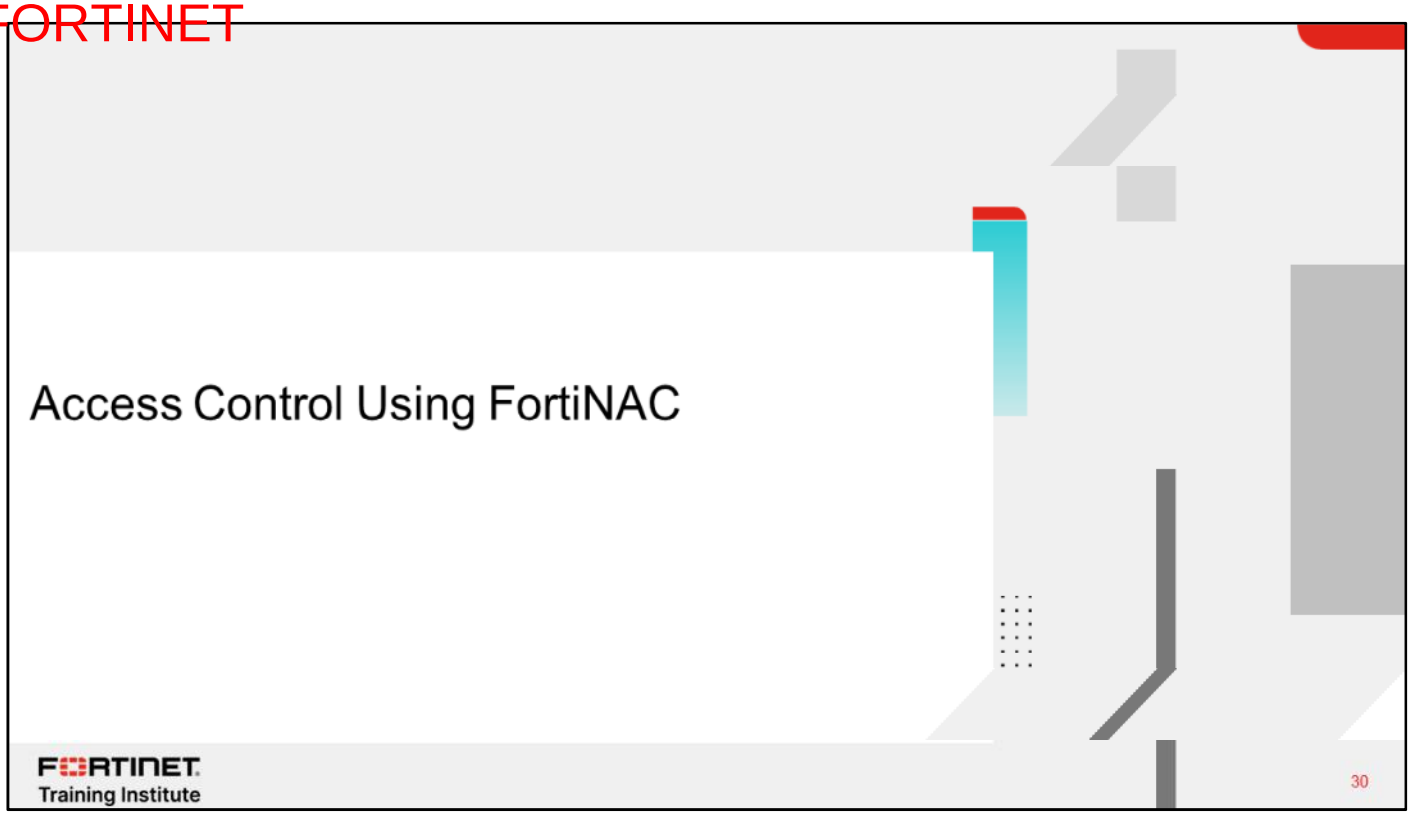


This slide shows an example of access control within an OT network.

FortiGate-1, FortiGate-2 and Edge-FortiGate are configured with FortiAuthenticator as remote authentication servers. All the FortiGate devices rely on FortiAuthenticator to authenticate users. Floor FortiGate devices are configured with authentication policies that allow only authenticated FSSO users to access PLCs. Edge-FortiGate is configured with a VPN with two-factor authentication. Edge-FortiGate also is configured with authentication policies that allow remote users access to servers behind the firewall. On Edge-FortiGate, you can allow a group of security auditors to access only syslog servers, while supervisors are allowed to access the assigned floors only.

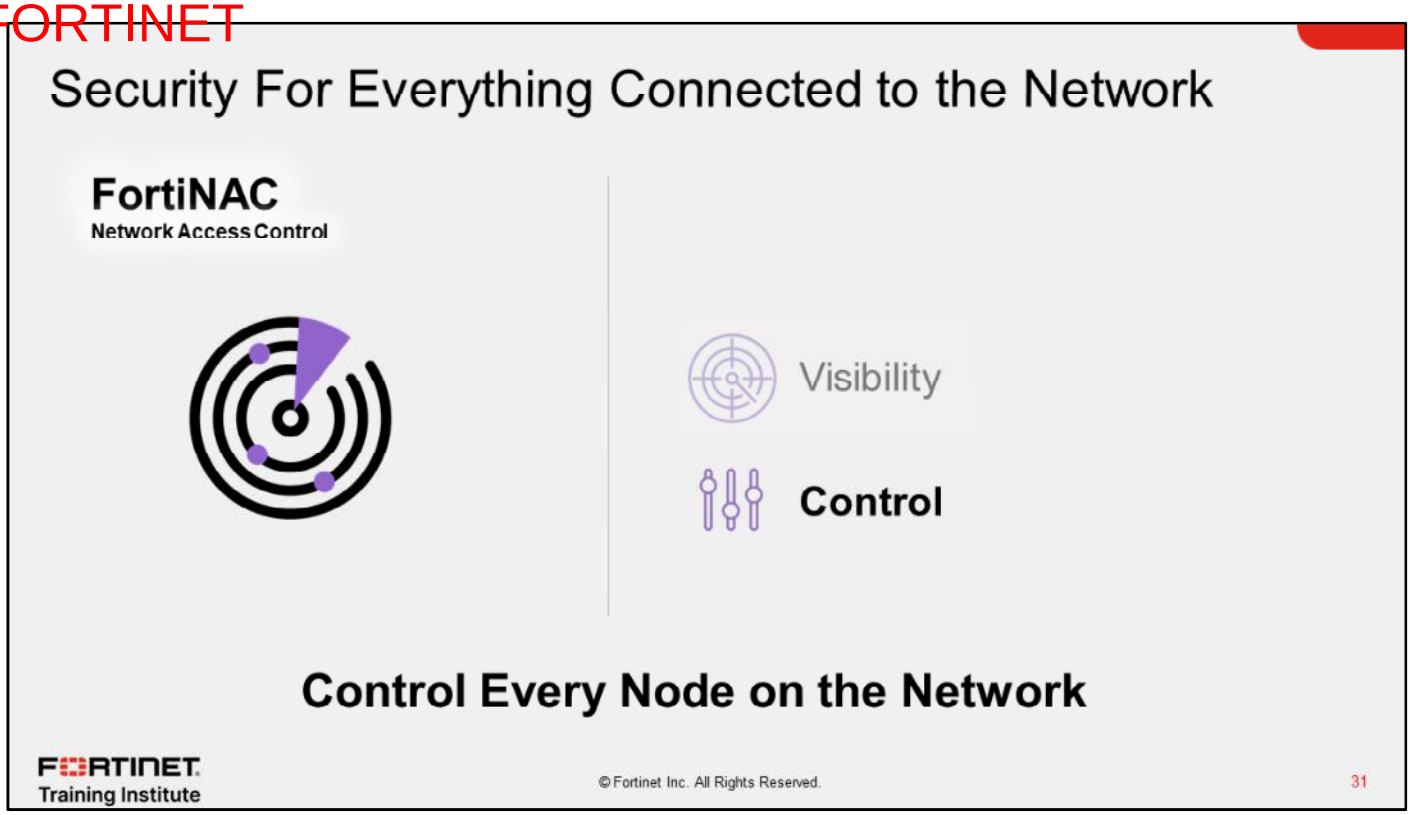
FortiAuthenticator is configured with FSSO, RADIUS, two-factor authentication with tokens, and an LDAP tree. Users assigned with FortiToken are shared and used by multiple firewalls in the network, and are not limited to one firewall or an HA pair.

DO NOT REPRINT
© FORTINET



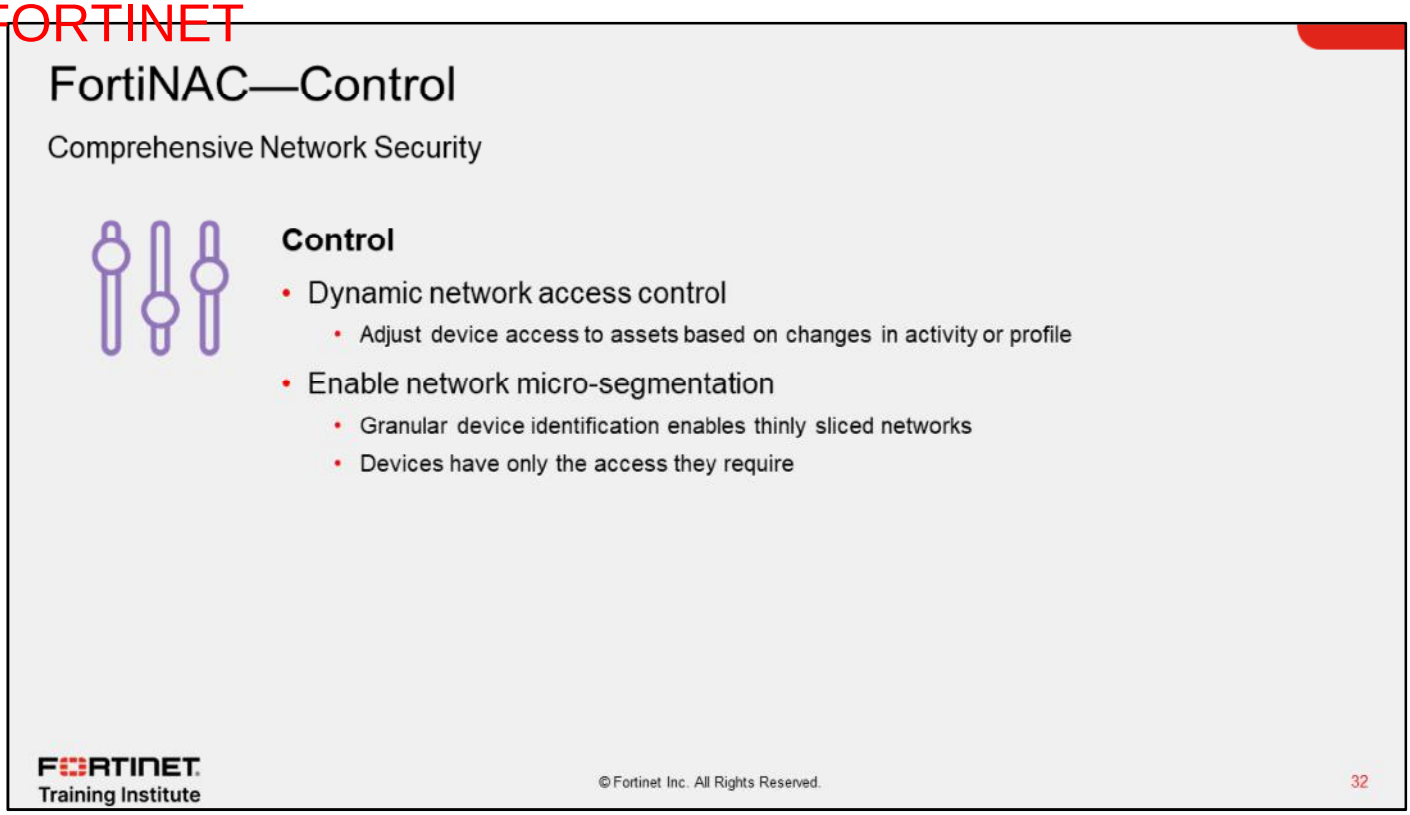
In this section, you will learn to implement access control using FortiNAC.

DO NOT REPRINT
© FORTINET



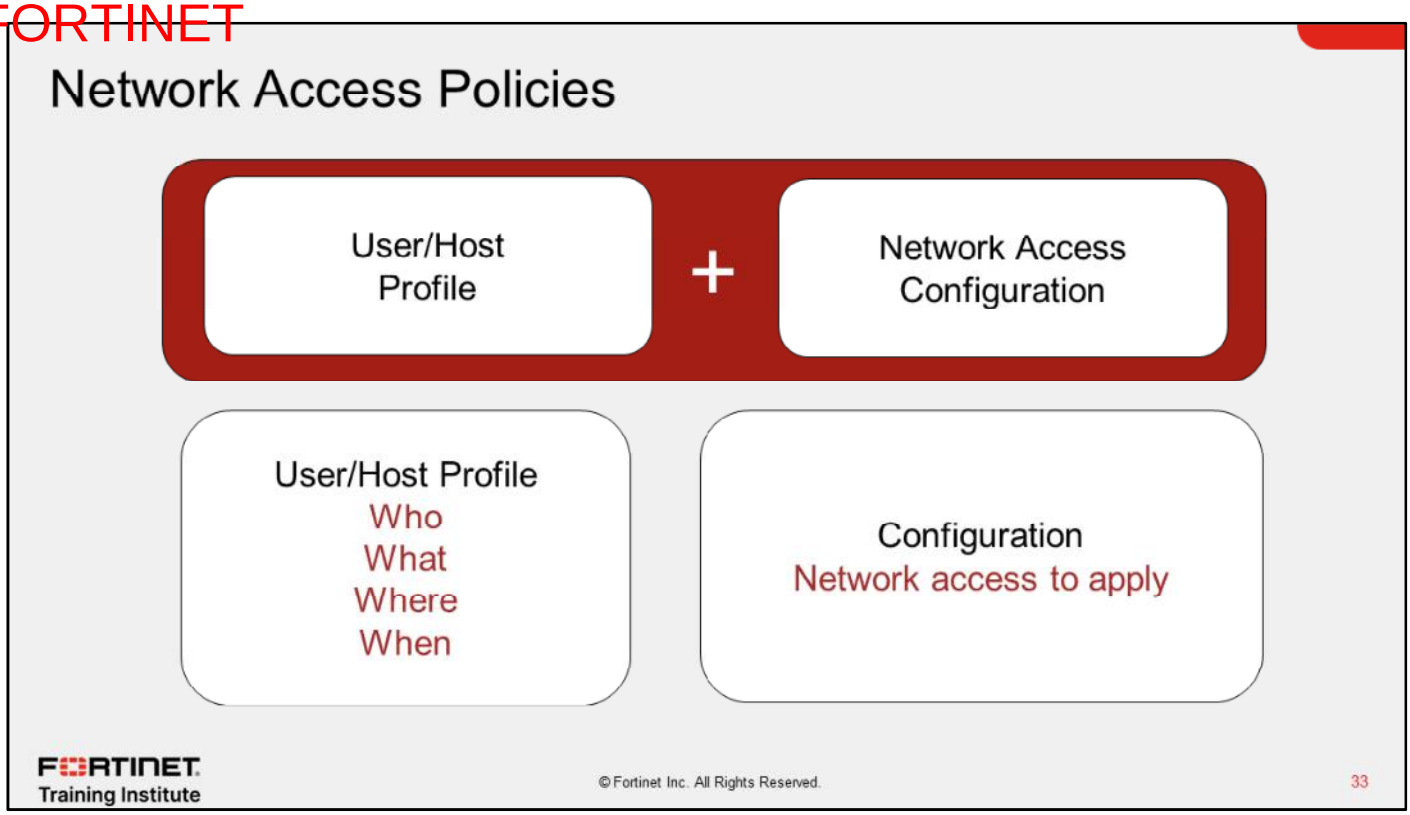
Remember that the two key capabilities that FortiNAC provides in an OT environment are visibility and control. Previously, you learned about the benefits of visibility and how visibility is achieved. In this section, you will learn about the FortiNAC control capabilities that are made possible by the detailed visibility information.

DO NOT REPRINT
© FORTINET



Controlling network access is the second part (after visibility) to securing a network environment. Access is granted only to endpoints that are designated as trusted and secure. This access can be dynamically adjusted based on changes at the device level. Because each endpoint with access to an environment is known and trusted, you can create granular policies to assign each endpoint exactly the access it needs to perform its job, and nothing more. This detailed segmentation further protects the individual endpoint, as well as all other endpoints. You can configure network access policies to perform this function.

DO NOT REPRINT
© FORTINET



A network access policy is composed of two different pieces. The first is the user/host profile, which is the piece that identifies if a device matches a particular policy. The second piece is the configuration, which is the policy-specific settings applied if the associated user/host profile is matched.

User/host profiles are a set of FortiNAC visibility parameters. These profiles can range from general to very specific, keying upon individual attributes, and applying AND, OR, and NOT logic across the following criteria:

Who/What by Group: Verifies if the device being evaluated is a member of a designated group.

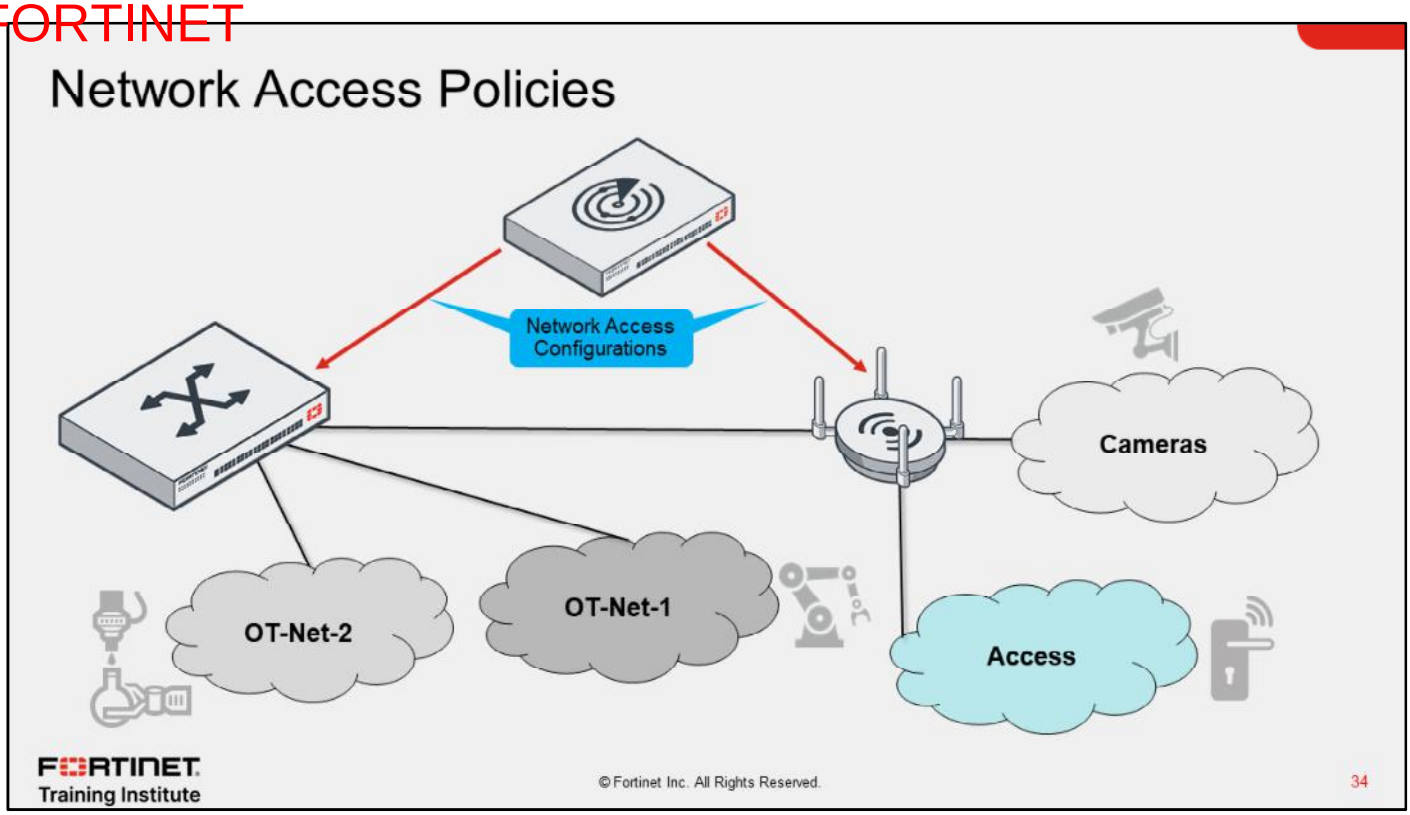
Where (Location): Point of connection based on port group (which could include SSID).
For example, cameras in building 1 could be provisioned differently from cameras in building 2. You can add location components as needed by selecting them from available port groups. When you add more than one port group, they are logically ORed together. If you set the location to **Any**, all locations will match the location requirement.

When: Profile will only match during designated days of the week or times of the day.

Devices are continuously evaluated to identify if a user/host profile matches. Whenever FortiNAC identifies a match, it applies the highest ranked network access policy.

For example, if a device matches a user/host profile that identifies a manufacturing robotic arm coming online, and that user/host profile is associated with a network access configuration, the configuration settings will be applied, provisioning the access appropriately. Logical networks defined at each point of connection could have that same policy provision on any number of different access values, dependent on location.

DO NOT REPRINT
© FORTINET

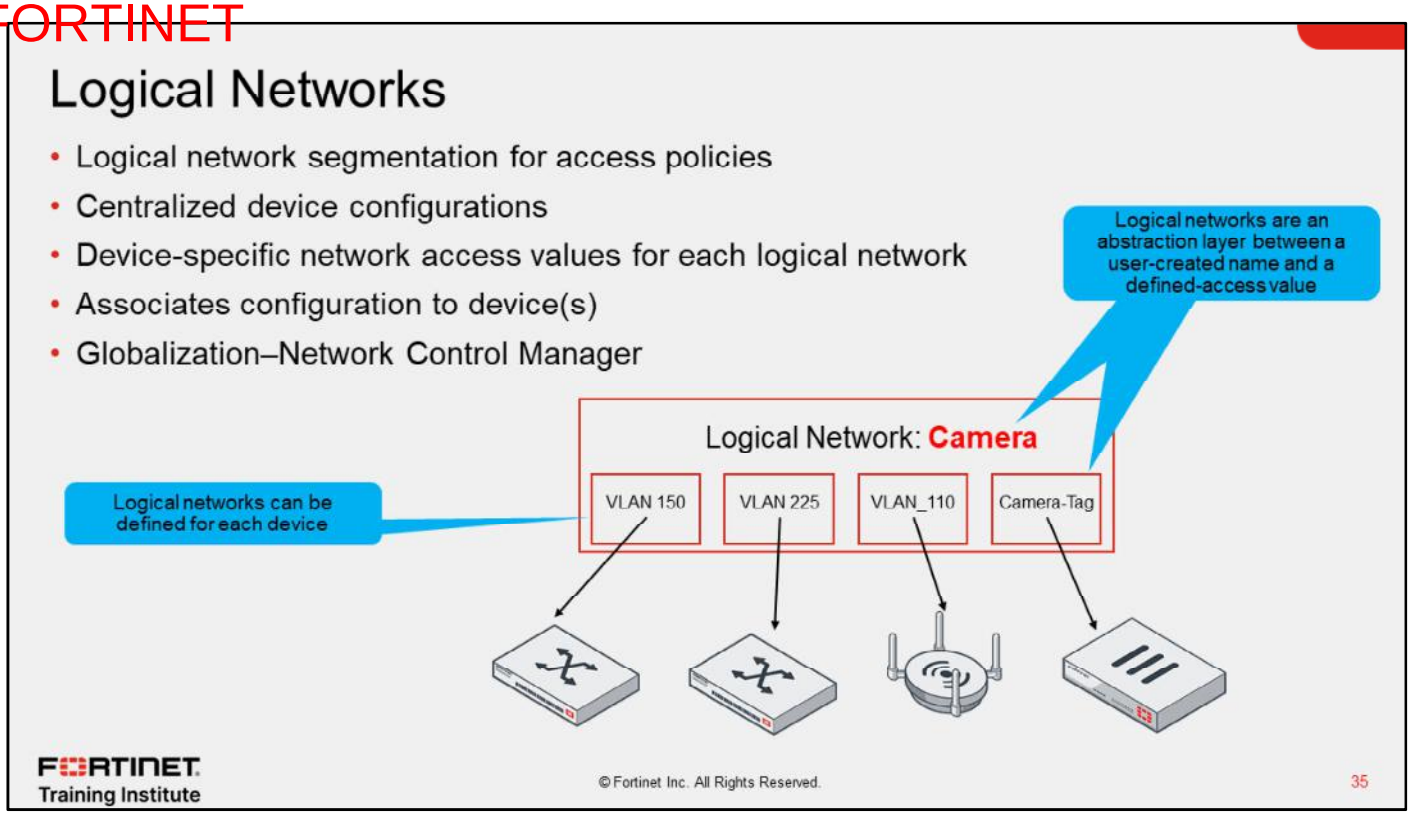


Network access policies are used to dynamically provision access to connecting endpoints, based on the matched user/host profiles associated with the network access configurations.

FortiNAC evaluates endpoints as they connect to the network. The evaluation identifies if a connected endpoint matches a user/host profile. Then, FortiNAC determines if a network access policy should be assigned. The network access policy defines the logical network to be used for provisioning.

For example, a device is connected to the network on a wired switch port. FortiNAC learns of the connection and finds the classified device in the database. The device matches a network access policy that assigns the logical network OT-Net-2. OT-Net-2 will be defined on the network infrastructure device, and may map to different values at different locations, such as VLAN 150 in one location, and VLAN 225 in another. This capability allows a single network access policy to provision devices to any number of different networks.

DO NOT REPRINT
© FORTINET



On FortiNAC, logical networks are representations of network configurations. Logical networks can represent different physical configurations for different infrastructure devices.

Logical networks are used to apply network access policies. Logical networks also translate logical access values to the physical values of infrastructure devices, decoupling policies from network configurations.

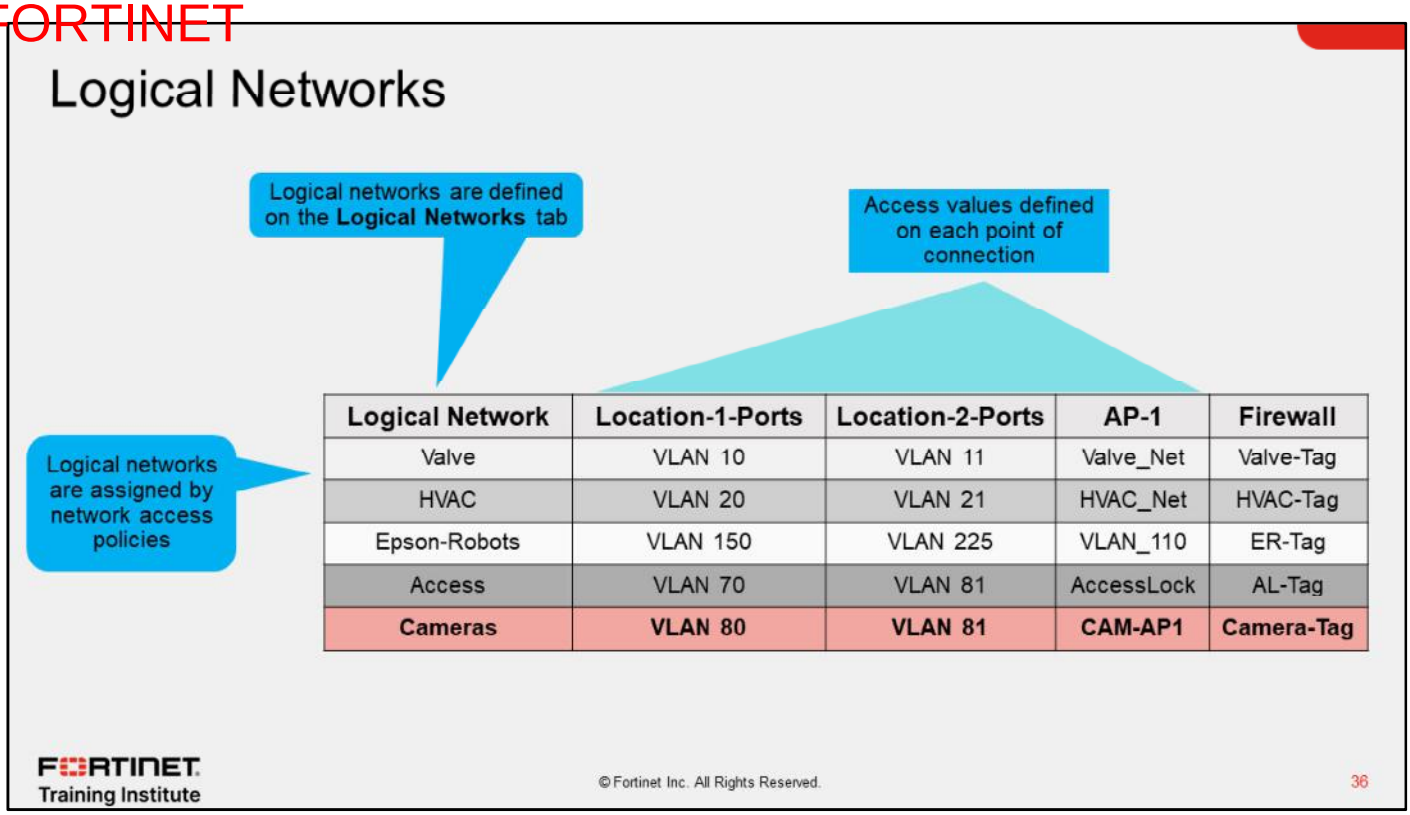
FortiNAC then uses the decoupled configuration values to provision the appropriate network access.
One logical network can represent <N> physical network segments, simplifying the configuration of network access policies.

Device-specific configurations for network infrastructure devices are performed on the device, or sets of devices, that associate the configuration values with the devices. This simplifies network access policy management by reducing the number of policies.

Logical networks allow network access policy support in the Network Control Manager, enabling global administration in distributed environments.

In the example shown on this slide, the logical network Camera defines three different access values for three different points of connection, as well as an access tag to be sent to the firewall. This logical network defines the Layer 2 access (VLAN) and the firewall policies that will be enforced (firewall polices applied because of the tag) from a single access policy.

DO NOT REPRINT
© FORTINET



This slide shows an example of how logical networks can be used.

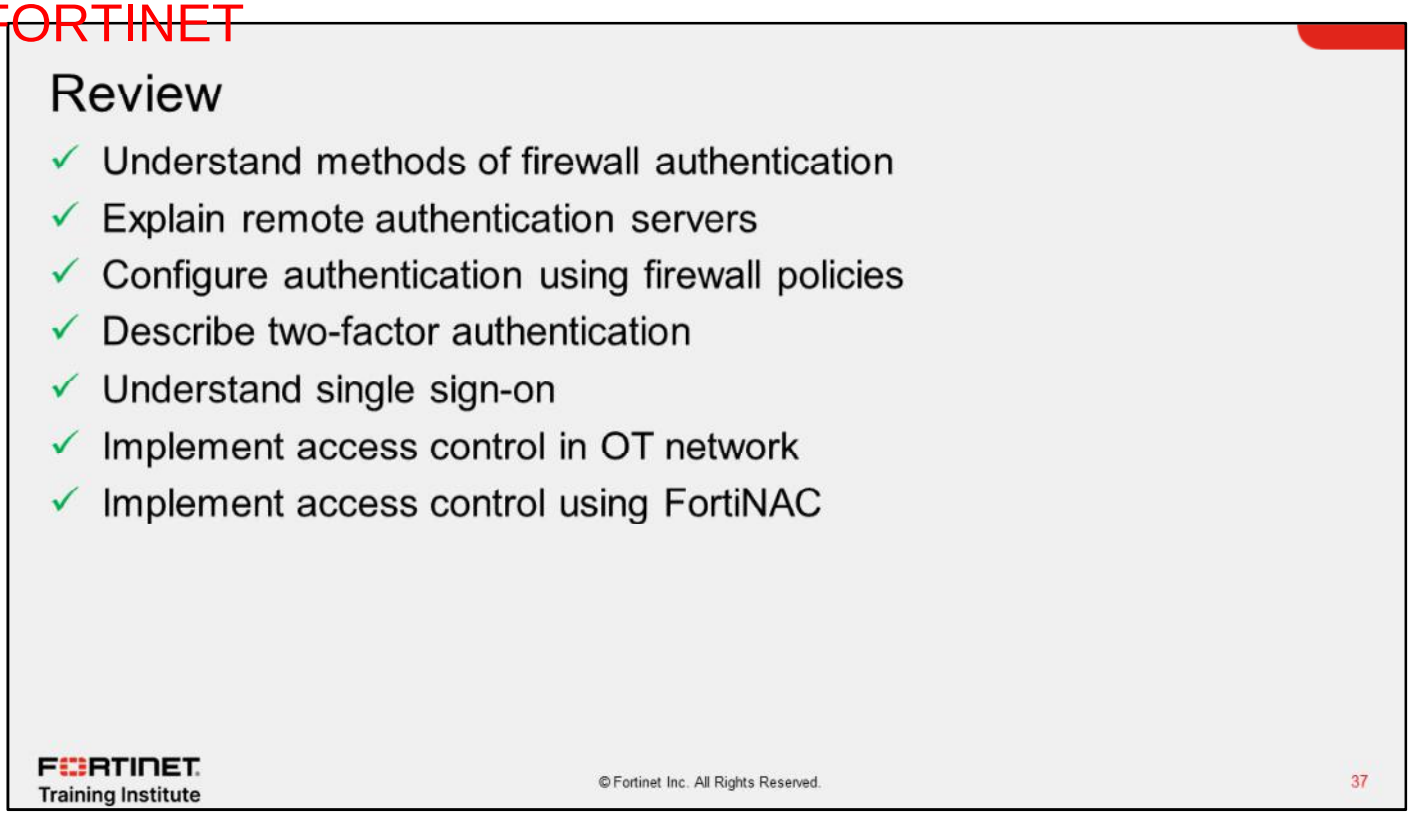
When an endpoint matches a network access policy, the policy provisions the device using a logical network. In the example shown on this slide, five network access policies have been developed to support the required endpoint-based segmentation on three defined points of connection. The defined points of connection could be devices, such as a switch, or more granular, such as port groups and SSIDs. A point of connection is normally a switch port or SSID. Because of this the firewall is not considered a point of connection in this example, because endpoints would not normally directly connect to it.

As you can see, a device identified as a camera, and assigned to the logical network **Cameras** is provisioned to **VLAN 80**. If the device is connected to **Switch-1**, it is provisioned to **VLAN 81**. If the device is connected to **Switch-2**, it is provisioned to VLAN 82, and so on. The values designated in the **AP-1** column are access values that may be vendor specific, depending on the vendor of the wireless access point (AP) or controller. These values could be VLAN names, groups, roles, interfaces names, and so on.

The **Firewall** column could represent a firewall tag that would result in the camera matching a specific firewall policy.

You can use logical networks to greatly decrease the number of network access policies, resulting in simplified policy creation and management.

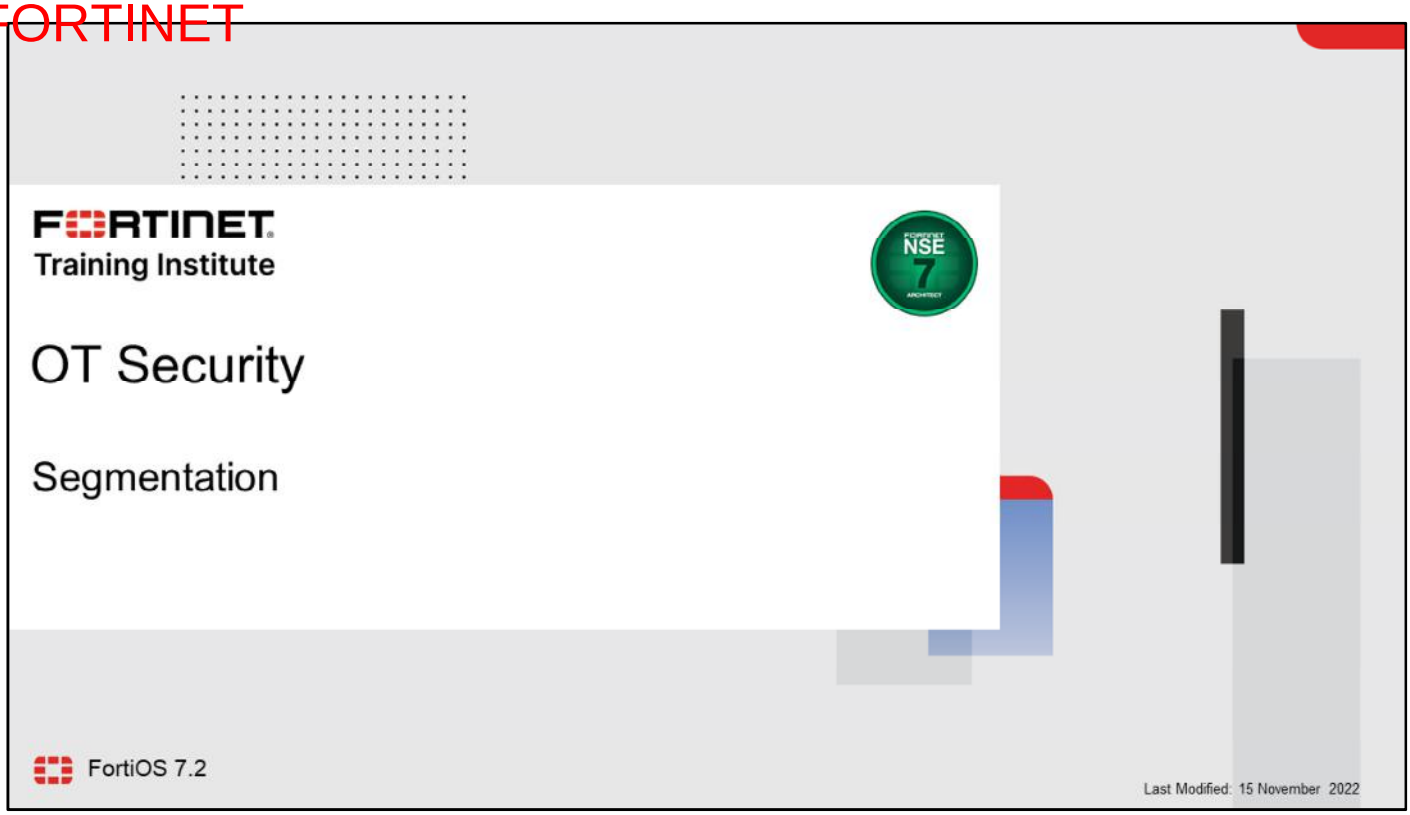
DO NOT REPRINT
© FORTINET



This slide shows the objectives that you covered in this lesson.

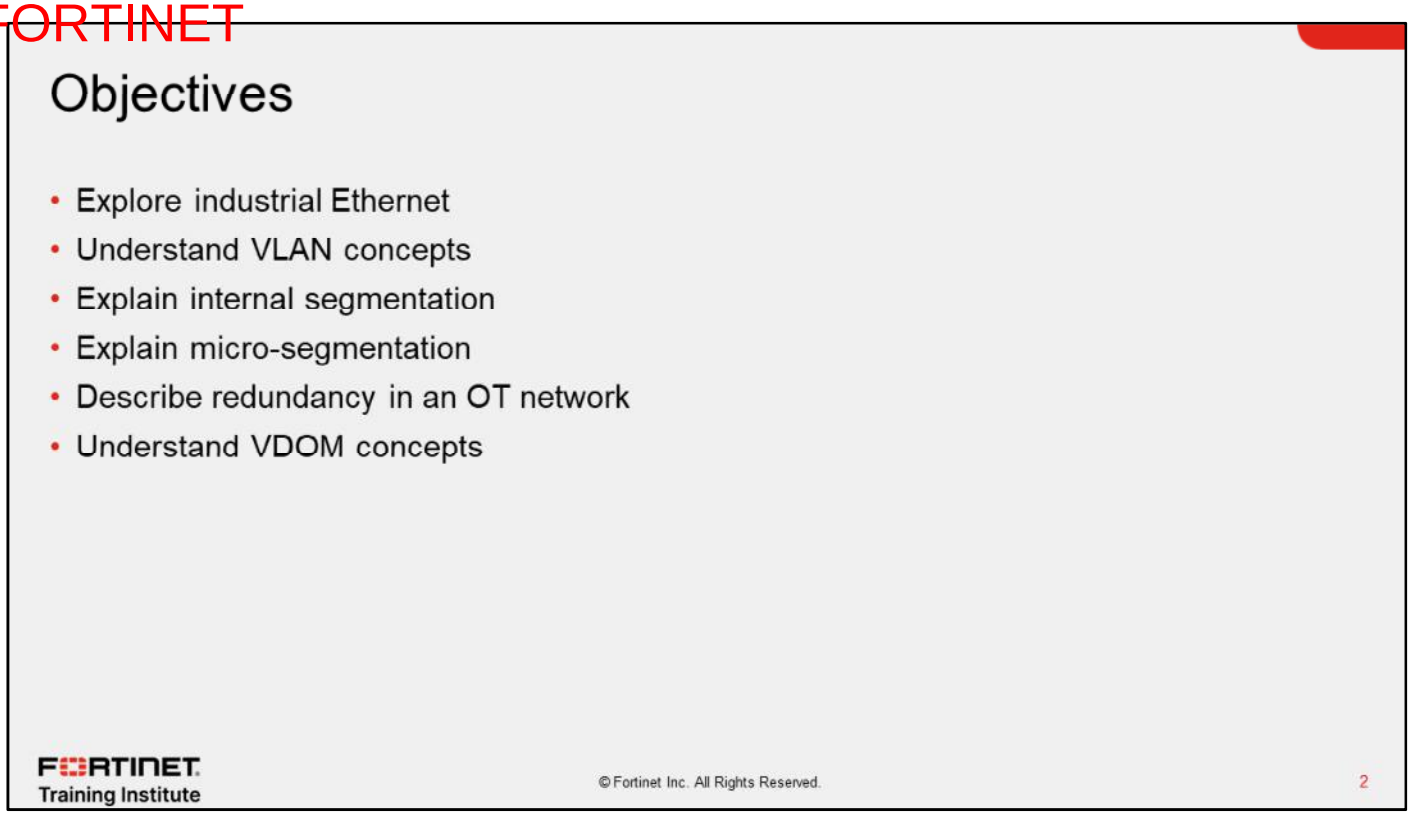
By mastering the objectives covered in this lesson, you learned how to understand and implement access control methods in an OT network.

DO NOT REPRINT
© FORTINET



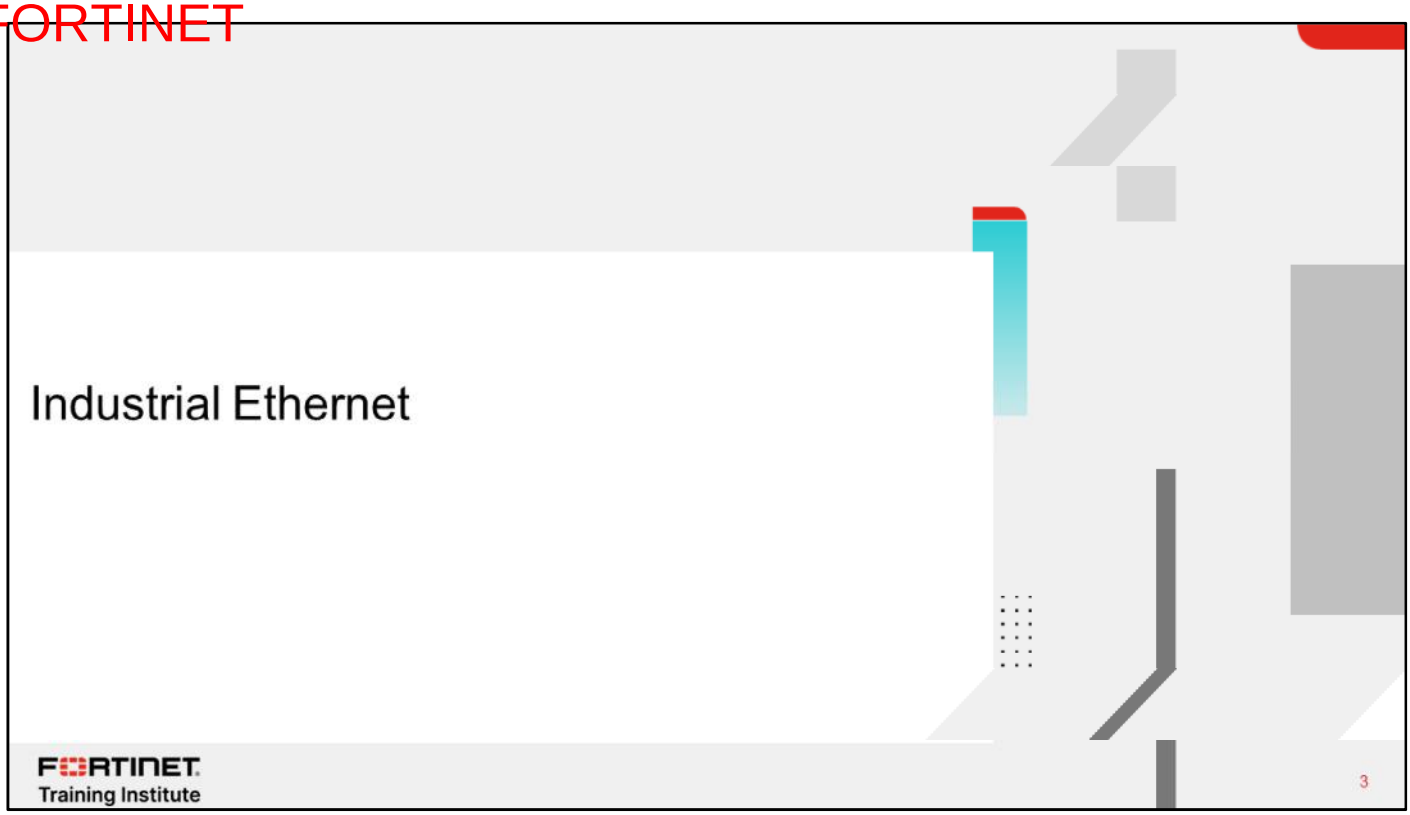
In this lesson, you will learn about network segmentation.

DO NOT REPRINT
© FORTINET



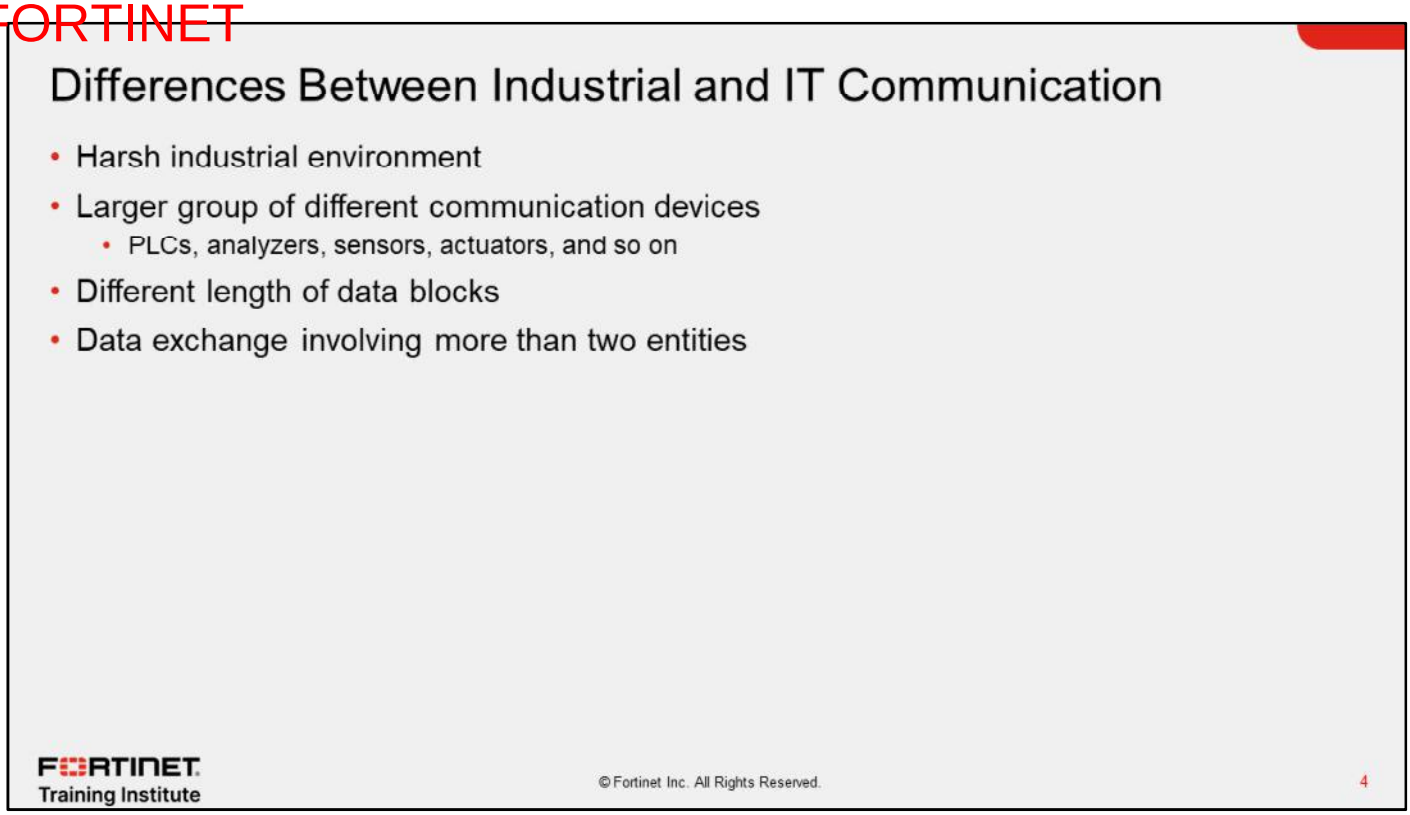
After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about different types of industrial Ethernet protocols.

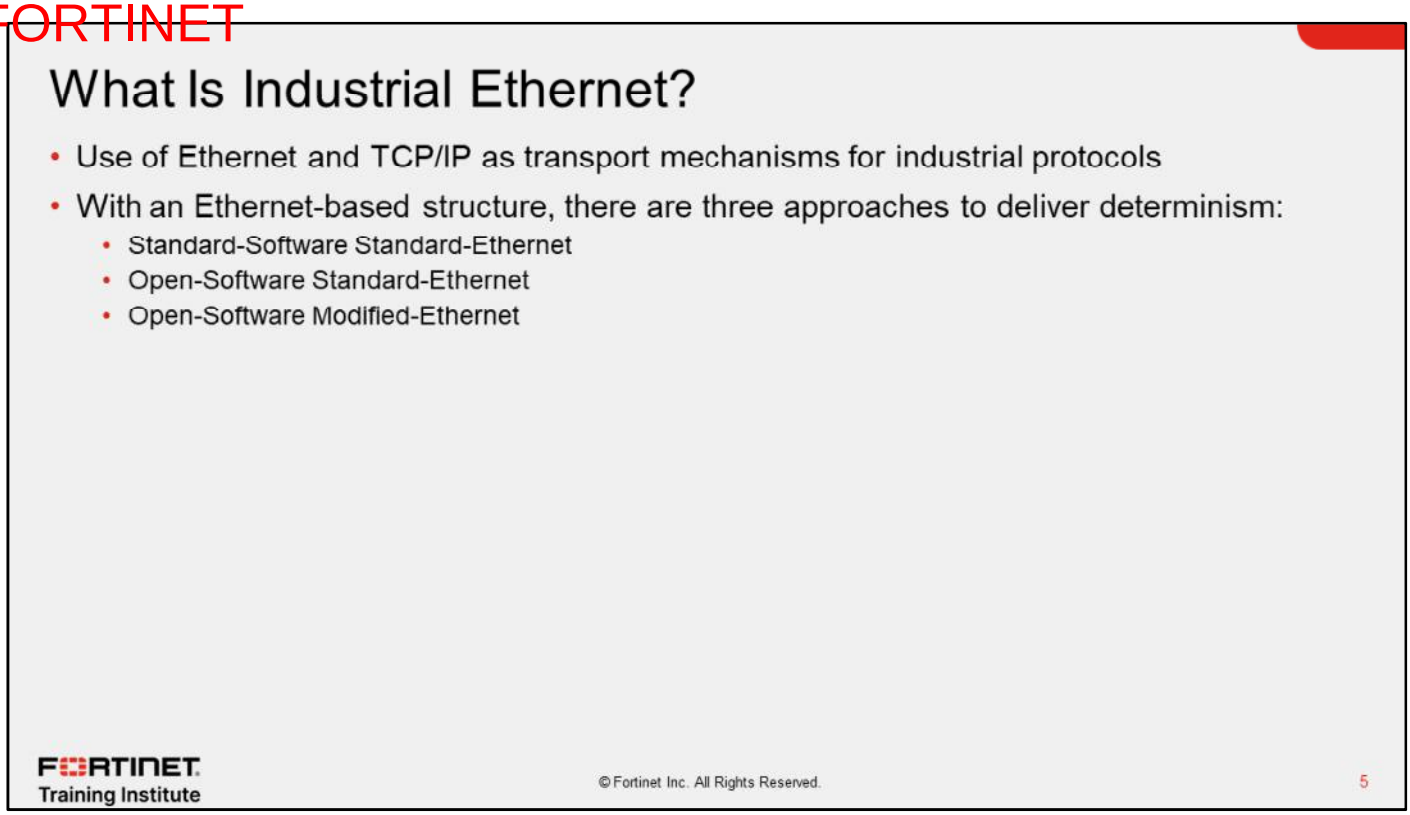
DO NOT REPRINT
© FORTINET



How different the industrial communication from IT/office communication?

- Industrial communication takes place in a harsh industrial environment that has to comply with mechanical and electrical robustness requirements.
- In industrial communication, there is a larger set of communication devices involved.
- There are different sizes of data blocks involved in industrial communication.
- The data exchange happens between more than two entities.

DO NOT REPRINT
© FORTINET



Industrial Ethernet is used to provide deterministic communication between machine controllers, actuators, sensors, and other units. It is a set of Ethernet that uses standard Ethernet hardware and TCP/IP protocol with a proprietary application layer. The application layer ensures the reliability and availability of the data transmission.

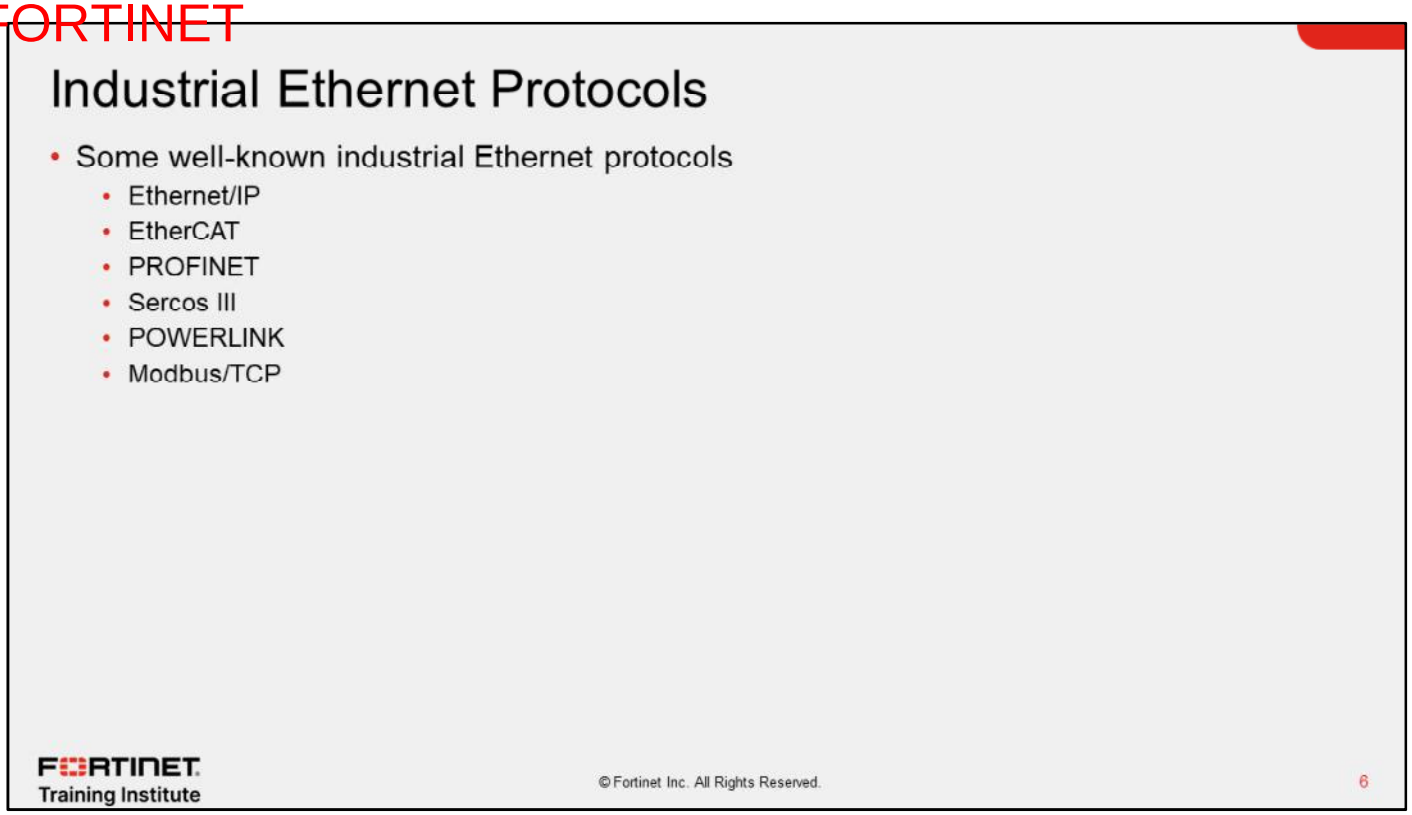
With an Ethernet-based structure, there are three approaches to deliver determinism:

- Standard-Software Standard-Ethernet:
  - This architecture uses standard Ethernet with the TCP/IP, with a built-in application layer mechanism to ensure real-time data transmission.
  - Example: Ethernet/IP

- Open-Software Standard-Ethernet:
  - This architecture uses standard Ethernet with new protocols to manage network access and synchronized data communication to prioritize the critical data transmission.
  - Example: POWERLINK

- Open-Software Modified-Ethernet:
  - This architecture uses standard Ethernet hardware, new protocols, and complementary hardware to ensure determinism.
  - Example: EtherCAT

DO NOT REPRINT
© FORTINET

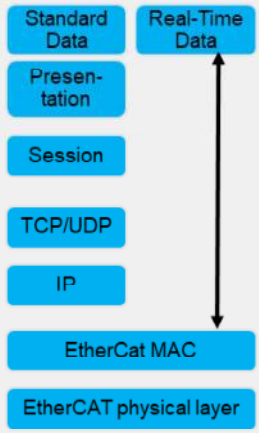


This slide shows some well-known industrial Ethernet protocols.

DO NOT REPRINT
© FORTINET

Ethernet/IP and EtherCAT

- Ethernet/IP
  - Only industrial protocol based entirely on Ethernet standards
  - Uses standard Ethernet physical, data link, network, and transport layers
  - Can support unlimited number of nodes
  - Requires limited range to avoid latency and to provide real-time data transmission
- EtherCAT
  - Offers real-time data transmission in primary-secondary configuration
  - With EtherCAT all secondary devices only collect relevant information they need
  - Skips Layers 3 to 6



FORTINET Training Institute

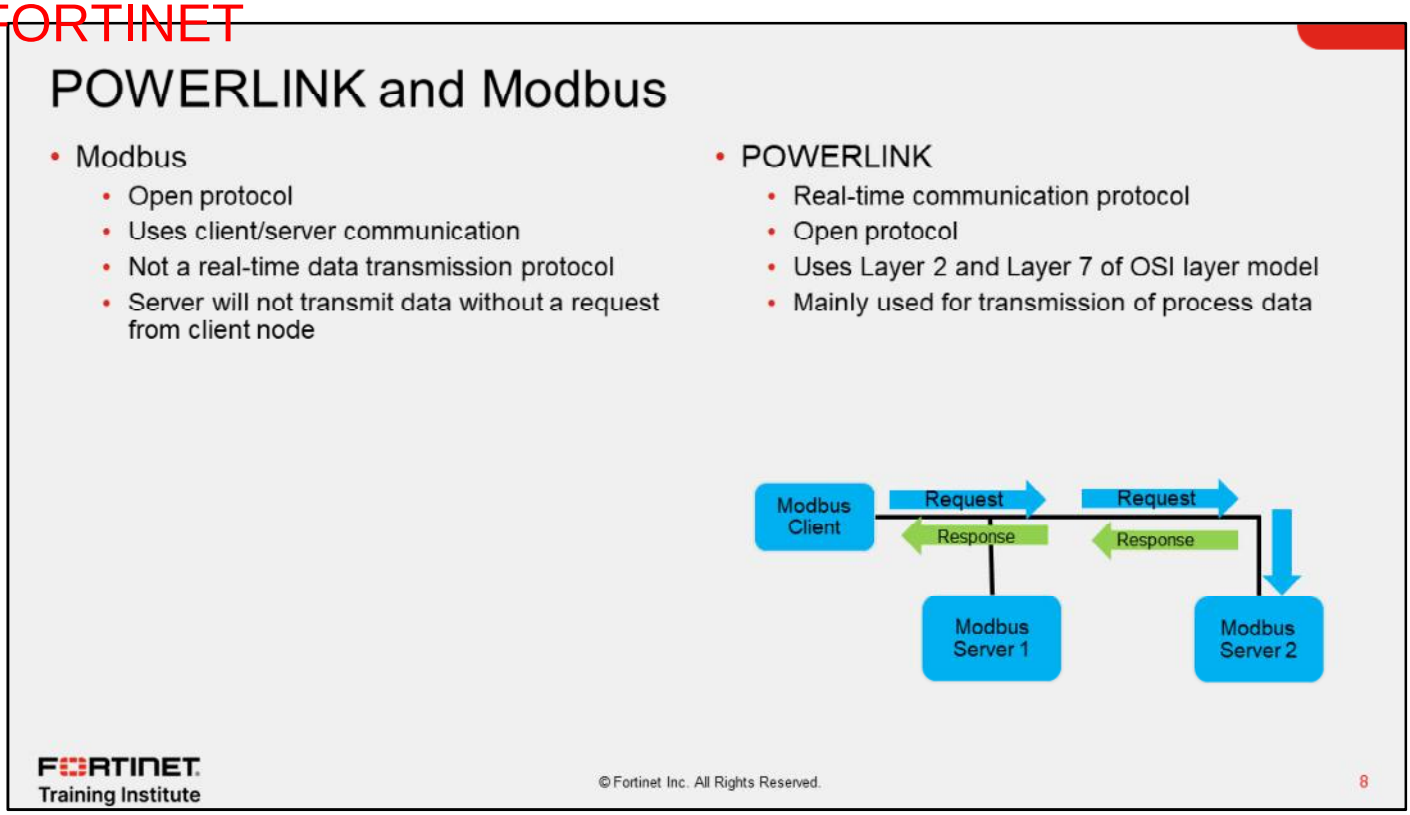
© Fortinet Inc. All Rights Reserved.

7

Ethernet/IP is one of the most popular application layer industrial Ethernet protocols. Ethernet/IP is the only protocol based entirely on Ethernet standards. It uses the standard physical, datalink, network, and transport layers. Because of its use of the standard Ethernet protocol, Ethernet/IP can support an unlimited number of nodes. It can be used for real-time communication if it is used within a limited range.

EtherCAT is one of the protocols that offers real-time communication in a primary-secondary configuration. EtherCAT skips Layers 3 to 6 to deliver real-time communication. The most important feature of the protocol is that secondary devices collect only the relevant information they need from the data packets.

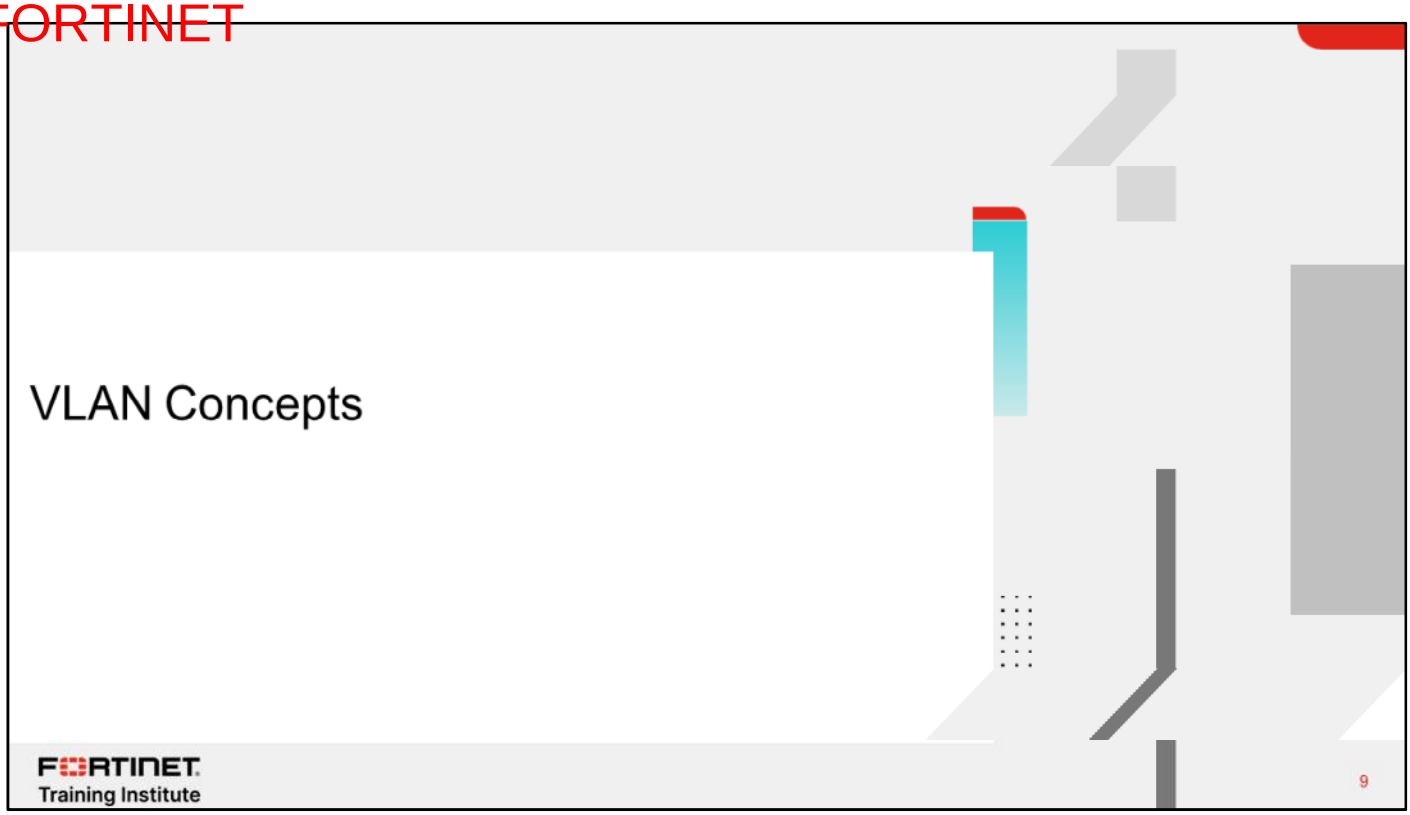
DO NOT REPRINT
© FORTINET



POWERLINK is a real-time communication protocol that relies on Layer 2 and Layer 7 of the OSI layer model. The POWERLINK protocol is for transmitting process data.

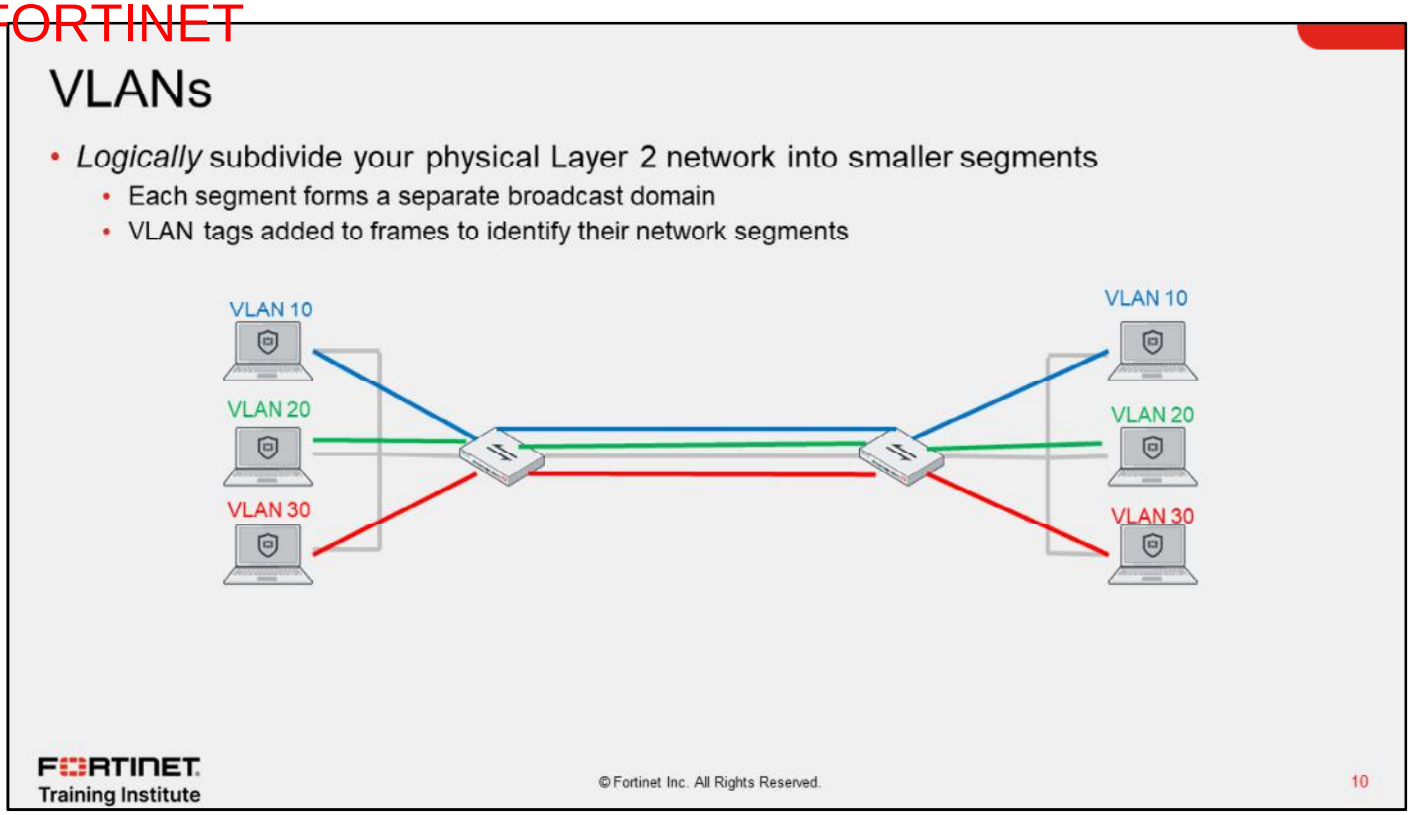
Modbus is an open protocol used in an OT network. Modbus uses client/server communication in which the server device will not transmit data without getting an offer from the client device. The Modbus protocol cannot be used for real-time data transmission.

DO NOT REPRINT
© FORTINET



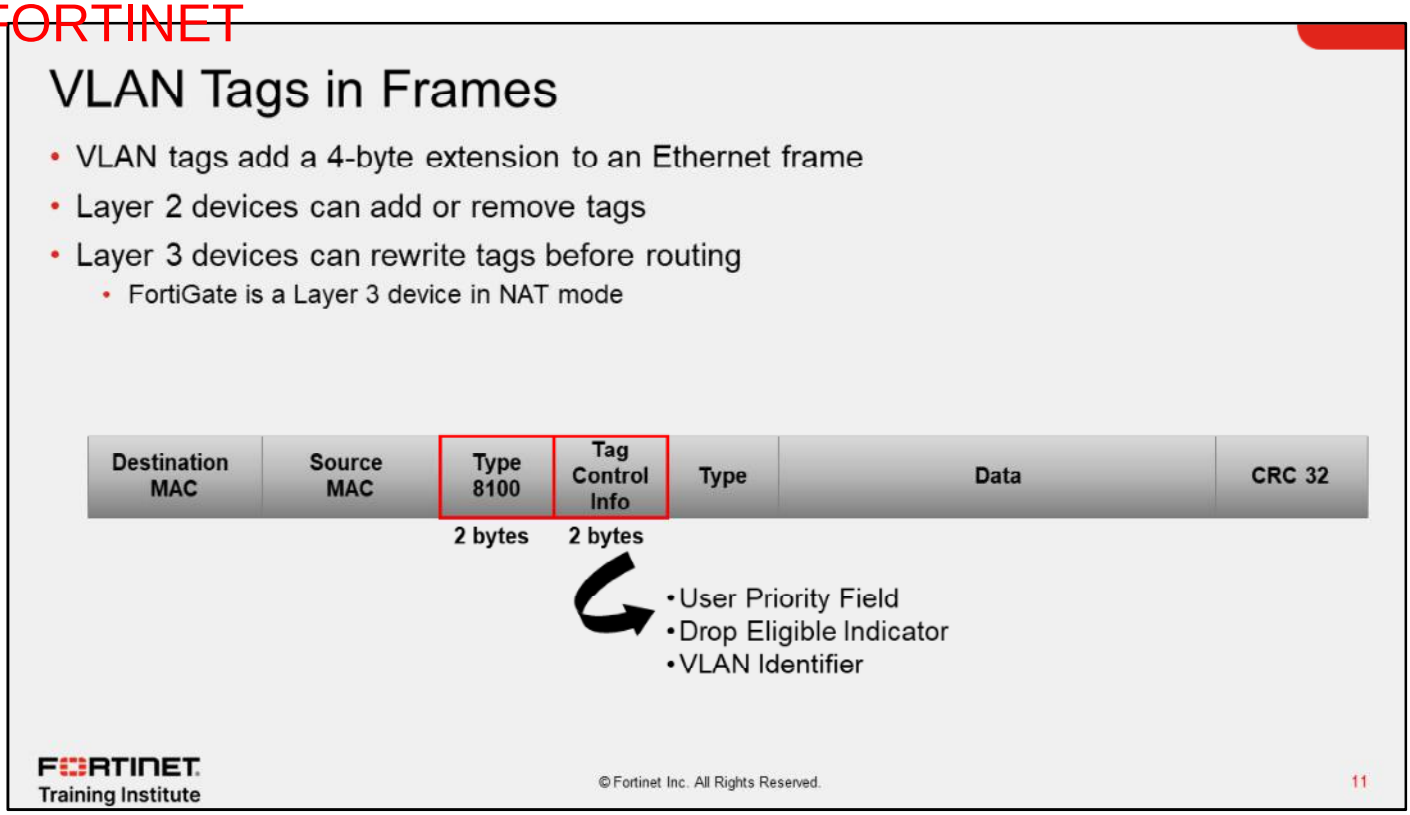
In this section, you will learn about VLAN concepts.

DO NOT REPRINT
© FORTINET



VLANs split your physical LAN into multiple logical LANs. VLAN are used to create multiple broadcast domains within a single broadcast domain. VLANs can spread across multiple switches, with each VLAN acting as its own broadcast domain. Multiple VLANs can coexist on the same physical interface, provided they have different VLAN IDs. In this way, a physical interface is split into two or more logical interfaces. A tag is added to each Ethernet frame to identify the VLAN to which it belongs.

DO NOT REPRINT
© FORTINET



This slide shows an Ethernet frame. The frame contains the destination and source MAC addresses, type, data payload, and a CRC code, to confirm that it is not corrupted.

In the case of Ethernet frames with VLAN tagging, according to the 802.1q standard, four more bytes are inserted after the MAC addresses. They contain an ID number that identifies the VLAN.

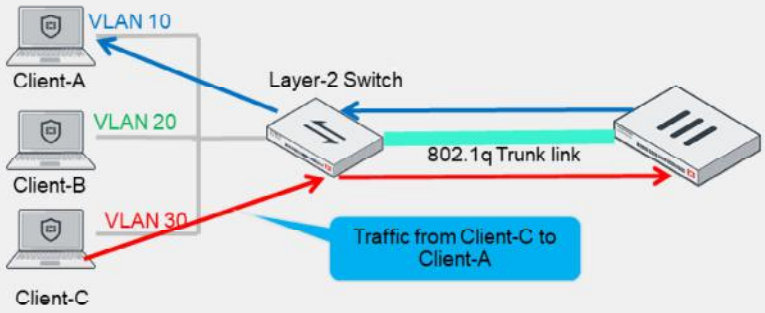
An OSI Layer 2 device, such as a switch, can add or remove these tags from Ethernet frames, but it cannot change them.

A Layer 3 device, such as a router or a FortiGate device, can change the VLAN tag before proceeding to route the packet. In this way, they can route traffic between VLANs.

DO NOT REPRINT
© FORTINET

Router on a Stick

- Ways to allow routing between VLANs
- Consists of a router and a switch connected through an Ethernet link configured as 802.1q trunk link
- Usually installed in a network without Layer 3 switches



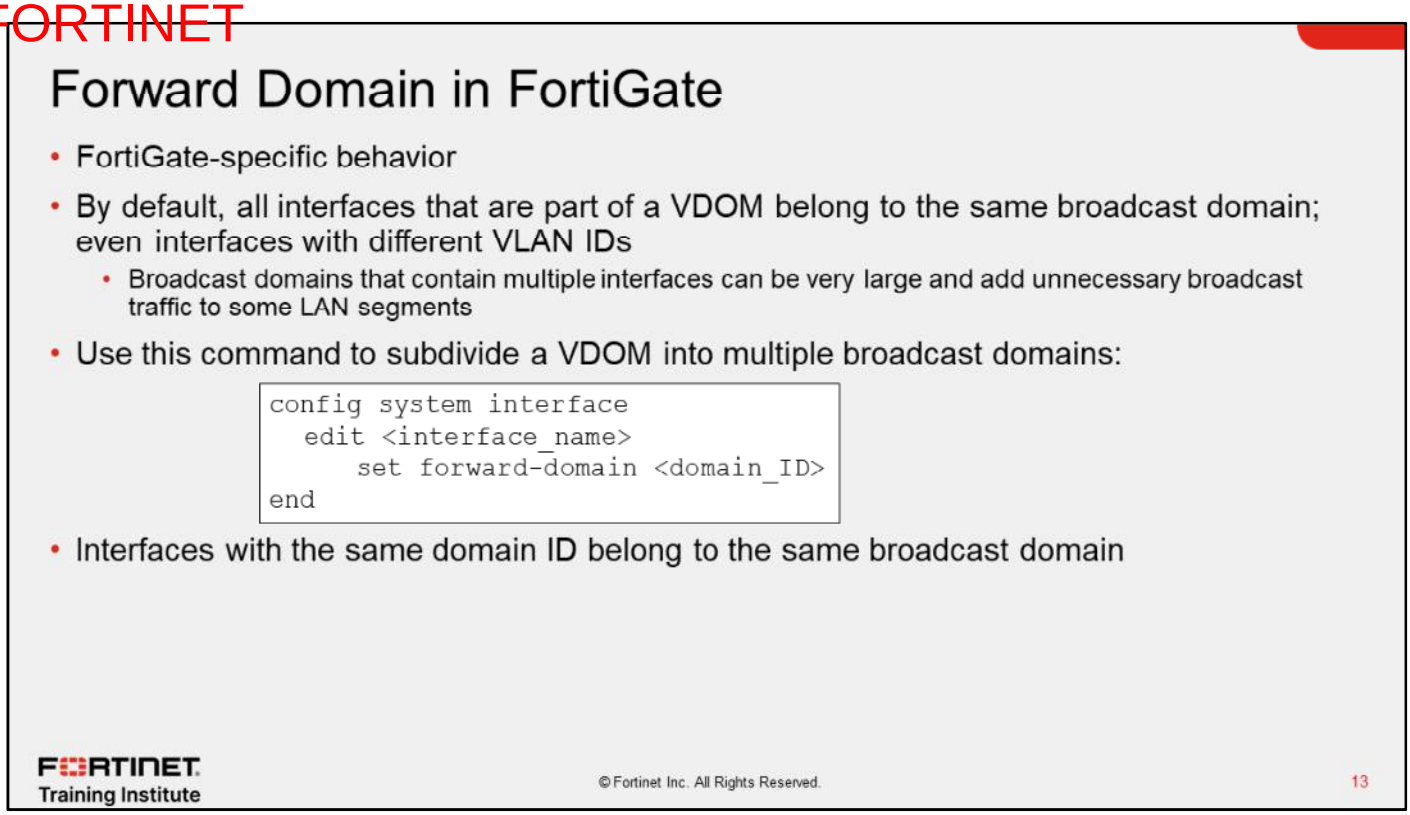
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

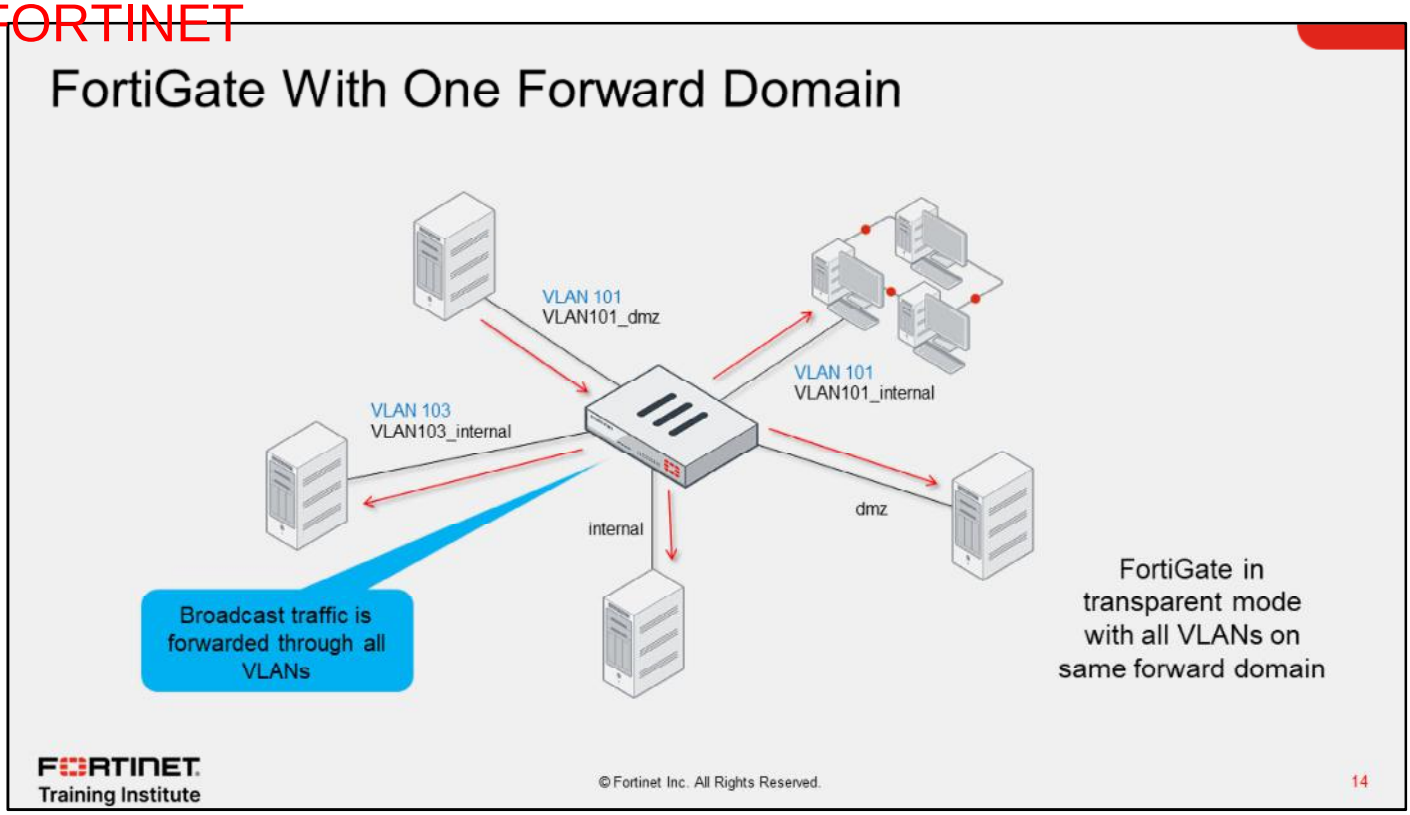
Router on a stick is used within an OT network to achieve inter-VLAN routing. You will need to configure the router interface to operate as an 802.1q trunk link that is connected to a switch interface that is configured in trunk mode as well. The router receives VLAN tagged traffic from the switch. The router then removes the tag and adds another VLAN tag based on the destination address.

DO NOT REPRINT
© FORTINET



Until you change the initial VDOM configuration, all interfaces, regardless of their VLAN ID, are part of the same broadcast domain. FortiGate will broadcast from every interface in the VDOM in order to find any unknown destination MAC addresses. On large networks, this could generate massive broadcast traffic and overwhelming replies—a broadcast storm.

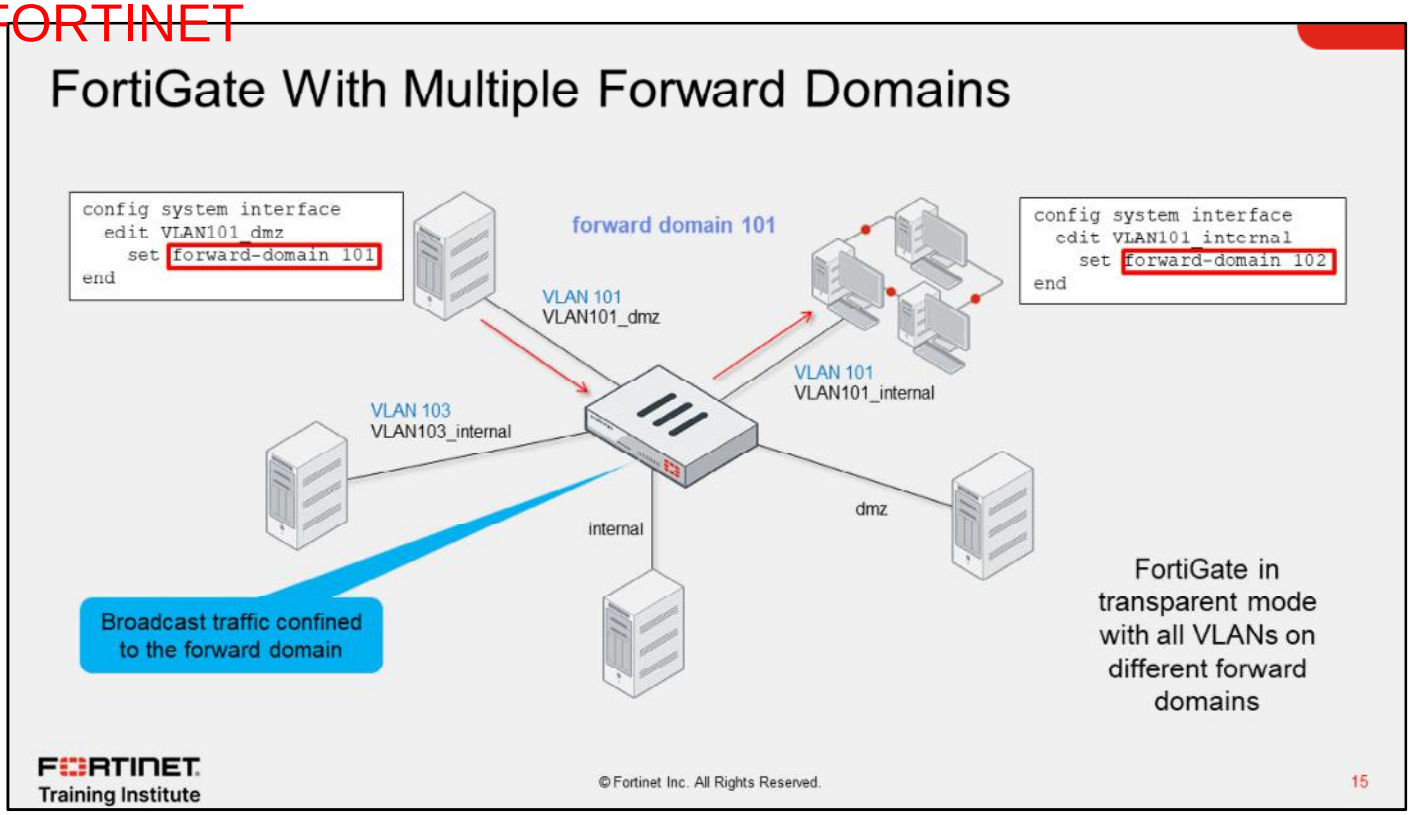
DO NOT REPRINT
© FORTINET



This slide illustrates a problem—a broadcast with all the interfaces on the forward domain 0 (default). One device sends an ARP request. The request reaches FortiGate through one of the interfaces in the VDOM.

Because all interfaces belong to the same forward domain, FortiGate rebroadcasts the request to all the other interfaces, even to interfaces that belong to different VLANs. This generates unnecessary traffic. After that, the ARP reply will still arrive on only one interface, and FortiGate will learn that the MAC is on that interface.

DO NOT REPRINT
© FORTINET

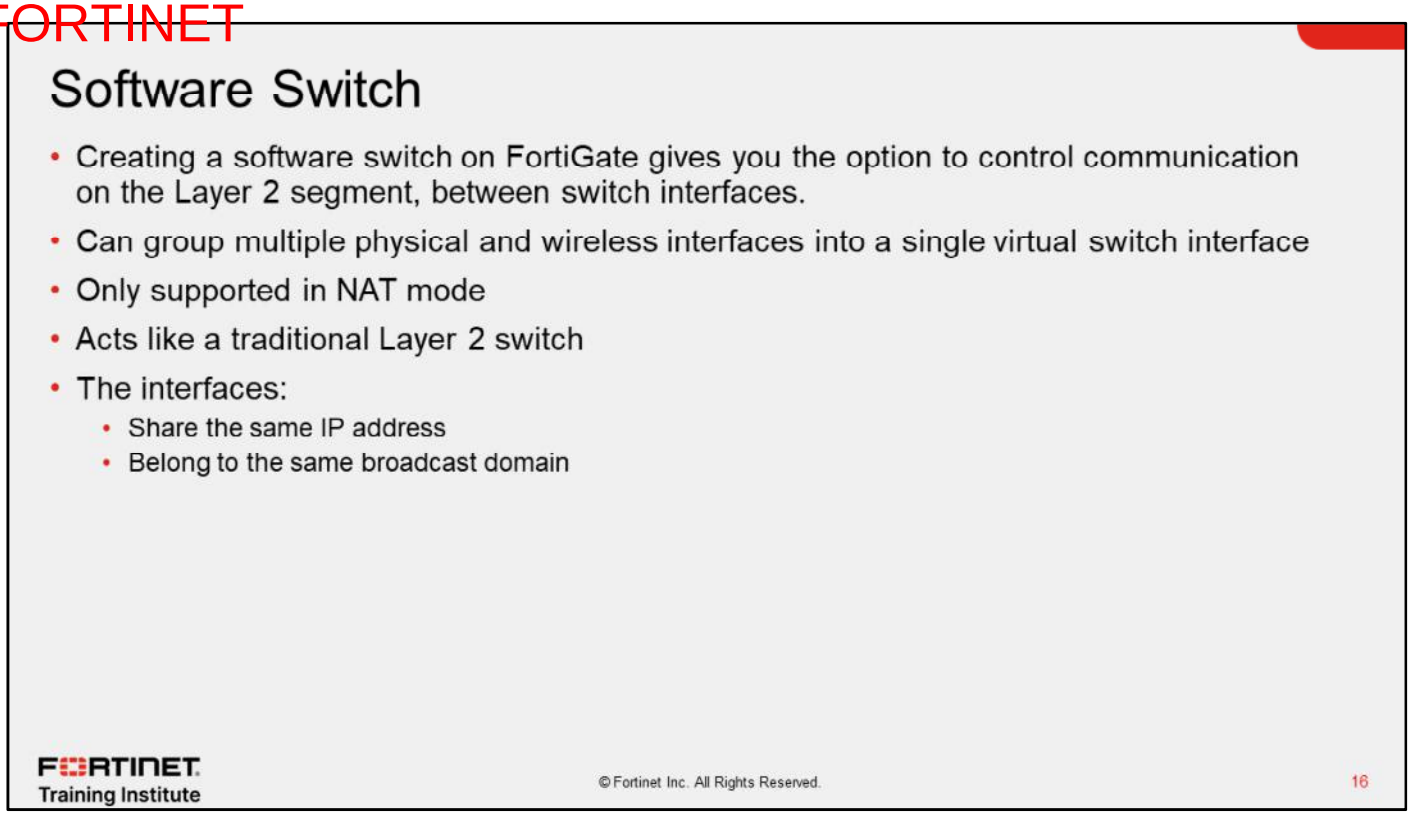


Forward domains are like broadcast domains.

The example on this slide shows the same network as before, but different forward domain IDs are assigned to each VLAN.

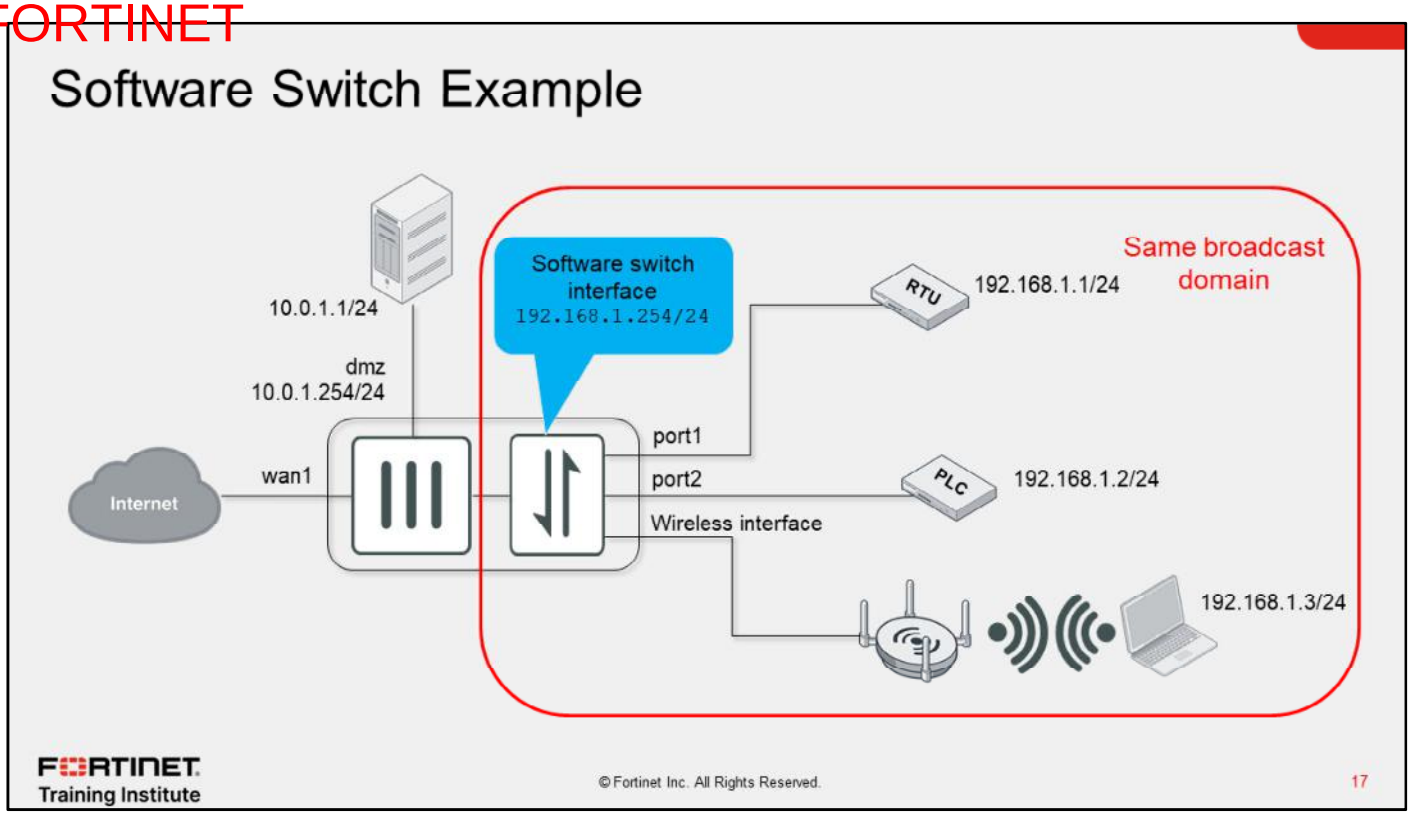
Traffic arriving on one interface is broadcast only to interfaces that are in the same forward domain ID.

DO NOT REPRINT
© FORTINET



A software switch groups multiple interfaces to form a virtual switch, which acts as a traditional Layer 2 switch. This means that all switch interfaces are part of the same broadcast domain. Creating a software switch on FortiGate provides the option to control the communication on the Layer 2 segment, between switch interfaces.

DO NOT REPRINT
© FORTINET

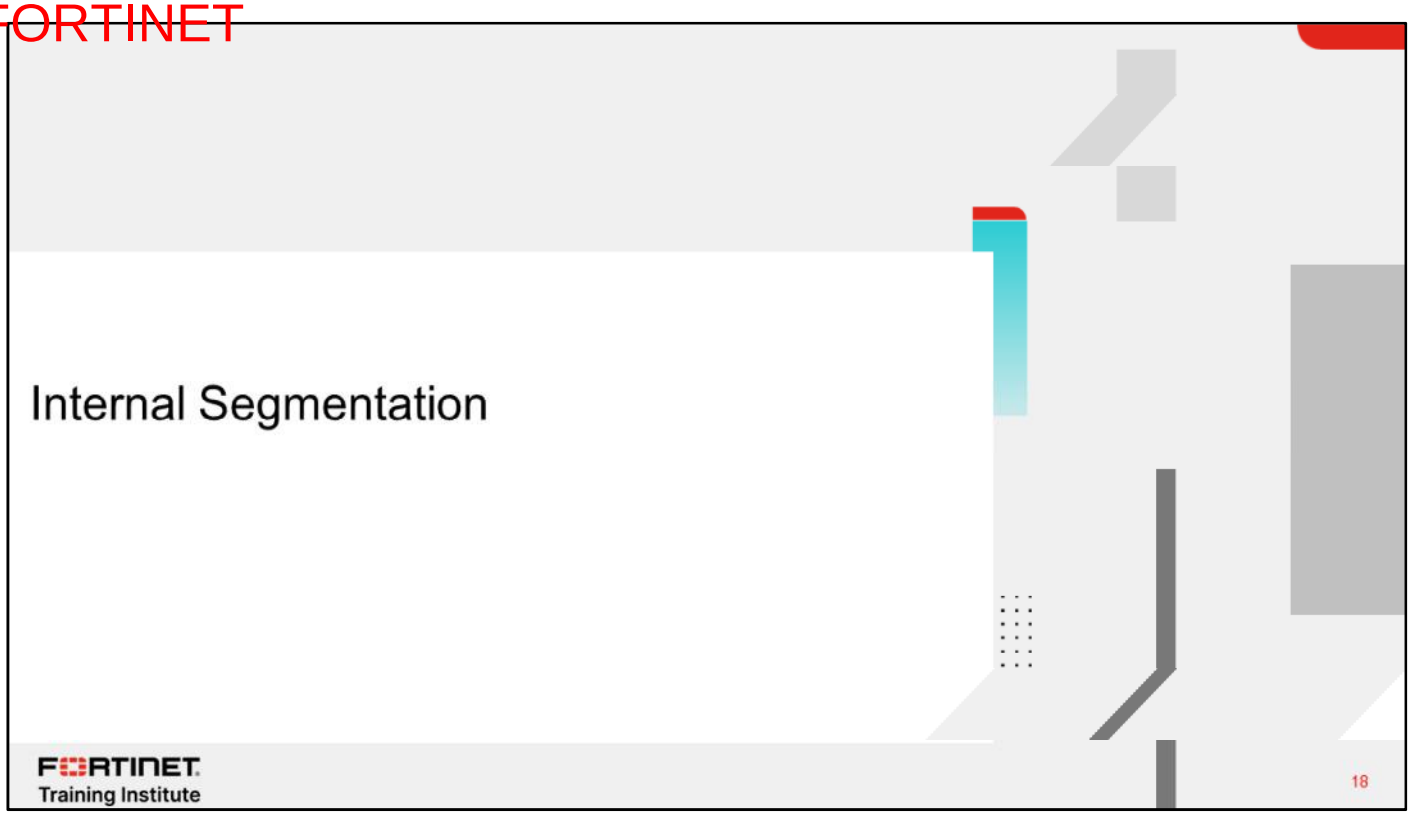


In the example shown on the slide, the administrator grouped a wireless interface with port1 and port2 to form a software switch. These three interfaces are part of the same broadcast domain. All the devices connected to the switch interfaces belong to the same IP subnet: `192.168.1.0/24`. This allows FortiGate to forward broadcast traffic from the wireless clients to port1 and port2.

The software switch interface itself has an IP address, which is also in the same subnet: `192.168.1.0/24`. This is the default gateway IP address for all the devices connected to the software switch.

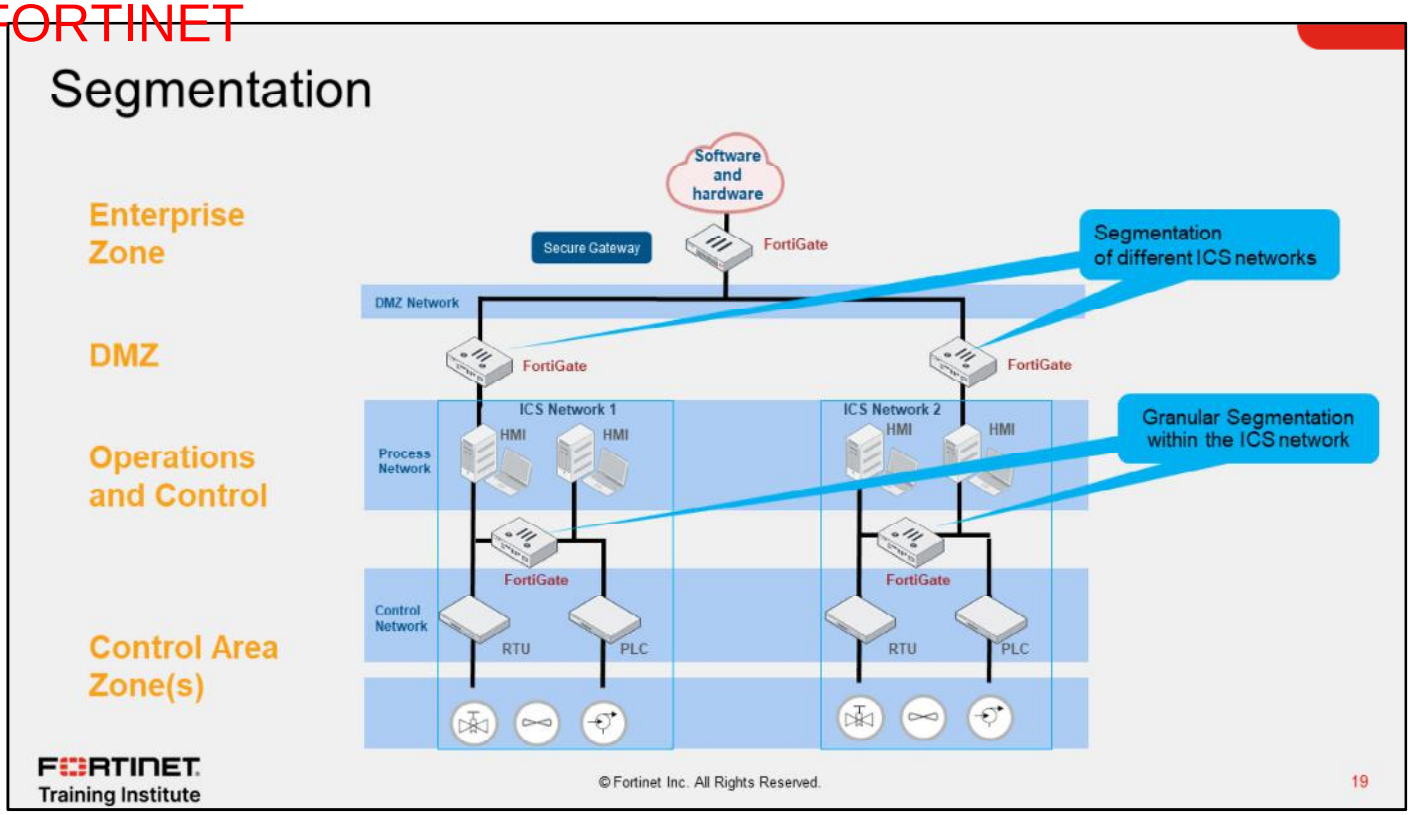
The server `10.0.1.1` is connected to an interface (dmz) that is not part of the software switch. So, it belongs to a different broadcast domain and IP subnet.

DO NOT REPRINT
© FORTINET



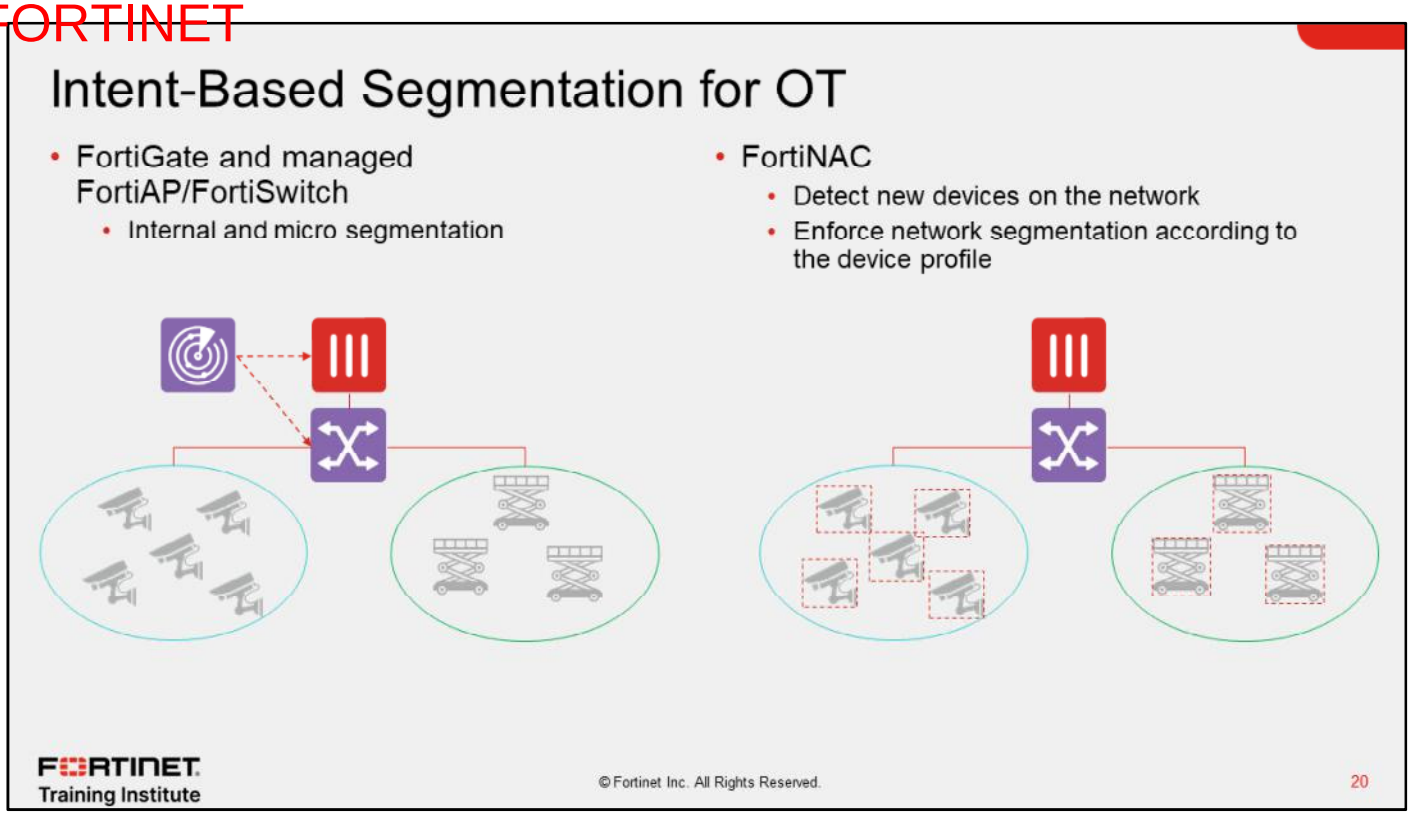
In this section, you will learn about internal segmentation using FortiGate.

DO NOT REPRINT
© FORTINET



Network segmentation is an architectural approach to dividing an OT network into multiple segments; each acting as its own network. This allows an OT network administrator to control the flow of the traffic subnets based on policies. In an OT network, segmentation is used to improve monitoring, boost performance, localize technical issues, and enhance security.

DO NOT REPRINT
© FORTINET

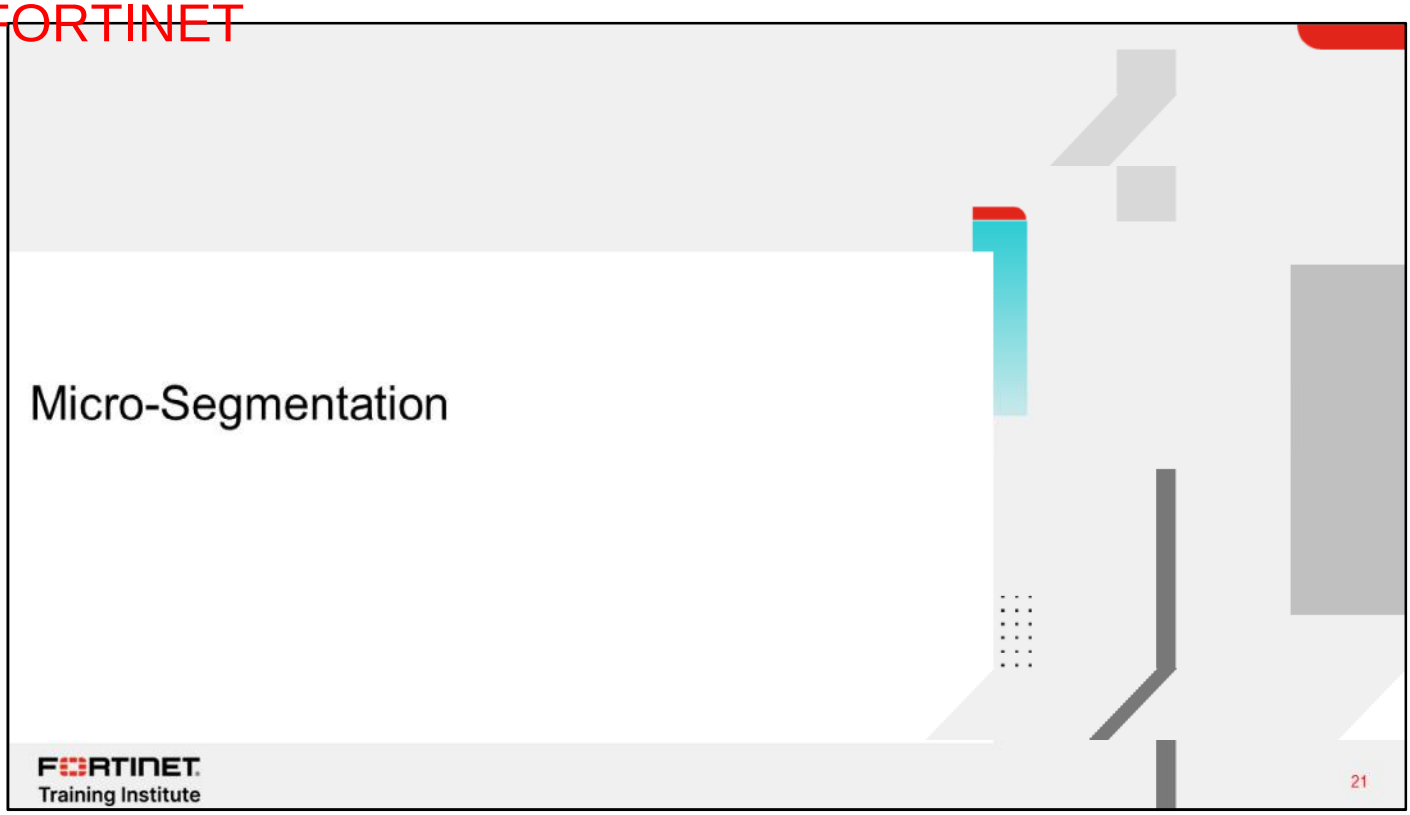


In an OT network, segmentation can be achieved with either FortiNAC, or FortiGate and managed through FortiSwitch/FortiAP.

You can use FortiNAC to detect devices on a network and place them in different device profiles. You can now segment the OT network based on the device profile created.

On the other hand, you can use FortiGate to implement internal segmentation and can use a managed FortiSwitch device to implement micro-segmentation.

DO NOT REPRINT
© FORTINET

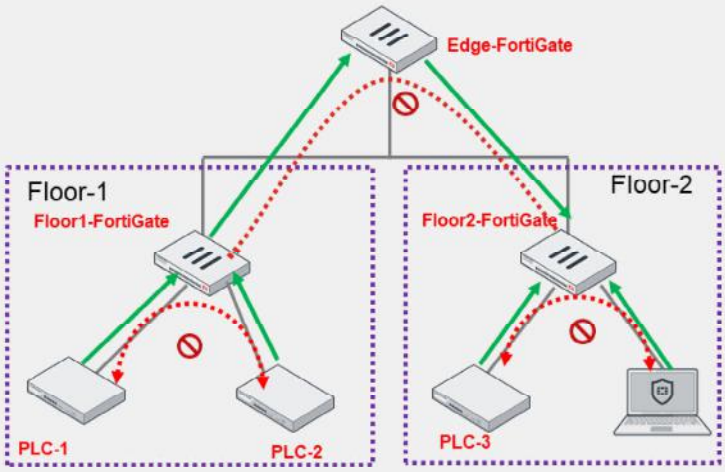


In this section, you will learn about implementing micro-segmentation.

DO NOT REPRINT
© FORTINET

Micro-Segmentation—Host Isolation

- Provide extra security to the process layer:
  - All intra-VLAN traffic is controlled from FortiGate
  - Hosts are not able to see each other
  - Host can communicate only with FortiGate
  - FortiGate implements the allowed access per host or group of hosts
  - Increase traffic visibility, which can be used for monitoring traffic behavior and for threat hunting



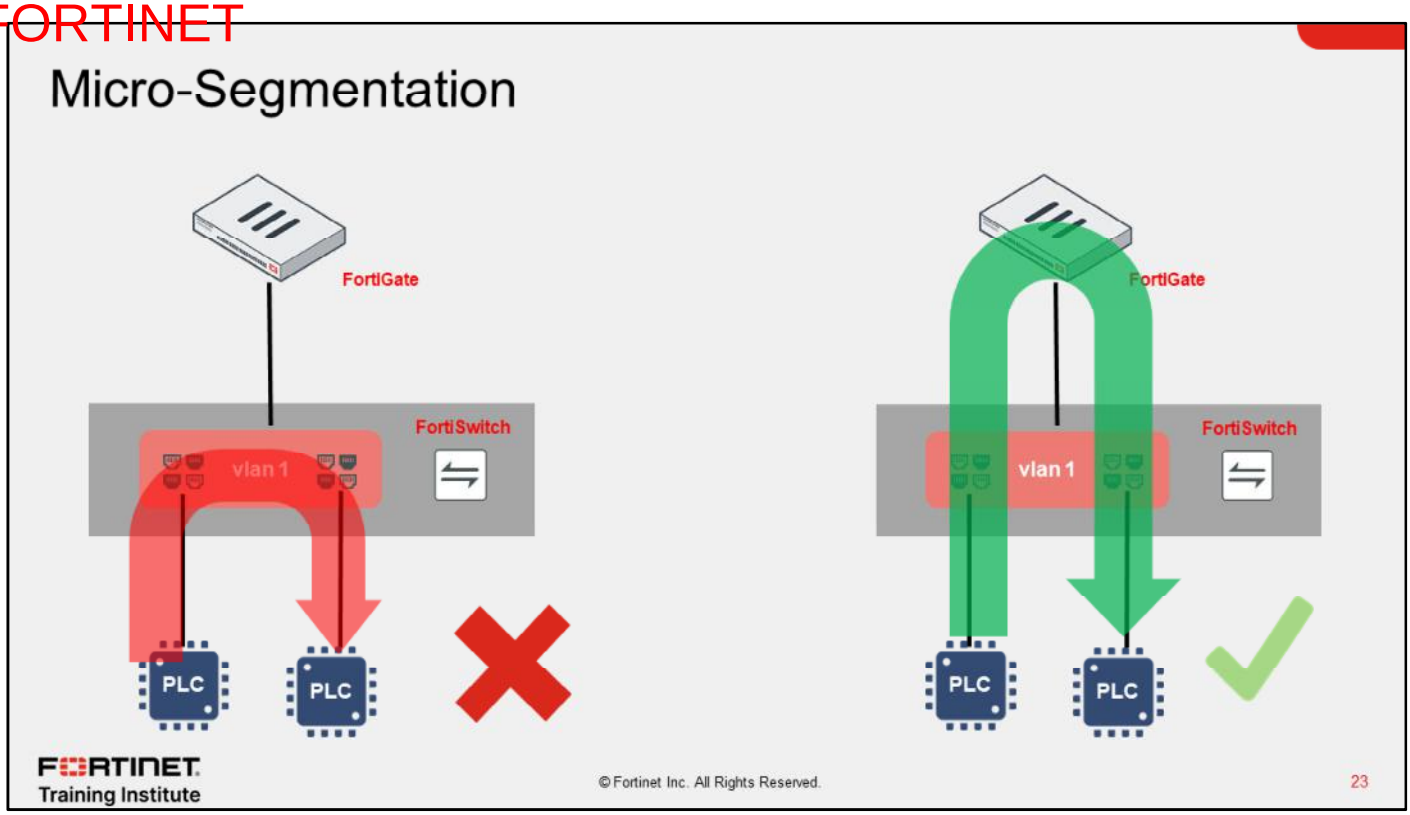
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Micro-segmentation can be used to provide extra security by managing traffic flows through firewall policies. By implementing micro-segmentation, you can control intra-VLAN traffic. By doing so, hosts on the same VLAN will not be able to detect and communicate with each other. The host will be able to communicate only with FortiGate, and you will need to create firewall policies to allow traffic between interfaces in the same VLAN.

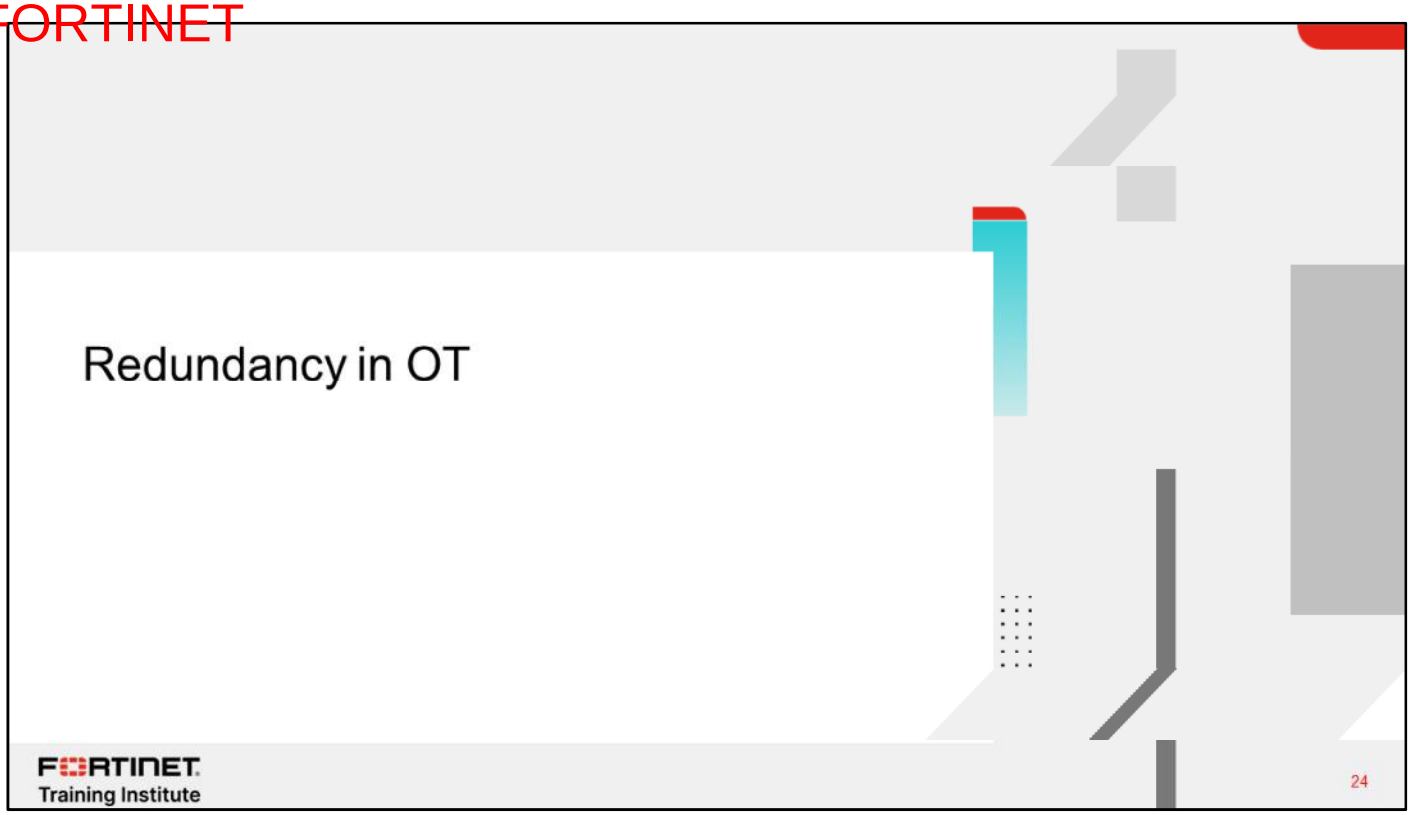
DO NOT REPRINT
© FORTINET



Micro-segmentation prevents direct device-to-device communication. Micro-segmentation can be configured using the access VLAN with the use of a standalone or managed FortiSwitch, as well as with an explicit intra-switch policy, when using a software switch.

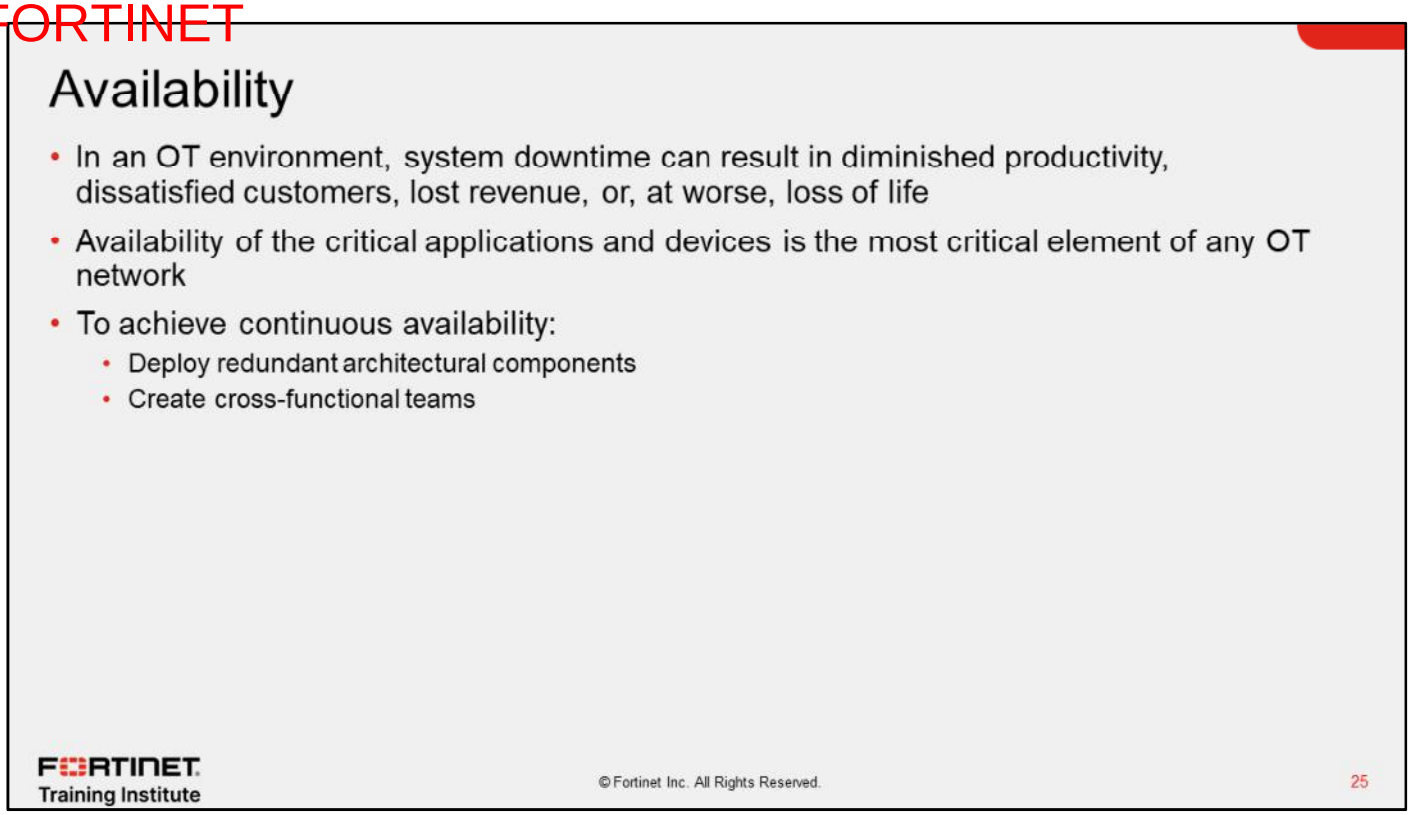
As shown on this slide, two PLCs are in the same VLAN and they are connected to a non-managed switch. Both PLCs can connect to each other because they are part of the same VLAN. However, with software-switch or managed FortiSwitch, you can control intra-VLAN traffic through firewall policies.

DO NOT REPRINT
© FORTINET



In this section, you will learn about different types of redundancy in an OT network.

DO NOT REPRINT
© FORTINET

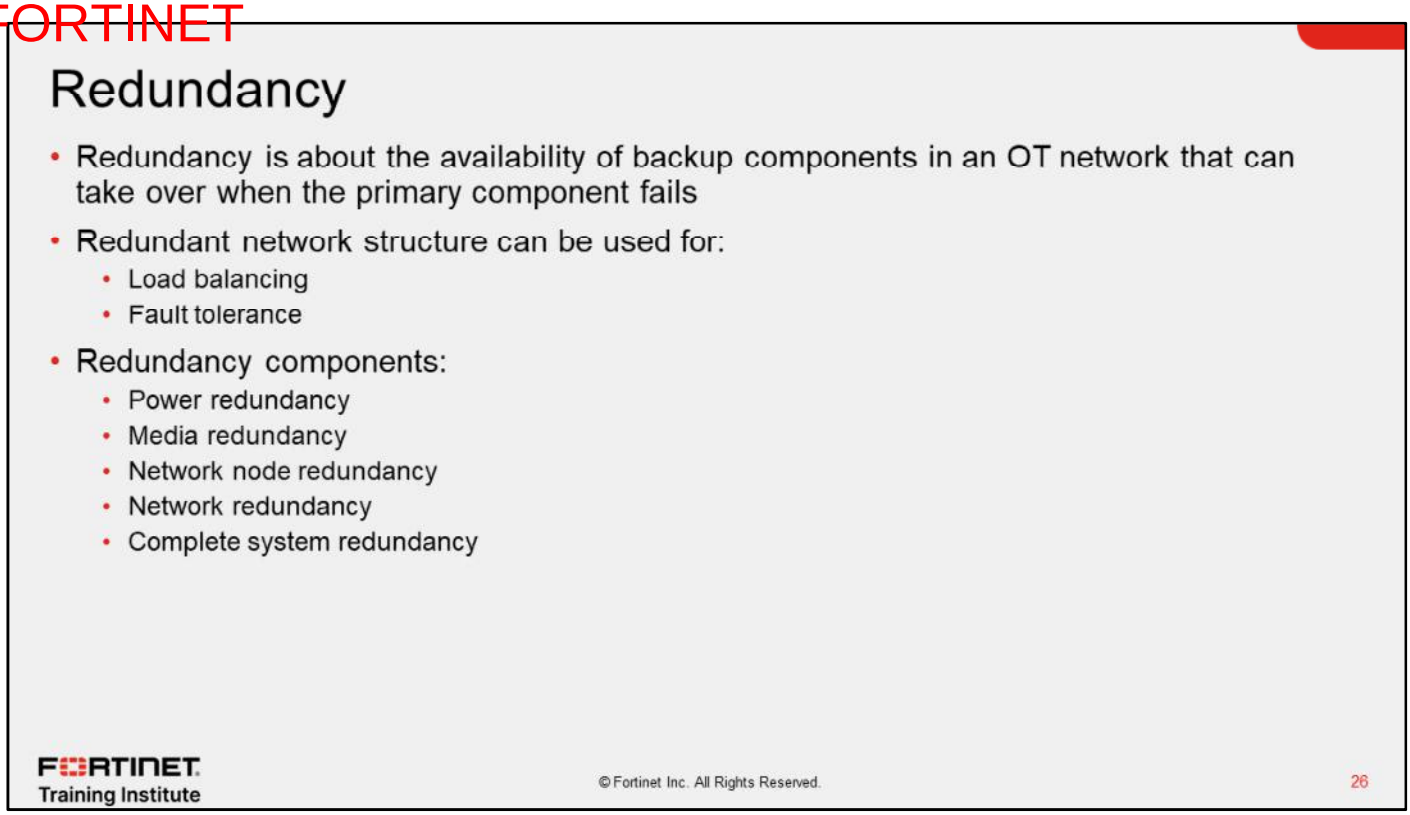


In an OT network, many intelligent systems are used where any downtime could lead, at best, to diminished productivity, dissatisfied customers, or lost revenue. For critical systems, such as medical devices, and surveillance solutions, downtime could lead to loss of life, loss of property, or significant environmental or health hazards.

To achieve continuous availability, redundant architecture components can be deployed in each tier to avoid single points of failure.

IT and OT teams each provide unique skills, perspectives, and experiences. Sharing knowledge and aligning business practices between IT and OT teams could help enterprises achieve both the reliability and availability of OT systems, and the scalability of IT systems.

DO NOT REPRINT
© FORTINET

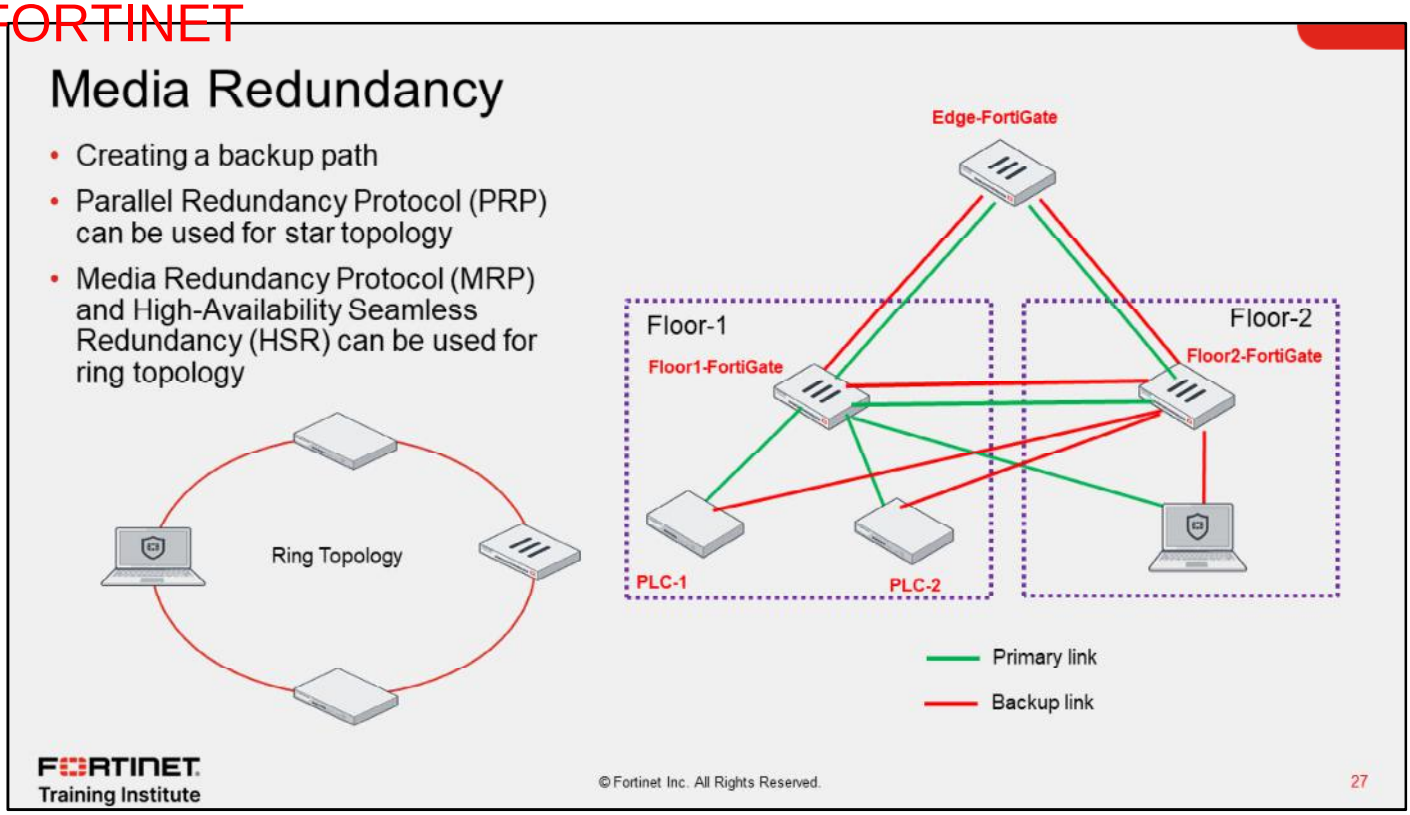


Redundancy is about the availability of backup components or links in an OT network that can take over when the primary component or link fails. In an OT network, redundancy can be used for two purposes. First, you can use the redundant links and redundant device for traffic and recourse load balancing. With this structure, you can share the resources and bandwidth and, at the same time, implement backup components and links ready for failover.

Secondly, you can implement redundancy for fault tolerance. In this structure, the links and components are used for backup only, and not to share the recourses or traffic.

You can divide redundancy component into five types:
1. Power redundancy
2. Media redundancy
3. Network node redundancy
4. Network redundancy
5. Complete system redundancy

DO NOT REPRINT
© FORTINET



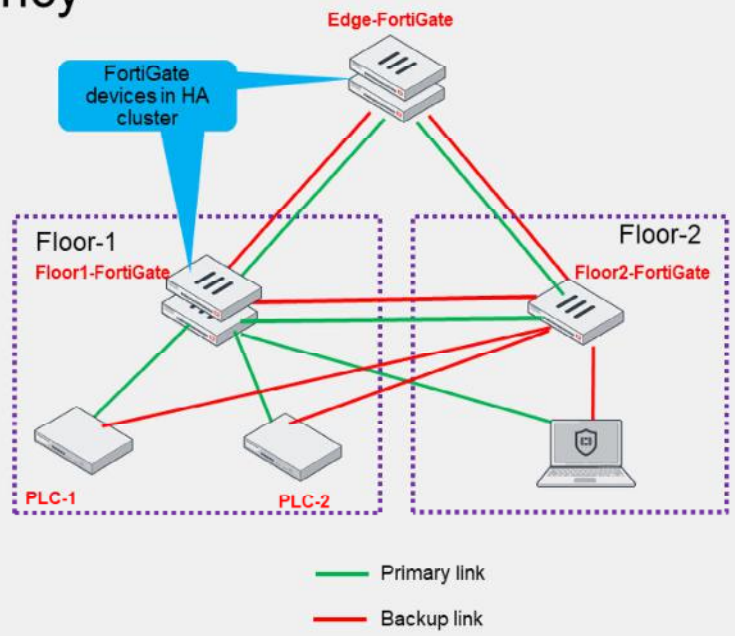
Media redundancy involves creating a backup path that can be used when part of the network fails. A ring topology or star topology can be used to achieve a redundant link. PRP is one of the OT protocols that can be used for a star topology to introduce media redundancy. MRP and HSR are some of the protocols that can be used to achieve a redundant network with ring topology.

Selecting a topology for redundancy can be crucial because, in many networks, star or mesh topologies can become costly. When cable cost is a concern, a ring topology can reduce the cost. For example, wind turbine monitoring and management requires a long wiring distance. In cases like this, a ring topology can decrease the cost of wiring comparatively.

DO NOT REPRINT
© FORTINET

Network Node Redundancy

- Entry points without redundancy can be implemented with a secondary device
- A switch or firewall connected to critical network can also be configured with a backup node



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

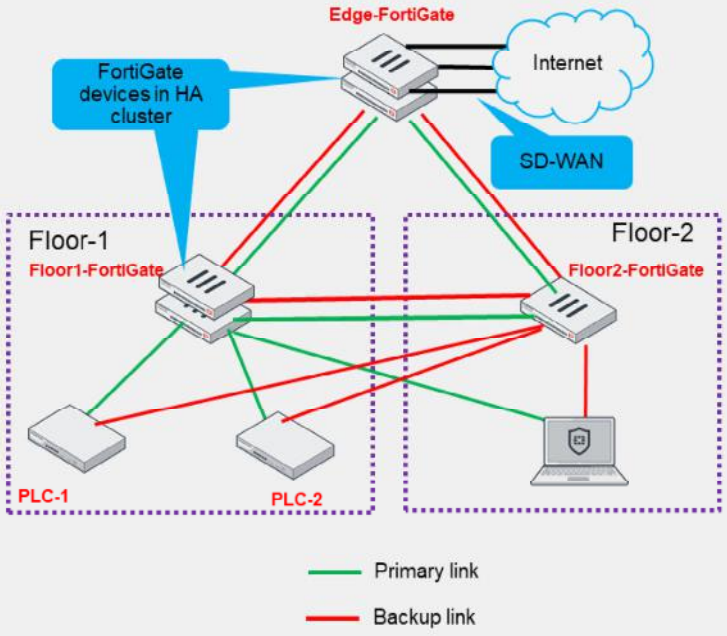
28

After implementing media redundancy, another challenge is implementing redundancy for entry points and nodes where redundancy is not possible. To resolve this issue, and to implement redundancy, you can use a device in an HA cluster for these nodes. Configuring devices with an active-passive HA cluster will provide redundancy when the primary unit fails. There are other factors that can be configured to trigger failover, including link health for critical infrastructure connections.

DO NOT REPRINT
© FORTINET

Network Redundancy

- OT network should be available 100% of the time, even remotely
- For internet access for the OT network, you should rely on more than one provider to make sure of the continuous network availability
- SD-WAN can be used to manage and route traffic through multiple ISPs



FORTINET Training Institute

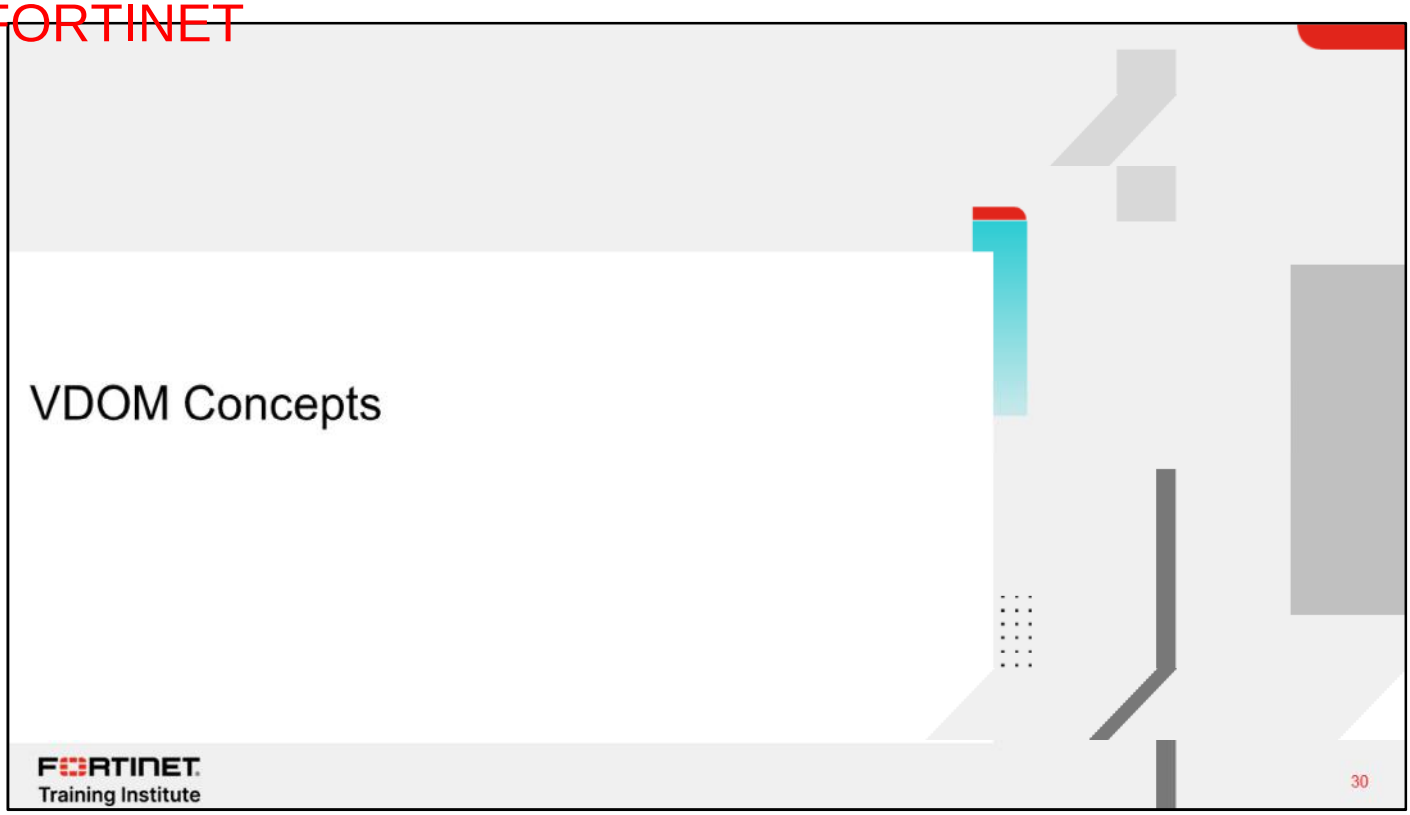
© Fortinet Inc. All Rights Reserved.

29

After implementing media and network node redundancy, you have reduced system downtime. However, when it comes to total redundancy, you have to consider continuous remote access and internet availability as well.

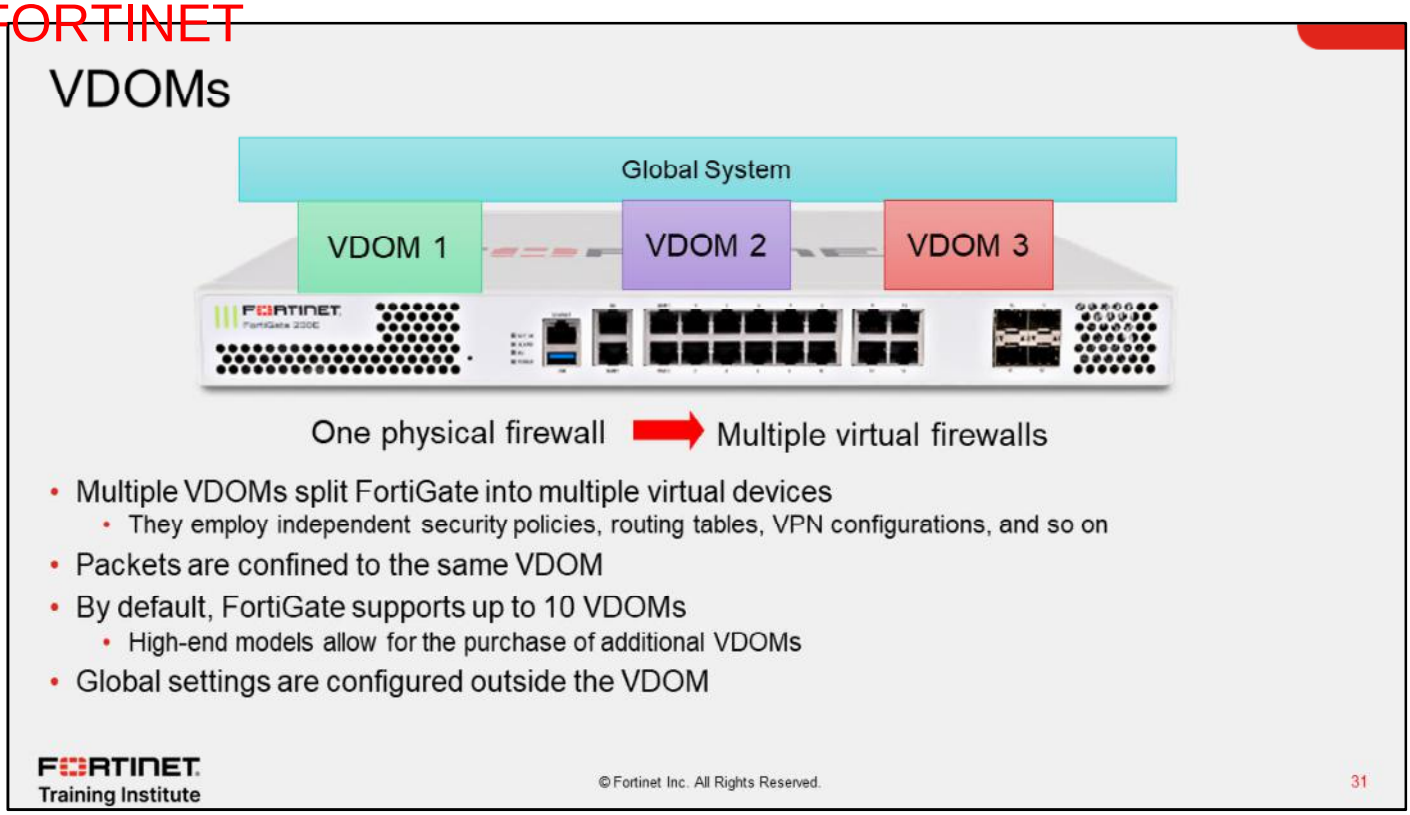
To resolve the issue, you can use more than one ISP, and use SD-WAN to manage the traffic on the ISP link. Using more than one ISP provides internet connections.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the key benefits and use cases for VDOMs.

DO NOT REPRINT
© FORTINET

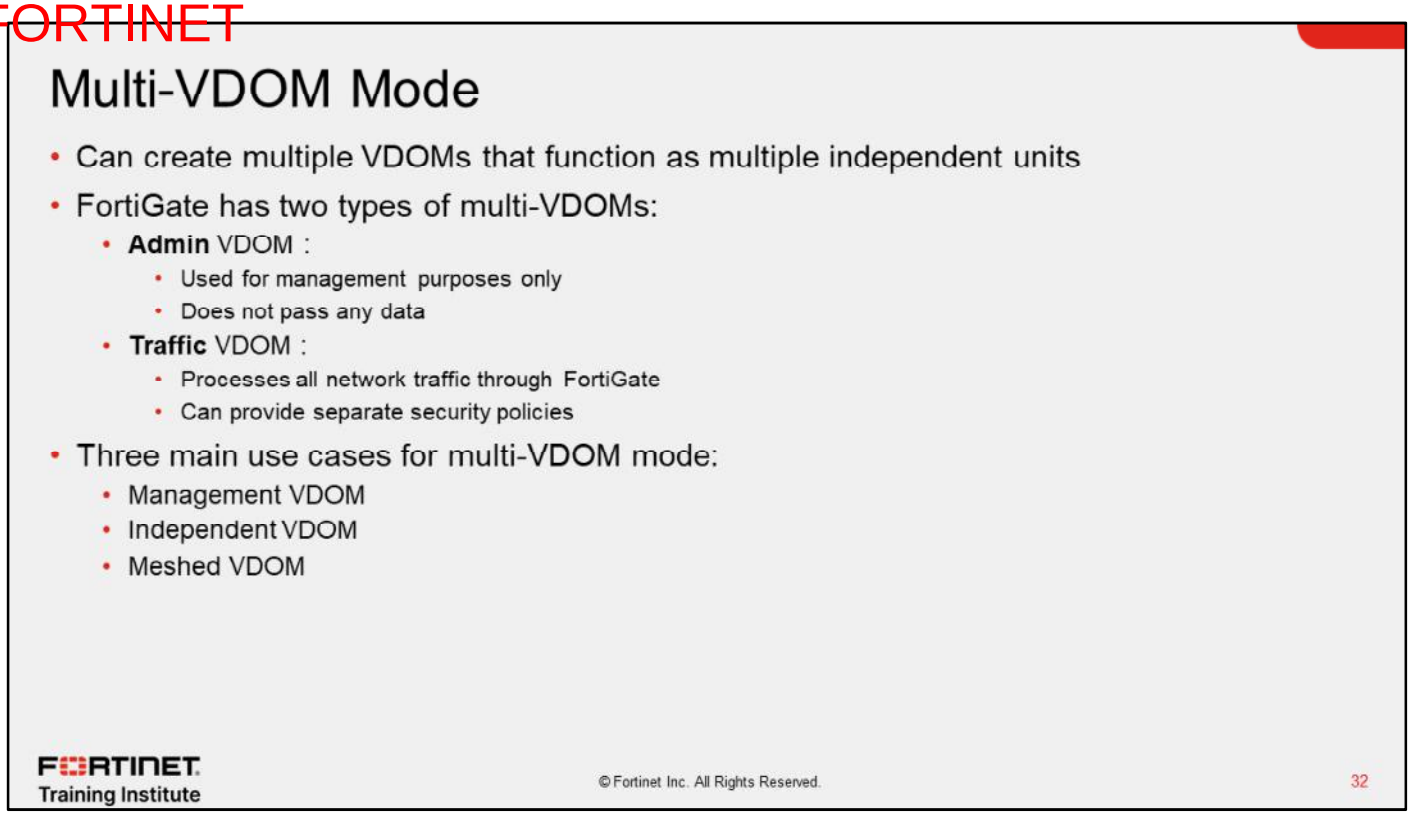


A VDOM splits your FortiGate into multiple logical devices and divides one security domain into multiple security domains.

Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, UTM inspection, and secure communication devices.

DO NOT REPRINT
© FORTINET



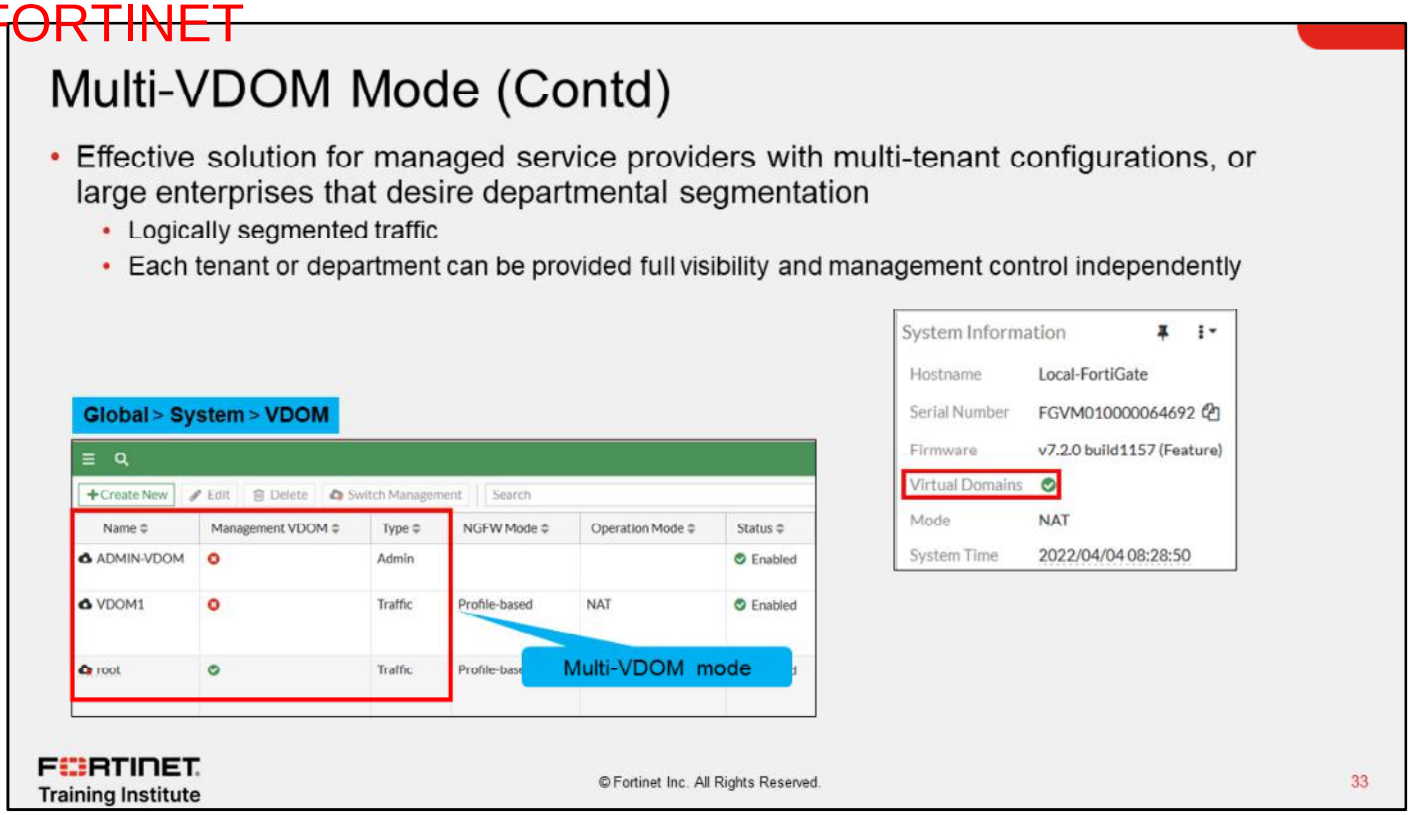
Use multi-VDOM mode when you want to create multiple logical firewalls from a single FortiGate. Each VDOM acts as an independent FortiGate.

Multi-VDOM mode works well for managed service providers leveraging multi-tenant configurations, or large enterprise environments that desire departmental segmentation. You can give each individual tenant or department visibility and control of their VDOM, while keeping other VDOMs independent and unseen.

Two types of VDOMs can be created in multi-VDOM mode: An admin VDOM and a traffic VDOM.
Admin VDOMs are for FortiGate administration, and traffic VDOMs permit traffic to travel through FortiGate.

Upon upgrade, if a FortiGate is in split-task VDOM mode, it is converted to multi-VDOM mode. The FG-traffic VDOM becomes a traffic VDOM. The root VDOM becomes an admin VDOM.

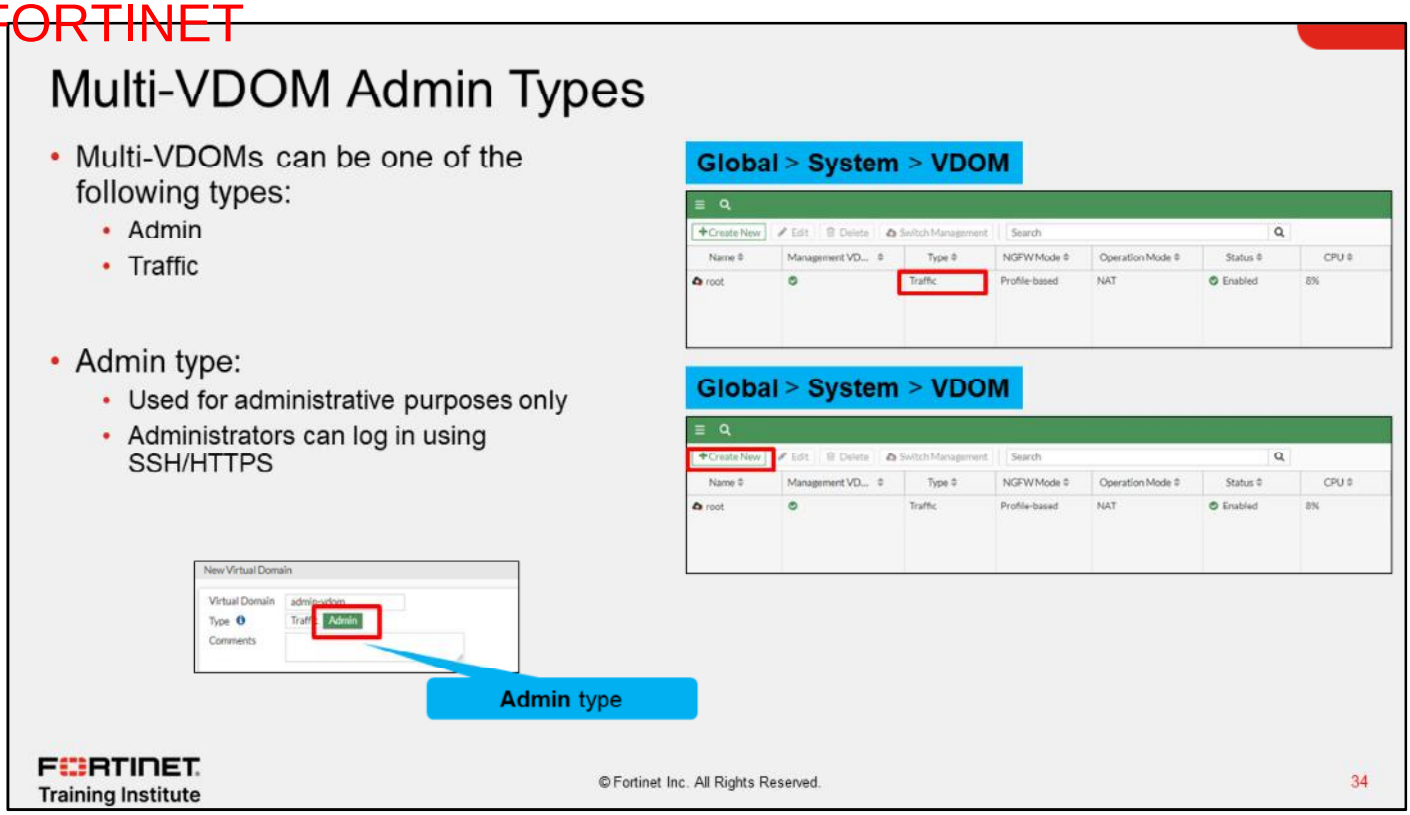
DO NOT REPRINT
© FORTINET



In multi-VDOM mode, you can create multiple VDOMs that function as multiple independent units.

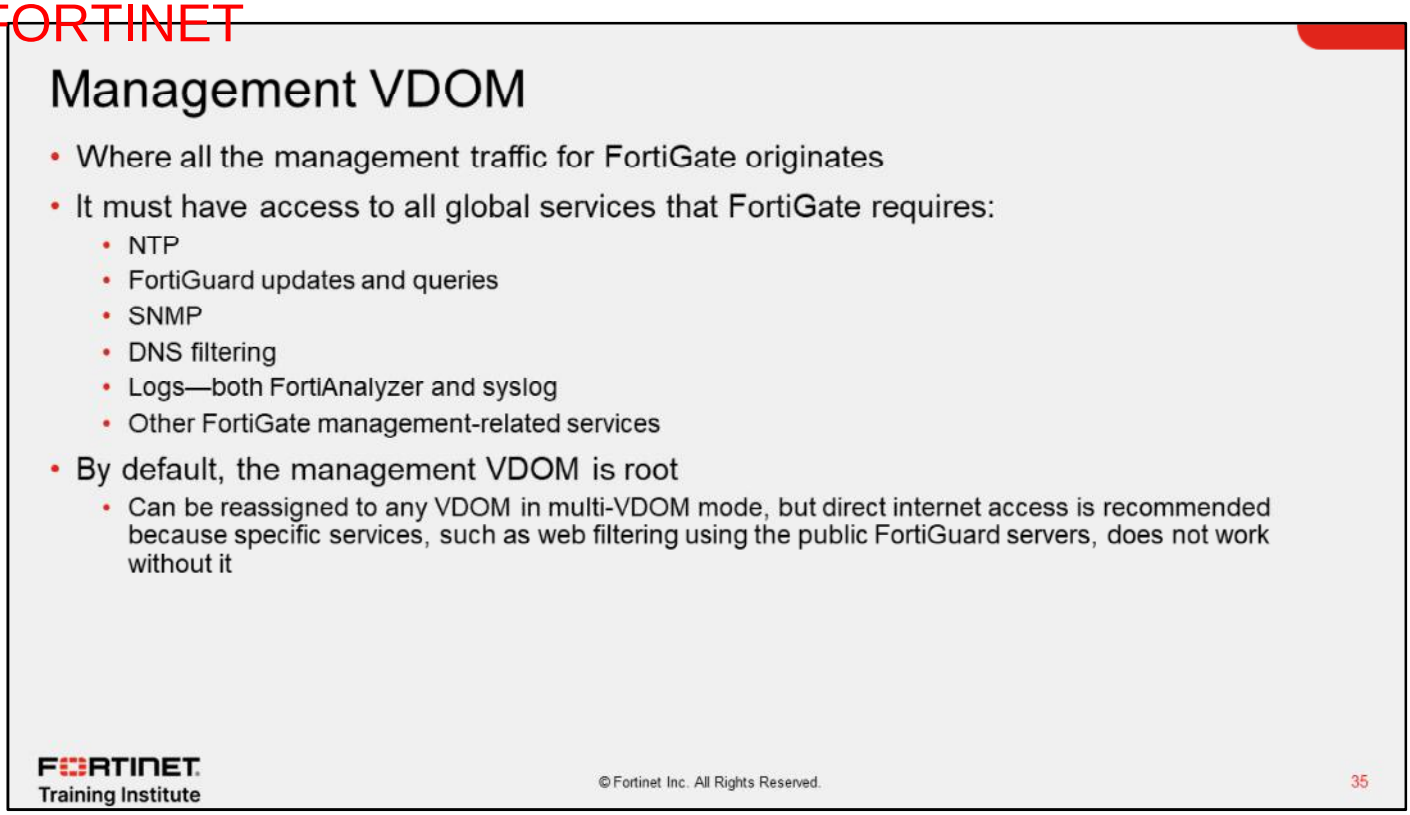
By default, the root is the management VDOM and can be used to do both management tasks and allow other traffic. You can select any VDOM to act as the management VDOM.

DO NOT REPRINT
© FORTINET



When you enable multi-VDOM mode, the root VDOM is created. It is the default management VDOM and is a traffic VDOM. You can create another VDOM (traffic or admin). FortiGate supports only one management VDOM.

DO NOT REPRINT
© FORTINET



Until now, you've learned about traffic passing *through* FortiGate, from one VDOM to another.

What about traffic originating *from* FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic from FortiGate.

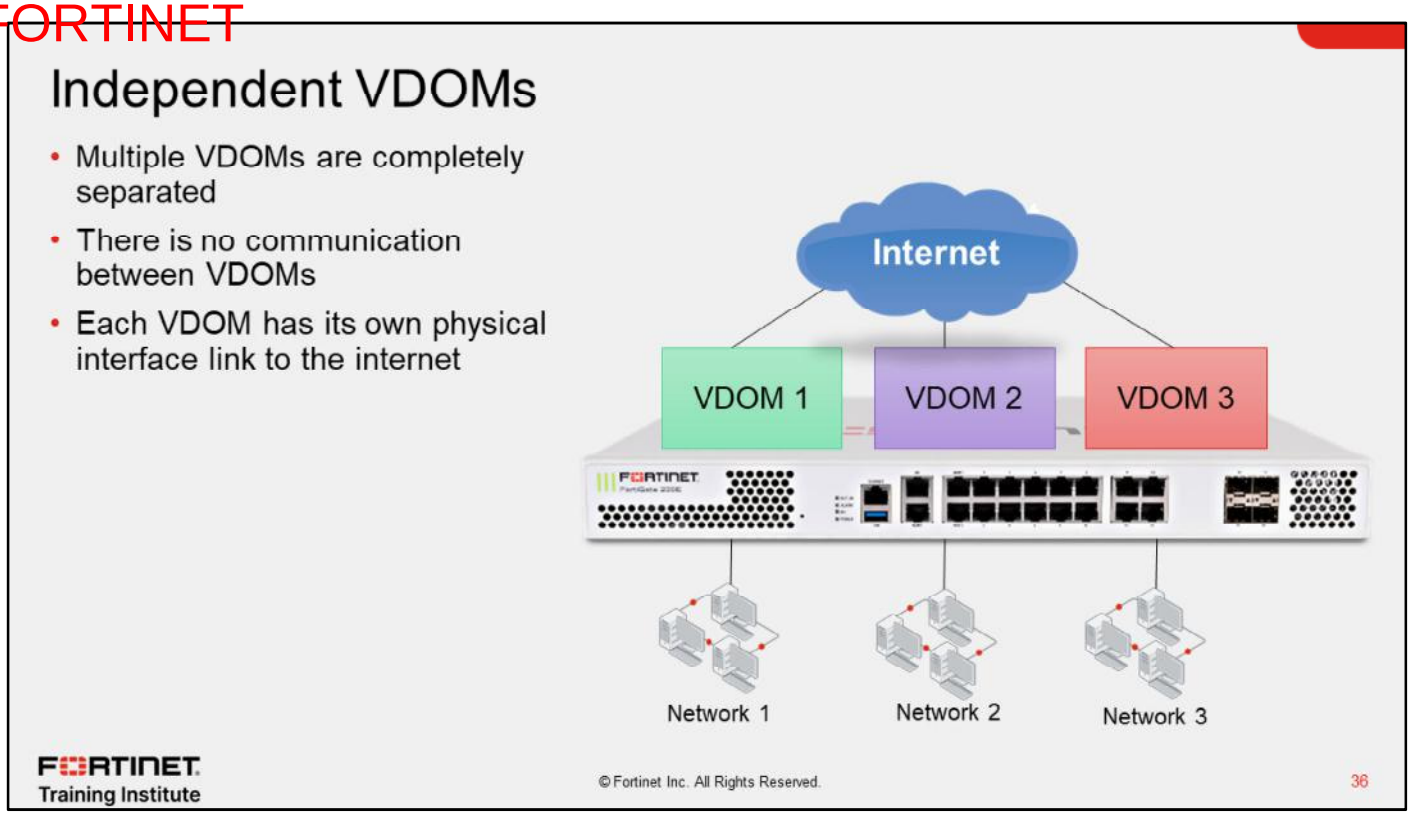
Traffic coming from FortiGate to those global services originates from the *management* VDOM. Only one VDOM on a FortiGate device is assigned the role of the management VDOM.

By default, the root VDOM acts as the management VDOM, but you can manually reassign this task to a different VDOM in multi-VDOM mode.

It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate. As such, the management function can be performed by any designated VDOM.

Similar to FortiGate without VDOMs enabled, the management VDOM should have outgoing internet access. Otherwise, features such as scheduled FortiGuard updates fail.

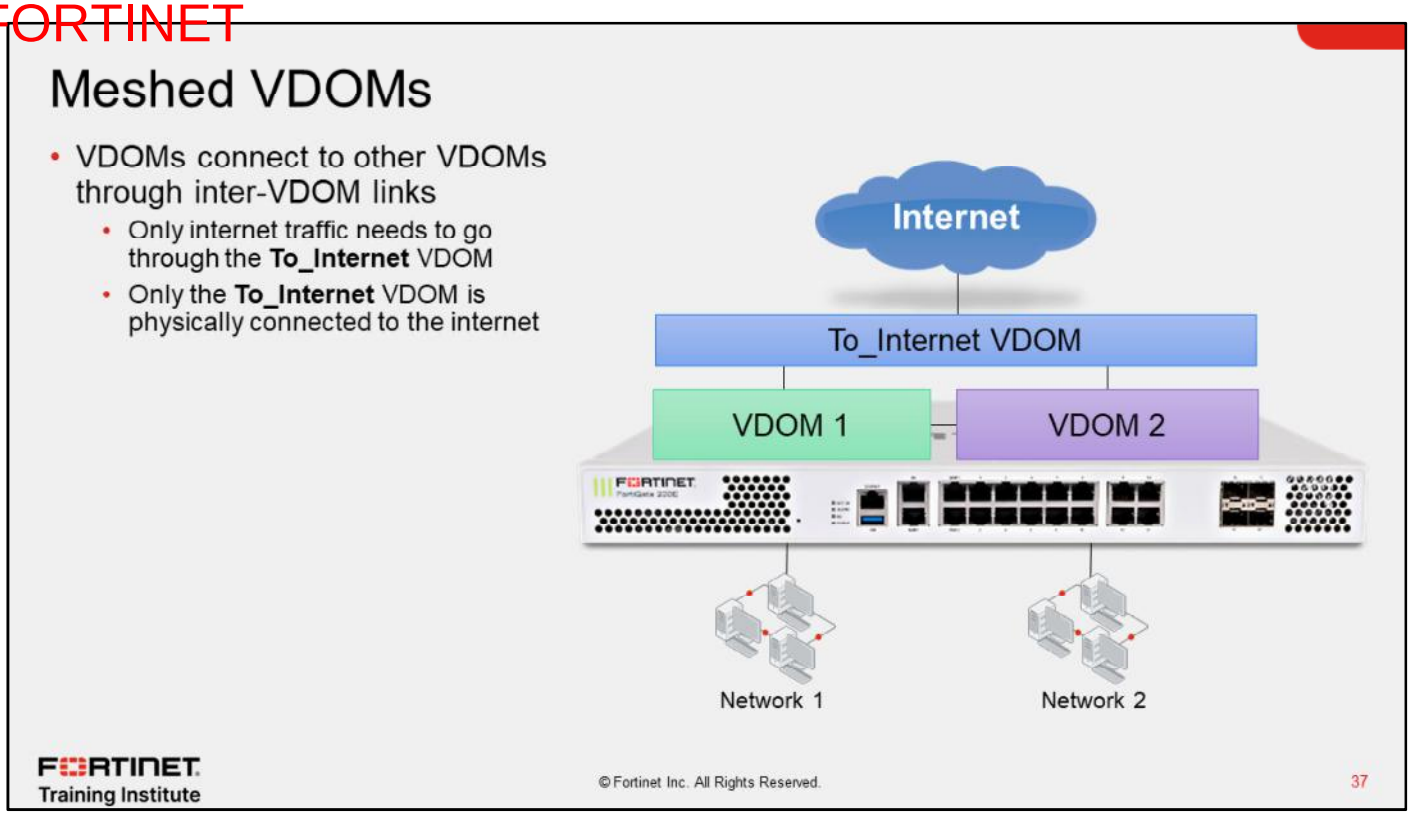
DO NOT REPRINT
© FORTINET



You can arrange your VDOMs in several ways. In the topology shown on this slide, each network accesses the internet through its own VDOM.

Notice that there are no inter-VDOM links. So, inter-VDOM traffic is not possible unless it physically leaves FortiGate, toward the internet, and is rerouted back. This topology would be most suitable in a scenario where multiple customers share a single FortiGate, each in their own VDOM, with physically separated ISPs.

DO NOT REPRINT
© FORTINET



In the example topology shown on this slide, traffic again flows through a single pipe in the **To_Internet** VDOM toward the internet. Traffic between VDOMs doesn't need to leave FortiGate.

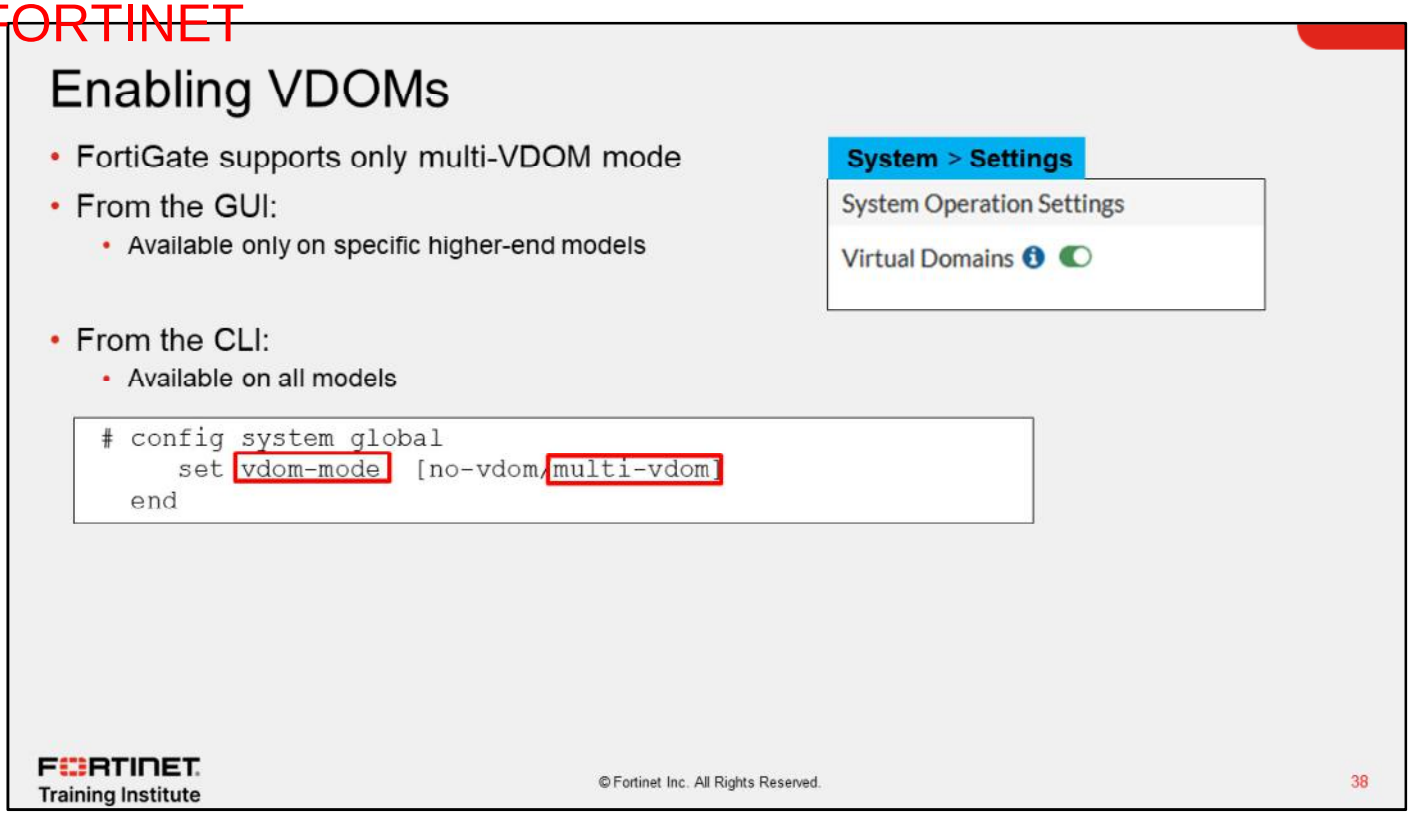
However, now inter-VDOM traffic doesn't need to flow through the **To_Internet** VDOM. Inter-VDOM links between VDOMs allow more direct communication.

Similar to the previous example topology, inspection can be done by either the **To_Internet** or originating VDOM, depending on your requirements.

Because of the number of inter-VDOM links, the example shown on this slide is the most complex, requiring the most routes and firewall policies. Troubleshooting meshed VDOMs can also be more time consuming.

However, meshed VDOMs also provide the most flexibility. For large businesses, inter-VDOM communication may be required. Also, inter-VDOM traffic performance may be better because of a shorter processing path, which bypasses intermediate VDOMs.

DO NOT REPRINT
© FORTINET

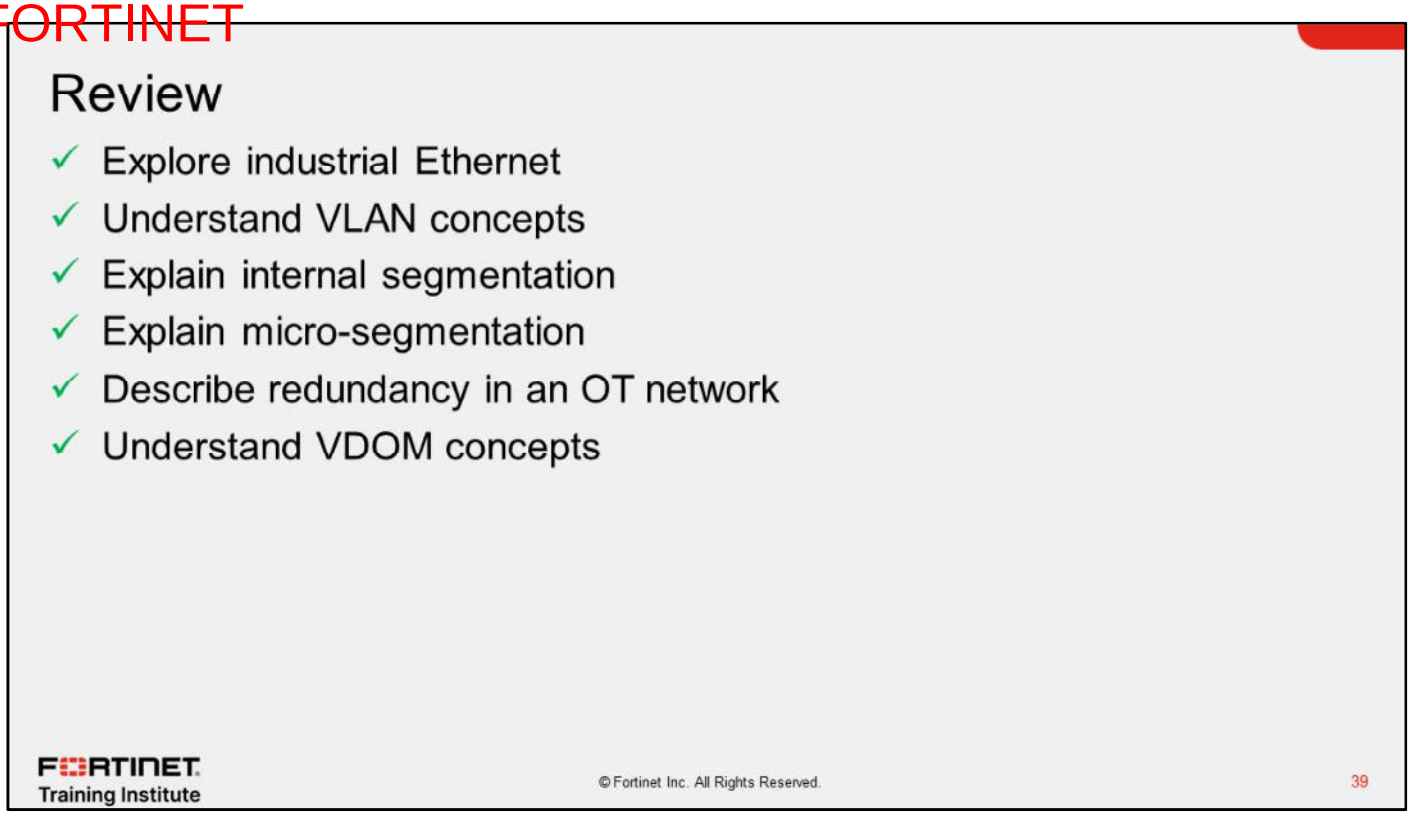


On the GUI, you can enable VDOMs under **System** > **Settings**. The GUI option is available only on higher-end FortiGate models. On other FortiGate models, you can enable VDOMs on the CLI only.

Enabling VDOMs does not cause FortiGate to reboot, but it does log out all active administrator sessions. Traffic continues to pass through FortiGate.

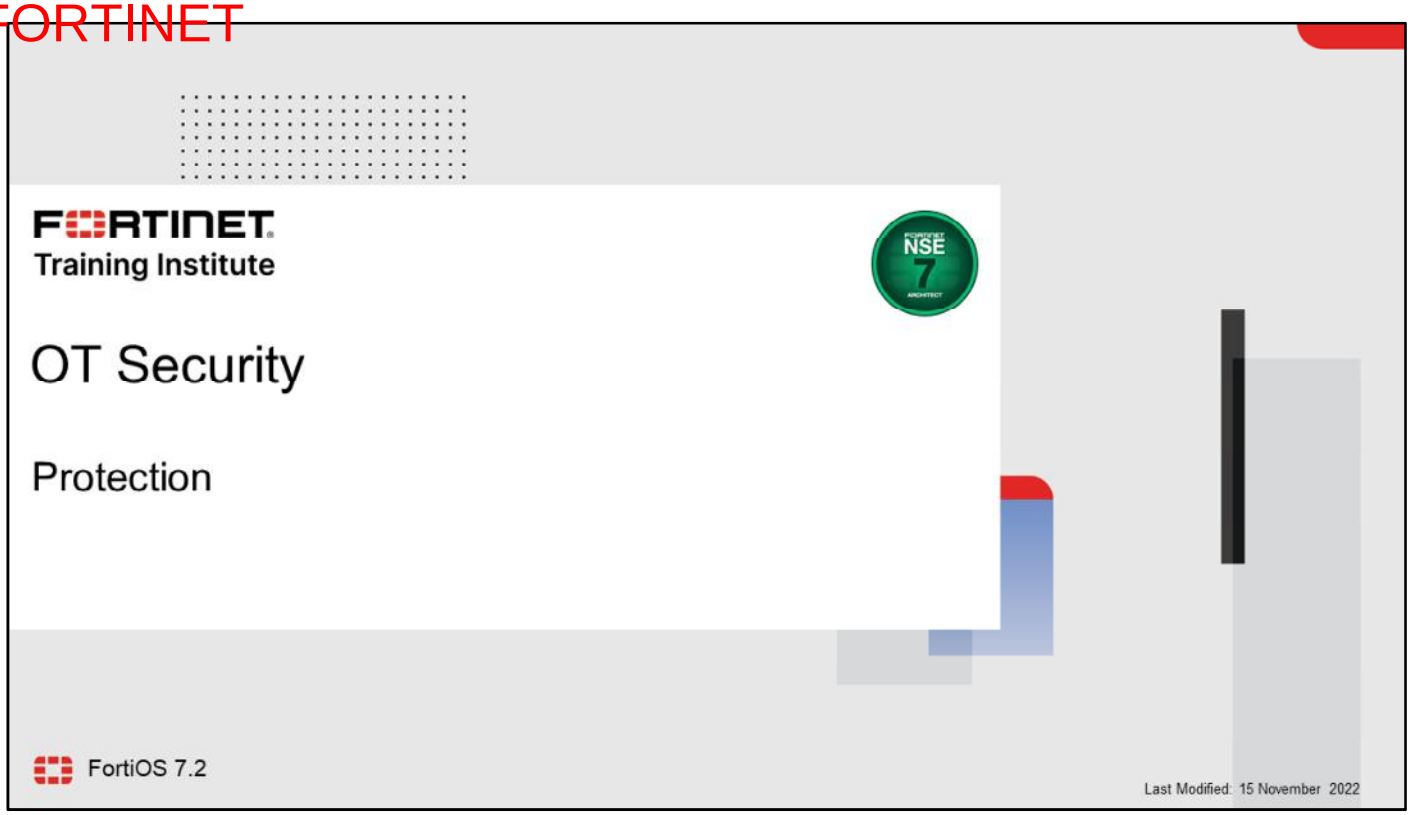
Enabling VDOMs restructures the GUI and CLI, which you will see when you log in again.

DO NOT REPRINT
© FORTINET



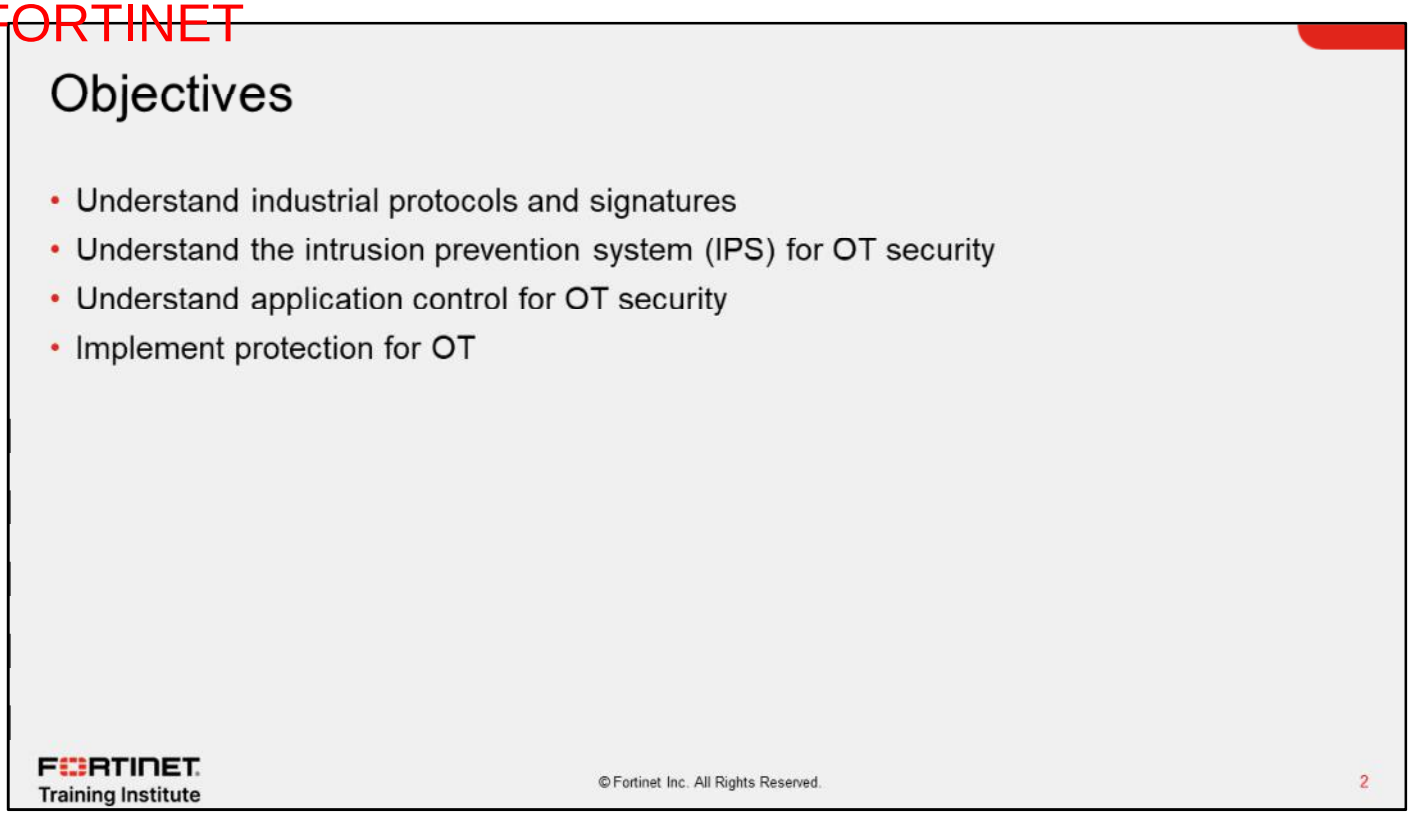
This slide shows the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about protection for an operational technology (OT) environment.

DO NOT REPRINT
© FORTINET



After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the industrial protocols and signatures for an operational technology environment.

DO NOT REPRINT
© FORTINET

Typical SCADA Components

- Programmable logic controllers (PLC) or remote terminal units (RTU) are low computational computers, built to control physical components, such as
  - Valves
  - Pumps
  - Motors
- They communicate with dedicated protocols that are prone to attacks





FORTINET Training Institute

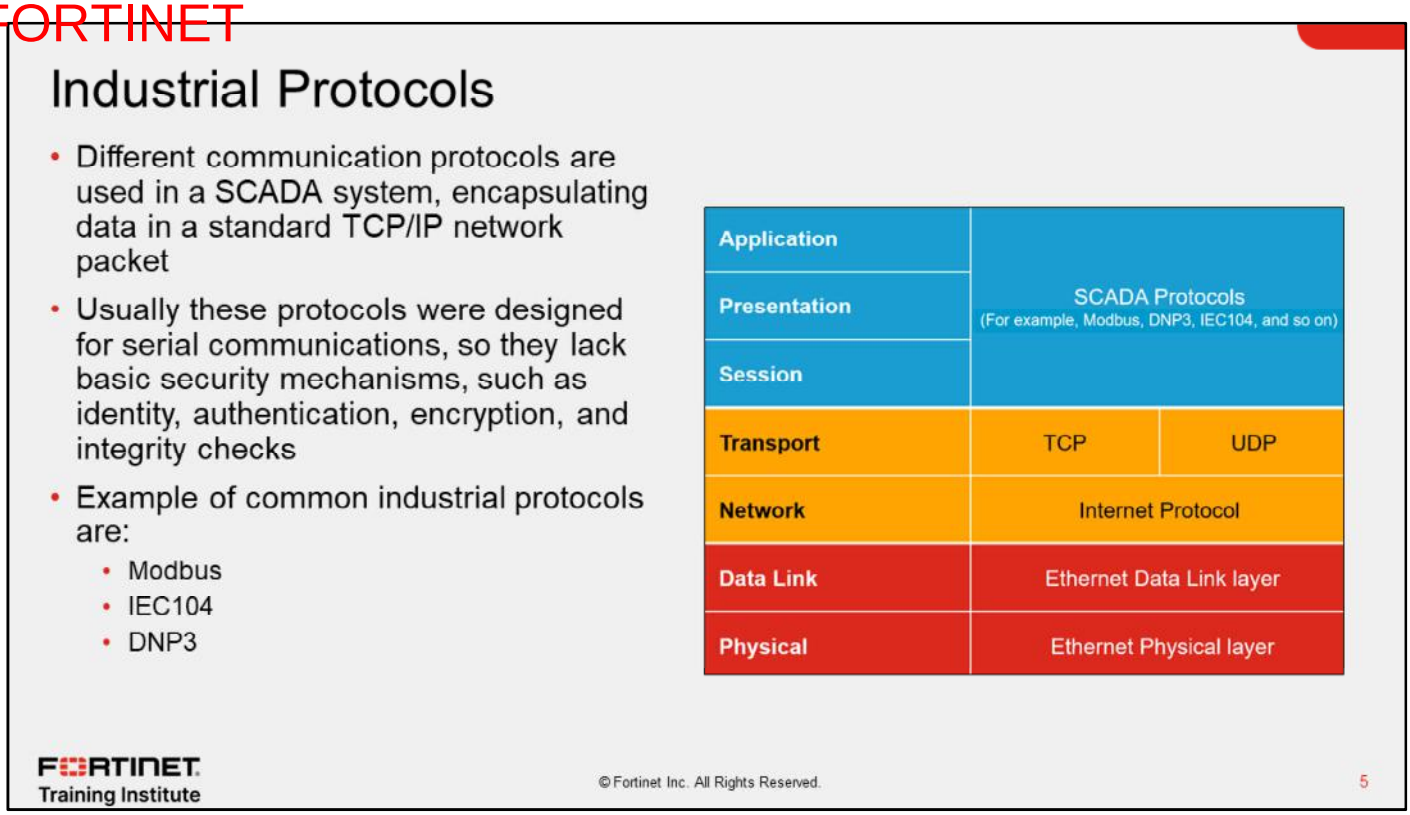
© Fortinet Inc. All Rights Reserved.

4

This slide shows typical Supervisory Control and Data Acquisition (SCADA) components, which include PLCs or RTUs.

PLCs or RTUs are low-performance computers built to control physical components, such as valves, pumps, and motors. They communicate using dedicated protocols that are prone to attacks.

DO NOT REPRINT
© FORTINET



Industrial communication protocols are used in a SCADA system, and data is encapsulated in standard TCP/IP packets.

Usually industrial protocols were designed for serial communications so they lack basic security mechanisms, such as identity, authentication, encryption, and integrity checks.

Some examples of industrial protocols are Modbus, DNP3, and IEC104. Newer versions of industrial protocols, such as EtherIP and POWERLINK, have some built-in security features.

DO NOT REPRINT
© FORTINET



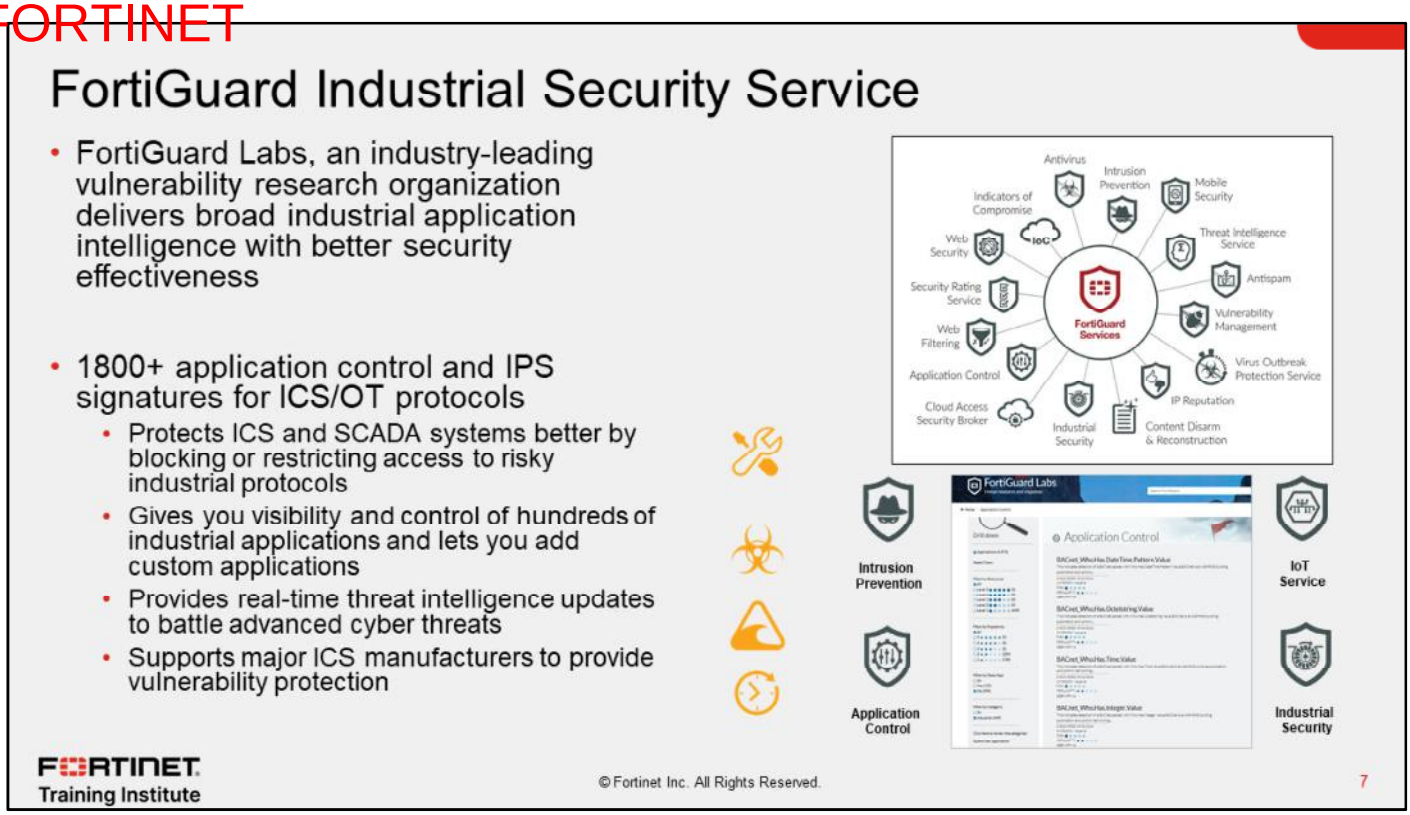
Industrial protocols do not include authentication of the data sent, so they are vulnerable to unauthorized connection or data modification throwing man-in-the-middle attacks.

Industrial protocols are ported from serial links to TCP/IP, therefore, most industrial protocols lack features like authentication, encryption, and TLS encryption, which makes them vulnerable to attacks.

FortiGate provides protection to vulnerable industrial protocols, using industrial signatures:
- IPS
- Application control
- Antivirus

FortiGuard maintains the updated industrial signatures and application vulnerabilities.

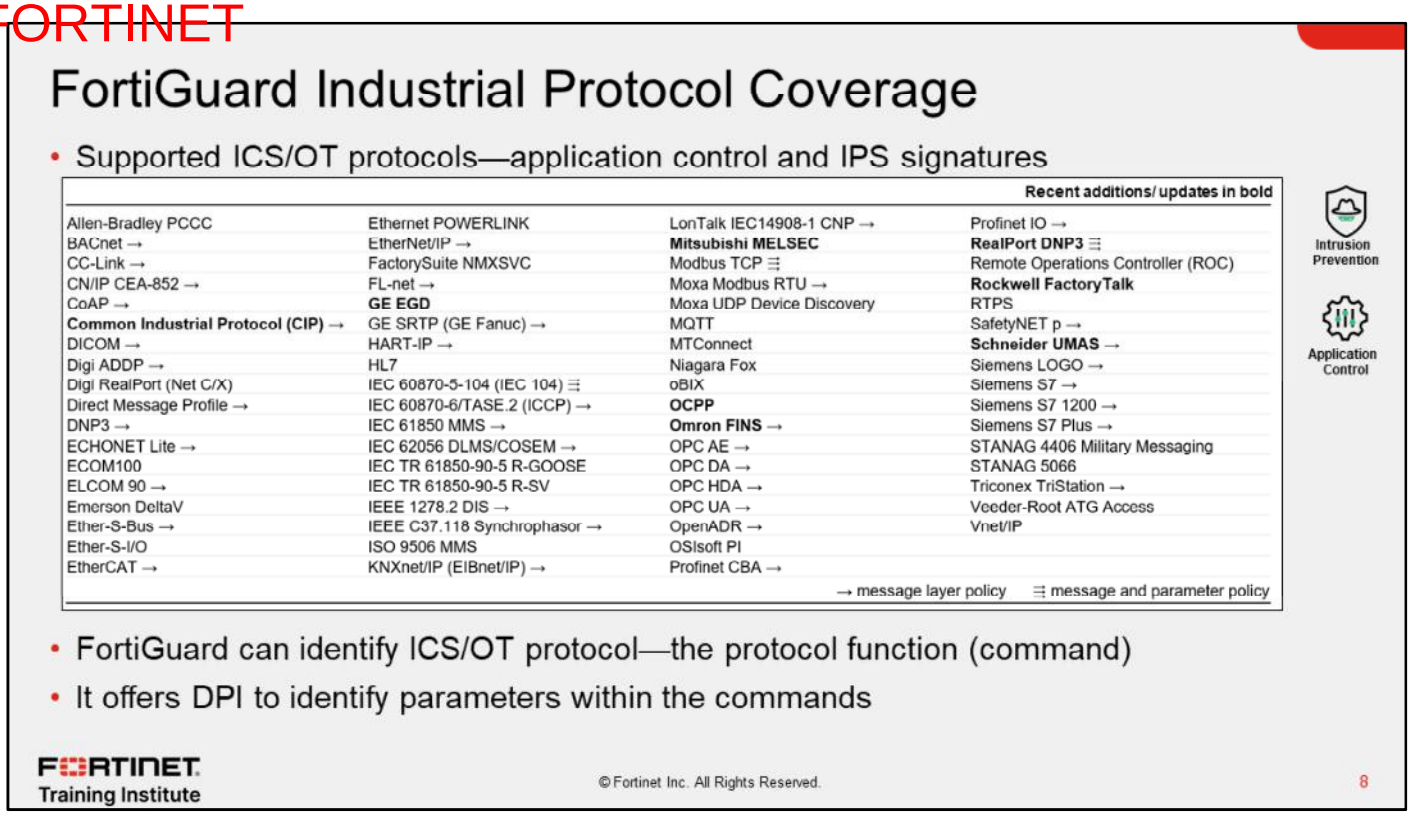
DO NOT REPRINT
© FORTINET



The intelligence delivered through the industrial security service comes from the global FortiGuard labs development team. FortiGuard labs, an industry-leading vulnerability research organization delivers broad industrial application intelligence with better security effectiveness.

- FortiGuard Protects ICS and SCADA systems by blocking or restricting access to risky industrial protocols
- It also gives you visibility and control of hundreds of industrial applications, and lets you add custom applications
- FortiGuard real-time threat intelligence updates protect against advanced cyber threats, and support major ICS manufacturers to provide vulnerability protection

DO NOT REPRINT
© FORTINET



This slide shows the industrial protocols and applications supported by FortiGuard.

FortiGuard is capable of identifying base ICS/OT protocols and protocol function codes like read-write function codes, and control codes, such as cause of transmission codes.

It is also capable of deep packet inspection (DPI), which identifies parameters within the commands, for example, values (discrete for specific function codes), memory addresses, and object types, to provide granular control over the ICS protocol payload.

DO NOT REPRINT
© FORTINET

FortiGuard Industrial Service



FORTINET Training Institute

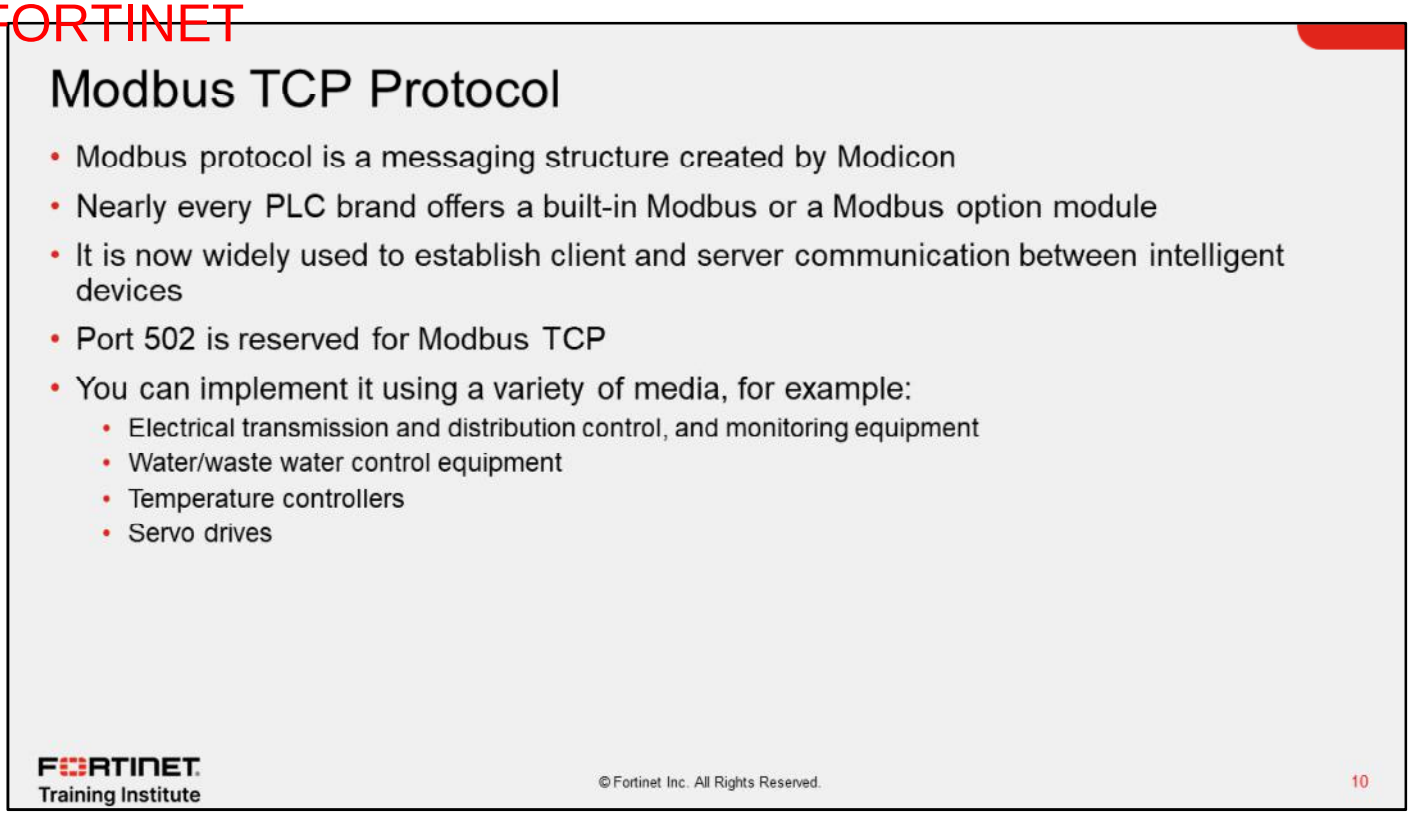
© Fortinet Inc. All Rights Reserved.

9

FortiGuard Industrial Service is bundled with the Enterprise subscription for ICS/OT customers.

You can also add it as a separate service—to add advanced threat protection (ATP) or unified threat protection (UTP) bundles.

DO NOT REPRINT
© FORTINET



Modbus is a data communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its PLCs. Modbus has become a default standard communication protocol and is now a commonly available means of connecting industrial electronic devices.

Modbus TCP/IP, also known as Modbus TCP, is simply the Modbus RTU protocol with a TCP interface that runs on Ethernet. The Modbus messaging structure is the application protocol that defines the rules for organizing and interpreting the data independent of the data transmission medium.

Modbus supports communication to and from multiple devices connected to the same cable or Ethernet network, for example, a device that measures temperature and a different device that measures humidity, both of which communicate the measurements to a computer.

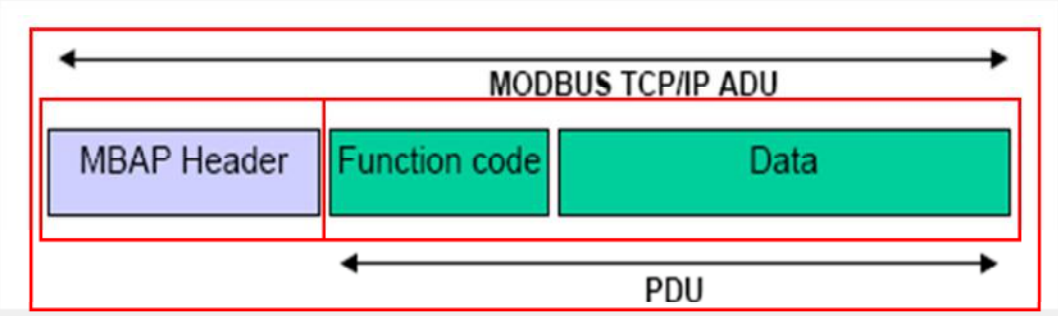
Modbus is often used to connect a system supervisory computer with an RTU in SCADA) systems in the electric power industry. Many of the data types are named for industrial control of factory devices, such as ladder logic, because of their use in driving relays. A single physical output is called a coil, and a single physical input is called a discrete input or contact.

You can access Modbus at the reserved system port 502 on the TCP/IP stack. Modbus is a request and reply protocol and offers services specified by function codes. Modbus function codes are elements of Modbus request and reply packet data units (PDUs).

DO NOT REPRINT
© FORTINET

Modbus TCP Frame Format

- Modbus Application Protocol (MBAP) header is for Modbus application with seven extra bytes at the beginning of the transmission
- MBAP packet is put into a TCP/IP wrapper
- No additional inherent security measures
- PDU (function code and data) of Modbus TCP is similar to Modbus RTU



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

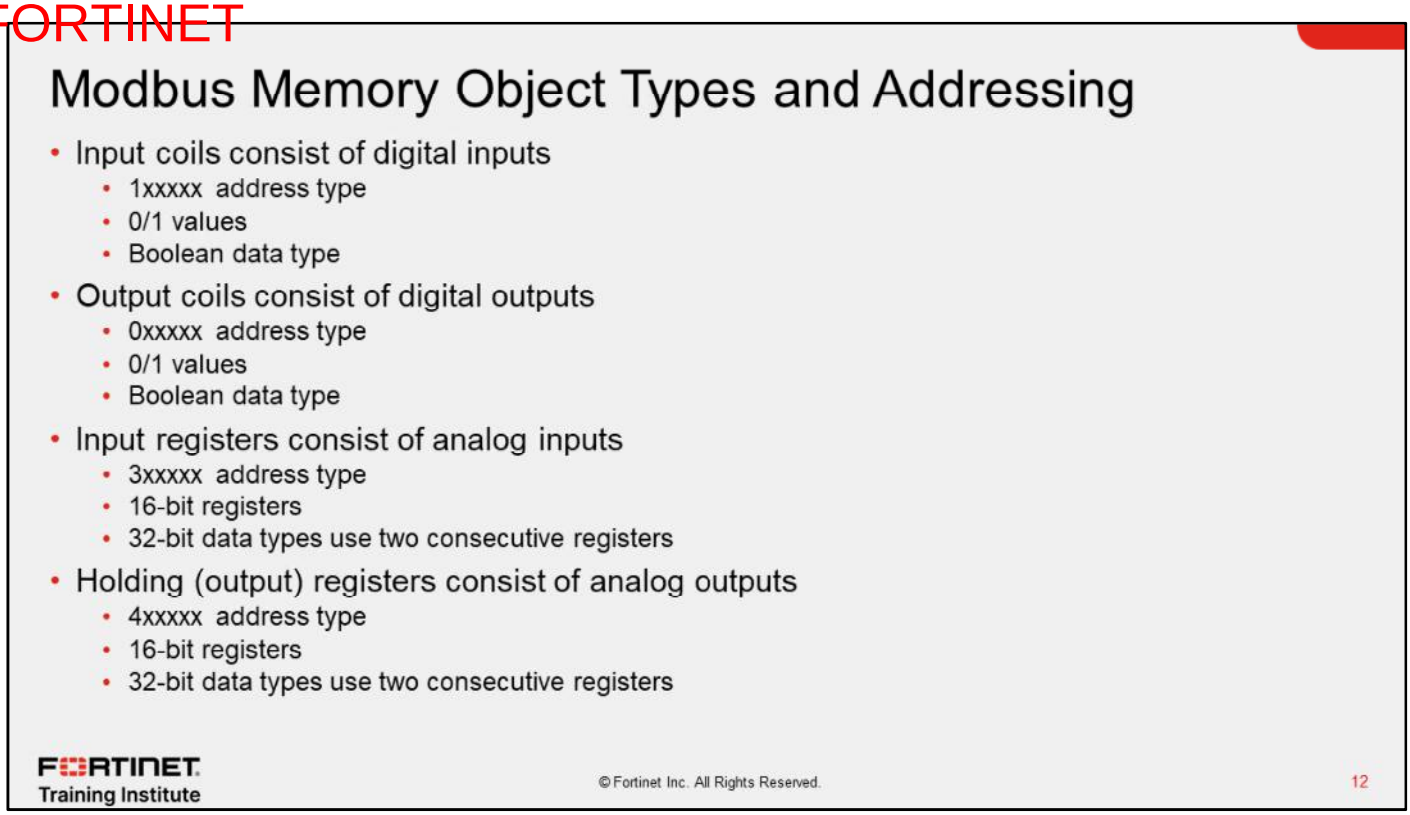
A dedicated header is used on TCP/IP to identify the Modbus Application Data Unit (ADU). It is called the MBAP header. This header provides some differences compared to the Modbus RTU ADU used on the serial line. The MBAP header is inserted with seven extra bytes at the beginning of the transmission.

A Modbus packet consists of an ADU, which encapsulates a PDU. An ADU consists of a PDU, whereas, a PDU consists of function code and data.

Modbus is a request and reply protocol and offers services specified by function codes.

Modbus function codes are elements of Modbus request and reply PDUs.

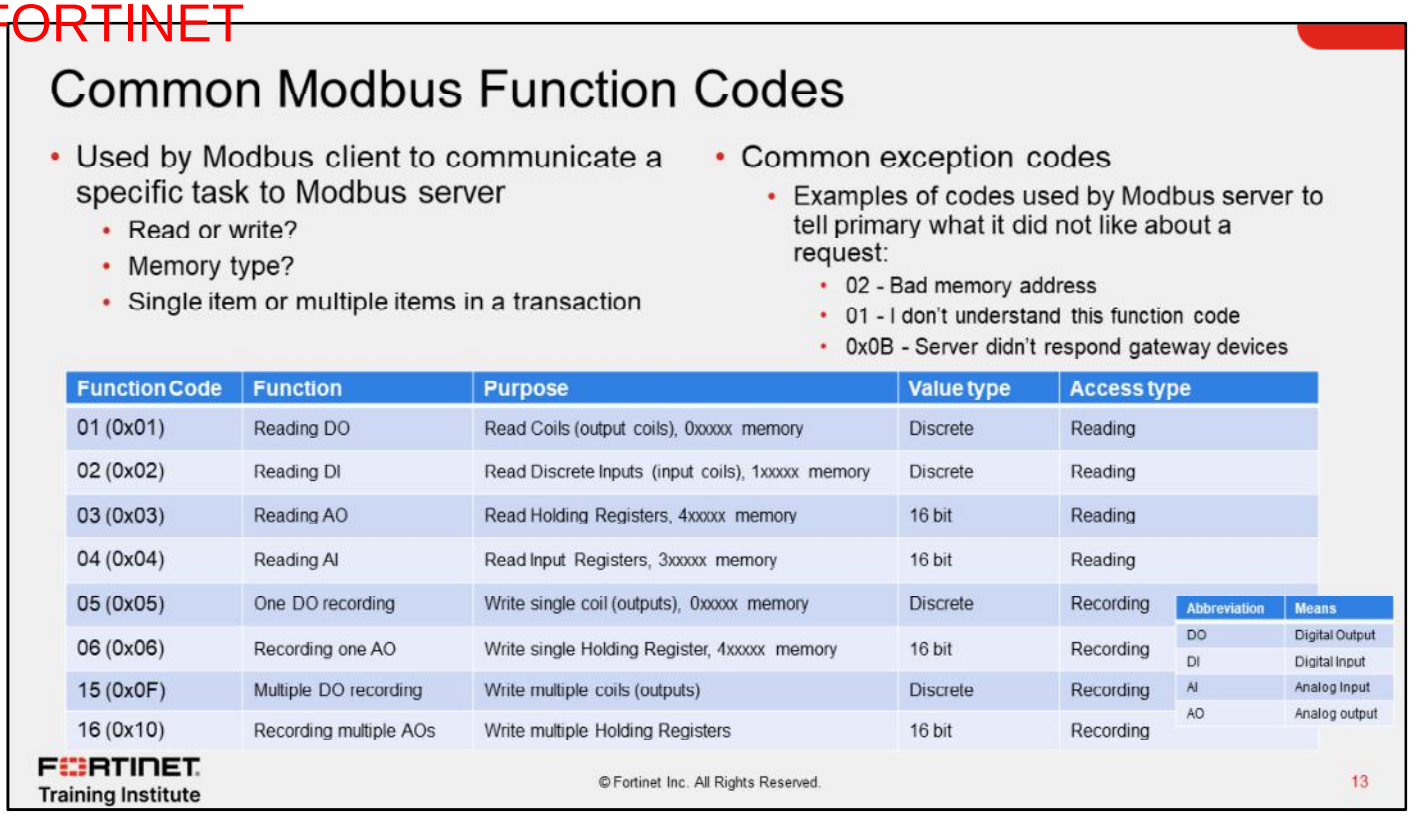
DO NOT REPRINT
© FORTINET



Modbus commands can instruct a Modbus device to change the values in one of its registers, which are written to coil and holding registers. Commands are used to read an input/output port, read data from coil ports, and command the device to send back one or more values contained in its coil and holding registers.

A Modbus command contains the Modbus address of the device it is intended for, for example, 1 to 247. Only the addressed device will respond and act on the command, even though other devices might receive the command.

DO NOT REPRINT
© FORTINET



Common Modbus Function Codes

- Used by Modbus client to communicate a specific task to Modbus server
  - Read or write?
  - Memory type?
  - Single item or multiple items in a transaction
- Common exception codes
  - Examples of codes used by Modbus server to tell primary what it did not like about a request:
    - 02 - Bad memory address
    - 01 - I don't understand this function code
    - 0x0B - Server didn't respond gateway devices

Function Code	Function	Purpose	Value type	Access type
01 (0x01)	Reading DO	Read Coils (output coils), 0xxxxx memory	Discrete	Reading
02 (0x02)	Reading DI	Read Discrete Inputs (input coils), 1xxxxx memory	Discrete	Reading
03 (0x03)	Reading AO	Read Holding Registers, 4xxxxx memory	16 bit	Reading
04 (0x04)	Reading AI	Read Input Registers, 3xxxxx memory	16 bit	Reading
05 (0x05)	One DO recording	Write single coil (outputs), 0xxxxx memory	Discrete	Recording
06 (0x06)	Recording one AO	Write single Holding Register, 4xxxxx memory	16 bit	Recording
15 (0x0F)	Multiple DO recording	Write multiple coils (outputs)	Discrete	Recording
16 (0x10)	Recording multiple AOs	Write multiple Holding Registers	16 bit	Recording

Abbreviation	Means
DO	Digital Output
DI	Digital Input
AI	Analog Input
AO	Analog output

FORTINET Training Institute

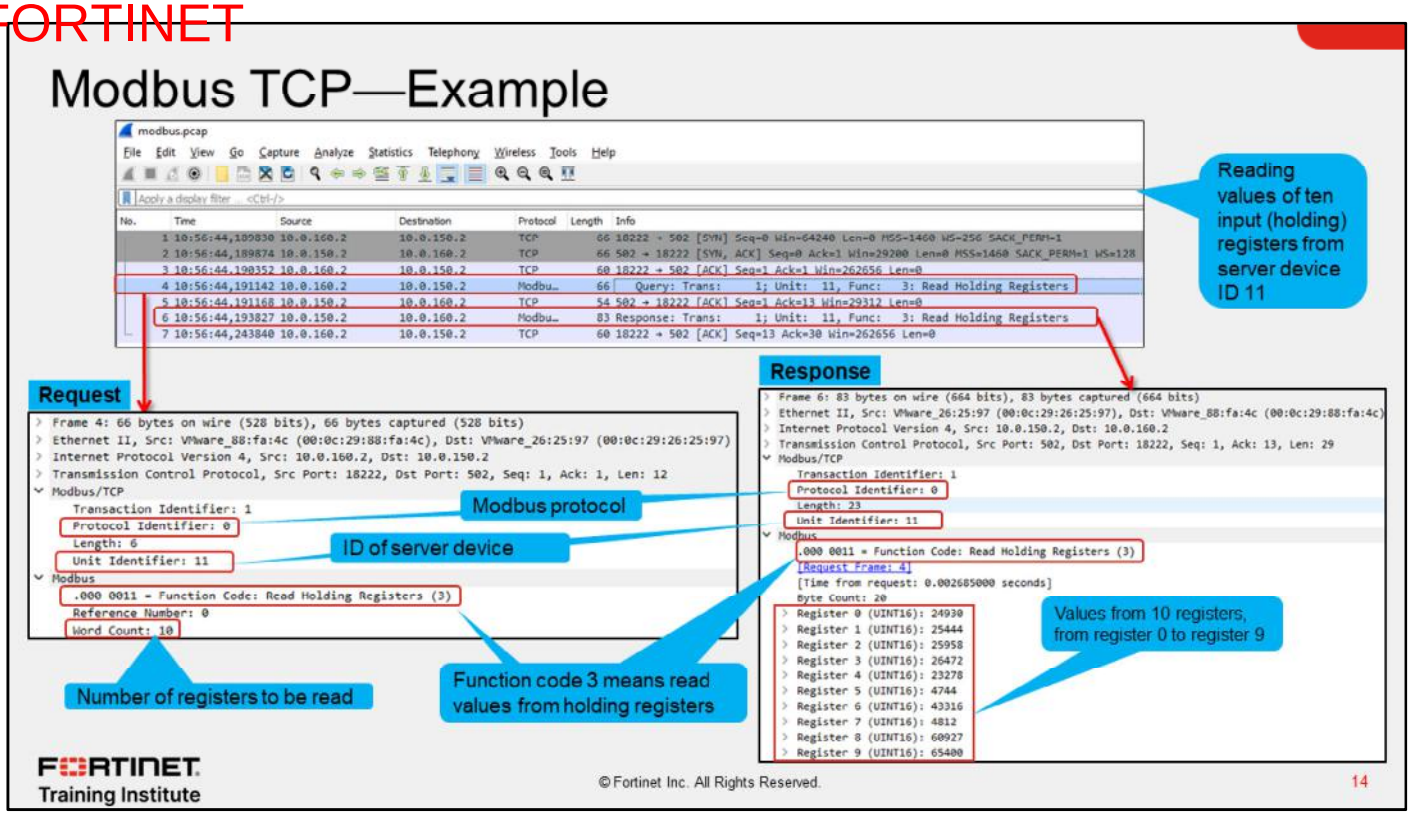
© Fortinet Inc. All Rights Reserved.

13

Function codes are used by the Modbus primary to communicate a specific task to the Modbus secondary, for example, read or write a specific memory type. A transaction can include a single item or multiple items.

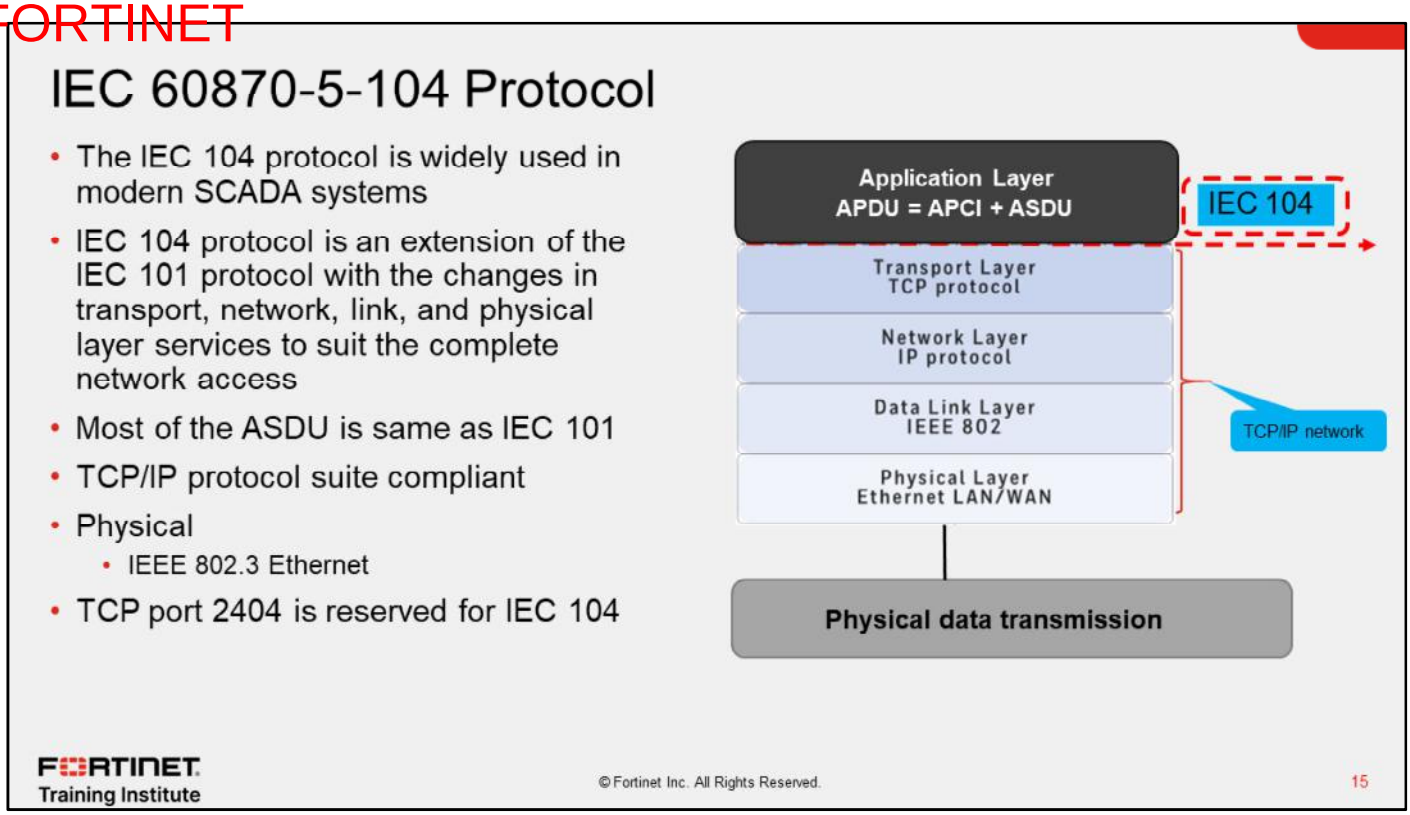
This slide shows a few common function and exception codes.

DO NOT REPRINT
© FORTINET



This slide shows an example of a Modbus TCP request and response while reading values of ten input (holding) registers from server device ID 11.

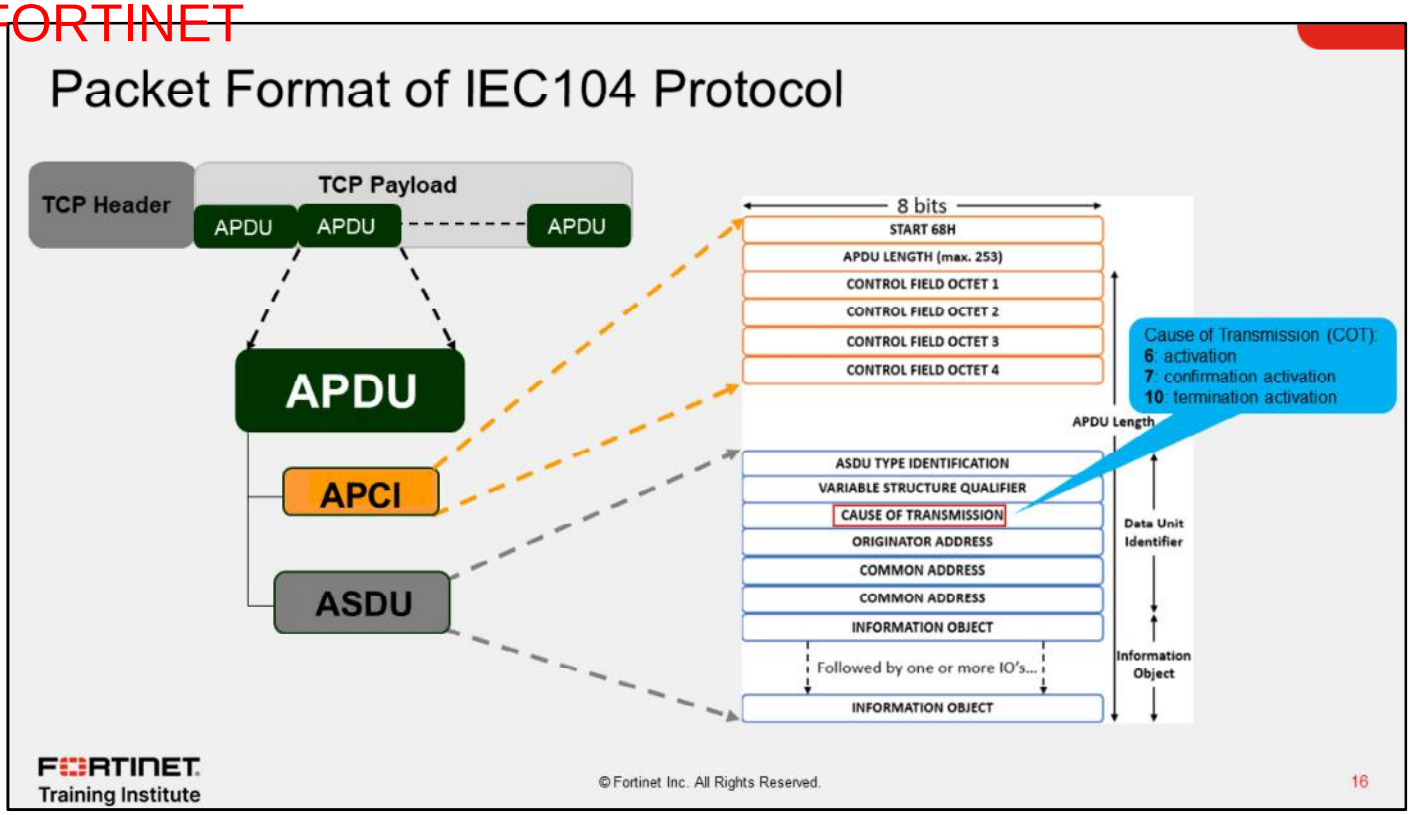
DO NOT REPRINT
© FORTINET



IEC 60870-5-104 (IEC 104) is a set of standards that define systems used for telecontrol SCADA in electrical engineering and power system automation applications. You can find this protocol from a remote station or substation to the control center, or inside a station or substation. The IEC 104 protocol is widely used in modern SCADA systems. It is an IP-compliant network protocol that is built on top of the previous serial communications standard IEC 101 to transport IEC 101 telecontrol messages over TCP using port 2404. IEC 104 encapsulates IEC 101 telecontrol messages into an Application Protocol Data Unit (APDU), which is transmitted as part of a TCP payload. Most of the Application Service Data Unit (ASDU) is same as of IEC 101.

The DNP3 protocol is similar to IEC 104. IEC 104 is used in Europe, and DNP3 is used in the USA. IEC 104 is mainly used in power plants. The biggest advantage of IEC 104 is that it enables communication through a standard network, which allows simultaneous data transmission between several devices and services.

DO NOT REPRINT
© FORTINET

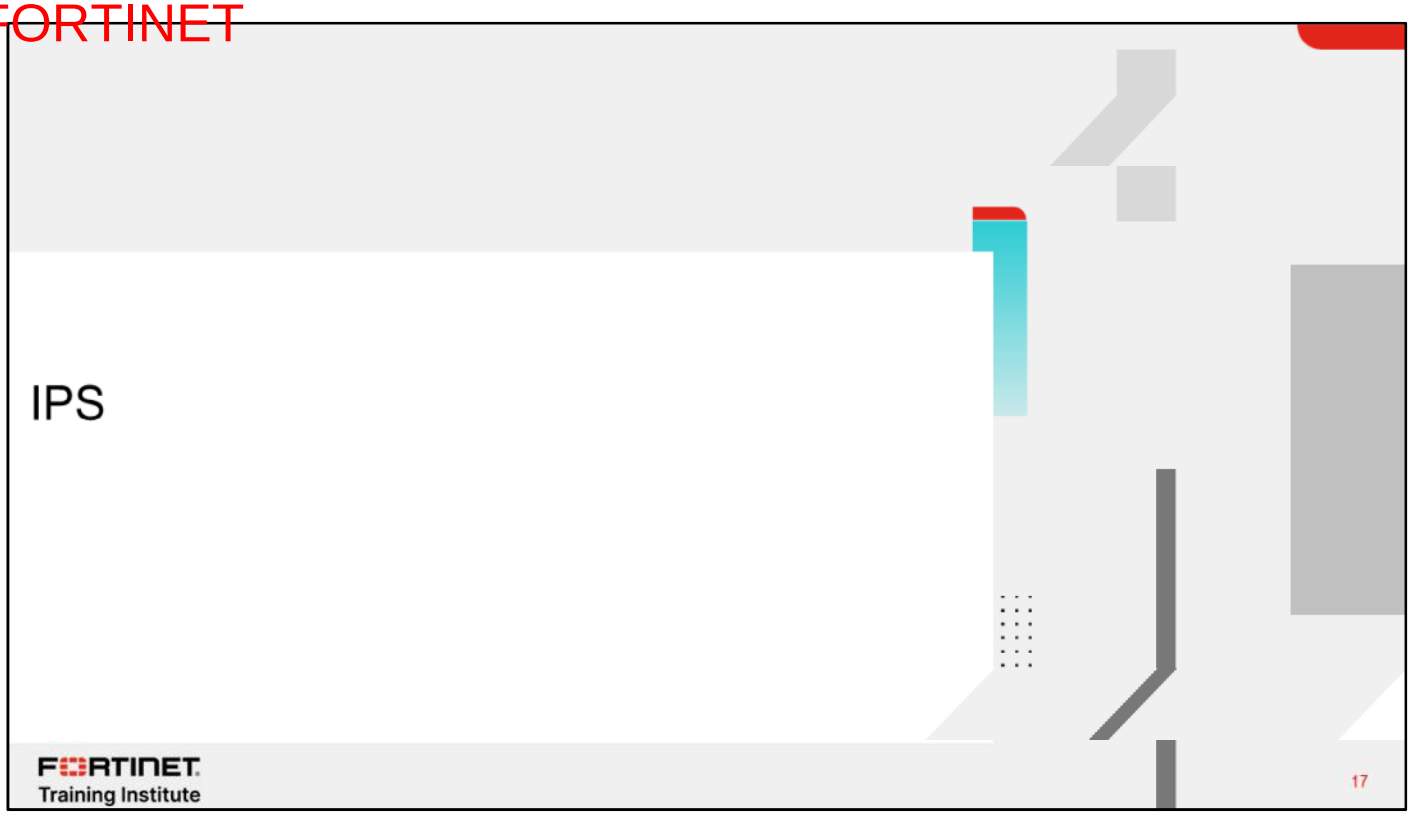


IEC 104 encapsulates IEC 101 telecontrol messages into an APDU, which is transmitted as part of a TCP payload. Each TCP payload can carry multiple APDUs up to the TCP maximum segment size (MSS).

APDU consist of two parts, APCI and ASDU:

- Application Protocol Control Information (APCI):
  - This part is the header with the protocol control information. Each APCI starts with a start byte with value 68H, followed by the 8-bit length of APDU, and four octets of control fields. The least significant two bits of the first control field octet determine the type of telecontrol message.
- Application Service Data Unit (ASDU):
  - The ASDU contains two main sections, the data unit identifier with the fixed length of six bytes, and the data itself, made up of one or more information objects. The data unit identifier defines the specific type of data, and provides addressing to identify the specific identity of the data, and includes additional information, such as COT. Each ASDU can transmit a maximum of 127 objects.

DO NOT REPRINT
© FORTINET



In this section, you will learn about intrusion detection and prevention for an operational technology environment.

DO NOT REPRINT
© FORTINET

Why Use IPS?

- Increased volume and sophistication of attacks on organizations
  - Driven by previously successful high-profile hacks and a highly profitable denied-market demand for stolen data
- More attacks against client and applications
  - Attacks are no longer targeted only at servers and server-based applications
- BYOD and remote workers increase risk of exposure



See attacks happening in real time around the world on the FortiGuard Labs live threat map.

FORTINET Training Institute

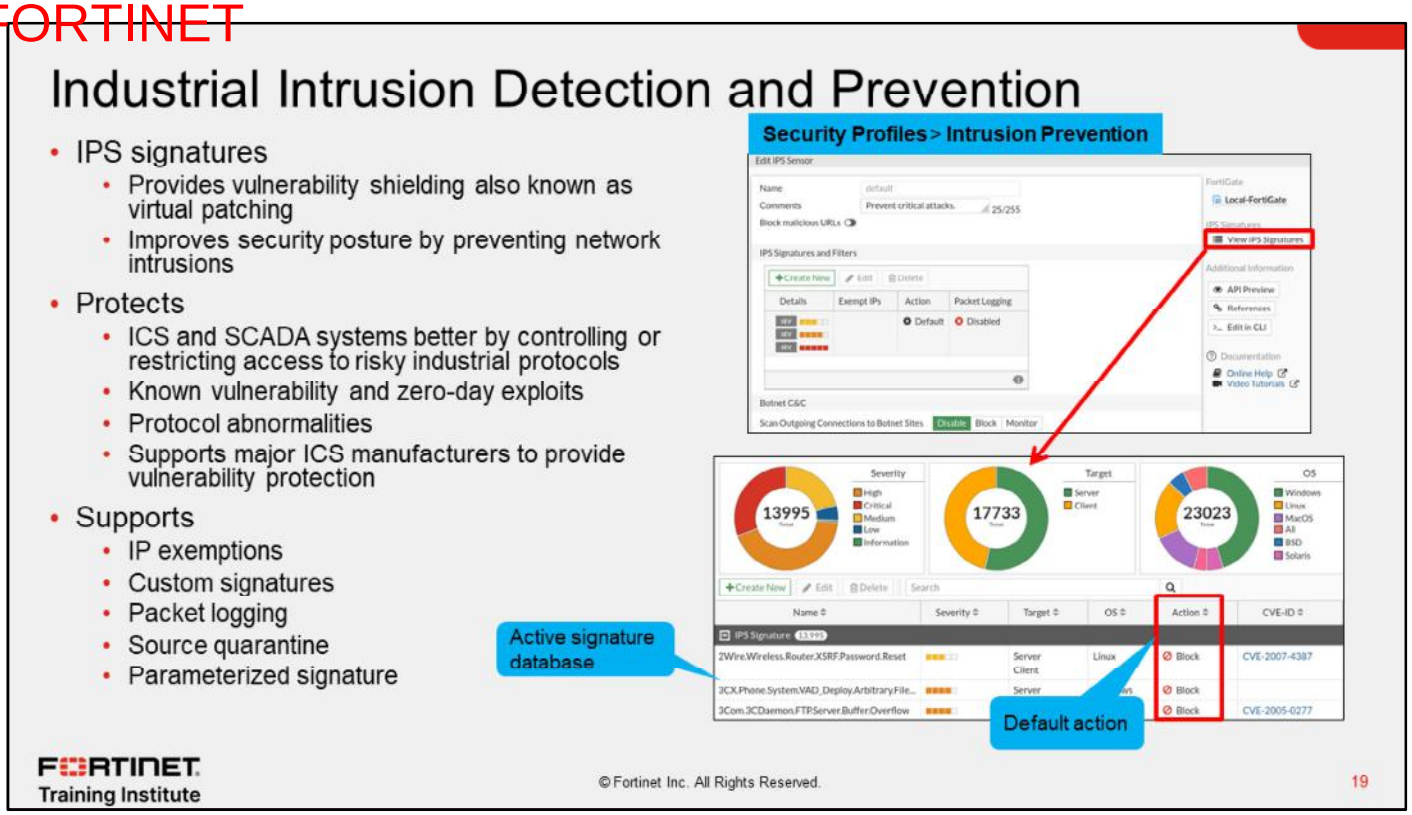
© Fortinet Inc. All Rights Reserved.

18

Organizations are under continuous attacks. Cybercriminals, motivated by previously successful high-profile hacks and a highly profitable denied market for stolen data, continue to increase both the volume and sophistication of their attacks on organizations. Many organizations encourage BYOD and flexible working environments, which has led to the explosion of any time, anywhere data consumption. This consumption increases the risk that sensitive data will be exposed to unauthorized access outside corporate boundaries.

Today’s threat landscape requires IPS to block a wider range of threats, while minimizing false positives.

DO NOT REPRINT
© FORTINET



IPS signatures provides vulnerability shielding, also known as virtual patching, and improves security posture by preventing network intrusions.

IPS protects ICS and SCADA systems better by controlling or restricting access to risky industrial protocols. It is aware of known vulnerabilities, zero-day exploits, and protocol abnormalities, and supports major ICS manufacturers to provide vulnerability protection.

IPS on FortiGate uses signature databases to detect known attacks. Protocol decoders can also detect network errors and protocol anomalies. The FortiGate flow engine has protocol dissectors to understand and expose the structure of various industrial protocols, such as Modbus, IEC 104, DNP3, OPC, and so on.

IPS supports:

- IP exemptions: You can exempt an IP address-specific host from a predefined signature. You can add IP exemptions to the IPS profile only if the signatures are mentioned explicitly.
- Custom signatures: If you can't find matching signatures, you can create custom signatures and add them to the IPS sensors.
- Supports packet logging: When you enable packet logging on a filter, FortiGate saves a copy of the packets that match any signatures included in the filter. You can analyze the packets later.
- Source quarantine: The quarantine is based on the attacker's IP address. Traffic from the attacker's IP address is refused until the expiration time from the trigger is reached.
- Parameterized signature: It supports a few of the ICS and OT protocols such as Modbus, IEC 104, and DNP3.

DO NOT REPRINT
© FORTINET

Choosing the Signature Database

- Regular
  - Common attacks with fast, certain identification (default action is block)
- Extended
  - Performance-intensive



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

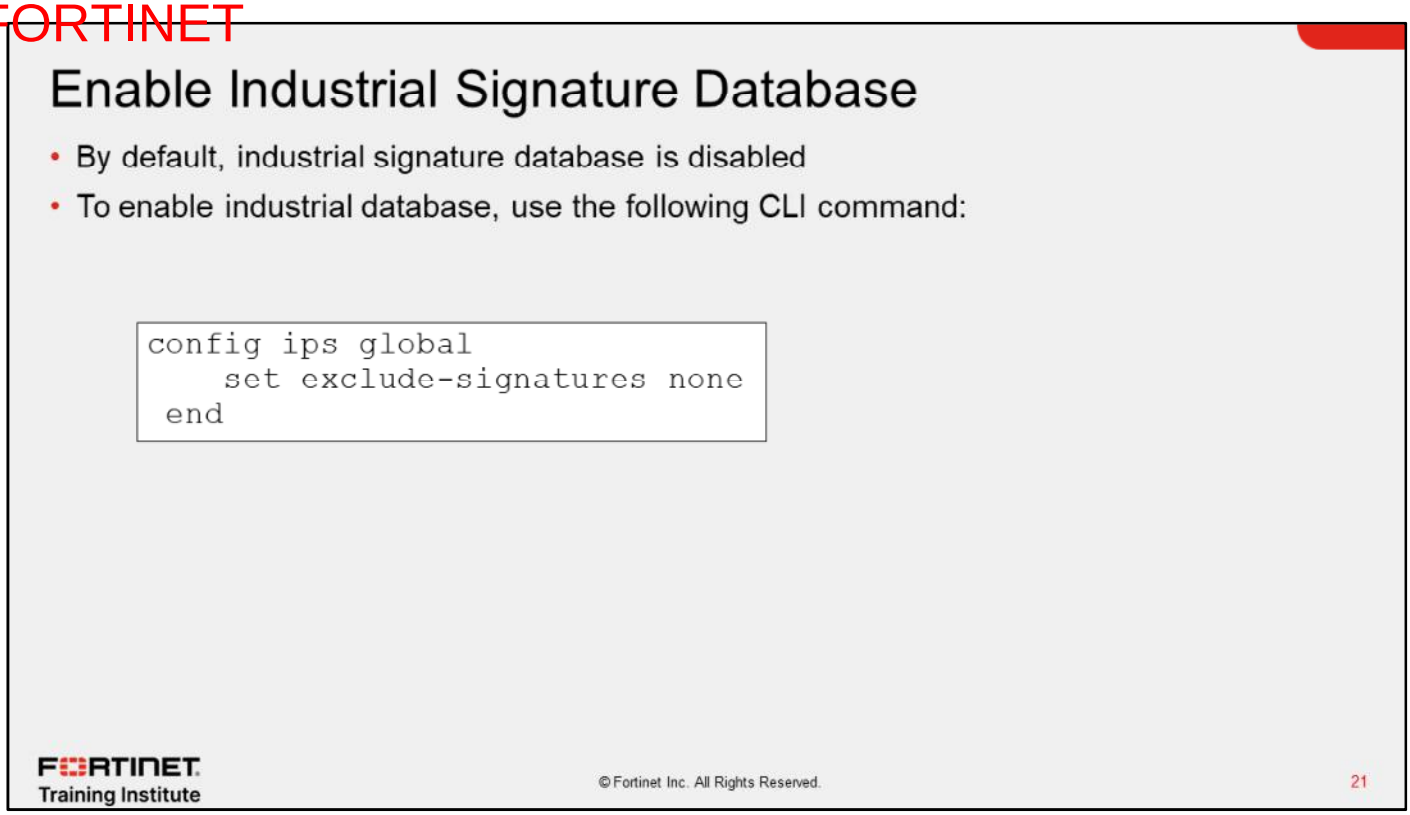
20

The IPS signature database is divided into the regular and extended databases. The regular signature database contains signatures for common attacks whose signatures cause rare or no false positives. It's a smaller database, and its default action is to block the detected attack.

The extended signature database contains additional signatures for attacks that cause a significant performance impact, or don't support blocking because of their nature. Also, because of its size, the extended database is not available for FortiGate models with a smaller disk or RAM.

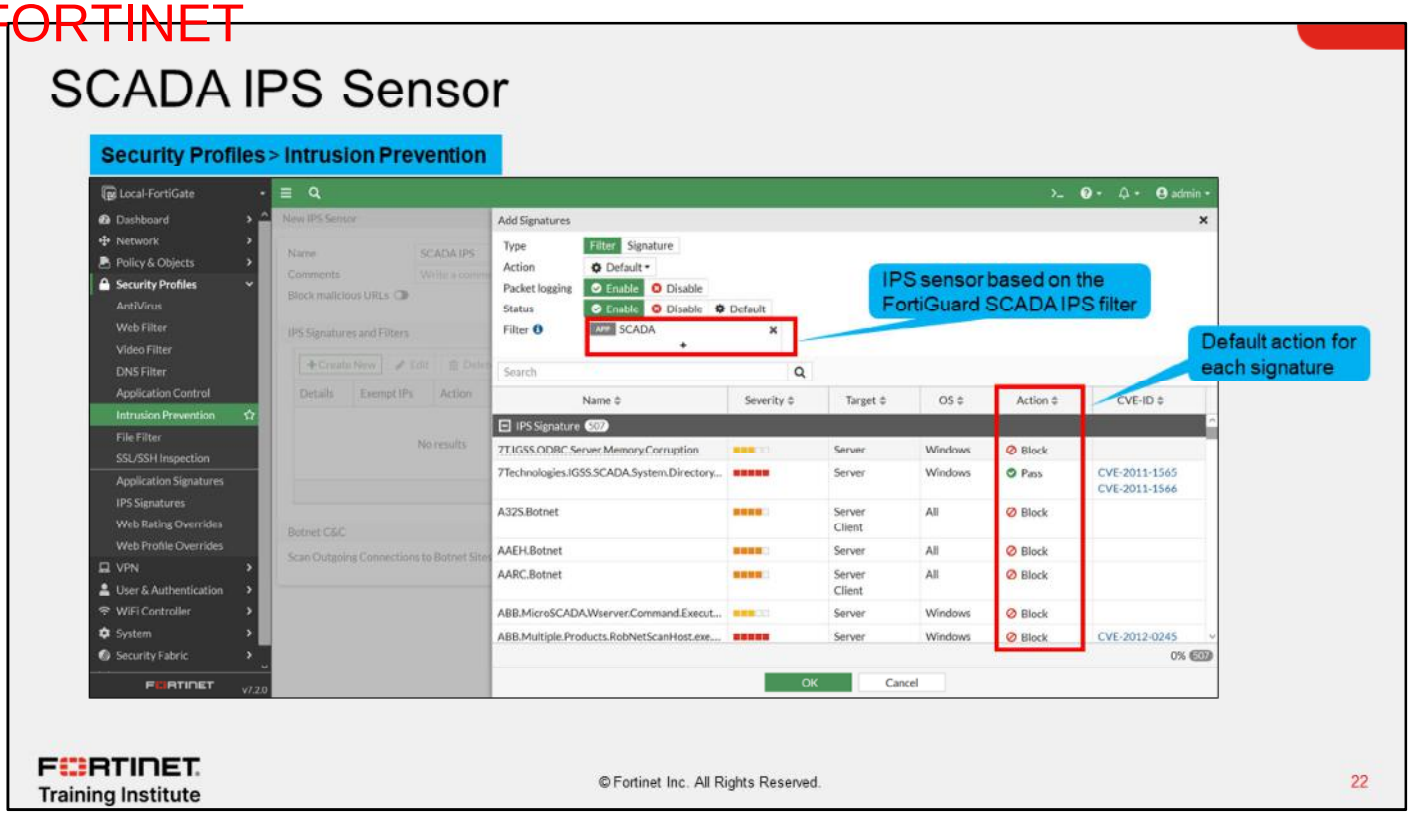
For high-security OT networks , you might be required to enable the extended signatures database.

DO NOT REPRINT
© FORTINET



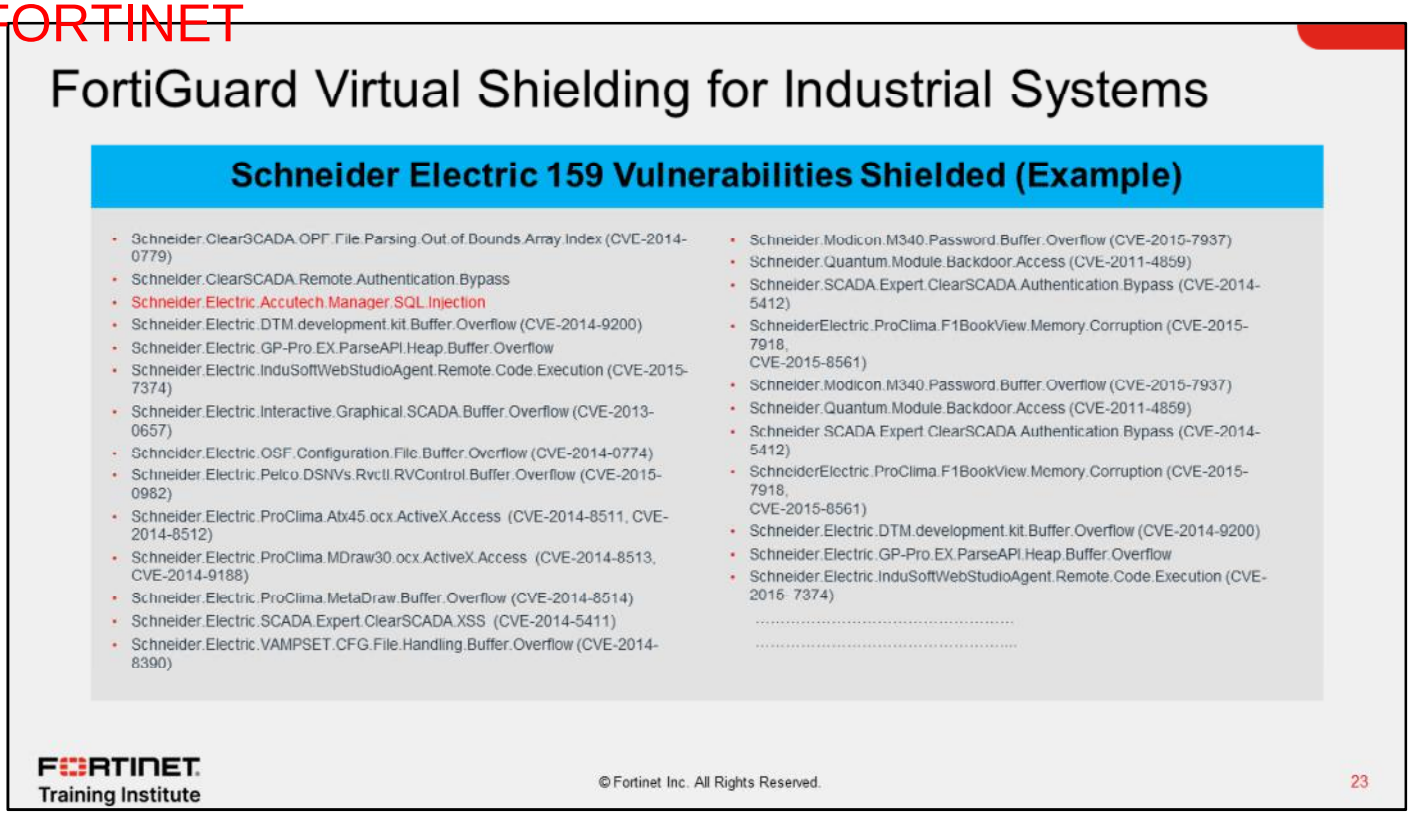
By default, the industrial database is disabled. To enable the industrial database, use the CLI command shown on this slide.

DO NOT REPRINT
© FORTINET



This slide shows an example of the IPS sensor based on the FortiGuard SCADA IPS filter. Each IPS signature has its own default action specified by the FortiGuard labs.

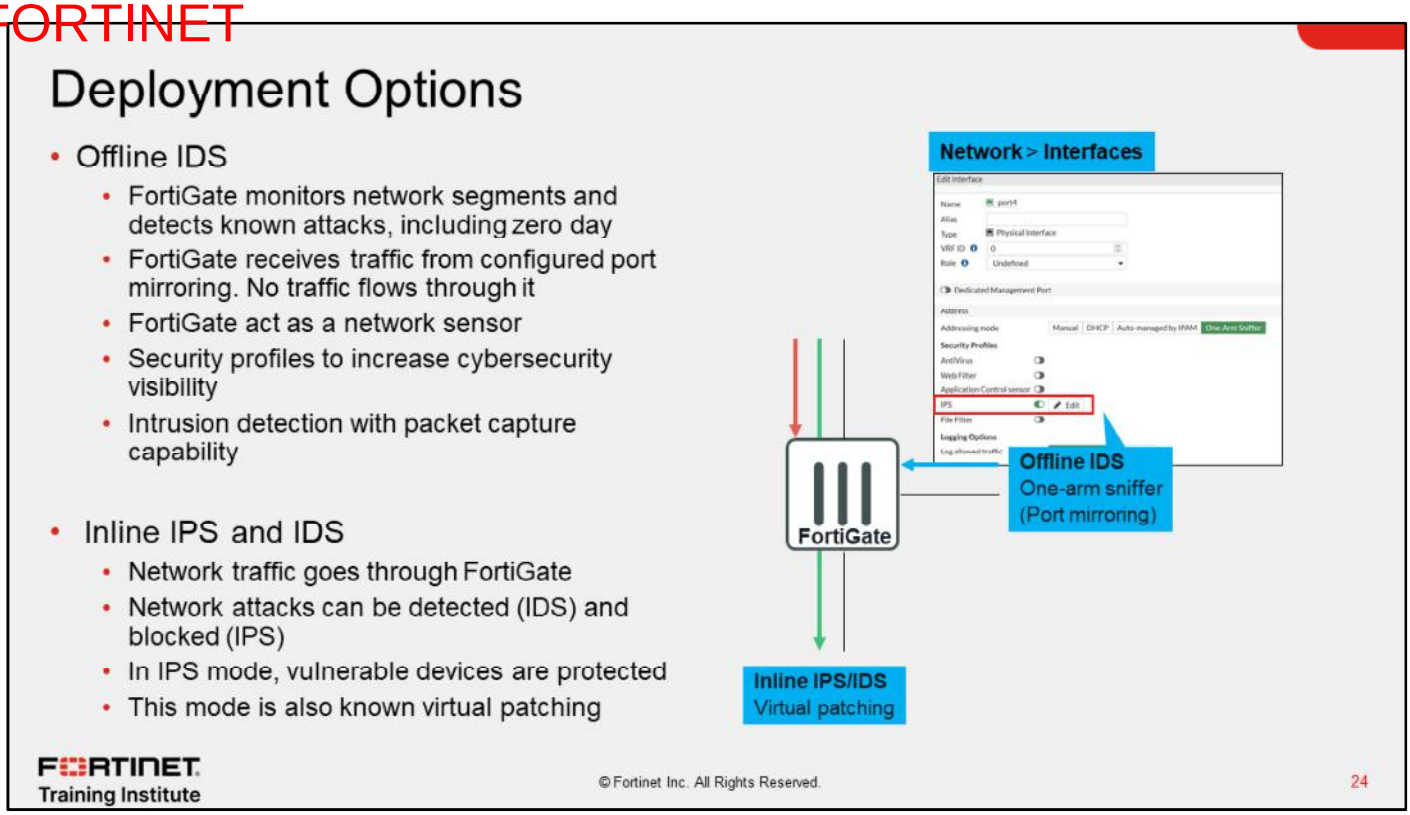
DO NOT REPRINT
© FORTINET



FortiGuard provides virtual shielding for industrial systems. Consider an example from Schneider Electric Accutech Manager. A vulnerability was found in the Schneider Electric Accutech Manager, which can be exploited by malicious users to conduct SQL injection attacks. Input passed through a specially crafted packet to port 2536 of the RF manager. Service is not correctly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. The vulnerability was reported for versions up to 2.00.4 of the Schneider Electric Accutech Manager.

This slide shows a few examples of known exploits for Schneider Electric covered by the FortiGate IPS feature.

DO NOT REPRINT
© FORTINET

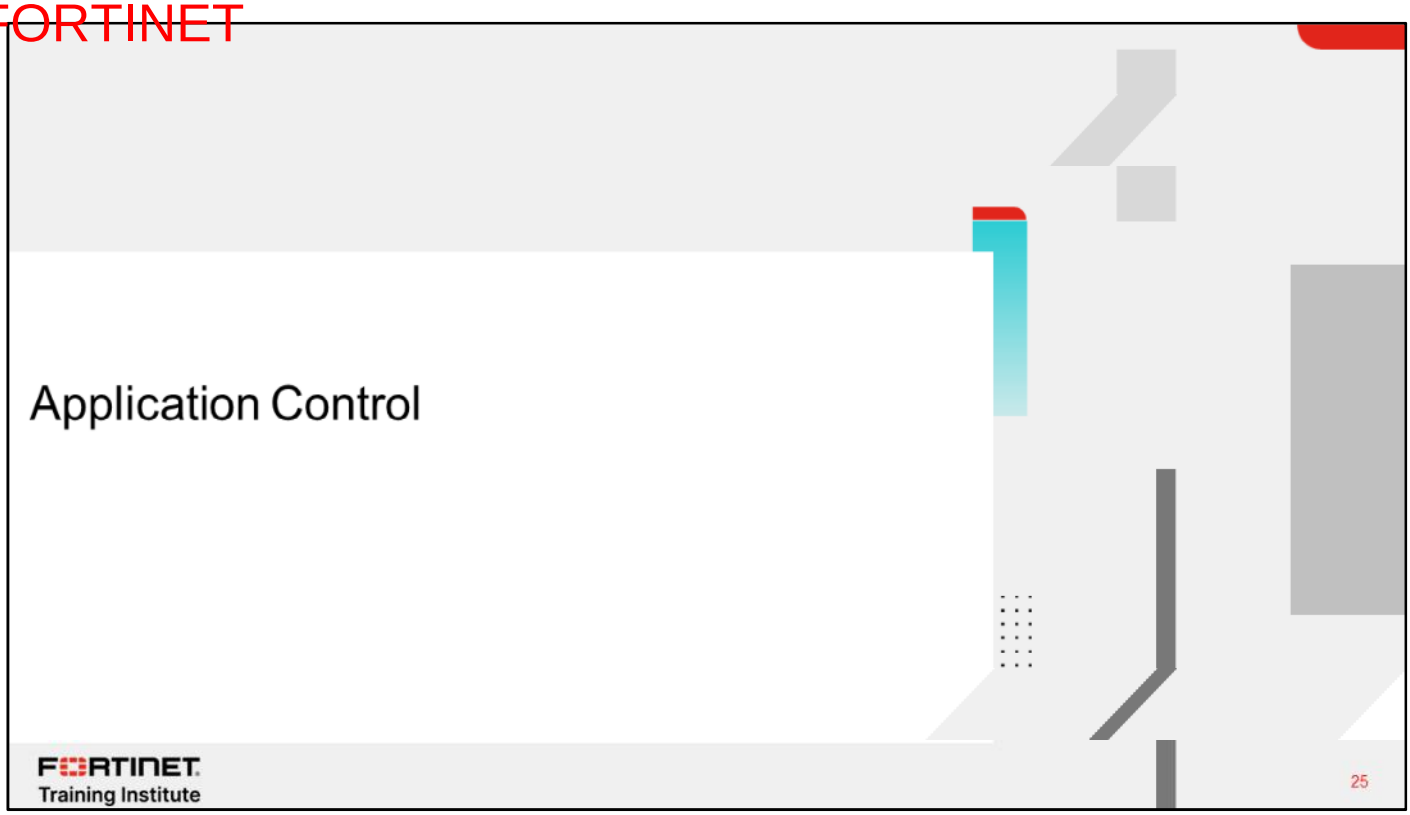


You can deploy FortiGate in two different modes:
- Offline IDS
- Inline IPS and IDS

If deployed in offline IDS
- FortiGate monitors network segments and detects known attacks, including zero day.
- FortiGate receives traffic from configured port mirroring. No traffic flows through it.
- FortiGate act as a network sensor.
- Security profiles increase cybersecurity visibility.
- Include intrusion detection with packet capture capability.

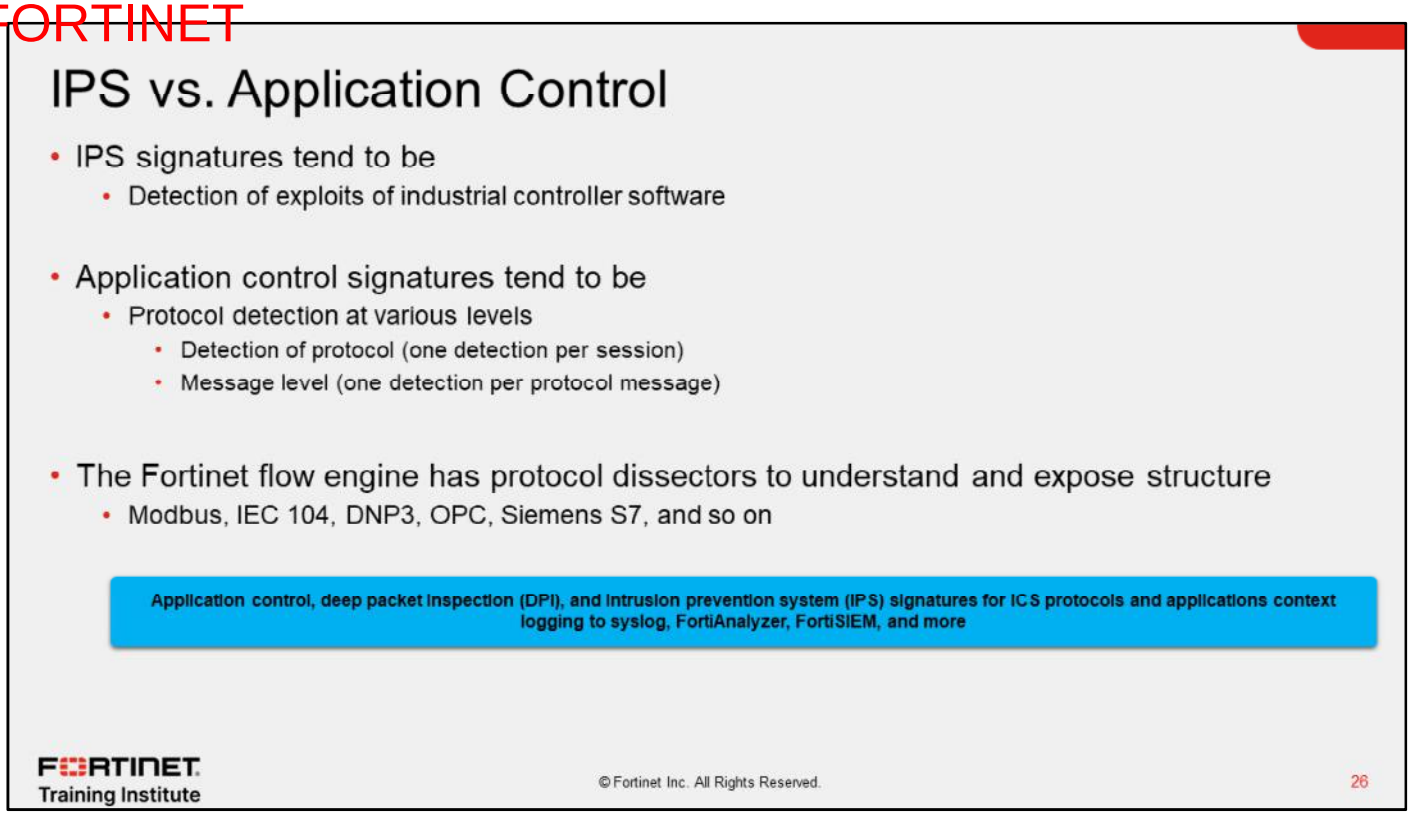
If deployed in inline IPS and IDS
- Network traffic goes through FortiGate.
- Network attacks can be detected (IDS) and blocked (IPS).
- In IPS mode, vulnerable devices are protected.
- This mode is also known as virtual patching.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the application control for an operational technology environment.

DO NOT REPRINT
© FORTINET



Generally, IPS signatures tend to be detection of exploits of industrial controller software, whereas application control signatures tend to be protocol detection at various levels.

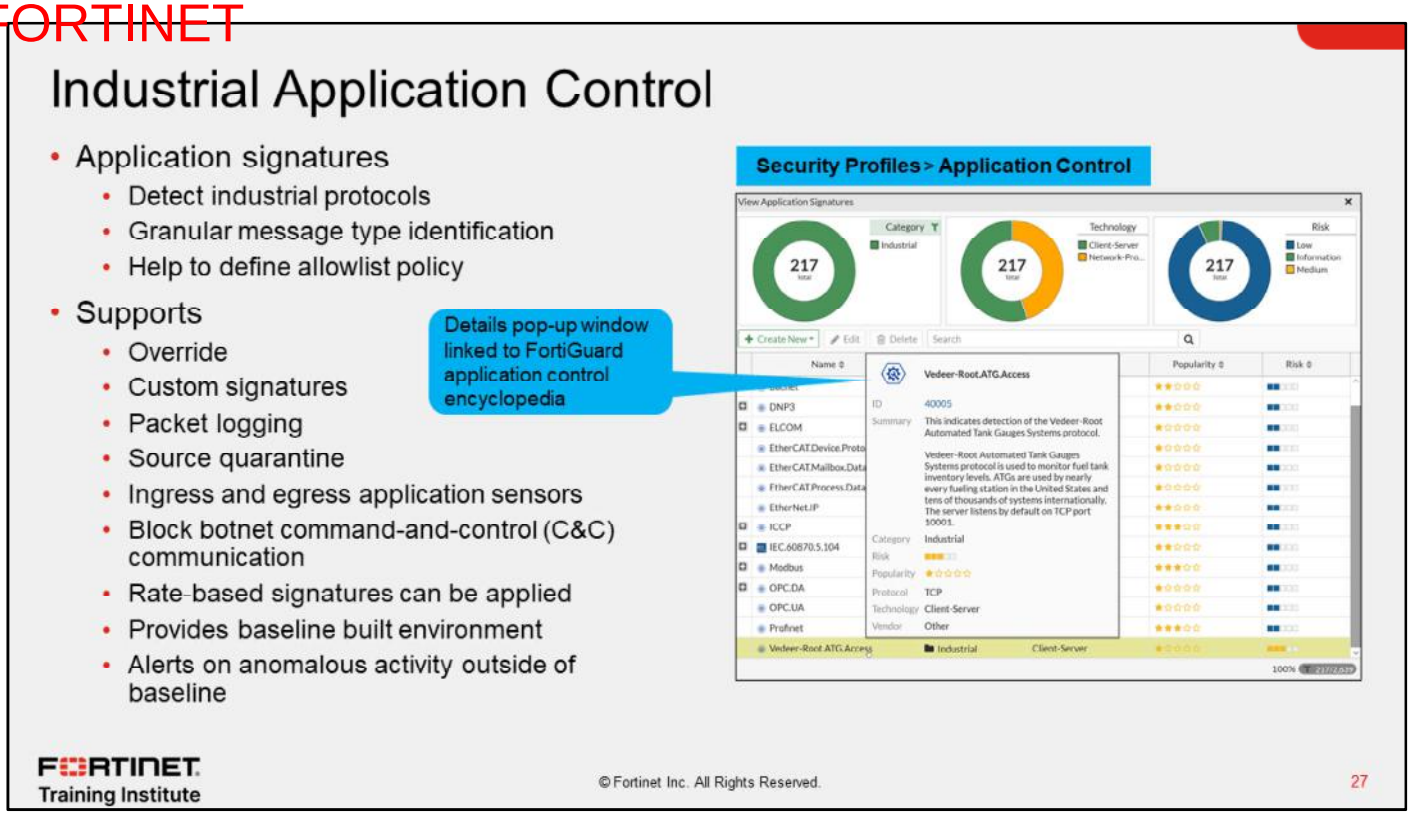
IPS detects the industrial software and software version-based vulnerabilities. As you learned earlier, several versions of Schneider Electric Accutech Manager were vulnerable to SQL injection attacks.

Application control detects the protocols used in the applications like Modbus IEC 104, and contents of the telecontrol messages, like function codes, object types, and so on.

The flow engine has protocol dissectors to understand and expose the structure of industrial protocols, for example Modbus, IEC 104, DNP3, OPC, Siemens S7, and so on.

Both IPS and application control send log and application context to syslog servers FortiAnalyzer, FortiSIEM, and so on.

DO NOT REPRINT
© FORTINET

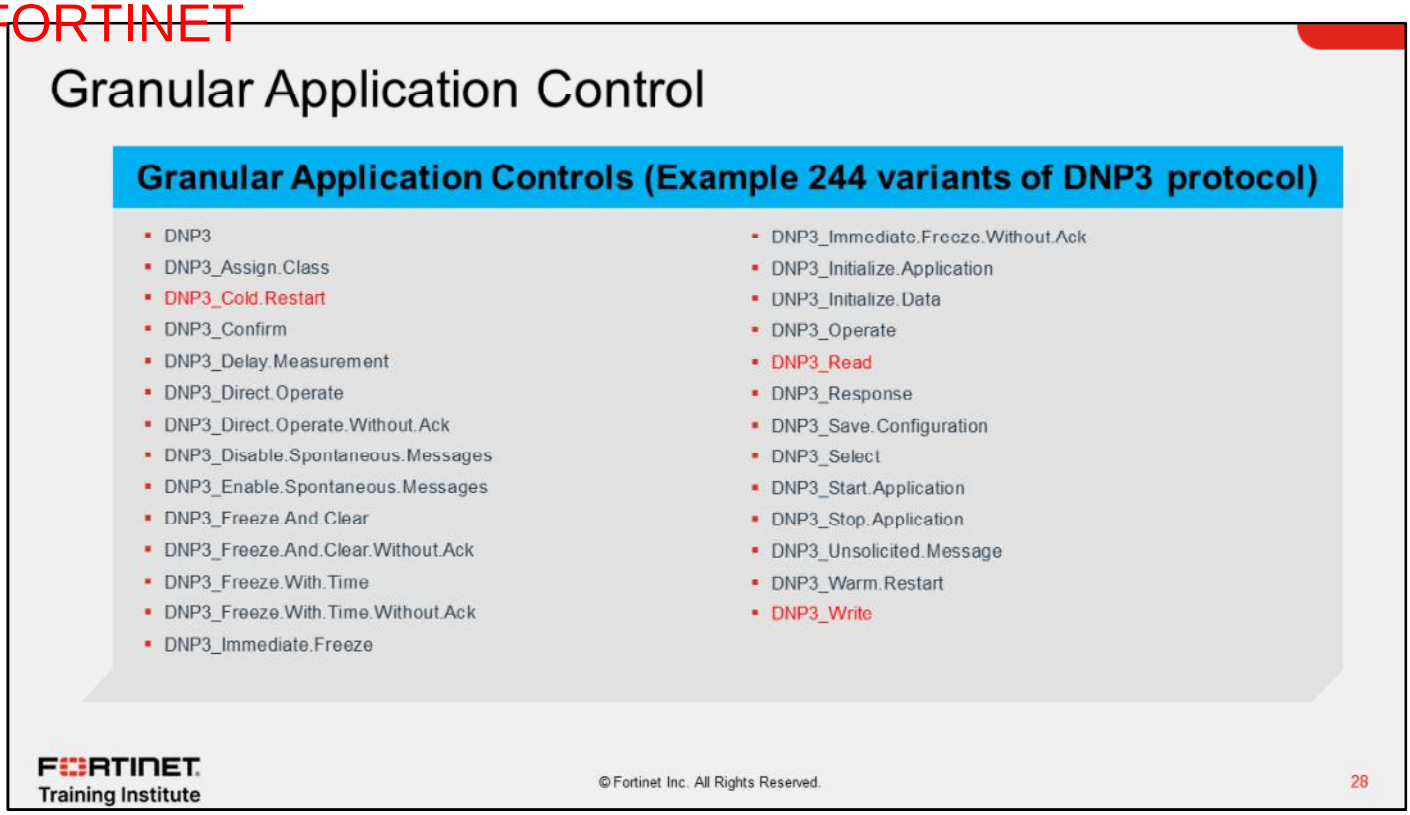


You can use application signatures to detect industrial protocols. Application signatures detect industrial protocols, perform granular message type identification, and help to define allowlist policy.

Application control feature supports:

- Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies, then the application control profile applies the action that you have configured for applications in your selected categories.
- Custom signatures: If you can't find matching signatures, you can create custom signatures and add them to the application control sensors.
- Packet logging: When you enable packet logging on a filter, FortiGate saves a copy of the packets that match any signatures included in the filter. The packets can be analyzed later.
- Source quarantine: The quarantine is based on the attacker's IP address, traffic from the attacker's IP address is refused until the expiration time from the trigger is reached.
- Ingress and egress application sensors for more granular application control.
- Block botnet C&C communication: You can set botnet C&C protection to block outgoing connections to botnet sites or just record log messages (monitor) when an outgoing botnet connection attempt is detected. The latest botnet database is available from FortiGuard.
- Can apply rate-based signatures: These are a subset of the signatures that are found in the database that are normally set to monitor. This group of signatures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, a little like DoS attacks.
- Application control also provides a baseline-built environment, and alerts on anomalous activity outside of the baseline.

DO NOT REPRINT
© FORTINET

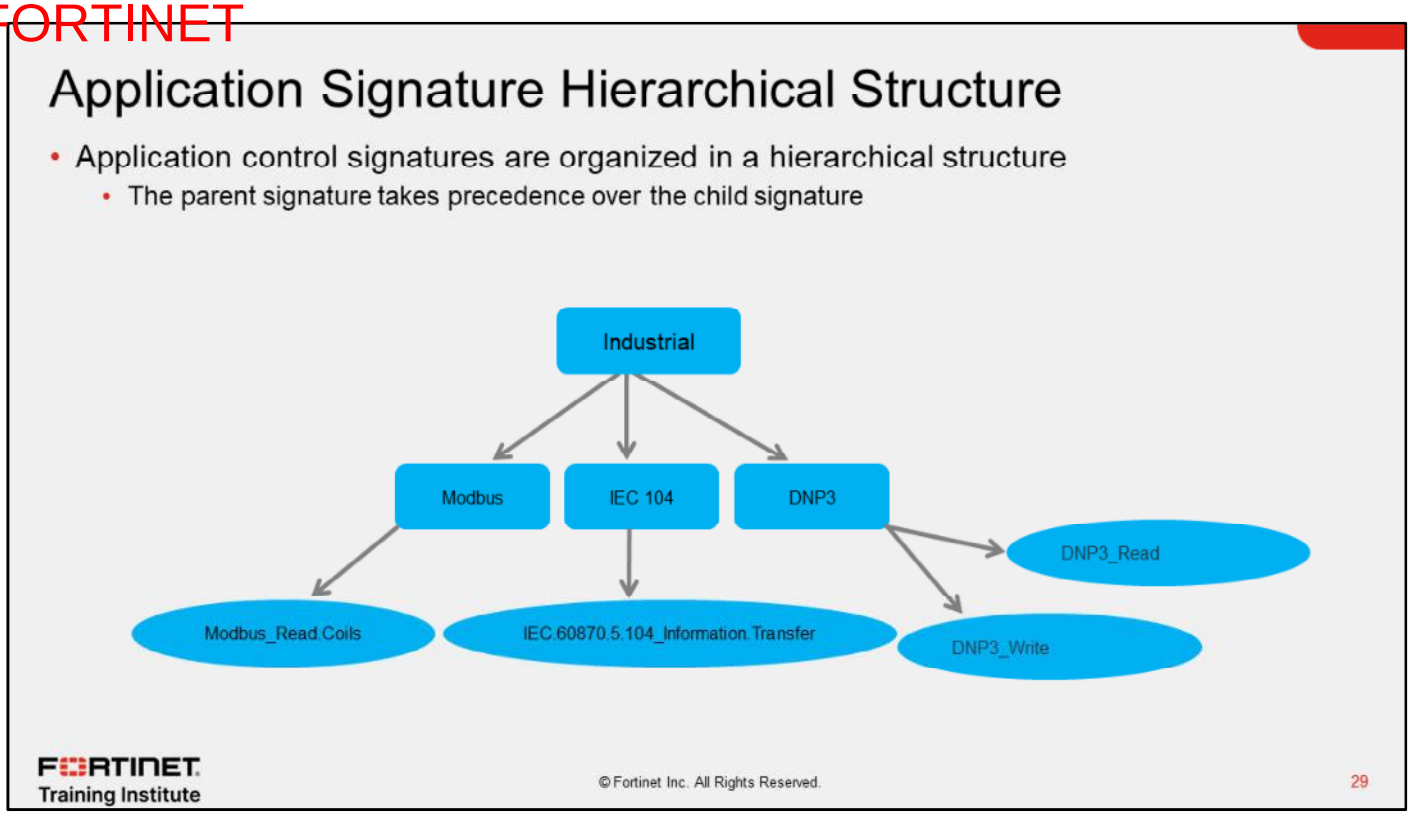


This slide shows some examples of granular application controls for the DNP3 protocol-based C&C functions.

Consider the example of the application DNP3_Cold.Restart. This indicates that a cold restart command was sent to a DNP3 device by an authorized DNP3 client. This will cause the device to restart and execute power up self-tests. The device will be unavailable for a time, and a malicious attacker can continuously send this command and cause a denial of service (DoS) condition.

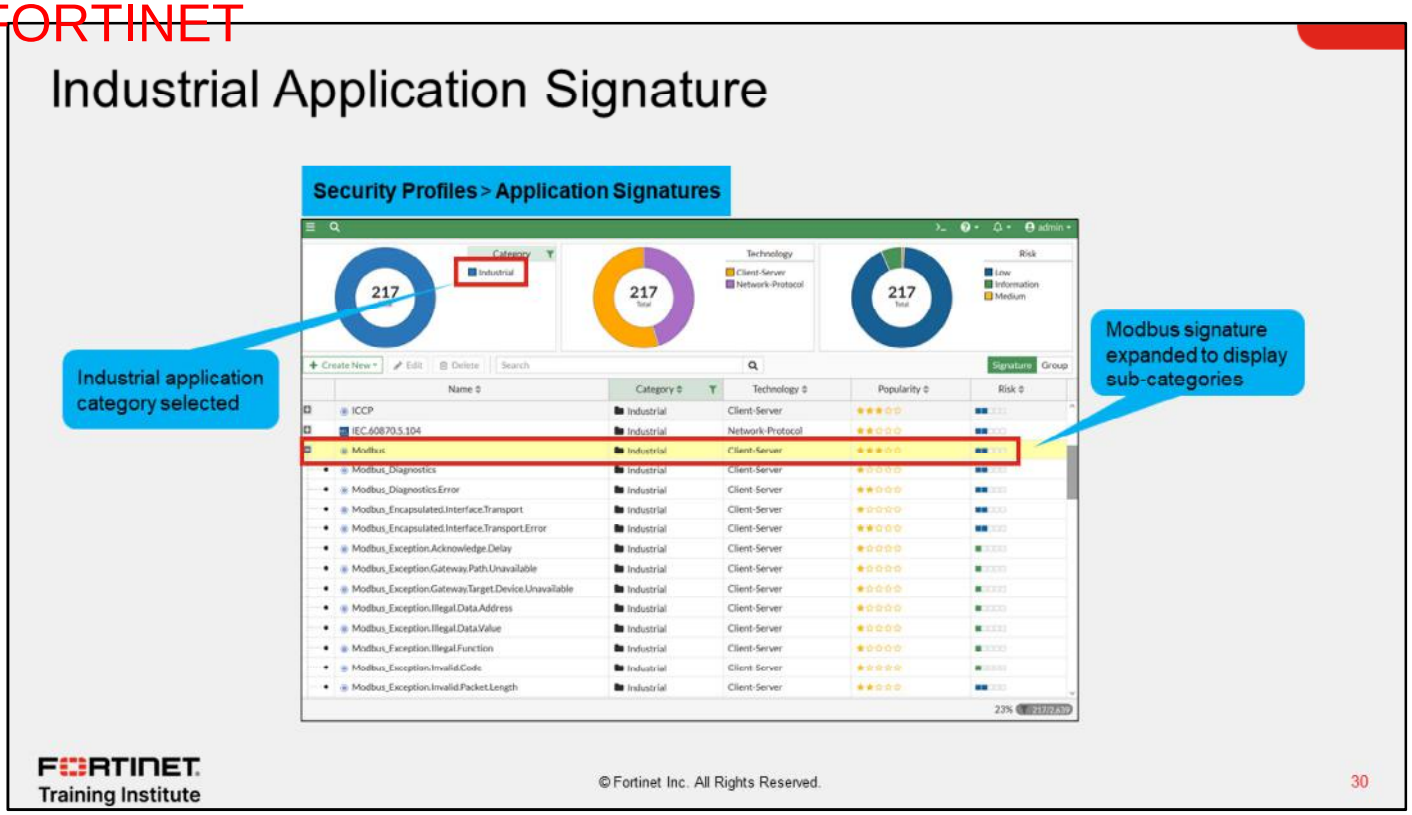
Similarly, application DNP3_Read indicates detection of the DNP3 read command, and DNP3_Write indicates the detection of the DNP3 write command.

DO NOT REPRINT
© FORTINET



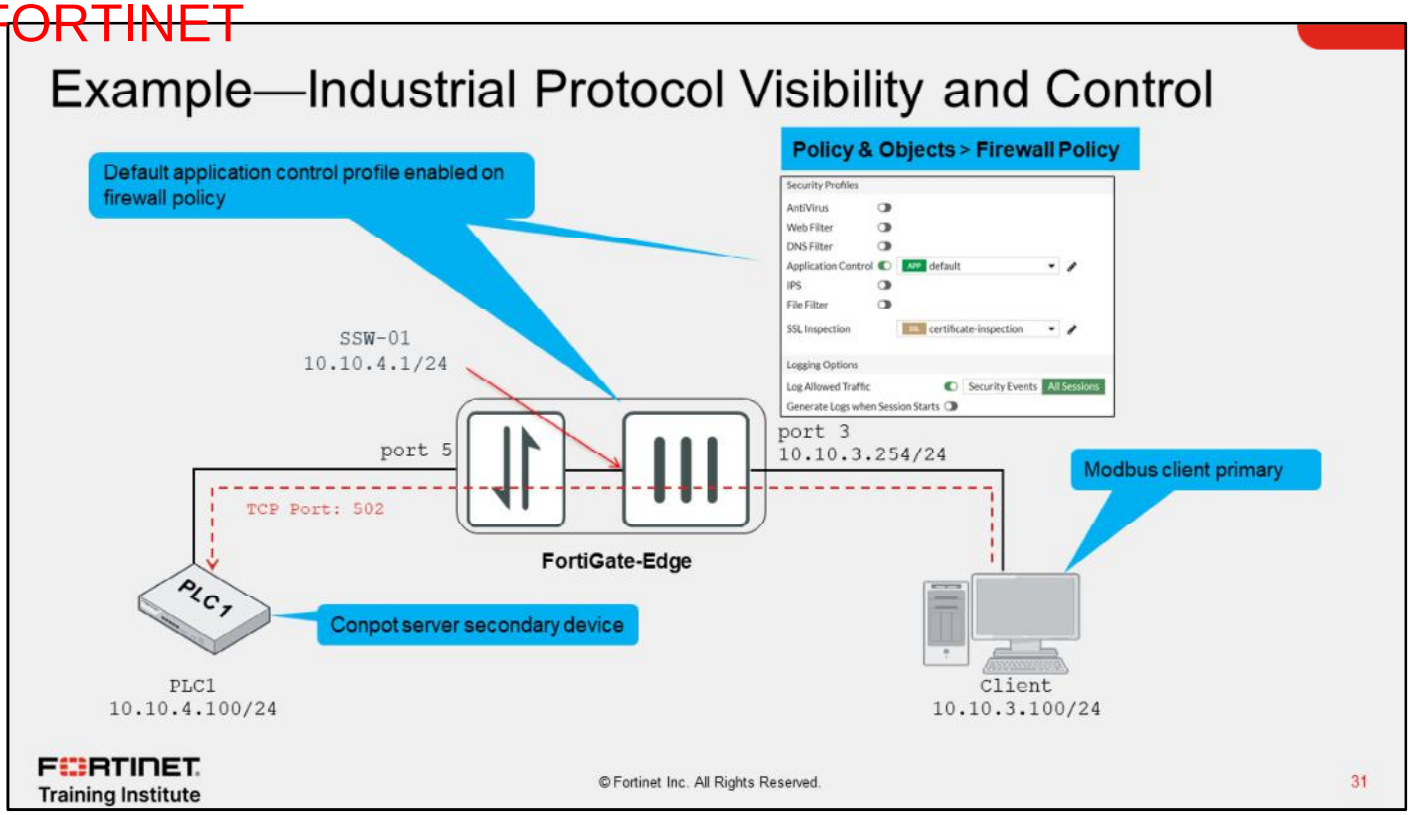
FortiOS gives administrators all the tools they need to inspect subapplication traffic. This gives you the ability to inspect the traffic with more granularity. You can block DNP3_Write, while allowing devices to collaborate using DNP3_Read.

DO NOT REPRINT
© FORTINET



FortiGate supports a variety of industrial protocols along with their subcategories. This slide shows Modbus as an example with its subcategories.

DO NOT REPRINT
© FORTINET



The example on this slide shows that you have implemented a Modbus TCP with a simulation server Conpot.

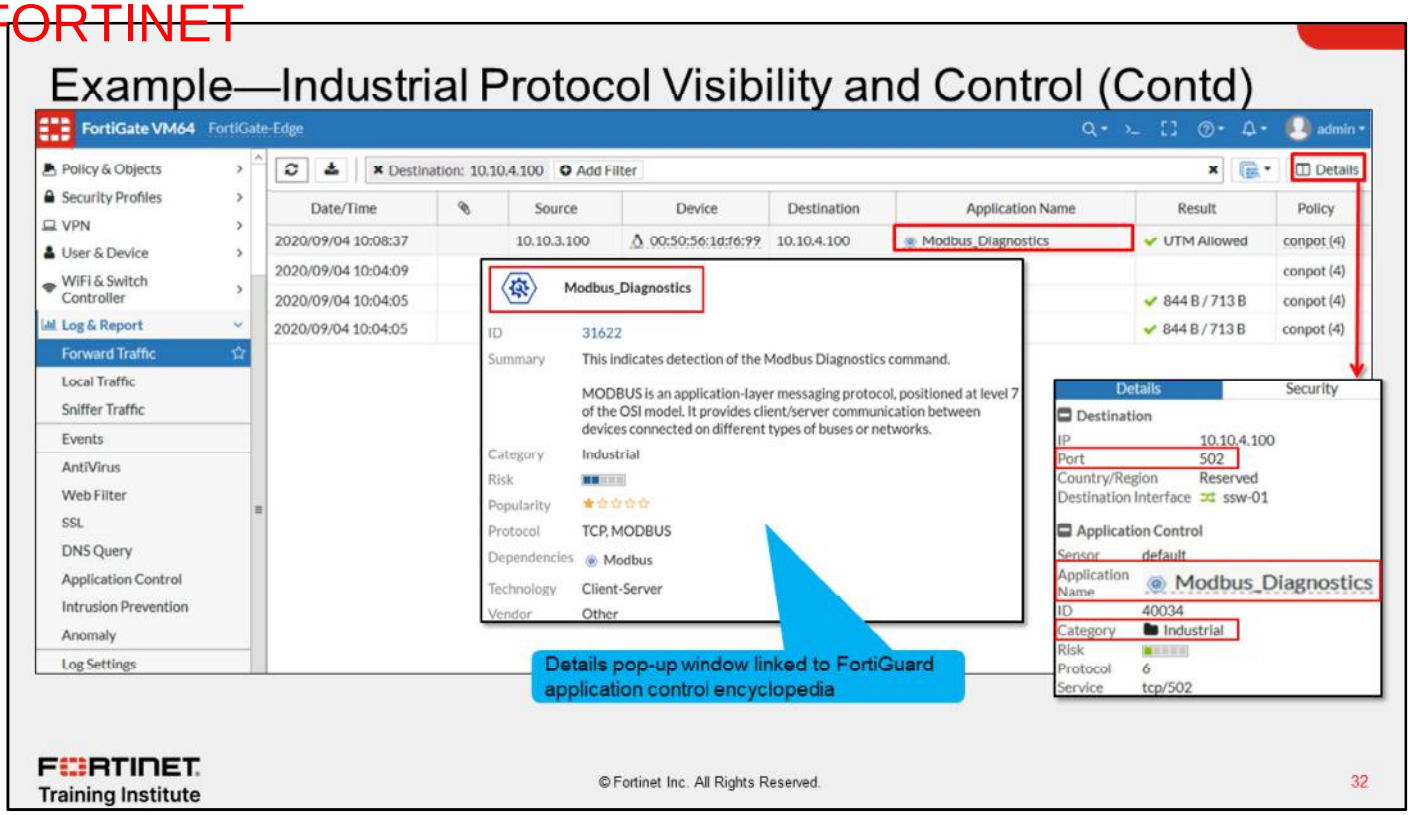
The Modbus `Client` is the primary device with an IP address of `10.10.3.100` connected to `port 3` of FortiGate. You have configured the Conpot server on `PLC1` as the secondary device, with an IP address of `10.10.4.100`, connected to `port5` of FortiGate.

You have configured internal segmentation by enabling a software switch on FortiGate, and port5 of FortiGate is a member of the software switch. The IP address of the switch interface is named `ssw-01` is `10.10.4.1`. Industrial signatures are enabled on FortiGate.

You have configured a firewall policy to allow and log all traffic from `port3` to the `ssw-01` interface of FortiGate for all services. A default application control profile is also enabled on the firewall for industrial protocol visibility in monitor status.

The Conpot server is running on `PLC1` to simulate a secondary device listening on TCP port 502. After you execute a script from the Modbus client primary to send traffic to PLC1 on TCP port 502, the traffic will be allowed, and identified as Modbus traffic by the default application control profile enabled on the firewall policy.

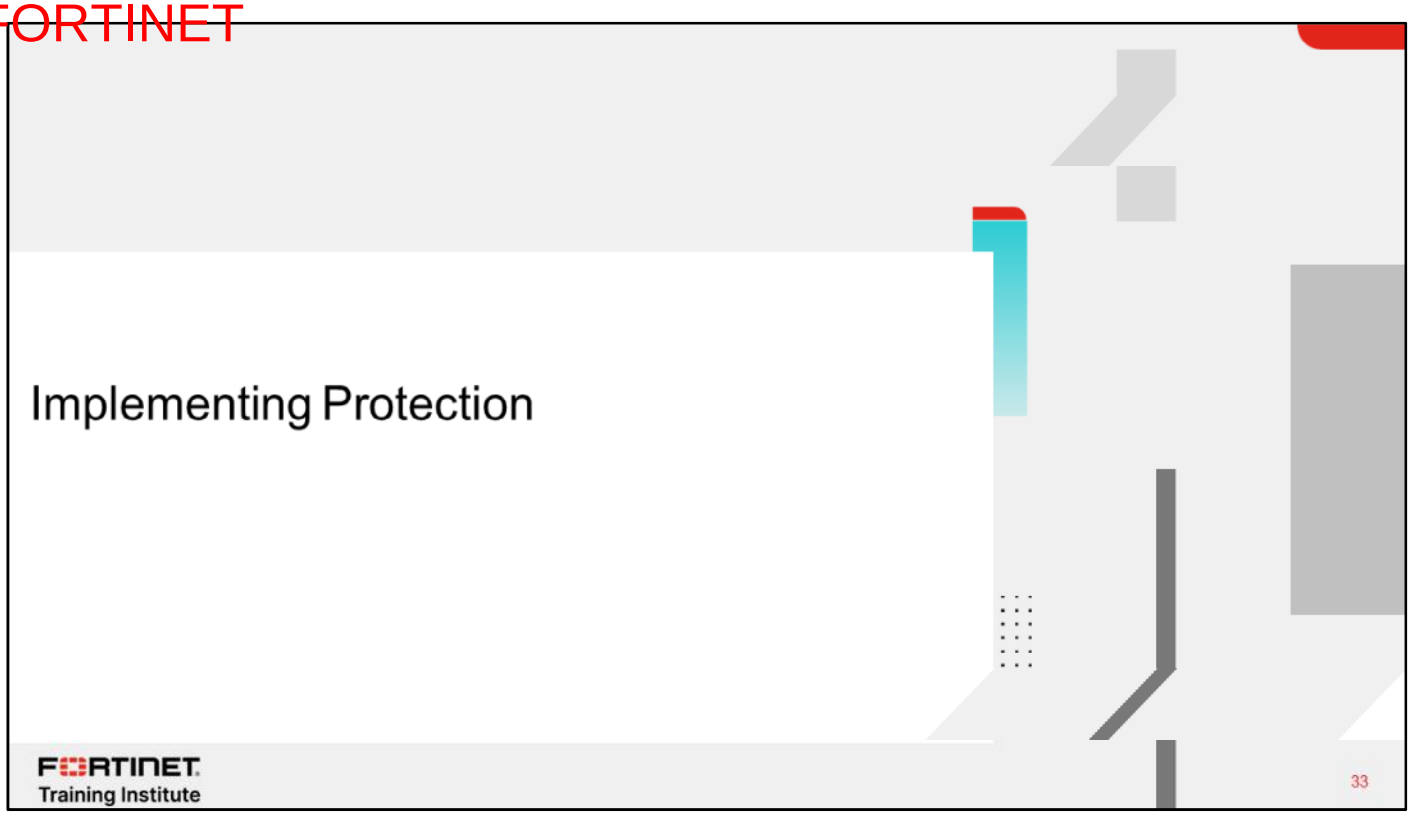
DO NOT REPRINT
© FORTINET



You can view logs for traffic sent from the Modbus client primary to the Conpot server `PLC1` secondary, on TCP port 502. This slide shows that the application name for the traffic is identified as **Modbus_Diagnostics**. This indicates detection of the `Modbus_Diagnostics` command.

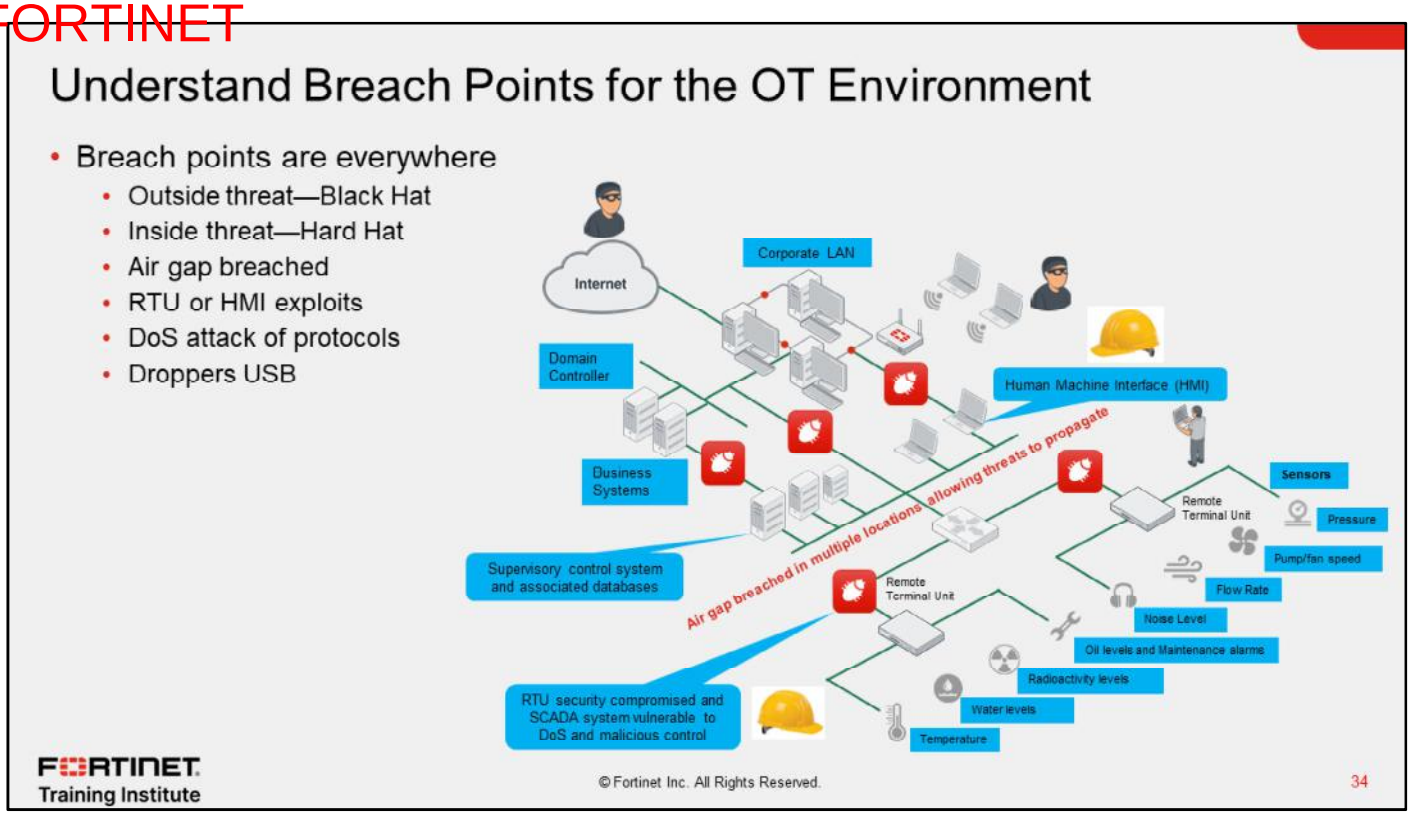
After you establish that the application is visible to FortiGate, you can configure control of the application status to monitor, block, quarantine, or allow.

DO NOT REPRINT
© FORTINET



In this section, you will learn about the implementation of protection for an operational technology environment.

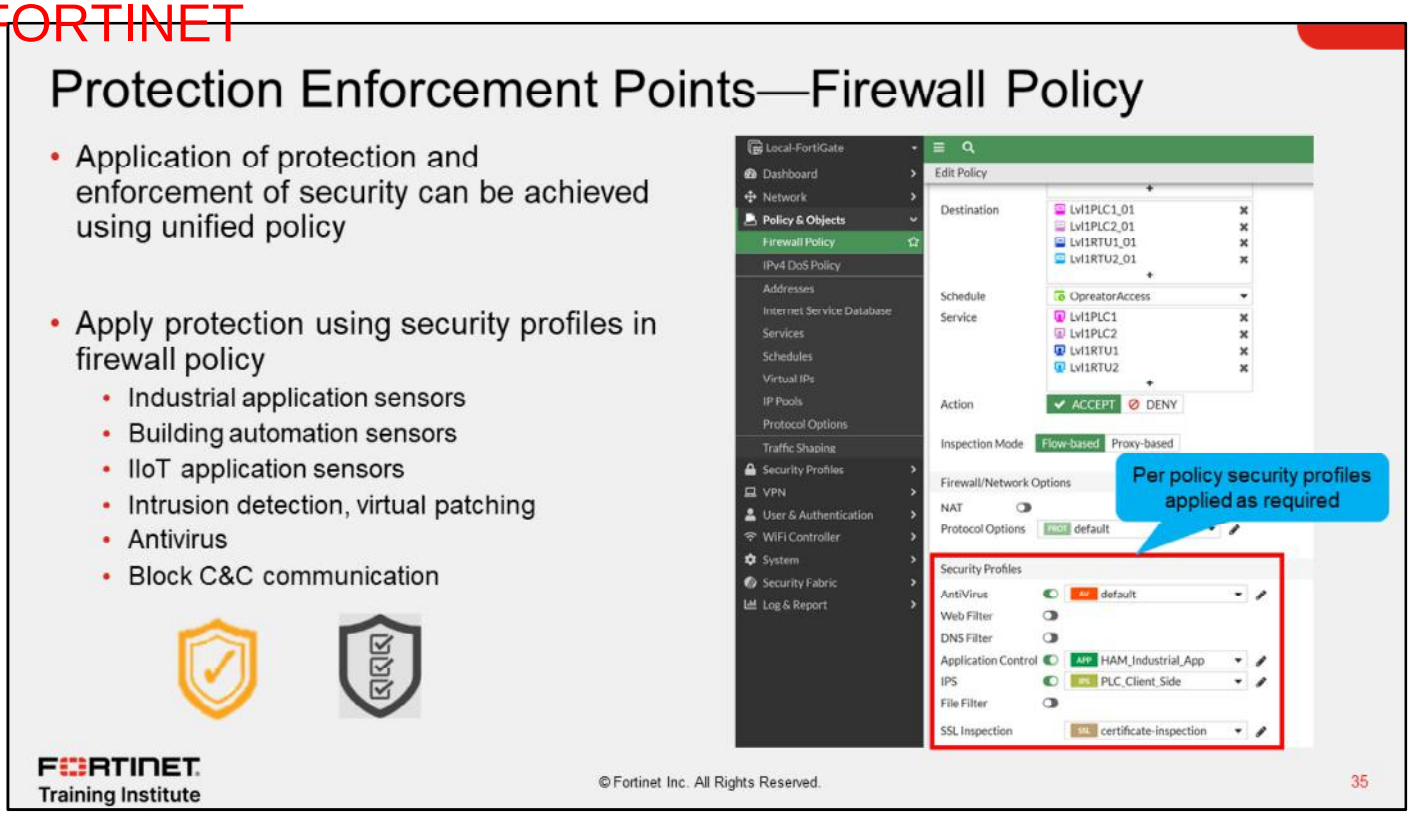
DO NOT REPRINT
© FORTINET



Breach points are everywhere in an OT environment, the most common breach points are:

- Outside threats from external hackers
- Inside threats can be from industrial system operators
- RTU security can be compromised, and the SCADA system is vulnerable to DoS and malicious control
- Air gap can be breached in multiple locations allowing threats to propagate
- DoS attack of industrial protocols
- RTU or HMI can be compromised through known exploits

DO NOT REPRINT
© FORTINET



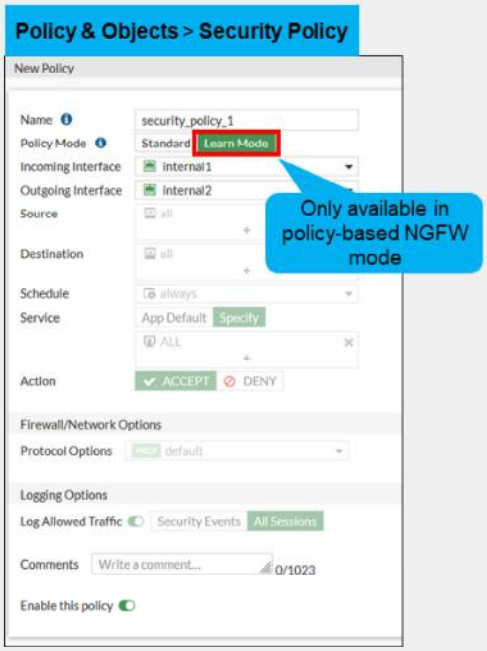
You can apply protection and enforce security with a unified policy using:

- Industrial application sensors
- Building automation sensors
- IIoT application sensors
- Intrusion detection, virtual patching
- Antivirus
- Block C&C communication

DO NOT REPRINT
© FORTINET

Security Policy—Learn Mode

- Learn mode firewall policy is available in NGFW mode firewall (policy-based)
- Learn mode requirements:
  - Source interfaces must have device identification enabled
  - FortiGate must send security logs to FortiAnalyzer
  - The security policy action must be set to **ACCEPT**
- The mode uses the prefixes fields in the UTM and traffic logs
- Policy analyzer management extension application (MEA) on FortiManager can review learn mode firewall policy logs



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

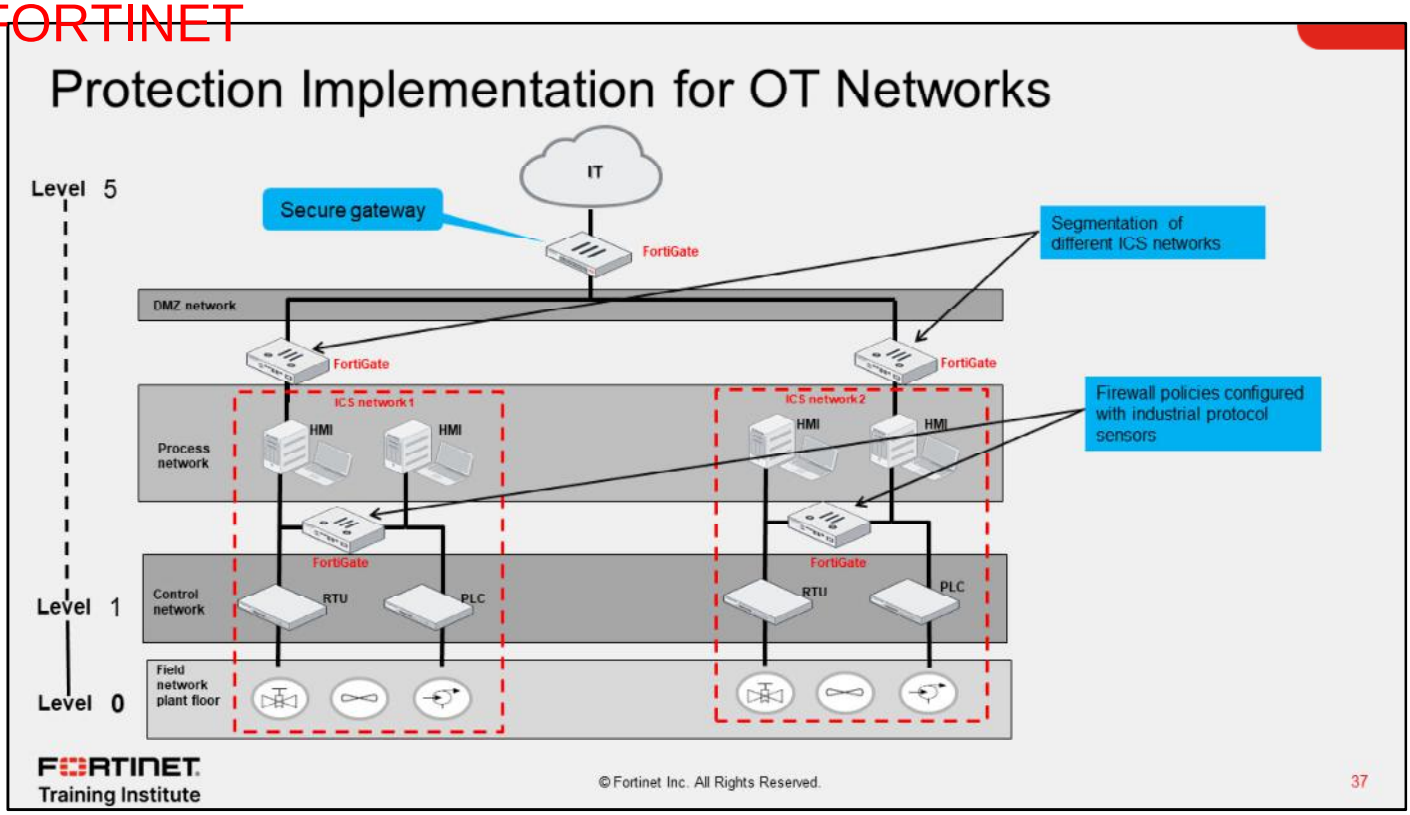
36

You can create security policies to monitor traffic that passes through the interfaces on FortiGate. This is known as the learn mode security policy and is available only if FortiGate is in policy-based NGFW mode.

To create a new learn mode security policy, there are a few other requirements that must be true:
- The incoming interfaces must have device detection enabled.
- The security policy action must accept traffic. Learn mode is not available if the action is set to deny traffic.
- FortiGate must send security logs to FortiAnalyzer.

If FortiManager is managing FortiGate, the policy analyzer MEA on FortiManager can review the logs sent by the managed FortiGate to FortiAnalyzer. Based on the analyzed traffic, FortiManager administrators can choose to automatically create a security policy to block malicious traffic, if detected.

DO NOT REPRINT
© FORTINET



The example on this slide shows an IT network and an OT network with two ICS environments. Remember, the first line of defense is securing the IT side.

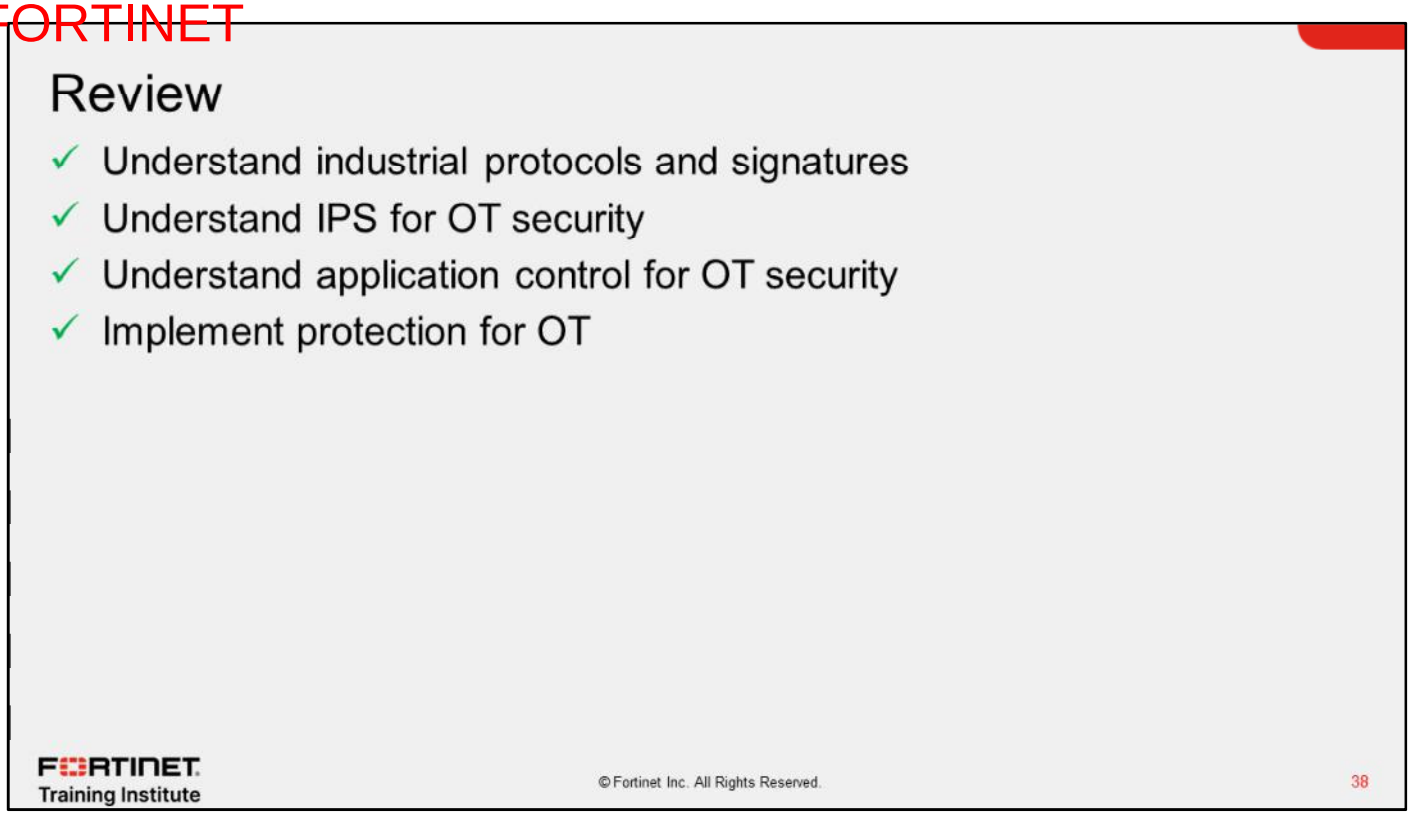
To protect the different ICS environments and limit the propagation of attacks coming from IT to the different ICS networks or elements, segmentation is recommended. In this example, FortiGate creates conduits that stop threats from propagating between ICS network 1 and ICS network 2.

Expanding on this concept, by placing FortiGate devices at strategic points within the ICS network itself, you can granularly segment different zones creating an extra layer of protection for the endpoints and controllers as well as protect the data flow and communications between them. FortiGate has specific ICS and SCADA-aware functionality, and can identify and police most of the common ICS and SCADA protocols. In parallel to this specific protocol support, additional vulnerability protection is provided for applications and devices from the major ICS manufacturers through a set of signatures.

This provides a more granular application-level control of the traffic between zones, and enables FortiGate to detect attempted exploits of known vulnerabilities relating to any of the supported vendor's solutions.

For a more thorough analysis of ICS networks and their processes and protocols, you must take a more proactive approach.

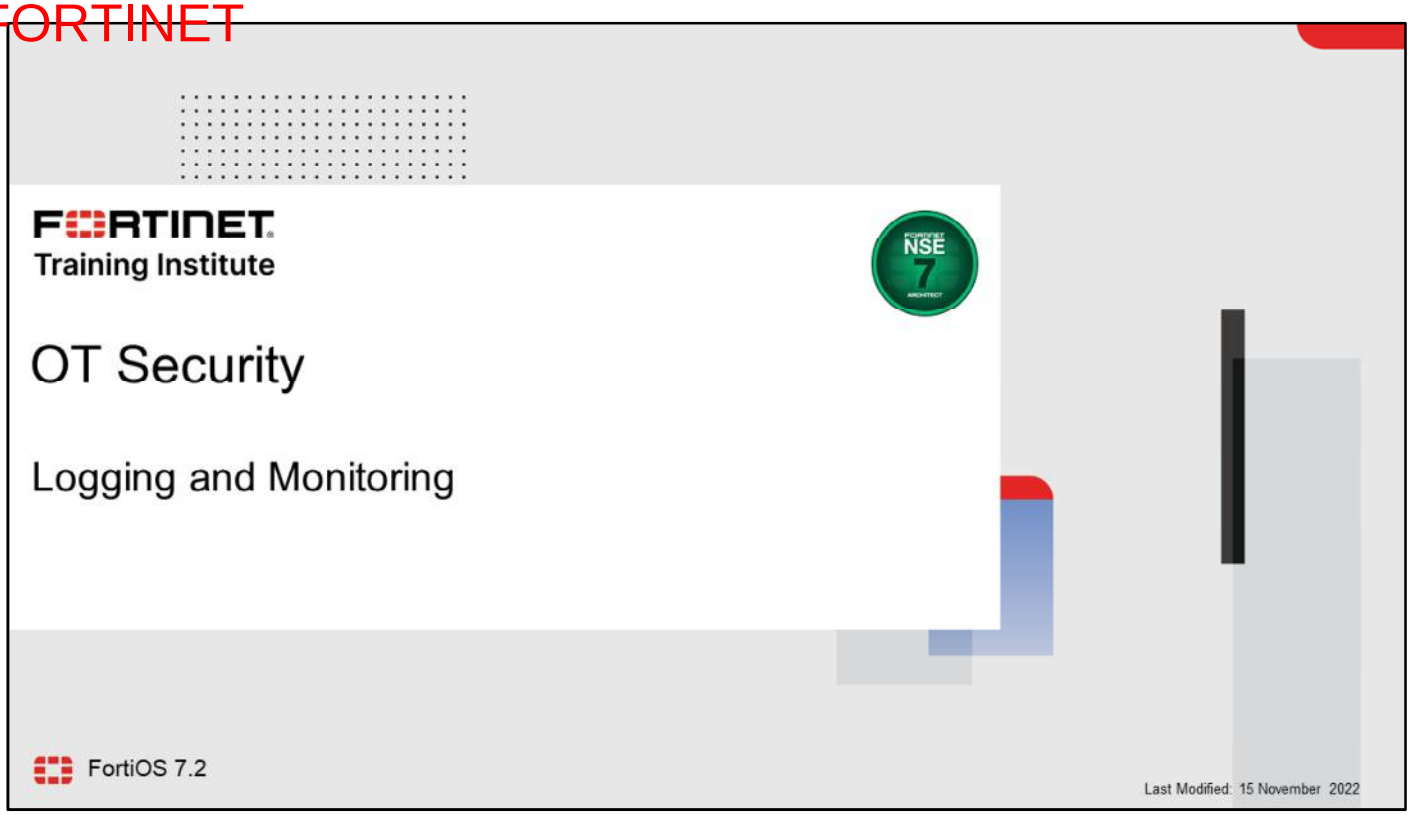
DO NOT REPRINT
© FORTINET



This slide shows the objectives that you covered in this lesson.

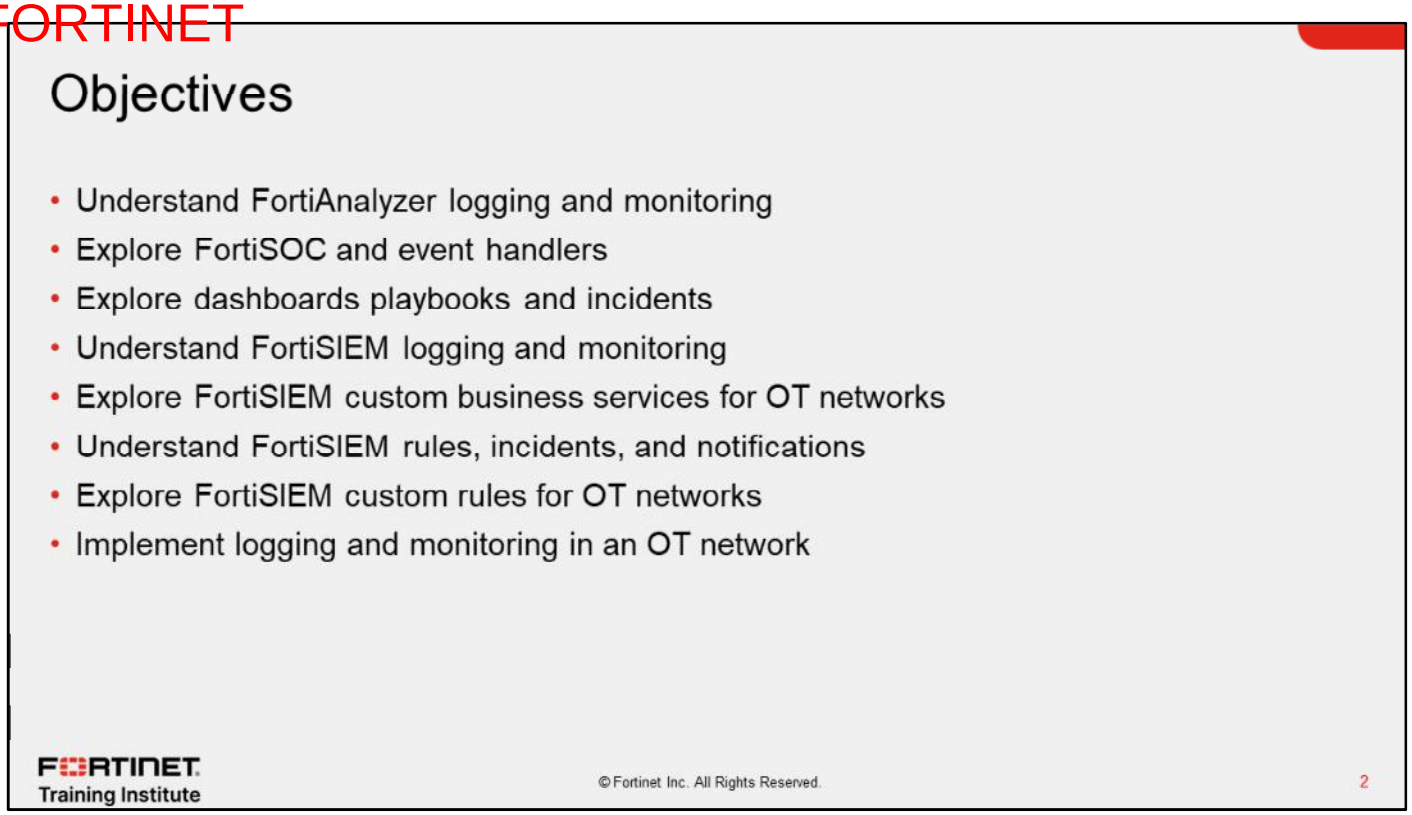
By mastering the objectives covered in this lesson, you learned about protection for an operational technology environment.

DO NOT REPRINT
© FORTINET



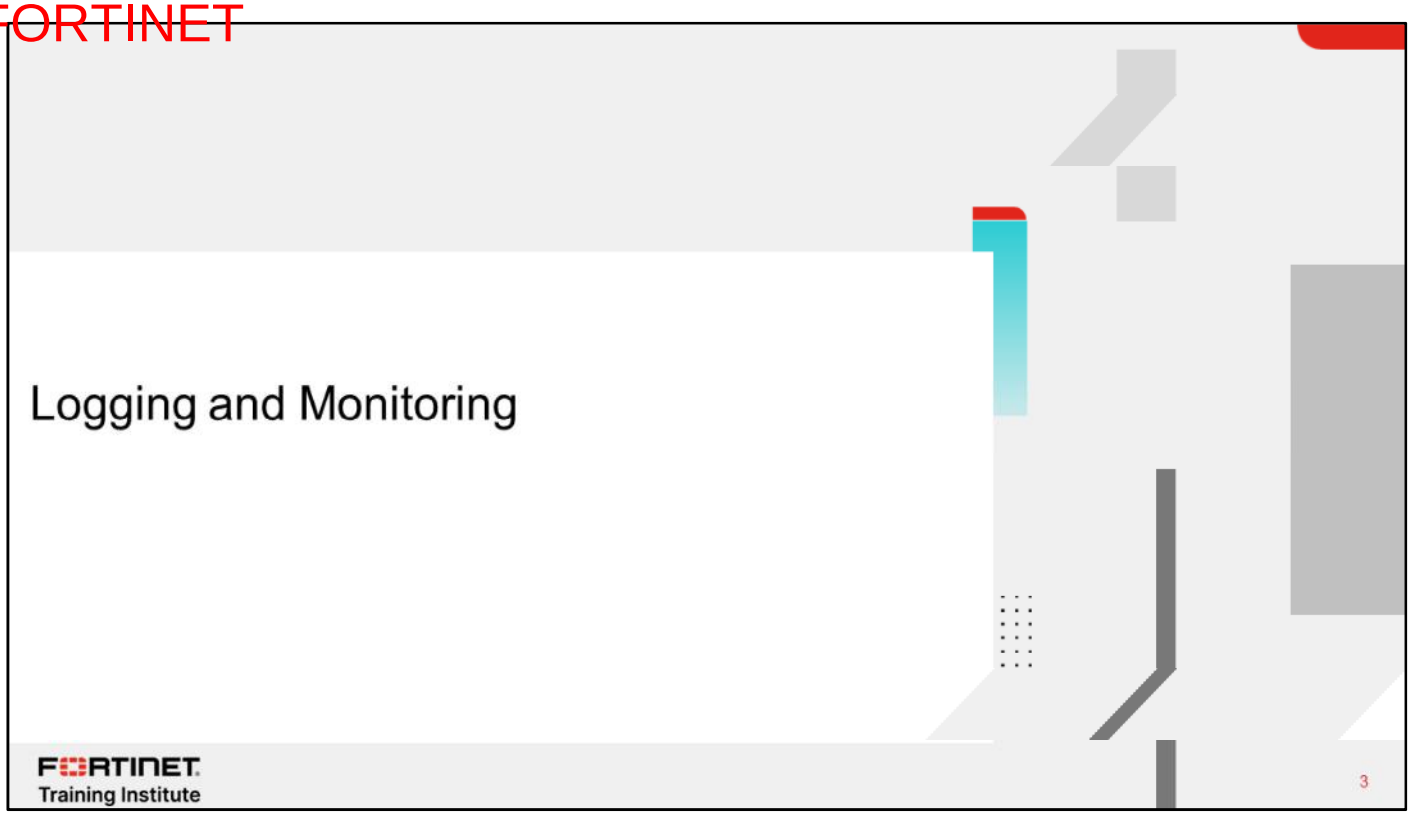
In this lesson, you will learn about the use of logging and monitoring devices—FortiAnalyzer and FortiSIEM—for operational technology (OT) security.

DO NOT REPRINT
© FORTINET



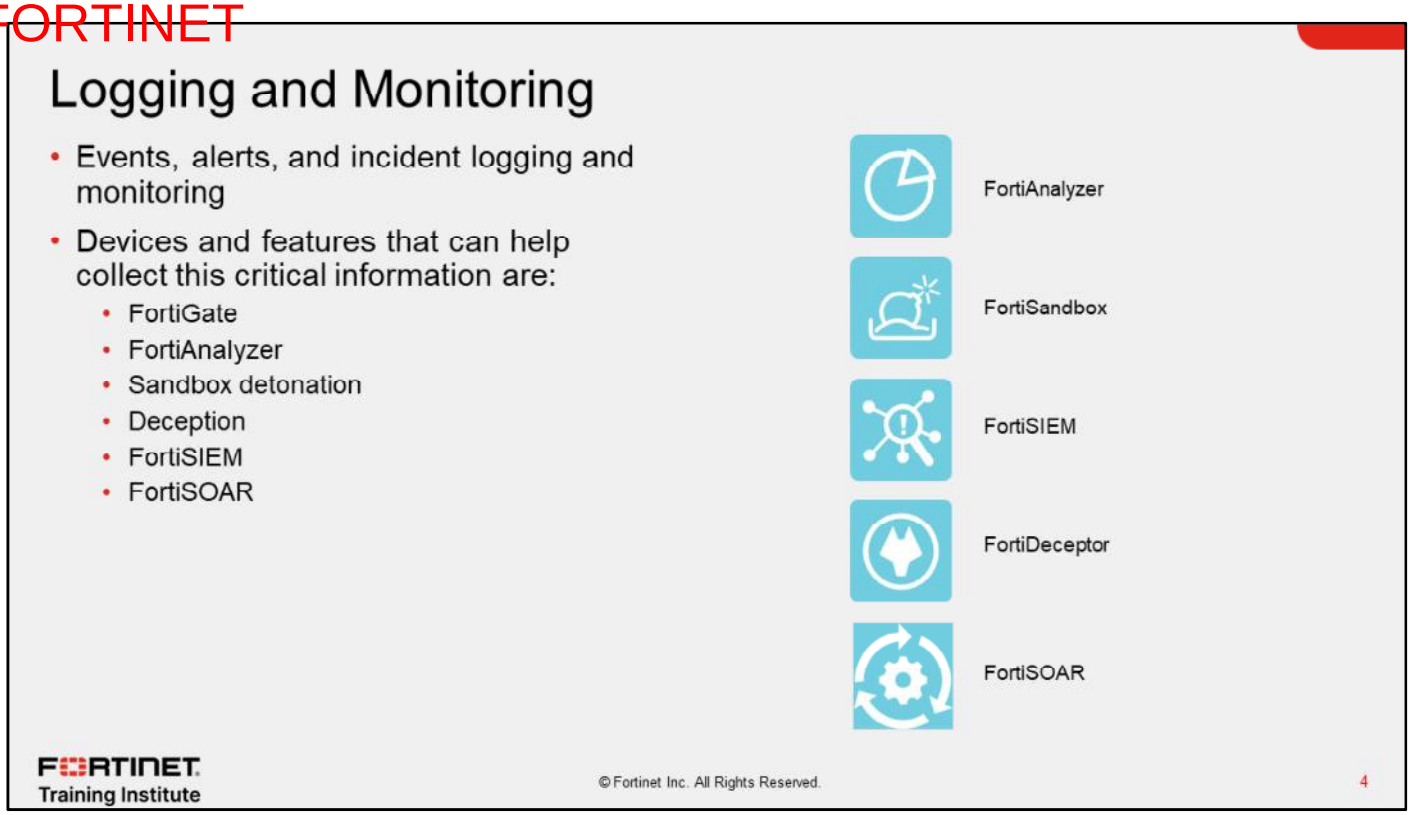
After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about logging and monitoring devices, FortiAnalyzer and FortiSIEM.

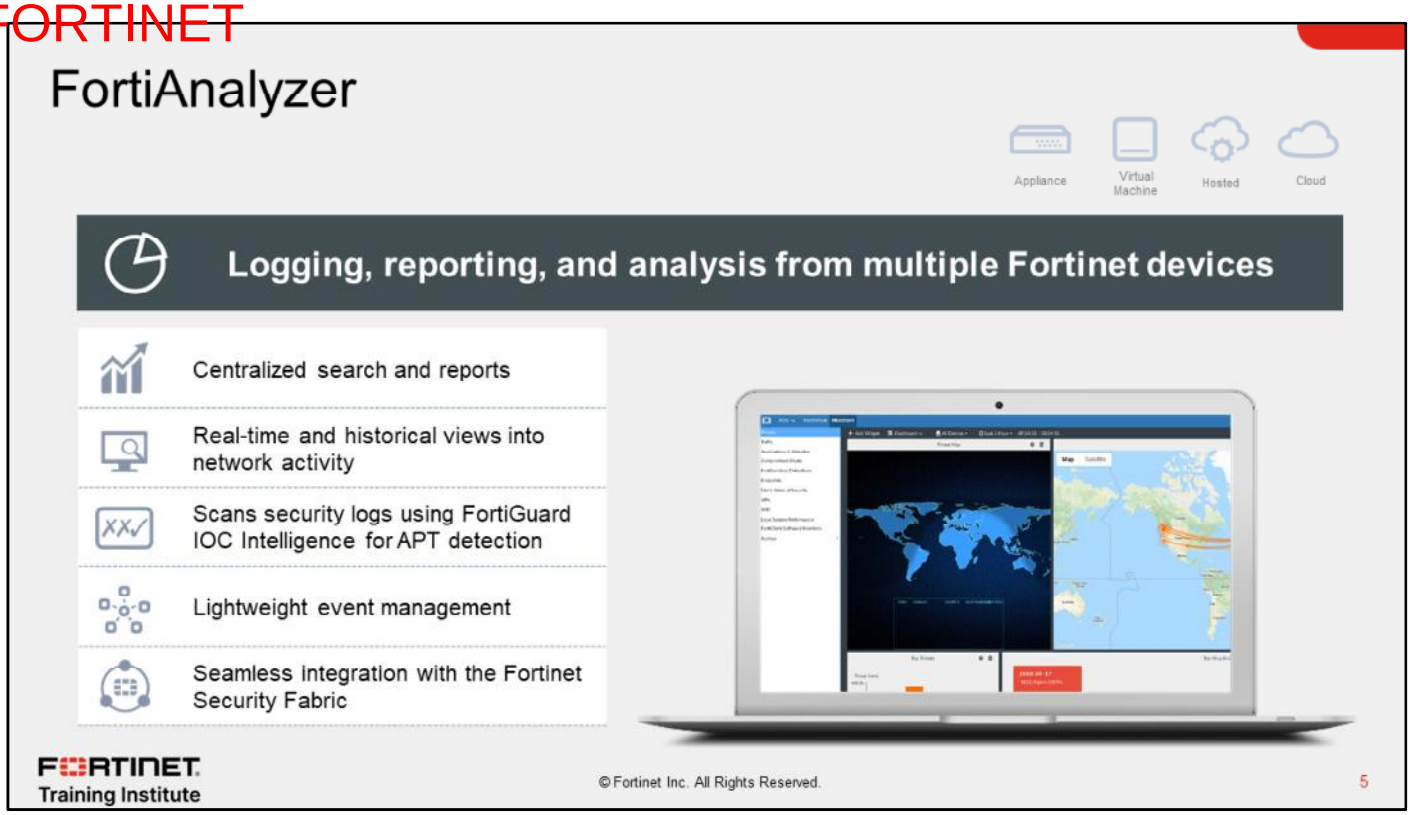
DO NOT REPRINT
© FORTINET



You need full log visibility in both the IT and OT environments. Logging and reporting is a crucial element in the framework because it helps auditors perform threat hunting and the spot possible threats to the OT network.

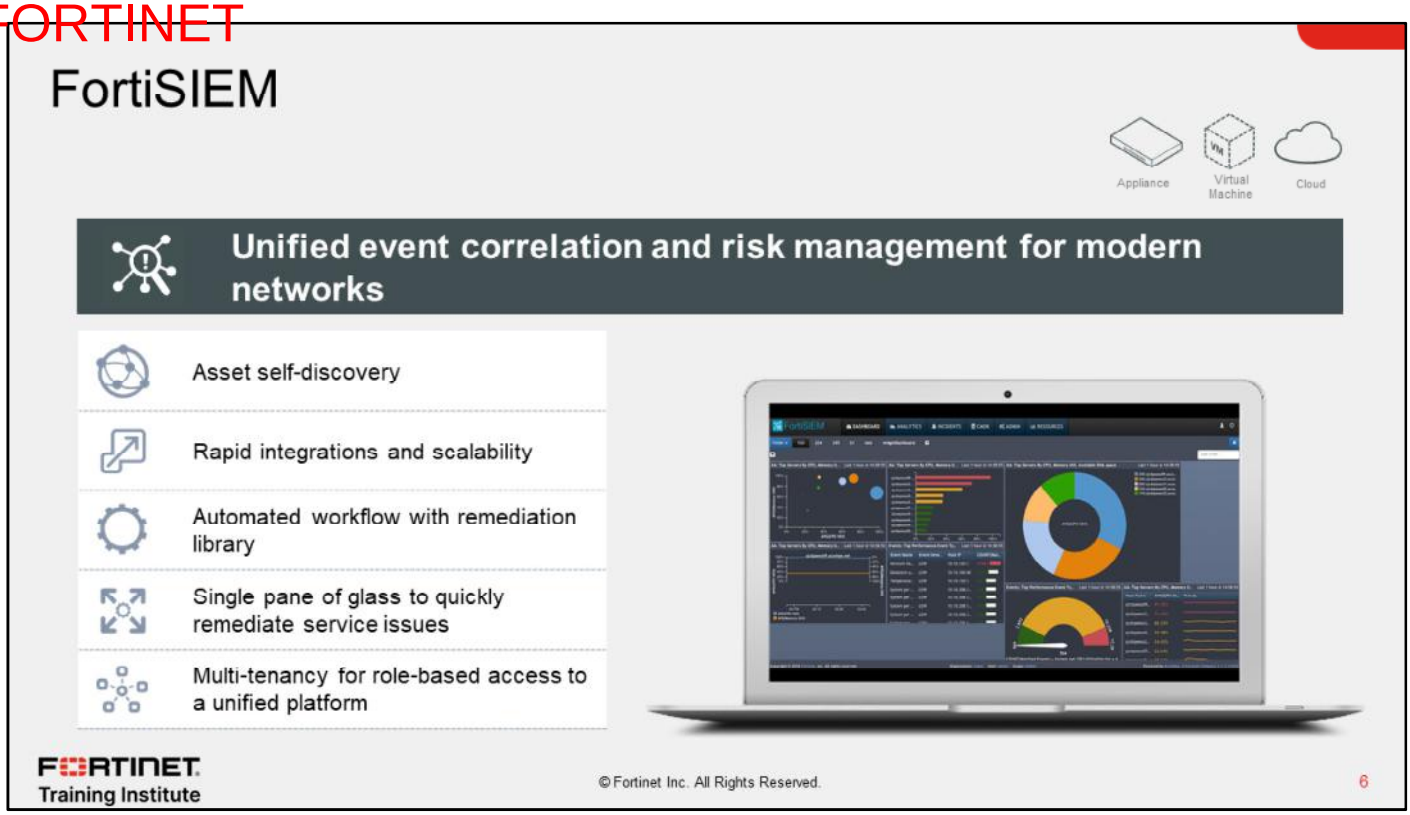
The advantages of the single-pane-of glass approach are key when reviewing an incident. Utilizing the Fortinet Security Fabric, operators and incident responders can link access logs, device information, and network traffic to provide a complete picture during post-incident forensics.

DO NOT REPRINT
© FORTINET



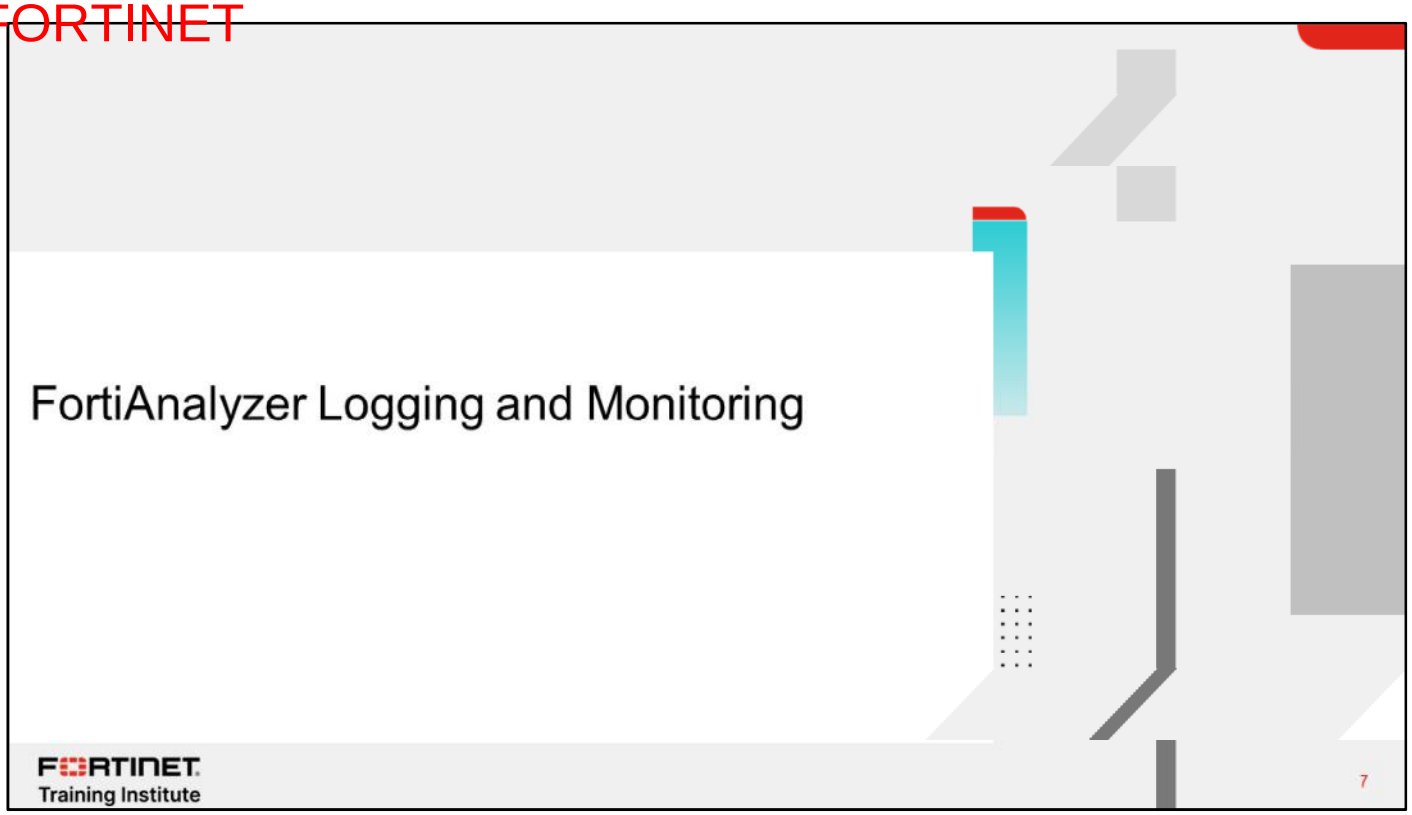
FortiAnalyzer is the foundation of the Security Fabric and provides logging, reporting, analytics, and automation for all on fabric devices and endpoints. FortiSOAR feature enables orchestration and automation across the Security Fabric environment.

DO NOT REPRINT
© FORTINET



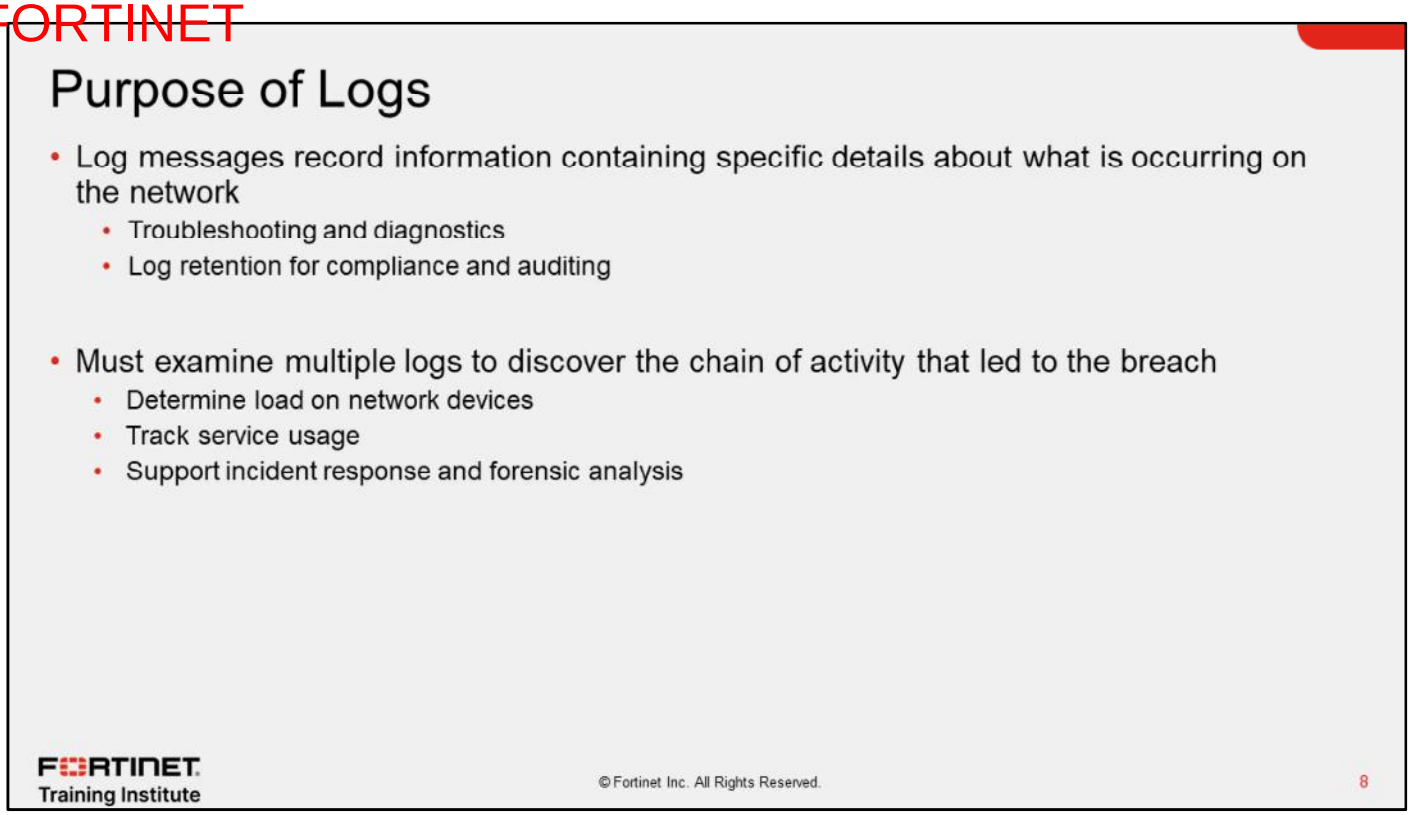
FortiSIEM brings multi-vendor visibility across your network. Higher levels of correlation and customization can be integrated with the Security Fabric, making threat hunting easy.

DO NOT REPRINT
© FORTINET



In this section, you will learn about logging and monitoring on FortiAnalyzer for OT networks.

DO NOT REPRINT
© FORTINET



Log messages help paint a picture of what is going on in your network.

You can determine the load on your network devices, track service usage, and identify any security breaches in your network.

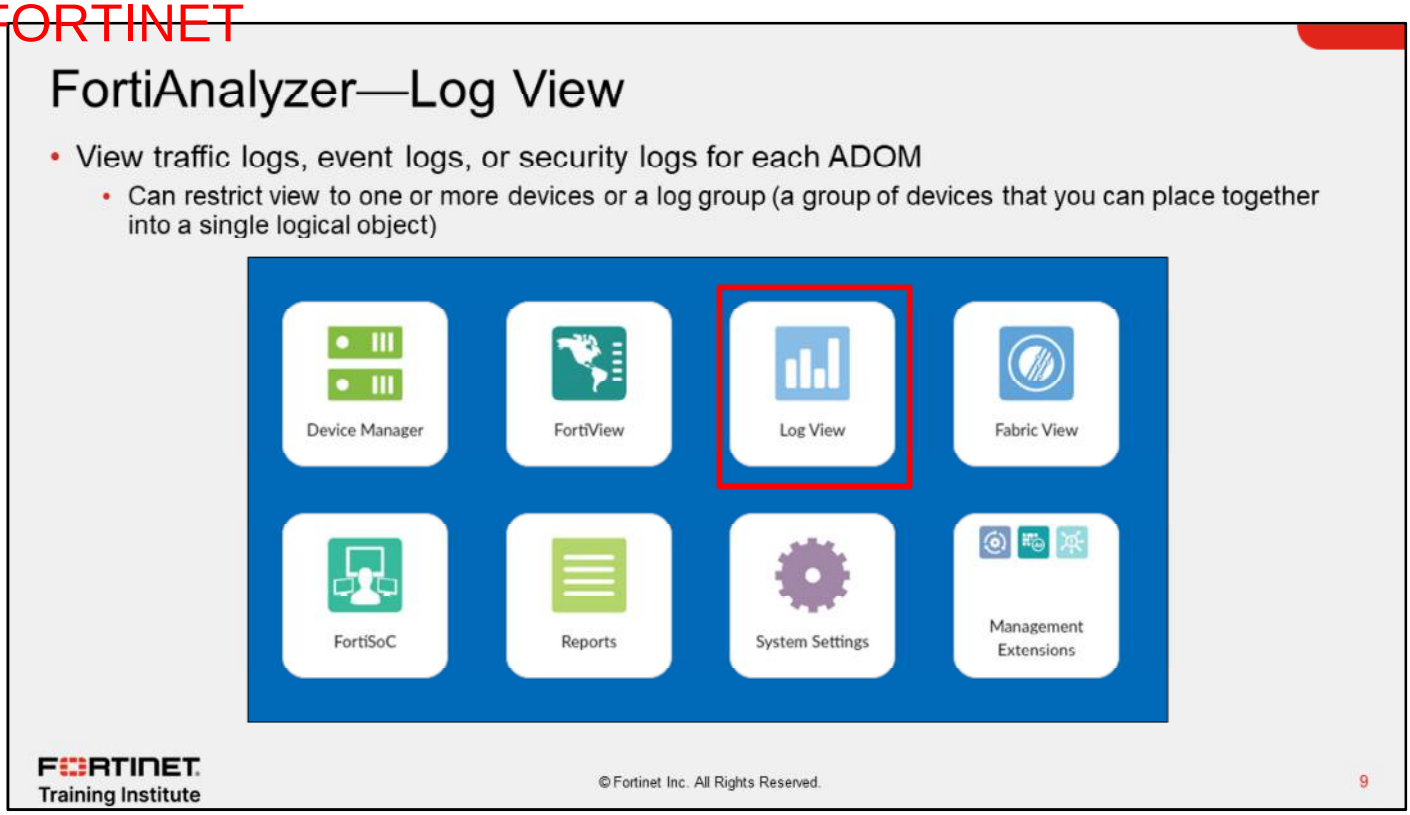
However, it is important to understand that logs are like a puzzle—you must put several pieces together in order to get a complete understanding of what is going on.

Multiple log messages are often required to determine the exact chain of activity that leads to a breach—a log in isolation often won't help you to best configure your network to prevent such breaches in the future.

For example, request and response logs of primary, and secondary PLC or RTU devices include read and write function codes, which will help to analyze, why a specific task was initiated, or ended by PLC or RTU.

This is why centralized log storage is so important.

DO NOT REPRINT
© FORTINET

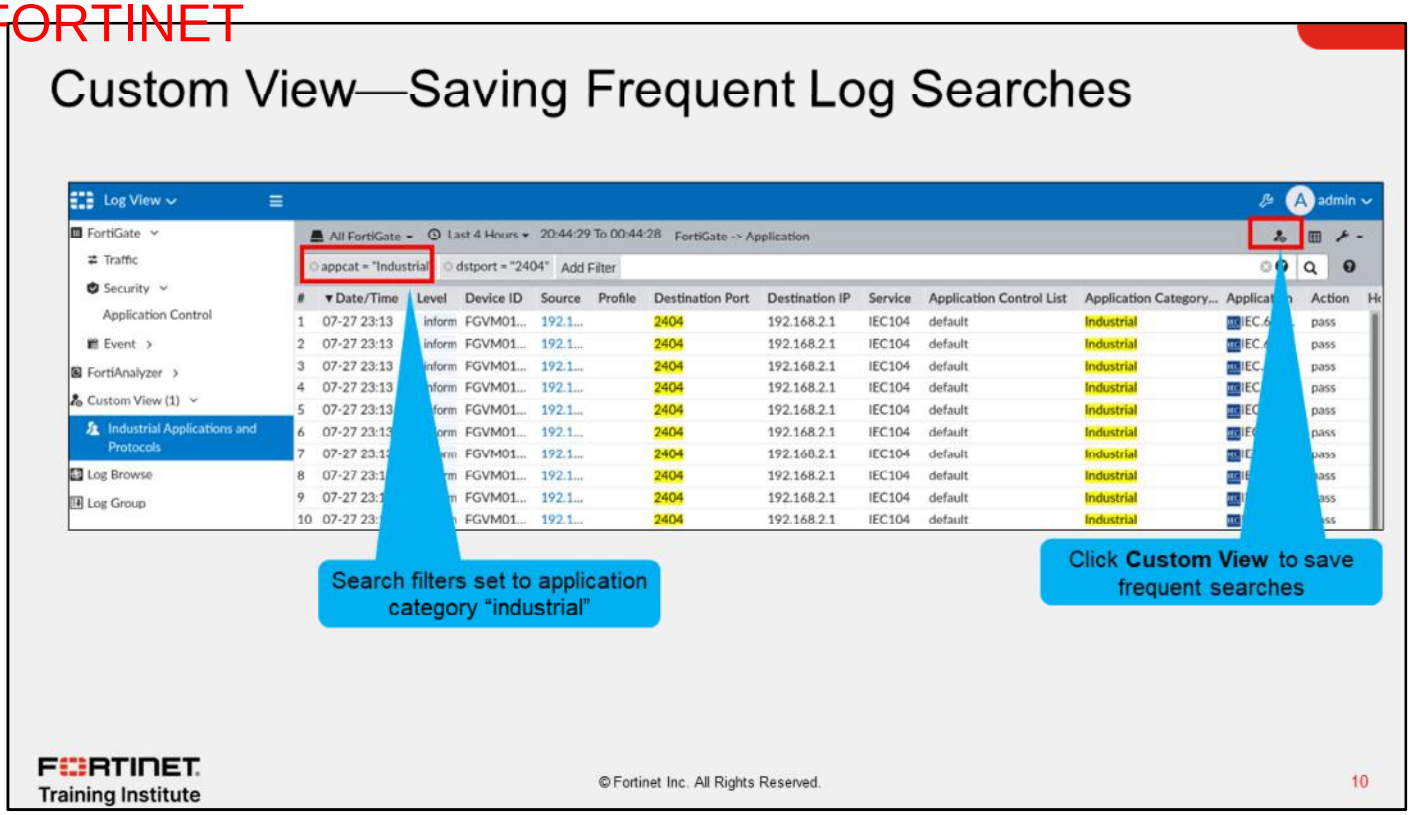


Log View allows you to view traffic logs, event logs, and security logs information for devices in each ADOM.

You can restrict the log view to one or more devices in the ADOM, or to a log group, which is a group of devices placed together in a single logical object.

Log groups are virtual. They don't have SQL databases or occupy additional disk space.

DO NOT REPRINT
© FORTINET

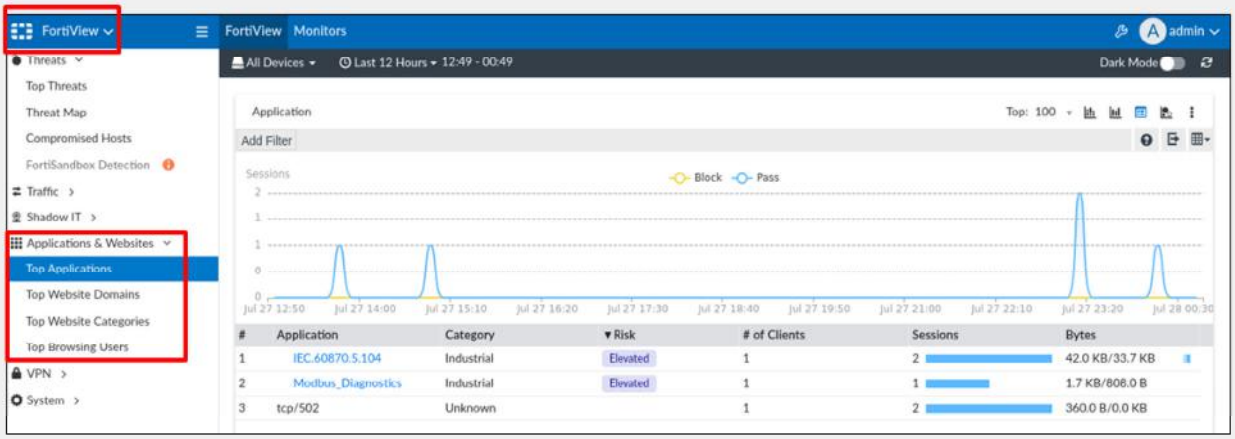


You can save frequent searches as a custom view **Custom View** on the tool bar. Set your filters, conduct your search, and then save the search under a custom view.

DO NOT REPRINT
© FORTINET

FortiAnalyzer—FortiView

- Integrates real-time and historical data into single, summary views
- Analytics logs only (archive logs not displayed)



FORTINET Training Institute

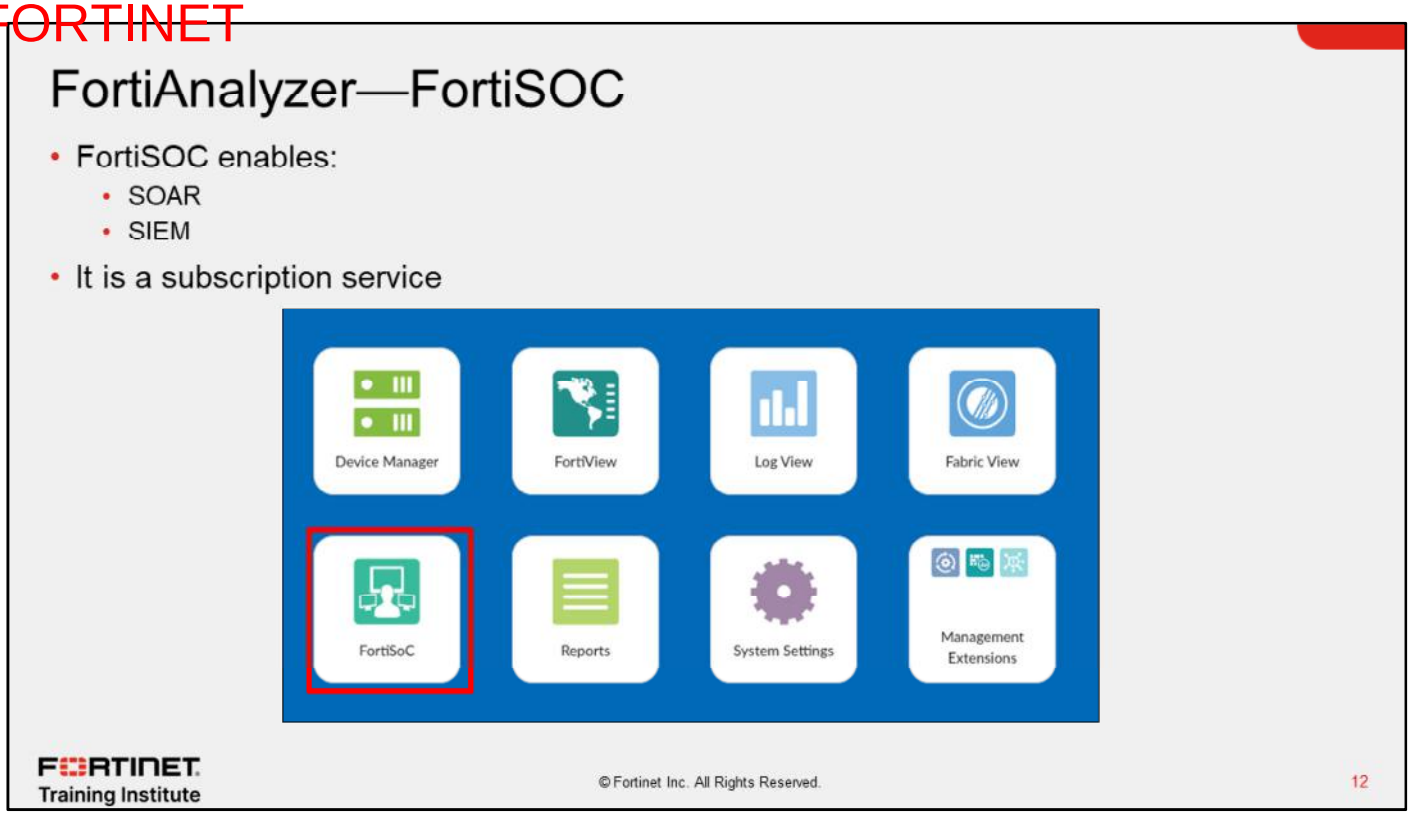
© Fortinet Inc. All Rights Reserved.

11

You can view summaries of log data in FortiView in both tabular and graphical formats. FortiView integrates real-time and historical data into a single, summary view. For example, you can view top applications and websites, top threats to your network, top sources of network traffic, and top destinations of network traffic. For each summary view, you can drill down into details.

The **FortiView** pane allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, user ID or IP address, application, and so on. You can use it to investigate traffic activity related to industrial applications, such as Modbus, and IEC104.

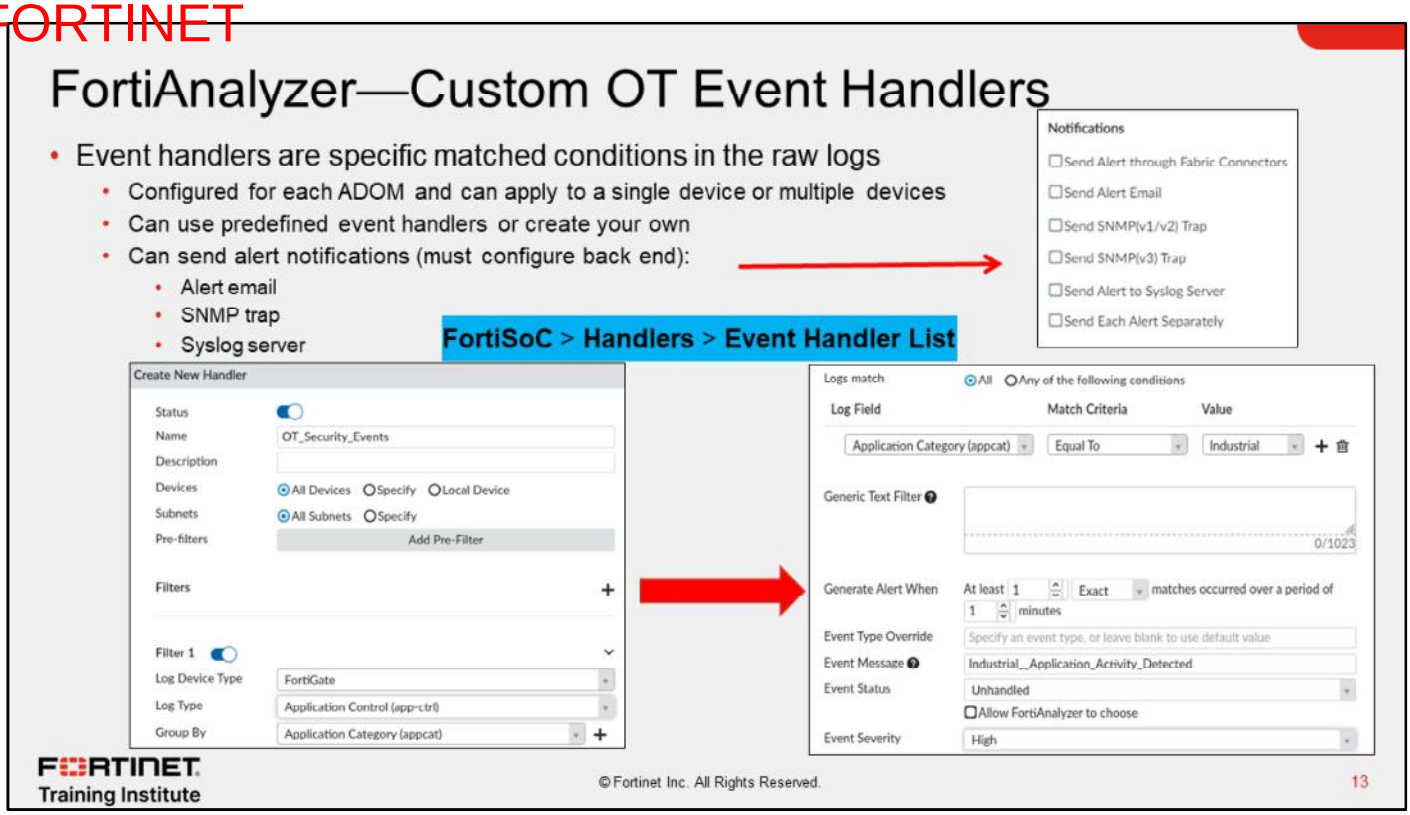
DO NOT REPRINT
© FORTINET



FortiSoC is a subscription service that enables security orchestration, automation, and response (SOAR), and security information and event management (SIEM) capabilities on FortiAnalyzer.

The FortiAnalyzer SIEM capabilities parse, normalize, and correlate logs from Fortinet products. FortiSoC provides event and incident management capabilities with playbook automation to accelerate incident response.

DO NOT REPRINT
© FORTINET

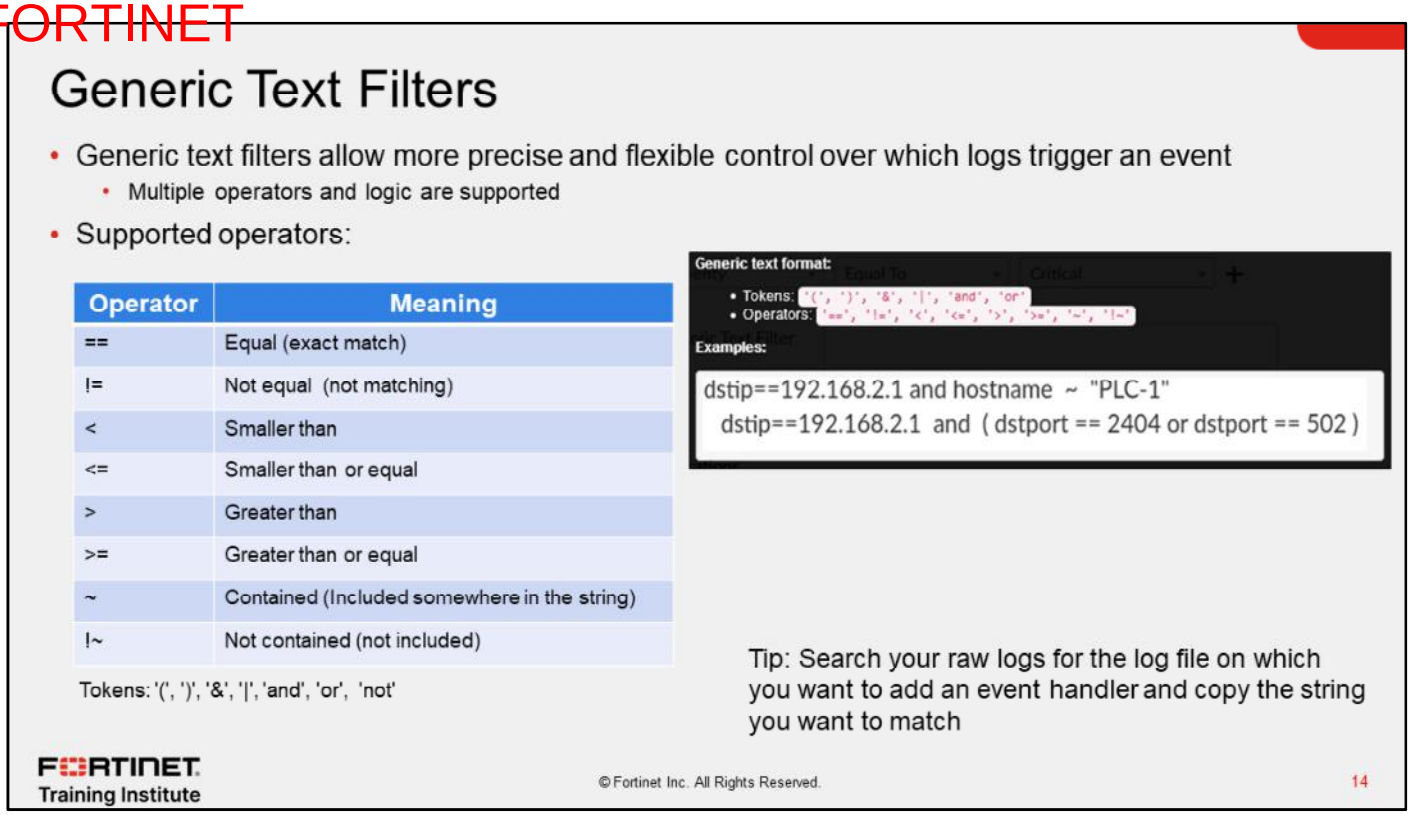


Event handlers are specific matched conditions in the raw logs that determine what events are to be generated.

The system includes a number of predefined event handlers that you can enable to generate events. You can also configure event handlers to send alert notifications by email, as SNMP traps, or to a syslog server. In order to use any of these notification methods, you must first set up the back end (for example, an email server for email notifications).

If none of the predefined event handlers meets your requirements, you can create custom event handlers.

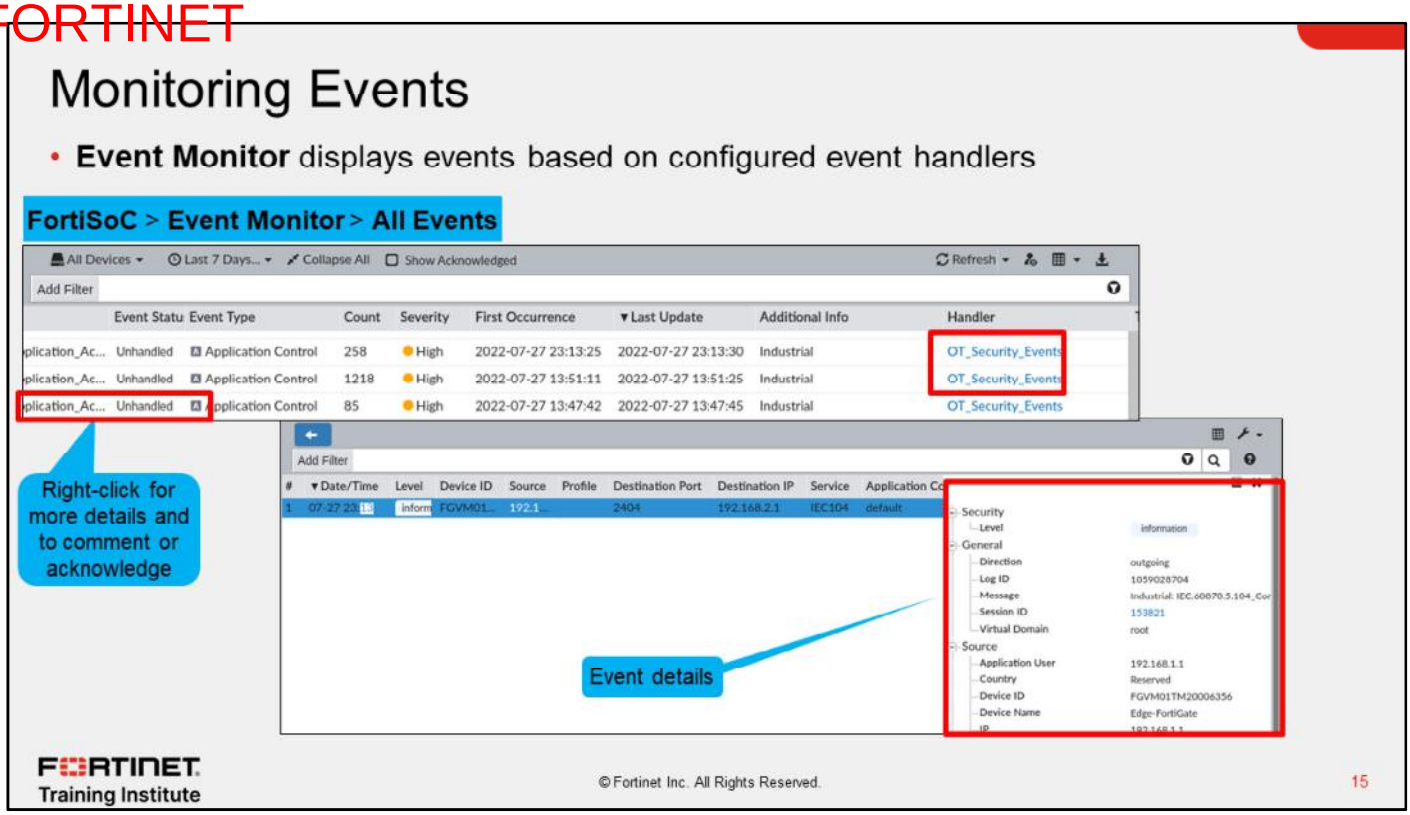
DO NOT REPRINT
© FORTINET



When configuring an event handler, the generic text filter allows more precise and flexible control over which logs trigger an event. Multiple operators and logic are supported.

As a tip, you can search your raw logs for the log file on which you want to add an event handler and copy the string you want to match.

DO NOT REPRINT
© FORTINET

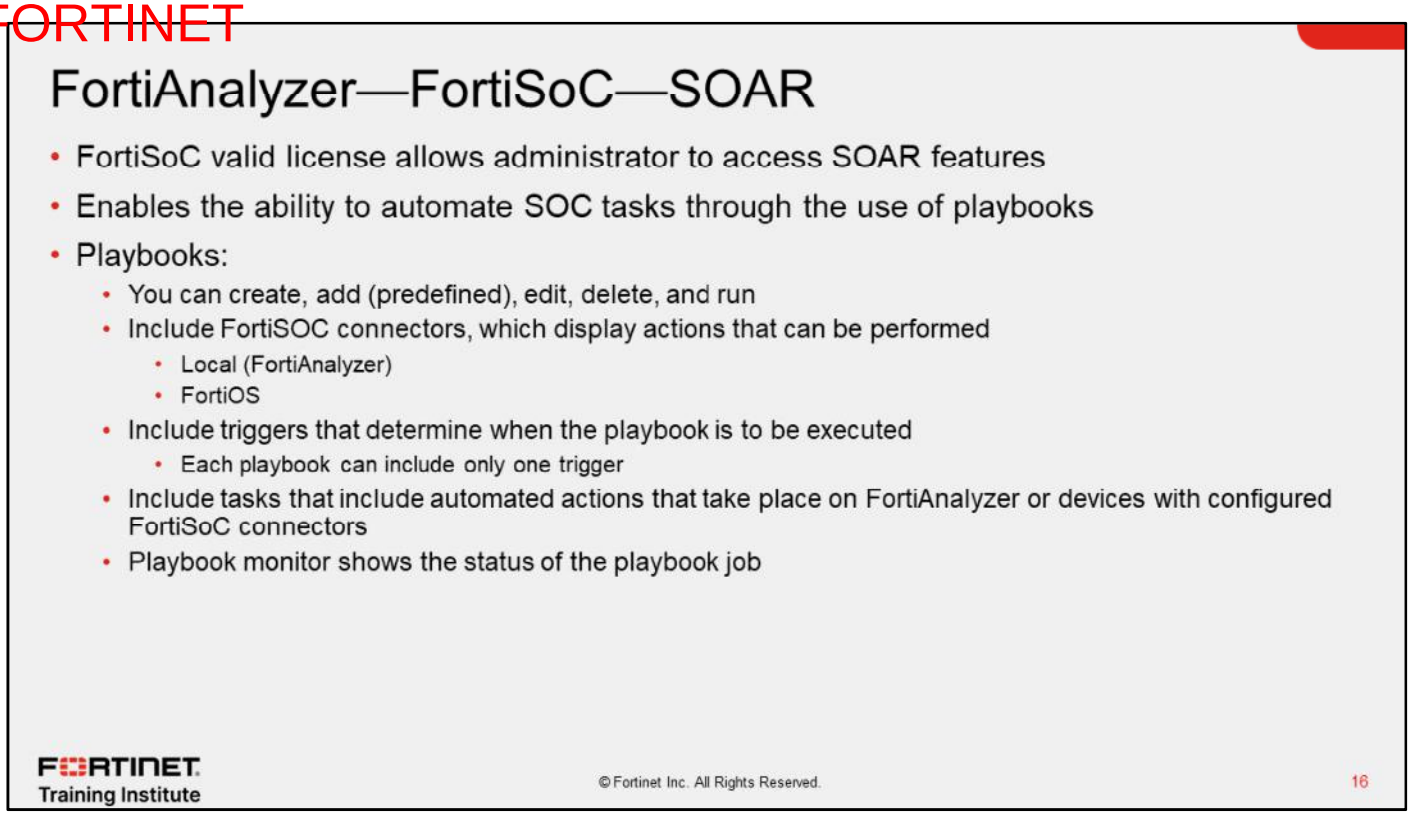


On the **FortiSoC** pane, the **Event Monitor** section shows all events generated by your enabled and configured event handlers.

Double-clicking an event provides more details about the event, including the associated logs. It also allows you to leave a comment for your records, and to acknowledge the event.

Event handlers work in raw logs, not in the database logs.

DO NOT REPRINT
© FORTINET



When FortiAnalyzer has a valid subscription license, the FortiSoC module is activated and administrators are able to access SOAR features. Task automation can be configured by SOC analysts using playbooks, which consist of a trigger and sequence of automated actions.

You can create playbooks from scratch or by using one of the predefined templates. Fabric connectors further enhance FortiSoC functionality by allowing playbooks to perform tasks using connected devices, including local FortiAnalyzer and FortiOS.

Playbooks include a starter event (trigger) that determine when a playbook is to be executed. Each playbook can only include one trigger. Triggers are always the first step in a playbook. After a playbook has been triggered, it flows through the remaining tasks as defined by the routes in the playbook using the trigger as a starting point.

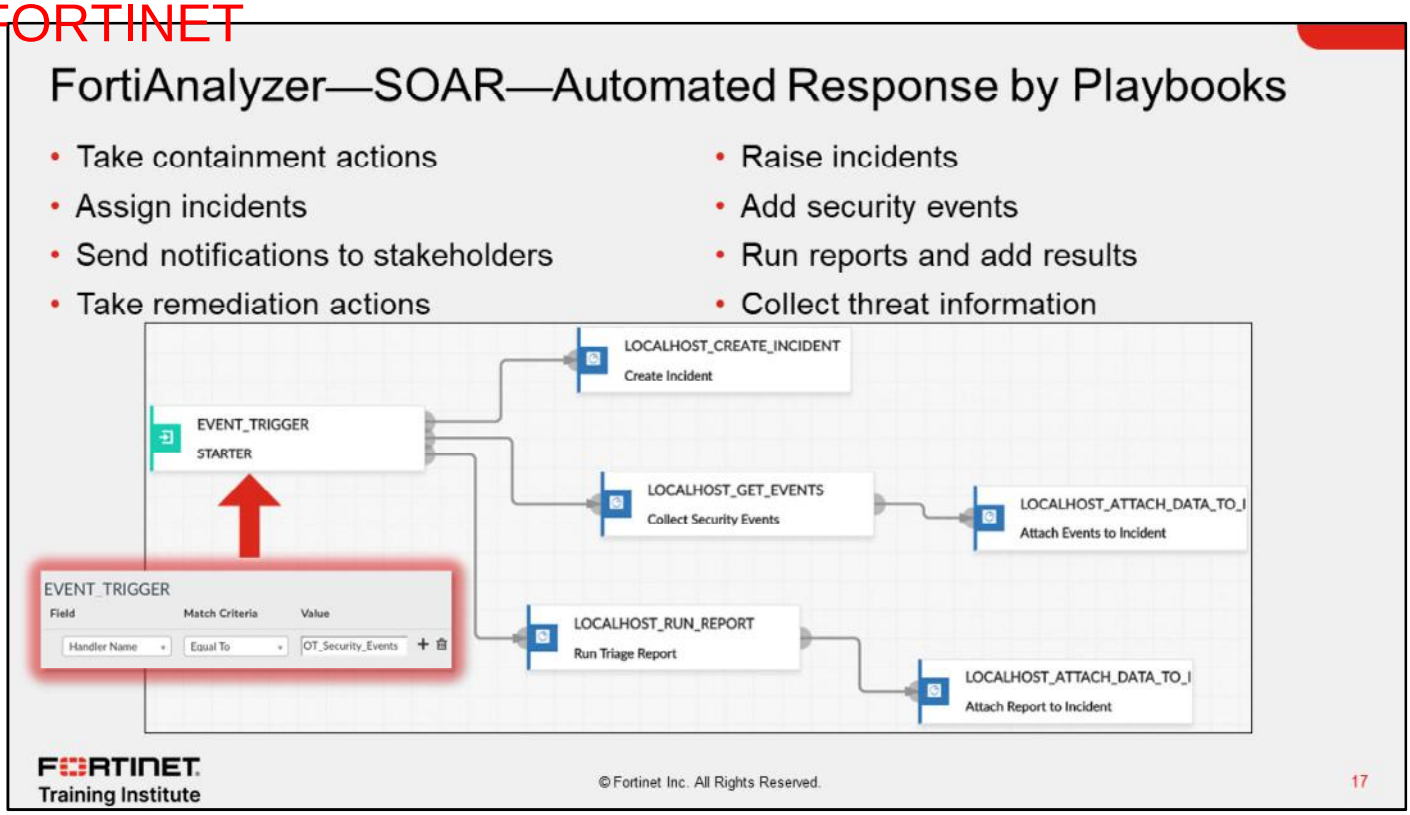
Tasks include automated actions that take place on FortiAnalyzer or devices with configured FortiSoC connectors. Tasks can be linked together in sequences. A task is run as soon as the playbook is triggered and all connected tasks preceding it are complete. Tasks can be configured with default input values or take inputs from the trigger or preceding tasks.

You can view the status of playbook jobs in **FortiSoC** > **Automation** >**Playbook Monitor**.
Status include:

- Running
- Success
- Failed

Note that playbook jobs that include one or more failed tasks are labelled as **Failed** in **Playbook Monitor**; however, individual actions may have been completed successfully.

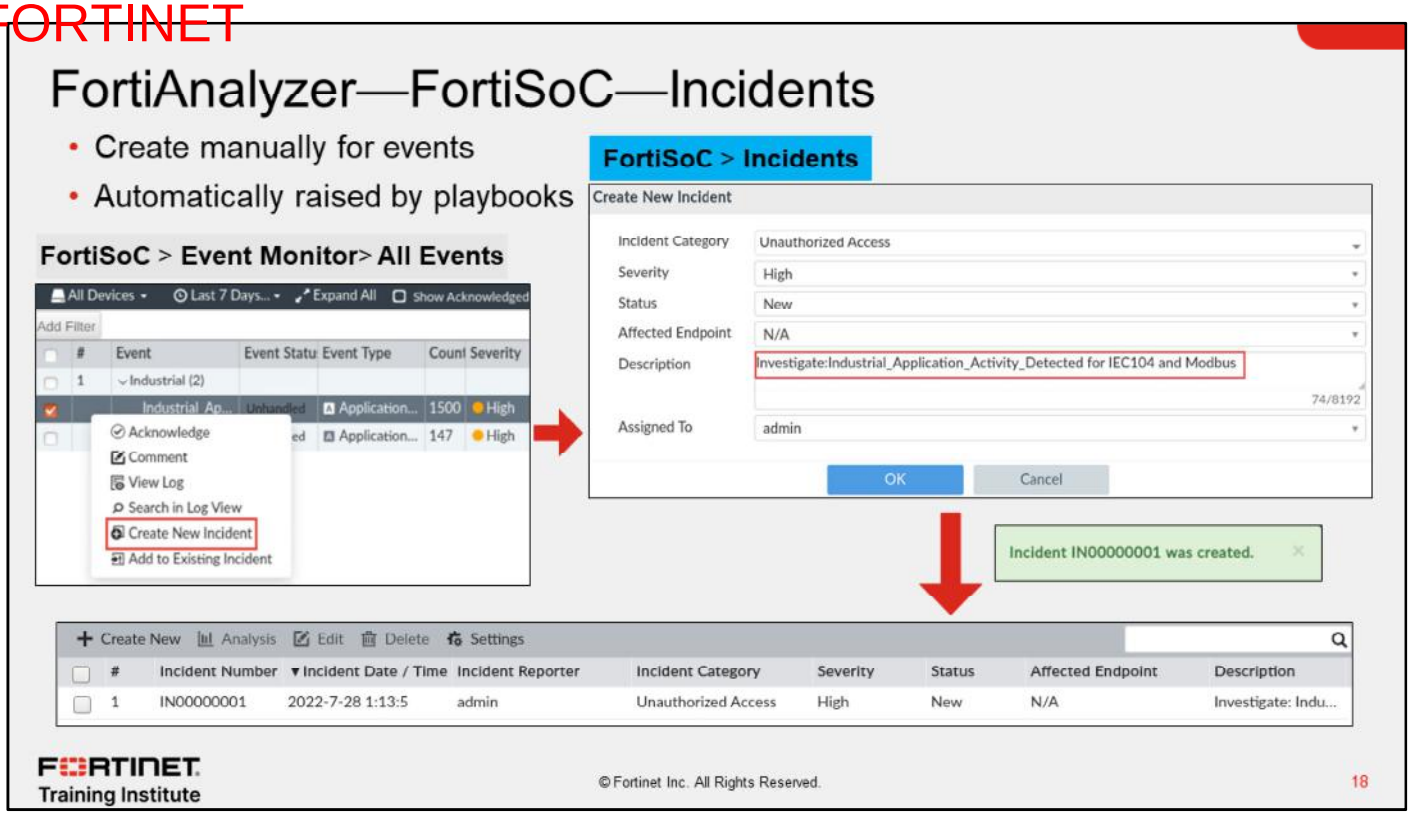
DO NOT REPRINT
© FORTINET



You can set automated responses for OT security events using playbooks. You can perform the following tasks by using playbooks:

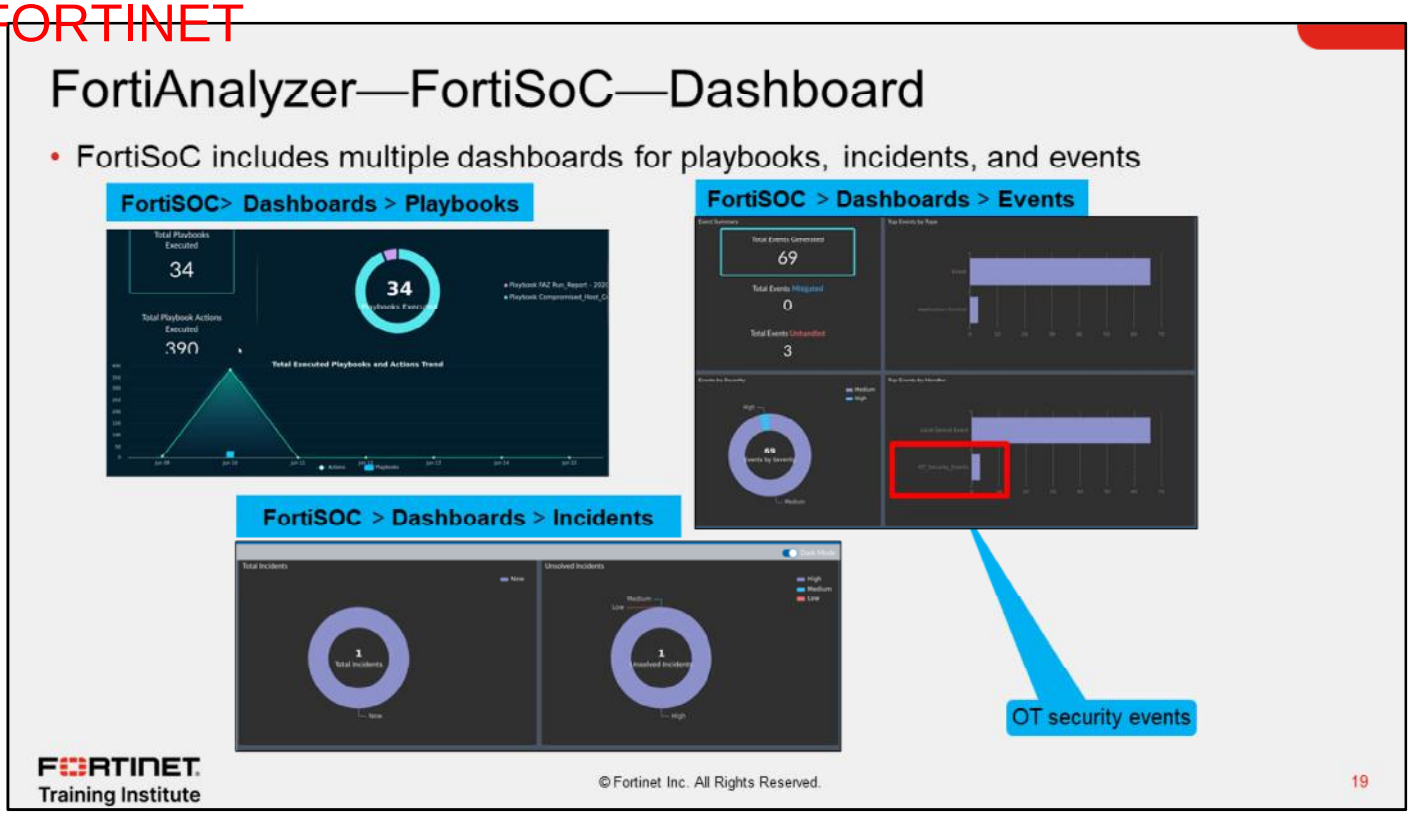
- Raise incidents
- Add security events
- Run reports and add results
- Collect threat information
- Take containment actions
- Assign incidents
- Send notifications to stakeholders
- Take remediation actions

DO NOT REPRINT
© FORTINET



You can create incidents for OT security events manually, or you can create a playbook task to raise the incident automatically.

DO NOT REPRINT
© FORTINET



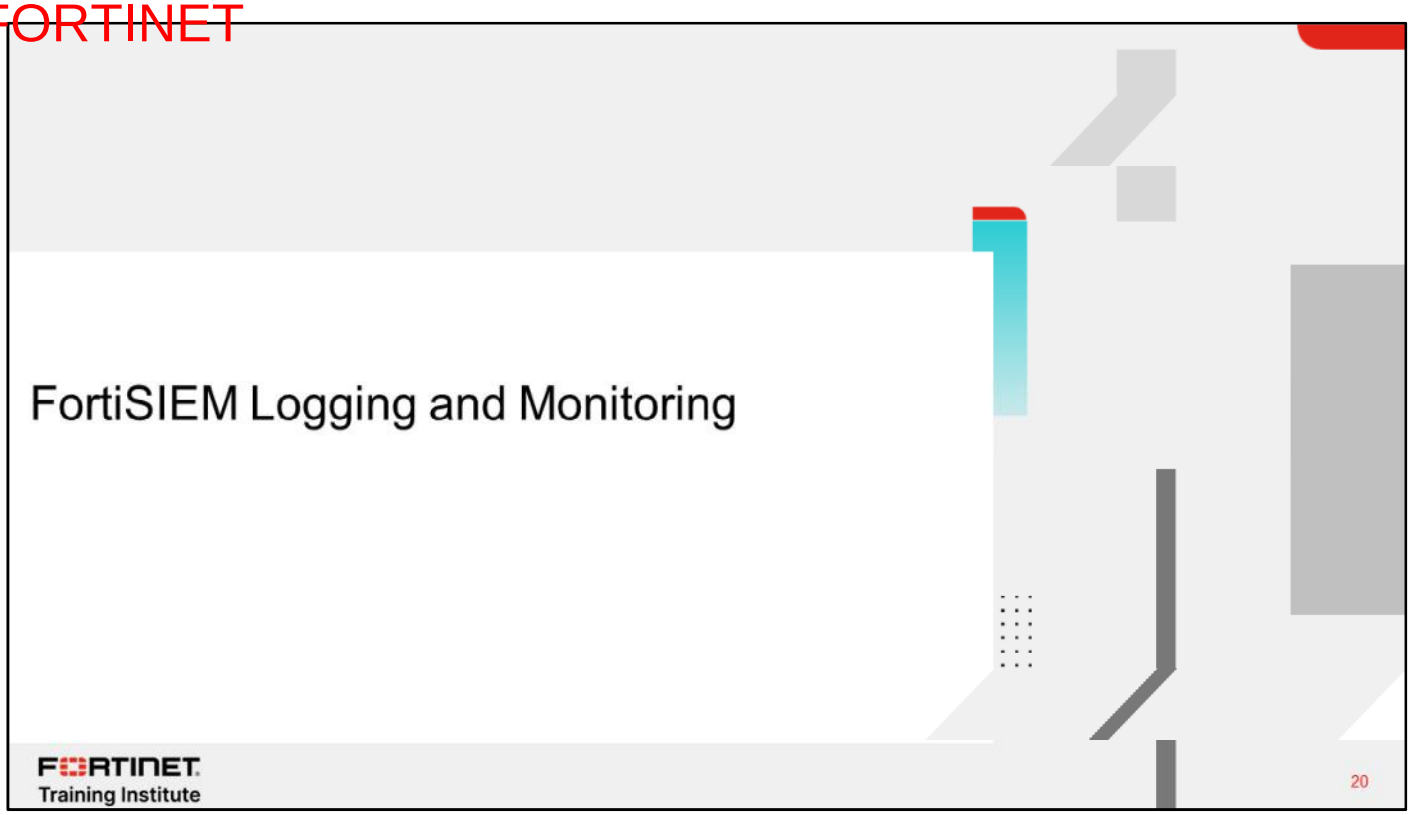
FortiSoC includes multiple dashboards for viewing information about:
- Playbooks
- Incidents
- Events

The **Playbooks** dashboard includes **Total Playbooks Executed**, **Total Playbook Actions Executed**, **Playbooks Executed**, **Overall Time Saved**, and **Total Executed Playbooks**, and **Actions**.

The **Incidents** dashboard includes **Total Incidents**, **Unsolved Incidents**, and **Incidents Timeline**.

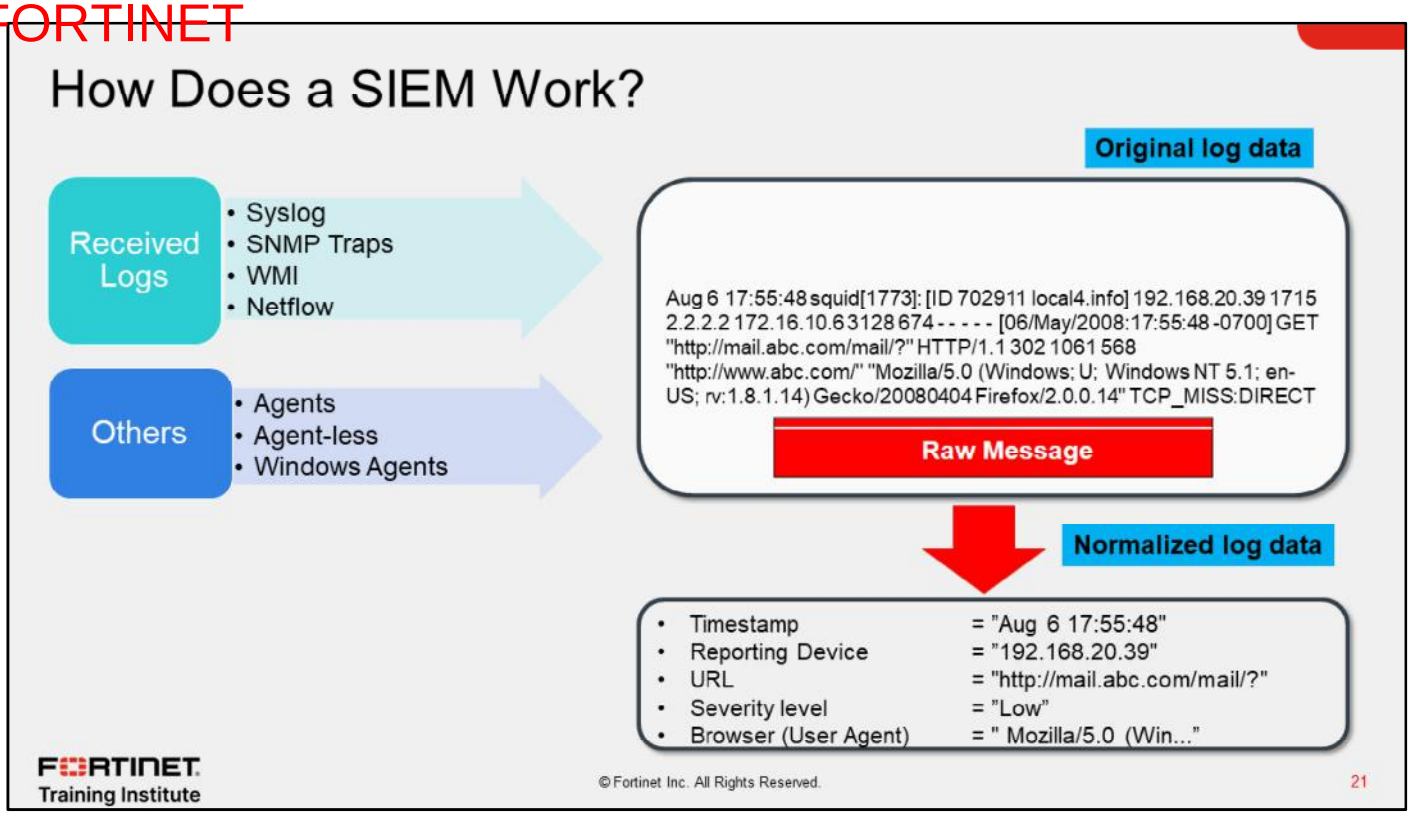
The **Events** dashboard includes **Total Events Generated/Mitigated/Unhandled**, **Events by Severity**, **Top Events by Type**, and **Top Events by Handler**.

DO NOT REPRINT
© FORTINET



In this section, you will learn about logging and monitoring on FortiSIEM for OT networks.

DO NOT REPRINT
© FORTINET

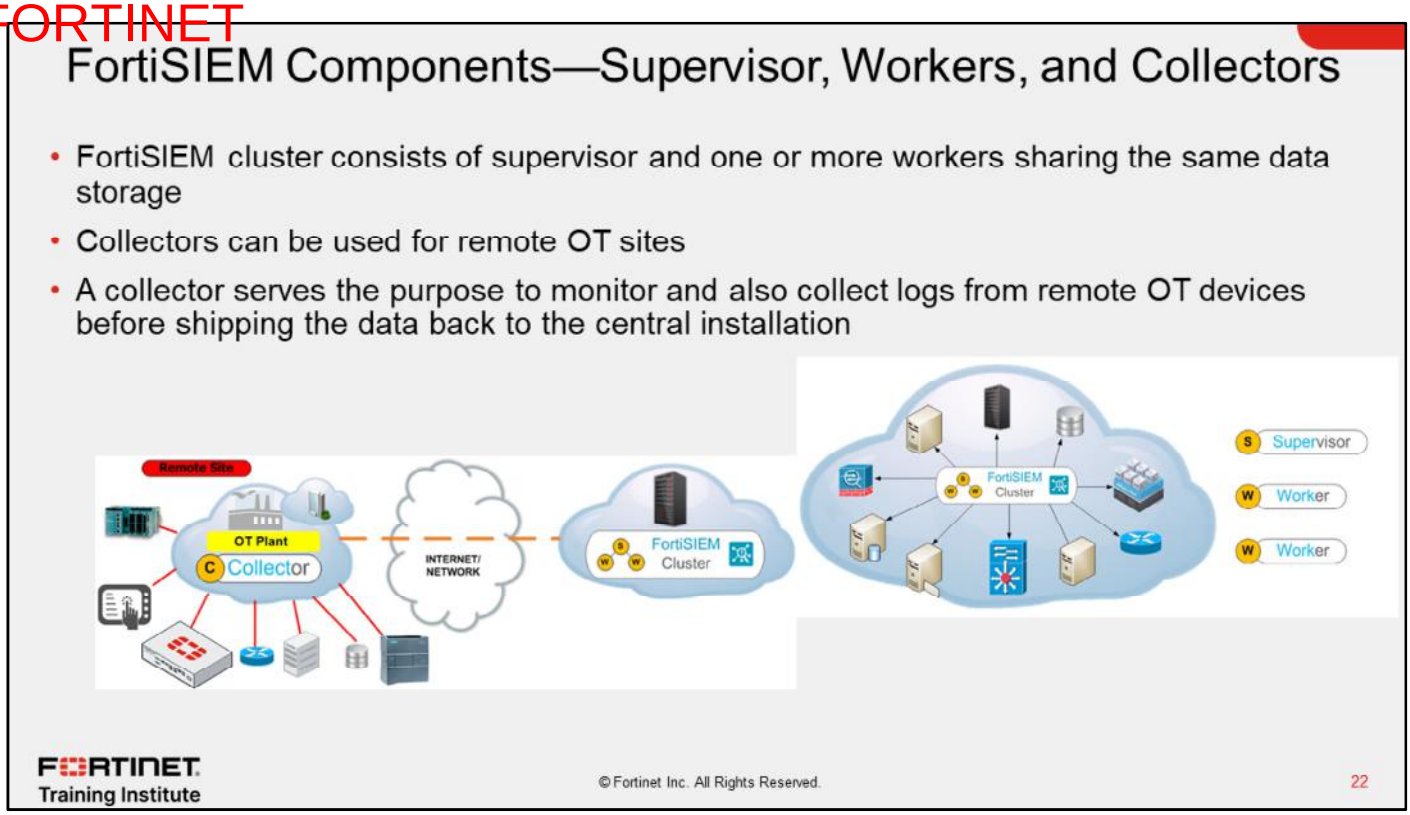


FortiSIEM receives logs from various sources, such as syslog and others. After receiving logs, FortiSIEM parses and normalizes data.

There are five primary data analysis tasks:

- Indexing the data and storing it in an event database
- Searching the data
- Correlating the data in a streaming mode to trigger rules (behavioral anomalies)
- Creating a user identity and location database for adding context to data
- Creating baselines for anomaly detection

DO NOT REPRINT
© FORTINET



FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

- For smaller deployments, FortiSIEM can be deployed in single, all-in-one hardware or virtual appliance that contains full functionality of the product.
- For larger environments that need greater event handling throughput, FortiSIEM can be deployed in a cluster of supervisor and worker virtual appliances.

There are three types of FortiSIEM nodes:

- Supervisor
- Worker
- Collector

A FortiSIEM cluster consists of a supervisor and one or more workers sharing the same NFS mount or elastic search for data storage. Supervisor and worker nodes reside inside the data centre and perform data analysis functions using distributed cooperative algorithms. For scalability, each of these tasks is divided into a heavyweight worker component executed by the worker nodes, and a lightweight master component executed by the supervisor node. The supervisor node is the GUI of FortiSIEM.

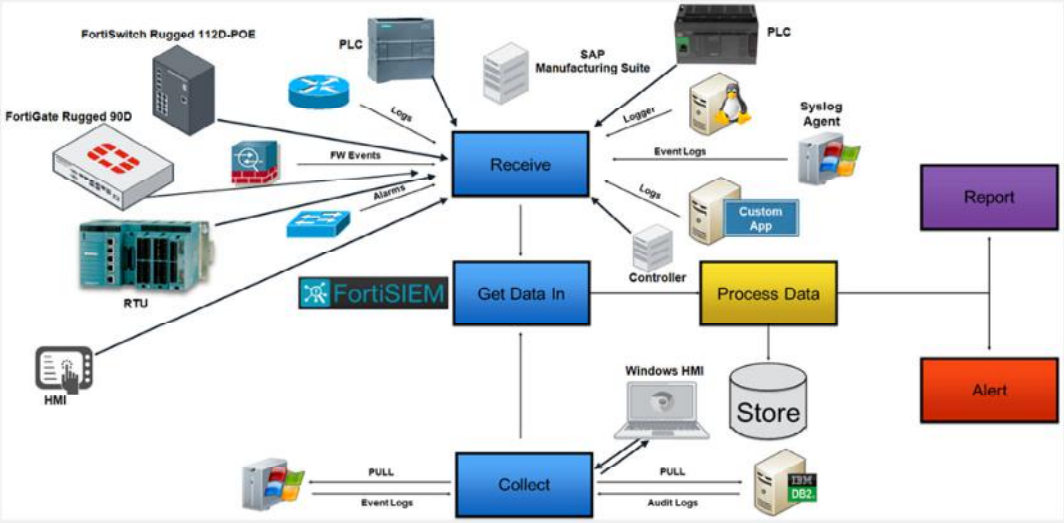
Collectors are used to scale data collection from various geographically separated network environments potentially behind firewalls. Collectors communicate to the devices, collect, parse, and compress the data and then send to the supervisor and worker nodes over a secure HTTP(S) channel in a load-balanced manner.

Collectors can be used for remote OT sites. A collector serves the purpose to monitor and also collect logs from remote OT devices before shipping the data back to the central installation. Under normal operation, data is not stored on the collector.

DO NOT REPRINT
© FORTINET

FortiSIEM Functionality

- This is a high-level view of how a traditional FortiSIEM functions



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

The primary job of a FortiSIEM is to process logs. However how do you get all of these logs into the FortiSIEM in the first place?

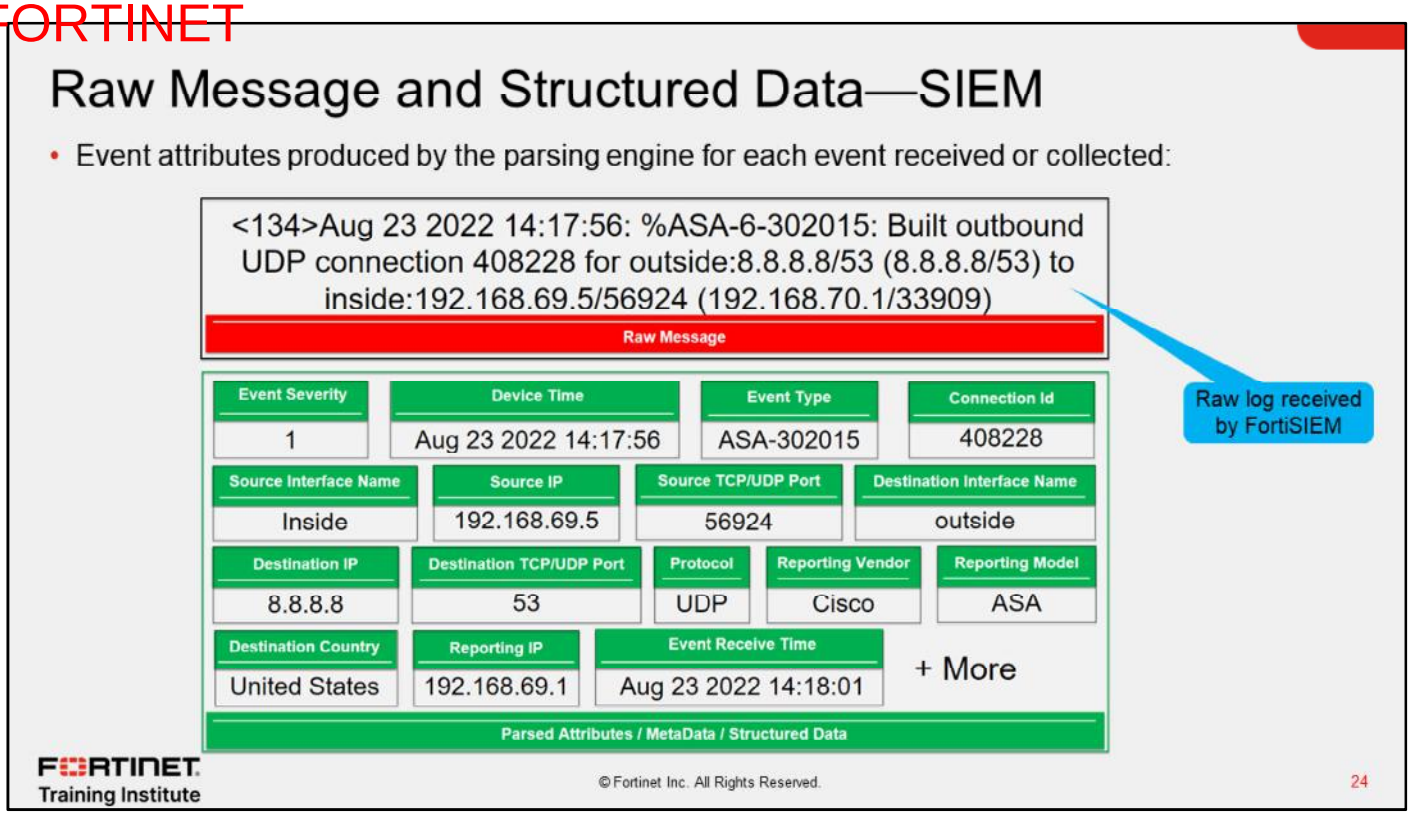
FortiSIEM either *receives* data from devices and applications, or it *collects* data from devices and applications.

Network devices, such as routers, switches, and firewalls, typically have *syslog capability*. That is, these devices have the ability to push out traffic and audit logs to a syslog collector. In a FortiSIEM network, the syslog collector is a supervisor, a worker, or a collector node.

Servers typically run a syslog daemon. This means that servers, like routers, have syslog capability. However, some servers, such as Windows servers, don't have the ability to send syslogs. You can install a syslog *agent* on these servers to give them syslog capability. The agent that you install can be a FortiSIEM agent, or a third-party agent. However, there are some types of information that you can collect without an agent. You can use the WMI protocol to pull events from Windows servers, and you can pull audit logs from databases using JDBC.

After FortiSIEM has received or collected data from the network, it processes and stores the data. At that point, you can generate reports and alerts, based on the data that FortiSEIM has collected.

DO NOT REPRINT
© FORTINET



One of the main functions of the parsing engine is to separate the entire log file into its essential elements. The parsing engine then examines each element to determine which ones hold important or useful information. It then puts all the identified information from the event into the FortiSIEM database.

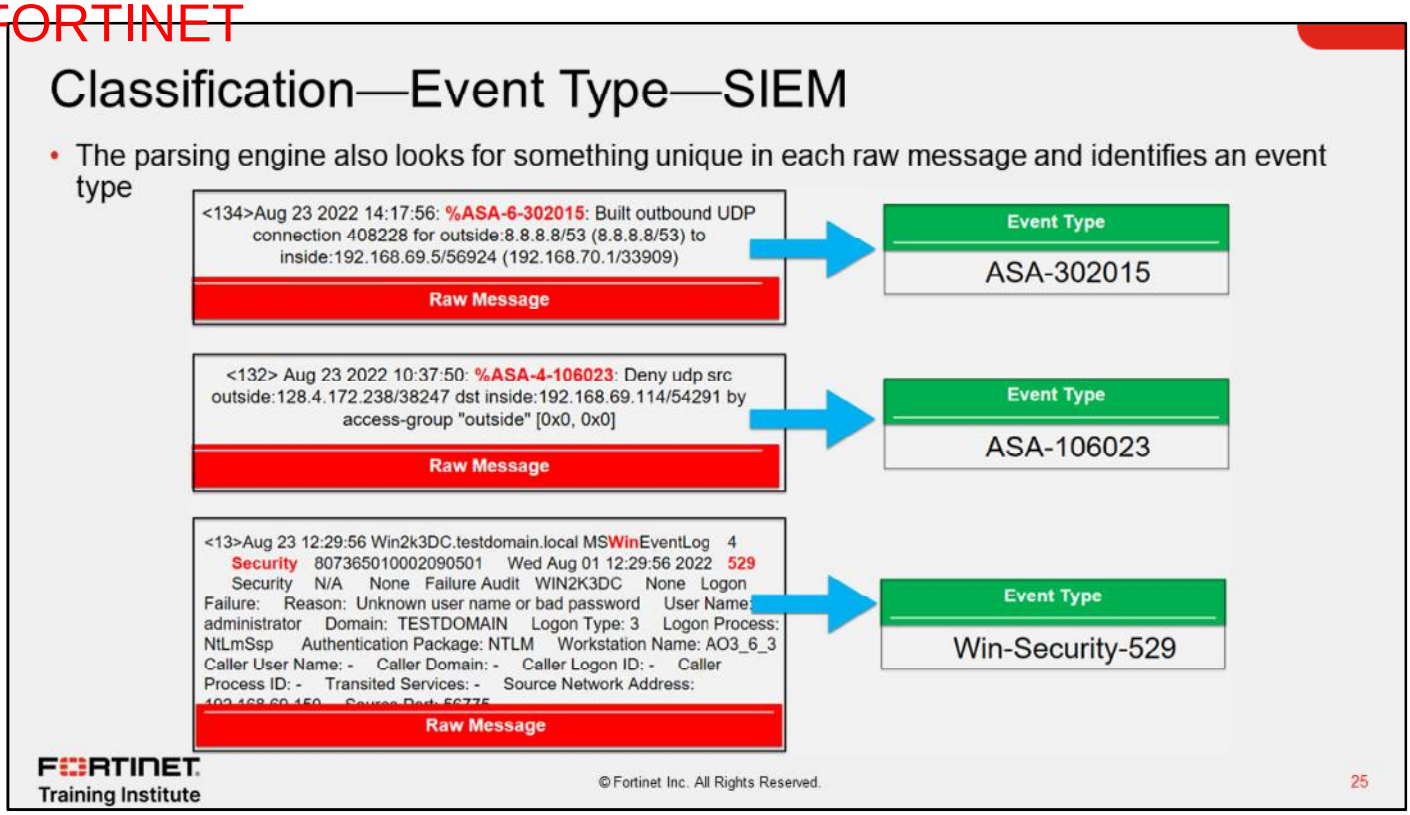
The example on this slide shows this message comes from a Cisco ASA. You can also see that there's a date, a time stamp, an interface name, and a couple of IP addresses and ports. You know the direction of the traffic was outbound, and the protocol was UDP.

For each event, whether it was received or collected, the parsing engine takes the raw message, extracts everything it can from it, and creates a normalized, structured data event from it.

Some of the attributes in the final event come from the raw message itself, such as the time the event took place on the device, the source IP address, the destination IP address, and ports. Some attributes are added by the parsing engine, such as the timestamp indicating when the event was received, and the event type. Still more attributes are added through enrichment from the CMDB database or the geolocation database, such as the destination country.

In the end, the final event is enriched with far more data than was originally sent. All of this additional data makes searching, filtering, and reporting more granular than would be possible otherwise.

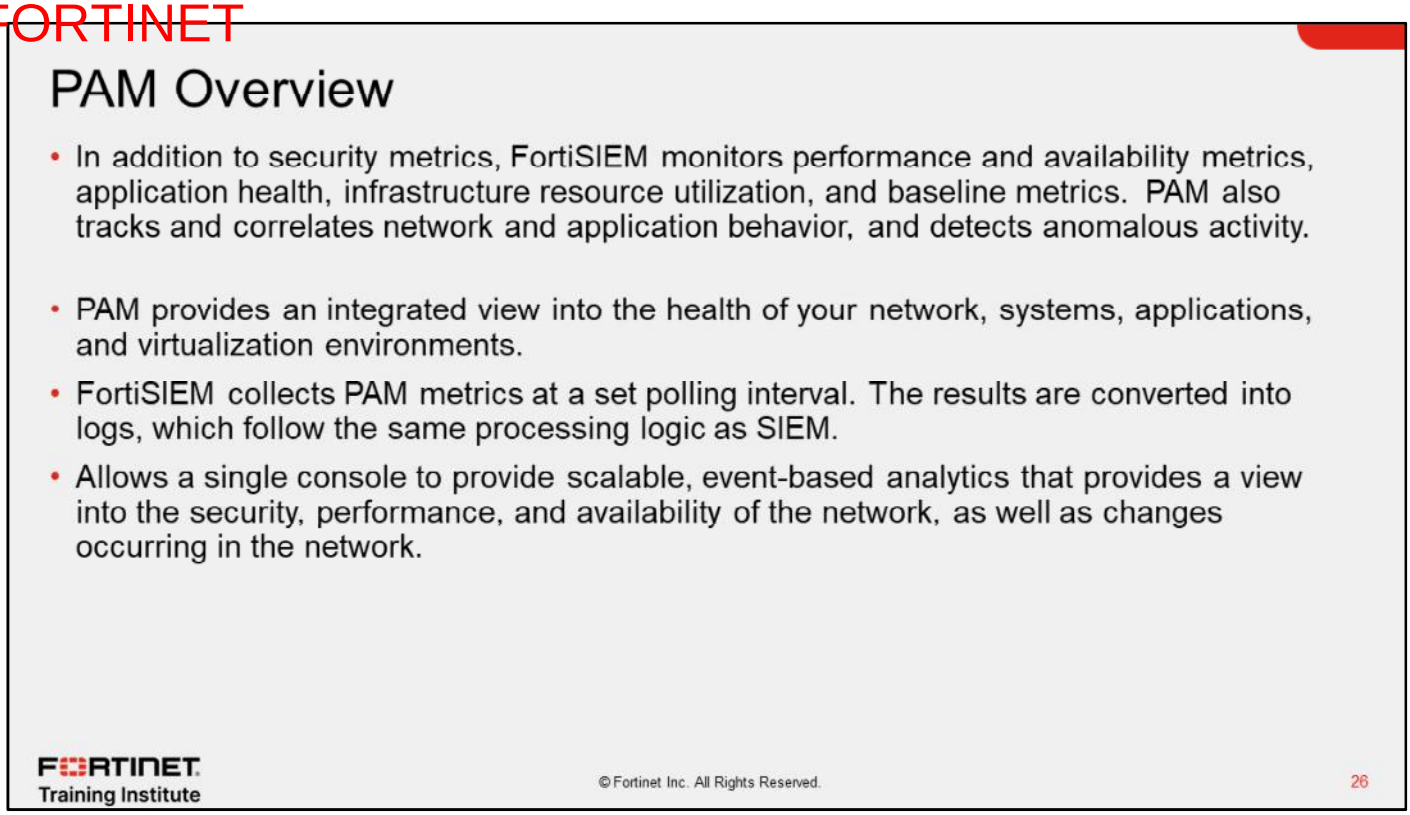
DO NOT REPRINT
© FORTINET



Another job of the parser is to give every message an event type. The parser looks for something unique in each message and assigns it an event identifier.

In the example shown on this slide, there are two different ASA messages. One message is an outbound UDP connection message, the other is a deny UDP connection message. The parser looks for unique key words in the message to identify what kind of message it is. Cisco uses unique identifying numbers in their messages, so, in this example, the parser can use those numbers to identify the event types. Windows also uses unique IDs in their event logs, which the parser can use to assign an event identifier.

DO NOT REPRINT
© FORTINET



FortiSIEM doesn't just collect security metrics, it also collects performance and availability information, from devices and applications.

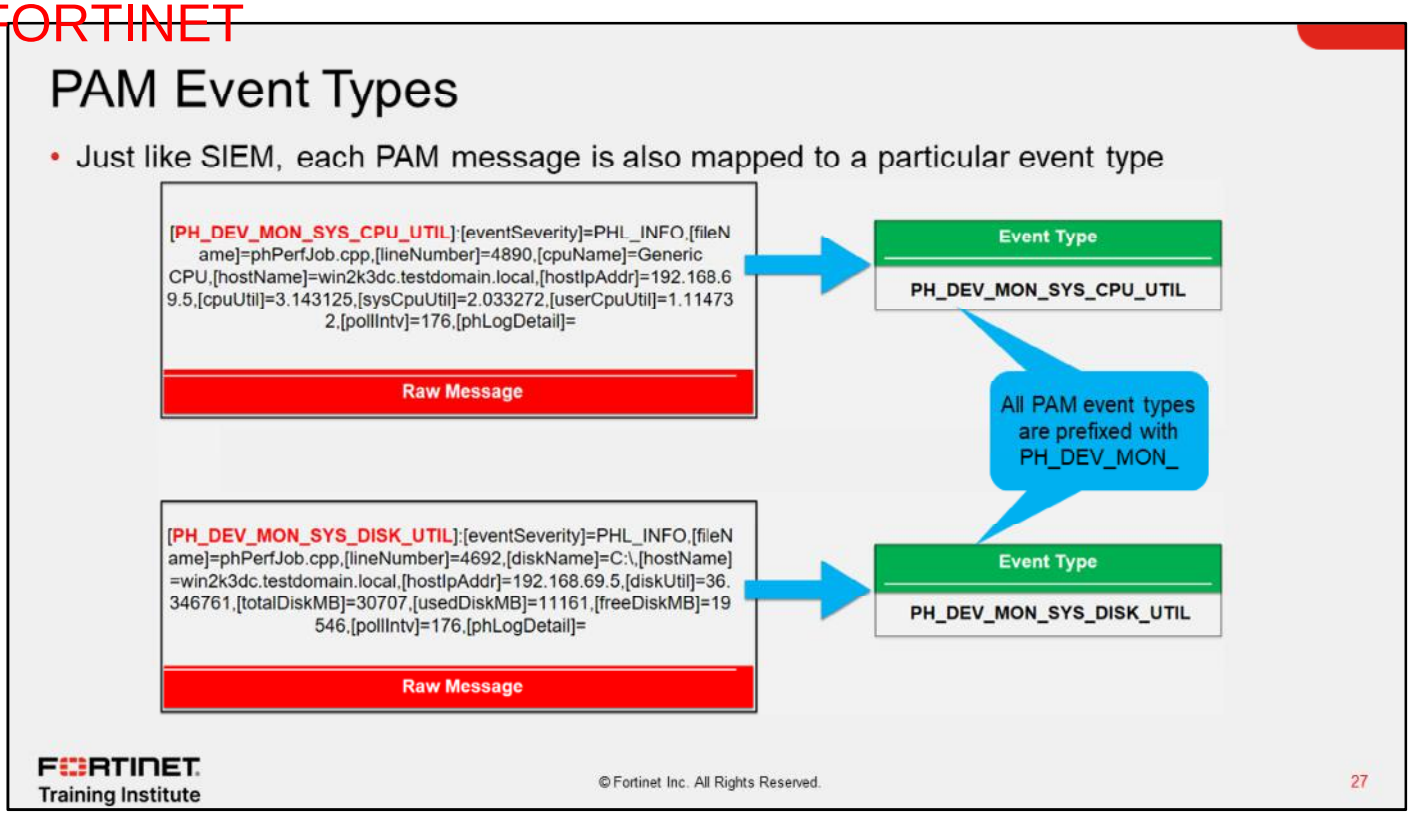
FortiSIEM performance and availability management (PAM), provides an integrated view into the health of your network, systems, applications, and the virtualization environment.

Using all of this information, FortiSIEM builds a baseline of the network and application behaviors. Then, by continuously comparing what is currently happening in the network against the baseline, FortiSIEM can detect anomalous activity.

FortiSIEM collects the performance metrics at a set polling interval, and converts the metrics into logs following the same processing logic that is used for SIEM data.

This process allows a single console to provide scalable, event-based analytics that provide a view into the security, performance, and availability of the network, as well as changes occurring in the network.

DO NOT REPRINT
© FORTINET



Just like SIEM, each PAM message is also mapped to a particular event type.

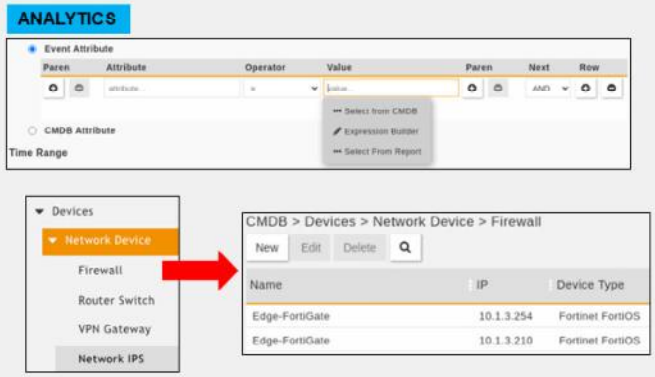
The example on this slide shows a system CPU utilization event and a disk utilization event, each mapped to a different event type.

All performance events have the prefix of `PH_DEV_MON`, which means a device monitoring event, or, put another way, an event derived from a performance monitoring poll.

DO NOT REPRINT
© FORTINET

Analytics—Search Operators and CMDB Lookups

Search Operator	Meaning
=	Equal (exact match)
!=	Not equal to
<	Smaller than
<=	Smaller than or equal
>	Greater than
>=	Greater than or equal
BETWEEN	Between two values
NOT BETWEEN	Not between two values
IN	In this list of value 1, value 2, value N
NOT IN	Not in this list of value 1, value 2, value N
CONTAINS	Contains this keyword
NOT CONTAINS	Does not contain this keyword
IS [NULL]	Is a null value, that is, the value is empty
IS NOT [NULL]	Is not a null value, that is, populated with a value
REGEX	Matches this regex pattern
NOT REGEX	Does not match this regex pattern



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

You can use many different operators in a structured search to filter events and extract the events you are searching for.

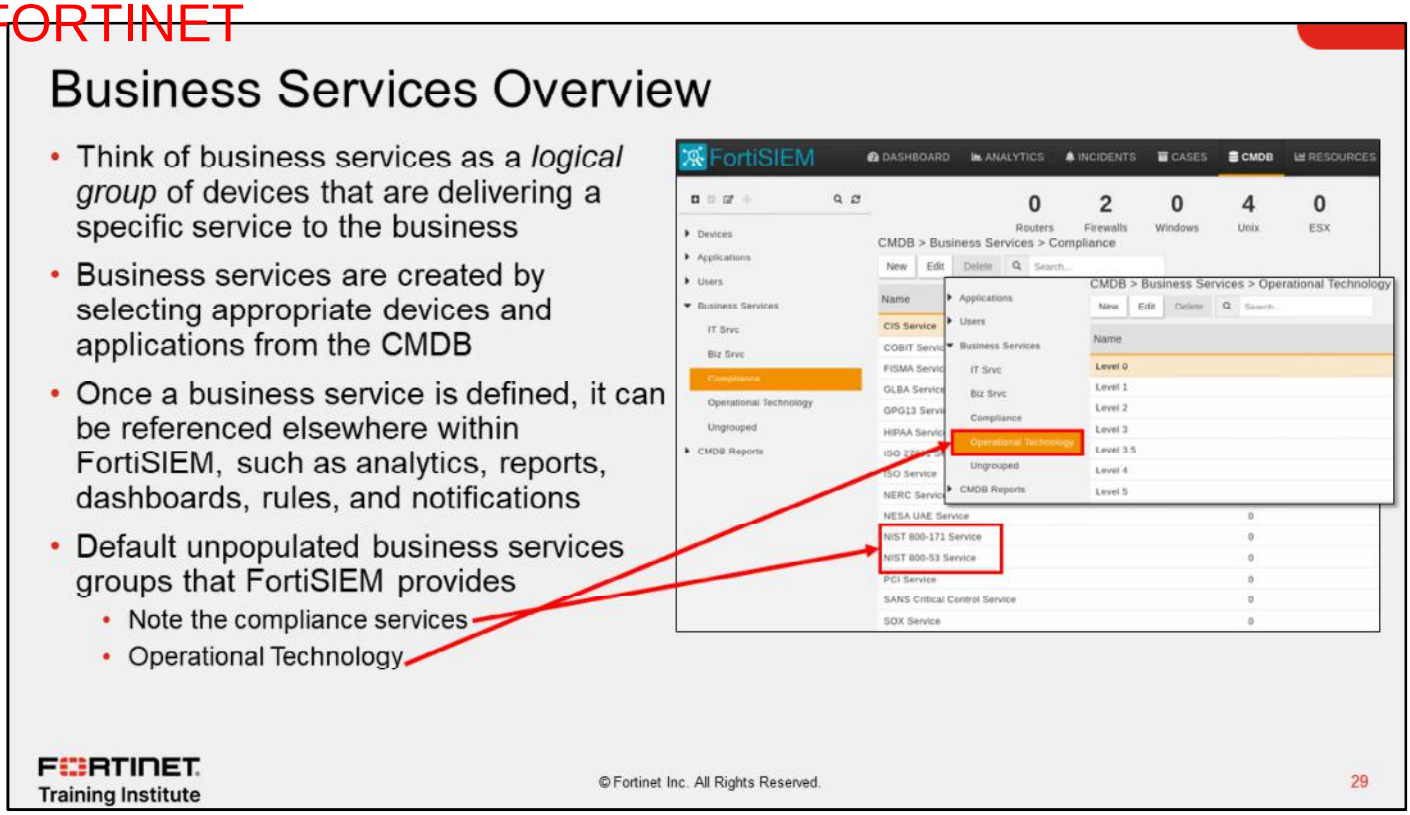
What if you want to list the events that come from all of your organization's firewalls? It's not uncommon for an organization to use firewall devices from different vendors. So, you could create a search that has conditions for each type of firewall in your network.

CMDB groups your devices into different categories, and FortiSIEM analytics allows you to reference the CMDB when building conditions in a structured search. So, you need to create only one condition that references the firewall group in the CMDB to search all of your organization's firewalls.

The condition would read something like the following: The **Reporting IP** address is **IN** the **Firewall** CMDB group, or The **Reporting IP** is **IN** the **Server** CMDB group.

The CMDB lookup option becomes available only when you are using the equal to, not equal to, in, and, not in operators.

DO NOT REPRINT
© FORTINET



In FortiSIEM, a business service can be thought of as a *logical group* of devices that are delivering a specific service to the business.

Business services are created by selecting appropriate devices and applications from the CMDB.

FortiSIEM also provides some unpopulated default groups such as the firewall business service, authentication business service, and VPN business service in which administrators can manually define which of their devices belong to those services.

After an administrator defines a service, it can be referenced elsewhere within FortiSIEM, such as analytics, reports, dashboards, rules, and notifications.

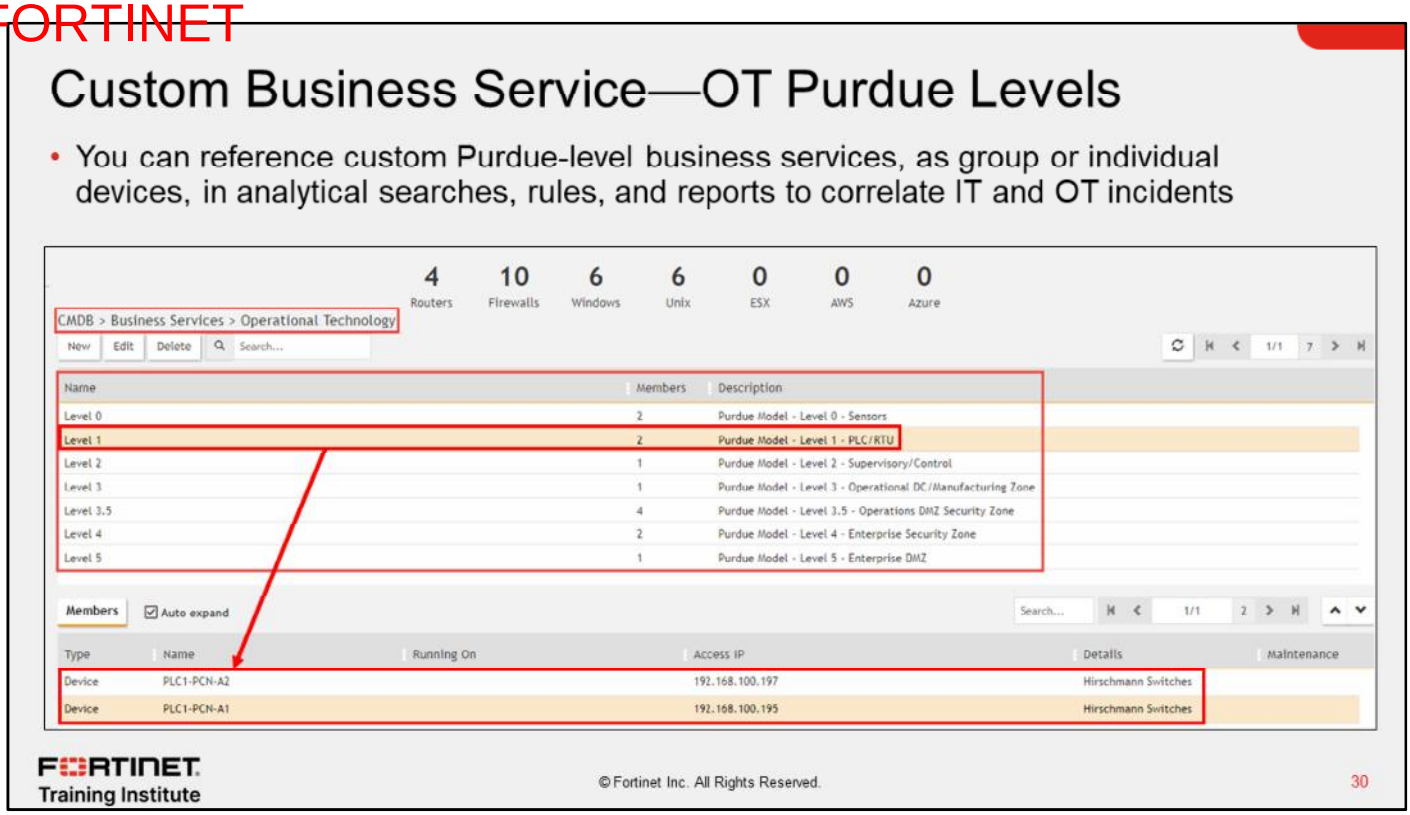
FortiSIEM provides a number of unpopulated default business services groups, and it includes an operational technology group.

As you can see, there are a few services for compliance purposes, such as NIST 800-171-service, NIST 800-53 service, FISMA services, HIPPA, GPG13, NERC, PCI, and there is a predefined business service group for OT.

The OT business service group includes subgroups for each level based on the Purdue model.

Any administrator can manually add devices, such as firewalls to the firewall service, DHCP and DNS servers to the DHCP/DNS services, or any of your PCI devices to the PCI service, and so on.

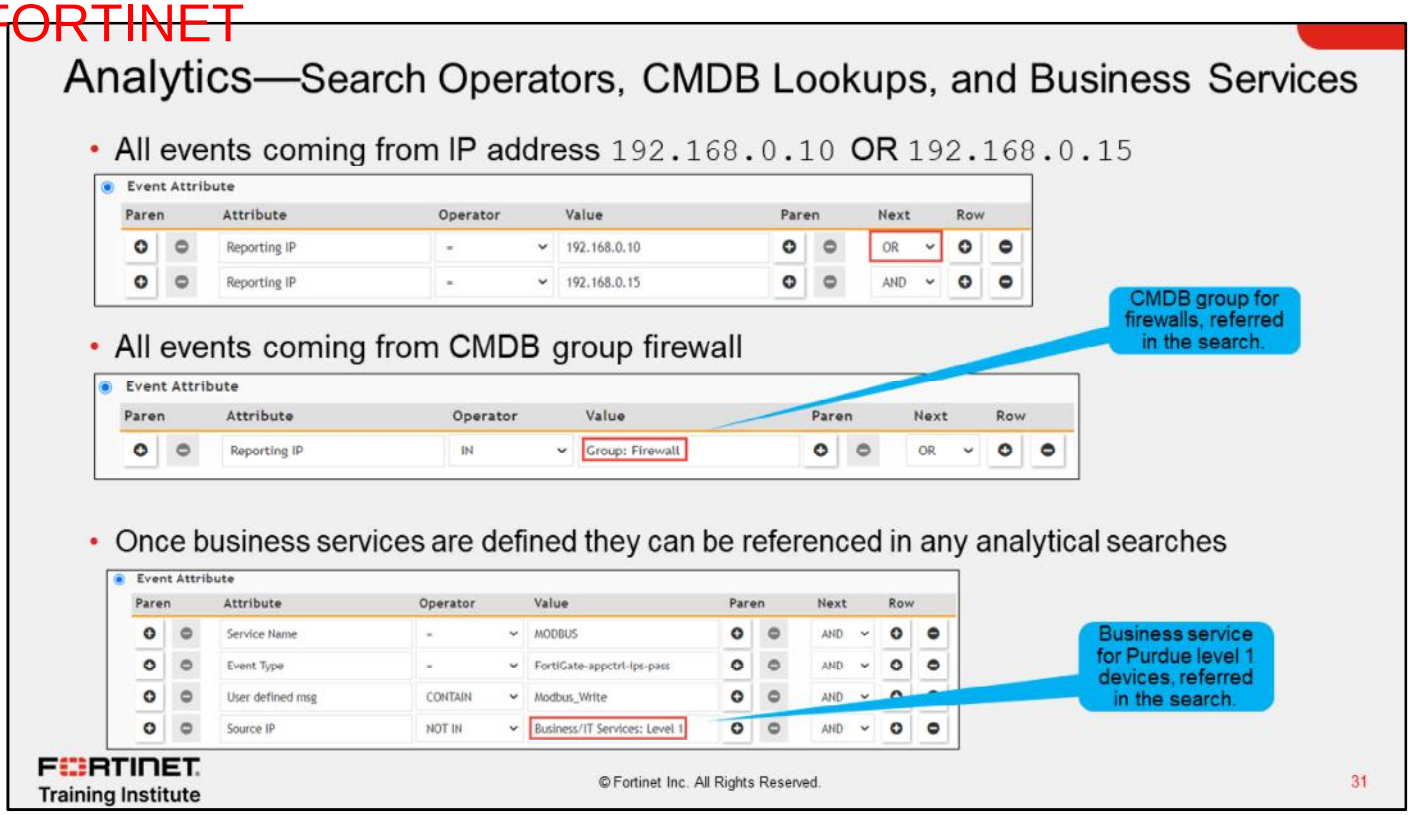
DO NOT REPRINT
© FORTINET



This slide shows an example of custom OT business services. Six groups have been created based on the Purdue model, and devices have been classified and mapped for each Purdue level using business units.

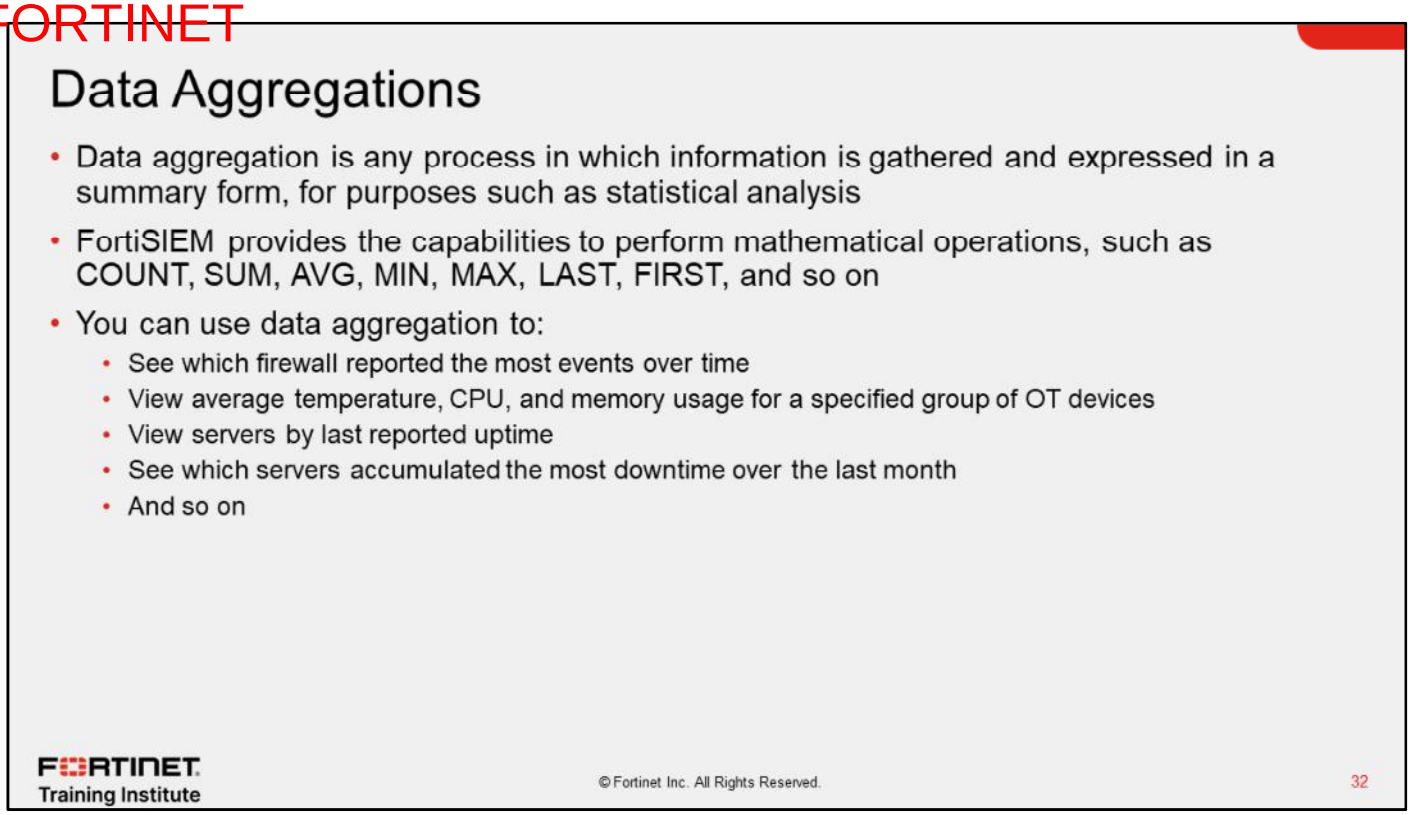
The example shown on this slide lists Purdue level 1 devices, **PLC1-PCN-A1**, and **PLC1-PCN-A2**. You can reference these Purdue-level business services, as group or individual devices, in analytical searches, rules, and reports to correlate IT and OT incidents.

DO NOT REPRINT
© FORTINET



This slide shows an example of searches based on search operators, CMDB lookup filters, and business services.

DO NOT REPRINT
© FORTINET



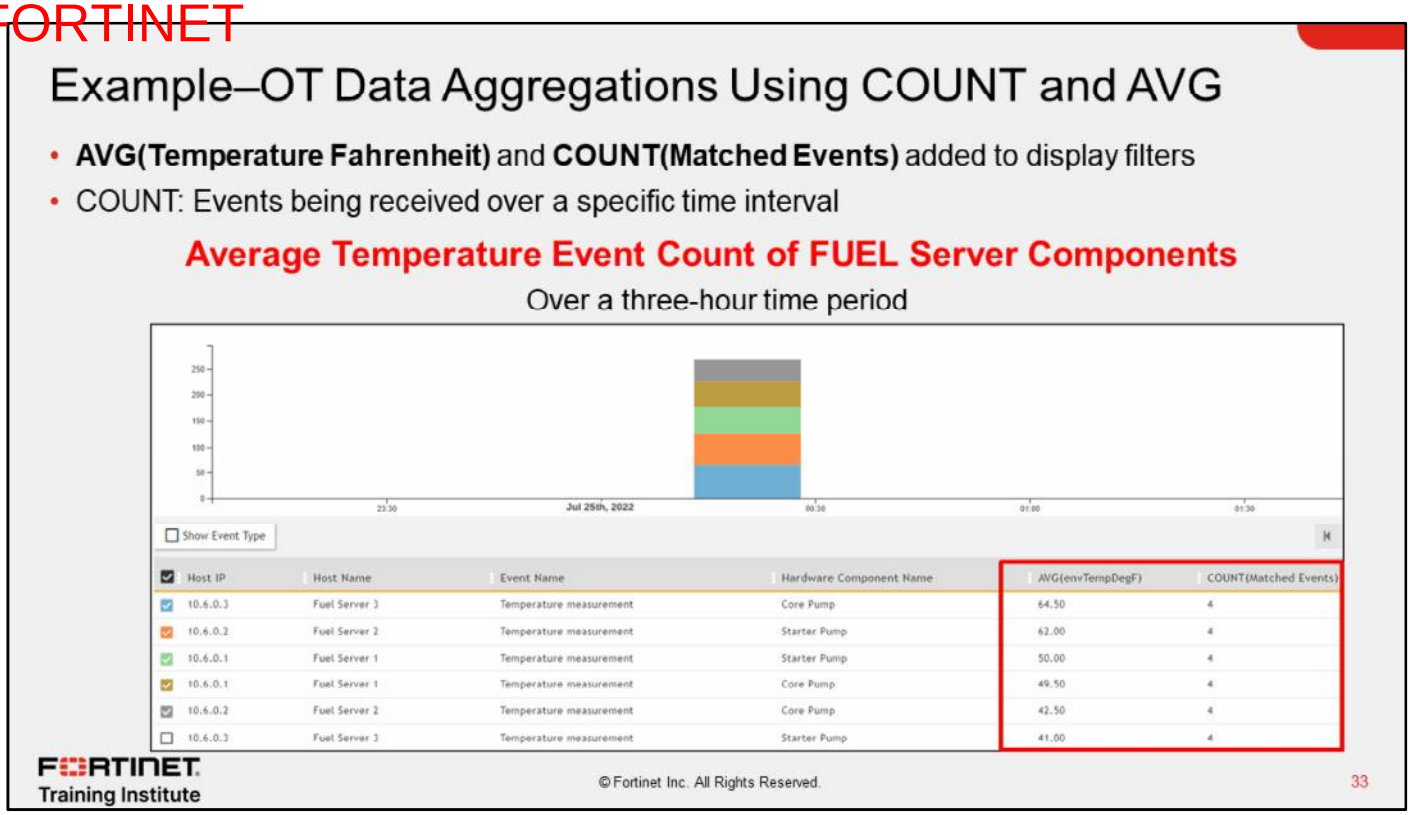
Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis.

FortiSIEM provides the capabilities to perform mathematical operations, such as COUNT, SUM, AVG, MIN, MAX, LAST, FIRST, and so on.

You can use data aggregation to:

- See which firewall reported the most events over time
- View average temperature, CPU, and memory usage for a specified group of OT devices
- View servers by last reported uptime
- See which servers accumulated the most downtime over the last month
- And so on

DO NOT REPRINT
© FORTINET



Now, you will look at an example determining average temperature metrics. In the example shown on this slide, you can see a series of events with performance metrics.

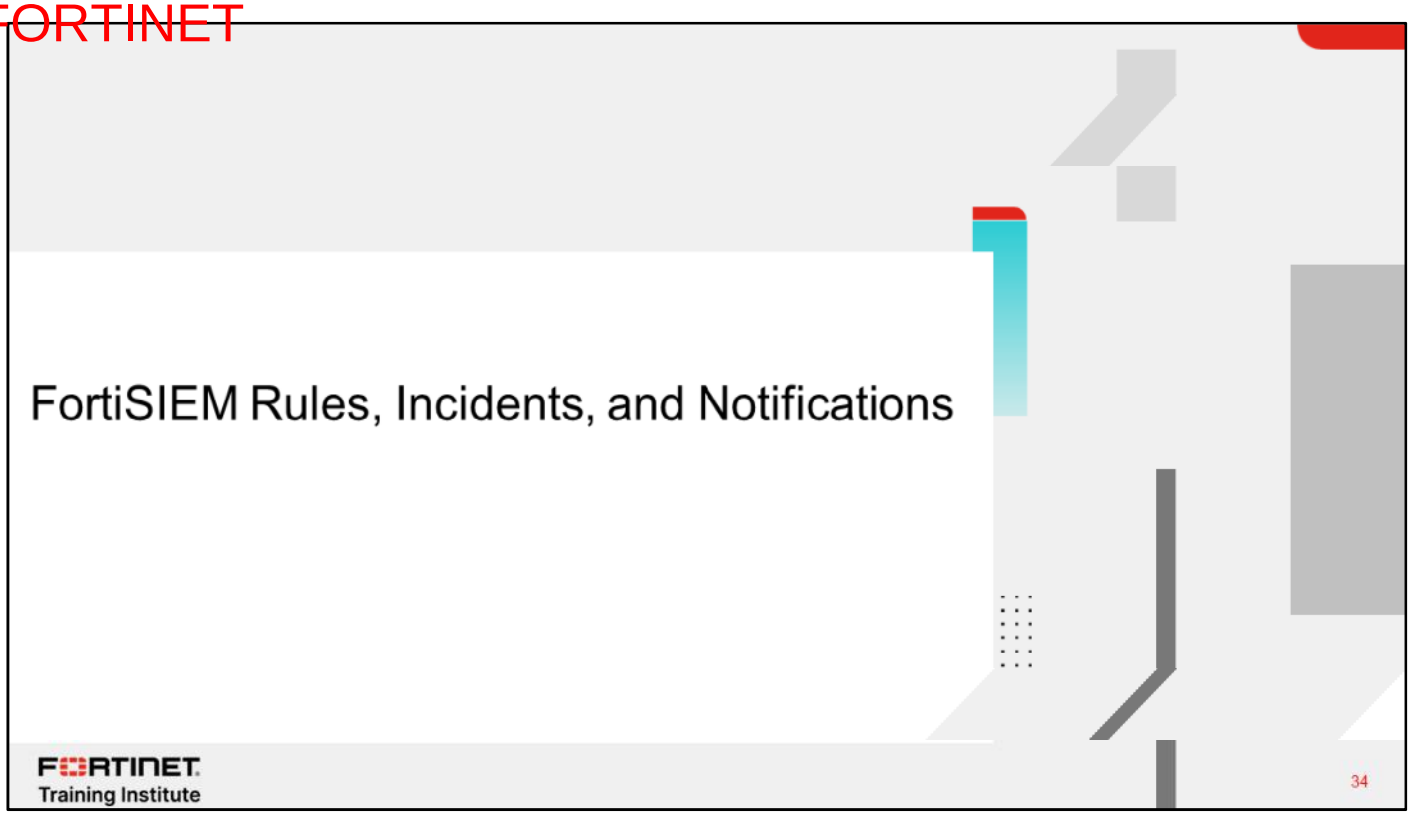
The events are being polled every three minutes, and the values for each event were taken when the event was polled.

This information, as it is, is not very useful. So how can you see the average temperature count values reported for fuel server systems?

Set up a structured query for the host IP and event type temperature over a three-hour period. Then, in the **Display Fields** section for **Group By**, select the attributes **Host IP, Host Name**, **Event Type**, **Hardware Component Name**. Add the aggregation function expressions **AVG** for the **Temperature Fahrenheit** attribute, and expression for **COUNT (Matched Events)**.

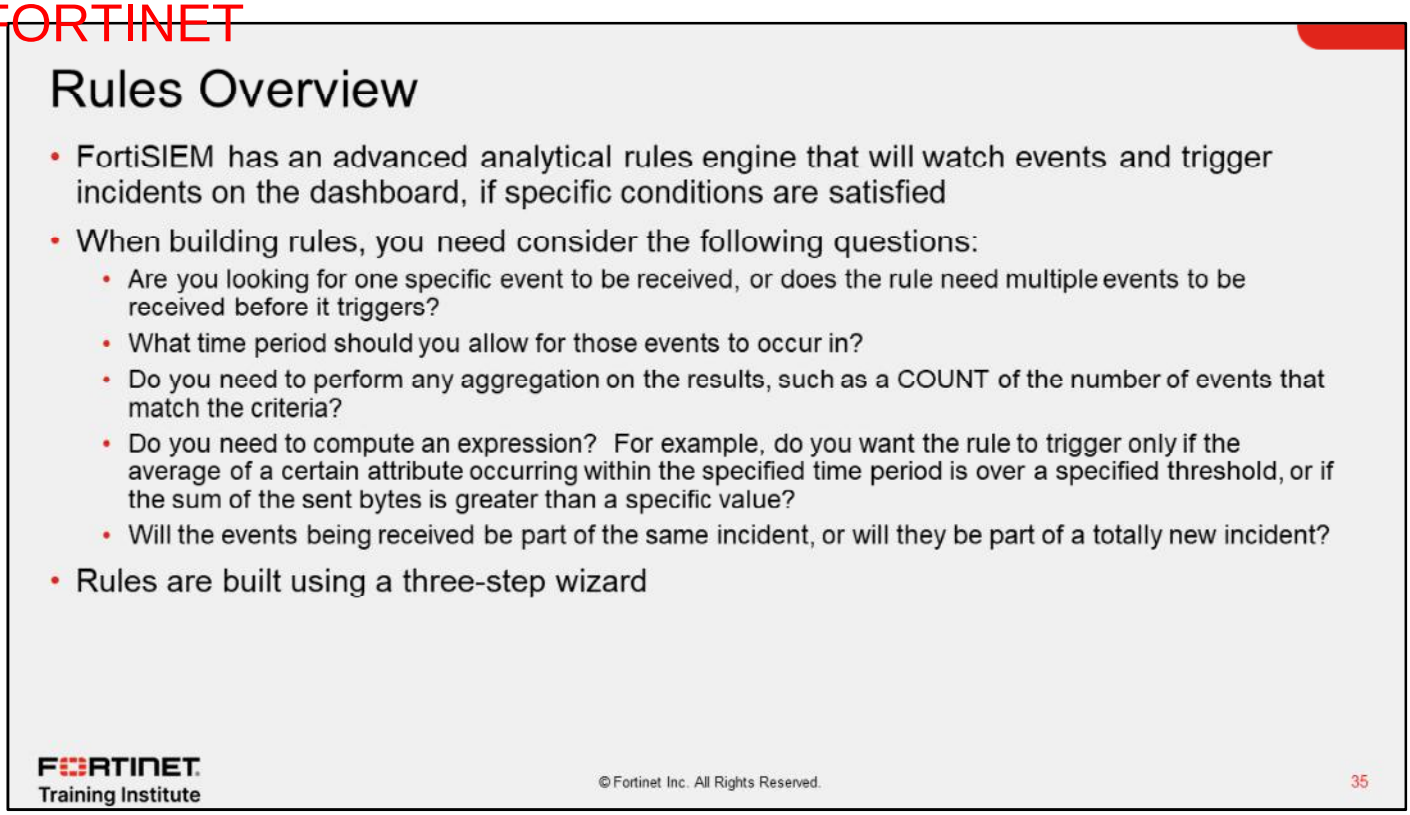
If you run the search, you will see aggregated data to display the average temperature in Fahrenheit count, for each hardware component of the fuel server.

DO NOT REPRINT
© FORTINET



In this section, you will learn about rules, incidents, and notifications on FortiSIEM for OT networks.

DO NOT REPRINT
© FORTINET

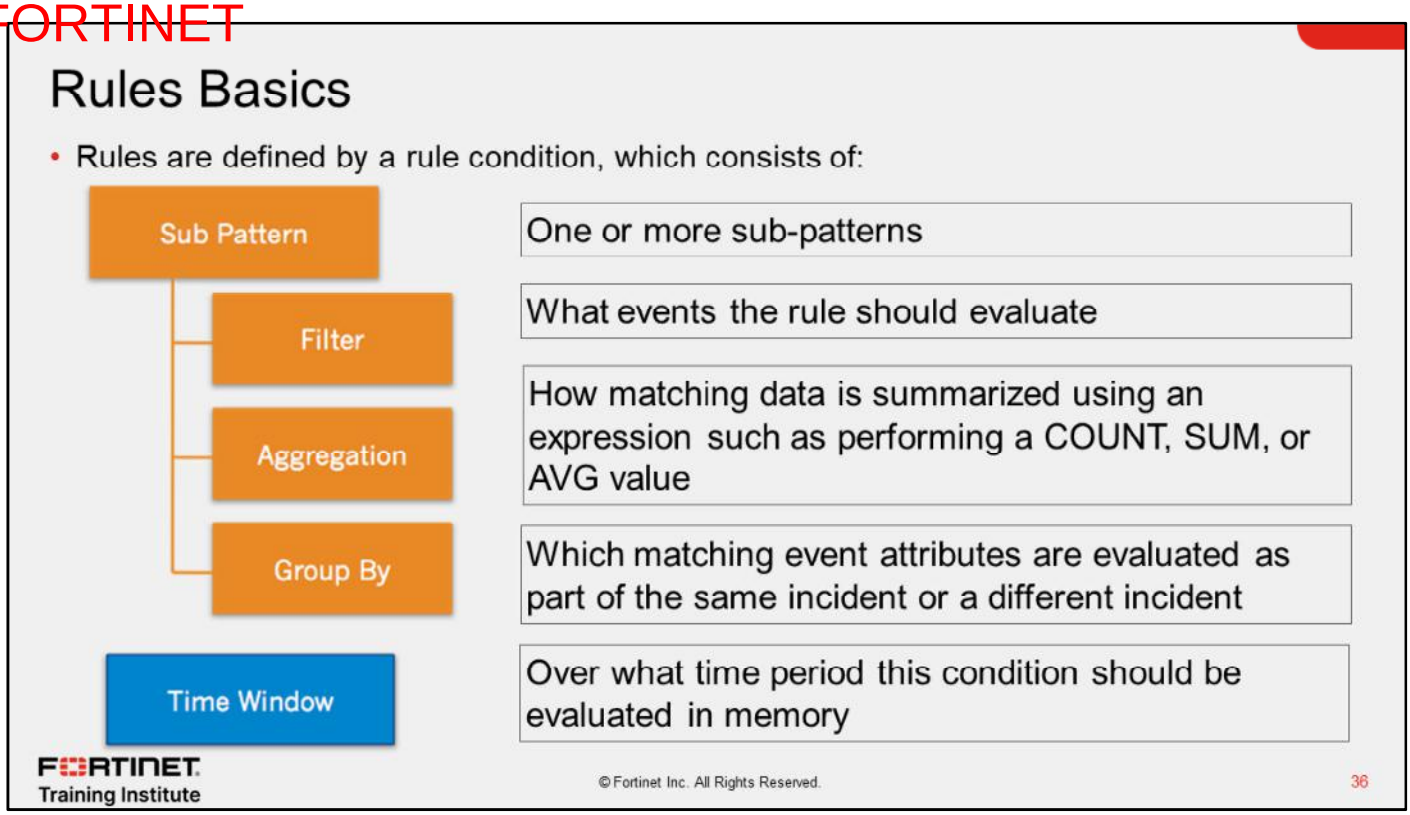


FortiSIEM has an advanced analytical rules engine that will watch events and trigger incidents on the dashboard, if specific conditions are satisfied.

When building rules you need consider the following questions:

- Are you looking for one specific event to be received, or does the rule need multiple events to be received before it triggers?
- What time period should you allow for those events to occur in?
- Do you need to perform any aggregation on the results, such as a COUNT of the number of events that match the criteria?
- Do you need to compute an expression? For example, do you want the rule to trigger only if the average of a certain attribute occurring within the specified time period is over a specified threshold, or if the sum of the sent bytes is greater than a specific value?
- Will the events being received be part of the same incident, or will they be part of a totally new incident?

DO NOT REPRINT
© FORTINET



Rules are defined by a rule condition, which consists of one or more sub-patterns.

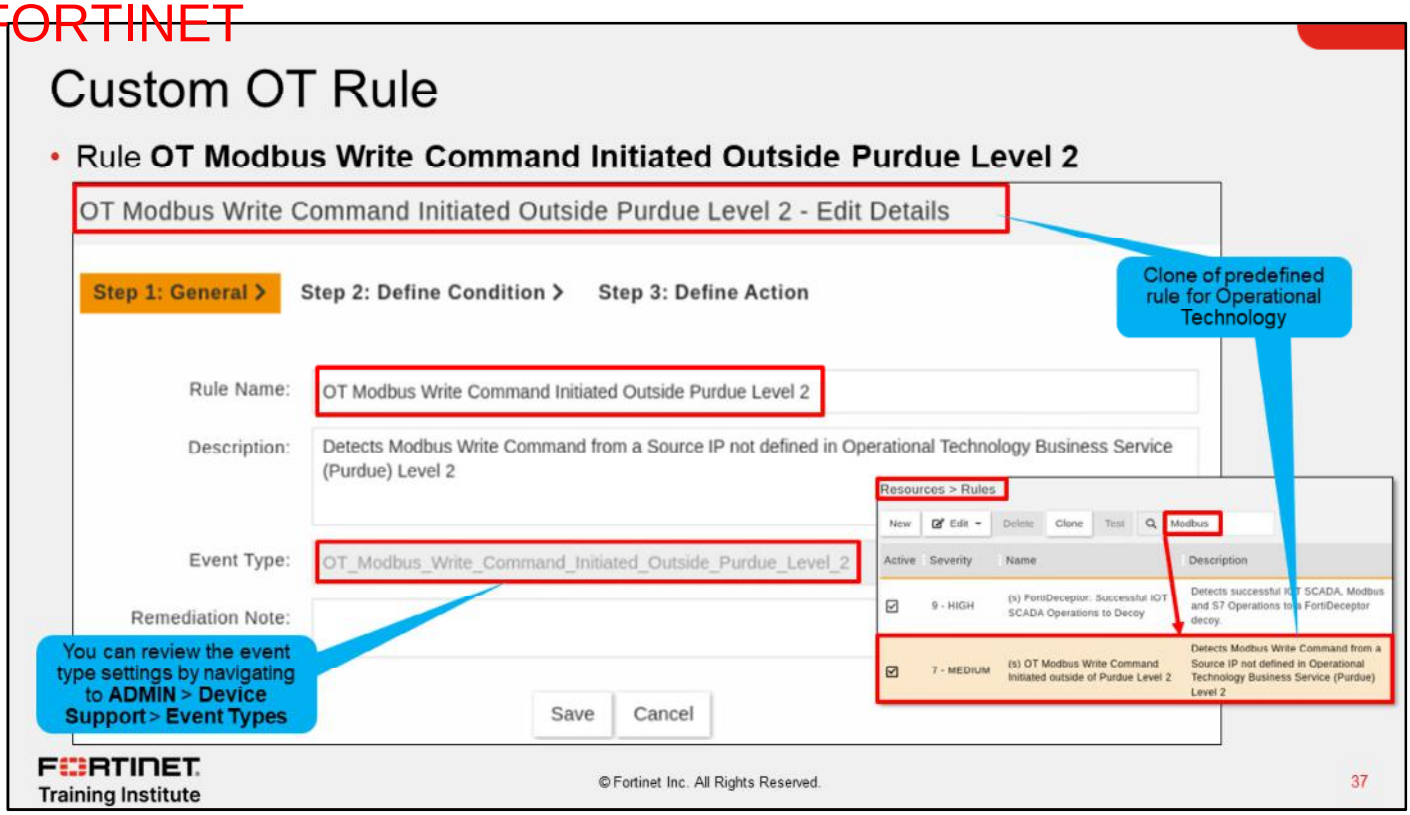
A sub-pattern is defined by filter, aggregation, and group by definitions. The filter is like a search condition. It specifies what event the rule should evaluate. For example, the rule might be looking for a particular reporting IP address, or an event type that is a logon failure.

The aggregation condition tells the rules engine how to summarize the matching data. For example, by counting the number of times a specific event occurred, adding up the values within a number of events, or calculating the average of the values.

The group by condition allows the rules engine to identify which matching event attributes are evaluated as part of the same incident, or as part of a totally different incident.

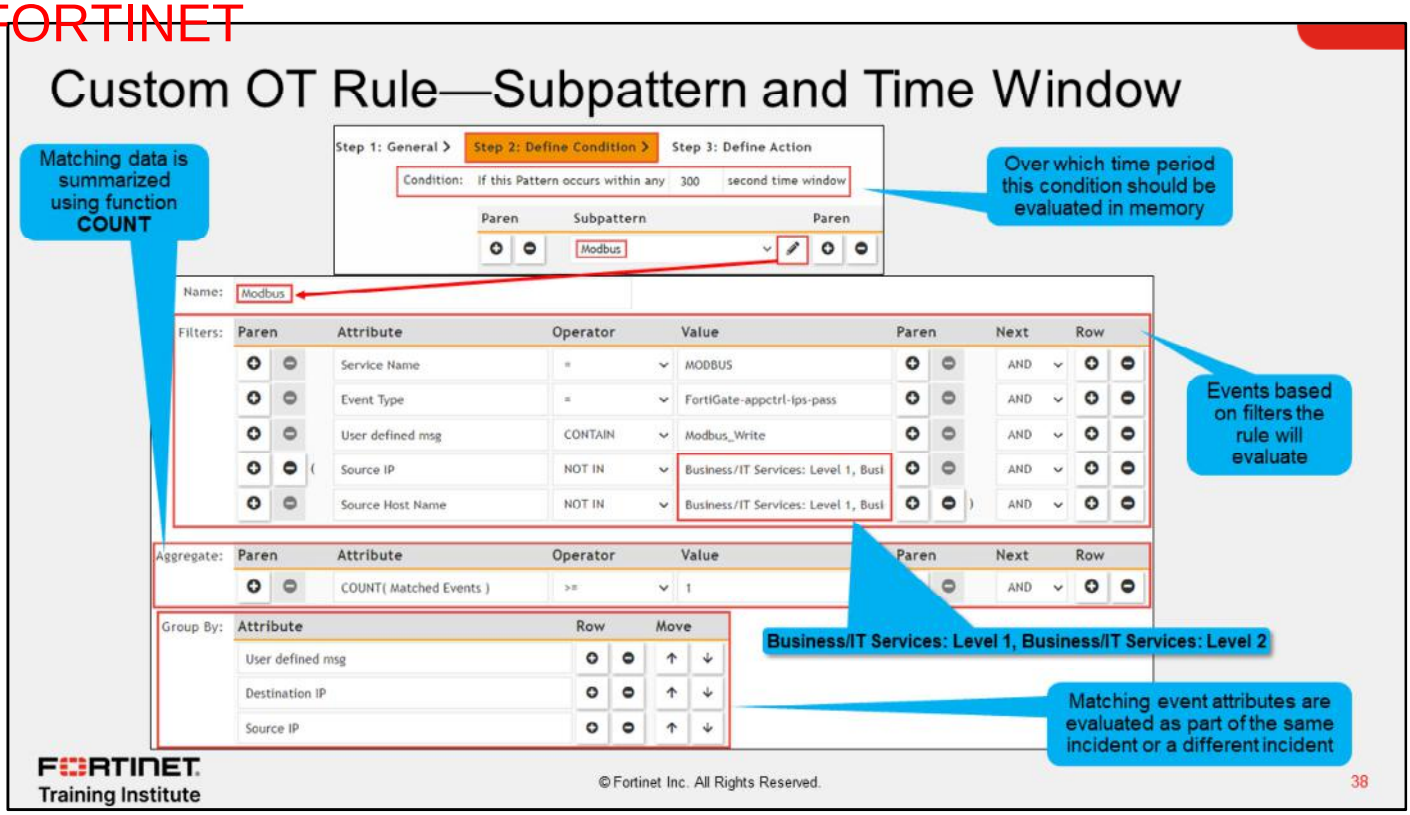
The time window tells the rules engine what time period over which this condition should be evaluated. For example, the engine could look for one or more login failures over a five-minute time period.

DO NOT REPRINT
© FORTINET



This slide shows an example of a custom rule for OT networks. The name of the rule is **OT Modbus Write Command Initiated Outside Purdue Level 2**. The rule is a clone of a predefined OT rule with a similar name. The purpose of the cloned custom rule is to detect a Modbus write command initiated outside of Purdue level 1 and 2 devices. The name you type in the **Rule Name** field is replicated in the **Event Type** field.

DO NOT REPRINT
© FORTINET



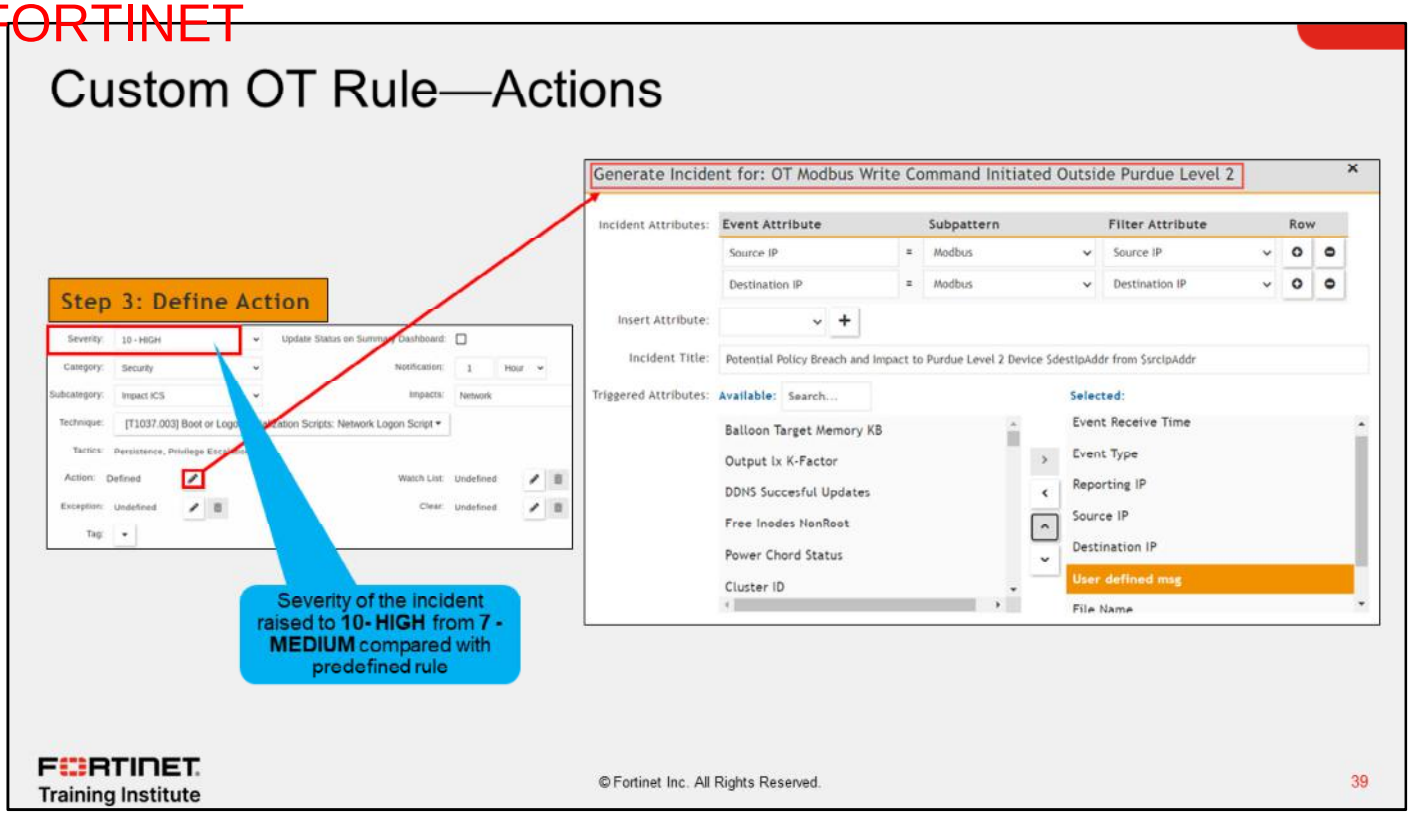
You can edit the subpattern and specify **Filters**, **Aggregate**, and **Group By** attributes.

In the example shown on this slide, the rule has a subpattern filter, which is defined by four conditions:

- In the first condition, the selected attribute is **Service Name**, the selected operator is equal to, and the value is **MODBUS**. So, this condition is looking for **Service Name** Modbus. This condition also includes the next logical operator, **AND**.
- In the second condition, the selected attribute is **Event Type**, the selected operator is equal to, and the selected value is **FortiGate-appctrl-ips-pass**. So, this condition is looking for the event type FortiGate application control with action pass. This condition also includes the next logical operator, **AND**.
- In the third condition, the selected attribute is **User defined msg**, the selected operator is **CONTAIN**, and the selected value is **Modbus_Write**. So, this condition is looking for the user-defined message, **Modbus_Write**. This condition also includes the next logical operator, **AND**.
- In the fourth condition, the selected attribute are **Source IP** and **Source Host Name**, the selected operators are **NOT IN**, and the selected value are **Business/IT Services: Level 1, Business/IT Services: Level 2**, and the condition is enclosed by parentheses. So, this condition is looking for **Source IP** and **Source Host Name** attributes not in the **Purdue level 1 and 2** business service group.
- This rule has an aggregate condition that specifies that the rule will look for one or more events that match the filter criteria over a time period defined as 300 seconds (or 5 minutes). It does this by using a **COUNT (Matched Events)** attribute, where the operator is equal to or greater than **1**.

The results should be grouped by the **User defined msg**, **Destination IP**, and **Source IP**. It is the **Group By** operation that tells the rules engine which matching event attributes to evaluate as part of the same incident, or as part of a different incident.
If event count is matched for the **Modbus_Write** command initiated from devices outside the Purdue level 1 and 2 business service group, then the rule engine will create an incident.

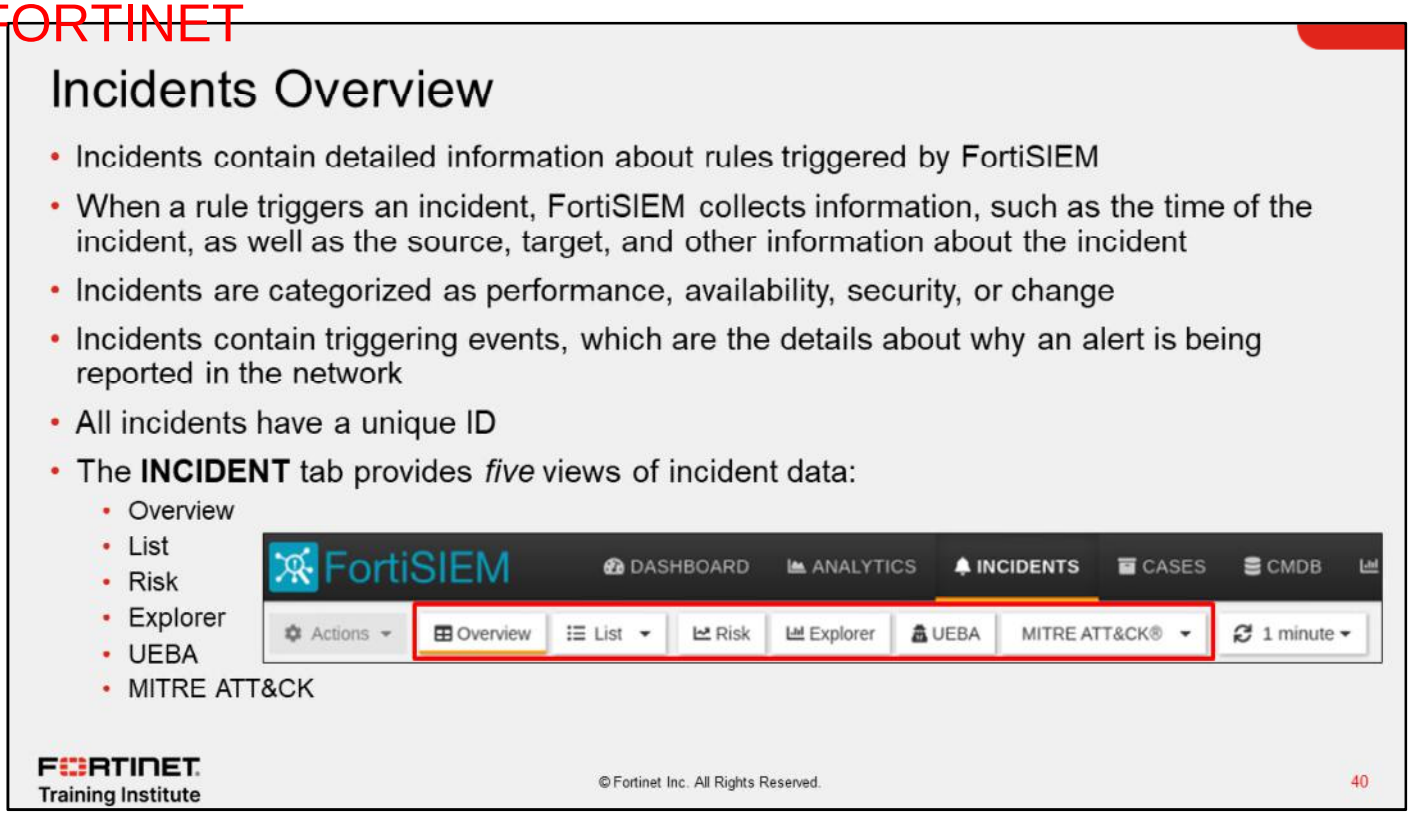
DO NOT REPRINT
© FORTINET



The third step sets the action criteria for the rule. You can select the **Severity** to associate with the incident triggered by the rule. You should select the **Category** of incidents to be triggered by the rule and the **Subcategory** from the available list, based on the selected incident **Category**.

You can configure incident attributes and triggered attributes by editing **Action**.

DO NOT REPRINT
© FORTINET



Incidents contain detailed information about rules that have been triggered by FortiSIEM. When FortiSIEM triggers a rule, it collects information, such as the time of the incident, source, target, and other information. The incident is then categorized as an incident related to performance, availability, security, or change. Incidents also contain the triggering events, which are the details about why an alert is being reported in the network.

All incidents have a unique ID.

When a correlation rule triggers, an incident is created in FortiSIEM. This section describes how to view and manage incidents in FortiSIEM.

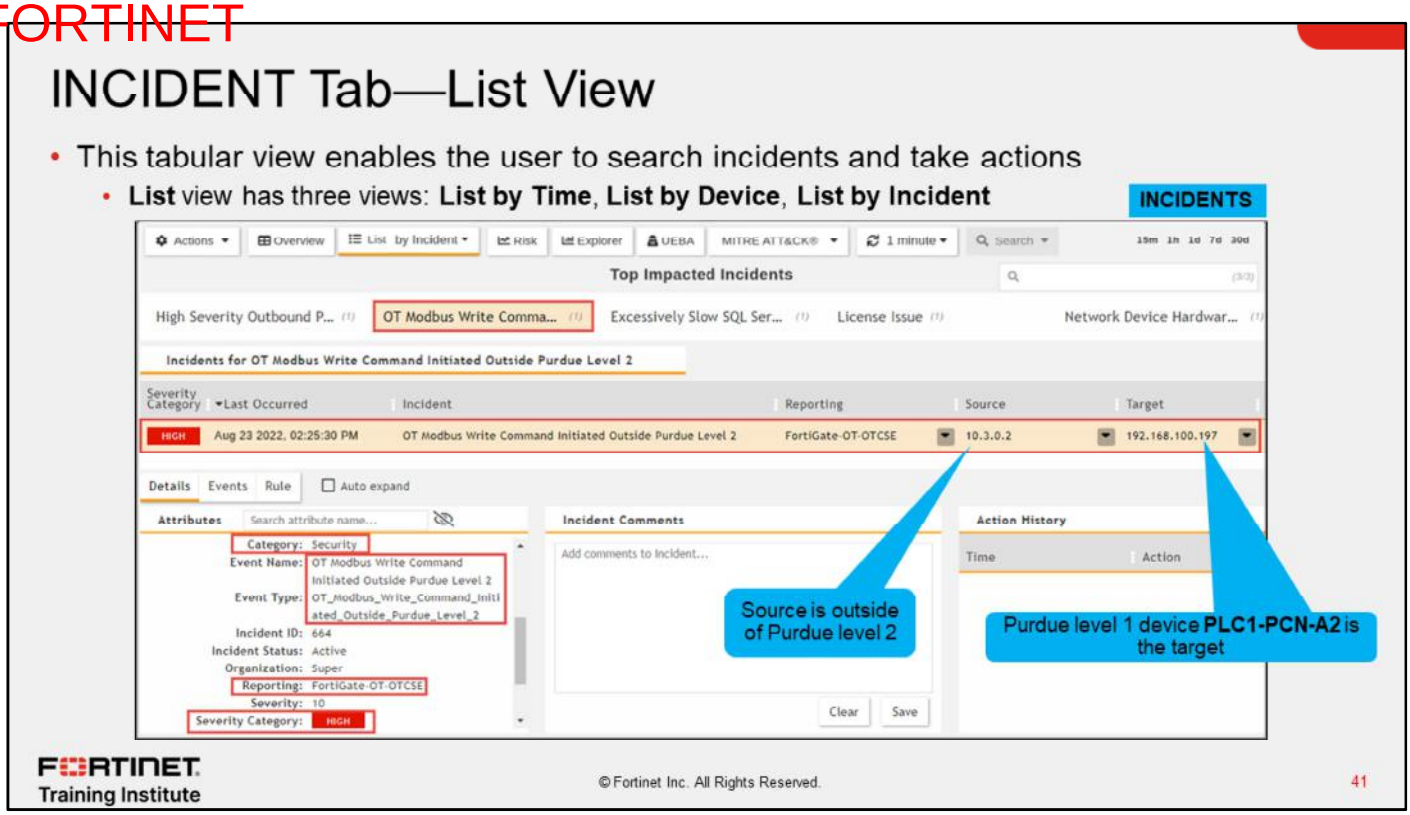
The **INCIDENT** tab provides *five* views for incident data:

- **Overview**: This view provides a top-down view of the various types of incidents and impacted hosts.
- **List**: This view enables the user to search incidents and take actions.
- **Risk**: This view organizes impacted entities (hosts, users) by risk, based on the triggered incidents.
- **UEBA**: Monitors the AI alerts obtained from FortiInsight.
- **MITRE ATT&CK**: Classifies security events detected by FortiSIEM into MITRE ATT&CK categories.

Overview provides a summarized view of your incident data similar to the dashboard.

FortiSIEM can cross-correlate incident data and perform lookups on selected external ticketing and work flow systems. FortiSIEM can also be configured to collect host vulnerability data to preform a CVE-based IPS false positive analysis.

DO NOT REPRINT
© FORTINET



In the **List** view, the user can search incidents and take action.

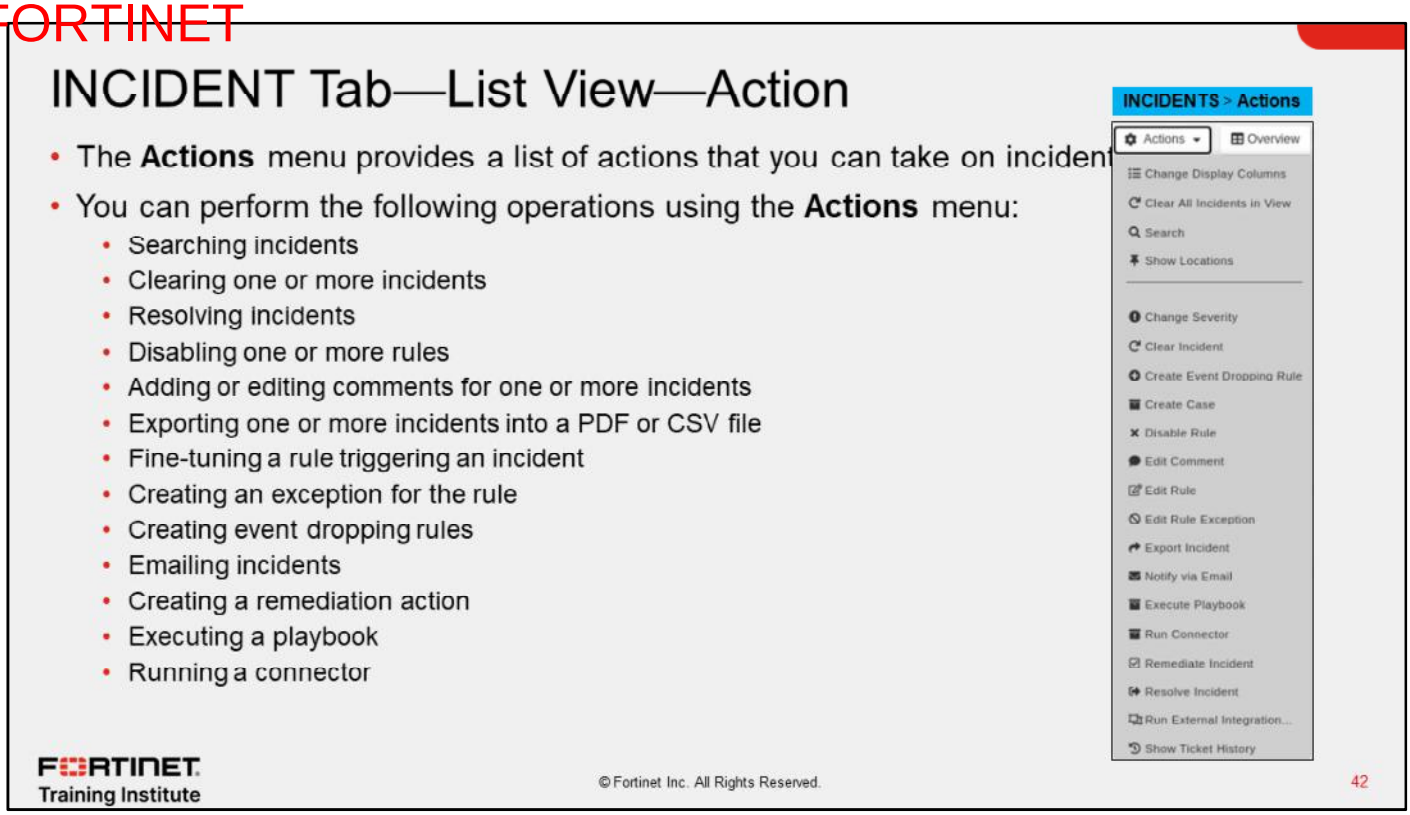
- Viewing incidents

  By default, the List view refreshes every minute. The refresh menu on the top bar allows you to disable the automatic refresh or choose a different refresh interval. By default, the refresh interval is the active incidents in the last two hours. The latest incident sorted by **Last Occurred** time is shown first.
- Acting on incidents

  The **Action** menu provides a list of actions that you can take on incidents.
- The incident **Details** pane displays evidence for why the incident was triggered
  - **Events**: **s**hows the set of events that triggered the incident
  - **Rule**: select the rule to see the events belonging to each sub-pattern

The example shown on this slide matched a count for the **Modbus_Write** command, initiated from devices outside the Purdue level 2 business service group. The command **Modbus_Write** is destined for Purdue level 1 device, **PLC1-PCN-A2**. The subpattern **Modbus** of the rule **OT Modbus Write Command Initiated Outside Purdue Level 2**, triggered an incident.

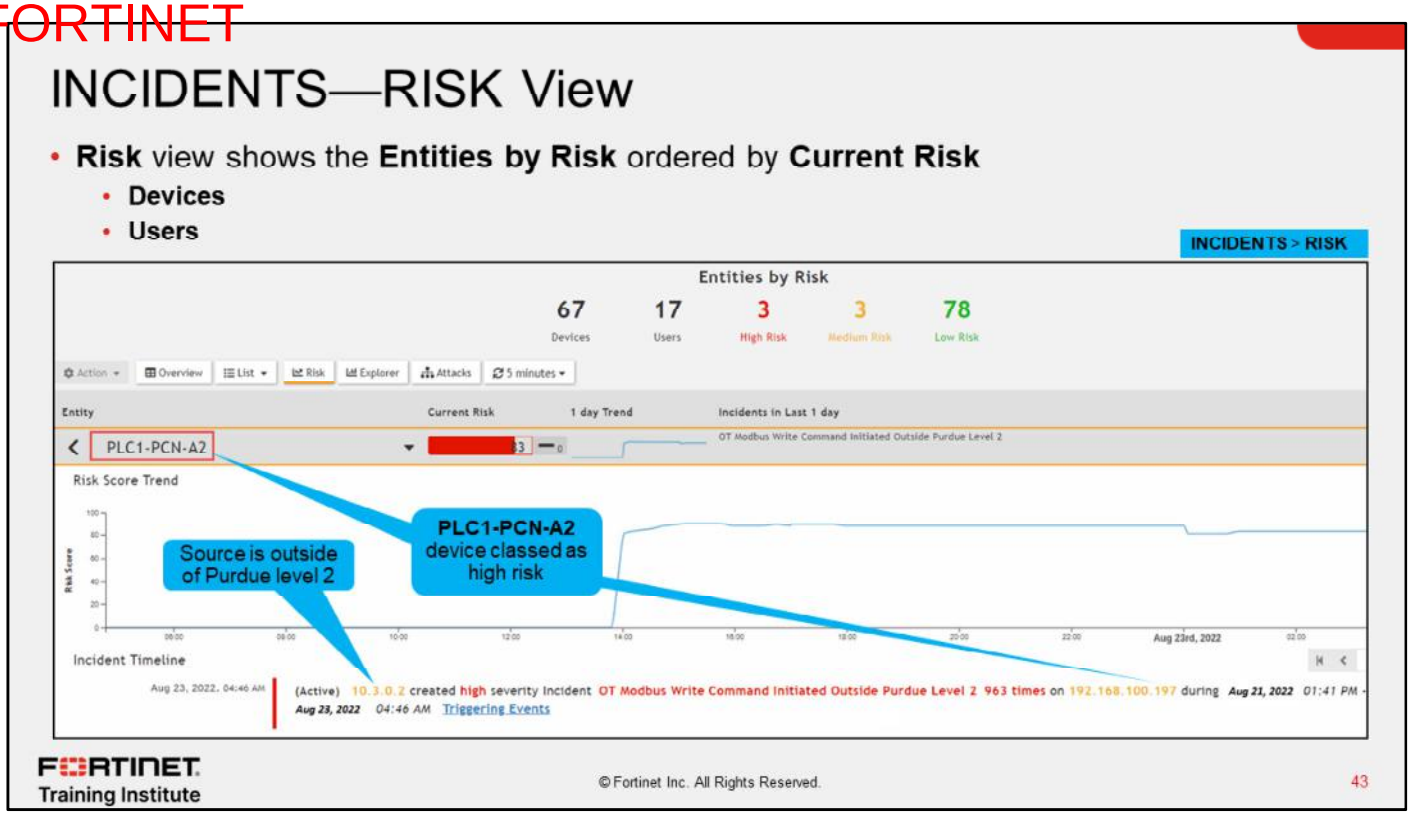
DO NOT REPRINT
© FORTINET



The **Actions** menu provides a list of actions that you can take on incidents. You can perform the following operations using the **Actions** menu:

- Searching incidents
- Clearing one or more incidents
- Resolving incidents
- Disabling one or more rules
- Adding or editing comments for one or more incidents
- Exporting one or more incidents into a PDF or CSV file
- Fine-tuning a rule triggering an incident
- Creating an exception for the rule
- Creating event-dropping rules
- Emailing incidents
- Creating a remediation action
- Executing a playbook
- Running a connector

DO NOT REPRINT
© FORTINET



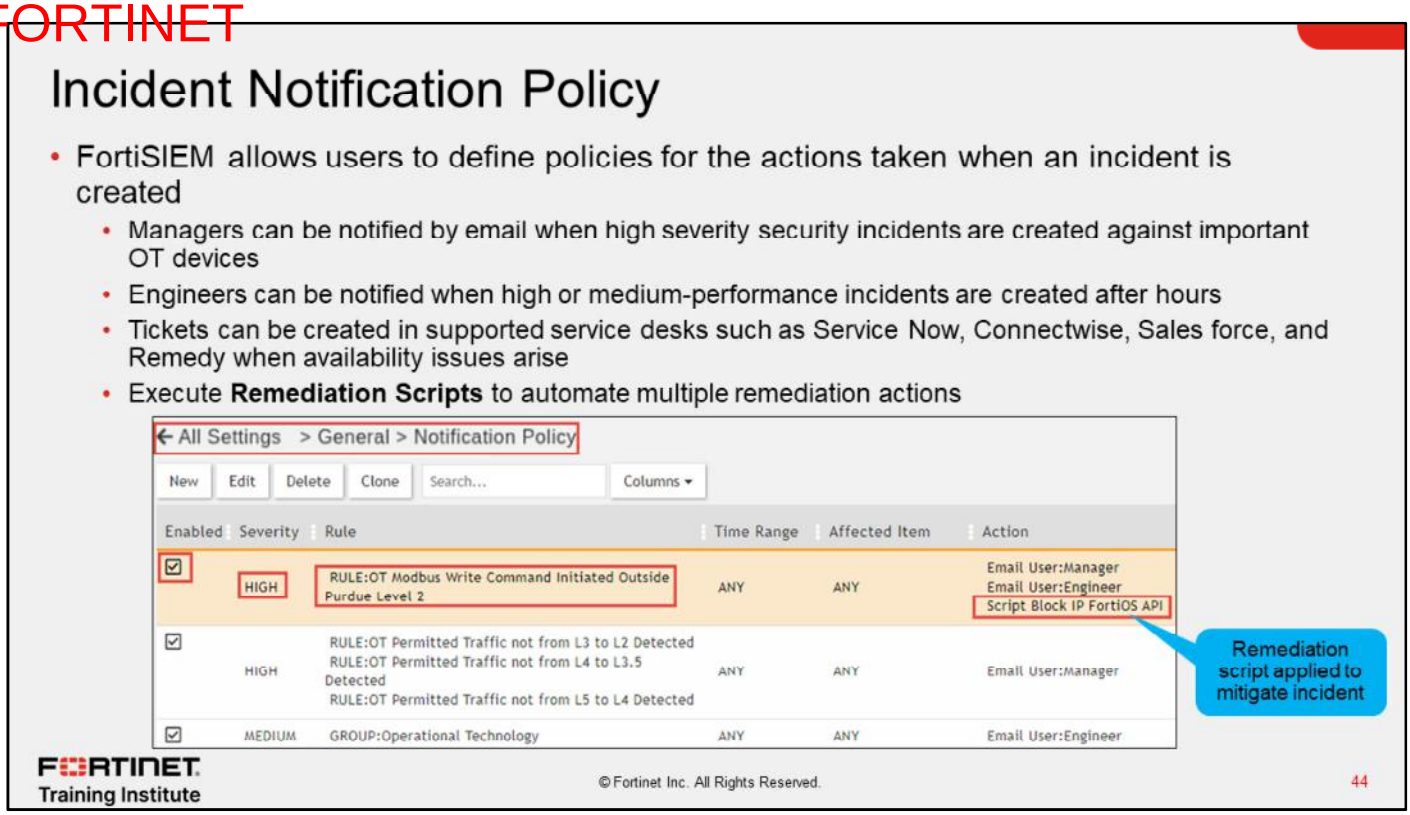
The **Risk** view shows the devices and users ordered by risk. Risk is calculated based on the triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence and vulnerabilities found.

Risk is only computed for devices in the CMDB, private IP addresses, and users found in logs or discovered through LDAP.

Devices and users are categorized by risk as follows:
- **Devices**: the number of devices with risk
- **Users**: the number of users with risk
- **High Risk**: the number of devices and users with high risk
- **Medium Risk**: the number of devices and users with medium risk
- **Low Risk**: the number of devices and users with low risk

The example on this slide shows the **PLC1-PCN-A2** device is classed as high risk because it may have been compromised. This is because a **Modbus_Write** command is initiated from a device with source IP address of 10.3.0.2, which is not in the Purdue Level 1 and 2 business service group, and the command **Modbus_Write** is destined for Purdue level 1 device **PLC1-PCN-A2**.

DO NOT REPRINT
© FORTINET



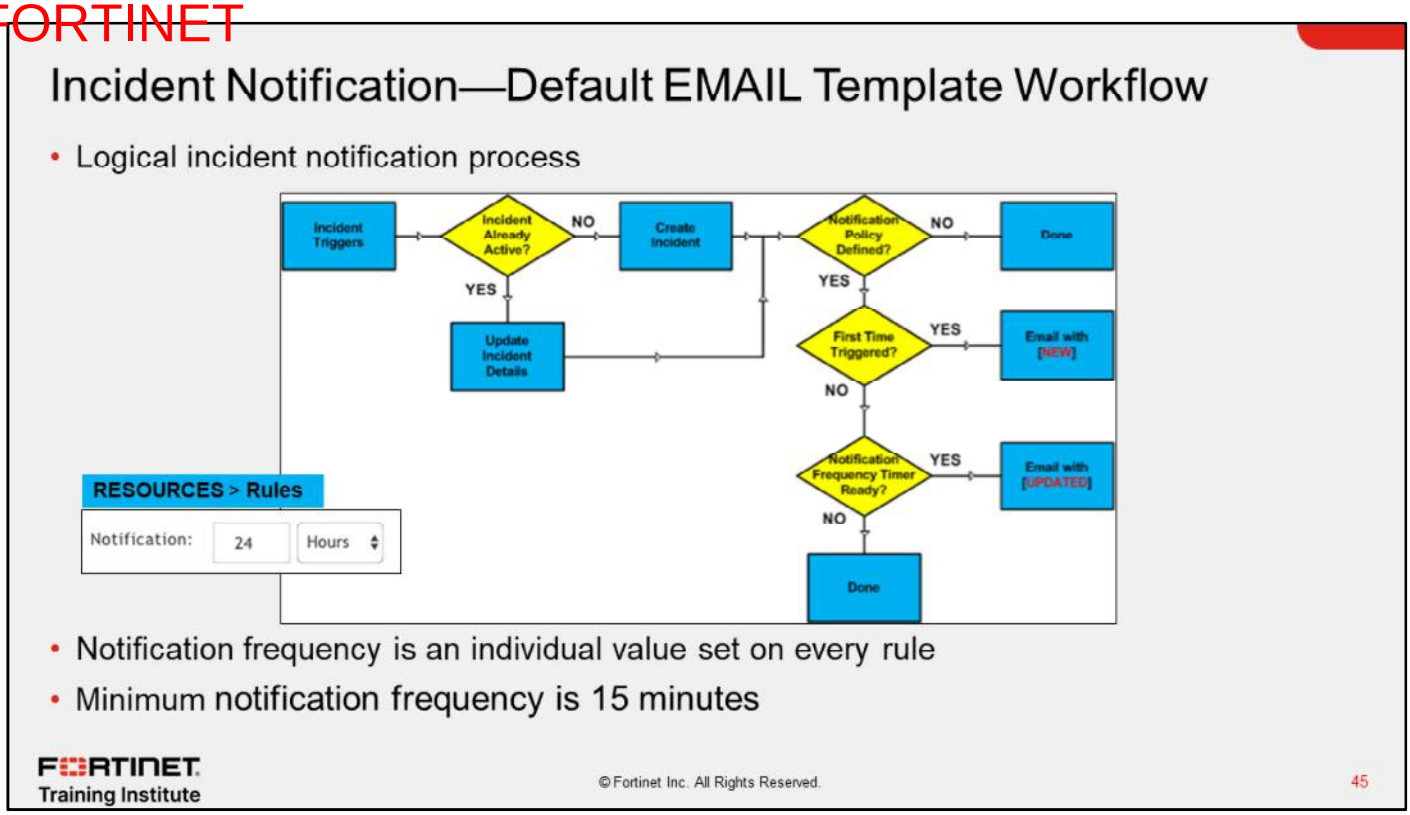
FortiSIEM allows users to define policies for the actions that are taken when an incident is created. The severity of an incident is determined by the rule itself. Each rule has a severity rating. You can use this information as a trigger in the notification policy.

- For example, managers can be notified by email when **HIGH** severity security incidents are created against important OT devices.
- Engineers can be notified when **HIGH** or **MEDIUM** performance incidents are created after hours. You can define time ranges within the policy to decide when to send notifications.
- You can create tickets in supported service desks, such as Service Now, Connectwise, and Remedy, when availability issues arise.
- You execute **Remediation Scripts** to automate multiple remediation actions.

Remediation can be performed either on an ad-hoc basis (for example, the user selects an incident that has already occurred to remediate) or using a notification policy, where the system takes the remediation action when an incident happens. First, make sure the remediation script for your scenario is defined. Check the existing remediation scripts in **ADMIN** > **Settings** > **General** > **Notification Policy** > **Run Remediation/Script**. If your device is not in the list, add the needed remediation script. Incidents can be mitigated by deploying a mitigation script. For example, you can block an IP in a firewall, or disable a user in active directory. Note that this type of incident mitigation from the incident page is somewhat ad hoc and must be manually set up by the user after the incident has triggered.

The example shown on this slide matched a count for the **Modbus_Write** command initiated from devices outside the Purdue level 2 business service group. The subpattern **Modbus** of the rule **OT Modbus Write Command Initiated Outside Purdue Level 2**, triggered an incident.
The notification policy to mitigate the incident was defined for the rule **OT Modbus Write Command Initiated Outside Purdue Level 2**, therefore, the source IP address of the host-initiated **Modbus_Write** command, was blocked using the FortiOS API.

DO NOT REPRINT
© FORTINET



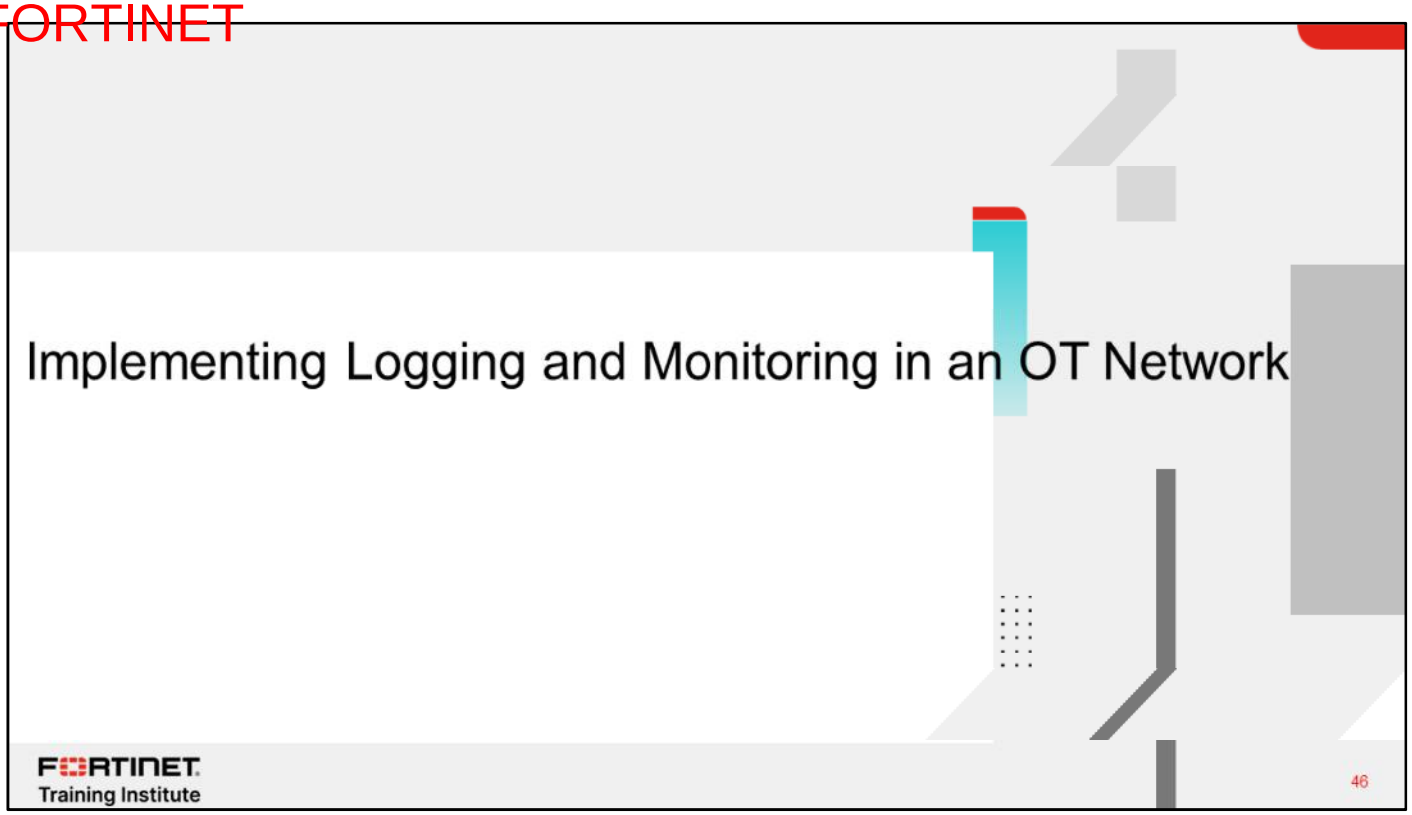
This slide shows the incident notification email workflow that occurs when you use the default template.

The first time an incident triggers, the system looks at whether there's an incident already active or not for the same condition. If there is not, then an incident is created. If there is already an incident opened for the same condition, it will update the incident details, meaning it will update the incident count, and it will also update the last seen time.

Next, the system looks to see if there is a notification policy defined for this incident and the conditions that are being tracked. If there is no policy defined, then the system is finished. If there is a policy defined, the system looks at whether this is the first time that this incident has triggered. If it is the first time, the system will send a notification email using the default template with the subject header, **NEW**.

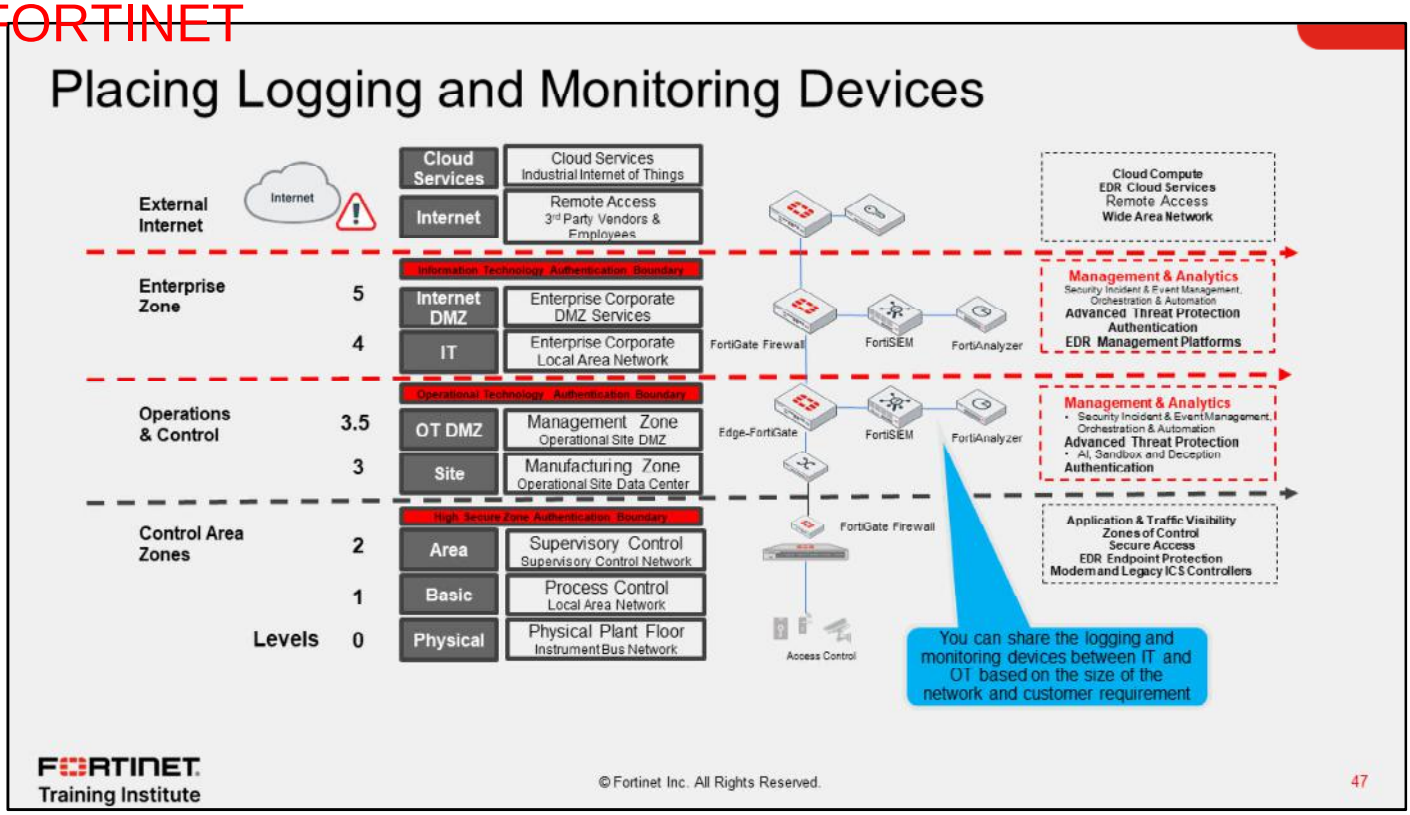
Every rule has a notification frequency value that you can set. The minimum is 15 minutes, but you can override it with whatever value you like. The idea is that, rather than sending an email every time an incident triggers, further notifications will be sent based on this frequency timer. If the incident in question triggered several times within that notification frequency period, only the first email would have been sent. But, after the notification frequency period elapses, the next time the incident triggers, another email notification will be sent. This time, the subject header will include the word **UPDATED**.

DO NOT REPRINT
© FORTINET



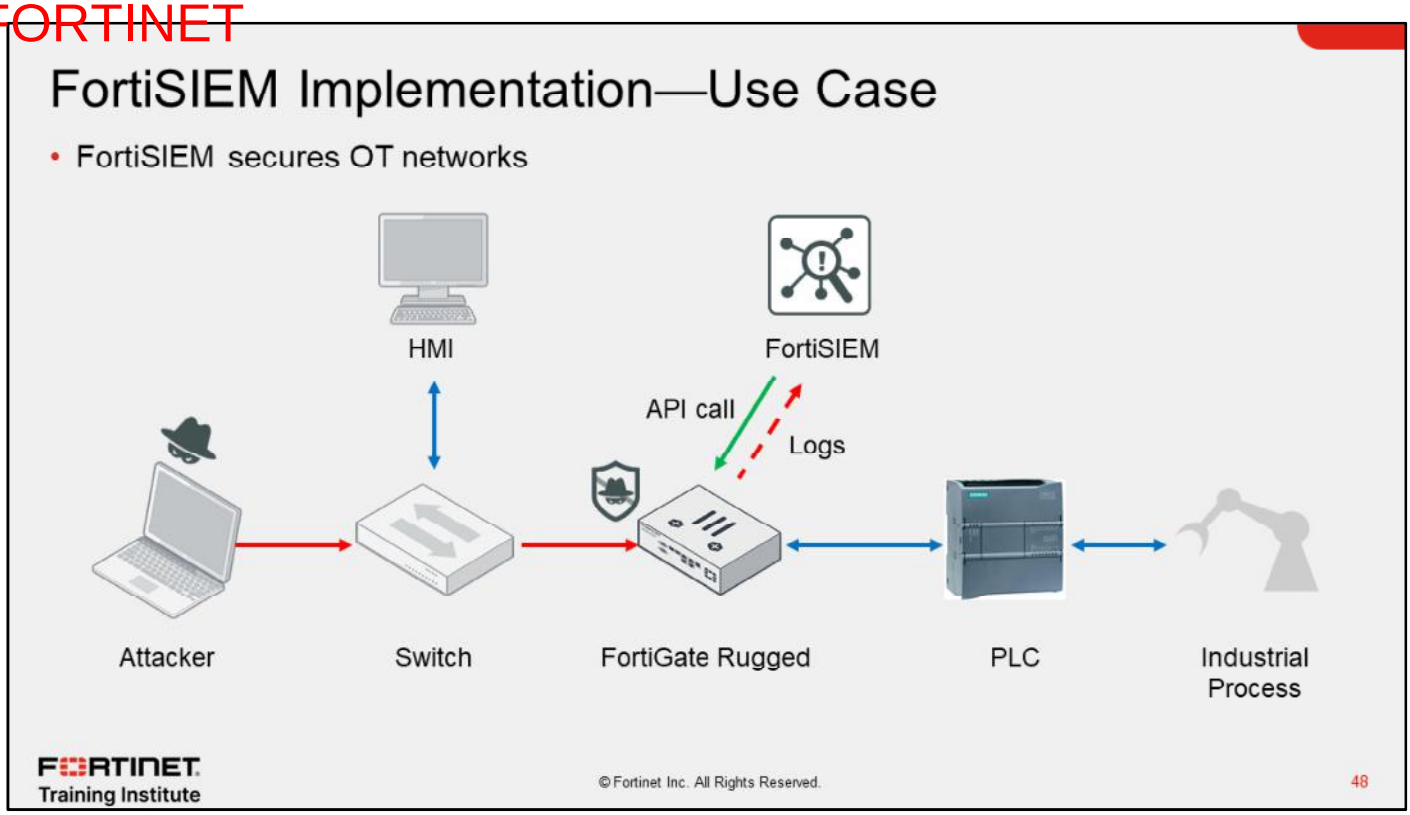
In this section, you will learn about implementing logging and monitoring devices in an OT network.

DO NOT REPRINT
© FORTINET



This slide shows the implementation of logging and monitoring devices. In the Purdue model, you can implement the FortiAnalyzer and FortiSIEM under the protection of the firewall in the OT DMZ management zone. These devices can be used for the entire OT network to correlate security events from all Purdue levels.

DO NOT REPRINT
© FORTINET



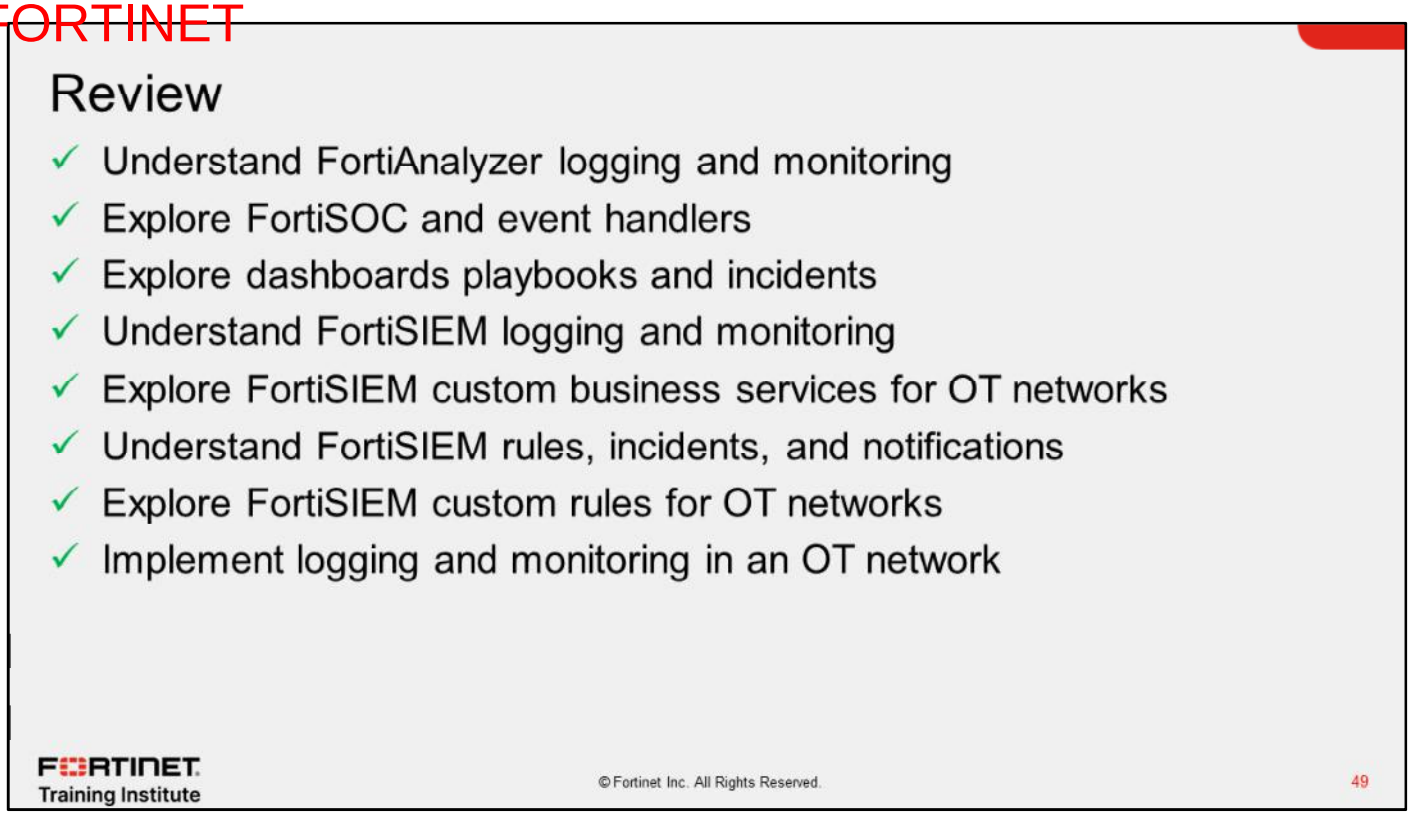
This slide shows an example of a FortiSIEM use case, how FortiSIEM can secure OT networks:

- FortiGate is used to secure SIEMENS PLC devices.
- FortiSIEM receives logging activity from FortiGate.
- Attacker gains access to a local system.
- Attacker scans PLC to determine make, model, and firmware version.
- FortiGate IPS signature detects this, and the attacker is blocked.
- Log of this event is sent to FortiSIEM.
- FortiSIEM makes an API call to FortiGate and bans the attacker's IP address.
- The administrator is notified of this event.

Conclusion:

- FortiSIEM can play an essential part in protecting SCADA/ICS networks from attack.
- FortiSIEM receives logs from network security devices, correlates this information and alerts and/or takes actions.
- FortiSIEM can make API calls to multiple FortiGate devices, and block the attacker's IP address.

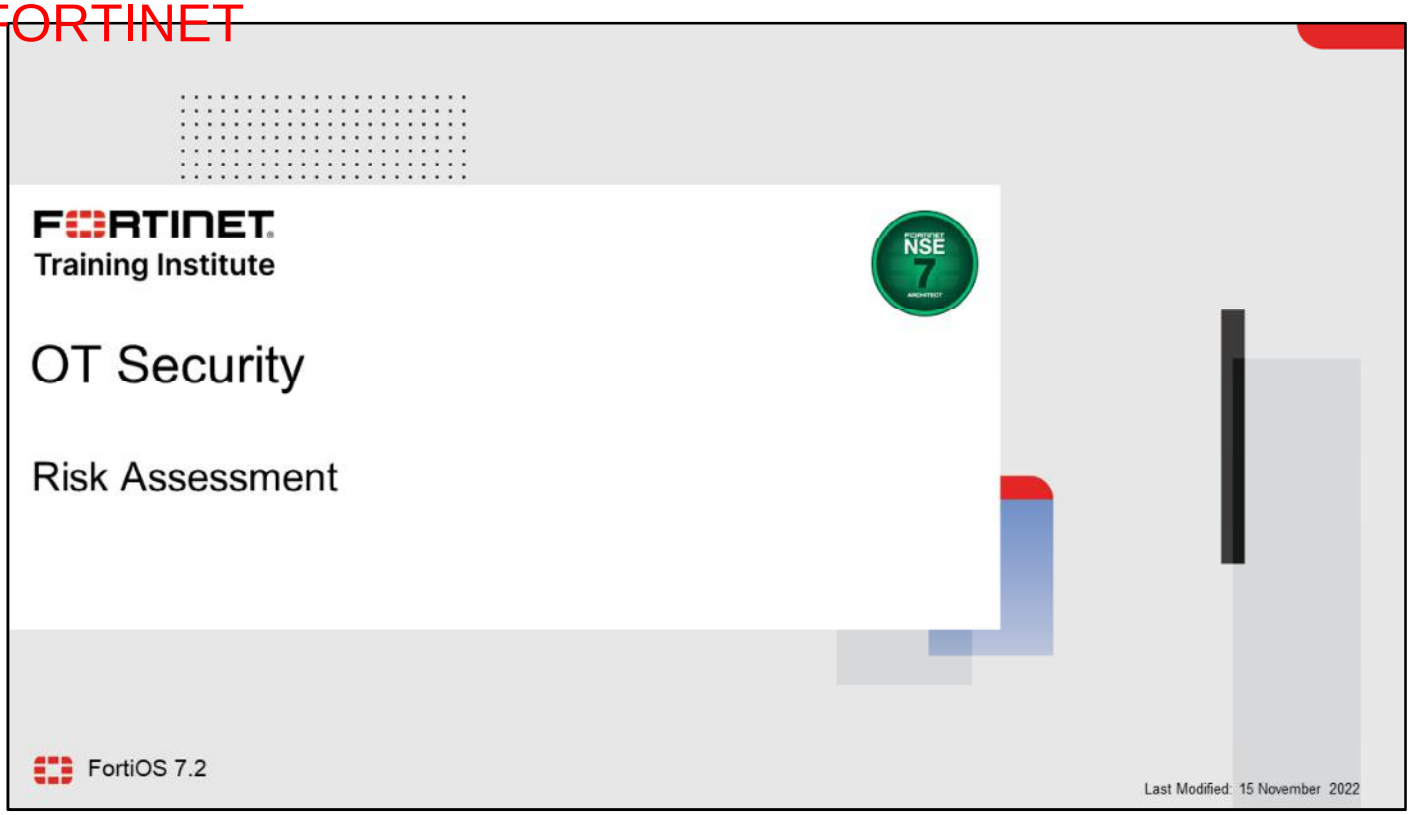
DO NOT REPRINT
© FORTINET



This slide shows the objectives that you covered in this lesson.

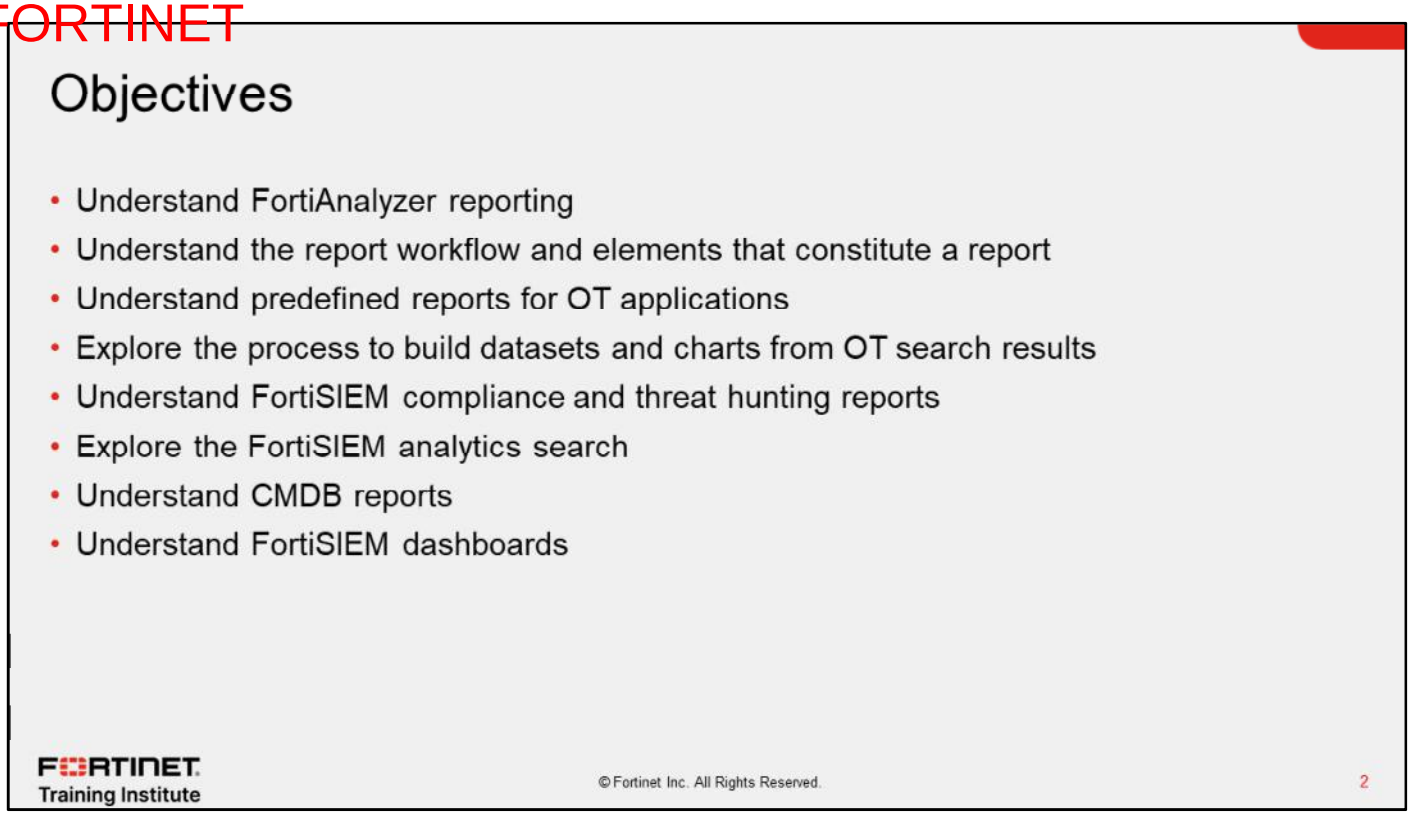
By mastering the objectives covered in this lesson, you learned how to use logging and monitoring devices, FortiAnalyzer, and FortiSIEM, for operational technology security.

DO NOT REPRINT
© FORTINET



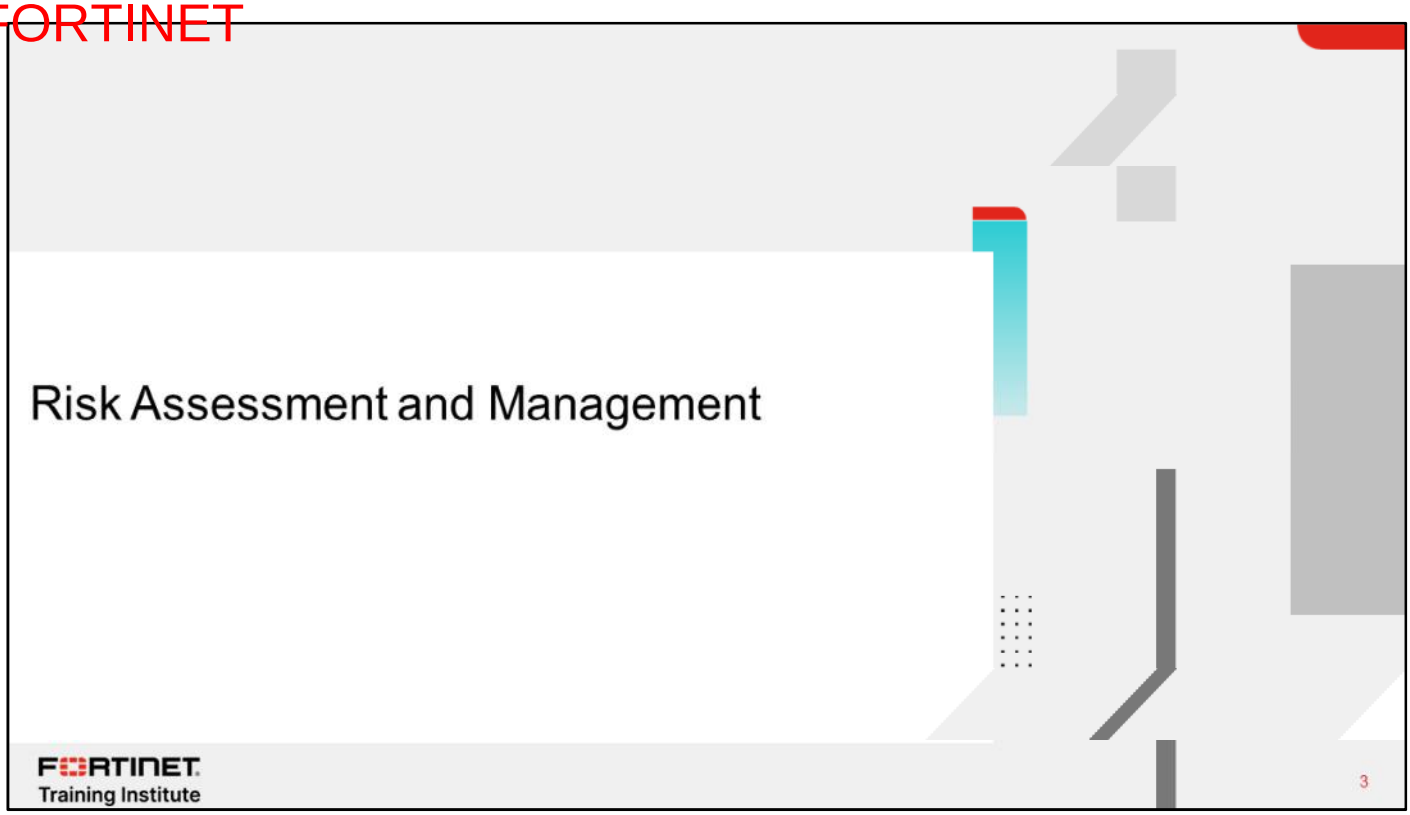
In this lesson, you will learn about reports on FortiAnalyzer and FortiSIEM. Reports can provide effective guidelines for developing a risk assessment strategy.

DO NOT REPRINT
© FORTINET



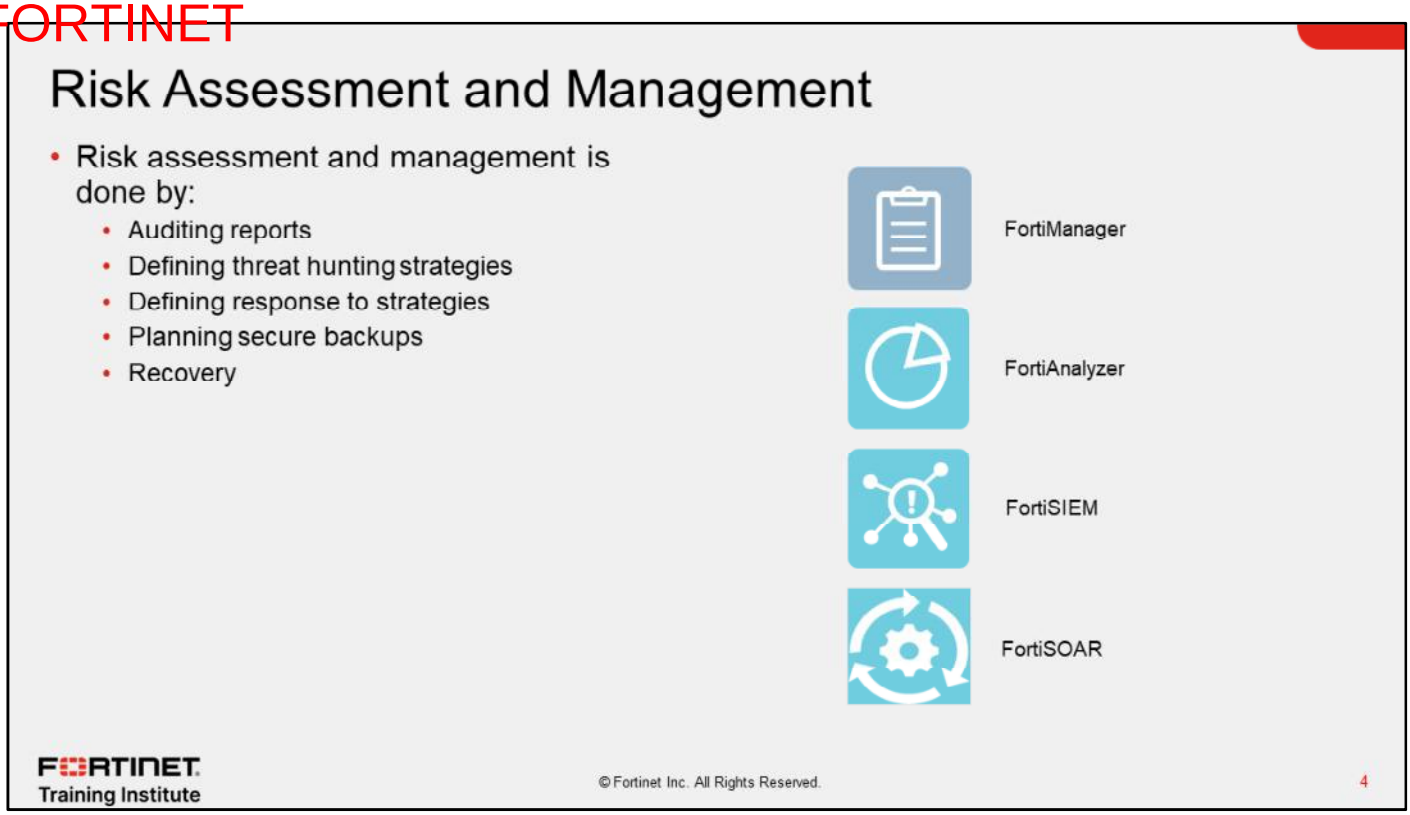
After completing this lesson, you should be able to achieve the objectives shown on this slide.

DO NOT REPRINT
© FORTINET



In this section, you will learn about risk assessment and management using reports on FortiAnalyzer and FortiSIEM. Reports can provide effective guidelines for developing a risk assessment and management strategy.

DO NOT REPRINT
© FORTINET

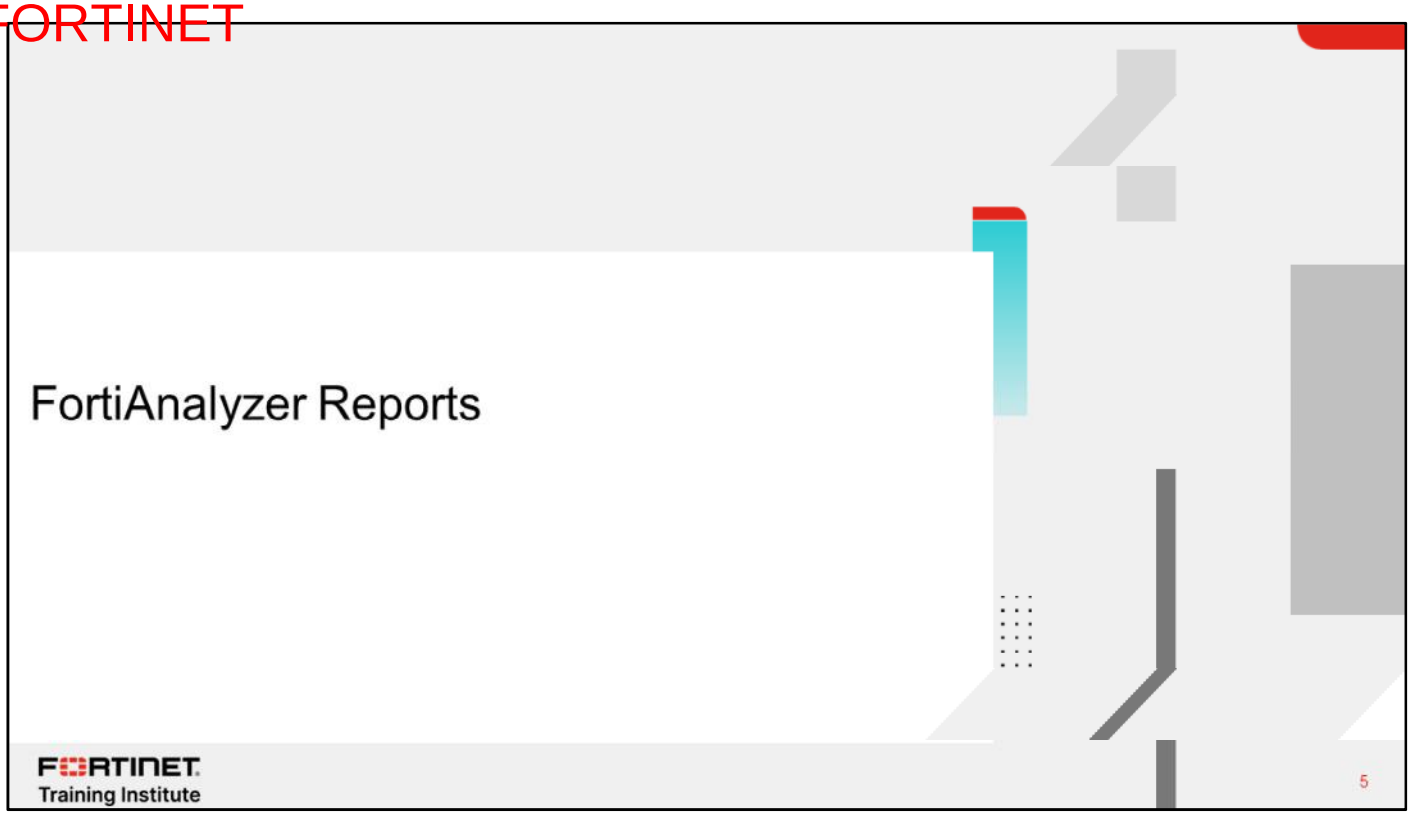


For any organization, planning a threat hunting strategy is a critical task. Auditors should be able to follow a set of guidelines for threat hunting through reports and respond to the threats in timely manner. FortiSOAR is a product that can be used to automate the response to reported incidents.

Risk management is also about evaluating what can go wrong before it happens. You need to consider how industrial control systems can be manipulated and what the physical, environmental, and financial consequences would be. This will drive the types of controls you will want to put in place.

FortiManager, together with FortiAnalyzer, will be able to provide a security rating for the Fortinet network security scope. It will provide a rating against ICS guidelines such as the NIST CSF or the CIS top 20s best practices.

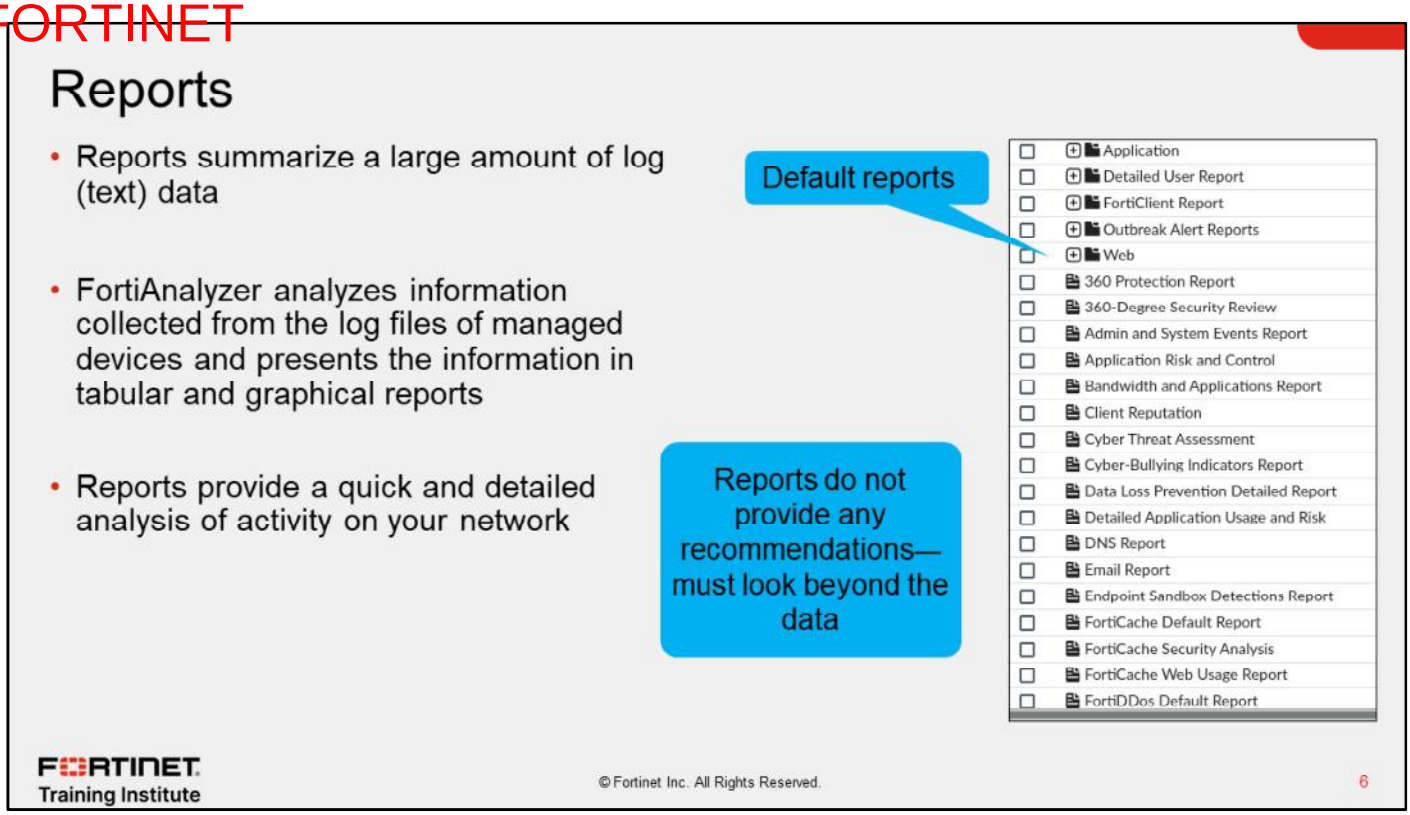
DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiAnalyzer reports for OT networks.

By demonstrating competence in understanding report concepts, you will be able to use reports to more effectively extract collected log data from your database.

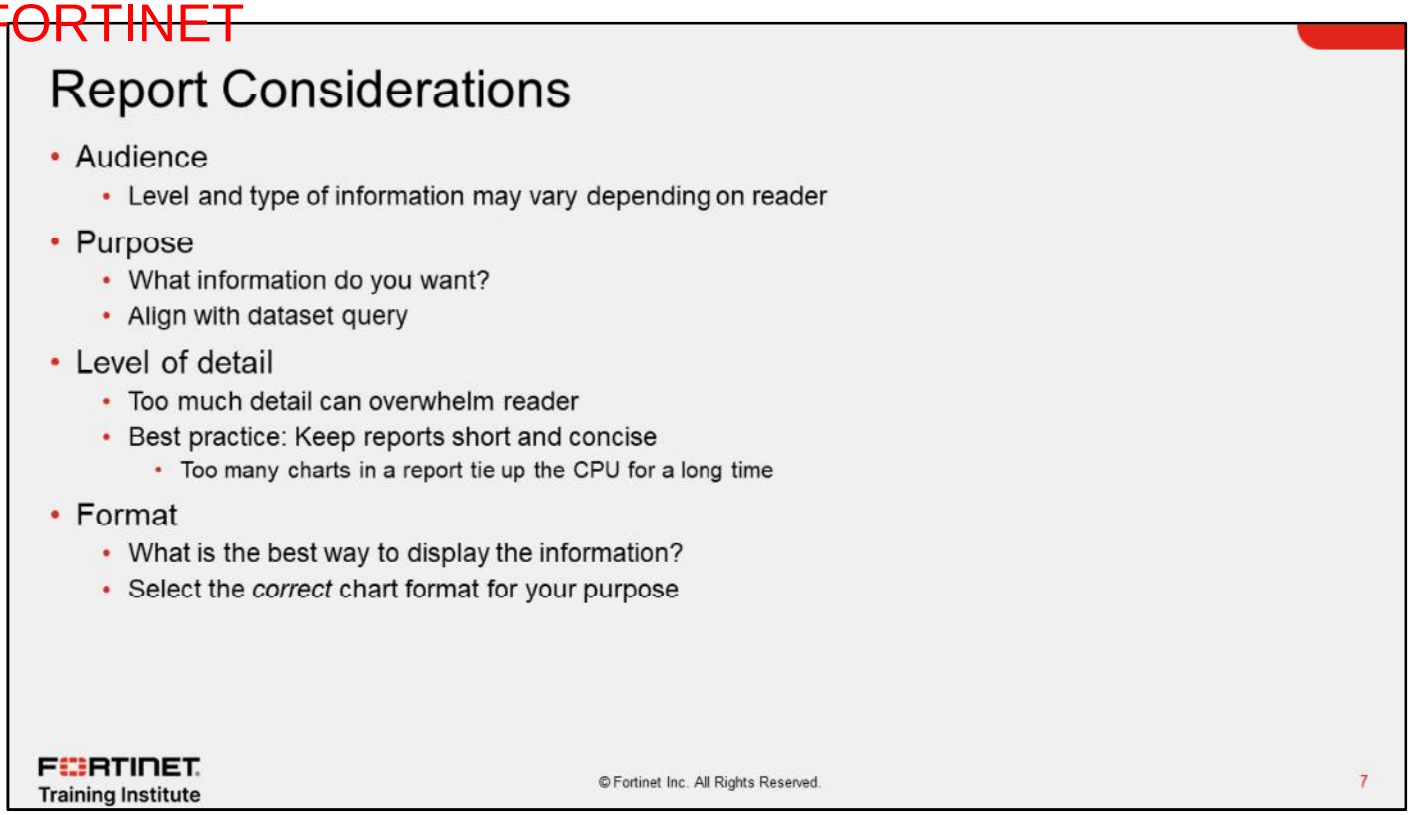
DO NOT REPRINT
© FORTINET



The purpose of a report is to summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier—and quicker—to digest. The patterns and trends that reports reveal already exist as several points of data within your database, but it would be difficult and time consuming to manually locate, cross-reference, and analyze multiple log files, especially if you don't know what trend or pattern you are looking for. After they are configured, reports do the investigation for you and provide a quick and detailed analysis of activity on your network. You can then use that information to better understand your network or improve your network security.

Reports do not provide any recommendations or give any indication of problems. Administrators must be able to look beyond the data and charts to see what is happening within their network.

DO NOT REPRINT
© FORTINET



Before you configure or create a report, there are certain factors you need to consider to ensure the report is as effective as possible.

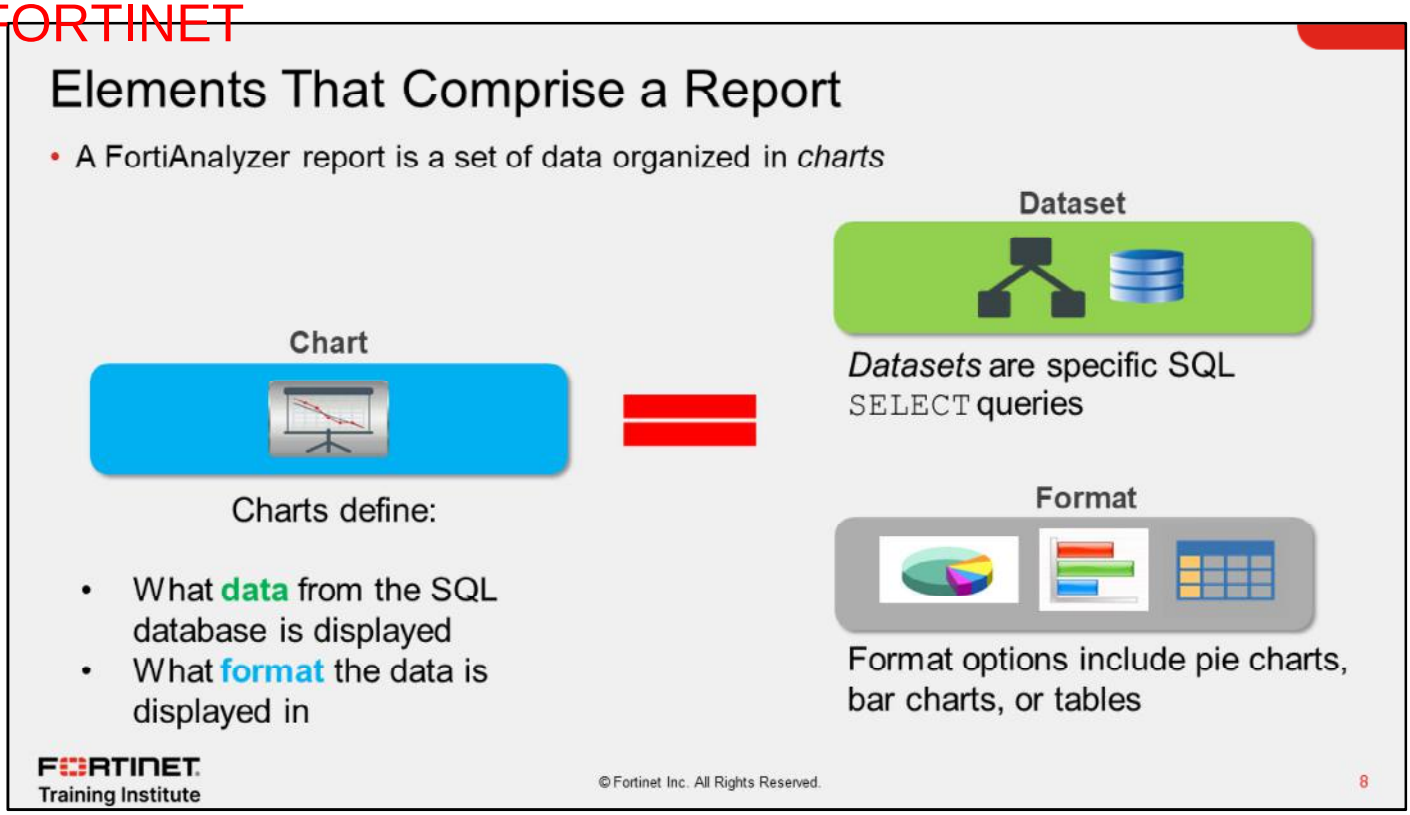
The first consideration is your audience. Who's going to be looking at this report? Depending on what they want to see and their level of skill, you may need to add, remove, or modify charts in order to convey the information appropriately.

The second consideration is your purpose. If you look at the predefined reports, each one focuses on a specific piece of information. They are based on specific datasets and contain charts that format that query. So, reports must be focused in order to be effective and easily digestible, and this is achieved by having a strong purpose.

The next consideration is the level of detail. A best practice is to keep reports short and concise. Not only will it focus your view of your network and users, but shorter reports have fewer charts and fewer queries to run. This helps with performance, because large reports affect CPU and memory.

The final consideration is the format. You need to know how you want to format the data so that it displays in the most digestible and informative way possible. A table chart, bar chart, and pie chart don't necessarily represent the same data with the same effectiveness. Based on your query, you may only be able to use one type of chart but, if options are available, you need to select the right chart. Think about how the data would best be represented visually, and about the audience consuming the data. Aside from the chart format, you can also change the design of the report by adding separators, page breaks, images, and renaming charts.

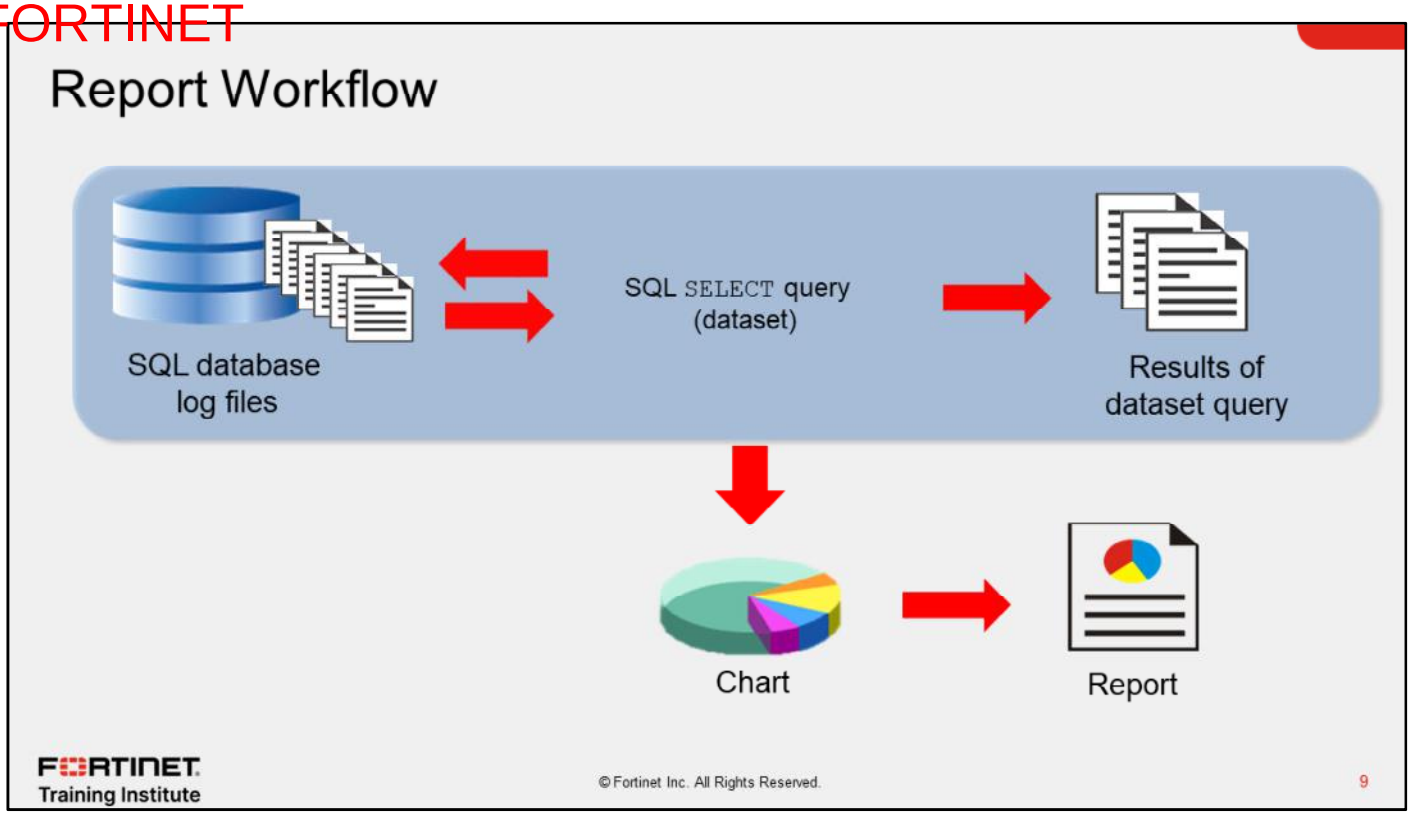
DO NOT REPRINT
© FORTINET



A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- Datasets, which are Structured Query Language (SQL) `SELECT` queries that extract specific data from the database
- The format in which to display that data (for example, pie charts, bar charts, or tables)

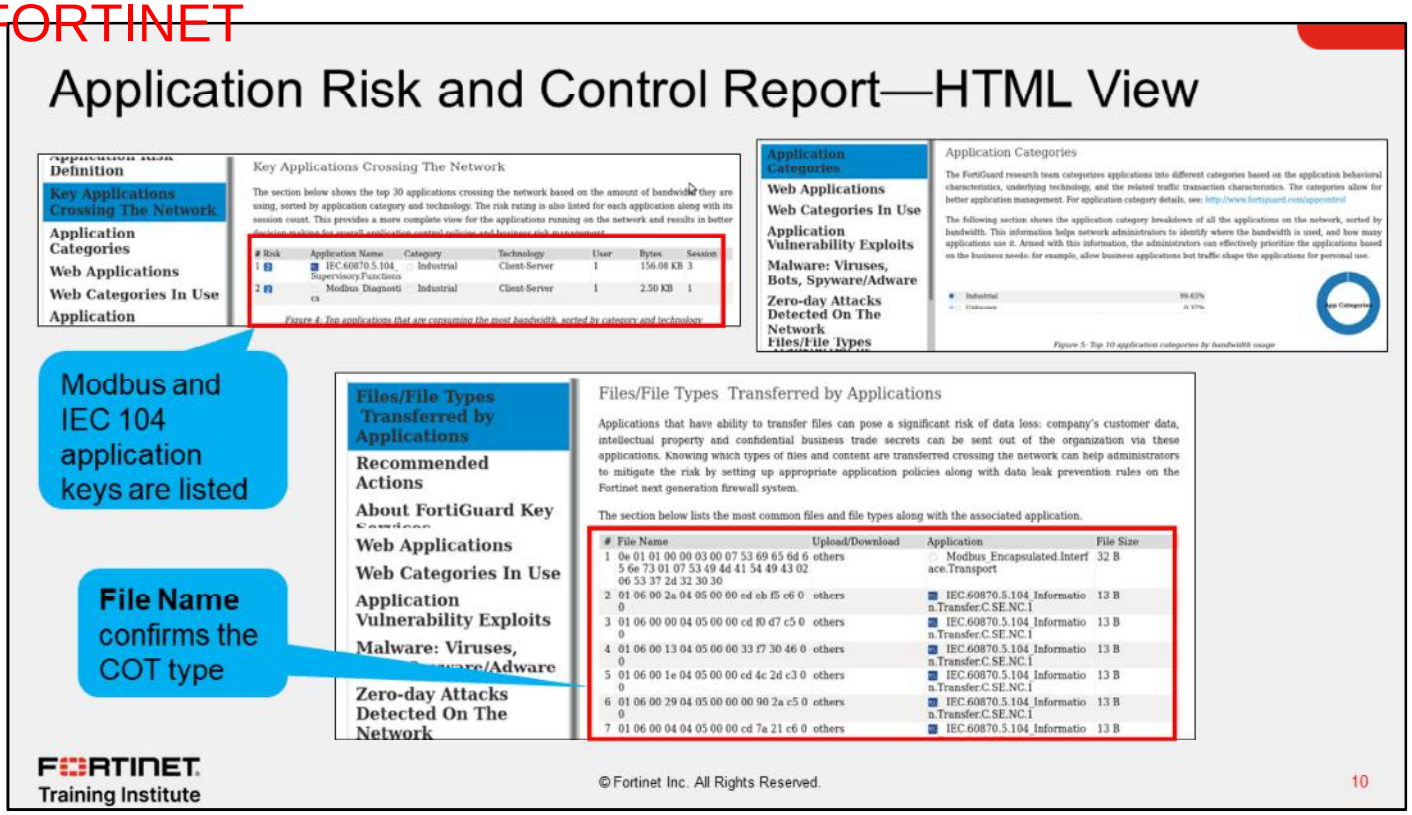
DO NOT REPRINT
© FORTINET



As the graphic on this slide shows, the SQL database contains all the raw logs. A SQL `SELECT` query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted.

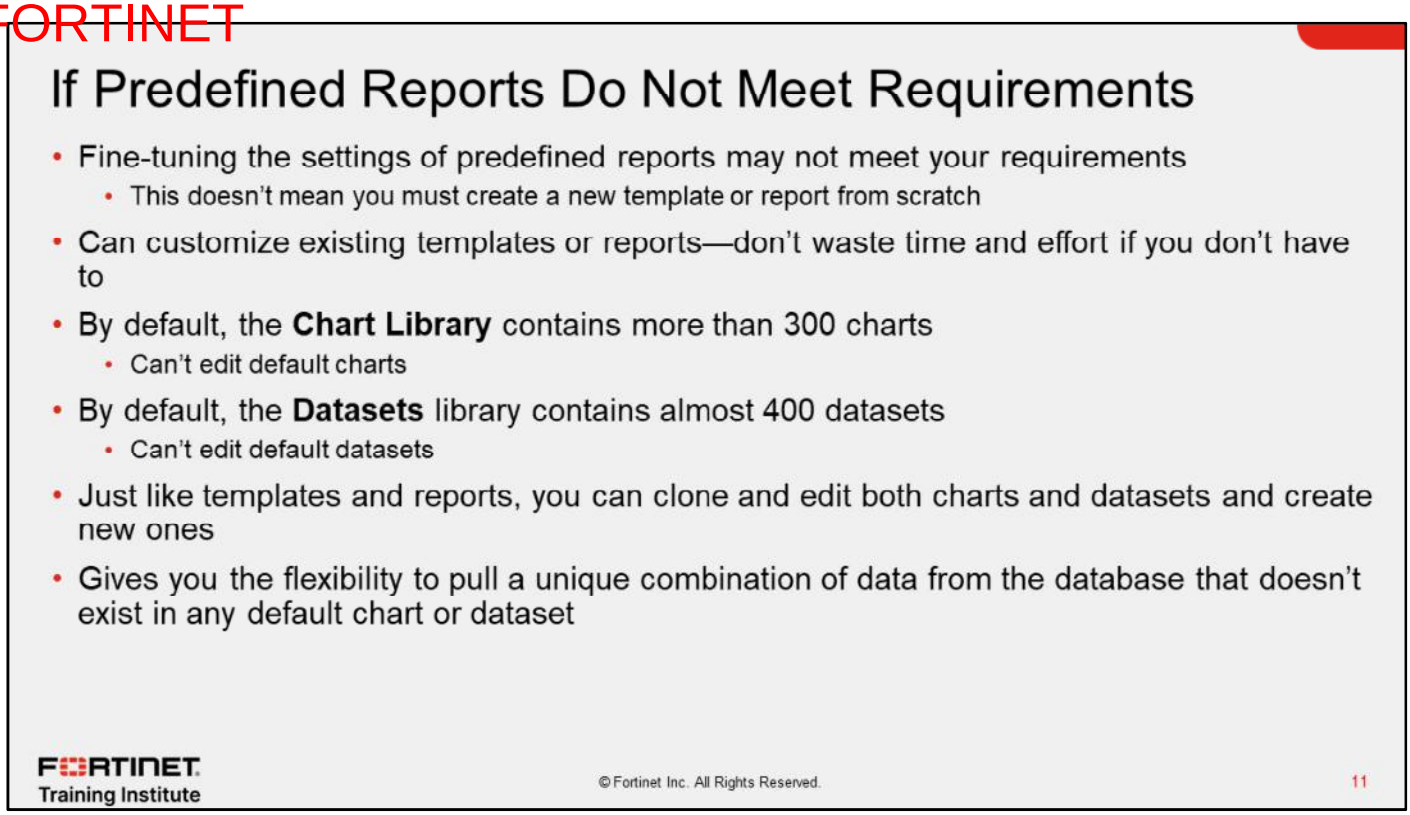
This subset of data populates a chart, and one or more charts exist within a report.

DO NOT REPRINT
© FORTINET



This slide shows an example of an application and risk control default report. The report is in HTML format. The report confirms that Modbus and IEC 104 are the key applications crossing the network. The category for these applications is industrial, and the file type confirms the cause of transmission (COT) for the IEC 104 application.

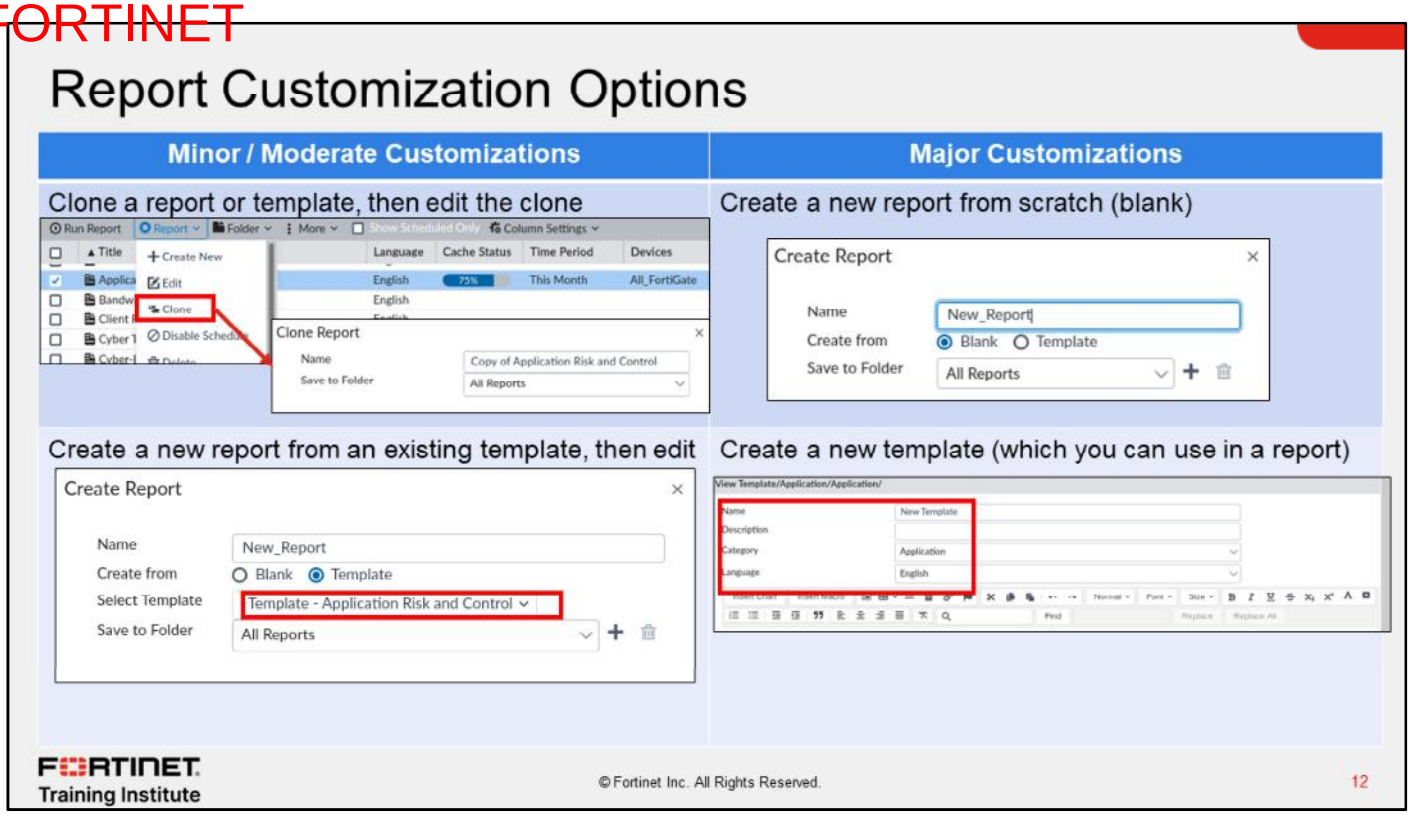
DO NOT REPRINT
© FORTINET



Predefined reports may not meet all of your organization's requirements, even after fine-tuning the report settings. While FortiAnalyzer provides the option to create new templates and reports from scratch, there are customization options available.

In some cases, simply adding or removing default charts from a report or template may not meet your requirements; you might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In this case, you can either clone and edit charts and datasets, or create new charts and datasets from scratch.

DO NOT REPRINT
© FORTINET



For minor or moderate changes to existing templates or reports, you can use cloning. For cloning, you would clone a report or template and then edit the *clone* to suit your requirements. For reports only, you can create a new report, but base it on an existing template. Then edit that new report to suit your requirements.

While you can directly edit the layout of predefined reports (but not templates), it is a best practice to clone and edit the predefined reports instead. This preserves the default reports if your direct edits to the report are not successful.

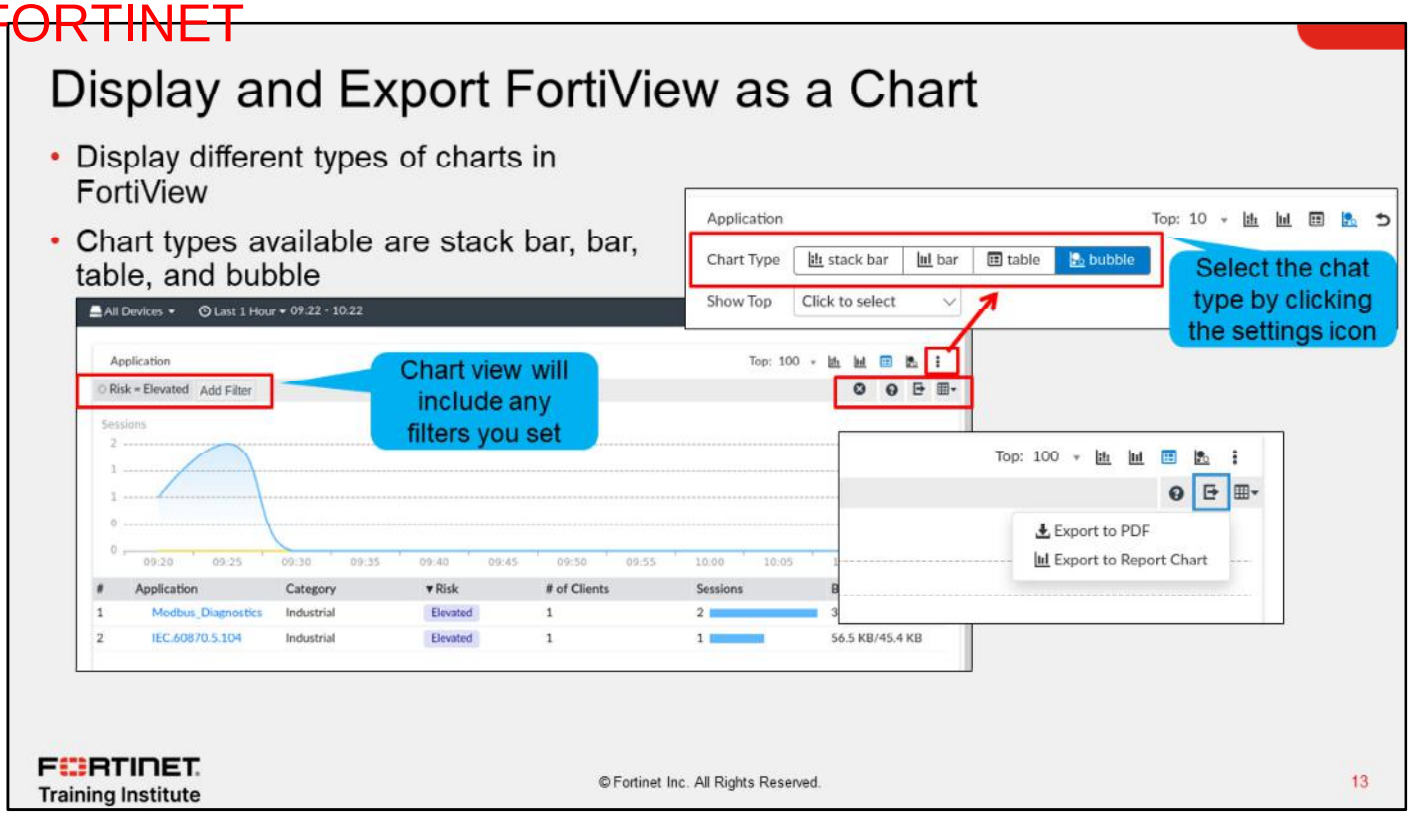
If major changes are required to existing templates or reports (that is, no report meets your needs), you can create a new report or template from scratch.

You can create a new report by selecting **Blank** on the **All Reports** page. As shown in the graphic on this slide, you can configure both the settings and the layout. As it is a new report, both the settings and the layout are blank and you must configure them.

Once you create the layout, you do have the option to save it as a template. You can then use that template for other reports you create. You can delete custom reports.

You can clone a report from the **All Reports** page. Again, you should clone when you need to make only minor to moderate changes, for example, when you want to borrow many of the elements, but not all, from an existing report. In the cloned report, you can edit the settings as well as the layout. Note that the **Layout** tab provides the option to save the layout as a template, if necessary. Unlike predefined reports, you can delete cloned reports. You can clone a template on the **Templates** page. Again, you should clone when you need to make only minor to moderate changes. For example, when you want to borrow many of the elements, but not all, from an existing template. In the cloned template, you can edit only the layout. Unlike predefined templates, you can delete cloned templates.

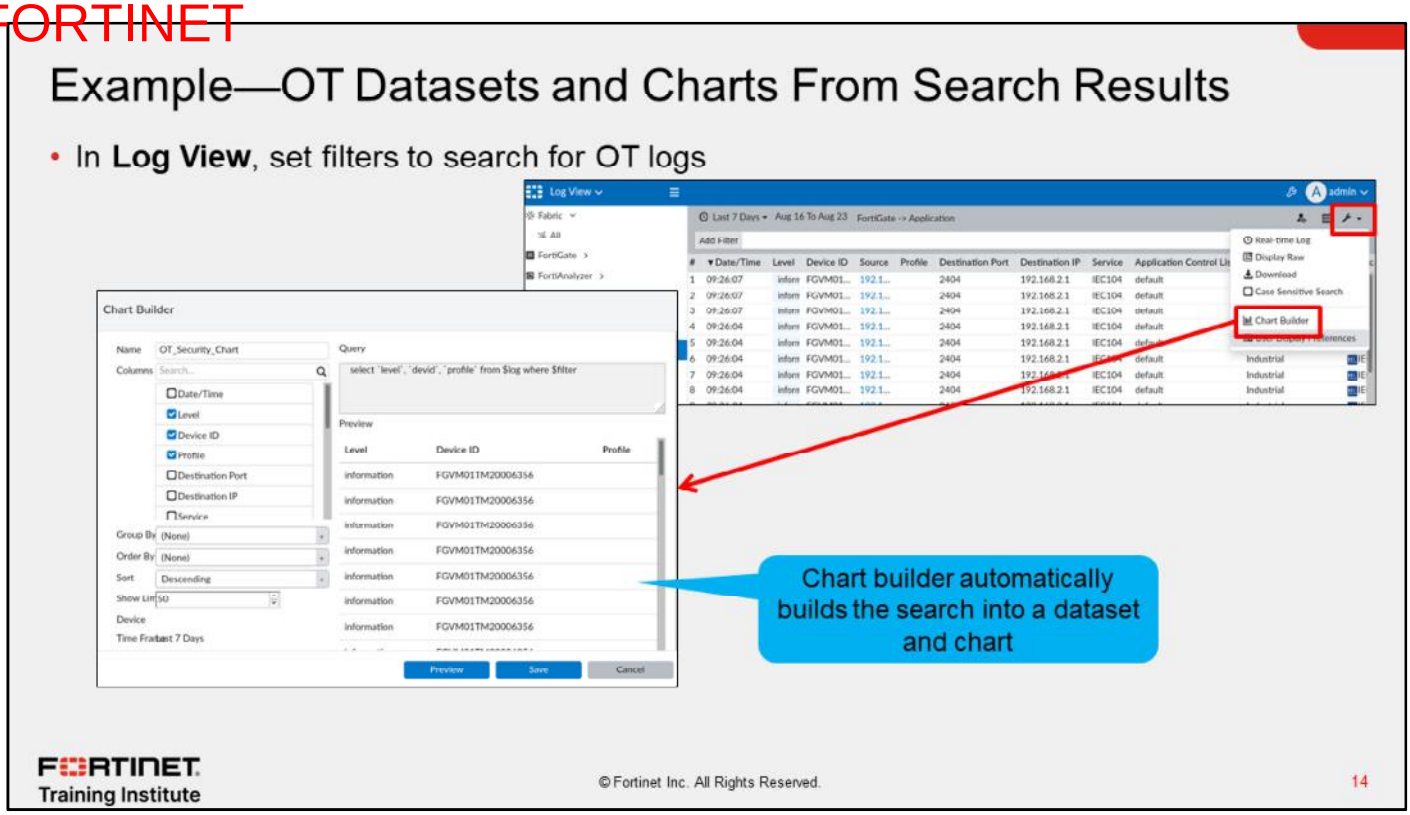
DO NOT REPRINT
© FORTINET



You can display and export a chart from FortiView. The chart export includes any filters you set on FortiView.

The current chart view is available to export as a PDF or report chart. The export will include any filters you set to display FortiView charts.

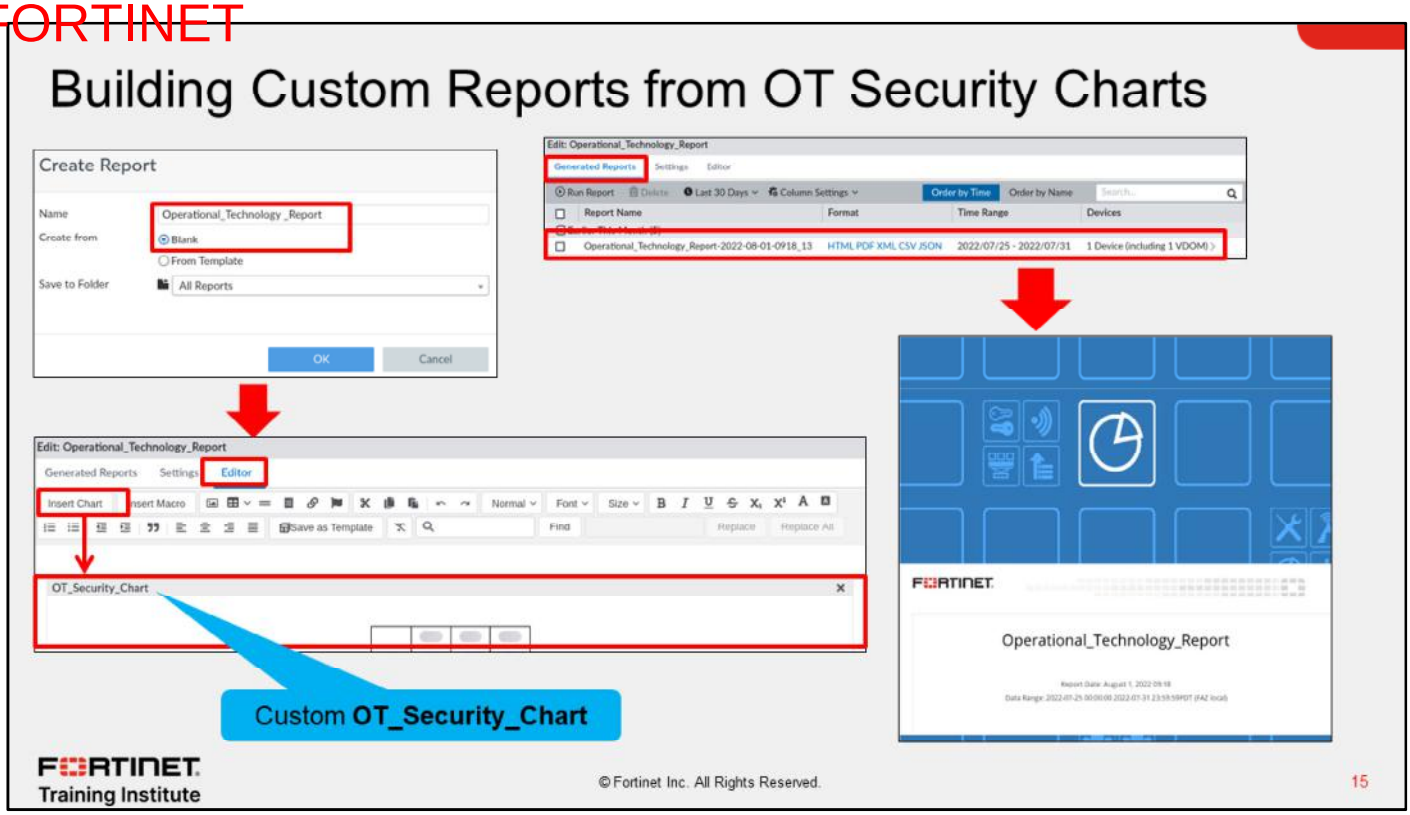
DO NOT REPRINT
© FORTINET



A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in **Log View**, and allows you to build a dataset and chart automatically, based on your filtered search results. In **Log View**, set filters to return the logs you want. Then, in the **Tools** menu, select **Chart Builder** to automatically build the search into a dataset and chart. You can also fine-tune the dataset further by:

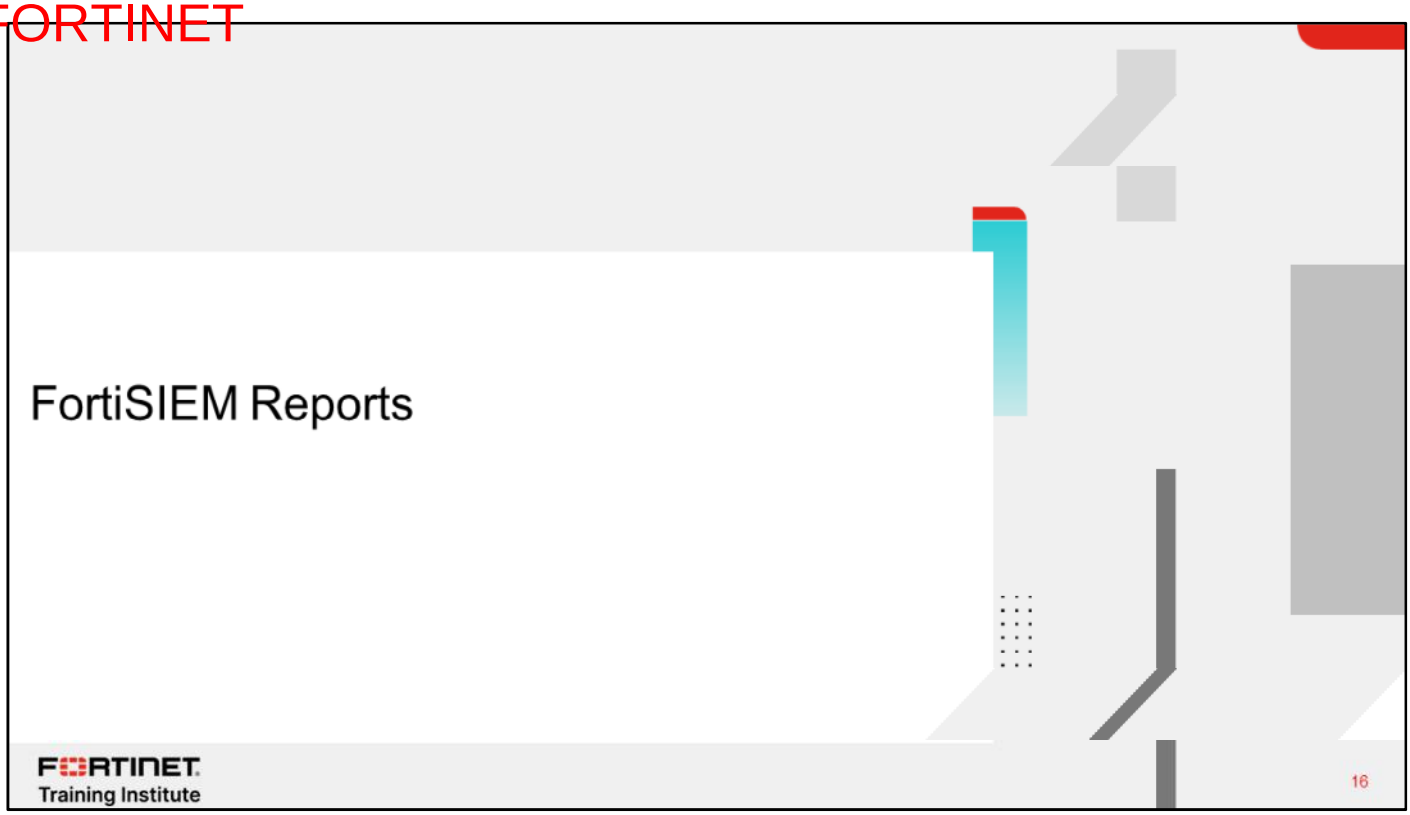
- Adding more columns
- Setting a group, order by, and sort filter
- Setting a limit on results
- Setting the device and time frame

DO NOT REPRINT
© FORTINET



You will build a custom report named `Operational_Technology_Report`, using a custom **OT_Security_Chart**. After you run the report, the report will be available for you to view in HTML, PDF, XML, and CSV formats. The example shown on this slide displays the report cover page in PDF format.

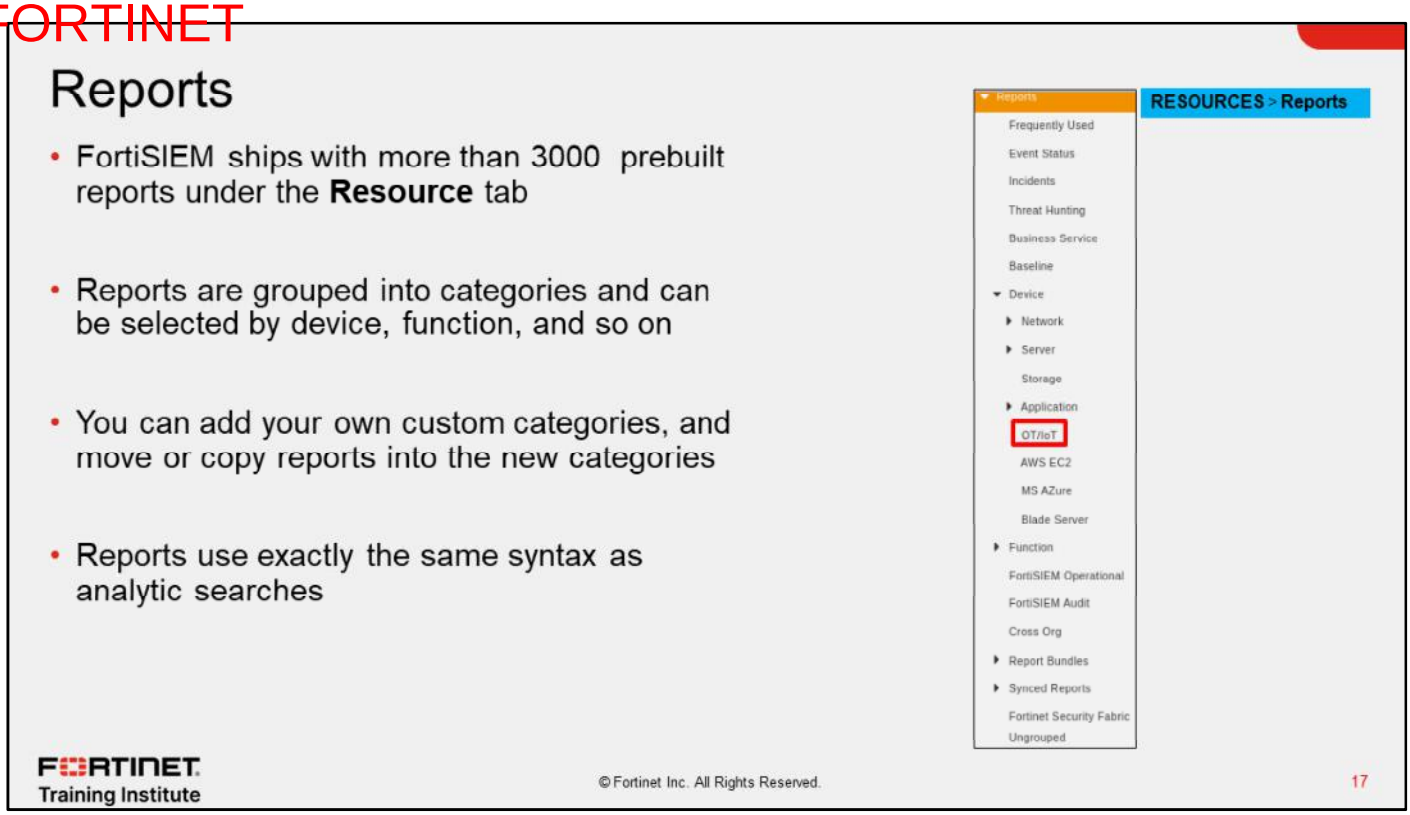
DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiSIEM reports for OT networks.

By demonstrating competence in reporting, you will be able to load, save, and schedule reports on FortiSIEM.

DO NOT REPRINT
© FORTINET

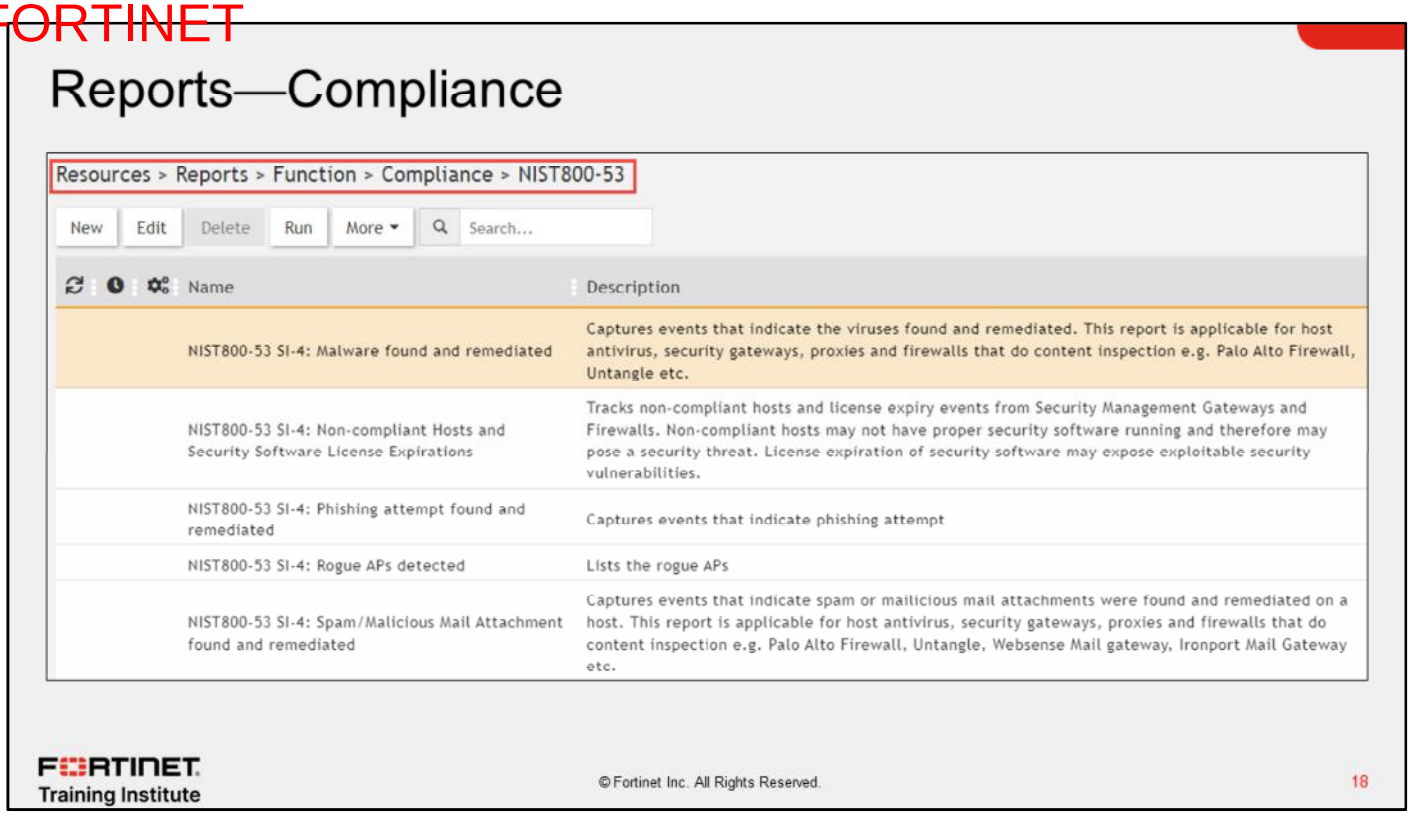


FortiSIEM ships with more than 2800 prebuilt reports. You can find reports by clicking **RESOURCES** > **Reports**.

The reports are grouped into several different categories and subcategories, making is easier for you to locate the report you are looking for. You can add custom categories, and move or copy reports into the new groups.

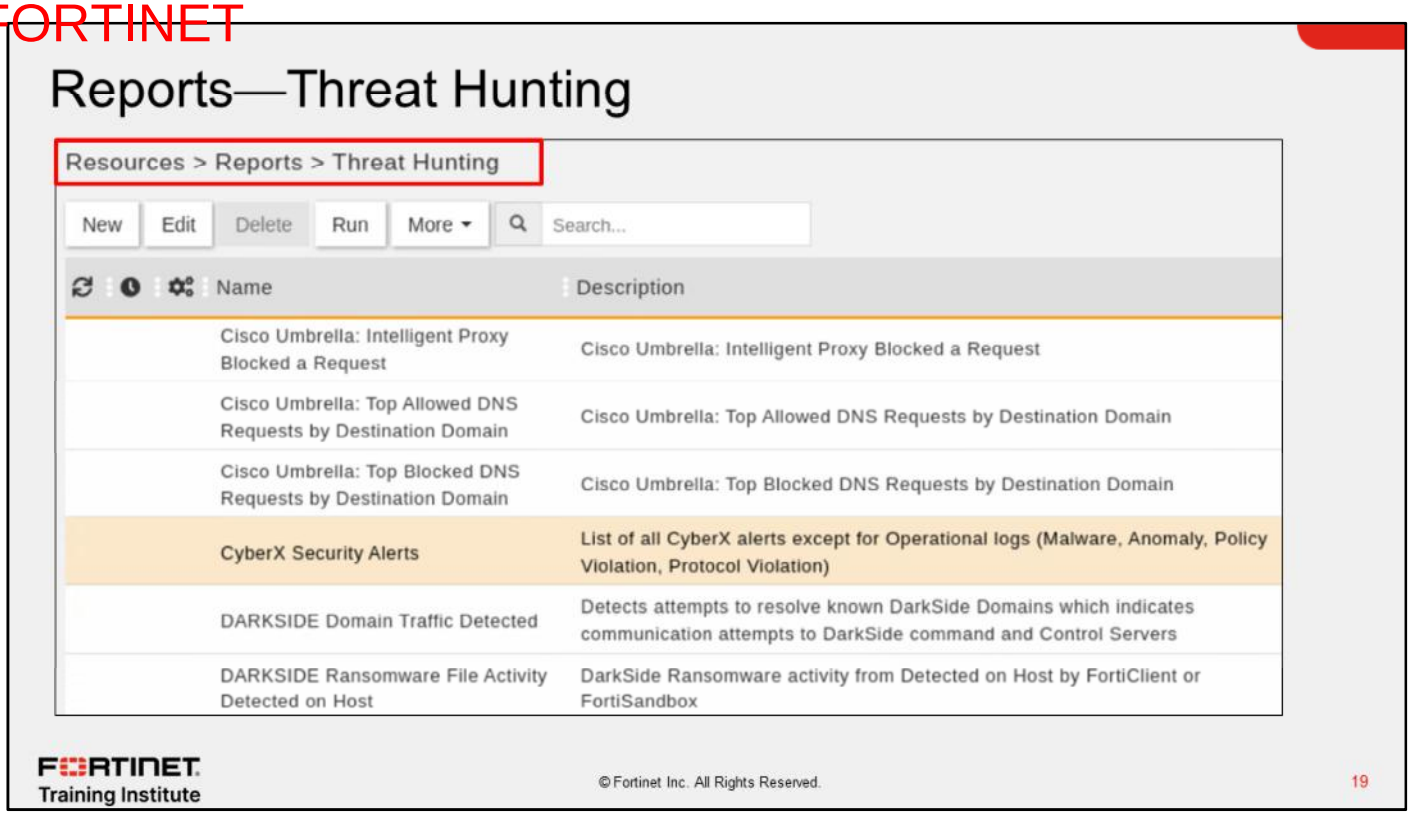
Reports use exactly the same syntax as analytic searches, making it easier for you to build your own custom reports and save them in the reports tree.

DO NOT REPRINT
© FORTINET



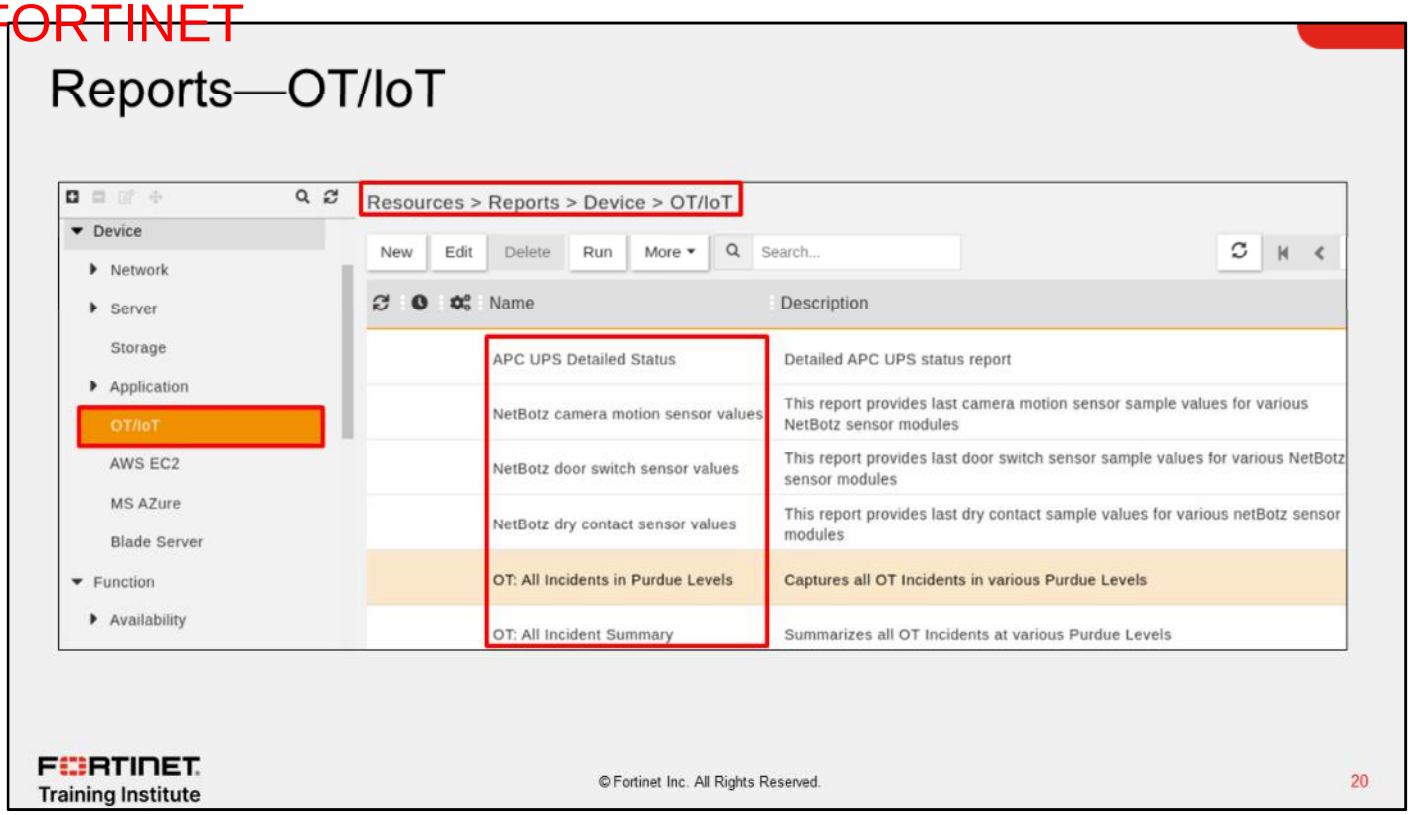
This slide shows an example of predefined compliance reports. You can clone and edit a predefined report, according to the compliance requirements of your OT network.

DO NOT REPRINT
© FORTINET



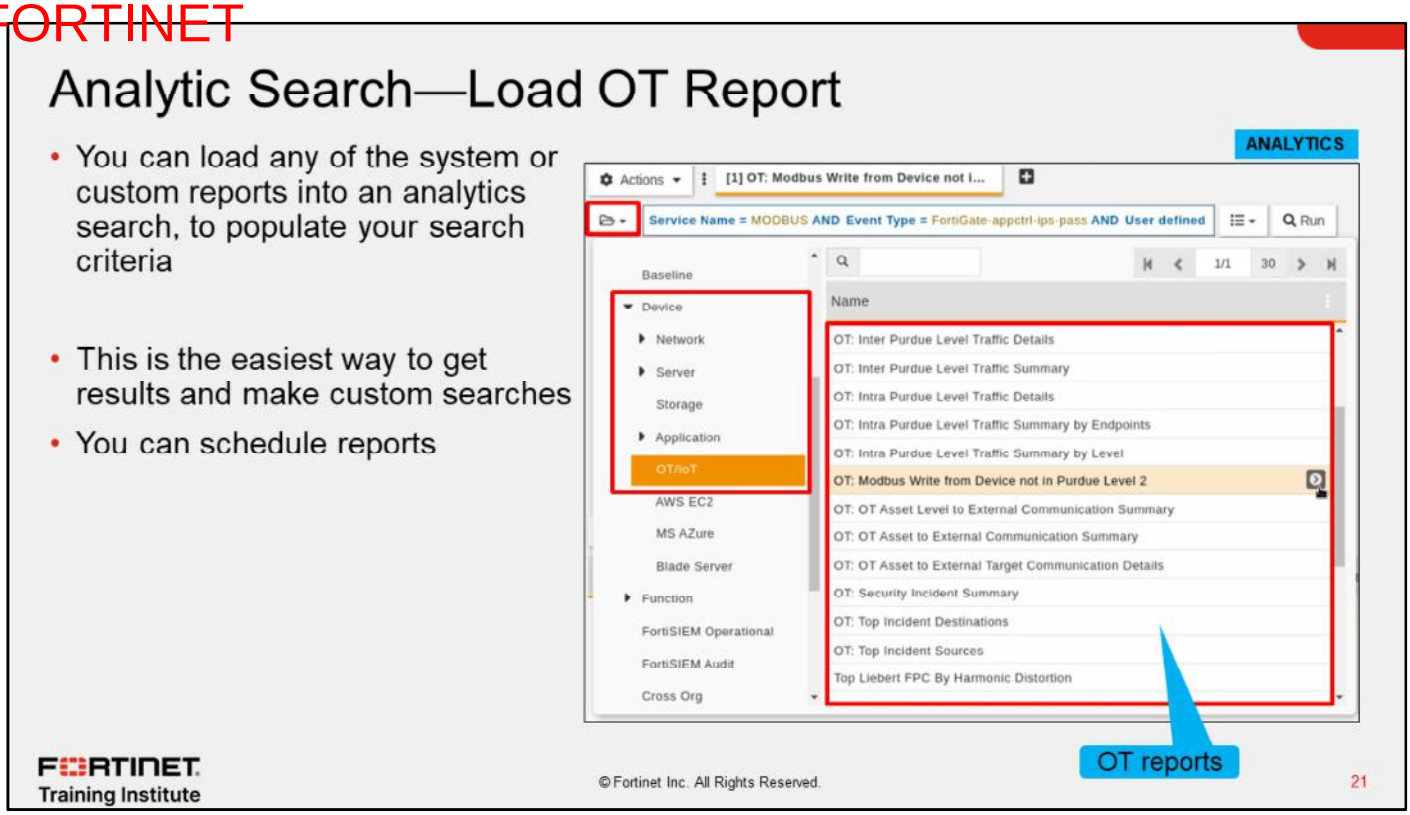
This slide shows an example of predefined threat hunting reports. You can clone and edit a predefined report, according to the threat hunting strategy requirements for your OT network.

DO NOT REPRINT
© FORTINET



This slide shows an example of predefined OT/IoT reports. You can clone and edit a predefined report, according to the requirements of your OT network.

DO NOT REPRINT
© FORTINET



You can load any of the system reports into an analytics search to populate your search criteria. If you click the folder icon, you can select a report group and, in the right section, select a report, and then click the white arrow to run the report. This action populates the search criteria.

This is the easiest way to get quick results and make your own custom searches.

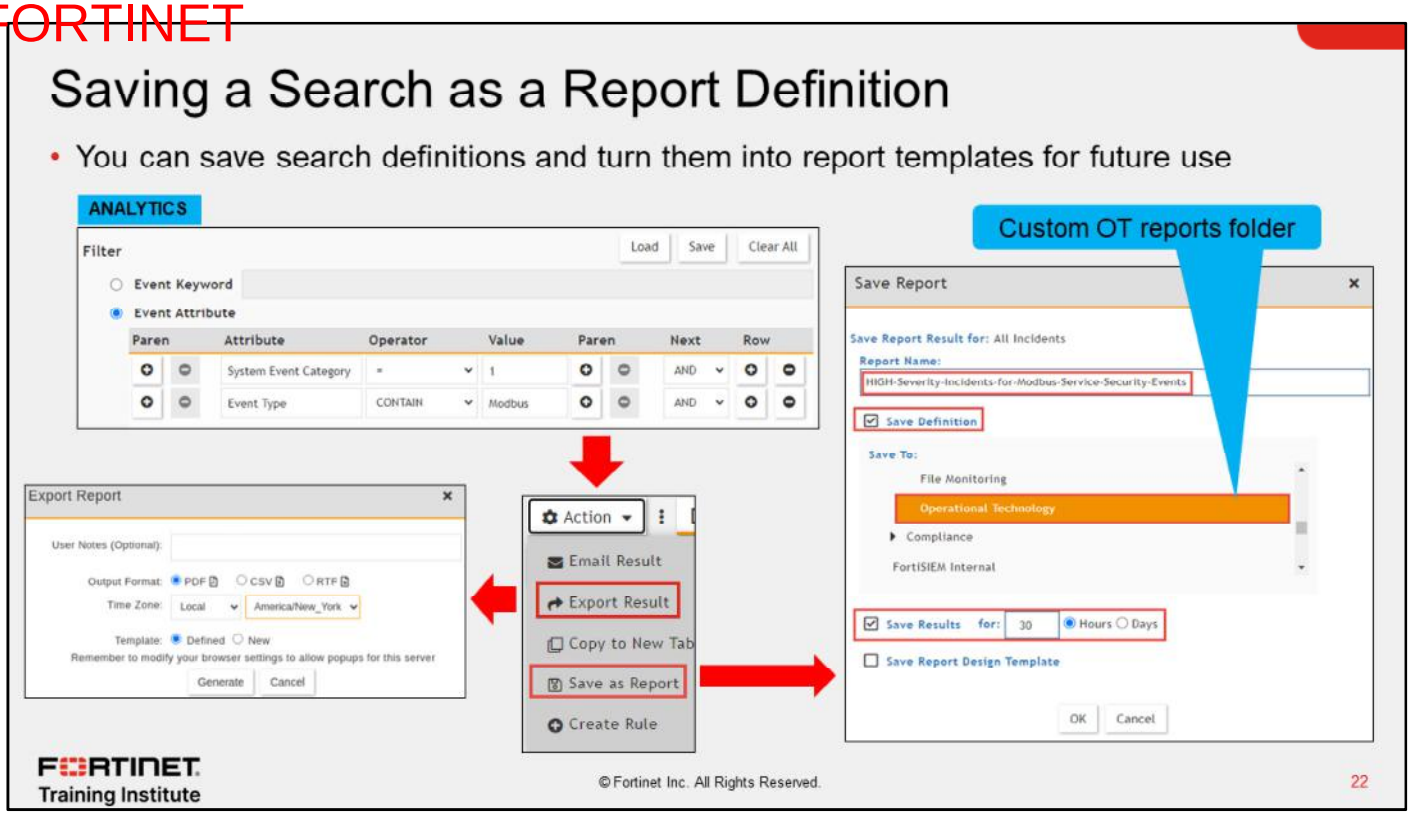
There are two places in the GUI where you can schedule a report.

The first is to select a report, in the lower section, click the **Schedule** tab, and then click **+** to specify when you want it to run.

The second is to select a report and, in the **More** drop-down list, select **Schedule**.

The functionality is the same for both of these methods. Scheduled reports are available in PDF, CSV, and RTF format.

DO NOT REPRINT
© FORTINET

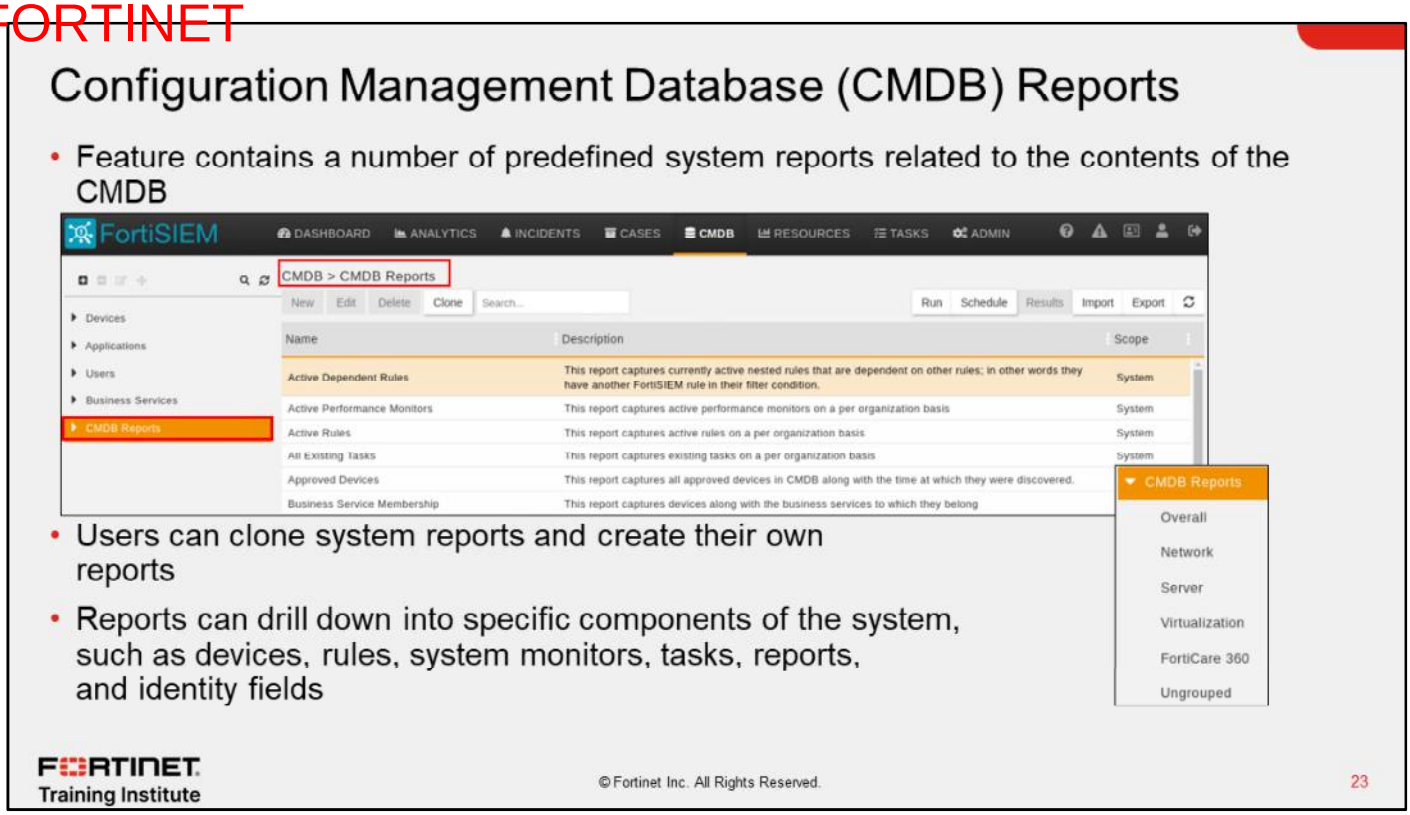


You can save searches and turn them into report definitions for future use by selecting **Save Definition** and providing a name for the report.

You can save the new report definition in any report category group. In the example shown on this slide, the report definition is saved in the custom report category group **Operational Technology**, but you can move it to another category, if you prefer. If you select **Save Results**, report results will also appear in the **Saved Results** section for the specified time period.

You can also save a rule subpattern definition as report.

DO NOT REPRINT
© FORTINET



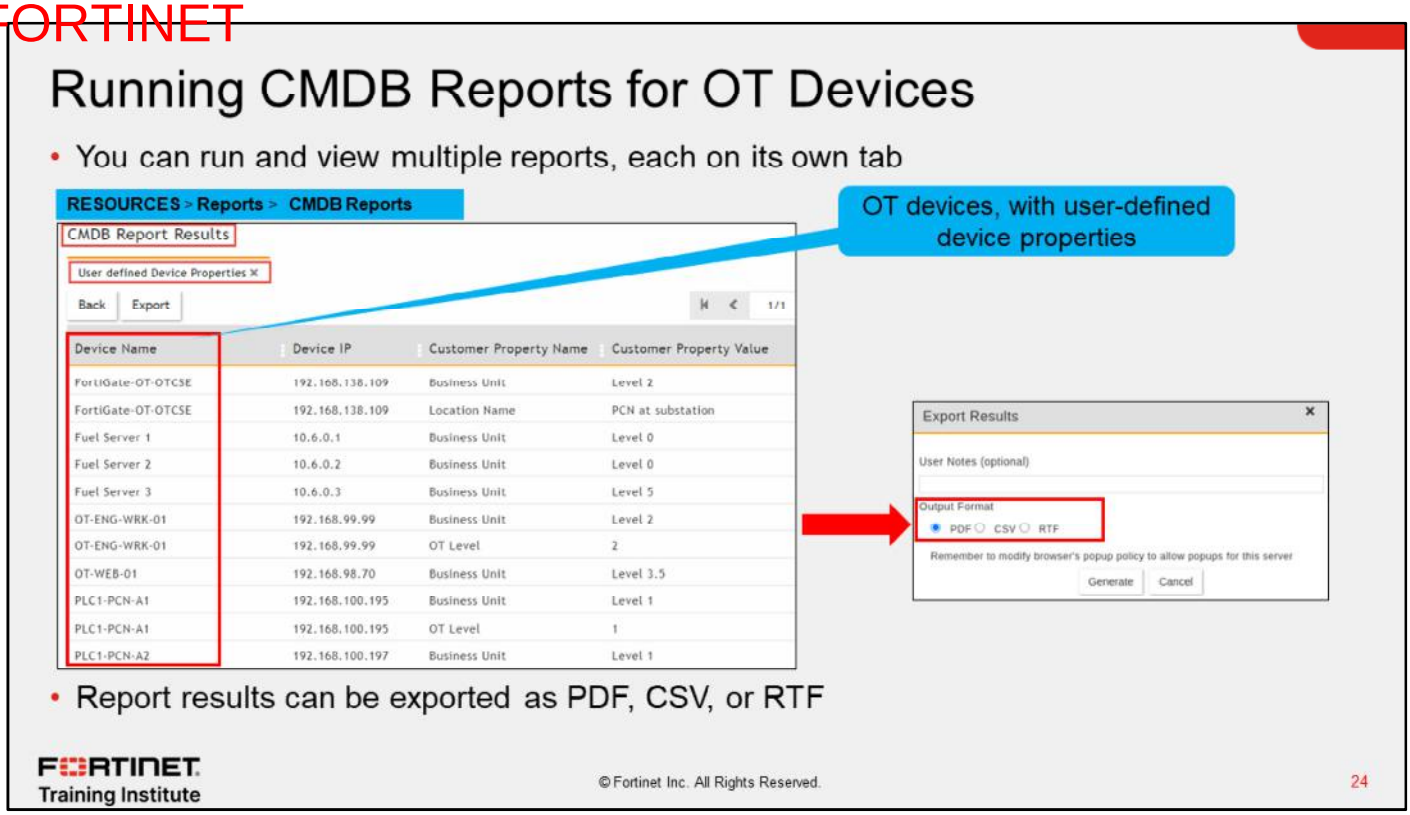
The FortiSIEM CMDB contains a lot of useful information, including system configurations, such as rules and report definitions.

The CMDB reporting feature contains a number of predefined system reports related to the contents of the CMDB.

Users can clone existing system reports, or create their own reports from scratch. These reports follow the same logic as rules and analytic reports in that, if you edit a system report, it will force you to save it with a different name.

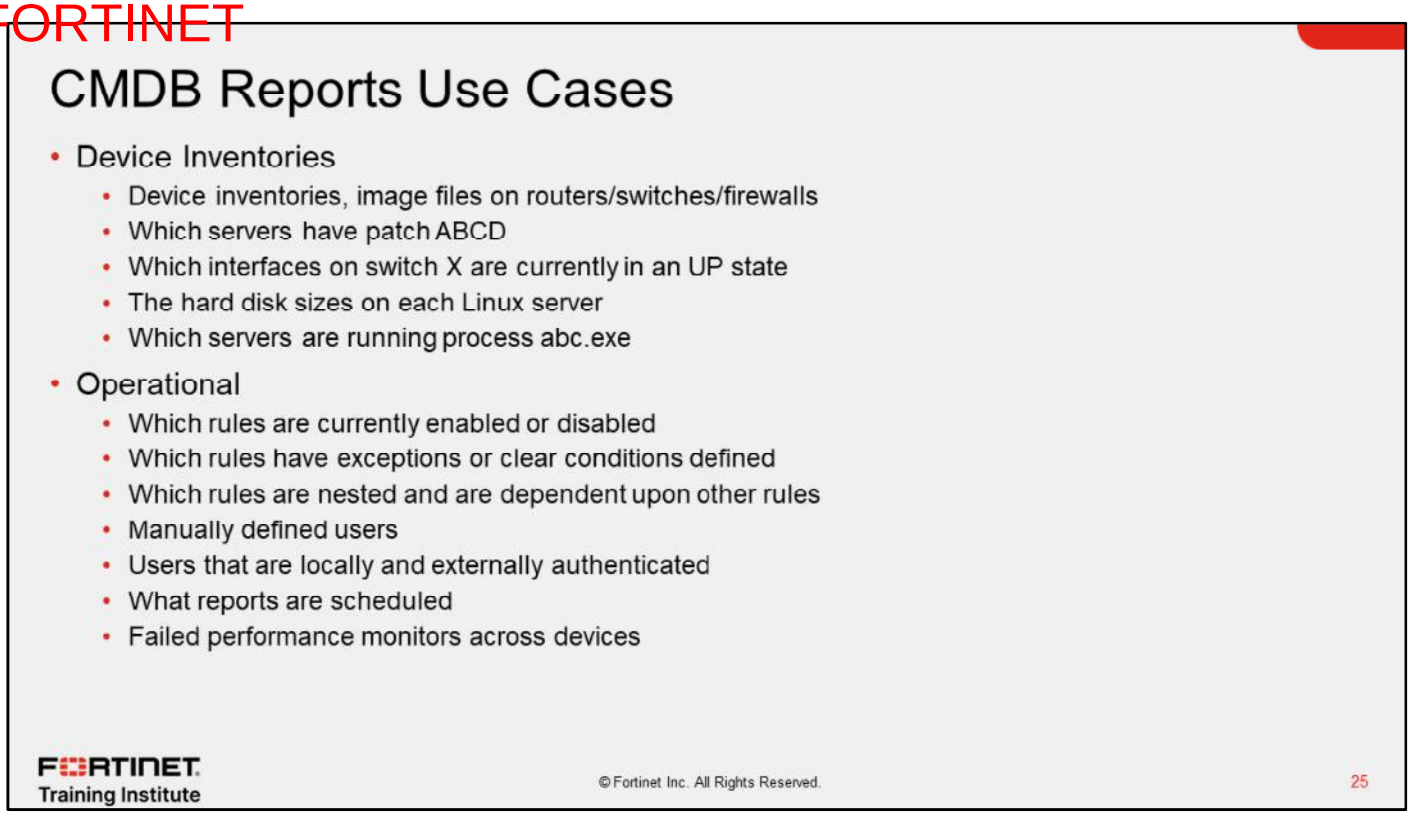
These reports can drill down into specific components of the system, such as devices, rules, system monitors, tasks, reports, identity fields, and more.

DO NOT REPRINT
© FORTINET



When you run CMDB reports, you can run and view multiple reports, each on its own tab. You can export the results as a PDF, CSV, or RTF file.

DO NOT REPRINT
© FORTINET



So what are some of the use cases for the CMDB reporting feature?

One use case for CMDB reports is device inventories. In FortiSIEM, you can run a device inventory report to look at image files on all routers, switches, and firewalls to identify vulnerable firmware versions. You can look at what servers have certain patches installed, or which interfaces on a switch are currently in an up or down state. You can also find answers to these questions:

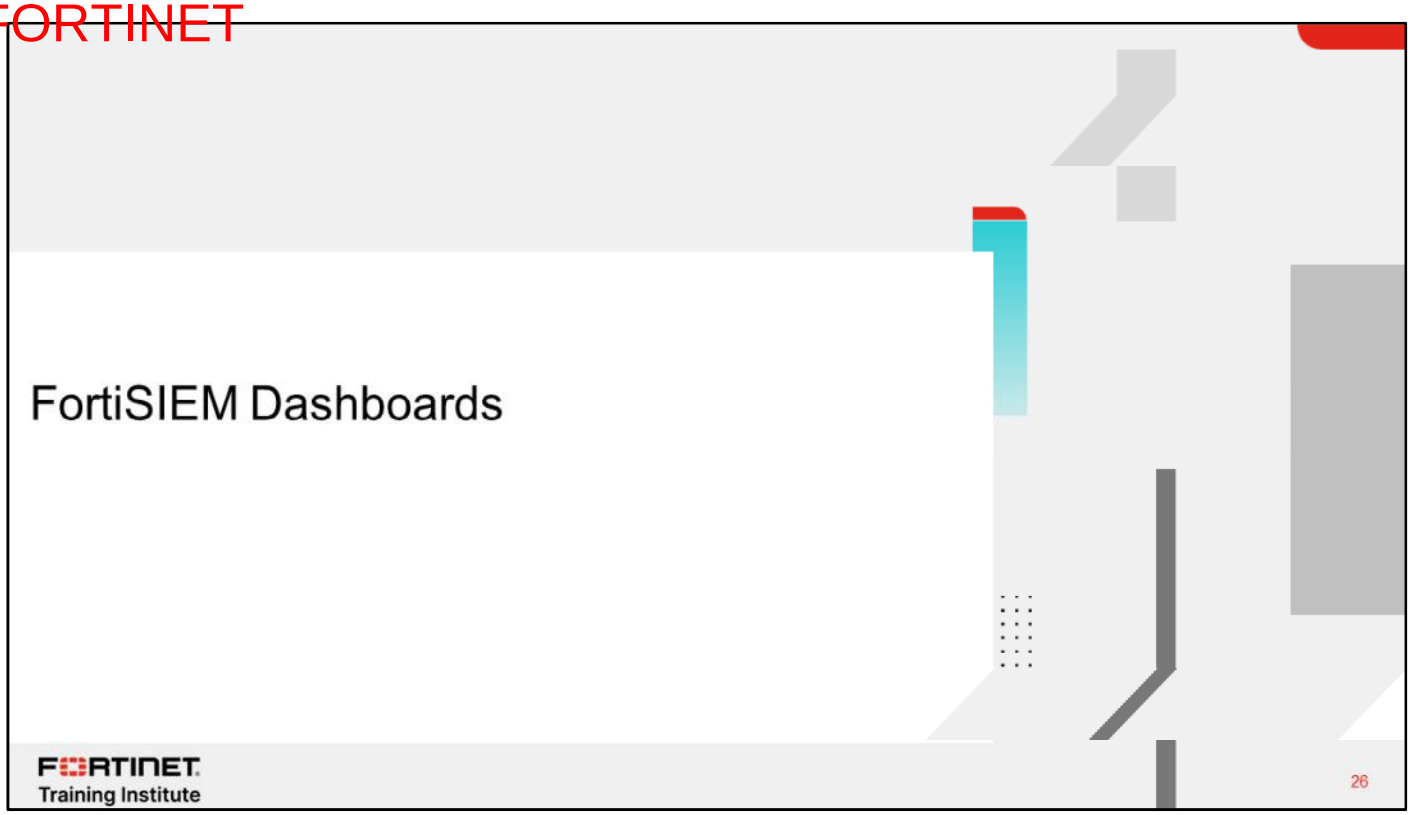
- Device inventories, image files on routers/switches/firewalls
- Which servers have patch ABCD
- Which interfaces on switch X are currently in an UP state
- The hard disk sizes on each Linux server
- Which servers are running process abc.exe

CMDB reports can also answer questions about FortiSIEM operations, such as:

- Which rules are currently enabled or disabled on the system?
- Which rules have exceptions or clear conditions defined?
- Which rules are nested or dependant on other rules? In FortiSIEM, rules can also reference other rules.
- Which users are manually defined?
- Which users are locally and externally authenticated?
- What reports are scheduled?
- Which devices have failed performance monitors?

There are many other use cases. The FortiSIEM reporting feature is rich with in-depth information about the devices in your network, as well as FortiSIEM itself.

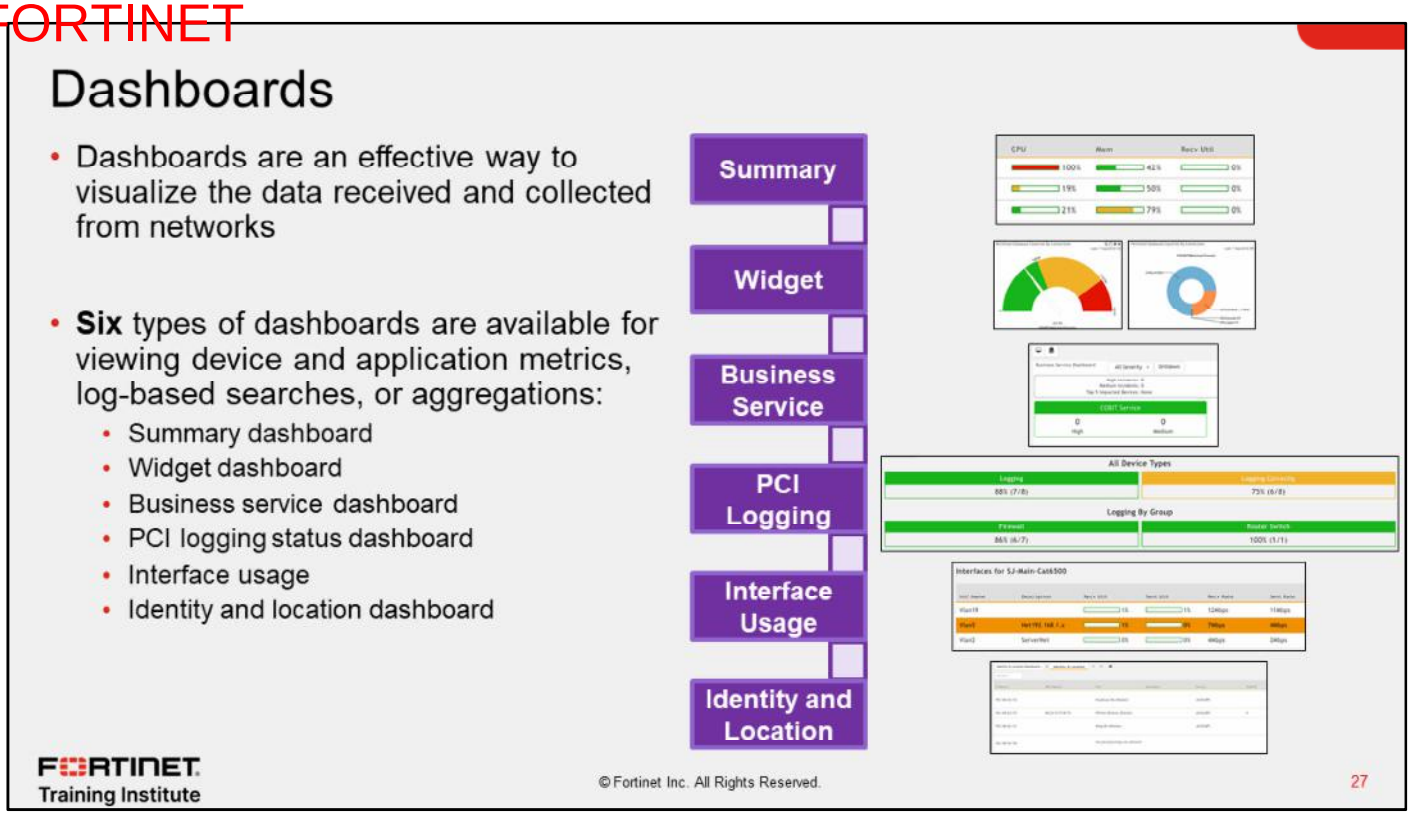
DO NOT REPRINT
© FORTINET



In this section, you will learn about FortiSIEM dashboards for OT networks.

By demonstrating competence in dashboards, you will be able to identify, modify, create, and customize dashboards for OT networks.

DO NOT REPRINT
© FORTINET

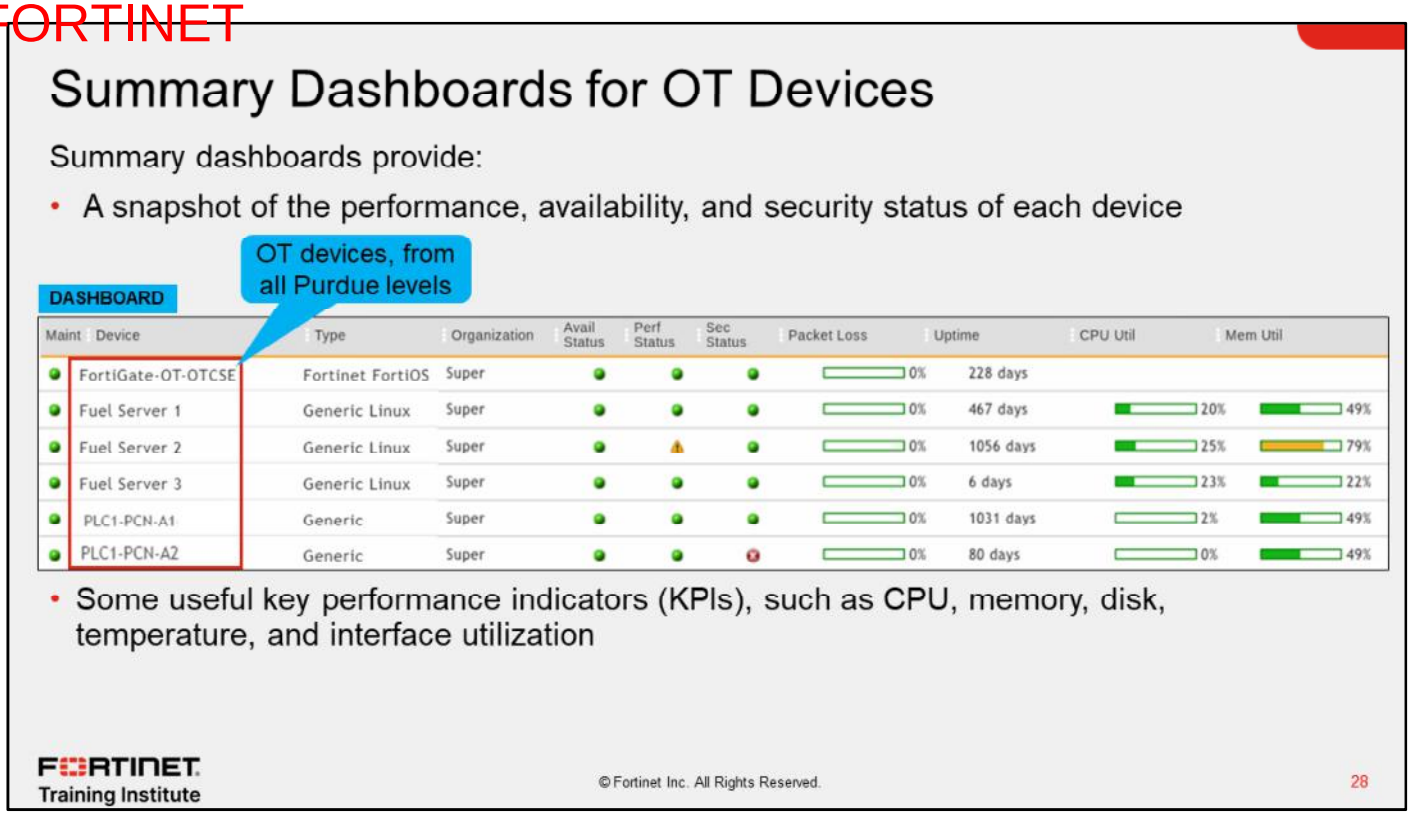


Dashboards are an effective way to visualize the data that has been received or collected from the devices in your network. There are six types of dashboards available for viewing device and application metrics, as well as any log-based search or aggregation of data:

- Summary dashboard
  - Summary dashboards show a near real-time view of health, up-time, incidents, and other key performance metrics of many devices in a single spreadsheet format—each row is a device and each column is a metric.
- Widget dashboard
  - Widget dashboards offer the more traditional top-down dashboard view—one chart for one metric. Each dashboard widget represents a report in the FortiSIEM system.
- Business service dashboard
  - Business service dashboards provide a top-down view of business service health.
- PCI logging status dashboard
  - PCI logging status dashboards provide an overview of which devices in PCI are logging and logging correctly.
- Interface usage
  - Interface usage dashboards provide an overview of the usage of individual interfaces of router and firewall devices.
- Identity and location dashboards
  - Identity and location dashboards provide a tabular view of network-identity-to-user-identity mappings.

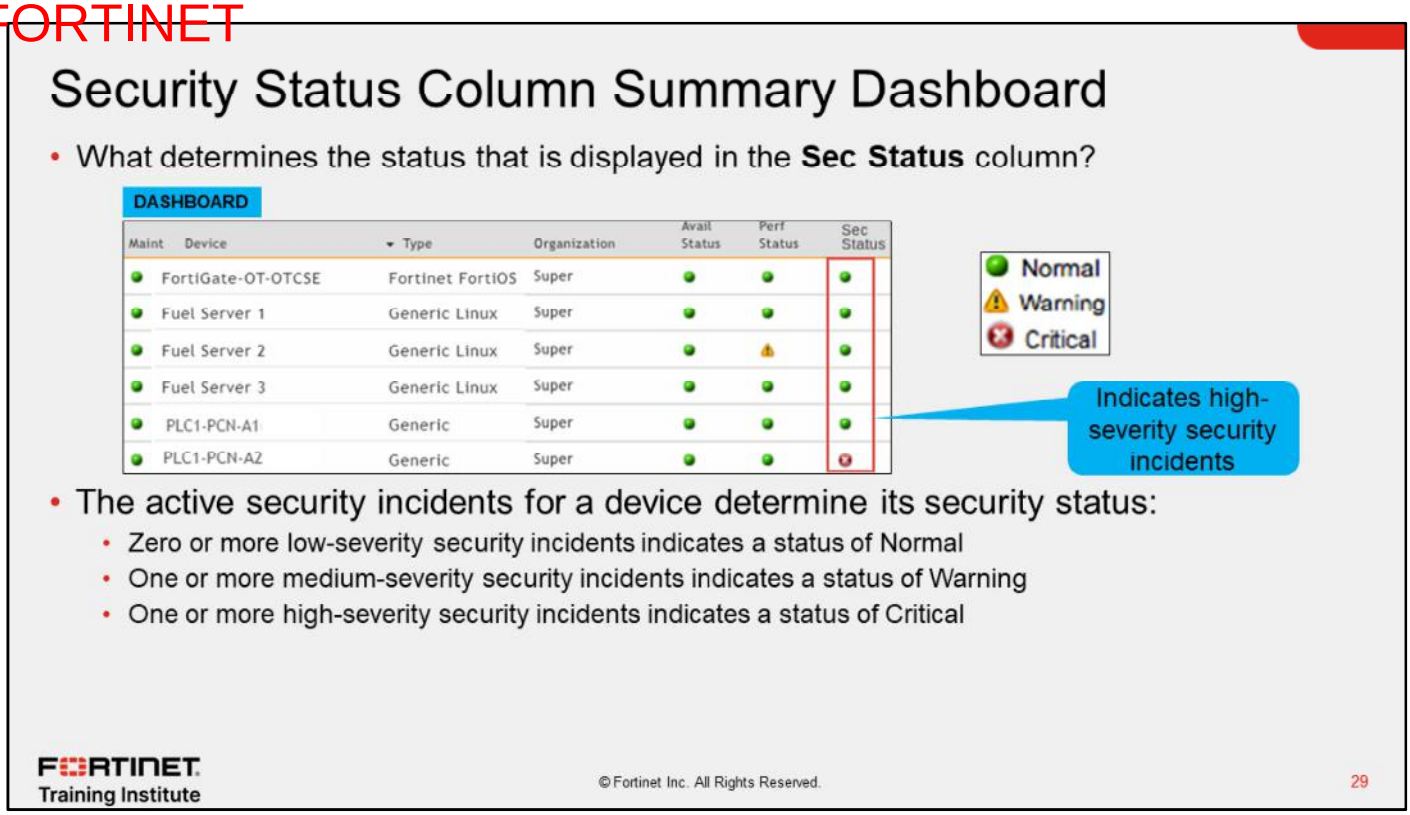
FortiSIEM comes with many default summary and widget dashboards.

DO NOT REPRINT
© FORTINET



Summary dashboards provide a snapshot of the performance, availability, and security status of each device in your environment. They also return some useful KPIs, such as CPU, memory, disk, and interface utilization.

DO NOT REPRINT
© FORTINET



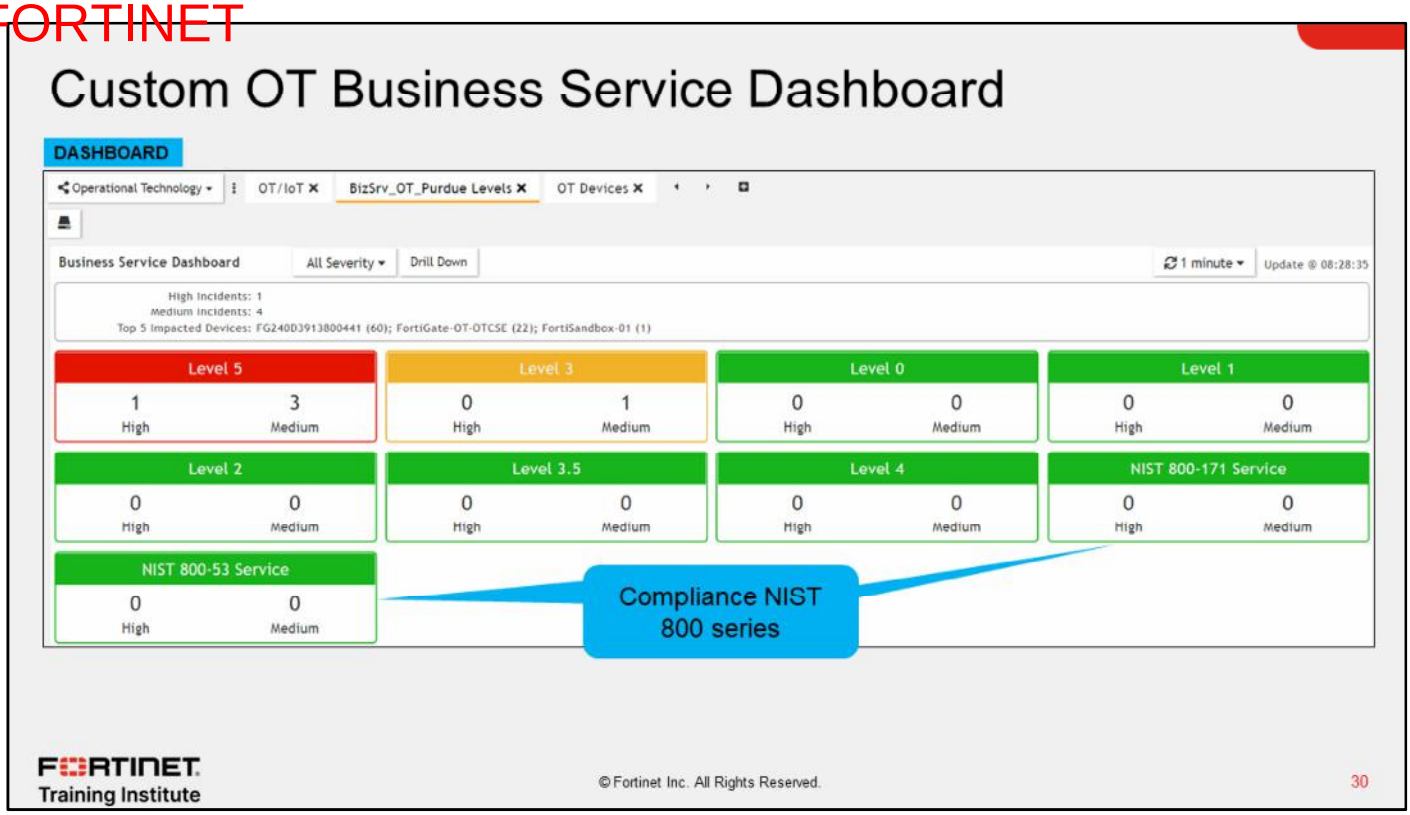
The **Sec Status** column shows the security status of the device. The device status can be: Normal, Warning, or Critical.

The active security incidents for a device determine its security status:
- If there are no security incidents or only low-severity incidents for a device, then that device is assigned a security status of Normal.
- If there are one or more medium-severity incidents for a device, then that device is assigned a security status of Warning.
- If there are one or more high-severity incidents for a device, then that device is assigned a security status of Critical.

The same is true for the **Perf Status** column.

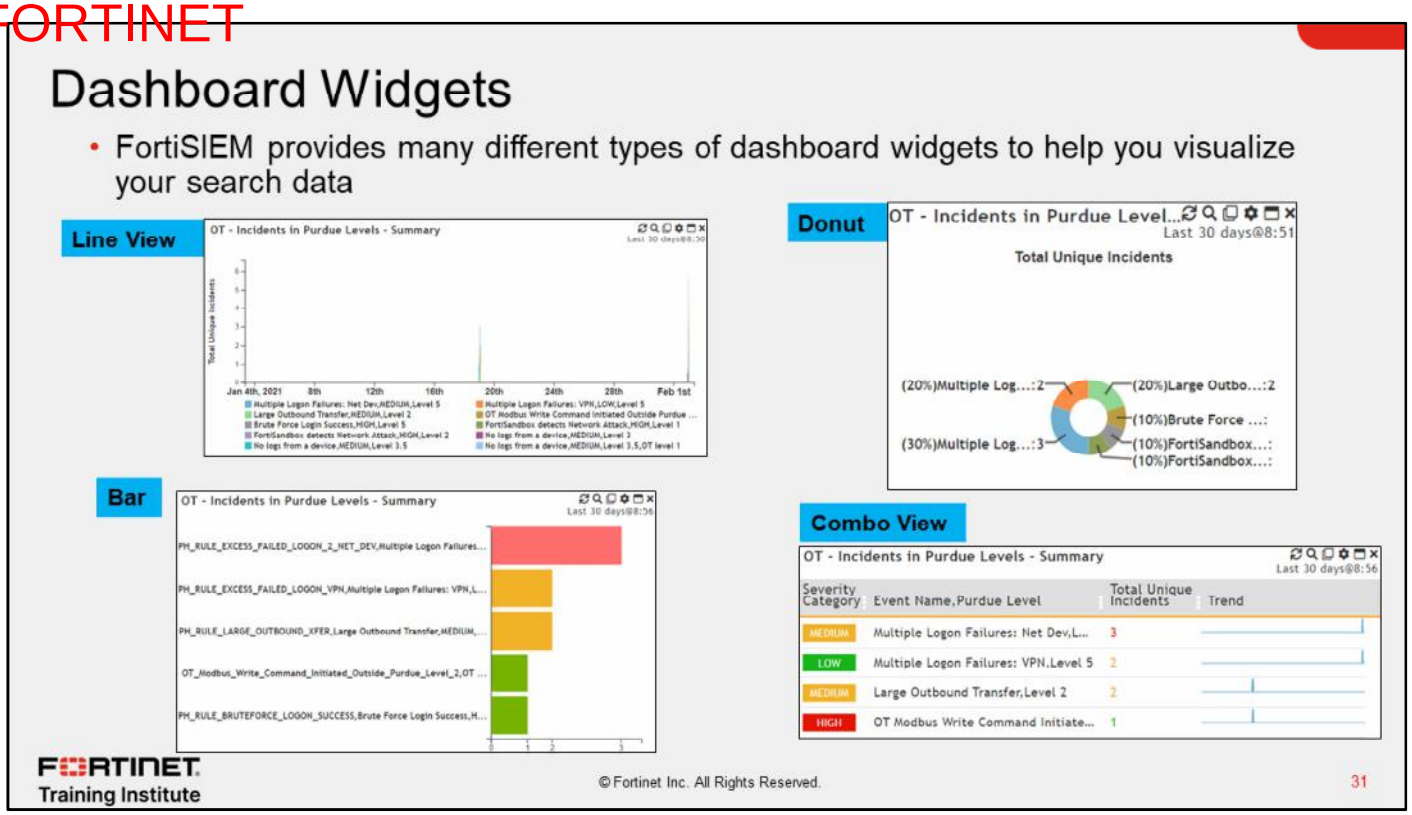
For **Avail Status** column, the status is determined by the PH_DEV_MON_PING_STAT event, which returns a packet loss percentage value:
- If the packet loss report is between 0% and 49%, the device is assigned an availability status of Up.
- If the packet loss report is between 50% and 98%, the device is assigned an availability status of Degraded.
- If the packet loss report is between 99% and 100%, the device is assigned an availability status of Down.

DO NOT REPRINT
© FORTINET



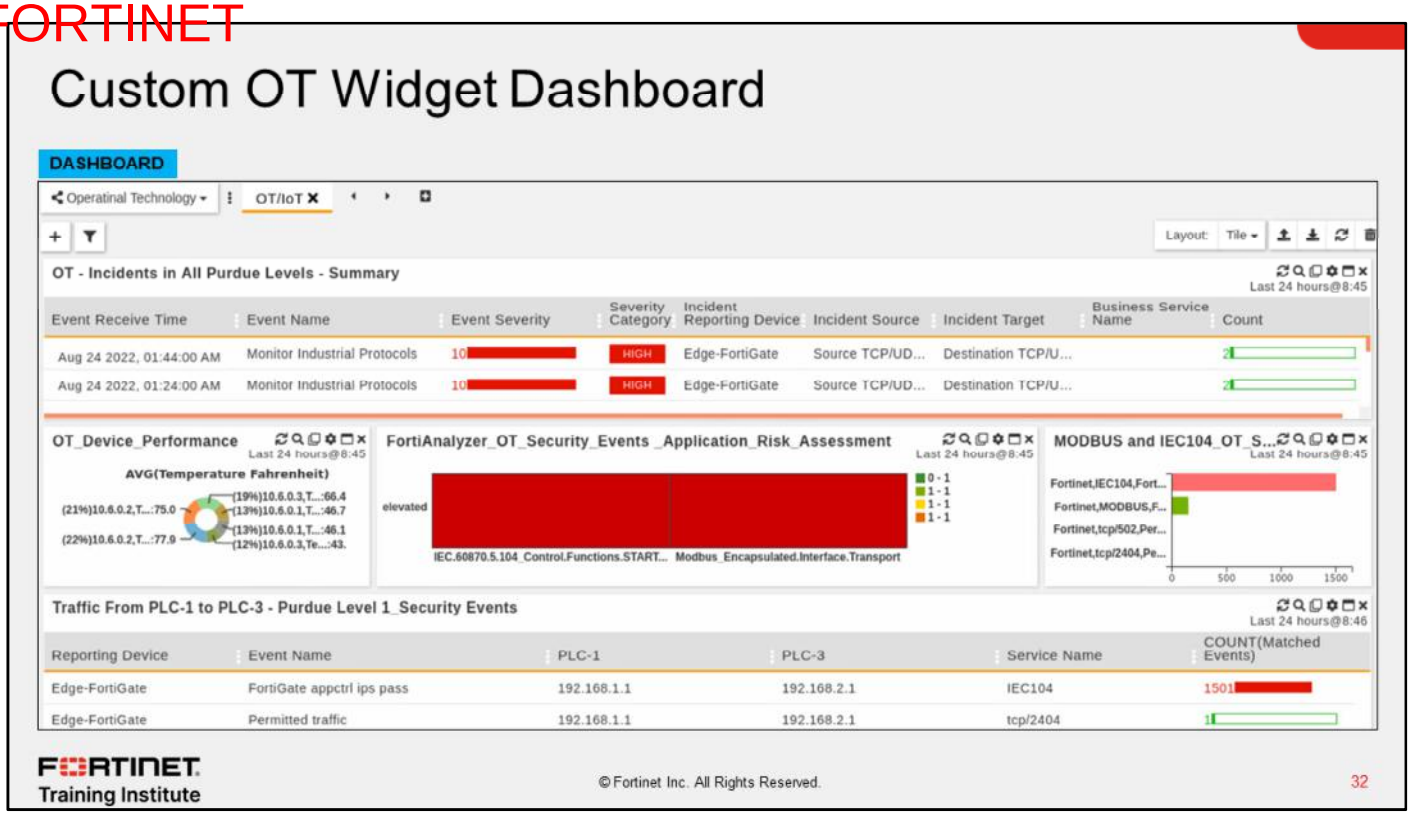
The slide shows an example of a custom OT business service dashboard for all Purdue levels, NIST 800-53 service, and NIST 800-171 service. Business service dashboards provide a top-down view of business service health. You can see the incidents related to each business service and then drill down on the impacted devices and incidents.

DO NOT REPRINT
© FORTINET



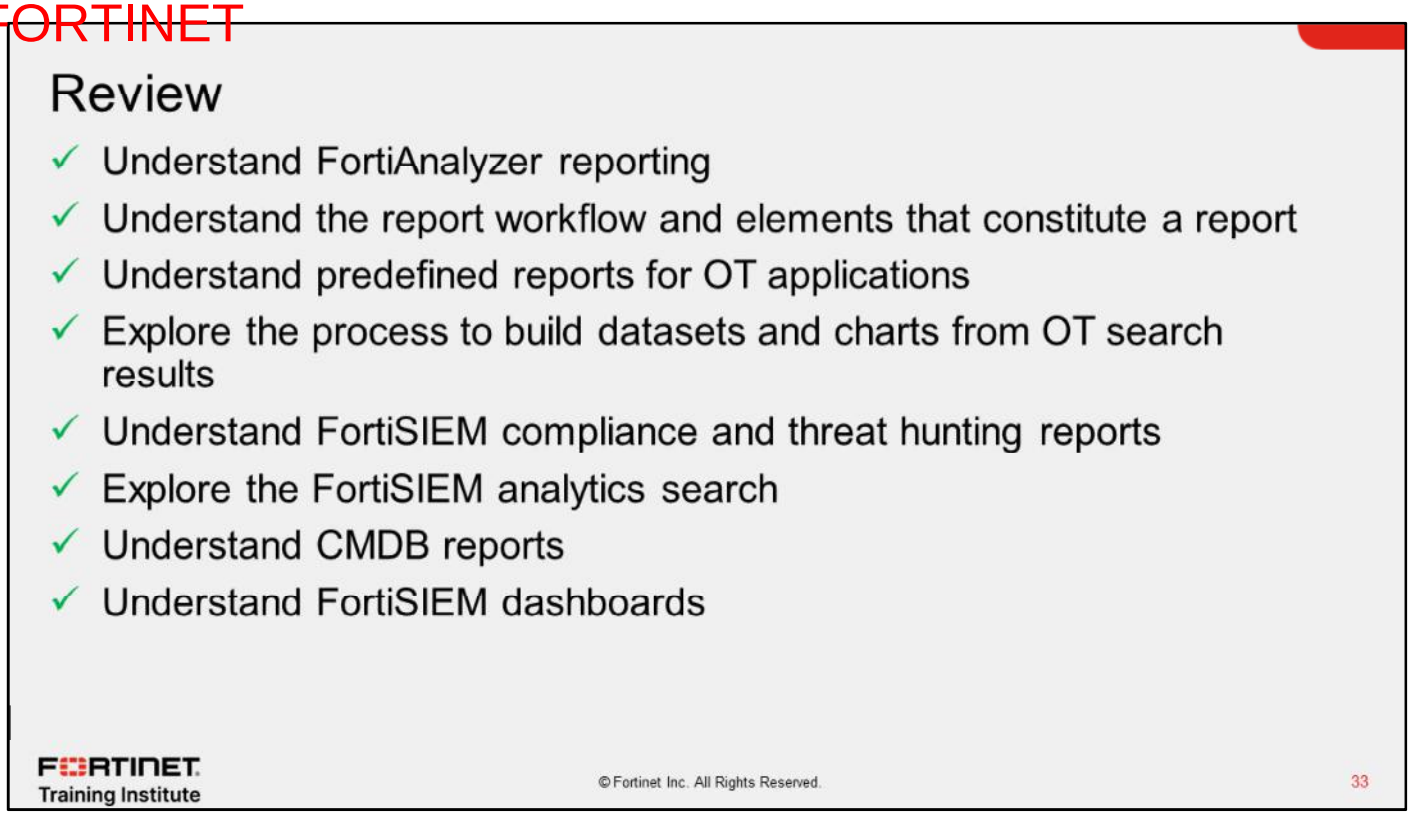
Dashboard widgets provide you with different ways to visualize your search data. Each dashboard widget represents a report in the FortiSIEM system. This slide shows some examples of the widgets that are available: line view, donut (pie chart), bar chart, and combo view. The combo view widget shows the current value, as well as a view of the trend of the value over time.

DO NOT REPRINT
© FORTINET



This slide shows an example of a custom OT widget dashboard. Widget dashboards are an effective way to visualize the data received and collected from OT networks.

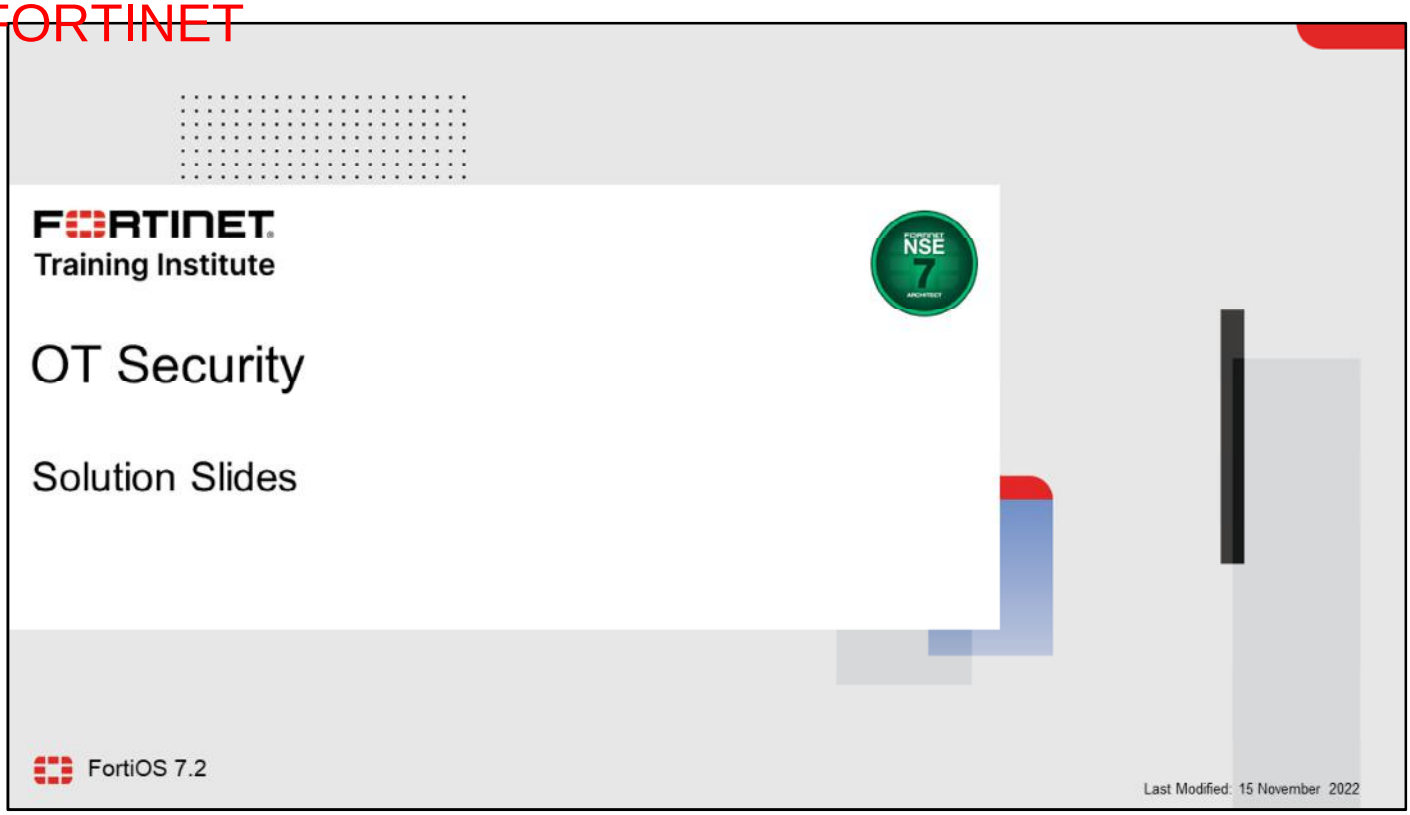
DO NOT REPRINT
© FORTINET



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to effectively use FortiSIEM and FortiAnalyzer reports as part of a risk assessment and management strategy.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about asset management in the OT network.

DO NOT REPRINT
© FORTINET



Now, you will review the solutions for Lab 8—Use Case 1.

DO NOT REPRINT
© FORTINET

Basic Connectivity

- Requirement:
  - Linux-Client must be able to access the following devices without access control:
    - FortiGate-1
    - FortiGate-2
    - FortiAnalyzer
- Solution:
  - Configure the following policies on Edge-FortiGate

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port5	port1	Linux-Client	FortiGate-1	ALL	Disable
port5	port2	Linux-Client	FortiGate-2	ALL	Disable
port5	port3	Linux-Client	FortiAnalyzer	ALL	Disable

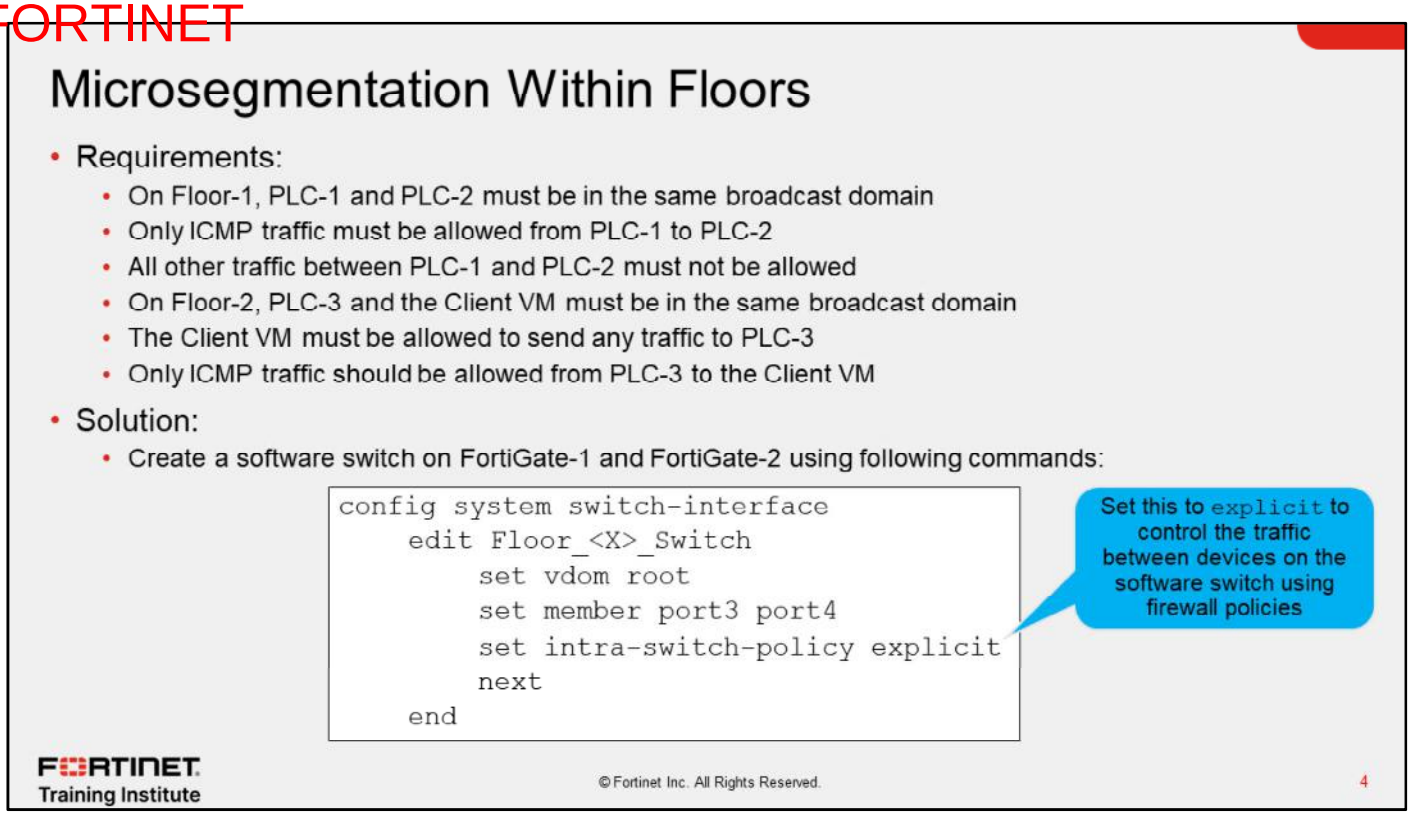
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

3

You must create three policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET



Based on the requirements, you could assume that the interfaces have to be in the same broadcast domain; however, the traffic must be controlled through FortiGate devices. To achieve this goal, use the commands shown on this slide to configure a software switch on FortiGate-1 and FortiGate-2.

DO NOT REPRINT
© FORTINET

Microsegmentation Within Floors (Contd)

- Solution (Contd)
  - Create software switch on FortiGate-1 :

```
config system interface
    edit Floor_1_Switch
        set ip 192.168.1.254 255.255.255.0
        set allowaccess ping
    next
end
```

  - Create software switch on FortiGate-2 :

```
config system interface
    edit Floor_2_Switch
        set ip 192.168.2.254 255.255.255.0
        set allowaccess ping
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

DO NOT REPRINT
© FORTINET

Microsegmentation Within Floors (Contd)

- Solution:
  - To allow access based on the requirements, create the following policies:
    - FortiGate-1:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port3	port4	PLC-1	PLC-2	PING	Disable

    - FortiGate-2:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port4	port3	Client	PLC-3	ALL	Disable
port3	port4	PLC-3	Client	PING	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

You will need to create policies on FortiGate-1 and FortiGate-2, as shown on this slide, to fulfill the requirement. The address objects are already created on the FortiGate devices. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Segment Floors

- Requirement:
  - All traffic between floors must be controlled through Edge-FortiGate
  - Allow Linux-Client to access PLC-1, PLC-2, PLC-3, and the Client VM over SSH without access control
- Solution:
  - Traffic is on two different interfaces with separate subnets, traffic is set up between floors, and traffic has to pass through Edge-FortiGate
  - To allow SSH traffic, create the following policies on Edge-FortiGate:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port5	port1	Linux-Client	PLC-1, PLC-2	SSH	Disable
port5	port2	Linux-Client	PLC-3, Client	SSH	Disable

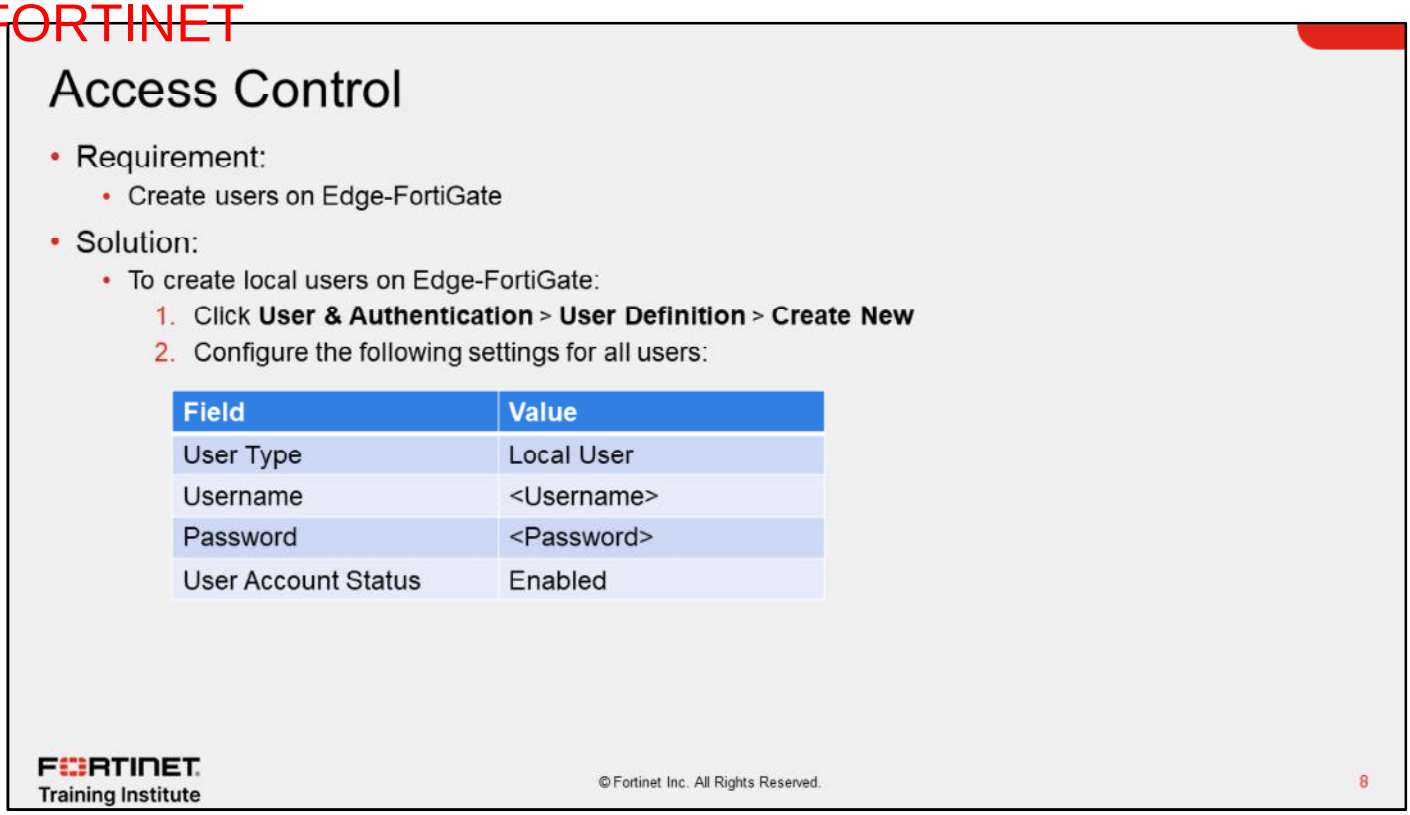
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

You will need to create two policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET



You will need to create the local users, as shown on this slide, to fulfill the requirement.

DO NOT REPRINT
© FORTINET

Access Control (Contd)

- Requirement:
  - Create policies to allow traffic from the Linux-Client VM to the following devices using access control:
    - supervisor must be allowed to access PLC-1, PLC-2, PLC-3, and the Client VM over HTTP
    - jradmin must be allowed to access PLC-3 over HTTP
    - sradmin must be allowed to access all PLCs on Floor-1 over HTTP
    - client1 must have access to the Client VM over HTTP
- Solution: Create following policies, in the order shown here, on Edge-FortiGate:

Source Interface	Destination Interface	Source Address	Source User	Destination Address	Service	NAT
port5	port1, port2	Linux-Client	supervisor	PLC-1, PLC-2,PLC-3,Client	HTTP	Disable
port5	port2	Linux-Client	jradmin	PLC-3	HTTP	Disable
port5	port1	Linux-Client	sradmin	PLC-1,PLC-2	HTTP	Disable
port5	port2	Linux-Client	client1	CLIENT	HTTP	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

You will need to create four policies, as shown on this slide, to fulfill the requirement. The address objects are already created on the FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Access Control (Contd)

- Solution:
  - To allow HTTP access based on the requirements, create the following policies:
    - FortiGate-1:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	Floor_1_Switch	Linux-Client	PLC-1, PLC-2	HTTP	Disable

    - FortiGate-2:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	Floor_2_Switch	Linux-Client	PLC-3, CLIENT	HTTP	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

You will need to create on FortiGate-1 and FortiGate a firewall policy to allow HTTP traffic from Linux-Client to PLC-1, PLC-2, PLC-3, and CLIENT. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Log Traffic

- Requirement:
  - Configure devices so Edge-FortiGate can send logs in real time to FortiAnalyzer for storage and reporting

- Solution:
  - On Edge-FortiGate:
    1. Click **Security Fabric** > **Fabric Connectors**
    2. Click **FortiAnalyzer logging**, and then click **Edit**
    3. In the **FortiAnalyzer Settings** section, click **Enabled**
    4. In the **IP address** field, type `10.1.3.210`, and then select **Real Time** in **Upload Options**
    5. Click **OK**, and then click **Accept**
    6. Click **Close**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

DO NOT REPRINT
© FORTINET

Log Traffic (Contd)

- Solution (Contd):
  - On FortiAnalyzer:
    1. Click **Device Manager**
    2. Click the **Unauthorized Devices**
    3. Select the **Edge-FortiGate** device, and then click **Authorize**, and then click **OK**
    4. Click **Close**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

DO NOT REPRINT
© FORTINET

Protect the OT Network

- Requirement:
  - Allow all Modbus traffic from the Client VM to PLC-2, except for traffic that matches the **Modbus_Exception.Illegal.Function** signature
  - Log all traffic from the Client VM to PLC-2

- Solution:
  - Remove the industrial signatures from the `exclude-signature` list from the CLI:
    - Use the following commands on the Edge-FortiGate CLI:

```
config ips global
      set exclude-signature none
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

DO NOT REPRINT
© FORTINET

Protect the OT Network (Contd)

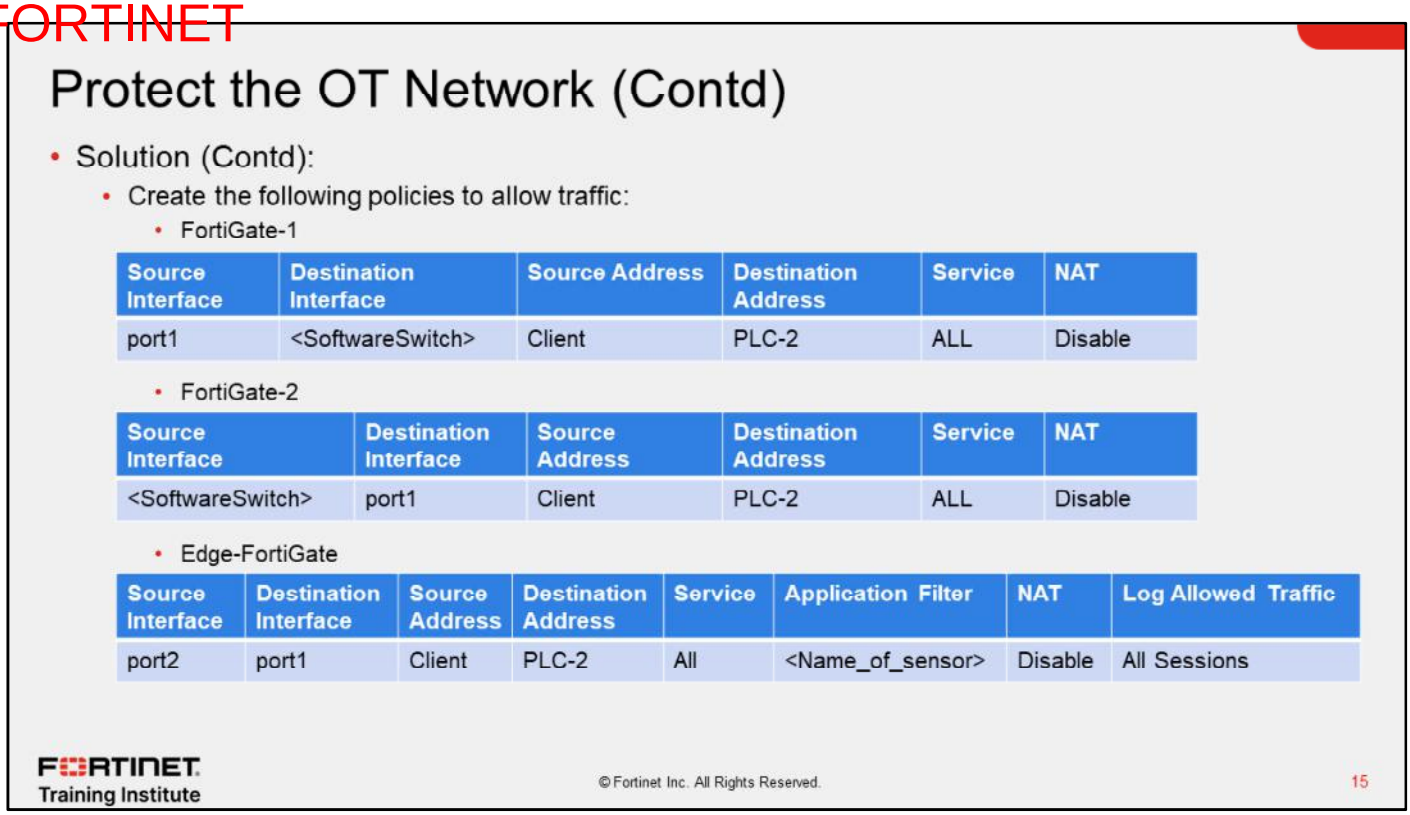
- Solution (Contd):
  - Create the following application filter on Edge-FortiGate:
    1. Click **Security Profiles** > **Application Control** > **Create New**
    2. In the **Name** field, type `Allow_Modbus_Transfer`
    3. Under **Application and Filter Overrides**, click **Create New**
    4. In the search field, type `Modbus` to list all matching signatures
    5. Look for the **Modbus_Exception.Illegal.Function** signature, and then click to select the signature
    6. Right-click the selected signature, and then click **Add selected**
    7. Click **OK**
    8. Click **OK** to save the application sensor

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

DO NOT REPRINT
© FORTINET



Protect the OT Network (Contd)

- Solution (Contd):
  - Create the following policies to allow traffic:
    - FortiGate-1

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	<SoftwareSwitch>	Client	PLC-2	ALL	Disable

    - FortiGate-2

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
<SoftwareSwitch>	port1	Client	PLC-2	ALL	Disable

    - Edge-FortiGate

Source Interface	Destination Interface	Source Address	Destination Address	Service	Application Filter	NAT	Log Allowed Traffic
port2	port1	Client	PLC-2	All	<Name_of_sensor>	Disable	All Sessions

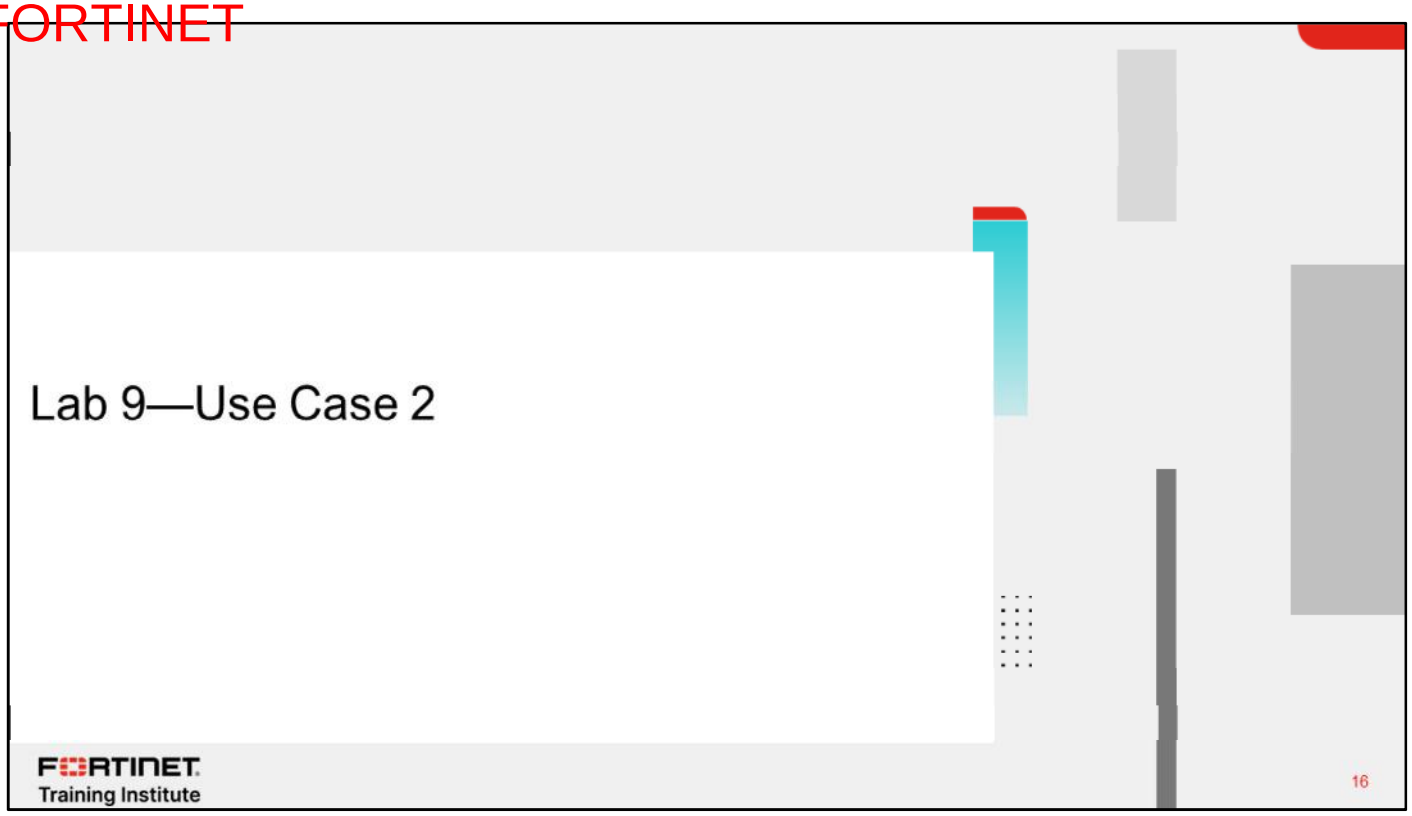
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

You will need to create the policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET



Now, you will review the solutions for Lab 9—Use Case 2.

DO NOT REPRINT
© FORTINET

Basic Connectivity

- Requirement:
  - Linux-Client must be able to access the following devices without access control:
    - FortiGate-1
    - FortiGate-2
    - FortiAnalyzer
    - FortiSIEM
- Solution:
  - On Edge-FortiGate configure the following policies:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port5	Floors	Linux-Client	FortiGate-1	ALL	Disable
port5	Floors	Linux-Client	FortiGate-2	ALL	Disable
port5	port3	Linux-Client	FortiAnalyzer, FortiSIEM	ALL	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

You will need to create four policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Administrator Accounts

- Requirements:
  - Create administrator accounts on FortiGate-1 and FortiGate-2
- Solution:
  - Create the following accounts on FortiGate-1 and FortiGate-2
    1. Click **System** > **Administrators** > **Create New** > **Administrator**
    2. Fill in the following, and then click **OK**:

Field	Value
Username	supervisor
Type	Local User
Password	fortinet
Confirm Password	fortinet
Administrator Profile	super_admin

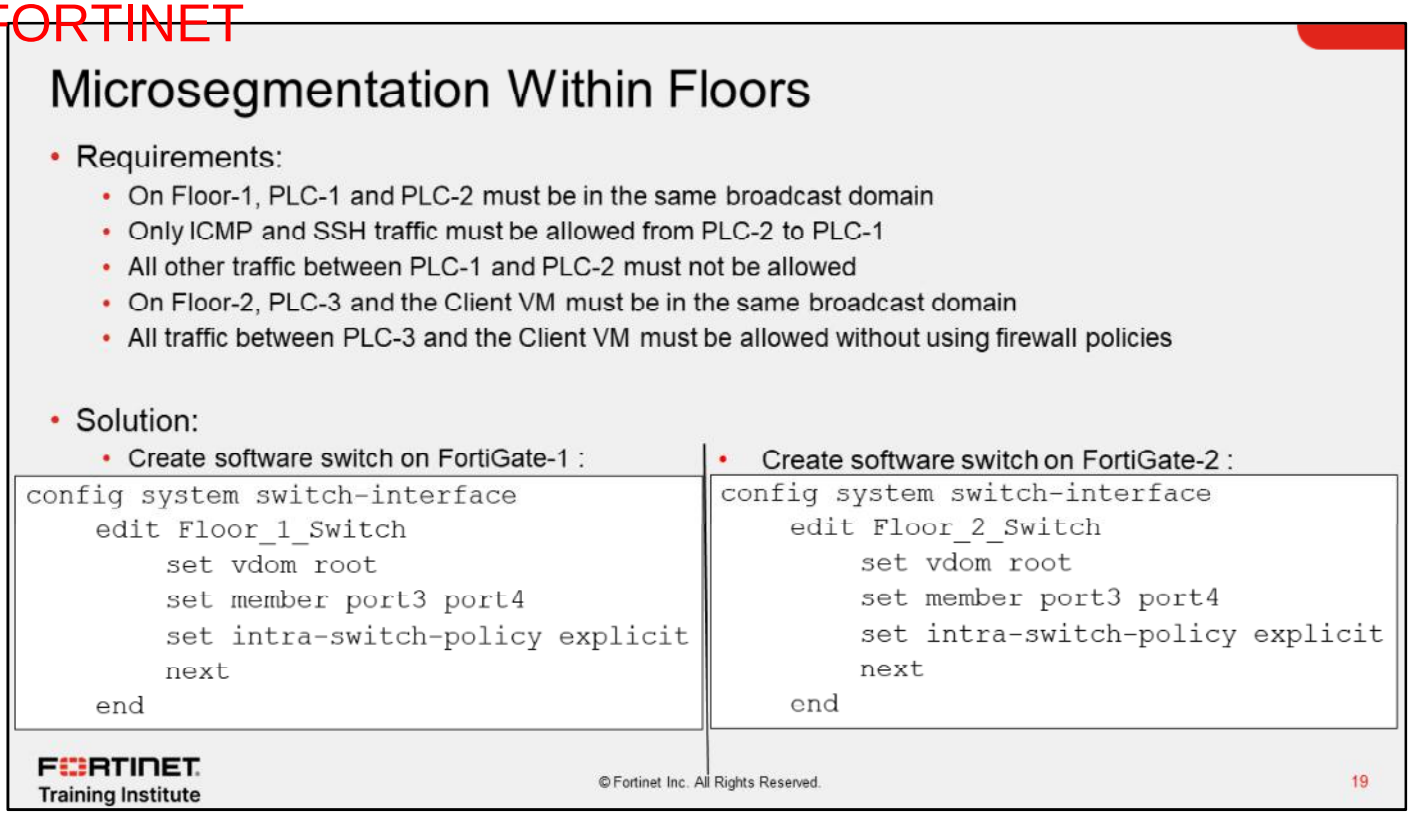
Field	Value
Username	admin_1
Type	Local User
Password	fortinet
Confirm Password	fortinet
Administrator Profile	super_admin_readonly

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

DO NOT REPRINT
© FORTINET



Based on the requirements, you could assume that the interfaces have to be in the same broadcast domain; however, the traffic must be controlled through FortiGate devices. To achieve this, use the commands shown on this slide to configure the software switch on FortiGate-1 and FortiGate-2.

DO NOT REPRINT
© FORTINET

Microsegmentation Within Floors (Contd)

- Solution (Contd)
  - Create software switch on FortiGate-1:

```
config system interface
    edit Floor_1_Switch
        set ip 192.168.1.254 255.255.255.0
        set allowaccess ping
    next
end
```

  - Create software switch on FortiGate-2:

```
config system interface
    edit Floor_2_Switch
        set ip 192.168.2.254 255.255.255.0
        set allowaccess ping
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

DO NOT REPRINT
© FORTINET

Microsegmentation Within Floors (Contd)

- Solution:
  - To allow access based on the requirements, create the following policies:
    - FortiGate-1:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port4	port3	PLC-2	PLC-1	SSH, PING	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

You will need to create policies on FortiGate-1, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate devices. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Segment Floors

- Requirement:
  - All traffic between floors must be controlled through Edge-FortiGate
  - Configure firewall policies and routes to allow Linux-Client to access PLC-1, PLC-2, PLC-3, and the Client VM over SSH without access control
- Solution:
  - Traffic is already on two different interfaces with separate subnets, with the routing setup between floors, traffic has to pass through Edge-FortiGate
  - Create the following policies on Edge-FortiGate to allow SSH traffic:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
Port5	Floors	Linux-Client	PLC-1, PLC-2, PLC-3, Client	SSH	Disable

  - Also, create the following static routes on Edge-FortiGate

Destination	Gateway Address	Interface	Status
192.168.1.0/24	10.1.1.1	port1	Enable
192.168.2.0/24	10.1.2.1	port2	Enable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

You will need to create policies and static routes, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate devices. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Access Control

- Requirement:
  - Create users on Edge-Fortigate
- Solution:
  - To create local users on Edge-FortGate:
    1. Click **User & Authentication** > **User Definition** > **Create New**
    2. Configure the following settings for all users:

Field	Value
User Type	Local User
Username	<Username>
Password	<Password>
User Account Status	enable

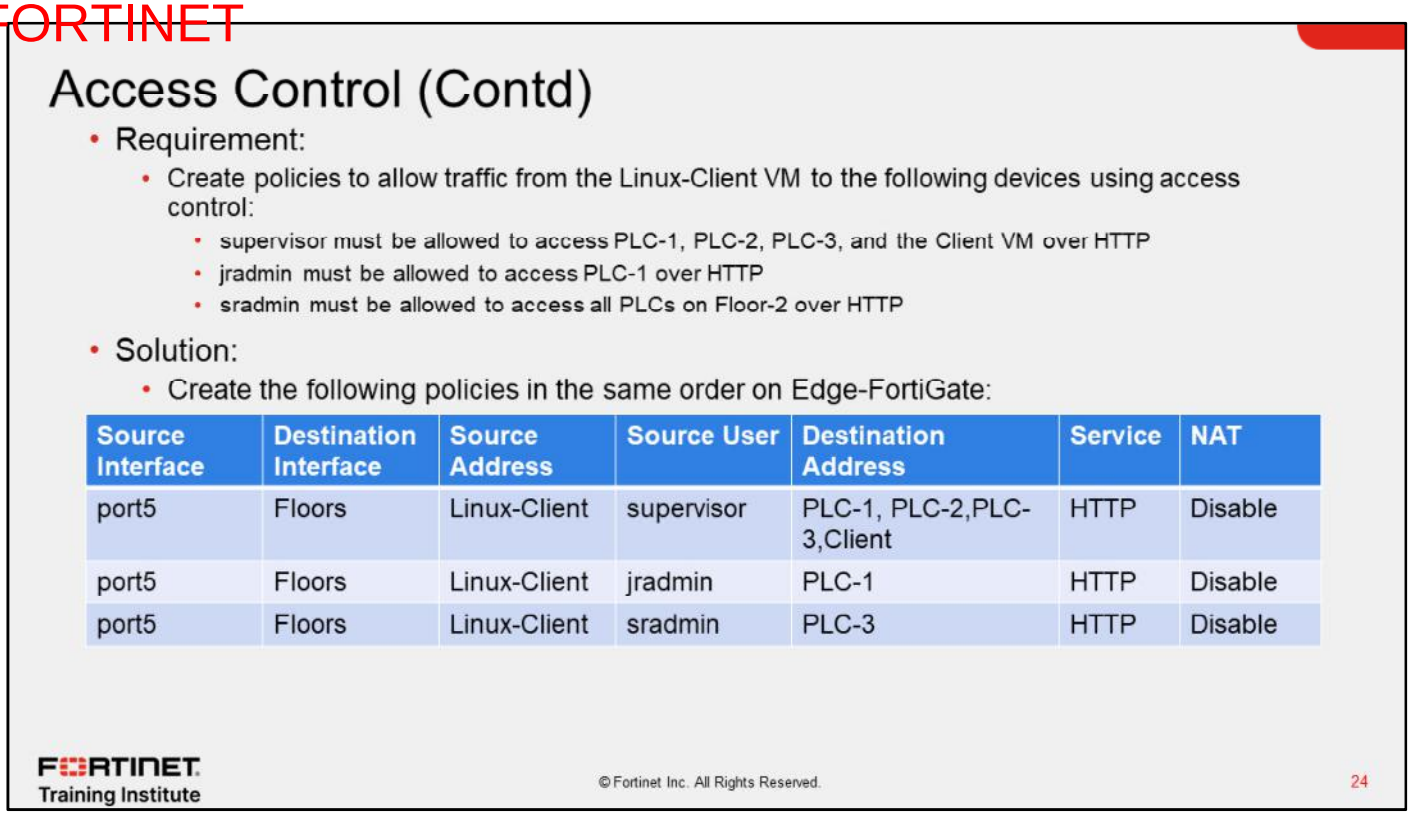
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

You will need to create local users, as shown on this slide, to fulfill the requirement.

DO NOT REPRINT
© FORTINET



You will need to create policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate devices. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Access Control (Contd)

- Solution:
  - To allow HTTP access based on the requirements, create the following policies:
    - FortiGate-1:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	Floor_1_Switch	Linux-Client	PLC-1, PLC-2	HTTP	Disable

    - FortiGate-2:

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	Floor_2_Switch	Linux-Client	PLC-3, CLIENT	HTTP	Disable

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

You will need to create on FortiGate-1 and FortiGate a firewall policy to allow HTTP traffic from Linux-Client to PLC-1, PLC-2, PLC-3, and CLIENT. The address objects are already created on FortiGate. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET

Log Traffic

- Requirement:
  - Configure devices so Edge-FortiGate can send logs in real time to FortiAnalyzer for storage and reporting
  - Configure devices so Edge-FortiGate can send logs to FortiSIEM
- Solution:
  - On Edge-FortiGate:
    1. Click **Security Fabric** > **Fabric Connectors**
    2. Click **FortiAnalyzer logging**, and then click **Edit**
    3. In the **FortiAnalyzer Settings** section, click **Enabled**
    4. Configure `10.1.3.210` as **IP address**, and select **Real Time** in **Upload Options**
    5. Click **OK**
    6. Click **Accept**, then click **Close**
  - On Edge-FortiGate:
    1. Click **Log & Report** > **Log Settings**
    2. Enable **Send logs to syslog**
    3. Enter `10.1.3.180` in **IP Address/FQDN** field
    4. Click **Apply**, then click **OK**. Click **Close**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

DO NOT REPRINT
© FORTINET

Log Traffic (Contd)

- Solution (Contd.):
  - On FortiAnalyzer:
    1. Click **Device Manager**
    2. Click the **Unauthorized Devices** that indicates that one device is unregistered
    3. Select the **Edge-FortiGate** device, and then click **Authorize**, **OK**, and **Close**
    4. Select the **Edge-FortiGate** device, and then click **Edit**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

DO NOT REPRINT
© FORTINET

Protect the OT Network

- Requirement:
  - Allow and monitor only IEC-104 traffic from PLC-2 to PLC-3, except traffic that matches the IEC.60870.5.104_Information.Transfer.C.BO.NA.1 signature
  - Block all other industrial signatures from PLC-2 to PLC-3
  - Log all traffic from PLC-2 to PLC-3
- Solution:
  - First remove industrial signatures from `exclude-signature` list from CLI
    - Use the following commands on the Edge-FortiGate CLI:

```
config ips global
      set exclude-signature none
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

DO NOT REPRINT
© FORTINET

Protect the OT Network (Contd)

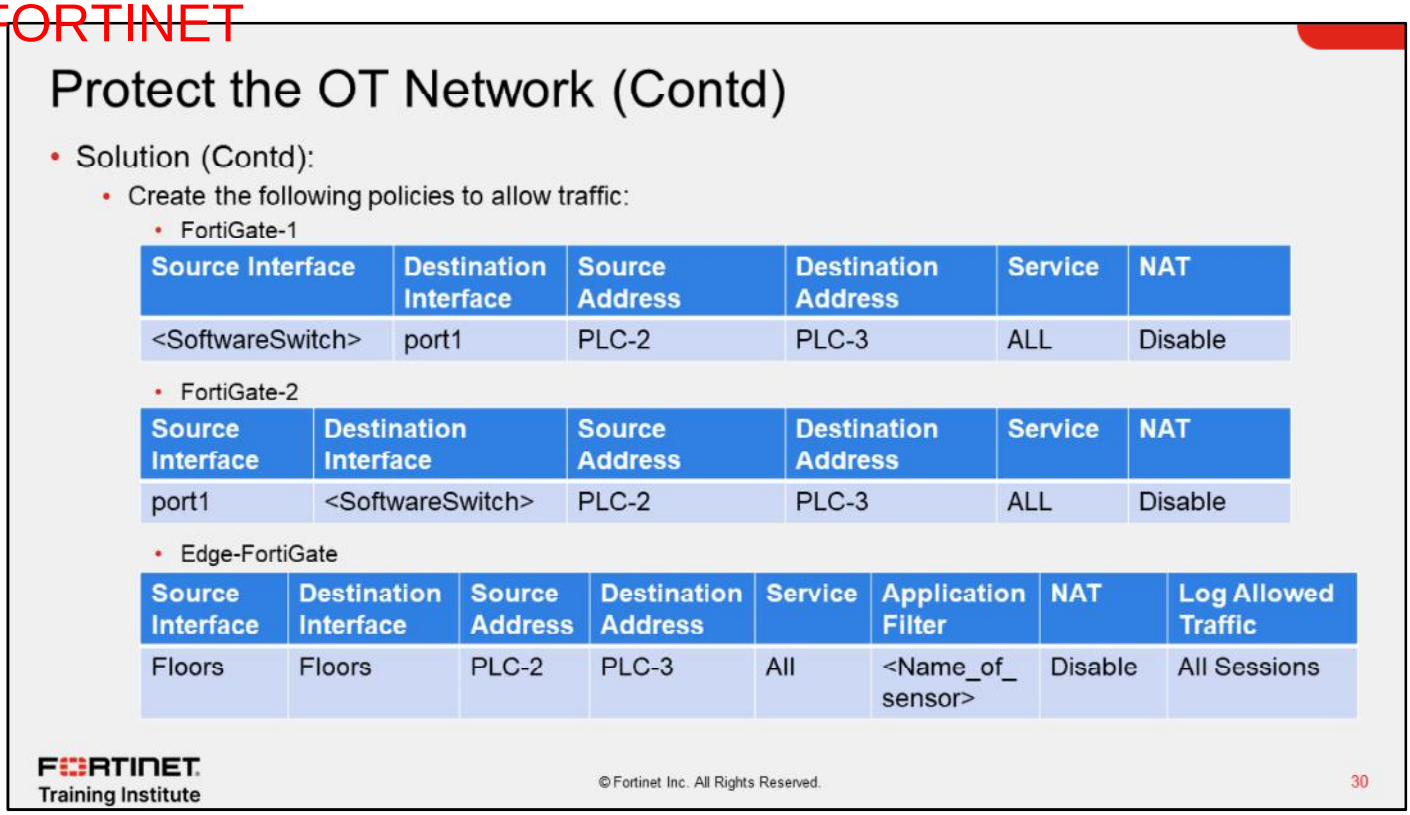
- Solution (Contd):
  - Create the following application filter on Edge-FortiGate:
    1. Click **Security Profiles** > **Application Control** > **Create New**
    2. In the **Name** field, type Allow_IEC-104_Transfer
    3. Under **Categories**, select **Block** for **All Categories**
    4. Under **Application and Filter Overrides**, click **Create New**
    5. In the search field, type `IEC.60870.5.104` to list all matching signatures
    6. Look for the **IEC.60870.5.104_Information.Transfer.C.BO.NA.1** signature, and then click to select the signature
    7. Right-click the signature, click **Add selected**, and then click **OK**
    8. Under **Application and Filter Overrides**, click **Create New**
    9. Change the **Action** to **Monitor**
    10. In the search field, type `IEC.60870.5.104` to list all matching signatures
    11. Press Ctrl, and then select the following signatures:
        - `IEC.60870.5.104_Control.Functions`
        - `IEC.60870.5.104_Control.Functions.STARTDT.ACT`
        - `IEC.60870.5.104_Control.Functions.STARTDT.CON`
        - `IEC.60870.5.104_Information.Transfer`
    12. Right-click any of the signatures, and then click **Add selected**, and click **OK**
    13. Click **OK** to save the profile

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

DO NOT REPRINT
© FORTINET



Protect the OT Network (Contd)

- Solution (Contd):
  - Create the following policies to allow traffic:
    - FortiGate-1

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
<SoftwareSwitch>	port1	PLC-2	PLC-3	ALL	Disable

    - FortiGate-2

Source Interface	Destination Interface	Source Address	Destination Address	Service	NAT
port1	<SoftwareSwitch>	PLC-2	PLC-3	ALL	Disable

    - Edge-FortiGate

Source Interface	Destination Interface	Source Address	Destination Address	Service	Application Filter	NAT	Log Allowed Traffic
Floors	Floors	PLC-2	PLC-3	All	<Name_of_ sensor>	Disable	All Sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

You will need to create policies, as shown on this slide, to fulfill the requirement. The address objects are already created on FortiGate devices. You can still use the /32 IP address. Refer to the topology for device IP addresses.

DO NOT REPRINT
© FORTINET



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.