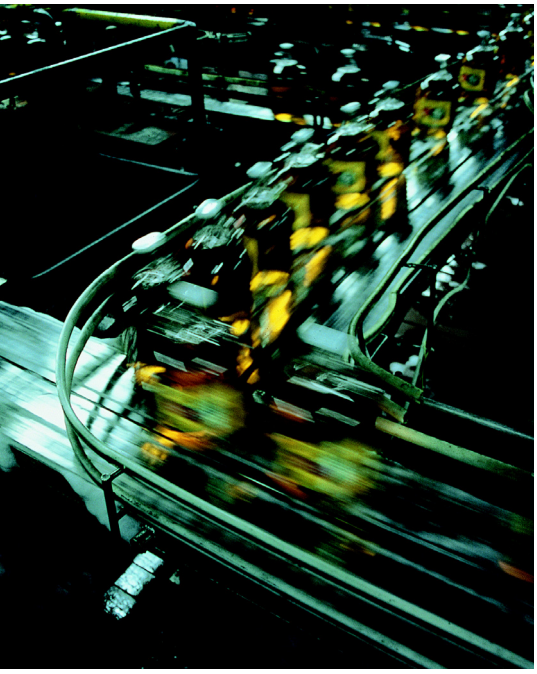


Deploying Network Security within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

December 2018

Document Reference Number: ENET-TD019A-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco® and Rockwell Automation®. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide industrial network infrastructure. CPwE can also help industrial operations achieve cost reduction benefits by using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology.

Industrial IoT (IIoT) offers the promise of business benefits using innovative technologies such as mobility, collaboration, analytics, and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Deploying Network Security within a Converged Plantwide Ethernet Architecture CVD (CPwE Network Security), which is documented in this Design and Implementation Guide (DIG), outlines several network security use cases for plant-wide Industrial Automation and Control System (IACS) network infrastructure. CPwE Network Security was tested and validated by Cisco Systems and Rockwell Automation.

Document Organization

This document is composed of the following chapters and appendices.

Chapter/Appendix	Description
Chapter 1, “CPwE Network Security Overview	Provides an overview of prevailing trends in IACS networking and the convergence of network security technology, specifically IACS operational technology (OT) with information technology (IT) network security solutions.
Chapter 2, “CPwE Network Security Solution Considerations	Covers the CPwE Network Security solutions and their various architectures, components, and their relation to each other.
Chapter 3, “CPwE Network Security Design Considerations	Covers design considerations that must be considered by OT engineers and IT security architects when deploying CPwE network security solutions.

Chapter/Appendix	Description
Chapter 4, “Configuring the Infrastructure	Describes how to configure CPwE Network Security infrastructure components such as Cisco Identity Services Engine (ISE), Cisco Stealthwatch, Cisco and Allen-Bradley® Stratix® industrial Ethernet switches (IES), and Cisco Industrial Network Directory (IND) and Rockwell Automation FactoryTalk® Network Manager (FTNM) network monitoring tool (NMT).
Chapter 5, “Implementation of Use Cases	Provides implementation steps for the specified network security use cases.
Chapter 6, “Troubleshooting the Infrastructure	Provides troubleshooting information.
Appendix A, “References”	List of references for CPwE design and implementation guides for network infrastructure services and security.
Appendix B, “Test Hardware and Software”	Hardware and software components used in CPwE Network Security testing.
Appendix C, “Acronyms and Initialisms”	List of acronyms and initialisms used in this document.
Appendix D, “About the Cisco Validated Design (CVD) Program”	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs).

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- Cisco site:
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Note

This release of the CPwE architecture focuses on EtherNet/IP™, which uses the ODVA, Inc. Common Industrial Protocol (CIP™), and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, and CIP Security™, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

CHAPTER 1

CPwE Network Security Overview

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A converged IACS network technology helps to enable the Industrial Internet of Things (IIoT).

As access methods to plant-wide IACS networks expand, the complexity of managing network access security and controlling unknown risks continues to increase. With a growing demand for in-plant access by trusted industry partners (for example, system integrator, OEM, or IACS vendor), IACS applications within the CPwE architecture (Figure 1-1) face continuous threats such as malware propagation, data exfiltration, network scanning, and so on. Furthermore, industrial operations face additional challenges such as legacy systems, lack of visibility on what type of IACS assets and devices are on the IACS network, and lack of security skills for the OT team.

No single product, technology, or methodology can fully secure plant-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical) utilizing diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture.

Defense-in-depth applies policies and procedures that address many different types of threats. The CPwE Industrial Security Framework (Figure 1-2), using a defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

With all the opportunities and challenges faced by industrial operations, there is a strong need in manufacturing and heavy industry markets for the following requirements:

- **Visibility**—Visibility of the current network devices and IACS assets present in the IACS network is very critical for the OT-IT security team to design and deploy a comprehensive industrial security access policy. Existing IT network monitoring tools are unable to gain full visibility of IACS network devices and IACS assets in a plant-wide network because the IACS assets communicate with IACS protocols. There is a need for a network monitoring tool (NMT) that can gain full visibility of IACS assets present in a plant-wide IACS network and pass this information to a security access policy design and implementation solution.

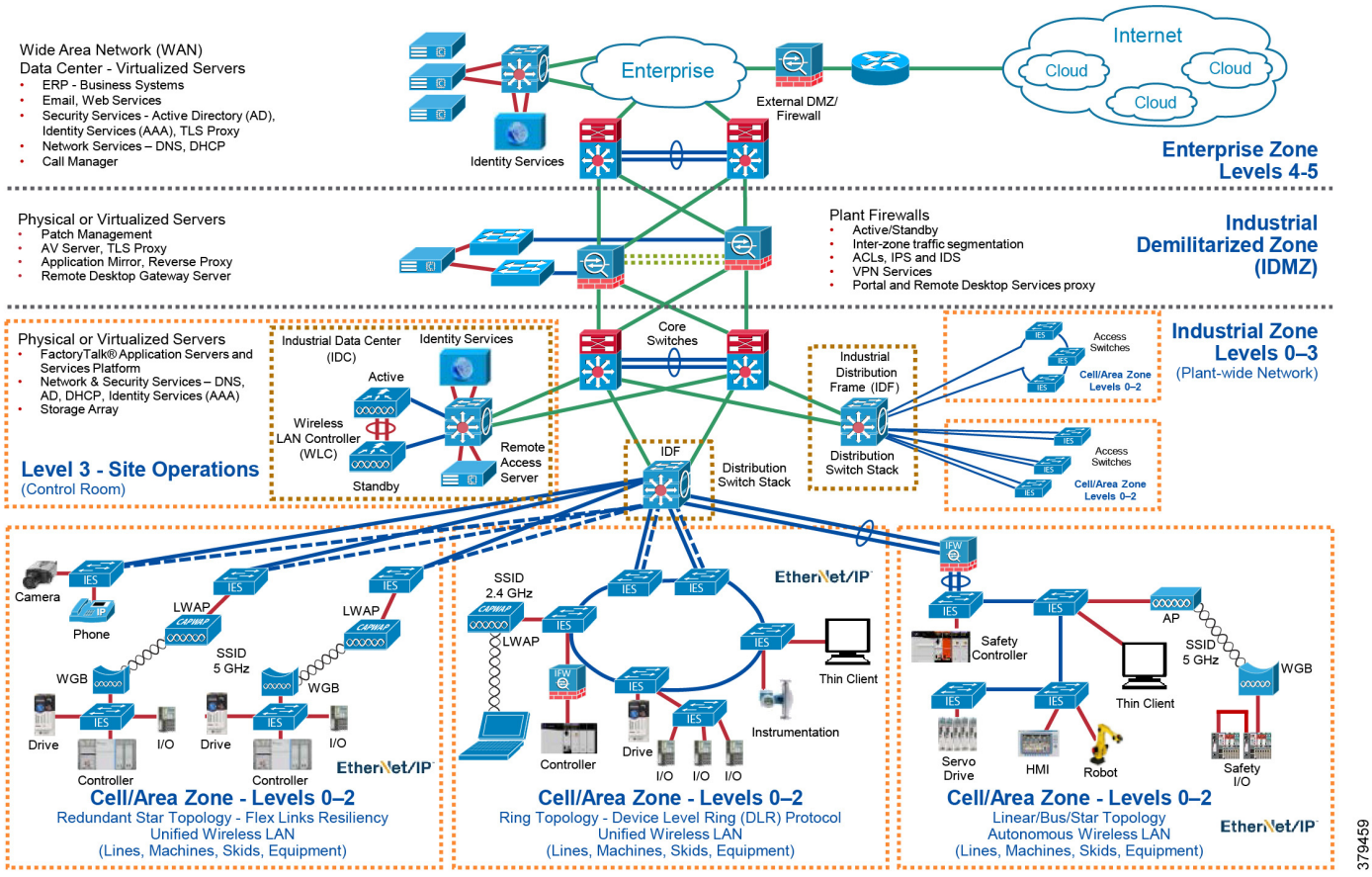
Note Cisco and Rockwell Automation recommend that the OT-IT security team be composed of a multi-discipline team of operations, engineering, safety, maintenance, and IT representatives to develop an industrial security access policy based on your risk tolerance and risk management.

- **Segmentation**—Segmentation (zoning) is an important piece of network architecture required by the OT-IT network design team for improving security and performance by grouping and separating network assets. Cyber criminals study ways to infiltrate the IACS network by looking at the most vulnerable point. Segmentation helps to prevent the spread of the infection and limits it only to those endpoints that an infected host can reach. A common segmentation method adopted by industrial operations is to segment the IACS network Industrial Zone (Figure 1-1) from the Enterprise Zone via an industrial DMZ (IDMZ), then use logical segmentation within that zone (following the IEC 62443-3-2 Zones and Conduits model). OT-IT then collaborates to design the access policy in the Industrial Zone by using access control lists (ACLs). However, the management of ACLs can be tedious and their larger size can affect the performance of network devices. Industrial operations are looking for a better solution to segment access control policies for the IACS network Industrial Zone that is easier to deploy and manage.
- **Anomaly detection and Mitigation**—When little to no access control methods to a plant-wide architecture are enabled, the possibility of IACS assets getting infected increases. When such an event happens, the OT-IT security teams need to identify the infected device, then based on the OT-IT industrial security access policy, decide how to address the threat based on the level of risk. Industrial operations need a method to detect anomalies, have the option to block threats, and identify compromised IACS assets. This detection and remediation method deployed in the plant-wide IACS network by the OT-IT team must be scalable and also should not change the currently deployed architecture.
- **Intent-based security for OT**—In many industrial operations, IT helps to defines industrial security policies, architecture, and design. OT depends on IT to enable and manage those policies. However, given that OT requirements are often fluid, the OT-IT security team needs a process that allows OT to express operational intent that results in dynamic industrial security access policy changes without having to depend on IT. For example, consider the network security use case associated with remote access. The IT team can create the general centralized access policy for remote access that has rules to allow a remote trusted industry partner expert to connect to an IACS asset. When the remote access is no longer needed, the OT team informs IT to revoke the access for the remote expert. Since this process is manual, in some cases there might be delays in providing or revoking the remote access. To overcome these challenges, an automated self-service process is needed where an OT engineer can request the remote access without IT intervention.

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures (Figure 1-1) provide design and implementation guidance, test results, and documented configuration settings that can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications.

CPwE Network Security describes several network security use cases that are solved using diverse security solutions and technologies. CPwE Network Security is brought to market through a strategic alliance between Cisco and Rockwell Automation.

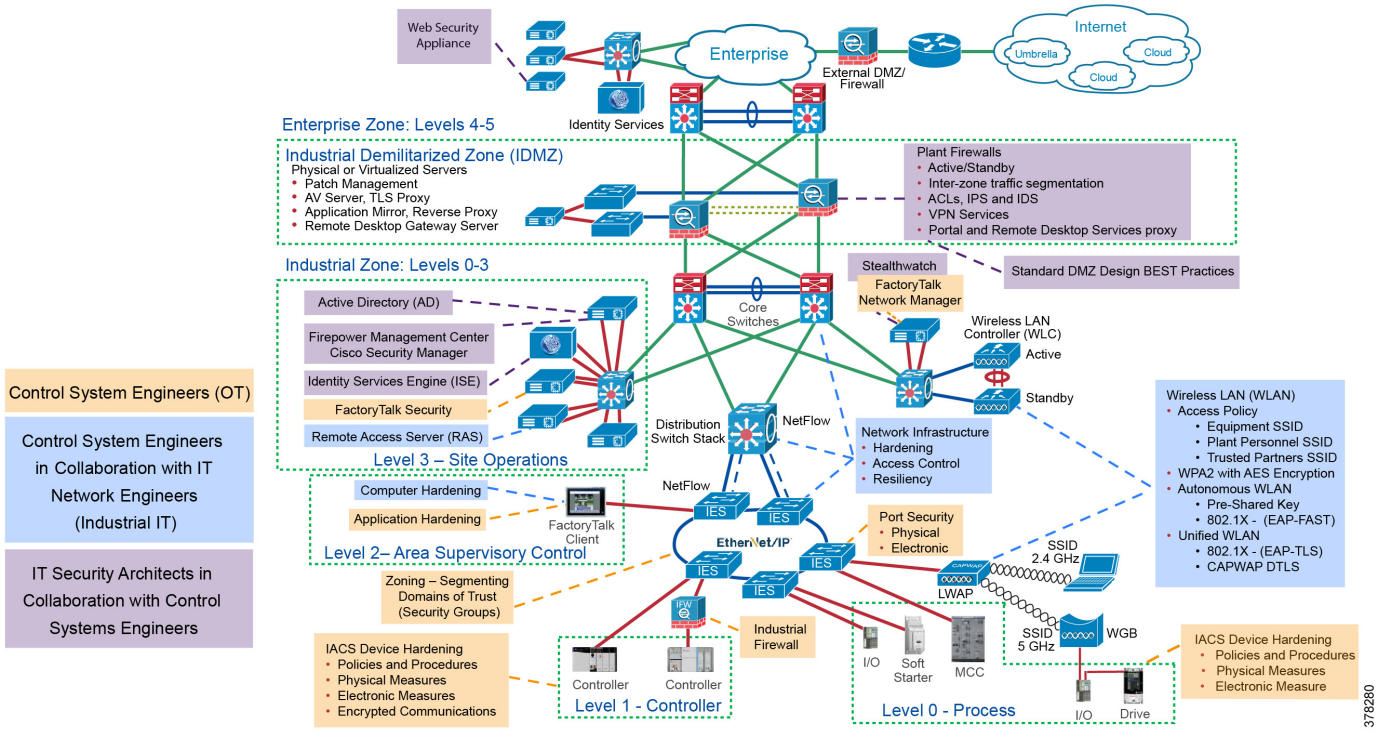
Figure 1-1 CPwE Architecture



There are many personae managing the plant-wide security architecture, with diverse technologies, as shown in Figure 1-2.

- Control System Engineers (highlighted in tan)—IACS asset hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network monitoring and change management, network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, and IACS application authentication, authorization, and accounting (AAA).
- Control System Engineers in collaboration with IT Network (highlighted in blue)—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), network monitoring and inspection, and wired and wireless LAN access policies.
- IT Security Architects in collaboration with Control Systems Engineers (highlighted in purple)—Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant firewalls, and Industrial Demilitarized Zone (IDMZ) design best practices.

Figure 1-2 CPwE Industrial Security Framework



CPwE Security Overview

Protecting IACS assets requires a defense-in-depth security approach where different solutions are needed to address different network and security requirements for a plant-wide architecture. This section summarizes the existing Cisco and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of industrial security.

- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several industrial security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide IACS network infrastructure.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html
- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Application Guide* outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk software from the machine to the enterprise to the cloud within a CPwE architecture.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf

  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html

- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing, deploying, and managing industrial firewalls throughout a plant-wide IACS network. The Industrial Firewall is ideal for IACS applications that need trusted zone segmentation.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

CPwE Network Security Solution Use Cases

There are four network security solution use cases that are addressed by CPwE Network Security:

- Visibility and Identification of network devices and IACS assets in Cell/Area Zone(s).
- Security Group Policy segmentation of IACS assets in Industrial Zone (Level 3 Site Operations and Cell/Area Zone(s)).
- Network flow and threat (e.g., malware) detection of network devices and IACS assets in the Industrial Zone.
- OT managed remote user (employee, partner) access (enterprise, internet) for network devices and IACS assets in the Industrial Zone.

These network security solution use cases apply to both brown field (legacy) and green field (new) deployments and follow the best practice framework of CPwE.

Visibility

IACS asset and network device visibility is a continuous process of discovering and identifying all the different IACS assets in the plant-wide network. From the industrial security perspective, it is imperative to have visibility of the IACS assets and network devices due to the following reasons:

- Gaining the visibility of all the IACS assets would allow an OT-IT security administrative team to logically group these IACS assets based on the function of the asset. Once all the assets are grouped into different sets, then it is easier to create a security group access level policy, which is more efficient than an individual policy.
- Helps to detect malicious activity. Knowing the infected device type helps identify if there is a known vulnerability to remediate similar endpoints in the network.

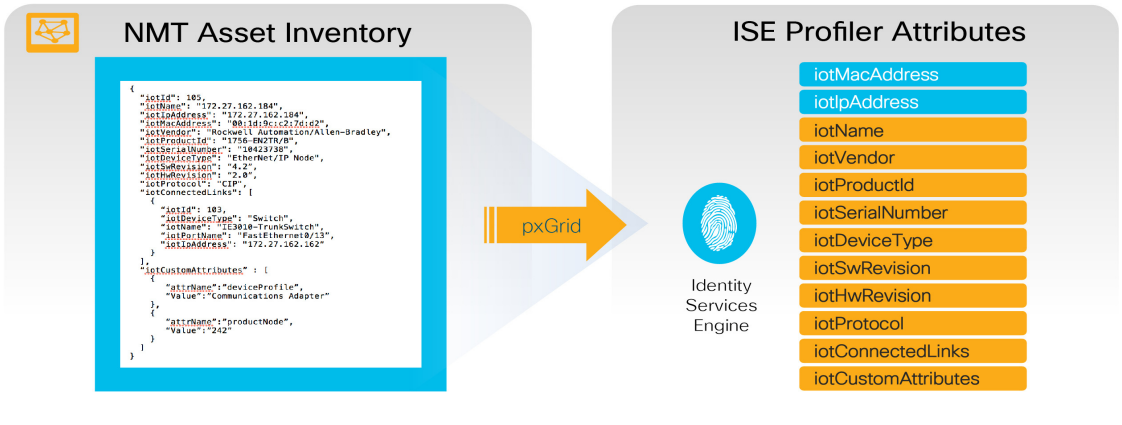
To gain visibility of assets in the enterprise networks, IT has used Cisco Identity Service Engine (ISE) with Cisco ISE Profiling Services (explained below). Cisco ISE is a security administration product that enables an OT-IT security administrative team to create and enforce access level security policies. One of the salient features of Cisco ISE[1] provides profiling services, detecting and classifying endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to pre-built or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Blackberry phones, and so on), desktop operating systems (for example, Windows 7, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.

However, for IACS assets, the ISE built-in probes will not be able to get all the information from the IACS asset to create a granular profiling policy. This is due to the fact that the IACS assets may not support some traditional IT protocols that ISE relies on to profile the device. To gain visibility of IACS assets CPwE Network Security uses Cisco's Industrial Network Director and Rockwell Automation's FactoryTalk Network Manager network monitoring tool (NMT). The NMT product was built to help the OT team gain full visibility of IACS network devices and IACS assets in the context of industrial operations and provides improved system availability and performance, leading to increased overall effectiveness. NMT uses industrial protocols such as the ODVA, Inc. Common Industrial Protocol (CIP) and PROFINET to enable a dynamic, integrated view of the connected IACS assets and network infrastructure. NMT is a lightweight and highly scalable network monitoring tool, which was built mainly for OT industrial operations.

NMT interfaces with Cisco ISE using Cisco pxGrid, which is an open, scalable, and IETF standards-driven data sharing and threat control platform to communicate device information through attributes to ISE. This integration allows exporting of the endpoints discovered by NMT to ISE. NMT also exports several attributes to ISE that would be used to create profiling policies for IACS assets, which is shown in Figure 1-3.

1. https://community.cisco.com/t5/technology-and-support/ct-p/technology-support

Figure 1-3 NMT Exporting Attributes to ISE



The integration between NMT and ISE provides the following benefits:

- Automatically enrolls IACS assets into the ISE endpoint database.
- Enables an OT-IT security administrative team to create granular profiling policies based on the attributes received from NMT.
- Allows the OT engineers to leverage the integration between NMT and ISE to automatically deploy new security policies in the network.

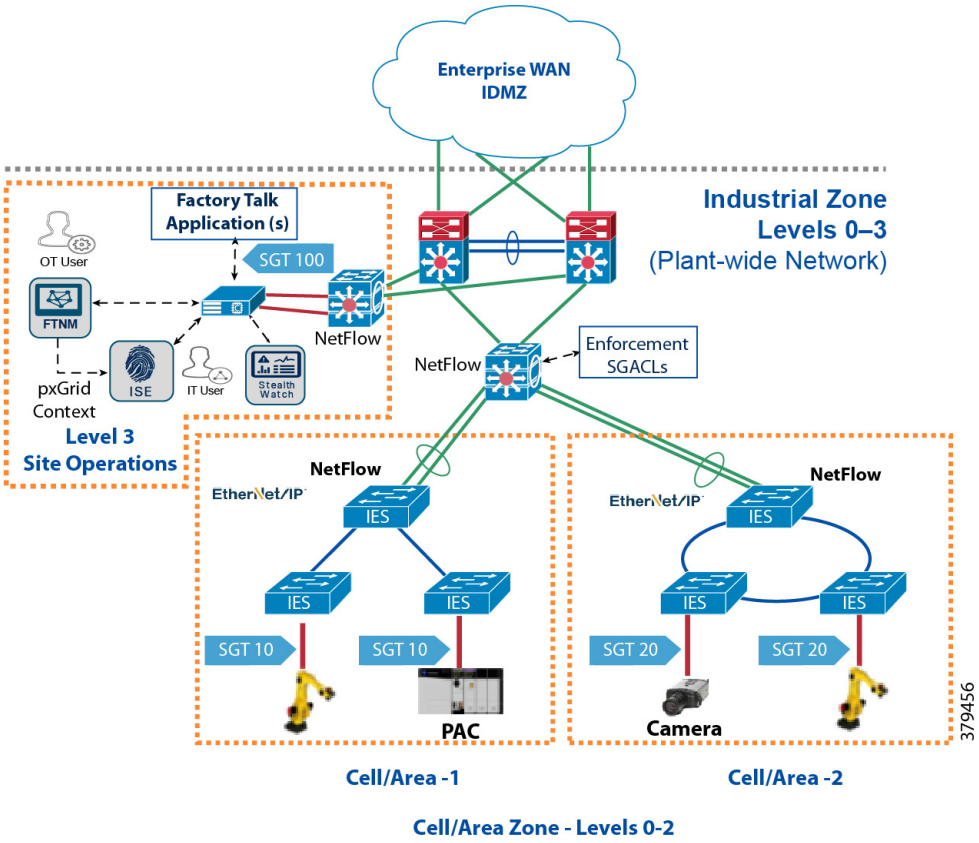
Segmentation

Segmentation is a practice of zoning the IACS network to create smaller domains of trust to help protect the IACS network from the known and unknown risks in the network. As shown in Figure 1-1, CPwE segments the IACS plant-wide architecture into different zones: Cell/Area Zone, Industrial Zone, IDMZ, and Enterprise Zone. OT/IT teams control the communication between the Enterprise and Industrial Zones through the IDMZ. This zoning creates strong boundaries and helps to reduce the risk of unauthorized communications.

The segmentation between Cell/Area Zones was typically done using VLANs with ACLs at the Layer 3 distribution switch. A group of IACS assets that are part of the same functional area (zone) and need to communicate with each other were put in the same VLAN. When IACS assets need to communicate with IACS assets located in a different functional zone, communication occurs via the distribution switch which uses ACLs to either permit or deny traffic. There are many benefits associated with segmentation, such as creating functional areas (building block approach for scalability), creating smaller connected LANs for smaller broadcast/fault domains and smaller domains of trust (security groups), and helping to contain any security incidents. For example, if there is a security group access policy to restrict the communication between the VLANs (zones), traffic from an infected host is contained within the VLAN. However, as the size of the ACL increases, the complexity of managing the ACL also increases.

To provide more flexibility and simplicity to network segmentation, CPwE Network Security uses Cisco TrustSec technology to define access policies using security groups. This allows the segmentation of IACS assets using Security Group Tags (SGT) which group the assets regardless of their location in the plant-wide network. This technology is available on the Allen-Bradley Stratix 5400/5410 and the Cisco IE 4000/5000 industrial Ethernet switch (IES). As shown in Figure 1-4, the IACS assets in Cell/Area Zone 10 are given an SGT of 10, the IACS assets in Cell/Area Zone 20 are given a tag of 20, and the FactoryTalk application(s) located within Level 3 Site Operations is given an SGT of 100.

Figure 1-4 Secure Group Assignment



Once the IACS assets are put in logical groups by the OT-IT security administrative team, the next step is to enforce the Secure Group Access Control List (SGACL) on the distribution switch. Enforcement of security access policy is achieved by defining a policy matrix in ISE; an example of such a policy is shown in Figure 1-5.

Figure 1-5 An Example of Secure Group Access Control List

Source \ Destination	SGT100	SGT10	SGT20
SGT100	✓	✓	✓
SGT10	✓	✓	⊘
SGT20	✓	⊘	✓

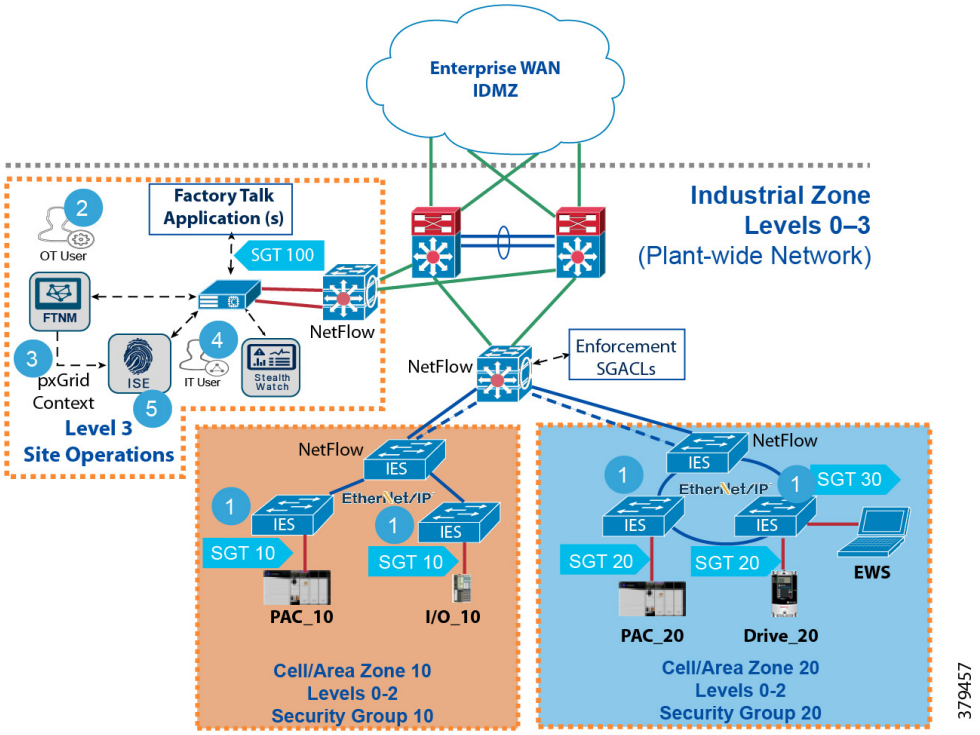
378873

As shown in Figure 1-5, all IACS assets in Cell/Area Zone 10 (SGT 10) are allowed to talk to each other, and all IACS assets in Cell/Area Zone 20 (SGT 20) are allowed to talk to each other. However, IACS assets in Cell/Area Zone 10 are not allowed to talk to IACS assets in Cell/Area Zone 20. The key point to observe is that FactoryTalk application(s) (SGT 100) is allowed to talk to all IACS assets in Cell/Area Zone 10 and Cell/Area Zone 20. This is required because the FactoryTalk application(s) may need to have access to all the IACS assets for managing industrial operations.

After the IACS assets are tagged, and the security access policy matrix is defined in ISE, the last step is to enforce the access policy in the Cell/Area Zone. As IACS assets attach to the network, they are authenticated to ISE using MAC Authentication Bypass (MAB), which is a port-based access control method using the MAC address of the IACS asset. An SGT assignment is also done. For example, as shown in Figure 1-4, when PAC_10 attaches to the IES in the Cell/Area Zone 10, it is assigned an SGT of 10. The distribution switch connecting the Cell/Area Zones needs to download the SGACL that is shown in Figure 1-5. Figure 1-6 shows the ordered sequence:

1. All of the IES are configured with MAB Open Access.
2. The OT user discovers IACS assets with NMT and tags them with custom attributes.
3. NMT sends the asset details to ISE via pxGrid.
4. The IT user pre-defines profiling rules in ISE to match custom attributes and assigns the SGT in Authorization policies. All the IACS assets attached to Cell/Area Zone 10 are assigned a SGT of 10, all the IACS assets attached to Cell/Area Zone 20 are assigned a SGT of 20, and the FactoryTalk application(s) is assigned a SGT of 100.
5. ISE distributes the TrustSec policy to the distribution switch to enforce Zone segmentation

Figure 1-6 Policy Enforcement of All the Traffic Going East-West and North-South between the Zones



Flow-based Anomaly Detection Using Stealthwatch Technology

Network flows are the communications between network devices. Having visibility to those devices allows the OT-IT security administrative team to have a baseline idea of typical traffic patterns within the plant-wide architecture. Complete visibility information has the following benefits:

- Is my security access policy working correctly?
- Are there any unauthorized network connections occurring in the network?
- Are there any abnormal connections established to the outside world?
- Is there any active malware spreading in the network?
- Is this occurring for the first time or it has been occurring for a while?

Cisco Stealthwatch[1] helps industrial operations to address all the questions that are important for doing any incident or regular operation analysis. CPwE Network Security integrates Stealthwatch technology and enables the OT-IT security administrative team to monitor real-time traffic and also detect if there is any network anomaly or if malware is propagating in the network. Cisco Stealthwatch collects the data on the switches themselves using NetFlow technology, which is more scalable than the traditional SPAN (switched port analyzer) method.

The SPAN method involves dedicating a source port for collecting the traffic and a destination port for analyzing the traffic. If the traffic analyzer is not directly attached to the source IES, then there are two alternatives:

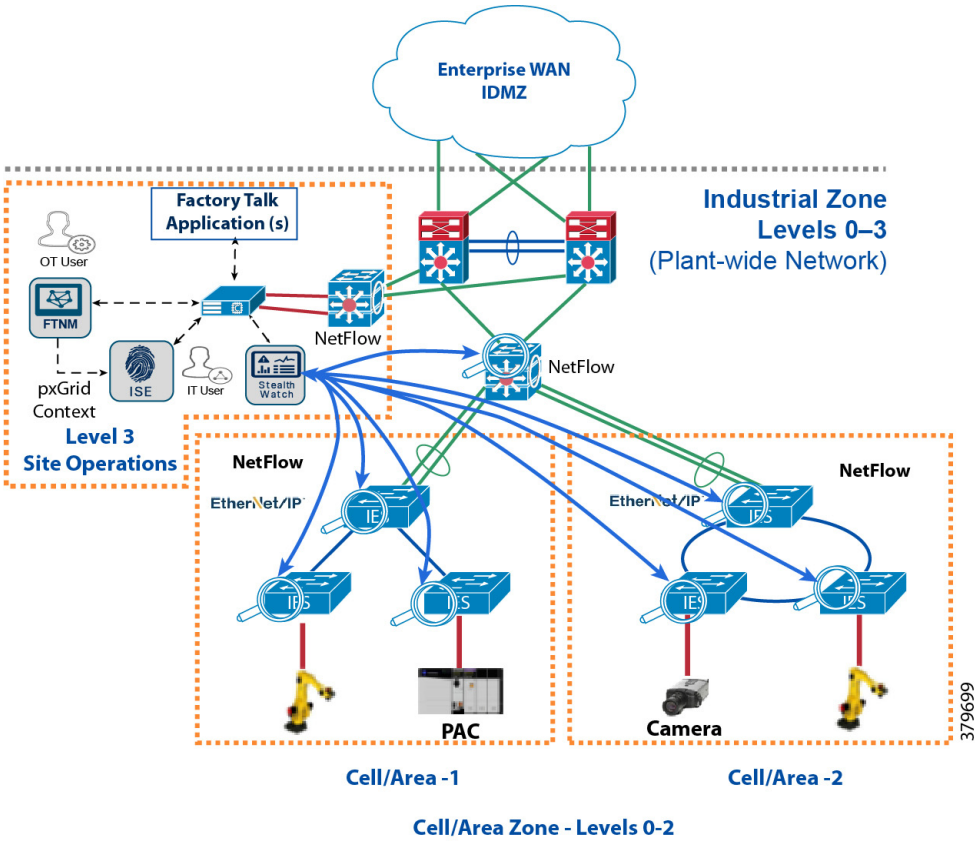
- Add a cable directly from the source IES to the destination switch.
- Configure remote SPAN (RSPAN) on the source IES, implement a dedicated RSPAN VLAN, then configure RSPAN on the destination switch.

Configuring remote SPAN allows the source traffic to be carried across multiple switches, but it increases the complexity of deployment. Second, if the captured traffic exceeds the interface bandwidth, then the traffic may be dropped. Third, if RSPAN is enabled on multiple IES, then the captured traffic coming from all the IES may impact the performance of the distribution/aggregation switch. Fourth, the traffic analyzer needs to be managed to see if it can handle the load coming from all the IES.

Furthermore, with the NMT and Stealthwatch integration, the OT-IT security administrative team may get contextual flow information. For example, if a PAC were communicating with a PAC, then Cisco Stealthwatch will provide visibility of the flow as well as IACS asset information.

1. https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/at-a-glance-c45-736510.pdf

Figure 1-7 Detecting Network Anomalies Using Cisco Stealthwatch

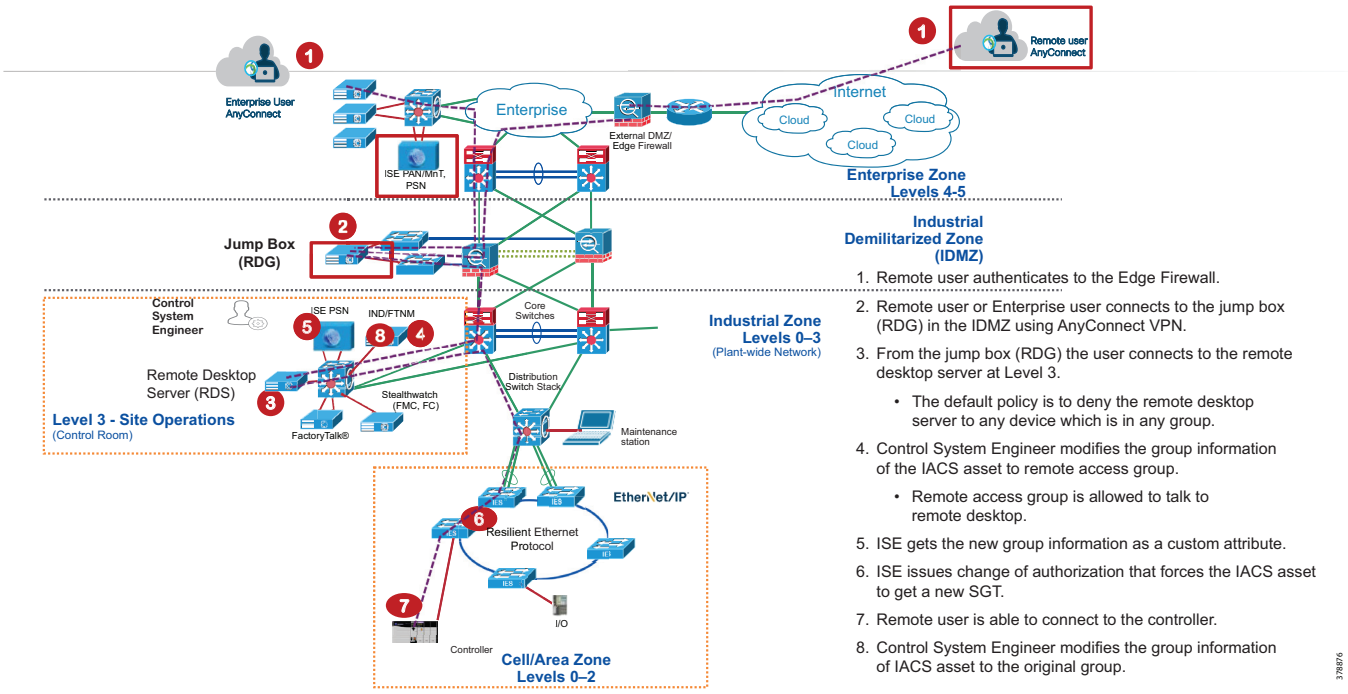


OT Influenced Remote Access—For Example Downtime

Securely Traversing IACS Data Across the IDMZ Design and Implementation Guide (CPwE IDMZ DIG) outlines the current best practices for deploying remote access in an IACS network environment. As described in the CPwE IDMZ DIG, the remote access user must be able to access the remote desktop server in the IDMZ zone and then use the remote desktop server to access the IACS assets in the Industrial Zone. The CPwE Network Security solution enhances this process by enabling OT staff to express intent using NMT and ISE, thereby automating the process of granting remote access as well as removing it.

CPwE Network Security design uses NMT, ISE, and TrustSec technology to meet the remote access requirement. The OT team can create groups in NMT for remote access. When remote access is required, the IACS assets are moved into those security groups and access is granted. When remote access is no longer required, the IACS assets are moved back to their normal security groups. NMT communicates these changes to ISE automatically, which configures network devices like the ASA firewall within the IDMZ.

Figure 1-8 OT Influenced Remote Accessing NMT Solution



CHAPTER 2

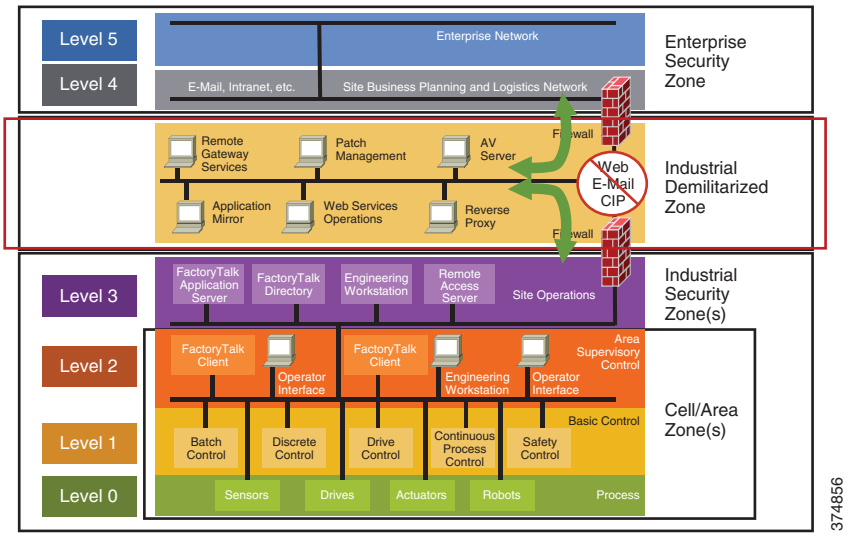
CPwE Network Security Solution Considerations

This chapter covers the CPwE Network Security Solution and its various solutions, components, and their relation to each other. CPwE Network Security Solution is an architecture that provides visibility, profiling, segmentation, network flow detection, malware detection, and OT influenced remote access services to the devices, equipment, and applications found in an Industrial Automation and Control Systems (IACS). The CPwE Network Security Solution architecture overview provides the background and description of an IACS network model.

CPwE Reference Architecture

The CPwE logical model employs commonly used industry standards such as Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) to organize the plant functions into Levels and IEC-62443 (formerly ISA99) to organize the Levels into functional and security Zones, as shown in Figure 2-1.

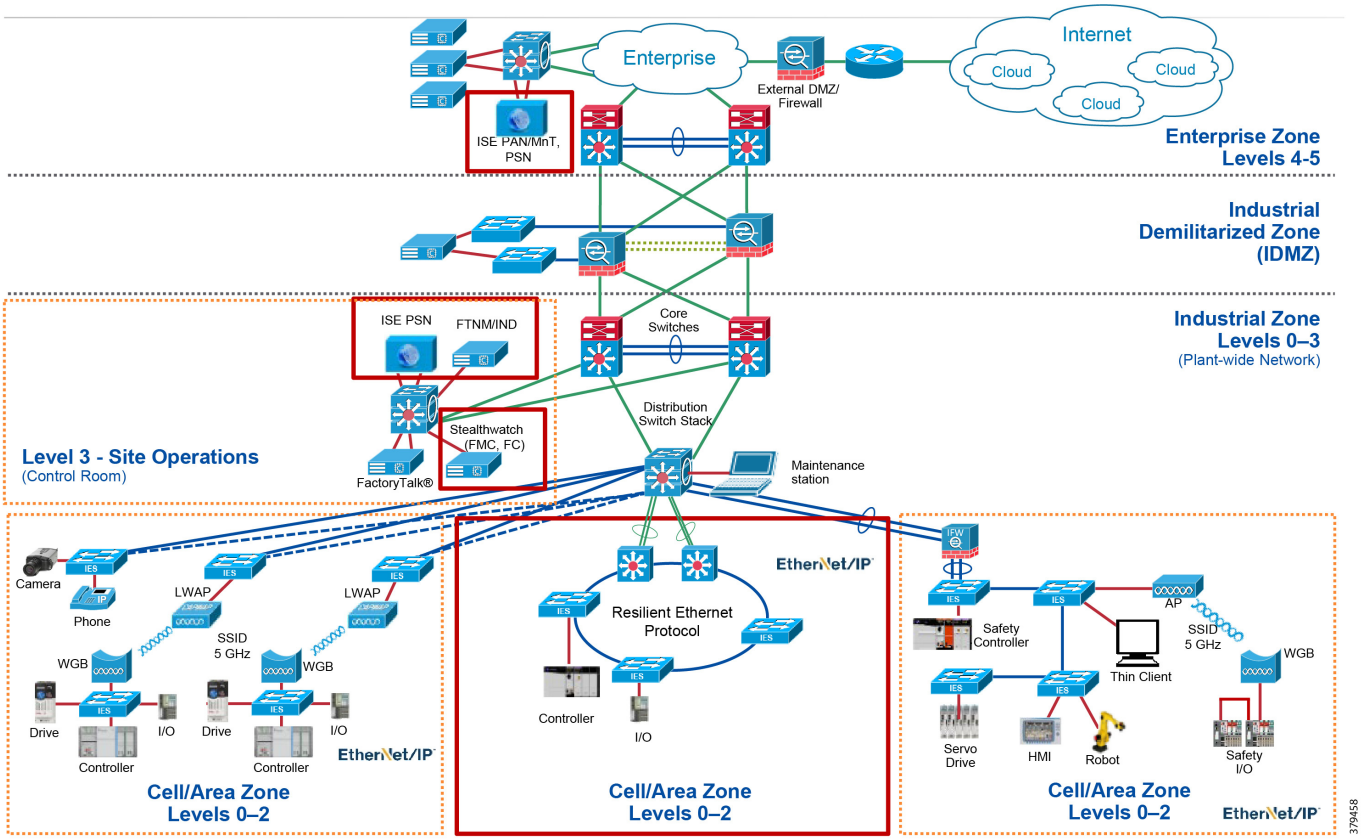
Figure 2-1 CPwE Logical Zoning Based on Purdue Model and IEC-62443



Cell/Area Zone

The Cell/Area Zone is a functional zone where the IACS assets interact with each other. The industrial network is a critical factor for the Cell/Area Zone because all the IACS assets must communicate to ensure that requirements for industrial operations are met. A plant-wide architecture may have one or multiple Cell/Area Zones. Each Cell/Area Zone can have the same or different network topologies. There could be different network topologies present throughout the entire plant-wide architecture. For the purpose of this CPwE Network Security CVD DIG, a ring topology was chosen for design, testing and validation because the ring topology design provides resiliency. Figure 2-2 depicts what Cisco and Rockwell Automation have validated as part of CPwE Network Security CVD.

Figure 2-2 CPwE Network Security Scope



Industrial Zone

The Industrial Zone comprises the Cell/Area Zone(s) (Levels 0 to 2) and Site Operations (Level 3) activities. The Industrial Zone is important because all the IACS applications, assets, and controllers critical to monitoring and controlling the plant-wide architecture industrial operations are in this zone. To preserve smooth industrial operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the enterprise operations.

System Components

Table 2-1 lists all the Cisco and Rockwell Automation components that are involved in this design.

Table 2-1 Cisco and Rockwell Automation Components

Role	Model	Software Release	Comments
Layer 2 Industrial Ethernet Switch	Cisco IE 4000/5000 Allen-Bradley Stratix 5400/5410	15.2(6)E2	Provides connectivity to IACS assets at Levels 0-2
Distribution Switch	Cisco Catalyst 3850	16.3.5B	Distribution/Aggregation switch connecting the Cell/Area Zones
Cisco Identity Service Engine		2.4	Policy Access Control
Industry Network Director/Factory Talk Network Manager		1.5	Network Monitoring Tool (NMT)
Stealthwatch Flow Collector		6.10.2	Flow anomaly detection
Stealthwatch Management Console		6.10.2	Dashboard
Core Switch	Cisco Catalyst 6880	15.2(1)SY1a	Provides core functionality to the design.

Cisco Industrial Ethernet 4000 and Allen-Bradley Stratix 5400 Series IES

These platforms have been selected for the CPwE Network Security Solution for the following reasons:

- Support for in-line tagging.
- Full NetFlow support.
- Bandwidth and capacity to grow with your networking requirements, including 20 Gbps nonblocking switching capacity with up to 20 Gigabit Ethernet ports per switch.
- Cisco IOS software features for smooth IT integration and policy consistency.
- Robust resiliency enabled by 4x Gigabit Ethernet uplink ports, Resilient Ethernet Protocol (REP) for ring topology, EtherChannel and Flex Links for redundant start topology, and redundant power input.
- True zero-touch replacement for middle-of-the-night or middle-of-nowhere situations.
- Simplified software upgrade path with universal images.
- Industrial environmental compliance and certifications.
- Industrial protocol support: e.g., EtherNet/IP and PROFINET.

Cisco Identity Service Engine

Cisco Identity Service Engine (ISE) brings awareness to all the devices that are accessing the network. It allows an OT-IT security team to design and implement a consistent security access policy in the IACS network. The users and device details are presented in a simple, flexible interface. ISE shares user, device, and network details through the Cisco Platform Exchange Grid (pxGrid) with NMT to enhance the security access policy. Cisco ISE can reduce risks and contain threats by dynamically controlling network access. More details about Cisco ISE can be found in the Cisco ISE Overview (https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~stickynav=1).

Cisco Industry Network Director and Rockwell Automation FactoryTalk Network Manager

A purpose-built platform for managing IACS networks, the Cisco Industrial Network Director and FactoryTalk Network Manager network monitoring tool (NMT) is designed to help operations teams gain full visibility of network devices and IACS assets in the context of industrial operations and provides improved architecture availability and performance, leading to increased overall equipment effectiveness (OEE).

NMT can also discover IACS assets such as PAC, I/O, RTU devices, etc. by communicating in their native communication protocol. NMT supports discovery of IACS assets that utilize the following industrial protocols:

- Common Industrial Protocol (CIP) for EtherNet/IP
- Profinet
- BACnet™
- Modbus®
- OPC-UA

NMT collects a set of attributes from IACS assets to provide visibility into IACS assets, as shown in Figure 1-3. NMT is able to show IACS asset information such as Vendor, Communication, Protocol, Product Name, Serial Number, and Device types.

Cisco Stealthwatch

Cisco Stealthwatch turns the network into a sensor (Network as a Sensor [NaaS]) and provides deeper visibility in your network by leveraging NetFlow and sFlow on switches, routers, and IPFIX on firewalls. With pxGrid integration to ISE Stealthwatch can help to quarantine security incidents, depending on the industrial security policy, and thereby protect potentially vulnerable IACS assets.

Cisco Stealthwatch provides real-time metadata into what each device is doing on the network, all of its network connections, interface utilization, and overall network performance. Also shown is various levels of machine-to-machine communication; if any IACS asset is infected, then Cisco Stealthwatch can detect IoT peer-to-peer malware. Malicious P2P traffic is hard to detect and block using traditional approaches that rely on lists of known IP addresses and hosts associated with command-and-control servers. Defense-in-depth security is required, but the capability to analyze and understand the information shown by combining different information points and vectors provides unequaled visibility for making operational decisions.

For example, Distributed Denial of Service (DDoS) attacks attempt to exhaust device resources, including network bandwidth, computing power, and operating system data structures. To launch a DDoS attack, malicious users first build a network of devices that will be used to produce the volume of traffic needed to deny services to users.

To create this attack network, attackers discover vulnerable devices on the network. Vulnerable devices are usually those that are not running antivirus software, running out-of-date software, or those that have not been properly patched. Vulnerable devices are then exploited by attackers to gain access to these devices. The next step for the attacker is to install attack tools on the compromised devices of the attack network. The devices that are running these attack tools are known as zombies and they can carry out any attack under the control of the attacker. Many zombies together form what is referred to as a botnet army. WAN saturation, an increase in host counts, and an increase in UDP packets are all common for a compromised organization.

An alternative approach to detect network attacks is to capture all traffic using RSPAN and observe the behavior of the packets to detect if there is any malicious attack occurring in the network. To capture all traffic, every switch needs to be configured with a port for redirecting the traffic to a central location, which often increases the cost of deployment. Moreover, if an attack is occurring in the network, then the IT security architect needs to use multiple programs to parse several captured files to detect the attack. With Cisco Stealthwatch, there is no need to invest in additional ports for capturing the traffic. Instead, the router or switch as a sensor captures the key pieces of the flow such as source IP address, destination IP address, source port, destination port, and other important fields that are part of a flow by using NetFlow which is built into the IES. Observing flows in a network can be used to quickly pinpoint where an attack is occurring in the network. In addition, to investigate how long a malicious behavior is occurring in the network, Cisco Stealthwatch can provide historical data for the flows that are interesting to obtain a detailed view on how long a particular attack has been occurring in a network.

Cisco Stealthwatch can detect and remediate a threat with over 94 different analytic algorithms on the contextual and flow information it receives which are used for anomaly detection. Events feed into high level alarm categories, which can generate an alarm. Some security events can alarm on their own. An alarm can have an associated response such as notify in the alarm table or generate a syslog message to a Security Information and Event Management (SIEM). Cisco Stealthwatch was deployed using the Network as a Sensor Cisco Validated Design guide and pxGrid was configured to communicate with ISE using self-signed based certificates.

- *Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide:*
  https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf
- *Stealthwatch® Management Console VE and Flow Collector VE Installation and Configuration Guide (for Stealthwatch System v6.9.0):*
  https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/virtual/installation/guide/SW_6_9_0_SMC_VE_and_Flow_Collector_VE_Installation_and_Configuration_DV_1_4.pdf

Cisco Catalyst 6880-X Product Details

The Cisco Catalyst 6880-X provides flexibility to build desired port density through two versions of base chassis (C6880-X-LE with standard FIB/ACL/NetFlow tables and C6880-X with larger FIB/ACL/NetFlow tables) along with optional port cards. The base chassis comes with 16 10G/1G ports and each port card supports 16 additional 10G/1G ports. Each system can be built up to 80 ports in 16-port increments. The port interface on the base module and the port cards support both 10 Gigabit Ethernet and 1 Gigabit Ethernet speeds, allowing customers to use their investment in 1 Gigabit Ethernet SFP and upgrade to 10 Gigabit Ethernet SFP+ when business demands change without having to do a comprehensive upgrade of the existing deployment. The port cards are hot swappable. For further information, visit the following page http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/data_sheet_c78-728228.html

Note CPwE Network Security CVD was tested and validated with the Catalyst 6880. Taking into account TrustSec technology, a Catalyst 9500 could be used.

Cisco Catalyst 3850 Switch

The Cisco Catalyst 3850 Series multigigabit and 10-Gbps network switches provide both wired and wireless to support the scalability of a large network. These switches support stacking and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at: https://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html#~stickynav=1

Note CPwE Network Security CVD was tested and validated with the Catalyst 3850. Taking into account TrustSec technology, a Catalyst 9300 could be used.

CHAPTER 3

CPwE Network Security Design Considerations

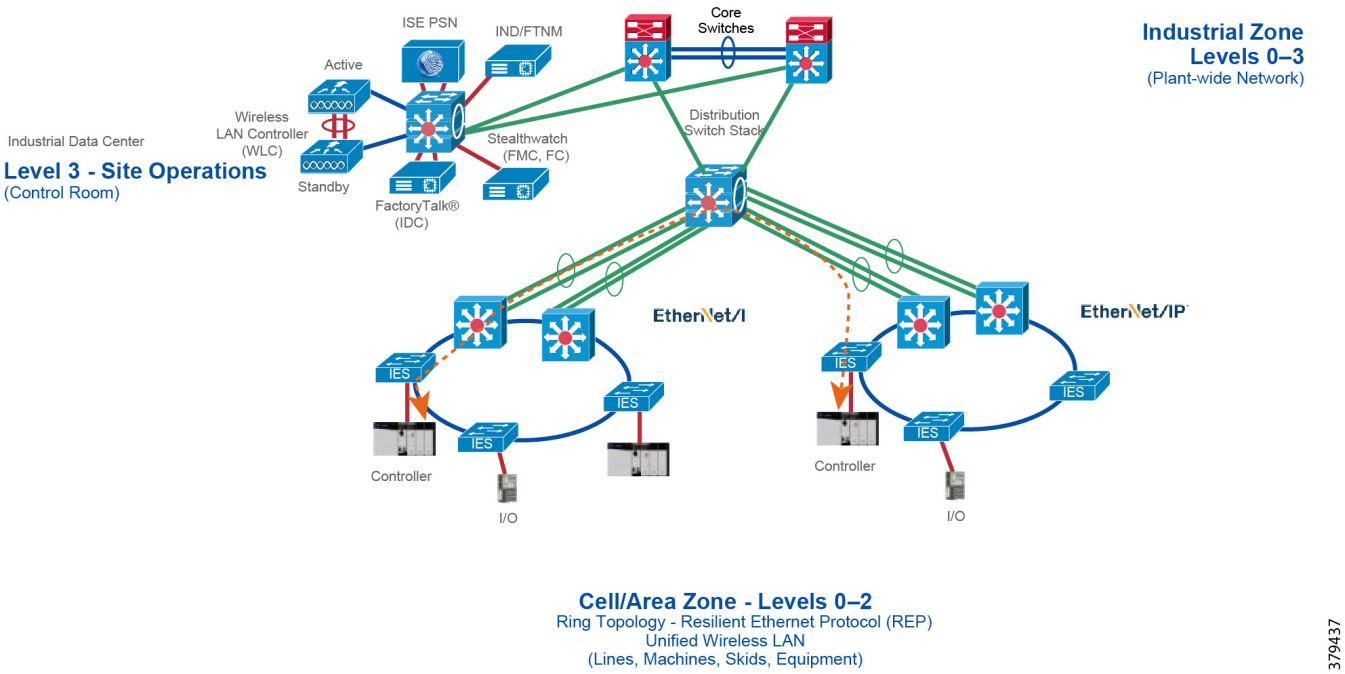
This chapter covers design considerations that must be considered by OT control system engineers and IT security architects when deploying CPwE Network Security solutions. These design considerations provide the rationale for choosing a particular option and are the basis for the deployment options described in Chapter 4, "Configuring the Infrastructure."

- Traffic Flows in a Network
- Segmentation—High Level
- Segmentation Using Downloadable Access Control Lists (dACLs)
- Segmentation Using Layer 3 Access Control List
- Segmentation—TrustSec
- Enforcement Point
- Scalable Group Tag Exchange Protocol Considerations
- NetFlow Data Collection
- Stealthwatch Deployment Considerations
- Cisco ISE Deployment Considerations
- IPDT Considerations

Traffic Flows in a Network

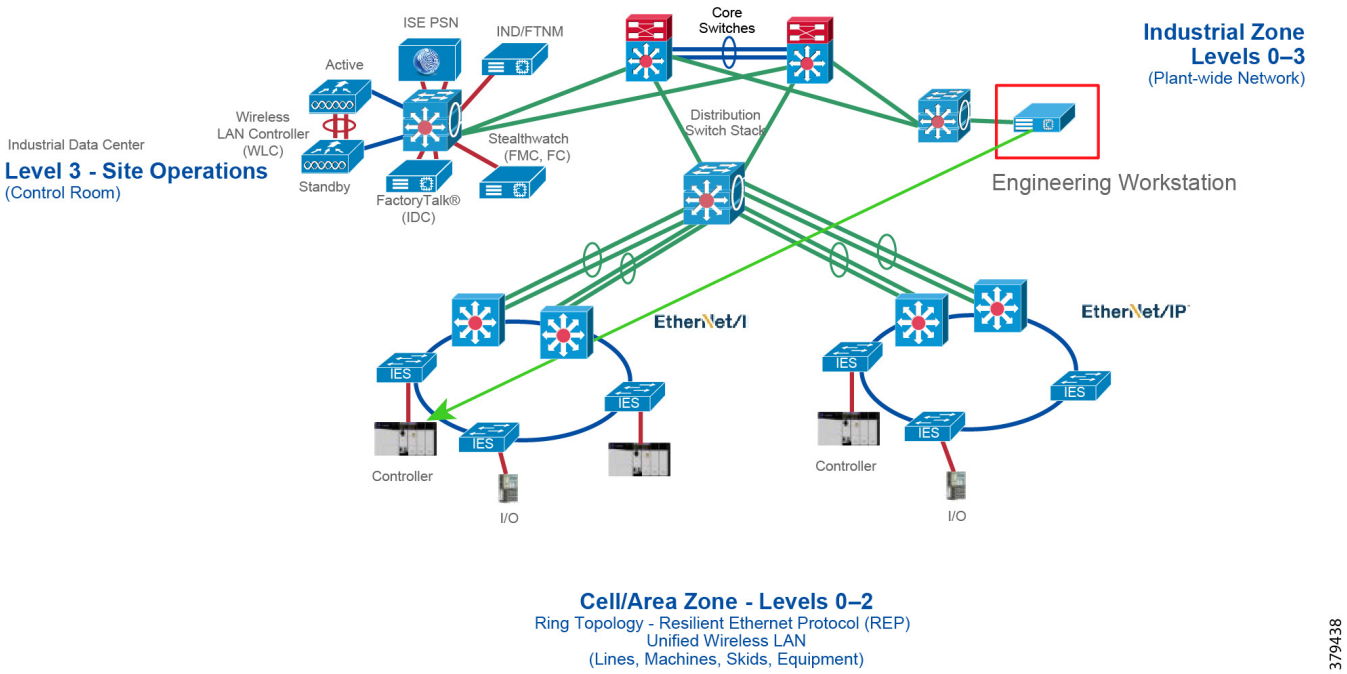
Horizontal communication among peer-to-peer IACS devices in a network is called East-West communication. Figure 3-1 depicts East-West communication in a plant-wide architecture.

Figure 3-1 East-West Traffic Flow in Cell/Area Zone



Allowing a server or any other device in Level-3 Site Operation, IDMZ, or Enterprise Zone to communicate with an IACS asset in the Cell/Area Zone is called North-South communication. In Figure 3-2, the Engineering Workstation (EWS) is accessing a controller in the Cell/Area Zone and this communication flow is defined as North-South communication.

Figure 3-2 North-South Communication in a Plant-wide Network



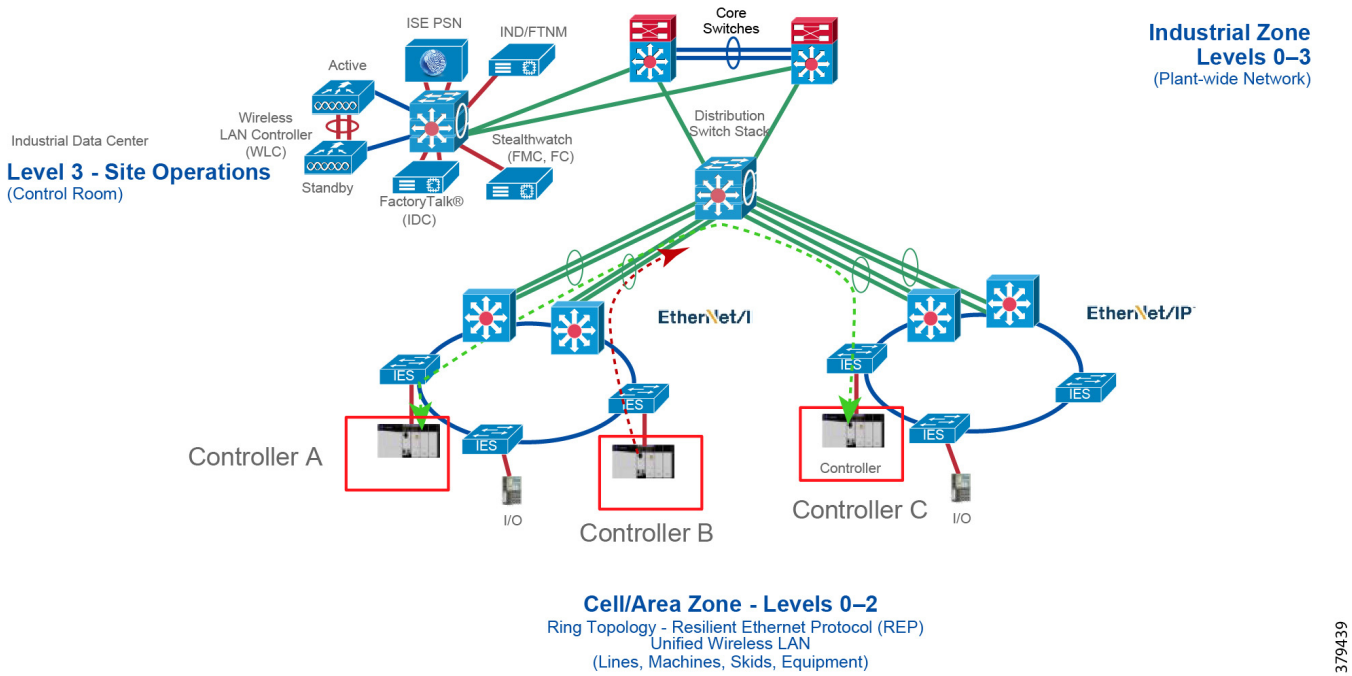
Segmentation—High Level

IT security architects in conjunction with a control system engineer should design an access policy that specifies the East-West and North-South communication flows that must be allowed in an IACS network. In an IACS network, having an open policy that allows every IACS asset to communicate with every IACS asset is convenient, but that approach increases the risk of cyber threat propagation. On the other hand, implementing a restrictive policy that does not allow any inter Cell/Area Zone communication is also counter-productive because certain IACS assets need to access other IACS assets that exist in different Cell/Area Zones. Since the exact requirements of a particular scenario are based on the current IACS application requirements, specifying a policy that would work for all the deployments is not possible. Hence in this CPwE Network Security CVD an access policy example is shown that can be customized for use in different environments.

Assumptions about the access policy for an IACS network:

- All the traffic within the Cell/Area Zone is implicitly permitted because it is assumed that a Cell/Area Zone is formed because a group of IACS assets need to communicate with each other, so no enforcement is applied to any IES in the Cell/Area Zone.
- All the traffic between any two different Cell/Area Zones will be enforced. As an example, in Figure 3-3 Controller_A in one Cell/Area Zone is allowed to access Controller_C in another Cell/Area Zone, but Controller_B is not allowed to access Controller_C.

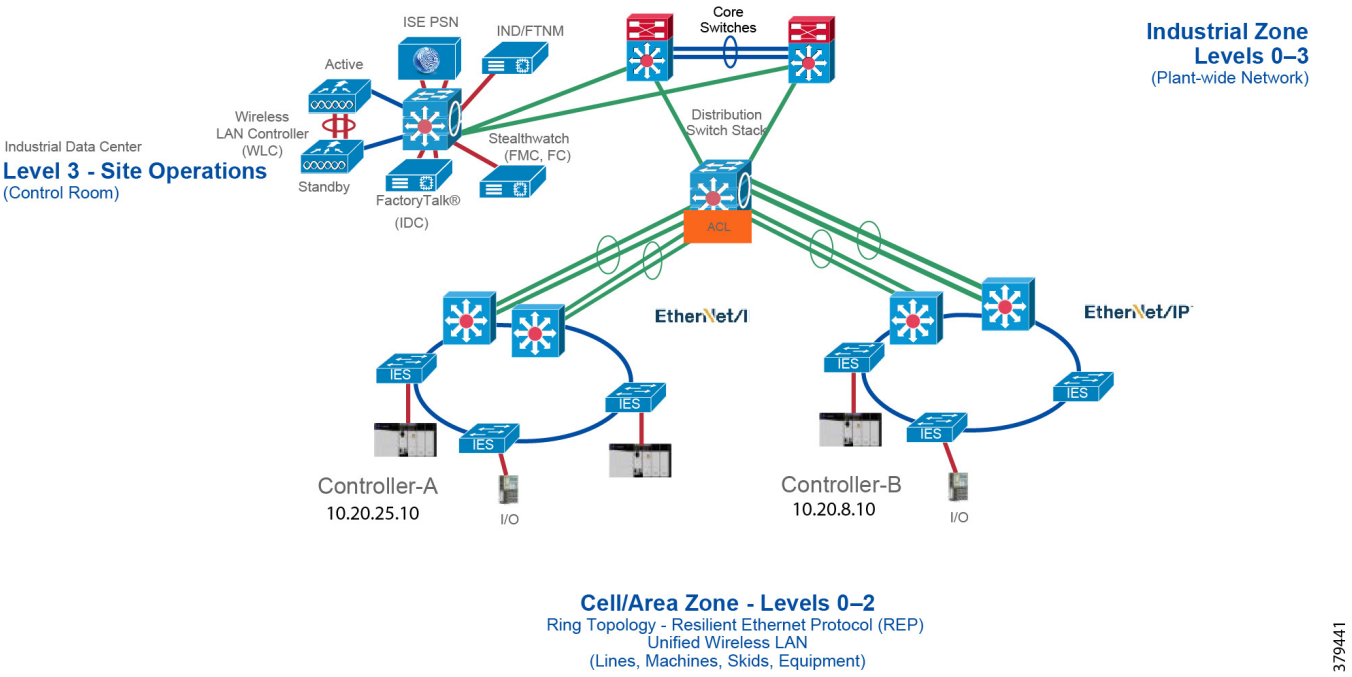
Figure 3-3 Example of Enforcement in East-West Traffic Flow



Segmentation Using Layer 3 Access Control List

When an IACS asset is not configured with MAC authentication bypass (MAB) and is unable to get a downloadable access control list (dACL) from ISE, use a static ACL on the distribution switch which is connecting different Cell/Area Zones. In Figure 3-4, ACL is applied on the distribution switch connecting the two Cell/Area Zones. In Figure 3-4, the ACL must allow communication between 10.20.25.10 and 10.20.8.10 so that Controller-A is able to establish communication with Controller-B.

Figure 3-4 Segmentation Using Layer 3 ACL

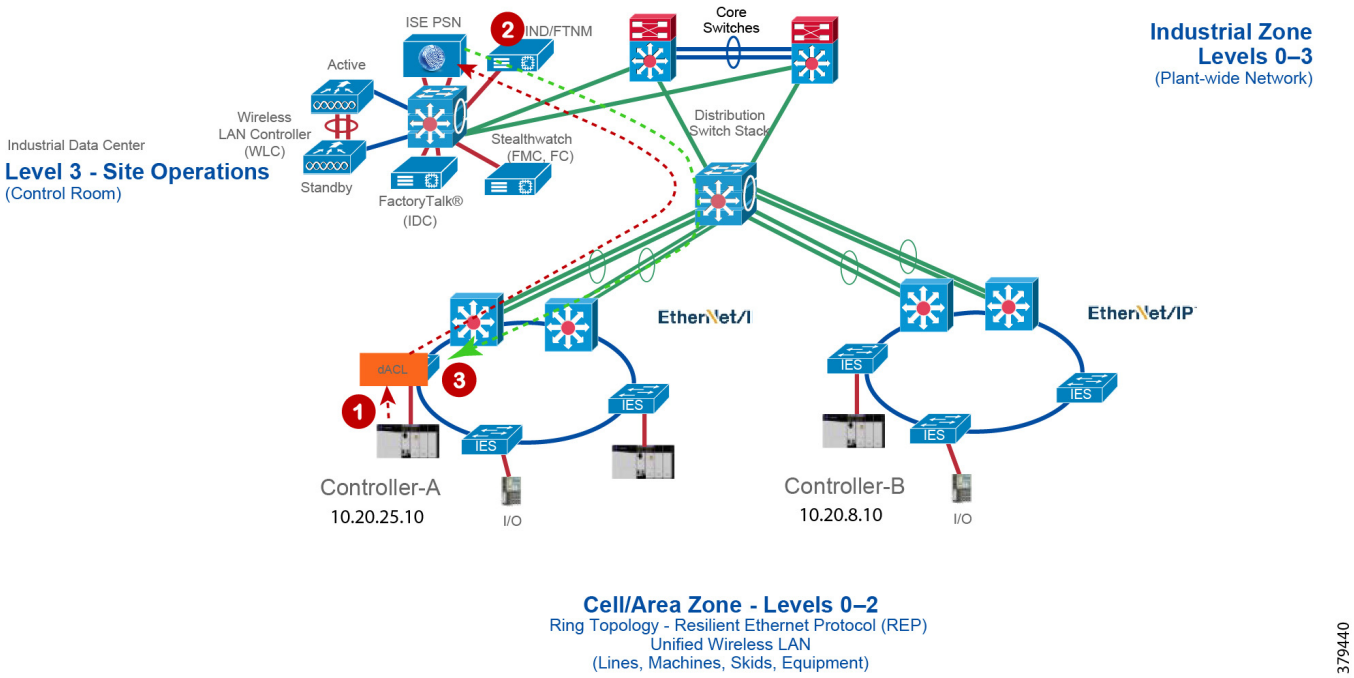


The above method has similar disadvantages in managing the ACL as the dACL. Whenever the controller IP address changes or is moved to a different location, then the ACL needs to be updated. The old entries need to be purged and the new entries added. This process can be burdensome and may lead to an IT security architect making mistakes.

Segmentation Using Downloadable Access Control Lists (dACLs)

As explained in Chapter 1, "CPwE Network Security Overview", Segmentation, segmentation is the practice of zoning the IACS network to create smaller domains of trust to help protect the IACS network from known and unknown risks in the network. This section describes the first approach to segmentation by using Downloadable Access Control Lists (dACLs). See Figure 3-5, which describes how a dACL is provisioned on a device when an IACS asset gets attached to the network. In Figure 3-5, there are two Cell/Area Zones connected via a distribution switch. There are two controllers: Controller-A (10.20.25.10) in Cell/Area Zone -1 and Controller-B (10.20.8.10) in Cell/Area Zone -2.

Figure 3-5 Segmentation Using dACL



1. The Controller connects to an access port on the IES which in-turn sends an 802.1X MAB authentication request to the Cisco ISE.
2. The Cisco ISE, upon receiving the request, processes the request using the configured authentication and authorization policy and sends the authorization result as a dACL to the distribution layer switch.
3. The dACL installed on the IES to which Controller-A is attached, determines the destination IP addresses with which this Controller can communicate. If a control needs to be imposed, then add an entry in the dACL.

The dACL must have Access Control Entries (ACEs) specifying which IP address is allowed to communicate with which IP address. In Figure 3-5, if CONTROLLER-A with IP address of 10.20.25.10 is permitted to communicate with CONTROLLER-B with IP address of 10.20.8.10, then the ACE must have a permit statement with 10.20.25.10 to 10.20.8.10.

The above method works in controlling access to a Cell/Area Zone and also between the Cell/Area Zones. However, this method has the following disadvantages:

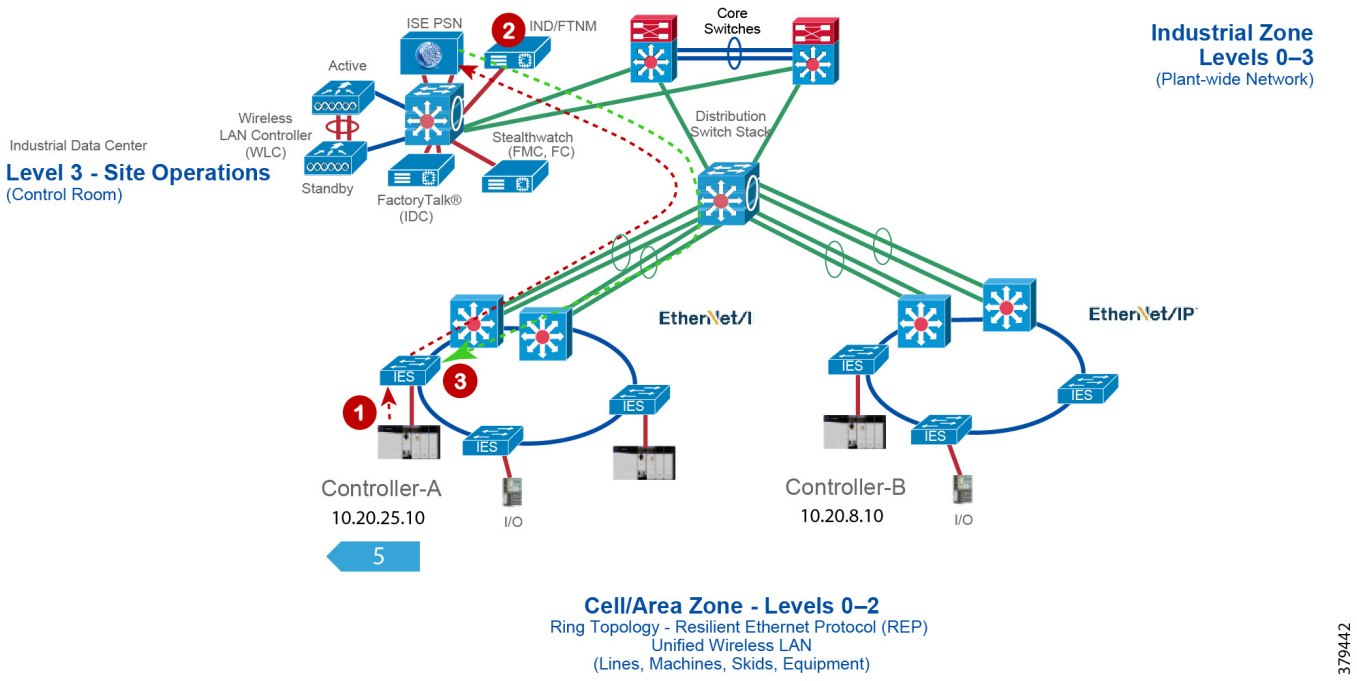
- Assume communication is allowed between CONTROLLER_A and CONTROLLER_B. If CONTROLLER_B moved to a new location with a different IP address, then the dACL needs to be updated.
- If a CONTROLLER_A is allowed to communicate with a particular server in the Industrial Zone and if the IP address of the server changes, then the dACL needs to be updated again.
- If there is a large dACL, then it could impact the performance of the distribution switch.

Segmentation—TrustSec

Cisco TrustSec technology assigns SGTs to IACS assets, networking devices, and users when they attach to a network. By using these tags, an IT security architect can define an access policy and enforce that policy on any networking device. Cisco TrustSec is defined in three phases: classification, propagation, and enforcement. When the users and IACS assets connect to a network, the network assigns them a specific SGT in a process called classification. Classification can be based on the results of the authentication and authorization policies and SGT is an end result of that process. For example, an IACS asset can be classified and assigned a specific tag if the IACS asset is a controller, I/O, HMI, or Windows workstation. Depending on the IACS asset type, a separate tag can be assigned to the IACS asset. Figure 3-6 shows how a controller is assigned an SGT value of 5. The process of SGT assignment is similar to how a dACL is pushed to the Cisco distribution switch when an IACS asset is attached to the IES. The only difference is that instead of a dACL, an SGT value is assigned. As shown in Figure 3-6, when Controller-A attaches to the IES, the IES goes through the 802.1X authentication and authorization with ISE and the result is a tag assignment to the IACS asset.

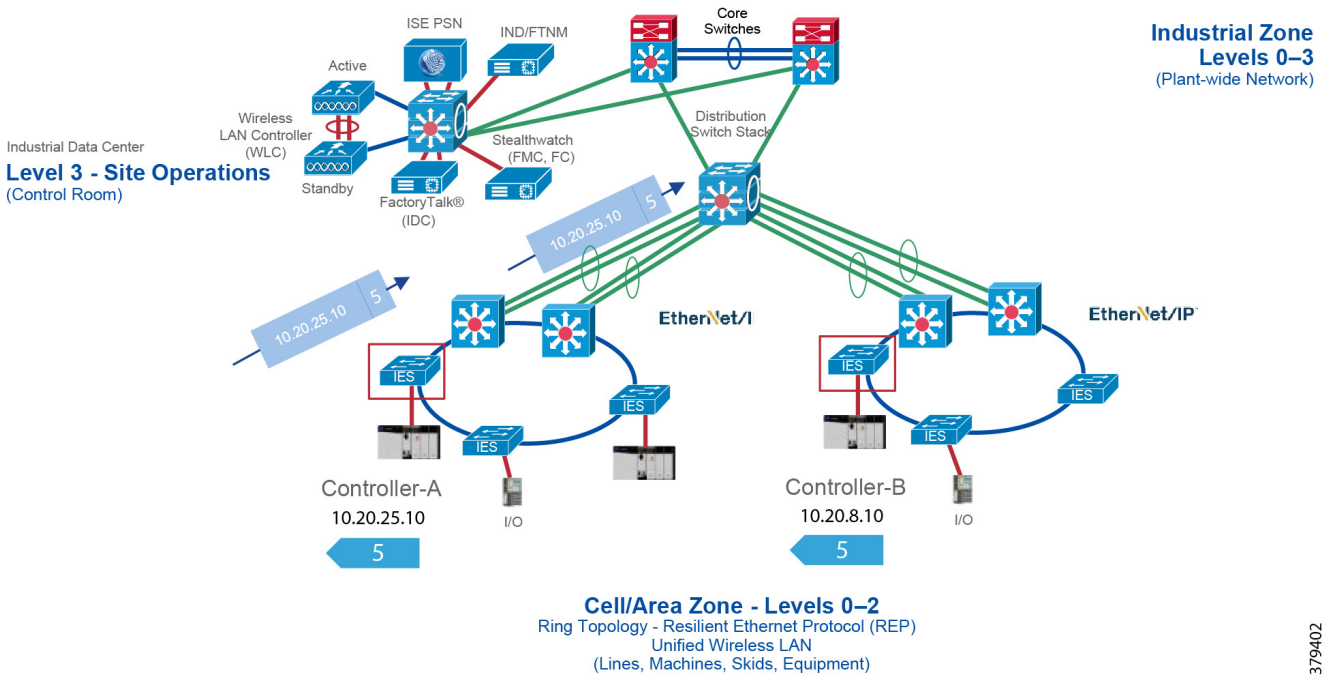
Apart from using Cisco TrustSec, customers can also use the methods described in the previous sections to segment the network, such as static ACLs and dACLs. However, the above two methods are difficult to manage, which can introduce errors during the deployment. Static ACLs need to be constantly managed, for example removing older entries and adding newer entries. Also, if the static ACL size becomes very large, then this can cause performance impact to the distribution switch. The second method using dACLs works well when the policy enforcement is done in the north-south communication flow—restricting communication from the Cell/Area Zone to any Zone above it. To restrict communication for the inter-Cell/Area Zone, dACL has the same limitation as static ACLs, namely the need to update the IP addresses whenever an IACS asset IP address changes.

Figure 3-6 Cisco TrustSec Device Classification



The next phase of TrustSec is propagation in which the SGT tag is made of the Ethernet frame and sent from one switch or router to another device. The SGT tag that is assigned to the IACS asset must propagate along with every packet generated by the IACS asset. Figure 3-7 shows how an SGT inserted frame is propagated in the network. In Figure 3-7, the Controller-A has IP address of 10.20.25.10 and is assigned an SGT value of 5. When an Ethernet frame is generated by Controller-A, the IES inserts the SGT value of 5 along with the IP address and sends it to the next switch. The incoming switch, if configured with SGT in-line tagging, propagates the same frame to the next switch and this information travels in hop-by-hop fashion to the destination.

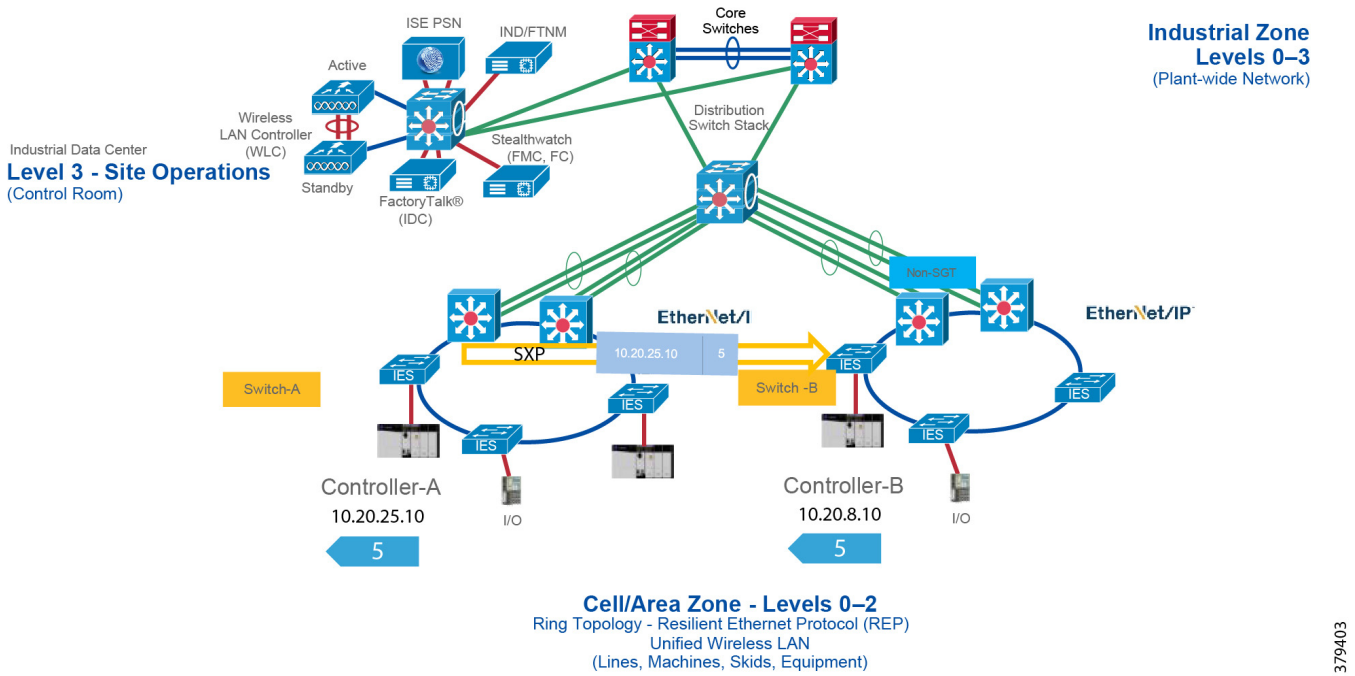
Figure 3-7 Cisco TrustSec SGT Propagation



The previous phase describes a scenario for propagation using a method called in-line tagging. However, in certain network topologies there could be a situation where a switch in the path from the source to the destination does not support in-line tagging. When that scenario happens, the non-SGT capable switch would ignore the SGT in the frame and would send a normal Ethernet frame on the out-going interface. In other words, for in-line tagging feature to work, all the switches in the path must support this feature or the technology would not be applicable.

To circumvent that problem, Cisco TrustSec also supports a different mechanism to transport SGT frames over a path when a non-SGT capable IES (e.g., Allen-Bradley Stratix 5700 or Cisco IE 2000) is present by using an exchange protocol called SGT Exchange Protocol (SXP). SXP is used to securely share SGT- to-IP address mapping. Figure 3-8 shows how to exchange SGT binding over SXP tunnel. In Figure 3-8, Controller-A is establishing communication with Controller-B using an SGT tag value of 5. As you can see there is a non-SGT device in the path and this switch would ignore the SGT enabled frame coming from the distribution switch. For SGT information to be sent to Switch-B, an SXP tunnel is required between Switch-A and Switch-B. This tunnel would carry the binding information, which is 10.20.25.10 mapped to SGT 5.

Figure 3-8 Cisco TrustSec SGT Propagation Using SXP Tunnel



The next stage of Cisco TrustSec is policy enforcement. The enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router, or switch. The enforcement device takes the source SGT and looks it up against the destination SGT to determine if the traffic should be allowed or denied. The advantage of Cisco TrustSec is that any switch, router, or firewall between the source and the destination can impose the policy, but the key requirement is that the enforcement point must be able to map the destination IP address to the tag value. This process is further explained in Figure 3-9. In this scenario Controller_A has been given SGT value of 5 and Controller_B, which is of similar device type, is also given an SGT value of 5. The IO device is given a different tag value because it is of a different device type. Now, in this scenario Controller_A is allowed to establish communication with Controller_C. However, the IO device is not allowed to establish communication with Controller_C. The access policy can be described in Table 3-1.

Table 3-1 Access Policy Example

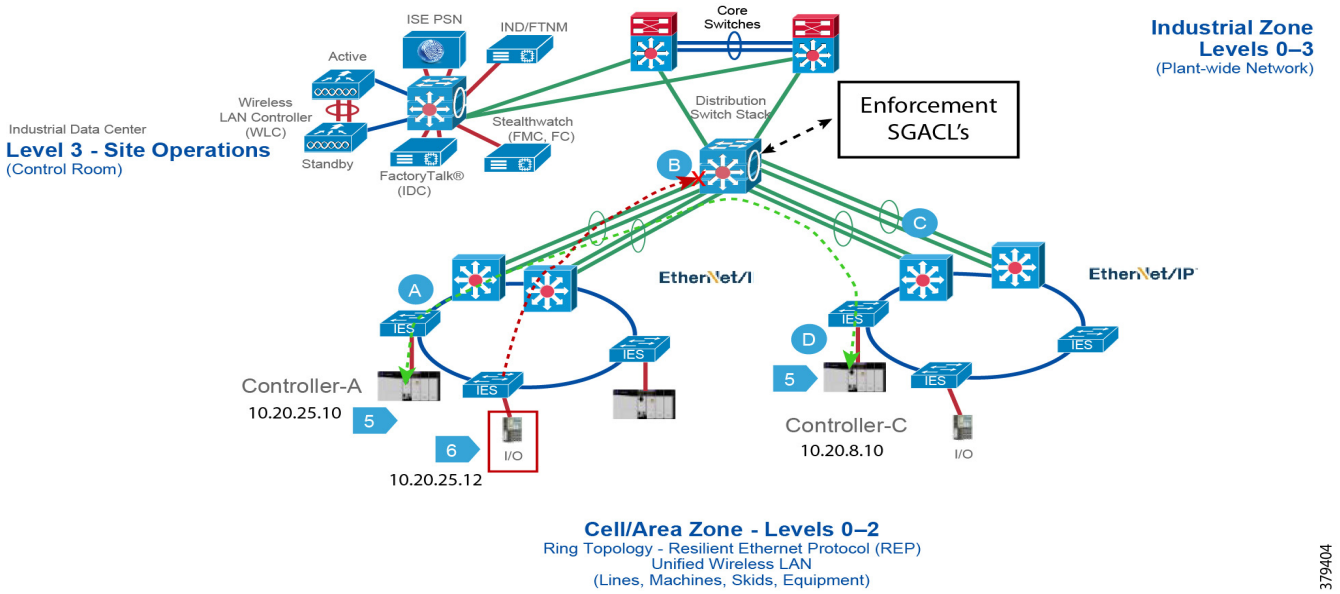
	SGT 5	SGT 6
SGT 5	Yes	No
SGT 6	No	No

The next step is to determine where to apply the policy. As shown in Figure 3-9, the enforcement can be at switches A, B, C, or D. However, as previously indicated, for a switch to enforce a policy it must be able to derive the destination IP address to the tag value. For example, at point A there are two flows occurring: 1) 10.20.25.10, 5 ---- 10.20.8.10, 5 and 2) 10.20.25.12,6 --- 10.20.8.10,5. If the access policy at point A is imposed, then the switch would be only able to understand the source tag, but it has no knowledge of the destination IP address to tag mapping. Switch A would see that the destination IP address is 10.20.8.10, but it does not know that 10.20.8.10 is mapped to tag value of 5, which should be allowed. The same behavior

would be seen if the policy is applied at the point B. If the policy is applied at point C or D it would work because both C, which is Layer 2 adjacent to D, and Switch D, which is directly attached to Controller C, would be able to enforce the policy correctly because it would be able to derive the association between the destination IP and the associated SGT value.

Even though applying access policy at the point which is closest to the IACS asset is the preferred choice, in some situations a policy needs to be applied at a different point. Whenever away from the IACS asset, the knowledge of the mapping between the SGT value and the IP address is lost. To circumvent that problem establish SXP tunnels to the IES that has IACS assets attached to it. The details of using SXP for deriving the mapping information are covered below.

Figure 3-9 Access Policy Enforcement Example



Enforcement Point

The IT security architect must next decide where in the design the access policy should be enforced. Policy enforcement occurs at the distribution switch and there are pros and cons associated with each design choice. For example, consider the case where the policy is enforced on an IES located in the Cell/Area Zone. As stated in the previous section, the basic assumption is that every IACS asset in the Cell/Area Zone must be able to access every other IACS asset. The second assumption is that policies are enforced on East-West communication going across the Cell/Area Zones. For example, two Cell/Area Zones, Cell/Area Zone-1 and Cell/Area Zone-2, and a PAC and I/O are both in the Cell/Area Zones. From a Cell/Area Zone-1 intra-zone policy perspective, every PAC and I/O in Cell/Area Zone-1 must be able to access one another. The inter-Cell/Area Zone security access policy is to block the communication between I/O in Cell/Area Zone-1 to PAC in Cell/Area Zone-2. This security access policy is shown in Table 3-2.

Table 3-2 Enforcement Point

	PAC-Cell/Area-1	I/O-Cell/Area-1	PAC-Cell/Area-2	I/O-Cell/Area-2
PAC-Cell/Area-1	Yes	Yes	No	No
I/O-Cell/Area-1	Yes	Yes	No	No
PAC-Cell/Area-2	No	No	Yes	Yes
I/O-Cell/Area-2	No	No	Yes	Yes

When designing a security policy using TrustSec, associate each IACS asset with a tag. If a PAC tag of 10 and I/O tag of 20 are assigned, designing the same matrix and restricting communication between 10 and 20, then two policy tables are needed: 1) Intra-Cell/Area Zone and 2) Inter-Cell/Area Zone.

Table 3-3 Intra-Cell/Area Zone Access Policy Enforcement

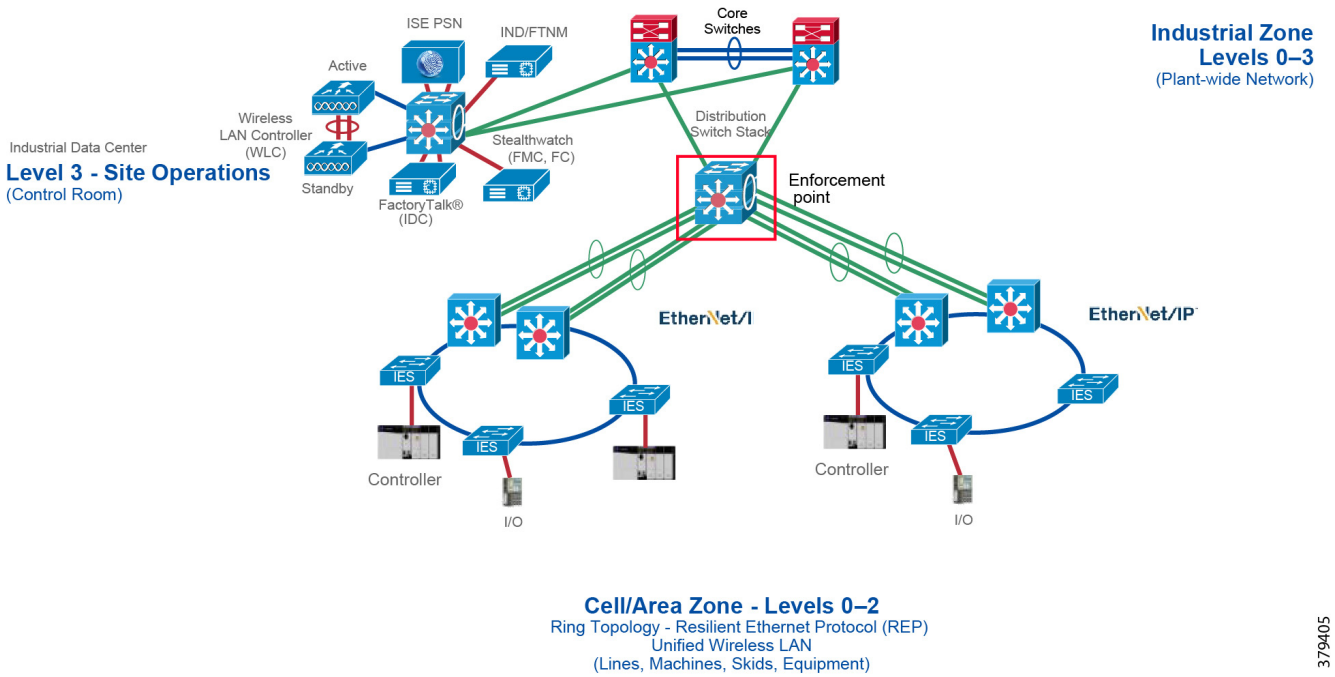
	SGT 10	SGT 20
PAC-Cell/Area-1 SGT 10	Yes	Yes
I/O-Cell/Area-1 SGT 20	Yes	Yes

Table 3-4 Inter-Cell/Area Zone Access Policy Enforcement

	SGT 10	SGT 20
PAC-Cell/Area-2 SGT 10	No	No
I/O-Cell/Area-2 SGT 20	No	No

As seen above, the Cell/Area Zone IES needs to have two tables implemented and that is not possible with the current design. The current TrustSec policy enforcement supports only a single matrix. To ensure both objectives are achieved, implement the security access policy on the distribution switch and do not have any enforcement on the Cell/Area Zone IES. By doing so, the Table 3-3 and Table 3-4 policy requirements have been met because when no policy is imposed on the Cell/Area Zone IES, then all the IACS assets on the Cell/Area Zone IES can communicate with each other. When Figure 3-9 is implemented on the distribution switch, then the inter-Cell/Area Zone or East-West communication can be restricted. Figure 3-10 shows the inter-Cell/Area Zone security access policy enforcement point. If the industrial security access policy requires intra-Cell/Area Zone access control, Cisco and Rockwell Automation recommend IACS application security such as CIP Security from ODVA, Inc.

Figure 3-10 Enforcement Point in CPwE Network Security



Scalable Group Tag Exchange Protocol Considerations

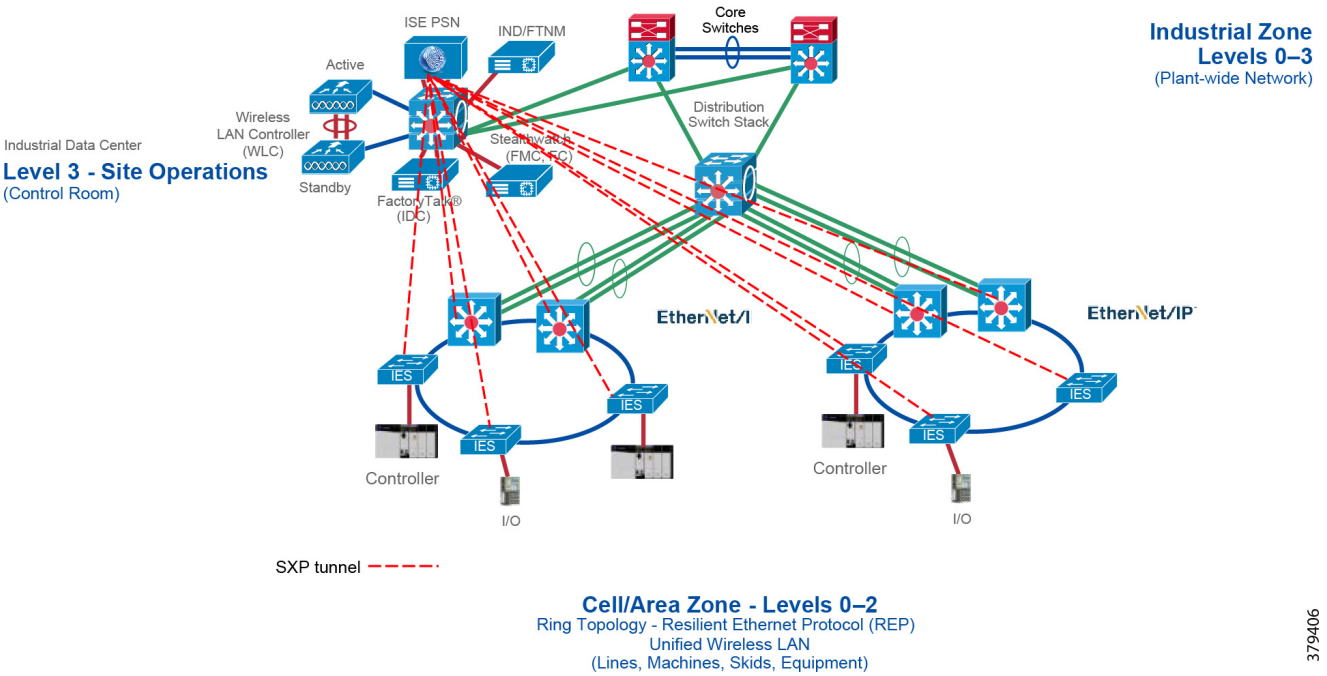
Scalable Group Tag Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up an SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them acts as both speaker and listener. Connections can be initiated by either peer, but mapping information is always propagated from a speaker to a listener.

As shown in the previous section, the enforcement is moved to the distribution switch, so the distribution switch needs to derive the destination IP address to SGT. This is because the Ethernet frame has only the source SGT information and to enforce the policy the distribution switch needs to learn the SGT binding associated with the destination IP address. To help the distribution switch to derive the destination tag, SXP tunnels are needed from the access layer IES to the distribution.

In the current design, SXP tunnels are established from the access layer IES to the Cisco ISE and the distribution switch also has an SXP tunnel to the Cisco ISE. This way the IP-SGT binding information is sent to the Cisco ISE and the distribution switch learns the IP-SGT binding information from the Cisco ISE. Figure 3-11 depicts the design.

Figure 3-11 SXP Design in CPwE Network Security CVD



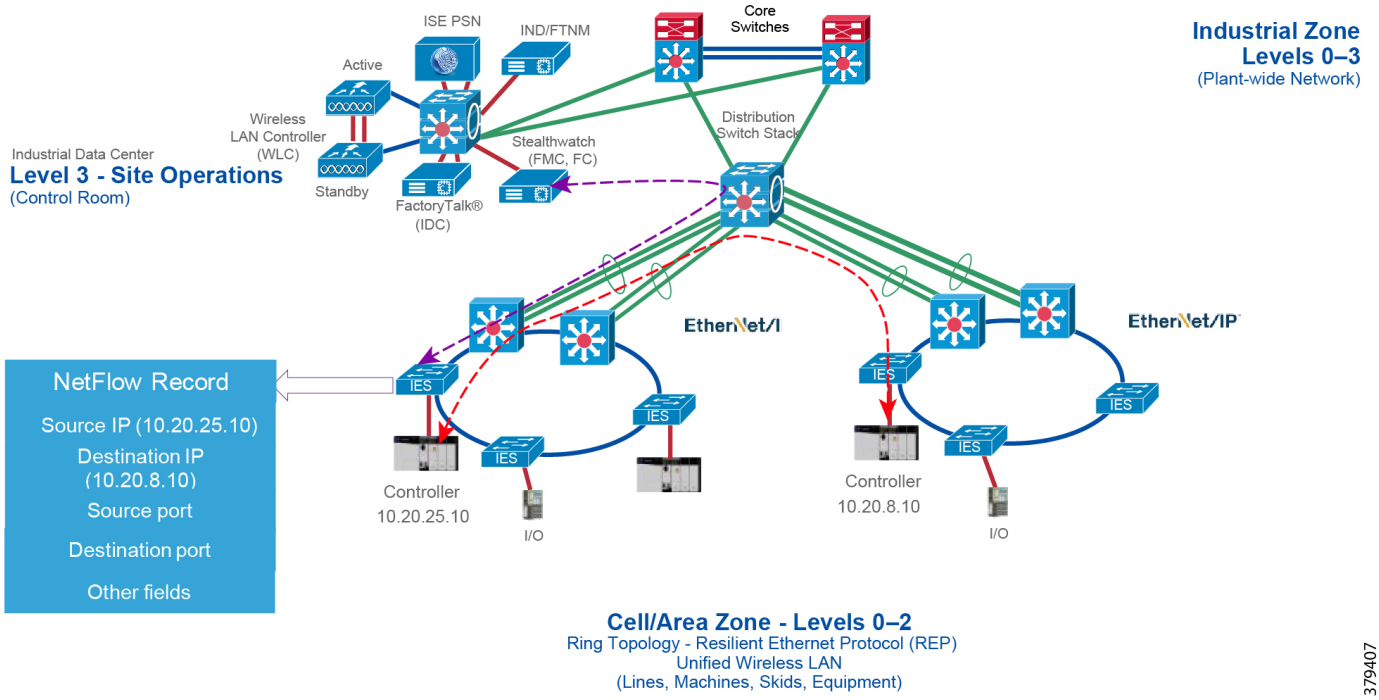
NetFlow Data Collection

A flow is a unidirectional connection between a source and a destination. To describe a full exchange between two devices, two independent unidirectional flows are needed. For example, when data is flowing between client and server, then there are two flows occurring: from client to server and from server to client. NetFlow is a protocol that creates flow records for the packets flowing through the switches and the routers in a network between the end devices and exports the flow records to a Flow Collector. The data collected by the Flow Collector is used for different applications to provide further analysis. Initially, NetFlow was used for providing traffic statistics in a network, but later it started gaining traction as a network security tool. In CPwE Network Security CVD, NetFlow is primarily used for providing security analysis, such as malware detection, network anomalies, and so on. There are many advantages in deploying NetFlow:

- NetFlow can be used for both ingress and egress packets.
- Each networking device in a network can be independently enabled with NetFlow.
- NetFlow does not require a separate management network to collect the traffic.

In a normal flow the 5-tuples information (source IP, destination IP, source port, destination port, and protocol) information is recorded as shown in Figure 3-12.

Figure 3-12 NetFlow Data Collection



With the latest releases of NetFlow, the switch/router can gather additional information such as ToS, source MAC address, destination MAC address, interface input, interface output, and so on. For NMT and ISE integration, collecting the MAC address of the device is very critical. If NMT does not gather the MAC address, then the device is not imported into ISE. The following **show** command output describes the flow record information collected at the IES in the Cell/Area Zone:

```
flow record Cisco Stealthwatch_Record
 description NetFlow record format to send to Cisco Stealthwatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
```

```
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect interface input
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

Configuration of flow records can be done by using NMT, which is discussed in more detail in Chapter 4, "Configuring the Infrastructure." The next important consideration is on managing flows. As network traffic traverses IES and distribution switches, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch flow collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and the standard CIP I/O connections). There are timers to determine whether a flow is inactive or a flow is long lived.

After the flow timeout the NetFlow record information is sent to the flow collector and deleted on the switch. Since the NetFlow implementation is done mainly to detect security-based incidents rather than traffic analysis, Cisco and Rockwell Automation recommend leaving the default value in the switch, which is 30 seconds for inactive timeout and 60 seconds for active timeout.

The next consideration is on enabling NetFlow in the network. Since in this CPwE Network Security CVD NetFlow is enabled for security perspective, the recommendation is to enable NetFlow monitoring on all the IES and distribution switch interfaces in the CPwE network.

Stealthwatch Deployment Considerations

The Stealthwatch solution has two different components, both of which are installed on different systems:

- Flow Collectors
- Stealthwatch Management console

The Flow Collector collects the NetFlow data from the networking devices, analyzes the data gathered, creates a profile of normal network activity, and generates an alert for any behavior that falls outside of the normal profile. Based on the network flow traffic, there could be one or multiple Flow Collectors in a network. The Stealthwatch Management Console (SMC) provides a single point for the IT Security Architect to get a contextual view of the entire network traffic.

Note For example, if there is a single Flow Collector and a single SMC, then there are two virtual or hardware appliances and each appliance has its own IP address and its own device credentials.

The SMC client allows an IT Security Architect to access the SMC graphical user interface by using a web browser. SMC enables the following:

- Centralized management, configuration, and reporting for up to 25 Flow Collectors
- Graphical Charts for visualizing traffic
- Drill down analysis for troubleshooting
- Consolidated and customizable reports

- Trend analysis
- Performance monitoring
- Immediate notification of security breaches

Some important considerations when deploying a Stealthwatch solution include:

- Stealthwatch is available as both hardware (physical appliances) and virtual appliances. To install hardware and software appliances, refer to the Stealthwatch guide at: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf.
- The resources allocation for the Stealthwatch Flow Collector are dependent on the number of flows per second expected on the network and the number of exporters (networking devices that are enabled with NetFlow) and the number of hosts attached to the each networking device. The scalability requirements for the Flow Collector are available at: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf.
- The Data Storage requirements must be taken into consideration, which are again dependent on the number of flows in the network. The sizing table for Data Storage is available at: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf.
- A specific set of ports needs to be open to the Stealthwatch solution in both the inbound and outbound directions. For example, HTTPS needs to be open inbound so that a client can access the Stealthwatch solution for managing the appliances. Similarly, certain ports such as DNS, NTP, and external log sources should be open in the outbound direction so that the Stealthwatch solution can reach those services. For the complete list of ports that are recommended to be open, refere to: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf.

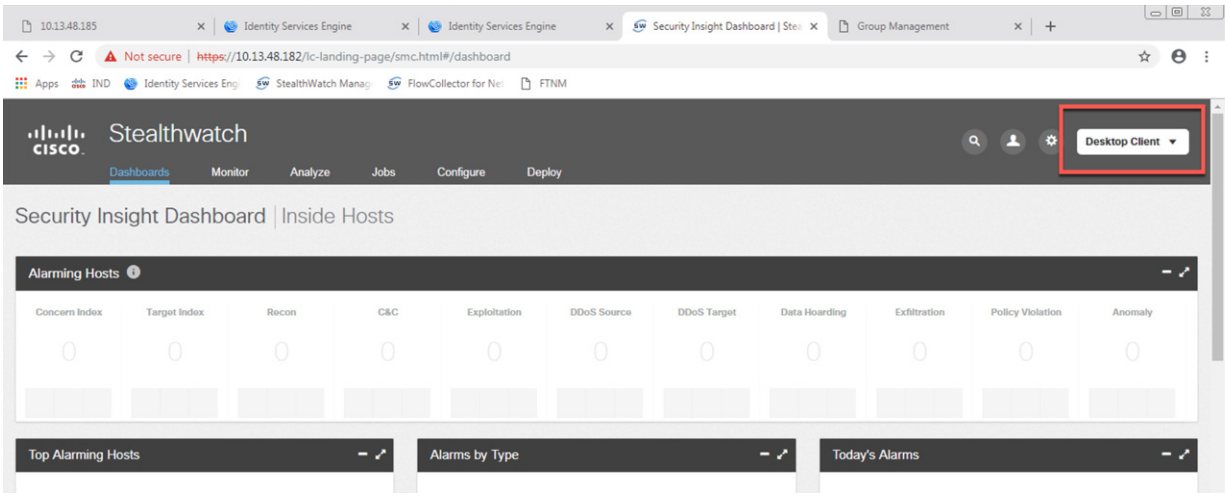
Stealthwatch Flow Collection

This section describes:

Launching the Stealthwatch Web Client

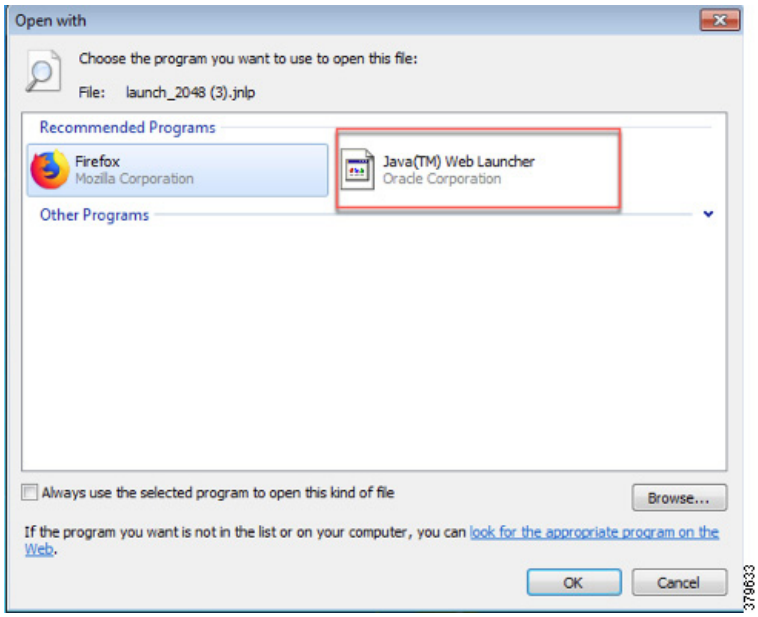
The Stealthwatch web client is a JAVA-based client that can be used to configure Stealthwatch and view flow data. To access the Stealthwatch web client, the IT Security Architect can use a web browser to establish a HTTPS connection to the Stealthwatch web client and then click the **Desktop Client** button, which is found in the upper-right corner of the screen as shown in Figure 3-13:

Figure 3-13 Desktop Client Button



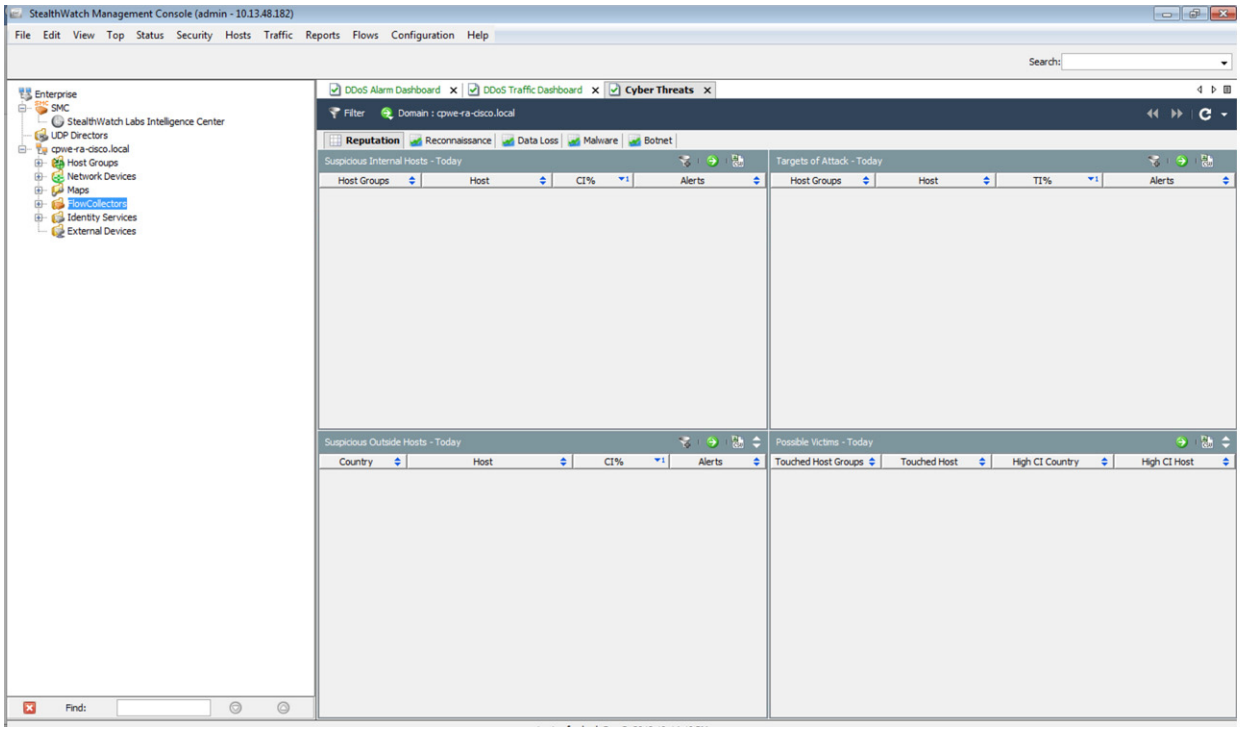
Clicking the **Desktop Client** button downloads the software on the computer where the HTTPS session was initiated. Opening the file displays Figure 3-14.

Figure 3-14 Software Installer



After a successful log in, the IT Security Architect sees the screen in Figure 3-15.

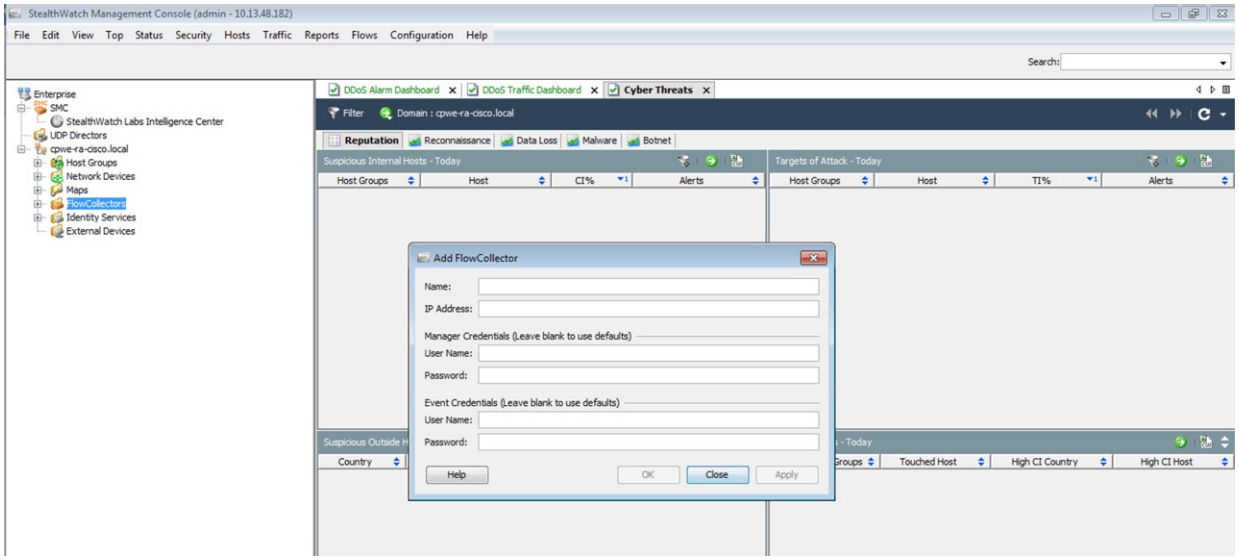
Figure 3-15 Stealthwatch Management Console



Configuring Flow Collector

Typically, the Flow Collectors are registered during the installation of the SMC. However, if a Flow Collector needs to be added to the SMC after the initial set up, then select the option **FlowCollector** -> **Add FlowCollector**.

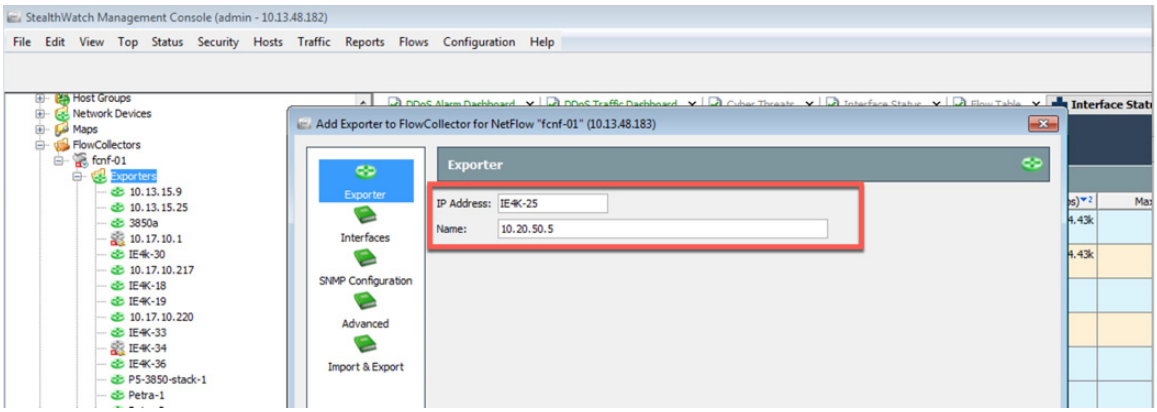
Figure 3-16 Adding a Flow Collector



Configuring Flow Exporters

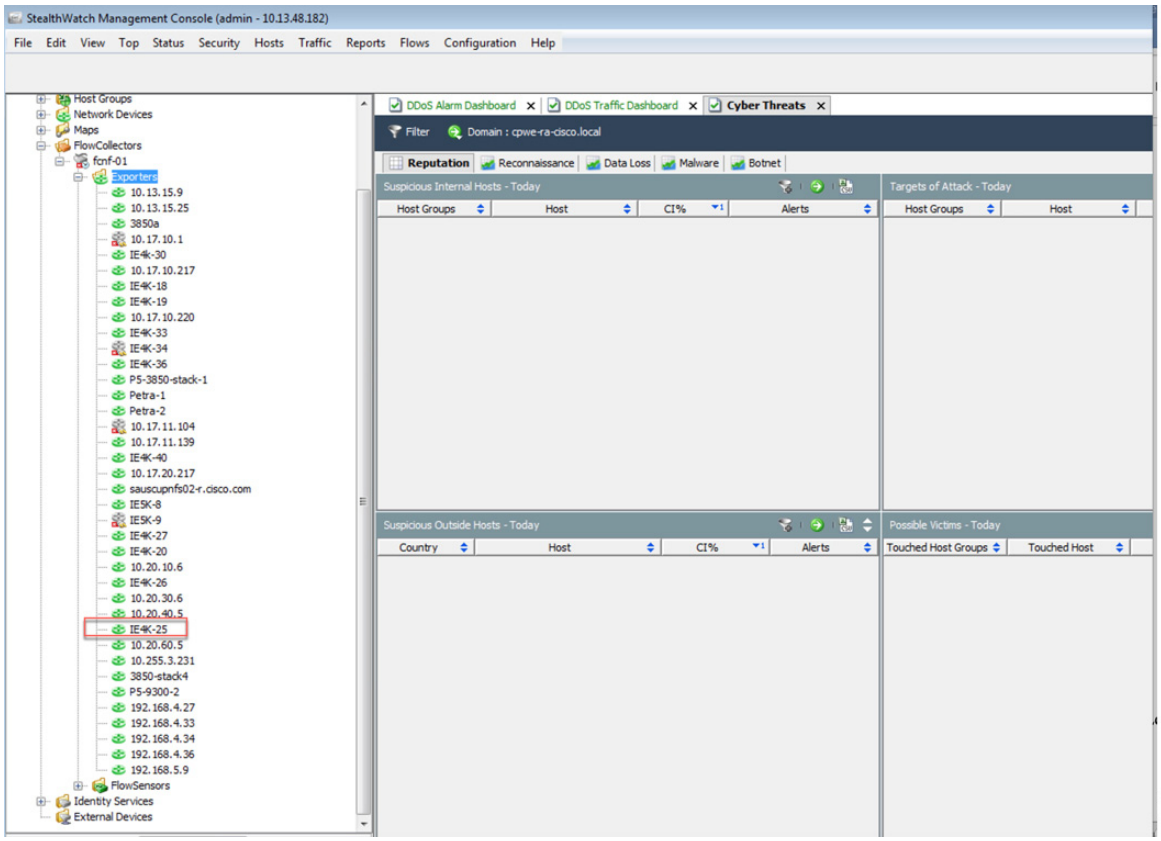
In Stealthwatch context, Flow Exporters are the networking devices that send the flows to the Stealthwatch Flow Collector. The configuration for the Flow Exporter is done by selecting **Exporter** -> **Configuration** -> **Add Exporter**, as shown in Figure 3-17.

Figure 3-17 Configure Flow Exporters



Once configured, the Flow Exporter should up in the tree under the Flow Collector, as shown in Figure 3-18.

Figure 3-18 Flow Exporters



Configuring the Host Groups

A host group is a “container” of hosts or IP addresses that share attributes and policies. Host groups enable the establishment of different thresholds or the bypassing of alerts for certain behavior. Using host groups correctly in the Stealthwatch solution helps ensure that you are alerted correctly about events and that the information provided to you is relevant. The following are some of the different attributes that are typically grouped together:

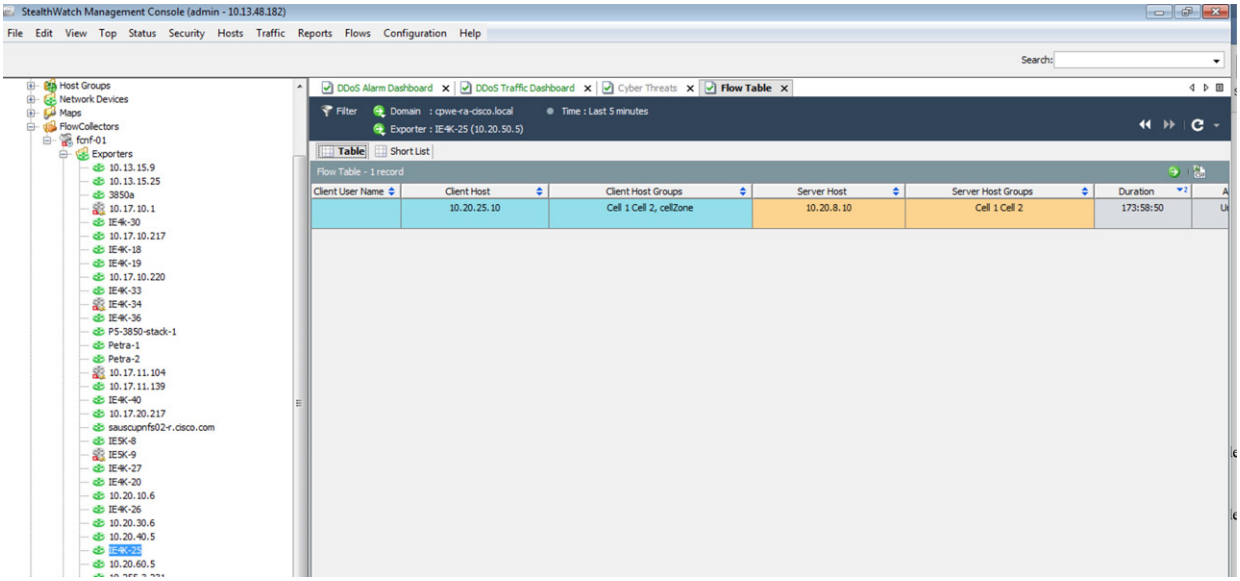
- Shared functions
- Exhibits similar behavior
- Can be managed as a single object
- To which a single policy can be applied

For more information about Host Groups, refer to:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/iot-threat-defense-mfg-design-implementation-guide.pdf

Viewing the Flows Generated by Flow Exporter

To view the flows generated by a Flow Exporter, select the **Flow Exporter** -> **Flows** -> **Flow Table**, as shown in Figure 3-19.

Figure 3-19 Flow Exporter Flows



Cisco ISE Deployment Considerations

Deploying Cisco ISE in a large network requires an IT security architect to consider several factors such as scalability and high-availability of the Cisco ISE deployment. Cisco and Rockwell Automation have developed a design and implementation guide on Deploying Identity and Mobility Services within CPwE. This design guide covers in depth many factors related to deploying a large-scale Cisco ISE deployment

model. The design considerations listed in the CPwE Identity and Mobility Services CVD are very much related to the current CPwE Network Security CVD effort. Cisco and Rockwell Automation encourage the reader to read this DIG to develop a good understanding of large-scale solution deployments. Some of the key recommendations given in the design guide are shown here as a quick reference.

In the distributed installation, the Cisco ISE system is divided into three discrete nodes (personas)—Administration, Policy Service, and Monitoring—which are described as follows:

- Policy Administration Node (PAN) allows the Enterprise IT team to perform all administrative operations on the distributed Cisco ISE system. The PAN (located in the Enterprise Zone) handles all system configurations that are related to functionality such as authentication and authorization policies. A distributed Cisco ISE deployment can have one or a maximum of two nodes with the Administration persona that can take on the primary or secondary role for high availability.
- Policy Service Node (PSN) provides client authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation. At least one node in a distributed setup should assume the Policy Service persona and usually more than one PSN exists in a large distributed deployment.
- Monitoring Node (MnT) functions as the log collector and stores log messages and statistics from all the Administration and Policy Service Nodes in a network. The MnT (located in the Enterprise Zone) aggregates and correlates the data in meaningful reports for the Enterprise IT and operational technology (OT) personnel. A distributed Cisco ISE system can have at least one or a maximum of two nodes with the Monitoring persona that can take on primary or secondary roles for high availability.

For optimal performance and resiliency, Cisco and Rockwell Automation provide these recommendations for the CPwE Identity and Mobility Services architecture:

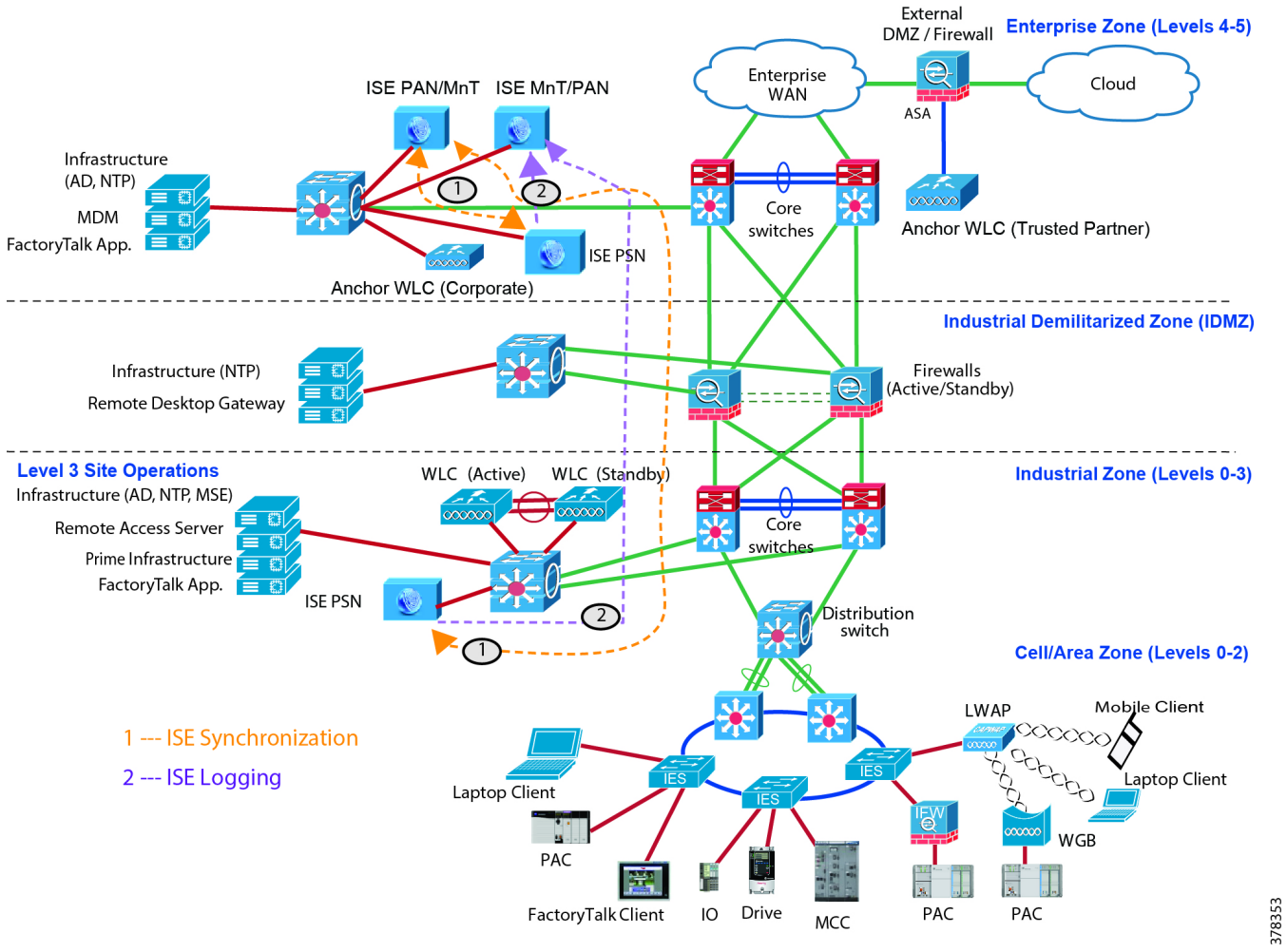
- Administration and Policy Service personas should be configured on different Cisco ISE nodes.
- Monitoring and Policy Service personas should not be enabled on the same Cisco ISE node. The Monitoring node should be dedicated solely to monitoring for optimum performance.
- A PSN should be placed in the Industrial Zone (Levels 0-3) to provide services for clients in the Industrial Zone. If the Enterprise and Industrial Zones become isolated, any existing clients will still be able to securely access the network. For best practices, see Appendix A, “References” for links to the CPwE IDMZ CVD DIG.
- A PSN should also be present in the Enterprise Zone to authenticate corporate mobile users who connect to the corporate network through the IDMZ in a secure data tunnel. This scenario is covered in detail later in the document.

Based on the recommendations above, a typical distributed Cisco ISE deployment in the CPwE architecture consists of the following nodes (hardware appliances or VM) as shown in Figure 3-20.

- One Primary Administration/Secondary Monitoring node
- One Secondary Administration/Primary Monitoring node
- One or several PSN in the Enterprise Zone
- One or several PSN in the Industrial Zone

Note The number of PSN in the Enterprise and Industrial Zones may depend on the company size, the number of active clients, redundancy requirements, and geographical distribution (for example, one PSN per each plant).

Figure 3-20 ISE Deployment Models



IPDT Considerations

IP Device Tracking (IPDT) is feature that allows an IES or any other switch or router to keep track of connected hosts attached to it. The IPDT feature must be enabled for several security features such as dot1x, MAB, Web-Auth, auth-proxy, and so on. The IPDT feature keeps mappings between IP addresses and mac-addresses. To do the tracking, the IES when enabled with IPDT feature sends an ARP probe with default interval of 30 seconds. The probes are implemented as per RFC5227 where the source IP address is set to 0.0.0.0. If the IPDT feature is enabled with a default source IP address of 0.0.0.0, then there could be conflict between the IES and an IACS asset that is also doing device tracking (the Duplicate IP address 0.0.0.0) problem is explained in: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problemsolution-product-00.html).

To avoid this problem, the recommended option is to modify the standard IP address used with the IPDT feature prior to the implementation of IPDT. The following command can be used in an IES:

```
ip device tracking probe auto-source fallback 169.254.26.64 0.0.0.0 override
```

This command uses the source of the probe to SVI if present and falls back to 169.254.26.64, which is a link-local IP address. The rational for using a link-local IP address as a fallback is based on the assumption that any device attached to the switch does not have a link-local IP address. The link-local IP address is used only to route packets within a local segment and if a router receives a link-local IP address then it does not forward the packet. The IT security architect must verify if there is any link-local IP address present in the network before enabling the command.

Note IP Device Tracking (IPDT), which operates in accordance with RFC 5227, must be enabled on the IES to implement RADIUS downloadable ACL, NetFlow, and SGT. IPDT uses ARP probes to determine the IP addresses of hosts on different ports; this behavior may disrupt IACS assets devices and applications. IPDT should only be enabled in the following situations on IES ports with 802.1X authentication:

- Maintenance ports and/or designated non-IACS equipment ports
- IACS ports with MAC Authentication Bypass if DACL is required by the security policy, with proper IPDT workaround applied and tested with IACS assets devices and applications

By default, IPDT should not be enabled on ports connected to IACS assets devices and applications if DACL functionality is not required. Refer to the URL below for more details and IPDT workarounds: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

CHAPTER 4

Configuring the Infrastructure

This chapter describes how to configure CPwE Network Security Solution infrastructure components such as Cisco ISE, Cisco IE and Allex-Bradley Stratix industrial Ethernet switches (IES), and NMT based on the design considerations of Chapter 3, "CPwE Network Security Design Considerations." This chapter provides screen shots for the specific features and also the CLI configuration of an IES. It includes the following major topics:

- NMT configuration
- Cisco ISE configuration
- IES configuration

Network Monitoring Tool

This section describes validated configuration for the NMT needed for the following features:

- Creation of Asset discovery profiles for IACS assets and networking devices.
- Creation of Access Profiles that will be used in discovering IACS assets and networking devices.
- Creation of groups for IACS assets and networking devices based on the Cell/Area Zone Groups.
- Creation of assetTags that will be used to provide additional attributes to Cisco ISE for profiling IACS assets.
- Detailed steps for pxGrid integration between NMT and Cisco ISE.

Installation

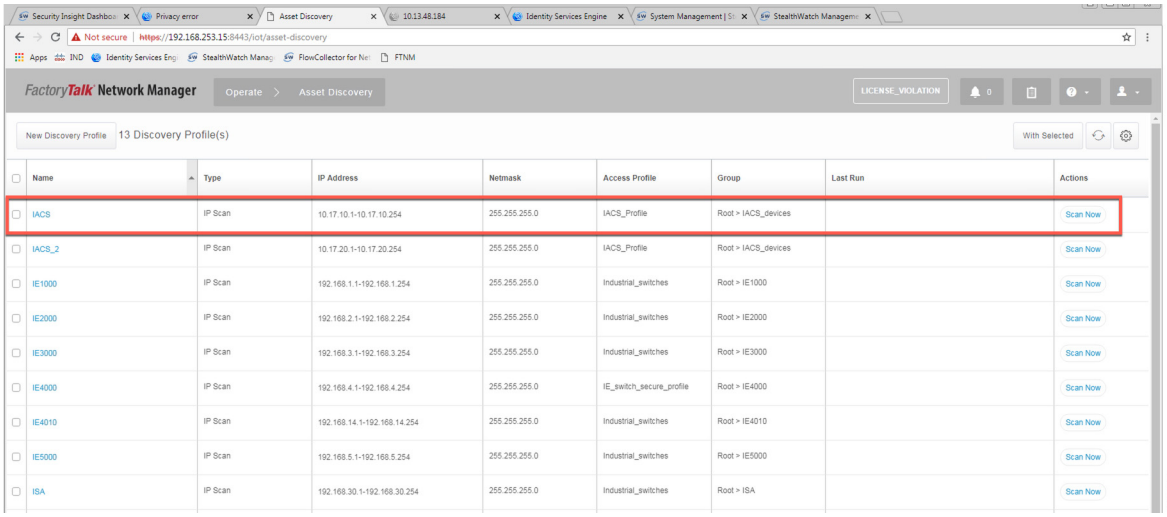
The installation notes for NMT can be found at:

- https://compatibility.rockwellautomation.com/Pages/MultiProductFindDownloads.aspx?crumb=112&refSoft=1&toggleState=&versions=57256
- https://www.cisco.com/c/en/us/td/docs/switches/ind/install/IND_1-5_install.html

Creating Asset Discovery Profile

The objective of creating an asset discovery profile is to define an IP address scope of different IACS assets and networking devices and scan those assets. If the IACS or networking device is reachable, then NMT scans the device, discovers the attributes, and moves them to the asset-inventory section. Figure 4-1 shows how different asset discovery profiles are defined in NMT.

Figure 4-1 Creating the Asset Discovery Profile

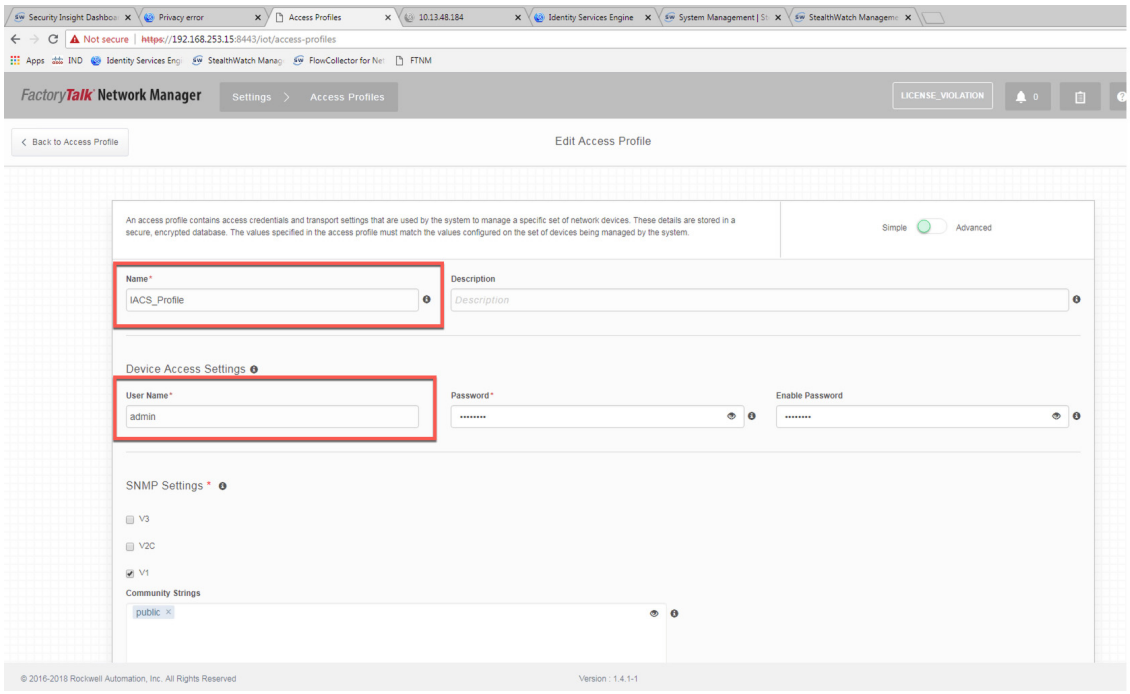


As shown in the first row of Figure 4-1, IACS profile is performing an IP scan for the IP address range 10.17.10.1 - 10.17.10.254. The Access_Profile used for this scan is IACS_PROFILE (explained in the next section) and all these devices are attached to a group called IACS_devices (also explained in the section below).

Configuring Access Profiles

The Access Profile is a template that has the common configuration parameters: username, password, and the SNMP community string information. When a group of devices use a different set of parameters, then a separate Access Profile can be defined. The Access Profile created in this section is tied to the Discovery Profile. Figure 4-2 shows the details of an Access Profile named IACS_PROFILE.

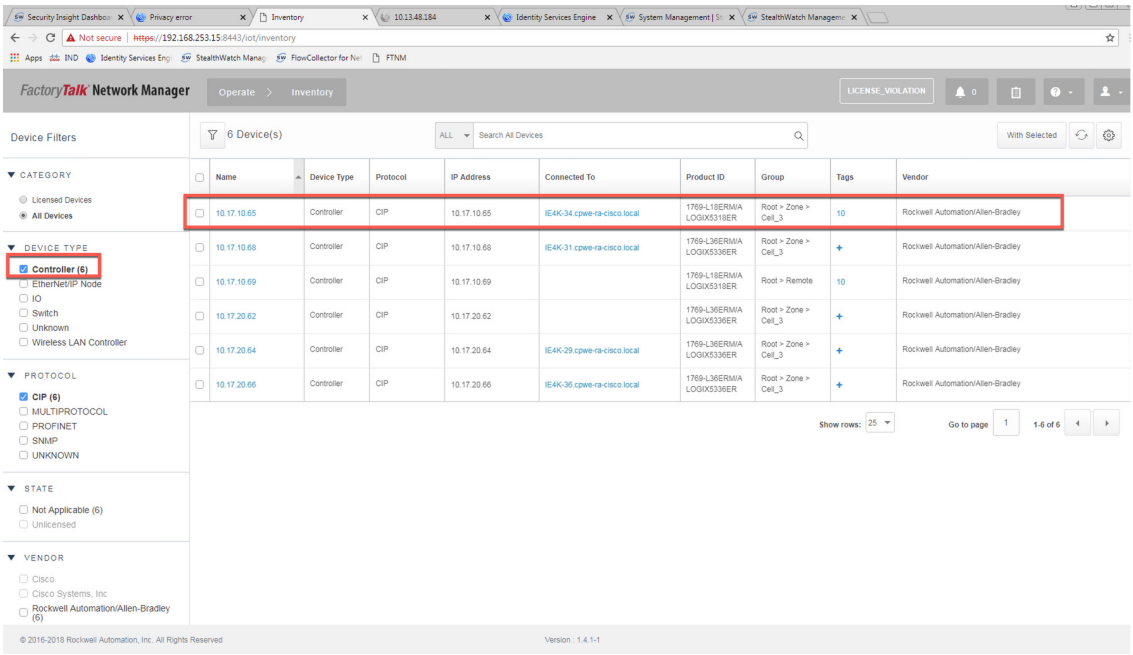
Figure 4-2 Configuring the Access Profile



Asset Inventory

NMT maintains list of devices that it has discovered in the Asset Inventory. Each element of the Asset Inventory provides information such as an IES that is attached to an IACS asset, the device type (Controller, IO, and other device types), the interface between the IACS device and the IES, the protocol used to communicate with the IACS asset, IP address of the IACS asset, group information of the device, vendor information, and so on. There are filters available for OT control system engineers to search for devices based on different criteria. Figure 4-3 shows a list of controllers that support the CIP protocol. As shown in Figure 4-3, NMT displays important information about the IACS asset.

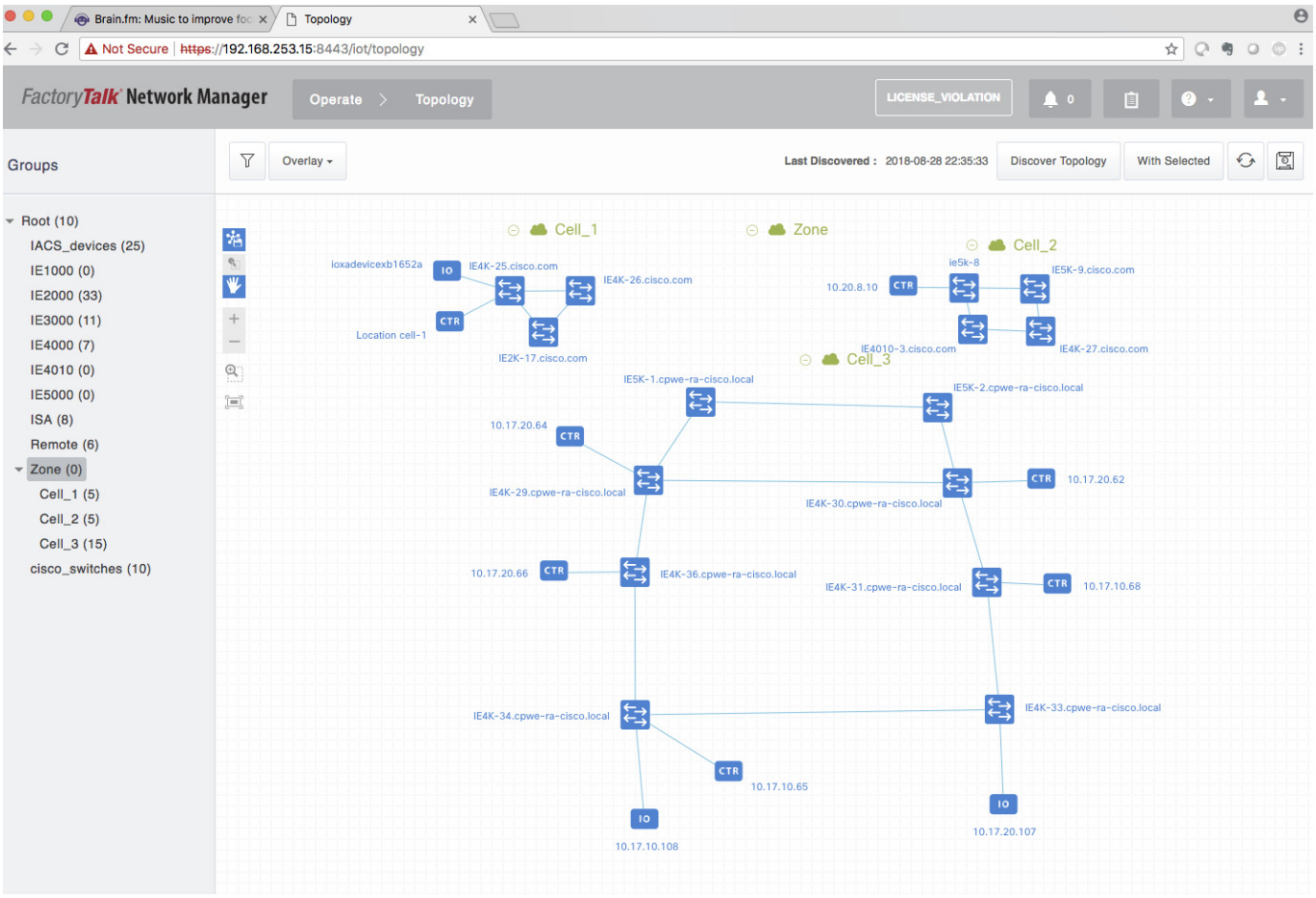
Figure 4-3 Asset Inventory of NMT



Group Management

Managing devices in separate groups not only simplifies the management of devices, but can also allow an OT control system engineer to influence an access policy for IACS assets. Figure 4-4 shows three groups that have been created based on the Cell/Area Zone topology.

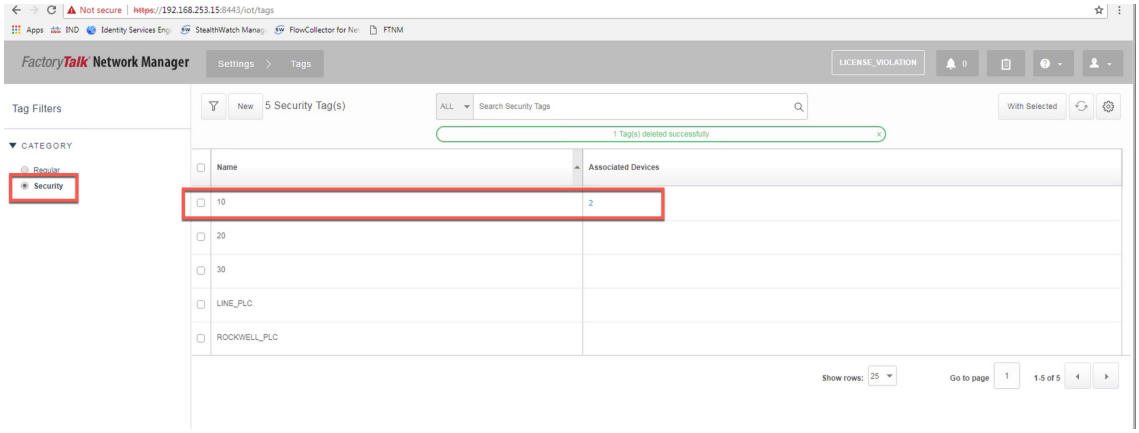
Figure 4-4 Topology Diagram for FTNM



Configuring Security Tags

NMT release 1.4 and greater supports another important feature called security tags. An OT control system engineer can tag a device with a security tag. This feature allows an OT control system engineer to express an intent for an IACS asset (for more information about intent, see OT Managed Remote User (Employee or Partner) Accessing from (Enterprise or Internet) to a Network Device or an IACS Asset in Chapter 5, "Implementation of Use Cases"). Figure 4-5 show how security tags can be created. In Figure 4-5 the security tag of 10 has been assigned to two devices.

Figure 4-5 Configuring Security Tags in NMT



Licensing

NMT comes up with a base license that allows an OT operator to create Asset Discovery Profiles, scan the assets, and export the asset attributes to Cisco ISE. To perform these tasks, no special license is required. However, if the OT operator would like to have access to features of NMT for managing IES devices, then licenses must be purchased.

Licensing features include:

- Switch diagnostics and monitoring such as:
  - Port utilization
  - Interface statistics
  - Syslog
  - CPU and memory usage
  - SD Flash capacity
  - Power supply status
  - Connected devices
  - Alarms
  - MAC and VLAN tables
  - Configuration backup and archives
  - DLR data
- CIP backplane bridging (does not work with Trustsec)

To obtain more information on licenses for NMT, see:

- https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf
- https://www.rockwellautomation.com/rockwellsoftware/products/factorytalk-network-manager.page

Configuring Cisco ISE

This section gives details on how to configuring Cisco ISE for the following components:

- Distribution Deployment
- pxGrid between Cisco ISE and NMT
- Enabling Profiling and configuring different profiling policies
- TrustSec Configuration

Distribution Deployment

As mentioned in the Cisco ISE Deployment Considerations, distributed deployment of ISE was chosen for this CPwE Network Security CVD DIG and also validated with the distribution deployment model. Figure 4-6 shows how different instances of ISE were used to achieve the distribution model:

Figure 4-6 Devices Present in Distributed ISE Deployment

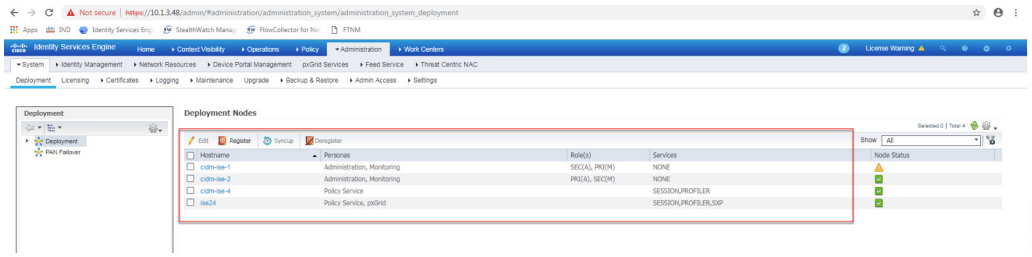


Table 4-1 describes the role for each of the ISE instances.

Table 4-1 ISE Instance Roles

Device Name	Role
cidm-ise-2	Primary role is for Administration and Secondary role is for Monitoring
cidm-ise-1	Primary role is for Monitoring and Secondary role is for Administration
cidm-ise-4	Policy Service Node
ise24	Policy Service Node

As shown in Table 4-1, cidm-ise-2 is the PAN node for this design, and all the administration tasks such as configuration of network devices, authentication policies, authorization policies, certificate management, checking logs and all other tasks must be done on this PAN. No configuration is done on the PSN nodes. The network access devices will use the IP address of the PSN node for RADIUS and CTS configuration. The

network access devices must not point to the PAN node. In this CPwE Network Security CVD DIG, when displaying information on navigation it would be mentioned as (ISE admin web), which means configuration is done on the PAN node.

Configuring pxGrid between Cisco ISE and NMT

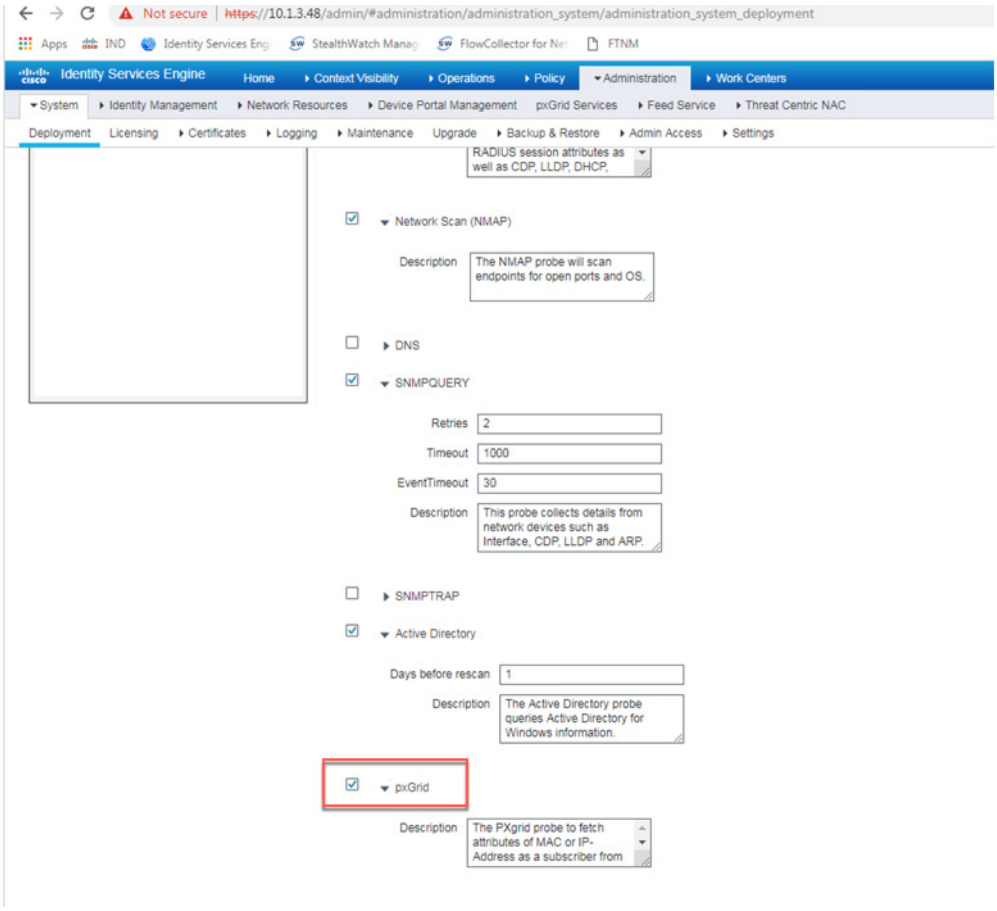
Enabling pxGrid registration between NMT and Cisco ISE involves a couple of steps. The pxGrid framework needs certificate-based authentication. So, both Cisco ISE and NMT need to present their certificates to each other for the registration process to be completed. The next sub-sections describe the following steps that need to be performed:

- Enabling pxGrid in Cisco ISE
- Enabling pxGrid Service in Cisco ISE Certificate
- Exporting the Cisco ISE Certificate
- Downloading NMT Certificate
- Importing NMT Certificate to Cisco ISE
- Configuring pxGrid on NMT
- Approving NMT Client in Cisco ISE

Enabling pxGrid in Cisco ISE

The pxGrid service needs to be enabled in the Cisco ISE. To enable pxGrid service, go to **(ISE admin web)—>Deployment**. Figure 4-7 shows how to enable pxGrid services in the Cisco ISE.

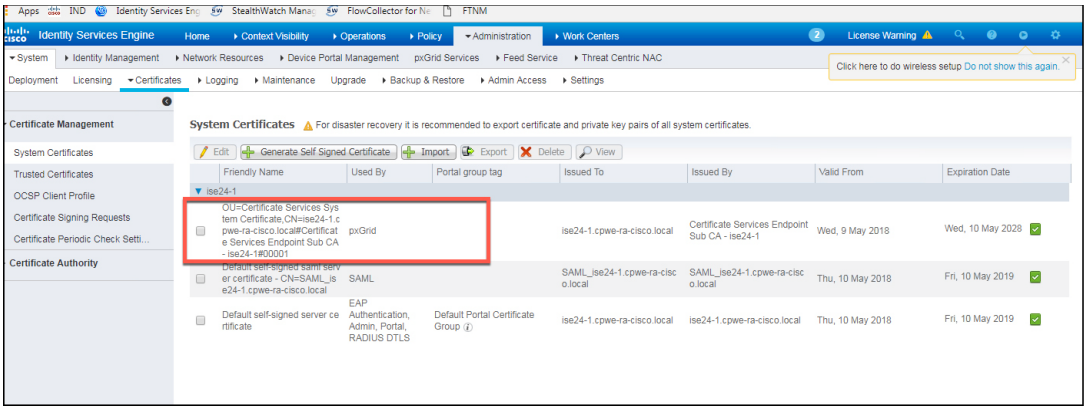
Figure 4-7 Enabling pxGrid Service in the Cisco ISE



Enabling pxGrid Service in Cisco ISE Certificate

For pxGrid registration between NMT and Cisco ISE to work, the root certificate for Cisco ISE needs to be exported into NMT. This step is done on the PAN PRI. The first step is to pick a certificate in **(ISE admin web)—> Administration—>Certificate—>System Certificate** and then enable pxGrid services in that certificate. Figure 4-8 shows pxGrid service enabled for a self-signed certificate in Cisco ISE.

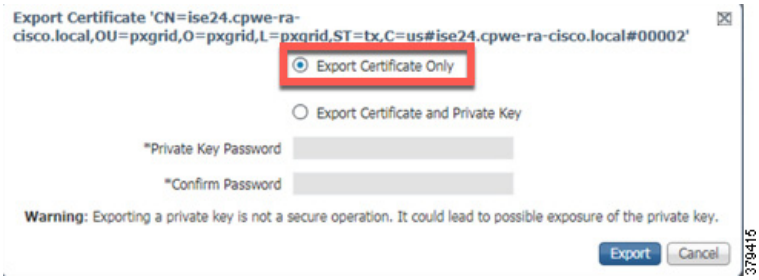
Figure 4-8 Cisco ISE Certificate with pxGrid Services Enabled



Exporting the Cisco ISE Certificate

The next step is to export the above certificate so that the exported certificate can be imported to NMT. After the export option is selected, the file will be downloaded into the local computer. The downloaded certificate needs to be saved and is used in the NMT pxGrid registration to ISE, which is shown in Configuring pxGrid on NMT.

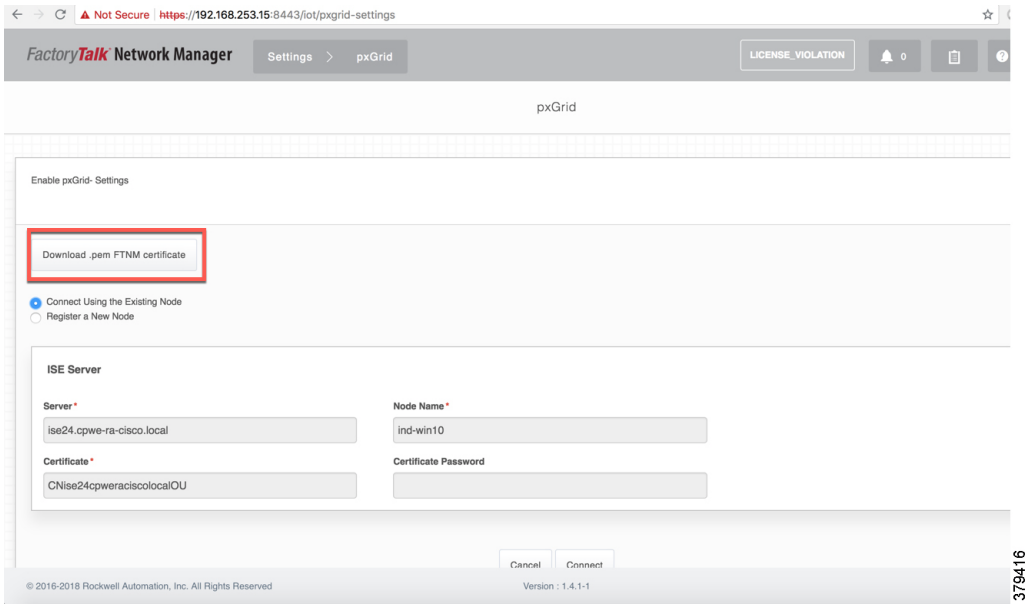
Figure 4-9 Exporting Cisco ISE Certificate



Downloading NMT Certificate

The self-signed certificate of the NMT must be exported from the NMT and must be imported to Cisco ISE as a trusted certificate. This step is mandatory because for the Cisco ISE to trust NMT, it must know the root certificate of NMT. Figure 4-10 shows the option for downloading the NMT certificate. When **Download .pem NMT certificate** is selected, the certificate is downloaded to the computer which must, in the next step, be imported into Cisco ISE.

Figure 4-10 Download NMT Certificate

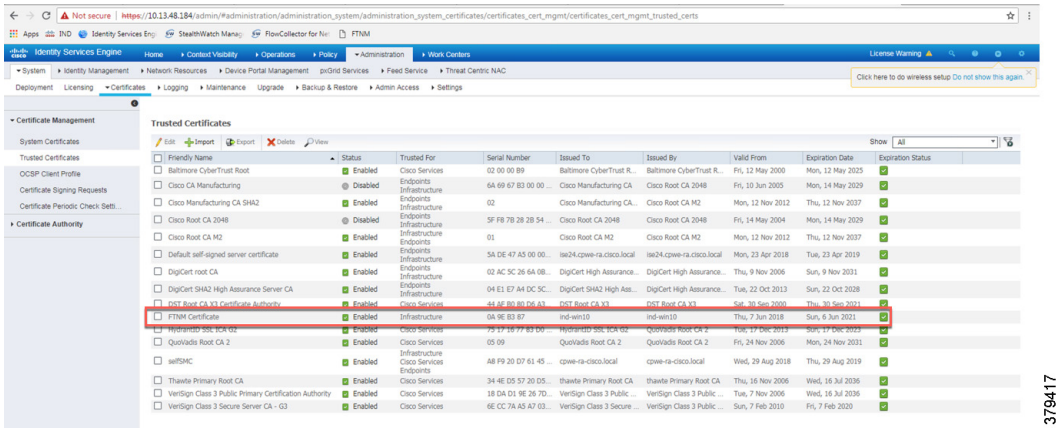


Importing NMT Certificate to Cisco ISE

The NMT certificate must be imported into:
(ISE admin web)—>Administration—>Certificates—>Trusted Certificates store

Figure 4-11 shows the status on Cisco ISE after the NMT certificate is imported into the Cisco ISE Trusted Certificates list.

Figure 4-11 Import NMT Certificate to Cisco ISE

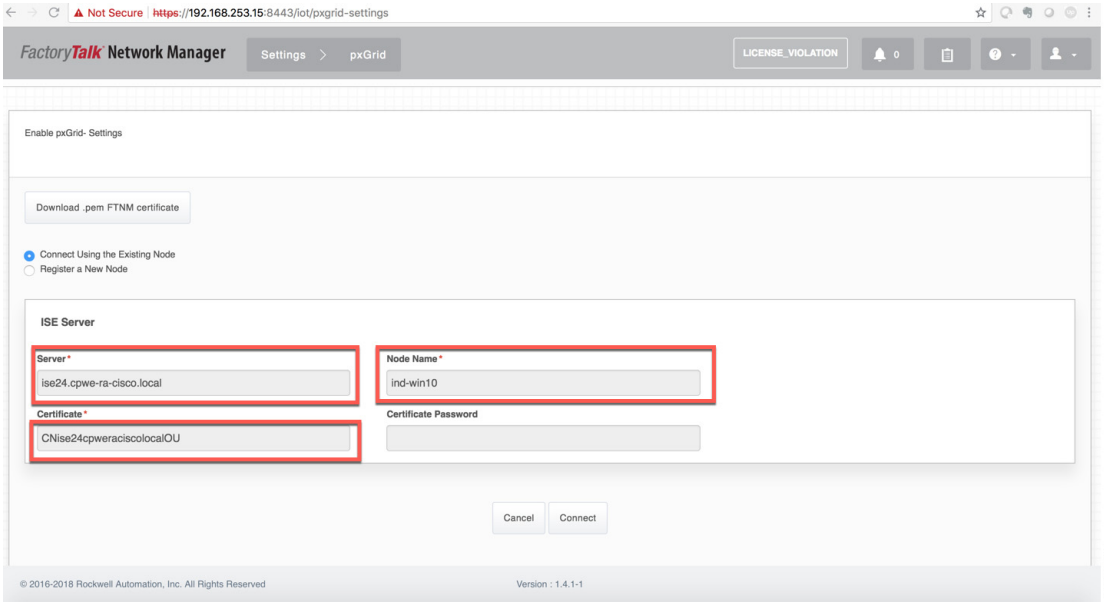


Configuring pxGrid on NMT

On the NMT, pxGrid registration needs to be performed. Figure 4-12 shows the parameters that must be provided for successfully registering NMT to Cisco ISE. The server information is the FQDN name of the Cisco ISE server and it must be resolvable by the NMT either by using DNS or using a local host to IP address mapping in the NMT server. The Node Name can be any name that is easier to remember and the Certificate field is the certificate that was downloaded in the previous step. When the connection is initiated from NMT

for pxGrid set up, the acknowledgment must say that pxGrid registration is successful. If no response is received, then further troubleshooting must be performed. When the registration is successful, the NMT will be listed under the web-clients list in Cisco ISE, which is shown in Figure 4-13.

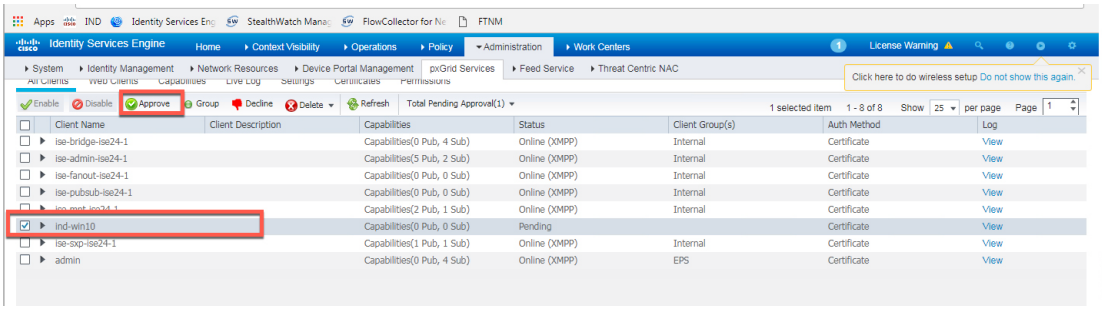
Figure 4-12 pxGrid Registration in NMT



Approving NMT Client in Cisco ISE

The NMT web-interface may report that the registration between NMT and Cisco ISE is successful. But the IT security architect must approve the NMT registration request on Cisco ISE as shown in Figure 4-13.

Figure 4-13 Approving NMT Client in Cisco ISE



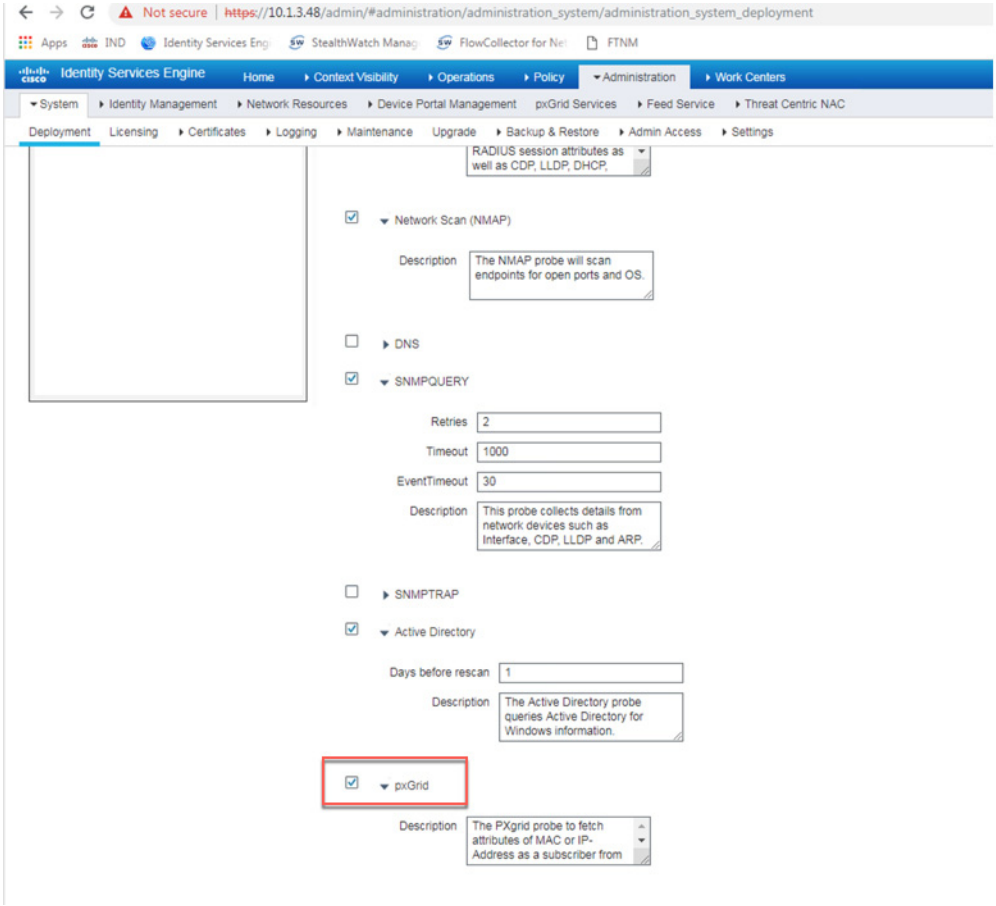
Profiling in Cisco ISE

Profiling in Cisco ISE happens using several probes such as RADIUS, DHCP, SNMP, and so on. Cisco ISE can profile different types of assets, but this CPwE Network Security CVD DIG focuses on profiling IACS assets using pxGrid probe.

Enabling pxGrid Probe in Cisco ISE

To discover IACS assets, Cisco ISE uses pxGrid probe to discover and profile IACS assets. To enable pxGRID probe, navigate to **(ISE admin web)—>Administration—>Deployment** and then select the appropriate PSN (ise24 in this CPwE Network Security CVD) and then select the profiling tab where an option is provided to enable the pxGRID probe. Figure 4-14 shows how to enable pxGrid probe in Cisco ISE.

Figure 4-14 Enabling pxGrid Probe in Cisco ISE



Creation of User Groups

In this CPwE Network Security CVD DIG some example groups were create to explain how OT control system engineers and IT security architects can create groups of devices and profile them. Table 4-2 gives an example on different roles for IACS assets in a plant-wide architecture. The description in Table 4-2 shows the permission needed for a particular user group. For example, a device classified as Level_3 group is a device that needs access to all the devices in the plant-wide architecture. Similarly, a device classified as Level_0_IO device has access to devices that are located in a particular Cell/Area Zone. The main intent of the Table 4-2 access policy example is only to provide a reference example for designing an access policy using TrustSec in a plant-wide network.

Table 4-2 Creation of Device Access Profile Groups

Device	Location in Plant-wide Network	Access Level
Engineering Workstation (EWS)	Level 3 site operations	Must have access to all the devices in the plant-wide architecture
Controller Interlocking	Cell/Area Zone	All the inter-locking PACs must have access to another inter-locking PAC
Level_2_HMI	Cell/Area Zone	LEVEL_2_HMI must have access to all the devices in Level_0 and Level_1
Level_1_Controller	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_IO	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_Robot	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_Drive	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_Generic	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
LOCAL_PARTNER	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
REMOTE_ACCESS	Cell/Area Zone	Access to a remote desktop server
REMOTE_DESKTOP	Level 3 site operations	Access to a device with SGT value = REMOTE_ACCESS
Production user (PROD_USER)	Level 3 site operations	Access to all devices in the plant-wide architecture
Operator Workstation (OWS)	Level 3 site operations	Access to all devices in the plant-wide architecture

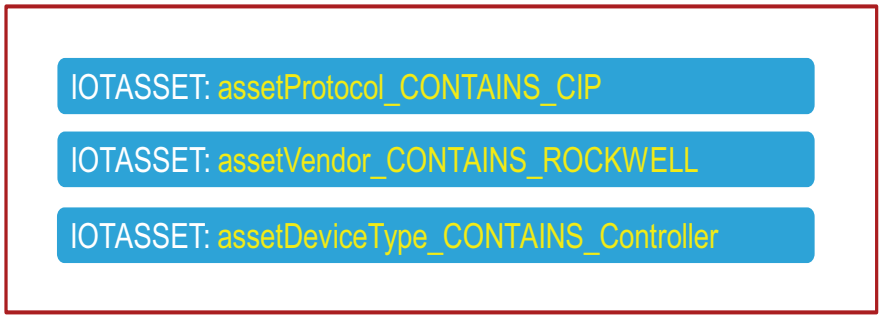
Profiling Policies in Cisco ISE

Profiling policies in Cisco ISE are used to profile IACS assets. This section shows how to create different profiling policies based on Table 4-2.The profiling policies shown here are meant as an example and should not be considered a method for the actual deployment.

Level_1_controller Policy

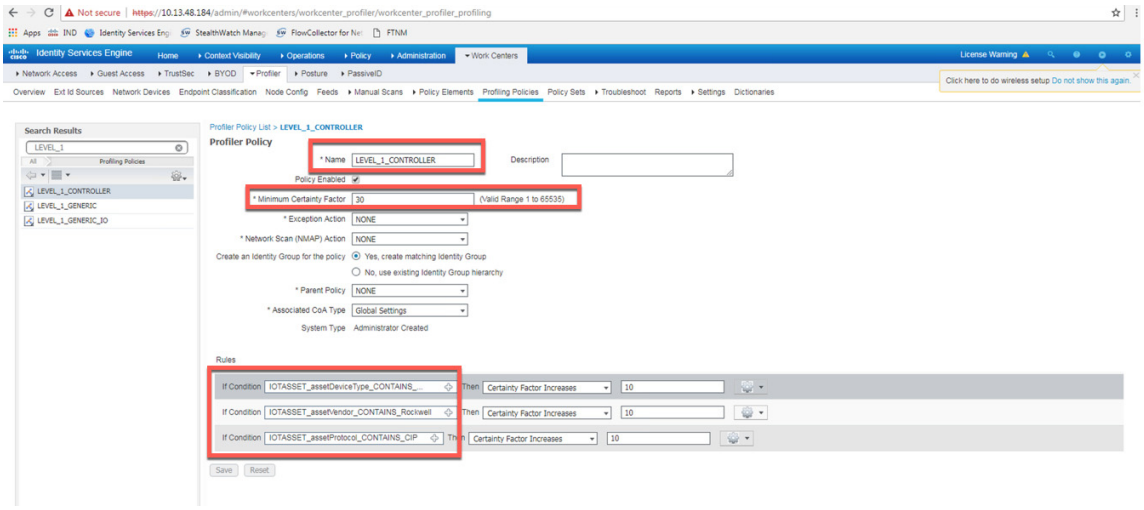
This policy is used to profile an IACS asset which is a controller. The key attributes used to profile this device are shown in Figure 4-15. As shown in Figure 4-15, the IOTASSET dictionary is used to match different conditions like protocol, assetVendor, and assetDeviceType. The values for the attributes assetVendor and assetDeviceType are obtained by ISE via the integration to NMT. When a new IACS asset is discovered by NMT, it provides the details of the asset to Cisco ISE and this information is used to fill in the attribute values of the IOTASSET dictionary.

Figure 4-15 Attributes Used to Profile a Controller



When a match is found for each condition, the certainty of the device matching the profile increases. If a profiling policy matches all three conditions, then the certainty factor goes higher. There is an option to specify the minimum certainty factor. For example, in Figure 4-15, if each condition match gives a certainty factor of 10, then if all three conditions match the certainty factor becomes 30. The profiling policy for the previous example can be made stringent by only allowing a device to be profiled if it gets certainty factor of 30 or it can be made very lenient by classifying it as Level_1_Controller if it matches at least one of the conditions. In this CPwE Network Security CVD DIG, the stringent choice was made when classifying a controller. Figure 4-16 shows the Level_1_controller policy defined in Cisco ISE.

Figure 4-16 Level_1_controller_policy in Cisco ISE



Level_0_IO_policy

The Level_0_IO_policy is used to profile I/O assets, which usually have a role which is very local to the Cell/Area Zone and will rarely have access outside the Cell/Area Zone. Figure 4-17 shows the high level idea for Level_0_IO_policy and Figure 4-18 shows the profiling policy used to profile I/O IACS assets.

Figure 4-17 High Level Attributes for Level_0_policy

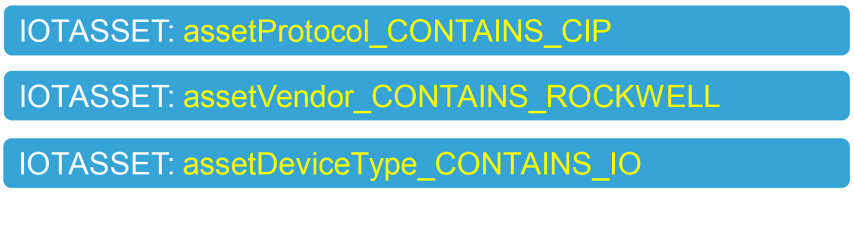
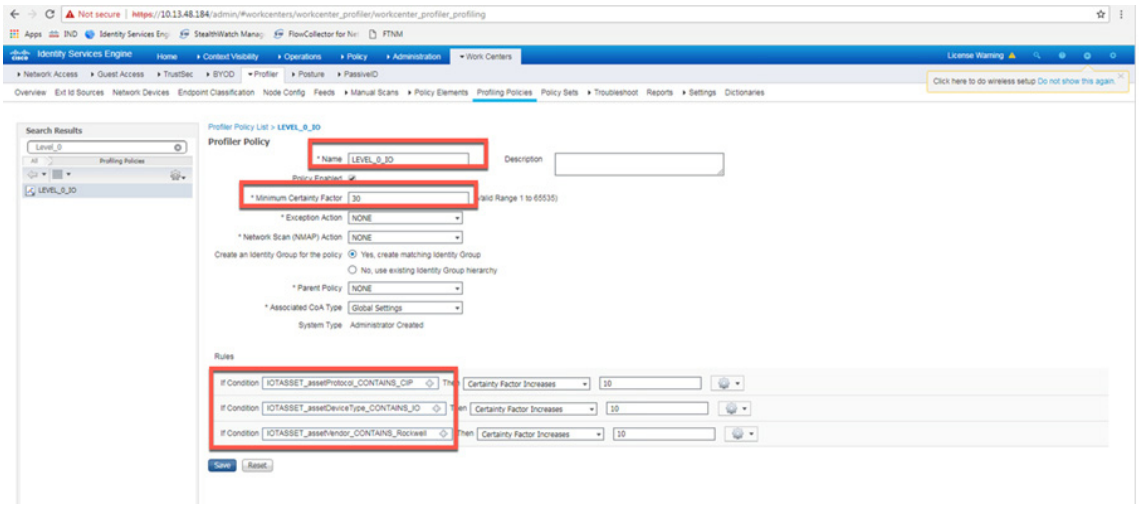


Figure 4-18 Level_0_IO_policy



Custom Attributes

Cisco ISE uses attributes defined in a dictionary to restrict access to IACS assets and other devices. In Figure 4-16 and Figure 4-18, IOTASSET dictionary was used to match attributes that were meant to match IACS assets. In addition, Cisco ISE allows a user to create custom attributes that a user can specify. A combination of pre-defined attributes provided by Cisco ISE along with user attributes allows an IT security architect to create more granular policies. In this CPwE Network Security CVD DIG, two custom attributes—assetGroup and assetTag—were used to create more granular policies. These attributes were sent from NMT to Cisco ISE using the pxGrid API in addition to the normal attributes. Configuring security tags shows how an OT control system engineer can use NMT to define security tags; this tag information is seen in Cisco ISE as assetTag. Figure 4-19 shows how to define custom attributes in Cisco ISE at **(ISE admin web)—> Administrator—>Identity Management—>Settings**.

Figure 4-19 Enabling Custom Attributes in Cisco ISE

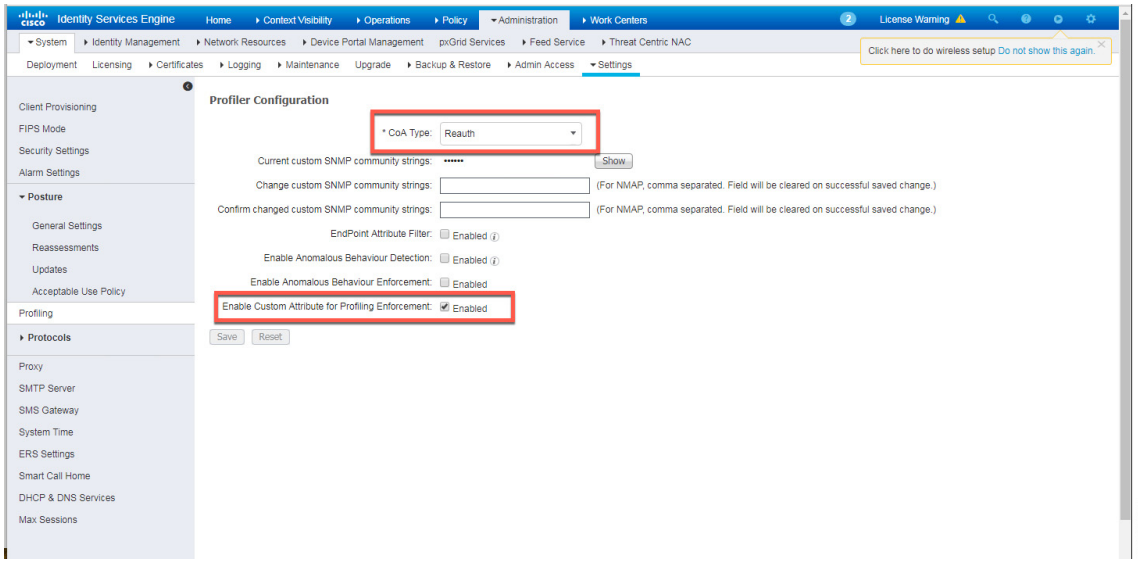
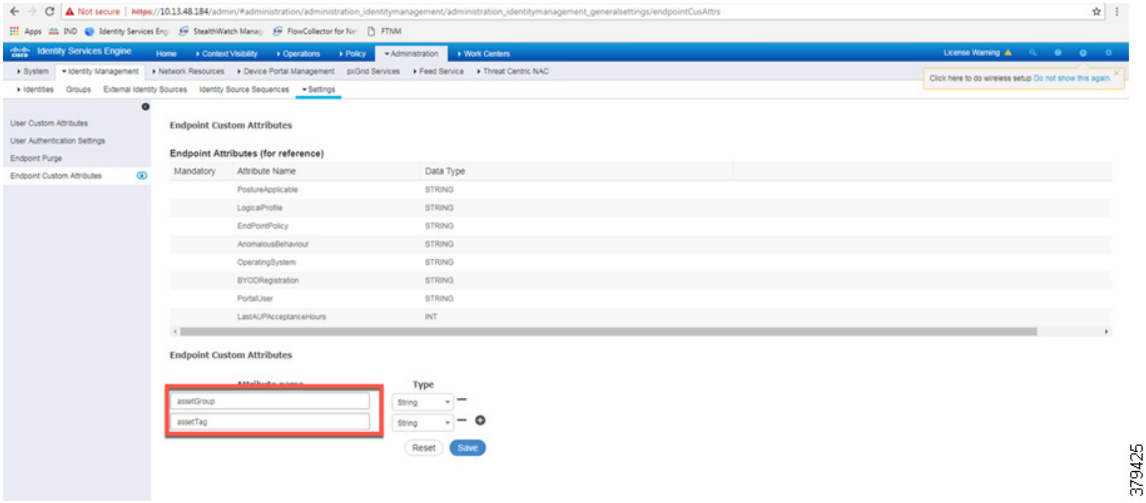


Figure 4-20 shows how to define the custom attributes by going to **(ISE admin web)—> Administration—>Identity Management—>Endpoint Custom Attributes**.

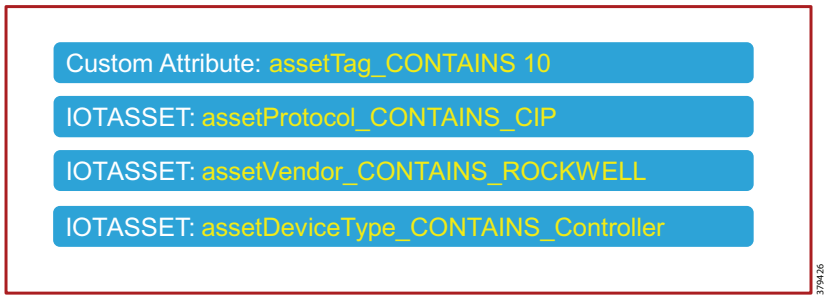
Figure 4-20 Custom Attribute Examples



Level_3_policy

Level_3_policy is used to profile IACS assets that need to access IACS assets across the Cell/Area Zones. For example, a Level_1_Controller in a Cell/Area Zone may need to access another Level_1_Controller in another Cell/Area Zone. This access may not be needed for all the Level_1_Controllers, but only for a few of them. Cisco ISE profiles a device as a Level_1_Controller based on the device attributes defined in the IOTASSET dictionary. There is a need for an additional attribute along with the normal attributes to classify a Level_1_Controller as Level_3. Custom attributes that were discussed in the previous section could be used in conjunction with the device attributes to classify as Level_3. Figure 4-21 shows the general idea of classifying the device as Level_3.

Figure 4-21 Level_3_Policy



The assetTag attribute is a custom attribute that was used in addition to the device attributes such as assetProtocol, assetVendor, and assetDeviceType. The minimum certainty factor now increases to 40 because four attributes used to match an IACS asset as Level_3 and each attribute by default has a certainty factor of 10. To understand how to create an assetTag in NMT, refer to Figure 4-5.

Remote_Access

This profiling access policy is used to classify IACS assets that are given access by a remote user to access the device. As shown in OT Influenced Remote Access—For Example Downtime in Chapter 1, "CPwE Network Security Overview," a remote user connects to a jump box in IDMZ (for best practices, see Appendix A, "References" for links to the CPwE IDMZ CVD DIG), then accesses a remote desktop server in the Industrial Zone, and from this remote desktop server a connection is made to an IACS asset that needs to be accessed. For example, an IACS asset in Cell/Area Zone currently classified as a Level_1_Controller needs to be accessed by the remote desktop server in the Industrial Zone. The current policy is that no IACS asset can be accessed by the remote desktop server unless the IACS asset is classified as Remote_Access. To change a Scalable Group Tag for an IACS asset, a Change of Authorization (CoA) must occur. NMT allows a control system engineer to express operational intent by changing the assetGroup of the IACS asset. Then Cisco ISE would re-profile the IACS asset, issue CoA to the IACS asset, and push a new Scalable Group Tag to the IACS asset. In this CPwE Network Security CVD DIG, assetGroup ='Remote' was defined in NMT as a group where IACS assets that need Remote_Access are placed by the OT control system engineer. Figure 4-22 illustrates the profiling policy used to match Remote_Access.

Note When a new SGT is assigned to an IACS asset, there is a loss of connectivity for a few seconds, during which time no application is able to access the IACS asset.

Figure 4-22 Profiling Access Policy for Remote Access

In this CPwE Network Security CVD DIG, only the custom attribute assetGroup was used to classify the device. As this policy is meant for all IACS assets, only the assetGroup was used to profile the device. The IT security architect can add additional matching conditions, for example, assetDeviceType="Controller" and assetGroup ="Remote".

Configuring TrustSec in Cisco ISE

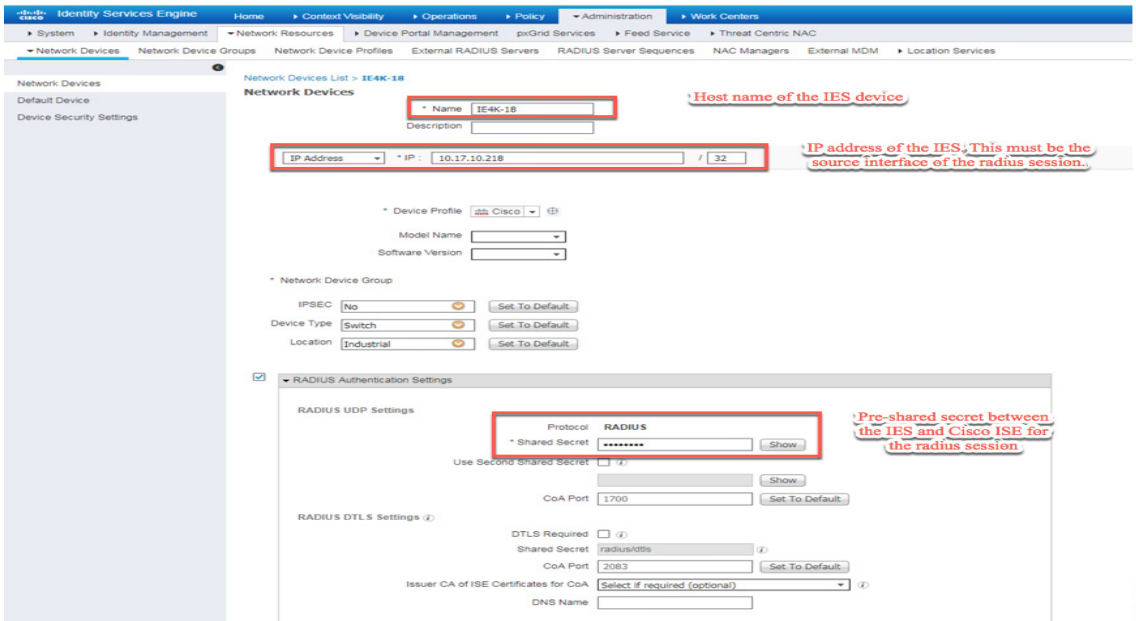
This section provides configuration details for different components that need to be configured on Cisco ISE to support TrustSec in IES and the Cisco Catalyst 3850.

- Adding IES to Cisco ISE
- Adding Scalable Group Tags
- SXP configuration

Adding IES to Cisco ISE

For Cisco ISE to assign Scalable Group Tags to IACS assets, IES details such as IP address and radius pre-shared secret key must be configured on Cisco ISE. Navigate to **(ISE admin web)—>Administration —>Network Devices** to configure the IES details. Figure 4-23 shows the information needed to establish successful radius configuration between an IES and Cisco ISE.

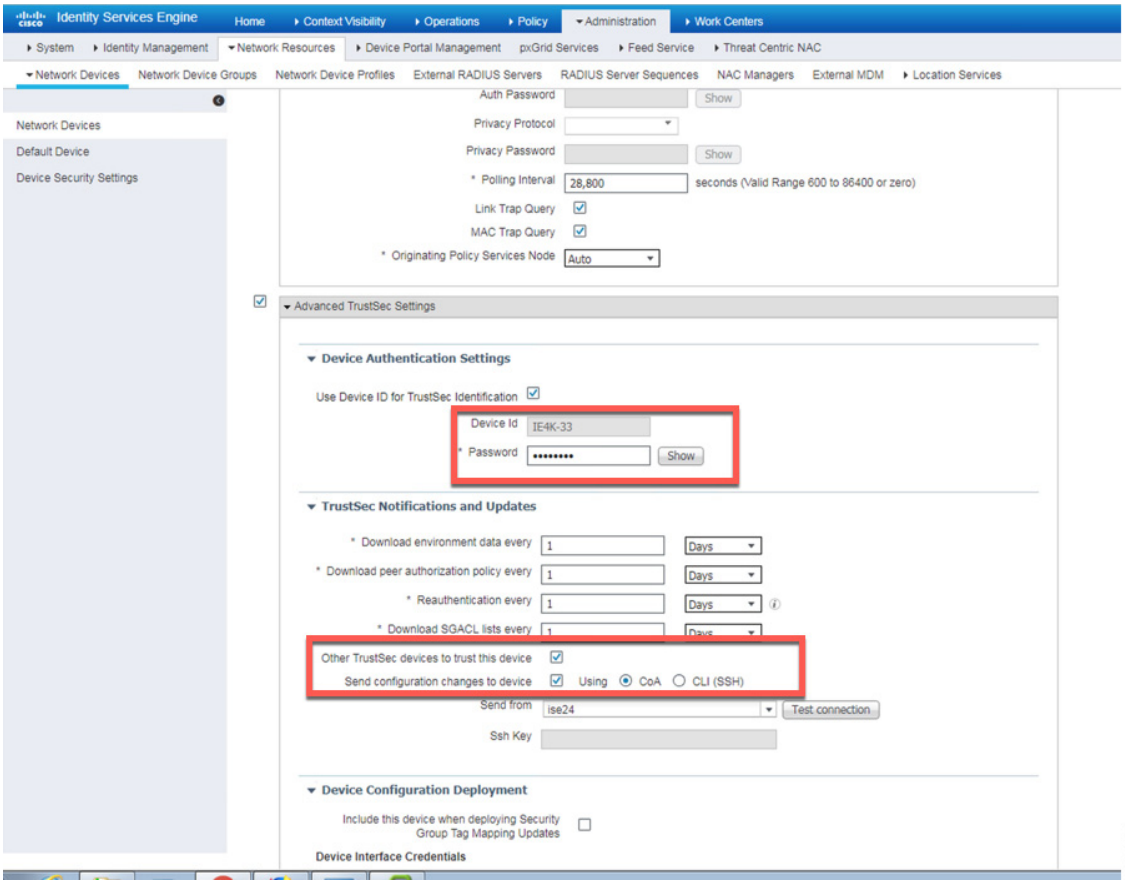
Figure 4-23 IES Radius Configuration



CTS Configuration on Cisco ISE

In the same frame as show in Figure 4-23. the CTS configuration for IES must be configured, as shown in Figure 4-24.

Figure 4-24 CTS Configuration for IES



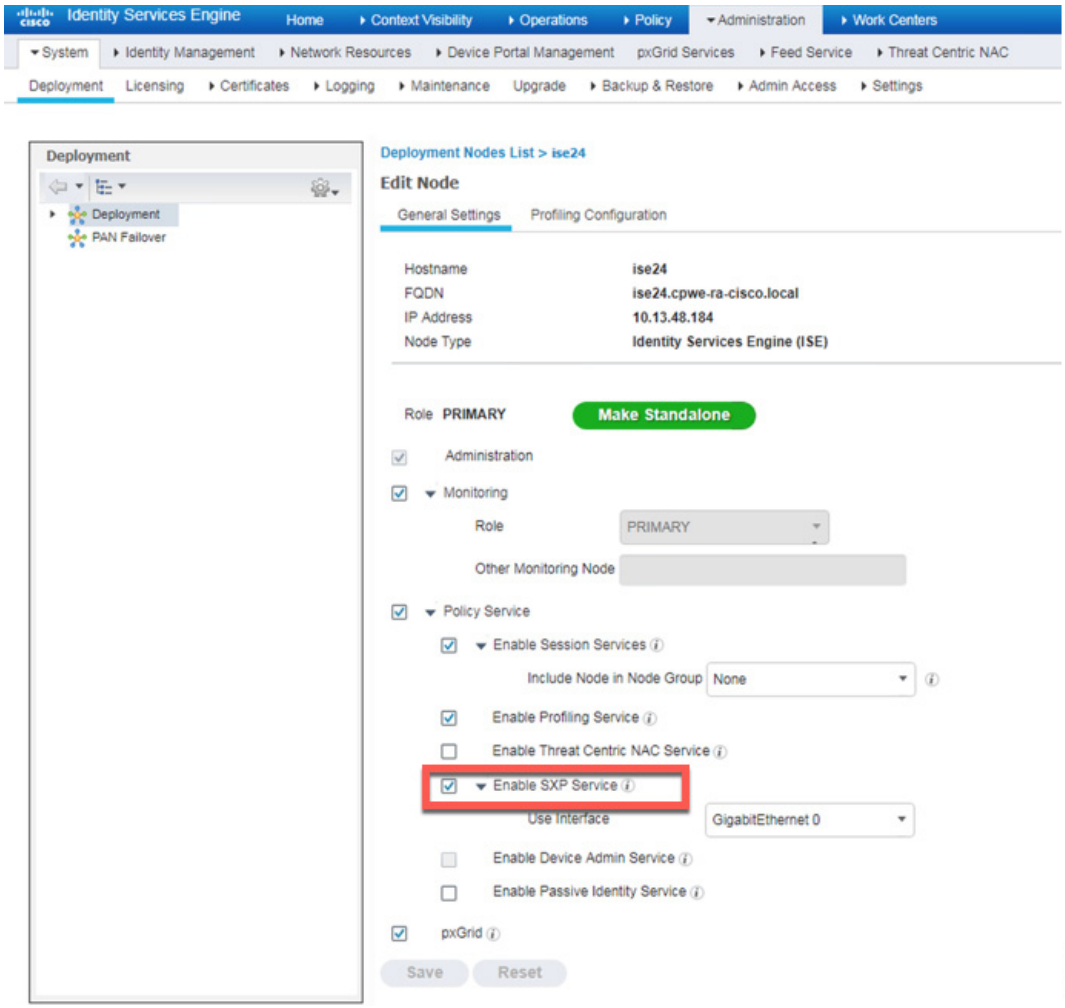
Configuring SXP in Cisco ISE

This section describes on how to enable SXP in Cisco ISE and configure SXP peers in Cisco ISE.

Enabling SXP Service in Cisco ISE

SXP service is enabled in Cisco ISE by going to **(ISE admin web)—>Administration—>Deployment**.

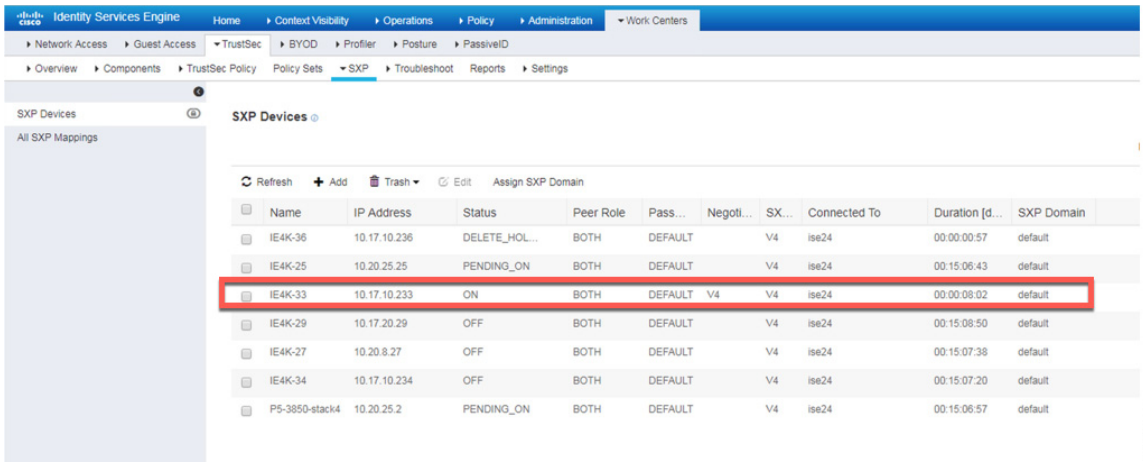
Figure 4-25 Enabling SXP Service in Cisco ISE



Configuring SXP Peers

The IES are configured as Speakers and Cisco ISE is enabled as a Listener. To configure SXP peer, the source and the destination IP addresses must match at the IES and the Cisco ISE. In Cisco ISE, a default configuration template can be used to fill in the rest of the parameters such as password. The location for configuring SXP can be found by going to **(ISE admin web)—>Work Centers—>SXP**.

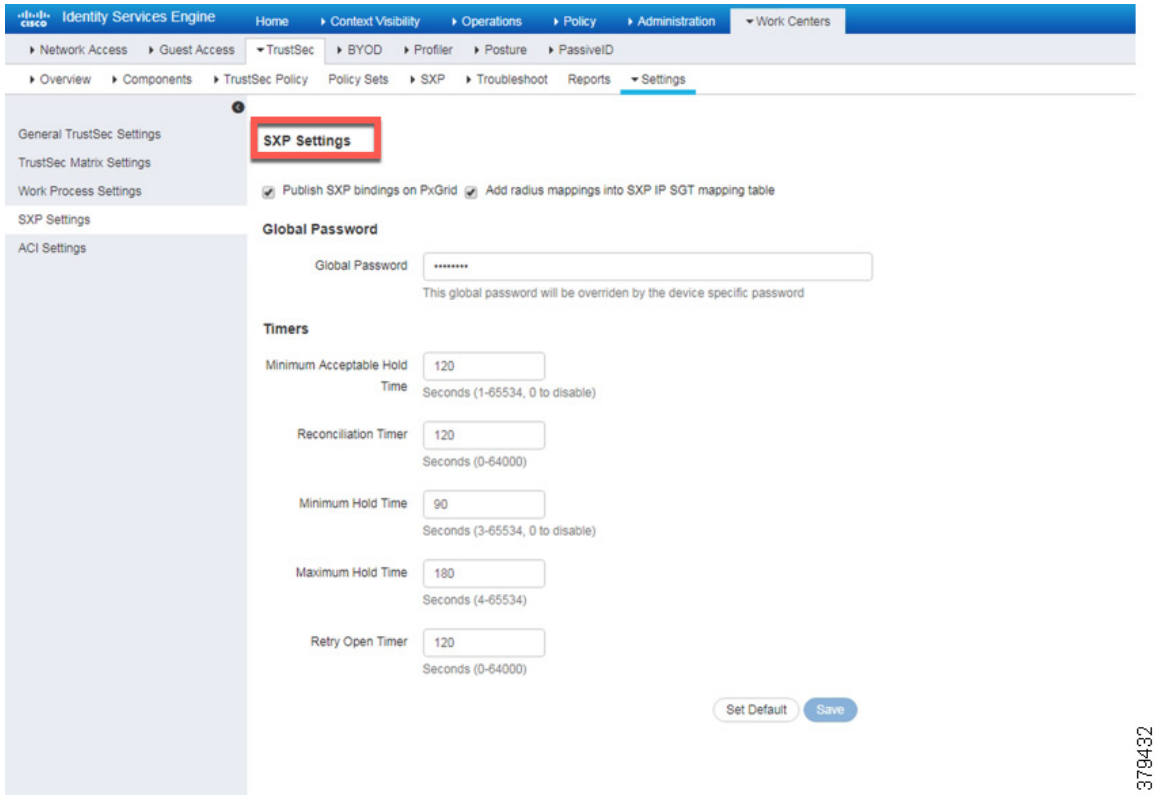
Figure 4-26 Configuring SXP Peers in Cisco ISE



Configuring SXP Default Parameters

The default parameters can be configured at **(ISE admin web)—>Work Centers—>TrustSec—>Settings**.

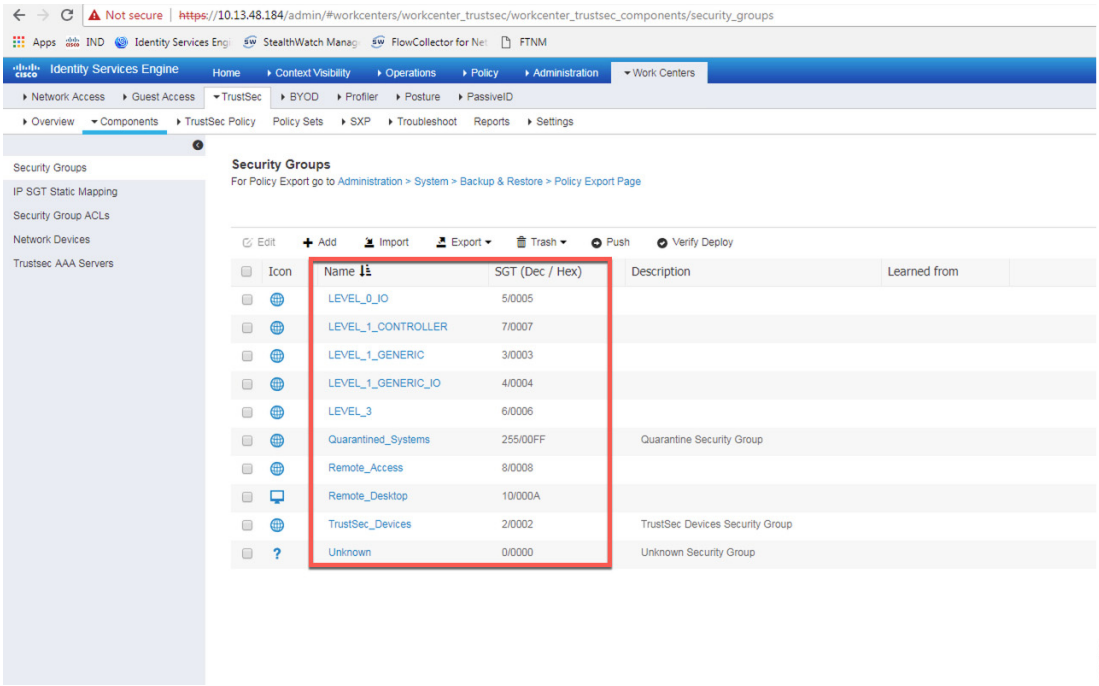
Figure 4-27 Configuring SXP Default Parameters



Configuring SGT Components

IACS assets need to be grouped based on the device function such as controller, IO, HMI, and so on. Each device when it is profiled, authenticated, and authorized has a SGT assigned to the device as an end result. The SGT assignment is done by Cisco ISE and the list of SGTs need to be defined by the IT security architect in Cisco ISE. In this CPwE Network Security CVD DIG, a few device profiles were tested to illustrate how SGT design could be done in a deployment. Creation of User Groups gives an overview on the user groups in a CPwE network architecture. Figure 4-28 shows an example of SGT assignment in Cisco ISE, which is located at **(ISE admin web)—>Work Centers—>TrustSec—>Components**.

Figure 4-28 Configuring SGT Components in Cisco ISE



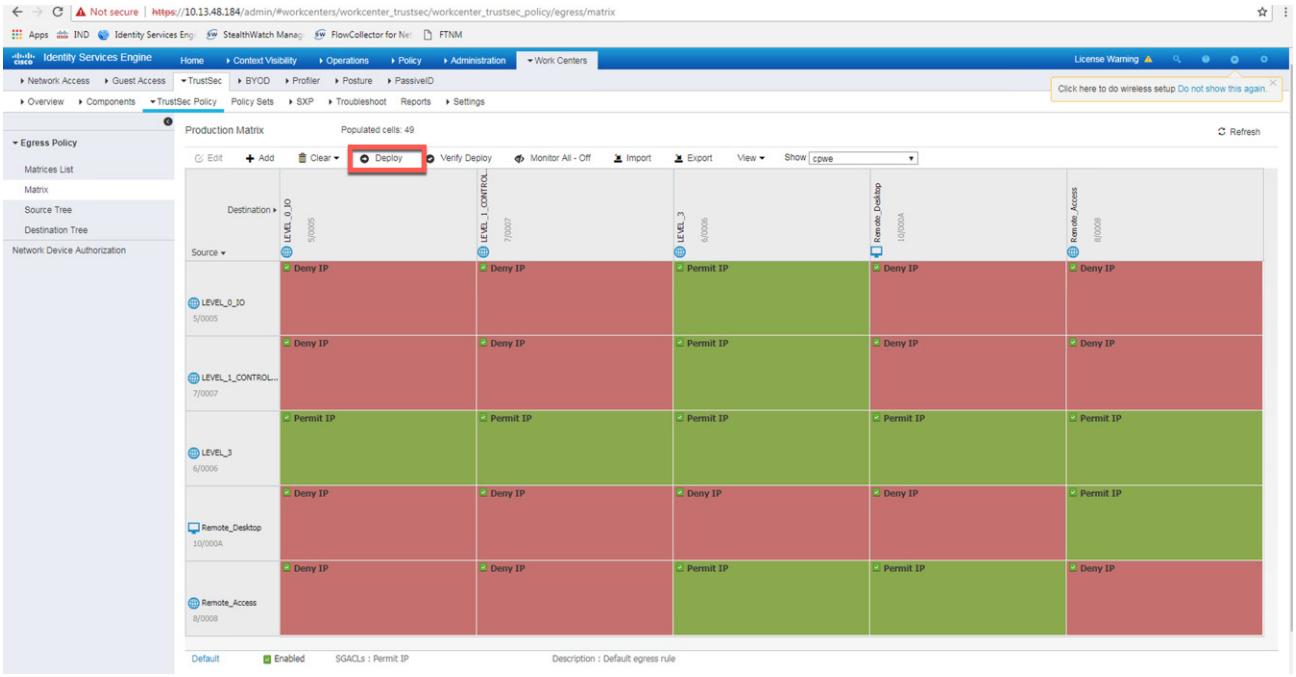
Configuring TrustSec Access Policy Matrix

This section describes how to design a policy matrix for Cisco ISE. Based on the example illustrated in Table 4-2, the following are policy matrix rules:

- IACS assets or any other devices that are assigned with the SGT group of Level_3 are allowed to access all the devices in the plant-wide network.
- IACS assets with SGT value of Level_1_Controller are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with SGT value of Level_0_Controller are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with Remote_Access are allowed to communicate with another device assigned with SGT value of Remote_Desktop and Level_3 (because Level_3 has access to all the devices).

Figure 4-29 shows the TrustSec Access Policy Matrix.

Figure 4-29 TrustSec Access Policy Matrix



As shown in Figure 4-29, Level_3 Controller is allowed to communication with the all the IACS assets, however Level_1_Controller and Level_0_IO can only communicate if they are present in the same Cell/Area Zone. After defining the TrustSec Policy in the ISE, it is downloaded to all IES and the distribution switch (Cisco Catalyst 3850) by selecting the "Deploy" option, as shown in Figure 4-29. The TrustSec policy matrix can become larger and it may be difficult to view the entire policy on a single screen. To prevent that problem, an option exists to filter the view that will display the matrix that has desired SGTs only. The Show box on top of the screen will enable that functionality and requires the user to create a custom view.

Authentication Policy

802.1X authentication policy involves three parties:

- The supplicant—A client device that wishes to attach to the network.
- The authenticator—A networking device that accepts authentication requests from the client and sends them to the RADIUS authentication server.
- The authentication server—One that validates a client's identity and sends back the success or failure RADIUS message.

In this CPwE Network Security CVD DIG, the supplicant is the IACS asset, the authenticator is the IES, and the authentication server is ISE.

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the IACS assets and the identity sources to be used for authentication. Cisco ISE evaluates the conditions and, based on whether the result is true or false, applies the configured result. The authentication protocol tested in this CPwE Network Security CVD DIG is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine what kind of network access to provide. This protocol is used to authenticate end devices that do not support any supplicant software in them, such as 802.1X EAP-TLS, EAP-FAST, and

so on. For more information about MAB, see: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

The authentication policy used in the Cisco ISE for this CPwE Network Security CVD DIG checks the protocol and the Identity Store as Internal Endpoints. To configure the authentication policy, navigate to **(ISE admin web)—>Policy—>Policy Sets—>Default** as shown in Figure 4-30, and select the arrow on the right to configure the authentication policy, as shown in Figure 4-31.

Note In the example shown in Figure 4-31, the default authentication policy set was used. In case the real deployment has a different authentication policy set, then the IT Security Architect must select the correct authentication policy set.

Figure 4-30 Navigation to Configure Authentication/Authorization Policy

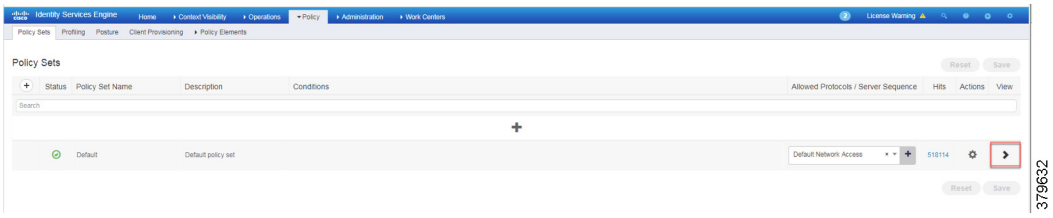
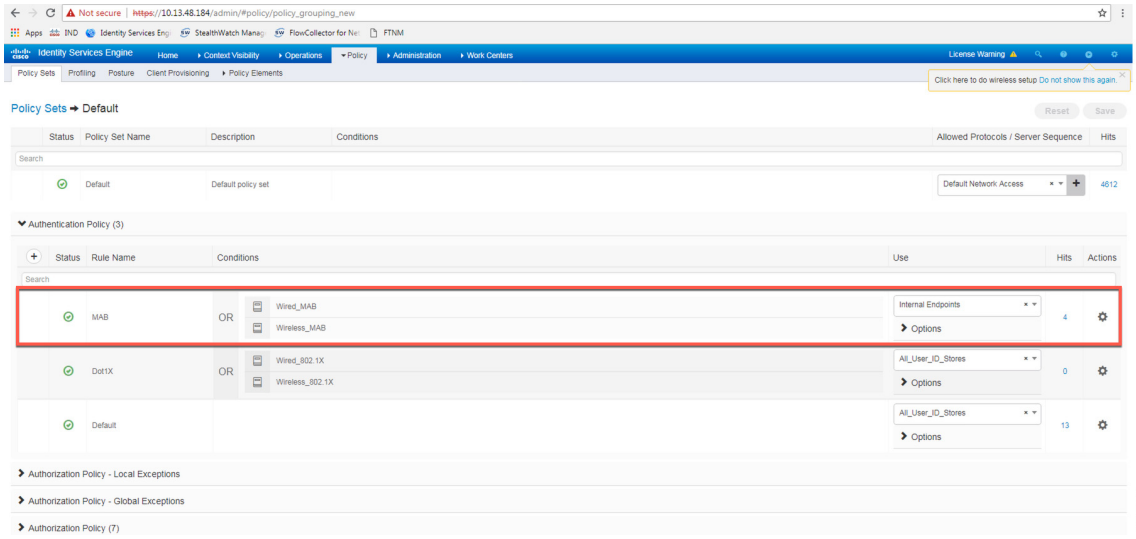


Figure 4-31 ISE Authentication Policy

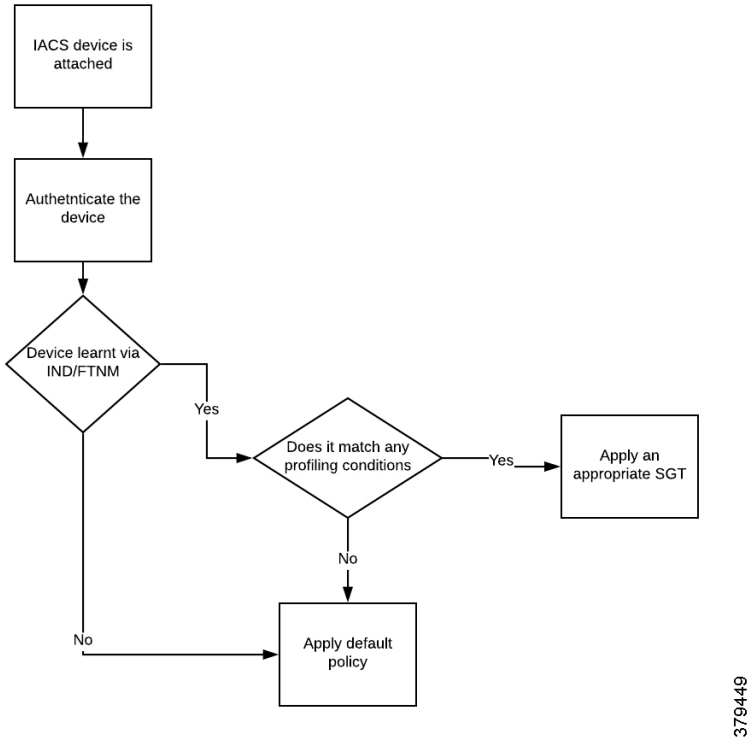


Authorization Policies

Authorization policies are critical to determine what the user is allowed to access within the network. Authorization policies are composed of authorization rules and can contain conditional requirements that combine one or more identity groups. The permissions granted to the user are defined in authorization profiles, which act as containers for specific permissions.

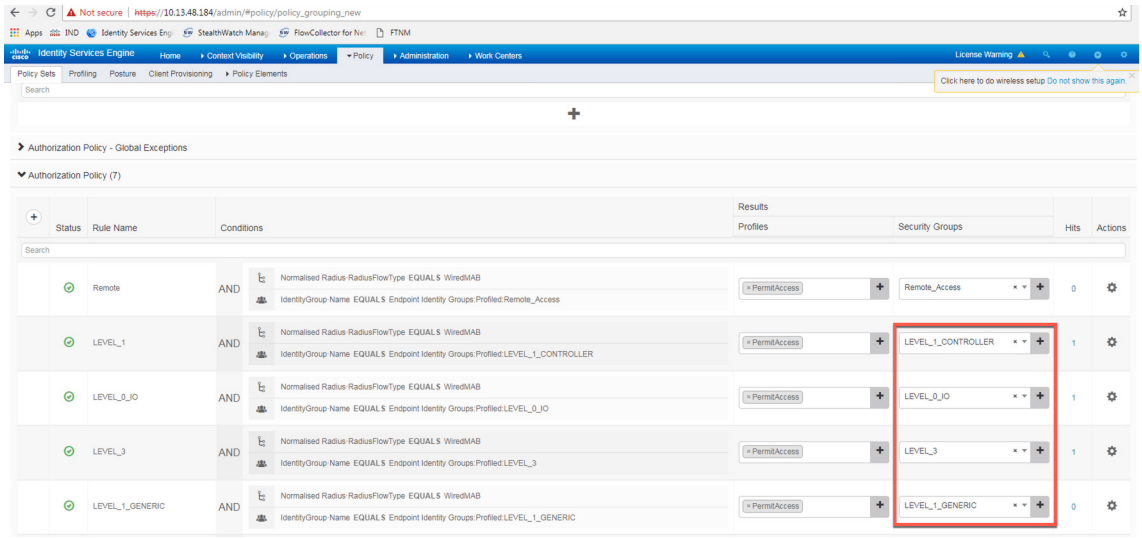
Authorization profiles group the specific permissions granted to a user or a device and can include attributes such as an associated VLAN, ACL, or a SGT. This CPwE Network Security CVD DIG uses SGT to grant permissions to an IACS asset. Configuring TrustSec Access Policy Matrix describes how the Policy Matrix was designed in the CPwE Network Security CVD DIG. When an IACS asset is authenticated and as part of the authorization policy, an appropriate SGT is assigned to the IACS asset. The TrustSec Policy Matrix determines the permissions associated with each IACS asset. Figure 4-32 shows the high-level steps when an IACS asset is connected to the network. To configure the authorization policy navigate to **(ISE admin web)—>Policy—>Policy Sets—>Default** and then select **Authorization Policy**.

Figure 4-32 AAA for an IACS Asset



The default policy can be designed based on how stringent the requirement is. One option is to assign a default SGT like LEVEL_GENERIC and classify devices that do not meet any of the authorization policy conditions. Or there could be a stringent design where, if an IACS asset is not being profiled by any of the existing conditions, then deny access to the network for that IACS asset. Figure 4-33 shows the authorization table for this CPwE Network Security CVD DIG.

Figure 4-33 Authorization Policy Conditions



Configuring IES

This section provides the configuration details for the IES in a CPwE network architecture. The configuration of key features deployed in the IES, such as TrustSec, NetFlow, and Radius server, are described below.

Configuring RADIUS AAA

Each IES must be configured to communicate with the Cisco ISE AAA server for authorizing IoT devices, users, and other systems. The AAA server shown in this configuration is pointing to the PSN node. The following configurations are performed via the command line interface (CLI) of the device.

Step 1 Enter configuration mode. At the global level specify the interface that has the IP address configured in Cisco ISE that will be used to source authentication requests. Enable AAA.

```
aaa new-model
!
!
aaa group server radius ISE
 server name ISE
!
aaa authentication login no-auth none
aaa authentication dot1x default group ISE
aaa authorization network cts-list group ISE
aaa authorization auth-proxy default group ISE
aaa accounting dot1x default start-stop group ISE
aaa session-id common
```

Step 2 Configure Change of Authorization (CoA):

```
aaa server radius dynamic-author
client <PSN_IP_ADDRESS> server-key 7 <SHARED_KEY>
!
```

Note This configuration done on the IES device must match the configuration done on Cisco ISE. Refer to Figure 4-23.

Step 3 Configure the radius server for TrustSec. In this CPwE Network Security CVD DIG, the name for the list is cts_list and this name should be tied to the `aaa authorization network` command shown in Step 1:

```
cts authorization list cts-list
!
```

Step 4 Configure the following RADIUS server attributes:

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
!
```

Step 5 Configure the RADIUS server, IP address, and shared secret that was entered in Cisco ISE:

```
radius server ISE
address ipv4 <PSN_IP_ADDRESS> auth-port 1812 acct-port 1813 pac key 7 <PAC_KEY>
!
```

Note This configuration done on the IES device must match the configuration done on Cisco ISE. Refer to Figure 4-24.

Step 6 Configure the AAA group name for RADIUS and specify the server created in step 5:

```
aaa group server radius ISE
 server name ISE
!
```

Step 7 Globally enable port-based authentication:

```
dot1x system-auth-control
!
```

Configuring Port-based Authentication

On the IES, the following configurations enable port-based authentication. Configure each interface that will have an endpoint device connected. For MAB and Dot1x methods to co-exist and function as expected, the order and priority must be properly specified as referenced in this application note:

Configuring MAB
http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

Add the following configuration to the interfaces where the IACS assets could be attached. In this CPwE Network Security CVD DIG, authentication open was applied to the port to ensure that the device remains connected even if for some reason the port is unable to authenticate to the RADIUS server. The default behavior of the port-based authentication is to block access to the network. By enabling authentication open, the port is not shut down and the IACS asset is able to communicate in the network by using the IP address assigned to it.

```
!
interface GigabitEthernet1/10
 description Connected to a Controller
```

```
 switchport access vlan 101
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
!
```

Configuring SDM Templates on IES

SDM templates will allow an OT control system engineer to prioritize resources for different features enabled on an IES. In this CPwE Network Security CVD DIG, the routing template is required to support SGT assignment on IES. To enable SDM mode to be “routing”, the following steps must be completed:

```
sdm prefer routing
```

After entering the command, the IES must be rebooted.

Configuring CTS Credentials on the IES

Specify the Cisco TrustSec device ID and password for the switch to use when authenticating with Cisco ISE and establishing the PAC file. This password and ID must match the Cisco ISE Network Devices configuration specified earlier in Figure 4-24.

```
switch# cts credentials id {switch ID} password {password}
```

Configuring SXP Tunnel on an IES

The SXP tunnel between Cisco ISE and an IES must be established because the SGT binding information (SGT value -IP address) should be sent to Cisco ISE, which would push this information to the enforcement point (Cisco Catalyst 3850). The following is the configuration of the SXP tunnel on the IES:

```
cts sxp enable
cts sxp default password 7 03070A180500701E1D
cts sxp connection peer 10.13.48.184 source 10.17.10.233 password default mode local
speaker hold-time 0
```

Configuring NetFlow on IES

Enabling NetFlow on an IES has three components: a Flow Record, a Flow Exporter, and a Flow Monitor. After all three components (explained below) have been configured, the Flow Monitor is applied to a physical interface.

Flow Record

A Flow Record defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. Custom flow records specify a series of match and collect commands that tell the Cisco device which fields to include in the outgoing NetFlow record.

The match fields are the key fields, meaning that they are used to determine the uniqueness of the flow. The collect fields are extra information that is included in the record in order to provide more detail to the collector for reporting and analysis. When a Flow Record is defined, all of the flow data traffic that enters (ingress) or leaves (egress) the device is captured.

In configuration mode, create ingress or egress flow records using the appropriate interface direction commands. In this CPwE Network Security CVD DIG, traffic was captured on the ingress interface of the IES to capture the traffic generated by the IACS assets.

This configuration includes required as well as optional flow record fields needed by Stealthwatch.

Step 1 Create Ingress Record, which in this CPwE Network Security CVD DIG is called a StealthWatch_Record:

```
flow record StealthWatch_Record
 description NetFlow record format to send to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect interface input
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

Note When the IES Device Manager was used to configure NetFlow on the ports by using the Stealthwatch template, then the *command collect counter packets long* was not applied to the IES device, and without this command, the Stealthwatch management console was not able to detect any flows coming from the IES device. To mitigate this behavior, the command *collect counter packets long* must be applied using CLI. If the IES CLI is used to configure NetFlow on the IES device, then the above mentioned configuration will work. This problem happens only when the Device Manager was used co configure NetFlow on the IES device.

Flow Exporter

The Flow Exporter defines where and how to send the NetFlow (Flow Records). In actuality a Flow Exporter defines a flow collector IP address and port as the destination and in this case the Stealthwatch Flow Collector is the destination.

```
flow exporter StealthWatch_Exporter
 description StealthWatch Flow Exporter
 destination 10.13.48.183
 source Vlan101
 output-features
 transport udp 2055
```

```
 option application-table
!
```

Flow Monitor

A Flow Monitor describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links together the Flow Record and the Flow Exporter. The Flow Monitor includes various cache characteristics such as the timers for exporting, the size of the cache, and, if required, the packet sampling rate (Sampled NetFlow/sFlow). As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and standard CIP I/O connections). There are timers to determine if a flow is inactive or if a flow is long lived. The times used in CPwE Network Security CVD are 30 seconds for inactive time out and 60 seconds for active time out.

Step 2 Create the Ingress flow monitor using the record and exporter created previously:

```
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
```

Step 3 Once the flow monitor has been created, it can be applied to all the access interfaces in an IES. Apply the flow monitor to an appropriate interface and the appropriate ingress/egress using input/output:

```
!
interface GigabitEthernet1/10
 description Connected to a Controller
 switchport access vlan 101
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
```

Note The IP flow monitor policy can be applied both in ingress and egress directions.

```
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
end
```

Configuring Distribution Switch—Cisco Catalyst 3850

As described in Segmentation—TrustSec in Chapter 3, "CPwE Network Security Design Considerations," the enforcement is moved to the distribution switch, no enforcement occurs in the Cell/Area Zone, and the East-West traffic flow, as explained in Traffic Flows in a Network in Chapter 3, "CPwE Network Security Design Considerations," is enforced at the distribution switch. This section describes the steps that need to be configured on the distribution switch to enable enforcement:

Configuring Radius Server

This is very similar to the configuration of IES, so refer to Configuring RADIUS AAA.

Configuring TrustSec

The configuration of TrustSec has the following components:

- Configuring cts
- Configuring sxp
- Configuring IPDT
- Configuring enforcement

Configuring cts

The cts configuration is similar to the IES, so refer to Configuring CTS Credentials on the IES.

Configuring sxp

SXP configuration on the distribution switch is similar to the IES, so refer to Configuring SXP Tunnel on an IES.

Configuring IPDT

There is a change in the way Cisco Catalyst 3850 platforms are configured with device-tracking compared to the IES. In the Cisco Catalyst 3850, the device-tracking feature must be enabled, a device-tracking policy must be created, and this policy must be attached to the interface where the IP device-tracking needs to be enabled. In this CPwE Network Security CVD DIG, IP device-tracking is enabled on interfaces (Port-channel3) that are attached to IES interfaces.

```
device-tracking tracking
!
device-tracking policy IPDT
 no protocol udp
 tracking enable
!
interface Port-channel3
 switchport trunk native vlan 101
 switchport trunk allowed vlan 101,102
 switchport mode trunk
 device-tracking attach-policy IPDT
end
```

```
P5-3850-stack-4#
```

Enforcement

In this CPwE Network Security CVD DIG, policy enforcement is done only on the Cisco Catalyst 3850 switch. To enable policy enforcement, the following commands must be enabled:

```
cts role-based enforcement
cts role-based enforcement vlan-list <vlan-id>
```

CHAPTER 5

Implementation of Use Cases

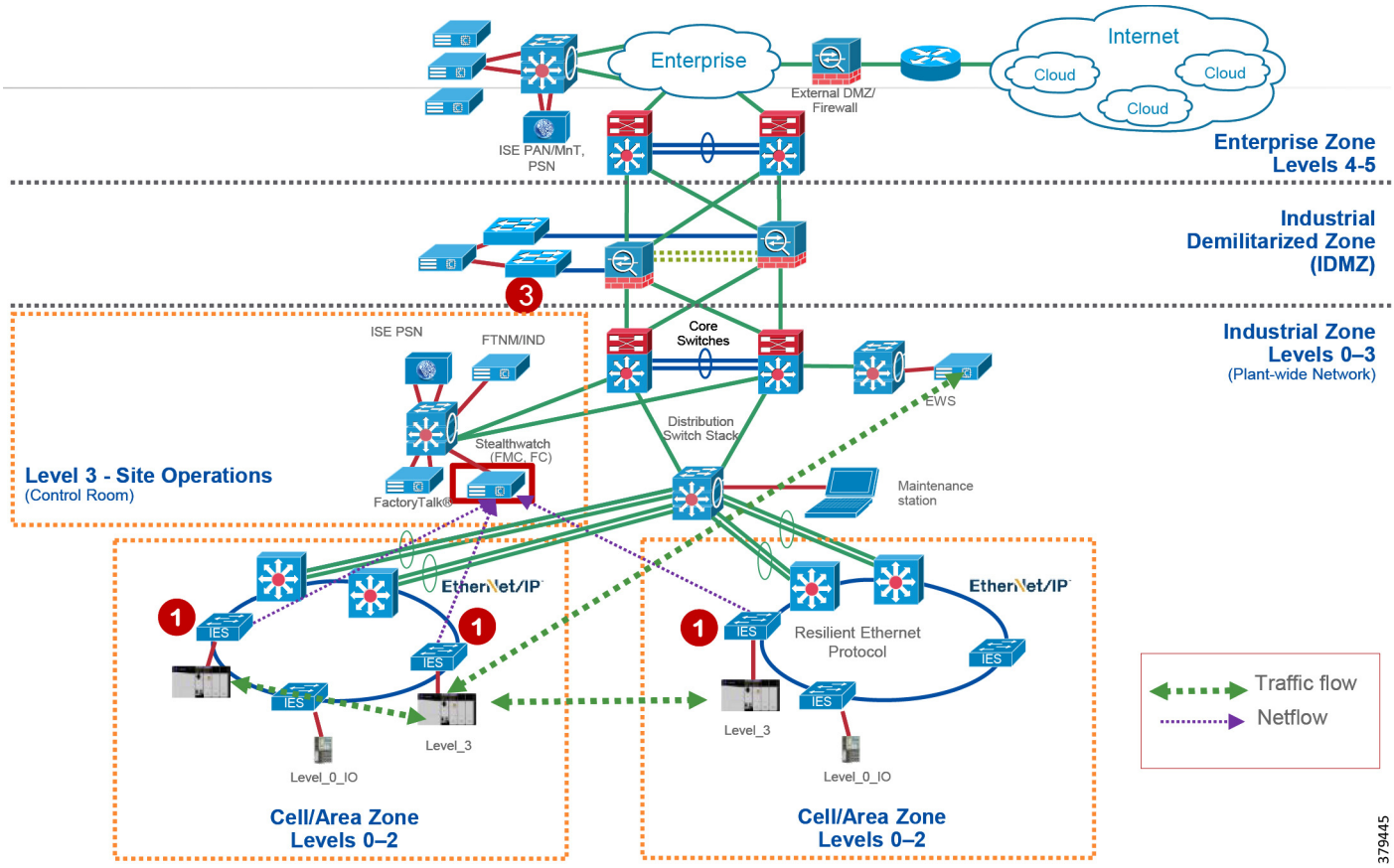
This section describes the implementation of the Network Security use cases documented in this CPwE Network Security CVD DIG. The objective is to provide more details about each of the following use cases and also how different components, such as IES, ISE, NMT, and Stealthwatch work together to support these use cases. This section describes the following use cases:

- Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone
- Security Group Policy Assignment of IACS Assets in Industrial Zone
- Network Detection of Network Devices and IACS Assets
- Malware Detection of Flows in Cell/Area Zone and Level-3 Site Operations
- OT Managed Remote User (Employee or Partner) Accessing from (Enterprise or Internet) to a Network Device or an IACS Asset

Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone

The purpose of this use case is to show how an OT control system engineer and IT security architect can work together to gain visibility of the network devices and IACS assets in the Cell/Area Zone. As explained in Segmentation—High Level in Chapter 3, "CPwE Network Security Design Considerations," to segment traffic flows going across in East-West or North-South direction it is important that the IT security architect gain visibility of the current network topology in the plant-wide network. The visibility must be granular enough that the IT security architect can know the type of the IACS asset—Controller, I/O, drive, HMI, and others. Figure 5-1 illustrates the high-level steps to perform this use case.

Figure 5-1 Visibility and Identification of Network Devices and IACS Assets in the Cell/Area Zone

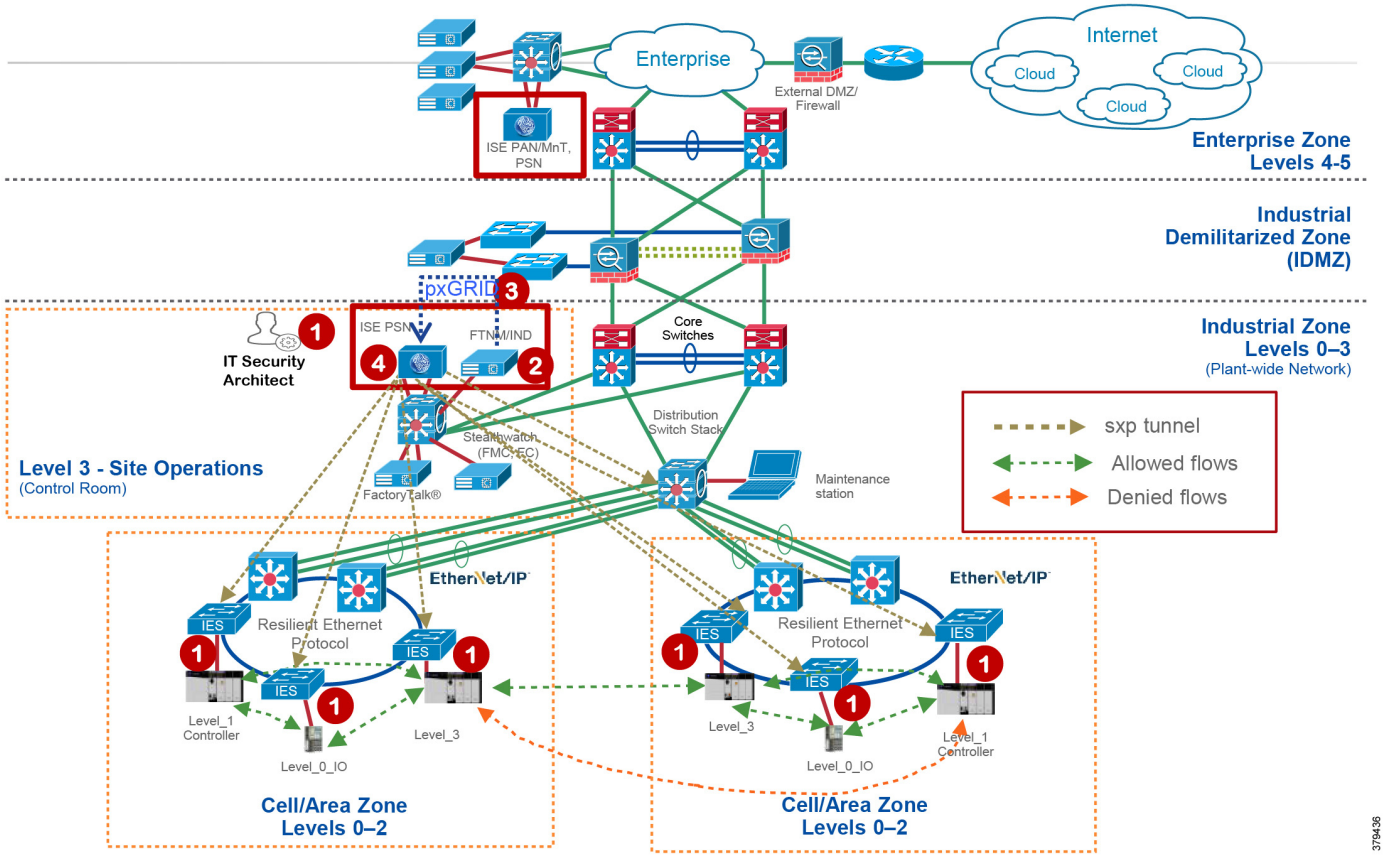


1. An OT control system engineer defines the IACS Asset Discovery profiles for IACS assets and the networking devices in NMT. Refer to Creating Asset Discovery Profile in Chapter 4, “Configuring the Infrastructure.”
2. OT control system engineer scans the IACS assets and the networking devices and verifies that the IACS assets and networking devices are grouped in Asset Inventory section of NMT. Refer to Asset Inventory in Chapter 4, “Configuring the Infrastructure.”
3. The IT security architect configures the pxGrid between NMT and ISE. Refer to Configuring pxGrid between Cisco ISE and NMT in Chapter 4, “Configuring the Infrastructure.”
4. IT security architect configures profiling policies in ISE to profile the IACS assets based on the attributes provided by NMT. Refer to Profiling in Cisco ISE in Chapter 4, “Configuring the Infrastructure.”
5. ISE is able to identify Level_1_Controller in a Cell/Area Zone. Refer to Level_1_controller Policy in Chapter 4, “Configuring the Infrastructure.”
6. ISE is able to identify Level_0_IO in a Cell/Area Zone. Refer to Level_0_IO_policy in Chapter 4, “Configuring the Infrastructure.”
7. ISE is able to identify Level_3 in a Cell/Area Zone. Refer to Level_3_policy in Chapter 4, “Configuring the Infrastructure.”

Security Group Policy Assignment of IACS Assets in Industrial Zone

This use case describes in detail about how to achieve segmentation of different traffic flows in a Cell/Area Zone. To understand traffic flows, refer to Traffic Flows in a Network in Chapter 3, "CPwE Network Security Design Considerations." The idea behind segmentation is defined in Segmentation—High Level in Chapter 3, "CPwE Network Security Design Considerations." Figure 5-2 provides the steps that an IT security architect needs to perform to achieve segmentation of different traffic flows.

Figure 5-2 Segmentation of Traffic Flows in Cell/Area Zone



1. The IT security architect must configure port-based authentication on all the IES. Refer to Configuring Port-based Authentication in Chapter 4, "Configuring the Infrastructure."
2. The IT security architect must configure TrustSec SGTs for different IACS assets - Level_1_Controller, Level_0_IO, and Level_3 in ISE. Refer to Configuring SGT Components in Chapter 4, "Configuring the Infrastructure."
3. The IT security architect must configure Authentication and Authorization policy in ISE. Refer to Authentication Policy and Authorization Policies in Chapter 4, "Configuring the Infrastructure."
4. The IT security architect must configure SXP tunnels from IES and the distribution switch to ISE. Refer to Configuring SXP Tunnel on an IES in Chapter 4, "Configuring the Infrastructure."
5. The IT security architect must configure the TrustSec Policy Matrix on ISE. Refer to Configuring TrustSec Access Policy Matrix in Chapter 4, "Configuring the Infrastructure."

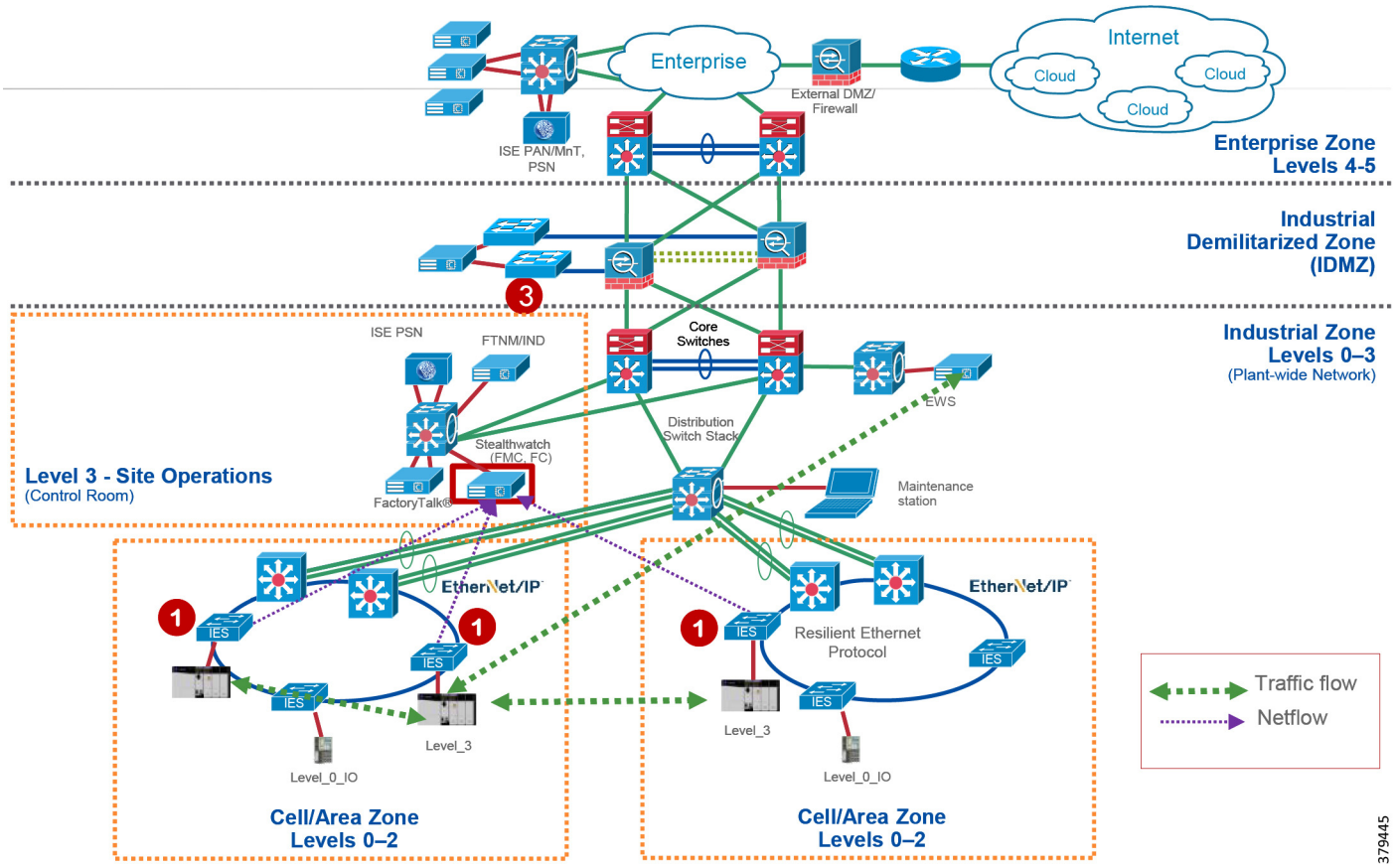
6. The IT security architect must configure the enforcement on the Cisco Catalyst 3850 distribution switch. Refer to Configuring Distribution Switch—Cisco Catalyst 3850 in Chapter 4, "Configuring the Infrastructure."

Network Detection of Network Devices and IACS Assets

This use case describes how an IT security architect can use Stealthwatch along with NetFlow enabled on IES and Cisco Catalyst 3850 to monitor the network flows in the plant-wide network. To detect traffic flows occurring in a plant-wide network, it is important that NetFlow is enabled on all the networking devices to capture the traffic flows that are sent to FlowCollector. Stealthwatch Management Console (SMC) retrieves the flow data from the FlowCollector and runs pre-built algorithms to display the network flows and also detect and warn if there is any malicious or abnormal behavior occurring in the network. In this CPwE Network Security CVD, three flows are shown to demonstrate the capability of Stealthwatch using NetFlow:

- Traffic between IACS assets in a Cell/Area Zone (Intra-Cell/Area Zone).
- Traffic between Level_3 IACS assets across the Cell/Area Zone (East-West or Inter-Cell/Area Zonel traffic).
- Traffic between the EWS server and a Level_3 IACS asset (North-South) traffic.

Figure 5-3 Network Flow Detection in Plant-wide Network



The following steps must be performed by the IT security architect to detect the above-mentioned flows:

1. IT security architect must enable NetFlow on all the IES and the Cisco Catalyst 3850 switches. Refer to Configuring NetFlow on IES in Chapter 4, "Configuring the Infrastructure."
2. IT security architect must use the host group feature in Stealthwatch to focus on certain flows if needed. A host group is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology. By grouping hosts into host groups, you can control how the Stealthwatch Flow Collectors monitor and respond to the behavior of those hosts as a group, rather than individually.

   To monitor specific application traffic such as CIP, the IT security architect must configure host groups based on subnets associated with the IACS assets and then create an appropriate filter to monitor CIP traffic. Example attributes for EtherNet/IP traffic would be TCP 44818 for CIP class 3 explicit traffic and UDP 2222 for CIP class 1 implicit I/O traffic.

   To configure host groups refer to https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf

Note Although Cisco Catalyst 6800 and 4500X core switches support NetFlow, the CPwE Network Security CVD was only tested and validated with NetFlow enabled on the IES and Catalyst 3850. Cisco and Rockwell Automation recommend that NetFlow be enabled throughout the plant-wide architecture.

Malware Detection of Flows in Cell/Area Zone and Level-3 Site Operations

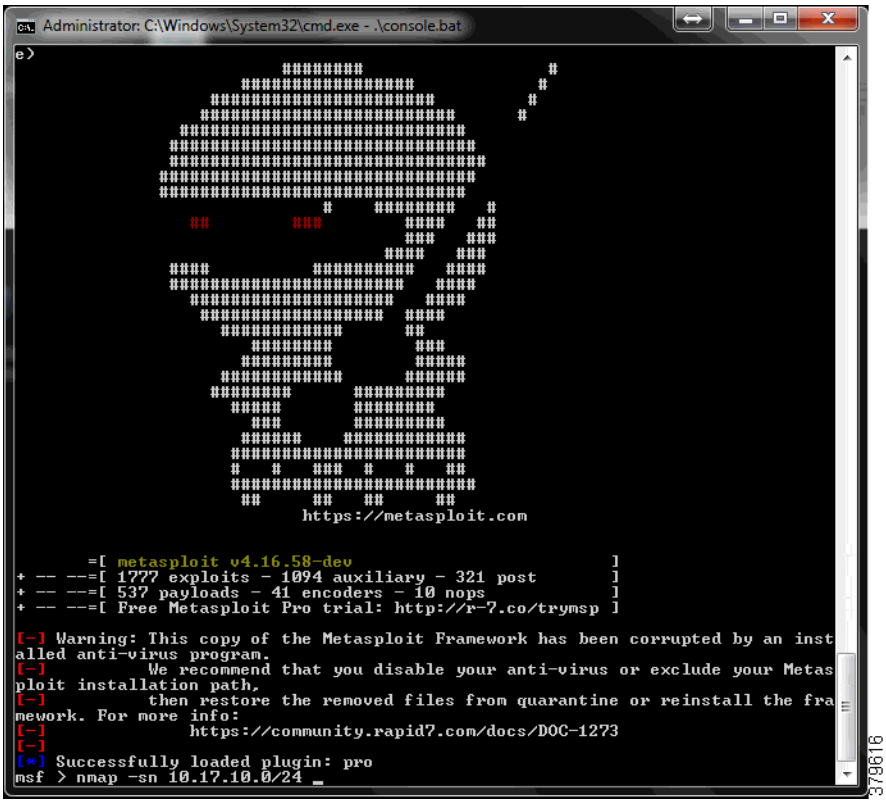
This section discusses how Stealthwatch using NetFlow data collected by the FlowCollector detects malware flows occurring in a plant-wide network. When malware is spreading in the network, it becomes very difficult to pinpoint where the malware propagation is occurring. An IT security architect needs to identify the source of the problem and then develop a remediation plan to address the problem. Stealthwatch has many inbuilt machine learning algorithms that can assist an IT security professional in detecting possible malware propagation in the network. Stealthwatch can detect any abnormal behavior occurring in the network and can also provide the IP address of the device that is causing the propagation. This information greatly simplifies the detection process.

Without Stealthwatch implemented in the network, the normal operation done by the IT security architect is to perform a number of steps that may involve many time-consuming operations, such as shutting down parts of the network, going through logs of many devices, checking the DNS log, and enabling debugs on many other devices to isolate the problem. All these steps not only take time to isolate, but also increase the risk of other vulnerable devices becoming infected. When active malware is detected, then quickly formulating a remediation plan is essential in building a defense against malware.

The malware behavior is to immediately scan the network to identify any other vulnerable devices in the plant-wide network. In this CPwE Network Security CVD, two traffic flows related to malware are discussed:

- An infected laptop attached to an IES. Figure 5-4 shows an example of how a scan can be performed by an infected laptop.

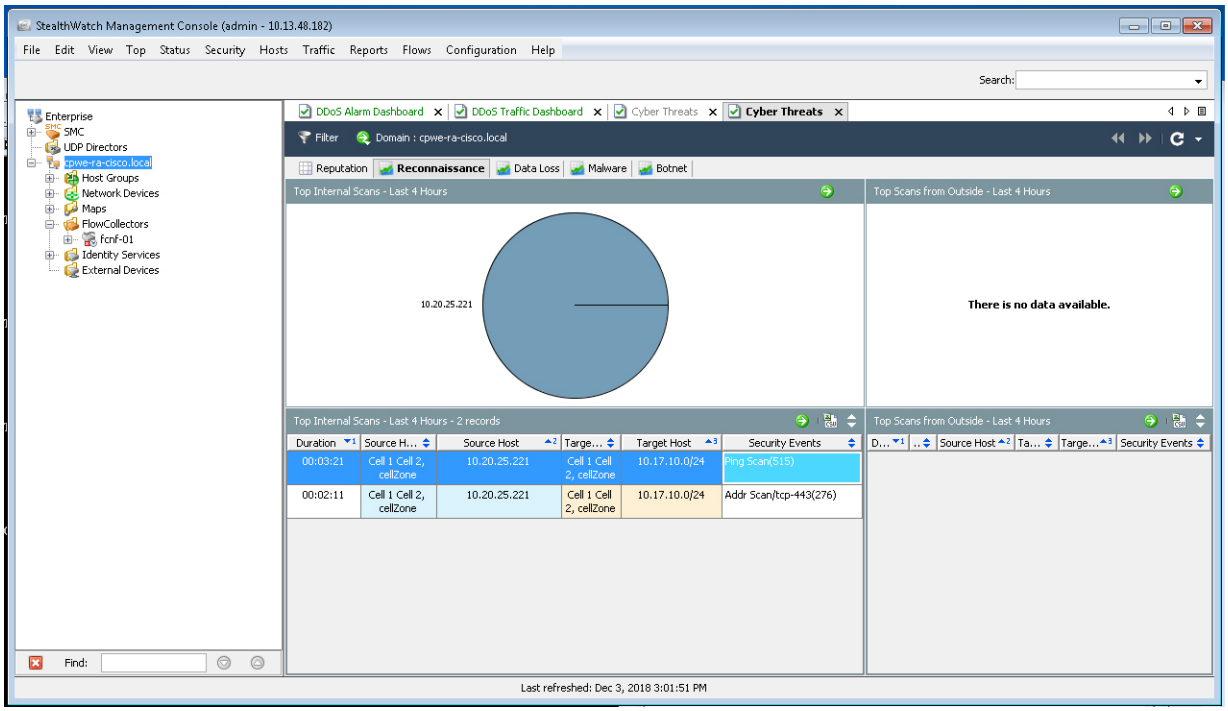
Figure 5-4 Scan by an Infected Laptop



- An infected laptop attached to a Layer-3 site operations center.

In both the cases, the infected laptop attempts to scan the entire IP address range to identify the next possible targets and attempt to infect them. Stealthwatch would immediately detect a possible infiltration by generating an alarm under High Concern Index. Any alarm that comes under High Concern Index must be immediately taken into consideration. Figure 5-5 shows how an alarm is displayed in the Stealthwatch Management Console. In Figure 5-5, the host 10.20.25.221 is attempting to do a scan for the 10.17.10.0/24 network.

Figure 5-5 Alarm Displayed in Stealthwatch Management Console

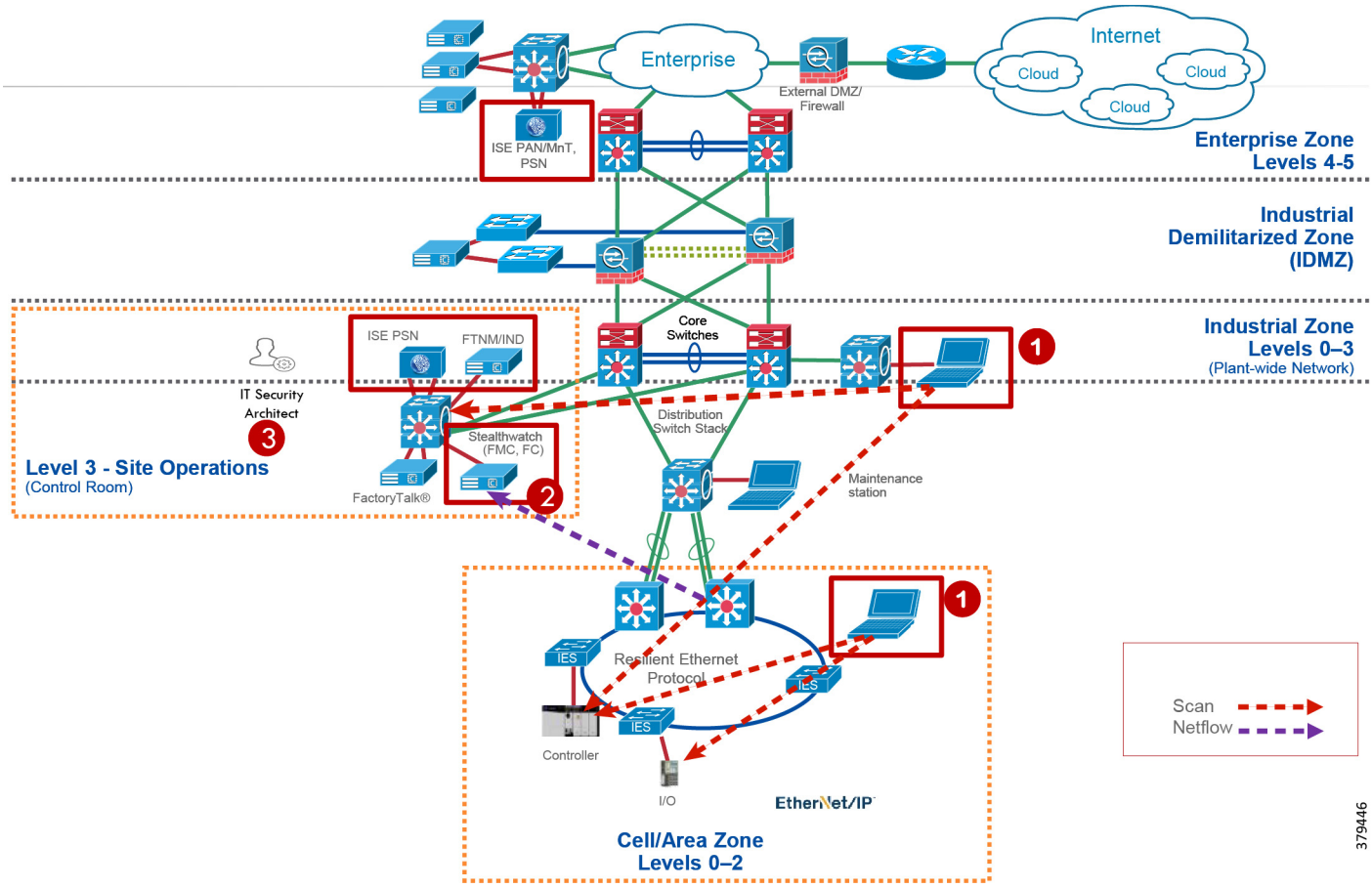


To understand more about alarms refer to:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf

Figure 5-6 shows the scenario where an infected laptop is connected to Cell/Area Zone or Level_3 operations and is being detected by the Stealthwatch. The steps involved are the following:

1. The IES in the Cell/Area Zone or the distribution switch in Level_3 operations is enabled with NetFlow. Refer to Configuring NetFlow on IES in Chapter 4, “Configuring the Infrastructure.”
2. The Stealthwatch Management Console reports an alarm indicating that there is a malicious activity occurring in the network.
3. IT security architect responds to the alarm by planning the next stage of remediation that can involve doing further investigation, restricting the access of the IACS asset, and so on.

Figure 5-6 Detection of Malware in the Cell/Area Zone

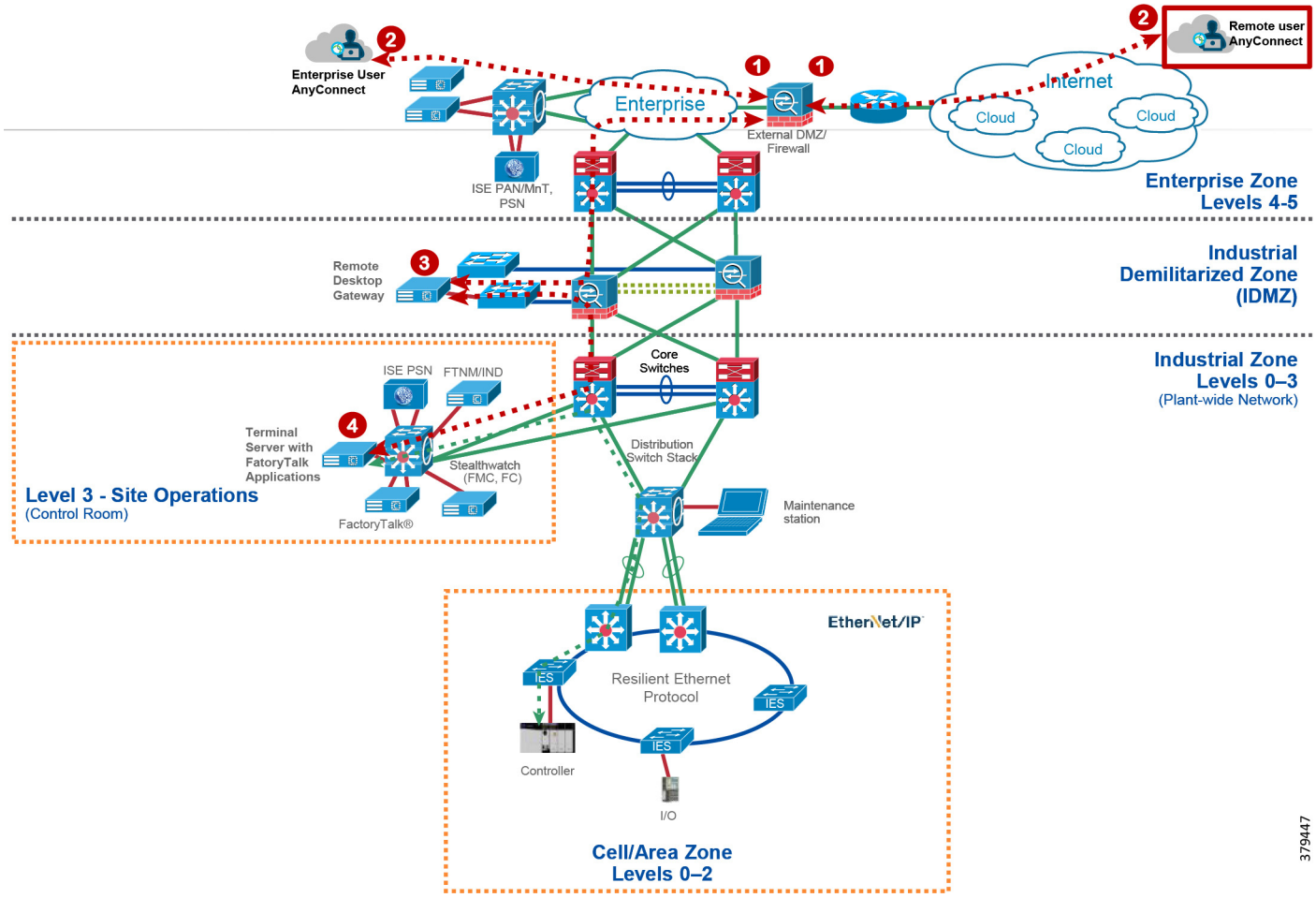


OT Managed Remote User (Employee or Partner) Accessing from (Enterprise or Internet) to a Network Device or an IACS Asset

This use case describes how a remote user employee or partner can access a networking device or an IACS asset from either internet or Enterprise Zone. The Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide (for best practices, see Appendix A, "References" for links to the CPwE IDMZ CVD DIG) that Cisco and Rockwell Automation team has developed provides design considerations and implementation details for providing remote access. The high-level steps for the remote access solution in CPwE IDMZ CVD as described in Figure 5-7 are the following:

1. A remote VPN gateway (ASA firewall) is enabled with VPN group that authenticates a remote user and authorizes a service, which in this case is to access a remote desktop gateway in the IDMZ.
2. The remote user, either employee or partner, uses a remote access VPN client (Cisco AnyConnect) to connect to the remote VPN gateway (ASA Firewall) and establishes a VPN session.
3. From the remote VPN gateway a connection is established to the remote desktop gateway in the IDMZ.
4. From the remote desktop gateway, a connection is established to the Terminal Server with FactoryTalk applications in the Level_3 - Site Operations.

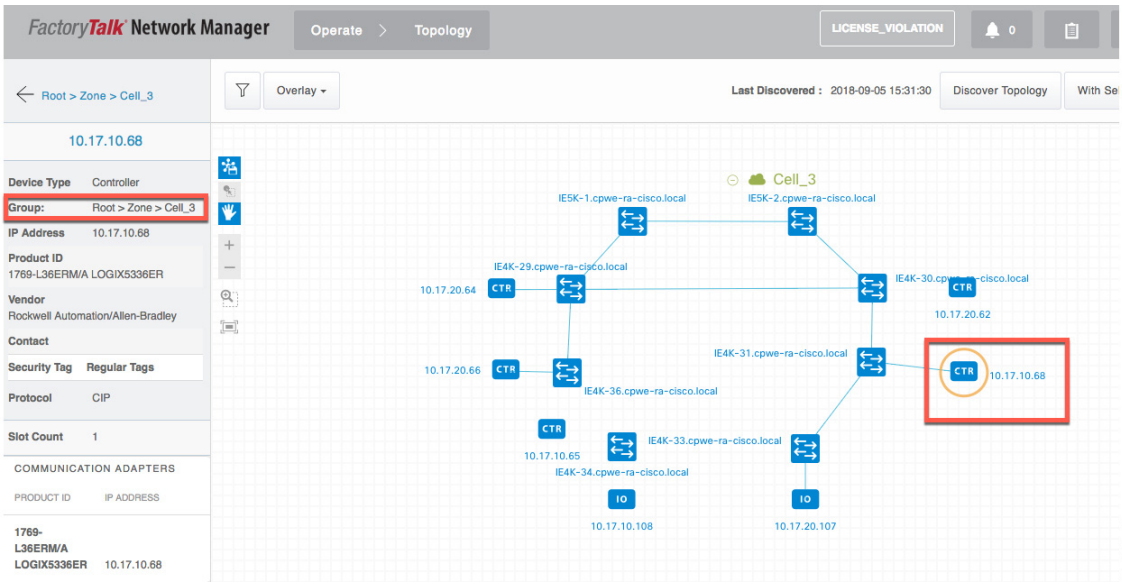
Figure 5-7 Remote User Access in CPwE Network



This use case builds on the previous Securely Traversing IACS Data Across the Industrial Demilitarized Zone CVD and expands the remote user use case by providing the means for an OT control system engineer to influence the remote access. In the CPwE IDMZ CVD, when a remote user needs access an OT control system engineer opens a request to IT security architect to enable remote access for IACS assets. The remote user than accesses the desired IACS asset. However, when the remote user no longer needs access to the IACS asset, then the OT control system engineer must open another case for removing access for a partner or an employee who no longer needs access. This process works, but when access is not removed in time then there could be a situation where a remote user has access to a networking device or IACS asset for longer than desired. Also, having this access open for a longer duration can open a window where a hacker can exploit this access to gain access to the networking device or IACS asset.

ISE-NMT integration via pxGrid provides a way for an OT control system engineer to express operational intent to ISE using NMT tool. The OT control system engineer expresses the intent by modifying the group of the networking device or IACS asset to a different group. In this CPwE Network Security CVD, a separate group called Remote_Access was defined to enable this feature. When an OT control system engineer changes the group of the IACS asset to the Remote_Access group, then remote access is enabled for that IACS asset and when the IACS asset is moved back to the original group, then the remote access to the IACS asset is revoked. The operation that needs to be done is to modify the group information of the IACS asset. Figure 5-8 shows the group information of an asset.

Figure 5-8 Modifying the Group Information of an IACS Asset



In this CPwE Network Security CVD, the remote access use case is demonstrated by creating a separate group called Remote. A device that needs Remote_Access needs to be moved to this group called Remote. When such an action is performed the following events are triggered:

1. The NMT sends a new device attribute “Remote” to ISE, which ISE reads as “assetGroup”. Refer to Remote_Access in Chapter 4, “Configuring the Infrastructure.”
2. ISE classifies this device as Remote_Access and since there is a new classification, ISE issues Change of Authorization to the IACS asset. This triggers a new authentication/authorization, which results in a new SGT assignment “Remote_Access”. Refer to Remote_Access in Chapter 4, “Configuring the Infrastructure.”
3. The Cisco Catalyst 3850 distribution switch downloads the new Secure Group Access Control (SGACL) from the ISE to allow access to Remote_Access. Refer to Configuring TrustSec Access Policy Matrix and Enforcement in Chapter 4, “Configuring the Infrastructure.” The traffic would flow from the FactoryTalk Application Server to the IACS asset.
4. Once the access to the IACS asset has been completed, the OT control system engineer moves the IACS asset back to the original group.
5. The NMT communicates the new group information to ISE, which derives this information using assetTag. ISE would profile this as normal IACS asset. Refer to Level_1_controller Policy in Chapter 4, “Configuring the Infrastructure.”
6. The Cisco Catalyst 3850 distribution switch has an existing policy that denies communication from Remote_Desktop to Level_1_Controller, so the communication from Remote_Desktop to Remote_Access is blocked.

Note When a new SGT is assigned to an IACS asset there will be a temporary loss of connectivity for few seconds before applications can communicate with the IACS asset. For the purpose of this CPwE Network Security CVD, the presumption is that OT has idled the IACS asset prior to enabling remote access.

Device Onboarding

This section discusses the different scenarios related to managing an IACS asset as it is attached to the network. The scenarios described here are the following:

- A new IACS asset attached to the IES.
- An onboarded IACS asset is moved to a different port in the IES.
- An onboarded IACS asset goes offline and comes back.
- Replacement of a failed IACS asset

Onboarding a New IACS Asset

Onboarding a new IACS asset successfully means the following in this CPwE Network Security CVD:

- The IACS asset is scanned successfully by the NMT.
- ISE learns about the IACS asset information from NMT using pxGrid probe.
- The IACS asset has successfully completed port-based authentication and authorization to ISE and receives an appropriate SGT value.
- The IACS asset initiates traffic flows both intra-Cell/Area Zone and inter-Cell/Area Zone.
- The distribution switch (Cisco Catalyst 3850) is able to download the policy matrix from ISE and then enforce the traffic flows generated by the IACS asset.
- Stealthwatch Management Console (SMC) is able to detect the traffic flows initiated by the IACS asset.
- SMC is able to generate an alarm if there is any malicious behavior generated by the IACS asset.

When all of the above activities are completed, then this CPwE Network Security CVD assumes that the IACS asset is onboarded successfully in the network. When all the activities are completed, an IT security architect has accomplished the following objectives:

- Visibility of the IACS asset—Device type, Location (where it is connected), IP address, MAC address
- Segmentation of the IACS asset—Enforce the traffic matrix and control access to the IACS asset and also restrict the traffic flows initiated by the IACS asset.
- Network flow detection—Gain full visibility of the traffic flows generated by the IACS asset—where it is talking and who is talking to this IACS asset.
- Malware detection—Protect the IACS asset or other devices in the network from an infected device. The IT security architect would gain an understanding of the source of the infection and can develop and execute an immediate remediation plan.

In the above sequence, it is important to understand which part of the tasks are automated and where there is a dependency on the engineer in deploying the solution. The following tasks are performed when a new IACS asset attaches to the network:

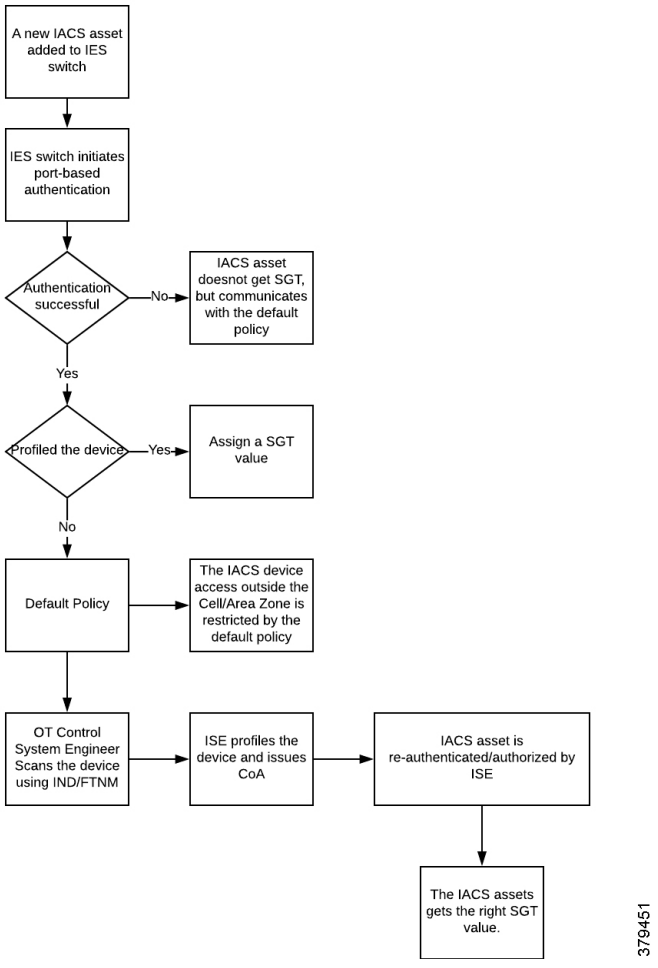
- Scanning of the IACS asset by the NMT—This is the only process where there is a dependency on the OT control system engineer to scan the IACS assets attached in the network. This process needs an OT control system engineer to press the scan button to learn about the IACS asset along with its attributes. Refer to Creating Asset Discovery Profile in Chapter 4, “Configuring the Infrastructure.”
- Profiling of the IACS asset by the ISE—The profiling policies are expected to be configured on ISE (refer to Profiling Policies in Cisco ISE in Chapter 4, “Configuring the Infrastructure”) and when an IACS asset needs to be authenticated and authorized, ISE matches the policies and applies the appropriate authorization profile (refer to Authorization Policies in Chapter 4, “Configuring the

Infrastructure"). There is no manual intervention needed and this process happens as per the design. However, if ISE did not learn about the IACS asset from the NMT and the IACS asset came online before that event, then ISE can only apply a default policy to the IACS asset.

- Whenever an OT control system engineer initiates a scan of the IACS asset, then the NMT and ISE would gain visibility of the device. When ISE learns about more information it profiles the IACS asset and when the profiling policy matches the authorization policies, then ISE issues Change of Authorization (CoA) to the IACS asset. This process triggers a new instance of authentication/authorization to the ISE and this process enables an IACS asset in getting the correct SGT value.
- NetFlow is enabled on all the ports where an IACS asset can get attached. So, whenever a new IACS asset is attached the traffic flow is automatically captured in SMC. There is no need for manual intervention by either OT control system engineer or by IT security architect.
- SMC also monitors if there is any malicious behavior happening in the network by enabling several machine learning algorithms on the data collected from the network using NetFlow. This process also happens automatically and there is no manual intervention needed.

Figure 5-9 shows a detailed process flow diagram for onboarding a new IACS asset.

Figure 5-9 Process Flow Diagram for On-boarding a New IACS Asset



An Onboarded IACS Asset Moves to a Different Port in an IES

This section discusses the behavior of the network when an IACS asset is moved to a different port in the IES. The scenario described here is for a situation where an IACS asset is currently on-boarded, authenticated, authorized, and has an SGT tag assignment done and, in that state, it is moved to a different port in the IES. The assumption is that the new port has an identical configuration to the previous one. In this scenario, the following steps will happen:

- The port-based authentication (refer to Configuring Port-based Authentication in Chapter 4, "Configuring the Infrastructure") will authenticate any device attached to it. So, the IACS asset needs to re-authenticate to the ISE.
- ISE sees that the new device is already profiled and it matches the IP Address and MAC address, so it authorizes the IACS asset and issues the same SGT value as in the previous case.
- The IACS device will have the same access as it had in the previous case.

An Onboarded IACS Asset Goes Offline and Comes Back

This section describes a situation where an onboarded IACS asset goes offline and comes back to the network. The underlying assumptions are similar to the previous section. The IACS asset before going offline was assigned a SGT and was communicating to other devices based on the access that the particular device was assigned. Now in that situation, the IACS asset has become offline and the reasons could be a failure of the asset, longer maintenance work, and so on. Once the device comes back the following are the sequence of the events:

1. If the IACS asset is present in the endpoint data store, then the authentication and authorization will happen in normal fashion. By default, the IACS assets are saved permanently in the PSN data base. So even if the IACS asset comes back after a longer duration, the IACS asset can retain its older privileges.
2. If the IACS asset is purged from the endpoint data store, then the ISE will not be able to profile the IACS asset and the default policy would be applied.
3. When the condition 2 happens where an IACS asset is removed from the ISE, then the OT control system engineer needs to re-scan the device (refer to Creating Asset Discovery Profile in Chapter 4, "Configuring the Infrastructure") and then ISE will be able to learn the device, profile it, issue CoA, and then push the IACS asset the original SGT value.

Replacement of a Failed IACS Asset

This section describes the workflow items that need to be performed by OT control system engineers to replace a failed IACS asset.

1. The new IACS asset needs to be connected to the same port where the previous IACS asset was connected.
2. The OT control system engineer needs to re-scan the IACS asset using NMT. The scan process will take a few minutes and depends on how many IACS assets are being scanned. The time taken to discover the IACS assets is linearly dependent on the number of IACS devices in the Access Discovery Profile.
3. Once the discover is completed by NMT, the information is sent immediately to ISE which re-profiles the device, issues CoA, and assigns SGT to the IACS asset.
4. Once the IACS asset is assigned the SGT, then the access of the new IACS asset would be same as the old one.

5. Only the OT control system engineer is required for the whole process, the rest of the infrastructure is automatic and the only process that needs to be done by the OT control system engineer is to re-scan the device.

CHAPTER 6

Troubleshooting the Infrastructure

This chapter includes the following major topics:

TrustSec Troubleshooting Tips on Cisco IE and Allen-Bradley Stratix IES and Cisco Catalyst 3850 Switches

The following section describes certain show commands that can be executed to view potential sources of problems related to Cisco TrustSec.

Note An IT engineer should have some expertise in TrustSec in order to troubleshoot any problems that are discovered. For complete information on Cisco TrustSec troubleshooting tips, refer to the following URL: https://community.cisco.com/t5/security-documents/trustsec-troubleshooting-guide/ta-p/3647576

IES is Unable to Register with Cisco ISE and Download the SGT Table Information

Verify whether the IES and Cisco ISE have the Right TrustSec Credentials Matched

This is the first step and it is possible that the IT security administrator might have a typo in the password or the ID information in the IES or the Cisco ISE. Refer to the following sections in Chapter 4, "Configuring the Infrastructure":

- Adding IES to Cisco ISE
- Configuring CTS Credentials on the IES

The credentials may be missing on the IES. Issue the following command:

```
IE4K-25#show cts credentials
CTS password is defined in keystore, device-id = IE4K-25
```

Verify Whether the PAC Key Between the IES and the Cisco ISE is Configured Correctly

The PAC key must match between the Cisco ISE and the IES. If there is a mismatch in the IES, then re-configure the key, which will force a new PAC provisioning in the IES. Refer to Configuring RADIUS AAA in Chapter 4, "Configuring the Infrastructure." To verify that the PAC is installed:

```
IE4K-25#show cts pacs
  AID: BA6AAD6CB6C10E7045A4CCD0DA18E706
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: BA6AAD6CB6C10E7045A4CCD0DA18E706
    I-ID: IE4K-25
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 12:45:25 EST Nov 10 2018
  PAC-Opaque:
000200B000030001000400010BA6AAD6CB6C10E7045A4CCD0DA18E706000060094000030100AA913A603C5310
9269B2EACF49C2DED3000000135B68B9AB00093A804EB1C0FC8CF53471B62A122C4BB434A3BE2D7C13B59F
A9D3BA8DF17CB7988B1E8BE7856DDC50C4F5CA6B20FE8E78270AB163FA73897FAFD7010325AEB3D8CD208D
92A1B7BBD2C483D01CA4EE6B8FB9B7AFBF9CA8A5AE2274ECDE5BB9C457674376A48865BADF98C43B2CFC9F
A8B8D3FD72FC538B
  Refresh timer is set for 8w4d

IE4K-25#
```

To clear the credentials:

```
clear cts credentials
clear cts pac
```

Verify that RADIUS is Operational from the IES

```
   IE4K-25#show aaa servers

RADIUS: id 1, priority 1, host 10.13.48.184, auth-port 1812, acct-port 1813
     State: current UP, duration 2488903s, previous duration 0s
     Dead: total time 0s, count 5968
     Quarantined: No
     Authen: request 2275, timeouts 0, failover 0, retransmission 0
             Response: accept 20, reject 2255, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 32ms
             Transaction: success 2275, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 2, timeouts 0, failover 0, retransmission 0
             Response: accept 2, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 50ms
             Transaction: success 2, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 38, timeouts 0, failover 0, retransmission 0
             Request: start 18, interim 0, stop 18
             Response: start 18, interim 0, stop 18
             Response: unexpected 0, server error 0, incorrect 0, time 29ms
             Transaction: success 38, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4w19h26m
     Estimated Outstanding Access Transactions: 0
```

```
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 15 hours, 42 minutes ago: 2
             low  - 0 hours, 0 minutes ago: 0
             average: 0
IE4K-25#
```

Verify that the CTS server-list is Pointing to the Right Policy Server Node

The command to verify the cts server-list is shown below:

```
IE4K-25#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = DISABLED

Installed list: CTSServerList1-000B, 1 server(s):
 *Server: 10.13.48.184, port 1812, A-ID 75FD68D130DA33A44480ED005C93FF49
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime =
20 secs
IE4K-25#
```

Verify that the IES has Downloaded the Right SGT Table Information

```
IE4K-25#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.13.48.184, port 1812, A-ID BA6AAD6CB6C10E7045A4CCD0DA18E706
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime =
20 secs
Multicast Group SGT Table:
Security Group Name Table:
    0-fd:Unknown
    2-fd:TrustSec_Devices
    3-fd:LEVEL_1_GENERIC
    4-fd:LEVEL_1_GENERIC_IO
    5-fd:LEVEL_0_IO
    6-fd:LEVEL_3
    7-fd:LEVEL_1_CONTROLLER
    8-fd:Remote_Access
    10-fd:Remote_Desktop
    255-fd:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 10:18:52 EDT Sun Sep 9 2018
Env-data expires in   0:01:08:23 (dd:hr:mm:sec)
Env-data refreshes in 0:01:08:23 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

```
IE4K-25#
```

IACS Asset is Unable to Authenticate to Cisco ISE

This section describes how to troubleshoot when an IACS device is unable to authenticate to Cisco ISE. To demonstrate the flow the IACS asset 10.17.10.65 is used to show the process.

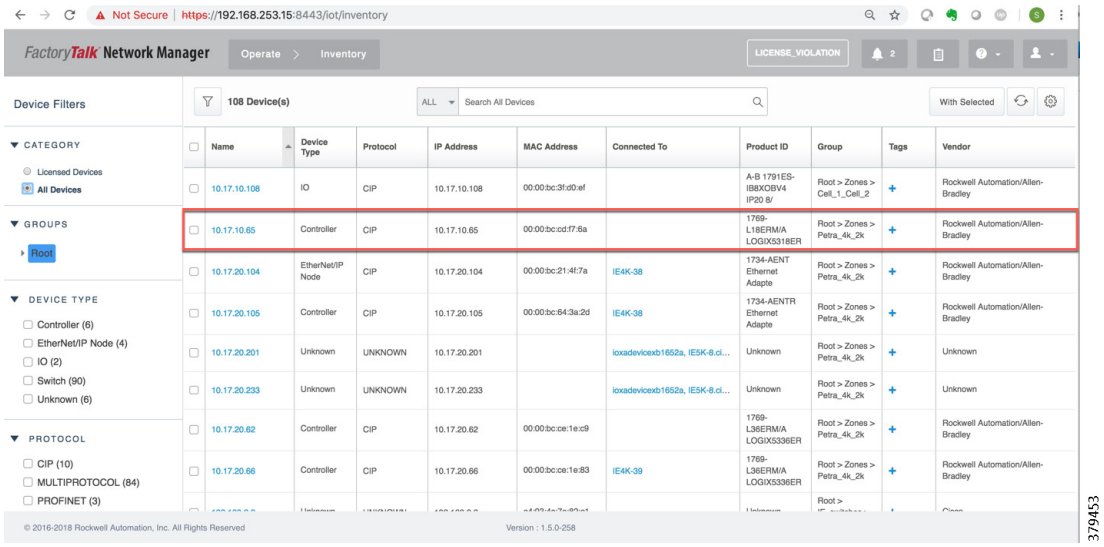
Verify the Authentication and Authorization State of IACS Assets Attached to an IES

```
IE4K-34# show authentication brief

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-----------------------------------------------------------------------------
Gi1/14     0000.bc3f.d0ef  m:OK            AZ: SA-                      409219s
Gi1/16     0000.bccd.f76a  m:OK            AZ: SA-                      409221s
Gi1/11     0000.bc2d.20ef  m:CF            UZ: SA- FA-                  409221s

Session count = 3

Key to Authentication Attributes:

 RN - Running
 ST - Stopped
 OK - Authentication Success
 CF - Credential Failure
 AD - AAA Server Failure
 NR - No Response
 TO - Timeout
 AR - AAA Not Ready

Key to Authorization Attributes:

 AZ - Authorized, UZ - UnAuthorized
 SA - Success Attributes, FA - Failed Attributes
 D: - DACL, F: - Filterid / InACL, U: - URL ACL
 V: - Vlan, I: - Inactivity Timer, O: - Open Dir

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
IE4K-34#
```

Verify that NMT has Discovered the IACS Asset 10.17.10.65

The first step would be to verify if NMT has discovered the IACS device 10.17.10.65.

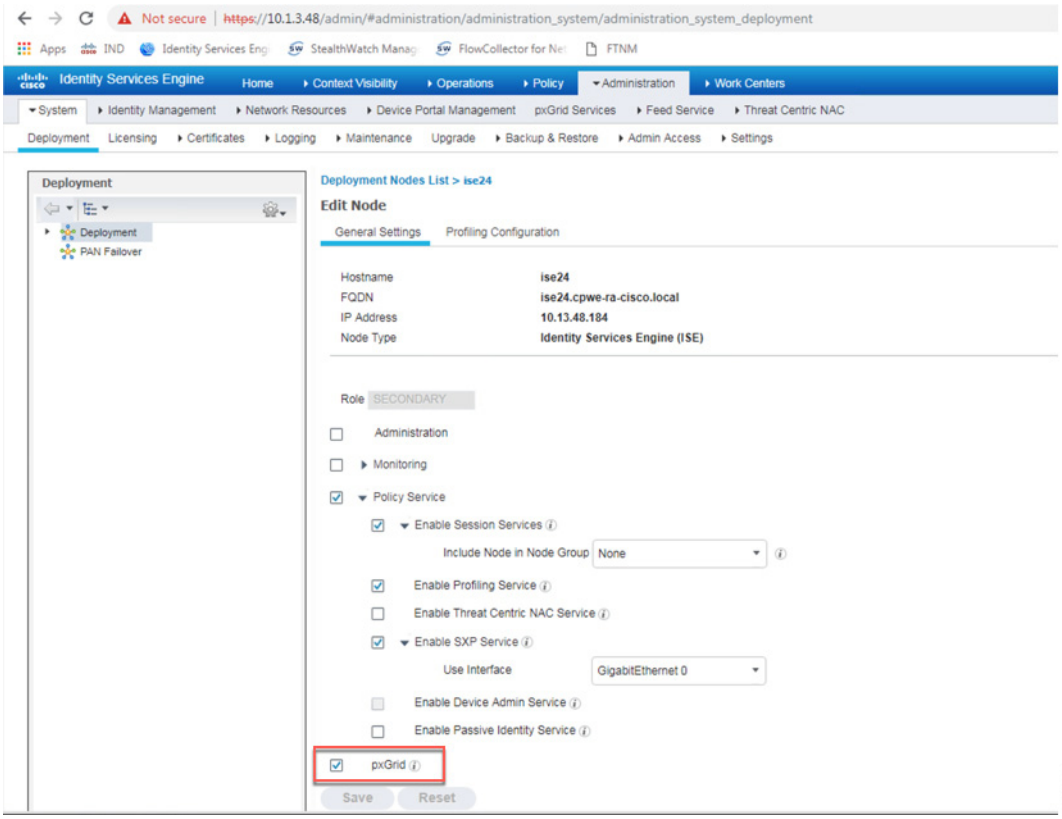
Figure 6-1 NMT Discovering IACS Asset 10.17.10.65



Verify that the pxGrid Service is Enabled at Cisco ISE

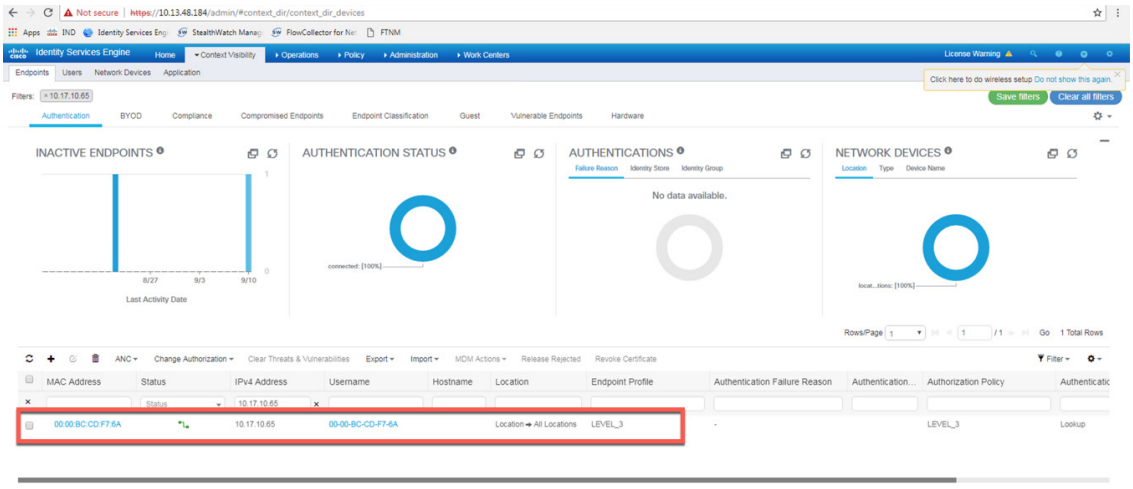
To verify that go to **(ISE admin web)—>Administration—>Deployment** and select the PSN (ise24 in this CPwE Network Security CVD):

Figure 6-2 Verifying that the pxGrid Service is Enabled at Cisco ISE



The next step is to verify if Cisco ISE has learned the IACS asset. Figure 6-3 shows that Cisco ISE has learned about the IACS asset.

Figure 6-3 Cisco ISE has Learned the IACS Asset 10.17.10.65



379454

Verify that Profiling Policies are Configured Correctly

ISE profiles the IACS assets based on the profiling policy. If conditions in the profiling policy are not configured correctly, then ISE will not be able to profile the IACS asset. Refer to Profiling in Cisco ISE in Chapter 4, "Configuring the Infrastructure" for information on configuring the profiling policies

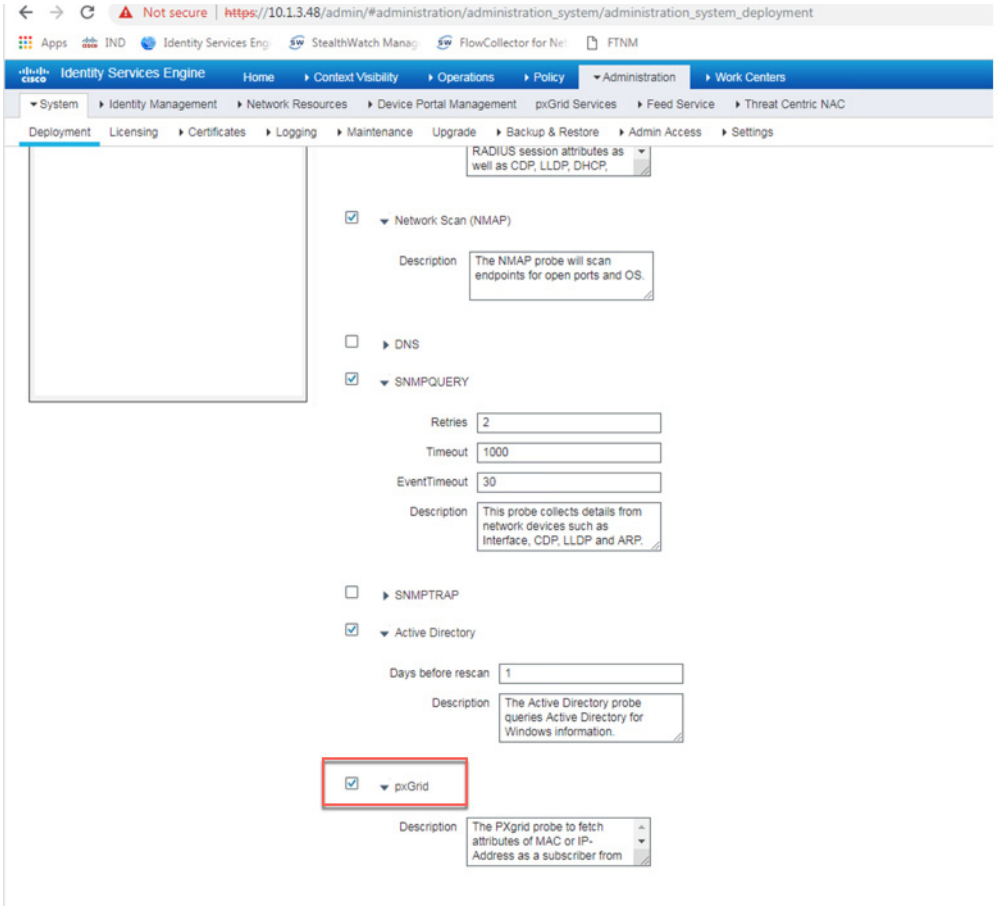
Verify that Authentication and Authorization Policies are Configured Correctly in Cisco ISE

To assign a SGT to an IACS asset, the authentication and authorization policy conditions must match to the IACS device attributes. Refer to Authorization Policies in Chapter 4, "Configuring the Infrastructure."

Verify that pxGrid probe is enabled at PSN

To verify that, go to **(ISE admin web)—>Administration—> Deployment—> Select the psn** (ise24 in this CVD) and select the tab profiling configuration.

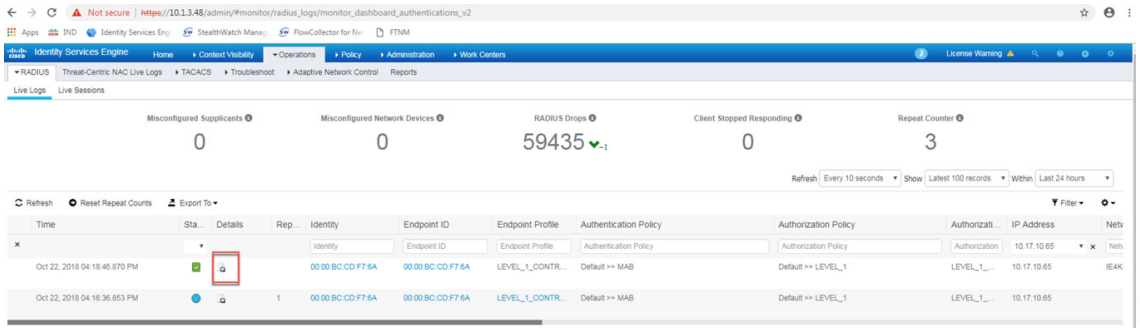
Figure 6-4 Verifying that pxGrid Probe is Enabled on the PSN



Verify Live Logs at ISE to Understand the Authentication/Authorization Flow

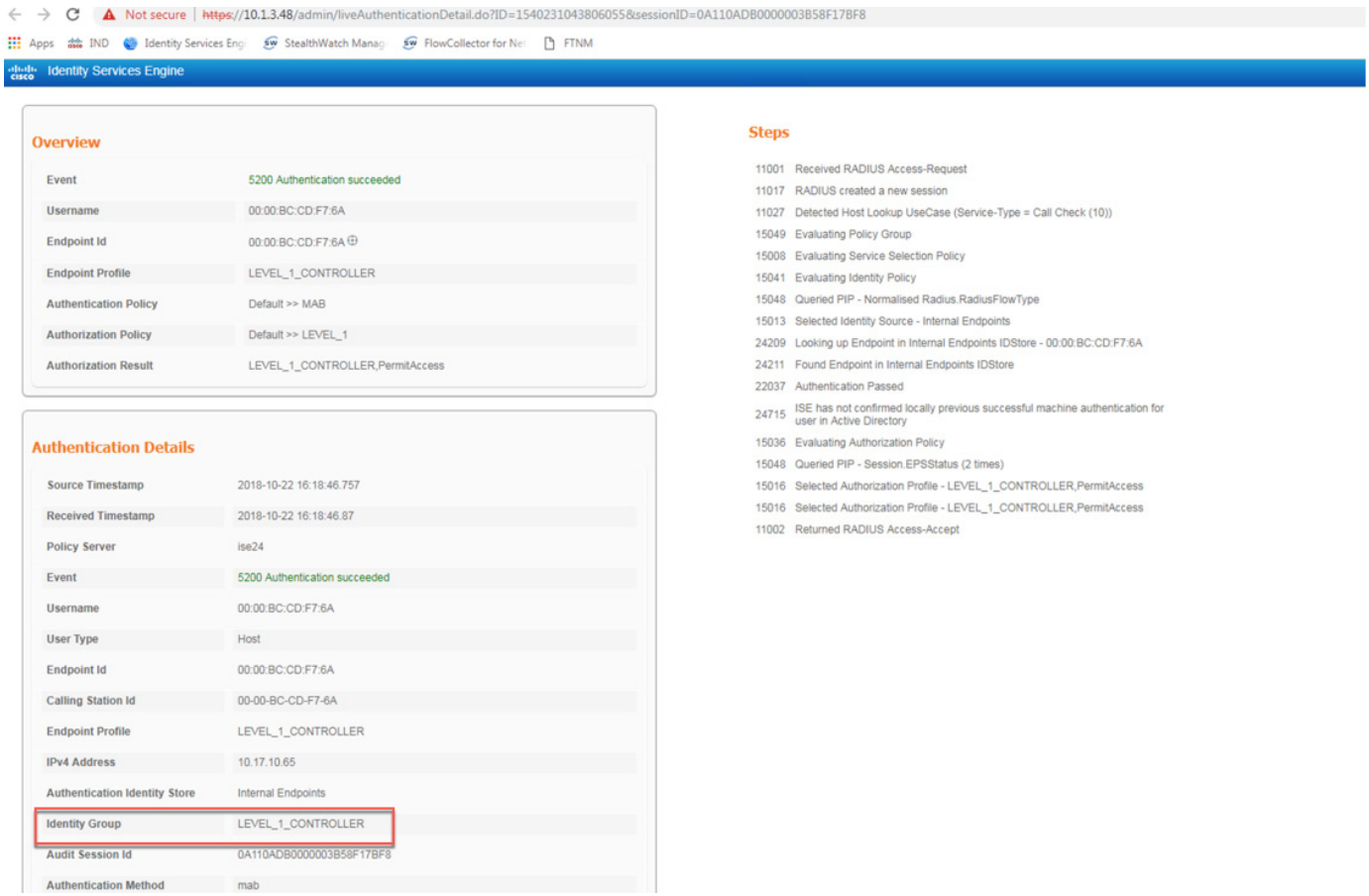
To see live logs, go to **(ISE admin web)—> Operation—> Live Logs** to get a list of devices that went through the authentication/authorization process.

Figure 6-5 Live Logs at ISE



Selecting the Details option will provide details about the complete exchange.

Figure 6-6 Authentication and Authorization Results of an IACS Asset



3850 Distribution Switch is not Enforcing the Policy Correctly

Different reasons for this problem to happen exist; it can be troubleshooted by going through the following steps:

Verify that SGT is Assigned to the Port on the IES

```
IE4K-25#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.13.15.25             4       INTERNAL
10.20.25.12             11      LOCAL
10.20.25.25             4       INTERNAL
10.20.25.221            5       LOCAL
10.20.26.25             4       INTERNAL
10.20.50.5              4       INTERNAL
192.168.4.25            4       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of INTERNAL bindings = 5
Total number of active   bindings = 7

IE4K-25#
```

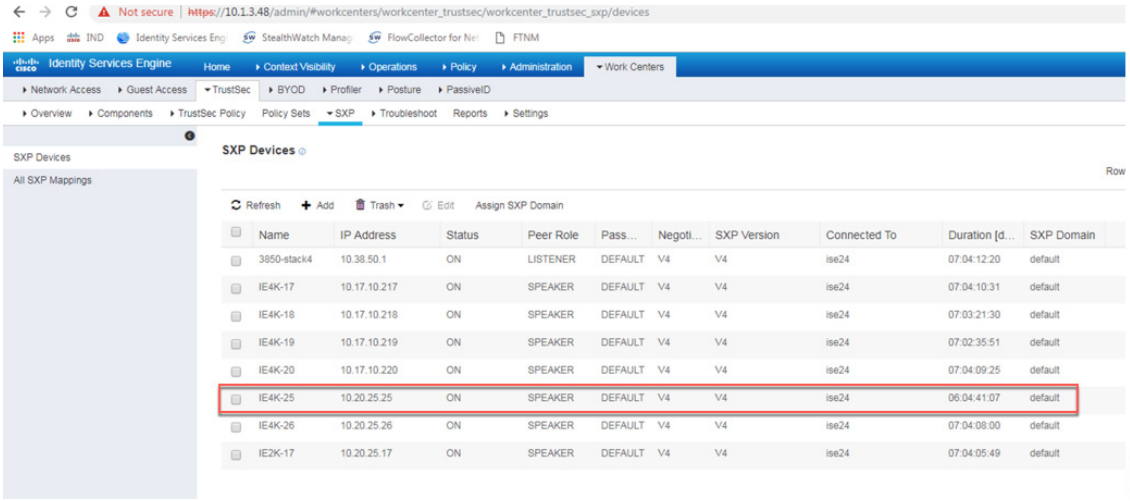
Verify that SXP tunnel is up Between the Cisco ISE and the IES Device

```
IE4K-25#show cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 10.13.48.184
Source IP        : 10.20.25.25
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 6:01:28:42 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

Verify that SXP Tunnel is Up at Cisco ISE to the IES (IE4K-25)

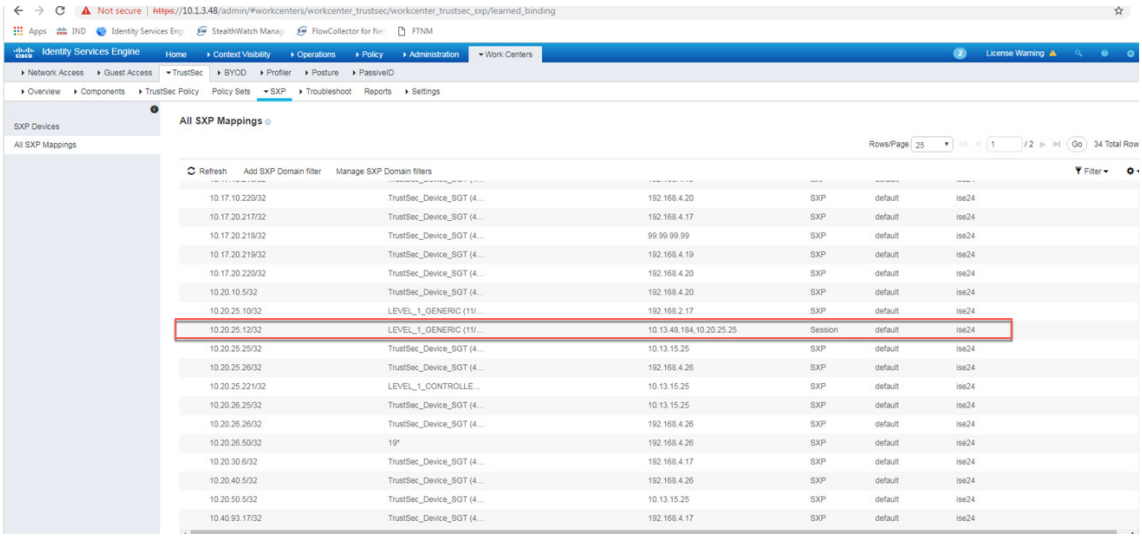
Navigate to **(ISE admin web)—> Work Centers—> TrustSec—> SXP Devices** and verify the SXP status.

Figure 6-7 Verifying the SXP Status of an IES Switch at ISE



Verify that Cisco ISE has Received the SGT-IP Mapping Information through the SXP Tunnel

Figure 6-8 Verifying the SXP Status of an IES Switch at ISE



Verify that 3850 is Receiving the SGT-IP Information through SXP Tunnel

```
P5-3850-stack-4#show cts sxp sgt-map brief
SXP Node ID(generated):0xC0A80A0B(192.168.10.11)
IP-SGT Mappings as follows:
IPv4,SGT: <10.13.15.25 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.10.65 , 5:LEVEL_1_CONTROLLER>
IPv4,SGT: <10.17.10.108 , 6:LEVEL_0_IO>
```

```
IPv4,SGT: <10.17.10.217 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.10.218 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.10.219 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.10.220 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.20.217 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.20.218 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.20.219 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.17.20.220 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.20.10.5 , 4:TrustSec_Device_SGT>
IPv4,SGT: <10.20.25.10 , 11:LEVEL_1_GENERIC>
```

Verify that Policy Matrix is Downloaded to the 3850 Distribution Switch

```
P5-3850-stack-4#show cts role-based permissions
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group
5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 5:LEVEL_1_CONTROLLER:
    Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group
5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 6:LEVEL_0_IO:
    Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group 6:LEVEL_0_IO:
    Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Cisco NetFlow Troubleshooting Tips

This section discusses some useful show commands for troubleshooting if NetFlow records are not showing up at the Stealthwatch management console.

Show Commands at the IES/3850 Distribution Switch

This section describes the various show commands that can be issued to troubleshoot the problem in a methodical fashion.

Verify that the NetFlow Record is Collecting the Right Parameters

```
IE4K-25#show flow record
flow record StealthWatch_Record:
  Description:        NetFlow record format to send to StealthWatch
  No. of users:       1
  Total field space:  59 bytes
```

```
  Fields:
    match datalink mac source address input
    match datalink mac destination address input
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

IE4K-25#
```

Verify that the Exporter is Configured with the Right IP Address

```
IE4K-25#show flow exporter
Flow Exporter StealthWatch_Exporter:
  Description:              StealthWatch Flow Exporter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.13.48.183
    Source IP address:      10.20.50.5
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            52254
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
  Options Configuration:
    application-table (timeout 600 seconds)
```

Verify that the Flow Monitor is Configured Correctly

```
IE4K-25#show flow exporter
Flow Exporter StealthWatch_Exporter:
  Description:              StealthWatch Flow Exporter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.13.48.183
    Source IP address:      10.20.50.5
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            52254
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
  Options Configuration:
    application-table (timeout 600 seconds)
```

Verify that the Flow Monitor is Applied to an Appropriate Interface

```
IE4K-25#show flow interface gigabitEthernet 1/10
Interface GigabitEthernet1/10
  FNF:  monitor:          StealthWatch_Monitor
```

```
direction:        Input
traffic(ip):      on
```

Verify that the Flow Information is Cached on the IES/3850 Switch

```
P5-3850-stack-4#show flow monitor name StealthWatch_Monitor cache
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               3

  Flows added:                              412595
  Flows aged:                               412592
    - Active timeout      (    60 secs)     184742
    - Inactive timeout    (    15 secs)     227850

DATALINK MAC SOURCE ADDRESS INPUT:       E865.49DF.7E41
DATALINK MAC DESTINATION ADDRESS INPUT:  0100.5E00.000A
IPV4 SOURCE ADDRESS:                     10.255.255.51
IPV4 DESTINATION ADDRESS:                224.0.0.10
TRNS SOURCE PORT:                        0
TRNS DESTINATION PORT:                   0
IP TOS:                                  0xC0
IP PROTOCOL:                             88
tcp flags:                               0x00
interface output:                        Null
counter bytes long:                      480
counter packets long:                    8

.Command to clear the flow data

clear flow record StealthWatch-Record-IN
clear flow monitor StealthWatch-Monitor-IN statistics clear flow monitor
StealthWatch-Monitor-IN cache clear flow exporter StealthWatch-Exporter statistics
```

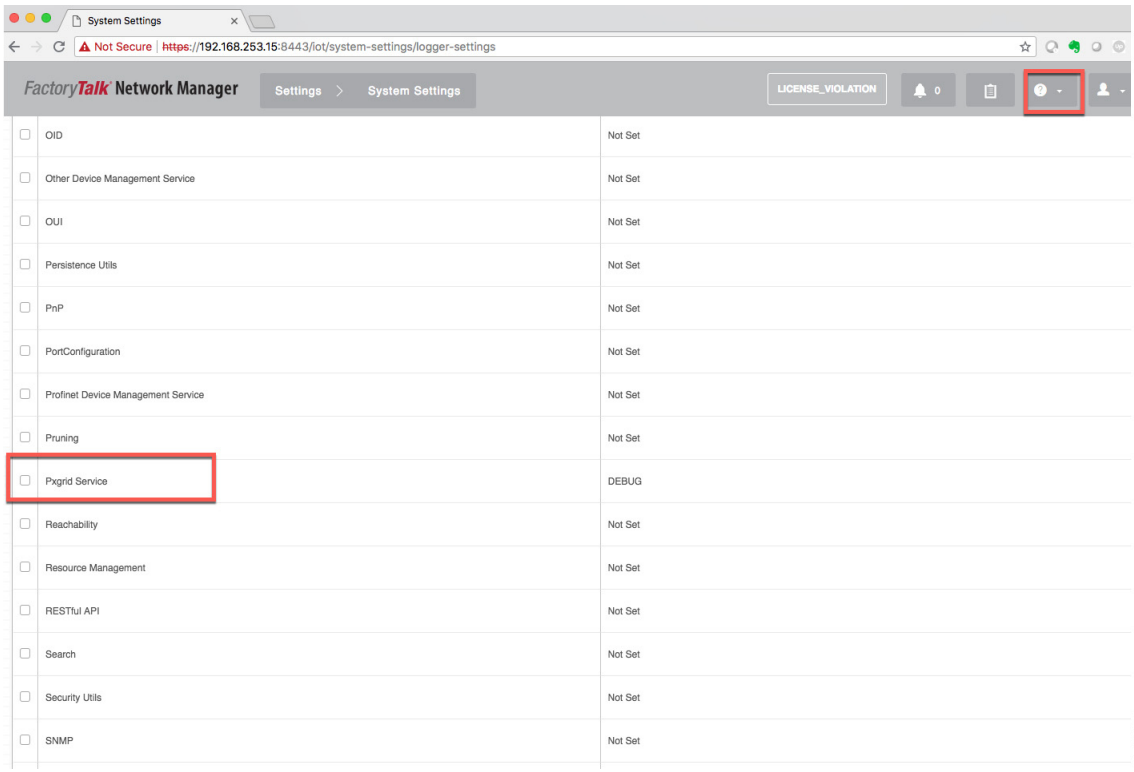
NMT Troubleshooting Tips

The configuration details for NMT can be found at:

- https://compatibility.rockwellautomation.com/Pages/MultiProductFindDownloads.aspx?crumb=112&refSoft=1&toggleState=&versions=57256
- https://www.cisco.com/c/en/us/td/docs/switches/ind/install/IND_1-5_install.html

A troubleshooting feature of NMT is to collect log information, which can help an IT security architect isolate a problem. Figure 6-9 shows how to collect logs for pxGrid in NMT.

Figure 6-9 Creating a Log File in NMT



After enabling the log files, to download logs select the “?” option in the top right corner as shown in Figure 6-9.

Cisco ISE Troubleshooting Tips

The following section provides high level troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco Identity Services Engine (ISE).

Note For complete information on Cisco ISE monitoring and troubleshooting tips, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_011001.html

Checking the Status of pxGrid

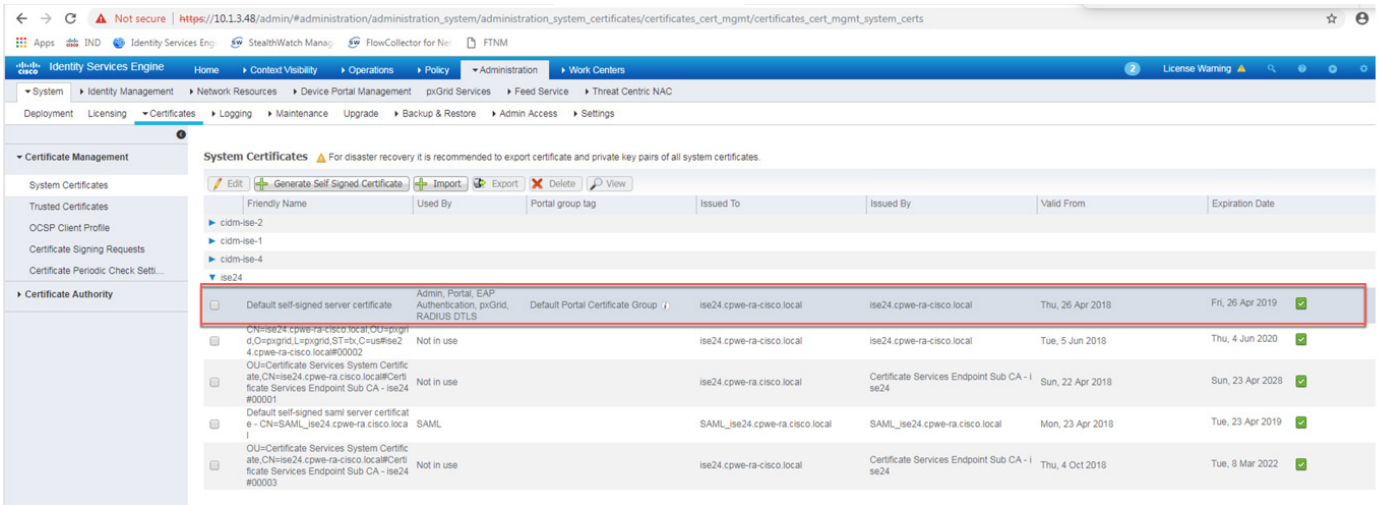
On the PSN, execute the following command to check the status of the pxGrid:

```
ise24/admin# show application status ise | include pxGrid
pxGrid Infrastructure Service          running          5736
pxGrid Publisher Subscriber Service    running          5880
pxGrid Connection Manager              running          5851
pxGrid Controller                      running          5902
ise24/admin#
```

Verify pxGrid Certificate in ISE PSN

From **(ISE admin Web)**, navigate to **Administration—>System—>Certificates—>System Certificates** and expand on PSN (ise24 in this CPwE Network Security CVD) to verify that system certificate is used for pxGrid.

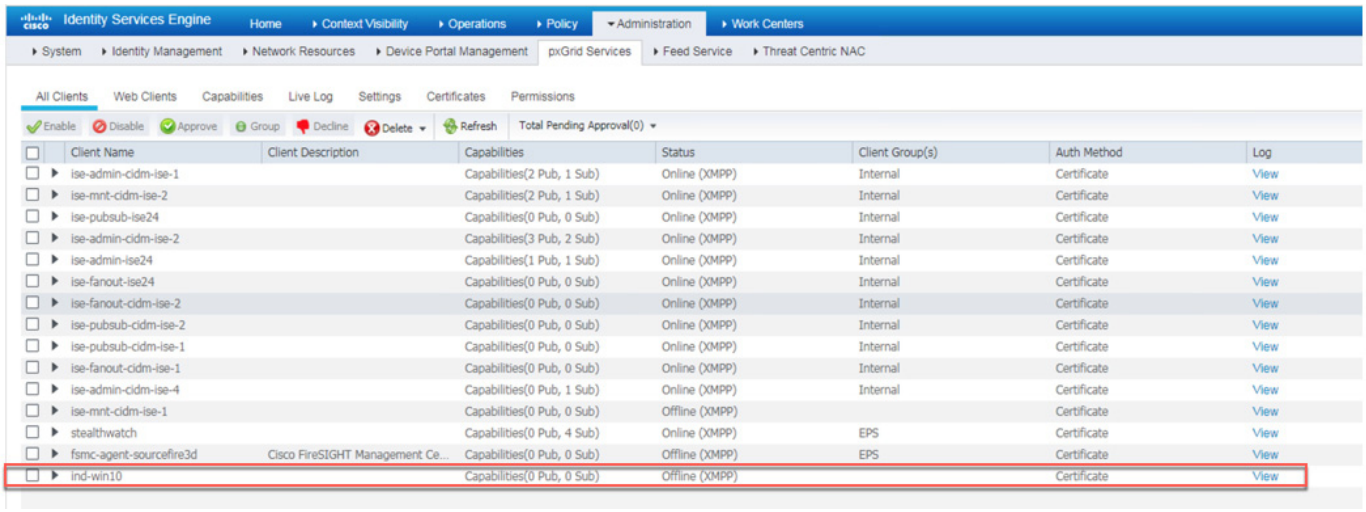
Figure 6-10 Verifying pxGrid Certificate in ISE PSN



Verify the NMT pxGrid Status in ISE

From **(ISE admin Web)**, navigate to **Administration—>pxGrid Services** and verify that NMT is registered as client.

Figure 6-11 Verifying the NMT pxGrid Status in ISE



Enable DEBUG on Profiler and pxGrid

In certain situations, it may be desired to enable debug on ISE and verify the exchange of information between the NMT and ISE via pxGrid. This section describes how to enable the debug.

Step 1 From (ISE admin web), navigate to **Administration—>System—>Logging—>Debug Log Configuration**.

Step 2 Select the **PSN** on the right panel (ise24 in this CPwE Network Security CVD DIG).

Step 3 Select **profiler** and change the logging levels to DEBUG and click **Save**.

Step 4 Select **pxgrid** and change the logging levels to TRACE and click **Save**.

To verify the log information, navigate to PSN (ise24) and issue the following command:

```
ise24/admin# show logging application profiler.log | include IND
2018-10-23 12:27:22,421 DEBUG  [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Looking for new publishers
...
2018-10-23 12:27:22,439 DEBUG  [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Existing services are:
[Service [name=com.cisco.endpoint.asset, nodeName=ind-win1
0, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://ind-win10:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2018-10-23 12:27:22,439 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- New services are: []
2018-10-23 12:27:22,451 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind-win10
2018-10-23 12:27:22,451 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{"offset":"0","limit":"500"}
```

```
2018-10-23 12:27:22,519 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2018-10-23 12:27:22,520 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content: "OUT_OF_SYNC"
2018-10-23 12:27:22,520 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Status is :"OUT_OF_SYNC"
2018-10-23 12:27:22,535 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind-win10
2018-10-23 12:27:22,535 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{"offset":"0","limit":"500"}
2018-10-23 12:27:22,602 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2018-10-23 12:27:22,602 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content: "OUT_OF_SYNC"
2018-10-23 12:27:22,602 INFO   [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Status is :"OUT_OF_SYNC"
2018-10-23 12:27:22,603 DEBUG  [ProfilerINDSubscriberPoller-84-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Static set after adding new
services: [Service [name=com.cisco.endpoint.asset, no
deName=ind-win10, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://ind-win10:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2018-10-23 12:27:22,612 INFO   [ProfilerINDSubscriberBulkRequestPool-533-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind-win10
2018-10-23 12:27:22,612 INFO   [ProfilerINDSubscriberBulkRequestPool-533-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{"offset":"0","limit":"500"}
--
2018-10-23 12:27:24,451 INFO   [ProfilerINDSubscriberBulkRequestPool-533-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2018-10-23 12:27:24,468 INFO   [ProfilerINDSubscriberBulkRequestPool-533-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content:
{"assets":[{"assetId":"50135","assetName":"192.168.4.31","asse
tIpAddress":"192.168.4.31","assetMacAddress":"","assetVendor":"Unknown","assetProductI
d":"Unknown","assetSerialNumber":"","assetDeviceType":"Unknown","assetSwRevision":"","
assetHwRevision":"","assetProtocol":"PROFI

NET","assetConnectedLinks":[{"assetId":"30189","assetName":"IE2K-21","assetIpAddress":
"192.168.2.21","assetPortName":"FastEthernet1/1","assetDeviceType":"Switch"},{"assetId
":"30158","assetName":"IE1K-2","assetIpA
```

APPENDIX A

References

This appendix includes the following major topics:

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing-Converged Plantwide Ethernet: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures-Converged Plantwide Ethernet: http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html
- *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html
- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.ht ml
- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture*:

  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html
- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

Other References

- *Stratix Managed Switches User Manual: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf*

APPENDIX B

Test Hardware and Software

Table B-1 Cisco and Rockwell Automation Components

Role	Model	Software Release	Comments
Layer 2 Industrial Ethernet Switch	Cisco IE 4000/5000 Allen-Bradley /Stratix 5400/5410	15.2(6)E2	Provides connectivity to IACS assets at Levels 0-2
Distribution switch	Cisco Catalyst 3850	16.3.5B	Distribution/Aggregation switch connecting the Cell/Area Zones
Cisco Identity Service Engine		2.4	Policy Access Control
Industry Network Director/Factory Talk Network Manager		1.5	Network Monitoring Tool (NMT)
Stealthwatch Flow Collector		6.10.2	Flow anomaly detection
Stealthwatch Management Console		6.10.2	Dashboard
Core Switch	Cisco Catalyst 6880	15.2(1)SY1a	Provides core functionality to the design.

APPENDIX C

Acronyms and Initialisms

Table C-1 lists the acronyms and initialisms commonly used in CPwE documentation.

Table C-1 Acronyms and Initialisms

Term	Description
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
ASDM	Cisco Adaptive Security Device Manager
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CIP	ODVA, Inc. Common Industrial Protocol
CLI	Command Line Interface
CoA	Change of Authorization
CPwE	Converged Plantwide Ethernet
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CVD	Cisco Validated Design
DACL	Downloadable Access Control List
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol

Table C-1 Acronyms and Initialisms (continued)

Term	Description
DIG	Design and Implementation Guide
DLR	Device Level Ring
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name System
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FIB	Forwarding Information Base
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IES	Industrial Ethernet Switch (Allen-Bradley Stratix, Cisco IE)
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPDT	IP Device Tracking
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology
LBS	Location Based Services
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching

Table C-1 Acronyms and Initialisms (continued)

Term	Description
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NMT	Network Monitoring Tool
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAC	Programmable Automation Controller
PAN	Policy Administration Node
PAT	Port Address Translation
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
PSN	Policy Service Node
PTP	Precision Time Protocol
pxGrid	Cisco Platform Exchange Grid
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SGT	Security Group Tags
SHA	Secure Hash Standard
SIG	Secure Internet Gateway

Table C-1 Acronyms and Initialisms (continued)

Term	Description
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
SYN	Synchronization
SXP	SGT Exchange Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
WAN	Wide Area Network
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

APPENDIX D

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation which follows the Cisco Validated Design (CVD) program.

CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to help achieve faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.
- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).
- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.
- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific sets of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see the Cisco Validated Designs at the following URL:

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

Publication ENET-TD019A-EN-P December 2018