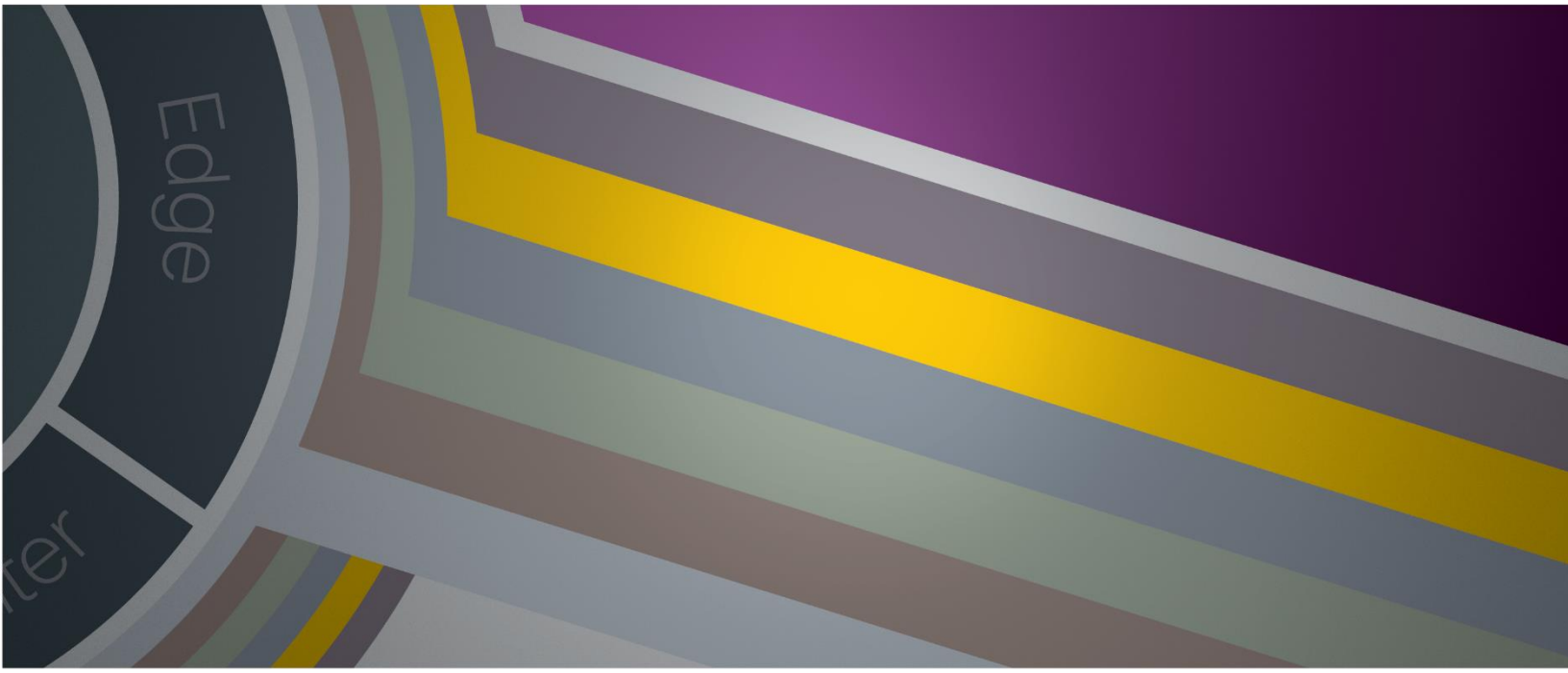


IoT Threat Defense for Manufacturing

SAFE Design Guide

Security Domain: Threat Defense

Updated May, 2018

Contents

Introduction

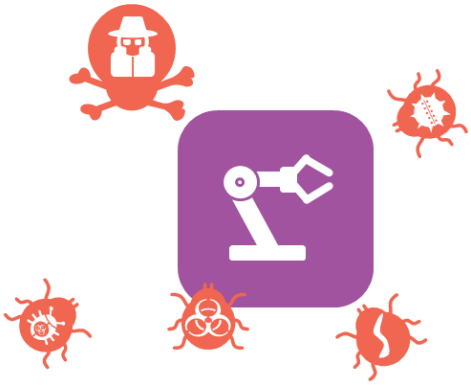
The Internet of Things (IoT) is impacting every business and fundamentally changing how we look at the devices that connect to a company. These things vastly expand the attack surface of a company. Manufacturing is one of the most targeted sectors; 32% of cyber-attacks occurred in manufacturing[1].

IoT devices and control systems are vulnerable. Hackers target manufacturing IoT devices because they have little or no security capabilities. Few use encryption, and many are unmanaged from a patching and vulnerability updates perspective. Security was simply not a part of their design. They can participate in sophisticated attacks such as DDoS or network invasion. They can be converted to zombies and used as agents of persistence. They can be used for ransom by shutting down or halting business entirely. Worst of all, they can be used to cause physical harm.

Many manufacturers struggle to integrate operational technology (OT) environments with the threats that exist in today's IT environments:

1. Systems, applications, and equipment are increasingly found to be vulnerable. Since 2009 the number of vulnerabilities discovered has grown 2,400%.
2. Some automation vendors are still shipping applications that require end-of-support platforms (e.g., Windows 98).
3. Base control protocols – the most commonly deployed E/IP-based control protocol lacked simple authentication until late 2015.

Despite these issues, the Internet of Things helps manufacturers gain efficiencies, harness intelligence from a wide range of equipment, improve operations, and increase customer satisfaction. That is why connectivity of these highly vulnerable environments almost doubled within three years.



[1] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

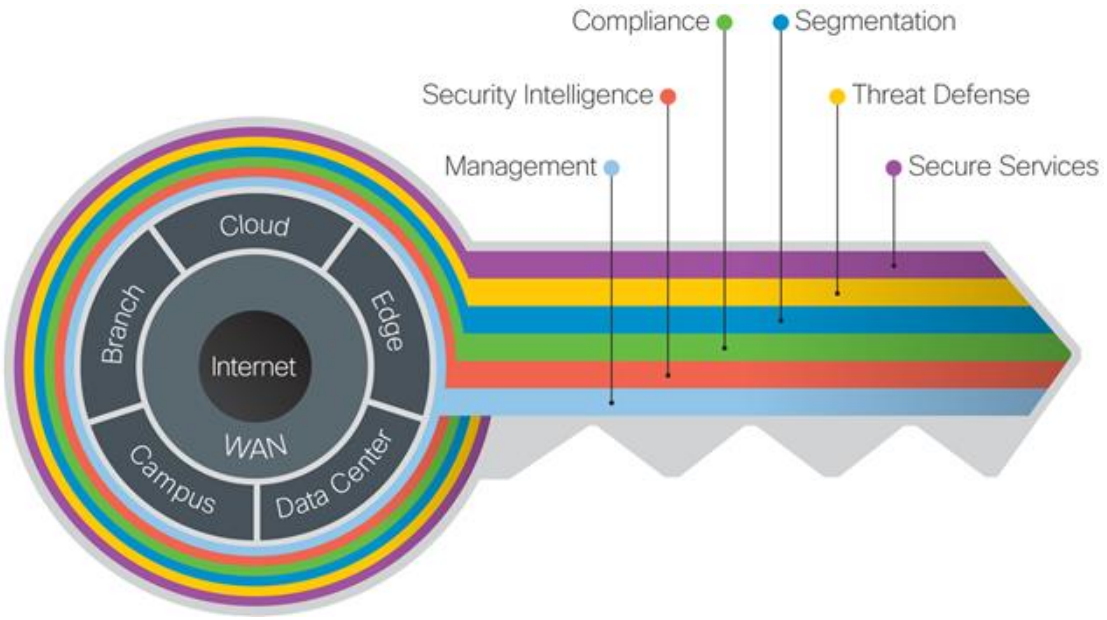
Return to Contents

The increasing demand for connecting more and more devices complicates security because attack surfaces are greatly increased. OT and IT professionals want to protect their manufacturer networks and devices to ensure safety and continuity of business.

Cisco's IoT Threat Defense solution solves these manufacturer challenges.

Cisco's IoT Threat Defense solution takes an architectural approach to protecting IoT using the SAFE model for security, which starts with the business flows/use cases. This design guide specifies the components and configurations used to validate this architecture, protecting manufacturers as they embark on their digital transformation journey to achieve Industry 4.0, or realize the Industrial IoT. It is part of the SAFE security reference architecture.

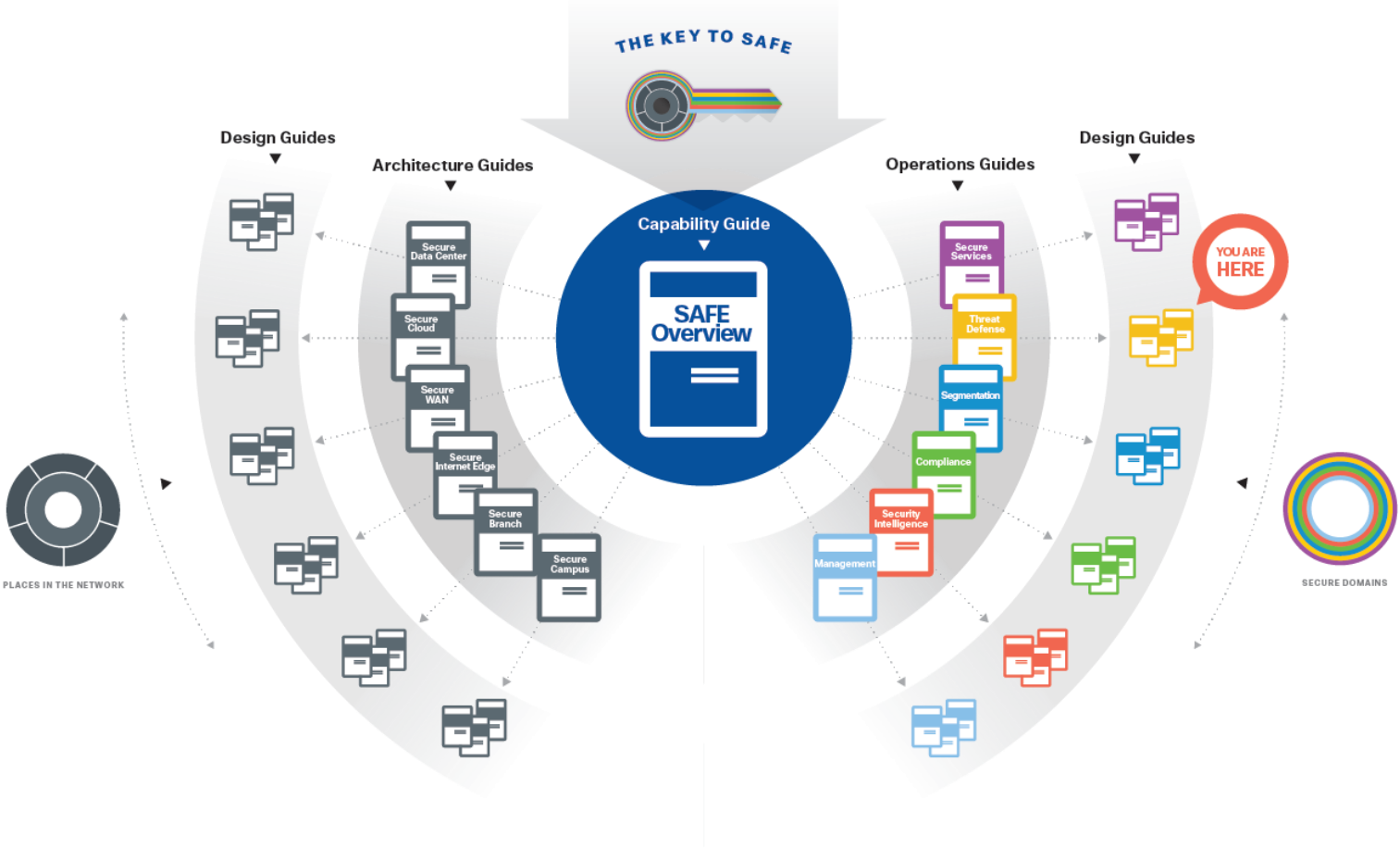
Figure 1 - Key to SAFE



The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains.

SAFE simplifies end-to-end security by using views of complexity depending on the audience needs. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures and designs, SAFE provides guidance that is holistic and understandable.

Figure 2– SAFE Guidance Hierarchy



More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here: www.cisco.com/go/safe

Return to Contents

Manufacturer Business Flows

SAFE uses the concept of business flows (communication flows) to simplify the identification of threats that can impact these activities, and thereby the security needed to protect business functions.

Business use cases that affect security in the manufacturing IoT space include the following:

- Securing the devices and applications that are present on network
- Providing remote access for support
- Defending against high risk activity on the same network

Figure 3 – Business Use Cases

Return to Contents

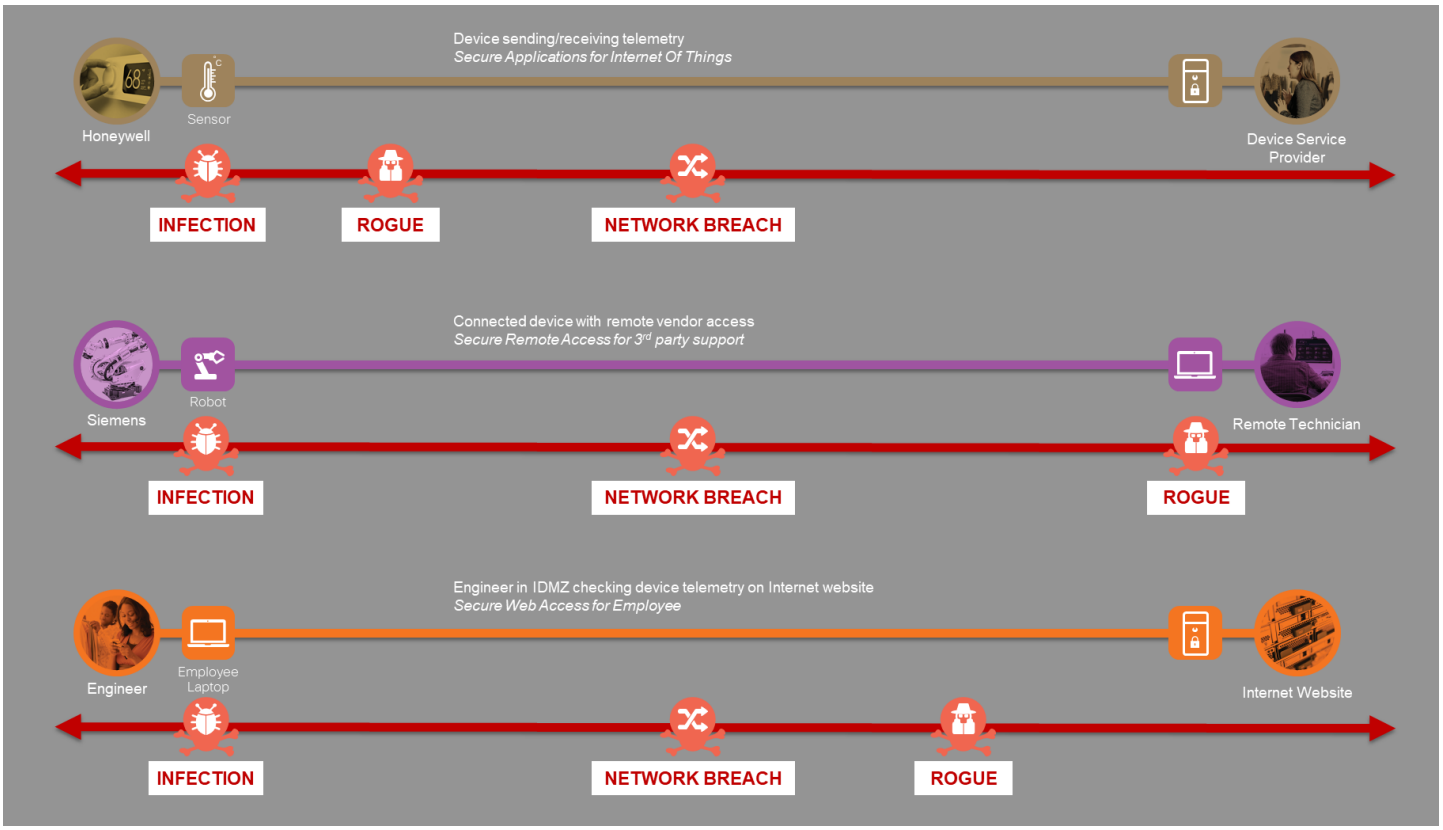
7

Manufacturing Attack Surface

The IoT Threat Defense solution protects systems by applying security controls to the attack surface found in manufacturer networks across all of their business use cases. The threats and risks that are present in manufacturer networks are around the devices, the humans and the network.

Rogue identity, infections, and advanced persistent threats allow hackers the ability to take control of your devices and networks. Legacy remote administration access to devices (such as modems) adds additional risk. Zero-day vulnerability attacks can bypass existing controls.

Figure 4 – Manufacturing Attack Surfaces



Return to Contents

Solution Overview

IoT Threat Defense for Manufacturing tackles the challenge these threats pose to IoT on four critical fronts:

Cisco IoT Threat Defense is a tested, layered architecture and services offering with several points of presence in the network to create a secure membrane around IoT devices. Secure segmentation of IoT devices means that all of the data and communications required for IoT devices to perform their functions flow freely, and desired business objectives can be securely realized. At the same time, Cisco provides the visibility and analysis to detect threats, defend against them, and maintain service resiliency. Secure remote access helps customers gain visibility and control over third-party access to their networks. The consulting and services component of the solution helps customers assess their IoT risk and assists customers with the design, deployment, and ongoing operation of a secure IoT environment.

Security Capabilities

To protect IoT devices and systems, specific capabilities are necessary to build the appropriate layers of defense. The SAFE methodology capabilities (Blue Circles) best suited for this defense are aligned with each of these areas. These capabilities work together to create several layers of defense protecting the organization and its IoT infrastructure.

Segmentation

Security starts with visibility. But for the IoT systems that you know you already have, segmentation comes first. Segmentation is about restricting network access and dividing the network based on role and function.

There are many ways an organization can be compromised and these highly vulnerable IoT devices can be accessed. The most common are e-mail phishing attacks and web-hosted malvertising, which infect user systems and then spread across a company's infrastructure, attaching to IoT devices with no impediment. For this reason, these IoT devices must be segmented from user environments and from each other.

These capabilities restrict network access and divide the network based on role and function.

Icon	Capability	Function
	Identity	Context-based identity of devices and users—Restricts connection to known users and devices including context items such as time of day, location, and posture.
	Profile	Profile devices—As devices are connected to the network, profiling defines the contextual elements necessary for device classification and categorization.
	TrustSec	Identity-based software-defined segmentation—Separates IoT systems and users based on role and policy, and stops unknown IoT devices from connecting to the network.
	Firewall	Identity-based firewall segmentation—Converges IO and OT without interfering with operational practice, and separates traffic based on role and policy.

↩Return to Contents

Visibility and Analytics

Once an initial level of segmentation has been implemented for known IoT devices and users, adding improved methods of visibility enables identification of undocumented devices on the network. Once all devices are identified and known, it becomes easy to detect and remediate threats that bypass existing controls.

These capabilities provide broad and deep visibility across the entire network.

Icon	Capability	Function
	Identity	Context-based identity of devices and users—Users and devices including context items such as time of day, location, and posture.
	DNS Security	DNS based security—Identifies Internet communications from every device on the network based on name resolution, blocks malicious domains, and breaks command & control callbacks.
	Intrusion Prevention	Intrusion prevention—Provides IoT visibility with deep packet inspection; blocks attacks, exploitation, and intelligence gathering
	Network Monitoring	Monitor infrastructure communications flows—Uses the information to better pinpoint nuisances in the network, and identifies and alerts on abnormal device traffic flows.
	Analysis and Anomaly Detection	Analyzes normal IoT network behaviors, creating a baseline for operations and known devices connected to the network. Generates alerts when abnormal activities start.
	Threat Intelligence	Threat intelligence—Provides knowledge of existing malware and communication vectors, and learned knowledge of emerging behavioral threats.

↩Return to Contents

Remote Access

To maintain your expensive and sophisticated modernization investments, you are likely to rely on your vendors for debugging and maintenance. For that to happen, you need to allow them remote access into your plant. Secure remote access replaces the legacy modems and other connectivity methods vendors used in the past, eliminating the back doors to your digitally connected network.

These capabilities provide and ensure secure remote connectivity to the company.

Icon	Capability	Function
	Identity	Context-based identity of devices and users—Restricts connection to known users and devices including context items such as time of day, location, and posture.
	VPN	Secure remote access VPNs—Provides secure encrypted access for remote operators, vendors, and providers based on role and policies.
	Anti-Malware	Client and network security—Inspects files for malware and viruses, quarantines and removes any threat quickly before it can spread and contaminate vulnerable IoT systems.

Return to Contents

Services

Despite the technological advances that the IoT represents, the human factor is the most important. People develop these technologies to help people, and people are needed to secure IoT environments. No doubt it is a daunting task. The good news is that the right planning and guidance greatly improves the likelihood of establishing a successful IoT security program.

All of the capabilities described above help to create a secure network. In preparation for deploying these, it is necessary to fully assess and evaluate your environment. Many of these services are difficult, if not impossible, for a company to objectively accomplish themselves:

- Security network penetration assessment
- Automation & control system risk assessment
- Privacy impact assessment
- Firewall & Stealthwatch deployment
- Security segmentation service
- ISE design & POC
- Solution support
- Incident response services

Services such as security network penetration assessment and automation & control system risk assessment can help you get the lay of the land. Include deployment and incident response services early on in your projects to ensure that you get the best results possible from your investment.

For more information about Cisco Services, please visit:

https://www.cisco.com/c/en/us/services/overview.html

For information about leveraging our Partner ecosystem, please visit:

https://www.cisco.com/c/en/us/solutions/partner-ecosystem.html

The latest news and information about Cisco's solution for IoT can be found here:

https://www.cisco.com/go/iot

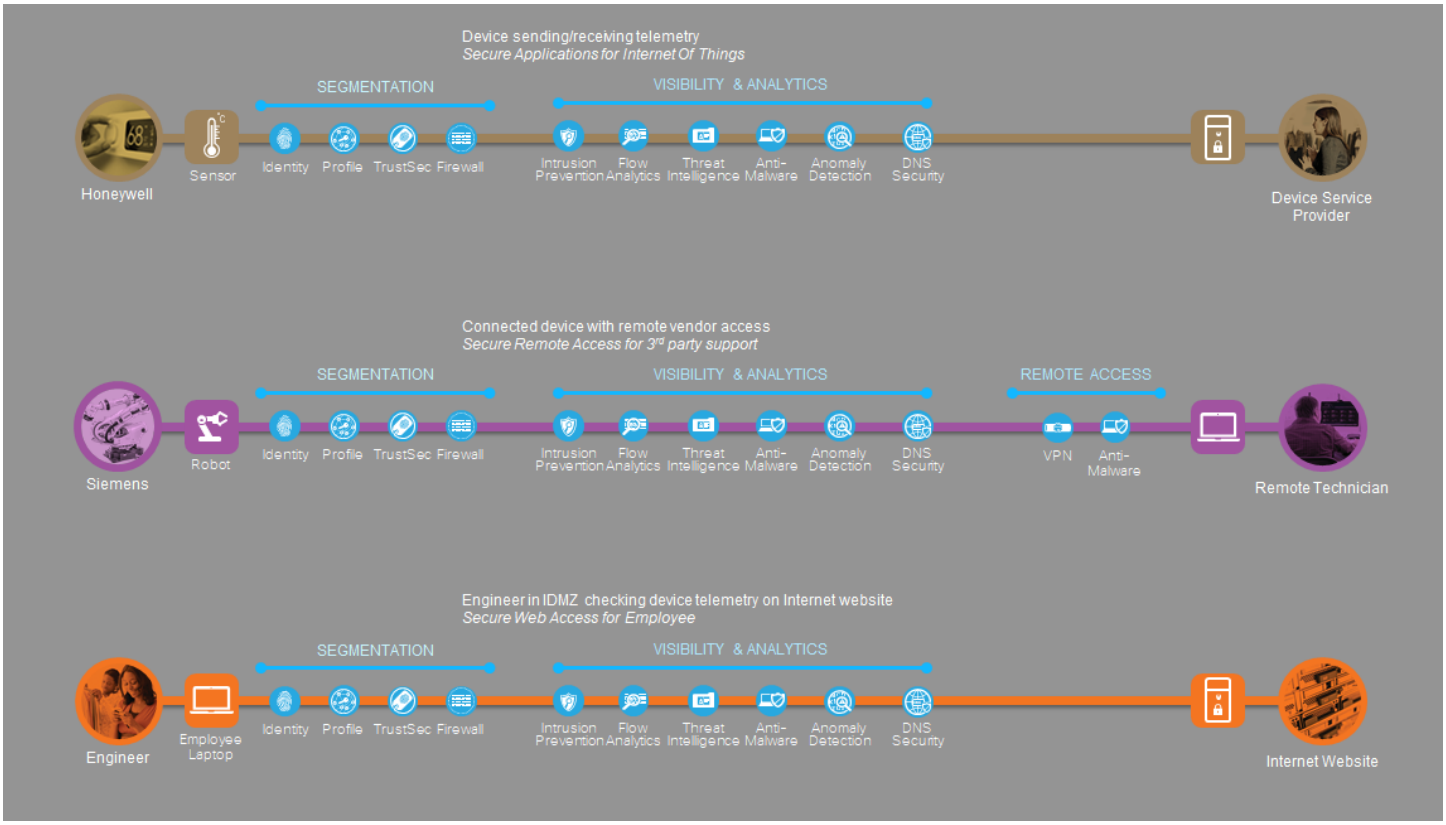
Return to Contents

Solution Architecture

The first step in developing a defense-in-depth architecture is to take all of the capabilities that can thwart threats and match them up with the real-world business functions/flows used in a typical industrial environment.

Each of these three business flows defined earlier are shown in Figure 5, with the key capabilities described above applied.

Figure 5 – SAFE Business Flows and Capabilities



Each of the capabilities are grouped by the area of focus: Segmentation, Visibility & Analytics, and Remote Access. These capabilities are implemented through product features. The following sections briefly describe each area and the products selected that align to the capabilities.

↩Return to Contents

Segmentation

Security starts with visibility. However, for the IoT systems that you know you already have, segmentation comes first. Segmentation is about building a secure place to protect what you have from the known and unknown risks on the network, and then with improved visibility you can identify and protect the IoT devices you discover. Segmentation puts these devices out of the reach of attackers, and prevents these devices from being used as pivot points to move through the network if they are compromised.

The US Department of Homeland Security, National Security Agency, international defense agencies, and leading network publications and analysts recommend network segmentation to limit the scope of a compromise and reduce the extent an adversary can move across the network. These segments become the control point through which the devices can send and receive traffic, giving us visibility focus areas via the segmentation. Cisco TrustSec with our Identity Services Engine (ISE) and our Next Generation Firewall provide north-to-south as well as east-to-west network segmentation, ensuring the safety and security of your network modernization projects.

Capability		Solution Component
	Identity	Cisco Identity Services Engine, Enterprise Directory Services
	Profile	Cisco Identity Services Engine
	TrustSec	Cisco Identity Services Engine, Network Switches, Firewalls, and Routers
	Firewall	Cisco’s ASA and Firepower Next Generation Firewalls

Return to Contents

Segmentation with ISE and TrustSec

Cisco ISE provides identity-based access control, context, and visibility (for example, user, device, location, and time) of IoT devices and users across the network. Cisco ISE is also a controller and orchestrator for TrustSec-based software segmentation policies. With Cisco TrustSec technology, you can control access to network segments and resources using the switches, routers and firewalls you already have. These role-based access control policies allow you to dynamically segment your network without the complexity of VLANs and manual switch-by-switch configurations.

This technology is ideal for implementing security at the switch level between IoT devices on the same switch, within or between cells, and creates the desired segmentation throughout the Industrial zone. It is managed centrally via ISE and scales for the world of IoT. It provides a true topology-independent segmentation architecture, by creating logical security groups based on the role of each device. These security groups can be enforced by VLANs (legacy infrastructure), port-based access control lists, and Security Group Tags (SGT) as we did in this design.

These TrustSec policies can be applied to specific traffic between any two network resources (devices) independent of their location. The TrustSec policy matrix defined in ISE provides an easy way for security administrations to view the policies from one single window across the entire organization

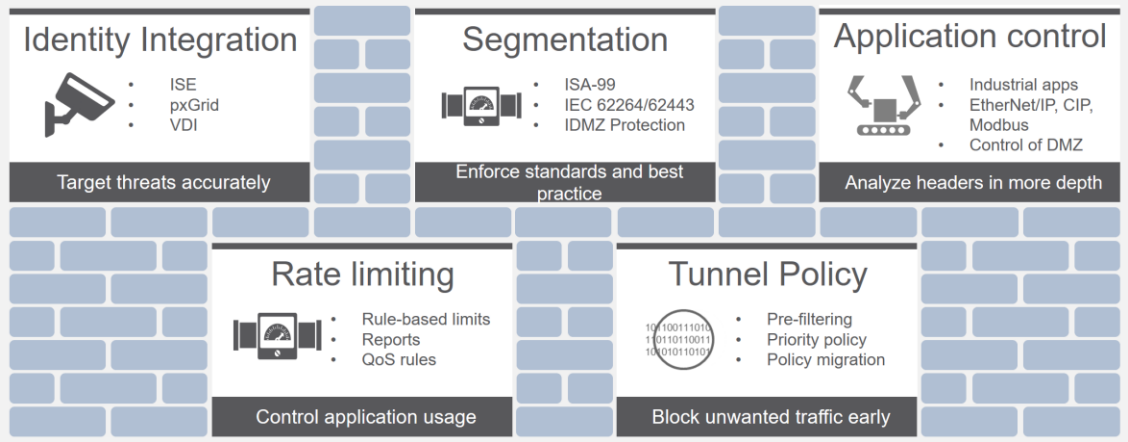
Using TrustSec policies, an infected device can be isolated and blocked from accessing other sensitive areas, regardless of network topology.

Segmentation with NGFW

The Cisco Firepower Next-Generation Firewall (NGFW) is a fully integrated, threat-focused next-gen firewall with unified management. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the device, each providing additional or alternate layers of defense against the threats to IoT. It also provides the anchor point for converging IT and OT security visibility without interfering with operational practice.

Figure 6 shows the capabilities of a firewall for the world of the IoT. We will go in depth on two important capabilities, segmentation and application control, for the lab/use case.

Figure 6 – IoT Capabilities with the NGFW



Tips for Segmentation in the IoT for SCADA Networks

1. The base rule set should be DENY ALL, PERMIT NONE.
2. Ports and services between the zone environment and an external network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
3. All “permit” rules should be both IP address- and TCP/UDP port-specific.
4. All rules shall restrict traffic to specific IP address or range of addresses.
5. All traffic on the zone is typically based only on routable IP protocols, either TCP/IP or UDP/IP. Thus, any non-IP protocol should be dropped.
6. Prevent traffic from transiting directly from the SCADA network to the enterprise network. All traffic should terminate in the DMZ.
7. All outbound traffic from the cell to the enterprise network should be source- and destination-restricted by service and port using firewall rules.
8. Allow outbound packets from the DMZ only if those packets have a correct source IP address assigned to the cell devices.

Devices in the cell zone should not be allowed to access the Internet.

Visibility and Analysis

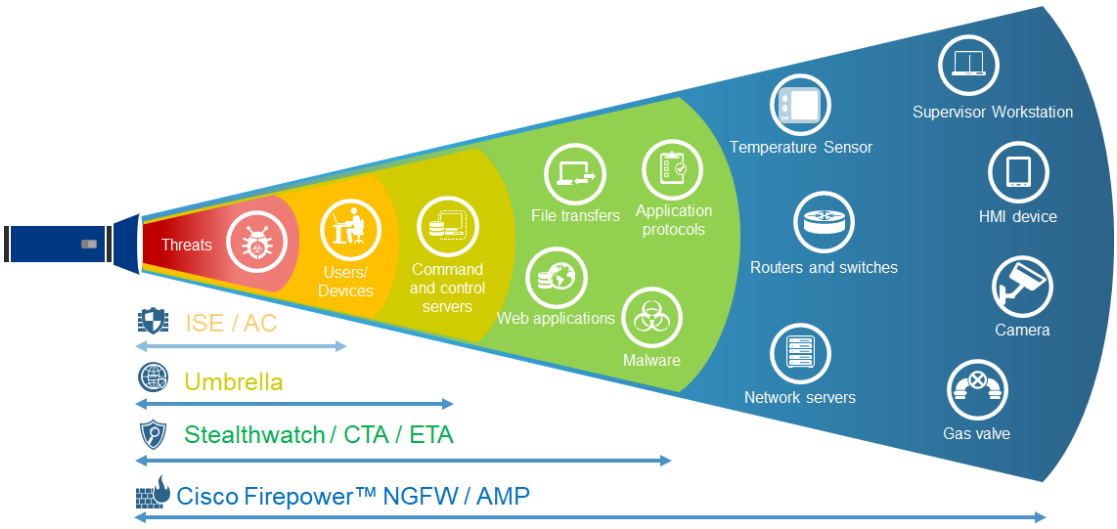
You cannot protect what you cannot see. Visibility across the network and connected devices is achieved via several methods. Within the enterprise and plant operations floors, each capability provides an increasing breadth of visibility and context. They provide visibility and security intelligence across an entire organization before, during, and after an attack. They continuously monitor the network and provide real-time anomaly detection and Incident response forensics.

Capability		Solution Component
	Identity	Cisco Identity Services Engine, Enterprise Directory Services, Cisco AnyConnect, Cisco Industrial Network Director
	DNS Visibility	Cisco Umbrella Secure Internet Gateway
	Intrusion Prevention	Cisco's ASA and Firepower Next Generation Firewalls
	Network Monitoring	Cisco Stealthwatch, network switches, firewalls and routers sending NetFlow.
	Analysis and Anomaly Detection	Cisco Stealthwatch with Cognitive Threat Analytics (CTA), Cisco Firepower, Umbrella Investigate
	Threat Intelligence	Cisco Talos

Return to Contents

To shine a light on threats, different technologies can provide varying depths of visibility.

Figure 7 – Various Depths of Visibility



The following describes the increasing level of visibility provided by each layer of technology.

The Cisco Identity Services Engine (ISE) provides enhanced visibility into who (identities of users and systems) and what (types of devices, including IoT devices) are connecting to your network. It builds contextual elements such as user/device roles, time of day, device posture, and location according to a specific security policy. Each of these contribute to define and enforce role-based access controls used by TrustSec.

Cisco Umbrella provides visibility into with what services IoT devices are communicating, in addition to clientless protection when connecting to the internet. These requests provide detailed insight into authorized and unauthorized communications of these minimally configured and often unmanaged IoT devices. Umbrella's advanced features include Secure Internet Gateway proxy capabilities for questionable domains.

Cisco Stealthwatch turns the network into a sensor, ingesting and analyzes traffic metadata collected as NetFlows from infrastructure and workstations, creating a baseline of the normal IoT communication of an organization and its users. From this baseline, it is then much easier to identify infections or sophisticated attackers infiltrating the network trying to take over. It can identify malware, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and insider threats. It monitors both north-south and east-west (lateral) movements to detect the widest range of attacks, and it can quarantine attackers, leveraging its integration with ISE. With the addition of Cisco Threat Analytics, internet communications are further analyzed to match known or identify new outbreaks.

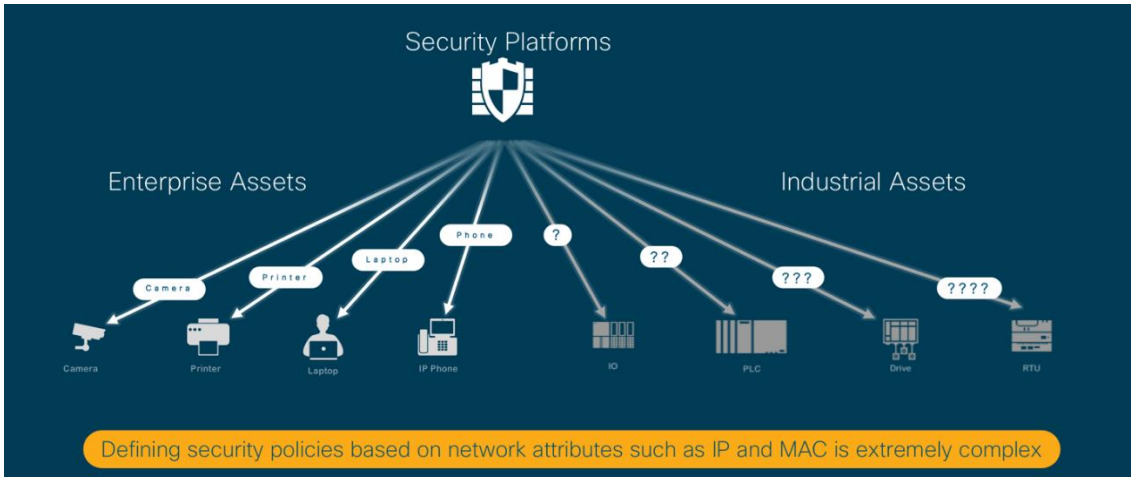
In addition to their segmentation capabilities, Cisco Firepower Next Generation Firewalls and Next Generation Intrusion Prevention Systems provide the deepest level of visibility by performing deep-packet protocol and payload inspection. They form the anchor point for converging IT and OT security without interfering with industrial operational practice. With their integrated network discovery, you have visibility into everything entering and exiting the industrial zone, from which granular security policies can be created and enforced. They uniquely see endpoint apps and operating systems, OT devices, and corresponding browsers, all while detecting the latest and most advanced forms of malware.

These enhanced visibility agents enable greater threat detection and more granular control of policies for your entire network environment: plant, mobile, and remote locations.

OT Security Challenge

The challenge in industrial environments is that most OT endpoints do not have ability to communicate their identity to the Network Infrastructure or Security platforms in the same way as IT endpoints do using 802.1x supplicants or other means.

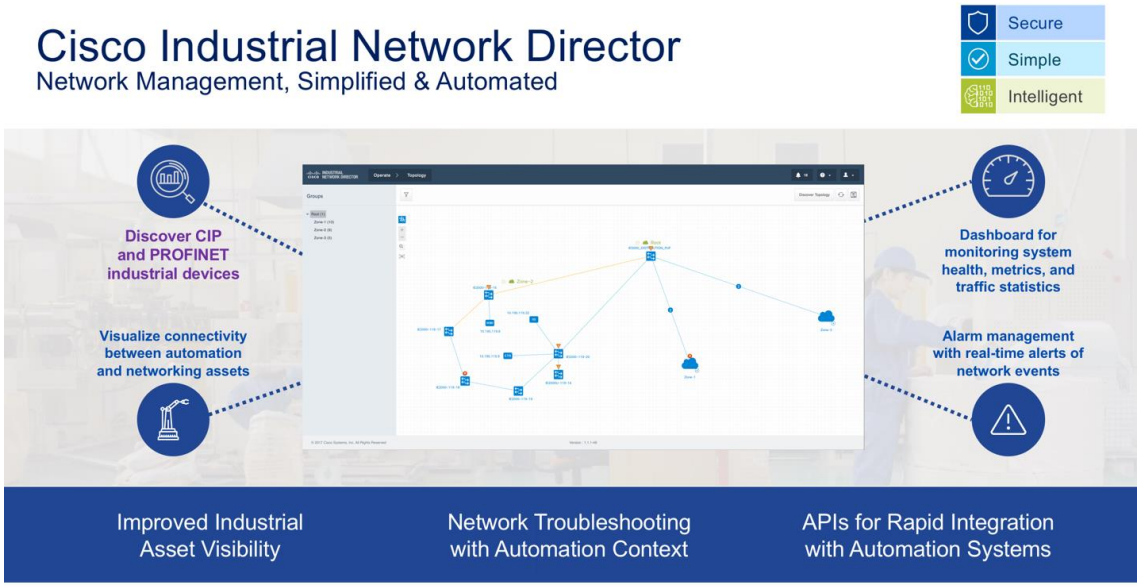
Figure 8 – IoT vs IT device identity challenge



When IT security platforms like the Cisco Identity Services Engine(ISE) do not receive the contextual information necessary to consistently apply security policies, this can lead to disruption of communication in the OT network and in turn lead to failure in the OT process.

Cisco Industrial Network Director (IND) is a purpose-built platform for managing industrial networks and ties the identity and context elements back in to Cisco ISE. It is designed to help operations teams gain full visibility of network and automation devices in the context of the automation process and provides improved system availability and performance, leading to increased overall equipment effectiveness (OEE).

Figure 9 – Cisco Industrial Network Director



Secure Remote Access

Increased connectivity has arguably more benefits than drawbacks, so it's no surprise that many equipment vendors, such as industrial and healthcare equipment vendors, require remote support in their support contracts. It saves the vendor's operational costs when they do not need to send a technician on-site, and remote support can reduce downtime for customers as the technician gets to work while still on the phone with the customer.

Capability		Solution Component
	Identity	Cisco Identity Services Engine, Enterprise Directory Services
	VPN	Cisco AnyConnect, Cisco's ASA and Firepower Next Generation Firewalls
	Anti-Malware	Cisco's Advanced Malware Protection for Endpoints and Networks

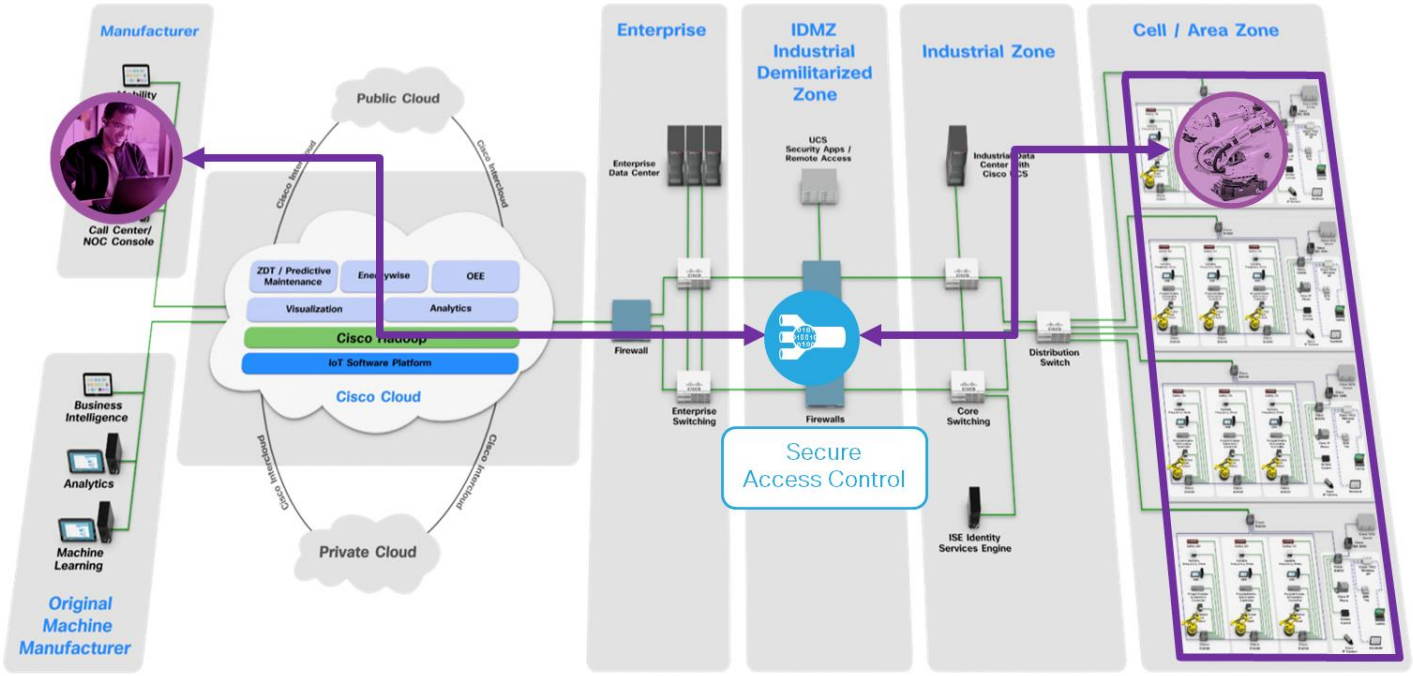
With a younger workforce and fewer experienced workers available, particularly for older systems and infrastructure, ensuring that the right resources are available in the right place and at the right time is challenging and often not possible. Companies may need a number of subject matter experts from different disciplines to collaborate on situations in real time—and they may want to avoid the expense of having to wait for them all to travel to the same location.

There are several drawbacks for the customer:

1. Remote access means that sensitive networks, such as an industrial control network, can be reached from the Internet.
2. Customers have equipment from multiple vendors, which means access needs to be granted for each of the vendors.
3. Customers often have no idea what devices are actually communicating with in the customer's environment or even whether the vendor's network is introducing security threats into the customer's network.

IoT Threat Defense provides secure communications from the remote party to the network and employs segmentation, visibility, and analysis to make sure remote users do not introduce threats but access only the systems for which they are allowed access.

Figure 10 – IoT Threat Defense Secure Communications

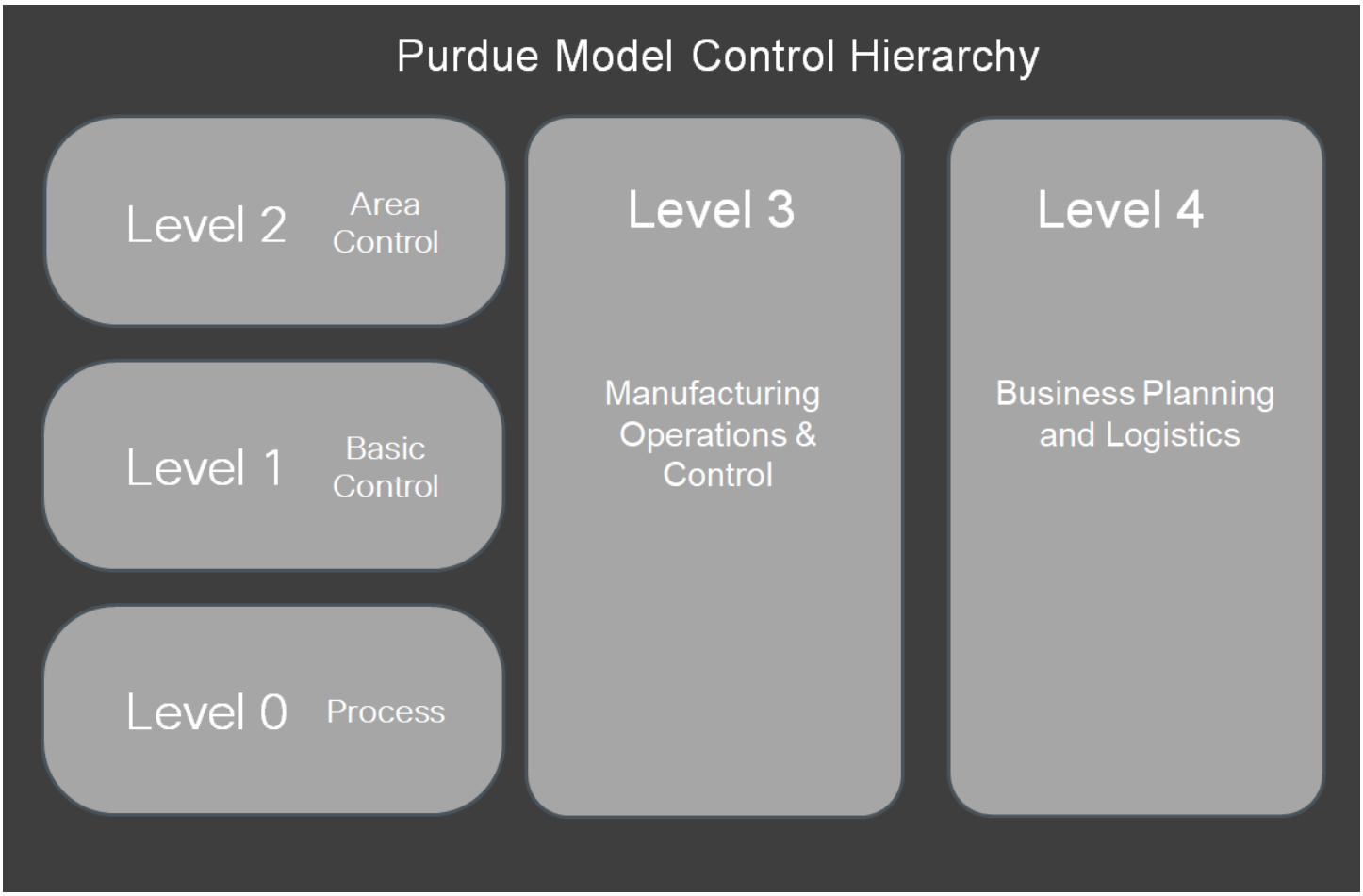


Return to Contents

Purdue Model for Control Hierarchy

Manufacturing OT staff recognized the need to connect their infrastructure to today's IT systems. This convergence of IT and OT is a common challenge being faced by most industries adopting IoT architectures, and it requires both OT and IT to have communication interfaces that allow mutual access and the exchange of information between systems. The interaction of these components in such a complex system requires a framework to define the flow of communication between components, which are dependent on the functions they perform in the process. A well-known framework used by many industries today is the Purdue Model for Control Hierarchy as shown in Figure 11.

Figure 11 – Purdue Model for Control Hierarchy



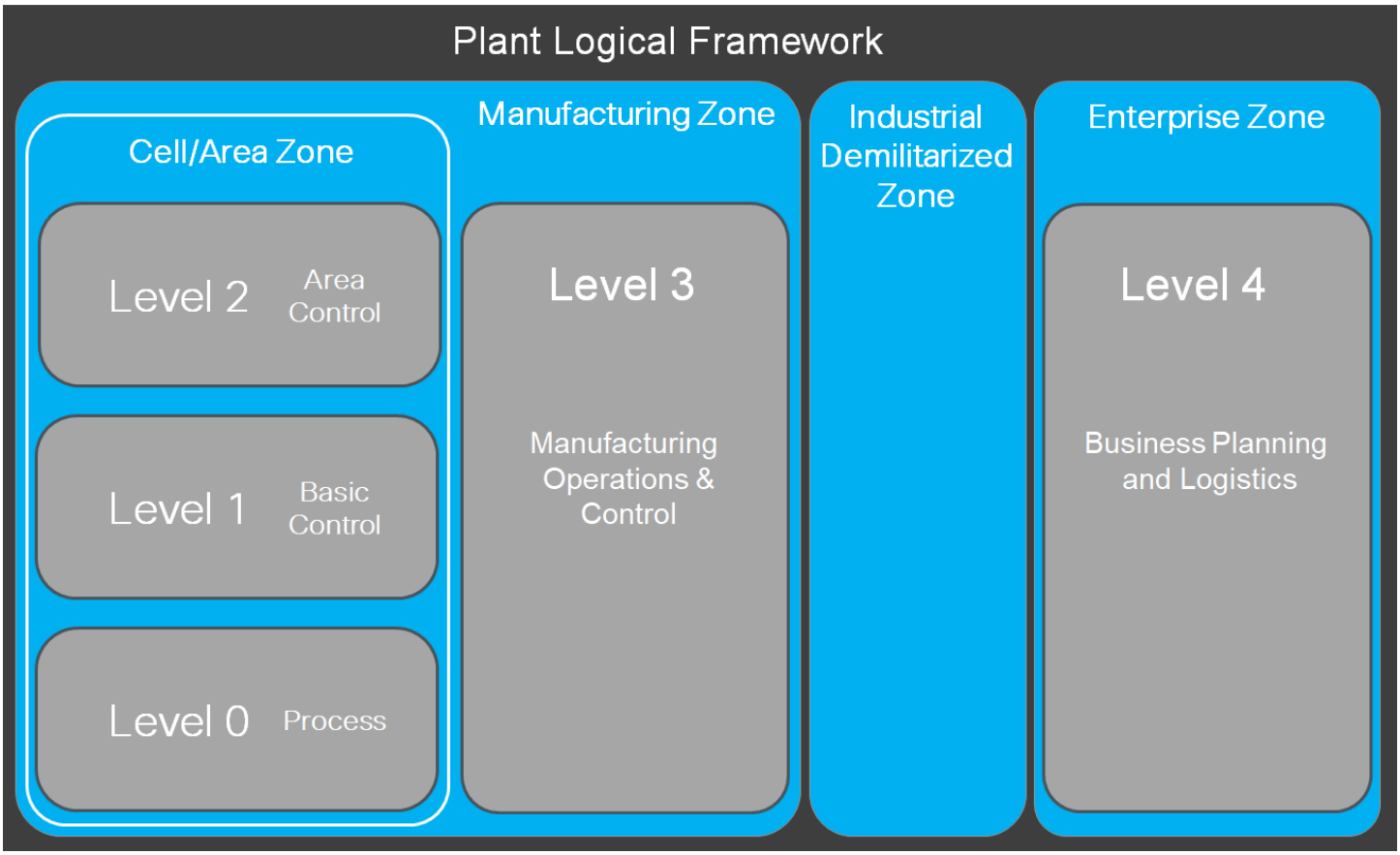
The Purdue Model for Control Hierarchy[2] is a common and well-understood model in the manufacturing industry that segments devices and equipment into hierarchical functions. It has been incorporated into many other models and standards in the industry.

[2] Reference ISBN 1-55617-265-6

Return to Contents

Based on this segmentation of the plant technology, the International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security (IACS) has identified the levels and logical framework zones as the Plant Logical Framework.

Figure 12 – Plant Logical Framework



The Purdue Model and ISA-99 have identified levels of operations and key zones for the IACS logical framework. In addition to the levels and zones, Cisco and Rockwell Automation include a demilitarized zone (DMZ) between the Enterprise and Manufacturing zones as part of Converged Plantwide Ethernet (CPwE) architecture. Emerging IACS security standards such as ISA-99, NIST 800-82, and Department of Homeland Security INL/EXT-06-11478 also include a DMZ as part of a defense-in-depth strategy. The purpose of the DMZ is to provide a buffer zone where data and services can be shared between the Enterprise and Manufacturing zones. The DMZ is critical in maintaining availability, addressing security vulnerabilities, and abiding by regulatory compliance mandates (e.g., Sarbanes-Oxley). In addition, the DMZ allows for segmentation of organizational control; for example, between the IT organization and manufacturing. This segmentation allows different policies to be applied and contained. For example, the manufacturing organization may apply security and quality-of-service (QoS) policies that are different from the IT organization. The DMZ is where the policies and organizational control can be divided.

These levels and zones form the base logical framework around which the IACS network infrastructure and services are designed and used for Cisco's CPwE Cisco Validated Design.

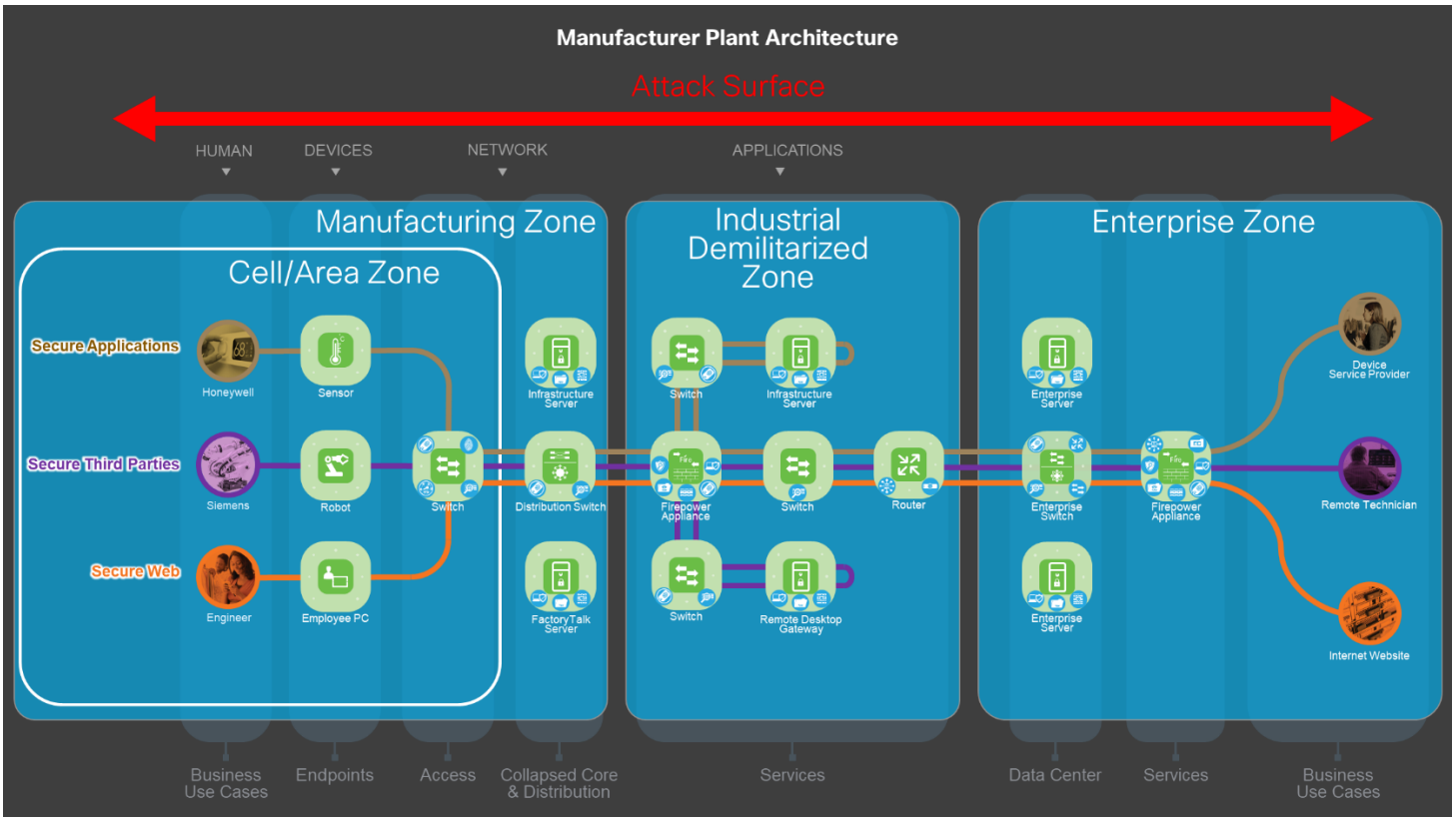
Return to Contents

Plant Architecture

The CPwE integrates the knowledge and expertise from both IACS as well as IT. The Cisco Enterprise Campus is the most relevant model for network architectures in this environment. The Enterprise Campus solution architecture incorporates key networking concepts and models; core, access, distribution, and services layers. In essence, the IACS network can be viewed as a specialized Campus network.

The IoT Threat Defense solution starts with the CPwE Cisco Validated Design and improves it with additional Segmentation, Visibility and Remote access elements. Using the SAFE Campus Reference Architecture and IoT Threat Defense business flows, we can easily show how the end-to-end architecture as shown in Figure 13 can include both IT and OT models, and the deployment of the capabilities protecting the flows.

Figure 13 – CPwE Reference Architecture in SAFE Format with Business Flows



Cell/Area Zone

The Cell/Area zone is a functional area within a plant facility; many plants have multiple Cell/Area zones. In an automotive plant, it may be a bodyshop or a sub-assembly process. In a food and beverage facility, it may be the batch mixing area. It may be as small as a single controller and its associated devices on a process skid, or multiple controllers on an assembly line. Each plant facility defines the Cell/Area zone demarcation differently and to varying degrees of granularity. For the purposes of this architecture, a Cell/Area zone is a set of devices, controllers, and so on, which are involved in the real-time control of a functional

aspect of the manufacturing process. To control the functional process, they are all in real-time communication with each other.

Cell zones contain the endpoints and access layer capabilities. Cell zones should be segmented from each other using TrustSec, VLAN's or firewalls, and highly sensitive plants may require segmentation within the cell itself using TrustSec or dedicated firewalls. Devices are profiled when connected to the network, ensuring they are placed in the proper policy/security group. Visibility of traffic to, from and within a cell is important to capture and monitor, enabling quick identification of problems or new threats.

Manufacturing Zone

The Manufacturing zone consists of the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. The Manufacturing zone is important because all the applications, devices, and controllers critical to monitoring and controlling the plant floor operations are in this zone. To preserve smooth plant operations and functioning of the applications and network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the plant/enterprise operations.

Cell zones are aggregated together at the Manufacturing Zone following best practice access to distribution layer connectivity and segmentation methods found in campus networks. Segmentation using TrustSec, and Visibility with Netflow are equally important here as the majority of operational communications are sourced from here, and this zone also contains many vulnerable older operating systems.

Industrial Demilitarized Zone

The Demilitarized Zone provides a buffer zone where services and data can be shared between the Manufacturing and Enterprise zones. In addition, the DMZ allows for easy segmentation of organizational control. Cisco recommends that the DMZ be designed so that no traffic traverses the DMZ. All traffic should originate/terminate in the DMZ. This chokepoint also provides the best place for gaining visibility with deep pack inspection of all traffic in and out of the plant.

Enterprise Zone

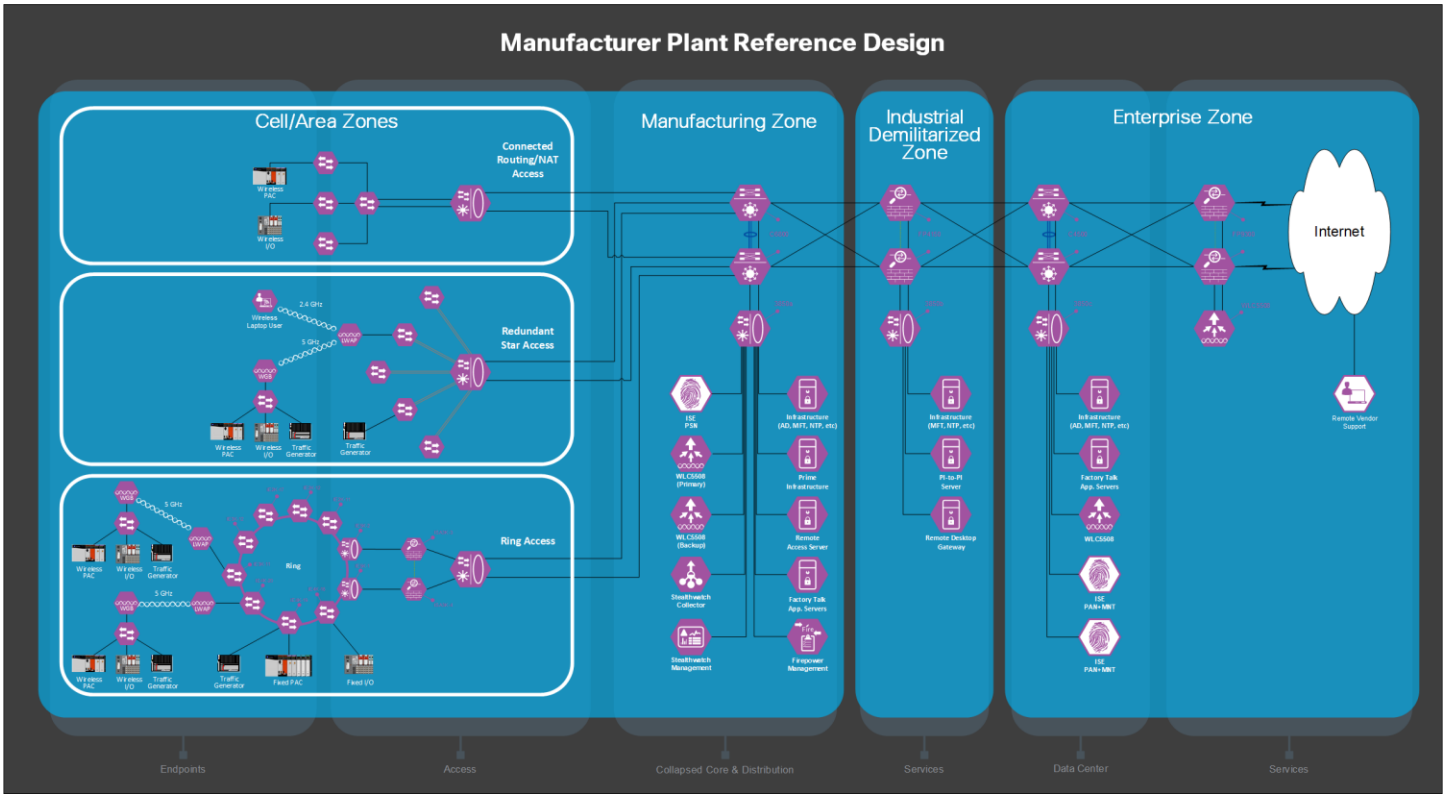
The Enterprise Zone is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. These functions and systems include wired and wireless access to enterprise network services.

It is also where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level. Often the external partner or guest access systems exist here, although it is not uncommon to find them in lower levels (e.g., Level 3) of the framework to gain flexibility that may be difficult to achieve at the enterprise level.

Plant Design

Moving from architecture to design is now greatly simplified when we understand where the capabilities are intended to be implemented. It requires selecting only the appropriate hardware with the necessary capability to feature mapping. Additional elements such as high-availability, resiliency, and scalability are now also taken into consideration. Figure 14 represents the reference design used in manufacturing plants.

Figure 14 – Manufacturer Plant Reference Design



Additional detailed lab diagrams Figure 36 and Figure 37 can be found in the appendix.

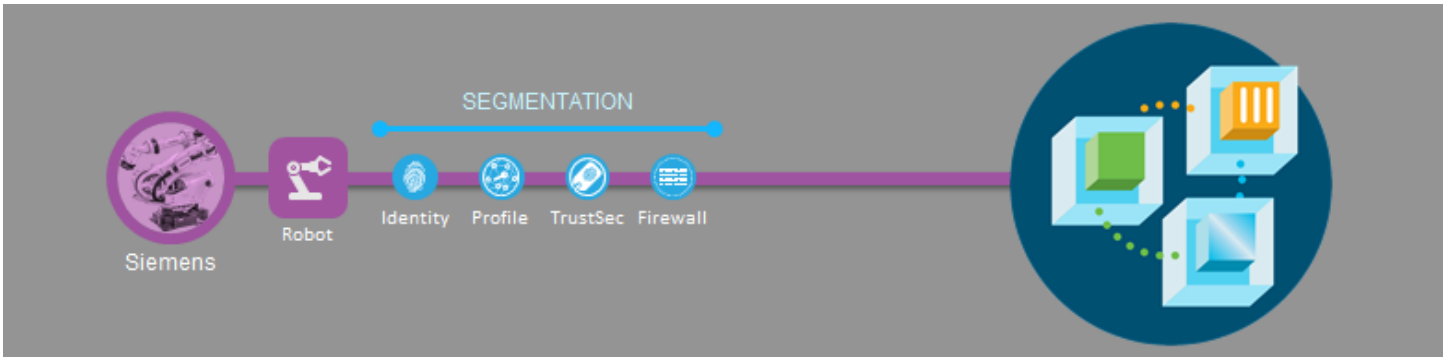
More information on CPwE can be found here: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/design-guide-listing.html

Return to Contents

Implementation

Each of the product sections describes how they were customized after a typical installation to best defend your company's IoT infrastructure. A tabular listing of all products and their versions is available in the appendix.

This solution requires enterprise-wide time synchronization with NTP, and recommends a CA Server for pxGrid certificates.



Identity Services Engine (ISE)

Authenticating users and devices as they connect to the network infrastructure is the first line of defense for protecting the company. It is the opportunity to segment known from unknown, trusted from untrusted. The contextual information gathered from the network provides visibility to users, devices, and other desired elements. This context nicely ties the identity to a device, and is used as conditions for policy enforcement.

This guide focuses on how to configure ISE for connecting IoT devices, and at a high level, users. Information on how to deploy ISE, and alternate configurations can be found here:

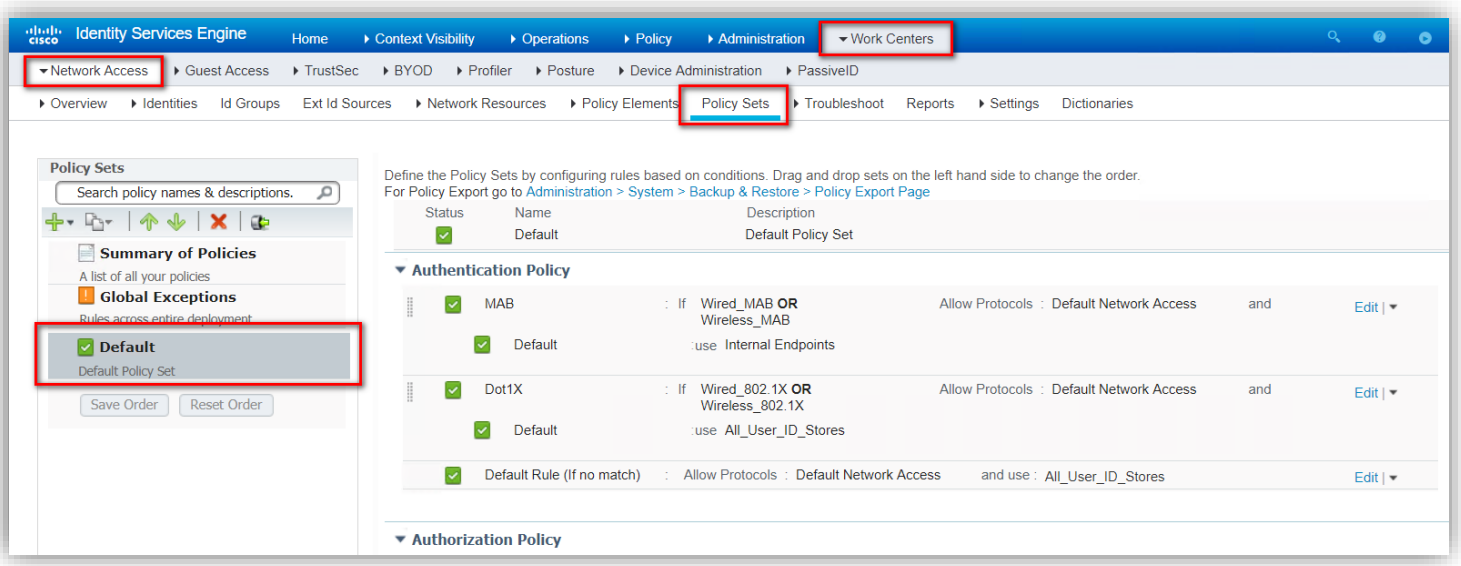
https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html

And here: https://communities.cisco.com/community/technology/security/pa/ise

Configuring Network AAA

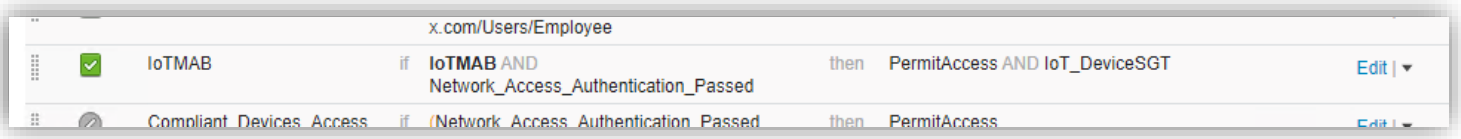
In manufacturing environments, the majority of IoT devices are connected via wired network connections due to the deterministic timing requirements of many control systems. However, these devices often do not support implementation or configuration of traditional network authentication standards such as 802.1x (Dot1x). For this reason, MAC Authentication Bypass (MAB) is used, which relies on the device's manufacturer assigned hardware MAC address for authentication.

ISE is an Authentication, Authorization and Accounting (AAA) server. This means you need to authenticate and authorize users and devices to get onto the network. In ISE, the authentication policy for MAB is turned on by default. Navigate to **WorkCenters > Network Access > Policy Sets** to view and edit these policies. In the screenshot below, a default policy set is used.



As shown in the default authentication policy, ISE first looks at a device's MAC address and tries to match it to a known manufacturer's MAC address to pass the authentication phase. These Internal Endpoints can be found under the **Administration > Identity Management > Groups** menu.

The next step is to authorize the users and devices. In our case, as in the screen below, we are profiling the endpoint and adding it to an endpoint group (e.g., IoTMAB or Siemens Device). We will look at how to do this later, but for now just think that the device is identified as an IoT device and added to an endpoint group. You can see the context being included as a condition in authorization rules. This is done by checking whether the device is part of IoTMAB endpoint group, and in making sure that the network authentication was successful. If so, the device is classified with a corresponding security group tag (SGT), a 16-bit number created for a single or group of assets.



A new IoT device can be identified in two ways:

1. By manually adding the MAC address of devices into an endpoint group or by importing using csv
2. By ISE profiling functionality

By adding a device to an endpoint group, a device becomes a known device. These devices can be assigned a security group tag as shown in the screenshot above. Unknown devices can be profiled, and ISE can detect these devices as controllers, cameras, printers, and other devices. When devices are unknown and not correctly profiled initially, you can add an authorization policy to restrict network access for these devices. After the device is fully profiled, it could be automatically added to an appropriate group that authorizes to a different segment appropriate for its role, as in the IoTMAB example.

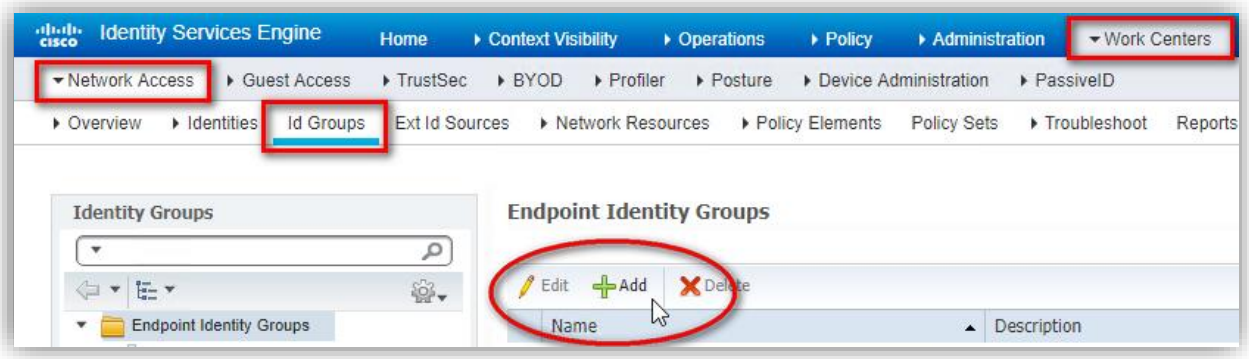
↩Return to Contents

NOTE:

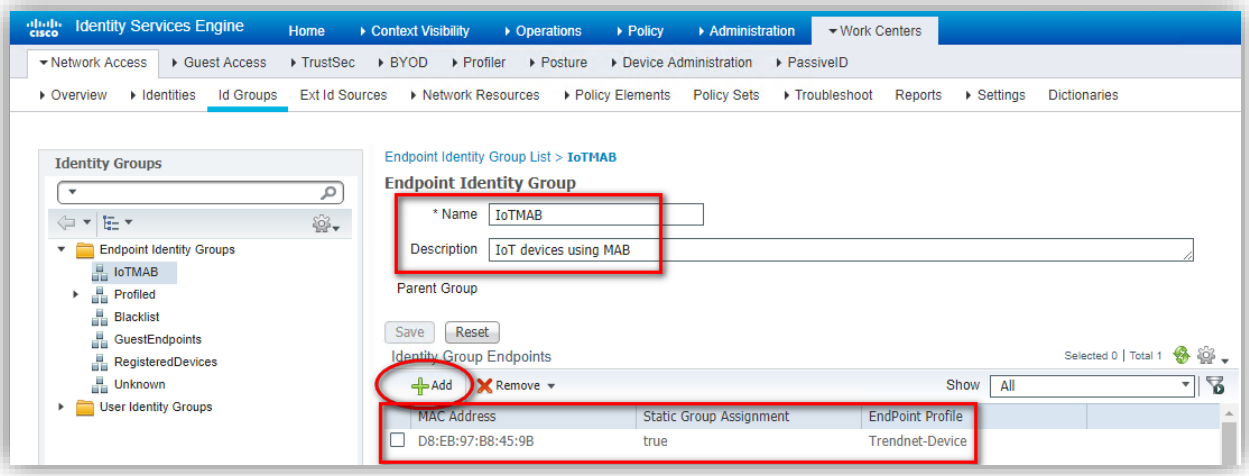
More on profiling can be found in the *ISE Profiling Design Guide*:
https://communities.cisco.com/docs/DOC-68156

For IoT devices that require MAB, add an authorization policy that permits access for IoT devices added to a specific Endpoint Identity Group.

Step 1: Create an Endpoint Identity Group called IoTMAB and add the device MAC addresses as appropriate. Select **Work Centers > Network Access > Id Groups** and click **Add**.



Step 2: Enter a group name and description. Click **Save**. Click **Add** and select the device MAC address from the list of learned endpoints.



For this use case, we are just creating a new endpoint group based on the MAC address, and then use the endpoint group in the authorization policy. You can see that the endpoint group is automatically associated with an Endpoint Profile (Trendnet-Device).

ISE uses the OUI information in the MAC address to match a profile to a device. It also uses information gathered from these IoT devices to match it to a profile. In our case, since we are using a white-listing of devices based on endpoint group, we should be ready now to identify and authorize the device.

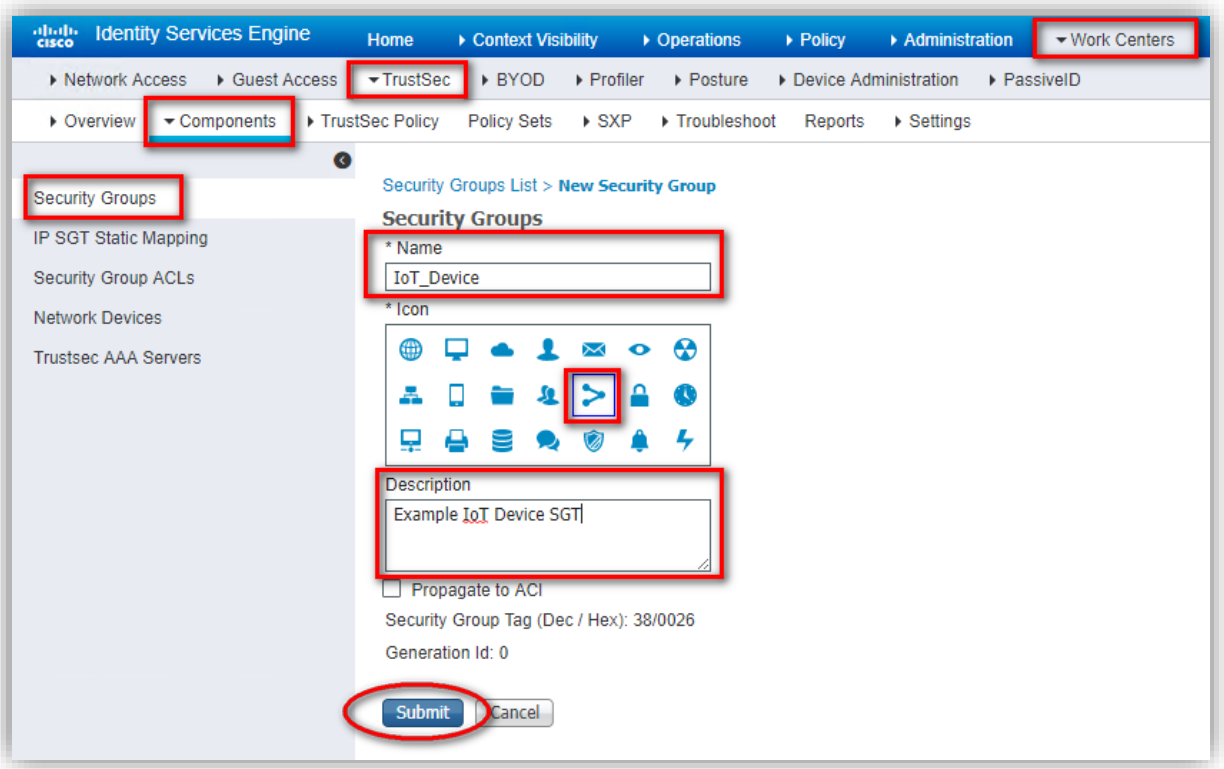
Another approach to identify devices is to use the ISE profiler service. Profiles for known devices are continually added via a feed from the Cisco cloud. To use this feature, you need to turn on the feed services in ISE. Navigate to **Work Centers > Profiler > Feed Service** to enable it.

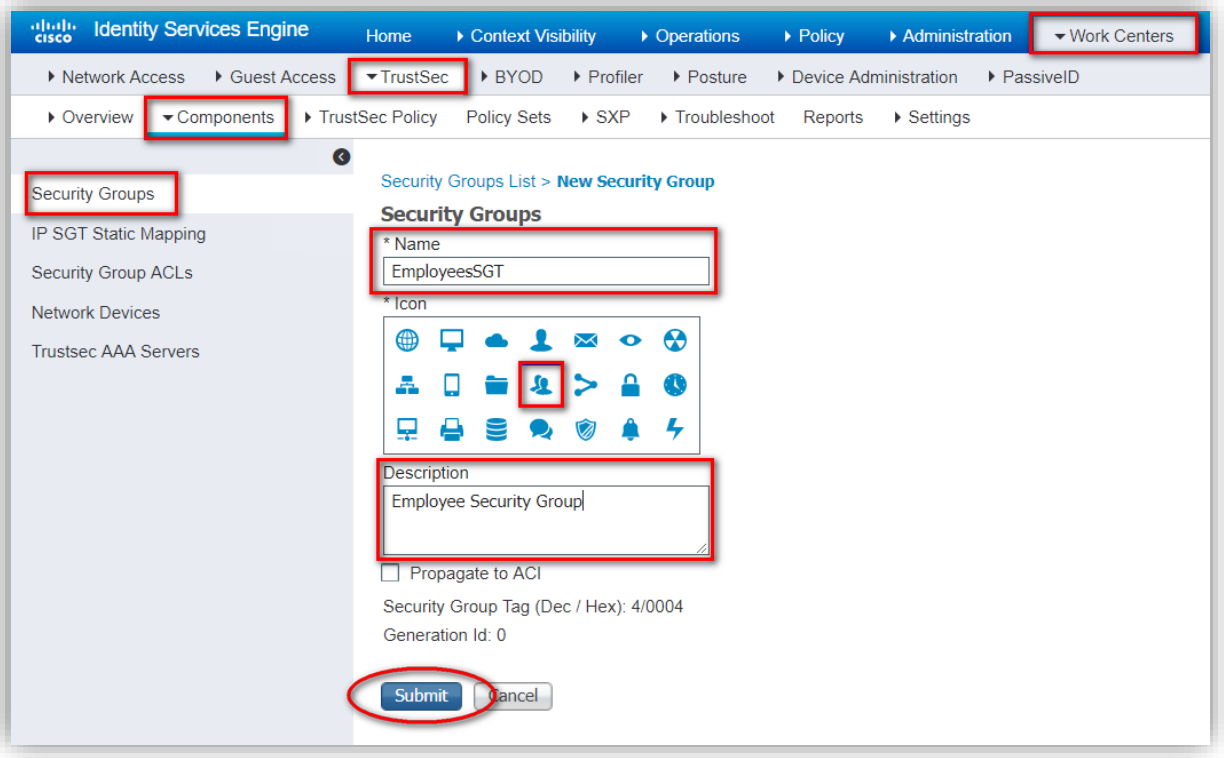
The profiler service is more dynamic in nature, so you don't need to whitelist the MAC address of the devices. Rather, ISE classifies the device and adds it to the appropriate Endpoint profile. These Endpoint profiles are

categorized based on vendor, device type, and so on, and are exposed via authorization policy conditions when you create an authorization policy using them.

For more details, please see the ISE Profiling Design Guide: https://communities.cisco.com/docs/DOC-68156

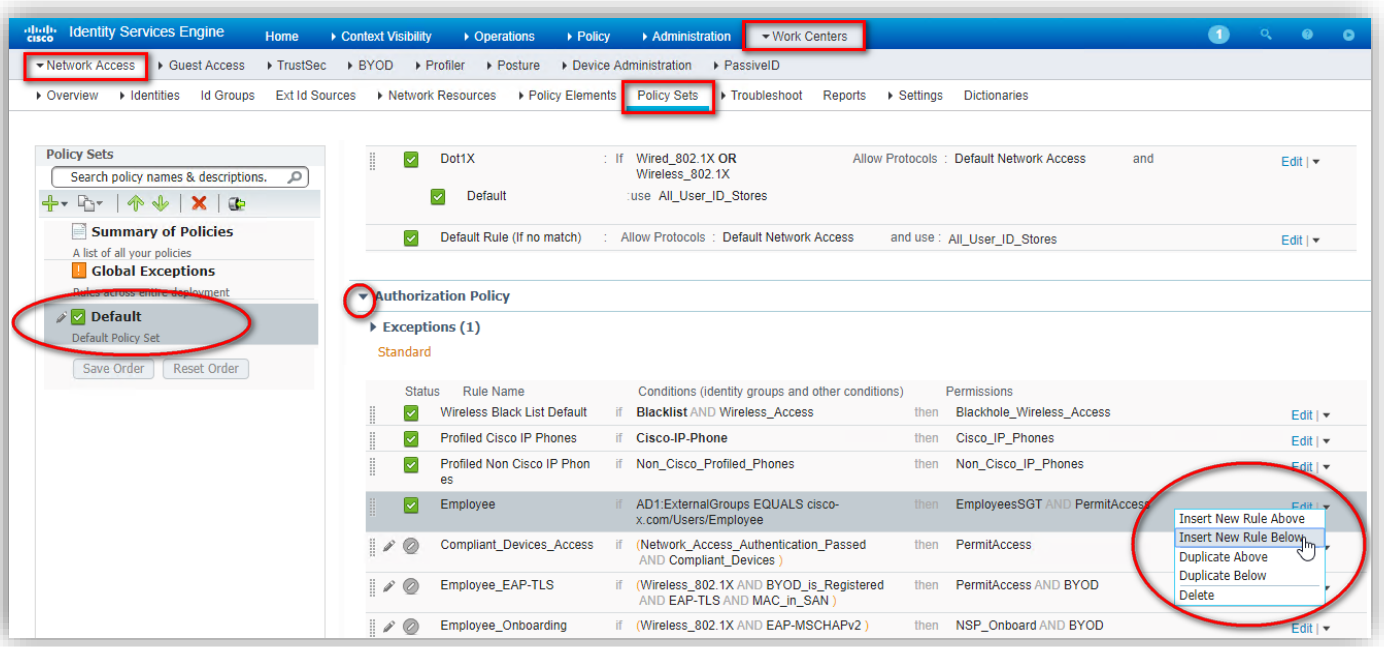
Step 3: Create Security Groups for your IoT devices, users, and systems. Choose **Work Centers > TrustSec > Components > Security Groups**. Click **Add** to add a new security group. Enter a name, icon, and description (optional) for the new security group. Click **Submit**.



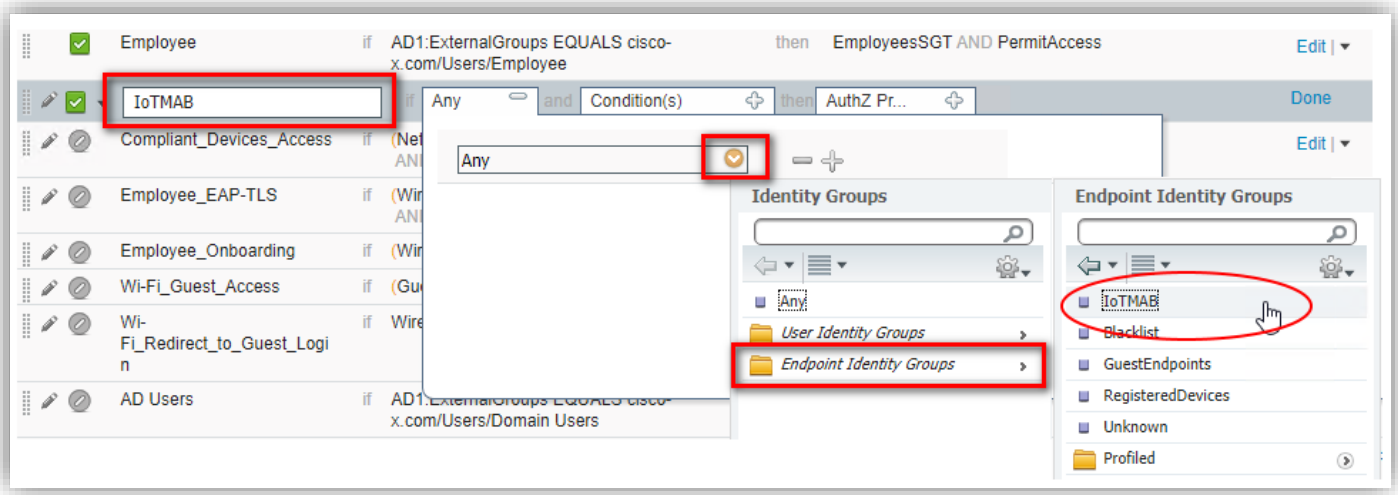


Return to Contents

Step 4: Create an Authorization rule to match the IoTMAB endpoint group and assign permissions and security group tags. Select **Work Centers > Network Access > Policy Sets.** Select **Default** under the policy sets on the left. Expand **Authorization Policy** and click the right side arrow to insert a new rule below the last active rule.

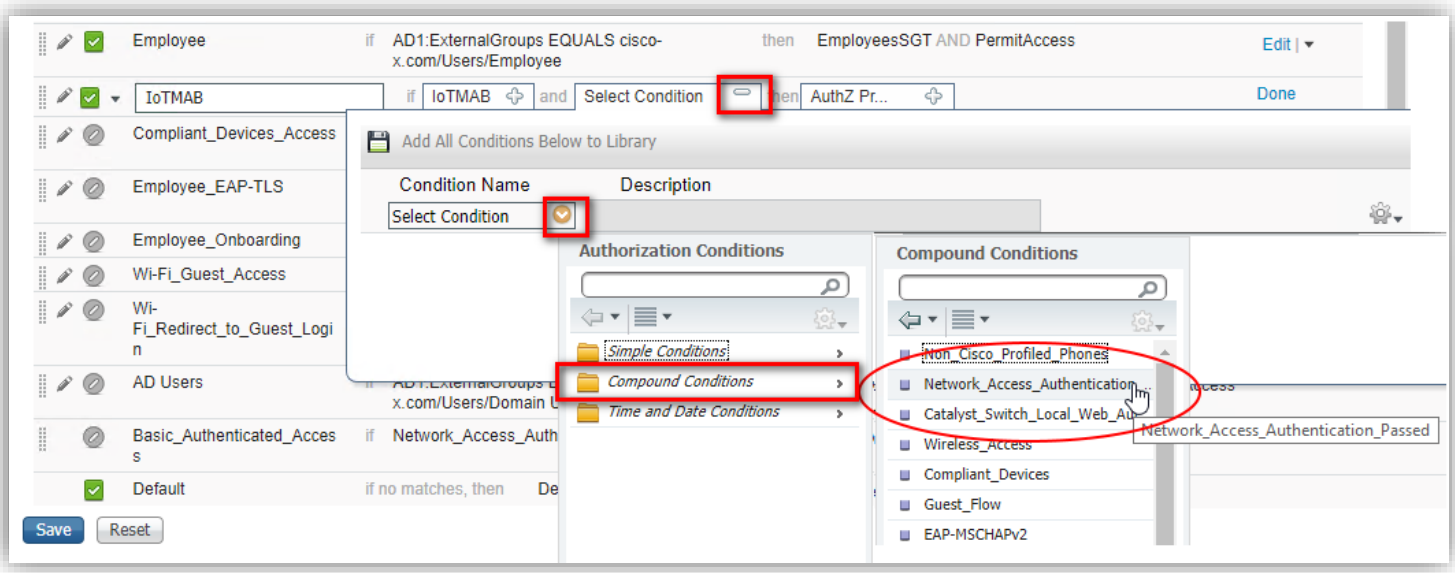


Step 5: Give the rule a name, and then select the endpoint identity group.

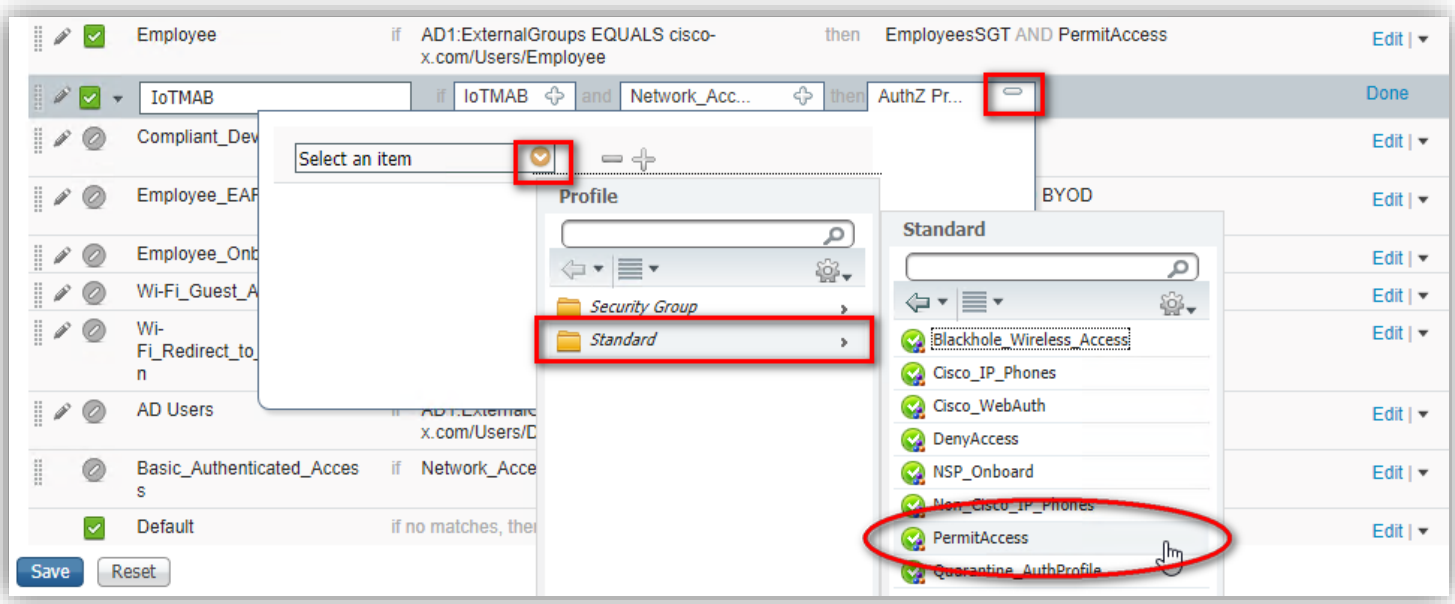


Return to Contents

Step 6: Select a compound condition from the library for Network_Access_Authentication_Passed.

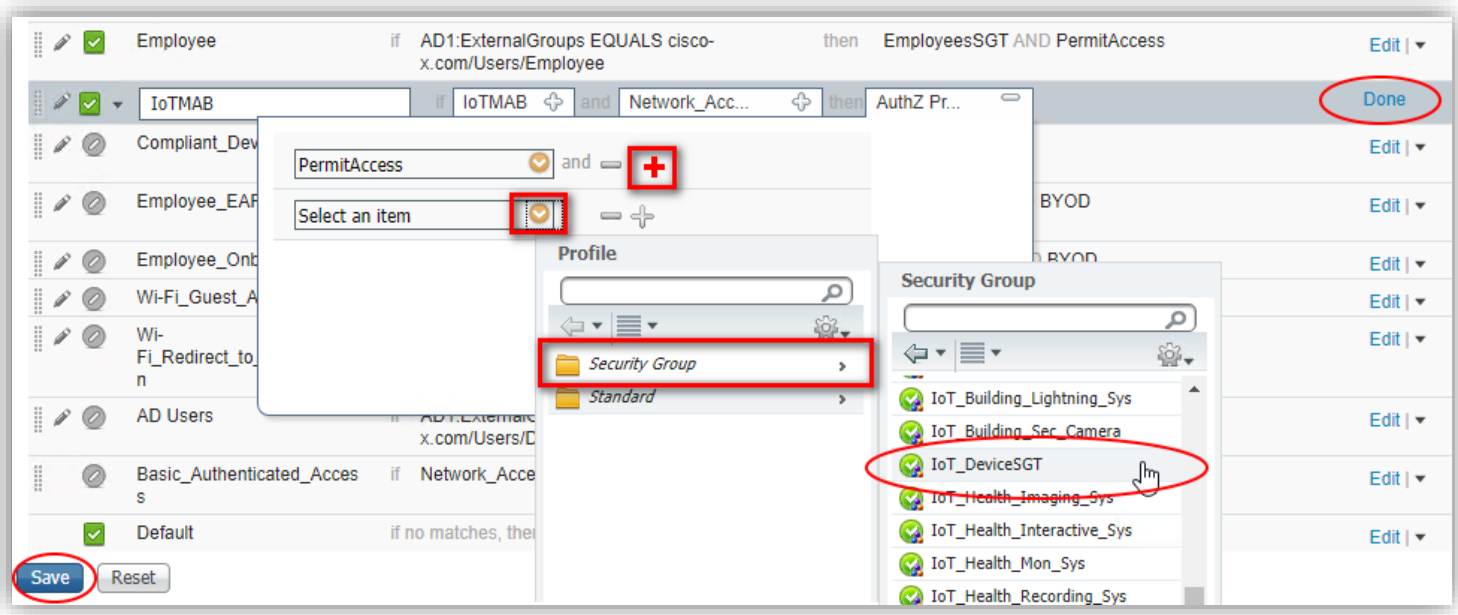


Step 7: Assign the standard permissions to Permit Access.



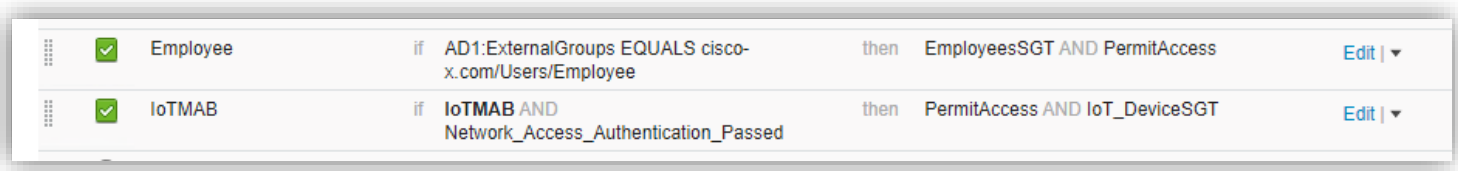
Return to Contents

Step 8: Click the "+" and assign the security group tag as the second permission. To finish editing, click **Done** and **Save**.



Repeat Steps 4 through 8 to add an authorization policy for dot1x authenticated users of a specific user identity group that would need access to the IoT devices. ISE supports internal and external identity stores for validating users such as Active Directory, LDAP, ODBC, and so on.

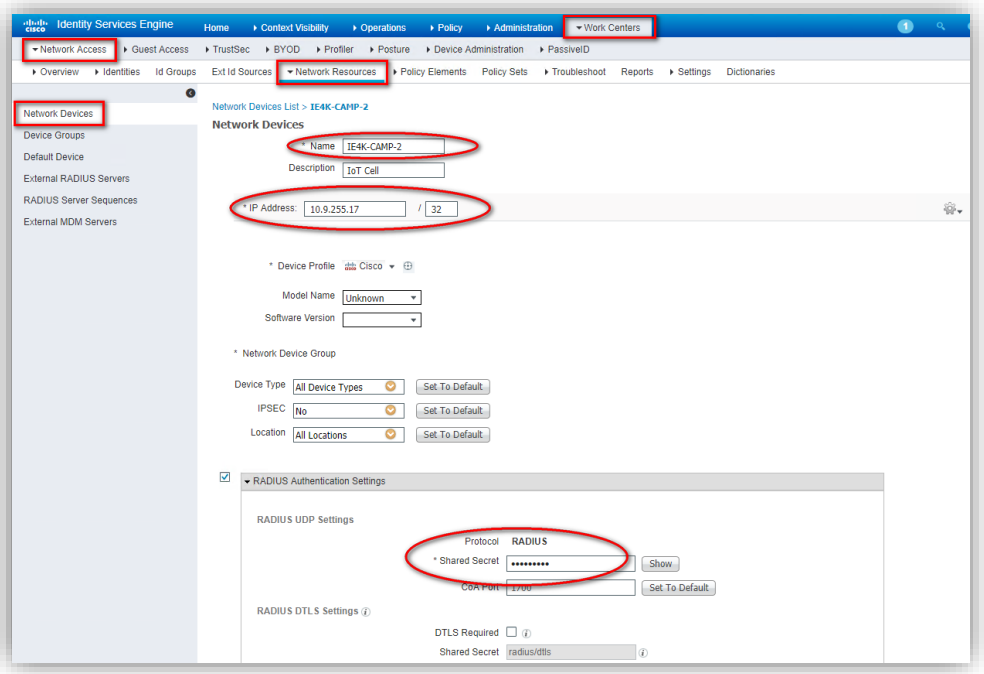
The dot1x authenticated user group in this example is verified against Active Directory. After specifying the identity, assign an appropriate SGT and access policy.



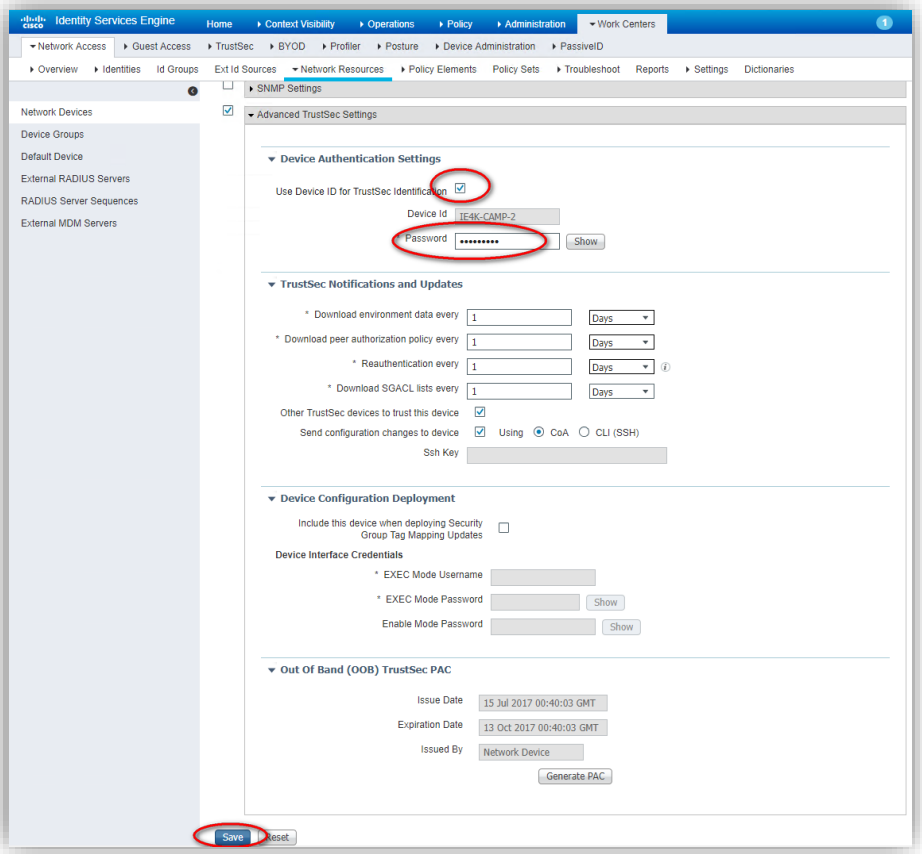
NOTE:

For details how to add an external identity store and use that in authentication/authorization policies, visit:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/ise_active_directory_integration/b_ISE_AD_integration_2x.html

Step 9: Add switches, firewalls and routers to ISE that will authenticate devices and users. Select **Work Centers > Network Access > Network Resources > Network Devices.** Click **Add**. Enter the name, IP address, and description (optional). Set the RADIUS shared secret, which will be the password used in the network device configurations.



Step 10. Scroll down and set the TrustSec device ID to use the device name. Set the password to be used for authentications. Click **Save**.



Return to Contents

AAA Switch Configuration

Each switch must be configured to communicate with the ISE AAA server for authorizing IoT devices, users, and other systems. A best practice is to do this end-to-end across the company, enabling the most comprehensive view of what is connected to the network.

The following configurations are performed via the command line interface (CLI) of the device for simplicity and consistency across a broader range of similar devices.

CONFIGURE RADIUS AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

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

```
ip radius source-interface Loopback0

aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

Step 2: 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 3: Configure the RADIUS Server, IP address, and shared secret that was entered in ISE.

```
radius server ISE01
 address ipv4 10.9.10.51 auth-port 1812 acct-port 1813
 pac key Cisco1234
```

Step 4: Configure the AAA group name for RADIUS and specify the server created in Step 3.

```
aaa group server radius ISE
 server name ISE01
```

Step 5: Configure the default authentication, authorization, and accounting to use the group created in Step 4.

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting update periodic 2880
aaa accounting dot1x default start-stop group ISE
```

Step 6: Enable ISE to automatically send policy updates to the switch when there is a change of authorization (COA). Enter the password specified in the ISE device configuration for Advanced TrustSec settings. This facilitates a bounce, re-authentication, or disabling of a switch port.

```
aaa server radius dynamic-author
 client 10.9.10.51 server-key Cisco1234
```

Step 7: Globally enable port-based authentication.

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

Step 8: Globally enable device tracking. This facilitates including the device IP address in RADIUS requests to ISE for authentication, enabling TrustSec IP-to-SGT mapping.

```
ip device tracking
```

Step 8b: For newer switch software versions, the `ip device tracking` command has been deprecated and functionality replaced with `device-tracking`. Enable tracking and create a policy that will later be applied to the switch interfaces.

```
device-tracking tracking
!
device-tracking policy IPDT
 tracking enable
```

NOTE:

For more information on IPDT best practices and workarounds, please visit: https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html

Step 8c: For switches with operationally critical systems, bounce and disable commands can be overridden and ignored with these configurations.

```
authentication command bounce-port ignore
authentication command disable-port ignore
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

ENABLE PORT AUTHENTICATION PER PORT

On the switch, the following configurations enable port-based authentication and IP device tracking. Configure each interface that will have an endpoint device connected. The dot1x method offers a secure way of authenticating users and mobile devices/workstations that have supplicant software. This software opens a secure communication session from the device to ISE. MAB is used for devices that do not have supplicants such as controllers, cameras, printers, and

other legacy IoT devices in operation. It is desirable in many deployments to be able to disconnect a device and connect an employee or vendor system for testing. To support this functionality both MAB and dot1x can be enabled. 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

Step 9: Add the following configurations to each device interface:

```
interface range GigabitEthernet1/0/1-24
 device-tracking attach-policy IPDT
 authentication event fail retry 0 action next-method
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

NOTE:

The **port-control auto** command is what activates enforcement, and can be added or removed for testing. Alternatively, **authentication open** enables monitor mode and could be used to test implementations without disrupting active operations.

38 TrustSec

Configuring TrustSec throughout the company involves several steps. First, define policies for which assets are allowed to communicate to other assets. These assets are the source and the destination of data traffic. An asset can be a group or a single entity based on how it is categorized. An SGT is given to these assets to classify them into categories.

Policies that use these security group categories are created separately in both ISE and firewall policy managers (e.g., Firepower Management Center, ASA Security Device Manager, Cisco Security Manager). After the desired policies are defined, each system is configured to share the SGT-to-IP address mappings information using the Security Exchange Protocol (SXP). Some environments, such as those with Industrial Ethernet Switches, require inline tagging of packets in addition to participation in SXP. Inline tagging modifies each packet, and adds the appropriate SGT. This information is then used for policy decisions by the next connected device as long as it trusts the tagged packets it receives. Enforcement is enabled on switches and firewall interfaces.

Sharing security information between multiple products means that IT security teams can find answers faster, without having to conduct lengthy and time-consuming investigations. So when a threat is detected, all of the technologies you see here work together to provide rapid threat containment. ISE is instructed to contain the infected endpoint either manually or automatically. This containment can involve moving the device to a sandbox for observation, moving it to a remediation domain for repair, or removing it completely. ISE then automatically updates the endpoint's access policy to one that's more restricted, effectively quarantining the endpoint from the network. The device can then be remediated or completely blocked from accessing the network.

The Cisco Platform Exchange Grid (pxGrid) provides a secure channel for Cisco and non-Cisco products to gather contextual information from ISE, and send specific instructions to ISE (e.g., to quarantine a device). For threat containment, it is essential to enable pxGrid services in ISE, and allow ISE-to-Firepower and ISE-to-Stealthwatch communication to happen.

Steps to install pxGrid can be found in the following guides;

- Rapid Threat Containment Design guide: https://communities.cisco.com/docs/DOC-68293
- How to Integrate Firepower and ISE via pxGrid: https://communities.cisco.com/docs/DOC-70354

The latest TrustSec Platform Capability Matrix can be found here:

https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html

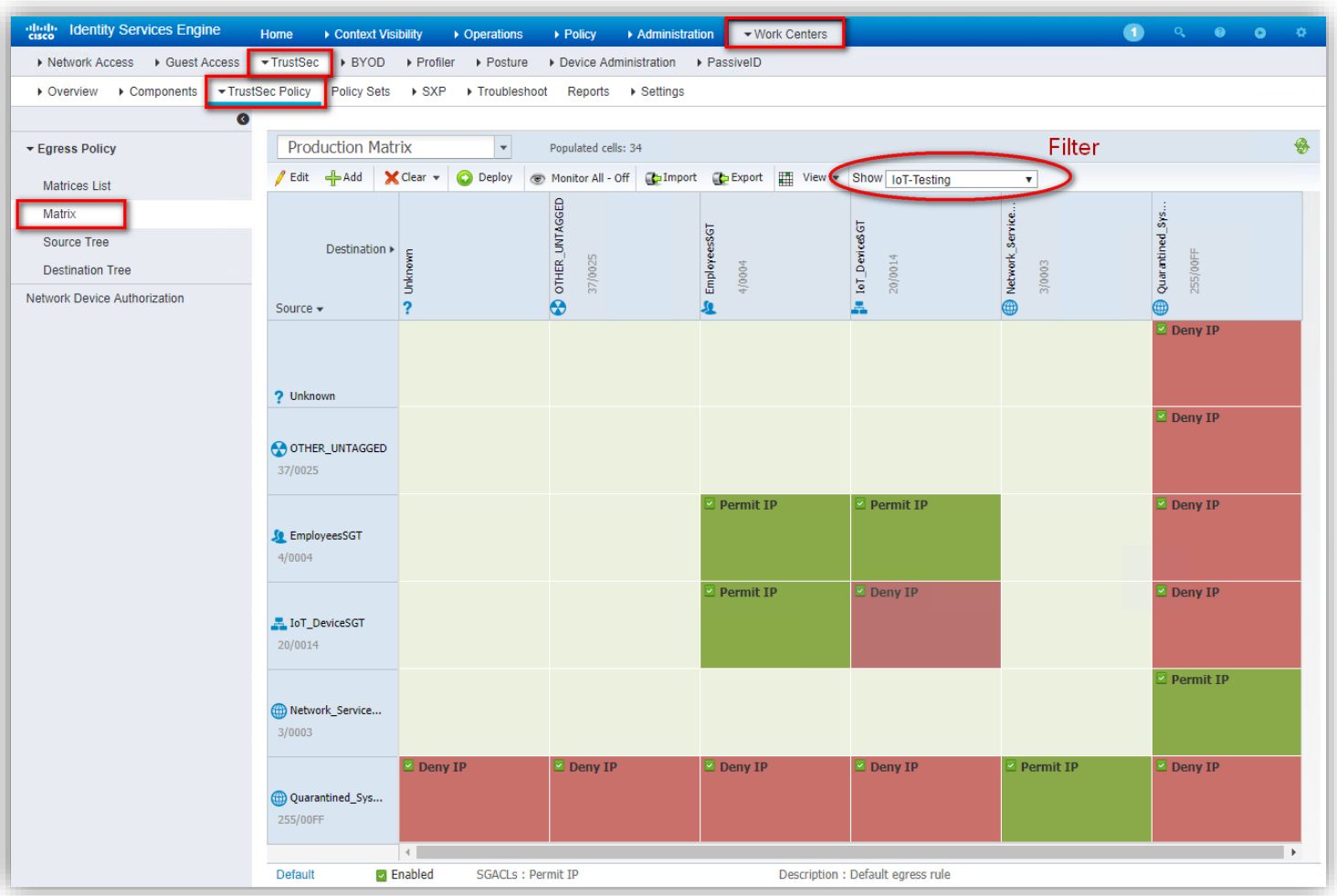
ISE - TrustSec Policy Matrix

The communications controlled by the ISE policy matrix, and enforced by switches, are unidirectional and not stateful, so consideration must include both requests and replies for proper symmetry and expected functionality. Enforcement happens when packets exit the access switch port with the destination device/security group attached.

ISE with TrustSec is ideal for implementing security at the switch level between IoT devices on the same switch, within or between cells, and creates the desired segmentation throughout the Industrial zone.

39

The TrustSec Policy Matrix (**Work Centers > TrustSec > TrustSec Policy > Matrix)** is a visual table showing source and destination security groups as rows and columns. Edit the policy cell to deny or restrict communication between groups. The default is to permit communication.



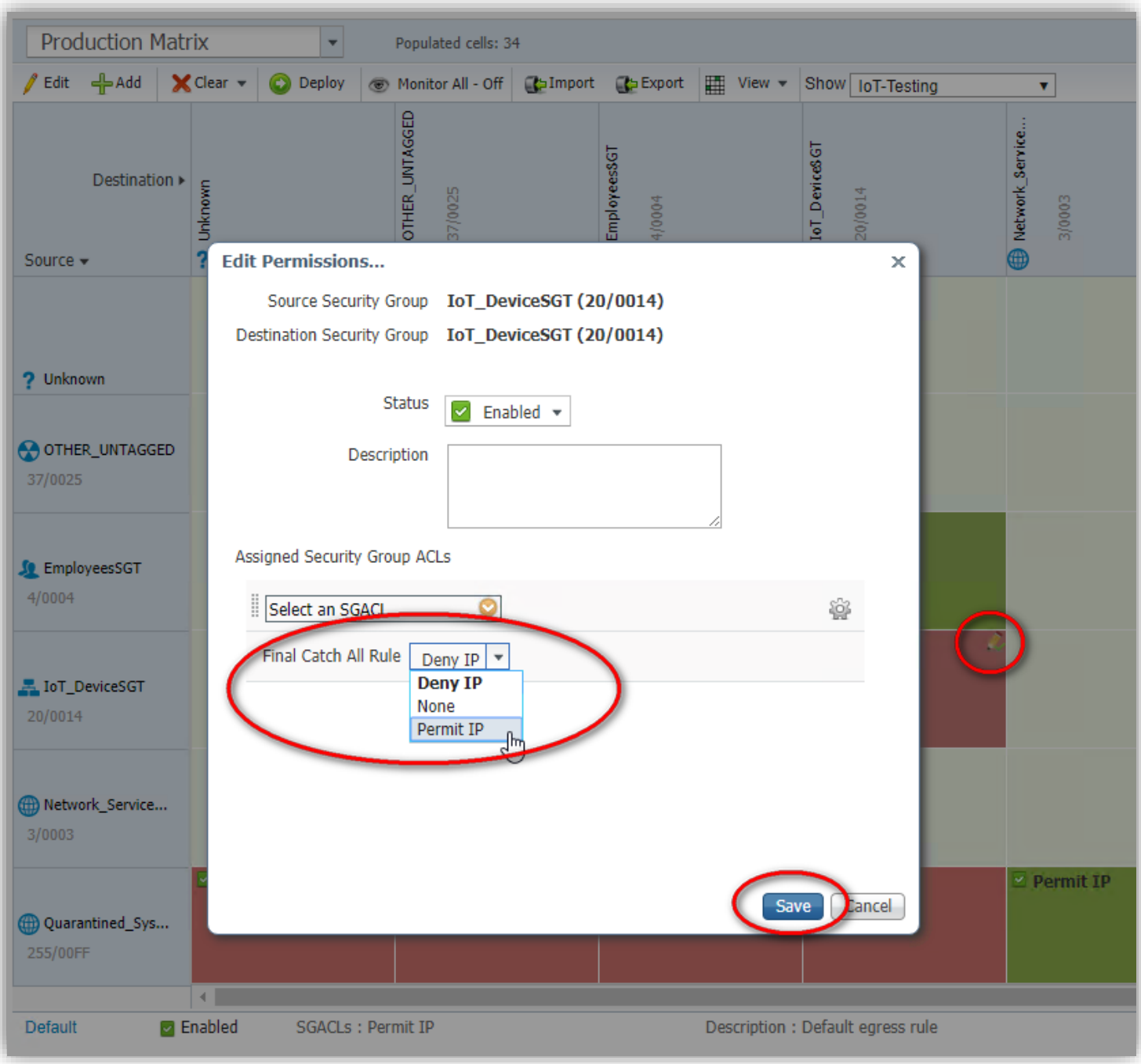
In this example, the Operations Employees are able to communicate with the IoT devices, but the IoT devices are not able to communicate with each other.

NOTE:

The matrix can be filtered to show only the groups you need to work with if desired

Return to Contents

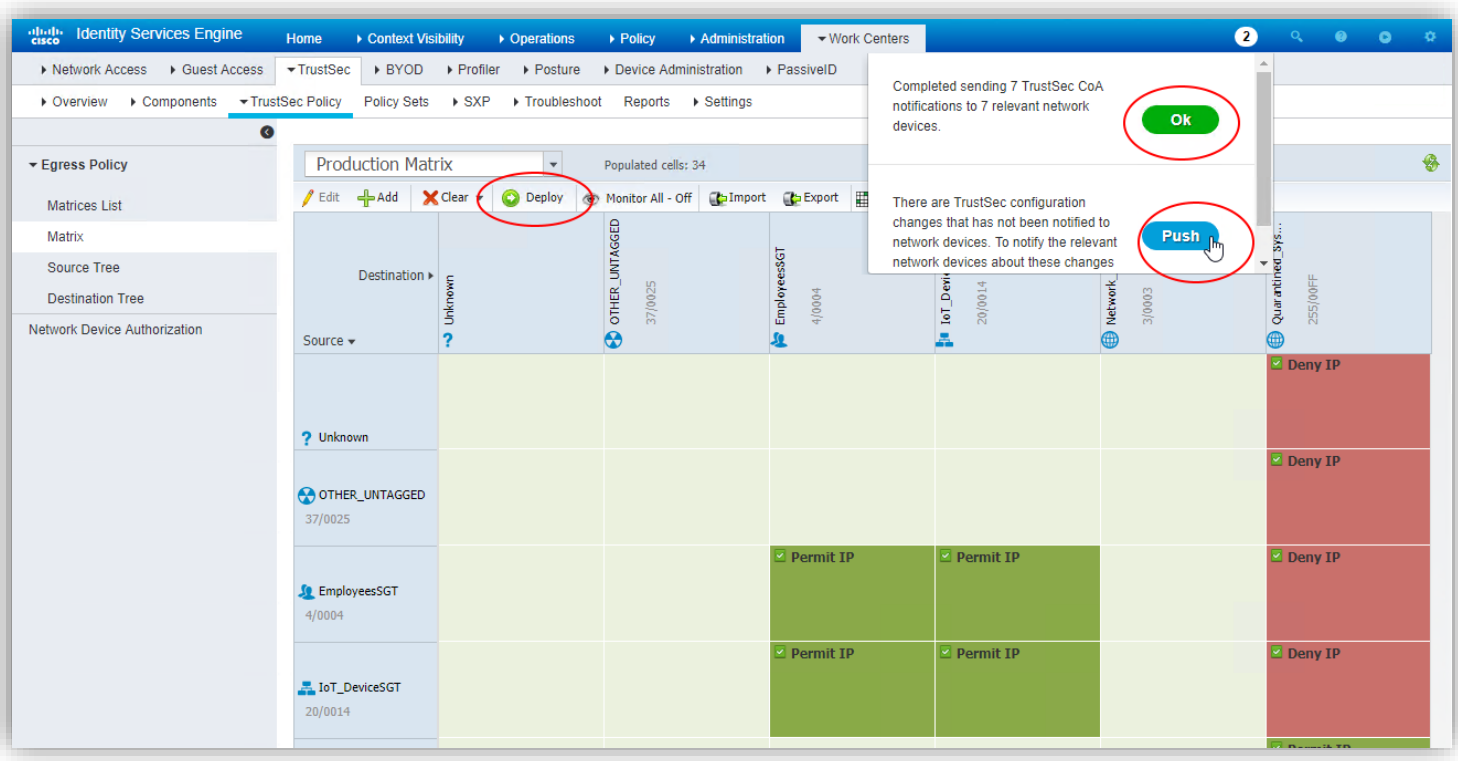
Step 1: Edit the policy to permit communication between the IoT devices. Click on the cell, click the pencil icon in the top right of the cell, select a security group access control list (SGACL) or change the Final Catch All Rule. Secure Group ACLs allow you to granularly open or block specific ports and protocols; however, in this example we are going to allow all IP communication by changing the Final Catch All Rule to Permit IP. Click Save.



Return to Contents

Step 2: After completing the policy changes, click the **Deploy** button, then the **push** button in the notification area. Click **OK** to acknowledge the CoA notifications.

The TrustSec Policy matrix also allows you to stage the configuration to a set of devices first, to see the impact of the change before deploying to a production device.



EXAMPLE NOTE:

If the destination device is connected to a switch without TrustSec enforcement enabled, communication is not blocked, even if a policy is configured to do so, and every other switch in the path is configured for TrustSec enforcement. Only the egress switch port with TrustSec enabled performs enforcement (the switch to which the device is connected). Reply traffic may be blocked when returning to the source device if specified in the policy.

Security Group Tag Exchange Protocol

The final part of segmentation for our three business use cases is sharing the information necessary to identify the flows across each network device traversed. This information consists of the security groups known by their tags (SGTs) and the device IP addresses that are contextually linked to the identities used to authenticate to ISE.

Security Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs to these network devices. 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 is assigned statically or dynamically, as we did in ISE, and is used by the 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 act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

As described in the architecture section, SXP is set up in a hub-spoke fashion with all network devices peering to the ISE server for SXP. If you have firewalls between your switches and the ISE server, special configurations must be added to permit SXP through both FTD and ASA Firewalls.

Policy Exceptions in ASA to Allow SXP

An SXP connection stays in the initializing state among two SXP peers interconnected by the ASA; as shown in the following example:

(SXP peer A) - - - - (ASA) - - - (SXP peer B)

Therefore, when configuring the ASA to integrate with Cisco TrustSec, you must enable the no-NAT, no-SEQ-RAND, and MD5-AUTHENTICATION TCP options on the ASA to configure SXP connections. Create a TCP state bypass policy for traffic destined to SXP port TCP 64999 among the SXP peers. Then apply the policy on the appropriate interfaces.

The following set of commands shows how to configure an ASA for a TCP state bypass policy using the CLI:

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options md5 allow OR tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
   message-length maximum 512
policy-map global_policy
 class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

For more information, please visit:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-trustsec.html

Return to Contents

43

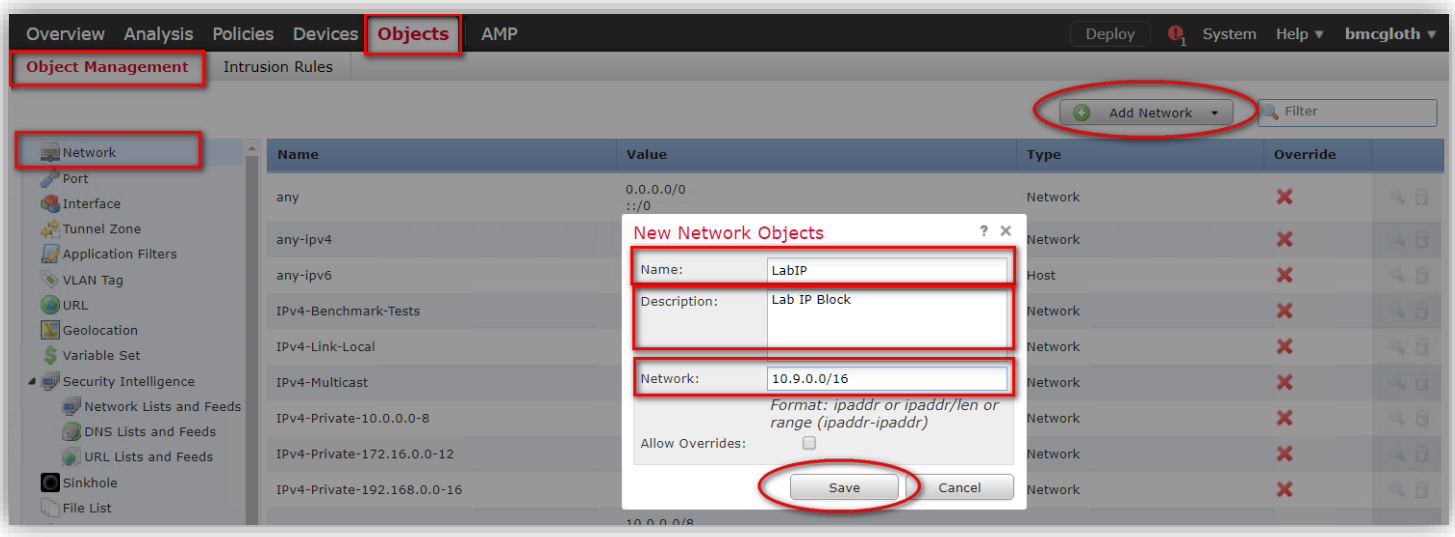
Policy Exceptions in FTD to Allow SXP

In FTD, the following high-level steps outline how to create a Flex-config modification to the firewall enabling the SXP protocol through.

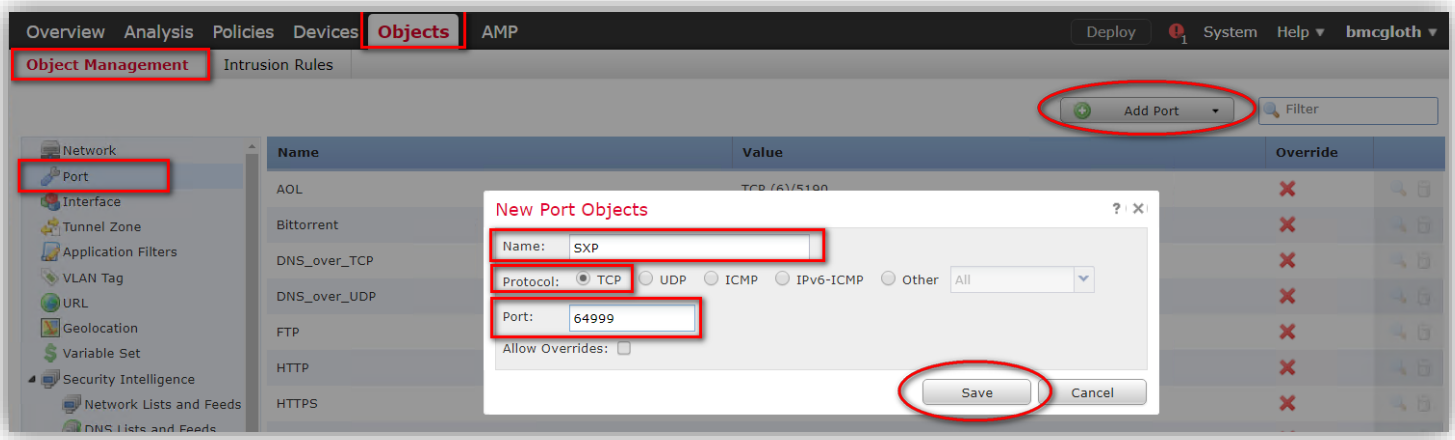
1. Create network objects (networks and protocols)
2. Create Extended ACL
3. Create Flex-config object
4. Add Flex config object to FTD Device

The following details the outlined steps. First, add objects for Extended Access List permitting port 64999 to all appropriate Switch IPs and ISE. In this example, we created a network object for the lab IP block.

Step 1: Starting in FMC, navigate to **Objects > Object Management > Network**. Click the **Add Network > Add Object** button in the upper right. Enter a Name, Description, and Network. Click **Save**.

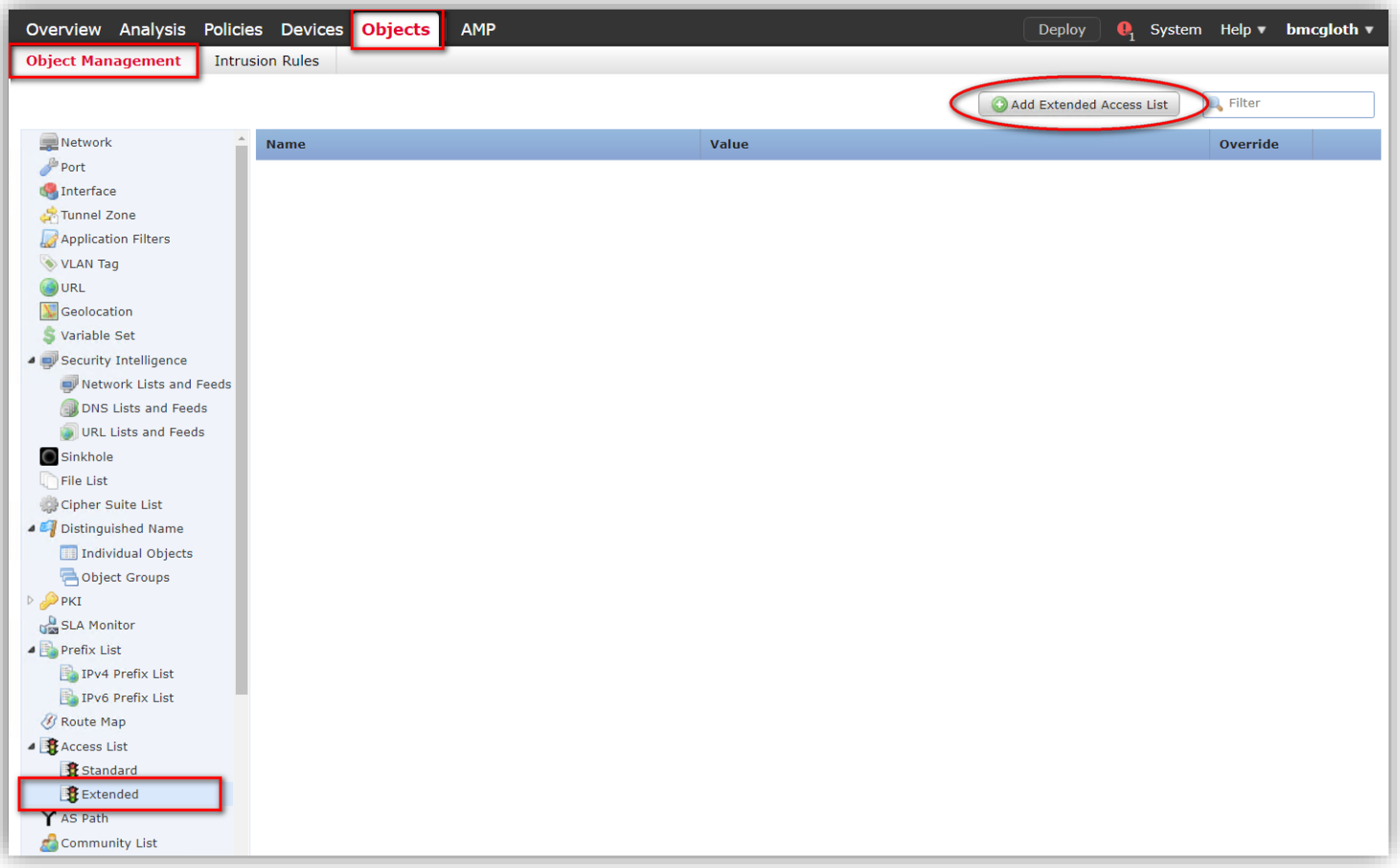


Step 2: Navigate to **Objects > Object Management > Port.** Click the **Add Port > Add Object** button on the upper right. Enter the Name **SXP**, select **TCP**, and enter **64999** for the Port. Click **Save**.

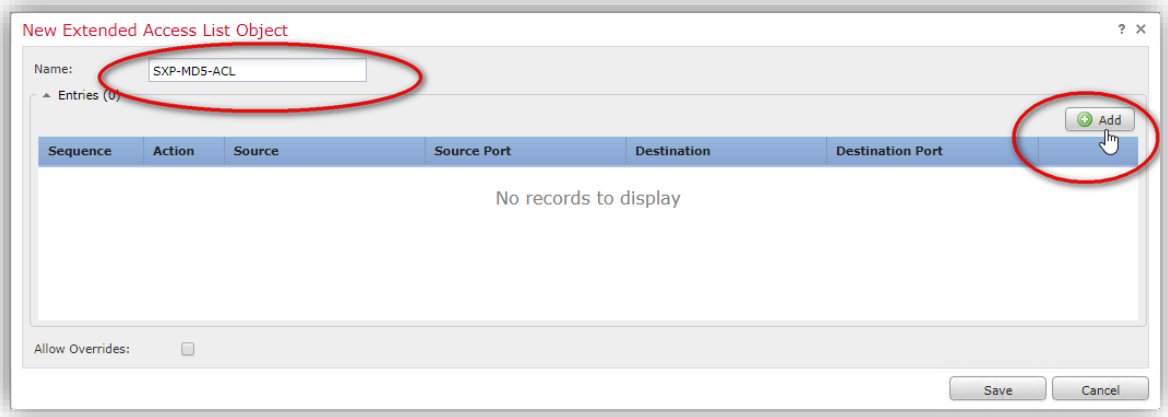


↩Return to Contents

Step 3: Navigate to **Objects > Object Management > Access List > Extended.** Click the **Add Extended Access List** button in the upper right.

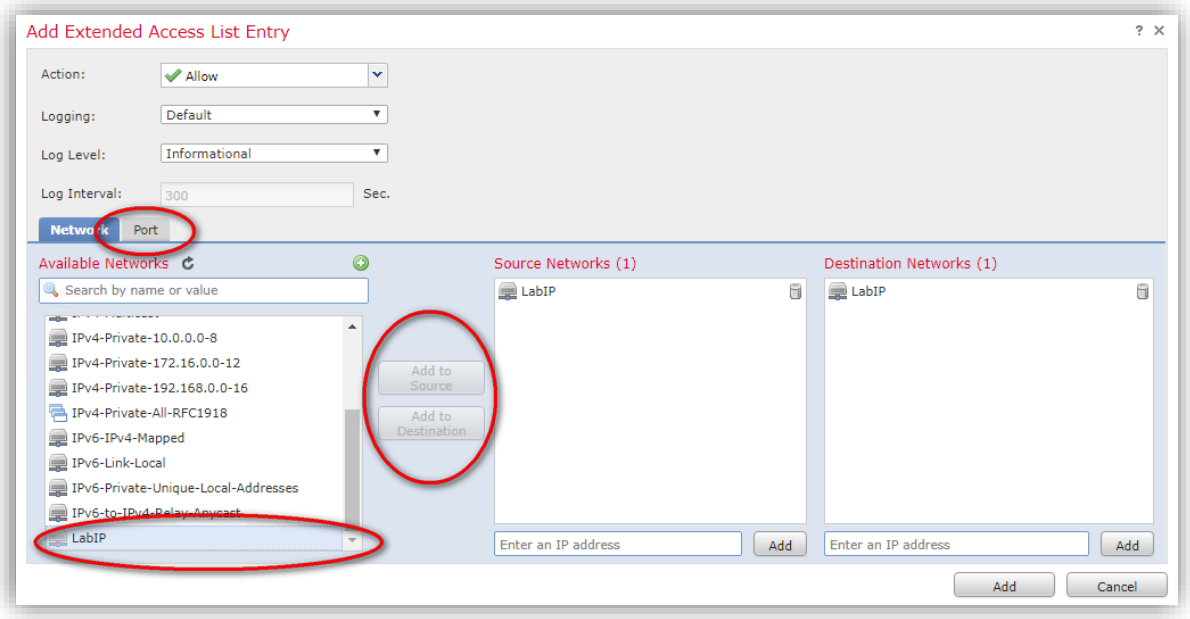


Step 4: Enter a Name. Click **Add** to start creating the access list entry.

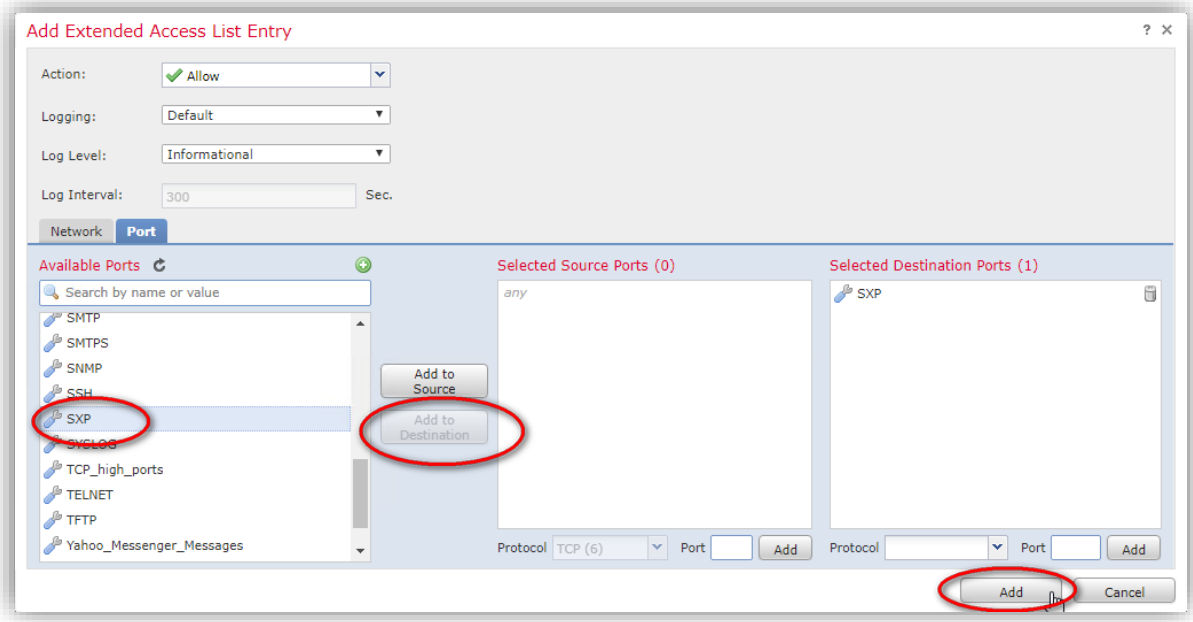


Return to Contents

Step 5: Select the proper network object you created earlier, and click **Add** to add the objects to the source and destination networks as appropriate for your environment. Click on the **Port** tab.



Step 6: Select the **SXP** port from the list of available ports, click **Add to Destination**. Click **Add** to complete the access list entry.



↩Return to Contents

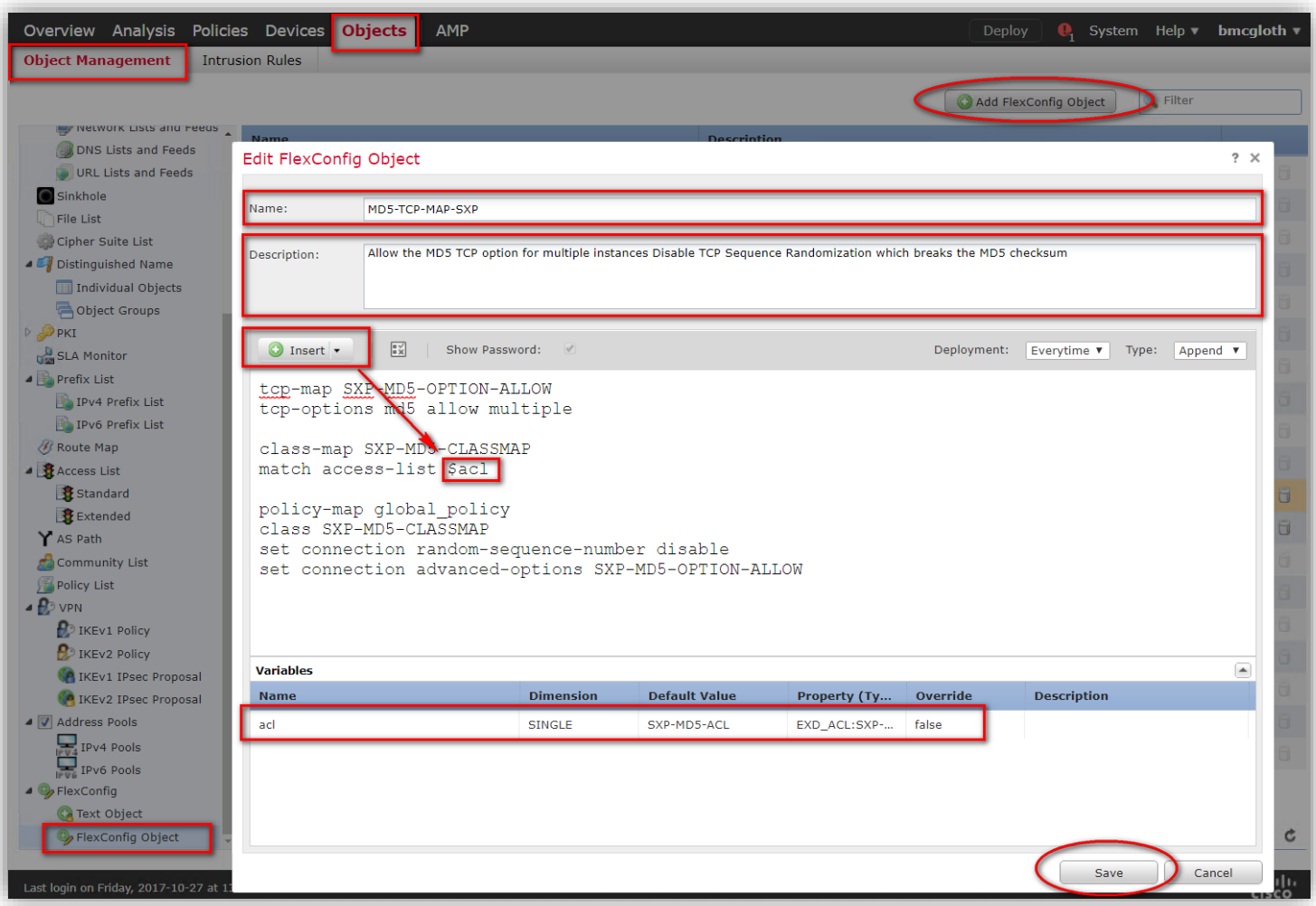
Step 7: Navigate to **Objects > Object Management > FlexConfig > FlexConfig Object.** Click the **Add FlexConfig Object** button in the upper right. Enter a **Name**. Paste in the configs for the tcp-map, tcp-options, and class-map.

```
tcp-map SXP-MD5-OPTION-ALLOW
  tcp-options md5 allow multiple

class-map SXP-MD5-CLASSMAP
  match access-list $acl
```

Click on **Insert** to assign the extended access list created in Step 4 as a variable: **$acl**. Paste in the global policy-map with the special connection options.

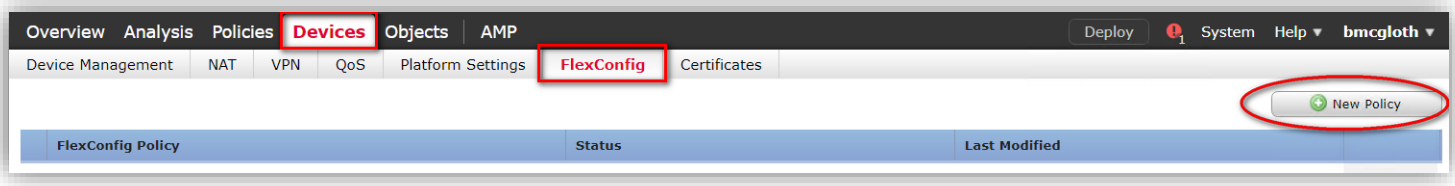
```
policy-map global_policy
  class SXP-MD5-CLASSMAP
   set connection random-sequence-number disable
   set connection advanced-options SXP-MD5-OPTION-ALLOW
```

Click **Save**.

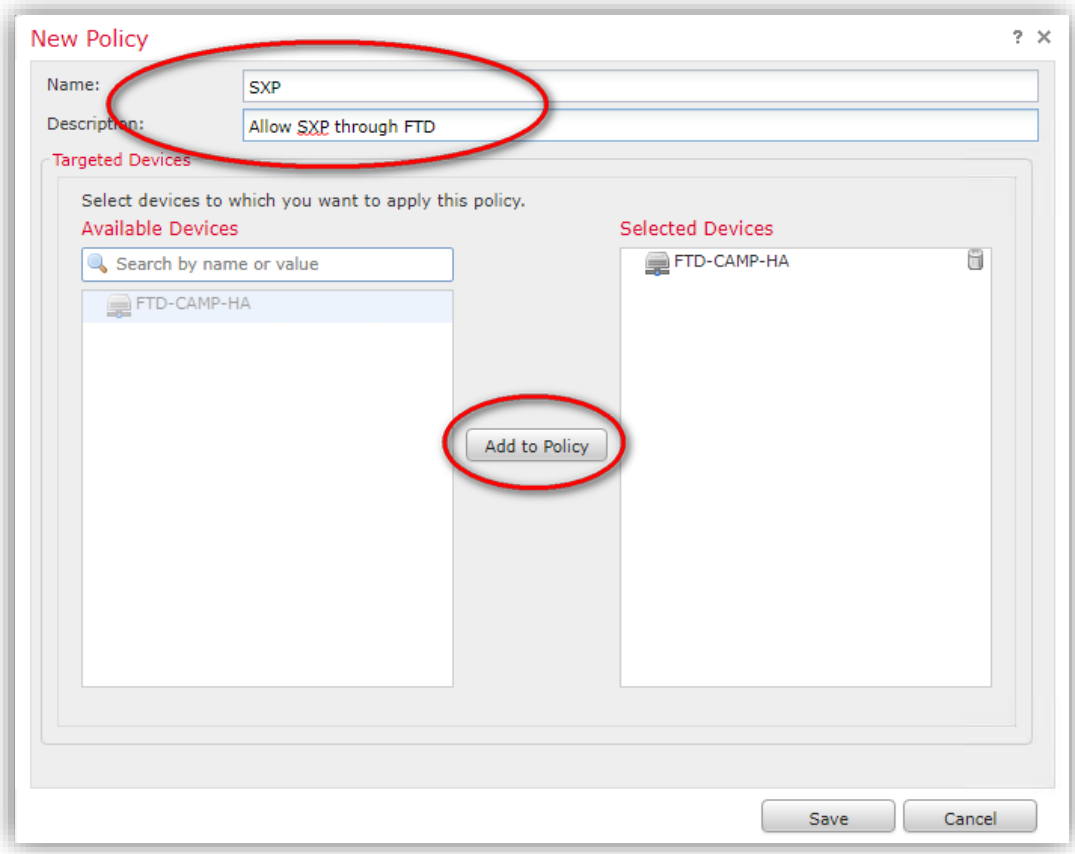


Return to Contents

Step 8: Create a new FlexConfig policy for the devices in the network. Navigate to **Devices > FlexConfig.** Click the **New Policy** button in the upper right.

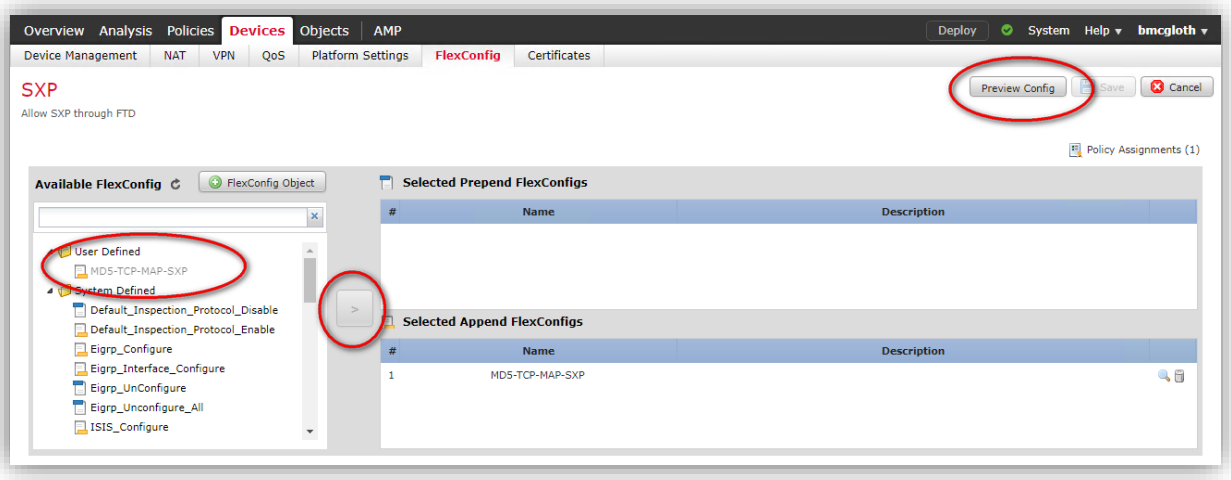


Step 9: Enter a **Name** and optional description. Select the device from the available devices and click the **Add to Policy** button. Click **Save**.



Return to Contents

Step 10. Select the newly defined FlexConfig from the menu on the left, and click the arrow to add it to the policy. Click **Save** in the upper right, then click **Preview Config** to check the results.



Step 11: Click **Deploy** to install the new configs in the firewalls.

SXP through the firewalls should now connect and function properly. Connectivity can be verified by checking the SXP connections table in ISE if peers have already been configured.

More information on FlexConfig can be found here:

http://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html

49

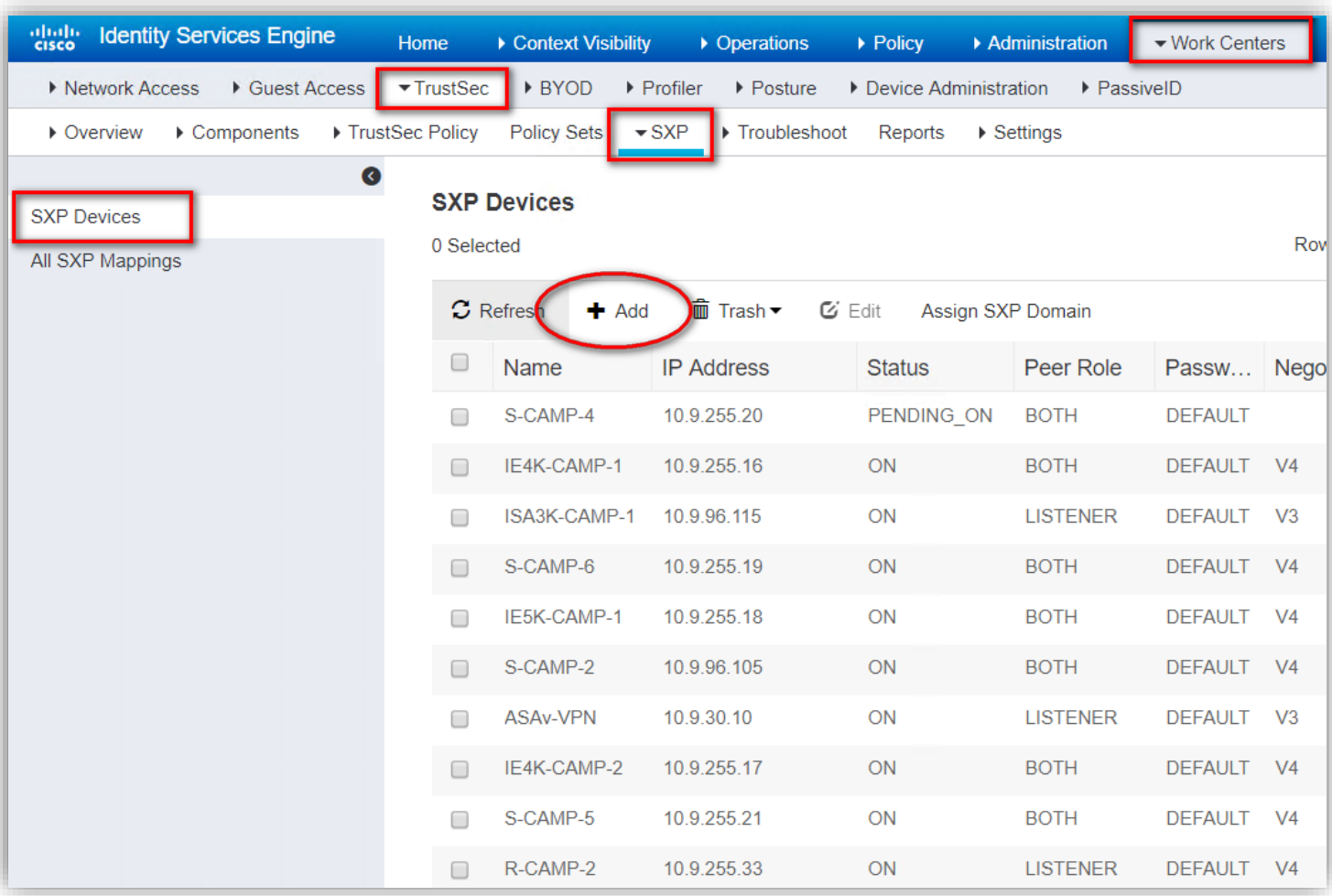
Configure SXP Device Peers in ISE

Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. A best practice is to configure them in bidirectional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

This design uses the best practice model of implementing SXP in a hub-and-spoke design between the ISE PSNs and each switch/firewall. The alternative of configuring device-to-device SXP relationships can be prone to misconfigurations during deployment, possibly causing loops.

To view the SXP peer devices that are added to Cisco ISE, choose Work Centers > TrustSec > SXP > SXP Devices. Add network devices to ISE that will communicate with SXP.

Step 1: Starting in ISE, navigate to Work Centers > TrustSec > SXP > SXP Devices.



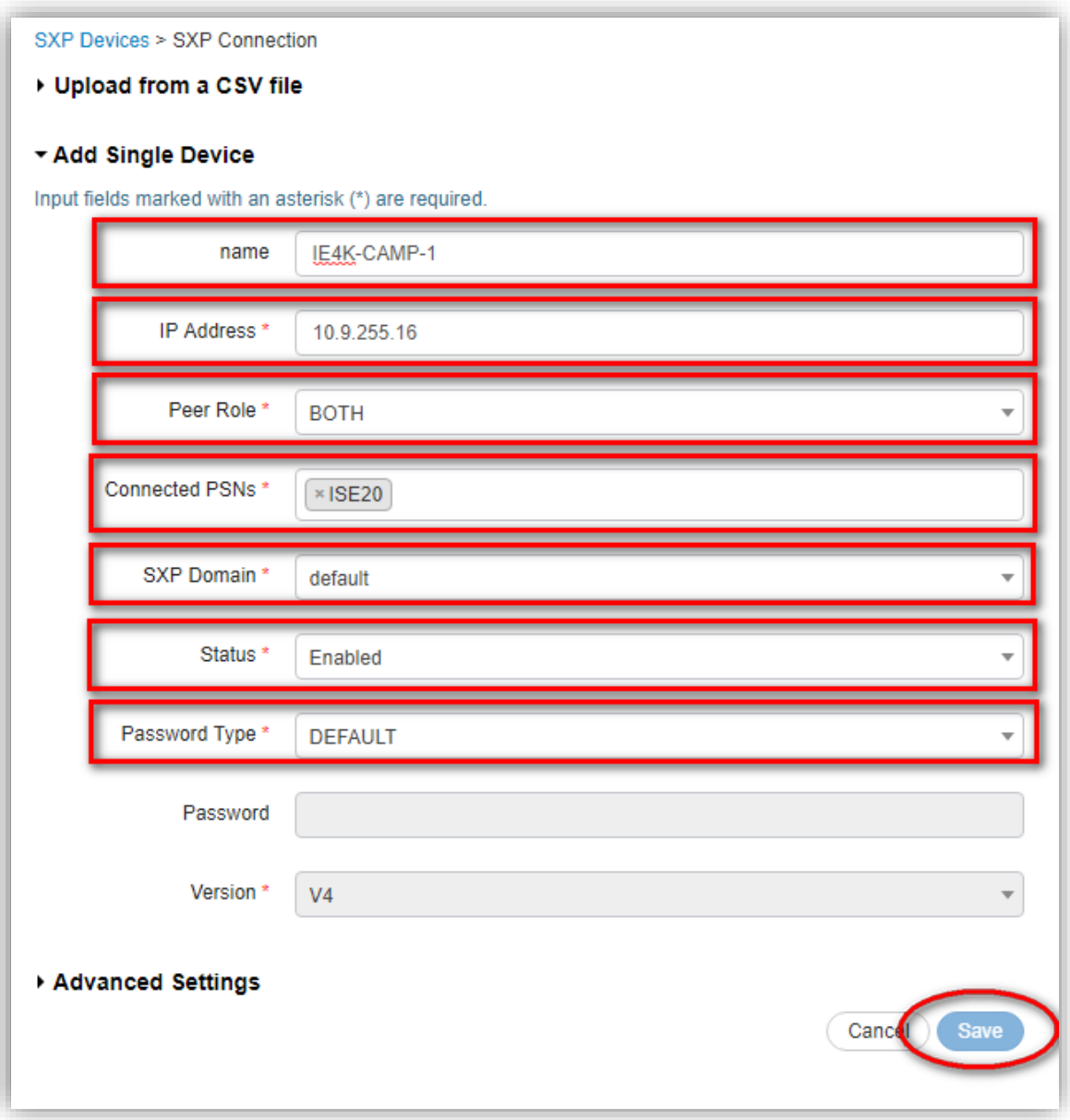
NOTE:

If the corresponding network device has not been configured for SXP communication yet, the status will show as *PENDING_ON.* The Peer Role for switches that do not support BOTH should be set to LISTENER

Step 2: Click the Add button at the top of the list.

Return to Contents

Step 3: Enter the Name, IP address, Peer Role, PSN, and Password for each switch or firewall that will connect to ISE using SXP. Click **Save**.



NOTE:

The SXP global default password can be specified instead of different device specific passwords. To set the Global Password, navigate to **Work Centers > TrustSec > Settings > SXP Settings.**

If the device does not support the **Peer Role** of **BOTH**, configure the device Peer Role as **LISTENER** in ISE.

Repeat these steps for each SXP switch, router, and firewall in the network.

Configure TrustSec and SXP on Network Devices

The following example shows how to enable SXP and to configure an SXP peer connection between the ISE PSN, the speaker, and a switch or ASA, the listener.

Step 1: Specify the Cisco TrustSec device ID and password for this switch to use when authenticating with ISE and establishing the PAC file. This password and ID must match the ISE Network Devices configuration specified earlier. At the device command line enter:

```
switch# cts credentials id {switch ID} password Cisco123
```

NOTE:

Make sure the *switch ID* and *password* are the same as configured in ISE TrustSec

Step 2: In Configuration mode, first enable Cisco TrustSec SXP before you can configure peer connections.

```
cts sxp enable
```

Step 3: As a best practice, specify the source IP address and configure a default password.

```
cts sxp default source-ip {loopback or interface IP}
cts sxp default password Cisco123
```

NOTE:

If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the switch.

Step 4: Configure the SXP peer connection to the ISE PSN. If the device does not support the peer mode BOTH, configure the peer as SPEAKER as shown below. This will match the hub-and-spoke design, and how the ISE-side SXP setting was configured earlier.

```
cts sxp connection peer ISEPSN password default mode peer both or
cts sxp connection peer ISEPSN password default mode peer speaker
```

Step 5: Verify the SXP connection is established.

```
show cts sxp connections
```

This displays detailed information about the SXP status and connections.

```
IE4K-CAMP-2#sh cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: 10.9.255.17
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          : 10.9.10.51
Source IP        : 10.9.255.17
Conn status      : On (Speaker) :: On (Listener)
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet Speaker Conn hold time   : 120 seconds
Listener Conn hold time   : 120 seconds
Local mode       : Both
Connection inst# : 1
TCP conn fd      : 1(Speaker) 2(Listener)
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 19:03:19:52 (dd:hr:mm:sec) :: 19:03:19:28
(dd:hr:mm:sec)

Total num of SXP Connections = 1
```

TrustSec Testing Commands

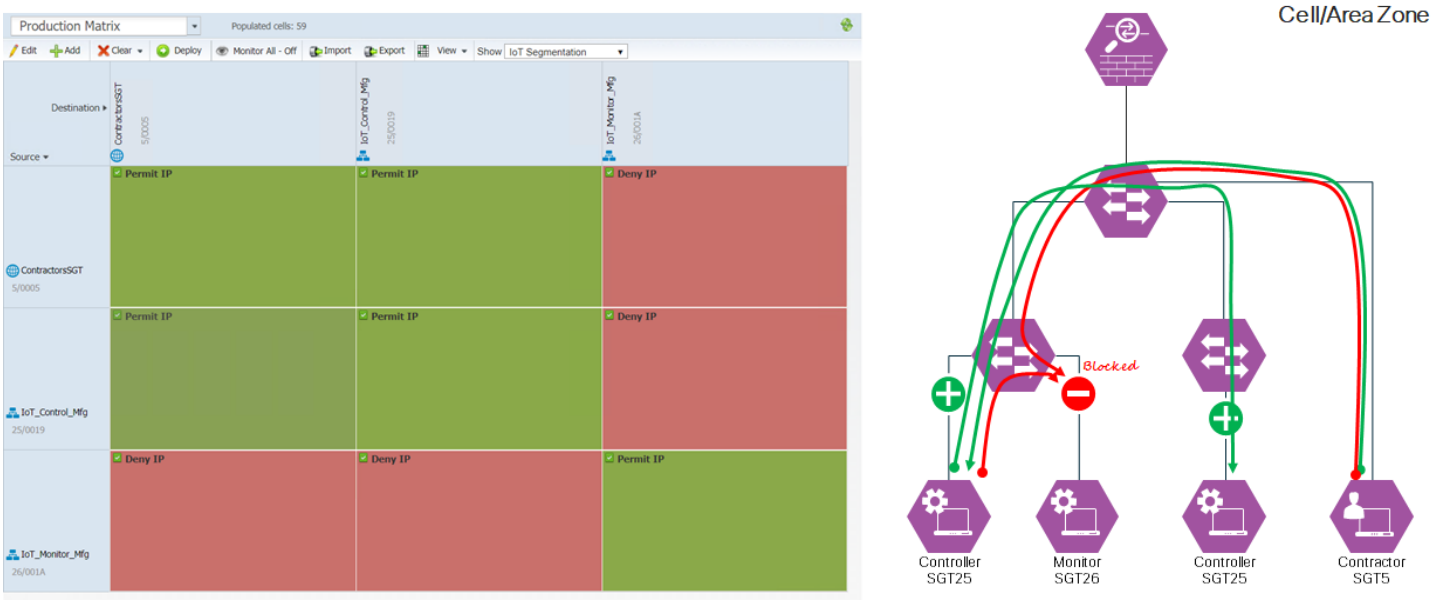
- show cts environment-data
- show cts pac
- show cts sxp sgt-map brief

53

Enable TrustSec Enforcement

Within the plant, using TrustSec for segmentation is a cost-effective and scalable alternative to a static VLAN method, to protect the IoT systems within and between cells at layer 1 and 2 of the Purdue model; for example, a flat network in a single cell where all devices are on the same VLAN and use static IP addressing on the same subnet, yet can be fully segmented using TrustSec Security group tags and the policy provided by ISE as shown in Figure 15.

Figure 15 - TrustSec policy to Enforcement



The following configurations add enforcement capabilities to the switches.

Step 1: Configure the switch to use RADIUS authorization for all network-related service requests (the ISE group was created earlier in this guide).

```
aaa authorization network cts-list group ISE
```

Step 2: Specify TrustSec AAA server group for cts authorizations.

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

Step 3: Specify the SGT for the switch to use for its own traffic.

```
cts sgt 2
```

Step 4: Enable role-based enforcement globally and per VLAN.

```
cts role-based enforcement
cts role-based enforcement vlan-list 115-117
```

Return to Contents

TrustSec enforcement on Industrial Ethernet 4K and 5K switches works only for directly connected devices, and for packets that include the SGT information when received and trusted. This is because SXP learned mappings are not able to be used for enforcement on these platforms. To segment communication within and between cells in a plant, the switches must also be configured for inline tagging to have enforcement function as desired. By tagging the packets being sent to these switches from upstream or downstream adjacent switches or firewalls, comprehensive enforcement can be achieved. To enable inline tagging, IP routing must first be enabled.

Steps 5-10 describe how to enable inline tagging on Industrial Ethernet switches as well as older Cisco Catalyst switches.

Step 5: Enable routing globally on the switch (requires software other than LAN Base).

```
IE4K-CAMP-2(config)#ip routing
```

Step 6: Before enabling inline tagging on switch interfaces, the SDM mode must also be changed to routing. Check the current mode using the `show sdm prefer` command.

```
IE4K-CAMP-2#sh sdm prefer
 The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  16K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    18K
    number of directly-connected IPv4 hosts:        16K
    number of indirect IPv4 routes:                 2K
  number of IPv6 multicast groups:                  0
  number of IPv6 unicast routes:                    0
    number of directly-connected IPv6 addresses:    0
    number of indirect IPv6 unicast routes:         0
  number of IPv4 policy based routing aces:         0.125k
  number of IPv4/MAC qos aces:                      1.875k
  number of IPv4/MAC security aces:                 1.875k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0
  number of IPv6 security aces:                     0
```

Step 7: If the SDM mode is not set to “routing”, enter configuration mode and enter the following global command:

```
sdm prefer routing
```

After entering the command, you will receive the following notification:

```
Changes to the running SDM preferences have been stored, but cannot take
effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Step 8: Save the switch configuration and reload the switch.

```
#Copy running-config startup-config
#reload
```

Step 9: After the switch has reloaded, enable manual TrustSec tagging for uplinks. Enable propagation of leaned SGTs (default) and manually tag unknown traffic with a defined SGT, and trust tagged packets received.

```
interface GigabitEthernet1/16
 cts manual
  propagate sgt
  policy static sgt 37 trusted
```

In this case, “trusted” indicates that ingress traffic on the interface should not have its tag overwritten.

NOTE:

In ISE, an SGT should be created to identify untagged traffic that may transit between systems.

Create an SGT for OTHER_UNTAGGED traffic when doing inline tagging; in our example, tag 37 was dynamically assigned from the ISE pool. Add new Security Groups by navigating in ISE to Work Centers > TrustSec > Components > Security Groups.

Step 10: TrustSec enforcement happens on the egress port of the switch with attached IoT device, so enforcement should be disabled on switch-to-switch and uplink trunk port interfaces. The following example disables role-based enforcement:

```
interface GigabitEthernet1/16
 switchport trunk allowed vlan 115-117
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 cts manual
  propagate sgt
  policy static sgt 37 trusted
 no cts role-based enforcement
```

TrustSec Troubleshooting Commands

- show cts interface brief
- show cts sxp sgt-map brief
- show cts role-based counters
- show cts role-based permissions
- show cts role-based sgt-map all
- cts refresh policy
- cts refresh environment-data
- show authentication interface gigabitEthernet 2/1
- show mab interface gigabitEthernet 2/1 details

More help can be found in the TrustSec Troubleshooting Guide:

https://communities.cisco.com/docs/DOC-69479

Return to Contents

56

TrustSec Firepower Policy

Firepower policies control flows into and out of the Industrial Demilitarized Zone as well as between Cell/Area zones. Purdue level 3 and above, enterprise and IDMZ, the Firepower 2100 and 4100 Series provide defense in depth across all parts of the business. Purdue level 3 and below, cell perimeter security, is best provided using devices such as the ISA3000 or ASA5506H in these harsh industrial environments.

Firepower Management Center is installed and configured following the Rapid Threat Containment design guide. This guide steps through installation, and establishing pxGrid connectivity back to ISE. For lab installation and testing, a Certificate Authority was installed and used instead of self-signed certificates.

The Rapid Threat Containment guide can be found here: http://cisco.com/go/rtc and an additional Firepower and ISE guide is available here: https://communities.cisco.com/docs/DOC-68292.

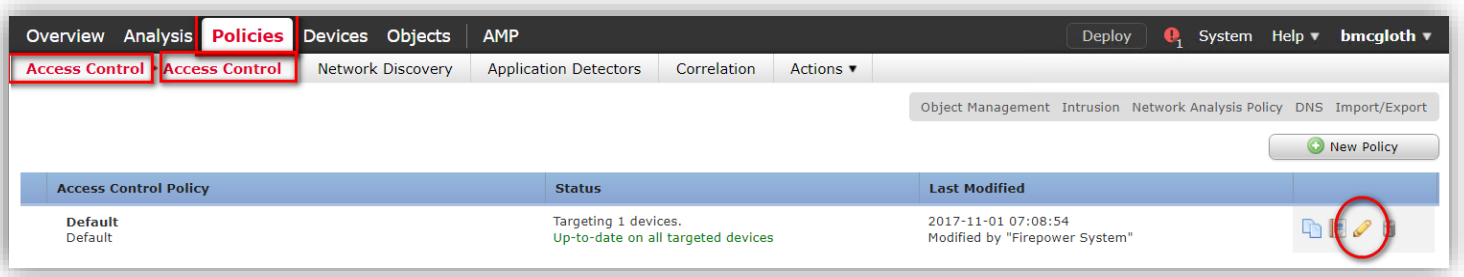
In this example policy, employees are able to connect to any internet URLs with the exception of categories blocked by corporate policy (Gambling, Peer-to-Peer, Malware, and Hacking). If a system is placed in Quarantine, all outbound web connectivity is blocked except that destined for the corporate support site “cleanme.cisco-x.com”.

pxGrid enables the use of SGTs as the traffic source, providing for a greatly simplified policy without the need to specify networks and device IP addresses.

Now we’ll add a rule to allow IoT devices to send telemetry to the corporate data lake in the cloud over HTTP and HTTPS.

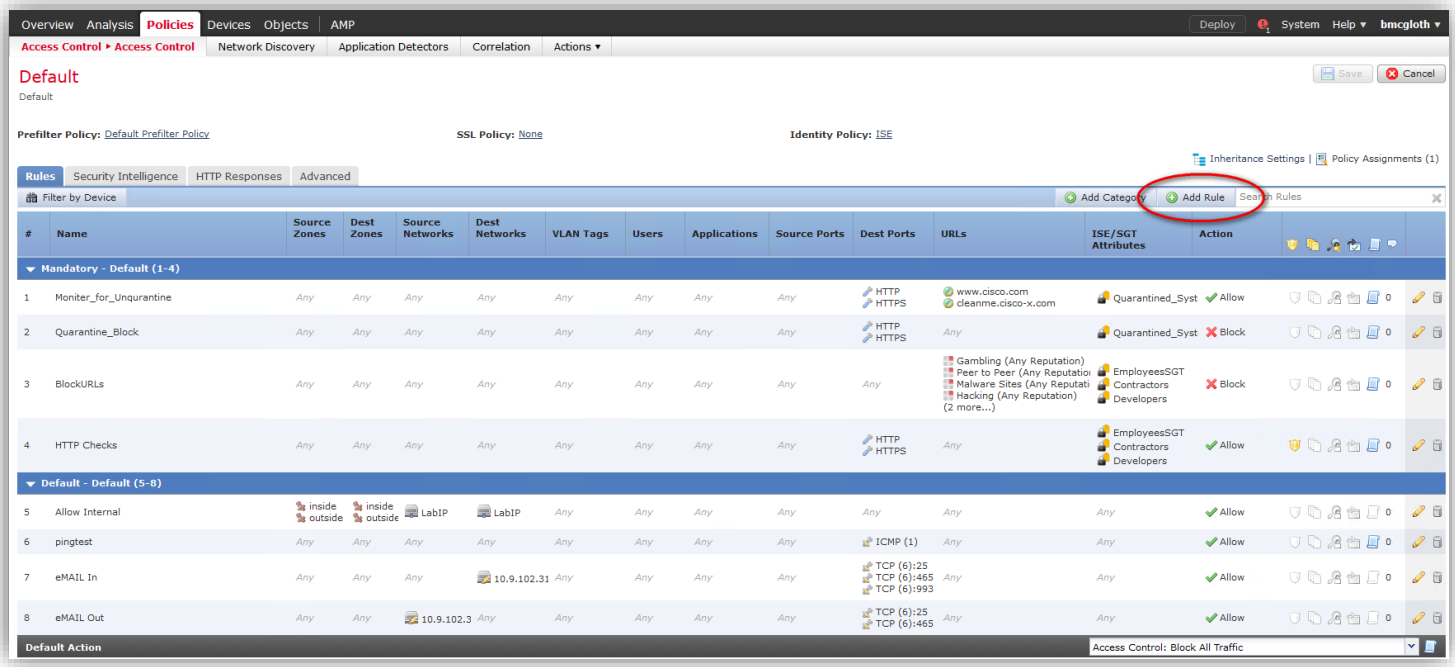
In Firepower, Management Center policies for next-generation firewalls and next-generation IPS systems are configured under the **Policies > Access Control > Access Control Policy > Default**.

Step 1. Edit the existing policy by clicking on the pencil on the right, or create a new policy.

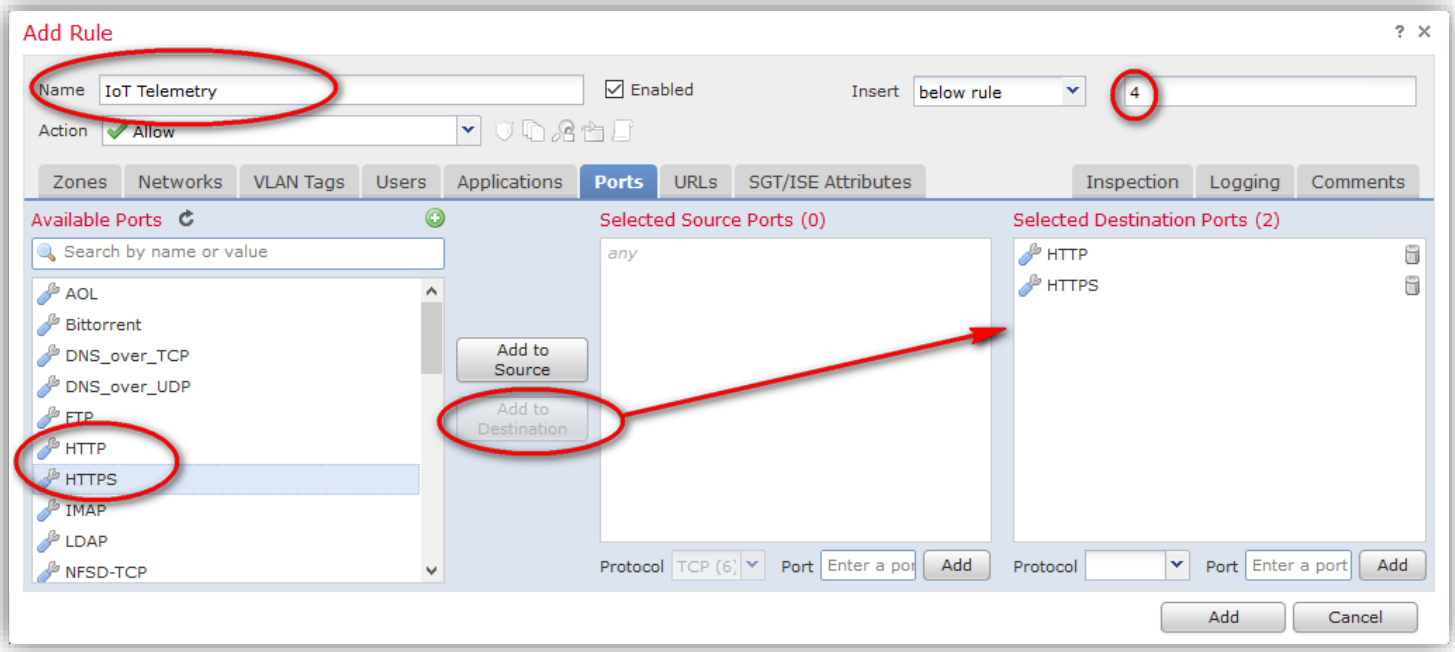


Return to Contents

Step 2. Click the **Add Rule** button at the top of the policy rules.

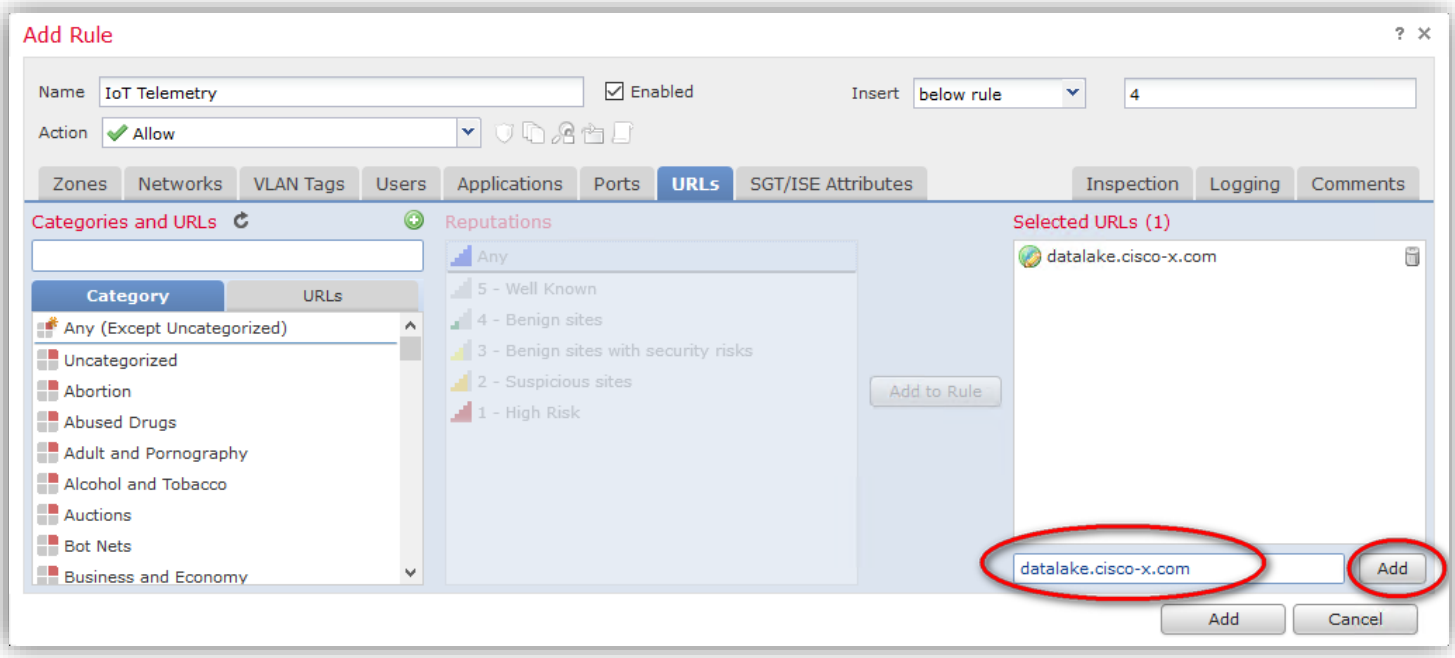


Step 3. Enter a descriptive name, specify where you want the rule to insert, and the destination ports.

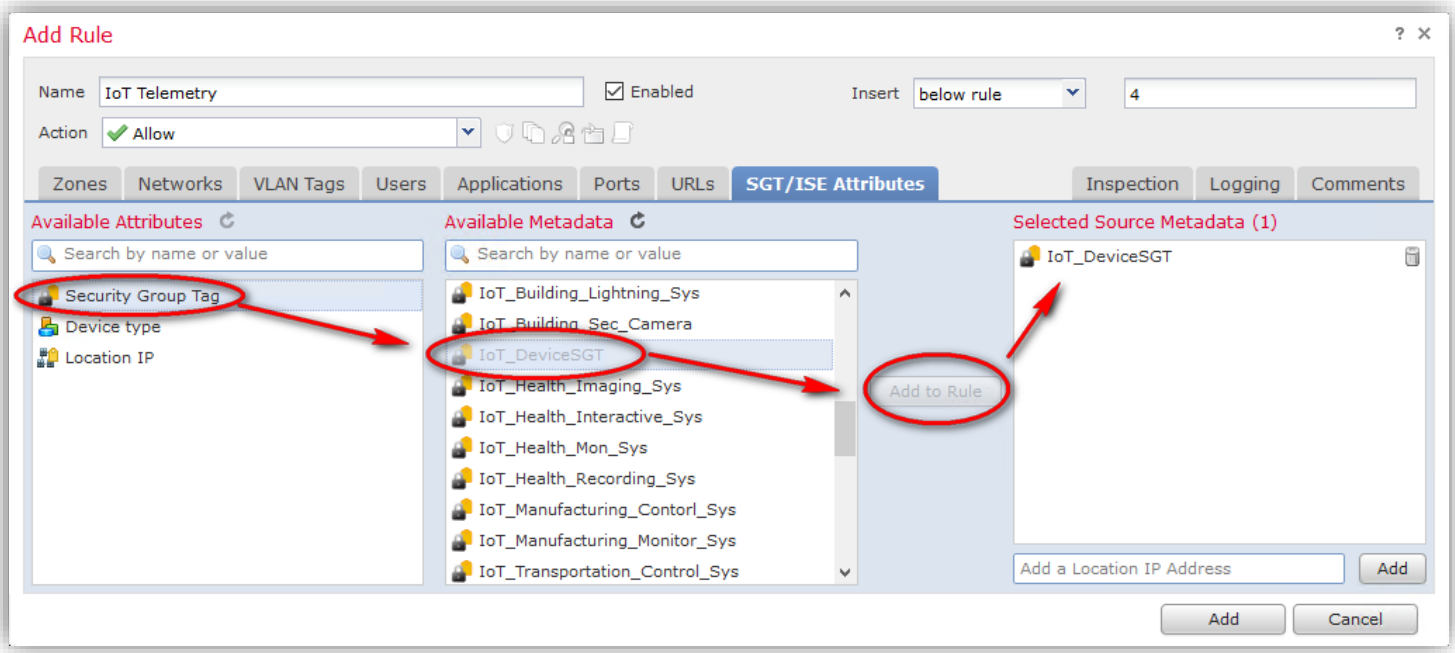


↩Return to Contents

Step 4. Enter the URL, click **Add** next to the box.



Step 5. Select the SGT group for the devices needing to send the telemetry.

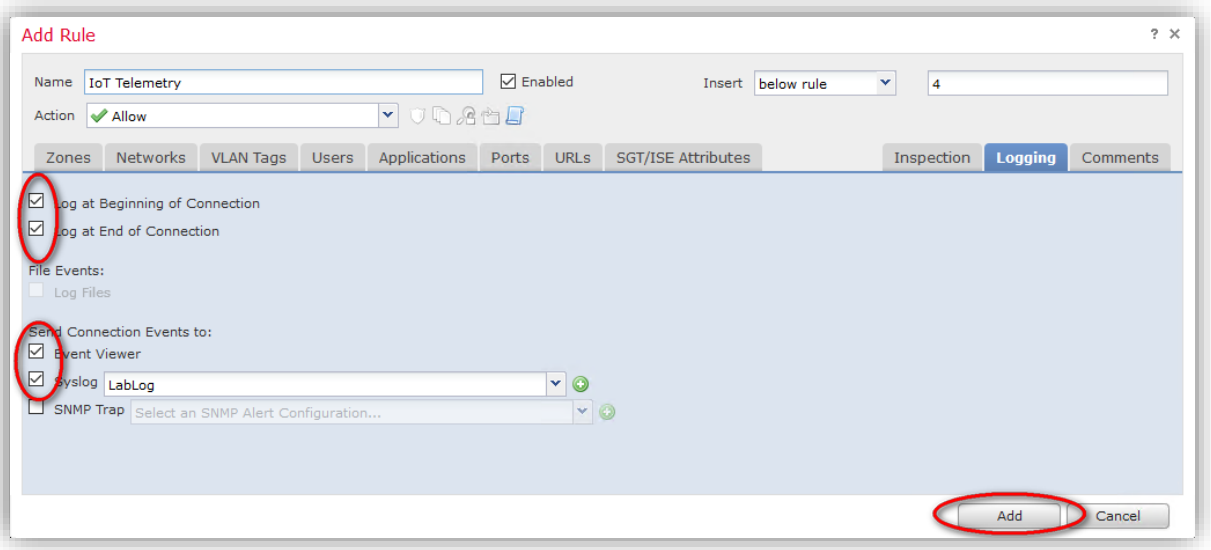


The available metadata from the Security Group Tag list above is retrieved from ISE via pxGrid. Steps to install pxGrid can be found in the following guides:

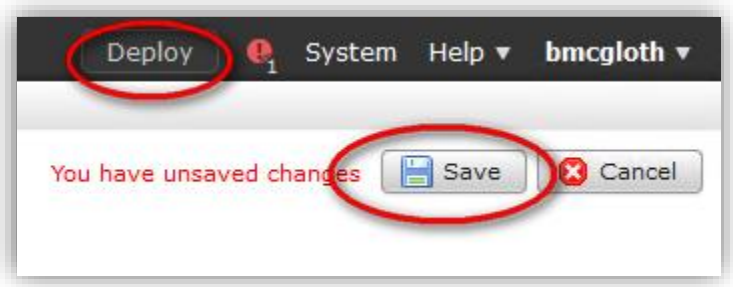
- Rapid Threat Containment Design guide: https://communities.cisco.com/docs/DOC-68293
- How to Integrate Firepower and ISE via PxGrid: https://communities.cisco.com/docs/DOC-70354

Return to Contents

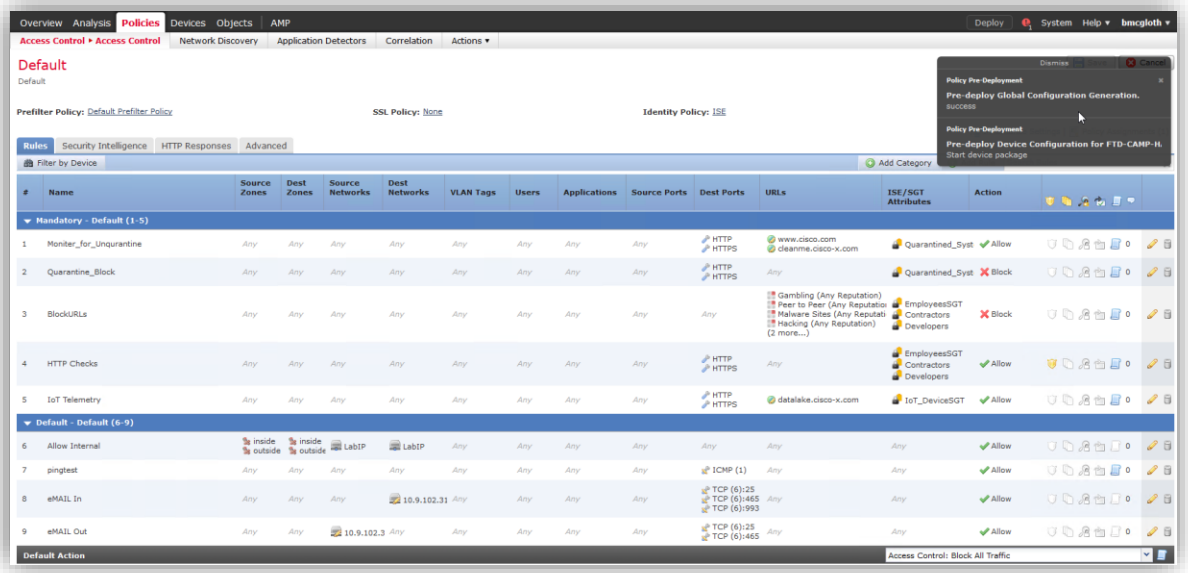
Step 6. Enable logging, and click **Add** when finished.



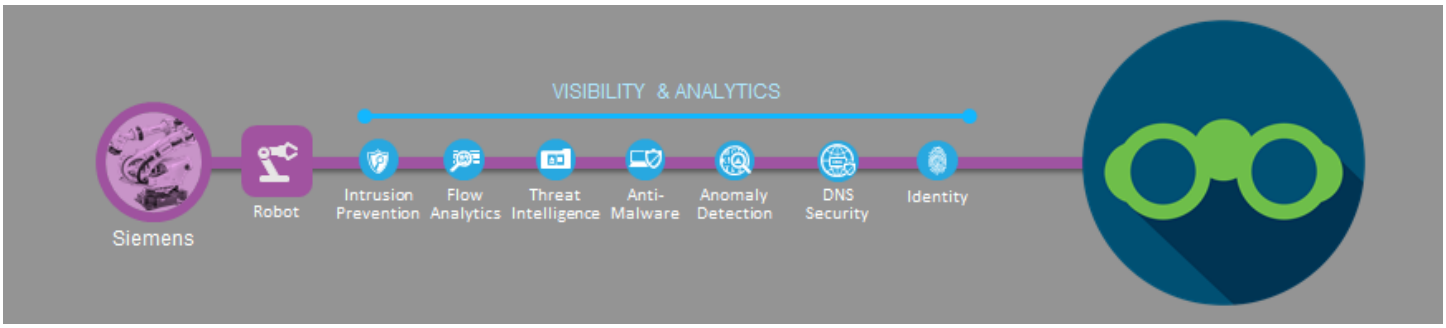
Step 7. Once all of your rules have been added, click **Save** and **Deploy** to implement them.



Step 8. Deployment completed.



↩Return to Contents

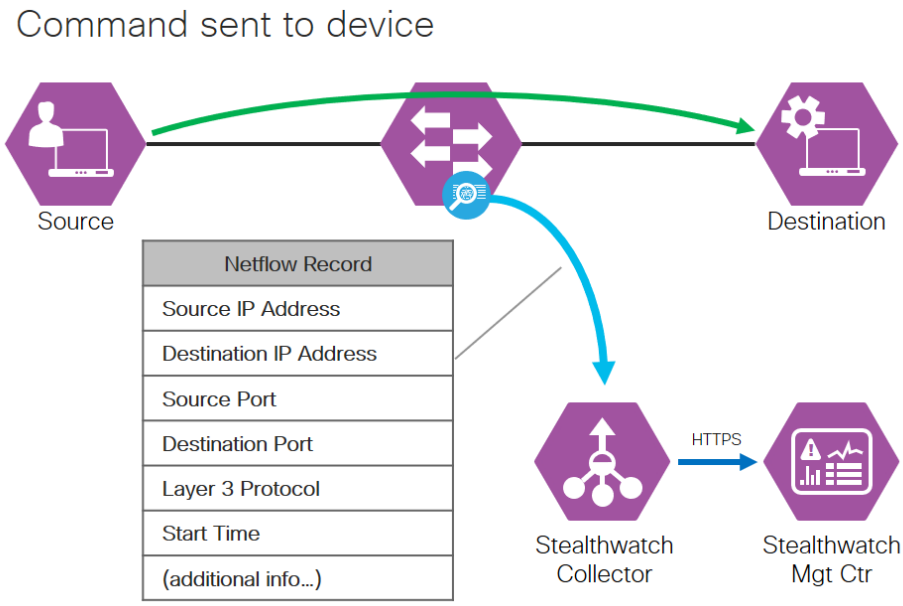


Stealthwatch

Cisco Stealthwatch turns the network into 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, it can quarantine attackers and thereby protect your vulnerable IoT devices.

NetFlow is comprised of metadata describing the “conversations” on the network as shown in Figure 16. It contains the important telemetry details of network communications, information about when the conversation occurred, how long it lasted, and what protocols were used. It provides visibility about the flows transiting the network, as well as enhanced network anomaly and security detection.

Figure 16 - NetFlow Records



Stealthwatch provides real-time insight into what each device is doing on the network, all of its network connections, interface utilization, and overall network performance. We can also see various levels of machine-to-machine communication, including 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 also being able to analyze and understand the information shown by combining various information points and vectors provides the unequaled visibility for making operational decisions.

For example, DoS attacks attempt to exhaust the device resources. These resources can be network bandwidth, computing power, or operating system data structures. To launch a DDoS attack, malicious users first build a network of devices that they will use to produce the volume of traffic needed to deny services to users.

⮌Return to Contents

To create this attack network, attackers discover vulnerable IoT devices on the network. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date software, or those that have not been properly patched. Vulnerable hosts are then exploited by attackers who use their vulnerability to gain access to these hosts. The next step for the intruder is to install attack tools on the compromised hosts of the attack network. The hosts 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 we call an army. WAN saturation, increase in host counts, and increase in UDP packets are all common for the compromised organization.

Stealthwatch detects attack traffic targeting your DNS servers and application servers that is causing other systems relying on DNS to fail and disrupting business operations. Stealthwatch can detect and remediate a threat with over 94 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 generate an 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 SIEM.

Cisco Stealthwatch was deployed using the Network as a Sensor Cisco Validated Design guide, and pxGrid was configured to communicate with ISE using CA-based certificates.

The Cisco Network as a Sensor design guide can be found here:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf

Stealthwatch Installation Guide:

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

Enabling NetFlow Export on Network Devices

This guide covers enabling NetFlow on CPwE network access devices, the Cisco Catalyst 3650/3850, and NetFlow Lite on the Industrial Ethernet 4000/5000 switches. Rather than NetFlow, the ISA3000 (ASA Series) uses Network Secure Event Logging (NSEL).

For information about enabling NetFlow on other devices, see the NetFlow Configuration Stealthwatch Wiki page (https://www.lancope.com/wiki/netflow-configuration).

Network Switches NetFlow

Enabling NetFlow on switches and routers entails three elements: a flow record, a flow exporter, and a flow monitor. After you have configured all three components, you apply the flow monitor to a wired or wireless interface such as a L2/L3 port, VLAN, or WLAN (SSID).

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 to provide more detail to the collector for reporting and analysis. When you create a flow record, you are telling the device to show all of the flow data traffic that enters (Ingress) or leaves (Egress) the device.

In configuration mode, create ingress and egress flow records using the appropriate interface direction commands. The match interface output and collect interface input cannot be configured in the ingress flow record. Also both interface input and interface output in the same flow record are not supported. Configure only one interface direction (input/output) in one flow record for the match and collect elements.

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

Not all devices support collecting and sending all of these options.

Step 1: Create Ingress record.

```
flow record StealthWatch-Record-IN
 description NetFlow record to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

Step 2: Create Egress record.

```
flow record StealthWatch-Record-OUT
 description NetFlow record to StealthWatch
 match datalink mac source address output
 match datalink mac destination address output
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

Cisco Industrial Ethernet switches implemented in the lab do not support the following record elements:

```
 match ipv4 ttl
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
```

Additionally, the timestamp options use a different syntax as follows:

```
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

For devices performing Network Address Translation, add the following command to track these permutations:

```
ip nat log translations flow-export v9 udp destination 10.9.10.32 2055
```

Optionally, to collect VLAN information, additional match statements can be added to non-routed interface records:

```
 match datalink vlan input/output
```

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.

Step 3: Create the flow exporter.

```
flow exporter StealthWatch-Exporter
 description StealthWatch Flow Exporter
 source Loopback0
 destination 10.9.10.32
 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). There are timers to determine whether a flow is inactive or a flow is long lived.

Step 4: Create the Ingress and Egress flow monitors using the records and exporter.

```
flow monitor StealthWatch-Monitor-IN
 description StealthWatch Ingress Flow Monitor
 exporter StealthWatch-Exporter
 cache timeout active 30
 cache timeout inactive 30
 record StealthWatch-Record-IN

flow monitor StealthWatch-Monitor-OUT
 description StealthWatch Egress Flow Monitor
 exporter StealthWatch-Exporter
 cache timeout active 30
 cache timeout inactive 30
 record StealthWatch-Record-OUT
```

Once the flow monitors have been created, they can be applied to the various device interfaces. Depending on the topology of the network and the flow information desired to track, input, output, or both monitors can be applied.

Step 5: Apply the flow monitors to the appropriate interfaces:

```
interface range GigabitEthernet1/1-16
 ip flow monitor StealthWatch-Monitor-IN input
 ip flow monitor StealthWatch-Monitor-OUT output
```

Troubleshooting Commands

Here are a few `show` and `clear` commands to keep handy for troubleshooting or viewing your NetFlow data from the switch. The following validation commands are for ingress (IN) flows. You may repeat the commands for in egress (OUT) traffic.

Commands to display NetFlow data:

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

Commands to reset NetFlow 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
```

Network Device SNMP

Additionally, SNMP can be configured to enable Stealthwatch to retrieve interface names automatically during discovery. As a best practice, and to meet today's compliance mandates, SNMP v3 should be implemented instead of v1 or 2.

Step 1: Configure an SNMP user to match the user credentials configured in Stealthwatch (this user will not be displayed in the normal device configuration)

```
snmp-server user V3User V3Group v3 auth sha Cisco1234 priv aes 128 Cisco1234
```

Step 2: Configure the permissions for the group to which the user is assigned.

```
snmp-server group V3Group v3 auth read V3Read write V3Write
```

Step 3: Define the appropriate views for read/write access.

```
snmp-server view V3Read iso included
snmp-server view V3Write iso included
```

Step 4: Define the IP addresses of the Management Console and collectors that will use the access.

```
snmp-server host 10.9.10.19 version 3 auth V3User
snmp-server host 10.9.10.31 version 3 auth V3User
snmp-server host 10.9.10.32 version 3 auth V3User
```

Network Firewall Flows

In the ASA, flows are exported using Network Secure Event Logging (NSEL) via the following configuration.

Step 1: Configure the global flow export destination and template.

```
flow-export destination management 10.9.10.32 2055
flow-export template timeout-rate 5
flow-export delay flow-create 5
```

Step 2: Create an access list to define the desired traffic flows.

```
access-list StealthWatch extended permit ip any any
```

Step 3: Create a class-map and specify the access list.

```
class-map StealthWatch_Map
 match access-list StealthWatch
```

Step 4: Apply the class map to the global policy (or another existing policy if desired).

```
policy-map global_policy
 class StealthWatch_Map
  flow-export event-type all destination 10.9.10.32
```

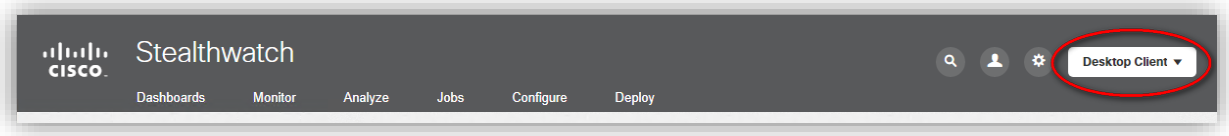
Stealthwatch Flow Collection

Once the devices have been configured to send NetFlow to the Stealthwatch collectors, further configurations can be added in Stealthwatch to identify these flows, categorize them, and create policies.

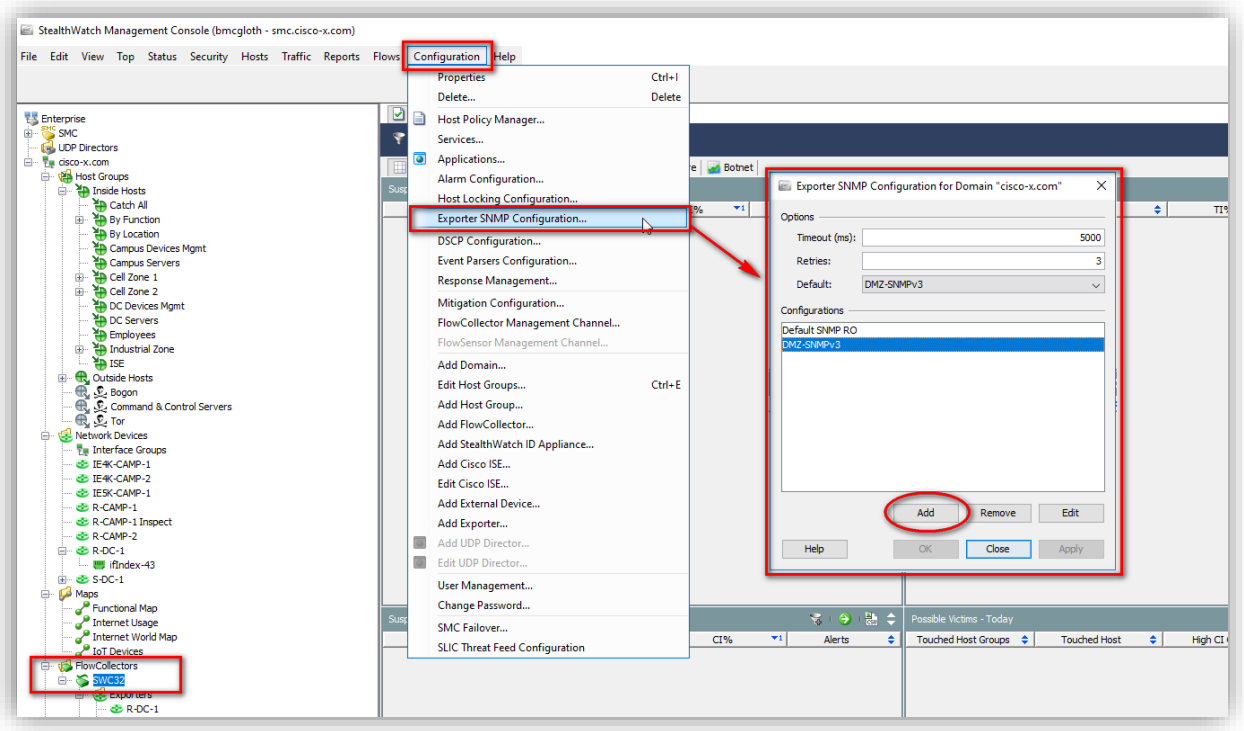
Stealthwatch Exporters

Each of the devices configured to send flows to Stealthwatch appear under the Exporters Interface Status table. Explicitly add the network devices to the Exporters list.

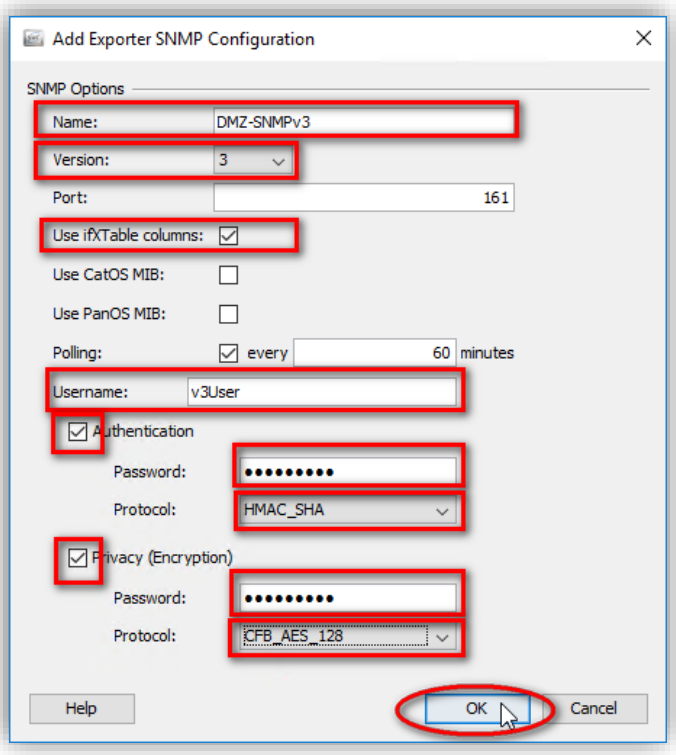
Step 1: Launch the Stealthwatch Java client and log in.



Step 2: First, add an SNMP exporter to be used for the new exporter profiles. Select a Stealthwatch Flow Collector, then on the Main Menu, select **Configuration > Exporter SNMP Configuration**. In the pop-up menu, click **Add**.

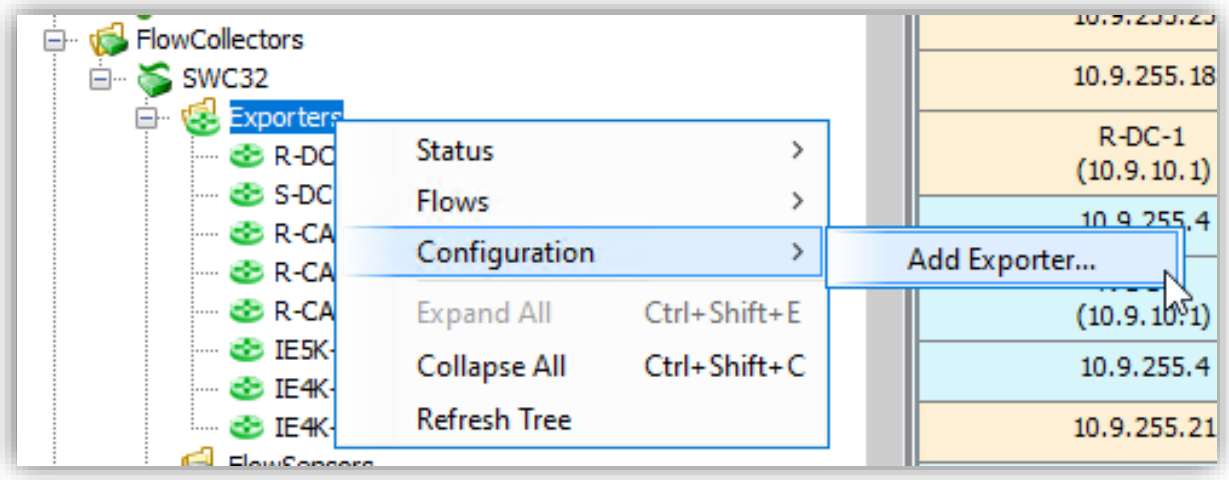


Step 3: Configure the new exporter to use the SNMP settings established for the network devices. Click OK and then **Close**.

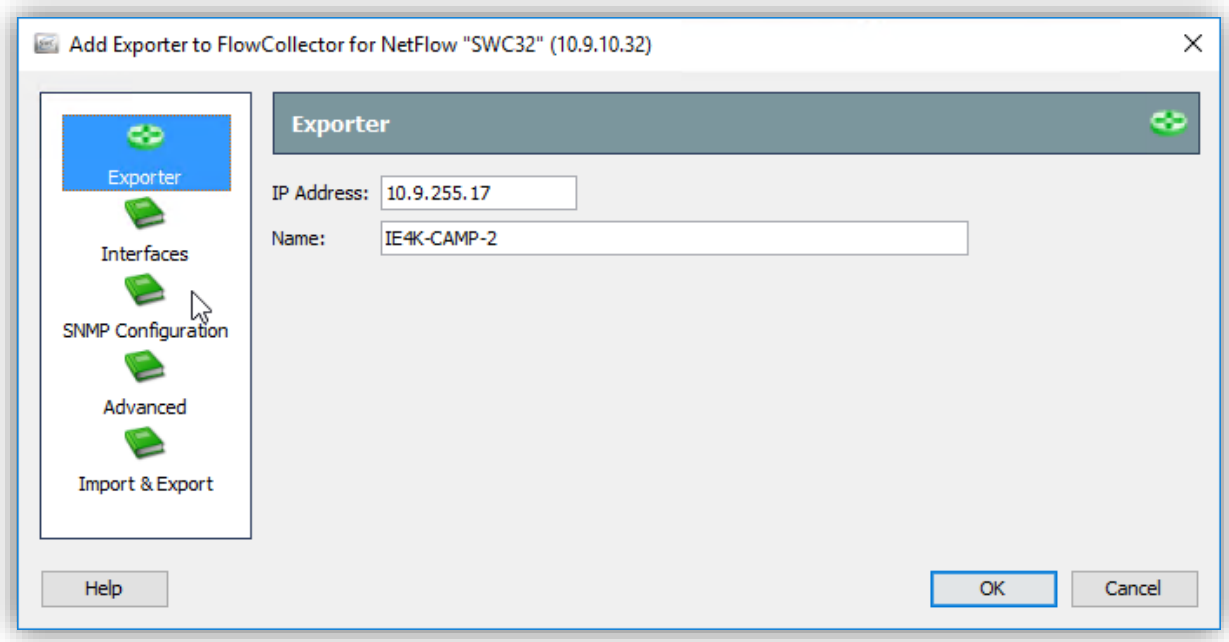


Return to Contents

Step 4: Expand the folder for a Stealthwatch Flow Collector, right-click the Exporters folder, and select **Configuration > Add Exporter** from the pop-up menu.

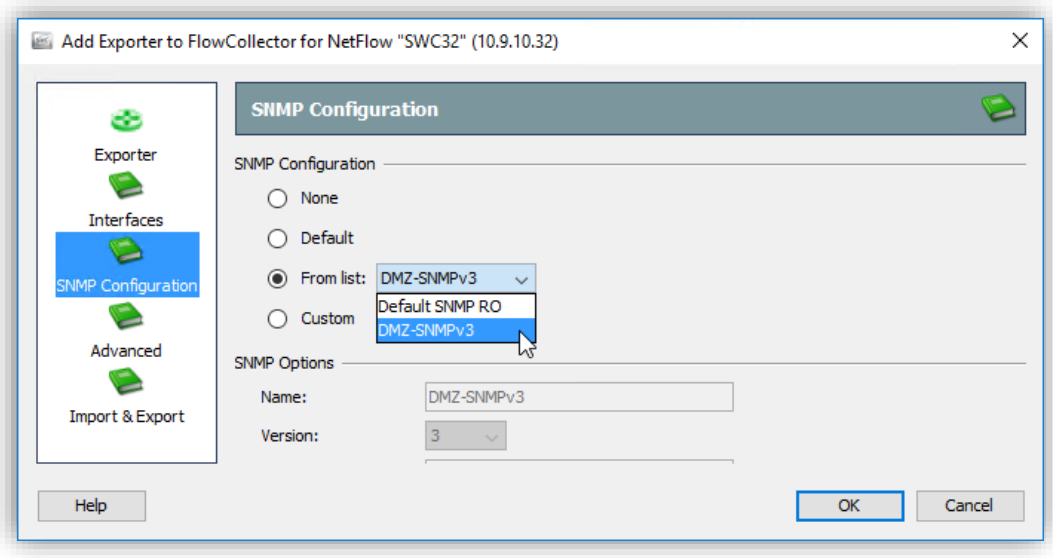


Step 5: Configure the IP address used by the device for sending NetFlow and add the device name.



Return to Contents

Step 6: Select the SNMP Configuration Icon, select the SNMP configuration from the list, and click **OK**.



Repeat Steps 4-6 for all devices sending NetFlows to Stealthwatch. Once complete, perform a Stealthwatch communication check with network devices using the following steps.

Step 7: Navigate to **Domain Name > Host Groups > Network Devices**, and make sure all the NetFlow-enabled Network Access Devices are listed.

Step 8: Expand Flow Collectors and make sure all the NetFlow-enabled Network Access Devices are listed.

Step 9: Verify NetFlow data collection. Expand Flow Collectors, right-click your Flow Collector, and navigate to **Status > NetFlow Collection Status**. Under Current NetFlow Traffic (bps), check the counters increment.

Step 10: Right-click the Flow Collection Status table header, and then check **Longest Duration Export** to enable the column to correlate the time duration for the flows.

Stealthwatch Host Groups

A host group is a " container" of hosts or IP addresses that share attributes and policies. Host groups enable establishing different thresholds or to bypass alerts for certain behavior. Using host groups correctly in the StealthWatch system will ensure that you are alerted correctly on events and that the information given to you is more relevant. The following are some of the different attributes you'd typically group together:

- Shared functions
- Exhibits similar behavior
- Can be managed as a single object
- To which a single policy can be applied
- To identify devices that you " own"

For IoT systems, we group different cell zones and other plant services similar to the groupings that would be used for TrustSec SGTs. StealthWatch will alert if IoT devices behave outside baseline behavior and thresholds, but using host groups can really trim down on any additional noise.

StealthWatch has several built-in host groups you can use. You can also define your own:

- Catch All–This contains all the RFC 1918 addresses, your private addresses, and your public IP addresses. Once an IP address is added to another host group, it will be removed from the Catch All container. It's the host group of last resort whenever a private IP address is not already assigned to another host group.
- By Function–This host group has several subgroups that have a pre-defined role policy. Some of the sub-groups include the following:
    - Proxy
    - NAT Gateway
    - Client IP Ranges (DHCP Ranges)
        - End User Devices
        - Guest Wireless Networks
        - Remote VPN IP Pool
        - Trusted Wireless
    - DMZ
    - Network Scanners
    - Other
        - Broadcast
        - Link-Local
        - Localhost
        - Multicast
    - Servers
        - Antivirus servers
        - Backup Servers
        - BigFix
        - Confidential Servers
        - Database Servers
        - DHCP Servers
        - DNS Servers
        - Domain Controllers
        - File Servers
        - Mail Servers
        - Multifunction
        - NTP Servers
        - SMS Servers
        - Terminal Servers

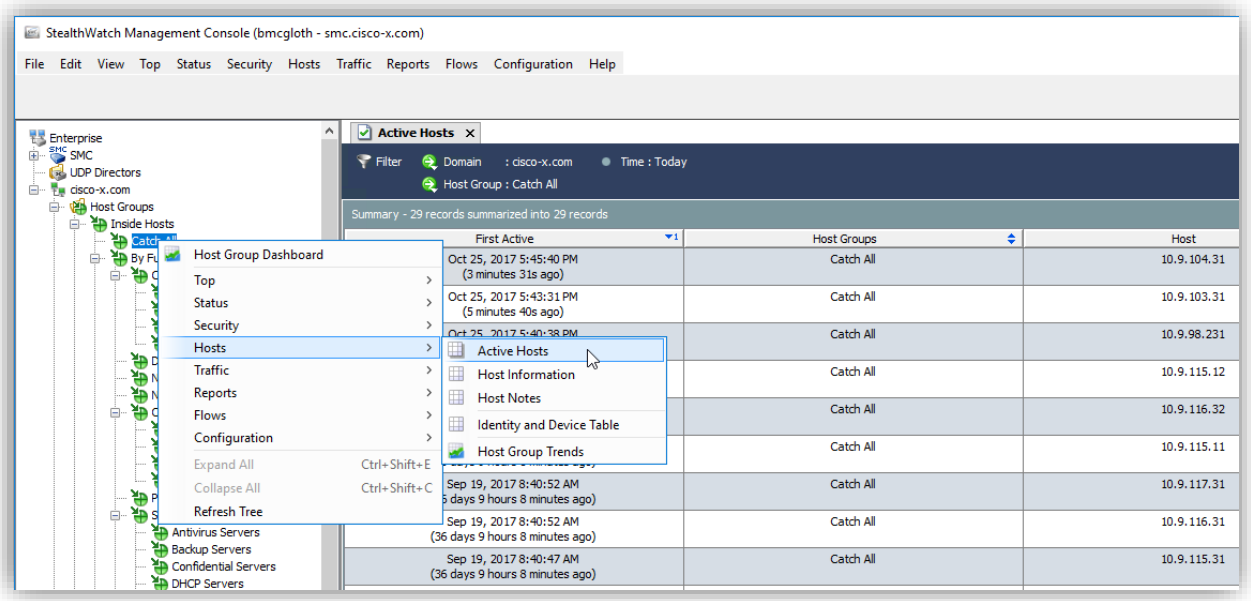
⮌Return to Contents

        - Web Servers
    - VoIP
        - VoIP Endpoints
        - VoIP Gateways
- By Location–There might be a situation where you want to group the devices by location. Each location can have their own DNS server or similar device types.
- Outside Hosts–This contains all the hosts identified as NOT being part of your network; basically, the internet.
- Command & Control Servers–This is only if you have the StealthWatch Labs Intelligence Center (SLIC) licenses. This host group contains known malicious hosts that should never be reached, and if a host is found trying to connect to it, you will most certainly get an alert.

Host groups are defined and managed in the Stealthwatch Java client, and information can be viewed by group in the Stealthwatch web interface. Hosts must be manually assigned to the appropriate groups. To view what hosts are in a given host group, do the following.

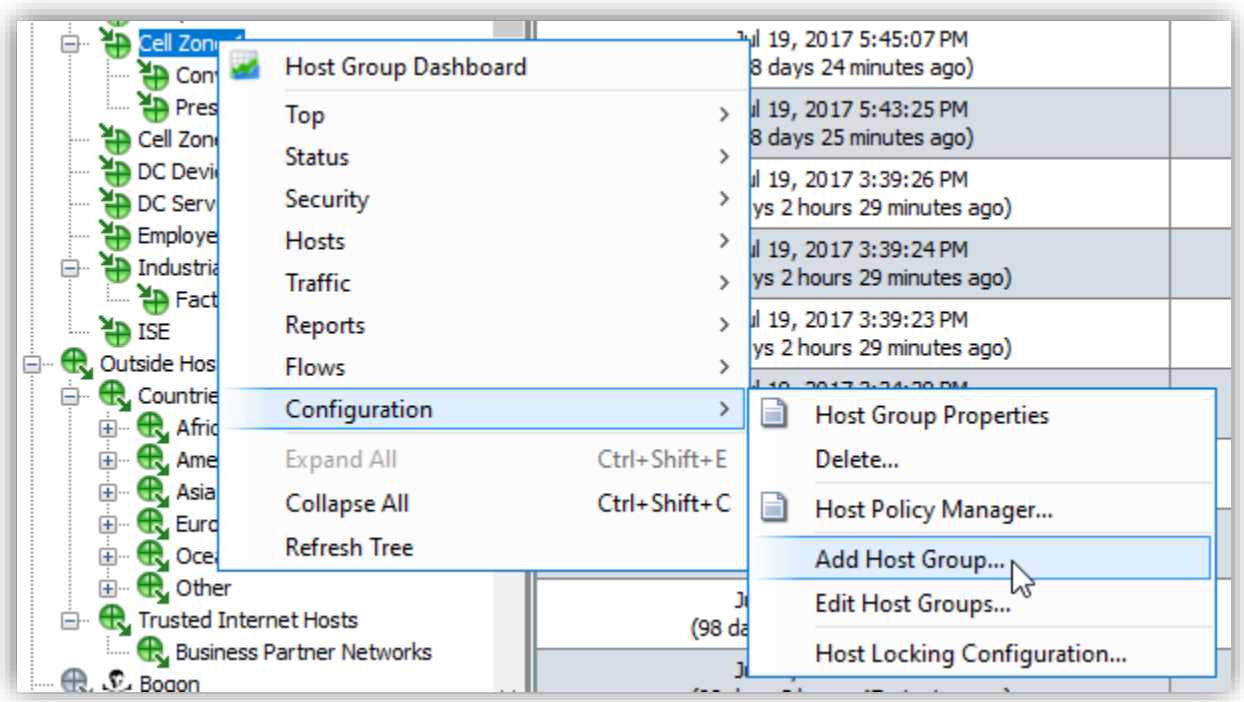
Step 1: Launch the Stealthwatch Java client and log in.

Step 2: Highlight the host group, right-click and from the menu, navigate to **Hosts > Active Hosts** to view the active hosts in that Host Group.

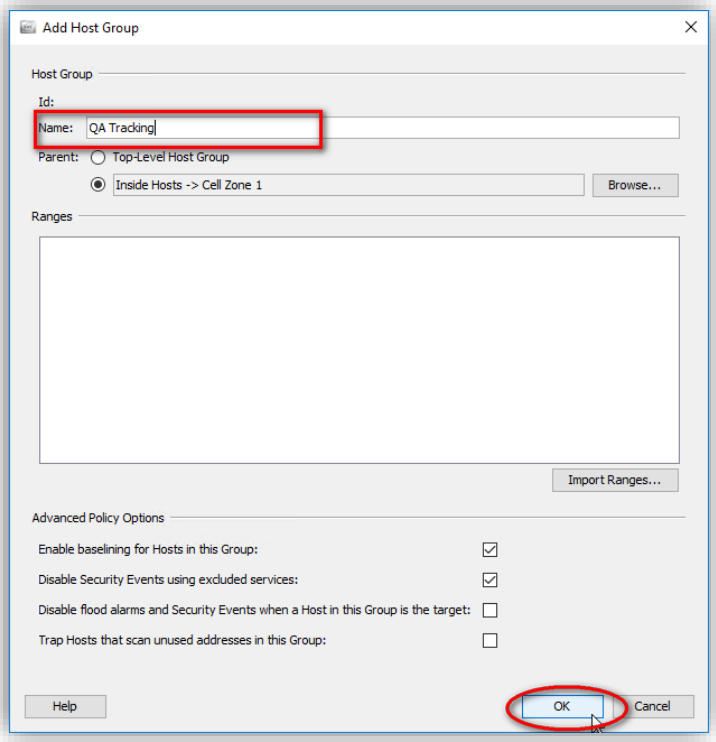


↩Return to Contents

Step 3: To create a new host group, highlight an existing group, right-click and navigate to **Configuration > Add Host Group...**

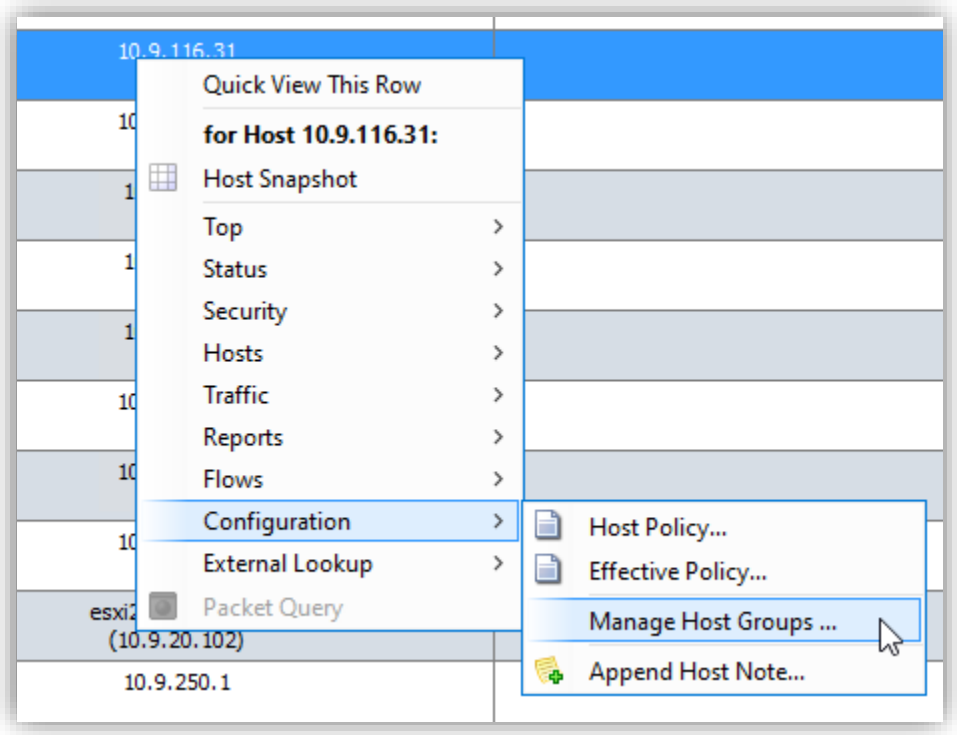


Step 4: Assign a name, and click **OK**.

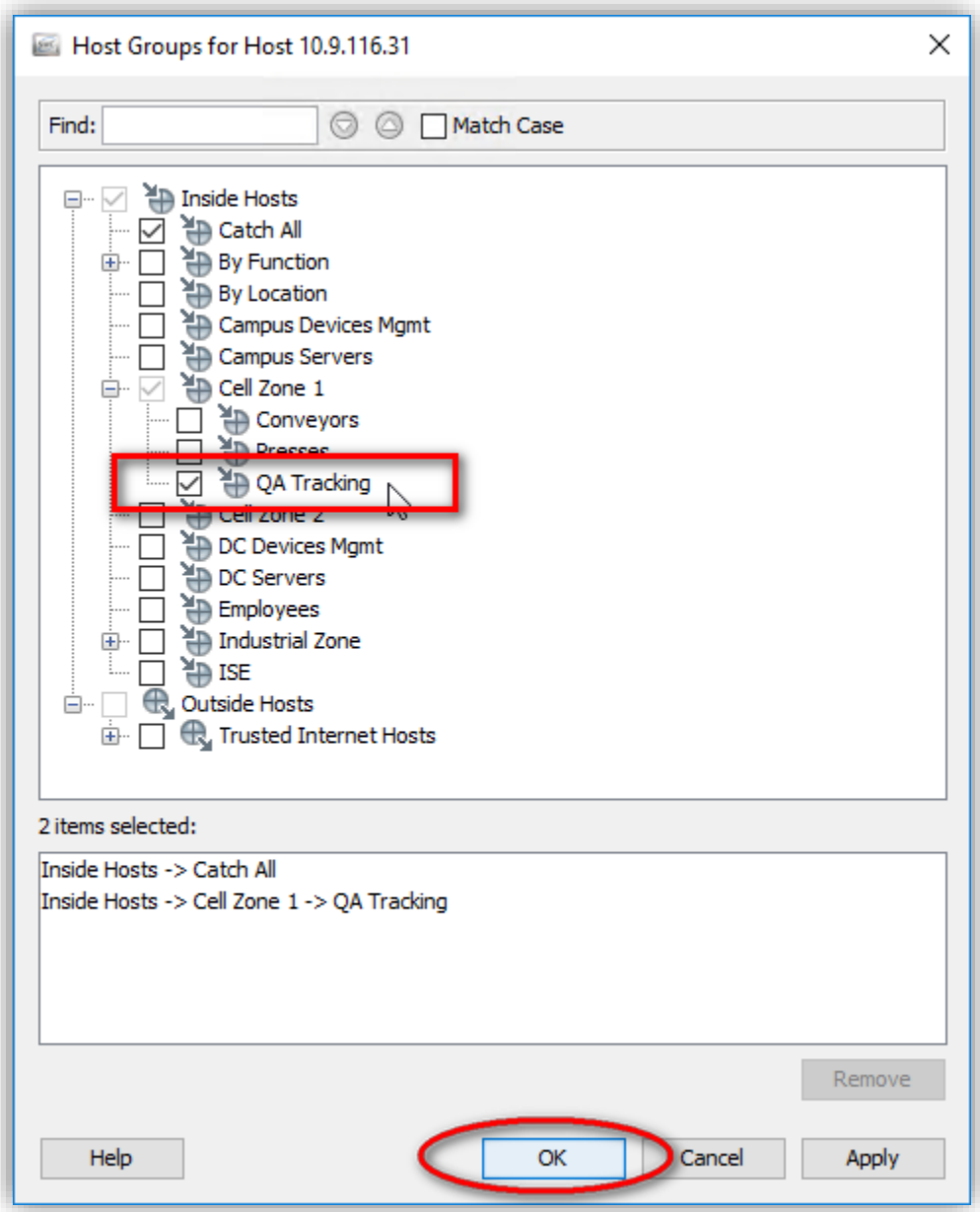


Return to Contents

Step 5: To move a host into a different host group, highlight an IP from the Active Hosts table, right-click and navigate to Configuration > Manage Host Groups...



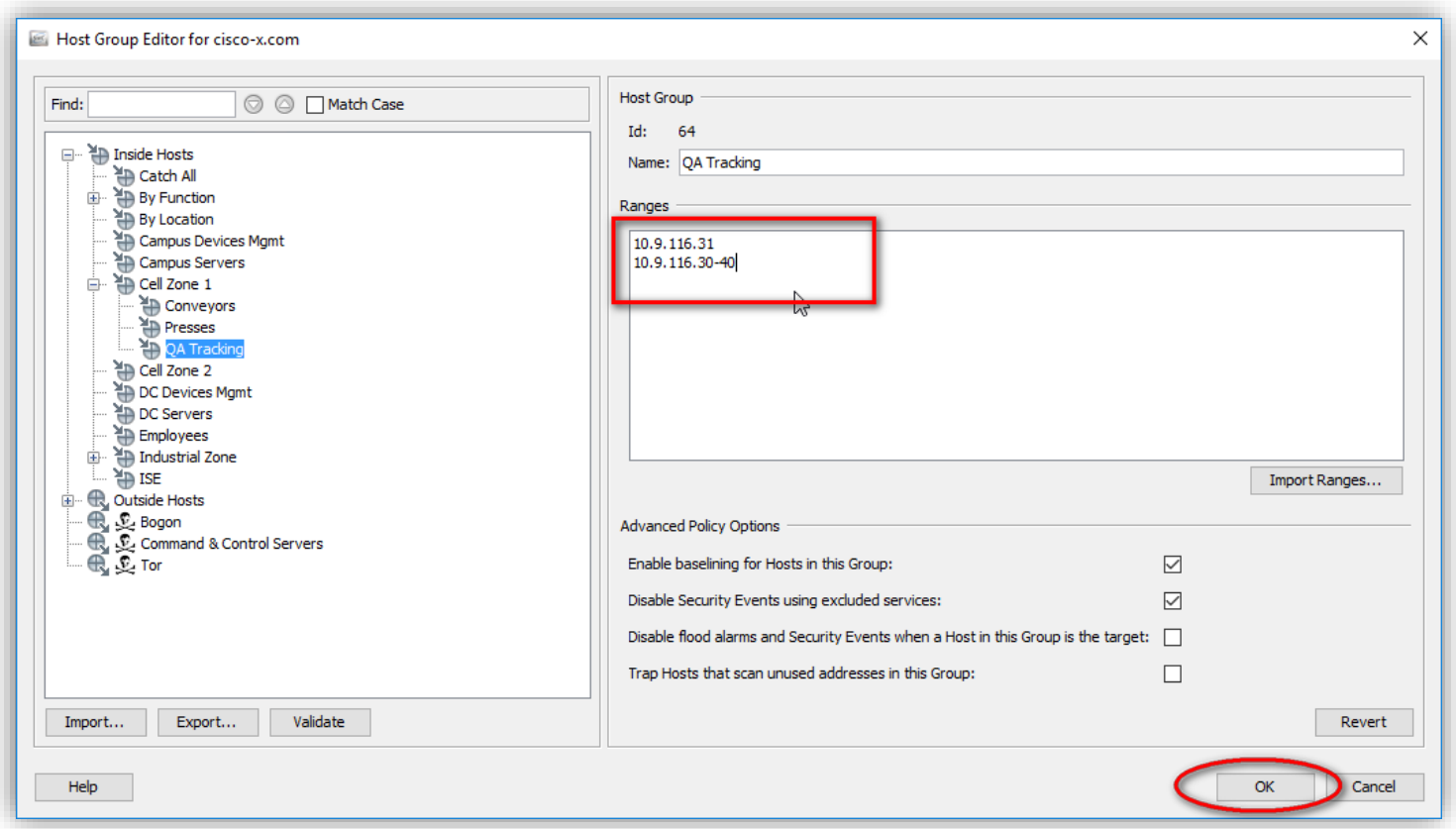
Step 6: From the pop-up, select the new host group to which to assign the device, then Click **OK**. A host may be a member of one or more host groups.



In addition to statically assigning hosts to groups, a range of IP addresses can be defined in the host group to more easily enable categorization. This works well for Industrial IoT systems because many are deployed with static IP addresses instead of DHCP, or use DHCP scopes for specific VLANs if TrustSec is not used for segmentation.

Return to Contents

Step 7: Assign ranges to host groups, highlight the host group, right-click, and navigate on the main menu to **Configuration > Edit Host Group.** Add the device IP address, a range of addresses, or subnets. Click **OK** when complete.

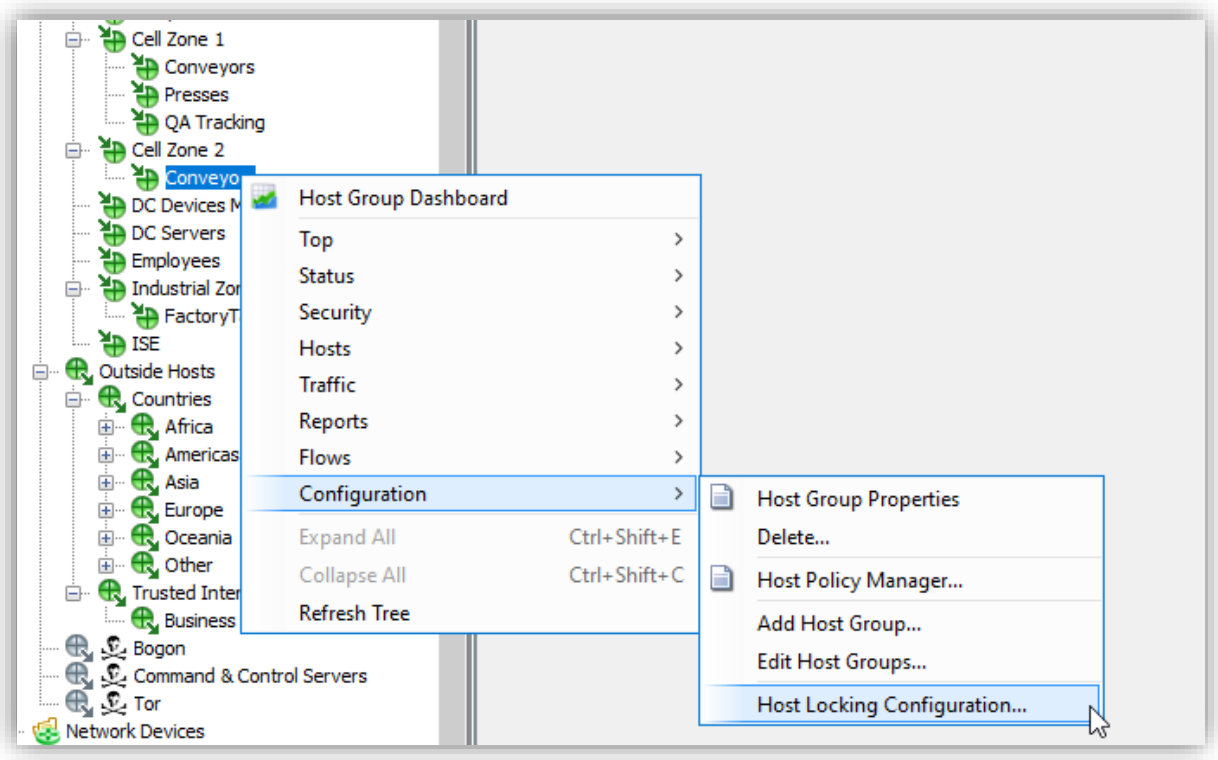


Return to Contents

Now that you have defined the relevant host groups, and assigned devices and IP ranges to them, Host Policies can be updated and new locking policies specified. These policies enable the visibility necessary to detect additional anomalies in the network specific to the devices and protocols deployed.

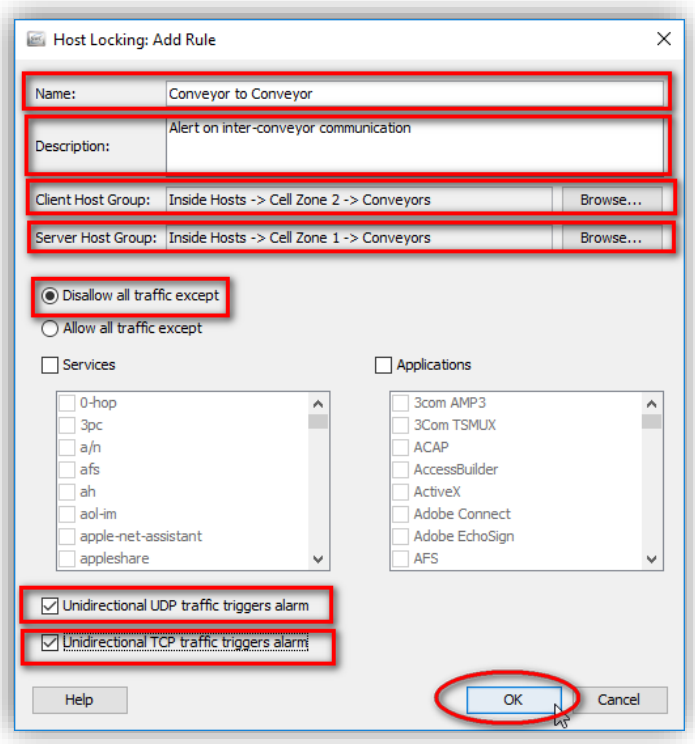
An example of this would be that your PLC from cell zone 1 should never interact with a conveyor system in cell zone 2. If you created a host locking policy that states that those two host groups should never communicate, Stealthwatch generates an alarm if it ever happens. This provides the visibility and alerting to ensure your security controls and segmentation are working correctly.

Step 8: Highlight a host group, right-click, and navigate to Configuration > Host Locking Configuration.



Return to Contents

Step 9: From the pop-up window that appears, click **Add**, Enter an appropriate name and description. Select the host groups, the traffic to disallow and alert on, and click **OK**.

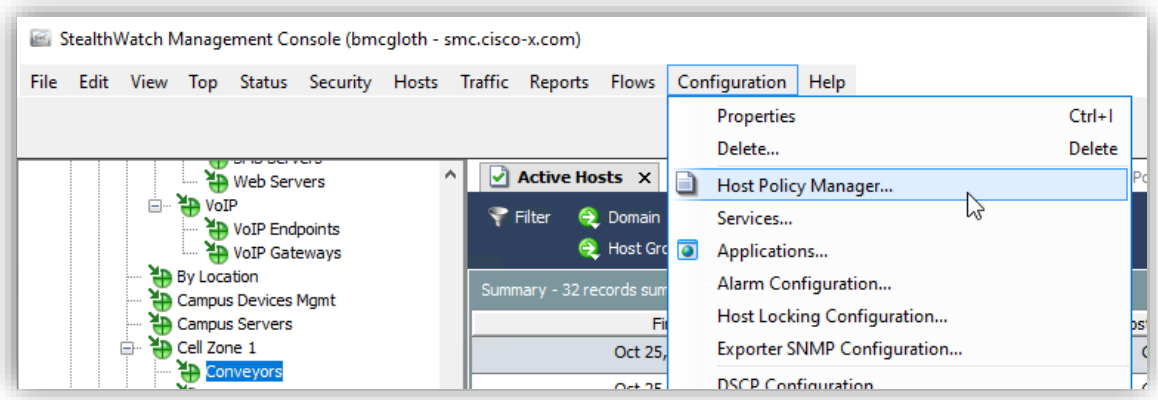


The Host Policy Manager dialog allows you to configure policies using the following sections:

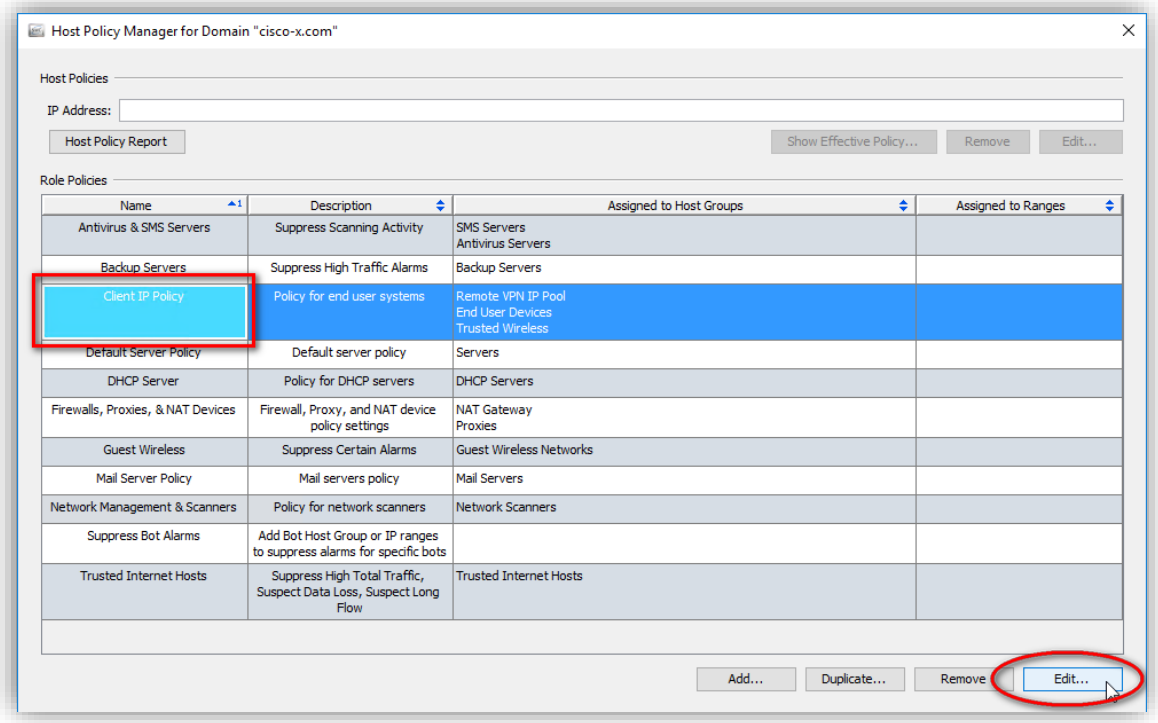
- Host Policies–Allows you to manage a policy for a single host
- Role Policies–Allows you to manage policies for hosts according to the roles that they perform in your system
- Default Policies–Allows you to manage the default policies for inside hosts or outside hosts

When determining which policies will apply for a particular host, the SMC first applies the default policy, then it applies the applicable role policy or policies, then finally it applies a host policy if one exists. If a host is affected by more than one role policy, the SMC determines for each alarm which policy's settings are used in the host's effective policy.

Step 10: Add the IoT host group to an existing policy. Select a host group. On the Main Menu, select **Configuration > Host Policy Manager...**

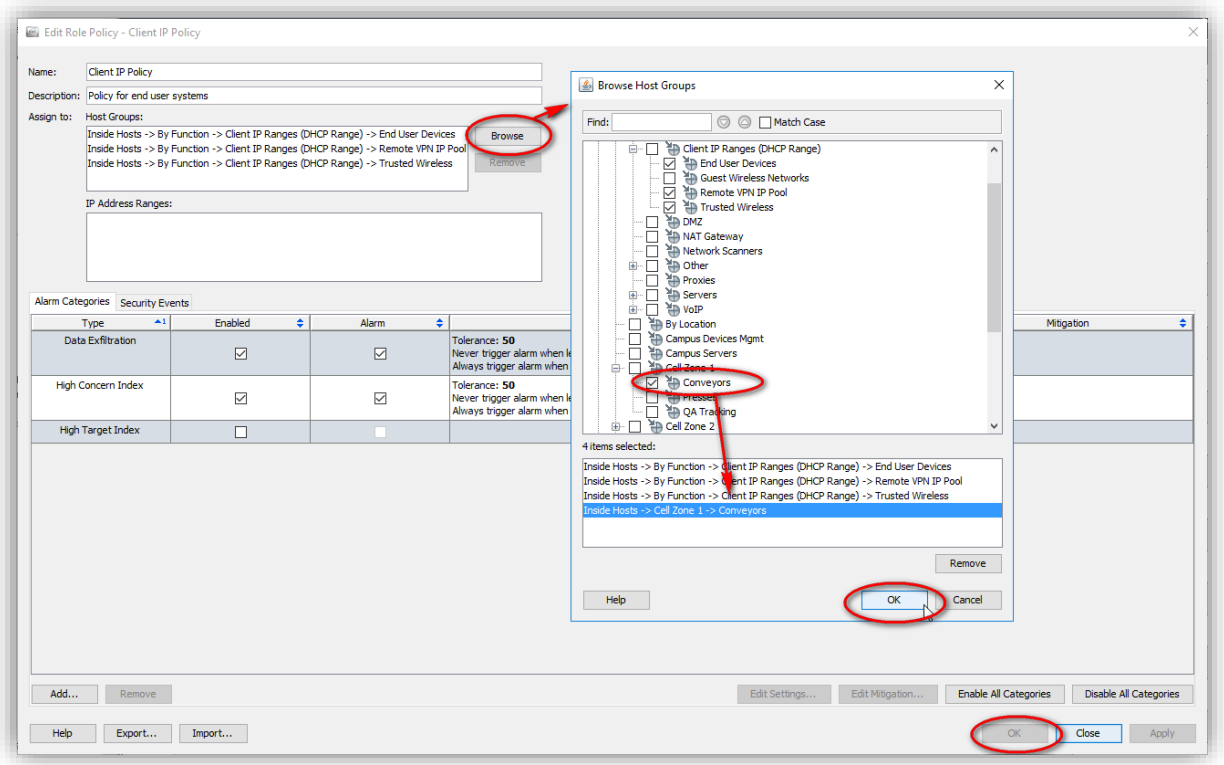


Step 11: Select the Client IP Policy, then click **Edit**.



↩Return to Contents

Step 12: Add the host group Conveyors in Cell Zone 1 to the policy. Click **OK**, **OK** and **Close**.



Create and apply new policies to host groups as appropriate for your organization.

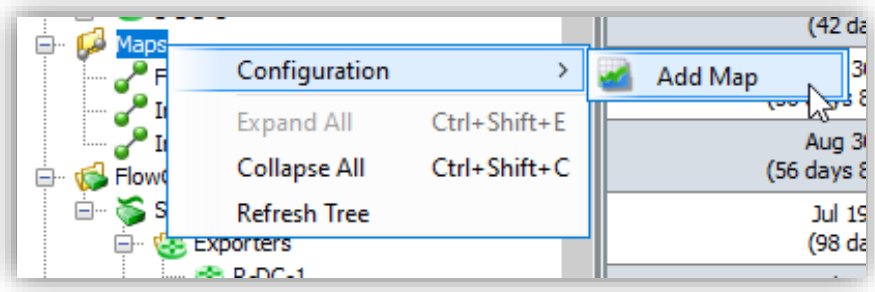
↩Return to Contents

Stealthwatch Maps

The map feature of the SMC lets you use drag-and-drop functionality to add host groups to a map, and then connect them, creating a host group relationship. The map then displays the status of the host groups, showing live data such as active alarms and traffic bandwidth. In addition, you can add images, lines, and text boxes to aid in the visual representation of your environment. You can change the domain or map using the filter. This feature allows you to graphically monitor the status of your entire system in near real-time.

When you open an existing map, it opens in View mode by default. View mode allows you to view a map and all the associated status information. When you save a map after editing it, the SMC sends the host group relationship information to the Stealthwatch Flow Collectors. The map becomes active and begins refreshing every minute. Now we'll add a new map for our IoT systems.

Step 1: On the Enterprise tree, right-click the **Maps** node. On the pop-up menu, select **Configuration > Add Map**.

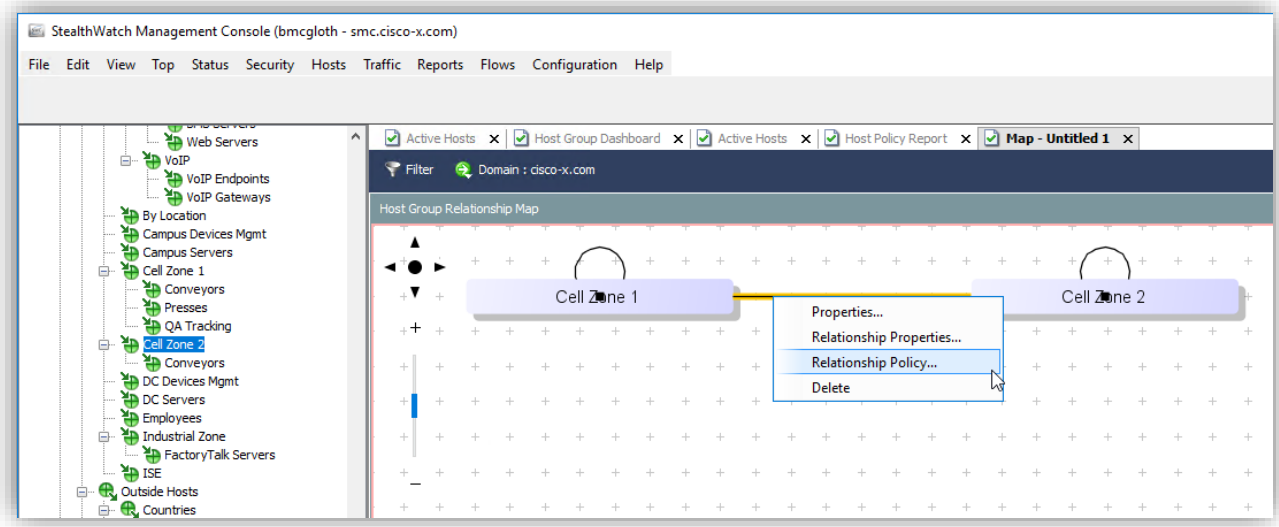


The map appears as a new document. You are now ready to configure it.

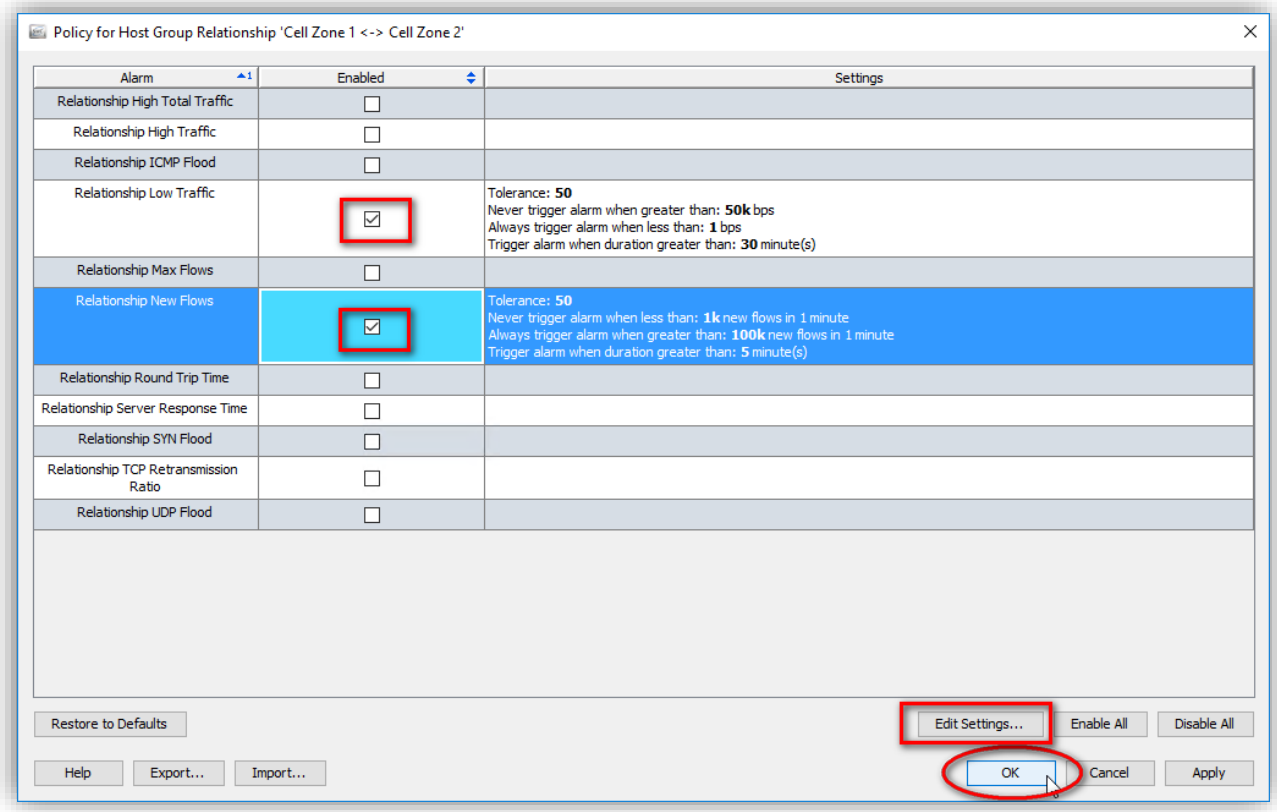
Step 2: Using the left mouse button, drag and drop the desired host groups from the Enterprise tree to the map.

Step 3: Create relationships between the host groups on the map. To do so, use the left mouse button to drag a line from one host group to another. If you want to monitor traffic within a host group, draw the line back to the same host group that you started from.

Step 4: Add a policy to the group relationship by selecting the line between the groups with the left mouse button, then right-click and select Relationship Policy.

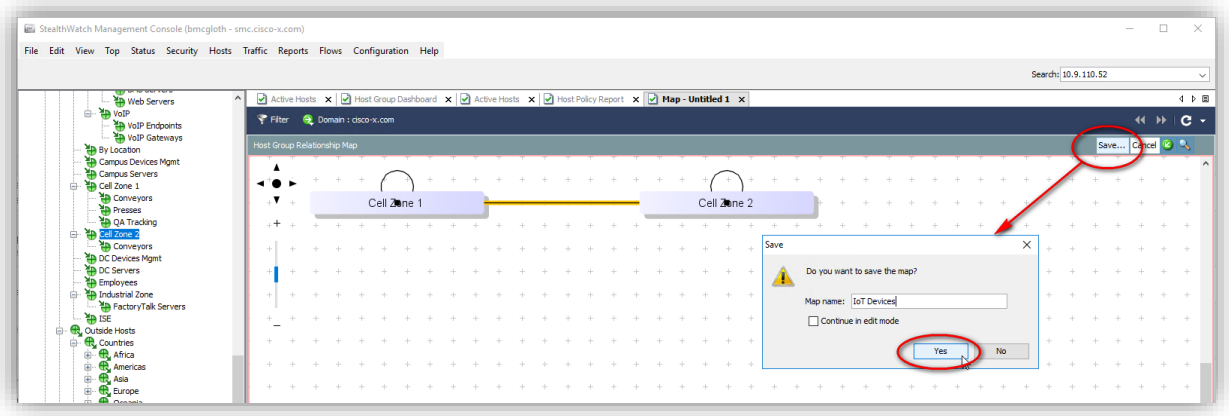


Step 5: Enable the desired policies and edit their settings if desired. Click **OK** to apply the map.

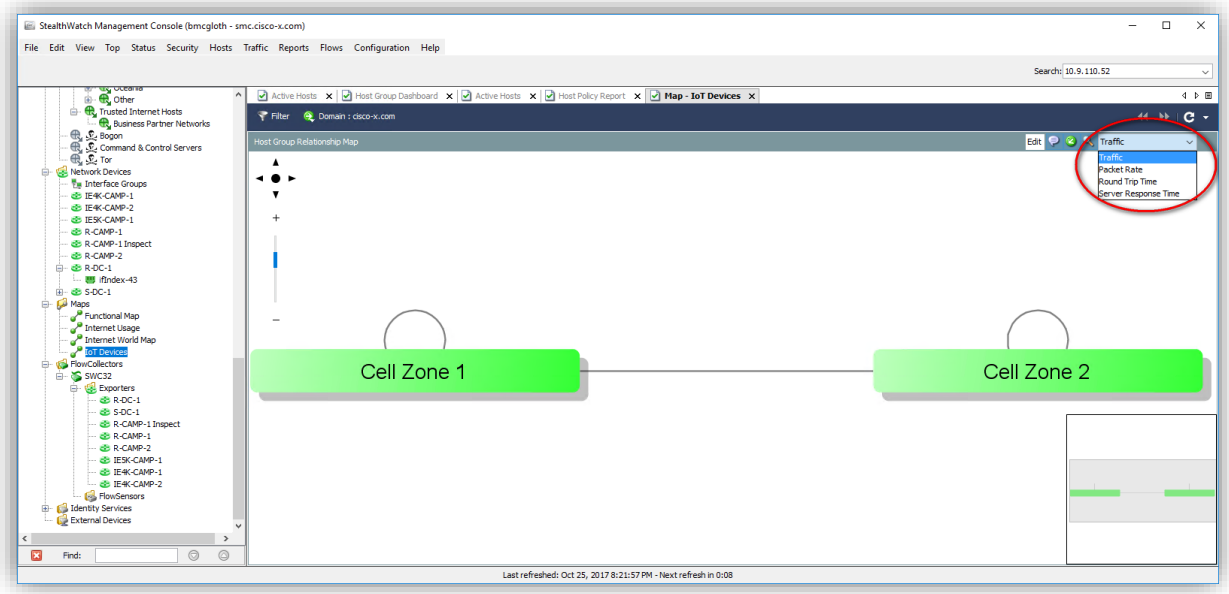


Return to Contents

Step 6: When finished customizing your map, click the **Save** button in the map's upper right corner, enter a Map name, and click **Yes**.



The SMC saves the map, and it becomes active immediately. Additional information can be viewed by selecting the dropdown in the upper right corner.



Return to Contents

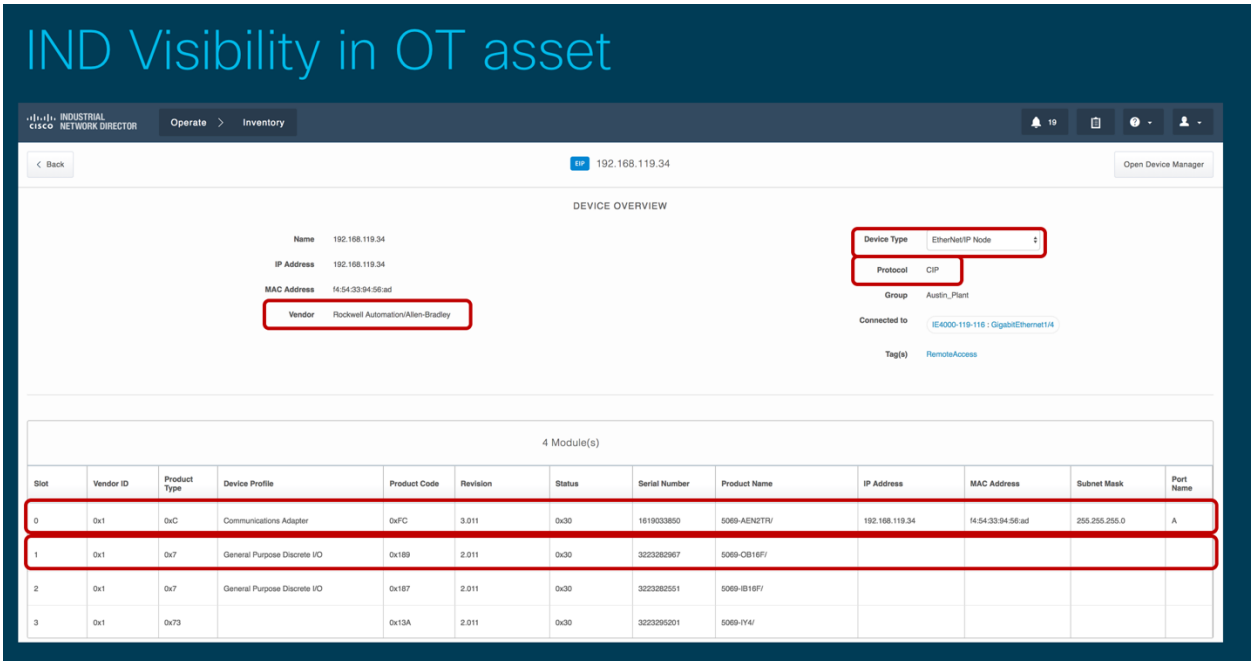
Industrial Network Director

Purpose platform built for managing industrial networks, the Cisco Industrial Network Director is designed to help operations teams gain full visibility of network and automation devices in the context of the automation process and provides improved system availability and performance, leading to increased overall equipment effectiveness (OEE) Industrial Network Director along with the ability management Industrial Ethernet Network it can also discover OT endpoints such as PLC, IO, RTU devices etc. IND discovers these devices by communicating in their Native communication protocol. IND supports discovery of OT endpoints that speak Industrial protocols:

- CIP (Common Industrial Protocol)
- Profinet
- BACNet
- Modbus

Cisco IND collects set of attributes from OT endpoints to provide visibility into OT assets, as shown in the picture below IND is able to show asset information like Vendor, Communication, Protocol, Product Name, Serial Number, Device type if it is a PLC, I/O, etc.

Figure 17 – IND Attributes



Return to Contents

Cisco IND Integration with ISE

IND is integrated with ISE using pxGrid (Platform Exchange Grid). IND is the source of OT asset attributes acting as a pxGrid Publisher as show in Figure *18*, ISE receives these attributes acting as a pxGrid Subscriber as shown in Figure *19*.

Figure 18 – IND pxGrid Server/ISE settings

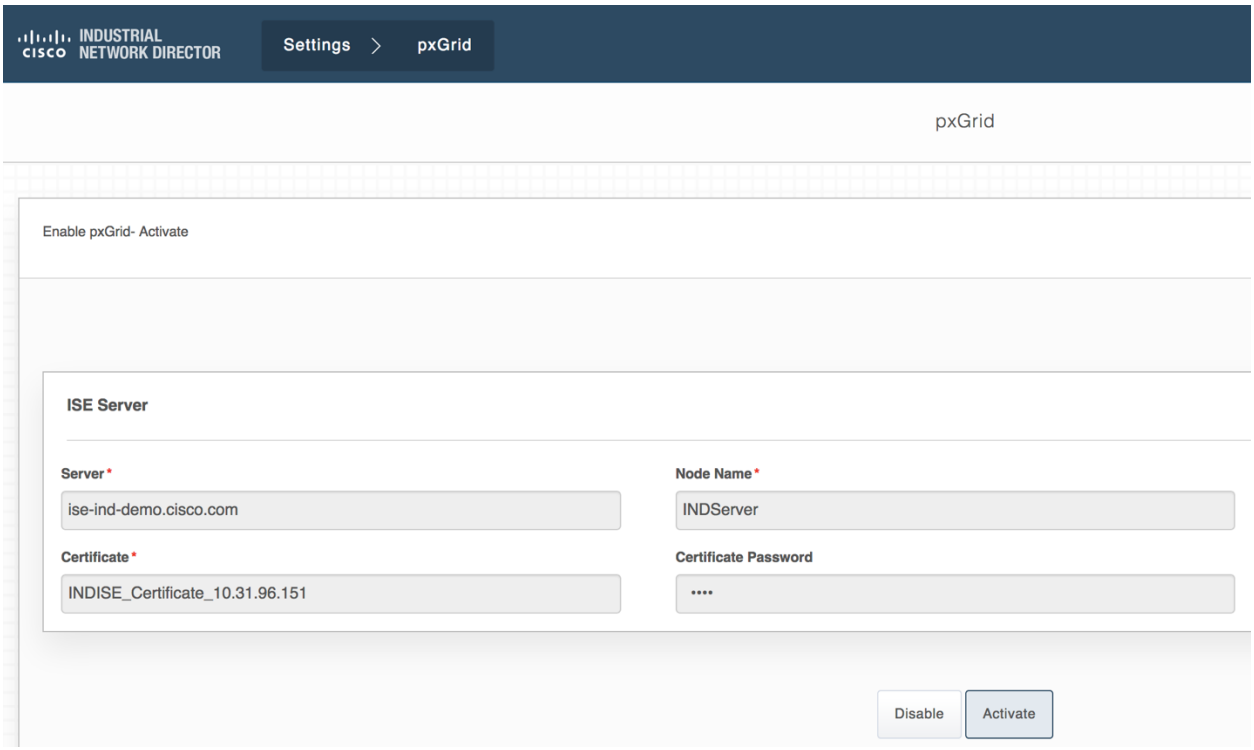
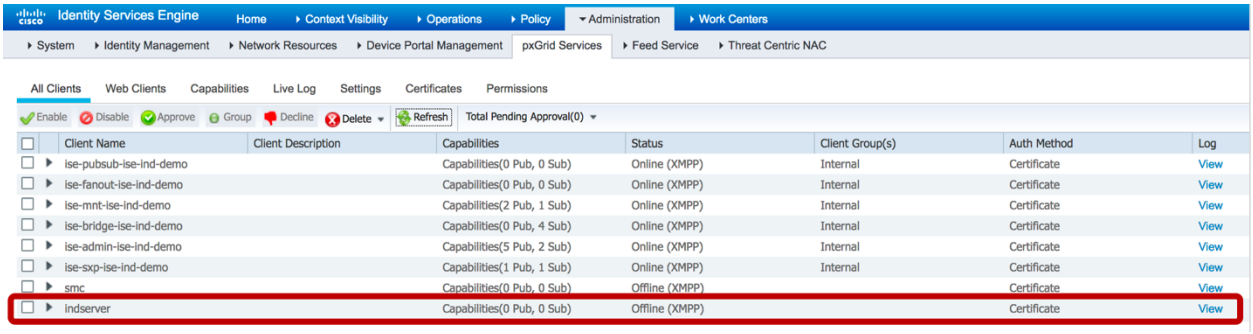


Figure 19 – IND registered as pxGrid publisher

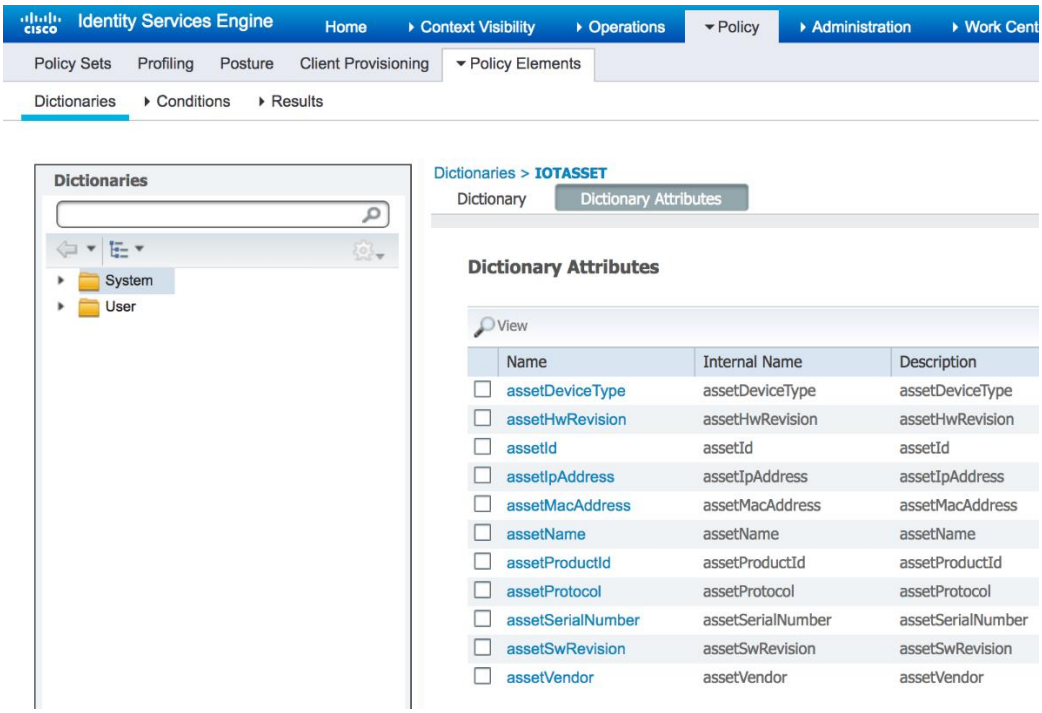


Return to Contents

85
IOTASSET Dictionary

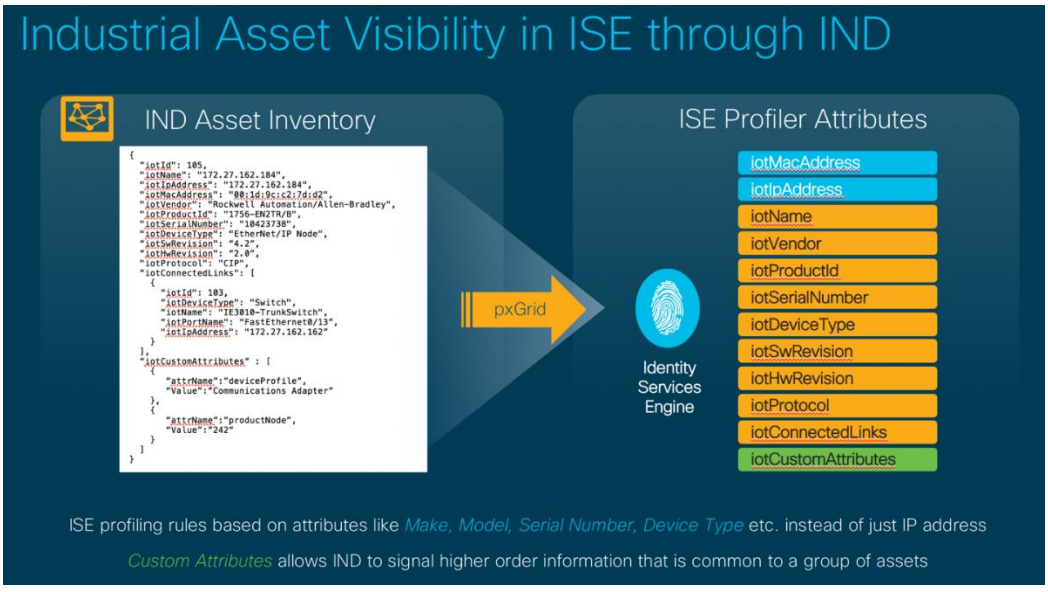
Cisco IND shares OT asset contextual information with ISE using pxGrid (Platform exchange grid), The new “IOTASSET” dictionary is created on ISE to receive OT asset attributes from IND. *Figure 20* below shows the IOTASSET dictionary and attributes specific to the OT asset.

Figure 20 – IOTAsset Dictionary Attributes



The IOTASSET dictionary attribute can be used to create profiling policies specific to OT device characteristics, which in turn can be used to push appropriate secure access policies to the network infrastructure (e.g., Switches, Firewalls etc.).

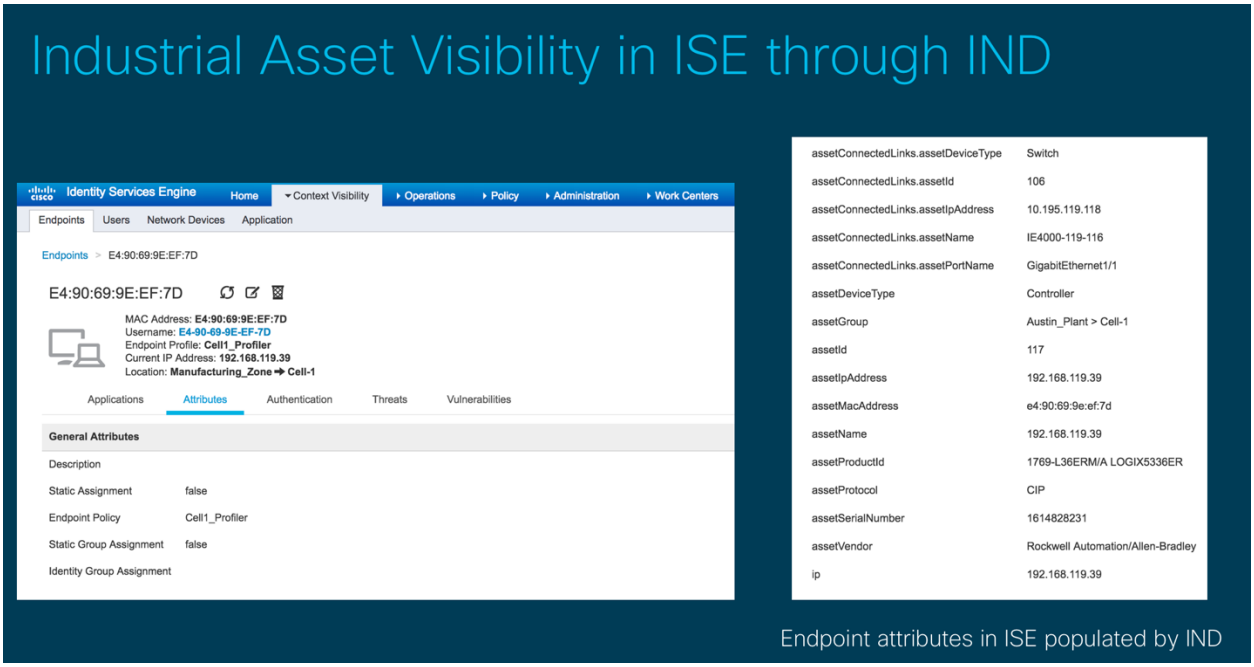
Figure 21 – Inventory Attributes



Return to Contents

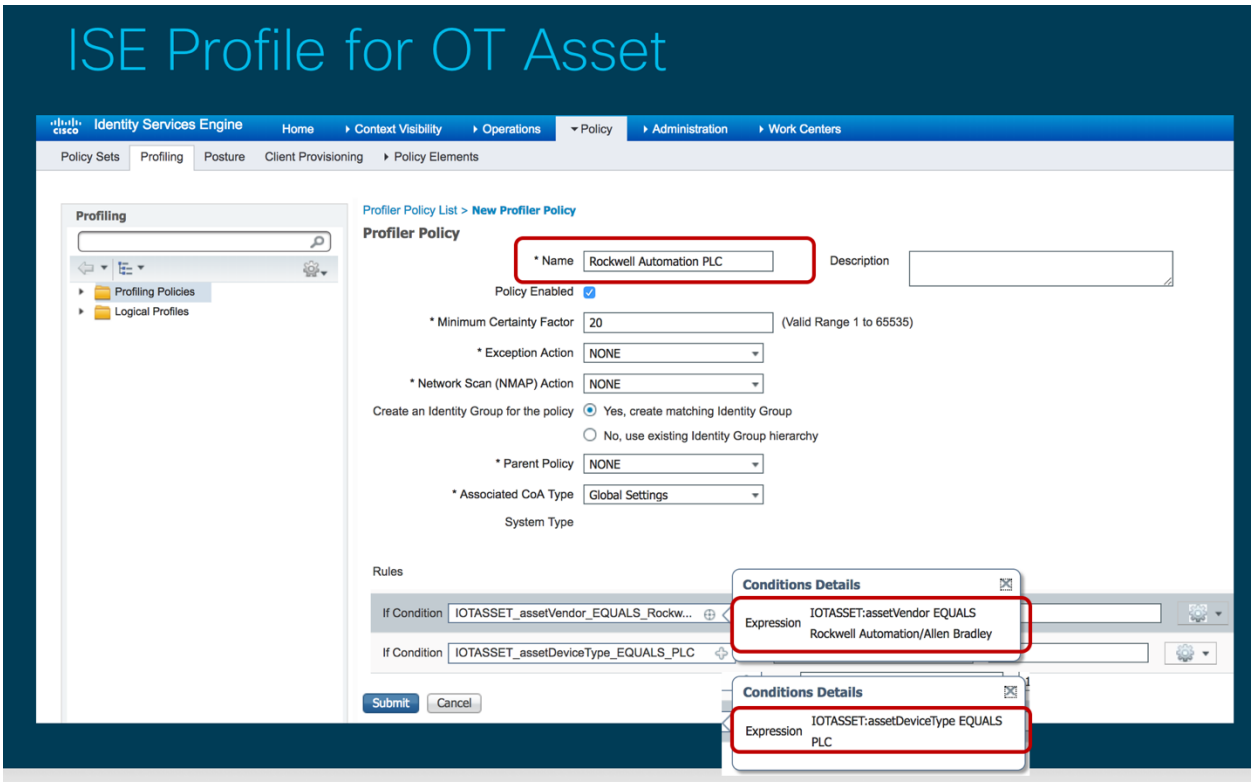
Figure *22* shows the asset attributes received from IND on ISE

Figure 22 – Asset Visibility



As shown in Figure *23* create new device profiles on ISE based on attributes received from IND.

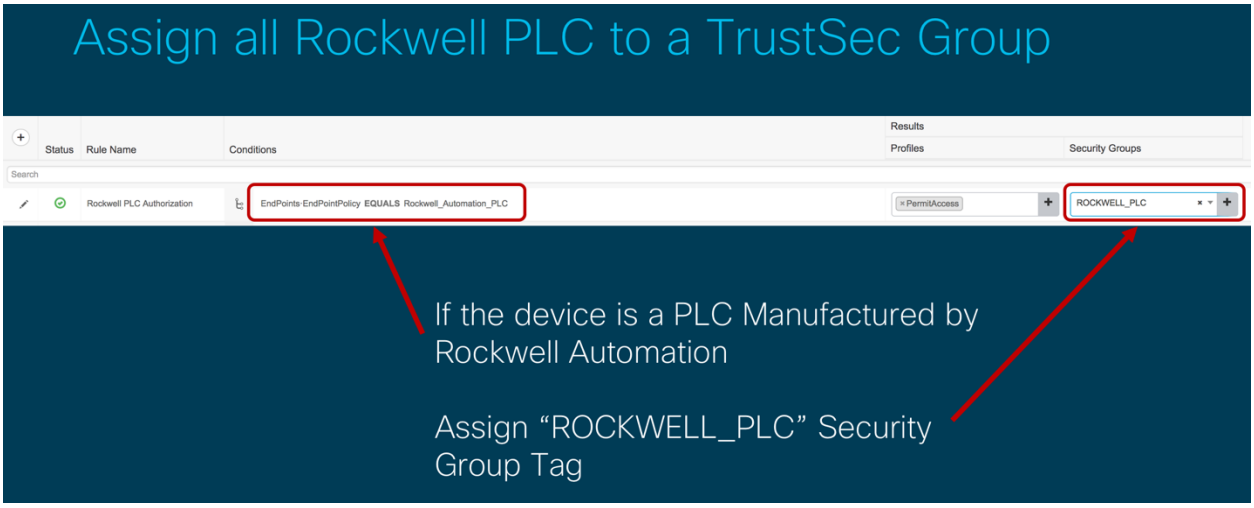
Figure 23 – Create ISE Profiler Policy



↩Return to Contents

Creating a Security policy on ISE based on the IOTASSET attributes to Group all PLC's manufactured by Rockwell Automation as shown in Figure *24*.

Figure 24 – Policy to Security Group



OT Intent based Security

Custom Attributes:

There are two new Custom attributes created on ISE and values for these attributes can be sent from IND for an asset:

1. assetGroup
2. assetTag

The custom attributes can also be used as regular OT asset attributes on ISE and can be used in Profiling devices and assign security policies for the devices.

As the Custom attribute values for a device are locally defined on IND, these can be manipulated based on "Users Intent" and trigger change in the policy on ISE.

Use Cases

Here we illustrate two customer use cases that can be fulfilled using IND & ISE integration and based on the user Intent:

1. Segmentation in OT Network
2. OT Intent based On-demand Remote Access

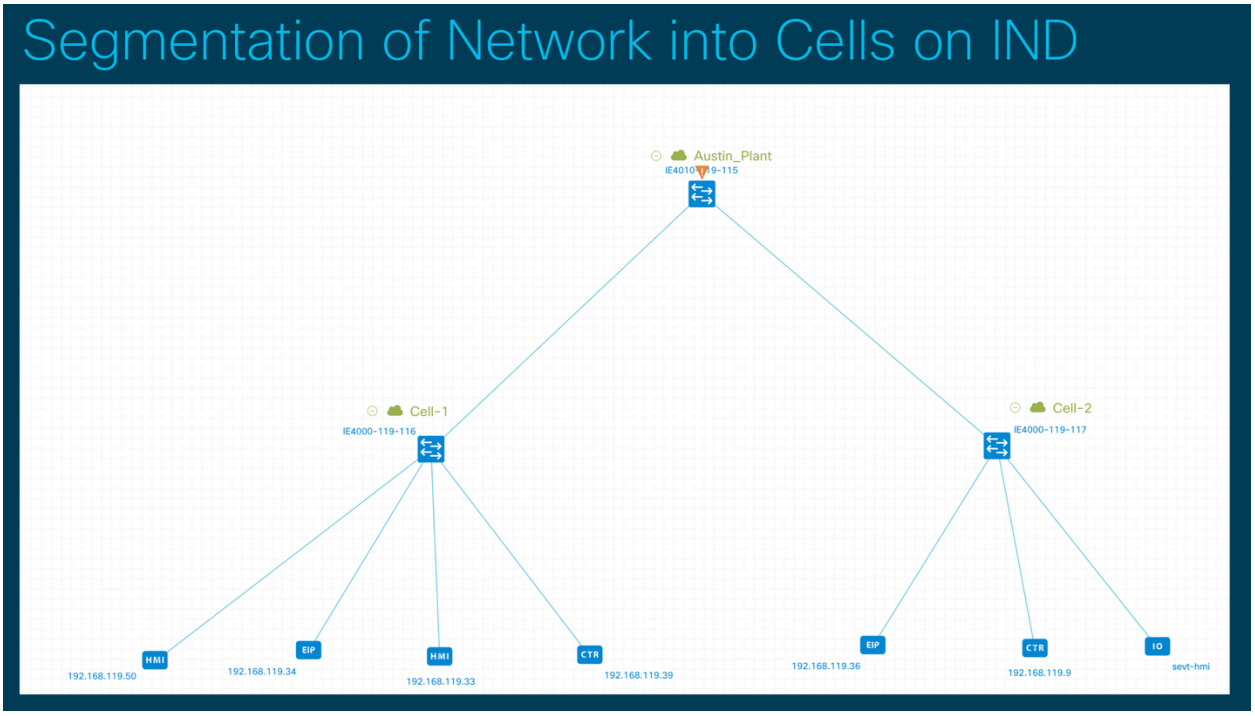
Segmentation in OT Networks

Segmentation in Industrial Networks is critical to ensure security. The security standards which govern Industrial Networks (e.g., ISA99, IEC62443 etc.) all prescribe segmentation as the start of a security journey.

On IND all the assets can be organized into different Groups to resemble the Physical location and Hierarchy in the Network. The Group in the IND can be sent as a Custom attribute(assetGroup) value to ISE to influence an endpoint profile on ISE.

As shown in Figure *25*, the network is segmented into 2 different cell's: Cell-1 and Cell-2

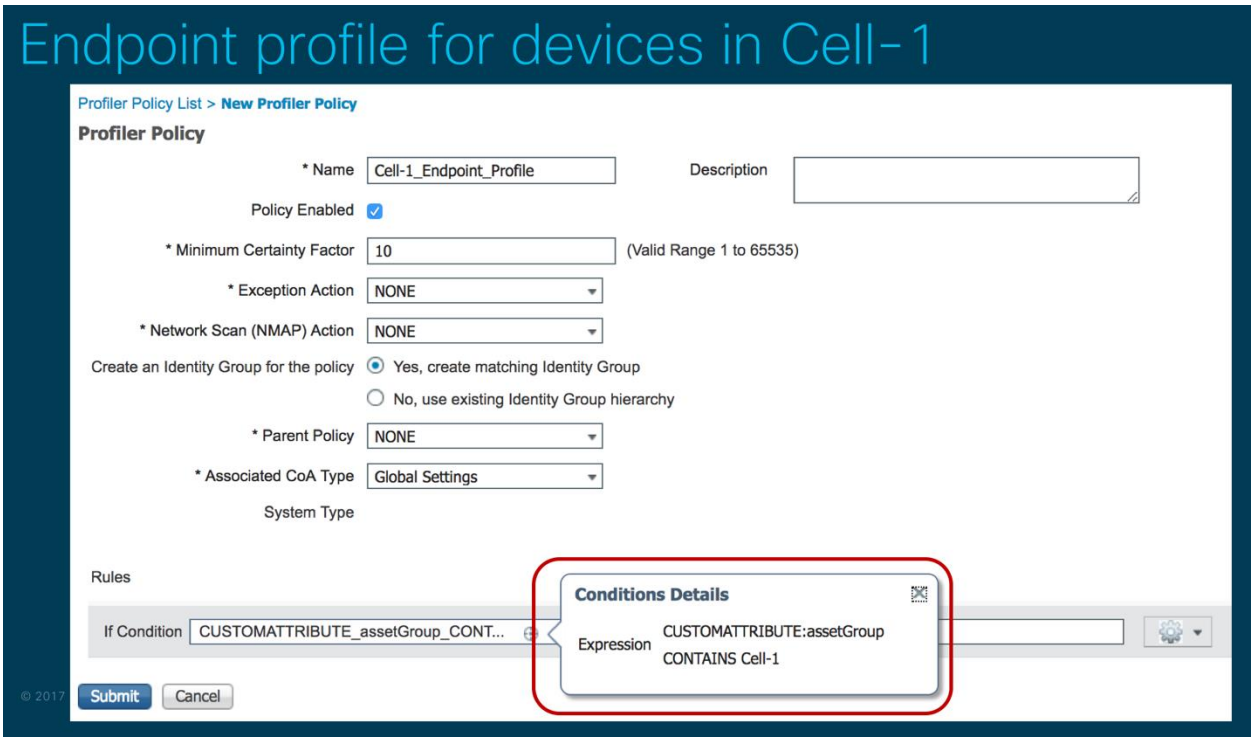
Figure 25 - IND Topology Diagram



Return to Contents

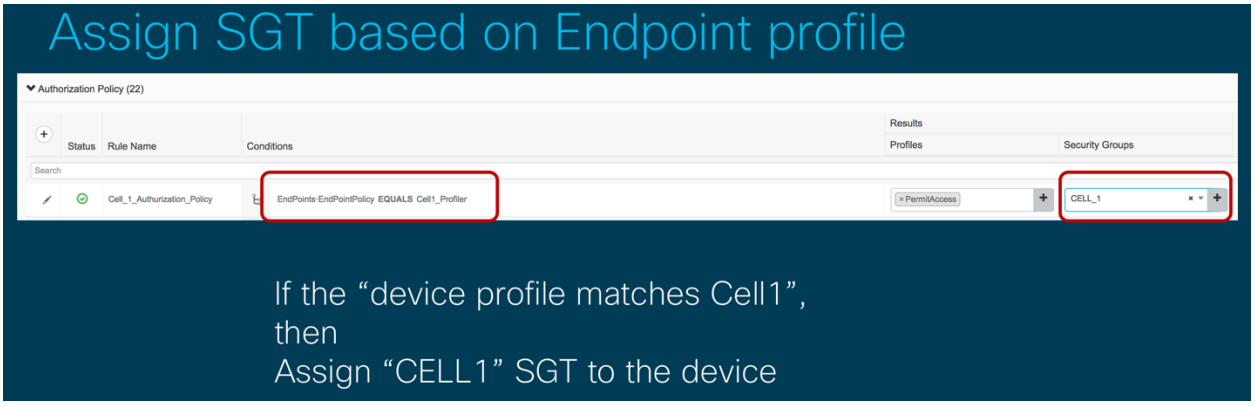
On ISE, the assetGroup custom attribute value is the group defined on IND, *Figure 26* shows the endpoint attributes for 2 devices received from IND. The devices have different values in the assetGroup custom attribute as both of them belong to 2 different Cells/groups on IND.

Figure 26 – Endpoint Attributes



Endpoint profiles on ISE can be created based on assetGroup custom attributes. As shown in Figure *27*, a Security Group Tag(SGT) can be assigned to endpoint as a result of Authorization policy which will be based on the Endpoint profile.

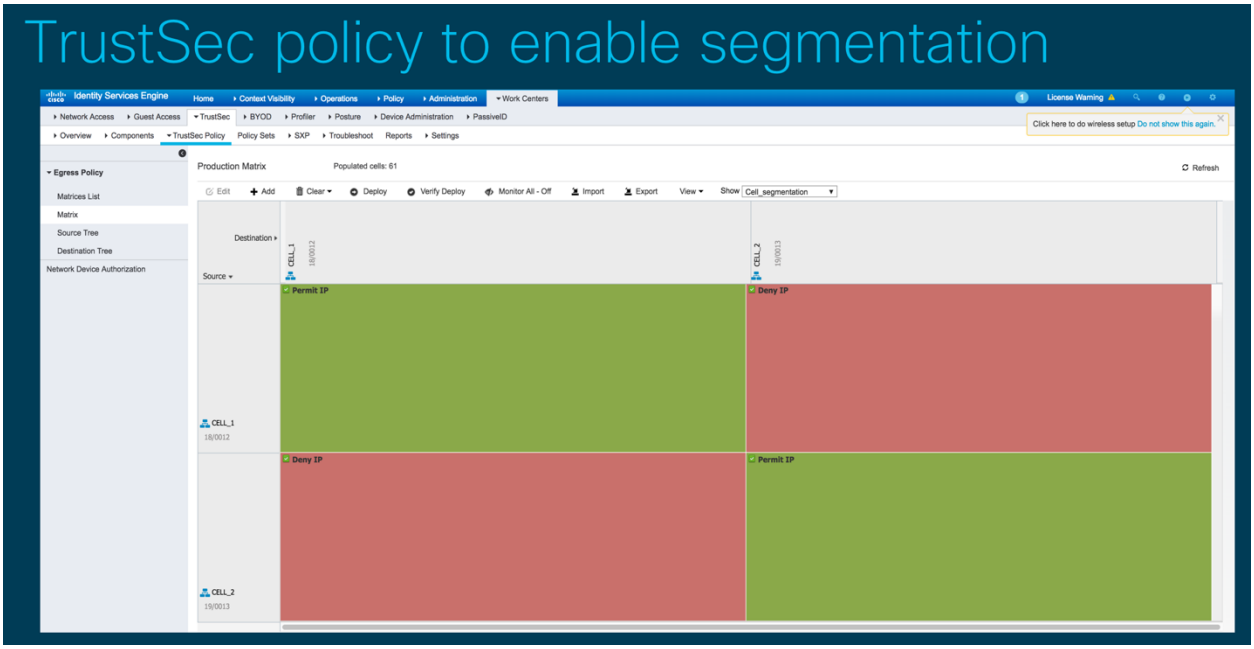
Figure 27 – Security Groups assigned



↩Return to Contents

Now Segmentation rules such as devices in Cell-1 segment cannot communicate with devices in Cell-2 segment can be created using SGT's on ISE as shown in Figure *28*. This way an OT operator does not need to write the segmentation policy but maintains full control over the devices in his network and can influence the segmentation policy by modifying the device groups on IND.

Figure 28 - ISE Segmentation Policy example

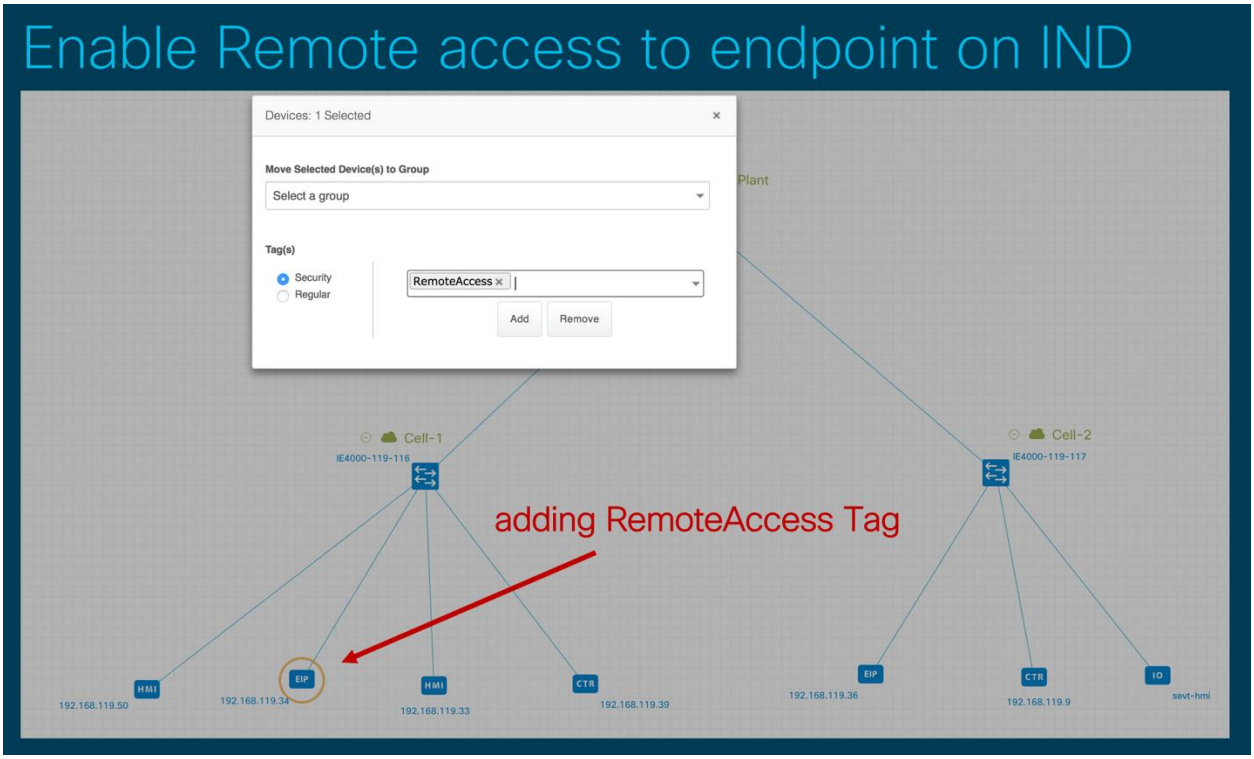


OT Intent based On-demand Remote access

In this use case we show case how remote access can be enabled by OT user when there is a need for maintenance by a vendor/machine builder from a remote location.

To enable remote access, we leverage the “assetTag” custom attribute on ISE to identify an asset which requires remote access and push the security policy across the switches and firewall to allow traffic from a remote user connected through a VPN.

Figure 29 - Adding the IND remote access tag

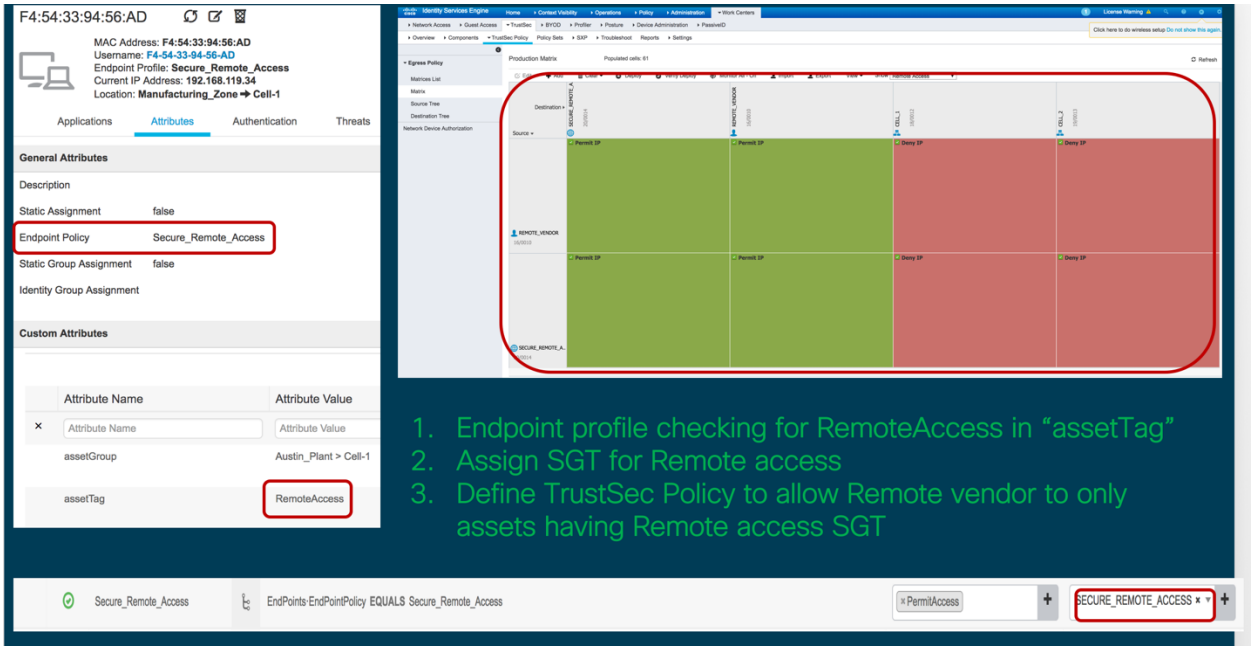


NOTE:

It is assumed that all the VPN Infrastructure is already in place and the VPN user is authenticated to ISE.

By default, all users do not have access to OT network even though they are authenticated. Whenever an OT asset requires maintenance, the plant operator changes the “assetTag” attribute as within IND to “RemoteAccess” that would allow access for a remote vendor..

Figure 30 – ISE & IND example remote access policy



↩Return to Contents

Firepower

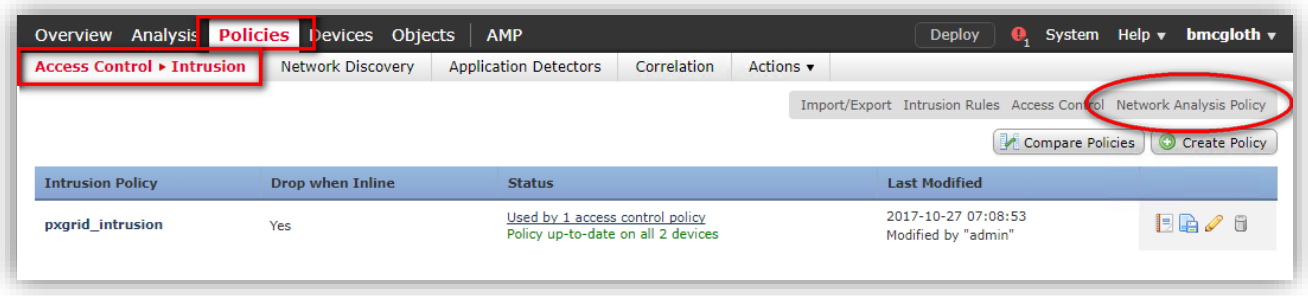
In addition to the segmentation capabilities of Firepower, deep packet inspection capabilities are also available. Firepower includes support for several Industrial protocols (DNP3, Modbus, IEC 60870, and CIP) providing protection for known vulnerabilities in addition to custom rules that can be created to test specific commands.

Deep Packet Visibility

Supervisory Control and Data Acquisition (SCADA) protocols monitor, control, and acquire data from industrial, infrastructure, and facility processes such as manufacturing, production, water treatment, electric power distribution, airport, and shipping systems, and so on. The Firepower System provides preprocessors for the Modbus and DNP3 SCADA protocols that you can configure as part of your network analysis policy.

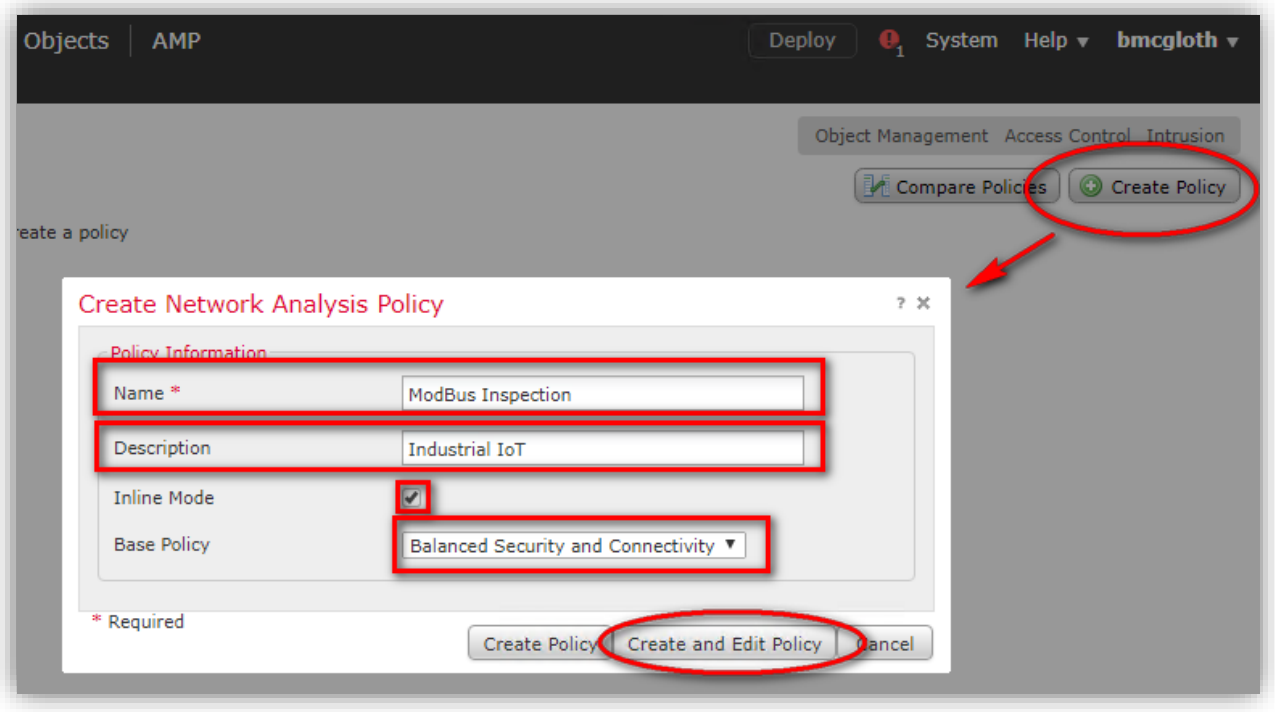
The Modbus protocol, which was first published in 1979 by Modicon, is a widely used SCADA protocol. The Modbus preprocessor detects anomalies in Modbus traffic and decodes the Modbus protocol for processing by the rules engine, which uses Modbus keywords to access certain protocol fields. For more details on Modbus and command protocols, please visit http://modbus.org. By default, Modbus inspection is disabled. You must create a Network Analysis Policy and apply it to the access control policy to enable Modbus inspection. The following steps create a policy and apply it.

Step 1: Choose **Policies > Access Control>Intrusion**, then click **Network Analysis Policy**.

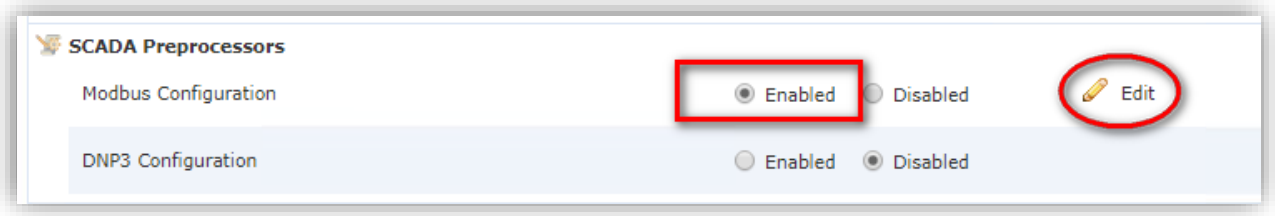


Return to Contents

Step 2: Click the **Create Policy** button in the upper right, name the policy, then click the **Create and Edit Policy** button.



Step 3: Click **Settings** in the navigation panel. If Modbus Configuration under SCADA Preprocessors is disabled, click **Enabled**. Click the edit icon next to Modbus Configuration.



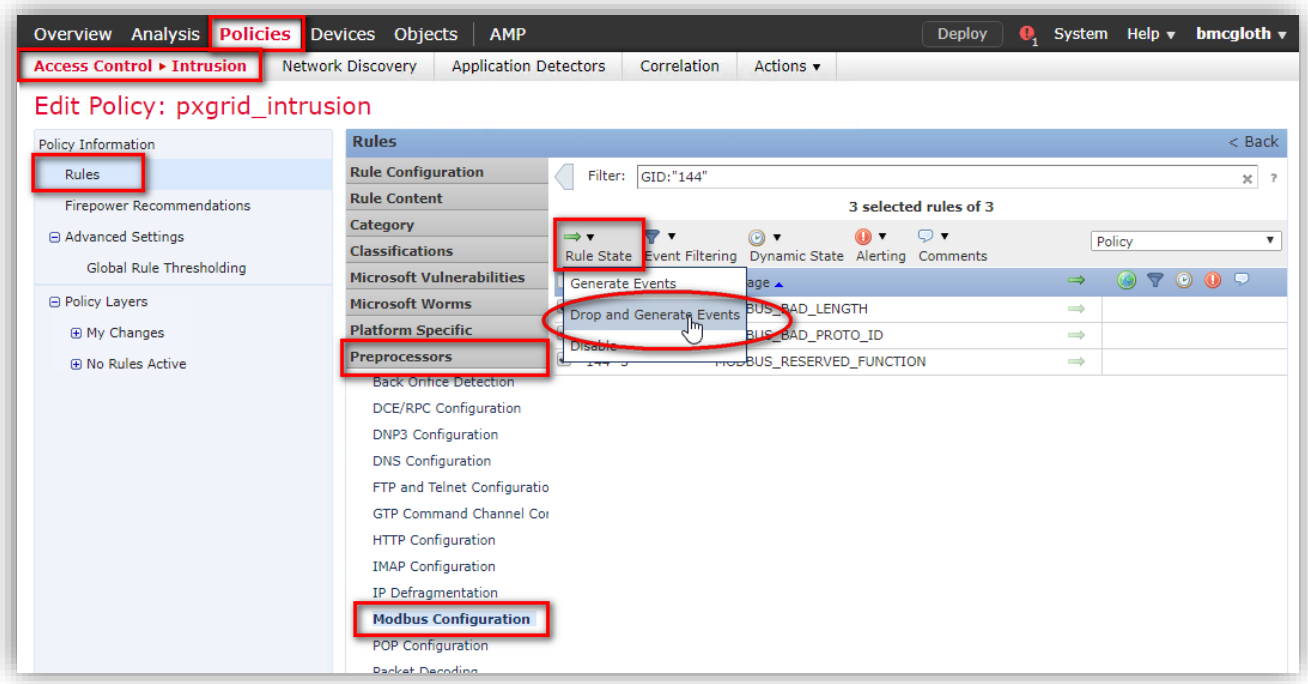
Step 4: Enter a value in the Ports field. Port 502 is the default. Separate multiple values with commas.

Step 5: To save changes you made in this policy since the last policy commit, click **Policy Information**, and then click **Commit Changes**.

If you leave the policy without committing changes, cached changes since the last commit are discarded if you edit a different policy.

Next, you must enable the Modbus preprocessor rules in the Intrusion Policy. Enable these rules to generate events and, in an inline deployment, drop offending packets.

Step 6: Choose **Policies > Access Control > Intrusion**, then click **Edit** next to the policy. Select **Rules > Preprocessors > Modbus Configuration**. Tick all three rules, then select **Drop and Generate Events** from the Rule State menu.



Step 7: To save changes you made in this policy since the last policy commit, click **Policy Information**, and then click **Commit Changes**.

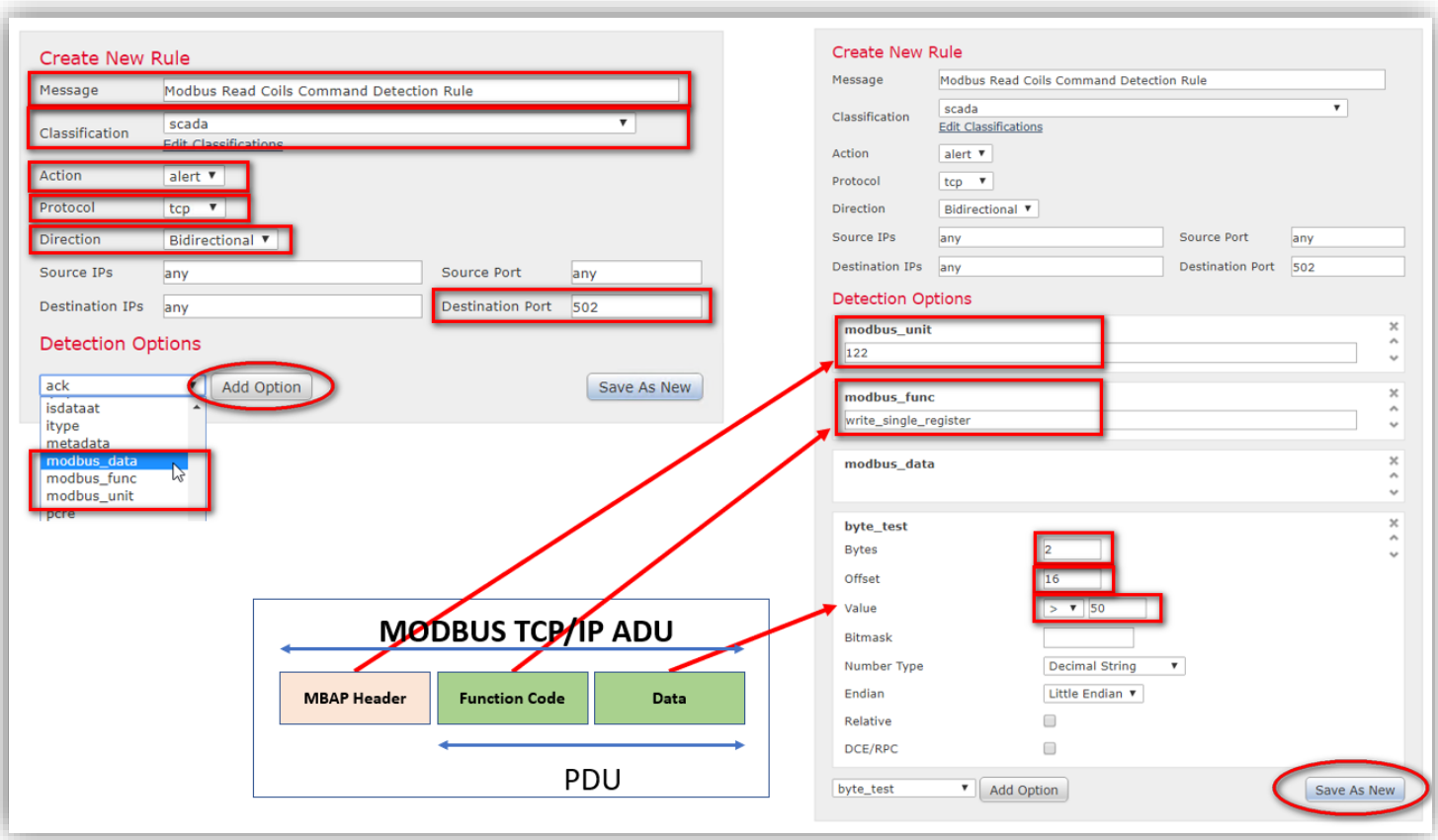
96

Modbus Command Inspection

Create custom inspection rules to test commands traversing the network and block unauthorized commands from reaching the Industrial IoT system.

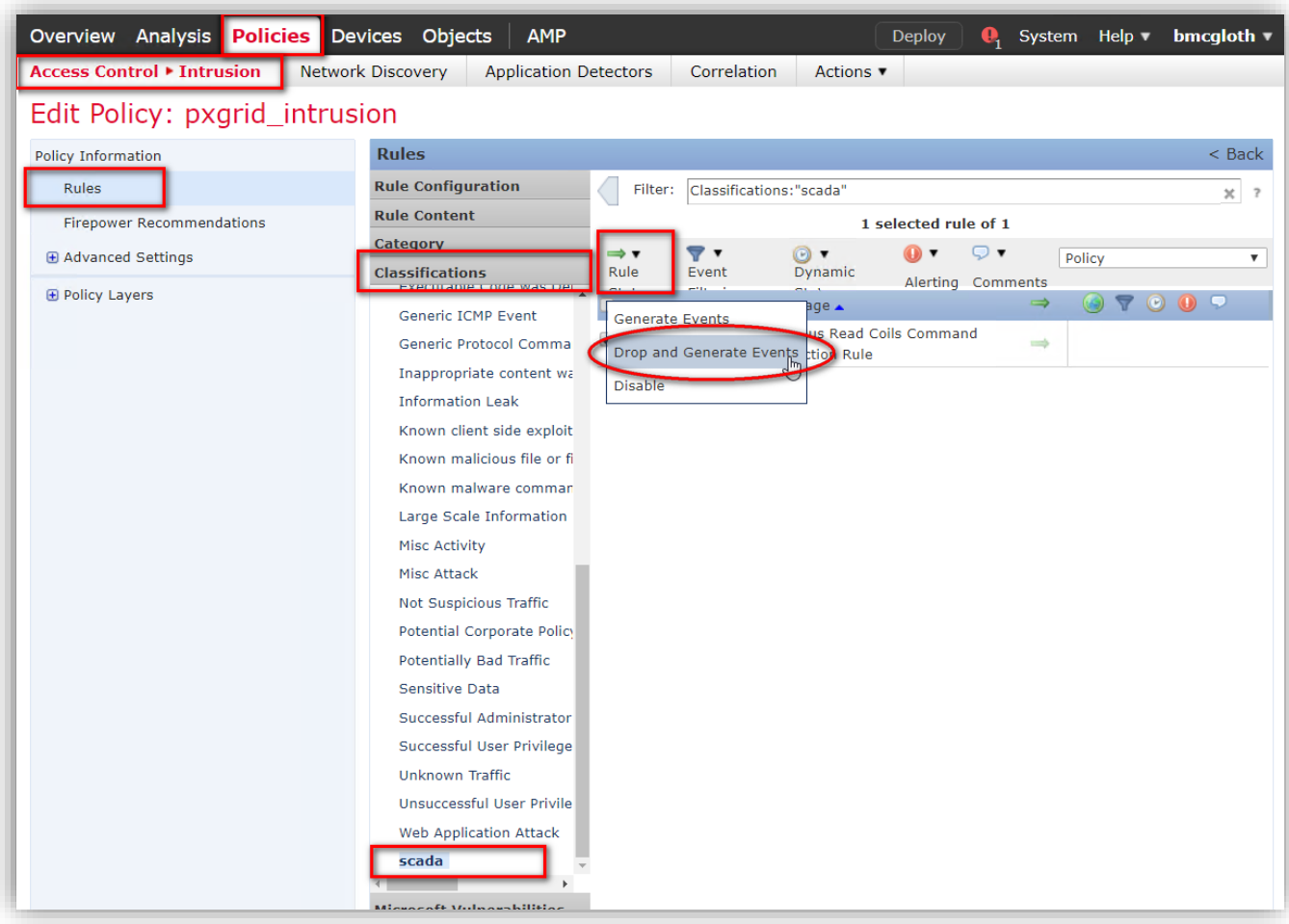
For example, create a rule to prevent a setpoint change greater than 50 for RTU-0122.

Step 1: Create a new rule to check Modbus commands. Choose **Objects > Intrusion Rules > Create New Rule**. Name the rule and specify the Modbus elements via the Detection Options. Click **Save as New**.



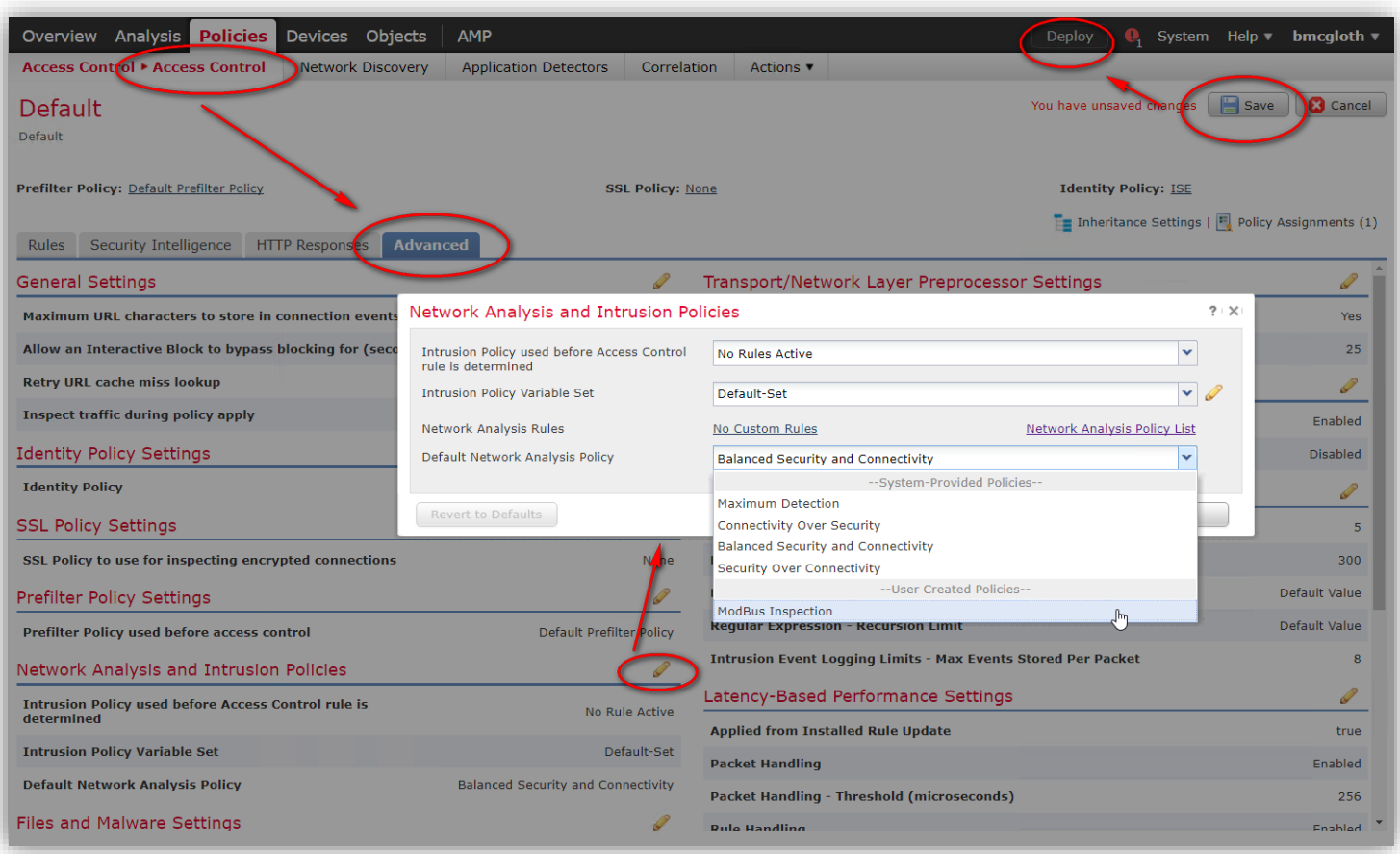
Return to Contents

Step 2: Choose **Policies > Access Control > Intrusion**, then click edit next to the policy. Select **Rules > Classifications > scada**. Tick the rule, then select **Drop and Generate Events** from the Rule State menu.



Step 3: To save changes you made in this policy since the last policy commit, click **Policy Information**, and then click **Commit Changes**.

Step 4: Add the network analysis Modbus Inspection policy to an access control policy with the updated Intrusion Prevention policy. Choose **Policies > Access Control > Access Control > Edit Default**, then click **Advanced** tab, and Edit the **Network Analysis**. Change Policy to **Modbus Policy**. Click **OK**, **Save,** and **Deploy**.



↩Return to Contents

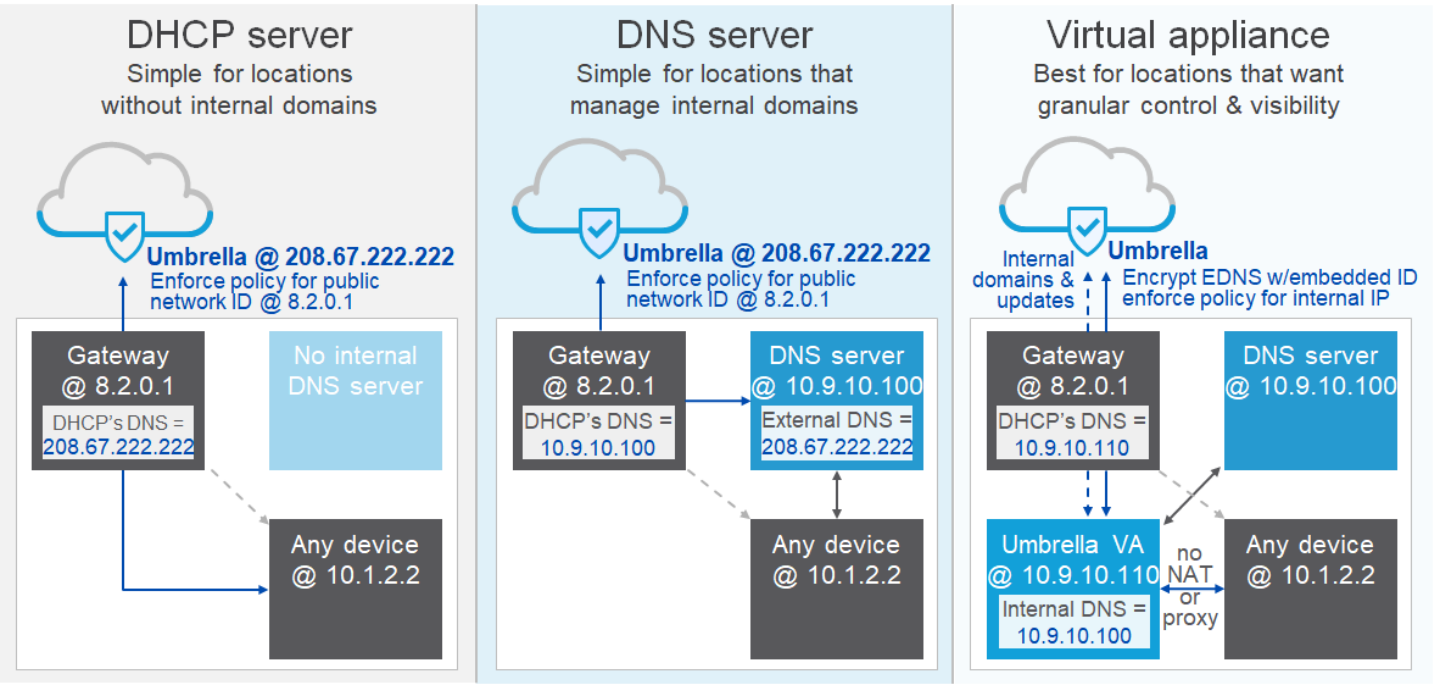
Umbrella

Cisco Umbrella provides one of the easiest methods to get basic visibility from the network through the use of DNS. Just about every device uses DNS to resolve domain names to system IP address for connectivity across every protocol. Cisco Umbrella can give you visibility with the simplest deployment options which are completely transparent to users and devices as shown in Figure 31.

The three most common deployment options are:

1. DHCP server—Best for remote IoT devices that communicate primarily to the Internet.
2. DNS server—Best for internal IoT devices that communicate primarily to the Internet with some internal communication; no endpoint visibility but IoT devices are protected from bad domains.
3. Virtual appliance—Best for internal IoT devices that communicate to both internal and Internet systems; provides visibility, protections, and policy options based on their internal identities.

Figure 31 - Umbrella Deployment options



For our Industrial IoT environment, almost all communication from the plant stays within the Industrial zone, but vendors are requesting customers enable telemetry reporting to cloud services. Many customers do not know whether their IoT devices are communicating with Internet services at all. For this level of granular visibility, a local presence in the network is needed.

This solution implements lightweight DNS forwarders deployed as virtual appliances in VMware or Hyper-V. Using DHCP or statically assigned DNS servers, we point all requests for internal and external domains first to the virtual appliances. The virtual appliance forwards requests for internal domains to the existing local DNS servers. Before it forwards requests for Internet domains to Umbrella, it embeds the local IPs into RFC-compliant extension mechanisms for DNS, so that we know which internal network device is making the request. Reporting for these internet destination queries is available in the Cisco Umbrella reporting console.

Return to Contents

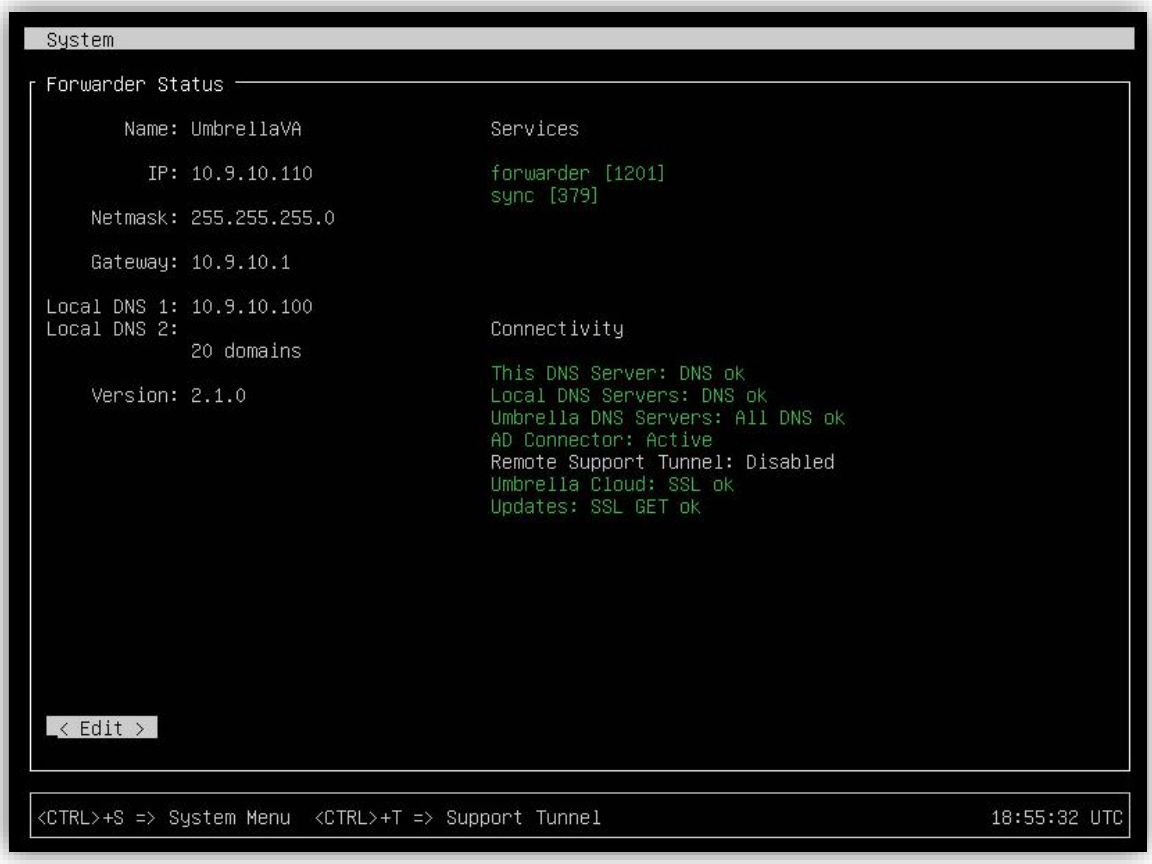
100

Umbrella Virtual Appliances

The Cisco Umbrella VAs were installed on VMware systems within the laboratory following the installation guide that can be found here: https://docs.umbrella.com/product/umbrella/1-introduction/

Upon completion of the installation steps, your Umbrella virtual appliance status console should look similar to Figure 32.

Figure 32 – Umbrella VA Status

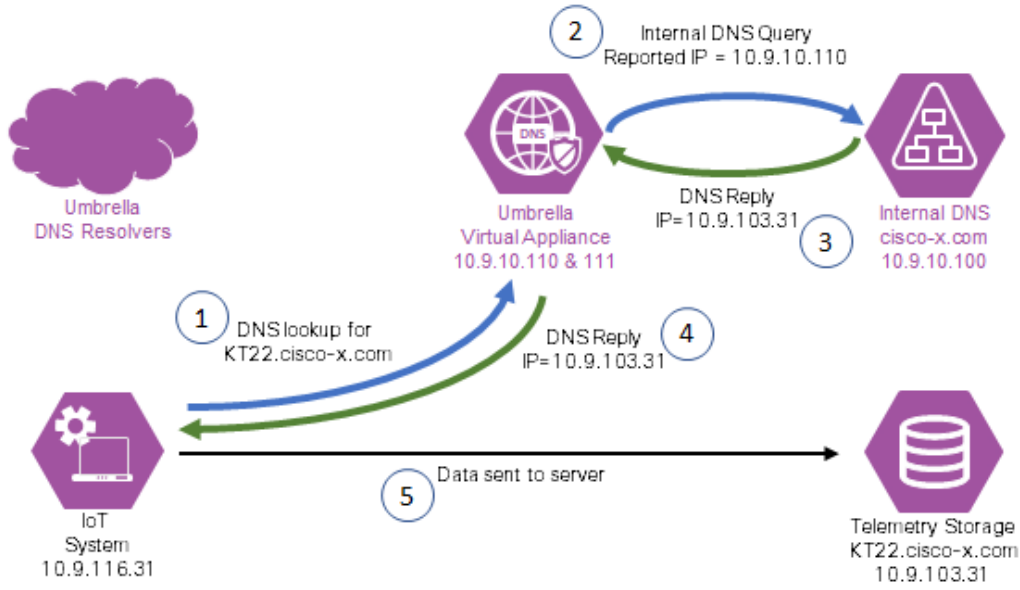


The IoT systems were configured to use the Umbrella virtual appliances (two deployed for high availability) as their DNS servers. The virtual appliances used the Microsoft Active Directory DNS server for internal resolutions.

↩Return to Contents

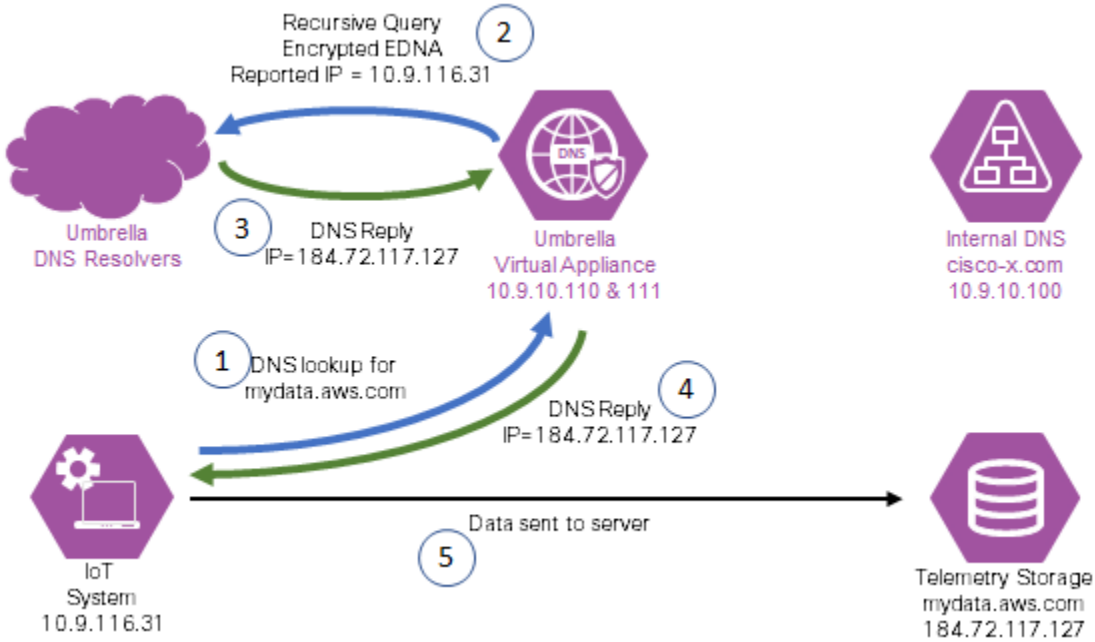
For an internal domain lookup as shown in Figure 33, the Umbrella virtual appliance sends the request to the internal DNS server, then forwards the reply back to the IoT system. These requests are not logged in the virtual appliance, and the logs in the internal DNS server show the virtual appliance as the source of the request.

Figure 33 – Internal Domain Lookup



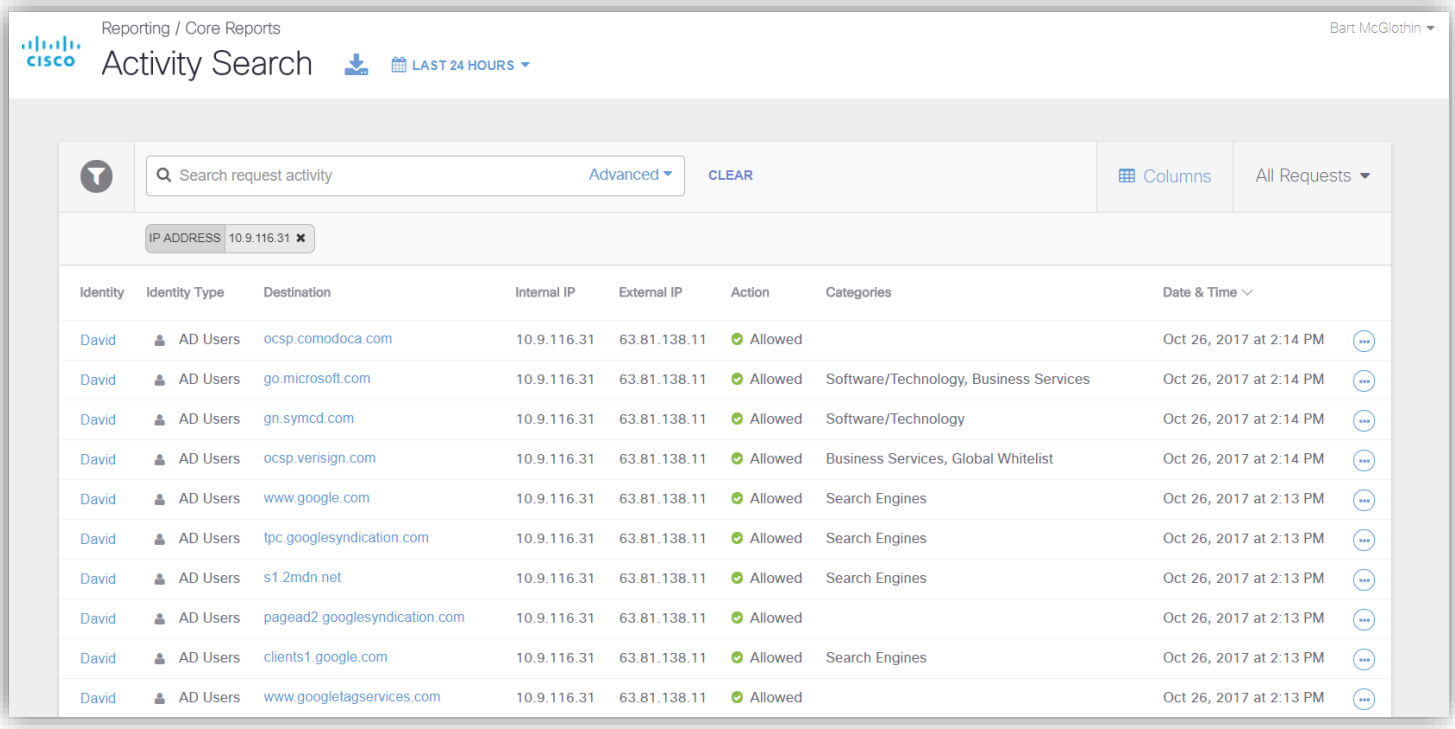
For an external Internet domain lookup as shown in Figure 34, the Umbrella virtual appliance sends the request to the Umbrella resolvers in the cloud with the additional information of the requester's IP address. Policies using this enhanced information can be customized based on the requesting devices. Once all of the policies have been applied to the request, the reply gets forwarded back to the IoT system and it is then able to establish communication.

Figure 34 – External Internet Domain Lookup

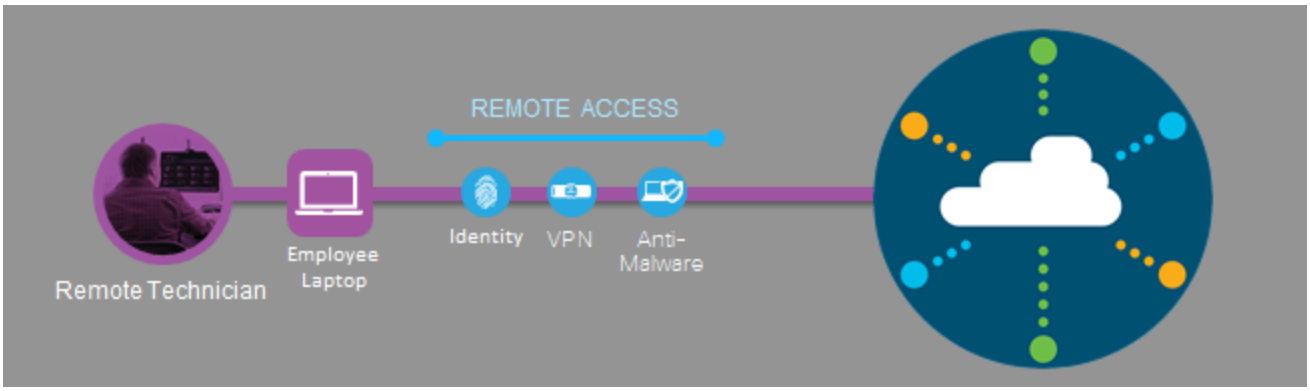


Return to Contents

These requests are logged and available to be reviewed via the Umbrella Reporting console.



Return to Contents



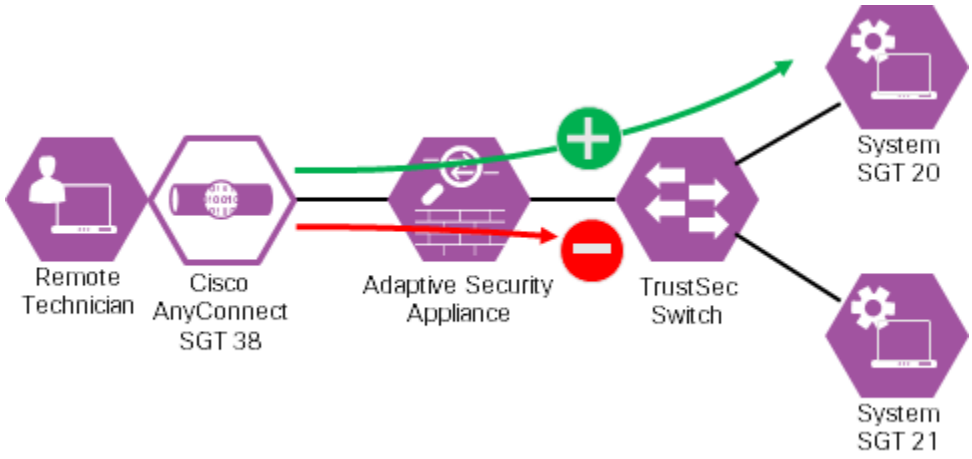
AnyConnect

To maintain your expensive and sophisticated modernization investments, you are likely to rely on your vendors for debugging and maintenance. For that to happen, there are multiple scenarios by which you either allow them remote access into your plant network, or you allow their people access to your plant floor directly. In either case, that access needs to cross multiple networks under different administrators. Doing so securely and on an as-needed basis is not easy. For Cisco, it becomes easier with our unique and strong place within the network and security plane.

1. First external technicians must cross the internet into your enterprise, traverse the industrial DMZ to a jump box and from there make their way across the plant network to exactly the one device you have asked them to address. That is complicated.
2. Second, let's assume they are on-site and need access to resources back at their headquarters. Reverse that process.

ASA supports security group tagging of VPN sessions. Security group tags simplify the use of group policies on the ASA. Cisco AnyConnect VPN is implemented with an ASA firewall. Remote vendors and partners are authenticated using ISE against Active Directory user/group accounts. ISE assigns the appropriate SGT based on an authorization policy. The ASA access policy permits the partner to access only the systems allowed based on the IP-SGT mapping of devices to security groups as shown in Figure 35.

Figure 35 - Cisco AnyConnect with SGT



Return to Contents

If there is no SGT in the attributes from the AAA server to assign to a VPN user, the ASA uses the SGT in the group policy. If there is no SGT in the group policy, then tag 0x0 is assigned.

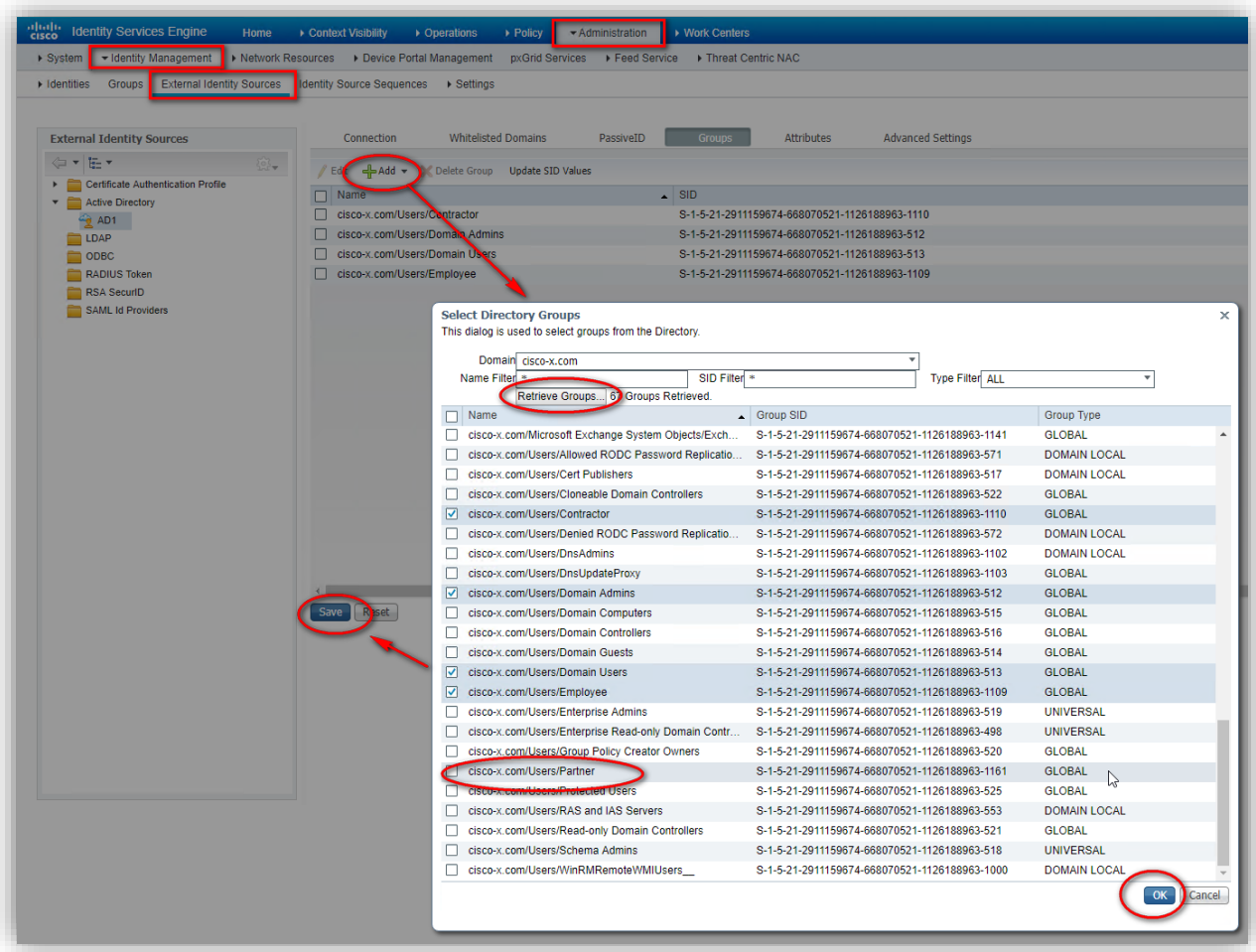
More detailed information regarding client VPNs and TrustSec can be found at the following URLs:

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/firewall/asa-98-firewall-config/access-trustsec.html#ID-2135-000006a9
- https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/117694-config-asa-00.html#anc6

ISE Configuration

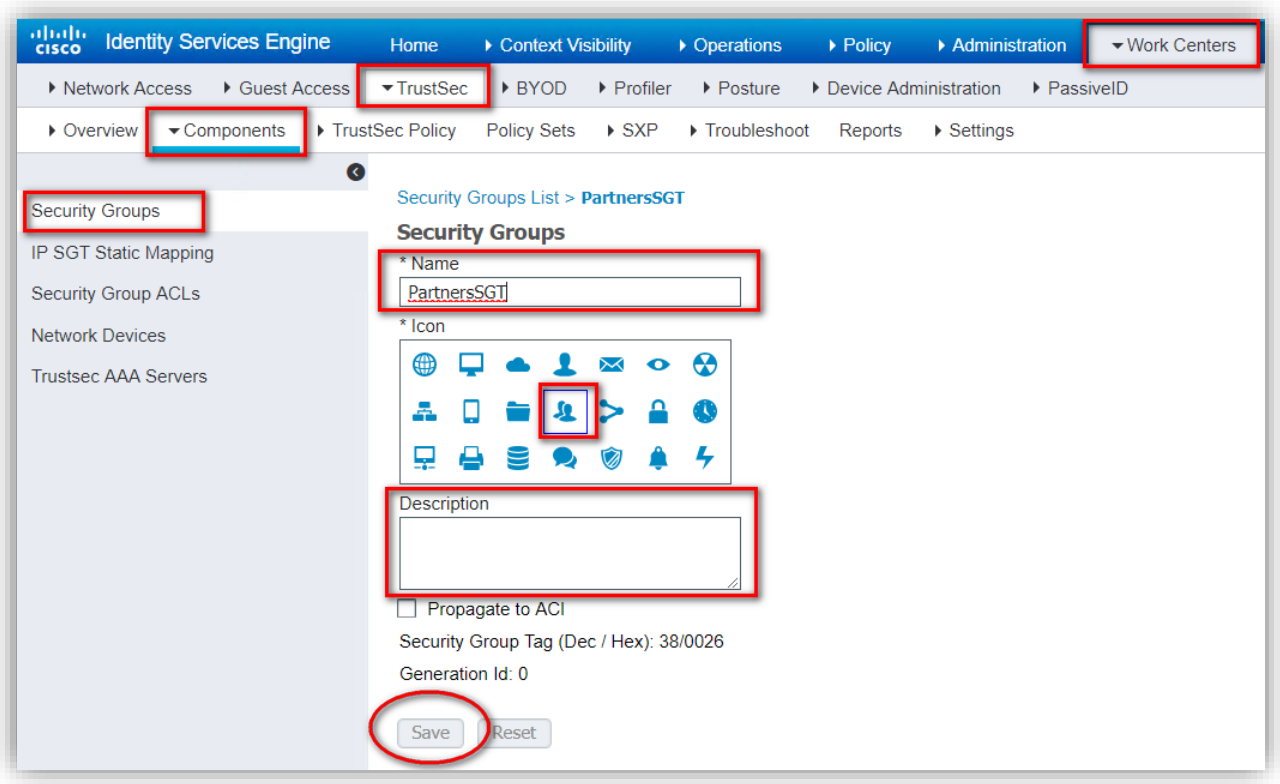
The follow steps outline adding the Partner group from Active Directory to the ISE Identity source, creating an associated Partner security group tag, adding an authorization policy for Partners, and adding the Remote Access ASA to ISE for Authentication.

Step 1: Choose **Administration > Identity Management > External Identity Sources** to add and configure the Partners group from Active Directory Users.

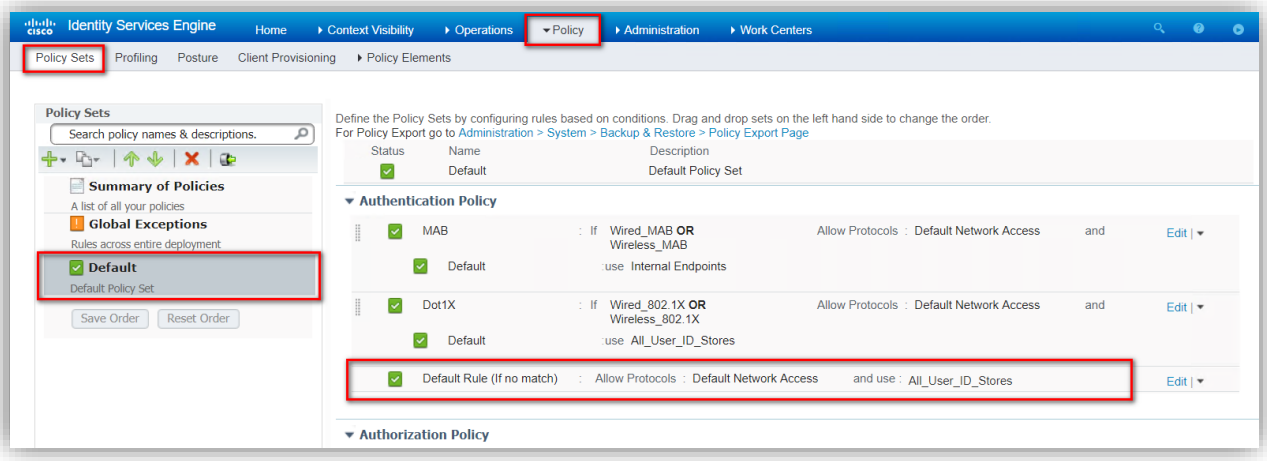


Return to Contents

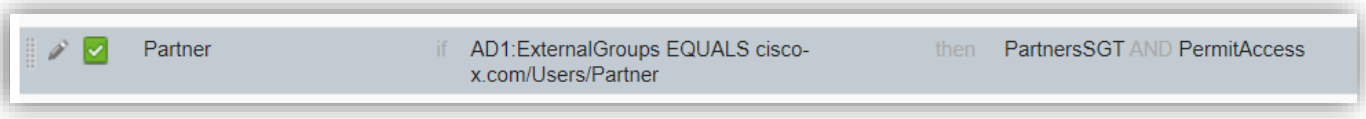
Step 2: Choose **Work Centers > TrustSec > Components > Security Groups > Add** to add and configure the Partner SGT group. Enter the Name, select the Icon, enter a description, and click **Save**.



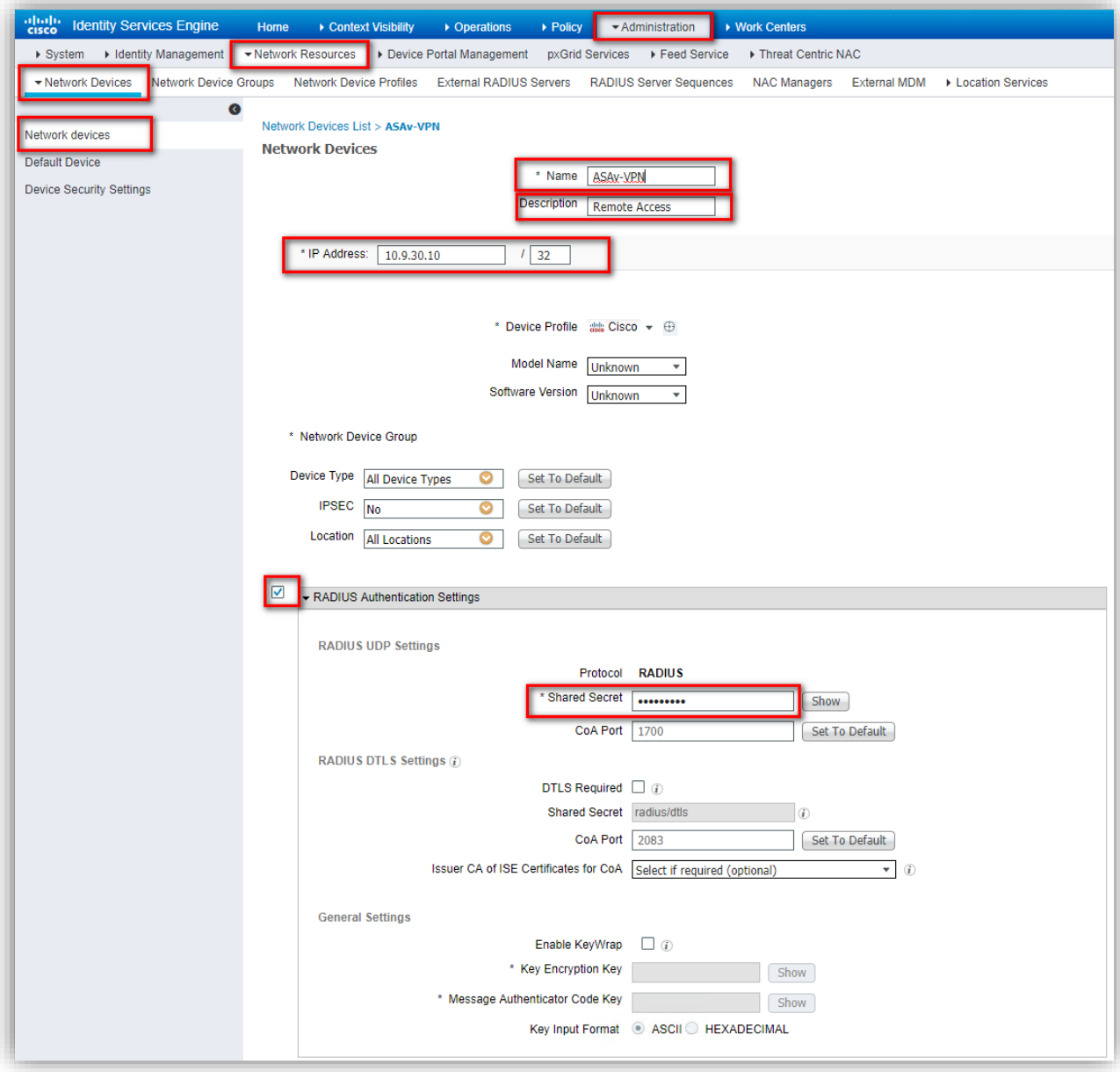
Step 3: Verify that your Authentication policy includes your partner identity store. Navigate to **Policy > Policy Sets > Default**.



Step 4: Choose **Policy > Policy Sets > Default > Authorization Policy** to add and configure the Partner authorization profile. Specify the Active Directory Identity Group, then assign the permissions of PermitAccess and the SGT group PartnersSGT.



Step 5: Choose **Administration > Network Resources > Network Devices** to add and configure the ASA as a network device. Click **Save**.



Return to Contents

ASA VPN Config

The following steps outline configuring the ASA for remote access VPN using the AnyConnect Client, authentication the remote users with ISE, assigning SGTs, and implementing a security policy based on these SGTs.

Step 1: Complete the basic VPN configuration using the CLI.

Define an IP pool for VPN users

```
ip local pool VPN_POOL 10.9.31.10-10.9.31.99 mask 255.255.255.128
```

Configure the VPN profile and policy.

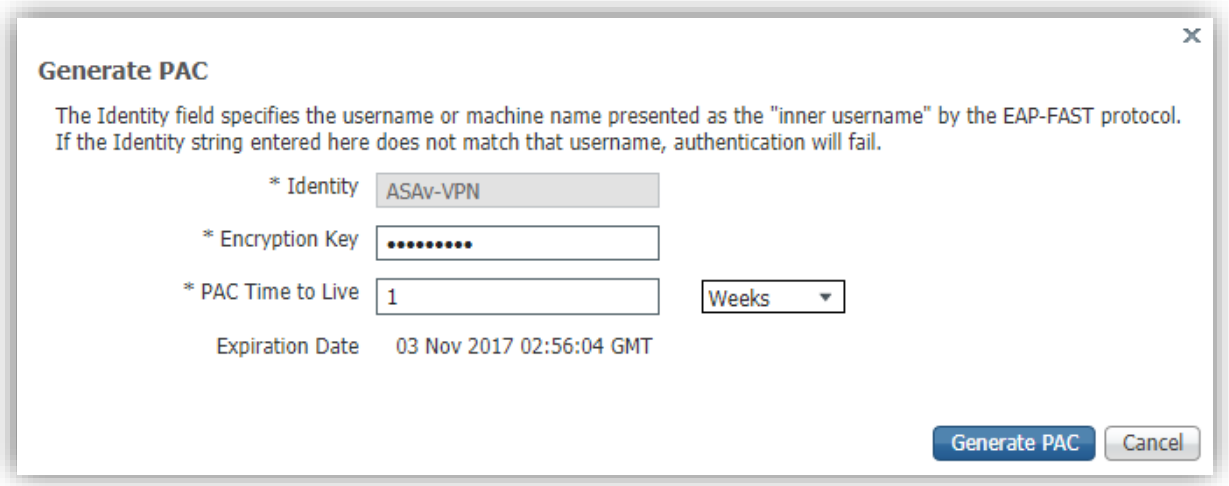
```
webvpn  enable outside
 anyconnect image disk0:/anyconnect-win-4.5.00058-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.5.00058-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy GroupPolicy_SSL_VPN internal
group-policy GroupPolicy_SSL_VPN attributes
 dns-server value 10.9.10.110 10.9.10.111
 vpn-tunnel-protocol ssl-client
 default-domain value cisco-x.com
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
!
tunnel-group SSL_VPN type remote-access
tunnel-group SSL_VPN general-attributes
 address-pool VPN_POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GroupPolicy_SSL_VPN
tunnel-group SSL_VPN webvpn-attributes
 group-alias SSL_VPN enable

Add the Remote Access VPN Pool to the enterprise routing updates.

prefix-list VPN_PREFIX seq 1 permit 10.9.31.0/25
route-map VPN_RM_POOL permit 1
 match ip address prefix-list VPN_PREFIX
!
router eigrp 101
 redistribute static route-map VPN_RM_POOL
```

Step 2: Complete the ASA AAA and TrustSec configuration.

```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.9.10.51
 key Cisco1234
 radius-common-pw Cisco1234
!
cts server-group ISE
cts sxp enable
cts sxp default password Cisco1234
cts sxp default source-ip 10.9.30.10
cts sxp connection peer 10.9.10.51 password default mode peer speaker
```

To join the TrustSec cloud, the ASA needs to authenticate with a Protected Access Credential (PAC). The ASA does not support automatic PAC provisioning, so the file needs to be manually generated on ISE and imported to the ASA.

Step 3: Choose Administration > Network Resources > Network Devices > ASAv-VPN > Advanced TrustSec Settings to generate a PAC on the ISE server. Choose Out of Band (OOB) PAC provisioning to generate the file.



Step 4: Import the PAC to the ASA.

The generated file could be put on an HTTP/FTP server. The ASA uses that to import the file.

```
ASA-VPN# cts import-pac ftp://10.9.10.19/ASAv-VPN.pac password Cisco1234 !PAC
Imported Successfully

ASA-VPN# show cts pac

PAC-Info:
Valid until: Jan 04 2018 19:48:53
AID:         f27245406549e7f85ace32f2bceb8a5e
I-ID:        ASAv-VPN
```

```
A-ID-Info:   Identity Services Engine
PAC-type:    Cisco TrustSec
PAC-Opaque:
000200b000030001000400010f27245406549e7f85ace32f2bceb8a5e0006009400030100da505
e29bedc2771e9b15748dd79aeb70000001359ee79c500093a80ade9899465c87f6a366a8bab90
56215c153c9b86e96e33e90ca49298fe0b144cd2a08748b9dd942150f51f40002a06f34a9ab59
17d8a2152164c1e6307ded78db2b79a8ee8a1e0a5b415e9f0661b97d9c2c9e8c3cb90d849d1c3
c5b4aabddb0f69ef913e3c26f7571c525e46ec7c9de4a4b1a
```

When you have the correct PAC, the ASA automatically performs an environment refresh. This downloads information from the ISE about current SGT groups.

```
ASA-VPN# show cts environment-data sg-table

Security Group Table:
Valid until: 19:50:32 PDT Oct 27 2017
Showing 40 of 40 entries
SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
ContractorsSGT                        5     unicast
EmployeesSGT                          4     unicast
IoT_DeviceSGT                        20     unicast
IoT_Manufacturing_Contorl_Sys        25     unicast
IoT_Manufacturing_Monitor_Sys        26     unicast
Network_Services                      3     unicast
OTHER_UNTAGGED                       37     unicast
PartnersSGT                          38     unicast
Quarantined_SystemsSGT              255     unicast
TrustSec_DevicesSGT                   2     unicast
Unknown                               0     unicast
```

Step 5: Tag packets inline and trust tagged packets.

```
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt
```

Remote Access access-list filters for group policies do not support security-group attributes. So interface-based access permissions must be configured for the VPN user policies to take advantage of TrustSec SGTs.

Step 6: Disable the default feature of VPNs to bypass interface access lists for inbound VPN sessions.

```
no sysopt connection permit-vpn
```

Step 7: Configure the ACL on the outside interface that allows for traffic from *PartnersSGT* to *IoT_DeviceSGT* using the Security Group name instead of the tag. Additionally, add access to the Remote Desktop Access server in the IDMZ.

```
object network RemoteAccessServer
 host 10.9.103.31
!
access-list outside_access_in extended permit ip security-group name
PartnersSGT any security-group name IoT_DeviceSGT any
!
access-list outside_access_in extended permit ip security-group name
PartnersSGT any object RemoteAccessServer
!
access-group outside_access_in in interface outside
```

Now the ASA will classify VPN users and perform enforcement based on SGTs.

Monitoring Cisco TrustSec

See the following commands for monitoring Cisco TrustSec:

- show running-config cts
- show running-config [all] cts role-based [sgt-map]—This command shows the user-defined IP-SGT binding table entries.
- show cts sxp connections—This command shows the SXP connections on the ASA for a particular user context when multiple context mode is used.
- show conn security-group—Shows data for all SXP connections.
- show cts environment-data—Shows the Cisco TrustSec environment information contained in the security group table on the ASA.
- show cts sgt-map—Shows the IP address-security group table manager entries in the control path.
- show asp table cts sgt-map—This command shows the IP address-security group table mapping entries from the IP address-security group table mapping database maintained in the datapath.
- show cts pac—Shows information about the PAC file imported into the ASA from the ISE and includes a warning message when the PAC file has expired or is within 30 days of expiration.

Validation Testing

Starting with Cisco's Converged Plantwide Ethernet (CPwE) Design, we added Stealthwatch for pervasive visibility capturing network flows and analyzing them. We implemented pxGrid communications between the Cisco Identity Services Engine, Firepower Management Center and Stealthwatch to enable the capabilities described in the Network as an Enforcer (NaaE) and Rapid Threat Containment design guides for the CPwE design.

We enabled profile-based segmentation for IoT devices using MAB, TrustSec using SGTs, and vendor-specific profiling. We enhanced secure remote access to the CPwE by adding TrustSec SGTs and policies to the industrial DMZ.

Solution validation testing was accomplished by creating a representative enterprise network of Windows servers, Client workstations, and various IoT systems and devices. IoT devices were based on both hardware Programmable Logic Controllers (PLC), PIC, building systems, and virtualized OS's such as Arduino. A majority of the communication flow and policy enforcement testing was from PCs where communications could be controlled more easily for testing purposes (for example, ping, trace, web calls, file transfers, authentication, and MAB).

Technologies

- Segmentation: ISE + TrustSec, Firepower,
- Visibility: ISE, Stealthwatch, Firepower, Umbrella
- Secure Remote Access: AnyConnect VPN,

Task list / Validations:

- Authenticate devices to network using 802.1x, MAB, profiles with SNMP, assign SGTs
- Collect, monitor, and analyze communication flows on Stealthwatch from all devices
- Configure Stealthwatch policies, if systems change communication - Alert (PLC-PLC change map)
- Segment the network via Industrial switches using TrustSec SGTs and SGACLs
- Trigger manual quarantine using of systems from the Stealthwatch console
- Trigger an automatic quarantine of a remote user system using Firepower Management Center with pxGrid integration to ISE, to remove a malware infected system from the network
- Visibility to what IoT devices are communicating on the Internet using Umbrella enterprise

All of these tasks were completed successfully using the implementation configurations provided in this guide.

Best Practices for Integration of IoT devices

The following best practices complement this solution:

1. Identify all services to which the IoT devices need access (create policies for communications).
2. Segment systems of IoT devices from each other, and test this segmentation regularly.
3. Authenticate access to the network wherever possible (devices, remote, enterprise) for everything.
4. Monitor IoT network communications and document normal flows, review and update as needed.
5. Identify who owns and manages/monitors the IoT devices themselves, so that any identified anomalies can be quickly escalated and acted upon.

⮌Return to Contents

112

Summary

IoT systems security is a challenge that continues to grow as more than 30 billion devices will come online over the next few years. If attacks are successful, they create a significantly negative business impact on an organization.

This solution accomplishes the goal of keeping your organization up and running through improved segmentation between users' devices and IoT systems, improved visibility of what is on the network and with who it is communicating, and replacing insecure modems and remote support systems with secure VPN-based remote access. This ensures that there is only a small chance of losing control of your critical systems.

To minimize security risks during IoT digitization and deployment, first gauge your company's readiness, and build a strong security foundation for IoT and the digital business transformation by integrating security and IoT efforts together.

Start with a security network penetration assessment followed by an automation and control systems risk assessment. With these risks and vulnerabilities identified, create an incident response plan and impact assessment aligning to the business as it functions today. Finally, create a roadmap to implement improved segmentation, visibility with analysis, and secure remote access to digitize your IoT and employee environments. Use the best practices described in this guide to improve the incident response plan and reduce the business impact of a successful attack.

⮌Return to Contents

References

Cisco SAFE Simplifies Security:
www.cisco.com/go/safe

Network as a Sensor:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-sensor.html
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf

Cisco Identity Services Engine with TrustSec (Network as an Enforcer):
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-enforcer.html

Cisco Rapid Threat Containment Solution:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

Cisco Stealthwatch:
http://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
http://www.network-node.com/blog/2016/5/31/stealthwatch-smc-client-part-1

Cisco Umbrella Security:
https://umbrella.cisco.com/products/features
DNS Best Practices:
https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html
Setting up DNS Forwarding for Windows Server 2012 and 2012 R2:
https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2

Cisco Advanced Malware Protection for Endpoints:
http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
Cisco Advanced Malware Protection:
http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Cisco Talos - Comprehensive Threat Intelligence:
http://www.cisco.com/c/en/us/products/security/talos.html
Cisco ThreatGrid:
http://www.cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html

Troubleshoot ISE and FirePOWER Integration for Identity Services
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html

Cisco TrustSec Switch Configuration Guide
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco Firepower Management Center:
http://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html

Cisco Industrial Network Director:
https://www.cisco.com/c/en/us/products/cloud-systems-management/industrial-network-director/index.html

↩Return to Contents

114

Appendix

Lab Diagrams

Figure 36 - Cisco IoT Threat Defense Lab–San Jose

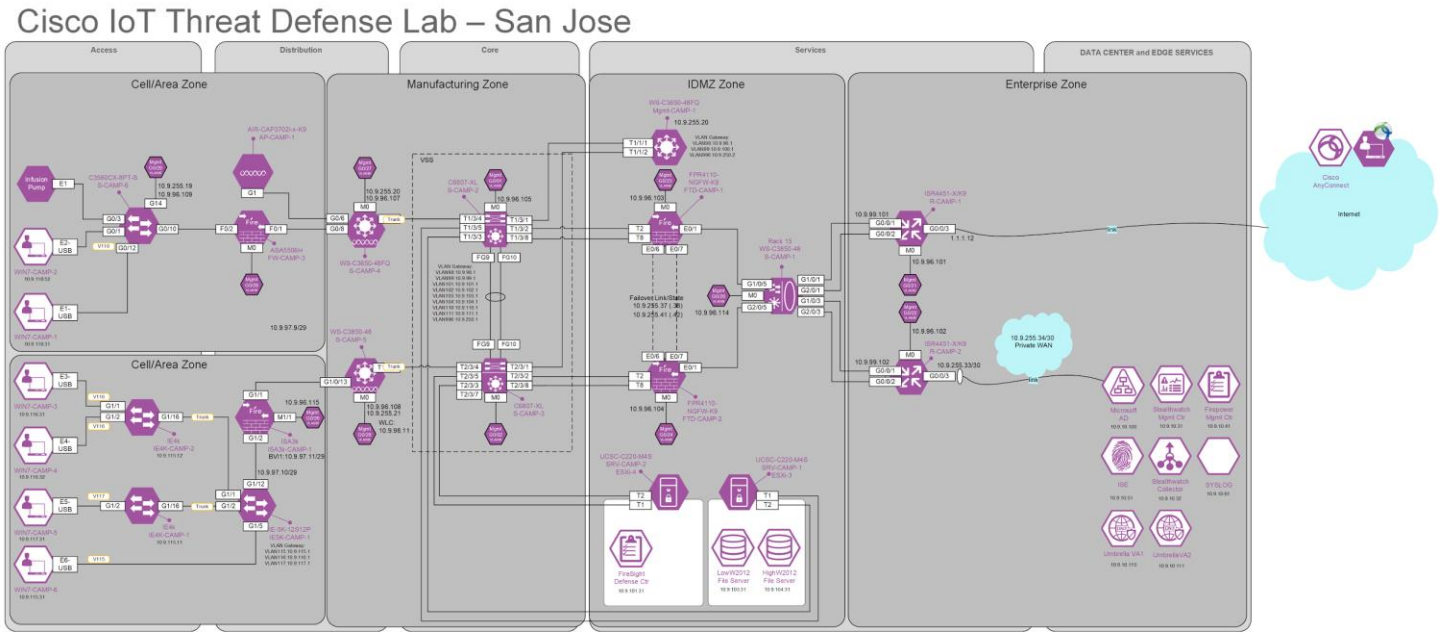
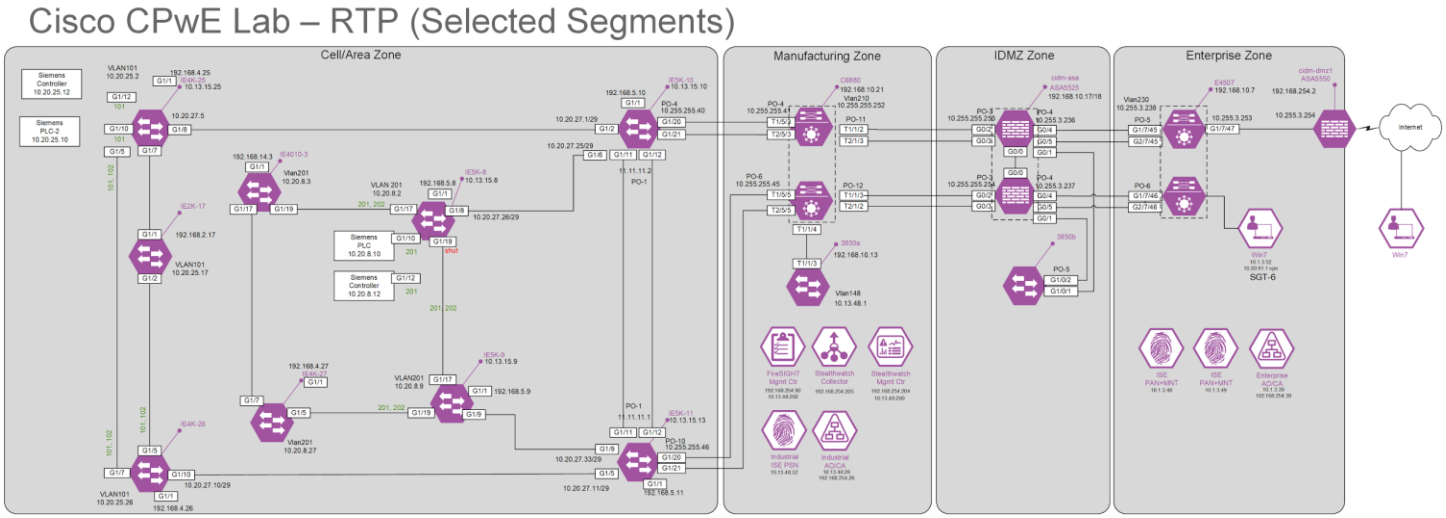


Figure 37 - Cisco CPwE Lab–RTP (Selected Segments)



Return to Contents

115

Solution Products

The following products were implemented for the validation testing of the IoT Threat Defense Solution.

Table 1 - Solution products validated

Product	Description	Platform	Version
Identity Service Engine	Authenticate and profile devices connecting to network	Virtual or Appliance	2.4.0.357
Industrial Network Director	Provides full visibility and control of the Industrial Ethernet infrastructure	Software	1.4.0-216
Firepower Management Center	Manage Firepower Threat Defense systems	Virtual or Appliance	6.2.0
FireSight Defense Center	Manage ISA3k Firewalls, non-FTD	Virtual	5.4.1.9
Stealthwatch	Collect and analyze NetFlow	Virtual or Appliance	6.9.0
Cognitive Threat Analytics	Analysis of flows from SW	Cloud	n/a
Umbrella	DNS based Secure Internet Gateway for security for on-network IoT	Cloud	2.1.0
AnyConnect	Secure Mobility Client	Windows	4.5.00058
Firepower Threat Defense	Security platforms running Firepower Threat Defense software image	Virtual and 2100, 4100, 9300	6.2.0
ASA	Firewall	ISA3000, ASA5500-X	9.7(1)4
ASA-ASDM	Local FW Mgmt	ISA3000, ASA5500-X	7.7(1)
NGIPS on ASA	Protection and Control	ISA3000, ASA5500-X	5.4.1.8+
Industrial Ethernet Switches	Ruggedized switches with IPSERVICES enabled	IE4K, IE5K, 3560CX	15.2(6)E1
Cisco Catalyst Switches	Core	6807-XL	15.4(1)SY
	Access / Distribution	3650, 3850	16.3.3

↩Return to Contents

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Return to Contents