Grid Security 3.1 Implementation Guide

October 2020

Contents

Grid Security 3.1 Implementation Guide

Introduction

Smart Grid is an electricity delivery system that is integrated with communications and information technology to enhance grid operations, improve customer service, lower costs, and enable new environmental benefits. This document describes the overall use of the network to monitor and manage the electrical system from power generation, through transmission and distribution, to end users in smart buildings, smart homes, and other sites connected to the utilities network. As the OT world collides with the traditional IT world, security is becoming increasingly important for utilities customers. Today's news includes many stories about hackers and terrorists that seek to gain access to critical networks in order to steal money, information, or even to disrupt service.

This solution seeks to address many of these concerns by providing a holistic approach to restricting access, protecting data, logging events and changes, and monitoring activity in the substation. The Substation Security solution addresses the NERC-CIPv5 CIP requirements. While only applicable in North America, much of the world is looking to NERC-CIP as the standard to secure their utility and other industrial operations.

The substation network must be protected from unauthorized access and cyberattacks. The substation network security services must guarantee the integrity of telemetry data and control commands to ensure confidentiality, integrity and availability of the electronic information communication system. These security services must be deployed at each networking protocol layer whenever it is applicable.

For more details please refer to Grid Security Design Guide that can be found at the following URL:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/DG/DA-GS-DG.html

Navigator

This document includes the following:

Access Control page 32	Explains the implementation details to perform access control and authorization.
Grid Visibility page 35	Explains the implementation details for enabling passive monitoring to enable the visibility for assets and application flows.
Threat Detection page 87	Explains the steps to implement threat detection to monitor and create alarms for any traffic outside of normal operations.

This Cisco Grid Security Implementation Guide provides a comprehensive explanation of the network and application level security implementation for protecting the smart grid systems. Utilities are interested in gaining visibility of SCADA Operational Technology and Engineering traffic flows occurring within and across substations. This guide addresses how to use Smart Grid systems to get this visibility. This guide also captures implementation details of mandatory compliance requirements of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). The solution architecture, possible deployment models, and recommended guidelines for deployment are discussed.

Audience

The audience of this guide comprises system architects, network/compute/ systems engineers, field consultants, Cisco customer experience specialists, and customers. Readers may be familiar with networking protocols, security concepts of firewall, encryption, deep packet inspection, public key infrastructure and Cisco substation automation solution architecture.

Document Objective and Scope

This guide helps provide details of the Grid Security Solution implementation that is an addition to Cisco Substation Automation 2.3.2 CVD Architecture and Cisco Distribution Automation – Secondary Substation Architectures here:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.pdf

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG.html

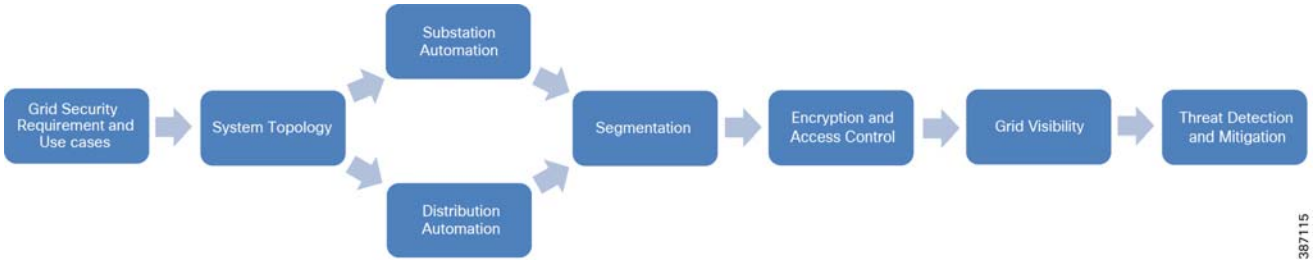
The scope addressed in this document is Cisco Information and Communication Technology (ICT) solution architecture and implementation for modern transmission substations and secondary substations, including the Cisco solution for process and station buses in substation LAN environment per IEC 61850 protocol standard. It describes how the fault-tolerant multi service network design is implemented, and how network segmentation is implemented across various substation application flows.

The methods by which utility actors like Human Machine Interface systems (HMI), Remote Terminal Unit (RTU), workforce PCs, laptops, IP cameras and phones get authenticated and authorized are discussed. How confidentiality and data integrity is implemented for various applications flows to and from substations is included. This document also explains how to achieve visibility of assets and Operational Technology (OT) application flows of the Smart Grid. How to perform threat detection and perform necessary remedies are also detailed.

Implementation Workflow

The user of this guide can pick the flow based on need, which can either be Grid Security implementation for Substation Automation deployments or Distribution Automation deployments. The following figure shows the flow of information in this implementation guide. The guide may also have cross references to other sections in this document or related guides to help the reader understand the bigger picture.

Figure 1 Grid Security Solution 3.1 Implementation Flow



Grid Security Requirements and Use cases

Security is an important success criterion for the modernization of the Electrical Grid and for all new developments. Most security requirements and regulatory compliances for Grid Security are well defined in NERC CIP and National Institute of Standards and Technology (NIST), and IEC 62351 specifications. NERC CIP requirements and the Cisco solution implementation to address the NERC CIP requirements are the focus of this guide.

NERC-CIP

The NERC-CIP serves as a reference for the US Department of Energy Cyber Security guidelines for electricity and oil and gas distribution. NERC-CIP is also an excellent reference model for other industries. This set of compliance standards are designed to improve reliability and protect Bulk Electrical Systems (BES) against “cybersecurity compromises that could lead to mis-operation or instability”.

These standards are not a definitive guide to security, but a framework designed to ensure that the right practices - not simply products or features - are in place to lessen the potential of disturbances. The NERC CIP standards focus on policy, process, and procedure while staying away from technical recommendations, with a few exceptions.

The Cisco integrated portfolio and information concerning cybersecurity for control networks, corporate networks, and physical security help you meet the challenging NERC CIP operational standards with minimal operator burden and capital expenditure.

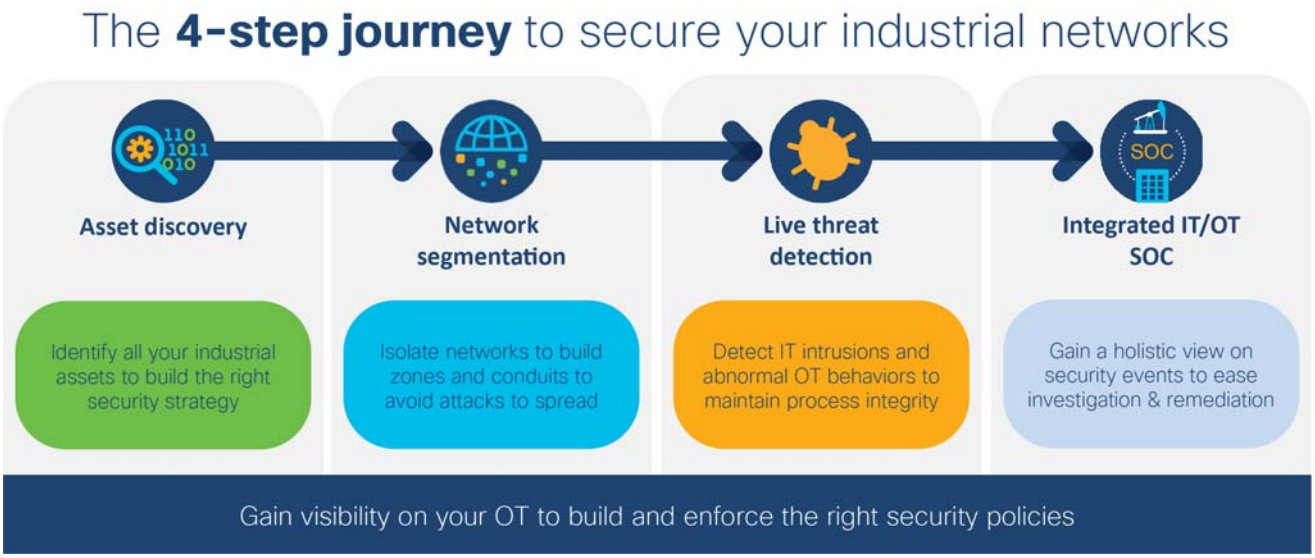
NERC-CIP requirements can be broadly classified into five categories:

- Critical Asset identification and categorization
- Segmentation to establish Electronically Secure Perimeter
- Access Control
- Threat Detection
- Enforce Controls

The NERC CIP standards are primarily focused on establishing policies, programs, and procedures. To help achieve compliance with the underlying technology, the following steps are recommended:

1. Discover your assets and systems
2. Establish physical and logical protection perimeters
3. Enforce controls at and within those perimeters to protect BES reliability and integrity
4. Gain a holistic view on security events to ease investigation and remediation.

Figure 2 Steps to Compliance



The NERC-CIP standards currently subject to enforcement are described in the following table.

Table 1 NERC CIP Standards requirements

Requirements	Summary	Explanation / Purpose	Solution Mapping
CIP-002-51a	Cyber Security – Critical Cyber Asset Identification	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of Cyber Security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.	Cisco Cyber Vision Cisco Stealth watch
CIP-003-8	Cyber Security – Security Management Controls	Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets.	ISA-3000 & FMC Cisco ISE
CIP-005-5	Cyber Security – Electronic Security Perimeter(s)	Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.	ISA-3000 IR1101 CGR-2010 IE-4000 Switches IE-5000 Switches
CIP-006-6	Cyber Security – Physical Security of Critical Cyber Assets	Addresses implementation of a physical security program for the protection of Critical Cyber Assets.	IoT Threat Defense and Grid Security Architecture

Table 1 NERC CIP Standards requirements

Requirements	Summary	Explanation / Purpose	Solution Mapping
CIP-007-6	Cyber Security – Systems Security Management	Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets with the Electronic Security Perimeters.	FMC, ISE
CIP-008-5	Cyber Security – Incident Reporting and Response Plan	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.	CyberVision, ISE, FMC
CIP-010-2	Cyber Security – Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability of the Bulk Electric System (BES).	Cisco FMC, CyberVision, Stealth watch, ISE
CIP-011-2	Cyber Security – Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability of the Bulk Electric System (BES).	Segmentation with ISA-3000, Encryption, TrustSEC
CIP-013-1	Supply Chain Management	To mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.	IEC 62443-4-1 & 62443-4-2 Certifications
CIP-014-2	Physical Security	To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability.	Meraki MV72 outdoor camera & analytics

The following requirements are the focus of this implementation guide:

- CIP-002 which focuses on cyber system discovery and categorization
- CIP-005 which mandates the establishment electronic security perimeters to protect High- and Medium-Impact cyber systems
- CIP-007 which focuses on system access controls (role-based access control), security event monitoring, discovery of open ports and services, anomalies detection in real time to enforce policies and perform threat mitigation

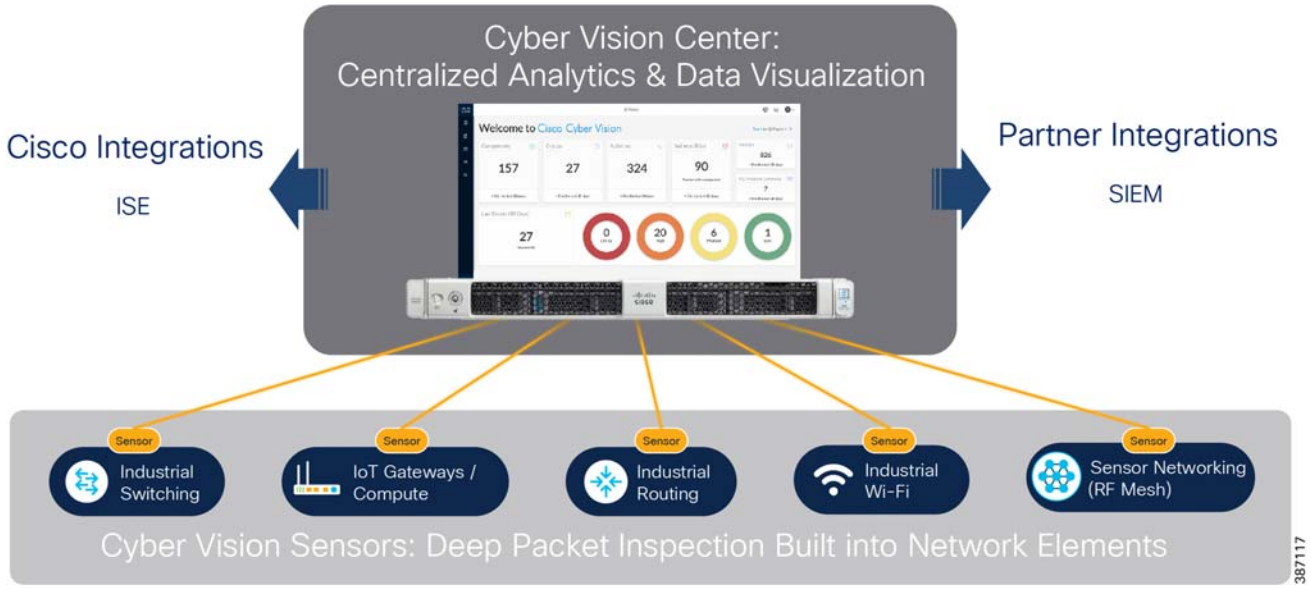
Asset Discovery and Identification

The foundational building blocks of NERC CIP compliance is to discover your cyber systems to categorize as required in CIP-002-5. The ability to passively discover devices, protocols, users, communications patterns, and so on, is used to build a picture of “normal.” Understanding what is normal enables base-lining and highlighting anomalies. Where control networks are intended to be static, anomaly detection is dynamic and white-listing is valuable. A white-listing approach allows permitted traffic to proceed as normal, and anomalous traffic is inspected for malicious content. By understanding the context in which events occur and the potential impacts to your environment, we help you to prioritize your team’s efforts efficiently and effectively.

Lack of visibility is a problem in ICS environments. Many customers don’t have accurate Asset Inventory, and are therefore blind to asset communications. A key advantage of the Cisco Grid Security Solution is that CIP-002-5 is comprehensively examined to understand the difference between acceptable discovery techniques in a control environment contrasted with the techniques an IT environment. It is possible to passively discover devices, protocols, users, communications patterns, and so on, to build a picture of “normal.”

The Cisco Cyber Vision Center (CVC) and sensors can passively discover and categorize assets, protocols and topologies of your OT networks. The Cisco Cyber Vision solution is two-tier architecture in which sensors are installed in OT premises and the Cyber Vision Center for centralized analytics & data visualization resides in the control center. These two aspects are connected by a segmented inline collection network that carries communication between them. Sensors and the cyber vision center application of Cisco Cyber Vision can easily integrate with the Identity Service Engine (ISE), Firepower, for policy enforcement.

Figure 3 Cisco Cyber Vision



The Grid Security Implementation page 20 section address in details about Cisco Cyber Vision solution implementation.

After assets have been identified and categorized, creation of electronic security perimeters (ESPs) is implemented. This implementation is discussed below.

Segmentation and Access Control

CIP-005-5 requires that an ESP must be established for all high-impact and medium-impact Bulk Electrical System (BES) Cyber Systems that are connected to a network via a routable protocol, regardless of whether that segment containing the BES Cyber System(s) has external connectivity to any other network segment. There may be BES Cyber Systems of varying impact classifications within a single ESP; all BES Cyber Systems in the ESP require the highest level of protection corresponding to the BES Cyber System with the highest impact classification. All External Routable Connectivity (ERC)

must be through an identified Electronic Access Point (EAP). This requires inbound and outbound access permissions, including the reason for granting access, and to deny all other access by default. Using one or more methods to detecting known or suspected malicious communications for both inbound and outbound communications is preferred.

An ESP can be defined by segmentation. Methods of segmentation include L2 VLANs, L3 VRFs, firewall interfaces and/or security contexts, and Security Group Tags (SGT) which can provide segmentation regardless of VLAN or IP address assignment. By creating logical zones within the substation, each with their own unique security requirements and using the capabilities of the Cisco ISA-3000 industrial firewall and the Cisco Identity Services Engine, a number of the key cybersecurity requirements can be met.

Access control is identification and authentication control in the utility environment, means to verify the identity of users (humans, software processes, devices) requesting access before activating communication. The aim is to prevent illegitimate (unauthenticated) access of selected devices or data. It is important to define what devices are connected to a network, at what location, and who is operating that device. Allow only known users. Limit number of devices connected to Substation Bus or Distribution Automation Gateways. Prevent rouge devices/users accessing the network. Control and limit access to the resources. Maintain logs of users OT transactions and events.

Threat Detection and mitigation

360° threat detection—Detect threats before it is too late. Abnormal traffic detection and mitigation post thread detection. Protect critical assets against cyber-attacks and insider threats. The anomaly detection is the process to determine which observed events are to be identified as abnormal because it has significant deviation from normal behavior which is called baseline.

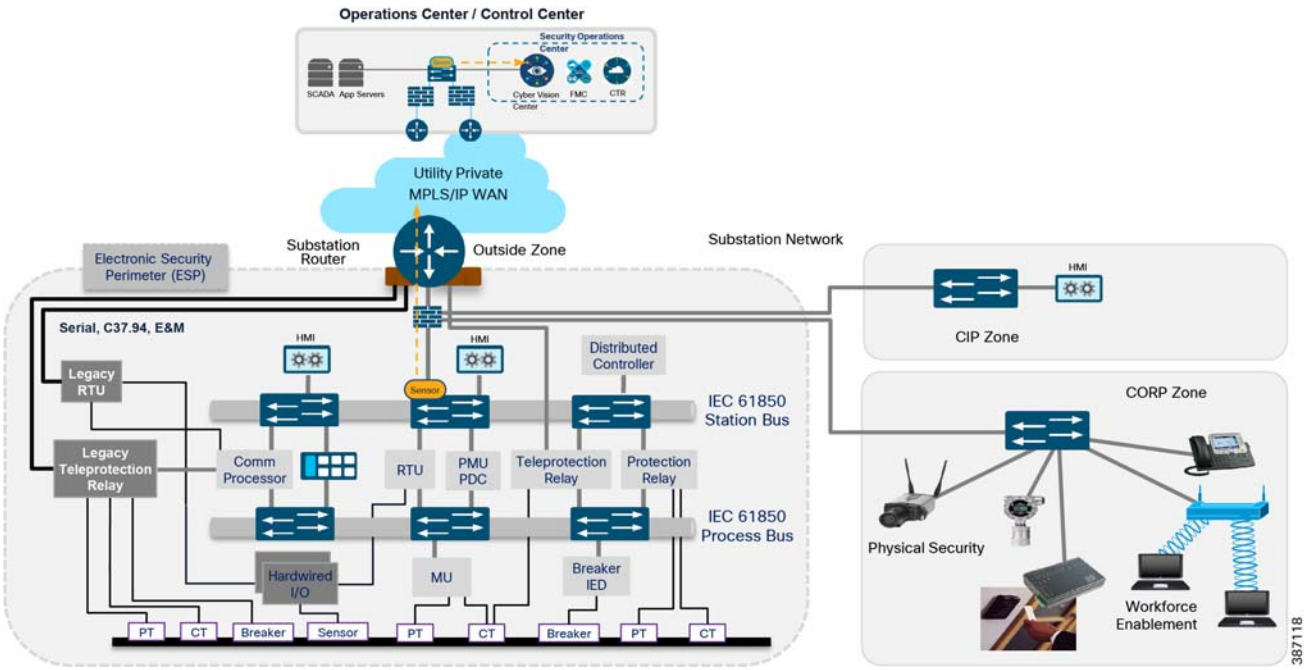
Substation design

Key components of a Substation design include:

- Network resiliency
- a Corporate Substation (CORPSS) zone
- a Critical infrastructure Perimeter (CIP) zone
- the Electronic Security Perimeter (ESP) zone
- the Outside zone

Relative firewall security levels are provided to illustrate trust levels between zones.

Figure 4 Grid Security Architecture for Substation Automation



Network Resiliency

High availability for Information and Communication Topology network layer provides network resiliency and better convergence at times of network faults. Various protocols can be used. Some legacy resiliency protocols within ring topology deployments are:

- Rapid Spanning Tree (RSTP) is a variant of spanning tree protocol (STP) that is known, used, and trusted by IT professionals who have used Cisco switches.
- Resilient Ethernet Protocol (REP) - a Cisco proprietary protocol described below.

  IEC 61850 implementation standards in the station bus and process bus, high performance applications in the utility substation mandate a number of key requirements to be addressed. The substation architecture must meet design requirements for GOOSE and Sample Values, both of which are multicast traffic types. This includes high availability (HA) and topology choices to meet scale, segmentation, and communications requirements. IEC 61850-5 provides guidance for HA and communication requirements based on a number of use cases in the standards. With these failover and recovery times at ZERO milli-seconds for some use cases, a truly “hitless” architecture is required. There are two choices to meet this hitless requirement:

- Parallel Redundancy protocol (PRP) supports either tree or ring topologies with no limits on node counts, and it can deliver a ZERO millisecond failover/recovery requirement. However, PRP has one drawback. PRP requires duplicate LANs (named LAN-A & LAN-B) and double the networking equipment hardware.
- Highly Available Seamless Ring (HSR) also delivers a ZERO millisecond fail-over/recovery requirement but is only available in a ring topology and scales to a limited number of devices. HSR does NOT require duplicate LANs (double the switching infrastructure) in the ESP.

For more details on design recommendations and implementation of network resiliency refer to the following: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.pdf

Electronic Security Perimeter (ESP) zone

The ESP zone contains components that play an active role in the proper functionality of the Critical Infrastructure/Smart Grid. These components should be regarded as being the most valued and trusted resources on the Substation network and highly protected.

With very few exceptions, outbound communications from this portion of the network must be significantly restricted. Any communication from this zone to any lower-security zone should leverage a "Pull" model – initiating the connection from the ESP zone. Inbound connections into the ESP zone should be discouraged except for any business-critical applications.

This zone is intended to provide limited network connectivity for industrial components such as IEDs and Protection Relays with direct user-level access restricted to appropriately-vetted employees that require direct Substation access for machine maintenance. Depending on the security model employed, access to the IEDs and Protection Relays can also be restricted to specific, well vetted, and highly audited hosts, denying access from personal/corporate laptops. Outbound connections are highly restricted from this zone.

Corporate Substation (CORPSS) zone

The Corporate Substation zone is a natural extension to the corporate/enterprise "General Purpose" network. Traffic from this zone can only access other corporate assets directly by passing through the Outside zone. Access to the other zones (CIP and ESP) requires additional credentials and access restrictions.

All employees can leverage this zone for basic connectivity to business resources including email, file shares, and general access to the Internet via the Outside zone

Critical Infrastructure Perimeter (CIP) zone

The CIP zone is a "DMZ" for the Substation. This zone is "semi-trusted" an has a Firewall security level between the Corporate Substation zone and the ESP zone. As such, this zone is designed to allow proxied user-level access between both the Corporate Substation and ESP zones – leveraging an information security (InfoSec) hardened Bastion host. Other support infrastructure may also exist in this zone such as a Secure Policy Server such as Cisco ISE or ACS, Network Services, and/or a user management server such as Lightweight Directory Access Protocol (LDAP) or Active Directory (AD).

Inbound connectivity into this zone is provided via a Remote Access VPN client or via a Courtesy port within the CIP zone switch network. The Courtesy Port will be discussed in detail in a later section of this document. As a user connects into the CIP zone, the user's level of access will be restricted to allow connectivity to ONLY the Bastion host. This Bastion host will have predefined levels of access inbound into the ESP zone and outbound towards the corporate network. All user-level connectivity between the ESP and Corporate Substation networks will be proxied via this Bastion host. Access to and from other resources within the CIP zone must also be significantly restricted to ensure the integrity of these resources and their interactions with the ESP zone.

Traffic can flow from any employee or contractor that has the proper credentials to operate the network and security resources within this zone. Membership in the appropriate Active Directory (AD) group can be leveraged to restrict Courtesy Port or Remote Access authentication and authorization accordingly.

Outside zone

This zone connects the Substation topology to the rest of the infrastructure, whether the infrastructure is owned by the Utility Corporation or provided by a 3rd party Service Provider. This zone is untrusted. The security postures of assets within this outside zone are, in most cases, outside of the control of the Utility Corporation.

The traffic allowed to traverse this interface should be encrypted, authenticated, and/or originally initiated from the inside zones (ESP, CIP, and CORPSS) of the ISA3000 firewall. The AnyConnect Remote Access endpoints can authenticate to the Outside interface to gain access to the CIP and ESP zones.

Because this zone is considered outside the Substation architecture, the protection of this zone is varied and relies solely on the protections provided by the WAN infrastructure.

In an actual Connected Utilities “Smart Grid” architecture, the Substation block may be repeated multiple times across the network architecture. Certain components of the Substation design may also be optional depending on the size, the function, and the topology of the substation.

Traffic segmentation within the Substation

Within substations the following VLANs are suggested to protect mission critical traffic from potential network attacks:

- OT SCADA VLAN – This VLAN is for SCADA traffic such as Modbus, DNP3, IEC61850 GOOSE. We are starting to see the Process bus and station bus become segmented based on common communication peers for security and operation performance benefits.
- Network Management VLAN – For all network management traffic. A designated management port is enabled within a VLAN that is used by the management system to communicate with the devices.
- Remote Workforce VLAN (Intranet) – The remote workforce accesses the substation network using on-site ruggedized PC or wire connected PC.
- Remote Workforce VLAN (Internet) – Partner or third-party crew is allowed on this VLAN to gain access to the Internet. Only outbound traffic is permitted.
- Physical Security VLAN – Video surveillance traffic, physical access traffic.
- Black Hole VLAN – As a security best practice, all unused ports are assigned to this VLAN.

VRF Segmentation at the substation router should follow VLAN segmentation.

Access Control

Ensure that only authorized personnel are accessing the network and valid devices are part of the grid network by using the suggestions below.

- Authenticating and authorizing field technicians or operations center staff before they can view or configure devices, track changes made – role-based access control (RBAC). For engineer/technician devices that need to access the substation, only 802.1x authenticated users should be permitted access.
- Authenticating users and endpoints connected to the substation / control center networks, via various different methods such as AAA and/or endpoint certificates. MAC Authentication Bypass (MAB) is used for endpoints do not have 802.1x supplicant.
- Limit the number of devices that can be connected to the port. Prevent rogue/unknown devices connected to the network.
- To protect LAN switches from being exploited, unused ports of all LAN switches at the substation must be shut down by default. All ports must be explicitly enabled. For those ports that are enabled, configure port security to protect the network from LAN-based attacks. This feature limits the number of MAC addresses that are able to connect to a switch, and ensures that only approved MAC addresses are able to access the switch.
- Port Security prevents MAC address flooding and ensures that only approved users can log onto the network. The following security policy applies to port security configuration:
  - The maximum number of secure MAC addresses for a port is one.
  - Specify static MAC addresses for IED or other IP-enabled control devices.
  - If the IED MAC is unknown in certain deployment scenarios, use sticky port security.

Bandwidth Control

Prevent a malicious user taking up the bandwidth and thereby starve critical application traffic. Prevent data traffic from the contractor occupying the network and affecting the control traffic. Rate limiters can limit traffic per VLAN, port or user to mitigate the impact of packet-blasting worms and limit amount of traffic a user can send onto the network. Operators can rate limit using either traffic policing or shaping functions.

Threat Detection

NERC/CIP 007 defines requirements for Threat detection. Baseline the OT Traffic for anomaly detection. Deep packet inspection of OT Traffic for attack detection and prevention.

Security Event Monitoring, Malicious Code Prevention, and Patch Management

For Anomaly detection discover the open ports and services for various OT flows in substation. This can be done with Cyber Vision Center and Cyber Vision Sensors as discussed in the implementation section. Enforce control policies from Identity Service Engine on the policy server to different network devices like firewall and network switches if a change in the baseline is detected.

SCADA/OT preprocessor features can be enabled on substation firewall for zero day attack detection of OT traffic. This preprocessor can be perform deep pack inspection of SCADA packet headers and OT commands. For more details on OT preprocessor refer to:

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

IPS with built-in signatures for malicious code prevention and end point posture assessment of for devices as laptops, workstations, servers connecting to Substation/CC LAN segments to detect any virus/spyware before allowing access to the network, forcing remediation such as installing software patches or updating anti-virus database.

Distribution Automation design

Distribution Automation (DA) refers to the monitoring and control of devices located on the distribution feeders, such as line reclosers, load break switches, sectionalizers, capacitor banks and line regulators and also devices located in the distribution substation. DA is an overlay network deployed in parallel to the distribution feeder. It enables two-way communication between controllers used in the distribution feeder and the intelligence application that resides in the Utility Control Center or Secondary Substation for improving grid reliability, availability, and control. This guide focuses on Secondary Substation Distribution Automation use case using IR1101 as Cellular Gateway.

DA Secondary Substation Architecture is a two-tier centralized Architecture. WAN tier i.e. cellular backhaul connects Distribution Substation/Grid to the Centralized Control Center. Cisco IR1101 can be positioned as Secondary Substation Router (SSR) to connect to various OT devices like RTU, IED, Meter Data concentrators, Capacitor Bank controllers and Voltage Regulator controller. The following figure illustrates a simplified topology.

DA use cases application flow can be classified as follows. Flow can be bidirectional.

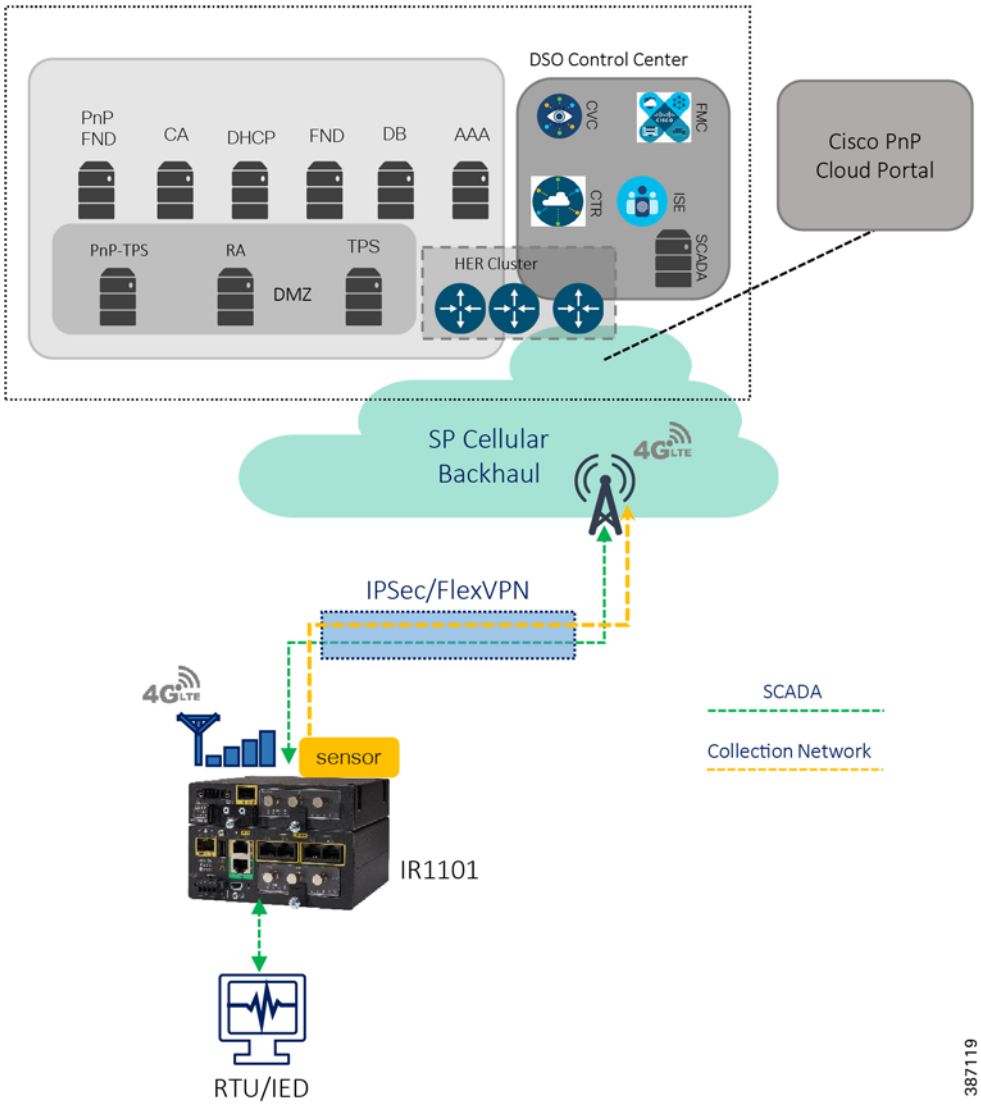
- SCADA <----> RTU <----> IEDs
- SCADA <----> IEDs
- IEDs <----> IEDS

Grid Security Solution Architecture implementation in this guide provides considerations for SCADA to IED application flows. It also considers the following as some of the security requirements for Distribution Automation Solution.

- Access Control
  - User and Device Identity

  - Authentication, Authorization & Accounting
- Data Confidentiality and Data Privacy
  - Network Segmentation
  - Security Connectivity and Encryption (VPN)
- Threat Detection and Mitigation
  - Security Zones with Firewall
  - Intrusion Prevention with SCADA signatures
- Device and Platform Integrity
- OT Visibility

Figure 5 Grid Security Architecture for Secondary Substation Automation



For more details of other use cases and flows related to Distribution Automation Solutions, refer to the Distribution Automation Design and Implementation Guides:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG.html
https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG.pdf

Network Resiliency in Distribution Automation

High availability is achieved by designing redundancy at multiple levels in the Distribution Automation solution as listed below:

- HER Level Redundancy
- WAN Backhaul Redundancy
- Control center level – dual control center and application level redundancy, explained in SCADA Services.

It is beyond the scope of this implementation guide to explain various mechanisms. Refer to the following guide for details.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG/DA-SS-DG-doc.html#12933

System Overview

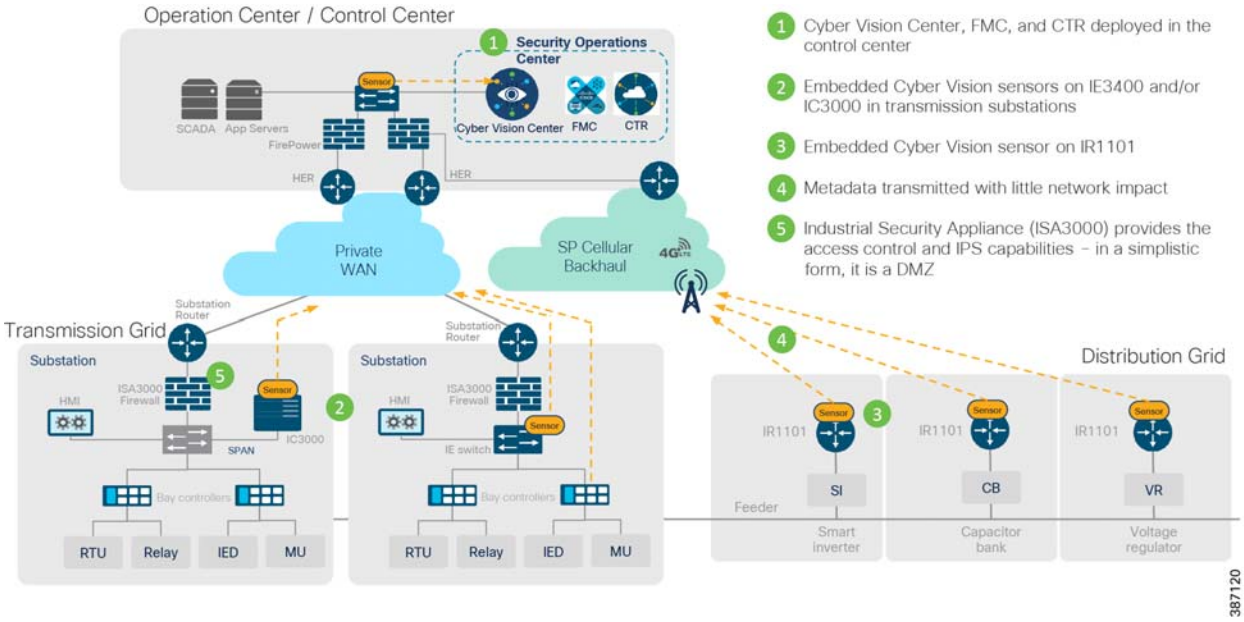
This section explains the topologies used for solution validation and the requirements for different components with features like licenses, IP addressing, and so on.

Topology

Cisco Substation Automation is a three-tier architecture including Substation LAN, Substation WAN, and Substation Control Center. The following figure illustrates a simplified Substation Automation topology. Cisco Distribution Automation Secondary Substation Architecture is a two-tier centralized Architecture. WAN tier i.e. cellular backhaul connects Distribution Substation/Grid to the Centralized Control Center. Cisco IR1101 can be positioned as Secondary Substation Router (SSR) or Distribution Automation (DA) Gateway for Feeder use cases. SSR and DA Gateways in turn connect to various OT devices like RTU, IED, Meter Data concentrators, Capacitor Bank controllers and Voltage Regulator controller. Figure 5 illustrates a simplified topology with IR1101 acting as Secondary Substation Router.

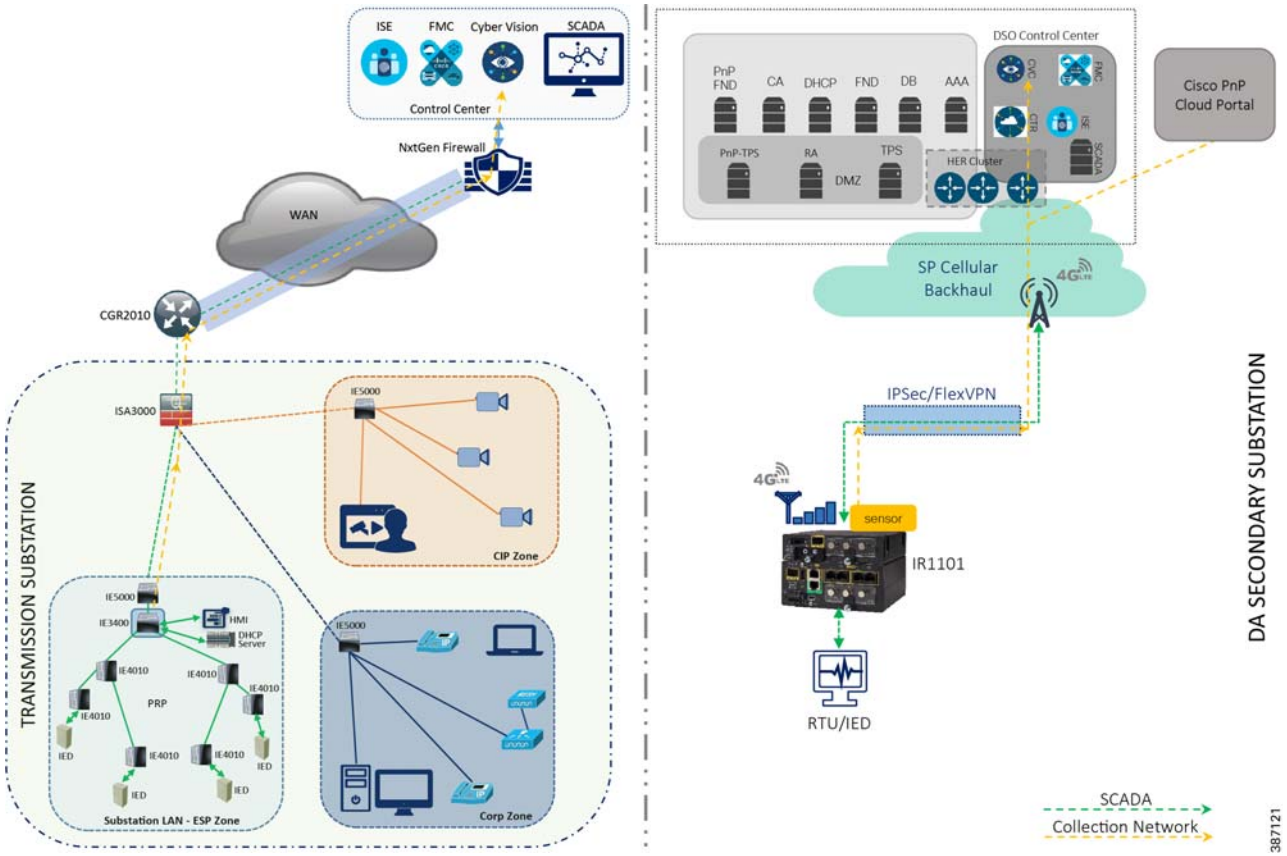
These architectures are represented in the following figure.

Figure 6 Grid Security Solution Logical Topology



To validate the designs and considerations, the solution testbed has been built in the lab as shown in the following figure. The focus of solution validation is on the components including the ISA3000, IC3000 as hardware sensor, IE3400 and IR1101 as network sensors, IE4000, IE5000, IE4010 switches. The control and data center applications that support them including Cisco Identity Services Engine, Cisco Cyber Vision Center and Firewall Management Center are also included. In this release of the solution, validation included configuring all components to work together to enable the desired use cases. Additional testing, including scale and performance, will be performed in a future release.

Figure 7 Grid Security Solution Validation Topology



IP Addressing/VLAN

This implementation assumes a simple topology for lab validation efforts. The following table lists the various IP Addresses and VLANs used for various components of the topology installed on a Cisco UCS server. ASR1K-Virtual acts as both NTP server and gateway to other components. Networks are defined for the virtual instances of different components for the reachability required. The following list includes networks defined in the UCS.

- VM_Network – Uses IP addresses in the lab subnet for access to the Internet. Traffic is untagged.
- VM_Internal_Communication – Uses IP addresses in subnet 192.168.3.x for internal communication between various VMs. Traffic is untagged.
- ISE_VLAN – Uses IP addresses in subnet 192.168.2.x for communication to Next Generation Firewall (NGFW). Traffic is tagged with VLAN 2.
- Collection_Network – Uses IP addresses in subnet 192.168.169.x for communication between Cyber Vision Center and Cyber Vision Sensors. Traffic is encrypted on IPSec tunnel when flowing over WAN or Internet. Traffic is tagged with VLAN 169.

Table 2 IP Addressing

Component	IP Addresses
Jump Host - Windows	192.168.3.106 192.168.2.206 192.168.169.206
Active Directory- Microsoft	192.168.2.204 192.168.3.104
Identity Services Engine	192.168.3.102 192.168.2.202
Cyber Vision Center	192.168.3.113
Firepower Management Console	192.168.3.177
Stealth Watch Management Console	192.168.2.210
Flow Collector	192.168.2.211
ASR 1K – Virtual – NTP Server	192.168.3.108 192.168.2.108 192.168.169.108

Hardware Software Matrix

The table below describes the hardware, software, and role of the main components of the solution. These software versions were used in the Cisco solution validation lab, and all were publicly available when this document was published.

Table 3 Hardware and Software Matrix

Device Role	Description	Hardware Platform	Software Release
Substation Firewall	Ruggedized firewall, Virtual Private Network (VPN) head-end (Site-to-site, RA), FirePOWER Intrusion Prevention System (IPS)	ISA3000	FTD: 6.6.0 build 90
Ruggedized Switch	Access switch-DANH,SANH,RedBox,etc., switch port security	IE4000	15.2(7)E2
Ruggedized Switch	Access switch, switch port security	IE5000	15.2(7)E2
Ruggedized Switch	Access switch, switch port security	IE4010	15.2(7)E2
Distribution Automation Gateway with Cyber Vision Sensor	Edge compute platform hosting Cisco Cyber Vision Sensor application (release 3.1.0) and acts as Network Sensor	IR1101	17.3.1
Ruggedized Switch with Cyber Vision Sensor	Edge compute platform hosting Cisco Cyber Vision Sensor application (release 3.1.0) and acts as Network Sensor	IE3400	17.3.1
Control/Data Center Firewall	Firewall, Site-to-site VPN	FPR4150	FTD: 6.6.0 build 90
AAA	Authentication, Authorization server for policy definition	Identity Services Engine (running as a virtual machine on Cisco Unified Computing System)	2.4.0.357 Patch 10

IPS	Centralized management and monitoring server for FirePOWER IPS devices	Firepower Management Center for VMWare	FMC: 6.6.0 build 90
Industrial Compute Gateway with Cisco Cyber Vision Sensor	Edge compute platform hosting Cisco Cyber Vision Sensor application (release 3.1.1) and acts as Hardware Sensor	IC3000 Cisco Cyber Vision Sensor application	IC3000-K9-1.2.1.SPA Application Version: CiscoCyberVision 3.1.1
Cisco Cyber Vision Center	Cisco Cyber Vision Center used to manage Cisco Cyber Vision sensor application hosted on IC3000 edge compute platform.	CVC	CiscoCyberVision -3.1.1.ova

Licensing

The following table describes the hardware, software, and the corresponding licenses required to enable features and functions relevant to the solution. These licenses were the ones certified in Cisco's solution validation lab, and all were publicly available at the time this document was published.

Table 4 Licenses and components

Device Role	Hardware Platform	License	Reference
Substation Firewall	ISA3000	Base Subscription required for the following licenses. Malware Threat	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
Ruggedized Switch	IE4000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html
Ruggedized Switch	IE5000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-5000-series-switches/datasheet-c78-734967.html
Ruggedized Switch	IE4010	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4010-series-switches/datasheet-c78-737279.html?cachemode=refresh
Secondary Substation Router	IR1101	network-advantage	https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html#Softwarelicensing
Ruggedized Switch	IE3400	network-advantage	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie3400-rugged-series/datasheet-c78-741760.html
Control/Data Center Firewall	FPR4150	Base Subscription required for the following licenses. Malware Threat	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
AAA - ISE	Identity Services Engine running as a virtual machine on Cisco Unified Computing System.	Traditional License with the following features: ■ Base ■ Plus ■ Apex ■ Device Admin	https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_0110.html

IPS	Firepower Management Center for VMWare	Firepower Management Center Virtual	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
Industrial Compute Gateway with Cisco Cyber Vision Sensor	IC3000 Cisco Cyber Vision Sensor application		IC3000-K9-1.2.1.SPA
Cisco Cyber Vision Center	CVC	Smart Licensing Essentials Advantage	https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_Release_3_0_0.pdf

Grid Security Implementation

Security is an important success criterion for the modernization of the Electrical Grid as well as for all new developments. Most of security requirements and regulatory compliance for Grid Security are well defined in NERC CIP and National Institute of Standards and Technology (NIST). The recommended features and steps for implementation are discussed in the sections that follow.

Segmentation

Dividing a larger computer network into several small subnetworks that are each isolated from one another is called as Network Segmentation. It works by controlling the way traffic flows among the different parts of the network. It could help to stop all traffic in one part from reaching another, or can limit the flow by traffic type, source, destination, and many other options. VLANs, Access-Lists and Zones are some of the features to achieve network segmentation.

Some of the benefits of network segmentation are:

- Improve operational performance.
- Limit cyberattack damage.
- Protect Vulnerable devices.

The following section lists the means to achieve segmentation for Grid Security Solution requirements.

Segmentation in Substation Automation LAN

As explained in the substation automation network design sections, VLANs and Firewall Zones are used for segmentation inside a substation LAN network. The following section lists the steps involved in provisioning the same.

VLAN for segmentation in switches

Network segmentation with virtual local area networks (VLANs) creates a collection of isolated networks within the Utility Network like Substation LAN. Each network is a separate broadcast domain. With proper planning, when configured, VLAN segmentation helps to restrict access to system attack surface. It reduces packet-sniffing capabilities and increases threat agent effort. Finally, authorized users only “see” the servers and other devices necessary to perform their daily tasks.

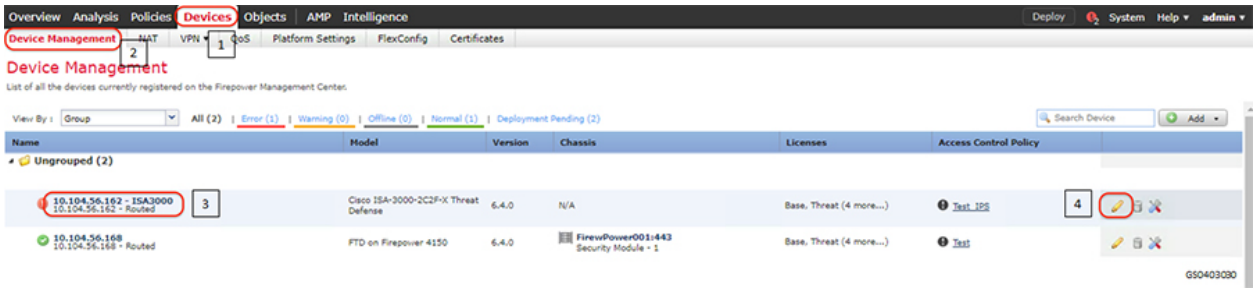
Another advantage of segmentation is protocol or device separation. Network architects can limit certain protocols or devices to certain segments of the network. For example, if IEC61850 GOOSE MMS or Sample Values exist on the network, they can each have their own VLAN in which to operate. This provides better management of data traffic and segments network traffic with similar network security requirements, yielding better resiliency during high-traffic communications, even during a cyberattack.

In this example, the Gigabit Ethernet1/2 interface on ISA3000 is configured with different VLANs so as to reach various devices in ESP zone. The ESP zone is further divided into multiple VLANs namely IES management for management of Industrial Ethernet Switches in ESP zone, IED for Utility devices in ESP Zone and IC3000 for IC3000 acting as Cisco Cyber Vision hardware sensors in ESP Zone. The switches in the ESP zone are also configured to allow these VLANs.

The following are the steps required to configure VLANs and corresponding sub interfaces on ISA3000 and Cisco Industrial Ethernet switches in Substation LAN network.

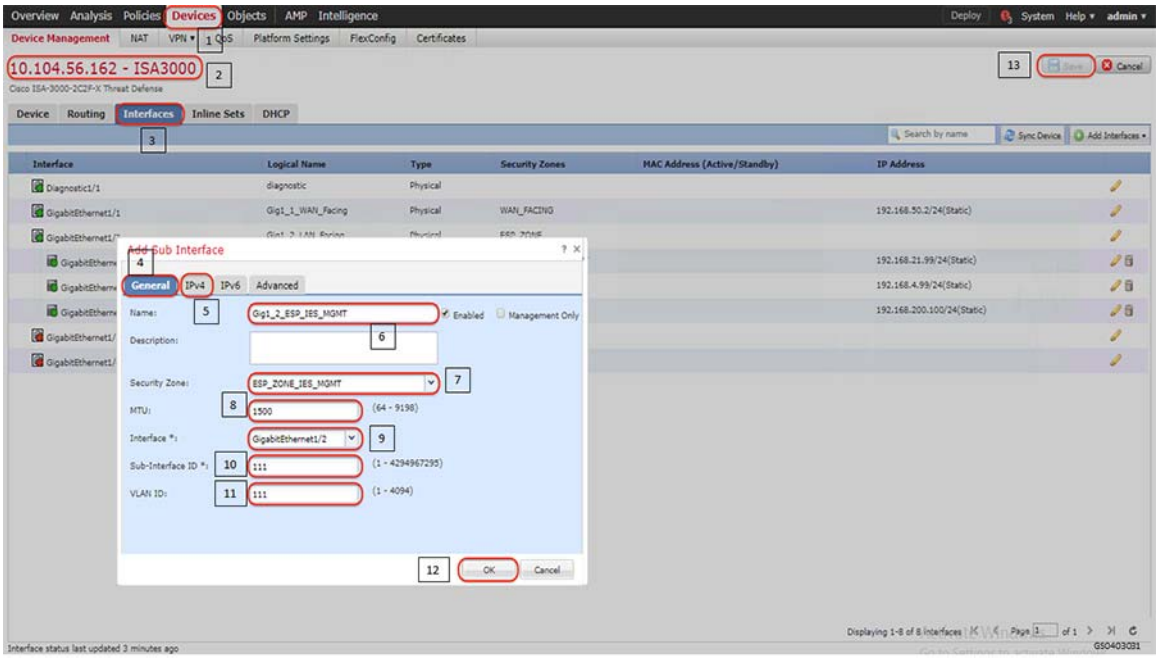
1. Identify and select the ISA3000 device in Firepower Management Center that needs to be configured for different VLANs as explained above. The required steps are highlighted in the following figure:

Figure 8 Selection of ISA3000 in FM



2. Configure the device interface for the required sub-interface, corresponding IP address and save as highlighted in the following figure.

Figure 9 Configuring ISA3000 sub interface using FMC



3. Repeat step 2 to configure remaining VLANs as required.

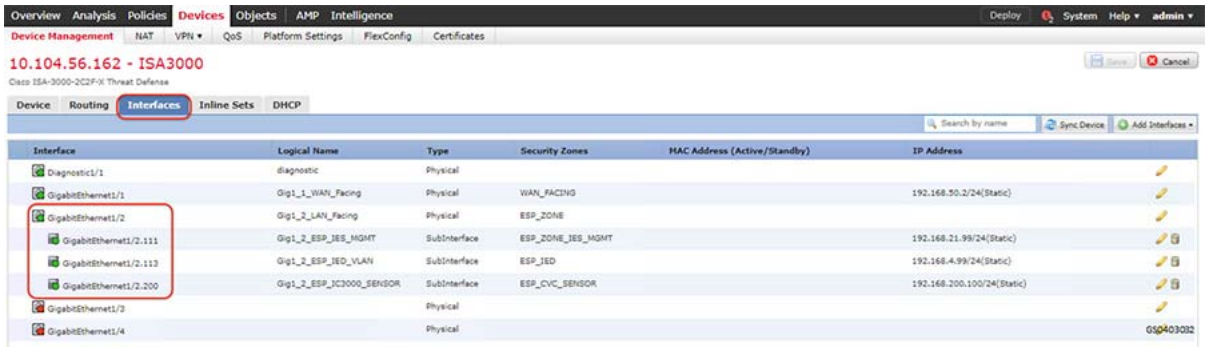
4. Use the following commands to configure VLANs on Industrial Ethernet Switches (IES).Repeat the step as required across the switches.

```
IES-Switch#config t
IES-Switch(config)#vlan 2
IES-Switch(config-vlan)#no shut
IES-Switch(config)#exit

!
interface GigabitEthernet1/1
 description connected to gig1/2 ISA3000
 switchport trunk allowed vlan 2,111,113,169,200
 switchport mode trunk
 service-policy input TestInputSCADA
!
```

Verification

After the interfaces are configured and saved and connected, the status of the interface on the Graphical User Interface would turn green as highlighted in the following figure.

Figure 10 Configured ISA3000 sub interfaces



Similarly, a successful creation of VLAN on Cisco Industrial Ethernet switch would ensure that the VLANs are part of the allowed list on the respective interfaces. The following is a sample output to check successful creation of the VLAN.

```
IES-Switch#show vlan id 111

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
111  ISE_MGMT_VLAN                    active    Gi1/1, Gi1/9, Gi1/11, PR1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
111  enet  100111     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------


VLAN Type              Ports
---- ----------------- ------------------------------------------------------------
```

Zones for segmentation in Firewall

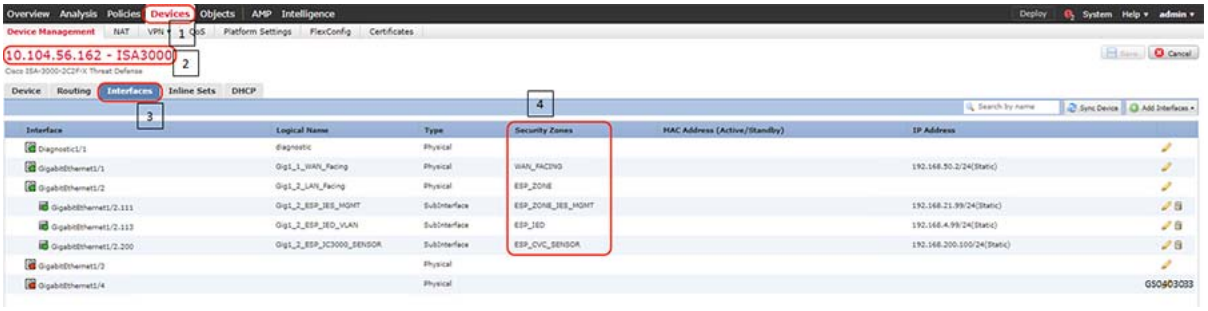
There are four key components of a Substation design as explained in earlier section of this document – a Corporate Substation (CORPSS) zone, a Critical infrastructure Perimeter (CIP) zone, the Electronic Security Perimeter (ESP) zone, and the Outside zone.

- ESP – this is the most secure zone containing critical components such as RTUs and IEDs. Access to the ESP zone is highly restricted. In the topology diagram, these are the components connected with ORANGE lines in the substation. This zone may contain multiple VLANs. This guide uses VLAN 111 for Industrial Ethernet Switch management, VLAN 113 for IEDs, VLAN 200 for Cisco Cyber Vision Hardware sensor.
- Multiservice/CIP – this acts as kind of a demilitarized zone (DMZ) for the substation. This can contain the jump server host which has access to the ESP. Other items like video surveillance cameras, and local logging/ authentication, authorization, and accounting (AAA) applications reside here. This zone may contain multiple VLANs on the same IE4000 switch.
- CorpSS – this is an extension of the corporate network in the substation. It provides Wi-Fi connectivity, voice service, and general connectivity for employees to access email, web, or possibly the Internet through the central site.

- Outside Zone/WAN – This zone connects the Substation topology to the rest of the infrastructure – whether the infrastructure is owned by the Utility/Corporation or provided by a 3rd party Service Provider. The traffic that should be allowed to traverse this interface should be encrypted, authenticated, and/or originally initiated from the inside zones (ESP, CIP, and CORPSS) of the ISA3000 firewall.

Follow the steps listed in VLANs for Segmentation in switches section to configure zones.

Figure 11 Configured ISA3000 sub interfaces



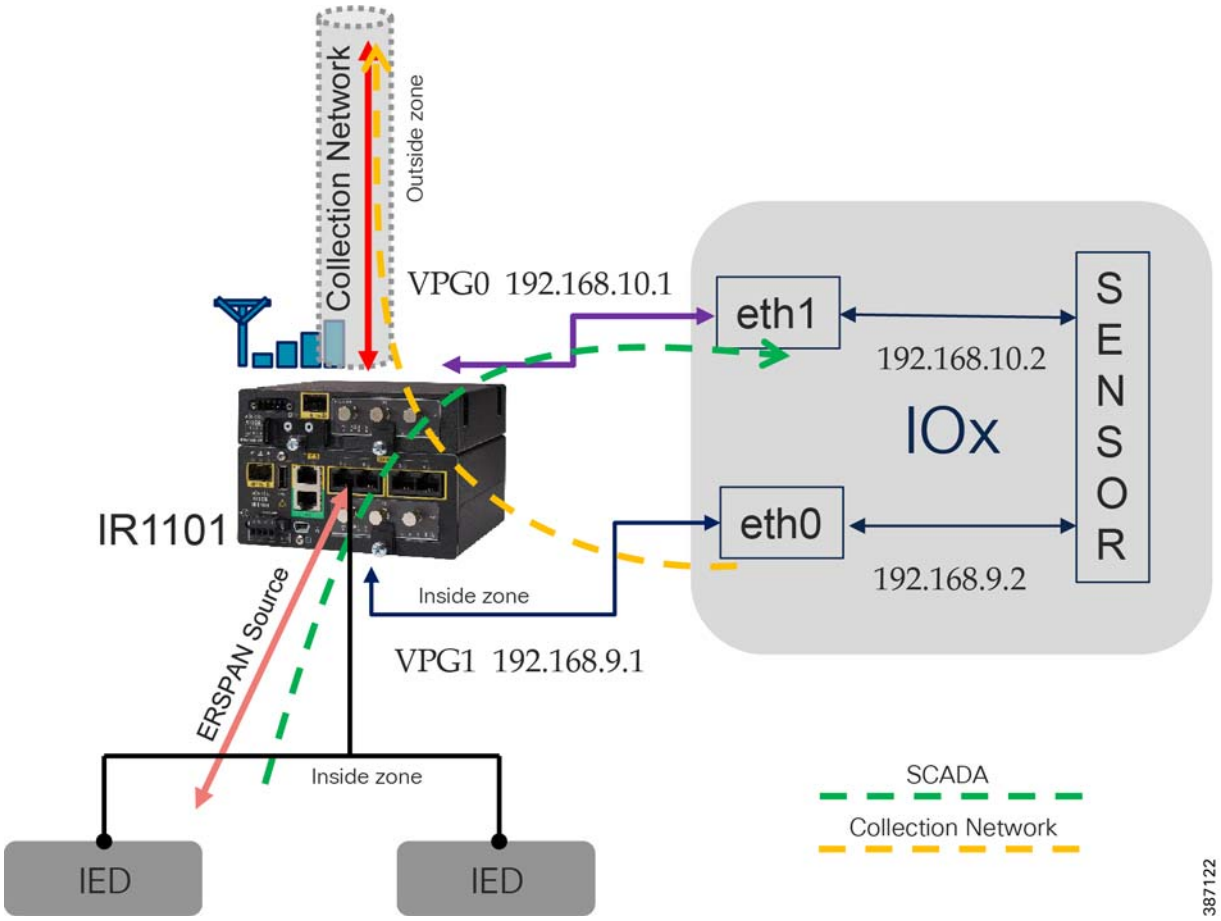
Segmentation in Distribution Automation – Secondary Substation Gateway

As explained in the distribution automation network design sections, VRFs and Firewall Zones are used for segmentation inside a Distribution automation network. The following section lists the steps involved in provisioning the firewall zones. Segmentation using VRFs will be addressed in future guides.

Zone based Firewall

All traffic originating or passing through from the SSRs and DA Gateways can be protected by enabling IOS zone-based firewall. Zone Based Firewall (ZBFW) IOS feature can be enabled to detect and block unwanted flows. The ZBFW mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones, also the traffic will be dynamically inspected as it passes through the zones. Zone based firewall will support Application inspection and control for HTTP, POP3, Sun RPC, IM Applications and P2P File sharing. WAN facing interface like Cellular or FlexVPN tunnel is placed in outside zone and interfaces connected to DA IEDs and Edge Compute Application (internal logical interface) are placed on inside zone. Interzone communication is denied, traffic will be denied among the interfaces that are in the different zones unless we specify a firewall policy. The following topology depicts the same.

Figure 12 Distribution Automation Zone based firewall and segmentation



The following firewall policy is defined between outside and inside zones.

- Allow following IPSEC FlexVPN ports
  - ISAKMP - UDP 500
  - ESP - Protocol 50
  - ISAKMP NAT-Traversal - UDP 4500 (NAT-T)
- In Grid Security Design SCADA traffic is interesting traffic will be encrypted by IPSEC FlexVPN. So, there is no requirement to open up SCADA protocol ports. If needed following SCADA ports can be opened. Modbus Port 502, DNP3 port 20000, IEC 60870-5-104 port 2404 and IEC 61850 MMS port 102.
- Open up ports number required for management application like FND, Cyber Vision Center and any other needed applications.

Intra-zone communication is allowed, traffic will flow implicitly among the interfaces that are in the same zone.

The following steps are required to configure zone-based firewall on secondary substation router.

1. Before you create zones, you should group interfaces that are similar when they are viewed from a security perspective. By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. Firewall zones are used for security features.

2. Configure Layer 3 and Layer 4 firewall policies.

```
!
class-map type inspect match-any IN-OUT
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
class-map type inspect match-any OUT-IN
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
!
```

3. Create security zones and zone pairs.

```
!
zone security INSIDE
zone security OUTSIDE
zone-pair security IN-OUT-PAIR source INSIDE destination OUTSIDE
 service-policy type inspect IN-OUT
zone-pair security OUT-IN-PAIR source OUTSIDE destination INSIDE
 service-policy type inspect OUT-IN
!
```

4. Assign the interfaces to the respective zones. In this example FlexVPN tunnel is the OUTSIDE interface.Collection network interface VirtualPortGroup1 and a VLAN1000 are INSIDE interfaces.

```
!
interface Tunnel0
 description IPsec tunnel to HER1.ipg.cisco.com
 ip unnumbered Loopback0
 ip nat outside
 zone-member security OUTSIDE
 ipv6 unnumbered Loopback0
 tunnel source Cellular0/1/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
 ip virtual-reassembly
!

!
interface VirtualPortGroup1
 description App Collection N/w
 ip address 192.168.9.1 255.255.255.0
 ip nat inside
 zone-member security INSIDE
 ip tcp adjust-mss 1160
!

!
interface Vlan1000
 ip address 192.168.0.1 255.255.255.0
 zone-member security INSIDE
!
```

5. The functioning of the feature can be verified using the following command.

```
IR1100_FCW23110H4A#show policy-map type inspect zone-pair sessions
  Zone-pair: IN-OUT-PAIR
```

```
  Service-policy inspect : IN-OUT

    Class-map: IN-OUT (match-any)
      Match: protocol icmp
      Match: protocol tcp
      Match: protocol telnet
      Match: protocol http
      Match: protocol https
      Match: protocol ssh
      Inspect
        Established Sessions
         Session ID 0x0001166D (192.168.9.2:52988)=>(192.168.109.109:443) tcp SIS_OPEN
          Created 339:35:19, Last heard 00:01:05
          Bytes sent (initiator:responder) [16479921:1287975]
         Session ID 0x0001166A (192.168.9.2:52952)=>(192.168.109.109:443) tcp SIS_OPEN
          Created 339:55:13, Last heard 00:02:15
          Bytes sent (initiator:responder) [921458:877843]
         Session ID 0x0001166C (192.168.9.2:52984)=>(192.168.109.109:443) tcp SIS_OPEN
          Created 339:36:30, Last heard 00:07:50
          Bytes sent (initiator:responder) [5677625:285189]
         Session ID 0x0001167D (192.168.9.2:44288)=>(192.168.109.109:10514) tcp SIS_OPEN
          Created 37:38:25, Last heard 00:01:04
          Bytes sent (initiator:responder) [1457094:7231]
         Session ID 0x0001166B (192.168.9.2:52960)=>(192.168.109.109:443) tcp SIS_OPEN
          Created 339:48:52, Last heard 00:02:11
          Bytes sent (initiator:responder) [22290656:892118]

Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
  Zone-pair: OUT-IN-PAIR
  Service-policy inspect : OUT-IN

    Class-map: OUT-IN (match-any)
      Match: protocol icmp
      Match: protocol tcp
      Match: protocol telnet
      Match: protocol http
      Match: protocol https
      Match: protocol ssh
      Inspect
        Established Sessions
         Session ID 0x00011649 (192.168.107.200:56784)=>(192.168.0.3:42145) tcp SIS_OPEN
          Created 678:09:23, Last heard 00:01:27
          Bytes sent (initiator:responder) [728222:897287]
         Session ID 0x00011648 (192.168.107.200:56783)=>(192.168.0.3:42145) tcp SIS_OPEN
          Created 678:09:36, Last heard 00:05:29
          Bytes sent (initiator:responder) [724367:892535]


    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
IR1100_FCW23110H4A#
```

IP Network Encryption

Site to Site VPN in Substation LAN

Based on NERC-CIP, the various zones in a Substation LAN as defined in the earlier section needs to communicate over an encrypted VPN tunnel to the centralized data center. IKEv2 is used to provide secure authentication and negotiation of the encryption and integrity methods to form the security association (SA). Cisco IP Security (IPsec) is used to provide encryption and integrity for payload data. However, traffic inside the Substation LAN network is not encrypted.

This section lists the basic steps to establish a simple IPSec tunnel between Cisco CGR2010 and Cisco FPR4150 devices using Firepower Management Console (FMC).

Before you begin:

- Cisco FPR4150 acts as Firepower Threat Defense (FTD) device.
- Cisco FPR4150 device runs FTD version 6.4.0.
- Cisco CGR2010 and Cisco FPR4150 devices required respective licenses to support strong encryption algorithms. Refer to data sheets and ensure the corresponding licenses are activated.

This section assumes that FTD devices are managed by FMC.

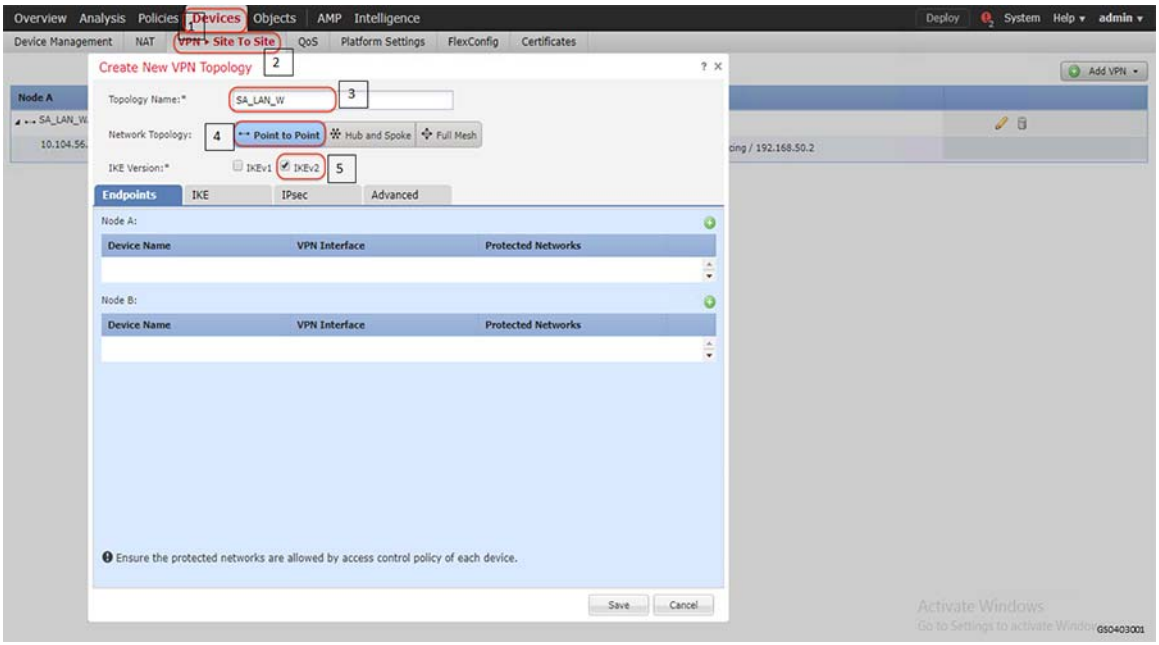
Upgrading FTD devices, setting up FMC and integrating FTD devices with FMC are out of scope for this guide. Refer the corresponding configuration guides.

Note: For details to setup FMC refer the following guide:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64.html

Summary

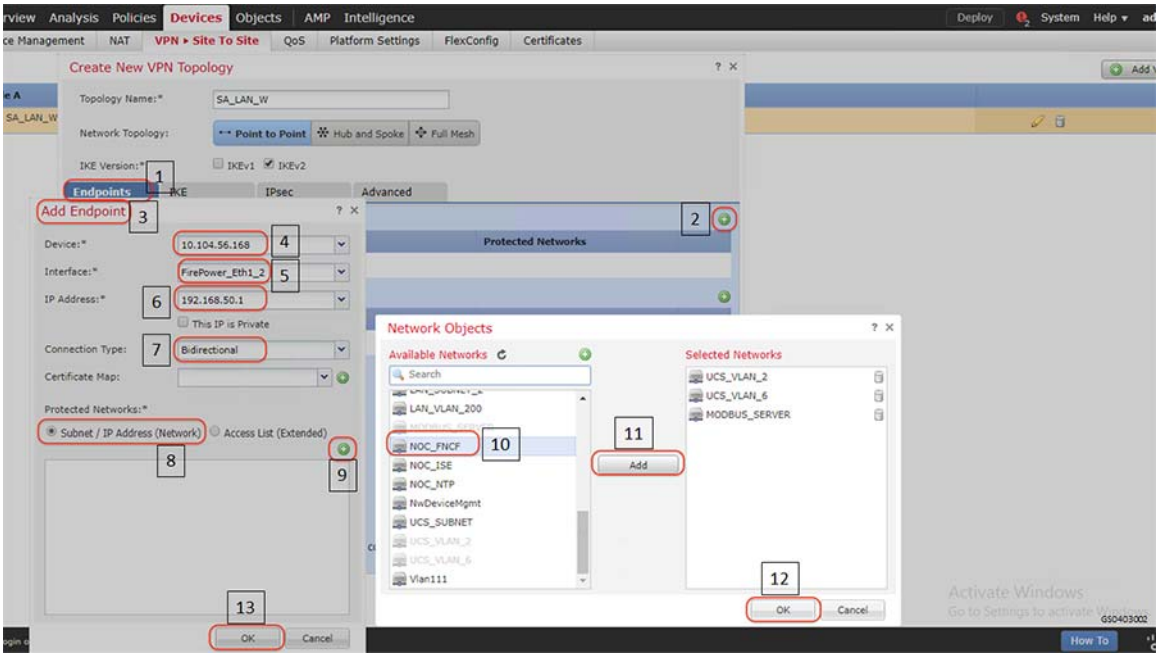
1. Choose **VPN Site to Site** option and the related properties as highlighted in the following figure.

Figure 13 VPN Site to Site configuration



2. Add nodes between which Cisco IPSec Site to Site IPSec VPN tunnel is to be established as highlighted in the following figure. The following figure highlights the steps to be followed for Node A. Repeat the steps for Node B to establish Cisco Site to Site IPSec VPN tunnel between the nodes. Highlights 8 to 13 show the steps to select and permit the networks reachable through the Site to Site IPSec VPN tunnel.

Figure 14 Adding Site to Site VPN nodes



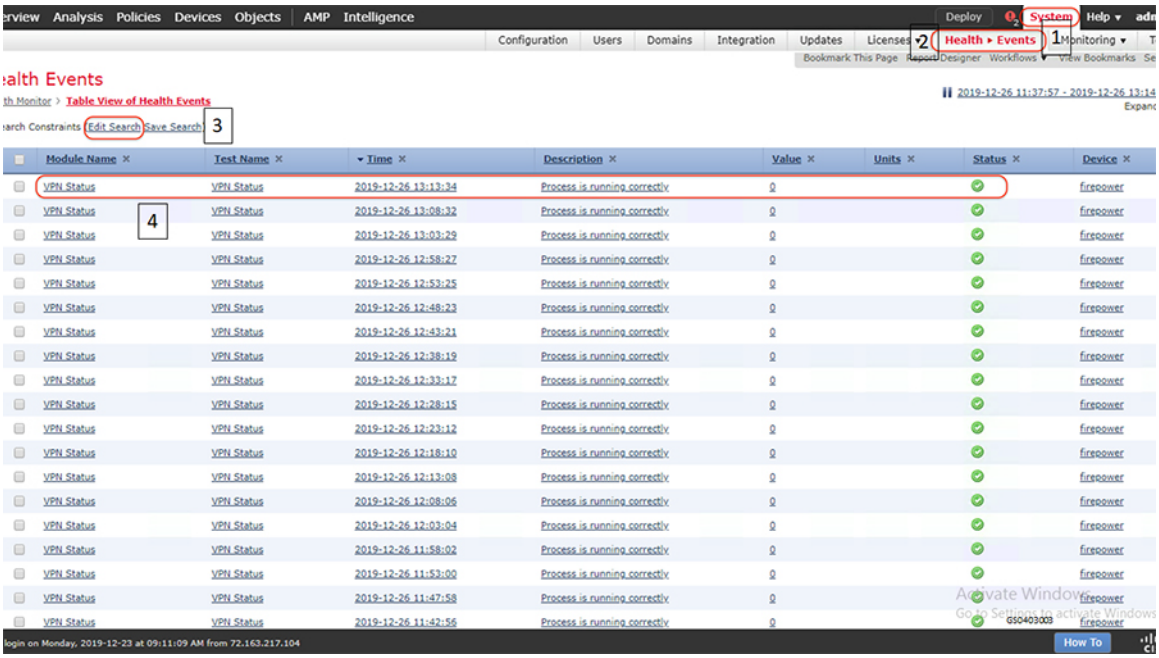
Note: Define the details of the IKE and IPsec transforms. It is critical that the Security parameters match between two peers so that they can successfully negotiate a security association.

Verification

Using GUI

- Select **System > Health > Events > Edit Search** and search for VPN as highlighted in the following figure.

Figure 15 Verifying Site to Site VPN status



Using Command Line Interface

Login to the consoles of the FTD devices and use the following command to check the status of the established Site to Site IPSec VPN tunnel. The command helps to check the status of the tunnel, statistics of encrypted and decrypted packets, the access-list permitting traffic from networks that needs to be encrypted by the Site to Site IPSec VPN tunnel.

```
firepower# show crypto ipsec sa
interface: FirePower_Eth1_2
    Crypto map tag: CSM_FirePower_Eth1_2_map, seq num: 1, local addr: 192.168.50.1
      access-list CSM_IPSEC_ACL_1 extended permit IP 192.168.2.0 255.255.255.0 192.168.21.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.21.0/255.255.255.0/0/0)
      current_peer: 192.168.50.2
      #pkts encaps: 97183, #pkts encrypt: 97183, #pkts digest: 97183
      #pkts decaps: 414798, #pkts decrypt: 414798, #pkts verify: 414798
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 97183, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 192.168.50.1/500, remote crypto endpt.: 192.168.50.2/500
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 872999AB
      current inbound spi : 165598D9
    inbound esp sas:
      spi: 0x165598D9 (374708441)
         SA State: active
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 18, crypto-map: CSM_FirePower_Eth1_2_map
         sa timing: remaining key lifetime (kB/sec): (4234651/10412)
```

```
          IV size: 8 bytes
          replay detection support: Y
          Anti replay bitmap:
           0xFFFFFFFF 0xFFFFFFFF
      outbound esp sas:
        spi: 0x872999AB (2267650475)
          SA State: active
          transform: esp-des esp-sha-hmac no compression
          in use settings ={L2L, Tunnel, IKEv2, }
          slot: 0, conn_id: 18, crypto-map: CSM_FirePower_Eth1_2_map
          sa timing: remaining key lifetime (kB/sec): (4192901/10412)
          IV size: 8 bytes
          replay detection support: Y
          Anti replay bitmap:
           0x00000000 0x00000001
      Crypto map tag: CSM_FirePower_Eth1_2_map, seq num: 1, local addr: 192.168.50.1
        access-list CSM_IPSEC_ACL_1 extended permit IP 192.168.169.0 255.255.255.0 192.168.200.0
255.255.255.0
        local ident (addr/mask/prot/port): (192.168.169.0/255.255.255.0/0/0)
        remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
        current_peer: 192.168.50.2
        #pkts encaps: 360403, #pkts encrypt: 360403, #pkts digest: 360403
        #pkts decaps: 445029, #pkts decrypt: 445029, #pkts verify: 445029
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 360403, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
        #TFC rcvd: 0, #TFC sent: 0
        #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
        #send errors: 0, #recv errors: 0
        local crypto endpt.: 192.168.50.1/500, remote crypto endpt.: 192.168.50.2/500
        path mtu 1500, ipsec overhead 58(36), media mtu 1500
        PMTU time remaining (sec): 0, DF policy: copy-df
        ICMP error validation: disabled, TFC packets: disabled
        current outbound spi: 105ED6B9
        current inbound spi : 588F2559
      inbound esp sas:
        spi: 0x588F2559 (1485776217)
          SA State: active
          transform: esp-des esp-sha-hmac no compression
          in use settings ={L2L, Tunnel, IKEv2, }
          slot: 0, conn_id: 18, crypto-map: CSM_FirePower_Eth1_2_map
          sa timing: remaining key lifetime (kB/sec): (3950895/11183)
          IV size: 8 bytes
          replay detection support: Y
          Anti replay bitmap:
           0xFFFFFFFF 0xFFFFFFFF
      outbound esp sas:
        spi: 0x105ED6B9 (274650809)
          SA State: active
          transform: esp-des esp-sha-hmac no compression
          in use settings ={L2L, Tunnel, IKEv2, }
          slot: 0, conn_id: 18, crypto-map: CSM_FirePower_Eth1_2_map
          sa timing: remaining key lifetime (kB/sec): (4006746/11183)
          IV size: 8 bytes
          replay detection support: Y
          Anti replay bitmap:
           0x00000000 0x00000001
firepower#
```

Recommended Practices

https://tools.cisco.com/security/center/resources/next_generation_cryptography#1

Site to Site VPN in Distribution Automation

FlexVPN is a flexible and scalable VPN solution based on IPSec and IKEv2. To secure DA data communication with the headend across the WAN, FlexVPN is recommended. The IoT FND establishes FlexVPN tunnels between the HERs and the DA Gateways as a part of the ZTD process.

FlexVPN, which integrates various topologies and VPN functions under one framework, simplifies the deployment of VPNs by providing a unified VPN framework that is compatible with legacy VPN technologies.

FlexVPN has some of the following benefits:

- Allows use of a single tunnel for both IPv4 and IPv6, when the medium supports it
- Supports NAT/PAT traversal
- Supports QoS in both directions: hub-to-spoke and spoke-to-hub
- Supports Virtual Routing and Forwarding (VRF)
- Reduces control plane traffic for costly links with support for tuning of parameters

Note: In this solution, IPSec is configured in the tunnel mode.

- KEv2 has fewer round trips in a negotiation than IKEv1: two round trips versus five for IKEv1 for a basic exchange
- Built-in dead peer detection (DPD)
- Built-in configuration payload and user authentication mode
- Built-in NAT traversal (NAT-T). IKEv2 uses ports 500 and 4500 for NAT-T
- Improved re-keying and collision handling
- A single Security Association (SA) can protect multiple subnets, which improves scalability. Support for Multi-SA Dynamic Virtual Tunnel Interfaces (DVTI) support on the hub.
- Asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different pre-shared keys, different certificates, or on one side a key and the other side a certificate.

In the FlexVPN model, the HER acts as the FlexVPN hub and the DA Gateways act as the FlexVPN spokes. The tunnel interfaces on the DA Gateways acquire their IP addresses from address pools configured during ZTD. These addresses only have local significance between the HER and the DA Gateways. Since the DA Gateway's tunnel addresses are both dynamic and private to the HER, NMS must address the DA Gateways by their loopback interface in this network architecture. Conversely, the DA Gateway sources its traffic using its loopback interface.

Before the FlexVPN tunnel is established, the DA Gateway can only communicate to the HER in the headend network. This is done over the WAN backhaul via a low priority default route. During FlexVPN handshake, route information is exchanged between the HER and the DA Gateway. The DA Gateway learns the headend routes (IPv4 and IPv6) through FlexVPN.

For details of implementation refer the following guide.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG/DA-SS-IG-doc.html#21265

Access Control

Access Control is one of the fundamental concepts of security in ICT networks. It is a method to limit access to the networks or resources or information for different users or devices. Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.

Different access control models are used based on the compliance and security requirements. For Utilities, NERC-CIP lists the following:

- Logical access control – Role based access control based on the user and the type of role for the user.
- Physical access control – Physical security in the form of cameras, badge readers and so on.
- Port Security – restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

This implementation guide focuses on logical access control model for different users and devices. To support the use cases and configuration shown in this document, Microsoft Windows 2012 R2 is configured as an Active Directory Domain Controller. Cisco ISE integrates with Active Directory (AD) as an Identity Source, which can provide user authentication and group membership. Cisco ISE also integrates with Cyber Vision Center as an Identity Source to collect grid device properties.

The following section lists various steps involved in implementation as validated in the lab.

Access control for different users

To perform the following task, you must be a Super Admin or Policy Admin.

1. Integrate ISE and Active Directory. The detailed configuration of Microsoft Active Directory and integrating with ISE is beyond the scope of this document.
2. ISE uses the concept of Network Device Groups to separate devices based on their type. Add individual devices like Cisco Industrial Ethernet switches to ISE and assign them to the applicable Network Device Group.
3. Configure the following on network devices that interacts with ISE for Authentication and Authorization.

```
!
aaa new-model
!
aaa group server radius ISE
 server-private 192.168.2.202 key sdu@123
 IP radius source-interface Vlan111
!
aaa group server radius AAASERVER
 server name CISCOISE
!
aaa authentication dot1x default group radius
aaa authorization network default group AAASERVER
aaa authorization network SGLIST group radius
aaa authorization auth-proxy default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
!
aaa server radius policy-device
 key sdu@123
!
aaa server radius dynamic-author
 client 192.168.2.202 server-key sdu@123
 server-key sdu@123
!
aaa session-id common
!
ip radius source-interface Vlan111
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 CISCOISE
 address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
 pac key sdu@123
!
```

4. Configure different policy elements like Dictionaries, Conditions and Results so as to build the policies that will provide the main functionality for ISE. Existing Dictionaries can be used for many of the scenarios involved in Grid Security Solution. Conditions can either be Simple or Compound. An example of a Simple condition would be to identify network devices by which zone they reside in within the Substation (ESP, Corporate Substation, or CIP/Multiservice).

5. Configure Authentication policy on ISE. The Utility network may support many types of authentication, however the primary methods validated in this document is 802.1X and MAB for wired connections. To add this method to the policy, go to **Policy > Policy Elements > Results > Authentication > Allow Protocols**.

6. Configure Authorization policy on ISE. The result of the ISE authorization policy is for a user or device to be granted (or denied) permission to access to some network resource. The Authorization Profile (accessed from **Policy > Policy Elements > Results > Authorization > Authorization Profiles**) is the construct used to define these end results which are ultimately pushed down to the Network Access Device which will enforce the policy.

7. For the purpose of validation, an Authorization Profile is applied for users in the "Administrator" Active Directory group that access the network through devices in the ESP zone. This profile applies network access control by using a downloadable access control list (DACL) that is dynamically pushed down to the IE switch.

For detailed steps with various capabilities refer to the following guide:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_010010.html

Verification

```
HSR-001#test aaa group AAASERVER administrator@substationLAN.cisco.com Sdu@123$
User successfully authenticated

USER ATTRIBUTES

username              0   "administrator@substationLAN.cisco.com"
CiscoSecure-Defined-  0   "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3"
HSR-001#
```

Port Security for different devices

To protect the Utility Network from being exploited, unused ports of all LAN switches or routers at the substation must be shut down by default as defined in NERC-CIP. In-use ports must be explicitly enabled. For those ports that are enabled, port security should be configured to protect the network from LAN-based attacks. This feature limits the number of MAC addresses that can connect to a switch or router and ensures that only approved MAC addresses are able to access the switch or router. Port security prevents MAC address flooding and ensures that only approved users can log onto the network. Allowed MAC addresses can either be statically configured or dynamically learned.

The following security policy applies to port security configuration:

- The maximum number of secure MAC address for a port is one (1).
- For IED or other IP-enabled control devices, specify a static MAC address.
- In case IED MAC is unknown in certain deployment scenarios, specify sticky port security.
- For onsite engineer/technician device access in the substation, only authenticated users are permitted access via the designated user access port (802.1x).

In this example, the GigabitEthernet1/11 interface is configured with port-security. The port will listen for the first MAC address that tries to communicate on the port. The switch will dynamically learn this address and start permitting it t0 communicate. The “sticky” configuration allows the dynamically learned address to be saved to the configuration so that it will survive a reload of the switch; otherwise dynamically learned addresses will be forgotten. By default, the switch will only allow a single secure MAC address on an interface. The violation command configures the action to take if an un configured MAC address tries to communicate on the port. In this case, “restrict” is configured so that frames from unknown MACs will be dropped and SYSLOG message and SNMP trap are generated.

```
interface GigabitEthernet1/1
 description Test_MAB
 switchport access vlan 111
 switchport mode access
 switchport port-security violation protect
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00bf.772c.4741
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast edge
end
```

This is very useful because the switch can be configured to allow secure devices (such as RTUs, IEDs, etc.) to connect. However, if a malicious person unplugs a secure device and tries to connect another device, it will immediately be denied access to the network. The log message below shows a violation when an unknown MAC tries to connect:

```
Aug 20 19:36:11.557: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 00bf.772c.4741 on port GigabitEthernet1/1
```

Grid Visibility

As discussed previously in this document, one of the important NERC-CIP requirements is to identify and categorize Cyber system assets. This requirement can be met with the Cisco Cyber Vision Center and Cyber Vision sensor.

The Cisco Cyber Vision solution is based on a 2-tier architecture made of inline network sensors namely Cisco IE3400 and Cisco IR1101, as well as a dedicated hardware sensor like Cisco IC3000. These sensors are dedicated to capture network traffic using various SPAN features, decode SCADA protocols as listed in the following table along with other supported IT protocols using the Cisco Deep Packet Inspection engine and send meaningful information to the Cisco Cyber Vision Center for passive monitoring. Support for visibility of legacy protocols is restricted to Cisco IR1101 as Cyber Vision Network sensor.

Table 5 SCADA Protocols supported by Cisco Cyber Vision

Protocols	Communication Type
MODBUS	TCP/IP
DNP3	■ TCP/IP ■ Serial over TCP Raw Socket (Enabled on Cisco IR1101)
T104	TCP/IP

Protocols	Communication Type
T101 to T104 (Enabled by SCADA Protocol Translation on Cisco IR1101)	T101/Serial to T104/IP
IEC 61850 MMS	TCP/IP
IEC 61850 GOOSE	Ethernet

Cisco Cyber Vision also enables visibility to the type of devices or components that are part of the network, the flows they generate. For e.g., the flow could be that of between a SCADA front end processor and its client like control commands, poll, and so on. The details of the device could be that of the type of the device like PLC or SCADA station or PC as appropriate, properties of the device like IP Address, Operating System, Manufacturer, etc. as can be derived from the flows or communication generated by the devices in the network. The figure highlights some of the details that could be deduced with the use of Cisco Cyber Vision. The Cisco Cyber Vision Center, a central platform gathers data from all the Edge Sensors across the network and acts as the monitoring, detection and management platform for the solution.

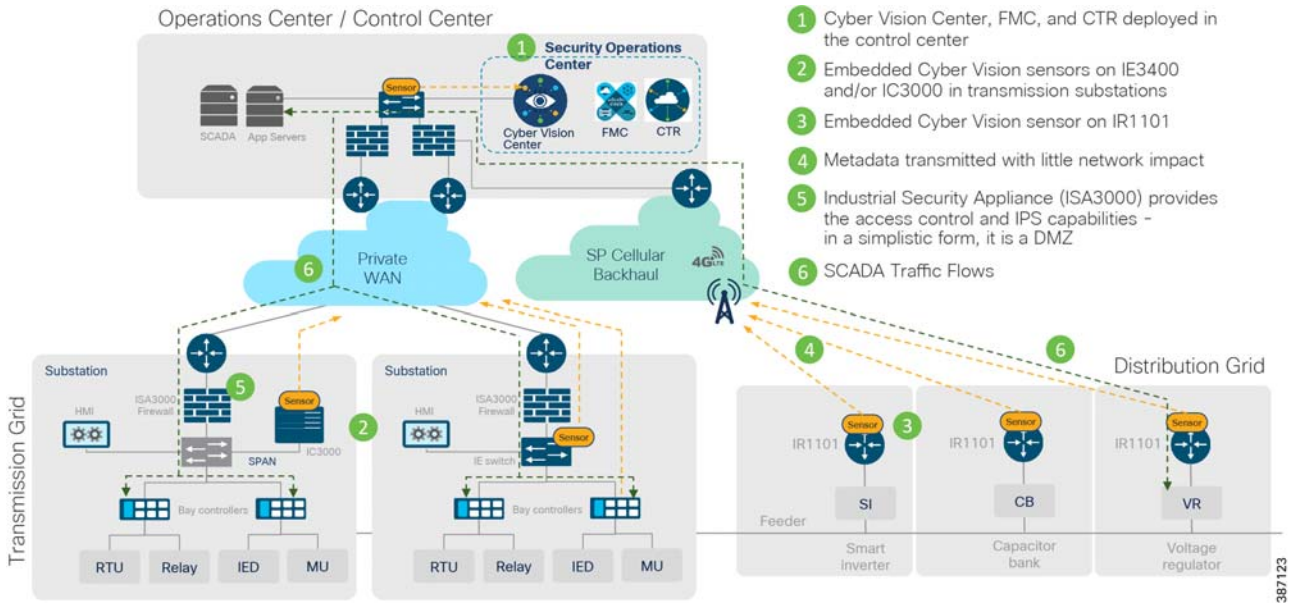
To operate, the Center relies on two separate networks, respectively connected to the following interfaces:

- The Administration network interface, which gives access to the user interface.
- The Collection network interface, which connects the Center to the sensors.

The Cisco Cyber Vision solution success depends on effectively capturing the traffic. Where to capture the traffic in a network is critical.

The following figure highlights the different sensors and traffic flow in the network that gets captured by the sensor and sent to the Center.

Figure 16 Grid Visibility Center and Sensors



Sensors in Substation LAN

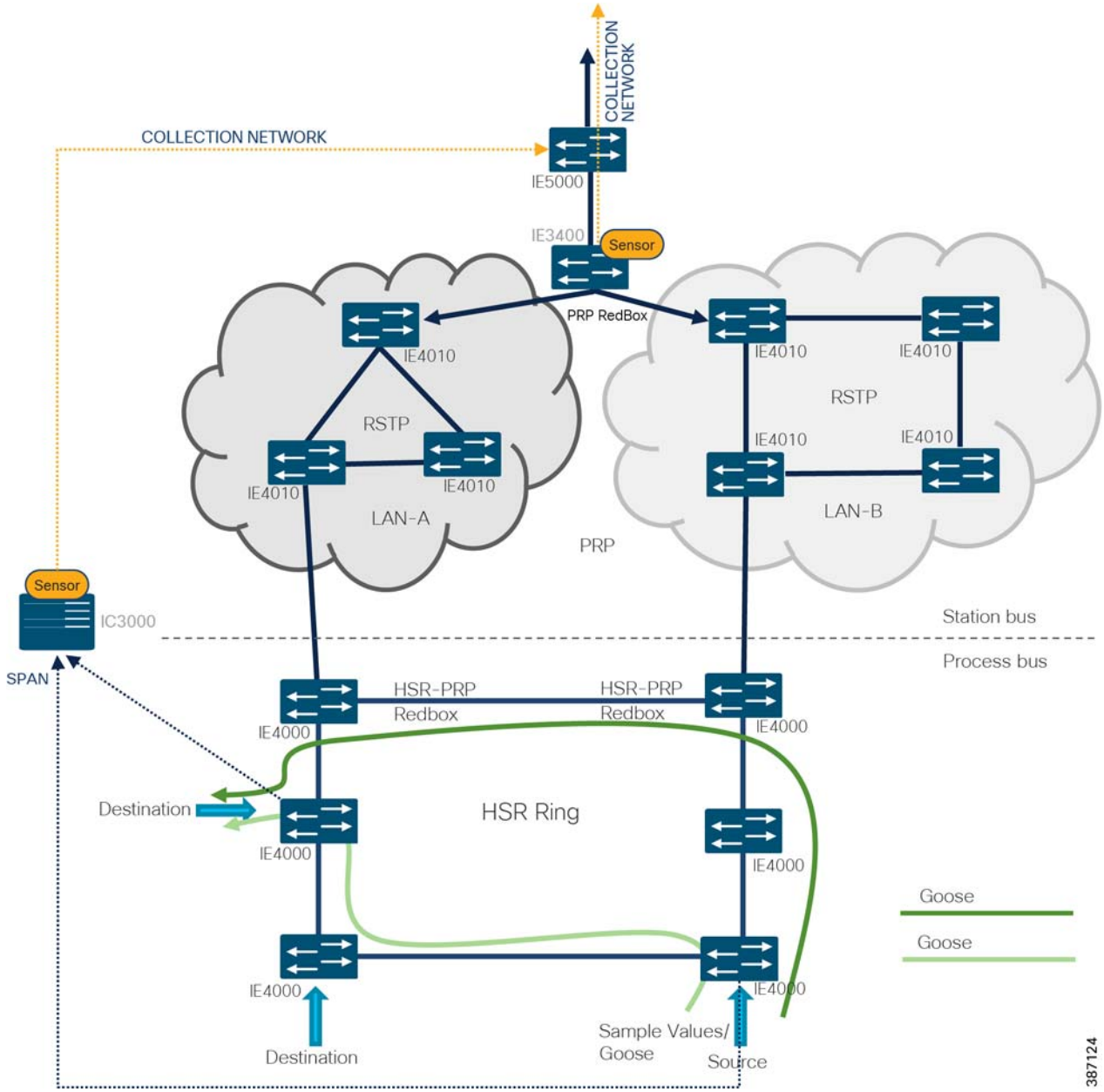
IC3000

Positioning IC3000 as Sensor

In addition to a management port, the IC3000 contains 4 independent data capture ports (two RJ45 copper ports and two SFP fiber ports) operating in SPAN mode, each of which can be connected to an on-site switch. The IC3000 data capture ports should be connected to switches with SPAN configured. This section explains the positioning of IC3000 as hardware sensor to capture traffic flowing in an HSR ring.

As per the following topology one of the ports of IC3000 positioned as Hardware sensor connects to IE4000 switches as required in the HSR ring and processes east-west traffic communication in the network while the IE3400 positioned as Network sensor processes north-south communication in the network. The copper ports of IC3000, **int1** or **int2,** are used to connect to these switches with SPAN configured to mirror the respective source and destination port traffic for inspection by the sensor application hosted on the IC3000 and forward the metadata to CVC for further processing.

Figure 17 IC3000 Positioning



After the sensor application on IC3000 gets registered to CVC, traffic starts to appear in CVC provided the SPAN ports of IC3000 are properly connected to those network switches having SPAN configured. Below section shows the sample switch configuration on IE4000 needed to inter-connect the IC3000 hosting sensor application with a SCADA system (Front End Processor or Controller or SCADA Outstation or IED) and thereafter enabling SPAN so that the sensor can process the incoming SCADA system traffic and report it to CVC.

```
IE4000#show run int fa1/5
!
interface FastEthernet1/5
description connected to SCADA Master system switchport mode trunk
switchport trunk allowed vlan 1,100
end

IE4000#show run int Gi1/2
```

```
!
interface GigabitEthernet1/2
description connected to IC3000 int1 port for span traffic switchport mode trunk
switchport trunk allowed vlan 1,100
end

!! SPAN configuration shown below!!
IE4000#show run | s monitor session
!
monitor session 1 source interface Fa1/5
monitor session 1 destination interface Gi1/2
! IE4000#
```

Note: While the recommendation is to use SPAN configuration on the IE switches to forward a copy of the network traffic to the Cyber Vision Sensor, it is important to note that currently RSPAN is not supported over an HSR ring network due to the DDTS CSCvr81772.

Configuring IC3000 as Hardware Sensor

This section focuses on the components listed below discussing the interactions between the Cisco Cyber Vision Sensor application hosted on the IC3000 and the Cisco Cyber Vision Center used for managing the sensor application in order to provide Grid visibility.

- Cisco IC3000 Industrial Compute Gateway
- Cisco Cyber Vision Sensor (CVS) application
- Cisco Cyber Vision Center (CVC)

The IC3000 Industrial Compute Gateway (IC3000) is an edge computing platform which extends the cloud computing paradigm to the edge of the network. It comes as a mid-range, low-power, fanless, edge server ruggedized for Industrial Applications powered by a 4 core 1.2GHz Intel Rangeley CPU with 8 GB of 1333MHz DDR3 memory, and a 100GB mSATA drive (internal). For connectivity purpose it supports 2x1GbE SFP and 2x10/100/1000Base-T with a management port.

For more details about the product, please refer to the link below:

https://www.cisco.com/c/en/us/support/routers/3000-series-industrial-compute-gateways/tsd-products-support-series-home.html

The IC3000 can be ordered with the Cisco Cyber Vision sensor application, which comes pre-installed by manufacturing. The Cisco Cyber Vision sensor application allows traffic from the network to be captured in offline or online mode. This captured data can be viewed from Cisco Cyber Vision Center.

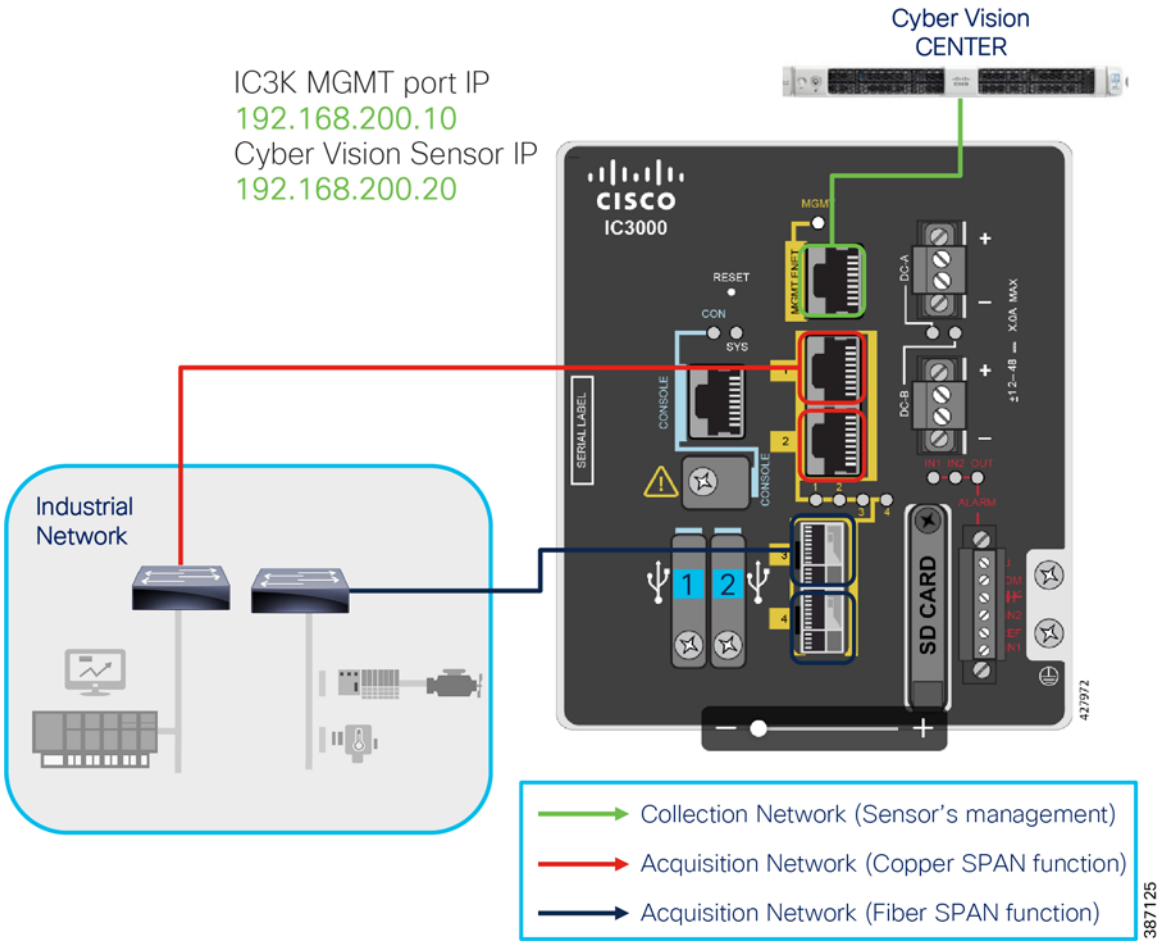
IC3000 using Online Mode

This guide focuses on the online mode of operation of Cisco Cyber Vision Sensor. As a pre-requisite it is recommended to have the Cisco Cyber Vision Center installed and running first. For details on setting up the CVC, please refer to the Cisco Cyber Vision Center quick start guides at the link below.

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Quickstart_Guide_Release_3_0_0.pdf

Figure 18 illustrates the IC3000 based hardware sensor's collection network and the available SPAN interfaces on the platform.

Figure 18 Cisco IC3000 based hardware sensor



As shown in the figure above, the IC3000 management port is connected to the collection network from where CVC is reachable. Whereas the copper SPAN ports are plugged into the switches with SPAN pre-configured to mirror the network traffic for inspection by the sensor hosted on the IC3000. This section focuses on the manual deployment of sensor onto the IC3000 platform using a USB device. In a later section, the CVC extension feature is used for deploying the sensor onto IC3000 platform.

The following IP address schema has been used in this guide to bring up the CVS application on IC3k and integrate it to the CVC.

CVC

- Admin Interface (eth0): 192.168.3.113
- Collection interface (eth1): 192.168.169.1
- Collection network gateway: 192.168.169.100
- NTP: 192.168.169.108

IC3000

- Host Mgmt. IP address: 192.168.200.10
- Host Mgmt. netmask: 255.255.255.0

- Host Mgmt. gateway: 192.168.200.100

CVS

- Sensor IP address: 192.168.200.20

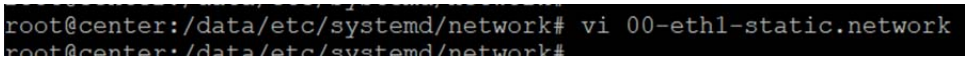
To bring up the IC3000 with sensor application (CVS) in online mode and have it registered with the CVC, please refer to the section “Cyber Vision Sensor Application in Online Mode” inside the Cisco Cyber Vision Sensor deployment guide using the link:

https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/DeploymentGuide-Cyber.html

Note that the process documented in the deployment guide above works fine when the CVC collection network and IC3000, sensor application management IP addresses are in same subnet. However, if they are in different subnets as shown in the IP schema above, then additionally a persistent static route needs to be added on the CVC as shown below to ensure reachability between CVC and the sensor application.

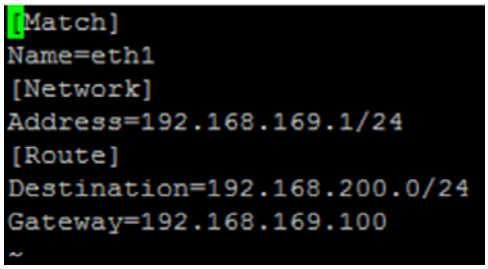
1. To do this login to the CVC console by connecting to the admin interface using ssh.
2. Navigate to the /data/etc/systemd/network/ directory and edit the **00-eth1-static.network** file to add a static route as shown below.

Figure 19 Network file to add a static route



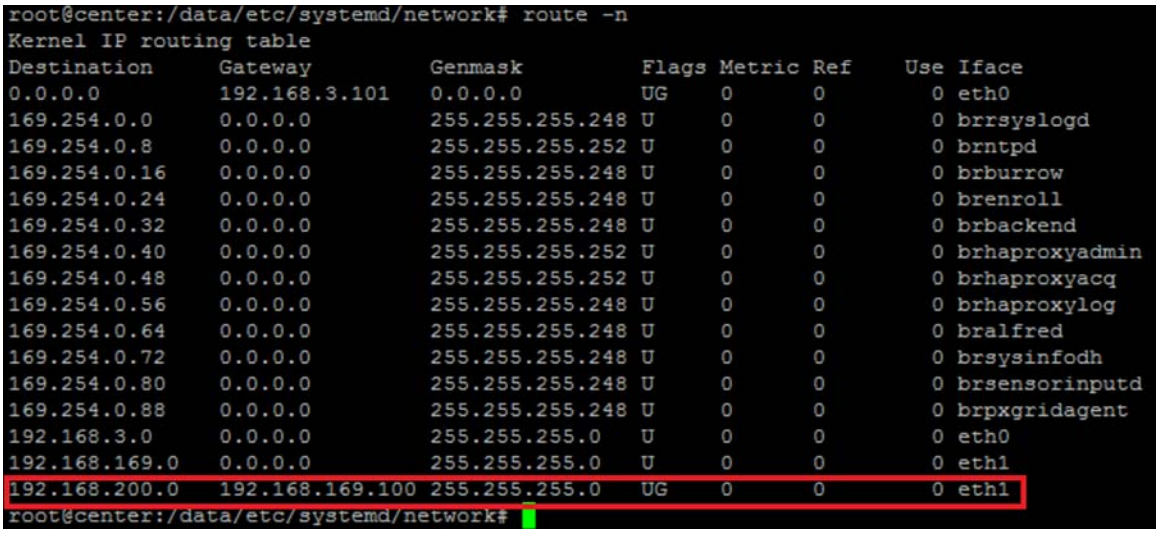
In this guide, the destination and gateway entries below have been used for the route entries.

Figure 20 Static route entry added



3. Reboot the system by issuing a reboot command on the cli.
4. After reboot, check the routing table to verify that the sensor subnet could be reached by the CVC collection interface (eth1).

Figure 21 CVC routing table



```
root@center:/data/etc/systemd/network# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.3.101   0.0.0.0         UG    0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.255.248 U     0      0        0 brrsyslogd
169.254.0.8     0.0.0.0         255.255.255.252 U     0      0        0 brntpd
169.254.0.16    0.0.0.0         255.255.255.248 U     0      0        0 brburrow
169.254.0.24    0.0.0.0         255.255.255.248 U     0      0        0 brenroll
169.254.0.32    0.0.0.0         255.255.255.248 U     0      0        0 brbackend
169.254.0.40    0.0.0.0         255.255.255.252 U     0      0        0 brhaproxyadmin
169.254.0.48    0.0.0.0         255.255.255.252 U     0      0        0 brhaproxyacq
169.254.0.56    0.0.0.0         255.255.255.248 U     0      0        0 brhaproxylog
169.254.0.64    0.0.0.0         255.255.255.248 U     0      0        0 bralfred
169.254.0.72    0.0.0.0         255.255.255.248 U     0      0        0 brsysinfodh
169.254.0.80    0.0.0.0         255.255.255.248 U     0      0        0 brsensorinputd
169.254.0.88    0.0.0.0         255.255.255.248 U     0      0        0 brpxgridagent
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.169.0   0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.200.0   192.168.169.100 255.255.255.0   UG    0      0        0 eth1
root@center:/data/etc/systemd/network#
```

To connect to the IC3000 via the console port, refer to the section “Unboxing, Installing and Connecting to the IC3000 Device” in the Cisco IC3000 Industrial Compute Gateway Deployment Guide using the link below:

https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/DeploymentGuide.html

The IC3000 is shipped with a factory installed image. Once the device is properly connected and powered up, the **ic3k>** prompt is visible. The version installed can be verified by running the show version command via the console.

For example:

```
ic3k>show version
Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2235V0SW
ic3k>
```

Similarly, the IP address obtained by IC3000 can be verified by running the show interfaces command and looking for the svcbr_0 interface details.

For example:

```
ic3k>show interfaces
< sample output omitted for convenience>
svcbr_0   Link encap:Ethernet  HWaddr d0:ec:35:ca:9e:20
          inet addr:192.168.200.10  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::d2ec:35ff:feca:9e20/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4021792 errors:0 dropped:3985245 overruns:0 frame:0
          TX packets:9689 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:357976072 (341.3 MiB)  TX bytes:11428207 (10.8 MiB)
```

Verify the reachability between IC3000 and CVC with a ping command from IC3000 as shown below:

```
ic3k>ping 192.168.169.1
PING 192.168.169.1 (192.168.169.1) 56(84) bytes of data.
64 bytes from 192.168.169.1: icmp_seq=1 ttl=64 time=1.79 ms
64 bytes from 192.168.169.1: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 192.168.169.1: icmp_seq=3 ttl=64 time=1.42 ms
64 bytes from 192.168.169.1: icmp_seq=4 ttl=64 time=1.40 ms
64 bytes from 192.168.169.1: icmp_seq=5 ttl=64 time=1.46 ms
```

```
--- 192.168.169.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.406/1.506/1.798/0.149 ms
ic3k>
```

IC3000 using CVC Extension

The previous section provided details deploying the sensor application on the IC3000 using the provisioning package. The package is downloaded from CVC to a USB device which is later inserted into the IC3000 hardware. With the latest CVC version, there is another cleaner and easier way to deploy the sensor application on the IC3000 hardware sensor (and even on other network-based sensor platforms like IE3400, IR1101) via the CVC Extension feature.

Note: The extension is not included in the center update and must be manually imported to the CVC under the **Admin -> Extensions** tab before using it for sensors deployment. The prerequisite for sensor deployment using the extension is that the IC3000 must be pre-configured with an IP address that is reachable from the Center. Refer to the Cisco IC3000 Industrial Compute Gateway Deployment guide here:

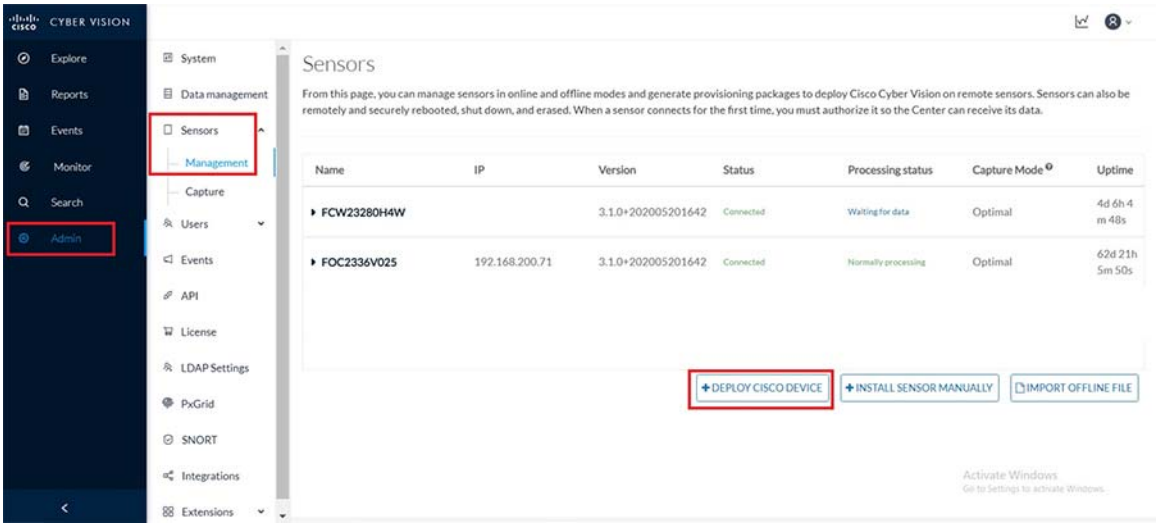
https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/b_IC3000_deployment_guide.html

Focus on the section Remote Device Management in the document linked below, which describes managing the device remotely over a non-link local address depending on the network topology.

https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/b_IC3000_deployment_guide/b_IC3000_deployment_guide_chapter_011.html#task_1076567

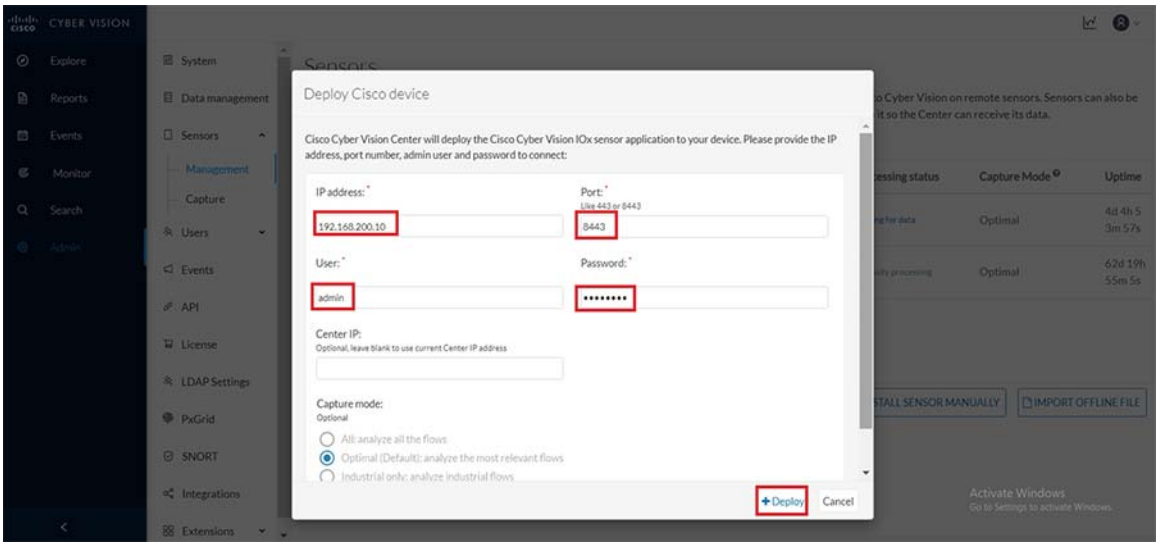
Once this is in place, deploying the sensor application onto IC3000 from the CVC is straight-forward. Login to the CVC web GUI and navigate to Admin tab on the left and click on **Sensors -> Management -> Deploy Cisco device** as shown below.

Figure 22 CVC Sensors management



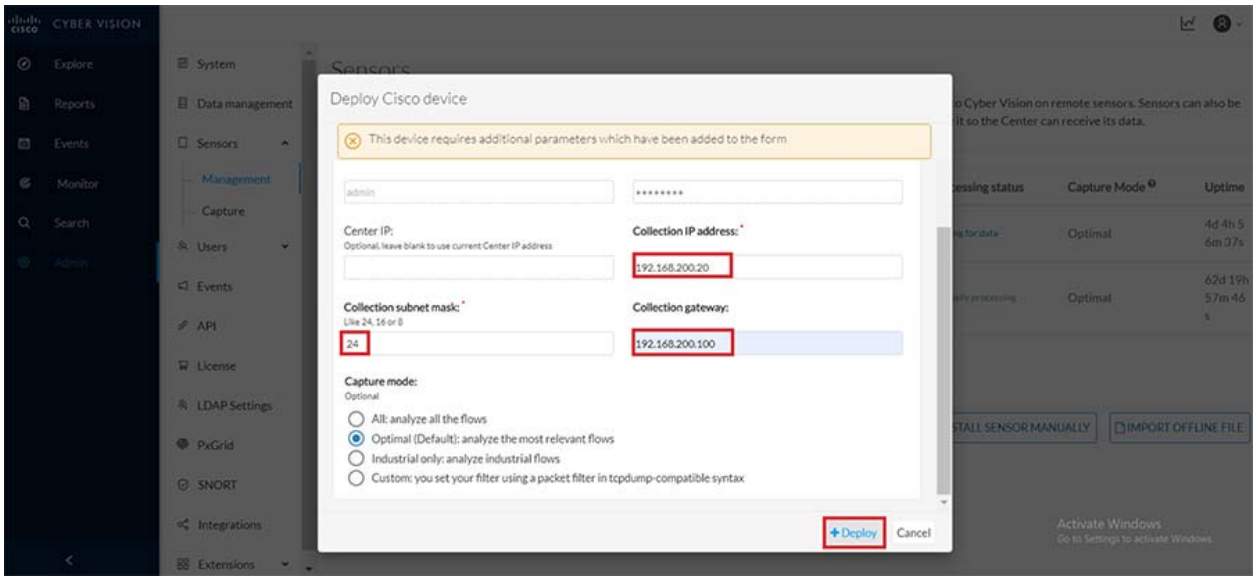
As a next step, fill in the details about the IC3000 like ip address, port number, username and password and then click on **Deploy** as shown below.

Figure 23 Deploy Cisco Device – IC3000



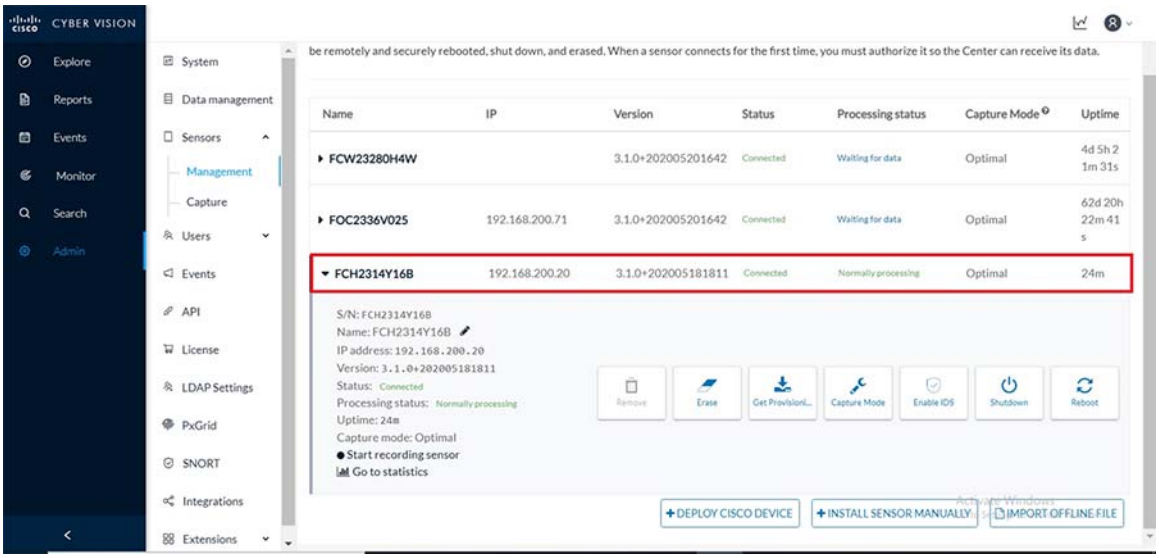
At this point if the reachability between CVC and IC3000 is intact, additional parameters would be requested about the sensor application being deployed onto IC3000 as shown below. Fill in these details like the address, subnet mask and the gateway address for the sensor and click on the **Deploy** button as shown below.

Figure 24 Sensor deployment on IC3000



After successful deployment the sensor shows in the list of managed sensors in the CVC as shown below.

Figure 25 Managed sensors in CVC



IE3400

Positioning IE3400 as Sensor

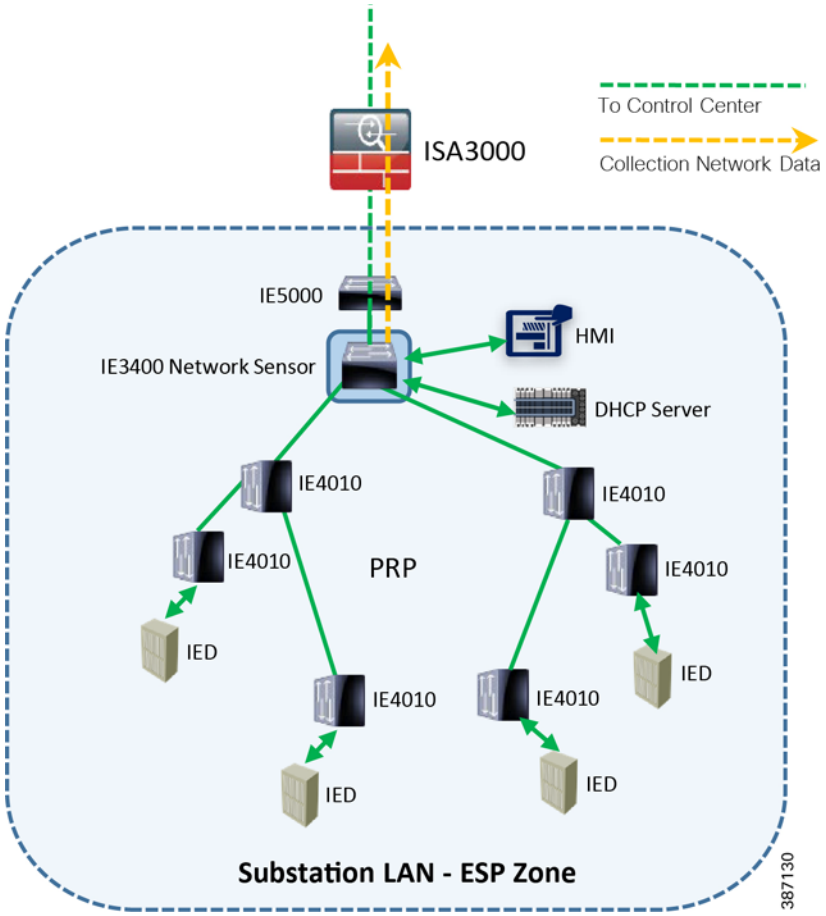
Figure 7 shows the overall Grid Security solution topology where IE3400 is located inside the Substation LAN – ESP zone within the Transmission substation. The following figure gives a closer look of IE3400 positioning within ESP zone in the overall Grid Security solution topology. Here IE3400 is positioned as a Parallel Redundancy Protocol (PRP) node. PRP is used to provide hitless redundancy (zero recovery time after failures) in Ethernet networks and comprises a scheme where the end nodes implement redundancy (instead of network elements connected in mesh or ring topologies using protocols like RSTP, REP, or MRP) by connecting two network interfaces to two independent, disjointed, parallel networks. Such end nodes are referred to as Dually attached nodes (DANs) and each of them have redundant paths to all other DANs in the network.

The DAN sends two packets simultaneously through its two network interfaces to the destination node. A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help the destination node distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet. If the second packet arrives successfully, it is discarded. If a failure occurs in one of the paths, traffic continues to flow over the other path uninterrupted, and zero recovery time is required.

A Redundancy Box (RedBox) is used when an end node that does not have two network ports and does not implement PRP needs to implement redundancy. Such an end node can connect to a RedBox, which provides connectivity to the two different networks on behalf of the device.

In this solution, IE3400 switch implements PRP Redbox functionality using Gigabit Ethernet port connections to each of the two LANs. PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN_A. The higher numbered port is the secondary port and connects to LAN_B. The PRP channel remains up as long as at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down.

Figure 26 Cisco IE3400 sensor IOx Application Interface Mapping



As shown in Figure 26, the IE3400 is connected to a single IE5000 switch using one of its Gigabit ethernet ports (Gi 1/8) configured as a trunk. The other side is connected to two adjacent IE4010 aggregation type switches via a Gigabit ethernet port each (Gi 1/1 & Gi 1/2). These two ports together are configured as a PRP channel link. Figure 40 shows this configuration.

```
IE3400-GS-PRP#show run int Gi1/8
!
interface GigabitEthernet1/8
 description provide connectivity via vlan200 to cvc subnet
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
end
!
IE3400-GS-PRP#show run int PRP-channel1
!
interface PRP-channel1
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
end
!
IE3400-GS-PRP#show run int Gi1/1
!
interface GigabitEthernet1/1
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
```

```
 prp-channel-group 1
!
IE3400-GS-PRP#show run int Gi 1/2
!
interface GigabitEthernet1/2
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 prp-channel-group 1
!
```

Notice the remote-span VLAN 2508 on IE3400 configured previously during sensor application install being excluded from all the trunk ports that are permitted to carry all other VLAN traffic flowing in the network. The necessary SPAN configuration needed for traffic to be mirrored to the sensor application on the IE 3400 is shown below:

```
IE3400-GS-PRP#show run | s monitor
monitor session 1 source interface Gi1/8
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
IE3400-GS-PRP#
```

After the PRP configuration is in place on the IE3400, any SCADA Controller or Front End Processor can then connect to the IE5000 switch. This switch is placed on top of the IE3400 and communicates through this IE3400. It acts as a PRP Redbox providing two redundant paths to the SCADA Outstation (IED) connected to the lowest IE4010 switches within the Substation LAN.

Note: The complete configuration for the IE5000 and the IE4010 switch connected to PRP Redbox switch (IE3400) has been provided in the Appendix B and C for reference.

PRP:

https://www.cisco.com/c/en/us/td/docs/switches/lan/industrial/software/configuration/guide/b_prp_ie4k_5k.html#id_42563

Note: The complete configuration of IE3400 has been provided in the Appendix A for reference.

Configuring IE3400 as Network Sensor

This section focuses on the components listed below discussing the interactions between the Cisco Cyber Vision Sensor application hosted on the IE3400 and the Cisco Cyber Vision Center used for managing the sensor application in order to provide Grid visibility.

- Cisco Catalyst IE3400 Rugged Switch
- Cisco Cyber Vision Sensor (CVS) application
- Cisco Cyber Vision Center (CVC)

The Cisco Catalyst IE3400 Rugged Series switches deliver advanced, high-speed Gigabit Ethernet connectivity in a compact form factor, and are designed for a wide range of industrial applications where hardened products are required. These switches extend intent-based networking to the IoT edge of the network. The modular design of the Cisco Catalyst IE3400 Rugged Series offers the flexibility to expand up to 26 ports of Gigabit Ethernet with a range of expansion module options.

The IE3400 Series runs Cisco IOS® XE, a next-generation operating system with built-in security and trust and can be managed with powerful management tools such as Cisco DNA Center and Industrial Network Director, and can be easily set up with a completely redesigned, user-friendly, modern GUI tool called WebUI.

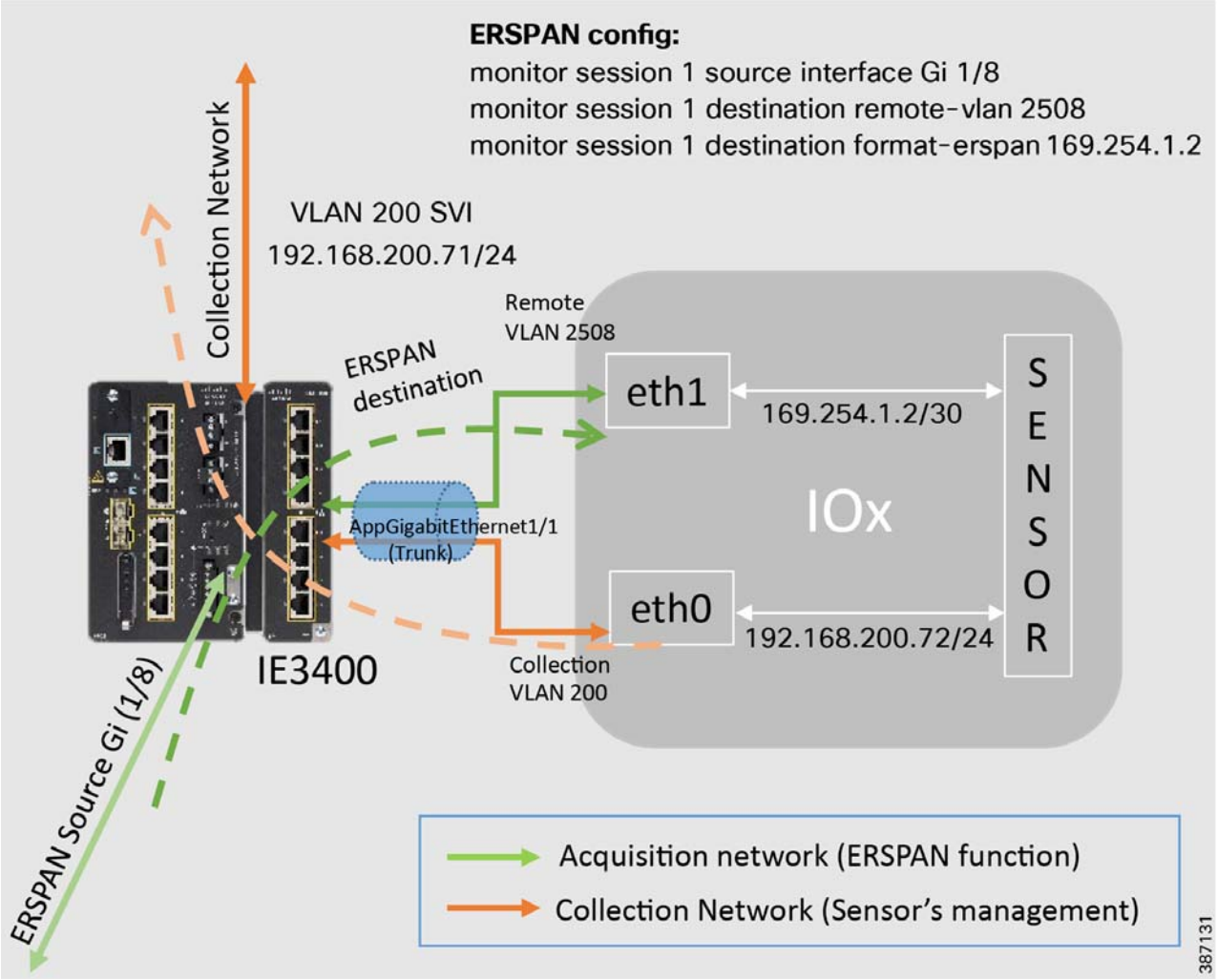
For more details about the product, please refer to the link below:

https://www.cisco.com/c/en/us/products/switches/catalyst-ie3400-rugged-series/index.html

This guide describes how to perform a clean installation of the sensor application (CVS) on an IE3400 switch. As a pre-requisite it is recommended to have the Cisco Cyber Vision Center installed and running.

The figure below illustrates the IE3400 sensor collection network, SPAN interfaces, ERSPAN configurations as applicable.

Figure 27 Cisco IE3400 network sensor IOx Application Interface Mapping



As shown in Figure 27, the network traffic traversing one of the physical ports on IE3400 (configured as ERSPAN source) is mirrored to the IOx based sensor which listens on port eth1. The sensor communicates to the CVC by connecting to the collection network using its eth0 port and also sends metadata of the inspected traffic to CVC for further processing.

The following IP address schema is used to bring up the CVS application on IE3400 and integrate it to the CVC.

CVC

- Admin Interface (eth0): 192.168.3.113
- Collection interface (eth1): 192.168.169.1
- Collection network gateway:
- 192.168.169.100

- NTP: 192.168.169.108

IE3400

- Admin IP address: 192.168.200.71
- Subnet mask: 255.255.255.0
- Management port: 443
- Admin username: admin
- Admin password: sentryo69!

CVS

- Capture IP address: 169.254.1.2
- Capture subnet mask: 30
- Capture VLAN number: 2508
- Collection IP address: 192.168.200.72
- Collection subnet mask: 24
- Collection gateway: 192.168.200.100
- Collection VLAN number: 200

The prerequisite the sensor application installation on the IE3400 is to configure the switch for access to the CLI (ssh or console port).

Below are the configuration prerequisites needed on IE3400 before installing the Sensor:

- Factory reset of the IE3400 (optional)
- configure access to ssh
- configure basic parameters.

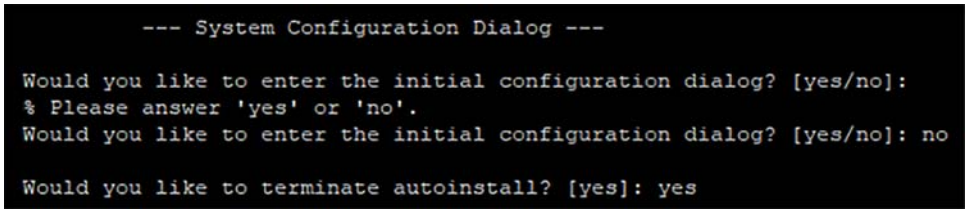
Elements to collect

- Console cable for connection to the IE3400 console port
- Ethernet cable for the connection to one of the IE3400 port
- IP addresses to be assigned to the IE3400 switch

1. Establishing a Serial connection
   - Establish the connection with the IE3400 on the console port (9600 baud).
2. If needed reset the switch
   a. Press and hold the **Express Setup** button for 15 seconds or more. The switch reboots. The system led turns green and the express setup led starts to blink green.
   b. Press the **Express Setup** button again for 1-3 seconds. LED for port 1/1 blinks green.

   The switch now behaves like a factory-default configured switch. To keep a default configuration, answer “no” to the first question, then “yes” to the second one as shown below.

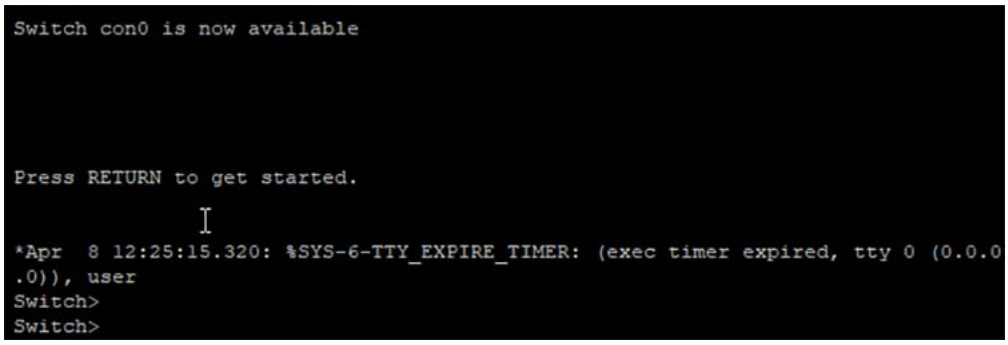
Figure 28 System Config Dialog on IE3400



3. Global parameters:

   – Establish the connection with the IE3400 on the console port (9600 baud).

Figure 29 Console access on IE3400



First enable the CLI, then go into the configuration terminal to setup a name to the switch and a password using the commands below.

```
enable
configure terminal
hostname IE3400
enable secret sentryo69!
```

4. Define switch ssh access and security parameters:

   Type the following command to set the IP address to access the device via SSH:

```
interface vlan 200
ip address 192.168.200.71 255.255.255.0
no shutdown
exit
```

   Add necessary security parameters:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username admin privilege 15 secret sentryo69!
```

   Generate ssh keys:

```
ip domain name ccv
crypto key generate rsa general-keys modulus 4096
```

   Save the configuration

```
exit
```

```
write mem
```

5. Test ssh access to the switch

   Test ssh connection to the IE3400 by connecting to the ip address configured. In this example it is 192.168.200.71. During login use the previously configured admin username and password and verify SSH connection works.

   – Login using admin/sentryo69!

   To bring up the IE3400 with sensor application (CVS) and have it registered with the CVC with the IP address schema mentioned earlier, follow steps 1 to 4 inside Section 3 “Procedure with the Local Manager” in the Cisco Cyber Vision IE3400 and CAT9300 installation guide available at the below link:

   https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IE3400_and_CAT9300_Installation_Guide_Release_3_1_0.pdf

   Once the above pre-requisite configurations on IE3400 are completed, proceed to Section 3 “Procedure with the Local Manager” in the Cisco Cyber Vision IE3400 and CAT9300 installation guide available at the below link. Specifically, just implement steps 1-4 shown in the guide as relevant to IE3400 on the previously configured IE3400 switch.

   https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IE3400_and_CAT9300_Installation_Guide_Release_3_1_0.pdf

Configure the IE3400 links with the necessary VLAN and SPAN configurations as shown below. This step is necessary before beginning to install the sensor application from the CVC onto the IE3400 switch.

1. Open the IE3400 CLI through ssh or via the console terminal, and first configure a vlan for the traffic mirroring. To do this type:

```
configure terminal
vtp mode off
vlan 2508
remote-span
exit
```

2. Then configure the appgigabitEthernet port which enables the communication to the IOx virtual application using below commands

```
interface AppGigabitEthernet 1/1
switchport mode trunk
exit
```

3. The SPAN session needs to be configured, interfaces which need to be monitored need to be added in the session as shown below

```
monitor session 1 source interface Gi1/8
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
```

4. One of the switch ports needs to be configured to enable the communication between the virtual sensor and the center. To do this type:

```
int gi1/8
description provide connectivity to CVC collection subnet
switchport mode trunk
switchport trunk allowed vlan 1-2507, 2509-4094
no shutdown
exit
```

5. Finally, the configuration needs to be saved as shown below

```
exit
write mem
```

Finally to bring up the IE3400 with sensor application (CVS) and have it registered with the CVC using the IP address schema mentioned earlier, proceed to Section 5 “Procedure with the CLI and the Cyber Vision sensor management extension” within the Cisco Cyber Vision IE3400 and CAT9300 installation guide available at the below link. Follow all the steps listed under this section post which CVS application would get installed on IE3400 and after a few minutes the sensor will appear as connected in the CVC.

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IE3400_and_CAT9300_Installation_Guide_Release_3_1_0.pdf

Note: The complete configuration of IE3400 has been provided in the Appendix A for reference.

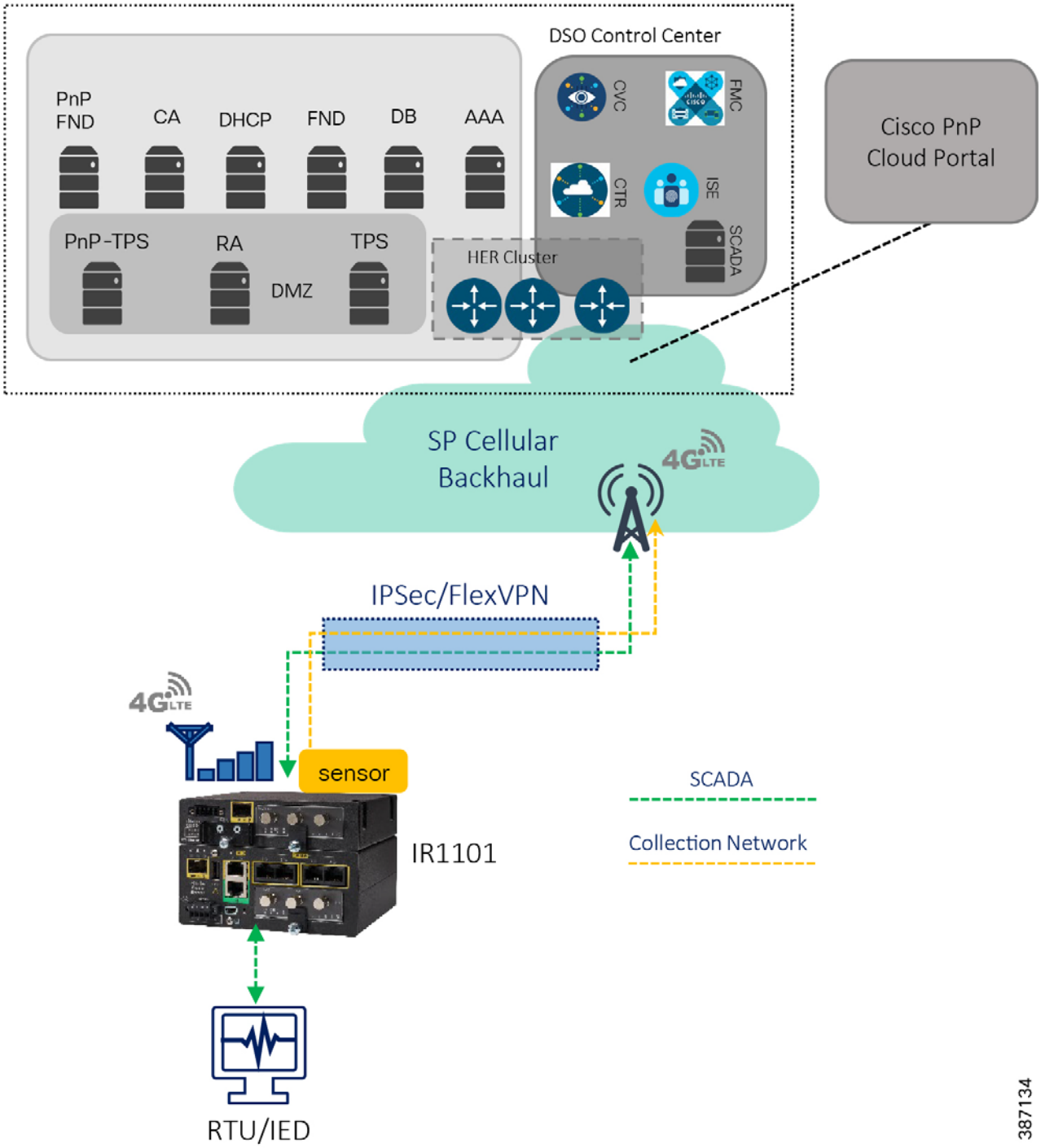
Sensors in Distribution Automation

IR1101

Positioning IR1101 as Sensor

As shown in the following topology, the Cisco IR1101 is connected via cellular backhaul over FlexVPN to Head End Router on DMZ. In the figure SCADA FEP as the DSO Control Center connects to HER and communicates with SCADA IED connected to Secondary Substation Router Cisco IR1101 over IPSec FlexVPN tunnel established over Cellular connection.

Figure 30 IR1101 Secondary Substation Router as Cisco Cyber Sensor



As per the topology shown in the above figure, Cisco IR1101 is positioned as the Secondary Substation router or DA gateway, and we have the IR1101 Cellular gateway with single LTE radio connected and FlexVPN Tunnel0 over primary LTE module is established and terminates on the HER cluster. SCADA, FND, CVC and other control center/utility applications are advertised via Tunnel0. Once the FlexVPN tunnel0 is established with the HER cluster, and with necessary routes advertised via Tunnel0, the communication could now happen with the Control center in a secure fashion.

Requirement for Inter-HER Routing Protocol in Control Center

Virtual Access interface on HER side corresponds to the (peer side of) the FlexVPN Tunnel0 interface on the IR1101. A routing protocol should be run between the HERs in the HER cluster, redistributing the virtual-access interfaces terminating on each HER. The goal is to make all HERs aware of the FlexVPN tunnels terminating on all other HERs, and to enable consistent routing of return traffic via the appropriate HER.

After enabling the end to end reachability between IR1101 and Head End, the application traffic will be encrypted by FlexVPN tunnel0. The encrypted traffic is monitored and redirected to the CVC by sourcing the tunnel interface of IR1101 on the ERSPAN and allowing the IOx to reach the CVC by enabling NAT on the VirtualPortGroup1 via Tunnel interface.

As per the Figure 27, The IR1101 is connected to the RTU/IEDs using Gig/FE interface, CVC and SCADA FEP is connected via Cellular backhaul over FlexVPN tunnel. The complete configuration of Cisco IR1101 and HER is provided in the Appendix C and D section of this guide.

Configuring IR1101 as Sensor

This section focuses on the components listed below discussing the interactions between the Cisco Cyber Vision Sensor application hosted on the IR1101 and the Cisco Cyber Vision Center used for managing the sensor application in order to provide Grid visibility.

- Cisco IR1101 Integrated Services Router Rugged
- Cisco Cyber Vision Sensor (CVS) application
- Cisco Cyber Vision Center (CVC)

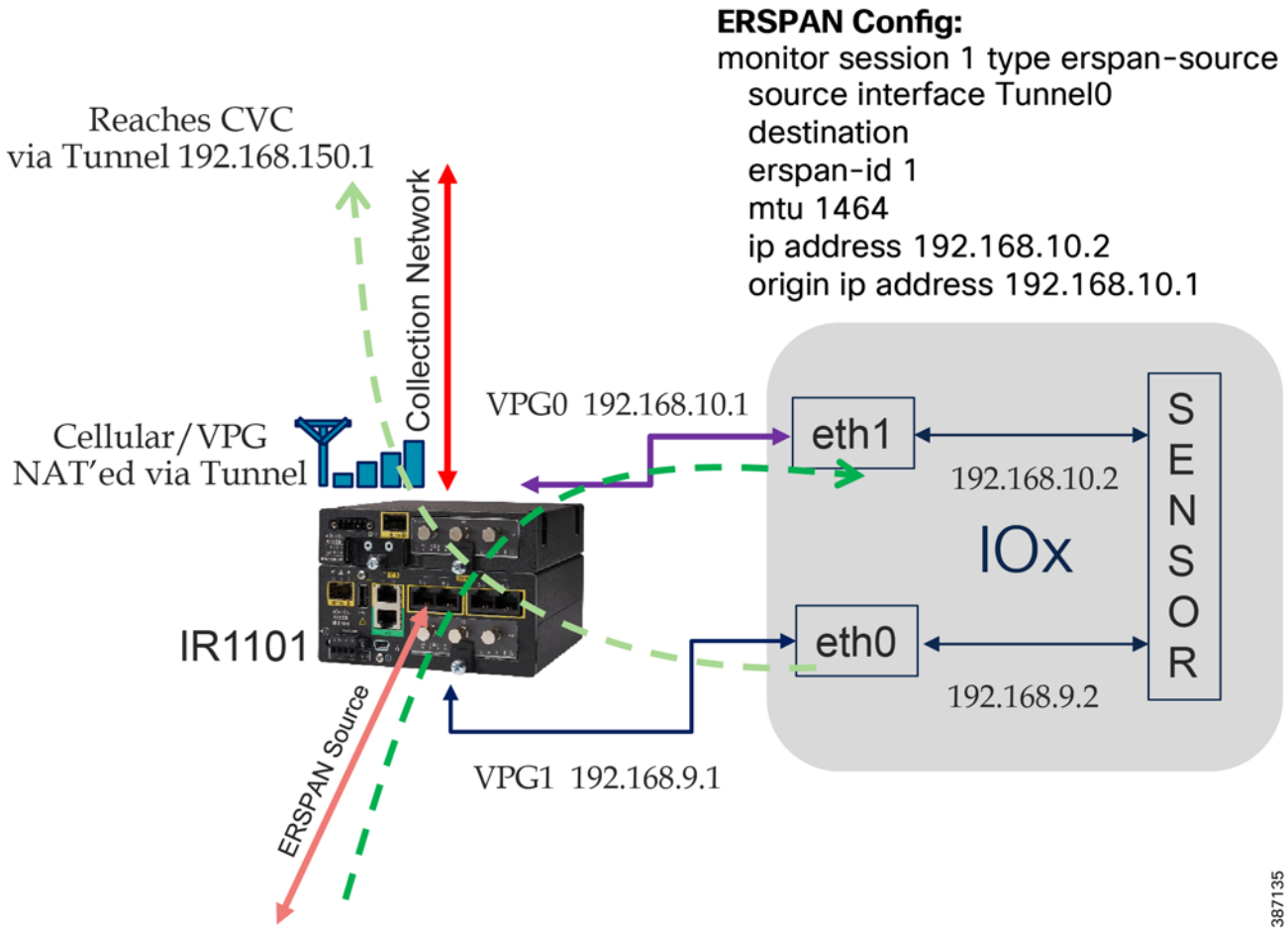
Cisco Cyber Vision Sensor application can be hosted as an Edge compute in IOX. Regular IOS perform the operation of routing the SCADA traffic. Sensor applications installed on IOX perform the role of passive sensor. The sensor application hosted on IR1101 needs two interfaces, one to connect the sensor to the collection network interface of the Cyber Vision Center and one to monitor the traffic on local IOS interfaces.

Cisco IR1101 IOx uses VirtualPortGroup as means to communicate between IOS and the IOx application. A logical mapping of VirtualPortGroup and IOx Application is shown in the following figure. This guide proposes to use Encapsulated Remote Switched Port Analyzer (ERSPAN) to monitor traffic on one or more routed ports or routed Switch Virtual Interfaces (SVI).

The ERSPAN source sessions copy traffic from the source routed ports or SVIs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session, the Cisco Cyber Vision Sensor application in this solution. Similarly, the application uses a separate interface to send the processed traffic to the collection network interface.

To enable reachability of the collection network interface of the Center for the sensor, its recommended to enable NAT on the VirtualPortGroup and overload using the IR1101 WAN facing interface. This section describes how to perform a clean installation of the sensor application (CVS) on Cisco IR1101. As a pre-requisite it is recommended to have the Cisco Cyber Vision Center installed and running.

Figure 31 Cisco IR1101 IOX Sensor interface mapping



The following IP address schema has been used in this guide to bring up the CVS application on IR1101 and integrate it to the CVC as highlighted in the above figure.

CVC

- Admin Interface (eth0): 192.168.117.11
- Collection interface (eth1): 192.168.109.109
- Collection network gateway: 192.168.109.1
- NTP: 192.168.109.1

IR1101

- Admin IP address: 192.168.150.16
- Subnet mask: 255.255.255.0
- Management port: 443
- Admin username: admin
- Admin password: sentryo69!

CVS

- Capture IP address: 192.168.10.2
- Capture subnet mask: 24
- Collection IP address: 192.168.9.2
- Collection subnet mask: 24
- Collection gateway: 192.168.9.1

Now for the sensor application install on IR1101, the prerequisite is to configure the switch for access to the CLI (ssh or console port).

Below are the configuration prerequisites needed on IR1101 before installing the Sensor:

- Factory reset of the IR1101 (optional)
- Configure access to ssh
- Configure basic parameters.

To bring up the IR1101 with sensor application (CVS) and have it registered with the CVC with the IP address schema mentioned earlier, follow steps 3. 1 to 3.5 inside Section 3 “Procedure with the Local Manager” inside the Cisco Cyber Vision IR1101 installation guide in below link.

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IR1101_Installation_Guide_Release_3_1_0.pdf

Below steps show the necessary configuration needed on IR1101 for the sensor application deployed to then register with the CVC.

1. Setup ERSPAN (Encapsulated Remote Switched Port ANalyzer). In order to receive traffic inside an IOx application, you should make sure the app is connected to a VirtualPortGroup, and has the correct IP address by issuing the following commands.

```
interface VirtualPortGroup0
    description App ERSPAN
    ip address 192.168.10.1 255.255.255.0
   end
```

And finally, create the monitor session,

```
monitor session 1 type erspan-source
source interface Tu0
destination
erspan-id 1
mtu 1464
ip address 192.168.10.2
origin ip address 192.168.10.1
```

2. Setup NAT

We need to add NAT rules so that the container can ping the outside. This will be on a different virtual port group than the ERSPAN to separate the traffic.

On Cellular interface,

```
interface Cellular0/1/0
 description Connection to DMZ UCS
 ip address negotiated
```

```
 ip nat outside
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
end
```

On Tunnel/Loopback interface,

```
interface Tunnel0
 description IPsec tunnel to HER1.ipg.cisco.com
  ip unnumbered Loopback0
  ip nat outside
   ipv6 unnumbered Loopback0
  tunnel source Cellular0/1/0
  tunnel destination dynamic
  tunnel protection ipsec profile FlexVPN_IPsec_Profile
  ip virtual-reassembly

interface Loopback0
 ip address 192.168.150.16 255.255.255.255
 ip nat outside
```

On VirtualPortGroup1,

```
interface VirtualPortGroup1
 description App Collection N/w
 ip address 192.168.9.1 255.255.255.0
 ip nat inside
  ip tcp adjust-mss 1160
end
```

Configure Access-list for the VirtualPortGroup1 to reach outside the container via tunnel interface.

```
ip access-list standard CV_LIST
 10 permit 192.168.9.0 0.0.0.255
!
ip nat inside source list CV_LIST interface Loopback0 overload
```

3. Finally, the configuration needs to be saved as shown below

```
exit
write mem
```

After a few minutes the sensor will now appear connected in Cisco Cyber vision after following any one of 3 ways to install sensor on Cisco IR1101 as mentioned in “Cisco Cybervision IR1101 installation Guide”.

After the pre-requisites are met (section 2 and section 3.1 to 3.5), there are 3 ways we can install Cyber Vision Sensor on IR1101.

1. Via Local Manager – Follow Section 3.6 to 3.10 on above guide
2. Via CLI – Follow section 4.1 to 4.3
3. Via Cisco Cyber Vision Center Extension – Follow section 5.1 to 5.2

Note: When IR1101 IoX sensor is deployed via Cyber Vision Extension Feature, make sure to configure “ip tcp adjust-mss 1160” on VirtualPortGroup1 of IR1101 and Virtual-template interface on Head End Router (in DMZ) where IR1101 Tunnel interface is connected.

OT Asset Visibility

After CVC starts seeing traffic coming in from the sensor, all the assets in the substation network along with the data exchanged and the associated events start showing up in the various pre-defined presets available in CVC like data, asset management (OT, IT, controllers etc.).

This section focuses on CVC capabilities to detect various SCADA protocol traffic flowing in the network along with the corresponding operations like poll, control being demonstrated between the SCADA Front End Processor or controller and SCADA Outstation control systems.

T104

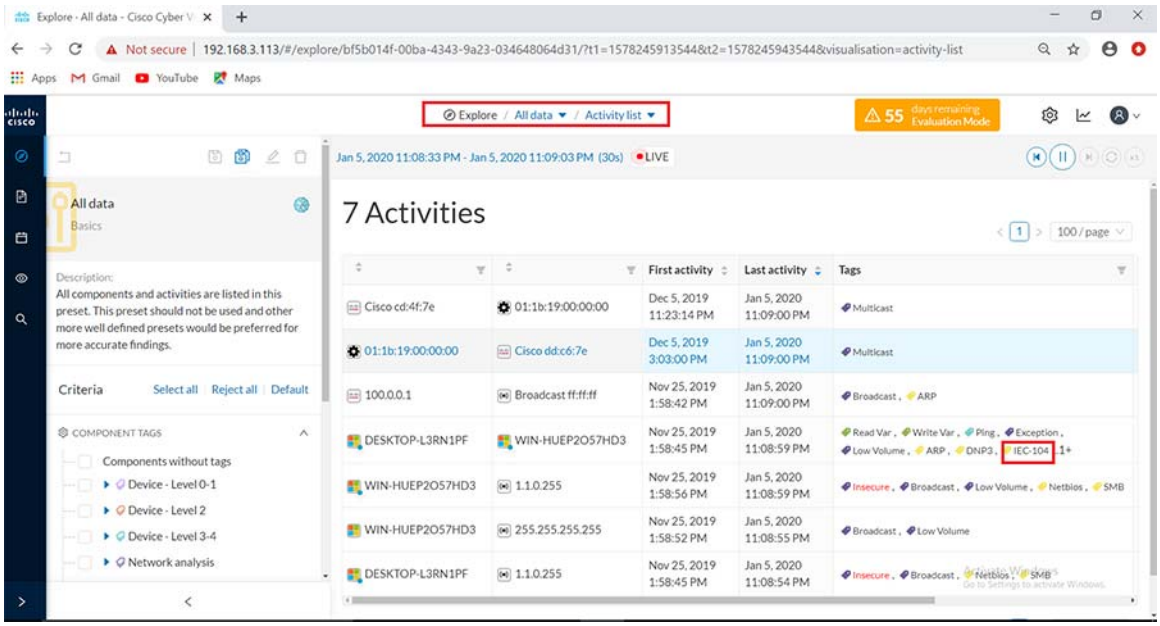
After the network data begins to display in CVC, selectively filter the flows detected by the system for SCADA protocol. For example, IEC-104 to view all the associated events, flows along with their tags as shown below.

Ensure reachability exists between SCADA server and SCADA client or IED systems and they are exchanging DNP3 traffic, specifically a Read (poll), Write (control) and Unsolicited reporting operations. For each of these operations being performed, refer to the Flow diagram showing T104 control flow in the DA Secondary Substation Implementation Guide available at the below location.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG/DA-SS-IG-doc.html#59958

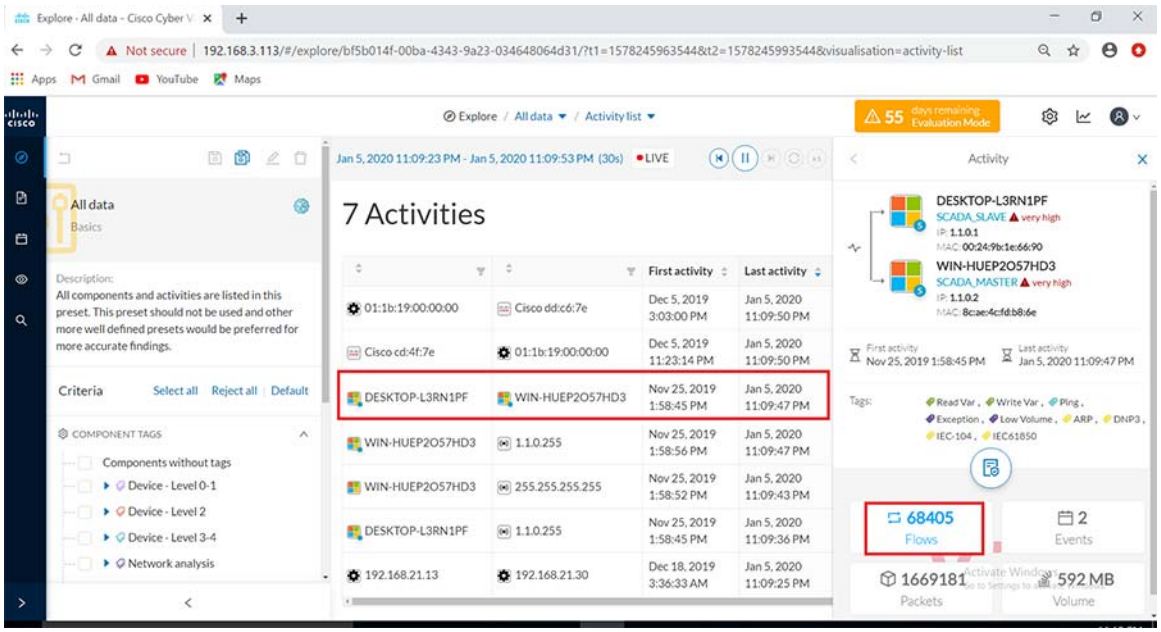
Follow the steps below to view these events in CVC.
Log in to the CVC and navigate to All Data > Activity list under the Explore tab. Look for the tags associated with IEC-104 and identify the activity of the associated systems exchanging T104 traffic as shown below.

Figure 32 Activity list for T104



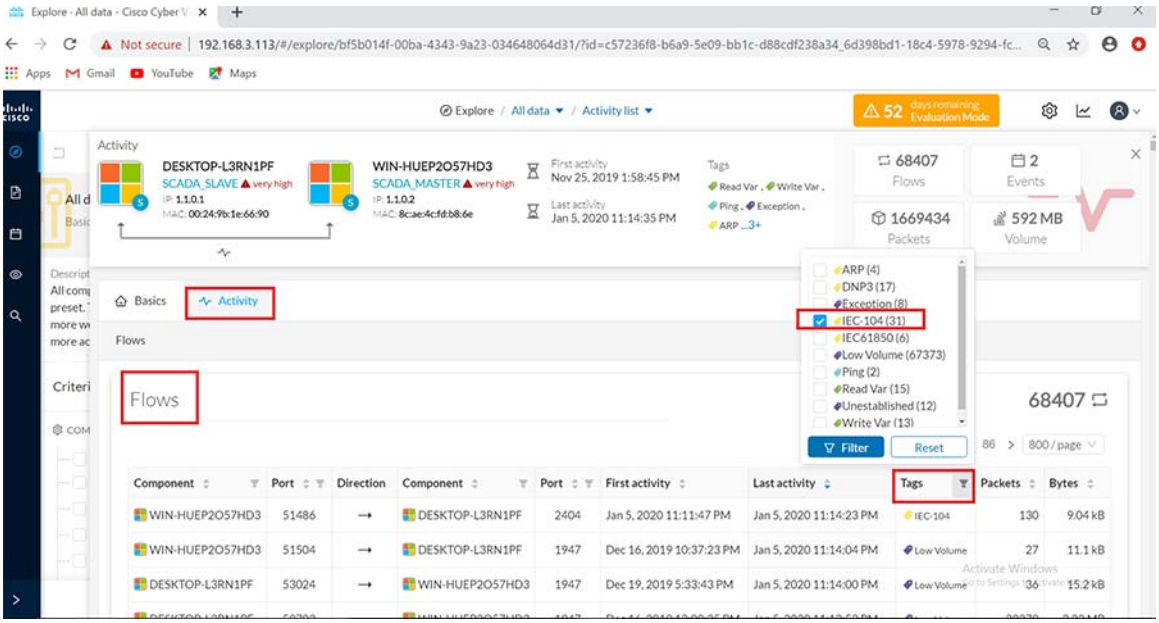
Click on this activity and navigate to **Flows** as shown below.

Figure 33 Total Flows for T104



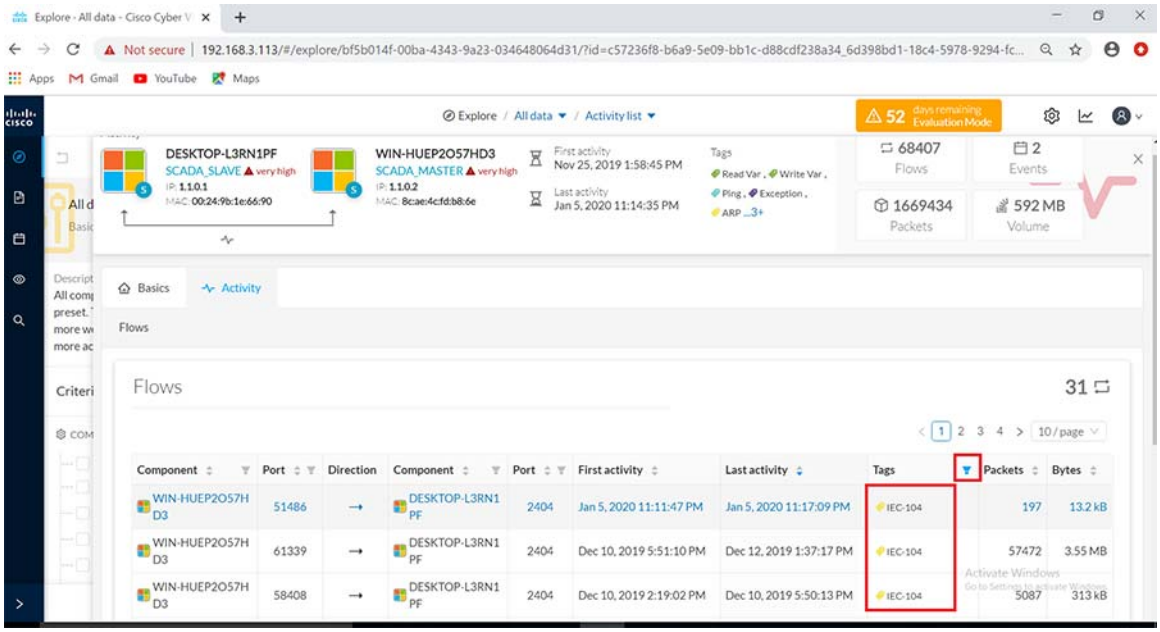
Under the activity selected, look on the **Flows** tab for the sub-tab tags and filter for IEC-104 traffic as shown below.

Figure 34 Filter tags for T104



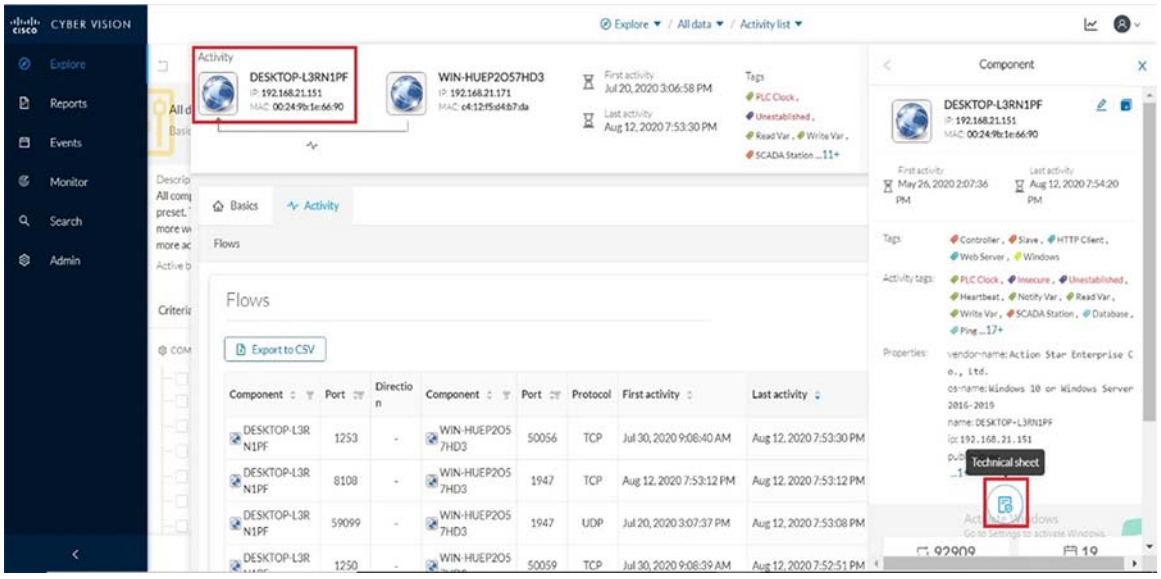
After the filter is applied, look for the T104 flows with the name IEC-104 which include the operations performed by the master on the slave as shown below.

Figure 35 T104 flow exchanges



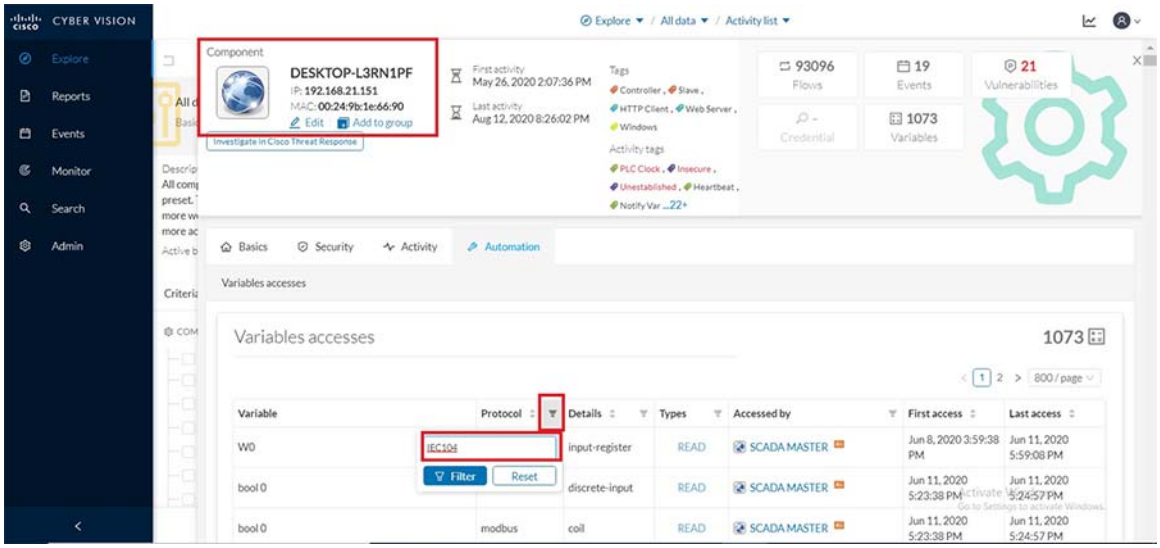
Click on the flows listed for IEC-104 one at a time to view more details about the flow properties. Look at the sub-tabs such as **Properties** or **Content statistics** to obtain more information on the operations performed. To obtain deeper visibility into the variables accessed for each operation, click on the component SCADA slave (DESKTOP-L3RN1PF) in the Activity panel on top of the **Flows** window as shown below. Next click on the **Technical sheet** for this component.

Figure 36 Technical sheet for IEC-104



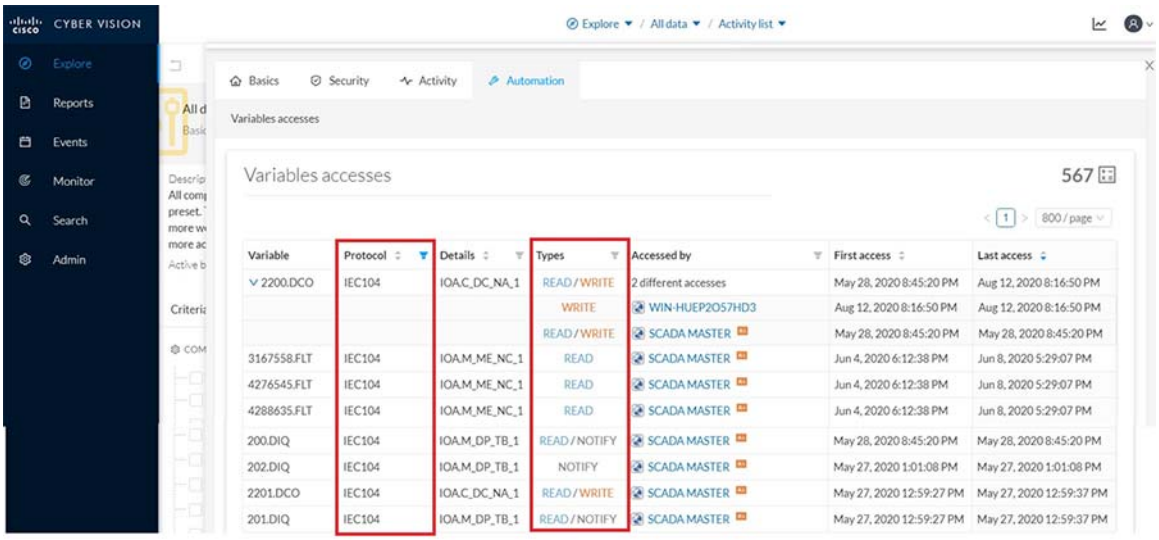
Next click on the **Automation** tab and under the column displayed for protocol, filter for IEC104 information as shown.

Figure 37 Filter for IEC104 variables under Automation tab



This would display information on the different variables accessed for each IEC104 operation performed as shown below. While Read and Write operations are indicated as is, Unsolicited operations are indicated as NOTIFY under the **Variable Types** column.

Figure 38 Variables Accessed for IEC104



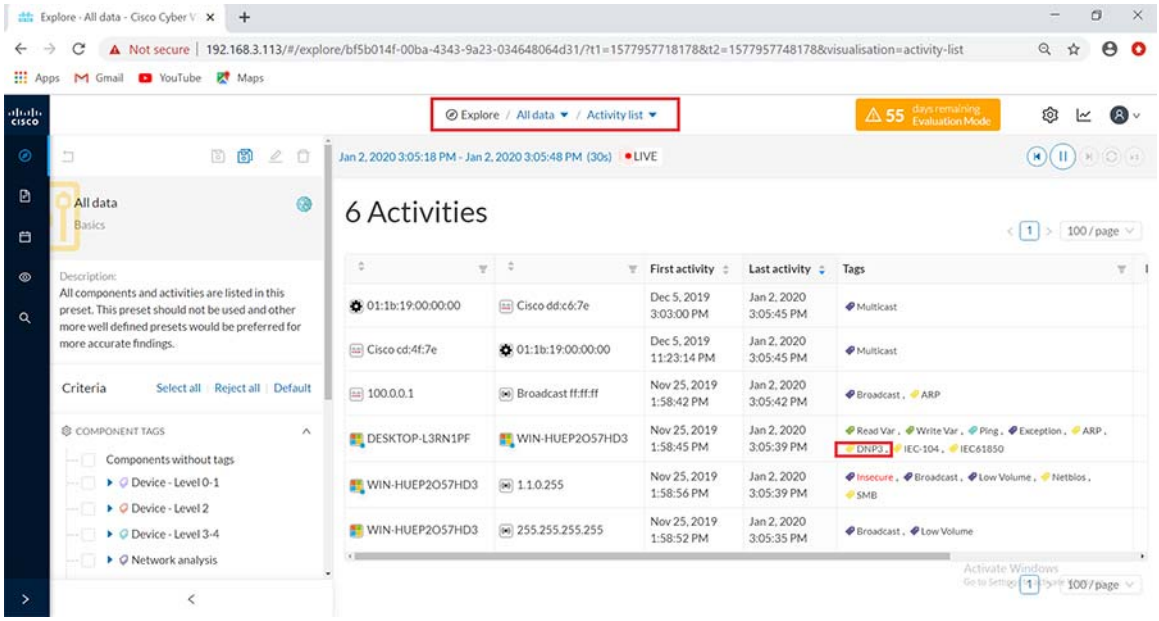
DNP3

After the network data begins to display in CVC, selectively filter the flows detected by the system for SCADA protocol. For example, **DNP3** to view all the associated events, flows along with their tags as shown below.

Ensure reachability exists between SCADA Front End Processor or Controller and SCADA Outstation or IED systems and they are exchanging DNP3 traffic, specifically a Read (poll), Write (control) and Unsolicited reporting operations. Follow the steps below to view these events in CVC.

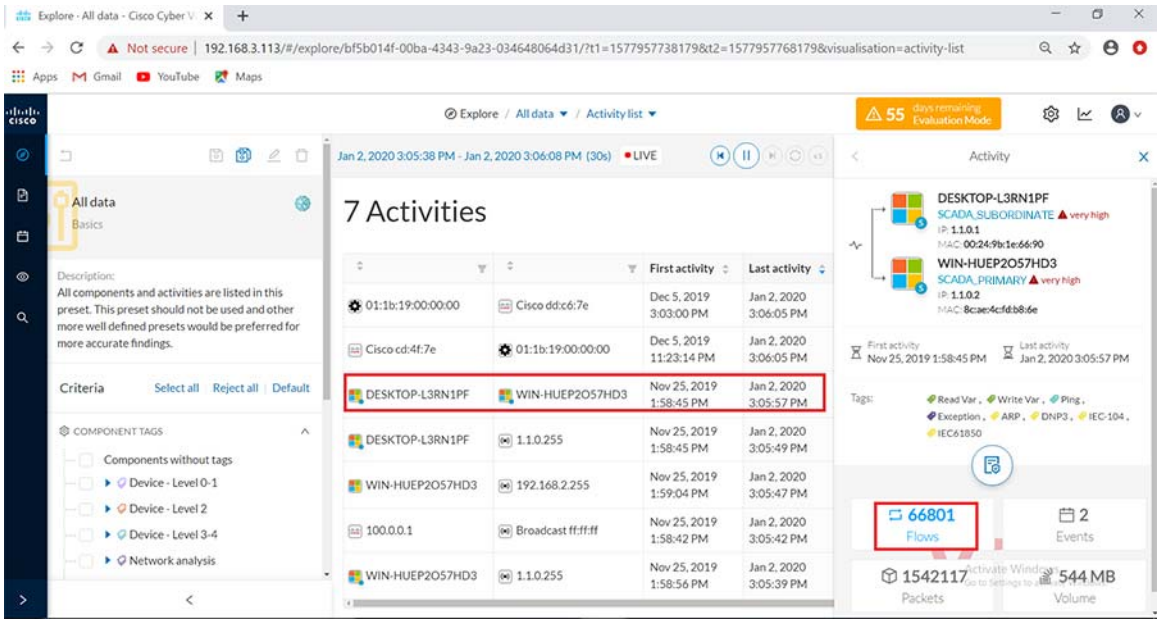
1. Login to the CVC and navigate to **All data > Activity** list under **Explore** tab. Look for the tags associated with DNP3 and identify the activity of the associated SCADA systems exchanging DNP3 traffic as shown below.

Figure 39 Activity list for DNP3



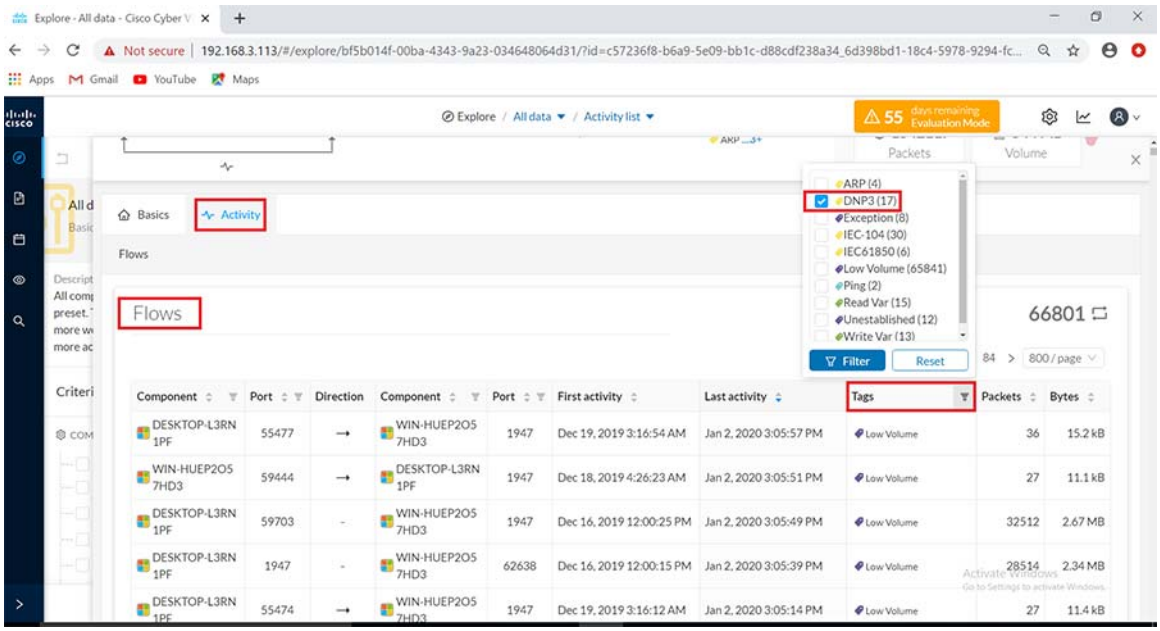
2. The figure above shows both the SCADA Front End Processor or Controller primary (WIN-HUEP2O57HD3) and SCADA IED subordinate systems (DESKTOP-L3RN1PF). The first and last activity when they exchanged DNP3 messages is also shown. Click on this activity and navigate to **Flows** as shown below.

Figure 40 Total Flows for DNP3



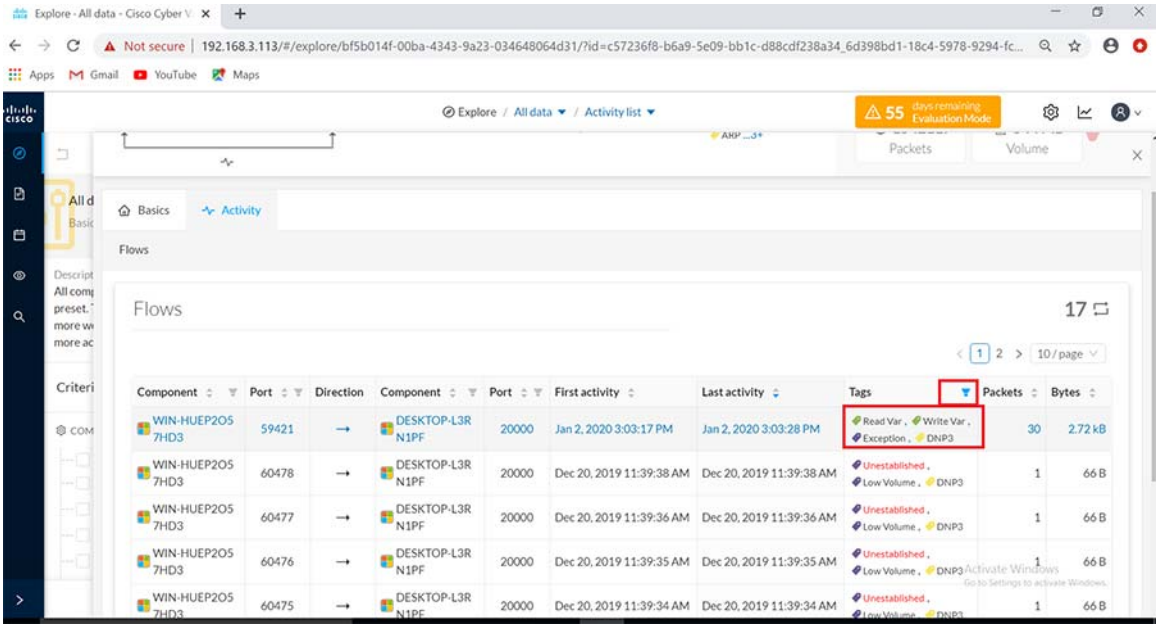
3. Under the activity selected, open the **Flows** tab. Look for the sub-tab **Tags** and filter for DNP3 traffic as shown below.

Figure 41 Filter tags for DNP3



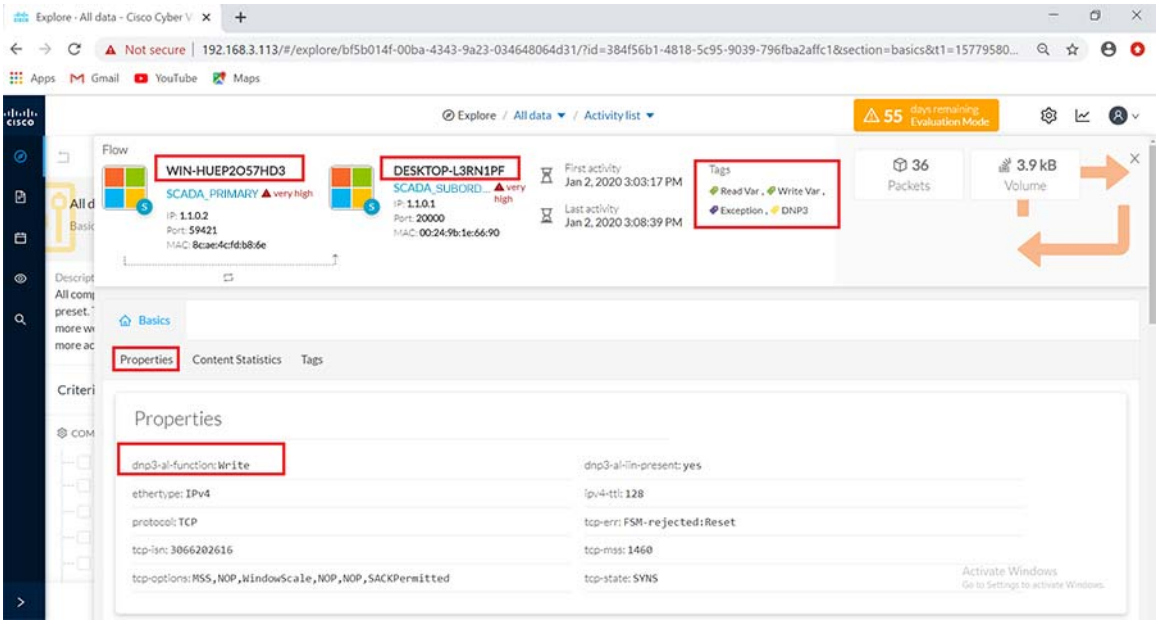
4. After the filter is applied, notice the DNP3 flows showing Read and Write operations performed by the SCADA SCADA Front End Processor or Controller primary on the SCADA IED subordinate system as shown below.

Figure 42 Read, Write exchanges in DNP3



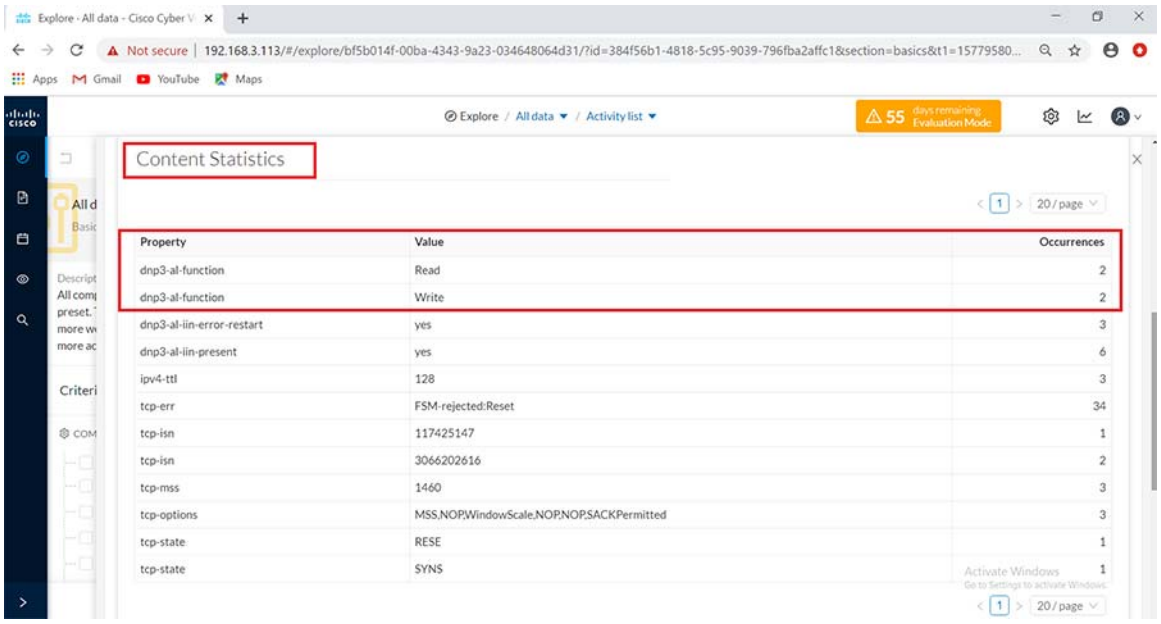
5. Click on the flow highlighted in above figure to show more details about the flow Properties for the DNP3 operations performed as shown below.

Figure 43 Flow properties in DNP3



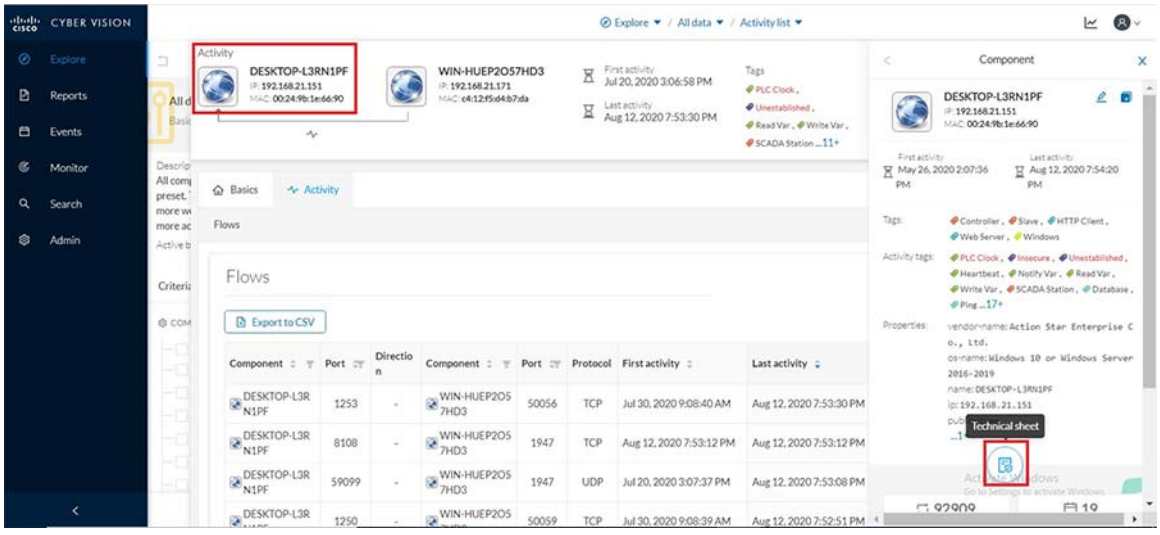
6. On the **Basics** tab, the Content Statistics sub-tab shows the different DNP3 operations performed by the SCADA primary on the subordinate system.

Figure 44 Flow Content Statistics for DNP3



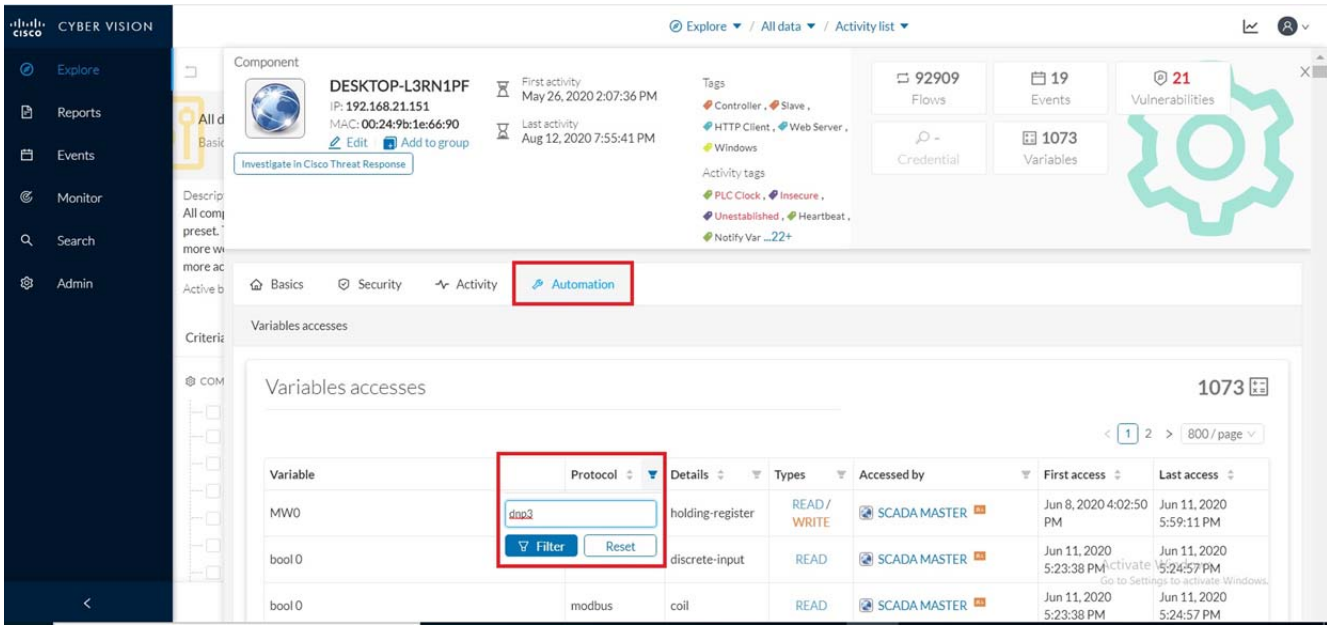
To view Unsolicited operations and the different variables accessed for each DNP3 operation, click on the component SCADA slave (DESKTOP-L3RN1PF) in the **Activity** panel on top of the **Flows** window as shown below. Next click on the **Technical sheet** for this component.

Figure 45 Technical sheet for DNP3



Next click on the **Automation** tab and under the column displayed for protocol, filter for DNP3 information as shown.

Figure 46 Filter for DNP3 variables under Automation tab



This would display information on the different variables accessed for each DNP3 operation performed as shown below. While Read and Write operations are indicated as is, Unsolicited operations are indicated as NOTIFY under the **Variable Types** column.

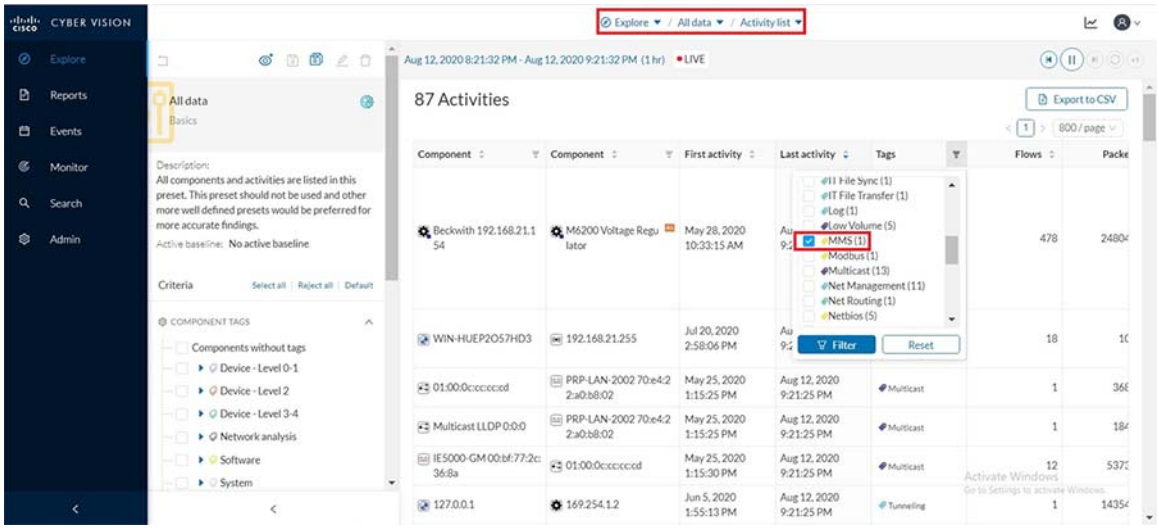
Figure 47 Variables Accessed for DNP3

IEC61850 MMS and GOOSE

Ensure reachability exists between SCADA primary and subordinate systems and they are exchanging IEC-61850 MMS traffic between them. Specifically issue a Read (poll) and Write (control) operation from primary to subordinate and view these events in the CVC as shown below.

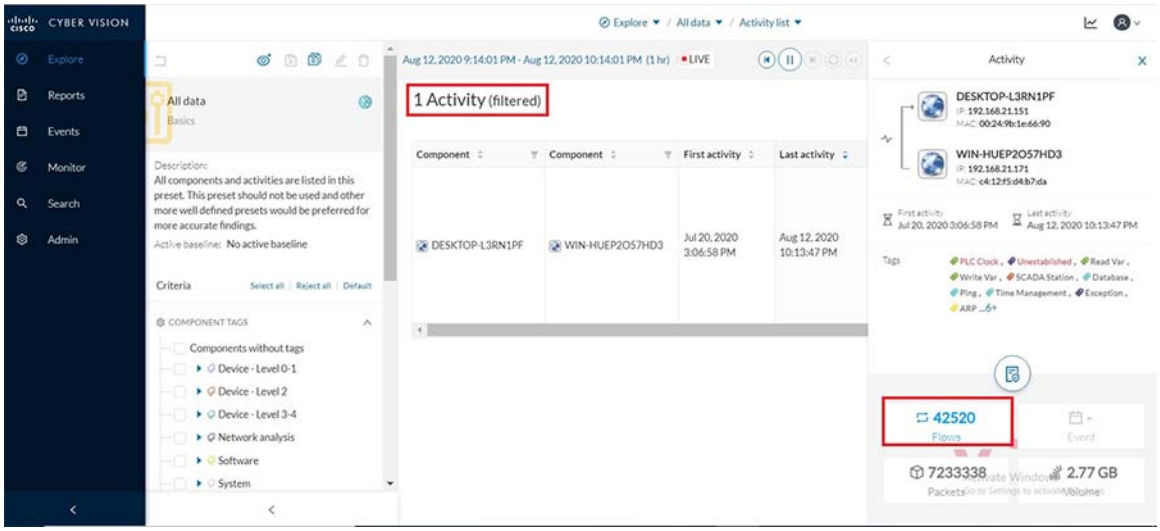
Log in to the CVC and navigate to **All Data > Activity** list under the **Explore** tab. Filter the list of activities displayed for MMS as shown below.

Figure 48 Activity list for MMS



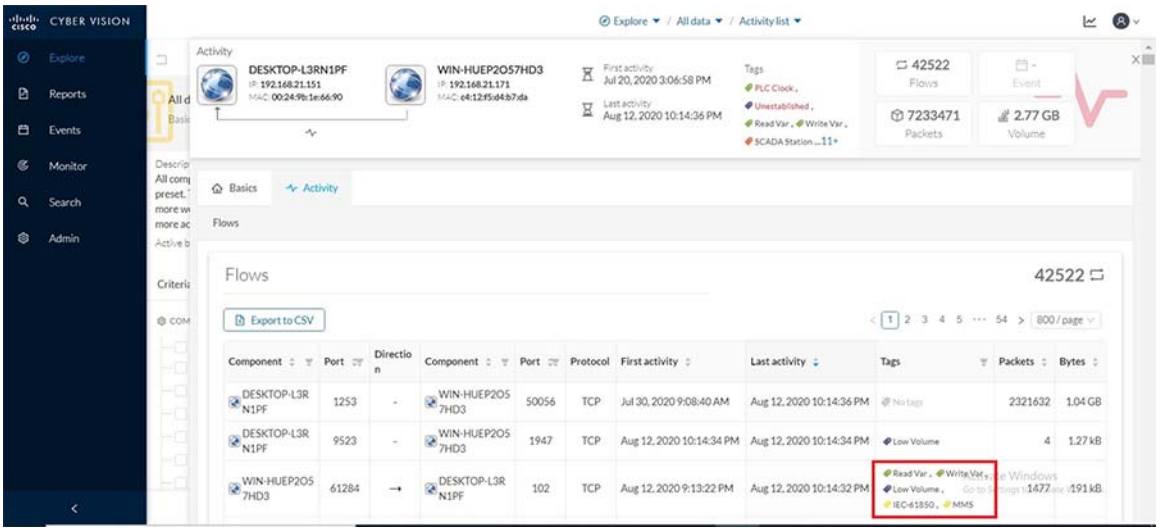
The filtered activity shows the SCADA primary (WIN-HUEP2O57HD3) and subordinate system components (DESKTOP-L3RN1PF) along with the first and last activity of their MMS messages exchanged. Click on this activity and navigate to **Flows** as shown below.

Figure 49 Total Flows for MMS



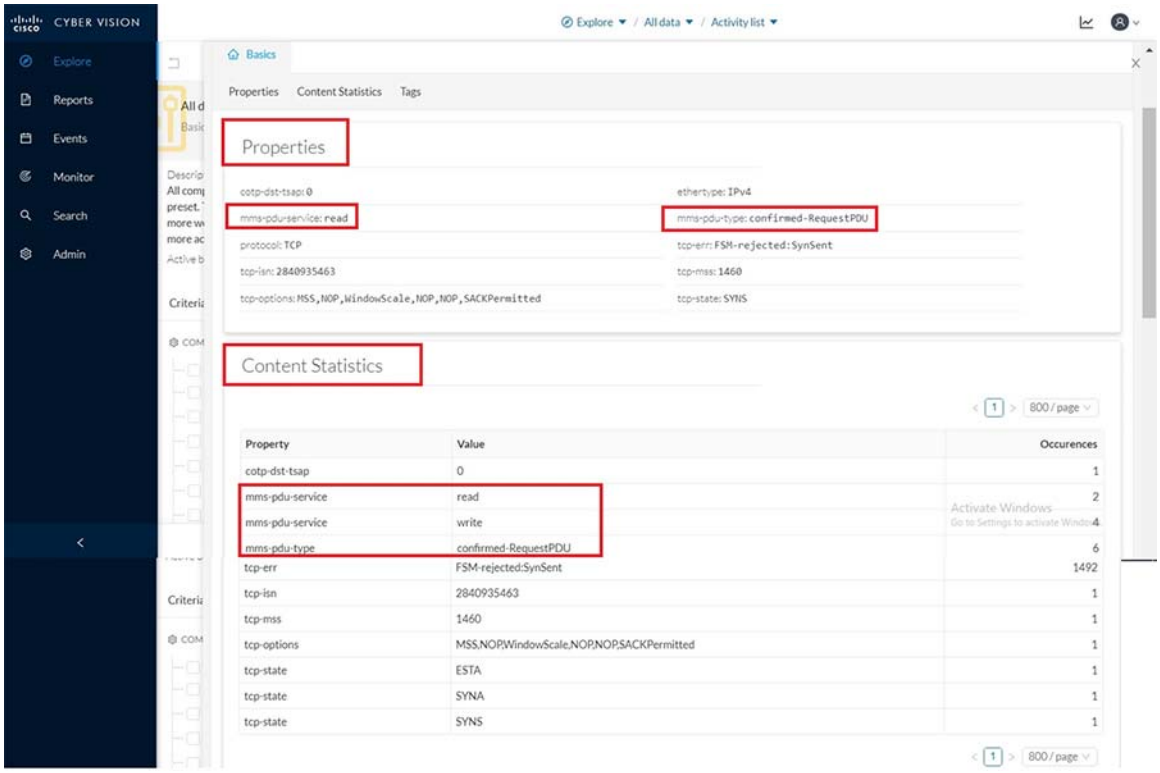
Under the listed flows for the selected activity, notice the MMS flow showing both Read and Write operation tags as shown below.

Figure 50 Read, Write tags for MMS



Once the filter is applied, look for the IEC-61850 flows. These include the operations performed by the primary on the subordinate as shown below.

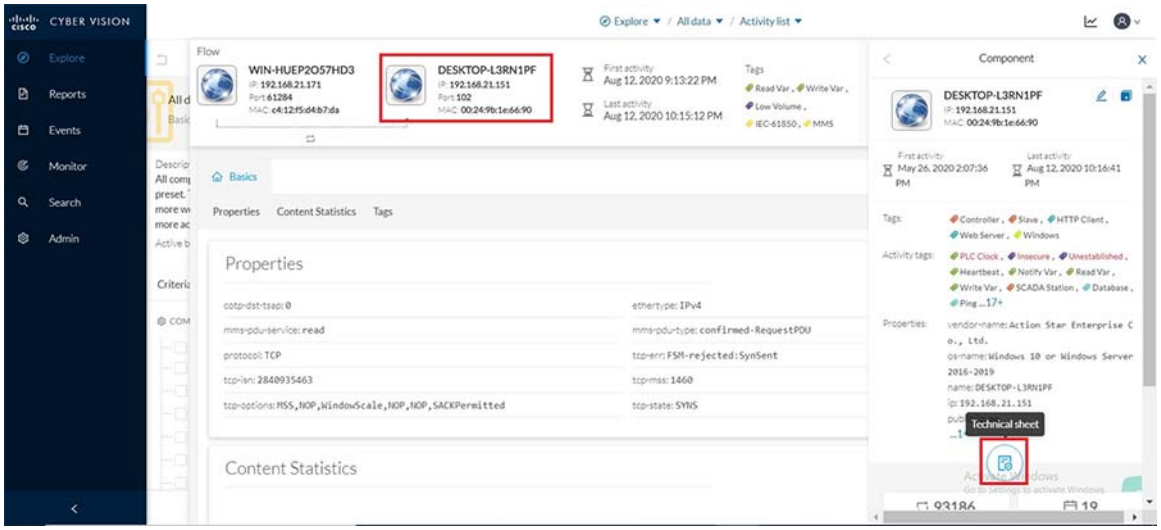
Figure 51 Flow properties in MMS



Notice that the **Content Statistics** sub-tab shows the different MMS operations performed by the SCADA primary on the subordinate system.

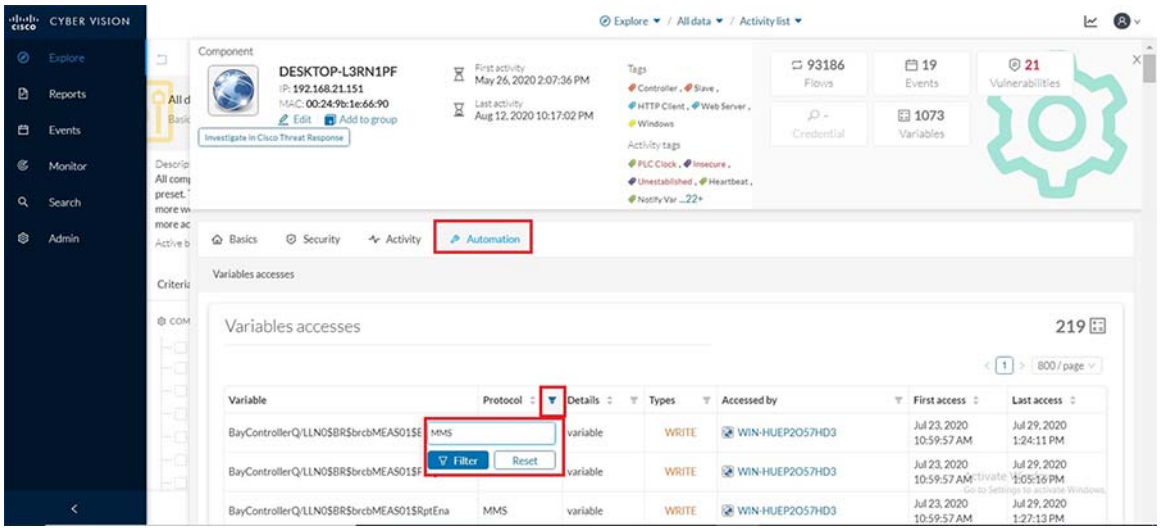
To view the different variables accessed for each MMS operation, click on the component SCADA subordinate (DESKTOP-L3RN1PF) in the **Activity** panel on top of the **Flows** window as shown below. Next click on the **Technical sheet** for this component.

Figure 52 Technical sheet for MMS



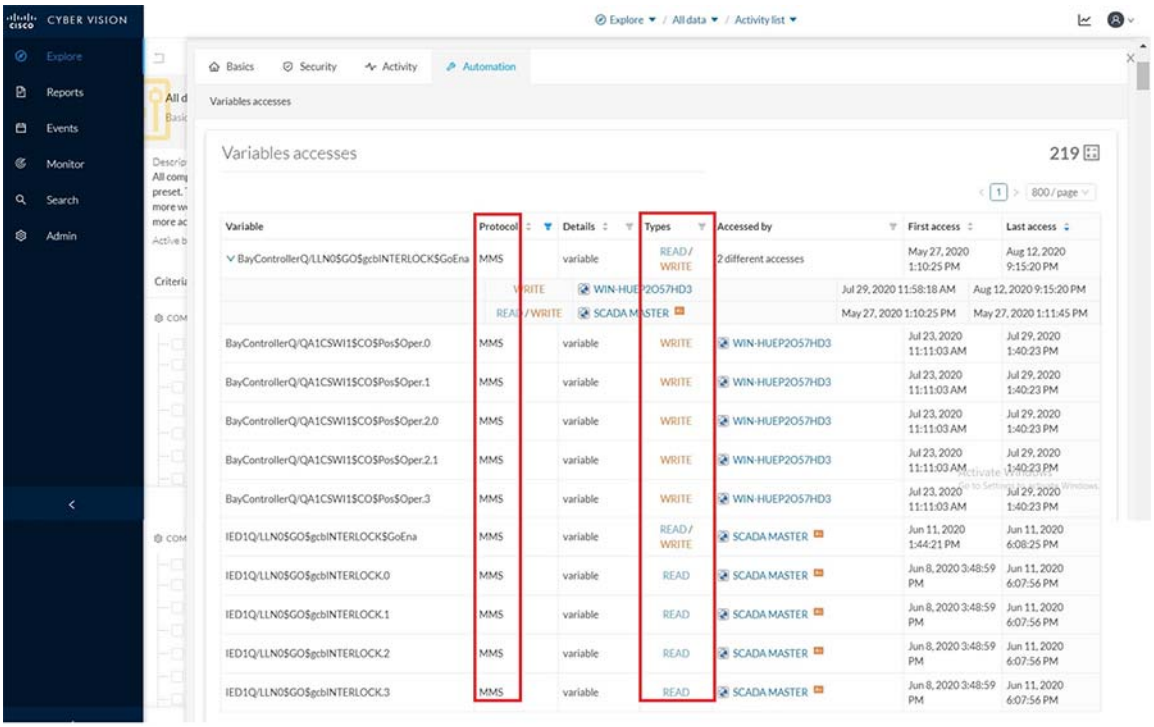
Next click on the **Automation** tab and under the column displayed for protocol, filter for **MMS** information as shown.

Figure 53 Filter for MMS variables under the Automation tab



This would display information on the different variables accessed along with the type of MMS operations performed as shown below.

Figure 54 Variables Accessed for MMS



Repeat the same steps as above but instead filter for **GOOSE** and notice the flows, tags and variables accessed as shown below for reference.

Figure 55 GOOSE activity/flows

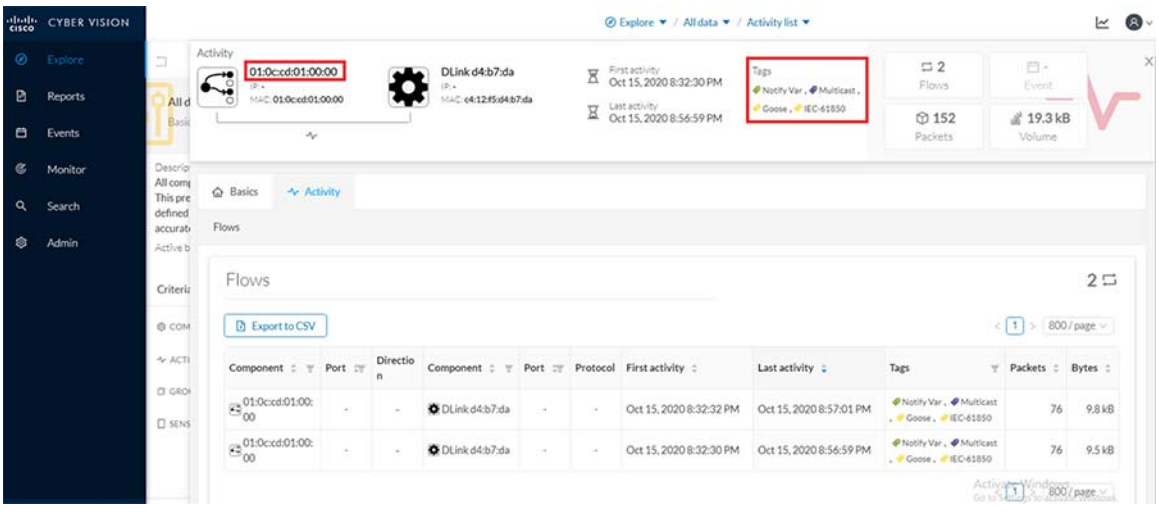
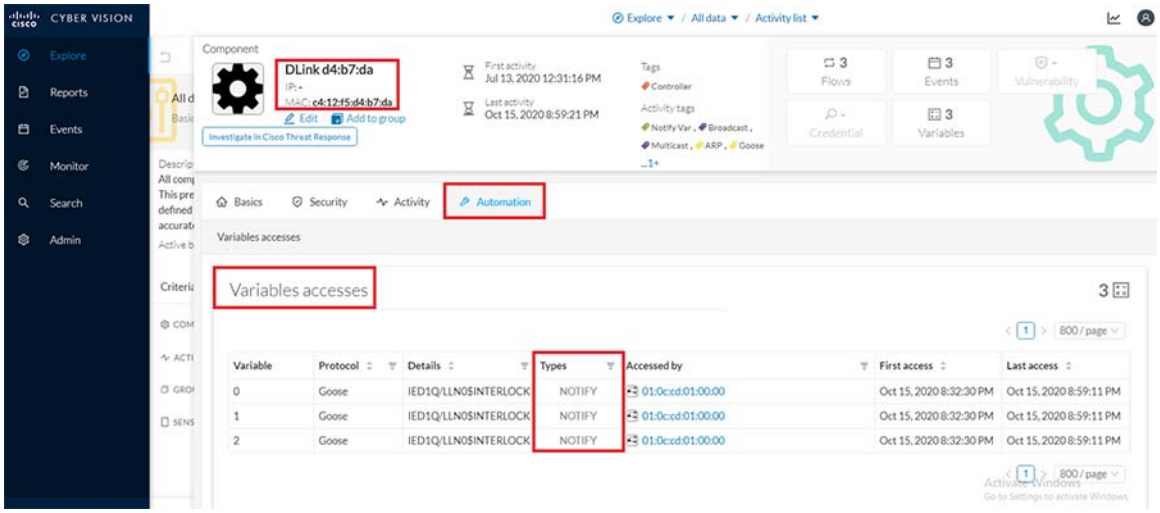


Figure 56 GOOSE variables accessed



Modbus

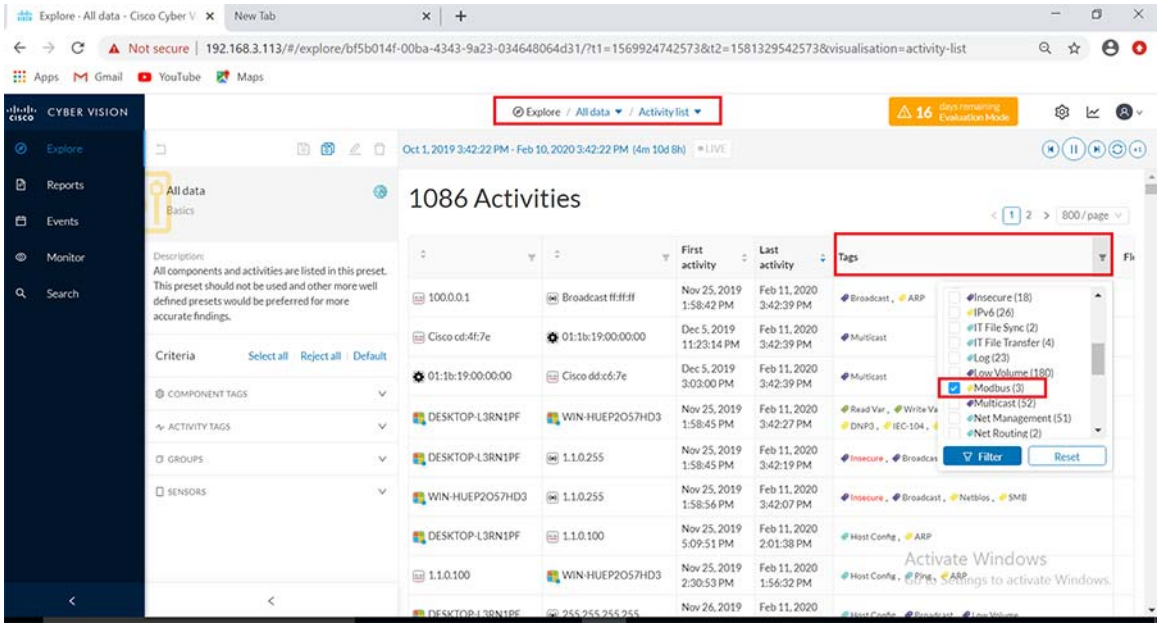
This section focuses on the capability of the sensor and CVC to detect real controller/IED devices connected to the network along with the associated flows exchanged between the IED and the SCADA primary system running the control software to manage the IED. Below shown is the sample switch configuration needed to inter-connect an IED (for example a Beckwith controller) with the IC3000 hosting sensor application and thereafter enabling SPAN for detection of this device and its flows by CVC.

```
IE4000#show run int gi 1/8
!
interface GigabitEthernet1/8
 description connected to IC3k int2 port for span traffic
 switchport mode trunk
 end

IE4000#show run int gi 1/9
!
interface GigabitEthernet1/9
 description connected to IED Beckwith controller switchport access vlan 111
 switchport mode access
end

!! SPAN configuration shown below!!IE4000#show run | s monitor session
!
monitor session 1 source interface Gi1/9
monitor session 1 destination interface Gi1/8
!
IE4000#
```

Once the switch SPAN configuration and the connectivity is completed as shown above, verify reachability exists between the IED device and its SCADA primary system. Then execute some read, write operations on the IED from the SCADA system so those flows can be detected by CVC as shown in detail below.

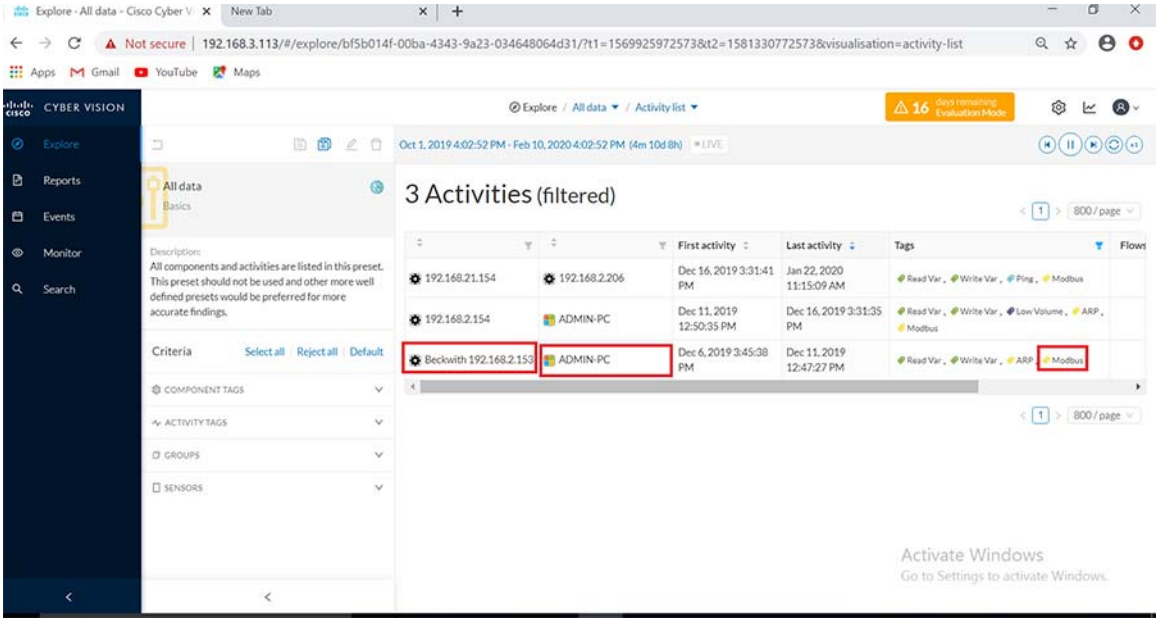
First login to the CVC and navigate to **All data > Activity** list under the **Explore** tab. Look for the tags associated with Modbus by filtering for the same as shown below.

Figure 57 Filter tags for Modbus



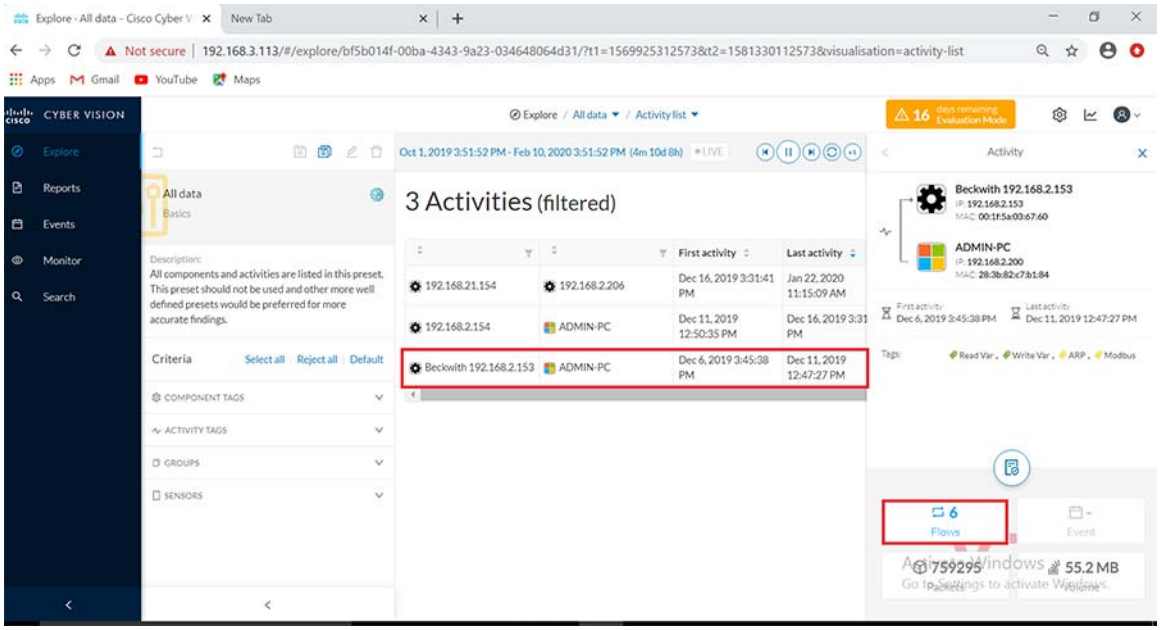
The above step provides all the activity of the associated systems exchanging Modbus traffic, specifically the IED (Beckwith controller) and the SCADA primary system (identified as ADMIN-PC) as shown below.

Figure 58 Activity list for Modbus



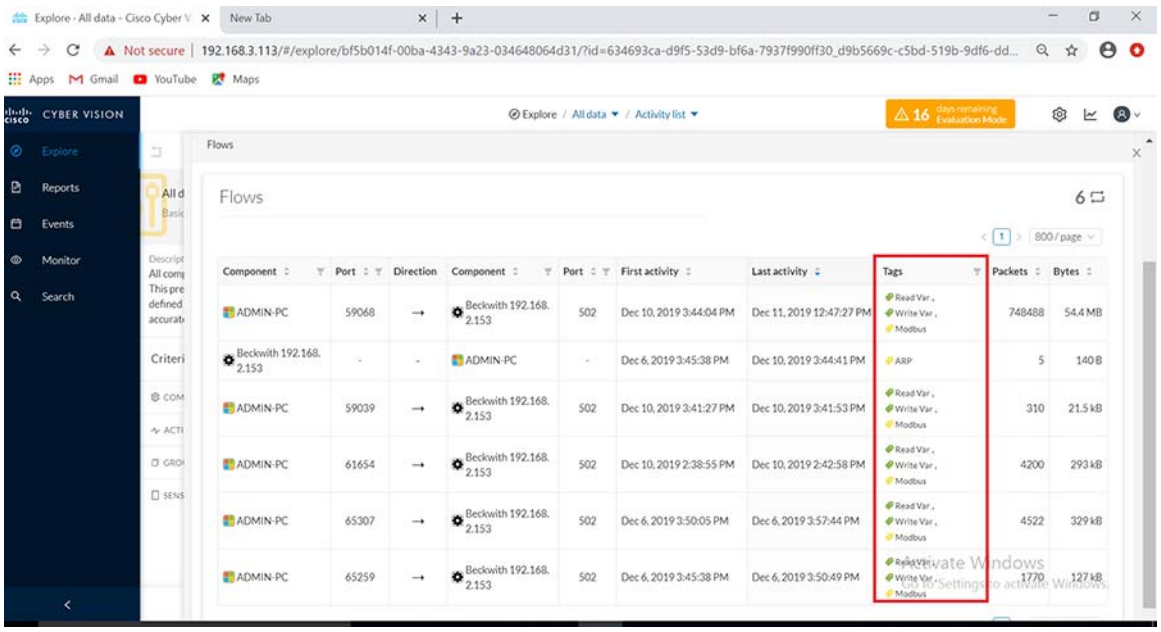
Next click on this activity and navigate to **Flows** as shown below.

Figure 59 Total Flows for Modbus



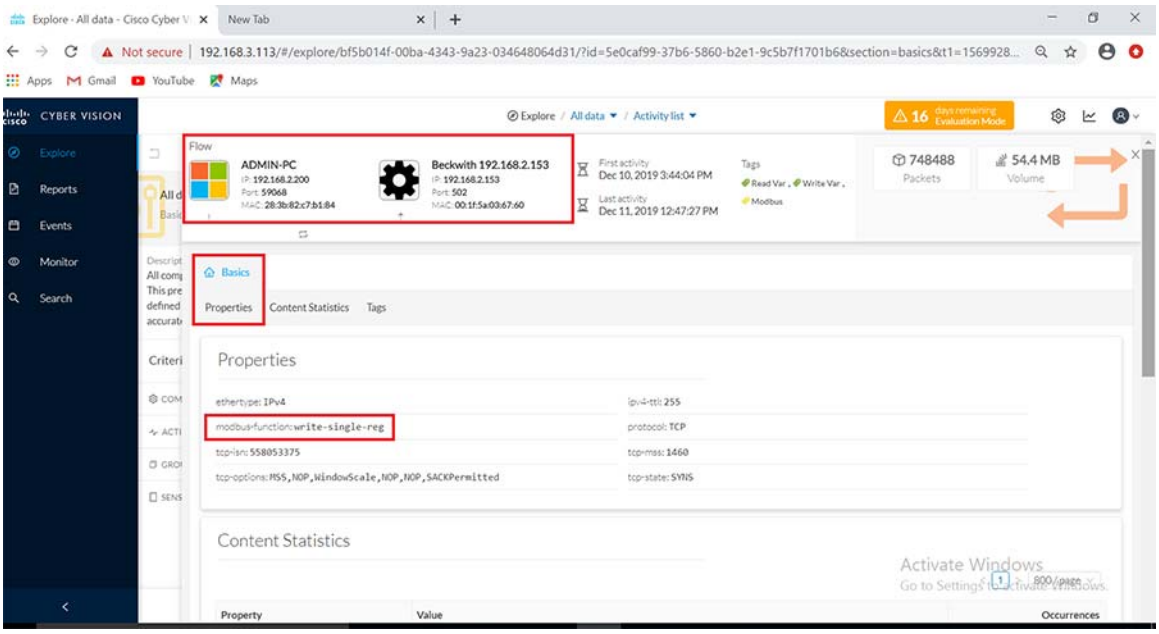
Notice all the Modbus related flows showing both Read and Write operation tags for the controller device as shown below.

Figure 60 Modbus flow exchanges



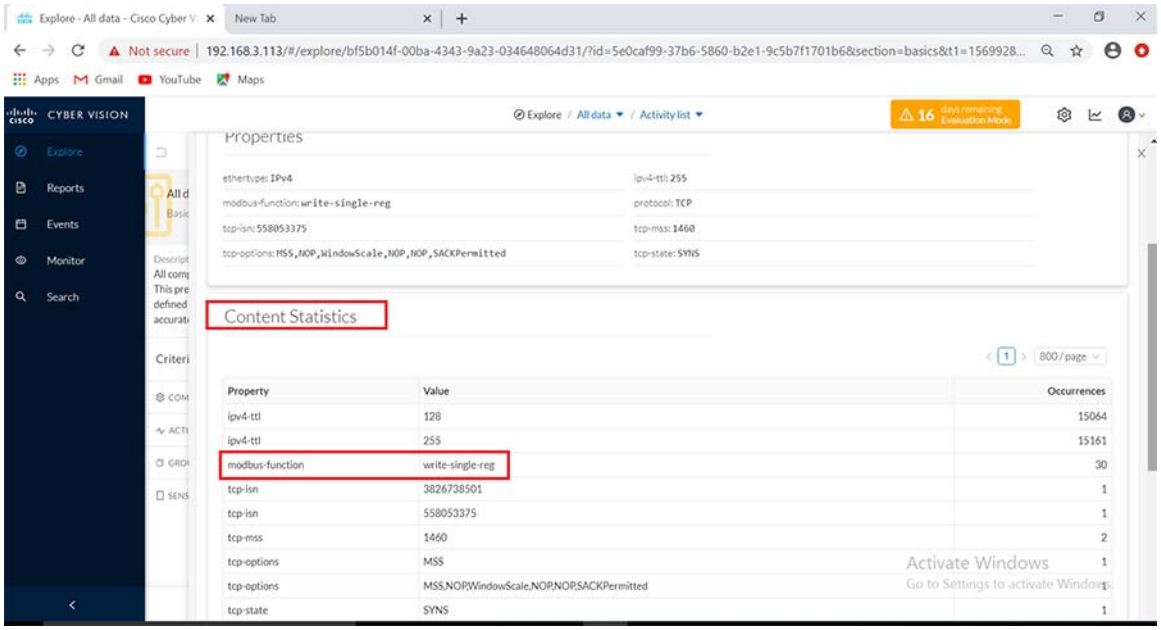
Clicking on any of the flows highlighted in above figure would show more details about the **Flow Properties** for the Modbus operations performed as shown below.

Figure 61 Flow properties in Modbus



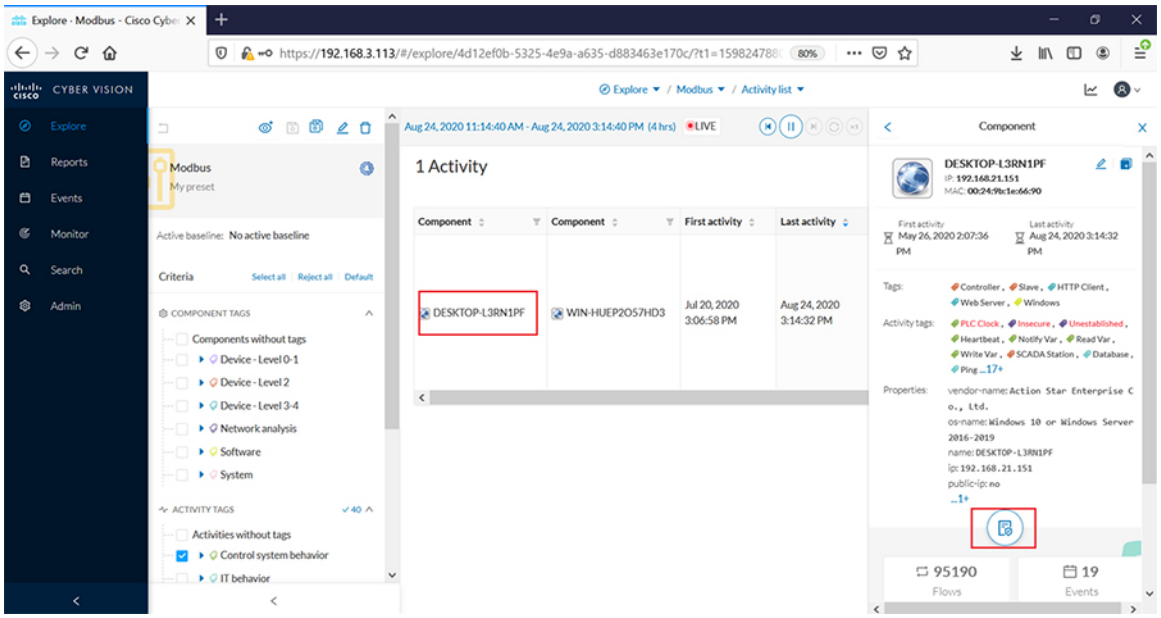
Additionally, under the **Basics** tab the **Content Statistics** sub-tab also shows more details about the Modbus operations performed on the controller.

Figure 62 Flow Content Statistics for Modbus



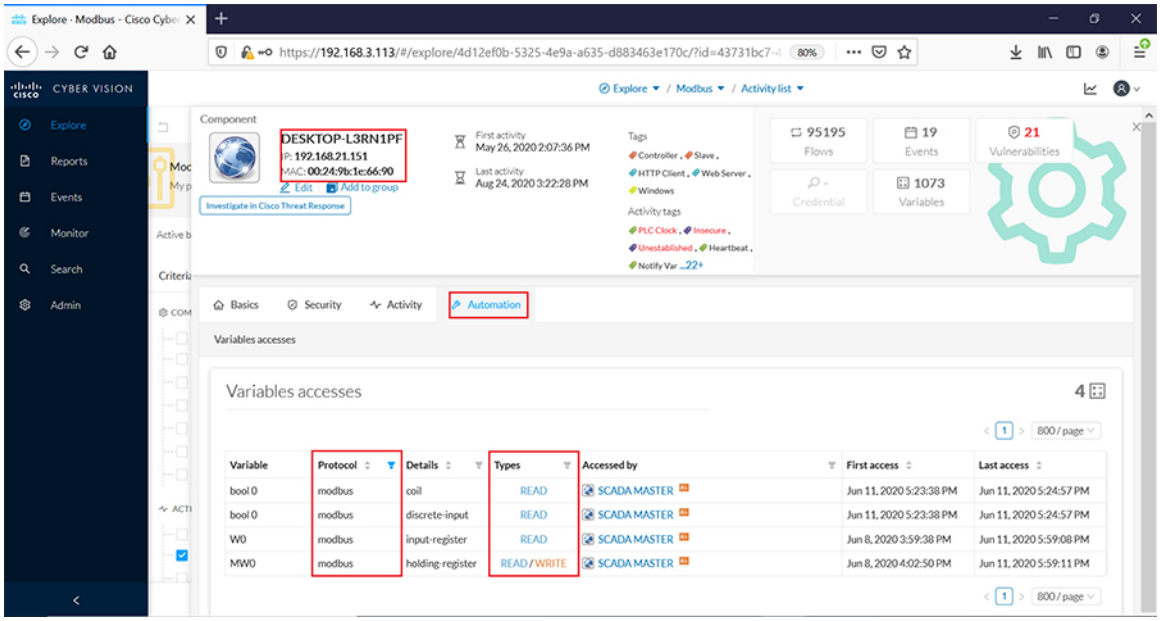
To view the different variables accessed for each Modbus operation, click on the component SCADA subordinate (DESKTOP-L3RN1PF) in the **Activity** panel on top of the **Flows** window as shown below. Next click on the **Technical sheet** for this component.

Figure 63 Technical sheet for Modbus



This would display information on the different variables accessed along with the type of Modbus operations performed as shown below..

Figure 64 Variables Accessed for Modbus

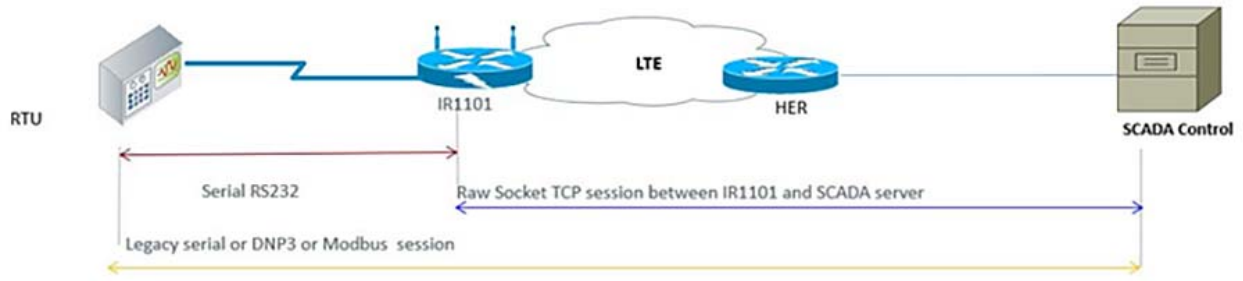


CVC includes an easy way to discover details about any connected IEDs in the network. Login to the CVC GUI and navigate to the **Search** tab on the left. Enter the IP address of a connected IED in the **Asset Search** field to display more details as shown below.

Legacy SCADA

Legacy SCADA is the way of transporting the stream of characters from one serial to another in the utility applications. This section describes how Cisco IR1101 is used to transport the serial data via IP network.

Figure 65 Legacy SCADA Flow



Raw Socket

Raw socket is a method of transporting serial data through an IP network. This feature can be used to transport SCADA data from Remote Terminal Units (RTUs). Raw Socket supports TCP or UDP as transport protocol. An interface can be configured anyone protocol but not both at the same time. This section shows the sample configuration for raw socket TCP on Cisco IR1101.

Serial interface configuration

```
GRID-IR1101#sh run int Async 0/2/0
Building configuration...

Current configuration : 66 bytes
!
interface Async0/2/0
 no ip address
 encapsulation raw-tcp
end
```

Corresponding line configuration

```
GRID-IR1101#sh run | sec line 0/2/0
line 0/2/0
 raw-socket tcp server 25000 192.168.150.16
 raw-socket special-char 7
 raw-socket packet-timer 500
 raw-socket packet-length 32
 transport preferred none
 stopbits 1
 databits 8
 parity none
```

In the above configuration IR1101 acts as a TCP server which listens on port 25000 (Port numbers vary for Modbus) and local binding IP of 192.168.150.16

Modbus

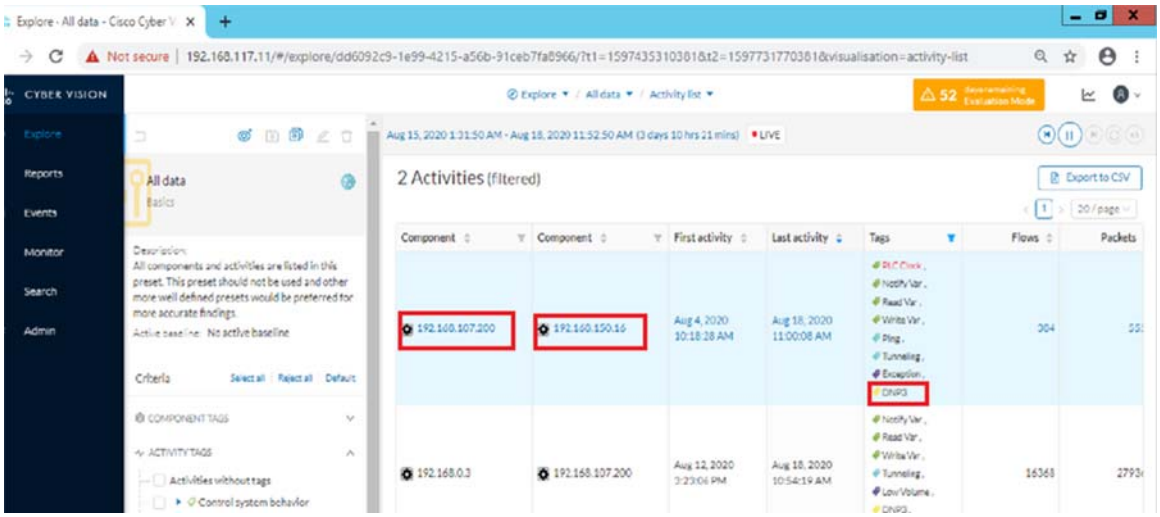
Cisco IR1101 supports transporting MODBUS serial over Raw Socket, but the Deep Packet Inspection of OT visibility is not supported in Cisco CyberVision Center. The same will be supported in future release. The configuration of raw-socket TCP on Cisco IR1101 is in the Raw Socket section.

Note: DDTS CSCvu86798 has been raised to track the feature support on Cisco CyberVision Center.

DNP3

Cisco IR1101 supports transporting DNP3 serial over Raw Socket and the deep packet inspection of OT traffic can be seen in Cisco CyberVision Center. Refer to the of raw-socket configuration of TCP on the Cisco IR1101 in the Raw Socket section.

Figure 66 Activities List for Raw Socket DNP3



Next click on this activity and navigate to **Flows** as shown below.

Figure 67 Total Flows for DNP3

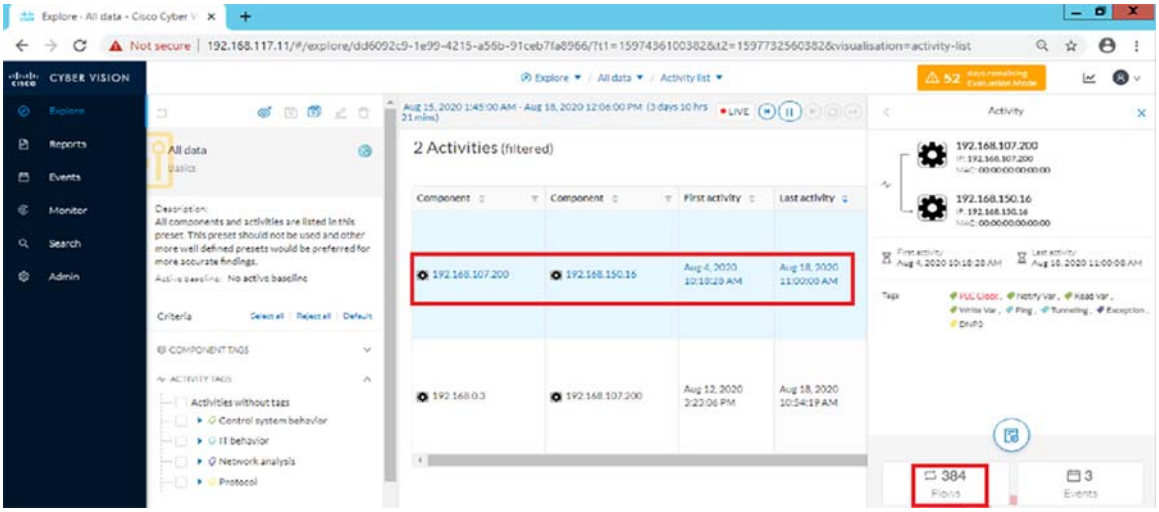


Figure 68 Flow Properties of Raw Socket DNP3

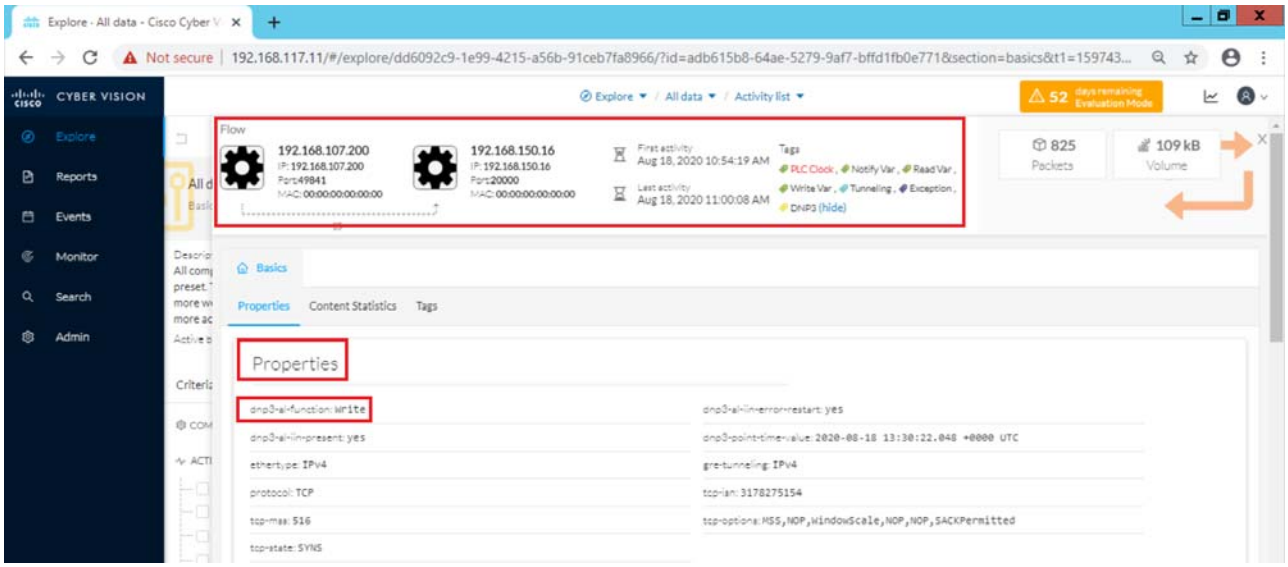
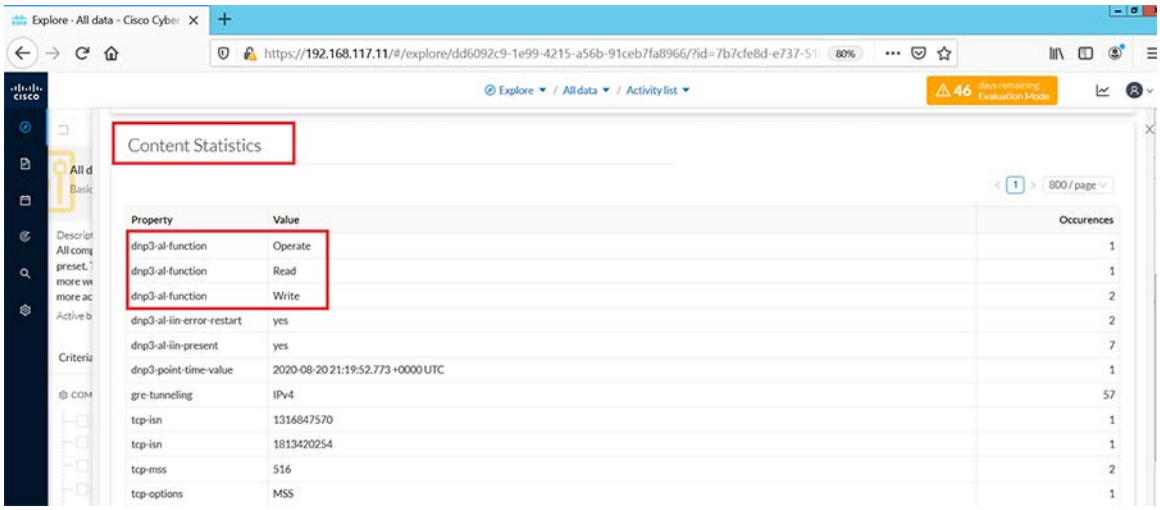
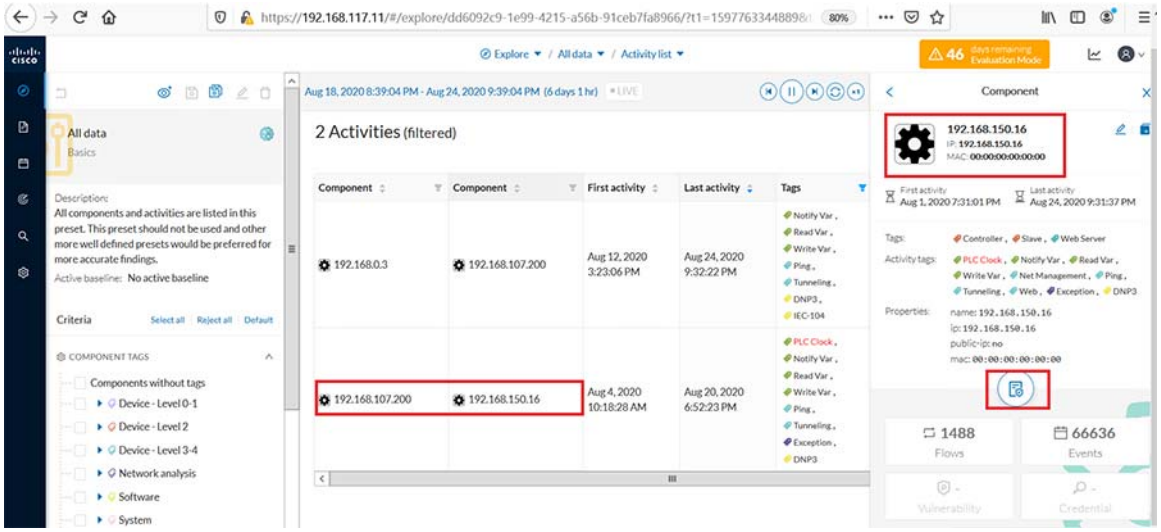


Figure 69 Flow Contents of Raw Socket DNP3



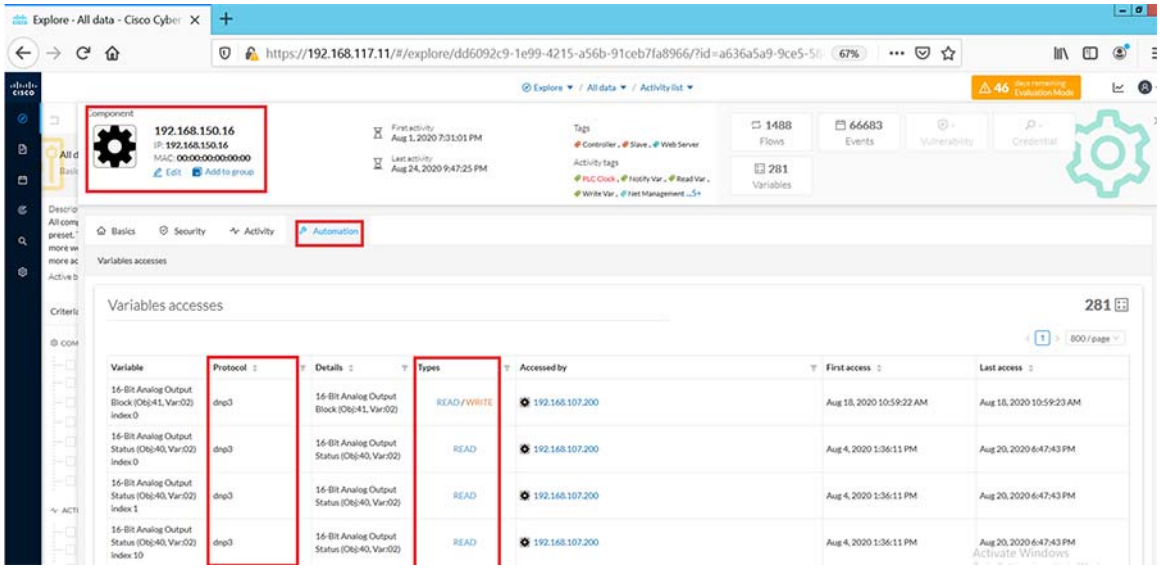
In the above figure, various operations performed such as read/write can be observed under **Flow** content statistics which can be viewed by selecting the SCADA FEP (192.168.107.200) and clicking on **Flows**.

Figure 70 Technical sheet for Raw Socket DNP3



In the above figure, 192.168.150.16 is the Tunnel IP of IR1101 where the Raw-socket terminates. Select **SCADA IEDs(192.168.150.16)** and click on the **Technical sheet** to observe the variables accessed for DNP3 by SCADA FEP.

Figure 71 Variable Accessed for Raw Socket DNP3



In the above figure, we can view the DNP3 variables accessed by SCADA FEP on IEDs.

Protocol Translation

In the network, the Control Center always serves as the master in the network when communicating with the IR1101. The IR1101 serves as a proxy master station for the Control Center when it communicates with the RTU.

The IR1101 provides protocol translation to serve as a SCADA gateway to do the following:

- Receive data from RTUs and relay configuration commands from the Control Center to RTUs.

- Receive configuration commands from the Control Center and relay RTU data to the Control Center.
- Terminate incoming requests from the Control Center, when an RTU is offline.

The IR1101 performs Protocol Translation for the following protocols:

- IEC 60870 T101 to/from IEC 60870 T104.
- DNP3 serial to DNP3 IP.

T101/T104 Protocol Translation

In this scenario, the RTU is connected to the Cisco IR1101 via the serial or Ethernet port, then the SCADA control and the RTU can communicate via Cisco IR1101 as the SCADA gateway. The communication between the RTU and SCADA control station can be Ethernet based (T104) or RS232 serial communication (T101) or by means of protocol translation. For each of these operations being performed, refer to the Flow diagram showing T104/T101 control flow in the DA Secondary Substation Implementation Guide available at the below location.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG/DA-SS-IG-doc.html#pgfId-296649

IR1101 SCADA Gateway Configuration

Line Configurations:

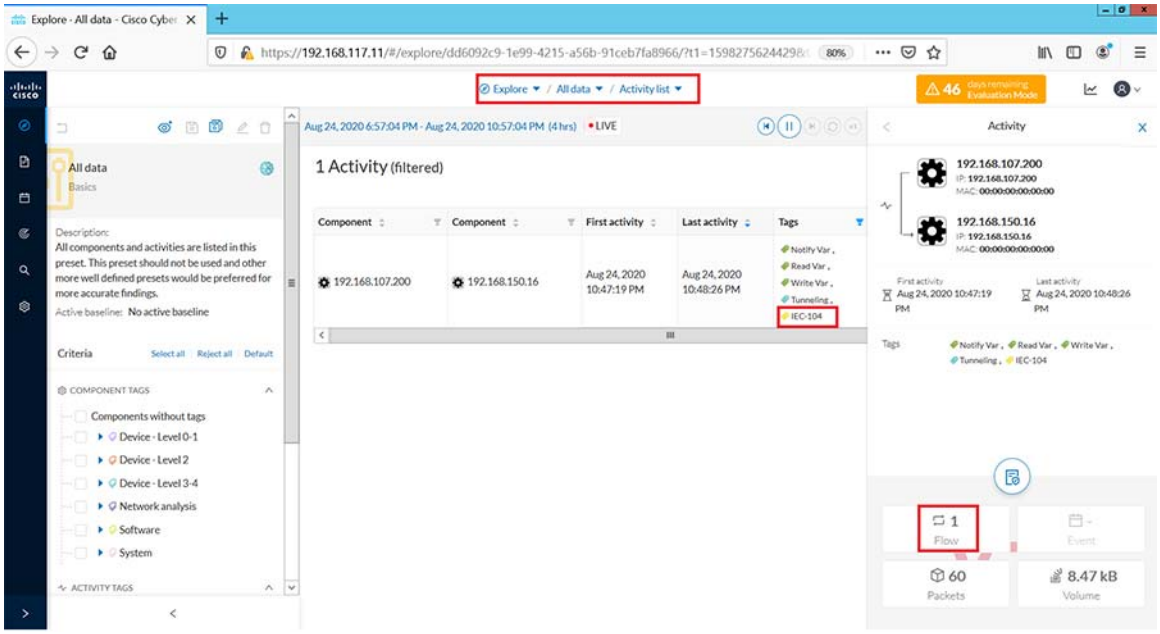
```
line 0/2/0
databits 8
stopbits 1
speed 9600
parity none
!

Serial Interface Configuration:

interface Async0/2/0
no ip address
encapsulation scada
!
```

SCADA Gateway for T101/T104 configuration:

```
scada-gw protocol t101
channel T101_ch1
  link-addr-size two
  bind-to-interface Async0/2/0
session T101_ses1
  attach-to-channel T101_ch1
  link-addr 13
sector T101_sec1
  attach-to-session T101_ses1
  asdu-addr 14
scada-gw protocol t104
channel T104_ch1
  t3-timeout 20
  tcp-connection 0 local-port default remote-ip 192.168.107.200
session T104_ses1
  attach-to-channel T104_ch1
sector T104_sec1
  attach-to-session T104_ses1
  asdu-addr 15
  map-to-sector T101_sec1
!
scada-gw enable
```

Once the above configurations are made on IR1101, it acts as a SCADA-GW for translating the T101 to/From T104. In the above case T104 is the SCADA FEP and T101 is the SCADA RTU.

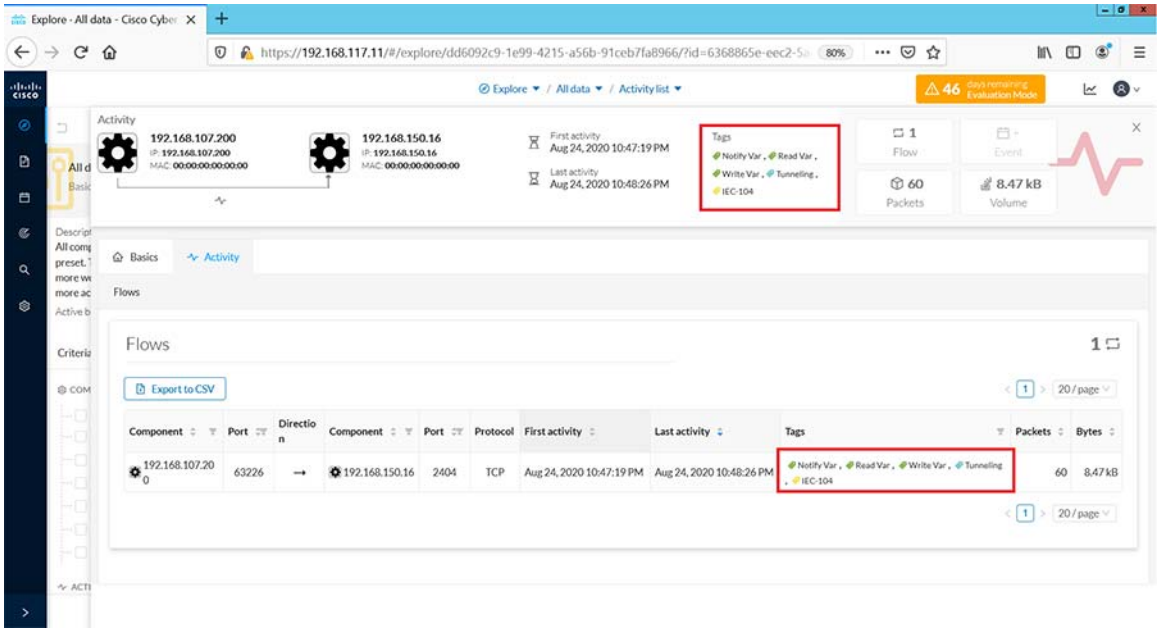
Figure 72 Activity list and Total Flows for Protocol Translation



Log in to the CVC and navigate to **All Data > Activity** list under the **Explore** tab. Look for the tags associated with **IEC-104** and identify the activity of the associated systems exchanging T104 traffic as shown below.

Click on this activity and navigate to **Flows** as shown below.

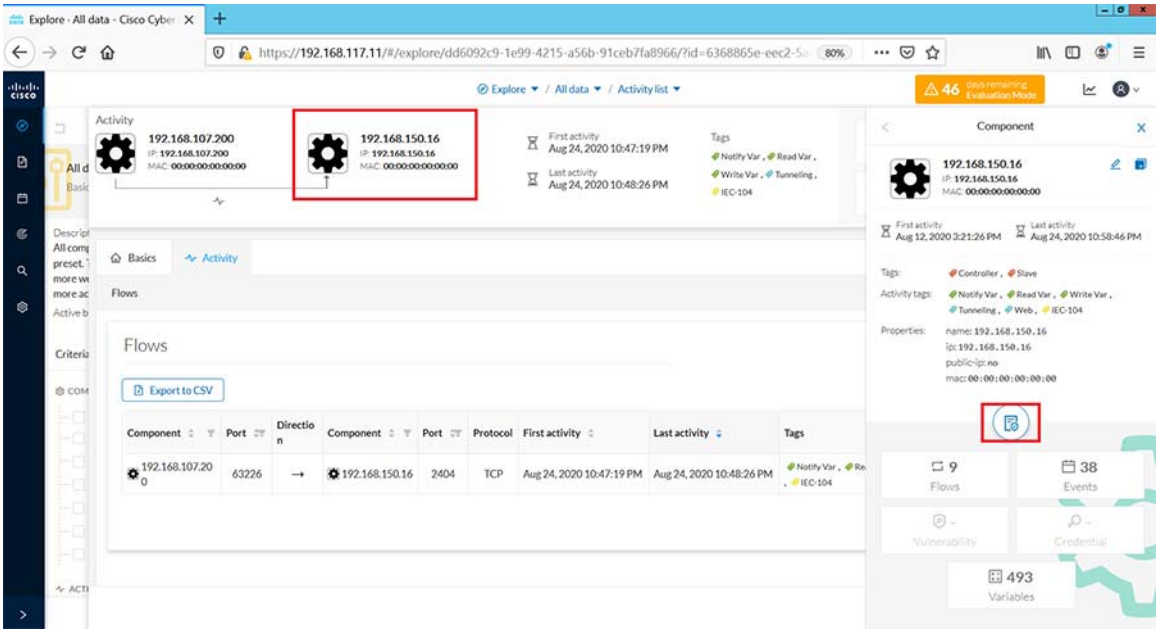
Figure 73 Tags and Flow Exchanges for Protocol Translation



Under the activity selected, filter the tags for I**EC104** and view the flow exchanges and tags applied for protocol translation.

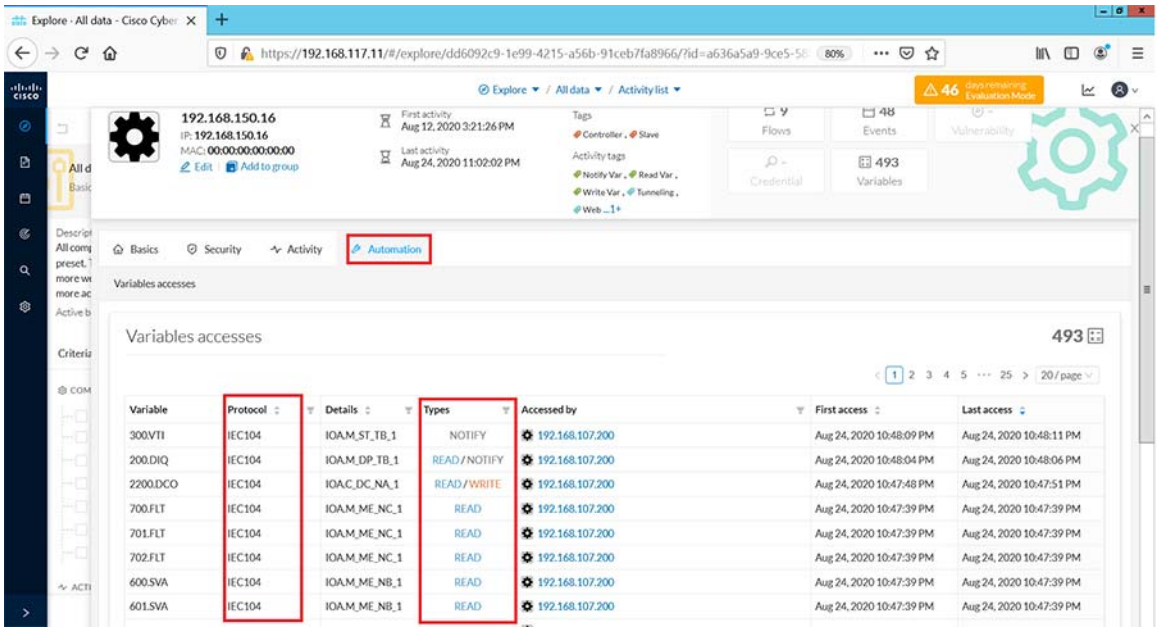
Click on the flows listed for IEC-104 one at a time to view more details about the flow properties. Look at the sub-tabs such as **Properties** or **Content** statistics to obtain more information on the operations performed. To obtain deeper visibility into the variables accessed for each operation, click on the component SCADA RTU (192.168.150.16) in the **Activity** panel on top of the **Flows** window as shown below. Next click on the **Technical sheet** for this component.

Figure 74 Technical Sheet for Protocol Translation



Next click on **Automation** tab and under the column displayed for protocol, filter for **IEC104** information.

Figure 75 Variables Accessed for Protocol Translation



This would display information on the different variables accessed for each IEC104 operation performed as shown above. While Read and Write operations are indicated as is, Unsolicited operations are indicated as NOTIFY under the **Variable Types** column.

OT Assets Anomaly Detection-Monitoring

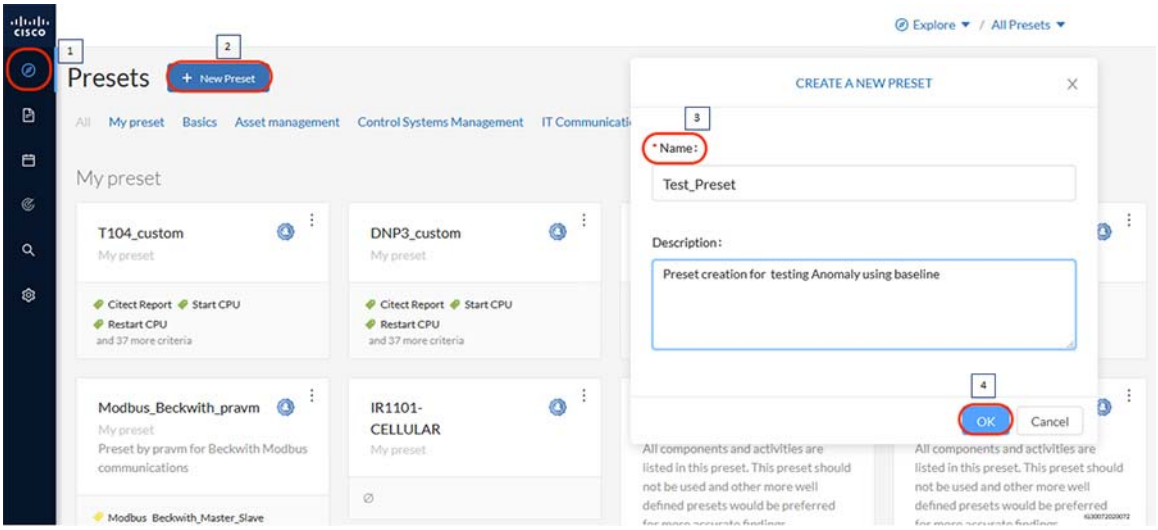
To detect changes within industrial networks, CVC provides a monitoring tool called Monitor mode which shows changes in network states from the baselines. Changes, either normal or abnormal, are noted when differences are found between a baseline and a comparison point. Comparisons that have been performed are reported in the Events pages. Events generated by CVC are used to identify and keep track of significant activities in the network like an activity, a property, or a change pertaining to hardware or software components.

In monitor mode, you will create an initial baseline which is a snapshot of the network state considered normal at a defined time of an outstation component and its controller or SCADA Front End Processor. The next step is to make a network change such as a flow trying to access a component or trying to modify variables and check if CVC detects this change and reports it as an event.

Follow the steps below for this example.

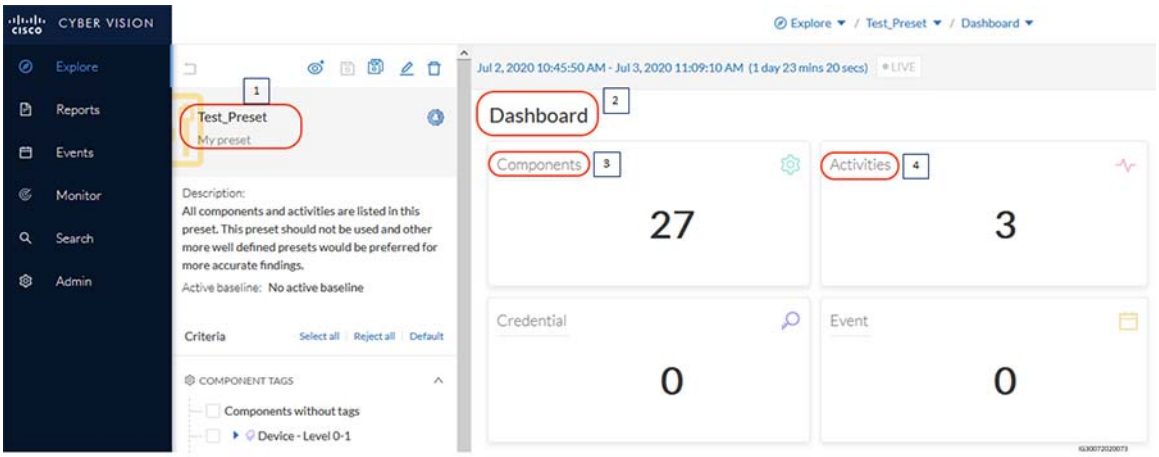
1. Create a preset named *Test_Preset* as shown in the following figure.

Figure 76 Create New Preset



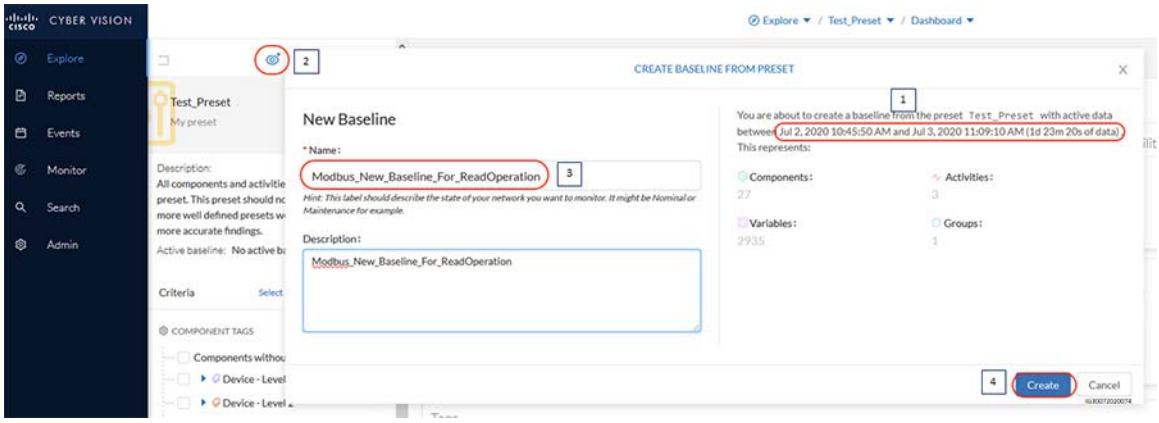
2. Select the created preset and check if the desired data like components, related activities, etc. are reflected as highlighted.

Figure 77 View Preset



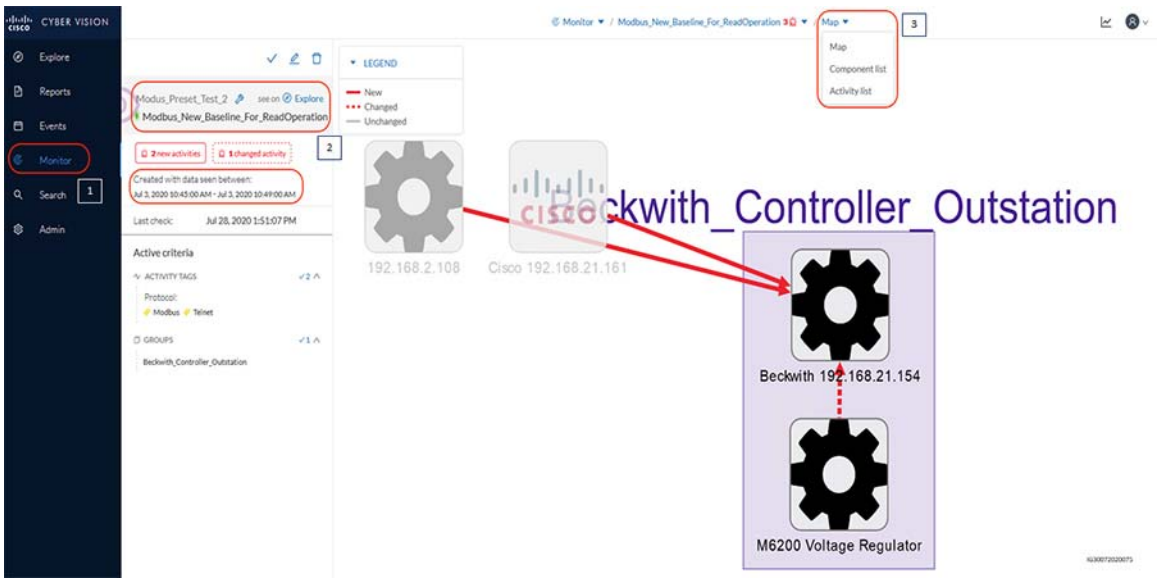
3. Create a baseline named ‘Modbus_New_Baseline_For_ReadOperation’ as shown in the following figure and click on **Create**. Ensure that the period for which baseline needs to be created is selected appropriately. It can be ensured by setting the time period in the preset created.

Figure 78 Creating a Baseline



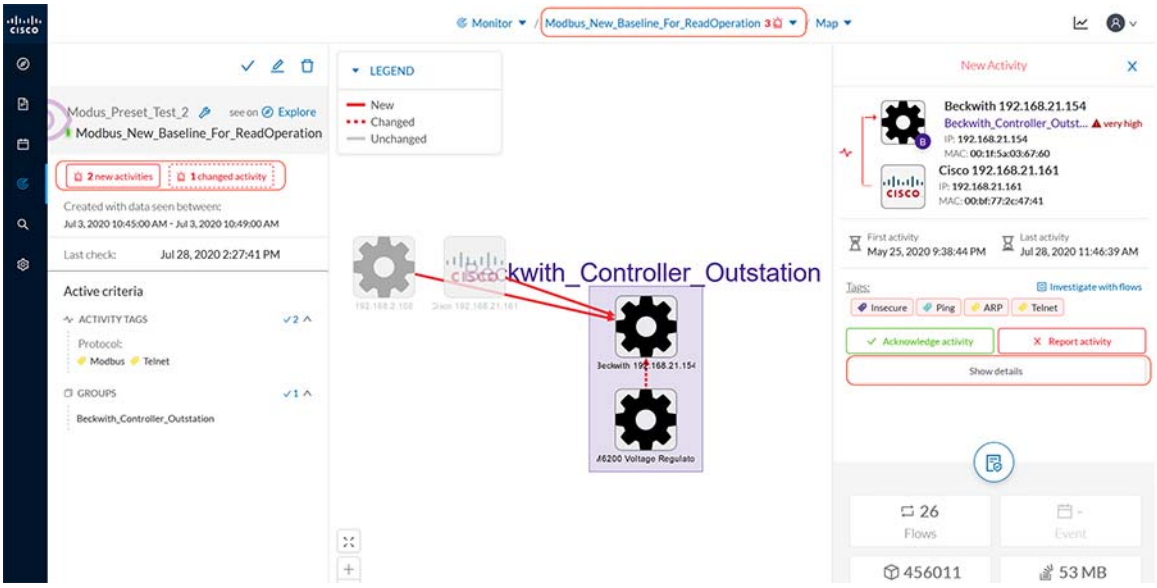
4. Once the baseline is created, the network map, the list of various components, activities, and variables in the network can be detected as highlighted in the following figure.

Figure 79 Viewing Baseline details



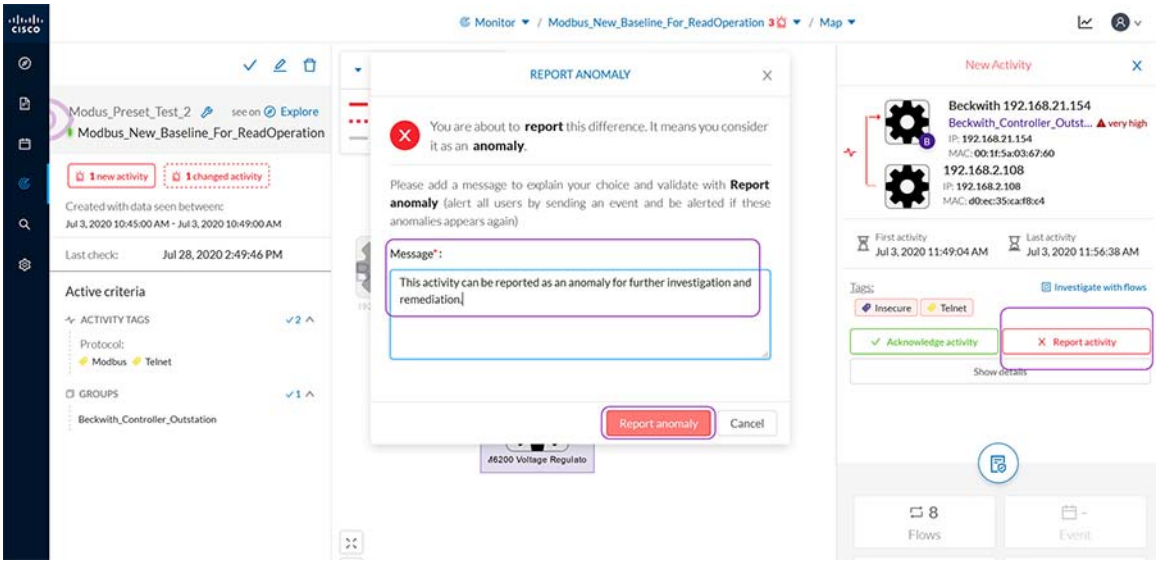
5. As described earlier, try to establish a connection to the outstation from different devices and also try to modify variables that are not part of the baseline. CVC should detect the changes as highlighted in the following figure.

Figure 80 CVC Detecting Changes in Baseline



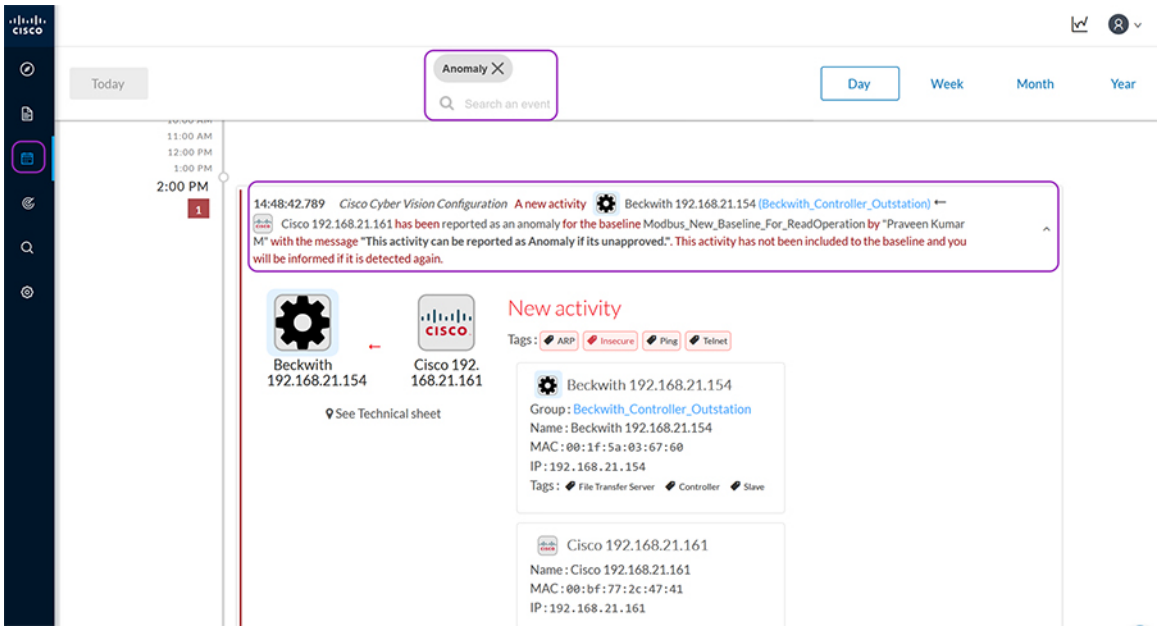
6. The CVC provides an option to either acknowledge the activity and approve or report the activity for further analysis and remediation if required. The following snapshot shows the steps to report the activity as an Anomaly.

Figure 81 Report Anomaly



7. CVC provides a separate category of events for Anomaly detection. To view these events, navigate to the **Events** page in the CVC GUI and search for **Anomaly** as shown below. The Anomaly events can also be sent to syslog servers with appropriate configuration. Click on the event to view more details about the new activity in the network as shown below. Notice that this is the same information seen from the Monitor mode page on doing a comparison with the baseline.

Figure 82 View Anomaly Detection Events



Refer to the following guide for more details and options that are available to configure baseline for detecting anomalies.

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_Release_3_1_0.pdf

Threat Detection

SCADA Modbus Preprocessor on ISA3000

Cisco ISA3000 Application identification goes beyond traditional port numbers and inspecting the entire frame to recognize the protocol/application. Most of the Industrial Firewalls in the market recognize protocols/applications using the port numbers. Using just the port numbers leads to misidentification when protocols are overloaded on the same port numbers.

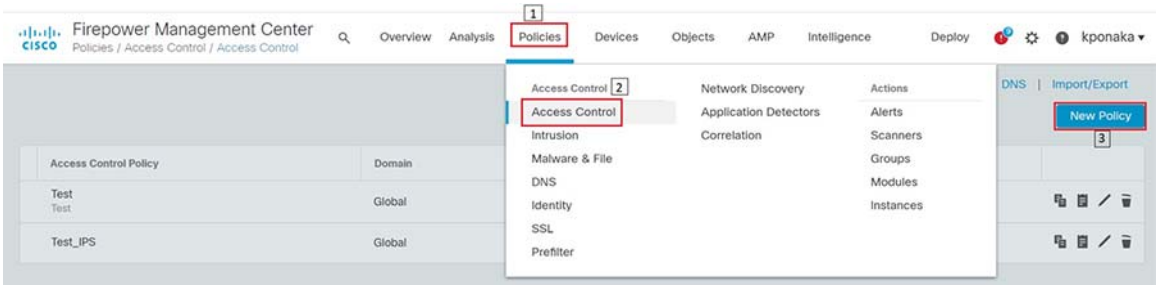
In this scenario, you will explore the OT Application identification supported on Cisco ISA3000. This allows you to see the OT protocols supported on Cisco ISA3000. You can experiment with creating rules to control OT traffic. An example of this is to allow Modbus TCP traffic and deny other protocols.

For details on the list of different OT protocols supported on ISA3000 refer to the following link.
https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-appliance-3000/data-sheet-c78-735839.pdf

Summary

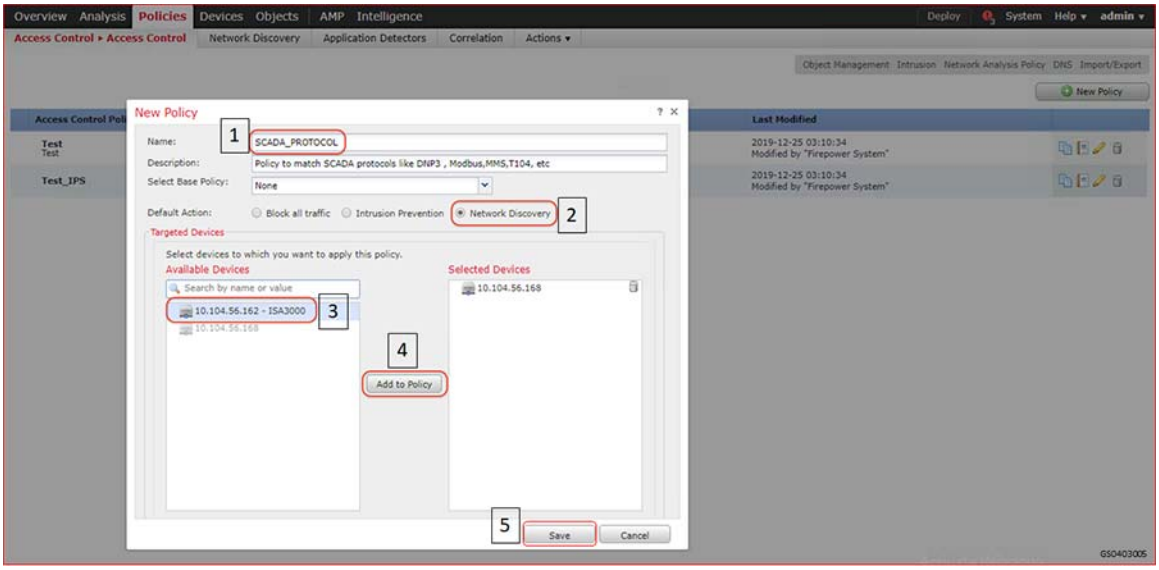
Navigate to **FMC > Policies > Access Control** as highlighted in the following figure. Click **Access Control**.

Figure 83 SCADA Preprocessor Creating New Access Control Policy



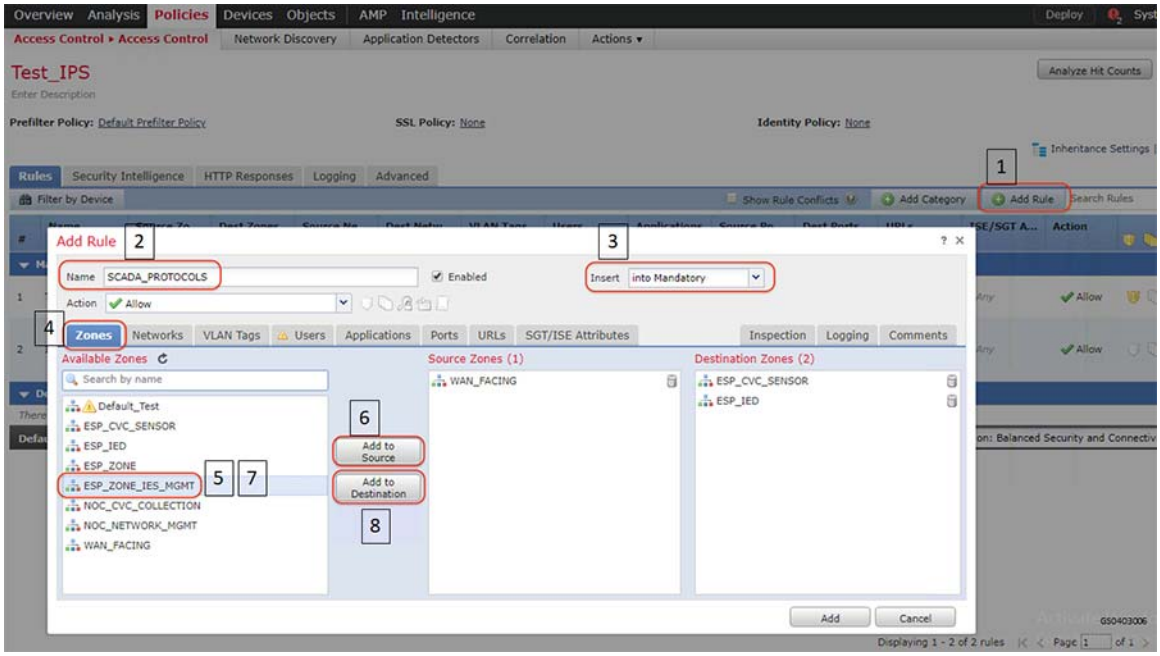
Enter access policy details like name, default action, and the device on which the policy should be applied as highlighted in the following figure.

Figure 84 SCADA Preprocessor New Access Control Policy properties



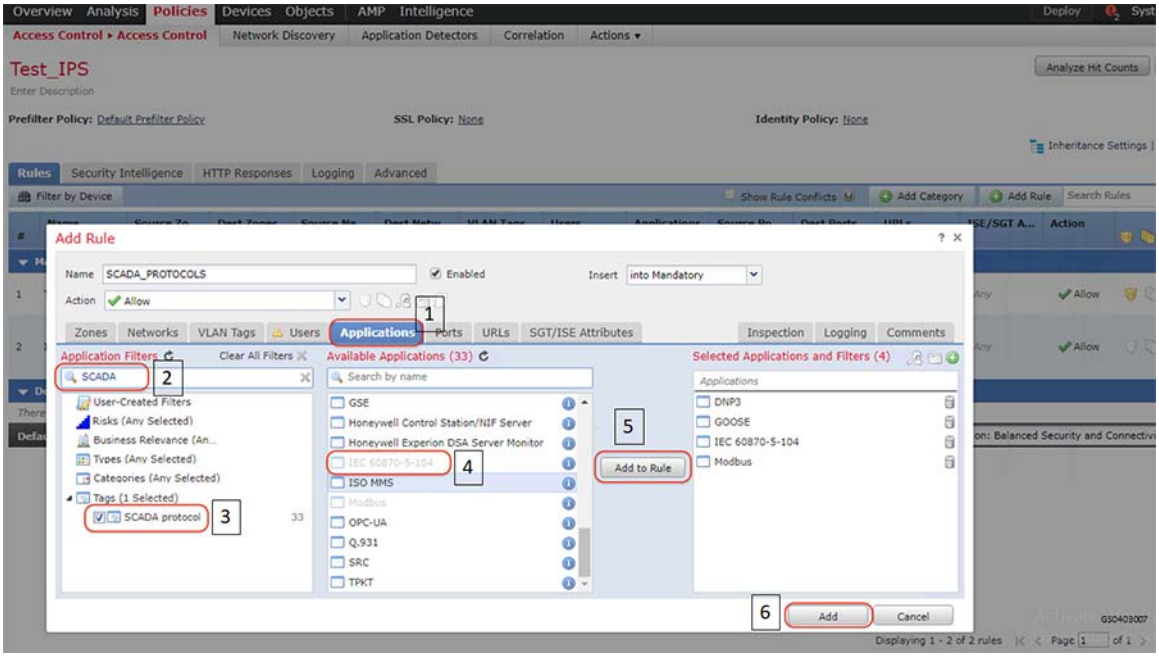
Click **Add Rule**, and then select zones as highlighted in the following figure.

Figure 85 SCADA Preprocessor Adding New Rule to the New Access Control Policy



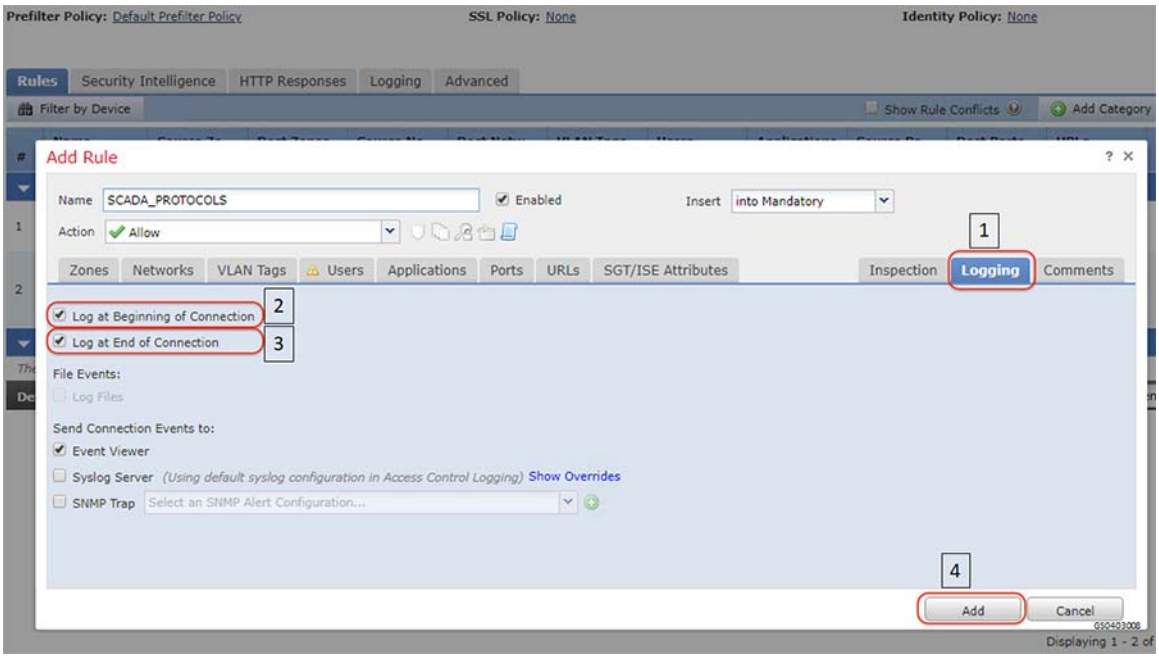
Click the **Applications** tab and select protocols of interest as highlighted in the following figure.

Figure 86 SCADA Preprocessor Selecting Applications for the New Rule



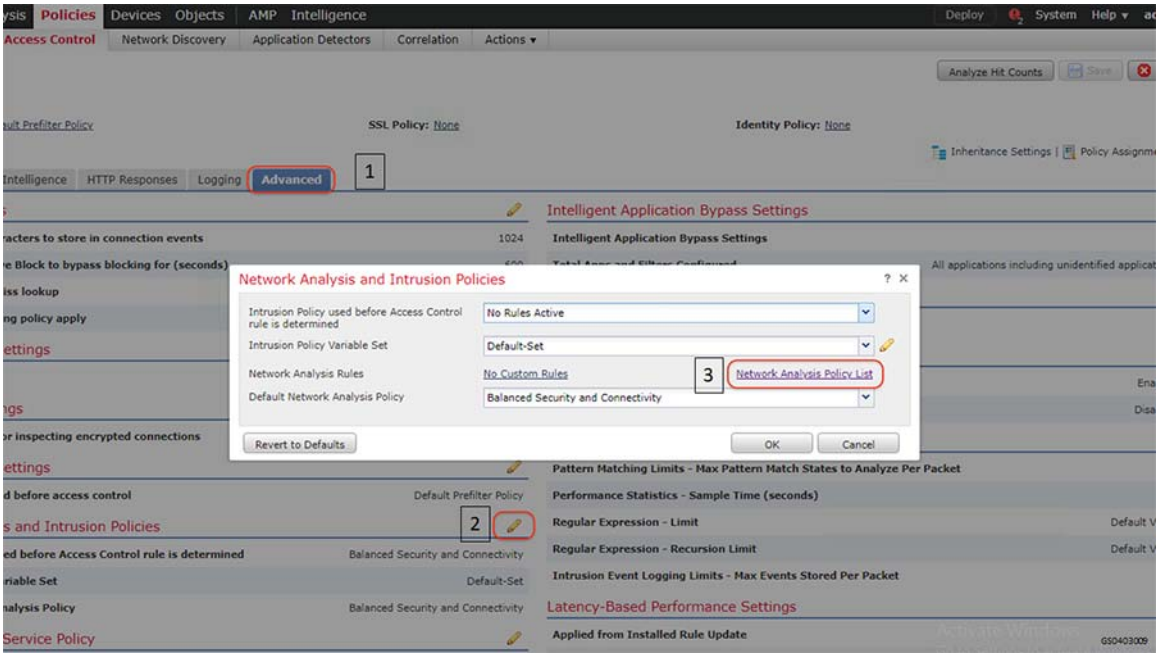
Enable logging by following the steps highlighted in the following figure.

Figure 87 SCADA Preprocessor Enabling Logging for the New Rule



After the rule is added, click the **Advanced** tab and proceed as highlighted in the following figure. Click **Network Analysis Policy List** to open the next window.

Figure 88 SCADA Preprocessor Network Analysis Policy

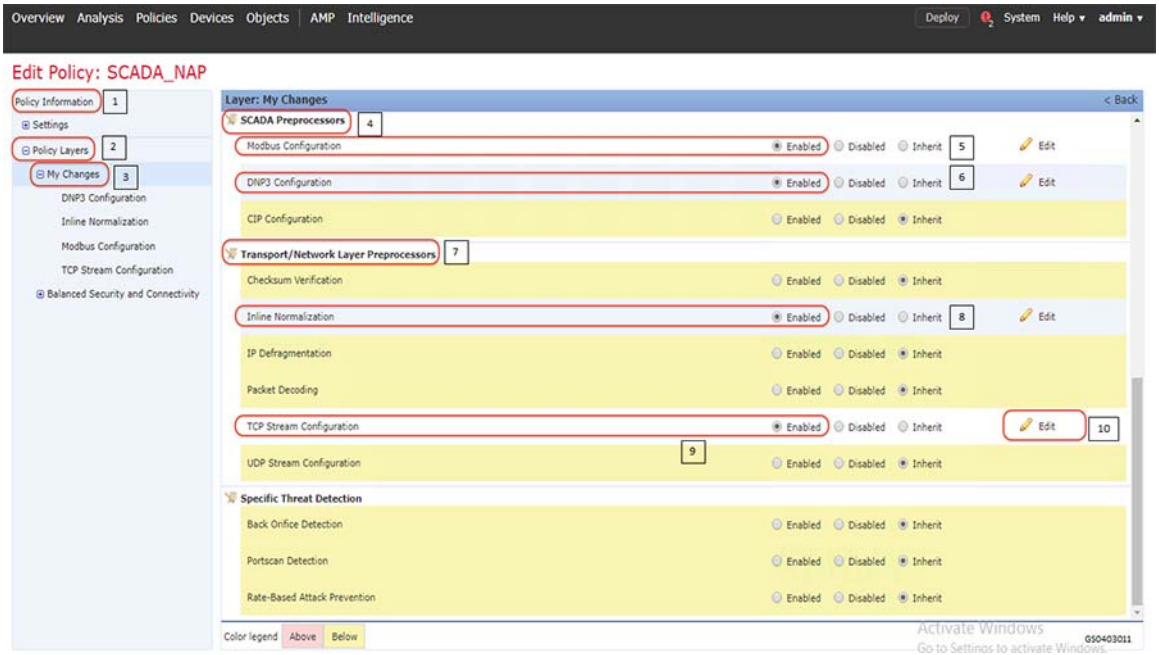


Click the **Create Policy** button and follow the steps as highlighted in the following figure.

Figure 89 SCADA Preprocessor Creating new Network Analysis Policy

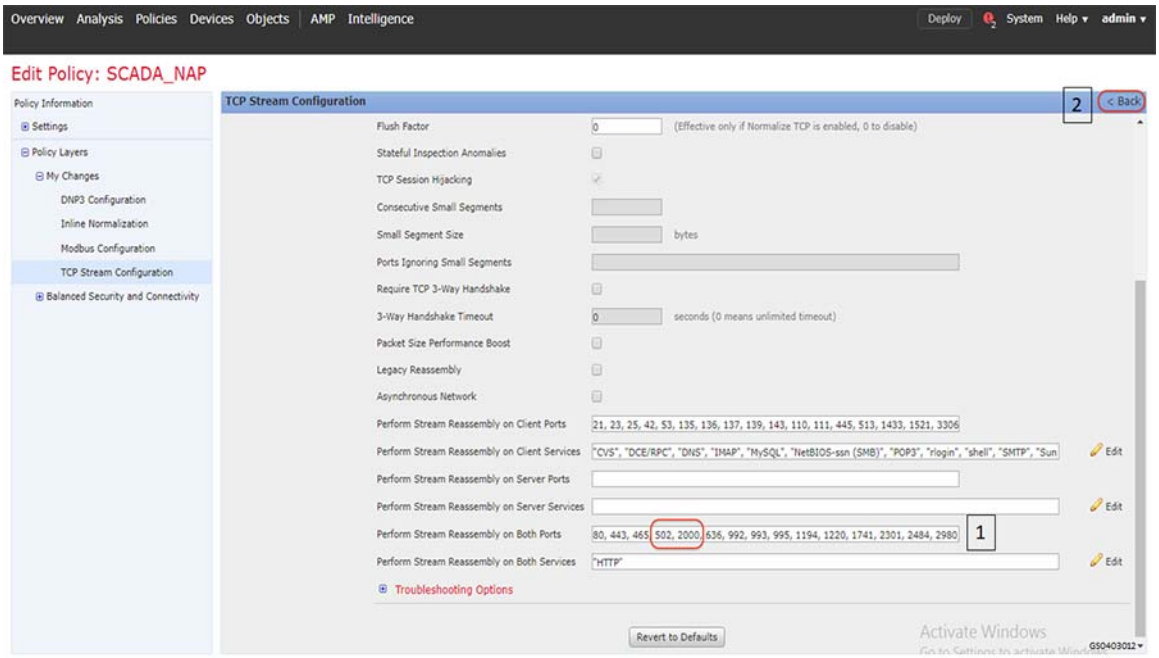
Click **My Changes** option listed under **Policy Layers** on the left hand side of the resulting window and follow the steps as highlighted in the following figure.

Figure 90 SCADA Preprocessor Editing Network Analysis Policy



Clicking the **Edit** button across TCP Stream Configuration as highlighted by number 10 in the previous figure, results in a new window. Scroll down to “Perform Stream Reassembly on Both Ports” settings and add ports **502** for Modbus and **2000** for DNP3. Click **Back** after modifications. Refer to highlights in the following figure.

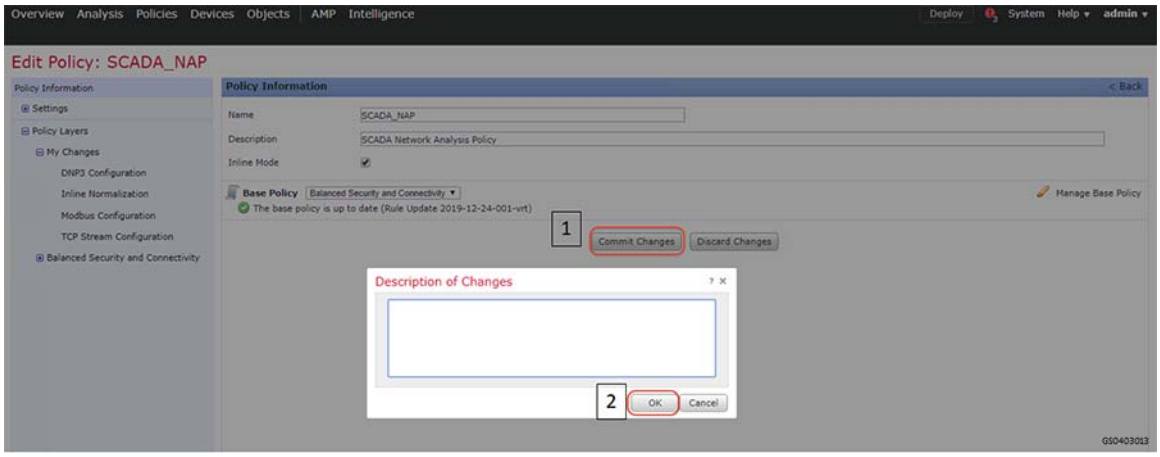
Figure 91 Preprocessor Adding Protocol properties



Click **Back** in the resulting window.

Click **Commit Changes** and proceed as highlighted in the following figure. The resulting window lists the newly-created policy.

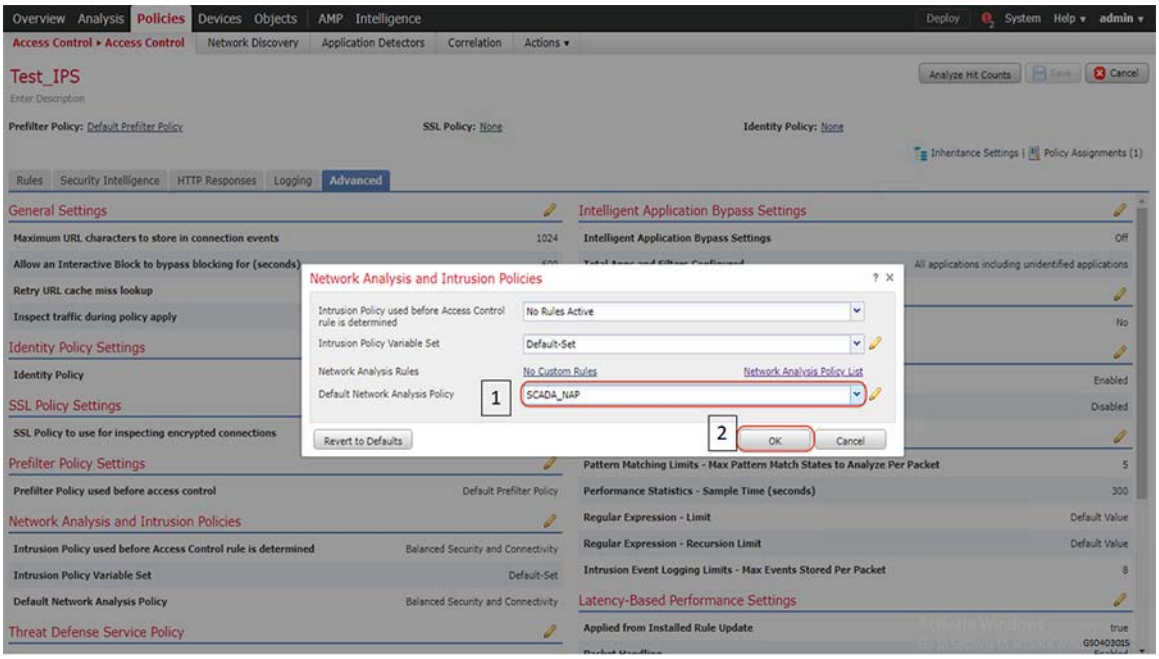
Figure 92 SCADA Preprocessor Commit new Network Analysis Policy



Navigate to the original window shown in Step 6 above.

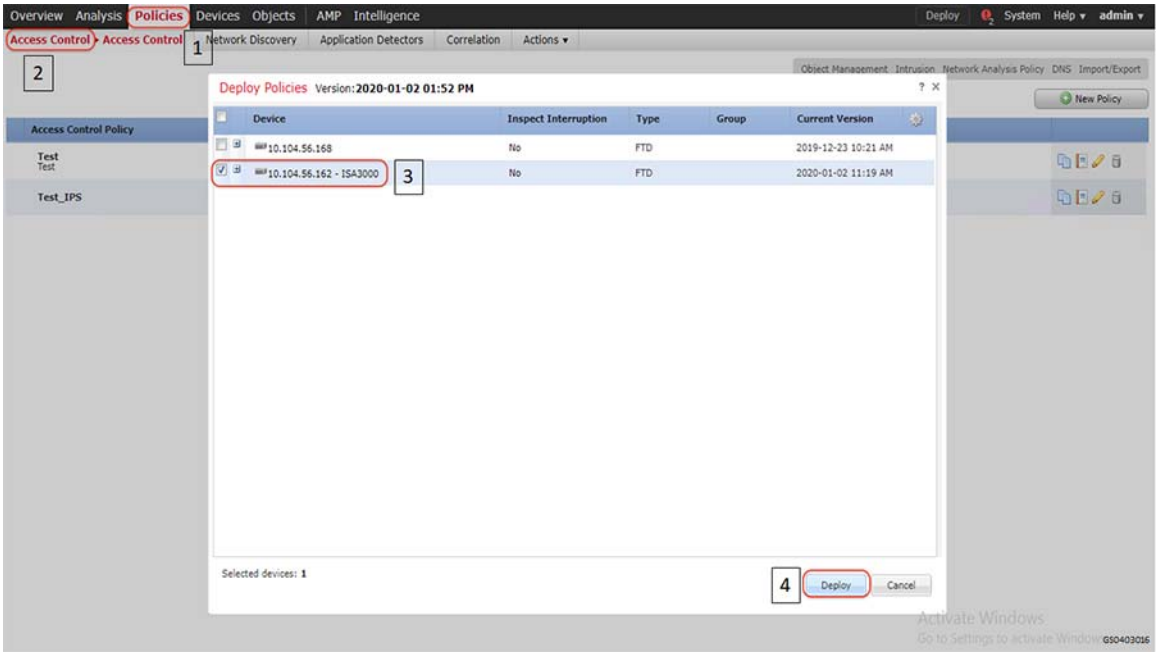
Click **Create Policy** button and follow the steps as highlighted in the following figure. The newly-created policy is listed in the drop down list for Default Network Analysis Policy. Select the appropriate policy and click **OK**. Save the policy by clicking **Save** button.

Figure 93 SCADA Preprocessor selecting new Network Analysis Policy



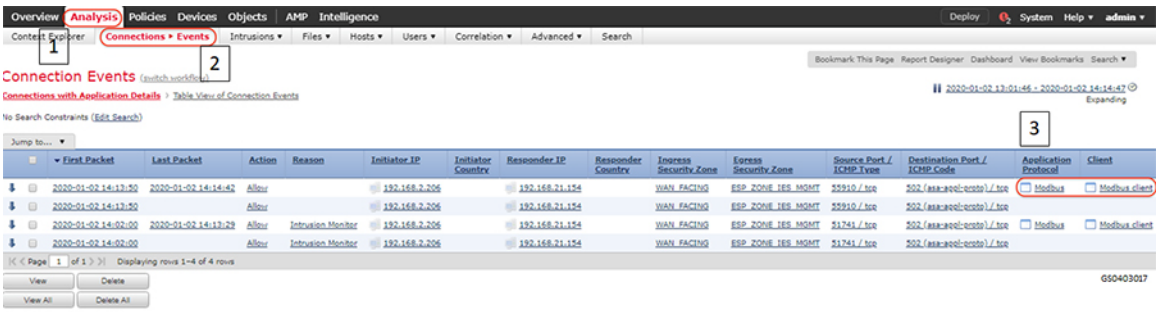
Deploy the policy on the intended device as highlighted in the following figure.

Figure 94 SCADA Preprocessor Deploying new Policy Verification



Initiate traffic and check if the applied policy classifies and identifies the type of application and the protocol it uses. This scenario was validated with Modbus application and firewall policy applied on ISA3000 as highlighted in the following figure.

Figure 95 SCADA Preprocessor verifying newly created Network Analysis Policy



SCADA DNP3 Preprocessor on ISA3000

Cisco ISA3000 Application identification goes beyond traditional port numbers and inspecting the entire frame to recognize the protocol/application. Most of the Industrial Firewalls in the market recognize protocols/applications using the port numbers. Using just the port numbers leads to misidentification when protocols are overloaded on the same port numbers.

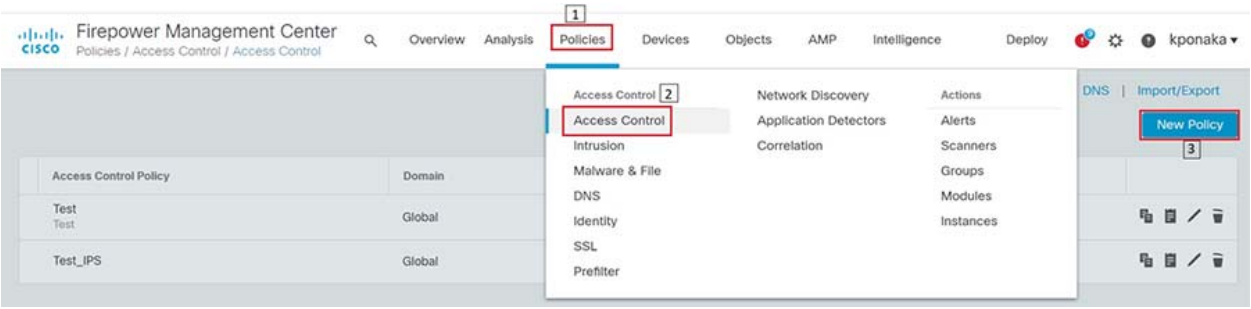
In this scenario, you will explore the OT Application identification supported on Cisco ISA3000. This allows you to see the OT protocols supported on Cisco ISA3000. You can experiment with creating rules to control OT traffic. An example of this is to allow **DNP3 traffic** and deny other protocols.

For details on the list of different OT protocols supported on ISA3000 refer to the following link. https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-appliance-3000/data-sheet-c78-735839.pdf

Summary

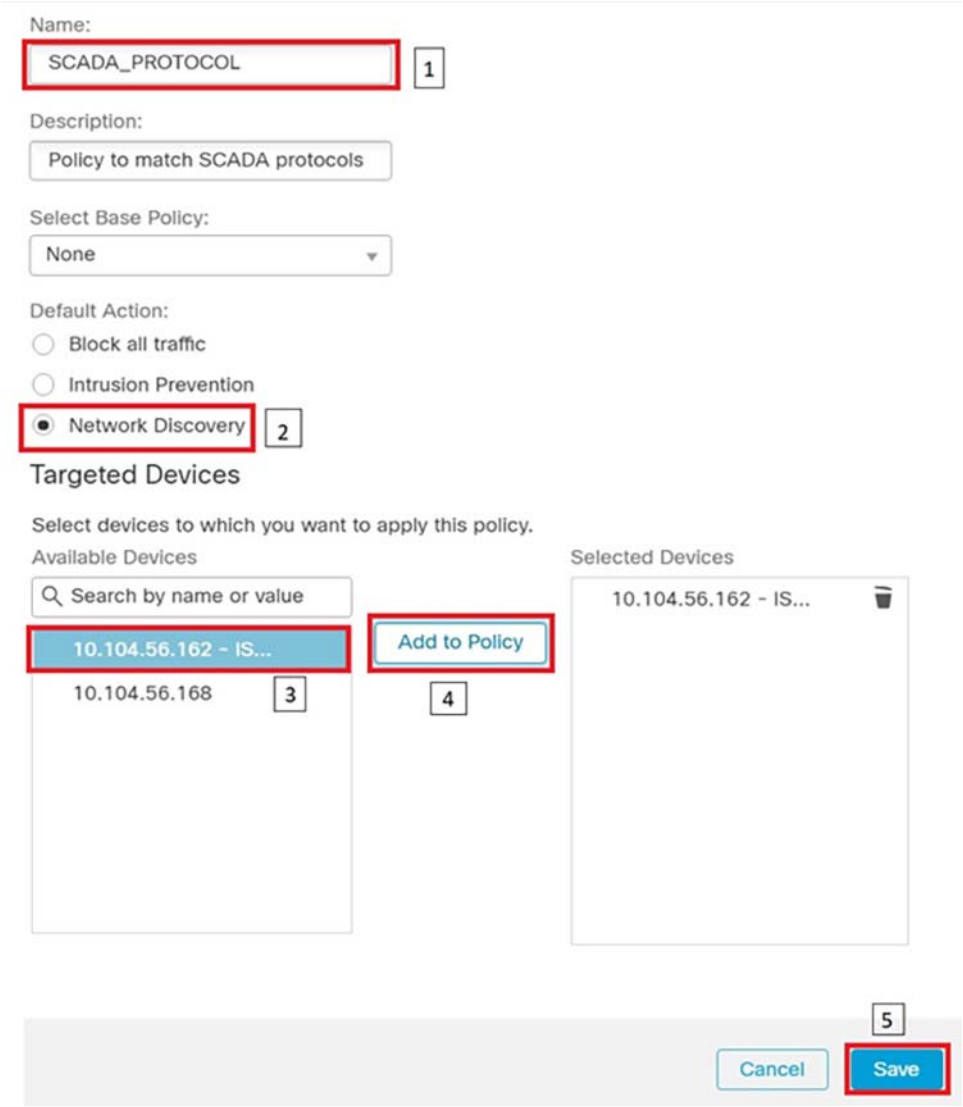
Navigate to **FMC > Policies > Access Control** as highlighted in the following figure. Click **Access Control**.

Figure 96 SCADA Preprocessor Creating New Access Control Policy



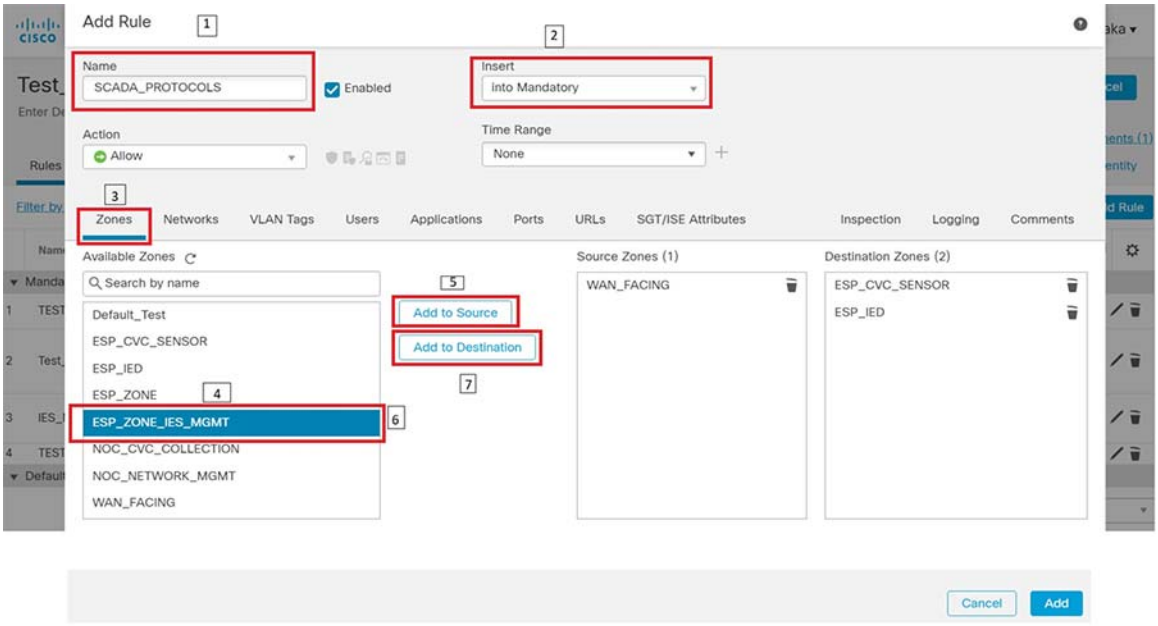
Enter access policy details like Name, default action and the device on which the policy should be applied as highlighted in the following figure.

Figure 97 SCADA Preprocessor New Access Control Policy properties



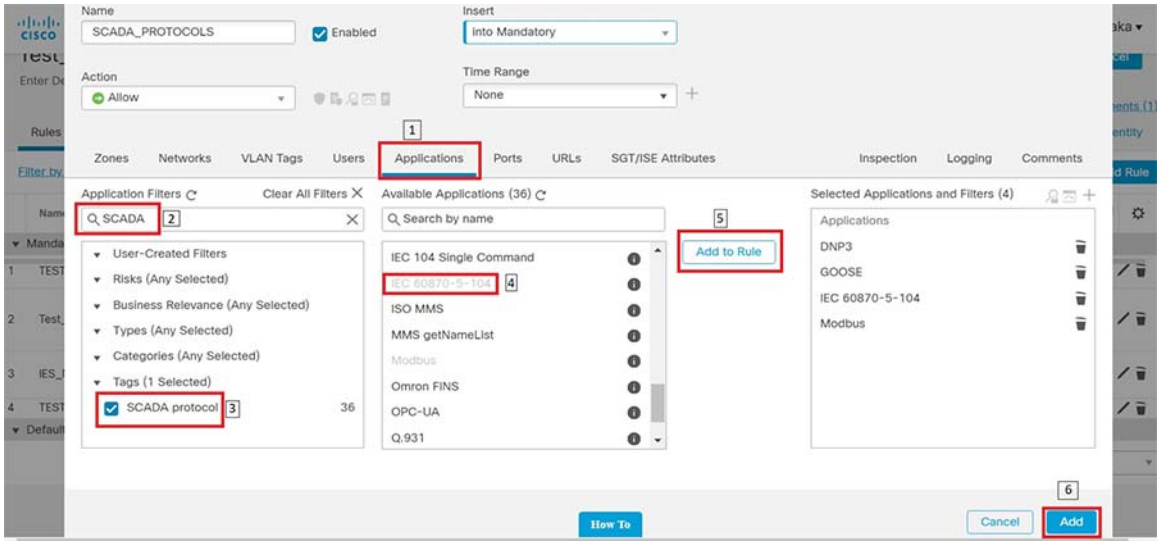
Click **Add Rule**, and then select zones as highlighted in the following figure.

Figure 98 SCADA Preprocessor Adding New Rule to the New Access Control Policy



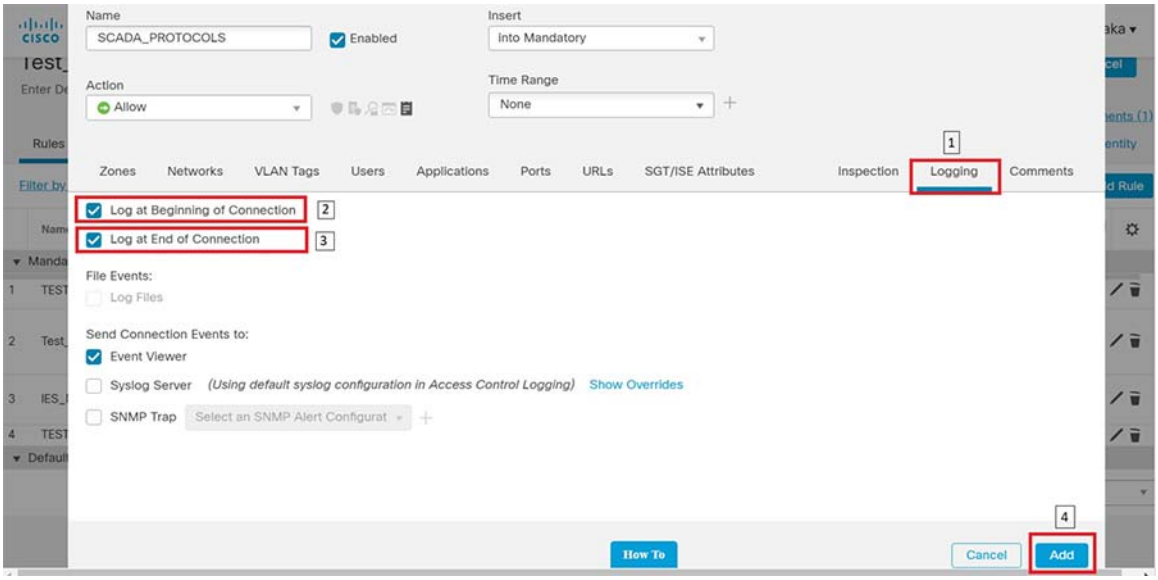
Click the **Applications** tab and select protocols of interest as highlighted in the following figure.

Figure 99 SCADA Preprocessor Selecting Applications for the New Rule



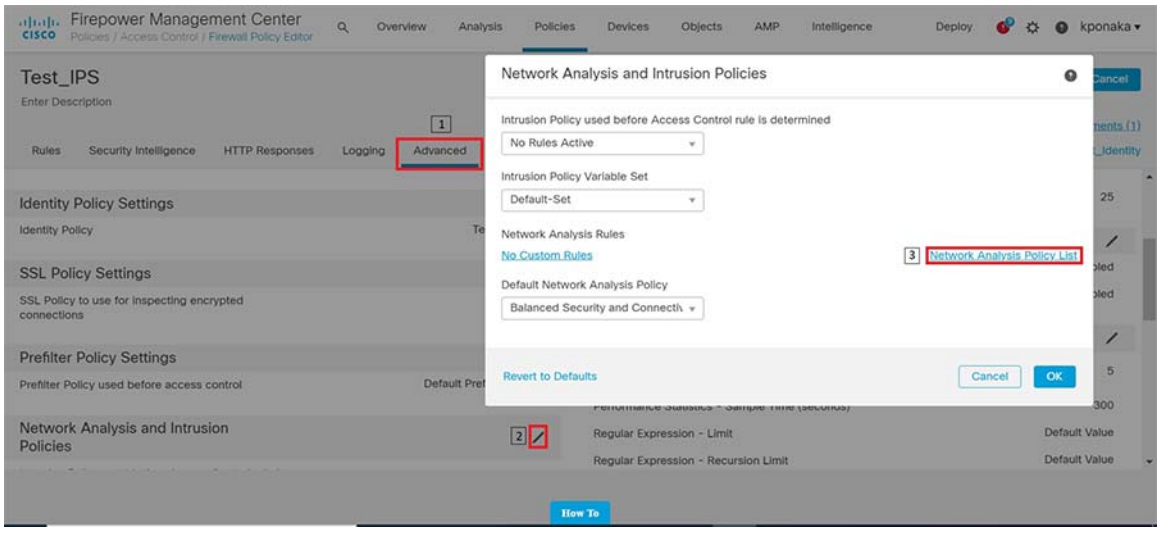
Enable logging by following the steps highlighted in the following figure.

Figure 100 SCADA Preprocessor Enabling Logging for the New Rule



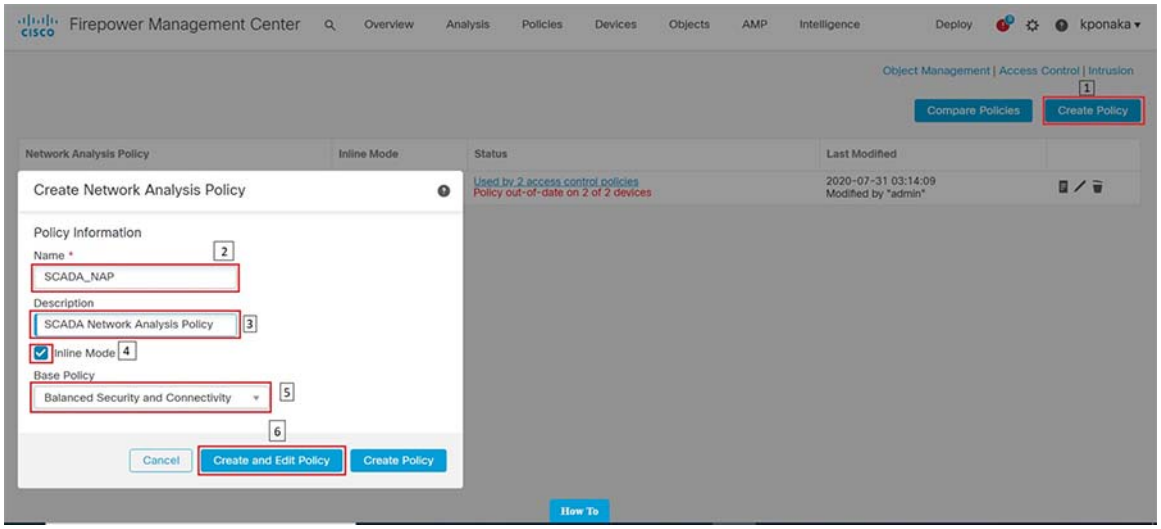
After the rule is added, click the **Advanced** tab and proceed as highlighted in the following figure. Click **Network Analysis Policy List** to open the next window.

Figure 101 SCADA Preprocessor Network Analysis Policy



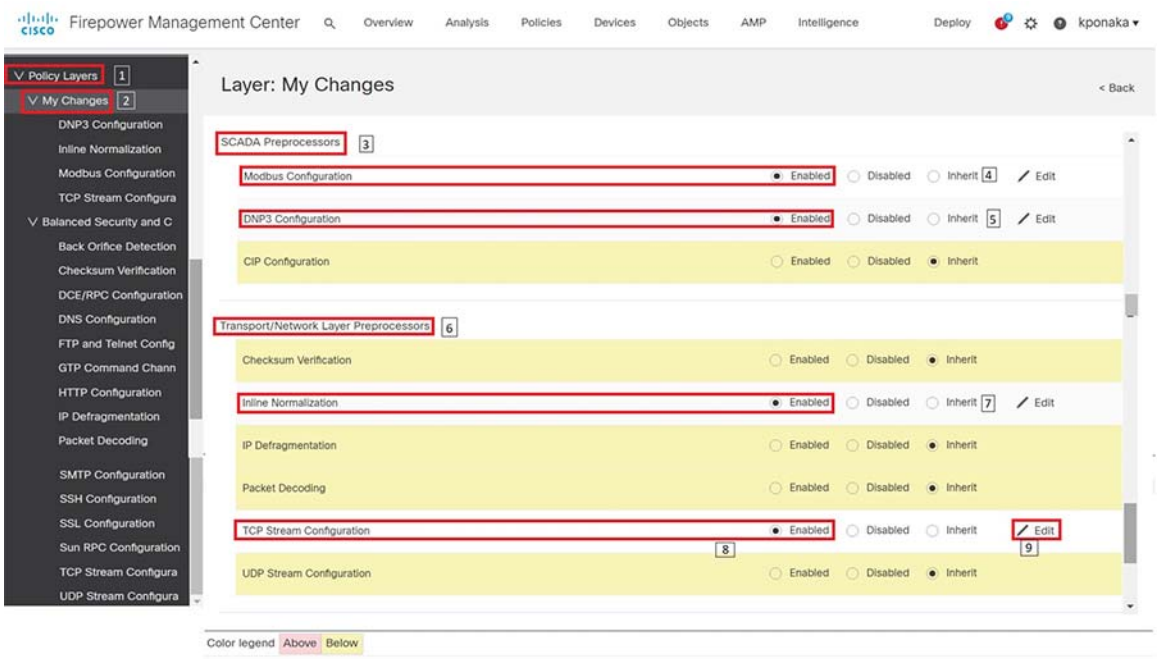
Click the **Create Policy** button and follow the steps as highlighted in the following figure.

Figure 102 SCADA Preprocessor Creating new Network Analysis Policy



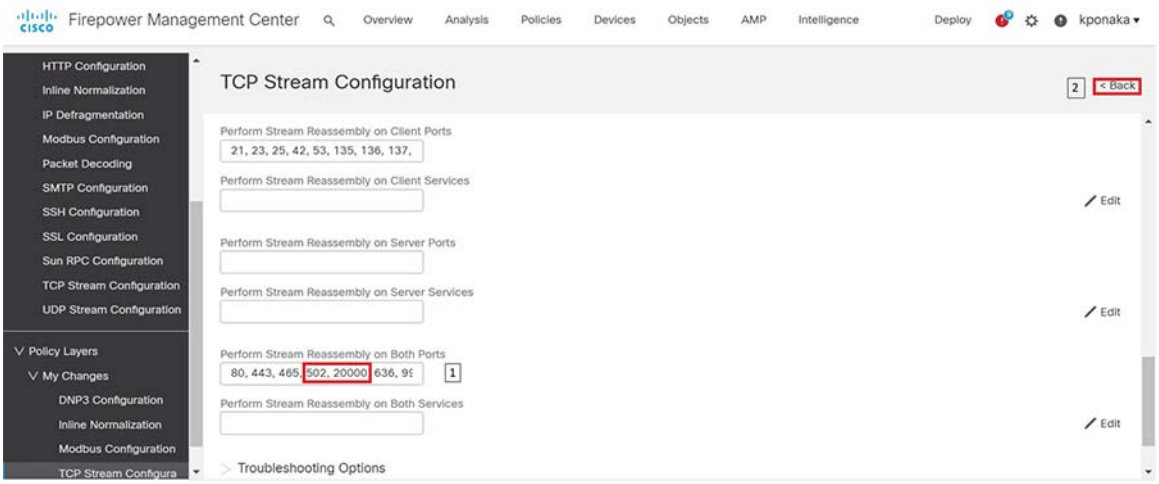
Click **My Changes** option listed under **Policy Layers** on the left-hand side of the resulting window and follow the steps as highlighted in the following figure.

Figure 103 SCADA Preprocessor Editing Network Analysis Policy



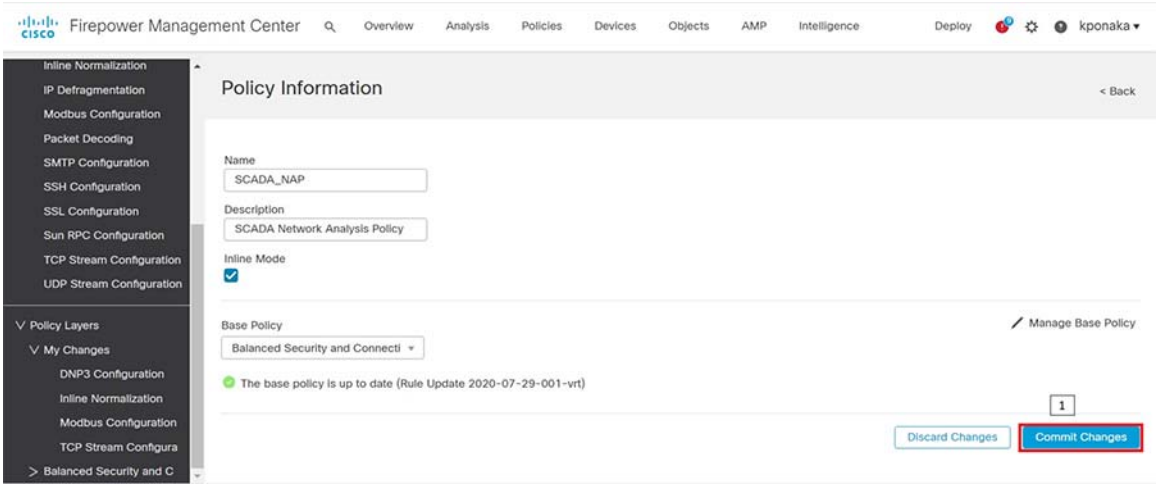
Clicking the **Edit** button across TCP Stream Configuration as highlighted by number 9 in the previous figure, results in a new window. Scroll down to “Perform Stream Reassembly on Both Ports” settings and add ports **502** for Modbus and **20000** for DNP3. Click **Back** after modifications. Refer to highlights in the following figure.

Figure 104 Preprocessor - Adding Protocol properties



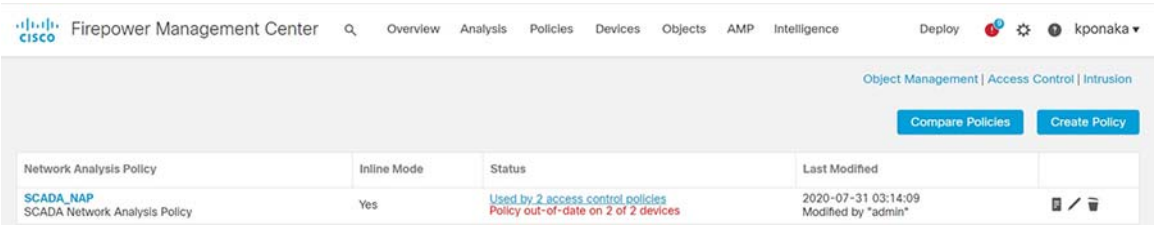
Click **Commit Changes** and proceed as highlighted in the following figure.

Figure 105 SCADA Preprocessor Commit new Network Analysis Policy



The resulting window lists the newly created policy.

Figure 106 SCADA Preprocessor new Network Analysis Policy

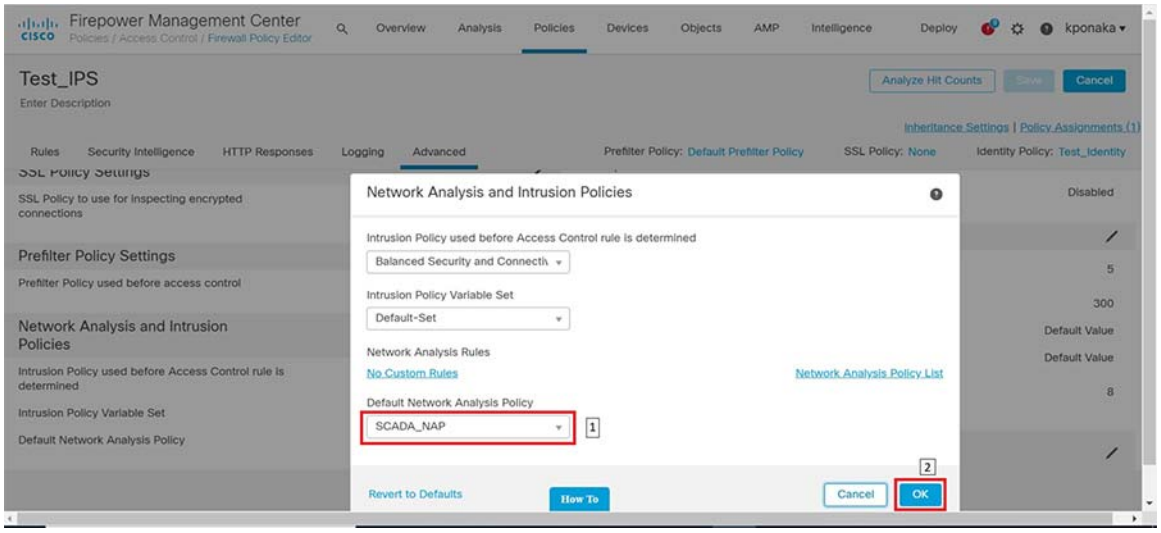


Next, navigate to the window shown in Figure 101 where a new Access control policy was created, and the newly created Network Analysis policy would be selected in the drop-down by following the steps highlighted in the following figure.

The newly created policy is listed in the drop-down list for **Default Network Analysis Policy**. Select the appropriate policy and click **OK**.

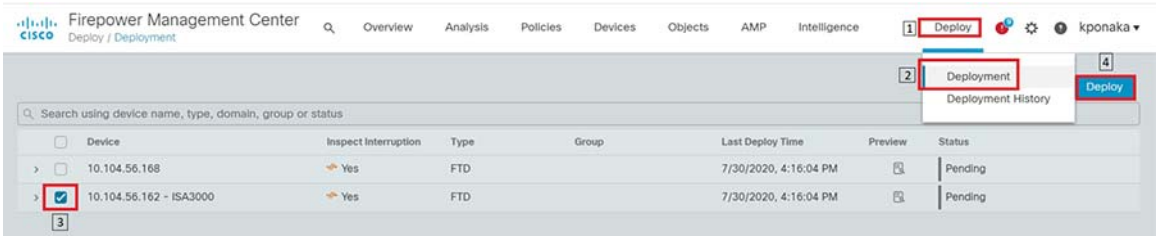
Save the policy by clicking **Save** button.

Figure 107 SCADA Preprocessor selecting new Network Analysis Policy



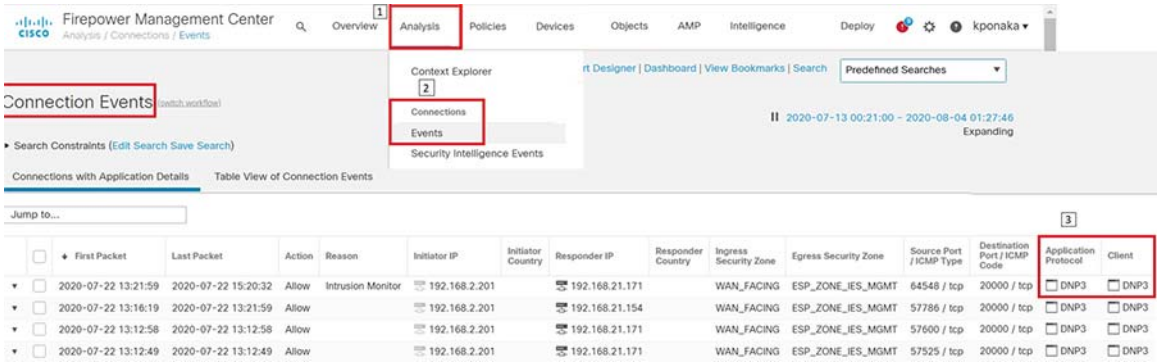
Deploy the policy on the intended device as highlighted in the following figure.

Figure 108 SCADA Preprocessor Deploying new Policy Verification



Initiate traffic and check if the applied policy classifies and identifies the type of application and the protocol it uses. This scenario was validated with DNP3 application and firewall policy applied on ISA3000 as highlighted in the following figure.

Figure 109 SCADA Preprocessor verifying newly created Network Analysis Policy



Deep Packet inspection of Modbus using ISA3000

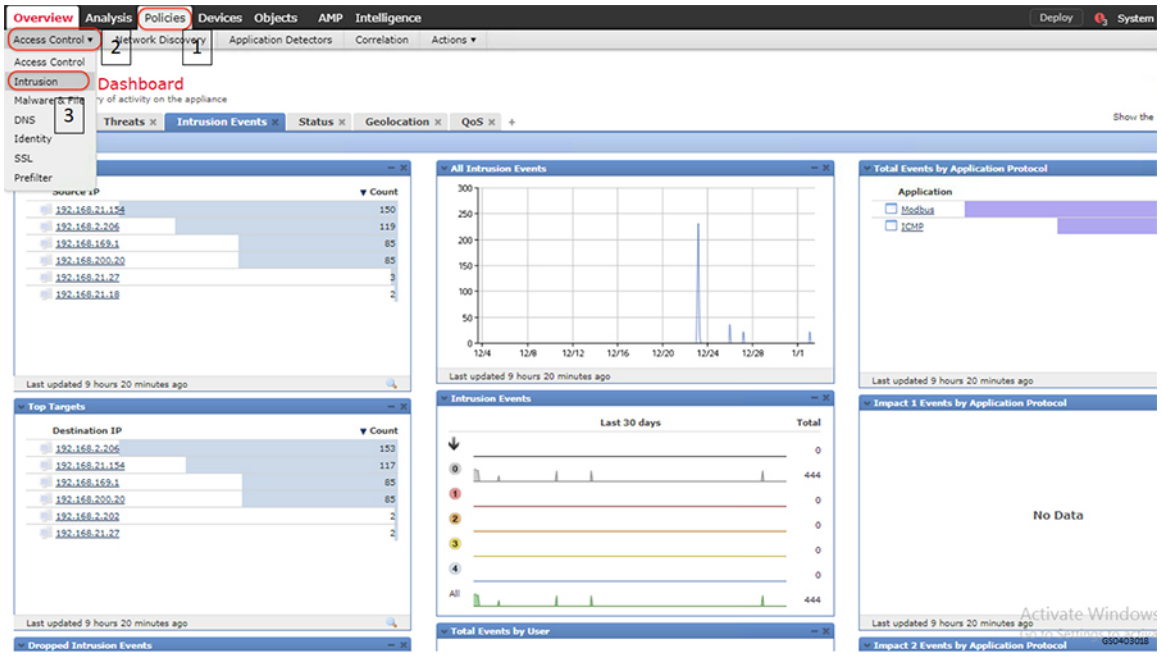
This scenario demonstrates how Cisco ISA3000 can be used to detect individual commands in a SCADA application. This functionality is extremely helpful in OT networks to provide visibility into the transactions that happen between endpoints and detect malicious behavior that may be result of a malware infection or an attack on Industrial Infrastructure. In particular, we will create IPS Rules on ISA3000 to detect individual Modbus commands such as READ or WRITE and generate an event for the same.

For details on the list of different OT protocols supported on ISA3000 refer to the following link. https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-appliance-3000/data-sheet-c78-735839.pdf

Summary

Navigate to **FMC > Policies > Access Control** and click Intrusion as highlighted in the following figure.

Figure 110 Navigation to create new intrusion policy



Click on **Intrusion Rules** as highlighted in the following figure.

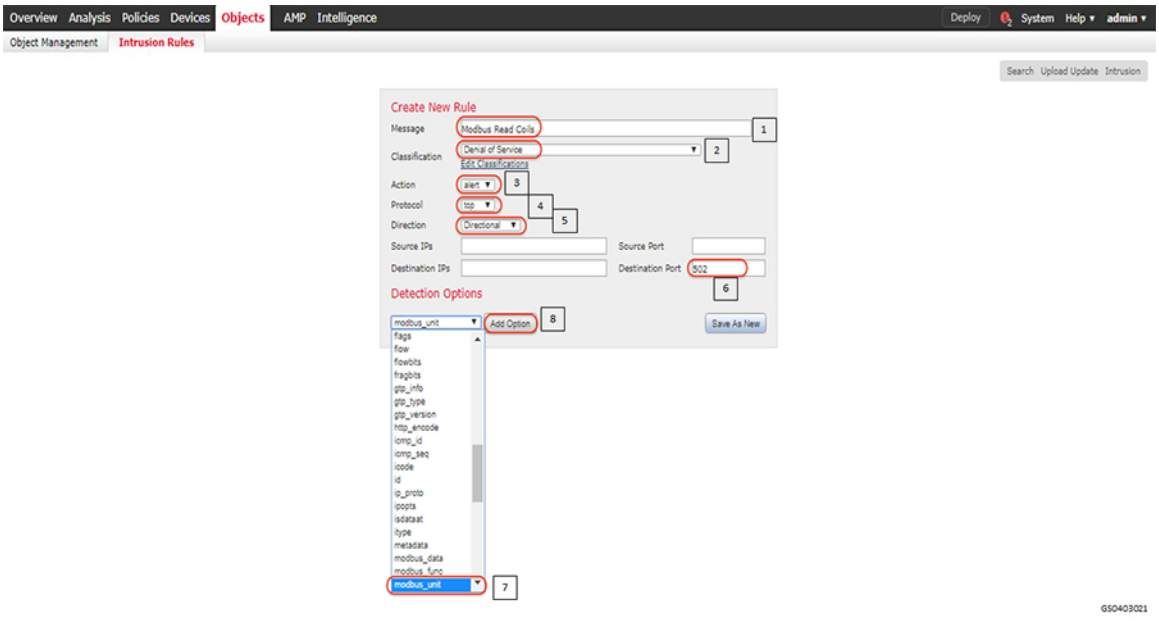
Figure 111 Navigation to create new intrusion rule

Click on **Create Rule** in the resulting page as highlighted in the following figure.

Figure 112 Create new intrusion rule

Fill in the details in the resulting page as highlighted in the following figure. As mentioned earlier, this scenario demonstrates Modbus Protocol command detection. The figure shows a rule being created for Modbus read coils command to Modbus Substation ID 1 (Modbus unit) and generate an alert for the same.

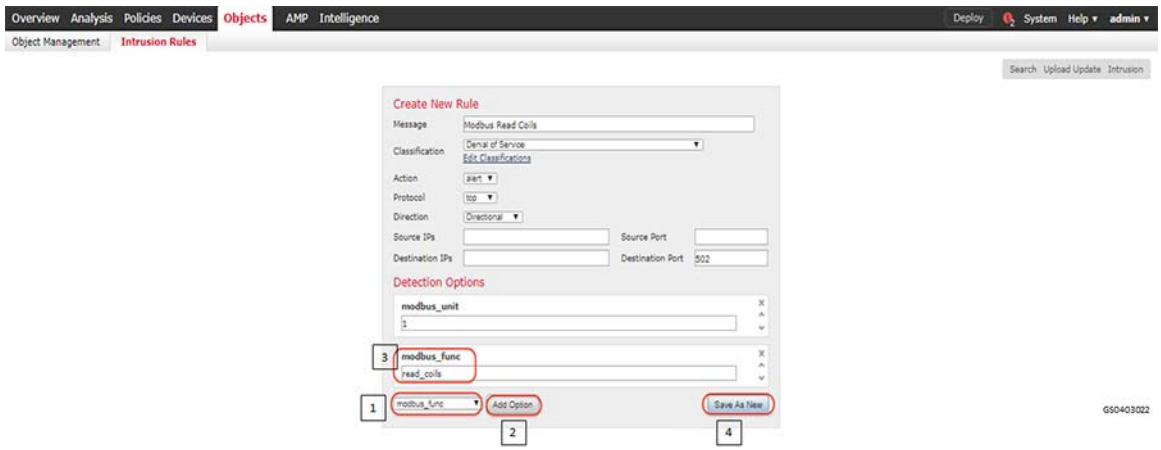
Figure 113 Defining intrusion rule properties



A Modbus will have a unit number often referred to as station ID. This example uses **1** for the emulated PLC.

Identify the command that needs to be inspected for as highlighted in the following figure. The figure shows Modbus Read Coils command.

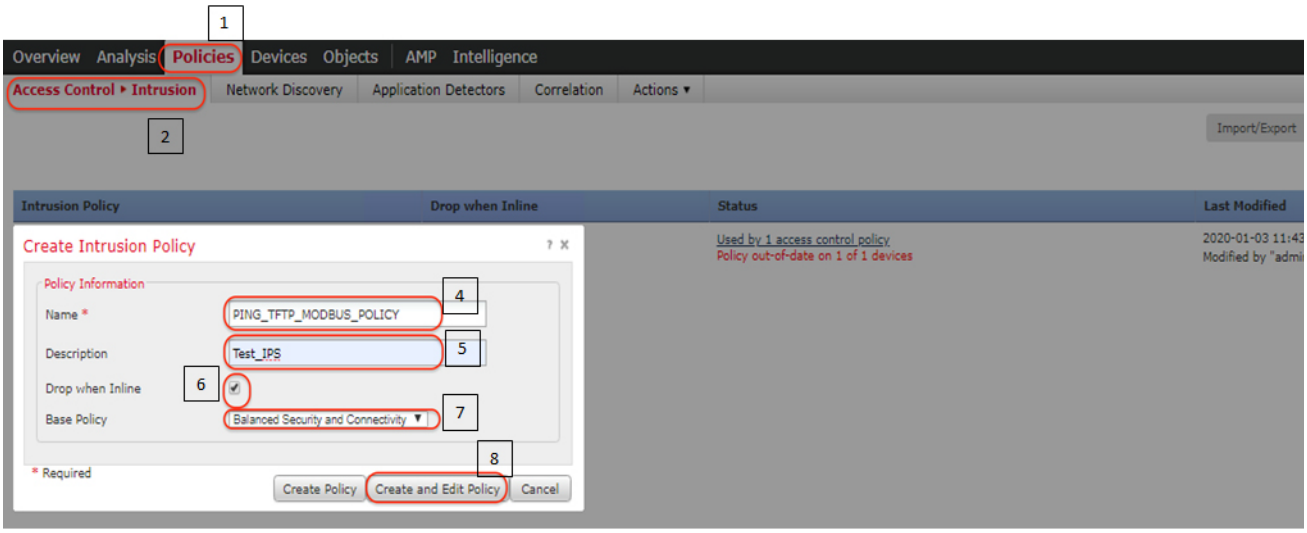
Figure 114 Define modbus function to be inspected



An IPS rule that can sort through all the traffic that gets sent across ISA3000 and find a Modbus flow that issues a Read Coils command to Modbus unit 1 has been created. This functionality opens up many possibilities for intrusion detection and enforcement. Once the rule is successfully added, we can add a few more rules by simply modifying the current rule and saving as new again. In our lab, we also created rules for Modbus commands viz. write_single_coil and write_multiple_coils.

Create a new **Intrusion Policy** with the newly created Intrusion rules as highlighted in the following figure.

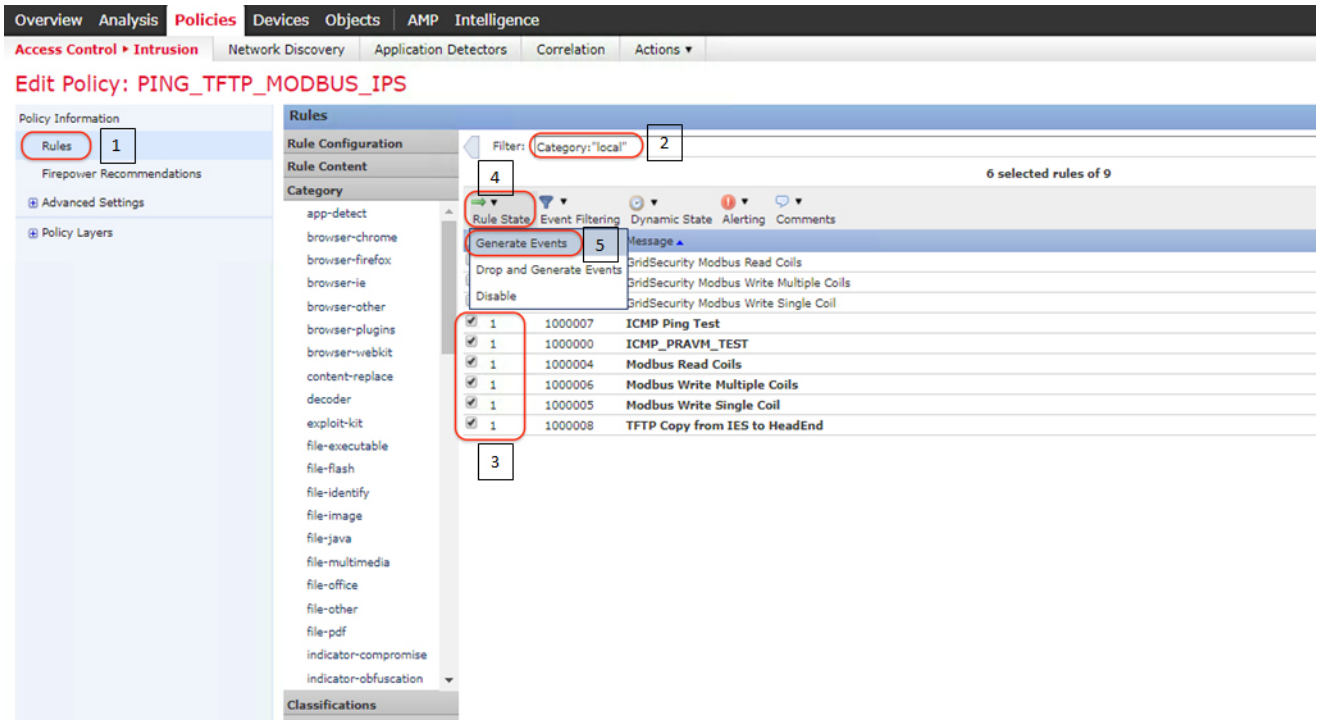
Figure 115 Create new intrusion policy



In the resulting edit policy window click rules and select the rules and corresponding actions for the rules as highlighted in the following figure.

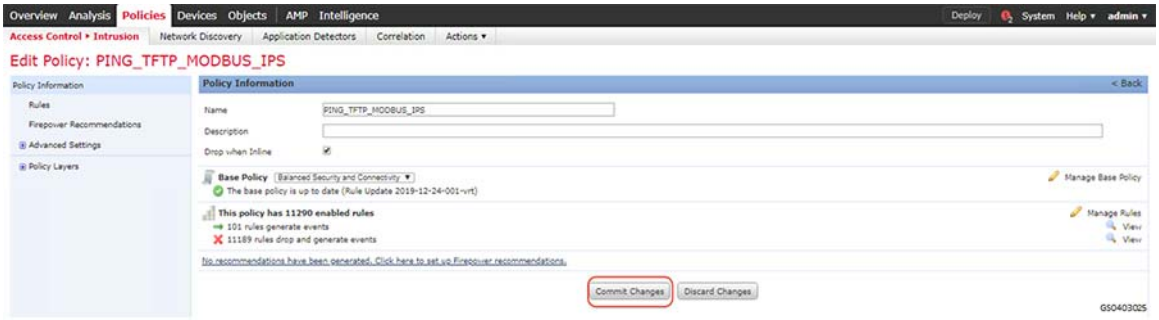
It is recommended to not select **Drop** action especially in OT environments, where **Availability** has higher priority than **Security**. Giving visibility to the user in the form of events is important.

Figure 116 Add intrusion rules to intrusion policy



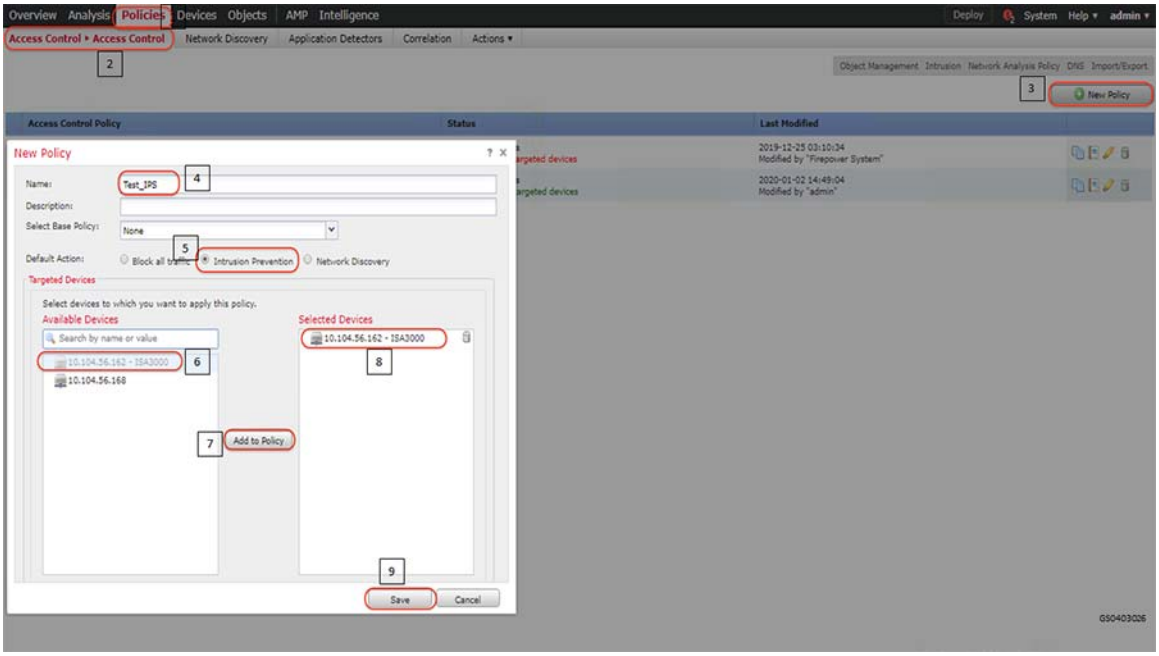
Commit the changes in the resulting window as highlighted in the following figure.

Figure 117 Commit changes to intrusion policy



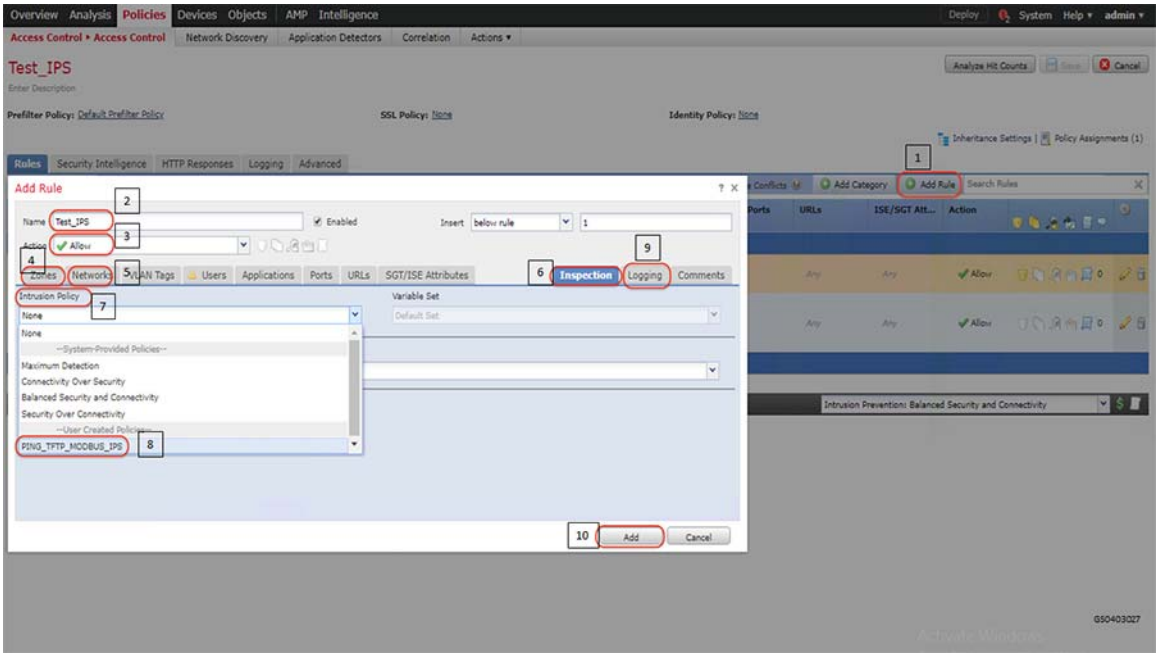
Create a new access control policy as highlighted in the following figure.

Figure 118 Create Access control policy for intrusion prevention



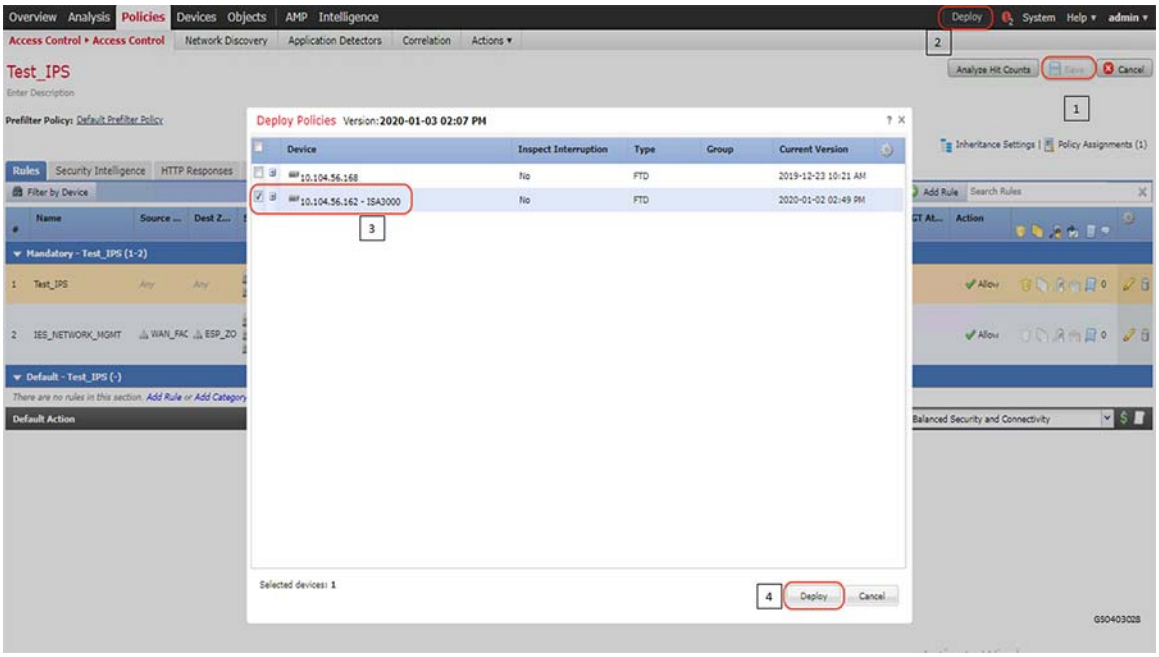
Add rule with the intended intrusion policy in the resulting window as highlighted in the following figure.

Figure 119 Attach intrusion policy to access control policy



Save the newly added rule and deploy the policy onto Cisco ISA3000 as highlighted in the following figure.

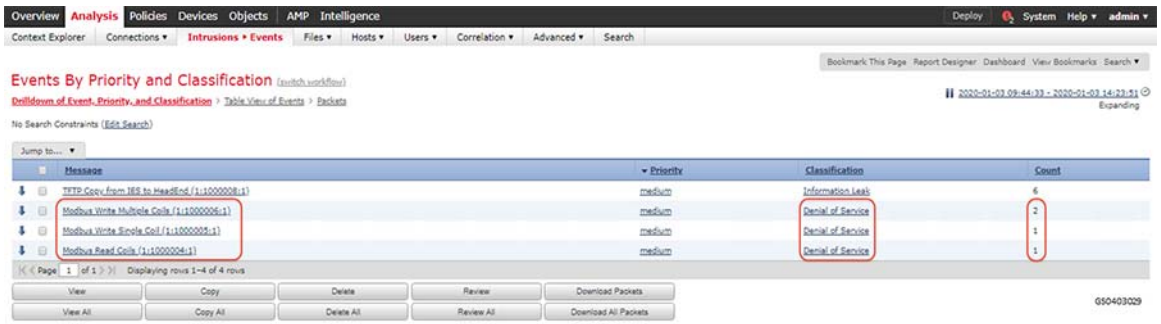
Figure 120 Deploy newly created Access control policy for intrusion prevention



Verification

Initiate traffic and check if the applied policy classifies and identifies the type of application and the protocol it uses. This scenario was validated with Modbus application and firewall policy applied on ISA3000 and ensuring that required events gets generated as highlighted in the following figure.

Figure 121 Verifying newly created Access control policy for intrusion prevention



Deep Packet inspection of DNP3 using ISA3000

This scenario demonstrates how Cisco ISA3000 can be used to detect individual commands in a SCADA application. This functionality is extremely helpful in OT networks to provide visibility into the transactions that happen between endpoints and detect malicious behavior that may be result of a malware infection or an attack on Industrial Infrastructure. In particular, we will create IPS Rules on ISA3000 to detect individual DNP3 commands for READ, WRITE and UNSOLICITED operations and generate events for the same.

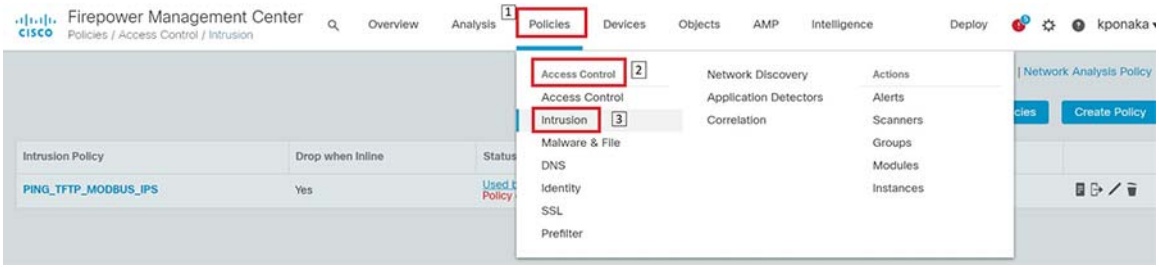
For details on the list of different OT protocols supported on ISA3000 refer to the following link.

https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-appliance-3000/data-sheet-c78-735839.pdf

Summary

Navigate to **FMC > Policies > Access Control** and click Intrusion as highlighted in the following figure.

Figure 122 Navigation to create new intrusion policy



Click on **Intrusion Rules** as highlighted in the following figure.

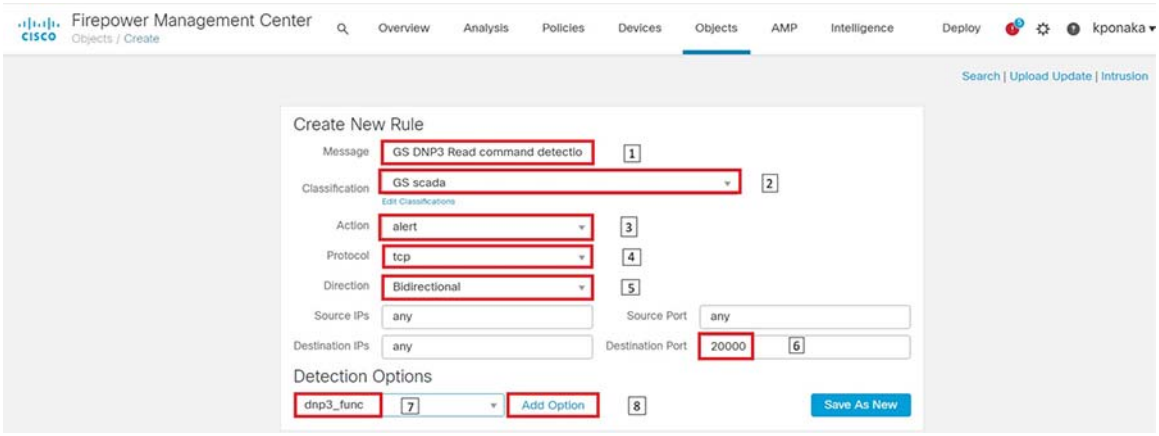
Figure 123 Navigation to create new intrusion rule

Click on **Create Rule** in the resulting page as highlighted in the following figure.

Figure 124 Create new intrusion rule

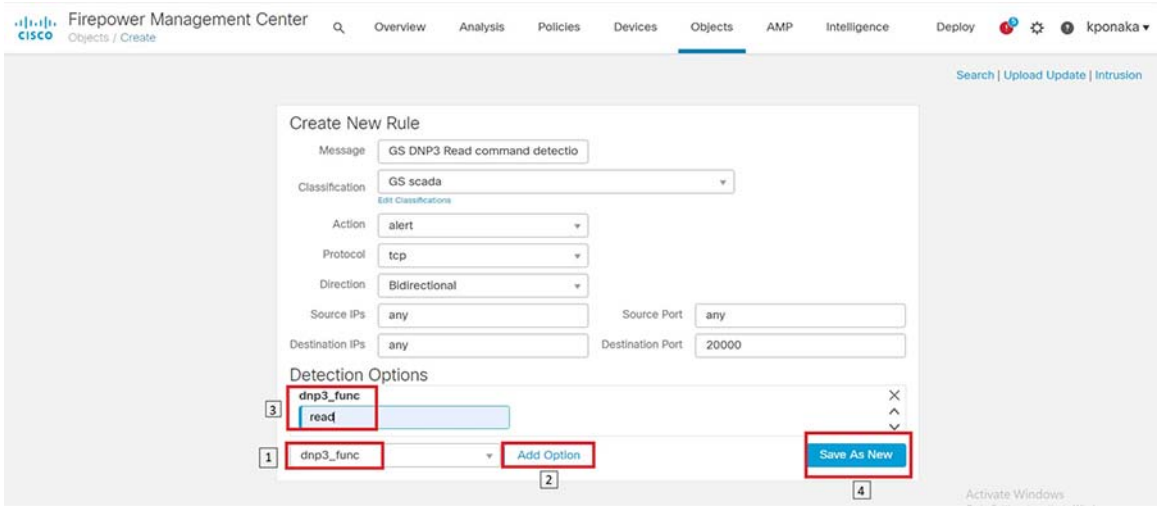
Fill in the details in the resulting page as highlighted in the following figure. As mentioned earlier, this scenario demonstrates DNP3 Protocol command detection. The figure shows a rule being created for DNP3 Read command and generate alerts for the same.

Figure 125 Defining intrusion rule properties



Identify the command to be inspected for as highlighted in the following figure. The figure shows the DNP3 Read command.

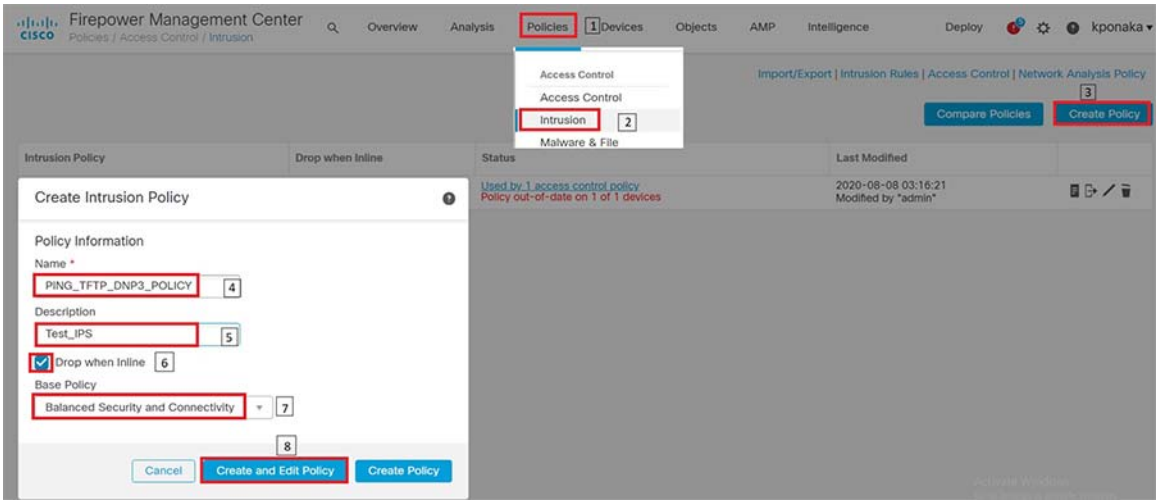
Figure 126 Define DNP3 function to be inspected



An IPS rule that can sort through all the traffic that gets sent across ISA3000 and find a DNP3 flow that issues a Read command has been created. This functionality opens up many possibilities for intrusion detection and enforcement. Once the rule is successfully added, we can add a few more rules by simply modifying the current rule and saving as new again. In our lab, we also created rules for Write and Unsolicited type DNP3 commands viz. write and enable_unsolicited.

Create a new Intrusion Policy with the newly created Intrusion rules as highlighted in the following figure.

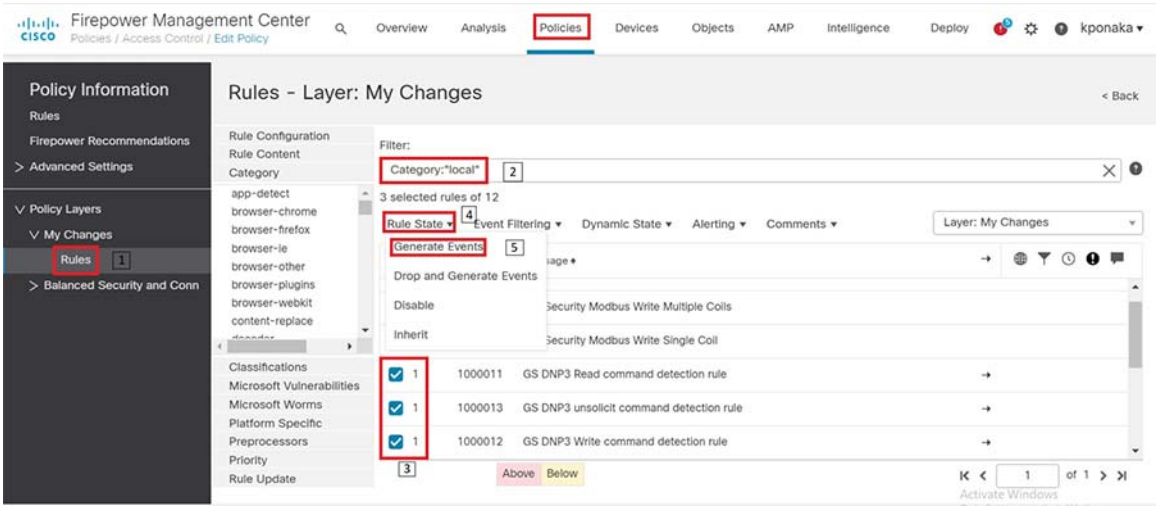
Figure 127 Create new intrusion policy



In the resulting edit policy window click rules and select the rules and corresponding actions for the rules as highlighted in the following figure.

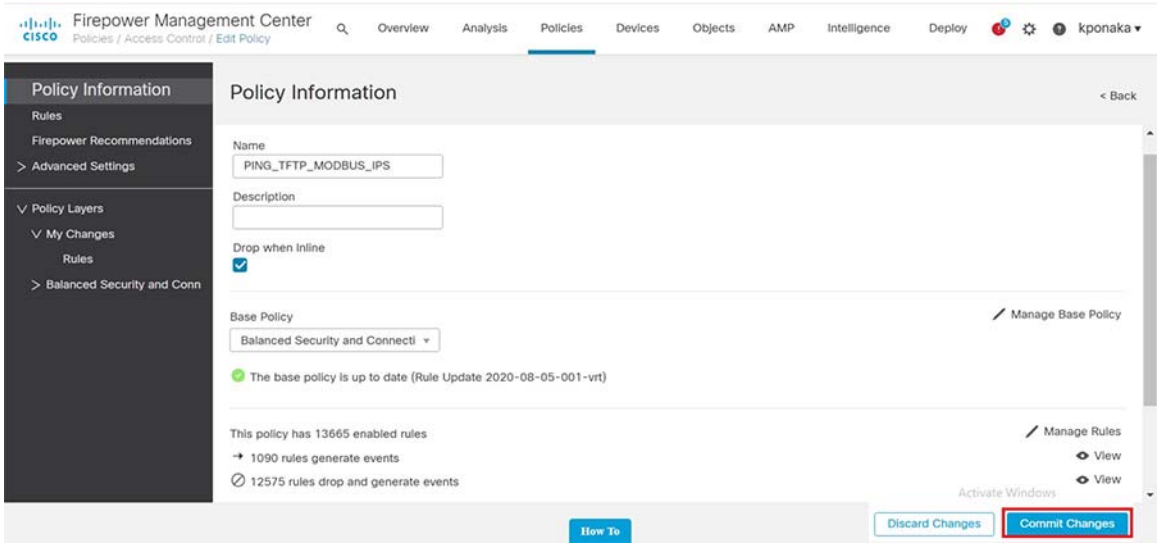
It is recommended to not select **Drop** action especially in OT environments, where **Availability** has higher priority than **Security**. Giving visibility to the user in the form of events is important.

Figure 128 Add intrusion rules to intrusion policy



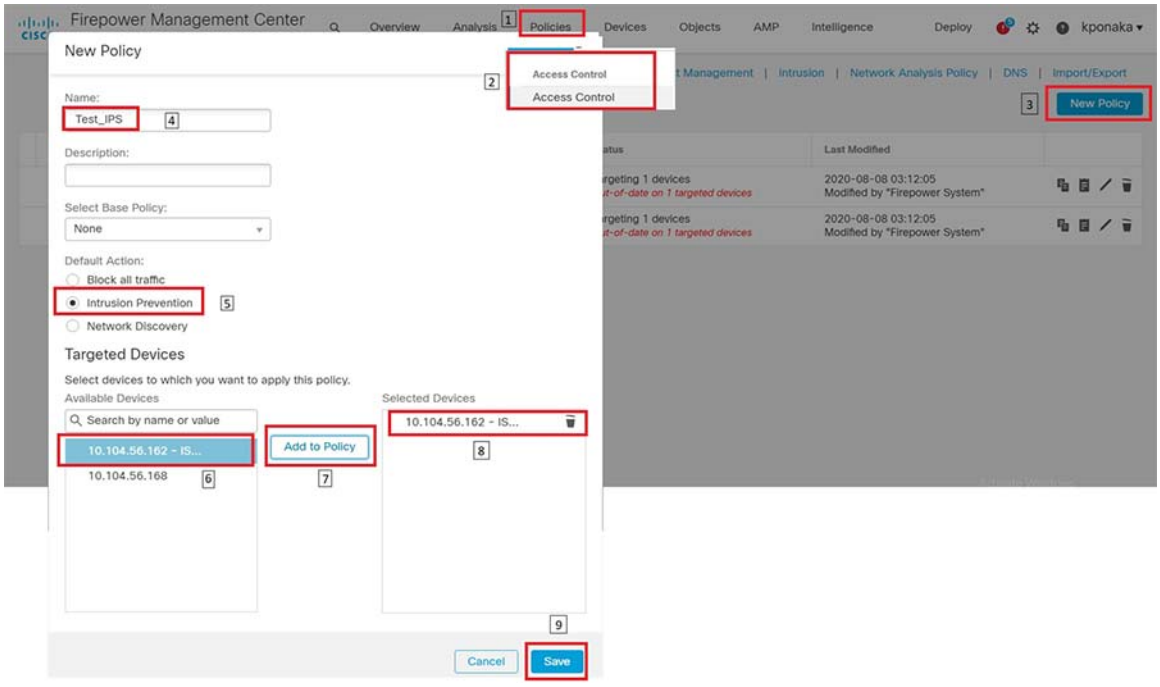
Click on the **Back** button at top right and then commit the changes in the resulting window as highlighted in the following figure.

Figure 129 Commit changes to intrusion policy



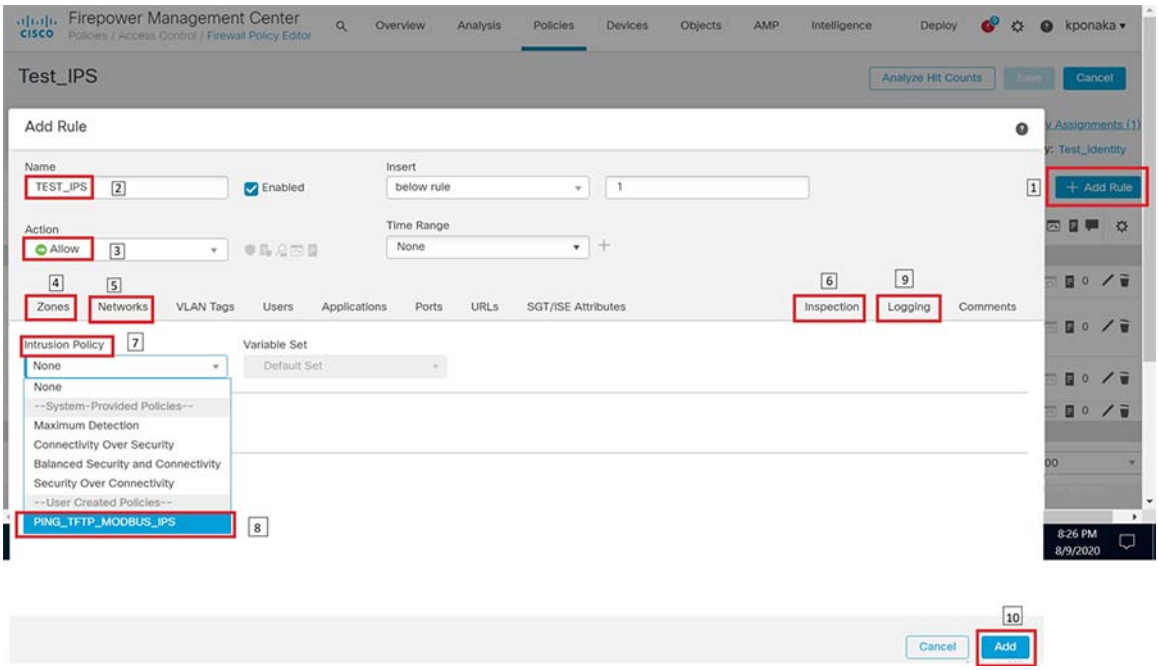
Create a new access control policy as highlighted in the following figure.

Figure 130 Create Access control policy for intrusion prevention



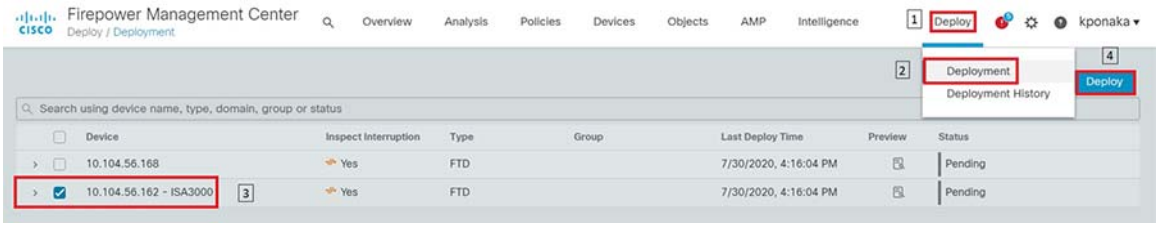
Add rule with the intended intrusion policy in the resulting window as highlighted in the following figure.

Figure 131 Attach intrusion policy to access control policy



Save the newly added rule and deploy the policy onto Cisco ISA3000 as highlighted in the following figure.

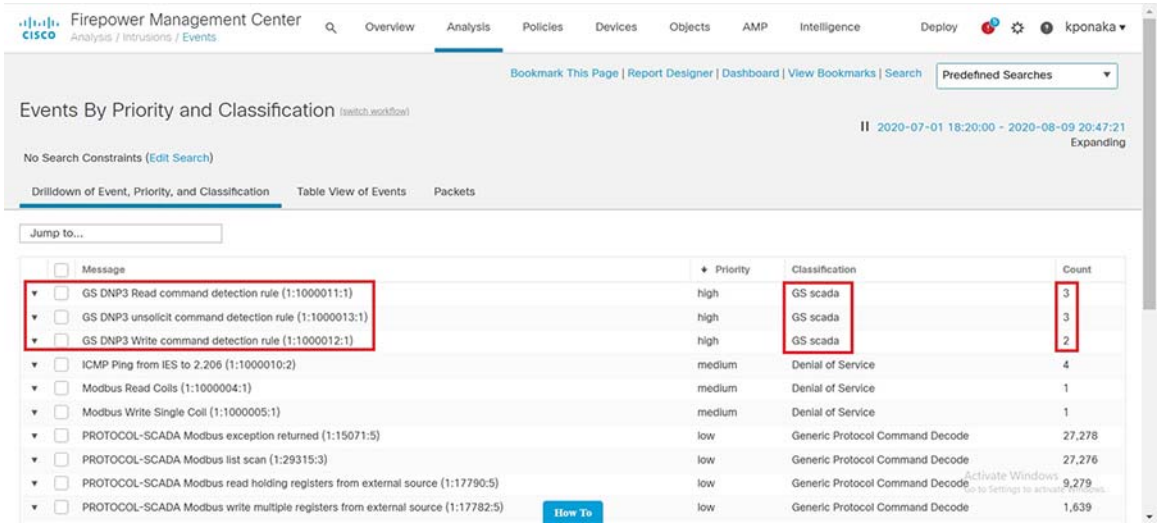
Figure 132 Deploy newly created Access control policy for intrusion prevention



Verification

Initiate traffic and check if the applied policy classifies and identifies the type of application and the protocol it uses. This scenario was validated with DNP3 application and firewall policy applied on ISA3000 and ensuring that required events gets generated as highlighted in the following figure.

Figure 133 Verifying newly created Access control policy for intrusion prevention



Appendix A – Running configuration

IE3400

```
!
version 17.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
no platform punt-keepalive settings
no platform bridge-security all
!
hostname IE3400-GS-PRP
!
enable secret 9 $9$HlvJo9UXZYRFWk$pjV3Uw9kz9lbIZlC6E3/Tq0sOjkDJEubzCXsV8/.1Ug
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
clock timezone UTC 5 30
rep bpduleak
ptp mode e2etransparent
vtp mode off
!
ip domain name ccv
!
login on-success log
!
no device-tracking logging theft
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-4038571180
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4038571180
 revocation-check none
 rsakeypair TP-self-signed-4038571180
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
```

```
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
  quit
crypto pki certificate chain TP-self-signed-4038571180
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34303338 35373131 3830301E 170D3230 30313133 32303536
  34355A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 30333835
  37313138 30308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100D6A4 A032BB16 2C1BB24D 367396F2 81D867A8 30009350 71B70430
  A6EE34EF 3CE35998 3051779F C7668243 5C13125F EA920C58 BCCAD6D9 931231CF
  CE2A9FAF 2A3CBB3C 6A0C740A 12BC5E23 F672D564 8C39A2F3 1292D7C1 49E9C74E
  4E473460 151402F1 7BC5E2F5 24BBC744 E9DDCAB4 6B605507 8CE66EF9 417D8A8F
  0FB4C98D 4996C385 30F51BE2 D710ADF1 59B870F1 56737D12 D6E19797 91ADBCBB
  ADA07655 F8DCC2B8 B0A7DF7B 3F764926 D0B74E7B 4861AD49 09E778A4 15ABF962
  E9BEDA38 4450B6CB B915AEF1 18E82C43 E4CBFE6F 24C5312F FB500624 996A1AD8
  4D59EA38 24DB608B A9BF80E7 3E85E810 58EAEB97 2D2C72AF 4E6B227F B79AF22C
  CE9901C6 C0AB0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 1487C66A 7A57FDFE DC628955 D2174D97 236B77E3
  4F301D06 03551D0E 04160414 87C66A7A 57FDFEDC 628955D2 174D9723 6B77E34F
  300D0609 2A864886 F70D0101 05050003 82010100 27EAFA7C C94189E6 A4FFBE9A
  07F5BC4C A16E4BAD 908E938A 6A4ECF7A 5185E2A9 A070694C 1AAB3DA1 750CCB62
  D15109D5 A62FE80E DAFA1E8D 57D42670 FB1B5196 4100D0E8 A1E03948 96FEE468
  A0206830 1AA5DD90 73B99AF2 C9718EC5 D06F6536 6C0384C7 9DE17C3F FBAACF95
  E0C2E1B4 70396783 7AE09C90 2651A5DD 1CC1759F 2A97D7EE 792A8186 FF4512C7
  900AD8D0 9431469D C2B8A629 CEE5AC45 EFA9F1E3 A041AE94 CB3A1DEC 9FCB8579
  FDE54191 219995B7 2EFCDFE3 C9CFEE95 5B6F7900 9D1C7CEC 20703CE3 FE54BB0D
  1FD74864 61F22A0D B9D13E91 09A89DB7 F6596E95 B0B4FA37 DD3E1F63 B34C7F4E
  CD5C8191 0E0A21DF AEBD1BA1 A4C5D6D7 6E37EEA9
  quit
!
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 90170
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
username admin privilege 15 password 0 XXXXXX
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
vlan 2,10,21,100-101,110-111,113,120,128,150,169,200,343,500-501,901,999
!
vlan 1021
```

```
!
vlan 2508
 remote-span
lldp run
!
interface PRP-channel1
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 prp-channel-group 1
!
interface GigabitEthernet1/2
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 prp-channel-group 1
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
 description provide connectivity via vlan200 to cvc subnet
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
 description PNP STARTUP VLAN
 switchport trunk allowed vlan 1021
 switchport mode trunk
!
interface AppGigabitEthernet1/1
 switchport mode trunk
!
interface Vlan1
 ip dhcp client client-id ascii FOC2336V025
 ip address dhcp
 shutdown
!
interface Vlan111
 ip address 192.168.21.32 255.255.255.0
!
interface Vlan200
 ip address 192.168.200.71 255.255.255.0
!
interface Vlan1021
 ip dhcp client client-id ascii FOC2336V025
 ip address dhcp
!
iox
ip http server
ip http authentication local
ip http secure-server
```

```
ip http client source-interface Vlan1
ip forward-protocol nd
ip route 192.168.2.0 255.255.255.0 192.168.21.99
ip route 192.168.3.102 255.255.255.255 192.168.2.202
ip route 192.168.169.0 255.255.255.0 192.168.200.100
!
ip tftp source-interface Vlan200
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
monitor session 1 source interface Gi1/8
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to
send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
pnp profile pnp-zero-touch
 transport http ipv4 192.168.106.10 port 80
end
```

IE5000

```
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
no service password-encryption
service sequence-numbers
!
hostname IE5000-GM
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
enable password XXXXXX
!
username admin privilege 15 password XXXXXX
aaa new-model
!
!
aaa group server radius AAASERVER
 server name AAASERVER
!
```

```
aaa authentication dot1x default group AAASERVER
aaa authorization exec default group AAASERVER
aaa authorization network default group radius
aaa authorization network SGLIST group AAASERVER
aaa authorization auth-proxy default group AAASERVER
aaa authorization configuration default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
!
!
!
!
!
aaa server radius dynamic-author
 client 192.168.2.202 server-key XXXXXX
!
aaa session-id common
ethernet cfm ieee
ethernet cfm global
ethernet cfm domain INTER_GIG_1_21 level 0
 service intf_state port
  mep mpid 1
  continuity-check
!
process cpu threshold type total rising 80 interval 300
clock timezone IST 5 30
clock calendar-valid
gnss
system mtu routing 1500
ip routing
!
ip dhcp limit lease log
ip dhcp excluded-address 40.40.0.1 40.40.0.10
ip dhcp excluded-address 40.40.0.1 40.40.0.2
ip dhcp excluded-address 1.1.0.100
ip dhcp excluded-address 77.77.77.1
!
ip dhcp pool Edge_Compute
 network 40.40.0.0 255.255.255.0
 default-router 40.40.0.1
 option 43 ascii 5A;K4;B2;I40.40.0.2;J9125
 option 42 ip 100.0.0.10
 lease infinite
   cip instance 1
!
ip dhcp pool DTM_Machines
 network 1.1.0.0 255.255.255.0
 lease infinite
   cip instance 2
!
ip dhcp pool ic3k-factory
 network 77.77.77.0 255.255.255.0
 default-router 77.77.77.1
   cip instance 3
!
!
login on-failure log
login on-success log
vtp mode off
!
!
!
!
!
ptp profile power
ptp mode gmc-bc pdelay-req
```

```
ptp gm-id 10
ptp domain 10
epm logging
!
!
flow record StealthWatch_Record
 description NetFlow record format to send to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect interface input
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter StealthWatch_Exporter
 description StealthWatch Flow Exporter
 destination 192.168.2.211
 source Vlan111
 output-features
 transport udp 2055
 option application-table
!
!
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
!
crypto pki trustpoint TP-self-signed-1999386240
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1999386240
 revocation-check none
 rsakeypair TP-self-signed-1999386240
!
!
crypto pki certificate chain TP-self-signed-1999386240
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31393939 33383632 3430301E 170D3138 30393034 31353334
  32385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39393933
  38363234 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100A7DE 4911F7FB EFE54267 A6E95206 AEEE7327 6D72E211 A7D13EE3 29A51CD2
  F1B17A32 DEB1342A 17F3E224 11F2476C 6AFD0201 0B518D9C 6E11BA80 0B3D4E89
  25A09196 390047E5 FF9D0CB1 4DB33821 C1A41680 BE6BADA6 87D33311 BB40D999
  CC4AAF57 FE8736B1 44327852 374ECFCC 60CB931D 159ABCFD 5A186E97 62A14340
  302F0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 144DBB3D 0E455323 1DF7A33C C79817DD BF95B32F 76301D06
  03551D0E 04160414 4DBB3D0E 4553231D F7A33CC7 9817DDBF 95B32F76 300D0609
```

```
  2A864886 F70D0101 05050003 81810090 4C281330 8C2FA3AF 6EB00C57 1971B7A3
  25EDD589 46B1D59E 47417930 9721A813 64B63189 B277D7CE B4F4EA9C 18E08409
  444EC614 9030ECFB A240A107 C5425237 CE00A923 8EE69E00 556FD7E3 DCCD2510
  71C7017D 6D978082 13521EB5 43C0E873 EE38466A CC77B30A 73F671C1 6EF6C8BB
  B8D47C03 AF031991 B5F3669C CE83E4
        quit
cts sxp default password XXXXXX
license boot level ipservices
archive
 log config
  logging enable
  logging size 200
  notify syslog contenttype plaintext
  hidekeys
memory free low-watermark processor 20000
memory free low-watermark IO 20000
dying-gasp primary syslog secondary snmp-trap
hsr-ring 2 supervisionFrameLifeCheckInterval 2000
!
mac access-list extended Goose_Match
 permit any any 0x88B8 0x0
mac access-list extended PTP_Match
 permit any any 0x88F7 0x0
mac access-list extended SV_Match
 permit any any 0x88BA 0x0
!
spanning-tree mode rapid-pvst
spanning-tree logging
spanning-tree extend system-id
errdisable recovery cause storm-control
!
alarm profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!

!
!
!
!
!
vlan 2,10,21,100-101,110
!
vlan 111
 name ISE_MGMT_VLAN
!
vlan 113,120,128,150,169,200,343,500-501
!
vlan 901
 remote-span
!
vlan 999,1092,4040
track timer interface msec 500
!
track 1 interface GigabitEthernet1/21 line-protocol
!
lldp run
!
class-map match-all SV
 match access-group name SV_Match
class-map match-all IP_Traffic
 match ip precedence 6
class-map match-all cos_2
```

```
 match cos  2
class-map match-all qos_group_11
 match qos-group 11
class-map match-all qos_group_22
 match qos-group 22
class-map match-all qos_group_44
 match qos-group 44
class-map match-all cos_4
 match cos  4
class-map match-all qos_group_1
 match qos-group 1
class-map match-all VLAN_1092
 match vlan  1092
class-map match-any qos_group_22_44
 match qos-group 22
 match qos-group 44
class-map match-all Goose
 match access-group name Goose_Match
class-map match-all PTP_Match
 match access-group name PTP_Match
class-map match-all VLAN_101
 match vlan  101
class-map match-all VlanPolicer
 match vlan  101
class-map match-all VLAN_100
 match vlan  100
!
policy-map TestOutSCADA
 class qos_group_1
  priority
  police 100000000
 class IP_Traffic
  shape average 900000000
policy-map Test_Out
 class qos_group_11
  police cir 2000000
   conform-action transmit
   exceed-action drop
  priority
 class qos_group_22
  shape average 4000000
 class qos_group_44
  police cir 4000000
   conform-action set-cos-transmit cos
   exceed-action drop
policy-map Test_Out_1
 class qos_group_22_44
  police cir 4000000
   conform-action set-cos-transmit cos
   exceed-action drop
  priority
policy-map Test_IP
 class IP_Traffic
  set precedence 6
policy-map TestInputSCADA
 class SV
  set qos-group 1
 class Goose
  set qos-group 1
policy-map child
policy-map TestChild
 class Goose
  police cir 4000000
```

```
    conform-action set-qos-transmit 22
    exceed-action drop
  class PTP_Match
   police cir 4000000
    conform-action set-qos-transmit 33
    exceed-action set-qos-transmit 33
  class cos_4
   police cir 2000000
    conform-action set-cos-transmit cos
    exceed-action drop
policy-map inputVlanClass
 class VLAN_1092
   service-policy TestChild
 class VLAN_100
   service-policy TestChild
 class class-default
   service-policy TestChild
policy-map Test
 class cos_2
  police cir 2000000
   conform-action transmit
   exceed-action transmit
 class SV
  police cir 2000000
   conform-action set-qos-transmit 11
   exceed-action drop
 class Goose
  police cir 4000000
   conform-action set-qos-transmit 22
   exceed-action drop
 class PTP_Match
  police cir 4000000
   conform-action set-qos-transmit 33
   exceed-action set-qos-transmit 33
 class cos_4
  police cir 2000000
   conform-action transmit
   exceed-action drop
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 100.100.100.2 255.255.255.255
 ip ospf 100 area 0
 downshift disable
!
interface PRP-channel1
 switchport mode trunk
 logging event trunk-status
 logging event subif-link-status
 shutdown
 spanning-tree portfast edge
 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport mode trunk
```

```
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 description connected to gig1/2 ISA3000
 switchport trunk allowed vlan 1,2,111,113,169,200
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
!
interface GigabitEthernet1/2
 description connected Ixia-port 3
 switchport trunk allowed vlan 1-99,101-109,111-119,121-4094
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
 spanning-tree portfast edge trunk
 service-policy input Test_IP
!
interface GigabitEthernet1/3
 description connected to IC3k-2 mgmt in vlan200
 switchport access vlan 200
 switchport mode access
 logging event trunk-status
 logging event spanning-tree
 logging event status
!
interface GigabitEthernet1/4
 description connected Ixia-5
 switchport trunk allowed vlan 120
 switchport mode trunk
 load-interval 30
 shutdown
 service-policy input TestInputSCADA
!
interface GigabitEthernet1/5
 description connected to ISA3000-2 .186
 no switchport
 ip address 192.168.62.2 255.255.255.0
!
interface GigabitEthernet1/6
 description connected to mgmt port of IC3k(Mani) in vlan200
 switchport access vlan 200
 switchport mode access
 logging event trunk-status
 logging event spanning-tree
 logging event status
!
interface GigabitEthernet1/7
 switchport mode trunk
!
interface GigabitEthernet1/8
 description connected to IE3400
 no switchport
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 description connected to IE3400
 no switchport
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 description connected to IE3400
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
!
interface GigabitEthernet1/11
 description connected to .171 192.168.2.x subnet
 switchport access vlan 111
 switchport mode access
 logging event trunk-status
 logging event spanning-tree
 logging event status
 spanning-tree portfast edge
!
interface GigabitEthernet1/12
 description connected to FND UCS
 switchport trunk allowed vlan 4040
 switchport mode trunk
 logging event trunk-status
 logging event spanning-tree
 logging event status
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
 description connected to ASR1K gi0/0/6
 switchport access vlan 200
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
!
interface GigabitEthernet1/17
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
 shutdown
 prp-channel-group 1
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/18
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
 shutdown
 prp-channel-group 1
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/19
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
```

```
 no cdp enable
 udld port disable
 no lldp transmit
 no lldp receive
 prp-channel-group 2
!
interface GigabitEthernet1/20
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 logging event trunk-status
 logging event spanning-tree
 logging event status
 no cdp enable
 udld port disable
 no lldp transmit
 no lldp receive
 prp-channel-group 2
!
interface GigabitEthernet1/21
 description connected to VDO-Anal 1/5
 switchport trunk allowed vlan 10
 switchport mode trunk
 shutdown
!
interface GigabitEthernet1/22
 switchport access vlan 4040
 switchport mode access
!
interface GigabitEthernet1/23
 switchport access vlan 4040
 switchport mode access
!
interface GigabitEthernet1/24
!
interface GigabitEthernet1/25
 description connected to IE4010-005
 switchport access vlan 100
 switchport mode access
 shutdown
 no cdp enable
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/26
 description connected to IE4010-001
 switchport access vlan 100
 switchport mode access
 shutdown
 no cdp enable
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/27
!
interface GigabitEthernet1/28
!
interface Vlan1
 description Machine Connection
 ip address 1.1.0.100 255.255.255.0
!
interface Vlan2
 description Connection to UCS
 no ip address
 shutdown
!
```

```
interface Vlan10
 ip address 10.0.0.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf bfd
 bfd interval 600 min_rx 600 multiplier 3
!
interface Vlan100
 ip address 100.0.0.1 255.255.255.0
!
interface Vlan111
 ip flow monitor StealthWatch_Monitor input
 ip address 192.168.21.13 255.255.255.0
 no ip redirects
!
interface Vlan112
 no ip address
 shutdown
!
interface Vlan113
 ip address 192.168.4.1 255.255.255.0
 shutdown
!
interface Vlan128
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan169
 ip address 192.168.169.100 255.255.255.0
 shutdown
!
interface Vlan200
 ip flow monitor StealthWatch_Monitor input
 ip address 192.168.200.52 255.255.255.0
!
interface Vlan343
 ip address 77.77.77.1 255.255.255.0
!
interface Vlan4040
 description Edge_Compute DHCP
 ip address 40.40.0.1 255.255.255.0
!
router ospf 100
 router-id 100.100.100.2
 nsf ietf
 timers throttle spf 50 200 200
 timers throttle lsa 50 200 200
 timers lsa arrival 100
 redistribute connected subnets
 network 10.0.0.0 0.0.0.255 area 0
 bfd all-interfaces
!
ip access-list logging hash-generation
ip forward-protocol nd
!
ip tcp path-mtu-discovery
ip http server
ip http secure-server
!
ip tftp source-interface Vlan128
ip route 20.20.100.0 255.255.255.0 192.168.200.51
ip route 172.168.25.0 255.255.255.0 192.168.200.51
ip route 192.168.2.0 255.255.255.0 192.168.21.99
ip route 192.168.3.102 255.255.255.255 192.168.2.202
ip route 192.168.4.0 255.255.255.0 192.168.62.1
ip route 192.168.5.0 255.255.255.0 192.168.2.99
ip route 192.168.6.0 255.255.255.0 192.168.200.99
```

```
ip route 192.168.121.0 255.255.255.0 192.168.200.51
!
!
ip radius source-interface Vlan111
ip sla 1
 icmp-echo 10.0.0.2
 frequency 5
ip sla schedule 1 life forever start-time now
ip sla reaction-configuration 1 react verifyError action-type trapAndTrigger
ip sla logging traps
ip sla enable reaction-alerts
logging host 192.168.2.176
!
snmp-server community public RO
snmp-server trap-source Vlan100
snmp-server enable traps event-manager
snmp-server enable traps syslog
snmp mib flash cache
!
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 attribute nas-port-id include circuit-id
!
radius server AAASERVER
 address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
 pac key XXXXXX
!
no cts role-based monitor enable
!
line con 0
 exec-timeout 0 0
line vty 5 15
!
ntp logging
ntp source Vlan111
ntp master
ntp peer 192.168.2.202
ntp server 192.168.2.108
mac address-table notification mac-move
!
End
```

IE4010

```
!
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
no service password-encryption
service internal
service sequence-numbers
!
hostname IE4010-005
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
```

```
no logging buffered
no logging monitor
 enable password ivsg@123
!
username admin password 0 ivsg@123
username ise-user-1 password 0 Ivsg@123
aaa new-model
!
!
aaa group server radius AAASERVER
 server name CISCOISE
!
aaa authentication dot1x default group radius
aaa authorization network default group AAASERVER
aaa authorization network SGLIST group radius
aaa authorization auth-proxy default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
!
aaa server radius policy-device
 key sdu@123
!
aaa server radius dynamic-author
  client 192.168.2.202 server-key sdu@123
 server-key sdu@123
!
aaa session-id common
process cpu threshold type total rising 80 interval 300
clock timezone IST 5 30
clock calendar-valid
system mtu routing 1500
device-sensor notify all-changes
ip routing
!
ip dhcp limit lease log
!
!
login on-failure log
login on-success log
vtp mode off
!
!
ptp profile power
 ptp allow-without-tlv
ptp mode p2ptransparent
ptp domain 10
epm logging
!
flow record StealthWatch_Record
 description NetFlow record format to send to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport tcp flags
 collect interface input
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

```
 !
flow exporter StealthWatch_Exporter
 description StealthWatch Flow Exporter
 destination 192.168.2.211
 source Vlan111
 output-features
 transport udp 2055
 option application-table
!
!
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
!
crypto pki trustpoint TP-self-signed-1999100800
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1999100800
 revocation-check none
 rsakeypair TP-self-signed-1999100800
 !
!
crypto pki certificate chain TP-self-signed-1999100800
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31393939 31303038 3030301E 170D3131 30333330 30313237
  35355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39393931
  30303830 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100986D 0A3FCF40 B3AEBEA4 3EE38CD4 4F67F884 B011B706 34C013CA 3E6F0228
  2D735522 B161DC60 ED1ADB78 089C0C68 699464B6 3BA26023 B6EE7CE9 7802D893
  793742EB C2366321 189BF291 6184A5A0 1DE90D05 B9C78868 06DBE3E2 425CAC3B
  4FF0EEE4 4ACC9A38 C23D6F9D 8993C931 E0B7CC24 E7463775 CA4B2EF7 0F584101
  3ED50203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 143534FA F1FC301F 0EC6053F DF83816F C077609E 6B301D06
  03551D0E 04160414 3534FAF1 FC301F0E C6053FDF 83816FC0 77609E6B 300D0609
  2A864886 F70D0101 05050003 8181001C CB2FD8F2 43EAF419 A1AC1378 0524E5B6
  5D6ABAED F2152528 730ED157 9A5FF93F 09D55CC4 6C35C4DE 22C4ED6F 8E1578D4
  E9126F6C AADABD3A 4E391299 82FE4CA3 9A408560 0810BBE9 76CD3AD7 4691E75E
  FBF0B6F7 8A3B1B6E A6A1CAA8 568F1D03 17DFA0F3 99F47C93 2A19F9C7 A44270E8
  20CC7018 9200FA2E 32649D69 A7E6FC
  quit
 cts sxp default password sdu@123
license boot level ipservices
archive
 log config
  logging enable
  logging size 200
  notify syslog contenttype plaintext
  hidekeys
memory free low-watermark processor 20000
memory free low-watermark IO 20000
dot1x system-auth-control
dying-gasp primary syslog secondary snmp-trap
!
mac access-list extended Goose_Match
 permit any any 0x88B8 0x0
mac access-list extended PTP_Match
 permit any any 0x88F7 0x0
```

```
mac access-list extended SV_Match
 permit any any 0x88BA 0x0
mac access-list extended block4711
 deny   host 00bf.772c.4711 any
 permit any any
!
 spanning-tree mode rapid-pvst
spanning-tree logging
spanning-tree extend system-id
!
alarm profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
transceiver type all
!
vlan 111-114,169
!
vlan 901
 remote-span
!
 vlan 999,4040
!
lldp run
!
class-map match-all SV
 match access-group name SV_Match
class-map match-all cos_2
 match cos  2
class-map match-all qos_group_11
 match qos-group 11
class-map match-all qos_group_22
 match qos-group 22
class-map match-all qos_group_33
 match qos-group 33
class-map match-all cos_4
 match cos  4
class-map match-all qos_group_1
 match qos-group 1
class-map match-all Goose
 match access-group name Goose_Match
class-map match-all PTP_Match
 match access-group name PTP_Match
!
 policy-map TestOutSCADA
 class qos_group_1
  priority
  police 100000000
policy-map Test_Out
 class qos_group_11
  police cir 2000000
   conform-action transmit
   exceed-action drop
  priority
 class qos_group_22
  shape average 4000000
 class qos_group_33
  shape average 4000000
policy-map TestInputSCADA
 class SV
  set qos-group 1
 class Goose
  set qos-group 1
```

```
policy-map Test
 class SV
  police cir 2000000
   conform-action set-qos-transmit 11
    exceed-action drop
 class Goose
  police cir 4000000
   conform-action set-qos-transmit 22
   exceed-action drop
 class PTP_Match
  police cir 4000000
   conform-action set-qos-transmit 33
   exceed-action set-qos-transmit 33
 class cos_2
  police cir 2000000
   conform-action transmit
   exceed-action transmit
policy-map inputTestCos
 class cos_4
  police cir 4000000
   conform-action transmit
   exceed-action drop
!
!
interface GigabitEthernet1/1
 description Test_MAB
 switchport access vlan 111
 switchport mode access
 switchport port-security violation protect
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00bf.772c.4741
 ip flow monitor StealthWatch_Monitor input
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
  spanning-tree portfast edge
!
interface GigabitEthernet1/2
 description Test_MAB
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
```

```
 interface GigabitEthernet1/7
 description connected IE4010-007 port-7
 switchport mode trunk
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/8
 description connected IE4010-008 port-8
 switchport mode trunk
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/9
 description Test_MAB
 switchport mode access
 ip device tracking probe count 100
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
  dot1x pae authenticator
 dot1x timeout tx-period 3
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
interface GigabitEthernet1/12
 description connected to 3850
 switchport access vlan 500
 switchport mode access
 shutdown
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
 description Test_MAB
 switchport mode access
 ip device tracking probe count 100
  authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
!
interface GigabitEthernet1/17
 switchport mode access
 ip device tracking probe count 100
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
```

```
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
!
 interface GigabitEthernet1/18
!
interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface GigabitEthernet1/21
!
interface GigabitEthernet1/22
!
interface GigabitEthernet1/23
!
interface GigabitEthernet1/24
!
interface GigabitEthernet1/25
 description connected IE5000-GM port17
 switchport mode trunk
 ip device tracking probe count 100
 spanning-tree portfast edge
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/26
  description connected IE5000-02 port-17
 switchport access vlan 150
 switchport mode access
 shutdown
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/27
 description connected IE4010-006 port-25
 switchport mode trunk
 spanning-tree portfast edge
 service-policy input TestInputSCADA
 service-policy output TestOutSCADA
!
interface GigabitEthernet1/28
 description connected to IE3400 gi1/1 port
 switchport mode trunk
 !
interface Vlan1
 no ip address
 shutdown
!
interface Vlan111
 ip address 192.168.21.24 255.255.255.0
!
ip forward-protocol nd
!
!
ip http server
ip http secure-server
```

```
ip route 192.168.2.0 255.255.255.0 192.168.21.99
ip route 192.168.3.102 255.255.255.255 192.168.2.202
!
!
ip access-list role-based DENY_RBALACH
 deny   ip
ip access-list role-based SGT_0_TO_24
 deny   icmp
ip access-list role-based test
!
 ip radius source-interface Vlan111
ip sla logging traps
logging host 10.104.56.173
logging host 192.168.2.176
cpu traffic qos qos-group 33
!
snmp-server community ISE RO
snmp-server enable traps snmp authentication linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server manager
snmp mib flash cache
!
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 attribute nas-port-id include circuit-id
!
radius server CISCOISE
 address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
 pac key sdu@123
!
no cts role-based monitor enable
!
 line con 0
 exec-timeout 0 0
line vty 5 15
!
ntp logging
ntp server 192.168.2.108
mac address-table notification mac-move
end
!
IE4010-005#
```

IR1101

```
version 17.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname IR1100_FCW23110H4A
!
boot-start-marker
boot system bootflash:ir1101-universalk9.17.02.01.SPA.bin
boot-end-marker
!
!
logging buffered 21474836
```

```
enable secret 9 $9$79dSpQQiQM8uXE$5GYZoiU3FPHHT/2fX6rhW1uwnBm9bxc5drGi1/Hbn6c
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
!
aaa session-id common
clock timezone IST 5 30
!
shutdown vlan 200
!
!
!
!
!
!
!
!
!
ip host ntp.ipg.cisco.com 123.108.200.124
ip host ra.ipg.cisco.com 72.163.222.228
ip host tps-san.ipg.cisco.com 72.163.222.234
ip domain name ipg.cisco.com
!
!
!
login block-for 60 attempts 3 within 30
login delay 3
login on-success log
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint LDevID
 enrollment retry count 4
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password
```

```
 fingerprint ECF92E2D5376D5E81D882E3F691FE983D15AD56C
 subject-name serialNumber=PID:IR1101-K9 SN:FCW23110H4A,CN=IR1100_FCW23110H4A.ipg.cisco.com
 revocation-check none
 rsakeypair LDevID 2048
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-216601841
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-216601841
 revocation-check none
 rsakeypair TP-self-signed-216601841
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_08_12_13_UTC_Thu_Jul_11_2019
 revocation-check none
!
crypto pki profile enrollment LDevID
 enrollment url  http://ra.ipg.cisco.com
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = ipg-rsa-root-ca
!
crypto pki certificate chain LDevID
 certificate 6500000370B836DA69A50167AD000300000370
  308205BC 308204A4 A0030201 02021365 00000370 B836DA69 A50167AD 00030000
  0370300D 06092A86 4886F70D 01010B05 00305B31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  13301106 0A099226 8993F22C 64011916 03697067 31183016 06035504 03130F49
  50472D52 53412D52 4F4F542D 4341301E 170D3139 30373131 30343335 32375A17
  0D323130 37313130 34343532 375A3052 31253023 06035504 05131C50 49443A49
  52313130 312D4B39 20534E3A 46435732 33313130 48344131 29302706 03550403
  0C204952 31313030 5F464357 32333131 30483441 2E697067 2E636973 636F2E63
  6F6D3082 0122300D 06092A86 4886F70D 01010105 00038201 0F003082 010A0282
  010100EF 69BC3E1D DB7C6E80 9195E56E C580F0AE A0ED274B 11E52A56 1D83AC7D
  2D7582FB E6DF6C65 CB4229ED B7EFFEE6 10BD3152 ED37254D 36E8343D A0170D6A
  90C004E2 AA9E2CDB F57C895D 3C117135 48417197 63F86865 C4340343 4B6D2BCB
  AAC40C2A A53380C6 97ACC258 8854E488 0C1D5975 E15E7FB9 D5117F99 2E9CDD69
  6ECF22E4 EBD3D042 9E3CF48E 78BA9A66 AC6B19C3 B9464EAA 61E4FF15 44141C27
  7FED0918 A0D05E98 4B6AEBED F81E6FA7 50E7C535 CEF97D86 EEEE6F23 3C566B38
  04F68141 68B79974 1C130F27 FC970EE3 6656EDDD 099CEFAD E40CDB3E 9234A849
  6F3F4C30 98E1ED4D 08F07060 66F216E1 9F85D573 A325E914 65A2E786 E78D091B
  34D08702 03010001 A3820280 3082027C 300B0603 551D0F04 04030204 F0301D06
  03551D0E 04160414 812246CB FAF9CFCB EDDAC4FF F1C96117 F2879AA6 301F0603
  551D2304 18301680 144050AD 98071BC6 1EAA8A0E 516FAB76 6A41C17C E53081DD
  0603551D 1F0481D5 3081D230 81CFA081 CCA081C9 8681C66C 6461703A 2F2F2F43
  4E3D4950 472D5253 412D524F 4F542D43 41283329 2C434E3D 57494E32 3031322D
  53455256 4552312C 434E3D43 44502C43 4E3D5075 626C6963 2532304B 65792532
  30536572 76696365 732C434E 3D536572 76696365 732C434E 3D436F6E 66696775
  72617469 6F6E2C44 433D6970 672C4443 3D636973 636F2C44 433D636F 6D3F6365
  72746966 69636174 65526576 6F636174 696F6E4C 6973743F 62617365 3F6F626A
  65637443 6C617373 3D63524C 44697374 72696275 74696F6E 506F696E 743081C6
  06082B06 01050507 01010481 B93081B6 3081B306 082B0601 05050730 028681A6
  6C646170 3A2F2F2F 434E3D49 50472D52 53412D52 4F4F542D 43412C43 4E3D4149
  412C434E 3D507562 6C696325 32304B65 79253230 53657276 69636573 2C434E3D
  53657276 69636573 2C434E3D 436F6E66 69677572 6174696F 6E2C4443 3D697067
  2C44433D 63697363 6F2C4443 3D636F6D 3F634143 65727469 66696361 74653F62
  6173653F 6F626A65 6374436C 6173733D 63657274 69666963 6174696F 6E417574
  686F7269 7479303C 06092B06 01040182 37150704 2F302D06 252B0601 04018237
  1508FCC9 3C82FD9A 6087F197 168491E9 21EBE947 811F86FD 9C1587ED F9070201
  64020107 301D0603 551D2504 16301406 082B0601 05050703 0106082B 06010505
```

```
  07030230 2706092B 06010401 8237150A 041A3018 300A0608 2B060105 05070301
  300A0608 2B060105 05070302 300D0609 2A864886 F70D0101 0B050003 82010100
  9DF9089C 8EBF4F0D 926DA739 53A8BEED 10F58824 1125CEA4 75461049 0582206C
  4A394D38 1CA8A561 E8742A02 29785C6C BC10977B A61A7530 FF448192 838AB253
  D6179C49 9F673170 1BF5B2EB 0DDBCA0A A67976C9 AAFF96D5 3ABD3F33 8A1C0C6B
  1DC5FFD4 B5985B15 D8D9D4DF DEF2324F 915582EF D07ABFE2 8A8A3E4F 7B3AE5D8
  477602B6 E17F92C6 BDB9FF42 8CC4CC3F 83304125 5B25B9F7 9DF5DFDF 6C50DF95
  CD7DE721 2024CF4F 93A53849 E881F053 A7525486 B3D9AD0F DE5EE213 2A85B74E
  CB4296F1 49E417B6 8103FE44 CF34F903 5CB61D22 A2AE21DE F0FCD5C1 4A864712
  B90E6F09 045C252C 21D1E270 9720F7FA 6E129D75 3876C893 E356FEAC 748F034C
        quit
 certificate ca 75DF1523320095AA45C3BA7A2911F45B
  308203B8 308202A0 A0030201 02021075 DF152332 0095AA45 C3BA7A29 11F45B30
  0D06092A 864886F7 0D01010B 0500305B 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31133011
  060A0992 268993F2 2C640119 16036970 67311830 16060355 0403130F 4950472D
  5253412D 524F4F54 2D434130 1E170D31 39303631 33303032 3431315A 170D3234
  30363132 30303334 31315A30 5B311330 11060A09 92268993 F22C6401 19160363
  6F6D3115 3013060A 09922689 93F22C64 01191605 63697363 6F311330 11060A09
  92268993 F22C6401 19160369 70673118 30160603 55040313 0F495047 2D525341
  2D524F4F 542D4341 30820122 300D0609 2A864886 F70D0101 01050003 82010F00
  3082010A 02820101 00B31C98 9963A4AF FCEA5095 5FB358F3 2000A52D 890867C9
  09FAD7BC 27790580 D7BBC6E8 A8378B0E 078C9D92 5E7F4C1D 035C4FCC 0CB66109
  8442134D 8053470B 73364248 3B91A884 5C84CAA0 16754DDD 79E294CB 9DF09709
  8372B46F FD2909CD B1ABC550 6F16D6E5 610C51AA 43FF335E 0FC249F2 E4736C3D
  4377A425 C99F0EBC 4A72FD61 5078EBCD 6285E324 F8DC95B3 03BDB2A8 194AB7B5
  705FCD45 26B1D4B7 418A8532 89EEE52E 8807EC71 8016BFCB 92D156D4 D51B5491
  9EE0BF6D E1C7C81F C07942AD 8E978EDC FBAC9ED7 E8522FB0 6A344BEB D2937FF3
  708C62D0 F1F265E3 D9910167 F80FEB3C 13859DC3 ACB8DB8B 564F0FA6 70B9E5D8
  70ECA170 2CAB5438 6B020301 0001A378 3076300B 0603551D 0F040403 02018630
  0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04 16041440 50AD9807
  1BC61EAA 8A0E516F AB766A41 C17CE530 1206092B 06010401 82371501 04050203
  03000330 2306092B 06010401 82371502 04160414 D378A26B 48EE13C7 4C59E17B
  1F93A6BF 91865A1B 300D0609 2A864886 F70D0101 0B050003 82010100 9AD3942A
  93DBB586 8C1949A0 6B7D2825 2883E0A3 A2BD05FF C8EAF23B F0FD2A57 16C2D62B
  BC282219 E2C7A34F 55A2F146 5CA344FD A2887178 7BA6F2C2 29C29CEF AE722230
  26FD11B7 08397E1D 114AB736 10E740CB 1AA17602 54F99552 52765F6C 4018F7A5
  CAC6A59D 54CA13DB B6E9066D 69EDAA8B C41B2780 E1EEEBAF C937DA5B B1A1BE4D
  B84BD00F CDE650CA D39E1B62 404CF9F6 B48FE19F 04328747 BA848F2B 9823BD09
  993329D8 6C1F8CD3 C248AD46 B6539314 C2967E62 41735CD1 E4C6820D 8067B27D
  CE8848B4 2B7FB5E0 CD82E726 B3E94F9F 935A7A63 90F5D2D3 0B061409 B1D61F6C
  0937E5ED 8AD1AD90 DE66E6E7 52C7E4F8 FA7F3143 D0E1311D 8E0C
  FFD8
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
```

```
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain TP-self-signed-216601841
 certificate self-signed 01
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313636 30313834 31301E17 0D313930 37313031 32333231
  355A170D 33303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3231 36363031
  38343130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 89520169 F5BBB8CA D27148C3 7DE1D5A6 E22C5F78 CAD50605 CB162992
  DA38EEAF 25613CAE 4AE0C08E BB3E7CEE DD8DDD2E C9BBB82E EB12645E 3E4FB258
  4870A2EE 409FE6DA 0C66CE33 8D423BAA 41C82D85 0F927D1F 9F34F047 BF2830EB
  4EF08EEC 4FA8CF29 07B486D5 5581AAD7 128B6203 FC16776B 63B36E80 A3296875
  B7CBF234 4746DA8E 1147DC56 AB968405 F428570C 58126532 B9B10F84 915041A5
  20970CAA 546C8D5F 4EF4C768 EF3DE969 E8BBAC56 24082B0C 3F835D8F E5C2C21A
  AE46F627 ED82BBE8 6F67C8B2 5F1C358A 7F59C052 0A52D271 C550C80C 65829BC7
  B7678466 F4F2F733 422C3C4A 6EA82500 1BE1E160 1E00D9F0 DC3C031E 60C56788
  7BC841E5 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 23041830 16801422 58C1E199 F7BCBAEA B278B9C8 4FF96A66 0F9DB230
  1D060355 1D0E0416 04142258 C1E199F7 BCBAEAB2 78B9C84F F96A660F 9DB2300D
  06092A86 4886F70D 01010505 00038201 01002CF3 4EE9A0F4 6642F317 30DB1122
  2479971D CA934853 C99A1F15 D23BB96D 79A89E67 5B96970C E5B238A0 C465FA40
  5BAD156F CB3F6CFC 8928F0F8 FA13BCC7 30EC4524 F09C07AD CF9D69AD E650A40A
  0A99D897 2FB22C45 8907FA20 713BF962 1A37B4EA B07A61AF 8DEB7E31 C9D53898
  2BDC6C1D 8708DAD4 C424FA1D D0C3A2A1 A1CD7228 3BCA2B37 692CFA76 1830B42A
  850E06F2 B9041F41 BFD4AA15 A7ECC10F 317B201A 3FD9BAE3 7A33B278 84C24703
  59B157C1 DCD9A350 F1E350A1 4A37EFB3 CF2C8219 30EF2F07 EE2F4EFE F6D622F0
  F2D255C6 3E19F013 F46C2791 E9B22038 A3CF66A1 C86E5968 7E20B5A6 3B12204B
  A6028063 014F8F34 604AF166 8C247B18 9125
        quit
crypto pki certificate chain fnd
 certificate ca 75DF1523320095AA45C3BA7A2911F45B
  308203B8 308202A0 A0030201 02021075 DF152332 0095AA45 C3BA7A29 11F45B30
  0D06092A 864886F7 0D01010B 0500305B 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31133011
  060A0992 268993F2 2C640119 16036970 67311830 16060355 0403130F 4950472D
  5253412D 524F4F54 2D434130 1E170D31 39303631 33303032 3431315A 170D3234
  30363132 30303334 31315A30 5B311330 11060A09 92268993 F22C6401 19160363
  6F6D3115 3013060A 09922689 93F22C64 01191605 63697363 6F311330 11060A09
  92268993 F22C6401 19160369 70673118 30160603 55040313 0F495047 2D525341
  2D524F4F 542D4341 30820122 300D0609 2A864886 F70D0101 01050003 82010F00
  3082010A 02820101 00B31C98 9963A4AF FCEA5095 5FB358F3 2000A52D 890867C9
  09FAD7BC 27790580 D7BBC6E8 A8378B0E 078C9D92 5E7F4C1D 035C4FCC 0CB66109
  8442134D 8053470B 73364248 3B91A884 5C84CAA0 16754DDD 79E294CB 9DF09709
  8372B46F FD2909CD B1ABC550 6F16D6E5 610C51AA 43FF335E 0FC249F2 E4736C3D
  4377A425 C99F0EBC 4A72FD61 5078EBCD 6285E324 F8DC95B3 03BDB2A8 194AB7B5
  705FCD45 26B1D4B7 418A8532 89EEE52E 8807EC71 8016BFCB 92D156D4 D51B5491
  9EE0BF6D E1C7C81F C07942AD 8E978EDC FBAC9ED7 E8522FB0 6A344BEB D2937FF3
  708C62D0 F1F265E3 D9910167 F80FEB3C 13859DC3 ACB8DB8B 564F0FA6 70B9E5D8
  70ECA170 2CAB5438 6B020301 0001A378 3076300B 0603551D 0F040403 02018630
  0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04 16041440 50AD9807
  1BC61EAA 8A0E516F AB766A41 C17CE530 1206092B 06010401 82371501 04050203
  03000330 2306092B 06010401 82371502 04160414 D378A26B 48EE13C7 4C59E17B
  1F93A6BF 91865A1B 300D0609 2A864886 F70D0101 0B050003 82010100 9AD3942A
  93DBB586 8C1949A0 6B7D2825 2883E0A3 A2BD05FF C8EAF23B F0FD2A57 16C2D62B
  BC282219 E2C7A34F 55A2F146 5CA344FD A2887178 7BA6F2C2 29C29CEF AE722230
```

```
  26FD11B7 08397E1D 114AB736 10E740CB 1AA17602 54F99552 52765F6C 4018F7A5
  CAC6A59D 54CA13DB B6E9066D 69EDAA8B C41B2780 E1EEEBAF C937DA5B B1A1BE4D
  B84BD00F CDE650CA D39E1B62 404CF9F6 B48FE19F 04328747 BA848F2B 9823BD09
  993329D8 6C1F8CD3 C248AD46 B6539314 C2967E62 41735CD1 E4C6820D 8067B27D
  CE8848B4 2B7FB5E0 CD82E726 B3E94F9F 935A7A63 90F5D2D3 0B061409 B1D61F6C
  0937E5ED 8AD1AD90 DE66E6E7 52C7E4F8 FA7F3143 D0E1311D 8E0C
  FFD8
        quit
!
license udi pid IR1101-K9 sn FCW23110H4A
license boot level network-advantage
diagnostic bootup level minimal
!
spanning-tree extend system-id
archive
 path bootflash:/archive
 maximum 8
memory free low-watermark processor 50357
!
!
username cg-nms-administrator privilege 15 secret 8
$8$ySUgIvEv2QnuH.$aq/YgVdQIDsh9p6z8uBYgHfO/GRaorJJNsf191sd24U
username cisco privilege 15 secret 8 $8$YZAIgrEXJkmAW.$F4cblmbX7B.GbBpfBM4vLb4ZPMfbTVoxTZMzVhCS7Mk
username admin privilege 15 password 0 sentryo69!
!
redundancy
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_IPv4_LAN
 route set access-list ipv6 FlexVPN_Client_IPv6_LAN
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 dpd 30 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 fragmentation
crypto ikev2 client flexvpn FlexVPN_Client_Secondary
  peer 1 72.163.222.232
  client connect Tunnel1
!
crypto ikev2 client flexvpn FlexVPN_Client
  peer 1 72.163.222.233
  client connect Tunnel0
!
!
controller Cellular 0/1/0
!
controller Cellular 0/3/0
```

```
!
!
vlan internal allocation policy ascending
!
track 3 interface Cellular0/1/0 line-protocol
 delay up 120
!
!
class-map type inspect match-any IN-OUT
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
class-map type inspect match-any OUT-IN
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol http
 match protocol https
 match protocol ssh
!
policy-map type inspect OUT-IN
 class type inspect OUT-IN
  inspect
 class class-default
policy-map type inspect IN-OUT
 class type inspect IN-OUT
  inspect
 class class-default
!
zone security INSIDE
zone security OUTSIDE
zone-pair security IN-OUT-PAIR source INSIDE destination OUTSIDE
 service-policy type inspect IN-OUT
zone-pair security OUT-IN-PAIR source OUTSIDE destination INSIDE
 service-policy type inspect OUT-IN
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.150.16 255.255.255.255
 ip nat outside
```

```
 ip tcp adjust-mss 1160
 ipv6 address 2001:DB8:BABA:FACE:C057:9B2B:AD54:3FD2/128
!
interface Loopback1
 no ip address
!
interface Loopback999
 description workaround for CSCvb49055
 ip address 169.254.1.1 255.255.255.255
!
interface Tunnel0
 description IPsec tunnel to HER1.ipg.cisco.com
 ip unnumbered Loopback0
 ip nat outside
 zone-member security OUTSIDE
 ipv6 unnumbered Loopback0
 tunnel source Cellular0/1/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
 ip virtual-reassembly
!
interface Tunnel1
 description IPsec tunnel to HER2.ipg.cisco.com
 ip unnumbered Loopback0
 shutdown
 ipv6 unnumbered Loopback0
 tunnel source Cellular0/3/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup0
 description App ERSPAN
 ip address 192.168.10.1 255.255.255.0
!
interface VirtualPortGroup1
 description App Collection N/w
 ip address 192.168.9.1 255.255.255.0
 ip nat inside
 zone-member security INSIDE
 ip tcp adjust-mss 1160
!
interface GigabitEthernet0/0/0
 ip address dhcp
 media-type rj45
!
interface FastEthernet0/0/1
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
 switchport mode trunk
!
interface FastEthernet0/0/4
 switchport access vlan 1000
 switchport mode access
!
interface GigabitEthernet0/0/5
 switchport trunk allowed vlan 300,600,1000
 switchport mode trunk
!
interface Cellular0/1/0
```

```
 description Connection to DMZ UCS
 ip address negotiated
 ip nat outside
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/1/1
 no ip address
 shutdown
!
interface Cellular0/3/0
 ip address negotiated
 shutdown
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 2
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/3/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan200
 description CVC Collection N/w
 ip address 192.168.200.54 255.255.255.0
!
interface Vlan600
 description "GOOSE_INTERCAB"
 no ip address
!
interface Vlan1000
 ip address 192.168.0.1 255.255.255.0
 zone-member security INSIDE
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
iox
ip forward-protocol nd
!
ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip http secure-trustpoint LDevID
ip http max-connections 200
ip http timeout-policy idle 1200 life 1600 requests 10
ip http timeout-policy linger 300
ip http session-idle-timeout 1200
ip http client connection timeout 60
ip http client source-interface Tunnel0
ip nat inside source list CV_LIST interface Loopback0 overload
ip tftp source-interface Tunnel0
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 8.8.4.0 255.255.255.0 Cellular0/3/0
```

```
ip route 8.8.8.0 255.255.255.0 Cellular0/1/0
ip route 172.16.101.200 255.255.255.255 10.10.32.1
ip route 192.168.169.0 255.255.255.0 192.168.200.100
ip ssh source-interface Loopback0
ip ssh rsa keypair-name LDevID
ip ssh version 2
!
ip access-list standard CV_LIST
 10 permit 192.168.9.0 0.0.0.255
ip access-list standard FlexVPN_Client_IPv4_LAN
 30 permit 192.168.0.1
 20 permit 192.168.0.3
 10 permit 192.168.150.16
 40 permit 192.168.9.0 0.0.0.255
!
!
ip sla 201
 icmp-echo 72.163.222.229 source-interface Cellular0/1/0
  threshold 1000
  frequency 5
ip sla schedule 201 life forever start-time now
ip sla 202
 icmp-echo 72.163.222.232 source-interface Cellular0/3/0
  frequency 600
ip sla schedule 202 life forever start-time now
ip access-list standard 10
 10 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer watch-list 2 ip 5.6.7.8 255.255.255.255
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
ipv6 route ::/0 Cellular0/3/0 253
!
!
snmp-server group cgnms v3 priv
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps c3g
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server host 192.168.103.243 version 3 priv cg-nms-administrator
snmp ifmib ifindex persist
!
tftp-server 192.168.150.16
tftp-server bootflash:crashinfo_RP_00_00_20200624-141107-IST
!
!
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
 sequence 20 permit ipv6 host 2001:DB8:BABA:FACE:C057:9B2B:AD54:3FD2 any
!
control-plane
!
scada-gw protocol t101
 channel T101_ch1
  link-addr-size two
  bind-to-interface Async0/2/0
```

```
 session T101_ses1
  attach-to-channel T101_ch1
  link-addr 13
 sector T101_sec1
  attach-to-session T101_ses1
  asdu-addr 14
scada-gw protocol t104
 channel T104_ch1
  t3-timeout 20
  tcp-connection 0 local-port default remote-ip 192.168.107.200/0
 session T104_ses1
  attach-to-channel T104_ch1
 sector T104_sec1
  attach-to-session T104_ses1
  asdu-addr 15
  map-to-sector T101_sec1
scada-gw enable
!
!
line con 0
 exec-timeout 0 0
 password Cisco@123
 transport preferred ssh
 stopbits 1
 speed 115200
line 0/0/0
line 0/2/0
 transport preferred none
 stopbits 1
line vty 0 4
 exec-timeout 40 0
 logging synchronous
 length 0
 transport input all
 transport output all
line vty 5
 exec-timeout 40 0
 logging synchronous
 transport input all
 transport output all
line vty 6 14
 transport input all
 transport output all
!
!
monitor session 1 type erspan-source
 source interface Tu0
 destination
  erspan-id 1
  mtu 1464
  ip address 192.168.10.2
  origin ip address 192.168.10.1
!
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to
send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
ntp server ntp.ipg.cisco.com minpoll 9
!
!
```

```
!
!
!
!
!
!
!
event manager environment wanmon_if_list1 {Cellular0/1/0 {ipsla 201} {recovery 2 {90 75} 0}}
event manager applet test
 event track 3 state up
 action 1 syslog msg "Entered EEM_TEST"
 action 2 syslog msg "Attempting to wait 10 seconds"
 action 3 wait 10
 action 4 syslog msg "Waited for 10 seconds"
 action 5 syslog msg "Completed EEM_TEST"
event manager policy tm_wanmon.tcl authorization bypass
!
End
```

Distribution Automation HER asr1000

```
    version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname HER1
!
boot-start-marker
boot-end-marker
!
!
vrf definition test
 rd 100:100
 route-target export 100:100
 route-target import 100:100
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
logging buffered 123456789
enable secret 5 $1$lYks$nJA5/flAnLI1r0m37h6ox1
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
aaa session-id common
clock timezone IST 5 30
```

```
!
!
!
!
!
!
!
!
!
!
!


ip host rsaca.ipg.cisco.com 10.0.0.102

no ip domain lookup
ip domain name ipg.cisco.com
!
!
!
ipv6 unicast-routing
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
!
!
!
crypto pki trustpoint TP-self-signed-2024465258
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2024465258
 revocation-check none
 rsakeypair TP-self-signed-2024465258
!
crypto pki trustpoint LDevID
 enrollment retry count 10
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number
 ip-address none
 password
 fingerprint ECF92E2D5376D5E81D882E3F691FE983D15AD56C
 revocation-check none
 rsakeypair LDevID
!
crypto pki profile enrollment LDevID
 enrollment url  http://rsaca.ipg.cisco.com/certsrv/mscep/mscep.dll
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = ipg-rsa-root-ca
!
crypto pki certificate chain TP-self-signed-2024465258
```

```
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32303234 34363532 3538301E 170D3138 31313135 31313030
  34365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 30323434
  36353235 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CC31 1D958E19 7464DA4E A7DCECCA F12A265A 950D8E09 B7F7E59B 36153DB8
  E5166AE4 6D66FFBB E205E3F7 120A2EF2 412112D8 2FAEB995 1985D286 0A9E0590
  A33CB26C 9839733C E3C96818 D937B1ED 5F97AB7A DA153D88 827DB355 F8A671E1
  30E825A9 A9B21038 6AF22547 19161058 9FAA7850 16F6AD67 D88876BA D80C4FEA
  31DF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14BA8A58 4B755ACC 2AC735B3 78E0E6CD 3B2B52CE 02301D06
  03551D0E 04160414 BA8A584B 755ACC2A C735B378 E0E6CD3B 2B52CE02 300D0609
  2A864886 F70D0101 05050003 81810036 C97E100D 320CDE9A 630AAC5D 560E9BB4
  2D3238FB B892779D 2E6FA617 A0CC3866 053FC901 ADD04A0A F3FBAE26 4AAFAF6E
  F5AC2B4D 94CBEA51 2C49A700 9BE722DC F5C4179F 2C00BB7E F8780682 75B99762
  CDAAE7DF 68EE0B29 9B6B2841 CFA3C566 DB1A6CAE 4895BD4B D6E98806 43512423
  D6C67198 EE5B227F 75BC0B9F 61F6CD
        quit
crypto pki certificate chain LDevID
 certificate 650000036898107CF0E2ADE235000300000368
  308205C5 308204AD A0030201 02021365 00000368 98107CF0 E2ADE235 00030000
  0368300D 06092A86 4886F70D 01010B05 00305B31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  13301106 0A099226 8993F22C 64011916 03697067 31183016 06035504 03130F49
  50472D52 53412D52 4F4F542D 4341301E 170D3139 30363234 31313432 34375A17
  0D323130 36323431 31353234 375A3039 31143012 06035504 05130B39 53503954
  4C4F4244 33313121 301F0609 2A864886 F70D0109 02131248 4552312E 6970672E
  63697363 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500 0382010F
  00308201 0A028201 0100AB70 6355F5F0 8786F686 E535E1F5 D0B3B9C6 14B9C0D2
  1AD916F7 AC0312A9 487B87B1 97B7C44A CADA1D86 232DFB55 13A7DB40 1467A942
  42D69866 049A631B B6B5E31E 56731A7C BE16BE66 F77D6A63 D1C44395 14902CDF
  3FBF802A 5A391BA7 6BDA9522 BBFB8D45 80A5800D A421D7CF 1C86C125 F8509D47
  3C01F794 38C6A130 E4F11D6C 78845C19 BA94FBB5 2EA74673 11F62C3B F3574BF6
  043A4FDF B451720A 9A8A145A 8EACFA1B CF1FB17B EFA59E73 9680D835 D159B8DE
  7E218063 A1F44FB3 4853202E 1B8865C7 343FD1EC E29351E0 DEB4DBC9 CACDF142
  A04698EE C4CBDFB3 B57D0FD4 3F159A81 5F0A73BC 5643A095 E3997D98 5A0B95B4
  18D54FAA 889A903E 0EAD0203 010001A3 8202A230 82029E30 0B060355 1D0F0404
  030204F0 301D0603 551D0E04 1604144F D476CC37 B9BF6BFB DC1AE91E 0ADE0C2A
  8EB64B30 1F060355 1D230418 30168014 4050AD98 071BC61E AA8A0E51 6FAB766A
  41C17CE5 3081DD06 03551D1F 0481D530 81D23081 CFA081CC A081C986 81C66C64
  61703A2F 2F2F434E 3D495047 2D525341 2D524F4F 542D4341 2833292C 434E3D57
  494E3230 31322D53 45525645 52312C43 4E3D4344 502C434E 3D507562 6C696325
  32304B65 79253230 53657276 69636573 2C434E3D 53657276 69636573 2C434E3D
  436F6E66 69677572 6174696F 6E2C4443 3D697067 2C44433D 63697363 6F2C4443
  3D636F6D 3F636572 74696669 63617465 5265766F 63617469 6F6E4C69 73743F62
  6173653F 6F626A65 6374436C 6173733D 63524C44 69737472 69627574 696F6E50
  6F696E74 3081C606 082B0601 05050701 010481B9 3081B630 81B30608 2B060105
  05073002 8681A66C 6461703A 2F2F2F43 4E3D4950 472D5253 412D524F 4F542D43
  412C434E 3D414941 2C434E3D 5075626C 69632532 304B6579 25323053 65727669
  6365732C 434E3D53 65727669 6365732C 434E3D43 6F6E6669 67757261 74696F6E
  2C44433D 6970672C 44433D63 6973636F 2C44433D 636F6D3F 63414365 72746966
  69636174 653F6261 73653F6F 626A6563 74436C61 73733D63 65727469 66696361
  74696F6E 41757468 6F726974 79302006 03551D11 0101FF04 16301482 12484552
  312E6970 672E6369 73636F2E 636F6D30 3C06092B 06010401 82371507 042F302D
  06252B06 01040182 371508FC C93C82FD 9A6087F1 97168491 E921EBE9 47811F86
  FD9C1587 EDF90702 01640201 07301D06 03551D25 04163014 06082B06 01050507
  03010608 2B060105 05070302 30270609 2B060104 01823715 0A041A30 18300A06
  082B0601 05050703 01300A06 082B0601 05050703 02300D06 092A8648 86F70D01
  010B0500 03820101 0010879F EA669BA7 F157B581 0E471536 B8323C10 FB38C767
  029131BA 8879F37F B619F78B 0947F9CE 5E26D838 27849327 0675C1A4 4C1E1E07
  4777C597 6649F42C AB199417 CC2F1F7D D3787197 586D8F26 EE6829A4 F961868C
```

```
  3C803BE8 ECD825FB FAFD2923 B5B5F684 501A5E09 D8C14B79 A840E960 1721971B
  BE6EDF96 0F037D72 588CC776 46A86ACA AD6BA075 C054F00A 5A7D80DE 2A6E798E
  D20AE6B4 5FE9ADC8 D024ABD9 776A3520 A230B0E2 1AE5E8DB 280032A4 AA453085
  639E65A9 F339AE8B 4CD6FC00 4FAC78B8 C1FE8591 2A8D0E60 C2E302E6 9DE4F940
  676F232B 4169DDA3 165AB907 6F457788 FBAE8D9F B28232C6 BC1238F7 EC5929EA
  E3669184 030B50A3 D8
        quit
 certificate ca 75DF1523320095AA45C3BA7A2911F45B
  308203B8 308202A0 A0030201 02021075 DF152332 0095AA45 C3BA7A29 11F45B30
  0D06092A 864886F7 0D01010B 0500305B 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31133011
  060A0992 268993F2 2C640119 16036970 67311830 16060355 0403130F 4950472D
  5253412D 524F4F54 2D434130 1E170D31 39303631 33303032 3431315A 170D3234
  30363132 30303334 31315A30 5B311330 11060A09 92268993 F22C6401 19160363
  6F6D3115 3013060A 09922689 93F22C64 01191605 63697363 6F311330 11060A09
  92268993 F22C6401 19160369 70673118 30160603 55040313 0F495047 2D525341
  2D524F4F 542D4341 30820122 300D0609 2A864886 F70D0101 01050003 82010F00
  3082010A 02820101 00B31C98 9963A4AF FCEA5095 5FB358F3 2000A52D 890867C9
  09FAD7BC 27790580 D7BBC6E8 A8378B0E 078C9D92 5E7F4C1D 035C4FCC 0CB66109
  8442134D 8053470B 73364248 3B91A884 5C84CAA0 16754DDD 79E294CB 9DF09709
  8372B46F FD2909CD B1ABC550 6F16D6E5 610C51AA 43FF335E 0FC249F2 E4736C3D
  4377A425 C99F0EBC 4A72FD61 5078EBCD 6285E324 F8DC95B3 03BDB2A8 194AB7B5
  705FCD45 26B1D4B7 418A8532 89EEE52E 8807EC71 8016BFCB 92D156D4 D51B5491
  9EE0BF6D E1C7C81F C07942AD 8E978EDC FBAC9ED7 E8522FB0 6A344BEB D2937FF3
  708C62D0 F1F265E3 D9910167 F80FEB3C 13859DC3 ACB8DB8B 564F0FA6 70B9E5D8
  70ECA170 2CAB5438 6B020301 0001A378 3076300B 0603551D 0F040403 02018630
  0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04 16041440 50AD9807
  1BC61EAA 8A0E516F AB766A41 C17CE530 1206092B 06010401 82371501 04050203
  03000330 2306092B 06010401 82371502 04160414 D378A26B 48EE13C7 4C59E17B
  1F93A6BF 91865A1B 300D0609 2A864886 F70D0101 0B050003 82010100 9AD3942A
  93DBB586 8C1949A0 6B7D2825 2883E0A3 A2BD05FF C8EAF23B F0FD2A57 16C2D62B
  BC282219 E2C7A34F 55A2F146 5CA344FD A2887178 7BA6F2C2 29C29CEF AE722230
  26FD11B7 08397E1D 114AB736 10E740CB 1AA17602 54F99552 52765F6C 4018F7A5
  CAC6A59D 54CA13DB B6E9066D 69EDAA8B C41B2780 E1EEEBAF C937DA5B B1A1BE4D
  B84BD00F CDE650CA D39E1B62 404CF9F6 B48FE19F 04328747 BA848F2B 9823BD09
  993329D8 6C1F8CD3 C248AD46 B6539314 C2967E62 41735CD1 E4C6820D 8067B27D
  CE8848B4 2B7FB5E0 CD82E726 B3E94F9F 935A7A63 90F5D2D3 0B061409 B1D61F6C
  0937E5ED 8AD1AD90 DE66E6E7 52C7E4F8 FA7F3143 D0E1311D 8E0C
  FFD8
        quit
!
!
!
!
!
!
!
license udi pid CSR1000V sn 9SP9TLOBD31
!
spanning-tree extend system-id
!
username cisco privilege 15 secret 5 $1$DT/Y$.RJ0OiRfsrI1MV/behwjx0
username jan privilege 15 secret 5 $1$jQhm$F5fPqe3rpVUx.qPTOrqDZ.
!
redundancy
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
no crypto ikev2 authorization policy default
!
crypto ikev2 authorization policy default_No_cert
 route set interface
 route set access-list FLEX_ACL
```

```
!
crypto ikev2 redirect gateway init
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_No_cert
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
crypto ikev2 policy FlexVPN_IKEv2_Policy_No_cert
 proposal FlexVPN_IKEv2_Proposal_No_cert
!
crypto ikev2 keyring ANY
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint LDevID
 dpd 10 2 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 1
!
crypto ikev2 profile FLEX_SERVER_PROF_No_cert
 match identity remote address 0.0.0.0
 match identity remote fqdn domain gs.com
 identity local address 72.163.222.229
 authentication local pre-share
 authentication remote pre-share
 keyring local ANY
 dpd 10 2 periodic
 aaa authorization group psk list FlexVPN_Author default_No_cert
 virtual-template 3
!
crypto ikev2 fragmentation
!
crypto ikev2 cluster
 standby-group DMZ_NW
 slave priority 90
 slave max-session 100
 no shutdown
!
!
cdp run
!
pseudowire-class L2TPv3_PW
 encapsulation l2tpv3
 ip local interface Loopback0
 ip tos value 136
!
!
!
!
```

```
!
!
crypto isakmp invalid-spi-recovery
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
 mode transport
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_No_cert esp-aes esp-sha256-hmac
 mode transport
crypto ipsec fragmentation after-encryption
crypto ipsec df-bit clear
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
 responder-only
!
!
crypto ipsec profile default_No_cert
 set transform-set FlexVPN_IPsec_Transform_Set_No_cert
 set pfs group14
 set ikev2-profile FLEX_SERVER_PROF_No_cert
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.150.1 255.255.255.255
 ip ospf 1 area 0
 ipv6 address 2001:DB8:BABA:FACE::1/128
 ipv6 enable
!
interface Loopback1
 ip address 192.168.160.1 255.255.255.255
!
interface Loopback10
 ip address 192.168.161.1 255.255.255.255
!
interface Port-channel30
 no ip address
 no negotiation auto
!
interface Port-channel32
 no ip address
 no negotiation auto
!
interface GigabitEthernet1
 description UCS_INTERNAL_MGMNT_NW
 ip address 10.0.0.11 255.255.255.0
 standby use-bia
 standby version 2
```

```
 standby 10 ip 10.0.0.75
 standby 10 priority 200
 standby 10 preempt
 standby 10 name mgmnt_nw
 negotiation auto
 ntp broadcast
!
interface GigabitEthernet2
 description DMZ_NW
 ip address 72.163.222.229 255.255.255.240
 standby use-bia
 standby version 2
 standby 72 ip 72.163.222.233
 standby 72 priority 200
 standby 72 preempt
 standby 72 name DMZ_NW
 negotiation auto
 cdp enable
!
interface GigabitEthernet3
 description TPS_FND_HER_NW
 ip address 192.168.103.11 255.255.255.0
 standby use-bia
 standby version 2
 standby 103 ip 192.168.103.75
 standby 103 priority 200
 standby 103 preempt
 standby 103 name tps_fnd_her_nw
 negotiation auto
 nat64 enable
 ipv6 address 2001:DB8:103::11/64
 ipv6 address 2001:DB8:103::75/64 anycast
 ntp broadcast
!
interface GigabitEthernet4
 description HER_CPNR_NW
 ip address 192.168.105.11 255.255.255.0
 standby use-bia
 standby version 2
 standby 105 ip 192.168.105.75
 standby 105 priority 200
 standby 105 preempt
 standby 105 name her_cpnr_nw
 negotiation auto
 ipv6 address 2001:DB8:105::11/64
 ipv6 address 2001:DB8:105::75/64 anycast
 ntp broadcast
!
interface GigabitEthernet5
 description DTM_MASTER
 ip address 172.16.107.101 255.255.255.0
 standby use-bia
 standby version 2
 standby 177 ip 172.16.107.1
 standby 177 priority 200
 standby 177 preempt
 standby 177 name DTM_MASTER_NW
 negotiation auto
 ipv6 address 2001:DB8:172:16:177::11/80
!
interface GigabitEthernet6
 description DTM_MASTER
 ip address 192.168.107.11 255.255.255.0
```

```
 standby use-bia
 standby version 2
 standby 103 ip 192.168.107.75
 standby 103 priority 200
 standby 103 preempt
 standby 103 name DTM_MASTER
 ip tcp adjust-mss 516
 negotiation auto
 nat64 enable
 ipv6 address 2001:DB8:107::11/64
 ipv6 address 2001:DB8:107::75/64 anycast
 ntp broadcast
!
interface GigabitEthernet7
 description for INTER_HER_ROUTING
 platform ring rx 256
 ip address 192.168.10.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet8
 platform ring rx 256
 no ip address
 load-interval 30
 negotiation auto
 no keepalive
!
interface GigabitEthernet8.1001
 platform ring rx 256
 encapsulation dot1Q 1001
 xconnect 192.168.150.18 1001 encapsulation l2tpv3 pw-class L2TPv3_PW
!
interface GigabitEthernet8.1002
 platform ring rx 256
 encapsulation dot1Q 1002
 xconnect 192.168.150.16 1002 encapsulation l2tpv3 pw-class L2TPv3_PW
!
interface GigabitEthernet9
 ip address 192.168.109.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet10
 platform ring rx 256
 no ip address
 negotiation auto
 service instance 1001 ethernet
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  l2protocol forward
  bridge-domain 1000
 !
 service instance 1002 ethernet
  encapsulation dot1q 1002
  rewrite ingress tag pop 1 symmetric
  l2protocol forward
  bridge-domain 1000
 !
 service instance 1003 ethernet
  encapsulation dot1q 1003
  rewrite ingress tag pop 1 symmetric
  l2protocol forward
  bridge-domain 1000
 !
 service instance 8000 ethernet
  encapsulation default
  l2protocol forward
```

```
  bridge-domain 1000
 !
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1200
 ip tcp adjust-mss 1240
 nat64 enable
 ipv6 unnumbered Loopback0
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Loopback1
 ip mtu 1200
 ip tcp adjust-mss 1240
 nat64 enable
 ipv6 unnumbered Loopback1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Virtual-Template3 type tunnel
 ip unnumbered Loopback10
 ip tcp adjust-mss 1160
 tunnel source GigabitEthernet2
 tunnel protection ipsec profile default_No_cert
!
router ospf 1
 redistribute static subnets
 network 192.168.10.0 0.0.0.255 area 0
!
!
virtual-service csr_mgmt
 ip shared host-interface GigabitEthernet1
 activate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 72.163.222.225
ip route 192.168.150.2 255.255.255.255 192.168.10.2
ip ssh rsa keypair-name ssh-key
ip ssh version 2
ip scp server enable
!
ip access-list standard FLEX_ACL
 permit 192.168.109.1
 permit 192.168.109.3
 permit 192.168.109.100
 permit 192.168.109.109
 permit 192.168.161.1
 permit 192.168.105.0 0.0.0.255
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit 10.0.0.11
 permit 192.168.103.11
 permit 192.168.109.1
 permit 192.168.109.3
 permit 192.168.107.11
 permit 192.168.103.75
 permit 192.168.107.75
 permit 192.168.109.100
 permit 192.168.107.100
```

```
 permit 192.168.109.109
 permit 192.168.103.100
 permit 192.168.107.150
 permit 10.0.0.200
 permit 192.168.107.200
 permit 172.16.107.11
 permit 192.168.103.243
 permit 192.168.150.1
 permit 192.168.105.0 0.0.0.255
ip access-list standard IR1101_WANMON_TEST
 deny   1.39.183.8 log
 permit any
!
ip access-list extended CAP
 permit ip any host 157.49.138.41
 permit ip host 157.49.138.41 any
ip access-list extended EXT_ATT_CAP_FILTER
 permit ip host 72.163.222.229 host 174.232.7.36
 permit ip host 174.232.7.36 host 72.163.222.22
 permit esp host 72.163.222.229 host 174.232.7.36
 permit esp host 174.232.7.36 host 72.163.222.22
!
!
ip prefix-list tunnel_prefix seq 5 permit 192.168.150.0/24
access-list 10 permit 192.168.150.0 0.0.0.255
!
route-map tunnel_map permit 1
 match ip address 10
 match ip route-source tunnel_prefix
!
!
!
!
!
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 permit ipv6 any any
 permit ipv6 host 2001:DB8:103::100 any
 permit ipv6 host 2001:DB8:BABA:FACE::1 any
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
!
line con 0
 stopbits 1
line vty 0 4
 exec-timeout 1800 0
 transport input ssh
line vty 5 24
 exec-timeout 1800 0
 transport input ssh
!
nat64 settings fragmentation header disable
nat64 map-t domain 1
 default-mapping-rule 2001:DB8:367:BABA::/64
 basic-mapping-rule
  ipv6-prefix 2001:DB8:267:1500::/56
  ipv4-prefix 10.153.10.0/24
```

```
  port-parameters share-ratio 1 start-port 1
ntp master
ntp server 10.64.58.51
netconf max-sessions 16
netconf ssh
!
end
```