Cisco Cyber Vision Architecture Guide

Total pages: 75

Cisco Cyber Vision Architecture Guide

Rev 1.00, December, 2021

Owner: Cisco IoT Security Escalation team

Author: Cisco IoT Security Escalation team

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.
A printed copy of this document is considered uncontrolled. Refer to the online version for the latest revision.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

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

Contents

1 Introduction

This guide provides directions, reference material, recommendations and examples to help support the design of a Cyber Vision system: Center, Sensors, Global Center and third-party systems that interact with Cyber Vision.

The core components—Centers, Global Center and Sensors—are introduced first, along with the 3-tier architecture, network interfaces and segments that constitute the core system.

Examples of common architectures are provided for different sizes and topologies of OT networks, or set of networks, to be monitored.

The next chapter covers different options for Center deployments: VM or appliance, location and both necessary and optional interactions with other systems.

The chapter on Sensors addresses location, configuration and models.

The last two chapters provide references for the final choice of equipment, sizing and network configuration:

- A comprehensive list of ports and routes to be configured
- Performance requirements and network bandwidth use

Although this guide includes most of the critical information about sensors and OT network topologies, references are provided to additional guides such as the Industrial Security Design Guide and the Cyber Vision Center and Cyber Vision Sensor installation manuals.

IMPORTANT: this document is valid for Cyber Vision versions 4.0.x. Changes are expected in 4.1 regarding hardware sensors and, possibly, Global Centers. Readers should retrieve an updated version of this guide if deploying Cyber Vision version 4.1 or later.

2 Cyber Vision Terminology

2.1 Solution components

Sensor, Center and Global center are Cyber Vision solution main components.

The Cisco Cyber Vision solution can be used either as a 2-tier or 3-tier architecture:

- **2-tier architecture:** One Center + Sensors
- **3-tier architecture:** Global Center + Centers + Sensors

Cisco Cyber Vision **Sensors** are deployed at the edges of the industrial network. They receive a copy of local or remote network traffic captured by SPAN features (mirroring) or a TAP (Test Access Point), perform deep packet inspection (DPI) and transfer the lightweight analyzed metadata to a Center.

The Cisco Cyber Vision **Center** is a central platform that gathers data from all of the edge Sensors and acts as the monitoring, detection and management platform for the whole solution. On some environments, such as virtual networks, environments based on cloud solutions or for POCs (Proof of Concepts), a Sensor DPI feature can also be activated on the Center's Ethernet interface(s).

The Cisco Cyber Vision **Global Center** is an optional third tier that connects to a group of Centers. This solution allows for central monitoring of all Centers deployed within an organization, providing centralized access to the devices, activities and events, reporting and management functions.

A Center that is configured to send data to a Global Center will be referred to as a "**Center with sync**" in this document. At Center setup[1], a decision has to be made between setting the device to be a "Center" (standalone) or a "Center with sync".

2.1.1 Center

The Center receives metadata from Sensors and stores it in an internal database (Postgresql). To safeguard the data collected from the industrial network and ensure maximum reliability, Cisco-supplied appliances include a RAID storage array, redundant internal cooling fans (x3) and dual hot-swappable power supplies.

Physical Server Appliances (Fall 2021)

- Cisco UCS C220 M5
- Cisco UCS C220 M3

Cyber Vision Center

Virtual Server

- VMware ESXI 6.x or later
- Microsoft Windows Server Hyper-V 2016 or later

[1] A Center that was initialized as a standalone cannot be linked to a Global Center later (version 4.0; this may change for future versions) without reinitialization and loss of data.

Cloud Server

- AWS[2]

2.1.2 Global Center

The Global Center gets a copy of all data from linked “Centers with sync,” except flow details and process variables. Global Centers are used to push (version 4.0) knowledge database (KDB) updates to Centers to upgrade threat detection mechanisms and sync them across the entire platform. Future versions of the architecture will be able to push software updates as well.

Physical Server Appliances

- Cisco UCS C220 M5
- Cisco UCS C220 M3

Cyber Vision
Global Center

Virtual Server

- VMware ESXI 6.x or later
- Microsoft Windows Server Hyper-V 2016 or later

Cloud Server

- AWS

A Global Center should be set up first, followed by the other Centers and, finally, the Sensors. Indeed, both Sensors and Centers with sync will simply buffer all data until they can forward it to their collecting device:

Sensor’s metadata -> Center with Sync -> Global center

2.1.3 Center with Sync

A Center with sync has the same functionality as a standalone Center, complemented by a different database structure and a mechanism to reach a Global Center.

We recommend installing a Center with sync after deploying a Global Center. This will allow the Center with sync to enroll with the Global Center as soon as it is started. Otherwise, data will be buffered until the Global Center is available. In cases where multiple days may have passed, this could result in a massive transmission once connected.

During the installation of a Center with sync, the user will be required to configure Global Center data synchronization.

Physical Server appliances

- Cisco UCS C220 M5
- Cisco UCS C220 M3

Cyber Vision
Center

Virtual Server

- VMware ESXI 6.x or later
- Microsoft Windows Server Hyper-V 2016 or later

[2] Setting up a Center in the cloud, whether standalone or with sync, means that the collection network encompasses OT, local IT and internet network layers, with Sensors establishing one-way TLS connections to the Center (syslog and RabbitMQ). Sensors should be configured with an internal time source to avoid adding firewall rules (NTP on UDP 123). The installation of direct OT to internet links is often prohibited, even as a secure channel.

Cloud Server

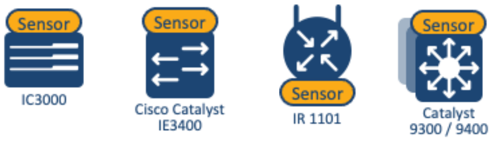
- AWS (the previous note in the Standalone Center section about direct OT-Internet connections applies to a Center with Sync as well)

2.1.4 Sensors

Edge Sensors are installed in the industrial network. These Sensors capture and analyze network traffic, decoding protocols using the Cisco Deep Packet Inspection (DPI) engine and sending meaningful information to the Cisco Cyber Vision Center.

Available Sensors (Fall 2021)

- Cisco IC 3000
- Cisco Catalyst IE3400 / IE3300
- Cisco Catalyst 9300 / 9400
- Cisco IR1101



In addition to these Sensors, one or more available Ethernet interfaces on the Center can be enabled to act as an embedded sensor. This requires either direct cabling or for traffic to be routed (RSPAN[3]) to the applicable interface(s).

2.2 Networks Segments

Three networks are involved in the Cyber Vision platform.

- **Administration Network**: used to access or manage the Center User Interface (UI) and interact with authorized external services (NTP, DNS, API orchestration, SIEM, etc.).
- **Collection Network**: used to manage all Cyber Vision Sensors. Must be isolated from the operational plant traffic (separate VLAN/subnet).
- **Industrial Network**: All industrial plant traffic and/or external interconnections meant to be analyzed by the Sensors. (SPAN traffic collected)

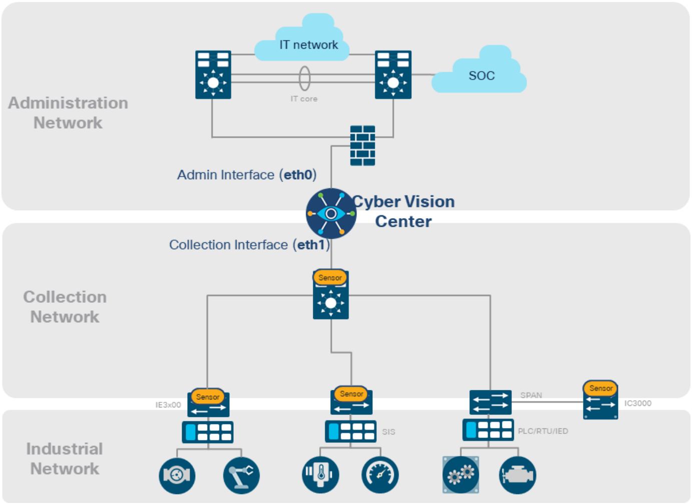


Figure 2-1 – Cyber Vision Network Segments

[3] ERSPAN to a Center DPI interface is not yet supported.

Best practice is to dedicate a separate (V)LAN to each segment. Nevertheless, it is possible to have two or even all three segments on the same LAN. If the Admin and Collection network share the same LAN, the Center must be configured to use a single interface. In these cases, eth1 shouldn’t be used for communication; the Admin and Collection interfaces should share a single IP address on eth0. This configuration (as either single or dual interface) is part of the initial Center setup and cannot be changed later.

Note that the “Administration Network” is used for both Client access (web GUI or API), syslog message forwarding and actual system administration (GUI or CLI using SSH). Throughout this guide, the term “Admin” covers both of these purposes: client access and administration.

2.2.1 Center Interfaces

By default, the Center is configured to use two interfaces (Dual Interface) in order to separate traffic between administration and collection networks. Clients with specific needs related to their network architecture can configure the Center to use a single interface.

How to choose the Center configuration between single vs dual interface?

- When the Center is located in a Data Center, it is usually easier to setup a single IP / VLAN for all connections
- When the Center is located in an iDMZ – between IT and OT: the choice depends on the DMZ internal architecture and clients location:
    - If two firewalls are used and most clients are in the IT area it makes sense to have the Center collection interface connected to the OT firewall and admin/access interface connected to the IT firewall
    - If most GUI clients are connecting from OT, a single interface makes more sense
- When the Center is located in the OT domain, the choice depends on the OT network architecture:
    - If the OT is a “flat” network (no subnets, no VLAN) then it doesn’t really make sense to setup two interfaces on the Center
    - If several VLANs are used, it is best to dedicate one VLAN to the collection network and another one to Center access/admin traffic, and two interfaces are needed on the Center

Dual Interface Center

Ethernet interfaces are allocated in the following way:

- **Administration network interface (eth0)** gives access to the user interface (GUI or API), to the CLI through SSH and is used for communication with other systems (syslog collector or SIEM, pxgrid, etc.).
- **Collection network interface (eth1)** connects the Center to the sensors.

The Center (physical or virtual appliance) has two preconfigured interfaces—eth0 and eth1—that are respectively allocated to the admin and collection networks by default.

Single Interface Center

In cases of incompatibility with the industrial network infrastructure or when the Center is setup in a remote data center, a single network interface (**eth0**) can be used for both Admin and Collection. A single IP address will be used to grant access to the Center and to manage the Sensors as well.

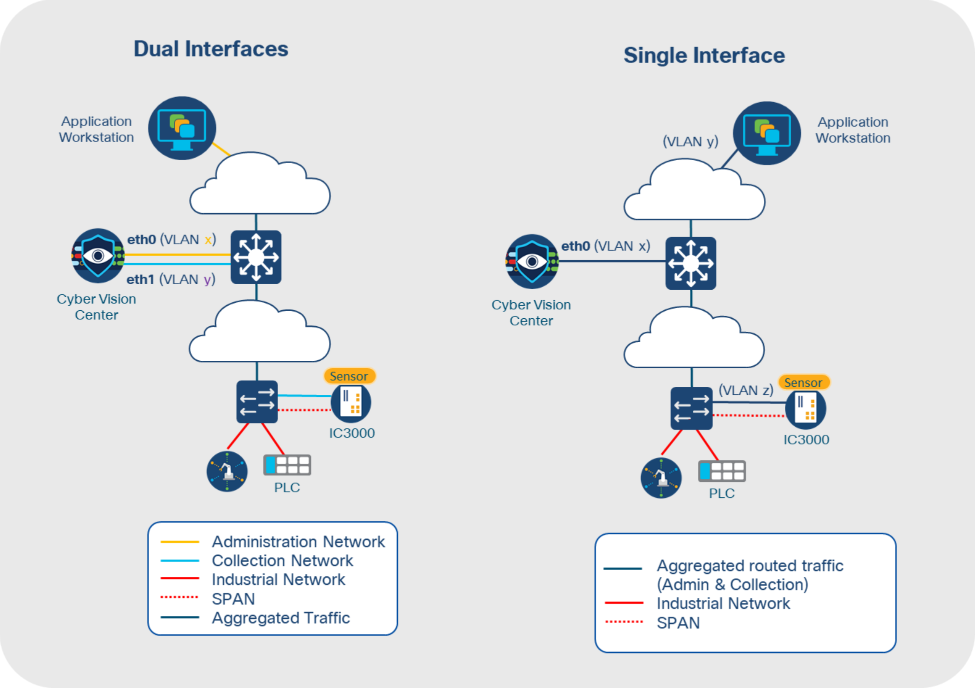


Figure 2-2 – Cyber Vision Center Dual Interface vs Single Interface

2.2.2 Sensor Interfaces

Sensors analyze data on the industrial network and interact with their enrolled Center. Each Sensor uses two networks and includes one or more optional Active Discovery interfaces. These networks can share the same LAN / subnet as the Center, although it is a best practice to use dedicated (V)LANs.

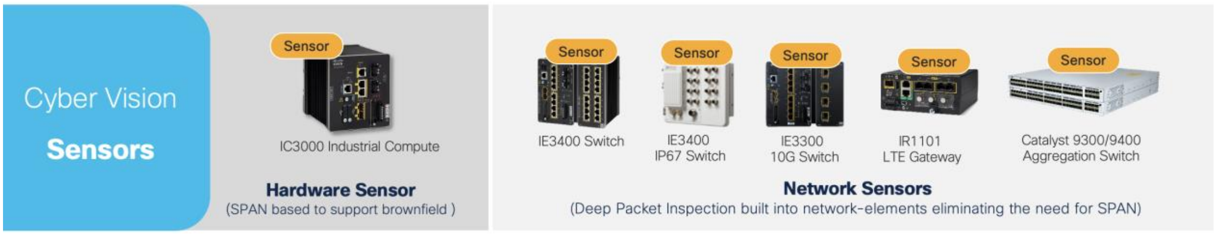


Figure 2-3 – Cyber Vision Sensors (Hardware and Network)

2.2.2.1 Hardware Sensors

- **Collection network interface (Mgt):** connects the Center to the Sensors.
- **Host device administration:** Local manager interface
  - On hardware sensors, the collection interface is used for both device management (access to the local manager web interface) and the sensor application, although two different IP addresses are used. As a result, the IP addresses for hardware device administration and sensor application collection need to be in the same subnet.
- **Industrial Network interface (Int1 – Int4)** receives SPAN traffic.
- (Optional) Active discovery interface(s) can either use the Mgt interface with a different IP address (required if the discovery IP is in the same subnet as Mgt) or an Industrial Network Interface that has been converted to Active Discovery

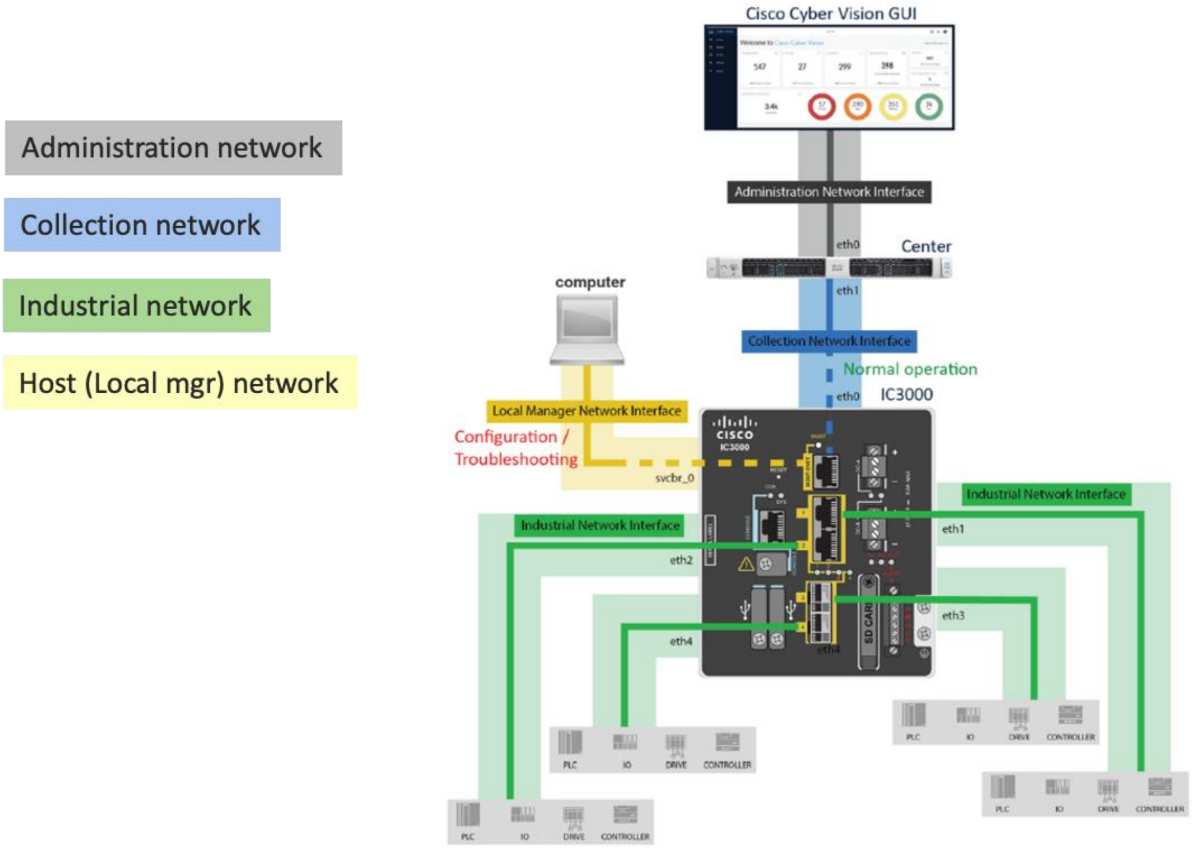
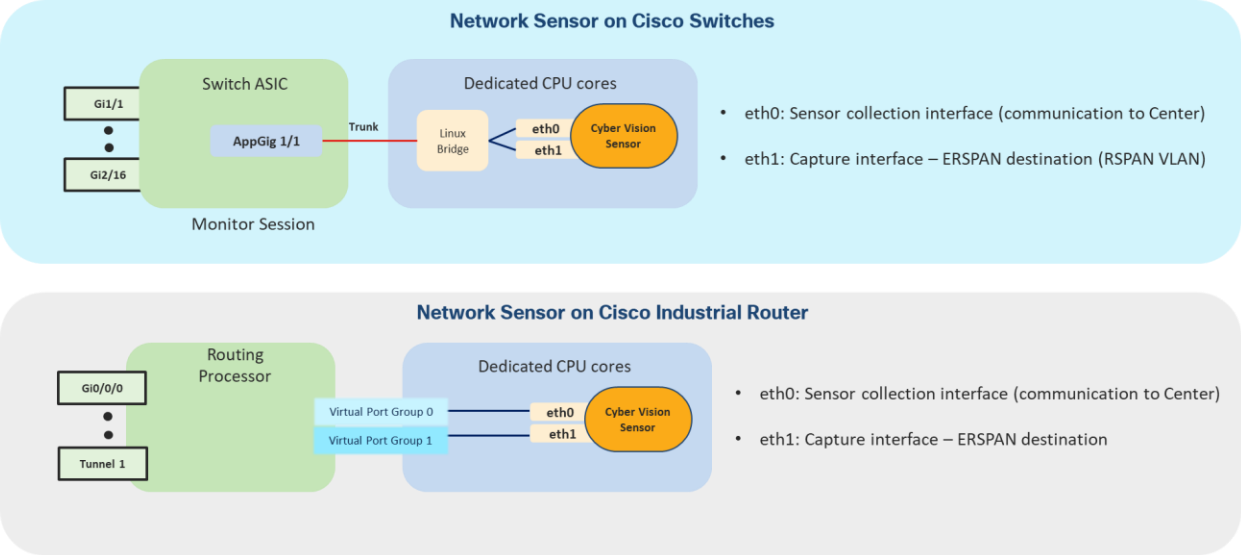


Figure 2-4 – Hardware Sensor Interfaces

Note that for the IC3000 Ethernet0 is used for both the collection interface (blue on the schematic above) and the local manager admin interface (yellow). Both need to be in the same VLAN if several VLANs are used.

2.2.2.2 Network Sensors

- **Administration network interface (IOx app eth0 Int)** connects the Center to the Sensors.
- **Host device administration**: Local manager interface
  - Any interface can be used as long as it is allowed to convey the traffic to the device's IP address for the local manager on the VLAN.
- **Industrial network interface (IOx app eth1 Int)** receives SPAN traffic.
- **(Optional) Active discovery interface(s)** can be mapped onto any IP / VLAN: the switch or router must be configured to allow that VLAN on the trunk and on selected ports.



- eth0: Sensor collection interface (communication to Center)
- eth1: Capture interface – ERSPAN destination (RSPAN VLAN)

- eth0: Sensor collection interface (communication to Center)
- eth1: Capture interface – ERSPAN destination

Figure 2-5 – Network Sensor Interfaces

More detailed instructions are provided in Chapter 5 Sensors.

2.3 Standalone, Centralized and Global Center Architectures

The type of architecture deployed depends on the use case and environment.

2.3.1 Defining Your Project

Solutions can be used for:

- **Short-term OT network assessment** projects, where it helps to clearly identify OT assets and their interactions to pinpoint vulnerabilities in both architecture and endpoints.
- **Long-term OT monitoring** to track and control process integrity in a plant and get control over industrial process assets and communications.

2.3.1.1 OT Network Assessment Project

This is the first step in any OT cybersecurity program. It seeks to assess various aspects of critical infrastructures (cybersecurity controls, control system architectures and their capabilities in terms of resiliency, availability and integrity) and provide options to mitigate and manage risks.

A Cyber Vision solution improves situational awareness, provides insight and identifies threats and vulnerabilities in your control system.

OT Assessment: OT Visibility

- Provide a comprehensive and detailed inventory of assets.
- Generate maps and lists of flows describing asset relationships.
- Identify existing issues and suggest corrective actions.

This kind of project doesn’t require a long-term deployment. A laptop may be used as the host for a Center VM to collect data from the OT network and analyze it.

The traffic collection can be performed in several ways:

- SPAN (monitoring session) the OT traffic to a hardware Sensor (e.g., IC3000) to send metadata live to the Center or store it on a USB stick (offline capture, available on hardware sensors only).
- Activate a Center DPI interface and use the laptop’s network interface card (NIC) to collect the OT SPAN traffic from different points.
- Generate external PCAPs from your OT SPAN traffic and play it into your platform.

2.3.1.2 OT Network Monitoring Project

After the assessment project and identification of all critical processes to be monitored, clients can move forward to the second step of a monitoring solution. OT networks must ensure systems are being used in accordance with their organization’s policies. This is often a key capability required to comply with legal or regulatory requirements (such as NIST CSF, NERC CIP, EU NIS...).

Cyber Vision provides the ability to detect actual or attempted attacks on industrial systems.

Operational Insights

OT network Monitoring

- Based on a prior assessment.
- Identify configurations changes.
- Control process integrity.
- Detect anomalies and malicious behaviors.

Threat Detection

- Real-time alerting.
- Integration with IT SOC.
- Automated incident responses

2.3.2 Common Architectures

The Cyber Vision platform can monitor several types of infrastructures ranging from small, local networks to large, geographically distributed ones. Although every deployment is uniquely adapted to the customer environment (which is profoundly variable), this section covers four typical architectures for the platform.

The Cisco Cyber Vision platform can be deployed as follows:

- **Standalone Architecture**
- **Multiple Standalone Architecture**
- **Centralized Multizone**
- **Global Architecture**

2.3.2.1 Standalone Architecture

A standalone architecture has one Center providing a Cyber Vision monitoring platform for one or several plants on a restricted network (geographically or physically).

In this case, the Center is either installed in the plant Control Room, in a specific server farm or an industrial DMZ (iDMZ).

Sensors can either be Hardware (dedicated appliances) or Network (switches or gateways with an embedded sensor app).

Note: This kind of plant could include zones that are completely isolated from the network. These zones can be surveyed using offline captures.

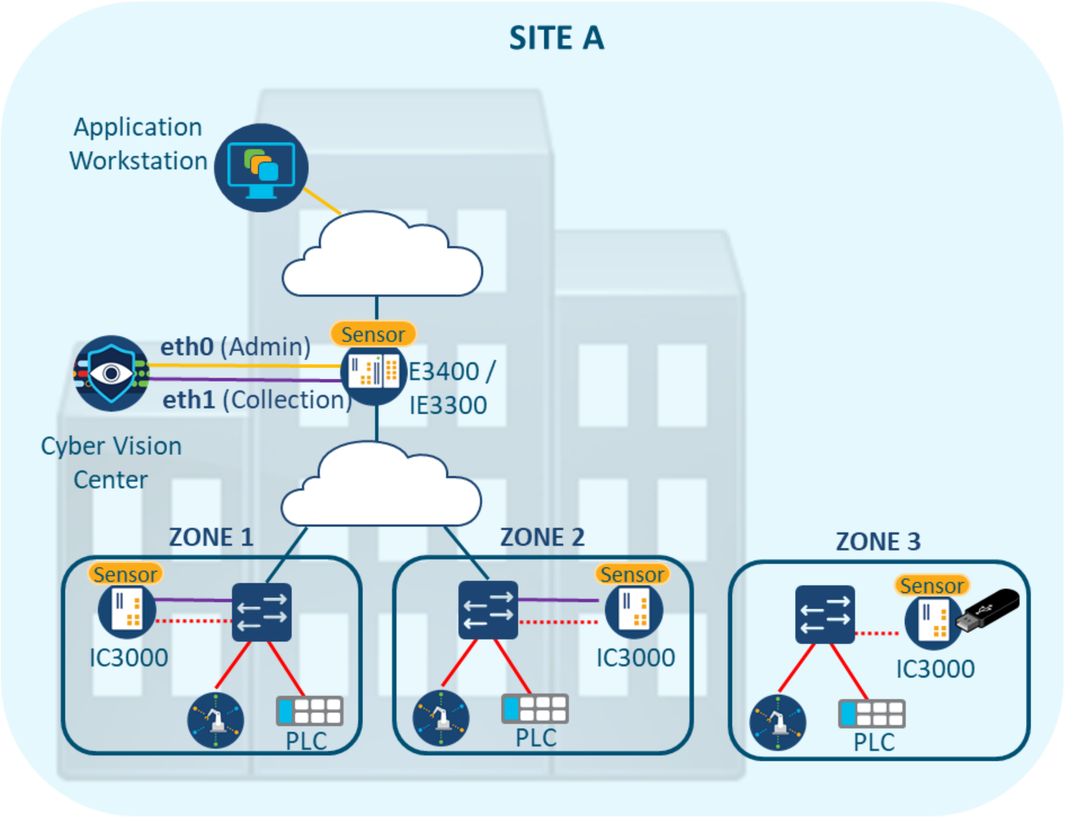


Figure 2-6 – Cyber Vision Standalone Architecture

2.3.2.2 Multiple Standalone Architecture

This architecture can be used when several isolated plants need to be monitored.

In it, a given standalone monitoring platform is reproduced in each plant.

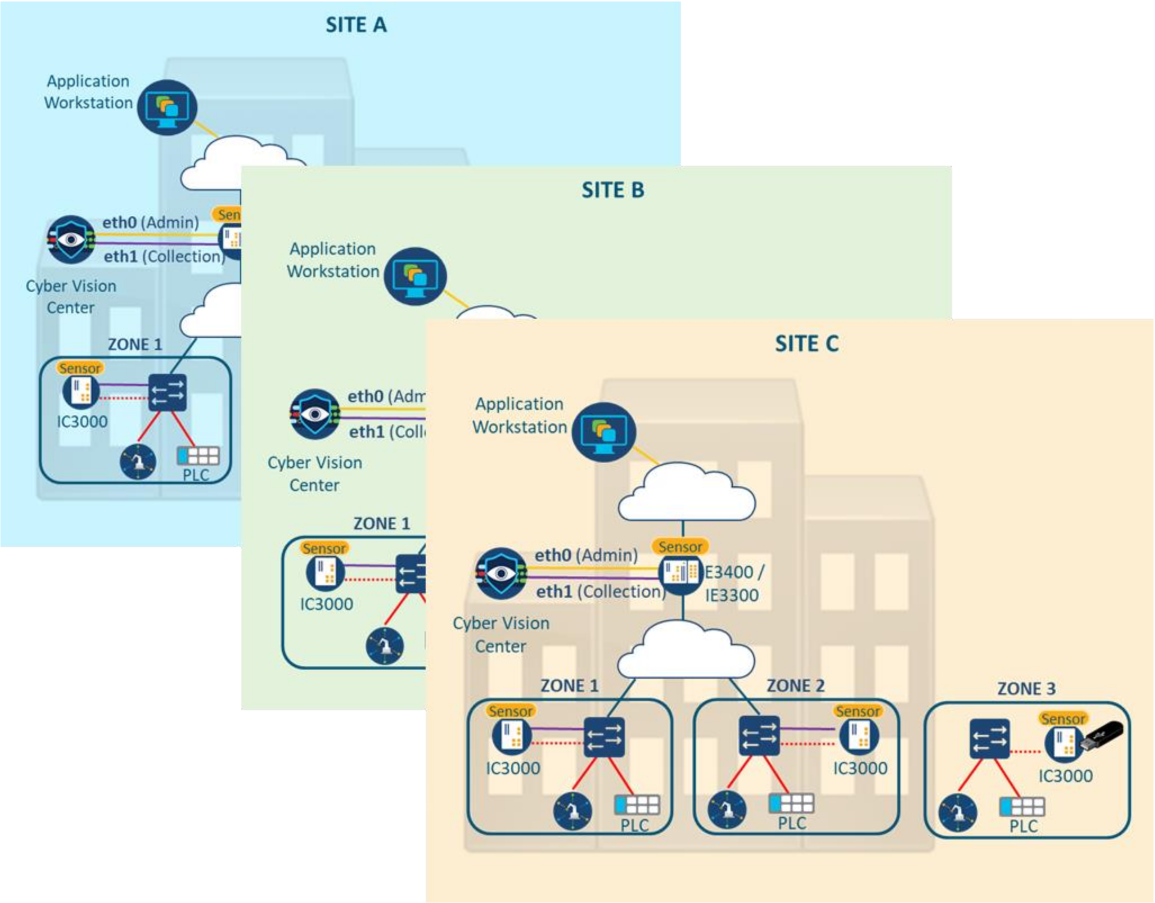


Figure 2-7 – Cyber Vision Multiple Standalone Architecture

2.3.2.3 Centralized Multizone

This architecture is often used on medium-to-large networks that include a distribution network (backbone) allowing communication between different plants or zones.

The Center aggregates data collected by Sensors on all systems under consideration and provides a centralized situational awareness for OT staff to identify relationships within the system.

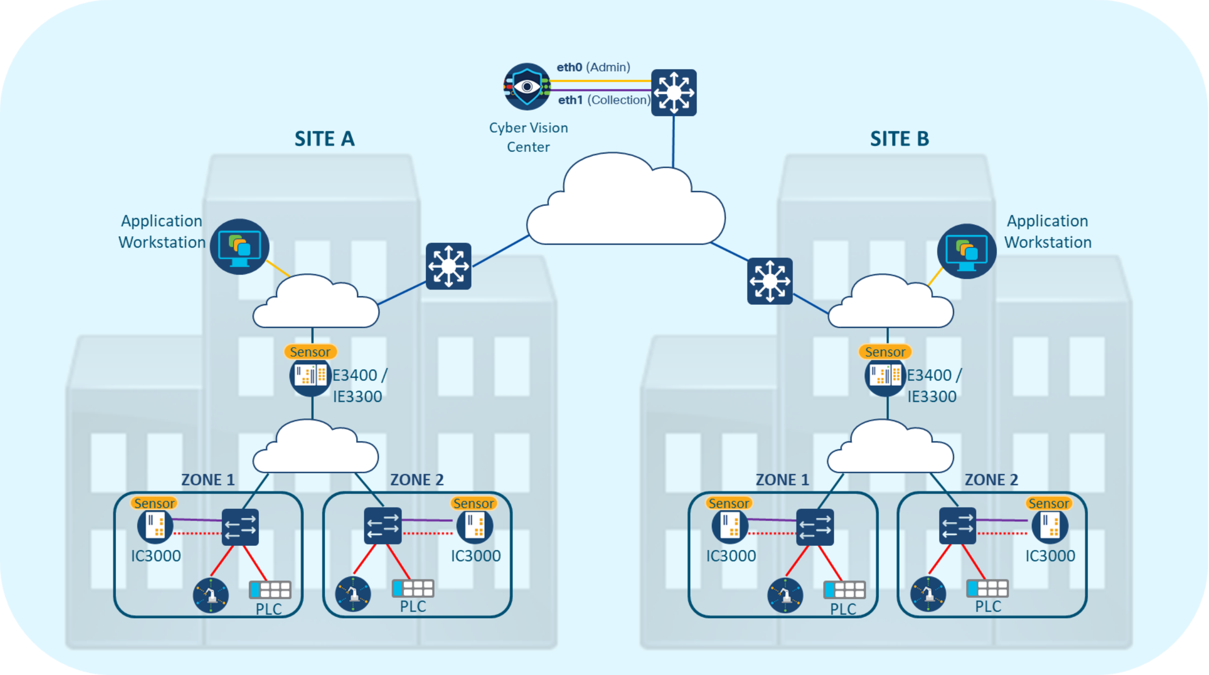


Figure 2-8 – Cyber Vision Centralized Multizone Architecture

2.3.2.4 Global Architecture

This architecture provides a global perspective for an entire organization. Each distributed site or plant is monitored by a Center, with a Global Center collecting data from each Center to allow the entire environment to be monitored from a central location (HQ/SOC).

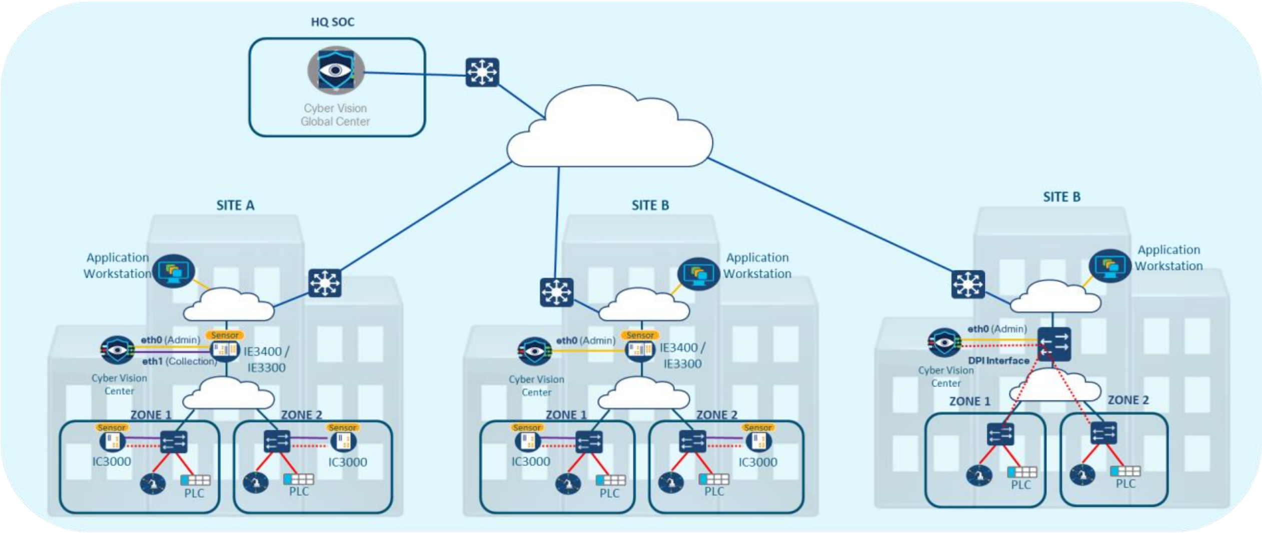


Figure 2-9 – Cyber Vision Global Architecture

2.3.3 Architecture Decision Matrix

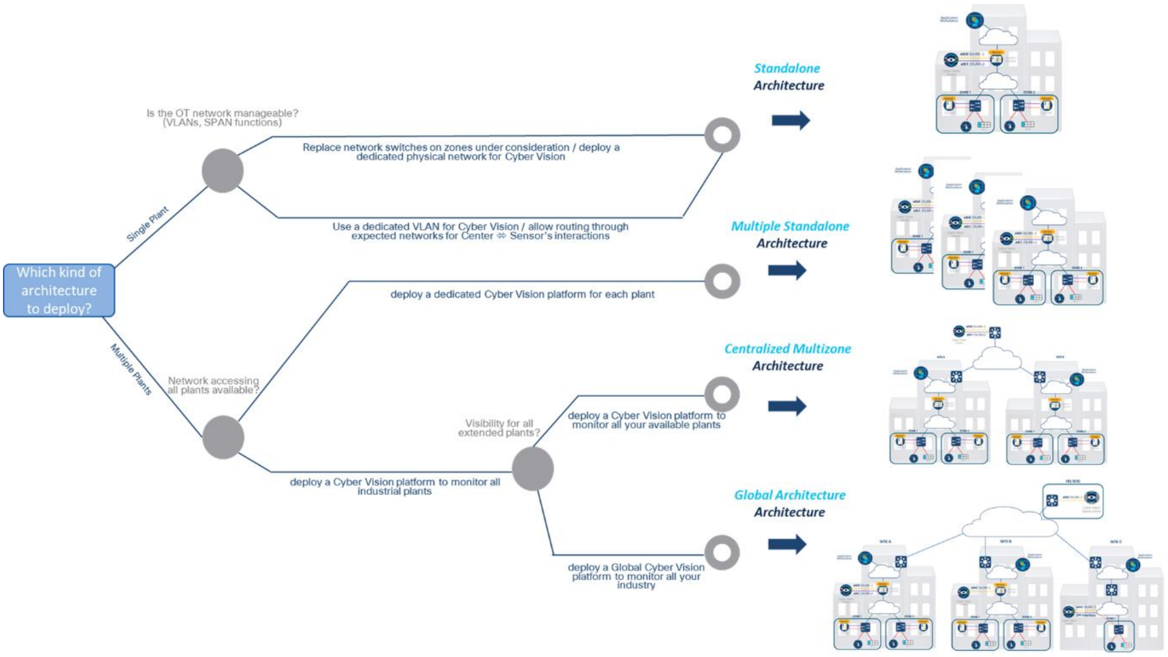

Which kind of architecture to deploy?
Single Plant
Multiple Plants
Is the OT network manageable? (VLANs, SPAN functions)
Replace network switches on zones under consideration / deploy a dedicated physical network for Cyber Vision
Use a dedicated VLAN for Cyber Vision / allow routing through expected networks for Center ⇔ Sensor's interactions
Network accessing all plants available?
deploy a dedicated Cyber Vision platform for each plant
deploy a Cyber Vision platform to monitor all industrial plants
Visibility for all extended plants?
deploy a Cyber Vision platform to monitor all your available plants
deploy a Global Cyber Vision platform to monitor all your industry
Standalone Architecture
Multiple Standalone Architecture
Centralized Multizone Architecture
Global Architecture Architecture

Figure 2-10 – Architecture Decision Matrix

2.4 Sensor Selection

Our recommendation is for customers to deploy the network sensor on the Catalyst IE3400 to provide visibility for the Cell/Area Zone. Sensors should be deployed at the edge to capture flows to and from end devices. Deploying a network/hardware Sensor at a switch where a controller is attached is an ideal choice for traffic monitoring, since all IO devices will respond to poll requests initiated by the controller. The network Sensor on the Catalyst IE3300 variant with 10G uplinks has the same advantages. Consider this option if your network needs additional bandwidth.

A Sensor may be installed on the Catalyst 9300, when it isn't possible to install a network Sensor on every device in the Cell/Area Zone, to capture flows that would otherwise be missed. For example, a Sensor installed on an industrial switch in a ring-based topology may miss a communication flow which is not in its traffic path. Deploying a network Sensor on the Catalyst 9300 will detect all inter-cell communication flows as well as flows coming from higher layers to the Cell/Area Zone. Figure 2-10 illustrates two flows that could be missed with the depicted Sensor placement. Installing a Sensor on the Catalyst 9300 would provide visibility to the north-south flow. Note that the maintenance station to I/O flow may go undetected if the flow doesn't cross the distribution switch, unless more Sensors are deployed.

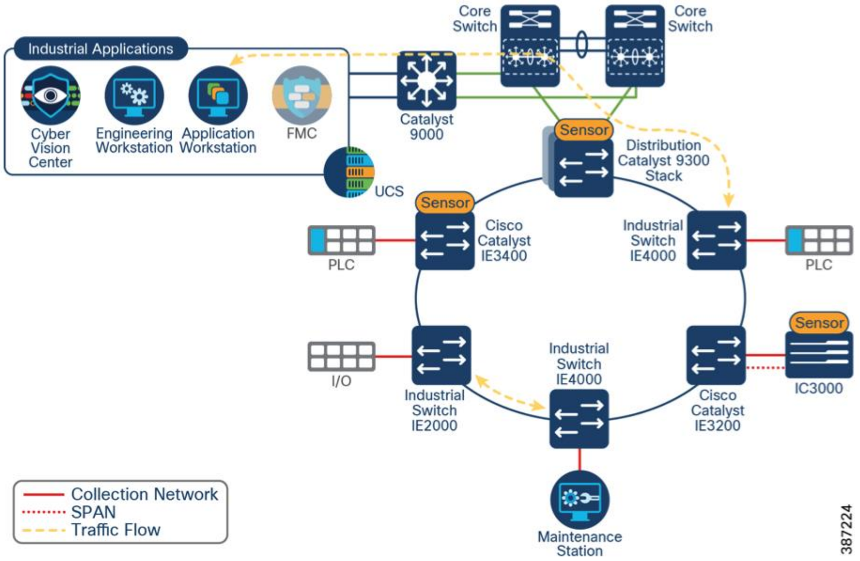


Figure 2-11 – Sensor Deployment Example

Finally, the IC3000 hardware Sensors are an option for brownfield deployments where it isn't possible to have switches that support a network Sensor. Hardware Sensors require SPAN or RSPAN to be enabled to process packets. A Cisco IC3000 deployed with Cisco Cyber Vision has two distinct sets of interfaces: a collection interface and mirror (or capture) interfaces. The collection interface is a Layer 3 interface that is used to transport the metadata to the Center. The capture interfaces collect SPAN traffic in the network from one or more VLANs.

Refer to the Industrial Security Design Guide for more examples[4] and sensor deployment options.

[4] https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.pdf

3 Cisco Cyber Vision – Common Architectures

Most industrial networks include equipment from several vendors and suppliers. Heterogeneous environments composed of different solutions and systems, managed by dozens of suppliers, are common. These environments support a large range of industrial protocols and different kinds of architecture developed over more than 15 years.

Cyber Vision can be used to both discover and monitor your industrial environment.

The Purdue model is used as a base framework for converged (IT – OT) network architectures. The Purdue model provides a standardized description of IT and OT systems by function and layer.

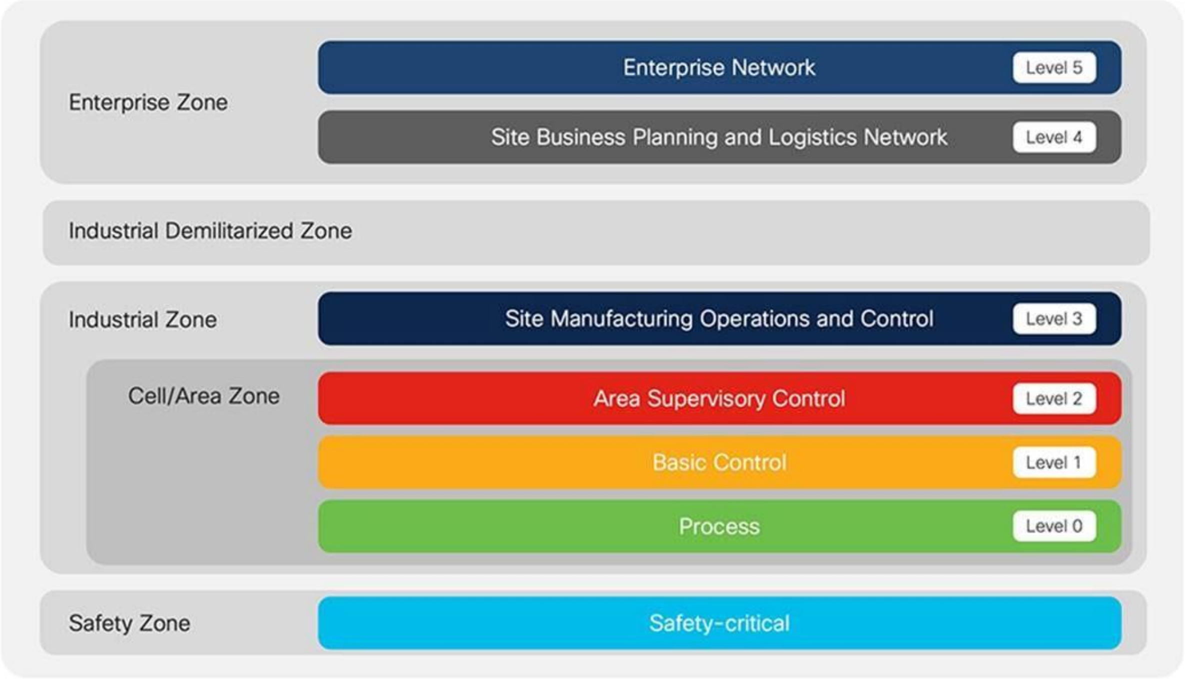


Figure 3-1 – Purdue Model

The iDMZ is not part of the Purdue model but is now commonly referred to as layer 3.5.

This document breaks the Purdue model down into different zones to provide a better understanding of industrial exchanges and how they can be tracked.

3.1 Industrial Automation Reference Architecture

The figure below highlights typical devices, applications, network infrastructure and security technology using the Purdue model framework to provide contextual information for the design and security implementation of industrial systems.

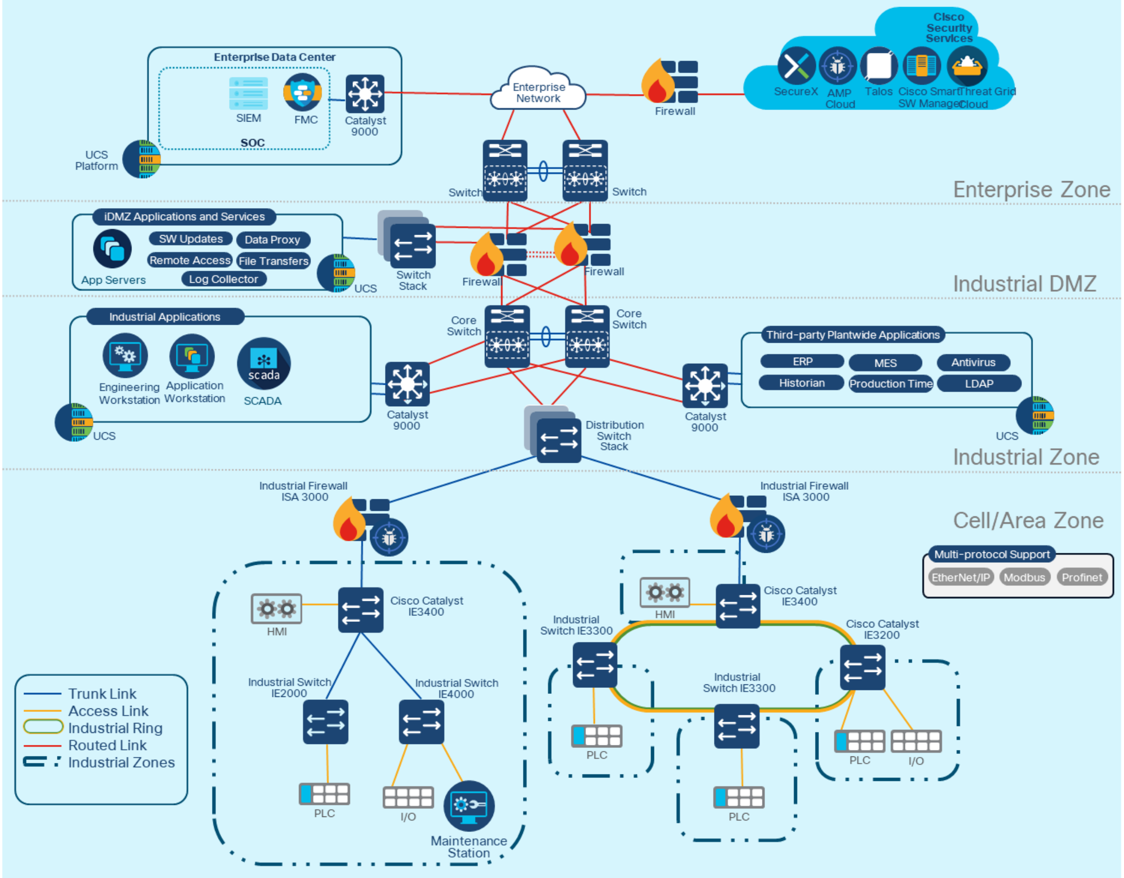


Figure 3-2 – Industrial Automation Reference Architecture

The Industrial Automation Reference Architecture is used in this document to describe Cyber Vision interactions with the environment. The architecture addresses the need to break down industrial processes into zones to monitor exchanges between them, as required in the ISA/IEC 62443 standard. Communication channels between zones are referred to as "conduits."

In the example given in the figure above, each production cell is considered a separate zone and all communications between zones can be monitored by activating a Cyber Vision sensor in the edge IE3400 switches.

The following architectures are covered in this document:

- Medium-sized segmented network (Center - dual interface)
- Medium-sized flat network (Center - single interface)
- Large network deployment (Center single interface + DPI interface)
- Distributed network deployment (Center with Sync - dual interface + GC)

- Cyber Vision integrations

As a part of this architecture reference (figure 3-2), we will describe how the Cyber Vision platform (Center and Sensors) should be deployed in these environments.

As required by the **ISA/IEC 62443-3-3** (**req. 5.2**), you must "*monitor and control communication at zone boundaries.*" This means that either firewalls (such as ISA3000) or passive Sensors should be deployed at the edge of each zone to control and monitor all network flows between them.

Sensors are usually deployed behind industrial firewalls, within a given zone. Switches within the zones are often configured to forward data through TRUNKs or Rings. In turn, those links allow all exchanges outside the zone to be monitored and give control over the enforcement of firewall rules.

The ISA/IEC standard doesn't require monitoring of flows within a zone, but it can still be deployed on a particular switch within the zone when necessary, such as when a risk has been identified by your risk analyses (such as for safety "SIS" systems).

Industrial Zone

At this level, the goal is to monitor all incoming and outgoing communications with both industrial applications and third-party plantwide application zones. Every application involved in the industrial plant operations will be tracked in these zones.

On this part of the system, application servers will reach the associated Cell/Area zones to interact with the plant and access the Enterprise zone through the Industrial DMZ (IDMZ). Pay attention when activating Sensor applications at this level, as you may end up monitoring communications through the Internet and pollute your detection strategy.

Cell/Area Zone

This part of the network is essential to plant operations and manages several processes. Each process may be segmented as a zone and should be monitored at its edges.

This area often uses L2 (Ethernet level) communications to enable industrial devices (PLC, I/O, IED, HMI, etc.) to work together.

For control and supervision, industrial devices are managed by application servers installed on the Industrial Zone. Connections can be initiated from the servers to monitor processes and configure devices, or they can be initiated by the devices themselves to send alerts about errors or update the status of processes.

Sensors should be activated on the switches that aggregate connections to the distribution level (IP Level). Check the sensor's DPI capability to ensure that the selected traffic can be analyzed (see chapter 5_Sensors). In cases where bandwidth exceeds the sensor's DPI capability, consider upgrading the switch model, adding a dedicated physical sensor or reducing the amount of traffic to be analyzed[5].

A reduction of the traffic to be analyzed can be accomplished in two ways:

- Change traffic mirroring (selection of ports or VLAN)
- Add a filter as a "capture mode" on the sensor configuration

[5] Sensor configuration allows to add a filter to ignore some traffic or to focus on specific communication types

This needs to be done carefully so that desired traffic is still monitored. Generally, this will be traffic between cells/zones. Often, traffic within a zone can be ignored.

All sensors perform DPI on traffic and extract properties that are sent to the Center to keep track of network behavior in terms of devices and activities and to provide access to process variables. This allows the system to use baselines to compare reference traffic with actual traffic and report any differences.

A selection of sensors can also perform threat detection based on Talos Snort signatures (IC3000, Catalyst 9x00 series, Center embedded sensors – to date).

3.2 Medium-Sized Network (Center - Dual Interface)

In this example, the Cyber Vision Center is installed at the level of the Industrial Zone and sensors are deployed in different zones (Industrial and Cell/Area) to track their exchanges. Two Catalyst 9400/9300 are used to track the Industrial Zone exchanges and other network/hardware sensors are deployed at the Cell/Area level to track plantwide system activities.

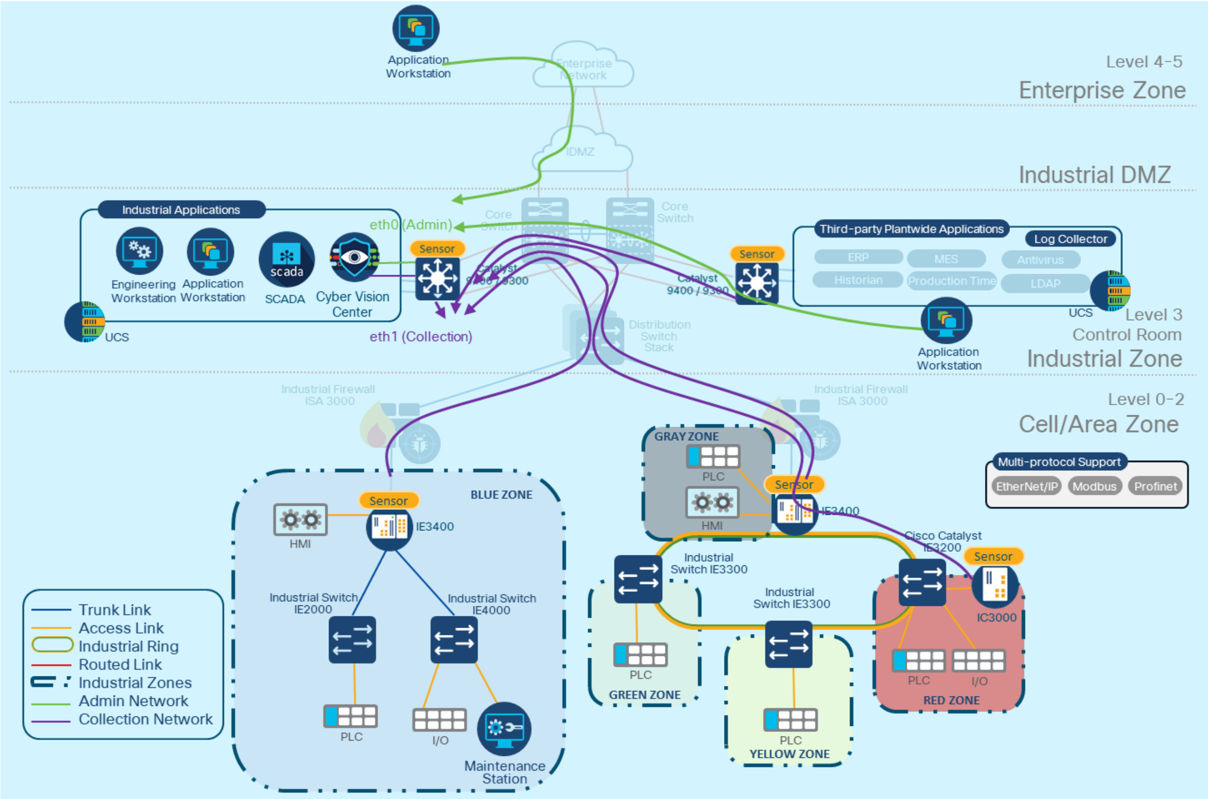


Figure 3-3 – Center Dual Interface Interactions

Administration and Collection flows between the Center and Sensors should be allowed on firewalls at different levels to enable access to your platform, see “Chapter 6 - Required UDP and TCP Flows for Cyber Vision” for the list of ports in use.

Industrial Zone

In this zone, the Catalyst 9400/9300 switches connect servers to the CORE network (IP routing). Servers are connected to a TRUNK or an access port on the switch and the third-party application or the Cell/Area Zone, with those connections passing through the iDMZ.

The Cyber Vision platform is designed to monitor a whole industrial plant. To ensure the best performance of the system, the traffic to be monitored should be carefully selected to avoid exceeding bandwidth limits and packet duplication at the Center. While this should be done before deployment, such tuning is typical during the first weeks based on actual traffic and using the appropriate diagnosis tools: Sensor packet inputs, deduplication levels, CPU/RAM load, etc.

It's best to have one dedicated Sensor per LAN. Avoid having several sensors monitoring the same traffic (both sides of a router, for example). Cyber Vision Centers will aggregate data on devices and activities, but more focused monitoring reduces system load and makes analysis and forensics easier.

For instance, avoid enabling both ACCESS and TRUNK port mirroring, as it doubles the number of packets fed to the DPI engine and the bandwidth used if the mirrored traffic is sent over RSPAN.

Traffic flowing between two zones and observed by several sensors can also be reduced by telling one sensor to ignore it and leaving the other unit to perform the DPI.

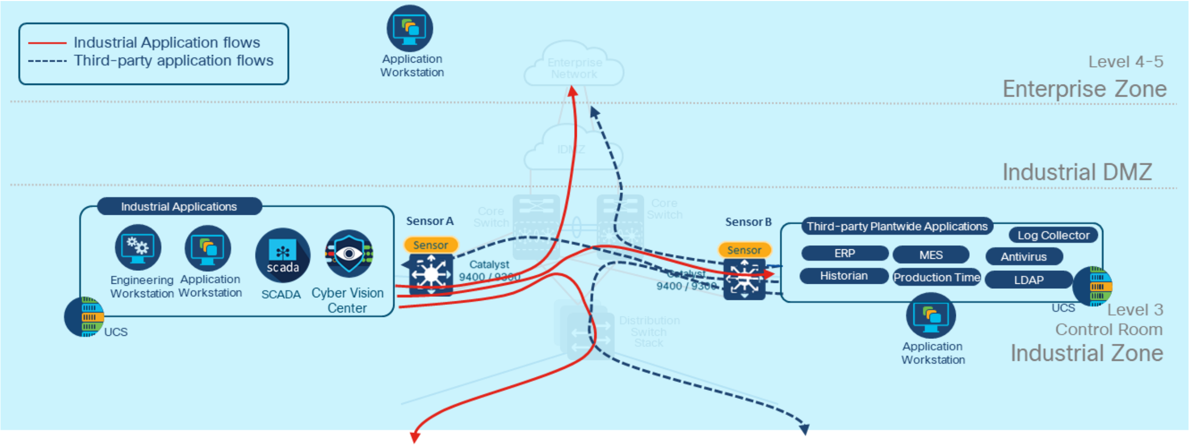


Figure 3-4 – Flows Between Zones

In this example, Sensor A (industrial application Sensor) shouldn't monitor subnets used by the third-party applications because they are already monitored by Sensor B.

Flows between the Cell/Area zone could be collected at this point (centralized point for monitoring the whole plant) or by Sensors installed in the Cells themselves. Note that the ISA/IEC 62443 standard requires monitoring flows between zones but not within zones. From a cybersecurity point of view, the focus should be on inter-zone traffic. However, process monitoring or detailed mapping may require monitoring intra-zone flows.

A focus on inter-zone communications further reduces the DPI load and the amount of information sent to the Center, making it easier to use field devices with lower DPI capabilities (such as a sensor embedded in a switch) to monitor relevant traffic.

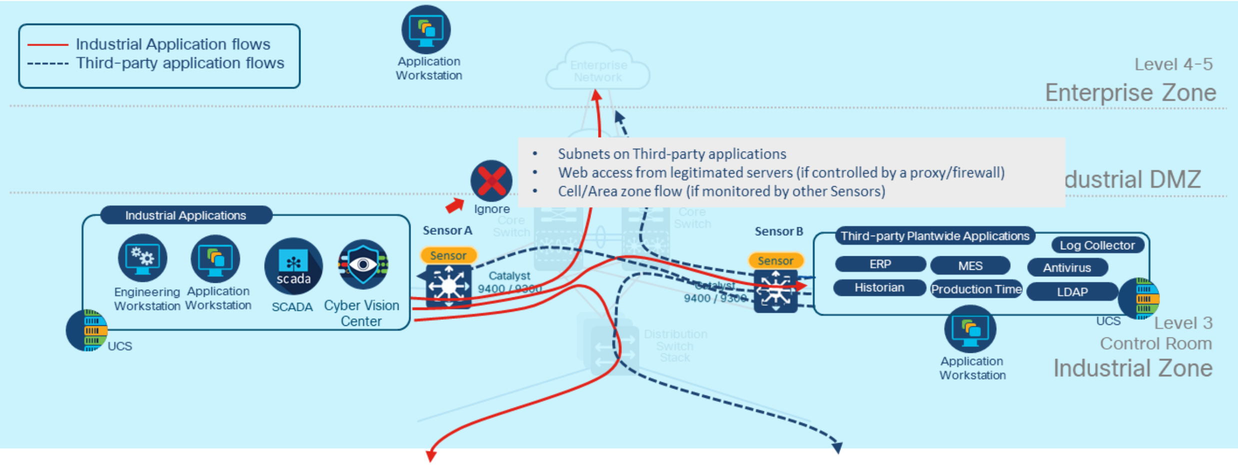


Figure 3-5 – Ignoring Flows Already Monitored in the Industrial Zone

In the example given above, where traffic would be analyzed by more than one Sensor, either the switch SPAN (mirroring) configuration or the Sensor capture mode (filter) should be altered in one of these Sensors. For instance, Sensor A can be configured to ignore the traffic between the two zones (since it is already analyzed by Sensor B) by removing the Ethernet port from the SPAN session, if there is a trunk A-B, or adding a filter on Sensor A to ignore traffic to and from the subnet of zone B.

Cell/Area Zone

Multiple and heterogeneous protocols and architectures exist at this layer. The best strategy is to identify different zones and the conduits that move data in and out of them, and then to monitor those conduits.

In the examples below, the Cell/Area zone is split into several smaller areas identified by colors. Each of the smaller areas corresponds to an industrial process or system. There might be a physical network and subnet dedicated to each zone, VLANs might be used on a single physical network, and sometimes all zones could share a single large LAN.

Note: In this last case, when all devices are on the same LAN, best practice would be to devise a plan to segment the network for security and not only for traffic monitoring. Monitoring is possible but high capability sensors are required as much more information than needed will be collected without a practical way to focus the monitoring.

Considering the blue zone (figure 3-6) at this plant, exchanges inside the zone usually don’t need to be monitored, but all incoming and outgoing traffic should be tracked and analyzed.

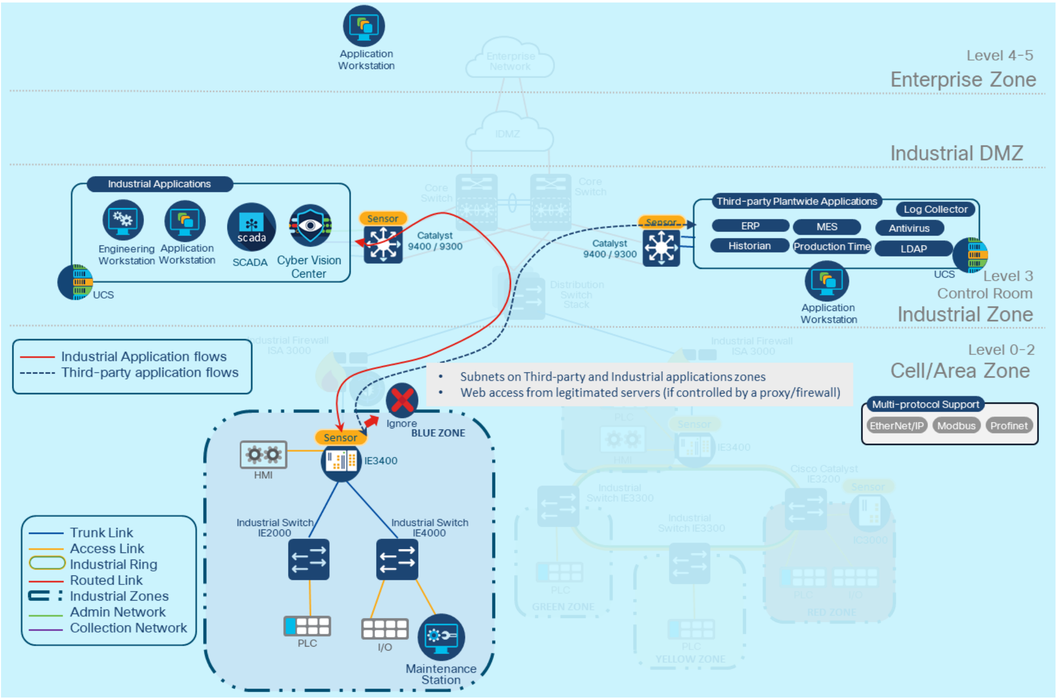


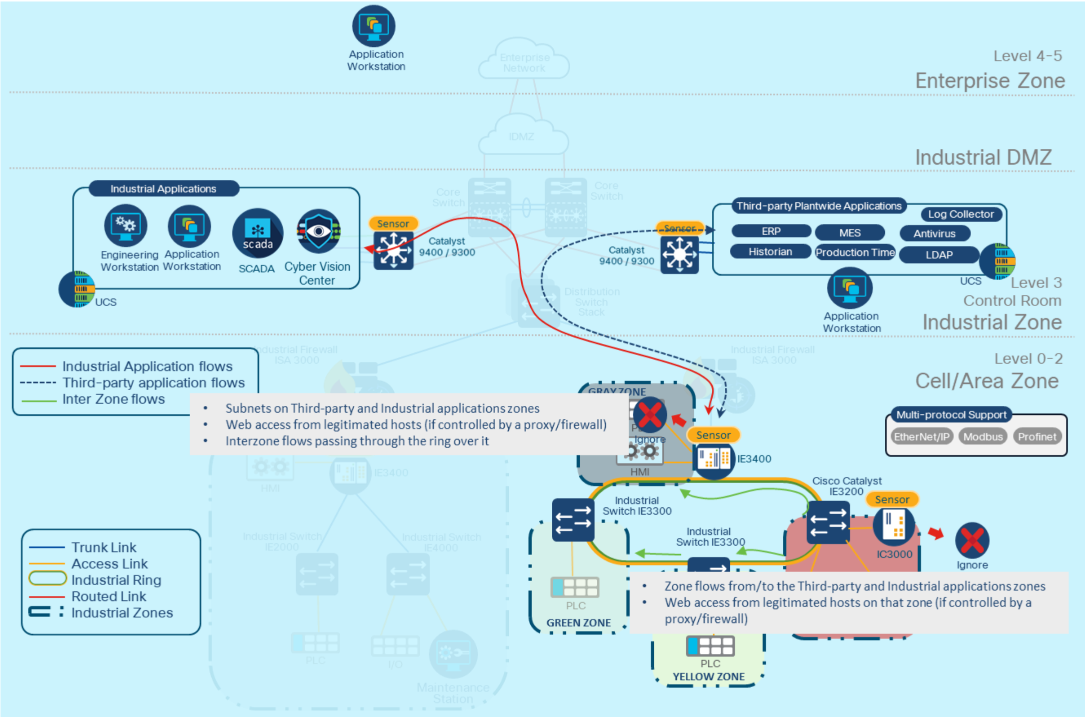
Figure 3-6 – Ignoring Flows Already Monitored on Cell/Area Zone

On this kind of architecture, we may want to collect all traffic from the switches on the distribution switch level. This could work well if the switch has the capability to monitor the whole network.

In our example, the IE3400 is performing a VLAN aggregation to the distribution network, making it a great point of collection for the entire Blue Zone. Other zones will be monitored by other sensors.

As identified in the first point (industrial zone), flows from the Blue Zone are forwarded to both application zones. This is why filters can be used to ignore those flows in sensors in the application zones.

The same strategy should be applied on Cell/Areas with aa self-healing ring network topology. In this second example, the different zones (Grey, Green, Yellow and Red) are all attached to a ring and reach the industrial application zone through a resilient network. All of this traffic is aggregated by the IE3400 at the top of the ring, as shown on figure 3-7.



- Subnets on Third-party and Industrial applications zones
- Web access from legitimated hosts (if controlled by a proxy/firewall)
- Interzone flows passing through the ring over it

- Zone flows from/to the Third-party and Industrial applications zones
- Web access from legitimated hosts on that zone (if controlled by a proxy/firewall)

Figure 3-7 – Flows on Cell/Area Zone

A monitoring session configuration on the IE3400 is enough to monitor exchanges and track communications between the Industrial Zone and Cell/Area zone. On the other hand, inter-zone flows (communication between the colored zones) will not be monitored if traffic doesn’t pass through it.

In our example, the Red Zone is allowed to access all other colored zones in this area (Gray, Green and Yellow). Even if traffic flowing through the IE3400 is monitored, it will miss traffic that only flows between IE3300 units. An additional sensor needs to be installed to track inter-zone communications from the Red Zone.

3.3 Medium-Sized Network Deployment (Single Interface)

The examples given above provide some idea of which industrial flows can be captured and monitored by the Cyber Vision platform. In this new example, the Center is deployed with a single interface. This means that Administration, Maintenance and Collection exchanges all pass through the same network interface.

The recommended configuration is for customers to deploy a Center with a dual interface, physically isolating access to these networks and increasing their protection. However, even if a Center is used with a single interface, the networks will still be logically isolated by the internal firewall and hardening process.

In this architecture example, we focus on Cyber Vision Center interactions on the industrial zone level, such as with a log collector (SIEM/Syslog), NTP server, Engineering Workstation, and so forth. We then cover a very common industrial networking application: mapping multiple OEM machines, production lines and/or systems configured with identical parameters (IP addresses, industrial programs) on the Cell/Area zone using Network Address Translations (NAT).

On the Cell/Area zone, all four colored zones (gray, green, yellow and red) are deployed on the same LAN (192.168.1.0/24). To avoid network routing conflicts, the firewall must perform a 1:1 NAT. The use of NAT mapping for IP addresses has an impact on the Sensor's deployment.

The IC3000 Hardware Sensor is deployed to monitor traffic within the red zone, to monitor this Safety System (SIS).

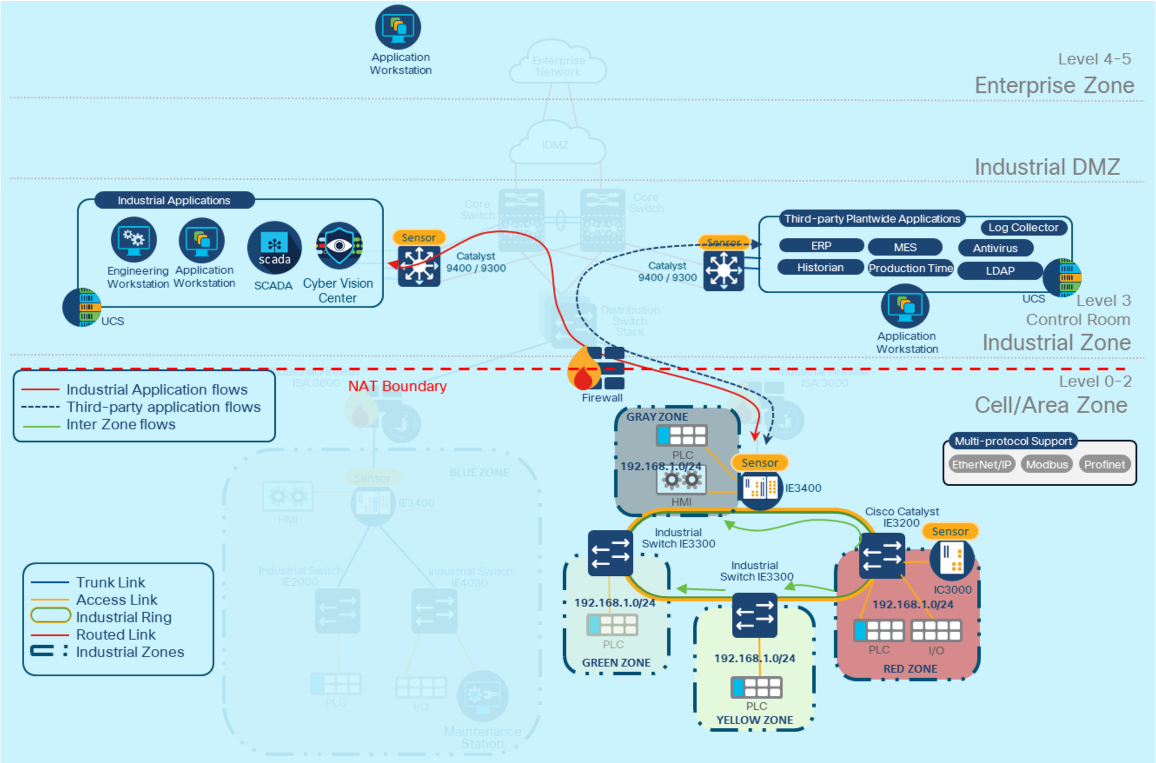


Figure 3-8 – Center Single Interface Interactions

Industrial Zone

In this zone, the Cyber Vision Center interacts with industrial and third-party plantwide application services. Both administration and maintenance flows from and to the Center pass through its admin (eth0) interface. The firewall should allow all required flows for the Cyber Vision system.

Application and Engineering Workstations

These system access the Center UI (user interface) through a native web-based environment and interact with the platform using their account profiles. This traffic is transported over HTTPS (TCP 443). The Center's Cyber Vision self-signed certificate should be installed on the workstation to grant secure access to it.

Another important flow required for maintenance and support tasks is SSH (Secure Shell, TCP 22). This service is required to securely import and export data to the Center.

Network Services

Services like the Network Time Protocol (NTP, UDP 123) and Syslog (UDP 514) are used by the Center. The first is used to synchronize time and the other sends Cyber Vision events to an external server (log collector or SIEM).

Syslog messages are forwarded in clear text or can be secured using TCP over TLS.

Cell/Area Zone

This zone is composed of the specific industrial zones under consideration. Generally, Sensors are deployed in this zone to control exchanges between them. If Sensors can't be installed in these zones, traffic can instead be analyzed with an offline Sensor, which generates an offline file that can be imported to the Center later. Another option would be to transport RSPAN/SPAN traffic to a DPI interface on the Center.

Our concern in this example is the network translation (NAT) performed at the edge of that zone to let the industrial servers reach the different colored zones, which are configured with the same subnet range (192.168.1.0/24, in our example). The IC3000 is deployed in the red zone and has an IP address on that network.

The complexity here is that, from the distribution network or Center's point of view, the subnet 192.168.1.0/24 isn't reachable. The Center will be able to access only the external routed address from that zone. To manage this situation, certain adjustments to the Center/Sensor configuration are required. (See 5.4.2.2 for NAT-specific configuration).

3.4 Large Network Deployment (Single + DPI)

The large network deployment example considers a Center deployed in a HQ Datacenter and monitoring Sensors deployed on different sites (maybe in different geographical locations).

Based on this architecture, we suggest using a virtual private network (VPN) solution to ensure confidentiality and integrity for these exchanges. Communication between the Center and Sensors is performed by a message broker mechanism (AMPQ – Advanced Message Queuing Protocol, TCP 5671) through a cyphered (TLS 1.3) session, which secures their exchange.

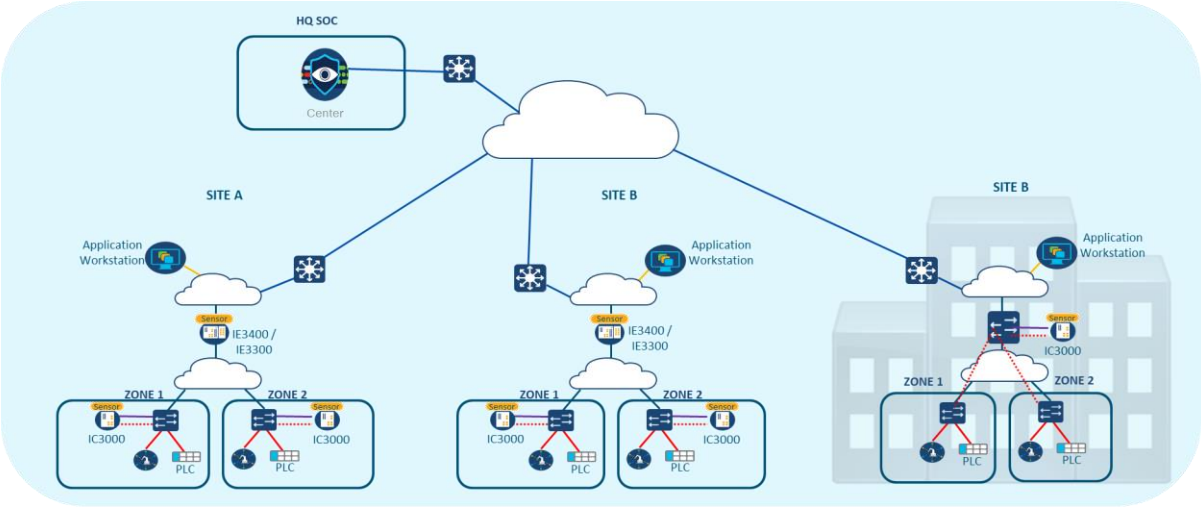


Figure 3-9 – Multi Site Deployment

To establish connectivity between the Center and Sensors on this architecture, all required flows will have to be allowed on the firewalls protecting the VPN. Interactions through the Cyber Vision platform don't significantly increase bandwidth consumption or result in higher network use due to their small payload of metadata analyses.

Industrial Zone

The Cyber Vision Center interacts with industrial and third-party plant-wide application services on this zone. Both administration and maintenance flows from and to the Center pass through its admin (eth0) interface. The firewall should allow all required flows for the Cyber Vision system.

3.5 Distributed Network Deployment (Dual + Global Center)

The figure below presents a global architecture connected to a Cyber Vision Global Center deployed within the HQ SOC.

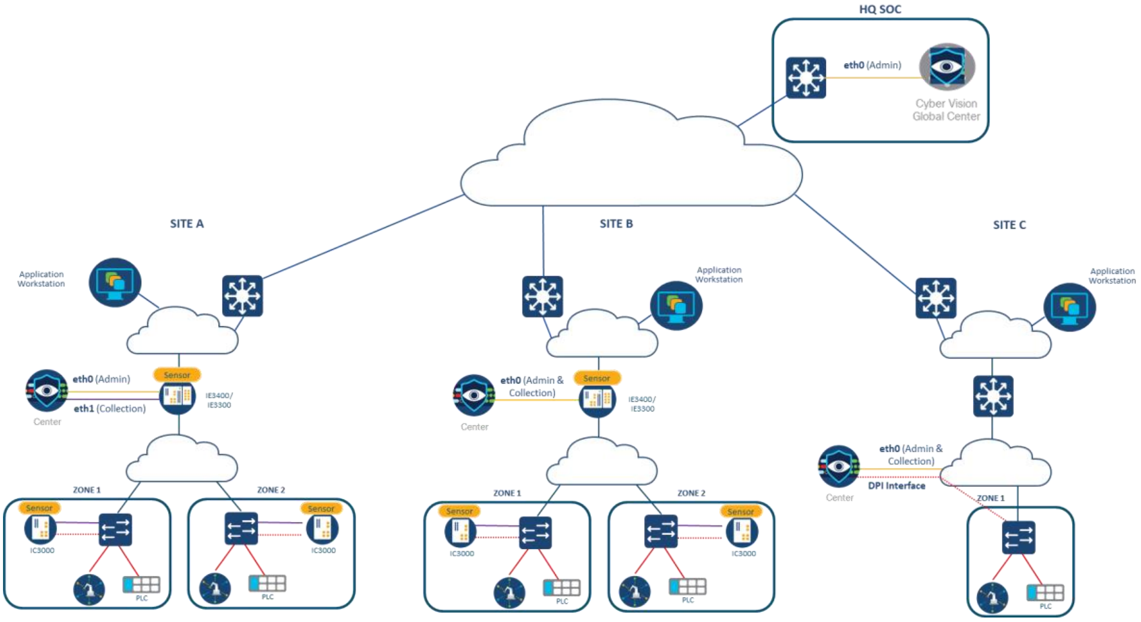


Figure 3-10 – Global Three-Tier Architecture

4 Cyber Vision Considerations for Center Deployments

4.1 Cyber Vision Centers

Two types of Center installation are possible, either as a physical appliance (Cisco UCS servers) or a Virtual Machine (VMWare or HyperV).

Several characteristics should be considered for each type. The Center can be standalone or a Center with sync.

Depending on the use, either **Single or Dual interface** can be selected, depending on the network topology and security requirements:

- If the Center is set in the iDMZ as a dual device attached to both the IT and OT networks, it is best to use two interfaces;
- If the Center is installed in a remote location (such as a corporate data center), it would be cumbersome to reserve two IP addresses and route two VLANs up to the data center server.

4.1.1 Center as VM

As a virtual machine, please make sure that the following conditions are met.

Required configuration for a VM:

Hypervisor:

- VMware vSphere 6.x or later.
- OR
- Microsoft Hyper-V Server 2016 or later.

OR

- Amazon AWS

Make sure hypervisor is set with the necessary rights for the instantiation of a new VM.

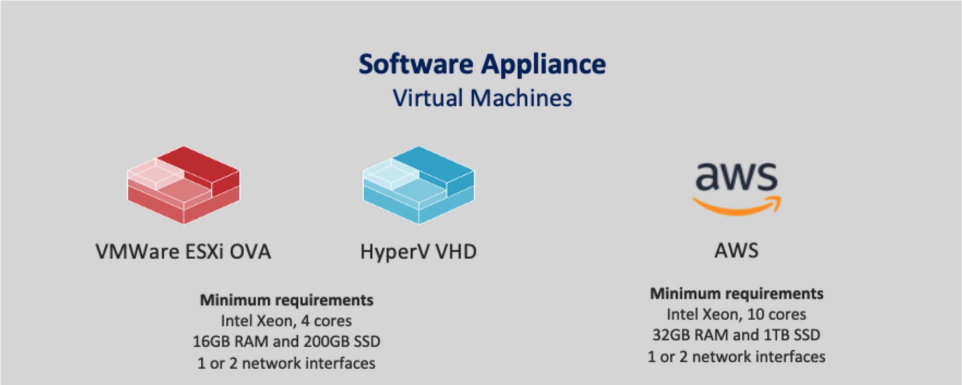
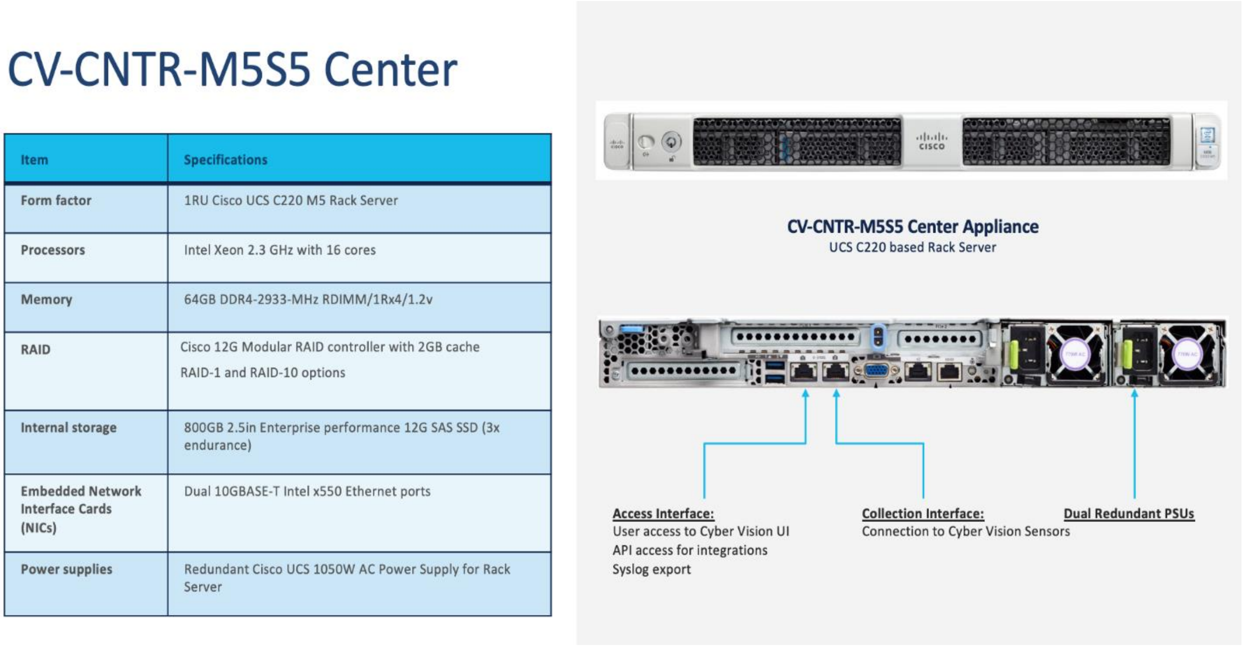


Figure 4-1 – Center VM Requirements

4.1.2 Center Appliances

Two appliance models are available for the Center:



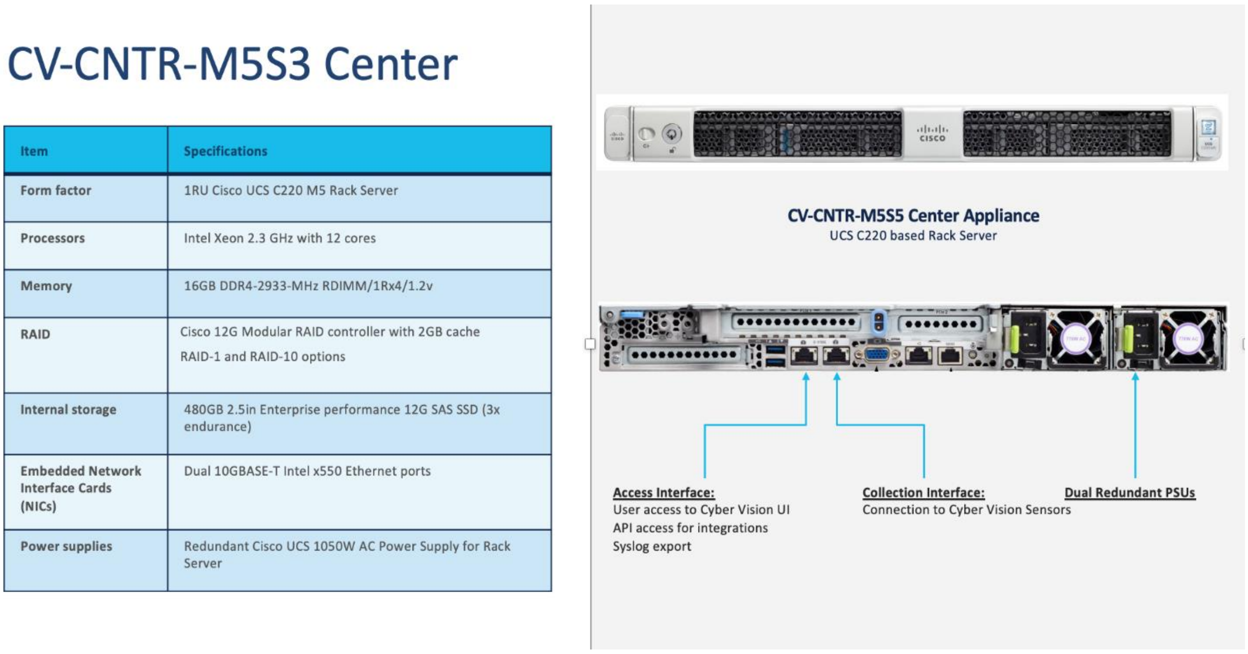
CV-CNTR-M5S5 Center

Item	Specifications
Form factor	1RU Cisco UCS C220 M5 Rack Server
Processors	Intel Xeon 2.3 GHz with 16 cores
Memory	64GB DDR4-2933-MHz RDIMM/1Rx4/1.2v
RAID	Cisco 12G Modular RAID controller with 2GB cache RAID-1 and RAID-10 options
Internal storage	800GB 2.5in Enterprise performance 12G SAS SSD (3x endurance)
Embedded Network Interface Cards (NICs)	Dual 10GBASE-T Intel x550 Ethernet ports
Power supplies	Redundant Cisco UCS 1050W AC Power Supply for Rack Server

CV-CNTR-M5S5 Center Appliance
UCS C220 based Rack Server

Access Interface:
User access to Cyber Vision UI
API access for integrations
Syslog export
Collection Interface:
Connection to Cyber Vision Sensors
Dual Redundant PSUs

Figure 4-2 – Center M5S5



CV-CNTR-M5S3 Center

Item	Specifications
Form factor	1RU Cisco UCS C220 M5 Rack Server
Processors	Intel Xeon 2.3 GHz with 12 cores
Memory	16GB DDR4-2933-MHz RDIMM/1Rx4/1.2v
RAID	Cisco 12G Modular RAID controller with 2GB cache RAID-1 and RAID-10 options
Internal storage	480GB 2.5in Enterprise performance 12G SAS SSD (3x endurance)
Embedded Network Interface Cards (NICs)	Dual 10GBASE-T Intel x550 Ethernet ports
Power supplies	Redundant Cisco UCS 1050W AC Power Supply for Rack Server

CV-CNTR-M5S5 Center Appliance
UCS C220 based Rack Server

Access Interface:
User access to Cyber Vision UI
API access for integrations
Syslog export
Collection Interface:
Connection to Cyber Vision Sensors
Dual Redundant PSUs

Figure 4-3 – Center M5S3

4.1.2.1 Access to the Center

An external device is required to access and configure the Center.

To do so, connect an external display to the VGA port (1) and a keyboard to any USB port (2) on the Center, or a console to the console serial port (3).

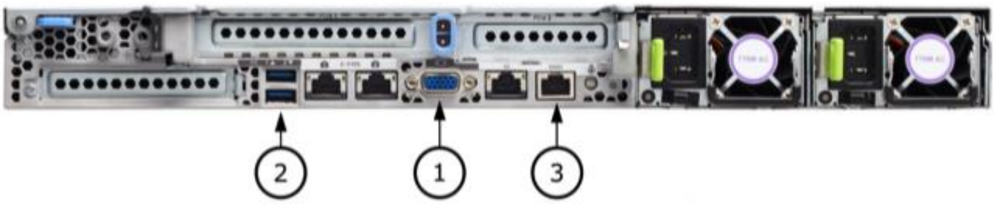


Figure 4-4 – Connecting to a Center Physical Appliance

Connect interfaces

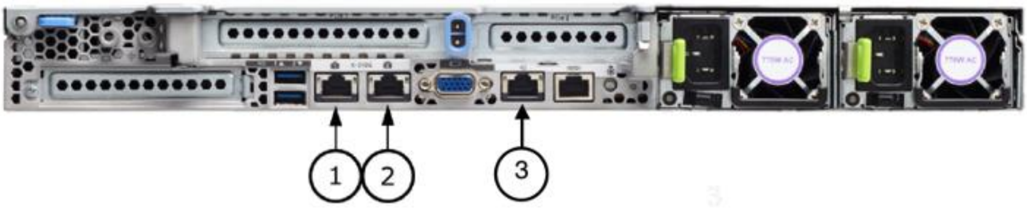


Figure 4-5 – Network and Admin Interfaces

Global Center:

- Connect the eth0 interface to the network (1).

Center with Dual Interface (two separate networks):

Administration interface (eth0): To connect the Center with the user interface or the Global Center, connect the administration network cable to the administration LAN port (1).

- Collection interface (eth1): To connect the Center with its Sensors, connect the collection network cable to the collection LAN port (2).

Center with Single Interface:

- Connect the eth0 interface to the network (1).

Administration and Collection will use the same interface.

NOTE: For CIMC usage, we recommend using the dedicated port for CIMC (3).

Additional Ethernet ports to allow for CenterDPI

- UCSC-MLOM-IRJ45: 4 port GE copper, MLOM card
- UCSC-PCIE-IRJ45: 4 port GE copper, PCIe card
- UCSC-PCIE-ID10GF: 2 port SFP+ card
- UCSC-PCIE-IQ10GF: 4 port SFP+ card

4.2 Center Location

The location of the Center depends on the type of Center used (global or standalone).

4.2.1 Global Center Location

A Global Center provides visibility on all attached centers. The Global Center must be installed in the correct location to ensure its security and availability.

A Global Center provides:

- An asset inventory;
- Visibility for vulnerabilities;
- An overview of activities (no detail on flows);
- Information on presets & events on remote Centers;
- Centralized KDB updates.

The Global Center can be installed in the industrial DMZ, the corporate data center or even in the cloud.

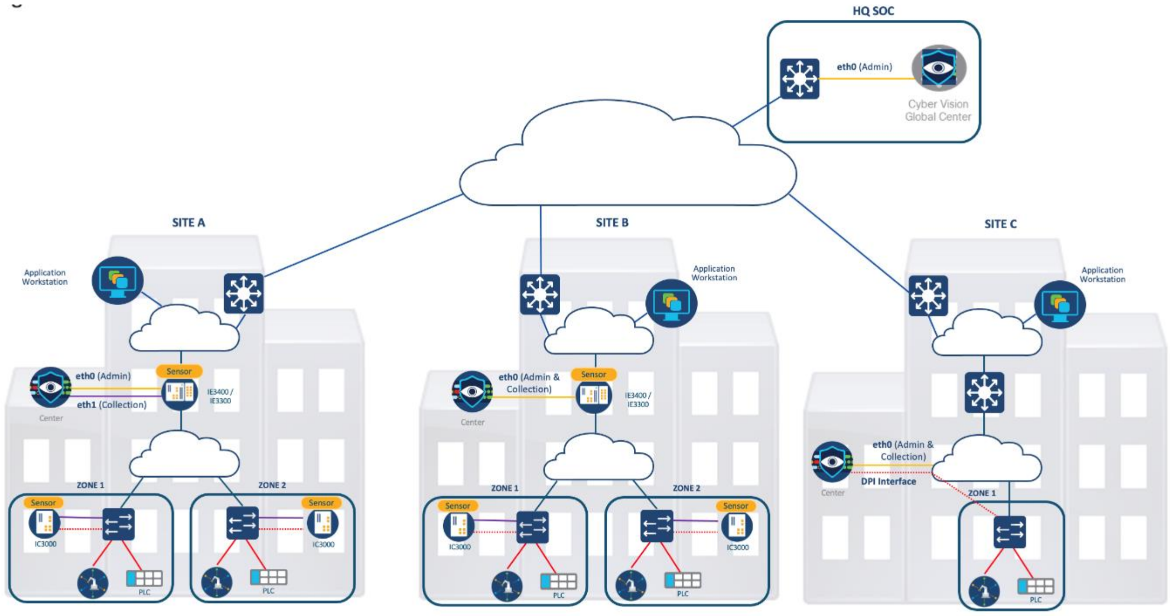


Figure 4-6 – Global Architecture

4.2.2 Standalone Center Location

Standalone Centers collect and process metadata from Sensors and store it on a local database.

Centers can be installed at different locations on the network. If we refer to the Purdue /ISA95 model, it can be installed on:

- Level 4 (Enterprise Zone)
- Level 3.5 (DMZ)
- Level 3 (Manufacturing Zone)
- Level 2 (Local HMI LAN)

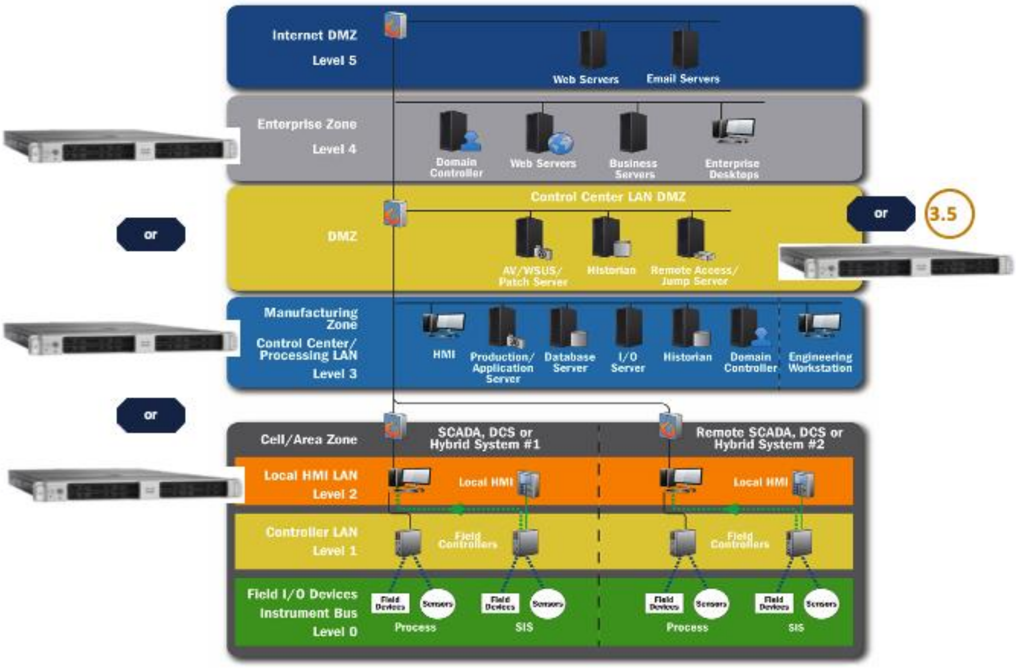


Figure 4-7 – ISA-95 / Purdue Model

4.3 Center Interactions

See chapter 6 “Required UDP and TCP Flows for Cyber Vision” for a comprehensive list of both required and optional communications that will have to be allowed in terms of routes and firewalls to allow the Center to interact and properly work with other components of the solution.

4.3.1 Center DPI

Virtual machines must be configured to ensure that a virtual interface is able to collect data from the network target.

For example, on VMware or Hyper-V, add the promiscuous mode and delete VTP on the switches.

On a physical UCS Center, you can add a dedicated NIC card for the DPI interface. Make sure you have the correct span configuration on the switch side to be able to collect data.

4.3.2 Sensors

Sensors capture traffic from designated networks and send meaningful data to the center. Sensors are enrolled with a Center and both components are in continuous communication.

For the initial communication during installation, the Sensor application should be reachable from the Center's collection interface. The following required and optional ports are involved in this initial communication:

- Required
  - AMPQ/TLS (TCP 5671)
- Optional
  - NTP (UDP 123): Sensor times need to be synced, but the NTP source can be different than the Center (default configuration).
  - SYSLOG (TCP 10514): useful to transfer Sensor log information to the Center.
  - SSH (TCP 22): facilitates Sensor troubleshooting and is required for IC3000 Sensor management through the web interface.

See chapter 6 "Required UDP and TCP Flows for Cyber Vision" for a comprehensive list of the required and optional communications that will need to be allowed in terms of routes and firewalls

4.3.3 License

First-time installations of Cisco Cyber Vision include a 90-day trial. Once the trial expires, a connection to the cloud is required to continue using Cisco Cyber Vision, allowing devices to be counted and billed.

Different licensing options exist depending on the network configuration, network policy and whether a third-party service provider is involved. An online environment can benefit from a direct connection to the cloud, possibly through a proxy, whereas an offline environment requires an additional license reservation. An industrial network with numerous Cisco Cyber Vision Centers to manage may be equipped with a local satellite and use Cisco Smart Software Manager Satellite On-Prem as its licensing service. Likewise, customers dealing with a third-party service provider must use a local On-Prem satellite, but under the Managed Service License Agreement.

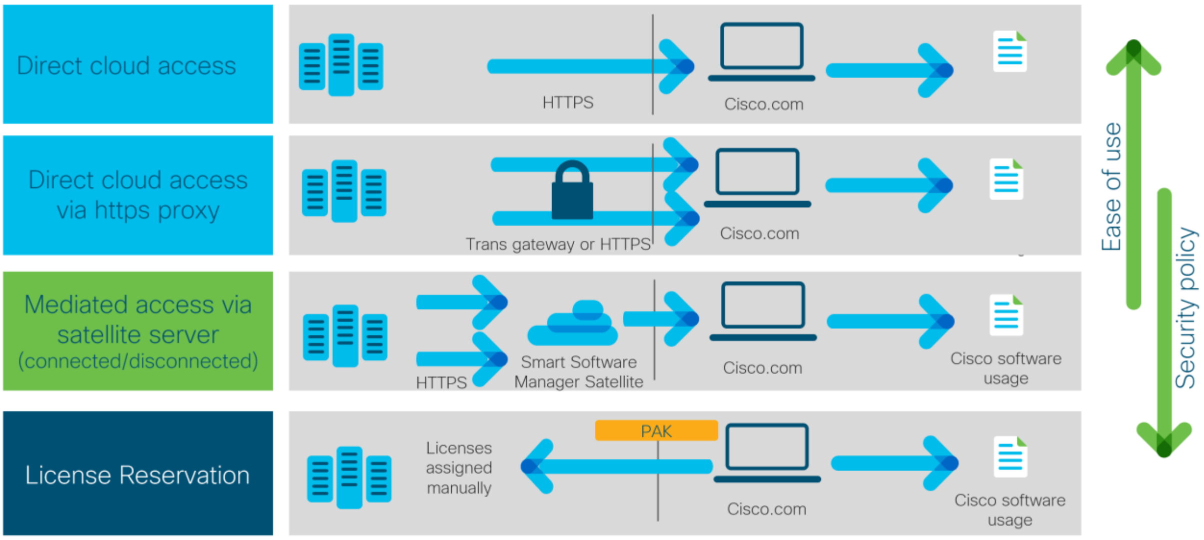


Figure 4-8 – Cyber Vision Licensing Options

Smart Licensing Services:

- Cisco Smart Software Manager (CSSM): licensing service located in the cloud.
- Cisco Smart Software Manager Satellite On-Prem (CSSM On-Prem): a local service, also named satellite, which connects to the cloud for license requests.

Online registration: flexible security policy, ease of use.

A number of Cisco Cyber Vision credits are purchased through a Smart Account and any Center from the package can use these credits. To retrieve a license and ensure credit management, the Cisco Cyber Vision Center sends usage information to the cloud directly over the internet or via an https proxy. No additional solution components are required for this connection mode.

Access: CSSM or CSSM On-Prem.

Offline registration: strong security policy.

As opposed to online registration, the association between credits and Centers is done manually by the user. Getting a license requires the License Reservation feature to be enabled and information to be copied and pasted between Cisco Cyber Vision and cisco.com.

Access: CSSM or CSSM On-Prem.

Managed Service License Agreement:

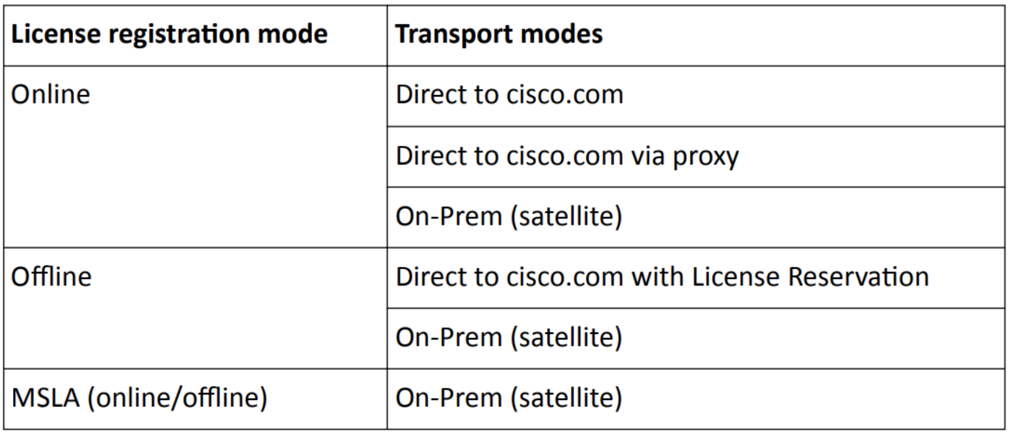
MSLA is a buying program used whenever there is a third-party service provider involved (the environment can be either online or offline). This mode requires the use of Cisco Smart Software Manager Satellite On-Prem, which is an on-site license server that completes the license request with cisco.com. The procedure to retrieve a license is very similar to the online method and is described under the same section.

Access: CSSM On-Prem.

On-Prem registration:

On-Prem registration is also available without MSLA. This can be especially useful in industrial networks with numerous Centers to manage. Each Cisco Cyber Vision Center sends usage information to a locally installed appliance named satellite. Information is sent periodically to cisco.com to keep the satellite in synchronization. This synchronization can occur automatically in connected environments or manually in disconnected environments.

Access: CSSM On-Prem.



License registration mode	Transport modes
Online	Direct to cisco.com
	Direct to cisco.com via proxy
	On-Prem (satellite)
Offline	Direct to cisco.com with License Reservation
	On-Prem (satellite)
MSLA (online/offline)	On-Prem (satellite)

Figure 4-9 – Cyber Vision Licenses

Internet access is required for online mode (can be through proxy). CSSM access is required.

For further details regarding licensing, you can consult this document:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Smart_Licensing_User_Guide_3_2_2.pdf

4.3.4 Active Directory (AD)

Centers can be integrated with an AD server to let non-admin users authenticate with their AD credentials. Users that were created on Cyber Vision remain available.

To use an AD server, you need a connection from the Center:

- AD server IP address
- Service port 389
- User root domain name
- Group names (admin is local, other users should match the existing groups on CCV)

Support for other LDAP servers, other than Active Directory, and other protocols (RADIUS) will be made available in future releases.

4.3.5 Syslog

The center can send events to a syslog server.

To ensure that the syslog server is reachable from the Center, the following information is required:

- IP address of the syslog server
- Protocol used
- Port 514 by default
- Syslog format

A secure mode can be used with a certificate.

4.3.6 NTP

At least one NTP source is needed to maintain synchronization with the Center; the use of several NTP sources is even better. The default configuration is for Sensors to use the Center as their NTP source, with the Sensor clock used to time stamp incoming packets.

The following details are needed for NTP:

- IP address of the NTP server (or FQDN)
- Key if available
- Port UDP 123

4.3.7 DNS

One or more optional DNS servers can be configured to provide third-party server information using names instead of IP addresses. DNS servers can also be used by scripts running on the Center (Python 3 supported).

The following details are required for the DNS server:

- IP address of the DNS server
- Port TCP 53

4.3.8 Cisco Identity Services Engine (ISE)

An integration with Cisco ISE is possible via pxGrid.

The following details are required to integrate the two products:

Cisco ISE

- The IP address for ISE administration
- The IP address of the pxGrid node.
- The FQDN of the pxGrid node.
- An administration account name and password.

Cisco Cyber Vision

- The IP address of the Center.
- The FQDN (Fully qualified Domain Name) of the Center.
- Cisco Cyber Vision administrator access.

Port TCP/8910 needs to be open for SSL communication.

For integration details check the configuration guide.

4.4 Setup and Configuration

4.4.1 Center Setup Considerations

When installing a Center, you should be aware that some information either cannot be modified later or is complicated to modify:

- Hostname
- PKI
- Dual or single interface
- DHCP for sensors
- Keyboard layout

4.4.2 Center Integrations (Scenarios with Different Integrations: LDAP, SIEM, Proxy, NAT etc.)

The following figure shows most integrations and the ports required to make sure the Center is working normally with each one.

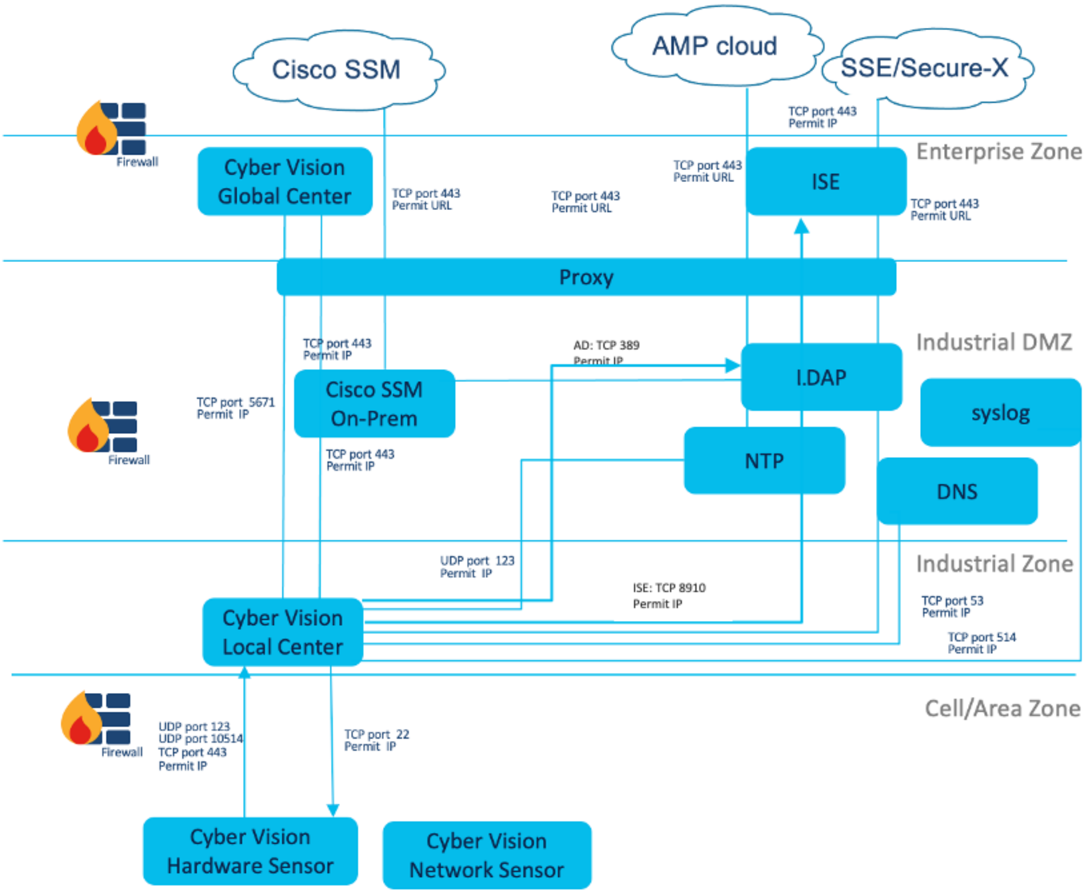


Figure 4-10 – Cyber Vision Interactions Flows

5 Sensors

5.1 Cyber Vision Sensors

Cyber Vision Sensors provide effective information monitoring on an industrial network. The Sensor DPI engine analyzes IT and OT protocols to detect abnormal behaviors and cyberattacks, including malware and advanced persistent threats (APT).

Cyber Vision Sensors are 100% passive (no packet injection on industrial traffic), unless the active discovery feature is activated. Sensors are designed to receive monitoring traffic (SPAN sessions or TAP devices), perform deep packet inspection, extract metadata and provide the Cyber Vision Center with meaningful insights from the plant.

Sensors should be deployed on different levels to improve network visibility.

For example, to extract meaningful information about the industrial plant, Sensors should be deployed as close to the Cell/Zones as possible. A Sensor's DPI, conducted at this level, will provide a complete analysis of industrial communication (ethernet or specific vendor protocol) and a complete packet/frame analysis that excludes any kind of supplementary encapsulation or translation (NAT/PAT).

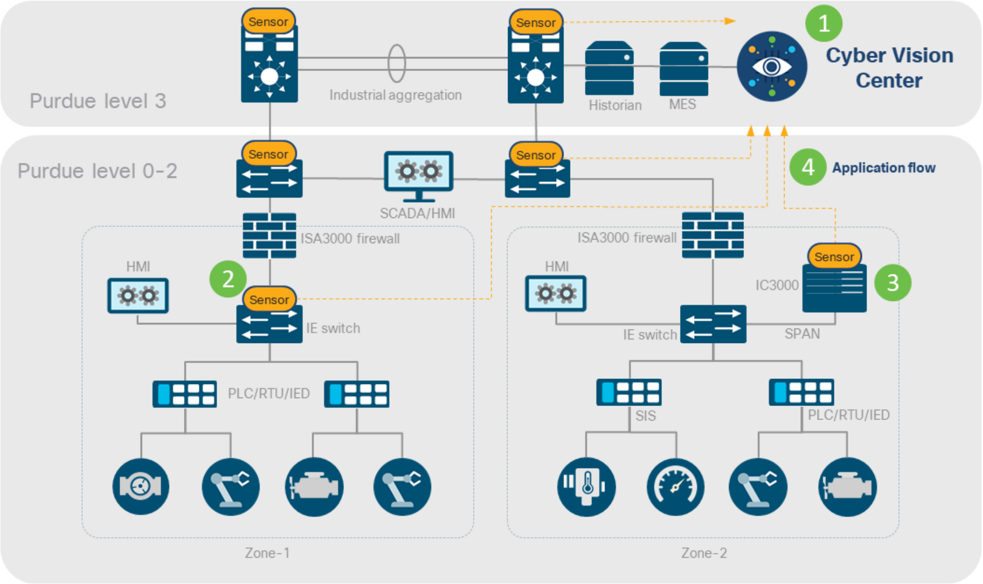


Figure 5-1 – Center-Sensor Interactions

1. Cyber Vision Center deployed on level 3 along with the manufacturing operations servers.
2. Cyber Vision Sensor embedded directly on IE3400 and Catalyst 9300 switches.
3. For brownfield switches, Cyber Vision deployed via one-hop SPAN using IC3000 hardware sensor.

4. Application-flow consists of lightweight metadata that is streamed from Sensors to the Center in-line through the network, eliminating the need for a network-wide SPAN.

5.2 Monitoring Industrial Flows

There are several concepts that should be considered when you begin capturing data from an industrial network, such as MAC address translation performed by routers, Multicast and Broadcast flows, etc. The way in which network devices are represented is determined by the point at which data is captured.

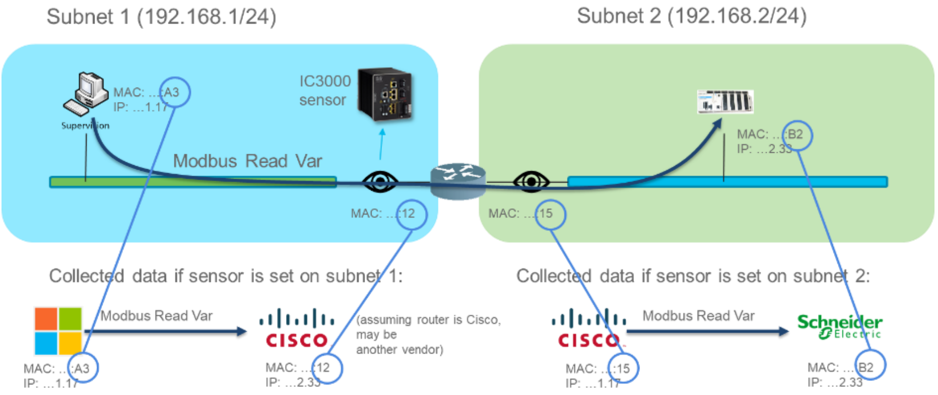


Figure 5-2 – Considerations for L3 Exchanges

In order to clearly identify meaningful process data and asset properties from your environment, such as vendor name or firmware version, Cyber Vision Sensors should be deployed as close to the system under consideration as possible.

Deploying Sensors by subnet or VLAN is highly recommended to avoid monitoring duplicated sources of flows in the environment. In these situations, filters should be configured on each Sensor to ensure it isn't monitoring systems that are already being monitored.

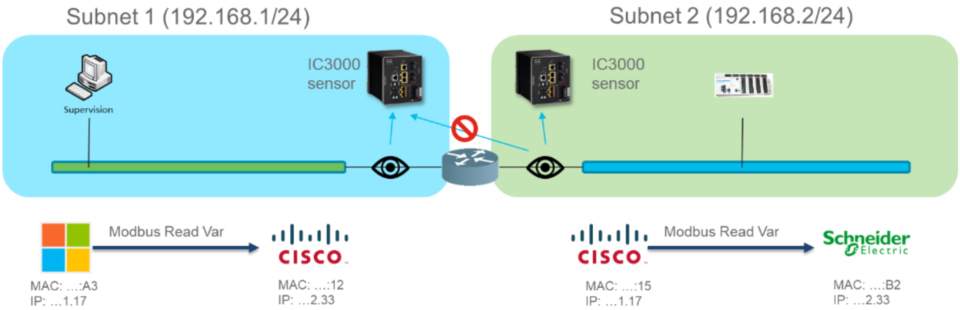


Figure 5-3 – Avoid any Double Monitoring of Subnets

5.2.1 Routers or Level-3 Switches

The Cisco Cyber Vision Sensor IOx container can be installed on routers or L3 switches (performing IP routing/forwarding). These network elements work on a distribution level which usually collects L2 plant flows (Cell/Ring zones) and their connection to the rest of the industrial system (SCADA, industrial applications, third-party applications, etc.).

Another particularity of industrial L3 switches is their support for industrial self-healing ring topologies and redundancy, the tokens of which are identified by the Sensors. Intra-zone monitoring is not required by cybersecurity frameworks or standards. However, flows between different zones should be monitored, especially if they have different security requirements.

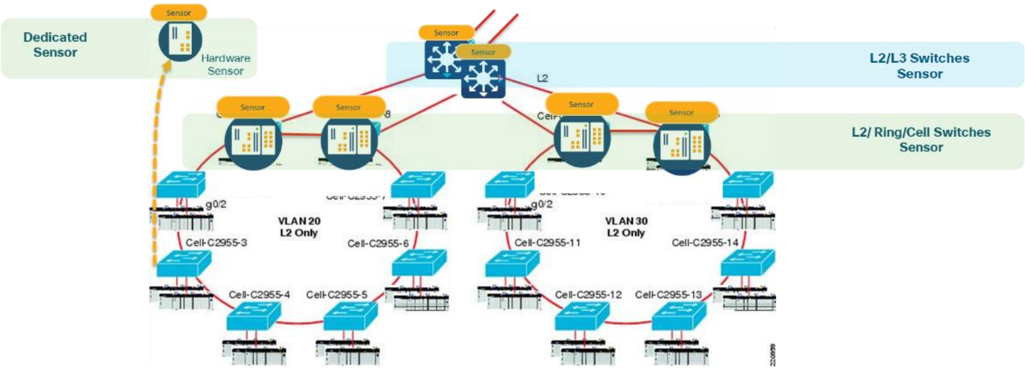
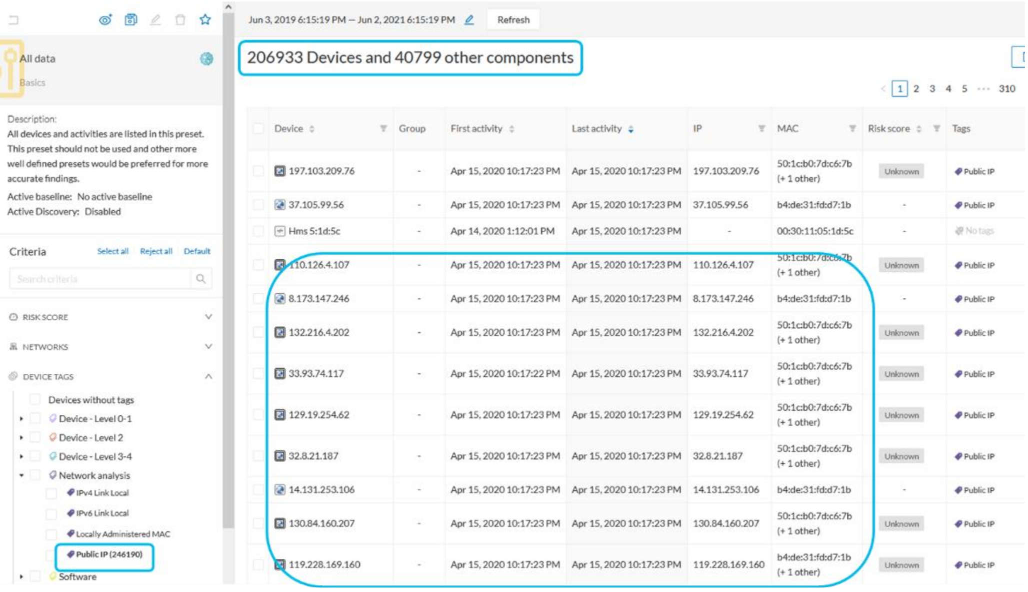


Figure 5-4 – Monitoring Redundant Industrial Architectures

Be careful when collecting data at higher levels (distribution level), especially if Internet traffic is being monitored. Monitoring Internet flows in addition to traffic on the industrial network will significantly increase the number of devices (and components) present in the Center database.

We recommend using distinct Sensors to monitor Cell/Area and industrial zones. Cell/Area zone Sensors should monitor flows between application servers, SCADA and the plant; industrial zone Sensors should control external flows to and from the industrial system.

The figure below shows the consequences of monitoring Internet traffic:



Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline
Active Discovery: Disabled

Jun 3, 2019 6:15:19 PM – Jun 2, 2021 6:15:19 PM

206933 Devices and 40799 other components

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
197.103.209.76	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	197.103.209.76	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
37.105.99.56	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	37.105.99.56	b4:de:31:fd:d7:1b	-	Public IP
Hms 5:1d:5c	-	Apr 14, 2020 1:12:01 PM	Apr 15, 2020 10:17:23 PM	-	00:30:11:05:1d:5c	-	No tags
110.126.4.107	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	110.126.4.107	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
8.173.147.246	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	8.173.147.246	b4:de:31:fd:d7:1b	-	Public IP
132.216.4.202	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	132.216.4.202	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
33.93.74.117	-	Apr 15, 2020 10:17:22 PM	Apr 15, 2020 10:17:23 PM	33.93.74.117	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
129.19.254.62	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	129.19.254.62	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
32.8.21.187	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	32.8.21.187	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
14.131.253.106	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	14.131.253.106	b4:de:31:fd:d7:1b	-	Public IP
130.84.160.207	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	130.84.160.207	50:1c:b0:7d:c6:7b (+ 1 other)	Unknown	Public IP
119.228.169.160	-	Apr 15, 2020 10:17:23 PM	Apr 15, 2020 10:17:23 PM	119.228.169.160	b4:de:31:fd:d7:1b (+ 1 other)	Unknown	Public IP

Figure 5-5 –Don’t Monitor Internet Traffic

Properly defining the points of traffic capture with customers is crucial. Too much data can be overwhelming and keep you from seeing what’s important to monitor; not enough data gives a false feeling of security.

5.2.2 L2 Switches

Cisco Cyber Vision IOx containers can be deployed on L2 switches, which are usually configured as access switches supporting one or several VLANs (broadcast domains). Maintenance stations and other industrial elements (PLC/HMI/IO) are connected through them to access specific environments.

Monitoring sessions on these switches can be configured around the switch’s ports (network interface), VLAN or TRUNK ports. This choice impacts how Sensors will monitor the system.

5.2.3 Dedicated Sensors

Dedicated or hardware Sensors are designed to analyze industrial processes through SPAN or TAP interfaces. These devices can receive SPAN (monitoring) traffic from Cisco elements without IOx features, third-party network elements or TAPs (Test Access Point).

Unlike L2/L3 Switches using Cyber Vision Sensors that are active on the network, dedicated Sensors are 100% passive (unless Active Discovery is activated), receiving only SPAN traffic.

5.3 Location

As described in the previous paragraphs, a Sensor’s location is essential for monitoring the flows between different parts of the industrial environment. Due to their limited behavior, critical systems (OT networks) are predictable (HMIs / PLCs, SCADA / PLCs, engineering station / PLCs and other gateway communication, etc.), unlike communications with the

Internet that can multiply: sensors should be positioned so as to monitor OT devices, not IT LAN.

At which level (Purdue) should sensors be positioned?

- IT-OT communications should be monitored for sure, therefore at least the link or trunk from the OT domain to the router/firewall separating OT from IT should be monitored
- It is also critical to set sensors at Cell/Area level. Deploying network/hardware sensor at a switch where all important PLCs are attached is an ideal choice to monitor the traffic because all the IO devices respond to the poll requests initiated by the controller. Deployment at Cell/Area level is needed to be able to:
  - Identify any rogue device present on the LAN;
  - Detect and/or monitor remote access activity, whether legitimate or rogue;
  - Detect firmware or program changes, to update the inventory and match vulnerabilities.
- Other locations may be useful depending on the network architecture: monitoring of the engineering stations, SCADA/DCS network, wireless access points…

5.4 Interactions

Cyber Vision Sensors are designed to analyze industrial traffic and share data only with their enrolled Center. These exchanges are performed securely through a TLS session controlled by the Center’s internal PKI (Private Key Infrastructure).

Since Cyber Vision 3.2.0 firmware, secure exchanges between Sensors and Center are managed by AMQPoTLS protocol (Advanced Message Queuing Protocol over TLS) through TCP port 5671. Earlier versions used HTTPS (TCP port 443).

Sensors must reach the Center on its specific collection interface when it’s deployed as a dual-interface server.

In addition to monitoring flow (metadata) exchanges between Sensors and the Center (TCP 5671), several other flows are required between these solution components:

- **NTP** – Network Time Protocol (UDP 123): **Must be in UTC**
- **Syslog** (TCP 514): Sensor’s logs pushed to the Center
- **HTTPS** (TCP 443): Allows the Center to reach the switch’s local manager for IOx Cyber Vision application deployments and updates.
- **SSH** (TCP 22): Used only for maintenance window actions.

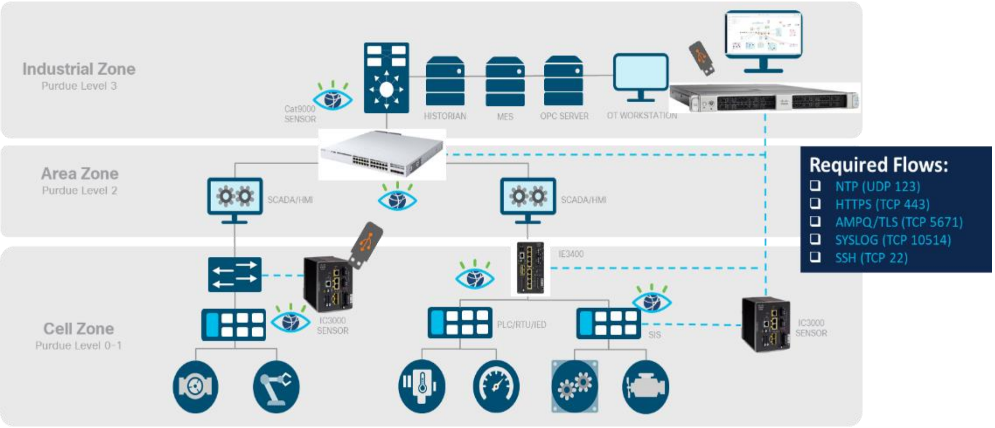


Figure 5-6 – Center ⬄ Sensor Required Flows

When deploying Sensors, all of these interactions should be allowed through firewalls and integrated into the secure architecture design to enable each of these elements.

Details for required flows are given in Chapter 6.

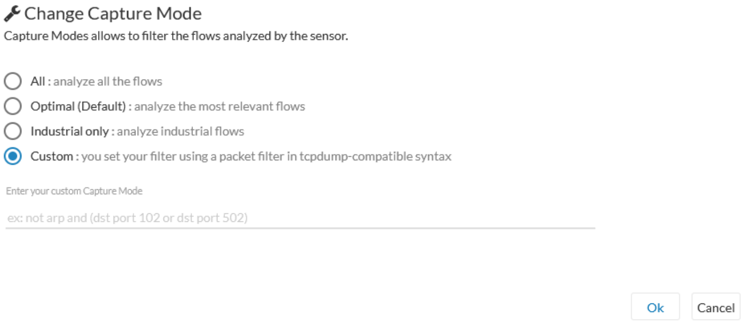
5.4.1 Capture Mode

Capture mode is involved in analyzing all incoming traffic on the Sensor's acquisition ports. When deployed, Sensors catch SPAN (Switched Port Analyzer) traffic and perform a DPI process on it. Metadata on the monitored flows is sent to the Center to provide a graphical representation of the network's elements and activities.

Network captures should be made as close to the zone under consideration as possible to help you to quickly identify events occurring in critical systems.

Industrial systems are heterogeneous. Several industrial protocols and communication modes are used, as well as Broadcast and Multicast exchanges, and Sensors should be configured to manage them.

By default, Sensors have four levels of capture available:



Change Capture Mode

Capture Modes allows to filter the flows analyzed by the sensor.

○ All : analyze all the flows

○ Optimal (Default) : analyze the most relevant flows

○ Industrial only : analyze industrial flows

● Custom : you set your filter using a packet filter in tcpdump-compatible syntax

Enter your custom Capture Mode

ex: not arp and (dst port 102 or dst port 502)

Figure 5-7 – Sensor Capture Modes

All

No filter is applied to the sensor’s DPI; all network flows will be captured and analyzed.

Optimal

Doesn’t analyze IPv4 or IPv6 multicast flows on capture ports.

The following tcpdump filter is configured on the Sensor:

filter: not dst net 224.0.0.0/4 and not ip6 multicast

Industrial Only

This filter could be applied to monitor flows on an “industrial only” area communicating through protocols such as Modbus (TCP 512) or CIP (Common Industrial Protocol – TCP 44818), and other usual protocols, such as OPC-UA (Dynamic ports).

Filter used when applied: port 102 or port 502 or port 44818 or portrange 1089-1091 or port 2085 or port 2404 or portrange 2540-2541 or portrange 2846-2847 or port 3480 or port 4000 or port 4840 or portrange 18245-18246 or port 20000 or port 47808 or portrange 55000-55003 or port 1981 or port 5313 or port 9940 or port 18507 or port 18519 or ether[12:2] & 0xffff == 0x8892 or ether[12:2] & 0xffff == 0x88E3

Custom

Custom filters are generally used to define what kind of flows should be removed from/added to the analysis process. These are required to avoid duplicated monitoring flows or to not monitor legitimated verbose flows.

Examples

In order to monitor a network management server’s activities other than SNMP requests (UDP 161), while still monitoring other hosts performing SNMP through the network:

not (host X.X.X.X and port UDP 161)

To exclude any monitoring of traffic coming from a legitimate host, based on its MAC address (e.g., a PCAP replay station used for tests).

```
not ether host 54:00:12:37:23:16
```

Monitoring can be stopped for any activity to/from an IP. This could be used during maintenance if there is a lot of activity from that device. If necessary, another sensor or dedicated system could be used to monitor that specific activity.

```
not host 192.168.7.200
```

Or, when sensors are present on two LANs with intensive communication between them, the Sensors should be set to exclude traffic from the other LAN to avoid duplicate monitoring.

```
not net 192.168.7/24
```

5.4.2 Network Considerations

Sensors have two types of network interfaces:

- Collection Interface
- Industrial Interface

5.4.2.1 Collection Interface

The Sensor's collection interface must be reachable from the Center's collection interface (eth1, or eth0 if deployed as a single-interface Center). All required management flows should be allowed between these elements.

If Sensors are disconnected from a Center, analyzed flow tables are stored on the Sensor's file system while disconnected. A queuing process running on the platform manages the data to be recovered, eliminating a loss of monitoring data.

A Sensor can directly communicate with its Center whenever they are connected on the same subnet (VLAN or broadcast domain), through a routed network that allows traffic between them or through a network translation (NAT/PAT) architecture. This latter case requires additional attention and should be configured manually.

To ensure each Sensor is connected to the Center, check the following requirements:

- The Center's collection IP address (or Mgt IP address if single-interface)
    - On a dual-interface Center, the Sensor's subnet must be reachable from the collection interface (eth1). On a routed network, a static route must be configured on the Center to comply with this rule.
- Sensor's collection IP address and gateway
- Center & Sensors must be configured in UTC time. (Local Manager time should also be in UTC)
- The following network flows must be allowed between them:
    - NTP (UDP 123)
    - AMQP/TLS (TCP 5671)
    - Rsyslog (TCP 10514)

  - SSH (TCP 22) – for maintenance, only in Hardware Sensors

5.4.2.2 NAT Considerations (important to read for hardware sensors)

Several types of NAT may be used: IP NATing to hide the actual IP addresses for the Center and/or Sensor from each other or port NATing (or PAT) to hide all sensor IP addresses from the Center (all incoming connections will appear to be sourced from the same IP address). In order to permit the connections listed in the next pages, the network administrator will need to account for the NATing in place.

In the case of IP NATing, the Sensor's real IP address—set during enrollment—will differ from the IP address used by the sensor for incoming connections (the local IP address). Centers will not be able to initiate communications with the sensor as the known IP address (defined during enrollment) isn't valid on the LAN. Indeed, this is the whole point in terms of security.

IC3000 configurations made on the web interface are propagated to the Sensor using an SSH connection. If SSH communications are authorized by the network administrators, one of the following methods must be used to make sure the Center is using the correct IP address to connect to the Sensor:

- Manual enrollment with the Sensor's "local" IP address and modification of the enrollment package with the "real" IP address set on the Sensor. Limitation: this process will have to be repeated if the enrollment package is downloaded again or modified packets needs to be stored.
- Manual or Extension-based enrollment with the Sensor's "real" IP address, followed by a replacement of the sensor IP address with the local IP address in the PostgreSQL DB (1 record in table sensor)
  - replace the Sensor's "real" IP address with the "local IP" address. Assuming the local IP is 192.168.0.132 and real IP is 10.10.69.132:

```
root@center:~# sbs db connect
ics => update sensor_info set ip = replace(ip,'real-IP','apparent_IP');
```

  - In this example, the SQL query reads:

```
update sensor_info set ip = replace(ip,'10.10.69.132', '192.168.0.132');
UPDATE N
```

Note: N is the total number of sensors. This message means the change was tested on each sensor, but only the one with the correct 'real IP address' was actually changed.

```
ics=> quit
root@center:~#
```

You can run the "sbs sensor" command to check each Sensor's 'local IP address'.

In any case, any action that can be performed on a hardware Sensor from the Web GUI can also be performed on the Sensor's CLI. As such, SSH is not required to operate Cyber Vision. In many cases, it is even banned for security reasons.

Future Cyber Vision releases will remove the SSH requirement for IC3000 sensors.

Industrial Interface

This capture port receives SPAN traffic, allowing all industrial exchanges to be analyzed and the Cyber Vision DPI process to be performed.

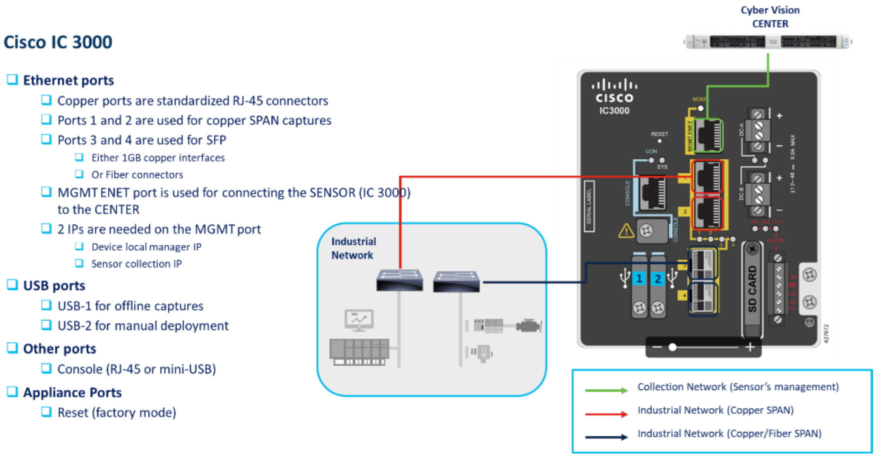
The SPAN traffic could be generated from third-party switches/routers, from Test Access Point (TAP) devices or from Cisco network elements allowed to deploy a Cyber Vision Sensor IOx application.

5.5 Hardware Sensors

Hardware Sensors are physical appliances dedicated solely to monitoring Industrial (OT) Networks. They have no switching or routing functions when used as a Cyber Vision Sensor. They can be used in two different modes: **Online** and **Offline**

5.5.1 Cisco IC3000 Industrial Compute gateway (IC3000)

The Cisco Industrial Compute Gateway IC3000 is used as a Hardware Sensor using a Cyber Vision Sensor IOx application (firmware 1.3.3 or later required).



Cisco IC 3000

- **Ethernet ports**
  - Copper ports are standardized RJ-45 connectors
  - Ports 1 and 2 are used for copper SPAN captures
  - Ports 3 and 4 are used for SFP
    - Either 1GB copper interfaces
    - Or Fiber connectors
  - MGMT ENET port is used for connecting the SENSOR (IC 3000) to the CENTER
  - 2 IPs are needed on the MGMT port
    - Device local manager IP
    - Sensor collection IP
- **USB ports**
  - USB-1 for offline captures
  - USB-2 for manual deployment
- **Other ports**
  - Console (RJ-45 or mini-USB)
- **Appliance Ports**
  - Reset (factory mode)

Figure 5-10 – IC3000

5.5.2 Online Mode

This is the most common way to deploy a Cyber Vision Platform. In this mode, Sensors are directly connected to the Center. Sensors will analyze captured OT traffic and send metadata to the Center's DPI process in real-time.

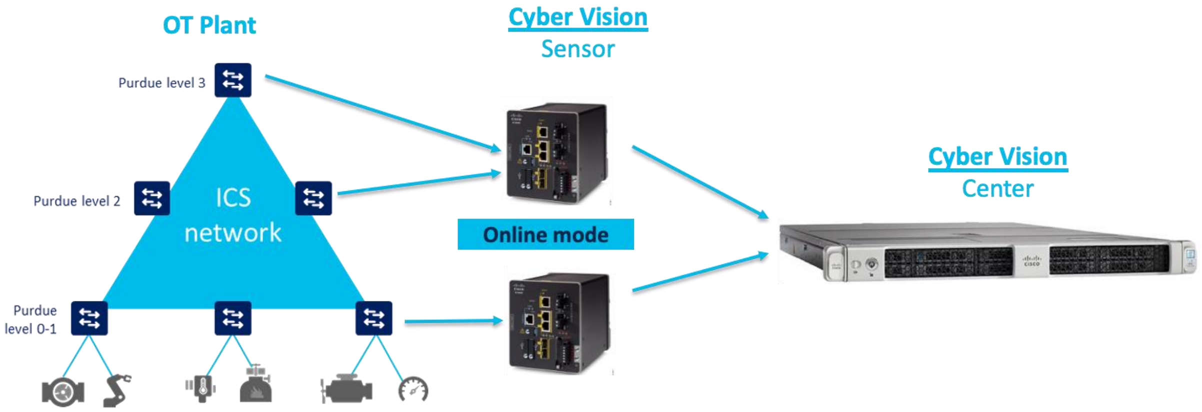


Figure 5-8 – Sensor's Online Mode

Sensors can be configured manually (through Local Manager) or using the Cyber Vision Sensor Management extension (automated deployment). They can be managed from the Cyber Vision admin menu (Sensor or extension sub-menu).

5.5.3 Offline Mode

Hardware Sensors can be used in offline mode to analyze data in isolated environments. Instead of sending metadata to a Center in real-time, hardware Sensors store analyzed data on a USB stick, allowing authorized people to push it to the Center.

Only hardware sensors can work in offline mode.

Sensors must be in factory mode (not enrolled with a Center) to allow the use of USB ports. When a Sensor is enrolled with a Center, its offline port is deactivated.

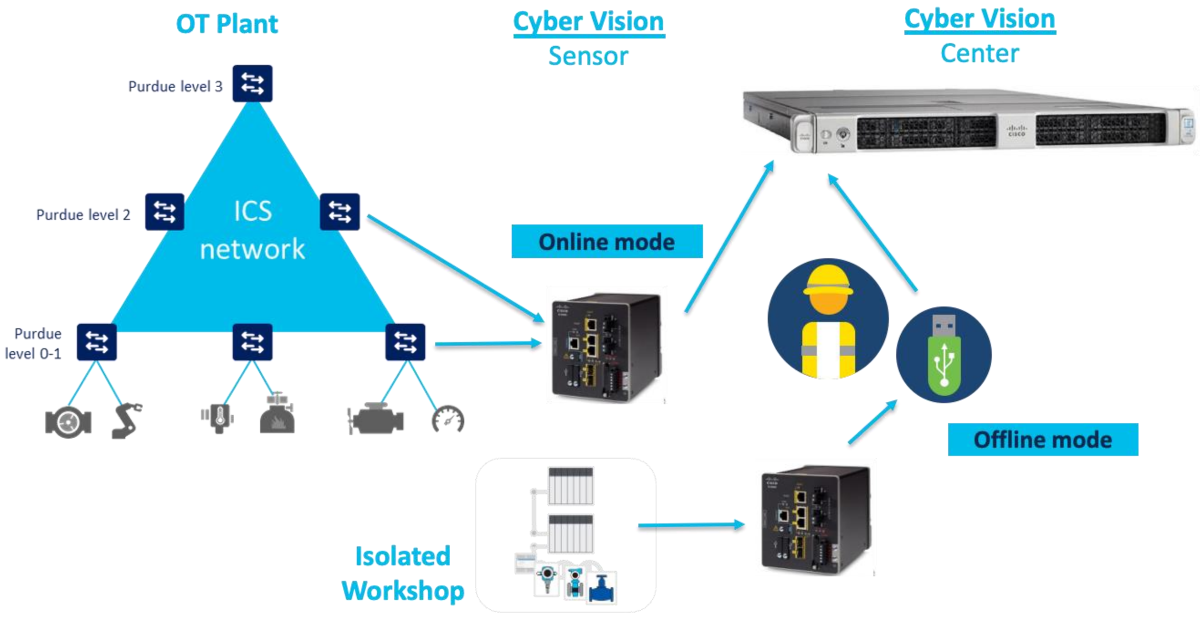


Figure 5-9 – Sensor in Offline Mode

5.6 Network Sensors

The Cyber Vision Network Sensor application can be installed on Cisco's switches and routers managing IOx applications (listed below). It allows the network element to perform both network management and network monitoring actions at the same place.

- Cisco Catalyst Industrial Ethernet 3300 Rugged Switch (IE3300)
  - Note: only the 10G version can run the Cyber Vision app. on iOX
- Cisco Catalyst Industrial Ethernet 3400 Rugged Switch (IE3400)
- Cisco Catalyst 9300 Series Switch (Catalyst 9300)
- Cisco Catalyst 9400 Series Switch (Catalyst 9400)
- Cisco Catalyst IR1101 Rugged Series Router (IR1101)

As an element of the industrial network, network Sensors only work in **online** mode.

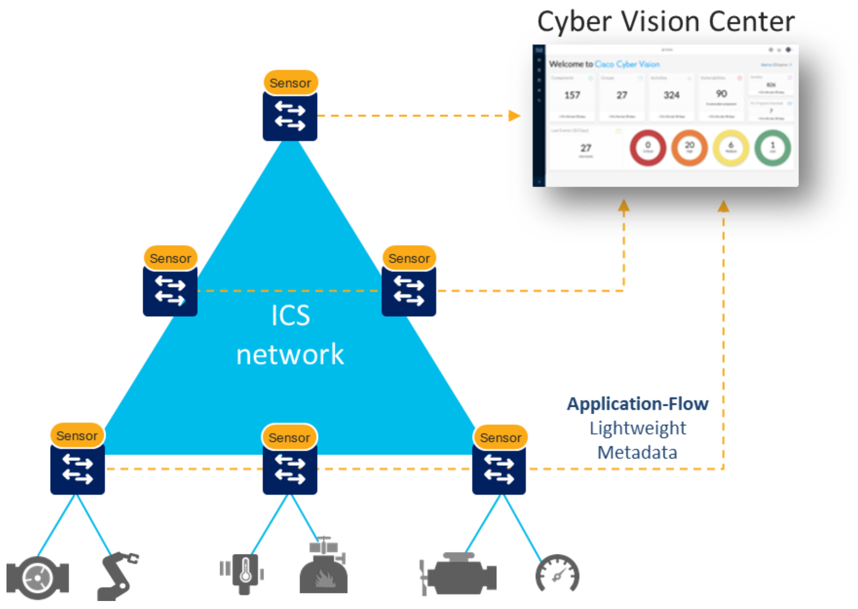
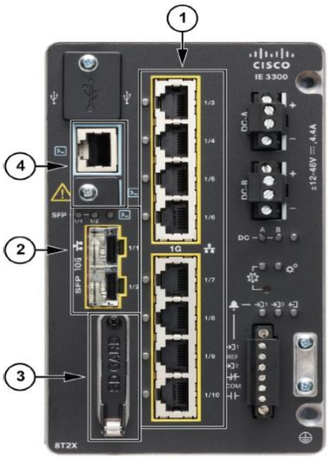


Figure 5-11 – Network Sensors

5.6.1 Cisco Catalyst Industrial Ethernet IE3300/IE3400 Rugged Switches

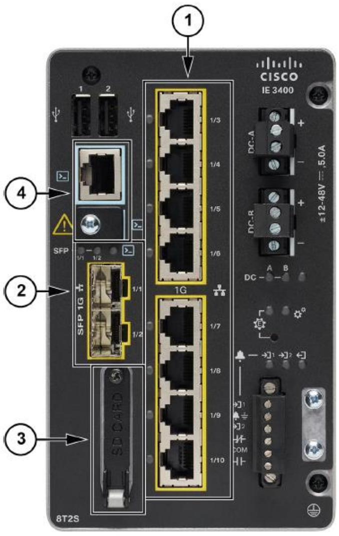
These industrial switches are generally deployed in the Cell/Area zone and are responsible for communication within that zone and exchanges to and from the manufacturing zone.

If used as a distribution switch (aggregating and managing inter-VLAN forwarding), it provides a privileged point for monitoring conduits between those zones.



- 8x RJ45 10/100/1000 BaseT connector **(1)**
- 2x SFP 10G fiber port **(2)**
- SD CARD **(3)**
- Console connectors **(4)** RJ-45 and mini-USB

Figure 5-12 – Cisco Catalyst IE3300 10G Rugged Series Switch



- 8x RJ45 10/100/1000 BaseT connector **(1)**
- 2x SFP 1G fiber port **(2)**
- SD CARD **(3)**
- Console connectors **(4)** RJ-45 and mini-USB

Figure 5-13 – Cisco Catalyst IE3400 Rugged Series Switch

IE3300/IE3400 Requirements

- Cisco IOS XE Version 17.02.01 (minimum)
- 4GB SD Card
- Time configuration on UTC zone
- MTU limitation to 1940 bytes due to monitored session by ERSPAN

The Cyber Vision Sensor IOx application is a separate feature that interacts with the switch's IOS XE software and collects network flows passing through its interfaces. Monitored sessions on the switch will be forwarded by an ERSPAN session to the IOx Sensor industrial interface.

The IOx Cyber Vision Sensor must interact with its Cyber Vision Center. That communication is performed by a collection interface at the IOx Sensor application level and is accessible through the AppGigabitInterface1/1.

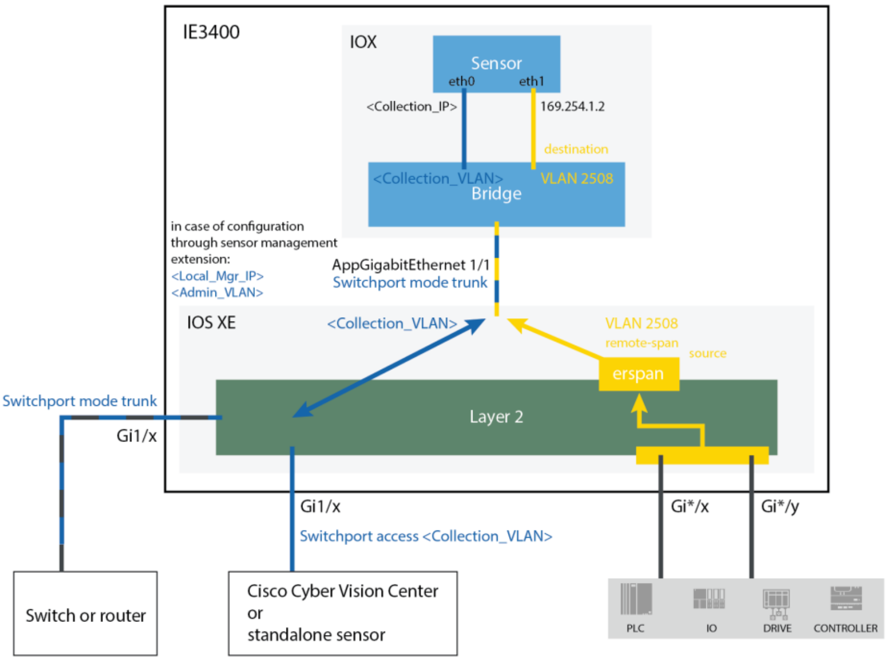
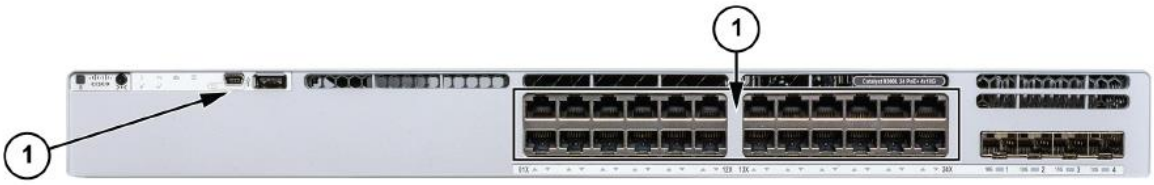


Figure 5-14 – IE3300/IE3400 Sensor Application Architecture

5.6.2 Cisco Catalyst 9300/9400 Series Switches

Cisco Catalyst 9300/9400 switches are often deployed at the manufacturing level as a core architecture, connecting different zones and their respective applications. It also manages communications to/from the enterprise level and, sometimes, even to the Internet.



- x24 RJ45 10/100/1000 BaseT connector **(1)**
- mini-USB console connector **(2)**

Figure 5-15 – Catalyst 9000 Front Panel

Catalyst 9300/9400 Requirements

- Cisco IOS XE Version 17.02.01 (minimum)
- 120 GB SSD Disk
- Time configuration on UTC zone

The Cyber Vision Sensor IOx application works similarly to the IE3300/IE3400 architecture, as shown below:

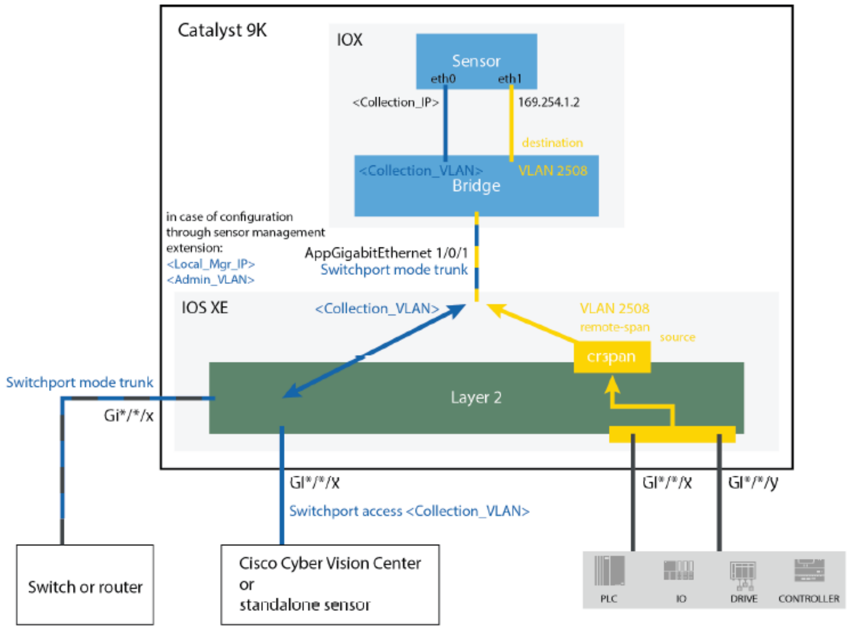
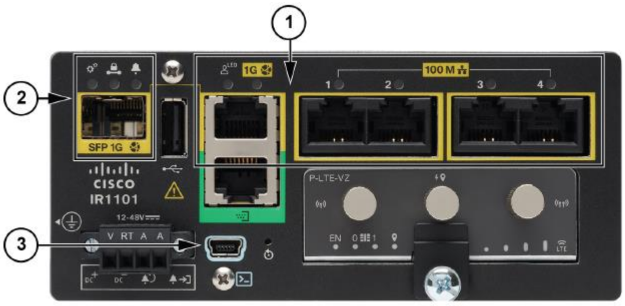


Figure 5-16 – Catalyst 9x00 Sensor Application Architecture

5.6.3 Cisco Catalyst IR1101 Rugged Series Router (IR1101)

The IR1101 is an industrial router that can be used as a Cyber Vision Sensor to monitor an industrial plant.



- 1x RJ45 10/100/1000 BaseT connector (the one on the left) **(1)**
- 4x RJ45 10/100 BaseT connector (the ones on the right) **(1)**
- SFP fiber port **(2)**
- mini-USB console connector **(3)**

Figure 5-17 – Cisco IR1101 Integrated Services Rugged Series Router

Catalyst IR1101 Requirements

- Cisco IOS XE Version 17.02.01 (minimum)
- Time configuration on UTC zone

The Cyber Vision Sensor IOx Application embedded on the router interacts with the IOS XE software through an internal bridge. All traffic passing though the routed interface Gi0/0 can be monitored using ERSPAN.

Virtual port groups must be used to differentiate ERSPAN and Management exchanges.

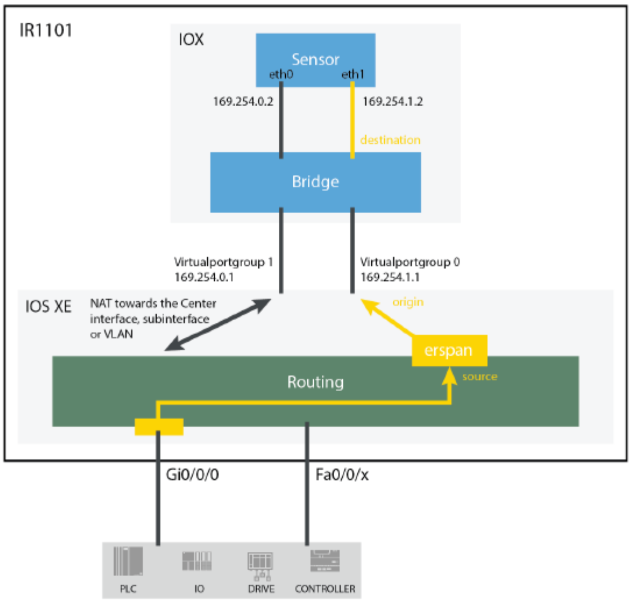


Figure 5-18 – Cisco IR1101 Sensor Application Architecture

IMPORTANT: Only traffic routed to the GigabitEthernet0/0 port can be spanned to the Sensor application.

6 Required UDP and TCP Flows for Cyber Vision

This section lists required and optional communications between Cyber Vision solution components and third parties. Protocols and ports, whether fixed or configurable, are listed in the tables below.

IMPORTANT: this document is valid for Cyber Vision versions 4.0.x. Changes are expected for 4.1 regarding hardware sensors and possibly for Global Centers. Readers must retrieve an updated version of this guide if deploying Cyber Vision version 4.1 or later.

6.1 Identification of Endpoints and Overview

The specific communications required by the Cyber Vision platform differ depending on the project phase and fall under one of three cases:

- Deployment and enrollment phase
  - Differences between manual deployment and deployment using the extension
- Normal operation, including standard maintenance
- Troubleshooting and support

Firewall rules should be restricted during normal operations for better security, and specific rules should be enabled on request for troubleshooting and/or redeployment. Enrollment may also be performed before physical setup on site.

The tables below list the ports and direction for each type of communication between the systems listed in this section.

Because some systems have several interfaces, the table will refer to both the “system” and the interface “sub-system / port”.

The systems with multiple interfaces are: Center, Center with Sync, Global Center, hardware Sensor or IOx sensor. These systems have the following sub-systems / ports:

- Local mgr (local manager) interface – manages the host device:
  - Ethernet port is fixed on hardware sensors (eth0 on IC3000, variable for each model of legacy Sentryo sensors);
  - Can be any port on an IOx sensor, as long as the Local mgr IP address can be reached on that interface;
  - Third port on UCS Center appliances (CIMC – see Center appliance chapter above).
- Collection interface – traffic between Sensor app and Center:
  - Ethernet port is fixed on hardware sensors;
    - Same physical port as Local mgr but has a dedicated IP address for the Cisco Cyber Vision sensor that differs from the Local mgr;

  - IOx sensors: any available port/VLAN can be used, see Cyber Vision switch guide for configuration (trunk configuration from that interface to the IOx application IP);
  - Center: may be the same ethernet port and IP as Admin/access (see below; chosen during Center setup).
- Center Admin/access Admin/access interface - the port and IP used to communicate with web clients (API and GUI) and third-party systems (syslog, LDAP, NTP, etc.):
  - May be the same ethernet port and IP address as Collection (chosen during Center setup).
- Active discovery interface(s) on Sensors – to poll a subnet or list of devices:
  - Any available port(s) can be used, an IP address/VLAN will be set and used as source. Switches must be configured accordingly (see Cyber Vision switch guide);
  - Packets are sent on the LAN only, therefore no specific route/firewall rules are required.
- Capture interface(s) on sensors – to get the raw traffic from the network:
  - Hardware sensors: any port not used for either Admin, Local mgr or Active Discovery;
  - IOx sensors: in addition to monitoring selected ports (SPAN configuration at IOS level), additional ports can be configured to receive RSPAN traffic from other sources, such as switches without IOx.

All other solution components have a single interface:

- Syslog collector: device receiving the syslog messages from Centers. May also act as an API client (splunk app, for instance);
- NTP source: time source for the whole system (Centers act as NTP relay servers);
- DNS server: answering standard DNS requests (UDP 53);
- SNMP server: server accepting SNMP traps (UDP 161);
- LDAP server: currently (4.0), non-admin Cyber Vision users can authenticate on an Active Directory server;
- GUI/API client: device using the center web server for either the GUI or API;
- Admin client: device used for system configuration or troubleshooting, usually also a GUI/API client but in some cases SSH access is restricted to selected clients (jump stations). Can be a laptop, a dedicated admin desktop, or a bastion or jump station.

6.2 Deployment and Enrollment Phase

The followings tables list the required and optional flows to allow (route and firewall rules) during different situations for the initial setup and Sensor / Center enrollment.

6.2.1 Centers

Center installation configurations can either be completed using the setup wizard on the console or a preconfigured VM package. In both cases, finalization of the configuration requires the following accesses.

Source		**Destination**			**Required?**	**Description and Further Information**
System	**Sub-system / port**	**System**	**Sub-system / port**	**Protocol – UDP/TCP - Port (configurable range)**		
Admin client	n/a	Center / Center with sync / Global Center	Admin port	SSH – TCP 22	Optional	Most actions can be performed using the console, but SSH access allows information to be copied and pasted (e.g., SSH key).
Admin client	n/a	Center / Center with sync / Global Center	Admin port	HTTPS – TCP 443	Required	Needed to create the first user, set the license, enroll a Center with sync to a Global Center and configure third-party systems.
Center with sync	Admin/ Access	Global Center	Access	AMPQ – TCP 5671	Required	Used when enrolling a Center with sync with a Global Center.
Center / Center with sync / Global Center	Admin/ Access	Cisco license server or Smart Software Satellite		HTTPS – TCP 443 (direct or proxy)	Optional	License may also be installed offline (copy/paste from Admin client) instead of online using an HTTPS connection.

6.2.2 Sensors – Enrollment Using the Sensor Management Extension

The preferred method, it allows for the installation, enrollment and maintenance of all Cisco sensors[6] (hardware or IOx). If the Sensor app needs to be installed or upgraded, it will be done automatically when upgrading the extension.

The host configuration (Local mgr IP address, password, NTP server) must be completed before deploying the app.

[6] IC3000 sensors require firmware version 1.3.3 or later for enrollment using the extension. If the sensor is running a version older than 1.3.3, we recommend upgrading the firmware before enrolling the sensor, whether using the extension or manually.

Source		**Destination**			**Required?**	**Description and Further Information**
System	**Sub-system / port**	**System**	**Sub-system / port**	**Protocol – UDP/TCP - Port (configurable range)**		
Admin client		Hardware Sensor (Cisco)	Local mgr	HTTPS – TCP 8443 & 8444	Required	Local mgr IP, NTP[7] & password configuration.
Center / Center with sync	Collection or Admin	Sensor	Local mgr	HTTPS – TCP 8443 (IC3000) or 443 (IOx)	Required	Although the default port for enrollment is the collection port, the admin port may be used if the route doesn't exist from Center collection to Sensor Local mgr.
Hardware Sensor / IOx sensor	Collection	Center / Center with sync	Collection	AMPQ – TCP 5671	Required	Successful enrollment is checked by seeing incoming data (Sensor processing status is "green").

[7] The NTP server may be unreachable at this step, but the time must be correct. If necessary, date & time can be set manually to ensure the enrollment works well. This is linked to the certificate's validity date.

6.2.3 Sensors – Manual Enrollment

Manual enrollment requires uploading the Sensor app to the device (if it isn't pre-installed) and making the enrollment package available either on a USB key or by copying the file to the Sensor Local mgr IOx data directory. See the relevant Sensor user manual for more information.

Although enrollment using the extension is preferred, manual enrollment is possible for Hardware Sensors:

- Cisco Hardware Sensors (currently IC3000 Industrial Compute) - shown as Cisco in the table below;
- legacy Sentryo sensors (Sensor3, Sensor5, Sensor7) - shown as Sentryo in the table below.

Source		**Destination**			**Required?**	**Description and Further Information**
System	**Sub-system / port**	**System**	**Sub-system / port**	**Protocol – UDP/TCP - Port (configurable range)**		
Admin client		Hardware Sensor (Cisco)	Local mgr	HTTPS – TCP 8443 & 8444	Required	App installation and configuration (port mapping), Local mgr fixed IP address, NTP & password configuration, enrollment file.[8]
FAT32 USB key		Hardware Sensor (Cisco & Sentryo)	USB port 2	n/a	Optional	Allows a hardware Sensor to be enrolled, including the Local mgr IP address and password.
Hardware Sensor / IOx Sensor	Collection	Center / Center with sync	Collection	AMPQ – TCP 5671	Required	Successful enrollment is checked by seeing incoming data (Sensor processing status is "green").

[8] R/W access to the IOx data directory, where the enrollment file needs to be uploaded, is not possible on IC3000 units running firmware version 1.3.2. This was fixed in version 1.3.3. One workaround for 1.3.2 is to set a temporary IP on the sensor app and use scp to copy the enrollment file to the same directory, since it is shared between the Host and App.

6.3 Normal Operation, Including Regular Maintenance

Source		Destination			Required?	Description and Further Information
System	Sub-system / port	System	Sub-system / port	Protocol – UDP/TCP - Port (configurable range)		
Hardware Sensor / IOx Sensor	Collection	Center / Center with sync	Collection	AMPQ – TCP 5671	Required	Sending metadata to Center (DPI results) and accepting instructions.
Hardware Sensor / IOx Sensor	Collection	Center / Center with sync	Collection	Secure syslog – TCP 10514	Optional	If not allowed, Center “diag” files will not include sensor logs.
Hardware Sensor / IOx Sensor	Collection	SNMP server		SNMP - UDP 161	Optional	Device CPU/RAM load information sent to server.
Hardware Sensor	Collection	Center / Center with sync or NTP source	Collection	NTP – UDP 123	Required	Enrollment default is for the Sensor app to get the time from the Center but this can be changed to a local source.
Hardware Sensor / IOx Sensor	Local mgr	Center / Center with sync or NTP source	Collection	NTP – UDP 123	Required	Same as above, regarding choice of source. Source to be configured using the Host local manager[9] web interface.
<raw RSPAN traffic>		IOx Sensor / Hardware Sensor / Center / Center with sync	Collection (Additional configuration required on IOx Sensors)	RAW traffic over RSPAN: specific VLAN	Required if RSPAN is used	IOx Sensors & Centers can be used with RSPAN traffic: switches on the route must be enabled to forward RSPAN traffic on a dedicated VLAN (<256).
Center / Center with sync	Collection	Hardware Sensor	Collection	SSH – TCP 22 (Cyber Vision version 4.0[10])	Optional	Required for capture mode changes, Snort updates, recording requests and App version update.

[9] This may seem redundant for hardware Sensors, since time is synced with the app. But, at reboot, the app first gets its time from the Host until it syncs with the NTP source. As such, the Host time needs to be correct as well.

[10] Version 4.1 will update the hardware Sensor configuration to use the AMPQ connection to get configuration changes, in line with IOx sensors.

Source		**Destination**			**Required?**	**Description and Further Information**
System	**Sub-system / port**	**System**	**Sub-system / port**	**Protocol – UDP/TCP - Port (configurable range)**		
Admin client		Hardware Sensor	Collection	SSH – TCP 22 (Cyber Vision version 4.0.x)	Optional	Alternate option if SSH isn't enabled from the Center. Actions will need to performed using CLI instead of the GUI.
API/GUI client		Center / Center with sync / Global Center	Admin/ Access	HTTPS – TCP 443	Optional	Standard web (GUI or API) access to the Center's interface.
Center with sync	Collection	Global Center	Access	AMPQ – TCP 5671	Required	Syncing data from Centers to a Global Center and getting Knowledge Base updates
Center / Center with sync / Global Center	Admin/Access	NTP source		NTP – UDP 123	Required	Note that Global Centers can't be used as an NTP source for Centers (version 4.0).
Center / Center with sync / Global Center	Admin/Access	DNS server(s)		DNS – UDP 53	Optional	Required if third-party systems are configured by name rather than IP address.
Center / Center with sync / Global Center	Admin/Access	AD server		LDAP – TCP 389 (configurable)	Optional	Required if non-admin users are managed by an Active Directory.
Center / Center with sync / Global Center	Admin/Access	Cisco license server or Smart Software Satellite		HTTPS – TCP 443 (direct or proxy)	Optional	Licenses can also be validated offline instead of using an HTTPS connection.
Center / Center with sync / Global Center	Admin/Access	Syslog collector		Syslog – UDP/TCP/TLS 514 (1024-65535)	Optional	Required if data must be sent to a SIEM or to comply with a centralized log collection requirement.

Source		Destination			Required?	Description and Further Information
System	Sub-system / port	System	Sub-system / port	Protocol – UDP/TCP - Port (configurable range)		
Center / Center with sync / Global Center	Admin/Access	SNMP server		SNMP - UDP 161	Optional	Device CPU and RAM load information sent to server.

6.4 Troubleshooting and Support

Troubleshooting and support need to be possible when the GUI (web server) is down. Most actions are performed on the CLI (SSH or console access).

Many troubleshooting activities require a connection to the Center or Sensor over SSH. This access doesn’t always have to be available. Most often, access is granted for a limited time, possibly with strong authentication through a bastion or jump station.

The source of the connection, shown as “Admin client” in the table below, will most often be the bastion or a jump station system.

Source		Destination		Protocol	Required?	Description and further information
System	Sub-system / port	System	Sub-system / port	UDP/TCP - Port (custom range)		
Admin client		Hardware Sensor	Local mgr	SSH – TCP 22	Required	On an IC3000 Sensor app, the console can be accessed through the Sensor Host SSH server.
Admin client		Center / Center with sync / Global Center	Admin/Access or Collection	SSH – TCP 22	Required	SSH for CLI, as well as file transfers that may be required using SCP: diag files, dumps, software updates.
Admin client		(all Cyber Vision components)		ICMP (ping)	Optional	To test routes (all Cyber Vision components answer ping requests).
Admin client		Hardware Sensor	Local mgr	HTTPS – TCP 8444 & 8443	Required	Allows checking and fixing device config.
Admin client		IOx Sensor	Local mgr	HTTPS – TCP 443	Required	Allows checking and fixing device config.

Source		**Destination**		**Protocol**	**Required?**	**Description and further information**
System	**Sub-system / port**	**System**	**Sub-system / port**	**UDP/TCP - Port (custom range)**		
Center / Center with sync / Global Center	Admin/ access	Admin client		Syslog – UDP 514	Optional	Allows configuration of syslog destination on Centers and checking incoming messages.
Admin client		Hardware Sensor / IOx Sensor	Capture	<RAW packets>	Optional	Allows testing interface/low level DPI. This is often not possible unless a direct cable connection is possible or RSPAN is setup.

6.5 Third-Party Systems

The following third-party systems can interact with Cyber Vision Centers during normal operation. This schematic, taken from the Industrial Security Design Guide[11], summarizes possible integrations, typical topologies and ports to open:

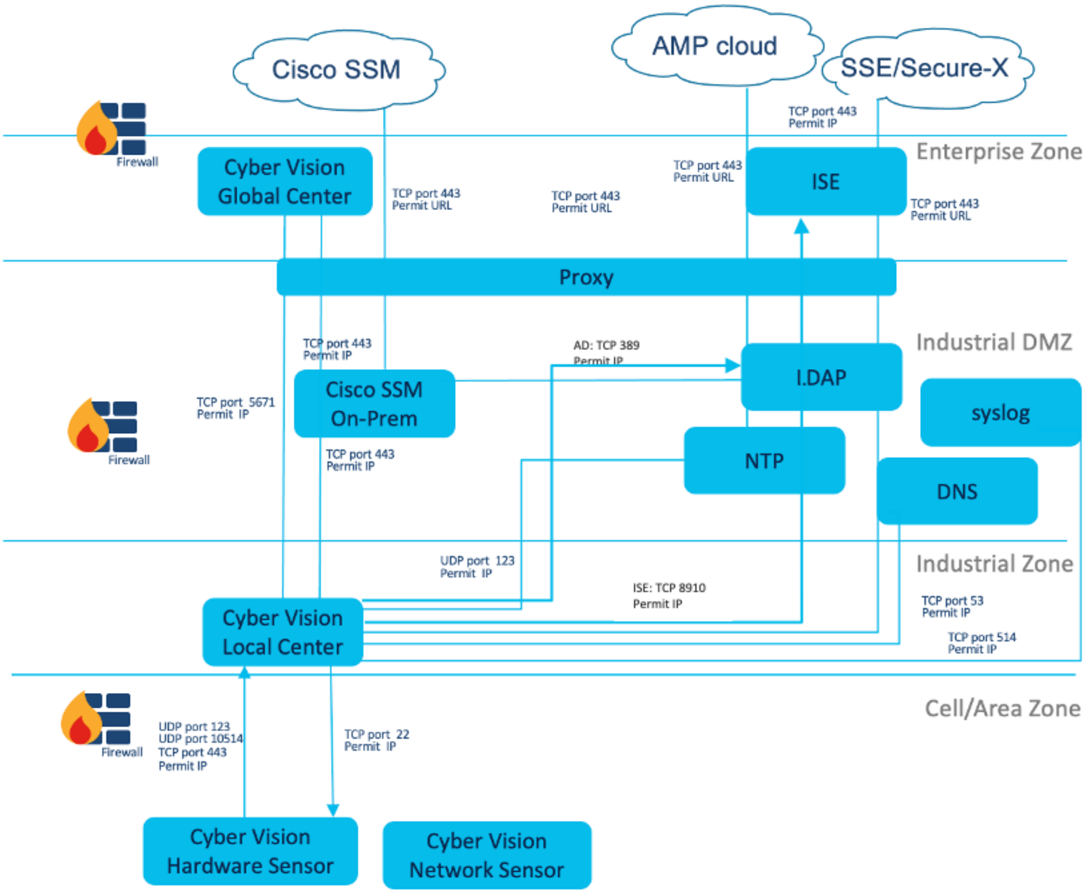


Figure 6-1 – Cyber Vision Interactions Flows

[11] https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.pdf

7 Performances & Limitations

7.1 Center Scale

The performance of Cisco Cyber Vision is validated for a given version and defined hardware. Cyber Vision 4.0.x is approved for two different hardware appliances:

	Specifications	
Item	CV-CNTR-M5S3	CV-CNTR-M5S5
Form factor	1RU Cisco UCS C220 M5 Rack Server	1RU Cisco UCS C220 M5 Rack Server
Processors	Intel Xeon 2.4 GHz with 10 cores	Intel Xeon 2.3 GHz with 16 cores
Memory	Two 16GB DDR4 2933MHz RDIMM	Four 16GB DDR4 2933 MHz RDIMM
RAID	Cisco 12G Modular RAID controller with 2GB cache RAID-1 and RAID-10 options	Cisco 12G Modular RAID controller with 2GB cache RAID-1 and RAID-10 options
Internal storage	Two or Four 480GB 2.5in enterprise performance 6G SAS SSD (3x endurance)	Two or Four 800GB 2.5in enterprise performance 12G SAS SSD (3x endurance)
Embedded network interface cards (NICs)	Dual 10GBASE-T Intel x550 Ethernet ports	Dual 10GBASE-T Intel x550 Ethernet ports
Power supplies	Redundant Cisco UCS 1050W AC Power Supply for Rack Server	Redundant Cisco UCS 1050W AC Power Supply for Rack Server

Performance using this reference hardware:

	Specifications	
Number	CV-CNTR-M5S5	CV-CNTR-M5S3
Max number of discovered components and devices	50,000	25,000
Max number of flows stored	8,000,000	4,000,000
Max number of sensors managed	150	75

If the Center is deployed as a virtual machine:

- the performance data given above will be valid if the Center is deployed on a hypervisor running on hardware similar to what has been validated (CPU, RAM SSD and IOP characteristics),
- the hypervisor always needs to give the Cyber Vision appliance the resources it requires. The Cyber Vision center needs to have enough processor, memory and disk capacities to run efficiently. Some latencies may impact the center performance and result in performance outage or service interruptions.

For AWS centers, the recommended sizes are:

- For 10,000 components w/o Center DPI:
  - CPU: Intel Xeon, 10 cores
  - RAM: 32GB minimum
  - Storage: 1TB SSD minimum, RAID-10
- For more than 10,000 components or Center DPI:
  - CPU: Intel Xeon, 16 cores
  - RAM: 64GB minimum
  - Storage: 1TB SSD minimum, RAID-10

Performance specifications of all Cyber Vision centers (Virtual or AWS) are limited to what is explained above (case of CV-CNTR-M5S5).

7.2 Center Performance: Disk Usage, RAM, IOP, CPU

Running a Center with a large database could place significant load on the use of several resources. Sufficient resources must be dedicated to the Center, especially in a virtual environment.

For example, a Center with more than 25,000 devices and components or with its DPI interface activated requires the following resources:

- CPU: 16 cores x 2.3Ghz available
- RAM: 64GB available
- Disk: 1 TB available, SSD mandatory
- IOPS: 225K random write IOPS

7.3 Sensor Performance

Sensor performance depends on the hardware used. The following table shows the maximum packets per second supported on a standard mix of protocols seen in industrial networks.

Platform	Max packets per second	Max number of flows
IC3000	12,000	15,000
IE3300/IE3400	9,600	12,000
IR1101	13,200	16,500
Catalyst 9300	30,000	21,000
Center DPI	300,000	Match Center

Remark:

- 12,000 pps @ average packet size of 750 bytes ~ 70 Mbps
- 12,000 pps @ average packet size of 1500 bytes ~ 140 Mbps

If maximum number of packets is regularly exceeded, Sensor will drop packets and may lead to unexpected behavior.

7.4 Network Bandwidth Used

7.4.1 Collection Network

The bandwidth required to link a Sensor and its Center is largely the product of the traffic on the OT network monitored by the Sensor. Incoming bandwidth and the types of protocols used have a significant impact on the size of the DPI results. These directly affect the bandwidth required between the Sensor and Center. As a result, figures could change dramatically depending on the application. In 4.0.0, the following figures have been observed:

- Standard bandwidth is less than 0.5% of the incoming traffic;
- Some applications show a bandwidth use between 1 and 5 % in average of the incoming traffic;
- A minimum of 4kpbs is observed in 4.0.0.

Sensors will store data locally when the Center is unreachable. When communications recover, the Sensor will try to send all of the flow tables it has stored locally as soon as possible. Without policies to prevent it, the Sensor could overwhelm the link during this transmission.

7.4.2 Center to Global Center

Synchronization between a Center and its Global Center isn't necessarily impacted by incoming traffic from the Sensor. Instead, synchronization between the Center and Global Center is more heavily dependent on the number of devices, components and activities.

Standard bandwidth between a Center and Global Center is less than the bandwidth of all incoming Sensors. In 4.0.0, observations have been similar to those for collection:

- Standard bandwidth is less than 0.5% of the incoming traffic;
- Some applications show a bandwidth use between 1 and 5 % in average of the incoming traffic;
- A minimum of 4kbps/s is observed in 4.0.0.

Centers will continue to load data on their own when the Global Center is unreachable. When communications recover, Centers will try to send the missing data to their Global Center as soon as possible. Without policies to prevent network overloads, Centers could overwhelm their link to the Global Center during this transmission.

(blank page)