CHAPTER 1

CPwE Network Security Overview

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

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

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

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

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

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

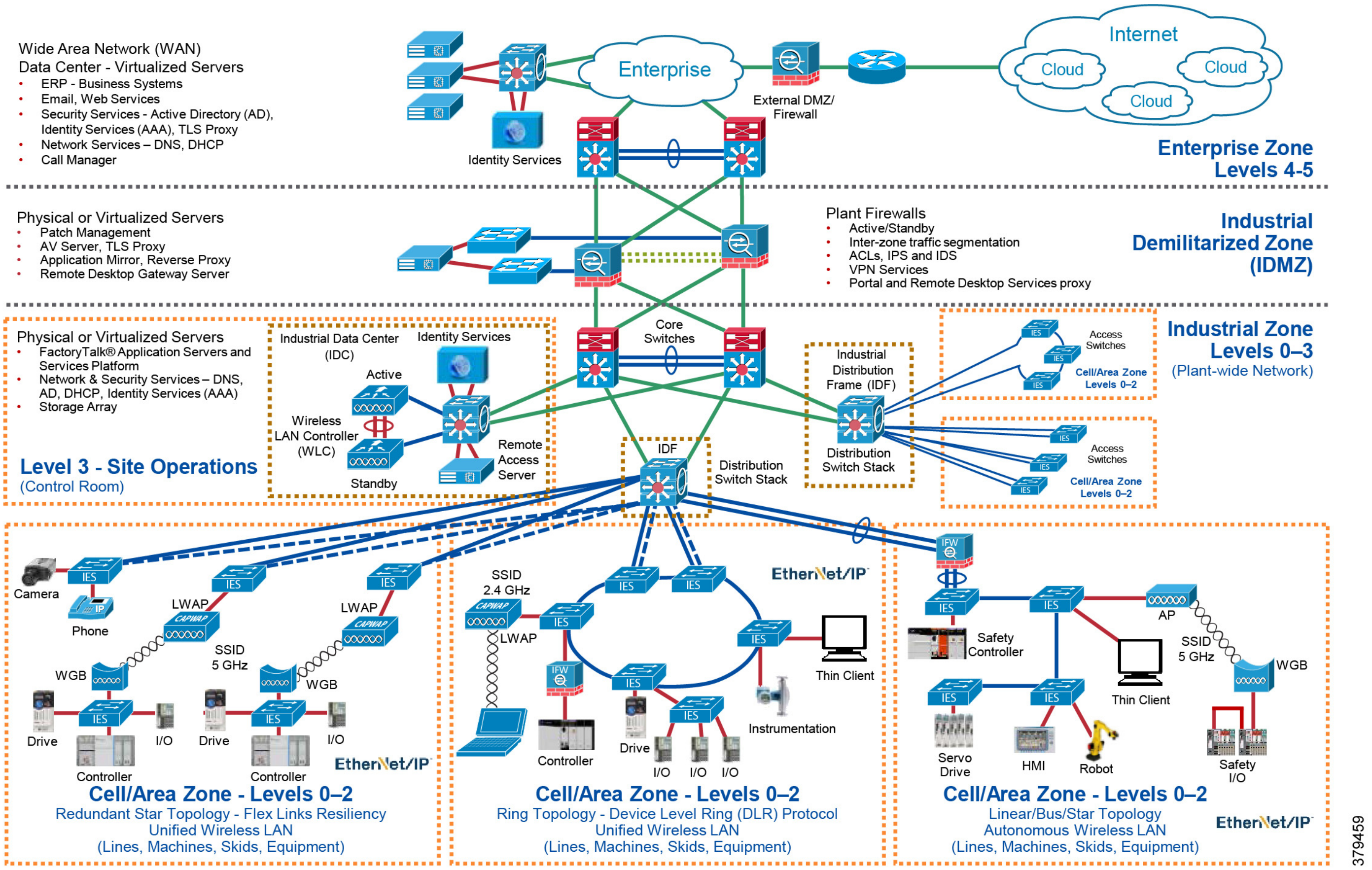
Note Cisco and Rockwell Automation recommend that the OT-IT security team be composed of a multi-discipline team of operations, engineering, safety, maintenance, and IT representatives to develop an industrial security access policy based on your risk tolerance and risk management.

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

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

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

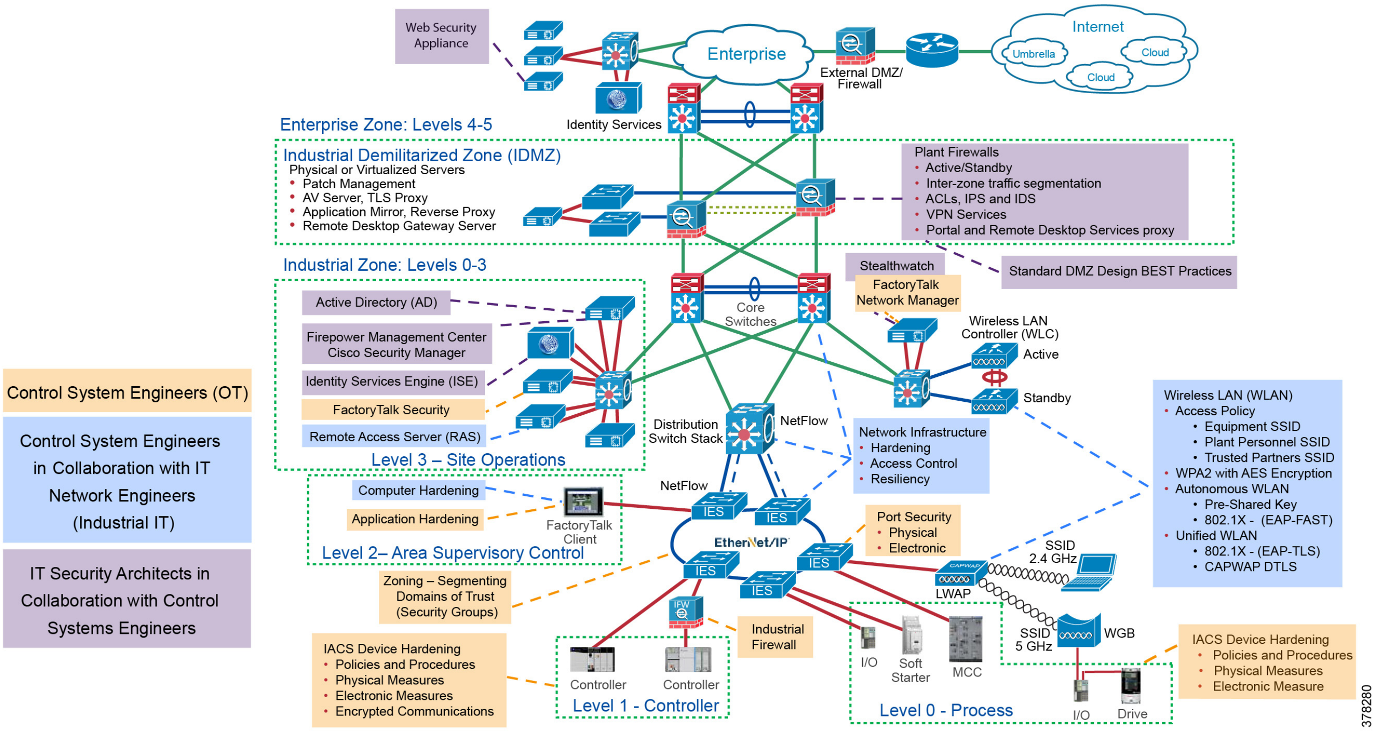
Figure 1-1 CPwE Architecture


Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• Storage Array
Industrial Data Center (IDC)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Level 3 - Site Operations
(Control Room)
Core Switches
Industrial Distribution Frame (IDF)
Distribution Switch Stack
IDF
Distribution Switch Stack
Access Switches
IES
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
Camera
Phone
IP
LWAP
CAPWAP
SSID 5 GHz
WGB
LWAP
WGB
Drive
I/O
Drive
I/O
Controller
Controller
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
SSID 2.4 GHz
LWAP
EtherNet/IP
IFW
Thin Client
Controller
Drive
Instrumentation
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
IFW
Safety Controller
AP
SSID 5 GHz
WGB
Thin Client
Servo Drive
HMI
Robot
Safety I/O
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
379459

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

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

Figure 1-2 CPwE Industrial Security Framework



CPwE Security Overview

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

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

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

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

CPwE Network Security Solution Use Cases

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

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

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

Visibility

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

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

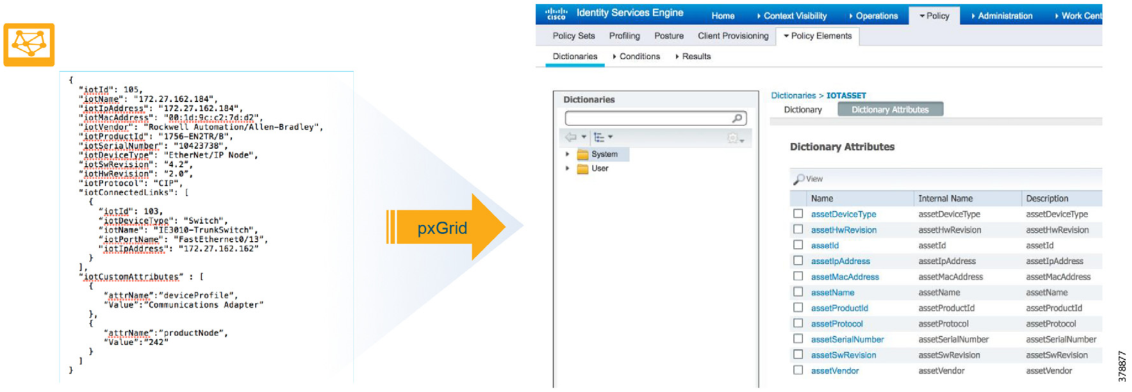
To gain visibility of assets in the enterprise networks, IT has used Cisco Identity Service Engine (ISE) with Cisco ISE Profiling Services (explained below). Cisco ISE is a security administration product that enables an OT-IT security administrative team to create and enforce access level security policies.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

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

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

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

Figure 1-3 NMT Exporting Attributes to ISE



```
{
  "iotId": 105,
  "iotName": "172.27.162.184",
  "iotIpAddress": "172.27.162.184",
  "iotMacAddress": "00:1d:9c:c2:7d:d2",
  "iotVendor": "Rockwell Automation/Allen-Bradley",
  "iotProductId": "1756-EN2TR/B",
  "iotSerialNumber": "10423738",
  "iotDeviceType": "EtherNet/IP Node",
  "iotSwRevision": "4.2",
  "iotHwRevision": "2.0",
  "iotProtocol": "CIP",
  "iotConnectedLinks": [
    {
      "iotId": 103,
      "iotDeviceType": "Switch",
      "iotName": "IE3010-TrunkSwitch",
      "iotPortName": "FastEthernet0/13",
      "iotIpAddress": "172.27.162.162"
    }
  ],
  "iotCustomAttributes" : [
    {
       "attrName":"deviceProfile",
       "Value":"Communications Adapter"
    },
    {
       "attrName":"productNode",
       "Value":"242"
    }
  ]
}
```

Dictionary Attributes

	Name	Internal Name	Description
□	assetDeviceType	assetDeviceType	assetDeviceType
□	assetHwRevision	assetHwRevision	assetHwRevision
□	assetId	assetId	assetId
□	assetIpAddress	assetIpAddress	assetIpAddress
□	assetMacAddress	assetMacAddress	assetMacAddress
□	assetName	assetName	assetName
□	assetProductId	assetProductId	assetProductId
□	assetProtocol	assetProtocol	assetProtocol
□	assetSerialNumber	assetSerialNumber	assetSerialNumber
□	assetSwRevision	assetSwRevision	assetSwRevision
□	assetVendor	assetVendor	assetVendor

The integration between NMT and ISE provides the following benefits:

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

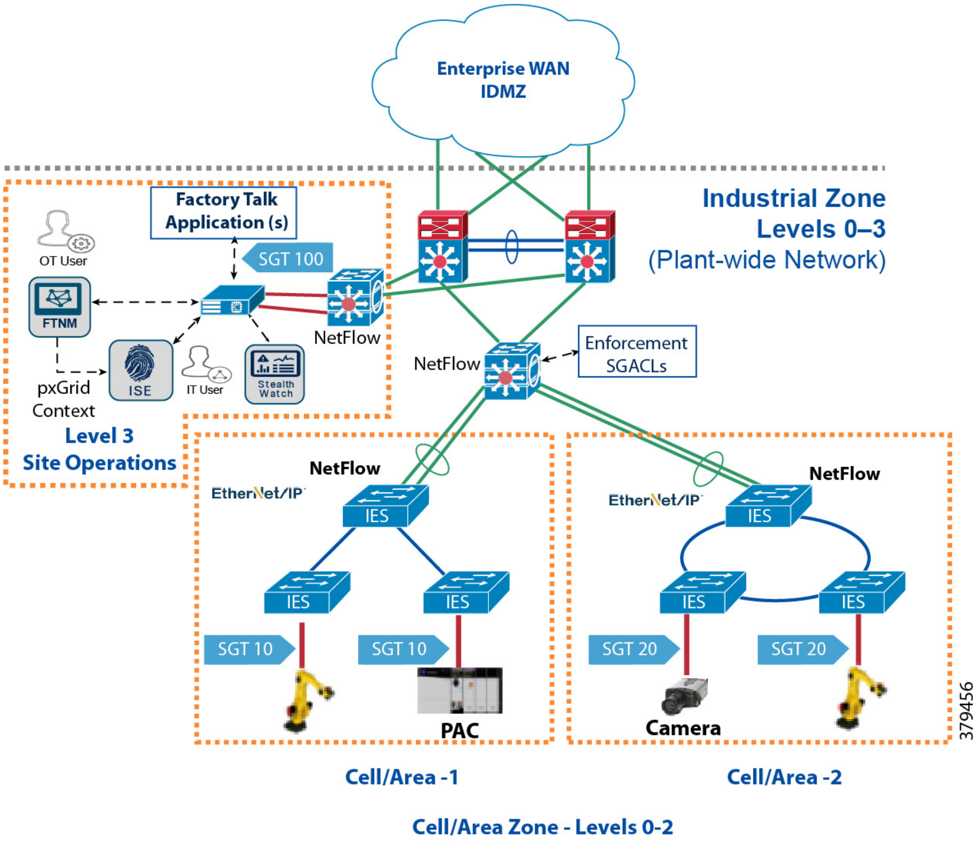
Segmentation

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

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

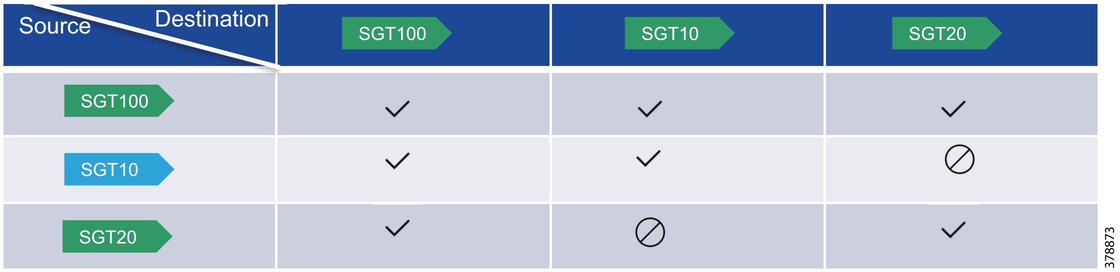
To provide more flexibility and simplicity to network segmentation, CPwE Network Security uses Cisco TrustSec technology to define access policies using security groups. This allows the segmentation of IACS assets using Security Group Tags (SGT) which group the assets regardless of their location in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

Figure 1-4 Secure Group Assignment



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

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



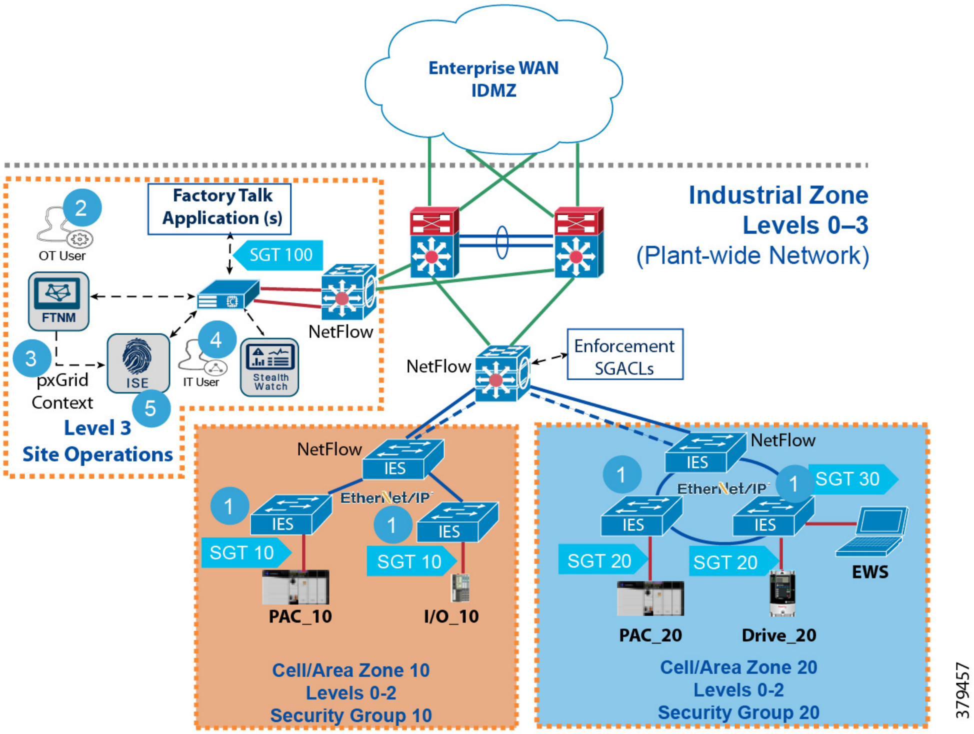
Source \ Destination	SGT100	SGT10	SGT20
SGT100	✓	✓	✓
SGT10	✓	✓	⊘
SGT20	✓	⊘	✓

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

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

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

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



Flow-based Anomaly Detection Using Stealthwatch Technology

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

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

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

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

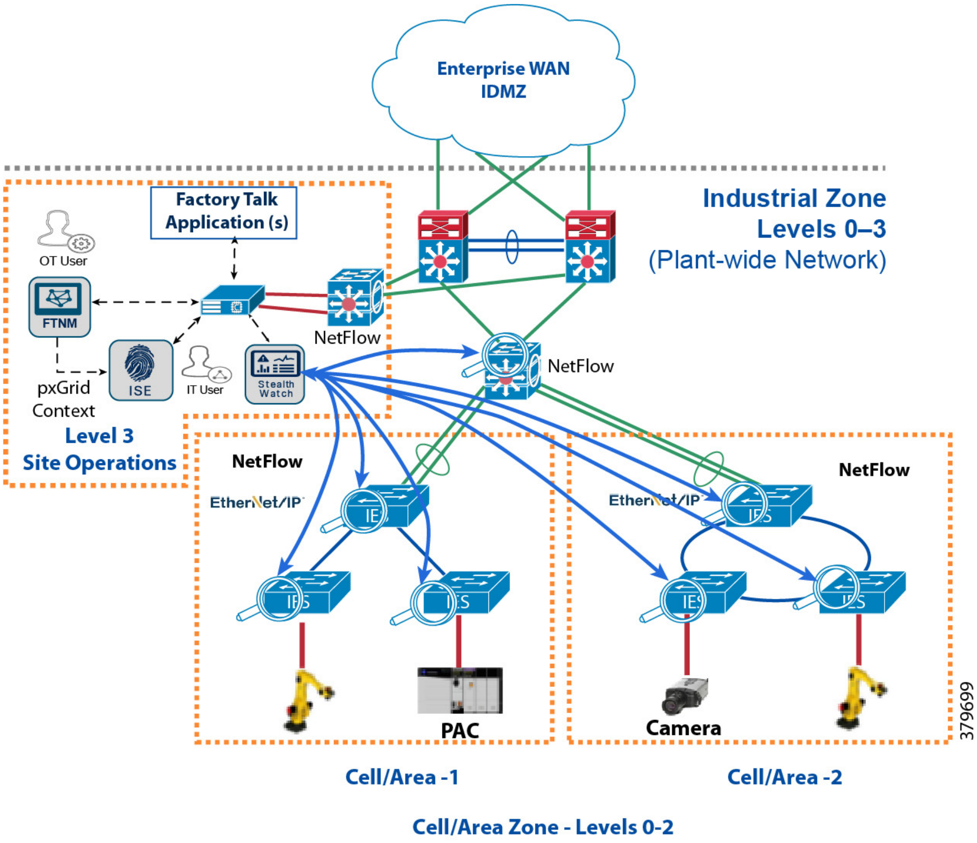
- Add a cable directly from the source IES to the destination switch.
- Configure remote SPAN (RSPAN) on the source IES, implement a dedicated RSPAN VLAN, then configure RSPAN on the destination switch.

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

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

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

Figure 1-7 Detecting Network Anomalies Using Cisco Stealthwatch

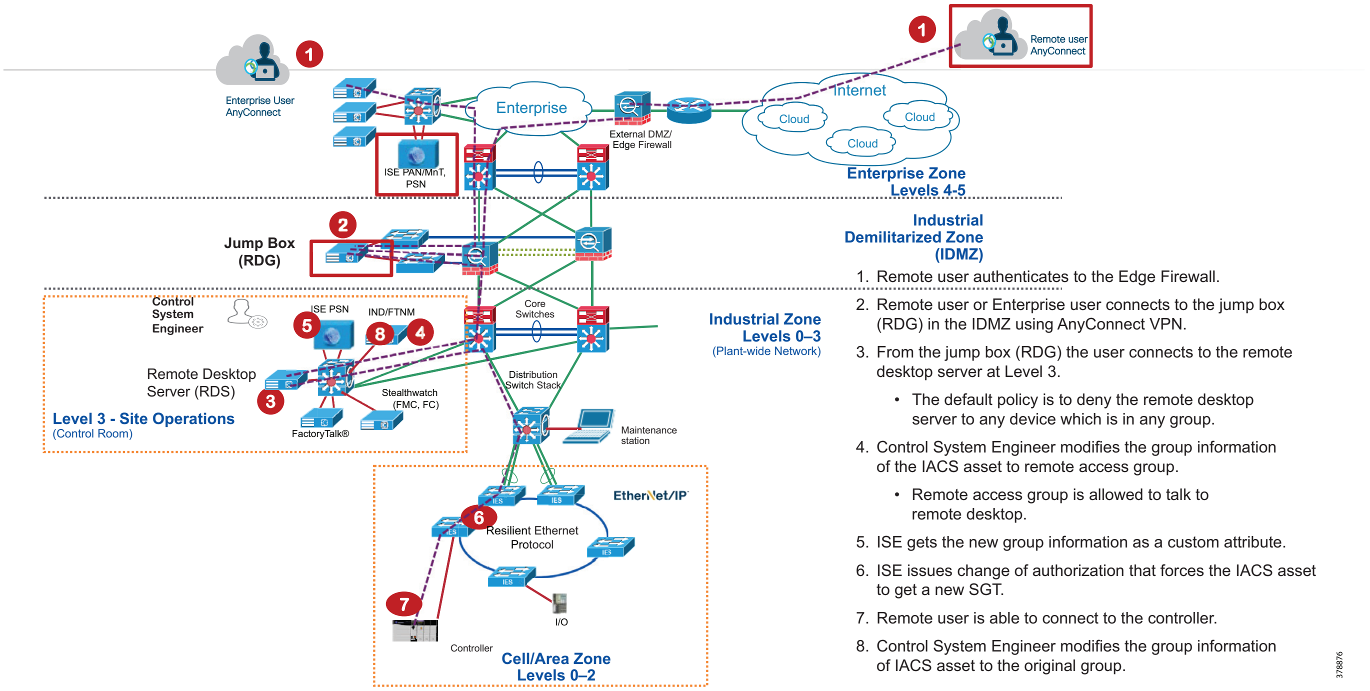


OT Influenced Remote Access—For Example Downtime

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

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

Figure 1-8 OT Influenced Remote Accessing NMT Solution



1. Remote user authenticates to the Edge Firewall.
2. Remote user or Enterprise user connects to the jump box (RDG) in the IDMZ using AnyConnect VPN.
3. From the jump box (RDG) the user connects to the remote desktop server at Level 3.
   - The default policy is to deny the remote desktop server to any device which is in any group.
4. Control System Engineer modifies the group information of the IACS asset to remote access group.
   - Remote access group is allowed to talk to remote desktop.
5. ISE gets the new group information as a custom attribute.
6. ISE issues change of authorization that forces the IACS asset to get a new SGT.
7. Remote user is able to connect to the controller.
8. Control System Engineer modifies the group information of IACS asset to the original group.