



Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense

Design and Implementation Guide

March 2022



Preface

Converged Plantwide Ethernet (CPwE) is a collection of architected, tested, and validated designs. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs achieve the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits by using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through an ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense (CPwE IDMZ), which is documented in this Design and Implementation Guide (DIG) outlines several security architecture use cases for design and deployment of an Industrial Demilitarized Zone (IDMZ) within Industrial Automation and Control System (IACS) applications. CPwE IDMZ was architected, tested, and validated by Cisco Systems and Rockwell Automation with assistance by Panduit.

CPwE IDMZ provides a comprehensive explanation of the IDMZ application design. It includes information about key requirements, possible deployment models, potential challenges, technology considerations, and guidelines for implementation and configuration of these specific use security cases within the CPwE framework.

Release Notes

This section summarizes the updates to CPwE IDMZ in this March 2022 release:

- New Design and Implementation Guide using Cisco Firepower Threat Defense (FTD) technology, Firepower Management Center (FMC), and Duo
- For design and implementation guidance using Cisco Adaptive Security Appliance (ASA) firewall technology, see *Securely Traversing IACS Data across the Industrial Demilitarized Zone*, ENET-TD009B-EN-P, dated May 2017

Summary of Specific Changes

This document contains the following changes from the previous version:

- Replaced Cisco ASA Firewall with Cisco Firepower Threat Defense (FTD)
 - Validation testing reflects the use of Cisco FTD with Firepower Management Center as the management platform.
 - Application detectors have been added to the recommended access control policies where applicable.
 - File policy has been added to the secure file transfer use case.
 - Resiliency chapter updated.
- Added the following use cases to the IDMZ design:
 - Multi-Factor Authentication
 - Managing product licenses in the Industrial Zone
 - Windows® Updates to devices in the Industrial Zone
 - Data brokering from Industrial Zone to Enterprise Zone
- Added the following technologies to the IDMZ design:
 - Cisco Telemetry Broker
 - Cisco Secure Access by Duo
 - Cisco Smart Software Manager On-Prem
 - Rockwell Automation® Thin Manager®

**Note**

For readers who have not yet updated their architecture and wish to view deployment considerations with Cisco ASA Firewall, the previous version of the document can be found at:

- Rockwell Automation site:
https://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

Document Organization

This document is composed of the following chapters and appendices:

Chapter	Description
CPwE IDMZ Overview	Overview of CPwE IDMZ, including discussion of Holistic Industrial Security, Industrial Demilitarized Zone and Converged Plantwide Ethernet IDMZ.
System Design Considerations	Provides a high level overview of the Industrial Automation and Control Systems (IACS) and basic design considerations for the Industrial Demilitarized Zone (IDMZ) of the CPwE architecture.
Configuring the Infrastructure	Describes how to configure IDMZ infrastructure in the CPwE architecture based on the design considerations of the previous chapters. It covers the configuration of the network infrastructure, network services, data traversal, remote access services and network and application security, all from an IDMZ perspective.

Chapter	Description
CPwE IDMZ Troubleshooting	Describes troubleshooting for Cisco Firepower Threat Defense failover and firewall rules.
Appendix A, “References”	List of references for CPwE and Cisco solutions and technologies.
Appendix B, “Test Hardware and Software,”	List of network hardware and software components used in the CPwE IDMZ testing.
Appendix C, “Acronyms and Initialisms”	List of all acronyms and initialisms used in the document.
Appendix D, “About the Cisco Validated Design (CVD) Program”	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs).

For More Information

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

- Rockwell Automation site:
<https://www.rockwellautomation.com/en-us/capabilities/industrial-networks/network-architectures.html>
- Cisco site:
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html



Note

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

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

CPwE IDMZ Overview

This chapter includes the following major topics:

- [CPwE IDMZ Introduction](#)
- [CPwE Overview](#)
- [CPwE Industrial Security Framework Overview](#)
- [Industrial Demilitarized Zone](#)
- [CPwE IDMZ Solution Use Cases](#)

CPwE IDMZ Introduction

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, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

IIoT helps offer the promise of business benefits by using innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

Many organizations and standards bodies recommend segmenting business system networks from plant-wide and site-wide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network in a level between the Industrial and Enterprise Zones, commonly referred to as Level 3.5. An IDMZ environment consists of numerous infrastructure devices, including firewalls, virtual private network (VPN) servers, IACS application mirrors, remote gateway services and reverse proxy servers, in addition to network infrastructure devices such as routers, switches and virtualized services. CPwE IDMZ details considerations to help with the successful design and implementation of an IDMZ to securely share IACS data between the business systems within the Enterprise Zone and industrial operations within the Industrial Zone.

CPwE Overview

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) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

- Smart IIoT devices-Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP), facilitating both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS devices
- Zoning (segmentation)-Smaller connected LANs, functional areas, and security groups
- Managed infrastructure-Managed Allen-Bradley® Stratix® industrial Ethernet switches (IES), Cisco Catalyst® distribution/core switches, FactoryTalk® Network Manager™ software, and Stratix® industrial firewalls
- Resiliency-Robust physical layer and resilient or redundant topologies with resiliency protocols
- Time-critical data-Data prioritization and time synchronization via CIP Sync® and IEEE-1588 Precision Time Protocol (PTP)
- Wireless-Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- Holistic defense-in-depth security-Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (for example, OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- Convergence-ready-Seamless plant-wide or site-wide integration by trusted partner application

Wide Area Network (WAN)

- Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services, Call Manager
- Security Services - Active Directory (AD), Identity Services (AAA), Web Security Appliance (TLS Proxy)
- Network Services – DNS, DHCP

Enterprise Zone Levels 4-5

Industrial Demilitarized Zone (IDMZ) Level 3.5

- Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Physical or Virtualized Servers

- Patch Management, AV Server
- Web Security Appliance (TLS Proxy)
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Level 3 - Site Operations (Control Room)

Cell/Area Zone - Levels 0-2

- Redundant LANs - Parallel Redundancy Protocol
- Enhanced Interior Gateway Routing Protocol – EtherChannel
- Hot Standby Router Protocol – Active/Standby (Skids, Equipment)

Cell/Area Zone - Levels 0-2

- Ring Topology - Device Level Ring (DLR) Protocol
- Redundant Star Topology - Flex Links Resiliency
- Unified Wireless LAN (Lines, Machines, Skids, Equipment)

EtherNet/IP™

Cell/Area Zone - Levels 0-2

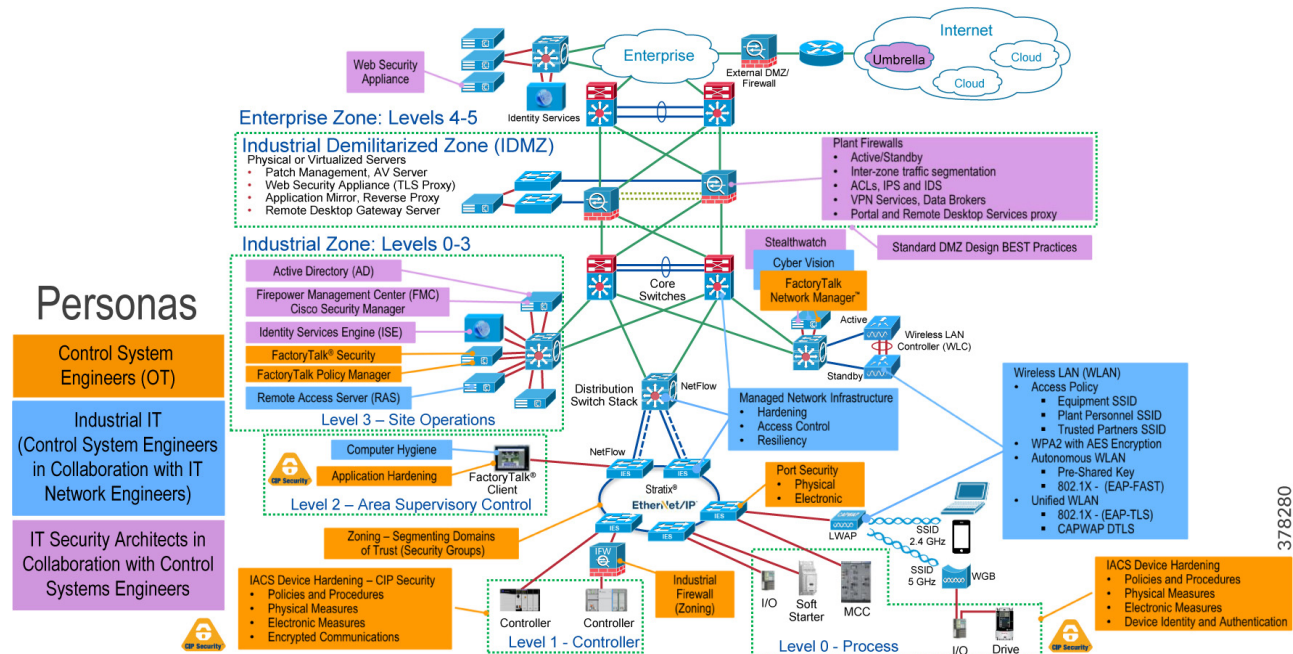
- Linear/Bus/Star Topology
- Redundant Star Topology - EtherChannel Resiliency
- Unified Wireless LAN (Lines, Machines)

No single product, technology, methodology or strategy can fully secure plant-wide or site-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) using diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture (Figure 1-2).

- Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense

- 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/site firewalls, Industrial Demilitarized Zone (IDMZ) design best practices, data brokers (for example, Web Security Appliance), and OpenDNS (for example, Umbrella).

Figure 1-2 CPwE Industrial Cybersecurity Framework



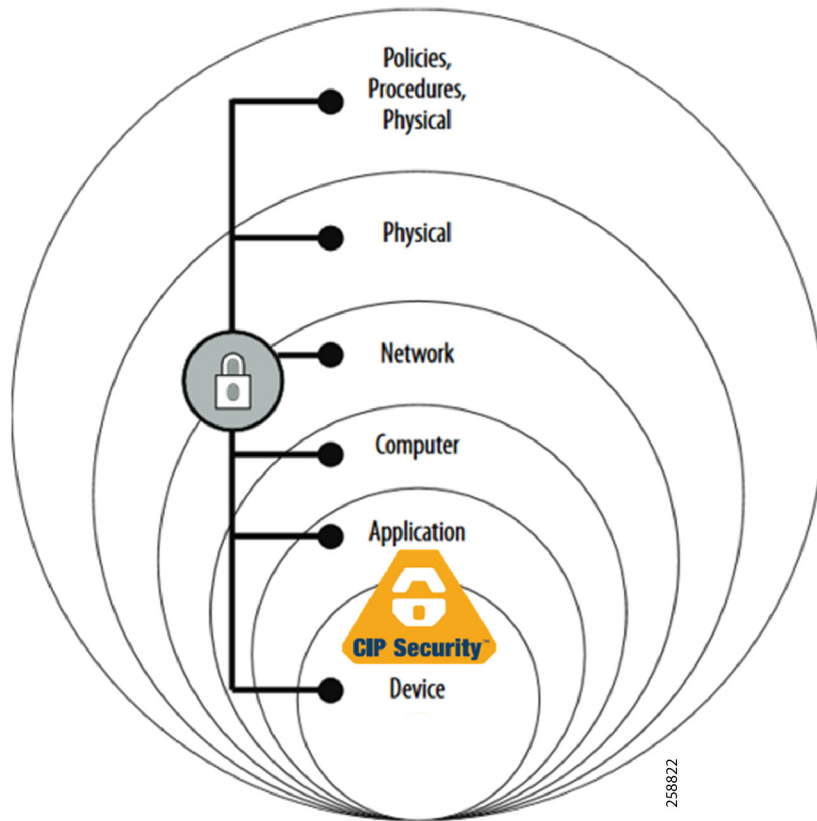
The CPwE Industrial Security Framework (Figure 1-2), using a defense-in-depth approach (Figure 1-3), is aligned to industrial security standards such as ISA/IEC-62443 Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Defense-in-depth applies policies and procedures that address many different types of threats.

To achieve a defense-in-depth approach, an operational process is required to establish and maintain the security capability. A security-operational process includes the following actions:

1. Identify IACS asset device types and locations within the plant-wide or site-wide network infrastructure.
2. Identify potential internal and external vulnerabilities and threats to those IACS assets and assess the associated risks.
3. Understand the application and functional requirements of the IACS assets including 24x7 operations, communication patterns, topology, required resiliency, and traffic types.
4. Understand the associated risks of balancing the application and functional requirements of IACS assets with the need to help protect the availability, integrity, and confidentiality of IACS asset data.

Figure 1-3 Defense-in-Depth Security



In a defense-in-depth security approach (Figure 1-3), different solutions are needed to address various network and security requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of the CPwE Industrial Security Framework (Figure 1-2).

- Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several industrial security architecture use cases, with Cisco ISE, for designing with visibility, segmentation, and anomaly detection throughout a plant-wide IACS network infrastructure.
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- 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 or site-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 Design Guide outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity from FactoryTalk applications to the Rockwell Automation 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
- 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-%20DIG.html>
- Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide outlines a comprehensive explanation of the CIP Security application design. It includes information about key requirements, possible deployment models, potential challenges, technology considerations, and guidelines for implementation and configuration of these specific use security cases within the CPwE framework.
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-%20DIG.html>

Industrial Demilitarized Zone

Sometimes referred to as a perimeter network, the IDMZ (see [Figure 1-4](#)) is a buffer that enforces data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the Industrial and Enterprise Zones. The demilitarized zone concept is commonplace to traditional IT networks and adoption for IACS applications.

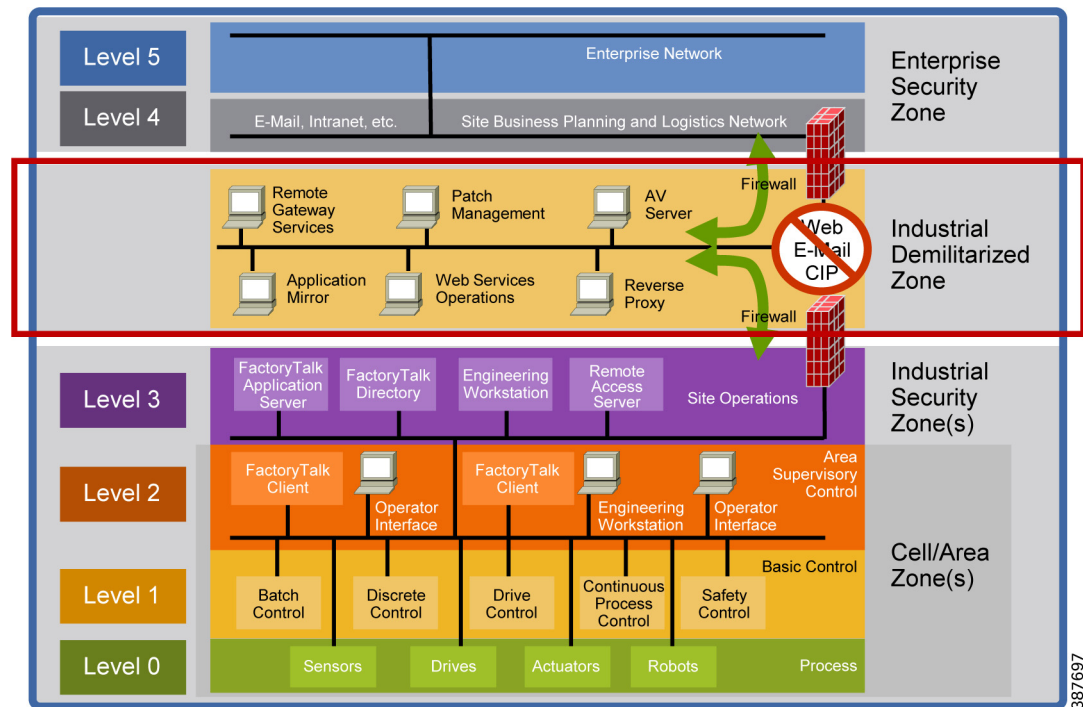
For secure IACS data sharing, the IDMZ contains assets that act as brokers between the zones. Multiple methods to broker IACS data across the IDMZ exist:

- Use application mirrors or proxies, such as:
 - PI-to-PI interface for FactoryTalk Historian
 - Secure File Transfer Gateway
 - Cisco Telemetry Broker

- Windows Server Update Services (WSUS)
- Use Microsoft® Remote Desktop (RD) Gateway services for secure remote access via Remote Desktop Connection client and ThinManager.

These broker methods, which help to hide and protect the existence and characteristics of the Industrial Zone servers from clients and servers in the Enterprise Zone, are highlighted in Figure 1-4 and are covered in CPwE IDMZ.

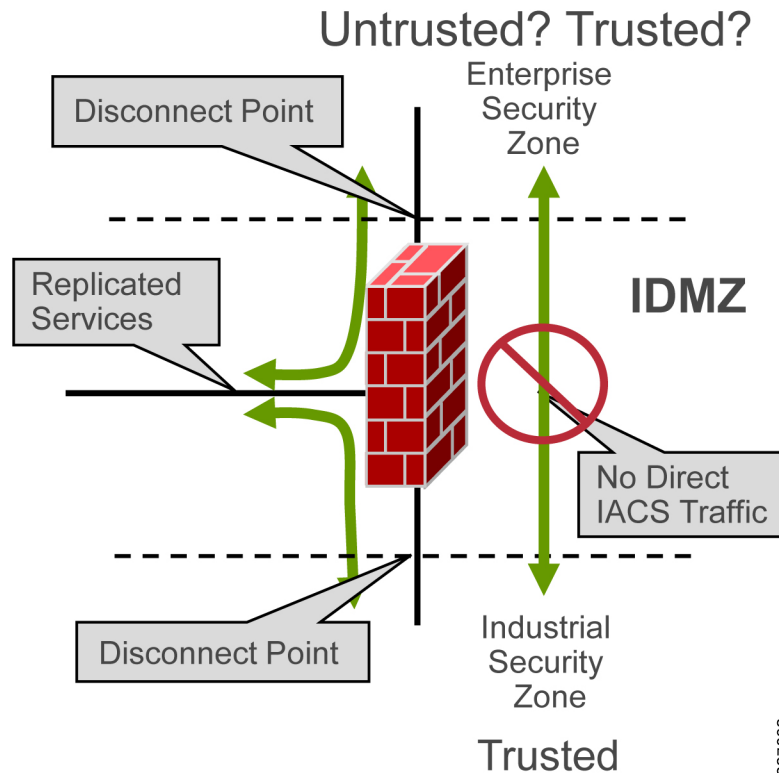
Figure 1-4 CPwE Logical Model



High-level IDMZ design principles (see Figure 1-5) include:

- All IACS network traffic from either side of the IDMZ terminates in the IDMZ; no IACS traffic directly traverses the IDMZ
- EtherNet/IP IACS traffic does not enter the IDMZ; it remains within the Industrial Zone
- Primary services are not permanently stored in the IDMZ
- All data is transient; the IDMZ does not permanently store data
- Functional sub-zones within the IDMZ are configured to segment access to IACS data and network services (for example, IT, Operations and Trusted Partner zones)
- A properly designed IDMZ will support the capability of being unplugged if compromised, while still allowing the Industrial Zone to operate without disruption

Figure 1-5 IDMZ High Level Concepts



CPwE IDMZ Solution Use Cases

CPwE IDMZ outlines key requirements and design considerations to help with successfully designing and deploying an IDMZ and implementing IACS data and network services between the Industrial and Enterprise Zones:

- An IDMZ overview and key design considerations
- A Resilient CPwE Architectural Framework:
 - Redundant IDMZ firewalls
 - Redundant distribution/aggregation Ethernet switches
 - Redundant core switches
- Methodologies to securely traverse IACS data across the IDMZ:
 - PI-to-PI interface for FactoryTalk Historian
 - Secure File Transfer Gateway
 - Cisco Telemetry Broker
 - Use Microsoft Remote Desktop (RD) Gateway services for secure remote access via Remote Desktop Connection client and ThinManager
 - WSUS Server
- Methodologies to securely traverse network services across the IDMZ

- CPwE IDMZ use cases:
 - IACS applications-for example, Secure File Transfer, FactoryTalk applications (FactoryTalk Historian, FactoryTalk® VantagePoint®, FactoryTalk View Site Edition, FactoryTalk ViewPoint, FactoryTalk AssetCentre, Studio 5000 Logix Designer®)
 - Network services-for example, AD, Cisco Identity Services Engine (ISE), Network Time Protocol (NTP), licensing management via Cisco Smart Software Manager On-Prem, and Windows Updates
 - Secure Remote Access
 - ThinManager access via Remote Desktop Gateway to IACS assets
 - Data Brokering via Cisco Telemetry Broker
- Important steps and design considerations for IDMZ implementation and configuration

System Design Considerations

This chapter includes the following major topics:

- [CPwE IDMZ Overview, page 2-1](#)
- [IDMZ Network Infrastructure Design, page 2-14](#)
- [IDMZ Design for Network Services, page 2-28](#)
- [Data Transfer through the IDMZ, page 2-46](#)
- [Remote Access Services, page 2-52](#)
- [Application Security, page 2-60](#)

This chapter provides a high-level overview of the basic design considerations for the Industrial Demilitarized Zone (IDMZ) of the CPwE architecture. CPwE IDMZ offers basic design and implementation guidance for the IDMZ, which IACS networking personnel could use to design and deploy their architecture. Often, the IDMZ is where IT networking resources are involved in the design, implementation and maintenance. For more complex deployments, Cisco and Rockwell Automation recommend the involvement of either external resources or Enterprise IT networking specialists.

**Note**

This chapter provides both general descriptions of product capabilities and specific design recommendations for the CPwE IDMZ architecture. Refer to [Configuring the Infrastructure](#) for more information about specific features and configuration steps that have been validated for the CPwE architecture.

CPwE IDMZ Overview

This section describes the concepts, objectives and main design principles of the IDMZ.

What is the IDMZ?

The Industrial Zone contains all IACS network and automation equipment that is critical to controlling and monitoring plant-wide operations. Hierarchically, the Industrial Zone includes Site Operations (Level 3) and multiple Cell/Area Zones (Levels 0 to 2).

To preserve smooth plant-wide operations and functioning of the IACS applications and network, the Industrial Zone requires clear segmentation and protection from the Enterprise Zone via security devices, replicated services and applications. The zone that separates the Enterprise Zone from the Industrial Zone is called the IDMZ. This insulation not only enhances security segmentation between the Enterprise and Industrial Zones, but may also represent an organizational boundary where IT and Operational Technologies (OT) responsibilities interface.

A Demilitarized Zone (DMZ) is sometimes referred to a perimeter network that exposes an organization's trusted external services and data to an untrusted network. Most of the time, the DMZ is understood as protecting a company's Enterprise assets from the Internet. A DMZ is a proven method to protect a trusted network like the Enterprise network from an untrusted network like the Internet.

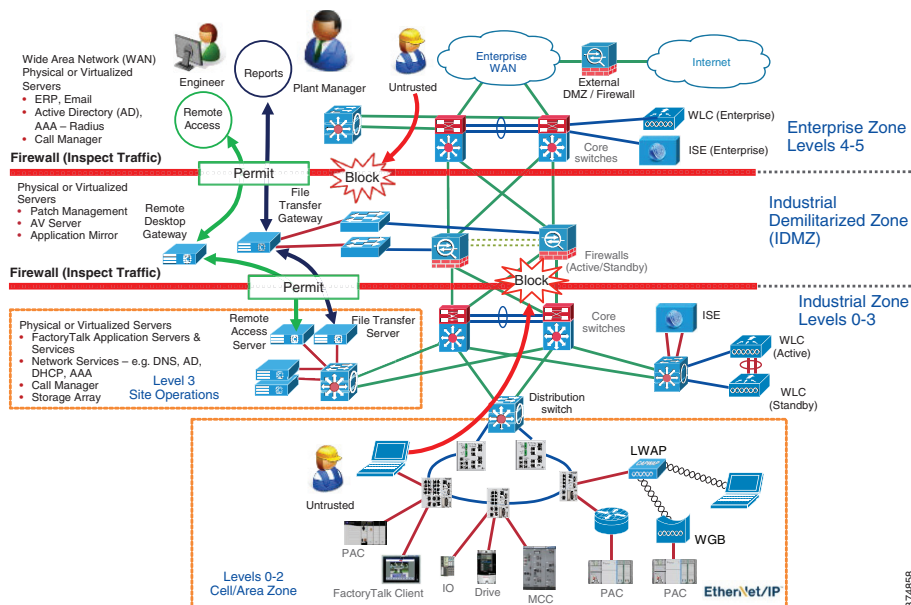
In the context of securing the Industrial Zone from the Enterprise, the IDMZ is placed between a trusted network (the Industrial Zone) and an untrusted network (the Enterprise Zone). The IDMZ functions in the same manner as a traditional DMZ because it allows traffic between the zones to be terminated within the DMZ and to be inspected as it enters and exits the IDMZ.

The IDMZ is comprised of:

- Boundary or “edge” security appliances like firewall(s) that can inspect traffic as it enters and exits each security zone
- Appliances and servers that replicate services like web proxies, data proxies, file transfer proxies, application and operating system patch proxies, and application proxies

In the most basic terms, the IDMZ is a termination end point for traffic from the untrusted Enterprise network. The traffic from the Enterprise that is destined for the Industrial Zone is terminated on a server or application proxy within the IDMZ. The firewalls can inspect the traffic as it enters or exits the IDMZ. The firewall can be configured to allow remote access or file requests from certain users, but block “untrusted” users or devices from entering or exiting the IDMZ (see [Figure 2-1](#)).

Figure 2-1 IDMZ Concepts



374858

This approach permits the Industrial Zone to function entirely on its own, without taking account of the connectivity status to the higher levels. A methodology and procedure should be deployed to buffer IACS data to and from the Enterprise Zone in the event of IDMZ connectivity disruption. As a best practice, Cisco and Rockwell Automation recommend that all IACS assets required for the operation of the Industrial Zone should remain in the Industrial Zone.

This separation is necessary because real-time availability and security are the critical elements for the traffic in the IACS network. Downtime in an IACS network is much more costly than downtime of similar scale in an enterprise environment. The cost of capital, the loss of product and material, missed schedules and the wasted time of plant personnel drive this very concrete impact on revenue and efficiency. Therefore, Cisco and Rockwell Automation recommend the deployment of Industrial Zone firewalls and an IDMZ between the Industrial and Enterprise Zones to securely manage the traffic flow between these networks.

IDMZ Objectives

Data and services must be shared between the Industrial and Enterprise Zones. Many of the benefits of converged industrial and enterprise networks rely on real-time communication and transfer of data between these zones. Without Industrial Zone firewalls and an IDMZ, data cannot be shared while also maintaining the security of the IACS network and its IACS systems.

The Industrial Zone firewall:

- Enforces and strictly controls traffic from hosts or networks into and out of each security zone
- Performs stateful packet inspection
- Optionally can provide intrusion detection/prevention
- Provides security and network management support
- Terminates VPN sessions with external or internal users
- Provides web portal services such as proxy services
- Enables Remote Desktop connectivity services for secure remote access via Remote Desktop Connection client and ThinManager to servers in the Industrial Zone

IDMZ offers a network on which to place data and services to be shared between the Enterprise and Industrial Zones. The IDMZ doesn't allow direct communication between the Industrial and Enterprise Zones, but meets the data and service sharing requirement. With the deployment of an IDMZ and Industrial Zone firewall, attacks and issues that arise in one zone cannot easily affect the other zone. In fact, by temporarily disabling the IDMZ and the firewalls, an IACS or IT network administrator can help to protect a zone until the situation is resolved in the other zone.

The IDMZ network design covers the following:

- IDMZ components
- IDMZ topology
- Firewall design and implementation considerations
- IACS application interoperability

IDMZ Design Principles

To design an IDMZ, the first exercise is to fully understand:

- Which Enterprise systems need to interact with the Industrial Zone systems

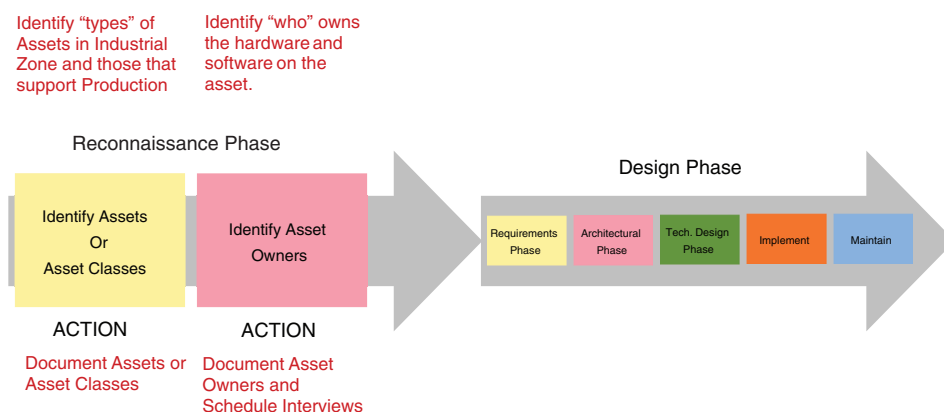
- Which Industrial Zone systems need to interact with Enterprise systems
- Which Enterprise users must interact with Industrial Zone systems and the tasks they perform with these systems
- Which Industrial Zone users must interact with Enterprise systems and the tasks they perform
- How long the Enterprise systems can stay disconnected from the Industrial Zone before IDMZ connectivity is restored

After getting the answers to these questions, you will be able to define the services and data that need to be replicated or proxied within the IDMZ.

The IDMZ design process consists of gathering stakeholder requirements and designing a solution to meet the requirements. In order to do so, you will gather requirements from the people who design, operate, change and maintain these systems. Before designing an IDMZ, you must identify the assets within the Enterprise and Industrial Zones that are needed to support the IACS process.

- The **Reconnaissance Phase** is used to identify the assets or "types" of assets in the Industrial Zone used to support production and those that will feed data or reports to Enterprise systems or Enterprise users (see [Figure 2-2](#)). The Reconnaissance Phase is used to identify the systems that are located in the Industrial Zone that will interact with the Enterprise Zone and ultimately have to communicate through the IDMZ to do so. During the Reconnaissance Phase, it is also important to compile a list of asset owners so they can be interviewed and their requirement documented.

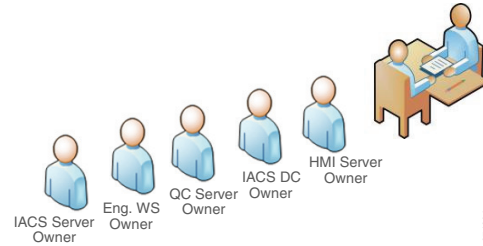
Figure 2-2 IDMZ—Network Reconnaissance (Design Pre-Work)



For example, it may be determined that access to a Human Machine Interface (HMI) server from the Enterprise engineering department is required. The asset owner, who would then be interviewed to gather their requirements, may state that gaining access to the HMI server to create faceplates or troubleshoot the system is required. All the system owners should be interviewed paying close attention to the tasks they perform within the system; those requirements are then the basis for design of the IDMZ solution (see [Figure 2-3](#)).

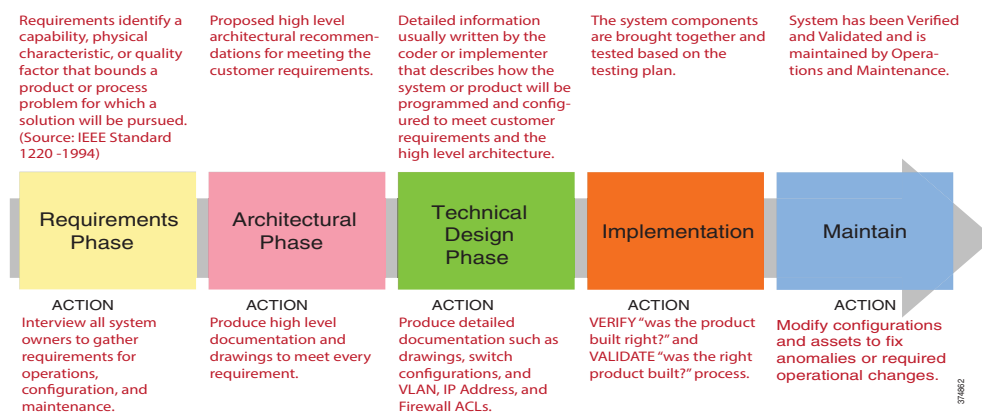
374859

Figure 2-3 System Owners Interview Process



After the Reconnaissance Phase is completed, the IDMZ design phase can begin. An example of an IDMZ design cycle is listed below (see Figure 2-4). While this is not the only methodology available, it has been successfully used in the design and implementation of an IDMZ.

Figure 2-4 IDMZ Design Methodology



- The **Requirements Phase** is used to record all user and system requirements. The IEEE 1220 standard states that "requirements are a statement identifying a capability, physical characteristic or quality factor that bounds a product or process problem for which a solution will be pursued". All stakeholder and system requirements should be documented during this phase so technical solutions can be engineered to meet all the requirements. Requirements are derived from system users, designers, engineers and vendors.
- The **Architectural Phase** is used to propose a high-level solution to the stakeholders to see if it is acceptable prior to committing time to working on the technical solution.

For example, let's suppose a requirement could be met with a solution that is available on a Linux operating system. Before moving forward, let's suppose the stakeholder is not familiar with nor can they support the Linux operating system. The Architectural Phase allows the technical team to propose a solution and gain consensus with the stakeholder before implementing the solution. In the last example, let's suppose the same solution is available in the Windows operating system and the stakeholder agreed to the solution. It is much better to gain consensus earlier when less technical implementation hours have been spent.

- The **Technical Design Phase** is when detailed information is written by the coder or the implementer that describes how the system or product will be programmed or configured to meet the customer's requirements. This reflects the proposed solutions in the Architectural Phase.
- The **Implementation Phase** is when the system components are brought together, tested, verified and validated per the testing plan.
- The **Maintain Phase** is when the operating systems are supported. Frequently configurations are modified to fix anomalies or to support operational changes.

IDMZ Security Policy

As mentioned previously, the IDMZ is meant to buffer and inspect traffic that is flowing between the Enterprise and Industrial Zones. When designing the IDMZ that help shape the security policies and design decisions, the following key points should be kept in mind:

- Eliminate direct traffic between the Enterprise and Industrial Zones. Every organization must assess the risk(s) if this rule is not followed. Exceptions are sometimes made if risk vs. reward metrics are accepted by the organization.
- Do not create firewall or security rules that allow IACS protocols through the Industrial Zone interface. IACS protocols are defined as those that are used by Distributed Control System (DCS) and Programmable Automation Controllers (PAC) vendors to communicate with controllers, I/O subsystems, human-machine interface (HMI) or computer systems that are used to program or monitor these types of equipment. An example of such a protocol is CIP.
- Where practical, use VLAN segmentation for the IDMZ assets. This policy will help to make it possible for the firewall to inspect traffic between the IDMZ hosts and make it more likely to catch a compromised IDMZ asset.
- Design the IDMZ to limit the number of inbound and outbound connections to help simplify the firewall and security rules. As a rule, IACS assets and their support systems should remain in the Industrial Zone as much as possible.
- Design the IDMZ with the ability to be disconnected from both the Enterprise and Industrial Zones. This could have a major impact on how the Industrial Zone or Enterprise Zone assets are deployed in order to support operations while the IDMZ is disconnected.
- Do not place permanent data stores in the IDMZ. The IDMZ is the buffer network between the Enterprise and Industrial Zone and is used for temporary data replication and services. If the IDMZ is compromised and an organization has placed valuable data stores in the IDMZ, it could affect the operation and compromise the critical data.

Cisco and Rockwell Automation recognize that each organization must determine their own risk tolerance as they design the IDMZ. The risk vs. financial investment will most likely have some impact on the technologies and architectures that are ultimately chosen for implementation. The best practices listed in this document are meant to provide solution examples that have been tested within the IDMZ.

CPwE IDMZ Security Policy Exceptions

As previously noted, the recommendation is to disallow direct communications between the Enterprise and Industrial Zones. Certain technologies, however, are not designed to be proxied through a demilitarized zone. Situations also exist where a customer makes a reasonable design decision that allows for more risk acceptance in order to trade for better performance or lowered cost of implementation and total life cycle cost.

The tested CPwE IDMZ architecture took security policy exceptions for the following systems and the rationale for each (see [Table 2-1](#)). These technologies are reviewed in more detail later in the document.

**Note**

In some cases, an addition of an asset in the IDMZ may help to avoid direct communication through the IDMZ. However, these solutions have not been validated as part of CPwE IDMZ.

Table 2-1 IDMZ Security Policy Exceptions

Asset or Technology	Rationale for Exception	Can Additional Assets be Placed in IDMZ?
Domain Controller Replication	Transport and application Layer security; End-to-end encrypted communication; Total cost of ownership	Yes—Additional DC located in IDMZ that would synchronize with the Enterprise and Industrial Zone DC
Identity Services Engine policy Synchronization and Logging	Can use company-wide distributed ISE deployment with Policy Administration Node (PAN) in the Enterprise Zone; Total Cost of Ownership	Yes—ISE Policy Service Node (PSN) located in the IDMZ
NTP Time Synchronization	Better accuracy by direct connection of Industrial NTP server to Enterprise NTP; NTP traffic can be authenticated by servers.	Yes—IDMZ NTP server could synchronize time with the Industrial Zone NTP server.

IDMZ Data Flow Example

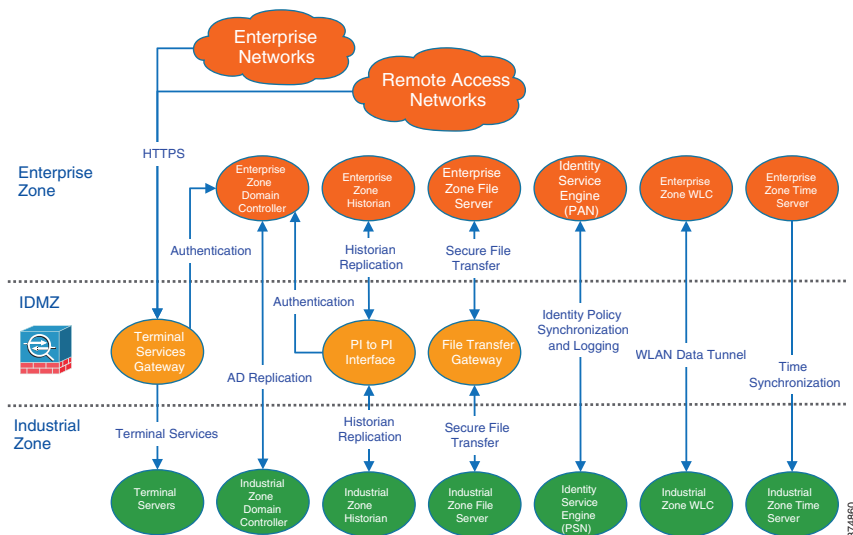
One of the results of developing an IDMZ security policy is a set of requirements for the network services and application data flow through the IDMZ. Figure 2-5 shows a high-level overview of what applications and protocols may have to be allowed through the IDMZ firewalls. As discussed in the previous section, certain network services may be allowed to communicate directly while IACS applications use IDMZ assets to exchange data.



Note

The applications and services shown here have been validated as part of the CPwE IDMZ solution and discussed in more details later in the document. The requirements for a particular IACS network may differ depending on business needs, security policies and existing infrastructure.

Figure 2-5 IDMZ Data Flow Example



Industrial Zone Security Policy

The convergence of plant-wide and enterprise networks provides greater access to IACS data, which allows manufacturers to make more informed real-time business decisions. This business agility provides a competitive edge for manufacturers who embrace convergence. Convergence also calls for evolved security policies for IACS networks, which no longer remain isolated within a plant-wide or site-wide area. IACS computing and controller assets have become susceptible to the same security vulnerabilities as their enterprise counterparts. A security policy needs to protect IACS assets. This security policy needs to balance requirements such as 24x7 operations, low Mean Time to Repair (MTTR) and high overall equipment effectiveness (OEE).

Securing IACS assets requires a comprehensive security model based on a well-defined set of security policies. Policies should identify both security risks and potential mitigation techniques to address these risks. Manufacturers also face an unclear demarcation line of network ownership and cultural differences between deploying enterprise and IACS assets. To address these obstacles, Cisco and Rockwell Automation recommend that manufacturers develop a IACS security policy, distinct from the enterprise security policy, based on the following considerations:

- Plant-wide or site-wide operation requirements
- Enterprise security policy best practices
- Risk assessment results
- A holistic security policy based on the defense-in-depth approach
- Industry security standards such as ISA-99/IEC-62443
- Manufacturers' corporate standards
- Deploying Network Security within a Converged Plantwide Ethernet Architecture located at:
 - *Deploying Network Security within a CPwE Architecture:*
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
 - *Deploying Network Security within a Converged Plantwide Ethernet Architecture:*
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/WP/CPwE-5-1-NetworkSecurity-WP/CPwE-5-1-NetworkSecurity-WP.html
- A rigorous and well-documented patch management process

IACS Operations Security

This section outlines some recommended best Operations Security (OpSec) practices for the IACS and IDMZ.

- OpSec encompasses all networks, security systems, computer systems, applications and control systems that are required to support the production of a product or service and the duty to keep all of these systems running securely. While this is a broad topic, the intent of OpSec is to help confirm that people and services, such as computer applications, have the proper rights and privileges to the resources they require to do their job while preventing access to resources that they are not entitled to use.
- OpSec involves the use of technical controls like firewalls, access control lists, anti-virus, anti-malware, allow and deny listing technologies to name a few. It also involves using non-technical controls like policies and procedures to recommend or enforce behaviors with business assets or guiding business conduct.
- OpSec is often synonymous with protecting data that is considered proprietary or that contains intellectual property by means of technical and non-technical controls.

Defining Roles

Every person within the organization should be assigned a role so that consistent security credentials can be assigned to every organizational member. Role-based access control (RBAC) is prevalently used within companies and is leveraged throughout the plant-wide or site-wide systems. As a best practice, it is recommended that RBAC be used within the IACS environment to manage user authentication and authorization of all IACS assets.

While defining roles, one must also consider the concept of Least Privilege and Need to Know:

- **Least Privilege** means an individual should have enough permissions and rights to fulfill their role in the company and no more.
- **Need to Know** describes the restriction of access to the sensitive data. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's duties.

Separation of Duties

Separation of Duties (SoD) is a term used to describe when more than one person is required to complete a task and is used as a method for discovering or preventing fraud. SoD at many organizations is implemented within the enterprise context in a fuller and more robust manner, but often lacks granularity or roles and responsibilities within the IACS systems. For instance, one might see well-defined roles within enterprise descriptions but larger categories within IACS.

Table 2-2 shows an example of user groups in an organization. In this case, defining who can create accounts and give users their roles is an example of SoD.

Table 2-2 User Role Examples

Organizational Role	Core Responsibilities	Account Creation
IT Domain Controller Admin	Configure and maintain corporate domain controllers	Yes
Enterprise Database Admin	Create new database tables and SQL Queries Maintain database	No
Network Admin	Installs and maintains WAN/LAN equipment	Yes—Infrastructure only
Security Admin	Defines, configures and maintains security systems	No
Production Admins	Defines, configures and maintains Industrial Zone software assets that contain common enterprise software such as anti-virus and OS patches	Yes—IACS only
Engineers	Defines, configures and maintains Industrial Zone assets related directly to production systems	No
Maintenance	Maintains Industrial Zone assets related directly to production systems	No
Operators	Monitors production equipment to support the IACS process	No
Trusted Partner	A non-employee resource that is working for the company that needs access to certain assets	No

It is important to define all the roles within the organization and then define what each role is authorized to do with each system and application. Documenting these roles and responsibilities can help identify possible issues such as the conflict of a user being able to change their own security role or conflicting organizational reporting relationships such as the Security Administrator reporting to the Network Administrator which have conflicting business goals.

Data Classification

Data classification helps identify the value of the data to the organization so sensitive data can be organized and protected according to its sensitivity of theft, loss or unavailability. Data classified by the levels of confidentiality, integrity and availability attributes allows security administrators to determine the value to their organization and choose the appropriate controls necessary to protect the data.

Data classification has traditionally started at the Level 3 Site Operations without much regard to classifying the data at lower levels. Most security professionals are familiar with traditional controls to protect data while in motion and at rest in a traditional host. However, technology advances within modern Programmable Automation Controllers (PACs) like the ControlLogix® family make it possible to apply data classifications methods at the Cell/Area Zone level. Implementing FactoryTalk Security within the controller gives the ability to control **who** can do **what** to **which** controller and is also capable of restricting access to data. This type of functionality makes it possible to limit data tampering by allowing the PACs to participate in data security.

Network Redundancy and Availability

Networks are built out of numerous hardware and software components that may fail or that may be subject to attacks. Implementing redundant designs helps eliminate single points of failure (SPOF), which improves the availability of the network and makes it more resistant to attacks.

The CPwE architecture is built with many options for redundancy:

- Backup and redundant uplink interfaces
- Network hardware redundancy:
 - Redundant stackable distribution switches
 - Active/standby and active/active failover in the distribution and core layer
 - Firewall redundancy
- Topological redundancy: designs built with redundant paths at both network and data link layers

Typically, redundant network and control strategies are applied to operationally critical processes where a business determines that hardware failure or loss of visibility into the process cannot be tolerated. It is also recognized that non-critical processes that do not have this same high availability requirement exist and therefore the network and control architectures will not be designed in the same fashion as critical processes.

As a best practice, it is recommended that each business determine the types of processes within each Cell/Area Zone and classify the availability requirements. This type of classification exercise will determine the availability requirements within each Cell/Area Zone and drive the network requirements. Once this exercise is complete, one should design and test modular network architectures to support each availability requirement.

Network Infrastructure Hardening

This section reviews some of the best practices for securing IACS network infrastructure.



Note

More information about network infrastructure hardening can be found in the following documents:

- *Cisco Guide to Harden Cisco IOS Devices*
 - <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>
- *Configuring Switch-Based Authentication*

- http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/software/release/15_2_2_e/configuration/guide/scg-ie2000/swauthen.html

Disabling Unnecessary Services

Switches come out of the box with a list of services turned on that are considered appropriate for most network environments. Disabling these unnecessary services has two benefits: it helps preserve system resources and it helps to eliminate the potential of security exploits on the disabled services.

Cisco and Rockwell Automation recommend the following best practices:

- Global services should be disabled on all routers and switches unless explicitly needed. Note that some of the services are enabled by default (BOOTP, IP source routing, and PAD). Other global services such as finger, identification (identd), and TCP and UDP small servers are disabled by default.
- IP-directed broadcast should remain disabled on all Layer 3 IP interfaces except those required for access by RSLinx® data servers to browse for known or available IACS EtherNet/IP devices on a different subnet.
- Cisco Discovery Protocol (CDP) should be disabled on interfaces where the service may represent a risk; for example, on external interfaces such as those at the Internet edge and ports that connect end devices.
- Services on access ports such as MOP, IP redirects and Proxy ARP should be disabled unless required.
- The Stratix 5800 meets IEC 62443 4-2 Security Level 2 when properly configured to comply with the certification requirements. [Table 2-3](#) provides which switch security features are required to be configured to meet the IEC 62443 4-2 certification requirements.

Table 2-3 Switch Security Features

Switch Security Feature	Required to Meet IEC 62443-2	Details
IOS Release is certified for IEC-62443 4-2	Yes	To verify if your IOS release is certified for IEC-62443 4-2, access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc
Configure Certificate Authority (CA)	Yes	A CA provides a chain of trusts for devices in the network. This mechanism provides the ability for a user or process to trust the connection to one of these devices on the network by validating its identity. For more information, see the Security Configuration Guide at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xr-17/sec-pki-xr-17-book/sec-pki-overview.html
Configure Authentication, Authorization, and Accounting (AAA)	Yes	AAA services provide flexible administrative control and accounting for network access. For more information, see the Security Configuration Guide at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-4/configuration_guide/sec/b_174_sec_9300_cg.html
Disable Telnet	Yes	Telnet is disabled by default during Express Setup. Keep Telnet disabled to secure remote access to the switch, such as when you are using the command-line interface (CLI) to manage the switch from a computer.
Transport Layer Security (TLS) 1.2	Yes	TLS 1.2 is enabled by default during Express Setup. Keep this feature enabled to secure the exchange of data through encryption.
Configuration of Type 9 password hashing	Yes	Hashing makes password storage more secure by transforming a password into data that cannot be converted back to the original password. For more information, see the User Security Configuration Guide at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Applying Port Security

Access to the network starts with physically accessing ports on switches. A number of techniques to limit the ability to access the network exist.

First, network access cannot be achieved if the network devices are physically secure with limited access. Placing the industrial Ethernet switches in locked rooms or cabinets and installing port locks to prevent access to unused ports on a switch are all recommended best practices by Cisco and Rockwell Automation.

Further, industrial Ethernet switches themselves can be configured to secure their ports from unknown access or misuse. Switch port security limits the access to the network by unknown devices and limits the number of devices or media access control (MAC) addresses on any network port. Port security builds a list of secure MAC addresses in one of the two following ways, configurable on a per-interface basis:

- Dynamic learning of MAC addresses, which defines the maximum number of MAC addresses that will be learned and permitted on a port, is useful for dynamic environments, such as at the access edge
- Static configuration of MAC addresses, which defines the static MAC addresses permitted on a port, is useful for static environments such as a server farm or a DMZ

**Note**

Although some implementers may consider static MAC address configurations per port for environments that need very high security, this method requires significant effort and network expertise to perform normal maintenance tasks such as replacing a failed device.

The Error Disable feature helps protect the switch and therefore the network from certain error conditions. For example, when the number of MAC addresses on a port is exceeded. When the error condition is discovered, the interface is put into the error disable state and does not pass traffic.

Cisco and Rockwell Automation recommend the following:

- Use dynamic learning to limit the number devices that can access a port. This allows, for example, only one MAC address to access an IACS network port on the industrial Ethernet switch.
- Apply the *errdisable recovery interval seconds* global configuration command to restore the port state. This command will periodically check to see if the error condition still exists on the interface. The interface will be enabled automatically when the error condition has cleared.
- Disable all unused ports on a switch and only enable them when required.

Securing Administrative Access

When considering the security of a network infrastructure, it is critical that the administrative access to network devices is protected. Cisco and Rockwell Automation recommend the following best practices:

- Set and protect local passwords:
 - Enable automatic password encryption
 - Define a strong local *enable* password using the *enable secret* global command
 - Configure local user accounts (individual usernames and passwords) on devices for administrative access, as opposed to a single password for every user
- For highly secure IACS networks, configure devices for Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) authentication against the centralized user database using a remote AAA server (for example, Cisco ISE). Use accounting features of the AAA to log access and configuration changes

**Note**

Local user authentication should be used as a backup in case the remote AAA server is not available.

- Implement legal notification banners that are presented on all interactive sessions to confirm that users are notified of the security policy being enforced and to which they are subject
- Use Secure Shell (SSH) protocol when available rather than the unsecured Telnet. Use at a minimum 1024-bit modulus size. The SSH feature requires configuring AAA or local accounts on a device.
- If possible, use HTTPS for device management instead of clear-text HTTP
- If Simple Network Management Protocol (SNMP) is used for device management, use only SNMP v3 for read-write access. Configure the maximum security level using authentication and encrypted communication (authPriv). If SNMP v3 is not supported, use SNMP v1 or v2 for read-only access.
- Explicitly define the protocols allowed for incoming and outgoing sessions on the device. Restricting outgoing sessions prevents the system from being used as a staging host for other attacks.
- Configure access control lists (ACL) to restrict management traffic to the device. For example, an ACL can be configured to allow SNMP traffic only from the designated management servers.
- Set idle and session timeouts for remote access. Enable TCP keepalives to detect and close hung sessions.
- Protect switch configuration files and store them in a secure location. When sending the files externally (for example, to technical support), remove critical information such as user credentials, passwords and secret keys from the files (even if encrypted).

**Note**

SSH, HTTPS and SNMP v3 require the cryptographic (K9) version of IOS on the Cisco IE Series and Allen-Bradley® Stratix industrial Ethernet switches. Some cryptographic features are subject to additional export and contract restrictions. For more information about the Cisco products, see *Export and Contract Compliance* at:

- http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

Contact your Rockwell Automation sales representative or distributor for details about Stratix products.

Computer Hardening

For computing assets within the Industrial Zone, implement IT best practices applied to Enterprise computers. Some best practices and general recommendations include the following:

- Secure physical access. Network equipment and servers should be in locked cabinets or rooms.
- Keep computers up-to-date on service packs and hot fixes, but disable automatic updates. Also, network developers should test patches before implementing them and schedule patching and regular network maintenance during operational downtime.
- Apply Microsoft updates that have been qualified by Rockwell Automation to computers running Rockwell Automation® software products. Before implementing qualified updates, verify them on a non-production system, or when the facility is non-active, to avoid unexpected results or side effects.
- Deploy and maintain anti-virus and antispyware software, but disable automatic updates and automatic scanning. Test definition updates before implementing them and schedule manually-initiated scanning during operational downtime since antispyware scanning can disrupt real-time operations. Automatic anti-virus and antispyware scanning has caused data loss and downtime at some IACS facilities.

- Prohibit direct Internet access. IACS assets should not have direct line of sight to the Internet. Any necessary communication (for example, firmware, patches and anti-virus updates) should be accomplished via the IDMZ proxy and application servers.
- Implement the best practice password policy such as enforcing password history, maximum password age, minimum password length and complex password requirements.
- Disable the guest account on clients and servers.
- Require that the built-in administrator account uses a complex password, has been renamed and has removed its default account description.
- Develop and deploy backup and disaster recovery policies and procedures. Test backups on a regular schedule.
- Implement a change management system to archive network, controller and computer assets (clients, servers and applications).
- Use Control+Alt+Delete, along with a unique user name and password to log in.
- Protect unnecessary or infrequently used USB ports, parallel and serial interfaces to prevent unauthorized hardware additions (modems, printers, USB devices, etc.).
- Uninstall the unused Microsoft Windows components, protocols and services not necessary to operate the plant-wide system.
- Install and run only legitimately purchased software.

Assessments and Baselining

Baselines are representative of a singular point in time in which a company can reference for future changes. Typically, the assessment process is used to obtain a baseline of:

- Computer systems
- Infrastructure components like firewalls, routers and switches
- Network traffic types, quantity and data flow diagrams
- Security control assessments
- Hardware, firmware and software inventories

Baselines are also used to define the minimum levels of security controls that should be implemented to adhere to an organization's standards.

Cisco and Rockwell Automation recommend implementing consistent standards for assessment methodology by generating assessment and baselining policies. These activities should be performed periodically with a method to record the improvement or failure of the security program execution.

IDMZ Network Infrastructure Design

This section describes IDMZ CPwE design recommendations for the following network infrastructure components and protocols:

- Industrial Zone firewalls
- Industrial Zone core switches
- IDMZ server network
- Routing protocols between zones

Industrial Zone Firewalls

The industrial firewalls are an essential aspect of protecting the IACS network and applications. The combination of firewalls and an IDMZ zone concept are key aspects of the defense-in-depth approach for IACS network security. An Industrial Zone firewall provides the following functions:

- Implements an IDMZ where data and services between the Enterprise and Industrial Zones can be securely shared
- Establishes traffic patterns between the network zones via assigned security levels and access rules
- Provides stateful packet inspection of all traffic between the various zones
- Provides Intrusion Prevention Services (IPS) and Deep Packet Inspection (DPI) capabilities for inspecting application data between the zones designed to identify and potentially stop a variety of attacks
- Allows remote access to the IACS network for authenticated and authorized users

The following sections provide an overview of Cisco Firepower Threat Defense firewall platform and recommendations for deploying it as part of the CPwE solution.

Industrial Firewall Functionality

Cisco Firepower Threat Defense (FTD) brings distinctive threat-focused next-generation security services to the industrial network. It provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks. Cisco Secure Firewall (Cisco Firepower Threat Defense) includes:

- Site-to-site and remote access VPN and advanced clustering provide highly secure, high-performance access and high availability to help achieve business continuity.
- Granular AVC supports more than 3,000 application-layer and risk-based controls that can launch tailored IPS threat detection policies to optimize security effectiveness.
- The industry-leading Cisco FTD provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats and automate defense response.
- Reputation- and category-based URL filtering offer comprehensive alerting and control over suspicious web traffic and enforce policies on hundreds of millions of URLs in more than 80 categories.
- Advanced Malware Protection (AMP) provides industry-leading breach detection effectiveness, a low total cost of ownership, and superior protection value that helps you discover, understand, and stop malware and emerging threats missed by other security layers

Firewall Resiliency

Configuring high availability, also called failover, requires two identical FTD devices connected to each other through a dedicated failover link and, optionally, a state link. FTD supports Active/Standby failover, where one unit is the active unit and passes traffic. The standby unit does not actively pass traffic, but synchronizes configuration and other state information from the active unit. When a failover occurs, the active unit fails over to the standby unit, which then becomes active.

The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

**Note**

More information about FTD resiliency features can be found in *Information About High Availability* at:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/high_availability_for_firepower_threat_defense.html
-

Failover System Requirements

This section describes the hardware and software requirements for FTDs in a failover configuration.

The two units in a failover configuration must meet these hardware requirements:

- Be the same model
- Have the same number and types of interfaces
- Have the same modules installed (if any)
- Have the same amount of RAM installed

If you are using units with different flash memory sizes in your failover configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

The two units in a failover configuration must meet these software requirements:

- Be in the same firewall mode (routed or transparent)
- Have the same software version
- Be in the same group or domain in Firepower Management Center (FMC)
- Have the same NTP configuration
- Be fully deployed in FMC with n uncommitted changed
- Not have DHCP or PPPoE configured on any interface
- (Firepower 4100/9300) Have the same offload mode, either both enabled or both disabled

Failover Link

The two FTD units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keepalives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

You can use any unused interface on the device as the failover link, however, you cannot specify an interface that is currently configured with a name. The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface should only be used for the failover link (and optionally for the Stateful Failover link).

The failover link can be connected in one of the following two ways:

- Using a switch, with no other device on the same network segment as the failover interfaces of the FTD device.
- Using an Ethernet cable to connect the appliances directly, without the need for an external switch

Stateful Failover Link

To use Stateful Failover, firewalls must have a Stateful Failover link to pass all connection state information. Three options exist for selecting an interface for a Stateful Failover link:

- A dedicated Stateful Failover interface
- Sharing an interface with the failover link

Sharing a failover link is the best way to conserve interfaces. However, if you have a large configuration and a high traffic network, you must consider a dedicated interface for the state link and failover link.



Note

By default, all information is sent in clear text over the failover and Stateful Failover links. For additional security, the failover communication can be encrypted using a failover key.

If you use the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.

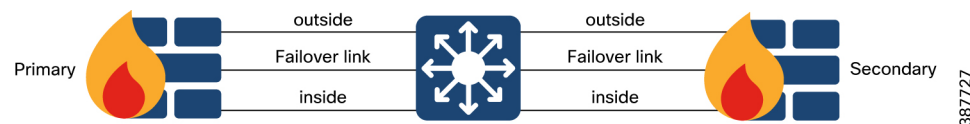
Avoiding Interrupted Failover and Data Links

We recommend that failover links and data interfaces travel through different paths to decrease the chance that all interfaces fail at the same time. If the failover link is down, the FTD device can use the data interfaces to determine if a failover is required. Subsequently, the failover operation is suspended until the health of the failover link is restored.

See the following connection scenarios to design a resilient failover network.

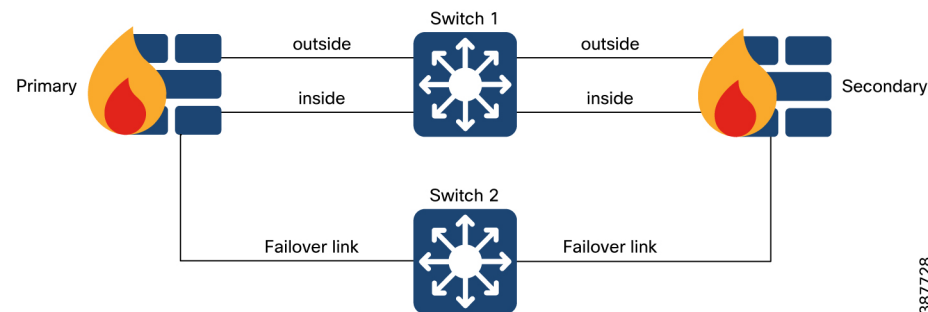
If a single switch or a set of switches are used to connect both failover and data interfaces between two FTD devices, then when a switch or inter-switch-link is down, both FTD devices become active. Therefore, the two connection methods shown in [Figure 2-6](#) and [Figure 2-7](#) are NOT recommended.

Figure 2-6 Connecting with a Single Switch—Not Recommended



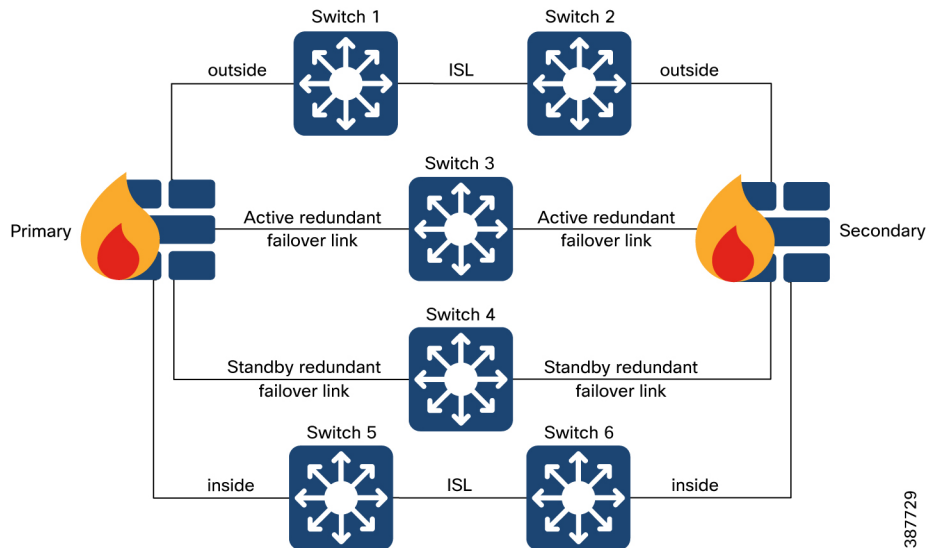
We recommend that failover links not use the same switch as the data interfaces. Instead, use a different switch or use a direct cable to connect the failover link, as shown in [Figure 2-7](#).

Figure 2-7 Connecting with a Double Switch—Not Recommended



The most reliable failover configurations use a redundant interface on the failover link, as shown in Figure 2-8.

Figure 2-8 Connecting with Redundant Interfaces—Recommended



Firewall Policy Design

IDMZ firewall is positioned between the Industrial Zone and the Enterprise Zone which follows the IDMZ security policy as described previously. The firewall design is primarily based on what application traffic needs to be permitted or denied, and what hosts can originate application connections that are allowed through the firewall.

The recommended and usual practice is to implement a restrictive policy on a firewall:

- Deny any service unless it is expressly permitted
- Restrict who is allowed to communicate to the necessary minimum

Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log (non-fast-pathed) network traffic.

Each managed device can be targeted by one access control policy. The network traffic data collected by the policy target devices can be used to filter and control that traffic based on:

- Simple, easily determined transport and network layer characteristics: source and destination, port, protocol, and so on
- The latest contextual information on the traffic, including characteristics such as reputation, risk, business relevance, application used, or URL visited
- Realm, user, user group, or ISE attribute
- Custom Security Group Tag (SGT)
- Characteristics of encrypted traffic; you can also decrypt this traffic for further analysis
- Whether unencrypted or decrypted traffic contains a prohibited file, detected malware, or intrusion attempt
- Time and day (on supported devices)

Each type of traffic inspection and control occurs where it makes the most sense for maximum flexibility and performance. For example, reputation-based blocking uses simple source and destination data, so it can block prohibited traffic early in the process. In contrast, detecting and blocking intrusions and exploits is a last-line defense.

Access Control Policy Default Action

A newly created access control policy directs its target devices to handle all traffic using its default action. In a simple access control policy, the default action specifies how target devices handle all traffic. In a more complex policy, the default action handles traffic that:

- Is not trusted by Intelligent Application Bypass
- Is not on a Security Intelligence Block list
- Is not blocked by SSL inspection (encrypted traffic only)
- Matches none of the rules in the policy (except Monitor rules, which match and log-but do not handle or inspect-traffic)

The access control policy default action can block or trust traffic without further inspection, or inspect traffic for intrusions and discovery data.

Deep Inspection Using File and Intrusion Policies

Deep inspection uses intrusion and file policies as the last line of defense before traffic is allowed to its destination.

- Intrusion policies govern the system's intrusion prevention capabilities.

For complete information, see An Overview of Intrusion Detection and Prevention at:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/overview_of_network_analysis_and_intrusion_policies.html

- File policies govern the system's file control and AMP for Networks capabilities.

For complete information, see File Policies and Malware Protection at:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/file_policies_and_advanced_malware_protection.html

Access control occurs before deep inspection; access control rules and the access control default action determine which traffic is inspected by intrusion and file policies.

By associating an intrusion or file policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy, a file policy, or both.

In an access control policy, you can associate one intrusion policy with each Allow and Interactive Block rule, as well as with the default action. Every unique pair of intrusion policy and variable set counts as one policy.

The creation and deployment of access control policies in FTD will be explored further in the document in relation to the use cases that are being secured.

Industrial Zone Core Network

The Industrial Zone core is the critical part of the plant network that is designed to be highly available and operate in an always-on mode. The core serves as the aggregator for all of the Cell/Area Zones and provides connectivity between end-devices, server-based applications and data storage. The Industrial Zone core connects via firewalls to the IDMZ.

The key design objectives for the core are:

- Provide the appropriate level of redundancy to allow for near immediate data-flow recovery in the event of any component (switch, supervisor, line card, or fiber) failure
- Permit the necessary hardware and software upgrade/change to be made without disrupting any network applications
- Avoid implementing any complex policy services in the core and have the minimal control plane configuration
- Do not have any directly attached user/server connections

In small-to-medium plants, it is possible to collapse the core into the two redundant distribution switches. However, for large plants, where a large number of Cell/Area Zones exist, this level of hierarchical segmentation is recommended.

Core Switch Architecture

The core switch architecture should meet the design requirements listed above to provide the required level of resiliency and performance. Large architectures normally use modular chassis-based core switches, such as Cisco Catalyst 4500/9300 or 9500 platforms.

**Note**

For more information on the Industrial Zone design and topology options, refer to Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide found at:

Rockwell Automation site:

- https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

Cisco site:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html

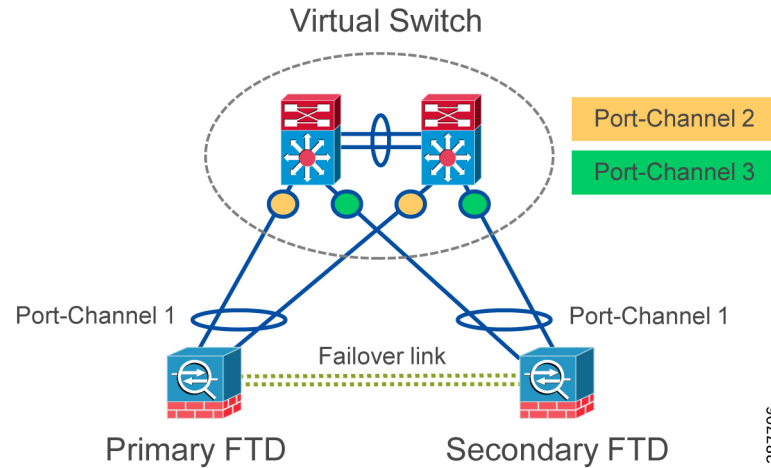
Connection to Redundant Firewalls

The IDMZ CPwE architecture recommends configuring redundant industrial firewalls in the active/standby mode with EtherChannels to the core switches. When a Virtual Switching System (VSS) is used, the FTD interfaces within the same EtherChannel can be connected to separate switches in the VSS.

**Note**

Separate EtherChannels should be created on the VSS switches for each FTD in an active/standby failover deployment (see [Figure 2-9](#)). A single EtherChannel on the VSS switch pair will not be established because of the separate FTD system IDs, and would not be desirable anyway because traffic should be sent only to the active FTD.

Figure 2-9 VSS and Active/Standby Firewalls



IDMZ Server Network

The IDMZ network hosts services that facilitate communication between the Enterprise and Industrial Zones, including RD Gateway for secure remote access via Remote Desktop Connection client and ThinManager, file transfer gateway, Historian connector (PI-to-PI Interface), and anti-virus and OS patch servers.

The design of the IDMZ server network will depend on the server farm size and IT management requirements and practices. Several scalable options exist:

- A redundant access/distribution switch pair (chassis-based, stack or stand-alone)
- A redundant distribution switch pair connecting multiple access switches in the redundant star topology
- Two or more switch blocks with separate distribution switches, for example to segregate servers into different management domains

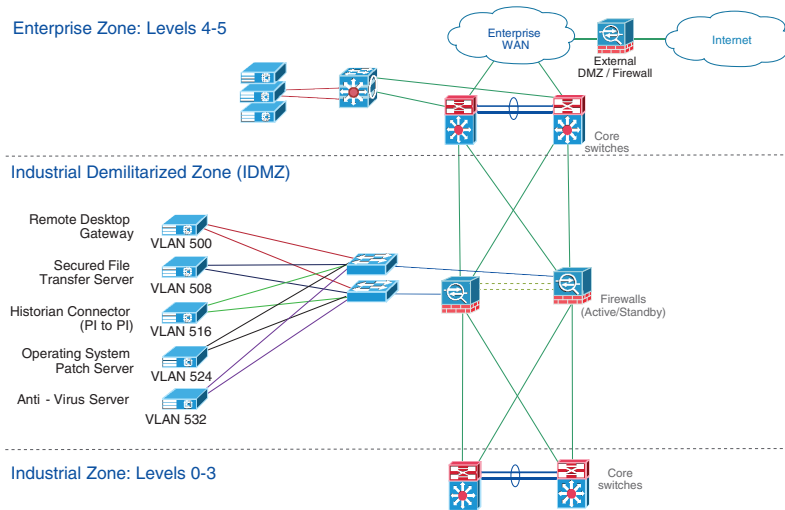
The resiliency features should include:

- Redundant server connections to access or distribution switches
- Redundant connections between distribution switches and industrial firewalls

IDMZ VLAN Segmentation

The IDMZ server network should be designed to meet the availability requirements and also designed to support traffic inspection between the hosts. In the example (see [Figure 2-10](#)), every IDMZ host such as the RD Gateway or the Secure File Transfer server has been put onto its own network or VLAN.

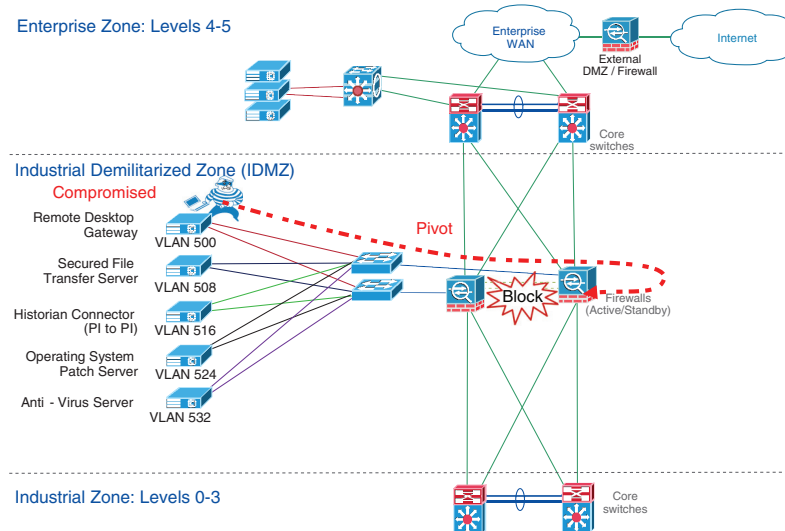
Figure 2-10 VLAN Segmentation in IDMZ Network



The IDMZ assets were placed on their own VLAN for strategic purposes. A “typical” piece of malware will compromise the asset and often attempt to either communicate outside the local network or it will attempt to infect other hosts on the same or other networks (see [Figure 2-11](#)).

If the compromised host attempts to communicate outside or within the IDMZ, a properly configured firewall will block the attempted pivot. If the firewall is configured to send alarm messages to a log or to a system monitor, then this incident can be investigated by the security team.

Figure 2-11 Compromised IDMZ Host



Routing Between Zones

In order to communicate between the Industrial and the Enterprise Zones, network infrastructure devices (Layer 3 switches, routers and firewalls) need to exchange IP subnet information via dynamic routing protocols or to have statically defined routes to destination IP subnets. This section provides recommendations and considerations for the routing protocol selection and design.

EIGRP Overview

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol. EIGRP is an advanced distance vector routing protocol. The Diffusing Update ALgorithm (DUAL) is used to obtain a loop-free topology during the network convergence. All routers involved in a topology change are able to synchronize at the same time. Routers that are not affected by topology changes do not need to synchronize. The EIGRP convergence time rivals that of any other existing routing protocol.

Some of the many advantages of EIGRP are:

- Very low usage of network resources during normal operation
- Only routing table changes are propagated, and not the entire table, during the convergence
- Rapid convergence times for changes in the network topology



Note

More information about EIGRP can be found in *Enhanced Interior Gateway Routing Protocol* at:

- <http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

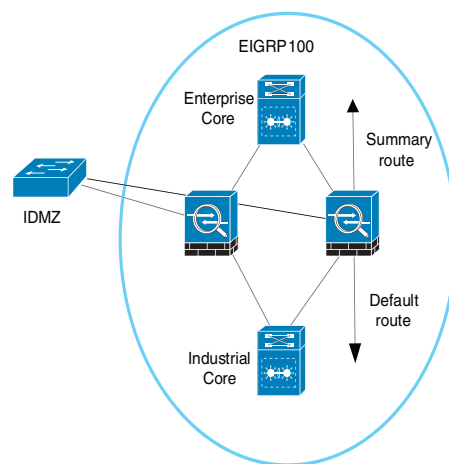
EIGRP Design

This section contains EIGRP design options and considerations, such as scalability, routing policy and configuration complexity.

Single EIGRP Domain

A single EIGRP domain is the simplest configuration for the routing protocol. In this design, all routers in both the Enterprise Zone and Industrial Zones participate in a common routing protocol instance, which is defined by the Autonomous System (AS) number (see [Figure 2-12](#)). The IDMZ firewalls actively participate in the routing protocol and summarize routes between the Enterprise and Industrial Zones. The firewall advertises a single default route to the Industrial Zone routers. On the enterprise side, it advertises a summary route for the Industrial Zone networks.

Figure 2-12 Single EIGRP Domain



This design, which allows for end-to-end routing from the Industrial Zone to the Enterprise Zone, works best if a single administrative team is responsible for all network devices across the company. Since all routers are a part of a common routing domain, the risk that routing protocol instability in one zone could affect other zones exists. This solution fits best with small-to-medium sized networks.

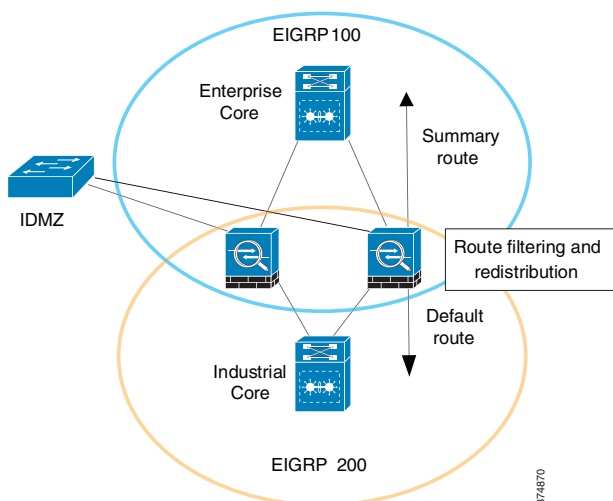
**Note**

A single EIGRP domain was used during the testing of this CPwE solution.

Multiple EIGRP Domains with Redistribution

In this design, the Enterprise Zone and each Industrial Zone are assigned a unique EIGRP domain. The routers in each zone use their own AS numbers while firewalls are configured for both AS. The IDMZ firewall acts as a boundary between the EIGRP process domains and redistributes routes between the processes (see [Figure 2-13](#)). In addition to redistribution, the firewalls also summarize routes advertising a single default route to the Industrial Zone. On the Enterprise side, it advertises summary routes for the Industrial Zone networks. The firewalls can also filter any routes that do not need to be advertised to either the Enterprise or Industrial Zones.

Figure 2-13 Multiple EIGRP Domains with Redistribution



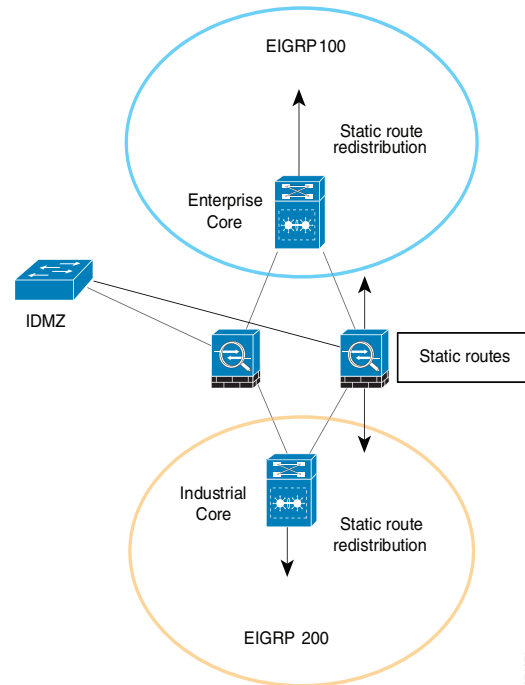
This design also allows for end-to-end routing between the Enterprise and Industrial Zones. However, this design divides the EIGRP routing process into smaller domains. This reduces the possibility of a routing protocol instability in one zone affecting another. This solution fits best with medium-to-large networks and easily accommodates environments with multiple Industrial Zones.

Multiple EIGRP Domains with Static Routes

In this case, similar to the previous design, the Enterprise and each Industrial Zone are assigned a unique EIGRP domain (AS number). The IDMZ firewalls act as a boundary between the EIGRP process domains; however, routes are not redistributed between zones.

Static routes must be configured on the routers connected to the firewalls and the firewalls themselves to forward traffic from the Enterprise Zone to the Industrial Zone and vice versa. The boundary router must also redistribute the static routes back into the routing protocol so the routes are reachable across the zone (see [Figure 2-14](#)).

Figure 2-14 Multiple EIGRP Domains with Static Routes



This design allows for end-to-end routing while completely isolating the routing processes in the Enterprise and Industrial Zones. This solution fits best when policy prevents running a routing protocol on the firewall or when the organizational structure has independent teams supporting routing and firewalls.

Protecting EIGRP

All routing protocols must be protected to prevent the distribution of faulty route information. The primary methods of protecting the integrity of the EIGRP routing table are:

- Passive interfaces
- Route authentication

By default, a router running the EIGRP routing protocol will attempt to establish a neighbor relationship with any routers on the local network. The risk that someone could introduce a rogue router and advertise false routes into the network exists. The *passive interface* command prevents the EIGRP process from establishing a neighbor relationship with any routers on the specified interface. This command is commonly used on LAN interfaces connecting to end devices.

The EIGRP protocol also supports route authentication. With route authentication, a shared key is configured on all routers. A router will only accept a route update from a neighbor that signed the update using a MD5 hash that includes the shared key.

OSPF Overview

The Open Shortest Path First (OSPF) routing protocol is an open standard protocol defined in IETF RFC 2328. The OSPF is an Interior Gateway Protocol used to distribute routing information within a single AS. OSPF uses Dijkstra's Shortest Path First algorithm in order to build and calculate the shortest path to all known destinations. OSPF is a link state protocol which means that each router must maintain a database of the state of each routed link in the network.

To reduce the overhead of the protocol, OSPF divides the network into multiple areas. Area 0 is the backbone of the network and all other areas must directly connect to the Area 0 through Area Border Routers (ABR). Dividing the routing protocol into multiple areas reduces the CPU and memory required to maintain the link state database.

Some of the many advantages of OSPF are:

- Open standard defined by the Internet Engineering Task Force (IETF)
- Multi-area design that reduces CPU and memory requirements on individual routers
- Link-state design for fast convergence



Note

More information about OSPF can be found in *OSPF Design Guide* at:

- <http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>

OSPF Design

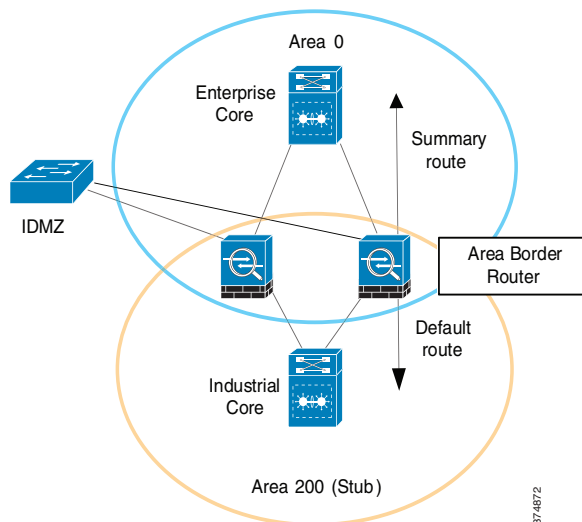
This section contains OSPF design options and considerations, such as scalability, routing policy and configuration complexity.

Single OSPF Domain

In the single OSPF domain design, Area 0 is contained in the Enterprise Zone. Each Industrial Zone is a new area in the OSPF network. The IDMZ firewalls function as the ABRs between the corporate backbone (Area 0) and the Industrial Zone area.

The Industrial Zone area should be configured as a Totally Stubby Area to reduce the overhead of routing within the zone. Optionally, the Industrial Zone area can be configured as a Stub Area or a Not-So-Stubby Area (NSSA) depending on the needs of the application. See [Figure 2-15](#).

Figure 2-15 Single OSPF Domain with Stub Areas



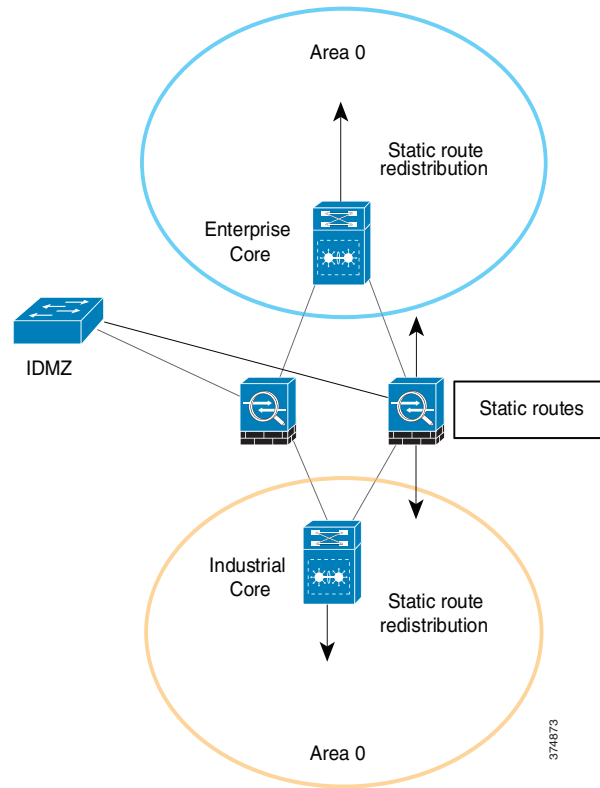
This design also allows for end-to-end routing between the Enterprise and Industrial Zones. OSPF naturally subdivides the routing protocol into areas. This solution fits best with medium-to-large networks and easily accommodates environments with multiple Industrial Zones.

Multiple OSPF Domains

This design treats the Enterprise and Industrial Zones as separate routing domains. Both zones have their own Area 0 backbone network. Because of this, the IDMZ firewalls do not run an instance of OSPF.

Static routes must be configured on the routers connected to the firewalls and the firewalls themselves to allow communications between the zones. The boundary routers must redistribute the static routes into the OSPF instance for the zone. See Figure 2-16.

Figure 2-16 Multiple OSPF Domains with Static Routes



This design allows for end-to-end routing between the Enterprise and Industrial Zones while completely segregating the routing processes in the zones. This solution fits best when policy prevents running a routing protocol on the firewall or when the organizational structure has independent teams supporting routing and firewalls.

Securing OSPF

OSPF supports route authentication to reduce the chance of malicious routes being added to the routing protocol. When route authentication is enabled, the OSPF router signs its route update with a shared key. The neighboring router will only accept route updates that are signed with the correct key.

By default, OSPF sends the authentication information in clear text. It is important to use type 2 authentication which uses an MD5 hash for authentication.

Selecting Routing Design

Table 2-4 summarizes features of the different design options for EIGRP and OSPF protocols. The main criteria for selecting the appropriate design should be the network size, configuration complexity and IT policies. Often, the existing enterprise network design determines the routing configuration in the Industrial Zone.

Table 2-4 Routing Design Selection Criteria

Routing Design	Network Size			Network Policy			Complexity		
	Small	Medium	Large	Routing Protocol on Firewall	Single Administrative Domain	Subdivides Routing Processes	Low	Medium	High
Single EIGRP domain	X	X		X	X		X		
Multiple EIGRP domains (redistribution)		X	X	X		X		X	
Multiple EIGRP domains (static routes)		X	X			X			X
Single OSPF domain		X	X	X		X		X	
Multiple OSPF domains		X	X			X			X

IDMZ Design for Network Services

In a converged IACS network, Industrial and Enterprise Zones can share certain network services to reduce cost of deployment and support and to be able to use same IT management resources. From a security perspective, user authentication and authorization policies have to be managed and applied throughout the whole infrastructure.

These services use network protocols to enable data replication and configuration synchronization across the IDMZ. Design considerations for the following network services are reviewed in this section:

- Active Directory Services
- Certificate Services
- Network Time Protocol (NTP)
- Identity Services
- Multi-Factor Authentication (MFA)
- Licensing
- Windows Updates

Active Directory Services

Microsoft Active Directory (AD) services play an essential role in managing, authenticating and authorizing users and network assets in an enterprise. Companies need a central repository of information about people and their access rights that apply to both the Industrial and Enterprise Zones. AD services in the Industrial Zone should be designed to allow secure replication of information across the IDMZ while being able to operate independently if necessary.

The following sections describe AD and provide design recommendations for the CPwE IDMZ.

Active Directory Overview

Active Directory Domain Services (AD DS) provides a distributed database of information about network resources and application data. AD DS organize network elements, such as users, computers and other devices, into a hierarchical structure that includes the Active Directory forest, domains in the forest, and organizational units (OUs) in each domain. A server that is running AD DS is called a Domain Controller (DC).

- A **forest** acts as a security boundary for an organization and defines the scope of authority for administrators. By default, a forest contains a single domain, which is known as the forest root domain.
- A **domain** is a logical group of network objects (computers, users, devices) that share the same AD database. An AD domain supports a number of core functions including network-wide user identity, authentication, and trust relationships.

Additional domains can be created in the forest to provide partitioning of AD DS data. Multiple domain structure can be used to control data replication and to scale globally over a network with limited bandwidth.

- **OUs** simplify the management of large numbers of objects by the delegation of full or limited authority to other users or groups. OUs are used more often than domains to provide structure and to simplify the implementation of policies and administration.

AD DS implements security with a logon authentication and access control to resources in the directory. Authorized network users and administrators can use a single network logon to access resources anywhere in the network. Policy-based administration allows simplifying management of even the most complex network.

Additional AD DS features include the following:

- A **schema** is the set of rules that defines the classes of objects and attributes that are contained in the directory, the name format and the constraints for these objects.
- A **global catalog** that contains information about every object in the directory. Users and administrators can use the global catalog to find directory information, regardless of which domain in the directory actually contains the data.
- A **replication service** that distributes directory data across a network. Any change to directory data is replicated to all DCs in the domain.
- **Operations master roles** (also known as Flexible Single Master Operations or FSMO) on designated DCs to perform specific tasks to confirm consistency and eliminate conflicting entries in the directory.
- **Active Directory Federation Services (AD FS)** can be deployed to manage access to protected resources for trusted partners including external third parties or other departments or subsidiaries in the same organization.

**Note**

For information about AD DS, refer to *Active Directory Domain Services* at:

- <https://technet.microsoft.com/en-us/windowsserver/dd448614>

Active Directory Architecture in IDMZ

This section provides design recommendations for the AD DS in the CPwE IDMZ architecture.

AD DS Deployment Model

The tested and validated deployment of the AD DS in the CPwE architecture is based on the AD implementation in a single domain with multiple sites.

A single AD domain for the Enterprise and Industrial Zones allows maintaining a single identity and access policy repository for all employees in a company. This approach can bring many benefits for the CPwE architecture, for example, secure remote access to the Industrial Zone from the enterprise.

The first domain controller you install automatically creates the first site, known as the Default-First-Site-Name. After installing the first domain controller, all additional domain controllers are automatically added to the same site as the original domain controller. The Enterprise Zone and IDMZ can be part of the Default-First site.

To deploy the CPwE architecture topology, the addition of an Active Directory Domain Controller (AD DC) in the Industrial Zone is required. The Industrial Zone is placed in its own AD site. Establishing separate sites for the Industrial and Enterprise Zones provides the following benefits:

- Efficient use of bandwidth for replication in case of WAN connectivity
- Detailed control of replication behavior, for example schedule
- Industrial assets can authenticate to the local DC

**Note**

AD DS should be installed in accordance with Microsoft best practices and deployment guidelines provided in *Deploy Active Directory Domain Services (AD DS) in Your Enterprise* at:

- <https://technet.microsoft.com/en-us/library/hh472160.aspx>

Active Directory Replication

The CPwE IDMZ architecture for AD implements bi-directional replication between the Enterprise DC and the Industrial Zone DC. An AD administrator should be able to create, delete and update accounts in the Industrial Zone and the changes will be replicated to the Enterprise Zone and vice versa.

Companies may also choose one-directional replication (Enterprise DC to Industrial DC only) due to security policies and management practices.

Site-to-site replication data can be compressed and sent on a schedule, depending on the available network bandwidth and requirements. The synchronous (scheduled) replication between sites is based on the Microsoft implementation of Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) over TCP/IP.

**Note**

For information about Active Directory replication, refer to the following resources:

- *How Active Directory Replication Works*
 - <http://social.technet.microsoft.com/wiki/contents/articles/4592.how-active-directory-replication-works.aspx>
- *Active Directory Replication Technologies*
 - <https://technet.microsoft.com/en-us/library/cc776877%28v=ws.10%29.aspx>

Firewall Design for AD Replication

Remote Procedure Call (RPC) dynamic port allocation is used by many server applications. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP, based on the implementation.

Some AD DS rely on Microsoft Distributed Component Object Model (DCOM) RPC for service replication. The default dynamic port range varies depending on the Windows platform (for example, 1025-5000 for Windows Server 2003 and 49152-65535 for Windows Server 2008), while the Cisco ASA used pinholing to limit the number of open ports across the firewall. Getting replication to function properly across security perimeters can be challenging. Three possible approaches exist:

- Open up the firewall to permit RPC's native dynamic behavior.
- Limit RPC's use of TCP ports and open the firewall for a small range of ports.
- Encapsulate the DC-to-DC traffic inside IP Security Protocol (IPsec) and open the firewall for the IPsec only between the DCs.

Cisco FTD uses application detectors to identify the commonly used applications in your network. These application detectors can then be used in access control rules, to provide a granular method of handling network traffic cross multiple managed devices, enabling simple rule creation for AD replication.

Specific to DEC/RPCC, Cisco FTD provides a preprocessor which normalizes the packet data into formats that the intrusion rules engine can analyze, enabling traffic to not only be policed by the access control rule, but for potential exploits to be detected through the IPS engine. More information regarding the DEC/RPC preprocessor in Cisco FTD can be found at:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/application_layer_preprocessors.html#ID-2244-00000019

More details of the DEC/RPC operations are listed below:

- An RPC service configures itself in the registry with a universally unique identifier (UUID). UUIDs are well-known identifiers unique for each service and common across all platforms.
- When an RPC service starts, it obtains a free high port and registers that port with the UUID. Some services use random high ports; others try to use the same high ports all the time (if they are available). The port assignment is static for the lifetime of the service.
- Once the service restarts with a new process or network server reload, the port assignment changes. This makes it impossible to know in advance which port an RPC service will use. The DEC/RPC inspection monitors the communication between the Endpoint Mapper (EPM) on a server and a client on the well-known TCP port 135. The embedded server IP address and port number are received from the EPM response messages.

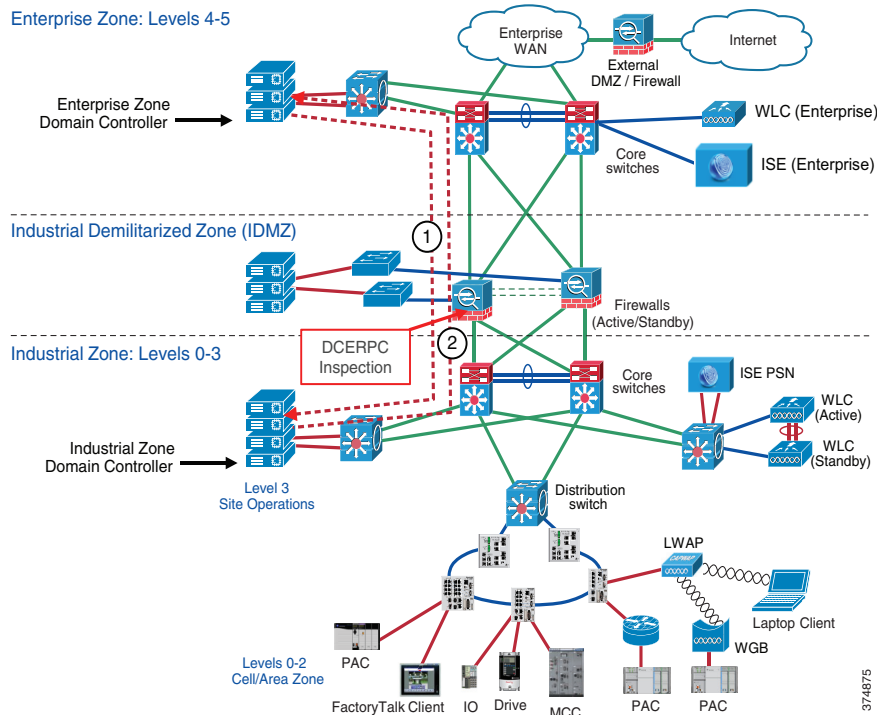
**Note**

For detailed information, refer to *Active Directory and Active Directory Domain Services Port Requirements* at:

- <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements>

Figure 2-17 illustrates the AD replication between the DCs in the Industrial and Enterprise Zones.

Figure 2-17 Domain Controller Bi-Directional Replication



1. The Enterprise Domain Controller replicates any changes to the Industrial Zone Domain Controller using the RPC protocol. The firewall inspects the RPC traffic and dynamically opens necessary ports.
2. The Industrial Domain Controller replicates any changes to the Enterprise Zone Domain Controller. The firewall inspects the RPC traffic and dynamically opens necessary ports.

In addition to RPC, other ports may need to be opened between the DCs, depending on the implementation. [Table 2-5](#) shows an example of protocols that may be required for AD replication. Note that this may not be a complete list depending on the AD configuration and the requirements.

Table 2-5 AD Replication Ports Example

Protocol / Service Name	TCP/UDP Port
SMB over IP	TCP 445
Kerberos	TCP/UDP 88
LDAP, LDAP SSL	TCP/UDP 389, 636
LDAP GC, LDAP GC SSL	TCP/UDP 3268, 3269
RPC	TCP/UDP 135

Authentication of IDMZ Resources

IDMZ hosts that belong to the AD domain have to authenticate to the Enterprise DC. Examples of such hosts include Terminal Services Gateway, anti-virus and Windows Update servers. To achieve this, the firewall access policy should allow certain protocols between the IDMZ and the Enterprise Zone. The policy should be restricted to specific IP addresses in the IDMZ that require authentication. The dynamic RPC inspection should also be included in the policy (see [Active Directory Replication](#), page 2-30).

Table 2-6 shows an example of protocols that may be required for AD authentication. Note that this may not be a complete list depending on the AD configuration and the requirements.

Table 2-6 AD Authentication Ports Example

Protocol / Service Name	TCP/UDP Port
SMB over IP	TCP 445
Kerberos	TCP/UDP 88, 464
LDAP, LDAP SSL	TCP/UDP 389, 636
DNS	TCP/UDP 53
RPC	TCP/UDP 135



Note

More information on AD port requirements can be found in *Active Directory and Active Directory Domain Services Port Requirements* at:

- <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements>

Certificate Services

This section provides an overview of certificate services and public key infrastructure (PKI).



Note

CPwE IDMZ does not cover PKI in depth nor does it recommend how to properly implement or manage PKI. For test purposes, firewalls and other devices using self-signed certificates as PKI management were beyond the scope of this CPwE DIG.

Certificate Services Overview

The Certificate Authority (CA) is a trusted entity that manages and issues security certificates and public keys that are used for secure communication in a public network. The CA is part of the PKI along with the Registration Authority (RA) who verifies the information provided by a requester of a digital certificate. If the information is verified as correct, the certificate authority can then issue a certificate.

PKI is a scalable architecture that includes software, hardware and procedures to facilitate the management of digital certificates. Certificate-based authentication methods can be required for:

- User network access, both wired and wireless
- Authentication of network devices, for example servers and wireless APs

Access Point (AP) Certificate Services can also be used to:

- Enroll users for certificates from the CA using the Web or the Certificates Microsoft Management Console (MMC) snap-in, or transparently through auto enrollment
- Use certificate templates to help simplify the choices a certificate requester has to make when requesting a certificate, depending upon the policy used by the CA
- Take advantage of the AD service for publishing trusted root certificates, publishing issued certificates, and publishing Certificate Revocation Lists (CRLs)
- Implement the ability to log on to a Windows operating system domain using a smart card

**Note**

For more information about AD Certificate Services, refer to *Active Directory Certificate Services* at:

- <https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx>

Certificate Authority Hierarchy

PKI supports a hierarchical structure with various CA roles in the network, depending on the scale of the system.

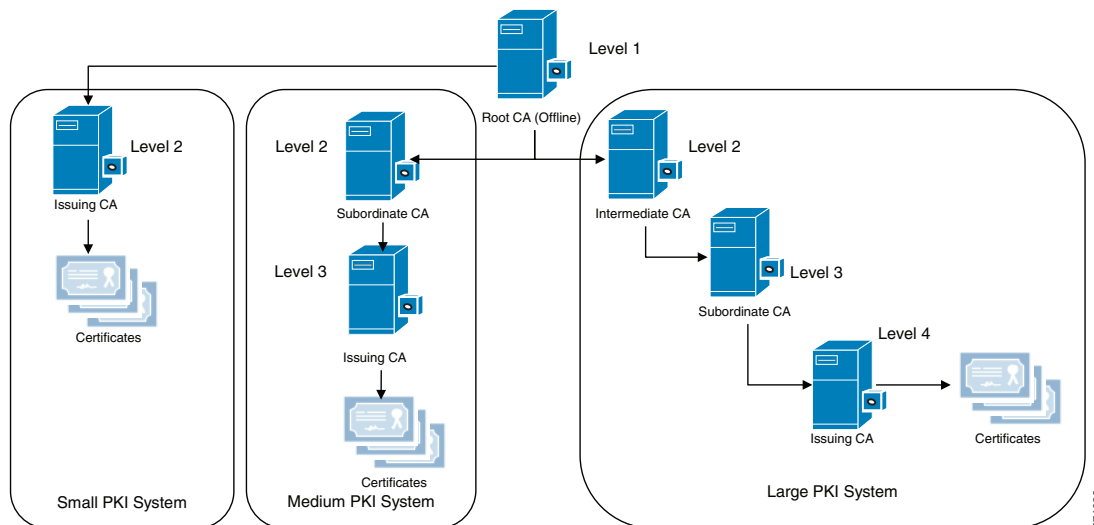
- Root CA is the most trusted CA in a CA hierarchy and is the first CA installed in the network. When a root CA remains online, it is used to issue certificates to the intermediate and subordinate CAs. Most times, the root CA remains offline to protect the private keys. The root CA rarely issues certificates directly to users, computers or services.
- Intermediate CAs are the next in hierarchy after the root CA. The intermediate CA issues certificates only to subordinate CAs.
- Subordinate CAs can be used to issue certificates to users and computers, or to issuing CAs.
- Issuing CA is used to issue certificates directly to users and computers.

AD Certificate Services can be deployed into Enterprise CA and stand-alone CA modes depend on the customer specific requirements:

- Enterprise CA is integrated with AD and use domain services for certificate management. Enterprise CAs are typically used for issuing user and computer certificates.
- Stand-alone CA is not dependent on AD and not part of a domain. A stand-alone mode is often used to implement a secure offline root CA.

Figure 2-18 shows the CA hierarchy and various deployment models depending on the system scale.

Figure 2-18 PKI Infrastructure Models Example



374923

Certificate Services Architecture in IDMZ

Similar to AD DS service, the deployment of the Active Directory Certificate Services (AD CS) in the CPwE architecture is based on the AD implementation in a single domain. To provide a local CA for each Industrial Zone, the root CA should be configured in the Enterprise Zone, with a subordinate CA in the secured Industrial Zone.

Enterprise Zone root and subordinate CAs will have full-fledged functionalities to provide the following services:

- **Certification Authorities (CAs)**—Root, intermediate, subordinate and issuing CAs are used to issue certificates to users, computers, and services, and to manage certificate validity.
- **CA Web Enrollment**—Web enrollment allows users to connect to a CA by means of a Web browser in order to request certificates and retrieve CRLs.
- **Online Responder**—The Online Responder service accepts revocation status requests for specific certificates, evaluates the status of these certificates, and sends back a signed response containing the requested certificate status information.
- **Network Device Enrollment Service**—The Network Device Enrollment Service allows routers and other network devices that do not have domain accounts to obtain certificates.
- **Certificate Enrollment Web Service**—The Certificate Enrollment Web Service enables users and computers to perform certificate enrollment that uses the HTTPS protocol. Together with the Certificate Enrollment Policy Web Service, this enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain.
- **Certificate Enrollment Policy Web Service**—The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information. Together with the Certificate Enrollment Web Service, this enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain.

Subordinate CA behind the IDMZ firewall is responsible for issuing and validating client's **Certificate Signing Request (CSR)** and authentication requests inside the Industrial Zone. Issuing certificates to users or devices inside an Industrial Zone, instead of forwarding all requests to Enterprise Zone Root-CA, allows certificate services to operate in case of incidents when the enterprise CA is not available.

Multiple Subordinate CAs inside the Industrial Zone can also achieve plant-wide smooth operation during a failure of any single subordinate CA.

Network Time Protocol

Time synchronization is a critical requirement in most industrial systems. Network Time Protocol (NTP) is one of the most common protocols governing time transfer in computer networks. The following sections present recommendations and considerations for deploying NTP in the CPwE IDMZ architecture.

NTP Overview

Network Time Protocol (NTP) version 4 is an IETF standard defined in RFC 5905. NTP uses a hierarchy of clocks with each level referred to as a stratum. This hierarchy begins at stratum 0, which is the primary reference clock.

- The primary reference clock (stratum 0) synchronizes to Coordinated Universal Time (UTC) using a GPS, radio, or atomic clock.
- Stratum 1 clocks synchronize directly with the reference clock and are the first clocks connected to the network.

- Stratum 2 clocks will synchronize against multiple stratum 1 clocks. Stratum 3 clocks will synchronize with multiple stratum 2 clocks and so on.

An NTP-enabled device never synchronizes to a device that is not synchronized itself. Additionally, an NTP-enabled device compares the time reported by several NTP devices, and will not synchronize to a device whose time is significantly different than others.

In general, a lower stratum will have higher precision and accuracy than a higher stratum clock. However, the quality of the components used in the NTP servers has a large impact on the accuracy and precision of time. For example, the stratum 4 server that is part of a hierarchy with high quality clocks and well performing networks may have a higher precision and accuracy than a stratum 3 server that uses poor quality clocks and networks in the hierarchy.

No more than one NTP transaction per minute is necessary to achieve 1 millisecond synchronization on a high-speed LAN. For larger systems (wide-area networks), NTP can routinely achieve 10 millisecond synchronization. However, the level of synchronization is not guaranteed and can be affected by the infrastructure. Asymmetric routes and network congestion can cause errors of 100 ms or more.

Windows Time Service Overview

Microsoft Windows clients and servers use the Windows Time Service (W32Time) to synchronize time across the domain. By default, W32Time uses a combination of AD and NTP to propagate time throughout the domain hierarchy. While AD uses a multi-master model for directory updates, some updates must happen using a single master model or FSMO roles.

One of the key FSMO roles in an AD domain is the Primary Domain Controller (PDC) emulator. In the Windows Time Service model, the Domain Controller that holds the PDC emulator role acts as the master time source for the domain. The PDC emulator should synchronize its clock to at least two reliable NTP sources.

The other domain controllers in the domain synchronize their clocks to the PDC emulator. In addition, the Windows clients synchronize their clocks to the local domain controller.



Note

It is important to understand that the W32Time service has limited accuracy and precision. It cannot reliably maintain time synchronization to more than a few seconds.

NTP Architecture in IDMZ

Various applications within the Industrial Zone use NTP for clock synchronization, for example:

- AD uses Kerberos protocol for authentication within the domain. Kerberos authentication uses timestamps to prevent replay attacks. By default, authentication request will fail if the client and server clocks differ by more than 5 minutes.
- Infrastructure devices such as routers, switches, and firewalls should synchronize their clocks via NTP. Many of these devices do not have onboard real-time clocks and will revert to a default date and time after a reboot. Devices such as these log critical event data to an internal or external syslog. Proper time stamps on these log entries are important for identifying and resolving faults in the device. Furthermore, synchronized clocks allow for system wide fault analysis involving multiple infrastructure devices.



Note

NTP and especially W32Time are not appropriate for high precision applications such as CIP Motion™ and Sequence of Events (SOE) applications using FactoryTalk Alarms and Events. These applications must use IEEE 1588 Precision Time Protocol (PTP) sourced from a reliable reference clock.

NTP Server Choice

The Enterprise Zone should have two reliable NTP servers that serve time for the enterprise systems. The enterprise time servers should synchronize to privately owned reference clocks to provide the most accurate and precise time. GPS time servers, which are relatively inexpensive, are a good choice for enterprise reference clocks. These clocks can be backed up by public time servers available on the Internet. However, public Internet time servers may not be reliable enough to be the sole primary reference for systems where accurate and precise time is critical.

The Industrial Zone should also have two reliable NTP servers. In medium precision applications, the industrial time servers can sync directly with the enterprise servers. However, consider deploying reference clocks in the Industrial Zone if high precision timestamps are required for the application. A number of vendors sell reference clocks that function as a NTP stratum 1 clock as well as a PTP grandmaster clock for CIP Sync and CIP Motion applications.

NTP Synchronization through IDMZ

Because of the critical role that time synchronization plays in most networks, NTP is one of the few protocols that directly traverse from the Enterprise Zone to the Industrial Zone. The Industrial Zone NTP servers should be allowed to communicate directly with the Enterprise NTP servers on UDP port 123. NTP servers should use NTP authentication to validate the identity of the source clock during synchronization. In addition, the IPS/IDS in the firewall should inspect the integrity of NTP traffic passing through.

AD domain controllers also need to synchronize using the NTP protocol. The synchronization rules will vary depending on the domain structure. In the single domain model, the domain controllers need visibility to the PDC emulator. In a multi-domain model, the domain controllers need visibility to the PDC emulator or a domain controller in the parent domain.

<https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-top>

**Note**

For more information on the Windows Time Service, refer to *Windows Time Service Technical Reference* at:

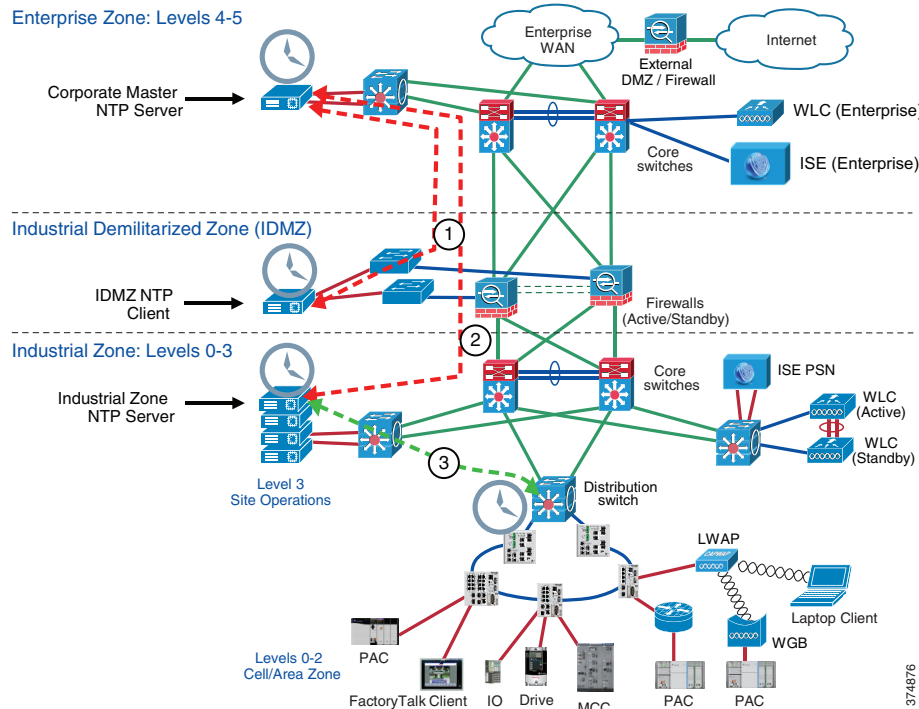
- <https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-top>

Figure 2-19 illustrates NTP data traversal across the IDMZ between NTP servers in different zones. In this example, the NTP server in the Enterprise Zone can be a corporate time source (stratum 1 or stratum 2) or a PDC emulator in the AD domain. The NTP server in the Industrial Zone can also be a domain controller that synchronizes to the PDC.

**Note**

Depending on the requirements, the Industrial Zone may have its own reference clock for NTP synchronization, such as a GPS clock.

Figure 2-19 NTP Synchronization across IDMZ



1. The NTP client in the IDMZ synchronizes time with the corporate Master NTP server in the Enterprise Zone.
2. The NTP server in the Industrial Zone synchronizes time with the corporate Master NTP server in the Enterprise Zone.
3. Industrial NTP clients synchronize their clocks with the Industrial NTP server.

Recommendations and considerations for the NTP deployment in the CPwE IDMZ architectures are summarized as follows:

- Deploy reference clocks (stratum 1) in the Enterprise Zone and Industrial Zone as needed.
- Use public NTP servers as a backup to private reference clocks.
- NTP servers should sync to at least two reliable clocks at a lower stratum.
- Synchronize the W32Time clock on the PDC Emulator to at least two reliable NTP servers.
- Be aware of limited accuracy and precision of the W32Time.
- Configure NTP authentication and inspect NTP traffic on the firewall.

Identity Services Engine

This section provides an overview of the distributed Cisco Identity Services Engine (ISE) architecture in the CPwE IDMZ.



Note

For more information about ISE deployment in the CPwE, refer to the *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at:

- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

ISE Overview

With the introduction of secure employee and contractor access, the use of the Cisco ISE as an identity and access control policy platform enables organizations to enforce compliance, enhance infrastructure security and streamline their service operations. The ISE architecture allows an organization to gather real-time contextual information from the network, users and devices to make proactive policy decisions by tying identity into various network elements including access switches and WLCs.

The ISE functions as the authentication and authorization server for the wired and wireless networks using RADIUS protocol. The ISE can use AD as an external identity database for resources such as users, machines, groups and attributes. Cisco ISE supports Microsoft AD Sites and Services when integrated with AD. ISE needs an identity certificate that is signed by a CA server so that it can be trusted by endpoints, gateways and servers.

Distributed ISE Architecture

In the distributed ISE architecture, multiple ISE nodes assume different roles (personas) in the network:

- **Policy Administration Node (PAN)** persona allows the Enterprise IT team to perform all administrative operations on the ISE system. The PAN handles all system-related configurations that are related to functionality such as authentication and authorization. An architecture can have one or a maximum of two PANs that can have the standalone, primary or secondary role.
- **Policy Service Node (PSN)** persona provides network access, plant personnel and guest access and client provisioning and profiling services. This persona evaluates the policies and provides network access to computers based on the result of the policy evaluation. More than one node can assume this persona and typically more than one PSN exists in a large distributed deployment.
- **Monitoring ‘n Troubleshooting (MnT) Node** persona functions as the log collector and stores log messages from all PANs and PSNs in a network. This persona provides advanced monitoring and troubleshooting tools that the Enterprise IT team can use to effectively manage a network and resources. A maximum of two MnTs can take on primary or secondary roles for high availability. At least one node in a distributed setup should assume the Monitoring persona. For optimum performance, an MnT persona should not be enabled on the same node as PSN or PAN and should be dedicated solely to monitoring.

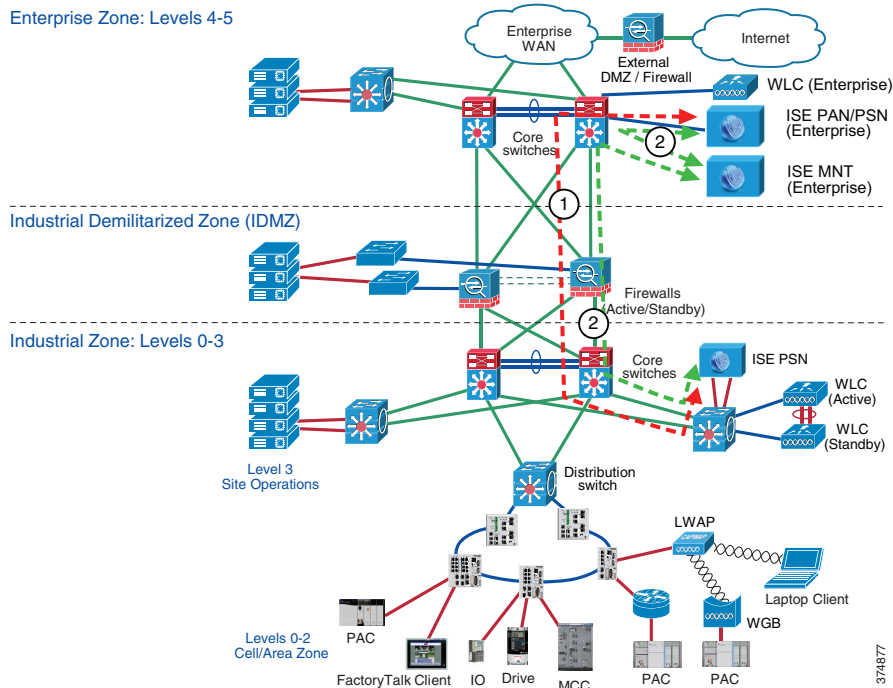
ISE Architecture in IDMZ

Within the CPwE IDMZ architecture, the recommendation is to deploy the Cisco ISE platform as a distributed solution (see [Figure 2-20](#)).

- The corporate IT department maintains the management of the ISE platform via PAN in the Enterprise Zone. The MnT is also deployed in the Enterprise Zone.
- One or multiple PSNs are deployed in the Industrial Zone for identity services. The PAN synchronizes its policy configurations with PSNs.
- The IDMZ firewall is configured to allow ISE synchronization and logging traffic between the nodes (see [ISE Configuration, page 3-14](#) for details).

Figure 2-20 Distributed ISE Architecture

Enterprise Zone: Levels 4-5



1. The Enterprise ISE PAN/PSN synchronizes its policy configurations with the Industrial ISE PSN.
2. The Enterprise and Industrial ISE PSNs send detailed logs to the Enterprise ISE MNT.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a security process that requires users to respond to requests to verify their identities before they can access networks or other online applications. MFA may use knowledge, possession of physical objects, or geographic or network locations to confirm identity.

MFA Overview

Authentication based on usernames and passwords alone is unreliable and unwieldy, since users may have trouble storing, remembering, and managing them across multiple accounts, and many reuse passwords across services and create passwords that lack complexity. Passwords also offer weak security because of the ease of acquiring them through hacking, phishing, and malware.

MFA requires means of verification that unauthorized users won't have. Since passwords are insufficient for verifying identity, MFA requires multiple pieces of evidence to verify identity. The most common variant of MFA is two-factor authentication (2FA). The theory is that even if threat actors can impersonate a user with one piece of evidence, they will not be able to provide two or more.

Proper multi-factor authentication uses factors from at least two different categories. Using two from the same category does not fulfill the objective of MFA. Despite wide use of the password/security question combination, both factors are from the knowledge category--and don't qualify as MFA. A password and a temporary passcode qualify because the passcode is a possession factor, verifying ownership of a specific email account or mobile device.

Processes vary among the different MFA methods, but a typical 2FA transaction happens like this:

- The user logs in to the website or service with their username and password.
- The password is validated by an authentication server and, if correct, the user becomes eligible for the second factor.
- The authentication server sends a unique code to the user's second-factor method (such as a smartphone app).
- The user confirms their identity by providing the additional authentication for their second-factor method.

In adaptive authentication, authentication rules continuously adjust based on the following variables:

- By user or groups of users defined by role, responsibility, or department
- By authentication method: for example, to authenticate users via push notification but not SMS
- By application: to enforce more secure MFA methods--such as push notification or Universal 2nd Factor (U2F)--for high-risk applications and services
- By geographic location: to restrict access to company resources based on a user's physical location, or to set conditional policies restricting use of certain authentication methods in some locations but not others
- By network information: to use network-in-use IP information as an authentication factor and to block authentication attempts from anonymous networks like Tor, proxies, and VPNs

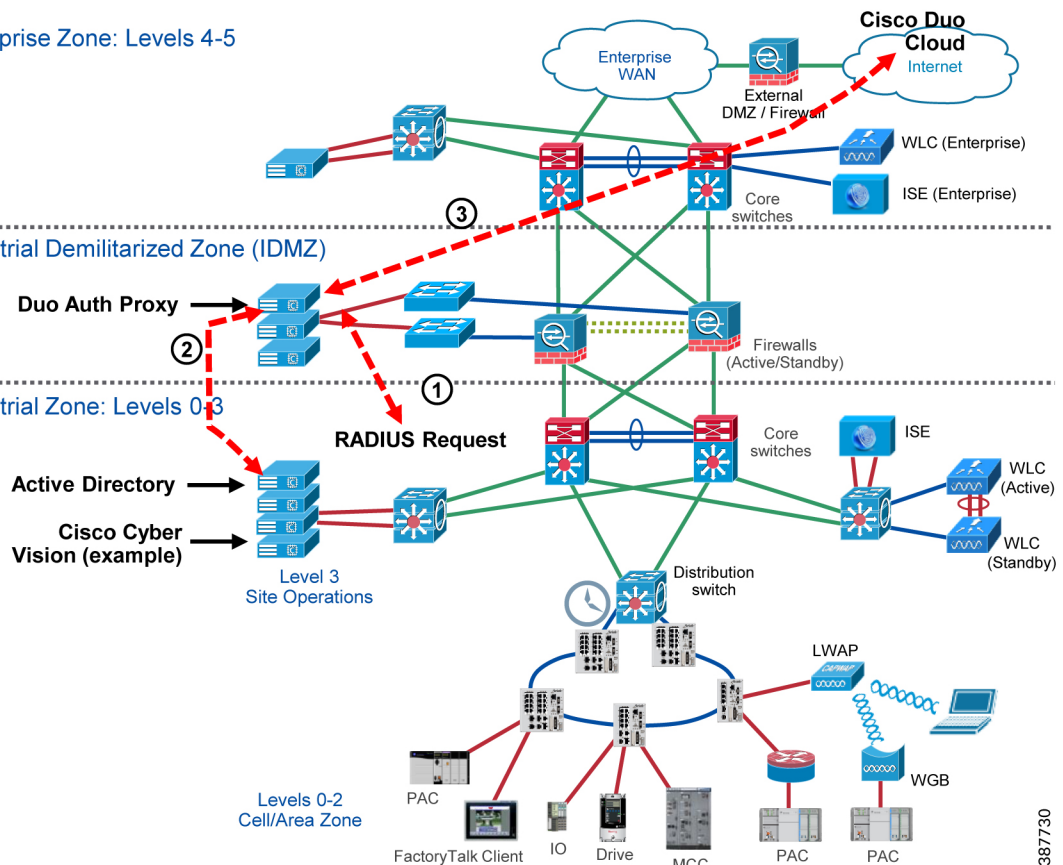
Multi-Factor Authentication Architecture in IDMZ

Figure 2-21 Cisco Secure Access by Duo IDMZ Architecture

Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone: Levels 0-3



Multi-factor authentication from Cisco's Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Many of Duo's application integrations do not require any local components. However, certain services do require a local Authentication Proxy service. This document makes use of the Duo Authentication Proxy for:

- Remote Access VPN
- Microsoft Remote Desktop Gateway
- Windows Logon and RDP

Duo's Authentication Proxy (sometimes referred to as the Authproxy) is a local service needed to properly configure certain Duo-protected applications. The Authentication Proxy can be installed on a physical or virtual host, on Windows or Linux machines. Once configured, Duo sends your users an automatic authentication request via Duo Push notification to a mobile device or phone call after successful primary login.

1. RADIUS Request is sent to Duo Authentication Proxy.
2. Duo Authentication proxy validates primary credentials with Active Directory.
3. Duo Authentication proxy, if credentials were valid, prompts the Duo cloud to send 2FA.
4. Duo Authentication proxy returns accept or deny response back to the application.

Licensing

Cisco Smart Licensing is a flexible software licensing method that simplifies the way you activate and manage licenses across your organization. With Smart Licensing, a pool of licenses is associated to a Cisco Smart Account. Like banking, new licenses are automatically deposited into your Smart Account, increasing your account balance of licenses (also known as entitlements). As licenses expire or are terminated, your inventory balance decreases.

Cisco Smart Software Manager On-Prem Overview

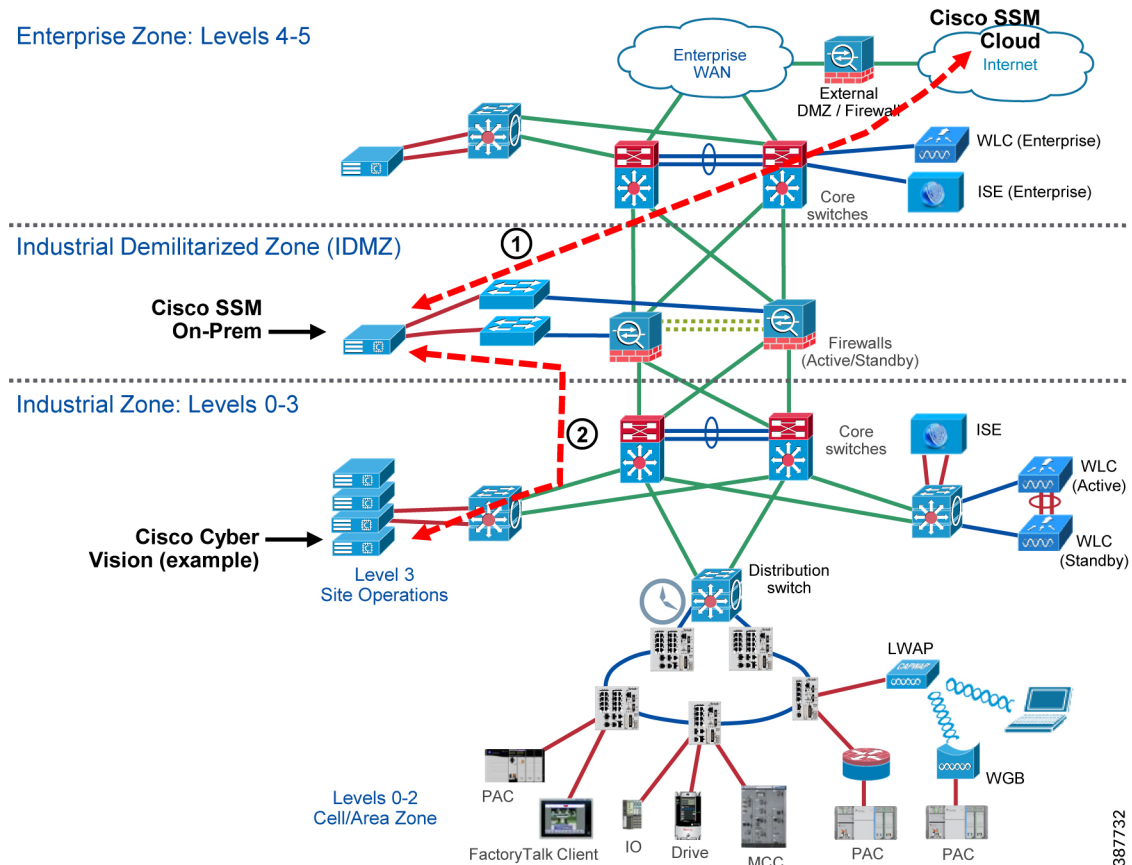
Cisco Smart Software Manager (SSM) On-Prem license server is a component of Cisco Smart Licensing. It works in conjunction with Cisco Smart Software Manager to intelligently manage customer product licenses, providing near-real-time visibility and reporting of the Cisco licenses that customers purchase and consume.

Cisco Smart Licensing requires products to be associated with Smart Accounts, which can be created on Cisco Software Central. A Smart Account is associated with a unique company ID and is like an online banking account containing Cisco entitlements and devices for that customer. From the Cisco Smart Software Manager, subaccounts (also called virtual accounts) can be created to represent various subdivisions or buying centers of the company.

Cisco SSM On-Prem is targeted for security-sensitive customers who are unable to manage their installed base with a direct Internet connection. For devices and applications in the industrial zone, the Cisco SSM On-Prem provides a mechanism to provide local control and management of their license usage, without the need for manual intervention.

Cisco Smart Software Manager On-Prem IDMZ Architecture

Figure 2-22 Cisco Smart Software Manager On-Prem IDMZ Architecture



1. Cisco SSM On-Prem is installed in the IDMZ.
2. If the Cisco SSM is in networking mode, it will continually synchronize with Cisco Smart Licensing cloud.
3. Products in the Industrial Zone request license reservation from the Cisco SSM On-Prem server.
4. Cisco SSM On-Prem server returns valid licenses to products in the Industrial Zone.

Windows Updates

Update management is the process of controlling the deployment and maintenance of interim software releases into production environments. Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services Server Role Description

A WSUS server provides features that you can use to manage and distribute updates through a management console. A WSUS server can also be the update source for other WSUS servers within the organization. The WSUS server that acts as an update source is called an upstream server. In a WSUS implementation, at least one WSUS server on your network must be able to connect to Microsoft Update to get available update information.

Windows Server Update Services IDMZ Architecture

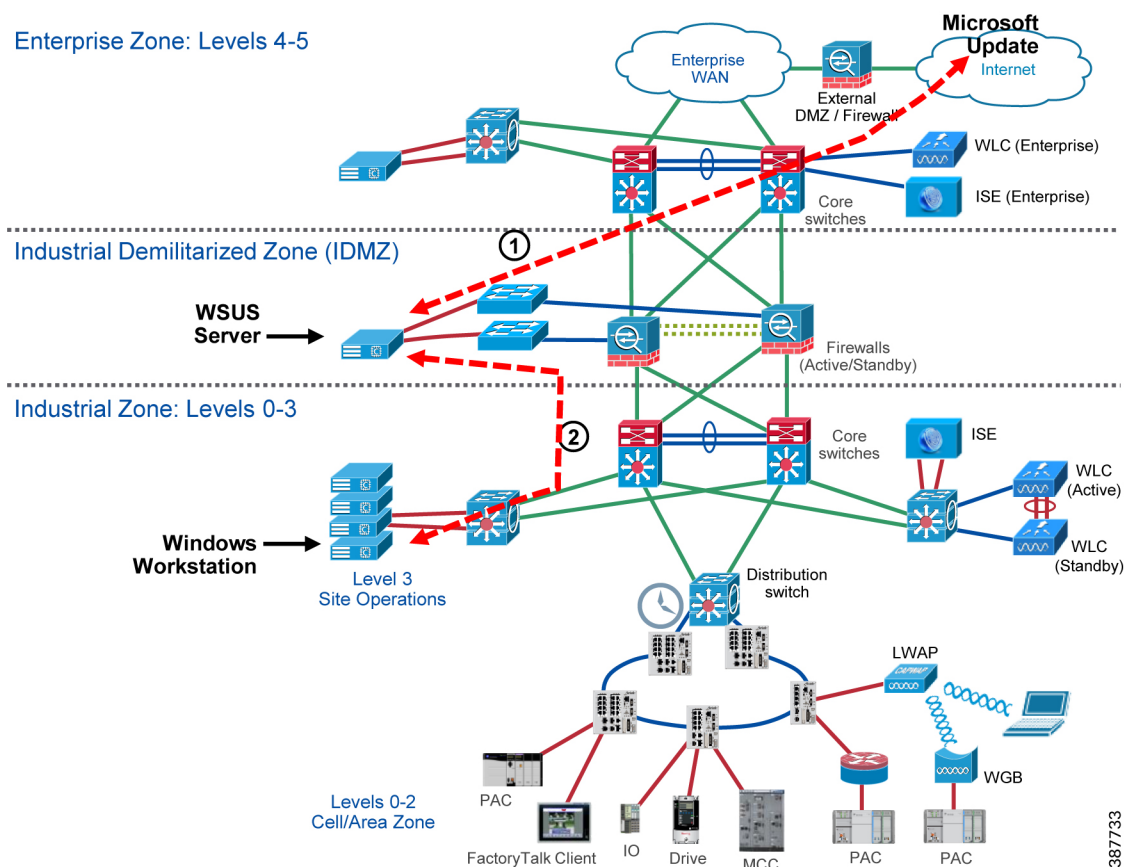
For this design, the WSUS server role will be deployed in the IDMZ and connect directly to Microsoft Update for periodic update checks. All Windows devices in the Industrial Zone will connect to the WSUS for updates.



Note

It is recommended that automatic updates are not enabled so that updates are not immediately installed. Updates should be installed during scheduled maintenance windows to reduce downtime.

Figure 2-23 Windows Server Update Services IDMZ Architecture



1. WSUS server role is installed on Windows Server in the IDMZ.
2. WSUS server is configured to use web proxy to pull Microsoft updates from the cloud.
3. Create computer groups to add client computers for update services.

4. Clients in the Industrial Zone will check the WSUS server for updates periodically. Updates can be installed locally on the client, but should not be automatically installed so changes can be approved by an administrator.

Data Transfer through the IDMZ

The key principle of the IDMZ is to meet the requirement to share necessary IACS data between the Industrial and Enterprise Zones while not allowing direct communication between the zones. This goal is achieved by placing gateways, application data mirrors, proxy servers and similar services in the IDMZ.

Two application examples in this section demonstrate how data can be transferred through the IDMZ in a secure way:

- FactoryTalk Historian data transfer
- Secure file transfer with Cisco Advanced Malware Protection

FactoryTalk Historian Data Transfer

Access to process and operational data is often a key requirement for setting up an industrial network. This data can, among other purposes, visualize process and production progress, identify improvement opportunities and assist in troubleshooting.

FactoryTalk Historian establishes a reliable foundation for capturing this data. The suite of software products can target a single machine (FactoryTalk Historian Machine Edition) or be a plant-wide system (FactoryTalk Historian Site Edition). It can also be extended across the global enterprise using the Rockwell Automation Global Enterprise Historian Strategy.

With FactoryTalk Historian Site Edition (SE), you can collect critical time-series data for various calculations, estimations, and statistical processes producing information to benefit a multitude of enterprise-wide processes and applications. An overview of the FactoryTalk Historian SE operation is provided below:

- At its core, FactoryTalk Historian Site Edition stores user defined data (tag + value pairs) into an archiving system on the FactoryTalk Historian SE server. A FactoryTalk VantagePoint client can access this data. These archives can also be queried through a specialized OLEDB connection (PI OLEDB) by means of a SQL query language like T-SQL.
- The data gets collected from PACs in the Industrial Zone through instances of RSLinx Enterprise and FactoryTalk[®] Linx running on separate servers. These servers have FactoryTalk[®] Live Data interfaces installed that relay the data collected by RSLinx to the FactoryTalk Historian SE server.
- It is best practice to install the FactoryTalk Historian SE server and two independent FactoryTalk[®] Live Data interfaces on separate physical or virtual server hardware for a more robust and redundant system.
- The FactoryTalk Historian SE server can be made part of a collective for even better redundancy.



Note

For more information on FactoryTalk Historian, refer to:

- <http://www.rockwellautomation.com/rockwellsoftware/products/factorytalk-historian.page?>

Application Requirements

In the Industrial Zone, FactoryTalk® Historian SE server functions as data (archives) repository, central point for data queries, coordinator for FactoryTalk® Live Data interfaces and access point for system setup and maintenance. It can be installed as a single server or several servers bound into a collective. A recommended two separate servers should have a FactoryTalk® Live Data interface installed along with an install of RSLinx Enterprise.

A requirement for the Enterprise Zone is to have a custom enterprise level reporting at multiple clients, which includes Industrial Zone historical data and trending. A FactoryTalk Historian server can be installed in the Enterprise Zone to provide centralized data aggregation from site historians.

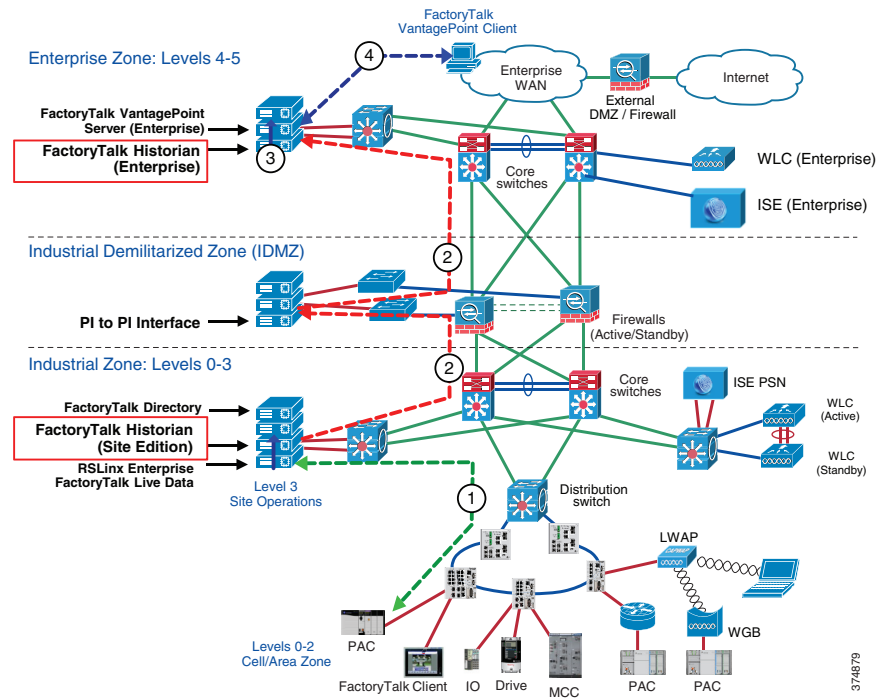
One of the main design goals of the CPwE is no direct traversal of data from the Enterprise Zone to the Industrial Zone or vice versa. In order to securely replicate production data to the Enterprise Zone, a PI-to-PI (Historian to Historian) replication service can be installed on a server in the IDMZ. The PI-to-PI Interface copies data between two instances of FactoryTalk Historian server (single server or a collective).

FactoryTalk Historian IDMZ Architecture

Figure 2-24 illustrates a recommended IDMZ architecture for the FactoryTalk Historian. Two Historian servers are installed, one in the Industrial Zone and one in the Enterprise Zone. A PI-to-PI Interface is installed in the IDMZ to copy data between the two instances of FactoryTalk Historian (either a single server or a collective).

A FactoryTalk VantagePoint server is also installed in the Enterprise Zone to collect data from the Historian in the Enterprise Zone.

Figure 2-24 FactoryTalk Historian Data Transfer



1. Controller data is sent to the FactoryTalk Historian SE data repository via RSLinx Enterprise and FactoryTalk® Live Data interfaces.

2. The PI-to-PI Interface pulls predefined data from the FactoryTalk Historian SE in the Industrial Zone and pushes the data to the FactoryTalk Historian in the Enterprise Zone.
3. FactoryTalk VantagePoint server in the Enterprise Zone gathers preconfigured data from the Enterprise Zone Historian to generate reports.
4. A FactoryTalk VantagePoint client requests a web report based on the data collected from the Enterprise Zone Historian data.

**Note**

By installing a second FactoryTalk VantagePoint server in the Industrial Zone, data can be visualized in both the Enterprise and the Industrial Zones.

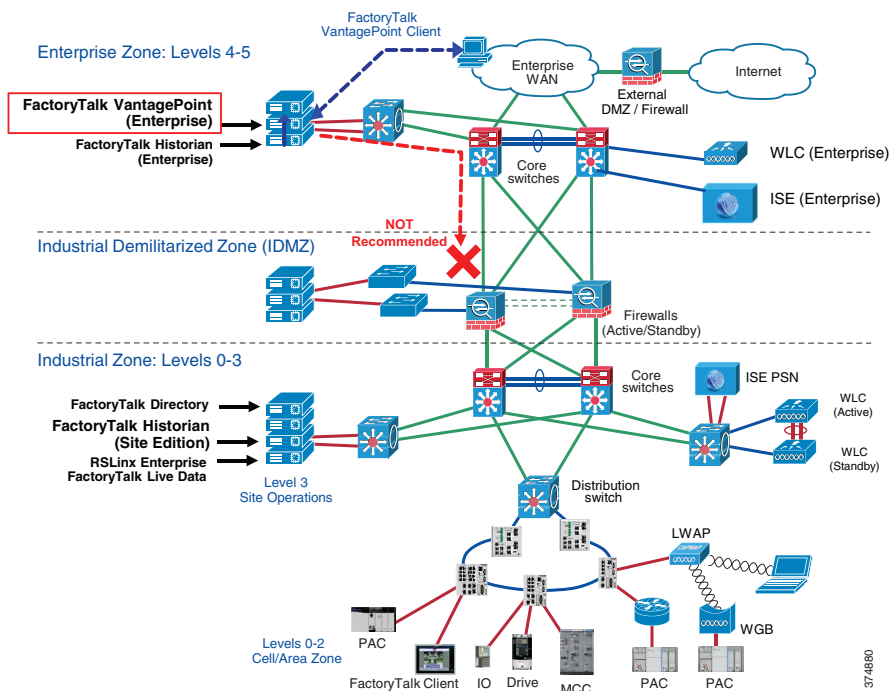
An overview of PI-to-PI Interface configuration and firewall rules for the Historian data transfer is provided in [FactoryTalk Historian Data Transfer Configuration, page 3-21](#).

FactoryTalk VantagePoint Connectivity to Historian Server

The previous example described connectivity of an Enterprise VantagePoint server getting data from the Enterprise Zone Historian.

- It is recommended that the FactoryTalk VantagePoint clients do not cross security boundaries to obtain FactoryTalk Historian information or connect to a FactoryTalk VantagePoint server in another security zone. For instance, it is not recommended for an Enterprise FactoryTalk VantagePoint server or client to connect directly to the Industrial Zone FactoryTalk Historian (see [Figure 2-25](#)).
- If a client in the Enterprise zone wants access to an asset in the Industrial Zone, the client can then access the server via one of the remote access methods available (described later in this chapter).

Figure 2-25 FactoryTalk VantagePoint in Enterprise Zone



374880

Secure File Transfer

Employees often need to transfer files between the Industrial and Enterprise Zones due to business requirements. Some examples of files that need to be passed between both zones are production reports, assembly line instructions, user manuals and software installation files. Traditional ways to move files, such as Windows file shares, email attachments, USB drives or third-party web-based solutions, can be insecure or introduce significant risks to the industrial environment. Secure File Transfer (SFT) solutions provide a secure way to accomplish the task in compliance with the IDMZ design principles.

Overview of Managed File Transfer (MFT) Solutions

Several products on the market provide the solution for a managed secure file transfer between the Enterprise and the Industrial Zone. These solutions require the installation of a file transfer server gateway in the IDMZ with SFT servers located in the Enterprise and Industrial Zones.

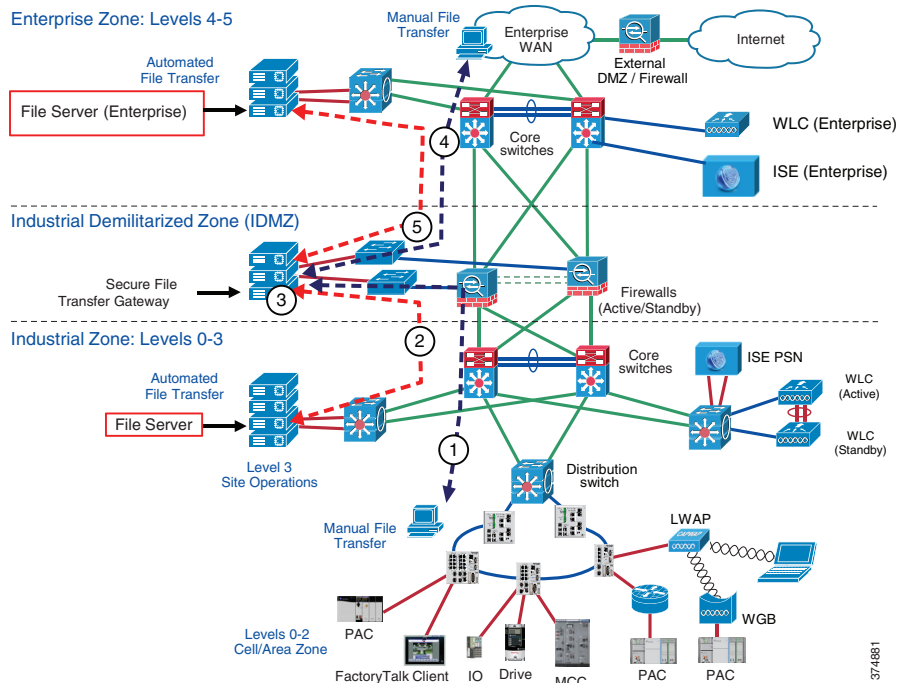
This approach allows for secure file transfers between the zones using the IDMZ gateway as a proxy. An industrial SFT system should have the following characteristics:

- All incoming connections are accepted on a hardened SFT gateway in the IDMZ using a secure protocol, for instance Secure File Transfer Protocol (SFTP), FTP over SSL or HTTPS.
- Files can be inspected by the Firewall during transit using Cisco AMP.
- Users can be authenticated against the AD to confirm that only certain people can send or receive files. Depending on the security policy, different groups of authorized users can be created in the Industrial and Enterprise Zones.
- No inbound connections are allowed from the IDMZ to the Industrial Zone. Only authorized users can initiate file transfer connections.
- Files are not stored permanently in the IDMZ.
- The system can provide audit trail tracking and extensive reporting.

Secure File Transfer Architecture

Figure 2-26 provides an overview of the SFT architecture for the CPwE IDMZ.

Figure 2-26 Secure File Transfer



The steps below describe a manual or automated file transfer that initiated from the Industrial Zone.

1. A manual file transfer is initiated from the Industrial Zone. An industrial user connects to the Secured File Transfer Gateway in the IDMZ.
2. In case of an automated transfer, a file server in the Industrial Zone connects to the gateway.
3. The user is authenticated on the Secure File Transfer Gateway and the file is transferred, inspected and saved. The file transfer is done via a secure encrypted protocol such as SFTP or HTTPS.
4. The IDMZ firewall validates the file does not contain any known malware.
5. The enterprise user logs onto the Secure File Transfer Gateway and retrieves the file.
6. In case of an automated transfer, a file server in the Enterprise Zone retrieves the file.

If the file transfer is initiated from the Enterprise Zone, the process is reversed.

Data Brokering

Network and Security administrators use multiple tools to get their jobs done and the need for these tools is growing. From cloud to on-premises, big vendors to homegrown, these tools compete for precious access to a limited number of data feeds. As administrators feel the pressure to install, evaluate, and implement these tools, all while staying under budget, they are hindered by the constraints of the data consumers and exporters. Network and security administrators should not have to analyze their data using multiple tools built for specific protocols. Rather than burdening the customer's workflow to fit the needs of the data, the data should be groomed to fit the needs of the customers and their tools.

Cisco Telemetry Broker Overview

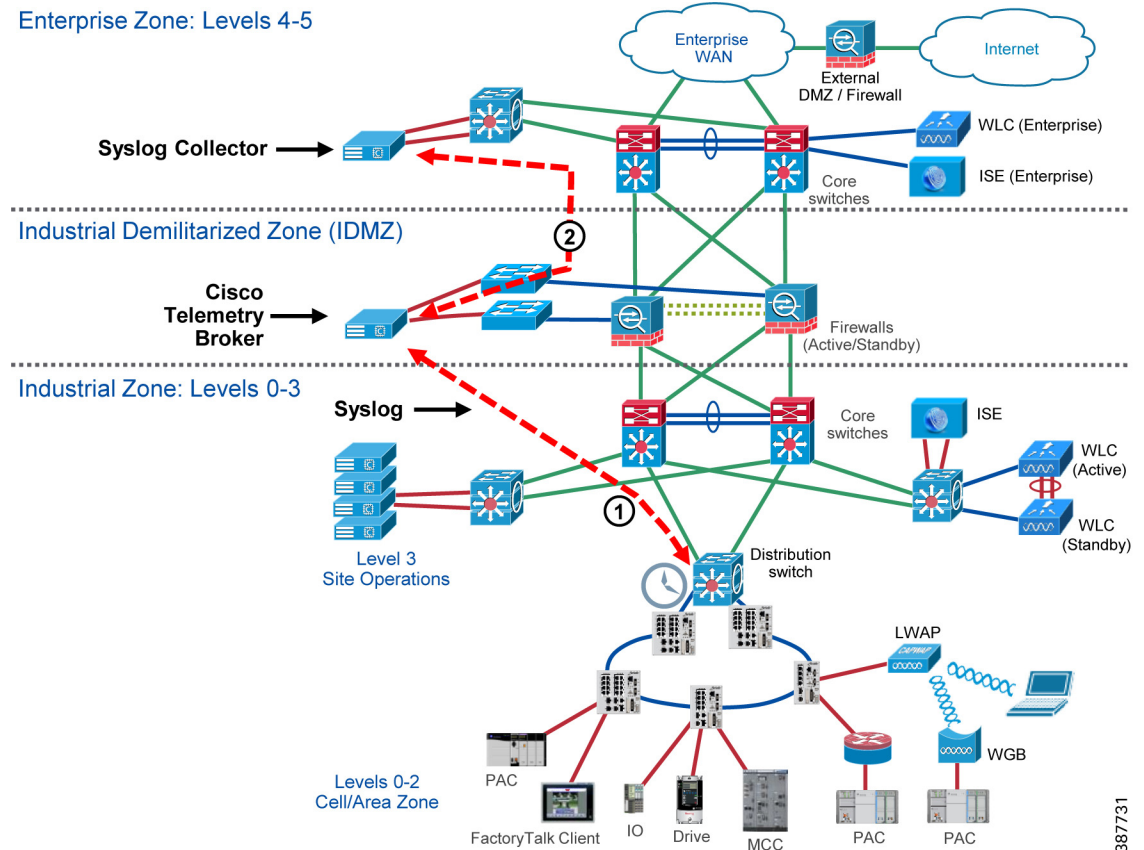
Cisco's Telemetry Broker has roots in the Secure Network Analytics UDP Director, which simply replicated UDP traffic to multiple destinations. The Cisco Telemetry Broker will build upon the successes of the UDP Director, while also creating a new market—the Telemetry Broker market. Cisco Telemetry Broker optimizes telemetry pipelines for the hybrid cloud. It vastly simplifies the consumption of telemetry data for customers' business critical tools by brokering hybrid cloud data, filtering unneeded data, and transforming data to a usable format.

Cisco Telemetry Broker provides several key functionalities that will address the growing concerns of our customers:

- **Brokering Data**—The ability to route and replicate telemetry data from a source location to multiple destination consumers and to quickly onboard new telemetry-based tools!
- **Filtering Data**—The ability to filter data that is being replicated to consumers for fine grain control over what consumers are able to see and analyze and save money by not sending data to expensive tools!
- **Transforming Data**—The ability to transform data protocols from the exporter to the consumer's protocol of choice and enable tools to consume multiple data formats!

Cisco Telemetry Broker IDMZ Architecture

Figure 2-27 Cisco Telemetry Broker IDMZ Architecture



Cisco Telemetry Broker supports multi-node setups, where a single Cisco Telemetry Broker manager can manage multiple broker nodes. Broker nodes will exist in the IDMZ, as their role in the network is to broker data from the Industrial Zone. The manager node, if deployed to manage just the broker nodes for a single network, may also exist in the IDMZ. However, for deployment scenarios that span across multiple IDMZs, the manager node should exist in the Enterprise zone where it can be linked to all instances of the broker node across a distributed network architecture.

Remote Access Services

This section provides an overview of CPwE IDMZ remote access solutions and examples for FactoryTalk applications. Specific technologies include:

- SSL VPN access using the FTD platform
- Microsoft RD Gateway
- ThinManager via Microsoft RD Gateway
- Cisco Duo Authentication for Microsoft Remote Desktop Gateway

Remote Access Overview

Quick and effective response to issues on the plant floor often requires real-time access to information and status from IACS applications as well as the skills and knowledge to take corrective action or optimize the IACS process. Secure remote access to industrial assets, data and applications provides companies with the ability to apply the right skills and resources at the right time, independent of their physical location. Companies can use internal experts or the skills and resources of trusted partners and service providers, such as OEMs and system integrators, without needing someone onsite.

To deploy secure remote access, CPwE architecture includes a number of network services and technologies that are widely deployed in enterprise networks such as VPN, terminal services and web access portals.

Remote Access Design Principles

In the past, companies relied completely on onsite personnel to provide support for IACS applications, or used methods such as dial-up access and separate dedicated networks for remote support. These remote access methods have limited bandwidth and capabilities and are therefore limited to very basic monitoring and updating functionality. At the same time, they often circumvent perimeter security defenses and do not have the visibility and support of the IT organization. This creates the threat of "back doors" into the Industrial Zone and can represent a significant security risk. As manufacturers and partners want to provide more service and support remotely, and respond to issues in real time, these methods are no longer sufficient.

To truly leverage the full value of a converged enterprise, remote access needs to be scalable, regardless of location or company, and it needs to be done securely and in combination with the necessary tools to effectively communicate, diagnose problems and implement corrective actions. However, access needs to be limited to those individuals who are authorized to access systems, and their authorized actions need to be aligned to corporate and plant policies and procedures.

Several guiding principles should be maintained when allowing remote access to IACS data and resources:

- Use User Access and Authentication Policies and Procedures:
 - Access to resources and services should be monitored and logged.
 - Every user must be a known entity to the organization and use a unique account.

- Users should be granted access to IACS data and resources based on the authorization policy on “as needed” basis.
- Users should verify their identity using MFA.
- Use of back-door solutions (such as modems, phone lines, and direct Internet access) may pose a significant risk and should be avoided.
- Written policies should be implemented specifying under what conditions and who may be granted access into the secured Industrial Zone. Industrial personnel and trusted partners should sign a security agreement acknowledging their responsibilities.
- Control the Applications:
 - IACS protocols, such as CIP or FactoryTalk Live Data, should be contained to the Industrial Zone.
 - As a best practice, partners and remote engineers should use versions of IACS applications on controlled application servers in the Industrial Zone. By restricting remote users to applications running on a RAS, companies can enforce change management, version control and regulatory compliance of the applications being used.
 - This best practice prevents viruses or other compromises of the remote system from affecting the Industrial Zone applications and systems. The use of IACS applications on a remote user's computer introduces significant risk to the IACS and should be avoided.
- No Direct Traffic:
 - No direct traffic is permitted between the Enterprise Zone (including the Internet) and the Industrial Zone, with exception for certain highly controlled network services as outlined previously in this guide.
 - Remote access to devices on the IACS network should require connecting through the IDMZ firewall and logging into or at least proxying through a server.
- Only One Path In or Out:
 - The path from the IDMZ into the Industrial Zone should be the only path in or out. The path from the enterprise LAN into the IDMZ should be the only path connecting the two zones.

These guiding principles encapsulate the key concepts of strictly controlling the remote access of IACS applications rather than trusting that remote users are doing the right thing when accessing the IACS applications.

SSL VPN Access

The Firepower Management Center supports the following types of VPN connections:

- Remote Access VPNs on FTD devices.

Remote access VPNs are secure, encrypted connections, or tunnels, between remote users and your company's private network. The connection consists of a VPN endpoint device, which is a workstation or mobile device with VPN client capabilities, and a VPN headend device, or secure gateway, at the edge of the corporate private network.

FTD devices can be configured to support Remote Access VPNs over SSL or IPsec IKEv2 by the Firepower Management Center. Functioning as secure gateways in this capacity, they authenticate remote users, authorize access, and encrypt data to provide secure connections to your network. No other types of appliances, managed by the Firepower Management Center, support Remote Access VPN connections.

FTD secure gateways support the AnyConnect Secure Mobility Client full tunnel client. This client is required to provide secure SSL IPsec IKEv2 connections for remote users. This client gives remote users the benefits of a client without the need for network administrators to install and configure clients on remote computers since it can be deployed to the client platform upon connectivity. It is the only client supported on endpoint devices.

- Site-to-site VPNs on Firepower Threat Defense devices.

A site-to-site VPN connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices, and between managed devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and IKEv1 or IKEv2. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

Client-based SSL VPN (Cisco AnyConnect)

The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. The Cisco AnyConnect client, which uses SSL, is designed for automated download and installation of the client software on the user's PC.

Other capabilities for the Cisco AnyConnect client include features that allow the client to reconnect if the tunnel goes down, to disable the tunnel if the client moves onto the trusted network or to bring up the tunnel if the client moves from a trusted to an untrusted network.

The Cisco AnyConnect VPN client provides secure SSL or IPsec (IKEv2) connections to the FTD for remote users with full VPN tunneling to corporate resources.

Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL or IPsec-IKEv2 VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, remote users must enter the URL in the form https://address. After the user enters the URL, the browser connects to that interface and displays the login screen.

After a user logs in, if the secure gateway identifies the user as requiring the VPN client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure connection, and either remains or uninstalls itself (depending on the security appliance configuration) when the connection stops. In the case of a previously installed client, after login, the FTD security gateway examines the client version and upgrades it as necessary.

MFA—Cisco Secure Access by Duo

AAA servers enable managed devices acting as secure gateways to determine who a user is (authentication), what the user is permitted to do (authorization), and what the user did (accounting). Some examples of the AAA servers are RADIUS, LDAP/AD, TACACS+, and Kerberos. For Remote Access VPN on FTD devices, AD, LDAP, and RADIUS AAA servers are supported for authentication.

Duo MFA for Cisco FTD supports push, phone call, or passcode authentication for AnyConnect desktop and AnyConnect mobile client VPN connections that use SSL encryption. The Duo proxy server will receive incoming RADIUS requests from the FTD, contact your existing local LDAP/AD or RADIUS server to perform primary authentication if necessary, and then contact Duo's cloud service for secondary authentication.

Microsoft Remote Desktop (RD) Gateway

Remote Desktop (RD) Gateway, formerly Terminal Services Gateway, is an available option in the Remote Desktop Services server role included with Windows Server Operating Systems. A Windows Server with the RD Gateway role enabled allows authorized remote users and thin clients using ThinManager to connect to resources from an internal corporate or private network to assets in the Industrial Zone from any device that can run the Remote Desktop Connection (RDC) client.

RD Gateway uses the Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users and internal network resources. The remote desktop user via a thin client using ThinManager or Microsoft Remote Desktop Connection client will have access to the desktop and applications of the remote computer as if they are sitting locally and accessing the computers keyboard and mouse and viewing the local display.

**Note**

For more information, refer to *Remote Desktop Services Overview* at:

- <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-deploy-infrastructure>

ThinManager

ThinManager by Rockwell Automation is a thin client and content delivery management platform that is purpose built around providing a safe and secure environment to mitigate risk in a connected industrial environment.

**Note**

For more information, refer to ThinManager Product Profile at:

- <https://thinmanager.com/profile/>

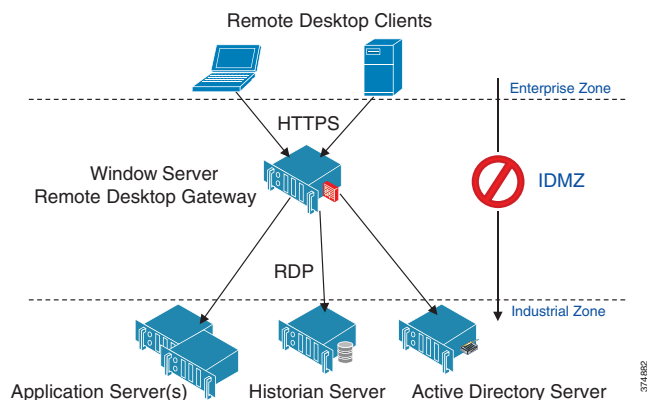
Network segmentation is critical to maintaining a secure environment across multiple layers of a control network. A ThinManager server should be located inside the Industrial Zone and/or the Enterprise Zone, depending on the use case and business needs. This separates the Industrial Security Zone and the Enterprise Security Zone and does not permit any network traffic to traverse the zone without being redirected by the Remote Desktop Gateway. By placing ThinManager inside the Industrial Zone and/or the Enterprise Zone, no traffic is required to traverse directly across the IDMZ in order to deliver Remote Desktop Services content to requesting clients.

RD Gateway is a critical component of the deployment that will be required to deliver Remote Desktop Services content from the Industrial Security Zone to the Enterprise Security Zone or vice versa. This applies for Remote Desktop content that will be used on thin clients or mobile clients using WinTMC, aTMC, or iTMC.

RD Gateway Architecture

The RD Gateway is placed within the IDMZ and acts as the gateway to the Industrial Zone assets to enterprise users who wish to access these computers (see [Figure 2-28](#)).

Figure 2-28 Remote Desktop Gateway Architecture



The RD Gateway uses two-factor authentication that verifies that a valid SSL certificate is being presented by the server and a valid user name and password is entered to authenticate the user's credentials.

The RD Gateway is designed to use HTTPS for the authentication process and initial connection establishment. Once the user is authenticated, the RD Gateway server connects to the requested Industrial Zone host via RDP. The firewall should be configured to allow HTTPS into the IDMZ from the Enterprise Zone and RDP from the remote desktop gateway to the Industrial Zone server(s).

RD Gateway Policies

The RD Gateway allows the administrator to configure **who** can connect to **what** through resource and connection policies.

- **RD Gateway Connection Authorization Policies (CAPs)** allow you to specify who can connect to the IDMZ RD Gateway server. The RD Gateway administrator can specify a user or user group that exists on the local RD Gateway server or in AD. The administrator can list specific conditions in each RD Gateway CAP, for example, you might require a group of users to use a smart card to connect through the RD Gateway.
- **RD Gateway Resource Authorization Policies (RAPs)** allow you to specify the Industrial Zone network resources that remote users can connect to through an RD Gateway server. When you create an RD Gateway RAP, you can use AD computer groups or single IP Addresses and associate it with the RD Gateway RAP.

Before CAPs and RAPs can be configured, the administrator should define user groups and computer groups for remote access and create security rules for those groups.

[Microsoft Remote Desktop Gateway Configuration, page 3-32](#) has an example of defining a remote access rules and configuring the RD Gateway policies.

FactoryTalk Application Examples

Industrial Zone assets oftentimes require access to configure, maintain, and troubleshoot the process from outside the Industrial Zone. Security policies usually require that each user must be authenticated and their access to the Industrial Zone assets must be limited based on their credentials.

The following FactoryTalk applications can be accessible via remote access technologies:

- Studio 5000 Logix Designer®
- FactoryTalk AssetCentre

- FactoryTalk View Site Edition (SE)
- FactoryTalk ViewPoint
- FactoryTalk VantagePoint
- FactoryTalk Historian
- FactoryTalk Metrics

Each of these applications will have design and runtime programs that will need to be accessed by a remote user.

RD Gateway Access for FactoryTalk Applications

A solution that meets the application requirements listed above is to use a RD Gateway located in the IDMZ. Two variants of this solution are considered:

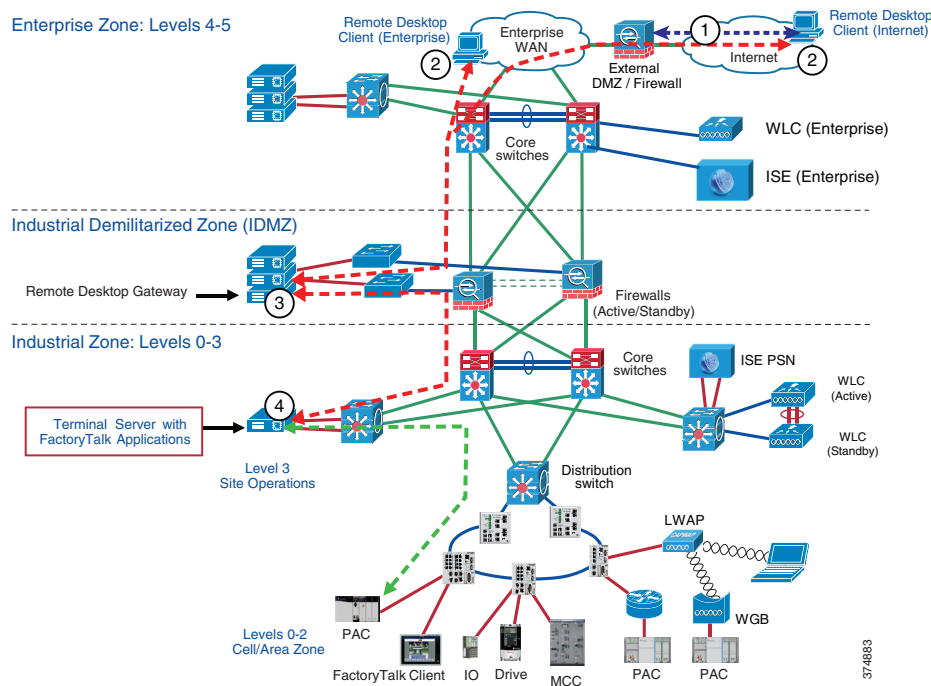
- Applications are installed and run on the terminal server in the Industrial Zone.
- Applications are installed and run on separate servers and accessed directly from the RD Gateway.

The choice of a solution depends on the existing deployment scheme, scale of operation, type of applications for remote access and whether a company chooses to implement more granular policies to restrict or control access.

RD Gateway Access to FactoryTalk Applications Installed on a Terminal Server

In this scenario, the required FactoryTalk design and runtime software is configured to run on the Terminal Server in the Industrial Zone. This scenario's workflow is described in [Figure 2-29](#).

Figure 2-29 RD Gateway Access to FactoryTalk Applications Installed on Terminal Server



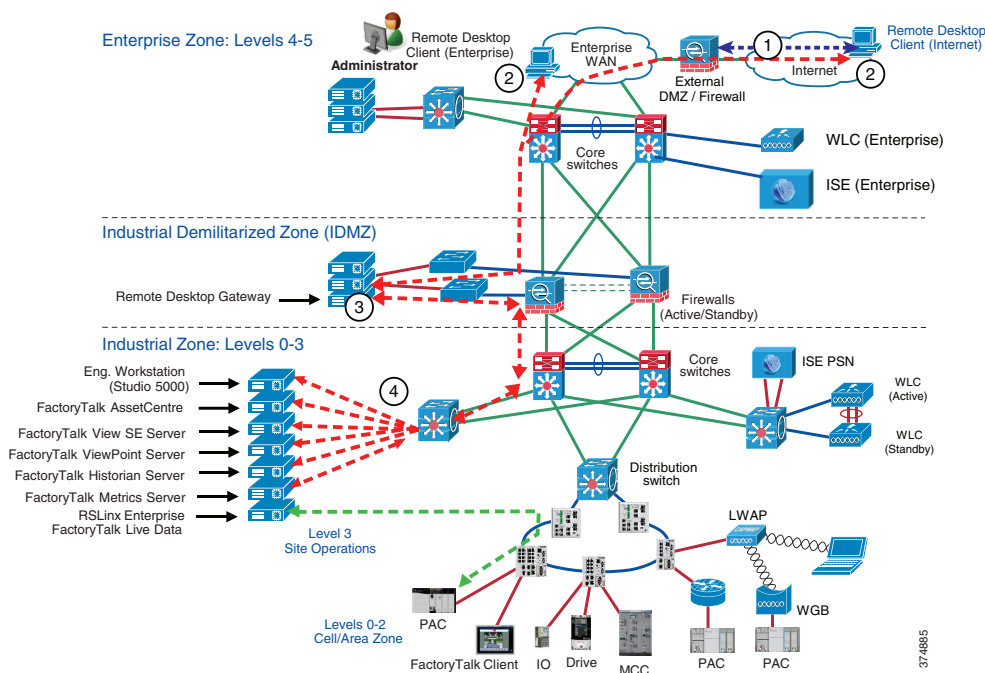
1. If the Remote Desktop client is outside the corporate network, a VPN session is established with the customer site.

2. The RDC application is launched from remote user's computer. The user enters Industrial Zone Remote Session Host's address (the Terminal Server running FactoryTalk applications) as the target desktop and starts the session.
3. The RD Gateway server in the IDMZ validates the SSL certificate and the username and password.
4. The Remote Session Host's desktop is now presented to the remote desktop user.

Direct Access to FactoryTalk Applications via RD Gateway

The RD Gateway is capable of being configured to allow certain users such as production administrators or corporate engineers to have direct access to Industrial Zone assets for configuration, maintenance and troubleshooting purposes without going through a terminal server. A variation to the prior solution is to use a RD Gateway located in the IDMZ to access FactoryTalk and other Industrial Zone assets directly. This scenario's workflow is described in Figure 2-30.

Figure 2-30 Direct Access to FactoryTalk Applications via RD Gateway



1. If the RD client is outside the corporate network, a VPN Session is established with the customer site.
2. Remote Desktop Connection application is launched from remote user's computer. The user enters Industrial Zone host's address as the target desktop and starts the session.
3. The RD Gateway server in the IDMZ validates the SSL certificate and the username and password.
4. The remote host's desktop is now presented to the remote desktop user.

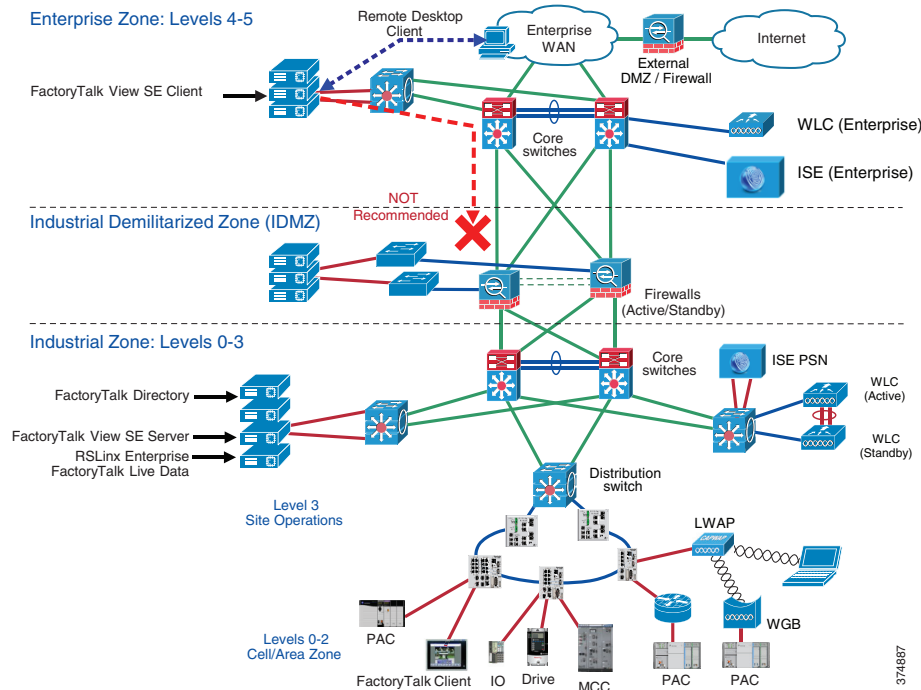
Examples of Non-Recommended Architectures

Previous examples described ways to access FactoryTalk applications remotely that comply with the security design principles for the IDMZ. Often companies try to deploy FactoryTalk applications across the IDMZ in a way that violates these principles, for convenience or cost saving purposes. This situation, which creates security risks, is strongly not recommended.

For example, [Figure 2-31](#) shows an architecture where a FactoryTalk View SE client is installed in the Enterprise Zone and communicates to the FactoryTalk View server and FactoryTalk Directory server in the Industrial Zone. To enable this scenario, a wide range of ports needs to be open on the firewall, including DCOM dynamic port range.

This architecture does not align with IDMZ security design principles and is not recommended.

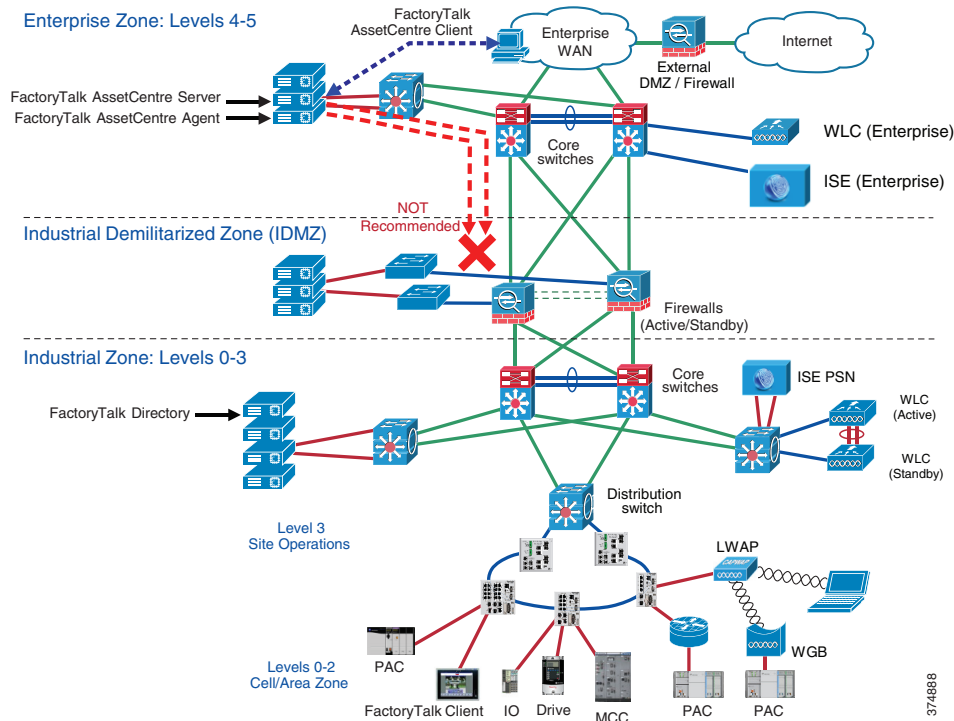
Figure 2-31 FactoryTalk View SE Client (Enterprise)—Not Recommended



In another example (see [Figure 2-32](#)), FactoryTalk AssetCentre server and agents are placed in the Enterprise Zone. This scenario also requires multiple ports to be opened. In addition to that, agents will have direct access to the assets in the Industrial Zone (for example, PACs), which violates IDMZ security policy.

This architecture does not align with IDMZ security design principles and is not recommended.

Figure 2-32 FactoryTalk AssetCentre (Enterprise)—Not Recommended



Application Security

Application security is the crucial part of the defense-in-depth security strategy. The components that provide application security may include:

- Application-level firewalls and proxies
- Application-level user authentication and authorization
- Application and OS hardening against threats such as code tampering, malware insertions, reverse-engineering and unauthorized use

The following sections review some of the application security methods:

- FactoryTalk Security
- Microsoft OS hardening

FactoryTalk Security

FactoryTalk Security is designed to provide a layer of application security. Its purpose is to protect against internal threats that are either malicious or accidental by limiting access to only those individuals who legitimately need access to specific automation assets.

FactoryTalk Security accomplishes this goal by allowing security administrators to define the answer to this question: “Who can carry out what actions upon which secured resources from where?”

- **Who** can use Rockwell Automation software products
 - ...to perform **what** specific actions

- ...on **which** Rockwell Automation hardware devices and other securable resources
- ...from **where** - that is, from which specific computers or workstations

How does FactoryTalk Security Protect the Application Layer?

When someone attempts to use a FactoryTalk-enabled software product to access a Rockwell Automation hardware device or other securable resource, FactoryTalk Security authenticates the person's identity and authorizes that person to access that resource and perform only allowed actions.

- **Authentication**—Verifies a user's identity and verifies that a request actually originated with that user.
- **Authorization**—Verifies a user's request to use a software product or to access a hardware device or secured resource against a set of previously defined access permissions.

FactoryTalk Security allows centralized administration of user accounts and access permissions. Security information, including user authentication and authorization, can be shared across all software products and hardware devices on a particular computer, throughout a plant or across an entire enterprise.

In the Windows domain environment, FactoryTalk Security accounts can be linked to the AD accounts and groups, which allows single identity for employees.



Note

For further details about FactoryTalk Security, see the *FactoryTalk Security System Configuration Guide* at:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-e.pdf

An example of how to configure FactoryTalk Security is given in [FactoryTalk Security Configuration, page 3-49](#).

Operating System Hardening

Software vulnerabilities and exploits have become an everyday part of life. Virtually every product has to deal with them and consequently users are faced with a stream of security updates. Security mitigation technologies are designed to make it impossible or more difficult for an attacker to exploit vulnerabilities in a given piece of software.

Rockwell Automation supports Microsoft AppLocker® as an OS hardening solution.



Note

Full description and implementation guides to these solutions can be found on the Rockwell Automation knowledge base site, with a valid support center account:

- 546989—*Using Rockwell Automation Software Products with AppLocker*
 - https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/546989

Microsoft AppLocker Overview

In order to further harden the desktop environments, Rockwell Automation and Cisco recommends restricting administrator credentials. Normally, running as a standard, non-administrative user is recommended as it limits configuration changes that can be made in the desktop environment. However, running as a standard user does not prevent the installation or execution of unknown or unwanted applications in your organization.

To meet these challenges, Microsoft introduced a new feature in Windows 7 and Server 2008 R2 called AppLocker. AppLocker allows you to specify which users or groups can run particular applications in your organization based on unique identities of files. If you use AppLocker, you can allow or deny applications by creating rules to allow or deny applications from running.

**Note**

-
- It is strongly recommended to define allow lists rather than deny lists.
 - For a more detailed explanation of Microsoft AppLocker, refer to the technical reference at:
 - <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-technical-reference>
-

Configuring the Infrastructure

This chapter describes how to configure IDMZ infrastructure in the CPwE architecture based on the design considerations of the previous chapters. It covers the configuration of the network infrastructure, network services, data transfer, remote access services and network and application security, all from an IDMZ perspective. The included configurations have been validated during the testing effort.

This chapter includes the following major topics:

- [Configuring IDMZ Network Infrastructure, page 3-1](#)
- [Configuring Network Services, page 3-11](#)
- [Configuring Data Transfer through IDMZ, page 3-21](#)
- [Configuring Remote Access Services, page 3-27](#)
- [Configuring Application Security, page 3-48](#)

Configuring IDMZ Network Infrastructure

This section describes validated configurations for the network infrastructure that establishes the IDMZ within the CPwE architecture, such as firewalls and switches.

Industrial Zone Firewall Configuration

The following firewall configuration steps are covered in this section:

- Configuration of the IDMZ firewall in active/standby mode
- Configuration of the IDMZ network interface on the firewall

Active/Standby Firewall Configuration

**Note**

This guide assumes that the user has already performed the initial setup and hardening of the Cisco Firepower 2100. For more details on these configurations, refer to:

- <https://www.cisco.com/c/en/us/support/security/firepower-2100-series/series.html#~tab-documents>

The following steps describe the initial configuration of the active and standby IDMZ firewalls:

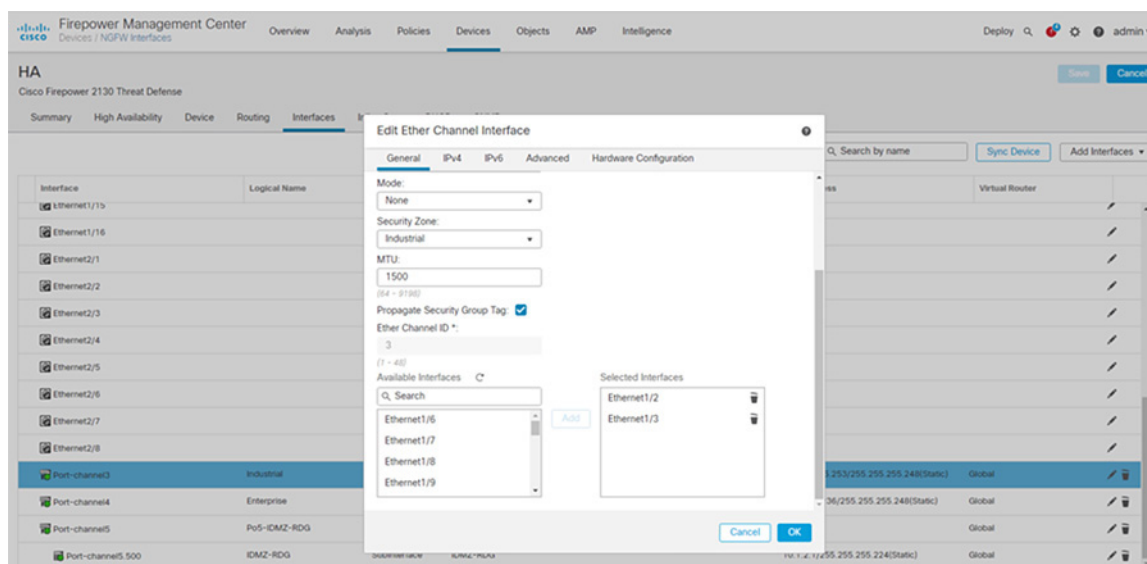
- Step 1 Configure interfaces for the Industrial and Enterprise Zones (see [Figure 3-1](#)):
- In Cisco FMC, select **Devices > Device Management** and click **Edit** for your FTD device. The **Interfaces** page is selected by default.
 - Click **Add Interfaces > Ether Channel Interface**.
 - On the **General** tab, set the **Ether Channel ID** to a number between 1 and 48.
 - In the **Available Interfaces** area, click an interface and then click **Add** to move it to the **Selected Interfaces** area. Repeat for all interfaces you want to make members.



Note Make sure all interfaces are the same type and speed. The first interface you add determines the type and speed of the EtherChannel. Any non-matching interfaces you add will be put into a suspended state. The FMC does not prevent you from adding non-matching interfaces.

- Click **OK**.
- Click **Save**. Make sure to **Deploy** changes when configuration is complete.

Figure 3-1 FMC EtherChannel Interface Configuration



- Step 2 Configure EIGRP as the dynamic routing protocol (see [Figure 3-2](#)):



Note FlexConfig is used to allow you to implement features that are not yet directly supported through FMC policies and settings. FlexConfig can be a useful tool when migrating from ASA to FTD and there are compatible features you are using (and continuing to use) that FMC does not directly support.

- In FMC, select **Objects > Object Management** and navigate to **FlexConfig > FlexConfig Object**.

- b. Click **Add FlexConfig Object**.
- c. Give a meaningful name to the object, and insert the desired EIGRP configuration for the FTD (see [Figure 3-2](#) for an example).

Figure 3-2 FMC EIGRP FlexConfig Object

Edit FlexConfig Object

Name:

Description: Configures eigrp. 1. Configures next hop. 2.

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert Deployment: Everytime Type: Append

```
router eigrp 101
network 10.1.2.0 255.255.255.0
network 10.255.3.0 255.255.255.0
network 10.255.255.0 255.255.255.0
passive-interface default
no passive-interface Industrial
no passive-interface Enterprise
```

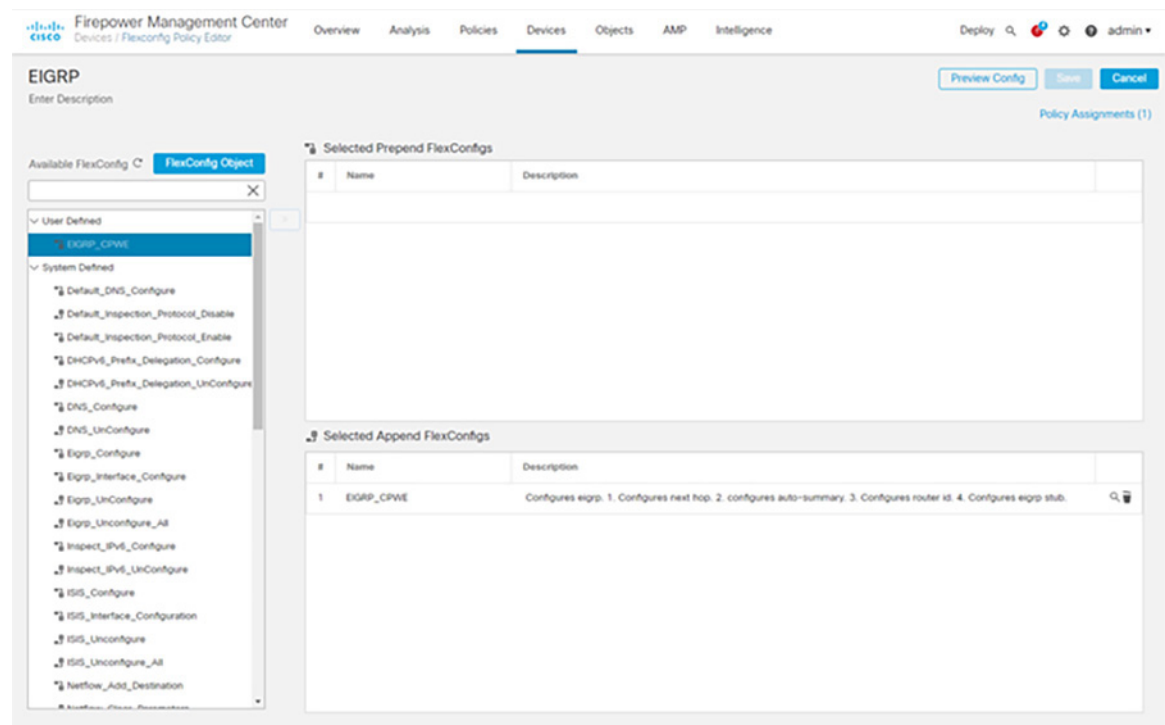
▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel Save

- d. Continuing in FMC, select **Devices > FlexConfig** and click **New Policy**.
- e. Give a meaningful name to the policy and in the **Available Devices** area, click an interface and then click **Add to Policy** to move it to the **Selected Devices** area. Repeat for all devices you want to make this policy to apply.
- f. Click **Save**.
- g. In the **Available FlexConfig** tab, under **User Defined**, select the FlexConfig object for EIGRP and click **>** to move it to the **Selected Append FlexConfigs** area.
- h. Click **Save and Deploy** changes to the FTD.

Figure 3-3 FMC EIGRP Configuration with FlexConnect



Step 3 Configure active/standby failover mode on each firewall and the failover link between the two (see Figure 3-4):

- In FMC, navigate to **Devices > Device Management**.
- From the **Add** drop-down menu, choose **High Availability**.
- Enter a display **Name** for the high availability pair.
- Under **Device Type**, choose **Firepower Threat Defense**.
- Choose the **Primary Peer** device for the high availability pair.
- Choose the **Secondary Peer** device for the high availability pair.
- Click **Continue**.
- Under **High Availability Link**, choose an Interface with enough bandwidth to reserve for failover communications.



Note Only interfaces that do not have a logical name and do not belong to a security zone, will be listed in the Interface drop-down menu in the Add High Availability Pair dialog.

- Type any identifying **Logical Name**.
- Type a **Primary IP** address for the failover link on the active unit. This address should be on an unused subnet. This subnet can be 31-bits (255.255.255.254 or /31) with only two IP addresses.



Note 169.254.1.0/24 and fd00:0:0::*:/64 are internally used subnets and cannot be used for the failover or state links.

- k. Optionally, choose **Use IPv6 Address**.
- l. Type a **Secondary IP** address for the failover link on the standby unit. This IP address must be in the same subnet as the primary IP address.
- m. If IPv4 addresses are used, type a **Subnet Mask** that applies to both the primary and secondary IP addresses.
- n. Optionally, under **Stateful Failover Link**, choose the same **Interface**, or choose a different interface and enter the high availability configuration information. This subnet can be 31-bits (255.255.255.254 or /31) with only two IP addresses.



Note 169.254.1.0/24 and fd00:0:0:0::/64 are internally used subnets and cannot be used for the failover or state links.

- o. Optionally, choose **Enabled** and choose the **Key Generation** method for IPsec Encryption between the failover links.
- p. Click **Add**. This process takes a few minutes as the process synchronizes system data.

Figure 3-4 FMC Failover Configuration

Step 4 Configure explicit **Deny All** rules between all zones (see [Figure 3-5](#)):

- a. In FMC, navigate to **Policies > Access Control**.
- b. Click **New Policy**.
- c. Enter a unique **Name** and, optionally, a **Description**.

- d. Specify the initial **Default Action**. Our intention is to **Block all traffic** which creates a policy with the **Access Control: Block All Traffic** default action.
- e. Choose the **Available Devices** where you want to deploy the policy, then click **Add to Policy** to add the selected devices.
- f. Click **Save**.

Figure 3-5 FMC Access Rules Configuration

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:
☒ Block all traffic
☐ Intrusion Prevention
☐ Network Discovery

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

HA

Add to Policy

Selected Devices

HA

Cancel

Save

**Note**

Later sections in this chapter describe the configuration of firewall rules and policies for specific network applications and services.

IDMZ Network Interface Configuration

The following steps describe the configuration of the firewall interfaces for the IDMZ network. In the recommended architecture, the IDMZ network is segmented into several VLANs, each corresponding to a specific service in the IDMZ.

- Step 1 Configure separate sub-interfaces for each network or application service hosted in the IDMZ (see [Figure 3-6](#)):



Note Before starting this procedure, confirm that the IDMZ-facing interface does not have an IP address, name, or security level configured. Otherwise, these configurations will be removed when the first sub-interface associated with that interface is created.

- a. In FMC, navigate to **Devices > Device Management** and **Edit** the device in which this VLAN applies.
- b. In the **Interfaces** tab, click **Add Interfaces > Sub Interface**.
- c. Give a meaningful **Name** to the sub interface.
- d. Assign a **Security Zone** for the sub interface.
- e. Assign the **Interface** to which the sub interface belongs.
- f. Assign the **VLAN ID** for the sub interface.
- g. Click **OK** to add the sub interface and then Save changes to the device.
- h. Define explicit **Deny All** rules for each sub-interface as described in the previous section to confirm isolation of each IDMZ service.

Figure 3-6 FMC Sub-interface Configuration

Edit Sub Interface

General IPv4 IPv6 Advanced

Name:
IDMZ-RDG

☒ Enabled
☐ Management Only

Description:

Security Zone:
IDMZ-RDG

MTU:
1500
(64 - 9198)

Propagate Security Group Tag: ☒

Interface *:
Port-channel5

Sub-Interface ID *:
500
(1 - 4294967295)

VLAN ID:
500
(1 - 4094)

Cancel OK

Industrial Zone Core Network Configuration

The following steps describe the configuration of the redundant network infrastructure between the Industrial Zone core network and the IDMZ firewall. The redundant core consisted of a pair of Cisco Catalyst 6500 switches in the VSS configuration.

Step 1 Enable Cisco StackWise Virtual on both switches and reload and configure Cisco StackWise Virtual link.



Note

For information on VSS and detailed steps on performing this conversion process, refer to:

- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/ha/b_169_ha_9500_cg/configuring_cisco_stackwise_virtual.html

Typical CLI output resulting from this conversion is shown below.


```

!
stackwise-virtual
  domain 1switch virtual domain 100 switch mode virtual
!

interface TwentyFiveGigE1/0/1
  stackwise-virtual link 1
interface TwentyFiveGigE1/0/2
  stackwise-virtual link 1
interface TwentyFiveGigE2/0/1
  stackwise-virtual link 1
interface TwentyFiveGigE2/0/2
  stackwise-virtual link 1

```

Step 2 Configure redundant EtherChannels between the VSS switch pair and the active and standby firewalls.

- a. Configure two EtherChannel interfaces on the VSS switch pair, one for each firewall connection, using the commands below:

```

!
interface Port-channel11
  description TO FIREWALL - FPR2130
  switchport access vlan 210
  switchport mode access
!
interface Port-channel12
  description TO FIREWALL - FPR2130
  switchport access vlan 210
  switchport mode access
interface Port-channel11 description To Primary FTD switchport
switchport trunk encapsulation dot1q switchport trunk allowed vlan <VLAN-LIST>
switchport mode trunk
!
interface Port-channel12 description To Secondary FTD switchport
switchport trunk encapsulation dot1q switchport trunk allowed vlan <VLAN-LIST>
switchport mode trunk
!

```

- b. Configure the members of both EtherChannel interfaces on the VSS switch pair using the commands below:

```

interface TwentyFiveGigE1/0/9
  description FPR-1 eth1/2
  switchport access vlan 210
  switchport mode access
  channel-group 12 mode active
!
interface TwentyFiveGigE1/0/10
  description FPR-2 eth1/3
  switchport access vlan 210
  switchport mode access
  channel-group 11 mode active
!
interface TwentyFiveGigE2/0/9
  description FPR-2 eth1/2
  switchport access vlan 210
  switchport mode access
  channel-group 11 mode active
!
interface TwentyFiveGigE2/0/10
  description FPR-1 eth1/3
  switchport access vlan 210
  switchport mode access
  channel-group 12 mode active!

```

!

IDMZ Server Network Configuration

The following steps describe the configuration of the redundant network infrastructure between the IDMZ switch and the IDMZ firewall.

Step 1 Configure EtherChannels between the IDMZ switch and the active and standby firewalls.

- a. Configure trunked EtherChannel interfaces on the IDMZ switch using the commands below:

```
!
interface Port-channel5
  description To Active Firewall
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
!
interface Port-channel6
  description To Standby Firewall
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
!
```

- b. Configure the members of the EtherChannel interface on the IDMZ switch using the commands below:

```
!
interface GigabitEthernet1/0/1
  description To Primary FTD
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
  channel-group 5 mode active
!
interface GigabitEthernet1/0/2
  description To Secondary FTD
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
  channel-group 6 mode active
!
interface GigabitEthernet2/0/1
  description To Primary FTD
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
  channel-group 5 mode active
!
interface GigabitEthernet2/0/2
  description To Secondary FTD
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <VLAN-LIST>
  switchport mode trunk
  channel-group 6 mode active
```

- Step 2 Configure the IDMZ switch with VLANs for each service that will be hosted in the IDMZ, according to best practices for IDMZ segmentation. Assign switch ports to appropriate VLANs.
-

Configuring Network Services

This section describes validated configurations for the network services that are allowed to traverse the IDMZ in order to provide necessary functions in both the Industrial and Enterprise Zones:

- Active Directory replication between Industrial and Enterprise Domain Controllers
- Time synchronization using NTP
- AAA Services
- Industrial and Enterprise ISE node synchronization traffic
- Tunneling of WLAN traffic between Industrial and Enterprise WLCs

Active Directory Configuration



Note

This section shows only what is needed to enable replication through the IDMZ. For more generalized AD configuration steps, refer to the *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at:

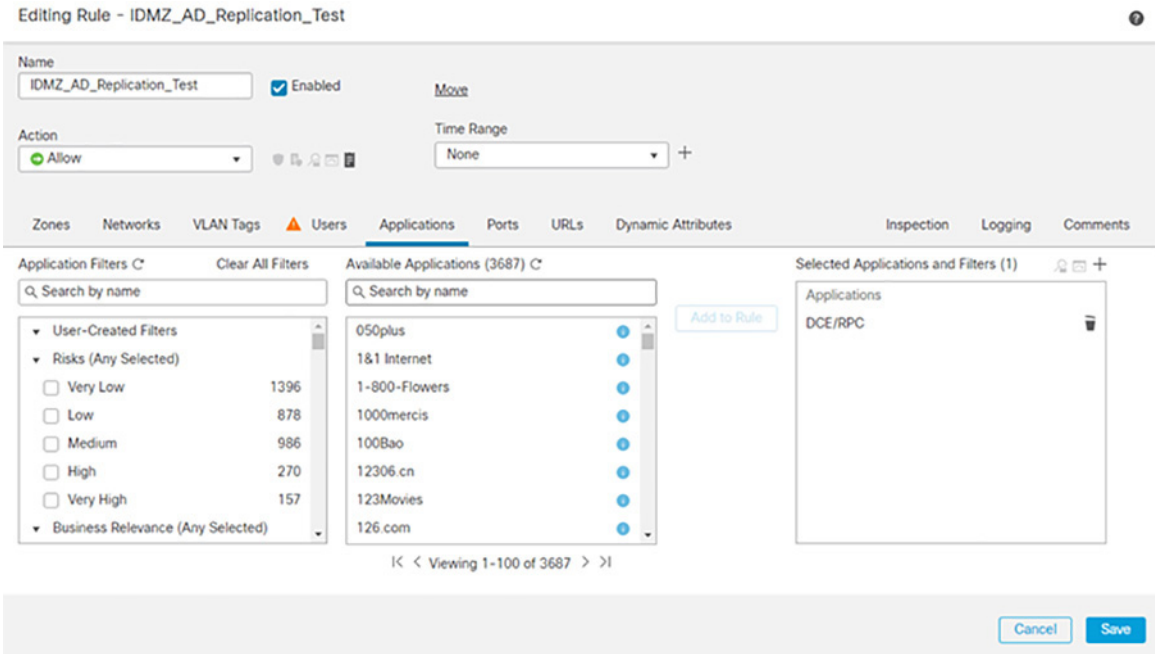
- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html
-

Firewall Rules for AD Replication

The following steps describe the configuration of firewall rules to allow replication of AD services across the IDMZ.

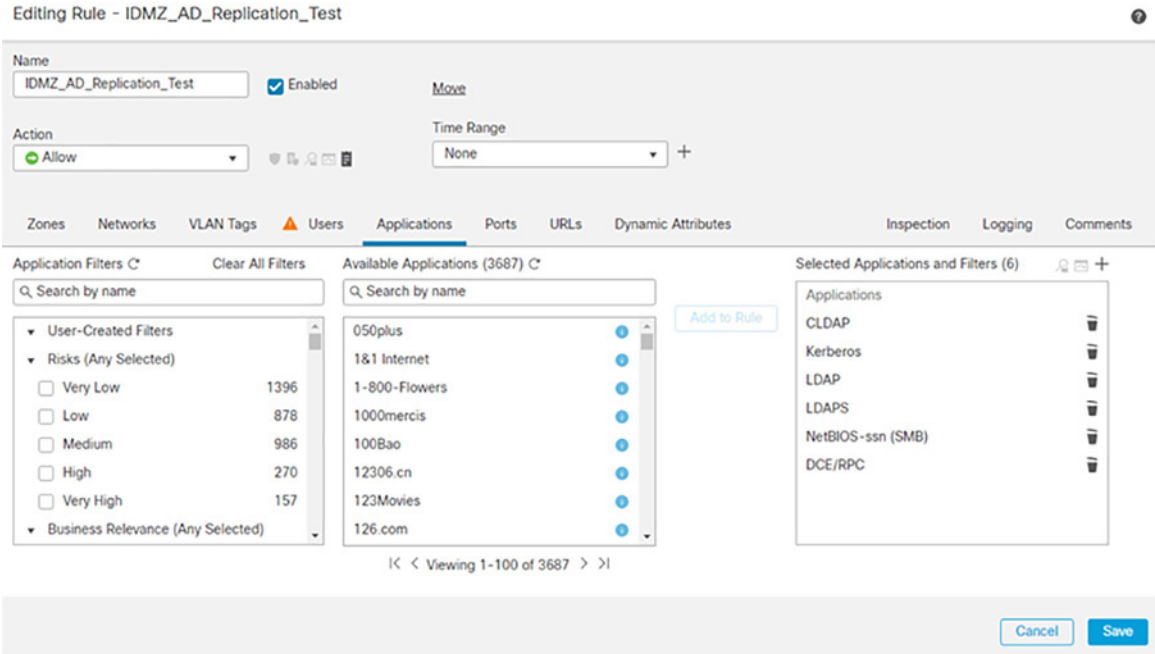
- Step 1 Configure the firewall to allow RPC traffic between the Enterprise and Industrial AD data centers:
- a. In FMC, navigate to **Policies > Access Control**.
 - b. **Edit** the rule assigned to the IDMZ firewall(s).
 - c. Click **+ Add Rule**.
 - d. In the **Zones** tab, click **Enterprise** as the **Source** and **Industrial** as the **Destination**.
 - e. In the **Networks** tab, enter the **Enterprise AD IP Address** object in the **Source Network** and the **Industrial AD IP Address** object in the **Destination Network**.
 - f. In the **Applications** tab, search for **DCE/RPC** and click **Add to Rule**.
 - g. In the **Logging** tab, click **Log at Beginning of Connection** to log connection events to FMC.
 - h. Repeat the rule in the reverse direction (Industrial to Enterprise)

Figure 3-7 IDMZ AD Replication Access Control Rule



Step 2 Configure the firewall to allow additional protocols for replication (Table 3-1). These protocols can be found in the **Applications** tab during policy creation.

Figure 3-8 Adding Additional Protocols for AD Replication



The access rules for AD replication are summarized in Table 3-1..

Table 3-1 Access Rules—AD Replication

Firewall Interface	Source	Destination	Permitted protocols
Industrial	Industrial DC	Enterprise DC	RPC (TCP/UDP port 135)
Enterprise	Enterprise DC	Industrial DC	LDAP (TCP/UDP port 389) LDAP SSL (TCP port 636) CLDAP (UDP port 389) Kerberos (TCP/UDP port 88) SMB (TCP/UDP port 445)

Firewall Rules for AD Authentication in IDMZ

Certain firewall rules should be configured to allow hosts in the IDMZ to authenticate to the Enterprise AD. The examples of the IDMZ hosts are RD Gateway and Reverse Web Proxy servers, anti-virus, Windows Update and other services that are hosted in the IDMZ. These rules are listed in Table 3-2.

Table 3-2 Access Rules—AD Authentication

Firewall Interface	Source	Destination	Permitted protocols
IDMZ	IDMZ hosts that authenticate to AD	Enterprise DC	RPC (TCP/UDP port 135) LDAP (TCP/UDP port 389) LDAP SSL (TCP port 636) LDAP GC (TCP port 3268) LDAP GC SSL (TCP port 3269) Kerberos (TCP/UDP port 88) Kerberos password change (TCP/UDP port 464) SMB (TCP/UDP port 445)

NTP Configuration

This section describe configuration that is required to enable NTP in the CPwE IDMZ architecture.

NTP Synchronization for Network Devices

Network devices use NTP or sometimes SNTP to synchronize their clocks.



Note

For best practices and sample configurations to enable NTP on network devices, refer to the product documentation at:

- <http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html>

NTP Synchronization for Windows Servers

Microsoft Windows Servers use the Windows Time Service to synchronize their clocks. If a server is a domain member, it can receive time information directly from the DC. Otherwise, it can be configured to synchronize with a separate NTP server.



Note

For more information and configuration guidelines, refer to *Windows Time Service Technical Reference* at:

- <https://technet.microsoft.com/en-us/library/cc773061.aspx>

NTP traffic should also be allowed between the Industrial and Enterprise DCs as part of the AD replication.

Firewall Rules for NTP Synchronization

The following steps describe the configuration of firewall rules to allow NTP traffic across the IDMZ (see [Table 3-3](#)):

- Step 1 Configure the firewall to allow NTP synchronization between the Enterprise and Industrial Zone NTP servers, and between the Enterprise and Industrial DCs.
- Step 2 Configure the firewall to allow synchronization (see [Table 3-3](#)) between IDMZ NTP clients (for example, Windows servers and IDMZ access/distribution switches) and the Enterprise Zone NTP server.

Table 3-3 Access Rules—NTP Synchronization

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Industrial NTP server	Enterprise NTP server	NTP (UDP port 123)
Industrial	Industrial DC	Enterprise DC	
IDMZ	NTP clients in IDMZ	Enterprise NTP server	

The access rules can be applied using Cisco FDM or FMC (see [Figure 3-8 on page 3-12](#) in the Active Directory section as an example with FMC).

AAA Services Configuration

Some IDMZ network devices such as switches may need to communicate to the enterprise AAA servers to authenticate network administrators to allow remote login to the device. [Table 3-4](#) lists the firewall rules that should be applied (depending on the AAA protocol in use):

Table 3-4 Access Rules—AAA Traffic

Firewall Interface	Source	Destination	Permitted Protocols
IDMZ	Network devices in the IDMZ	Enterprise AAA servers	RADIUS (UDP port 1812, 1813) TACACS+ (TCP port 49)

ISE Configuration

As part of a distributed ISE setup, the nodes must be able to securely communicate to synchronize their policy configurations and centralize logs. Since ISE nodes exist in both the Industrial and Enterprise Zones, the following steps describe the configuration of the IDMZ firewall rules for the distributed ISE services across the IDMZ (see [Table 3-5](#)).



Note

For information about ISE deployment in the CPwE, refer to the *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at:

- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

**Note**

For more information about ISE services and TCP/UDP ports that the distributed IES system may use, refer to:

- http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/installation_guide/b_ise_InstallationGuide14/b_ise_InstallationGuide14_appendix_01010.html

- Step 1** Configure the firewall to allow the ISE PSN in the Industrial Zone to synchronize its configuration with the PSN/PAN in the Enterprise Zone using HTTPS and JGroups protocols.
- Step 2** Configure the firewall to allow the ISE PSN in the Industrial Zone to send its logs to the ISE MNT in the Enterprise Zone.

Table 3-5 Access Rules—ISE Synchronization and Logging

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Industrial ISE PSN node	Enterprise ISE PSN/PAN node	HTTPS (TCP port 443) JGroups (TCP port 12001)
Enterprise	Enterprise ISE PSN/PAN node	Industrial ISE PSN node	HTTPS (TCP port 443) JGroups (TCP port 12001)
Industrial	Industrial ISE PSN node	Enterprise ISE MNT node	HTTPS (TCP port 443) Secure Syslog (TCP port 6514) UDP port 20514 TCP port 1468

The access rules can be applied using Cisco FMC (see [Figure 3-8 on page 3-12](#) in the Active Directory section as an example).

Cisco Smart Software Manager (SSM) On-Prem Configuration

The following example will present a scenario and show the configuration steps to manage smart licensing in the Industrial Zone using an on-premise licensing server.

**Note**

For details on the configuration of Cisco SSM On-Prem, refer to *Cisco Smart Software Manager On-Prem Installation Guide* at:

- https://www.cisco.com/web/software/286285517/147683/Smart_Software_Manager_On-Prem_7_Installation_Guide.pdf

Installing the Virtual Appliance

- Step 1** Install the virtual appliance on ESXI:
- a. Download the SSM iso file.

- b. Log in to the VMWare vSphere web user interface console.
- c. From the side menu, right-click **Virtual Machine** and then choose **Create/Register VM**.
- d. Choose Create a New Virtual Machine.
- e. Enter the **name** of the VM.
- f. In the **Guest OS Family** drop-down menu, choose **Linux**.
- g. In the **Guest OS Version** drop-down menu, choose **Other Linux (64-bit)**.
- h. Under **CPUs**, select the following settings: **2** or **4 Cores**.
- i. Under **Memory**, configure the **supported memory size** (8 gigabytes are recommended) for your deployment.
- j. Under **New Hard Disk**, configure 200 gigabytes (recommended).
- k. Under **Network**, allocate at least **1 virtual network interface** card.
- l. Under **SCSI Controller**, select **LSI Logic Parallel**.
- m. Under **New CD/DVD Drive**, select **Datastore ISO file**.
- n. Mount the ISO file for Cisco SSM.
- o. Once finished, power on the virtual appliance.

Step 2 Create an account on Cisco SSM:

- a. Open the Cisco SSM On-Prem Administration workspace using the URL:
https://<ip_address>:8443/admin.
- b. When the login screen appears, login using these credentials: admin/CiscoAdmin!2345.



Note

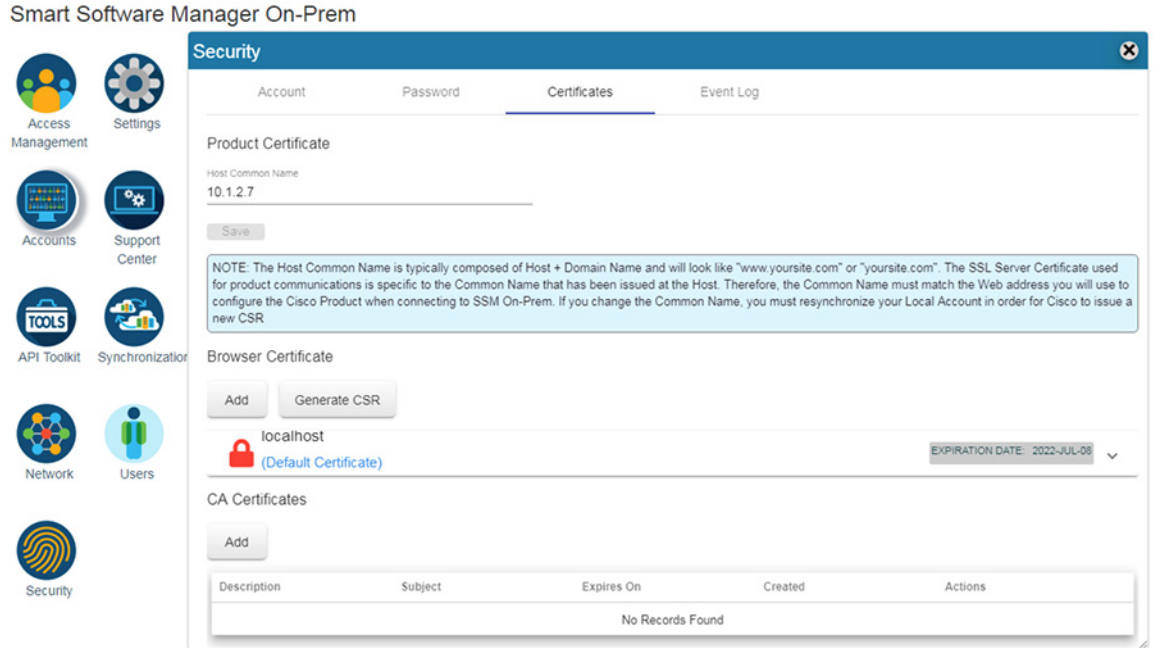
For security reasons, you will be required to immediately change the admin password or disable the account after you create a new local account to be used for administration.

Step 3 Configure the Host Common Name:

The SSM ON-PREM-URL is the Common Name (CN) for the product. The CN is set in the Administration Workspace within the Security Widget, and is entered in the form of a Fully Qualified Domain Name (FQDN), hostname, or IP address of the SSM On-Prem. The CN must match what is used on the product as part of the call home configuration.

- a. In Cisco SSM, open the **Security** Widget.
- b. In the **Certificates** tab, enter the **Host Common Name** (IP Address).
- c. Click **Save**.

Figure 3-9 Adding Certificates to Cisco SSM On-Prem



Step 4 Configure NTP settings.

Currently, you can set the time manually or allow it to synchronize with NTP. The time zone for your SSM On-Prem system can also be set with UTC+0 which allows for all the timestamps to be displayed in UTC time. UTC+offset enables the timestamp to be displayed in the system's local time.

- In Cisco SSM, open the **Settings** Widget and select the **Time Settings** tab.
- Select **Time Zone** from the drop-down menu.
- Turn on **Synchronize with NTP server**.
- Enter the **NTP server address**.
- Click **Synchronize now**.
- Click **Apply**.

Figure 3-10 Cisco SSM On-prem NTP Settings

Settings

< Syslog CSLU Language Email **Time Settings** Message >

Current Time (UTC-0)
Tue, Sep 21 2021 01:35:37

Time Zone
Time Zone
UTC-0

Time Setting (UTC-0)
☐ Manually Set Time
 Date
 9/21/2021
 Hour: 1 Minutes: 35 Seconds: 17

☒ Synchronize With NTP Server

Server Address 1	Port 1	Server Address 2	Port 2
0.centos.pool.ntp.org	123		

☐ Use NTP/Chrony Authentication for Server 1
 ☐ Use NTP/Chrony Authentication for Server 2

[Synchronize Time Now](#)

Apply **Reset**

Step 5 Register On-Prem appliance with Cisco SSM Cloud.

It is necessary to register with Cisco Smart Software Manager (<https://software.cisco.com>) to use the Smart Software Manager On-Prem. To complete this process, ensure you meet the following requirements:

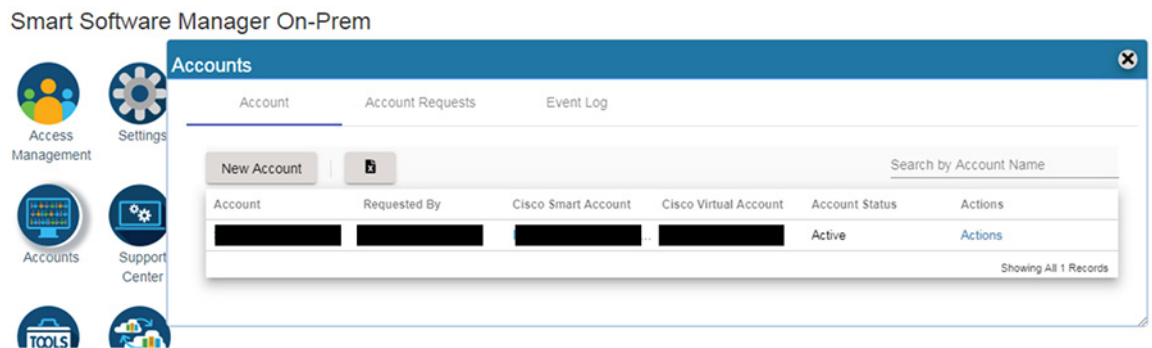
- Access to a Smart Account.
- A valid CCO User ID and Password to access the Smart Account.
- Either Smart Account or Virtual Account access to a Cisco Smart Account.
- Either an eligible existing or new Cisco Virtual Account.

With these requirements met, you will be able to proceed with the registration process by completing these steps to register (request) a local account.

- In Cisco SSM, open the **Accounts** widget.
- Click **New Account**.
- Enter the required information:
 - Local Account Name
 - Cisco Smart Account
 - Cisco Virtual Account

- Email (for notification)
 - d. Click **Submit**.
 - e. The Account request then is listed on the **Account Requests** tab in the **Accounts** widget.
- Step 6 Approving the request:
- a. In Cisco SSM, open the **Accounts** widget.
 - b. In the **Account Requests** tab, select **Approve** under the **Actions** drop-down menu.
 - c. Click **Next**.
 - d. When prompted, enter your **CCO ID credentials** to allow Cisco Smart Account/Virtual Account access on the Cisco SSM.
 - e. Click **Submit**.
 - f. Verify that the local Account is listed as **Active** under the **Accounts** tab.

Figure 3-11 Account Management in Cisco SSM On-prem



Step 7 Synchronization with the Cloud.

Online synchronization assumes there is an Internet connection to Cisco Smart Software Manager from SSM On-Prem. On each local Account, you can choose to perform either a Standard Synchronization Now action or Full Synchronization Now action. Manual synchronization is used when the customer network is not connected to the Internet. For details on that deployment see Smart Software Manager On-Prem Installation Guide.

- a. In **Cisco SSM**, click the **Synchronization** Widget.
- b. On the local **Account**, under **Actions**, select **Standard Synchronization Now** or **Full Synchronization Now**.
- c. Enter your **Cisco Smart Account** credentials.
- d. Click **OK**.

Configuring Firewall Rules for Cisco SSM On-Prem

The following steps describe the configuration of firewall rules for the Cisco SSM On-Prem to allow Industrial Clients to get licensed behind the IDMZ.

**Note**

If using a web proxy in the IDMZ a rule should already exist in the firewall for the web proxy to forward all HTTPS towards the enterprise zone.

- Step 1** Configure the firewall to allow Cisco SSM On-Prem to synchronize with the Cloud and for clients to access Management portal from Enterprise zone (see [Table 3-6](#)).

Table 3-6 Required Access Rules—Cisco SSM On-Prem to Cisco SSM Cloud—1

Firewall Interface	Source	Destination	Permitted Protocols
IDMZ	Cisco SSM On-Prem	Cisco SSM Cloud	HTTPS (port 443)
Enterprise	Enterprise Client	Cisco SSM On-Prem	HTTPS (port 443)

- Step 2** Configure firewall to allow Industrial Clients to register with Cisco SSM On-Prem (see [Table 3-7](#)).

Table 3-7 Required Access Rules—Cisco SSM On-Prem to Cisco SSM Cloud—2

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Industrial Client software	Cisco SSM On-Prem	HTTPS port 443)

WSUS Configuration

This section describe configuration that is required to enable WSUS in the CPwE IDMZ architecture.

Deploying WSUS

For information and configuration guidelines for planning and deploying WSUS refer to:

- <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services>

In this design guide, the WSUS server in the IDMZ was set to automatically collect updates from Microsoft Update and for Industrial zone updates to be installed manually.

Firewall Rules for WSUS

To get updates from Microsoft Update, the WSUS server uses port 443 for the HTTPS protocol. It is assumed for this design guide that all traffic traversing port 80/443 will do so through a web proxy and therefore no additional firewall rules need to be deployed for the outbound interface.

For clients connecting from the Industrial zone to the WSUS, the following is required:

- Step 1** Configure the firewall to allow Windows clients to pull updates from the WSUS (see [Table 3-8](#)).

Table 3-8 Required Access Rules—Windows Clients to WSUS Server

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Industrial Client software	Cisco SSM On-Prem	HTTPS port 443)

Configuring Data Transfer through IDMZ

This section describes validated configurations that allow essential data to traverse the IDMZ between the Enterprise and Industrial Zones as described in [System Design Considerations](#).

The following configuration steps are covered in this section:

- PI-to-PI Interface configuration and firewall rules for FactoryTalk Historian data transfer
- Firewall rules for secure managed file transfer using SolarWinds Serv-U solution as an example

FactoryTalk Historian Data Transfer Configuration

This section provides necessary steps to enable FactoryTalk Historian data transfer across the IDMZ.



Note

For general information about FactoryTalk Historian installation and configuration, refer to:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/in/hse-in025_-en-e.pdf

PI to PI Interface Configuration

An overview of PI-to-PI installation and configuration steps is provided here.



Note

For complete information, refer to the following documents:

- *FactoryTalk Historian to Historian Interface Installation and Configuration Guide*:
 - http://literature.rockwellautomation.com/idc/groups/literature/documents/in/h2h-in001_-en-e.pdf
- *FactoryTalk Historian to Historian Interface User Guide*:
 - http://literature.rockwellautomation.com/idc/groups/literature/documents/um/h2h-um001_-en-e.pdf

- Step 1 Install the FactoryTalk Services platform on the PI to PI server in the IDMZ.
- Step 2 Install FactoryTalk Historian To Historian Interface (PI-to-PI Interface) on the PI-to-PI server in the IDMZ.
- Step 3 Obtain a PI-to-PI license activation file and activate the interface using FactoryTalk Activation Manager. Assign the license activation to the target server using the FactoryTalk Administration Console.

Step 4 Create a PI-to-PI Interface Instance in the Interface Configuration Utility (ICU).

- Go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility**. The ICU dialog box appears.
- Select **Interface > New Windows Interface Instance** from EXE. Click **Browse** to locate the executable file for the PI-to-PI Interface, for example *C:\Program Files (x86)\Rockwell Software\FactoryTalk Historian\PIPC\Interfaces\FTPtoPI\FTPtoPI.exe*.
- Under Host PI Server/Collective, select the **Enterprise Zone Historian server**. Complete the following information and then click **Add**.

Under:	Type:
Point Source	FTSS
Interface ID	1
Service ID	1

- Under Scan Classes, create one scan class at a 15 second frequency.
- In the PI-to-PI sub menu, go to the **Required** tab, and type the **Source host**, which is the Industrial Zone FactoryTalk Historian SE server. It may be either a DNS name or an IP address.
- In the **Service** tab, click **Create**.

Step 5 Create a **Test Target Point** on the Enterprise FactoryTalk Historian server.

- Go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > System Management Tools**. The System Management Tools dialog box appears.
- Under **Collectives and Servers**, select the **Enterprise Zone FactoryTalk Historian server**.
- Under **System Management Tools**, select **Points > Point Builder**. Click the toolbar icon to create a new point.
- In the **General** tab, complete the following information:

Under:	Type:
Name	MyTempTag
Point Source	FTSS
Exdesc	STAG=BA.Temp.1

- In the **Classic** tab, complete the following information:

Under:	Type:
Location1	1 (This is the interface ID as specified in the ICU)
Location4	1

- Save the point.

Step 6 In order for the PI-to-PI Interface to be allowed to interact with either one of the FactoryTalk Historian Servers, a trust has to be created for its executable. Configure an application trust for FTPITOPi.exe with the Pladmin user on the Enterprise FactoryTalk Historian server.

- On the **Enterprise FactoryTalk Historian SE Server**, go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > System Management Tools**. The System Management Tools dialog box appears.
- Under **Collectives and Servers**, select the **Enterprise Zone FactoryTalk Historian server**.

- c. Under **System Management Tools**, select **Security > Mappings & Trust**. Go to the Trusts tab. Click **New Trust** in the toolbar and then click **Advanced**.
- d. In the **Add New Trust** dialog box, provide the following information:

Item name	Description
Trust Name	PI_to_PI_Trust
IP Address	IP address of the server with the PI to PI interface installed
Netmask	255.255.255.255
Application Information	Ftpitopi.exe
PI Identity	In the PI User dialog box, select PIAdmin

Step 7 Configure an application trust for FTPITOPi.exe with the PIadmin user on the Industrial Zone FactoryTalk Historian server. The steps are same as for the Enterprise server above.

Step 8 Start and verify the PI-to-PI Interface:

- a. Go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility**. The ICU dialog box appears.
- b. Under **Interface**, select the interface you have just created. On the toolbar, click **Start**. The status of the interface at the bottom of the dialog box should change to Running.
- c. To verify that the PI-to-PI Interface is working properly, you need to check whether the current values of the tag at the Industrial Zone and Enterprise Zone FactoryTalk Historian servers match each other. This can be done using System Management Tools by selecting **Data > Current Values** and searching for the tag.

Firewall Rules for FactoryTalk Historian Data Transfer

The following steps describe the configuration of firewall rules to allow FactoryTalk Historian data across the IDMZ using a PI-to-PI Interface (see [Table 3-9](#)).

- Step 1** Configure firewall to allow incoming connections from the Industrial Zone Historian to the PI-to-PI server using PI Server Client protocol (TCP port 5450) and RPC (TCP port 135).
- Step 2** Configure firewall to allow incoming connections from the Enterprise Zone Historian to the PI-to-PI server on the same ports.
- Step 3** Configure firewall to allow incoming connections from the PI-to-PI server to both Historians.

Table 3-9 Access Rules—Historian Data Transfer

Firewall Interface	Source	Destination	Permitted protocols
Industrial	Industrial Zone Historian	PI to PI server	PI Server Client Access
Enterprise	Enterprise Zone Historian	PI to PI server	(TCP port 5450)
IDMZ	PI to PI server	Industrial Zone Historian Enterprise Zone Historian	RPC (TCP port 135)

In addition to Steps 1-3, the PI-to-PI server needs to authenticate to the DC through the firewall, therefore it should be included in the list of IDMZ hosts that are allowed to do so (see Active Directory Configuration sections).

Secure File Transfer Configuration

To facilitate secure file transfer (SFT) between the Enterprise and Industrial Zones via the IDMZ, many implementations are available to choose from.

In the context of the IDMZ, a client based in the Industrial Zone can upload to and download files from the SFT Server (located in the Enterprise Zone) via the Gateway (located in the IDMZ). As per IDMZ best practices, no direct connections are opened between the Industrial and Enterprise Zones, and no data resides permanently in the IDMZ. In a similar manner, an enterprise client can upload to and download files from the Industrial SFT Server via the IDMZ Gateway.

The following steps describe the configuration of firewall rules to allow SFT services across the IDMZ, using FTP as the mode of transport (see Table 3-10 and Table 3-11):

- Step 1 Configure the firewall to allow incoming client connections from the Industrial Zone clients to the IDMZ-based gateway server. The clients use the FTP protocol, which can be configured in an application rule.
- Step 2 Configure the firewall to allow incoming client connections from Enterprise Zone clients to the IDMZ-based gateway server. The clients use the FTP protocol.



Note If using SFTP for file transfer, the connection must be decrypted so the file contents can be checked. For information on doing decryption using Cisco FTD. See Understanding Traffic Decryption at: https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/understanding_traffic_decryption.html

Table 3-10 Access Rules—Managed File Transfer Industrial to Enterprise

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Any (or specific clients in Industrial Zone)	SFT Gateway in IDMZ	FTP, SFTP

Table 3-11 Access Rules—Managed File Transfer (Serv-U) Enterprise to Industrial

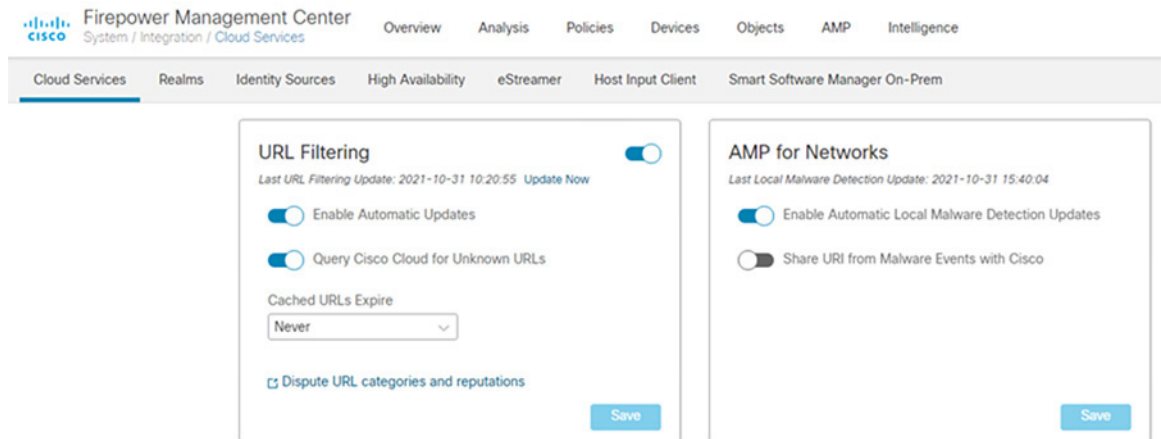
Firewall Interface	Source	Destination	Permitted Protocols
Enterprise	Any (or specific clients in Enterprise Zone)	MFT Gateway in IDMZ	FTP, SFTP

The access rules can be applied using Cisco FMC web interface (see Figure 3-8 on page 3-12 in the Active Directory section as an example).

- Step 3 Connect to the AMP Cloud.
 - a. In FMC, navigate to **System > Integration**.

- b. Click **Cloud Services**.
- c. Select **Enable Automatic Local Malware Detection Updates** to stay up to date with the latest signatures updates.
- d. Configure the firewall to allow outgoing connections from the IDMZ to the cloud. By default, Firepower uses port 443/HTTPS to communicate with the AMP public cloud to obtain file disposition date. Note: If using a web proxy in the IDMZ, forward all traffic through the web proxy.

Figure 3-12 FMC URL Filtering Updates



Step 4 Create a File Policy:

- a. In FMC, navigate to **Policies > Access Control > Malware & File**.
- b. Click **New File Policy**.
- c. Give a **Name** and optional **Description**. Click **Save**.
- d. Click **+ Add Rule**.
- e. In the **Action** drop down list, choose **Block Files**.
- f. Under **File Type Categories**, click all categories you wish to block and click **Add**.



Note

Note: The order of precedence of file-rule action is:

- Block Files
- Block Malware
- Malware Cloud Lookup
- Detect Files

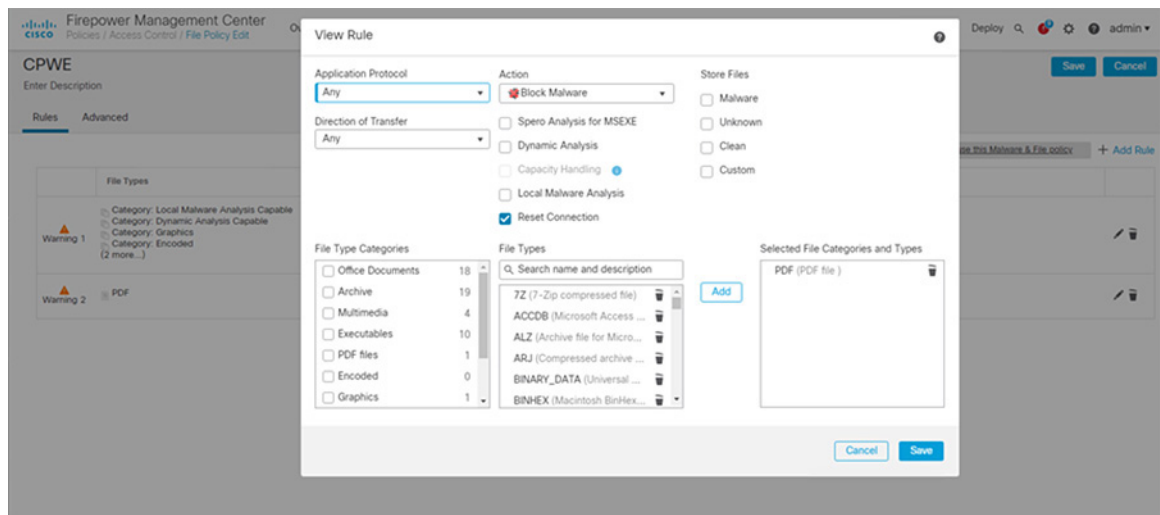
- g. Click **Save**.
- h. Click **+ Add Rule**.
- i. In the **Action** drop down list, choose **Block Malware**.

**Note**

Block Malware rules allow you to calculate the SHA-256 hash value of specific file types, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

- j. Under **File Type Categories**, click all categories you wish to allow into the Industrial zone and click **Add**.
- k. Click **Save**.

Figure 3-13 FMC File Policy

**Step 5** Add File Policy to Access Control Rule:

- a. In FMC, navigate to **Policies > Access Control**.
- b. Edit the access control rule created earlier for allowing FTP.
- c. Go to the Inspection tab, and in the **File Policy** drop down menu, choose the File Policy created in Step 4.
- d. Click **Save**.
- e. **Save** the policy and **Deploy** changes.

Figure 3-14 Editing Access Rule in FMC for FTP

Editing Rule - FTP

Name: FTP ☒ Enabled [Move](#)

Action: Allow Time Range: None

Zones Networks VLAN Tags **Users** Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Intrusion Policy: None Variable Set: Default Set

File Policy: CPWE

[Cancel](#) [Save](#)

Configuring Remote Access Services

This section describes validated configurations that allow remote users securely access desktop applications that are hosted in the Industrial Zone via the IDMZ.

The following configuration steps are covered in this section:

- SSL VPN Configuration
 - Client-based SSL VPN (Cisco AnyConnect) to the Enterprise firewall
- Microsoft RD Gateway configuration
- ThinManager RD Gateway Configuration
- DUO SFT Authentication

SSL VPN Configuration

This section provides configuration steps for the firewall to implement SSL VPN access for remote users.

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_remote_access_vpns.html



Note

Additional information about VPN configuration on the FTD can be found in *Remote Access VPNs for Firepower Threat Defense* at:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_remote_access_vpns.html

Client-based SSL VPN Configuration

The following steps describe the configuration of client-based (Cisco AnyConnect) SSL VPN on the **Enterprise edge firewall** to allow remote access from the Internet.

- Step 1 Load the AnyConnect client images to the FMC (images are downloaded from Cisco):
- In FMC, navigate to **Objects > Object Management**.
 - Click on **VPN > AnyConnect File**.
 - Click **Add AnyConnect File**.
 - Give a meaningful name to the AnyConnect File, add the headend package using the **Browse** button, and on the **File Type** drop down menu click **AnyConnect Client Image**.
 - Repeat for all packages that have been downloaded (Windows, Mac, etc.).

Figure 3-15 Loading AnyConnect Files in FMC

The screenshot shows a web-based form titled "Add AnyConnect File". It contains the following fields and controls:

- Name:** A text input field containing "AC-4.10-win".
- File Name:** A text input field containing "anyconnect-win-4.10.01075-webdeploy". To its right is a blue button labeled "Browse..".
- File Type:** A dropdown menu with "AnyConnect Client Image" selected.
- Description:** An empty text input field.
- Buttons:** At the bottom right, there are two buttons: "Cancel" (light blue) and "Save" (dark blue).

- Step 2 Add Duo Authentication Proxy as RADIUS Server in FMC:
- In FMC, navigate to **Objects > Object Management > AAA Server > RADIUS Server Group**.
 - Click **Add RADIUS Server Group**.
 - Give a meaningful name to the server group and add the **IP Address/Hostname** where the Duo Authentication Proxy resides.
 - Click **Save**.

Figure 3-16 Add RADIUS Server to FMC

The screenshot shows the 'Add RADIUS Server Group' configuration window. The fields are as follows:

- Name: IDMZ_Duo_Auth_Proxy
- Description: (empty)
- Group Accounting Mode: Single
- Retry Interval: 10 (1-10) Seconds
- Realms: (empty)
- Enable authorize only: ☐
- Enable interim account update: ☐
- Interval: 24 (1-120) hours
- Enable dynamic authorization: ☐
- Port: 1700 (1024-65535)
- RADIUS Servers (Maximum 16 servers):

IP Address/Hostname
192.168.1.4

At the bottom are 'Cancel' and 'Save' buttons.

Step 3 Create VPN Address Pool:

- In FMC, navigate to **Objects > Object Management > Address Pools > IPv4 Pools**.
- Click **Add IPv4 Pools**.
- Give a meaningful name to the address pool and add the **IPv4 Address Range** you wish to assign to VPN users.
- Click **Save**.

Figure 3-17 Editing IPv4 address pool for remotes access VPN

Edit IPv4 Pool

Name*
IDMZ-VPN-POOL

IPv4 Address Range*
10.0.0.3-10.0.0.10
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask
255.255.255.0

Description

☒ Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

Cancel Save

Step 4 Add a VPN Split Tunnel List:

- a. In FMC, navigate to **Objects > Object Management > Network**.
- b. In the **Add Network** drop down, click **Add Object**.
- c. Add the **Network** subnet that you would like roaming users to reach through the tunnel. In this design guide, roaming users will only use the VPN tunnel to access private subnets.
- d. Repeat for each subnet or host that you would like to be reachable by roaming users.

Figure 3-18 Configuring Network Range for Split Tunnel Configuration

Edit Network Object

Name
IDMZ_Subnet

Description

Network
☐ Host ☐ Range ☒ Network ☐ FQDN

192.168.128.0/24

☐ Allow Overrides

Cancel Save

- Navigate to **Objects > Object Management > Access List > Standard**.
- Click **Add Standard Access List**.
- Give a meaningful name to the split tunnel and add the network object(s) from the previous steps.
- Click **Save**.

Figure 3-19 Editing Access List for VPN Access

Edit Standard Access List Object

Name
IDMZ_TunnelList

▼ Entries (1)

Add

Sequence No	Action	Network
1	Allow	IDMZ_Subnet

☐ Allow Overrides

Cancel Save

Step 5 Complete the AnyConnect VPN wizard:

- a. In FMC, navigate to **Devices > VPN > Remote Access**.
- b. Click **Add**.
- c. Add a meaningful name and click the **FTD(s)** that this policy will apply. Click **Next**.
- d. Under **Authentication Server**, choose the **Duo Authentication Proxy** that was configured in a previous step.
- e. Add the **IPv4 Address Pool** that was created for VPN users.
- f. Under **Group Policy**, click +.
- g. Give a meaningful name to the policy.
- h. In the **General > DNS/WINS** tab, add the DNS server for the internal network. Note: If this network object does not already exist in FMC, it can be added using the + button.
- i. In the **General > Split Tunneling** tab, click **IPv4 Split Tunneling** drop down and choose **Tunnel networks specified below**. Repeat for IPv6 if applicable.
- j. Under **Standard Access List**, choose the Split Tunneling list that was created in a previous step. This will ensure that only the traffic that has been specified will use the tunnel.
- k. Under **DNS Request Split Tunneling**, click **DNS Requests** drop down and choose **Send only specified domains over tunnel**.
- l. Enter the domain list for the internal network. All other DNS requests will be sent to Umbrella (when configured).
- m. Click **Next** on the Remote Access VPN wizard.
- n. Select the AnyConnect Client images that were uploaded in a previous step. Click **Next**.
- o. On the **Interface group/Security Zone** drop-down menu, choose the FTD interface that users will access for VPN connections.
- p. In the **Certificate Enrollment** drop-down menu, choose the device certificate that will be used to authenticate the VPN gateway. Note: This design guide used a self-signed certificate that was created using the + button.
- q. Click **Next**.
- r. Validate the policy information and click **Finish**.
- s. Click **Deploy** to send remote access policy to the FTD.

**Note**

While out of scope for this guide, it is recommended to create access control rules on the firewall to limit access to VPN users. This can be achieved by using the IPv4 address pool reserved for VPN users and creating an allow list of services they should be able to reach on the network.

Microsoft Remote Desktop Gateway Configuration

The following example will present a scenario and show the configuration steps to achieve the requirements. It is assumed that the user has completed the initial setup of the RD Gateway role server in the IDMZ.

**Note**

For details on the configuration of the RD Gateway feature on the Microsoft Windows Server, refer to *Deploying Remote Desktop Gateway Step-by-Step Guide* at:

- <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-build-and-deploy>

Defining User Groups and Remote Access Rules

In our scenario, we have the following actors shown in [Table 3-12](#) that will be assigned to the following Active Directory User Groups:

Table 3-12 Users and User Groups

User	User Group	Role
Oscar Operator	Operators	Monitors production equipment to support the IACS process
Martha Maintenance	Maintenance	Maintains Industrial Zone assets related directly to production systems
Ed Engineer	Engineers	Defines, configures, maintains Industrial Zone assets related directly to production systems
Alice Admin	Production Administrators	Defines, configures, maintains Industrial Zone software assets that contain common enterprise software such as Antivirus, OS patches, etc.
Beth Oemone	OEM 1	Trusted Partner: a non-employee resource that is working for the company that needs access to certain assets.
Bob Oemtwo	OEM 2	
Maintenance, Engineers, Production Administrators, OEM1, OEM2	IDMZ RDG Users	This group contains all user groups that can have access to Industrial Zone resources via RD Gateway

We will now define the Industrial Zone assets each AD user group will be allowed to access through the RD Gateway. Duo Authentication for Remote Desktop Gateway adds two-factor authentication to your RemoteApp Access logons and blocks any connections to your Remote Desktop Gateway server(s) from users who have not completed two-factor authentication when all connection requests are proxied through a Remote Desktop Gateway. Users automatically receive a 2FA prompt in the form of a push request in Duo Mobile or a phone call when logging in. This configuration does not support passcodes or inline self-enrollment.

Installing Duo's RD Gateway plugin disables Remote Desktop Connection Authorization Policies (RD CAP) and Resource Authorization Policies (RD RAP). The CAPs and RAPs become inaccessible from the Remote Desktop Gateway Manager and previously configured policy settings are ignored by Remote Desktop Gateway. If operational requirements mandate continued use of RD CAPs/RAPs, you may want to consider installing Duo for Windows Logon at your RDS session hosts instead.

With this in mind, the remainder of the document will focus on the use of RD CAPs/RAPs. For prerequisites, installation instructions and troubleshooting tips for MFA with the RD gateway, see Duo Authentication for Microsoft Remote Desktop Gateway on Windows 2012 or later.

Now that we have defined the computer groups, users, user groups and what each group is authorized to access through the RD Gateway, we will show the configuration steps to meet these requirements.

It is worthwhile mentioning that FactoryTalk Security is discussed in this guide as a means to secure Rockwell Automation applications. Application security can also be achieved by limiting the applications available to each user or user group(s) desktop.

Configuring Active Directory

Before we configure the RD Gateway, we want to leverage the AD users and groups we have planned in the previous section so configuring these users within AD is our first step. The section assumes the reader has some familiarity with AD and how to create users, user groups and computer groups.

**Note**

For more detailed information on the Microsoft AD functionality, refer to *Active Directory Users and Computers* at:

- [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/c754217\(v=ws.11\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/c754217(v=ws.11)?redirectedfrom=MSDN)

-
- Step 1 Create AD users and groups as described in Table 17 using the Active Directory Users and Computers management console.
- a. Create AD users groups (Operators, Engineers, Maintenance, OEM1, OEM2 and ProdAdmins).
 - b. Create AD users and assign to the corresponding groups.
 - c. Create an AD group that will be allowed to access Industrial Zone assets. In our example it will be named IDMZ RD Gateway Users.
 - d. Add user groups from Step 1 (Engineers, Maintenance, OEM1, OEM2 and ProdAdmins) to the IDMZ RD Gateway Users group.
 - Note that the Operators group will not be added since our policy does not allow remote access for operators.
- Step 2 Create computer groups as described in Table 3-12.
- a. Create IDMZ RD Gateway Remote Hosts computer group.
 - b. Add the IACS Terminal Server (TERM01) to the IDMZ RD Gateway Remote Hosts group.
 - c. Create IACS Hosts computer group that will contain Industrial Zone assets for remote access.
 - d. Add the appropriate servers to the IACS Hosts group per Table 3-12. The exact list of servers for remote access will depend on the environment and business needs.
-

Configuring RD Gateway Policies

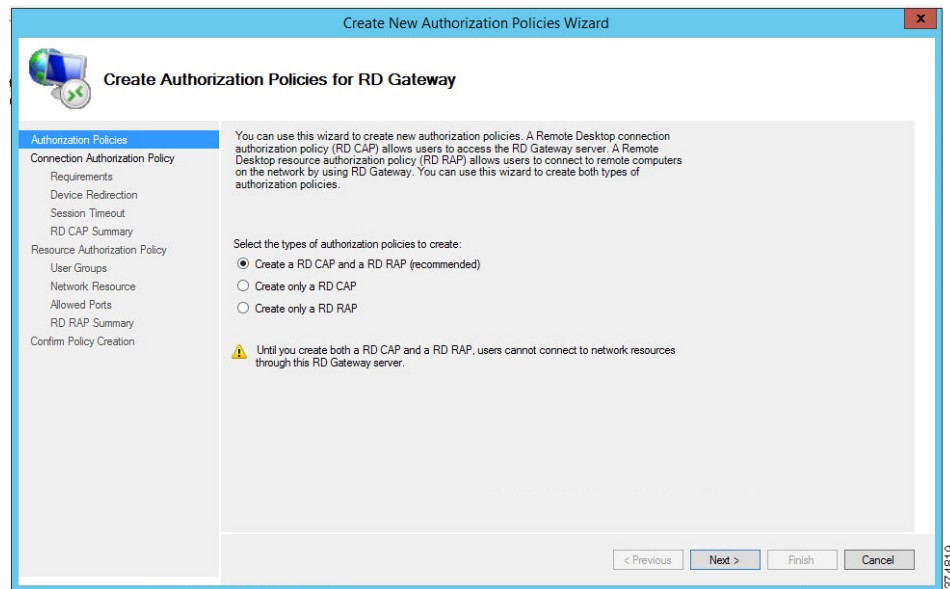
After defining remote access rules and creating corresponding users, user groups and computer groups in the AD, the administrator should configure the RD Gateway policies (CAPs and RAPs) to match the rules.

In our example, we will configure two CAPs and RAPs to support the scenario in Table 3-12.

- A CAP and RAP will exist to allow users to connect to the terminal server in the Industrial Zone.
- A CAP and RAP will also exist to allow Production Administrators and Engineers to access all the IACS servers.

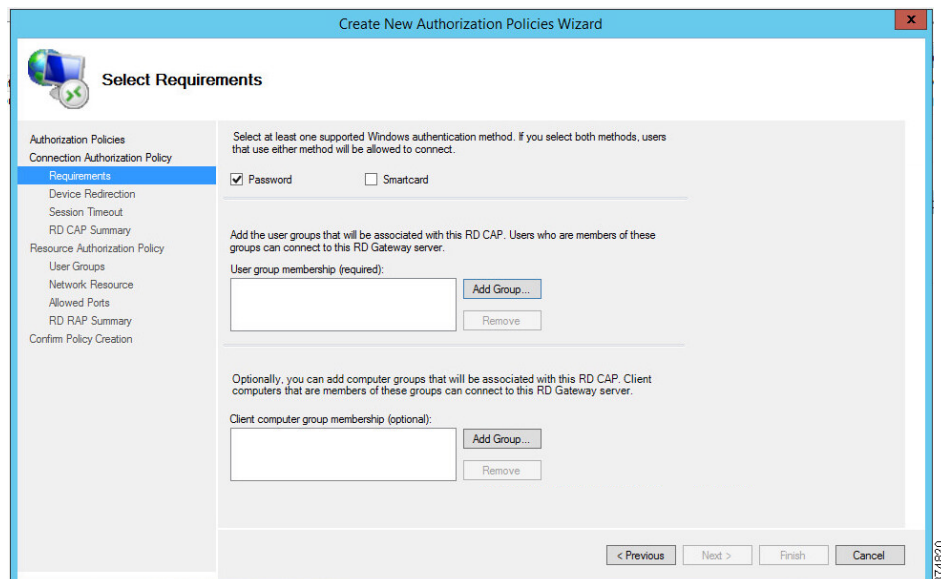
- Step 1 Configure IDMZ RDG Remote Host CAP using the RDG Manager. The IDMZ RDG Remote Host scenario will allow the authorized users to access the terminal server in the Industrial Zone.
- From the **RDG Manager**, the **Policies** folder and select **Create New Authorization Policies**. In the dialog box (see [Figure 3-20](#)), select **Create RD CAP** and a **RD RAP** (recommended) and then click **Next**.

Figure 3-20 RDG Policy Wizard



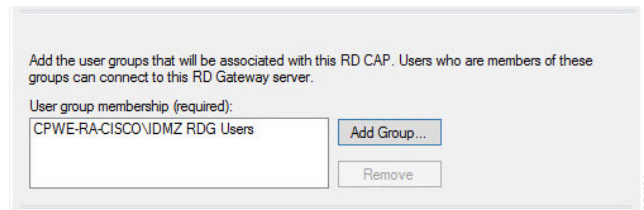
- Name the CAP as **IDMZ RDG CAP** and then click **Next** to proceed to the Requirements page.
- Each CAP allows the administrator to select a Password, a Smartcard or both as an authentication method. In our example, we are allowing the user to use a password (see [Figure 3-21](#)).

Figure 3-21 CAP Requirements - Authentication Method



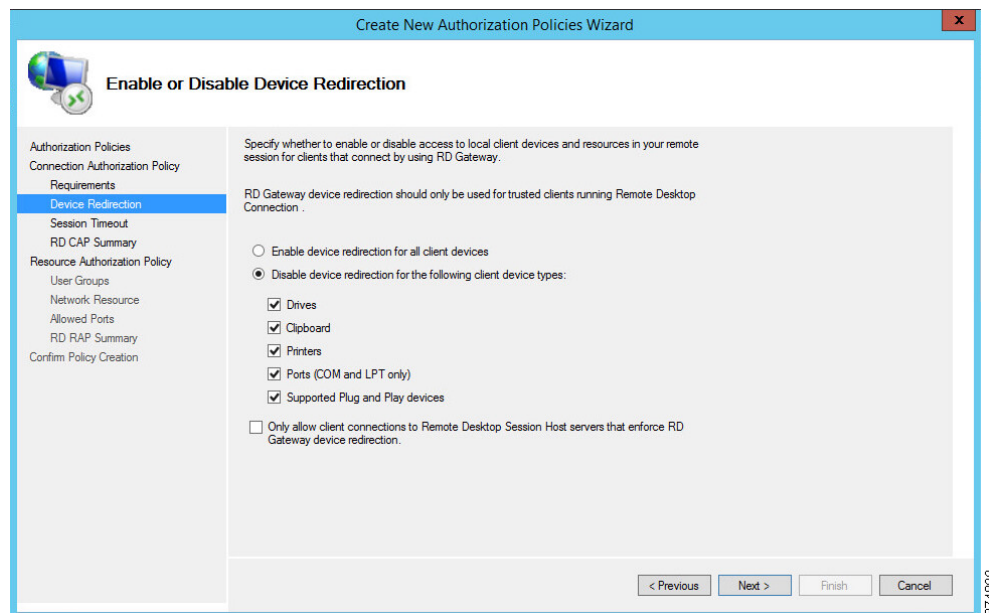
- d. With the Password option selected, we will now add user groups that will be associated with this CAP. Click **Add Group** in the **User Group Membership** section. In the **Selection Group** dialog box, find and select **IDMZ RDG Users** group to associate it with the RDG CAP (see [Figure 3-22](#)). Click **Next**.

Figure 3-22 CAP Requirements—User Group



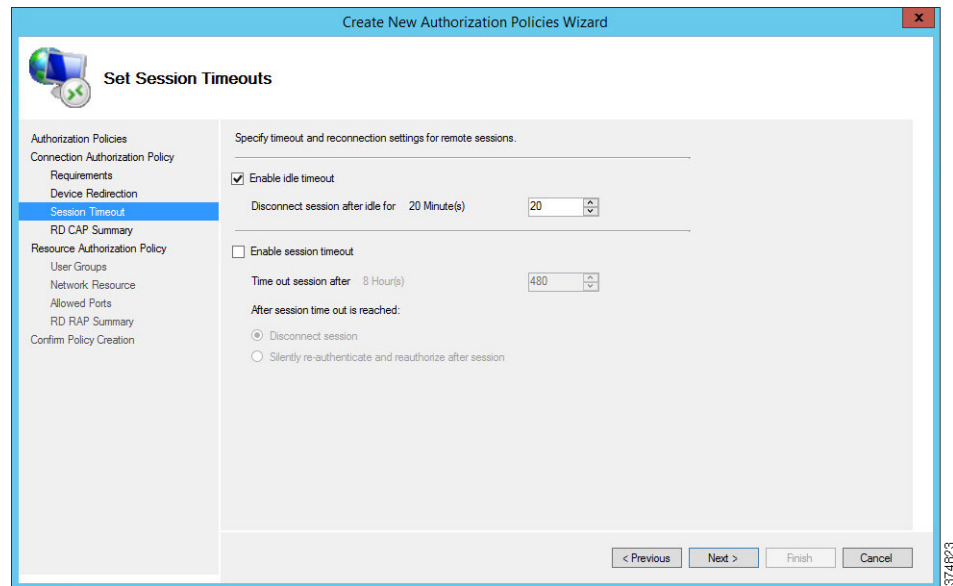
- e. The CAP also allows the administrator to enable or disable device redirection. Device redirection controls access to devices and resources on a client computer in RDP sessions. For instance, Drives redirection specifies whether to prevent the mapping of client drives in an RDP session. For our example, we will disable device redirection to bolster security (see [Figure 3-23](#)). After disabling device redirection, click **Next** to continue.

Figure 3-23 CAP - Device Redirection



- f. The CAP allows the administrator to specify idle timeout and automatic session disconnection. In our example, we have chosen to disconnect if the session has been idle for 20 minutes. Your security policy will dictate the idle timeout and session timeout parameters. After the timeout parameters have been entered, click **Next** to continue.

Figure 3-24 CAP—Idle and Session Timeouts

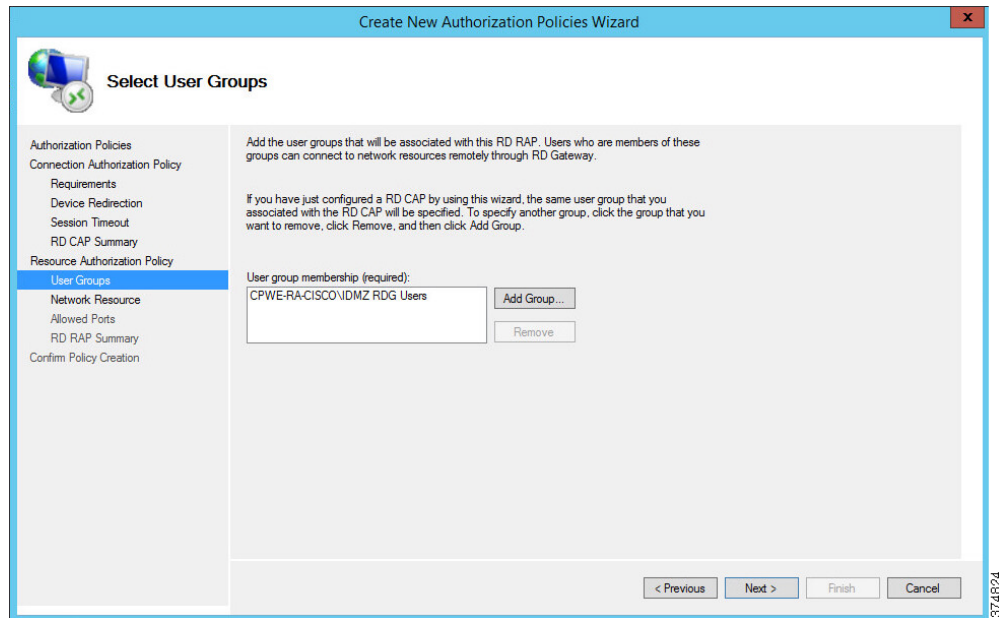


- g. Once the CAP configuration steps are completed, the administrator can review the entire details of the configuration before submitting the content.

Step 2 Configure IDMZ RDG Remote Host RAP using the RDG Manager. The RAP will specify what resources the authorized remote users can access in the Industrial Zone.

- a. In Step 1, we completed our CAP configuration. We will now continue the wizard to configure a Resource Authorization Policy. Name the RAP as **IDMZ RDG RAP** and then click **Next**.
- b. The RAP allows the administrator to specify the user groups that can have access to the Industrial Zone resources. We specified the IDMZ RDG Users group in the CAP so the RAP is prepopulated with the same group (see [Figure 3-25](#)). This group will be allowed to access the terminal server in the next step. Click **Next** to continue.

Figure 3-25 RAP—User Groups



- c. The Network Resource page allows the administrator to specify the network resources that the IDMZ RDG Users can access. Previously, we defined a computer group named IDMZ RDG Remote Hosts that included our terminal server TERM01. Click Browse, find and select IDMZ RDG Remote Hosts computer group to add to this RAP (see [Figure 3-26](#) and [Figure 3-27](#)).

Figure 3-26 RAP—Network Resources

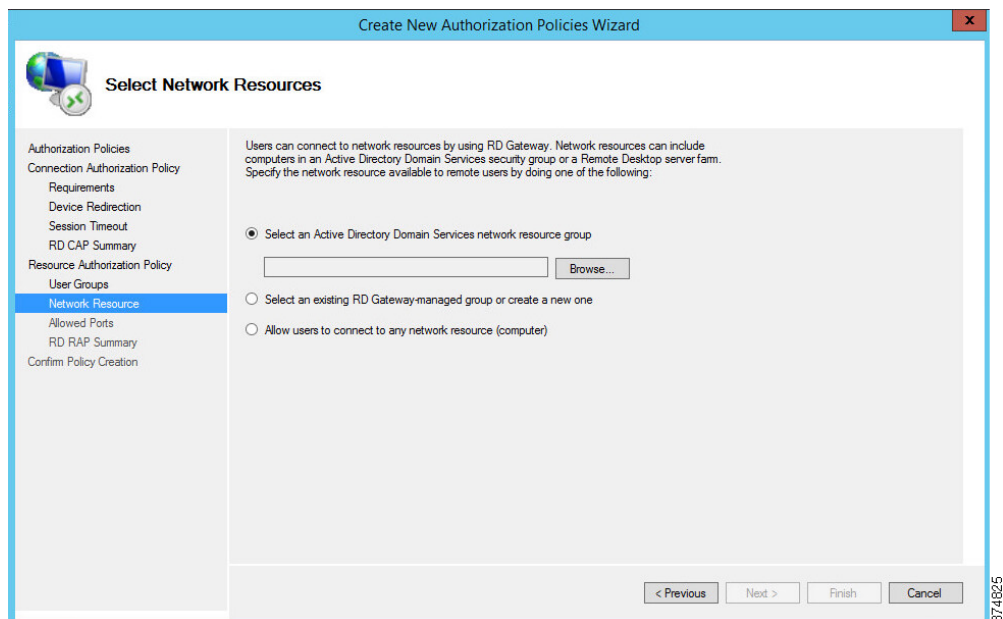
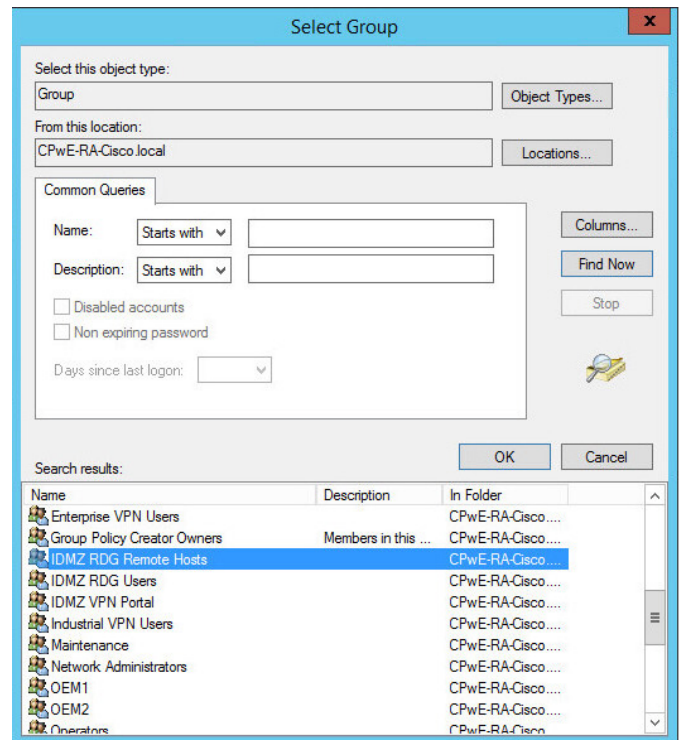
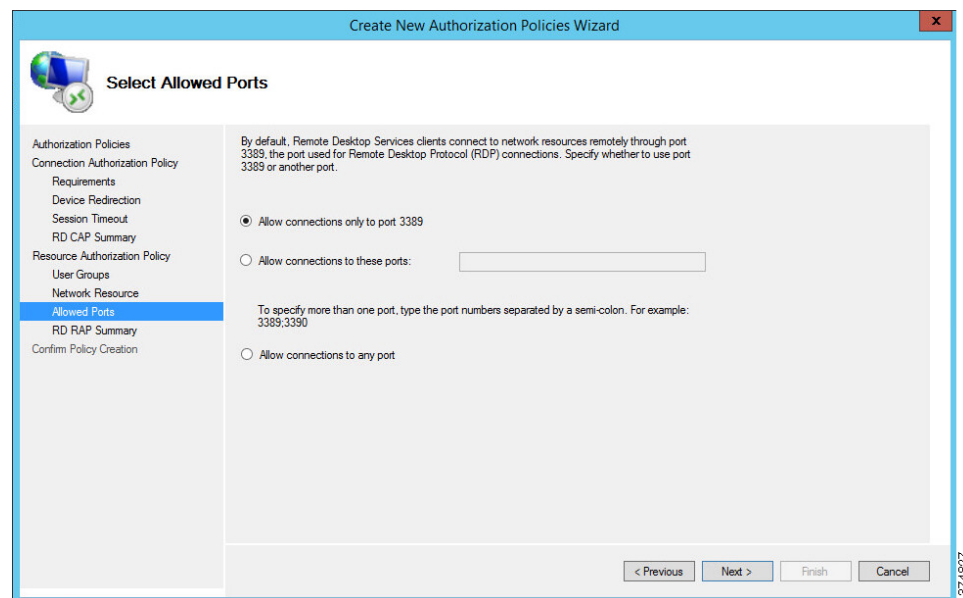


Figure 3-27 RDG Remote Hosts Computer Group



- d. By default, the RDG connects to IACS resources on port 3389 (RDP). For this example, we have not changed the default connection port number (see Figure 3-28). If a different port or group of ports is selected, make sure that the firewall rules reflect that. Click **Next**.

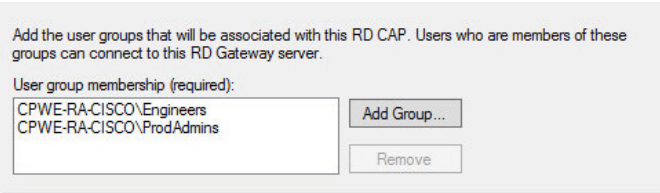
Figure 3-28 RAP—Allowed Ports



- e. The CAP and RAP configuration is now complete. In Steps 1 and 2, we defined policies for remote access to the terminal server in the Industrial Zone via RD Gateway.

- Step 3 Configure IACS Remote Host CAP using the RD Gateway Manager. The IACS Remote Host scenario will allow the production administrators and engineers to access the Industrial Zone servers in the IACS Hosts group (Table 19). Configuration of this CAP is similar to Step 1.
- Start the wizard to create a new CAP and a RAP. In our example, the CAP will be named **RDG IACS Remote Hosts CAP**.
 - Select the authentication method (password or smartcard) depending on the security policy.
 - Add user groups that will be associated with this CAP. In our example, **Engineers and ProdAdmins** groups will be selected.

Figure 3-29 Remote Host CAP User Groups



- Configure Device Redirection policy to control access to devices and resources on a client computer in remote desktop sessions. For our example, we will disable device redirection to bolster security.
 - Specify idle and session timeout parameters.
- Step 4 Configure IACS Remote Host RAP using the RDG Manager after the CAP is created. Configuration of this CAP is similar to Step 2.
- Name the policy (**RDG IACS Remote Hosts RAP** is used in our example).
 - Same user groups that we associated in the CAP should be prepopulated in the RAP. In our example, Engineers and ProdAdmins groups will have access to the Industrial Zone resources.
 - Specify the network resources that Engineers and ProdAdmins groups can access. Previously, we defined a computer group named IACS Hosts that included our Industrial Zone servers and computers. This group will be added to the RAP.

Figure 3-30 ICS Hosts Computer Group

Name	Description	In Folder
Engineer		CPWE-RA-Cisco....
Engineers		CPWE-RA-Cisco....
Enterprise Ad...	Designated admi...	CPWE-RA-Cisco....
Enterprise Re...	Members of this ...	CPWE-RA-Cisco....
Enterprise VP...		CPWE-RA-Cisco....
Group Policy ...	Members in this ...	CPWE-RA-Cisco....
IACS Hosts	IACS Hosts	CPWE-RA-Cisco....
IDMZ RDG R...		CPWE-RA-Cisco....

- Accept the default RDP port 3389. This completes the RAP configuration.

Verifying the RD Gateway Policies

In order to verify the functionality of the RD Gateway, the appropriate SSL certificates must be installed on the computers that will be used in conjunction with the RD Gateway. CPwE IDMZ does not cover PKI in depth nor does it recommend how to properly implement or manage PKI. For test purposes, firewalls and other devices used self-signed certificates as PKI management was beyond the scope of this CPwE DIG.

Configuring Firewall Rules for RD Gateway

The following steps describe the configuration of firewall rules for the Microsoft RD Gateway to allow secure RDP sessions from Enterprise clients to Industrial servers:

- Step 1** Configure the firewall to allow RDP sessions to traverse the IDMZ via the RD Gateway (see [Table 3-13](#)).

Table 3-13 Access Rules—Remote Desktop Gateway

Firewall Interface	Source	Destination	Permitted Protocols
Enterprise	Any	RDG server in the IDMZ	HTTPS (TCP port 443)
IDMZ	RD Gateway server in the IDMZ	Industrial servers and/or workstations accessible via RDG	RDP (TCP port 3389)

- Step 2** Configure the firewall to allow RD Gateway to authenticate to the Enterprise DC (see AD configuration section for details). Normally the RD Gateway would be part of the firewall object for IDMZ hosts that authenticate to the DC.

ThinManager Remote Desktop Gateway Configuration

Configuring Firewall Rules for ThinManager with RD Gateway

The following steps describe the configuration of firewall rules for the Microsoft RD Gateway to allow secure RDP sessions from Enterprise thin clients to Industrial servers:

- Step 1** Configure the firewall to allow RDP sessions from thin clients to traverse the IDMZ via the RD Gateway (see [Table 3-14](#)).

Table 3-14 Required Access Rules—Thin Clients with Remote Desktop Gateway

Firewall Interface	Source	Destination	Permitted Protocols
Enterprise	Thin client IP addresses	RDG server in the IDMZ	HTTPS (TCP port 443)
IDMZ	RD Gateway server in the IDMZ	Industrial servers and/or workstations accessible via RDG	RDP (TCP port 3389)

Table 3-15 Optional Access Rules—ThinManager with Remote Desktop Gateway

Firewall Interface	Source	Destination	Permitted Protocols	Purpose
Enterprise	ThinManager Server IP addresses	Remote Desktop Server	RPC/DCOM (TCP 135)	Host Monitoring of Remote Desktop Server
Enterprise	ThinManager Server IP addresses	Remote Desktop Server	ICMP	Enforce Primary Display Client Feature
Industrial	ThinManager Server IP addresses	Remote Desktop Server	ICMP	Enforce Primary Display Client Feature

**Note**

Table 3-15 citing optional access rules for ThinManager with Remote Desktop Gateway does not have an IDMZ brokered connection and requires direct access through the IDMZ. This may not be acceptable based on risk tolerance and user policies.

- Step 2 Configure the firewall to allow RD Gateway to authenticate to the Enterprise DC (see AD configuration section for details). Normally the RD Gateway would be part of the firewall object for IDMZ hosts that authenticate to the DC.

ThinManager Configuration for Use with RDG

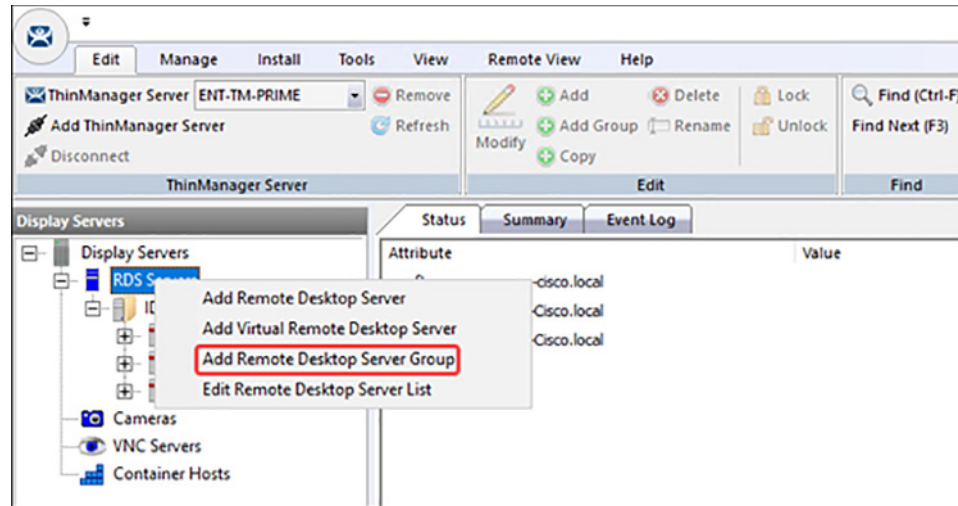
Access to an RD Gateway is configured in the Display Server and Display Client in ThinManager with the assumption that a device on the industrial or enterprise network might need to access resources across the network security boundary such as the IDMZ. The below sections regarding Remote Desktop Gateway and ThinManager explain how to use the Microsoft RD Gateway with ThinManager and thin clients. These steps assume the following:

- RD Gateway setup is completed as per the previous sections.
- ThinManager Remote Desktop Display Servers and Display Clients have basic ThinManager configurations complete.

Configure the Remote Desktop Server Group

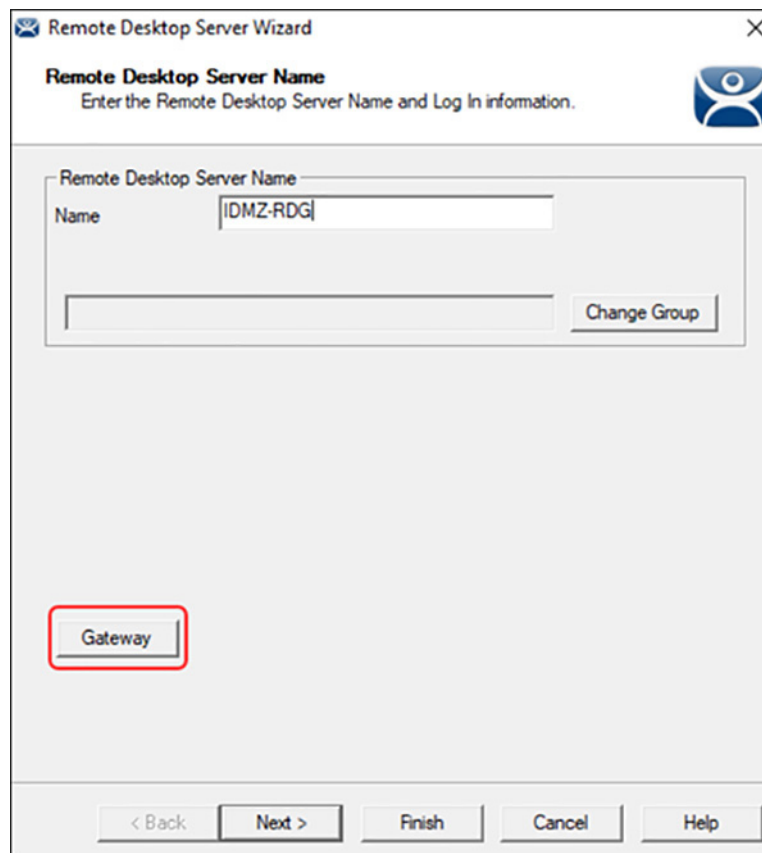
- Step 1 Create **Remote Desktop Server Group** by navigating to **Display Servers** in ThinManager, right clicking on **RDS Servers** and selecting **Add Remote Desktop Server Group**.

Figure 3-31 Add Remote Desktop Server Group



Step 2 Enter a name for the **Remote Desktop Server Group** in the **Name** field and select the **Gateway** button to open the RDP Gateway window.

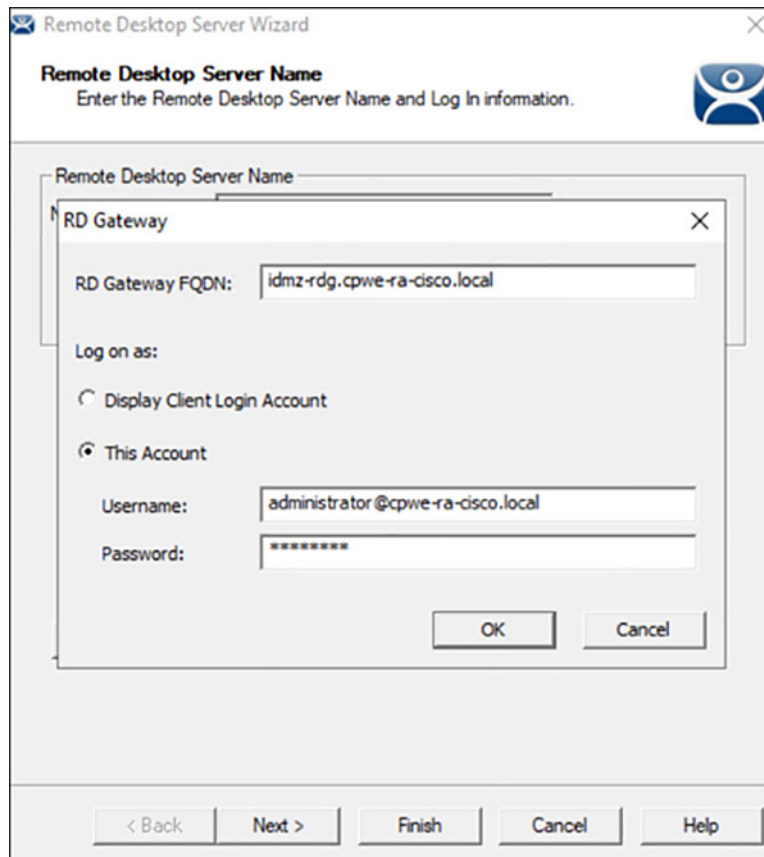
Figure 3-32 RDP Gateway Window



Step 3 Enter the **Fully Qualified Domain Name (FQDN)** of the RD Gateway in the Gateway Name field.

- Step 4 Enter an administrative account and password in the Username and Password fields, if desired. The administrative account should be entered in the User Principal Name (UPN) format.
- If credentials are provided all the terminals will use those credentials to log into the RD Gateway.
 - If left blank the terminal will use the terminal username and password to log into the RD Gateway.
- Step 5 Select the **OK** button to accept.

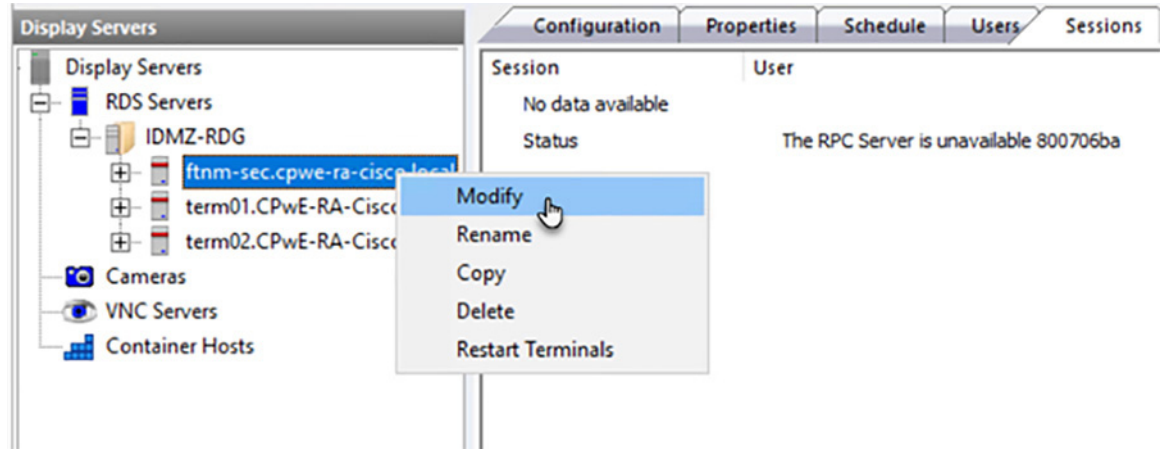
Figure 3-33 RD Gateway



The Remote Desktop Server Group will be empty and will need member servers. These are added from the Remote Desktop Server wizard of each server. Add the Remote Desktop Servers to the Remote Desktop Server Group.

- Step 6 On the **Display Server** branch of the ThinManager tree, right click on a RDS Server icon, and select **Modify** to open the Remote Desktop Server wizard.

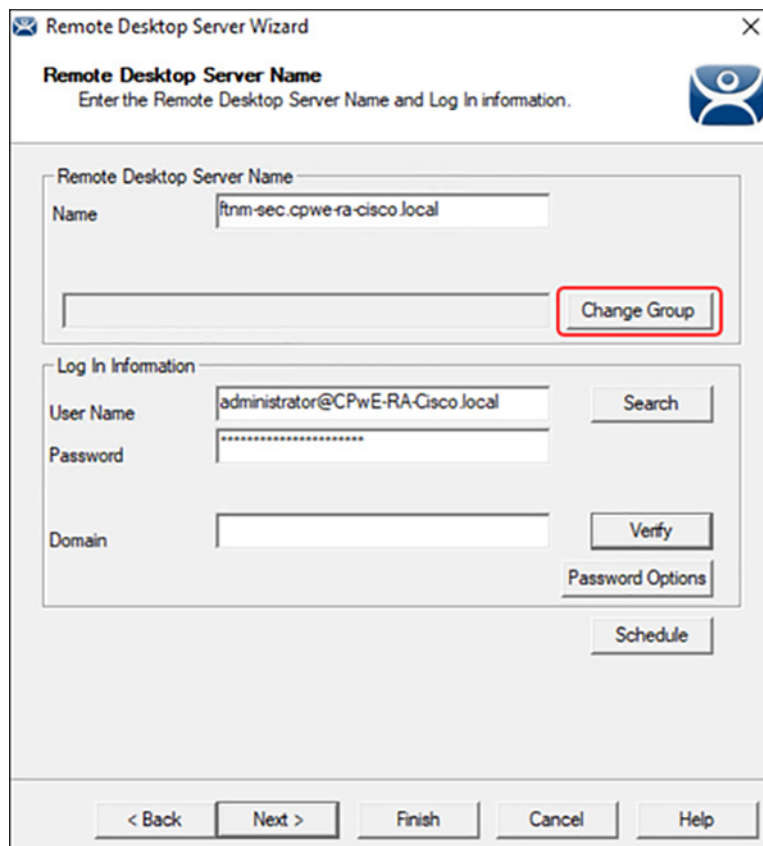
Figure 3-34 Remote Desktop Server Wizard

**Note**

Servers will show a red status and the RPC Server error shown above if the optional access rules in [Table 3-15](#) are not configured

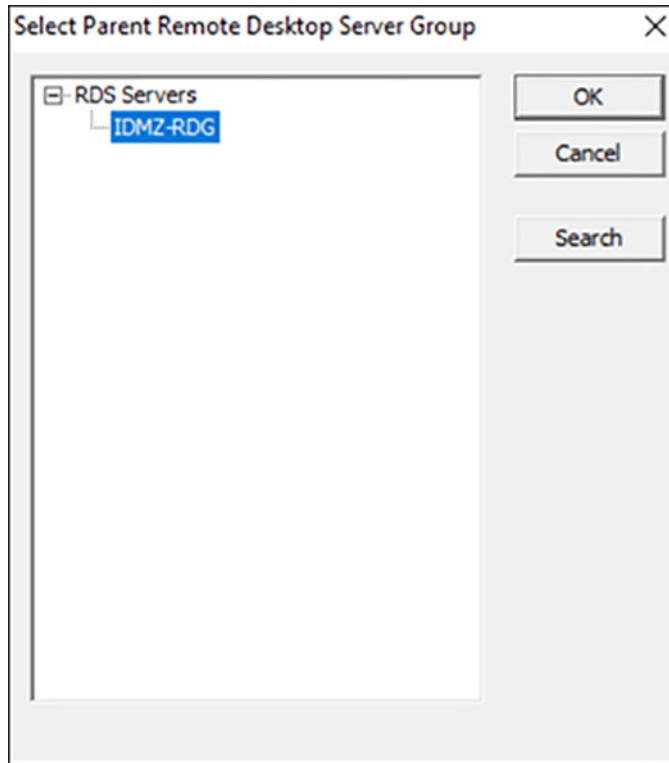
Step 7 Select the **Change Group** button to open the Select Parent Remote Desktop Server Group window.

Figure 3-35 Select Parent Remote Desktop Server Group Window



- Step 8 On the **Parent Remote Desktop Server Group** window select the **Remote Desktop Server Group** and select the **OK** button.

Figure 3-36 Select Parent Remote Desktop Server Group



- Step 9 This will put the **Remote Desktop Server** into the **Remote Desktop Server Group** once you select the **Finish** button to close the wizard. The new status will show in the Group field.

Figure 3-37 Group Field

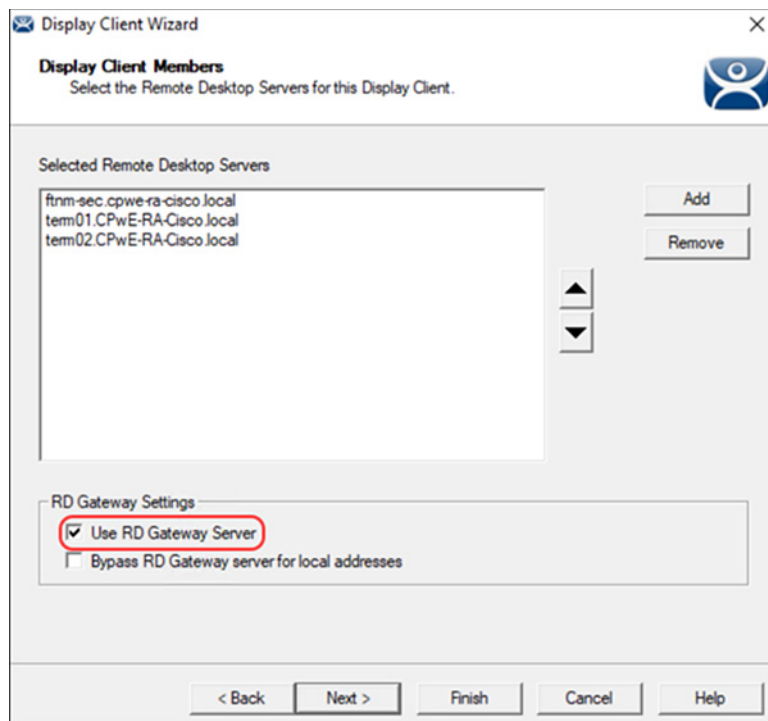
- Step 10 Once the Remote Desktop Server wizard is closed the ThinManager tree will reflect the changes to the membership in the tree.

Configure the Display Client

Access to the RD Gateway is assigned in the Display Client wizard:

- Step 1 Open the Display Client branch of the ThinManager tree, right click on the **Remote Desktop Server** icon, and select **Add Display Client** to open the Display Client wizard.

Figure 3-38 Display Client Wizard



The RD Gateway settings are on the Display Client Members page of the Display Client wizard. Assign the Remote Desktop Servers by selecting the Remote Desktop Server Group. There are two RD Gateway settings:

- **Use RD Gateway**—This checkbox, if selected, prompts the Display Client to use the Microsoft RD Gateway
- **Bypass RD Gateway server for local address**—This checkbox, if selected, allows the Display Client to use a Remote Desktop Server without going through the RD Gateway if the terminal and Remote Desktop Server are on the same subnet.
- Leaving both unchecked will create a display client without access to the RD Gateway or the other network or subnet.

Step 2 Once the desired RD Gateway Settings have been configured click **Finish**.



Note

For more information on ThinManager configuration see ThinManager Manuals and Guides at:

- <https://thinmanager.com/support/manuals/>

Configuring Application Security

This section contains guidelines for configuring application security in the CPwE IDMZ, specifically FactoryTalk Security and Microsoft Windows hardening.

FactoryTalk Security Configuration

FactoryTalk Security is not a separate product - it is fully integrated into the FactoryTalk Directory - you will not find it on the Start menu, or in the Add or Remove Programs list in Control Panel.

The FactoryTalk Administration Console is your tool for working with FactoryTalk Security. Using this tool, you can:

- Browse your FactoryTalk system and view the applications, servers, and devices within it
- Create system-wide security settings, and security settings that affect all instances of FactoryTalk-enabled products
- Secure the FactoryTalk Network Directory or FactoryTalk Local Directory
- Secure resources in your FactoryTalk system, including applications and data
- Secure hardware networks and devices

In order to better describe how to configure FactoryTalk Security, we will walk through a scenario and configure FactoryTalk Security to meet the scenario's requirements. In this small example, we will configure the “Deny Privileges” shown in [Table 3-16](#) for users of Studio 5000® software:

Table 3-16 FactoryTalk Security Authorization Example

User Group	Studio 5000 Deny Privileges List
Operators	Deny All Studio 5000 Privileges
Maintenance	Deny Controller: Secure, Firmware: Update
Engineer	No Restrictions
Production Administrator	No Restrictions
OEM 1	Deny Controller: Secure, Firmware: Update, Tag: Force
OEM 2	Deny Controller: Secure, Firmware: Update, Tag: Force

The following section will show how to configure FactoryTalk Security to accomplish these requirements. This example will be configuring a ControlLogix controller named CLX_C.

FactoryTalk Security User Groups Configuration

You can add two different types of user accounts to your FactoryTalk system:

- **FactoryTalk User or Group Accounts**—These accounts are separate from the user's Microsoft Windows account. This allows you to specify the account's identity (for example, the user name), set up how the account operates (for example, whether the password expires), and specify the groups the account belongs to.
- **Windows-linked User or Group Accounts**—These accounts are managed and authenticated by the Windows operating system, but linked into the FactoryTalk Security services. A Windows-linked user account is added to the FactoryTalk system from a Windows domain or workgroup. You cannot change any Windows-linked account information, but you can change the groups the user belongs to. Adding Windows linked accounts to FactoryTalk means you maintain only one identity for users while still having separate Windows and FactoryTalk security parameters.

The Windows-linked user group Windows Administrators account is added to the FactoryTalk Administrators group, giving all Windows Administrators accounts on a local computer full access to the FactoryTalk Network Directory.

**Note**

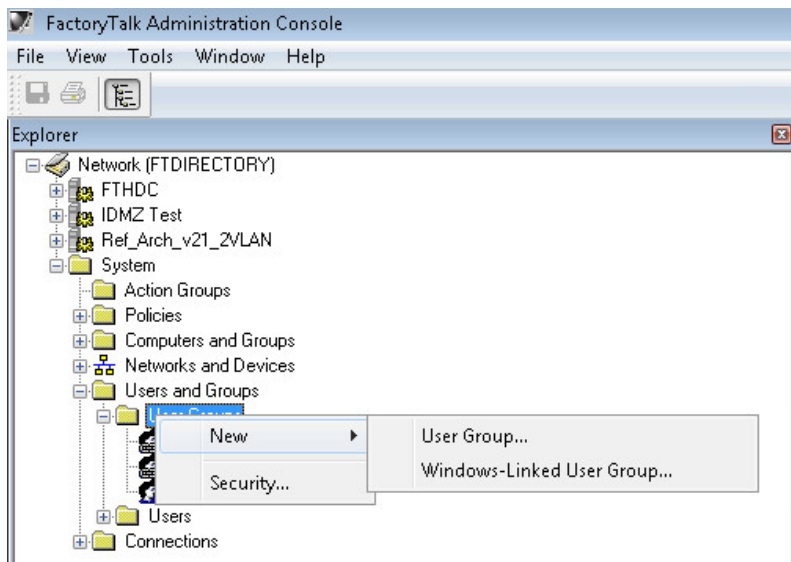
You can remove the default level of access for Windows Administrators after installation. Typically, different groups are responsible for managing FactoryTalk and Windows security parameters.

The Windows-linked user group Authenticated Users is added to the FactoryTalk Network Directory and FactoryTalk Local Directory if you install the FactoryTalk Services Platform on a new computer. You can remove this level of access after installation.

In our example, we are going to add the Windows users groups Operators, Engineers, Maintenance, Production Administrators, OEM1 and OEM2 (Table 3-12).

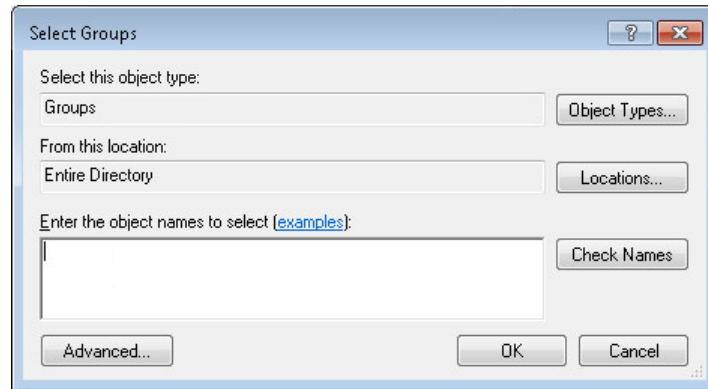
- Step 1 Add Windows-linked users groups to the FactoryTalk Network Directory.
- Open the FactoryTalk Administration Console: **Start > All Programs > Rockwell Software > FactoryTalk Administration Console** and then log on to the **FactoryTalk Network Directory**.
 - Right-click **User Groups** and select **Windows Linked User Group** (see Figure 3-39).

Figure 3-39 FactoryTalk Administration Console—Add User Group



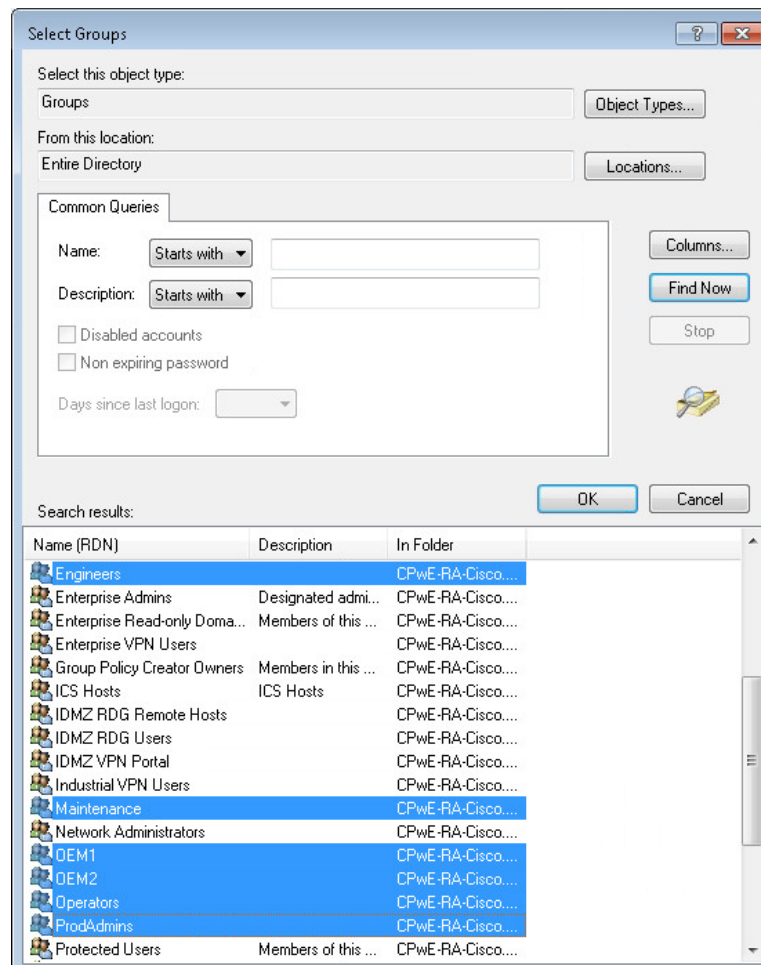
- In the New Windows Linked User Group dialog box, click **Add > Locations > Entire Directory > OK**. The **Select Groups** dialog box will reappear with the **From this location** field changed from the local computer name to the entire directory (see Figure 3-40).

Figure 3-40 Select Groups—Location



- d. Click **Advanced** > **Find Now** to search all of the User Group within the domain. Select Engineers, Maintenance, Operators, OEM1, OEM2 and ProdAdmins groups (see Figure 3-41). Click **OK**.

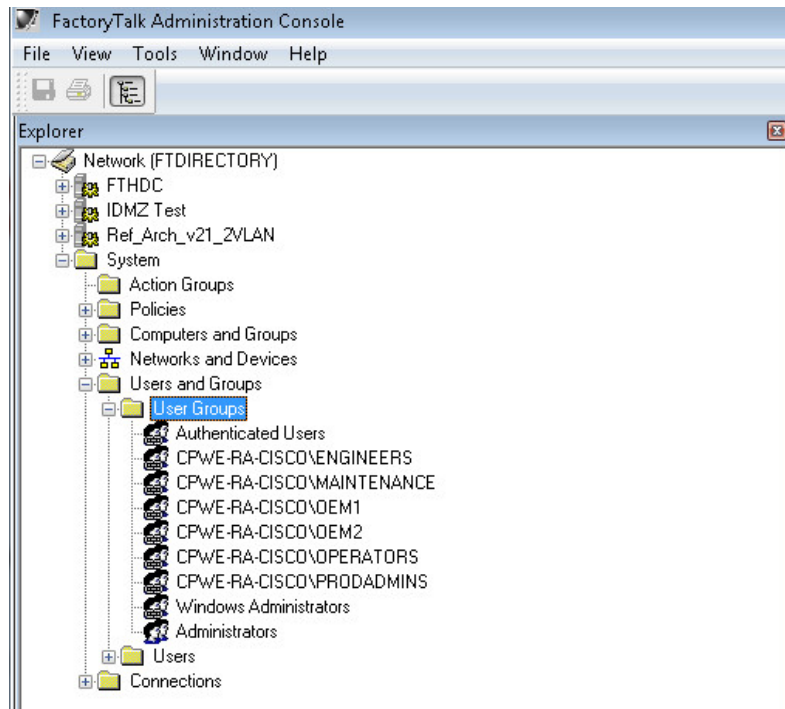
Figure 3-41 Select Groups—Advanced



- e. Verify that the correct groups were added and click **OK**. The FactoryTalk New Windows-Linked User Group dialog box will show the domain users that are to be added. Click **OK** to complete the configuration.

- f. Once the user groups are added, you will see them listed under the User Groups folder in the FactoryTalk Administration Console.

Figure 3-42 FactoryTalk Administration Console—User Groups Created



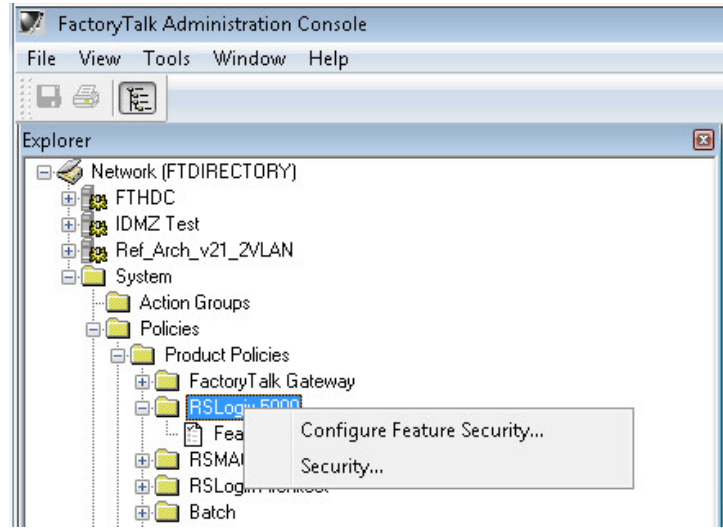
Studio 5000 Product Policies Configuration

FactoryTalk Security allows the security administrator fine granularity of actions that can be secured for Studio 5000, FactoryTalk View SE and other Rockwell Automation products. In our example, we will start by configuring the Studio 5000 product policies, in particular who can secure and unsecure a controller.

- A **policy** is a setting that applies across the entire FactoryTalk IACS system. For example, all FactoryTalk products that share a single FactoryTalk Directory use the same audit policy setting that records a user's failure to access a secured object or feature because the user has insufficient security permissions. If you disable this policy, none of the FactoryTalk products in your system will record failed attempts to access secured objects or features.
- A **product policy** secures either a system-wide feature or system-wide configuration data that is specific to a particular product. Each FactoryTalk product provides its own set of product-specific policies, which means that the product policies available on your system vary, depending on which FactoryTalk products you have installed.

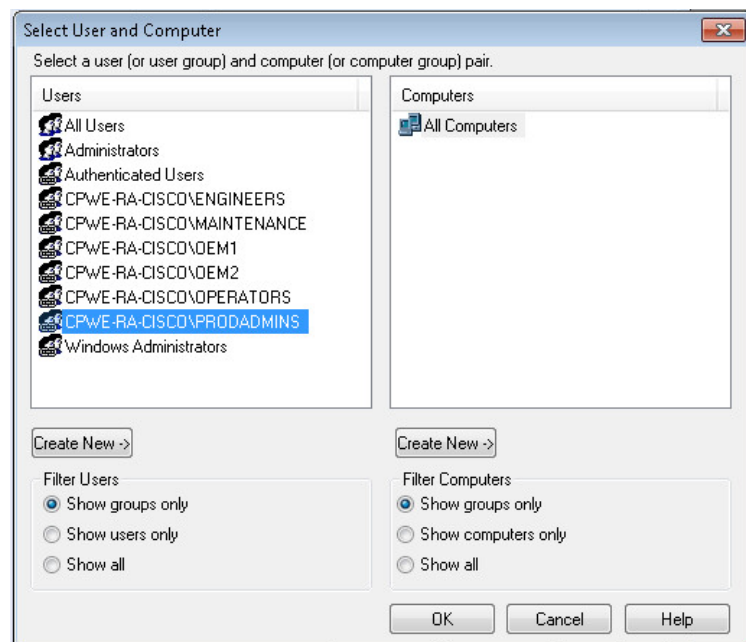
- Step 1 Configure Studio 5000 policies to align with the User Groups requirements in [Table 3-12 on page 3-33](#).
- Under **System > Policies > Product Policies**, right-click **RSLogix 5000** and select **Configure Feature Security** (see [Figure 3-43](#)).

Figure 3-43 FactoryTalk Administration Console—Product Policies



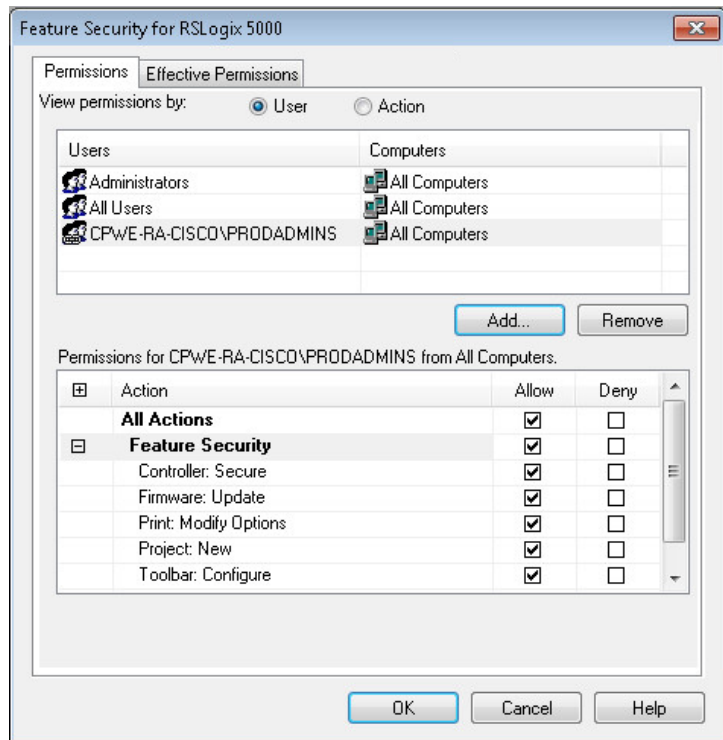
- b. First we need to add the User Groups and then assign permissions. On the **Feature Security** dialog box, select **Add** to display the list of available user groups. Remember that we have added Windows-linked users in a previous step so they will be included in the list of users. Select **PRODADMINS** and click **OK** (see Figure 3-44).

Figure 3-44 Feature Security—Select User Group



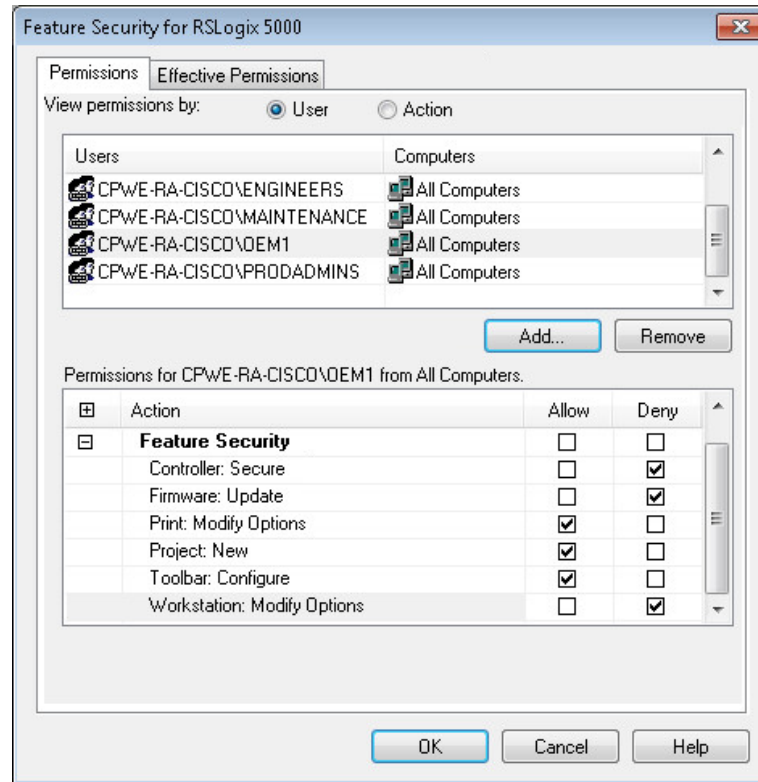
- c. The PRODADMINS group is now added to the user list in the Feature Security dialog box. We will now assign Studio 5000 product policy permissions to this group. We want to allow the Production Administrators unrestricted security access, so we select **Allow** on all Studio 5000 actions (see Figure 3-45).

Figure 3-45 Feature Security—Allow All



- d. Repeat the same step for each user group according to [Table 3-12 on page 3-33](#). In our example, the Maintenance group should not be allowed to update the firmware. We can select **Deny** for Firmware: Update action to achieve this requirement.
- e. We also wanted to stricter control over the OEM1 and OEM2 group. We can simply select **Deny** for additional actions to meet our requirements (see [Figure 3-46](#)).

Figure 3-46 Feature Security—Deny



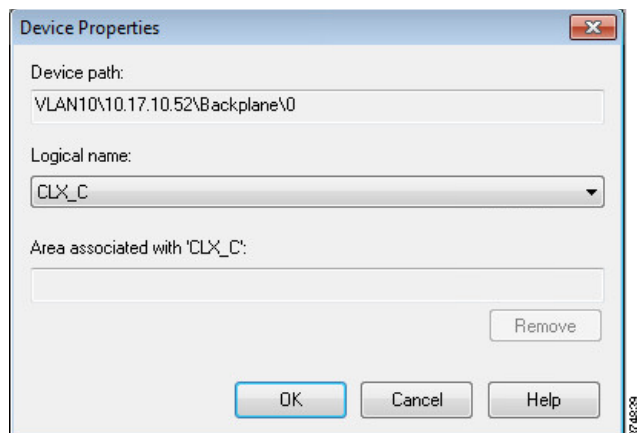
- f. Once permissions for all groups have been configured and applied, a Security Settings warning dialog will appear. It reminds that Deny entries take precedence over Allow entries if a user is a member of two groups.

Controller Security Configuration

Now that we have created FactoryTalk user groups and assigned Studio 5000 product policies, it is time to set the granular security permissions for each group specific to a controller. Actions such as Tag: Force or Tag: Create can be secured through FactoryTalk Security.

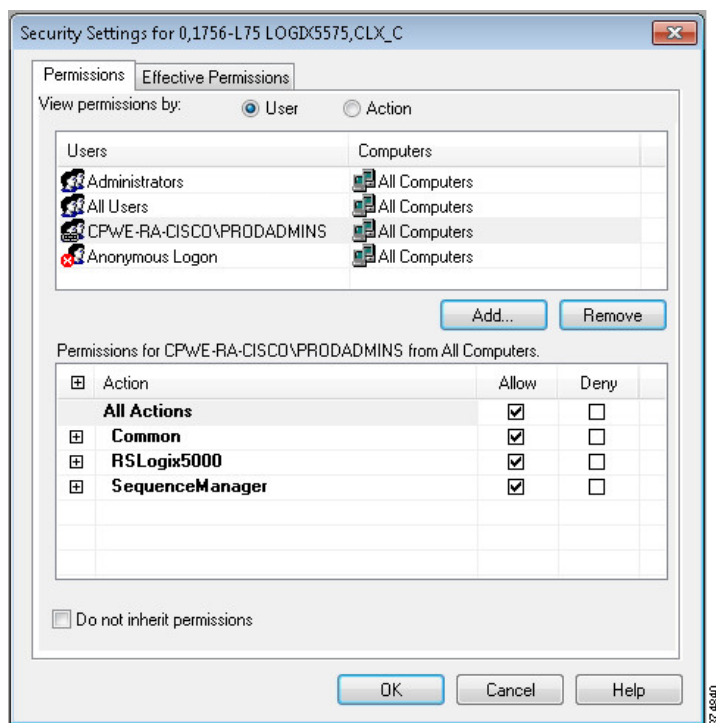
- Step 1 Add a logical name to the controller.** It is recommended that security settings be applied to the controller's logical name. The logical name is the same as the name shown on the controller properties dialog. Security settings for a logical name apply to the offline project as well as when the project is downloaded to the controller.
- a. To set the logical name in the FactoryTalk Administration Console, expand the **Networks and Devices** topology and navigate to the controller. In our example, the controller is named CLX_C. Right-click the controller and select **Properties**.
 - b. Select the **Logical** name that coincides with your controller's name. If the name does not appear in the **Networks and Devices** tree, you need to manually update the path information for the controller.

Figure 3-47 Controller Properties—Logical Name



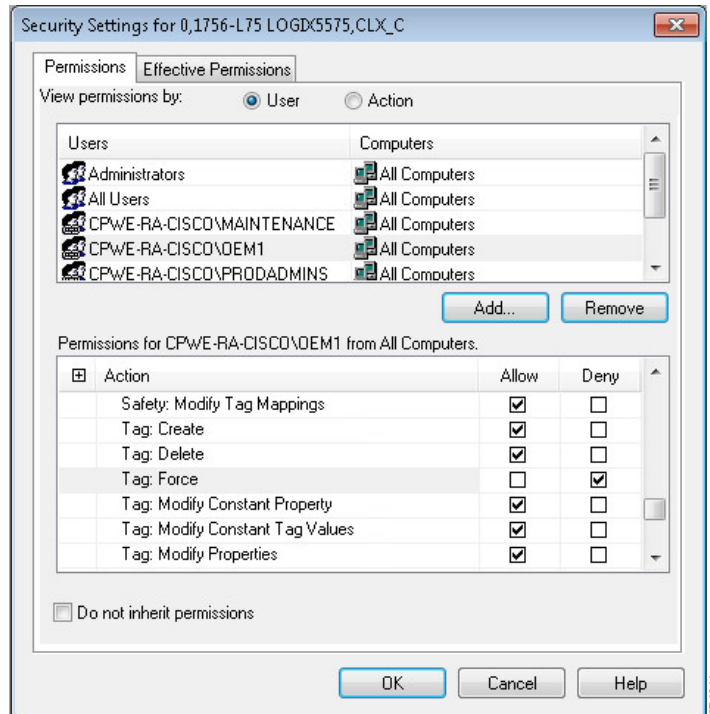
- Step 2 **Assign Studio 5000 permissions to the controller based on the user group.** In our example, we will assign all Studio 5000 permissions on the CLX_C controller to the Production Administrators group (PROADMIN) while setting a Deny permission to the Tag: Force to the OEM1 group.
- Select the controller in the **Network and Devices** branch of the FactoryTalk Administration console. In our example, this is **CLX_C**. Right-click and select **Security**.
 - The **Security Settings** screen allows the security administrator to add users and user groups and assign permissions to each. Click **Add** to find and select the **Production Administrators (PROADMIN)** user group.
 - The **Security Settings** screen will now show the PROADMIN group. We want to allow all actions to the CLX_C controller for this group so select **Allow** in the **All Actions** row (see Figure 3-48).

Figure 3-48 Controller Permissions—Allow All



- d. Now we will deny the **Tag: Force** permission for the OEM1 group. From the **Security Settings** screen, click **Add** and select the **OEM1 group** to add to the configuration list. Expand the **RSLogix 5000** permission set and select **Deny** for the **Tag: Force** action (see [Figure 3-49](#)).

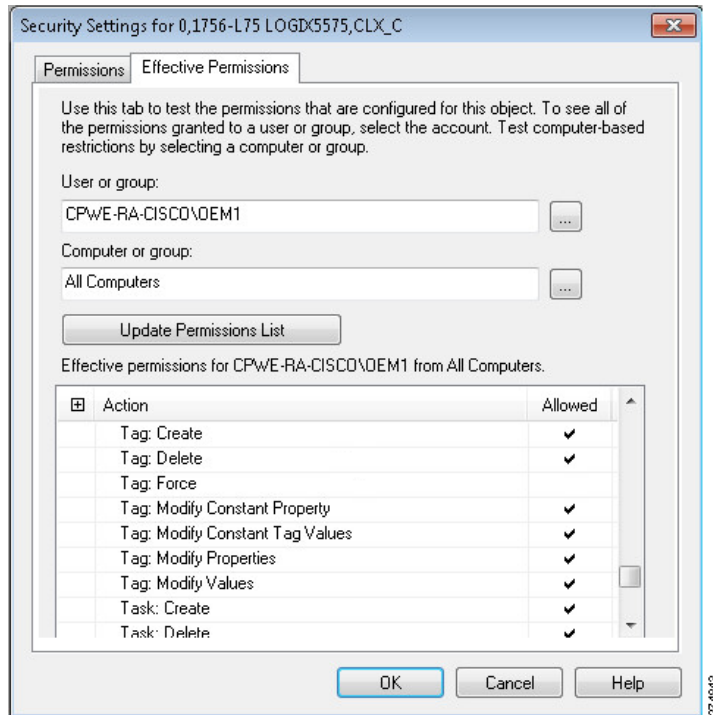
Figure 3-49 Controller Permissions—Deny



Step 3 Verify effective permissions for the groups. FactoryTalk Security is very flexible and allows users and user groups to inherit security permissions. Because of this flexibility, tools exist to check the effective permission for each user, user group and device. In this step, we will check the effective permissions of the OEM1 group to verify they are not allowed to “Tag: Force” on the CLX_C controller.

- a. Select the controller in the **Network and Devices** branch of the FactoryTalk Administration console. Right-click and select **Security**.
- b. Once the **Security Settings** dialog box opens, select the **Effective Permissions** tab. Browse to the desired user group (in our example, OEM1). The Effective Permissions will be shown for the OEM1 group. In our example, we see that **Tag: Force** action is not allowed (see [Figure 3-50](#)).

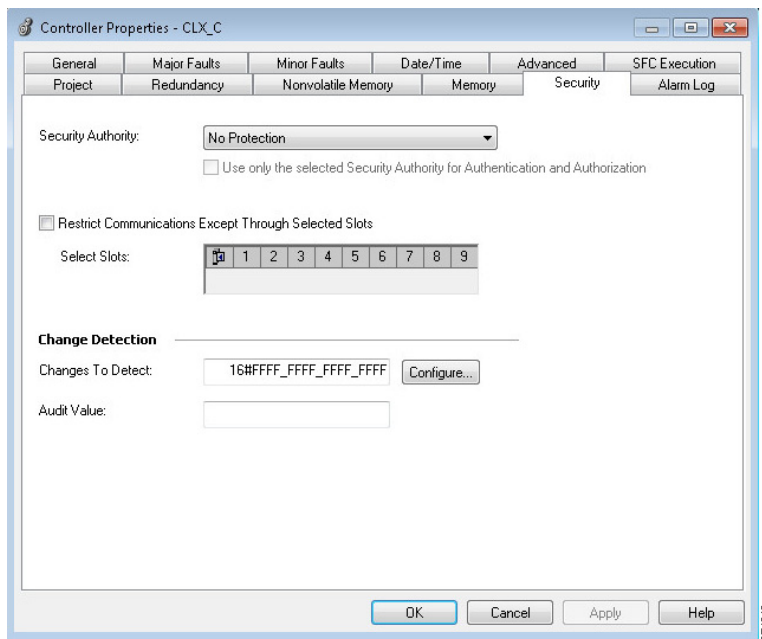
Figure 3-50 Controller Security—Effective Permissions



Step 4 **Apply FactoryTalk Security to the controller in Studio 5000.**

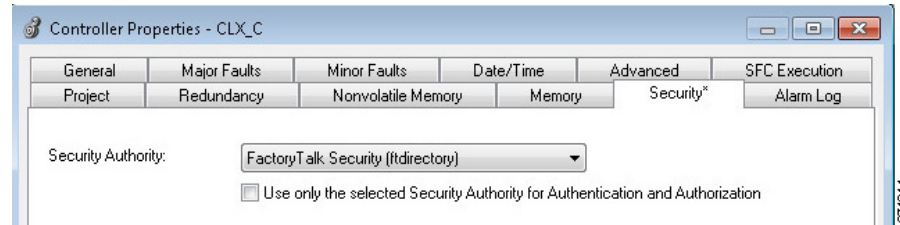
- Open the CLX_C project with Studio 5000. Right-click the **Controller** folder and select **Properties**. Within the Controller Properties screen, select the **Security** tab. You will notice that the **Security Authority** will be set to **No Protection** (see Figure 3-51).

Figure 3-51 Controller Properties—No Protection



- b. Change the Security Authority option to **FactoryTalk Security** (see Figure 3-52) and click **OK**. The Logix Designer warning dialog box is displayed. Select **Yes** to secure the controller.

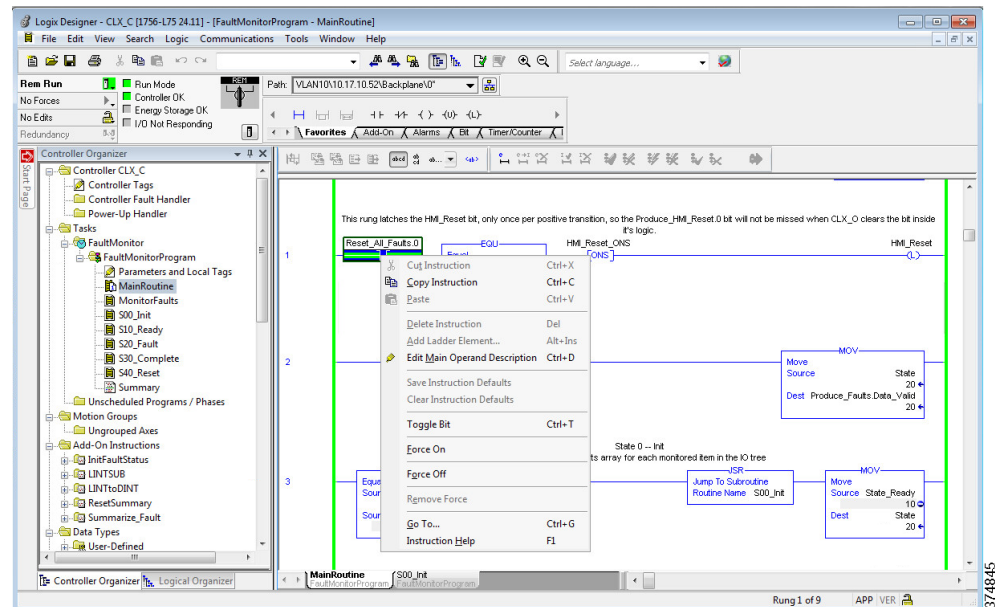
Figure 3-52 Controller Properties—FactoryTalk Security



Step 5 **Test the FactoryTalk Security configuration on the controller.**

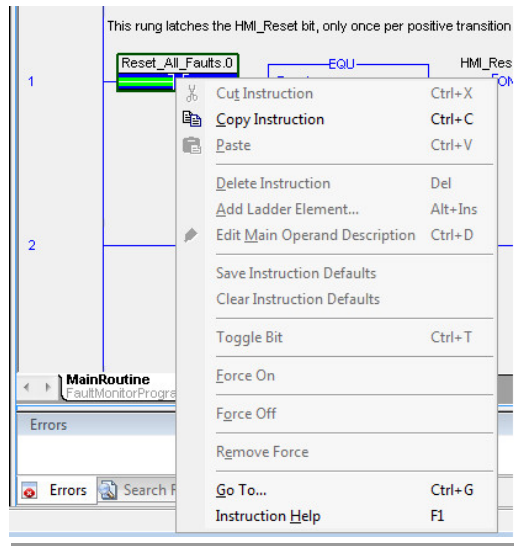
- a. Log onto FactoryTalk Security as a **Production Administrator**. In the Studio 5000, when online with the controller. Right-click the tag. The Force On and Force Off actions are available for a tag (see Figure 3-53).

Figure 3-53 Force Tag Actions Available



Step 6 Log onto FactoryTalk Security as an **OEM1**. The Force On and Force Off actions are now disabled (see Figure 3-54).

Figure 3-54 Force Tag Actions Disabled



OS Hardening Configuration

This section provides a high-level overview of OS hardening configuration steps using Microsoft technologies outlined in [Operating System Hardening](#), page 2-61.

Microsoft AppLocker Configuration

AppLocker uses the Application Identity service (AppIDSvc) for rule enforcement. For AppLocker rules to be enforced, this service must be set to start automatically in the Group Policy Object (GPO).

While the configuration options are unique to each customer and application, Rockwell Automation has provided a sample policy you can use as a guideline to help assist you to get started.



Note

This sample policy can be downloaded from the following Knowledgebase article:

- https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546989

For more information about AppLocker rules, see:

- <http://technet.microsoft.com/en-us/library/dd759068.aspx>

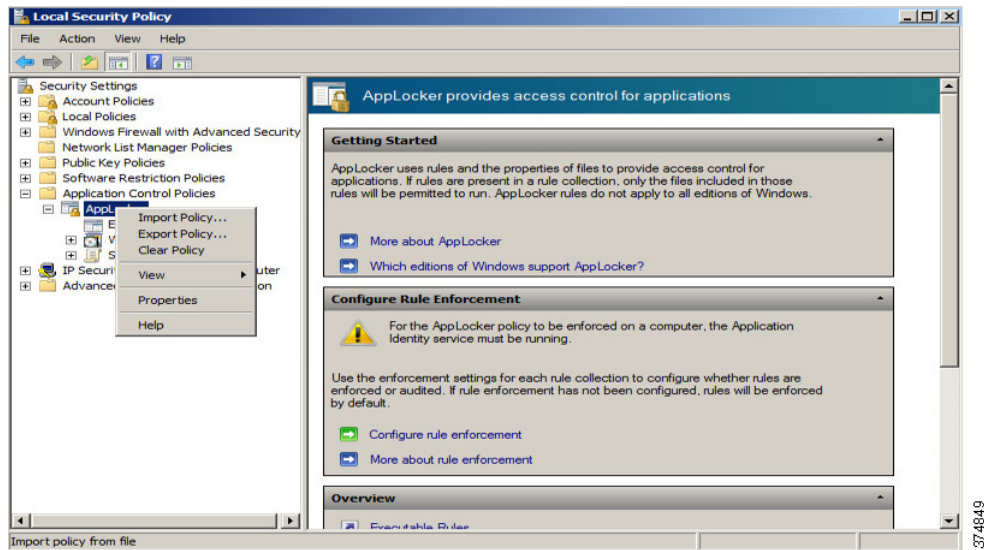


Note

Before continuing, it is suggested to use audit-only mode to deploy the policy and understand its impact before enforcing it and rolling it out to a production environment.

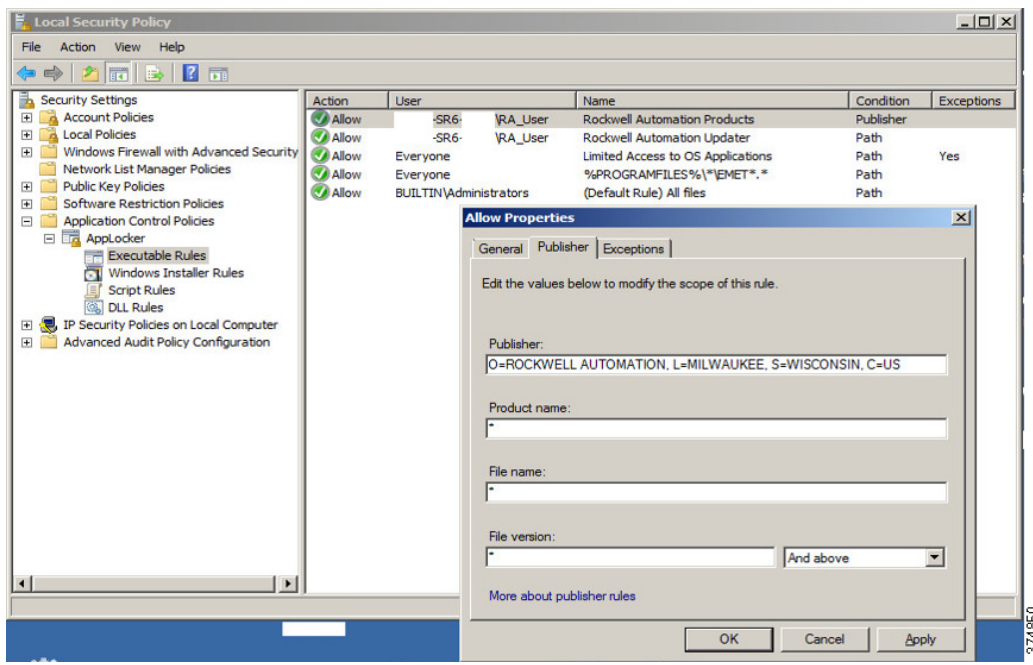
- Step 1 Import the Rockwell Automation example policy.
- Open the **Local Group Policy Editor** by going to **Start > Run** and entering **gpedit.msc**.
 - Navigate to **Application Control Policies > AppLocker**. Right-click **AppLocker** and select **Import Policy** (see [Figure 3-55](#)).

Figure 3-55 Group Policy Editor—Import AppLocker Example Policy



- c. Navigate to the place where you downloaded the AppLocker_RAUser.xml file and import it. This will replace any existing policies with the example one.
- d. Now within the AppLocker policy, rules can be observed and used to expand upon (see Figure 3-56).

Figure 3-56 Group Policy Editor—AppLocker Policy Details



Cisco Telemetry Broker Configuration

The following example will present a scenario and show the configuration steps to traverse network data across the IDMZ using the Cisco Telemetry Broker. It is assumed that the user has the necessary knowledge to configure network devices to send netflow and/or syslog to a given IP address.

**Note**

For details on the configuration of the Cisco Telemetry Broker, refer to *Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide* at:

- https://www.cisco.com/c/dam/en/us/td/docs/security/Telemetry_Broker/Deployment/TB_1_1_Virtual_Appliance_Deployment_and_Configuration_Guide_DV_3_0.pdf

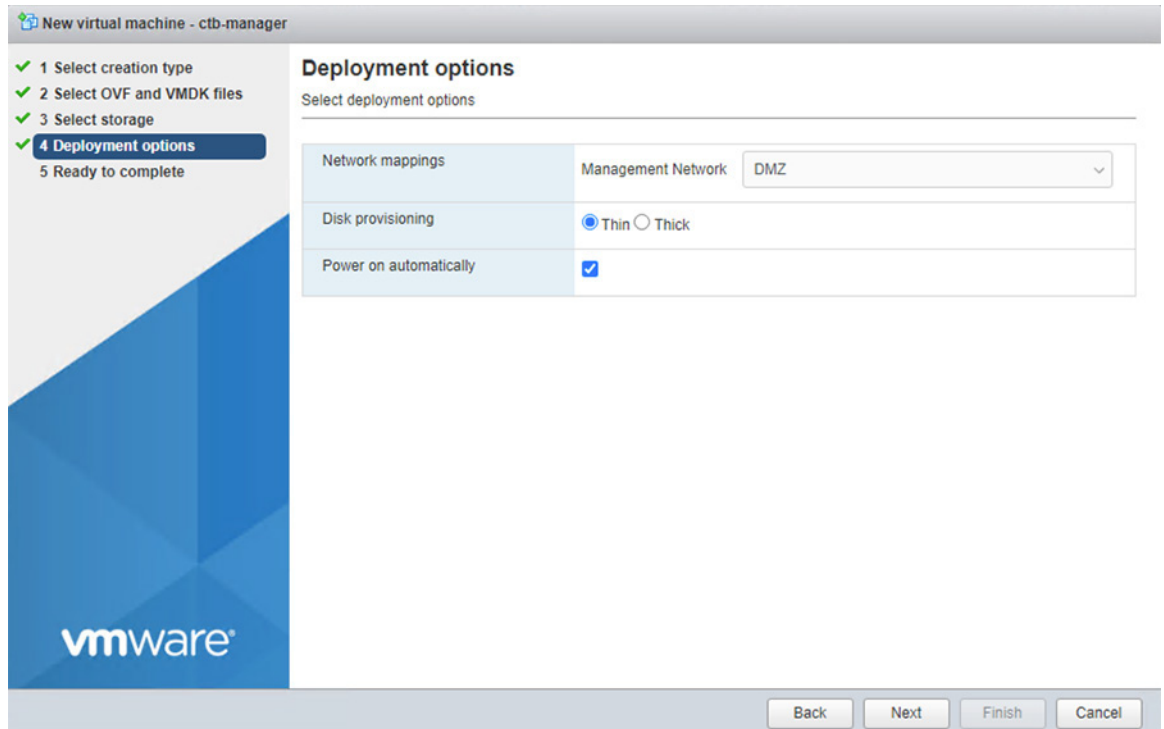
Installing the Virtual Appliances

In our scenario, both the Manager node and Broker node were installed on the ESXI platform. For other supported platforms, see the guide linked above.

Step 1 Install the Manager Node:

- a. Download the Manager Node OVA file.
- b. Log in to the VMWare vSphere web user interface console.
- c. From the side menu, right-click **Virtual Machine** and then choose **Create/Register VM**.
- d. Choose Deploy a virtual machine from an OVF or OVA file.
- e. Enter the name of the OVA file.
- f. Configure the settings as shown in [Figure 3-57](#).

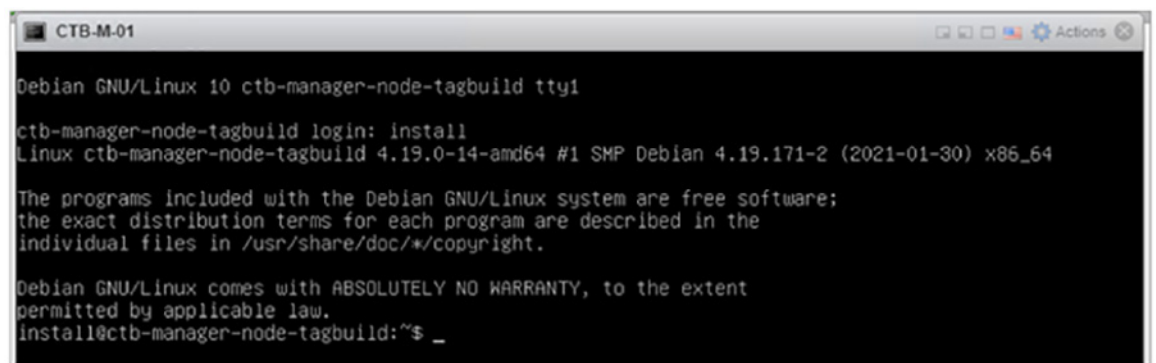
Figure 3-57 ESKI Deployment Options



g. Click **Finish**.

From the manager node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is install; there is no password).

Figure 3-58 CTB Manager Node CLI



Step 2 Run the **sudo ctb-install** command.

Enter the following information:

- Password for the admin user. The password must meet the following requirements:
 - Contain at least 8 characters
 - Contain at least 1 lowercase letter
 - Contain at least 1 uppercase letter

- Contain at least 1 digit
- Contains at least 1 of these special characters: @ # \$ % ^ & * ! + ?
- Cannot be a commonly used phrase or sequence
- Cannot resemble any identifying attributes of the user (such as the username)
- IPv4 address, subnet mask, and default gateway address for the Management Network interface
- Valid DNS nameserver IP address that is reachable from the virtual machine

If this is the first time you are logging in to the manager web interface, you must first create the first Superuser account before you install any broker nodes. We suggest assigning the username of **webadmin** so as not to confuse it with the admin user.

- h. In a web browser, navigate to the following site to create it: https://<manager_ip_address>
- i. To log out, type **exit**.

Step 3 Install the Broker Node:

- a. Download the Broker Node OVA file.
- b. Log in to the VMWare vSphere web user interface console.
- c. From the side menu, right-click **Virtual Machine** and then choose **Create/Register VM**.
- d. Choose Deploy a virtual machine from an OVF or OVA file.
- e. Enter the name of the OVA file.
- f. Configure the settings as shown in [Figure 3-59](#). Note: Deployment type will differ depending on network. For more information see Cisco Telemetry Broker.

Figure 3-59 ESXI Deployment Options

New virtual machine - ctb-broker

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

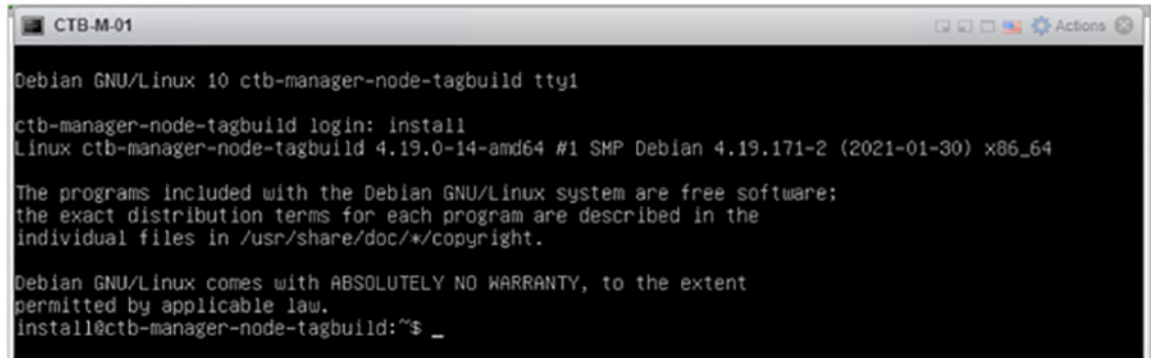
Network mappings	Management Network: DMZ
	Telemetry Network: DMZ
Deployment type	1 Gbps Deployment
	This deployment option is best suited for processing telemetry at a rate of 1 Gbps or below. It uses 2 CPUs and 4G of RAM.
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

Back Next Finish Cancel

- g. Click **Finish**.

- h. From the manager node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is install; there is no password).

Figure 3-60 CTB Broker Node CLI



```

CTB-M-01
Debian GNU/Linux 10 ctb-manager-node-tagbuild tty1
ctb-manager-node-tagbuild login: install
Linux ctb-manager-node-tagbuild 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
install@ctb-manager-node-tagbuild:~$ _

```

- i. Run the **sudo ctb-install** command.
Enter the following information:
 - Password for the admin user. The password must meet the following requirements:
 - Contain at least 8 characters
 - Contain at least 1 lowercase letter
 - Contain at least 1 uppercase letter
 - Contain at least 1 digit
 - Contains at least 1 of these special characters: @ # \$ % ^ & * ! + ?
 - Cannot be a commonly used phrase or sequence
 - Cannot resemble any identifying attributes of the user (such as the username)
 - IPv4 address, subnet mask, and default gateway address for the Management Network interface
 - Valid DNS nameserver IP address that is reachable from the virtual machine
- j. Run the **sudo ctb-manage** command.
Enter the following information:
 - IP address of the manager node
 - Username of the super user account you create in the manager node
 - Password of the super user account you create in the manager node
- k. To logout, type **exit**.

Step 4 Add the Broker node to the Manager Node.

In Cisco Telemetry Broker, click **Broker Nodes** from the main menu:

- a. In the **Broker Nodes** table, click the applicable broker node.
- b. In the **Telemetry Interface** section, click the **Edit** icon.
- c. Configure the IP AddressPrefixLen, and Gateway address.
- d. **Save** your changes.
- e. Click **Destinations** from the main menu.

- f. In the upper right corner of the page, click + **Add Destination**.
- g. Enter a destination **Name**.
- h. Enter a **Destination IP Address** and **Destination UDP Port** for this destination.
- i. Enable **Check destination availability** if you want to establish an inactivity interval between the manager node and the destination. This allows you to identify when a destination is nonresponsive or not receiving telemetry.
- j. Click **Save**.

Figure 3-61 Add Destination for Data Forwarding

Add Destination

Destination Name
Syslog

Destination IP Address
10.1.3.86

Destination UDP Port
514

☒ Check Destination Reachability
Allows Telemetry Broker to detect non-responsive destinations. Disable this if your destination or firewall rule configuration will result in false positive alerts.

Cancel Save

Step 5 Create a forwarding rule in Cisco Telemetry Broker.

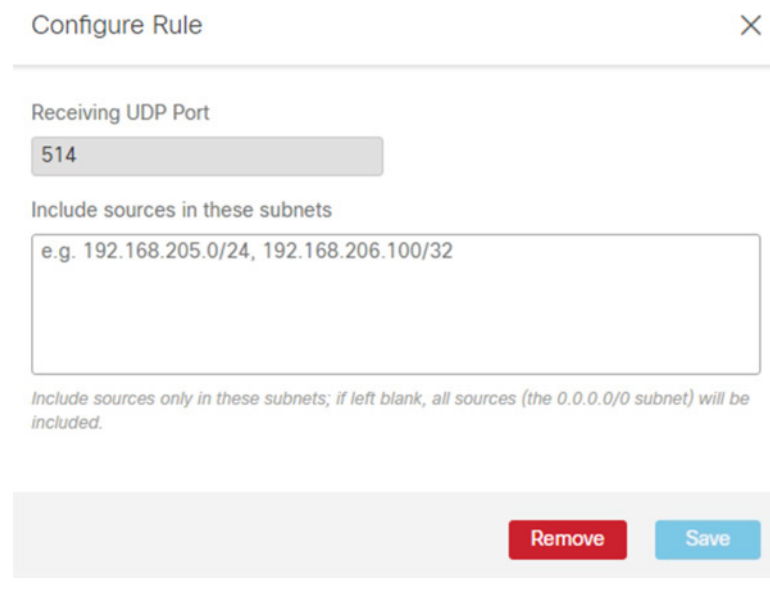


Note

You must add at least one rule to the destination before it will receive telemetry.

- a. In Cisco Telemetry Broker, click **Destinations** from the main menu.
- b. In the lower left corner of the applicable destination summary, click + **Add rule**.
- c. Enter a **Receiving UDP Port**.
- d. If you want to specify subnets over which this destination will receive certain traffic, add one or more **Subnets**.
- e. Click **Save**.

Figure 3-62 Configure Rule in CTB



Configure Rule

Receiving UDP Port

514

Include sources in these subnets

e.g. 192.168.205.0/24, 192.168.206.100/32

Include sources only in these subnets; if left blank, all sources (the 0.0.0.0/0 subnet) will be included.

Remove Save

Configuring Firewall Rules for Cisco Telemetry Broker

The following steps describe the configuration of firewall rules for the Cisco Telemetry Broker to allow Industrial Clients to send UDP data outside of the network. Although the Cisco Telemetry Broker supports any UDP message, the tests done in this lab was for Netflow and Syslog message traversal.

- Step 1 Configure the firewall to allow telemetry to traverse the IDMZ via the Cisco Telemetry Broker (see [Table 3-17](#)).

Table 3-17 Required Access Rules—Network Telemetry via Cisco Telemetry Broker

FirewallInterface	Source	Destination	Permitted Protocols
Industrial	Industrial Zone Switches	Cisco Telemetry Broker – Broker Node	Netflow (UDP port 2055)
Industrial	Industrial Zone Switches	Cisco Telemetry Broker – Broker Node	Syslog (UDP port 514)
IDMZ	Cisco Telemetry Broker – Broker Node	Netflow Collector	Netflow (UDP port 2055)
IDMZ	Cisco Telemetry Broker – Broker Node	Syslog Collector	Syslog (UDP port 514)

CPwE IDMZ Troubleshooting

This chapter includes the following major topics:

- [Cisco FTD](#)
- [Cisco Secure Access by Duo](#)

Cisco FTD

Cisco Firepower Threat Defense Troubleshooting TechNotes:

- <https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-tech-notes-list.html>

Cisco Secure Access by Duo

Duo Authentication Proxy:

- <https://duo.com/docs/authproxy-reference#troubleshooting>

Duo Authentication for Microsoft Remote Desktop Gateway:

- <https://duo.com/docs/rdgateway#troubleshooting>

Duo Authentication for Windows Logon and RDP:

- <https://duo.com/docs/rdp#troubleshooting>

References

This appendix, which lists the references used in the IDMZ system, includes the following major topics:

- [Converged Plantwide Ethernet \(CPwE\), page A-1](#)
- [Active Directory Services, page A-3](#)
- [Application Security, page A-4](#)
- [Core Switch Architecture, page A-4](#)
- [FactoryTalk Historian, page A-5](#)
- [Identity Services, page A-5](#)
- [Industrial Demilitarized Zone Firewalls, page A-5](#)
- [Network Infrastructure Hardening, page A-6](#)
- [Network Time Protocol, page A-6](#)
- [Remote Access Server, page A-7](#)
- [Routing Between Zones, page A-7](#)

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing—Converged Plantwide Ethernet
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures—Converged Plantwide Ethernet
<http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page>
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf>
- Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:

- Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html
- OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td018_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/WP/CPwE-5-1-OEM-WP/CPwE-5-1-OEM-WP.html>
- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - 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
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html>
- Cloud Connectivity to a Converged Plantwide Ethernet Architecture:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html

- Deploying Network Security within a Converged Plantwide Ethernet Architecture:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-%20DIG.html>
- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html>
- Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide:
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/PRP/DIG/CPwE-5-1-PRP-DIG.html>
- Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide:
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf
 - Cisco site:
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Active Directory Services

Active Directory Domain Services:

- <https://technet.microsoft.com/en-us/windowsserver/dd448614>

Deploy Active Directory Domain Services (AD DS) in Your Enterprise

- <https://technet.microsoft.com/en-us/library/hh472160.aspx>

How Active Directory Replication Works

- <http://social.technet.microsoft.com/wiki/contents/articles/4592.how-active-directory-replication-works.aspx>

Active Directory Replication Technologies

- <https://technet.microsoft.com/en-us/library/cc776877%28v=ws.10%29.aspx>

Active Directory and Active Directory Domain Services Port Requirements

- <https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx>

Active Directory Certificate Services

- <https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx>

Active Directory Users and Computers

- <https://technet.microsoft.com/en-us/library/cc754217.aspx>

Application Security

FactoryTalk Security System Configuration Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-e.pdf

Using Rockwell Automation Products with Microsoft Enhanced Mitigation Experience Toolkit (EMET):

- https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546988

Using Rockwell Automation Software Products with AppLocker :

- https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546989

How AppLocker Works:

- <http://technet.microsoft.com/en-us/library/ee460948%28v=ws.10%29.aspx>

The EMT configuration can be downloaded from the knowledgebase article at:

- https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546988

Core Switch Architecture

Virtual Switching Systems (Release 15.1SY Supervisor Engine 2T Software Configuration Guide):

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/virtual_switching_systems.html

Virtual Switching Systems (Catalyst 6500 12.25X Software Configuration Guide):

- <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vs.html>

Data Brokering

Cisco Telemetry Broker:

- <https://www.cisco.com/c/en/us/products/security/telemetry-broker/index.html>

Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide:

- https://www.cisco.com/c/dam/en/us/td/docs/security/Telemetry_Broker/Deployment/TB_1_1_Virtual_Appliance_Deployment_and_Configuration_Guide_DV_3_0.pdf

FactoryTalk Historian

FactoryTalk Historian website

- <http://www.rockwellautomation.com/rockwellsoftware/products/factorytalk-historian.page?>

FactoryTalk Historian Installation and Configuration Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/in/hse-in025_-en-e.pdf

FactoryTalk Historian SE Historian To Historian Interface Installation and Configuration Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/in/h2h-in001_-en-e.pdf

FactoryTalk Historian SE FactoryTalk Historian To Historian Interface User Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/um/h2h-um001_-en-e.pdf

Identity Services

Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

Cisco Identify Services Engine Hardware Installation Guide, Release 1.4 Cisco SNS-3400 Series Appliance Ports Reference:

- http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/installation_guide/b_ise_InstallationGuide14/b_ise_InstallationGuide14_appendix_01010.html

Industrial Demilitarized Zone Firewalls

Cisco Secure Firewall:

- <https://www.cisco.com/c/en/us/products/security/firewalls/index.html>

Cisco Firepower 2100 Getting Started Guide; Deployment with FMC:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/firepower-2100-gsg/ftd-fmc.html

Cisco Firepower Management Center Configuration Guide:

- <https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67.html>

Licensing

Cisco Smart Licensing:

- <https://www.cisco.com/c/en/us/products/software/smart-accounts/software-licensing.html>

Cisco Smart Software On-Prem User Guide:

- https://www.cisco.com/web/software/286285517/147683/Smart_Software_Manager_On-Prem_7_User_Guide.pdf

Multi-Factor Authentication

Cisco Multi-Factor Authentication:

- <https://www.cisco.com/c/en/us/products/security/adaptive-multi-factor-authentication.html>

Cisco Duo Authentication Proxy:

- <https://duo.com/docs/authproxy-reference>

Cisco FTD VPN with AnyConnect:

- <https://duo.com/docs/cisco-firepower>

Duo Authentication for Windows Logon and RDP:

- <https://duo.com/docs/rdp>

Duo Authentication for Microsoft Remote Desktop Gateway on Windows 2012 and Later:

- <https://duo.com/docs/rdgateway>

Network Infrastructure Hardening

Cisco Guide to Harden Cisco IOS Devices:

- <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

Software Configuration Guide, Cisco IOS Release 15.2(2)E (Industrial Ethernet 2000 Switch) Configuring Switch-Based Authentication:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/software/release/15_2_2_e/configuration/guide/scg-ie2000/swauthen.html

Network Time Protocol

Windows Time Service Technical Reference:

- <https://technet.microsoft.com/en-us/library/cc773061%28v=ws.10%29.aspx>

Network Time Protocol: Best Practices White Paper:

- <http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html>

Windows Time Service Technical Reference:

- <https://technet.microsoft.com/en-us/library/cc773061.aspx>

Remote Access Server

Remote Access VPN for Firepower Threat Defense:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_remote_access_vpns.html

Remote Desktop Services Overview:

- <https://technet.microsoft.com/en-us/library/hh831447.aspx>

Deploying Remote Desktop Gateway Step-by-Step Guide:

- <https://technet.microsoft.com/en-us/library/dd983941%28v=ws.10%29.aspx>

Routing Between Zones

Enhanced Interior Gateway Routing Protocol White Paper:

- <http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

OSPF Design Guide:

- <http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>

APPENDIX B

Test Hardware and Software

The network hardware and software components used in the CPwE IDMZ testing are listed in [Table B-1](#). Rockwell Automation software versions are listed in [Table B-2](#).

Table B-1 Network Hardware and Software

Role	Product	SW Version	Notes
Core switch	Catalyst 9400	17.6.1	Virtual Switching System (VSS)
Core switch	Catalyst 9500	17.6.1	Virtual Switching System (VSS)
Distribution switch	Catalyst 9300	17.6.1	Switch stack
Access switch	Cisco IE 2000, IE4000, Stratix 5700	15.2(8)E1	
Access switch	Cisco IE 3x00, Stratix 5800	17.6.1	
Firewall	Firepower 2130	FTD 7.0	Active and Standby
Firewall Management	Firepower Management Center	7.0	
Identity Services Engine (ISE)	Cisco ISE VM	2.7 Patch 1	Distributed ISE
Client	Microsoft Windows laptop	Windows 7	

Table B-2 Rockwell Automation Software

Product	Version
FactoryTalk Historian Site Edition	7.01
FactoryTalk Service Platform	6.21 (CPR 9 SR 12)
FactoryTalk Activation Manager	4.06
FactoryTalk Historian to Historian Interface	3.10.01
FactoryTalk AssetCentre	11.00
FactoryTalk View Site Edition	12.00
FactoryTalk Link (aka RSLinx Enterprise)	6.21 (CPR 9 SR 12)
RSLinx Classic	4.21
ThinManager	12.00

APPENDIX

C

Acronyms and Initialisms

The following is a list of all acronyms and initialisms used in this document.

Term	Definition
AAA	authentication, authorization and accounting
ACL	access control lists
AD	Active Directory
AD CS	Active Directory Certificate Services
AD DC	Active Directory Domain Controller
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
AMP	Advanced Malware Protection
API	application programming interface
AppIDSvc	Application Identity service
ASA	Adaptive Security Appliance
ASDM	Cisco Adaptive Security Device Manager
AVC	Application Visibility and Control
CA	Certificate Authority
CAP	RD Gateway Connection Authorization Policies
CAPWAP	control and provisioning of wireless access points
CDP	Cisco Discovery Protocol
CIP	Common Industrial Protocol
COFF	Common Object File Format
CPwE	Converged Plantwide Ethernet
CRL	Certificate Revocation Lists
CVD	Cisco Validated Design
CWS	Cisco Cloud Web Security
DCE/RPC	Distributed Computing Environment/Remote Procedure Calls
DCOM	Microsoft Distributed Component Object Model
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNS	Domain Name Services
DPI	Deep Packet Inspection
DUAL	Diffusing Update ALgorithm

Term	Definition
EIGRP	Enhanced Interior Gateway Routing Protocol
EMET	Enhanced Mitigation Experience Toolkit
EPM	Endpoint Mapper
FSMO	Flexible Single Master Operations
GLBP	Gateway Load Balancing Protocol
GPO	Group Policy Object
HSRP	Hot Standby Routing Protocol
HMI	human-machine interface
IACS	Industrial Automation and Control System
IAT	Import Address Table
IDMZ	Industrial Demilitarized Zone
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention Services
IPsec	IP Security
ISE	Cisco Identity Services Engine
LACP	Link Aggregation Control Protocol
LWAP	Lightweight Access Points
MAC	media access control
MEC	Multi-chassis EtherChannel
MMC	Microsoft Management Console
MNT	Monitoring Node
MTTR	Mean Time To Repair
NAT	Network Address Translation
NGIPS	next-generation IPS
NSF	nonstop forwarding
NSSA	Not-So-Stubby Area
NTP	Network Time Protocol
OEE	overall equipment effectiveness
OIR	online insertion and removal
OpSec	Operations Security
OSPF	Open Shortest Path First
OU	organizational units
PAC	Programmable Automation Controllers
PAN	Policy Administration Node
PDC	Primary Domain Controller
PE	Windows Portable Executable
PSN	Policy Service Node
PTP	Precision Time Protocol
RA	registration authority
RADIUS	Remote Authentication Dial-In User Service
RAP	RD Gateway Resource Authorization Policies
RAS	Remote Access Servers
RBAC	Role-based access control
RD	Remote Desktop
RDC	Remote Desktop Connection
RDP	Remote Desktop Protocol

Term	Definition
RF	Radio Frequency
RPC	Remote Procedure Call
SFT	Secure File Transfer
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SoD	Separation of Duties
SOE	Sequence of Events
SPOF	single points of failure
SSH	Secure Shell
SSO	Stateful Switch Over
TACACS+	Terminal Access Controller Access Control System Plus
UTC	Coordinated Universal Time
UUID	universally unique identifier
VLAN	virtual LAN
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
VSL	virtual switch link
VSS	Virtual Switching System
WLAN	wireless LAN
WLC	wireless LAN controller
WSE	Web Security Essentials

About the Cisco Validated Design (CVD) Program

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

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

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

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

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

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

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

Panduit Corp. is a world-class provider of engineered, flexible, end-to-end electrical and network connectivity infrastructure solutions that provides businesses with the ability to keep pace with a connected world. Our robust partner ecosystem, global staff, and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com

US and Canada:
Panduit Corp.
World Headquarters
18900 Panduit Drive
Tinley Park, IL 60487
iai@panduit.com
Tel. 708.532.1800

Asia Pacific:
One Temasek Avenue #09-01
Millenia Tower
039192 Singapore
Tel. 65 6305 7555

Europe/Middle East/Africa:
Panduit Corp.
West World
Westgate London W5 1XP Q
United Kingdom
Tel. +44 (0) 20 8601 7219

Latin America:
Panduit Corp.
Periférico Pte Manuel Gómez
Morin #7225 - A
Guadalajara Jalisco 45010
MEXICO
Tel. (33) 3777 6000

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to <http://newsroom.cisco.com>. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

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.

Catalyst, Cisco, and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to be more productive and the world more sustainable. In support of smart manufacturing concepts, Rockwell Automation helps customers maximize value and prepare for their future by building a Connected Enterprise.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000
Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788
Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600
Fax: (32) 2 663 0640

Allen-Bradley, ControlLogix, FactoryTalk, FactoryTalk Network Manager, FactoryTalk Policy Manager, FactoryTalk VantagePoint, Rockwell Automation, RSLinx, Stratix, Studio 5000, Studio 5000 Logix Designer and ThinManager are trademarks of Rockwell Automation, Inc..

CIP, CIP Motion, CIP Security, CIP Sync, and EtherNet/IP are trademarks of ODVA, Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

Trademarks not belonging to Rockwell Automation are property of their respective companies