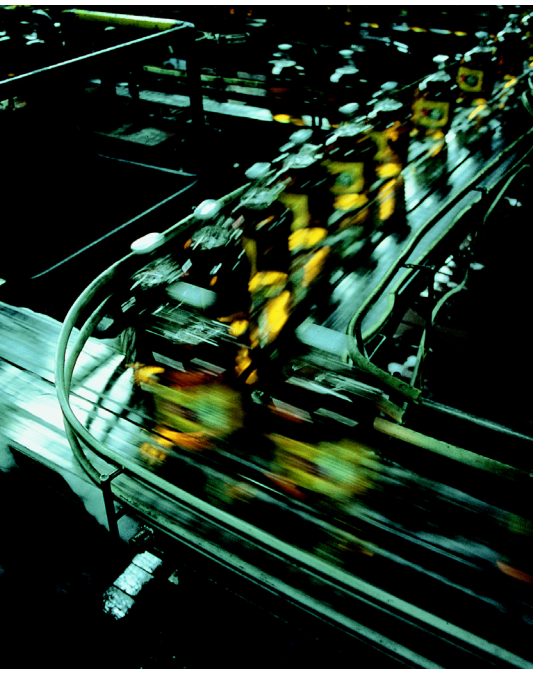


Securely Traversing IACS Data across the Industrial Demilitarized Zone

Design and Implementation Guide

March 2022

Cisco Validated Design

Document Reference Number: ENET-TD009C-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation and that follow the Cisco Validated Design (CVD) program. 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 manufacturers with the design and deployment of a scalable, reliable, secure and future-ready plant-wide industrial network infrastructure. CPwE can also help manufacturers achieve the benefits of cost reduction using proven designs that facilitate quicker deployment while helping to reduce risk in deploying new technology.

This Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide (DIG) outlines key requirements and design considerations to help with the successful design and deployment of an Industrial Demilitarized Zone (IDMZ) within Industrial Automation and Control System (IACS) plant-wide architectures.

Release Notes

This document remains unchanged from the May 2017 release other than this release note, which advises readers of a new version of this document that removes the use of Cisco ASA firewalls and provides guidance on new use cases and architecture components. This document will remain active for readers who still utilize Cisco ASA in their IDMZ design and are not yet ready to move to Firepower devices.

Summary of Specific Changes

The new March 2022 release of this document (link below) contains the following changes from this May 2017 release:

- 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®

The updated version of this design guide, *Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense*, can be found at:

- Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td013_-en-p.pdf
- Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_2_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.
CPwE IDMZ Troubleshooting	Describes troubleshooting for Adaptive Security Appliance (ASA) failover and firewall rules.
References	List of references for CPwE and Cisco solutions and technologies.
Test Hardware and Software	List of network hardware and software components used in the CPwE IDMZ testing.
Acronyms and Initialisms	List of all acronyms and initialisms used in the document.

For More Information

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

Rockwell Automation site:

- http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page

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 the following URL:

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

CHAPTER 1

CPwE IDMZ Overview

This chapter includes the following major topics:

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 network technology convergence through the use of standard Ethernet and Internet Protocol (IP) technology, which helps to enable the Industrial Internet of Things (IIoT).

By default, a converged IACS network is generally open. Openness facilitates both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS products. This openness also requires that configuration and architecture secure and harden IACS networks. The degree of hardening depends upon the required security stance. Business practices, corporate standards, security policies, application requirements, industry security standards, regulatory compliance, risk management policies and overall tolerance to risk are key factors in determining the appropriate security stance.

Many organizations and standards bodies recommend segmenting business system networks from plant-wide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network located 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 is the underlying architecture that provides standard network services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures, through testing and validation by Cisco and Rockwell Automation, provide design and implementation guidance, test results and documented configuration settings that can help to achieve the real-time communication, reliability, scalability, security and resiliency requirements of modern IACS applications.

The Securely Traversing IACS Data across the Industrial Demilitarized Zone CVD (Cisco and Rockwell Automation Validated Design), which is documented in this Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide (DIG), details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ. The CPwE IDMZ CVD is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation®.

Holistic Industrial Security

No single product, technology or methodology can fully secure IACS applications. Protecting IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical and physical), utilizing diverse technologies, at separate IACS levels that address different types of threats.

Note The CPwE Security architecture includes recommendations for a physical IDMZ to recognize IACS application traversal through the Industrial Zone to the Enterprise Zone, and Identity Services for devices accessing the Cell/Area Zone network. Each is part of CPwE's overall security architecture and is available as a separate CVD, adding to CPwE's holistic industrial security approach.

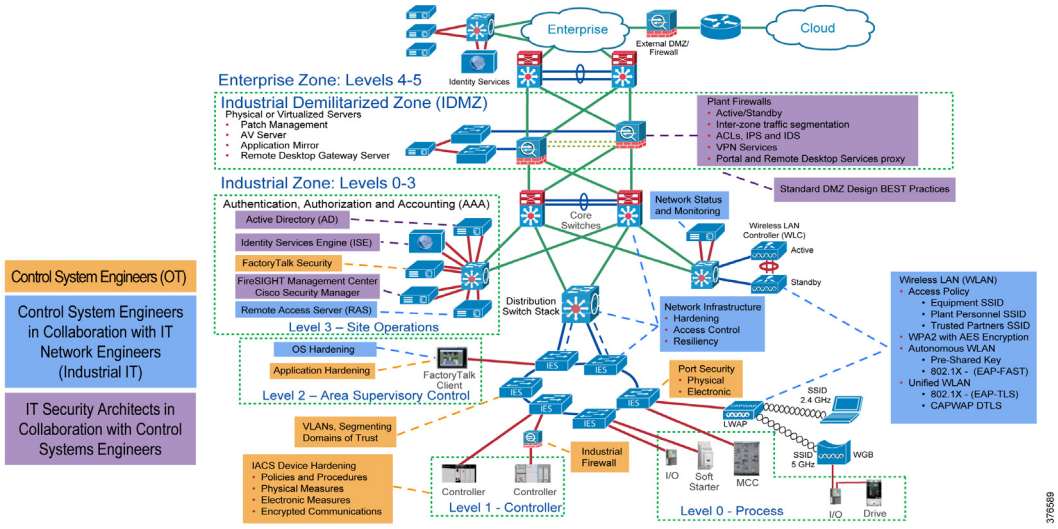
The CPwE Industrial Network Security Framework (see Figure 1-1), which uses a defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA-99) IACS Security (Zones and Conduits) and NIST 800-82 Industrial Control System (ICS) Security (Cybersecurity Framework—Identify, Protect, Detect, Respond, Recover).

Designing and implementing a comprehensive IACS network security framework should serve as a natural extension of the IACS. Network security should not be implemented as an afterthought. The industrial network security framework should be pervasive and core to the IACS. However, for existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the security stance of the IACS.

CPwE defense-in-depth layers (see Figure 1-1) include:

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

Figure 1-1 CPwE Industrial Network Security Framework



Industrial Demilitarized Zone

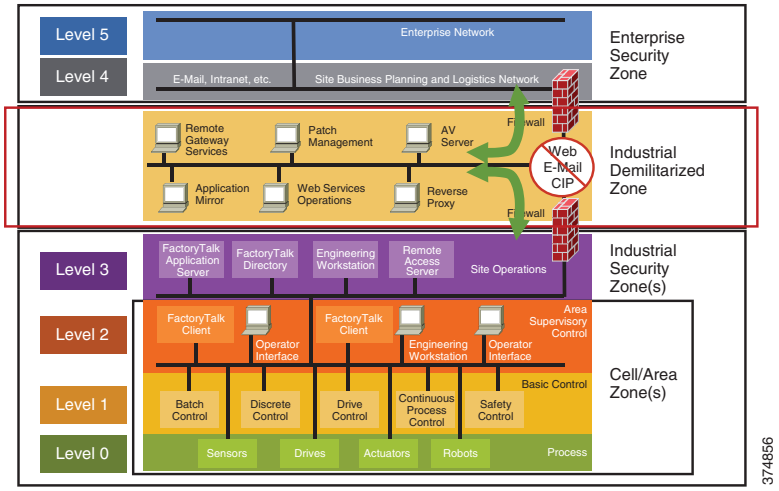
Sometimes referred to as a perimeter network, the IDMZ (see Figure 1-2) is a buffer that enforces data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the Industrial and Enterprise Zones. The demilitarized zone concept is commonplace in traditional IT networks, but is still in early 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 an application mirror, such as a PI-to-PI interface for FactoryTalk® Historian
- Use Microsoft® Remote Desktop (RD) Gateway services
- Use a reverse proxy server

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 1-2 and are covered in CPwE IDMZ.

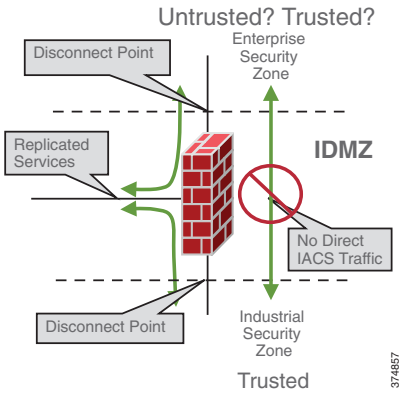
Figure 1-2 CPwE Logical Model



High-level IDMZ design principles (see Figure 1-3) 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 1-3 IDMZ High Level Concepts



Converged Plantwide Ethernet IDMZ

The CPwE IDMZ CVD 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:
  - Application mirror
  - Reverse proxy
  - Remote Desktop Gateway Services
- 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® Mobil, FactoryTalk View Site Edition, FactoryTalk ViewPoint, FactoryTalk AssetCentre, Studio 5000 Logix Designer®)
  - Network services—for example, AD, Cisco Identity Services Engine (ISE), Wireless LAN Controller (WLC) Control And Provisioning of Wireless Access Points (CAPWAP), Network Time Protocol (NTP)
  - Secure Remote Access
- Important steps and design considerations for IDMZ implementation and configuration

CHAPTER 2

System Design Considerations

This chapter includes the following major topics:

This chapter provides a high level overview of the basic design considerations for the Industrial Demilitarized Zone (IDMZ) of the CPwE architecture. This CVD 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. Please 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 IACS 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.

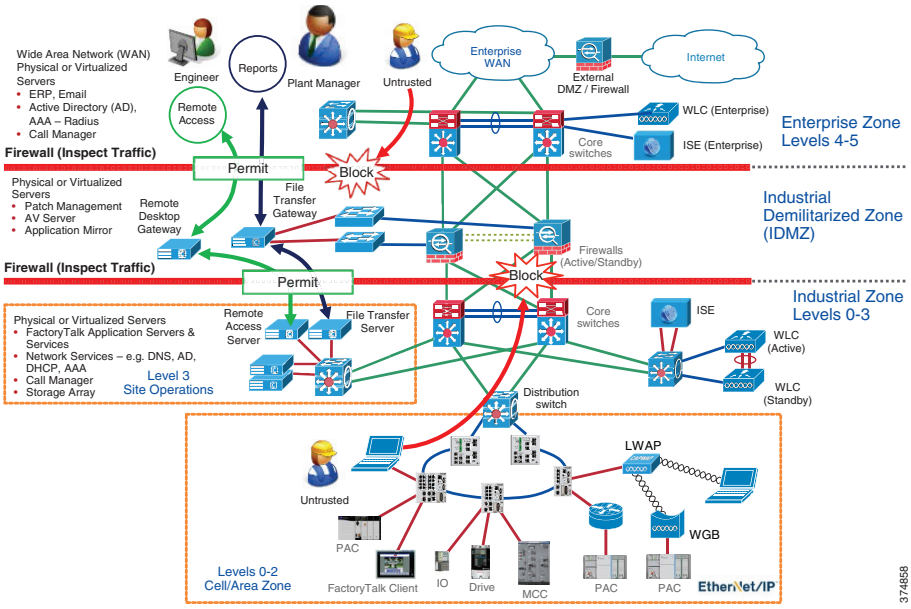
In the context of securing the Industrial Zone from the Enterprise, the IDMZ is placed between a trusted network (the Industrial Zone) and an untrusted network (the Enterprise Zone). The IDMZ functions in the same manner that a traditional DMZ insofar as it allows traffic between the zones to be terminated 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 2-4).

Figure 2-4 IDMZ Concepts



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 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

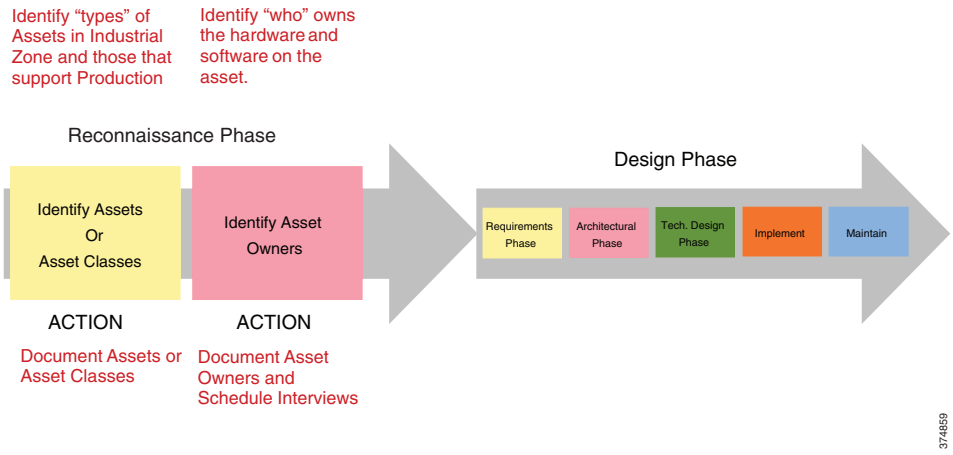
- Which Enterprise users must interact with Industrial Zone systems and the tasks they perform with these systems
- Which Industrial Zone users must interact with Enterprise systems and the tasks they perform
- How long the Enterprise systems can stay disconnected from the Industrial Zone before IDMZ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

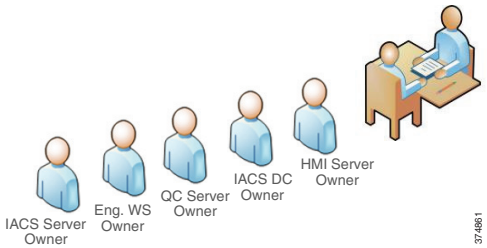
- The **Reconnaissance Phase** is used to identify the assets or "types" of assets in the Industrial Zone used to support production and those that will feed data or reports to Enterprise systems or Enterprise users (see Figure 2-5). The Reconnaissance Phase is used to identify the systems that are located 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 2-5 IDMZ / Network Reconnaissance (Design Pre-Work)



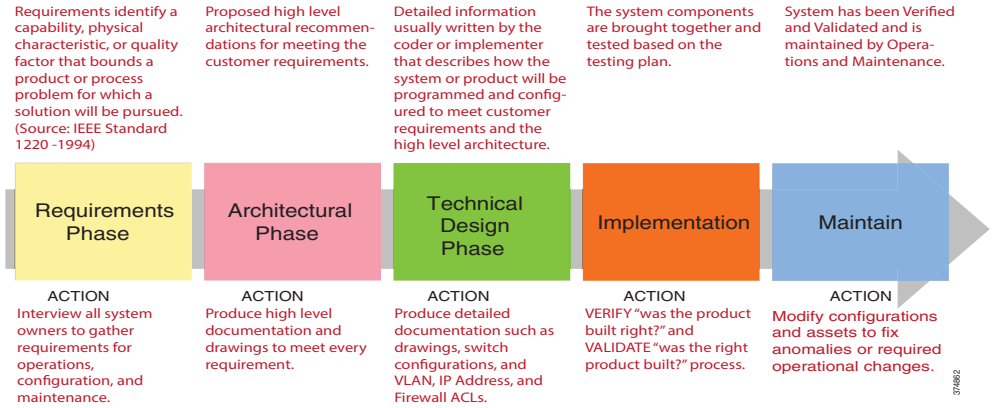
For example, it may be determined that access to a Human Machine Interface (HMI) server from the Enterprise engineering department is required. The asset owner, who would then be interviewed to gather his or her requirements, may state that gaining access to the HMI server to create faceplates or troubleshoot 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 2-6).

Figure 2-6 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 2-7). While this is not the only methodology available, it has been successfully used in the design and implementation of an IDMZ.

Figure 2-7 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: for example, wireless LAN (WLAN) guest tunnel between the Industrial Zone WLC and Enterprise Zone / Guest anchor WLC. 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 CPwE IDMZ architecture tested in this CVD 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 in this CVD.

Table 2-1 IDMZ Security Policy Exceptions

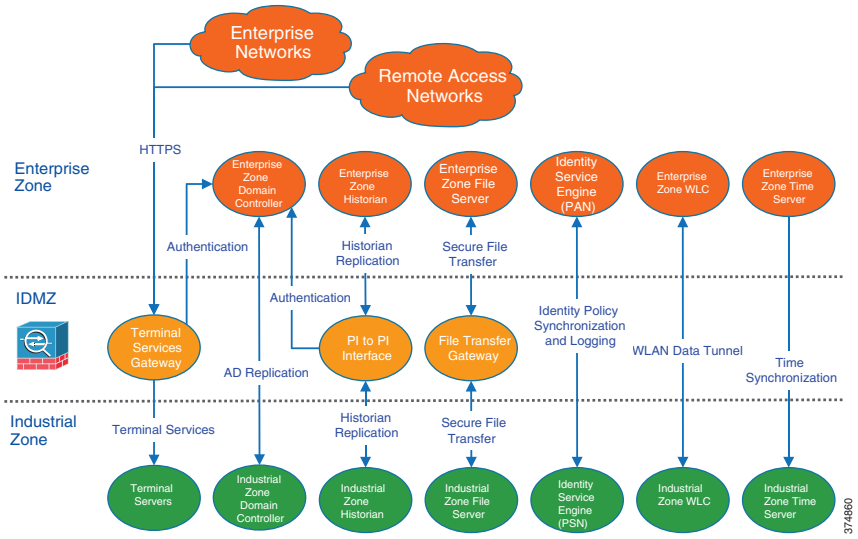
Asset or Technology	Rationale for Exception	Can Additional Assets be Placed in IDMZ?
Domain Controller Replication	Transport and application Layer security; End-to-end encrypted communication; Total cost of ownership	Yes—Additional DC located in IDMZ that would synchronize with the Enterprise and Industrial 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
WLAN Data Tunnel between Industrial Zone WLC and Enterprise Zone/Guest Anchor WLC	Enterprise WLAN infrastructure enforcement of authorization policies for corporate/guest users located in the Industrial Zone; WLAN data is isolated from the Industrial Zone in a secure tunnel	No
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 2-8 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 2-8 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 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 operation requirements
- Enterprise security policy best practices
- Risk assessment
- A holistic security policy based on the defense-in-depth approach
- Industry security standards such as ISA-99
- Manufacturers' corporate standards
- Segmented IACS Network Security Framework
- 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, white and blacklisting technologies just 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 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 his 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 UPD 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.

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 the following URL:

- 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 ASA firewall platform and recommendations for deploying it as part of the CPwE solution.

Cisco ASA Platform Overview

The Cisco ASA with FirePOWER™ Services 5500-X is a next-generation firewall, combining the most widely deployed stateful inspection firewall in the industry with an extensive suite of network security services. In addition to comprehensive stateful inspection firewall capabilities, the ASA 5500-X optionally provides broad and deep network security through an array of integrated cloud- and software-based security services, including Application Visibility and Control (AVC), Web Security Essentials (WSE), Cisco Cloud Web Security (CWS), and the only context-aware, next generation IPS - with no need for additional hardware modules.

The ASA 5500-X Next Generation Firewall is part of the ASA 5500-X Series, which is built on the same proven security platform as the rest of the ASA family of firewalls and delivers exceptional application visibility and control along with superior performance and operational efficiency.

Note For more information on the Cisco ASA firewall platform, refer to *Cisco ASA with FirePOWER Services* at the following URLs:

- http://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html
- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf

Industrial Firewall Functionality

Cisco ASA Firewall Platform with FirePOWER Services 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 ASA with FirePOWER Services features these comprehensive capabilities:

- 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 ASA with FirePOWER next-generation IPS (NGIPS) 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.

Table 2-3 ASA Firewall Features and Benefits

Feature	Benefits
Next-generation firewall (NGFW)	Industry's first threat-focused NGFW; provides ASA firewall functionality, advanced threat protection and advanced breach detection and remediation combined in a single device
Proven ASA firewall	Rich routing, stateful firewall, Network Address Translation (NAT), and dynamic clustering for high-performance, highly secure and reliable access with Cisco AnyConnect® VPN
Market-leading Next-Generation IPS (NGIPS)	Superior threat prevention and mitigation for both known and unknown threats
Advanced malware protection (AMP)	Detection, blocking, tracking, analysis and remediation to protect the enterprise against targeted and persistent malware attacks
Full contextual awareness	Policy enforcement based on complete visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats and URLs
Application control and URL filtering	Application-layer control (over applications, geolocations, users and websites) and ability to enforce usage and tailor detection policies based on custom applications and URLs
Enterprise-class management	Dashboards and drill-down reports of discovered hosts, applications, threats and indications of compromise for comprehensive visibility
Streamlined operations automation	Lower operating cost and administrative complexity with threat correlation, impact assessment, automated security policy tuning and user identification
Purpose-built, scalable	Highly scalable security appliance architecture that performs at up to multi-Gigabit speeds; consistent and robust security across small office, branch offices, Internet edge and data centers in either physical and virtual environments
On-device management	Simplifies advanced threat defense management for small and medium-sized business with small scale deployments
Remote Access VPN	Extends secure corporate network access beyond corporate laptops to personal mobile devices, regardless of physical location; support for Cisco AnyConnect Secure Mobility Solution, with granular, application-level VPN capability, as well as native Apple® iOS and Android® VPN clients
Site-to-site VPN	Protect traffic, including VoIP and client-server application data, across the distributed enterprise and branch offices
Third-party technology ecosystem	Open API that enables the third-party technology ecosystem to integrate with exist-ing customer work streams
Integration with Snort and OpenAppID	Open source security integration with Snort and OpenAppID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
Collective Security intelligence (CSI)	Unmatched security and web reputation intelligence provides real-time threat intelligence and security protection

Firewall Resiliency

The ASA supports two failover modes, active/active failover and active/standby failover. Each failover mode has its own method for determining and performing failover.

- In active/standby failover, one unit is the active unit that passes traffic. The standby unit does not actively pass traffic. When a failover occurs, the standby unit becomes active. You can use active/standby failover for ASAs in single or multiple context modes.
- In an active/active failover configuration, both ASAs can pass network traffic. In active/active failover, you divide the security contexts on the ASA into 2 failover groups. A failover group is simply a logical group of one or more security contexts. One group is assigned to be active on the primary ASA, and the other group is assigned to be active on the secondary ASA. When a failover occurs, it occurs at the failover group level.

The active/active failover mode has certain limitations:

- Active/active failover is only available to ASAs in multiple context modes
- VPN is not supported in multiple context mode or active/active failover
- The load on each device should not exceed 50% of the capacity

Both failover modes support stateful or stateless failover:

- When a stateless failover occurs, all active connections are dropped. Clients need to reestablish connections when the new active unit takes over. Stateless (regular) failover is not recommended for certain firewall features such as clientless SSL VPN.
- When stateful failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

Note More information about ASA resiliency features can be found in *Information About High Availability* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ha_overview.html

Failover System Requirements

This section describes the hardware and software requirements for ASAs 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)
- Be in the same context mode (single or multiple)
- Have the same major and minor software version. However, you can temporarily use different versions of the software during an upgrade process; for example, you can upgrade one unit from Version 8.3(1) to Version 8.3(2) and have failover remain active. It is recommended to upgrade both units to the same version to confirm long-term compatibility.
- Have the same AnyConnect images. If the failover pair has mismatched images when a hitless upgrade is performed, then the clientless SSL VPN connection terminates in the final reboot step of the upgrade process, the database shows an orphaned session, and the IP pool shows that the IP address assigned to the client is "in use."

Failover Link

The two ASA 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. 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 ASA
- 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 regular data interface, such as the inside interface

Sharing a data interface with the Stateful Failover interface is not recommended. Doing so can leave the network vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems.

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.

Connecting to Redundant Switches

To provide redundancy when connecting to distribution or core switches, two or more physical interfaces on the firewalls should be configured as EtherChannels. Cisco ASA firewalls support Link Aggregation Control Protocol (LACP), which is based on the IEEE 802.3ad standard.

An EtherChannel can be connected to a single switch that supports LACP, or a redundant pair of switches that is configured as a single logical unit, for example in a stack or using Virtual Switching System (VSS) technology. The VSS design recommendations and configurations are covered later in the document.

Resiliency Recommendations

The following recommendations can be made for industrial firewall resiliency in the CPwE architecture:

- Configure Active/Standby failover mode in a single security context
- Use Stateful Failover configuration
- Connect the firewalls using a dedicated interface for the failover and Stateful Failover link
- Encrypt failover communication with a failover key
- Use EtherChannels on the active and standby units to connect to redundant core switches

Firewall Policy Design

IDMZ firewall is positioned between highly secure Industrial Zone and less secure 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

Two types of port assignment can be considered for firewall policy design:

- **Static Ports Assignment**—Predefined or well-known TCP/UDP ports are used to configure firewall access rules for most of the applications. Examples of such applications are Domain Name Services (DNS), Network Time Protocol (NTP), Remote Desktop Protocol (RDP), HTTPS and other protocols where one or several fixed ports are used to communicate. Selecting and enabling a set of protocols /ports should be based on each customer's environment and security requirements.
- **Dynamic Ports Assignment**—Some applications use dynamic ports for communications which are negotiated during the initial protocol exchange. An example of such application is Remote Procedure Call (RPC) dynamic port allocation used by many server applications. To effectively secure the application traffic, a firewall has to inspect the application layer in the packet and dynamically open the negotiated port or range of ports between hosts. Well-designed firewall policy should avoid opening large static port ranges for RPC and similar applications.

Application documentation is the first source of information about what ports an application requires. If such information is not available, a test environment allows capturing and analyzing traffic. Cisco ASA firewalls have built-in packet capture tools to help with that. It is, however, not recommended to leave "open" a firewall in a production environment for analysis or troubleshooting.

After application ports have been defined, the list of hosts that can use these ports should also be determined. To simplify access rule configuration, **objects and object groups** are defined on the firewall. Objects are reusable components that are defined and used in ASA configurations in the place of inline IP addresses or TCP/UDP ports. Objects make it easy to maintain your configurations because you can add or modify an object in one place and have it be reflected in all other places that are referencing it.

- Using "any" as source or destination in the firewall access policy is highly discouraged except for certain cases if a source is unknown (for example, a remote VPN user's PC).

The latter sections of this guide have specific examples of configuring firewall access rules.

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.

Note For more information on the Industrial Zone design and topology options, refer to Chapter 4 of the *CPwE Design and Implementation Guide*, found at the following URLs:

Rockwell Automation site:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

Cisco site:

- http://www.cisco.com/en/US/docs/solutions/Verticals/CPwE/CPwE_DIG.html

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 4500/6500/6800 platforms. In addition to having redundant hardware components, core switches should be configured as resilient pairs utilizing VSS technology.

VSS Overview

VSS enables unprecedented functionality and availability of network design by integrating network and systems redundancy into a single node. The end-to-end network enabled with VSS capability allows flexibility and availability described in this design guide.

This virtualization of the two physical chassis into single logical switch fundamentally alters the design of campus topology. One of the most significant changes is that VSS enables the creation of a loop-free topology. In addition, VSS also incorporates many other Cisco innovations such as Stateful Switch Over (SSO) and Multi-chassis EtherChannel (MEC) that enable non-stop communication with increased bandwidth to substantially enhance application response time. Key business benefits of the VSS include the following:

- Reduced risk associated with a looped topology
- Non-stop business communication through the use of a redundant chassis with SSO-enabled supervisors
- Better return on existing investments via increased bandwidth to the access and distribution layer
- Reduced operational expenses through increased flexibility in deploying and managing new services with a single logical node
- Reduced configuration errors and elimination of First Hop Redundancy Protocols, such as Hot Standby Routing Protocol (HSRP), Gateway Load Balancing Protocol (GLBP) and Virtual Router Redundancy Protocol (VRRP)
- Simplified management of a single configuration and fewer operational failure points

Note More information on VSS design and implementation can be found in *Virtual Switching Systems (VSS)* at the following URL:

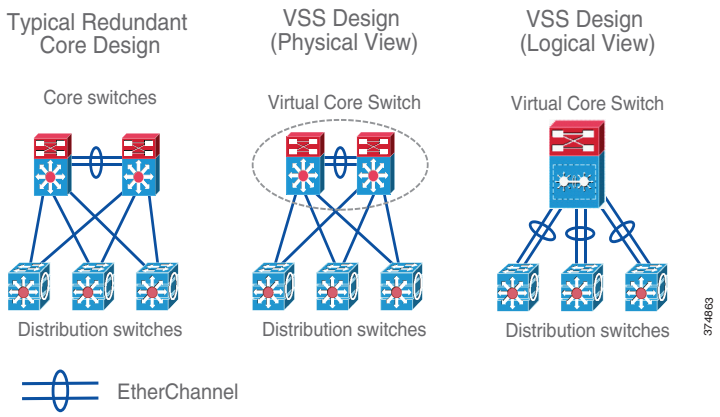
- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/virtual_switching_systems.html

VSS Topology

Network administrators increase network reliability by configuring switches in redundant pairs and by provisioning links to both switches in the redundant pair. Redundant network elements and redundant links can add complexity to network design and operation. Virtual switching simplifies the network by reducing the number of network elements and hiding the complexity of managing redundant switches and links.

Figure 2-9 compares a traditional redundant core network design (two stand-alone physical chassis) and a VSS core design from the physical and logical perspective. VSS mode combines a pair of switches into a single network element and manages the redundant links, which externally act as a single port channel. VSS mode simplifies network configuration and operation by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

Figure 2-9 Traditional vs. VSS Core Design



Active and Standby Chassis

When you create or restart a VSS, the peer chassis negotiate their roles. One chassis becomes the active chassis, and the other chassis becomes the standby.

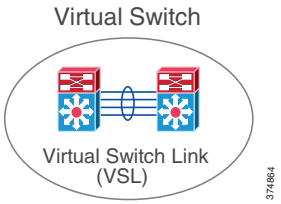
The active chassis controls the VSS. It runs the Layer 2 and Layer 3 control protocols for the switching modules on both chassis. The active chassis also provides management functions for the VSS, such as module online insertion and removal (OIR) and the console interface.

The active and standby chassis perform packet forwarding for ingress data traffic on their locally hosted interfaces. However, the standby chassis sends all control traffic to the active chassis for processing.

Virtual Switch Link

For the two chassis of the VSS to act as one network element, they need to share control information and data traffic. The virtual switch link (VSL) is a special link that carries control and data traffic between the two chassis of a VSS (see Figure 2-10). The VSL is implemented as an EtherChannel with up to eight links. The VSL gives control traffic higher priority than data traffic so that control messages are never discarded. Data traffic is load balanced among the VSL links by the EtherChannel load-balancing algorithm.

Figure 2-10 Virtual Switch Link



The VSL EtherChannel supports only 10-Gigabit or 40-Gigabit Ethernet ports on the Cisco 6500 and 6800 platforms, and 10-Gigabit or 1-Gigabit ports on the Cisco 4500 platform. The ports can be located on the supervisor engine (recommended) or on one of the switching modules.

- Use 10-Gigabit ports for the VSL EtherChannel, if available, on Cisco 4500 switches
- Use the supervisor engine ports (10-Gigabit) for the VSL. Optionally, you can configure the VSL port group on switching modules for additional capacity.

Redundancy and High Availability

In VSS mode, supervisor engine redundancy operates between the active and standby chassis, using SSO and nonstop forwarding (NSF). The peer chassis exchange configuration and state information across the VSL and the standby supervisor engine runs in hot standby mode.

The standby chassis monitors the active chassis using the VSL. If it detects failure, the standby chassis initiates a switchover and takes on the active role. When the failed chassis recovers, it takes on the standby role.

If the VSL itself fails, the standby chassis assumes that the active chassis has failed, and initiates a switchover. After the switchover, if both chassis are active, the dual-active detection feature detects this condition and initiates recovery action.

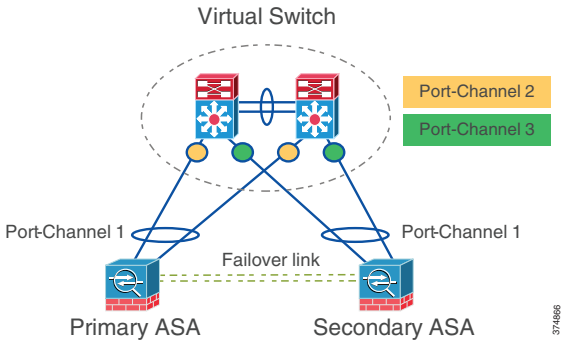
The CPwE architecture recommends enabling SSO and NSF on the industrial core switches in the VSS mode.

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 VSS is used, the ASA 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 ASA in an active/standby failover deployment (see Figure 2-11). A single EtherChannel on the VSS switch pair will not be established because of the separate ASA system IDs, and would not be desirable anyway because traffic should be sent only to the active ASA.

Figure 2-11 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, 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

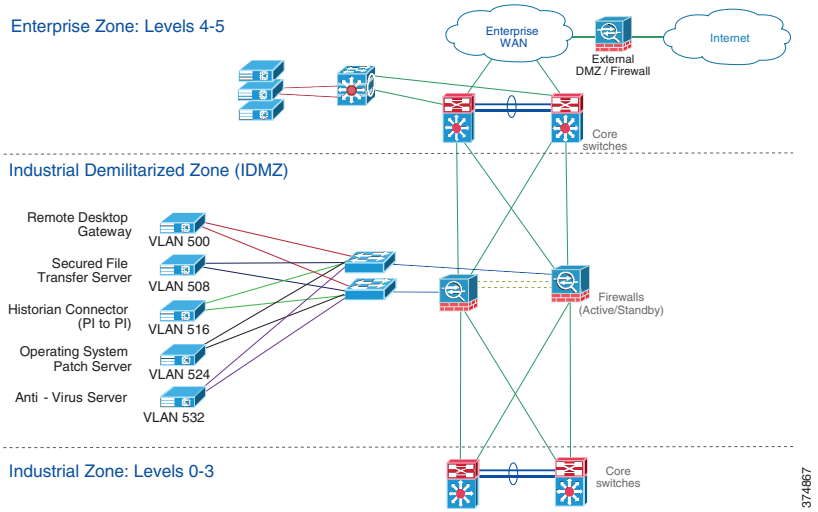
The resiliency features should include:

- 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 2-12), every IDMZ host such as the RD Gateway or the Secure File Transfer server has been put onto its own network or VLAN.

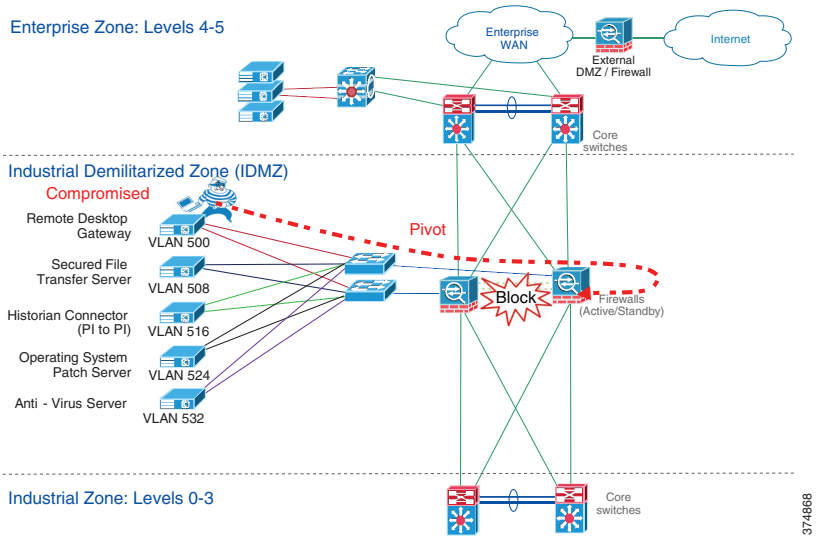
Figure 2-12 VLAN Segmentation in IDMZ Network



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 2-13).

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 2-13 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 the following URL:

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

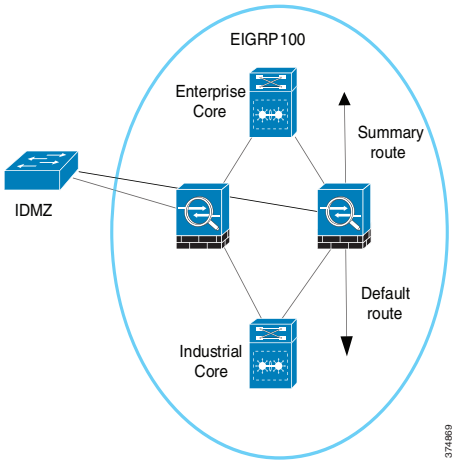
EIGRP Design

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 2-14). 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 2-14 Single EIGRP Domain



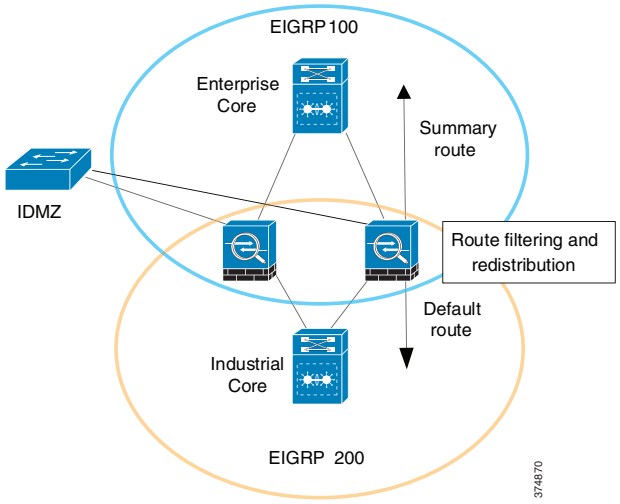
This design, which allows for end-to-end routing from the Industrial Zone to the Enterprise Zone, works best if a single administrative team is responsible for all network devices across the company. Since all routers are a part of a common routing domain, the risk that routing protocol instability in 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 2-15). 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 2-15 Multiple EIGRP Domains with Redistribution



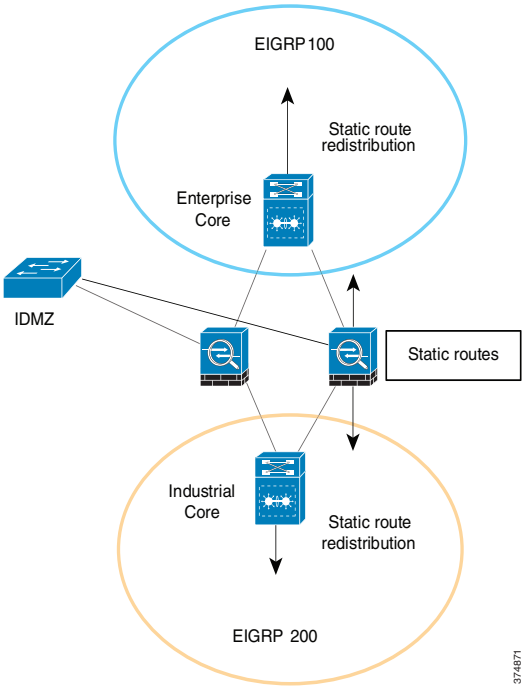
This design also allows for end-to-end routing between the Enterprise and Industrial Zones. However, this design divides the EIGRP routing process into smaller domains. This reduces the possibility of a routing protocol instability in one zone affecting another. This solution fits best with medium-to-large 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 2-16).

Figure 2-16 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 the following URL:

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

OSPF Design

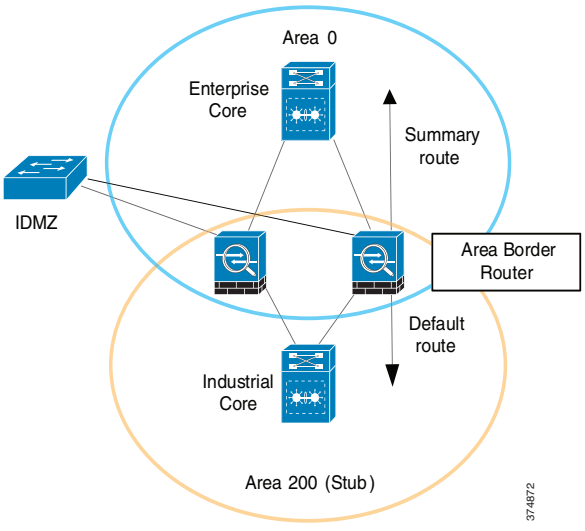
This section contains OSPF design options and considerations, such as scalability, routing policy and configuration complexity.

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 2-17.

Figure 2-17 Single OSPF Domain with Stub Areas



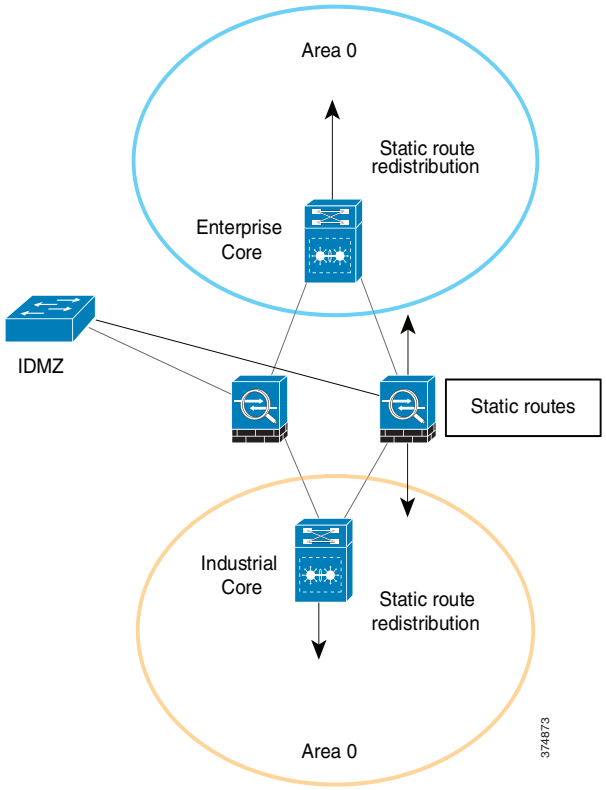
This design also allows for end-to-end routing between the Enterprise and Industrial Zones. OSPF naturally subdivides the routing protocol into areas. This solution fits best with medium-to-large networks and easily accommodates environments with multiple Industrial Zones.

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 2-18.

Figure 2-18 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
- WLAN Personnel Access

Active Directory Services

Microsoft 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, please refer to *Active Directory Domain Services* at the following URL:

- 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 the following URL:

- 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, please 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). Getting replication to function properly across security perimeters can be challenging. Three possible approaches exist:

- Open the firewall wide 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.

Given the limitation of leaving the firewall wide open, and lack of deep inspection capabilities for IPsec tunnel traffic because of encryption that IPsec applies, Cisco ASA implements a **DCERPC inspection** mechanism to target the requirement for secure AD replication. The DCERPC Pinhole feature dynamically opens necessary ports for a limited time in order to avoid opening a large port range on the firewall for the RPC traffic.

More details of the DCERPC operations are listed below:

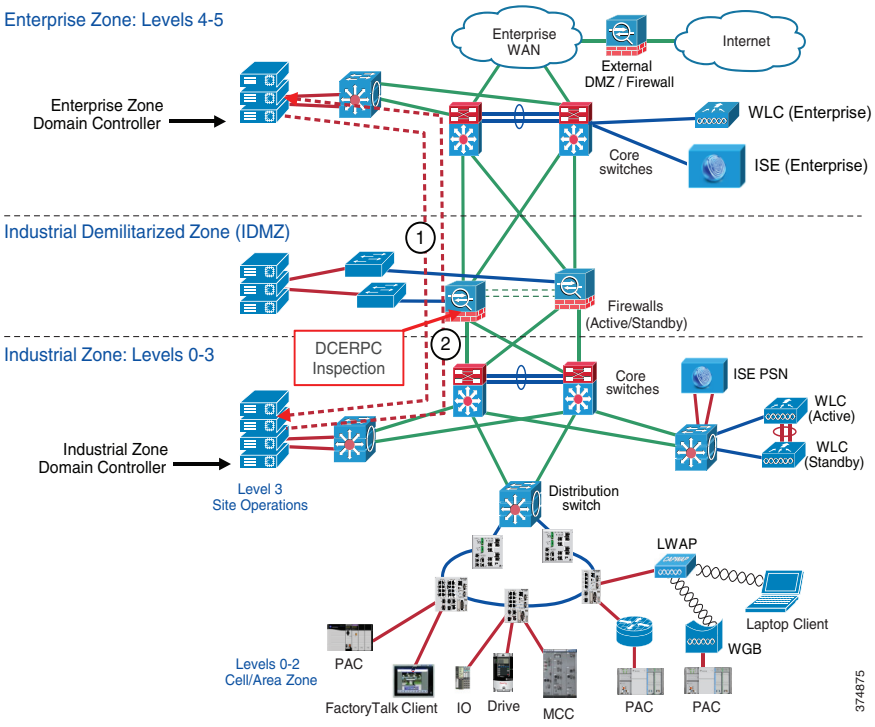
- An RPC service configures itself in the registry with a universally unique identifier (UUID). UUIDs are well-known identifiers unique for each service and common across all platforms.
- When an RPC service starts, it obtains a free high port and registers that port with the UUID. Some services use 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 DCERPC 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.
- Because a client can attempt multiple connections to the server port returned by the EPM, creation of multiple pinholes is allowed. User configurable timeouts are allowed for multiple pinholes.

Note For detailed information, please refer to *Active Directory and Active Directory Domain Services Port Requirements* at the following URL:

- https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx

Figure 2-19 illustrates the AD replication between the DCs in the Industrial and Enterprise Zones.

Figure 2-19 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. Please 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 2-32).

Table 2-6 shows an example of protocols that may be required for AD authentication. Please 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 the following URL:

- https://technet.microsoft.com/en-us/library/dd772723(v=ws.10).aspx

Certificate Services

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

Note This CVD 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 document.

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, please refer to *Active Directory Certificate Services* at the following URL:

- 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.

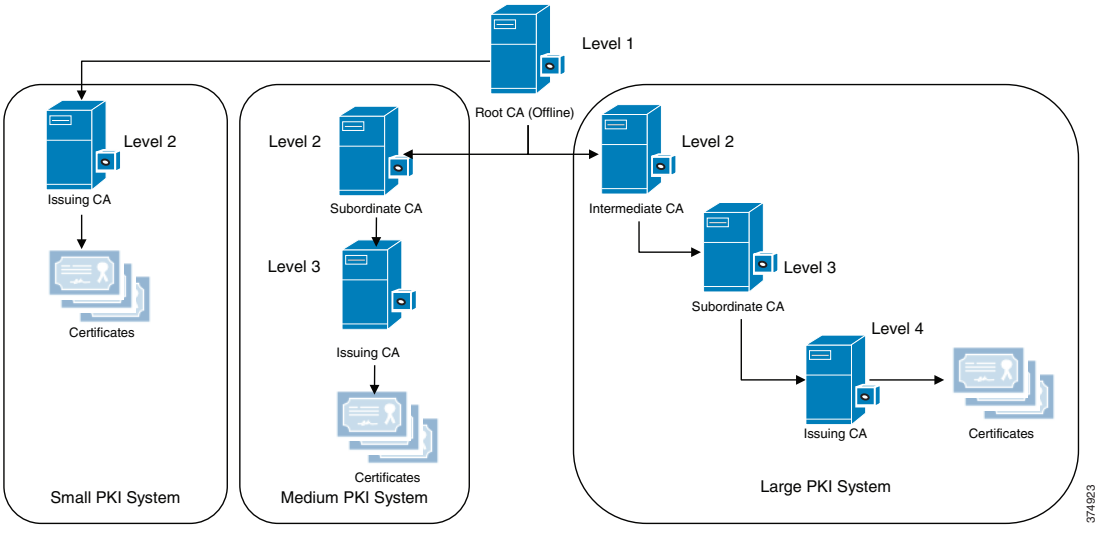
- Root CA is the most trusted CA in a CA hierarchy and is the first CA installed in the network. When a root CA remains online, it is used to issue certificates to the intermediate and subordinate CAs. Most times, the root CA remains offline to protect the private keys. The root CA rarely issues certificates 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 2-20 shows the CA hierarchy and various deployment models depending on the system scale.

Figure 2-20 PKI Infrastructure Models Example



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.

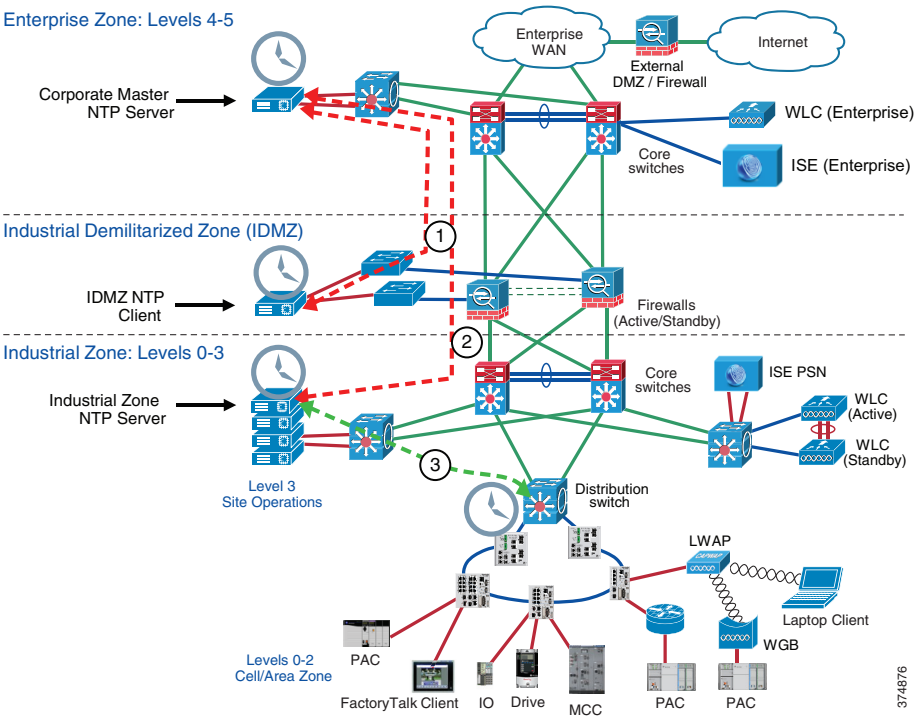
Note For more information on the Windows Time Service, refer to *Windows Time Service Technical Reference* at the following URL:

- https://technet.microsoft.com/en-us/library/cc773061%28v=ws.10%29.aspx

Figure 2-21 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 2-21 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 the following URL:

- 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.

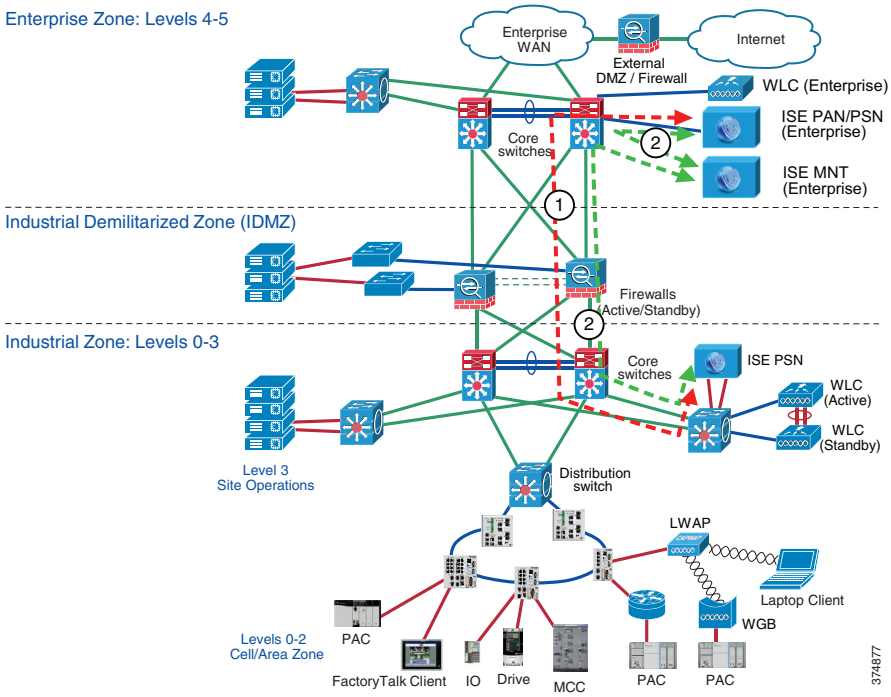
ISE Architecture in IDMZ

Within the CPwE IDMZ architecture, the recommendation is to deploy the Cisco ISE platform as a distributed solution (see Figure 2-22).

- 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 3-18 for details).

Figure 2-22 Distributed ISE Architecture



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 Mn1T.

WLAN Personnel Access

This section provides an overview of the Cisco Unified WLAN architecture in the CPwE IDMZ.

Note This design guide addresses specifically WLAN data traversal through IDMZ. The WLAN personnel access in the Industrial Zone is covered in more details in the *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at the following URL:

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

Unified WLAN Overview

The CPwE WLAN architecture is tailored to address IEEE 802.11 wireless networking of IACS equipment and plant personnel within the Industrial Zone of the plant. The Cisco Unified WLAN architecture has the ability to address large-scale plant-wide 802.11 wireless needs.

The Unified WLAN architecture allows for centralized management and control of the wireless access points distributed throughout the plant. By utilizing a WLC and Lightweight Access Points (LWAP), a centralized management model is created, thus introducing security and self-healing mechanisms to the wireless architecture. The Unified WLAN architecture also introduces foundational services, including intrusion prevention and wireless guest access, for better control over devices seeking to connect to the WLAN.

Note Information about Cisco Unified WLAN can be found at the following URL:

- http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-mobility/index.html

Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture provides the CPwE WLAN architecture for IACS applications:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

WLAN Personnel Access Architecture in IDMZ

One of the main use cases for wireless access in the Industrial Zone is connectivity for corporate employees and trusted partners (OEMs, vendors) on the plant floor. Corporate employees should have access to resources in the Enterprise Zone while being isolated from the Industrial Zone network. In case of the trusted partner access, a user should be directed to a secure portal outside the Industrial Zone where access only to certain assets is provided based on user's identity.

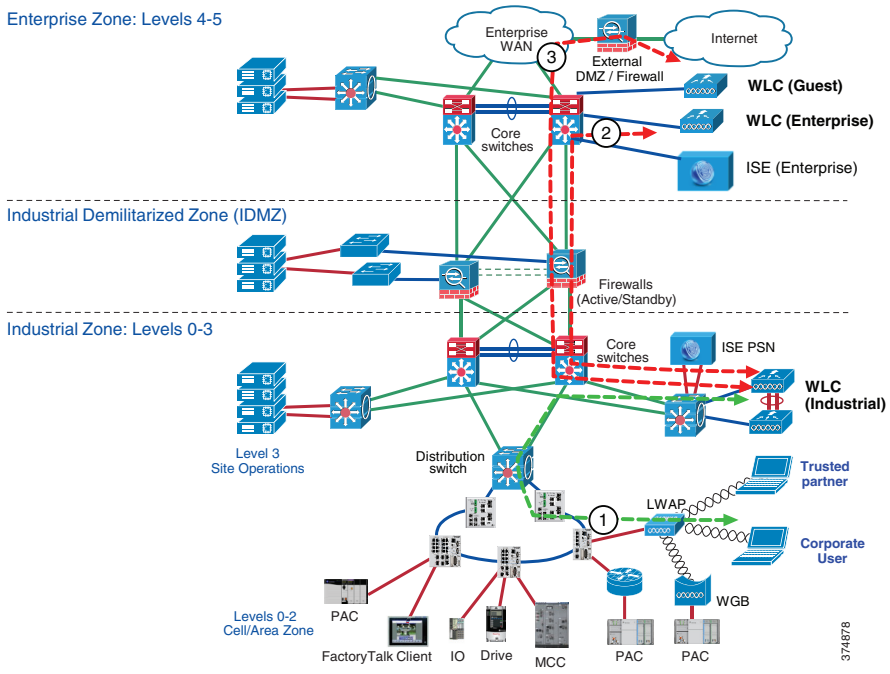
CPwE architecture achieves these goals by providing secure path for wireless user's data through the IDMZ. As part of the Unified WLAN architecture, the Industrial Zone WLC and the "anchor" WLCs in the Enterprise Zone or the corporate DMZ create a secure communication tunnel that provides complete segmentation of user's data. The exact data path depends on the wireless Service Set Identifier (SSID), which is different for an industrial employee, a corporate Employee and a trusted partner.

The CPwE IDMZ architecture provides authentication and authorization for wireless users for granular access to resources in the Enterprise Zone or to a remote access portal in the IDMZ.

The IDMZ firewall needs to allow the tunneled communication between WLCs. Details are provided in WLAN Access Configuration, page 3-19.

Figure 2-23 demonstrates the wireless access for a corporate user and a trusted partner and WLAN data traversal through IDMZ.

Figure 2-23 WLAN Data Traversal



1. A corporate user or trusted partner connects as a wireless client to a lightweight AP and authenticates to the WLAN. The data packets from the user's wireless device are encapsulated in the CAPWAP tunnel and are sent to the Industrial WLC.
2. In the case of the corporate user, the WLAN traffic is sent in the secure tunnel between the Industrial and the Enterprise Anchor WLC. Depending on the user's access level and the application, the user can then access corporate resources or IDMZ applications such as RD Gateway.
3. In the case of the trusted partner or guest user, the data is sent in the secure tunnel to the Guest Anchor WLC, which is located in the corporate DMZ. The user then can be given the appropriate access, for example, to a VPN portal.

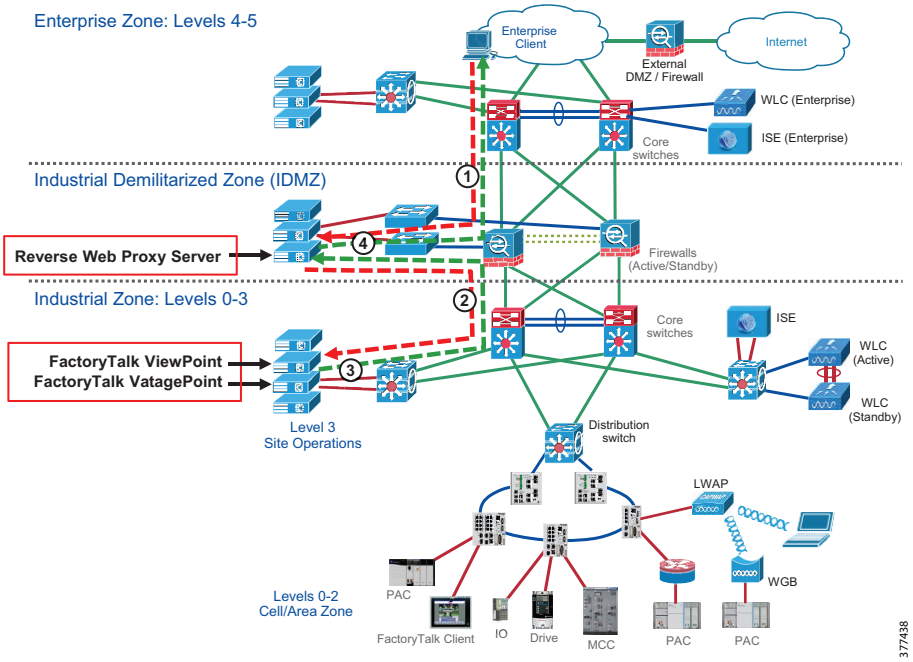
FactoryTalk Application Access through the IDMZ

Building upon the CPwE IDMZ broker services approach, a reverse web proxy server is deployed in the IDMZ. This allows secure access from clients in the Enterprise Zone to FactoryTalk Applications in the Industrial Zone.

For the purpose of this CVD, Microsoft's IIS web server with the addition of Application Request Routing (ARR) was used as the reverse web proxy solution. This setup uses URL rewrites to broker service sessions between Enterprise Zone clients and Industrial Zone FactoryTalk Application servers.

For this CVD, two specific FactoryTalk applications were configured, tested and validated: FactoryTalk VantagePoint Mobile and FactoryTalk ViewPoint. Figure 2-24 shows this particular setup. The four bulleted steps describe the request flow, as seen from an enterprise client accessing resources from a FactoryTalk Application server in the Industrial Zone.

Figure 2-24 Reverse Web Proxy Operation



1. A client in the Enterprise Zone requests the desired FactoryTalk Application resource by sending an HTTP(S) request to the reverse web proxy server.
2. The reverse web proxy server uses an inbound URL rewrite rule to relay this request to the targeted FactoryTalk Application server located in the Industrial Zone.
3. The FactoryTalk Application server responds to the reverse web proxy with the requested resources.
4. The reverse web proxy uses an outbound URL rewrite rule to parse the response, looking for any references pointing back to the FactoryTalk Application server, and changes those references to point to itself. The reverse web proxy server then forwards the adjusted response to the enterprise client.

For a detailed description of how to configure the IIS reverse web proxy server and the FactoryTalk VantagePoint and FactoryTalk ViewPoint servers, please refer to Configuring the Infrastructure.

Data Transfer through 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
- Managed file transfer

FactoryTalk Historian Data Transfer

Access to process and operational data is often a key requirement for setting up an industrial network. This data can, amongst 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 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 the following URL:

- 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.

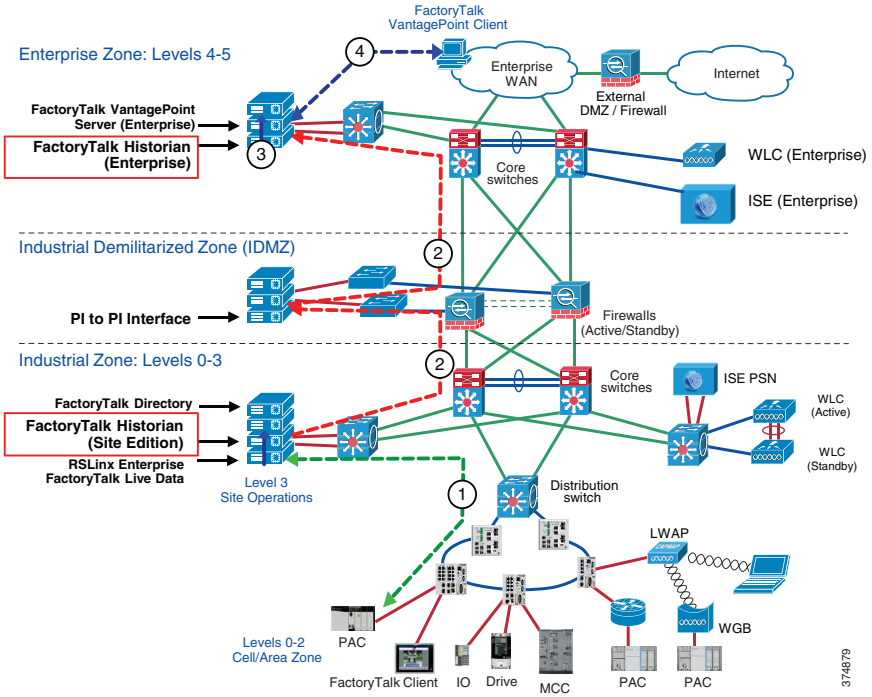
One of the main design goals of the CPwE is no direct traversal of data from the Enterprise Zone to the Industrial Zone or vice versa. In order to securely replicate production data to the Enterprise Zone, a PI-to-PI (Historian to Historian) replication service can be installed on a server in the IDMZ.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

FactoryTalk Historian IDMZ Architecture

Figure 2-25 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 2-25 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 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.

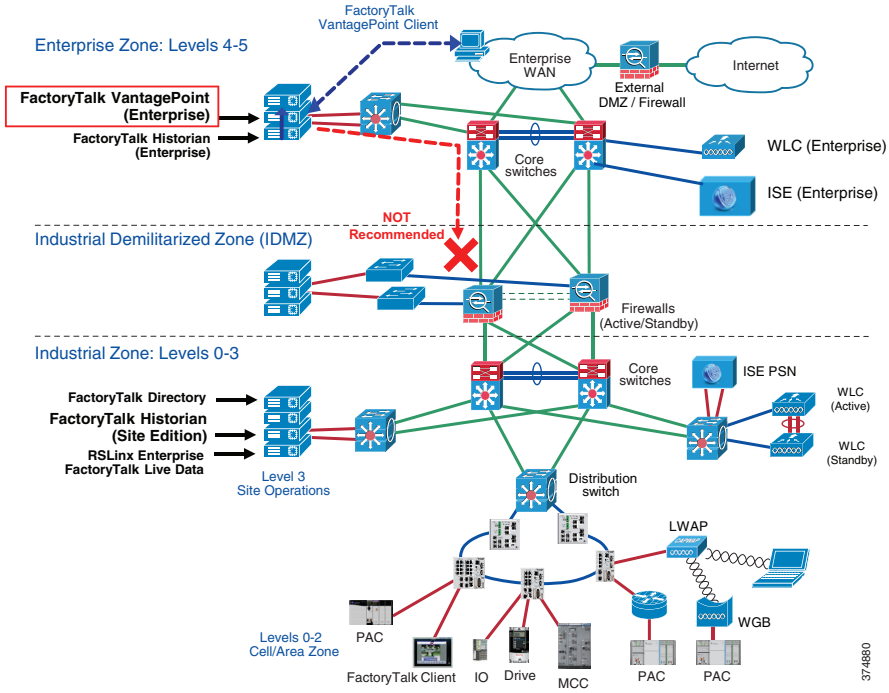
An overview of PI-to-PI Interface configuration and firewall rules for the Historian data transfer is provided in FactoryTalk Historian Data Transfer Configuration, page 3-44.

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 VantagePoint clients do not cross security boundaries to obtain Historian information or connect to a VantagePoint server in another security zone. For instance, it is not recommended for an Enterprise VantagePoint server or client to connect directly to the Industrial Zone Historian (see Figure 2-26).
- 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 2-26 FactoryTalk VantagePoint in Enterprise Zone



Managed 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 unsecure or introduce significant risks to the industrial environment. Managed File Transfer (MFT) solutions provide a secure way to accomplish the task in compliance with the IDMZ design principles.

Overview of 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 MFT servers located in the Enterprise and Industrial Zones.

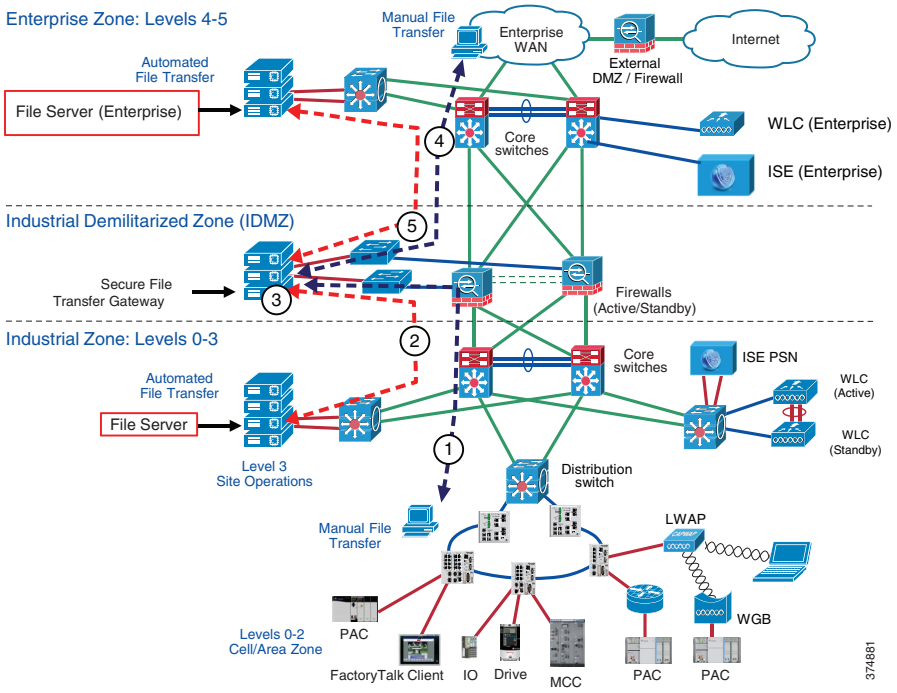
This approach allows for secure file transfers between the zones using the IDMZ gateway as a proxy. An industrial MFT system should have the following characteristics:

- All incoming connections are accepted on a hardened MFT gateway in the IDMZ using a secure protocol, for instance Secure File Transfer Protocol (SFTP), FTP over SSL or HTTPS.
- 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.

MFT Architecture

Figure 2-27 provides an overview of the MFT architecture for the CPwE IDMZ.

Figure 2-27 Managed 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 enterprise user logs onto the Secure File Transfer Gateway and retrieves the file.
5. 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.

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 Cisco ASA firewall platform
- Microsoft RD Gateway
- Cisco ASA RDP Plug-In Portal

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.
  - 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 Cisco ASA firewalls support a number of VPN technologies, including web-portal based SSL VPNs for client-based or clientless remote access, and IPsec VPN for secure tunnel site-to-site communication. SSL access can be more flexible and is likely to be accessible from more locations than IPsec, as few companies block HTTPS access out of their networks.

Two models can be applied for remote access VPN with Cisco ASA firewall:

- **Integrated Design Model**—Remote Access VPN is integrated on the same Cisco ASA appliances that provide firewall functions. This integration offers lower capital investment and reduces the number of devices to manage.
- **Standalone Design Model**—Remote Access VPN is deployed on a pair of standalone Cisco ASA appliances. This design offers greater operational flexibility and scalability while providing a simple migration path from an existing VPN installation.

The SSL VPN can be implemented as a software client-based VPN (AnyConnect client on the user's PC) or as a clientless SSL VPN.

Note Additional information about remote access and VPN technologies can be found in the *Secure Remote Worker Design Guide:* at the following URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/srw-design-guide.pdf

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 ASA 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 clientless VPN connections. The ASA 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 ASA configuration) when the connection terminates. In the case of a previously installed client, when the user authenticates, the ASA examines the revision of the client and upgrades the client as necessary.

Clientless SSL VPN

The ASA Clientless SSL VPN provides SSL remote access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. This browser-based VPN lets users establish a secure, remote-access VPN tunnel to the ASA. After authentication, users access a portal page and can access specific supported internal resources. The network administrator provides access to resources on a user group basis. Users have no direct access to resources on the internal network.

SSL VPN Configuration, page 3-49 contains configuration examples for the AnyConnect VPN and clientless SSL VPN on the ASA platform.

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 2008 R2. A Windows Server with the RD Gateway role enabled allows authorized remote users 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 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.

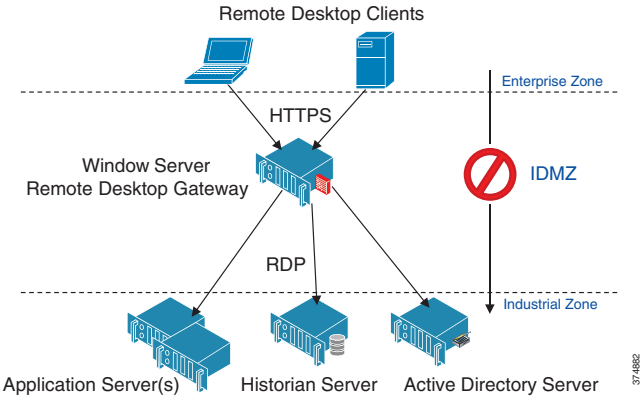
Note For more information, refer to *Remote Desktop Services Overview* at the following URL:

- https://technet.microsoft.com/en-us/library/hh831447.aspx

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 3-62 has an example of defining a remote access rules and configuring the RD Gateway policies.

Cisco ASA RDP Plug-In

The ASA clientless SSL VPN portal supports access to Microsoft Terminal Servers in the Industrial Zone using an RDP Java plug-in. The plug-in uses the Proper Java RDP applet as the client. The advantage of the plugin is that it does not rely on an RDP client on the local computer. However, the Proper Java RDP client has a number of limitations when compared to Microsoft's Remote Desktop Connection client:

- No remote audio
- No local printers
- No local drives

The client establishes a connection to the ASA clientless VPN web portal using SSL. The firewall then creates a RDP session to the internal network resources. The remote desktop user has 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.

ASA RDP Plug-In Architecture in the IDMZ

The RDP plug-in is installed on the ASA firewall and is accessed through the clientless VPN web portal. The portal authenticates and authorizes users against AD. After authenticating, the user is presented number of bookmarks on the portal.

The RDP bookmarks allow for preconfigured RDP sessions to the terminal servers in the Industrial Zone. The bookmarks use a URL to pass configuration parameters to the plug-in. The portal may need to have multiple bookmarks to the same terminal server with different options such as screen resolution.

By default, clients connected to the ASA web portal will have access to all hosts in the Industrial Zone using the following protocols listed in Table 2-7:

Table 2-7 Protocols Available via ASA Web Portal

URL Protocol	Application
http://	Web traffic
https://	Secure web traffic
cifs://	Windows file shares
ftp://	File transfer protocol
citrix://	Citrix client*
rdp://	Remote desktop protocol client*
ssh://	Secure shell client*
telnet://	Telnet client*
vnc://	VNC client*

* Applications marked with an asterisk require a firewall plug-in.

It is important to use Web ACLs to limit portal access to specific sites in the Industrial Zone. Web ACLs allow the firewall to restrict which URLs are accessible from the VPN portal. The ACLs allow for the use of wildcards matching multiple URLs in one entry. Like all ACLs, an implicit *deny all* rule exists in the end that is enforced when the ACL is applied.

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:

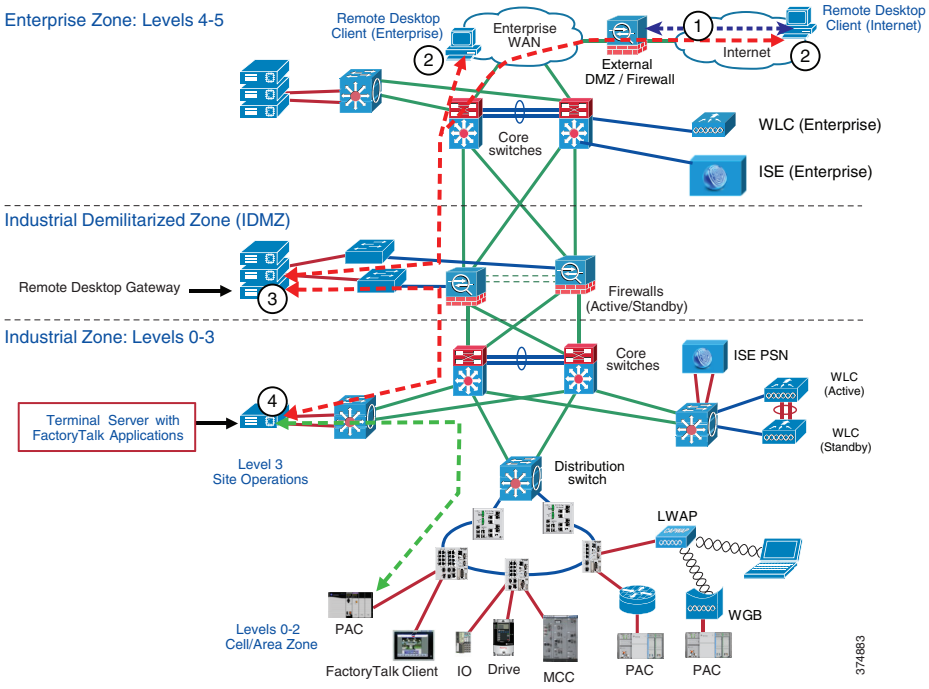
- Applications are installed and run on the terminal server in the Industrial Zone.
- Applications are installed and run on separate servers and accessed directly from the RD Gateway.

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

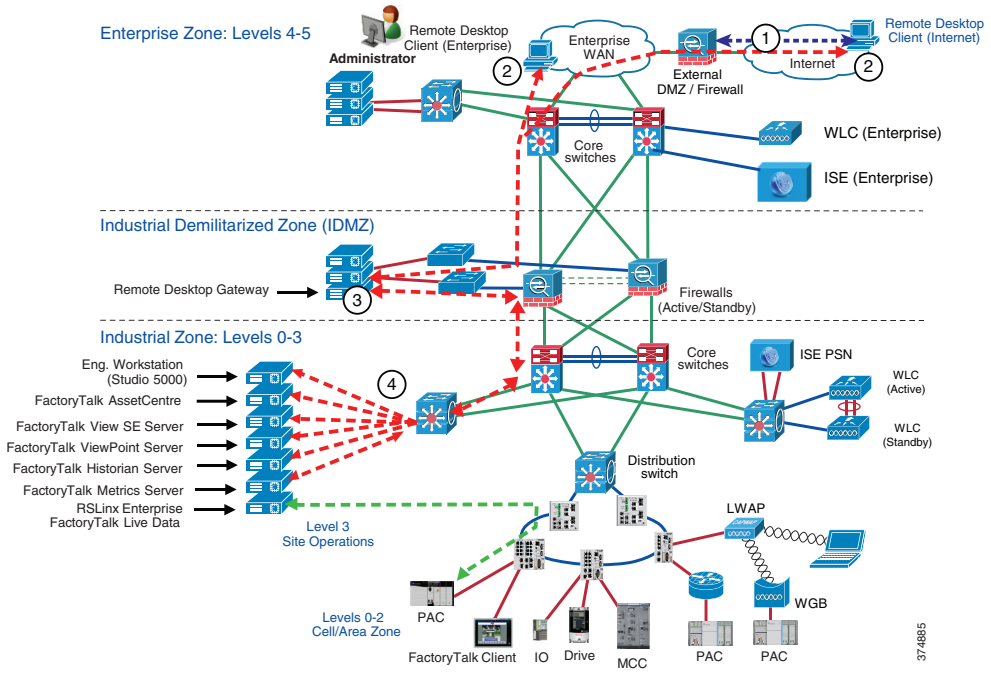


1. If the Remote Desktop client is outside the corporate network, a VPN session is established with the customer site.
2. The RDC application is launched from remote user's computer. The user enters Industrial Zone Remote Session Host's address (the Terminal Server running FactoryTalk applications) as 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

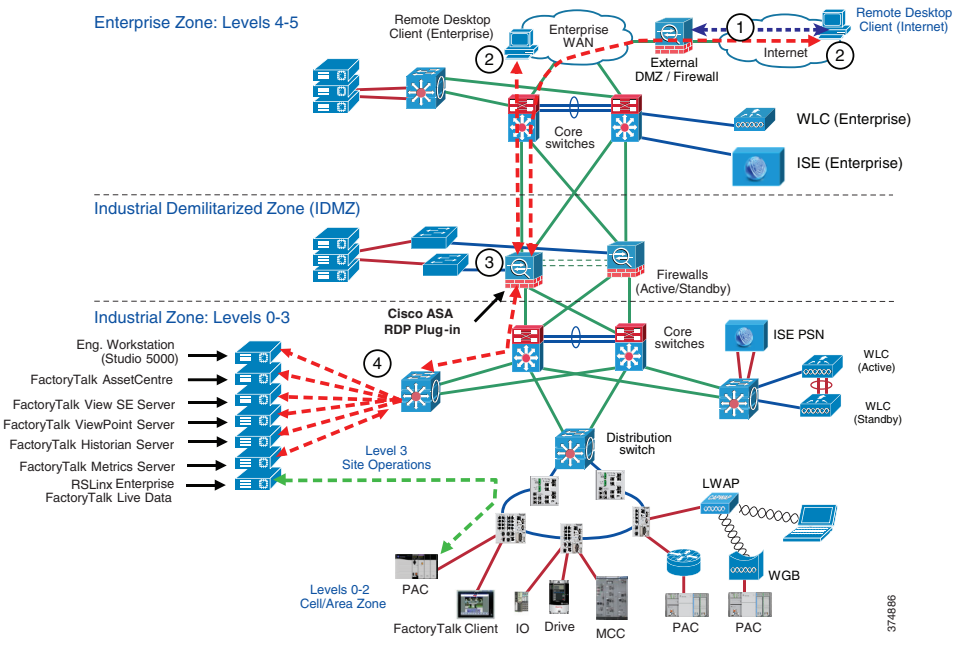


1. If the RD client is outside the corporate network, a VPN Session is established with the customer site.
2. Remote Desktop Connection application is launched from remote user's computer. The user enters Industrial Zone host's address as the target desktop and starts the session.
3. The RD Gateway server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

FactoryTalk Application Access via ASA Remote Desktop Plug-In

Access to FactoryTalk applications via the ASA Remote Desktop (RD) Plug-in is similar to the direct RD Gateway access described in the previous section. The traffic flow is presented in Figure 2-31.

Figure 2-31 Access to FactoryTalk Applications via Cisco ASA RD Plug-in



1. If the RD client is outside the corporate network, a VPN Session is established with the customer site.
2. User enters the Cisco ASA Firewall URL in the Internet browser and is authenticated to the firewall.
3. The ASA portal presents the pre-configured URLs of the Industrial Zone servers running FactoryTalk applications to the remote user.
4. The Remote Session Host's desktop is now presented to the remote desktop user.

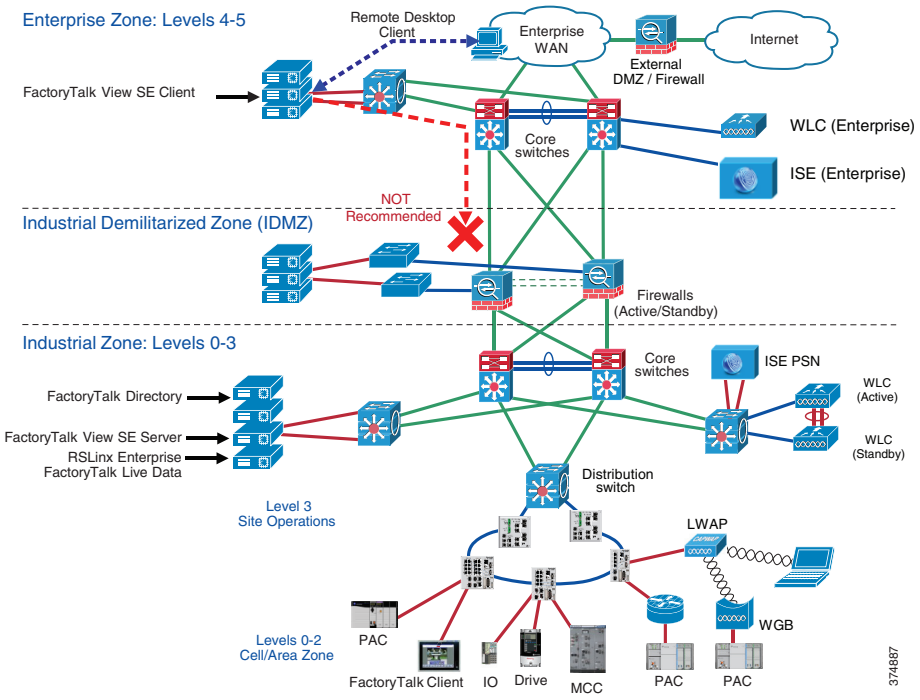
Examples of Non-Recommended Architectures

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 2-32 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 configuration is not recommended.

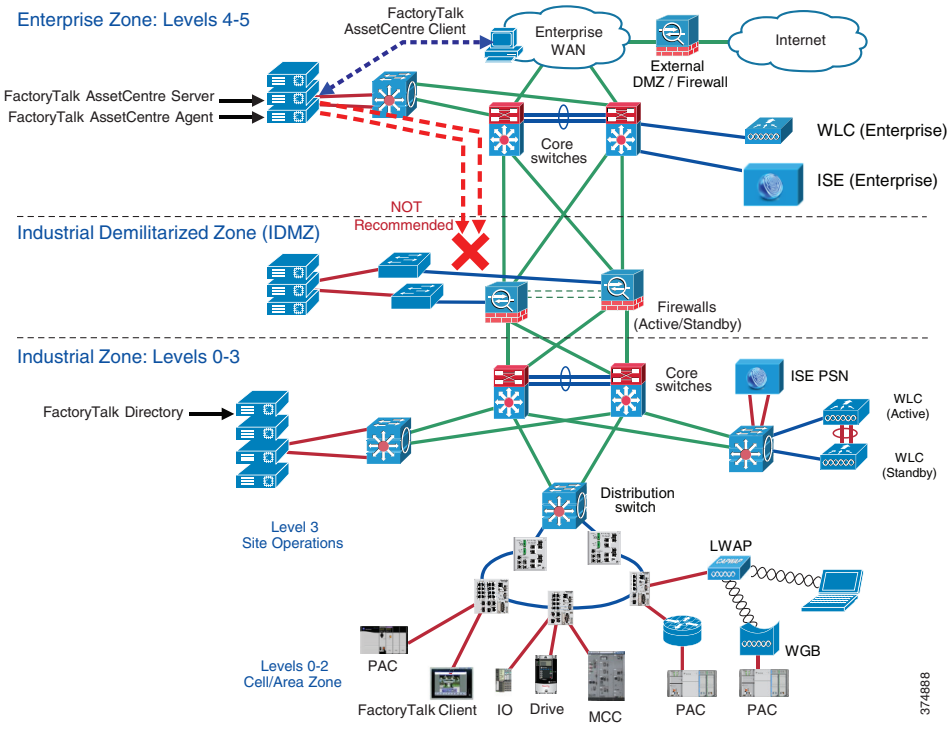
Figure 2-32 FactoryTalk View SE Client (Enterprise) - Not Recommended



In another example (see Figure 2-33), 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 configuration is not recommended.

Figure 2-33 FactoryTalk AssetCentre (Enterprise) - Not Recommended



FactoryTalk Application Access through IDMZ

This section describes fundamental concepts of web proxy technologies that help protect web-based resources from one security area to another. This section also describes the reverse web proxy technology as a method for providing the ability to access FactoryTalk Applications data securely through the Industrial Demilitarized Zone within the CPwE architecture.

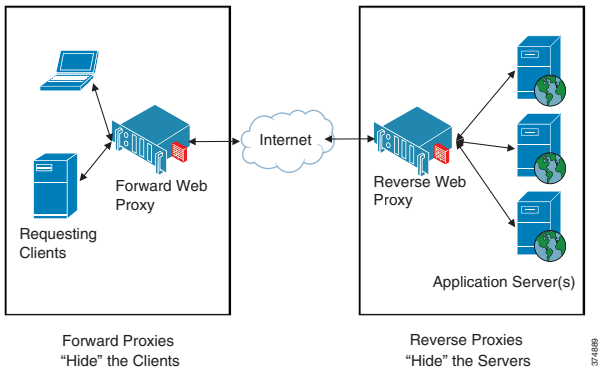
Web Proxies

Web proxy servers are used to help protect the client or the server's identity by relaying a web client's request and a web server's response. Web proxy servers can also be used to log user interactions, act as web page caching services, perform load balancing, or filter and block web pages.

Other than specifying the web proxy name or IP address in the browser configuration, the user's interaction with the web proxy servers is transparent. Two main types of web proxies exist (see Figure 2-34):

1. Forward web proxies that send the requests of a client to a web server and "hide" the identity of the requesting client.
2. Reverse web proxies that receive client requests and forward the request to the destination web server. Reverse web proxies also "hide" the identity of the web server.

Figure 2-34 Web Proxies



FactoryTalk Application Access through the Industrial Demilitarized Zone

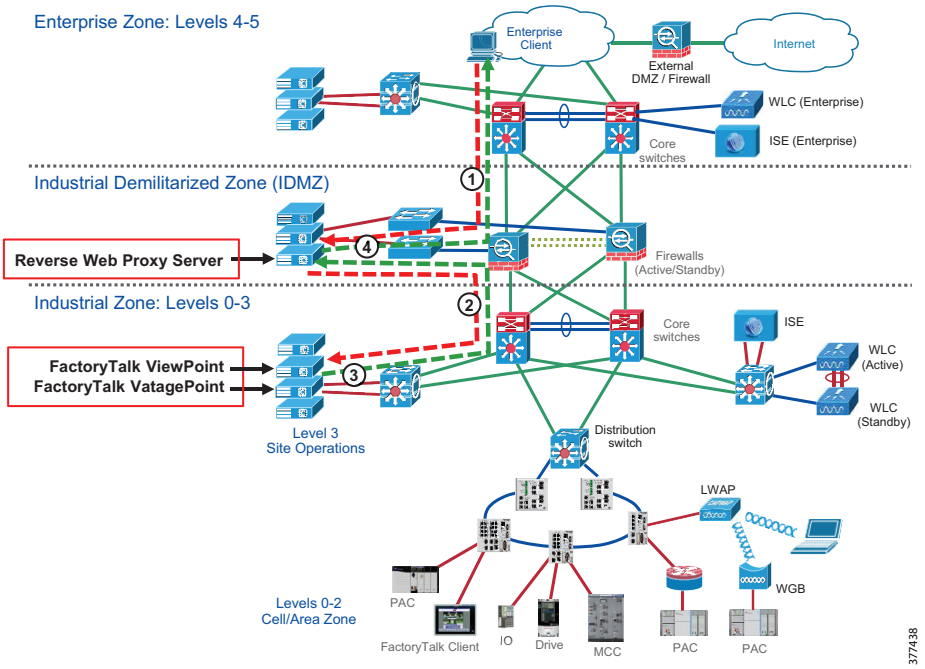
Building upon the CPwE IDMZ approach of broker services that allows secure access from clients in the Enterprise Zone to FactoryTalk Applications in the Industrial Zone, a reverse web proxy server is deployed in the IDMZ.

For this CVD, the Microsoft IIS web server, in conjunction with Application Request Routing (ARR), was used as the reverse web proxy solution. This setup uses URL rewrites to broker service sessions between Enterprise Zone clients and Industrial Zone FactoryTalk Application servers.

Two specific FactoryTalk applications—FactoryTalk VantagePoint Mobile and FactoryTalk ViewPoint—were configured, tested and validated.

Figure 2-35 shows this particular setup.

Figure 2-35 Reverse Web Proxy Operation



The four numbered steps describe the request flow sent by an enterprise client accessing resources from a FactoryTalk Application server in the Industrial Zone.

1. A client in the Enterprise Zone requests the desired FactoryTalk Application resource by sending an HTTP(S) request to the Reverse Web Proxy server.
2. The Reverse Web Proxy server uses an inbound URL rewrite rule to relay this request to the targeted FactoryTalk Application server located in the Industrial Zone.
3. The FactoryTalk Application server responds to the Reverse Web Proxy with the requested resources.
4. The Reverse Web Proxy uses an outbound URL rewrite rule to parse the response, looking for any references pointing back to the FactoryTalk Application server, and changes those references to point to itself. The Reverse Web Proxy server then forwards the adjusted response to the enterprise client.

For a detailed description about how to configure the IIS reverse web proxy server and the FactoryTalk VantagePoint Mobile and FactoryTalk ViewPoint servers, please refer to Configuring the Infrastructure.

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, please see the *FactoryTalk Security System Configuration Guide* at the following URL:

- 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 3-73.

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 two such solutions:

- Microsoft Enhanced Mitigation Experience Toolkit (EMET)
- Microsoft AppLocker®

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

- 546988—*Using Rockwell Products with Microsoft Enhanced Mitigation Experience Toolkit (EMET)*
  - https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546988
- 546989—*Using Rockwell Automation Software Products with AppLocker*
  - https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546989

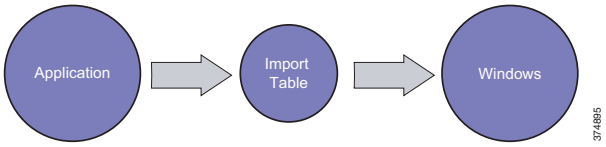
Microsoft Enhanced Mitigation Experience Toolkit Overview

Enhanced Mitigation Experience Toolkit (EMET) doesn't run as a service or attach to an application like a debugger. Instead, in order to enable mitigations for applications, EMET is leveraging a shim infrastructure in Windows called the Application Compatibility Framework behind the scenes. This is a highly optimized low level interface and, as such, EMET presents no additional resource overhead on the protected applications.

A Shim Infrastructure implements a form of application programming interface (API) hooking. Specifically, it leverages the nature of linking to redirect API calls from Windows to alternative code—the shim itself. The Windows Portable Executable (PE) and Common Object File Format (COFF) specification includes several headers, and the data directories in this header provide a layer of indirection between the application and the linked file.

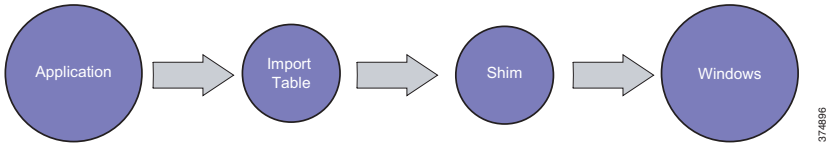
For example, if the executable makes a call to a Windows function, the call to external binary files will take place through the Import Address Table (IAT), as shown in Figure 2-36.

Figure 2-36 Application Call to Windows through IAT



Using the shim infrastructure, you can modify the address of the Windows function resolved in the import table, and then replace it with a pointer to a function in the alternate shim code (see Figure 2-37).

Figure 2-37 Application Redirected to Shim prior to Calling Windows



EMET leverages this shim architecture to enforce Protection Profiles. EMET Protection Profiles are XML files that contain pre-configured EMET settings.

Note For a more detailed explanation of Microsoft EMET, please refer to *The Enhanced Mitigation Experience Toolkit* at the following URL: http://support.microsoft.com/kb/2458544

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 Whitelist or Blacklist applications by creating rules to allow or deny applications from running.

Note

- It is strongly recommended to define whitelists rather than blacklists.
- For a more detailed explanation of Microsoft AppLocker, please refer to *How AppLocker Works* at the following URL:
  - http://technet.microsoft.com/en-us/library/ee460948%28v=ws.10%29.aspx

CHAPTER 3

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

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 ASA. For more details on these configurations, refer to the following URL:

- http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

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 3-38):

a. Select **Interfaces** within the **Device Setup** pane.

b. Click **Add** to the right of the interface list, and then choose **EtherChannel Interface**.

c. Enter values for the Port-channel ID and Interface Name fields. For the enterprise-facing EtherChannel, enter Security Level as **0**, and for the industrial-facing EtherChannel, enter Security Level as **100**.

d. Select **Enable Interface** option.

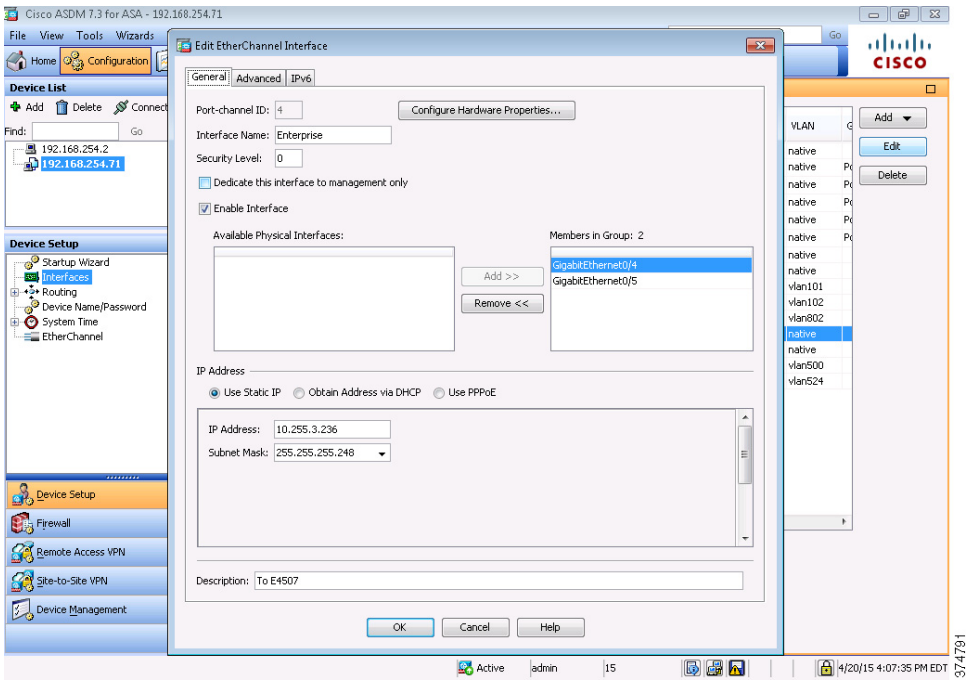
e. Select physical interfaces that should be included within the EtherChannel, and then click **Add**.

f. Select **Use Static IP** option and enter the IP address and subnet mask for the EtherChannel.

g. If desired, fill in the **Description** field to help identify the purpose of this EtherChannel, and then click **OK**.

h. Click **Apply** at the bottom of the window to make all changes take effect.

Figure 3-38 ASA EtherChannel Interface Configuration



Step 2 Configure EIGRP as the dynamic routing protocol (see Figure 3-39):

a. Select **Routing > EIGRP > Setup** within the **Device Setup** pane.

b. In the **Process Instances** tab, enter the **EIGRP Process number**, and then click **Advanced**.

c. For the Router ID field, click either **Automatic** (to assign the highest local IP address as the ID) or **IP Address** (to assign an ID manually). Disable the **Auto-Summary** option and enable the **Log Neighbor Changes** and **Log Neighbor Warnings** options. Leave all other settings as default and then click **OK**.

d. In the **Networks** tab, define each subnet that should be advertised by EIGRP by clicking **Add** and filling in the **IP address** and **Netmask** fields.

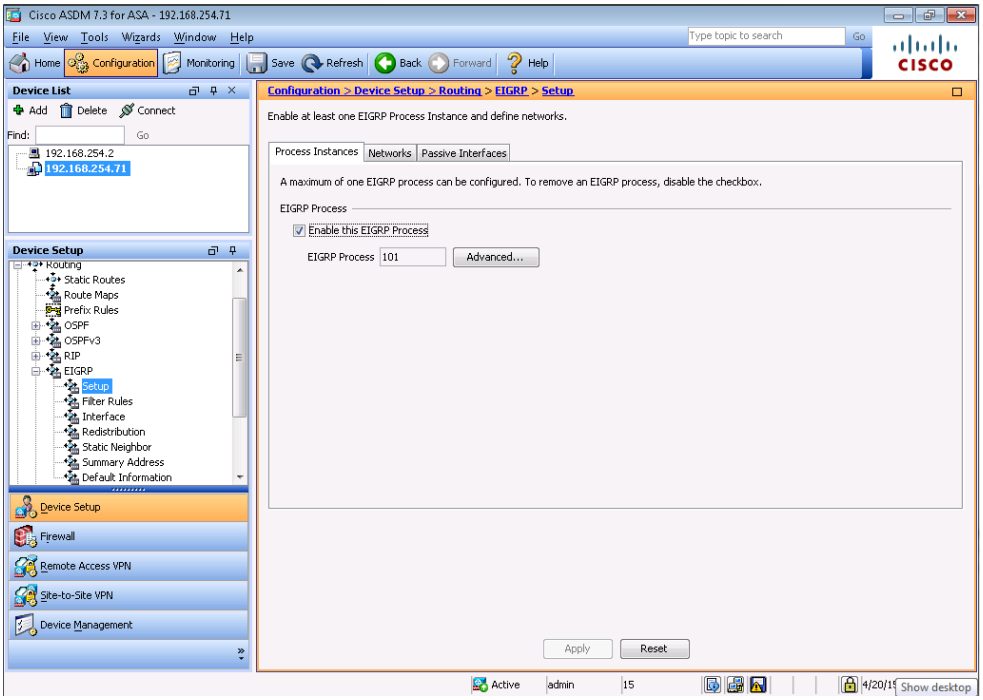
e. In the **Passive Interfaces** tab, select **Suppress Routing Updates** on All Interfaces. This prevents interfaces with IP addresses in the Networks list from attempting to form neighborships with adjacent devices. To add exceptions to this option for the industrial and enterprise-facing interfaces and allow neighborships to form, click **Add** to select each interface and then click **OK**.

f. To enable authentication between EIGRP neighbors for increased security, select **Interface** under **EIGRP** in the Device Setup pane. Select the desired interface from the list and click **Edit**. Select **Enable MD5 Authentication**, and then enter a shared secret key value and ID. Finally, click **OK**.

g. To enable summarization of advertised EIGRP routes for increased security and efficiency, select **EIGRP > Summary Address** in the **Device Setup** pane. Click **Add**, and then enter the summary IP address, netmask, and interface that will advertise the summary route. Leave the Administrative Distance field blank and then click **OK**.

h. Click **Apply** at the bottom of the window to make all changes take effect.

Figure 3-39 ASA EIGRP Configuration



Step 3 Configure active/standby failover mode on each firewall and the failover link between the two (see Figure 3-40):

a. Select **High Availability** and **Scalability > Failover** within the Device Management pane.

b. In the **Setup** tab, select **Enable Failover**, For greater security, enter a shared key in the appropriate field to encrypt the communications between the active and standby fire-walls.

c. Under **LAN Failover**, select a physical interface to transmit failover information. Fill in the **Logical Name** field with any desired value, as well as the **Active IP** and **Standby IP** fields (select any IP address range not already being used) and the **Subnet Mask** field (typically 255.255.255.252 for a point-to-point connection).

d. Select the **Preferred Role** to identify whether this firewall should be the primary (active) or secondary (standby). Under **State Failover**, select a physical interface (may be the same as LAN Failover interface if desired).

Note When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit via the State Failover link.

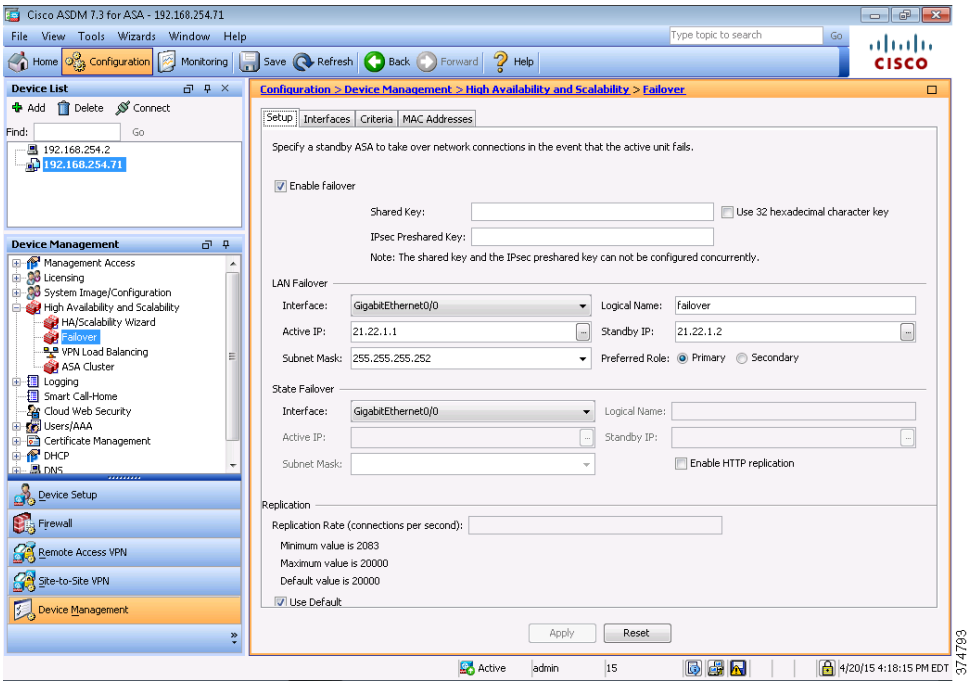
e. In the **Interfaces** tab, assign a standby IP address for each interface within the same subnet as the active one. For any interfaces that should be monitored for loss of connectivity to trigger a firewall failover, select the **Monitored** option.

f. In the **Criteria** tab, enter **1** as the Number of failed interfaces that triggers failover. Change values under **Failover Poll Times** as desired.

g. Click **Apply** at the bottom of the window to make all changes take effect.

h. Repeat the above process for the second firewall (changing the Preferred Role accordingly).

Figure 3-40 ASA Failover Configuration



Step 4 Configure explicit **Deny All** rules between all zones (see Figure 3-41):

Note Traffic from interfaces with a lower security level to interfaces with a higher security level is implicitly denied by default. However, to confirm complete isolation of all zones and prevent confusion, the user should overwrite these implicit rules with explicit ones.

a. Select **Access Rules** within the **Firewall** pane.

b. For each interface, right-click the interface name and then select **Add Access Rule**.

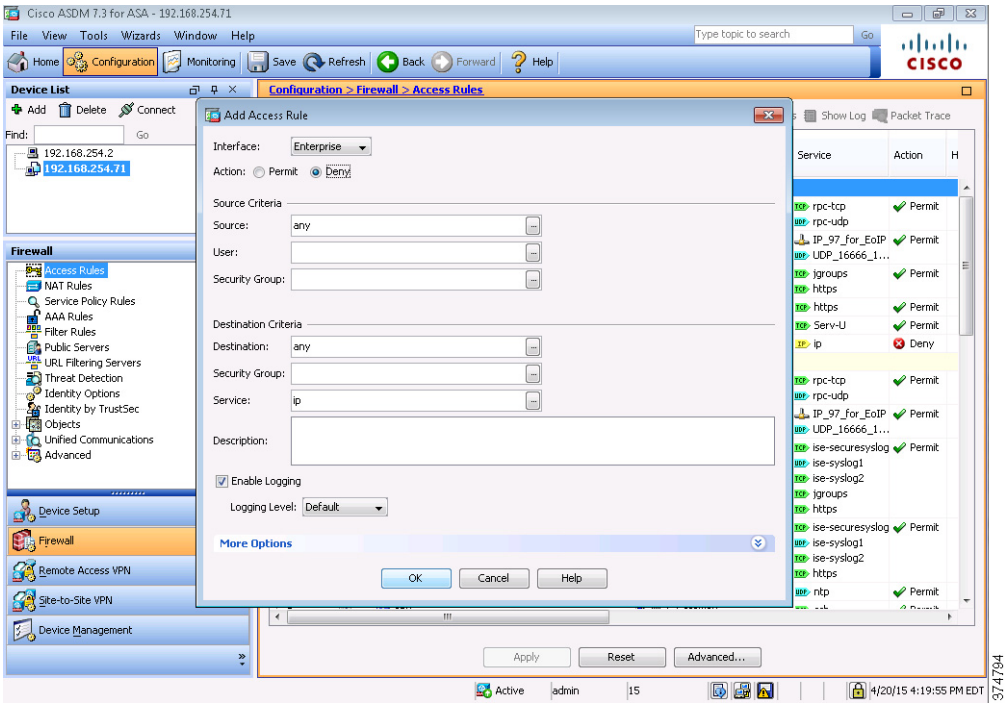
c. Create a **Deny** rule with **Source as Any** and **Destination as Any**, and then click **OK**.

d. Click the new rule, and then click **Move Down** (down arrow) at the top of the pane until the rule is at the bottom of the interface rule list. Since firewall rules are evaluated in order, the **Deny All** rule must be at the bottom to only deny traffic that does not match any permit rules for the interface.

e. Click **Apply** at the bottom of the window to make all changes take effect.

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

Figure 3-41 ASA Access Rules Configuration



The equivalent CLI configuration for Steps 1-4 is shown below:

```
interface GigabitEthernet0/2
 channel-group 3 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
```

```
 channel-group 3 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 4 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 4 mode active
 no nameif
 no security-level
 no ip address
!
interface Port-channel3
 description To Industrial Zone
 lacp max-bundle 8
 nameif Industrial
 security-level 100
 ip address 10.255.255.34 255.255.255.248 standby 10.255.255.35
!
interface Port-channel4
 description To Enterprise Zone
 lacp max-bundle 8
 nameif Enterprise
 security-level 0
 ip address 10.255.3.236 255.255.255.248 standby 10.255.3.237
!
router eigrp 101
 network 10.255.255.0 255.255.255.0
 network 10.255.3.0 255.255.255.0
 passive-interface default
 no passive-interface Industrial
 no passive-interface Enterprise
!
failover
failover lan unit primary# (or secondary)
failover lan interface failover GigabitEthernet0/0
failover link failover GigabitEthernet0/0
failover interface ip failover 21.22.1.1 255.255.255.252 standby 21.22.1.2
monitor-interface Enterprise
monitor-interface Industrial
!
access-list Enterprise_access_in extended deny ip any any
access-list Industrial_access_in extended deny ip any any
access-group Industrial_access_in in interface Industrial
access-group Enterprise_access_in in interface Enterprise
```

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 3-42):

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. Select **Interfaces** within the **Device Setup** pane. Click **Add** to the right of the interface list, and then click **Interface**.

b. Select the **Hardware Port** from the drop-down that corresponds to the IDMZ-facing interface. Enter the **VLAN ID** that will be used by the specific service. Finally, enter the **Security Level** as **50**.

c. Select **Enable Interface**.

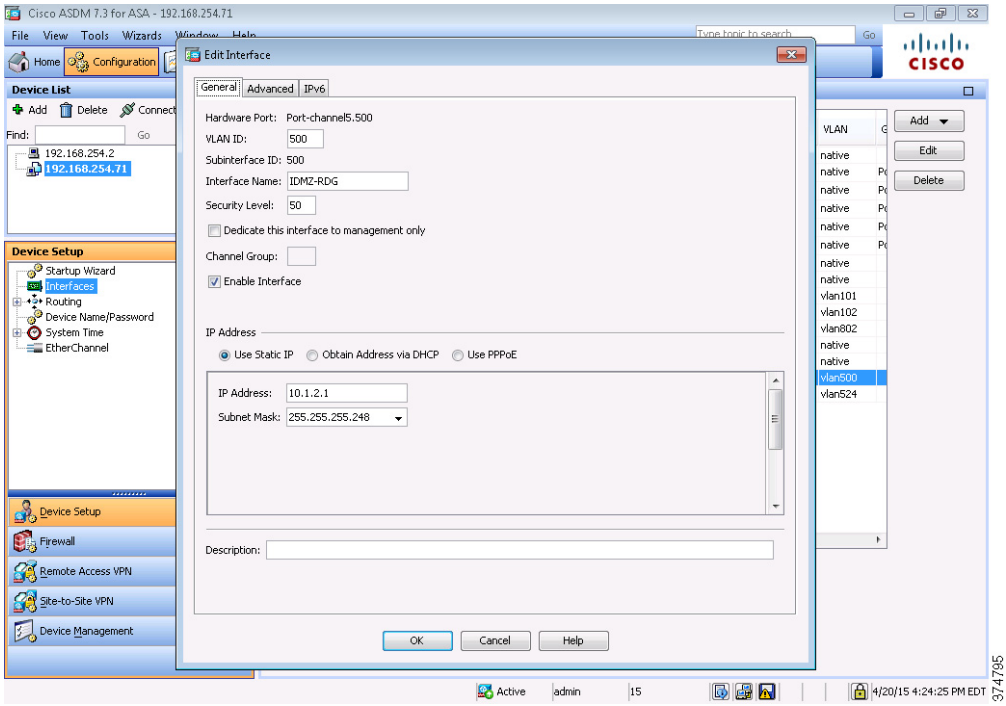
d. Select **Use Static IP**, and then enter the IP address and subnet mask for the sub-interface.

e. If desired, fill in the **Description** field to help identify the purpose of this sub-interface, and then click OK.

f. Click **Apply** at the bottom of the window to make all changes take effect.

g. Define explicit **Deny All** rules for each sub-interface as described in the previous section to confirm isolation of each IDMZ service.

Figure 3-42 ASA Sub-interface Configuration



The equivalent CLI configuration for Step 1 is shown below:

```
interface Port-channel5
 description To IDMZ
 lacp max-bundle 8
 no nameif
 no security-level
 no ip address
!
```

```
interface Port-channel5.500
 vlan 500
 nameif IDMZ-RDG
 security-level 50
 ip address 10.1.2.1 255.255.255.248 standby 10.1.2.2
!
interface Port-channel5.524
 vlan 524
 nameif IDMZ-MFT
 security-level 50
 ip address 10.1.2.25 255.255.255.248 standby 10.1.2.26
!
access-list IDMZ-MFT_access_in extended deny ip any any
access-list IDMZ-RDG_access_in extended deny ip any any
access-group IDMZ-RDG_access_in in interface IDMZ-RDG
access-group IDMZ-MFT_access_in in interface IDMZ-MFT
```

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 Convert the switch pair from standalone to VSS mode.

Note For information on VSS and detailed steps on performing this conversion process, refer to the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vss.html

Typical CLI output resulting from this conversion is shown below. Two 10 Gbps interfaces on the supervisor modules were used for the virtual switch link (VSL). In this example, Port-channel 10 and virtual link 1 is configured on the physical chassis 1, and Port-channel 20 and virtual link 2 on the physical chassis 2.

```
!
switch virtual domain 100
 switch mode virtual
!
interface Port-channel10
 no switchport
 no ip address
 switch virtual link 1
 mls qos trust cos
 no mls qos channel-consistency
!
interface Port-channel20
 no switchport
 no ip address
 switch virtual link 2
 mls qos trust cos
 no mls qos channel-consistency
!
interface TenGigabitEthernet1/5/4
 no switchport
 no ip address
 mls qos trust cos
 no cdp enable
```

```
 channel-group 10 mode on
!
interface TenGigabitEthernet1/5/5
 no switchport
 no ip address
 mls qos trust cos
 no cdp enable
 channel-group 10 mode on
!
interface TenGigabitEthernet2/5/4
 no switchport
 no ip address
 mls qos trust cos
 no cdp enable
 channel-group 20 mode on
!
interface TenGigabitEthernet2/5/5
 no switchport
 no ip address
 mls qos trust cos
 no cdp enable
 channel-group 20 mode on
!
```

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-channel1
 description To Primary ASA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan <VLAN-LIST>
 switchport mode trunk
!
interface Port-channel2
 description To Secondary ASA
 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 GigabitEthernet1/1/1
 description To Primary ASA port 1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan <VLAN-LIST>
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/1/2
 description To Secondary ASA port 2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan <VLAN-LIST>
 switchport mode trunk
 channel-group 2 mode active
```

```
!
interface GigabitEthernet2/1/1
 description To Secondary ASA port 1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan <VLAN-LIST>
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet2/1/2
 description To Primary ASA port 2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan <VLAN-LIST>
 switchport mode trunk
 channel-group 1 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 ASA
 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 ASA
 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 ASA
```

```
 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 ASA
 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 the following URL:

- 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.

Note For more details on how to configure DCE/RPC on Cisco ASA, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa917/asdm717/firewall/asdm-717-firewall-config/inspect-basic.html#ID-2095-00000007

Step 1 Enable the DCE/RPC Pinhole feature to avoid opening a large dynamic port range on the firewall for the RPC traffic:

a. Select **Service Policy Rules** in the **Firewall** pane, and then click **Add** (see Figure 3-43).

b. Select the interface to apply the policy, assign policy name and description and then click **Next**.

c. Enter the traffic class name in the **Create a New Traffic Class** field. Select **TCP** or **UDP Destination Port** as the Traffic Match Criteria, and then click **Next** (see Figure 3-44).

d. Select TCP port 135 (DCE/RPC service) as the **Traffic Match Destination Port** and enter the **Service** name, and then click **Next** (see Figure 3-45).

e. Select the **DCERPC** check box under the **Protocol Inspect** tab, and then click **Finish** (see Figure 3-46).

Note By default, the DCE/RPC pin hole is opened for 2 minutes.

Figure 3-43 Add Service Policy Rule - Service Policy Configuration

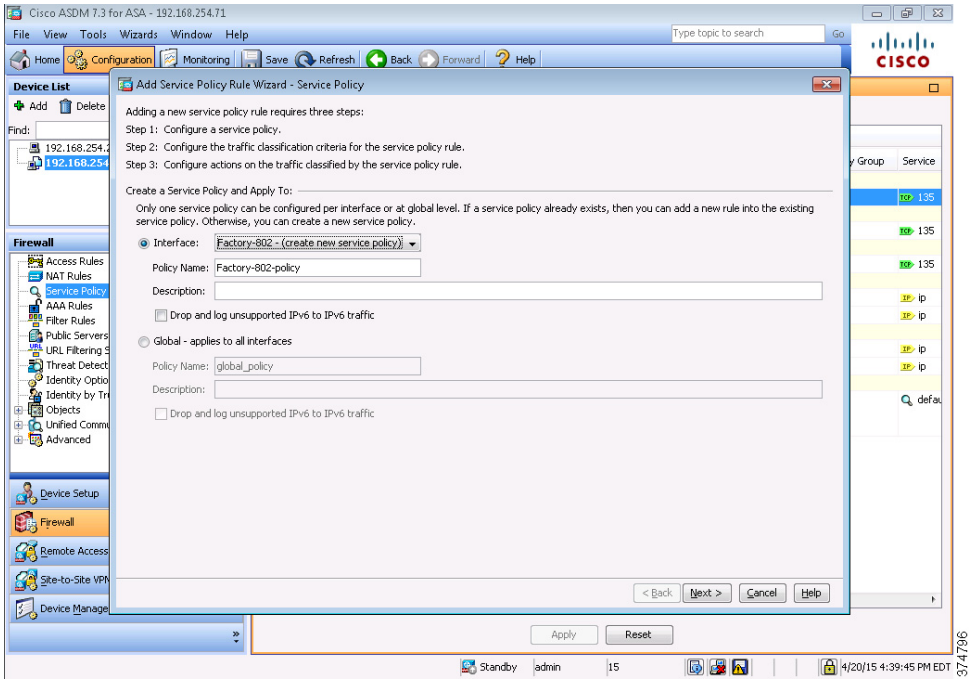


Figure 3-44 Add Service Policy Rule - Traffic Classification Criteria

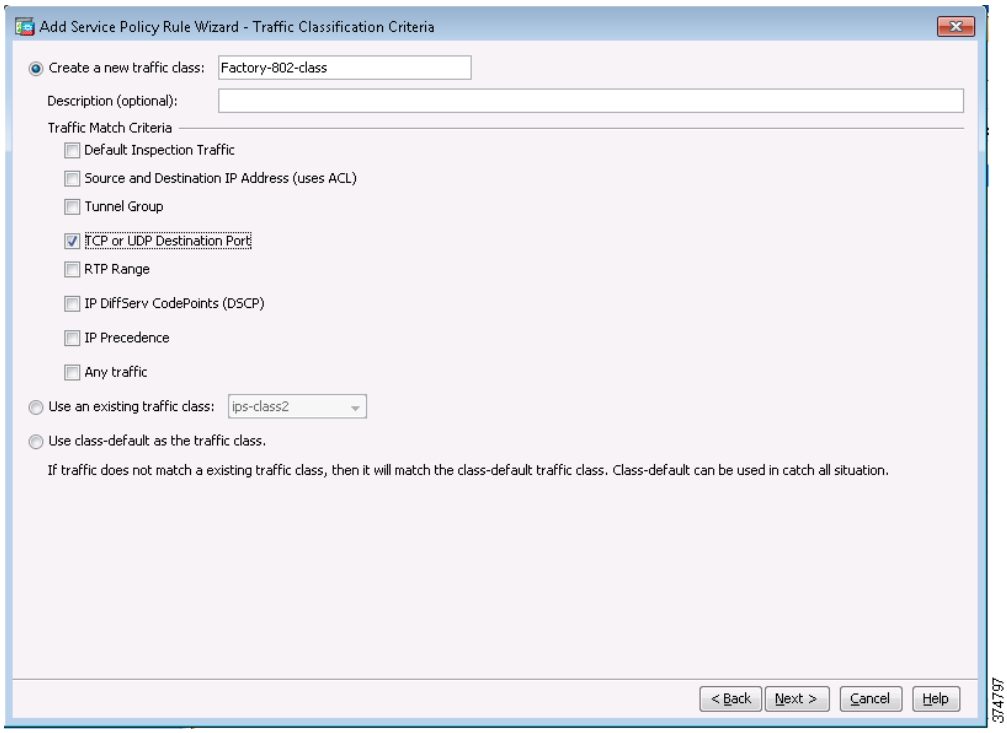


Figure 3-45 Add Service Policy Rule - DCE/RPC Traffic Match

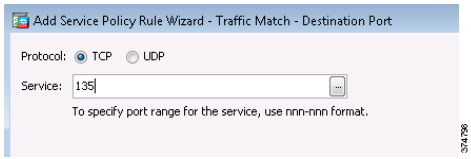
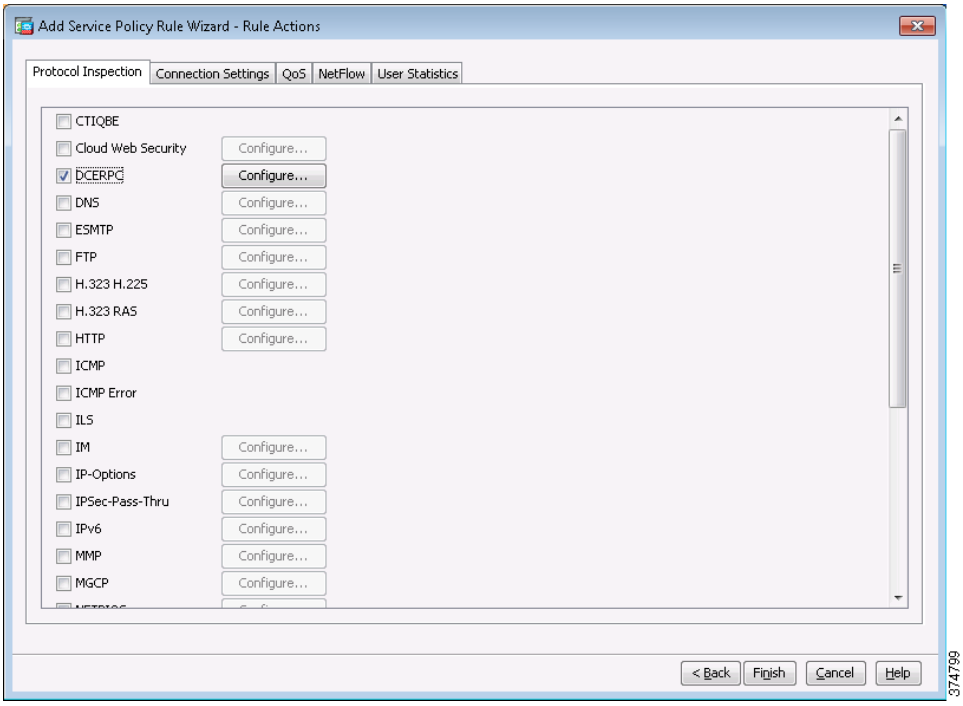


Figure 3-46 Add Service Policy Rule - DCE/RPC Protocol Inspection



Step 2 Configure the firewall to allow RPC traffic between the Enterprise and Industrial AD data centers:

a. Select **Access Rules** within the **Firewall** pane.

b. Right-click the industrial-facing interface and select **Add Access Rule**.

c. Create a **Permit** rule with the following parameters:

```
Source = <Industrial AD server>, Destination = <Enterprise AD server>, Service =
rpc-tcp, rpc-udp (TCP/UDP port 135)
```

d. Click **OK** (see Figure 3-47).

e. Right-click the enterprise-facing interface and select **Add Access Rule**.

f. Create a **Permit** rule with the following parameters:

```
Source = <Enterprise AD server>, Destination = <Industrial AD server>, Service =
rpc-tcp, rpc-udp (TCP/UDP port 135)
```

g. Click **OK** (see Figure 3-48).

h. Click **Apply** at the bottom of the window to make all changes take effect.

Step 3 Configure the firewall to allow additional protocols for replication (Table 3-8). These protocols can be grouped in an object on the firewall for simplified configuration.

Figure 3-47 Add Access Rule - RPC Industrial to Enterprise

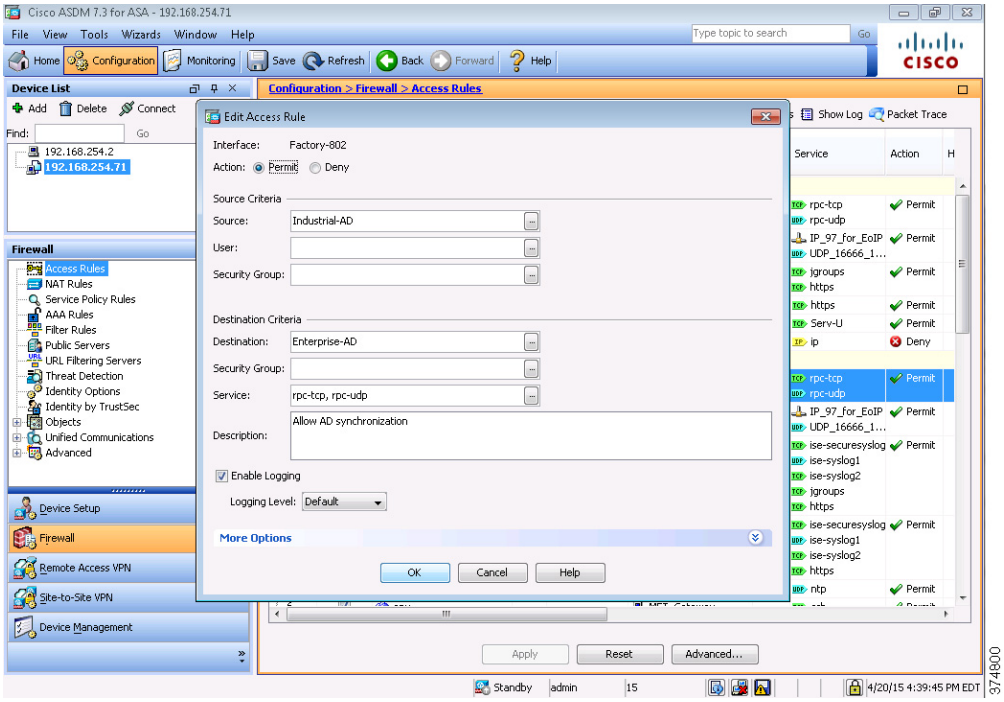
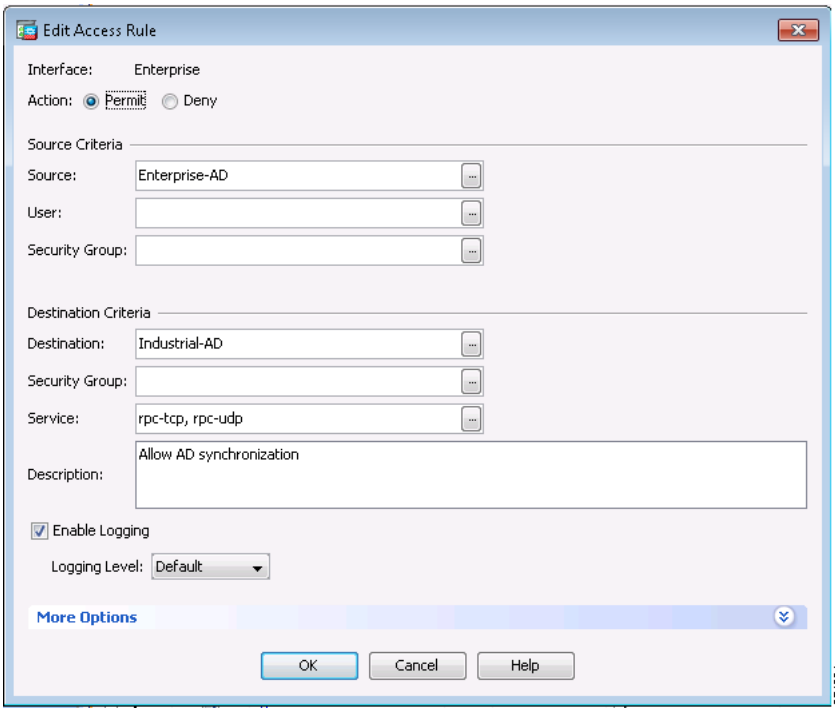


Figure 3-48 Add Access Rule - RPC Enterprise to Industrial



The access rules for AD replication are summarized in Table 3-8..

Table 3-8 Access Rules - AD Replication

Firewall Interface	Source	Destination	Permitted protocols
Industrial	Industrial DC	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) SMB (TCP/UDP port 445)
Enterprise	Enterprise DC	Industrial DC	

The equivalent CLI configuration for Steps 1-2 is shown below (RPC only, other protocols will require additional access rules):

```
object service rpc-tcp
 service tcp destination eq 135
object service rpc-udp
 service udp destination eq 135
object-group service DM_INLINE_TCPUDP_1 tcp-udp
object-group service DM_INLINE_SERVICE_9
 service-object object rpc-tcp
 service-object object rpc-udp
object-group service DM_INLINE_SERVICE_18
 service-object object rpc-tcp
 service-object object rpc-udp
access-list Enterprise_access_in extended permit object-group DM_INLINE_SERVICE_18
object Enterprise-AD object Industrial-AD
access-list Industrial_access_in extended permit object-group DM_INLINE_SERVICE_9
object Industrial-AD object Enterprise-AD
class-map dcerpc
 match port tcp eq 135
policy-map type inspect dcerpc dcerpc_map
 parameters
  endpoint-mapper epm-service-only lookup-operation
policy-map interface_dcerpc
 class dcerpc
  inspect dcerpc dcerpc_map
service-policy interface_dcerpc interface Enterprise
```

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 3-9.

Table 3-9 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 the following URL:

- 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 the following URL:

- 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 3-10):

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 3-10) between IDMZ NTP clients (for example, Windows servers and IDMZ access/distribution switches) and the Enterprise Zone NTP server.

Table 3-10 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 ASA web interface (see Figure 3-47 on page 3-15 in the Active Directory section as an example).

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 3-11 lists the firewall rules that should be applied (depending on the AAA protocol in use):

Table 3-11 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 3-12).

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 the following URL:

- 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, please refer to this URL:

- 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 3-12 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 ASA web interface (see Figure 3-47 on page 3-15 in the Active Directory section as an example). The equivalent CLI configuration for Steps 1-2 is shown below:

```
object-group service DM_INLINE_SERVICE_5
 service-object tcp destination eq https
 service-object object jgroups
object-group service DM_INLINE_SERVICE_2
 service-object object ise-securesyslog
 service-object object ise-syslog1
 service-object object ise-syslog2
 service-object tcp destination eq https
access-list Enterprise_access_in extended permit object-group DM_INLINE_SERVICE_5
object cidm-ise-2 object cidm-ise-1
access-list Industrial_access_in extended permit object-group DM_INLINE_SERVICE_5
object cidm-ise-1 object cidm-ise-2
access-list Industrial_access_in extended permit object-group DM_INLINE_SERVICE_2
object cidm-ise-1 object cidm-ise-3
```

WLAN Access Configuration

The following steps describe validated firewall configurations that allow tunneling of WLAN client data between the Industrial WLC and the Enterprise Anchor WLC or Guest Anchor WLC.

Note For configuration of WLCs to allow WLAN access for corporate users, trusted partners and guests across the IDMZ, refer to the *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at the following URL:

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

Step 1 Configure the firewall to allow communication between the Industrial WLC and Enterprise and Guest anchor WLCs (see Table 3-13).

Table 3-13 Access Rules - WLAN Data Tunneling

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Industrial WLC	Enterprise WLC Guest WLC	EoIP (IP protocol 97) CAPWAP (UDP port 16666, 16667)
Enterprise	Enterprise WLC Guest WLC	Industrial WLC	EoIP (IP protocol 97) CAPWAP (UDP port 16666, 16667)

Note The access rules above enable "old mobility" mode for WLCs, which uses an Ethernet over IP (EoIP) tunnel that sends control traffic via UDP port 16666 and client data via IP protocol type 97.

The access rules can be applied using Cisco ASA web interface (see Figure 3-47 on page 3-15 in the Active Directory section as an example). The equivalent CLI configuration for Step 1 is shown below:

```
object-group network DM_INLINE_NETWORK_2
 network-object object WLC_Corporate_Anchor
 network-object object WLC_Guest_Anchor
object-group service DM_INLINE_SERVICE_13
 service-object object IP_97
 service-object object UDP_16666
access-list Industrial_access_in extended permit object-group DM_INLINE_SERVICE_13
object WLC_Industrial object-group DM_INLINE_NETWORK_2
```

```
access-list Enterprise_access_in extended permit object-group DM_INLINE_SERVICE_13
object-group DM_INLINE_NETWORK_2 object WLC_Industrial
```

Configuring FactoryTalk Application Access through the IDMZ

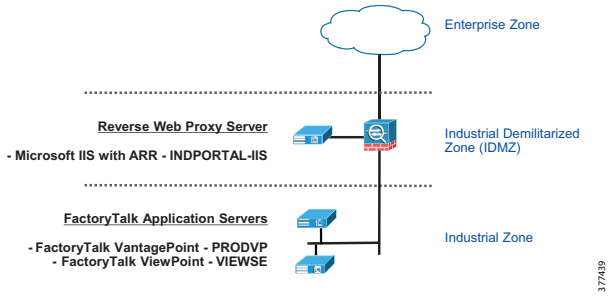
This section provides configuration steps for setting up access through the Industrial Demilitarized Zone for two specific FactoryTalk applications, namely FactoryTalk VantagePoint Mobile and FactoryTalk ViewPoint. The configuration procedure for the IIS reverse web proxy server in the IDMZ is included.

For this CVD, the operating system and FactoryTalk Application versions shown in Table 3-14 were used:

Table 3-14 OS and FactoryTalk Application Versions

Server	Operating System	FactoryTalk Application	CVD-Specific Name
Reverse Web Proxy	Windows Server 2012 R2	--	INDPORTAL-IIS
FactoryTalk Vantage Point Mobile	Windows Server 2012 R2	FactoryTalk VantagePoint System Server 7.0	PRODVP
FactoryTalk ViewSE	Windows Server 2012	ViewSE 8.20 with FactoryTalk ViewPoint 8.20	VIEWSE

Figure 3-49 Reverse Web Proxy Test Architecture



Firewall Rules for FactoryTalk Web Applications

Certain firewall rules should be configured to allow the reverse web proxy server in the IDMZ to authenticate to the Enterprise AD. See Table 3-15.

Table 3-15 Access Rules for Reverse Web Proxy to Authenticate to the Enterprise AD

Firewall Interface	Source	Destination	Permitted Protocols
Enterprise	Enterprise DC	IISRevProxy	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) DNS (TCP/UDP port 53) NETBIOS (TCP/UDP port 137) NETBIOS (UDP port 138) NETBIOS (TCP port 139)
DMZ_Rev_Web_Proxy Interface	IISRevProxy	Enterprise DC	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) DNS (TCP/UDP port 53) NETBIOS (TCP/UDP port 137) NETBIOS (UDP port 138) NETBIOS (TCP port 139)

Firewall rules should be configured to allow the Enterprise FactoryTalk ViewPoint and FactoryTalk VantagePoint Mobile clients to communicate to the reverse web proxy server in the IDMZ. These rules are listed in Table 3-16.

Table 3-16 Access Rules for Enterprise Clients to Access Reverse Web Proxy

Firewall Interface	Source	Destination	Permitted Protocols
Enterprise	Enterprise Client(s)	IISRevProxy	HTTP (TCP port 80) HTTPS (TCP port 443)

Firewall rules should be configured to allow the reverse web proxy server in the IDMZ to communicate with FactoryTalk ViewPoint and FactoryTalk VantagePoint server(s). These rules are listed in Table 3-17

Table 3-17 Access Rules for Reverse Web Proxy to Access FactoryTalk ViewPoint and FactoryTalk VantagePoint Servers

Firewall Interface	Source	Destination	Permitted Protocols
DMZ_Rev_Web_Proxy Interface	IISRevProxy	FactoryTalk ViewSE and/or FactoryTalk VantagePoint Mobile server(s)	HTTP (TCP port 80) HTTPS (TCP port 443)

Configuring the Reverse Web Proxy

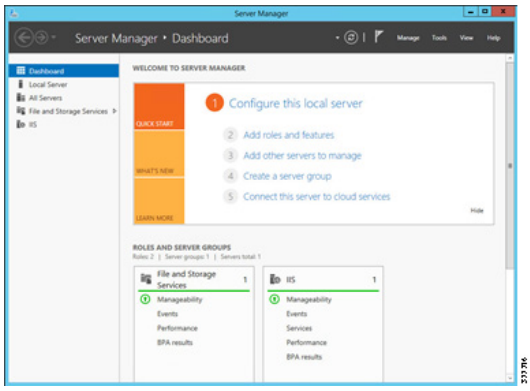
This section assumes that the reverse web proxy server has been built, patched and joined to the domain. The administrator will need to have appropriate access rights to the server and domain to complete the setup.

Installing the Internet Information Server Role and Application Request Routing

To enable the IIS role and add AAR with URL rewrite on the reverse web proxy server, complete the following steps

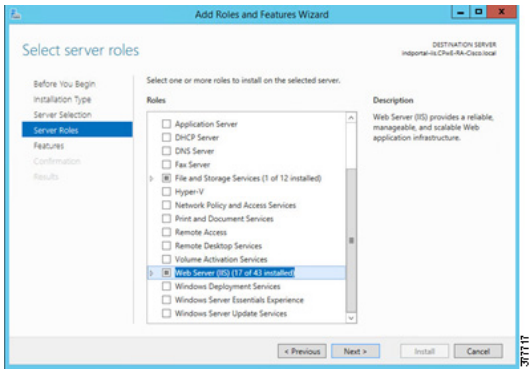
Step 1 Open the **Server Manager** and click **Add Roles and Features**, as shown in Figure 3-50.

Figure 3-50 Open the Server Manager



Step 2 From the **Add Roles and Features Wizard** screen (as shown in Figure 3-51), click the **Web Server (IIS)** check box and then follow the installation instructions, leaving all the default options.

Figure 3-51 Click the Web Server (IIS) Check Box

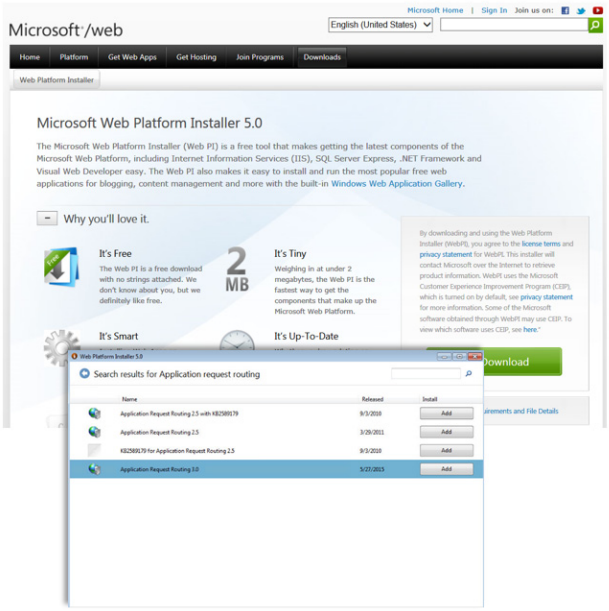


Step 3 The ARR option is added via the Microsoft Web Platform installer at the following URL:

- https://www.microsoft.com/web/downloads/platform.aspx.

Download and install the Platform installer and search for “Application Request Routing,” as shown in Figure 3-52.

Figure 3-52 Download and Install the Platform Installer



Configuring HTTPS

In order to authenticate the reverse web proxy server to enterprise clients and establish a secure channel between the two, the IIS server needs to have a domain certificate installed.

Note It is assumed at this point that the reader's setup has a working Public Key Infrastructure (PKI) configured.

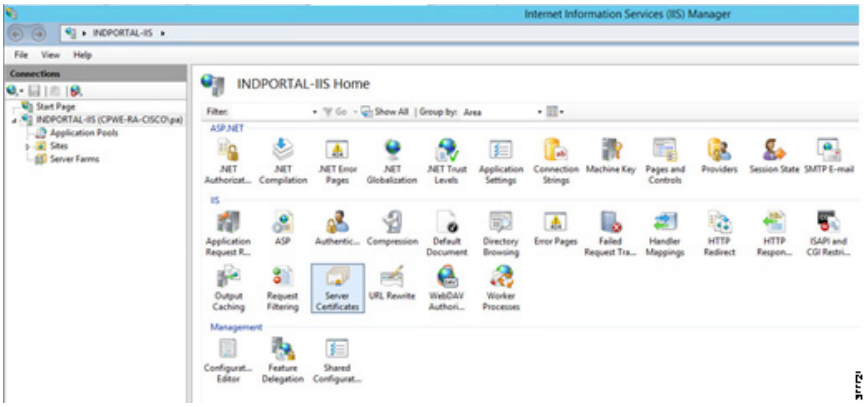
Installation of a domain certificate is necessary on the reverse web proxy (IIS) server as well as on the FactoryTalk application servers. To configure the IIS server, which will be similar to the FactoryTalk Application servers, complete the following steps:

Step 1 Click the **Internet Information Services (IIS) Manager** icon, as shown in Figure 3-53.

Figure 3-53 Open the Internet Information Services (IIS) Manager

Step 2 From the IIS home screen, click **Server Certificates**, as shown in Figure 3-51.

Figure 3-54 Click Server Certificates



Step 3 On the right side, click **Create Domain Certificate**, as shown in Figure 3-55, and then enter the relevant information needed to create a certificate, as shown in Figure 3-56.

Figure 3-55 Click Create Domain Certificate

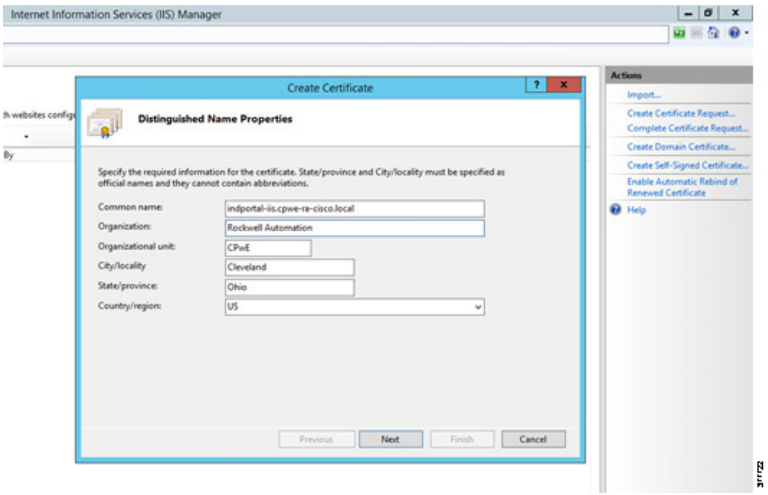
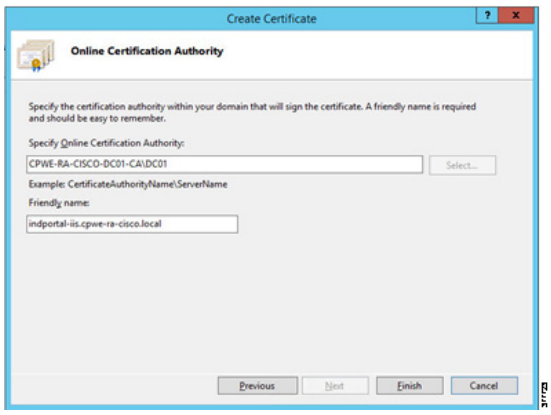
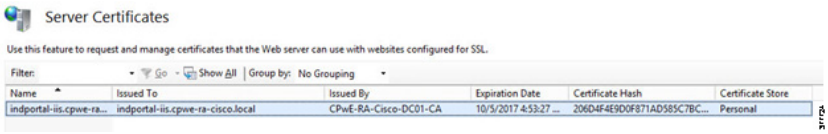


Figure 3-56 Enter Information to Create a Certificate



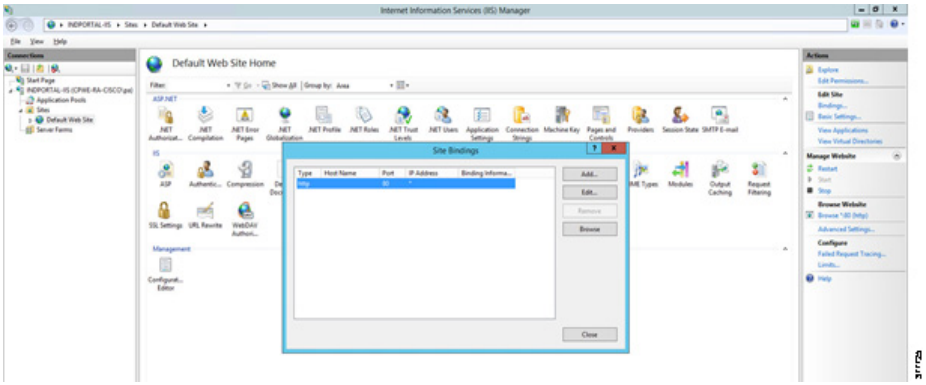
Step 4 Click **Finish**. The screen shown in Figure 3-57 will display.

Figure 3-57 Server Certificates Screen



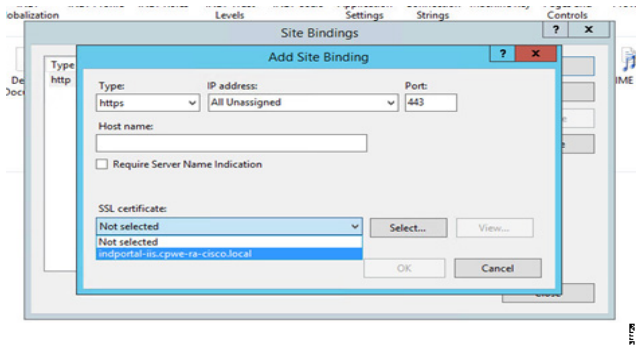
Step 5 To bind the newly created certificate to the default web page, as shown in Figure 3-58, open the **Sites** directory on the left, click **Default Web Site** and then click **Bindings** in the **Actions** pane.

Figure 3-58 Bind the Newly Created Certificate to the Default Webpage



Step 6 Click **Add**, change **Type:** to **https** and then click the newly created certificate from the SSL Certificate drop down menu, as shown in Figure 3-56.

Figure 3-59 Click the Newly Created Certificate



Step 7 Click **OK** and then click **Close**. The reverse web proxy is now configured to accept both HTTP as well as HTTPS requests.

Configuring URL Rewrite Rule

Relaying of traffic, which is done by the URL rewrite engine of the reverse web proxy, will change the destination of incoming HTTP(S) request URLs and forward them to the targeted resource. The response from the targeted resource will be touched up or “corrected” to have referrals back to the targeted resource point to the proxy server instead.

In order for the proxy to forward an incoming request to a FactoryTalk Application server in the Industrial Zone, an inbound rule needs to be written. The rule parses the incoming URL, determines the requested resource, changes the URL to point to the corresponding FactoryTalk Application server and then forwards the request to that destination.

The response from the FactoryTalk Application server needs to be inspected for references and links back to itself. If such links are present for objects like icons or images, the reverse web proxy server URL rewrite engine will use an outbound rule to change these references to point to the address of the proxy server before forwarding the response to the originating client.

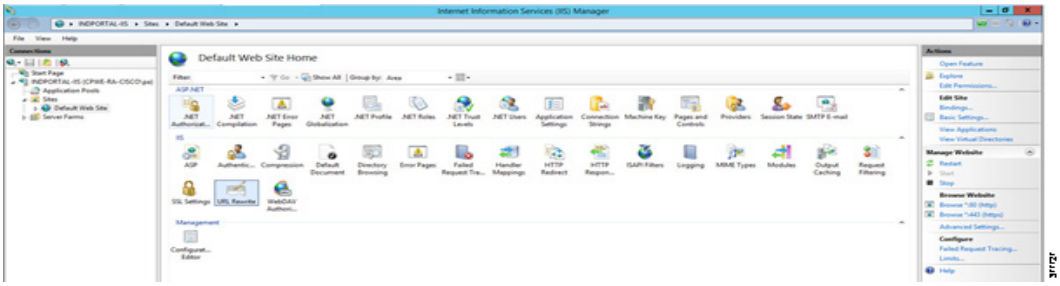
The following are detailed configuration instructions on how to create inbound and outbound rules to work with the FactoryTalk VantagePoint Mobile and FactoryTalk ViewPoint application servers respectively.

Creating URL Rewrite Rules for the FactoryTalk VantagePoint Mobile Application

To create an inbound URL rewrite rule on the reverse web proxy server to relay requests aimed at the FactoryTalk VantagePoint Mobile Application, complete the following steps:

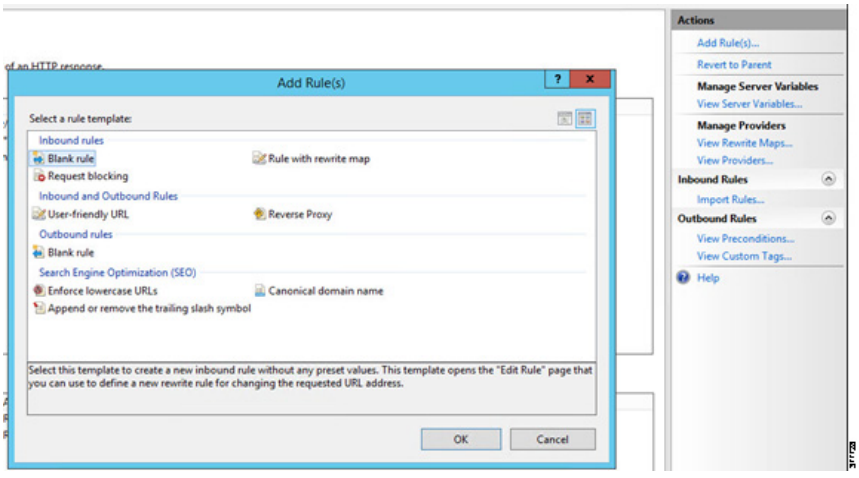
Step 1 Open the reverse web proxy's IIS manager, navigate to the **Default Web Site** folder and then open the **URL Rewrite** options panel, as shown in Figure 3-60.

Figure 3-60 Open the URL Rewrite Options Panel



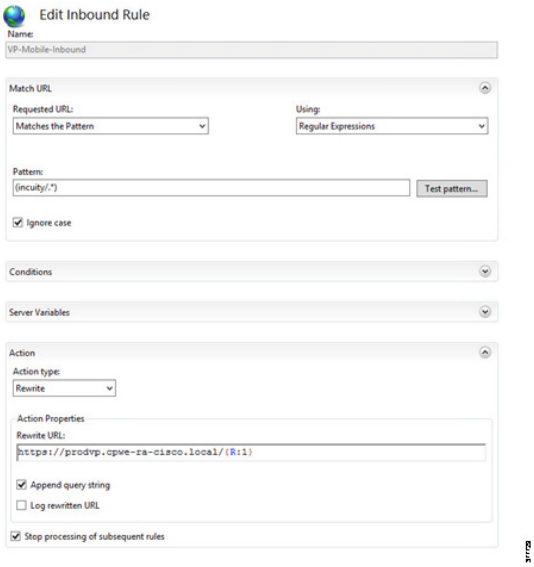
Step 2 Under **Actions**, click **Add Rule(s)**… and then choose a blank inbound rule, as shown in Figure 3-61.

Figure 3-61 Add Blank Inbound Rule



Step 3 Enter data in the fields shown in Figure 3-62. The pattern *incuity* is the FactoryTalk VantagePoint Mobile application that runs on the FactoryTalk VantagePoint Mobile server.

Figure 3-62 Edit Inbound Rule



This rule will parse the incoming request URL for the string *incuity/* and, if found:

- replaces the leading part of the URL *https://**indportal**-iis.cpwe-ra-cisco.local/'*
- with *https://prodvp.cpwe-ra-cisco/*, leaving the trailing part of the request URL intact.

This inbound rewrite rule enables the reverse web proxy server to:

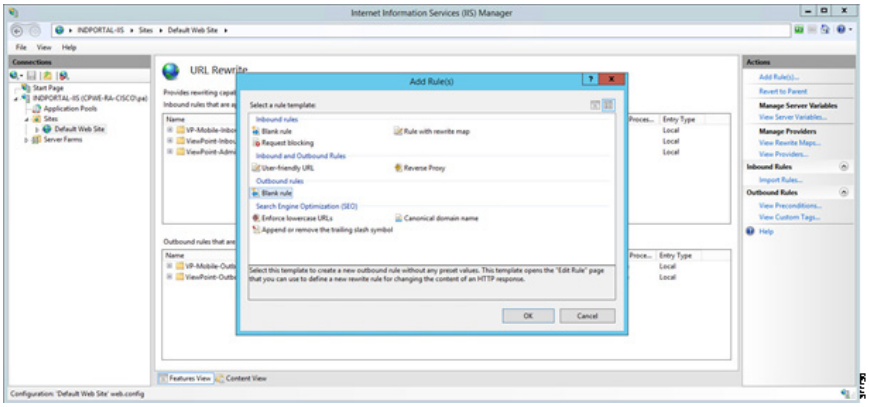
- change an incoming request URL like *https://indportal-iis.cpwe-ra-cisco.local/incuity/thinui/index.html*
- to *https://**prodvp**.cpwe-ra-cisco.local/incuity/thinui/index.html*
- and forward it to the FactoryTalk VantagePoint hosting server (PRODVP).

The response from the FactoryTalk VantagePoint server might contain local references to URLs and links to image and icon objects that need to be rewritten by the reverse web proxy.

To create an outbound URL rewrite rule on the reverse web proxy server to address these local references, complete the following steps:

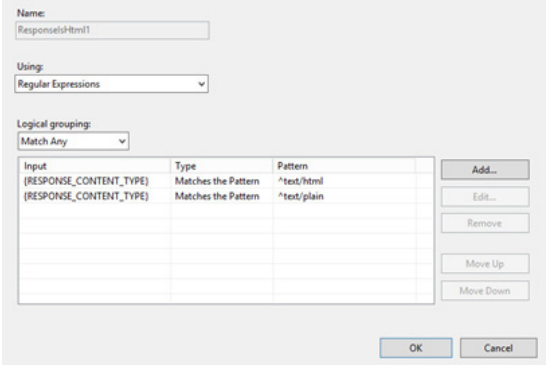
Step 1 From the URL rewrite page, click **Add Rules(s)…** and then choose the blank outbound rule option, as shown in Figure 3-63.

Figure 3-63 Choose the Blank Outbound Rule Option



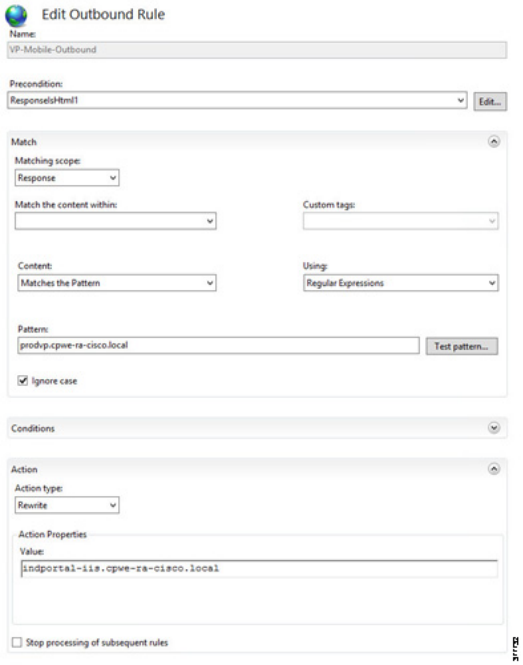
Step 2 Create a Precondition that the outbound rule will use to determine that the response is HTML code. This is achieved by choosing the **<Create New Precondition…>** option from the **Precondition** drop-down menu and then entering in the data, as shown in Figure 3-61.

Figure 3-64 Create a Precondition



Step 3 Select the newly created precondition for the outbound rule and then enter data in the fields, as shown in Figure 3-65.

Figure 3-65 Enter Data in Newly Created Precondition



This rule will parse the response of the internal FactoryTalk Application server and if the response is HTML, it will:

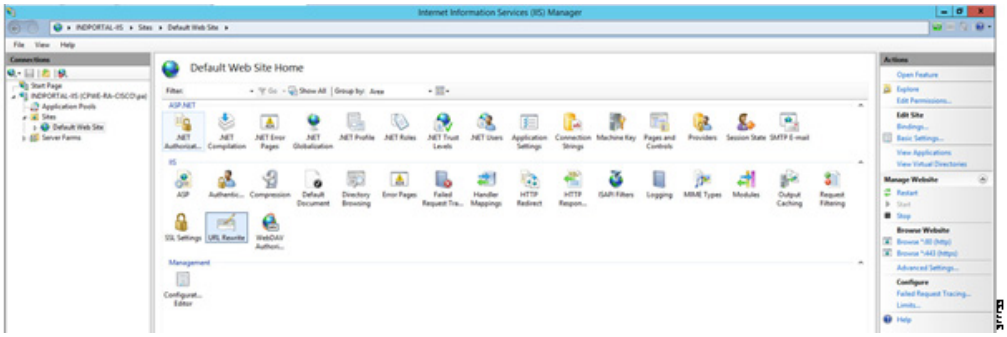
- replace any occurrences of *prodvp.cpwe-ra-cisco.local*
- with *indportal-iis.cpwe-ra-cisco.local*

URL Rewrite Rules for the FactoryTalk ViewPoint Application

To create an inbound URL rewrite rule on the reverse web proxy server to relay requests aimed at the FactoryTalk ViewPoint Application, complete the following steps:

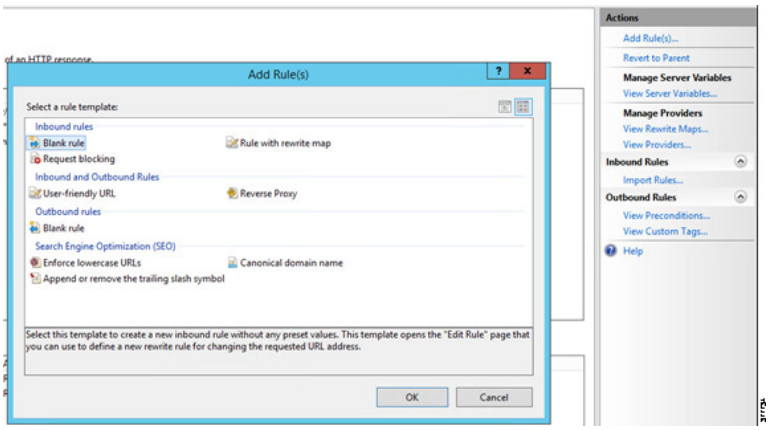
Step 1 Open the reverse web proxy's IIS manager, navigate to the **Default Web Site** folder and then open the **URL Rewrite Options** panel, as shown in Figure 3-66.

Figure 3-66 Open the URL Rewrite Options Panel



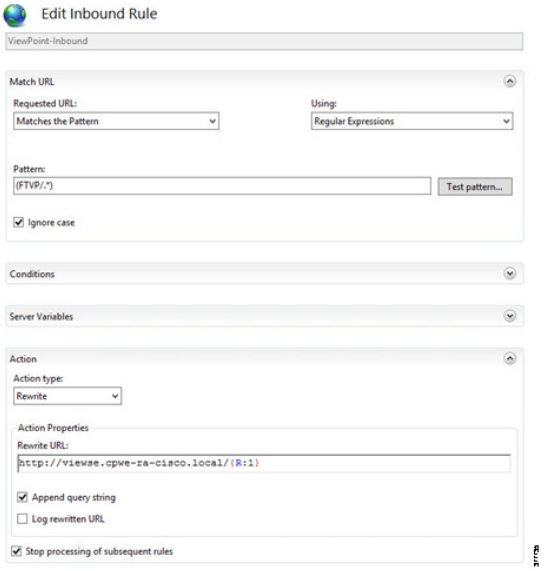
Step 2 Under **Actions**, click **Add Rule(s)…** and choose a blank inbound rule, as shown in Figure 3-64.

Figure 3-67 Choose a Blank Inbound Rule



Step 3 Fill in the fields shown in Figure 3-68, with **FTVP** being the FactoryTalk ViewPoint application web application that runs on the FactoryTalk ViewPoint server.

Figure 3-68 Make FTVP the FactoryTalk ViewPoint Application Web Application



This rule will parse the incoming request URL for the string *FTVP/* and if found replaces the leading part of the URL *https://**indportal**-iis.cpwe-ra-cisco.local/* with *https://viewse.cpwe-ra-cisco/*, leaving the trailing part of the request URL intact.

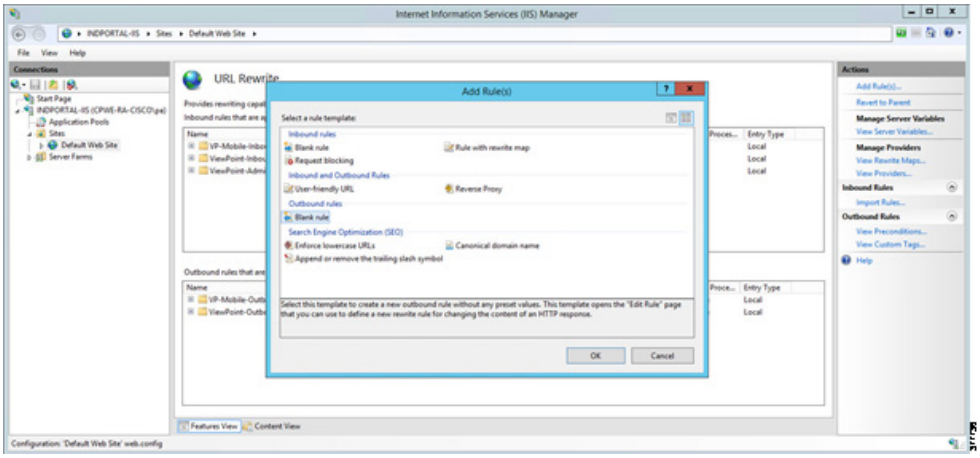
This inbound rewrite rule enables the reverse web proxy server to change an incoming request URL like *https://indportal-iis.cpwe-ra-cisco.local/FTVP/ViewPoint.aspx?raml=Main&area=/* to *https://**viewse**.cpwe-ra-cisco.local/FTVP/ViewPoint.aspx?raml=Main&area=/* and forward it to the FactoryTalk ViewPoint hosting server (VIEWSE).

The response from the FactoryTalk ViewPoint server might contain local references to URLs and links to image and icon objects that need to be rewritten by the reverse web proxy.

To create an outbound URL rewrite rule on the reverse web proxy server to address these local references, complete the following steps:

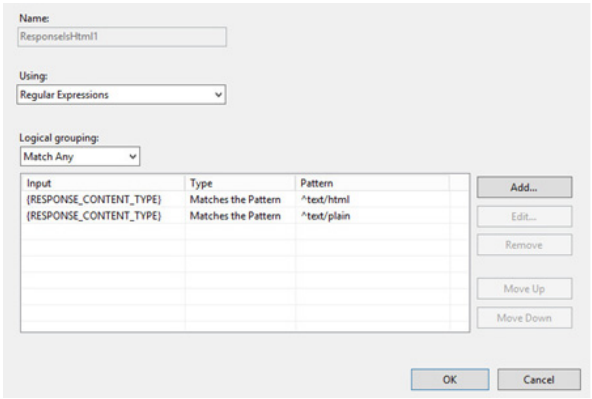
Step 1 From the URL rewrite page, click **Add Rules(s)…** and then choose the blank outbound rule option, as shown in Figure 3-69.

Figure 3-69 Choose the Blank Outbound Rule Option\



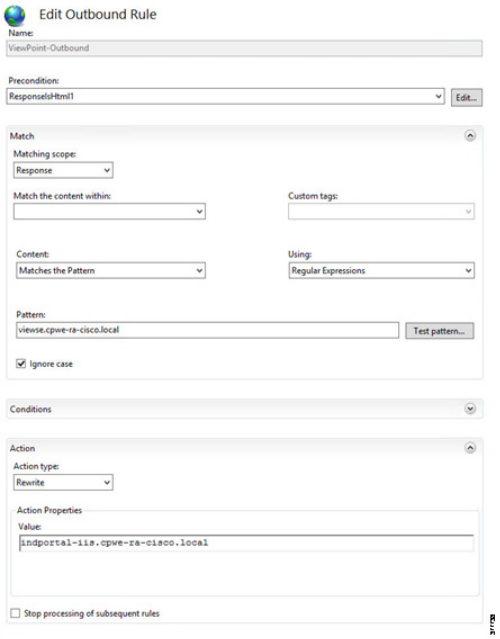
Step 2 Create a Precondition that the outbound rule will use to determine that the response is HTML code. This is achieved by choosing the **<Create New Precondition…>** option from the **Precondition** drop-down menu and then entering in the data, as shown in Figure 3-70.

Figure 3-70 Create a Precondition



Step 3 Choose the newly created precondition for the outbound rule and enter data in the fields, as shown in Figure 3-71.

Figure 3-71 Choose the Newly Created Precondition for the Outbound Rule



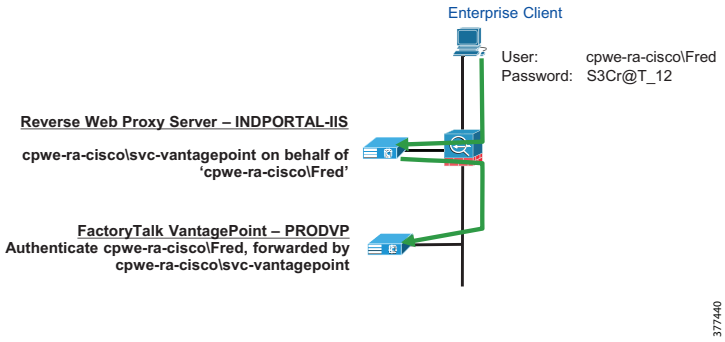
This rule will parse the response of the internal server and determine if the response is HTML. If yes, it will replace any occurrences of *viewse.cpwe-ra-cisco.local* with *indportal-iis.cpwe-ra-cisco.local*

User Authentication Configuration

The reverse web proxy can pass the user's credentials on to the targeted FactoryTalk application servers. To accomplish this, a domain service account, that “relays” the enterprise client's credentials needs to be set up. This service account will be assigned to the IIS ApplicationPools that are used by the reverse web proxy server and the FactoryTalk Application servers. Then that service account needs to be tied to the IIS reverse web proxy server Service Principal Name (SPN) entries in Active Directory to allow the account Kerberos relaying. As a final step to make authentication work, the FactoryTalk Web Application settings need to be tuned to use the appropriate authentication methods for incoming requests.

Figure 3-72 illustrates what the authentication process will look like from a high level perspective.

Figure 3-72 Reverse Web Proxy Authentication Relaying



Configuration changes, which need to be made to the domain setup via a Domain Controller, the reverse web proxy setup, the FactoryTalk VantagePoint Mobile setup and the FactoryTalk ViewPoint setup, will be discussed in the following sections. These configuration changes will requires rights to create and modify accounts and to create service principal names in the domain.

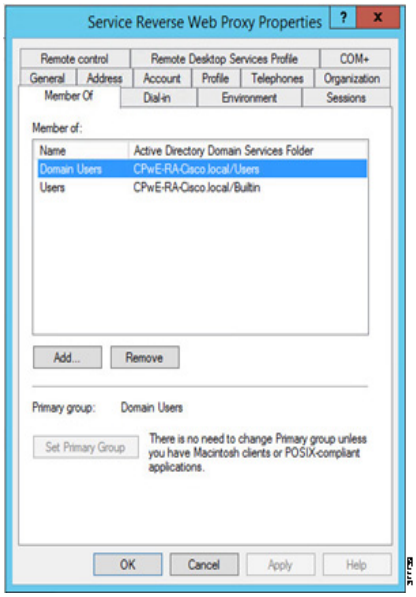
Configuring the Domain Controller

To configure the domain controller, complete the following steps:

Step 1 Create the service account to be used by the ApplicationPools on the web servers.

Create the service login account in the domain, as shown in Figure 3-73. This account must be a member of the following security groups. In this example, the service account is called *svc-indportal-iis*.

Figure 3-73 Create the Service Login Account in the Domain

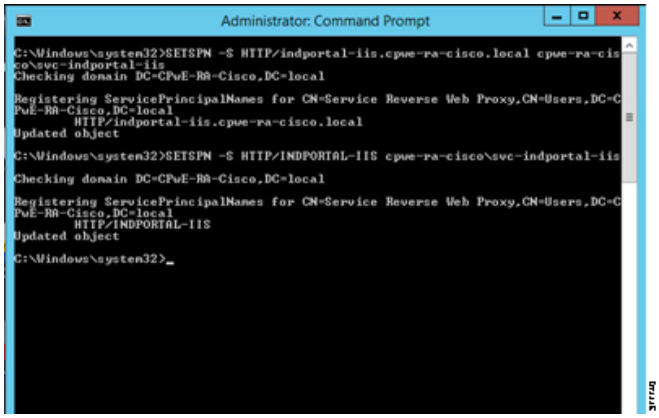


Note A Service Principal Name (SPN) is a unique identifier of a service instance. SPNs are used by Kerberos authentication to associate a service instance with a service logon account. This allows a client application to request that the service authenticate an account even if the client does not have the account name. An SPN needs to be created for the service account that was just configured to allow it to broker authentication between the enterprise client and the resource in the Industrial Zone.

Step 2 From an elevated command prompt on the domain controller, enter the following commands to create the SPN for the service account. Refer also to Figure 3-74.

- *SETSPN -S HTTP/indportal-iis.cpwe-ra-cisco.local cpwe-ra-cisco\svc-indportal-iis*
- *SETSPN -S HTTP/INDPORTAL-IIS cpwe-ra-cisco\svc-indportal-iis*

Figure 3-74 Create an SPN for the Service Account



Note These commands are specific for the lab environment that was used to create this CVD. The syntax for the command is as follows, where servername is the computer name for the reverse web proxy server:

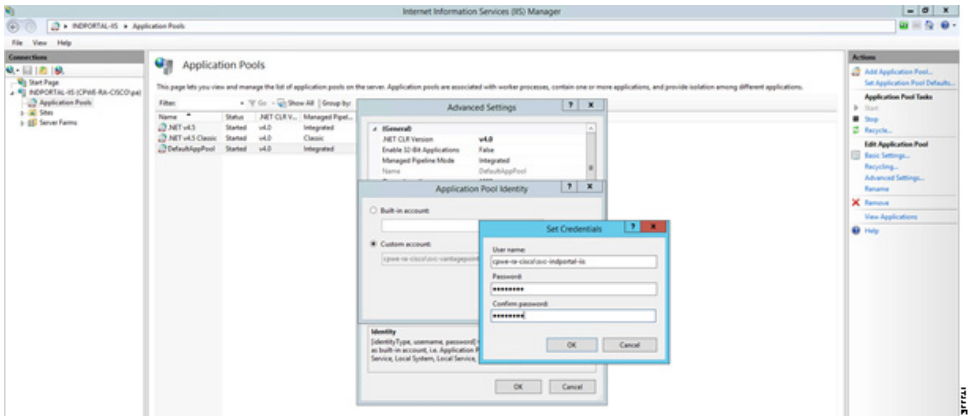
- *SETSPN -S HTTP/<fully-qualified-servername> <domain-name>\<service-account-name>*
- *SETSPN -S HTTP/<netbios-servername> <domain-name>\<service-account-name>*

Configuring the Reverse Web Proxy Server Authentication

On the reverse web proxy server (INDPORTAL-IIS) server, in IIS Manager:

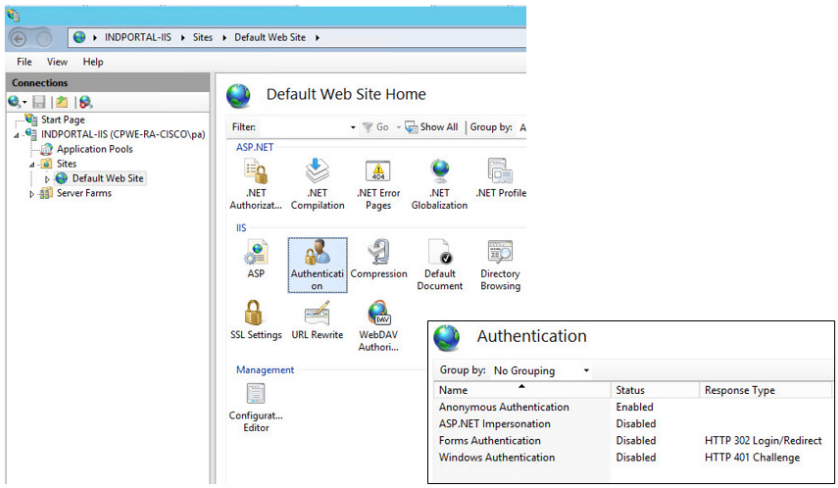
Step 1 Change the identity used for the **DefaultApplicationPool** ApplicationPool to *svc-indportal-iis,* as shown in Figure 3-75:

Figure 3-75 Change the ApplicationPool Identity



Step 2 Change the authentication methods for the Default Web Site to only enable the **Anonymous Authentication** method, as shown in Figure 3-76.

Figure 3-76 Change the Authentication Methods for the Default Web Site



Configuring the FactoryTalk VantagePoint Application Server

Configuring HTTPS

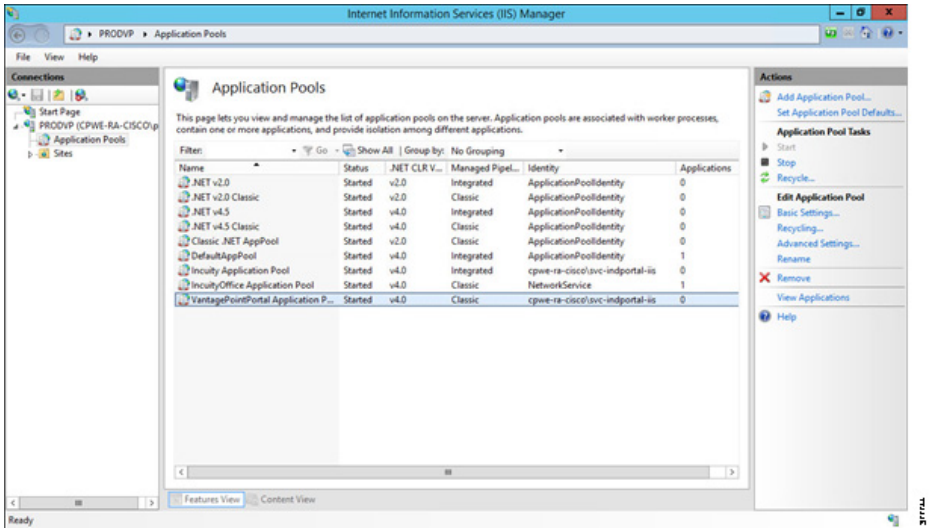
HTTPS must be configured on the FactoryTalk VantagePoint application servers. To configure the HTTPS server refer to Configuring HTTPS, page 3-35.

FactoryTalk VantagePoint Web Server Authentication Configuration

On the FactoryTalk ViewPoint server (PRODVP), in IIS Manager:

Step 1 Change the identity used for the **VantagePointPortalApplicationPool** and the **IncuityApplicationPool** ApplicationPools to *svc-indportal-iis,* as shown in Figure 3-77.

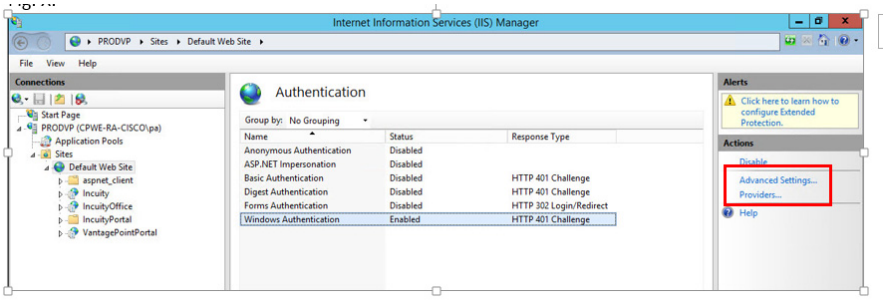
Figure 3-77 Change the ApplicationPools Identity



Step 2 Change the appropriate authentication methods for the Default Web Site.

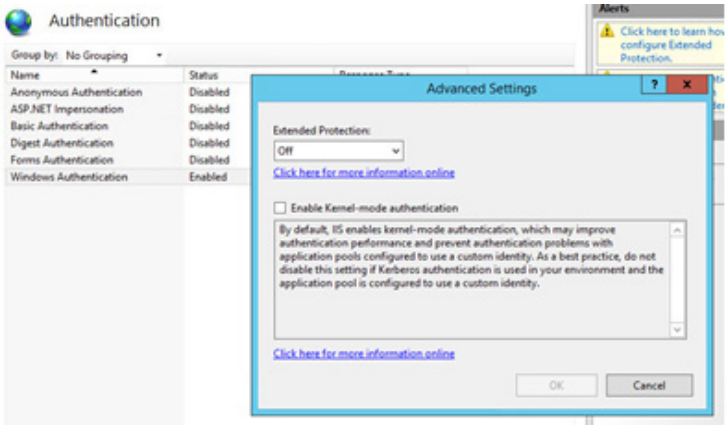
a. Only enable **Windows Authentication** as the accepted authentication method, as shown in Figure 3-78.

Figure 3-78 Enable Windows Authentication as the Accepted Authentication Method



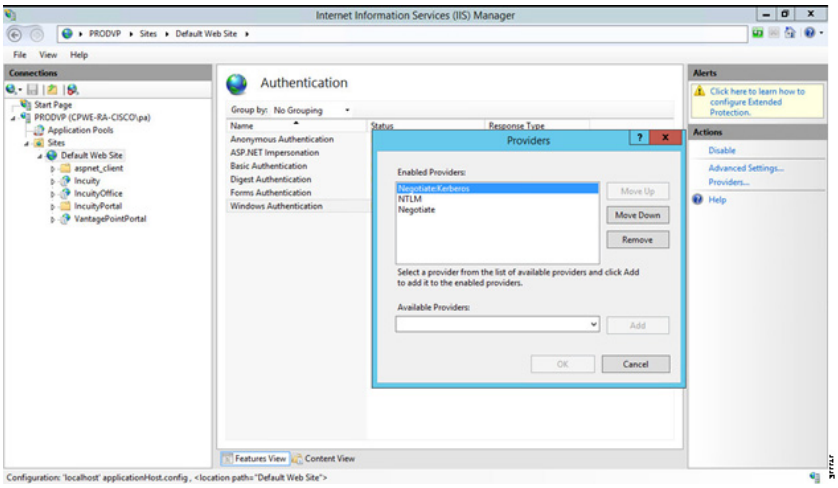
b. Disable **Kernel-mode authentication** from the advanced settings of the **Windows Authentication** method, as shown in Figure 3-79.

Figure 3-79 Disable Kernel-mode Authentication



c. Add **Negotiate:Kerberos** to the **Providers** and reorder them to match Figure 3-80.

Figure 3-80 Add Negotiate:Kerberos to the Providers

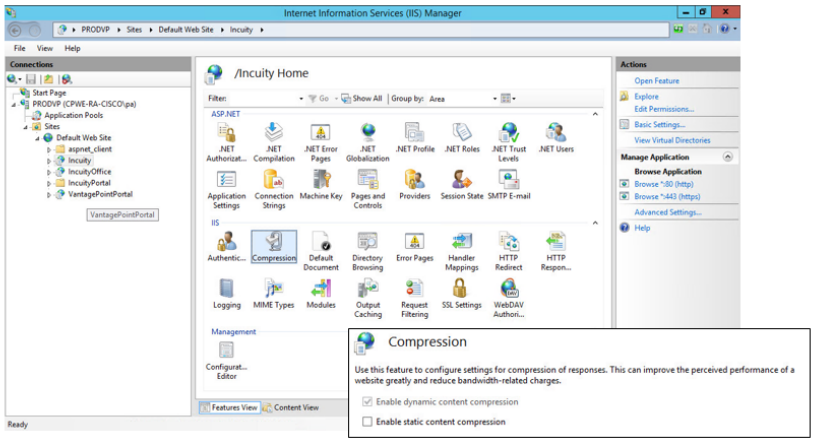


FactoryTalk VantagePoint Mobile Web Server Compression Configuration

The reverse proxy server requires that the server send the page as uncompressed data. Enabling compression would help prevent the proxy from substituting the URLs in the page.

Within IIS Manager, for the Incuity web application, as shown in Figure 3-81, click **Compression** and then uncheck the **Enable static content compression** check box.

Figure 3-81 click Compression and then Uncheck the Enable Static Content Compression Check Box



Configuring FactoryTalk ViewPoint Application Server

HTTPS Configuration

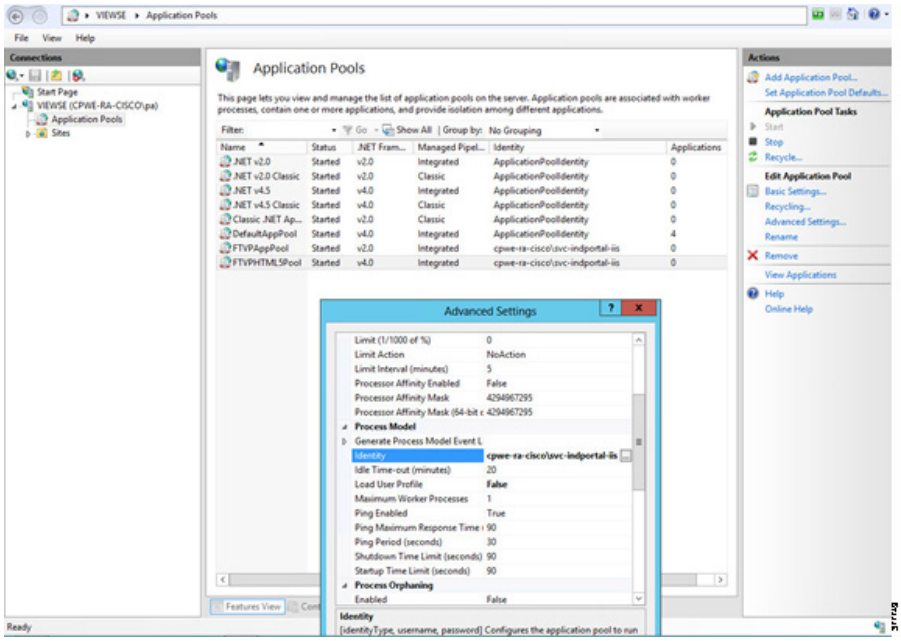
HTTPS must be configured on the FactoryTalk VantagePoint application servers. To configure the HTTPS server, please refer to Configuring HTTPS, page 3-23.

FactoryTalk ViewPoint Web Server Authentication Configuration

On the FactoryTalk ViewPoint (VIEWSE) server, in IIS Manager:

Step 1 Change the identity used for the **FTVPHTML5Pool** and the **FTVPAppPool** ApplicationPools to *svc-indportal-iis*, as shown in Figure 3-82.

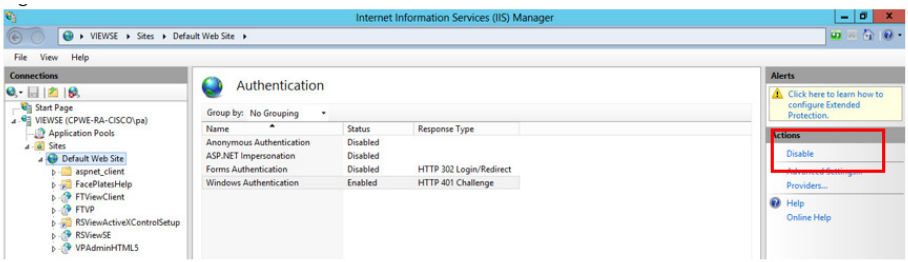
Figure 3-82 Change the Application Pools Identity



Step 2 Change the appropriate authentication methods for the Default Web Site:

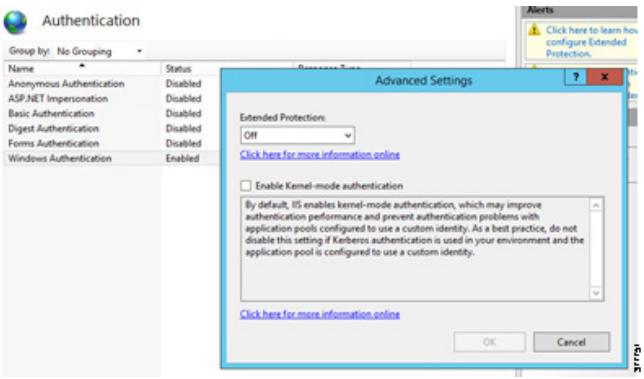
a. Only enable **Windows Authentication** as the accepted authentication method, as shown in Figure 3-83.

Figure 3-83 Enable Windows Authentication as the Accepted Authentication Method



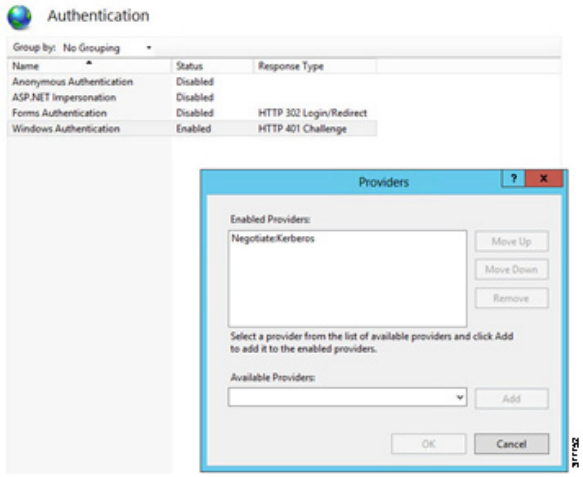
b. Disable **Kernel-mode authentication** from the advanced settings of the **Windows Authentication** method, as shown in Figure 3-84.

Figure 3-84 Disable Kernel-mode Authentication



c. Add **Negotiate:Kerberos** to the providers and remove all other providers, as shown in Figure 3-85.

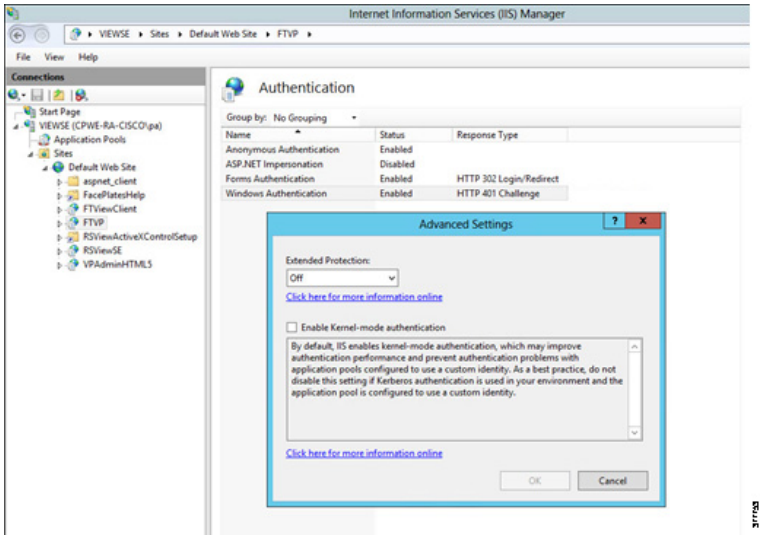
Figure 3-85 Add Negotiate:Kerberos to the Providers



Step 3 Change the settings for the **Windows Authentication** method of the FTVP web application and leave all other authentication methods as default.

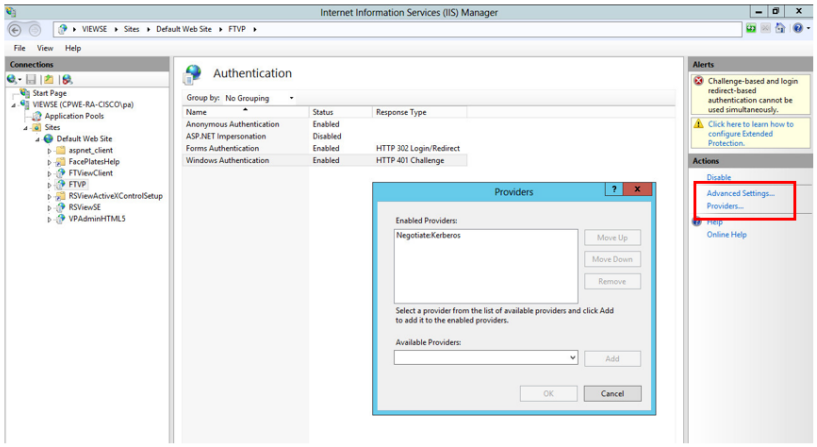
a. Disable **Kernel-mode authentication** from the advanced settings of the **Windows Authentication** method, as shown in Figure 3-86.

Figure 3-86 Disable Kernel-mode Authentication



b. Add **Negotiate:Kerberos** to the **Windows Authentication** method providers and remove all others, as shown in Figure 3-87.

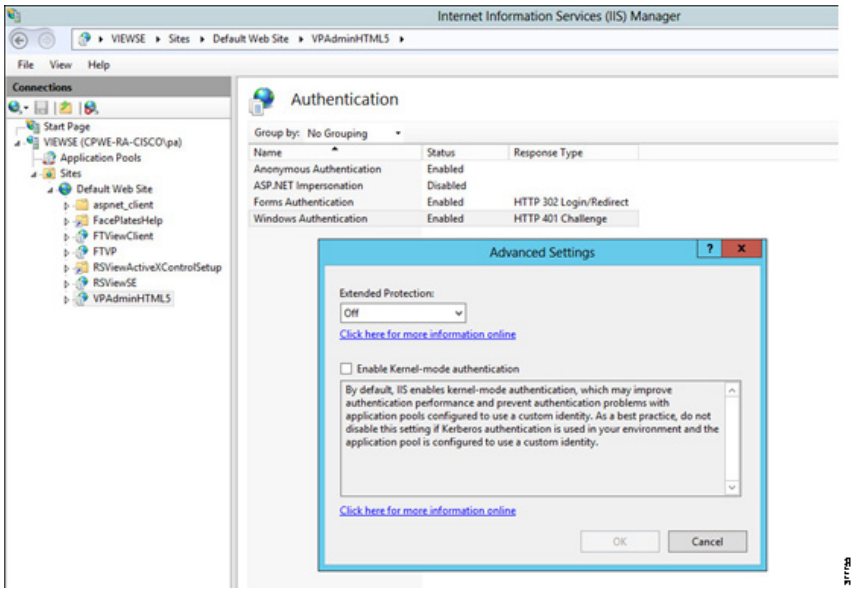
Figure 3-87 Add Negotiate:Kerberos to the Windows Authentication Method Providers



Step 4 Change the settings for the **Windows Authentication** method of the **VPAdminHTML5** web application and leave all other authentication methods as default.

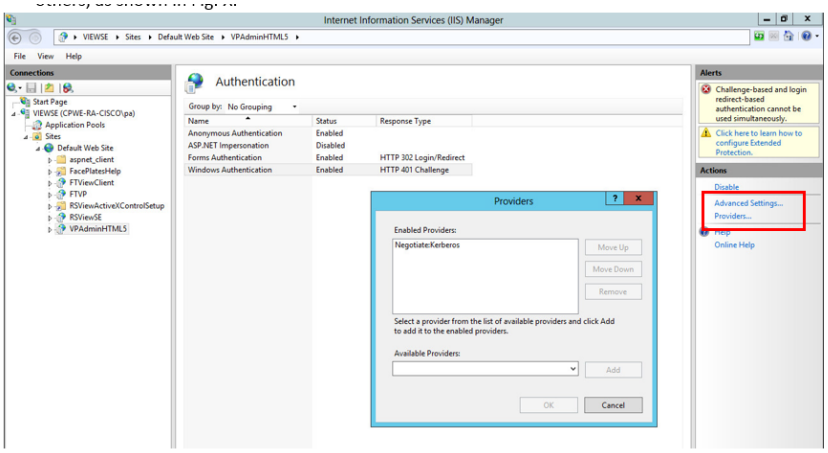
a. Disable **Kernel-mode authentication** from the advanced settings of the **Windows Authentication** method, as shown in Figure 3-88.

Figure 3-88 Disable Kernel-mode Authentication



b. Add **Negotiate:Kerberos** to the **Windows Authentication** method providers and remove all others, as shown in Figure 3-89.

Figure 3-89 Add Negotiate:Kerberos to the Windows Authentication Method Providers



FactoryTalk ViewPoint Web Server Compression Configuration

The reverse proxy server requires that the server send the page as uncompressed data. Enabling compression would prevent the proxy from substituting the URLs in the page.

Within IIS manager, for the FTVP and VPAdminHTML5 web applications, click **Compression** and then uncheck the **Enable static content compression check box**, as shown in Figure 3-90 and Figure 3-91.

Figure 3-90 fTVP Web Application—Enabling Compression

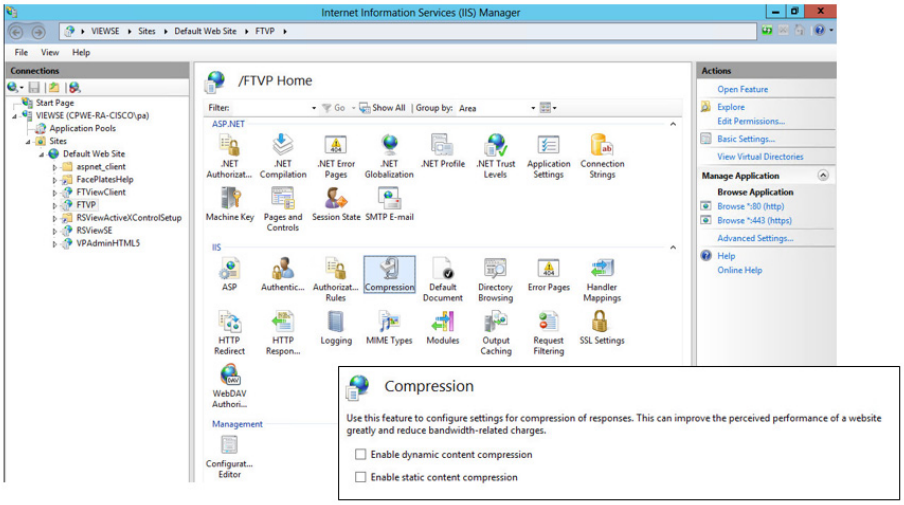
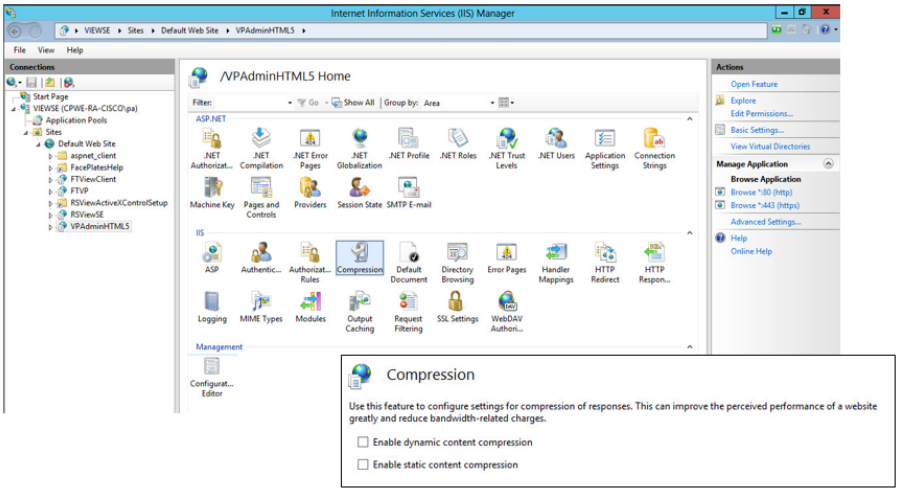


Figure 3-91 VPAdminHTML5 Web Application—Enabling Compression



Testing the Configuration

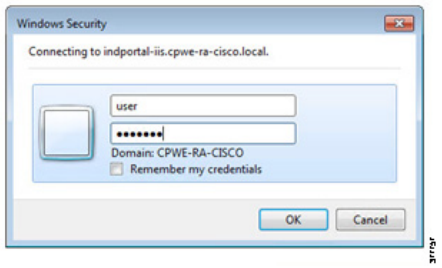
Testing the FactoryTalk VantagePoint Mobile Application

In order to test access through the reverse web proxy, open a web browser and navigate to the following URL:

- https://indportal-iis.cpwe-ra-cisco.local/incuity/thinui

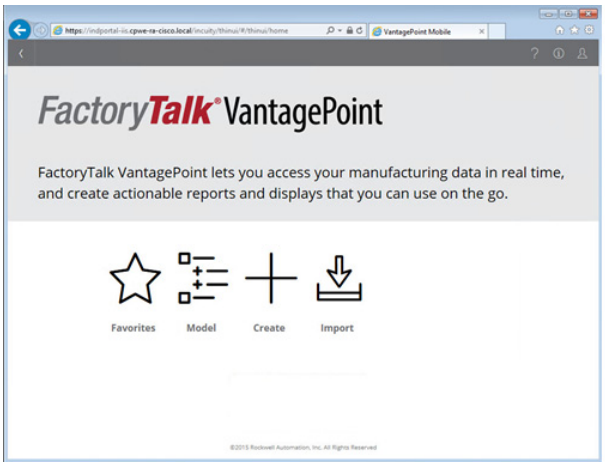
At this point, the reverse web proxy server will forward the request to the FactoryTalk VantagePoint Mobile web app and, after authentication, the screen shown in Figure 3-92 will display.

Figure 3-92 Windows Security Screen



Access to the mobile app is established from an Enterprise Zone client to the FactoryTalk application in the Industrial Zone through the reverse web proxy that sits in the Industrial Demilitarized Zone, as shown in Figure 3-93.

Figure 3-93 FactoryTalk Vantage Point



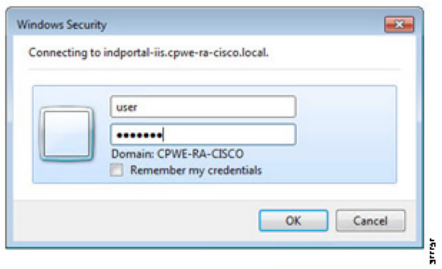
Testing the FactoryTalk ViewPoint Web Application

In order to test access through the reverse web proxy, open a web browser and navigate to the following URL

- https://indportal-iis.cpwe-ra-cisco.local/FTVP/

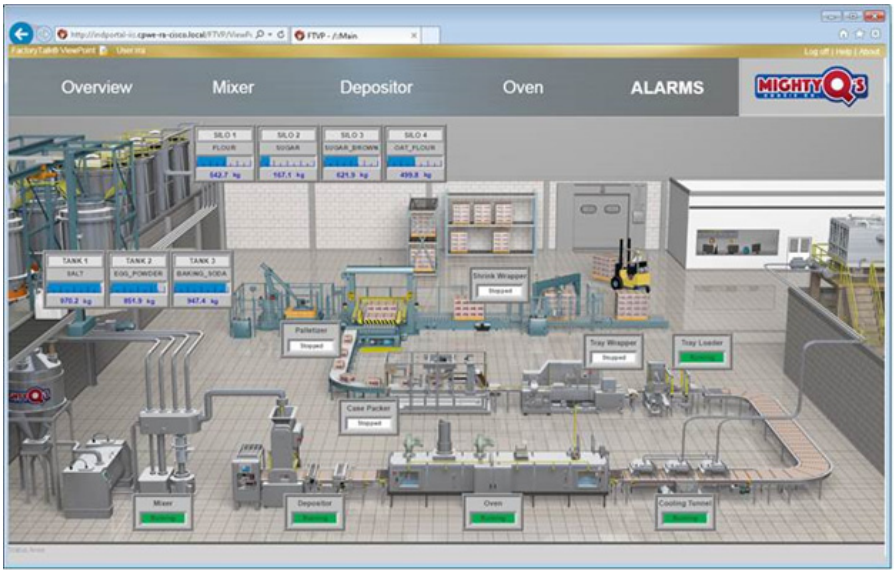
At this point, the reverse web proxy server will forward the request to the FactoryTalk ViewPoint web application and after authentication, the screen shown in Figure 3-94 will display.

Figure 3-94 Windows Security Screen



Access to the mobile app is established from an Enterprise Zone client to the FactoryTalk application in the Industrial Zone, through the reverse web proxy that sits in the Industrial Demilitarized Zone, as shown in Figure 3-95.

Figure 3-95 Reverse Web Proxy in the IDMZ



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 the following URL:

- 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 SE 3.0 H2H Interface Installation and Configuration Guide*:
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/in/h2h-in001_-en-e.pdf
- *FactoryTalk Historian SE 3.0 H2H 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).

a. Go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility**. The ICU dialog box appears.

b. 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\FTPItoPI\FTPItoPI.exe*.

c. 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

d. Under Scan Classes, create one scan class at a 15 second frequency.

e. 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.

f. In the **Service** tab, click **Create**.

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

a. Go to **Start > All Programs > Rockwell Software > FactoryTalk Historian SE > System Management Tools**. The System Management Tools dialog box appears.

b. Under **Collectives and Servers**, select the **Enterprise Zone FactoryTalk Historian server**.

c. Under **System Management Tools**, select **Points > Point Builder**. Click the toolbar icon to create anew point.

d. In the **General** tab, complete the following information:

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

e. In the Classic tab, complete the following information:

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

f. 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 PIadmin user on the Enterprise FactoryTalk Historian server.

a. 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.

b. 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 3-18).

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 3-18 Access Rules - Historian Data Transfer

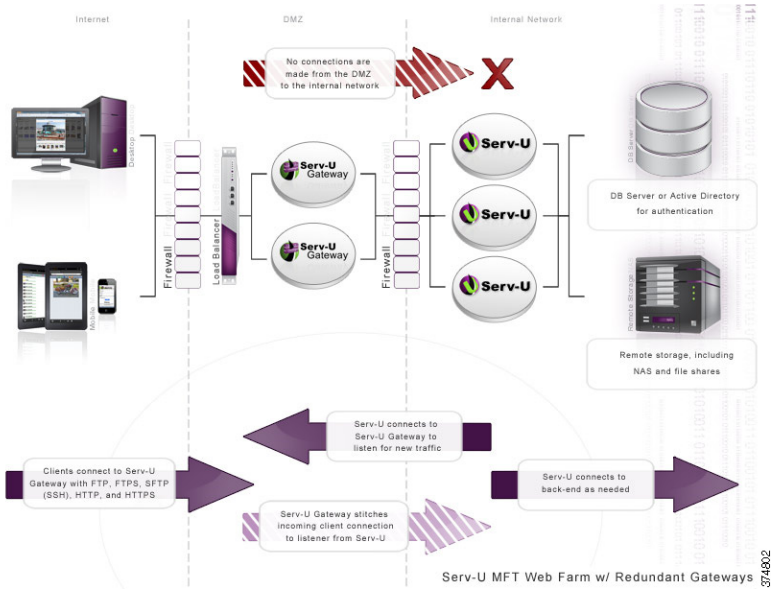
Firewall Interface	Source	Destination	Permitted protocols
Industrial	Industrial Zone Historian	PI to PI server	PI Server Client Access (TCP port 5450) RPC (TCP port 135)
Enterprise	Enterprise Zone Historian	PI to PI server	
IDMZ	PI to PI server	Industrial Zone Historian Enterprise Zone Historian	

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).

Managed File Transfer Configuration

To facilitate secure managed file transfer (MFT) between the Enterprise and Industrial Zones via the IDMZ, many implementations are available to choose from. For testing purposes, the SolarWinds Serv-U MFT Server and Gateway software was selected to provide this function. See Figure 3-96

Figure 3-96 Serv-U MFT Implementation (from http://www.solarwinds.com)



As shown above, the Serv-U Gateway listens for incoming connections via a secure file transfer protocol such as SFTP. These connections are then "stitched" through the Gateway using a separate proprietary port and forwarded to the MFT Server.

In the context of the IDMZ, a client based in the Industrial Zone can upload to and download files from the MFT 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 MFT Server via the IDMZ Gateway.

The following steps describe the configuration of firewall rules to allow secure MFT services across the IDMZ, using Serv-U as an example (see Table 3-19 and Table 3-20):

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 Secure FTP protocol using SSH TCP port 22.

Step 2 Configure the firewall to allow incoming client connections from Enterprise Zone clients to the IDMZ-based gateway server. The clients use the Secure FTP protocol using SSH TCP port 22.

Step 3 Configure the firewall to allow the MFT server in the Enterprise Zone to communicate with the MFT gateway about any incoming connections. The server uses the Serv-U proprietary listening TCP port 1180.

Step 4 Configure the firewall to allow the MFT server in the Industrial Zone to communicate with the MFT gateway about any incoming connections. The server uses the Serv-U proprietary listening TCP port 1180.

Table 3-19 Access Rules - Managed File Transfer (Serv-U) Industrial to Enterprise

Firewall Interface	Source	Destination	Permitted Protocols
Industrial	Any (or specific clients in Industrial Zone)	MFT Gateway in IDMZ	Secure FTP / SSH (TCP port 22)
Enterprise	Enterprise MFT server	MFT Gateway in IDMZ	Serve-U listening port (TCP port 1180)

Table 3-20 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	Secure FTP / SSH (TCP port 22)
Industrial	Industrial MFT server	MFT Gateway in IDMZ	Serve-U listening port (TCP port 1180)

The access rules can be applied using Cisco ASA web interface (see Figure 3-47 on page 3-15 in the Active Directory section as an example). The equivalent CLI configuration for Steps 1-4 is shown below:

```
access-list Industrial_access_in extended permit tcp any object MFT_Gateway eq ssh
access-list Enterprise_access_in extended permit object Serv-U object MFT_Server_Ent
object MFT_Gateway
access-list Enterprise_access_in extended permit tcp any object MFT_Gateway eq ssh
access-list Industrial_access_in extended permit object Serv-U object MFT_Server_Ind
object MFT_Gateway
```

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
  - Clientless SSL VPN configuration to the IDMZ firewall
- Microsoft RD Gateway configuration
- ASA RDP plug-in configuration

SSL VPN Configuration

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

Note Additional information about VPN configuration on the Cisco ASA firewall can be found here in the *Cisco ASA Series VPN ASDM Configuration Guide* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm.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 ASA flash (images are downloaded from Cisco).

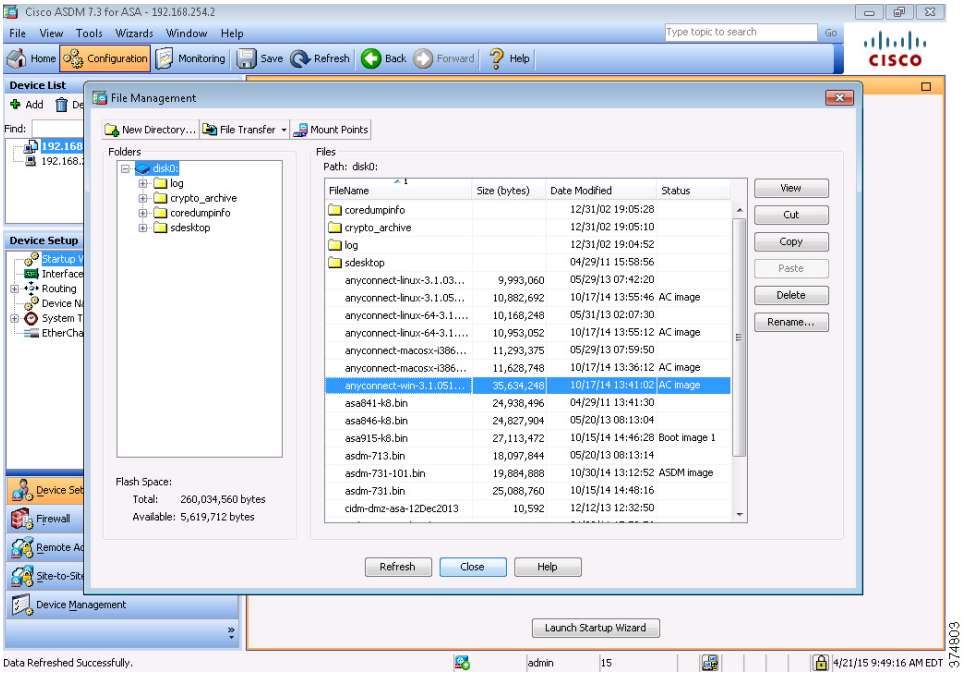
a. Navigate to **Tools > File Management** (see Figure 3-97).

b. Click **File Transfer**, and then select **Between Local PC and Flash**.

c. Browse to the correct location on your local file system and copy each AnyConnect client image to the Cisco ASA flash memory by selecting the image and then clicking the right arrow. Repeat this step for each desired OS (Windows, Linux and OS X).

d. After completing the file transfers for all client images, click **Close**.

Figure 3-97 Loading AnyConnect Client Images



Step 2 Complete the AnyConnect VPN wizard.

a. Navigate to **Wizards > VPN Wizards > AnyConnect VPN Wizard**. Click **Next**.

b. In the Connection Profile Name box, enter any desired name. In the VPN Access Interface list, choose the primary Internet (outside) connection and then click **Next** (see Figure 3-98).

c. Under VPN Protocols, select **SSL** and clear **IPsec**. Select the ASA's certificate in the **Device Certificate** box and then click **Next** (see Figure 3-99).

Figure 3-98 AnyConnect VPN Wizard - Connection Profile

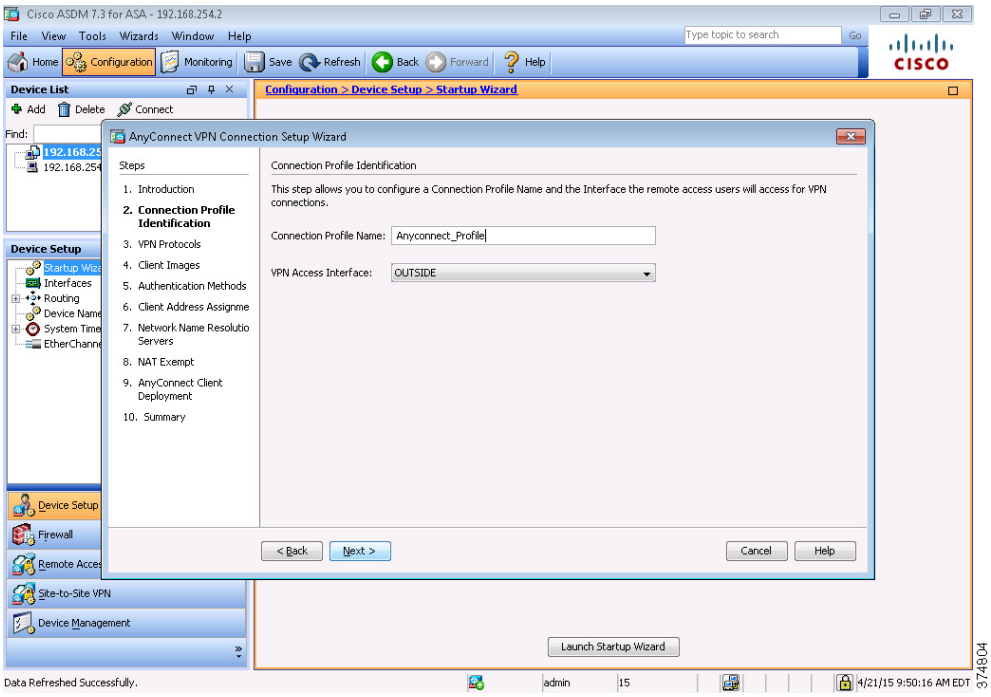
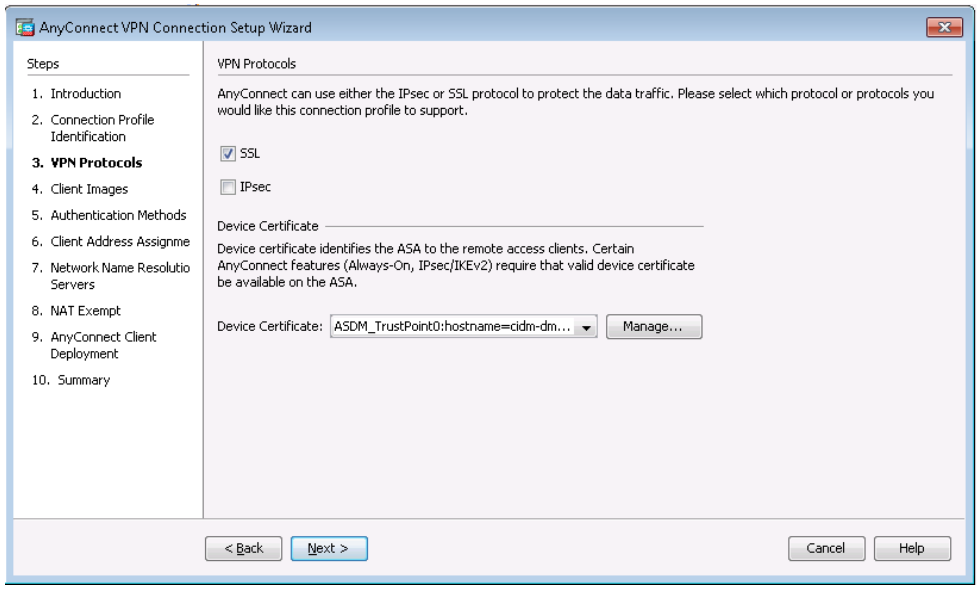


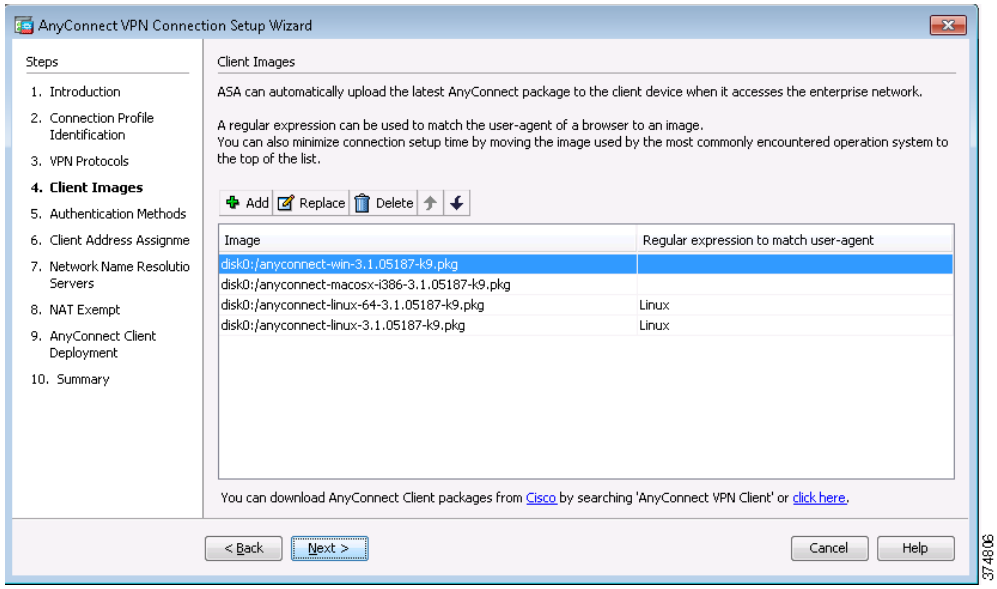
Figure 3-99 AnyConnect VPN Wizard - Protocols



d. On the Client Images page, click **Add > Browse Flash**. Select the appropriate AnyConnect client image to support your user community (Windows, Linux, OS X) and then click **OK**.

e. Repeat the process for all the required Cisco AnyConnect client images. If necessary, reorder the list of images so that the most commonly used image is listed first and least commonly used images are listed last. Click **Next** (see Figure 3-100).

Figure 3-100 AnyConnect VPN Wizard - Client Images

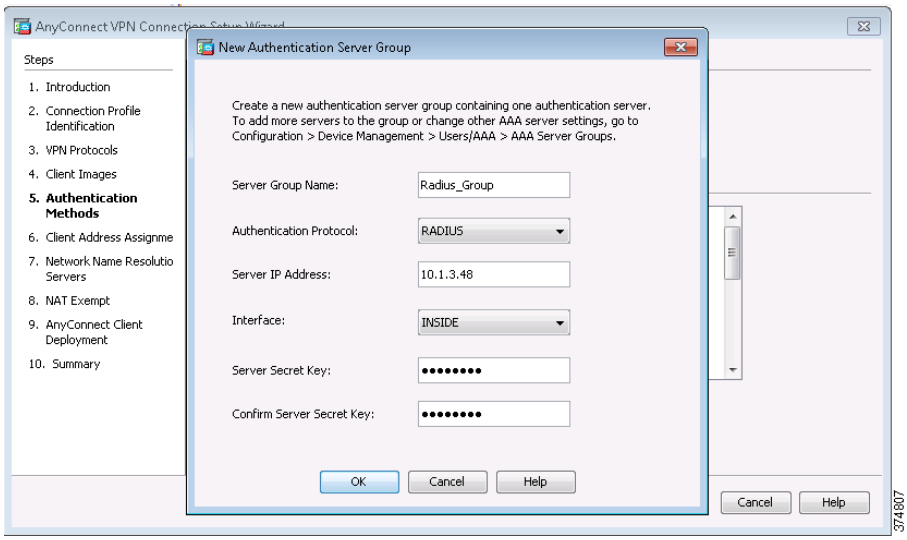


f. On the Authentication Methods page, next to AAA Server Group, click **New**. Enter the following values, and then click **OK** (see Figure 3-101):

- **Server Group Name**: Any desired name
- **Authentication Protocol**: RADIUS
- **Server IP Address**: IP address of the RADIUS server, for example Enterprise ISE node
- **Interface**: Name of the enterprise-facing (inside) connection
- **Server Secret Key**: Any desired secret key
- **Confirm Server Secret Key**: Repeat secret key

On the **Authentication Methods** page, click **Next**.

Figure 3-101 AnyConnect VPN Wizard - Authentication Server



g. On the Client Address Assignment page, in the IPv4 Address Pool tab, click **New**.

h. On the Add IP Pool dialog box, enter the IP Pool name, the IP range and the subnet mask to assign to the VPN clients and then click **OK** (see Figure 3-102).

i. Verify that the pool you just created is selected, and then click **Next**.

j. On the **Network Name Resolution Servers** page, enter the **Enterprise DNS Server IP address** and **Domain Name** and then click **Next** (see Figure 3-103).

k. Click **Next** on the **NAT Exempt** page and the **AnyConnect Client Deployment** page. On the **Summary** page, click **Finish**.

Figure 3-102 AnyConnect VPN Wizard - Client Address

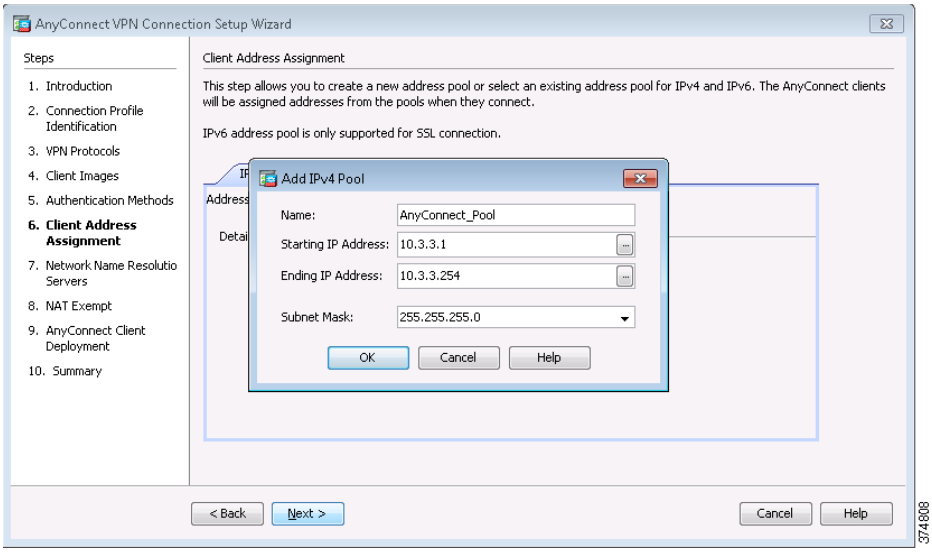
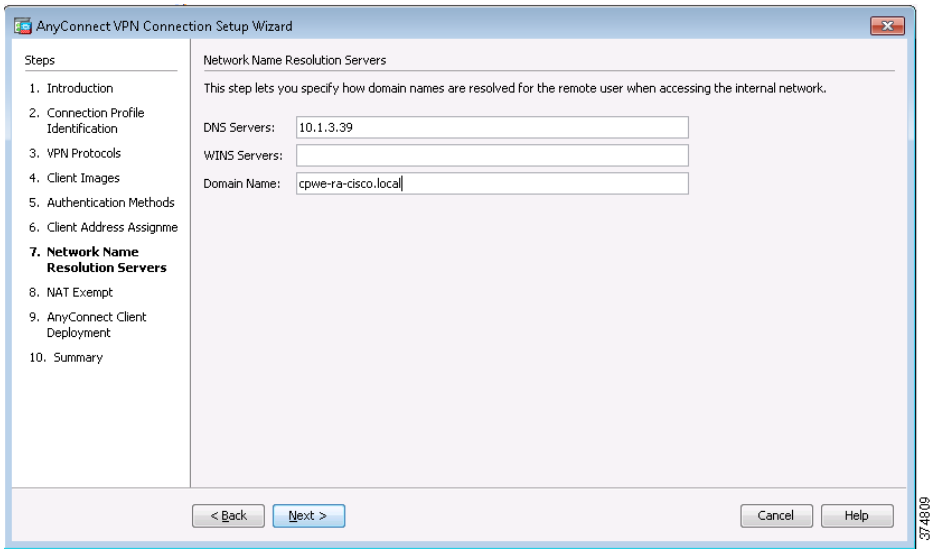


Figure 3-103 AnyConnect VPN Wizard - Name Servers



Step 3 Configure the Group Policy.

a. Select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Click **Add**.

b. On the **Add Internal Group Policy** dialog box (see Figure 3-104), enter the policy name. For **Banner**, clear the **Inherit** check box, then enter a banner message that will be displayed for a remote user. Expand the **More Options** pane.

c. For **Filter**, clear the **Inherit** check box, and then click **Manage**. On the **ACL Manager** dialog box, click the **Standard ACL** tab, click **Add** and then click **Add ACL**.

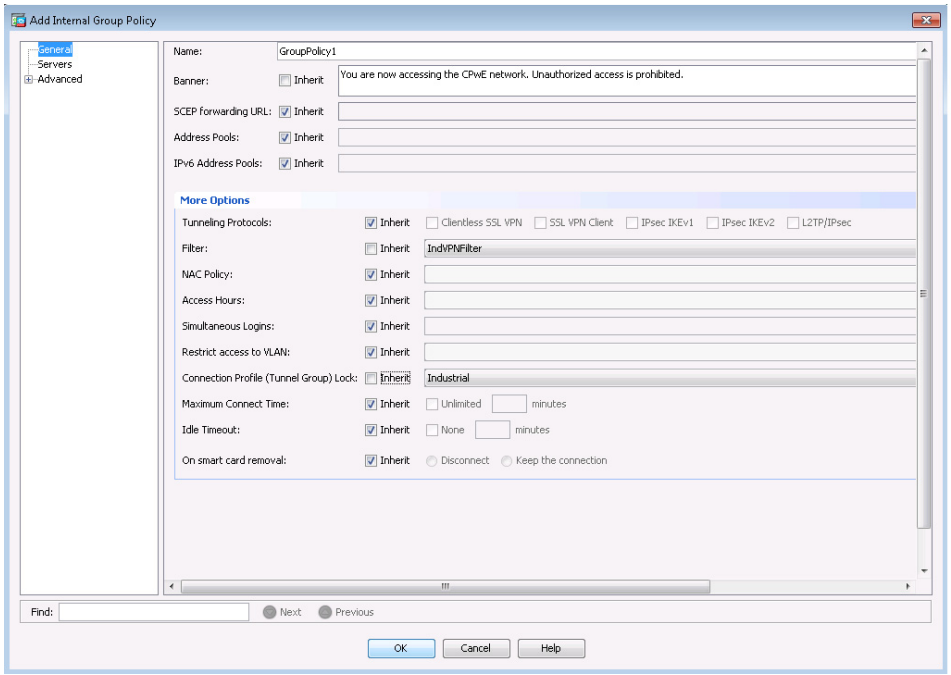
d. On the **Add ACL** dialog box, enter an **ACL Name**, and then click **OK**. Click **Add** and then **Add ACE**. On the **Add ACE** dialog box, for **Action**, select **Permit**.

e. In the **Address** box, enter the IP address and subnet mask that the remote user is allowed to access (for example, the IDMZ ASA web portal) and then click **OK**. On the **ACL Manager** dialog box, click **OK**.

f. If multiple connection profiles will be available for a remote user, the Tunnel Group Lock feature will restrict which user can access which group depending on a RADIUS attribute that is received during the authorization phase. To enable this feature, clear the **Inherit** check box for **Connection Profile (Tunnel Group) Lock**, then select the **Connection Profile** name that should be locked to this group policy.

Note For the Group Lock feature to function, the RADIUS server must be configured to send attribute 85 (Tunnel-Group-Lock) containing the group name that the user is authorized for.

Figure 3-104 AnyConnect VPN Group Policy - General

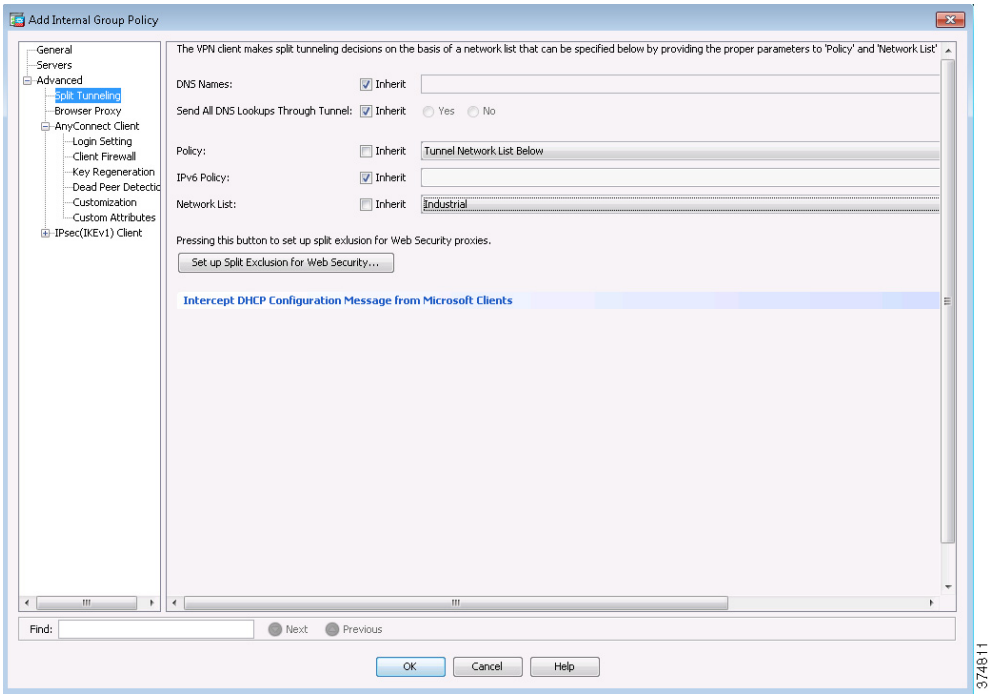


g. If users should be able to access other locations on the Internet while connected to the remote access VPN, split tunneling should be enabled. Expand the **Advanced** option in the left pane, and then click **Split Tunneling** (see Figure 3-105).

h. For **Policy**, clear the **Inherit** check box and select **Tunnel Network List Below**.

i. For **Network List**, clear the **Inherit** check box and click **Manage**. On the **ACL Manager** dialog box, add the **Extended ACL** that permits IP subnets corresponding to network destinations that should be sent through the VPN tunnel.

Figure 3-105 AnyConnect VPN Group Policy - Split Tunneling



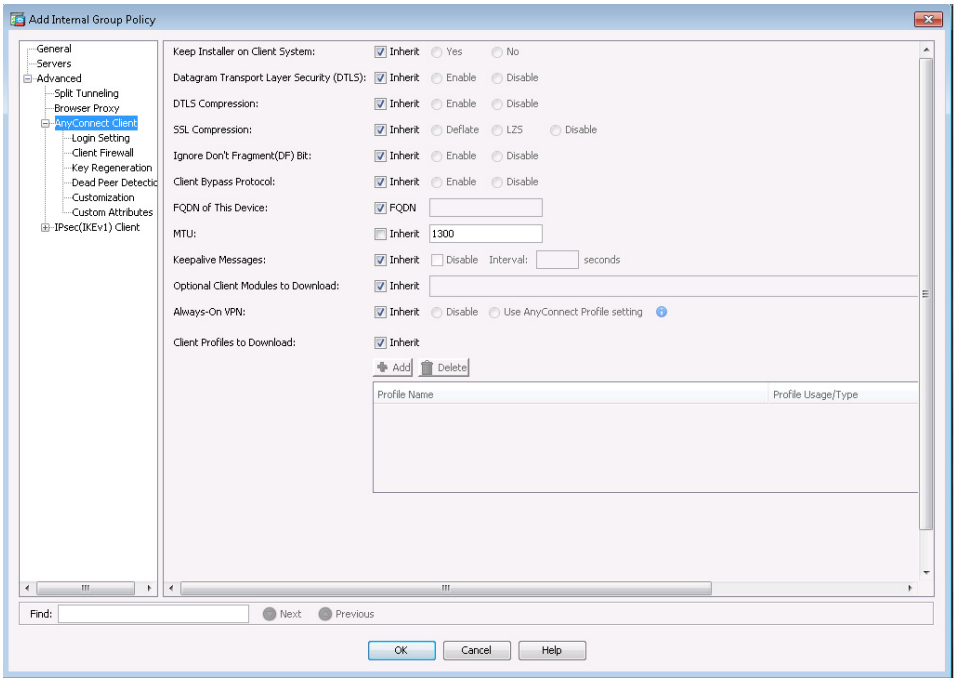
j. In certain cases, when using DTLS/TLS with SSL, users may see a VPN reconnection after 1 minute. This can happen due to fallback from DTLS to TLS and MTU renegotiation if DTLS is not allowed through the corporate firewall. To prevent this, adjust the MTU size for the session to confirm it will not be renegotiated.

Click **AnyConnect Client** in the left pane, then clear the **Inherit** check box and enter a value of **1300** (see Figure 3-106).

Note For more information regarding this AnyConnect issue, refer to the following URL:

- http://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116881-technote-anyconnect-00.html

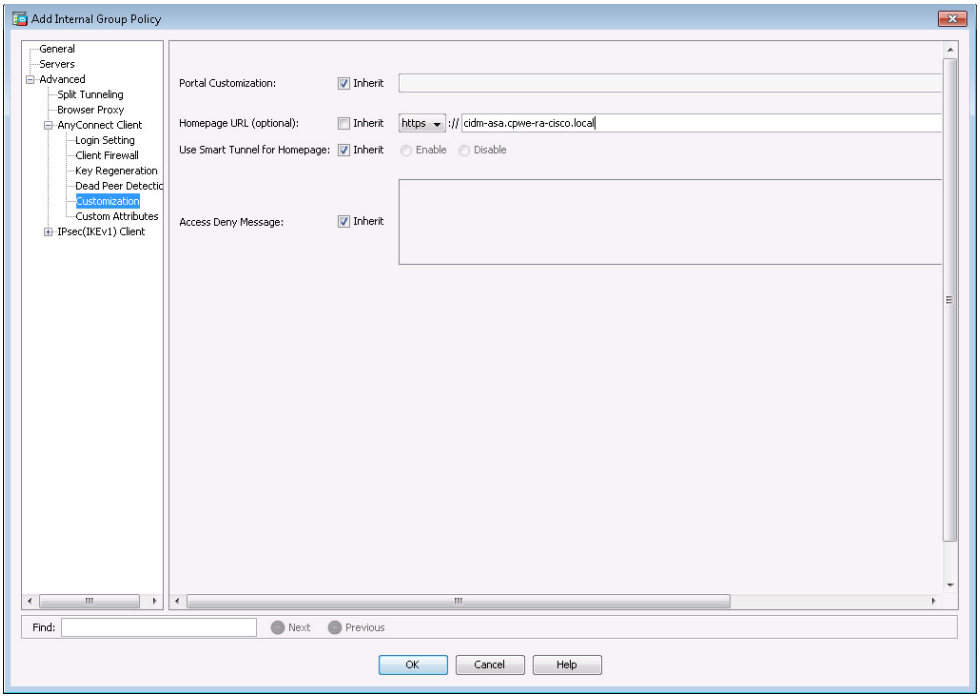
Figure 3-106 AnyConnect VPN Group Policy - MTU



k. If users should have a browser window pop up automatically after login to direct them to the IDMZ ASA web portal (or any other destination), the **Homepage URL** feature should be enabled. Expand **AnyConnect Client under Advanced** in the left pane, and then click **Customization**. For **Homepage URL**, clear the **Inherit** check box and type the URL that should be automatically accessed by the user after login (see Figure 3-107).

l. Click **OK** on the **Add Internal Group Policy** dialog box. In the **Group Policies** pane, click **Apply**.

Figure 3-107 AnyConnect VPN Group Policy - Homepage URL



Step 4 Add local users as a backup AAA option, and then associate the group policy to the connection profile (see Figure 3-108).

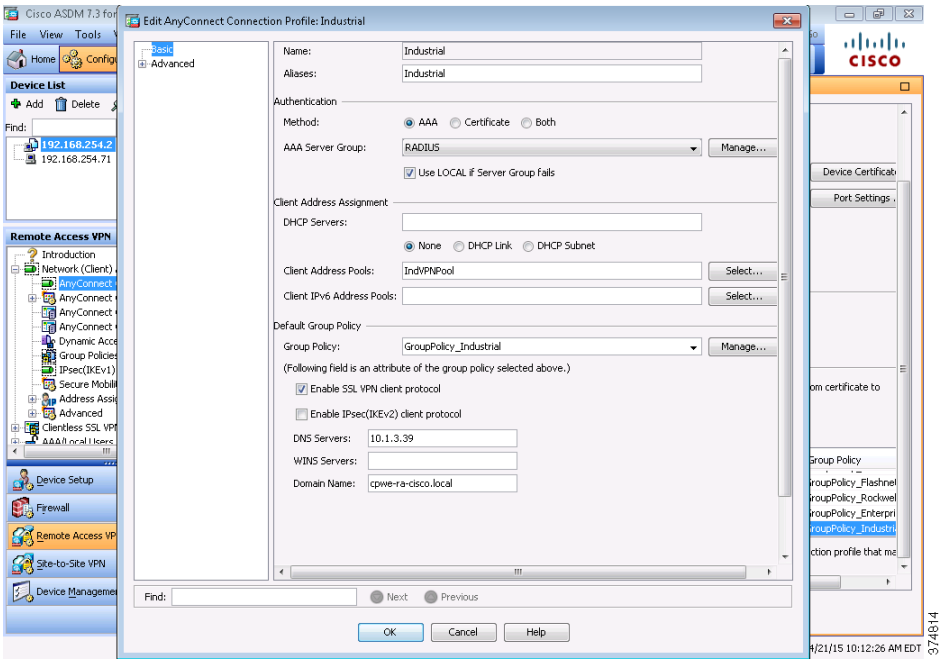
a. Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Click the connection profile created earlier and then click **Edit**.

b. Under the **AAA Server Group** field, confirm that **Use LOCAL if Server Group Fails** is selected. Choosing this setting will allow local administrators to access the VPN even if the connection to the RADIUS server fails.

c. For **Group Policy**, choose the group policy created earlier that should be associated with this connection profile.

d. Click **OK** and then click **Apply** to confirm the changes.

Figure 3-108 AnyConnect Profile - Local Authentication



The equivalent CLI configuration for Steps 1-4 is shown below:

```
ip local pool IndVPNPool 10.255.3.249-10.255.3.252 mask 255.255.255.240
aaa-server RADIUS protocol radius
aaa-server RADIUS (INSIDE) host 10.1.3.48
 key *****
!
access-list Industrial extended permit ip 10.255.3.232 255.255.255.248 any
access-list Industrial extended permit ip 10.255.3.240 255.255.255.240 any
access-list Industrial extended permit ip 10.1.3.0 255.255.255.0 any
access-list Industrial extended permit ip object IDMZ-RDG any
!
webvpn
 enable OUTSIDE
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.05187-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-3.1.05187-k9.pkg 2
 anyconnect image disk0:/anyconnect-linux-64-3.1.05187-k9.pkg 3 regex "Linux"
 anyconnect image disk0:/anyconnect-linux-3.1.05187-k9.pkg 4 regex "Linux"
 anyconnect enable
 tunnel-group-list enable
!
group-policy GroupPolicy_Industrial internal
group-policy GroupPolicy_Industrial attributes
 wins-server none
 dns-server value 10.1.3.39
 vpn-filter value IndVPNFilter
 vpn-tunnel-protocol ssl-client
 group-lock value Industrial
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Industrial
 default-domain value cpwe-ra-cisco.local
 client-bypass-protocol enable
 webvpn
  anyconnect mtu 1300
  homepage value https://cidm-asa.cpwe-ra-cisco.local
  always-on-vpn profile-setting
```

```
!
tunnel-group Industrial type remote-access
tunnel-group Industrial general-attributes
 address-pool IndVPNPool
 authentication-server-group RADIUS LOCAL
 default-group-policy GroupPolicy_Industrial
tunnel-group Industrial webvpn-attributes
 group-alias Industrial enable
```

Clientless SSL VPN Configuration

The following steps describe the configuration of clientless SSL VPN on the IDMZ firewall to allow Web-based access to industrial resources from the Enterprise Zone:

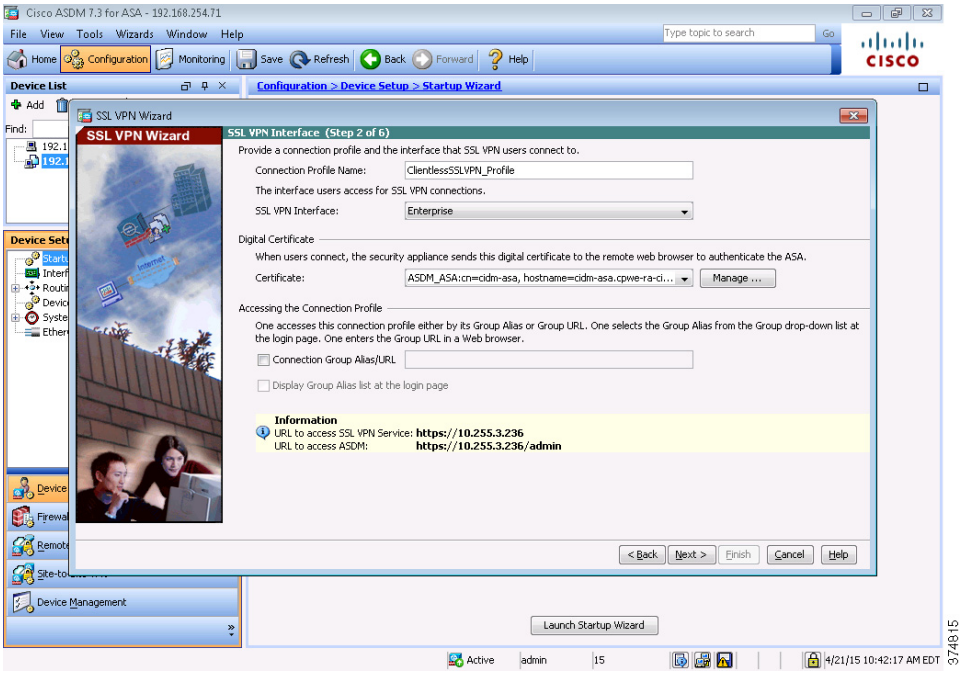
Step 1 Complete the clientless SSL VPN wizard.

a. Navigate to **Wizards > VPN Wizards > Clientless SSL VPN Wizard**. Click **Next**.

b. In the **Connection Profile Name** box, enter any desired name. In the **SSL VPN Interface** list, choose the enterprise-facing connection. Select the ASA's certificate in the **Digital Certificate** box and then click **Next** (see Figure 3-109).

Note The Information box at the bottom of the window indicates the URL that should be used to access the clientless SSL VPN service. If users are automatically directed to the IDMZ VPN portal after connecting to the Enterprise edge firewall, the Homepage URL value in the group policy of the Enterprise firewall should match (or resolve via DNS to) the one shown here.

Figure 3-109 SSL VPN Wizard - Connection Profile

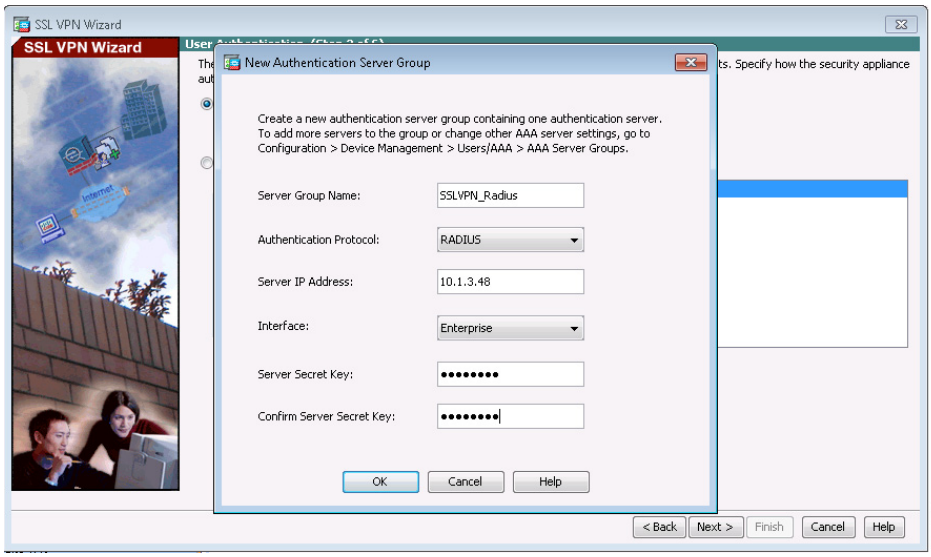


c. Verify that **Authenticate using a AAA server group** is selected, and then click **New**. In the **New Authentication Server Group** dialog box, enter the following values and then click **OK** (see Figure 3-110):

- **Server Group Name**: Any desired name
- **Authentication Protocol**: RADIUS
- **Server IP Address**: IP address of the RADIUS server, for example the Enterprise ISE node
- **Interface**: Enterprise-facing connection
- **Server Secret Key**: Any desired secret key
- **Confirm Server Secret Key**: Repeat secret key

On the **User Authentication** page, click **Next**.

Figure 3-110 SSL VPN Wizard - Authentication Server



d. Verify that **Create New Group Policy** is selected, and then enter any desired name for the group policy. Click **Next**.

e. If bookmarks should be displayed after users log into the SSL VPN portal, click **Manage** next to **Bookmark List**. Click **Add** and then enter a **Bookmark List Name**.

f. Click **Add**, select **URL with GET or POST** method and then click **OK**. Enter an alias for the bookmark in the **Bookmark Title** box.

g. In the **URL** box, select the appropriate protocol from the drop-down list, then enter the desired URL.

- For more complex protocols like RDP, clicking **Assistant** will assist with forming the URL correctly
- If any more advanced options are needed, such as **Smart Tunnel**, select them in the lower part of the dialog box

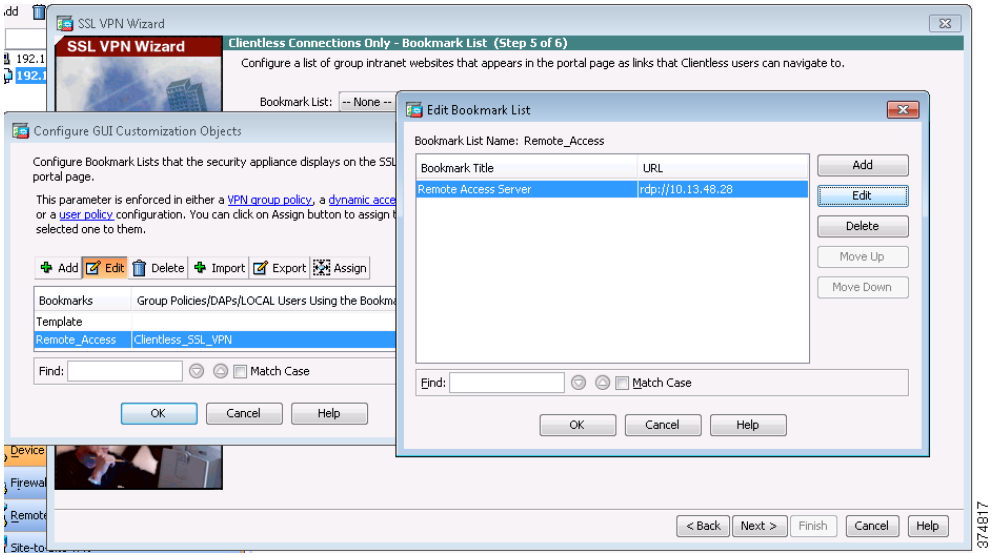
h. Click **OK**, and then repeat the process for any additional bookmarks. Once complete, click **OK**.

i. In the **Configure GUI Customization Objects** dialog box, select the bookmark list and click **Assign**. In the **Assign Bookmarks** dialog box, select the box next to the group policy created earlier and then click **OK**.

j. Finally, click **OK** and verify that the correct bookmark list appears in the drop-down before clicking **Next** (see Figure 3-111).

k. Verify the attributes shown and then click **Finish** to complete the wizard.

Figure 3-111 SSL VPN Wizard - Bookmarks



Step 2 Configure the Clientless SSL VPN group policy:

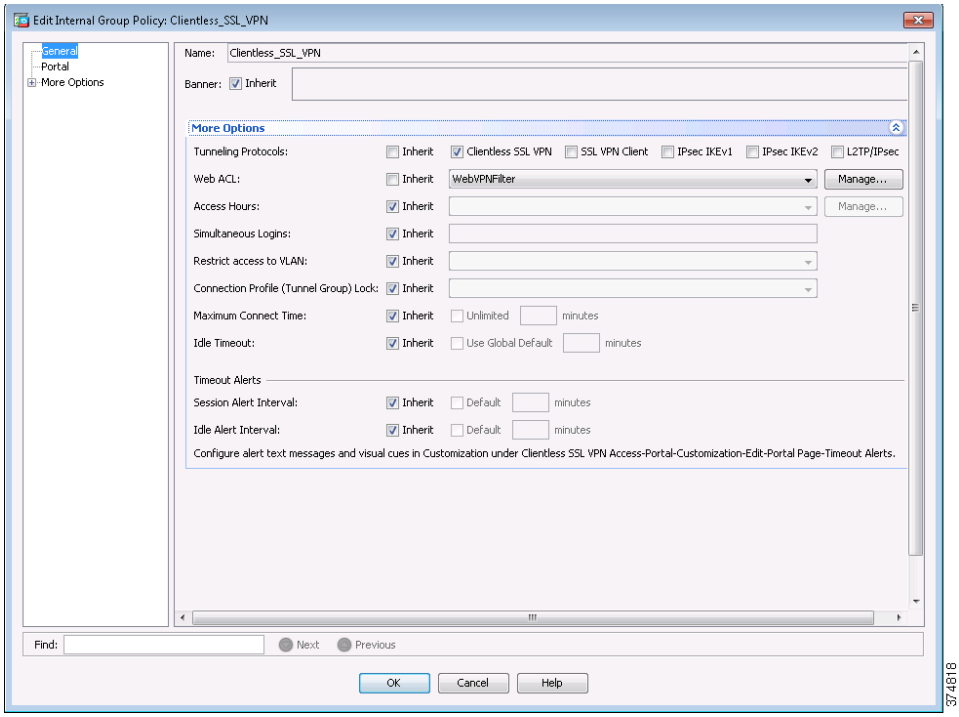
a. Go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**. Select the group policy created earlier and click **Edit** (see Figure 3-112). Expand the **More Options** pane.

b. For T**unneling Protocols**, clear the **Inherit** check box, and then clear all check boxes except for **Clientless SSL VPN**.

c. For **Web ACL**, clear the **Inherit** check box, and then click **Manage**. On the **ACL Manager** dialog box, configure the ACL for the URLs that the user is allowed to access (for example, the Remote Access Server via RDP). Once complete, click **OK**.

d. In the **Edit Internal Group Policy** dialog box, click **OK**. In the **Group Policies** pane, click **Apply**.

Figure 3-112 Clientless SSL VPN Group Policy



Note If the user will be creating RDP sessions via the SSL VPN portal, then set up the ASA RDP plug-in. For this procedure, refer to ASA RDP Plug-In Configuration, page 3-72.

The equivalent CLI configuration for Steps 1-2 is shown below:

```
access-list WebVPNFilter webtype permit url rdp://10.13.48.28/*
aaa-server RADIUS (Enterprise) host 10.1.3.48
 key *****
webvpn
 enable Enterprise
group-policy Clientless_SSL_VPN internal
group-policy Clientless_SSL_VPN attributes
 vpn-tunnel-protocol ssl-clientless
 default-domain value cpwe-ra-cisco.local
 webvpn
  url-list value Remote_Access
  filter value WebVPNFilter
  always-on-vpn profile-setting
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group RADIUS
 default-group-policy Clientless_SSL_VPN
```

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 the following URL:

- https://technet.microsoft.com/en-us/library/dd983941%28v=ws.10%29.aspx

Defining User Groups and Remote Access Rules

In our scenario, we have the following actors shown in Table 3-21that will be assigned to the following Active Directory User Groups:

Table 3-21 Users and User Groups

User	User Group	Role
Oscar Operator	Operators	Monitors production equipment to support the IACS process
Matt 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
Al Admin	Production Administrators	Defines, configures, maintains Industrial Zone software assets that contain common enterprise software such as Antivirus, OS patches, etc.
Joe 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. In our simple example, the rules shown in Table 3-22 will be implemented on the RD Gateway to allow access from the Enterprise Zone to the Industrial Zone.

Table 3-22 User Groups Authorization

User Group	Industrial Zone Access
Operator	None
Maintenance	Terminal Server
Engineer	FactoryTalk Directory (FTDIRECTORY) Production Database (PRODDATA) Production Engineering Workstation (PRODEWS) Production File Server (PRODFS) Industrial Zone Historian (PRODHIST) Production Mfg. Intelligence Server (PRODMIS) Production Operator Workstation (PRODOWS) Production SQL Server (PRODSQL) Production VantagePoint Server (PRODVP) FactoryTalk ViewSE Server (VIEWSE)
Production Administrator	FactoryTalk Directory (FTDIRECTORY) Production Database (PRODDATA) Production Engineering Workstation (PRODEWS) Production File Server (PRODFS) Industrial Zone Historian (PRODHIST) Production Mfg. Intelligence Server (PRODMIS) Production Operator Workstation (PRODOWS) Production SQL Server (PRODSQL) Production VantagePoint Server (PRODVP) FactoryTalk ViewSE Server (VIEWSE)
OEM 1	Terminal Server
OEM 2	Terminal Server

It's also possible to leverage the ability to organize computer resources into groups so administration is easier. In our example, we will create two computer groups (see Table 3-23) to help us manage terminal servers and IACS servers.

Table 3-23 AD Computer Groups

Computer Group	Industrial Zone Asset(s)
IDMZ RD Gateway Remote Hosts	Terminal Server 01 (TERM01)
IACS Hosts	FactoryTalk Directory (FTDIRECTORY) Production Database (PRODDATA) Production Engineering Workstation (PRODEWS) Production File Server (PRODFS) Industrial Zone Historian (PRODHIST) Production Mfg. Intelligence Server (PRODMIS) Production Operator Workstation (PRODOWS) Production SQL Server (PRODSQL) Production VantagePoint Server (PRODVP) FactoryTalk ViewSE Server (VIEWSE)

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, please refer to *Active Directory Users and Computers* at the following URL:

- https://technet.microsoft.com/en-us/library/cc754217.aspx

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 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 3-23.

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 3-23. 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.

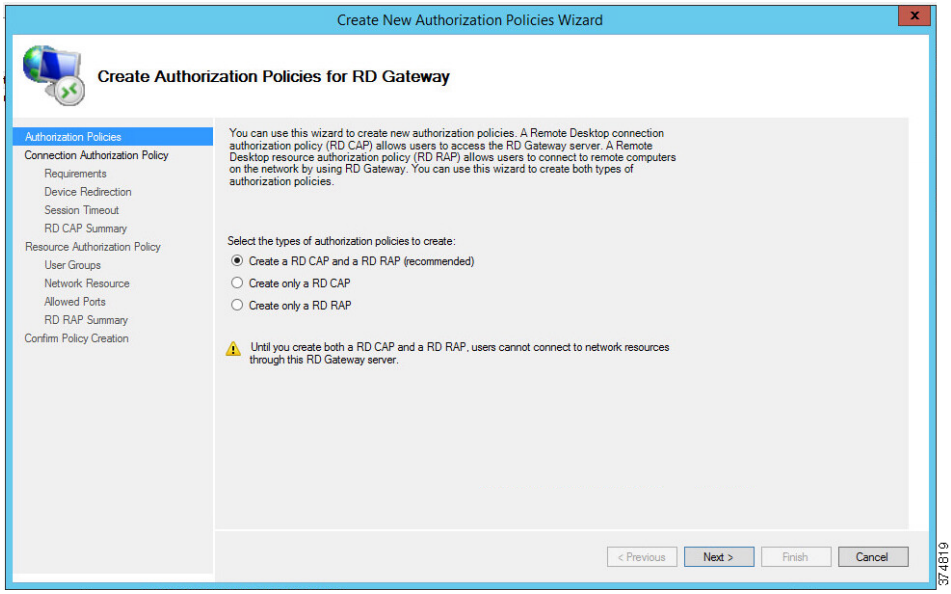
In our example, we will configure two CAPs and RAPs to support the scenario in Table 3-21.

- 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.

a. From the **RDG Manager**, the **Policies** folder and select **Create New Authorization Policies**. In the dialog box (see Figure 3-113), select **Create RD CAP** and a **RD RAP** (recommended) and then click **Next**.

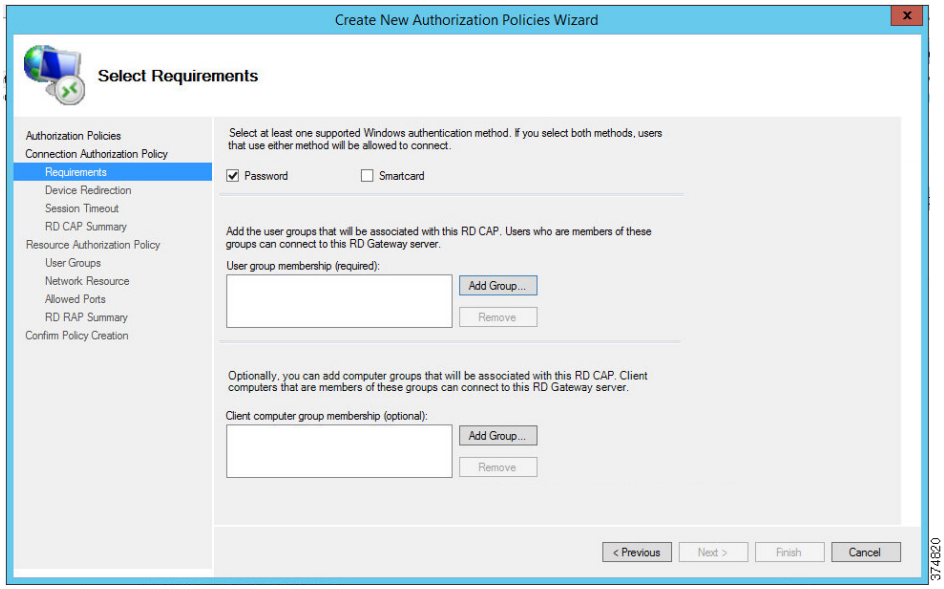
Figure 3-113 RDG Policy Wizard



b. Name the CAP as **IDMZ RDG CAP** and then click **Next** to proceed to the Requirements page.

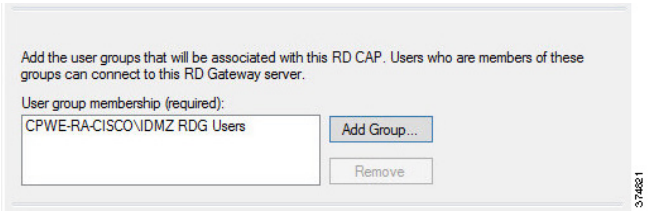
c. Each CAP allows the administrator to select a Password, a Smartcard or both as an authentication method. In our example, we are allowing the user to use a password (see Figure 3-114).

Figure 3-114 CAP Requirements - Authentication Method



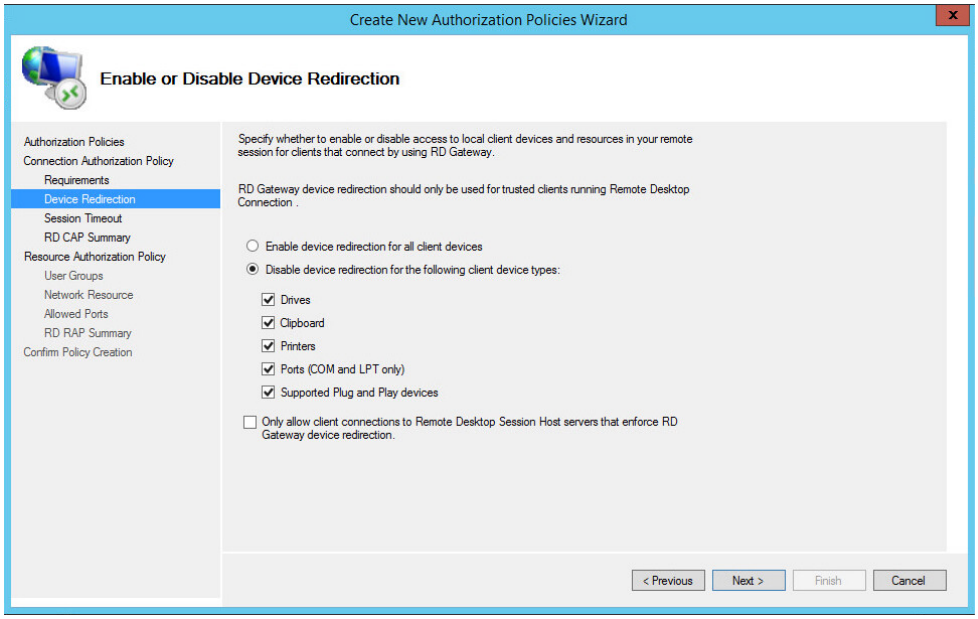
d. With the Password option selected, we will now add user groups that will be associated with this CAP. Click **Add Group** in the **User Group Membership** section. In the **Selection Group** dialog box, find and select **IDMZ RDG Users** group to associate it with the RDG CAP (see Figure 3-115). Click **Next**.

Figure 3-115 CAP Requirements - User Group



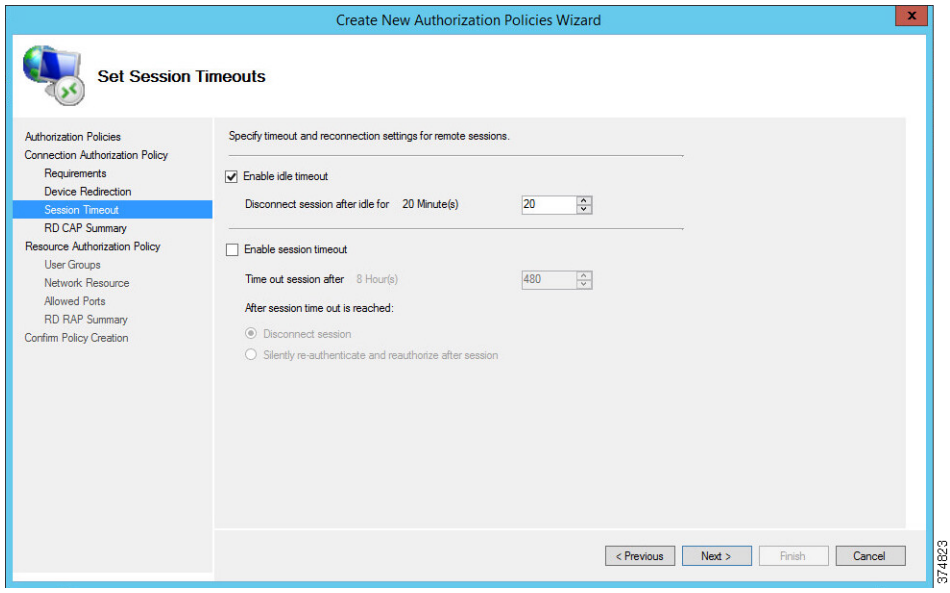
e. The CAP also allows the administrator to enable or disable device redirection. Device redirection controls access to devices and resources on a client computer in RDP sessions. For instance, Drives redirection specifies whether to prevent the mapping of client drives in an RDP session. For our example, we will disable device redirection to bolster security (see Figure 3-116). After disabling device redirection, click **Next** to continue.

Figure 3-116 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 3-117 CAP - Idle and Session Timeouts



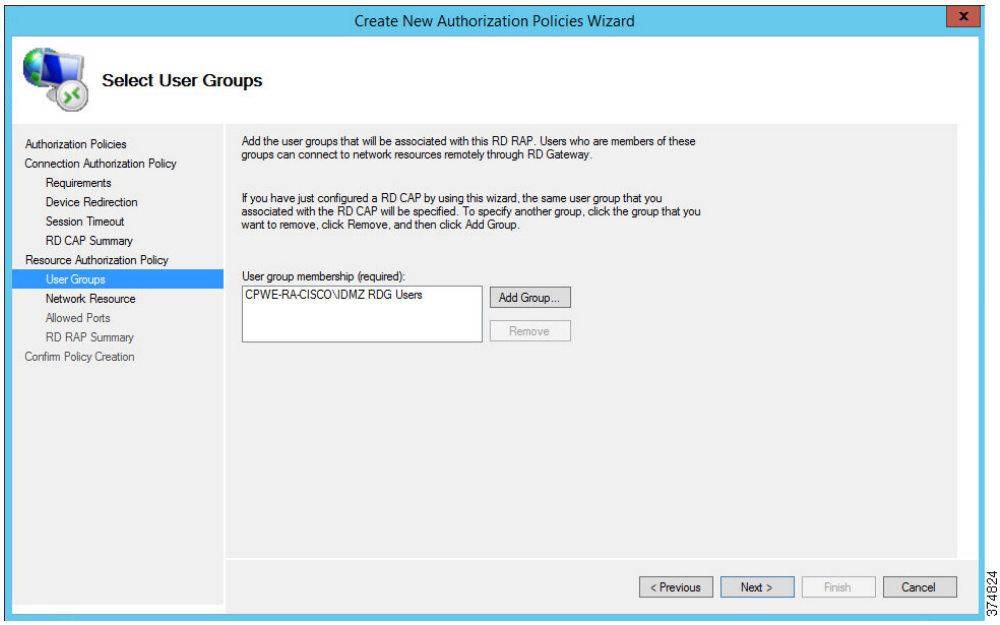
g. Once the CAP configuration steps are completed, the administrator can review the entire details of the configuration before submitting the content.

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 3-118). This group will be allowed to access the terminal server in the next step. Click **Next** to continue.

Figure 3-118 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 3-119 and Figure 3-120).

Figure 3-119 RAP - Network Resources

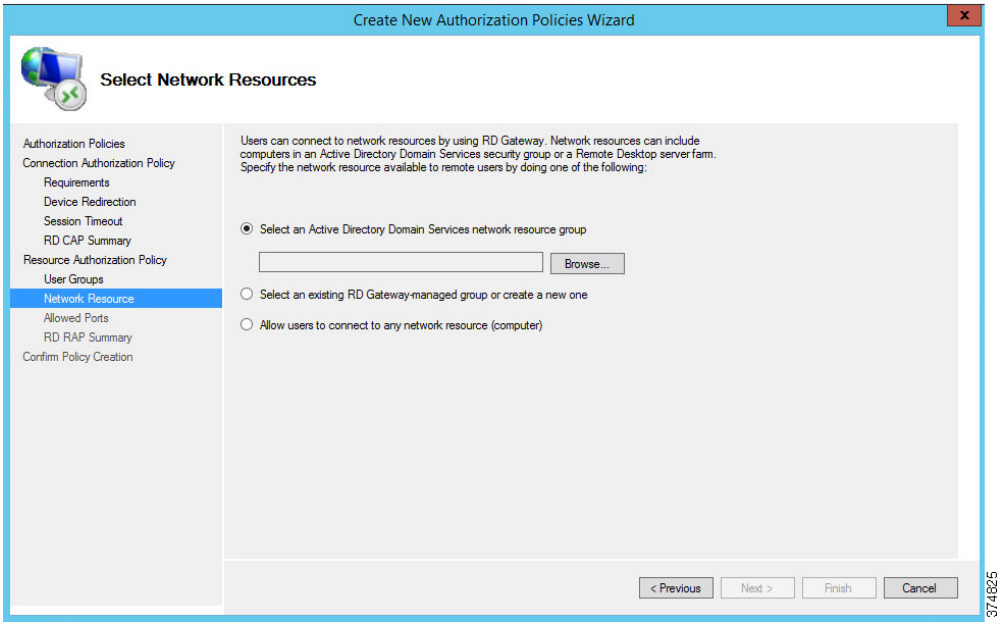
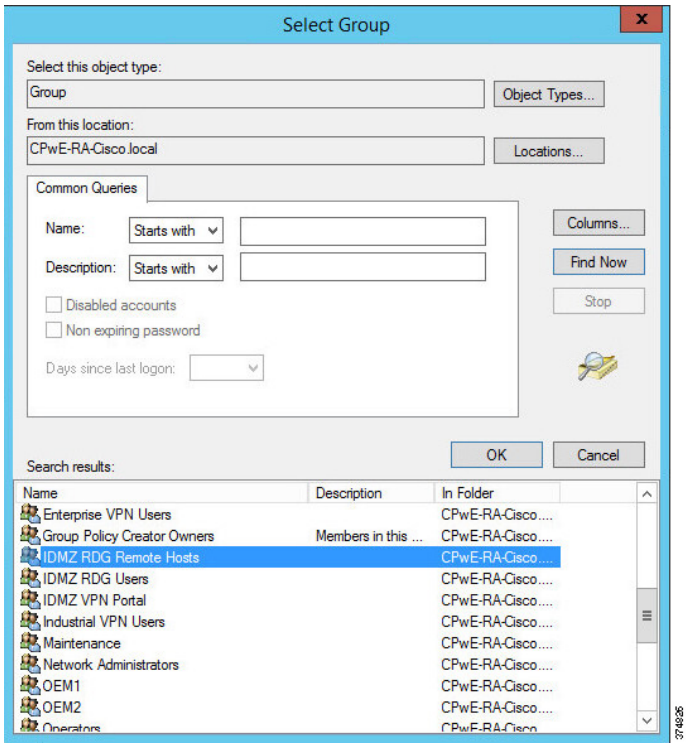
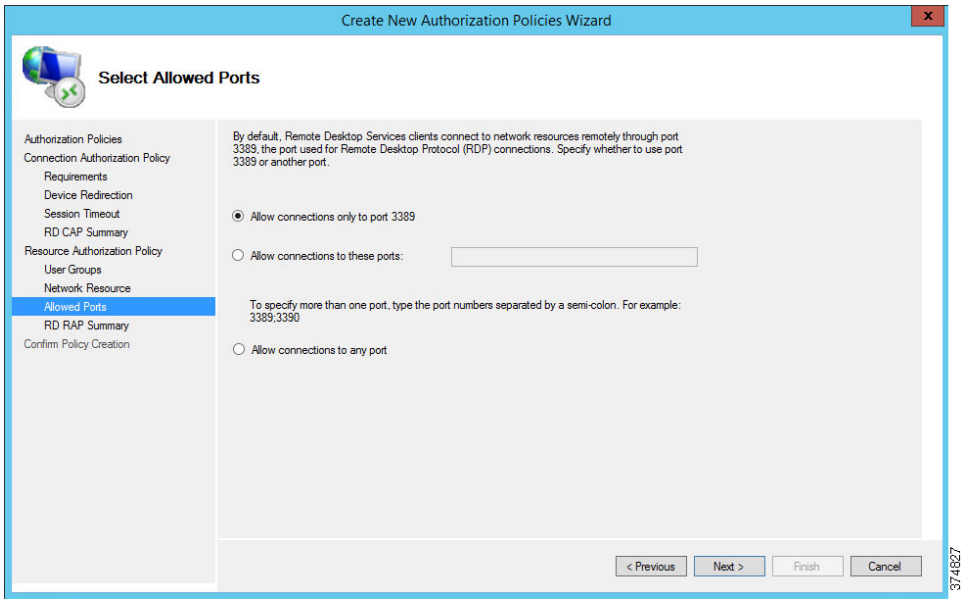


Figure 3-120 RDG Remote Hosts Computer Group



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 3-121). If a different port or group of ports is selected, make sure that the firewall rules reflect that. Click **Next**.

Figure 3-121 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.

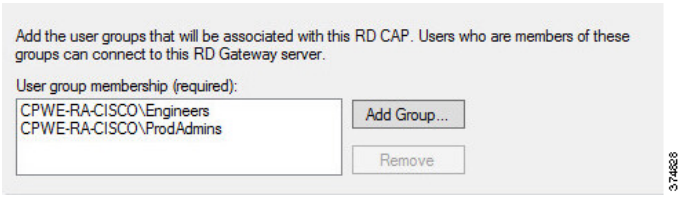
Step 3 Configure IACS Remote Host CAP using the RD Gateway Manager. The IACS Remote Host scenario will allow the production administrators and engineers to access the Industrial Zone servers in the IACS Hosts group (Table 19). Configuration of this CAP is similar to Step 1.

a. Start the wizard to create a new CAP and a RAP. In our example, the CAP will be named **RDG IACS Remote Hosts CAP**.

b. Select the authentication method (password or smartcard) depending on the security policy.

c. Add user groups that will be associated with this CAP. In our example, **Engineers and ProdAdmins** groups will be selected.

Figure 3-122 Remote Host CAP User Groups



d. 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.

e. Specify idle and session timeout parameters.

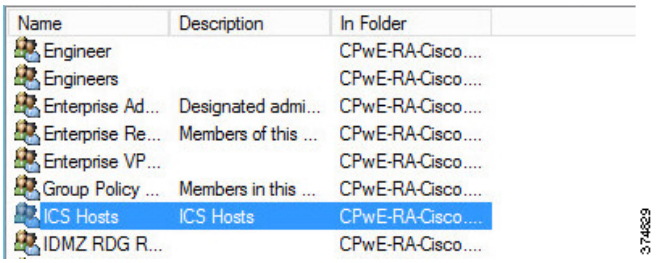
Step 4 Configure IACS Remote Host RAP using the RDG Manager after the CAP is created. Configuration of this CAP is similar to Step 2.

a. Name the policy (**RDG IACS Remote Hosts RAP** is used in our example).

b. 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.

c. 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 3-123 ICS Hosts Computer Group



d. 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. This CVD 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 document.

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 3-24).

Table 3-24 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 accessible via RDG, for example RAS	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.

The access rules can be applied using Cisco ASA web interface (see Figure 3-47 on page 3-15 as an example). The equivalent CLI configuration for Step 2 is shown below:

```
access-list Enterprise_access_in extended permit tcp any object RDG eq https
access-list IDMZ-RDG_access_in extended permit object rdp object RDG object RAS
```

ASA RDP Plug-In Configuration

The following steps describe the configuration of the ASA RDP plug-in to enable RDP sessions via the SSL VPN portal:

Step 1 Complete the initial RDP plug-in installation by downloading the plug-in file from Cisco and following the setup procedure found at the following URL:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm/webvpn-configure-gateway.html

Step 2 To allow Java to launch the RDP plug-in with the recommended security settings, the client will need to add the SSL VPN portal URL to their site exceptions list:

a. On the client PC, select **Start > All Programs > Java > Configure Java**.

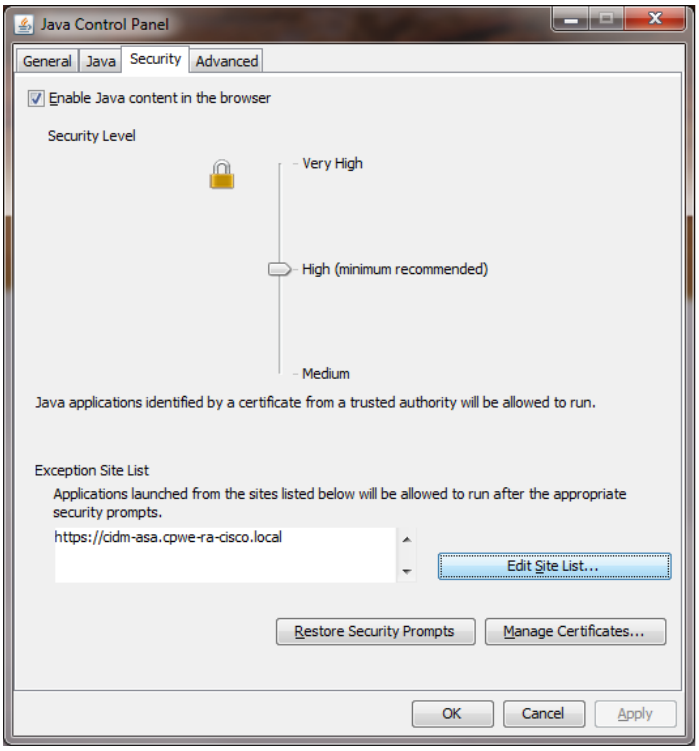
b. Select the **Security** tab and then click **Edit Site List** (see Figure 3-124).

c. Click **Add**, and then enter the full portal URL under **Location**. Click **OK**.

d. Click **OK** to apply the settings and close the **Configure Java** window.

Note This procedure was verified with Java SE Version 7, Update 67.

Figure 3-124 Java Security Settings for RDP Portal



Step 3 Configure RDP bookmarks for preconfigured RDP sessions to the terminal servers in the Industrial Zone. The bookmarks use a URL to pass configuration parameters to the plugin. The portal may need to have multiple bookmarks to the same terminal server with different options such as screen resolution. See Table 3-25.

An example URL may look like this: *rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value*

Table 3-25 RDP Bookmark Parameters

Parameter Name	Description	Options
Geometry	Size of the client screen in pixels	W x H
bpp	Bits-per-pixel (color depth)	8|16|24|32
Domain	Login domain	
Username	Login username	
Password	Login password: Use the password with care, because it is used at the client-side and can be observed.	
Console	This is used in order to connect to the console session on the server	Yes/No
Force Java	Set this parameter to "Yes" in order to use only the Java Client. The default setting is "No."	Yes/No
Shell	Set this parameter to the path of the executable/application that is started automatically when you connect with RDP (rdp://server/?shell=path, for example)	

Note Most of the connection parameters are optional. However, it is important to set the Force Java parameter to "Yes." This prevents the client from attempting to load the ActiveX version of the plug-in which was not validated in this design.

Step 4 Configure Web ACLs to limit portal access to specific sites in the Industrial Zone. Web ACLs allow the firewall to restrict which URLs are accessible from the VPN portal. The ACLs allow for the use of wildcards matching multiple URLs in one ACE. Like all ACLs, an implicit deny all exists that is enforced when the ACL is applied.

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 3-26 for users of Studio 5000® software:

Table 3-26 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.

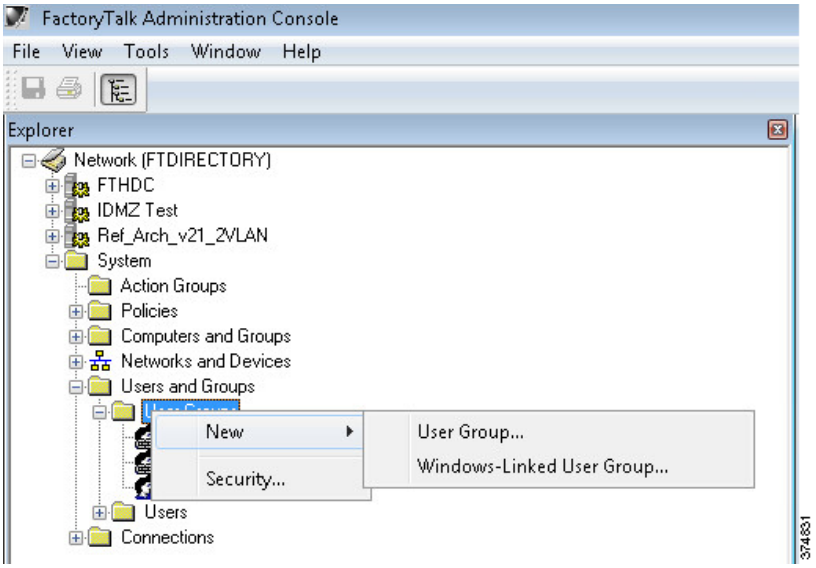
In our example, we are going to add the Windows users groups Operators, Engineers, Maintenance, Production Administrators, OEM1 and OEM2 (Table 22).

Step 1 Add Windows-linked users groups to the FactoryTalk Network Directory.

a. Open the FactoryTalk Administration Console: **Start > All Programs > Rockwell Software > FactoryTalk Administration Console** and then log on to the **FactoryTalk Network Directory**.

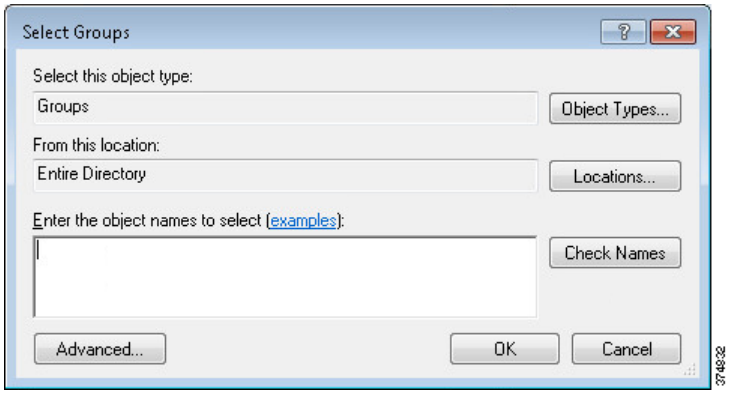
b. Right-click **User Groups** and select **Windows Linked User Group** (see Figure 3-125).

Figure 3-125 FactoryTalk Administration Console - Add User Group



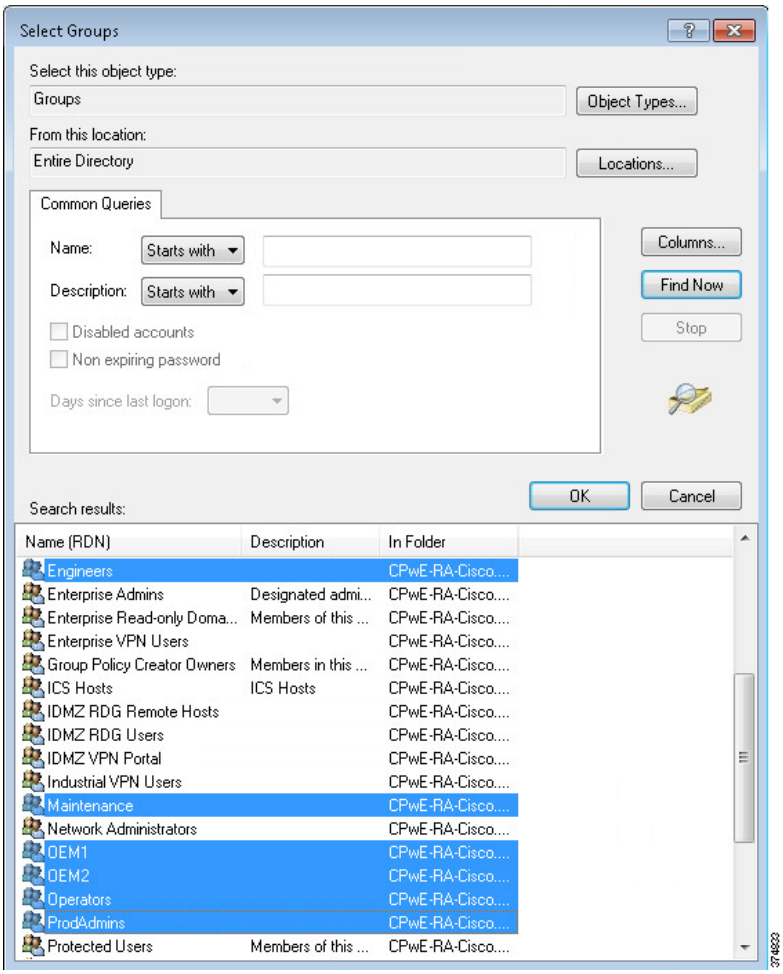
c. In the New Windows Linked User Group dialog box, click **Add > Locations > Entire Directory > OK**. The **Select Groups** dialog box will reappear with the **From this location** field changed from the local computer name to the entire directory (see Figure 3-126).

Figure 3-126 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 3-127). Click **OK**.

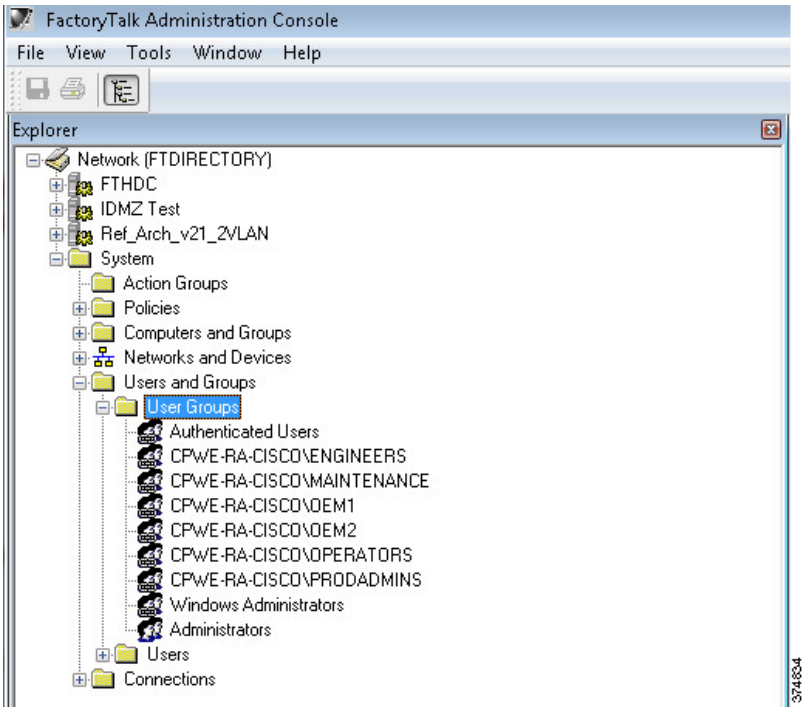
Figure 3-127 Select Groups - Advanced



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 3-128 FactoryTalk Administration Console - User Groups Created



Studio 5000 Product Policies Configuration

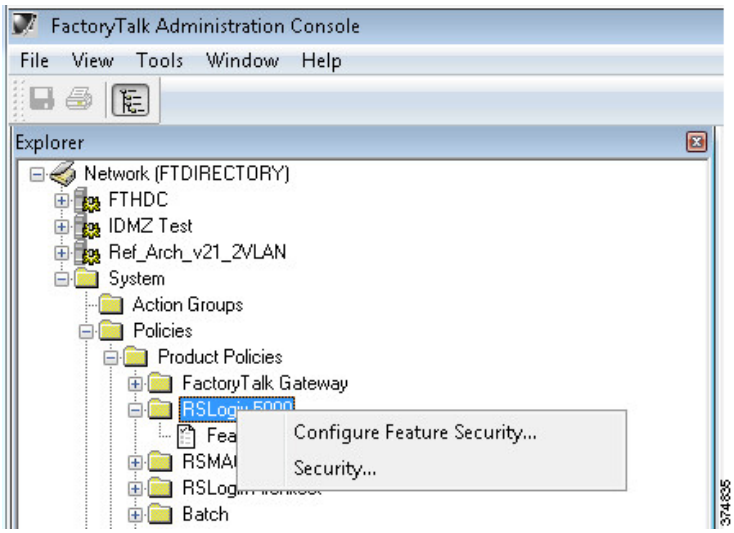
FactoryTalk Security allows the security administrator fine granularity of actions that can be secured for Studio 5000, FactoryTalk View SE and other Rockwell Automation products. In our example, we will start by configuring the Studio 5000 product policies, in particular who can secure and unsecure 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 3-22 on page 3-63.

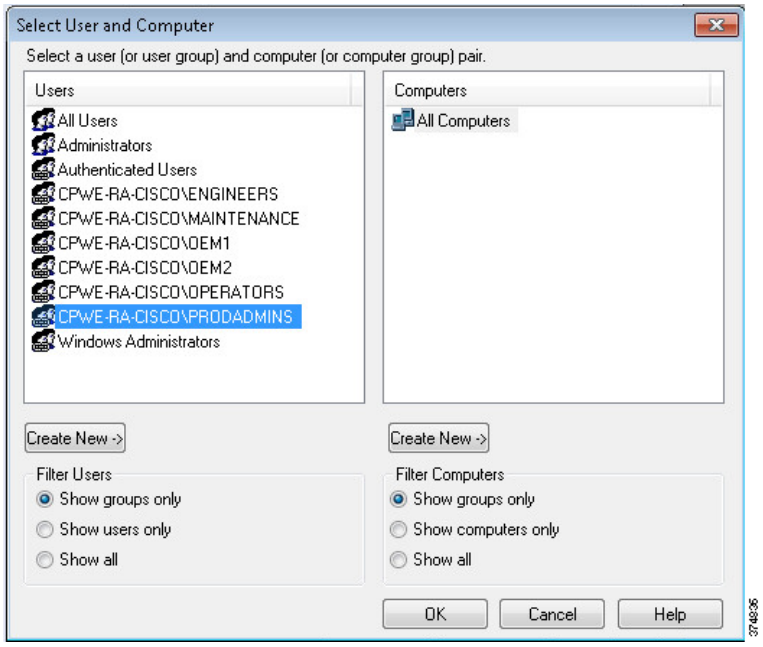
a. Under **System > Policies > Product Policies**, right-click **RSLogix 5000** and select **Configure Feature Security** (see Figure 3-129).

Figure 3-129 FactoryTalk Administration Console - Product Policies



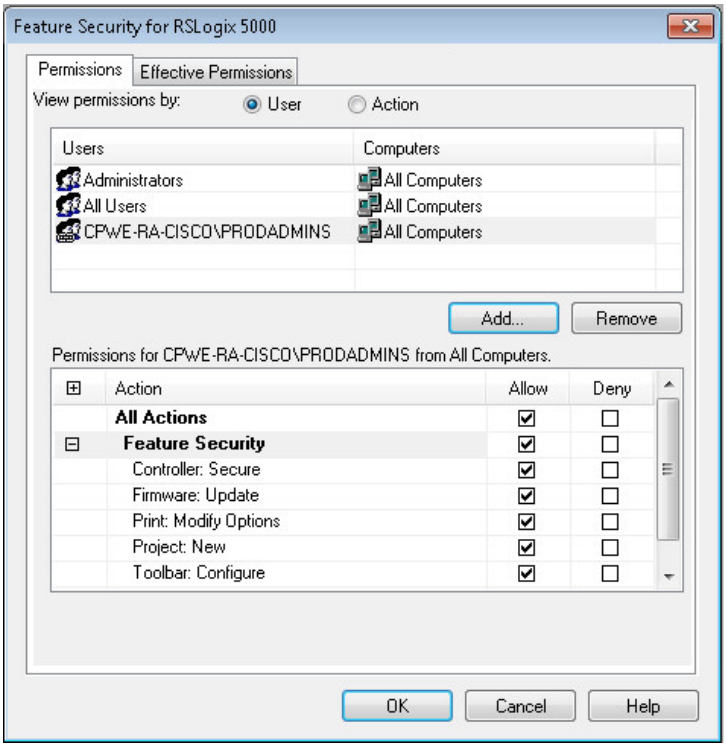
b. First we need to add the User Groups and then assign permissions. On the **Feature Security** dialog box, select **Add** to display the list of available user groups. Remember that we have added Windows-linked users in a previous step so they will be included in the list of users. Select **PRODADMINS** and click **OK** (see Figure 3-130).

Figure 3-130 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 3-131).

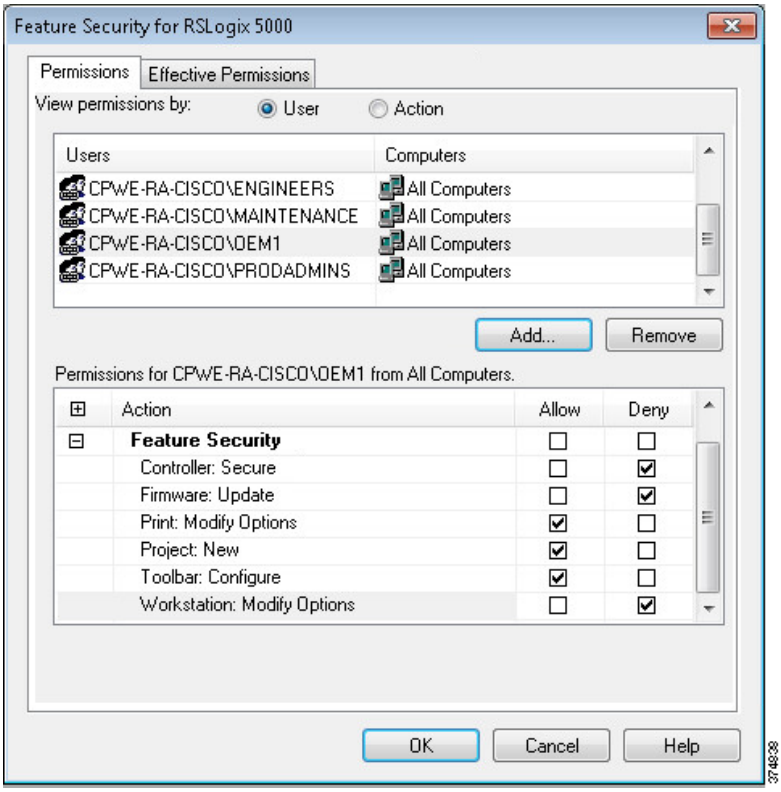
Figure 3-131 Feature Security - Allow All



d. Repeat the same step for each user group according to Table 3-22 on page 3-63. 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 3-132).

Figure 3-132 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

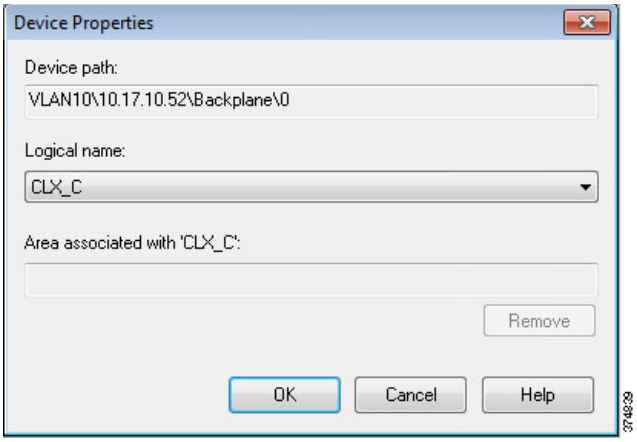
Now that we have created FactoryTalk user groups and assigned Studio 5000 product policies, it is time to set the granular security permissions for each group specific to a controller. Actions such as Tag: Force or Tag: Create can be secured through FactoryTalk Security.

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 3-133 Controller Properties - Logical Name



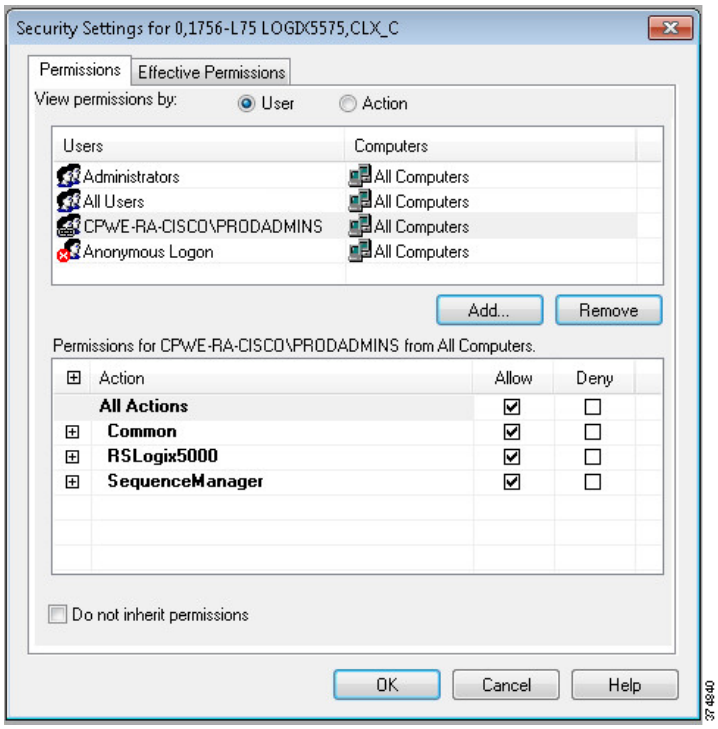
Step 2 **Assign Studio 5000 permissions to the controller based on the user group**. In our example, we will assign all Studio 5000 permissions on the CLX_C controller to the Production Administrators group (PRODADMIN) while setting a Deny permission to the Tag: Force to the OEM1 group.

a. 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**.

b. 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 (PRODADMINS)** user group.

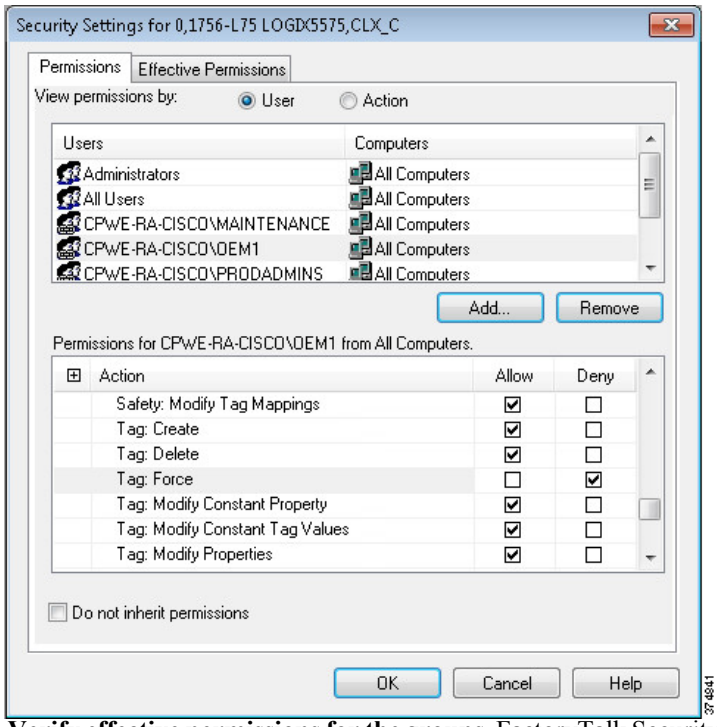
c. The **Security Settings** screen will now show the PRODADMINS group. We want to allow all actions to the CLX_C controller for this group so select **Allow** in the **All Actions** row (see Figure 3-134).

Figure 3-134 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 3-135).

Figure 3-135 Controller Permissions - Deny

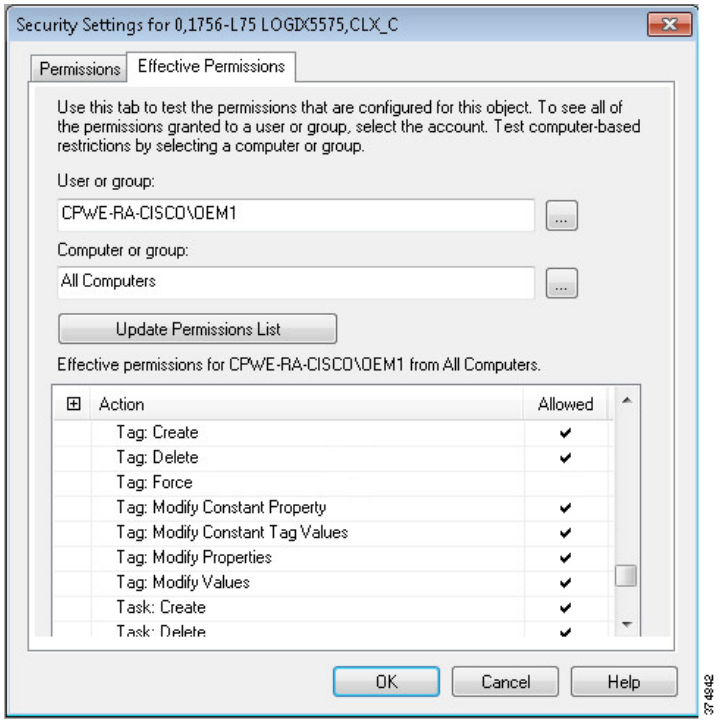


Step 3 **Verify effective permissions for the groups**. FactoryTalk Security is very flexible and allows users and user groups to inherit security permissions. Because of this flexibility, tools exist to check the effective permission for each user, user group and device. In this step, we will check 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 3-136).

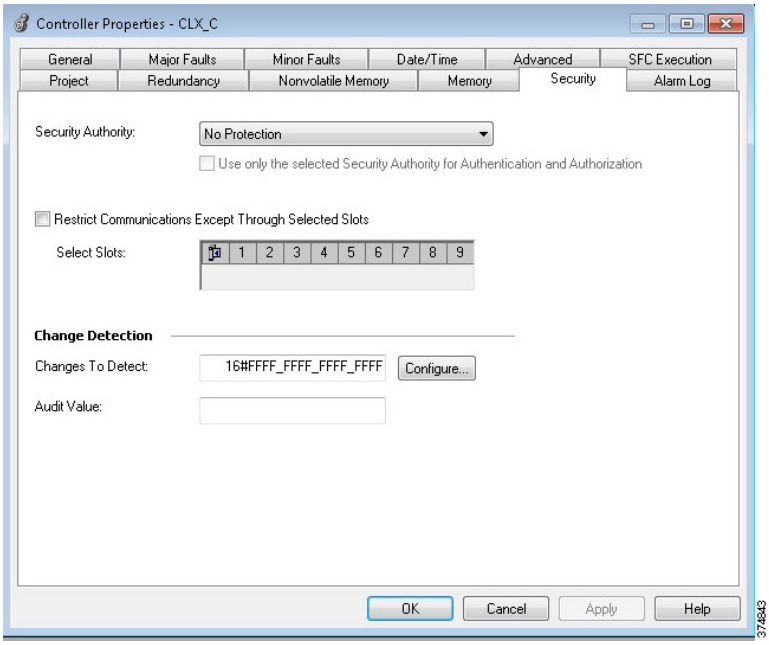
Figure 3-136 Controller Security - Effective Permissions



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

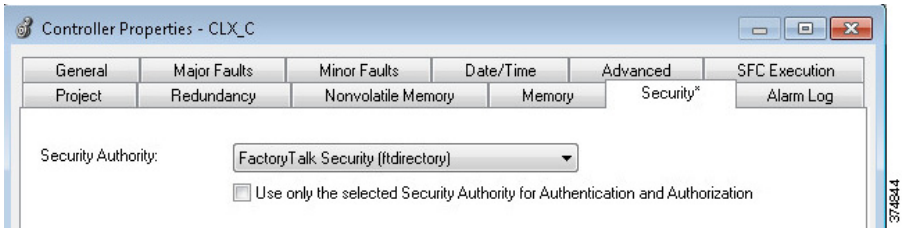
a. Open the CLX_C project with Studio 5000. Right-click the **Controller** folder and select **Properties**. Within the Controller Properties screen, select the **Security** tab. You will notice that the **Security Authority** will be set to **No Protection** (see Figure 3-137).

Figure 3-137 Controller Properties - No Protection



b. Change the Security Authority option to **FactoryTalk Security** (see Figure 3-138) and click **OK**. The Logix Designer warning dialog box is displayed. Select **Yes** to secure the controller.

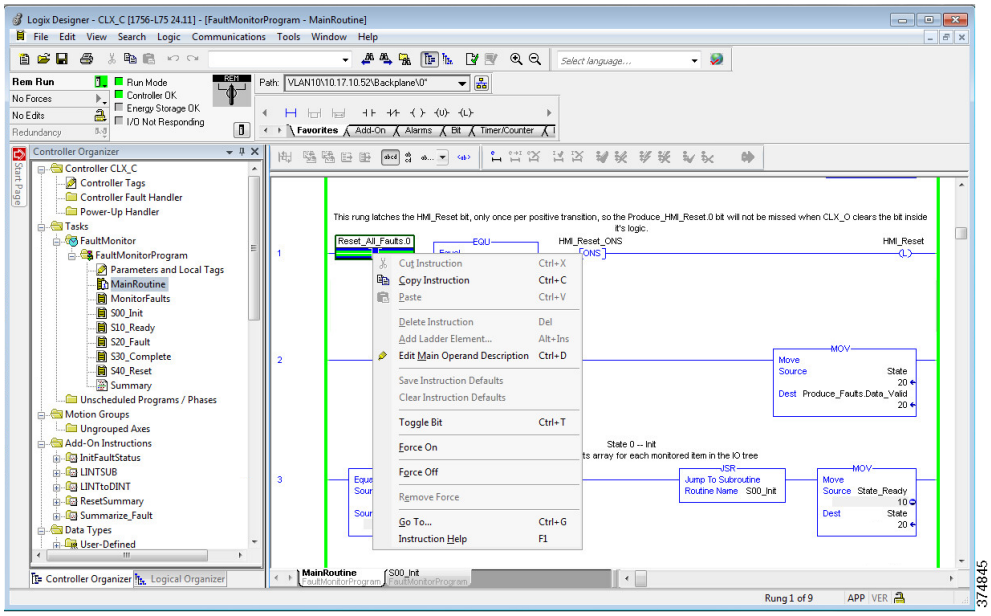
Figure 3-138 Controller Properties - FactoryTalk Security



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

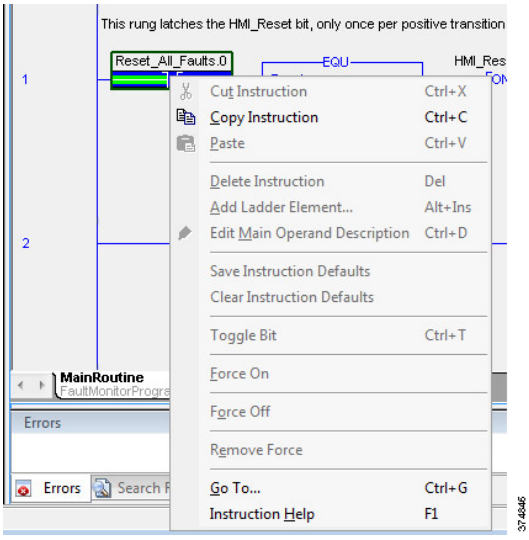
a. Log onto FactoryTalk Security as a **Production Administrator**. In the Studio 5000, when online with the controller. Right-click the tag. The Force On and Force Off actions are available for a tag (see Figure 3-139).

Figure 3-139 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 3-140).

Figure 3-140 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 2-63.

Microsoft EMET Configuration

Rockwell Automation has tested EMET to work with several Rockwell Automation Software products and has compiled an .xml file to allow customers to import a pre-configured Rockwell Automation EMET Package.

Note The EMT configuration can be downloaded from the knowledgebase article at the following URL:

- https://rockwellautomation.custhelp.com/app/answers/detail/a_id/546988

Note Before continuing, please be aware that some security mitigation technologies may break some applications. It is important to thoroughly test EMET in all target use scenarios before rolling it out to a production environment.

The high level steps of setting up EMET with the Rockwell Automation protection profile are listed below:

Step 1 Install Microsoft EMET.

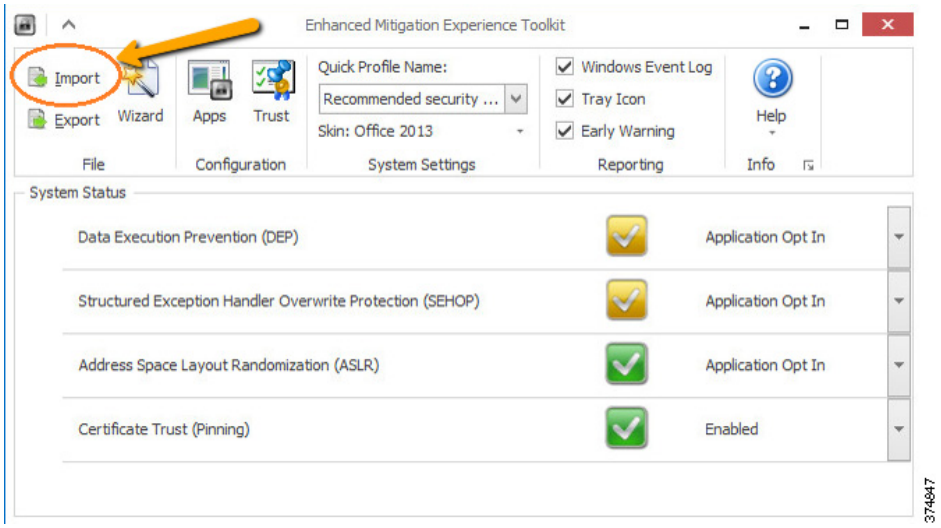
Note For download and installation instructions, refer to the following URL:

- http://support.microsoft.com/kb/2458544

Step 2 Download the latest .xml protection profile and copy it to the EMET Protection Profiles Directory.

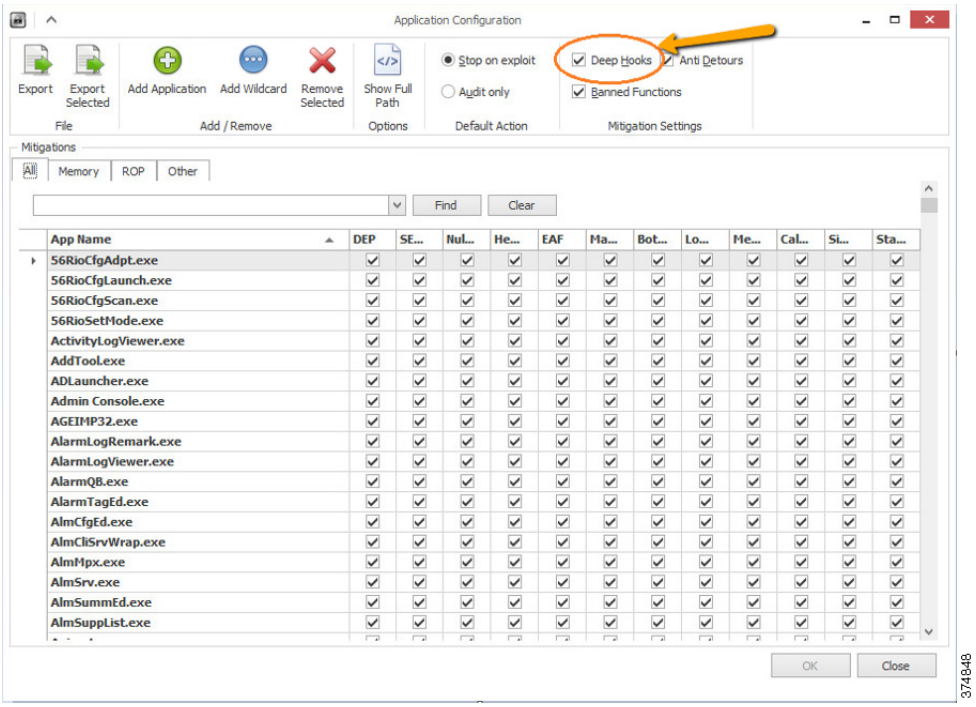
Step 3 Open the EMET GUI and import the downloaded .xml protection profile (see Figure 3-141).

Figure 3-141 EMET - Import Protection Policy



Step 4 In the Application configuration of EMET, enable **Deep Hooks** (see Figure 3-142).

Figure 3-142 EMET - Enable Deep Hooks



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 the following URL:

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

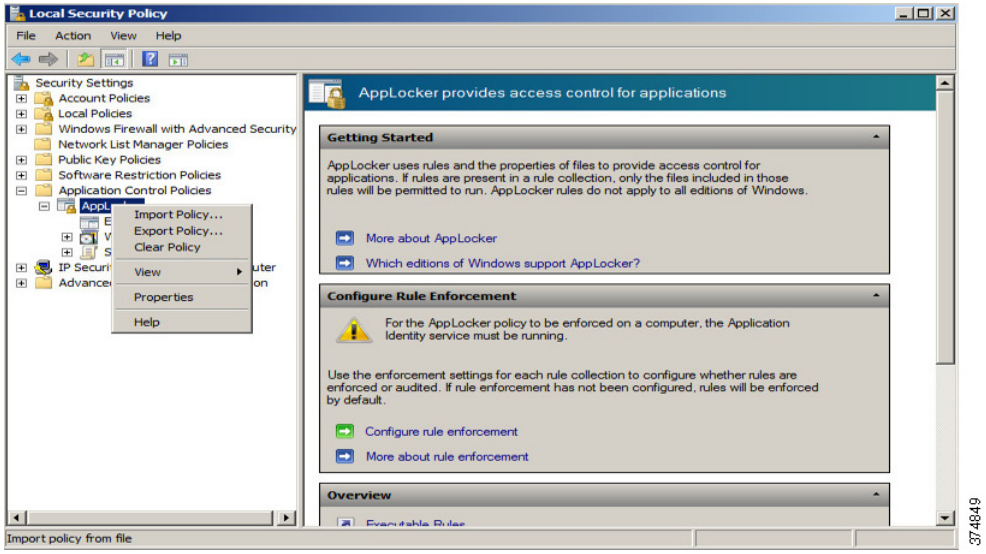
Note Before continuing, it is suggested to use audit-only mode to deploy the policy and understand its impact before enforcing it and rolling it out to a production environment.

Step 1 Import the Rockwell Automation example policy.

a. Open the **Local Group Policy Editor** by going to **Start > Run** and entering **gpedit.msc**.

b. Navigate to **Application Control Policies > AppLocker**. Right-click **AppLocker** and select **Import Policy** (see Figure 3-143).

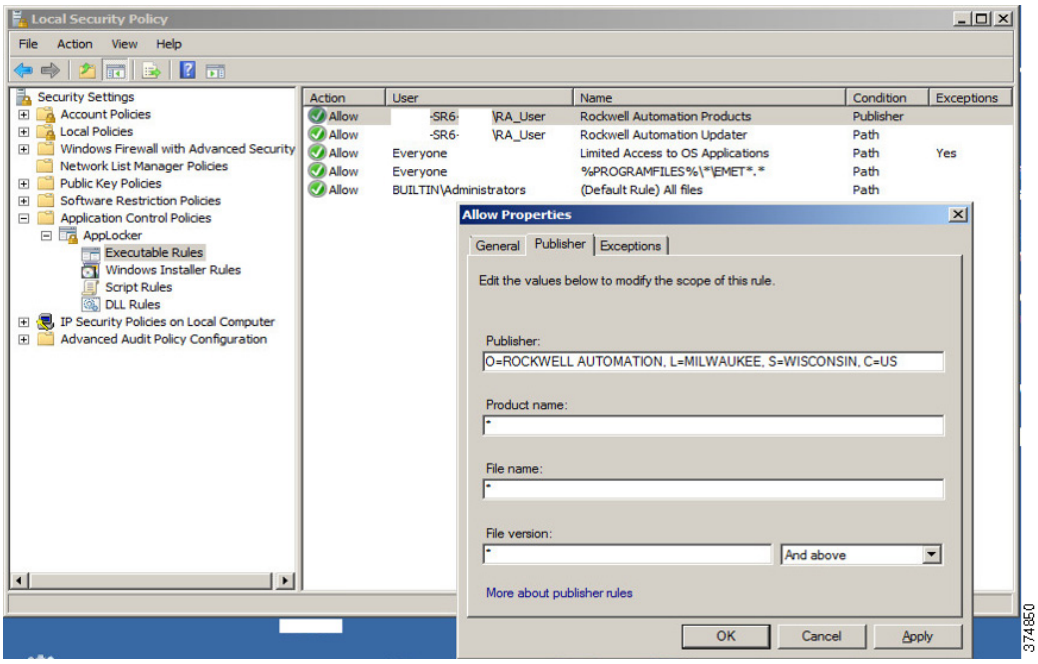
Figure 3-143 Group Policy Editor - Import AppLocker Example Policy



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 3-144).

Figure 3-144 Group Policy Editor - AppLocker Policy Details



CHAPTER 4

CPwE IDMZ Troubleshooting

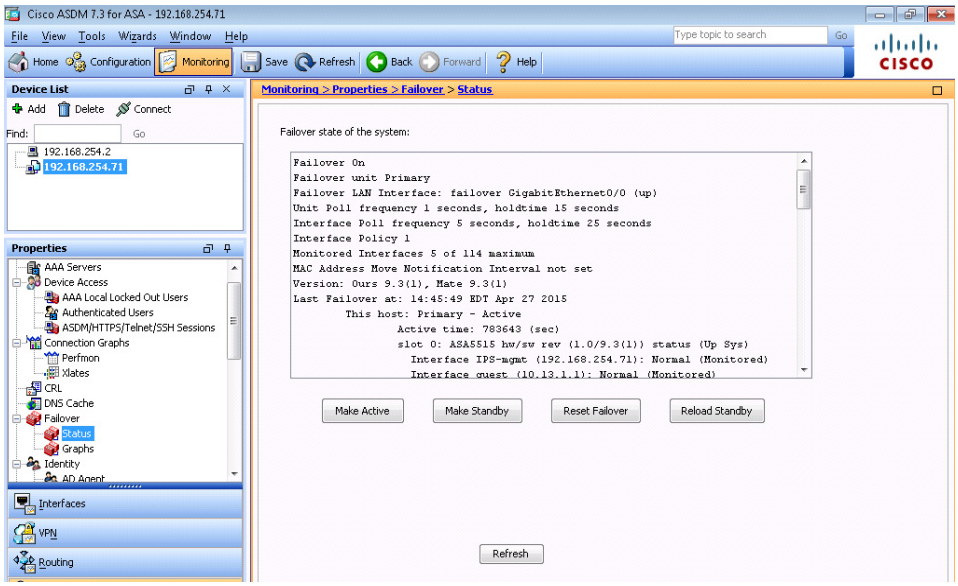
This chapter includes the following major topics:

ASA Failover Troubleshooting

This section provides information on troubleshooting failover status for an active/standby ASA pair.

Figure 4-145 shows Cisco Adaptive Security Device Manager (ASDM) page that provides basic failover status information and the ability to initiate failover operations (**Monitoring > Properties > Failover > Status**):

Figure 4-145 ASA Failover Status



The text box shows the current output of the show failover CLI command. More details about this output are provided later in this section.

In addition, the buttons below the text box allow the user to initiate any of the four available failover operations:

- **Make Active**—If the current unit is in the standby mode, trigger a failover to make the current unit active (equivalent of failover active CLI command).
- **Make Standby**—If the current unit is in the active mode, trigger a failover to make the current unit standby.
- **Reset Failover**—If one or both of the units in the failover pair are in a failed state, force them to reset and attempt to join the pair (equivalent of failover reset CLI command).
- **Reload Standby**—Reboot the standby unit (equivalent of failover reload-standby CLI command).

While the ASDM is useful for basic troubleshooting and operations, the ASA CLI provides much more detailed troubleshooting information. The following output shows the many options available:

```
cidm-asa# show failover ?
  descriptor  Show failover interface descriptors. Two numbers are shown for
              each interface. When exchanging information regarding a
              particular interface, this unit uses the first number in messages
              it sends to its peer. And it expects the second number in
              messages it receives from its peer. For troubleshooting, collect
              the show output from both units and verify that the numbers
              match.
  exec        Show failover command execution information
  history     Show failover switching history
  interface   Show failover command interface information
  state       Show failover internal state information
  statistics  Show failover command interface statistics information
```

Some of the more frequently-used commands are detailed below:

- **show failover**—This command serves as a starting point for troubleshooting and provides a detailed summary of all aspects of the failover pair. These include: whether failover is enabled, the current unit's configured role (primary or secondary), the failover interface and its status, polling timer values, software versions of both units, timestamp of last failover event, active and standby status of both units, how long the currently-active unit has been active, all monitored interfaces and their status and statistics related to stateful failover.

  An example of the command output is shown below:

```
cidm-asa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/0 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 114 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.3(1), Mate 9.3(1)
Last Failover at: 14:45:49 EDT Apr 27 2015
        This host: Primary - Active
                Active time: 848635 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/9.3(1)) status (Up Sys)
                  Interface IPS-mgmt (192.168.254.71): Normal (Monitored)
                  Interface guest (10.13.1.1): Normal (Monitored)
                  Interface employee (10.13.2.1): Normal (Monitored)
                  Interface Factory-802 (10.255.255.34): Normal (Monitored)
                  Interface Enterprise (10.255.3.236): Normal (Monitored)
                  Interface IDMZ-RDG (10.1.2.1): Normal (Not-Monitored)
                  Interface IDMZ-MFT (10.1.2.25): Normal (Not-Monitored)
                slot 1: SFR5515 hw/sw rev (N/A/) status (Unresponsive/Up)
```

```
Other host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASA5515 hw/sw rev (1.0/9.3(1)) status (Up Sys)
          Interface IPS-mgmt (192.168.254.72): Normal (Monitored)
          Interface guest (10.13.1.2): Normal (Monitored)
          Interface employee (10.13.2.2): Normal (Monitored)
          Interface Factory-802 (10.255.255.35): Normal (Monitored)
          Interface Enterprise (10.255.3.237): Normal (Monitored)
          Interface IDMZ-RDG (10.1.2.2): Normal (Not-Monitored)
          Interface IDMZ-MFT (10.1.2.26): Normal (Not-Monitored)
        slot 1: SFR5515 hw/sw rev (N/A/5.3.1-152) status (Up/Up)
          ASA FirePOWER, 5.3.1-152, Up
```

Stateful Failover Logical Update Statistics:

```
Link : failover GigabitEthernet0/0 (up)
Stateful Obj    xmit       xerr       rcv        rerr
General         813706     0          113160     0
sys cmd         113160     0          113160     0
up time         0          0          0          0
RPC services    0          0          0          0
TCP conn        393371     0          0          0
UDP conn        186561     0          0          0
ARP tbl         120516     0          0          0

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       17      113160
Xmit Q:         0       690     1275783
```

- **show failover history**—This command provides a timestamped history for the current unit of all state changes since coming online. If a unit is in an unexpected or failed state, this command can indicate what happened just before the unit arrived at this state. An example of the command output for a normally functioning active unit is shown below:

```
cidm-asa# show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
14:45:39 EDT Apr 27 2015
Not Detected              Negotiation               No Error

14:45:49 EDT Apr 27 2015
Negotiation               Just Active               No Active unit found

14:45:49 EDT Apr 27 2015
Just Active               Active Drain              No Active unit found

14:45:49 EDT Apr 27 2015
Active Drain              Active Applying Config    No Active unit found

14:45:49 EDT Apr 27 2015
Active Applying Config    Active Config Applied     No Active unit found

14:45:49 EDT Apr 27 2015
Active Config Applied     Active                    No Active unit found

==========================================================================
```

- **show failover state**—This command provides the status of both members of the failover pair: whether configured as primary or secondary, and whether in active or standby mode. It also indicates the reason for the most recent failure event of either unit and the timestamp of that event. An example of the command output for a normally functioning failover pair is shown below:

```
cidm-asa# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Firewall Rules Troubleshooting

This section provides information on some of the troubleshooting tools available in the Cisco ASDM for understanding which packets are being allowed or denied through the firewall.

The **packet tracer** feature allows the user to enter packet parameters, including the ingress interface, packet type, source and destination IP addresses and ports, and see whether or not the packet is allowed to traverse the firewall. In addition, it shows the detailed flow of the packet through each layer of the firewall and which layer, if any, is causing the packet to be dropped.

The packet tracer function can be accessed by going to **Tools > Packet Tracer**. Figure 4-146 shows an example of a packet that can successfully traverse the firewall, whereas Figure 4-147 shows a packet that is dropped.

Figure 4-146 Packet Tracer - Successful Traversal

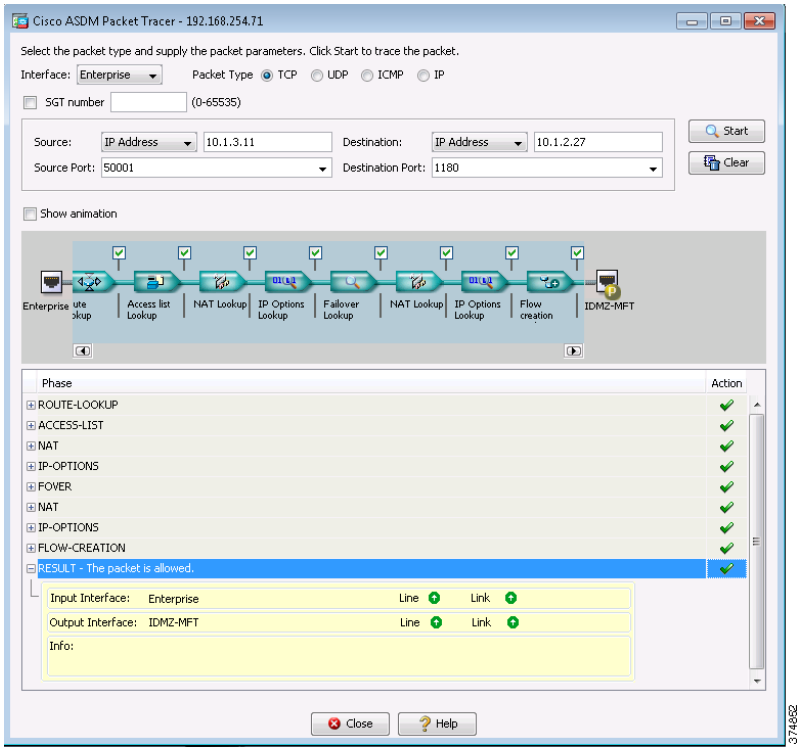
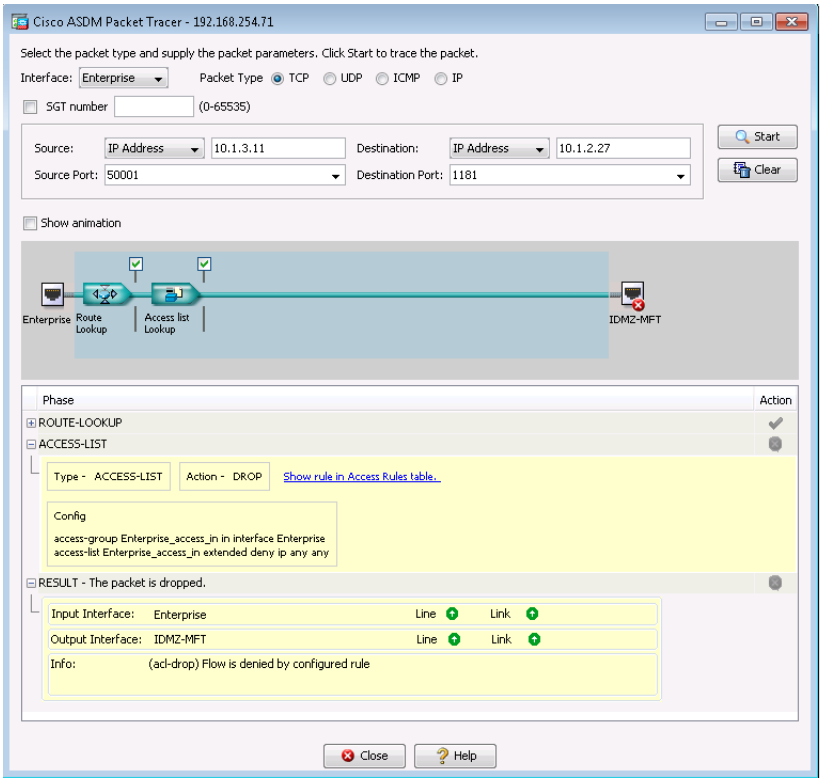


Figure 4-147 Packet Tracer - Failed Traversal

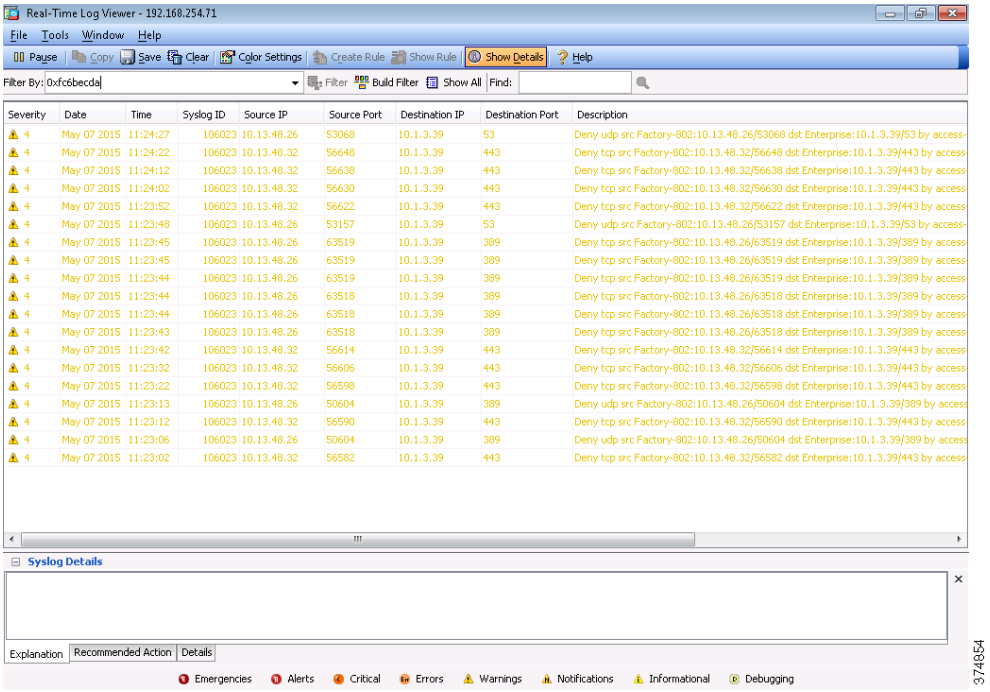


The **real-time logs** feature allows the user to see all traffic arriving at a particular interface and whether that traffic is being allowed or dropped on the firewall.

To show the logs for a certain access rule, select and right-click the rule under the desired ingress interface, and then click **Show Log**. This will load the **Log Viewer** window and automatically filter log entries to show only ones applying to that access rule. To clear the filter and see all packets being processed at that interface, click **Show All** in the **Filter** toolbar.

Figure 4-148 shows an example of a filtered real-time log.

Figure 4-148 100 Real-Time Log Viewer



APPENDIX A

References

This appendix, which lists the references used in the IDMZ system, includes the following major topics:

Converged Plantwide Ethernet (CPwE)

- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (CPwE):*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_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: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html

- 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: http://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: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html
- *Deploying Identity Services within a Converged Plantwide Ethernet Architecture:*
  - 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
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.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 the following URL:

- 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/vss.html

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 ASA with FirePOWER Services:

- http://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html

Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6 Information About High Availability:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ha_overview.html

Cisco ASA 5500-X Series Next-Generation Firewalls Configuration Guides

- http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.4:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/asdm74/firewall/asa-firewall-asdm/inspect-dbdir-mgmt.html

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

Secure Remote Worker Design Guide:

- https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/srw-design-guide.pdf

Remote Desktop Services Overview:

- https://technet.microsoft.com/en-us/library/hh831447.aspx

ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.3:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm.html

AnyConnect Client Reconnects Every Minute Which Causes a Disruption in Traffic Flow:

- http://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116881-technote-anyconnect-00.html

Deploying Remote Desktop Gateway Step-by-Step Guide:

- https://technet.microsoft.com/en-us/library/dd983941%28v=ws.10%29.aspx

ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.3 Basic Clientless SSL VPN Configuration:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm/webvpn-configure-gateway.html

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 6500	15.1(2)SY4	Virtual Switching System (VSS)
Core switch	Catalyst 4500E	3.6.1E	Virtual Switching System (VSS)
Distribution switch	Catalyst 3750-X	15.2(3)E	Switch stack
Access switch	Cisco IE 2000, Stratix 5700	15.2(3)EA	
Access switch	Cisco IE 3000, Stratix 8000	15.2(3)EA	
Lightweight Access Point	Cisco Aironet 3602E	8.0.100.0	
Wireless LAN Controller (WLC)	Cisco 5508	8.0.100.0	
Firewall	Cisco ASA 5515-X	9.3(1)	Active and Standby
Identity Services Engine (ISE)	Cisco ISE 3415 / 3495	1.3	Distributed ISE
Client	Microsoft Windows laptop	Windows 7	

Table B-2 Rockwell Automation Software

Product	Version
FactoryTalk Historian Site Edition	4.0
FactoryTalk Service Platform	2.60.00 (CPR 9 SR 6)
FactoryTalk Activation Manager	3.62.11 (CPR 9 SR 6.1)
FactoryTalk Historian to Historian Interface	3.08.07
FactoryTalk AssetCentre	6.00
FactoryTalk View Site Edition	8.00.00 (CPR 9 SR 7)
FactoryTalk ViewPoint Site Edition	8.00.00
RSLinx Enterprise Edition	5.70.00 (CPR 9 SR 7)
RSLinx Classic	3.71.00 (CPR 9 SR 7.1)
FactoryTalk Metrics	11.50
Report Expert	3.20.00

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
FTLD	FactoryTalk Live Data
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
MFT	Managed File Transfer
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

Term	Definition
RDC	Remote Desktop Connection
RDP	Remote Desktop Protocol
RF	Radio Frequency
RPC	Remote Procedure Call
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

Publication ENET-TD009C-EN-P March 2022