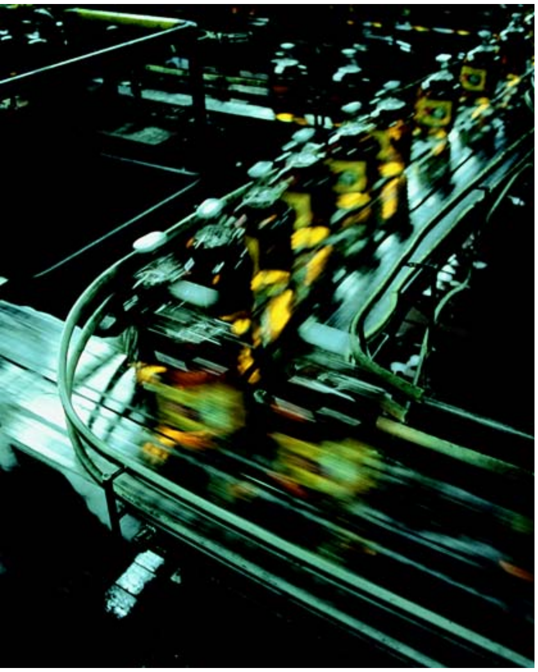


Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Design Guide

January 2020

Document Reference Number: ENET-TD017B-EN-P

Preface

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

Industrial IoT (IIoT) offers the promise of business benefits by using innovative technology such as mobility, collaboration, analytics, and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security and safety best practices. Cloud Connectivity to a Converged Plantwide Ethernet Architecture CRD (CPwE Cloud Connectivity), which is documented in this design guide, outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity from FactoryTalk® applications and industrial operations to the Rockwell Automation® cloud within a CPwE architecture. CPwE Cloud Connectivity was architected, tested, and verified by Cisco Systems and Rockwell Automation with assistance by Panduit.

Release Notes

This section summarizes the extensions to CPwE Cloud Connectivity in this January 2020 release:

- Extensions to technology use cases
- Extensions to test results and details
- Addition of Cisco Web Security Appliance and related infrastructure configuration
- Addition of technology troubleshooting and verification

Document Organization

This document contains the following chapters and appendices:

Chapter	Description
Chapter 1, “CPwE Cloud Connectivity Overview”	Presents an introduction to CPwE Cloud Connectivity architecture and the security architecture use cases.
Chapter 2, “CPwE Cloud Connectivity Design Considerations”	Presents an overview of CPwE Cloud Connectivity technology and design and deployment considerations, including security policy, architectural, and technology considerations, and FactoryTalk AssetCentre, FactoryTalk Activation Manager, and ControlFLASH Plus^{TM} test cases
Chapter 3, “Configuring the Infrastructure”	Walk-through of the configuration of the various devices and infrastructure used as part of this CRD.
Chapter 4, “Verifying and Troubleshooting the Deployment”	Troubleshooting and verification tips associated with the use of the Cisco Web Security Appliance and the associated redirection technology.
Appendix A, “References”	List of references for CPwE design and implementation guides for network infrastructure services and security.
Appendix B, “Acronyms and Initialisms”	List of acronyms and initialisms used in this document.
Appendix C, “About the Cisco Validated Design (CVD) Program”	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs.)

For More Information

More information on CPwE Design and Implementation Guides can be found at 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 uses the ODVA, Inc. Common Industrial Protocol (CIP™) and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, CIP, CIP Safety^{TM}, CIP Security^{TM}, or CIP Sync^{TM}, see the following URL:

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

CHAPTER 1

CPwE Cloud Connectivity Overview

This chapter includes the following major topics:

Cloud Connectivity Architecture Introduction

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

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

Cloud-based services help to enable data collaboration and remote monitoring of dashboards by industrial operations and/or trusted industry partners (for example, system integrator, OEM or IACS vendor) for IACS applications within the CPwE architecture (Figure 1-1). A holistic industrial security stance is necessary to help protect the integrity of safety and security best practices while also helping to enable restricted cloud-based services. No single product, technology or methodology can fully secure plant-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical and physical), utilizing diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture.

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

CPwE Cloud Connectivity outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk applications from industrial operations to the Rockwell Automation cloud within a CPwE architecture (Figure 1-1).

Note This design guide helps with meeting the following IEC-62443 3-3 Functional Requirements:
- FR3 SR 3.2 RE1: Malicious code protection on entry and exit points
- FR5 SR 5.2: Zone boundary protection
- FR5 SR 5.3: General purpose person-to-person communication restrictions

CPwE Overview

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

CPwE key tenets include:

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

Figure 1-1 CPwE Architectures

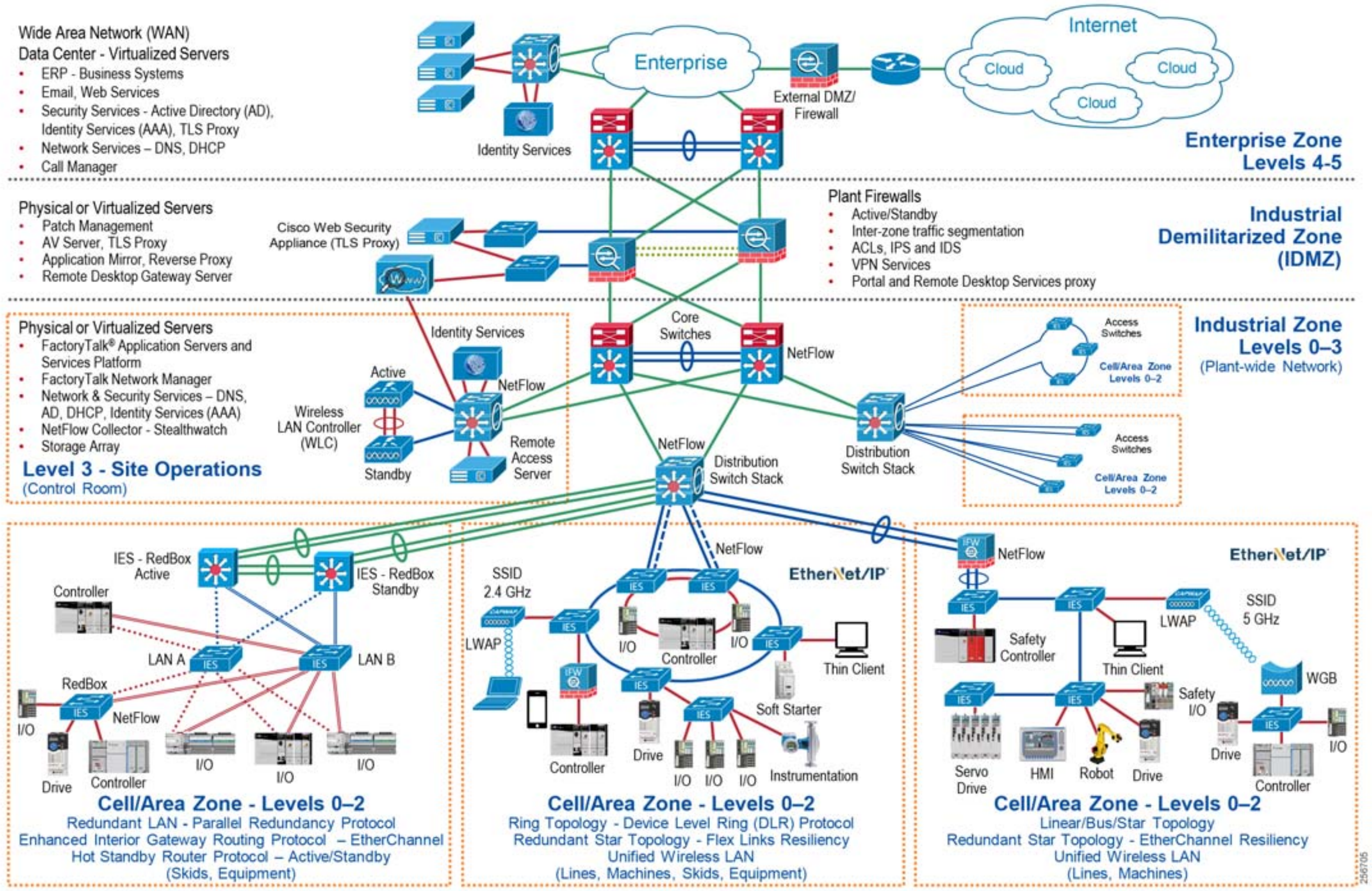
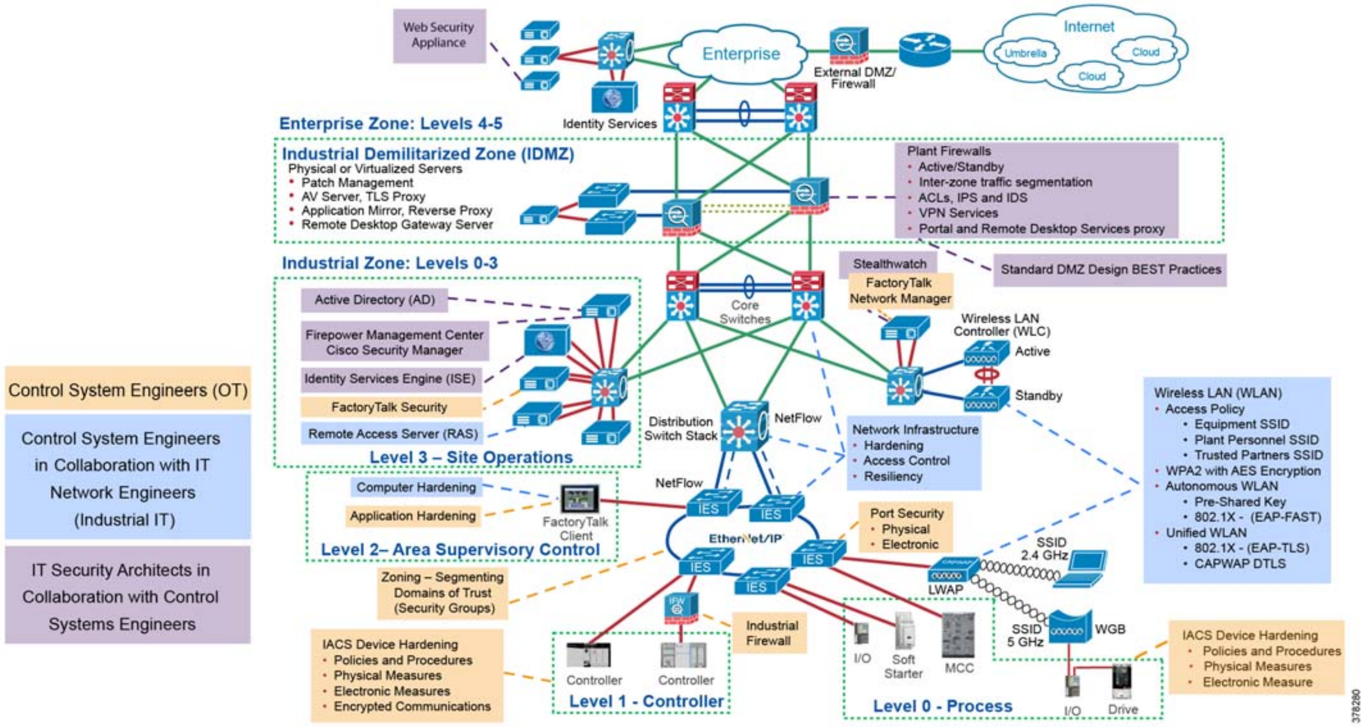

Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone
Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Cisco Web Security Appliance (TLS Proxy)
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
NetFlow
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone
Levels 0–3
(Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
IES
I/O
NetFlow
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
NetFlow
SSID
2.4 GHz
EtherNet/IP
LWAP
IES
I/O
Controller
I/O
IFW
Thin Client
Controller
Drive
Soft Starter
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
IFW
NetFlow
EtherNet/IP
IES
Safety Controller
LWAP
SSID
5 GHz
Thin Client
WGB
Safety I/O
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
256705

Figure 1-2 CPwE Industrial Security Framework



CPwE Cloud Connectivity

An IACS is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, distribution, pulp and paper, oil and gas, mining and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete and hybrid combinations. One of the challenges facing industrial operations and OEMs is the need to establish and secure connectivity from IACS applications to cloud-based services to take advantage of the business benefits associated with the IIoT.

CPwE Cloud Connectivity describes several security architecture use cases that are addressed using diverse security solutions and technologies, managed by different persona, at different levels of the plant-wide security architecture as shown in Figure 1-2.

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

CPwE Cloud Connectivity outlines the concepts, requirements and technology solutions for reference designs developed around a specific set of security architecture use cases. These use cases were tested for solution functional validation by Cisco Systems and Rockwell Automation with assistance by Panduit. The following is a synopsis for this release of CPwE Cloud Connectivity:

- End-to-end outbound cloud connectivity
  - Tested and verified as part of this design guide—End-to-end FactoryTalk solution use cases—Platinum, Gold, Silver, and Bronze
  - Referenced only—Cisco Kinetic, Cisco IoT Gateway, any public cloud service
- Security Stance Overview
  - Risk management—Risk assessment considerations, risk tolerance, and risk mitigation
  - One size does not fit all
  - Trusted versus untrusted security zones
  - Policies and procedures to balance business benefits (such as innovation) with risk management
- End-to-end FactoryTalk Solutions Capabilities Overview
  - FactoryTalk AssetCentre
  - ControlFLASH Plus
  - FactoryTalk Activation Manager
  - Rockwell Automation Cloud API—Currently this API is used to ascertain product life cycle status and acts as the cloud endpoint.
- Design and Deployment Considerations for End-to-End FactoryTalk Solution
  - Establishing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
  - Securing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
  - Securing the plant-wide IACS network from the Industrial Zone ingress/egress point
  - Securing access to the Rockwell Automation cloud
  - Securing access to the Industrial Demilitarized Zone (IDMZ) Cisco Web Security Appliance acting as the Transport Layer Security (TLS) proxy

Security Architecture Use Cases

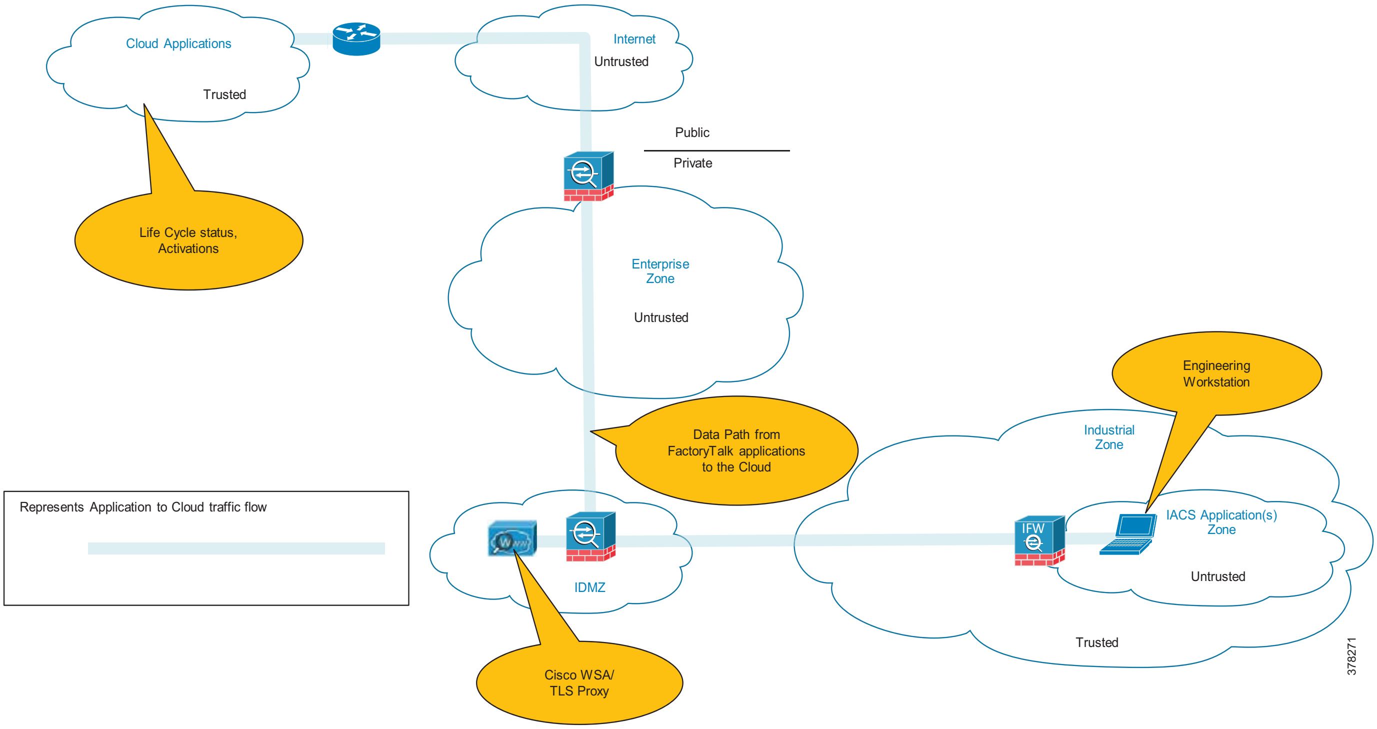
One size does not fit all when it comes to risk tolerance. What’s acceptable by one industrial operator may be unacceptable to another and vice versa. The CPwE architecture supports scalability, which includes the degree of holistic and diverse industrial security technologies (Figure 1-2) applied to a plant-wide security architecture. Scalable security comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their tolerance to risk. Industrial operators should also ensure that the cloud provider and internet service provider (ISP) are trusted. They are required to help protect connectivity and data per the industrial operator’s security policies.

- **Platinum Security Architecture**—The Industrial Zone communicates with the Rockwell Automation Cloud via Transport Layer Security (TLS). In keeping with the Industrial Demilitarized Zone (IDMZ) concept of brokered services, a TLS proxy is located in the IDMZ (Figure 1-3). For testing and verification purposes, the TLS proxy that was used is the Cisco Web Security Appliance (Cisco WSA). This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial

Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to help protect the Industrial Zone from the ingress/egress point of the TLS traffic.

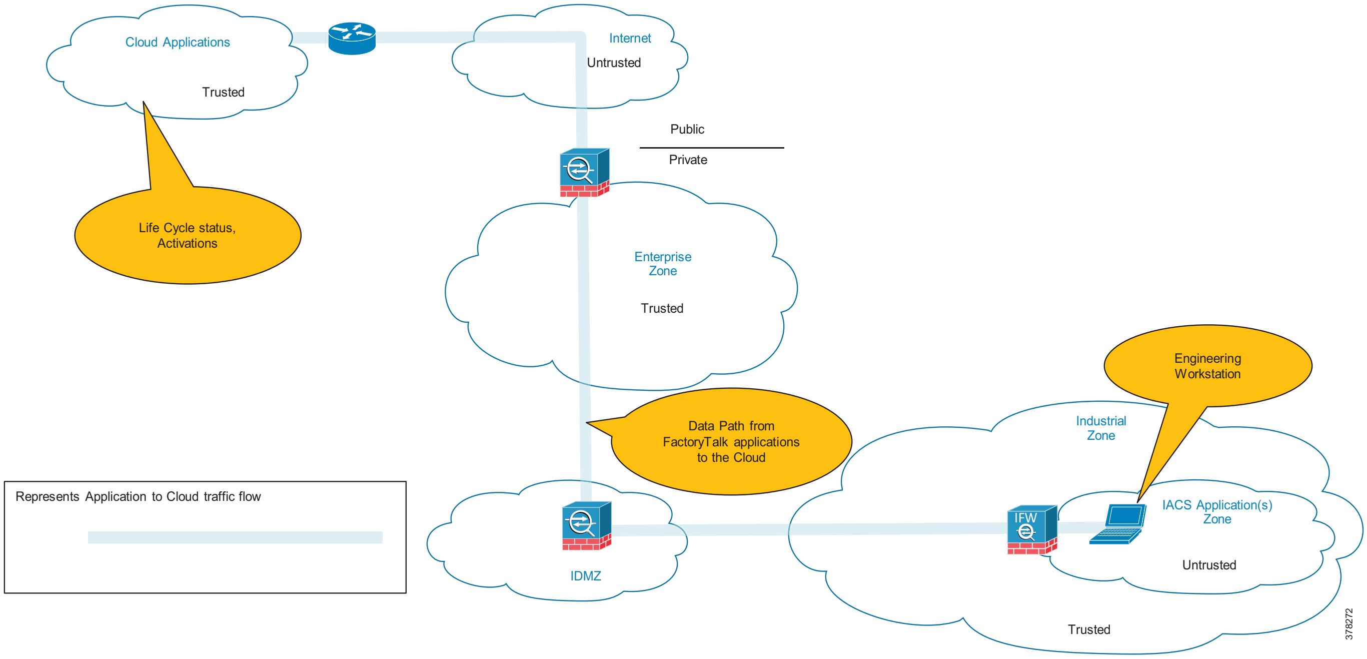
This is the security architecture recommended by Cisco, Panduit, and Rockwell Automation for industrial operations that require cloud-based connectivity yet have a lower tolerance to risk. Some industrial operators may already have a TLS proxy located in their Enterprise DMZ that buffers their Enterprise Zone from the Internet. This security architecture could be implemented to leverage that existing TLS proxy. A third option is to have a TLS Proxy located in the cloud like the Cisco Umbrella Intelligent Proxy. This solution only proxies the traffic that is destined for domains that are proven to be harmful.

Figure 1-3 Platinum Security CPwE Cloud Connectivity Use Case



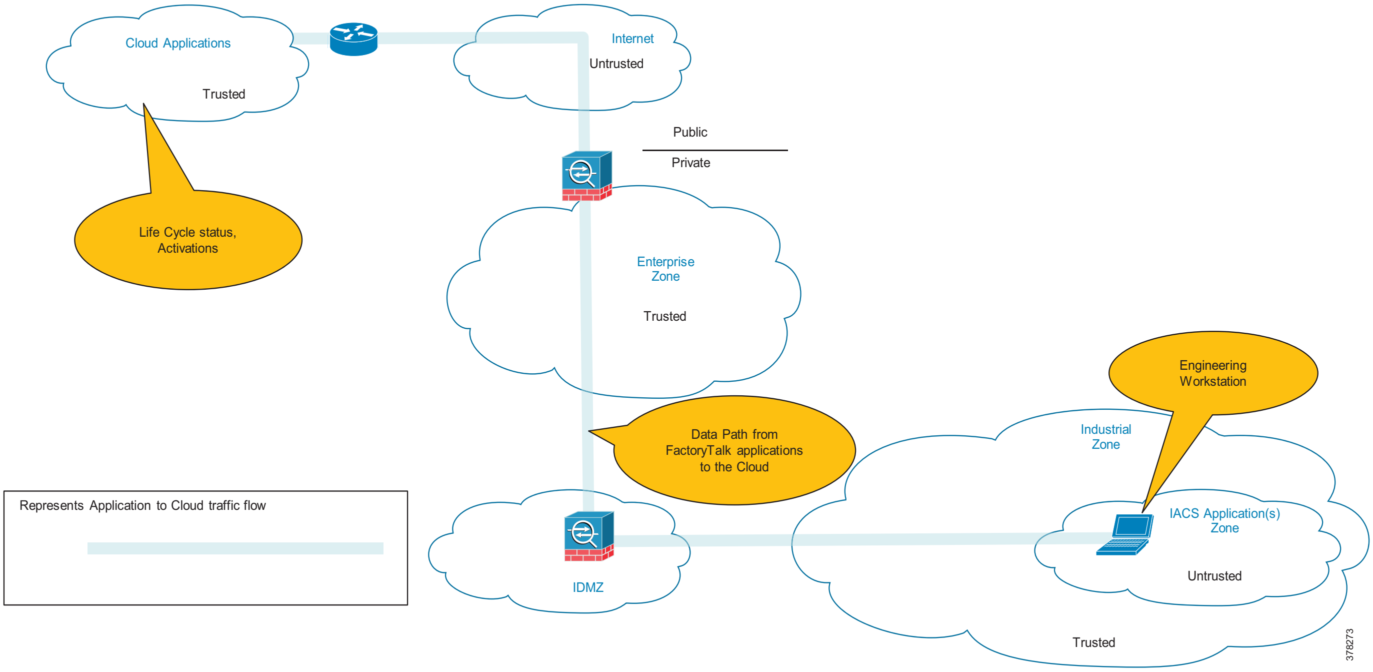
- **Gold Security Architecture**—This security architecture could be deployed when a TLS proxy is not present and when multiple layers of diverse industrial security best practices (Figure 1-2) have been followed. This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to help protect the Industrial Zone from the ingress/egress point (Figure 1-4).

Figure 1-4 Gold Security CPwE Cloud Connectivity Use Case



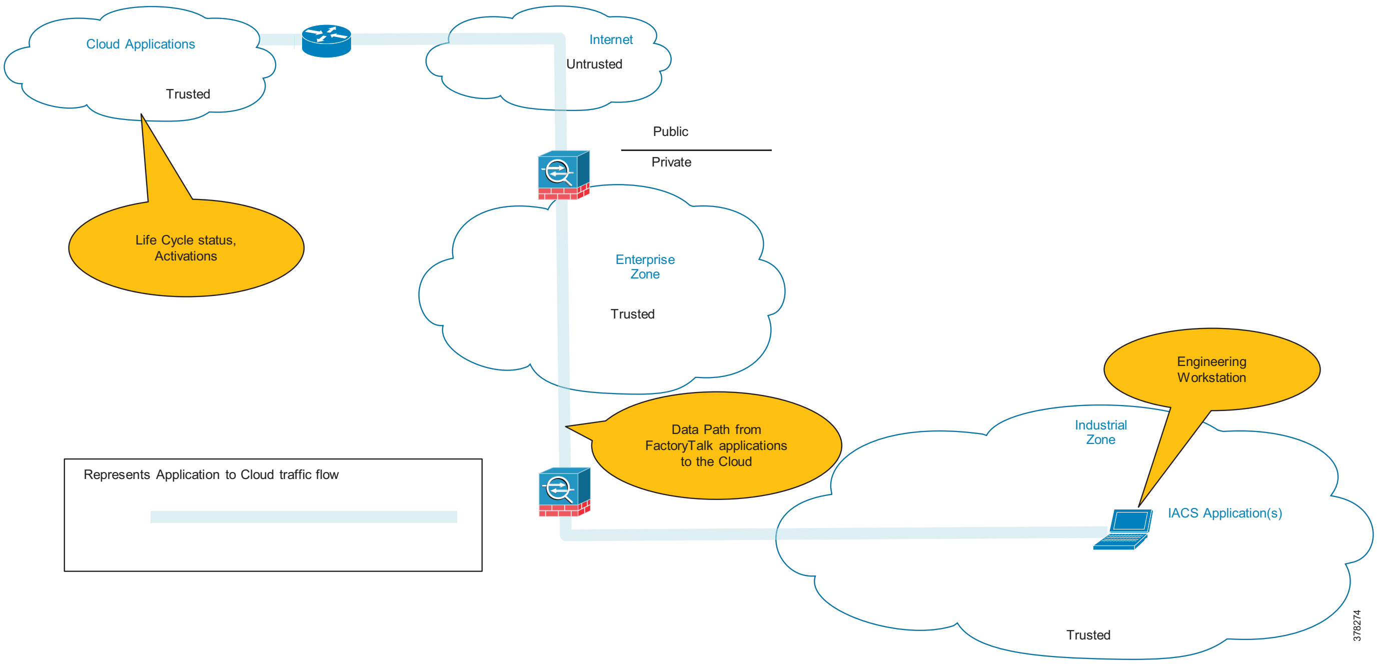
- **Silver Security Architecture**—This security architecture has an IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. No additional Industrial Firewall(s) exist that enforce security policies to help protect the Industrial Zone from the ingress/egress point (Figure 1-5).

Figure 1-5 Silver Security CPwE Cloud Connectivity Use Case



- **Bronze Security Architecture**—This security architecture has the fewest defensive layers of diverse industrial security best practices for threat protection and detection. A Firewall is the only buffer between the Enterprise and Industrial Zone. No additional Industrial Firewall(s) exist to enforce security policies to help protect the Industrial Zone from the ingress/egress point. Only industrial operations with a higher tolerance to risk should consider this security architecture for cloud-based connectivity (Figure 1-6).

Figure 1-6 Bronze Security CPwE Cloud Connectivity Use Case



CPwE Industrial Security Overview

Protecting IACS assets requires a defense-in-depth security approach (Figure 1-2) where different solutions are needed to address various network and security requirements for a plant-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of industrial security.

- *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several network security use cases for plant-wide IACS network infrastructure to help enable IIoT innovation within the CPwE framework.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several industrial security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk applications, throughout a plant-wide IACS network infrastructure.

  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD. html
- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing, deploying, and managing industrial firewalls throughout a plant-wide IACS network. The Industrial Firewall is ideal for IACS applications that need trusted zone segmentation.
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

CHAPTER 2

CPwE Cloud Connectivity Design Considerations

This chapter provides an overview of design considerations—using diverse technologies for threat detection and prevention—to integrate an end-to-end IACS solution from the skid/equipment/machine to the enterprise to the cloud within a CPwE architecture. Although this design guide focuses on end-to-end FactoryTalk solution uses cases, the holistic and diverse industrial security technology best practices apply generically to IACS device to cloud use cases. This chapter includes the following major topics:

It is important to mention that this design guide does not discuss options for the method used by the various cloud connected solutions to connect to the cloud application; these design decisions have already been made by the developers. In this design guide, the various cloud connected solutions use the TLS protocol to establish secure communication with the cloud applications. This design guide does not suggest options for gateway to cloud communication. This design guide does provide infrastructure recommendations to monitor the TLS traffic between the Industrial Zone and the cloud application for anomalous traffic, as well as recommendations for firewall configurations to limit the traffic from the Industrial Zone to the cloud.

Security Policy Considerations

Most companies understand the need for security and, therefore, have policies governing enterprise systems such as the internet or email use. It is, however, common for security policies to often be insufficient or, in some cases, nonexistent in Industrial Zone systems.

With the recent popularity of providing computing resources, analytics, application software, and data storage in the cloud, there is a natural desire to extend this capability to industrial operations. Vendors are providing industrial operators with cloud-based Software as a Service (SaaS) not only to leverage their expertise in areas such as analytics, but to deliver on the promise of cloud-based technologies to also allow their customers to view data anywhere and from any device.

Enterprise IT has adopted the use of cloud-based resources, which has positioned that department to be aware of and responsible for:

- Cloud security policy considerations and ultimately the generation of cloud security policies
- Cloud infrastructure security best practices
- Cloud application security best practices

The opportunity for OT and IACS assets to send data securely to a trusted cloud to provide information on product quality, skid/equipment/machine operations, and performance has been sufficiently advantageous to realizing the development of cloud connected devices. Cloud connected devices are typically dual role where they support communication to IACS devices and to a trusted cloud-hosted application.

Risk Assessment and Risk Management

Until recently most industrial operations have been segmented with no connectivity to the internet unless there was a specific business need for highly restricted remote support, site-to-site communications through a VPN tunnel, or other less common purposes. With today’s desire to send information to cloud-based services, one must consider the risk versus reward proposition of sending industrial operational data to trusted cloud applications. According to organizations such as Rockwell Automation, Cisco Systems, and Open Web Application Security Project (OWASP), the following risks should be considered:

- Data Ownership and Protection

  The traditional approach to business software applications is to run them in-house on an infrastructure built and maintained by the organization using the applications. Therefore, all data resides within the organization and it has complete control over the data and how it is protected. An organization using cloud services must understand to what extent the cloud provider’s personnel have access to their data. When an organization uses these cloud-enabled services, they are outsourcing business processes to the cloud provider which requires access to the organization’s data. The industrial operator should confirm that both the cloud provider and the Internet Service Provider (ISP) are trusted and provide the necessary network and security services to help protect connectivity and data as required by their business and security policies.

- User Identity Management and Federation

  Organizations must understand how cloud providers identify users and manage their accounts for accessing data in the cloud. In addition, they must understand the risks associated with logon accounts and how the cloud provider mitigates these risks. These risks include password guessing, password theft, password reset, hijacking of user login sessions, and revocation of access. As an alternative to creating a separate island of user names and passwords, some cloud providers may offer integration with an organization’s in-house authentication systems. Through integration, existing in-house logon accounts managed by the organization can be used to access data in the cloud.

- Regulatory Compliance

  Organizations using cloud providers face different challenges regarding regulatory compliance for data stored in the cloud. They must consider whether data entrusted to a cloud provider carries legal/regulatory protection and breach notification requirements, such as protected health information (PHI) governed by HIPAA and HITECH, personally-identifiable information (PII) governed by state privacy laws, and payment card information regulated by the Payment Card Industry’s (PCI's) Data Security Standard (DSS).

- Business Continuity and Resiliency

  Business continuity and resiliency refer to the ability of an organization to conduct business operations in adverse situations. Adverse situations include disruptions not only to the information technology infrastructure, but also any disruptions affecting the ability of the cloud service provider to deliver its services at defined service levels, including, for example, the loss of key personnel or the loss of access to business offices.

  When an organization uses a cloud provider, the organization cedes control of business continuity planning for the data and services entrusted to the provider. As a result, the organization must consider carefully how the cloud provider would maintain continuity of services if affected by adverse situations.

- User Privacy and Secondary Uses of Data

  Organizations must understand how a cloud provider helps protect and use information about different types of users. They should consider to what extent a cloud provider can disclose information about its employees, its customers, or its business. This information includes specific information or aggregate statistics. It includes information collected from an individual’s use of the cloud provider’s information systems, such as characteristics of user behavior (for example, links clicked, options selected, etc.) and productivity measurements.

- Service and Data Integration

  Organizations must understand how their users will access the data and services of a cloud provider. Typically, this access will be over the internet or a virtual private network (VPN) using a web browser or a software application downloaded from the cloud provider. If the organization will be interfacing any of its systems with the systems of the cloud provider, they must understand the technical aspects of how the interface will work. An example of this may be if the organization wants to implement "back-end" or batch processing of Health Level 7 (HL7) or Electronic Data Interchange (EDI) transactions. In both cases (user access and system interfaces), organizations must understand the risks associated with electronic communication across the internet or wide area networks (WANs). This includes interception of data in transit, falsification or corruption of data, and verification of client and server endpoints.

- Multi-tenancy

  In a cloud computing environment, multi-tenancy refers to the sharing of information technology infrastructure among multiple clients (different customers of a single cloud service provider). This infrastructure includes telecommunications circuits, network equipment, servers, storage, and application software. Multi-tenancy allows cloud providers to achieve economies of scale, which would be impossible for an individual organization to attain, enabling organizations to obtain higher levels of service at lower costs.

  Risks with multi-tenancy include one client accessing the data of another client, unintentional mixing of one client’s data with another client’s data, one client affecting the quality of service provided to another client, and cloud provider application software upgrades affecting client business operations. While cloud providers can be expected to have adequately mitigated these risks given that multi-tenancy is core to the cloud business model, an organization should understand how the cloud provider achieves isolation between clients. Isolation approaches include use of virtualization technologies such as virtual machines, application-level isolation through processes, threads, or application-managed contexts, and database-level isolation using separate database instances, tablespaces, or record identifiers

- Incident Response and Forensic Analysis

  Incident response and forensic analysis refer to activities conducted by an organization when there is a security incident requiring immediate response and subsequent investigation. These incidents include malicious acts or mistakes by the employees or former employees of the organization, resulting in data breaches. When an organization uses a cloud provider, it does not have access to the underlying log files and other low-level system-level information typically used for forensic examination.

- Infrastructure and Application Security

When an organization uses a cloud service provider, it trusts the provider to properly secure its applications and infrastructure. This is a highly complex activity requiring an extensive array of personnel with advanced technical skill sets and threat knowledge.

- Non-production Environment Exposure

  A cloud provider typically operates multiple environments where cloud data and services exist. These environments include what is normally referred to as a production environment, which is where cloud subscribers have the primary copy of their data and where they conduct their business operations.

  Cloud providers also typically operate other environments for purposes such as software development, testing, training, and demonstrations to potential customers. These other environments may be populated with copies of data from the production environment. In other words, an organization's data may be copied into several places to support the necessary business operations of the cloud provider. The data contained in these copies may or may not be de-identified, a process whereby individual customer information is rendered untraceable to a specific customer and individual business information is made untraceable to an organization.

Architectural Considerations

Network and security technology architecture decisions are made with several key factors in mind to help determine how IACS is implemented. Some of the key architectural decision factors are:

- Align the architecture to support security policies.
- Consider best practices for safety and security provided by IACS vendors.
- Technical security controls such as zoning, firewalls (protection and detection), end host protection, application security, and proxy services to support an organization's security policy.
- Technical control deployments will align with an organization's risk profile while balancing business aspects and budget constraints.

In the following sections four different security architectures are reviewed, which have been classified as Platinum through Bronze to denote, respectively, higher-layered through lower-layered security architectures. Cisco, Rockwell Automation, and Panduit realize there are many different possible combinations that could be covered, so four security architectures were selected to help provide a scalable solution to cover the typical scenarios found within plant environments.

Regardless of which multi-layered security architecture is deployed, the manufacturer must confirm that the cloud provider and ISP are trusted and provide the necessary network and security services to help protect connectivity and data as required by the manufacturer's business and security policies.

Cisco, Rockwell Automation, and Panduit recommend that a risk assessment be conducted to survey IACS assets and identify any potential threat vectors before the selection and deployment of any security architecture.

Architectures at a Glance

Four architectures are discussed in this design guide, each with varying key security technologies to help monitor and limit the traffic between the cloud connected devices and the cloud application. Table 2-1 summarizes the architectures.

Table 2-1 Architectures at a Glance

Architecture	TLS Encrypted Communications between the Industrial Zone and Cloud Applications	IDMZ	Industrial Firewall at the Cell/Area Zone	TLS Monitoring	DNS Protection
Platinum	X	X	X	X	
Platinum Architecture with Cisco Umbrella	X	X	X	X	X
Gold	X	X	X		
Silver	X	X			
Bronze	X				

The IDMZ offers a buffer between the Enterprise and the Industrial Zone networks and is a widely accepted method for providing a layered security model. In this design guide, one option is to place the TLS proxy in the IDMZ.

The Industrial Firewall placed within the Cell/Area Zone can be used to limit the traffic of the cloud connected devices to the DNS server and the cloud. The industrial firewall device is used to define the boundary of the security zone and is used if the cloud connected device is compromised as a means to limit the traffic reaching other IACS applications within the Industrial Zone.

TLS URL filtering and monitoring can be accomplished by the Cisco WSA or through the Cisco Umbrella service. TLS monitoring is used to spot unusual traffic patterns or payload sizes in an attempt to monitor and alert the end user to possible malicious traffic. In addition, decryption policies within the Cisco WSA can allow for advanced malware protection by examining the payloads of traffic.

Cisco Umbrella is a security solution that helps protect against threats by helping ensure that any IACS traffic to the internet or cloud is going to safe websites or domains. DNS requests are sent to the Umbrella service, which is constantly updated with information received from Cisco’s Talos security intelligence team. This helps ensure that web traffic from end users or the cloud connected device is legitimate, but it can also block malware, phishing, and command and control callbacks over any port or protocol. If the cloud connected device was in any way compromised, Cisco Umbrella would keep the malware from reaching websites that could jeopardize the network.

See the Cisco Umbrella page at: https://umbrella.cisco.com.

Platinum Security Architecture

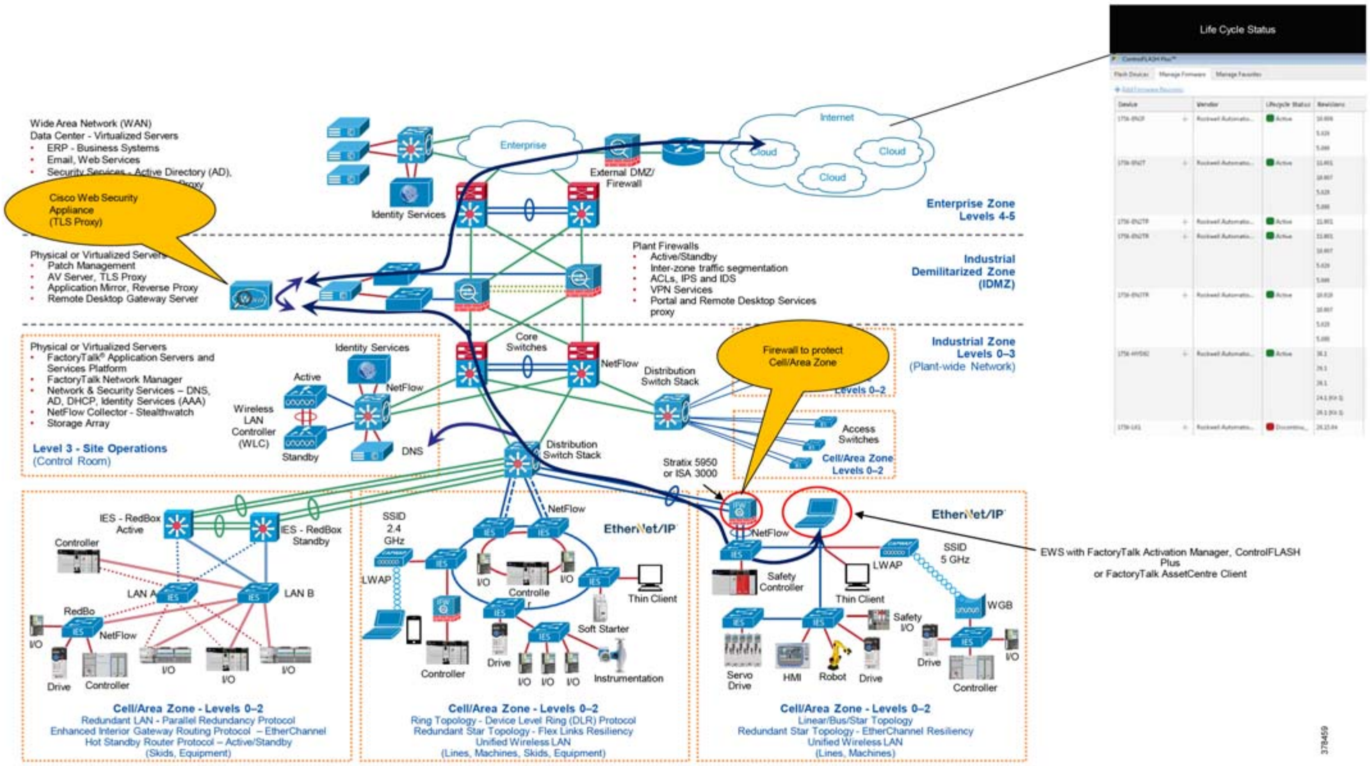
This security architecture provides multiple layers of defense-in-depth using diverse technologies for threat detection and prevention. This helps to prevent a single vulnerability from taking down IACS operations within the Industrial Zone. The cloud connected device typically is configured to communicate with the IACS devices using the CIP protocol and send and retrieve data to and from the cloud based on IACS device, such as lifecycle status information. The Platinum architecture contains an IDMZ for brokered services such as a TLS proxy and is the Cisco, Rockwell Automation, and Panduit security architecture recommended for manufacturers that require cloud-based connectivity yet have a lower tolerance to risk.

There are several key security technologies for threat detection and prevention that help to create this multi-layered security architecture, including:

- A TLS proxy that can inspect the outbound and inbound encrypted TLS traffic between the cloud connected device and the cloud-based software.
- Zoning—An IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone.
- Zoning—An Industrial Firewall which creates a security zone, to help enforce security policies within a Cell/Area Zone, that helps protect the Industrial Zone from the ingress/egress point of the TLS traffic.

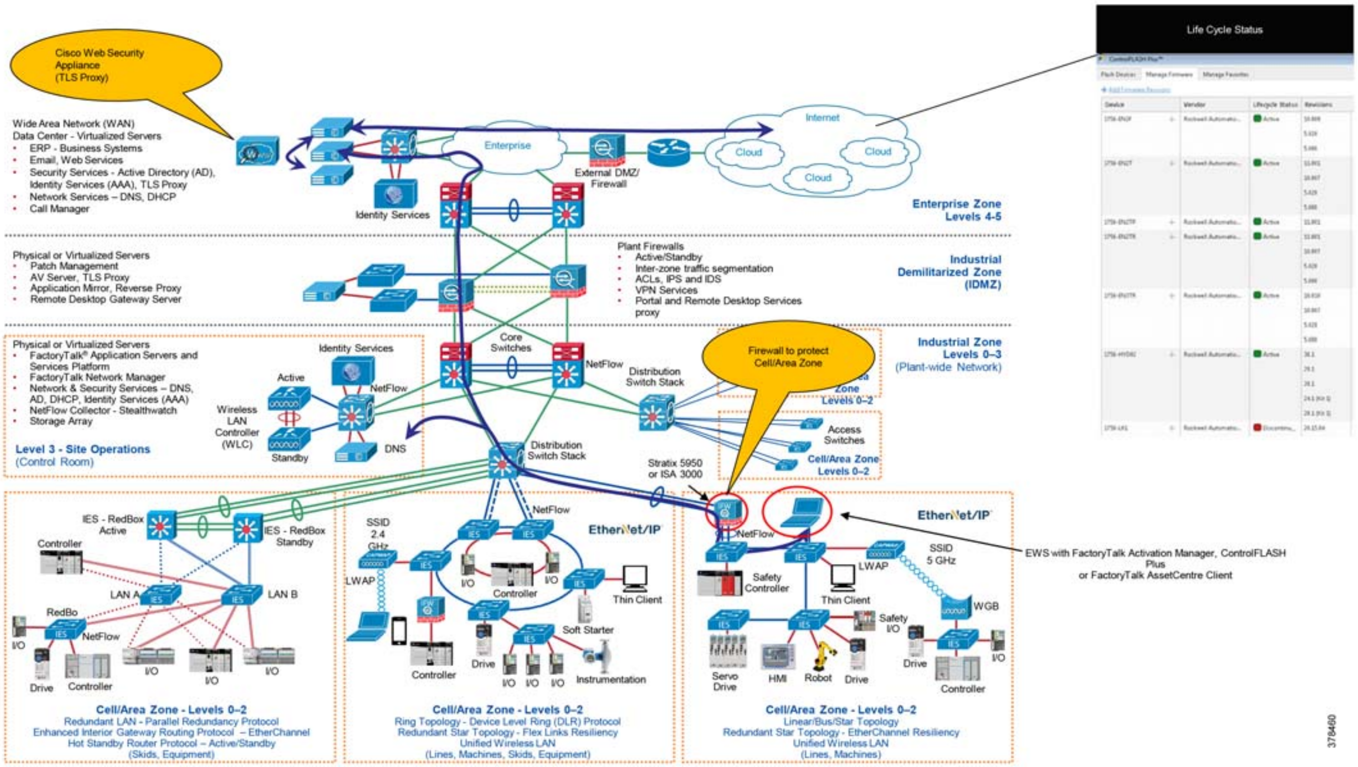
A TLS proxy, such as the Cisco WSA could be in the IDMZ to monitor and inspect the traffic between the cloud connected device and the cloud-based application. See Figure 2-1.

Figure 2-1 Platinum Security CPwE Cloud Connectivity Use Case with TLS Proxy in the IDMZ


Life Cycle Status
Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD),
Proxy
Cisco Web Security Appliance (TLS Proxy)
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
FactoryTalk Network Manager
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
NetFlow Collector - Stealthwatch
Storage Array
Level 3 - Site Operations (Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Core Switches
NetFlow
Distribution Switch Stack
Firewall to protect Cell/Area Zone
Levels 0–2
Industrial Zone Levels 0–3 (Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0–2
Distribution Switch Stack
Stratix 5950 or ISA 3000
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Soft Starter
Drive
I/O
I/O
I/O
Instrumentation
Controller
NetFlow
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus or FactoryTalk AssetCentre Client
378459

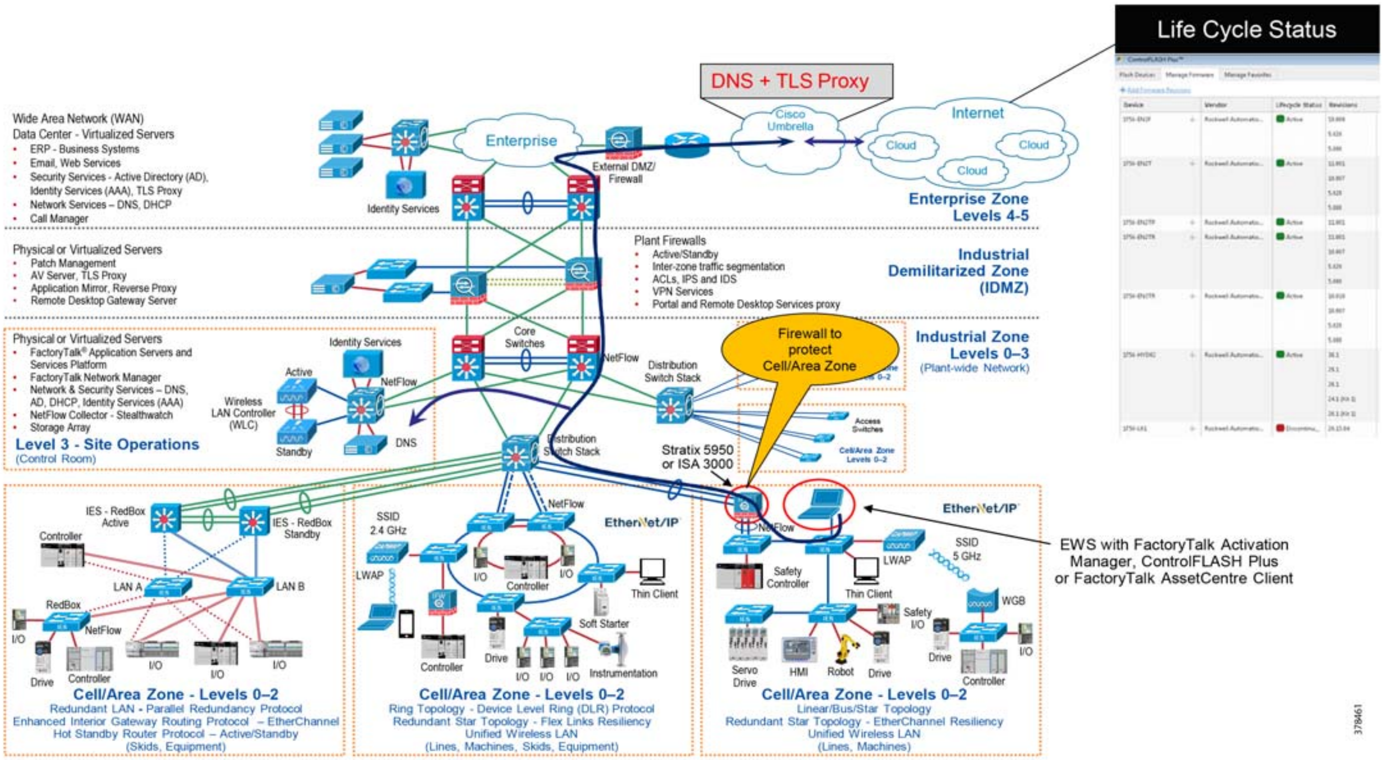
Some organizations may have already implemented a TLS proxy in the Enterprise Zone and want to use these same appliances for Industrial Zone cloud connectivity as shown in Figure 2-2. This does not follow one of the key tenets of the IDMZ, which is brokered services but still provides TLS proxy services to the IACS. In addition, an IDMZ TLS proxy can be used to broker inspected traffic to an upstream proxy device that may exist in the Enterprise Zone.

Figure 2-2 Platinum Security CPwE Cloud Connectivity Use Case with TLS Proxy in the Enterprise Zone


Life Cycle Status
Cisco Web Security Appliance (TLS Proxy)
Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
Internet
Cloud
Cloud
Cloud
External DMZ/ Firewall
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Level 3 - Site Operations (Control Room)
Core Switches
NetFlow
Distribution Switch Stack
Firewall to protect Cell/Area Zone
Zone Levels 0–2
Industrial Zone Levels 0–3 (Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0–2
Distribution Switch Stack
Stratix 5950 or ISA 3000
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Controller
Drive
Soft Starter
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
NetFlow
SSID 5 GHz
LWAP
Safety Controller
Thin Client
WGB
Safety I/O
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus or FactoryTalk AssetCentre Client
378460

Another architecture option for providing TLS proxy services is to use a cloud-based solution such as the Cisco Umbrella TLS proxy and DNS services. See Figure 2-3.

Figure 2-3 Platinum Security CPwE Cloud Connectivity Use Case with TLS Proxy Provided by Cisco Umbrella Cloud Solution

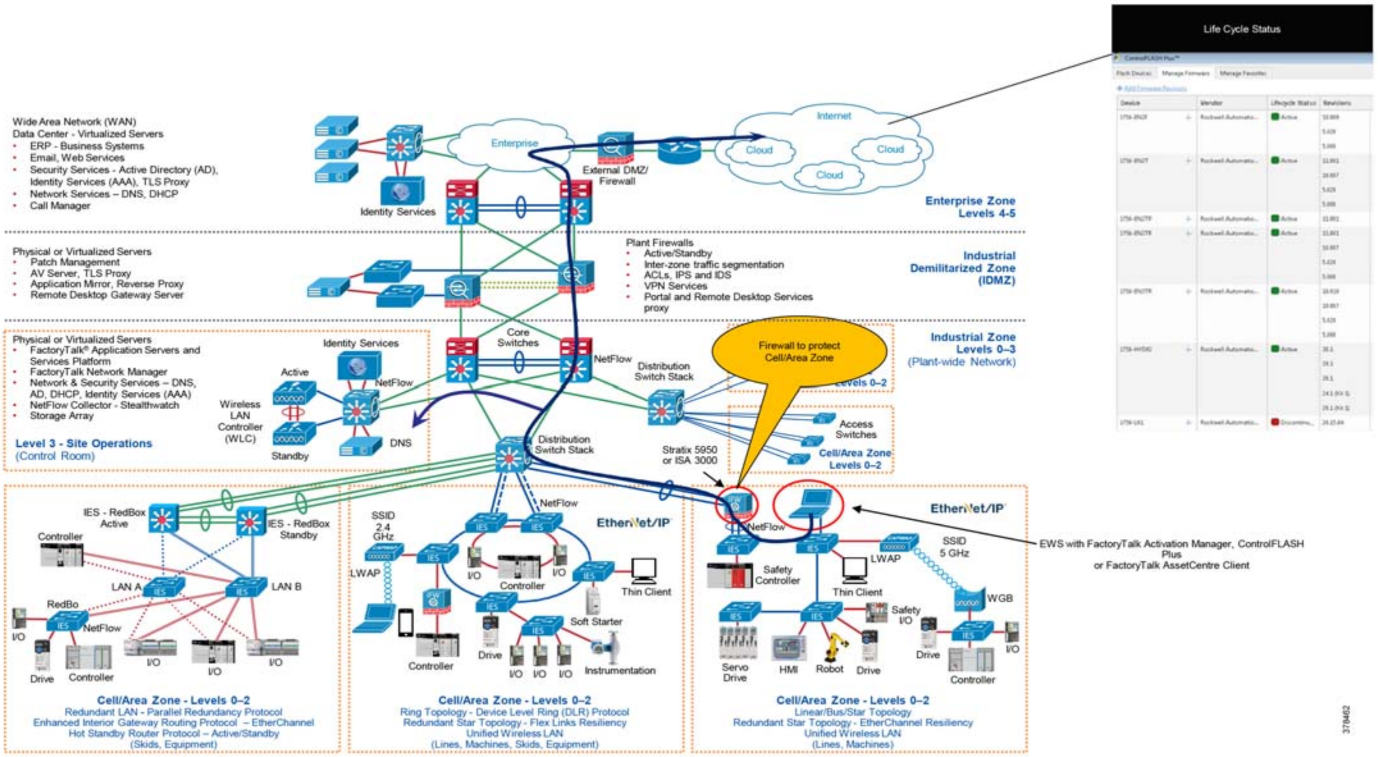

Life Cycle Status
DNS + TLS Proxy
Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Cisco Umbrella
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
FactoryTalk Network Manager
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
NetFlow Collector - Stealthwatch
Storage Array
Level 3 - Site Operations (Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Core Switches
NetFlow
Distribution Switch Stack
Firewall to protect Cell/Area Zone
Industrial Zone Levels 0–3 (Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0-2
Distribution Switch Stack
Stratix 5950 or ISA 3000
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
NetFlow
EtherNet/IP
LWAP
I/O
Controller
I/O
Thin Client
Soft Starter
Controller
Drive
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
NetFlow
EtherNet/IP
SSID 5 GHz
LWAP
Safety Controller
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus or FactoryTalk AssetCentre Client
378461

Gold Security Architecture

The Gold security architecture is depicted without a TLS proxy but still incorporates zoning with an IDMZ and Industrial Firewall(s). See Figure 2-4.

In this architecture, the TLS traffic between the cloud connected device and the cloud-based application is no longer inspected through the TLS proxy. However, firewalls can provide URL filtering and whitelisting/blacklisting to lower overall risk of the architecture. This presents the possibility of undetected malware traveling between the cloud-based application and the cloud connected device.

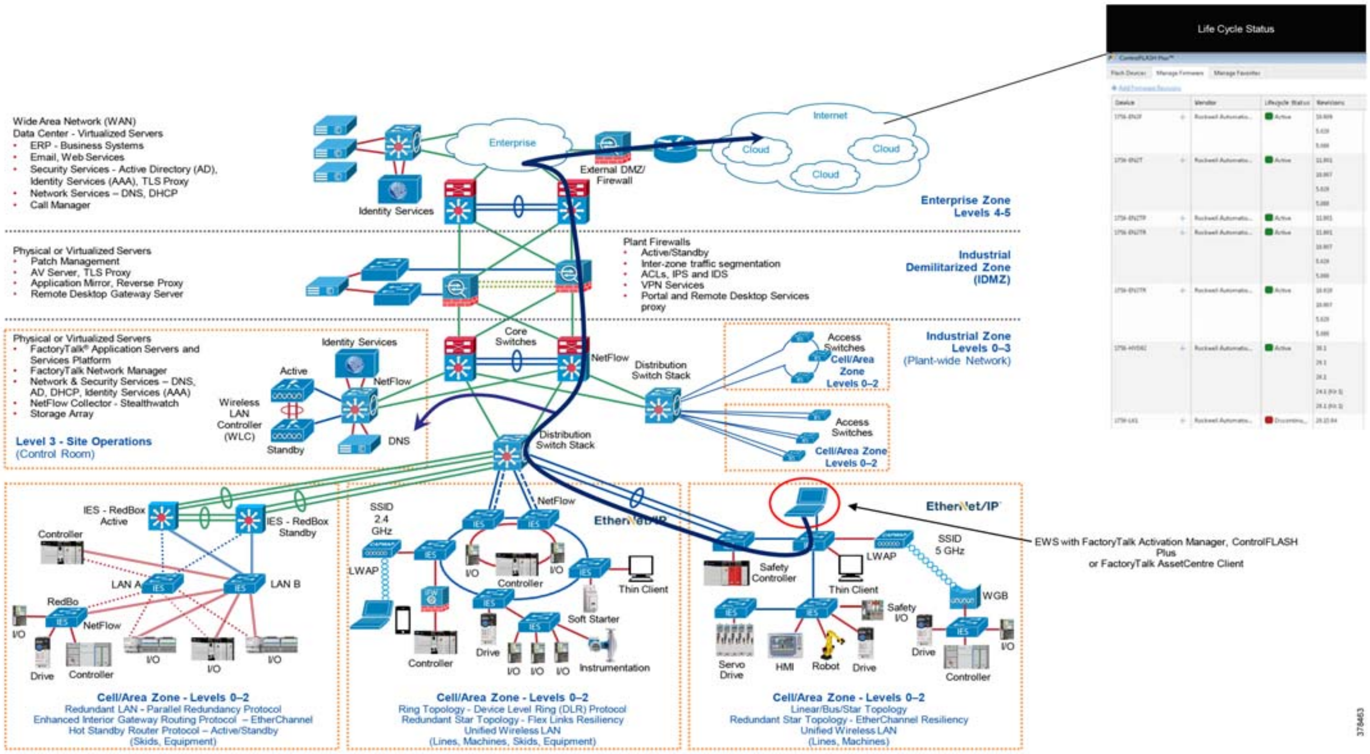
Figure 2-4 Gold Security CPwE Cloud Connectivity Use Case


Life Cycle Status
Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Core Switches
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Firewall to protect Cell/Area Zone
Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0–2
Stratix 5950 or ISA 3000
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Soft Starter
Controller
Drive
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
NetFlow
SSID 5 GHz
LWAP
Safety Controller
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus or FactoryTalk AssetCentre Client
378462

Silver Security Architecture

This architecture keeps the IDMZ concept with firewall(s) and replicated services to buffer (zoning) the Industrial Zone from the Enterprise Zone. The biggest difference between this architecture and the Gold architecture is there are no Industrial Firewall(s) acting as a security boundary (zoning) for the Cell/Area Zones. Industrial firewalls define smaller, more granular security zones that help enforce security policies to help protect the Industrial Zone from the ingress/egress point of the TLS traffic. See Figure 2-5.

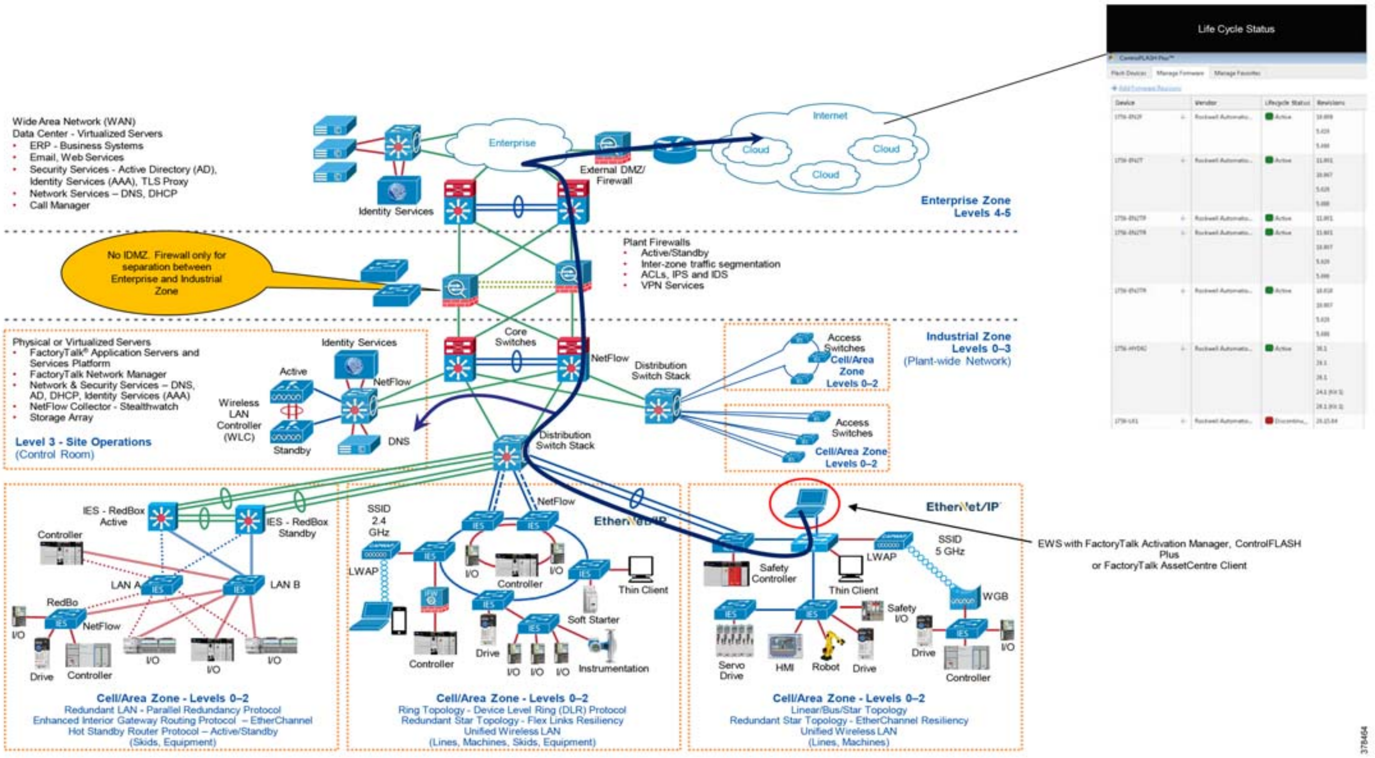
Figure 2-5 Silver Security CPwE Cloud Connectivity Use Case


Life Cycle Status
ControlFLASH Plus™
Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Core Switches
NetFlow
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
Distribution Switch Stack
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Controller
Drive
Soft Starter
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus
or FactoryTalk AssetCentre Client
378463

Bronze Security Architecture

This security architecture has the fewest defense layers of diverse industrial security best practices and is only recommended for manufacturers with a higher tolerance to risk. See Figure 2-6.

Figure 2-6 Bronze Security CPwE Cloud Connectivity Use Case


Life Cycle Status
Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
No IDMZ. Firewall only for separation between Enterprise and Industrial Zone
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
FactoryTalk Network Manager
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
NetFlow Collector - Stealthwatch
Storage Array
Level 3 - Site Operations (Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
DNS
Core Switches
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3 (Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBo
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Soft Starter
Controller
Drive
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
WGB
Safety I/O
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
EWS with FactoryTalk Activation Manager, ControlFLASH Plus or FactoryTalk AssetCentre Client
378464

While a firewall is used to define security boundaries, many security standards organizations, as well as Rockwell Automation and Cisco Systems, maintain that a firewall alone is not an acceptable layered security architecture for most risk averse manufacturers. When using a firewall, simple “permit” and “deny” rules define the traffic that is allowed through the firewall device. If the firewall permits traffic from a host in the Enterprise Zone to the Industrial Zone and either host is compromised, it is unlikely the firewall will deny or detect malicious traffic.

For further information about deploying firewalls, see:

- NIST 800-41 Guidelines on Firewalls and Firewall Policy:
  http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (document number ENET-TD002A-EN-P):
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf

Trusted versus Untrusted Security Zones

Security zones are established by grouping assets with common and related security requirements. These zones allow for technical and non-technical controls to be implemented to mitigate risk. Assets within the security zone are considered "trusted" while any assets outside the security zone are considered "untrusted".

This concept aligns with the IEC 62443-3-2 standard that discusses the zones and conduits model where the security zones represent assets with common security requirements and the conduits represent the communication channels that exist between the security zones.

When implementing a cloud connected device within the Industrial Zone, one must consider if the cloud connected device should be placed within its own security zone or within an existing security zone. For instance, if the cloud connected device is placed within a new security zone, communication to each IACS asset in another security zone must be considered "untrusted" and therefore a technical security control such as an industrial firewall should be implemented to limit and inspect the traffic to other security zones. If the cloud connected device is placed within an existing security zone, then the communications to IACS devices within the same security zone is considered "trusted".

Most open industrial protocols do not support device authentication and authorization, so the best method of risk mitigation is to create security zones and secure the communications between the security zones. With the inclusion of CIP Security to Rockwell Automations portfolio, the cloud connected device could be limited to the number of devices to which it has access. This can be used to enforce conduits within a security zone with devices that may have varying risk tolerance. Understanding device-to-device IACS communication is paramount when implementing technical controls because limiting traffic to known communication paths and protocols is the foundation for successfully implementing these types of controls.

Each designer and implementer must determine their security profile (through a risk assessment process) to determine the placement of the cloud connected device within the Industrial Zone.

Technology Considerations

There are different security technologies used within CPwE Cloud Connectivity to provide a scalable and multi-layered security architecture.

The following section briefly discusses the technologies described in the previous security architectures.

Transport Layer Security (TLS)

The first common technology used for communications between the FactoryTalk applications and the cloud applications is the IETF TLS. TLS provides encrypted communications between the two participating endpoints, which in CPwE Cloud Connectivity is the FactoryTalk application and the cloud hosted destination software. A consideration of the participating endpoints in TLS is ensuring a trust relationship between the devices accomplished using digital certificates. TLS traffic presents a challenge to monitor or inspect because the traffic is encrypted and therefore two commonly used methods are utilized to provide TLS proxy functionality:

- The first method is to provide a TLS proxy that is capable of decrypting, inspecting, and re-encrypting the traffic. This method can cause latency and the proxy could create a network bottleneck.
- An alternative method of providing the TLS monitoring is Cisco Encrypted Traffic Analytics (ETA), which monitors the encrypted traffic looking for malware without opening the packet. ETA inspects the initial data packet of the connection and monitors the sequence of packet lengths and times thereafter, which offers clues about traffic contents beyond the beginning of the encrypted flow. In general, ETA does not provide the same security features and benefits of using the Cisco Web Security Appliance.

For more information on the Cisco Web Security Appliance, Cisco Umbrella, and Cisco ETA see:

- Cisco Web Security Appliance:
  https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html
- Cisco Umbrella:
  https://umbrella.cisco.com
- Cisco Encrypted Traffic Analytics:
  - https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html
  - https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2019JUL.pdf

Industrial Demilitarized Zone (IDMZ) Proxy Technologies

A key tenant in the Platinum, Gold, and Silver architectures is the use of the IDMZ. This security zone provides a buffer between the Enterprise and Industrial Zone. The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services among the Industrial Zone, the Enterprise Zones, and the cloud. 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 Gateway (RDG) services.
- Use a Web Security Appliance with TLS proxy server capabilities.

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 covered in *Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide* (see URLs below).

In Platinum architectures (Figure 2-1) the TLS proxy is placed in the IDMZ to monitor TLS traffic between the cloud connected device and the cloud.

For a complete understanding of an IDMZ, see the *Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide*:

- Rockwell Automation site:
  http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
- Cisco site:
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

Proxy Servers and Capabilities

A proxy server resides between a trusted zone and untrusted zone, typically in the IDMZ. It provides additional protection by helping prevent direct communication between the clients within the trusted zone to servers within the untrusted zone. The goal of a proxy is to be the middle man (proxy) between clients and servers.

In essence, it works as an intermediate device that intercepts a request from an originator or client device then proceeds to make the connection on behalf of the client to the target or server device. Once the connection has been established by the target or server device, the proxy server continues to "proxy" the data stream until the connection is closed.

A Forward Proxy is configured to handle requests for a group of clients to an unknown, untrusted or arbitrary group of resources that are outside of their control.

A Reverse Proxy is where the proxy is intended to be on the same network as the HTTP(S) servers and its purpose is to serve up content for these HTTP(S) servers. In this scenario, the reverse proxy is helping protect the servers that are providing the content to the clients.

A TLS proxy is a forward or reverse proxy that uses a TLS connection to provide secure communications between an originator or client device and a target or server device. It can be dual homed to allow for the usage of the Web Cache Communication Protocol (WCCP) to redirect traffic to the TLS proxy from the IDMZ ASA firewalls.

Cisco Web Security Appliance (WSA)

The Cisco WSA is an all-in-one highly secure web gateway that brings strong protection, complete control, and investment value. It offers an array of competitive web security deployment options, each of which includes the market-leading global threat intelligence infrastructure from Cisco. The Cisco WSA correlates threats collected from their network to produce a behavior score, known as a web-reputation score, on which to act. It applies and enforces web-reputation scores on parent sites and subsites. The Cisco WSA defends against malware and advanced persistent threats using multiple layers of anti-malware technologies and intelligence from Cisco Talos updated every three to five minutes. Every piece of web content accessed from HTML to images to Flash files is analyzed using security and context-aware scanning engines. Cisco WSA analyzes traffic in real time, breaks it into functional elements, and pushes elements to best-designed malware engines for inspection while maintaining high processing speeds.

Cisco Advanced Malware Protection (AMP)

Cisco AMP is an additionally licensed feature available to all Cisco WSA devices. AMP is a comprehensive malware-defeating solution that provides malware detection and blocking, continuous analysis, and retrospective alerting. AMP augments the malware detection and blocking capabilities already offered in the Cisco WSA with enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. Cisco AMP provides the ability to sandbox PDF, Microsoft Office software, archived/compressed files, and Windows portable executable file. The Cisco AMP feature was not tested as part of this CRD.

WSA Proxy Modes—Transparent and Explicit Proxies

Since the goal of a proxy is to be the middle man between HTTP(S) clients and HTTP(S) servers the Cisco Web Security Appliance (WSA), as a web proxy, will have two sets of TCP sockets per client request:

- Client->WSA
- WSA->Origin server

The WSA can be configured for “transparent” or “forward” from its web user interface. This is slightly misleading, as this is really “transparent” or “explicit” mode, both of which are forward proxy deployments. Reverse proxy is where the proxy is intended to be on the same network as the HTTP(S) servers and its purpose is to serve up content for these HTTP(S) servers.

The main difference between transparent and forward mode on the WSA is that in transparent mode, the WSA will respond to both transparent and explicit HTTP(S) requests. Whereas in explicit, the WSA ONLY responds to explicit HTTP(S) requests. For transparent redirection, the Web Cache Communication Protocol (WCCP) is used to intercept and forward traffic.

The WSA will always send its upstream request as a transparent style request, since the WSA is acting as its own client, UNLESS the WSA is configured to specifically use an explicit upstream proxy such as a proxy in the Enterprise Zone.

The ability of the WSA HTTP proxy to obtain the request from the client can be defined as one of two ways: Transparent or Explicit.

Each of these deployments have several specific configuration requirements:

1. Explicit proxies require that each workstation and web browser have its proxy settings pointing to the proxy server. All web traffic unless otherwise specified is sent to the proxy.
   a. For HTTPS traffic, the proxy servers certificate must be installed in the workstations trust store
2. Transparent proxies require another technology to redirect traffic to the proxy such as Policy Based Routing (PBR) or Web Cache Communication Protocol (WCCP). Only traffic that passes through the redirecting device and is configured to be redirected is sent to the proxy.
   a. For HTTPS traffic, the proxy servers' certificate must be installed in the workstations trust store

There are a few differences between explicit and transparent HTTP(S) requests:

1. An explicit request has a destination IP address of the configured proxy. A transparent request has a destination IP address of the intended web server (DNS resolved by the client).
   a. Depending on which deployment is being used, this item should be considered when configuring firewalls along the communication path
2. When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with its own IP information back to the client.
3. The URI for a transparent request does not contain the protocol with the host:
   - Transparent—GET / HTTP/1.1
   - Explicit—GET http://www.google.com/ HTTP/1.1

Both will contain an HTTP Host header that specifies the DNS host.

Web Cache Communication Protocol (WCCP)

The WCCP specifies interactions between one or more routers, layer 3 switches or firewalls and one or more web proxies. Regarding the Platinum Architecture, WCCP is enabled on the Ingress interface of the IDMZ Firewall but can also be utilized on most Layer 3 switches that provide full routing services. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic that flow through a group of routers. The selected traffic is redirected to a group of web proxies in order to optimize resource usage and lower response times.

The flow of work for redirection has these steps:

1. The user enters a URL into a browser.
2. The URL is forwarded to domain name system (DNS) for address resolution.
3. The URL is resolved to the IP address of the web server.
4. The client initiates a connection to the server with a SYN request.
5. On the device, the WCCP web proxy service intercepts the HTTP(S) request (TCP port 80 or 443) and redirects the request to proxies via GRE:

- If using HTTPS the proxy requires a certificate exchange between the proxy and the client to transparently proxy HTTPS. This requires that the proxy's certificate be imported into the trusted store of each web browser on each workstation. Self-signed certificates were evaluated as part of the CPwE testing using the Cisco WSA.
- If there is a cache hit, the proxy responds to the original GET with the requested content and uses the source IP address of the origin server in the response pack.
- If the requested content is not already stored on the proxy, there is a cache miss:
  - The proxy establishes a connection to the origin server, uses its own IP address as the source, and sends the HTTP GET.
  - The server responds to the proxy with content.
  - The proxy writes a copy of the cacheable content to the disk.

WCCP Service Groups

Once connectivity is established, the device and web proxies form service groups to handle the redirection of traffic whose characteristics are part of the service group definition.

A web proxy transmits a WCCP2_HERE_I_AM message to each WCCP enabled device in the group at HERE_I_AM_T (10) second intervals to join and maintain its membership in a service group. The message may be by unicast to each device or by multicast to the configured service group multicast address. Multicast functionality was not evaluated as a part of the CPwE testing.

- The Web-Cache Identity Info component in the WCCP2_HERE_I_AM message identifies the web proxy by IP address.
- The Service Info component of the WCCP2_HERE_I_AM message identifies and describes the service group in which the web proxy wishes to participate.
  - For the testing completed as a part of the CPwE a user-configurable Service Group was created.

Table 2-2 Service Groups

Service Group	Type	Description
Service 0	Web-cache	Web caching service that permits the device to redirect HTTP traffic to the proxy.
Service 53	DNS	DNS caching service that permits the device to redirect DNS client requests transparently to the proxy.
Service 60	FTP-native	Caching service that permits the device to redirect FTP native requests transparently to a single port on the proxy.
Service 70	https-cache	Caching service that permits the device to intercept port 443 TCP traffic and redirect this HTTPS traffic to the proxy.
Service 80	rtsp	Media streaming service that permits the device to redirect Real Time Streaming Protocol (RTSP) client requests to a single port on the proxy.
Service 81	mmst	Media caching service that permits the device to use TCP-based Microsoft Media Server (MMST) redirection to route Windows Media Technology (WMT) client requests to TCP port 1755 on the proxy.
Service 82	mmsu	Media caching service that permits the device to use User Datagram Protocol (UDP)-based Microsoft Media Server (MMSU) redirection to route WMT client requests to UDP port 1755 on the proxy.
Service 83	wmt-rtsp	Media streaming service that allows the device to redirect RTSP requests from Windows Media Service 9 clients to UDP port 5005 on the the CE.
Service 90-97	user configurable	User-defined WCCP services that support up to eight ports for each WCCP service. When you configure these user-defined services, you must specify whether to redirect the traffic to the HTTP caching application, to the HTTPS application, or to the streaming application on the proxy.

Table 2-2 Service Groups

Service Group	Type	Description
Service 98	custom-web-cache	Caching service that permits the device to transparently redirect HTTP traffic to the proxy on multiple ports other than port 80.
Service 99	reverse-proxy	Caching service that permits the device to redirect HTTP reverse proxy traffic to the proxy on port 80.

A service group is identified by Service Type and Service ID. There are two types of service groups:

- Well-known services
- Dynamic services

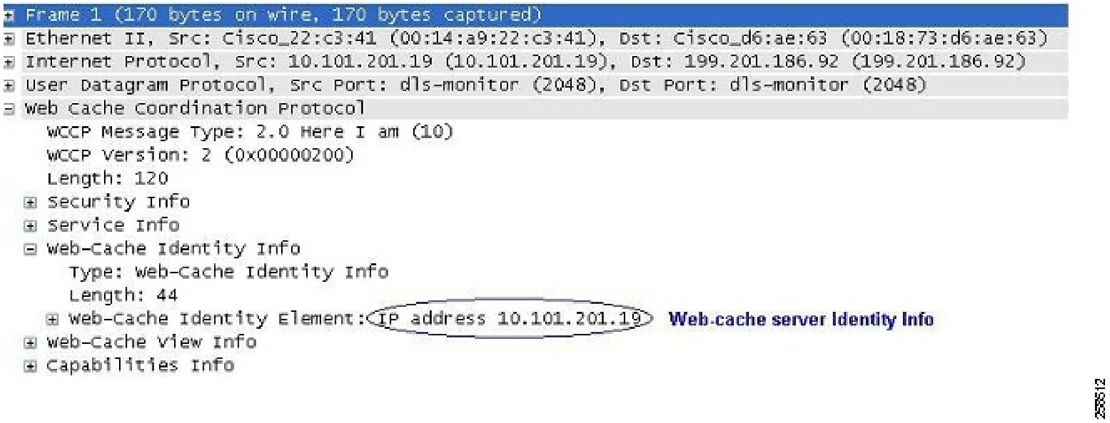
Well-known services are known by both the redirecting device and web caches and do not require a description other than a Service ID.

In contrast, dynamic services must be described to a redirecting device. The device may be configured to participate in a particular dynamic service group, identified by Service ID, without any knowledge of the characteristics of the traffic associated with that service group. The traffic description is communicated to the device in the WCCP2_HERE_I_AM message of the first web proxy to join the service group. A web proxy uses the Protocol, Service Flags, and Port fields of the Service Info component to describe a dynamic service. Once a dynamic service has been defined, the device discards any subsequent WCCP2_HERE_I_AM message that contains a conflicting description. The device also discards a WCCP2_HERE_I_AM message that describes a service group for which it has not been configured.

The numbers 0 to 254 are dynamic services, and the web cache service is a standard, or well-known, service. What this means is that when the web cache service is specified, the WCCP v2 protocol has predefined that TCP destination port 80 traffic is to be redirected. For the numbers 0 to 254, each number represents a dynamic service group. The WCCP proxies are to define a set of protocols and ports that are to be redirected for each service group. Then, when the device is configured with that same service group number (wccp 0 ... or wccp 1 ...), the device performs redirection on the specified protocols and ports as directed by the device.

Figure 2-7 is an example that shows Web-Cache Identity Info.

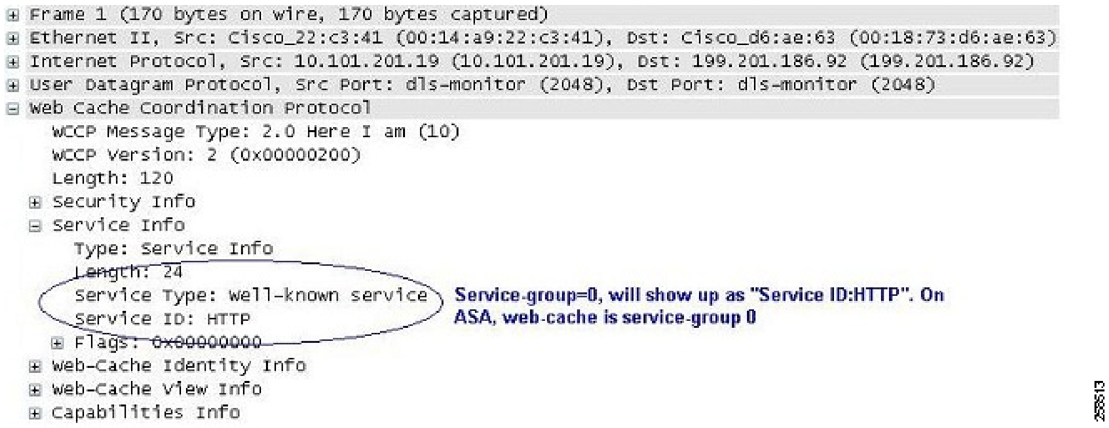
Figure 2-7 Web-Cache Identity Info



```
⊞ Frame 1 (170 bytes on wire, 170 bytes captured)
⊞ Ethernet II, Src: Cisco_22:c3:41 (00:14:a9:22:c3:41), Dst: Cisco_d6:ae:63 (00:18:73:d6:ae:63)
⊞ Internet Protocol, Src: 10.101.201.19 (10.101.201.19), Dst: 199.201.186.92 (199.201.186.92)
⊞ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
⊟ Web Cache Coordination Protocol
    WCCP Message Type: 2.0 Here I am (10)
    WCCP Version: 2 (0x00000200)
    Length: 120
  ⊞ Security Info
  ⊞ Service Info
  ⊟ Web-Cache Identity Info
      Type: Web-Cache Identity Info
      Length: 44
    ⊞ Web-Cache Identity Element: IP address 10.101.201.19
  ⊞ Web-Cache View Info
  ⊞ Capabilities Info
```

Figure 2-8 is an example that shows that the Web-Cache is part of service group 0.

Figure 2-8 Web-Cache Part of Service Group 0

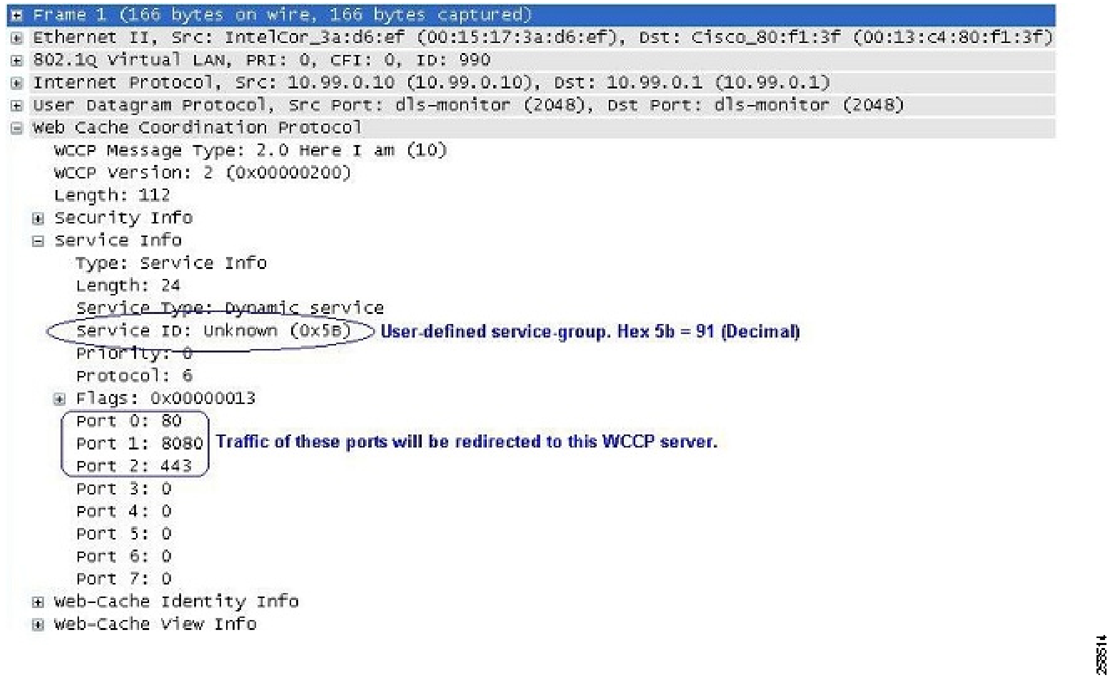


```
⊞ Frame 1 (170 bytes on wire, 170 bytes captured)
⊞ Ethernet II, Src: Cisco_22:c3:41 (00:14:a9:22:c3:41), Dst: Cisco_d6:ae:63 (00:18:73:d6:ae:63)
⊞ Internet Protocol, Src: 10.101.201.19 (10.101.201.19), Dst: 199.201.186.92 (199.201.186.92)
⊞ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
⊟ Web Cache Coordination Protocol
    WCCP Message Type: 2.0 Here I am (10)
    WCCP Version: 2 (0x00000200)
    Length: 120
  ⊞ Security Info
  ⊟ Service Info
      Type: Service Info
      Length: 24
      Service Type: Well-known service
      Service ID: HTTP
    ⊞ Flags: 0x00000000
  ⊞ Web-Cache Identity Info
  ⊞ Web-Cache View Info
  ⊞ Capabilities Info
```

Service-group=0, will show up as "Service ID:HTTP". On ASA, web-cache is service-group 0

Figure 2-9 is an example that shows a Web-Cache server as part of custom service group 91 and the ports whose traffic is redirected to the server.

Figure 2-9 Web-Cache Server Part of Service Group 91 and Redirected Ports



```
⊞ Frame 1 (166 bytes on wire, 166 bytes captured)
⊞ Ethernet II, Src: IntelCor_3a:d6:ef (00:15:17:3a:d6:ef), Dst: Cisco_80:f1:3f (00:13:c4:80:f1:3f)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 990
⊞ Internet Protocol, Src: 10.99.0.10 (10.99.0.10), Dst: 10.99.0.1 (10.99.0.1)
⊞ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
⊟ Web Cache Coordination Protocol
    WCCP Message Type: 2.0 Here I am (10)
    WCCP Version: 2 (0x00000200)
    Length: 112
  ⊞ Security Info
  ⊟ Service Info
      Type: Service Info
      Length: 24
      Service Type: Dynamic service
      Service ID: Unknown (0x5B)
      Priority: 0
      Protocol: 6
    ⊞ Flags: 0x00000013
      Port 0: 80
      Port 1: 8080
      Port 2: 443
      Port 3: 0
      Port 4: 0
      Port 5: 0
      Port 6: 0
      Port 7: 0
  ⊞ Web-Cache Identity Info
  ⊞ Web-Cache View Info
```

User-defined service-group. Hex 5b = 91 (Decimal)

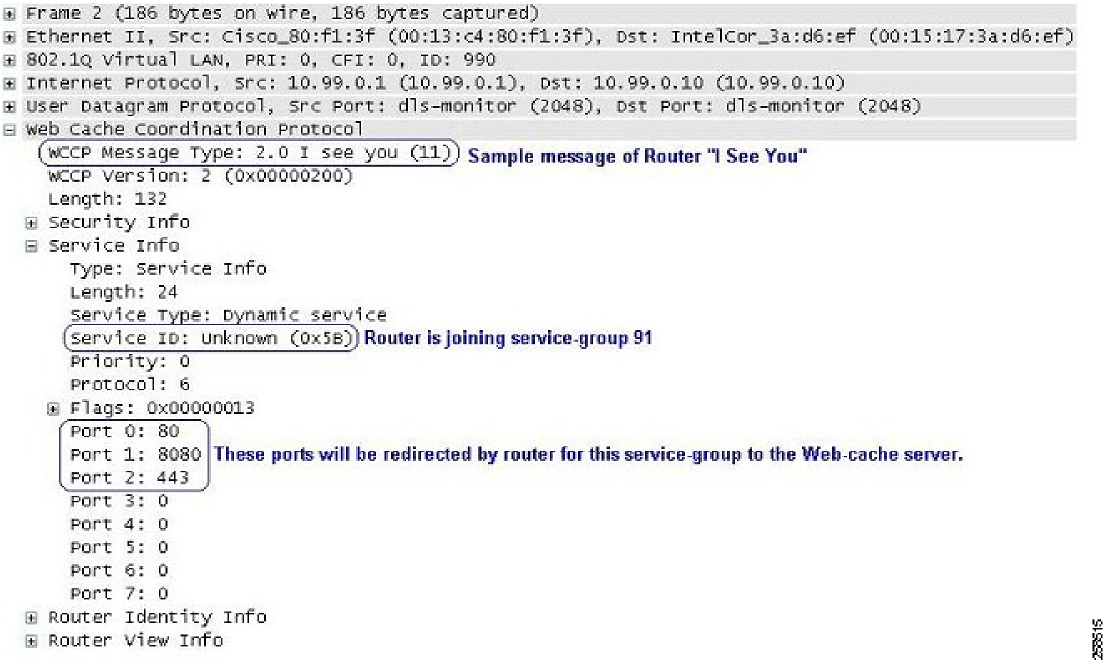
Traffic of these ports will be redirected to this WCCP server.

The device responds to a WCCP2_HERE_I_AM message with a WCCP2_I_SEE_YOU message.

- If the WCCP2_HERE_I_AM message was unicast, the router responds immediately with a unicast WCCP2_I_SEE_YOU message.
- If the WCCP2_HERE_I_AM message was multicast, the router responds with the scheduled multicast WCCP2_I_SEE_YOU message for the service group.

Figure 2-10 is an example of the device’s “I See You” message, which shows that the router joins service group 91 (a custom service group) and redirects ports 80, 8080, and 443 to the web proxy server.

Figure 2-10 "I See You" Message



```
⊞ Frame 2 (186 bytes on wire, 186 bytes captured)
⊞ Ethernet II, Src: Cisco_80:f1:3f (00:13:c4:80:f1:3f), Dst: IntelCor_3a:d6:ef (00:15:17:3a:d6:ef)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 990
⊞ Internet Protocol, Src: 10.99.0.1 (10.99.0.1), Dst: 10.99.0.10 (10.99.0.10)
⊞ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
⊟ Web Cache Coordination Protocol
    WCCP Message Type: 2.0 I see you (11)
    WCCP Version: 2 (0x00000200)
    Length: 132
  ⊞ Security Info
  ⊟ Service Info
      Type: Service Info
      Length: 24
      Service Type: Dynamic service
      Service ID: Unknown (0x5B)
      Priority: 0
      Protocol: 6
    ⊞ Flags: 0x00000013
      Port 0: 80
      Port 1: 8080
      Port 2: 443
      Port 3: 0
      Port 4: 0
      Port 5: 0
      Port 6: 0
      Port 7: 0
  ⊞ Router Identity Info
  ⊞ Router View Info
```

Sample message of Router "I See You"

Router is joining service-group 91

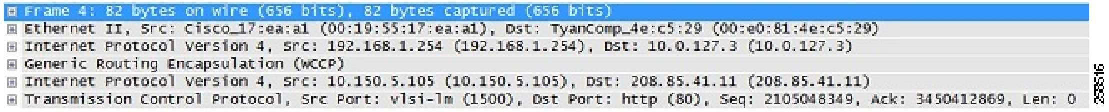
These ports will be redirected by router for this service-group to the Web-cache server.

When you redirect traffic using WCCP, keep the following behavior in mind:

- The device selects the highest IP address configured on any interface as the WCCP router ID. This address is used to establish a GRE tunnel with the device. When the device redirects packets to the WCCP-enabled device, the device sources the redirect from the router ID IP address (even if it is sourced out another interface) and encapsulates the packet in a GRE header. For WCCP to work, the interface whose IP address is chosen as the router ID must be in the UP state and there must be a route to the device.

Figure 2-11 is an example of a GRE packet.

Figure 2-11 GRE Packet



```
⊞ Frame 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
⊞ Ethernet II, Src: Cisco_17:ea:a1 (00:19:55:17:ea:a1), Dst: TyanComp_4e:c5:29 (00:e0:81:4e:c5:29)
⊞ Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 10.0.127.3 (10.0.127.3)
⊞ Generic Routing Encapsulation (WCCP)
⊞ Internet Protocol Version 4, Src: 10.150.5.105 (10.150.5.105), Dst: 208.85.41.11 (208.85.41.11)
⊞ Transmission Control Protocol, Src Port: vlsi-lm (1500), Dst Port: http (80), Seq: 2105048349, Ack: 3450412869, Len: 0
```

- An inbound access rule always takes higher priority over WCCP. For example, if an interface ACL does not permit a client to communicate with a server, then the matching traffic is simply dropped, it is not redirected.
- TCP intercept, authorization, URL filtering, inspection engines, and IPS features are not applied to a redirected flow of traffic.
- When a device cannot service a request and returns a packet to the redirecting device, then the contents of the traffic flow is subject to all the other configured features of the device.
- If you have two WCCP services and they use two different redirection ACLs that overlap and match the same packets (with a deny or a permit action), the packets behave according to the first service group found and installed rules. The packets are not passed through all service groups.

Limitations

Note These limitations may be based on the device. The limitations below are from a Cisco ASA.

- WCCP redirection is supported only on the ingress of an interface. The only topology that the ASA supports is when client and proxy are behind the same interface of the ASA and the proxy can directly communicate with the client, without going through the device.
- Multiple routers in a service group.
- Multicast WCCP.
- The Layer 2 redirect method.
- WCCP source address spoofing.
- Wide Area Application Services (WAAS) devices.
- AAA for network access does not work in combination with WCCP.
- Does not support IPv6 traffic for redirection.
- When the ASA determines that a packet needs redirection, it ignores TCP state tracking, TCP sequence number randomization, and NAT on these traffic flows.
- WCCP does not support ACLs that include a user, user group, service group, or a fully qualified domain name object.
- The maximum number of services, including those specified with a dynamic service identifier is 256.

Industrial Firewall (IFW)

Another key tenant in the Platinum and Gold architectures is the use of Industrial Firewalls to enforce security policies within the Cell/Area Zone. In some cases, the cloud connected device will communicate with Industrial Zone IACS assets to gather information such as device inventory and verify lifecycle status with the cloud. The Industrial Firewall can be configured to constrain the communication of the cloud connected device to appropriate IACS devices. The Industrial Firewall with CIP deep packet inspection (DPI) can also be configured to limit the types of CIP commands that can be sent to a device. The placement of the Industrial Firewall will dictate the amount of security granularity one can achieve with this device.

For a complete understanding of an IFW, see the *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:

- Rockwell Automation site:
  http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
- Cisco site:
  http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html

Cloud Connected Devices to Cloud Applications Test Cases

CPwE Cloud Connectivity tested the following items:

- Cloud connected devices using FactoryTalk AssetCentre and ControlFLASH Plus connecting to the Rockwell Automation cloud API.

  - The Rockwell Automation Cloud API is a cloud residing application providing lifecycle status information.
- FactoryTalk Activation Manager’s ability to reach out to the cloud for activation validity purposes such as Get New Activation, Rehost and Renew.
- IDMZ and Industrial firewall configurations as well as the Cisco WSA configurations while positioned within the IDMZ.

Platinum Security Architecture-Cloud Connected Devices Use Case

The Platinum security reference architecture that was tested contained the following key components that were configured and functionally verified:

- Cisco Web Security Appliance
- FactoryTalk AssetCentre Server and Client
- ControlFLASH Plus connecting to various Rockwell Automation assets
- FactoryTalk Activation Manager
- Centralized Activation Server
- Standalone FactoryTalk Activation Manager client
- DNS server required to resolve the various cloud IP Addresses.
- Allen-Bradley Stratix 5950 Industrial Firewall—This firewall was configured to allow DNS requests and TLS traffic to the Cloud.
- IDMZ ASA firewalls—This firewall was configured to allow DNS requests and TLS traffic to the Cloud.

Gold Security Architecture—Cloud Connected Devices Use Case

The gold security reference architecture that was tested contained the following key components that were configured and functionally verified:

- FactoryTalk AssetCentre Server and Client
- ControlFLASH Plus connecting to various Rockwell Automation assets
- FactoryTalk Activation Manager
- Centralized Activation Server
- Standalone FactoryTalk Activation Manager client
- DNS serverr equired to resolve the various cloud IP Addresses.
- Allen-Bradley Stratix 5950 Industrial Firewall—This firewall was configured to allow DNS requests and TLS traffic to the Cloud.
- IDMZ ASA firewalls—This firewall was configured to allow DNS requests and TLS traffic to the Cloud.

CHAPTER 3

Configuring the Infrastructure

This chapter provides an overview of the configuration used in testing to validate the functionality of the Cisco WSA. This chapter is not intended to provide step-by-step procedures to configure the Cisco WSA because of the variability in network architectures and the potential impact on device configuration. However, this chapter discusses specific items related to FactoryTalk applications, their interaction with the Cisco WSA, and the steps required to help ensure that they will interoperate with the Cisco WSA and efficiently complete their functions.

Cisco Web Security Appliance

System Setup Wizard

From an out-of-box state, the most efficient way to complete the setup of the Cisco WSA is to use the System Setup Wizard. While this design guide does not describe in detail the System Setup Wizard, it does provide important information to be aware of during this phase of Cisco WSA deployment. Important items from the System Setup Wizard that affect the functionality of the Cisco WSA and FactoryTalk Applications are defined in the sections following Table 3-1.

Table 3-1 Network and System Settings

Property	Description
Default System Hostname	The system hostname is the fully-qualified hostname used to identify the appliance in the following areas: • Command line interface (CLI) • System alerts • End-user notification and acknowledgment pages • When forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.
DNS Server(s)	• Use the Internet's Root DNS Servers—You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network. **Note**: Internet root DNS servers will not resolve local host names. If you need the appliance to perform this action, you must use a local DNS server or add the appropriate static entries to the local DNS using the CLI. • Use these DNS Servers—Provide the address(es) for the local DNS server(s) that the appliance can use to resolve host names.
NTP Server	The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet. The default is time.sco.cisco.com.
Time Zone	Provide time-zone information for location of the appliance; affects time stamps in message headers and log files.
Appliance Mode of Operation	• Standard—Used for standard on-premise policy enforcement. • Cloud Web Security Connector—Used primarily to direct traffic to the Cloud Web Security service from Cisco for policy enforcement and threat defense. • Hybrid Web Security—Used in conjunction with the Cloud Web Security service from Cisco for cloud and on-premise policy enforcement and threat defense.

Network and Network Context

Note When you use the Web Security Appliance in a network that contains another proxy server, it is recommended that you place the Web Security Appliance downstream from the proxy server, closer to the clients. A system with multiple proxies was not tested and validated as a part of this design guide.

Table 3-2 Network and System Settings

Property	Description
Is there another web proxy on your network?	Is there another proxy on your network such that traffic must pass through it? Will it be upstream of the Web Security Appliance? If yes for both points, select the checkbox. This allows you to create a proxy group for one upstream proxy. You can add more upstream proxies later. This was not tested or validated as a part of this design guide.
Proxy group name	A name used to identify the proxy group on the appliance.
Address	The hostname or IP address of the upstream proxy server.
Port	The port number of the upstream proxy server.

Network and Network Interfaces and Wiring

You can use the host name specified here when connecting to the appliance management interface (or in browser proxy settings if M1 [Management] is used for proxy data), but you must register it in your organization's DNS.

Table 3-3 Network and Network Interfaces and Wiring

Setting	Description
Ethernet port	(Optional) **Check Use M1 port for management only** if you want to use a separate port for data traffic. If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. You must also define different routes for management and data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic. You can enable and configure the P1 port only in the System Setup Wizard. If you want to enable the P2 interface, you must do this after finishing the System Setup Wizard.
IP Address and Netmask	The IP address and network mask to use when managing the Web Security appliance on this network interface.
Hostname	The host name to use when managing the Web Security appliance on this network interface.

Network and Routes for Management and Data Traffic

Note If you enable "Use M1 port for management only", this configuration section will have separate configuration options for management and data traffic; otherwise one joint configuration section will be shown.

Table 3-4 Network and Routes for Management and Data Traffic

Property	Description
Default Gateway	The default gateway IP address to use for traffic through the Management and Data interfaces.
Static Routes Table	Optional static routes for management and data traffic. Multiple routes can be added. • Name—A name used to identify the static route. • Internal Network—The IPv4 address for this route's destination on the network. • Internal Gateway—The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Network and Transparent Connection Settings

Note By default, the Cloud Connector is deployed in transparent mode, which requires a connection to a Layer 4 switch or a version 2 WCCP router. The version 2 WCCP router was tested and validated as a part of this design guide.

Table 3-5 Network and Transparent Connection Settings

Property	Description
Layer 4 Switch or No Device	Specifies that the Web Security appliance is connected to a Layer 4 switch for transparent redirection or that no transparent redirection device is used and clients will explicitly forward requests to the appliance.
WCCP v2 Router	Specifies that the Web Security Appliance is connected to a version 2 WCCP-capable router. If you connect the appliance to a version 2 WCCP router, you must create at least one WCCP service. You can enable the standard service on this screen or after the System Setup Wizard is finished, where you can also create multiple dynamic services. When you enable the standard service, you can also enable router security and enter a passphrase. The passphrase used here must be used on all appliances and WCCP routers within the same service group. A standard service type (also known as the "web-cache" service) is assigned a fixed ID of zero, a fixed redirection method (by destination port), and a fixed destination port of 80. A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options.

Security and Security Settings

Table 3-6 Security and Security Settings

Option	Description
Global Policy Default Action	Specifies whether to block or monitor all web traffic by default after the System Setup Wizard completes. You can change this behavior later by editing the Protocols and User Agents settings for the Global Access Policy. The default setting is to monitor traffic.
Layer 4 Traffic Monitor	Specifies whether the Layer 4 Traffic Monitor should monitor or block suspected malware by default after the System Setup Wizard completes. You can change this behavior later. The default setting is to monitor traffic.

Table 3-6 Security and Security Settings

Option	Description
Acceptable Use Controls	Specifies whether to enable Acceptable Use Controls. If enabled, Acceptable Use Controls allow you to configure policies based on URL filtering. They also provide application visibility and control, and related options such as safe search enforcement. The default setting is enabled.
Reputation Filtering	Specifies whether to enable Web Reputation filtering for the Global Policy Group. Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. The default setting is enabled.
Malware and Spyware Scanning	Specifies whether to enable malware and spyware scanning using Webroot, McAfee, or Sophos. The default setting is that all three options are enabled. Most security services will be automatically enabled/disabled to match the services normally available for cloud policies. Similarly, policy-related defaults will not be applicable. At least one scanning option must be enabled. If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware. You can further configure malware scanning after you finish the System Setup Wizard.
Cisco Data Security Filtering	Specifies whether to enable Cisco Data Security Filters. If enabled, the Cisco Data Security Filters evaluate data leaving the network and allow you to create Cisco Data Security Policies to block particular types of upload requests. The default setting is enabled.

Interface Configuration

The Cisco WSA that was tested and validated was configured in a dual-homed type of architecture (Figure 3-1). Overall three interfaces and IP addresses were dedicated to the device:

- M1 Interface and IP address

  This is intended for management of the Cisco WSA only and should be out-of-band.

- P1 Interface and IP address

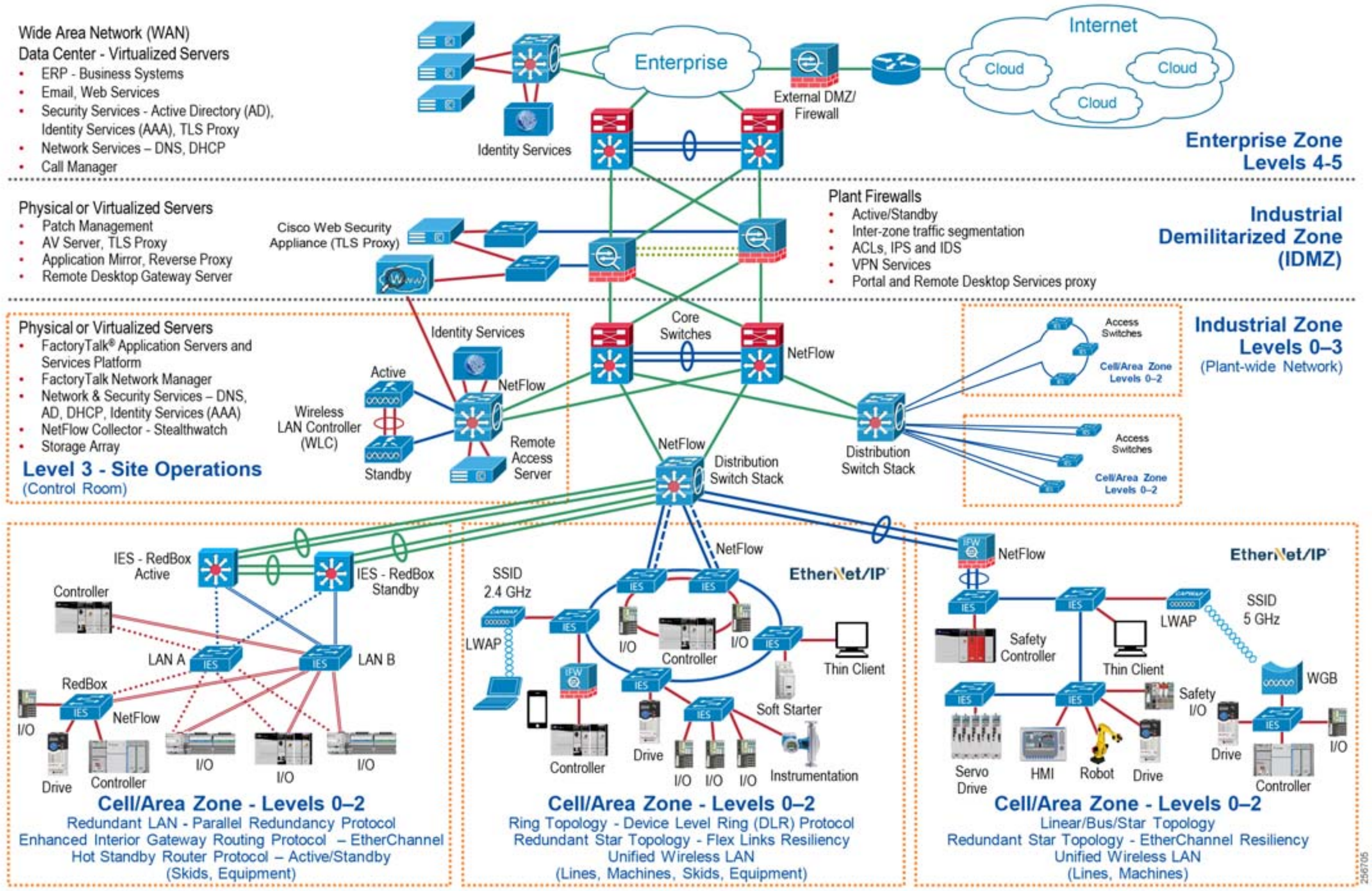
  This interface resides in the same subnet as the firewall interface in the Industrial Zone and should be Layer 2 accessible from the IDMZ firewall. All WCCP traffic is forwarded to this interface.

- P2 Interface and IP address

  This interface resides in the IDMZ and is the internet facing interface of the Cisco WSA. Once traffic has been analyzed and approved, it is sent via P2.

Once the three interfaces are configured and defined, routing tables for each interface can be configured to ensure that the desired connectivity is achieved. Typically, a default route on the P2 or IDMZ interface is used to help ensure that cloud and web traffic can reach its destination on the internet.

Figure 3-1 Cisco WSA Network Architecture

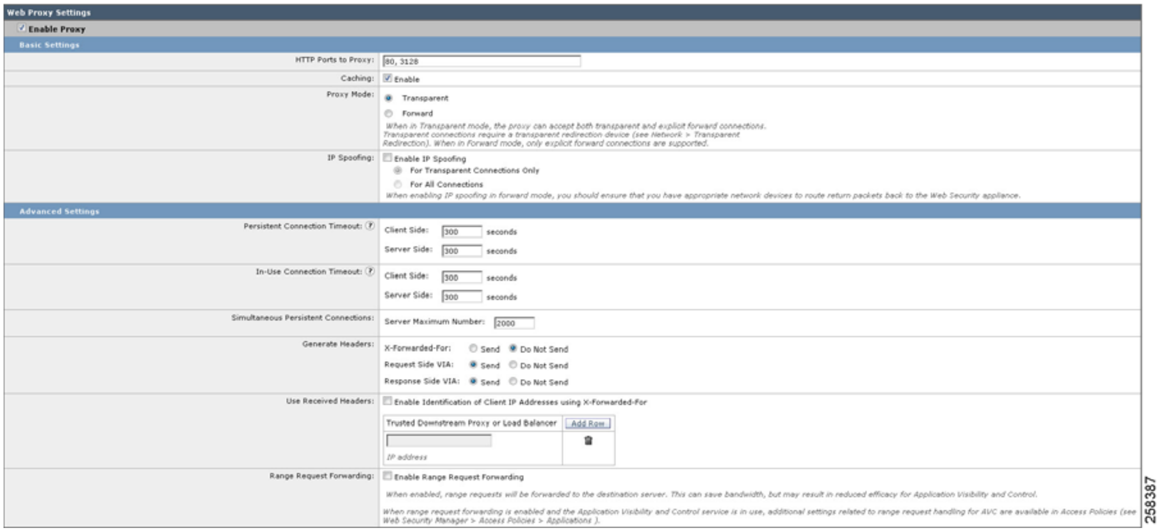

Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Cisco Web Security Appliance (TLS Proxy)
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Core Switches
NetFlow
Active
Wireless LAN Controller (WLC)
Standby
NetFlow
Remote Access Server
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0–3
(Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
NetFlow
SSID 2.4 GHz
EtherNet/IP
LWAP
I/O
Controller
I/O
Thin Client
Soft Starter
Controller
Drive
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
NetFlow
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
WGB
Safety I/O
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
256705

Web Proxy Configuration

The configuration of the proxy stays in a mostly default state and can be accessed and viewed by navigating to **Security Services**->**Web Proxy**. The HTTP ports that are to be proxied by the Cisco WSA can be defined in the configuration. Additionally, a proxy mode must be selected depending on the type of deployment that will be used with the Cisco WSA. The types of deployment, Transparent and Forward, were defined and discussed in Chapter 2, "CPwE Cloud Connectivity Design Considerations." Transparent and Forward proxy modes were both tested and validated, however there is a difference in the overall configuration of the network and end devices between the two proxy modes. This chapter focuses on Transparent Mode configuration, but notes which configurations are not required for Forward Mode deployments. Figure 3-2 shows the Web Proxy Settings that were used during testing.

Caching is a feature that is typically used to attempt to reduce traffic and resources used on the network by saving a version of the webpage and providing it to clients. For testing and validation purposes, the caching feature was enabled but is not required.

Figure 3-2 Web Proxy Settings



Web Proxy Settings

☑ Enable Proxy

Basic Settings

HTTP Ports to Proxy:	80, 3128
Caching:	☑ Enable
Proxy Mode:	● Transparent ○ Forward *When in Transparent mode, the proxy can accept both transparent and explicit forward connections. Transparent connections require a transparent redirection device (see Network > Transparent Redirection). When in Forward mode, only explicit forward connections are supported.*
IP Spoofing:	□ Enable IP Spoofing ● For Transparent Connections Only ○ For All Connections *When enabling IP spoofing in forward mode, you should ensure that you have appropriate network devices to route return packets back to the Web Security appliance.*

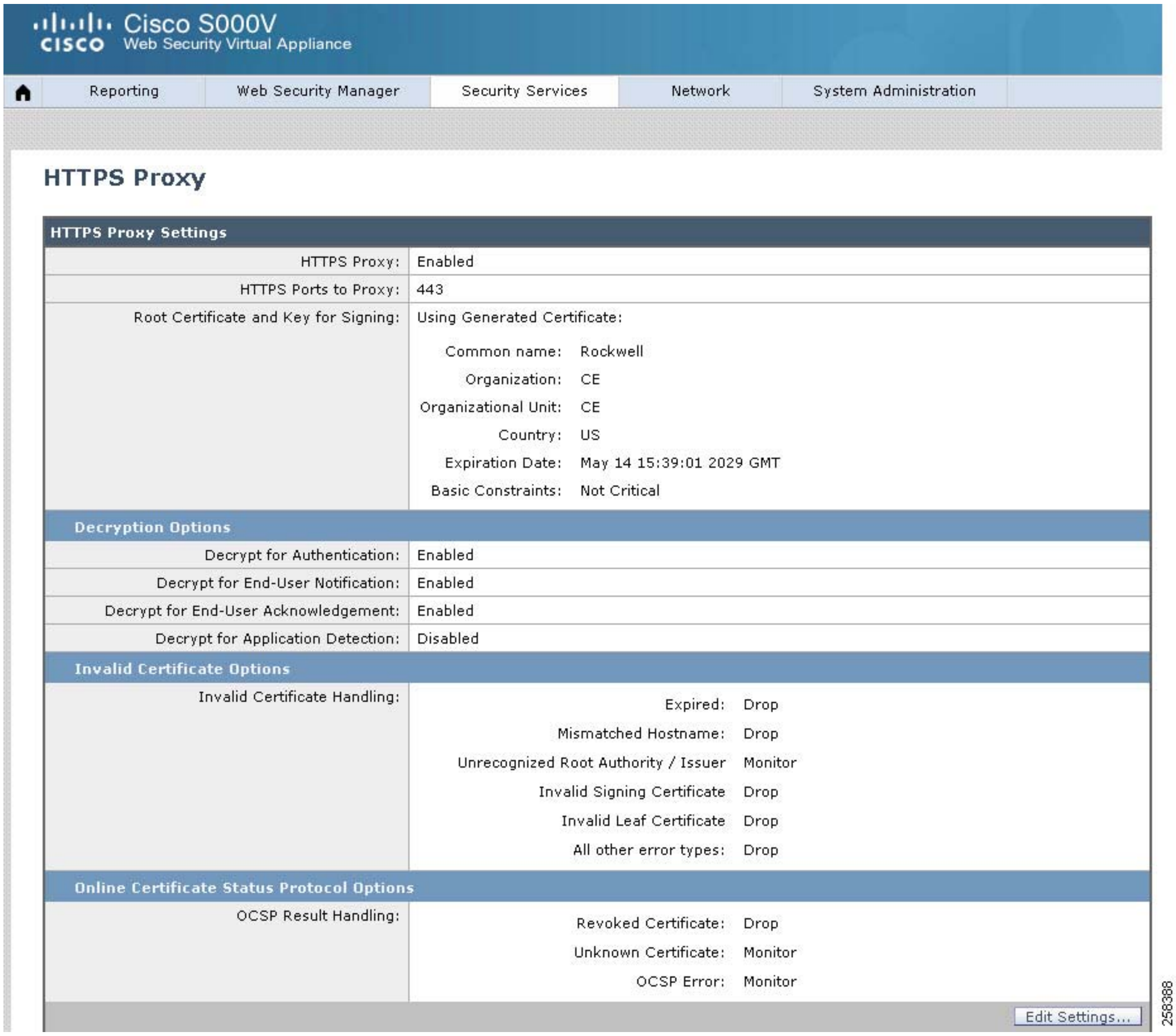
Advanced Settings

Persistent Connection Timeout: ?	Client Side: 300 seconds Server Side: 300 seconds
In-Use Connection Timeout: ?	Client Side: 300 seconds Server Side: 300 seconds
Simultaneous Persistent Connections:	Server Maximum Number: 2000
Generate Headers:	X-Forwarded-For: ○ Send ● Do Not Send Request Side VIA: ● Send ○ Do Not Send Response Side VIA: ● Send ○ Do Not Send
Use Received Headers:	□ Enable Identification of Client IP Addresses using X-Forwarded-For Trusted Downstream Proxy or Load Balancer Add Row *IP address*
Range Request Forwarding:	□ Enable Range Request Forwarding *When enabled, range requests will be forwarded to the destination server. This can save bandwidth, but may result in reduced efficacy for Application Visibility and Control.* *When range request forwarding is enabled and the Application Visibility and Control service is in use, additional settings related to range request handling for AVC are available in Access Policies (see Web Security Manager > Access Policies > Applications).*

HTTPS Proxy Configuration

The HTTPS proxy feature is a separate configuration that is required for use with most cloud applications. This configuration is located under **Security Services**->**HTTPS Proxy**. Once this feature is enabled, a port (443 by default) must be entered to inform the Cisco WSA which HTTPS traffic to proxy. This value should remain 443 as shown in Figure 3-3 unless a solution is being implemented that changes the HTTPS traffic default port.

Figure 3-3 HTTPS Proxy Settings



HTTPS Proxy

HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Generated Certificate: Common name: Rockwell Organization: CE Organizational Unit: CE Country: US Expiration Date: May 14 15:39:01 2029 GMT Basic Constraints: Not Critical
Decryption Options	
Decrypt for Authentication:	Enabled
Decrypt for End-User Notification:	Enabled
Decrypt for End-User Acknowledgement:	Enabled
Decrypt for Application Detection:	Disabled
Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Drop Mismatched Hostname: Drop Unrecognized Root Authority / Issuer Monitor Invalid Signing Certificate Drop Invalid Leaf Certificate Drop All other error types: Drop
Online Certificate Status Protocol Options	
OCSP Result Handling:	Revoked Certificate: Drop Unknown Certificate: Monitor OCSP Error: Monitor

Additional configuration relating to the HTTPS proxy includes decryption options and certificate related options.

Decryption options include those shown in Table 3-7, which are left in the default state for testing and validation.

Table 3-7 Decryption Options

Decryption Option	Description
Decrypt for Authentication	For users who have not been authenticated before this HTTPS transaction, allow decryption for authentication.
Decrypt for End-User Notification	Allow decryption so that AsyncOS can display the end user notification. Note: If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”.

Table 3-7 Decryption Options (continued)

Decryption Option	Description
Decrypt for End-User Acknowledgment	For users who have not acknowledged the web proxy before this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment.
Decrypt for Application Detection	Enhances the ability of AsyncOS to detect HTTPS applications.

Certificate Configuration Options

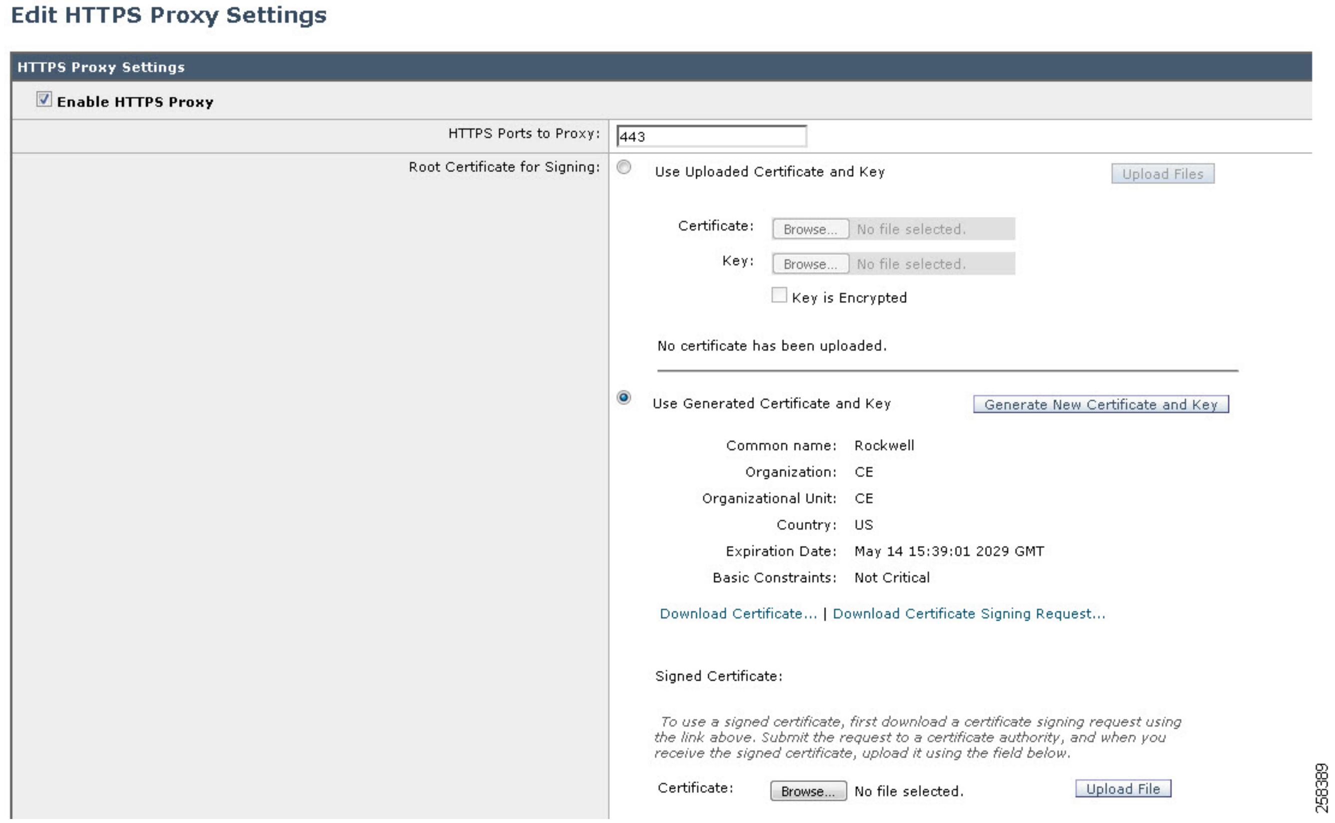
There are two parts to the certificate configuration options, including **Invalid Certificate** and **Online Certificate Status Protocol** (OSCP). These options can generally be uniformly applied to most architectures, but some are application-dependent. If internal or not well-known certificate authorities (CA) are in use (such as Rockwell Automation CA), the **Unrecognized Root Authority/Issuer** option needs to be set to **Monitor** instead of **Drop**. During the testing and validations outlined in this design guide, these options remained set to **Monitor**. OSCP is an internet protocol used for obtaining the revocation (validity) status of X.509 digital certificates and is defined in RFC 6960.

Since cloud applications and most web traffic typically use TLS or other forms of encrypted traffic to send data, the Cisco WSA must act as a man-in-the-middle (MiTM) to allow for the decryption, inspection, and re-encryption of traffic passing through it. To allow for this MiTM process to take place, the Cisco WSA must have a valid certificate to present to a requesting client, which must be trusted by that client. This can be a self-signed certificate generated by the Cisco WSA or from another certificate authority (CA). During the HTTPS Proxy configuration, the certificate that the Cisco WSA presents to the client is configured using either method. For testing and validation, a certificate generated by the Cisco WSA (self-signed) was used to decrypt traffic.

This is completed by using the **Generate New Certificate and Key** process located in the configuration section. Some information is then provided, such as common name, organization and expiration date and entered into the certificate in case a requesting user must verify. This information is shown in Figure 3-4.

After the certificate has been generated, the **Download Certificate** link can be used to download and distribute the certificate. The usage of this certificate is described in Windows Certificates, which describes the configuration of the EWS machines.

Figure 3-4 Certificate Details



Edit HTTPS Proxy Settings

HTTPS Proxy Settings

☑ Enable HTTPS Proxy

HTTPS Ports to Proxy: 443

Root Certificate for Signing:

○ Use Uploaded Certificate and Key

Certificate: No file selected.

Key: No file selected.

□ Key is Encrypted

No certificate has been uploaded.

● Use Generated Certificate and Key

Common name: Rockwell
Organization: CE
Organizational Unit: CE
Country: US
Expiration Date: May 14 15:39:01 2029 GMT
Basic Constraints: Not Critical

Download Certificate... | Download Certificate Signing Request...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

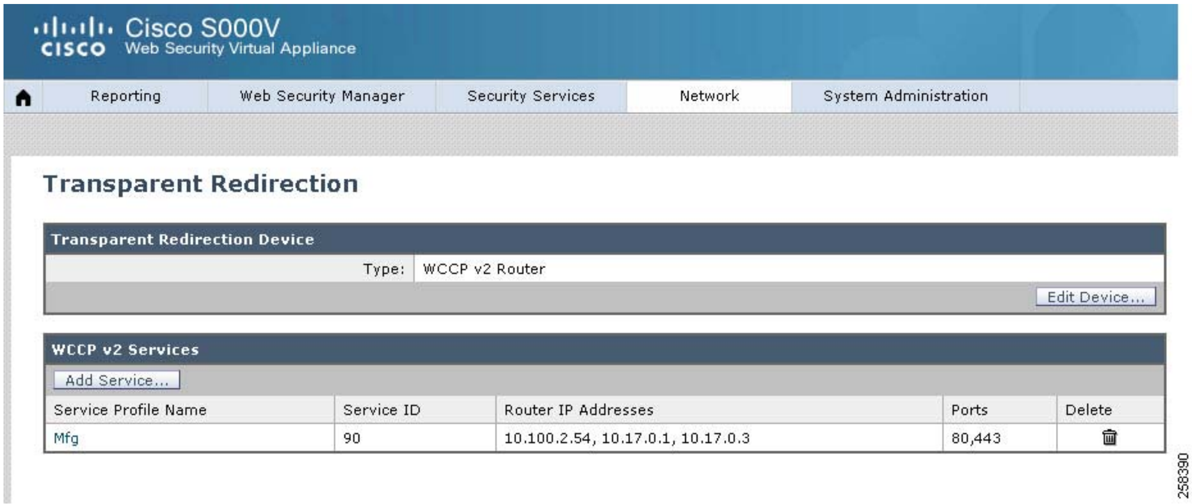
Certificate: No file selected.

Once the certificate has been exported/downloaded or the signing request had been completed, the certificate will be used on individual client computers or devices.

Redirection Configuration

When using transparent redirection on the Cisco WSA, a method must be used to send web traffic from the infrastructure to the Cisco WSA. Typical redirection methods were described in Chapter 2, “CPwE Cloud Connectivity Design Considerations.” For testing and validation, the WCCP v2 router redirection method was selected as shown in Figure 3-5.

Figure 3-5 Redirection Type



Transparent Redirection

Transparent Redirection Device

Type: WCCP v2 Router

Edit Device...

WCCP v2 Services

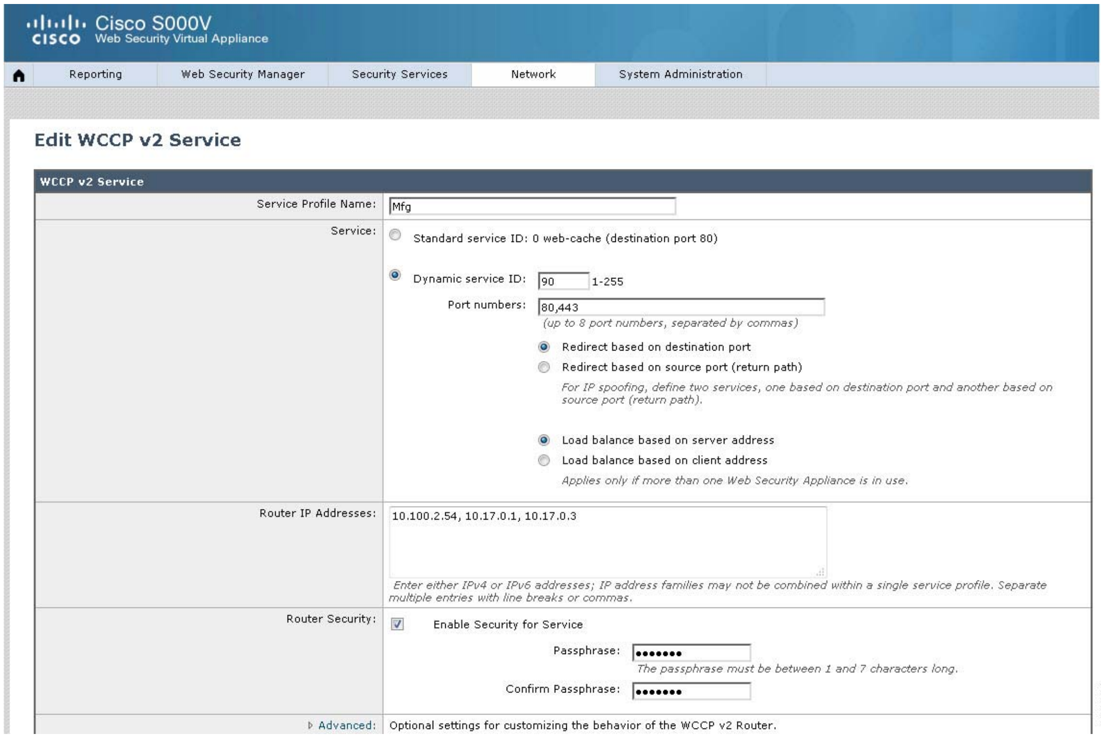
Add Service...

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
Mfg	90	10.100.2.54, 10.17.0.1, 10.17.0.3	80,443	🗑

Once the WCCP v2 redirection method has been selected, the WCCP v2 services must be defined. These services, described in Chapter 2, "CPwE Cloud Connectivity Design Considerations," allow for the group of WCCP v2 devices to send specific traffic types to the Cisco WSA. In our test case, a custom service ID of 90 was used to define both HTTP (Port 80) and HTTPS (Port 443) traffic. This service ID is then used throughout the infrastructure devices to allow for adjacency between the infrastructure and the Cisco WSA.

The configuration of the WCCP v2 services has several items that must be defined as shown in Figure 3-6.

Figure 3-6 WCCP Service Profile



Edit WCCP v2 Service

WCCP v2 Service

Service Profile Name: Mfg

Service:
○ Standard service ID: 0 web-cache (destination port 80)
● Dynamic service ID: 90 1-255
Port numbers: 80,443
(up to 8 port numbers, separated by commas)
● Redirect based on destination port
○ Redirect based on source port (return path)
For IP spoofing, define two services, one based on destination port and another based on source port (return path).
● Load balance based on server address
○ Load balance based on client address
Applies only if more than one Web Security Appliance is in use.

Router IP Addresses: 10.100.2.54, 10.17.0.1, 10.17.0.3
Enter either IPv4 or IPv6 addresses; IP address families may not be combined within a single service profile. Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service
Passphrase: •••••••
The passphrase must be between 1 and 7 characters long.
Confirm Passphrase: •••••••

▷ Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

- The WCCP v2 service must have a service profile name. This name is for organizational purposes on the Cisco WSA and is not shared across additional infrastructure devices.
- The dynamic service ID was selected for the Service, as mentioned above, which allows the user to define the port numbers (up to eight) that will be used for the WCCP v2 redirection. Additional ports can be added to the service ID if needed. This is used on additional devices through the infrastructure and is shown in a Cisco ASA configuration in Cisco Adaptive Security Device Manager (ASDM) Configuration.
- The Router IP Addresses define the WCCP v2 devices, such as routers, switches, and firewalls that exist in the infrastructure. These devices are responsible for forwarding target web traffic defined by the service ID to the Cisco WSA.

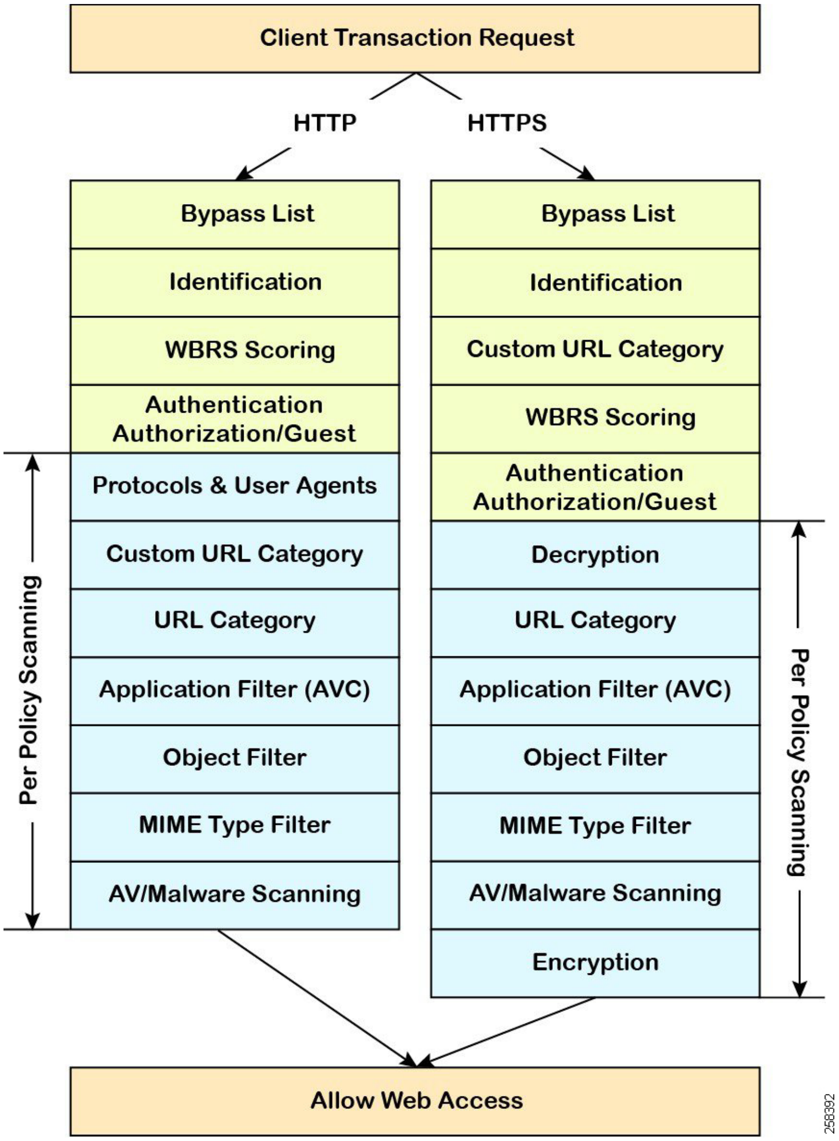
Cisco WSA Rule Configuration

Once web traffic (HTTP or HTTPS) is received by the Cisco WSA, policies and rules exist to restrict, decrypt, monitor, or pass-through the traffic. The purpose and definition of each of these actions is defined in Table 3-8. Additionally, Figure 3-6 defines the logical flow of data as well as the various lists and technologies that are processed during the flow of traffic.

Table 3-8 Web Traffic Action

Option	Description
Monitor	Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.
Drop	The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.
Pass through	The appliance passes through the connection between the client and the server without inspecting the traffic content. However, with a standard pass-through policy, the WSA does check the validity of the requested server by initiating an HTTPS handshake with the server. This validity check includes server certificate validation. If the server fails the check, the transaction is blocked. You can skip validation checks for specific sites by configuring policies that incorporate custom categories, which include these sites, thereby indicating that these sites are trustworthy-these sites are passed through without validity checks. Exercise care when configuring policies that allow validity checks to be skipped.
Decrypt	The appliance allows the connection, but inspects the traffic content. It decrypts the traffic and applies access policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying access policies, you can scan the traffic for malware.

Figure 3-7 Cisco WSA Logical Flow



A few items shown in Figure 3-7 are defined below; not all items are defined since some were not used or did not affect the testing and validation:

- Bypass List
  - This is used for applications or web traffic that may have issues being sent to a proxy or if there is a specific application that would not need to be inspected by the Cisco WSA. Items that are within the Bypass List are allowed through the Cisco WSA without additional examination.
- Custom URL Category
  - Custom URL Categories are used to websites that may not be well-known enough to fall into one of the existing pre-defined URL Categories. The Rockwell Automations website falls under the Business and Industry category and does not require a Custom URL category.

    - All transactions resulting in unmatched categories are reported on the **Reporting** -> **URL Categories** page as uncategorized URLs. Many uncategorized URLs are generated from requests to websites within the internal network. Cisco, Panduit, and Rockwell Automation recommend using custom URL categories to group internal URLs and allow all requests to internal websites.
- Web Reputation Score (WBRS) Scoring
    - WBRS is an innovative method that analyzes the behavior and characteristics of a web server and provides the latest defense in the fight against spam, viruses, phishing, and spyware threats.
    - WBRS uses real-time analysis on a vast, diverse, and global dataset in order to detect URLs that contain some form of malware. It is a critical part of the Cisco security database, which helps protect from blended threats from email or web traffic.
    - WBRS differs from a traditional URL blacklist or whitelist because it analyzes a broad set of data and produces a highly granular score of -10 to +10, instead of the binary good or bad categorizations of most malware detection applications. This granular score offers administrators increased flexibility; different security policies can be implemented based on different WBRS scoring ranges.
- Decryption Policies
    - Decryption policies define the handling of HTTPS traffic within the web proxy:
        - When to decrypt HTTPS traffic.
        - How to handle requests that use invalid or revoked security certificates.
    - You can create decryption policies to handle HTTPS traffic in the following ways:
        - Pass through encrypted traffic.
        - Decrypt traffic and apply the content-based access policies defined for HTTP traffic. This also makes malware scanning possible.
        - Drop the HTTPS connection.
        - Monitor the request (take no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decrypt action.
- URL Category
    - The category that a URL falls into is determined by a filtering categories database. The Web Security Appliance collects information and maintains a separate database for each URL filtering engine. The filtering categories databases periodically receive updates from the Cisco update server.
    - The URL categories database includes many different factors and sources of data internal to Cisco and from the internet.

Decryption Policy

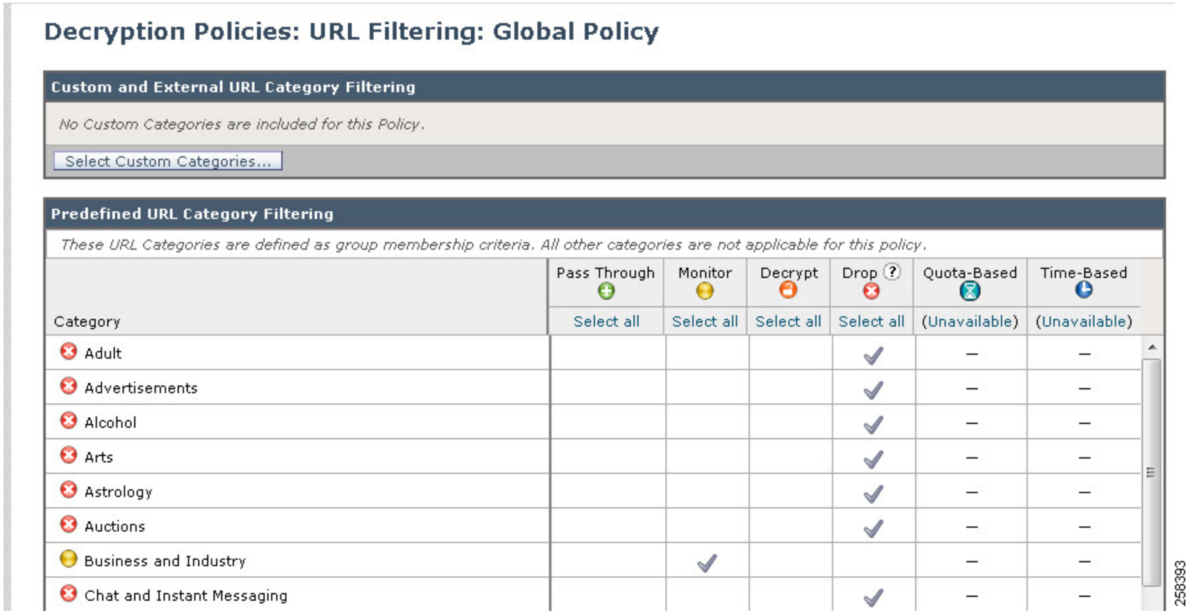
The decryption policy configuration of the Cisco WSA is dependent on the types of applications and software that may be sending HTTP and HTTPS traffic throughout the infrastructure. For testing and validation, the focus was to help ensure that Rockwell Automation software and applications continued to function while the proxy was in place and providing inspection. Based on the testing of current offerings that offer cloud connectivity by Rockwell Automation, the following software was tested:

- FactoryTalk AssetCentre
    - Lifecycle status information
- FactoryTalk Activation Manager
    - Activation retrieval, renewal, and rehosting

- ControlFLASH Plus
  - Lifecycle status information
  - Firmware and release notes downloads

The Rockwell Automation software mentioned above reaches out to rockwellautomation.com as the primary domain name for all requests. The rockwellautomation.com domain name is a known good domain name and is categorized under the Business and Industry URL category. Any subdomain such as api.rockwellautomation.com would also fall under this URL category. For minimal access the following decryption policy can be set to Decrypt, Monitor, or Pass-Through as shown in Figure 3-8.

Figure 3-8 Decryption Policy



Decryption Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult				✓	–	–
Advertisements				✓	–	–
Alcohol				✓	–	–
Arts				✓	–	–
Astrology				✓	–	–
Auctions				✓	–	–
Business and Industry		✓			–	–
Chat and Instant Messaging				✓	–	–

Infrastructure Device WCCP v2 Configuration

In the previous sections WCCP v2 was described as the method of redirection that would be used for HTTP and HTTPS traffic within the infrastructure. For Cisco IOS devices, the configuration for WCCP v2 is standard, but specific device documentation should be cross-referenced with the configurations outlined in this design guide. The configuration for WCCP v2 in this section is shown both from Command Line Interface (CLI) as well as Cisco ASDM. This generally will allow the application of WCCP v2 redirection to Cisco ASA and route and switch devices. This allows the user to have multiple choices where redirection could be applied depending on network architecture and traffic flow.

For WCCP, the device chooses the highest reachable IP address configured on an interface and uses that as the router ID. This is the same process that Open Shortest Path First (OSPF) follows for the router ID. When the device redirects packets to the proxy the device sources the redirect from the router ID IP address (even if it is sourced out another interface) and encapsulates the packet in a GRE header.

The GRE connection is unidirectional. The device encapsulates redirected packets in GRE and sends them to the proxy. The device does not process any GRE-encapsulated responses from the proxy. The proxy must communicate directly to the inside host.

Command Line Interface Configuration

Note If using WCCP on a Cisco ASA, the commands below should exlude **ip**. For example, **ip wccp web-cache** on the Cisco ASA would be **wccp web-cache**.

Issue the following commands:

Step 1 enable

Enable privileged EXEC mode. Enter your password if prompted.

```
Device> enable
```

Step 2 configure terminal

Enters global configuration mode.

```
Device# configure terminal
```

Step 3 ip wccp version {1 | 2 }

Specifies which version of WCCP to configure on a device. WCCPv2 is the default running version.

```
Device(config)# ip wccp version 2
```

Step 4 ip wccp {web-cache | service-number} [group-address multicast-address] [redirect-list access-list] [group-list access-list] [password password [0 | 7]]

Specifies a web-cache or dynamic service to enable on a device, specifies the IP multicast address used by the service group (optional), specifies any access lists to use, specifies whether to use MD5 authentication, and enables the WCCP service.

- During testing the service-number used was 90.
- A redirect list is recommended and is described below.

Note The password length must not exceed eight characters.

```
Device(config)# ip wccp 90 password rockwell
```

Step 5 interface type number

Targets an interface number for which the web cache service will run and enters interface configuration mode.

```
Device(config)# interface Gigabitethernet 0/0
```

Step 6 ip wccp {web-cache | service-number} redirect {in}

Enables packet redirection on an outbound or inbound interface using WCCP. As indicated by the **out** and **in** keyword options, redirection can be specified for outbound interfaces or inbound interfaces.

```
Device(config-if)# ip wccp 90 redirect in
```

Step 7 exit

Exits interface configuration mode.

```
Device(config-if)# exit
```

Step 8 interface type number

Targets an interface number on which to exclude traffic for redirection and enters interface configuration mode.

```
Device(config)# interface GigabitEthernet 0/2/0
```

Step 9 ip wccp redirect exclude in

(Optional) Excludes traffic on the specified interface from redirection.

```
Device(config-if)# ip wccp redirect exclude in
```

Redirect Access-List

The redirect access-list allows you to control which traffic should be redirected and is used with the **ip wccp** command. It is recommended to add deny statements to the redirect list for RFC 1918 addresses such as 10.0.0./8, 172.16.0.0/12, and 192.168.0.0/16 to help ensure that local traffic is not forwarded to the proxy. The following example shows how to redirect traffic only from subnet 10.1.1.0:

```
device(config)# ip access-list extended 100
device(config-ext-nacl)# permit ip 10.1.1.0 255.255.255.0 any
device(config-ext-nacl)# exit
device(config)# ip wccp web-cache redirect-list 100
device(config)# interface vlan 40
device(config-if)# ip wccp 90 redirect in
```

Group-List Access-List

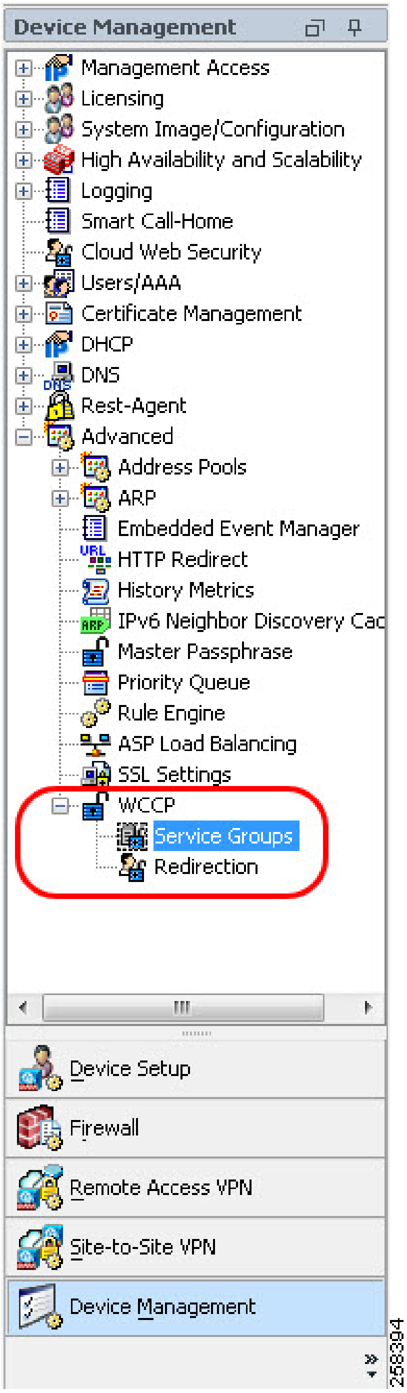
To achieve better security, you can use a standard access-list to notify the redirecting device about the IP addresses that are valid addresses for the Cisco WSA attempting to register with the current device. The following example shows a standard access-list configuration session where the access-list number is 10 for some sample hosts. When this access-list is applied to the **ip wccp** command, only proxies that are listed in the access-list will be added to the group.

```
device(config)# access-list 10 permit host 11.1.1.1
device(config)# access-list 10 permit host 11.1.1.2
device(config)# access-list 10 permit host 11.1.1.3
device(config)# ip wccp 90 group-list 10
```

Cisco Adaptive Security Device Manager (ASDM) Configuration

Step 1 Choose **Configuration**->**Device Management**->**Advanced**->**WCCP**->**Service Groups** (Figure 3-9).

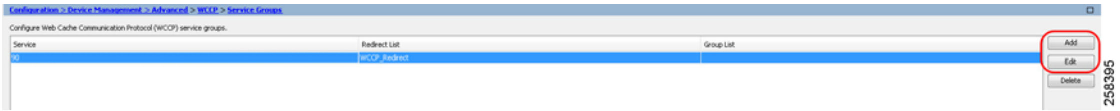
Figure 3-9 ASDM Menu



Step 2 Do any of the following (Figure 3-10):

- To add a new service group, click **Add**.
- To edit a service group, select it and click **Edit**.

Figure 3-10 WCCP Service Group



Configuration > Device Management > Advanced > WCCP > Service Groups

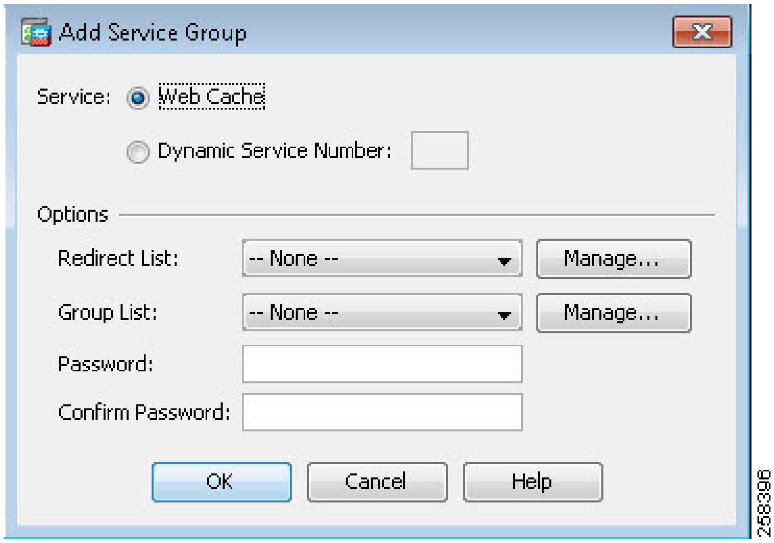
Configure Web Cache Communication Protocol (WCCP) service groups.

Service	Redirect List	Group List
90	WCCP_Redirect	

Step 3 In the Add/Edit Service Group dialog box, configure the following options (Figure 3-11).

- Service—The type of service, one of:
  - Web Cache—The standard service, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the WCCP-enabled device. This exludes TCP port 443 HTTPS traffic.
  - Dynamic Service Number—The Cisco WSA device defines the services associated with this dynamic service number (0-254); on the ASA, you are simply associating the number with this group. For testing and validation, the dynamic service number of 90 was used.
- Redirect List—(Optional) An ACL whose permit entries define the traffic that should be redirected for this service. Click **Manage** to create new ACLs or to view the contents of an ACL.
- Group List—(Optional) An ACL whose permit entries define the WCCP-enabled devices that can provide this service.
- Password, Confirm Password—(Optional) A password up to seven characters long, which is used for MD5 authentication for messages received from the service group. You must configure the same password on the Cisco WSA.

Figure 3-11 Add Service Group



Add Service Group

Service: ● Web Cache

○ Dynamic Service Number:

Options

Redirect List: -- None --

Group List: -- None --

Password:

Confirm Password:

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes.

Configure WCCP Packet Redirection

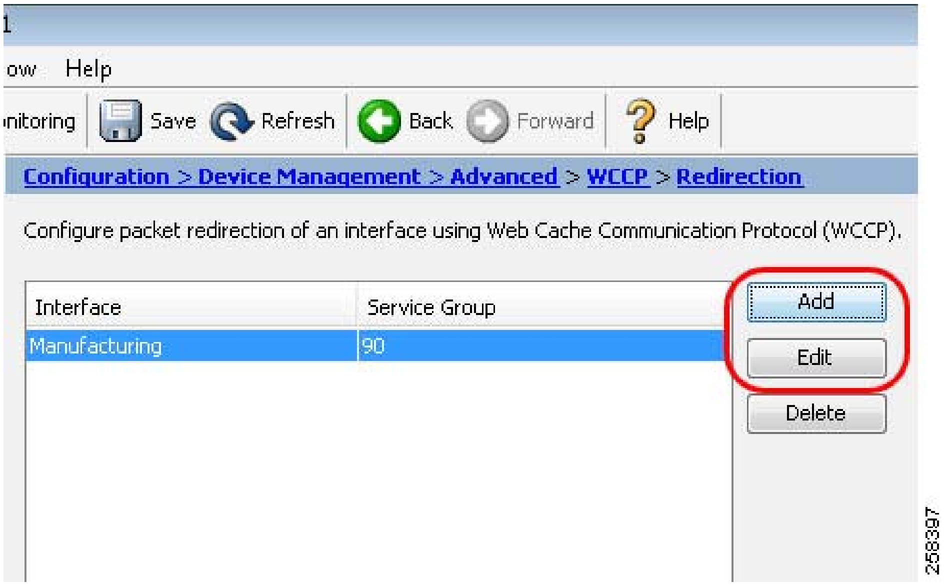
To configure packet redirection on the ingress of an interface using WCCP, perform the following steps:

Step 1 Choose **Configuration**->**Device Management**->**Advanced**->**WCCP**->**Redirection**.

Step 2 Do any of the following (Figure 3-12):

- To add redirection for an interface and service group, click **Add**.
- To edit redirection for an interface and service group, select it and click **Edit**.

Figure 3-12 WCCP Redirection



Configuration > Device Management > Advanced > WCCP > Redirection

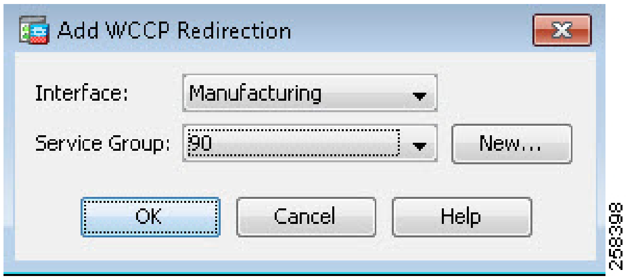
Configure packet redirection of an interface using Web Cache Communication Protocol (WCCP).

Interface	Service Group
Manufacturing	90

Step 3 In the Add/Edit WCCP Redirection dialog box, configure the following options (Figure 3-13):

- Interface—The interface whose inbound traffic you want to redirect to the WCCP-enabled device.
- Service Group—The WCCP service group for which you are redirecting traffic. Click **New** if you need to create a group.

Figure 3-13 WCCP Redirection Interface



Interface: Manufacturing

Service Group: 90

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes. Be sure to save the startup configuration once complete.

Workstation Configuration

With the Cisco WSA and WCCP v2 configuration complete, the workstations that are intended to use the proxy must be configured. Depending on the proxy configuration, transparent or explicit, the configuration varies slightly. However, both methods still require the importation of certificates generated by the Cisco WSA.

This section focuses on the Windows Operating System (Windows 7) and its associated web browsers and certificate stores. Once the certificate has been imported, a trust is created between the workstation and the Cisco WSA.

No workstation configuration besides the importation of the certificates is needed to help ensure the success of the transparent proxy deployment. With this in mind, there is no subsection listed for Transparent Redirection.

Windows Certificates

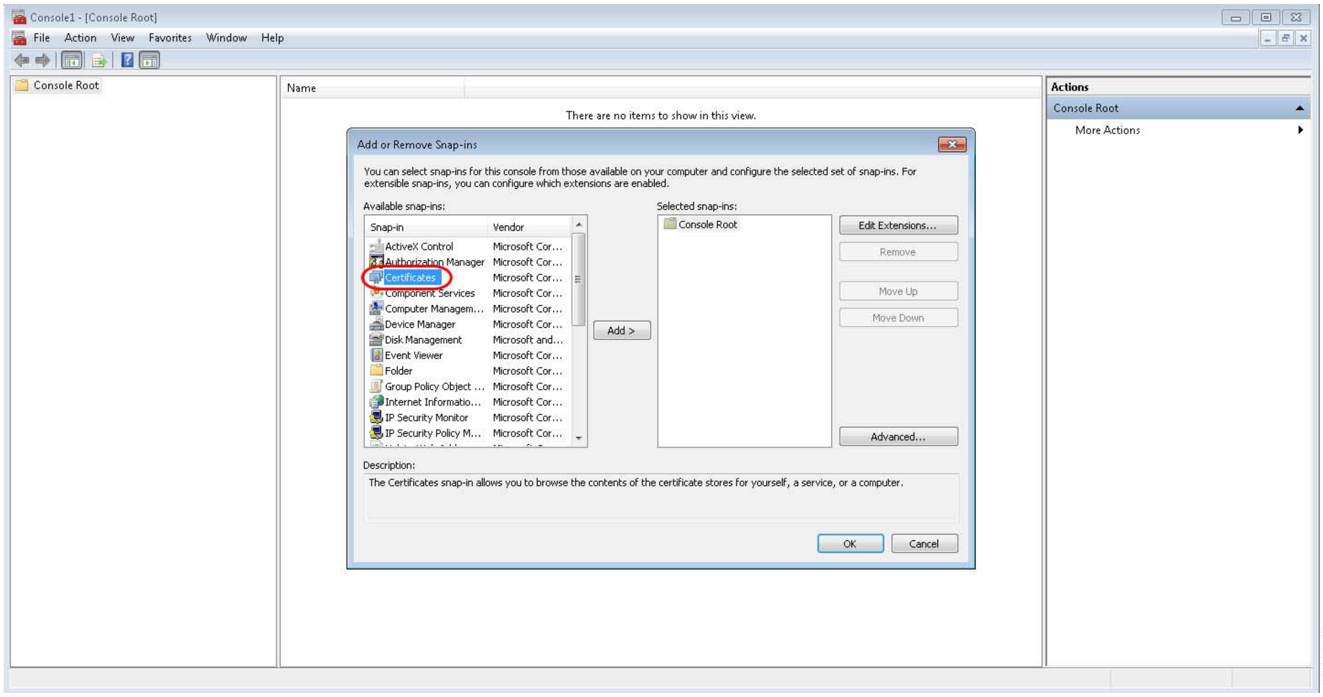
As previously mentioned, the Cisco WSA providing TLS proxy services must have the ability to decrypt the data coming from the application or EWS. To provide this service, a certificate that is used (generated by the Cisco WSA or a root CA) on the Cisco WSA must be stored on each EWS that wishes to send traffic to the cloud through the Cisco WSAs TLS proxy service. Based on testing and validation it is recommended to add the Cisco WSA certificate to each pertinent web browser and the Microsoft certificate store. This can be accomplished manually or through Group Policy; for testing this was completed manually.

Step 1 **Start**-> **Run**. Type **MMC.exe**.

Step 2 Click **File**->**Add/Remote Snap-in**.

Step 3 In the Available snap-ins list, click **Certificates** and click **Add** (Figure 3-14).

Figure 3-14 Add or Remove Snap-ins



Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Name
Actions
Console Root
More Actions
258399

There are no items to show in this view.

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

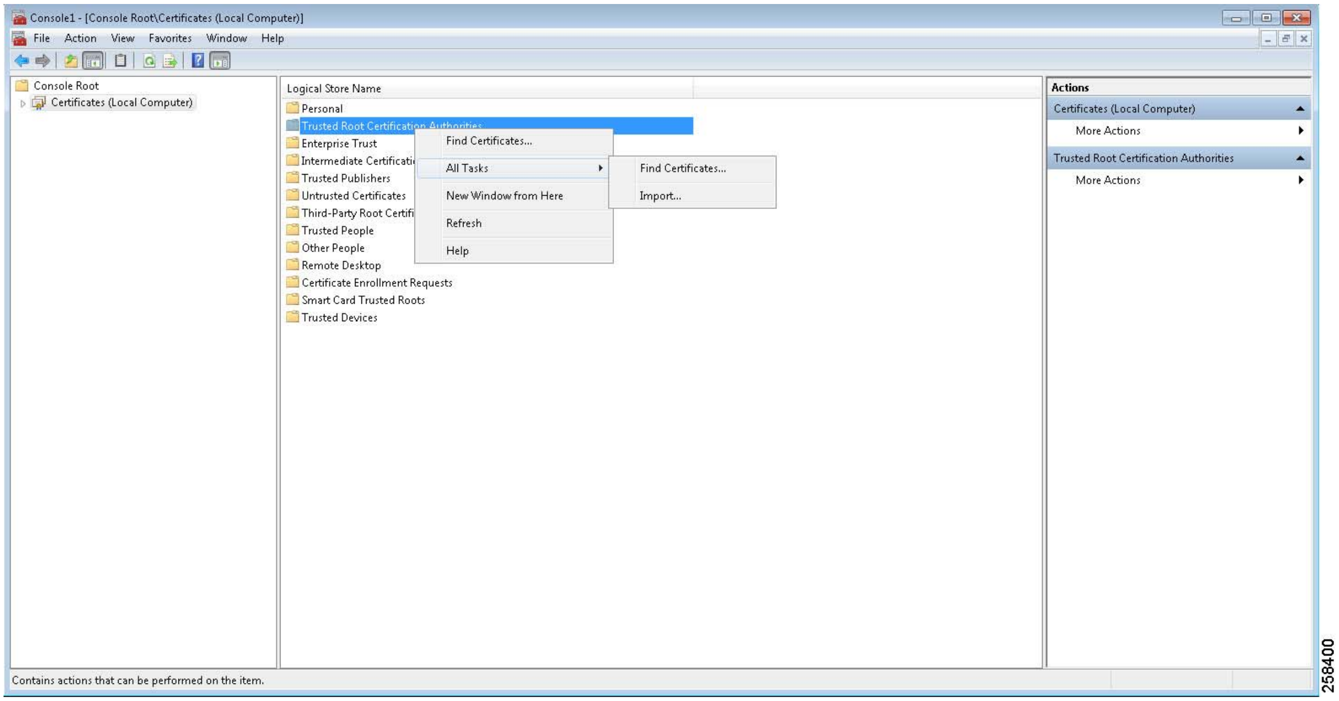
Step 4 Depending on security posture and how the application is being used, select **My User Account**, **Computer Account**, or **Service Account** and click **Next**.

Generally, for a single user computer, **My User Account** is the acceptable choice.

Step 5 Once finished, click **OK**.

Step 6 In the MMC window, click **Certificates** then right-click **Trusted Root Certification Authorities**->**All Tasks**->**Import…** (Figure 3-15).

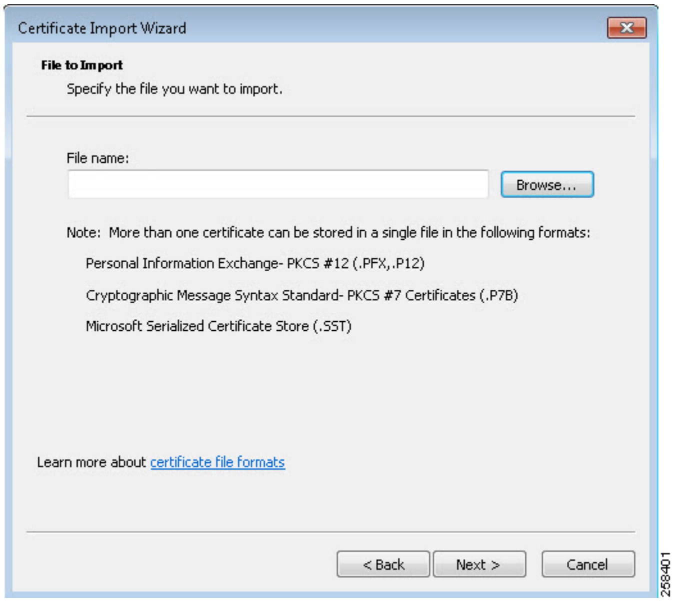
Figure 3-15 All Tasks->Import



This opens the Certificate Import Wizard where the certificate downloaded from the Cisco WSA in the previous section should be selected.

Step 7 Once the wizard is launched, click **Next** for the first prompt and then the **File to Import** window displays prompting for a file name (Figure 3-16).

Figure 3-16 Certificate Import Wizard


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

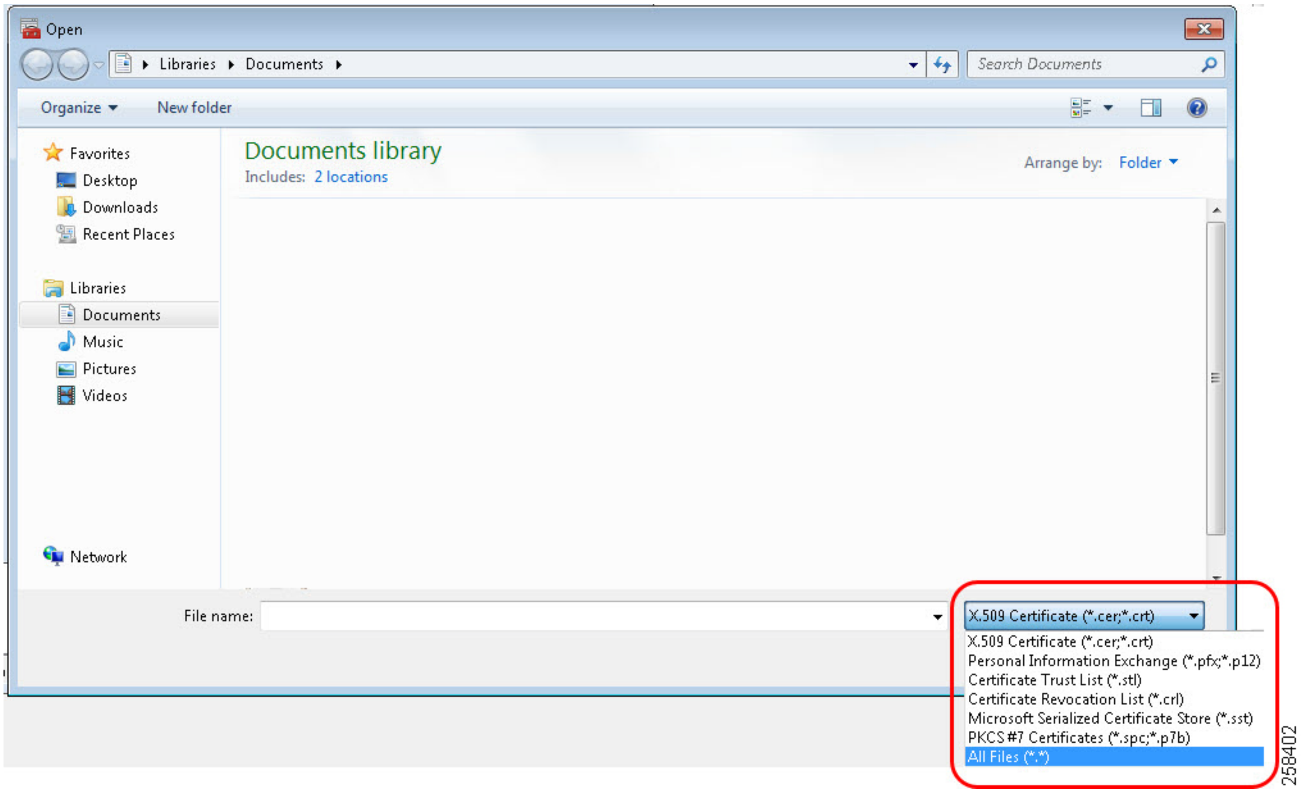
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

When browsing for the certificate using this method, it is important to note that the certificate that was downloaded from the Cisco WSA is a .pem file extension. By default, the browse feature in the certificate import wizard is looking for X.509. To locate the .pem certificate from the Cisco WSA, the file type in the browse window must be adjusted and set to **All files** (*.*) (Figure 3-17).

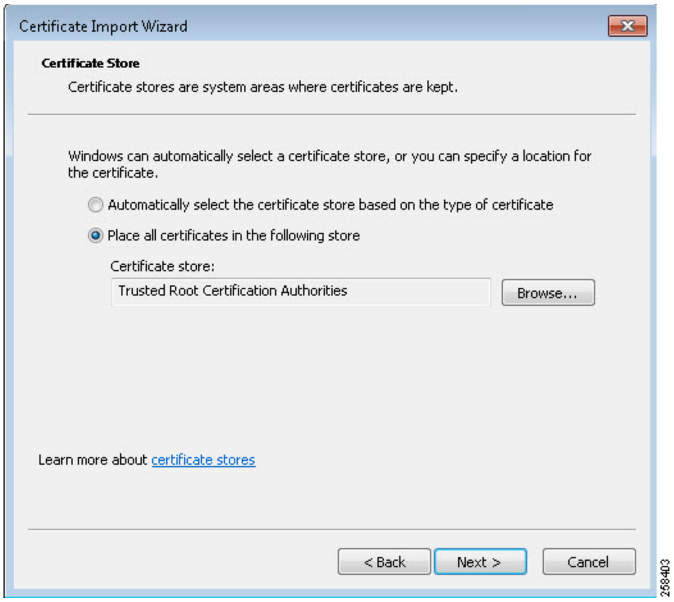
Figure 3-17 Select Certificate


Open
Libraries
Documents
Search Documents
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Network
Documents library
Includes: 2 locations
Arrange by: Folder
File name:
X.509 Certificate (*.cer;*.crt)
X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p12)
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.sst)
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)
258402

Step 8 Once the certificate has been selected, click **Next** to display the **Certificate Store** screen (Figure 3-18).

Step 9 On this screen ensure that the **Place all certificates in the following store** is set to **Trusted Root Certification Authorities**, then click **Next**.

Figure 3-18 Certificate Store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

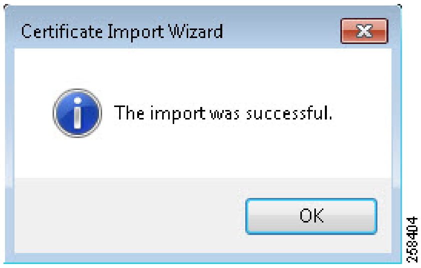
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Step 10 Verify the settings on the final screen and click **Finish**.

A window displays indicating that the import was successful (Figure 3-19).

Figure 3-19 Successful Import



Certificate Import Wizard

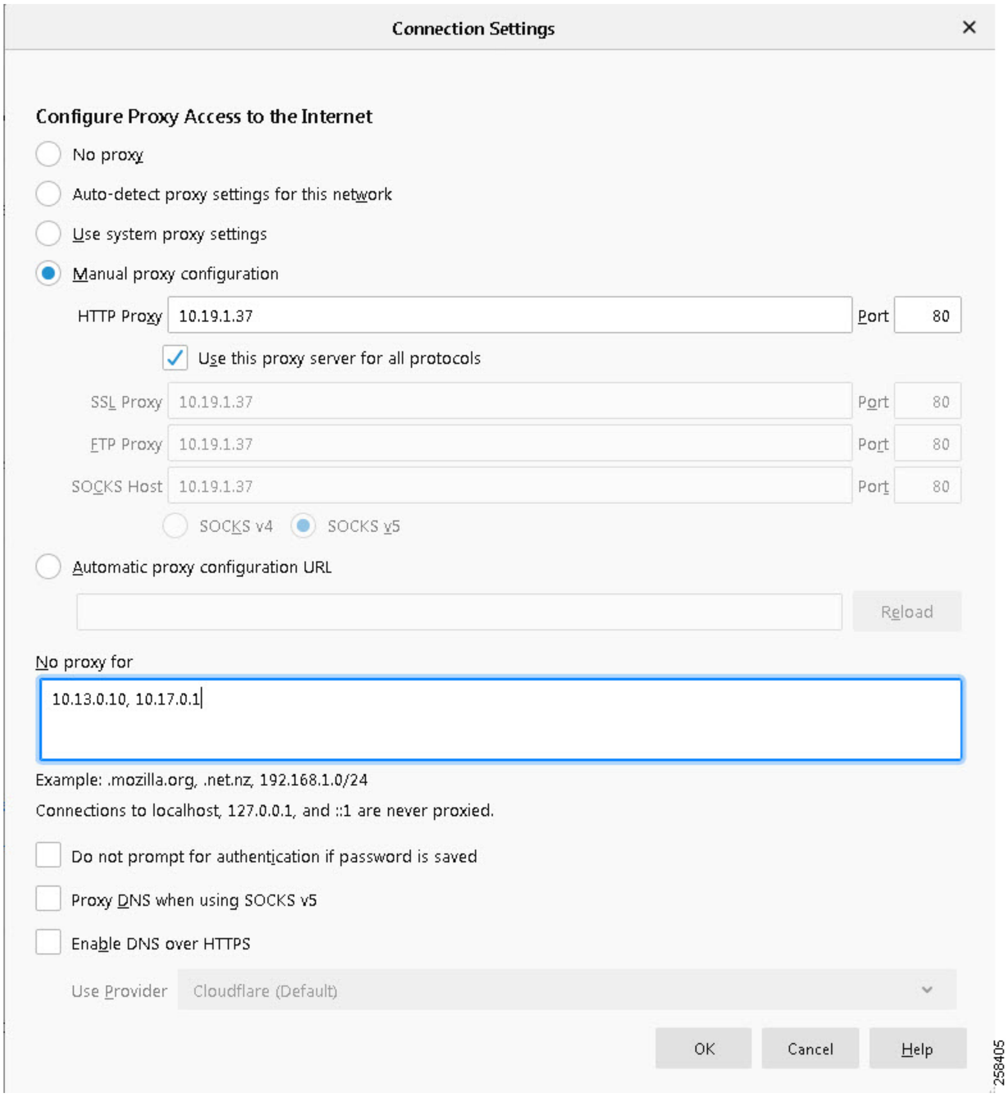
The import was successful.

Note It is also required that each web browser in use in the system (including Internet Explorer, even if not used for browsing) also has the same certificate imported into the browser as a certificate authority. Because there are various web browsers with different interfaces, this design guide does not detail the process.

Explicit Redirection

Explicit redirection of web traffic follows similar setup requirements as the WCCP transparent redirection method. The explicit redirection method does not require the dual-homed approach that was described in Interface Configuration. Explicit redirection only requires a single interface (besides management) and can exist solely in the IDMZ. The certificate must be imported to the various locations as descried in Windows Certificates. The biggest difference between the two redirection methods is that the explicit redirection requires the user to configure each web browser to explicitly redirect to the Cisco WSA proxy. As with the certificate importation, each browser has a different method to access the proxy settings and each browser is required to be set up to point to the Cisco WSA. The example below of the proxy configuration was taken from FireFox (Figure 3-20).

Figure 3-20 FireFox Connection Settings



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 10.19.1.37 Port 80

☑ Use this proxy server for all protocols

SSL Proxy 10.19.1.37 Port 80

FTP Proxy 10.19.1.37 Port 80

SOCKS Host 10.19.1.37 Port 80

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

10.13.0.10, 10.17.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

Some important items to note in the above configuration:

- These settings could be applied via Group Policy if applicable, however, this is not detailed in this design guide.
- The **HTTP Proxy** field is where the IP address of the Cisco WSA is entered and the **Port** field is the expected port for that protocol.
- The checkbox **Use this proxy server for all protocols** is used to ensure that the address is consistent for HTTP and SSL/HTTPS. The correct port is applied based on protocol and what is shown in the **Port** field has no bearing.

- The **No proxy for field** is required for any applications that use HTTP traffic as their form of communication. Any servers or devices that the computer would communicate with via HTTP or HTTPS should be listed here. In most circumstances, entering the subnet addresses with the mask of the local network is sufficient. Ideally the proxy should only be used for traffic that is moving from a trusted to an untrusted network. When addresses are not defined in the **No proxy for field**, even basic web traffic like attempting HTTP to an Allen-Bradly 1756-EN2TR would be sent to the proxy and would not reach the end device. Even services such as the interaction between FactoryTalk AssetCentre server and FactoryTalk AssetCentre client use HTTP traffic. It is important to understand the traffic usage in the network before deploying explicit proxying.

CHAPTER 4

Verifying and Troubleshooting the Deployment

This chapter provides an overview of some of the verification and troubleshooting tools that can be used to complete the verification and any troubleshooting of the proxy deployment. It also provides a basic overview of some of the items on the Cisco WSA, infrastructure devices, and Windows Operations Systems to assist in basic verification and troubleshooting. However, it does not specifically prescribe action items as a result of the troubleshooting steps due to the fluidity of the deployment and potential architectural differences.

There are several methods of verifying and troubleshooting the deployment of the proxy and the associated redirection services in the infrastructure.

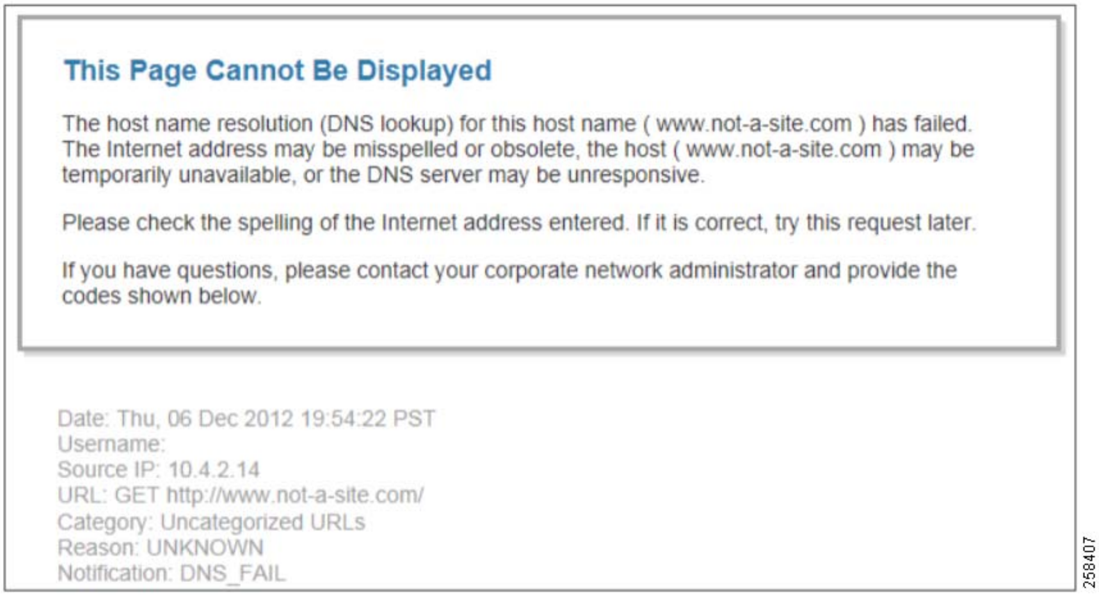
Web Browser Verification

Verification of the functionality of WCCP and the Cisco WSA can occur within the web browser itself by testing some addresses that may or may not be blocked depending on the configuration of the Cisco WSA:

- One address should be resolvable externally on the internet, for instance www.rockwellautomation.com, which should return without issue. This proves the client has internet access but does not prove the connection is going through Cisco WSA.
- The other address should be something not resolvable externally or something that may have been configured to be blocked. This request should return an error from the Cisco WSA, not the browser; proving that Cisco WSA is serving the content.

  The Cisco WSA returns an error like that shown in Figure 4-1.

Figure 4-1 Cisco WSA Error



This Page Cannot Be Displayed

The host name resolution (DNS lookup) for this host name (www.not-a-site.com) has failed. The Internet address may be misspelled or obsolete, the host (www.not-a-site.com) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

If you have questions, please contact your corporate network administrator and provide the codes shown below.

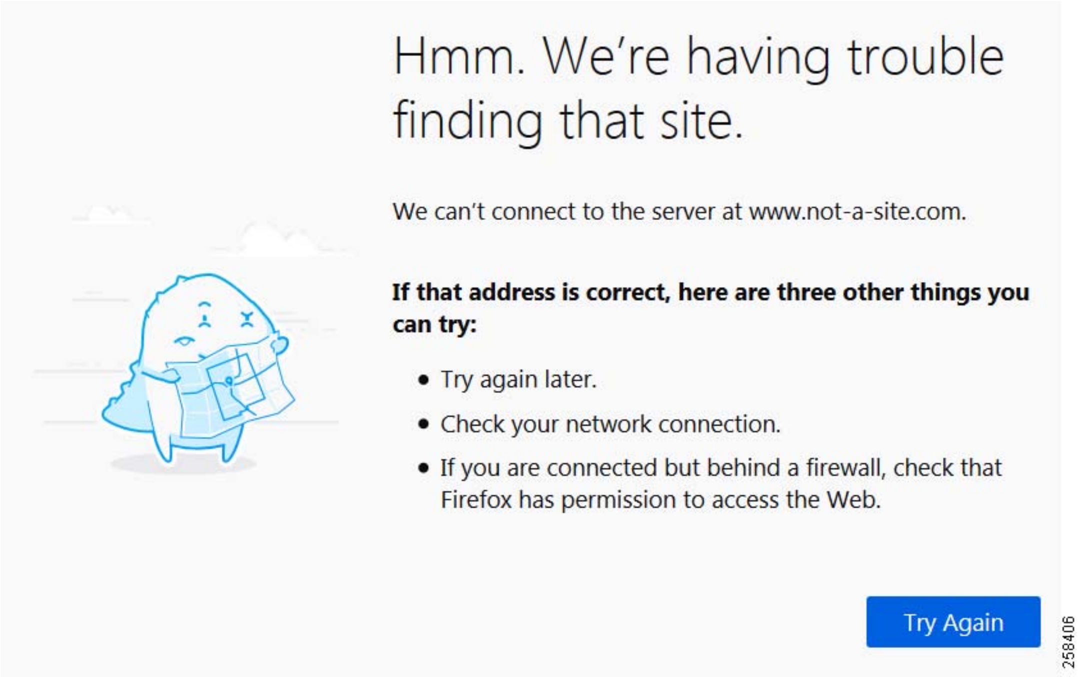
Date: Thu, 06 Dec 2012 19:54:22 PST
Username:
Source IP: 10.4.2.14
URL: GET http://www.not-a-site.com/
Category: Uncategorized URLs
Reason: UNKNOWN
Notification: DNS_FAIL

Some important items to note from the above error:

- URL—This is the website that was requested.
- Category—If the website is known and classified into one of the Cisco WSAs categories, this would be shown here. This is a good tool to determine which categories to allow or block if web sites are not working as expected. In this case, the requested URL is not categorized.
- Reason—This is the reason that the webpage is being blocked.
- Notification—This is a summary of the error shown to the user.

If the web request is not directed by the Cisco WSA, the web browser returns an error. An example with the Firefox browser returns an error similar to what is shown in Figure 4-2.

Figure 4-2 FireFox Connection Error



Hmm. We're having trouble finding that site.

We can't connect to the server at www.not-a-site.com.

If that address is correct, here are three other things you can try:

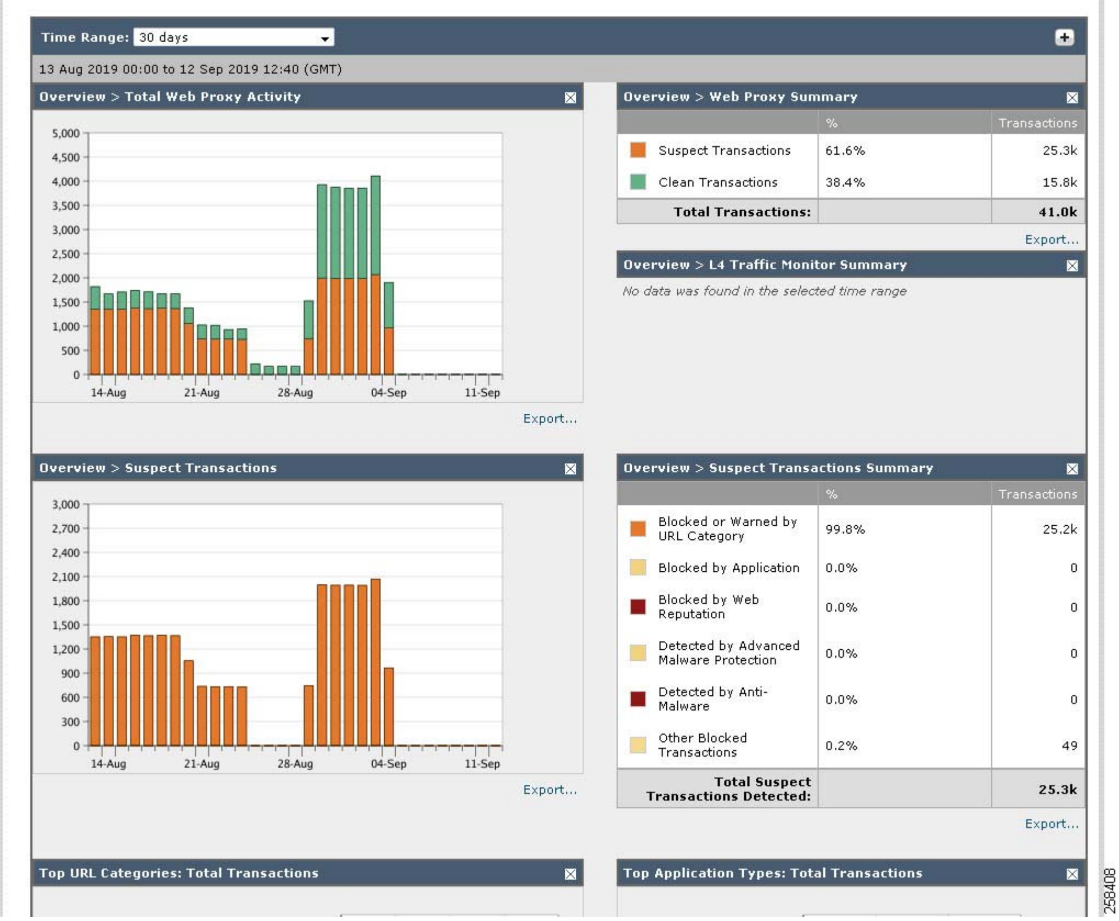
- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Cisco WSA Tools

From the home page of the Cisco WSA, there are several reporting tools that are available for verification, log management, and troubleshooting. These tools can be used to verify if the deployment of the Cisco WSA was successful. The Cisco WSA inspects all traffic that is forwarded to it and organizes it into two categories, Suspect Transactions and Clean Transactions. Based on the configuration of the Cisco WSA and overall usage, the ratios of Suspect to Clean may vary.

Figure 4-3 shows the reporting details from the Cisco WSA home page detailing the summary of traffic and the details of the Suspect Transactions.

Figure 4-3 Web Proxy Reporting



Time Range: 30 days

13 Aug 2019 00:00 to 12 Sep 2019 12:40 (GMT)

Overview > Total Web Proxy Activity

Export...

Overview > Web Proxy Summary

	%	Transactions
🟧 Suspect Transactions	61.6%	25.3k
🟩 Clean Transactions	38.4%	15.8k
Total Transactions:		**41.0k**

Export...

Overview > L4 Traffic Monitor Summary

No data was found in the selected time range

Overview > Suspect Transactions

Export...

Overview > Suspect Transactions Summary

	%	Transactions
🟧 Blocked or Warned by URL Category	99.8%	25.2k
🟨 Blocked by Application	0.0%	0
🟥 Blocked by Web Reputation	0.0%	0
🟨 Detected by Advanced Malware Protection	0.0%	0
🟥 Detected by Anti-Malware	0.0%	0
🟨 Other Blocked Transactions	0.2%	49
Total Suspect Transactions Detected:		**25.3k**

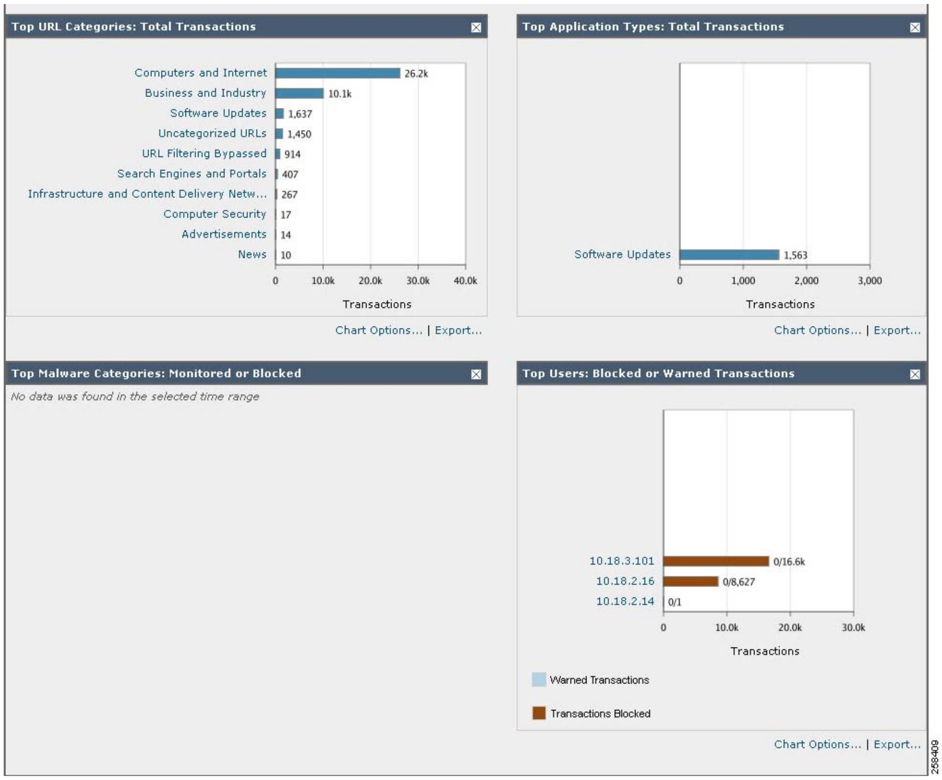
Export...

Top URL Categories: Total Transactions

Top Application Types: Total Transactions

Additional information is shown in the lower half of the home page of the Cisco WSA. This information provides a more granular overview of the top URL categories as well as the top users as shown in Figure 4-4.

Figure 4-4 URL and User Reporting



Top URL Categories: Total Transactions

Top Application Types: Total Transactions

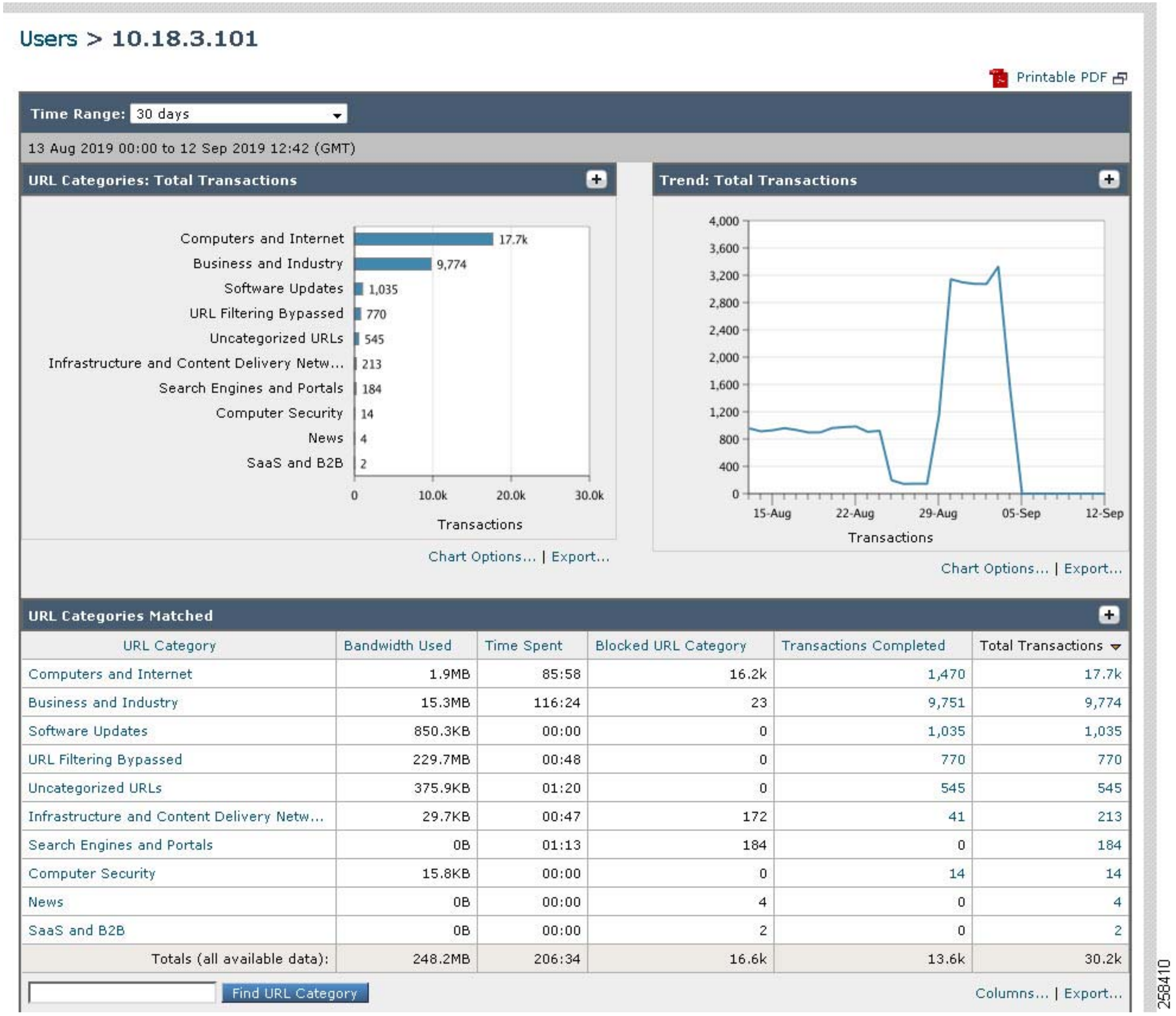
Top Malware Categories: Monitored or Blocked

No data was found in the selected time range

Top Users: Blocked or Warned Transactions

These reporting options and top application types contain hyperlinks that provide more details. For example, clicking the IP address 10.18.3.101 under the top users section would provide additional information (Figure 4-5). Additional granularity is provided for each user, such as the amount of bandwidth and time spent in each of the URL categories.

Figure 4-5 User Report



Users > 10.18.3.101

13 Aug 2019 00:00 to 12 Sep 2019 12:42 (GMT)

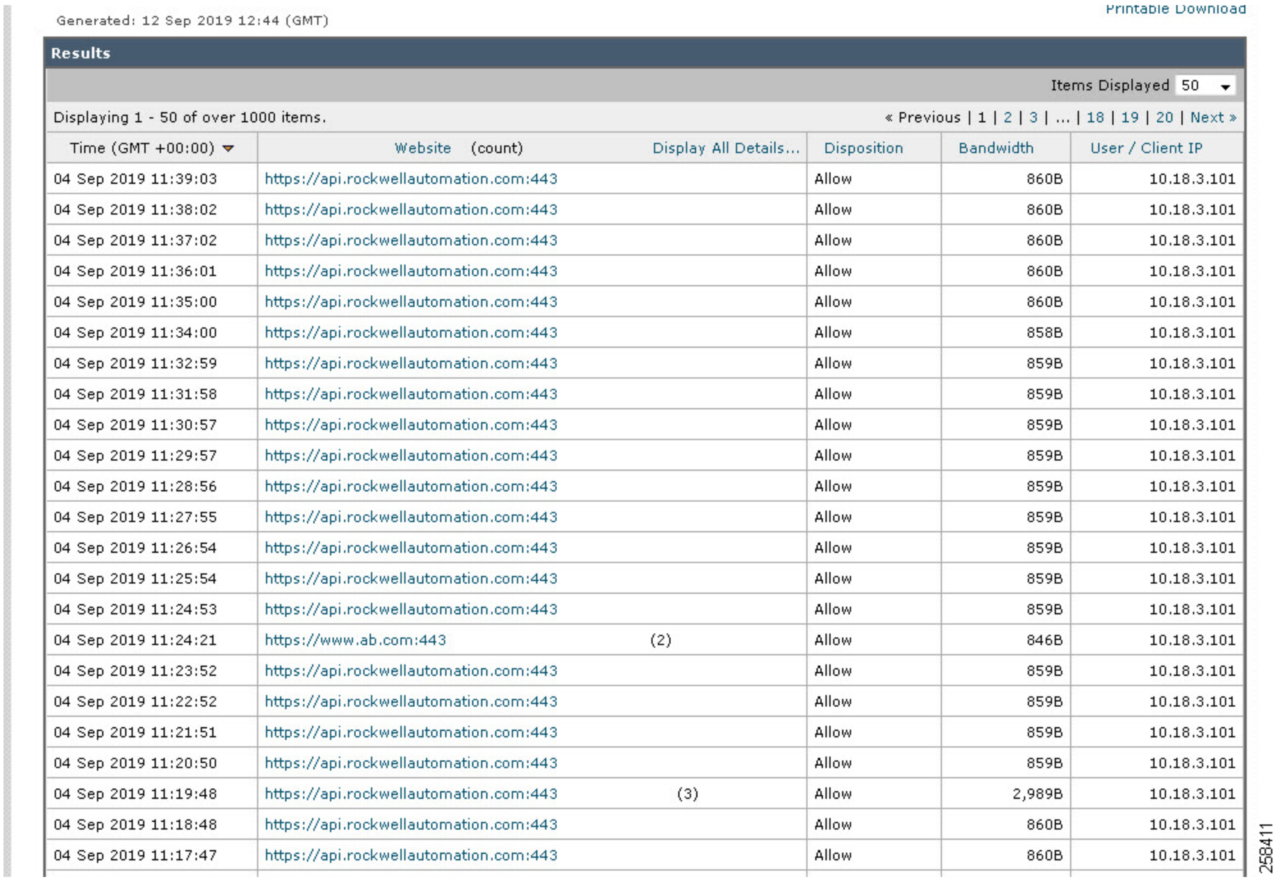
URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Computers and Internet	1.9MB	85:58	16.2k	1,470	17.7k
Business and Industry	15.3MB	116:24	23	9,751	9,774
Software Updates	850.3KB	00:00	0	1,035	1,035
URL Filtering Bypassed	229.7MB	00:48	0	770	770
Uncategorized URLs	375.9KB	01:20	0	545	545
Infrastructure and Content Delivery Netw...	29.7KB	00:47	172	41	213
Search Engines and Portals	0B	01:13	184	0	184
Computer Security	15.8KB	00:00	0	14	14
News	0B	00:00	4	0	4
SaaS and B2B	0B	00:00	2	0	2
Totals (all available data):	248.2MB	206:34	16.6k	13.6k	30.2k

Similar to the previous page, this report on user 10.18.3.101 has additional hyperlinks that can provide more details about the content the user is viewing. In Figure 4-5, clicking one of the numbers in the transactions completed column will provide the URLs that were accessed by the user under each individual URL category.

Figure 4-6 shows the breakdown of the URLs that have been accessed by the user. Additional information, such as full URL, content type, destination IP address, and Cisco WSA independent tracking can be accessed by clicking the individual URLs.

Figure 4-6 User URL Reporting



Printable Download

Generated: 12 Sep 2019 12:44 (GMT)

Results

Items Displayed 50

Displaying 1 - 50 of over 1000 items. « Previous | 1 | 2 | 3 | ... | 18 | 19 | 20 | Next »

Time (GMT +00:00)	Website (count) Display All Details...	Disposition	Bandwidth	User / Client IP
04 Sep 2019 11:39:03	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:38:02	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:37:02	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:36:01	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:35:00	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:34:00	https://api.rockwellautomation.com:443	Allow	858B	10.18.3.101
04 Sep 2019 11:32:59	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:31:58	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:30:57	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:29:57	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:28:56	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:27:55	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:26:54	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:25:54	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:24:53	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:24:21	https://www.ab.com:443 (2)	Allow	846B	10.18.3.101
04 Sep 2019 11:23:52	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:22:52	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:21:51	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:20:50	https://api.rockwellautomation.com:443	Allow	859B	10.18.3.101
04 Sep 2019 11:19:48	https://api.rockwellautomation.com:443 (3)	Allow	2,989B	10.18.3.101
04 Sep 2019 11:18:48	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101
04 Sep 2019 11:17:47	https://api.rockwellautomation.com:443	Allow	860B	10.18.3.101

There are many filtering options offered in the reporting and web tracking pages of the Cisco WSA to fine-tune and search specific URLs, actions, file sizes, etc.

Cisco CLI Verification and Troubleshooting

Since most WCCP deployment will rely on Layer 2 redirection, a good first step in troubleshooting deployment issues is to ensure that the WCCP device is able to ping the Cisco WSA. Additionally, using debug tools for WCCP is uninstructive about the performance of the device due to the low number of messages that are generated. In addition to general debugging, the **show** commands can provide helpful information about the state of the deployment and the status of the current redirection service ID.

Note Some devices exclude the **ip** in the command. For example, the above command **show ip wccp** is valid on a Catalyst 4500X, but on the Cisco ASA 5525 the command is **sh wccp**.

Table 4-1 WCCP Debug and Detail Commands

Debug Command	Result
show ip wccp web-cache detail	Displays proxy server and WCCP router statistics for a particular service group.
show ip wccp <service ID> view	Displays service group information.
debug ip wccp events	Displays information about significant WCCP events.
debug ip wccp packets	Displays information about every WCCP packet received or sent by the router.

Examples of the debug types of messages you will see are shown below:

- WCCP-EVNT:D90: Here_I_Am packet from 10.19.1.37: authentication failure
  - This indicates that if authentication (a password) is used for the WCCP service, there is a mismatch between the WCCP device and the Cisco WSA configuration.
- After initial configuration, verification of the WCCP success is shown:
  - WCCP-PKT:D90: Sending I_See_You packet to 10.18.3.37 w/ rcv_id 00000001
  - WCCP-EVNT: Adding NP rule to exclude WCCP redirection of web cache 10.18.3.37
  - WCCP-PKT:D90: Received valid Here_I_Am packet from 10.18.3.37 w/rcv_id 00000001
  - WCCP-EVNT:D90: Built new router view: 1 routers, 1 usable web caches, change # 00000002
  - WCCP-PKT:D90: Sending I_See_You packet to 10.18.3.37 w/ rcv_id 00000002

Table 4-2 Device Commands

Command	Result
show ip wccp	Displays global WCCP statistics.
show ip wccp <service ID>	Displays information about all known proxies.
show ip interface	Displays whether web cache redirecting is enabled on an interface.
show ip wccp / show ip wccp <service ID>	Displays a count of the number of packets redirected.
clear ip wccp	Clears the counter displayed by the show ip wccp and show ip wccp web-caches.

Using the **sh wccp** command, general information regarding the WCCP service can be viewed:

```
device# sh wccp 90
```

Table 4-3 Global WCCP Information

Router information:		
Router identifier	10.100.2.254	Defines the address and the devices ID. If this does not list an IP address, the Cisco WSA and the device may not be able to communicate.
Protocol version	2.0	Defines the WCCP version.

Table 4-3 Global WCCP Information (continued)

Router information:		
Service Identifier	90	Defines the Service ID that is shared with the Cisco WSA.
Number of Cache Engines	1	Defines number of Proxies in the group.
Number of Routers	1	Defines how many other devices are redirecting.
Total Packets Redirected	40	Defines the amount of traffic WCCP has sent to the Cisco WSA.
Redirect access-list	WCCP_Redirect	Defines which access-list is used to determine adjacency.
Total Connections Denied Redirect	0	Define how many packets were blocked.
Total Packets Unassigned	0	Defines how many packets did not fit into a category.
Group access-list	-none-	Defines which traffic should be redirected.
Total Messages Denied to Group	0	Defines how many messages were not sent due to the group access-list.
Total Authentication Failures	4	Invalid password between device and Cisco WSA.
Total Bypassed Packets Received	0	Packets set to bypass redirection.

APPENDIX A

References

This appendix includes the following reference sections:

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing—Converged Plantwide Ethernet
  http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures—Converged Plantwide Ethernet
  http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf
- Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf

- Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site:
http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide:
  - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html
- OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide:
  - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td018_-en-p.pdf
  - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/WP/CPwE-5-1-OEM-WP/CPwE-5-1-OEM-WP.html
- Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide:
  - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf
  - Cisco site:
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture Design Guide:
  - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td014_-en-p.pdf

  - Cisco site:
    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Deploying Network Security within a Converged Plantwide Ethernet Architecture:
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture:
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html
- Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture:
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/PRP/DIG/CPwE-5-1-PRP-DIG.html

Rockwell Automation FactoryTalk

- FactoryTalk
  https://www.rockwellautomation.com/rockwellsoftware/overview.page

Cisco IoT Threat Defense

- Cisco IoT Threat Defense
  https://www.cisco.com/c/en/us/solutions/security/iot-threat-defense/index.html
- Cisco Web Security Appliance (WSA)
  https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html
- Outbound Security—Cisco Umbrella
  https://umbrella.cisco.com/

APPENDIX B

Acronyms and Initialisms

.

Table B-1 Acronyms and Initialisms

Term	Definition
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
ASDM	Cisco Adaptive Security Device Manager
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CE	Cache Engine
CIP	Common Industrial Protocol
CoA	Change of Authorization
CPwE	Converged Plantwide Ethernet
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CVD	Cisco Validated Design
DIG	Design and Implementation Guide
DACL	Downloadable Access Control List
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol

Table B-1 Acronyms and Initialisms (continued)

Term	Definition
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name System
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
DSS	Data Security Standard
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EDI	Electronic Data Interchange
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
ETA	Cisco Encrypted Traffic Analytics
FIB	Forwarding Information Base
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
HL7	Health Level 7
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IES	Industrial Ethernet Switch (Allen-Bradley Stratix, Cisco IE)
IFW	Industrial Firewall
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPDT	IP Device Tracking
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology
LBS	Location Based Services
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation

Table B-1 Acronyms and Initialisms (continued)

Term	Definition
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAN	Policy Administration Node
PAT	Port Address Translation
PCI	Payment Card Industry
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PHI	Protected Health Information
PII	Personally-Identifiable Information
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
PSN	Policy Service Node
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SHA	Secure Hash Standard
SIG	Secure Internet Gateway

Table B-1 Acronyms and Initialisms (continued)

Term	Definition
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
SYN	Synchronization
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
WAN	Wide Area Network
WCCP	Web Cache Communication Protocol
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

APPENDIX C

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation which follows the Cisco Validated Design (CVD) program.

CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to help achieve faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.
- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).
- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.
- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific sets of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see the Cisco Validated Designs at the following URL:

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

Panduit Corp. is a world-class provider of engineered, flexible, end-to-end electrical and network connectivity infrastructure solutions that provides businesses with the ability to keep pace with a connected world. Our robust partner ecosystem, global staff, and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com

US and Canada:
Panduit Corp.
World Headquarters
18900 Panduit Drive
Tinley Park, IL 60487
iai@panduit.com
Tel. 708.532.1800

Asia Pacific:
One Temasek Avenue #09-01
Millenia Tower
039192 Singapore
Tel. 65 6305 7555

Europe/Middle East/Africa:
Panduit Corp.
West World
Westgate London W5 1XP Q
United Kingdom
Tel. +44 (0) 20 8601 7219

Latin America:
Panduit Corp.
Periférico Pte Manuel Gómez
Morin #7225 - A
Guadalajara Jalisco 45010
MEXICO
Tel. (33) 3777 6000

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to be more productive and the world more sustainable. In support of smart manufacturing concepts, Rockwell Automation helps customers maximize value and prepare for their future by building a Connected Enterprise.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000
Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788
Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600
Fax: (32) 2 663 0640

Publication ENET-TD017B-EN-P January 2020