Preface

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

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

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

Release Notes

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

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

Summary of Specific Changes

This document contains the following changes from the previous version:

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

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

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

Document Organization

This document is composed of the following chapters and appendices:

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

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

For More Information

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

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

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

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