THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

TRC Tech Talks

Online Seminars

Secure Cloud Connectivity to CPwE

June 2nd, 2020

Introductions

Brandon Singh
Presenter
Network Specialist
The Reynolds Company
– Dallas / Fort Worth

Mike Masterson
Panelist
Automation Specialist
The Reynolds Company
– Houston

Joe Belaschky
Panelist
Automation / Network
Specialist
The Reynolds Company
– Houston

2020 Online Events - Register to receive a calendar invite

User Group

Thursday, June 18

ControlLogix Redundancy
10:00 am

Tech Talks

Wednesday, June 3rd

Overload Migration
10:00 am

Thursday, June 4th

Industrial Networking Series Part 3: Resilient Networks – Device Level Ring (DLR)
10:00 am

Tuesday, June 16th

Industrial Networking Series Part 4: Resilient Networks – Parallel Redundancy Protocol (PRP)
10:00 am

Wednesday, June 17th

Industrial Networking Series Part 5: Connected Plantwide Ethernet Architectures
10:00 am

Tuesday, June 23rd

Industrial Networking Series Part 6: Securing Control System Network with CIP Security
10:00 am

https://www.reynoldsonline.com/eventsUnit.action

ROKLive

ROK VIRTUAL LIVE

A Rockwell Automation Virtual Event

June 10 – 19, 2020
Online/Virtual Seminars & Labs
Registration opens in May

CLOUD CONNECTIVITY TO A CONVERGED PLANTWIDE ETHERNET ARCHITECTURE

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Design Guide

Design Guide

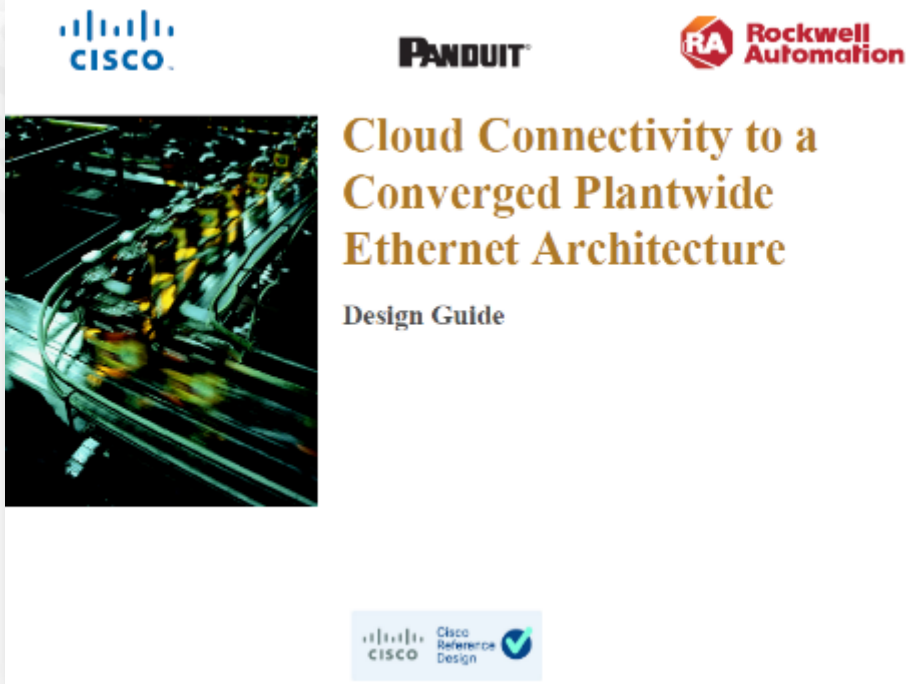
- ENET-TD017

Whitepaper

- ENET-WP019

Updates to the existing document include:

- Upgrade from Application Guide to Cisco Reference Design
- Extensions to technology use cases
- Extensions to test results and details
- Addition of the Cisco Web Security Appliance and related infrastructure configuration
- Addition of technology troubleshooting and verification



Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Design Guide

Cisco Reference Design

Agenda

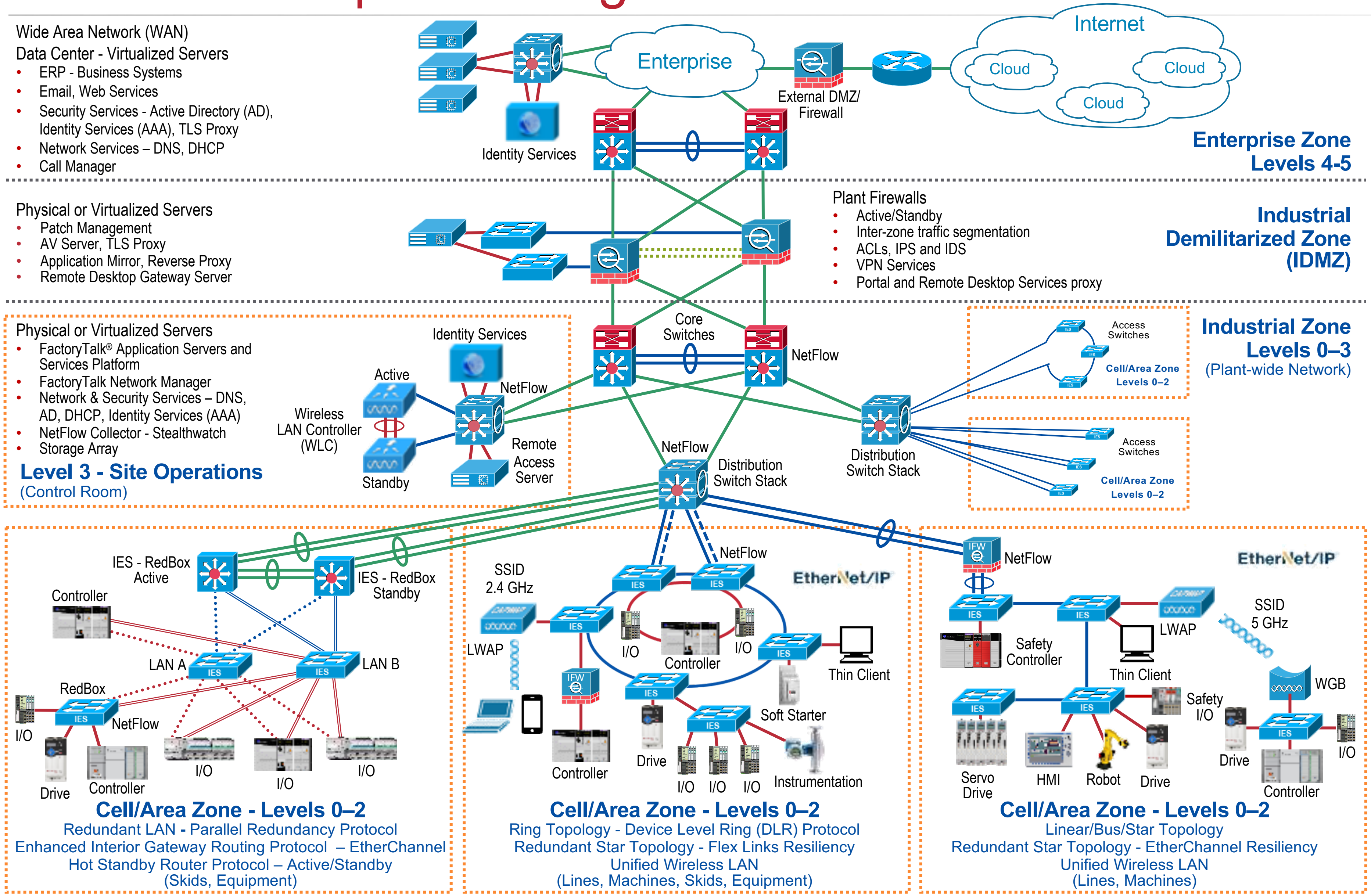
1 Overview

2 Review of Use Cases

3 Technology Considerations

CPwE Overview

Converged Plantwide Ethernet (CPwE), a holistic blueprint for digital transformation



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

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)

Industrial Zone Levels 0–3
(Plant-wide Network)

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)

Collection of tested and validated network and security architectures

Simplify network and security design by connecting industrial operations and business systems

An open solution that adheres to regulatory standards creates flexibility and scalability

A converged infrastructure built on a common architecture framework makes the network data-ready

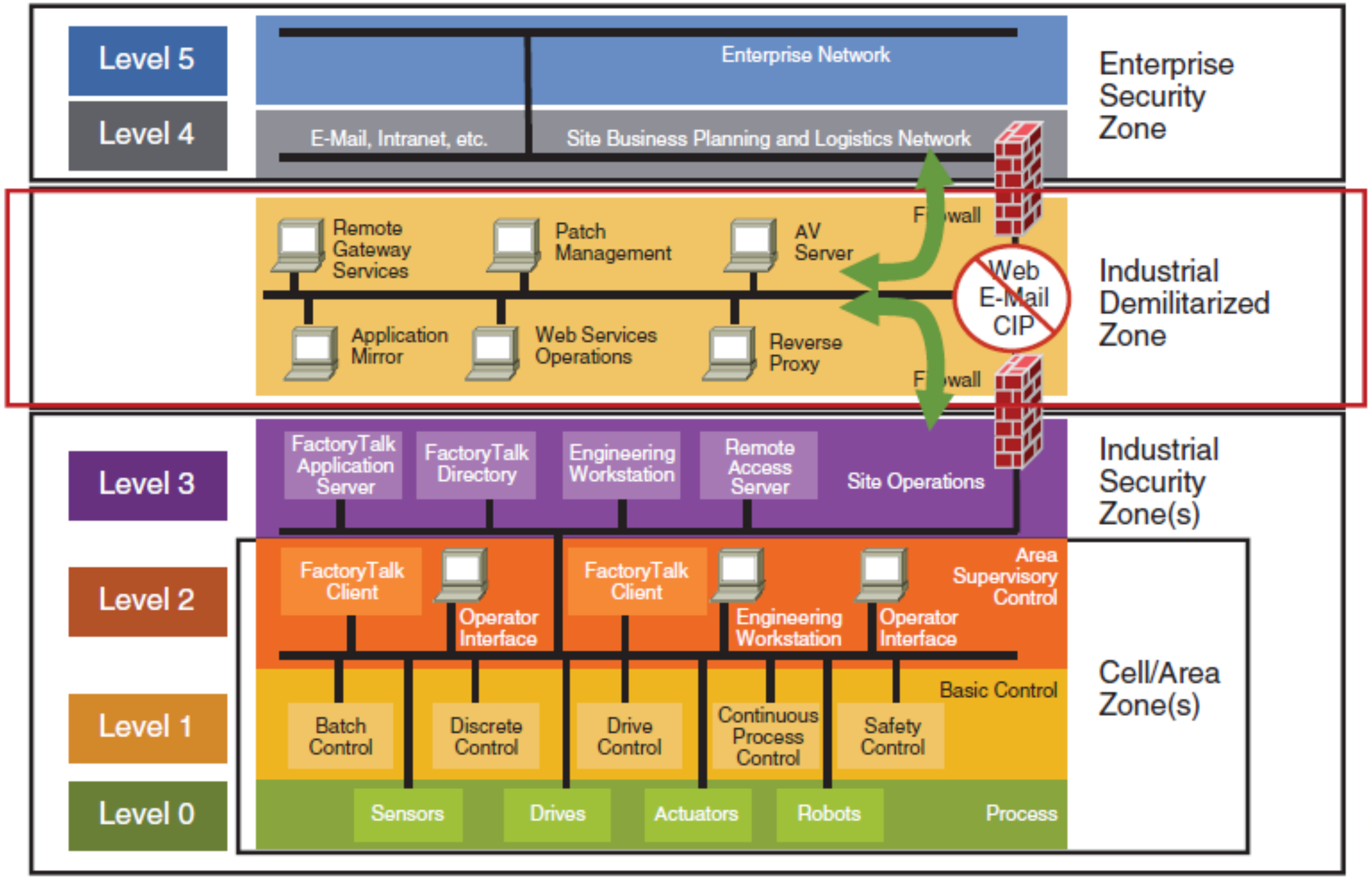
CPwE Reference Architecture

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Logical Design

CPwE logical model employs commonly used industry standards such as

- Purdue Model and ISA95
  - Control Hierarchy to organize the plant functions into levels
- IEC-62443 (formerly ISA99)
  - Organizes the levels into channels, zones and conduits

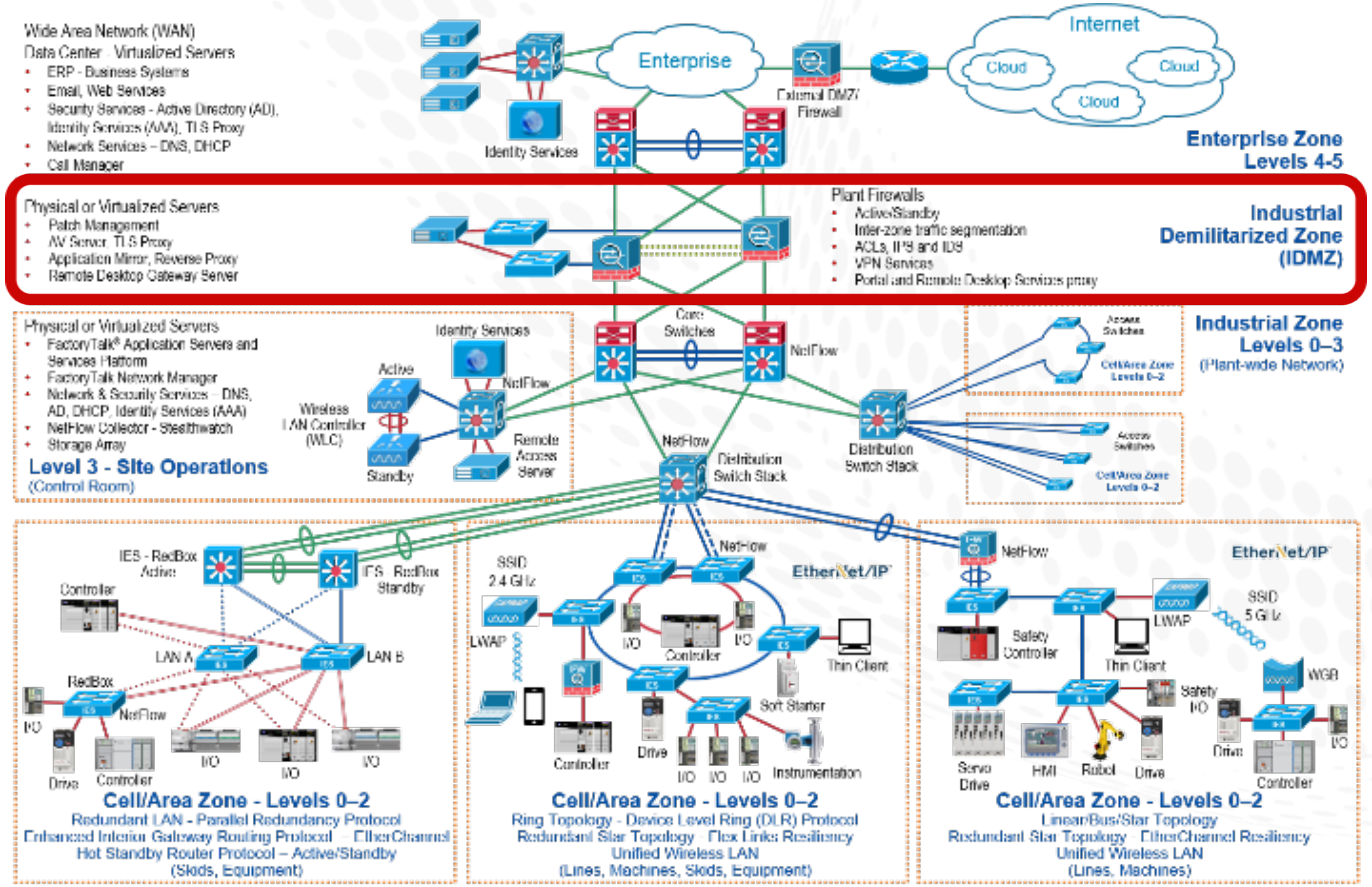


Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Industrial Demilitarized Zone (IDMZ)

- Key tenant in the Platinum, Gold, and Silver architectures is the use of the IDMZ
- Provides a buffer between the Enterprise and Industrial Zone
- The IDMZ provides multiple methods to securely broker data to and from the Enterprise and Industrial Zones
  - Application mirrors, such as a PI-to-PI interface for FactoryTalk Historian.
  - Microsoft® Remote Desktop Gateway (RDG) services.
  - Cisco Web Security Appliance with TLS proxy server capabilities.



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
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
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
LWAP
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)
NetFlow
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
WGB
Safety I/O
I/O
Drive
Servo Drive
HMI
Robot
Drive
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

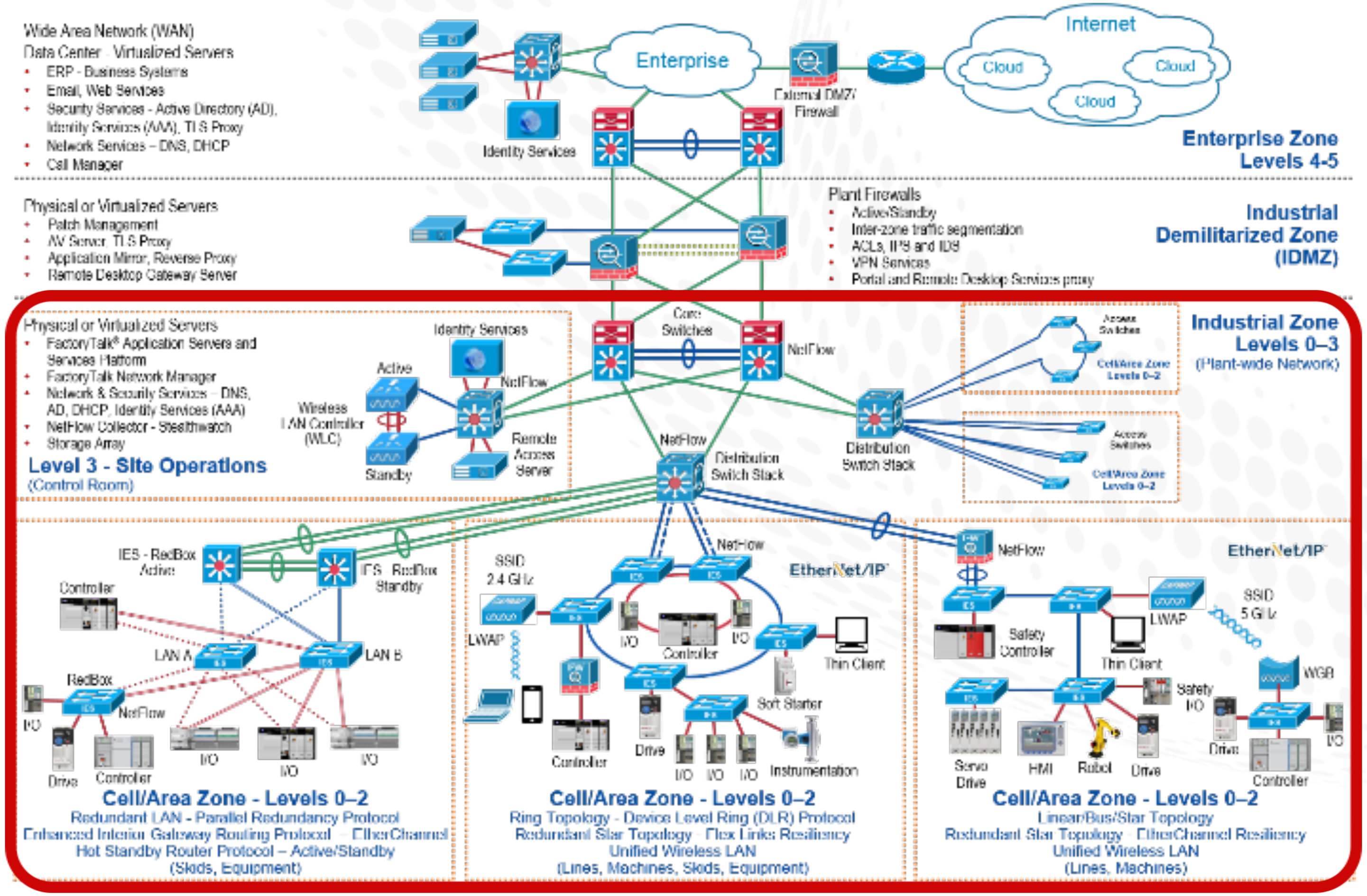
Rockwell Automation

CPwE Reference Architecture

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Industrial Zone

- The Industrial Zone (Levels 0-3) contains the Cell/Area Zone(s) (Levels 0 to 2) and Site Operations (Level 3)
- To preserve smooth industrial operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the enterprise operations



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

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)

Industrial Zone
Levels 0–3
(Plant-wide Network)

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)

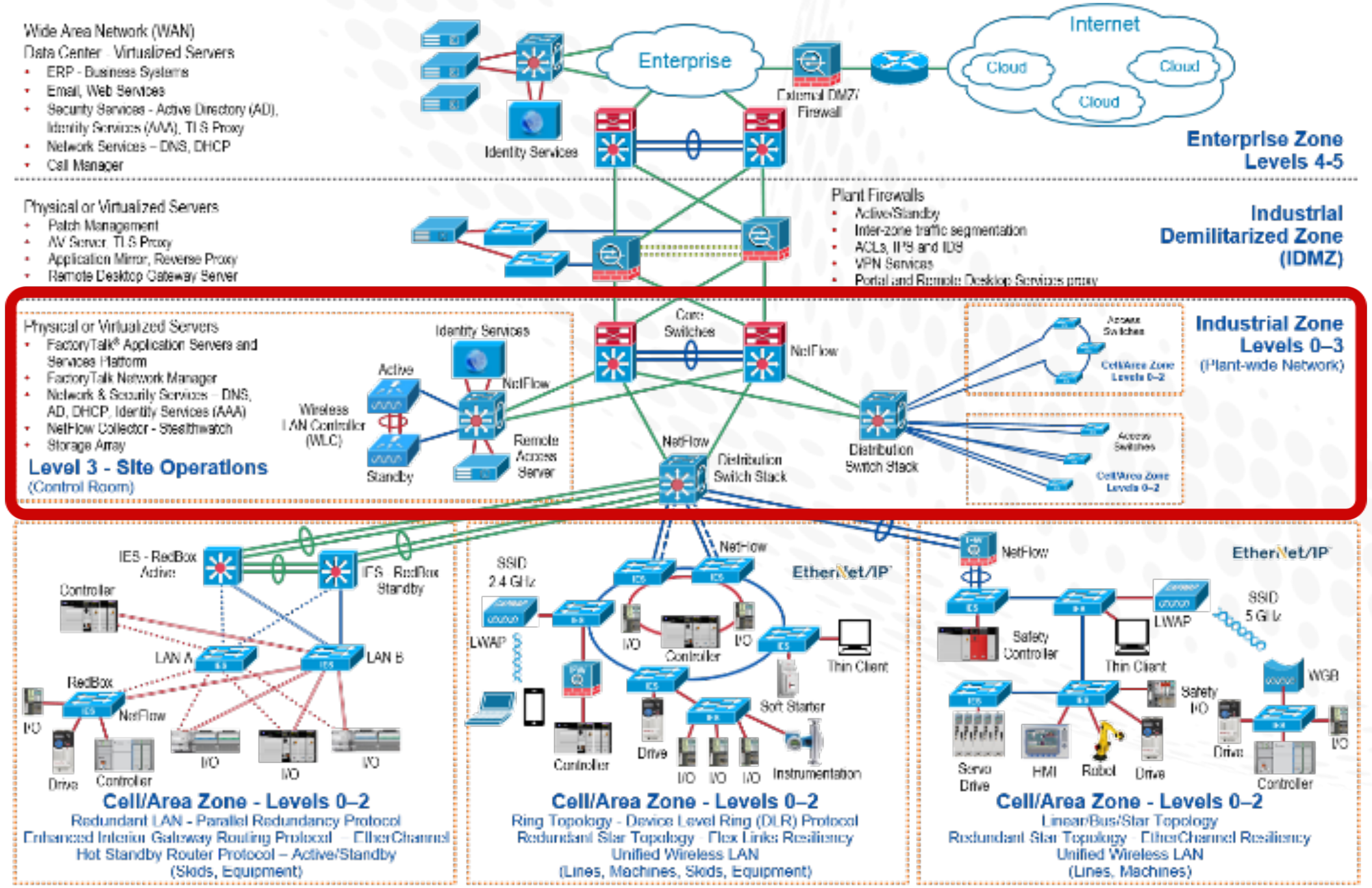
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

CPwE Reference Architecture

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Level 3 Site Operations

- Level 3 Site Operations contains the assets that are critical to monitoring and controlling the plant-wide or site-wide industrial operations



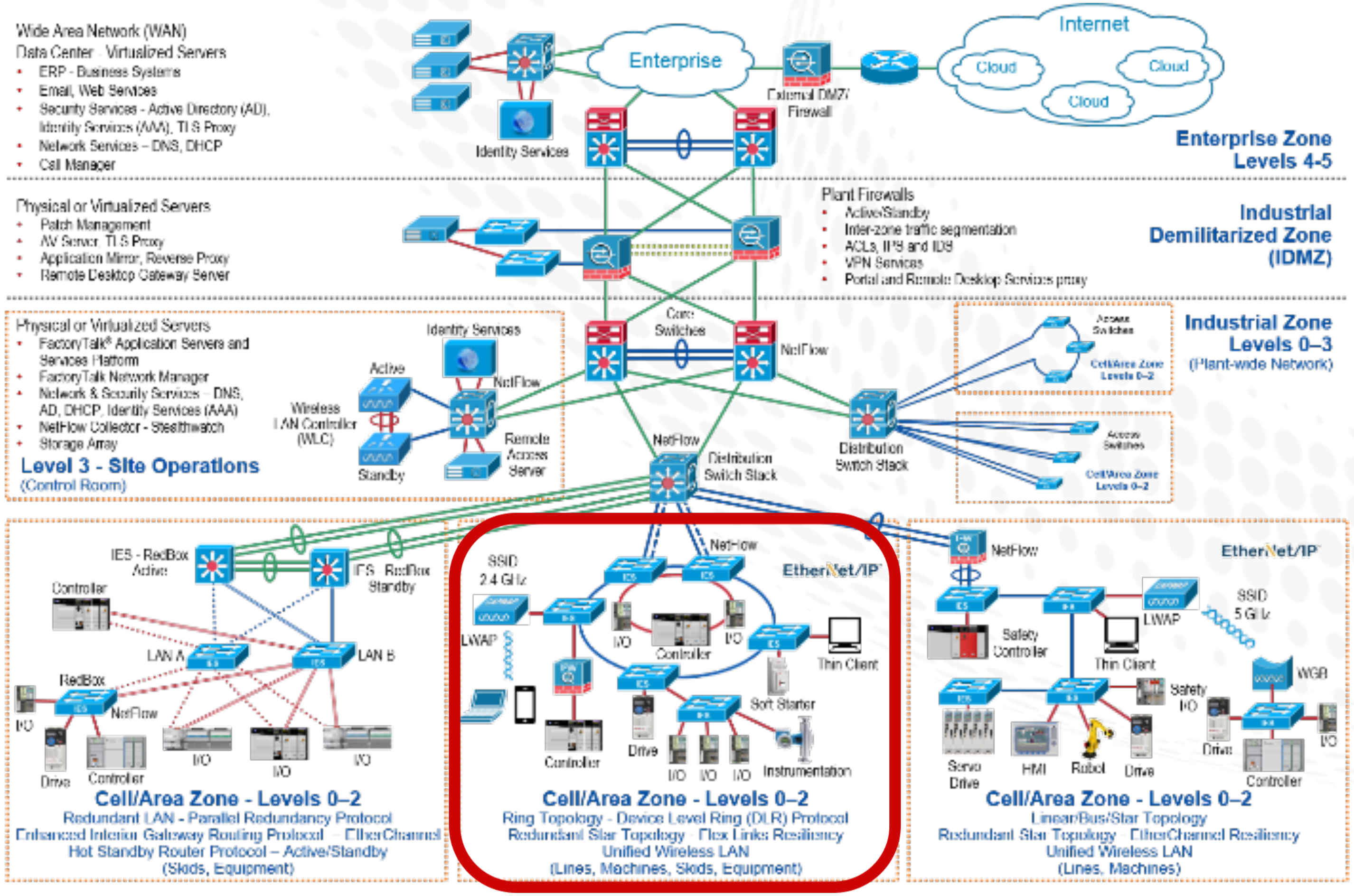
Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise 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
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
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)
NetFlow
EtherNet/IP
LWAP
SSID 5 GHz
Safety Controller
Thin Client
Safety I/O
WGB
Drive
I/O
Servo Drive
HMI
Robot
Drive
Controller
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

CPwE Reference Architecture

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Cell/Area Zone

- A functional zone where Level 0-2 IACS assets interact with each other. This area is critical because IACS assets must communicate to ensure that industrial operations continue



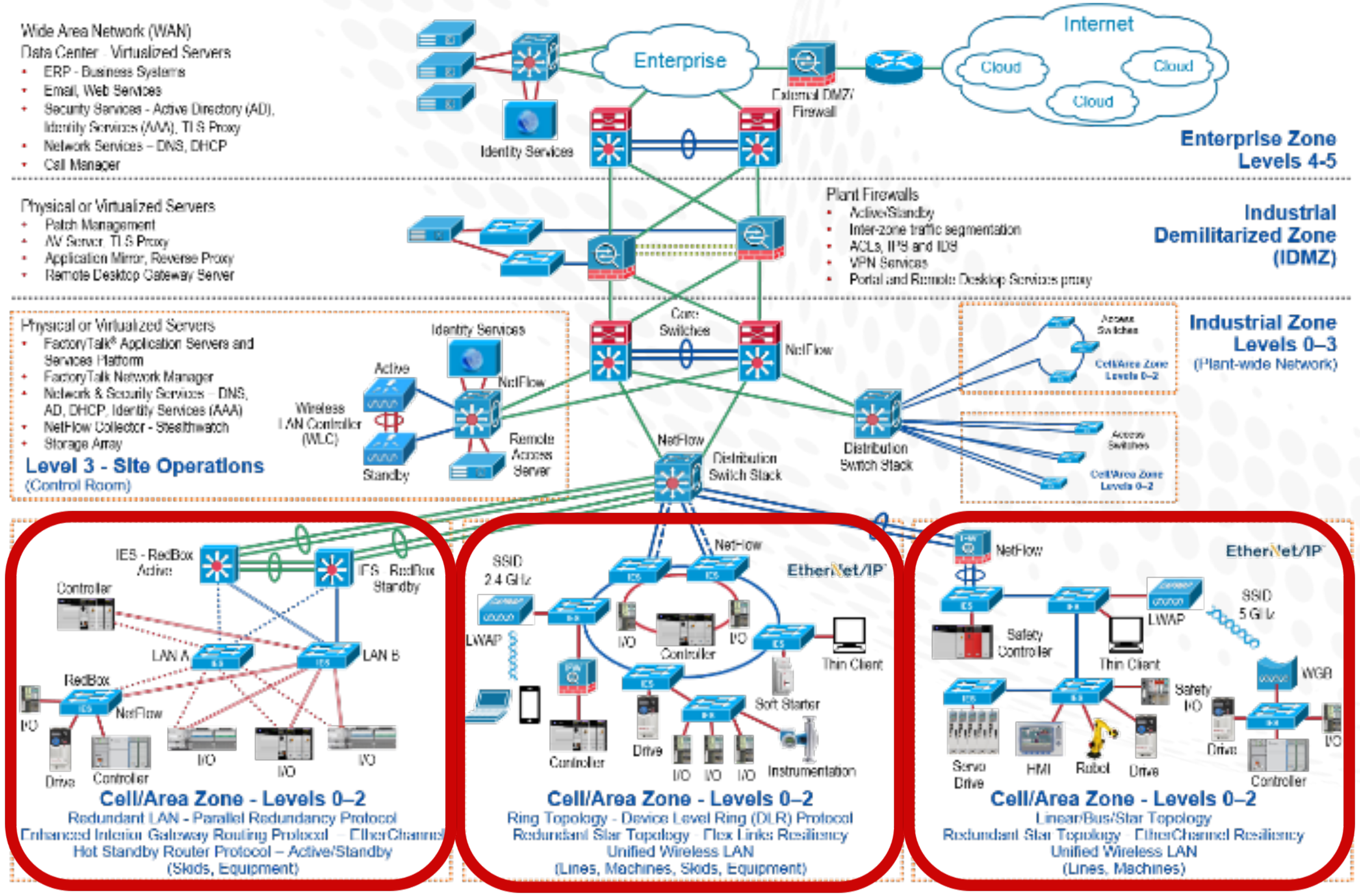
Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise 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
Wireless LAN Controller (WLC)
Standby
NetFlow
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
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)
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)

CPwE Reference Architecture

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Cell/Area Zone

- A functional zone where Level 0-2 IACS assets interact with each other. This area is critical because IACS assets must communicate to ensure that industrial operations continue
- A plant-wide or site-wide architecture may have one or multiple Cell/Area Zones.
  - Each can have the same or different network topologies
- In general, for the Cloud Connectivity to a Converged Plantwide Ethernet Architecture, the Cell/Area Zone design choice is not relevant



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

Physical or Virtualized Servers
- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

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)

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

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone
(IDMZ)

Industrial Zone
Levels 0–3
(Plant-wide Network)

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)

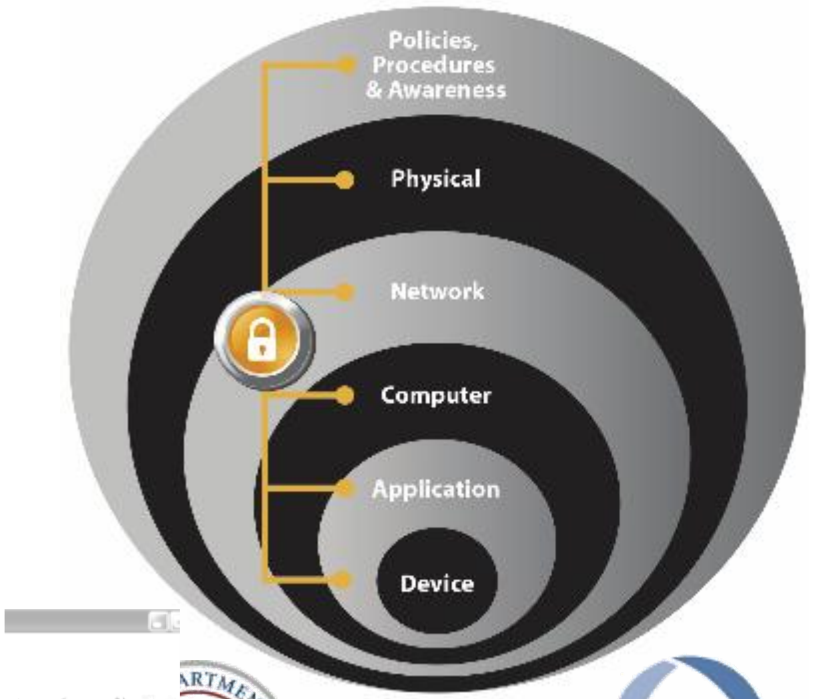
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

Defense-in-Depth

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

A secure application depends on multiple layers of diverse protection and industrial security must be implemented as a system



- **Defense in Depth**
- Shield targets behind multiple levels of diverse security countermeasures to reduce risk
- **Openness**
- Consideration for participation of a variety of vendors in our security solutions
- **Flexibility**
- Able to accommodate a customer's needs, including policies & procedures
- **Consistency**
- Solutions that align with Government directives and Standards Bodies

Rockwell Automation

Defense-in-Depth

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

A secure application depends on multiple layers of diverse protection and industrial security must be implemented as a system

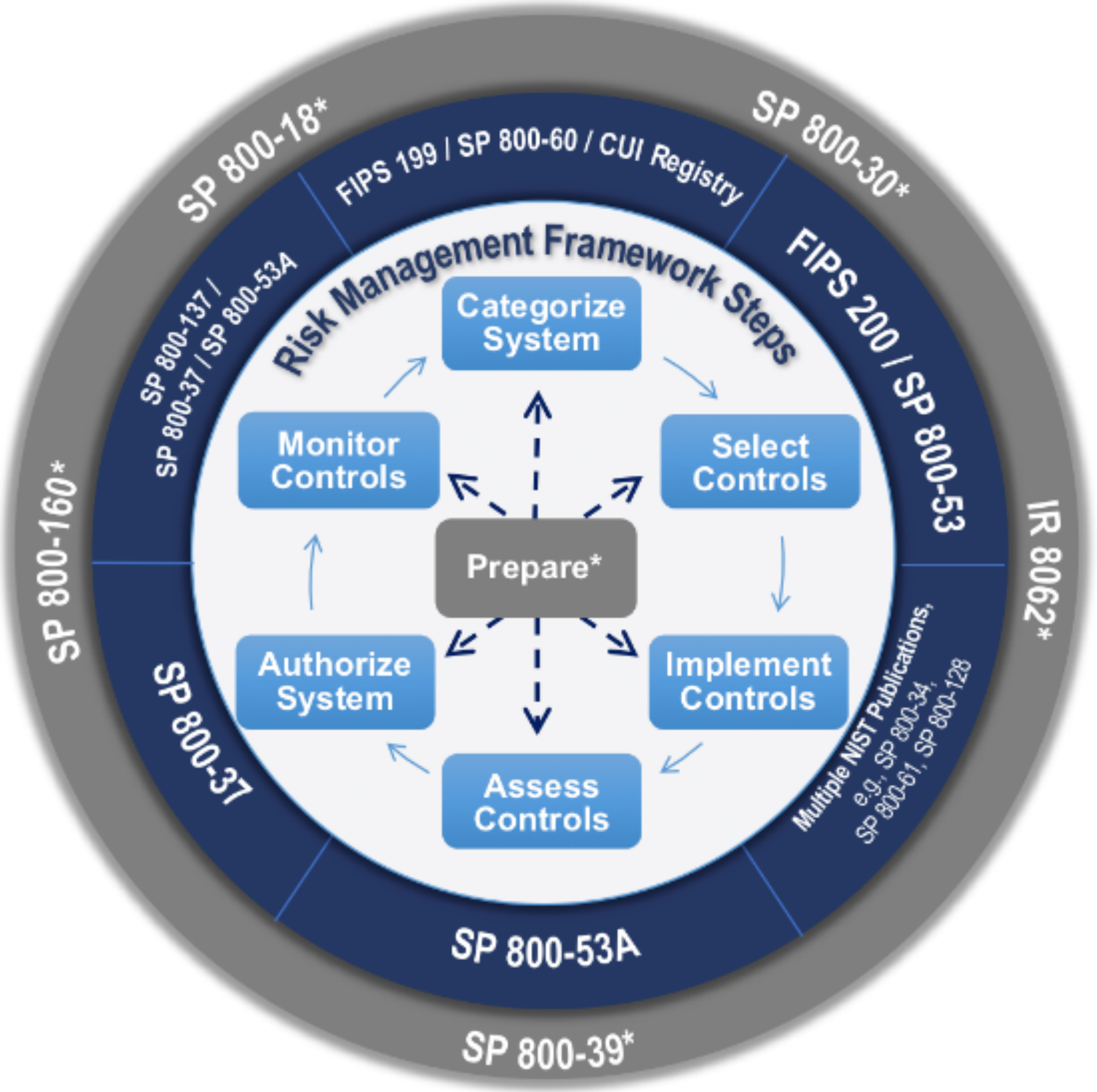
- ***Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture*** *outlines several industrial security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide IACS network infrastructure*
  - *https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf*
- ***Deploying Network Security within a Converged Plantwide Ethernet Architecture*** *outlines several network security use cases for plant-wide Industrial Automation and Control System (IACS) network infrastructure. These use cases include segmentation, visibility, anomaly detection and mitigation and intent-based security for OT*
  - *https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf*
- ***Securely Traversing IACS Data Across the Industrial Demilitarized Zone*** *details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data to the Enterprise*
  - *https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf*
- ***Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture*** *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*
  - *https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf*

Defense-in-Depth

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Risk Assessments and Risk Management

- The management of organizational risk is a key element in the organization's security program
    - Provides an effective framework for selecting the security controls necessary to protect individuals and the operations and assets
- The NIST Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle



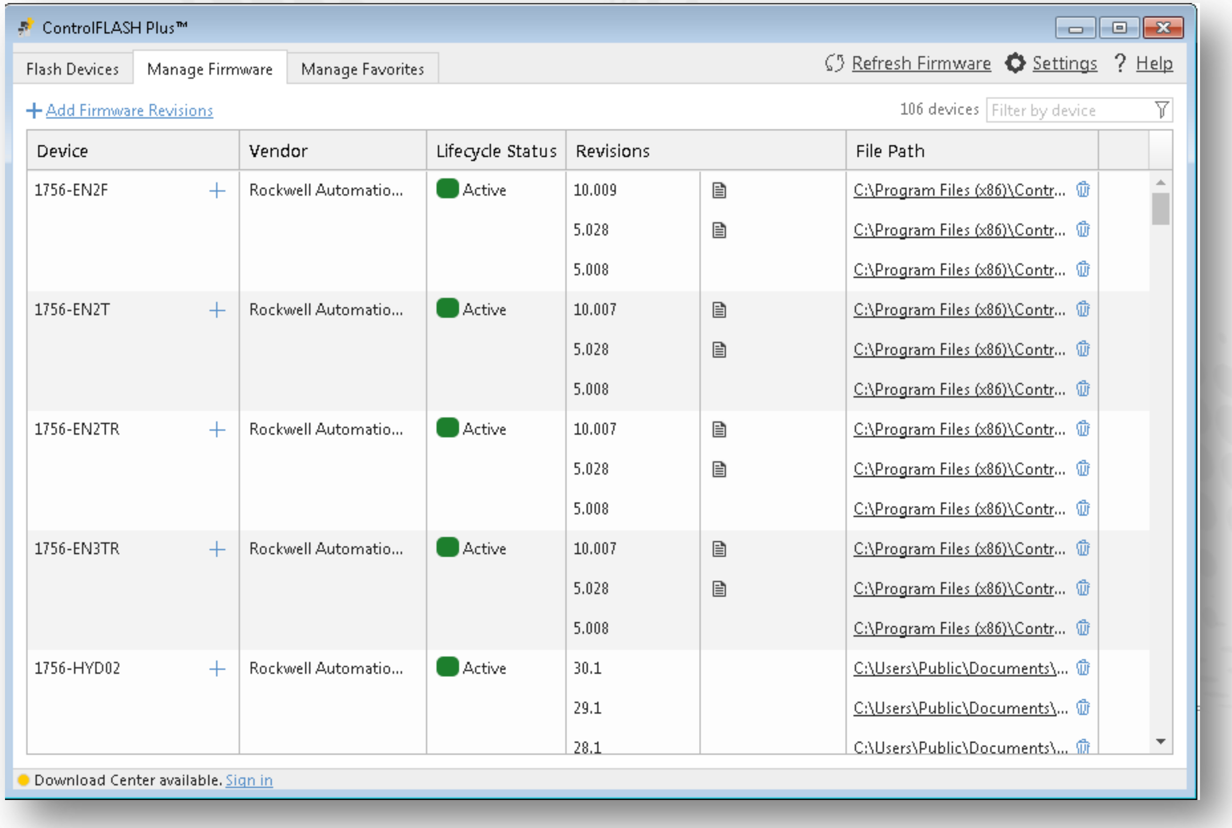
Review of Use Cases

Cloud Connectivity Use Cases

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

ControlFLASH Plus

- ControlFLASH Plus has the ability to reach out to the cloud to check Lifecycle Status and revision availability of the specific devices. This information is obtained from Rockwell Automations Product Compatibility and Download Center (PCDC) via an API
- When signed into the Product Compatibility and Download Center within ControlFLASH Plus cloud connectivity allows you to download firmware revisions, release notes and view important notices
- Cloud endpoints (URLs) that ControlFLASH Plus may reach out to via TLS/HTTPS reside within the rockwellautomation.com high-level domain



106 devices

Device		Vendor	Lifecycle Status	Revisions		File Path
1756-EN2F	+	Rockwell Automatio...	🟩 Active	10.009	🗎	C:\Program Files (x86)\Contr...
				5.028	🗎	C:\Program Files (x86)\Contr...
				5.008		C:\Program Files (x86)\Contr...
1756-EN2T	+	Rockwell Automatio...	🟩 Active	10.007	🗎	C:\Program Files (x86)\Contr...
				5.028	🗎	C:\Program Files (x86)\Contr...
				5.008		C:\Program Files (x86)\Contr...
1756-EN2TR	+	Rockwell Automatio...	🟩 Active	10.007	🗎	C:\Program Files (x86)\Contr...
				5.028	🗎	C:\Program Files (x86)\Contr...
				5.008		C:\Program Files (x86)\Contr...
1756-EN3TR	+	Rockwell Automatio...	🟩 Active	10.007	🗎	C:\Program Files (x86)\Contr...
				5.028	🗎	C:\Program Files (x86)\Contr...
				5.008		C:\Program Files (x86)\Contr...
1756-HYD02	+	Rockwell Automatio...	🟩 Active	30.1		C:\Users\Public\Documents\...
				29.1		C:\Users\Public\Documents\...
				28.1		C:\Users\Public\Documents\...

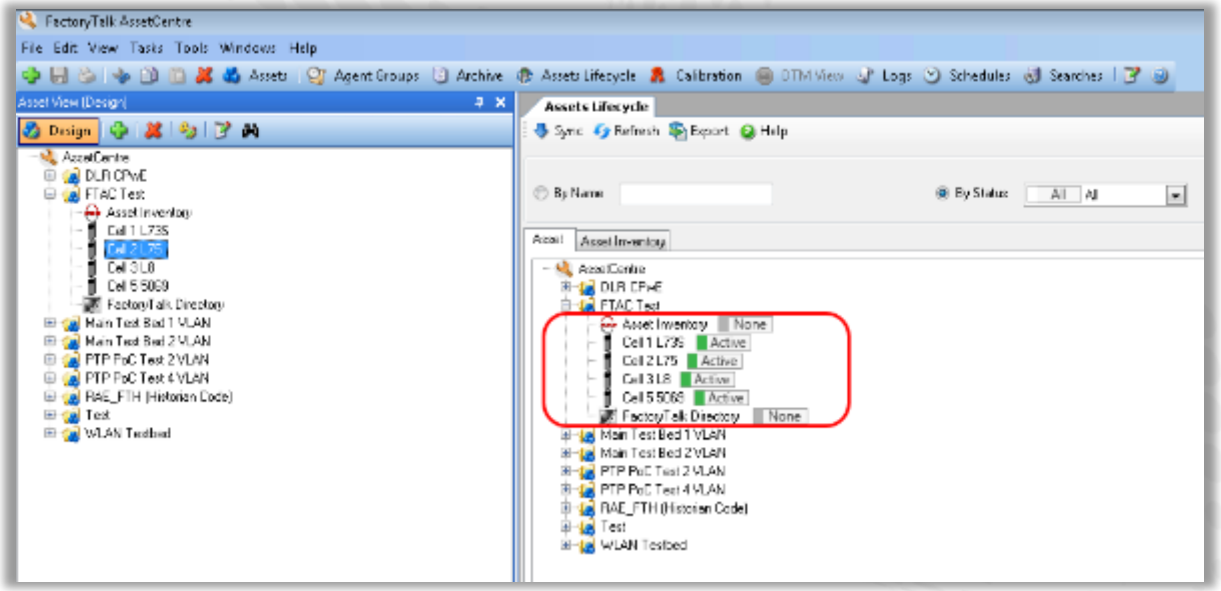
● Download Center available. Sign in

Cloud Connectivity Use Cases

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

FactoryTalk AssetCentre

- FactoryTalk AssetCentre has the ability to reach out to the cloud to check the Lifecycle Status of the specific devices. This information is obtained from Rockwell Automations Product Compatibility and Download Center via an API
- The retrieval of Lifecycle Status information from the PCDC occurs from the FactoryTalk AssetCentre server



AssetCentre
- DLR CPwE
- FTAC Test
  - Asset Inventory None
  - Cell 1 L73S Active
  - Cell 2 L75 Active
  - Cell 3 L8 Active
  - Cell 5 5069 Active
  - FactoryTalk Directory None
- Main Test Bed 1 VLAN
- Main Test Bed 2 VLAN
- PTP PoC Test 2 VLAN
- PTP PoC Test 4 VLAN
- RAE_FTH (Historian Code)
- Test
- WLAN Testbed

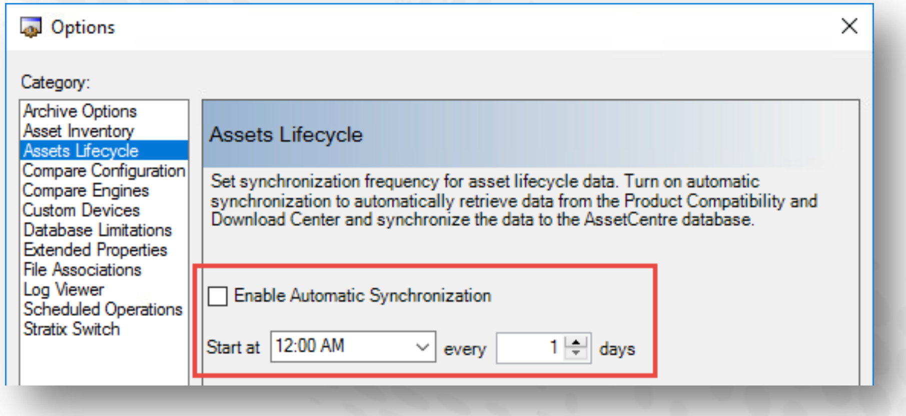
Cloud Connectivity Use Cases

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

FactoryTalk AssetCentre

- FactoryTalk AssetCentre has the ability to reach out to the cloud to check the Lifecycle Status of the specific devices. This information is obtained from Rockwell Automations Product Compatibility and Download Center via an API
- The retrieval of Lifecycle Status information from the PCDC occurs from the FactoryTalk AssetCentre server
  - This can be a scheduled or manual process initiated from the FactoryTalk AssetCentre client
- Cloud endpoints (URLs) that FactoryTalk AssetCentre may reach out to via TLS/HTTPS reside within the rockwellautomation.com high-level domain

Scheduled synchronization:



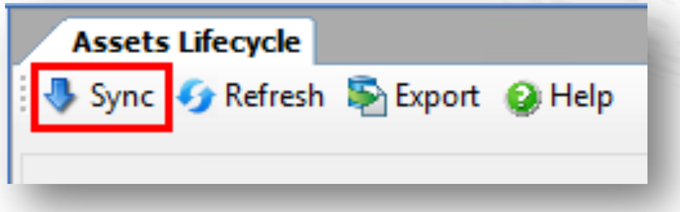
Assets Lifecycle

Set synchronization frequency for asset lifecycle data. Turn on automatic synchronization to automatically retrieve data from the Product Compatibility and Download Center and synchronize the data to the AssetCentre database.

☐ Enable Automatic Synchronization

Start at 12:00 AM every 1 days

Manual synchronization:

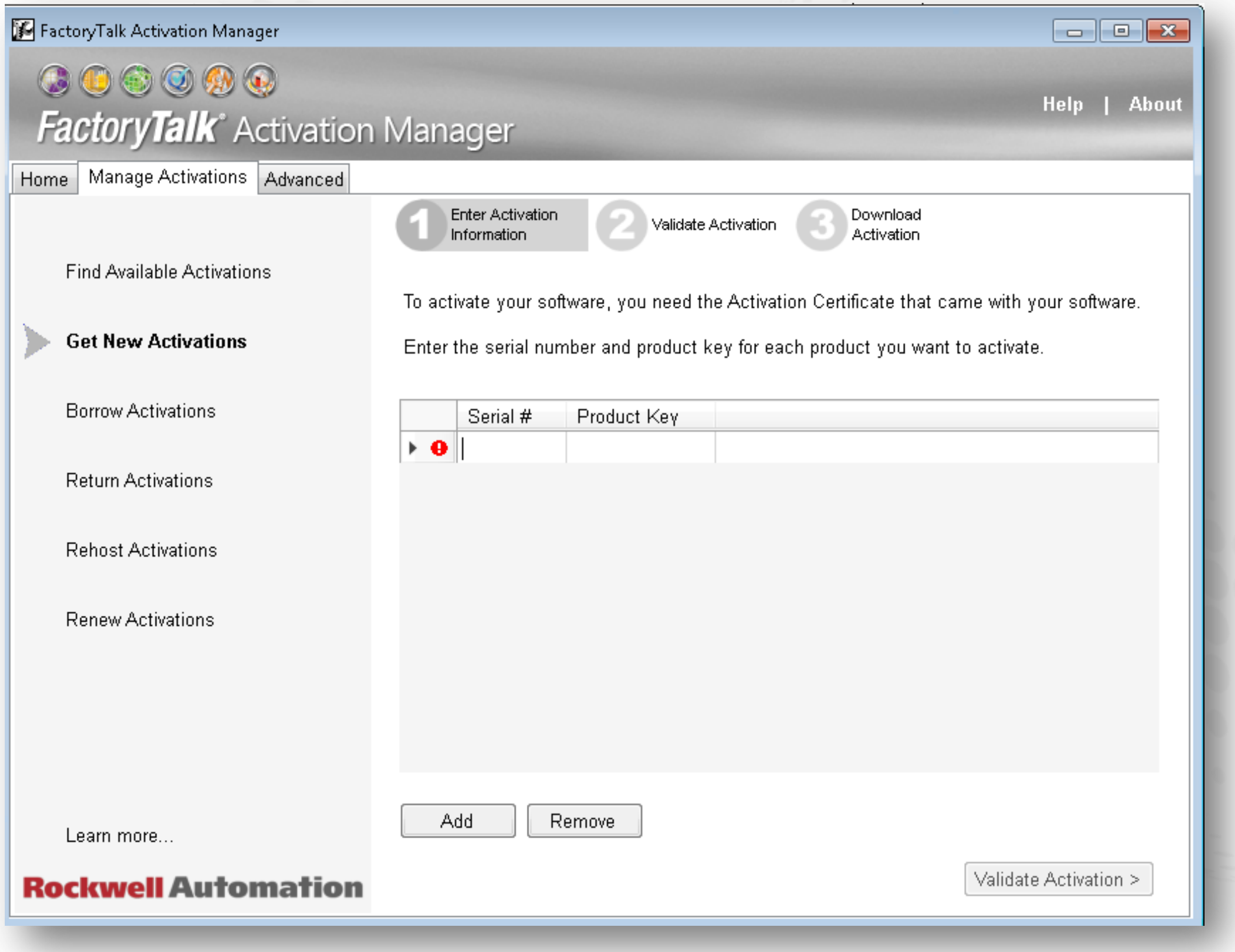


Cloud Connectivity Use Cases

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

FactoryTalk Activation Manager

- FactoryTalk Activation Manager has the ability to reach out to the cloud to obtain new activations and rehost/renew existing activations
- Cloud endpoints (URLs) that FactoryTalk Activation Manager may reach out to via TLS/HTTPS reside within the rockwellautomation.com high-level domain.



To activate your software, you need the Activation Certificate that came with your software.

Enter the serial number and product key for each product you want to activate.

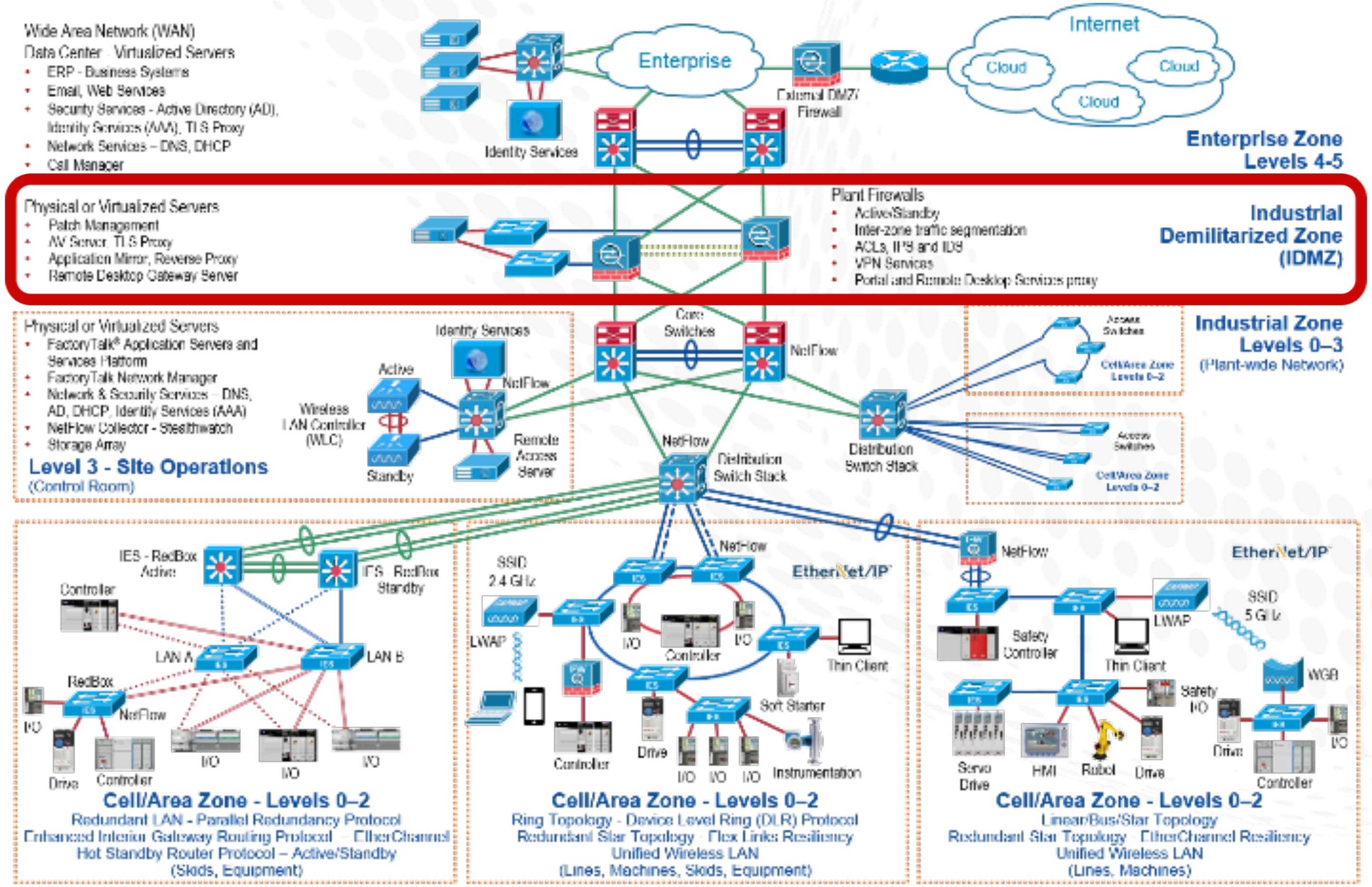
Technology Considerations

Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Industrial Demilitarized Zone (IDMZ)

- Key tenant in the Platinum, Gold, and Silver architectures is the use of the IDMZ
- Provides a buffer between the Enterprise and Industrial Zone
- The IDMZ provides multiple methods to securely broker data to and from the Enterprise and Industrial Zones
  - Application mirrors, such as a PI-to-PI interface for FactoryTalk Historian.
  - Microsoft® Remote Desktop Gateway (RDG) services.
  - Cisco Web Security Appliance with TLS proxy server capabilities.



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

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)

Industrial Zone Levels 0–3
(Plant-wide Network)

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)

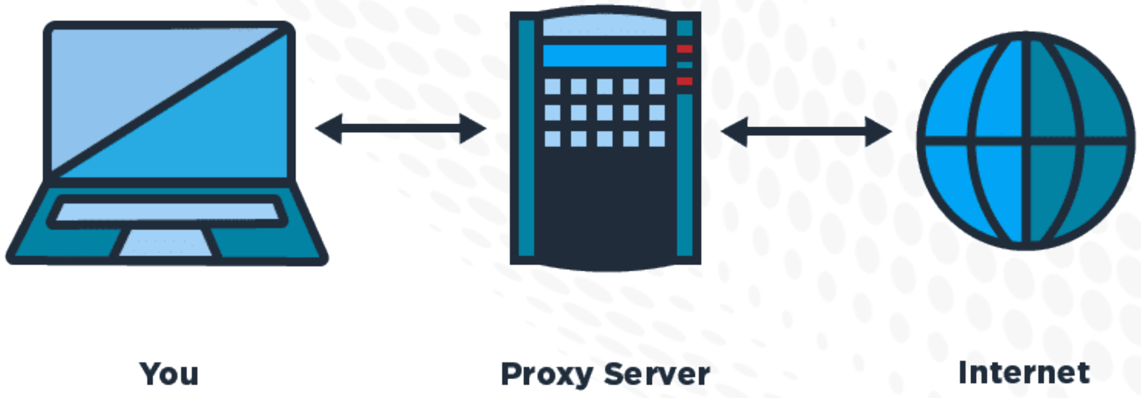
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Servers and Capabilities

- Resides between a trusted zone and untrusted zone, typically in the IDMZ
    - Intercepts requests from a client device then proceeds to make the connection on behalf of the client to the server
- Forward Proxies handle requests for a group of clients to an unknown and untrusted device outside of their control (i.e. on the Internet)
- Reverse Proxies are intended to protect servers on the same network as the clients

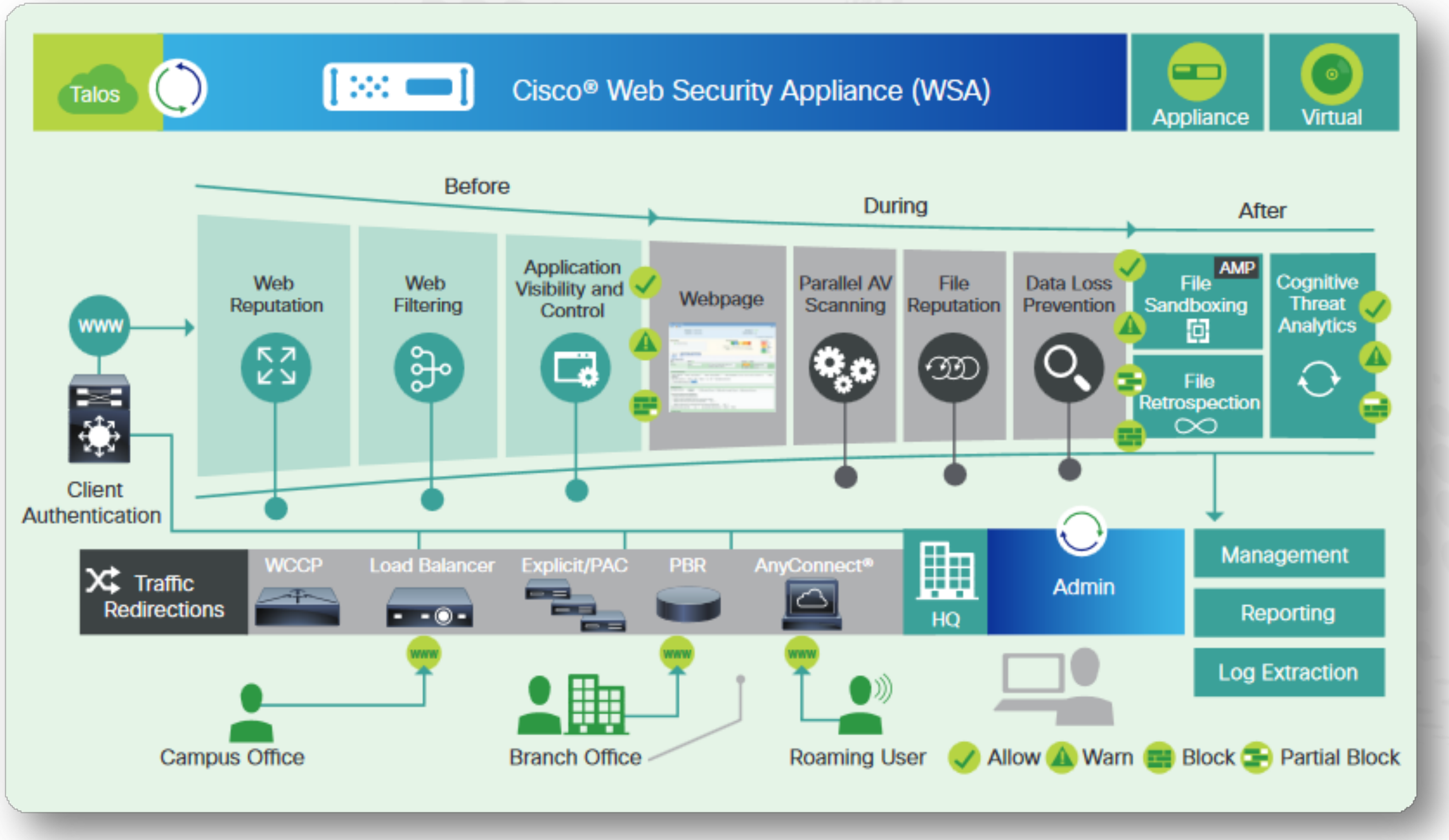


Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Cisco Web Security Appliance

- Physical or Virtual appliance designed for web security
- Analyzes and categorizes known and unknown URLs and blocks those falling below a defined security threshold
- Provides forward proxy services including a TLS proxy
- Contains integrated Malware detection by analyzing HTML, images, Flash files and more

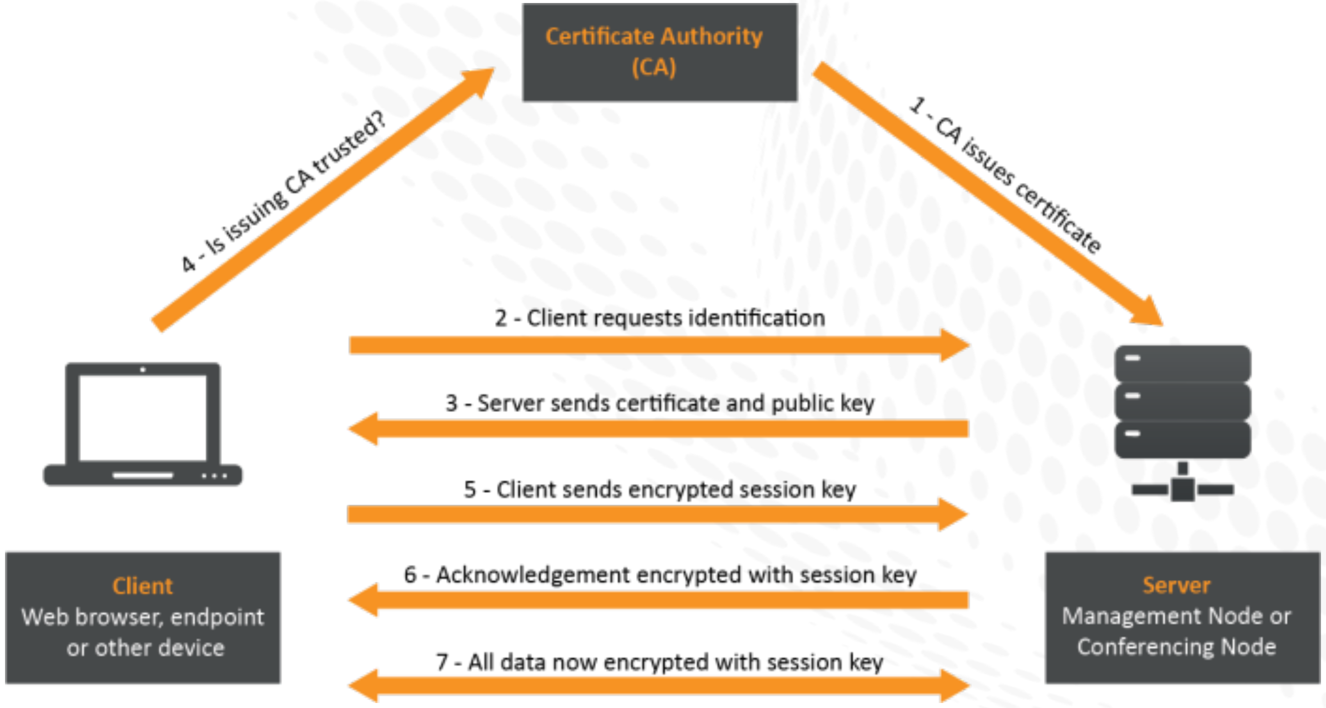


Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Transport Layer Security (TLS)

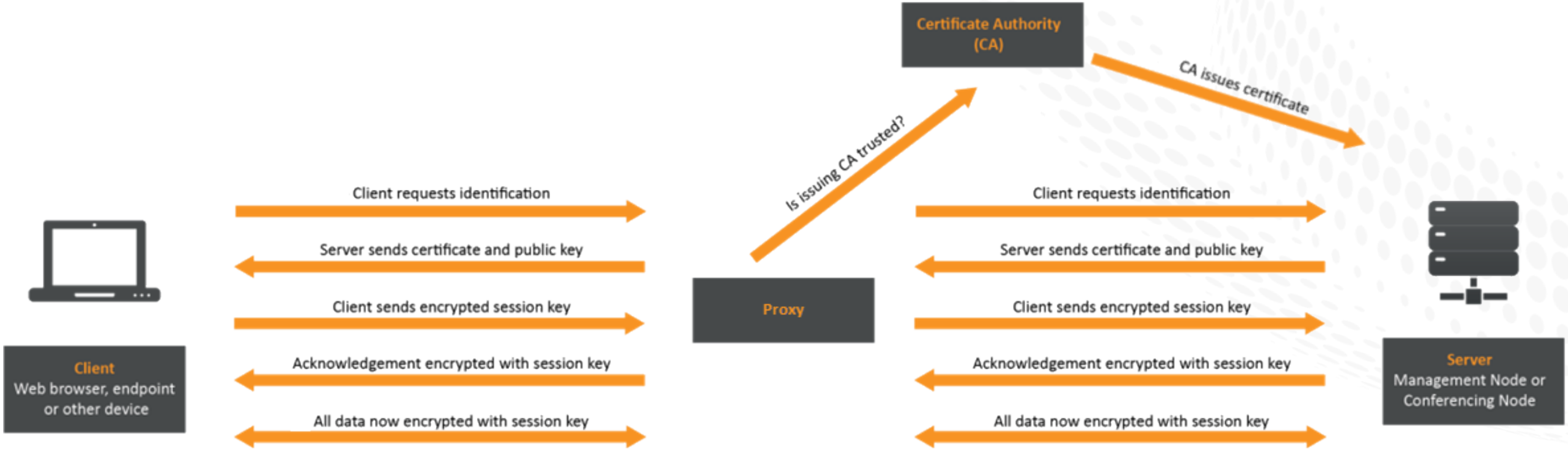
- TLS provides encrypted communications between two participating endpoints
  - In the CPwE Cloud Connectivity the endpoints may be a FactoryTalk application and the cloud hosted destination
- A consideration of the participating endpoints in TLS is ensuring a trust relationship between the devices accomplished using digital certificates.
- TLS traffic presents a challenge to monitor or inspect with traditional tools because the traffic is encrypted
  - TLS proxies can be used to decrypt and inspect traffic


Certificate Authority (CA)
1 - CA issues certificate
4 - Is issuing CA trusted?
2 - Client requests identification
3 - Server sends certificate and public key
5 - Client sends encrypted session key
6 - Acknowledgement encrypted with session key
7 - All data now encrypted with session key
Client
Web browser, endpoint or other device
Server
Management Node or Conferencing Node

Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Transport Layer Security (TLS) - Proxy

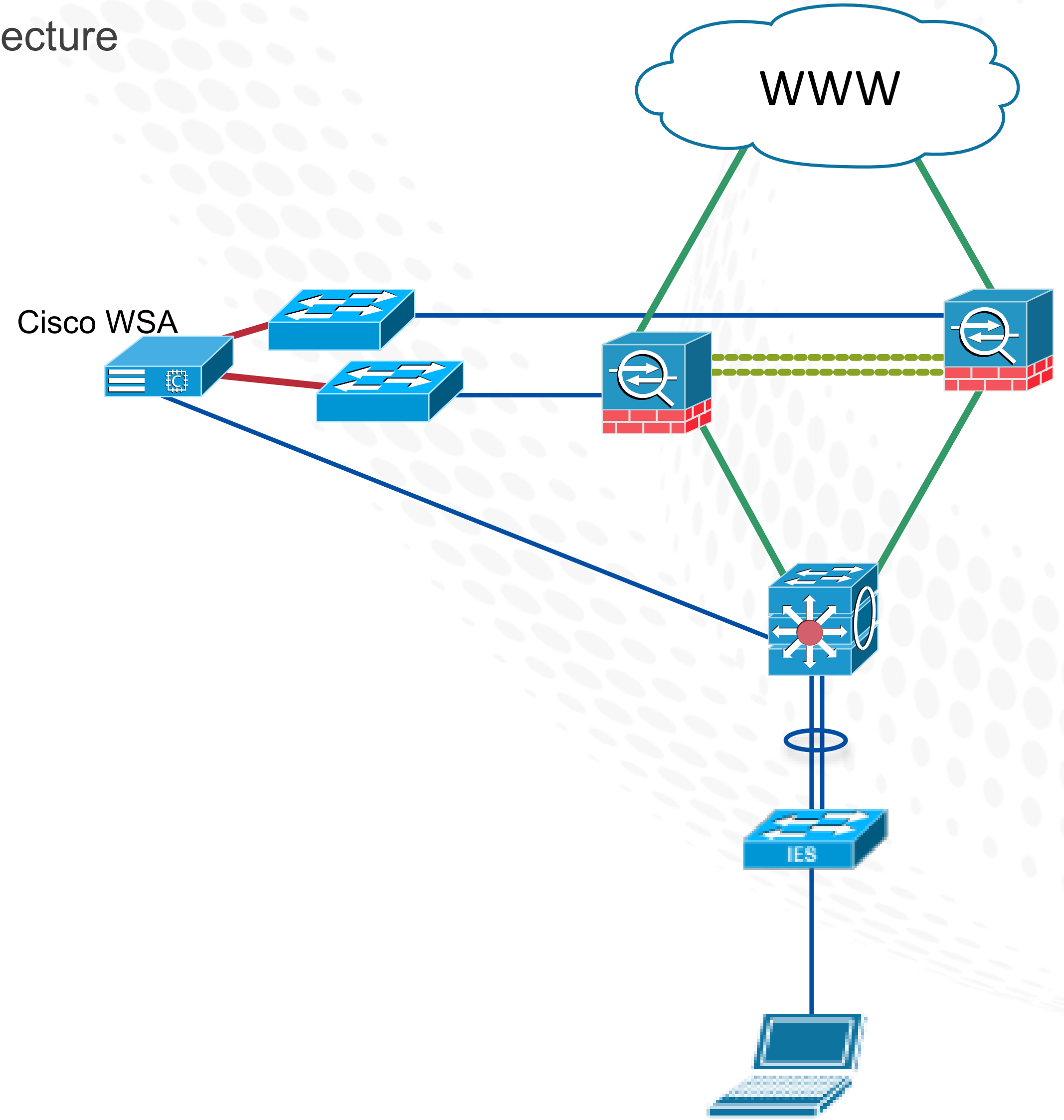

Certificate Authority (CA)
CA issues certificate
Is issuing CA trusted?
Client requests identification
Server sends certificate and public key
Client sends encrypted session key
Acknowledgement encrypted with session key
All data now encrypted with session key
Proxy
Client requests identification
Server sends certificate and public key
Client sends encrypted session key
Acknowledgement encrypted with session key
All data now encrypted with session key
Client
Web browser, endpoint or other device
Server
Management Node or Conferencing Node

Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent vs Explicit

- Proxies require a method to intercept web traffic in order to inspect and take action upon it
- In either mode, the client initiates its HTTP(S)/TLS connection to the WSA then the WSA initiates its HTTP(S)/TLS connection to the web server
- Transparent proxies rely on the infrastructure to intercept and redirect traffic
- Explicit proxies rely on the client to send the traffic directly (Windows Proxy Settings)

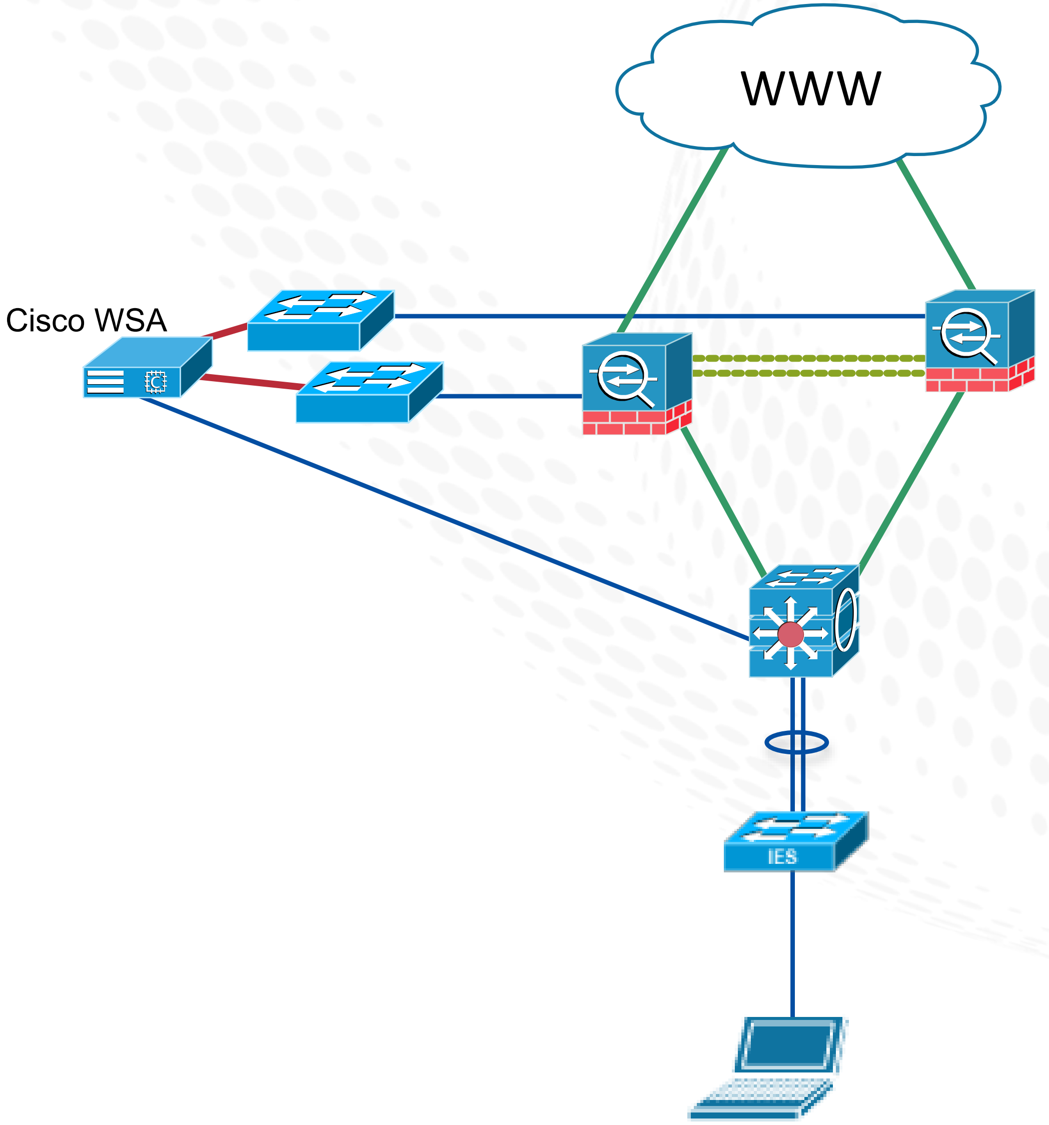


Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent

1. User initiates web connection
2. Cisco ASA forwards select traffic to WSA
3. Cisco WSA forwards allowed traffic to the web
4. Cisco WSA receives response from web
5. Cisco WSA forwards return traffic to application
6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent

1. User initiates web connection

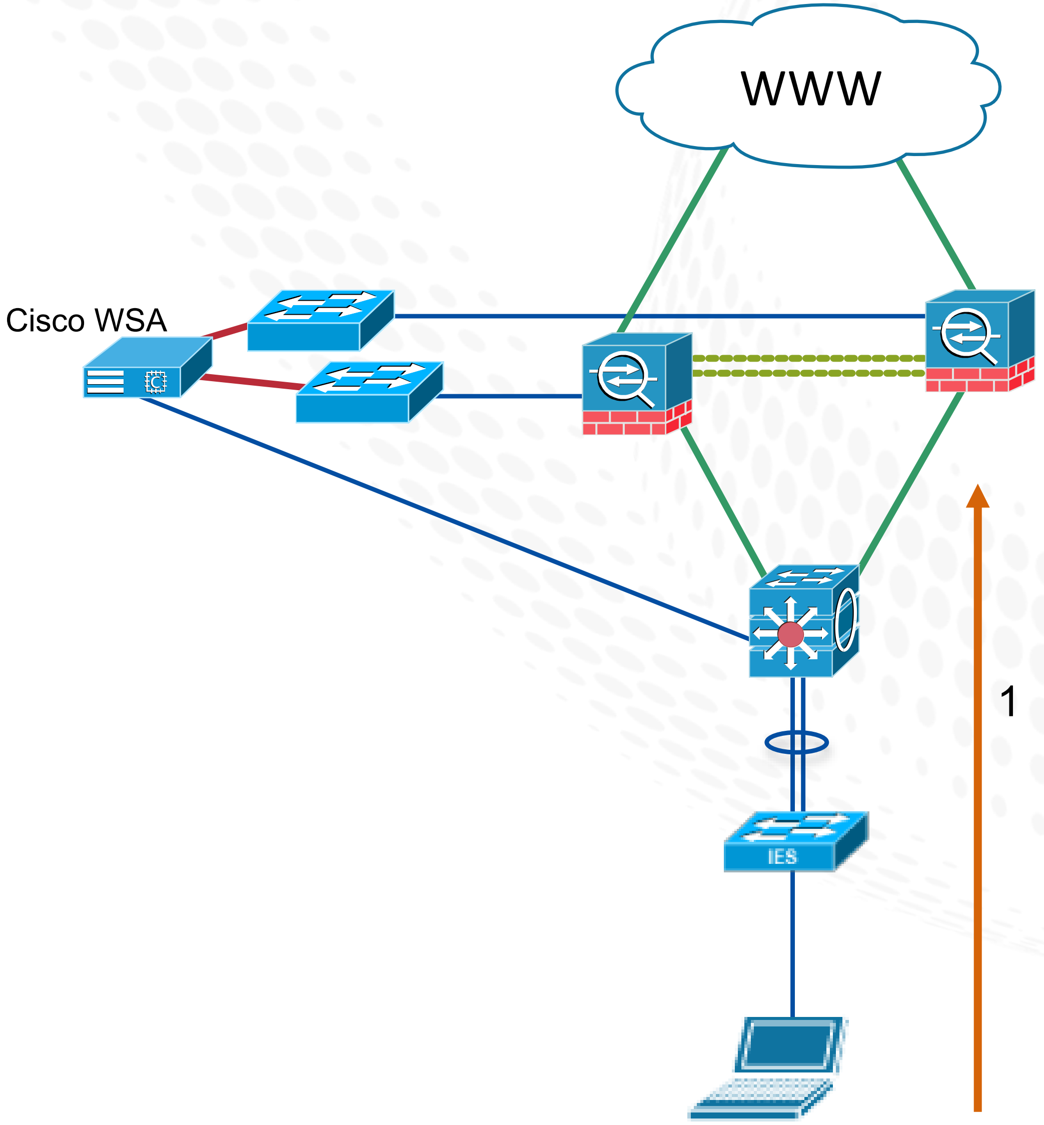
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

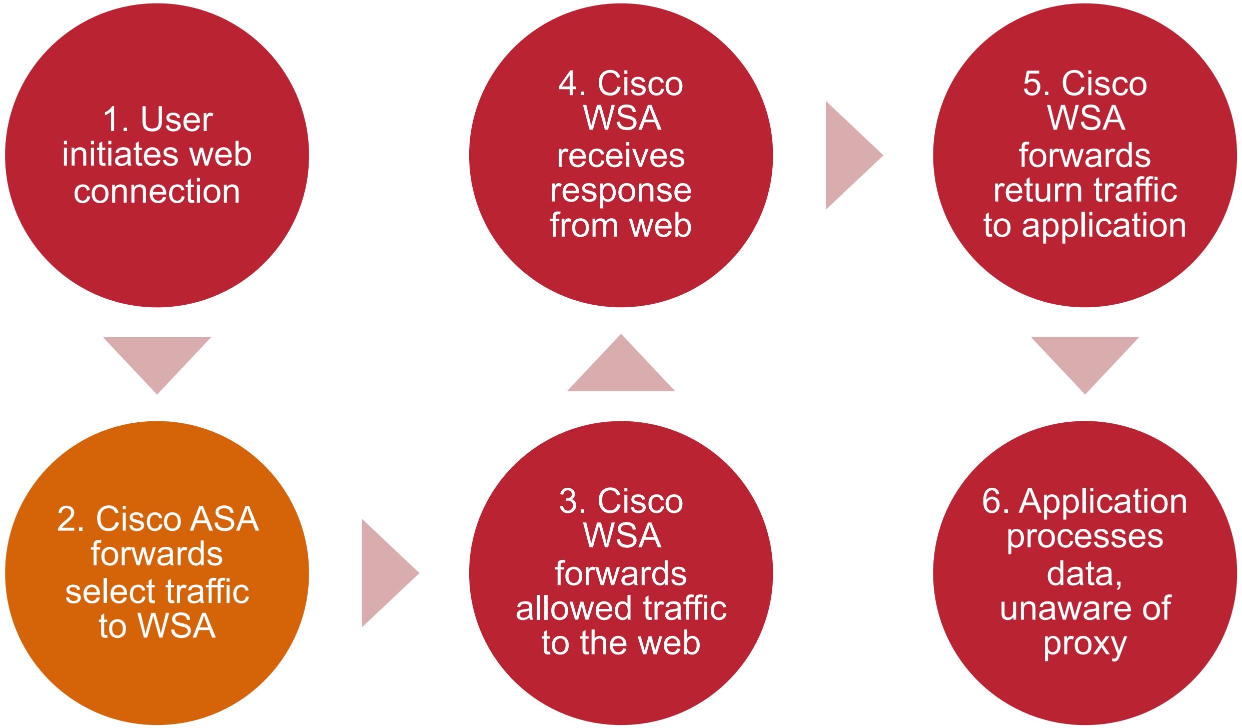
6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent



1. User initiates web connection

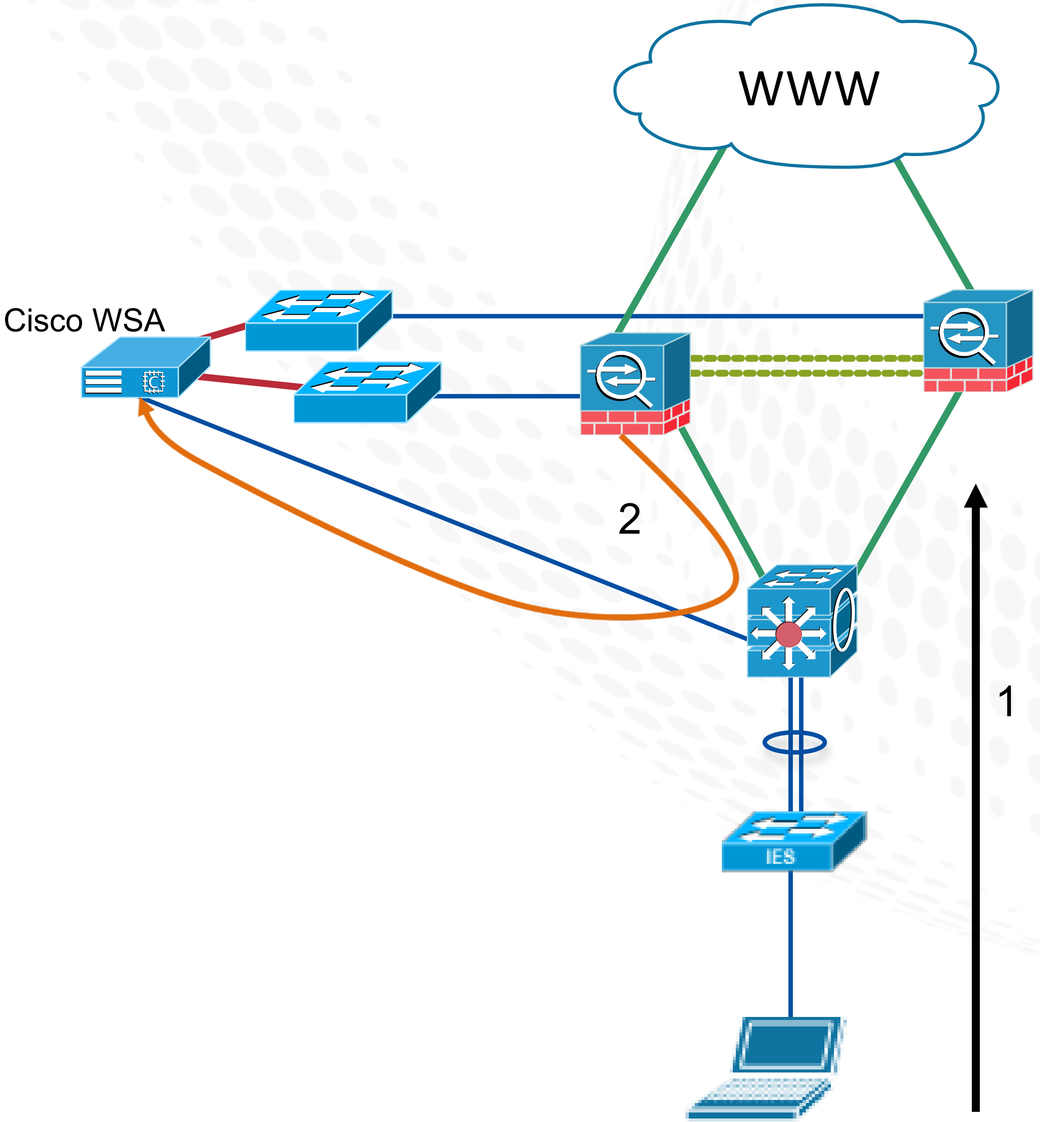
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

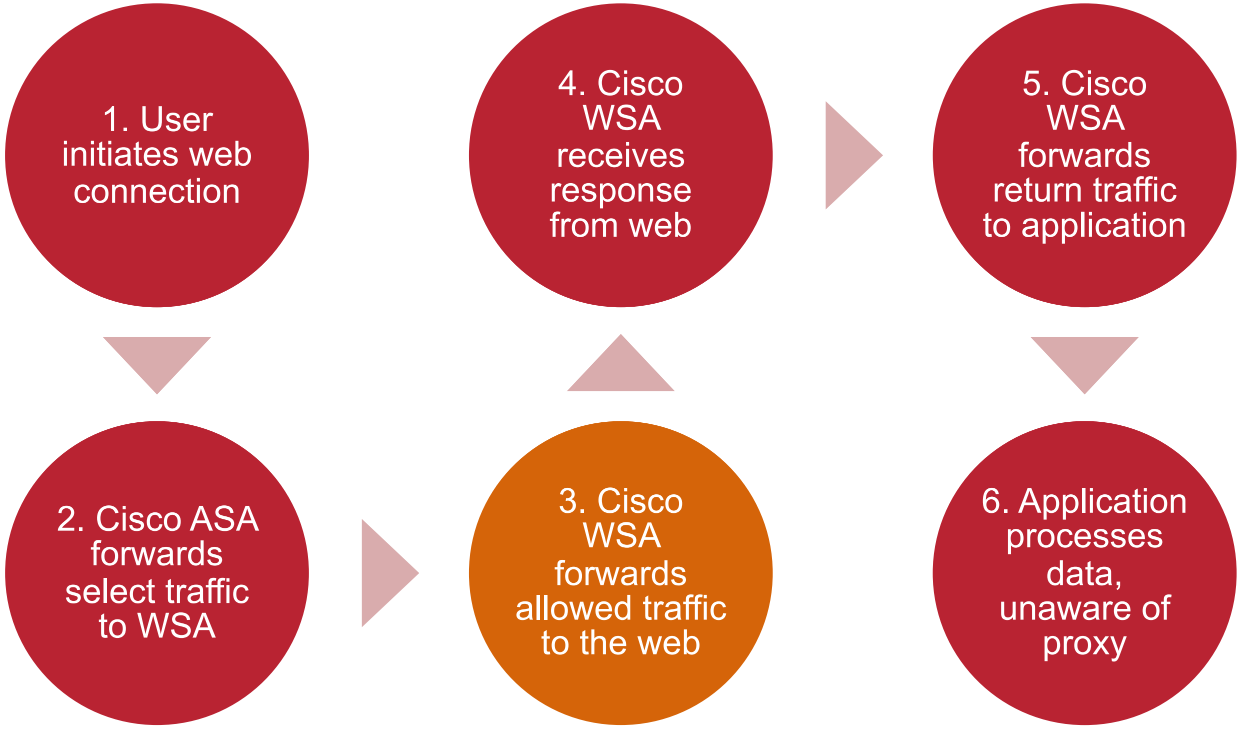
6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent



1. User initiates web connection

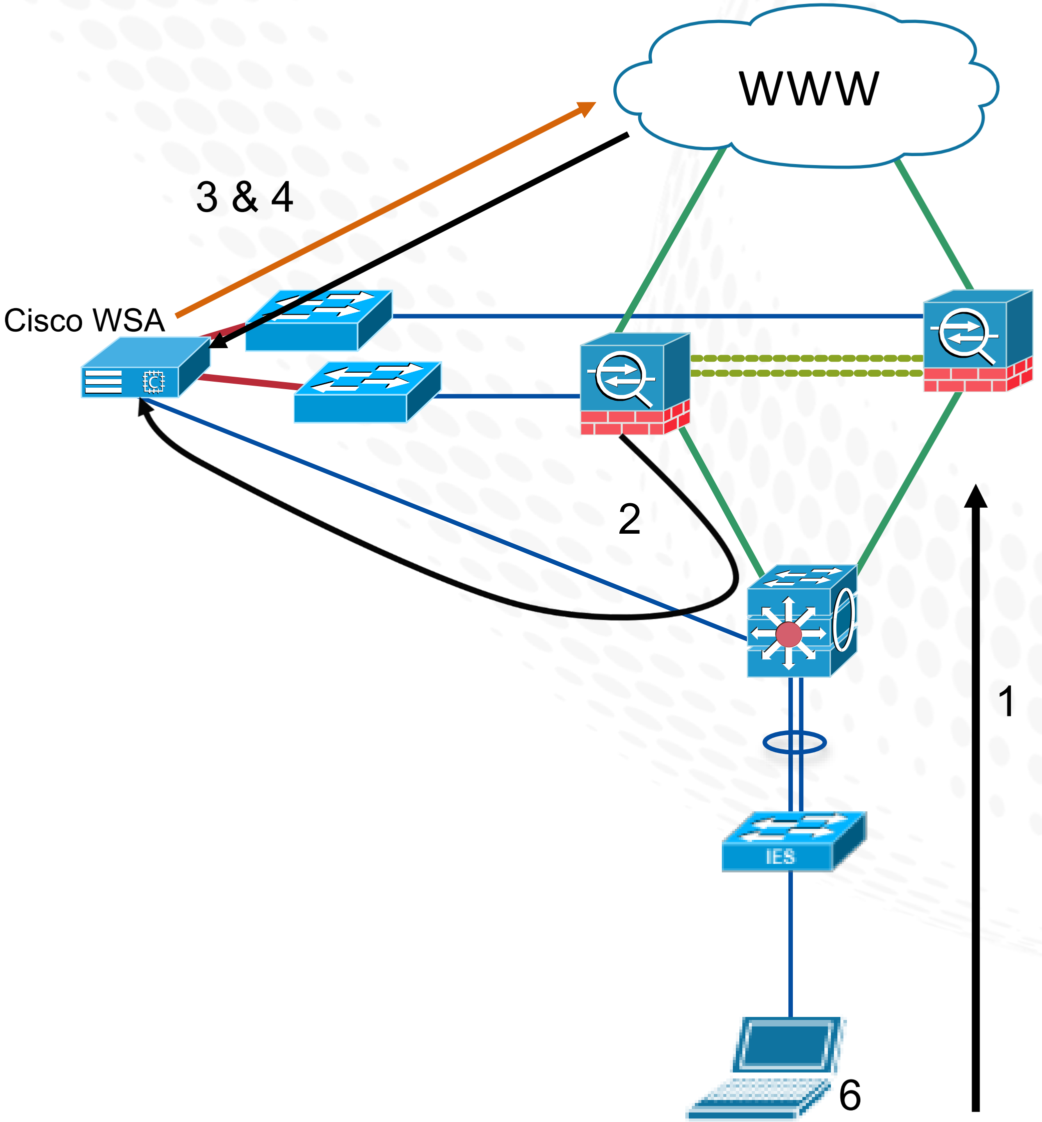
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent

1. User initiates web connection

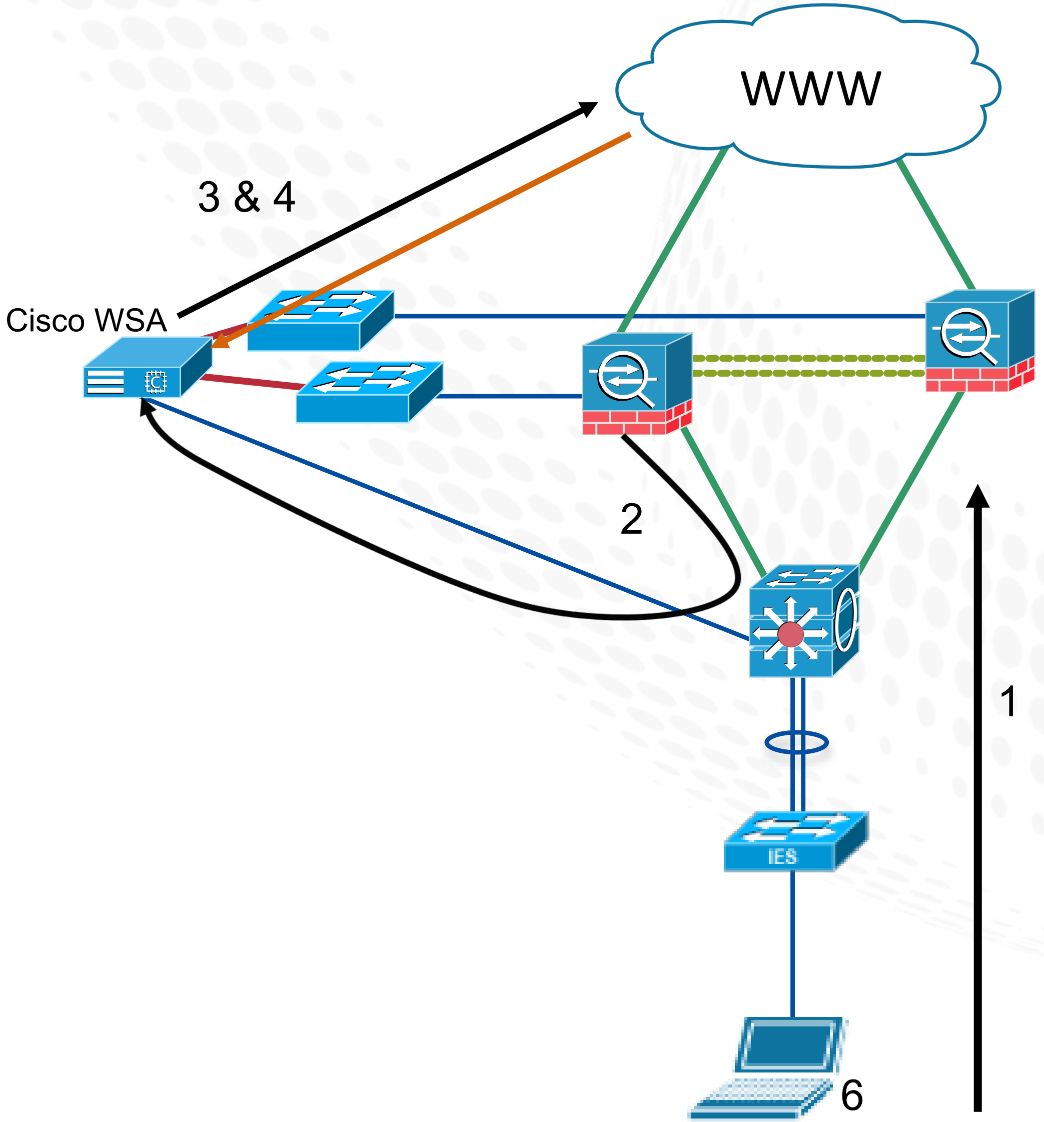
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

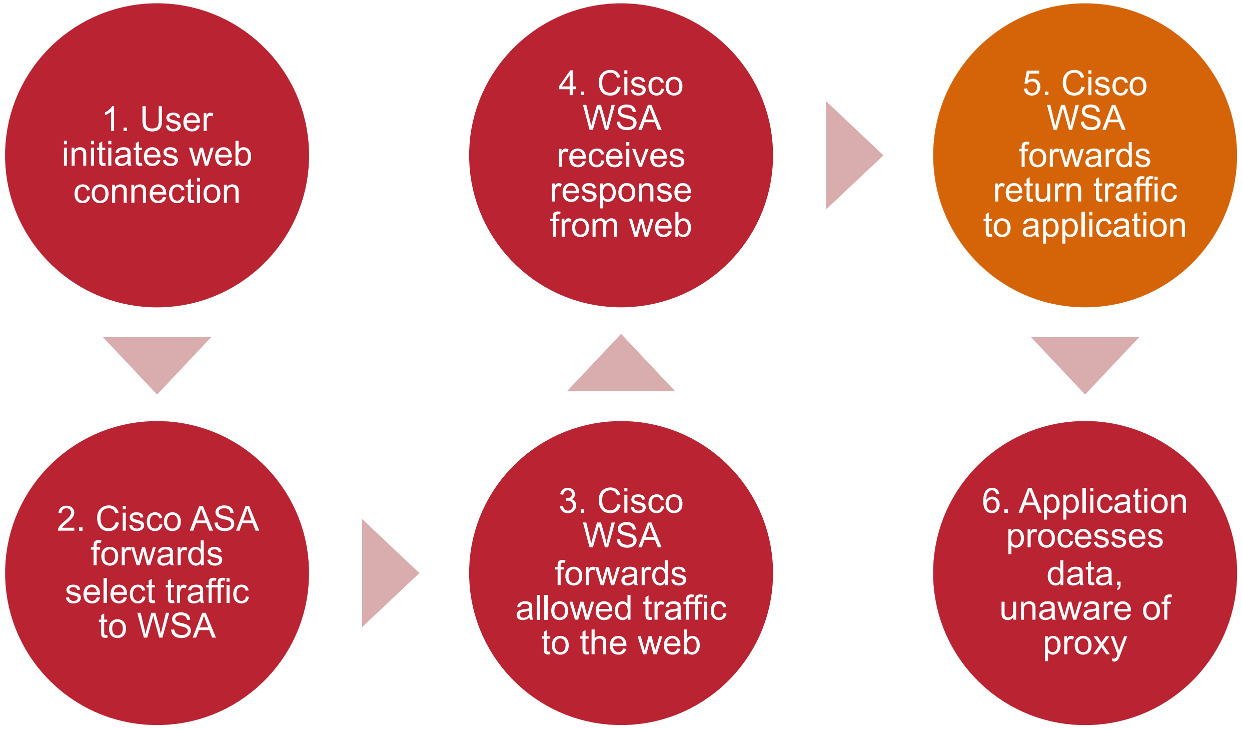
6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent



1. User initiates web connection

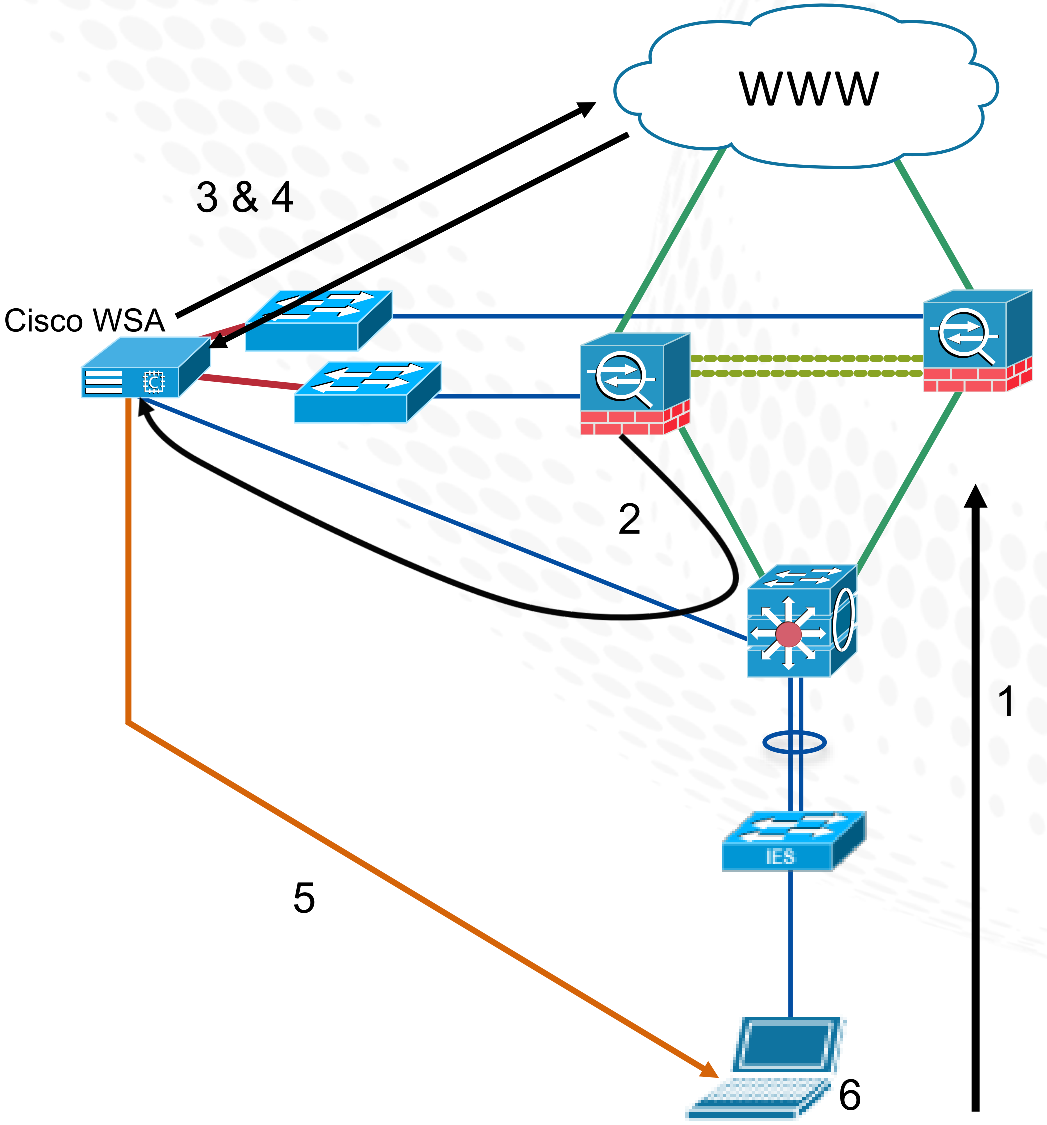
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

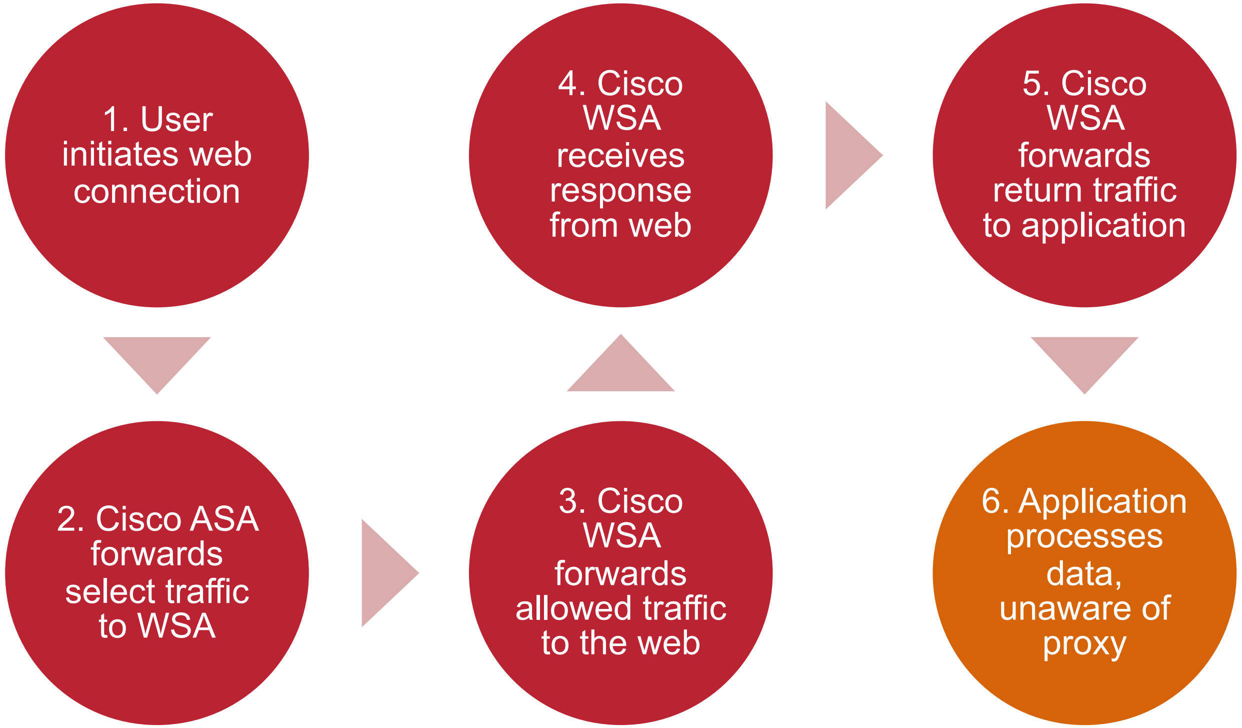
6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Transparent



1. User initiates web connection

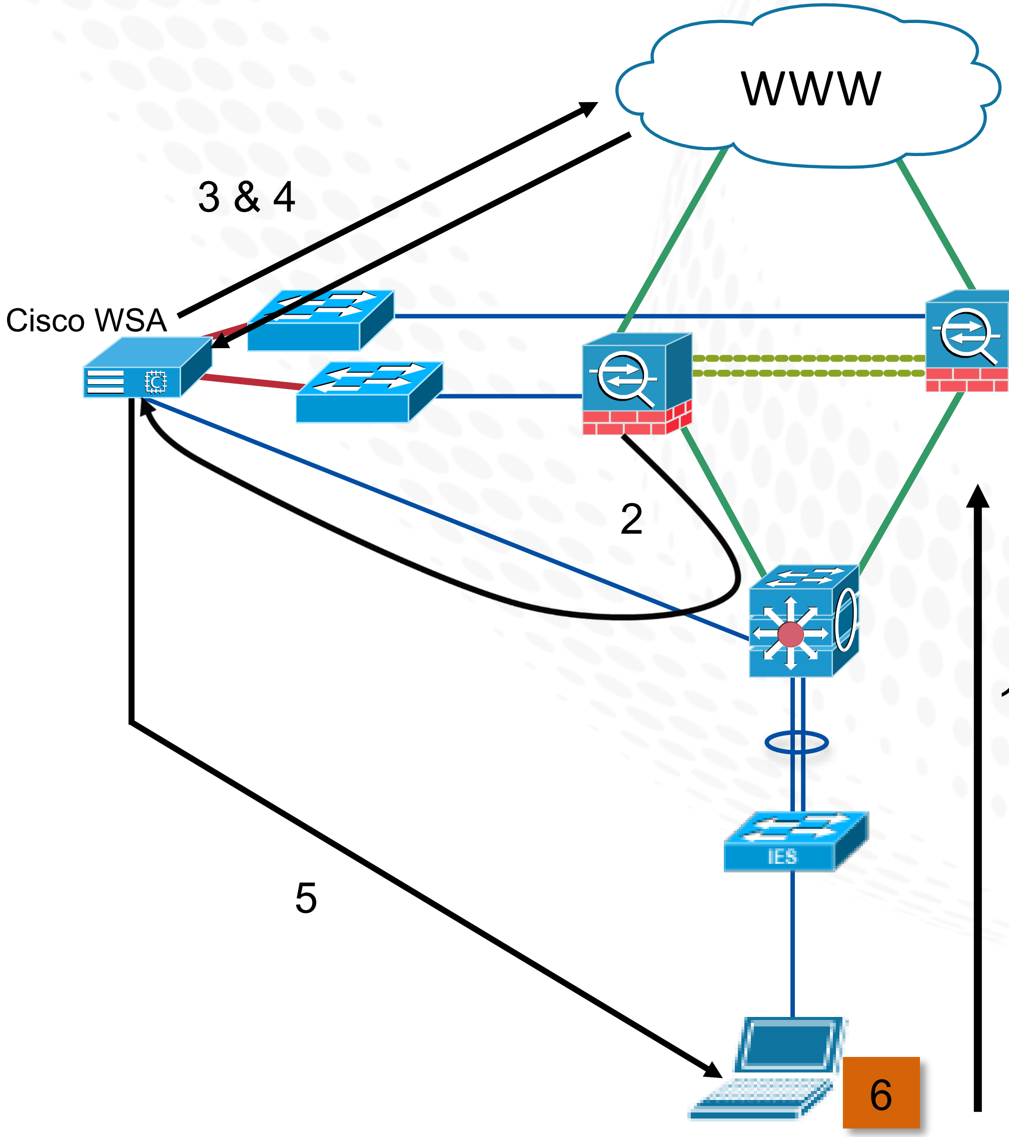
2. Cisco ASA forwards select traffic to WSA

3. Cisco WSA forwards allowed traffic to the web

4. Cisco WSA receives response from web

5. Cisco WSA forwards return traffic to application

6. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit

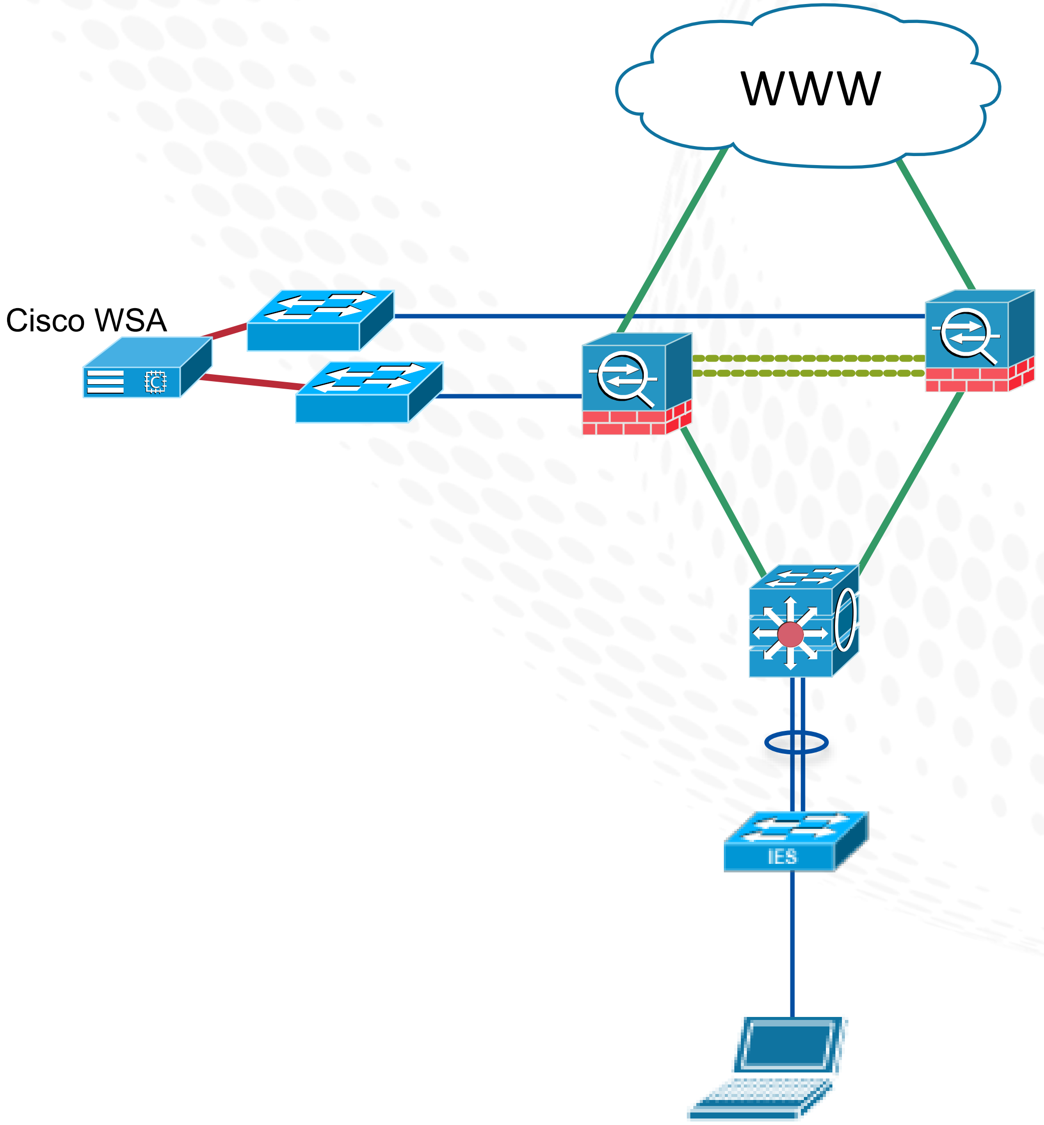
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

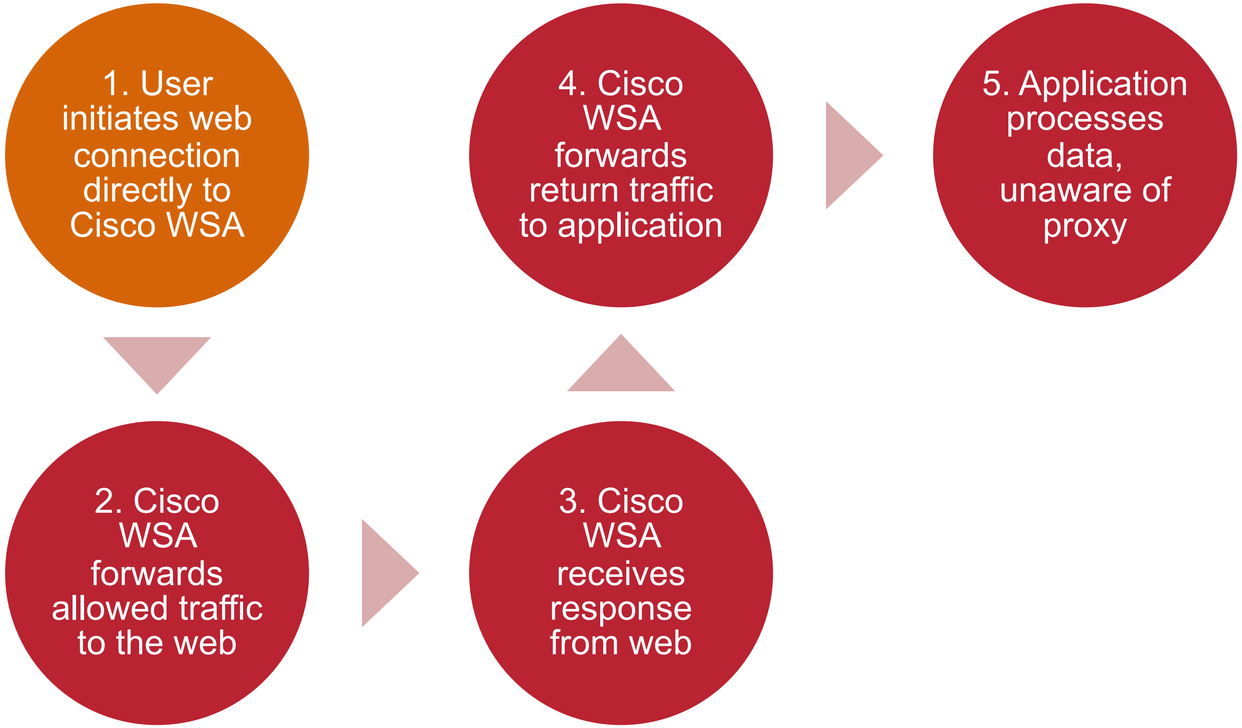
5. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit



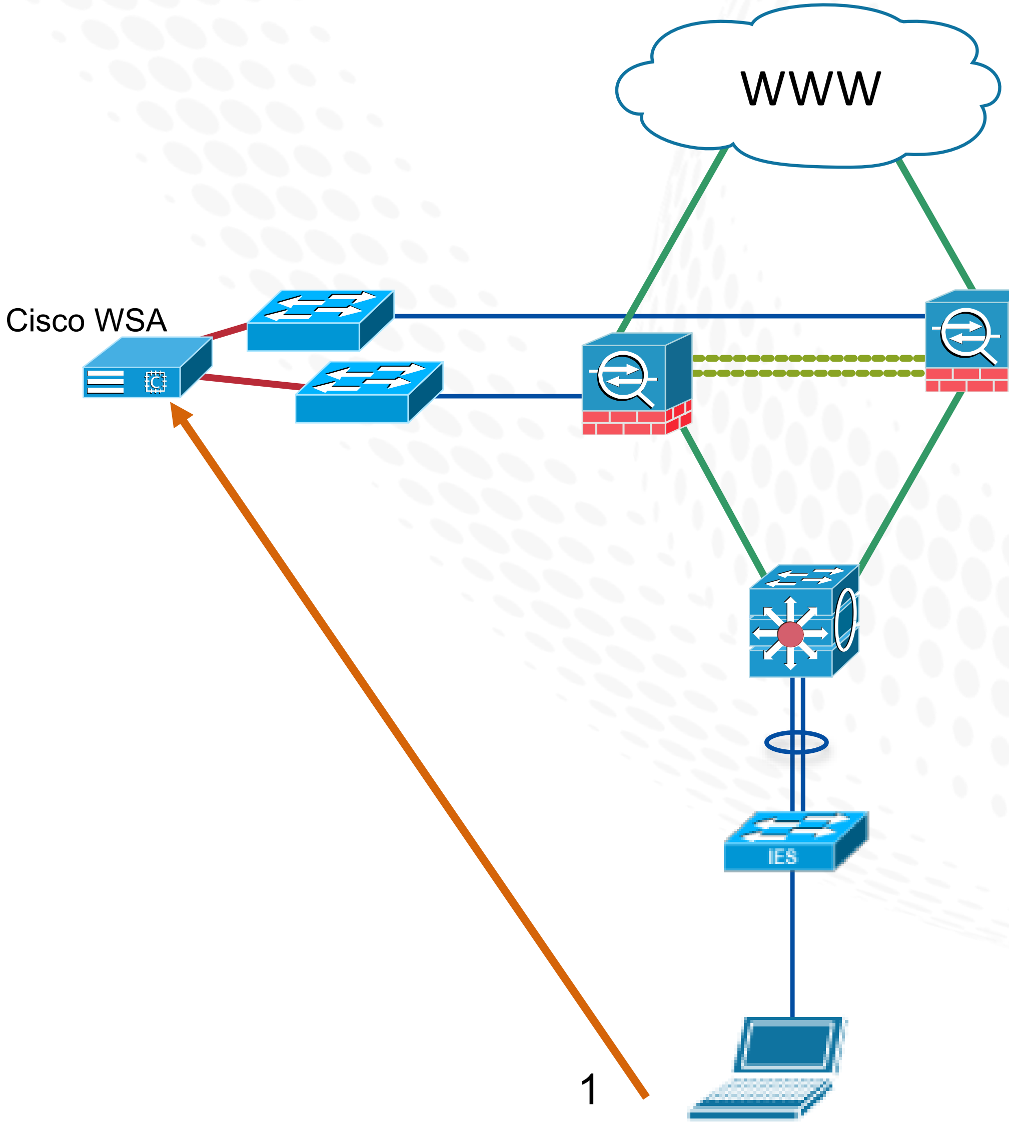
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

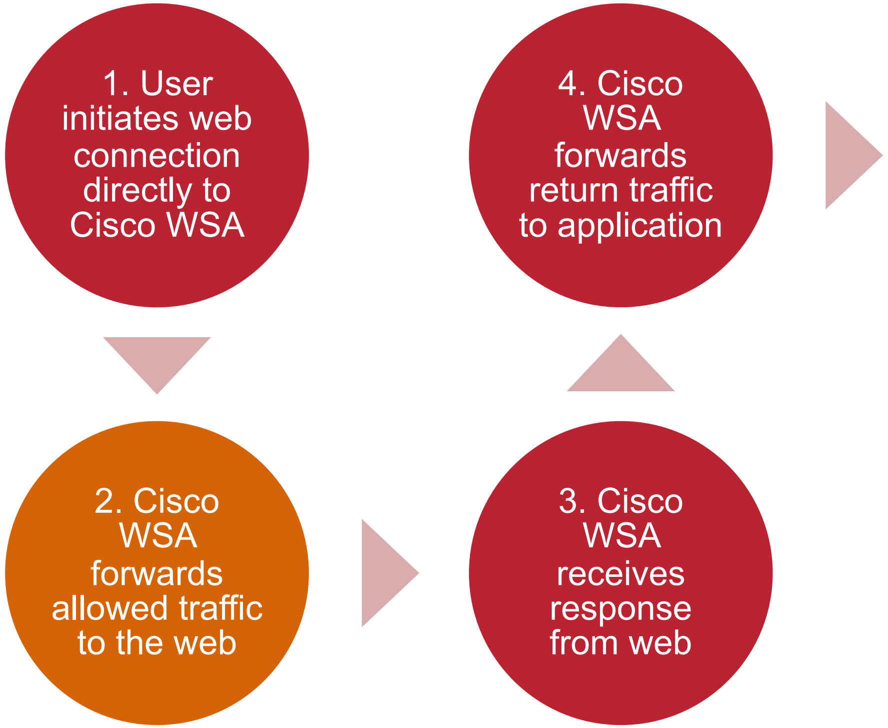
5. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit



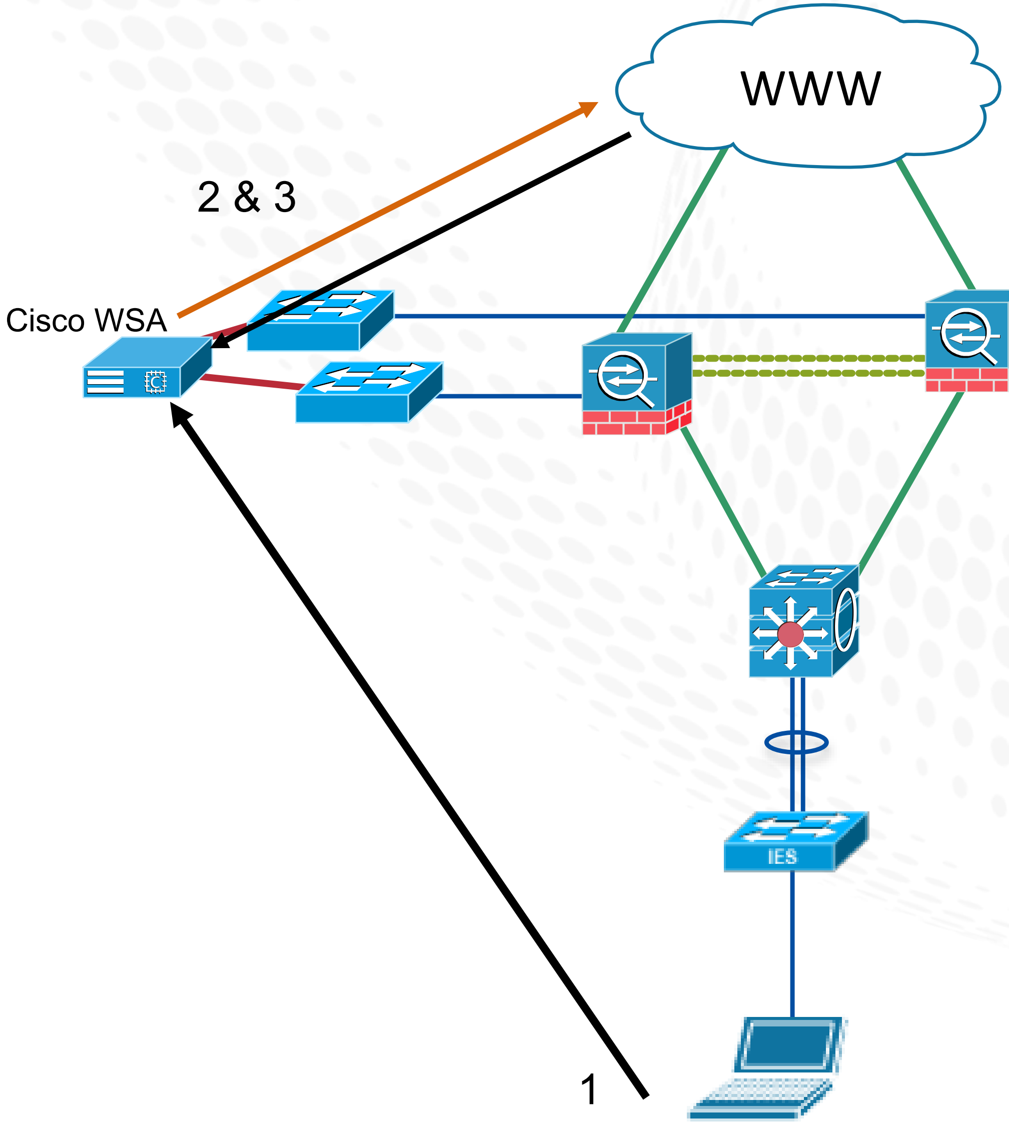
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

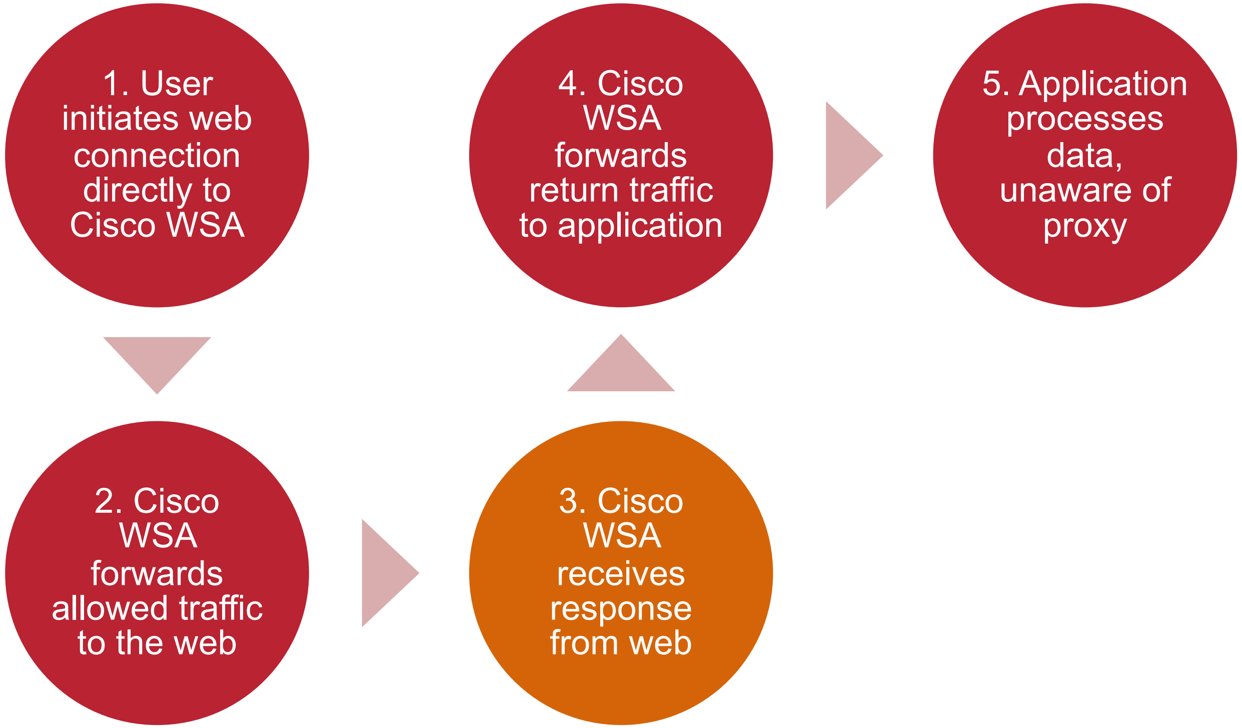
5. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit



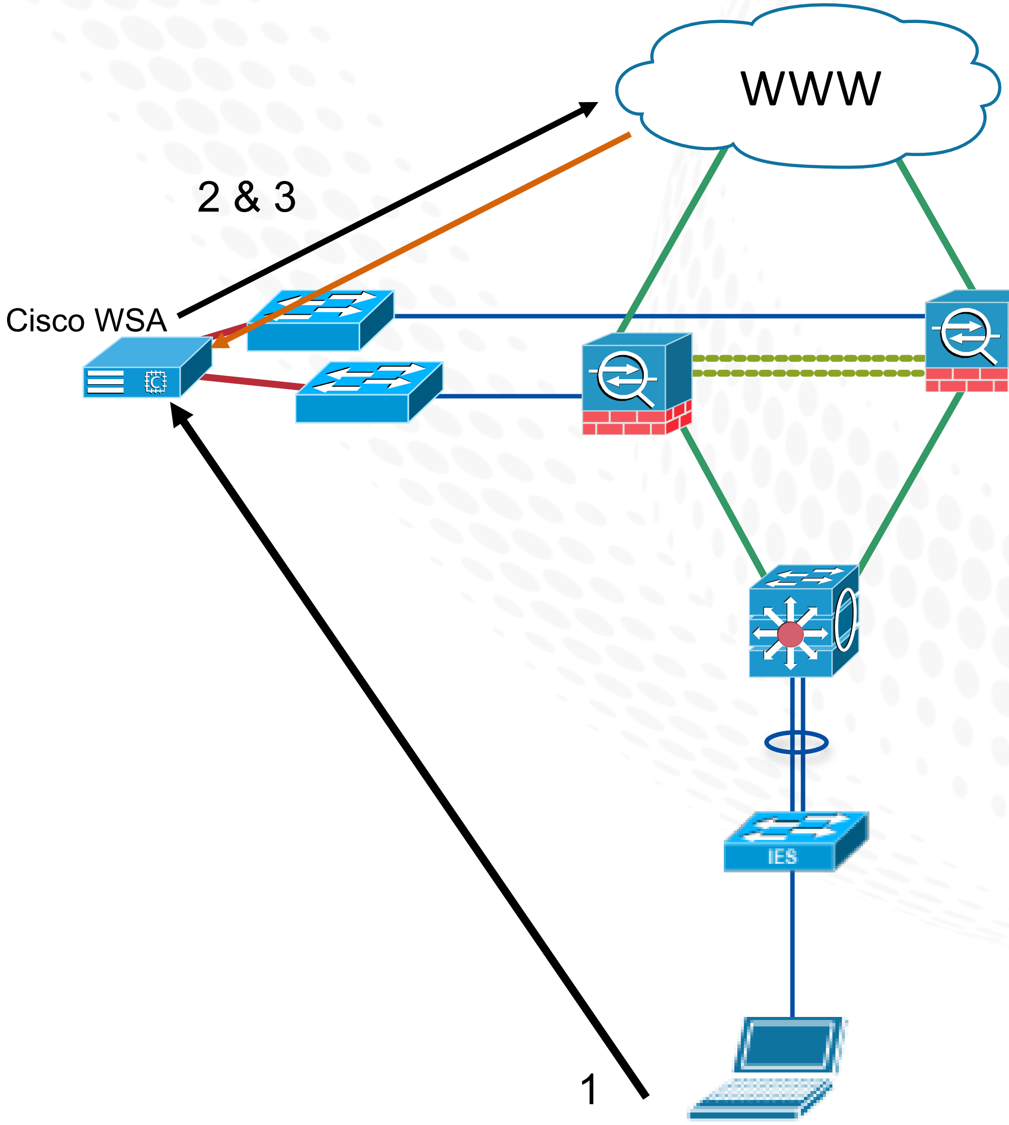
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

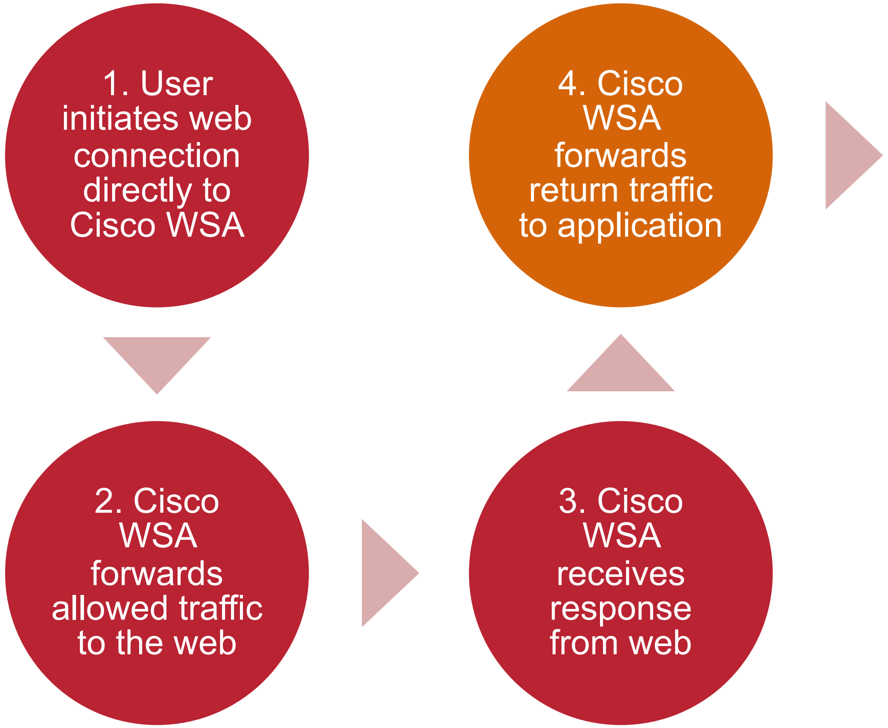
5. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit



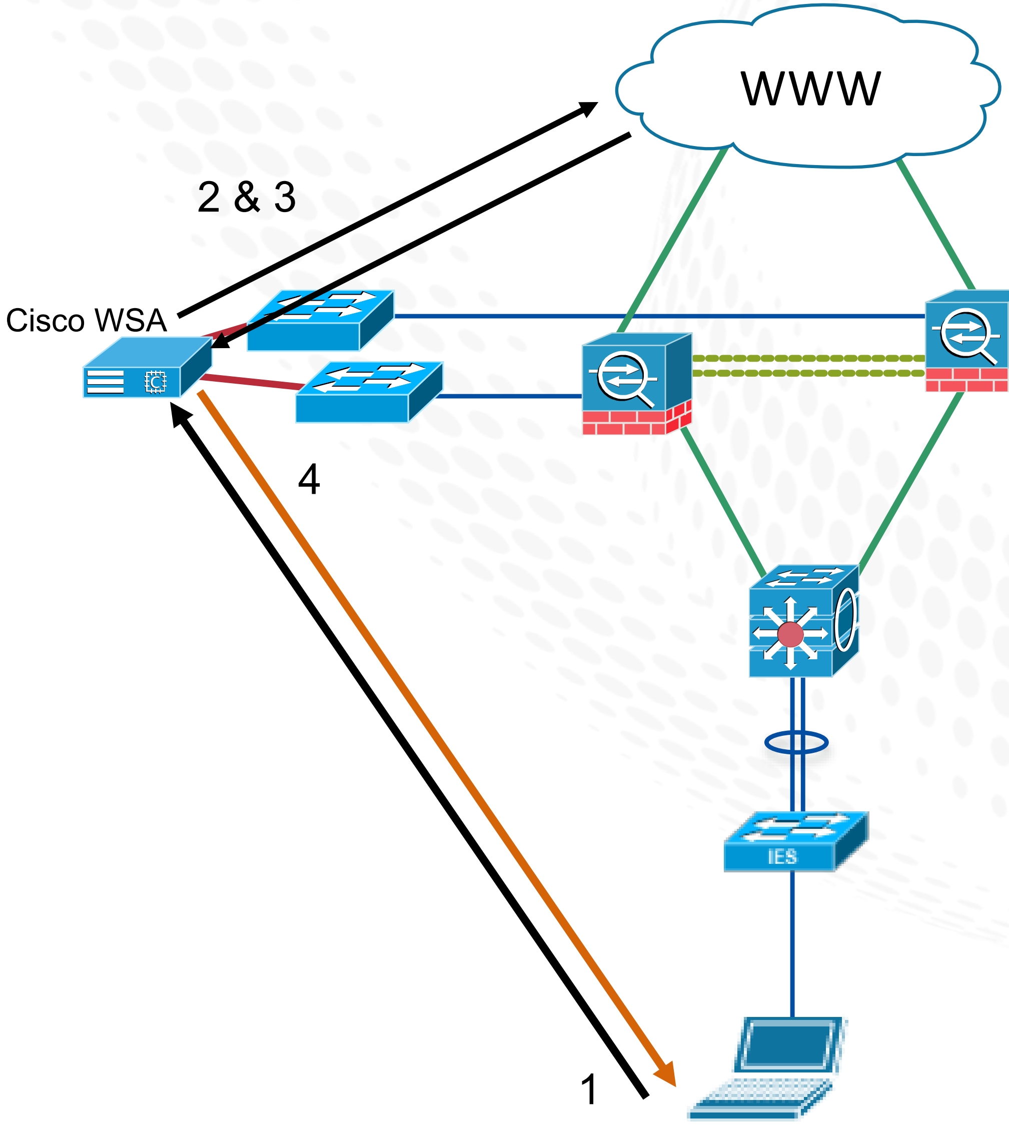
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

5. Application processes data, unaware of proxy



Cloud Connectivity Technologies

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

Proxy Server – Explicit

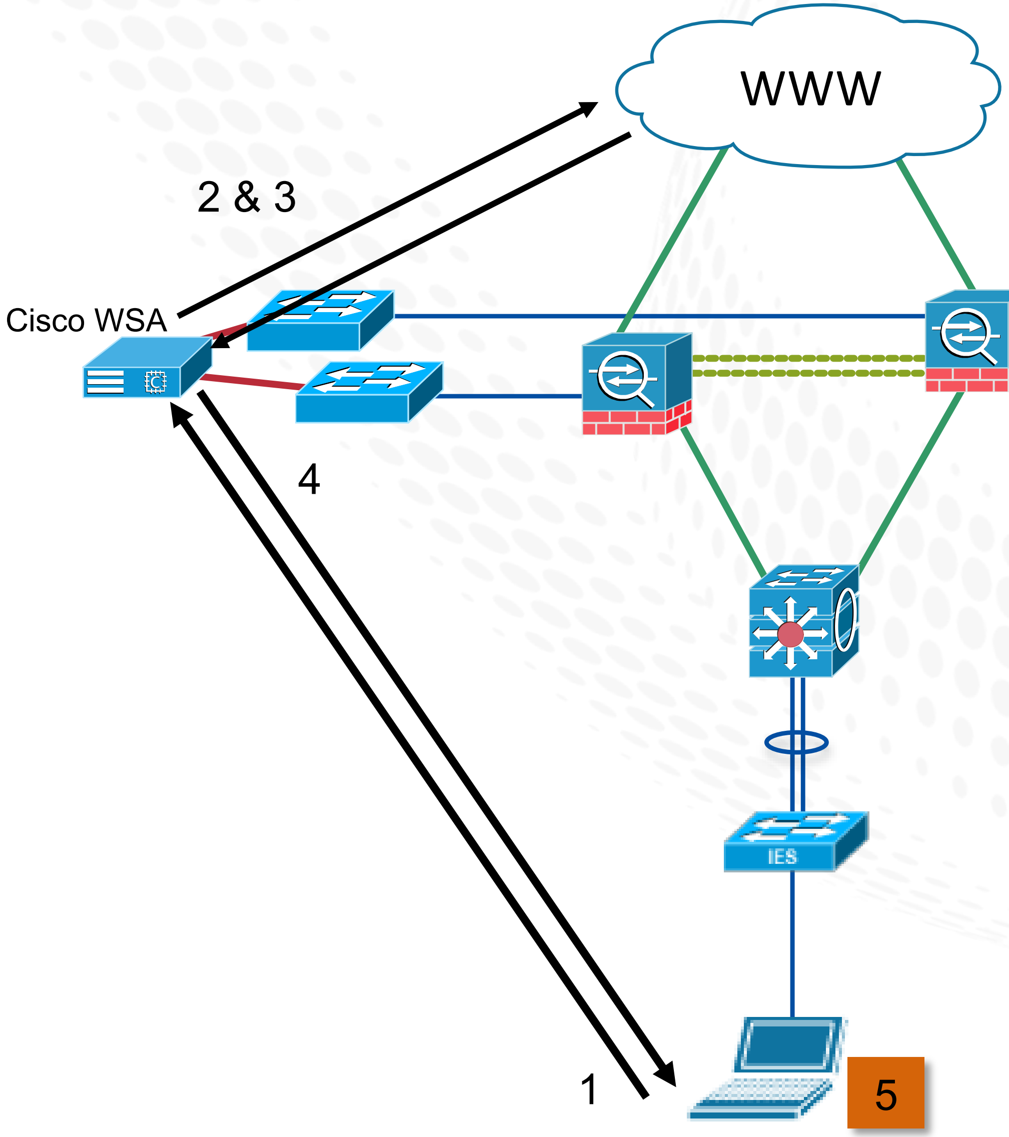
1. User initiates web connection directly to Cisco WSA

2. Cisco WSA forwards allowed traffic to the web

3. Cisco WSA receives response from web

4. Cisco WSA forwards return traffic to application

5. Application processes data, unaware of proxy



THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

Rockwell Automation

Thank you for attending

TRC Tech Talks

Online Seminars