Deploying SD-WAN in Air Gap Networks

Mohamed Bahardeen
IIOT Solution Engineering Manager

Rodney Smith
SDWAN Solutions Engineer

Cisco Webex App

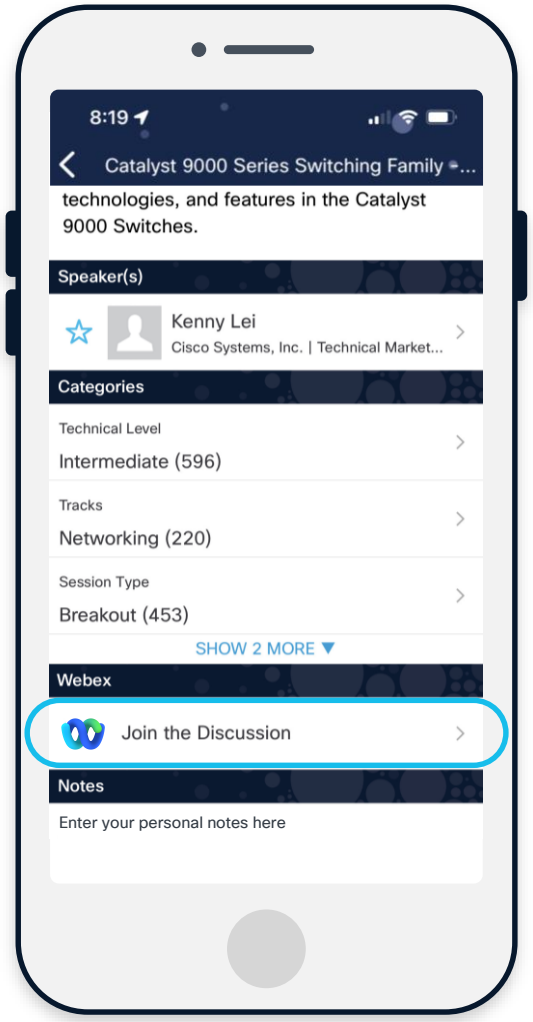
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



Agenda

01 Why Air Gap Networks?

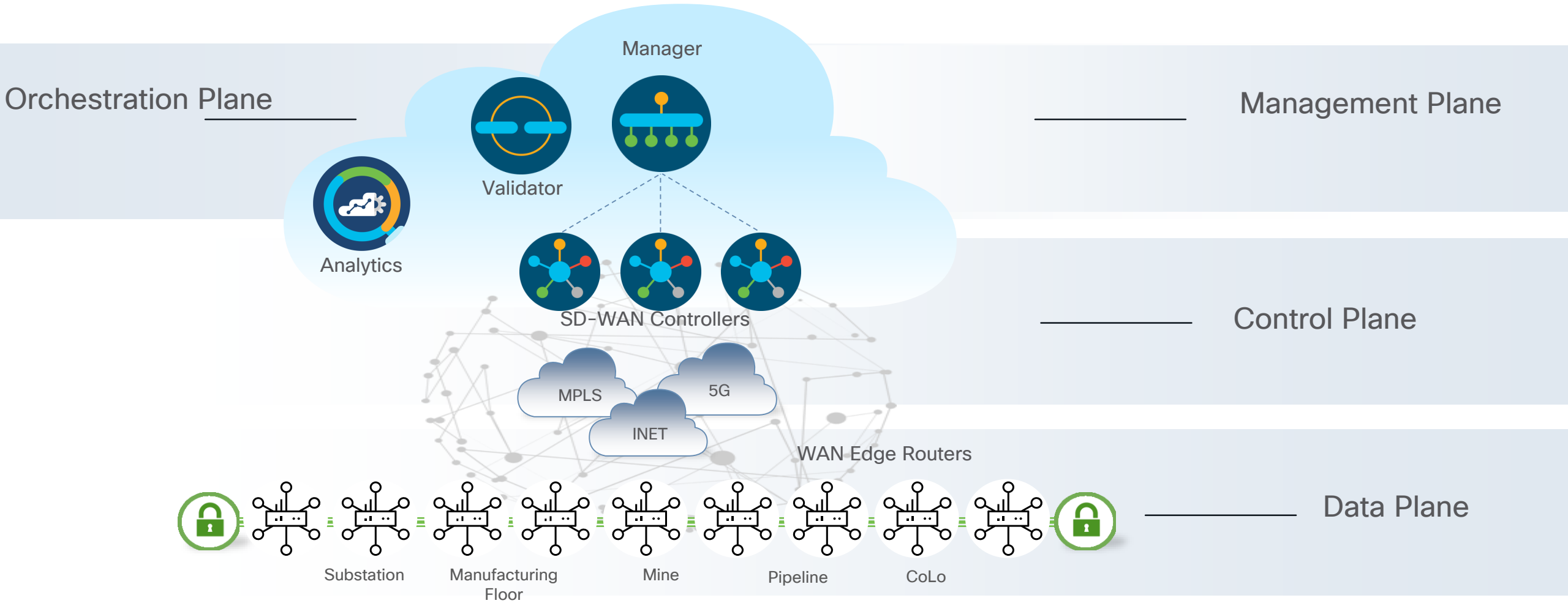
02 Why SD-WAN for Air Gap Networks?

03 Building an Air Gap SD-WAN Fabric

04 Additional Considerations

Session Expectations

Cisco Catalyst SD-WAN Solution Components



Why Air Gap Networks?

Securing What Matters Most

74% of data breaches involved network-based attacks

– 2021 IBM Cost of a Data Breach Report

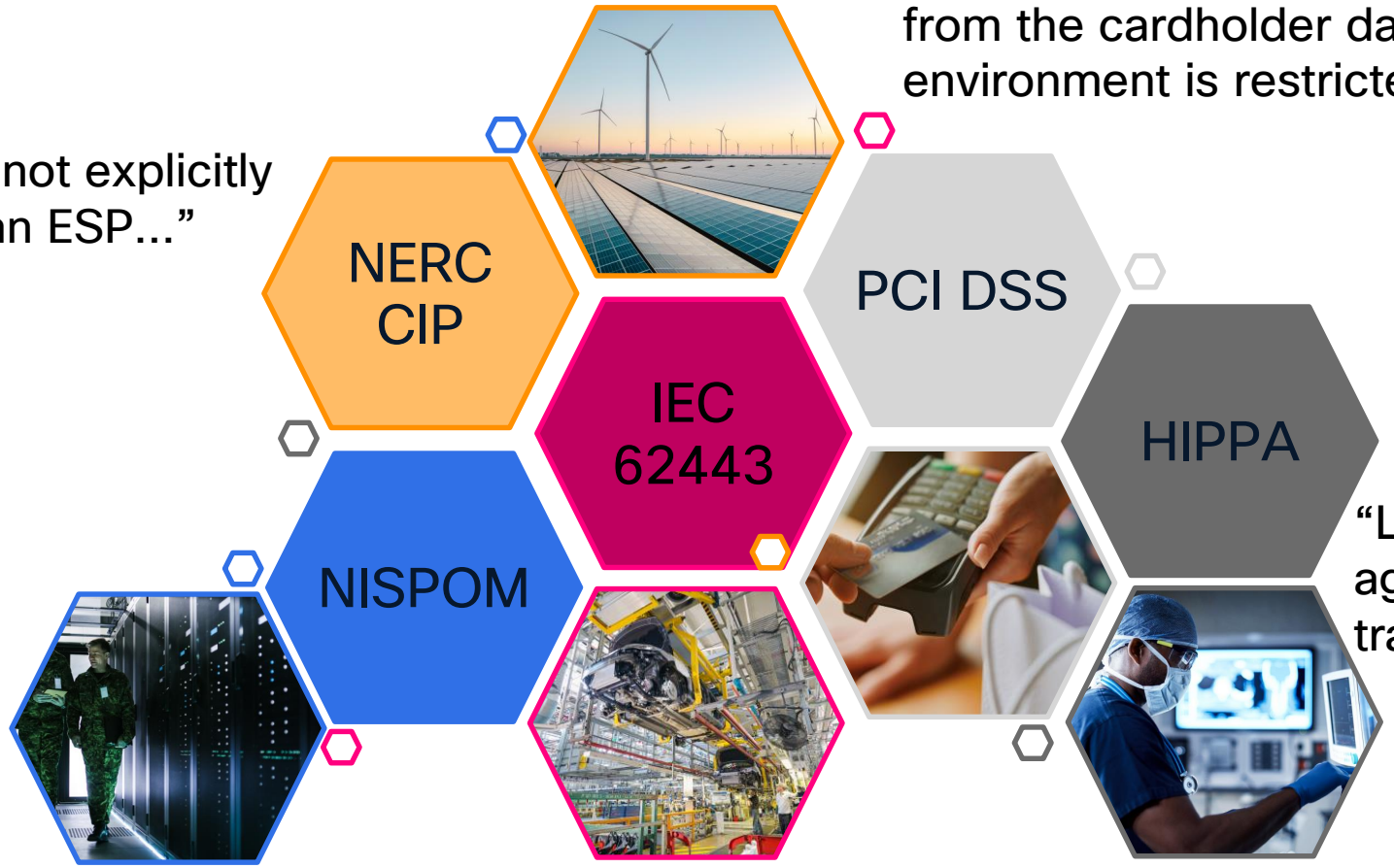
Air-gapping critical systems reduces breach costs by up to **30%** compared to networked system

– 2023 Gartner Cyber Security Trends

Regulations Drive Requirements

“Network access to and from the cardholder data environment is restricted…”

“Deny all traffic not explicitly allowed within an ESP…”



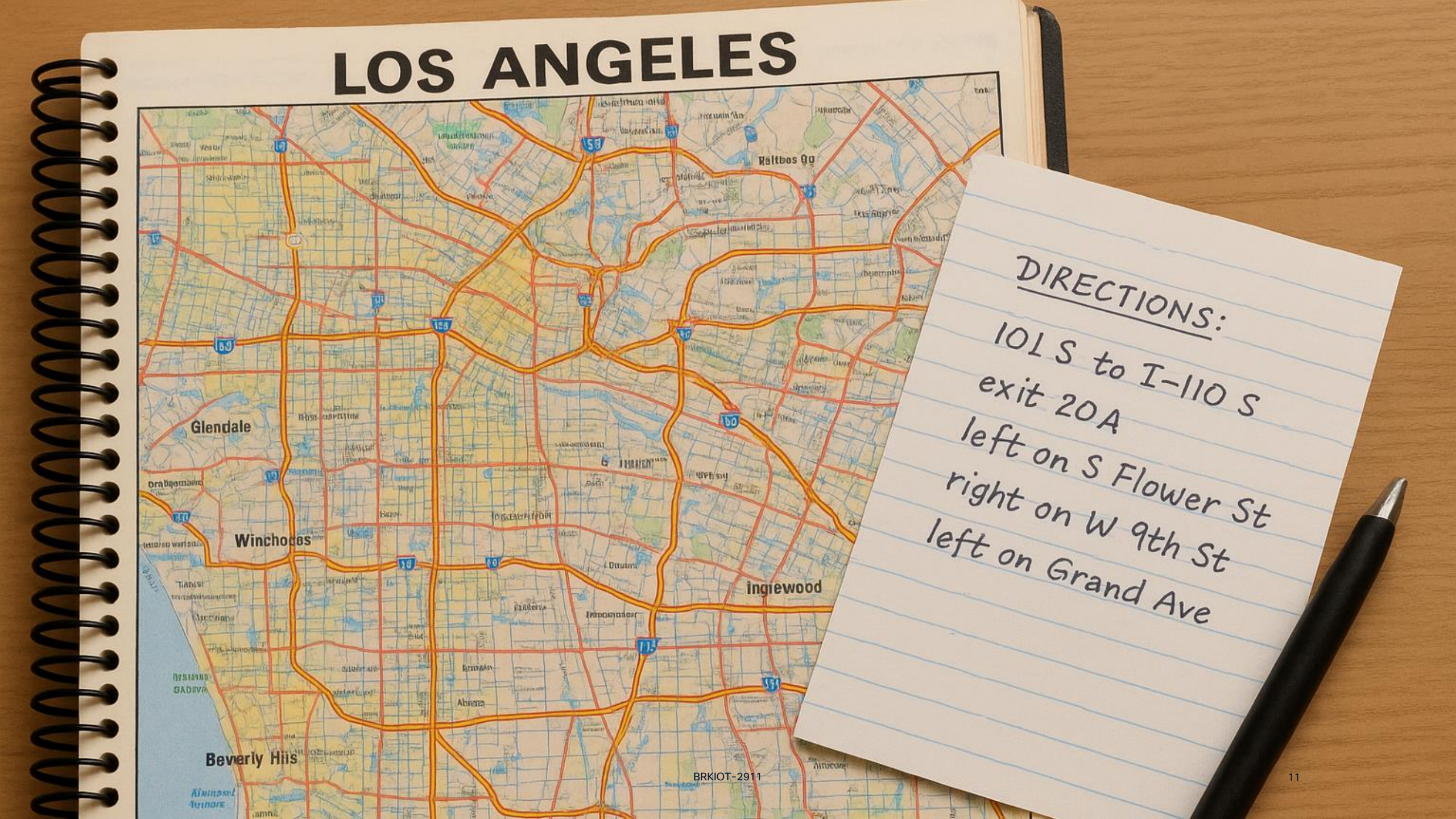
“Limit access, guard against unauthorized transmission…”

“Separation from unclassified networks”

“Segment networks and protect boundaries…”

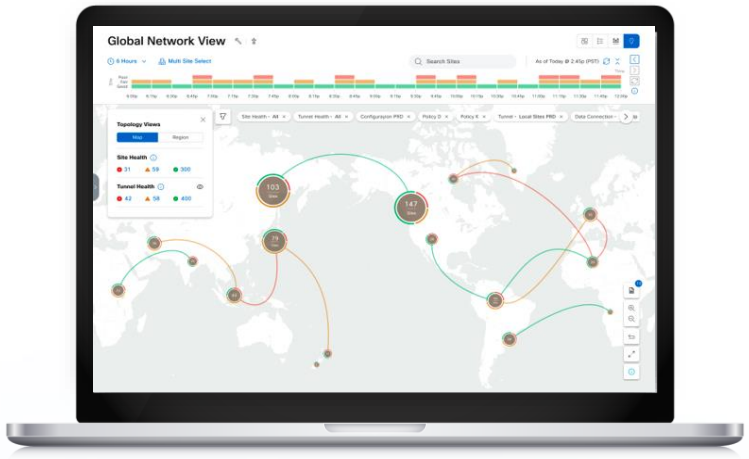
What Industry Do You Represent ?

Why SDWAN for Air Gap Networks?


LOS ANGELES
Glendale
Winchodes
Ingiewood
Beverly Hils
DIRECTIONS:
101 S to I-110 S
exit 20A
left on S Flower St
right on W 9th St
left on Grand Ave


Bobby
9:41
Rerouting
Add a stop
24
1 hr 51m
123 m
1hr 54 min
123 m
Exit in1-94E

SD-WAN for Air Gap Networks Provide



Single Platform

Automation

Zero-Touch, Templates, Guided Workflows

Monitoring

Network health data
Enhanced topology

Advanced Security

Zero Trust, Segmentation

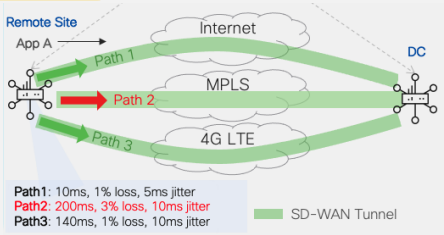
Application Experience

App Routing, QoS

Enhanced Application Experience

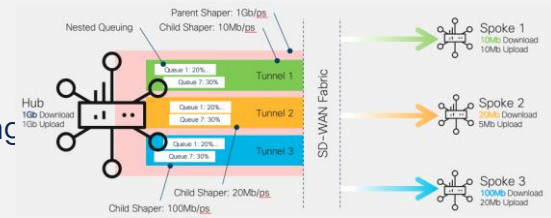
Application Aware routing

- Detects brownout conditions in overlay path.
- SLA based traffic steering
- Automatic failover to secondary path if primary path fails.



Quality of Service (QOS)

- Manage and avoid network congestion
- Guaranteed Bandwidth
- Traffic queueing and shaping
- Prioritize critical application traffic over other traffic.



Forward Error Correction

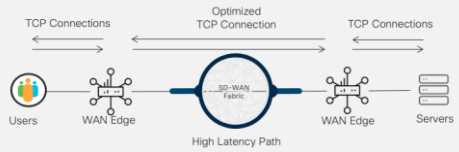
- Protects against packet loss
- Protocol agnostic (TCP/UDP)
- Enhances Application quality of experience

Packet Duplication

- Send duplicate packets over alternate path
- Mitigate packet loss for critical voice or video traffic
- Enhances Application quality of experience

TCP optimization

- BBR2 Congestion control algorithm
- Window scaling
- Large Initial windows
- Selective acknowledgement
- Helps in reducing latency and increase throughput



DRE, LZW

- Traffic optimization techniques
- Byte level caching & Data compression
- Protocol agnostic

Advanced Security Capabilities

Fabric Security

- Encrypted Control Plane
- Encrypted Data Plane
- Enhanced Security – Pairwise keys
- HW Based Device Authentication (SUDI)

Sec-Ops Monitoring & Visibility

- Manager SecOps Dashboard
- End-to-End Monitoring & Visibility

Embedded Security

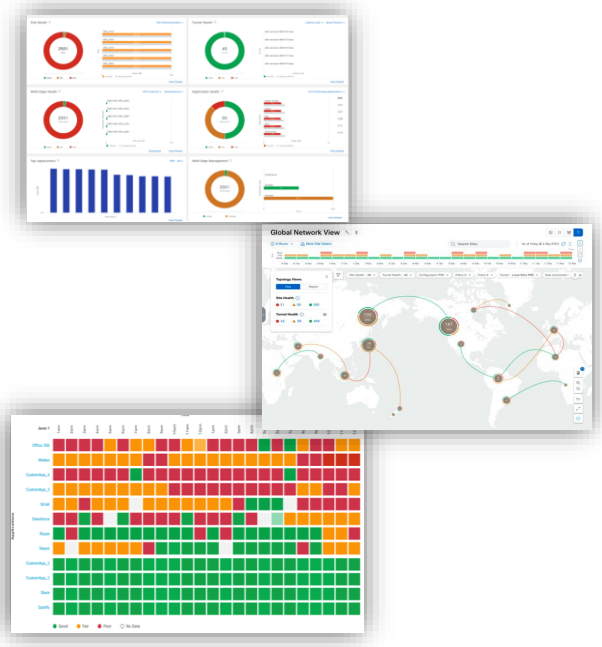
- Firewall Stateful ZBFW
- Segmentation With Multi-Topology
- TrustSec
- IPS Protection
- Zero Trust
- Unified Policy & Logging

L4-7 Security

- DNS security
- Simplified Configuration
- Traffic Steering Policies
- Layer-7 Health Check
- IPsec Tunnel Connection
- Traffic Load Balancing (ECMP)
- Cyber Vision
- Secure Equipment Access

Troubleshooting & Monitoring

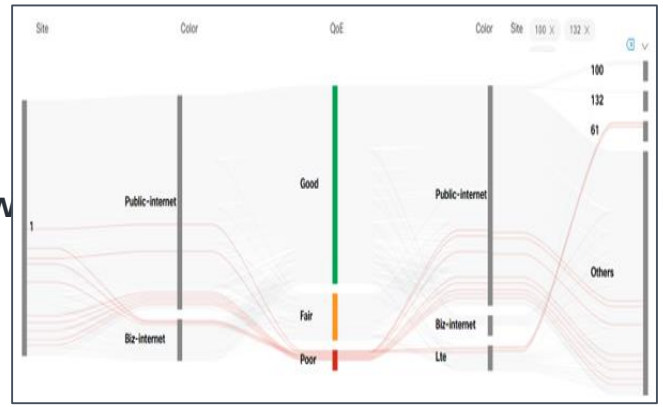
Visibility into Network & Applications



Historical Trends & Daily/Weekly/Monthly Aggregates

Troubleshooting w/ Extensive Traffic Analysis

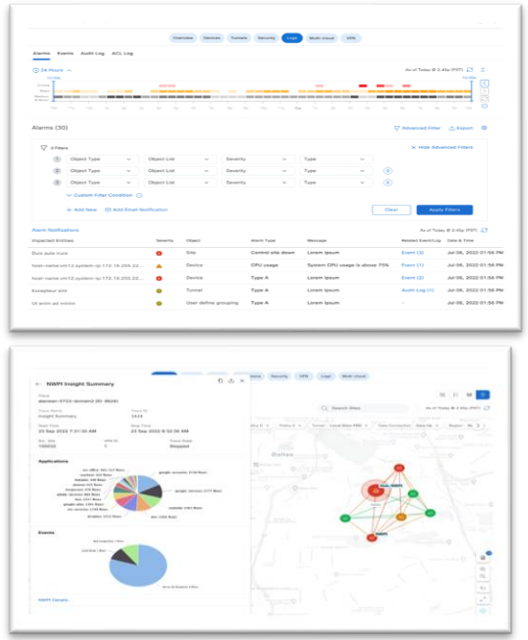
Traffic flow patterns



Underlay path tracing

App distribution across circuits

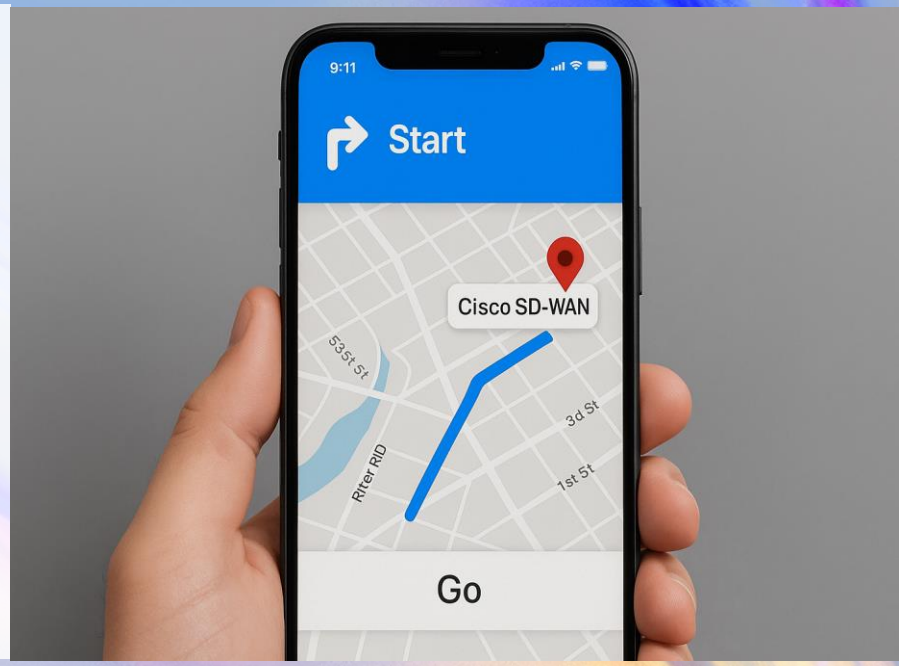
Advanced Troubleshooting



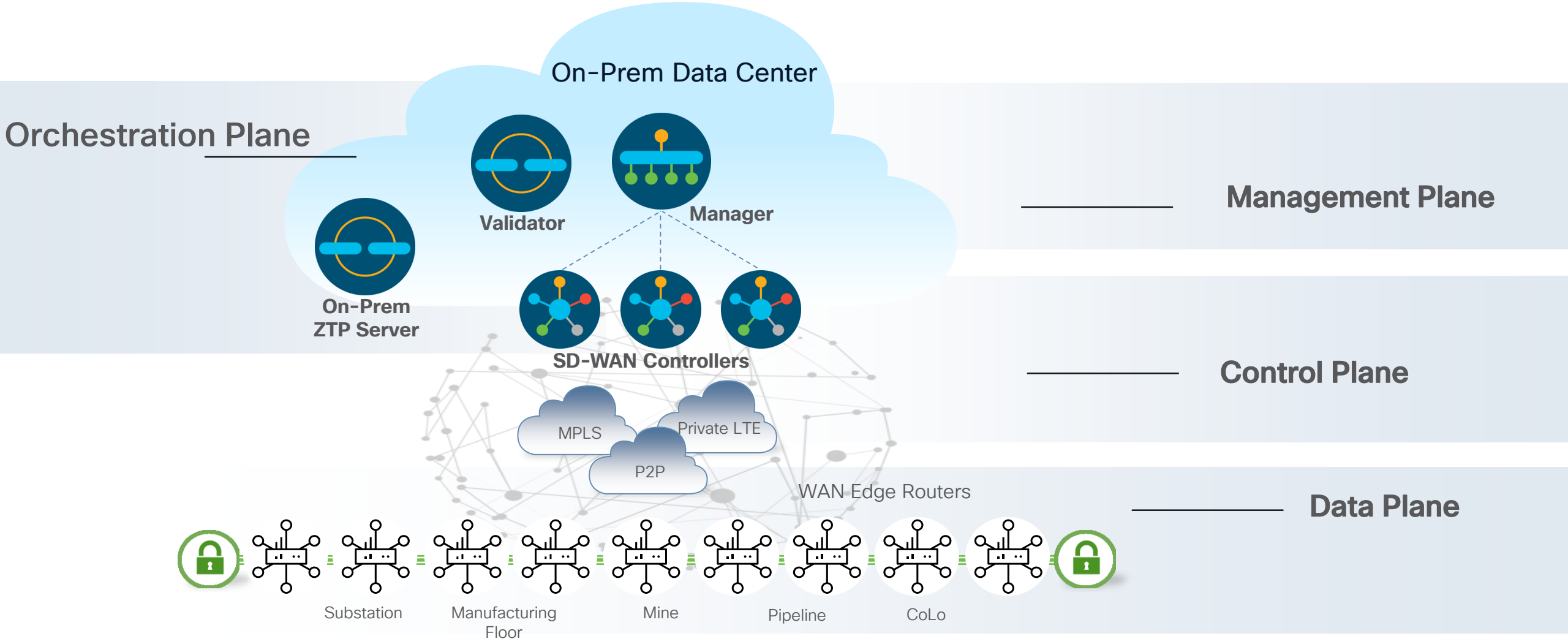
Site Topology w/ Troubleshooting Tools

Alarm Correlation

Building an Air Gapped SDWAN Fabric

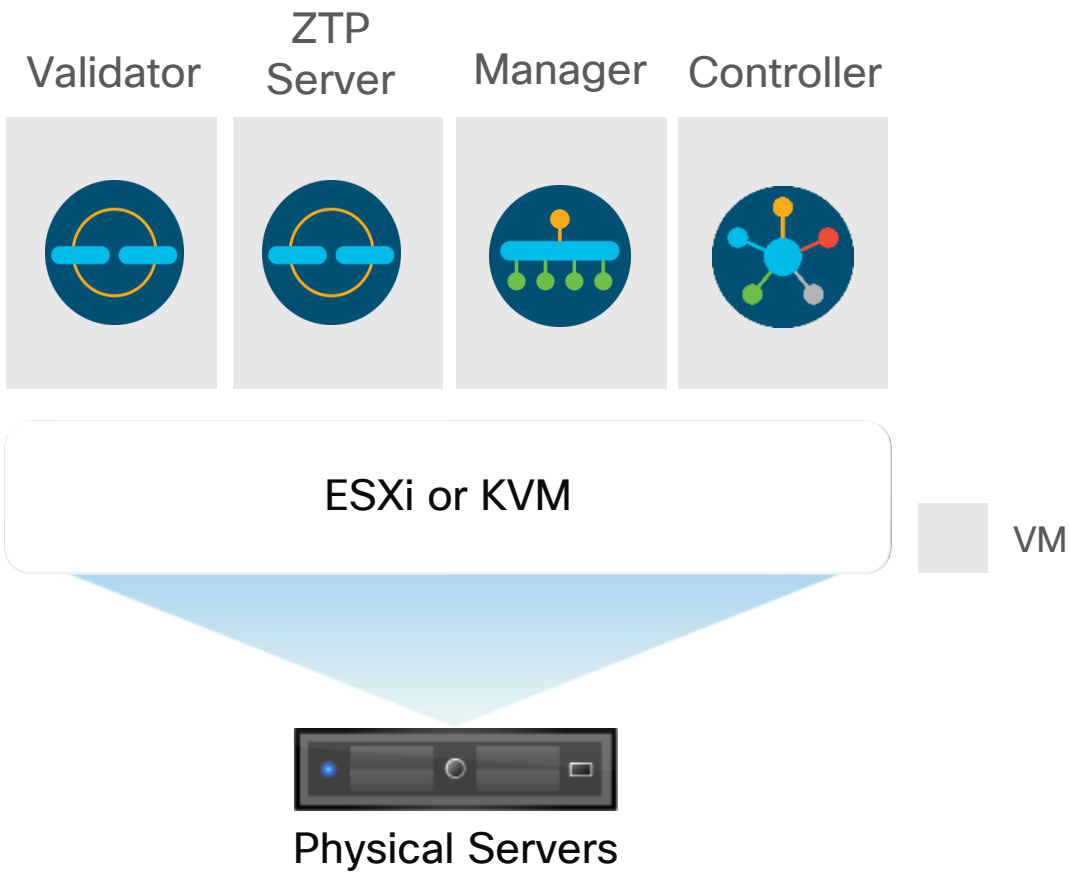


Cisco Catalyst SD-WAN Solution Components

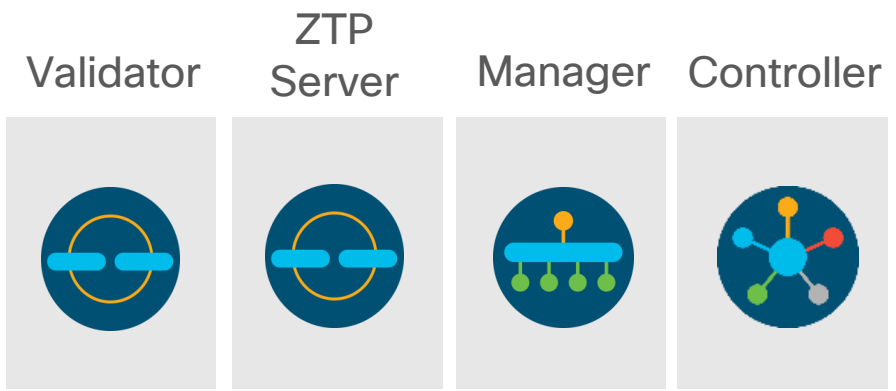


Control Element Deployment Options

On-Premise



Hosted



Certified Cloud (PCI, SOC2/ISO/C5)*

Gov. Cloud (FedRAMP)*

Please see the Cisco Catalyst SD-WAN Getting Started Guide for details on Resource Requirements of all components

Comprehensive Portfolio of Data Plane Elements

SD-WAN + Services

C8500 Secure Router
Data Center

C8400 Secure Router
Campus

C8300 Secure Router
Large Branch

C8200 Secure Router
Medium Branch

C8100 Secure Router
Small Branch

Catalyst 8000V

Catalyst 8500L/8500

Catalyst 8300

Catalyst 8200

ISR1K / ISR 1100-4G/6G

Rugged Series Routers

IR 1101

IR 8300

IR 1800

IR 8140

450Mhz
(PIM)

Anterix
900Mhz
(PIM)

4G LTE
(PIM)

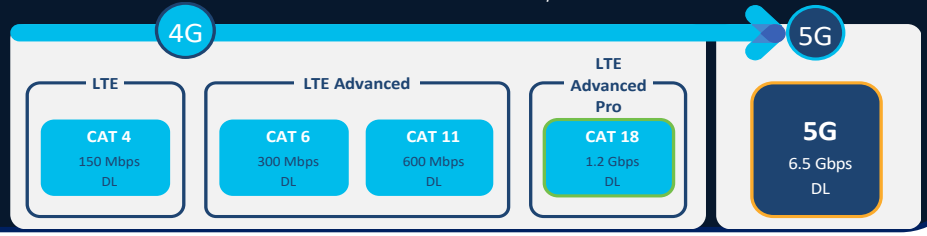
5G/sub-6
(PIM)

CG522
5G/Sub-6 GHz

Cellular
LTE / 5G

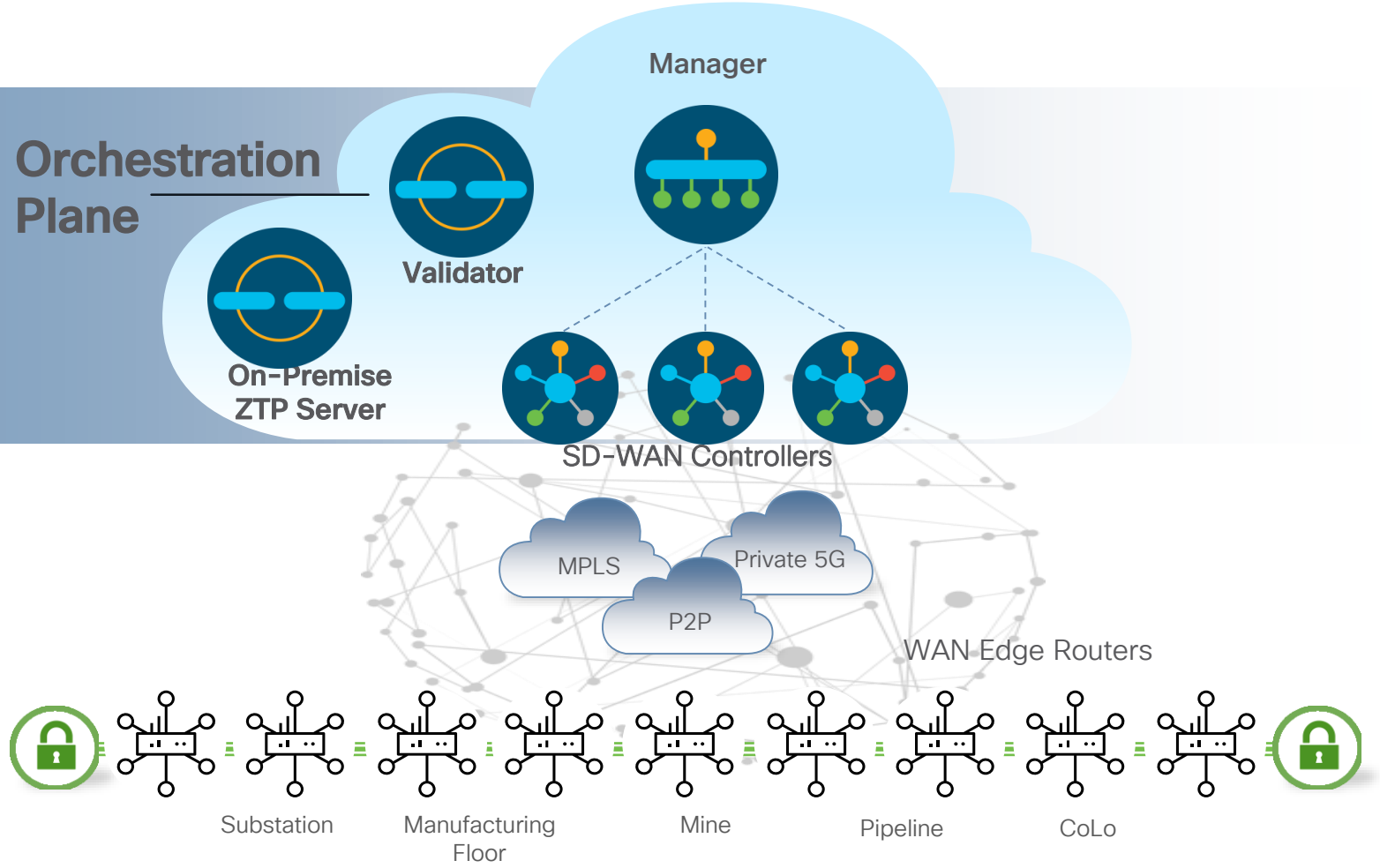
CBRS

FIRSTNET
Built with AT&T



Orchestration Plane for Air Gap

Cisco Catalyst SD-WAN Solution Elements



Orchestration Plane

SD-WAN Validator and On-Prem ZTP Server

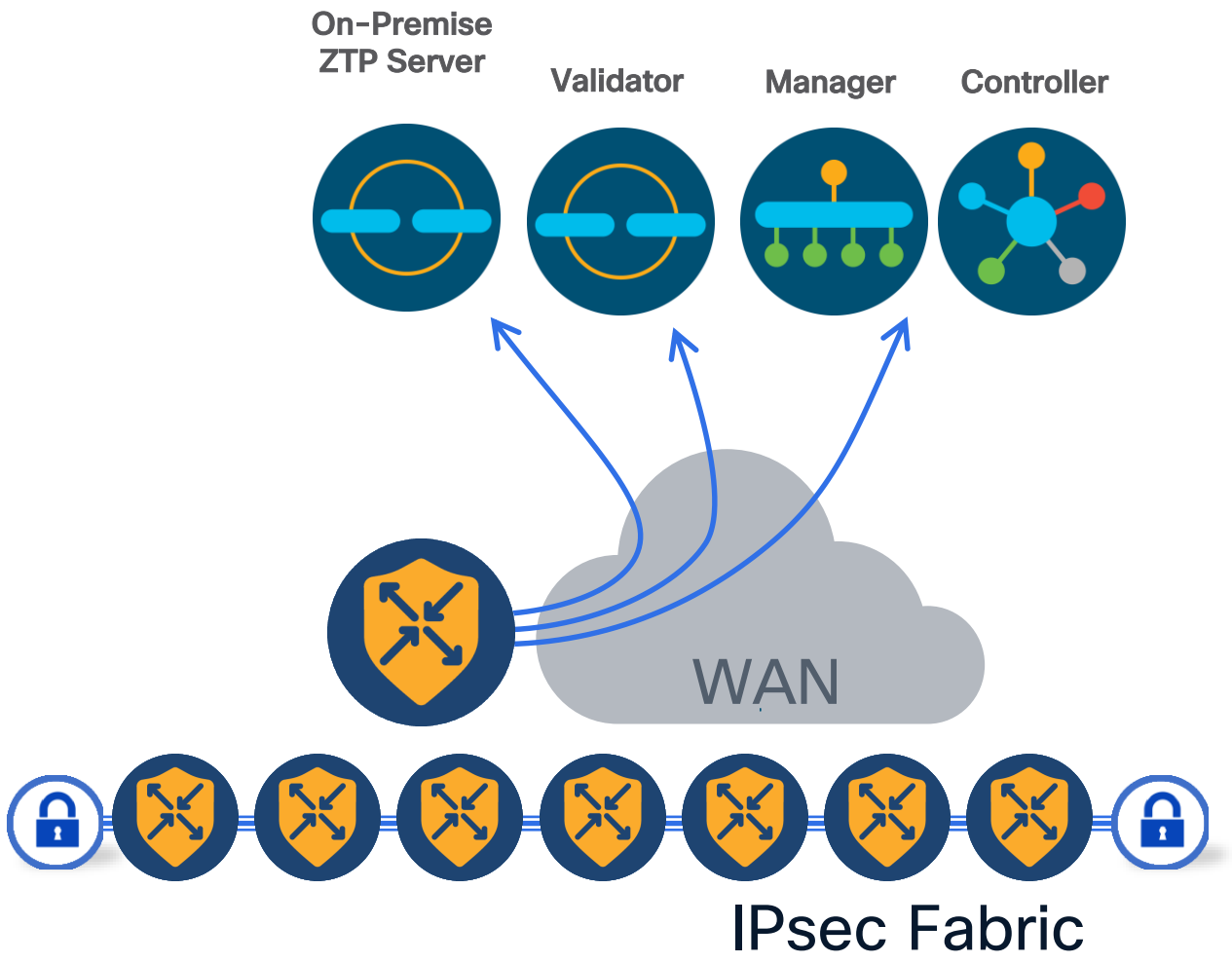
On-Premise ZTP Server

- Automates secure day-zero onboarding and deployment of WAN Edge devices with factory settings.
- Performs same function as **devicehelper.cisco.com** but for air gap deployments.

Validator

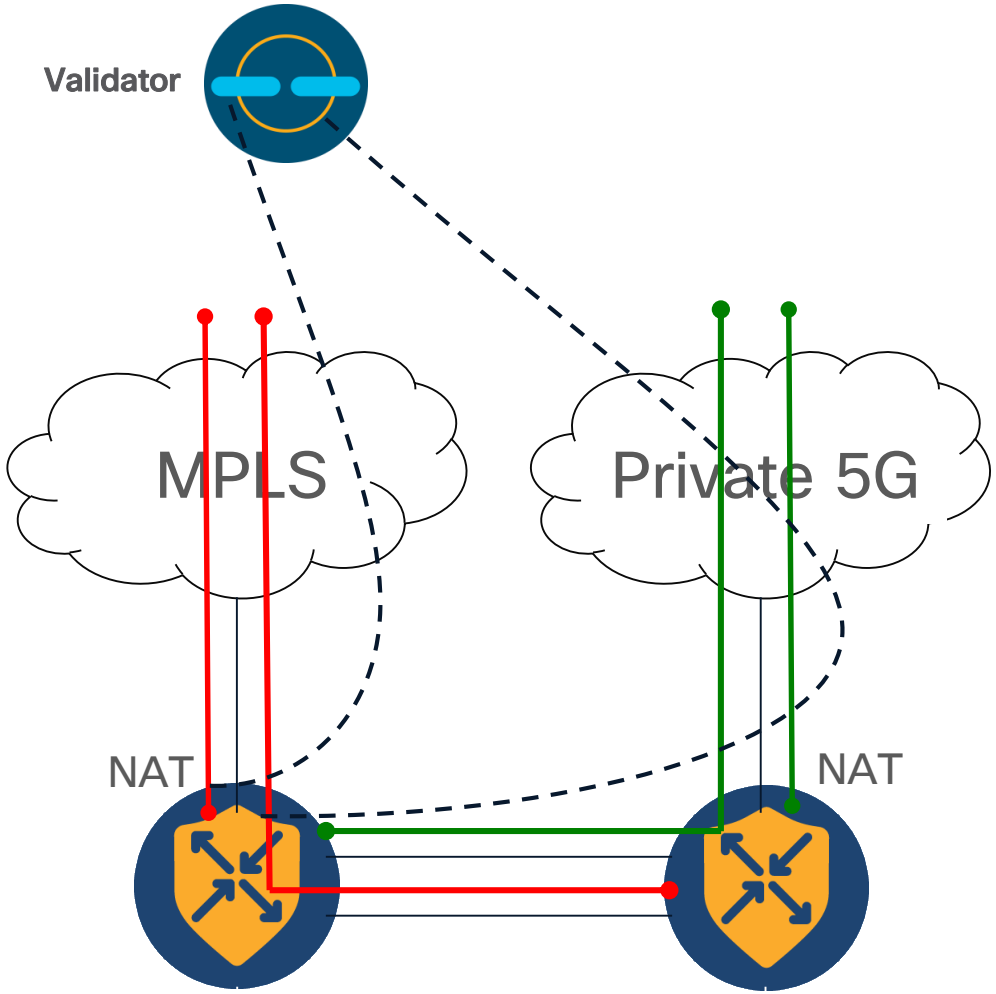
- Orchestrates control and management plane
- Functionally the same with no difference to non-air gapped deployment

Options for Onboarding Devices in Air gap



- **DHCP**: Connect the SD-WAN appliance to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- **AutoIP**: Allows SD-WAN appliances to "learn" their static IP assignment through ARP requests/responses. Programs itself with 8.8.8.8 for DNS server which would need to be represented in the air gap network if this choice is used.
- **Browser**: ZTP option to pre-stage SD-WAN Appliance. Requires L2 module.
- **USB**: Option to bootstrap SD-WAN appliance
- **Cellular**: If cellular network can provide APN information OTA, otherwise use options above

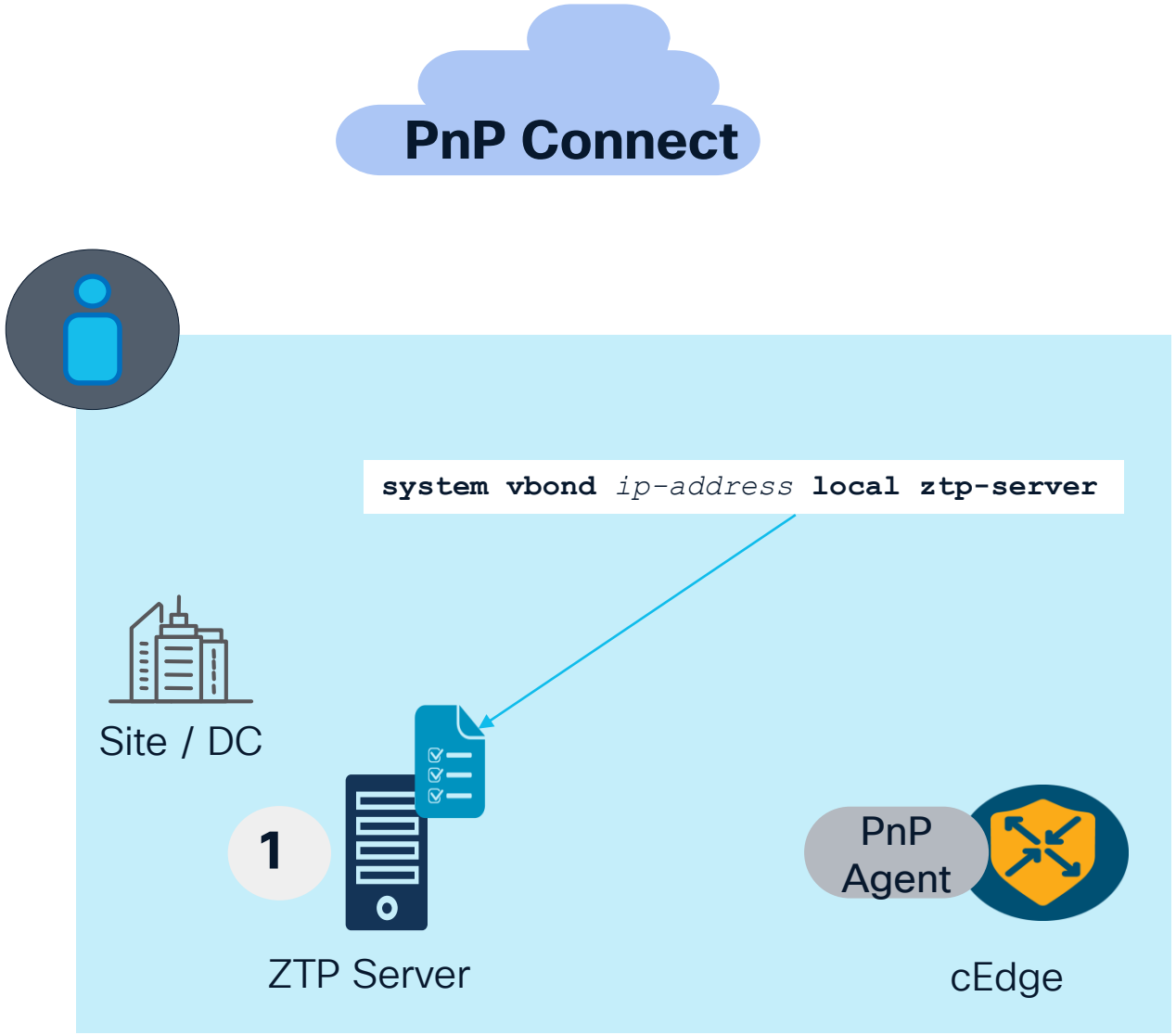
TLOC Extension in Air gap



- Hybrid Networks: TLOC extension avoids NAT when using private IPs for tunnels. Typically requires use of BGP to advertise TLOC extension subnet
- Air Gap Networks: TLOCs can use NAT for TLOC-extensions if no NAT gateway exists between the WAN circuit and validator
- Note: Make sure to use public color for TLOC when using NAT and TLOC-Extension

On-Prem ZTP Overview

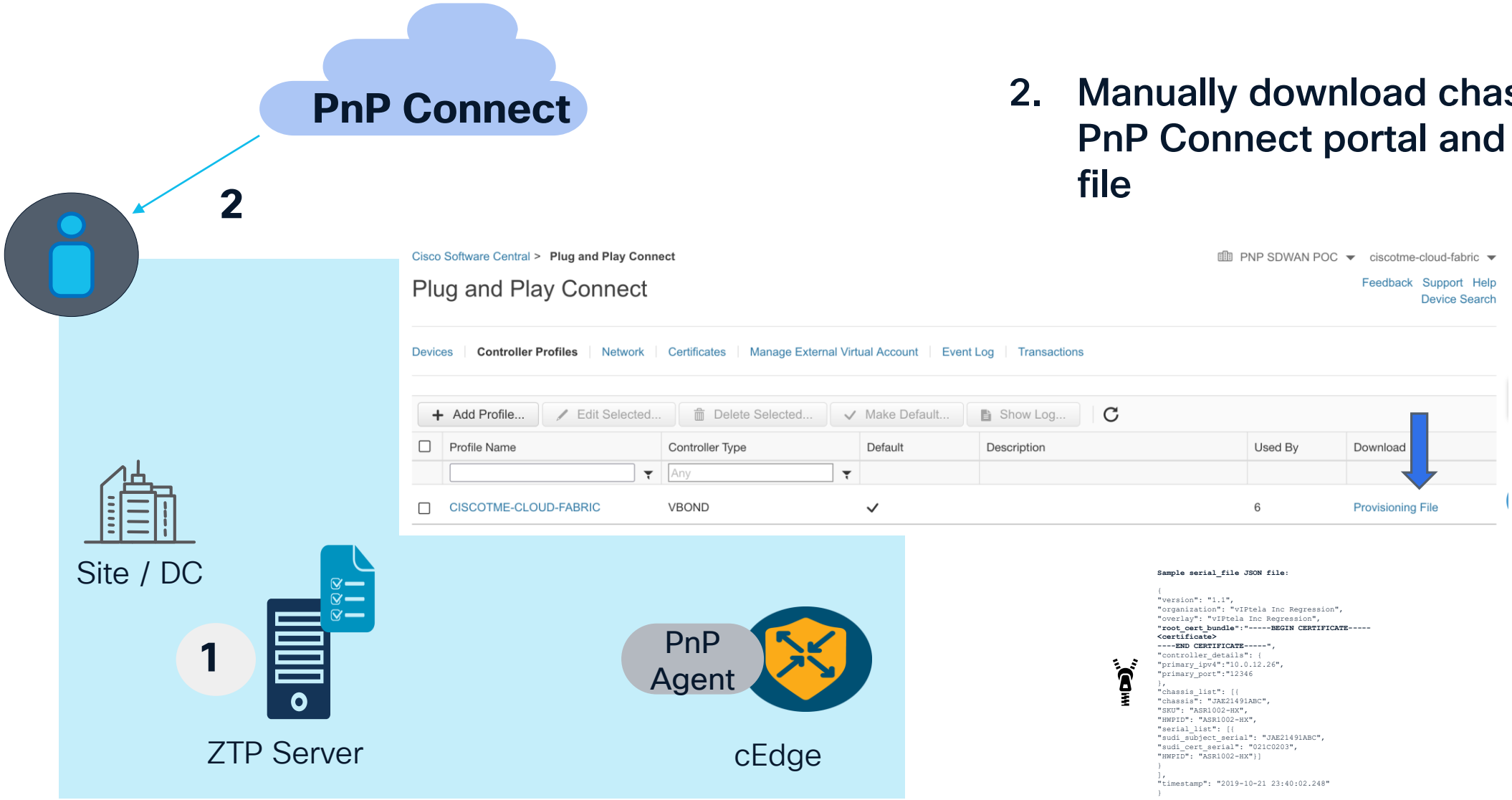
1. Start ZTP server by configuring a Validator as a ZTP server.



On-Prem ZTP Overview

1. Start ZTP server by configuring a Validator as a ZTP server.

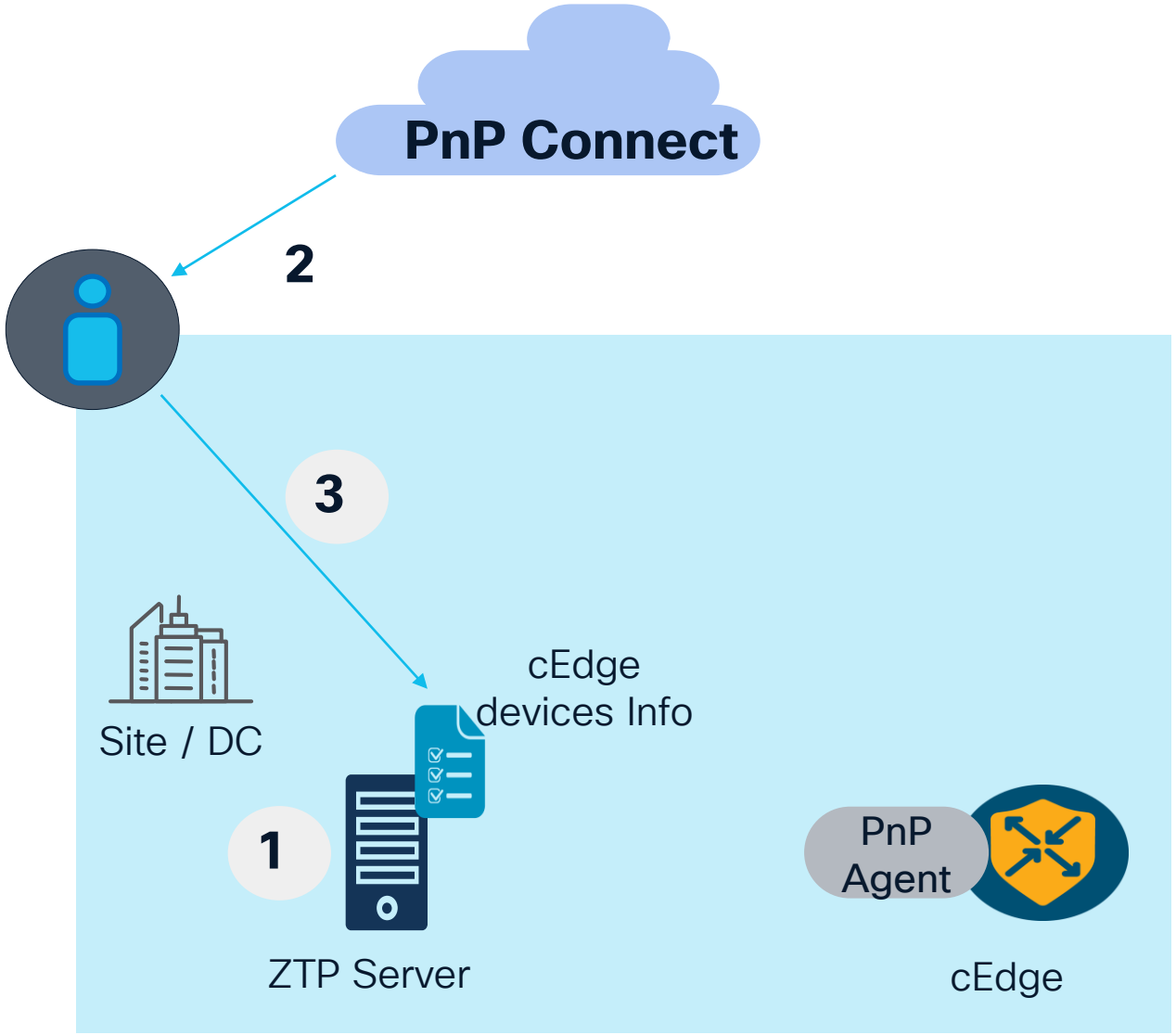
2. Manually download chassis zip file from PnP Connect portal and extract JSON file



Sample serial_file JSON file:


```
{
"version": "1.1",
"organization": "vIPtela Inc Regression",
"overlay": "vIPtela Inc Regression",
"root_cert_bundle":"-----BEGIN CERTIFICATE-----
<certificate>
-----END CERTIFICATE-----",
"controller_details": {
"primary_ipv4":"10.0.12.26",
"primary_port":"12346
},
"chassis_list": [{
"chassis": "JAE21491ABC",
"SKU": "ASR1002-HX",
"HWPID": "ASR1002-HX",
"serial_list": [{
"sudi_subject_serial": "JAE21491ABC",
"sudi_cert_serial": "021C0203",
"HWPID": "ASR1002-HX"}]
}
],
"timestamp": "2019-10-21 23:40:02.248"
}
```

On-Prem ZTP Overview



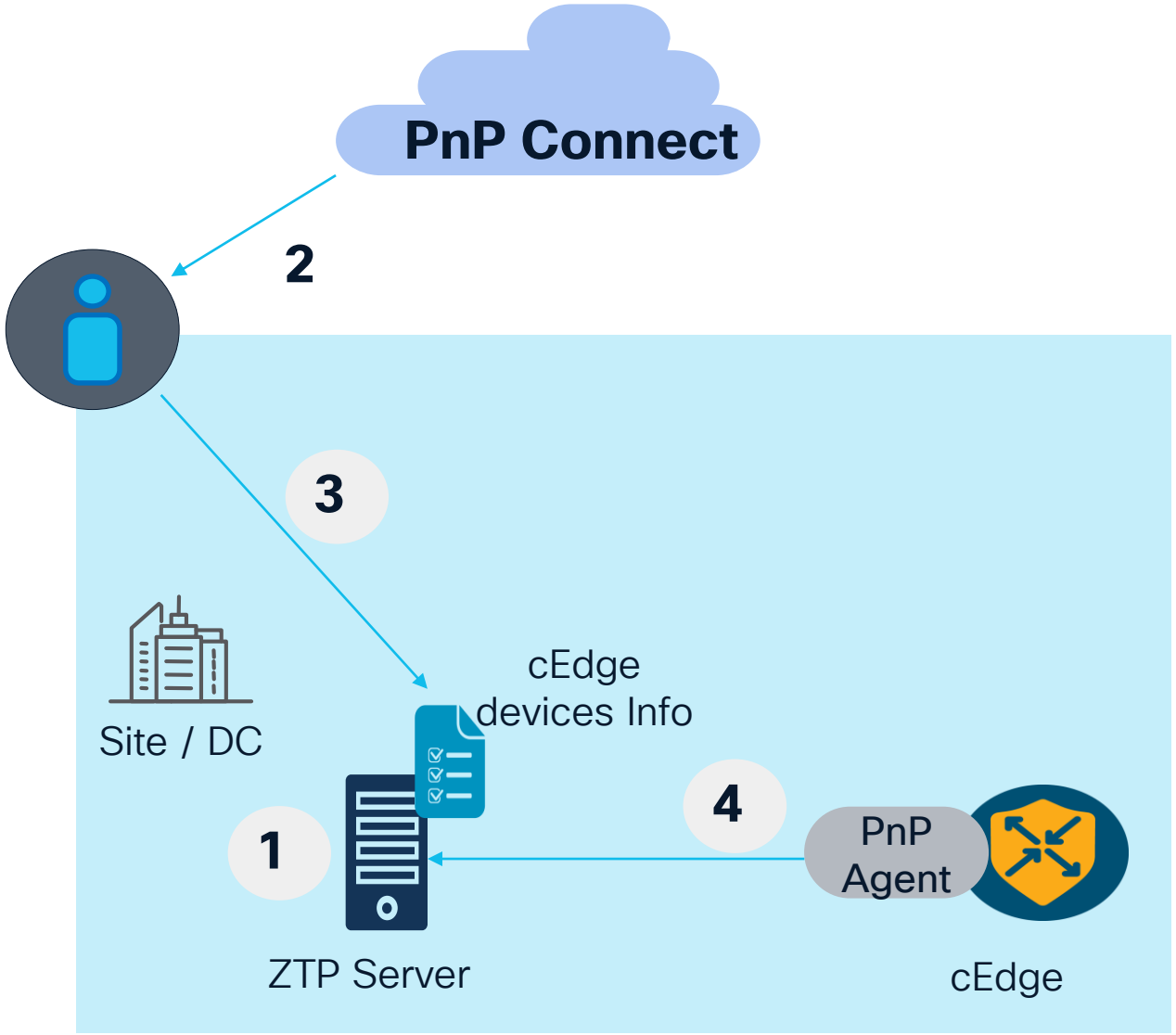
1. Start ZTP server by configuring a Validator as a ZTP server.

2. Manually download chassis zip file from PnP Connect portal and extract JSON file

3. Upload/add JSON file to ZTP server and verify cEdge information

```
Add - Validator# request device-upload chassis-file JSON-file-name
Verify -Validator# show ztp entries
Verify - Validator# show orchestrator valid-devices
```

On-Prem ZTP Overview



1. Start ZTP server by configuring a Validator as a ZTP server.

2. Manually download chassis zip file from PnP Connect portal and extract JSON file

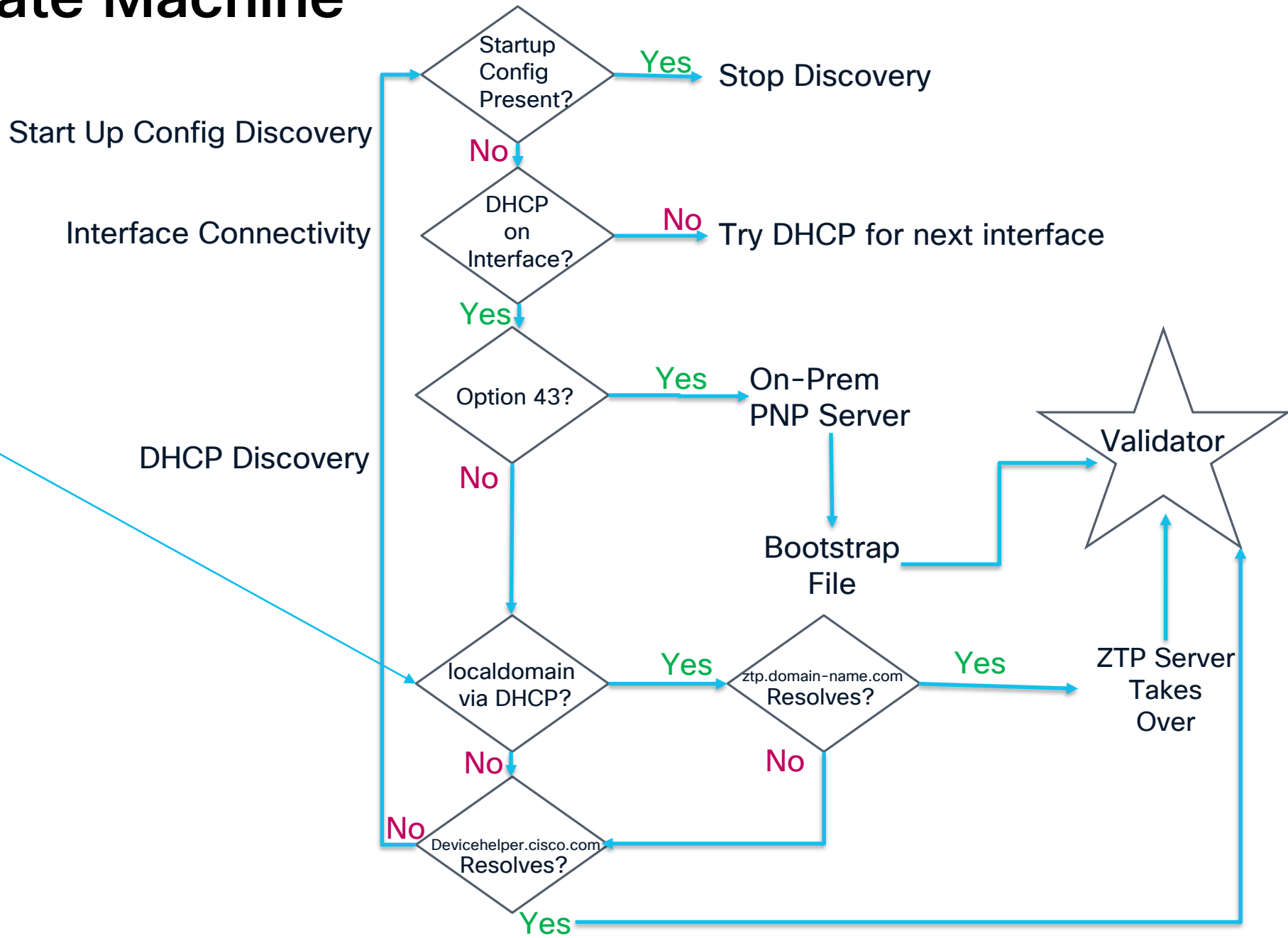
3. Upload/add JSON file to ZTP server and verify cEdge information

4. Power-ON cEdge. PnP agent connects to ZTP server

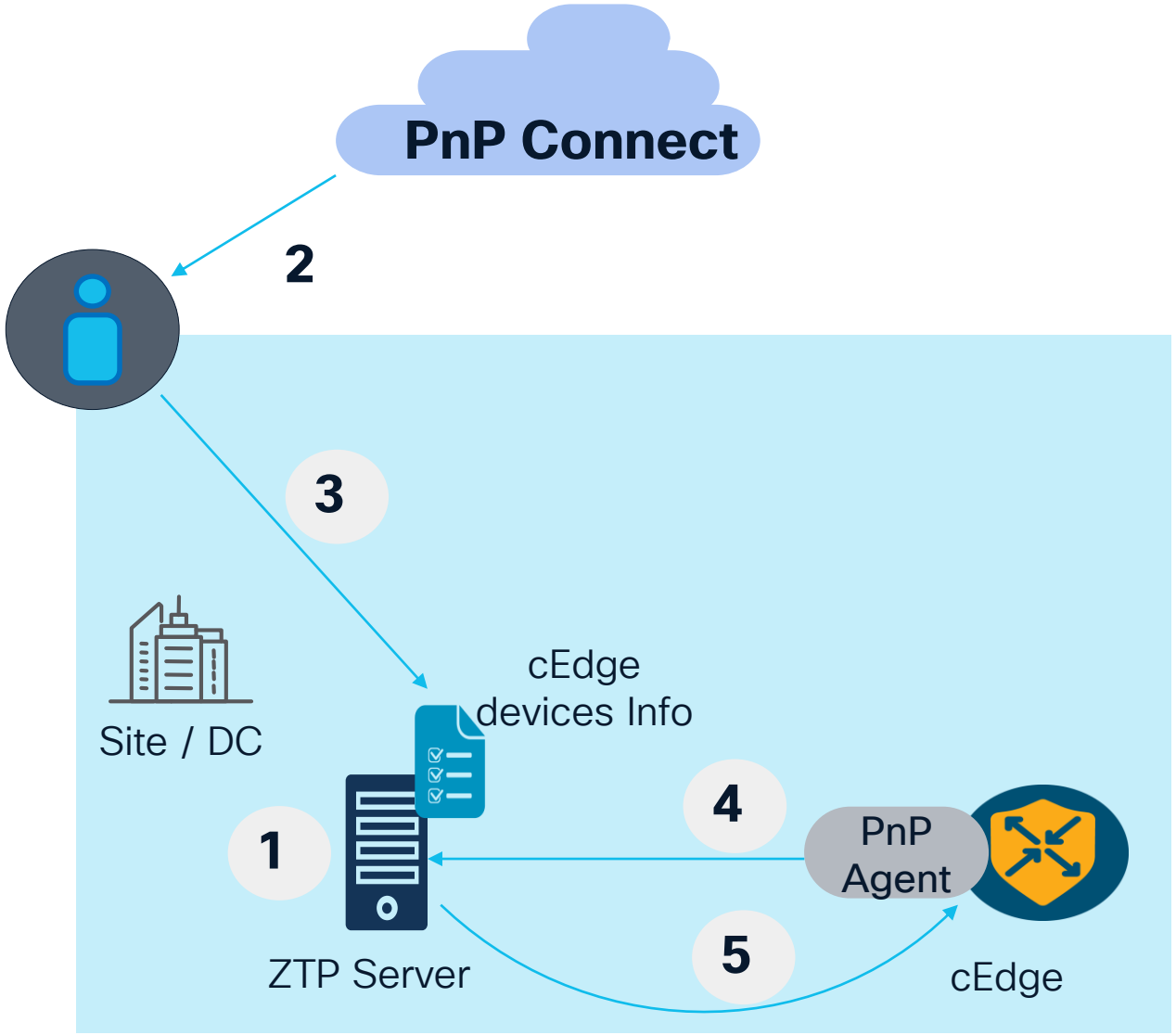
ZTP Discovery State Machine

PnP-agent on cEdge tries to connect to the on-prem ZTP server

If not available, it will try to connect to the cloud-based PnP server.

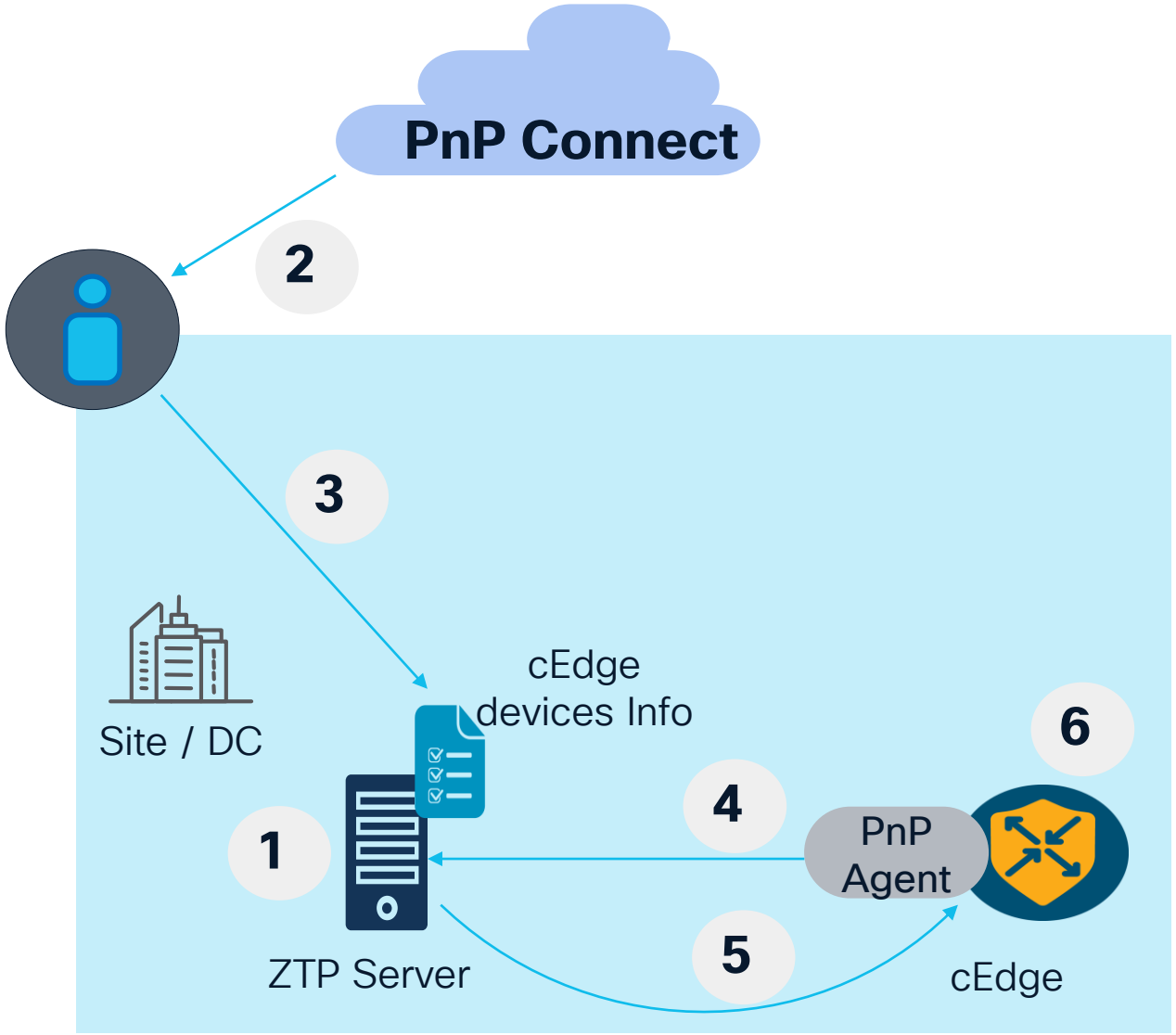


On-Prem ZTP Overview



1. Start ZTP server by configuring a Validator as a ZTP server.
2. Manually download chassis zip file from PnP Connect portal and extract JSON file
3. Upload/add JSON file to ZTP server and verify cEdge information
4. Power-ON cEdge. PnP agent connects to ZTP server
5. ZTP server authenticates cEdge and provides Validator IP or FQDN + OrgName + EntRootCA(Optional)

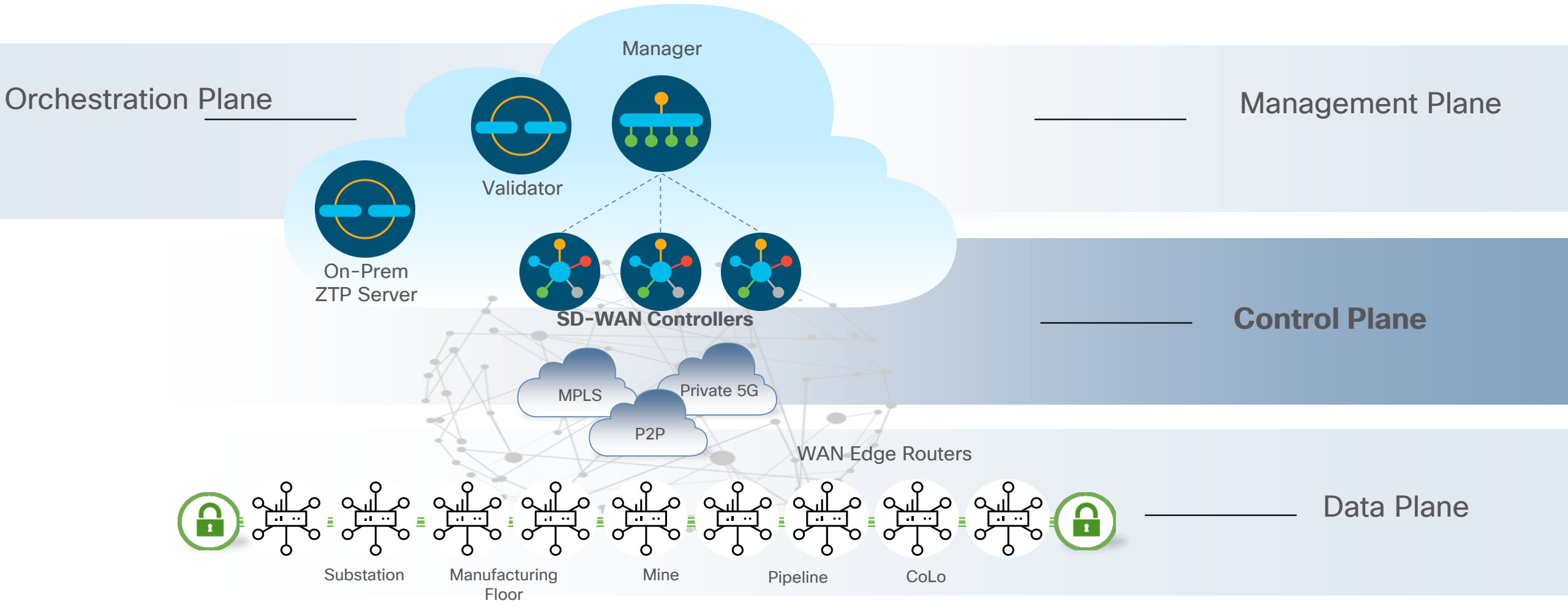
On-Prem ZTP Overview



1. Start ZTP server by configuring a Validator as a ZTP server.
2. Manually download chassis zip file from PnP Connect portal and extract JSON file
3. Upload/add JSON file to ZTP server and verify cEdge information
4. Power-ON cEdge. PnP agent connects to ZTP server
5. ZTP server authenticates cEdge and provides Validator+OrgName+EntRootCA
6. Update RootCA on cEdge if JSON file specifies it as Default

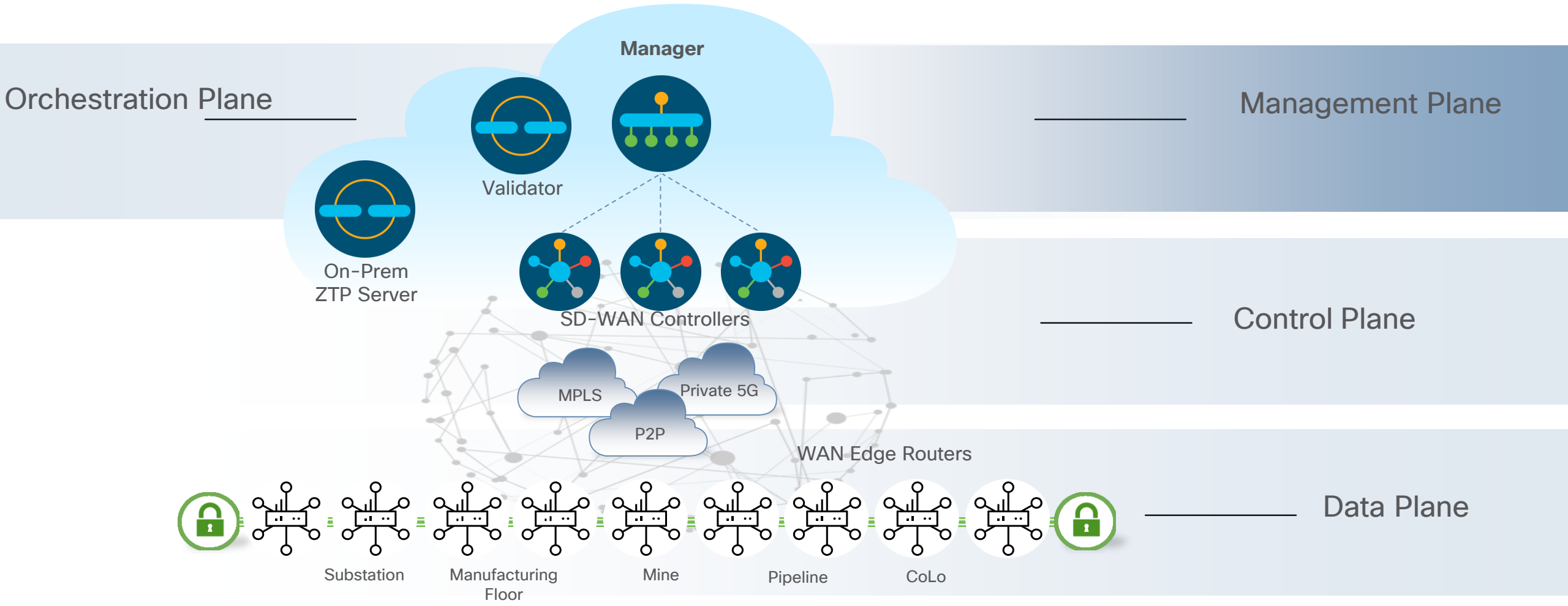
For Details See ZTP Configuration Guide

Cisco Catalyst SD-WAN Solution Components

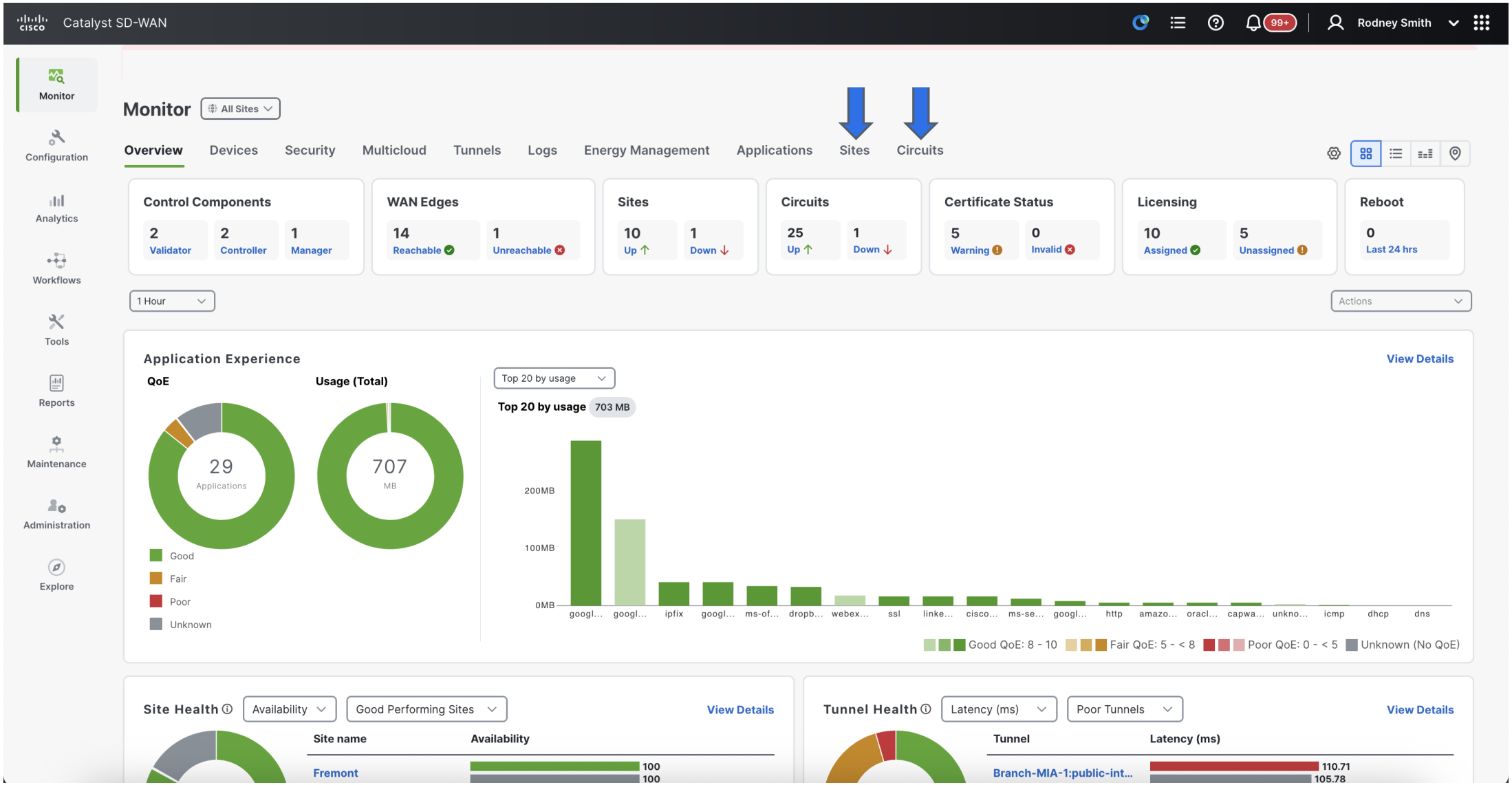


Management Plane for Airgap

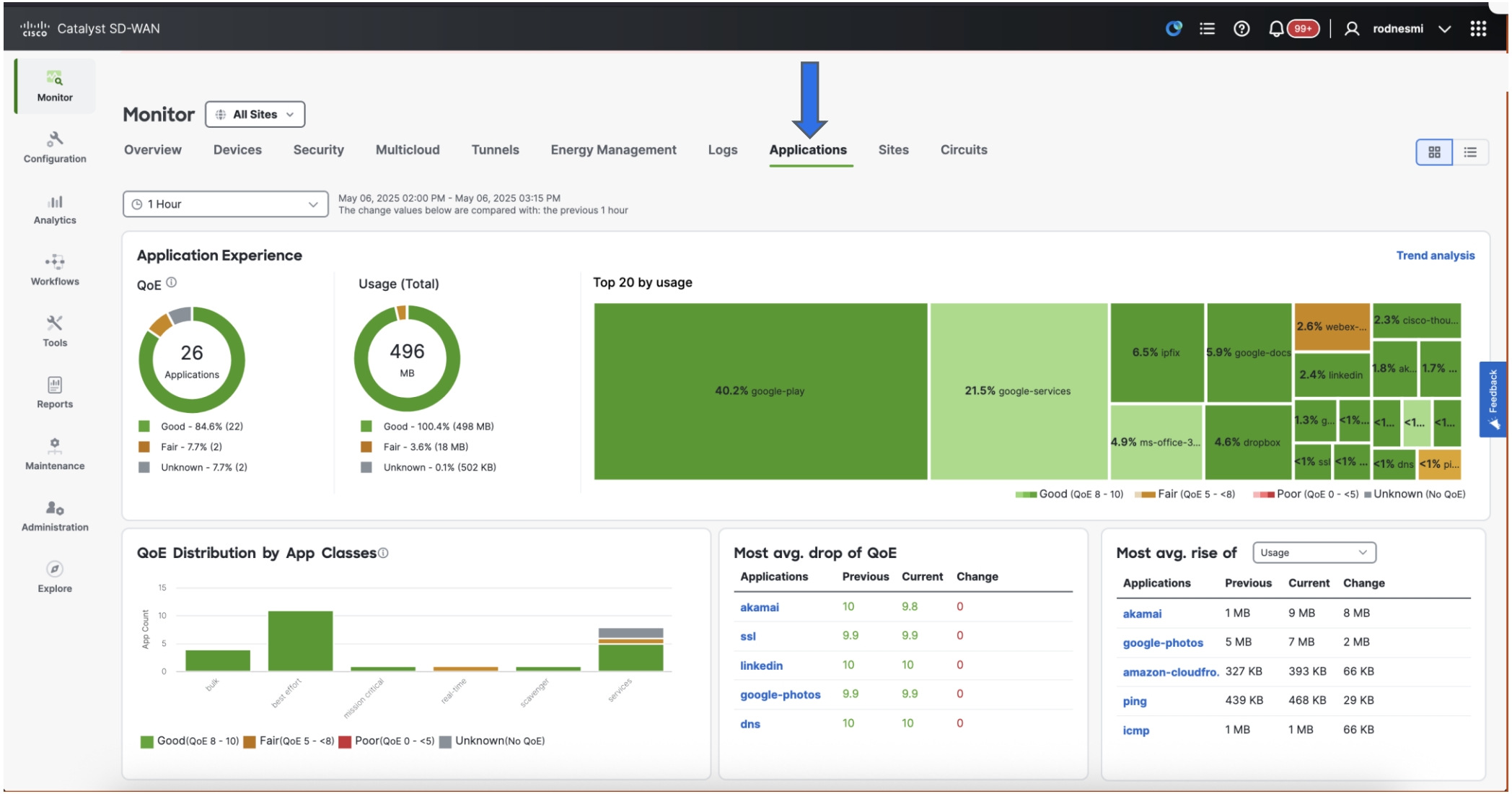
Cisco Catalyst SD-WAN Solution Components



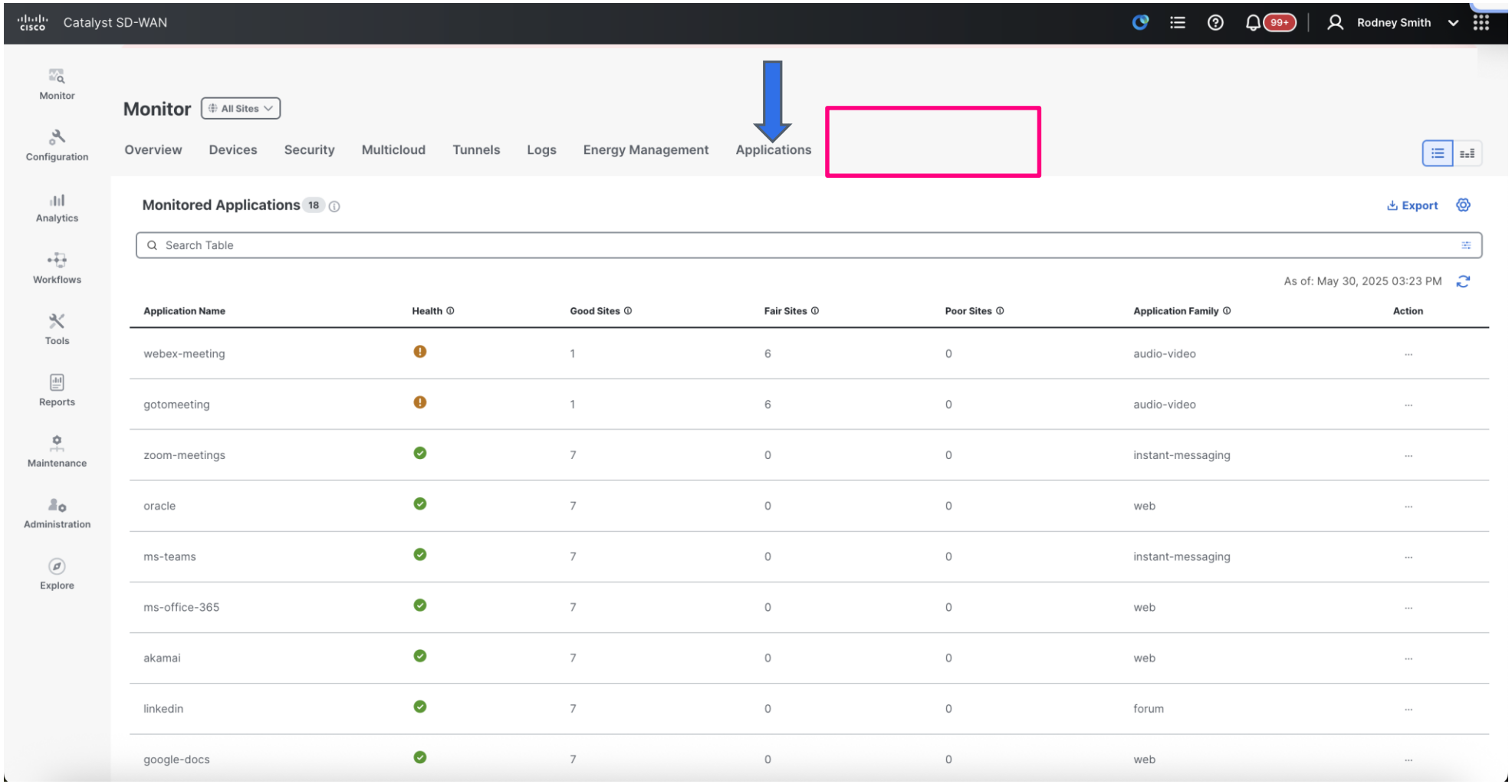
SD-WAN Manager Dashboard - With Cloud Connectivity



SD-WAN Manager Applications - With Cloud Connectivity



SD-WAN Manager Applications - No Cloud Connectivity



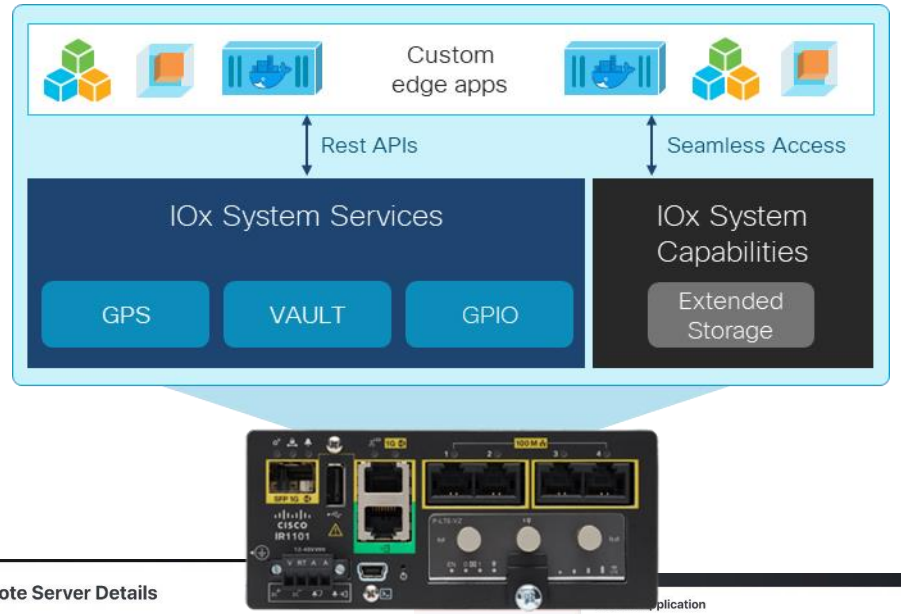
SD-WAN Container Application Management

Cisco Apps

ThousandEyes *

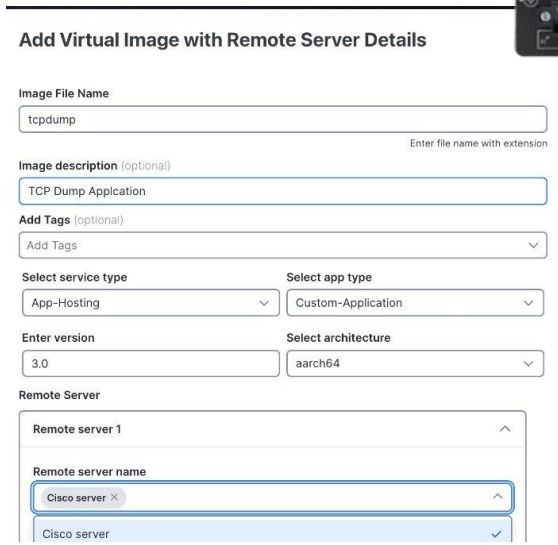
Cisco Secure Equipment Access *

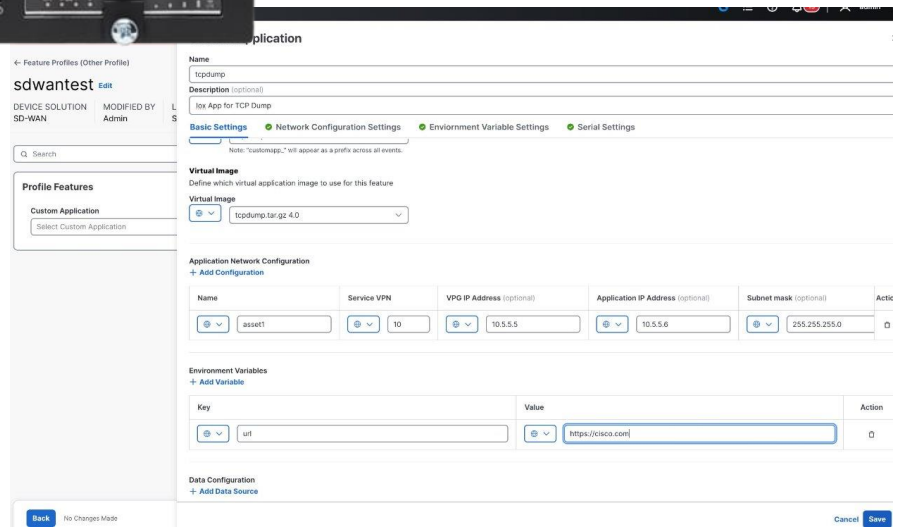
Cisco Cyber Vision



3rd Party Apps

IgnitionEDGE
EPG EXIMPROD GRUP
OPEN FMB
EATON
CYLUS
Tantalus Transforming Utilities and Communities.



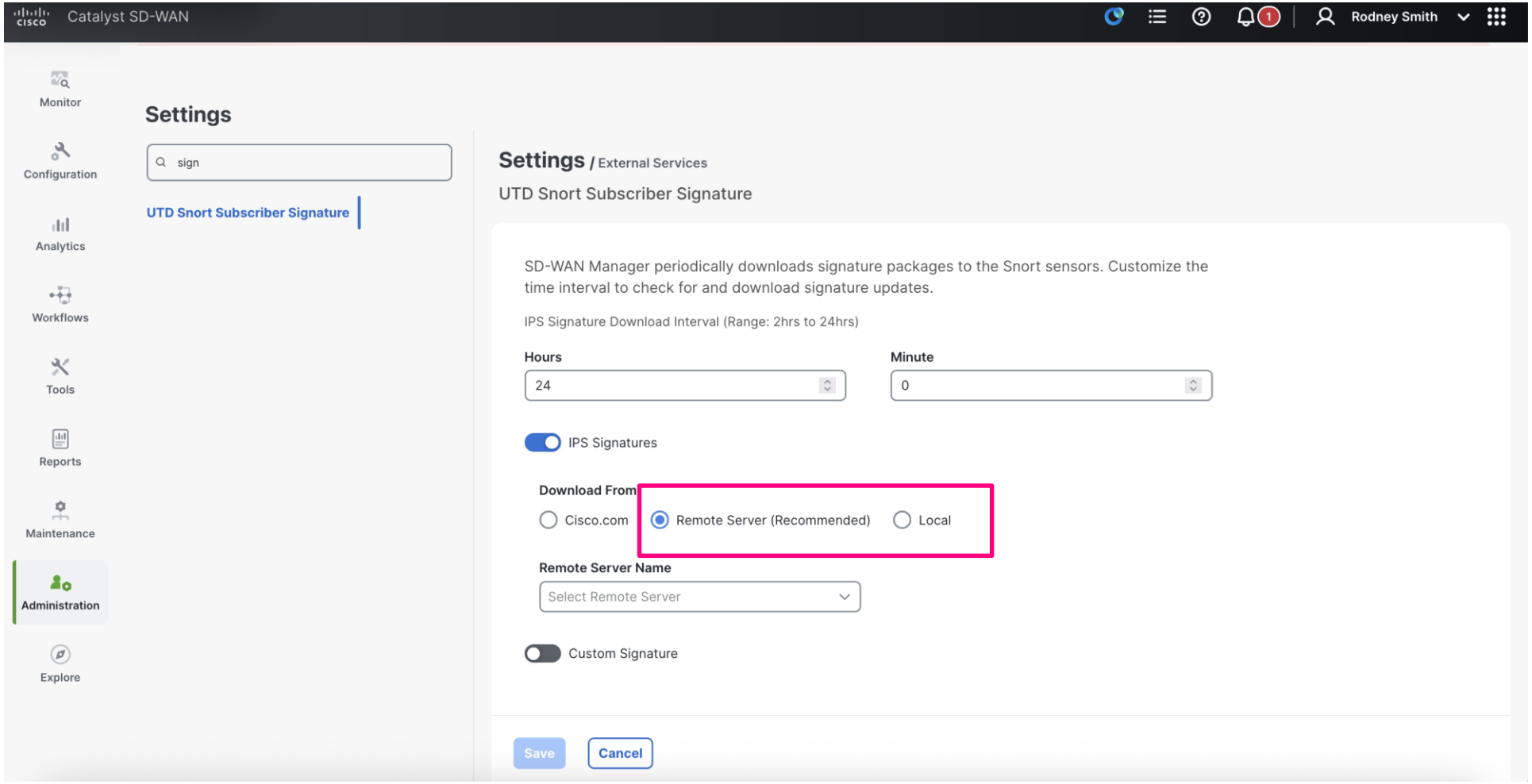


*Requires cloud access

For details consult the installation guide

SD-WAN Manager IPS Signature Offline

- Download the latest signatures from Cisco, then use Remote Server or Local option to update signatures offline.



We recommend:

Remote Server option to avoid scaling issues

Remotes servers can be:

HTTP

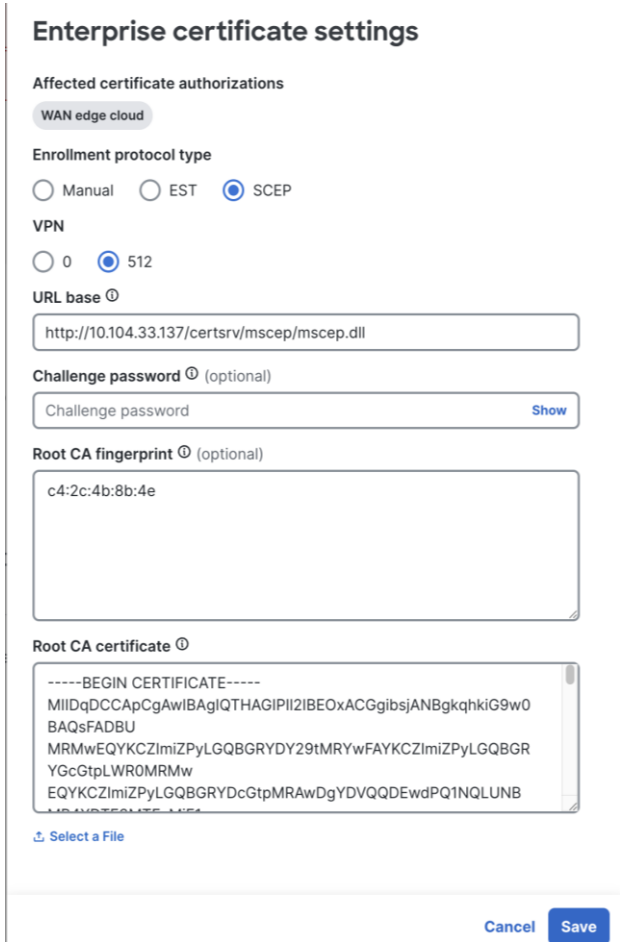
FTP

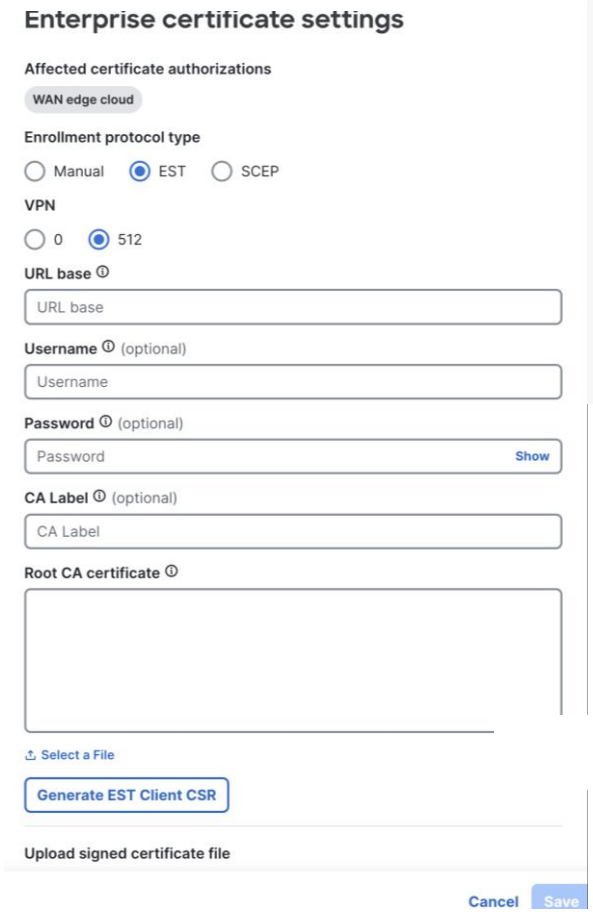
SCP

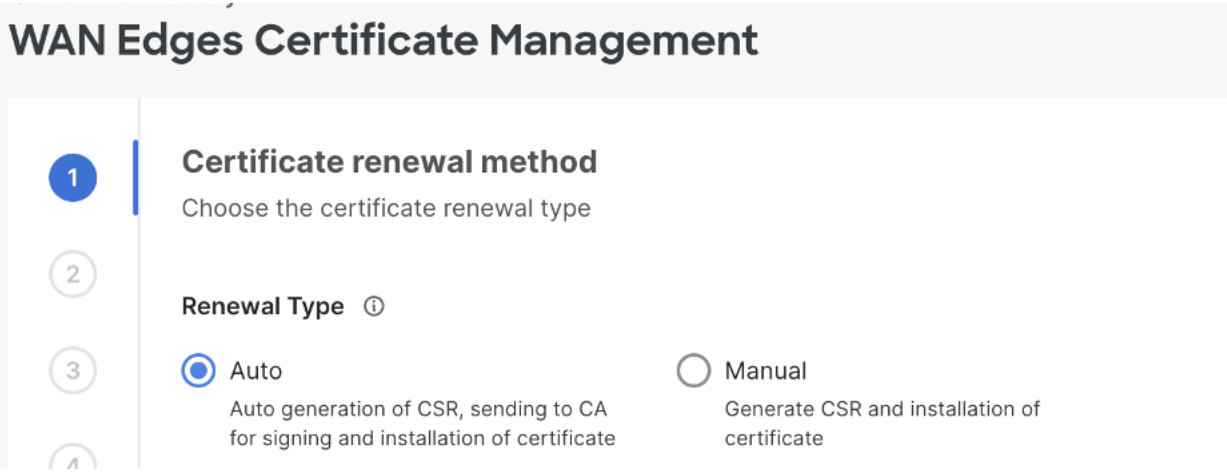
For details, visit the configuration guide

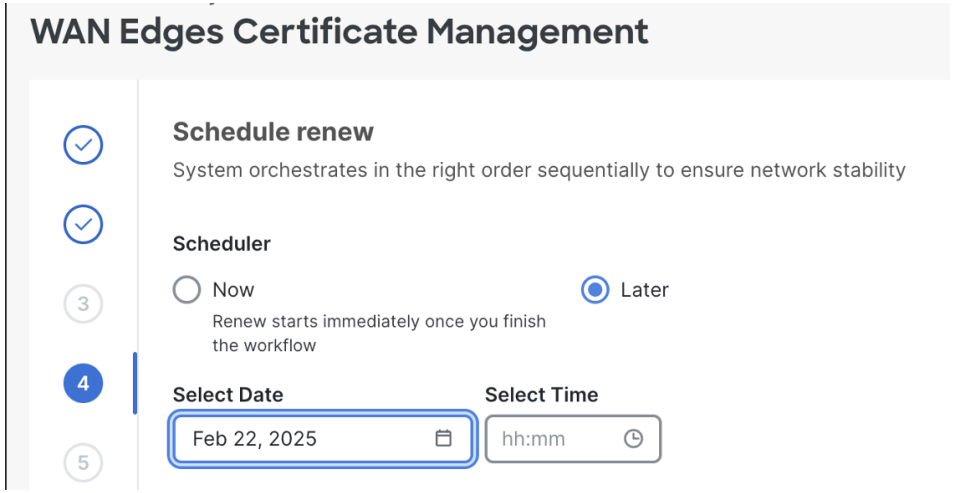
Enterprise Certificate Configuration: Simple Certificate Enrollment Protocol/Enrollment over Secure Transport (20.18)

New!









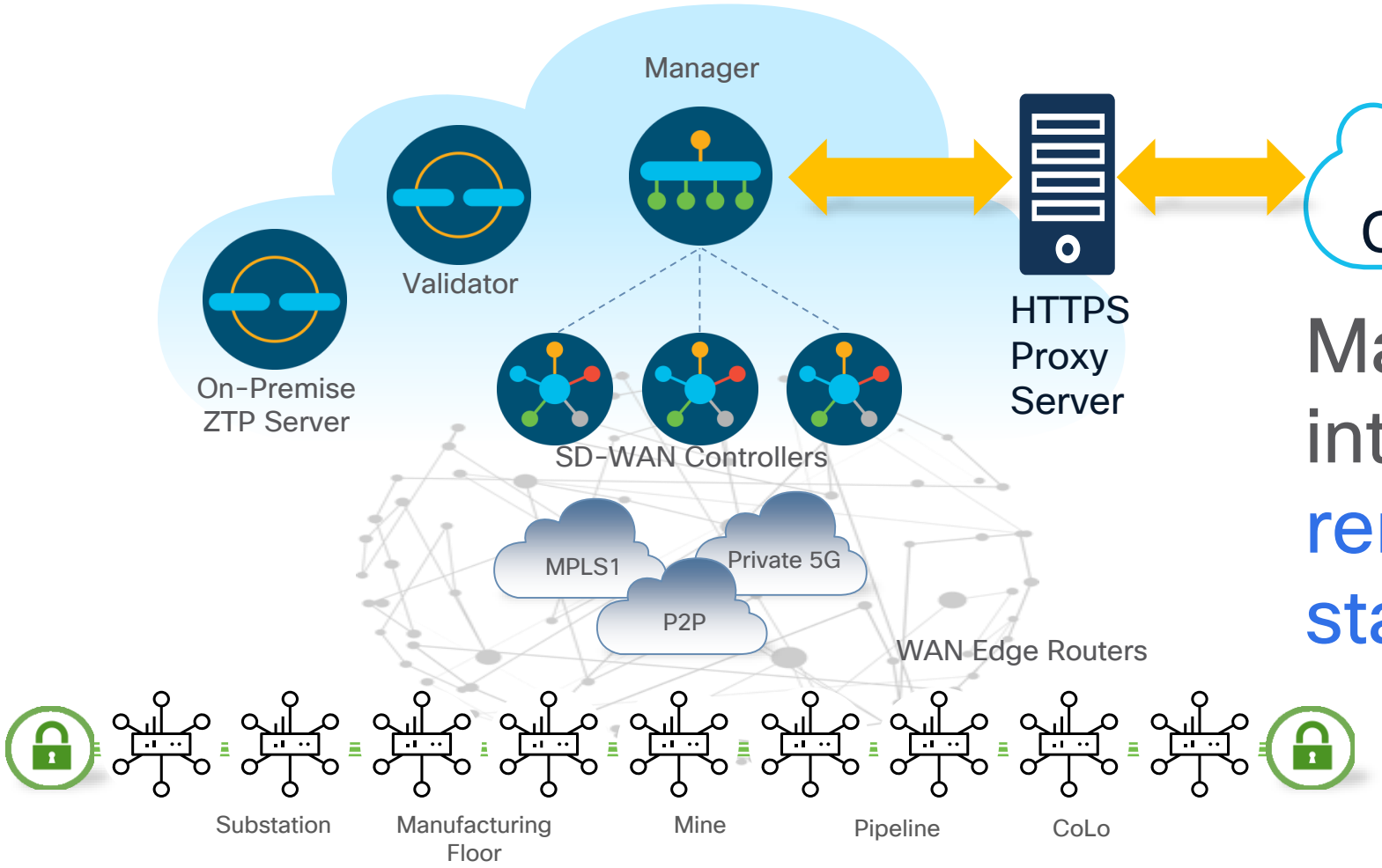
SD-WAN Manager Services Cloud Only Features

- **Following require connectivity to public internet and Cisco subscription to support**
  - Mainly Cloud Services - Analytics / Threat Grid / ThousandEyes / AI Assistant / Umbrella
  - Application signatures fed from cloud via SD-AVC. SD-AVC as a service still functions in airgap
  - Cloud for OnRamp for Multicloud
  - TAC Case integration
  - Meraki Integration

- Synchronizing information via Cisco Smart Account
- Microsoft and Webex telemetry
- Cisco DNA Portal for providing online documentation
- Controller Certificate Authorization (Automatic)
- DUO MFA
- Cisco Catalyst SD-WAN Portal features:
  - Configuration feature template migration to configuration group
  - Configuration Catalogs

Additional Considerations for Air Gap Networks

Cisco Catalyst SD-WAN – Partial Air Gap



Manager connected to internet via proxy, remaining elements stay air gapped

*See Configuration Guide for further details

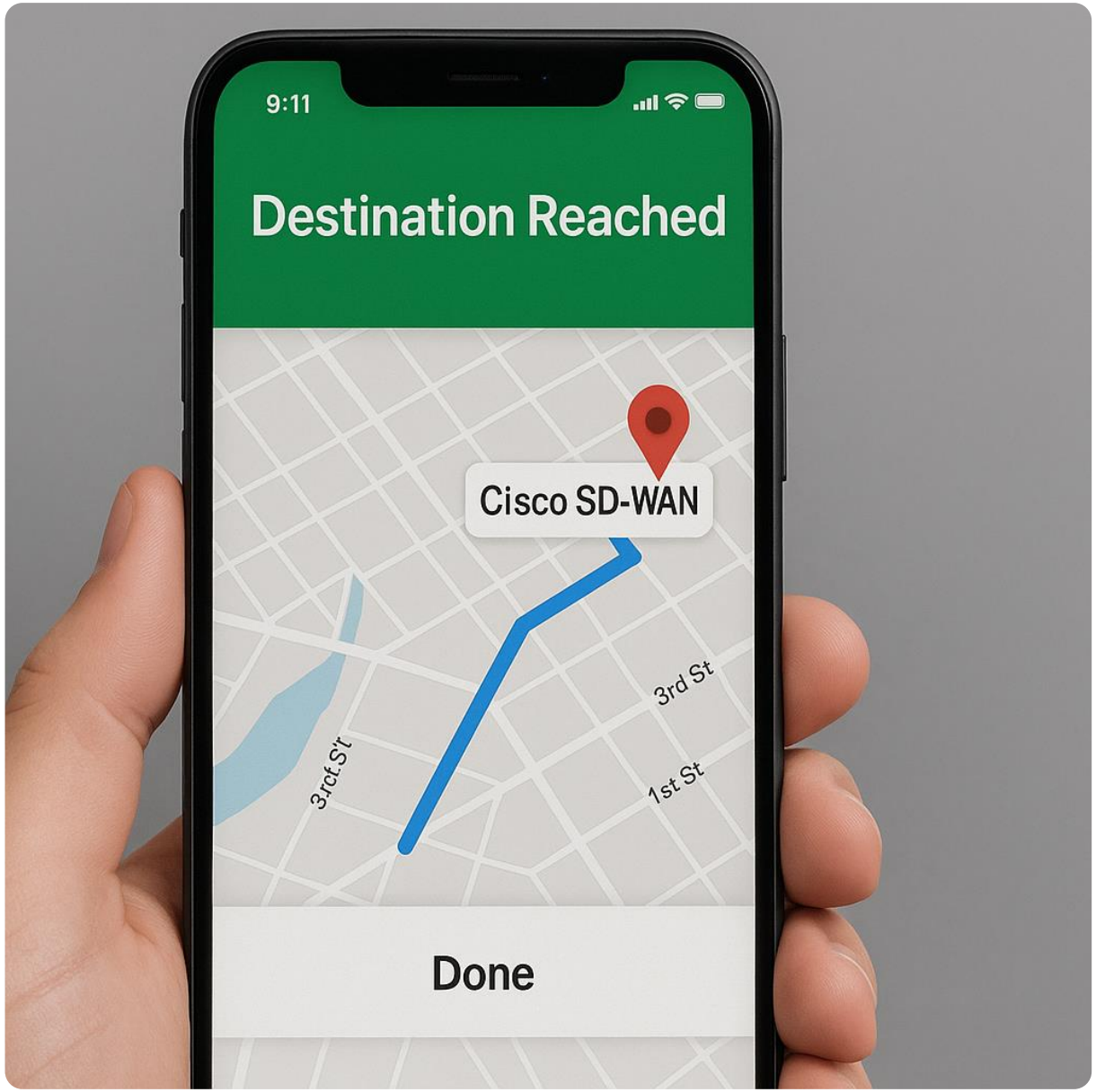
Comparison of Deployment Types Partial Air Gap to Full Air Gap

	Partial Air Gap (Only SD-WAN Manager has access to internet)	Full Air Gap (All control elements)
Cisco SD-WAN Analytics	Yes	No
Cisco Smart Software Manager (CSSM) for Licensing	Yes	Partial, on-prem CSSM*
Smart Account Management – Cisco PKI Certificate Management TAC Case integration PNP Connect device sync	Yes	No
Cisco Catalyst SD-WAN Portal – Configuration Catalog Migration Assistant	Yes	No
IPS Signature automatic updates	Yes	Partial, Offline updates
Interactive Helper & Online Documentation	Yes	No
Managed Cellular Activation via Cisco IoT Control Center	Yes	No
DUO MFA	Yes	No
ThousandEyes WAN Insights / Predictive Path Insights	Yes	No

*Learn more watch BRKXAR-1013

Key Takeaways

- **Cisco SD-WAN supports Air Gap Networks**
- ZTP automation can be done
- SD-WAN Provides Automation, Monitoring, Troubleshooting, Advanced Security Capability and Enhanced Application Experience compared
- Separation of Orchestration, Management, Control and Data Planes allows greater deployment flexibility with Air Gap environments
- SD-WAN Manager accessing cisco.com via HTTPS proxy enables additional capabilities whilst still ensuring a completely Air Gapped control and data plane



Complete your session evaluations

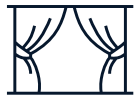
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

cisco Live !


CISCO

Explicit vs Implicit Definitions

Industry	Regulation	Key Section	Requirement	Details
Government, Military, Intelligence	NISPOM (U.S.)	32 CFR, Part 117 Source: 32 CFR Part 117, NISPOM	"Physical or logical separation from unclassified networks..."	Directly **mandates** isolation for classified systems, often air-gapped.
Energy and Utilities	NERC CIP (U.S.)	CIP-005-7, R1 & R2 Source: NERC CIP Standards, specifically CIP-005-7	"Deny all traffic not explicitly allowed within an ESP..."	**Implies** air-gapping by requiring strict isolation of critical energy assets.
Industrial Manufacturing	IEC 62443 (Global)	SR 1.1, SR 1.2, SR 7.1 Source: IEC 62443 Series, particularly IEC 62443-3-3	"Segment networks and protect boundaries..."	**Implies** air-gapping for OT systems to restrict communication between zones.
Financial Services	PCI DSS (U.S.)	Requirement 1.1, 1.2, 1.3 Source: PCI DSS v4.0	"Network access to and from the cardholder data environment is restricted..."	**Implies** air-gapping as a method to isolate cardholder data environments.
Healthcare	HIPAA (U.S.)	§ 164.310, § 164.312(a)(1), (e)(1)	"Limit access, guard against unauthorized transmission..."	**Implies** air-gapping by requiring ePHI protection; common for sensitive systems

Appendix A – On-Premise ZTP
Getting the JSON file with device details

The JSON file can be extracted from the .zip chassis file which can be downloaded from PnP Connect portal.

tar -xvf serialFile.viptela.tar
x ***viptela_serial_file***
x viptela_serial_file.sig
x cisco_cert.cer

Sample serial_file JSON file:

```
{
"version": "1.1",
"organization": "vIPtela Inc Regression",
"overlay": "vIPtela Inc Regression",
"root_cert_bundle":"-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----",
"controller_details": {
"primary_ipv4":"10.0.12.26",
"primary_port":"12346"
},
"chassis_list": [{
"chassis": "JAE21491ABC",
"SKU": "ASR1002-HX",
"HWPID": "ASR1002-HX",
"serial_list": [{
"sudi_subject_serial": "JAE21491ABC",
"sudi_cert_serial": "021C1ABC",
"HWPID": "ASR1002-HX"}]
}
],
"timestamp": "2019-10-21 23:40:02.248"
}
```

Appendix A – On-Premise ZTP
Add cEdge device information

- Use the following command to load the JSON file onto the ZTP server
  Validator# **request device-upload chassis-file** *JSON-file-name*

- **Cert Sudi#** followed by **Subject Sudi#** is order of precedence for import at the ZTP server. This means that **Subject Sudi#** is imported for validation only when **Cert Sudi#** is not present in the JSON file.

NOTE: On-Prem ZTP for vEdges uses a CSV file for router chassis information.

Appendix A – On-Premise ZTP
Verify cEdge device information

Verify the list of router chassis numbers present on the on-Prem ZTP server, using one of the following commands:

```
Validator# show ztp entries

Validator# show orchestrator valid-devices
```