

Next-Generation Industrial SD-WAN

Secure, Scalable and Satellite-Ready Networking

Cameron Dry
Solutions Engineer

CISCO Live !

Cisco Webex App

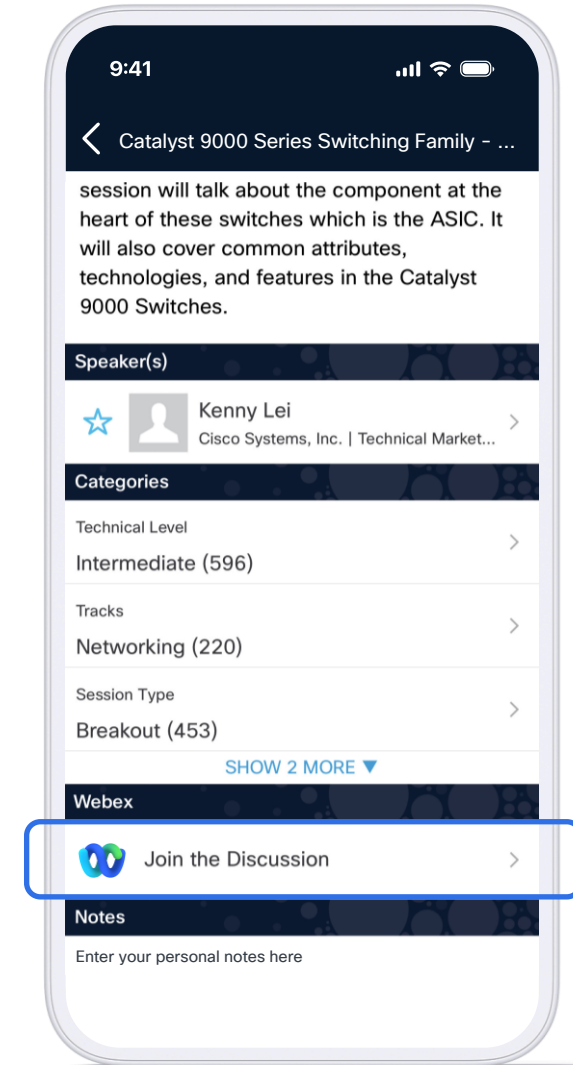
Questions?

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 14 November 2025.



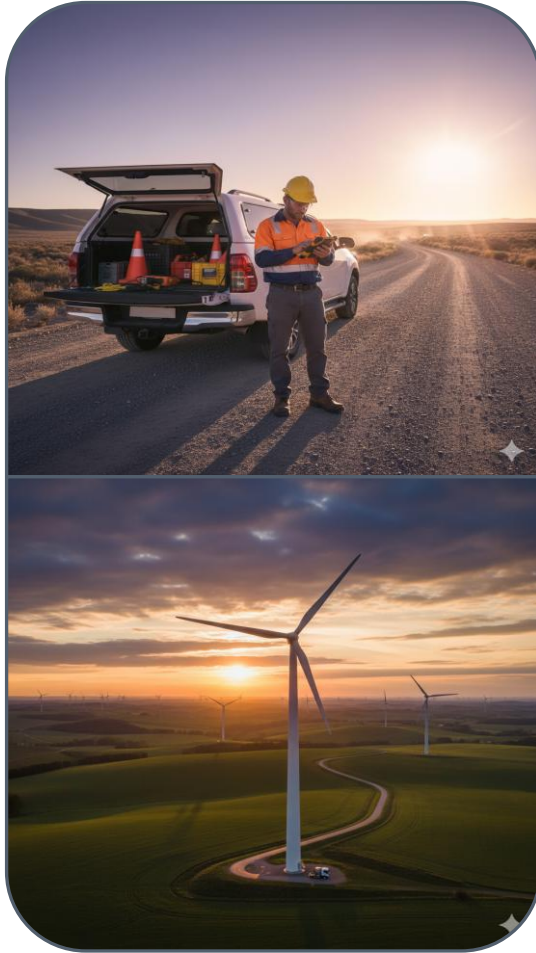
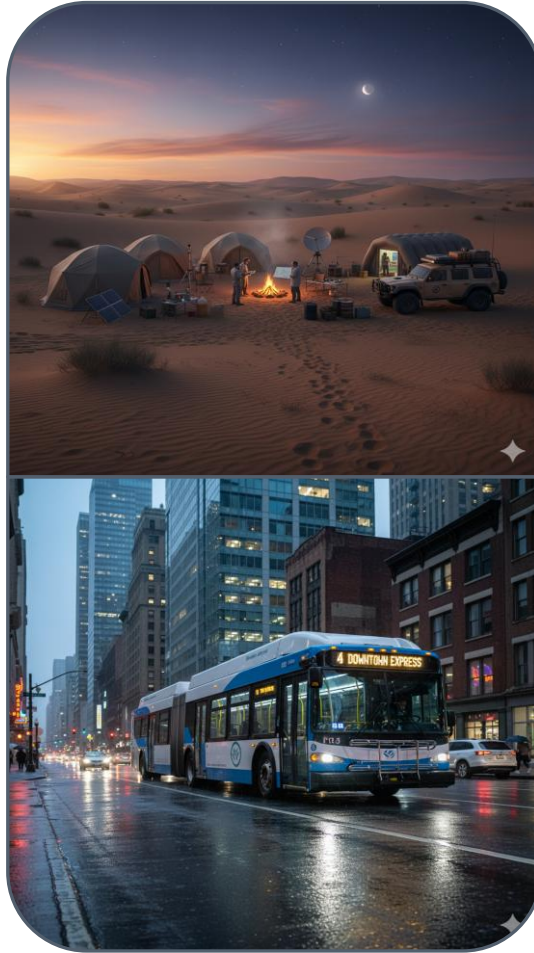
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2528>

Agenda

- 01 Industrial Requirements**
- 02 Industrial SD-WAN
Architecture Review**
- 03 Design Considerations for
Industrial SD-WAN**
 - On-premise Controllers
 - Streamlined Provisioning
 - Non-Terrestrial and Cellular Deployments
 - Edge Intelligence
- 04 Additional Information**

Industrial Requirements

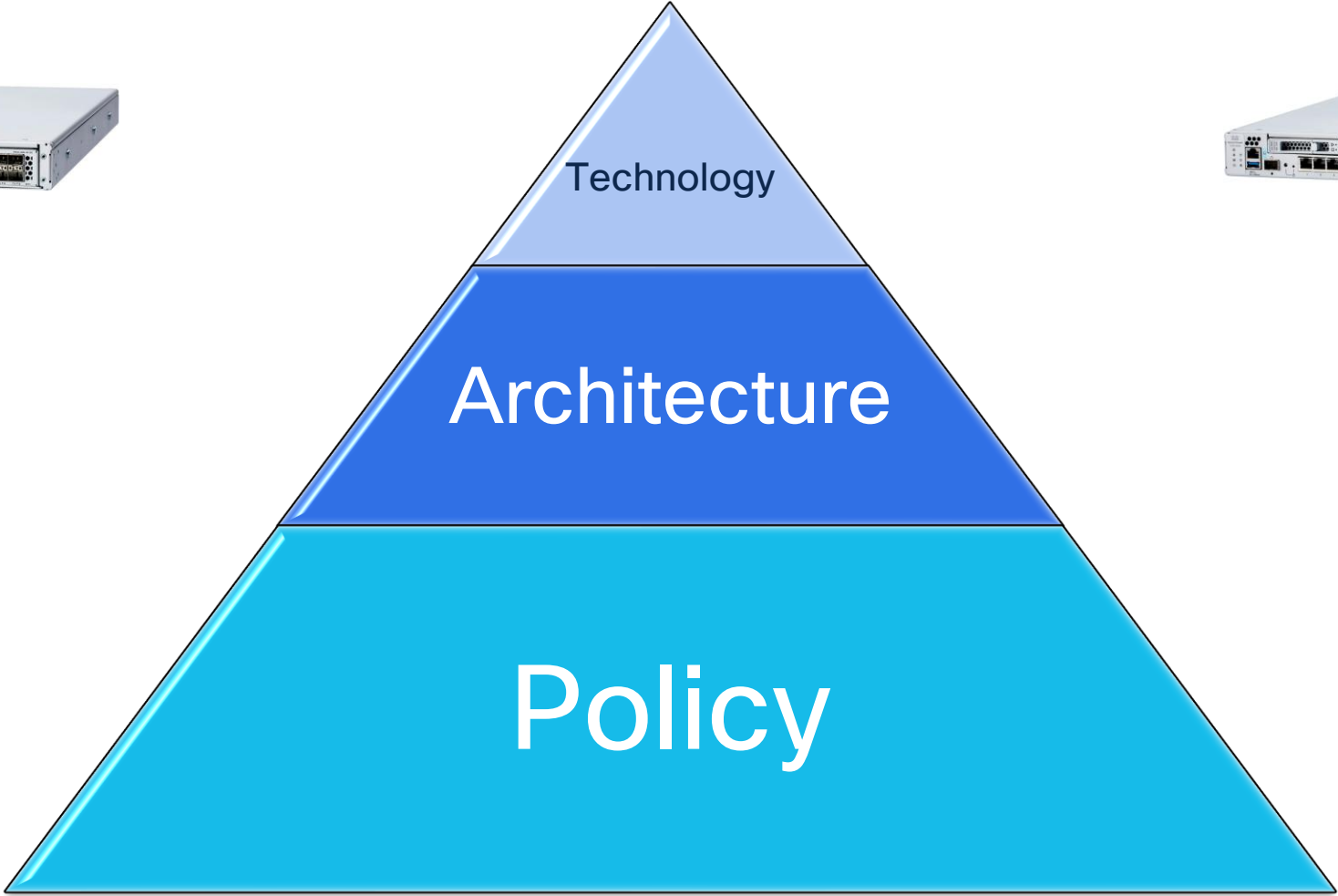
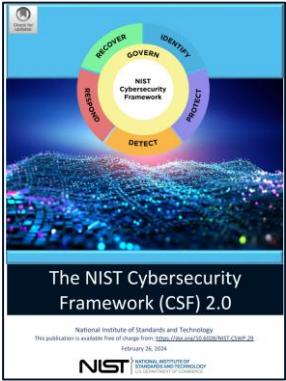
Business goals – any use case, any location, any technology



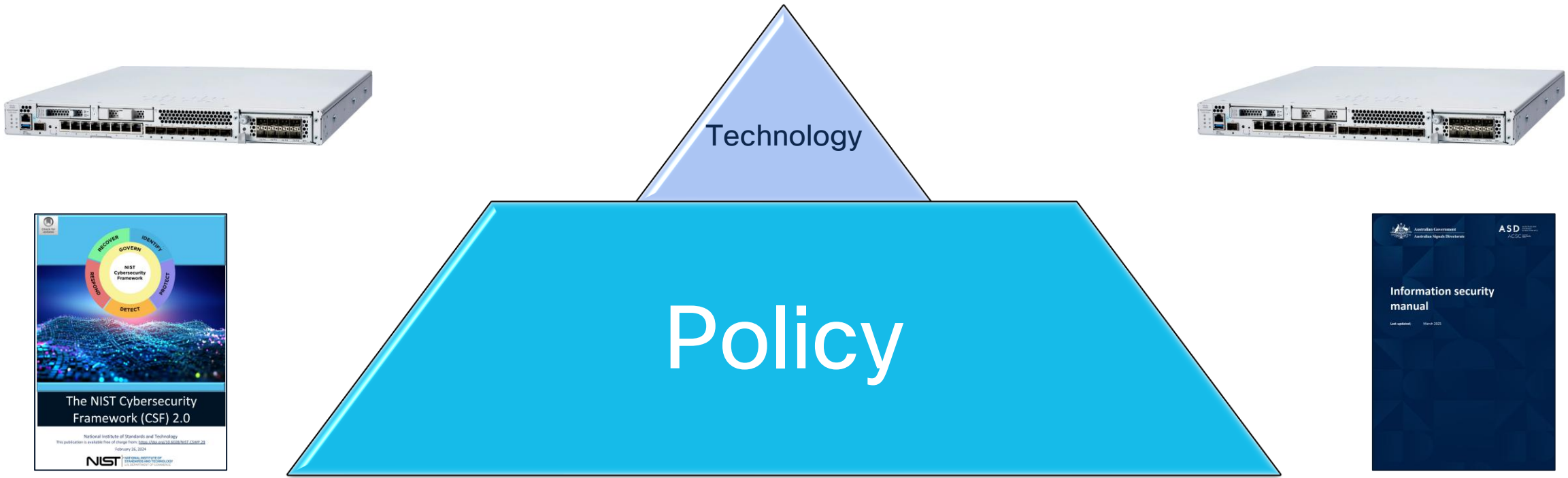
Network operator goals – single architecture that is...



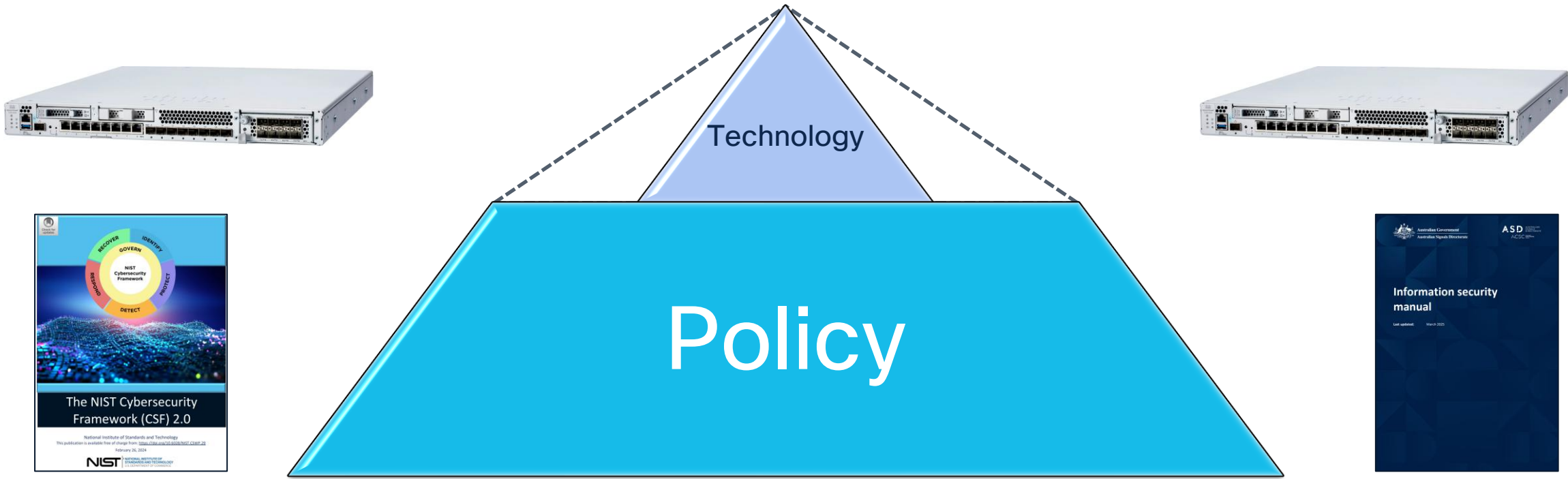
The importance of architecture in security



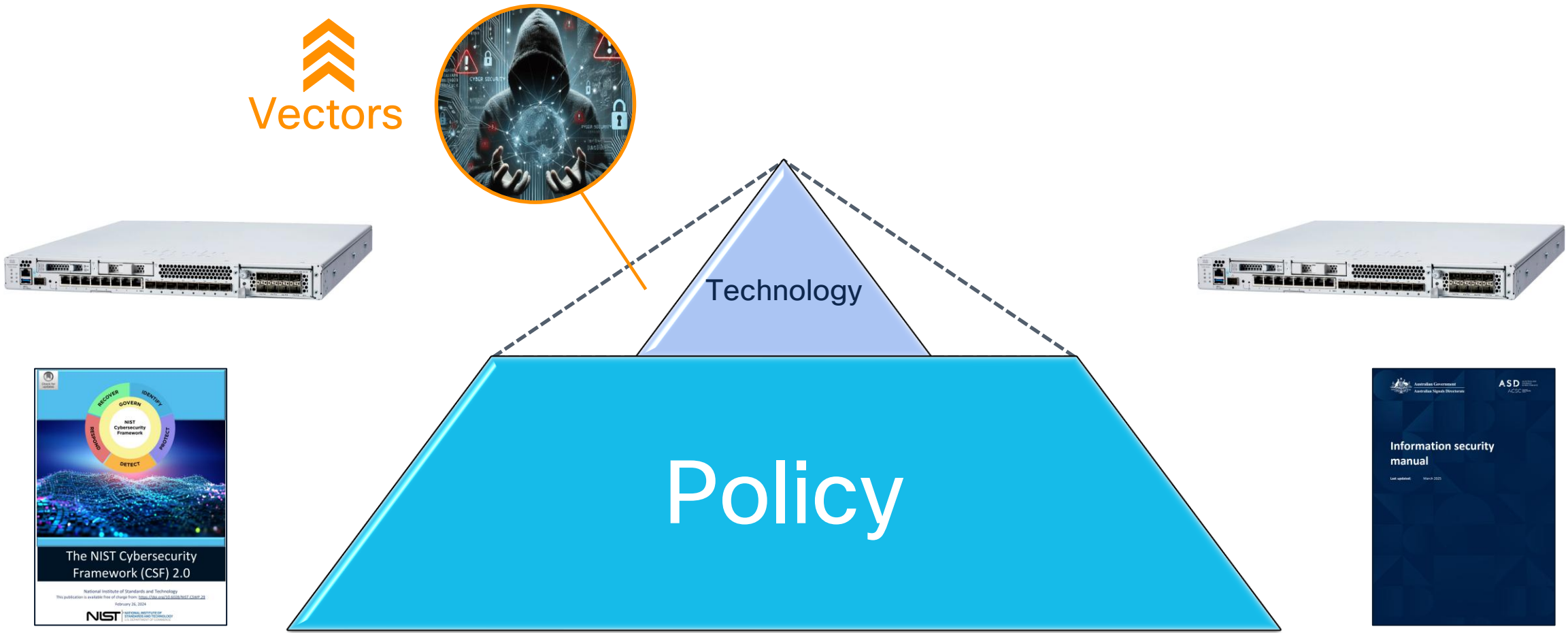
The importance of architecture in security



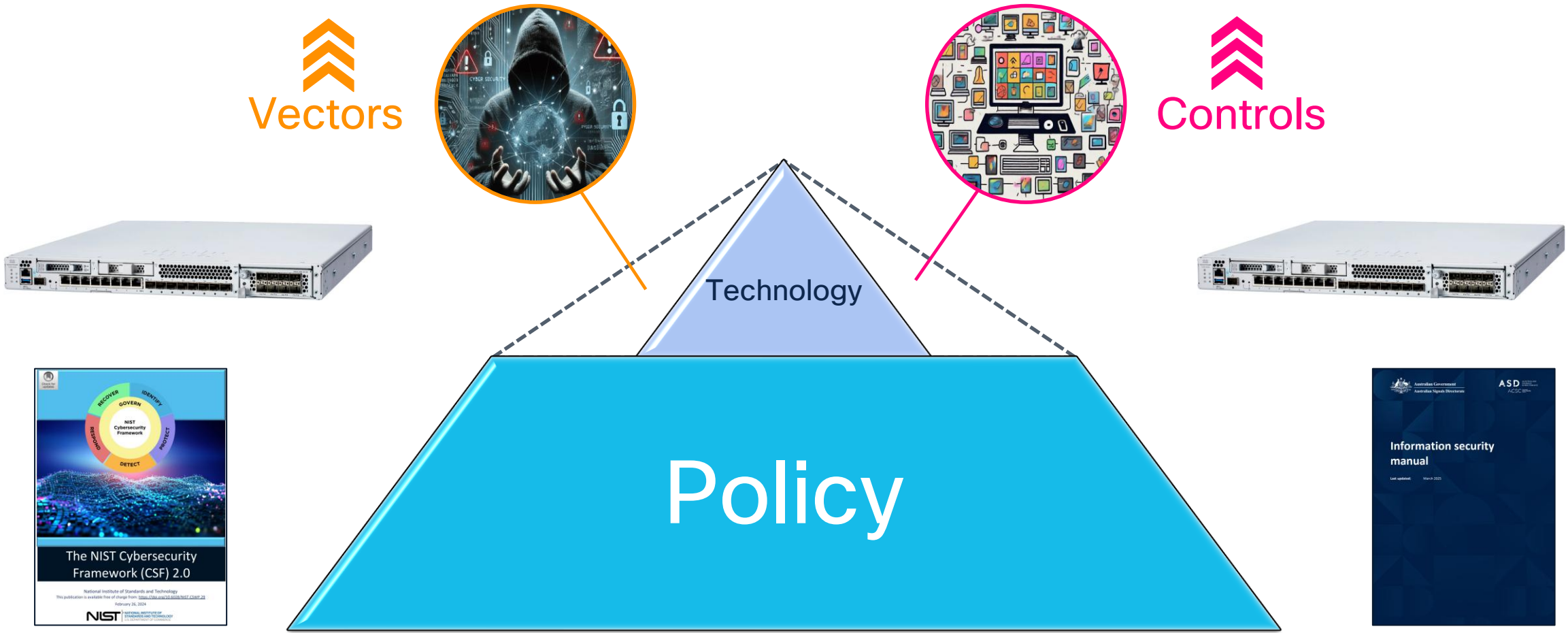
The importance of architecture in security



The importance of architecture in security



The importance of architecture in security



Cisco SD-WAN secure architecture delivers...



Zero Trust Access:
User *and* Network



Network
Segmentation



Data Privacy
and Integrity

Secure Software Defined WAN

Industrial SD-WAN Architecture Review

Cisco Catalyst SD-WAN Solution Components

Orchestration Plane



Validator

Management Plane



Manager

Control Plane

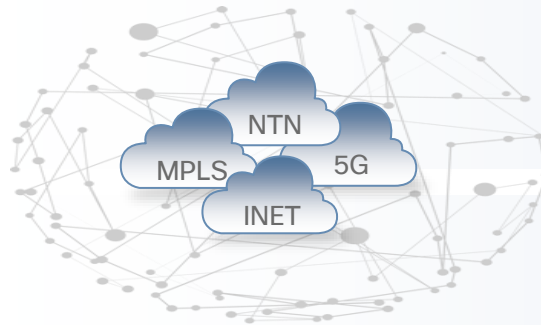
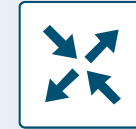


Controller

Cloud



On-premise

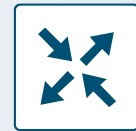


Router



Router

Data Plane



Router



IR8140H



IR1101



IR1800



IR8340



8000v

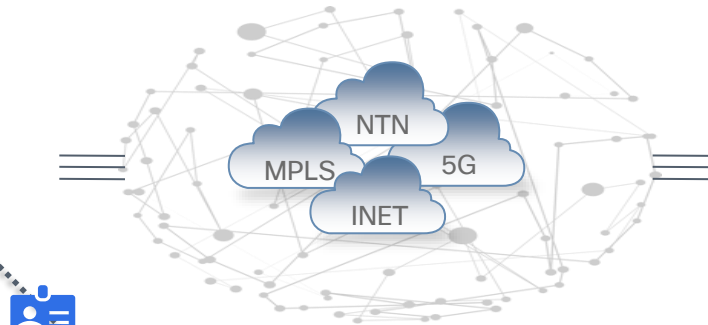
Zero Trust Network Fabric

Remote
Users

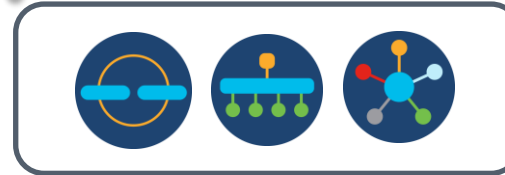
Public/Private
Cloud, SaaS



WAN
Edge



WAN
Edge



IdP



OT



IT

Orchestration, Management and Control Plane

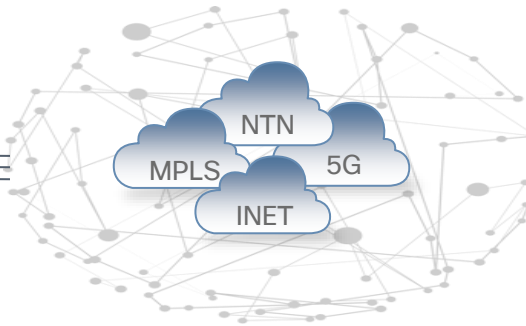
Zero Trust Network Fabric

Remote
Users

Public/Private
Cloud, SaaS



WAN
Edge



WAN
Edge



Orchestration, Management and Control Plane



IdP



OT

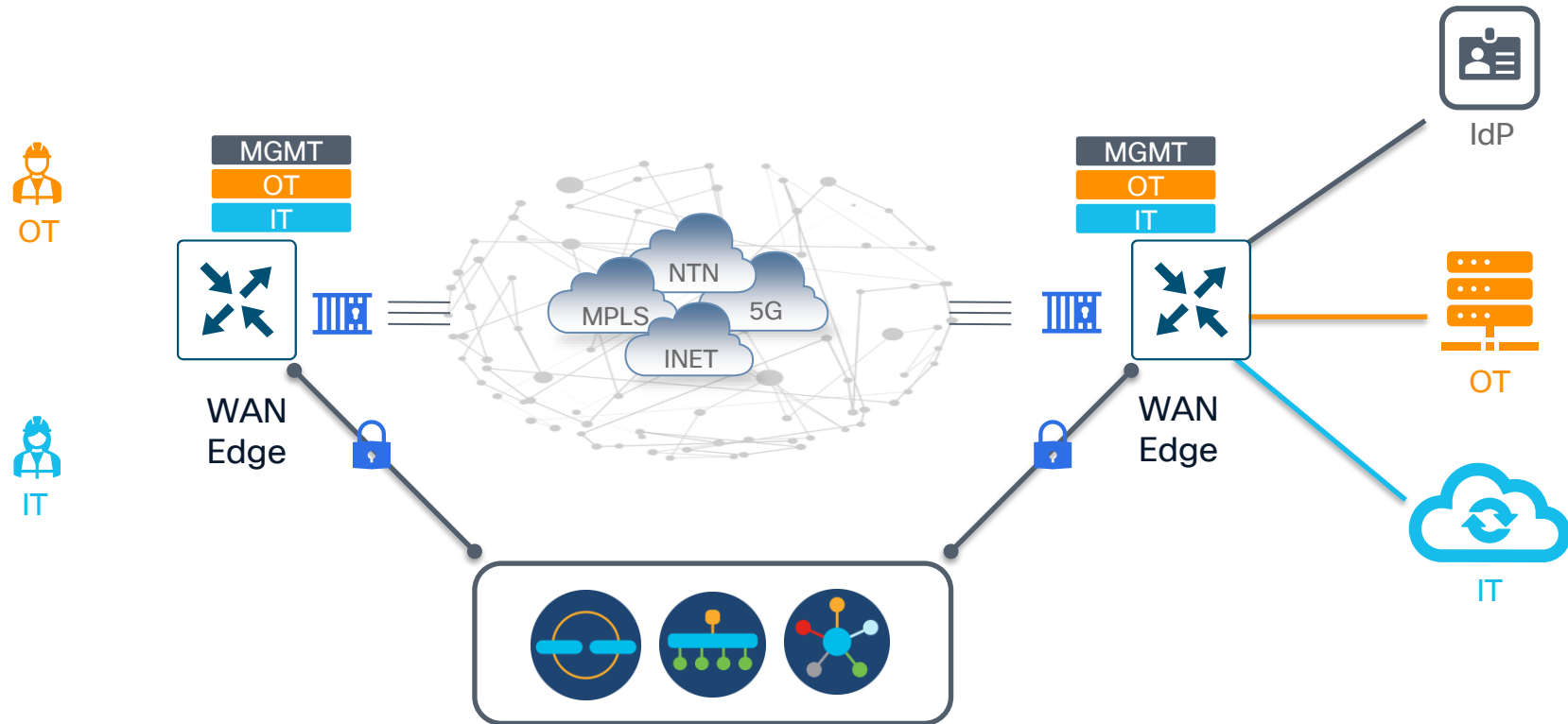


IT

Network Segmentation

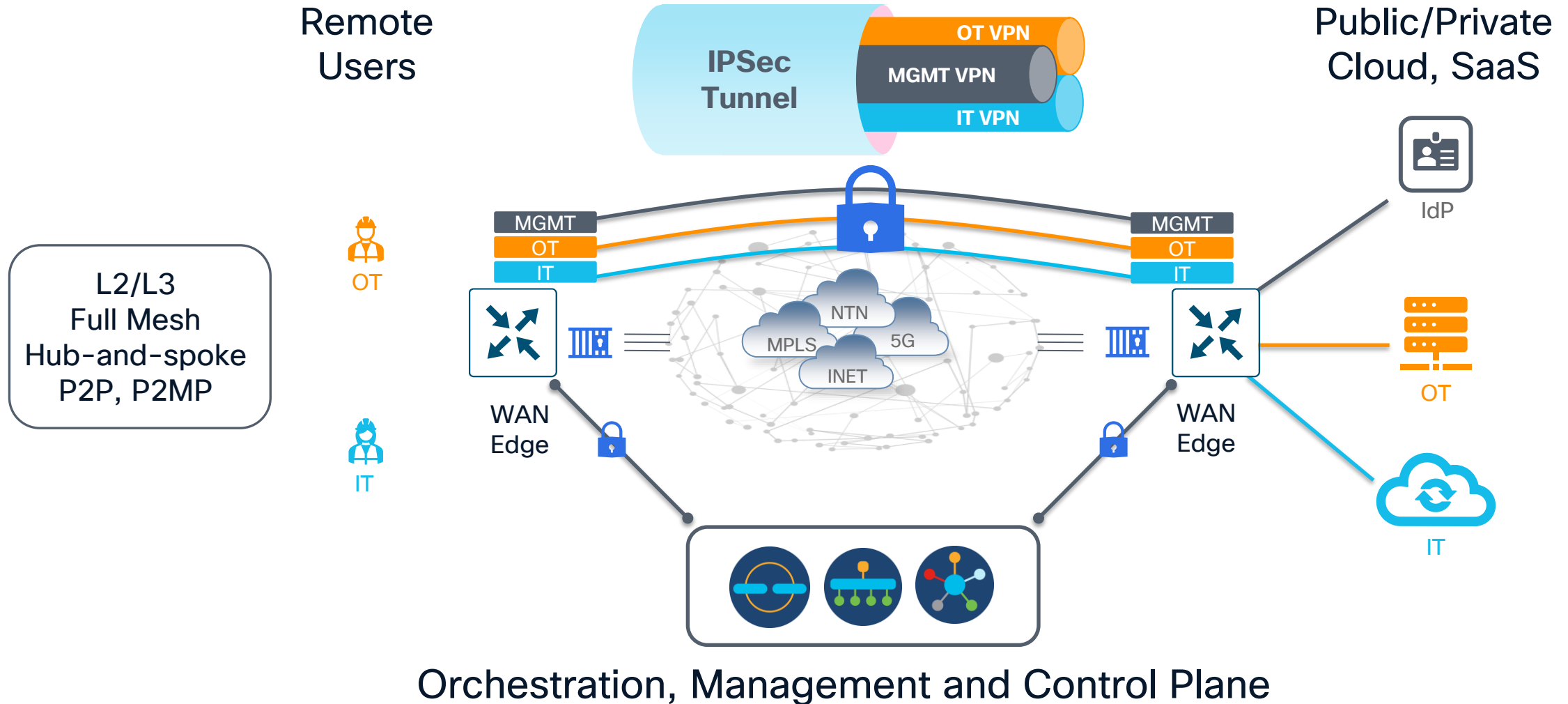
Remote
Users

Public/Private
Cloud, SaaS

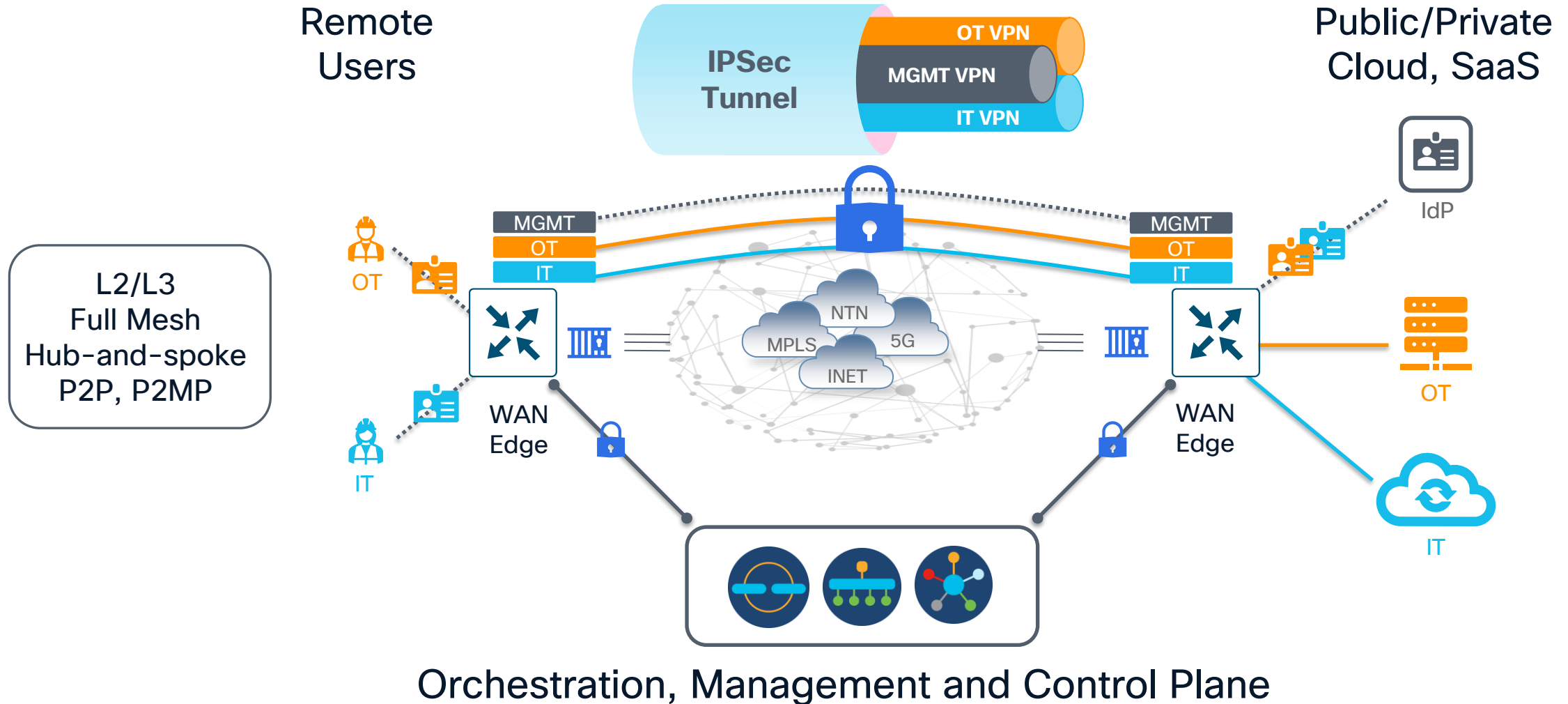


Orchestration, Management and Control Plane

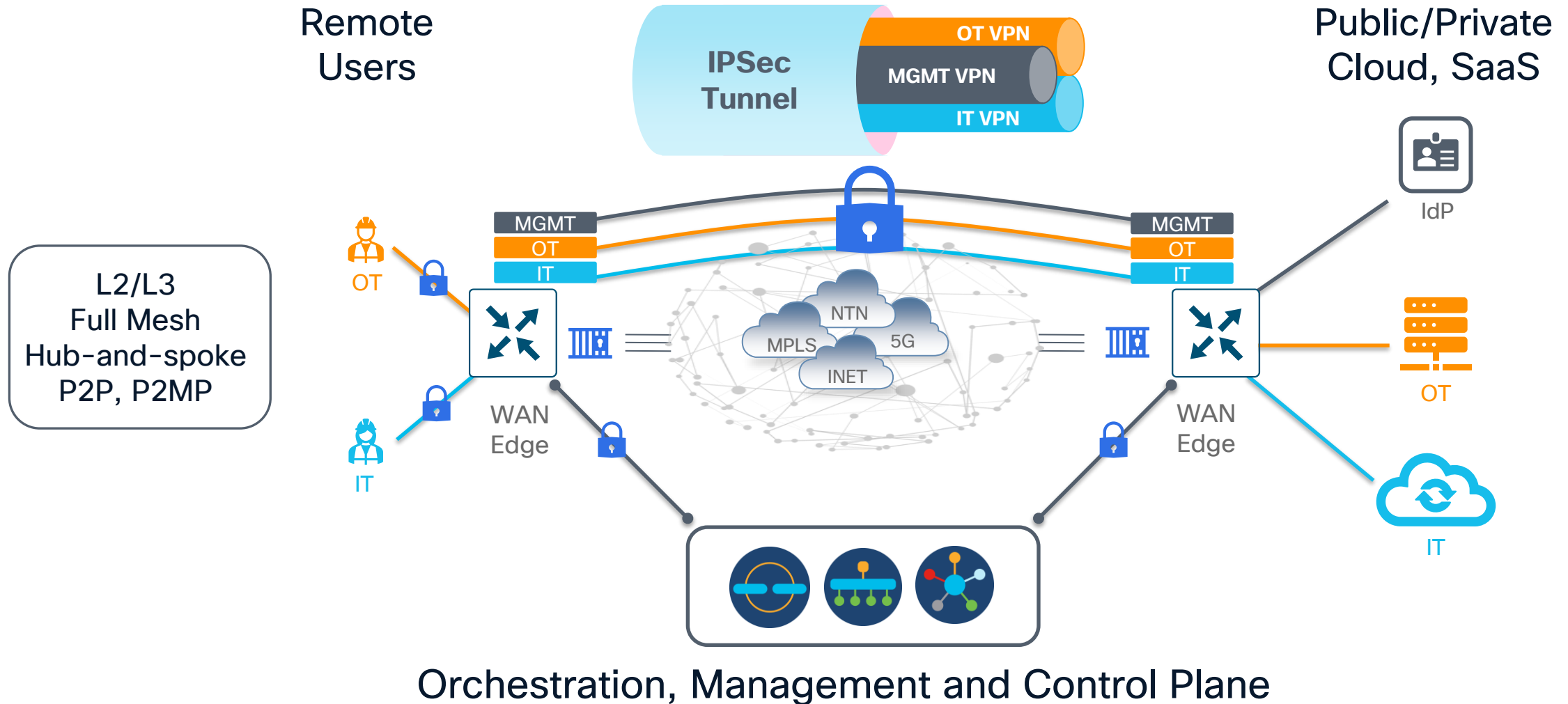
Data Privacy and Integrity



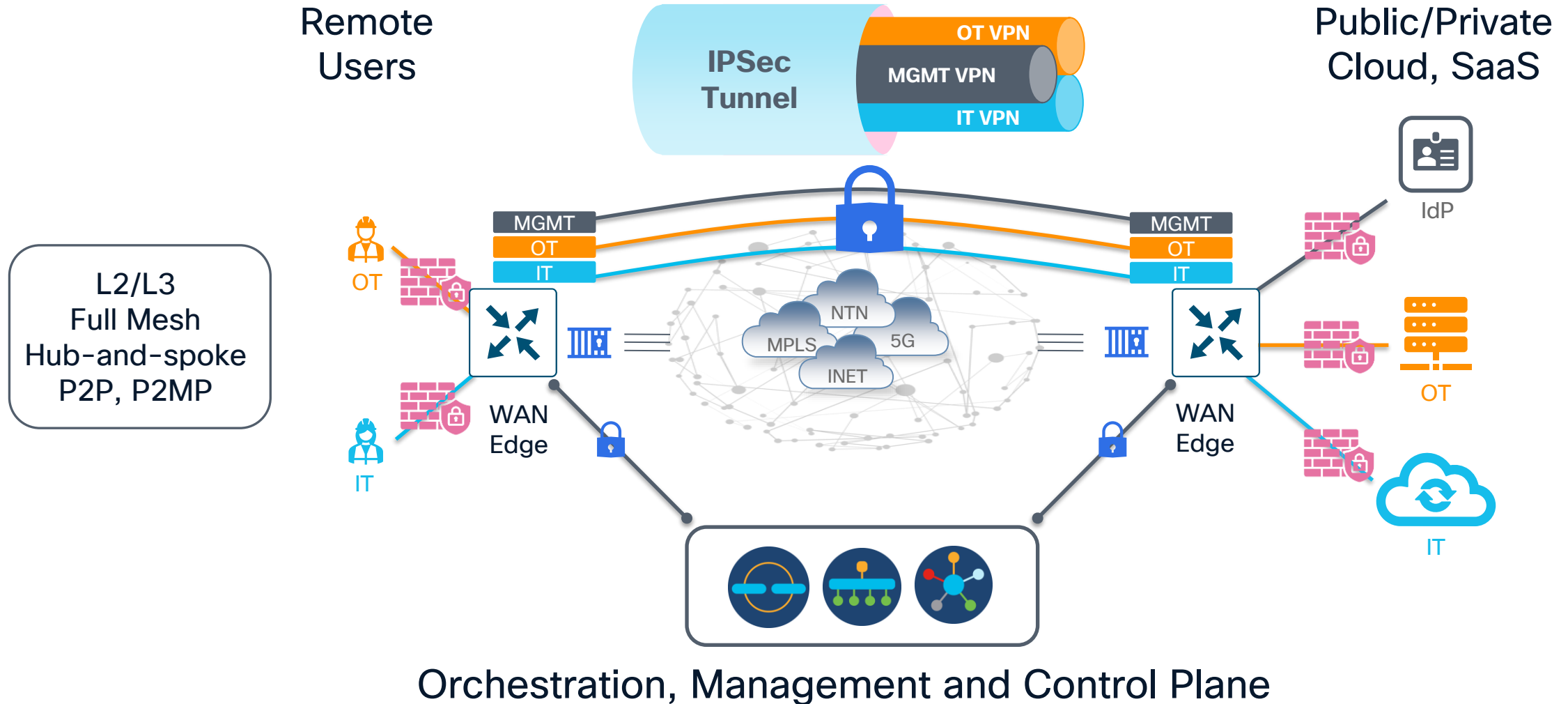
Zero Trust User Access



User Segmentation



Technology Application - Security



Industrial Routers with Next-Gen Firewall (NGFW)



IR1101, IR1833

IR1835

IR8340



Application Firewall
>5000 layer 7 apps classified (1500 on box)



Network Segmentation
Virtual Isolation between network segments



DoS Protection
Protection against denial-of-service attacks



URL Policies
Custom Domains only



Secure Internet Gateway / SSE
DNS / Web Security with Cisco Umbrella



TrustSec
SGT Enforcement across the firewall

+



Snort IDS/IPS
Most widely deployed IPS engine in the world



URL Filtering
Custom Domains & Web Reputation Score



Advanced Malware Protection
File Reputation & Sandboxing

+



SSL Decryption
Detect Threats in Encrypted Traffic



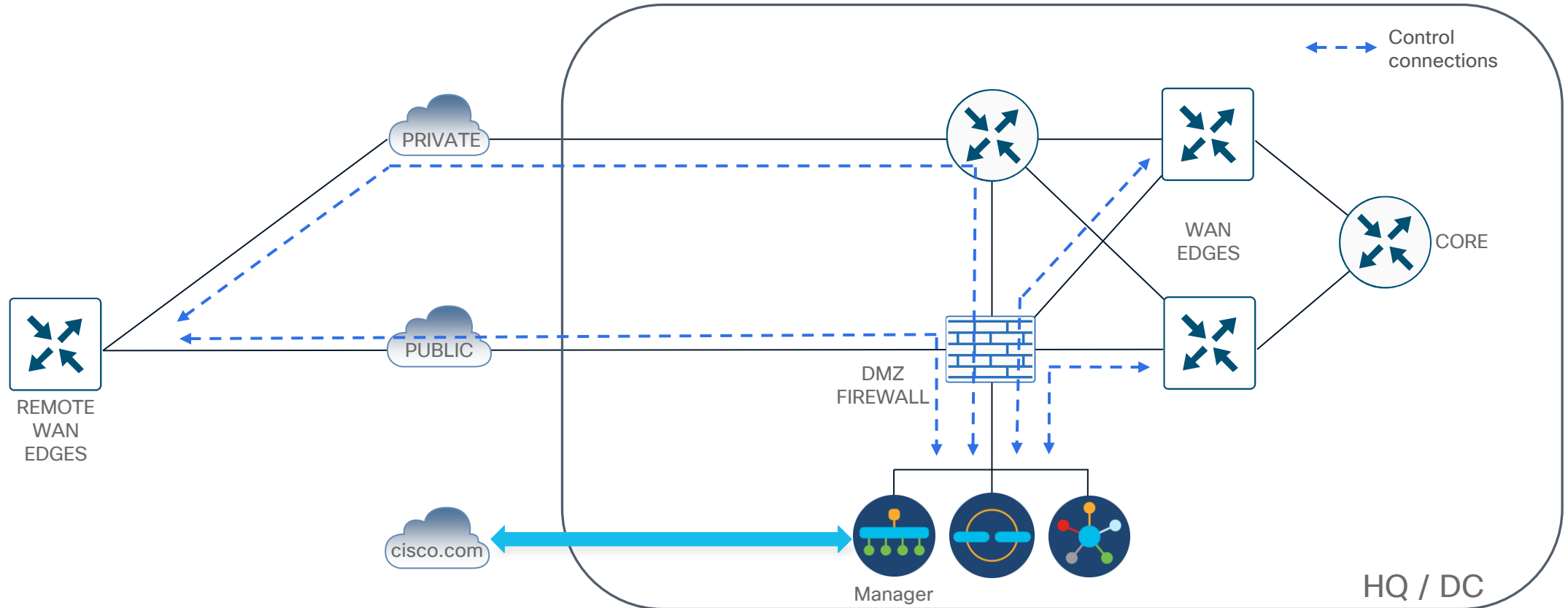
Full TrustSec Support
SGT Enforcement across switch ports

Design Considerations for Industrial SD-WAN

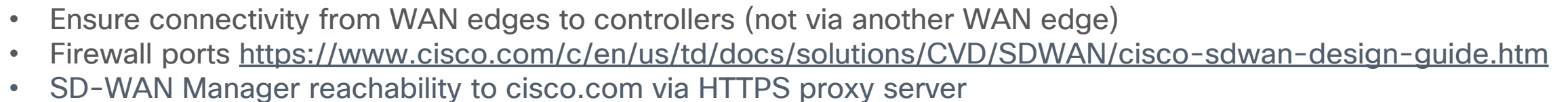
On-premise Controllers



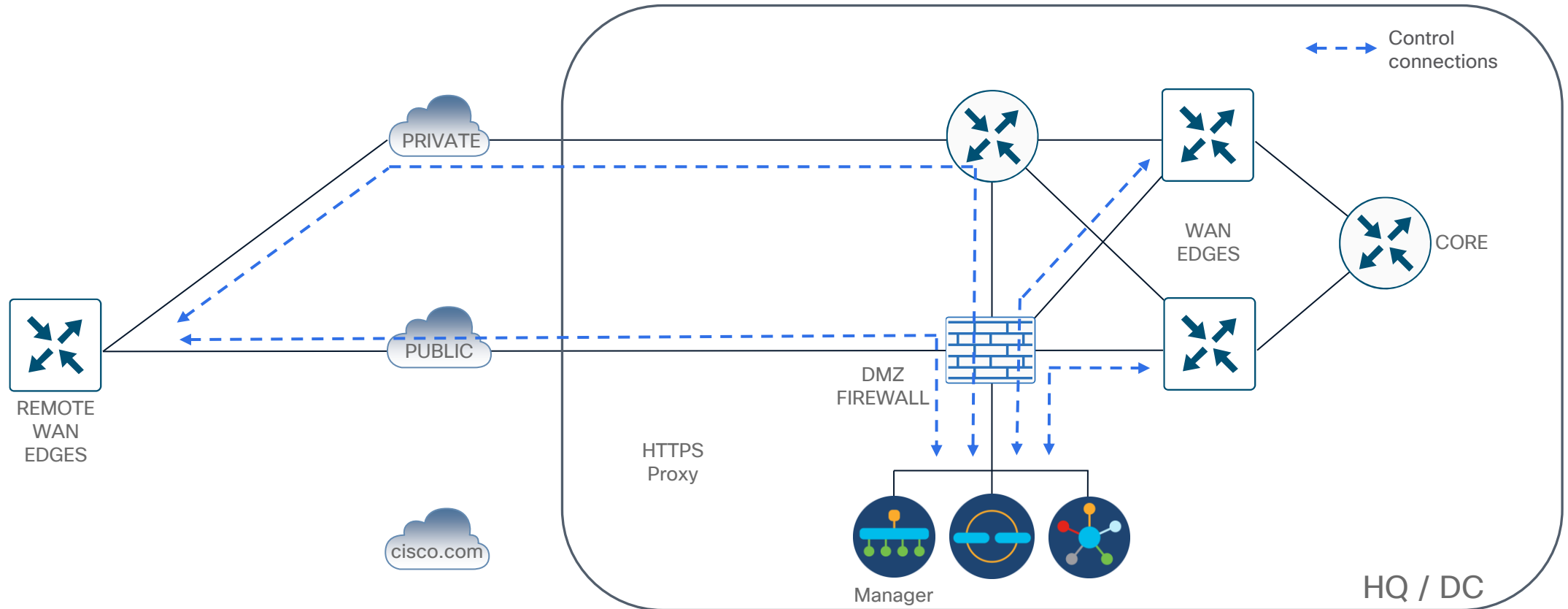
On-Premise Controllers - Full Connectivity



- Ensure connectivity from WAN edges to controllers (not via another WAN edge)
- Firewall ports <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.htm>
- SD-WAN Manager direct reachability to cisco.com via DMZ firewall

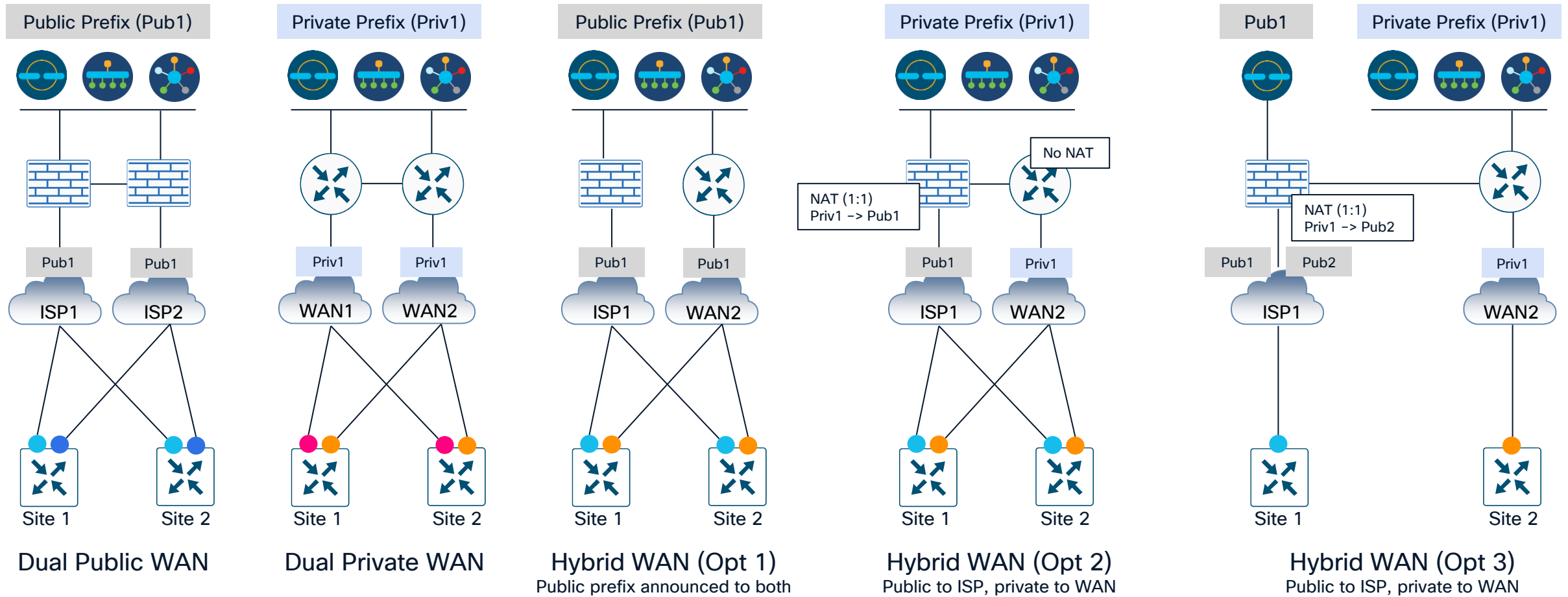


On-Premise Controllers - Full Air Gap



- Ensure connectivity from WAN edges to controllers (not via another WAN edge)
- Firewall ports <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.htm>
- No SD-WAN Manager reachability to cisco.com - offline updates only

On-Premise Controllers - Supported Topologies



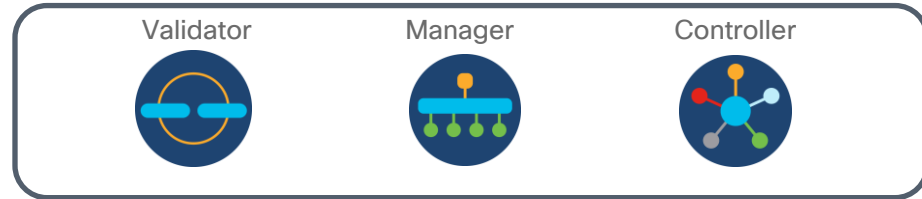
Comparison of Deployment Types Partial Air Gap to Full Air Gap

Feature	Partial Air Gap	Full Air Gap
Cisco SD-WAN Analytics	Yes	No
Cisco Smart Software Manager (CSSM) for Licensing	Yes	Partial with on-premise CSSM
Smart Account Management – Cisco PKI Certificate Management TAC Case integration PNP Connect device sync	Yes	No
Cisco Catalyst SD-WAN Portal – Configuration Catalog and Migration Assistant Advisory features – EoX, PSIRT, Field notices and reports	Yes	No
Software image repository	Yes	Manual
IPS Signature automatic updates	Yes	Manual
Interactive Helper & Online Documentation	Yes	No
Multifactor authentication	Yes	No
ThousandEyes WAN Insights / Predictive Path / SaaS telemetry	Yes	No

Streamlined Provisioning

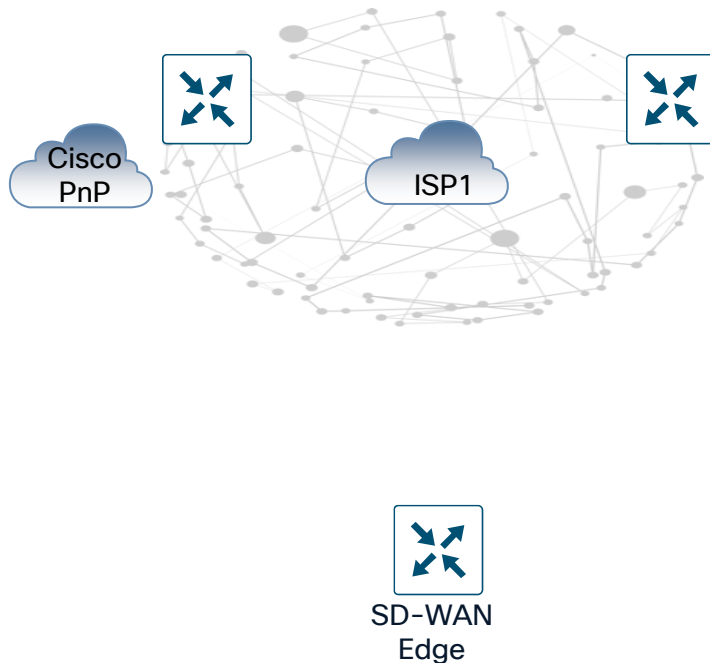


Streamlined Provisioning - Public Transport

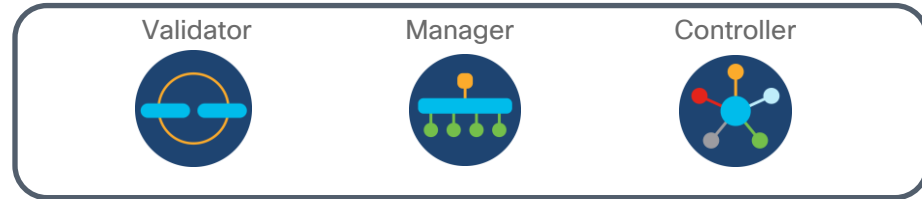


Scenario

1. SD-WAN edge router has access to PnP portal.



Streamlined Provisioning - Public Transport

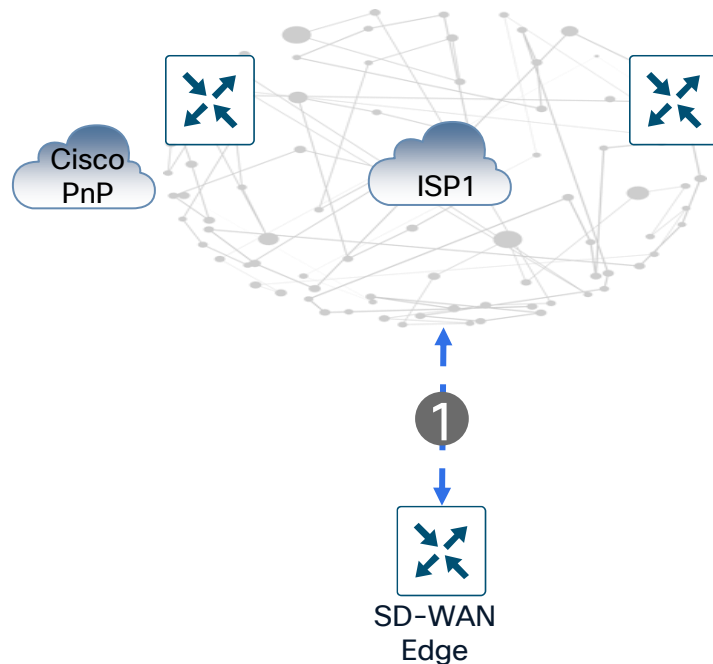


Scenario

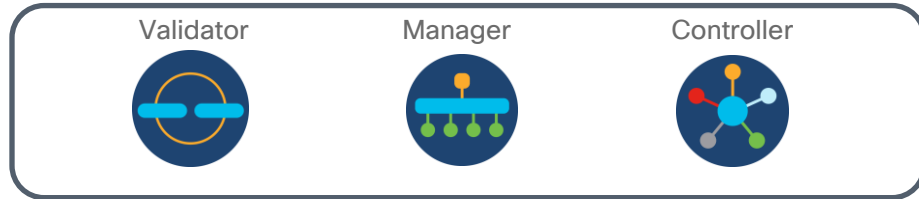
1. SD-WAN edge router has access to PnP portal.

Steps:

1. Router receives IP address from ISP via DHCP



Streamlined Provisioning - Public Transport

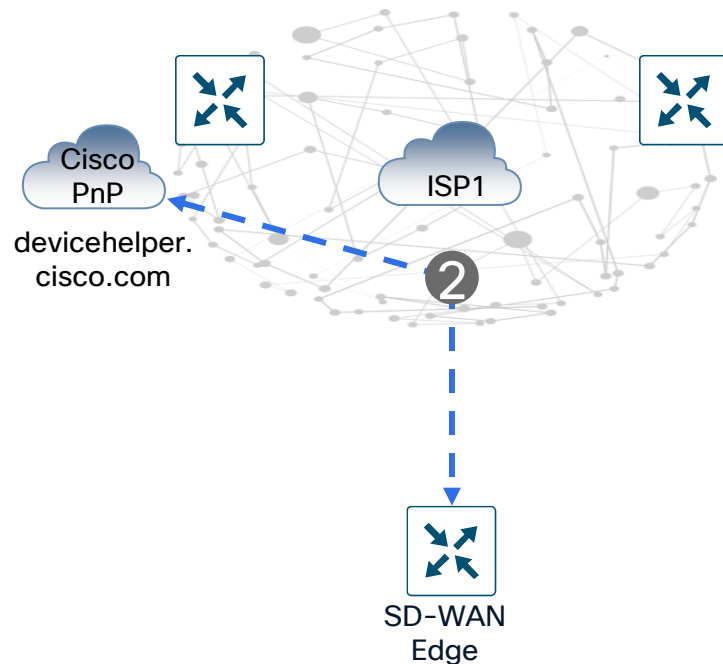


Scenario

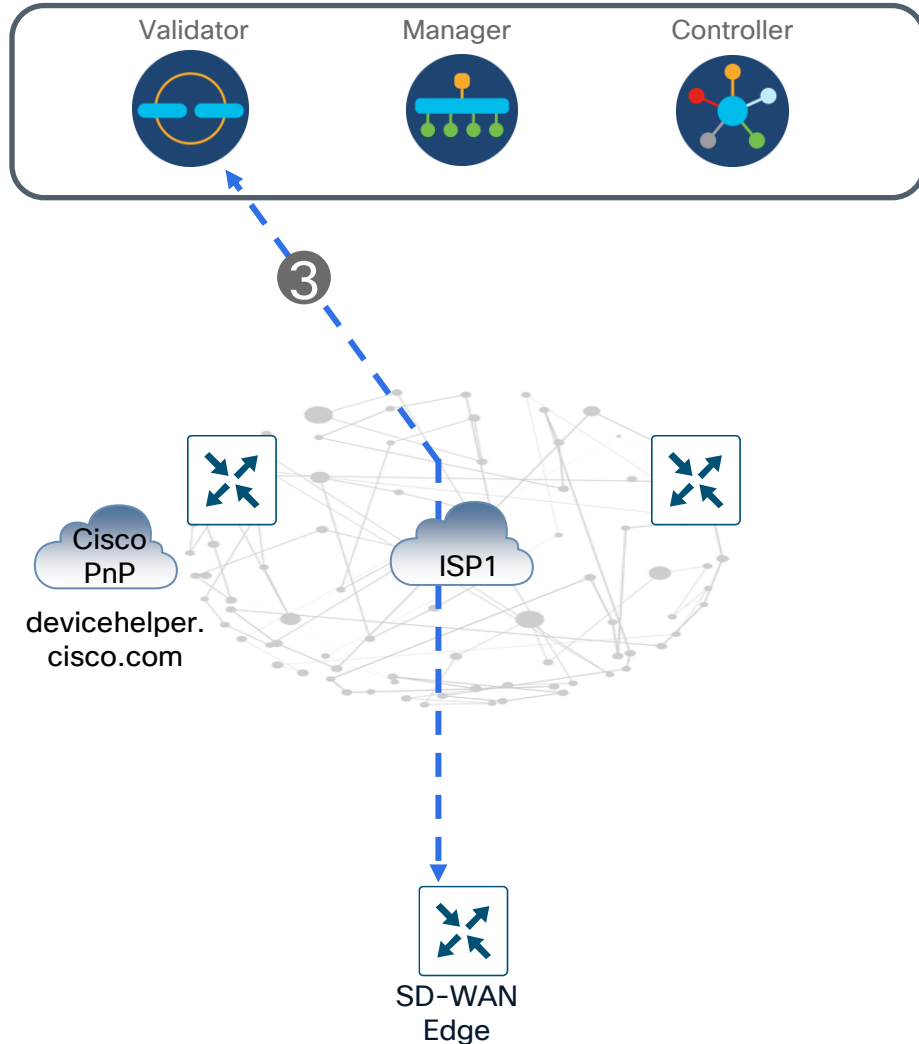
1. SD-WAN edge router has access to PnP portal.

Steps:

1. Router receives IP address from ISP via DHCP
2. Router authenticates to Cisco PnP portal and receives DNS hostname of Validator



Streamlined Provisioning - Public Transport



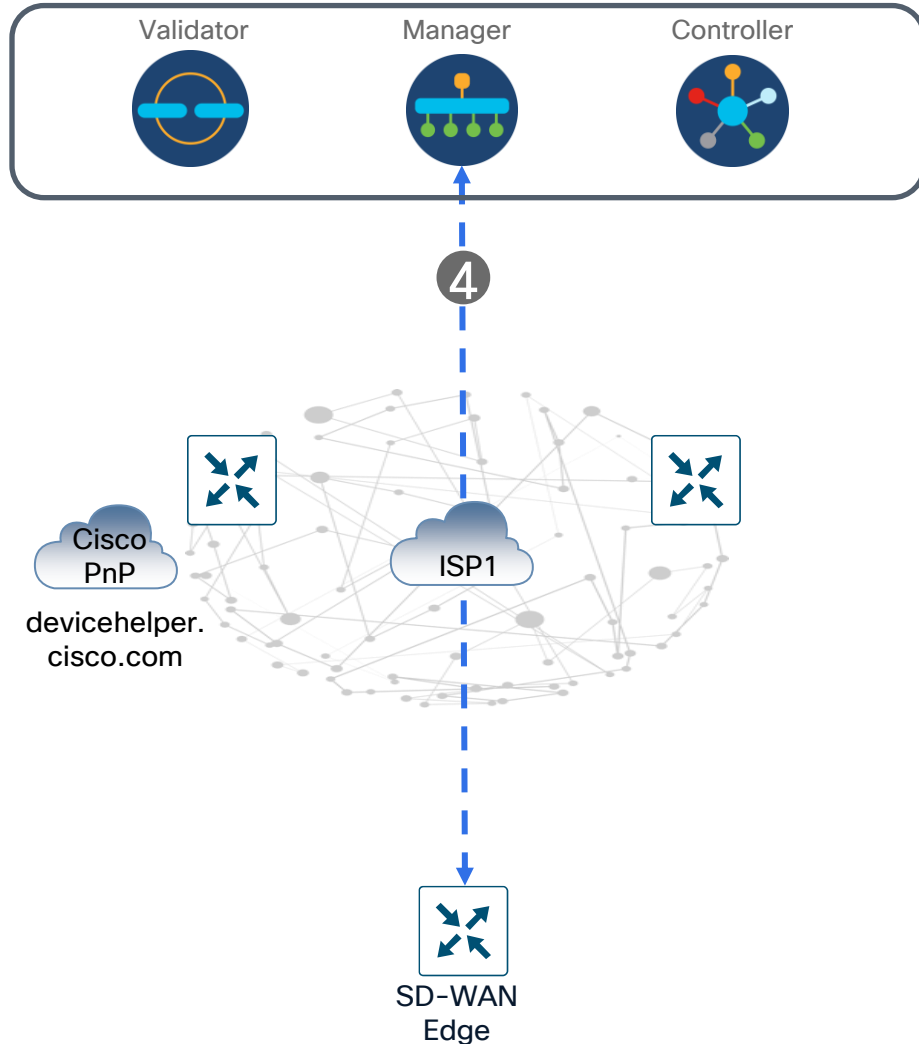
Scenario

1. SD-WAN edge router has access to PnP portal.

Steps:

1. Router receives IP address from ISP via DHCP
2. Router authenticates to Cisco PnP portal and receives DNS hostname of Validator
3. Router authenticates with Validator and receives Manager and Controller information

Streamlined Provisioning - Public Transport



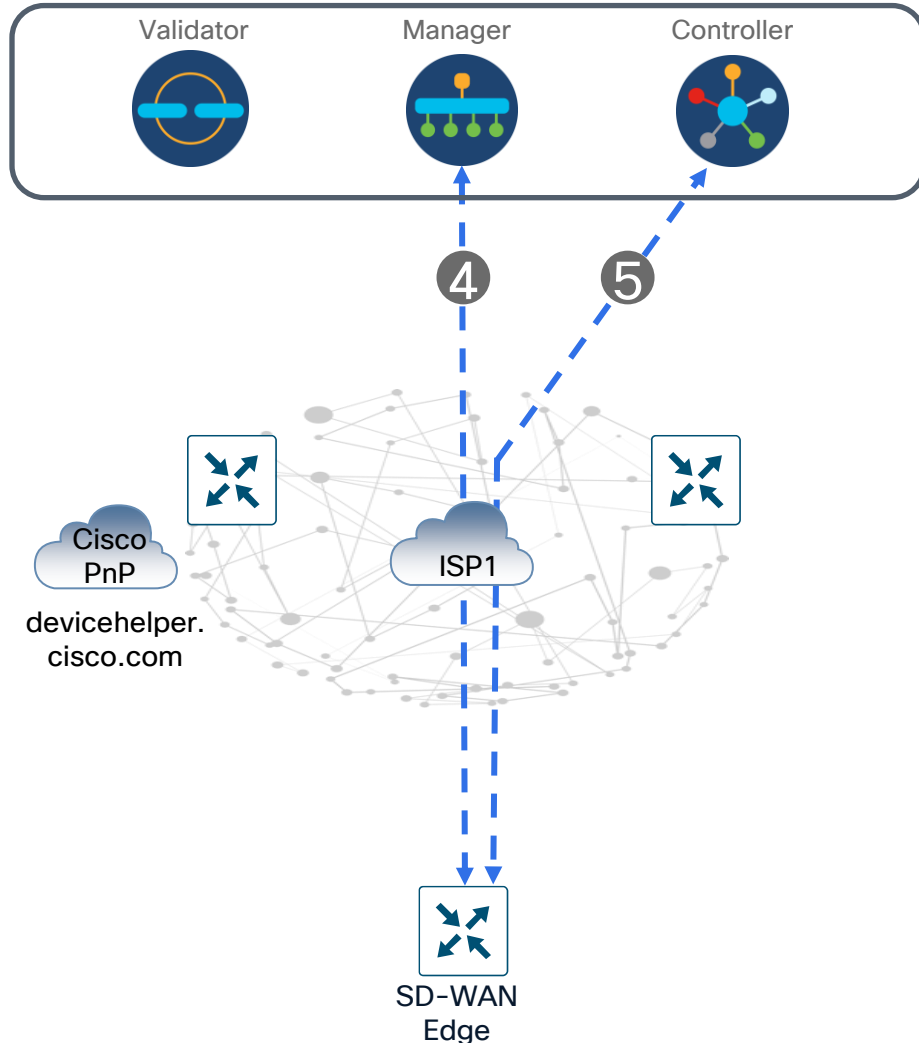
Scenario

1. SD-WAN edge router has access to PnP portal.

Steps:

1. Router receives IP address from ISP via DHCP
2. Router authenticates to Cisco PnP portal and receives DNS hostname of Validator
3. Router authenticates with Validator and receives Manager and Controller information
4. Router authenticates with Manager and receives running configuration

Streamlined Provisioning - Public Transport



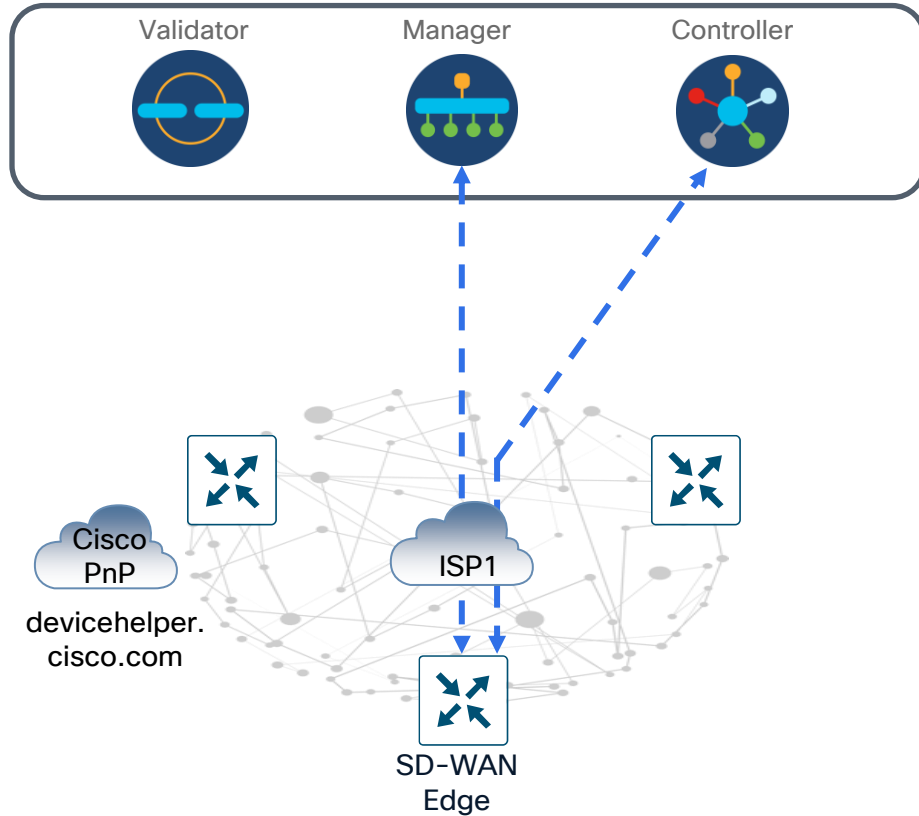
Scenario

1. SD-WAN edge router has access to PnP portal.

Steps:

1. Router receives IP address from ISP via DHCP
2. Router authenticates to Cisco PnP portal and receives DNS hostname of Validator
3. Router authenticates with Validator and receives Manager and Controller information
4. Router authenticates with Manager and receives running configuration
5. Router peers with Controller and establishes data plane

Streamlined Provisioning - Public Transport



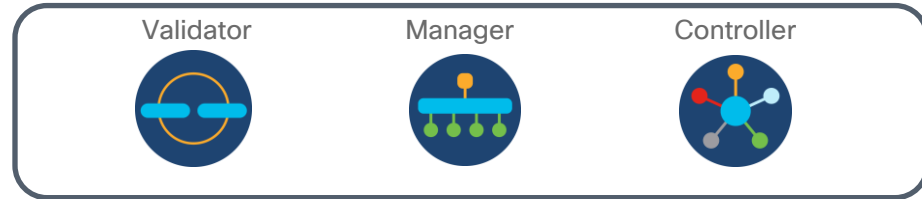
Scenario

1. SD-WAN edge router has access to PnP portal.

Steps:

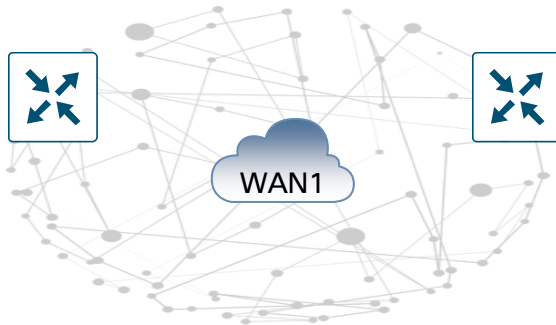
1. Router receives IP address from ISP via DHCP
2. Router authenticates to Cisco PnP portal and receives DNS hostname of Validator
3. Router authenticates with Validator and receives Manager and Controller information
4. Router authenticates with Manager and receives running configuration
5. Router peers with Controller and establishes data plane
6. Router participates in the SD-WAN fabric

Streamlined Provisioning - Private Transport

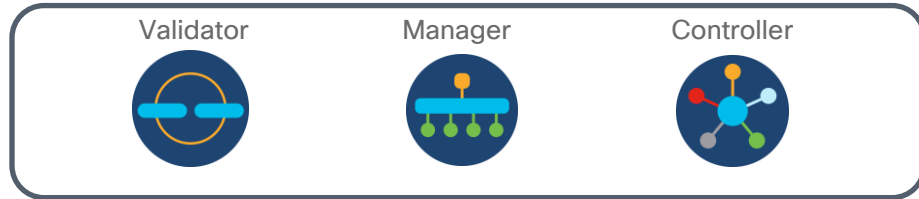


Scenario

1. SD-WAN edge router has no access to PnP portal:
 - a. Private network - MPLS, pLTE/5G
 - b. Address not received via DHCP
 - c. Interface preconfiguration required - subint, PPPoE, APN
 - d. Cyber policy



Streamlined Provisioning - Private Transport

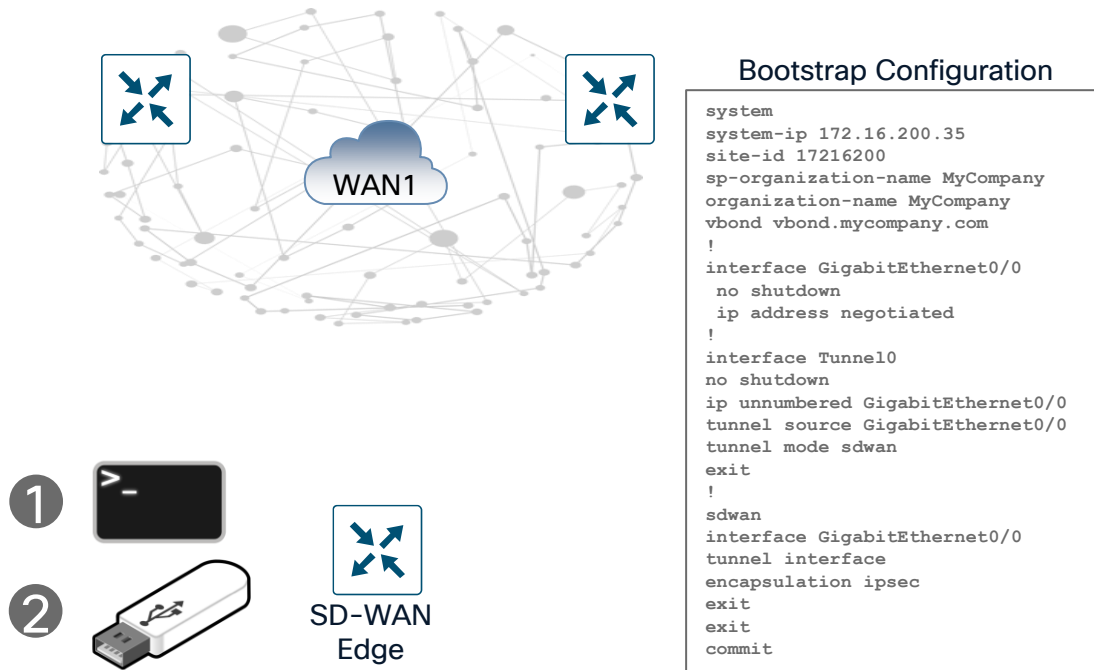


Scenario

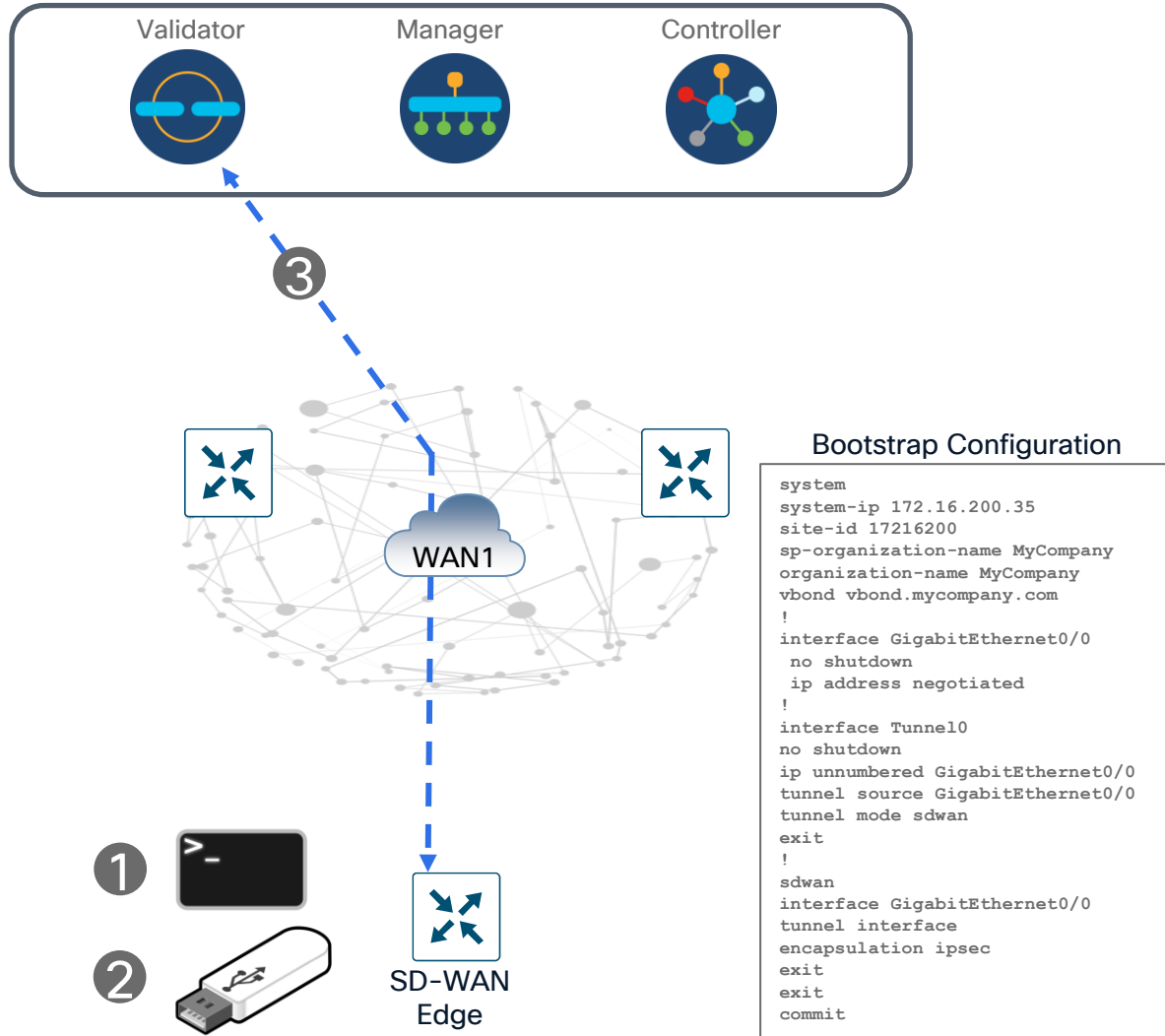
1. SD-WAN edge router has no access to PnP portal:
 - a. Private network - MPLS, pLTE/5G
 - b. Address not received via DHCP
 - c. Interface preconfiguration required - subint, PPPoE, APN
 - d. Cyber policy

Options

1. CLI Method:
 - a. Console into router and apply bootstrap config
 - b. Reboot of router will initiate steps 3 - 5
2. USB Method:
 - a. Format USB drive as FAT-32 and add *ciscosdwan.cfg* text file
 - b. Insert USB into router in factory default state and power up
 - c. Router will read USB drive, apply *ciscosdwan.cfg*, and initiate provisioning steps 3 - 5
 - d. USB drive is only read if router has no config - may be left in for DR



Streamlined Provisioning - Private Transport



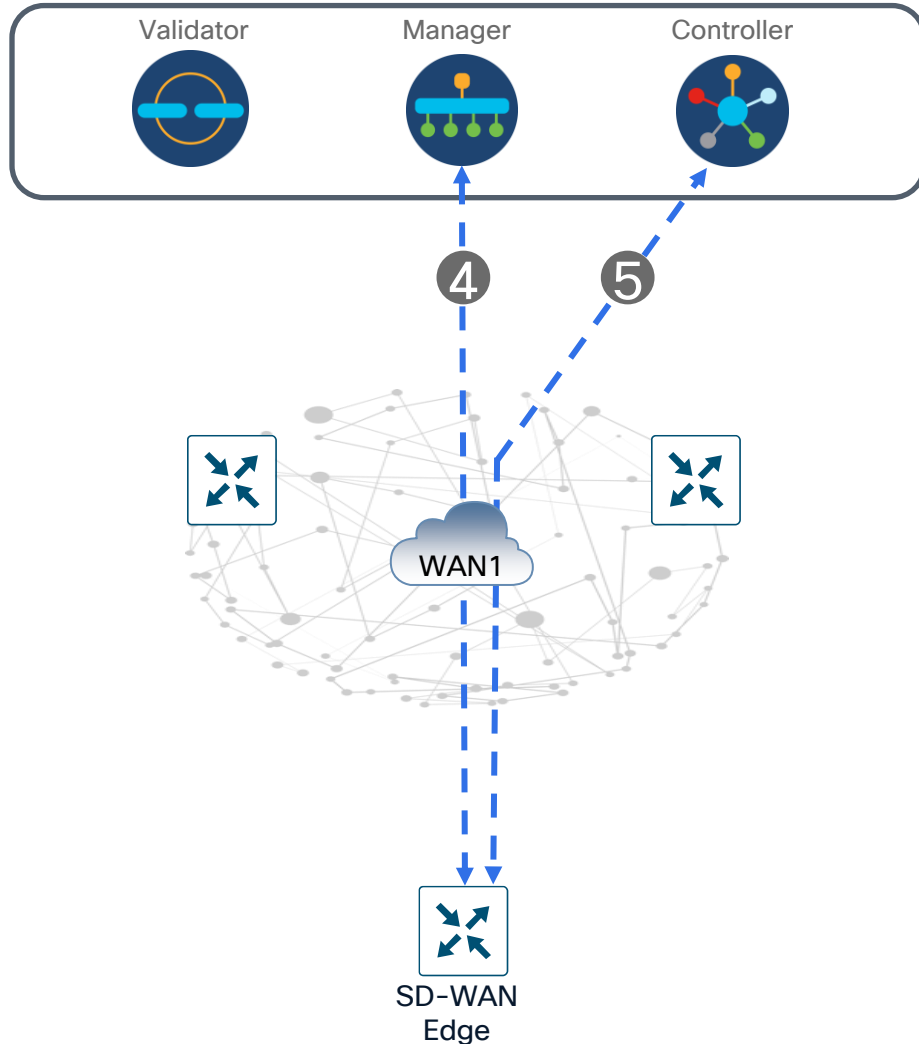
Scenario

1. SD-WAN edge router has no access to PnP portal:
 - a. Private network - MPLS, pLTE/5G
 - b. Address not received via DHCP
 - c. Interface preconfiguration required - subint, PPPoE, APN
 - d. Cyber policy

Options

1. CLI Method:
 - a. Console into router and apply bootstrap config
 - b. Reboot of router will initiate steps 3 - 5
2. USB Method:
 - a. Format USB drive as FAT-32 and add *ciscosdwan.cfg* text file
 - b. Insert USB into router in factory default state and power up
 - c. Router will read USB drive, apply *ciscosdwan.cfg*, and initiate provisioning steps 3 - 5
 - d. USB drive is only read if router has no config - may be left in for DR

Streamlined Provisioning - Private Transport



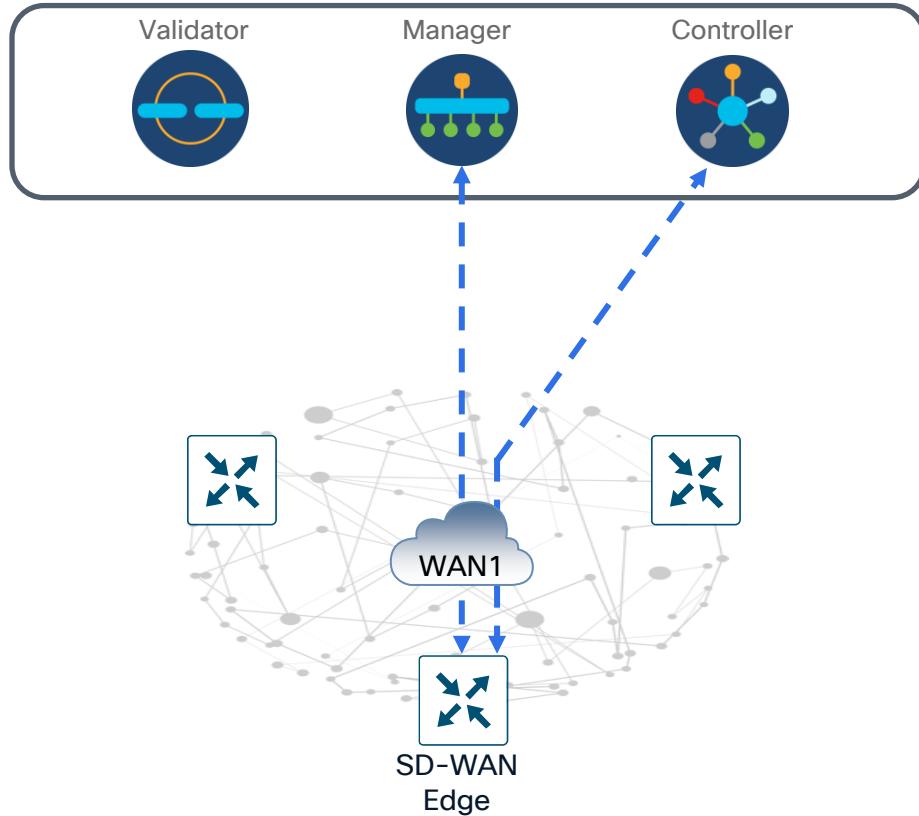
Scenario

1. SD-WAN edge router has no access to PnP portal:
 - a. Private network - MPLS, pLTE/5G
 - b. Address not received via DHCP
 - c. Interface preconfiguration required - subint, PPPoE, APN
 - d. Cyber policy

Options

1. CLI Method:
 - a. Console into router and apply bootstrap config
 - b. Reboot of router will initiate steps 3 - 5
2. USB Method:
 - a. Format USB drive as FAT-32 and add *ciscosdwan.cfg* text file
 - b. Insert USB into router in factory default state and power up
 - c. Router will read USB drive, apply *ciscosdwan.cfg*, and initiate provisioning steps 3 - 5
 - d. USB drive is only read if router has no config - may be left in for DR

Streamlined Provisioning - Private Transport



Scenario

1. SD-WAN edge router has no access to PnP portal:
 - a. Private network - MPLS, pLTE/5G
 - b. Address not received via DHCP
 - c. Interface preconfiguration required - subint, PPPoE, APN
 - d. Cyber policy

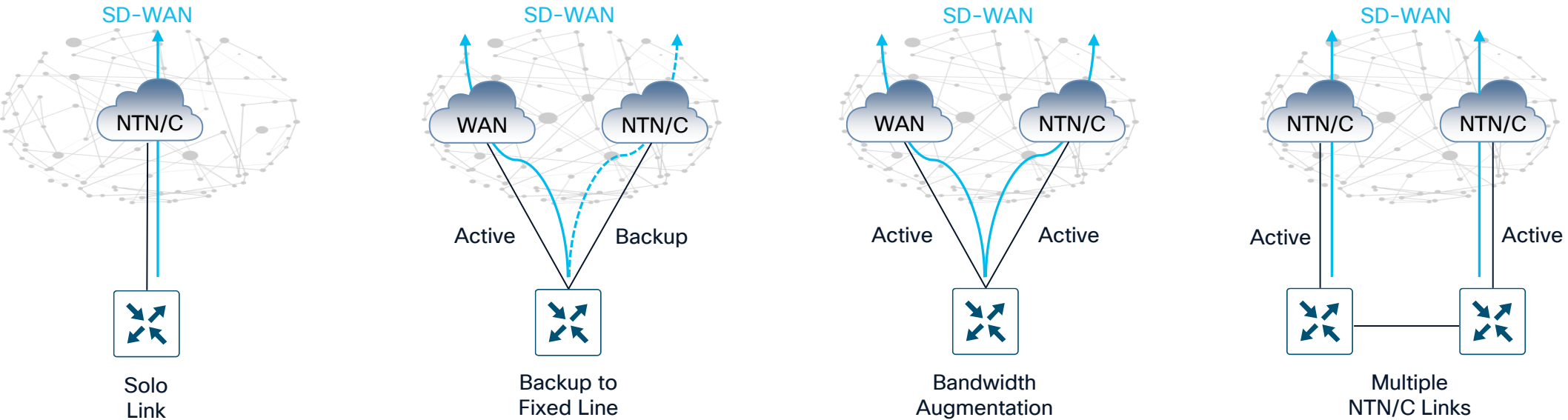
Options

1. CLI Method:
 - a. Console into router and apply bootstrap config
 - b. Reboot of router will initiate steps 3 - 5
2. USB Method:
 - a. Format USB drive as FAT-32 and add *ciscosdwan.cfg* text file
 - b. Insert USB into router in factory default state and power up
 - c. Router will read USB drive, apply *ciscosdwan.cfg*, and initiate provisioning steps 3 - 5
 - d. USB drive is only read if router has no config - may be left in for DR

Non Terrestrial and Cellular Deployments (NTN/C)



NTN/C Use Cases



Mobile Fleet



Distributed Sensors

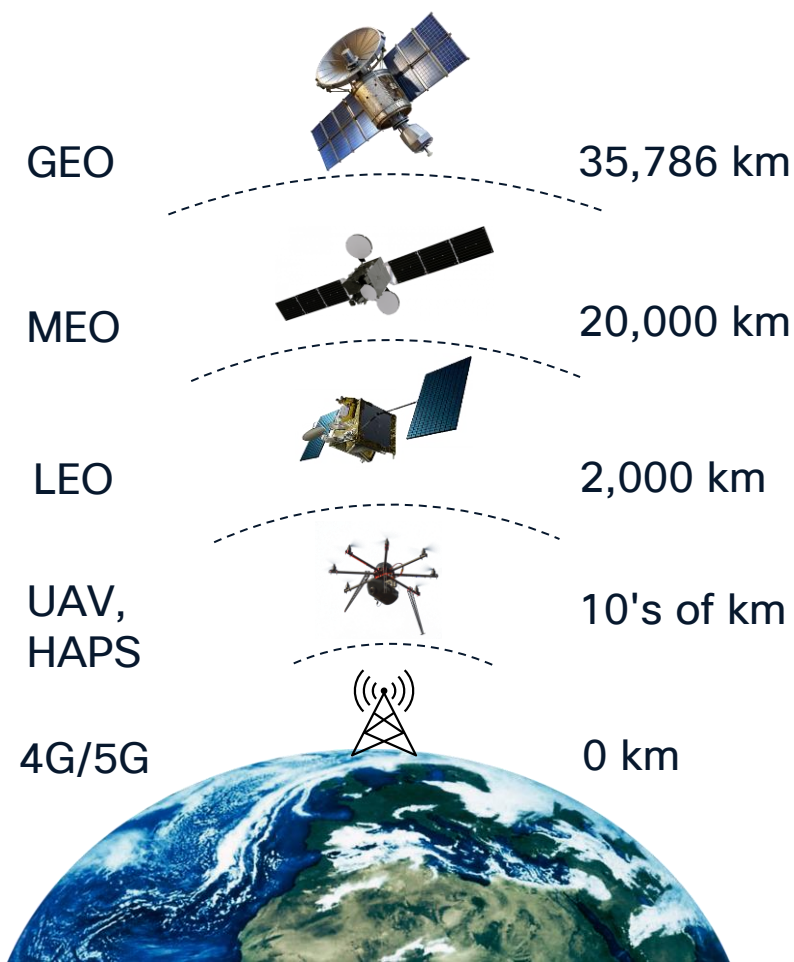


Remote Locations



Out-of-band management

NTN/C Characteristics



Platforms	Altitude Range	Round Trip Time	Typical UE Throughput
Geostationary Earth Orbit (GEO) satellite	35,786 km	480 ms	100 Mbps
Medium-Earth Orbit (MEO) satellite	7,000–25,000 km	125–150 ms	50–1000+ Mbps
Low-Earth Orbit (LEO) satellite	300 – 1,500 km	25–75 ms	30–200+ Mbps
UAV platform (including HAPS)	8 – 50 km (20 km for HAPS)	<10 ms	10–1000+ Mbps
Terrestrial Cellular 4G/5G	0 km	<50 ms	10–1000+ Mbps

UE: User Endpoint, UAV: Unmanned Aerial Vehicle, HAPS: High Altitude Platform Station

Improving Efficiency on NTN/C Services

Challenge

1. NTN/C connectivity has **lower upload speed** (2-20Mbps) relative to download speed.
2. SD-WAN **control traffic** can consume a high proportion of this bandwidth in full mesh topologies with default timers:
 - a. BFD probes over each IPsec tunnel (2.2 Kbps per tunnel)
 - b. OMP to/from controllers (up to 80 Kbps)
 - c. Statistics upload to Manager (1.2 Mbps)
3. Control traffic is automatically **mapped to Q0** on the WAN edge, which can contend with user real-time traffic also in Q0.

Solution

1. **Minimise** the number of IPsec tunnels
 - a. Hub-and-spoke instead of full mesh
 - b. Dynamic On Demand tunnels
 - c. NTN/C as a last-resort circuit when used as a backup to terrestrial links
2. **Preference the connection** to SD-WAN Manager over terrestrial links where available.
3. **Disable unnecessary statistics** collection when NTN/C is the only transport.
4. QoS design with **Adaptive QoS** and 2-level policer / Split LLQ.
5. SD-WAN **timer** optimisation.

Optimisations for NTN/C – Cisco Validated Profiles (CVP)

Feature	Default SD-WAN Value	CVP Catalog Optimised Value
Overlay Management Protocol (OMP) Advertisement interval Hold time	1 sec 5 min	1 min 90 min
Bidirectional Forwarding Detection Hello interval Hold time Poll interval	1 sec 6 sec 10 min	10 sec 60 sec 20 min
Cellular Tunnel Interface Hello Interval Hello Tolerance (hold time)	1 sec 12 sec	1 min 5 min
Monthly traffic volume	5.14 GB	500 MB

Improving Application Performance

Challenge

1. Satellite networks can experience higher **latency** due to congestion.
2. Satellite communications report average **packet loss** of 1-2%, with occasional spikes up to 4% or higher due to factors like atmospheric interference and handoffs.
3. TCP's reliability mechanisms can result in lowered **throughput** - even 1% packet loss may degrade application performance by 70%.
4. Many industrial **applications** require low latency, do not tolerate packet loss or produce significant quantities of data.

Solution

1. **Application-Aware Routing (AAR)** and **Predictive Path Recommendations (PPR)** can intelligently re-route traffic based on SLA violations.
2. **Quality of Service** protects mission critical applications.
3. **Forward Error Correction** reconstructs lost packets.
4. **Packet Duplication** policies replicate traffic flows over multiple links to reduce the impact of loss.
5. **TCP Optimization** proxies local TCP connections with enhanced congestion management (BBR2).
6. **Data Compression** such as DRE/LZW reduces the amount of traffic sent over the WAN.
7. **IoX** edge compute to analyse data locally on the router instead of centrally.

Improving Application Performance

Application Aware Routing

- Measures performance of overlay paths
- SLA based traffic steering at layer 7
- Automatic failover to secondary path if primary path SLA fails



Packet Duplication

- Send duplicate packets over alternate path
- Mitigate packet loss for critical traffic
- Enhances application quality of experience



Quality of Service (QoS)

- Manage and avoid network congestion
- Traffic queueing and shaping
- Prioritize critical application traffic



TCP optimization

- BBR2 congestion control algorithm
- Window scaling
- Selective acknowledgement
- Reduces latency and increase throughput



Forward Error Correction

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



DRE, LZW Compression

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



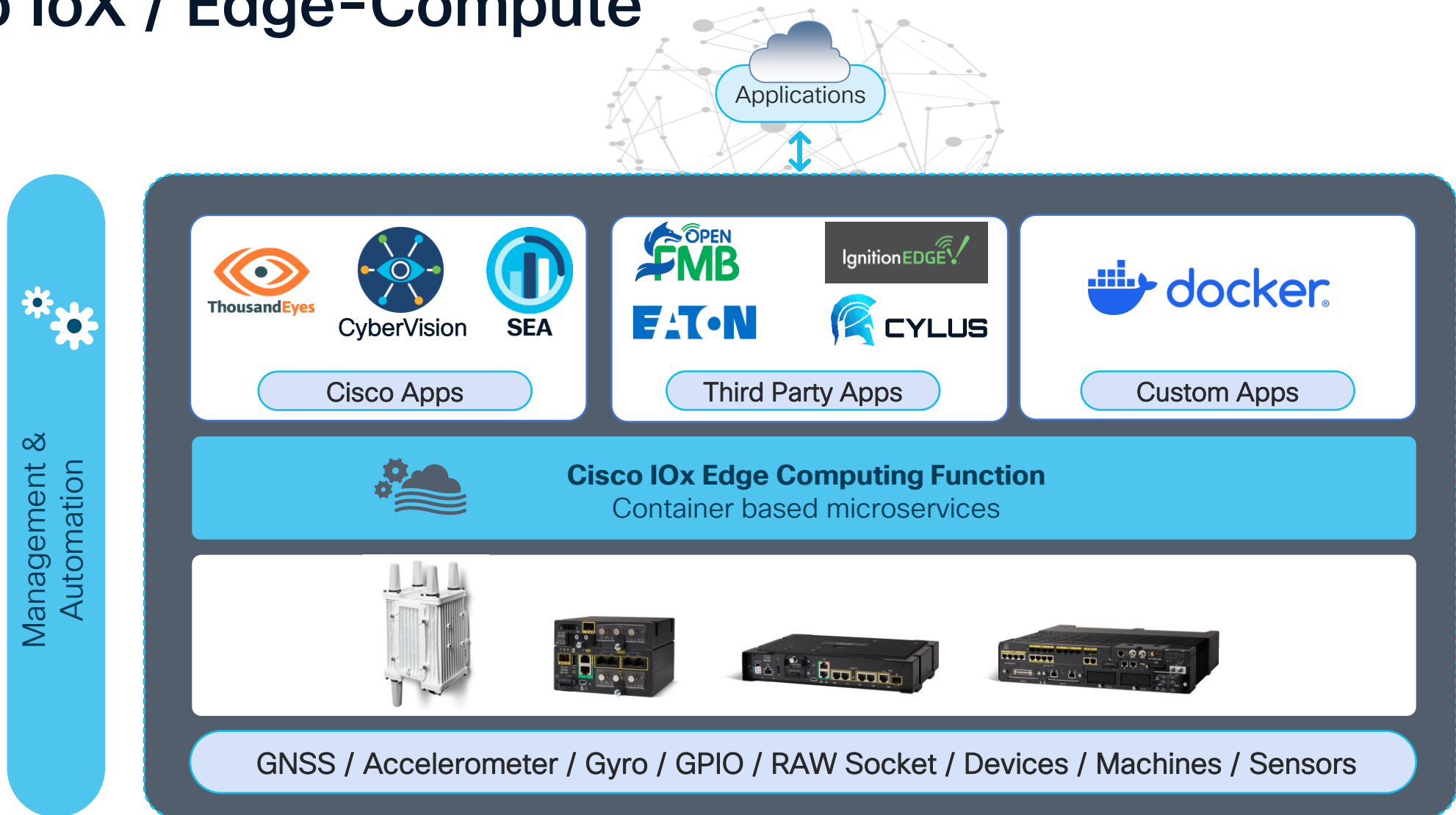
Improving Application Performance

Test	Throughput/Goodput		
	Download	Upload	Improvement
Speedtest Baseline (UDP)	250 Mbps	17 Mbps	-
iPerf3 Baseline (TCP)	55 Mbps	9 Mbps	-
iPerf3 Baseline + Packet Duplication	70 Mbps	11 Mbps	130% download 120% upload
iPerf3 + Forward Error Correction	130 Mbps	11 Mbps	238% download 120% upload
iPerf3 with TCP optimization	230 Mbps	18 Mbps	418% download 200% upload
FTP 4.33GB file download baseline	250 seconds	-	-
FTP 4.33GB file download DRE/LZW + TCP optimization	86 seconds	-	290%

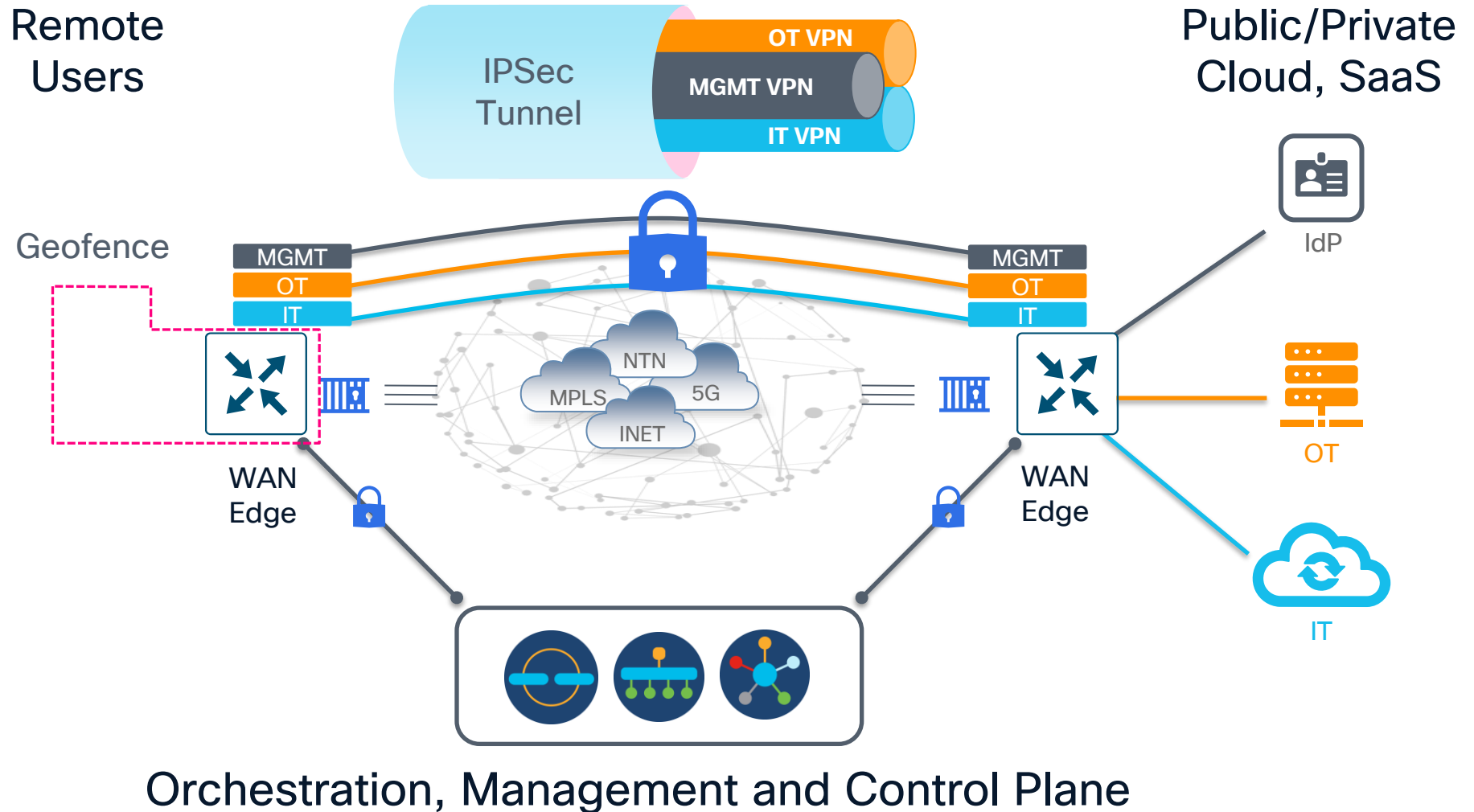
Edge Intelligence with loX



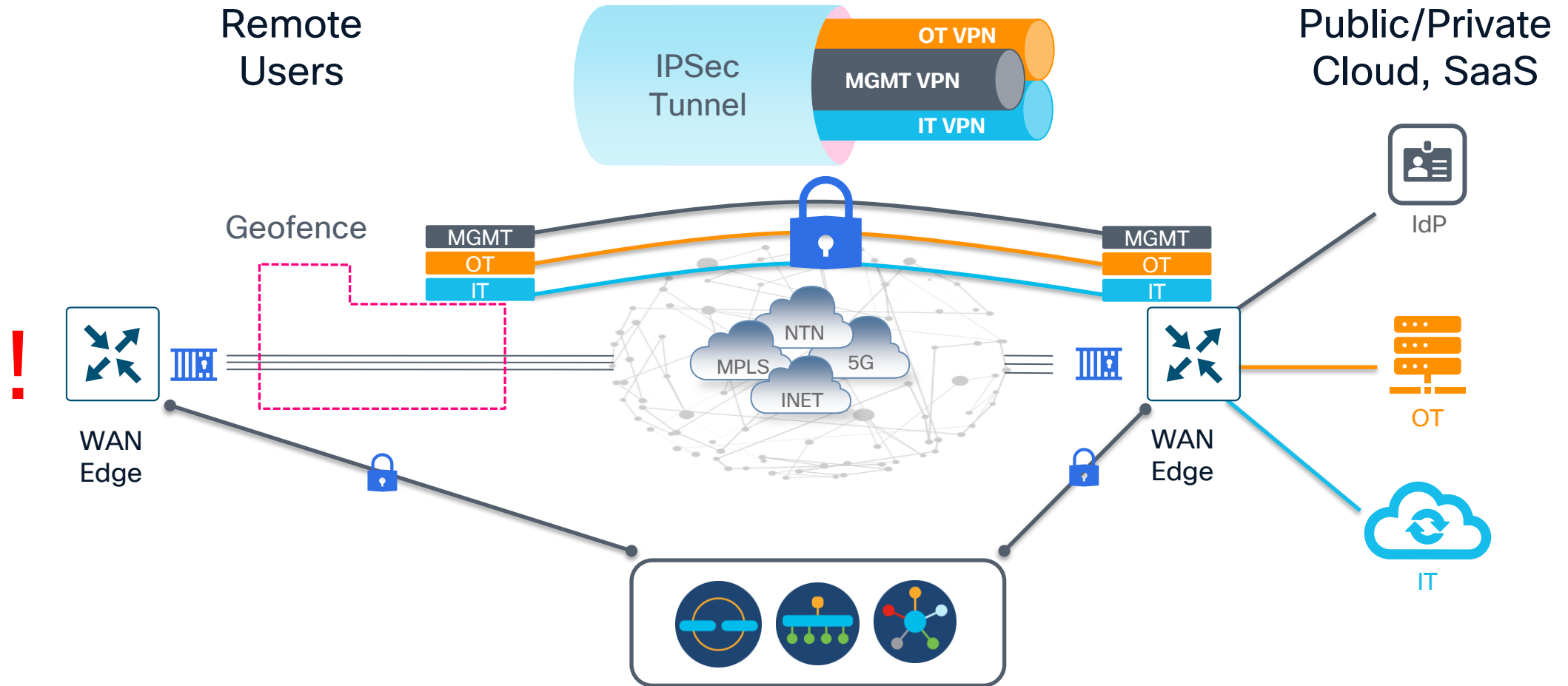
Cisco IoX / Edge-Compute



Custom Application - Geofencing

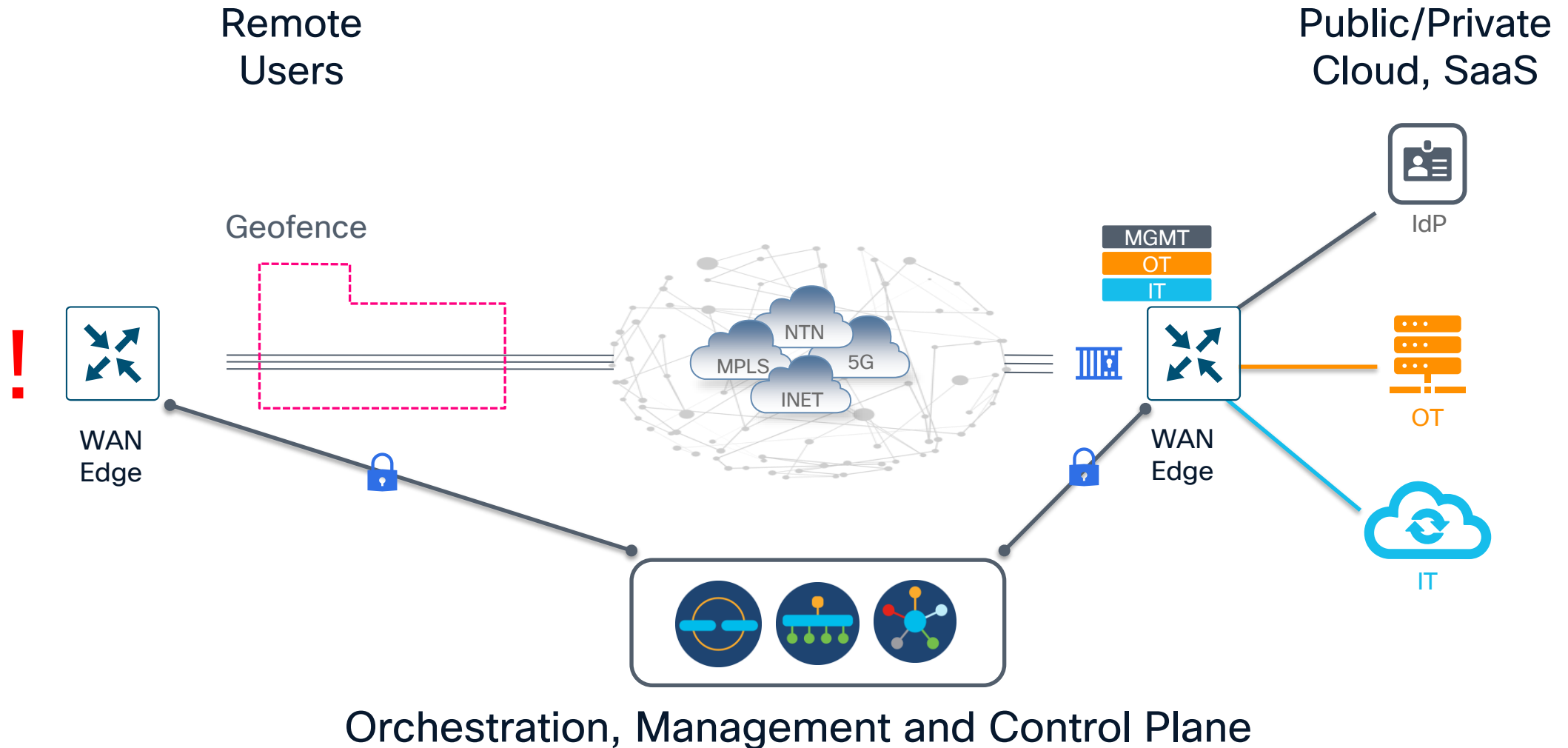


Custom Application - Geofencing



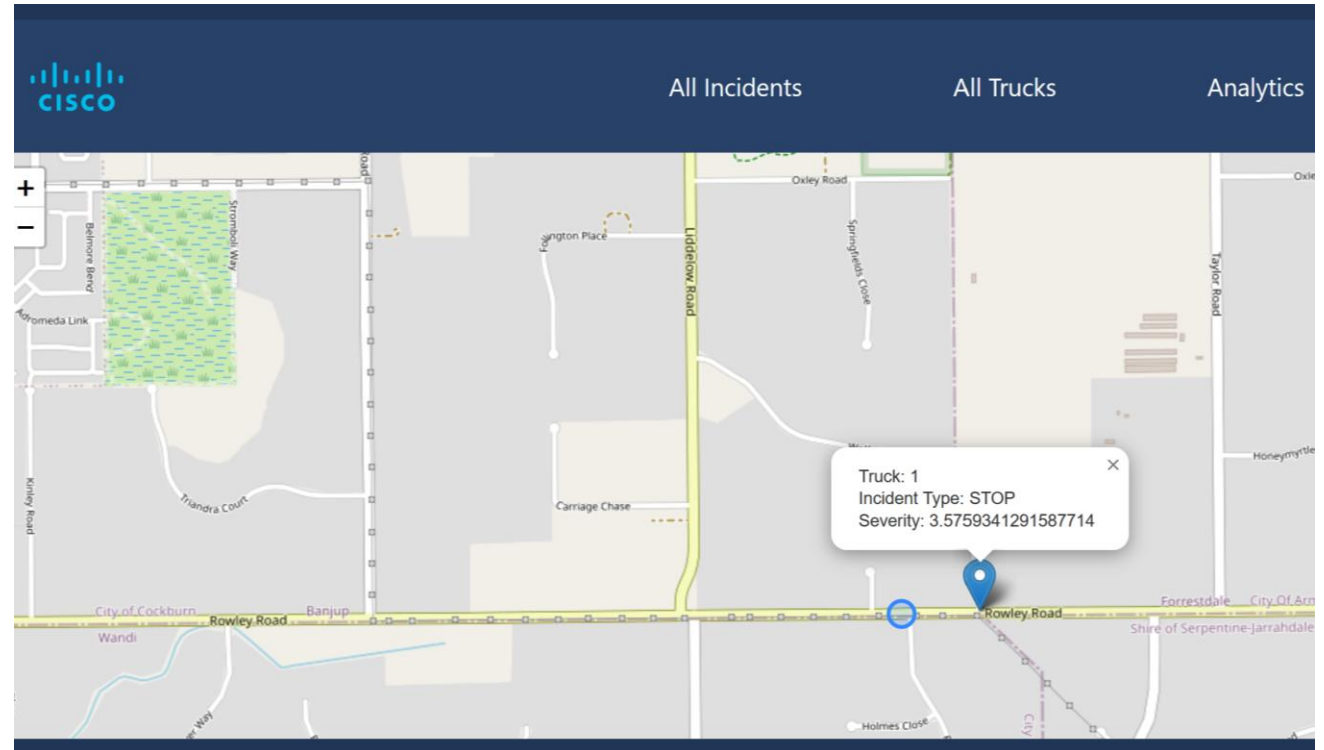
Orchestration, Management and Control Plane

Custom Application - Geofencing



Custom Application - Vehicle Safety

1. IR1835 with GNSS module
 - a. Accelerometer and gyroscope
 - b. Connected to vehicle CANBUS
2. Custom application on loX detects:
 - a. Vehicle location and velocity
 - b. Accident - sudden stop, rollover
 - c. Mechanical issues
 - d. Road surface degradation
 - e. Adverse driver behaviour
3. Event notification via
 - a. Dashboard, SMS, Webex, Splunk



Additional Information

Cisco Industry Validated Design Guides



Manufacturing



Extended enterprises



Utilities



Cities



Roadways



Transportation



Ports



Mining



Oil and gas

<https://www.cisco.com/c/en/us/solutions/design-zone/industries.html>

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



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



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

Contact me at: cadry@cisco.com

Thank you

CISCO Live !

