cisco Live!

Let's go

The bridge to possible

Cisco Catalyst SD-WAN Architecture and Overlay Security

Shamil Fernando - *Global Technical Solutions Architect*

BRKENT-2716

Cisco Webex App

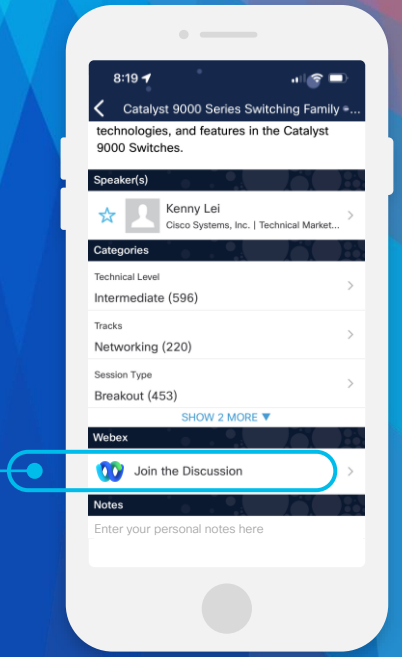
Questions?

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 December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2716

Agenda

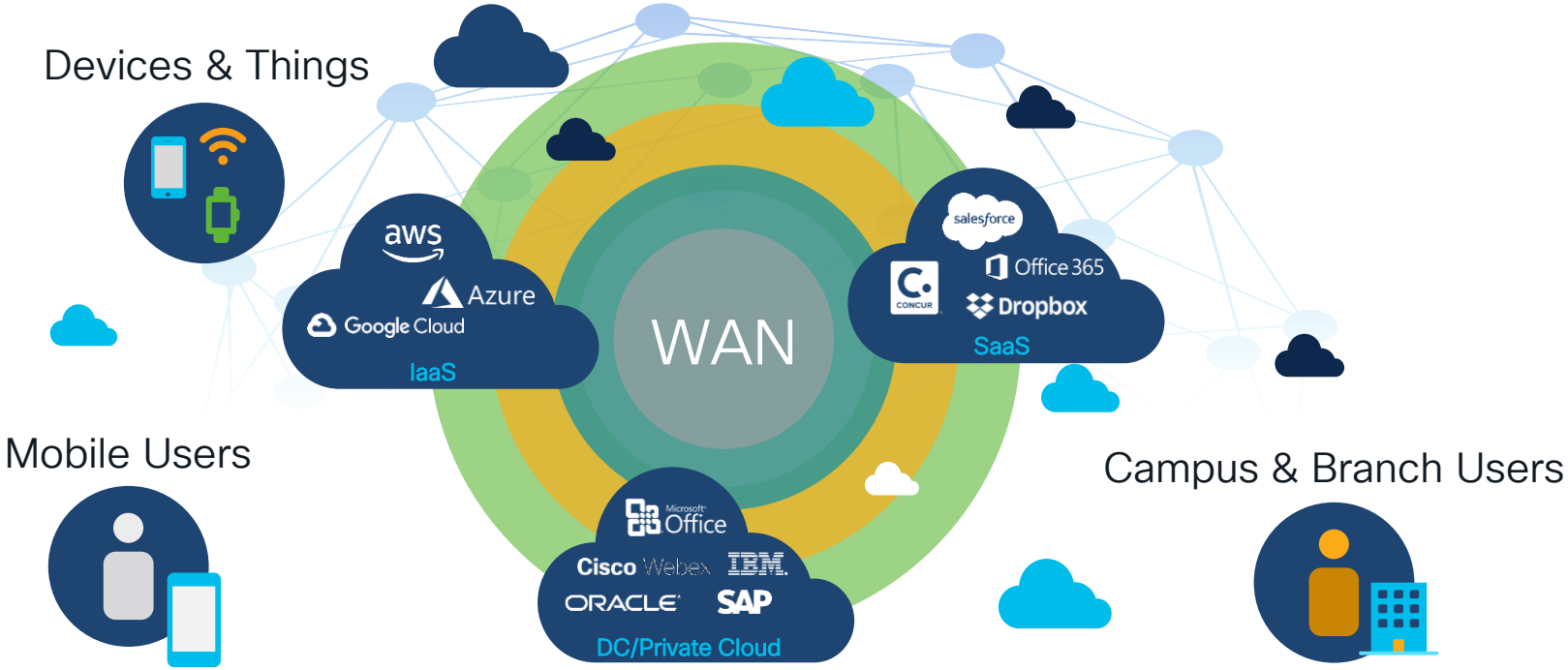
- Catalyst SD-WAN
- Architecture
- Fabric Security
- Overlay Management Protocol (OMP)
- Wrap-Up
- Q&A

New Naming: Cisco Catalyst SD-WAN

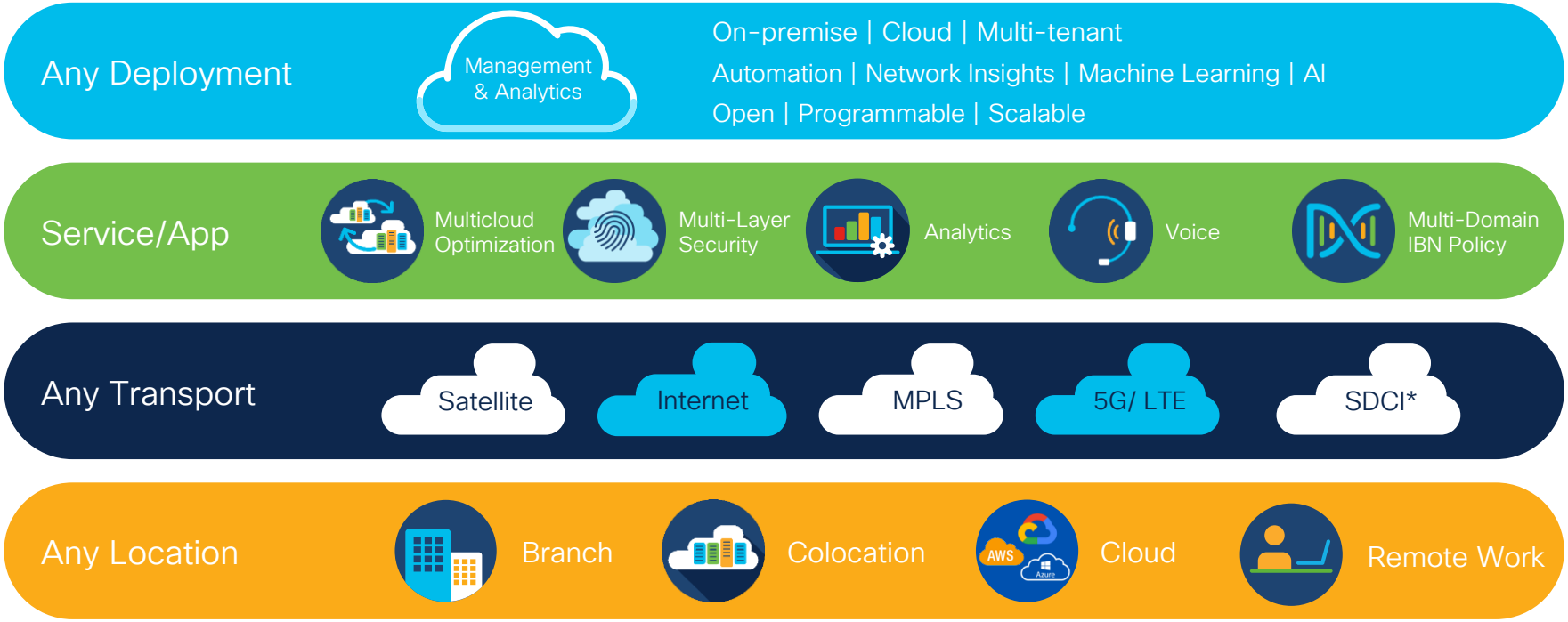
Old Name	New Name (rebranding)	Documentation	Displayed on Screens	API/CLI - Documentation
Cisco SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN
vManage	Cisco Catalyst SD-WAN Manager	SD-WAN Manager	Manager	vManage
vAnalytics	Cisco Catalyst SD-WAN Analytics	SD-WAN Analytics	Analytics	vAnalytics
vBond	Cisco Catalyst SD-WAN Validator	SD-WAN Validator	Validator	vBond
vSmart	Cisco Catalyst SD-WAN Controller	SD-WAN Controller	Controller	vSmart
Self Service Portal	Cisco Catalyst SD-WAN Portal	Cisco Catalyst SD-WAN Portal	Cisco Catalyst SD-WAN Portal	SD-WAN Portal
Cloud-Delivered Cisco SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	NA

Catalyst SD-WAN

Today Applications are Moving to Multiple Clouds



Flexible Architecture for Intent-based Networking



* Software Defined Cloud Interconnect

SD-WAN Architecture

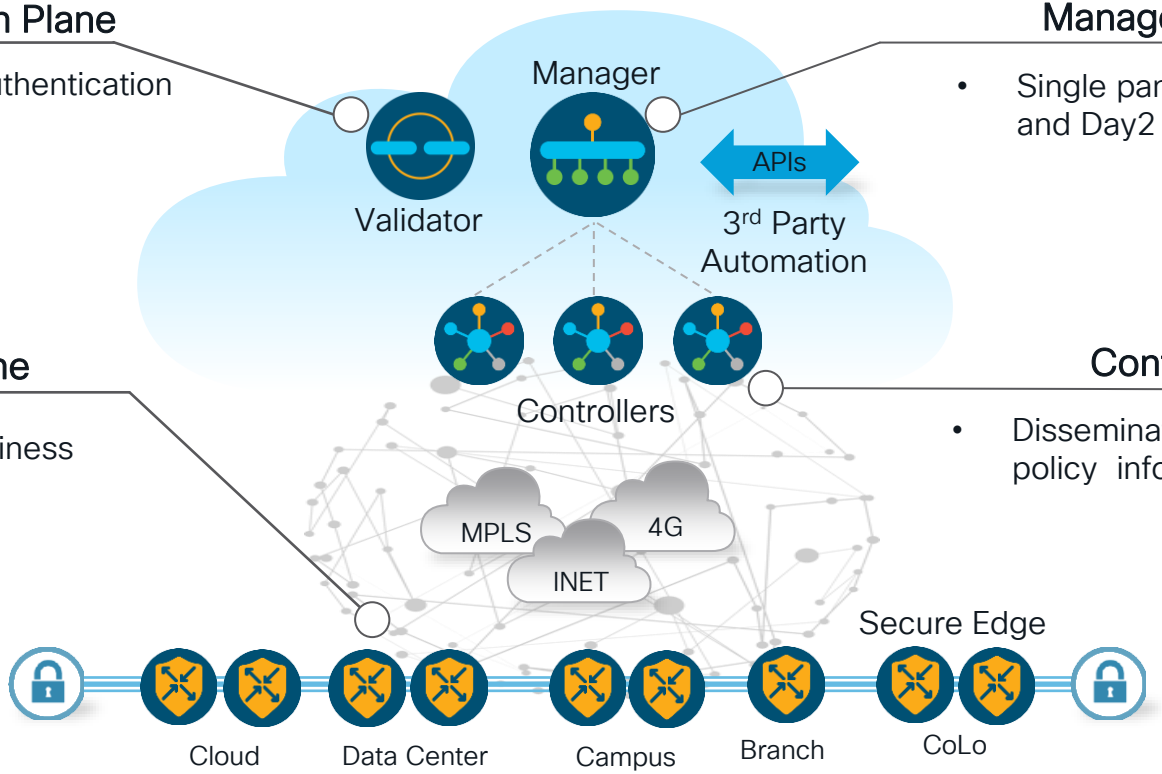
Cisco Catalyst SD-WAN Architecture

Orchestration Plane

- First point of authentication

Management Plane

- Single pane of glass for Day0, Day1 and Day2 operations



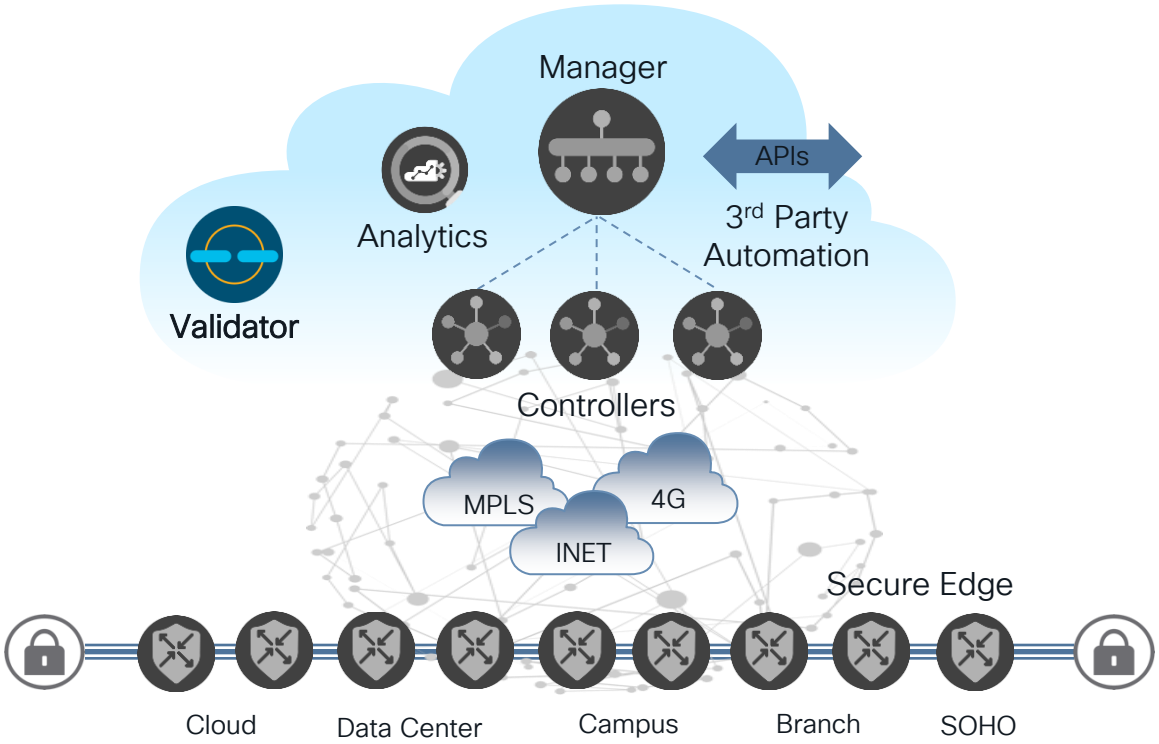
Data Plane

- Implements business intent policies

Control Plane

- Disseminates control plane and policy information between Edges

Cisco Catalyst SD-WAN Solution Elements

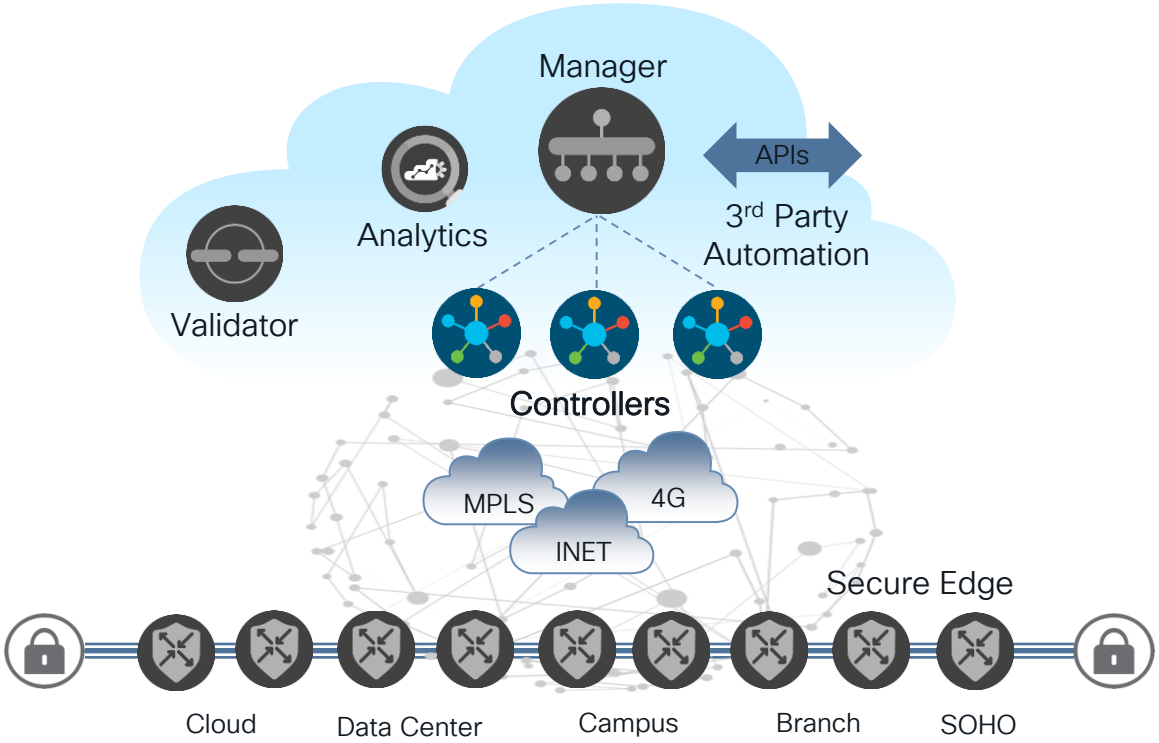


Orchestration Plane

Validator

- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of Controllers/ Manager to all Secure Edges
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient

Cisco Catalyst SD-WAN Solution Elements

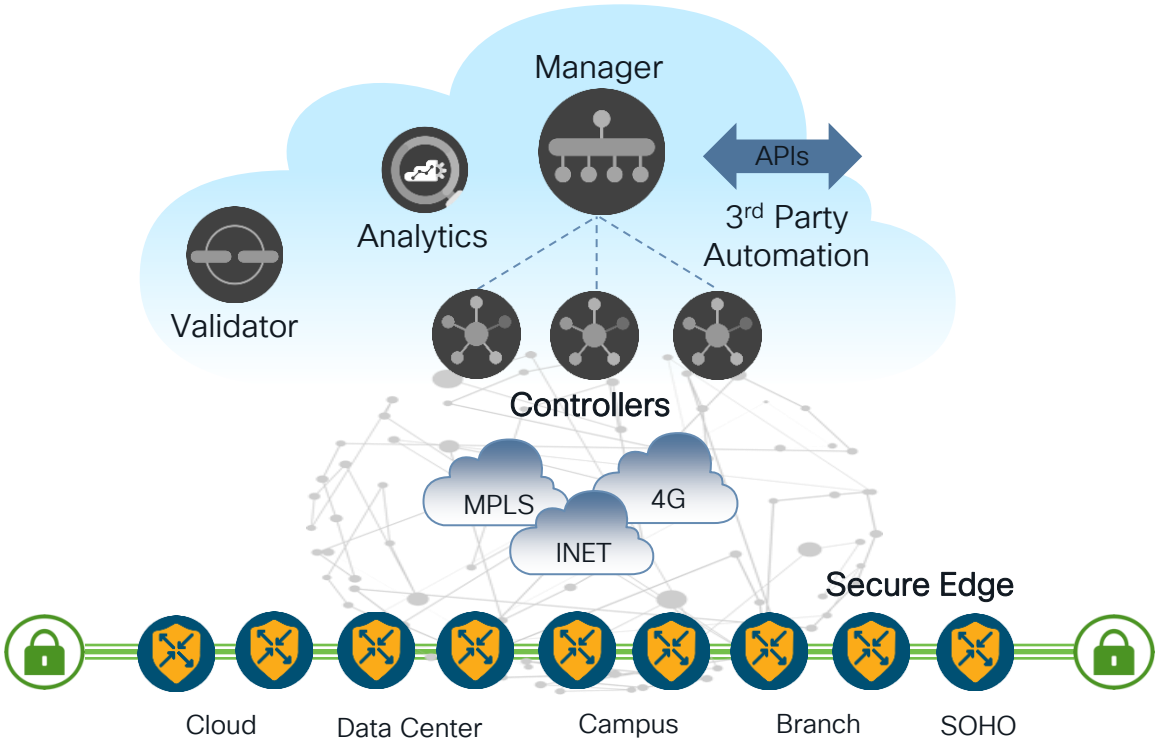


Control Plane

Controller

- Facilitates fabric discovery
- Dissimilates control plane information between Secure Edges
- Distributes data plane and app-aware routing policies to the Secure Edges
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

Cisco Catalyst SD-WAN Solution Elements

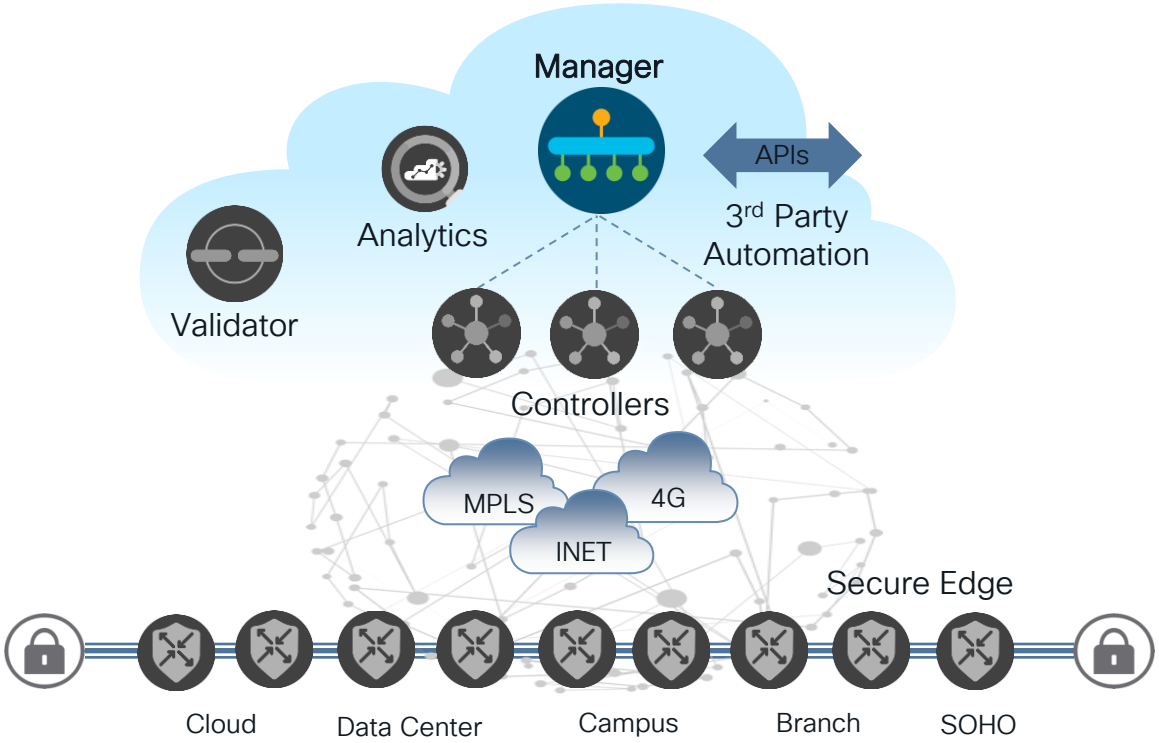


Data Plane

Secure Edge

- Provides secure data plane with remote Secure Edge Devices
- Establishes secure control plane with Controller (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, EIGRP, RIP and RIPng
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mbps to 100Gbps)

Cisco Catalyst SD-WAN Solution Elements



Management Plane

Manager

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

Catalyst SD-WAN Fabric Deployment Models

Reduce operational burden of customers

Customer Hosted
(On-Prem, AWS & Azure)

- Customer Data Center
- MSP Data Center

Cisco Hosted
(AWS & Azure)

- Standard Environment (Shared and Dedicated)
- Certified Environment (PCI, SOC2, ISO, C5, etc.)
- Gov. Cloud (FedRAMP)

Cloud-delivered

- Life Cycle Management of SD-WAN Fabric
- Agile and scalable service access
- Operational simplicity
- Rich analytics providing actionable insights

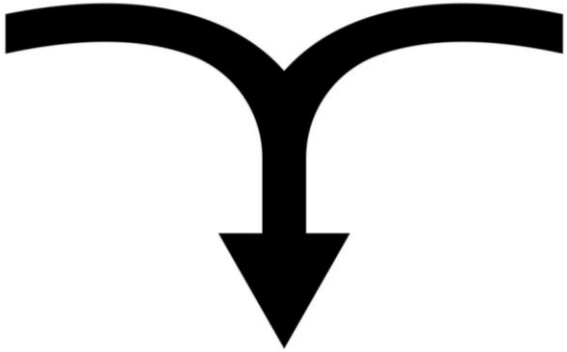
Flexible deployment models aligned to your business needs

SD-WAN Fabric Security

Cisco Catalyst SD-WAN Secure Edge

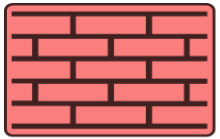
Network Team

Router (Private Links)



Security Team

Firewall (Public Links)



Cisco Catalyst Secure Edge

(Private & Public Links)

Catalyst SD-WAN Security Fundamentals

Secure Edge Parameter Protection

- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- Trust Anchor Module (TAm)
- Secure Boot of Signed Images
- Runtime Defenses (RTD)

Onboarding & Authentication

- Devices Onboarding Process
- Zero Trust
- Certificate-based Authentication & Whitelisting
- Automate Custom Certificate Authority (CA)
- Management through using SD-WAN Manager

Transport Security

- IKE less IPsec (Key exchange using a controller, high scale)
- Key - Using RNG (NIST SP 800-90A)
- Key Rotation - 24hr Default
- Anti-Replay Protection

Least Access Principle

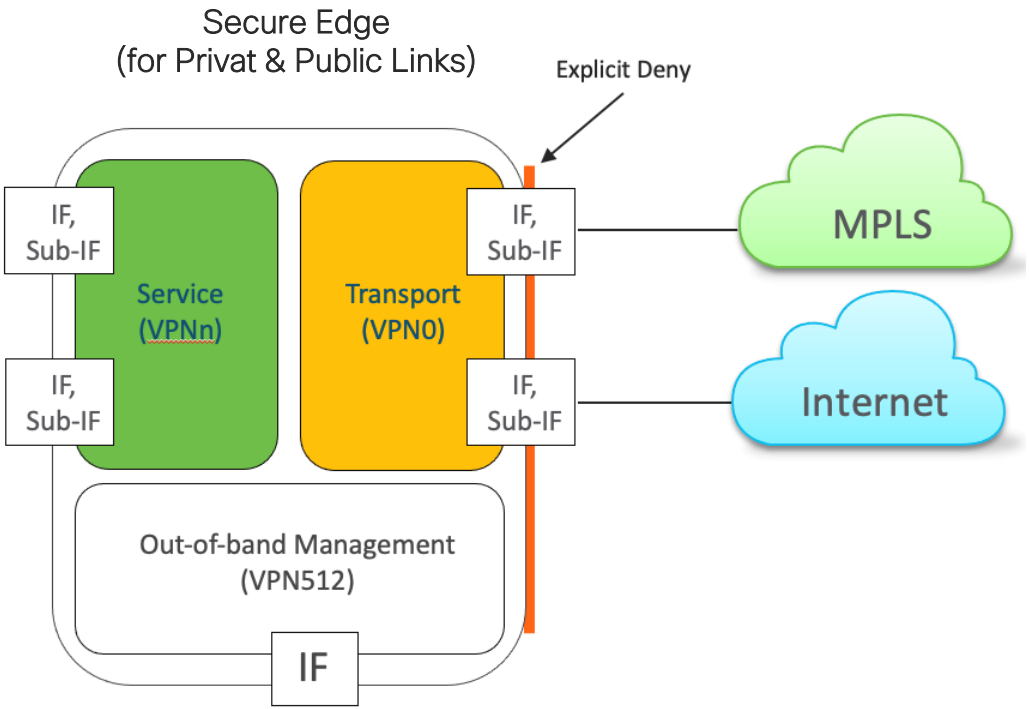
- Segmentation (VRF) - True VRF with separate route table & different topology each VRF
- Overlay Management Protocol (OMP)

Secure Edge Parameter Protection

- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- Trust Anchor Module (TAm)
- Secure Boot of Signed Images
- Runtime Defenses (RTD)

Secure Edge – Parameter Protection

Trust Zone
Untrust Zone



- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation

Cisco Trustworthy Technologies

Secure Boot of Signed Images

- Prevents malicious code from booting on a Cisco platform
- Automated integrity checks
- Monitors startup process and shuts down if compromised
- Faster identification of threats

Trust Anchor module (TAm)

- Tamper-resistant chip with X.509 cert installed at manufacturing
- Provides unique device identity and anti-counterfeit protections
- Secure, non-volatile on-board storage and RNG/crypto services
- Enables zero-touch provisioning and minimizes deployment costs

Runtime Defenses (RTD)

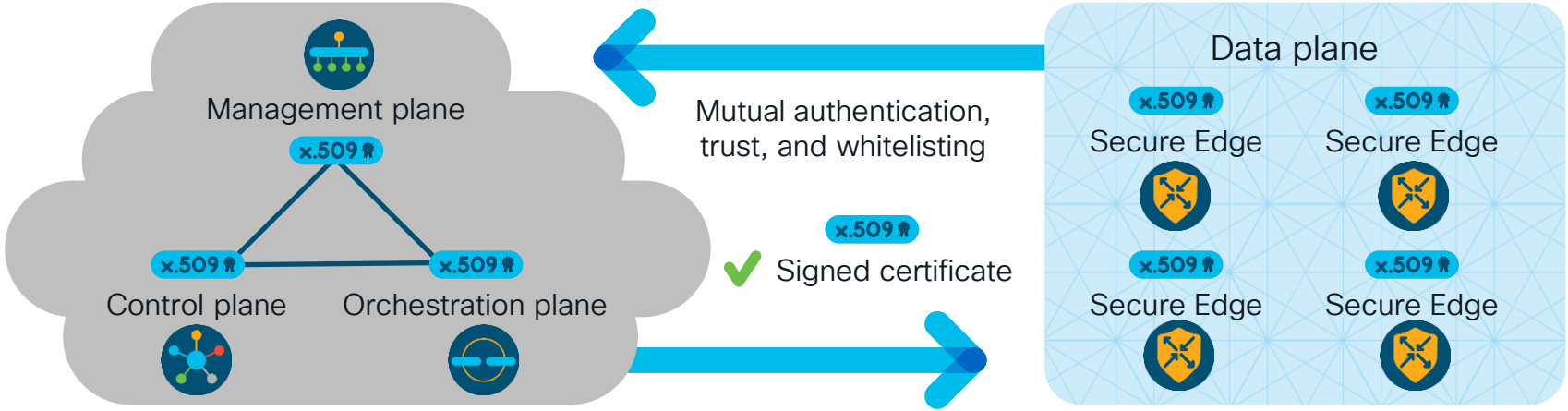
- Protects against injection of malicious code into running software
- Makes it harder for attackers to exploit vulnerabilities in running software
- Runtime technologies include ASLR, BOSC, and X-Space

Trustworthy technologies enhance the security and resilience of Cisco solutions

Onboarding & Authentication

- Devices Onboarding Process
- Zero Trust
- Certificate-based Authentication & Whitelisting
- Automate Custom Certificate Authority (CA)
- Management through using SD-WAN Manager

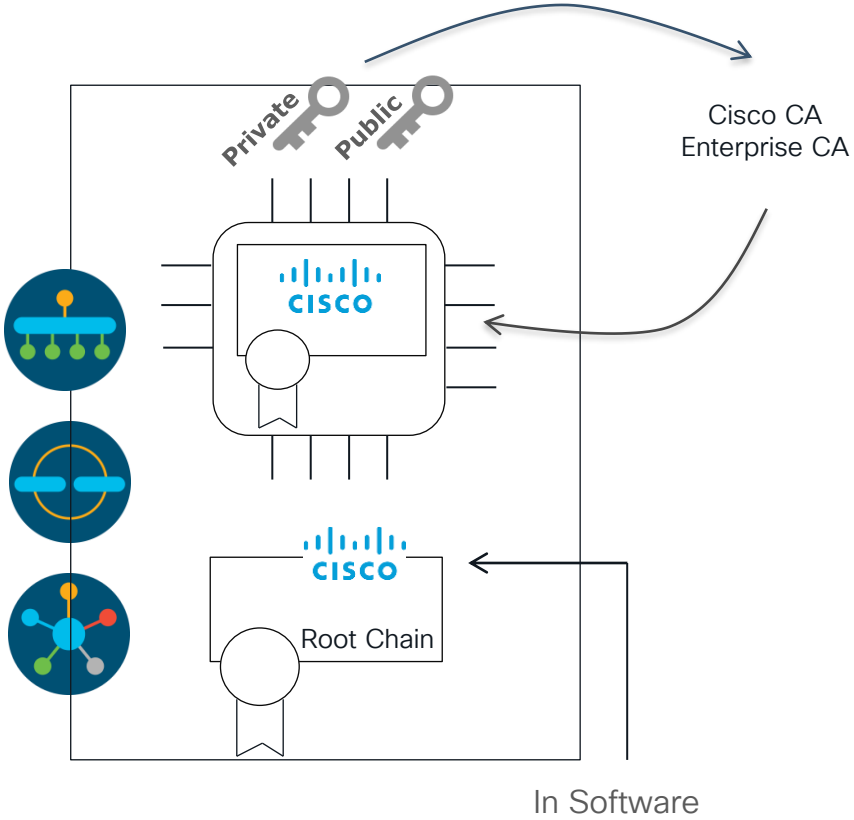
SD-WAN Fabric with Zero-Trust Authentication



- Mutual certificate-based authentication
- Validator validates Controller and Manage certificate serial numbers against authorized white-list

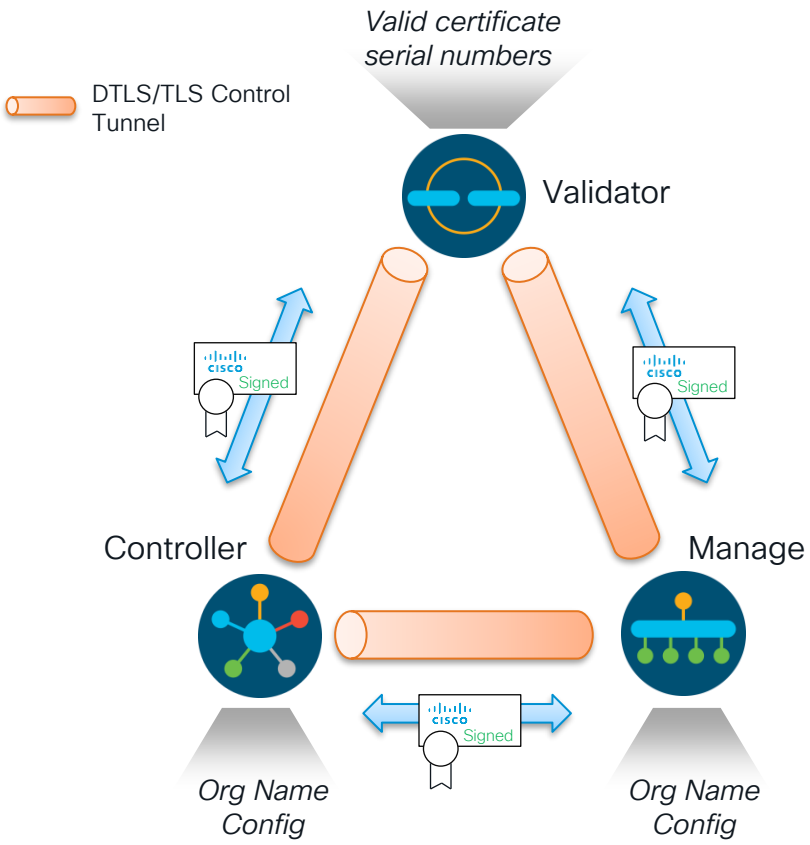
- Embedded device identity (TPM)
- AES 256-GCM-based encryption
- Frequent key rotation (default: 24 hours)

Cisco SD-WAN Controller Identity



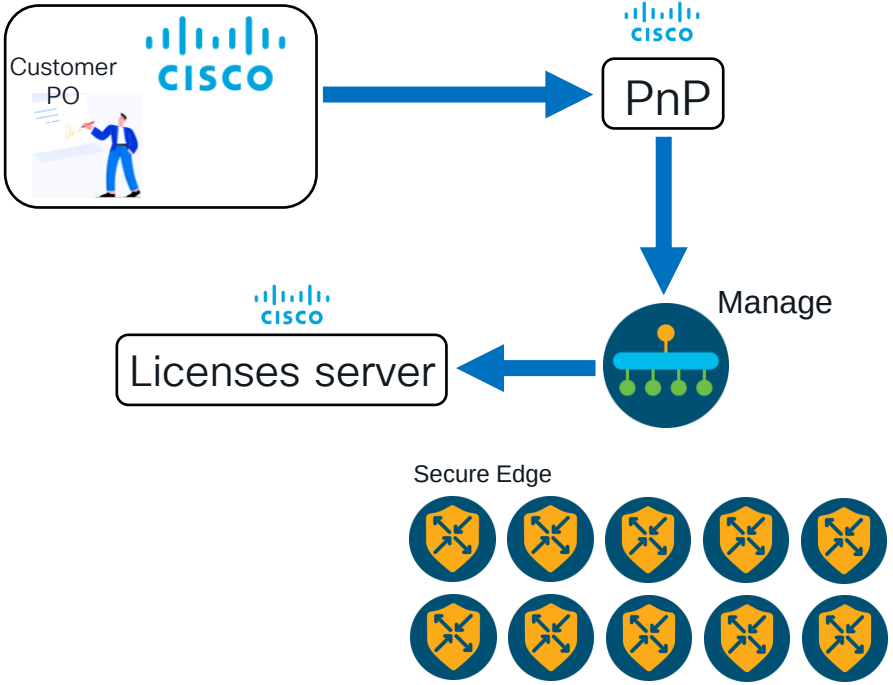
- Private and public keys are generated on the control element
- Certificate is generated
- Certificate is signed by Cisco CA / Enterprise CA
- Certificate is installed into the control element
- Control element has a root CA trust chain for Cisco root CA

Secure Control Channel: Control Elements



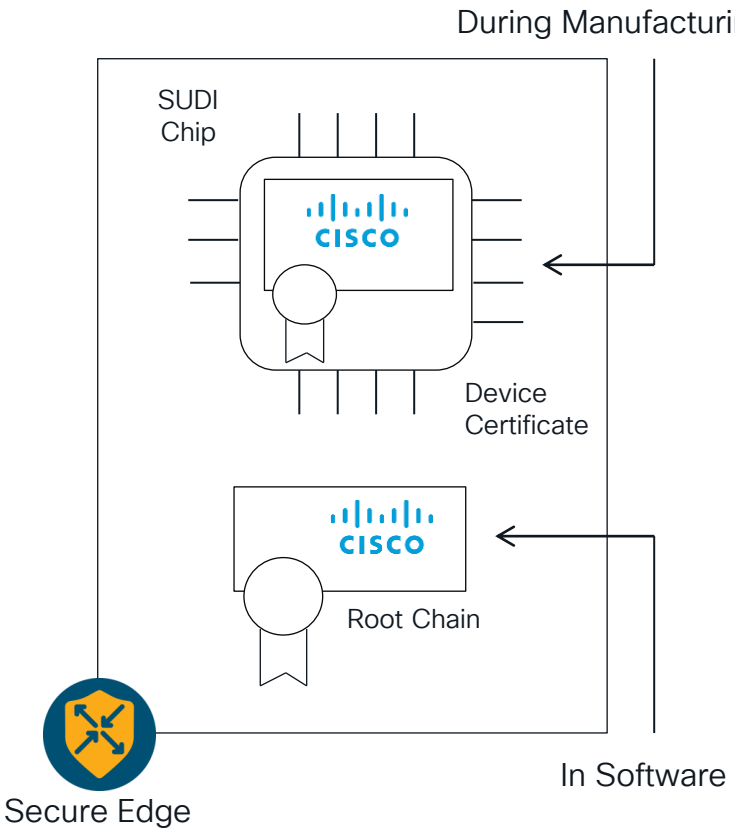
- Certificates are exchanged and mutual authentication takes place
- Validator validates Controller and Manage certificate serial numbers against authorized white-list
- Controller and Manage validate Validator Orchestrator certificate organization name against locally configured one
- DTLS/TLS secure connection is established

Catalyst SD-WAN Onboarding Process



- Customer/Partner sends the PO to Cisco with service account (CA) virtual account (VA) info.
- Cisco uploaded the Secure Edge Devices serial numbers to PnP
- Cisco Manager downloads the serial numbers from PnP
- Only downloaded serial numbers can participate on the overlay.

Cisco Secure Edge Identity



- Each physical Cisco Secure Edge is uniquely identified by the chassis ID and certificate serial number
- Certificate is stored in on-board SUDI chip (Secure Unique Device Identifier) - Trusted Platform Module.
  - Installed during manufacturing process
- Certificate is signed by Cisco root CA
  - Trusted by Control Plane elements
- Cisco root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be automatically installed during PnP

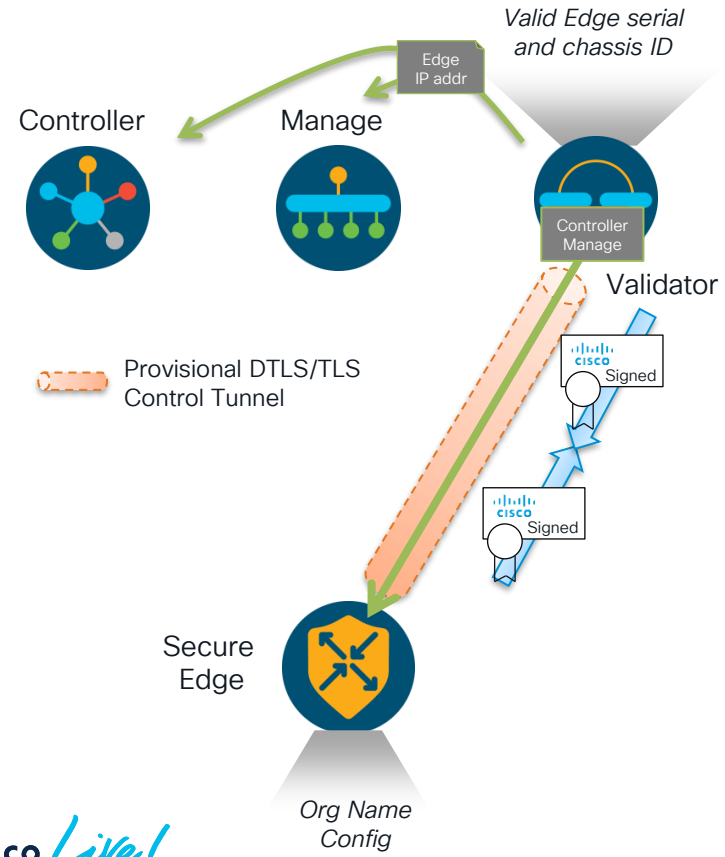
Secure Bring-up with Approval

Chassis Number	Certificate Serial	Hostname	IP Address	Validate ↓
9391da23-f0d1-4259..	0334D73E5EC036F87ABE...	DataCenter	1.1.1.5	invalid | staging | valid
4de0b85f-a2ae-42ec...	585A0084DEA8396DD77B..	RemoteSite	1.1.1.4	invalid | staging | valid
5f05358a-bef7-4e15...	248792F938E6EA8BEE6FD..	AWS	1.1.1.6	invalid | staging | valid

- Single stage (Zero Touch Provisioning) – Identity is automatically trusted
- Two stage (One Touch Provisioning) – Identity is not automatically trusted. Requires administrator validation.
- Staging Mode – Identity is automatically trusted for control, but not for data. Requires administrator validation.

Secure Control Channel: Secure Edge

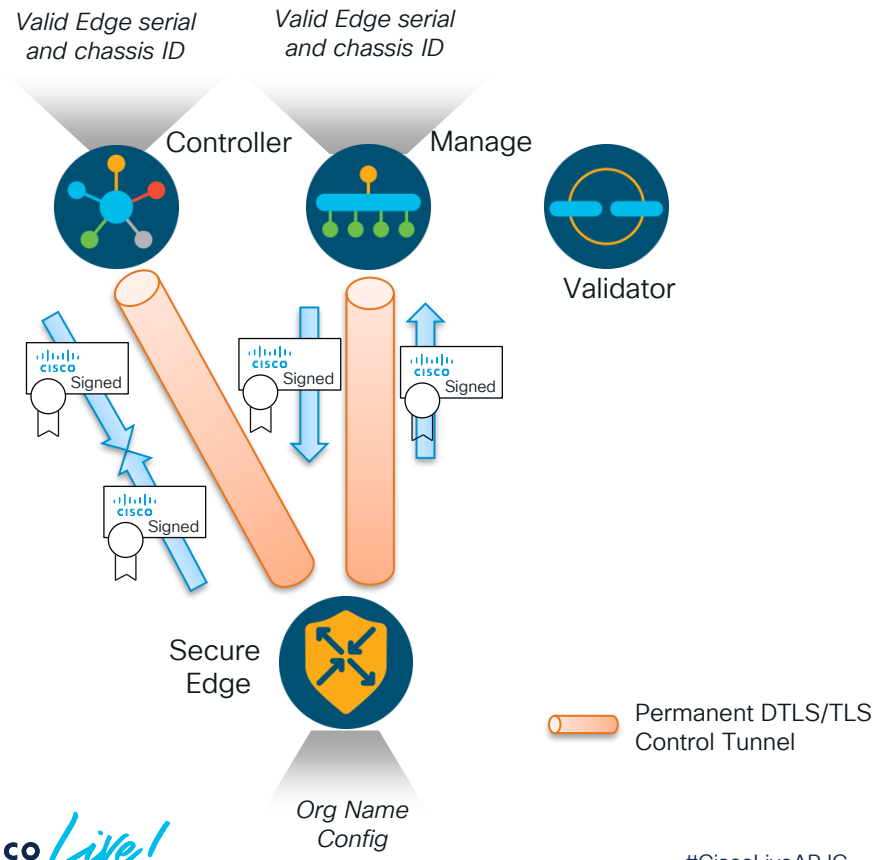
Connection to Validator Orchestrator



- Certificates are exchanged and mutual authentication takes place between Validator and Secure Edge
  - Over encrypted tunnel
- Validator validates Secure Edge serial number and chassis ID against authorized Edge white-list
- Secure Edge validates Validator certificate organization name against locally configured one
- Provisional DTLS/TLS tunnel is established between Validator and Secuer Edge
- Validator returns to Secure Edge a list of Controllers and Manage
- Validator notifies Controller and Manage of Secure Edge public IP address
- Provisional DTLS/TLS tunnel between Validator and Secure Edge is terminated

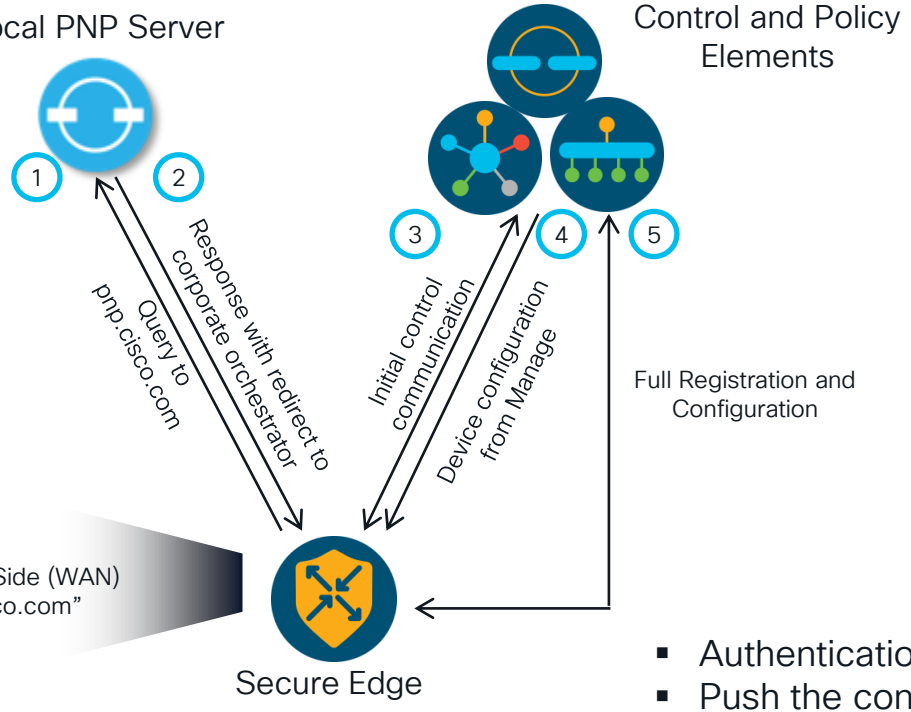
Secure Control Channel: Secure Edge

Connection to Controller and Validator Manage



- Certificates are exchanged and mutual authentication takes place between Controller , Manage and Secure Edge
  - Over encrypted tunnel
- Controller and Manage validate Secure Edge
- Verify serial number and chassis ID against authorized Secure Edge white-list
- Secure Edge validates Controller and Manage certificate organization name against locally configured one
- Permanent DTLS/TLS tunnel between Controller , Manage and Secure Edge is established

Zero Touch Bring up



Assumption:

- **DHCP. Non-DHCP** on Transport Side (WAN)
- Add Entry to Local DNS “pnp.cisco.com”
- DNS to resolve pnp.cisco.com*

* Factory default config

- Authentication
- Push the configuration
- Enforce the version

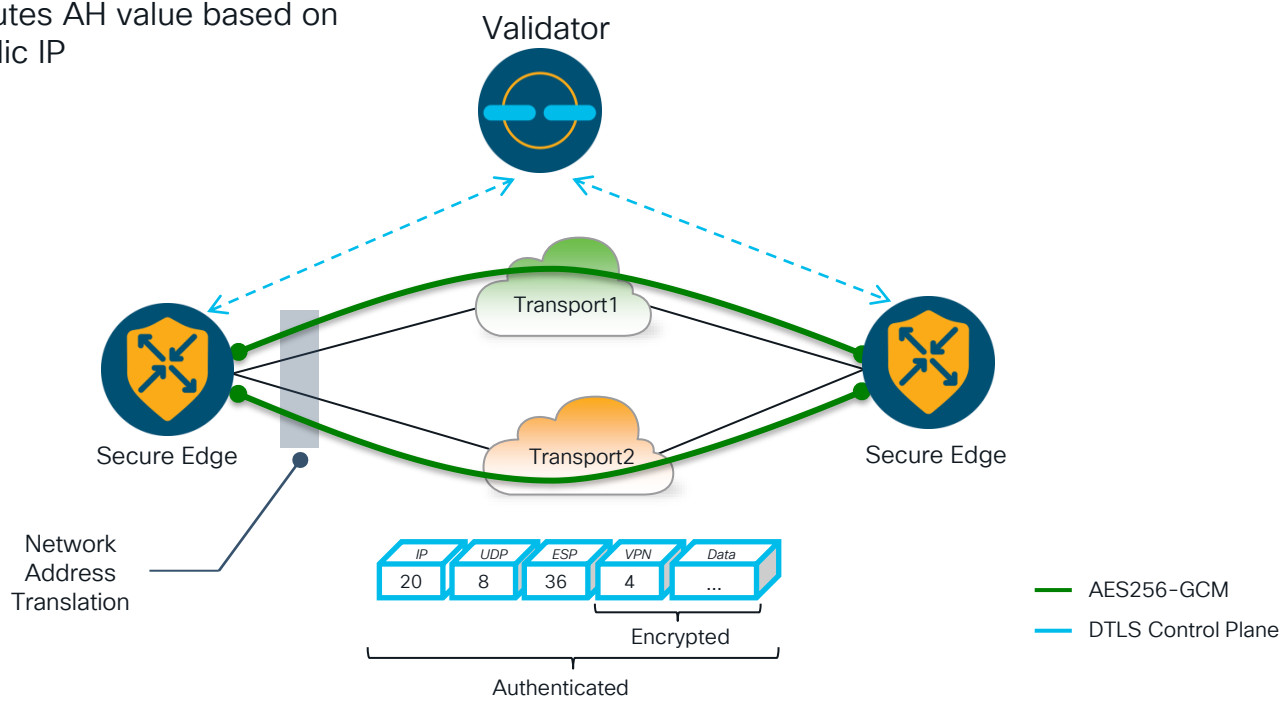
Transport Security

- IKE less IPsec (Key exchange using a controller, high scale)
- Key - Using RNG (NIST SP 800-90A)
  - Key Rotation - 24hr Default
    - Anti-Replay Protection

Data Plane Integrity

- Validator discovers WAN Edge public IP address, even if traverses NAT
- Validator communicates IP Info controler
- WAN Edge computes AH value based on the post NAT public IP

- Packet integrity (+IP headers) is preserved across NAT
- Man-in-the-Middle Attack Mitigation

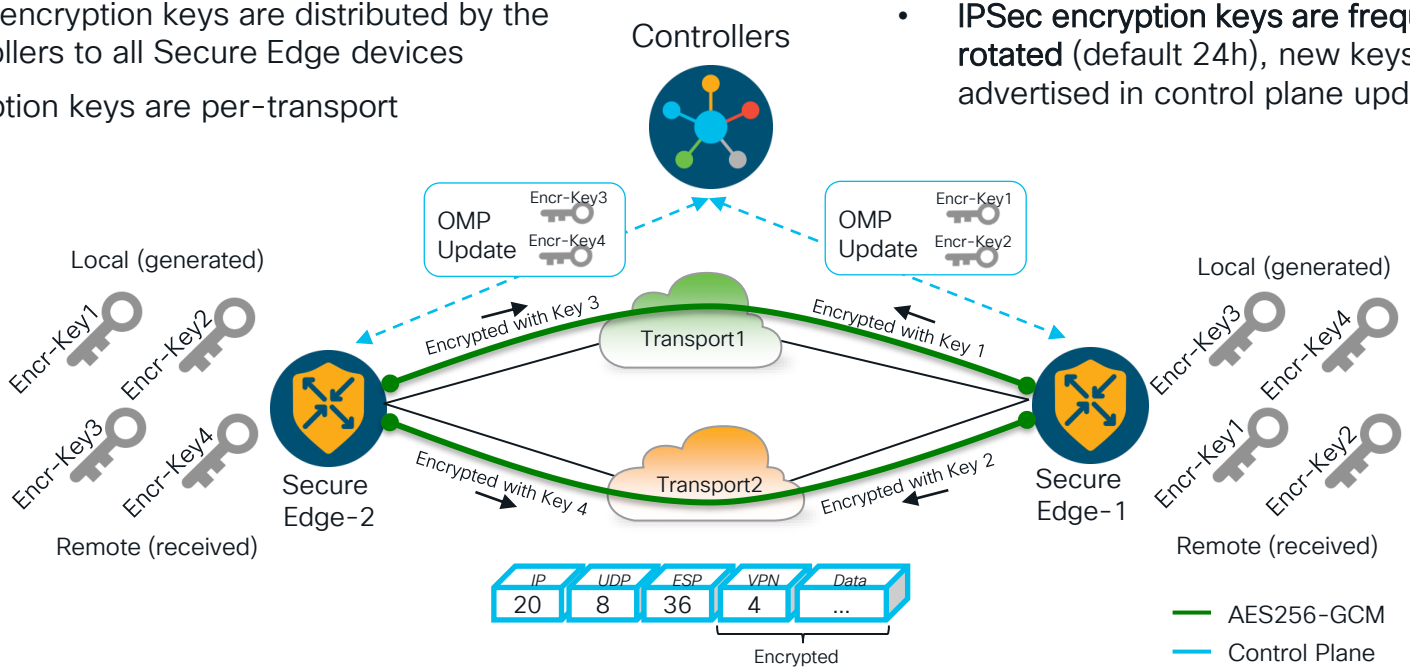


Data Plane Privacy

Centralized Encryption Key Distribution

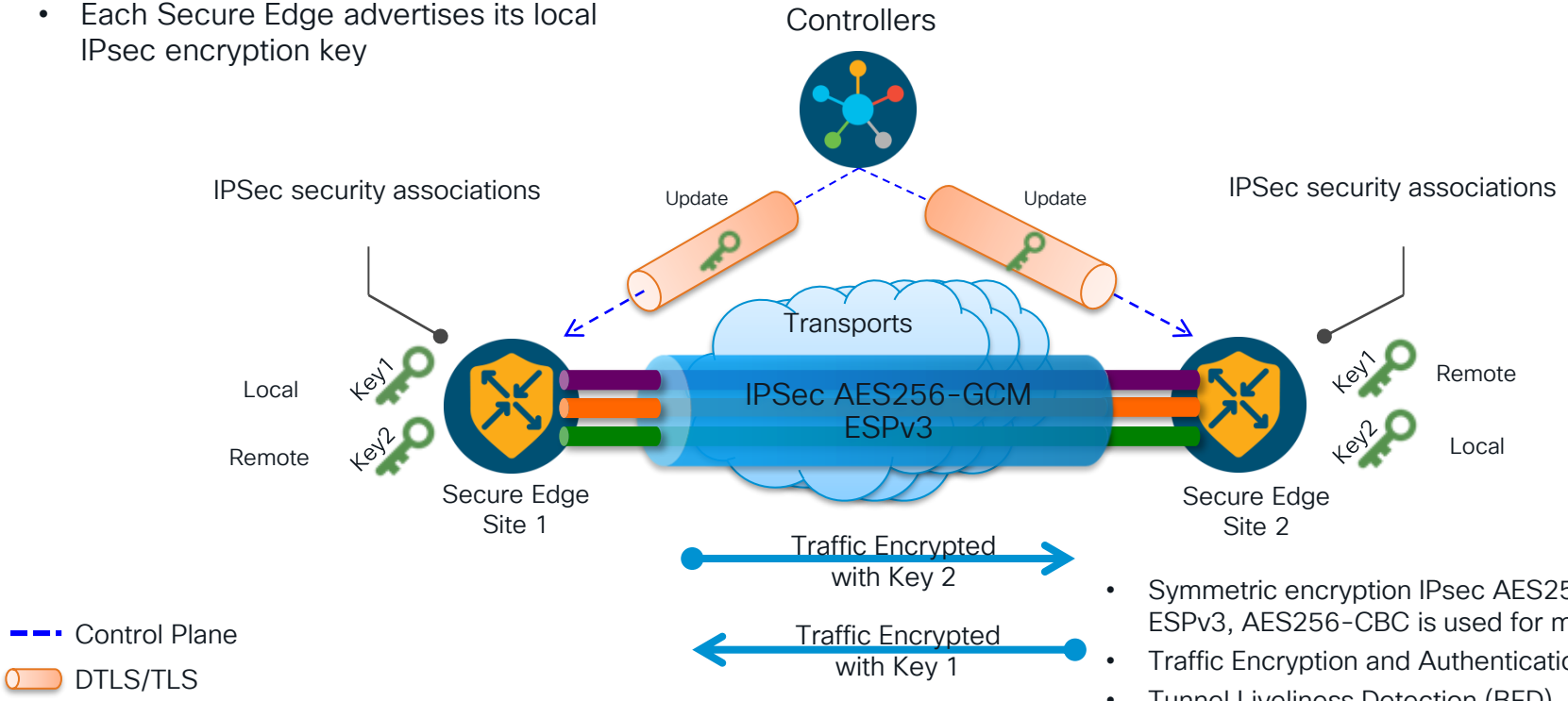
- Each Secure Edge device advertises its local IPsec encryption keys as OMP TLOC attributes
- IPSec encryption keys are distributed by the Controllers to all Secure Edge devices
- Encryption keys are per-transport

- Use AES256-GCM/CBC ESPv3 for data authenticity (integrity) and confidentiality
- **IPSec encryption keys are frequently rotated** (default 24h), new keys are advertised in control plane updates



Data Plan - SD-WAN Transport Security

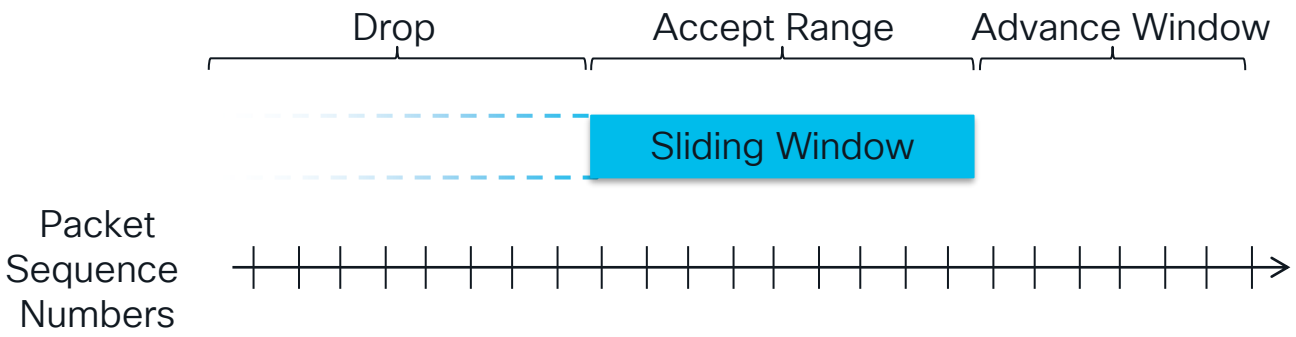
- Each Secure Edge advertises its local IPsec encryption key



- Symmetric encryption IPsec AES256-GCM ESPv3, AES256-CBC is used for multicast
- Traffic Encryption and Authentication Header
- Tunnel Liveliness Detection (BFD)
- Anti-Replay Protection
- Rekey 24 hours

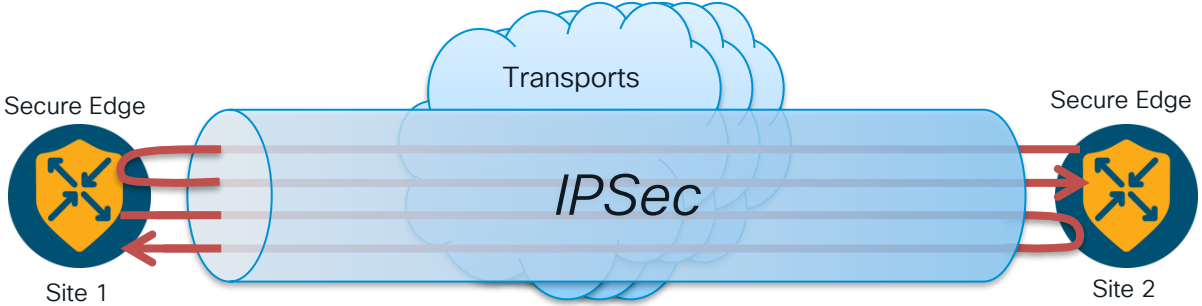
Anti-Replay Protection

- Encrypted packets are assigned sequence numbers. Secure Edge drop packets with duplicate sequence numbers
  - Replayed packet
- Secure Edge drop packets with sequence numbers lower than the minimal number of the sliding window
  - Maliciously injected packet
- Upon receipt of a packet with higher sequence number than received thus far, Secure Edge will advance the sliding window
- Sliding window is COS aware to prevent low priority traffic from “slowing down” high priority traffic

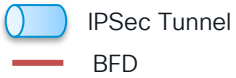


Tunnel Liveliness Detection

Bidirectional Forwarding Detection



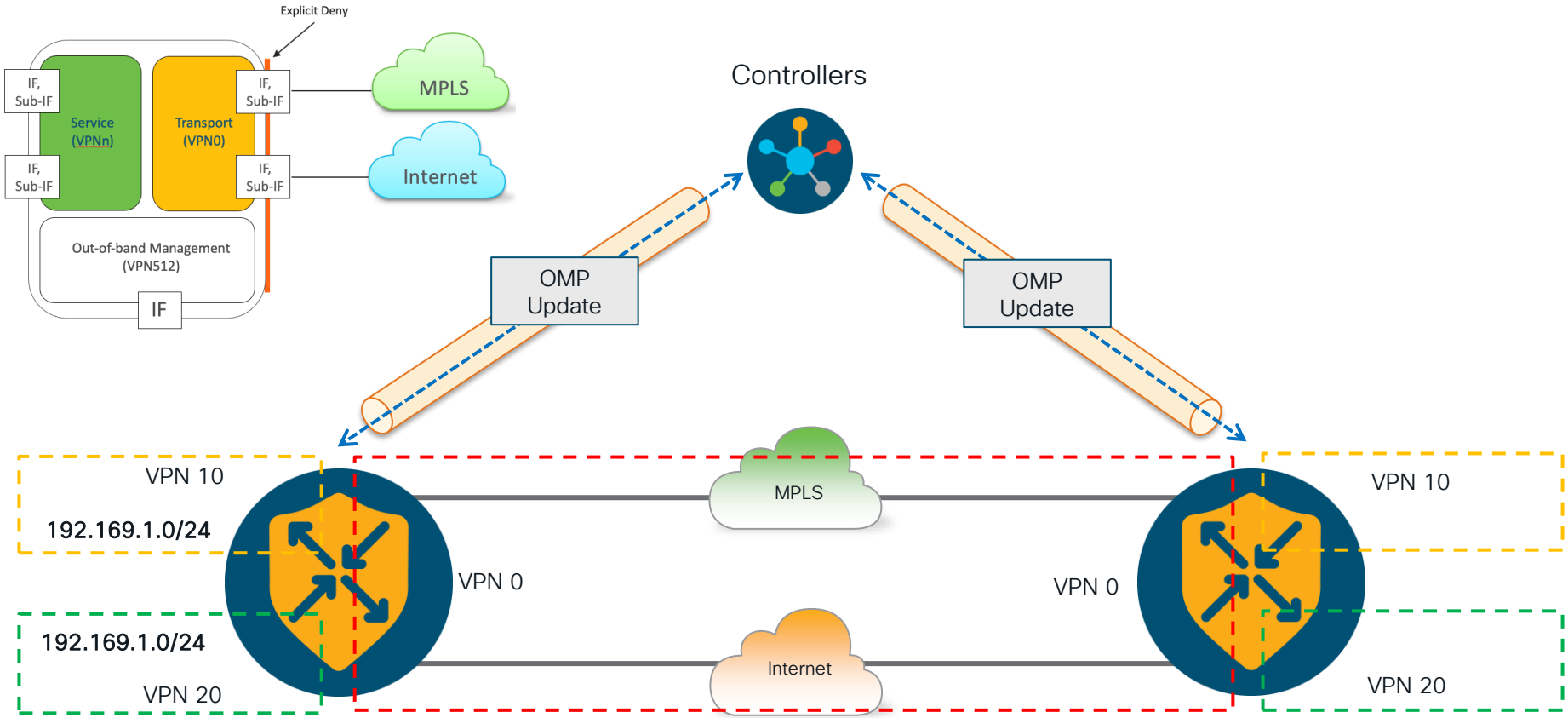
- Path liveliness and quality measurement detection protocol
  - Up/Down, loss/latency/jitter, IPSec tunnel MTU
- Runs between all Secure Edges
  - Inside IPSec tunnels
  - Automatically invoked after each IPSec tunnel establishment
  - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
  - Fully customizable per-Edge, per-color



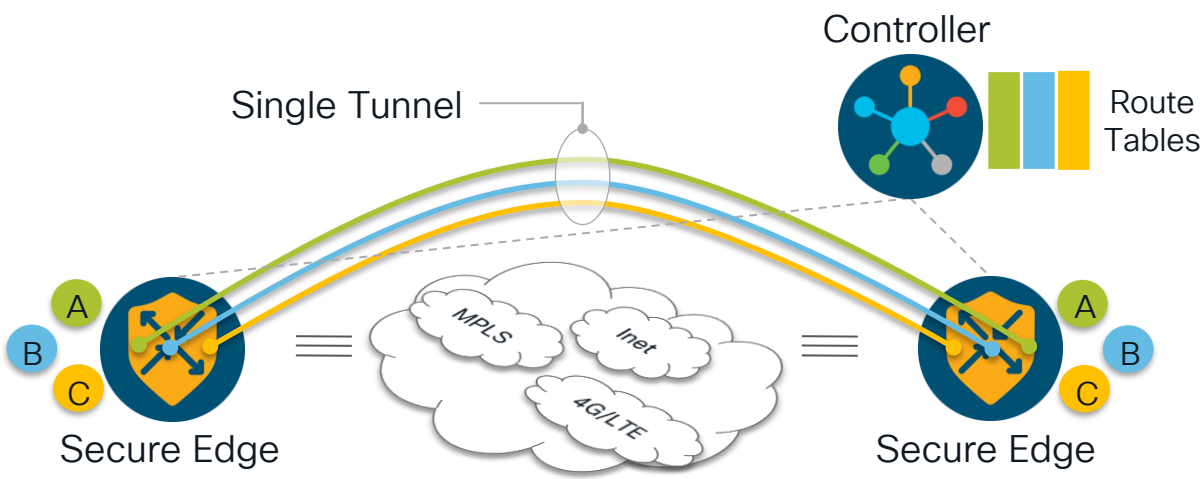
Least Access Principle

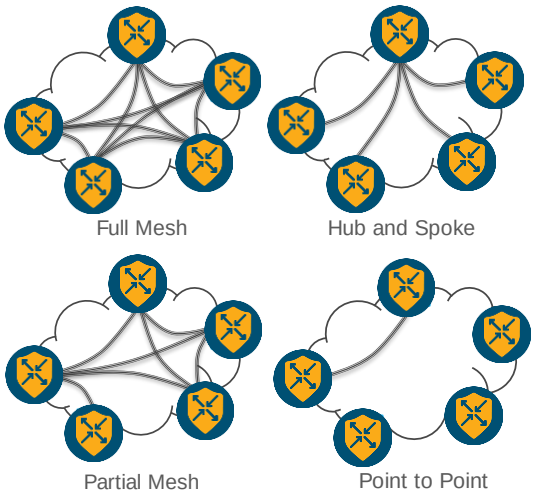
- Segmentation (VRF) - True VRF with separate route table & different topology each VRF
- Overlay Management Protocol (OMP)

End-to-End Segmentation



End-to-End Segmentation with Multi-Topology

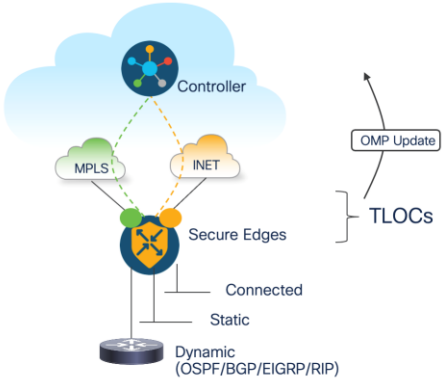




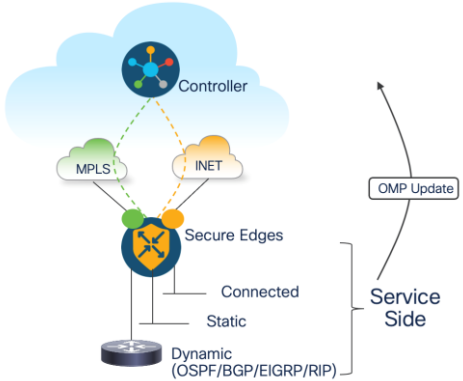
Segment connectivity across the SD-WAN fabric without reliance on underlay transport

Secure Edge maintain per-VPN routing table for complete control plane separation

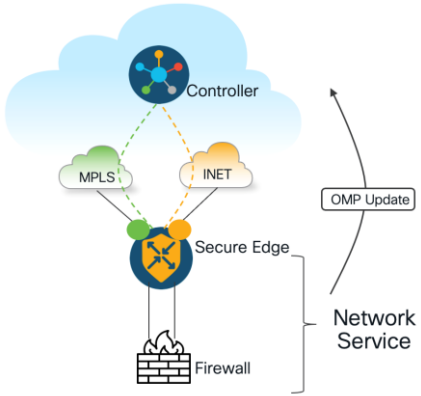
Overlay Management Protocol (OMP)



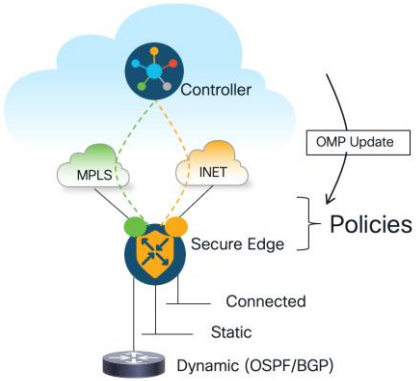
- Routes connecting locations to physical networks
- Advertised to Controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Preference
  - Weight



- Routes learnt from local service side (connected, Static or Dynamic)
- WAN Edge Advertise to Controller
- Controller distribute to other WAN edges
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - VPN-ID
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric



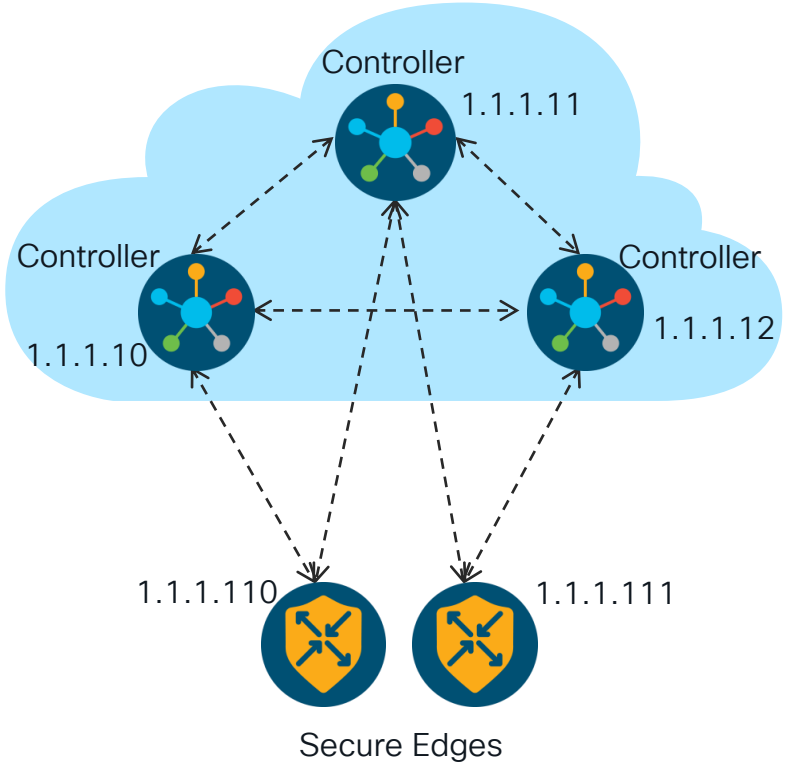
- Routes for advertised network services, i.e. Firewall, IDS, IPS, generic
- Advertised to Controller
- Most prominent attributes:
  - VPN-ID
  - Service-ID
  - Label
  - Originator System IP
  - TLOC



- Polices are configured on Controller
- Data policies are advertised using OMP
- Data policies advertised from Controller to WAN edges in XML format

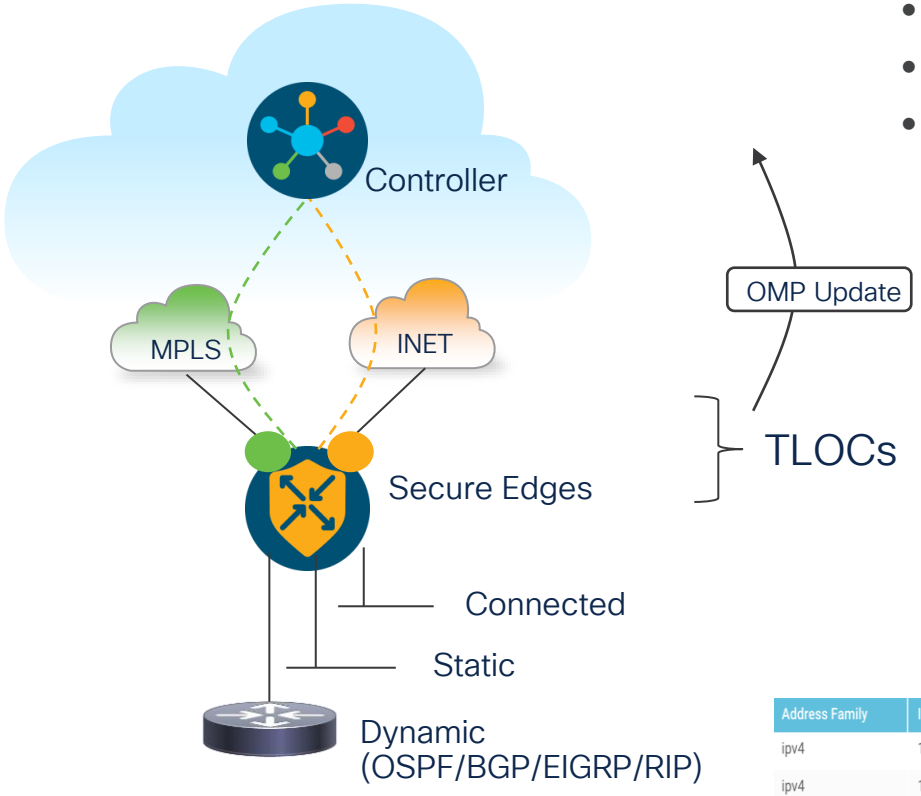
Overlay Management Protocol (OMP)

Overlay Management Protocol (OMP)



- OMP is a TCP based extensible control plane protocol
- Runs between WAN Secure Edges and Controllers and between the Controllers
  - on TLS/DTLS connections
- OMP carries routes, TLOCs, Services and data policies
- Advertises control plane and security context
- Dramatically lowers control plane complexity and raises overall solution scale
- OMP orchestrates routing and secure connectivity between sites

OMP - TLOC Routes

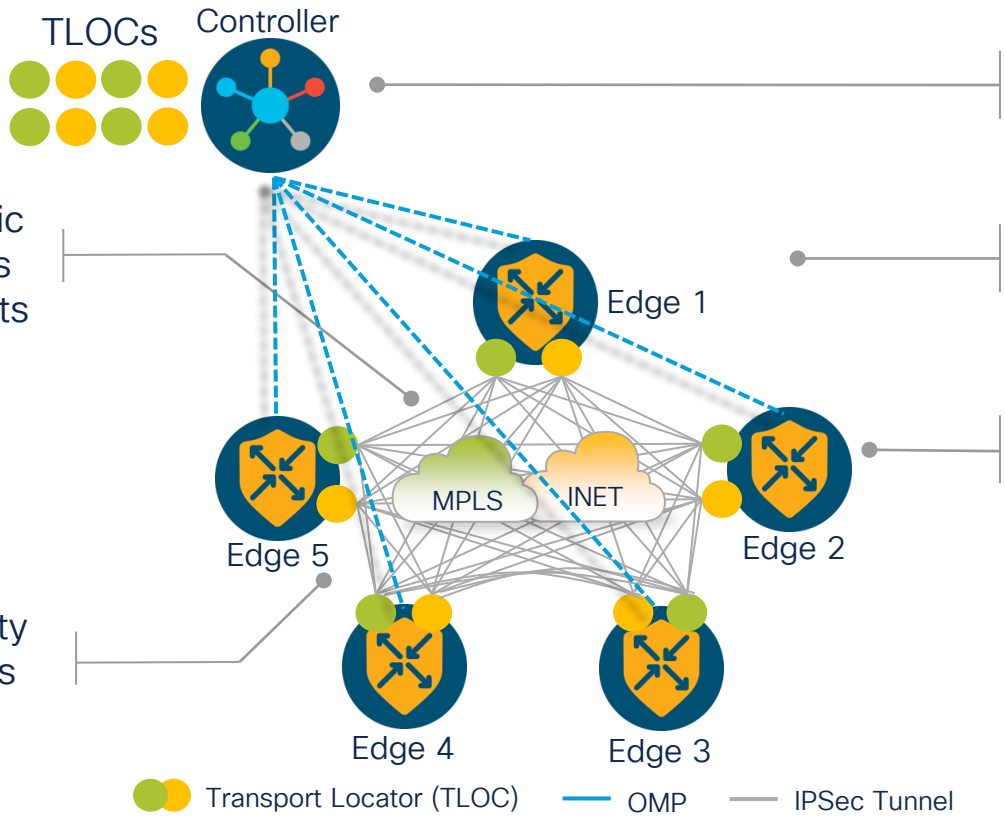


- Routes connecting locations to physical networks
- Advertised to Controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Preference
  - Weight

OMP – Advertised TLOCs

Address Family	IP	Color	Encap	To Peer	Tloc Spi	Auth Type	Encrypt Type	Public IP	Public Port
ipv4	1.1.1.10	public-internet	ipsec	1.1.1.1	292	sha1-hmac a...	des des3	10.1.6.5	12346
ipv4	1.1.1.10	blue	ipsec	1.1.1.1	292	sha1-hmac a...	des des3	10.2.5.5	12346

OMP - TLOC Routes



Controller advertise TLOCs to Edges in OMP TLOC routes

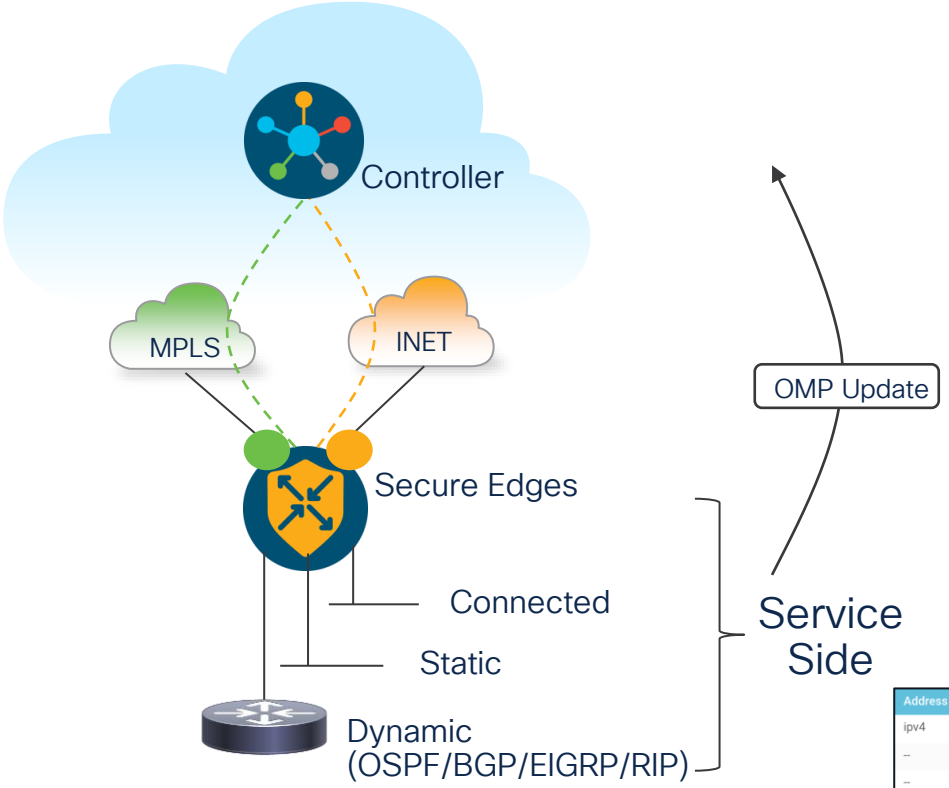
SD-WAN Fabric with TLOCs as tunnel endpoints

TLOCs advertised to Controllers in OMP TLOC routes

Local TLOCs (System IP, Color, Encap Pub IP/Port, Priv IP/Port)

BFD for quality and liveliness detection

OMP - Routes

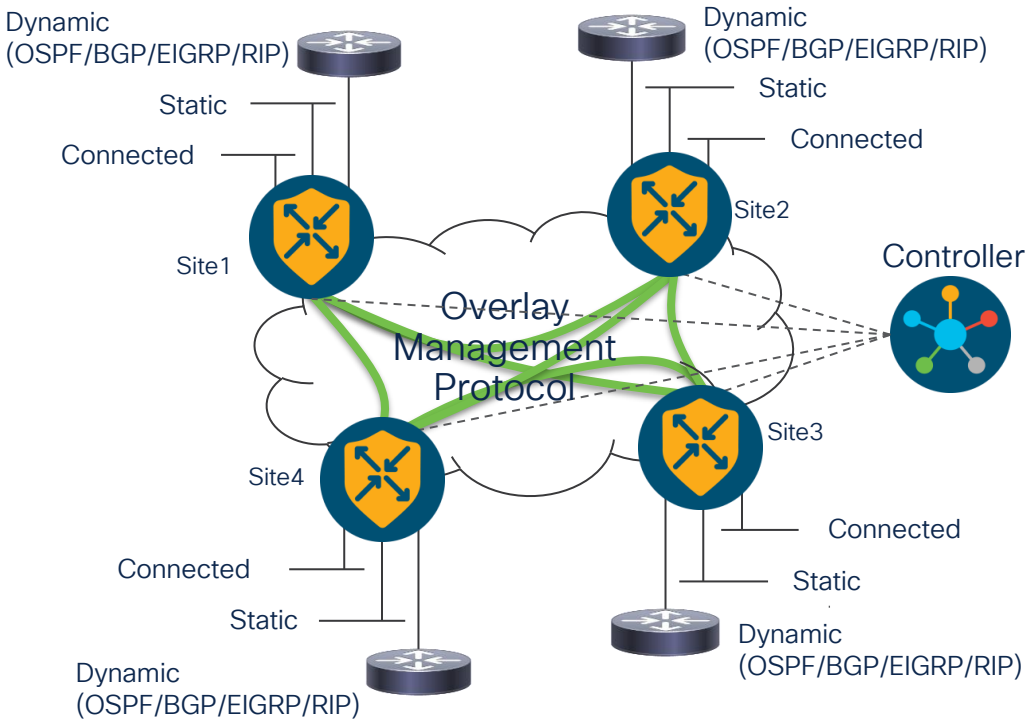


- Routes learnt from local service side (connected, Static or Dynamic)
- WAN Edge Advertise to Controllers
- Controller distribute to other WAN edges
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - VPN-ID
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric

OMP Received Routes

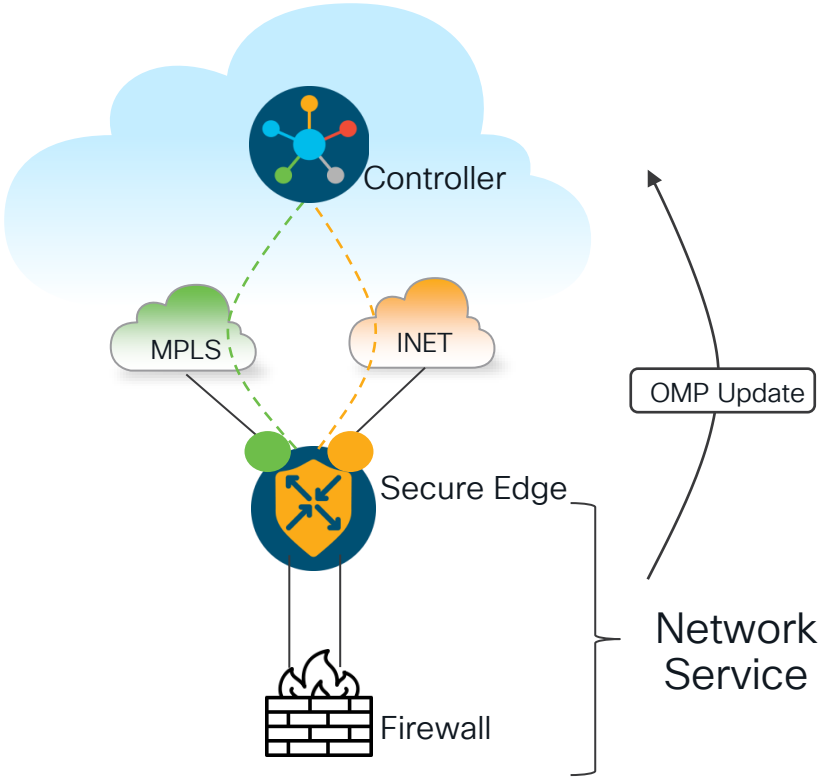
Address Family	VPN ID	Prefix	From Peer	Path Id	Label	Status	Attribute Type	Tloc IP
ipv4	1	172.16.0.0/24	1.1.1.1	3	1002	C I R	installed	1.1.1.11
--	--	--	1.1.1.1	4	1002	C I R	installed	1.1.1.11
--	1	172.16.1.0/24	0.0.0.0	69	1002	C Red R	installed	1.1.1.10
--	--	--	0.0.0.0	74	1002	C Red R	installed	1.1.1.10

OMP - Routes



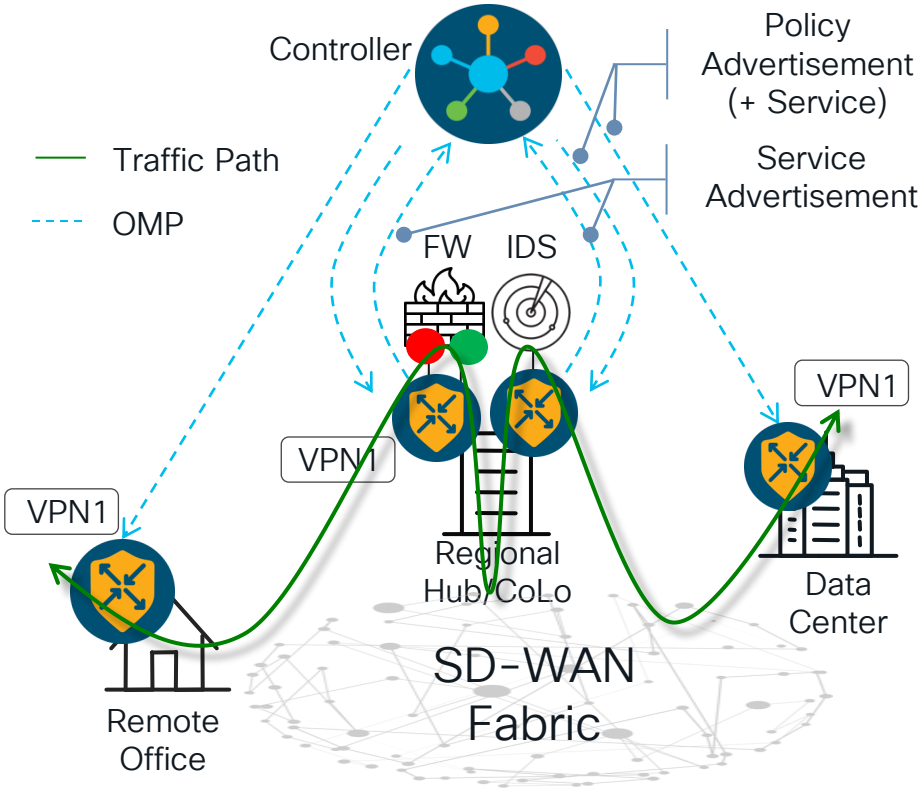
- Uniform control plane protocol
- OMP learns and translates routing information across the overlay
  - OMP routes, TLOC routes, network service routes
  - Unicast and multicast address families
  - IPv4 and IPv6 (future)
- Distribution of data-plane security parameters and policies
- Implementation of control (routing) and VPN membership policies

OMP - Network Service Routes



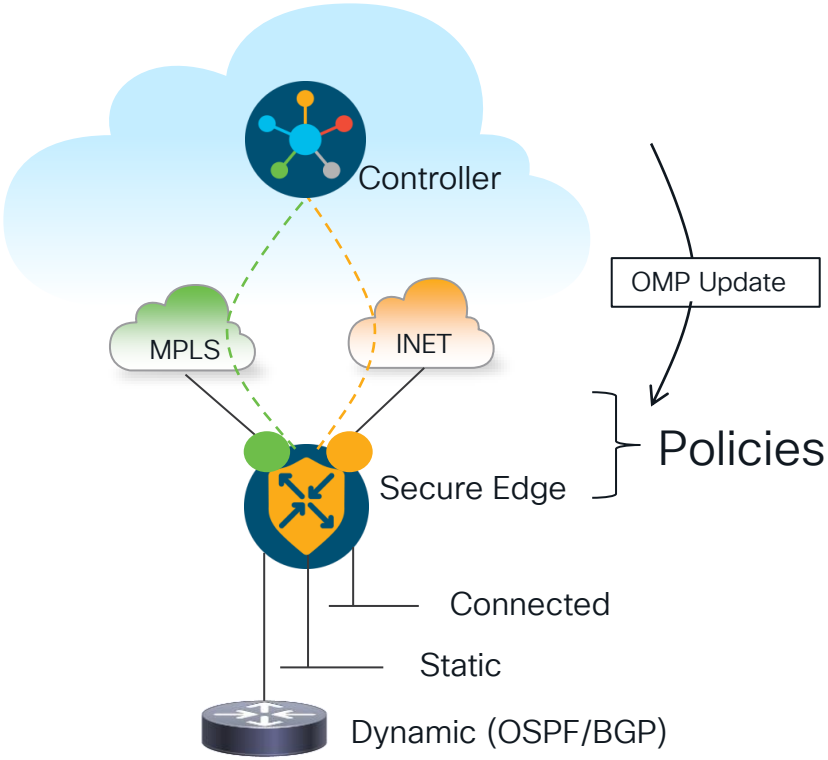
- Secure Edge for advertised network services, i.e. Firewall, IDS, IPS, generic
- Advertised to Controllers
- Most prominent attributes:
  - VPN-ID
  - Service-ID
  - Label
  - Originator System IP
  - TLOC

OMP - Network Service Routes



- Service nodes are connected to Edge
  - Directly or IPSec IKE v1/v2
  - Routed or bridged
- Service nodes can be connected to different Secure Edges
  - Can be in different sites
- Secure Edges advertise service
  - Service route + Service label
  - Specific VPN
- Control or data policies are used to insert the service nodes

OMP - Policies



- Polices are configured on Controller
- Data policies are advertised using OMP
- Data policies advertised from Controller to Secure WAN edges

Wrap-Up

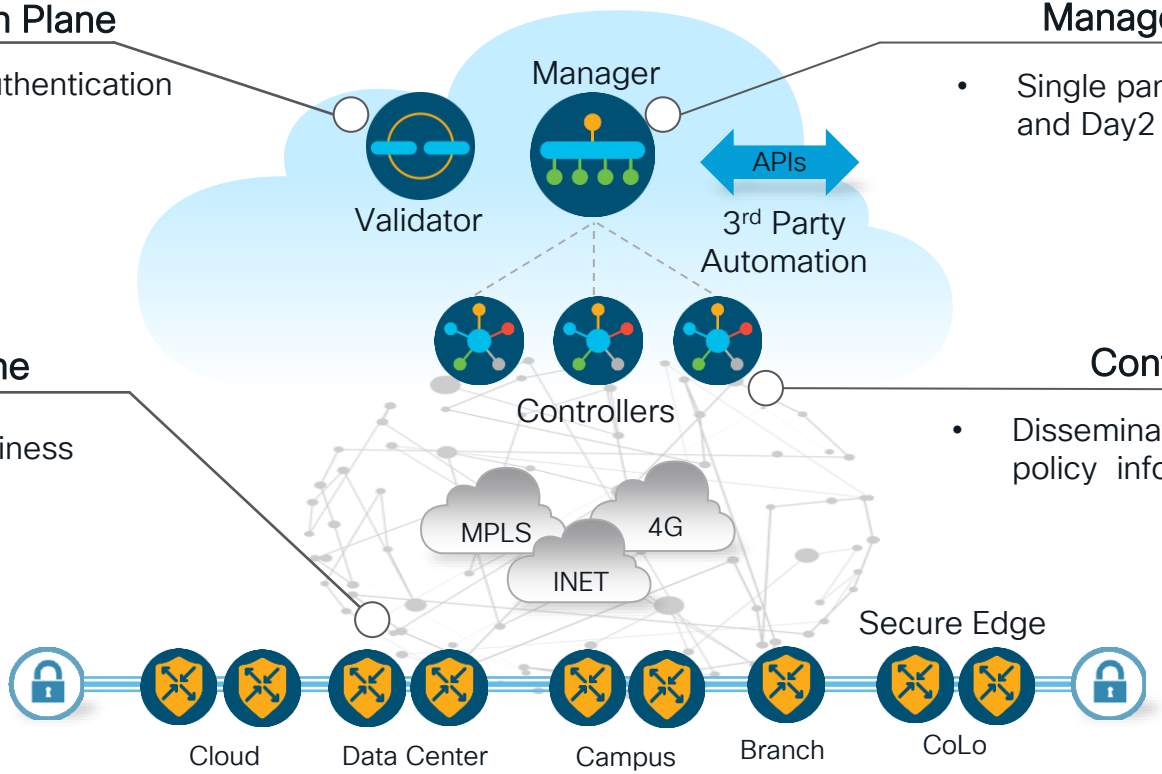
Cisco Catalyst SD-WAN Architecture

Orchestration Plane

- First point of authentication

Management Plane

- Single pane of glass for Day0, Day1 and Day2 operations



Data Plane

- Implements business intent policies

Control Plane

- Disseminates control plane and policy information between Edges

Catalyst SD-WAN Security Fundamentals

Secure Edge Parameter Protection

- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- Trust Anchor Module (TAm)
- Secure Boot of Signed Images
- Runtime Defenses (RTD)

Onboarding & Authentication

- Devices Onboarding Process
- Zero Trust
- Certificate-based Authentication & Whitelisting
- Automate Custom Certificate Authority (CA)
- Management through using SD-WAN Manager

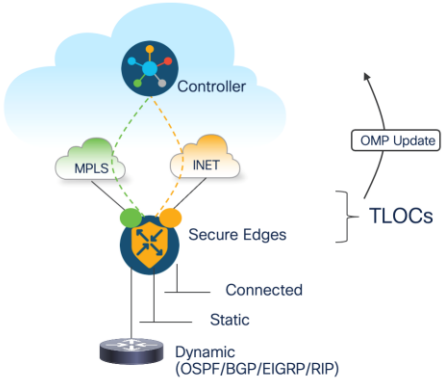
Transport Security

- IKE less IPsec (Key exchange using a controller, high scale)
- Key - Using RNG (NIST SP 800-90A)
- Key Rotation - 24hr Default
- Anti-Replay Protection

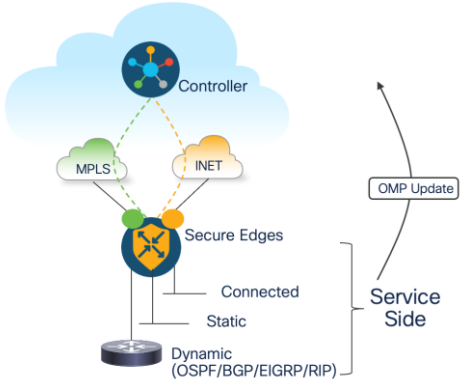
Least Access Principle

- Segmentation (VRF) - True VRF with separate route table & different topology each VRF
- Overlay Management Protocol (OMP)

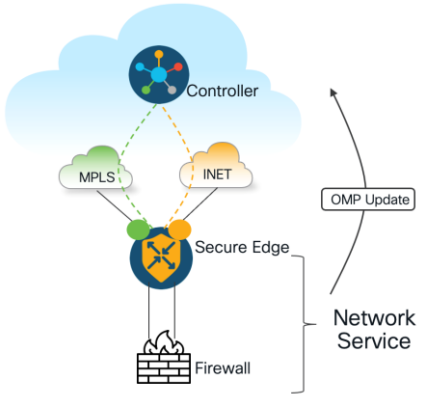
Overlay Management Protocol (OMP)



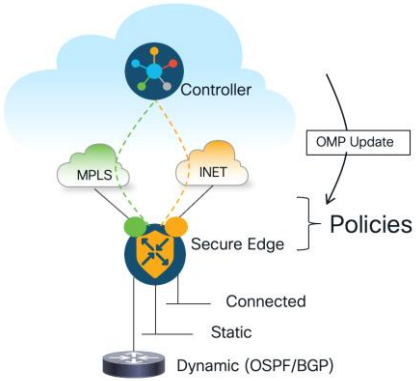
- Routes connecting locations to physical networks
- Advertised to Controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Preference
  - Weight



- Routes learnt from local service side (connected, Static or Dynamic)
- WAN Edge Advertise to Controller
- Controller distribute to other WAN edges
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - VPN-ID
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric



- Routes for advertised network services, i.e. Firewall, IDS, IPS, generic
- Advertised to Controller
- Most prominent attributes:
  - VPN-ID
  - Service-ID
  - Label
  - Originator System IP
  - TLOC



- Polices are configured on Controller
- Data policies are advertised using OMP
- Data policies advertised from Controller to WAN edges in XML format

cisco Live!

Did you know?

You can have a one-on-one session with a technical expert!

Visit Meet the Expert in The HUB to meet, greet, whiteboard & gain insights about your unique questions with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am - 4:00pm**
Friday	**10:30am - 1:30pm**

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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!

Let's go