cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Securing End-to-End from Campus and Branch to Cloud with Catalyst 9k

IPsec and MACsec

Raj Kumar Goli, Technical Marketing Engineer

BRKENS-3094

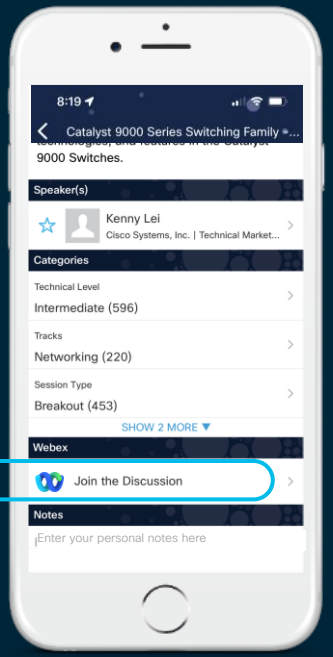
Cisco Webex App

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



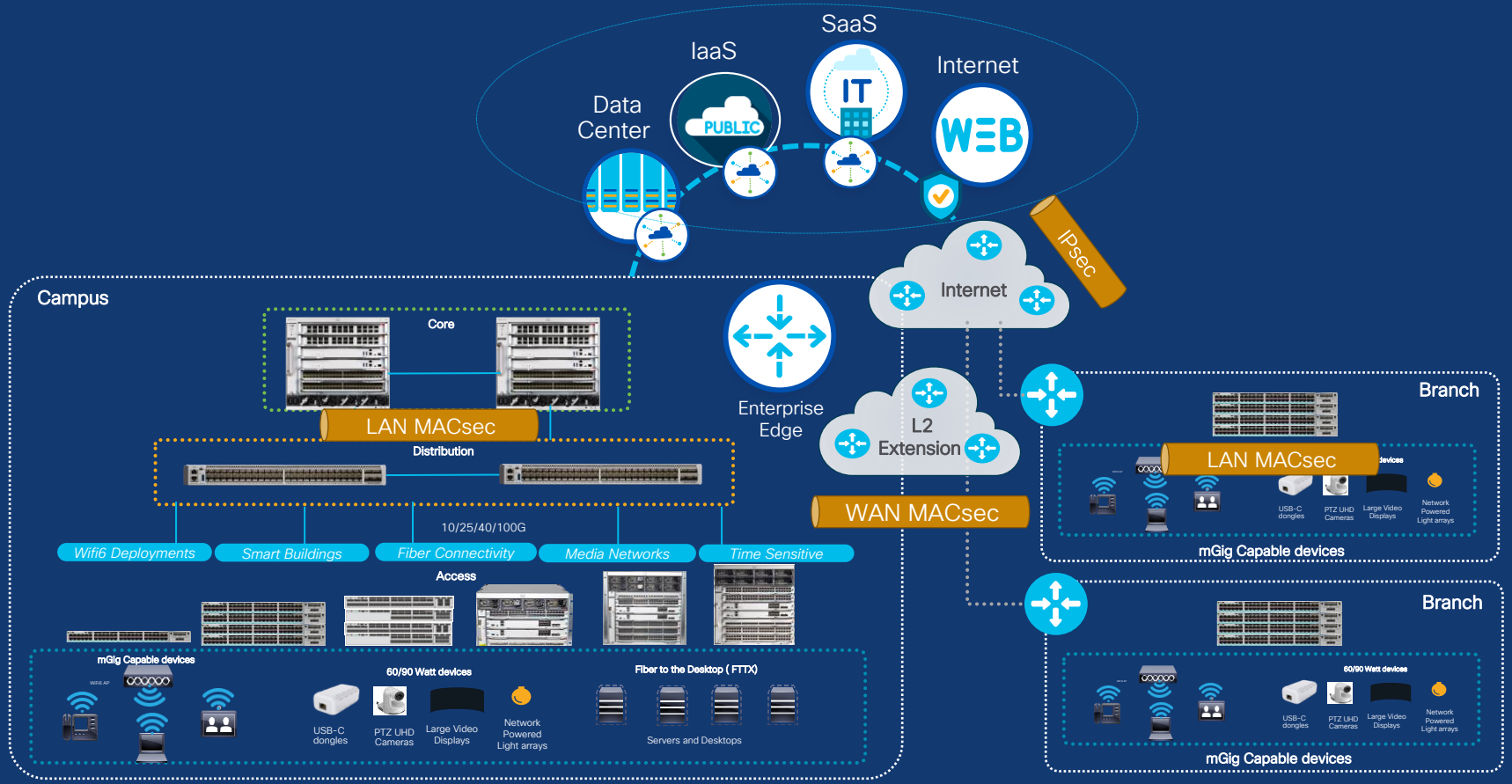
https://ciscolive.ciscoevents.com/ciscolivebot/#BRBRKENS-3094

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda

- Securing LAN with MACsec
- IPsec Overview on Cat9k
- IPsec Use Cases
- WAN MACsec Introduction and Use Cases

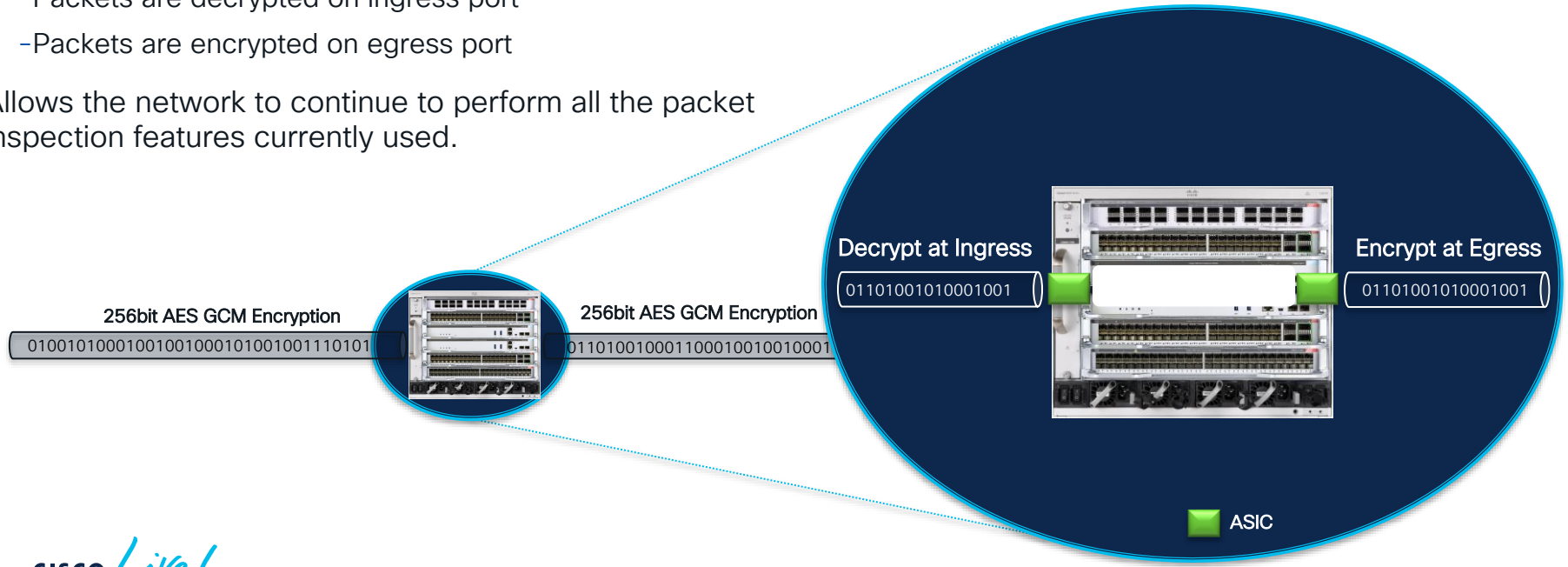
End-to-End Security for Campus



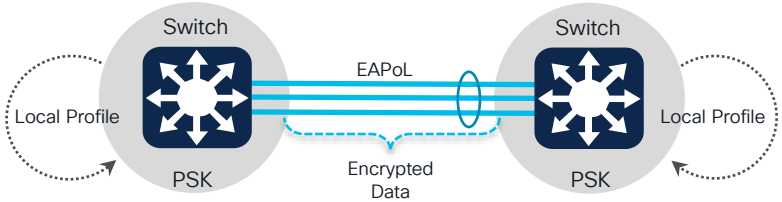
What is MAC Security (MACsec)?

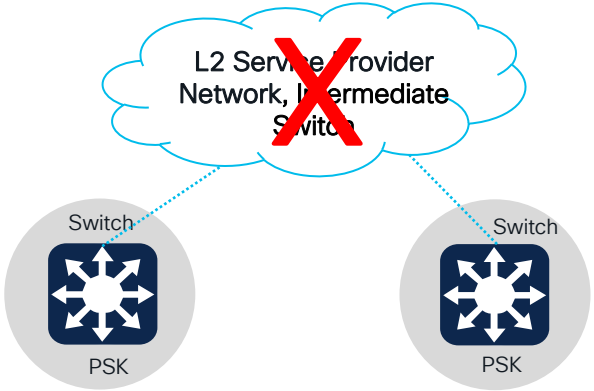
Hop-by-Hop Encryption via IEEE802.1AE

- Hop-by-Hop vs End-to-End “Bump-in-the-wire” model
  - Packets are decrypted on ingress port
  - Packets are encrypted on egress port
- Allows the network to continue to perform all the packet inspection features currently used.



MACsec Switch to Switch Topology



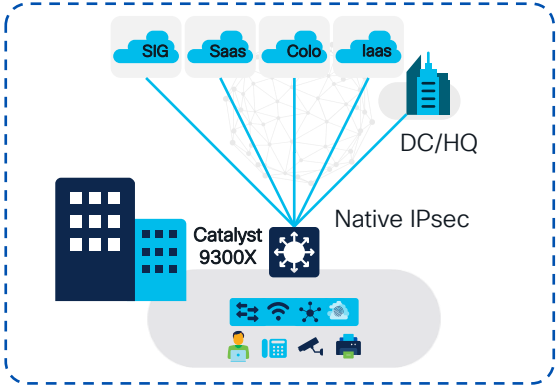


IP Security

Catalyst 9300X – Purpose built for the new edge

Software
Cisco IOS® XE 17.6.2
With Cisco DNA Advantage
(HSEC key for export control)

Cisco Catalyst 9300X



Encryption	Authentication
AES-128-CBC	HMAC/SHA1
AES-128/256-GCM	GMAC

Tunnel mode

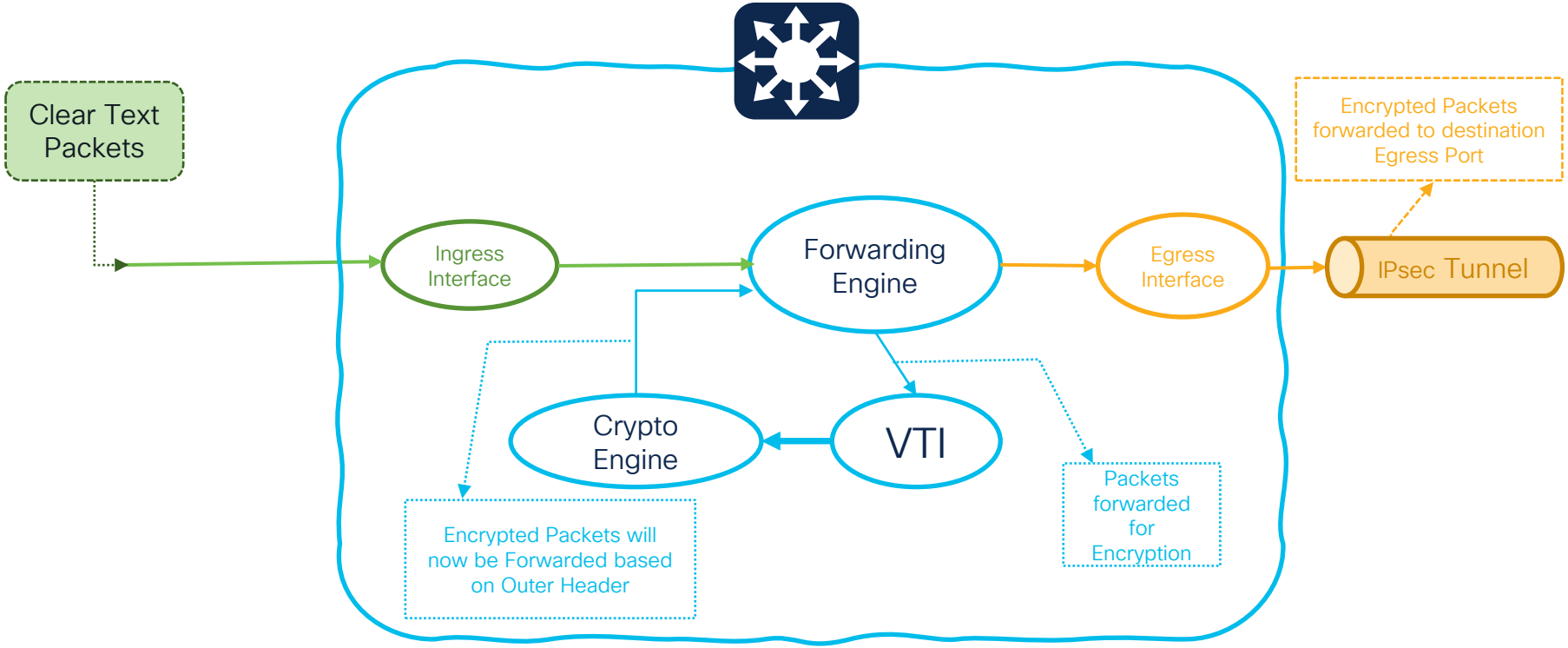
Encapsulation – ESP

IKEv2

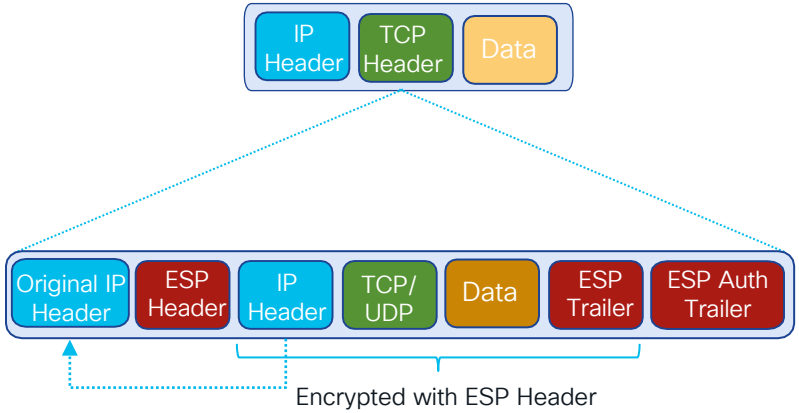
- Static virtual tunnel interface
- IPv4/IPv6
- OSPF/BGP
- Policy Based Routing
- Multicast Routing
- NAT traversal*
- Layer 3 segmentation over IPsec*
- Layer 2 extension over IPsec*

* Roadmap.

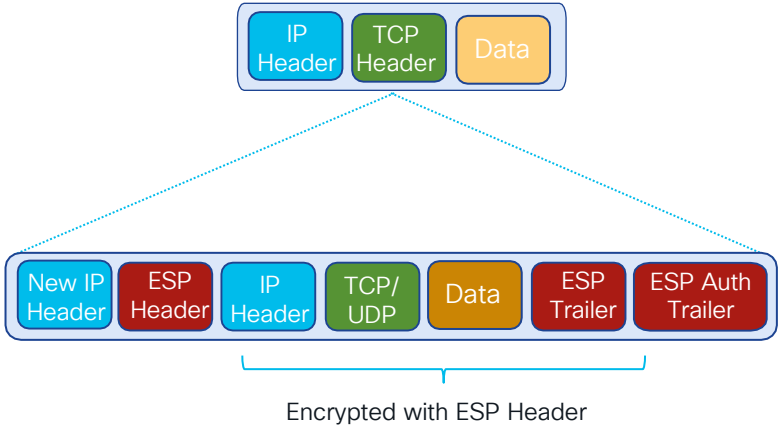
IPsec Packet Flow – Encryption



Transport Mode



Tunnel Mode



Supported IKEv2 Proposal (Software)

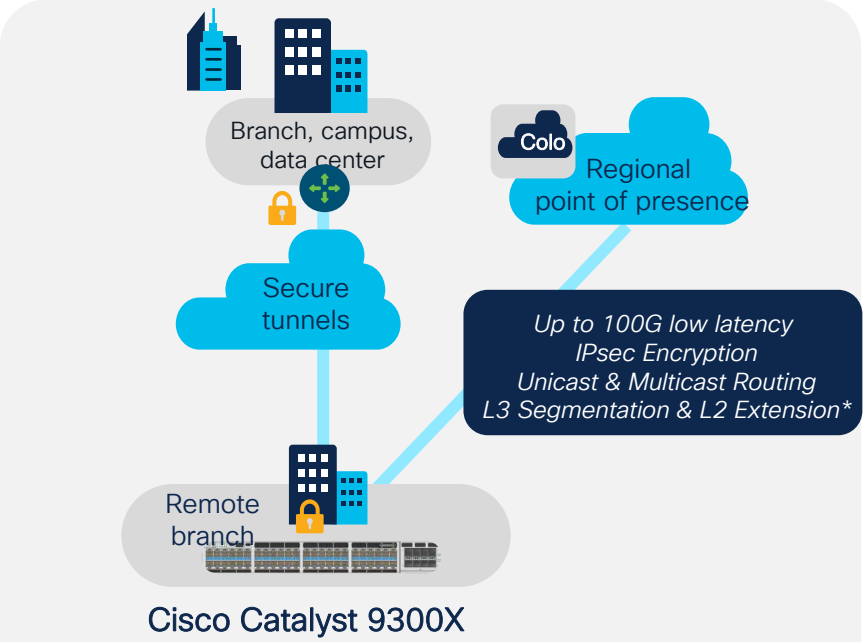
IKE	Encryption	Integrity	Deffie Helman
IKEv2	des 3des aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-gcm-128 aes-gcm-256	md5 sha1 sha256 sha384 sha512	1 – 768 MODP 2 – 1024 MODP 5 – 1536 MODP 14 – 2048 MODP 15 – 3072 MODP 16 – 4096 MODP 19 – 256 ECP 20 – 384 ECP 21 – 521 ECP 24 – 2048 (256 sub groups) MODP

Supported Transform Sets (Hardware)

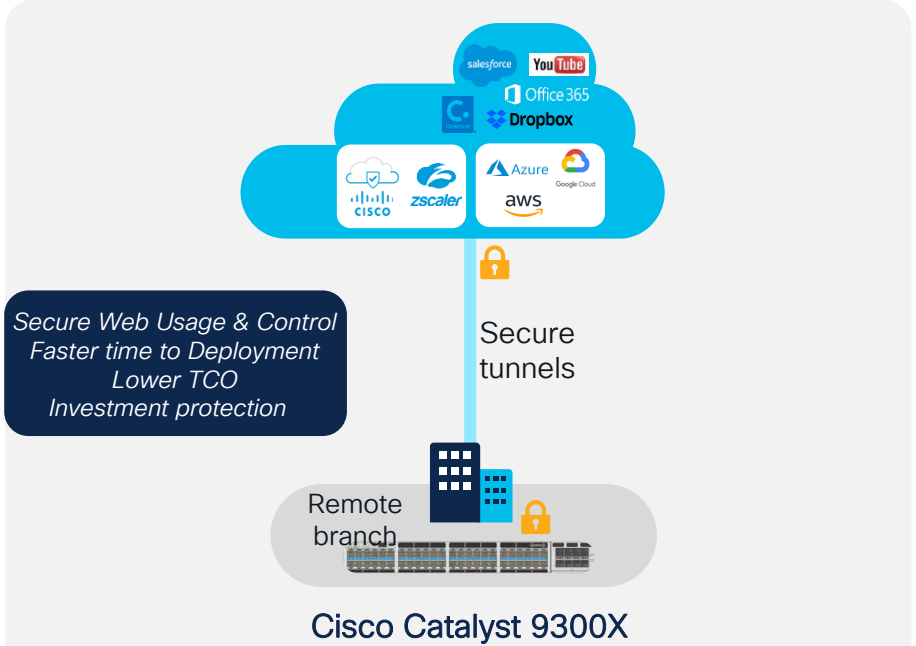
Transform SET (HW) Encryption	Bandwidth
esp-aes + esp-sha-hmac	Upto 15 Gbps
esp-gcm 128 (gmac is derived)	Upto 100 Gbps
esp-gcm 256 (gmac is derived)	Upto 100 Gbps

Catalyst 9300X – Purpose built for the **New Edge**

Secure connectivity to anywhere

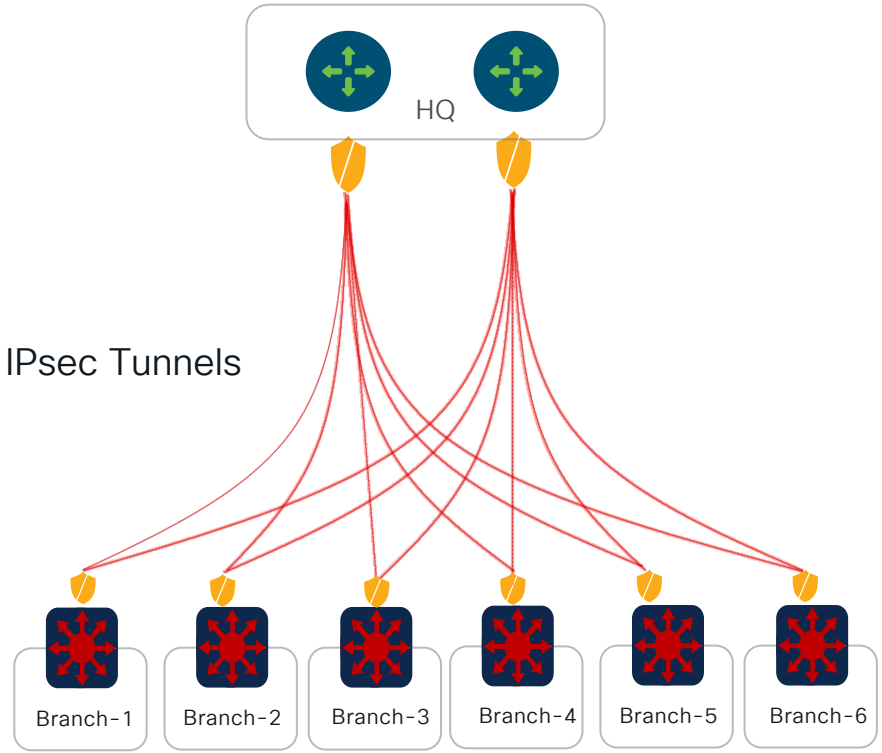


Site to site
100G line-rate IPsec encryption with low-latency forwarding



Site to cloud
Standards-based IPsec for secure direct internet access and cloud-native workloads

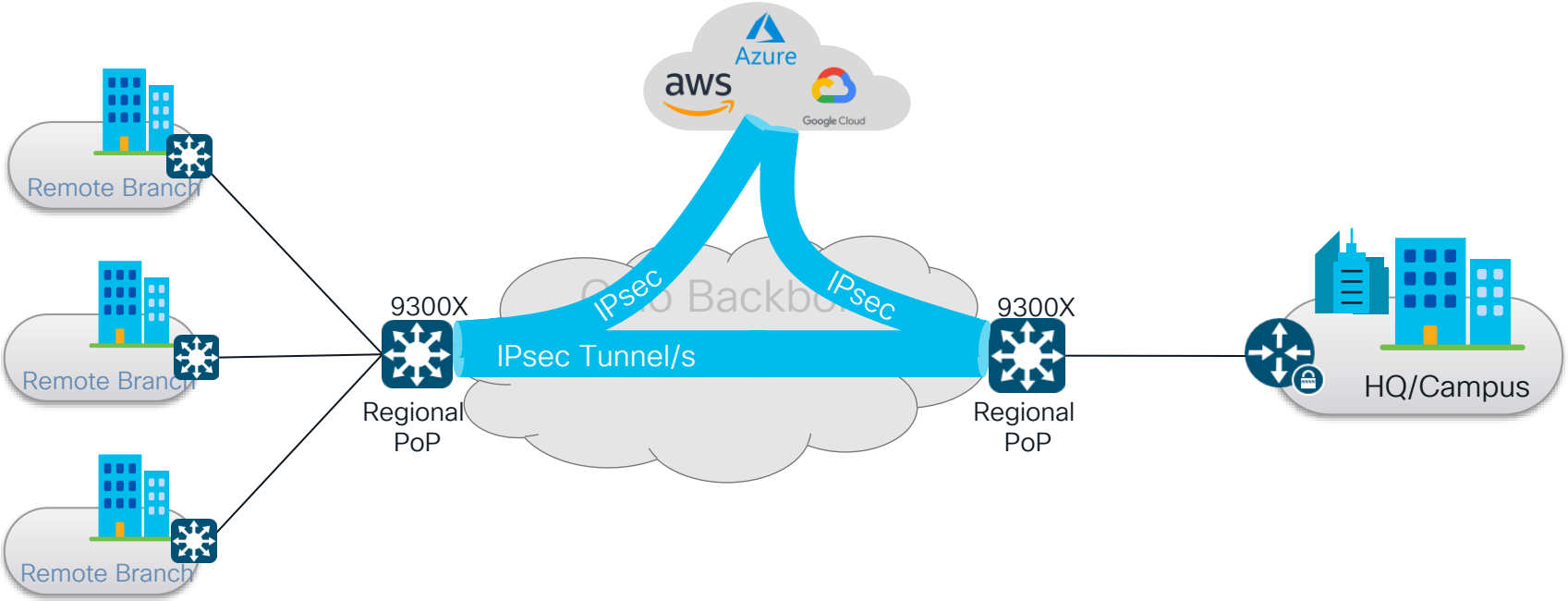
Catalyst 9300X – Site-to-Site IPsec



- High Speed Secure Connectivity
- OSPF/BGP
- Multicast Routing
- IPv4/IPv6
- L3 segmentation over IPSEC*
- L2 Extension over IPSEC*

* 17.9.1

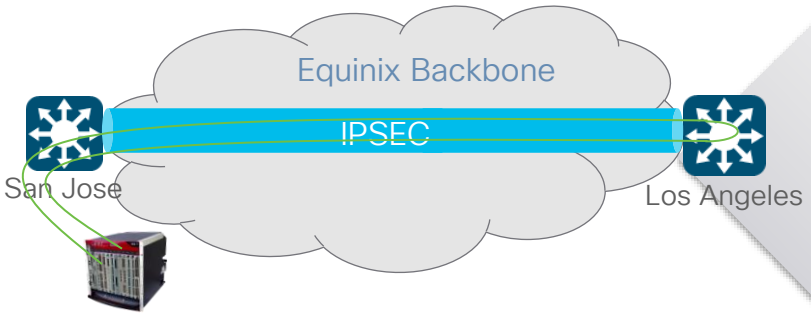
IPsec Colo Connectivity



Key Benefits

- Up to 100G IPsec throughput
- pay-as-you grow model
- Incremental transition to Cloud Infrastructure

C9300X IPsec Colo Connectivity



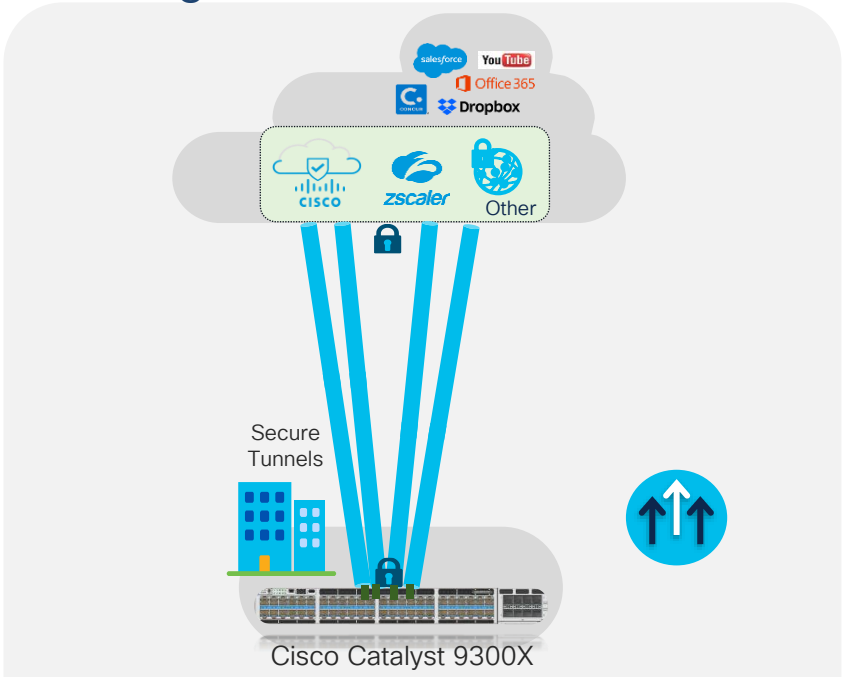
Tunnels	Packet Sizes	Throughput	Avg Latency		Min Latency		Max Latency	
			Base	IPsec	Base	IPsec	Base	IPsec
1	100	6.5	8.355	8.365	8.352	8.361	8.372	8.380
1	256	8.0	8.360	8.368	8.357	8.364	8.373	8.381
1	512	9.0	8.366	8.374	8.363	8.371	8.380	8.392
1	1024	9.4	8.373	8.380	8.370	8.377	8.386	8.393
1	1400	9.4	8.379	8.386	8.376	8.383	8.391	8.399
1	2048	9.4	8.385	8.392	8.382	8.389	8.401	8.412
1	9000	9.4	8.487	8.496	8.484	8.493	8.505	8.514

Consistent latency with/without IPsec encryption/decryption

- Less than 1ms difference with/without encryption/decryption
- Multicast and Unicast traffic deliver the same results
- Consistent results for IPv4, IPv6, and IPv4 over IPv6, and IPv6 over IPv4

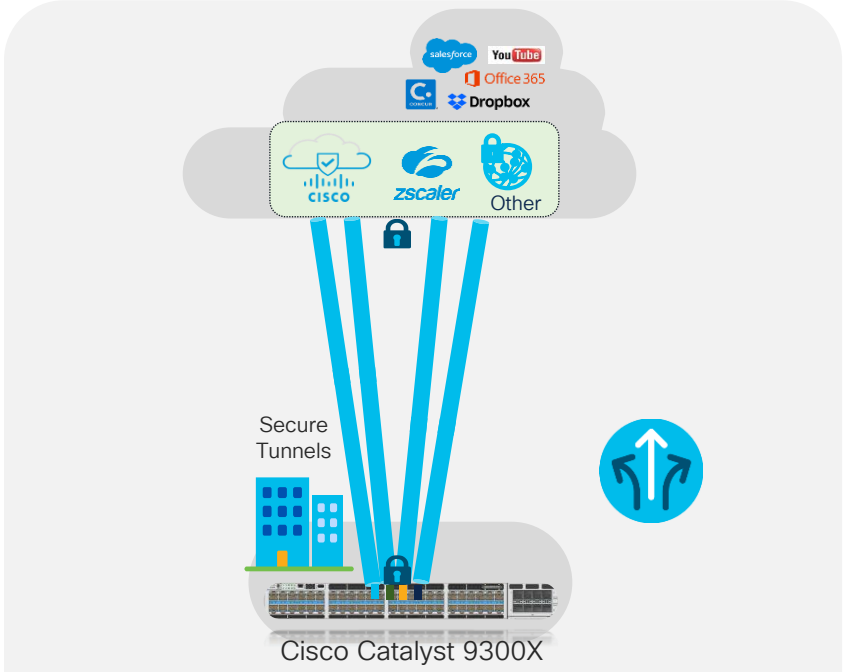
Site-to-Cloud: Secure Internet Gateway

Securing Internet Traffic



Redirect all Internet bound Traffic

ECMP via Multiple Tunnels | *Active/Active*

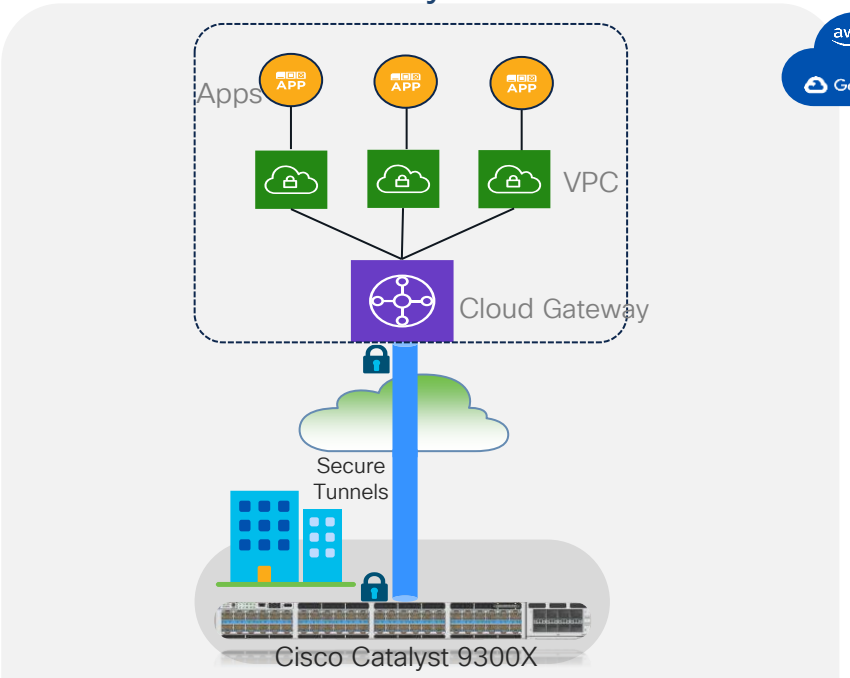


Selective Traffic forwarding

Policy Based Routing | *Set interface* | *Active/Backup*

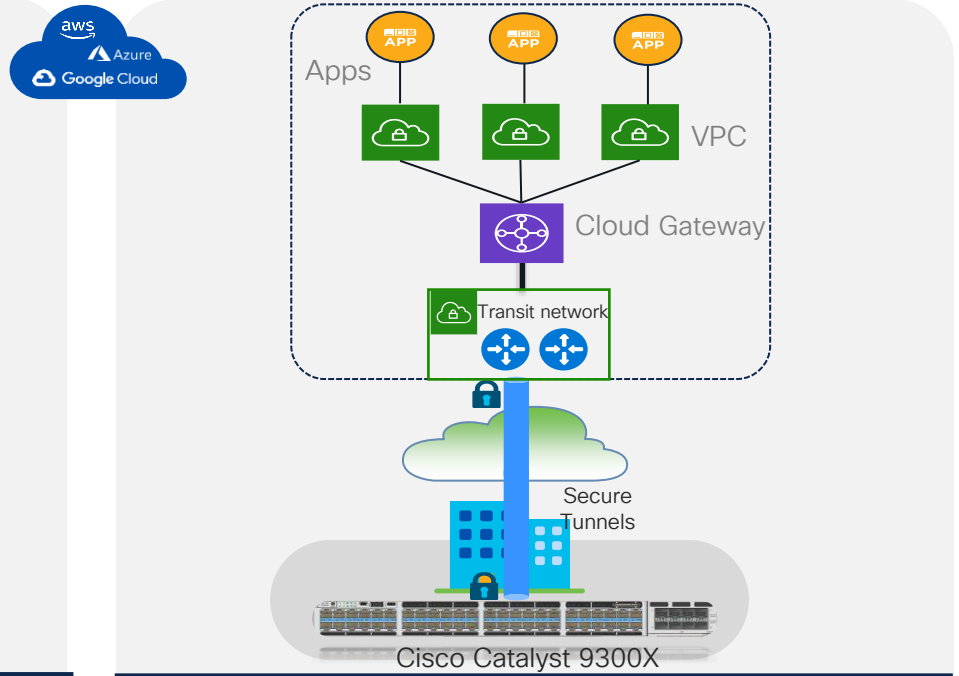
Site-to-Cloud: Cloud Service Providers

Secure connectivity to Native Cloud Resources



Native IPSEC termination on CSP's

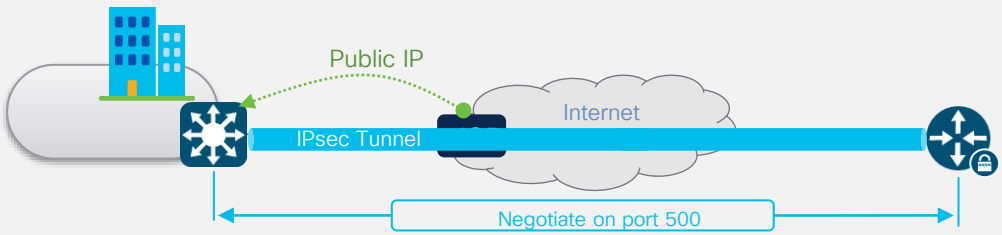
Static/BGP | Active/Backup | Active/Active



IPSEC termination on CSP's Transit Networks

Static/BGP | Active/Backup | Active/Active

IPsec NAT Traversal

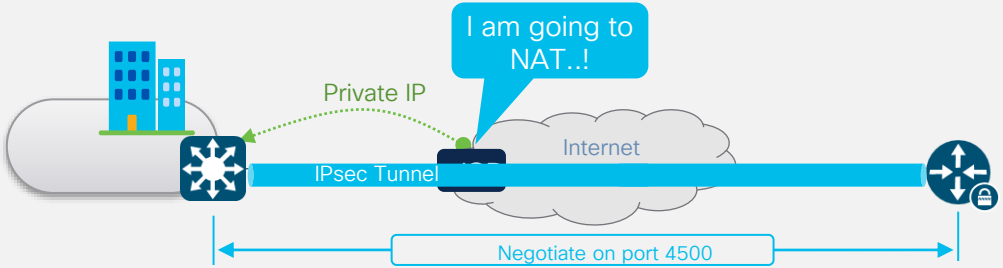


Without NAT-T

- Source or Destination are not natted
- IPsec negotiated on port 500

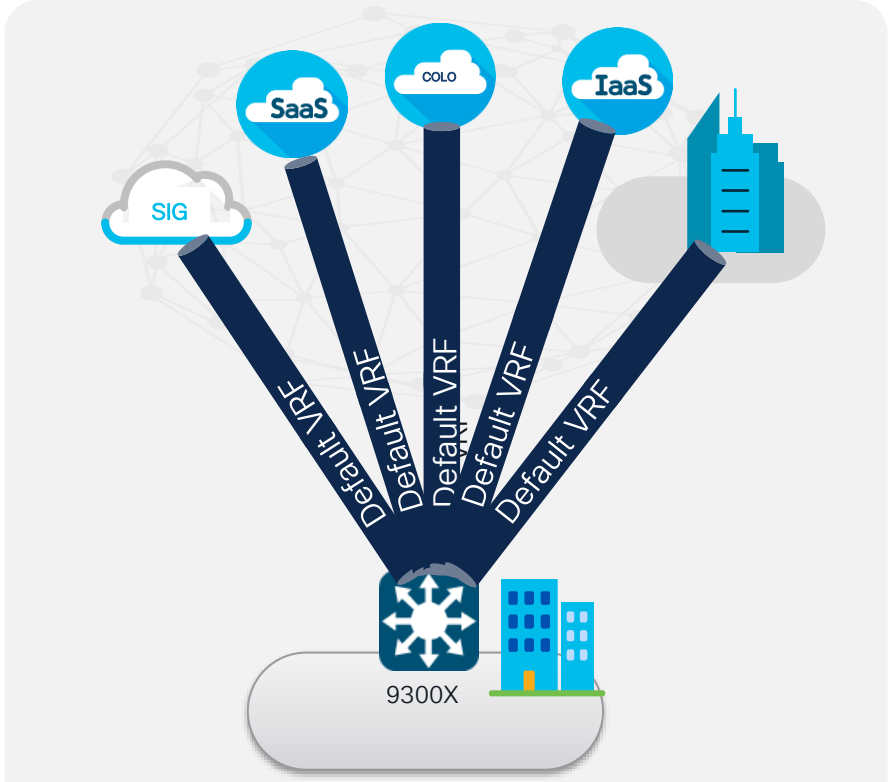
With NAT-T*

- Source or Destination can be natted
- Upon NAT detection, IPsec can be negotiated on port 4500

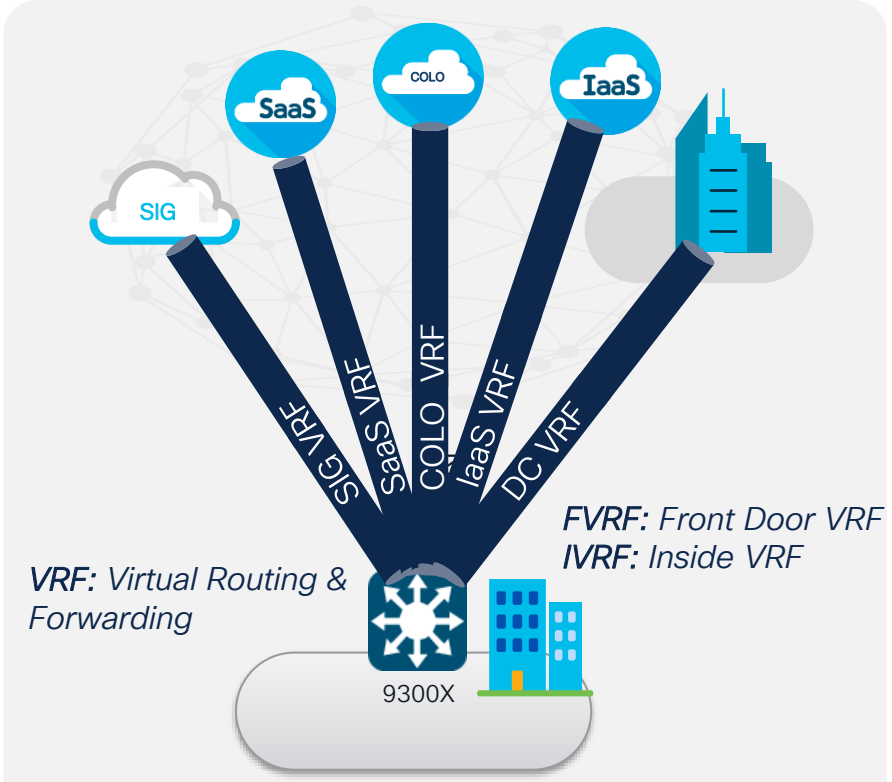


* - 17.9.1

VRF Aware IPsec



Prior to 17.9.1

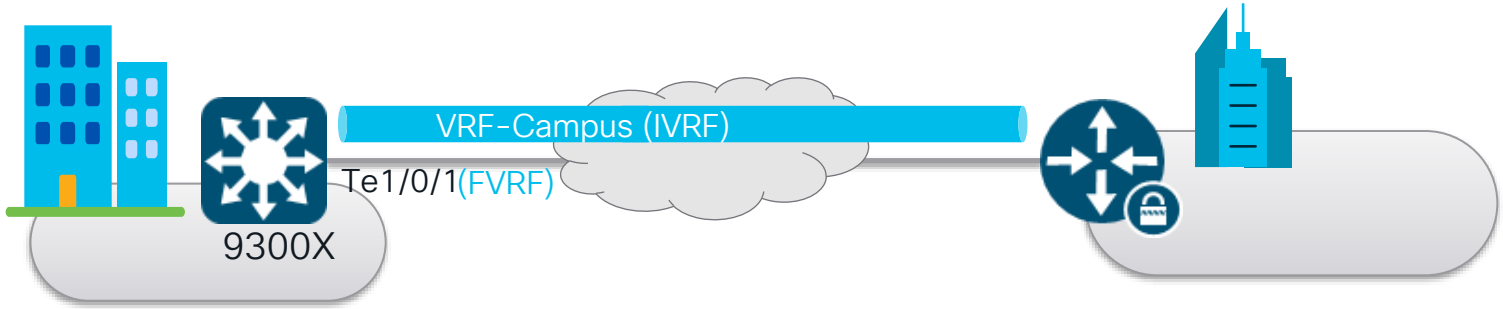


VRF: *Virtual Routing & Forwarding*

FVRF: *Front Door VRF*
IVRF: *Inside VRF*

VRF aware IPSEC (17.9.1)

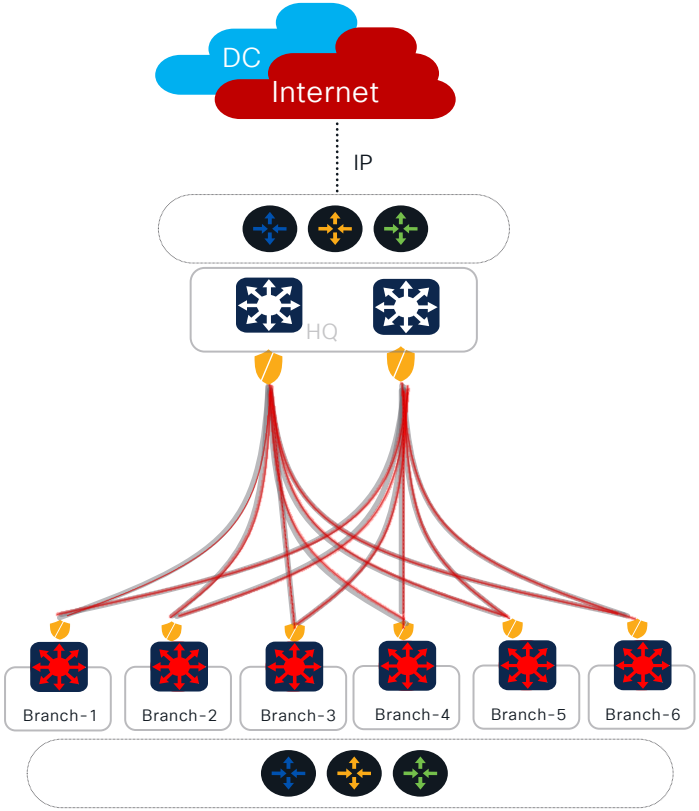
VRF Aware IPsec



VRF	FVRF	IVRF
FVRF vrf definition WAN1-VRF address-family ipv4 address-family ipv6 IVRF vrf definition Campus address-family ipv4 address-family ipv6	int Te1/0/1 ip add 128.107.251.22 255.255.25 vrf forwarding WAN1-VRF	interface Tunnel4 vrf forwarding Campus ip unnumbered Te1/0/1 tunnel source Te1/0/1 tunnel mode ipsec ipv4 tunnel destination 146.112.83.8 tunnel vrf WAN1-VRF tunnel protection ipsec profile prf_umb

BGP EVPN over IPsec

Secure Fabric



Scale and Performance Matrix

IPsec		EVPN	
Tunnel	128	Peers	128
SA	256	VRF | L3VNI	256
Performance	100Gbps	Unicast Prefix	39000

Ingress Replication	
Layer 2 Extension	BGP EVPN
Layer 3 Overlay	BGP EVPN
Underlay-1	OSPF/BGP
Secure Overlay	IPsec

Key Benefits

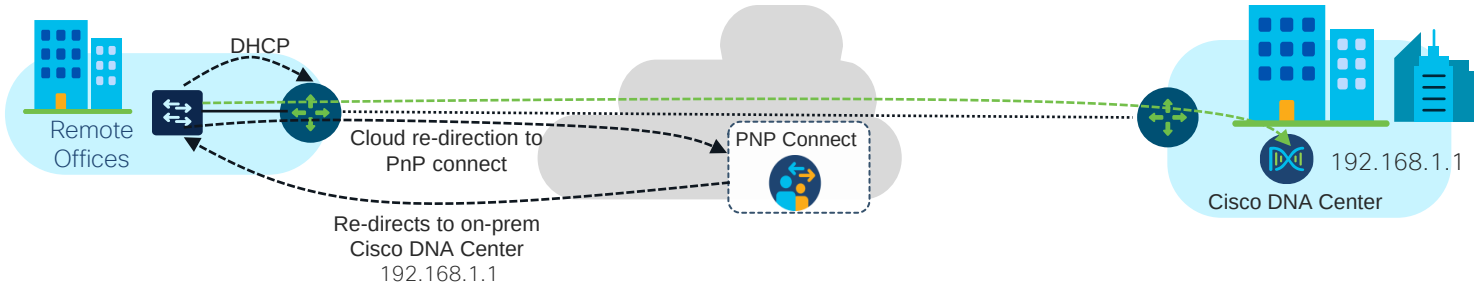
- Scalable Segmentation over IPSEC
- Secure End-to-End Fabric

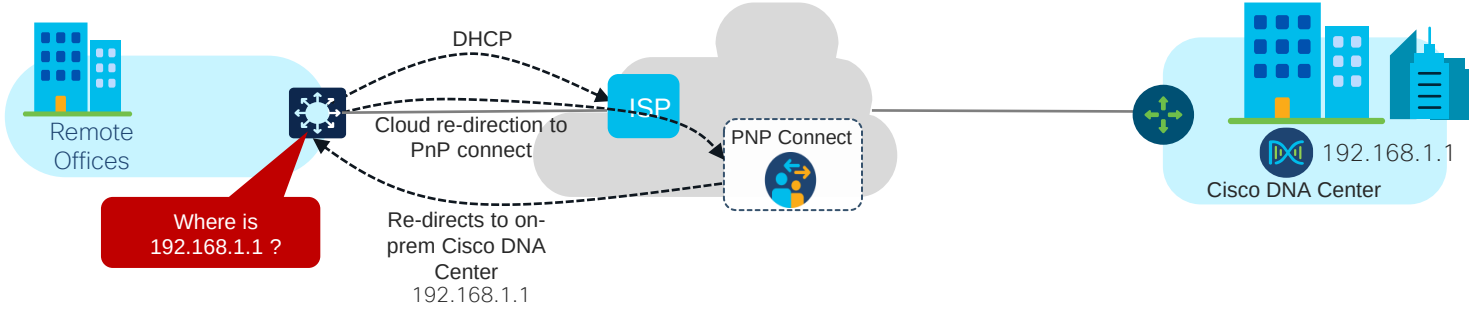
Catalyst 9k Edge – Automation & Monitoring

*17.9.1
*DNAC: 2.3.4

	Turnkey*	DIY
Day 0: Onboarding	DNA Center	ZTP
Day 1: Tunnel Provisioning	DNA Center	NETCONF/RESTCONF, Python, Ansible, Terraform, CLI
Day N: Tunnel Monitoring	DNA Center	SNMP, Telemetry

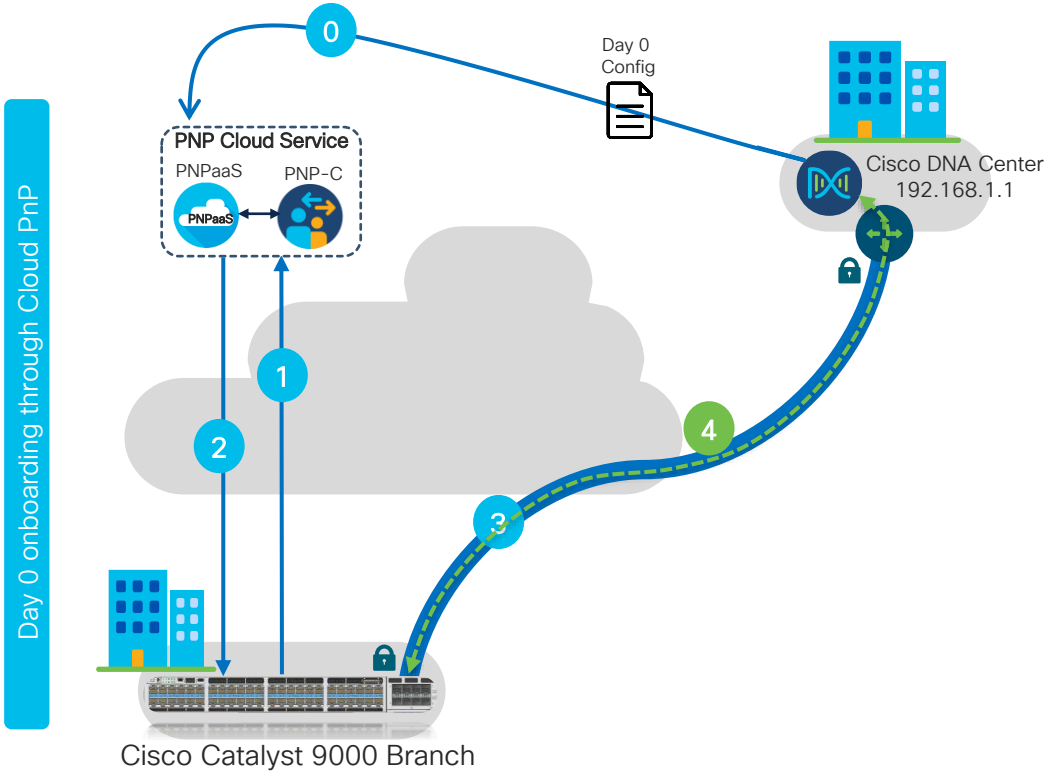
Day 0 On-boarding Challenges





Problem: No connectivity to On-Prem DNA Center

Day 0 Automation Workflow for Cat9k Edge



0 Cisco DNAC uploads Day 0 config to PnPaas

1 C9KEdge sends PnP Connect request

2 PnPaas provisions Day 0 Config

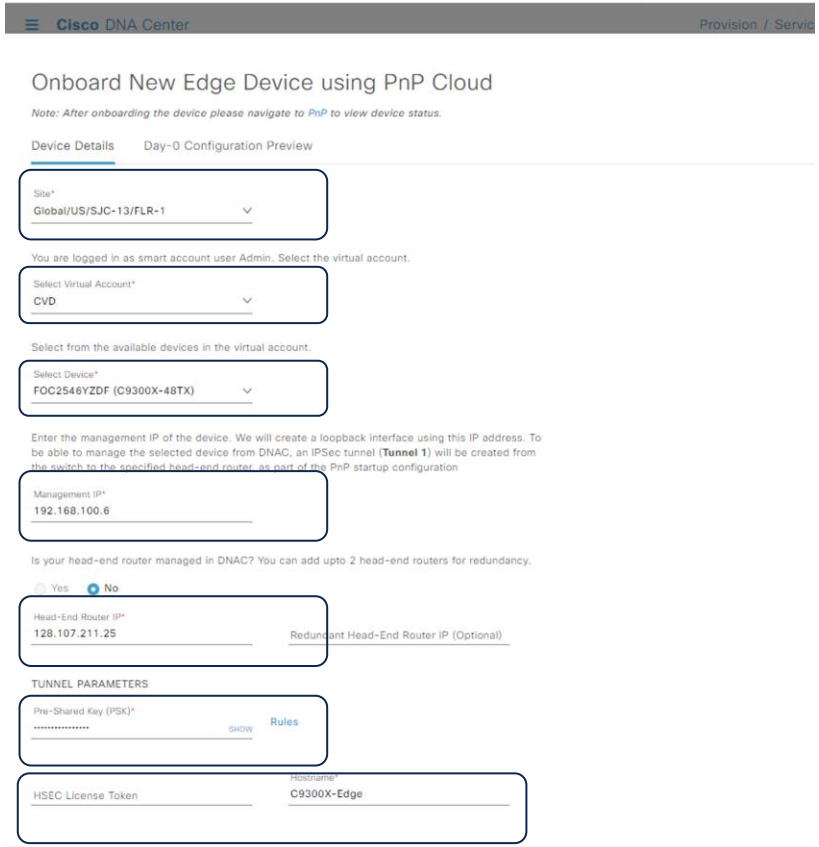
3 C9KEdge forms a tunnel to Corp DC

4 C9KEdge is managed via DNA Center

Day 0: Secure Automatic Provisioning

Day N Automation Workflow for Cat9k Edge

Day N Automate Secure tunnels via DNA Center



1. Choose your site
2. Select a SA/VA
3. Pick the SN of the device
4. Assign a Management IP
5. Choose Head End Router
6. Define a Hostname
7. Define a Hostname

Day N Automation Workflow for Cat9k Edge

Day N Automate Secure tunnels via DNA Center

Choose Site and Device

Select the device that you intend to use for this tunnel.

Site

Select the site first and then select from eligible devices.

Site*: Global/AMER/San Jose/Bldg 1/Floor 1

Device*: C9300X-SJ-02

Number of Tunnels*: 4

Learn More

Enter the tunnel name and select the source interface for each tunnel. We will auto-generate the tunnel number.

TUNNEL 1

Tunnel Name*: SJ-ATT

Tunnel Source Interface*: GigabitEthernet0/0/0 (192.168.33.44)

☑ Use the same interface for Tunnel IP

TUNNEL 2

Tunnel Name*: SJ-ATT-2

Tunnel Source Interface*: GigabitEthernet0/0/0 (192.168.33.44)

☑ Use the same interface for Tunnel IP

TUNNEL 3

Tunnel Name*: SJ-Verizon

Tunnel Source Interface*: GigabitEthernet0/0/1 (192.168.12.12)

Cisco Umbrella

Select the Cisco Umbrella data center location.

Tunnel 1 Data Center Location*: Santa Clara, CA — View Details

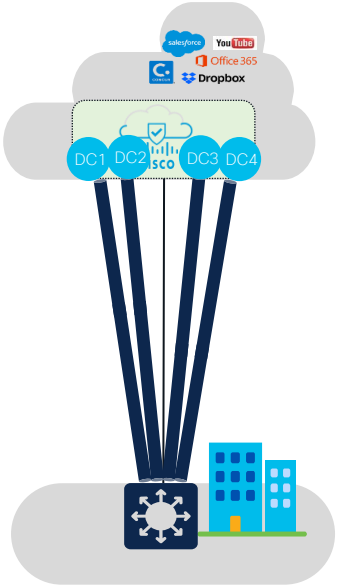
Tunnel 2 Data Center Location*: Santa Clara, CA — View Details

Tunnel 3 Data Center Location*: Santa Clara, CA — View Details

Tunnel 4 Data Center Location*: Santa Clara, CA — View Details

☐ Use same data center location for all tunnels

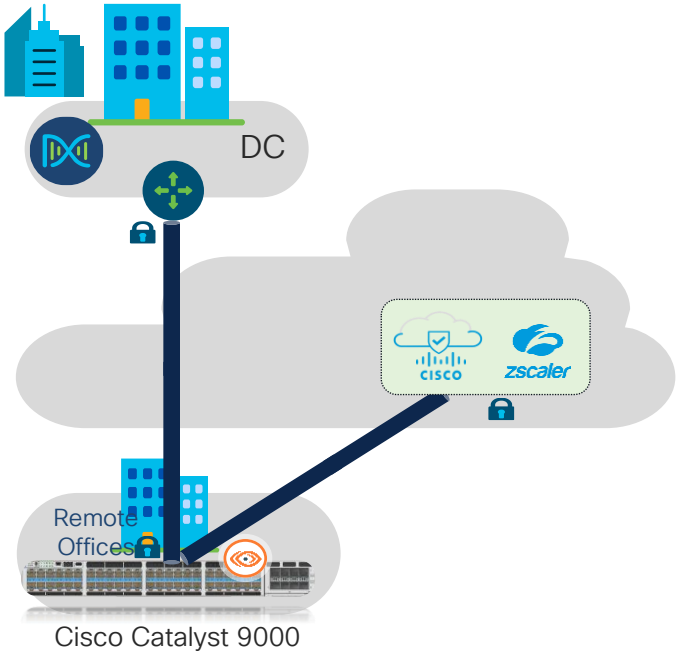
Exit | All changes saved | Review | Back | Next

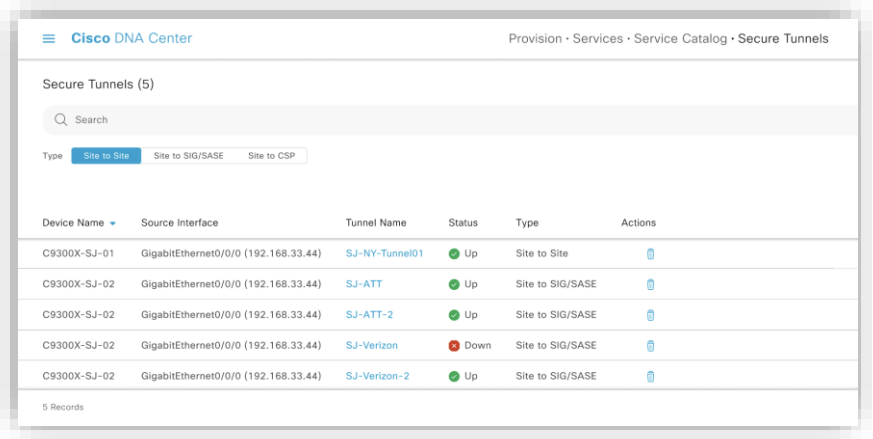


Day 0 + Day N: Automate Secure tunnels to Internet Gateways

Tunnel Monitoring via Cisco DNA Center

Day N Tunnel Assurance





Cisco DNA Center — Provision · Services · Service Catalog · Secure Tunnels

Secure Tunnels (5)

Search

Type: Site to Site | Site to SIG/SASE | Site to CSP

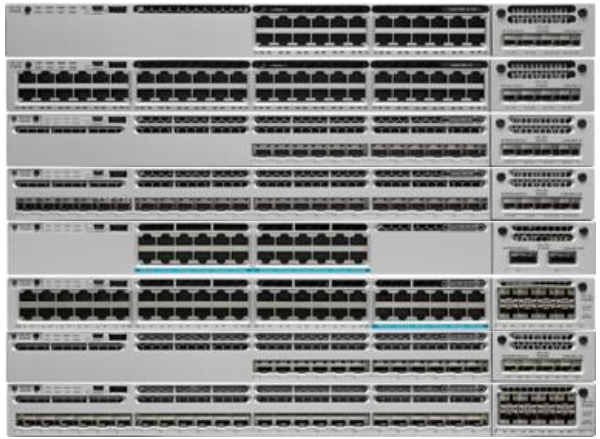
Device Name	Source Interface	Tunnel Name	Status	Type	Actions
C9300X-SJ-01	GigabitEthernet0/0/0 (192.168.33.44)	SJ-NY-Tunnel01	Up	Site to Site	
C9300X-SJ-02	GigabitEthernet0/0/0 (192.168.33.44)	SJ-ATT	Up	Site to SIG/SASE	
C9300X-SJ-02	GigabitEthernet0/0/0 (192.168.33.44)	SJ-ATT-2	Up	Site to SIG/SASE	
C9300X-SJ-02	GigabitEthernet0/0/0 (192.168.33.44)	SJ-Verizon	Down	Site to SIG/SASE	
C9300X-SJ-02	GigabitEthernet0/0/0 (192.168.33.44)	SJ-Verizon-2	Up	Site to SIG/SASE	

5 Records

Day 0 + Day N: Automate Secure tunnels to Internet Gateways + Tunnel Monitoring

IPsec supported in Stacking

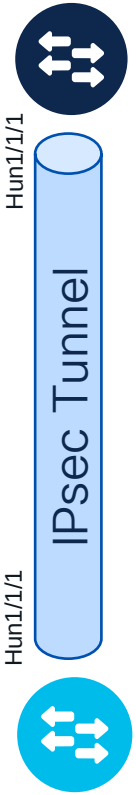
- Only stack made of Catalyst 9300X switches
- Distributed IPsec processing is not supported
- Active Switch will process IPsec encapsulation / decapsulation
- High Availability, ISSU, xFSU are not supported



Catalyst 9300X Stack

IPsec Site to Site / Point to Point with PSK

Step:



Site A

IKEv2

```
crypto ikev2 proposal sitetosite
 encryption aes-cbc-256
 integrity sha512
 group 19 20 21
crypto ikev2 dpd 10 5 periodic
```

IKEv2 Policy

```
crypto ikev2 policy hun_ipsec
  match address local 172.16.0.1
  proposal sitetosite
crypto ikev2 policy peers
  match fvrf any
  proposal sitetosite
```

IKEv2 Peer

```
crypto ikev2 keyring auth-keyring
  peer 172.16.0.2
  address 172.16.0.2
  pre-shared-key Cisco12345Cisco12345
```

IKEv2 Peer Profile

```
crypto ikev2 profile auth_Hun
  match identity remote address 172.16.0.2 255.255.255.255
  identity local address 172.16.0.1
  authentication remote pre-share
  authentication local pre-share
  keyring local auth-keyring
  no config-exchange request
```

Site B

IKEv2

```
crypto ikev2 proposal sitetosite
encryption aes-cbc-256
 integrity sha512
 group 19 20 21
crypto ikev2 dpd 10 5 periodic
```

IKEv2 Policy

```
crypto ikev2 policy hun_ipsec
 match address local 172.16.0.2
 proposal sitetosite
crypto ikev2 policy peers
 match fvrf any
 proposal sitetosite
```

IKEv2 Peer

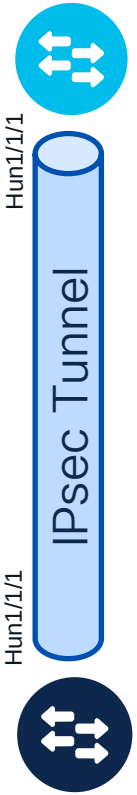
```
crypto ikev2 keyring auth-keyring
   peer 172.16.0.1
   address 172.16.0.1
   pre-shared-key Cisco12345Cisco12345
```

IKEv2 Peer Profile

```
crypto ikev2 profile auth_Hun
  match identity remote address 172.16.0.2 255.255.255.255
  identity local address 172.16.0.1
  authentication remote pre-share
  authentication local pre-share
  keyring local auth-keyring
  no config-exchange request
```

1 2 3 4

IPsec Site to Site / Point to Point



Site A

Transform Set

```
crypto ipsec transform-set auth-ipsec esp-gcm 256
  mode tunnel
```

IPsec Profile

```
crypto ipsec profile site-to-site
  set security-association lifetime seconds 28800
  set security-policy limit 1 (optional)
  set transform-set auth-ipsec
  set ikev2-profile auth_Hun
```

Physical Port

```
interface HundredGigE1/1/1
  no switchport
  ip address 172.16.0.1 255.255.255.0
```

Create IP in IP tunnel

```
interface Tunnel1
 ip address 30.30.30.1 255.255.255.0
 tunnel source HundredGigE1/1/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile site-to-site
```

Routes

```
ip routing
ip route 10.10.10.0 255.255.255.0 30.30.30.2
ip route 24.24.24.24 255.255.255.255 30.30.30.2
```

Site B

Transform Set

```
crypto ipsec transform-set auth-ipsec esp-gcm 256
 mode tunnel
```

IPsec Profile

```
crypto ipsec profile site-to-site
  set security-association lifetime seconds 28800
  set security-policy limit 1 (optional)
  set transform-set auth-ipsec
  set ikev2-profile auth_Hun
```

Physical Port

```
interface HundredGigE1/1/1
  no switchport
  ip address 172.16.0.2 255.255.255.0
```

Create IP in IP Tunnel

```
interface Tunnel1
 ip address 30.30.30.2 255.255.255.0
 tunnel source HundredGigE1/1/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile site-to-site
```

Routes

```
ip routing
ip route 10.10.10.0 255.255.255.0 30.30.30.1
ip route 24.24.24.24 255.255.255.255 30.30.30.1
```

Step:

5

6

7

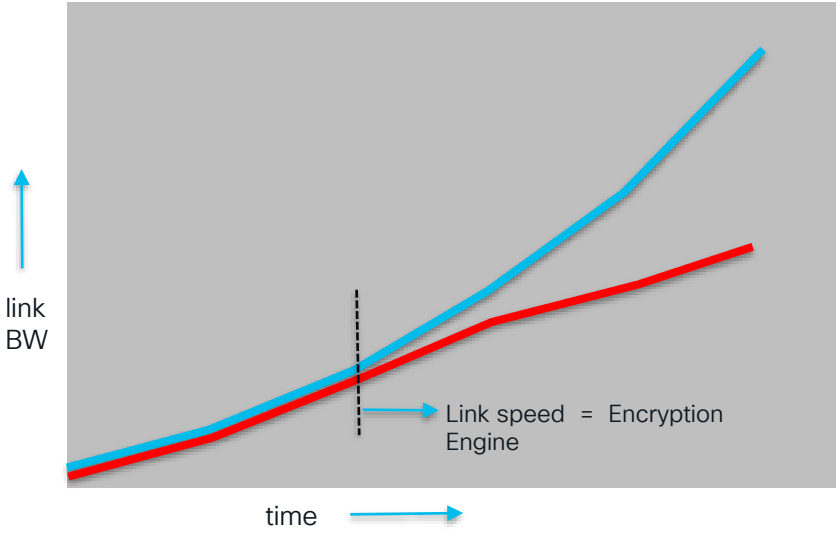
8

9

WAN MACsec

Link Speeds Out-Pacing IP Encryption

Link Speeds Out-Pacing IP Encryption

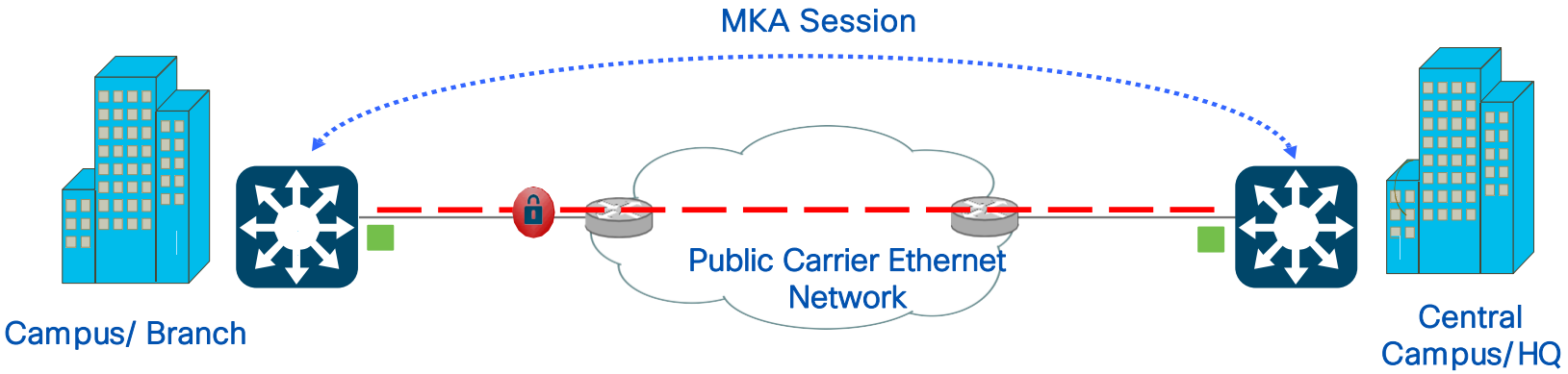


- Bandwidth application requirements out-pacing IP encryption capabilities
- Bi-directional and packet sizes further impact encryption performance
- IPsec engines dictate aggregate performance of the platform (much less than the switch router forwarding throughput)
- Encryption must align with link speed (100G+) to support next-generation applications.

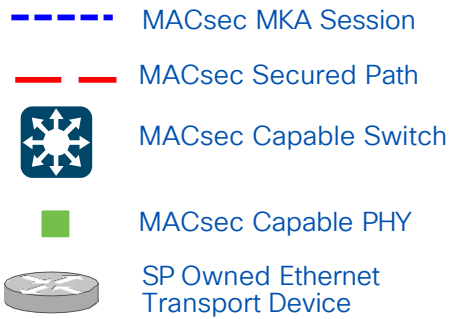
Link Speed

IPsec Encryption Speed

What is WAN MACsec?



- IEEE 802.1AE standards-based Layer 2 encryption that provides data confidentiality and integrity for media access independent protocols.
- Optimize MACsec + WAN features to accommodate running over L2 public Ethernet transport.
- "line-rate" encryption mitigating packet eavesdropping, tampering, and injection.



New Enhancements to 802.1AE for WAN/Metro-E Transport

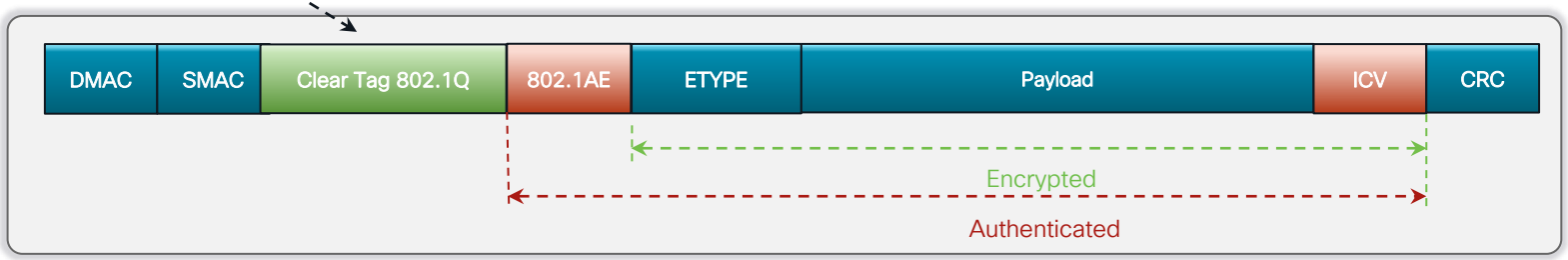
- AES-256 (AES/GCM) support
- Standards Based MKA key framework
  - (defined in 802.1X-2010) within Cisco security
- Vital Network Features to Interoperate over Public Carrier Ethernet Providers
  - 802.1Q tag in the clear
  - Ability to change MKA EAPoL Destination Address, Ether-type value
  - Ability to configure Anti-replay window size

	WAN MACsec	LAN MACsec
Connection Type	Over L2 MPLS, VPLS, EoMPLS, QinQ, Multiple Point to Point	Only Directly Connected Devices
AES 128	✓	✓
AES 256	✓	✓
IPv4 and IPv6 Independent	✓	✓
Performance	Line rate on all Ports (C9600X, C9500X)	Line rate on all Ports
Overhead	32 Bytes	32 Bytes

Dot1Q Clear Tag

- Adds Extra 802.1Q tag which is not considered as MACsec and is forwarded by the service provider devices.
- Leverages a “well known” ether type value.
- Enable on Physical port and all SubInterfaces will use Clear Tag on this physical port

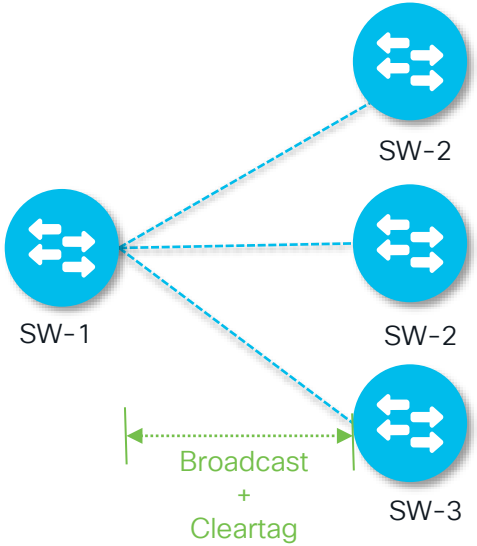

```
interface TenGigabitEthernet1/0/4
macsec dot1q-in-clear 1
```



MKA EAPoL Destination MAC Tuning

Destination Mac Change capability

- Leverage “broadcast” address as the destination MAC EAPoL address. Provider
  switch will forward as standard “broadcast” all “F”s ethernet frame to all Peers
- Some Service Provider switches might Consume the Multicast frame and not send it to all peers
- Can be used with or without “Clear Tag”

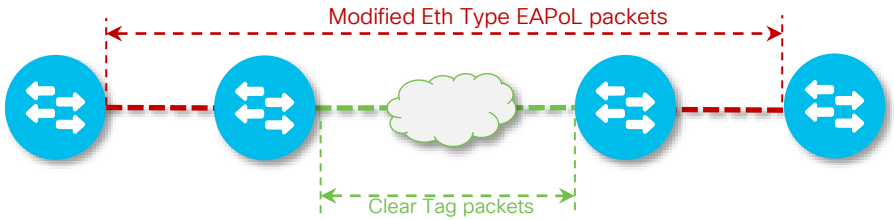


“Broadcast” DMAC is required for P2MP cases

```
interface TenGigabitEthernet1/0/4
    eapol destination-address broadcast
    macsec dot1q-in-clear 1
```

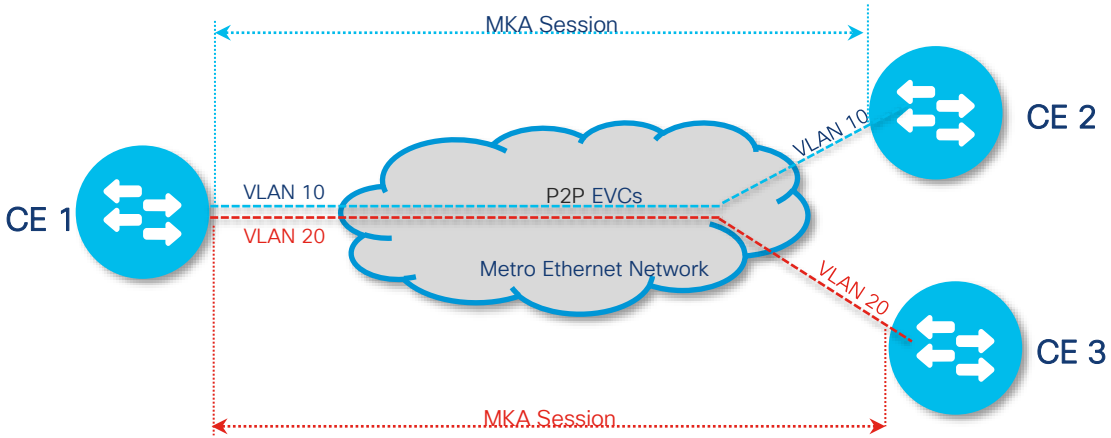
MKA EAPoL EtherType Tuning

- Provider bridge will **NOT ingest frame** as ether-type 0x876F as it is assumed "well known".
- Leverages a "well known" ether type value.
- By default, EAPoL EthType is 0x888E
- Can be used with or without "Clear Tag"




```
interface TenGigabitEthernet1/0/4
    eapol eth-type 876F
    macsec dot1q-in-clear 1
```

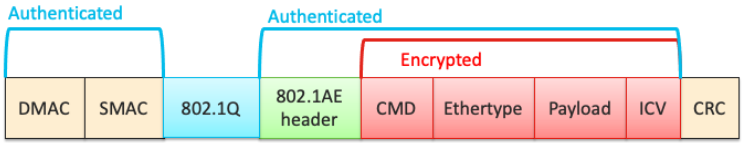
Deployment: VLAN-based E-Line Service (P2P)



Security Associations **from CE 1**:

Tx: CE 1 → CE 2
CE 1 → CE 3

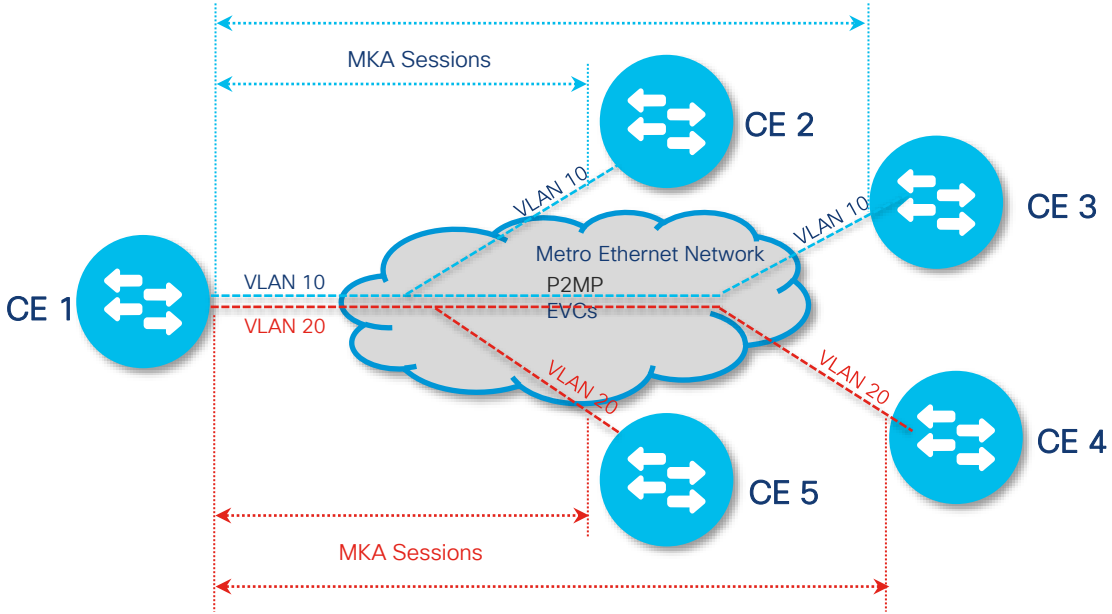
Rx: CE 2 → CE 1
CE 3 → CE 1



VLAN/Subinterface

MACsec encryption on WAN links connecting PE nodes for P2MP secure connectivity across MPLS core.

Deployment: VLAN-based E-LAN Service (P2MP)



Security Associations **from CE 1**:

Tx: CE 1 → CE 2, CE 3 (shared SA)

CE 1 → CE 4, CE 5 (shared SA)

Rx: CE 2 → CE 1

CE 3 → CE 1

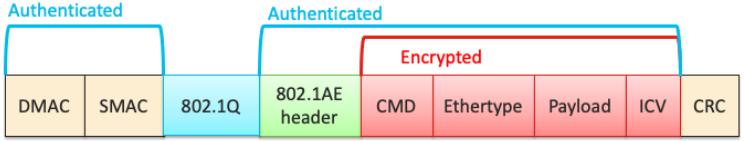
CE 4 → CE 1

CE 5 → CE 1

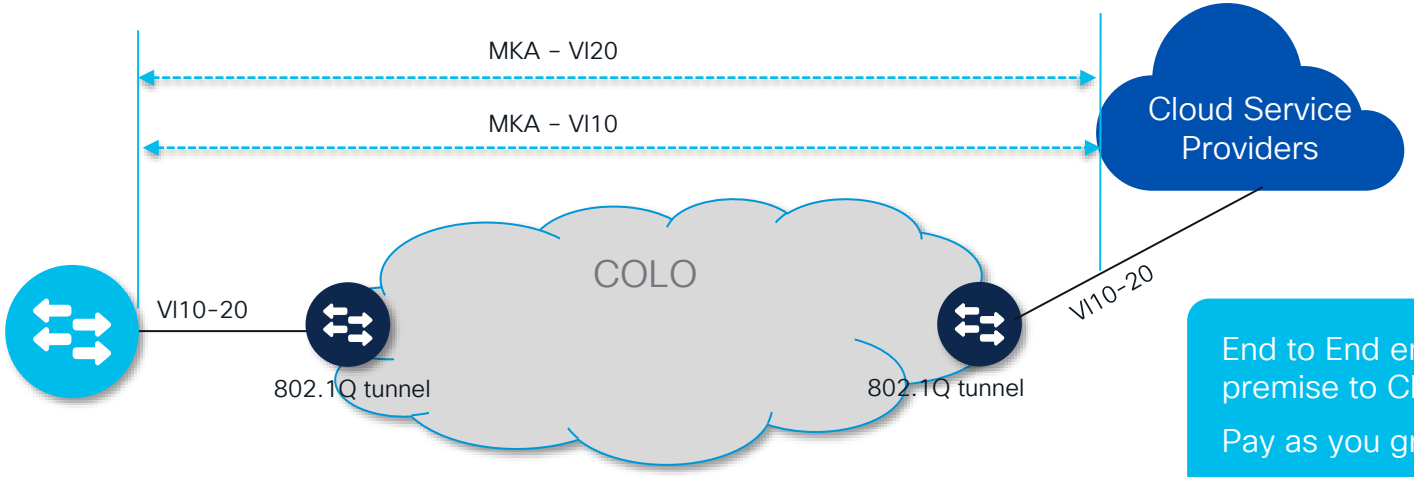
When a peer is added/removed to shared SA, REKEY is transparent without traffic drop

EAPoL DMAC is required to be Broadcast

VLAN/Subinterface



Deployment: Extending to Cloud Service Providers

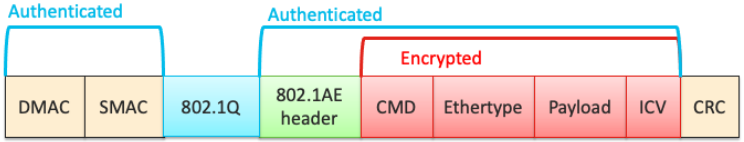


End to End encryption from On-premise to Cloud Infrastructure

Pay as you grow models

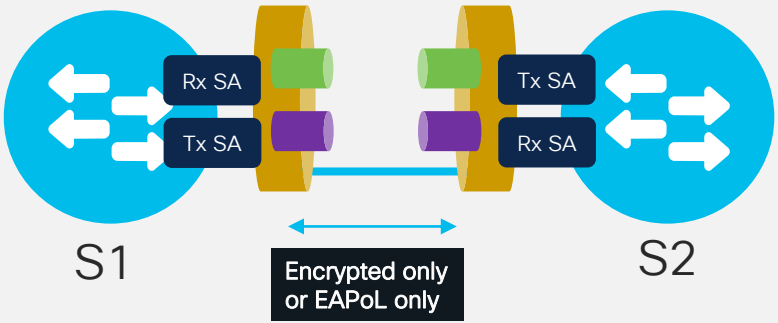
EAPoL DMAC is required to be Broadcast

VLAN/Subinterface



Must-Secure

17.7.1

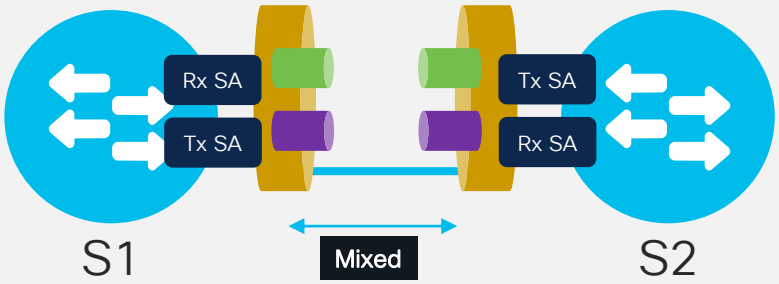


Must-Secure Properties

- Only EAPoL allowed if MKA session is down
- When MKA session is torn down or SAK is not re-keyed properly, interface will drop all traffic except EAPoL

Should-Secure

17.8.1



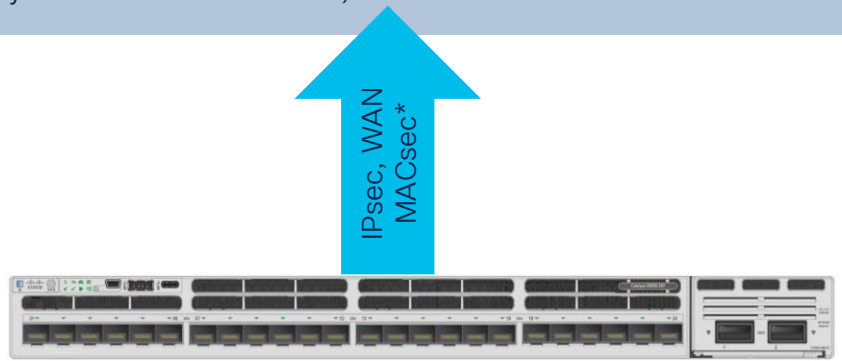
Should-Secure Properties

- All Encrypted and Decrypted packets are allowed
- Will try to encrypt if MKA session is UP
- When a MKA session is torn down or SAK is not re-keyed properly then interface can send traffic in clear instead of dropping it.

HSEC K9 key for Catalyst 9300X, 9500X, 9600X

HSEC K9 Key

- New add-on license in addition on top of subscription based on DNA Advantage
- Legally required by US law, requiring authorization prior to use.
- Can only be obtained for 9600X, 9500X and 9300X switches.



Orders via CCW (drop shipped from Cisco) can have SLAC installed at factory prior to shipping.

Notes

- Required for enabling IPsec on 9300X WAN MACsec on 9500X, 9600X switches.
- Without the HSECK9 Key IPsec & WAN MACsec cannot be enabled.
- With stack and Stackwise Virtual, it is recommended individual HSEC K9 keys per switch.

How

- Authorization code (SLAC – Smart Licensing Authorization Code) required on the system.
- One time code installation on the switches. No subsequent action needed.

WAN MACsec Supported Platforms and Scale

	WAN MACsec	LAN MACsec
C9600X,C9500X	✔	✔
C9300X	HW Capable	✔
C9400X	HW Capable	✔
C9200-C9600	➖	✔

SCALE	C9600X	C9500X
Total number of WAN MACsec session	192	192

C9600X Supports WAN MACsec on C9600-LC-40YL4CD with Gen 2 SUP

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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!

ALL IN

#CiscoLive