
cisco Live!
Let's go

The bridge to possible

Securing End-to-End from Campus and Branch to Cloud with Catalyst 9000

Raj Kumar Goli, Technical Marketing Engineer

Agenda

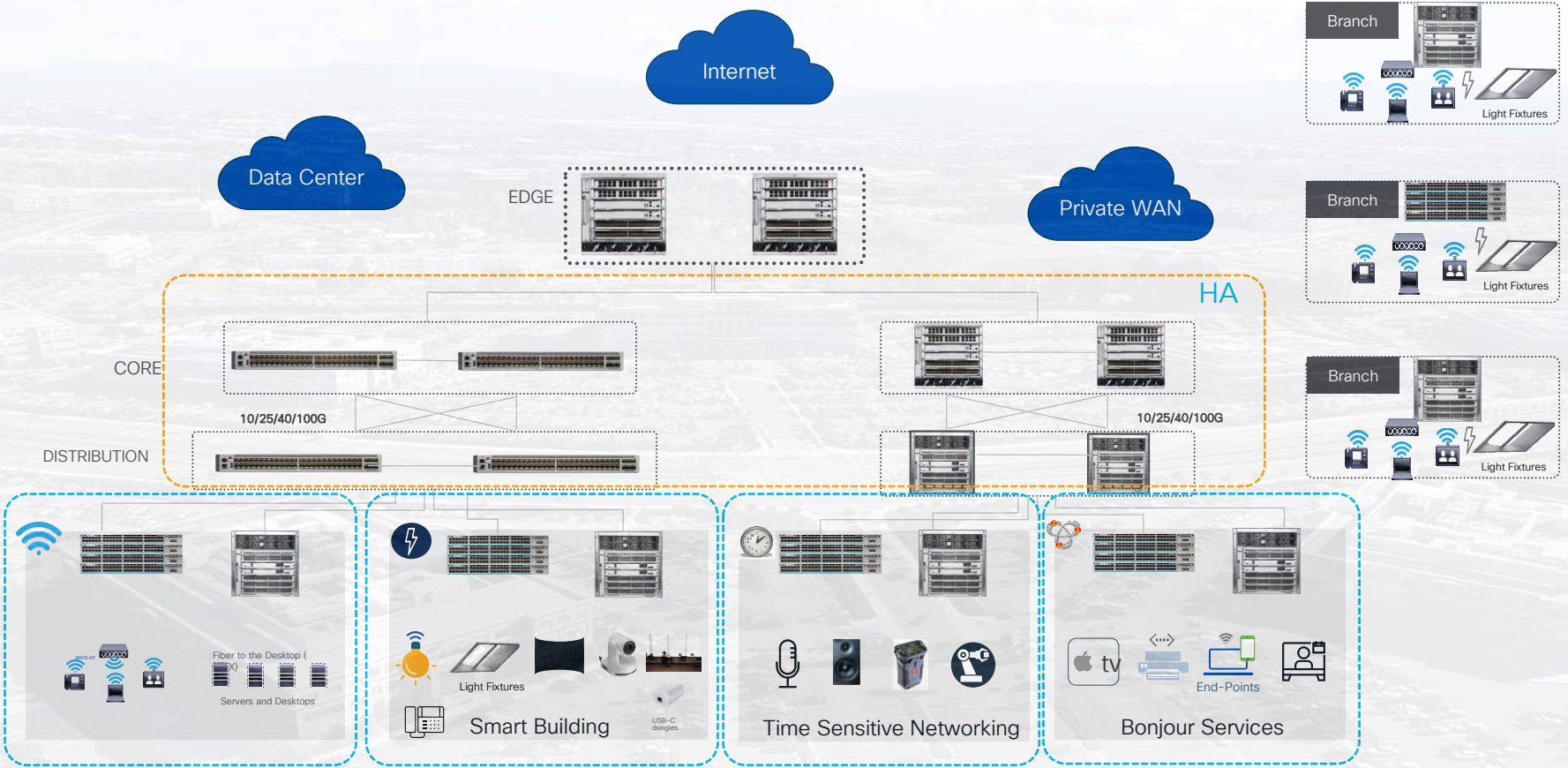
Catalyst 9000 being the bridge to secure end-to-end communication

- *Securing Infrastructure* with Cisco Trustworthy Solutions
- *Securing Endpoints* with *native connectors* & *Hosted Applications* (Cisco Secure Cloud Analytics, Cisco Umbrella, Adaptive Security Appliance)
- Auto-profiling and securing endpoints using *Endpoint Analytics* and *Trust Analytics*
- Securing Transport with *MACsec* and *IPsec* (Site-Site, Site-Cloud)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

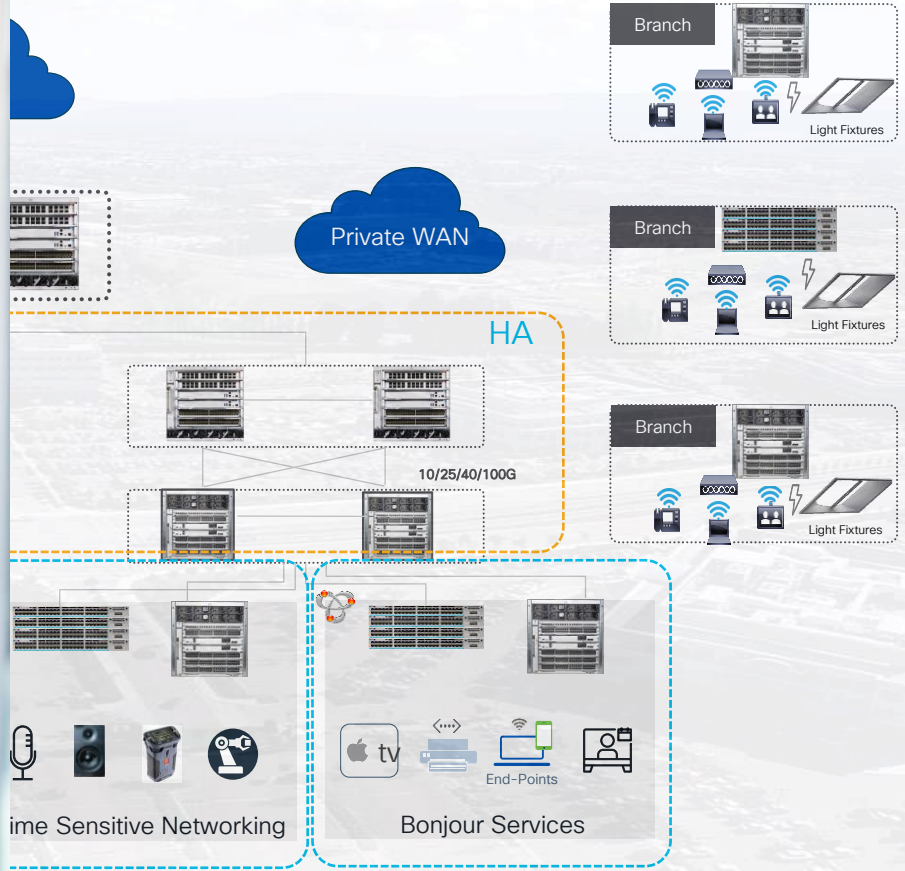
Typical Enterprise or Campus





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

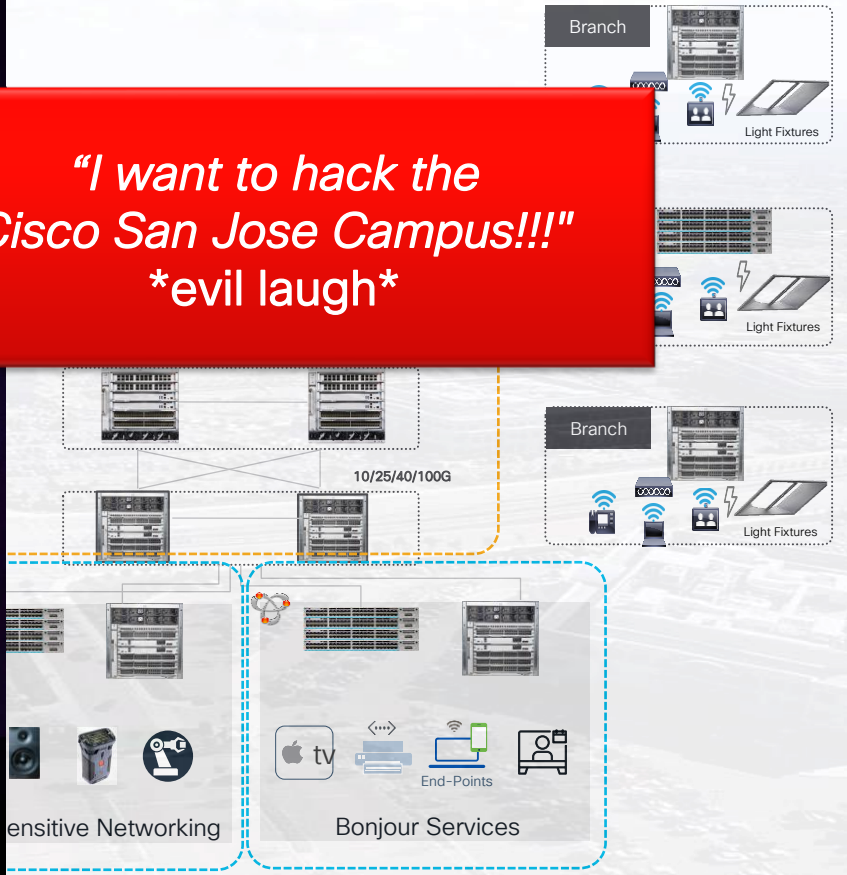




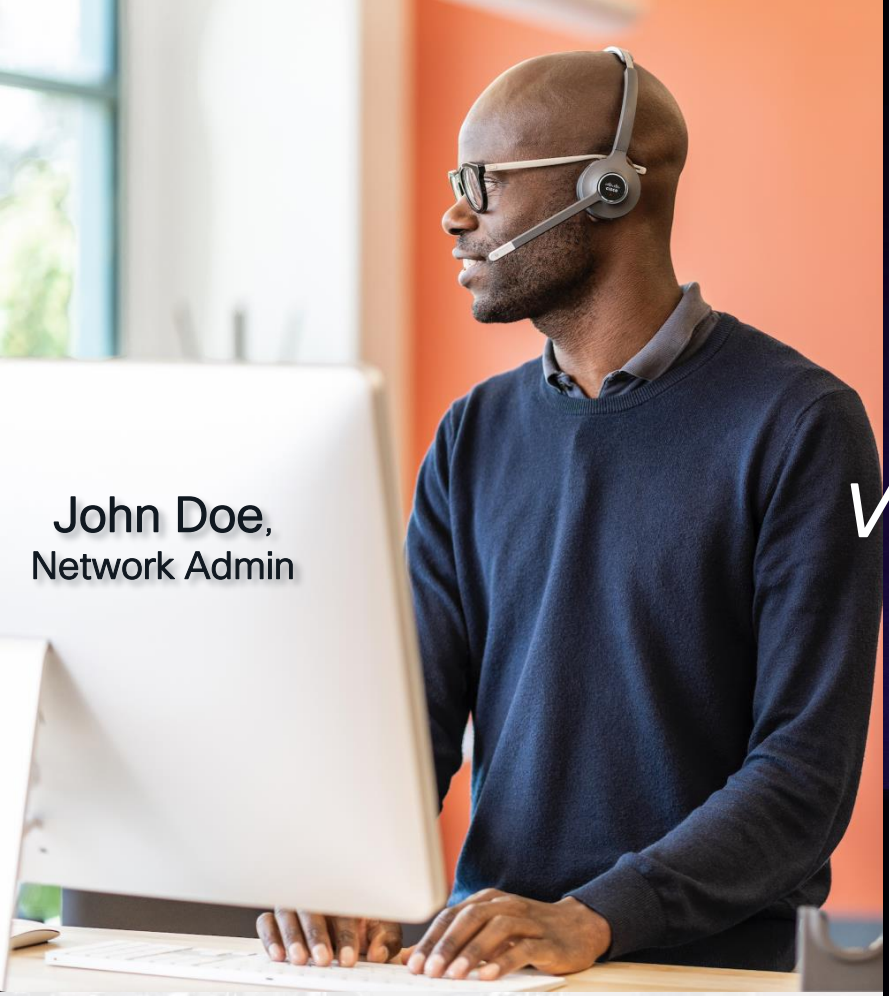
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



"I want to hack the Cisco San Jose Campus!!!"
evil laugh



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

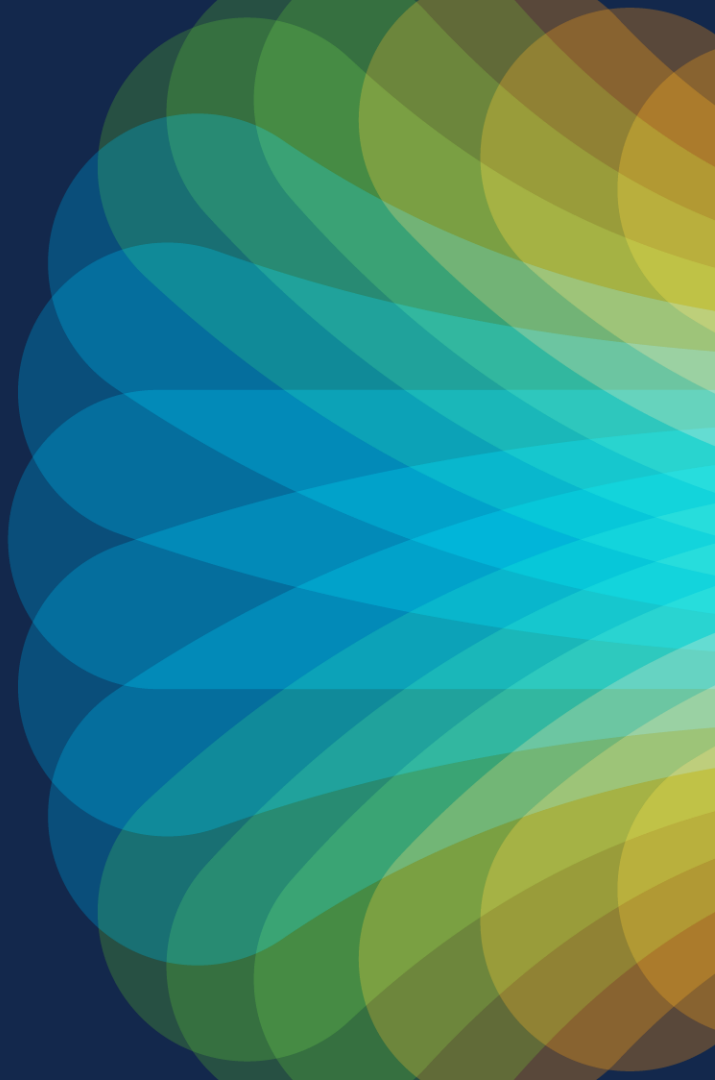


VS.

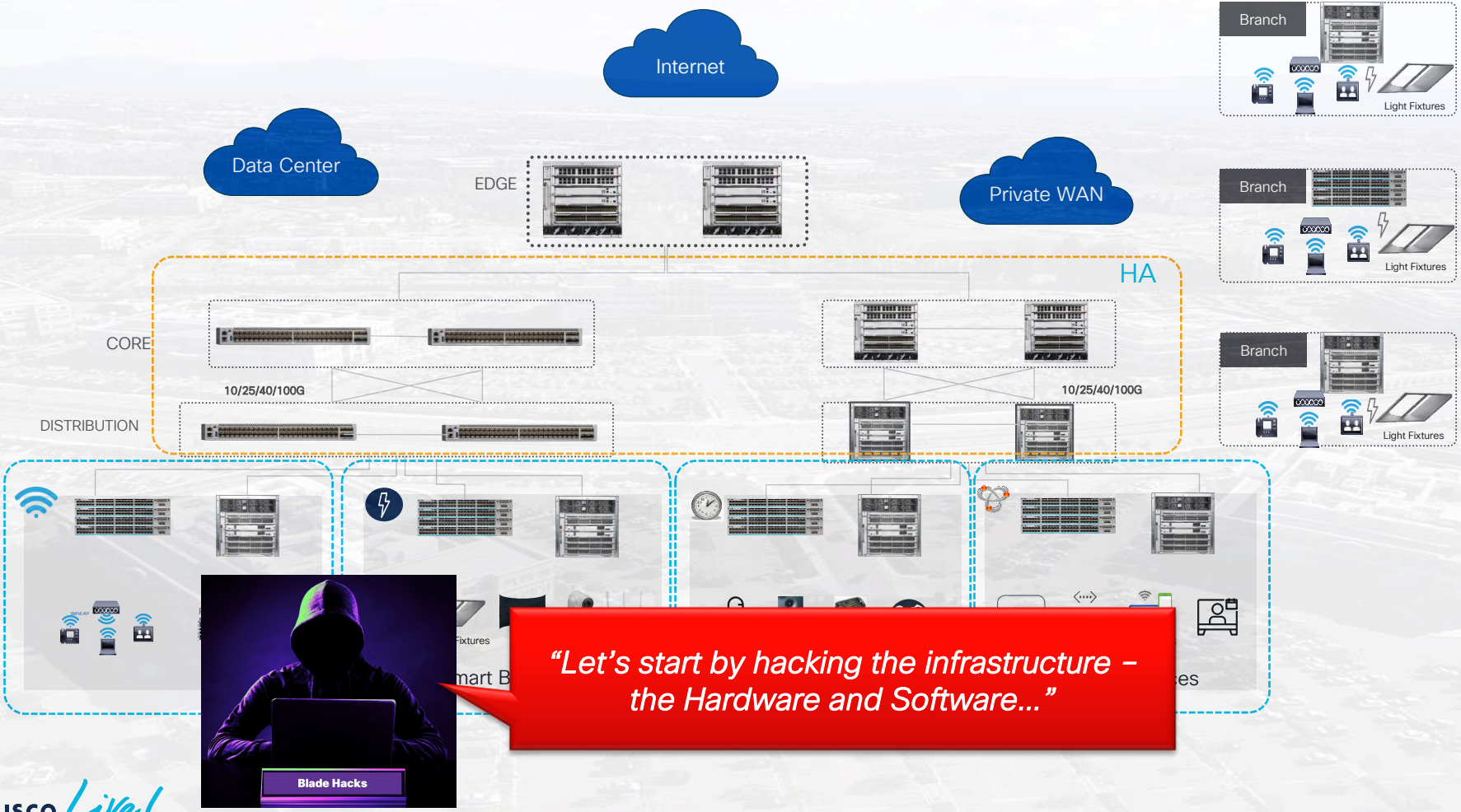


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing Infrastructure with Cisco Trustworthy Solutions



cisco Live!

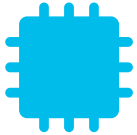


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where can attacks happen ?



Supply Chain Attack



HW Tampering Attack



BIOS/ ROMMON Attack



SW Binary Attack

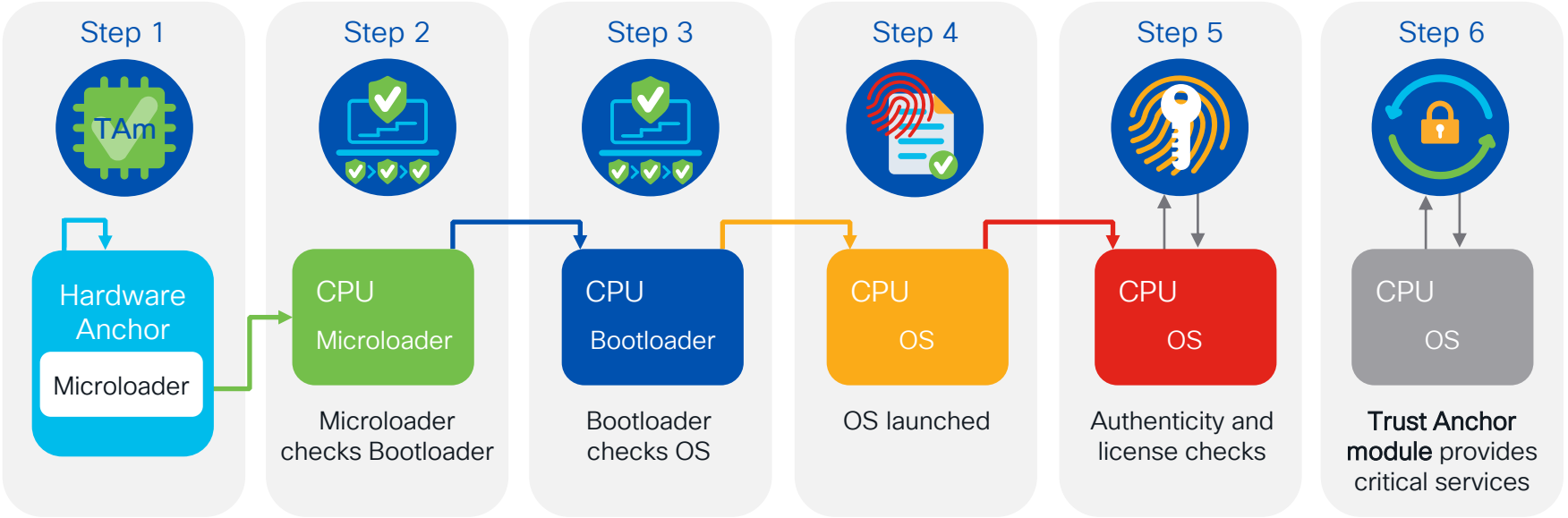


Runtime Attack



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Platform with Trustworthy Technologies



Confidentiality | Integrity | Authenticity

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

So, what's the score between John Doe and Blade Hacks?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



"What if the infrastructure is secure?!!

I can easily make users/devices access malicious sites or steal their credentials..."

Internet

Data Center

Private WAN

Branch

Light Fixtures

Branch

Light Fixtures

Branch

Light Fixtures

Light Fixtures

USB-C dongles

Smart Building

Time Sensitive Networking

tv

End-Points

Bonjour Services

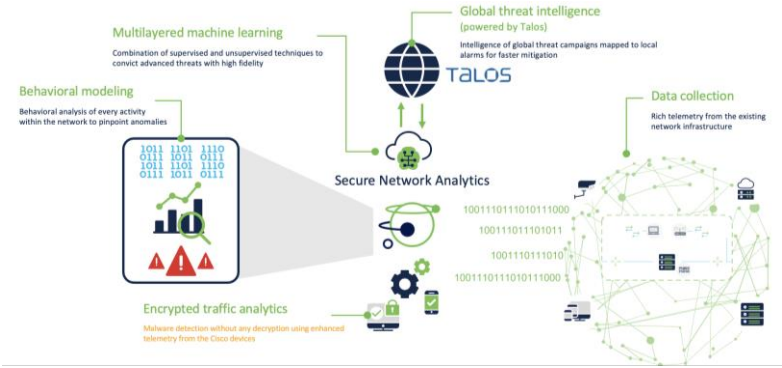
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Blade Hacks can attack an endpoint user...

Attack Persona	Attack Flow
 Lateral Movement and Data exfiltration	User opens email with malicious content. Based on that the attacker has stolen privileges and will start to download data from financial database on intermittent intervals
 Unskilled employee with privileged access	Locate access from unusual places. Like typical patterns is Las Vegas as entry point all over sudden we get access from location in Asia.
 Angry employee malicious insider	We get unusual servers that the user gets logged in from
 Victimized employee compromised credentials	We get unusual traffic encryption from that computers

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing Endpoints with Secure Cloud Analytics connector



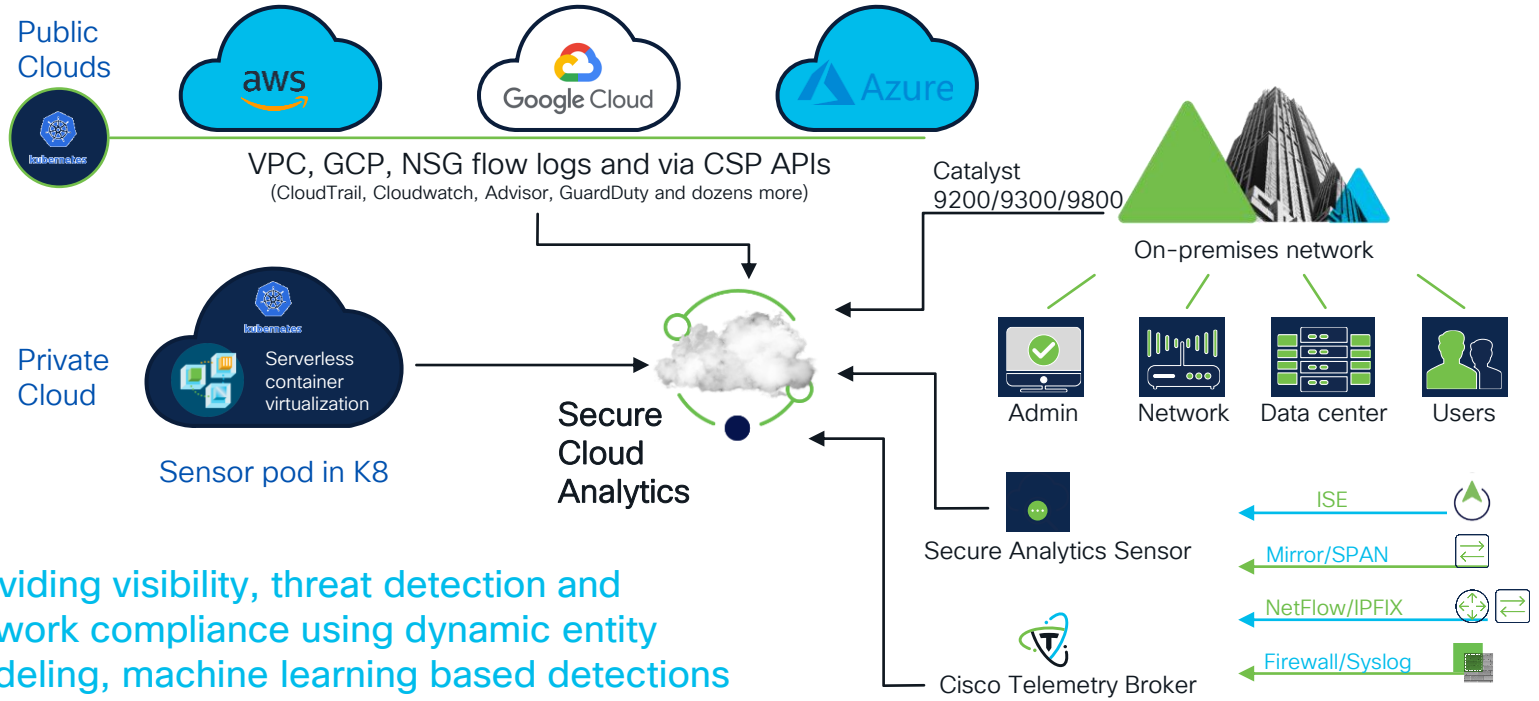
Secure Cloud Analytics - See it ALL!

- Capture enhanced NetFlow for encrypted traffic analysis from Cisco ASR, ISR and **Catalyst 9000 platforms**
- A Trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection
- Cloud Telemetry ingest
- East west and north south visibility
- Light meta data collection using the existing infrastructure

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Analytics

Flexible security for dynamic environments

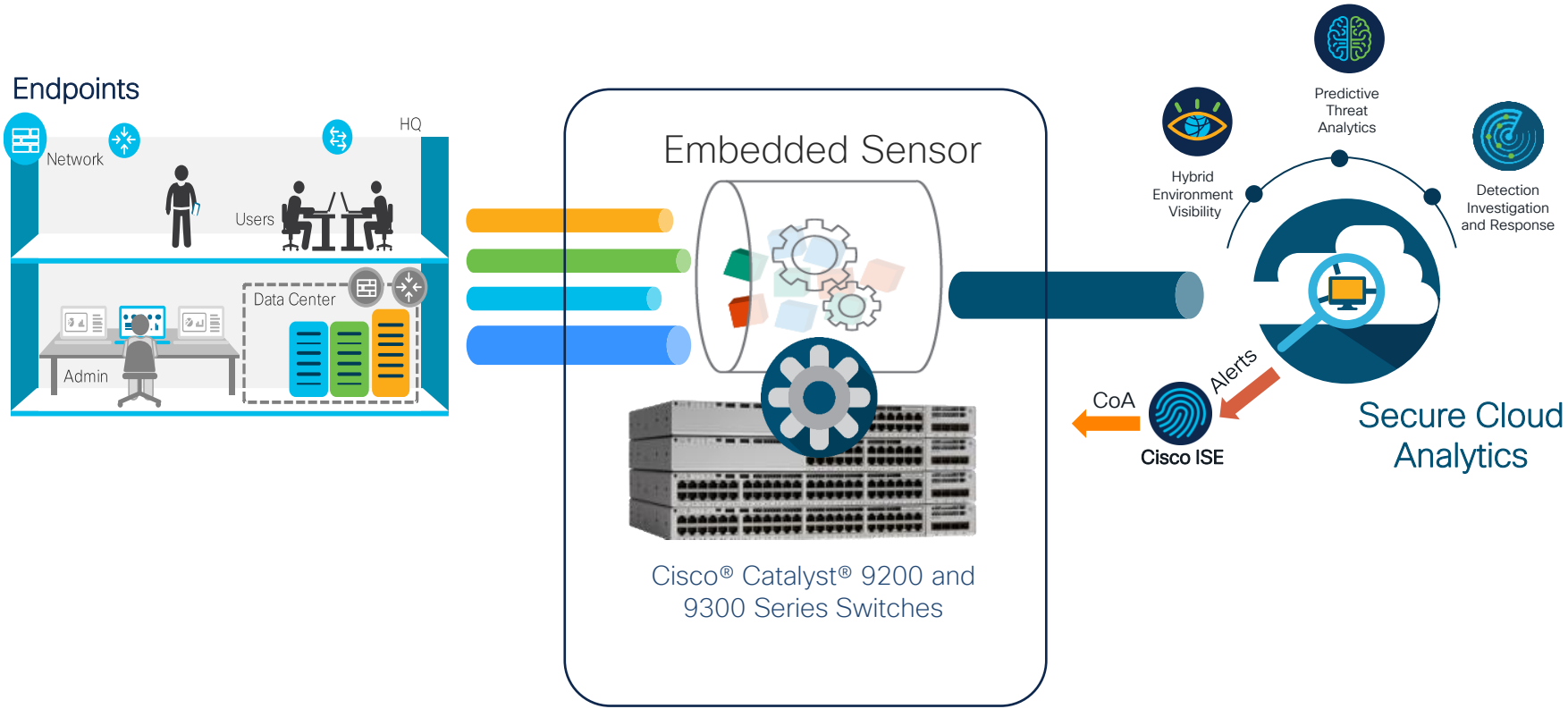


Providing visibility, threat detection and network compliance using dynamic entity modeling, machine learning based detections

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Analytics Sensor on C9K

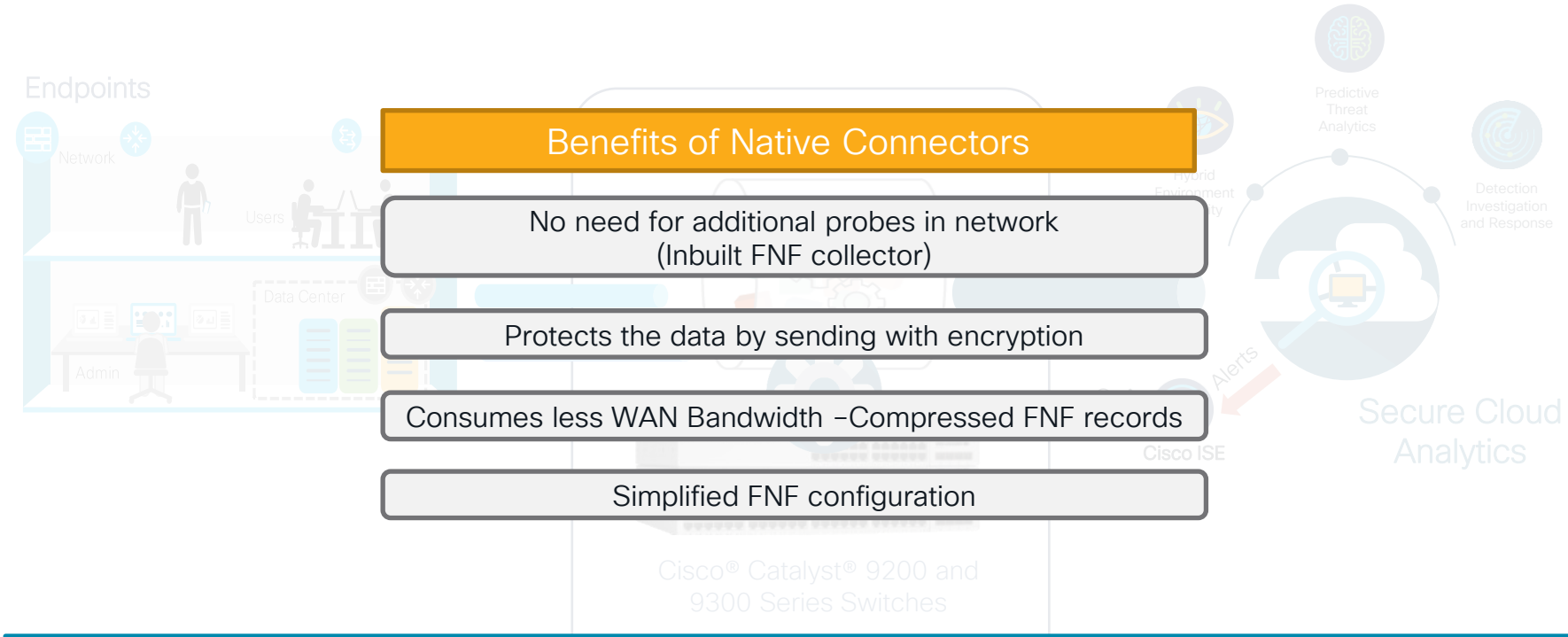
Add Advanced Cloud Security to your network



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Analytics Sensor on C9K

Add Advanced Cloud Security to your network



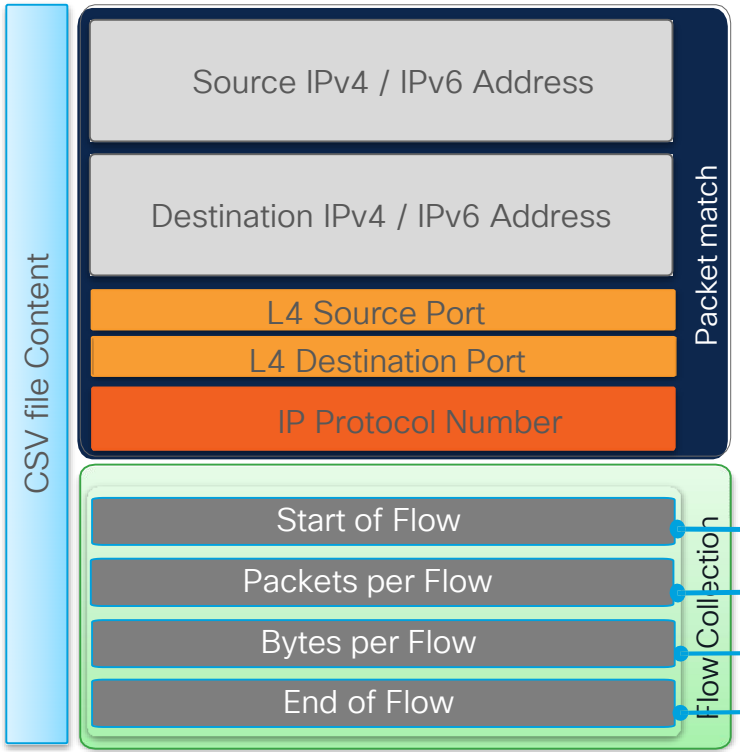
Benefits of Native Connectors

- No need for additional probes in network (Inbuilt FNF collector)
- Protects the data by sending with encryption
- Consumes less WAN Bandwidth –Compressed FNF records
- Simplified FNF configuration

Available on Cisco Catalyst 9200 and 9300 Switches

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Format For Upload



- CSV files are uploaded every 1 minute
- CSV files contain IPv4 and IPv6 Flows
- CSV files are stored locally on flash before uploaded /tmp folder
- CSV files are compressed to reduce BW consumption
- 9-tuple flow data

- Start – the start time for this flow in Unix Epoch
- Packets – the number of packets transmitted
- Bytes – the number of bytes transmitted
- End – the end time for this flow in Unix Epoch

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identify every entity in any environment

Detect entities across the network

Overview for March 22, 2020

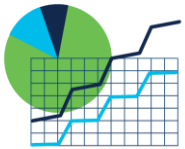
Device	Attendance	Connections
iccwh1adb2c.resource.comcast.net	13%	24293
10.201.0.16	100%	15236
10-10-30-16.suddenlink.net	83%	10113
10-10-101-24.suddenlink.net	85%	4420
i-02c4108c67a7087dc	100%	3237
gke-cluster-1-default-pool-a8eba68f-fc...	100%	3142
gke-cluster-1-default-pool-a8eba68f-5...	100%	3130
192.168.50.136	100%	2872
gke-cluster-2-default-pool-a4aaac6b-s1...	100%	2754
gke-cluster-1-default-pool-a8eba68f-gh...	100%	2749



Detect any entity



Track entity traffic



Profile entities for security analytics

Internal and external traffic flows

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
2/17/20 2:29 AM	192.168.48.211	192.168.48.212	443 (https)	59108	TCP	5,226	5,322	11	9
2/17/20 2:29 AM	192.168.48.211	192.168.48.212	443 (https)	59102	TCP	4,660	5,915	12	10
2/17/20 2:29 AM	192.168.1.105	208.67.222.220	55525	53 (domain)	UDP	378	228	2	2
2/17/20 2:29 AM	192.168.1.105	208.67.222.220	49858	53 (domain)	UDP	378	228	2	2

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key features with Secure Network Analytics

Visibility everywhere

Analyze enterprise telemetry from any source, provide end to end visibility across the extended network in the cloud or with remote workers

Encrypted traffic analytics

Analyze encrypted traffic to detect malware and ensure policy compliance without decryption

Immediate threat remediation

Use the network to remove the infected host by applying a relevant policy through Automated Response



Unique threat detection

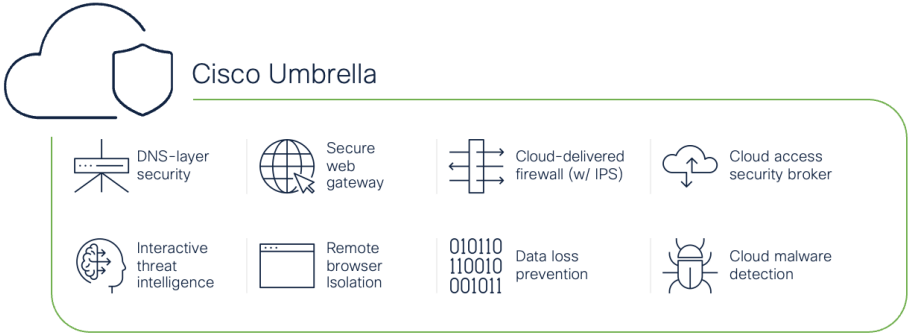
Combination of multi-layer machine learning and behavioral modeling provides the ability to detect inside as well as outside threats

Smart segmentation

Use logical functional business groups that, monitor the effectiveness of segmentation policies through contextual alarms

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing Endpoints with Umbrella connector



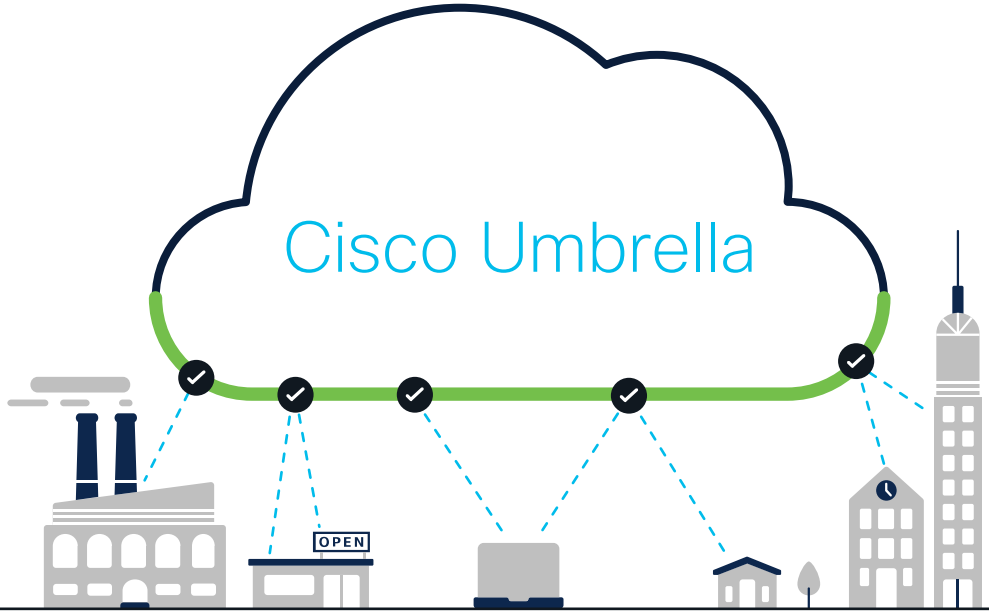
Provides Secure access to the internet and usage of cloud applications

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Umbrella DNS-layer security

Visibility and protection for all activity, anywhere

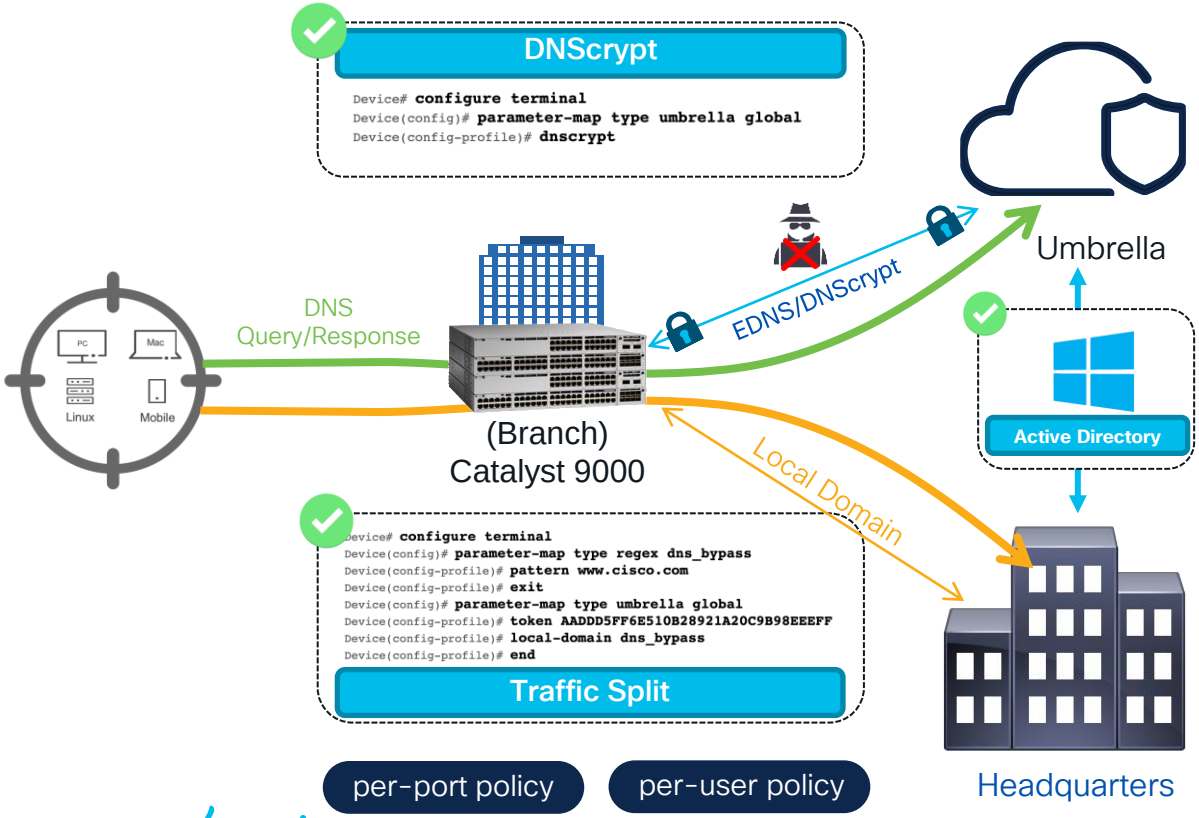
- See all internet traffic
- Block attacks earlier
- Contain malware if already inside
- Easily enforce content web filtering
- Discover, manage or block cloud apps
- Gain context for faster investigation



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Umbrella Native Connector

Available on Catalyst 9200 & 9300 series switches





- Built into the foundation of the internet
- Content filtering for guests and corporate users
- Prevents malware from infecting your branch office network

- Reduce backhaul by splitting off traffic for internal or trusted resource
- Encrypted DNS to secure connection



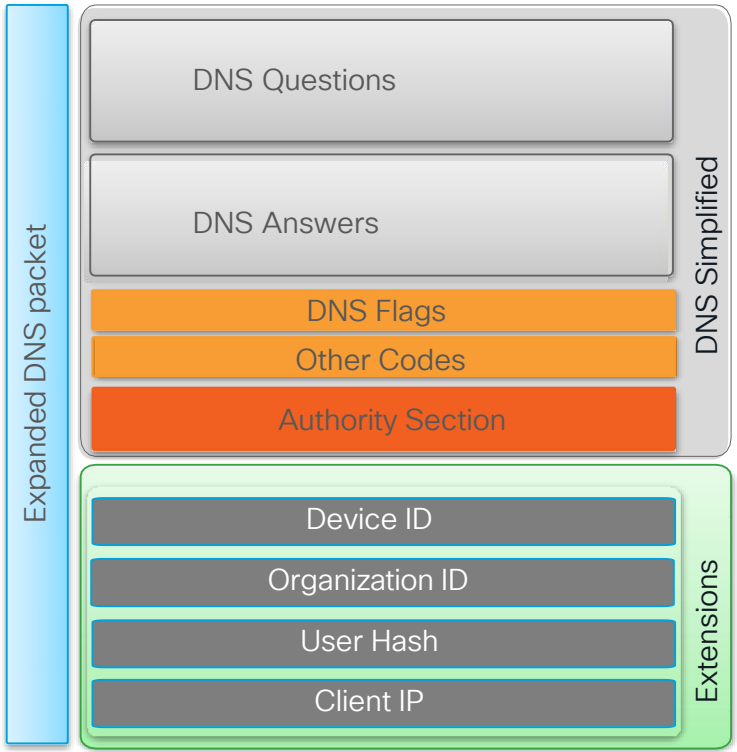
C9300



C9200

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

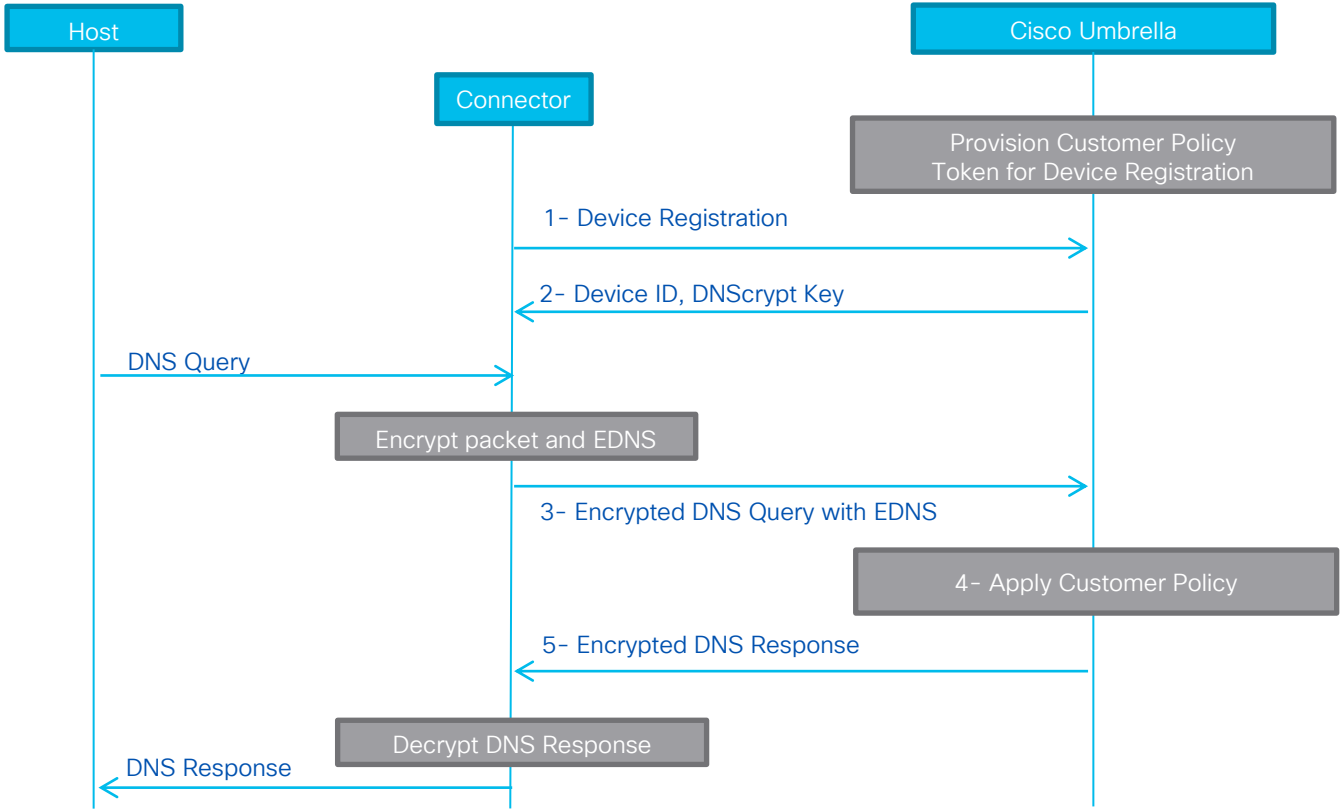
What is EDNS (Expand DNS messages) ?



- A method to Extend or Expand DNS messages (RFC 6891)
- EDNS adds information to DNS messages in the form of *pseudo-resource-records* included in the "additional data" section of a DNS message
- Umbrella uses EDNS for sending device-id, organization-id, username hash and client-ip information to Umbrella cloud

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Umbrella flow Sequence with DNSCrypt



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key features with Umbrella Connector

Register and use Umbrella knowledge

- No need for endpoints to know site rating
- Switch intercepts the DNS Query to ANY DNS server unless Net Admin created a policy to redirect to local sites

Static Policy Per Port

Assign a static policies per ports and link them to a policy in Umbrella portal

Provides unified policy regardless of the endpoint type

- the TAG name is defined by the Net Admin
- The same TAG name can be assigned to many ports

Per User Policy

Umbrella + AD Integration to detect user and pass on right policy

- Bob is part of Employee group in AD
- Sam is part of Guest group in AD

Traffic Split to cloud and on premise

- DNS Queries for Trusted Cloud Apps Protected by Cisco Umbrella
- Untrusted Internet Traffic tunneled through HQ
- Direct Internet Access for trusted Cloud Apps

DNS Crypt to protect the traffic

DNS traffic is encrypted and cannot be intercepted

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing IT & OT Endpoints with ASAc Firewall

Cisco Secure Firewall ASAc



Catalyst 9300X/9300/9300L

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IOS-XE 17.12.2
ASA 9.20.2

Cisco ASAc Hosted on Catalyst 9300/L(LM)/X

Seamless Firewall Service Insertion in the Network

Use Cases

- **Stateful inspection** of traffic flowing across IT/OT domains for security compliance
- Reduces the attack surface by logically **segmenting** the network
- Enforce **granular access controls** across the network
- Connect isolated OT/IoT clusters securely using **IPsec tunnels**
- **Secure remote management** of internal resources with SSL/TLS VPN
- Avoid network bottlenecks by replacing the physical firewall appliances



Technical Specifications

ASAv Feature parity

Reuse ASAv license

Throughput

589 Mbps (450 Byte) C9300

913 Mbps (450 Bytes) C9300X

250 IPSec / VPN Connections

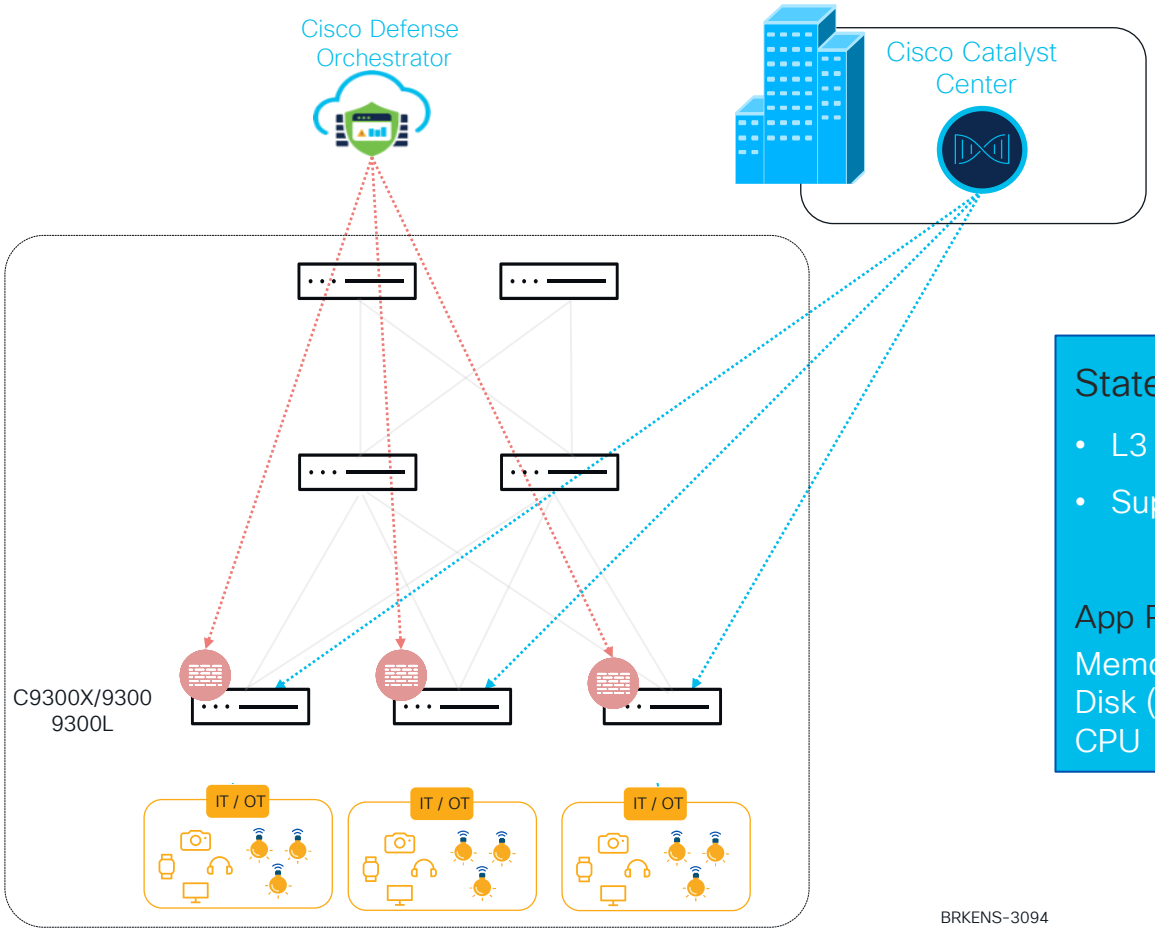
10 logical interfaces

Routed Mode Firewall

App Hosting HA (Cold)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stateful Inspection with ASAc hosted on Cat9k



Stateful Inspection Firewall

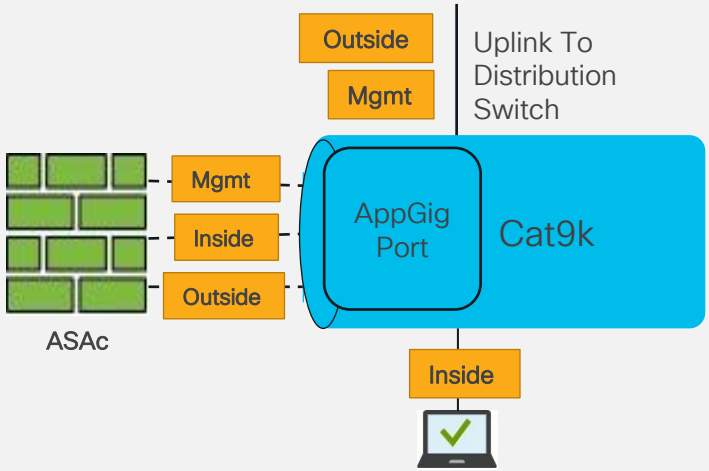
- L3 Firewall (Routed Mode only)
- Support for SGT

App Resources

Memory (RAM)	: 2 GB
Disk (SSD)	: 40 MB
CPU	: 1 Core

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ASAc Application Hosted on Cat9k



Licenses

Catalyst 9300 DNA-Advantage - C9300-DNA-A

ASAc5 (100M) - L-ASA-C-5S-K9=
ASAc10 (1G) - L-ASA-C-10S-K9=

OR

ASAv (100M) - L-ASA-V-5S-K9=
ASAv (1G) - L-ASA-V-10S-K9=

Application Hosting Infra on Cat9K

Resources Reserved for App Hosting	9300	9300X
AppGig Port(s)	1x1G	2x10G
vCPUs	2	4
RAM	2GB	8GB

Resources Required to Host ASAc Application

Resources	ASAc
No of virtual interface	3-10
No of vCPU	2
Memory	2GB
Firewall Mode	Router
Context	Single

Note : There is no room for any other app to be installed on C9300 if ASA is hosted. C9300X may host another app along with ASAc*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

So, what's the score between John Doe and Blade Hacks?

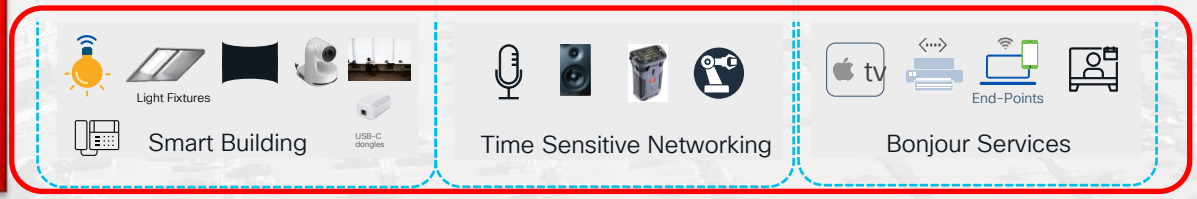


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



"Sheesh...The security is heavy here!!!

My next hope is to breach the dear endpoints to gain access..."

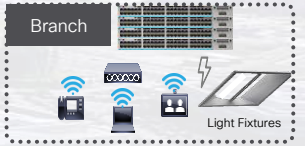


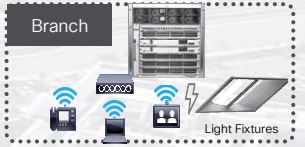










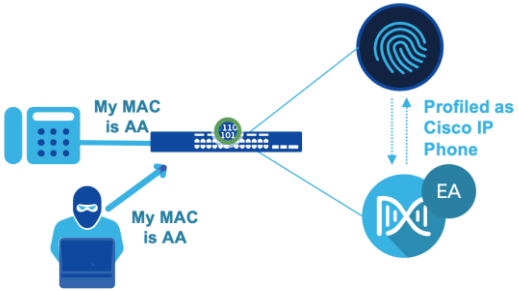
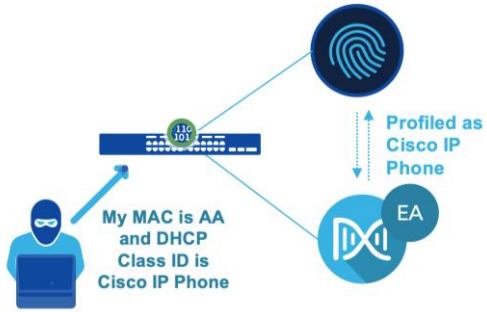


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auto-profiling and securing endpoints

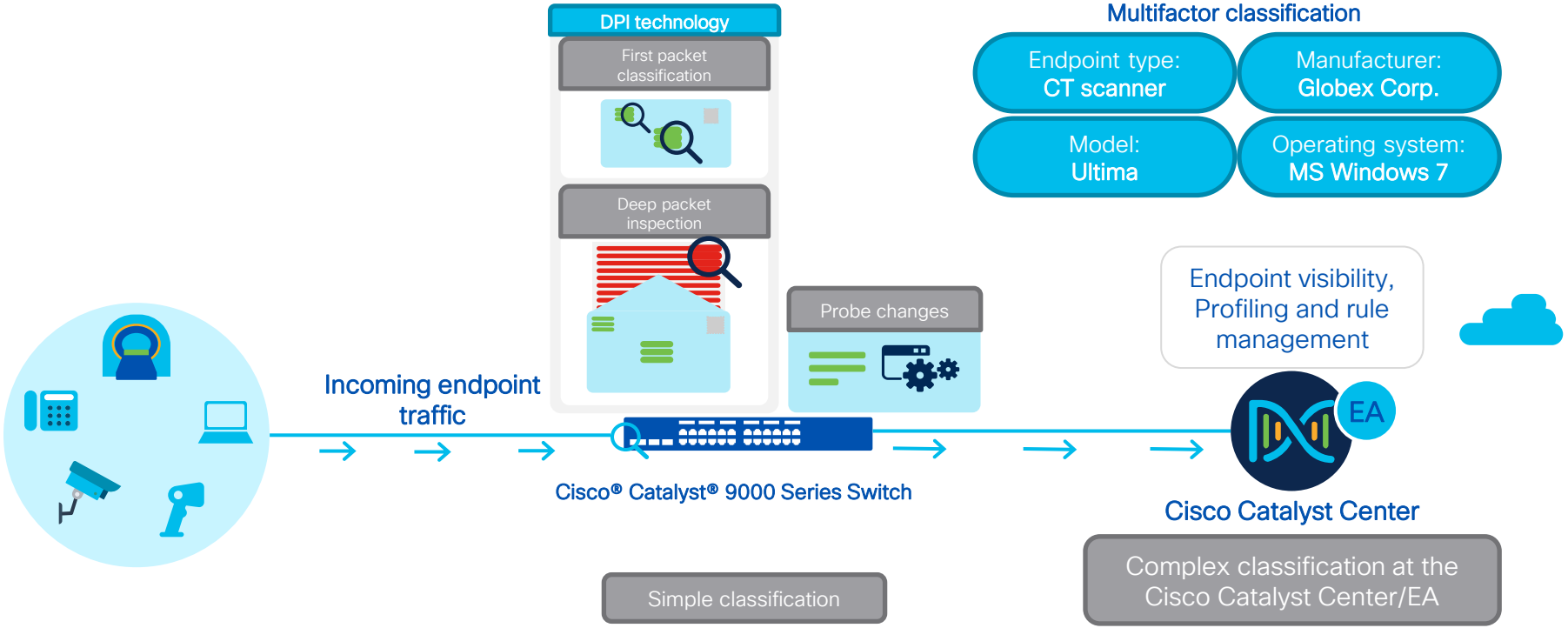


How Blade Hacks can attack an endpoint user…

Attack Persona	Attack Flow
 **MAC Spoofing**	 Impersonate the MAC address of another authorized endpoint in order to gain the same privileges
 **Attribute Spoofing**	 Impersonate class/type of the device in order to get privileged network access

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

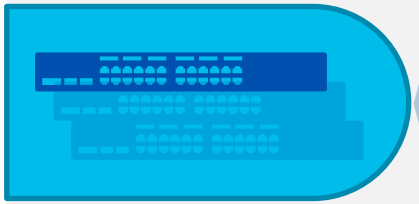
EA Profiling using NBAR on Catalyst 9000 Series Switch



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Traffic Telemetry Protocols

Support for 1400+ application protocols
Protocol library gets updated via Cisco catalyst center



Cisco® Catalyst ® 9000 Series Switch (Traffic Telemetry-Embedded)

Data plane protocols:

Infrastructure:	DNS
Healthcare:	DICOM, HL7
Web/IOT:	HTTP, SSL, MQTT, COAP…
Building automation:	BACNET
Multicast:	mDNS…
Media and communication:	RTSP, RTCP, SIP
Others:	CIFS, MS-SQL, NetBIOS

Discovery protocols:

CDP, LLDP, SNMP, DHCP, …

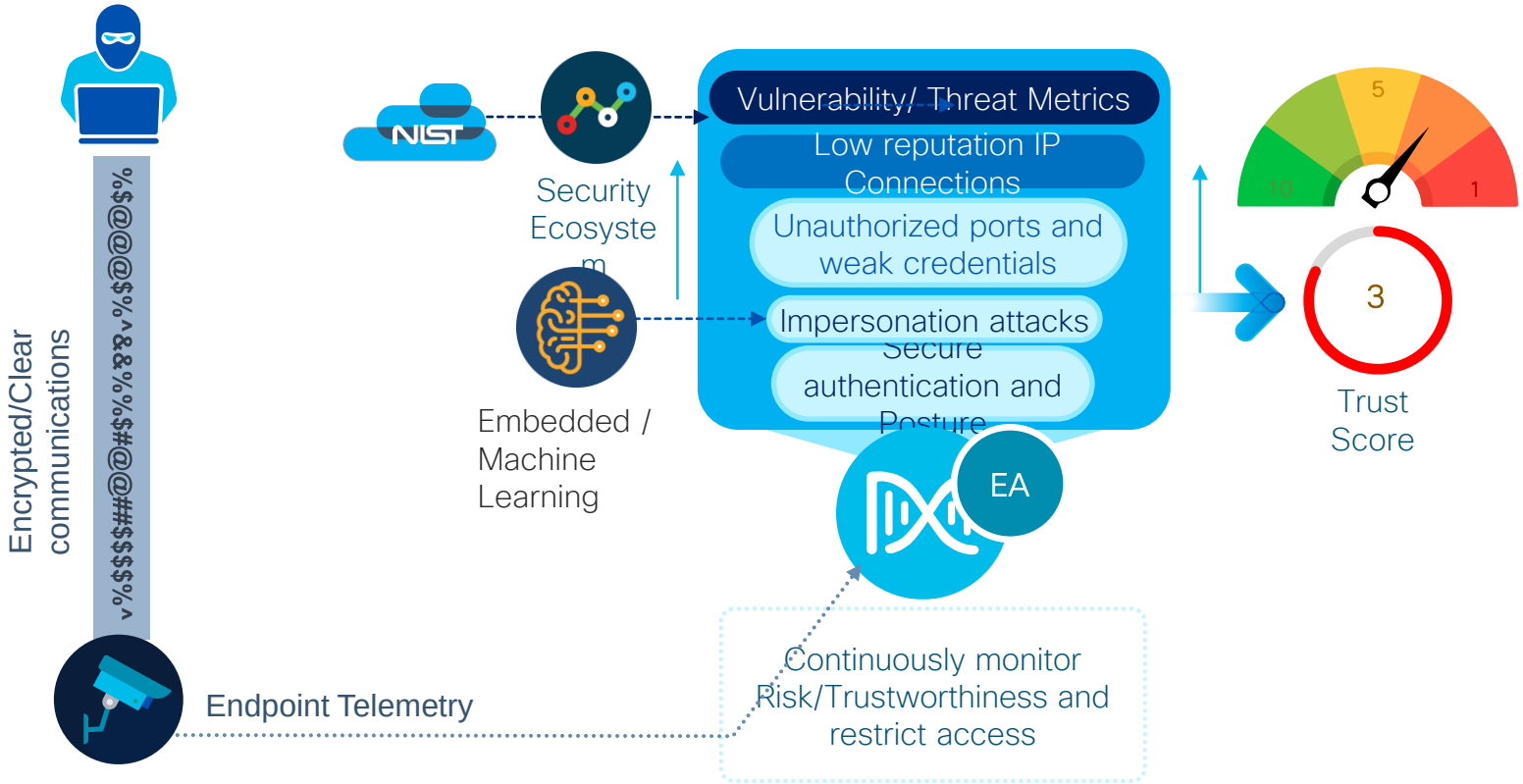
Traffic Telemetry conduit

- Conduit for classification and protocol library update from Cisco catalyst center
- Gleans endpoint discovery information from switches

Protocol Library: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

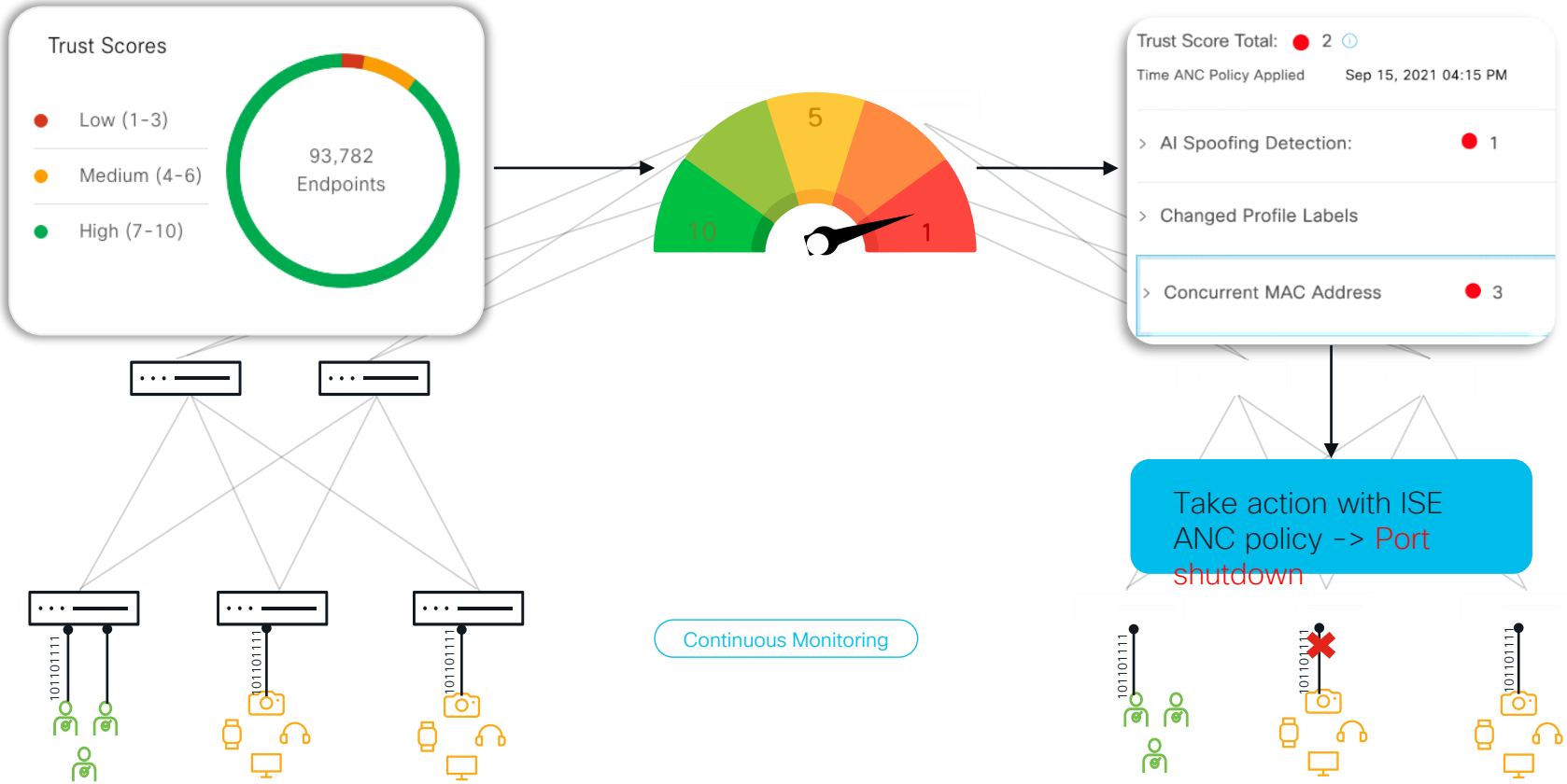
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continuous validation of endpoints for Trusted Access



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Trust Analytics



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco DNA Center

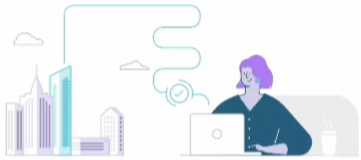
Explore

Learn about new capabilities in this release on the Cisco DNA Center YouTube Channel.

Stay up to date with your network and Cisco DNA Center through our insight email

Receive announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email.

Insights



Assurance Summary

Health

Healthy as of May 12, 2023 12:47 PM

84%	90%	95%
Network Devices	Wireless Clients	Wired Clients

View Details

Critical Issues

Last 24 Hours

4	6
P1	P2

View Details

Trends and Insights

Last 30 Days

4	5
AP Performance Advisories	Trend Deviations

View Details

Network Snapshot

Sites

Network Devices

Application QoS Policies

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key features with Endpoint & Trust Analytics

DPI-based endpoint profiling

- DPI-based endpoint profiling is a more deterministic approach to profiling, using active learning from endpoint connections and application traffic from sensors embedded in Cisco® hardware.

Cisco ISE integration

- Provides a way to gather attributes from sources such as AD, RADIUS, and external Identities.
- Cisco ISE assigns the right security policies, using EA profile labels.

ML clustering and crowdsourcing

- Reduce unknown endpoints in the network with ML. ML will cluster endpoints that have common attributes.
- Admin gets suggestions on labels learned from other customers with similar sets of endpoints.

ServiceNow integration

- Device owners can use ServiceNow to create assets (endpoints) that EA will learn.
- Admins can create custom rules to label endpoints using CMDB attributes.

Trust Analytics

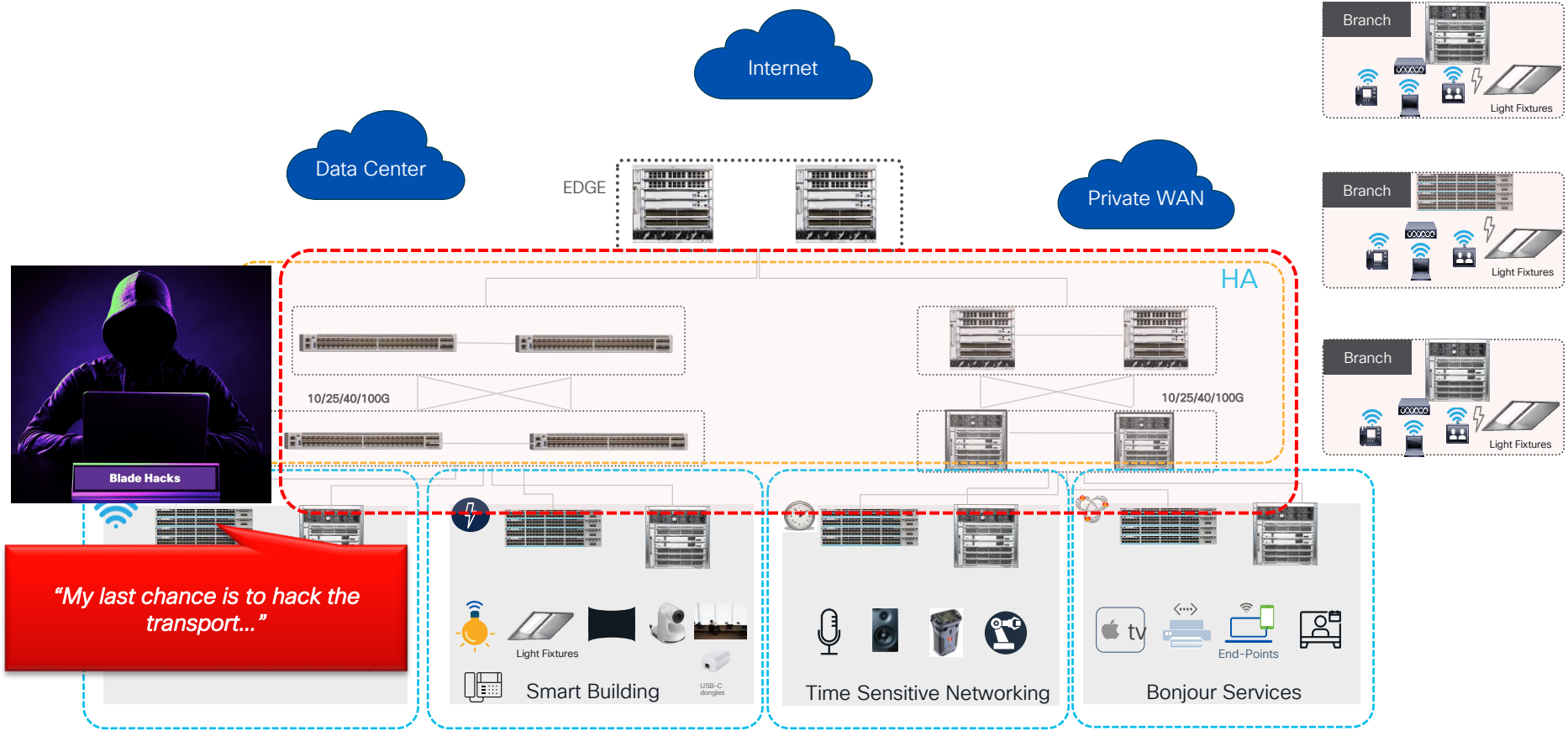
- EA performs ongoing validation of endpoint anomalies/risk from impersonation, insecure interfaces, unauthorized endpoints, behavioral variation and will be expanded to other areas of vulnerability/threats.
- Overall Trustworthiness of the endpoint is evaluated and used for Trusted access. Mitigation action can be taken from DNAC.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

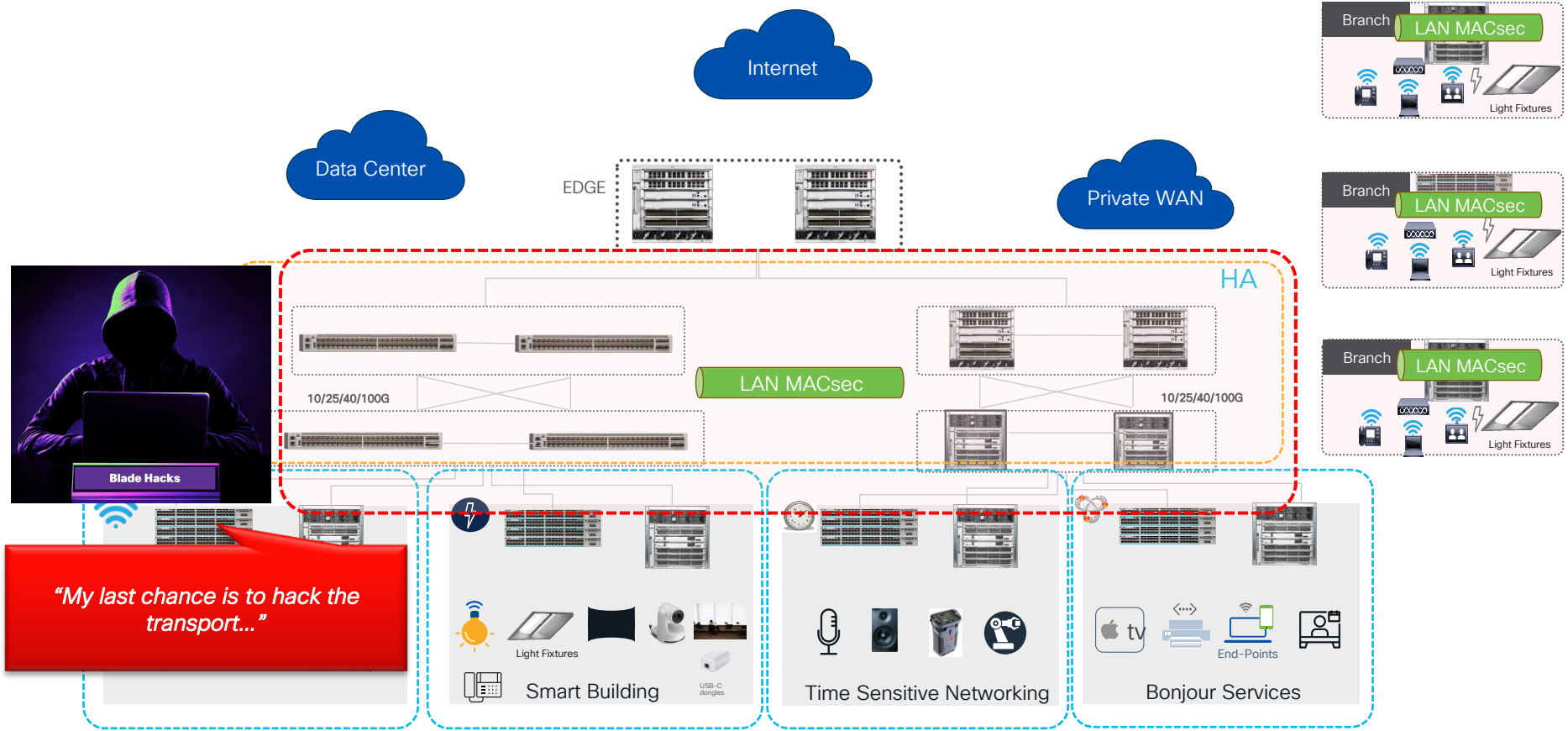
So, what's the score between John Doe and Blade Hacks?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

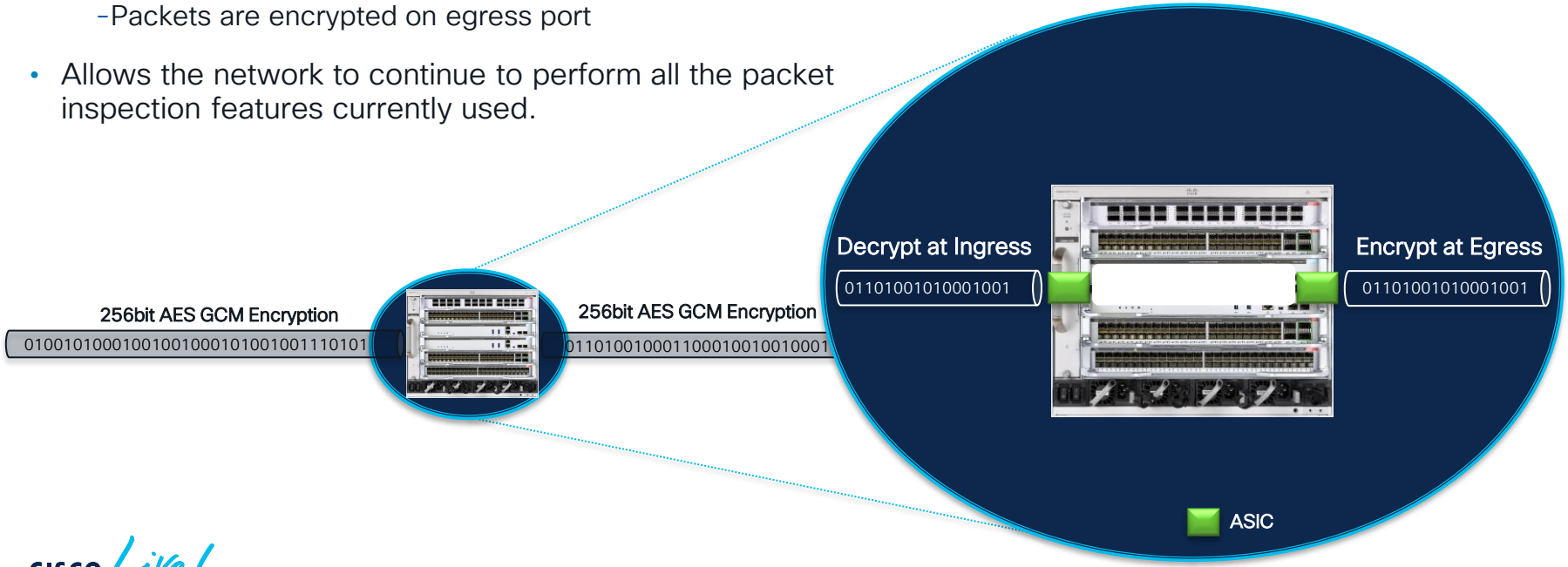


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is MAC Security (MACsec)?

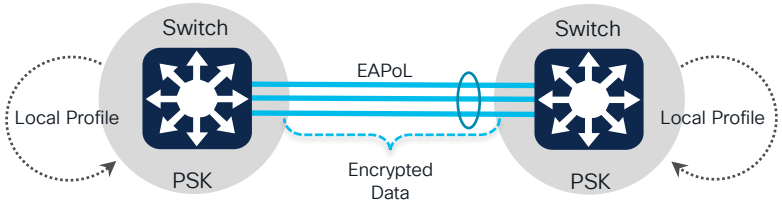
Hop-by-Hop Encryption via IEEE802.1AE

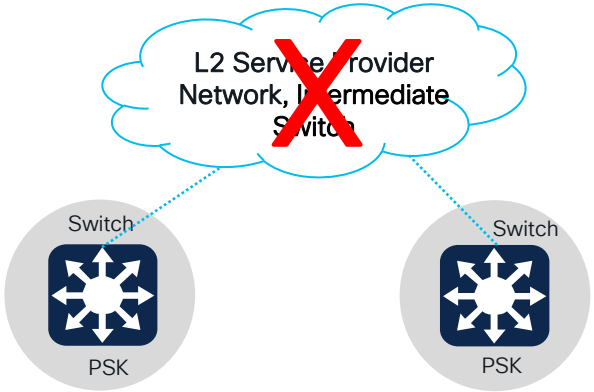
- Hop-by-Hop vs End-to-End “Bump-in-the-wire” model
  - Packets are decrypted on ingress port
  - Packets are encrypted on egress port
- Allows the network to continue to perform all the packet inspection features currently used.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

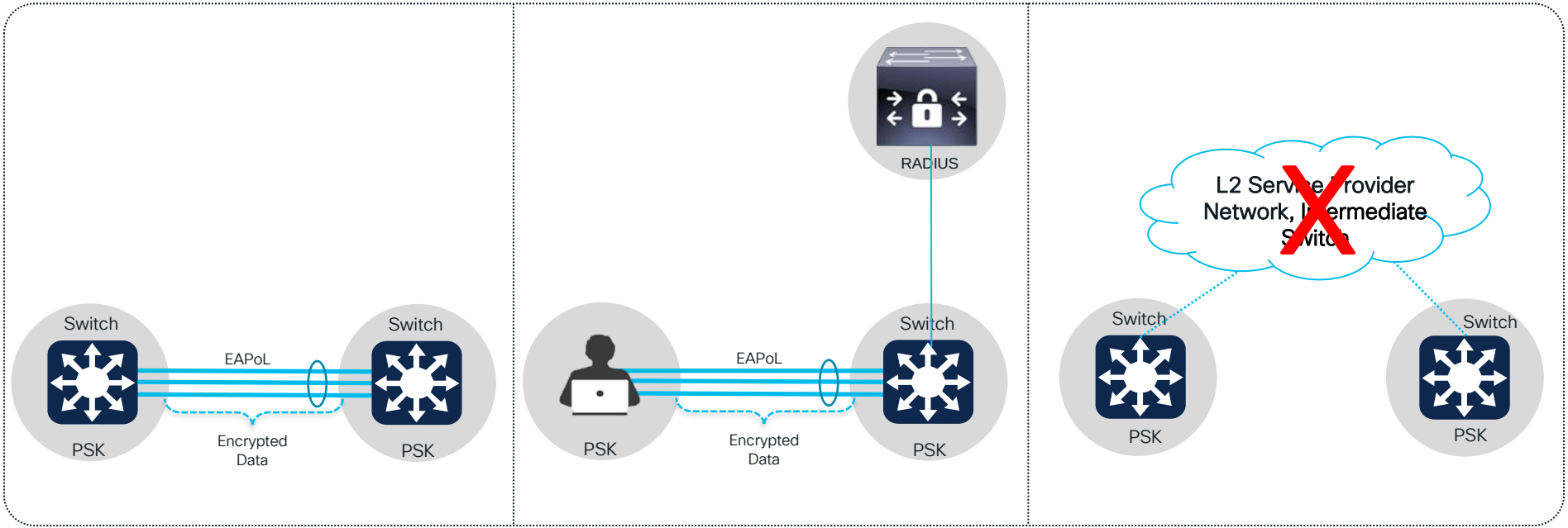
MACsec Switch to Switch Topology





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

MACsec Topologies



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



"I will try the unmanaged transport..."

L2 Extension

Internet

EDGE

HA

10/25/40/100G

10/25/40/100G

DISTRIBUTION

Branch

Light Fixtures

Branch

Light Fixtures

Branch

Light Fixtures

Fiber to the Desktop (

Servers and Desktops

Light Fixtures

Smart Building

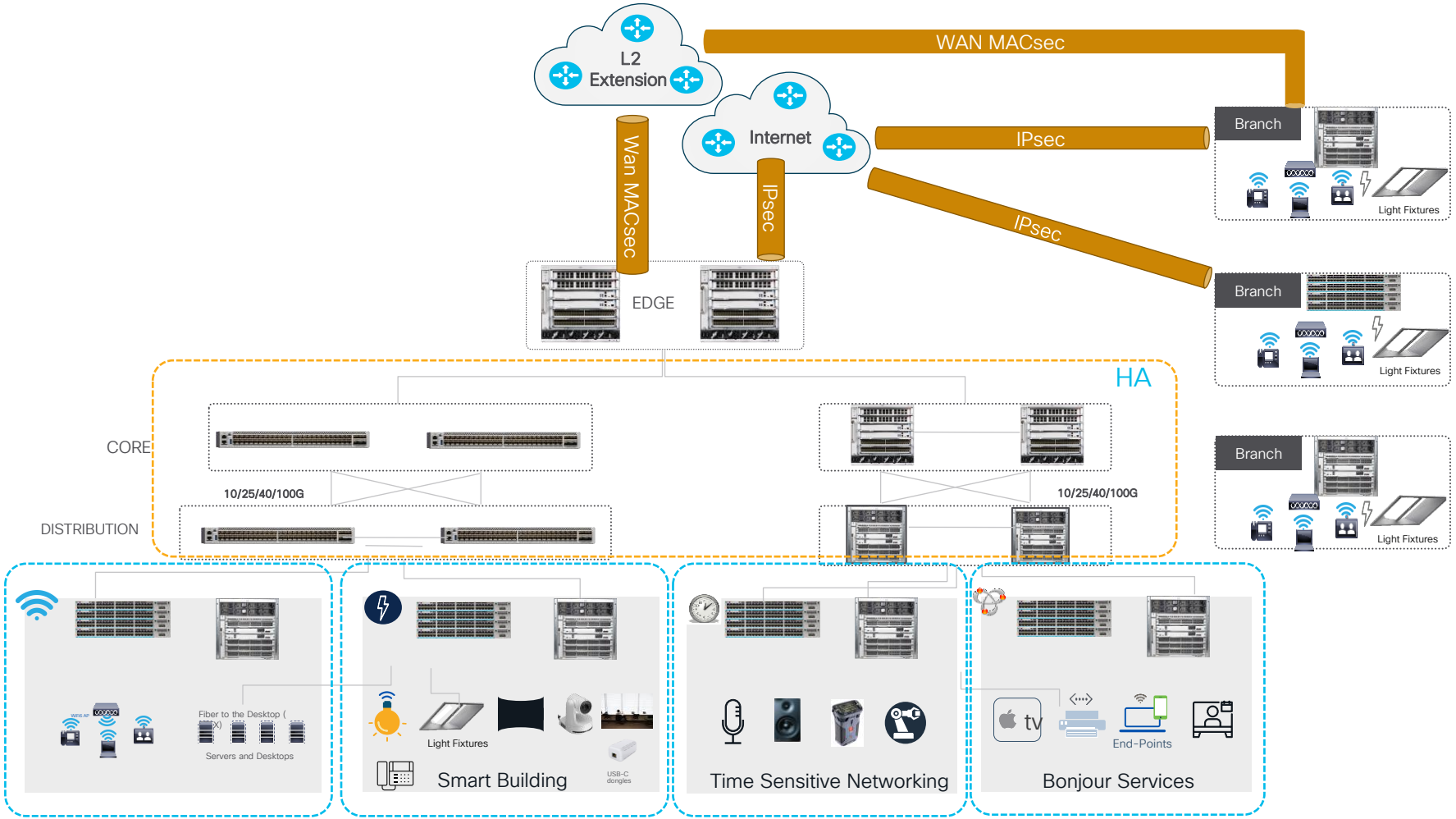
USB-C dongles

Time Sensitive Networking

tv

End-Points

Bonjour Services


L2
Extension
Internet
WAN MACsec
IPsec
IPsec
Wan MACsec
IPsec
EDGE
Branch
Light Fixtures
Branch
Light Fixtures
Branch
Light Fixtures
HA
CORE
DISTRIBUTION
10/25/40/100G
10/25/40/100G
Fiber to the Desktop (
Servers and Desktops
Light Fixtures
Smart Building
USB-C
dongles
Time Sensitive Networking
tv
End-Points
Bonjour Services

Internet is the new Enterprise WAN



DMAC	SMAC	ETYPE	IP	ESP Header	IP	L4	PAYLOAD	ESP Trailer	ESP Auth

Encrypted

Always watching for packets to steal !

Secure WAN

Secure access to apps and data from

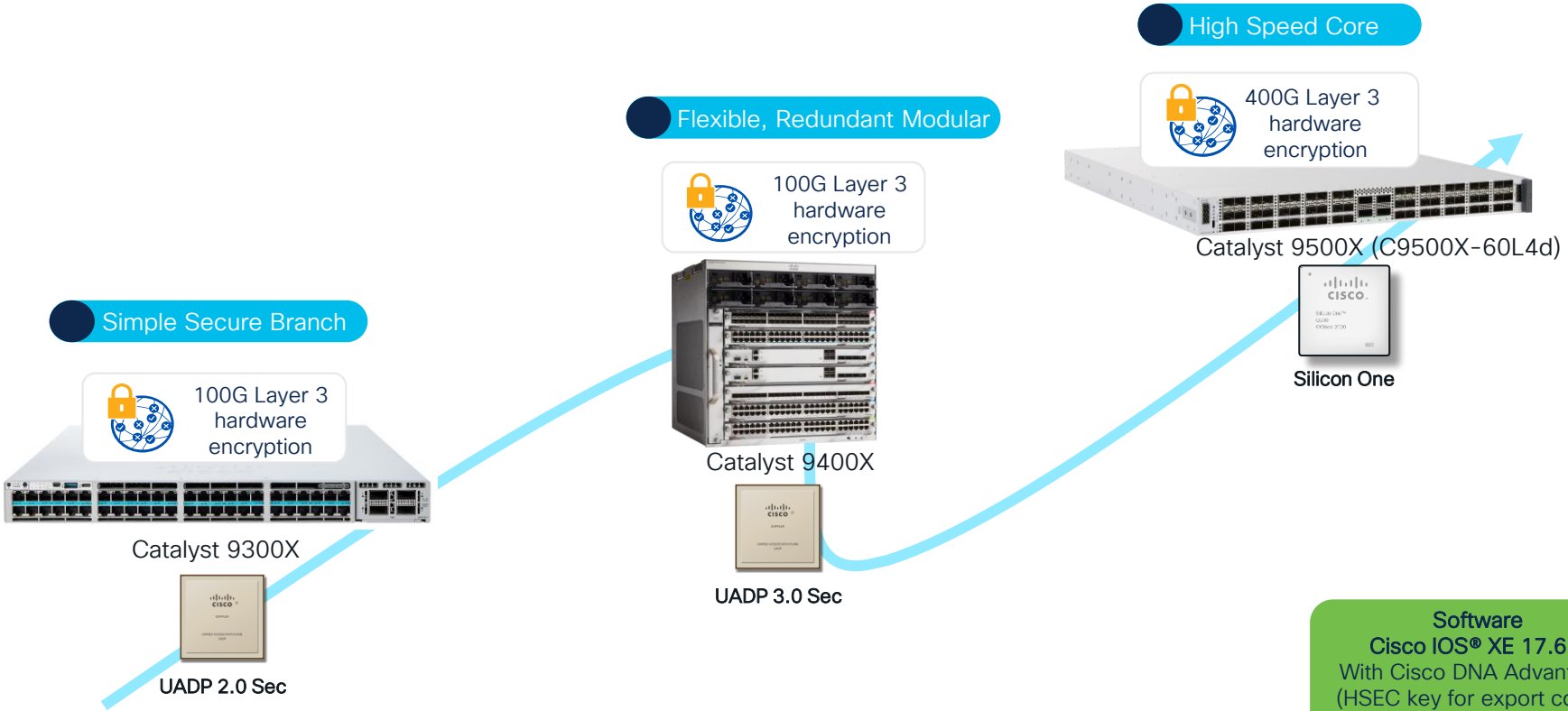
MultiCloud Access

Securely connect a hybrid workforce to apps anywhere

Remote Branch

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

High-Speed IPsec Encryption with Cat9k

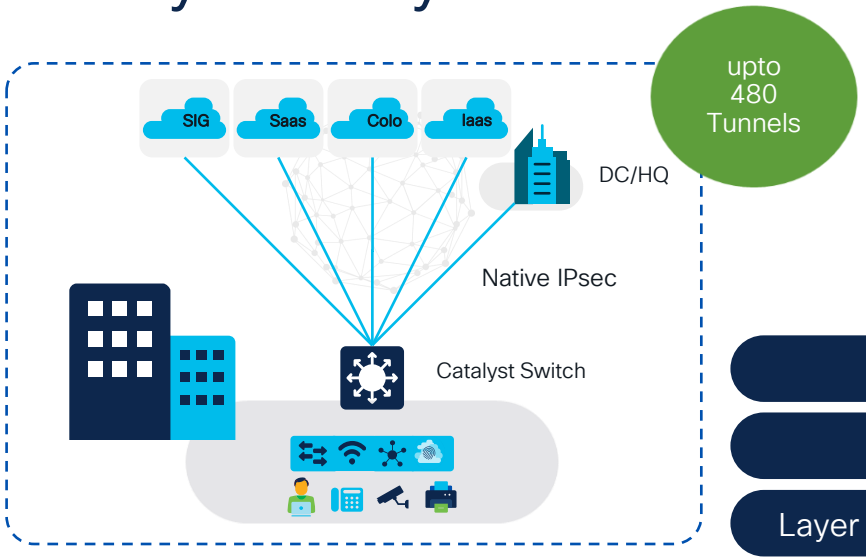


Software
Cisco IOS® XE 17.6.2
With Cisco DNA Advantage
(HSEC key for export control)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Connectivity to Anywhere

- Static virtual tunnel interface
- IPv4/IPv6
- OSPF/BGP
- Policy Based Routing
- VRF-aware



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

Tunnel mode

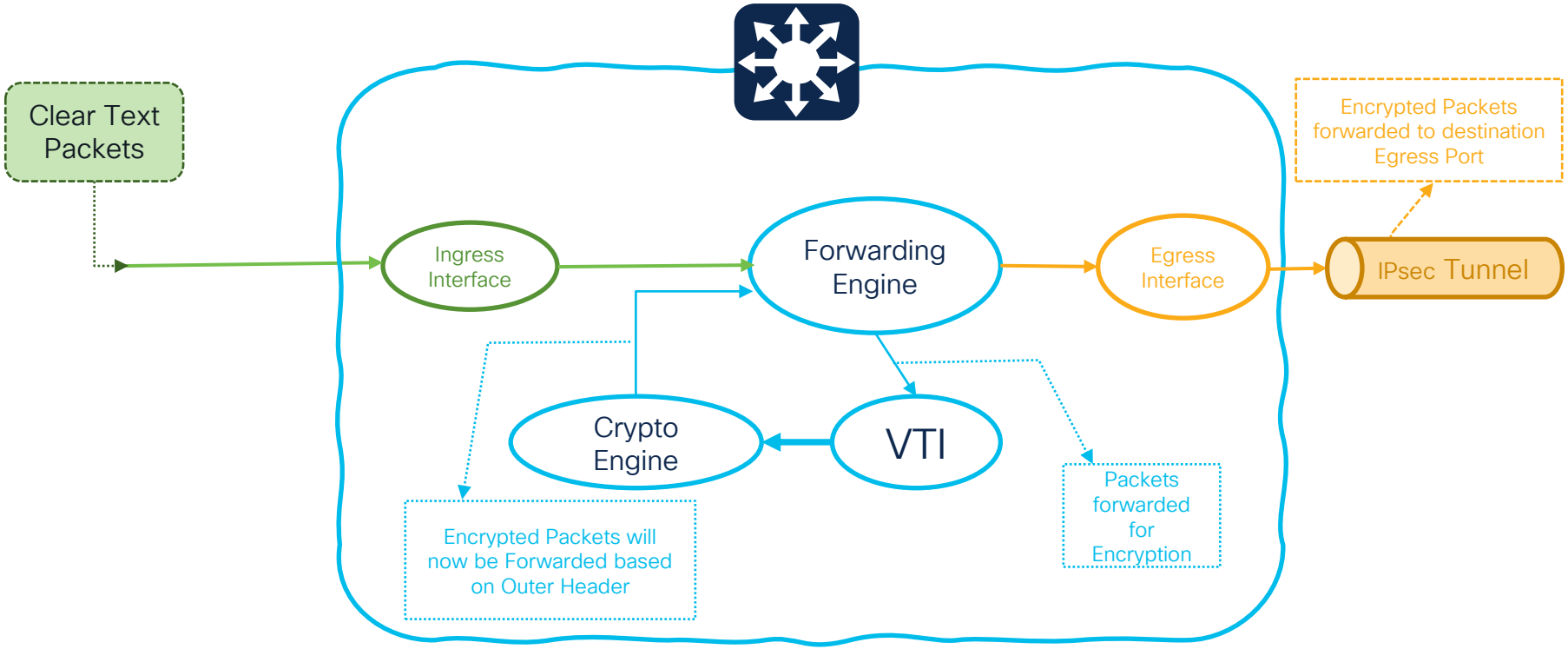
Encapsulation – ESP

IKEv2

- Multicast Routing
- NAT traversal
- Layer 3 segmentation over IPsec
- Layer 2 extension over IPsec

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec Packet Flow – Encryption



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Supported IKEv2 Proposal (Software)

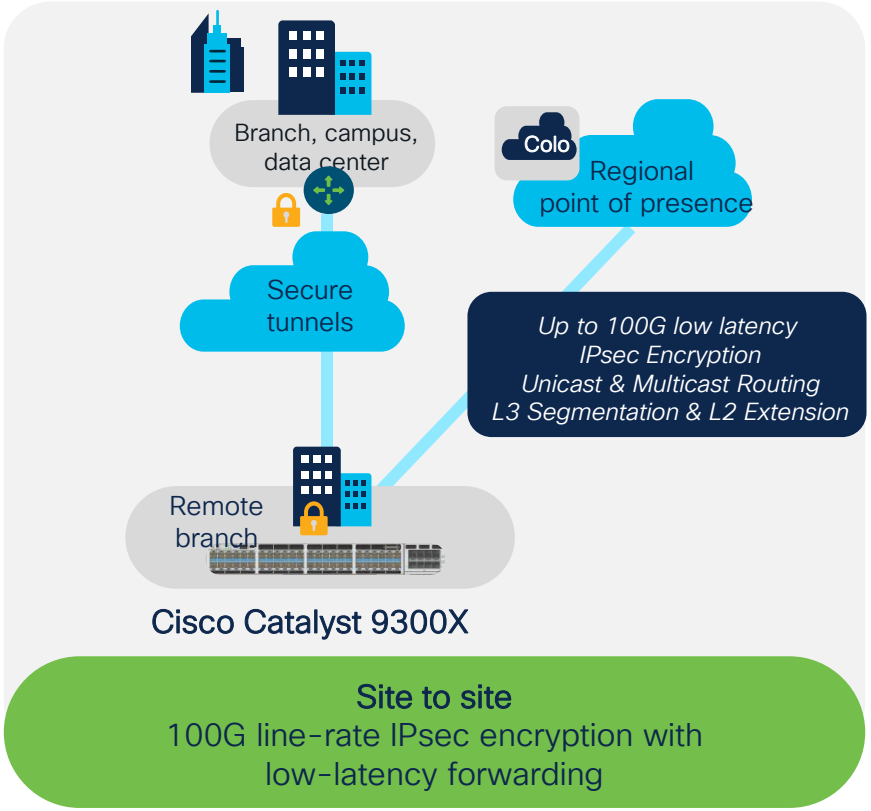
IKE	Encryption	Integrity	Deffie Helman
IKEv2	des 3des aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-gcm-128 aes-gcm-256	md5 sha1 sha256 sha384 sha512	1 – 768 MODP 2 – 1024 MODP 5 – 1536 MODP 14 – 2048 MODP 15 – 3072 MODP 16 – 4096 MODP 19 – 256 ECP 20 – 384 ECP 21 – 521 ECP 24 – 2048 (256 sub groups) MODP

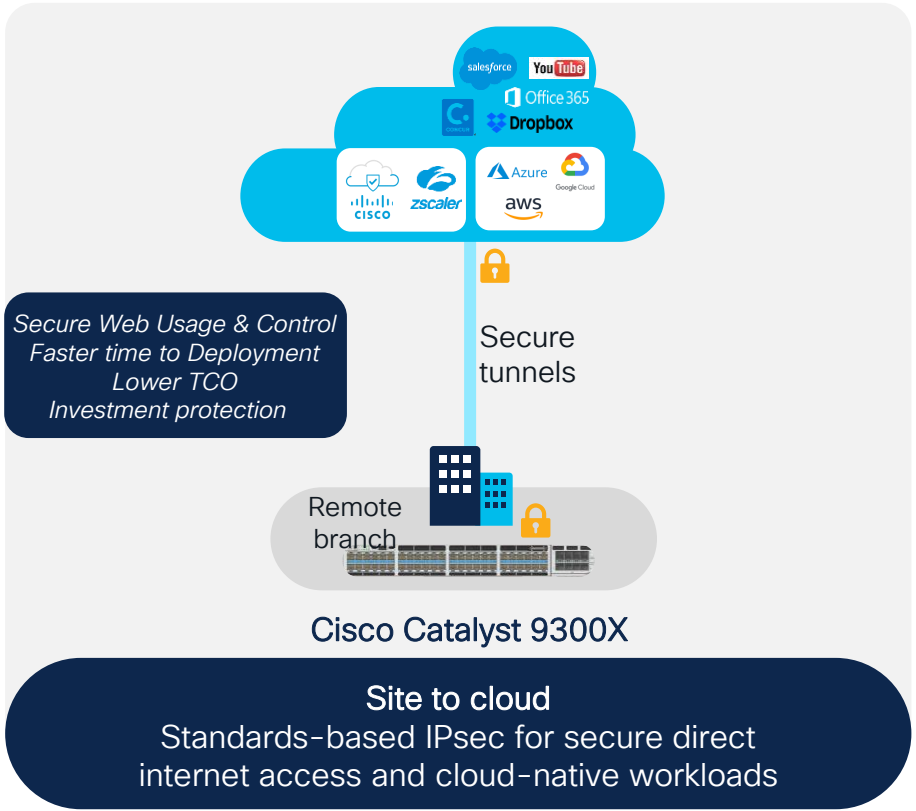
Supported Transform Sets (Hardware)

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

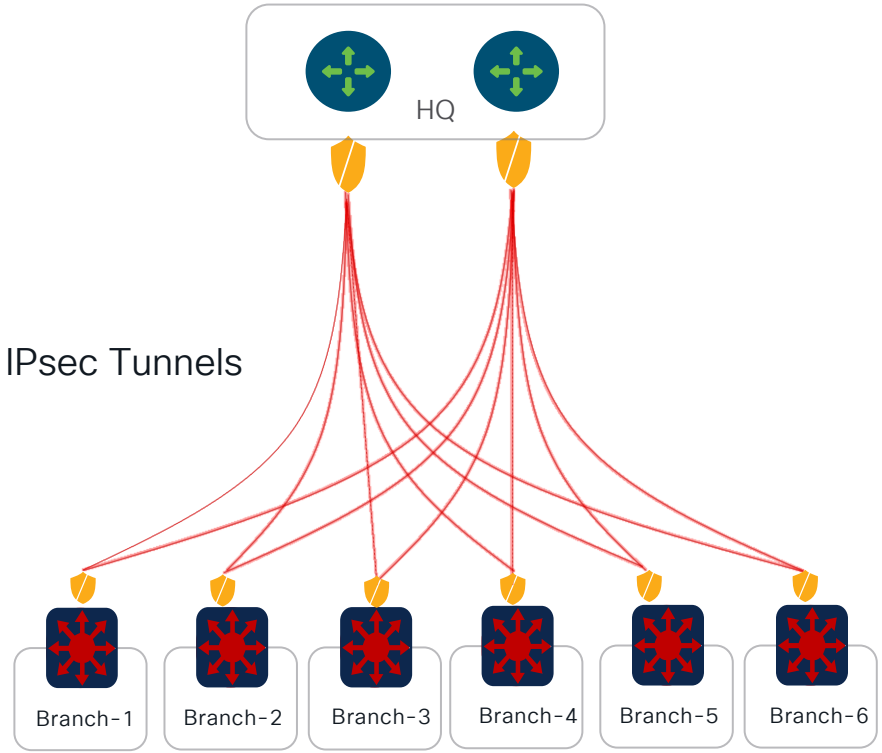
Catalyst 9k – Secure connectivity to anywhere





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

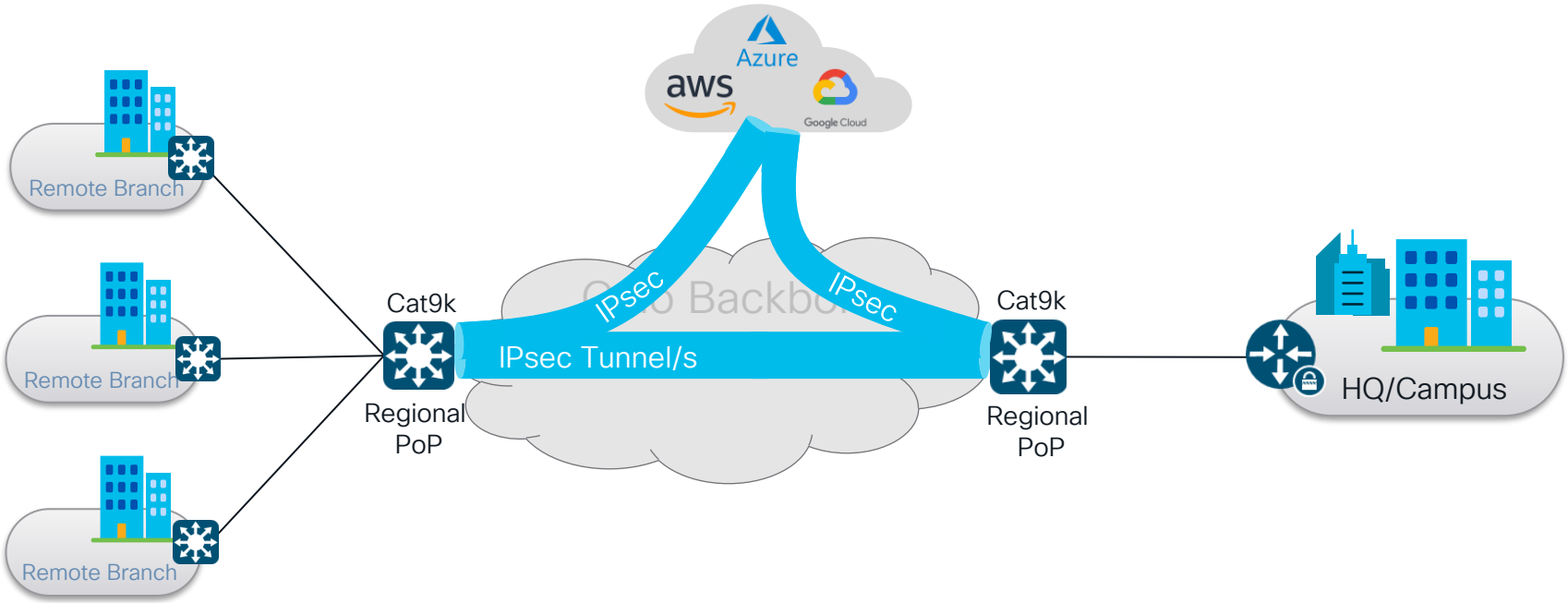
Catalyst 9000 – Site-to-Site IPsec



- High Speed Secure
- IPv4/IPv6
- VRF Aware
- OSPF/BGP
- Multicast Routing
- L3 segmentation over IPSEC
- L2 Extension over IPSEC
- NAT Traversal

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec Colo Connectivity

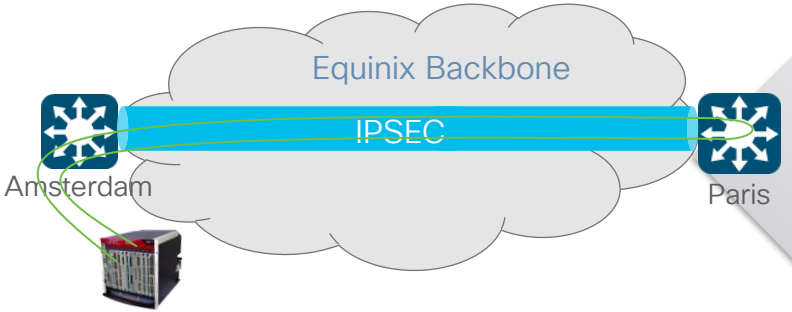


Key Benefits

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

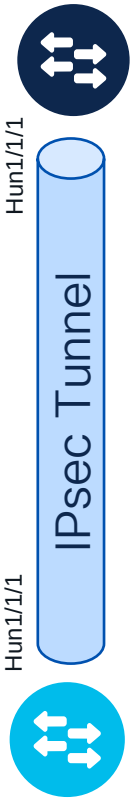
Consistent latency with/without IPsec encryption/decryption

- 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

Original test was done between San Jose and Los Angeles, US

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

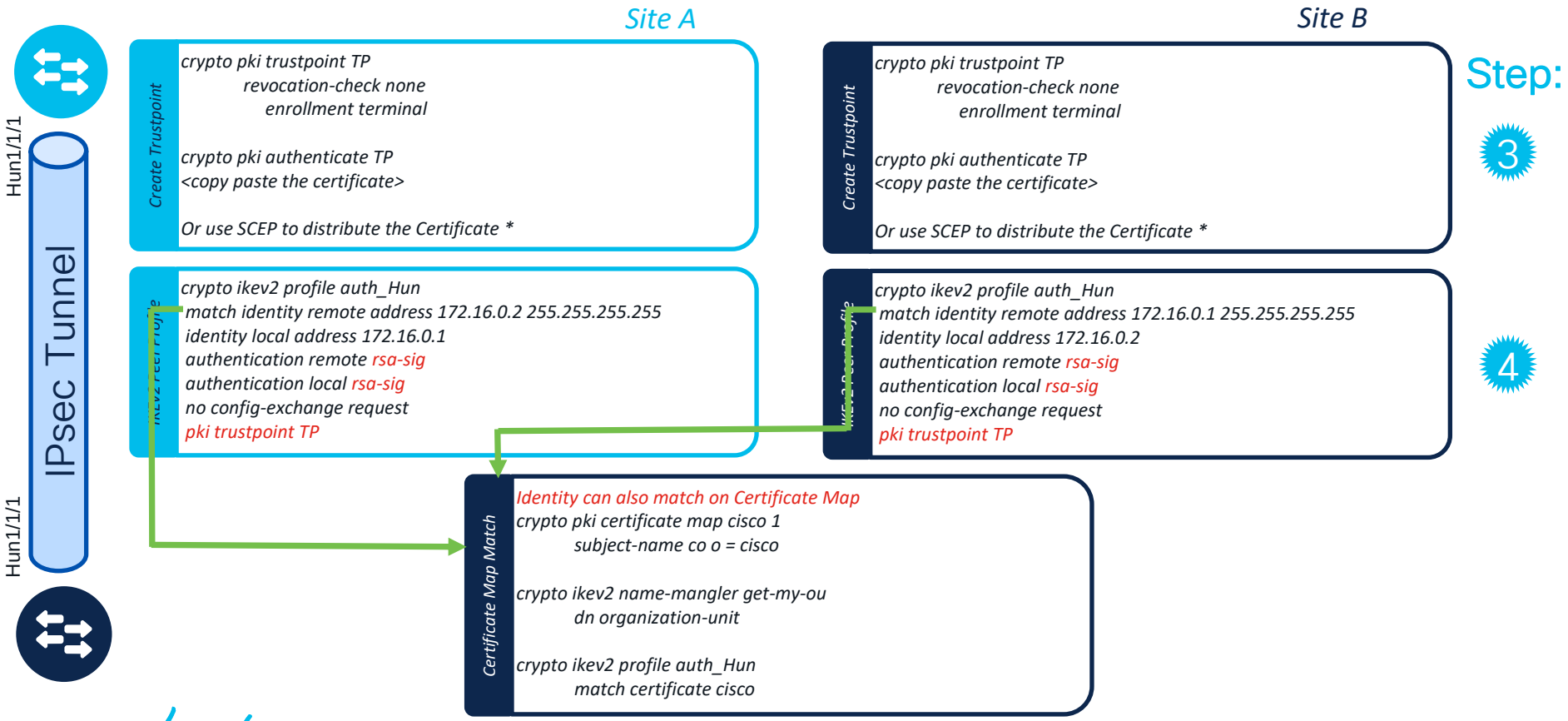
IPsec Site to Site / Point to Point with PSK



	Site A	Site B	Step:
IKEv2	crypto ikev2 proposal sitetosite encryption aes-cbc-256 integrity sha512 group 19 20 21 crypto ikev2 dpd 10 5 periodic	crypto ikev2 proposal sitetosite encryption aes-cbc-256 integrity sha512 group 19 20 21 crypto ikev2 dpd 10 5 periodic	1
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	crypto ikev2 policy hun_ipsec match address local 172.16.0.2 proposal sitetosite crypto ikev2 policy peers match fvrf any proposal sitetosite	2
IKEv2 Peer	crypto ikev2 keyring auth-keyring peer 172.16.0.2 address 172.16.0.2 pre-shared-key Cisco12345Cisco12345	crypto ikev2 keyring auth-keyring peer 172.16.0.1 address 172.16.0.1 pre-shared-key Cisco12345Cisco12345	3
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	crypto ikev2 profile auth_Hun match identity remote address 172.16.0.1 255.255.255.255 identity local address 172.16.0.2 authentication remote pre-share authentication local pre-share keyring local auth-keyring no config-exchange request	4

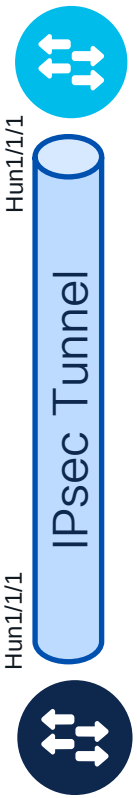
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec Site to Site / Point to Point with PKI / Certificate



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec Site to Site / Point to Point

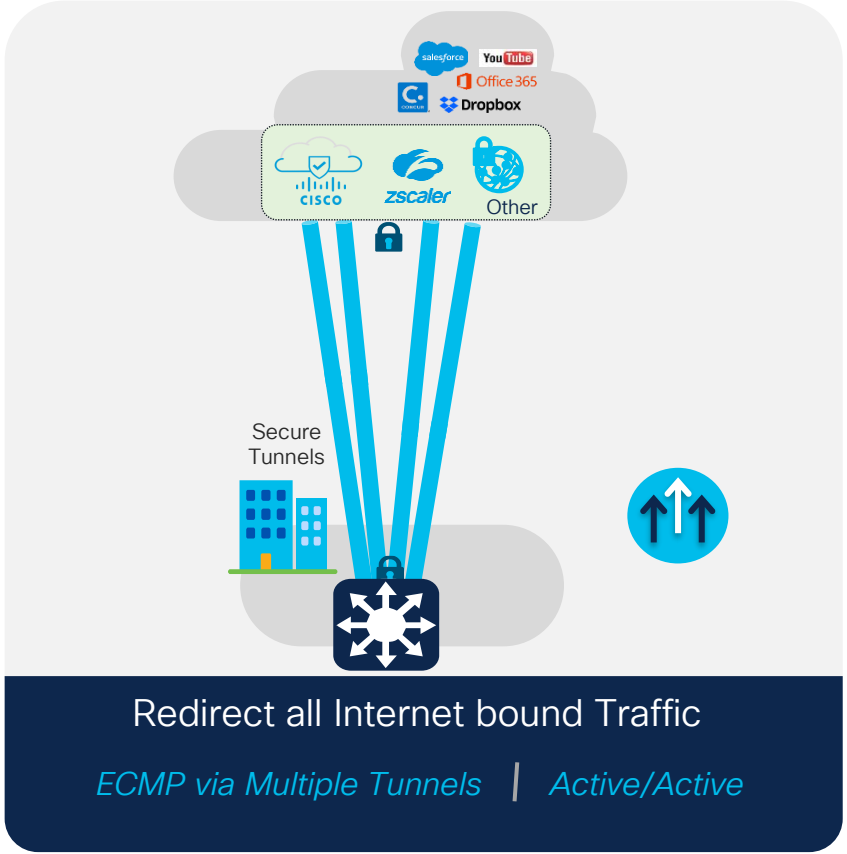


	Site A	Site B	Step:
Transform Set	crypto ipsec transform-set auth-ipsec esp-gcm 256 mode tunnel	crypto ipsec transform-set auth-ipsec esp-gcm 256 mode tunnel	5
IPsec Profile	crypto ipsec profile site-to-site set security-association lifetime seconds 28800 set security-policy limit 1 (optional) set transform-set auth-ipsec set ikev2-profile auth_Hun	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	6
Physical Port	interface HundredGigE1/1/1 no switchport ip address 172.16.0.1 255.255.255.0	interface HundredGigE1/1/1 no switchport ip address 172.16.0.2 255.255.255.0	7
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	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	8
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	ip routing ip route 10.11.10.0 255.255.255.0 30.30.30.1 ip route 24.25.24.24 255.255.255.255 30.30.30.1	9

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

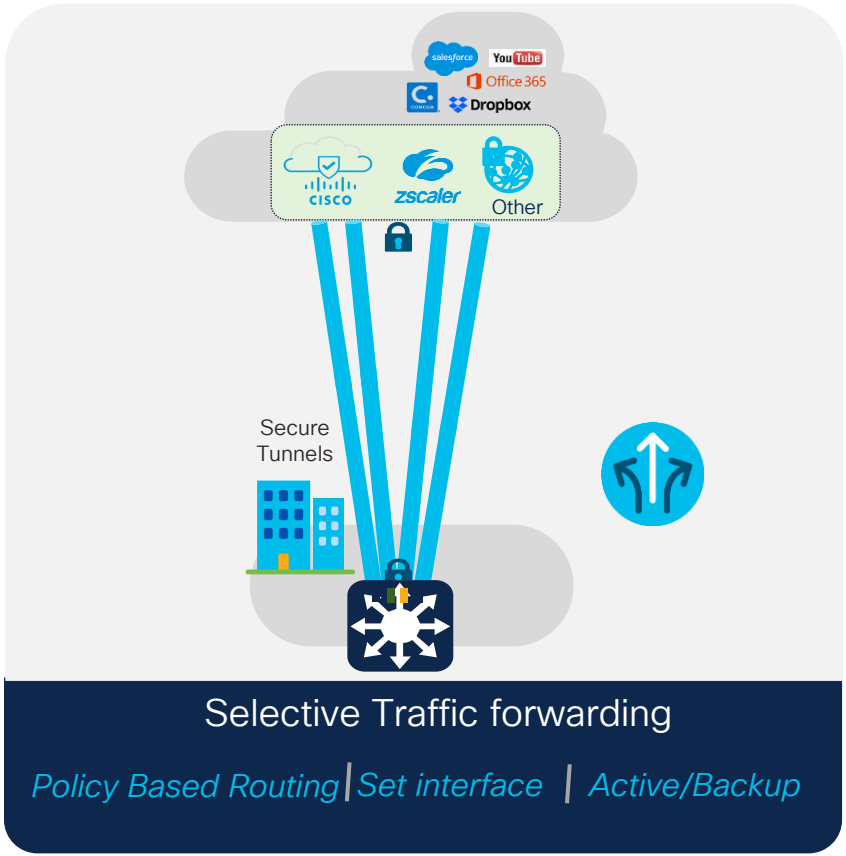
Site-to-Cloud: Secure Internet Gateway

Securing Internet Traffic



Redirect all Internet bound Traffic

ECMP via Multiple Tunnels | *Active/Active*



Selective Traffic forwarding

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella SIG / Zscaler

IKEv2

```
crypto ikev2 proposal umb_sig
 encryption aes-cbc-128
 integrity sha1
 group 19 20 21
crypto ikev2 nat keepalive 20
crypto ikev2 dpd 10 5 periodic
```

IKEv2 Policy

```
crypto ikev2 policy umb_sig
 match fvrf any
 proposal umb_sig
```

IKEv2 Keyring

```
crypto ikev2 keyring umb_sig
 peer umbrella
  description ikev2_peer_146.112.85.8
  address 146.112.85.8
  pre-shared-key Cisco12345Cisco12345
```

IKEv2 Data Center Profile

```
crypto ikev2 profile umb_sig
   match identity remote address 146.112.85.8 255.255.255.0
   identity local email atlan-edge2-tun@7971867-595120711-umbrella.com
   authentication remote pre-share
   authentication local pre-share
   keyring local umb_sig
   dpd 10 2 periodic
   no config-exchange request
```



IPsec Tunnel



Catalyst 9k

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella SIG / Zscaler

Transform Set

```
crypto ipsec transform-set umb_sig esp-aes esp-sha-hmac
 mode tunnel
```

IPsec Profile

```
crypto ipsec profile umb_sig
 set transform-set umb_sig
 set ikev2-profile umb_sig
```

Physical/Virtual Port

```
interface Vlan2
 no switchport
 ip address 128.107.251.122  255.255.255.0
 load-interval 30
```

Create IP in IP tunnel

```
interface Tunnel1
 ip unnumbered GigabitEthernet1/0/1
 tunnel source GigabitEthernet1/0/1
 tunnel mode ipsec ipv4
 tunnel destination 146.112.85.8
 tunnel protection ipsec profile umb_sig
```

Routes

```
ip route 0.0.0.0 0.0.0.0 Tunnel1
ip route 146.112.85.8 255.255.255.255 128.107.251.65
```

Policy Based Routing

```
route-map UMB_PBR_RM permit 10
 match ip address UMB_PBR_ACL
 set interface Tunnel1 Tunnel2
route-map UMB_PBR_RM permit 20
!
ip access-list extended UMB_PBR_ACL
 10 permit ip host 192.168.1.10 any
```

OR



IPsec Tunnel



Catalyst 9k

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella SIG



IPsec Tunnel



Cisco Umbrella

Deployments / Core Identities

Add A New Tunnel

Tunnel Name

test-tunnel123

Device Type

Other

For example, AWS, Azure, or OCI.

Tunnel ID and Passphrase

Tunnel ID Format

Email IP Address

Tunnel ID

test-tunnel123 @{org}-{tunnel}.umbrella.com

Passphrase

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

Passphrases match

Site

Associate Tunnel with Site

Default Site

Routing

Add all public and private address ranges used internally by your organization. For more information, see Umbrella's Help. For multiple values, use comma separators.

IP Address Ranges (Optional)

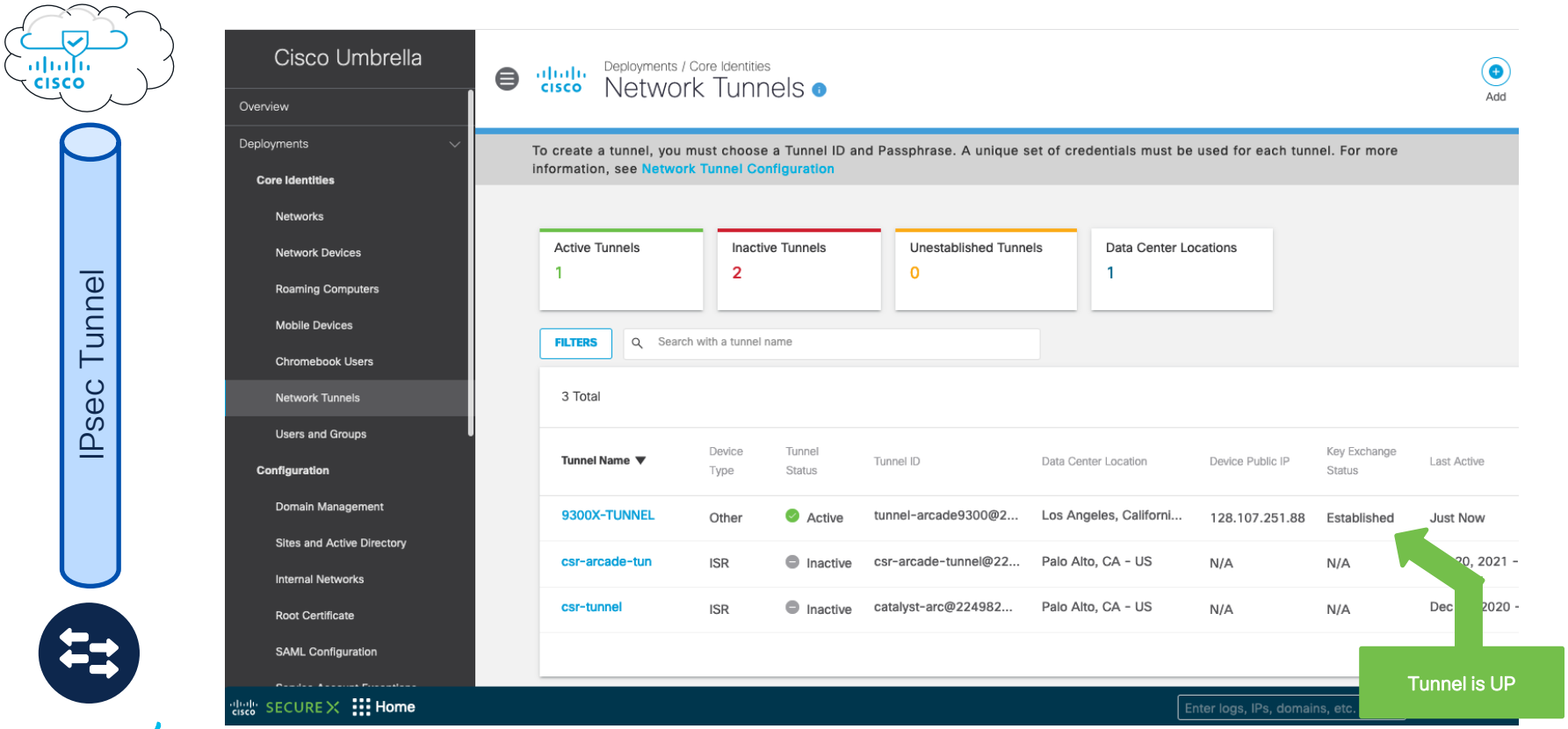
For example, 203.0.113.0/24

ADD

CANCEL SAVE

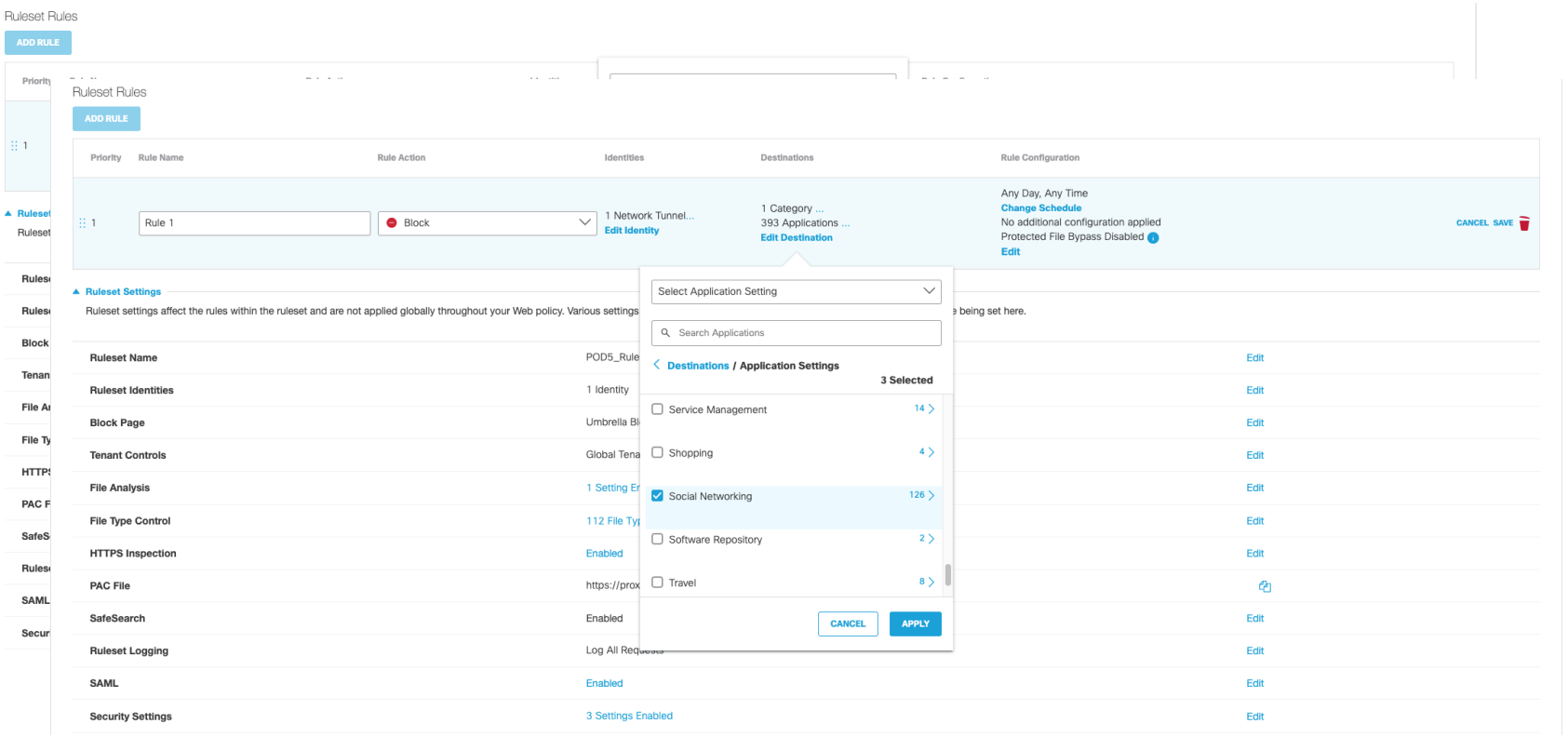
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella SIG



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

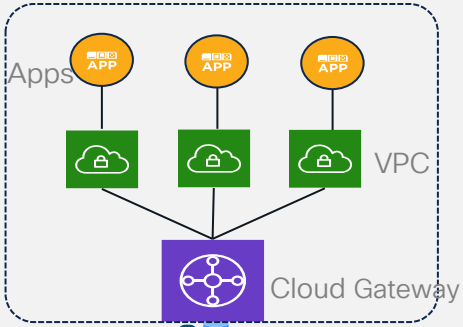
IPsec to Umbrella SIG



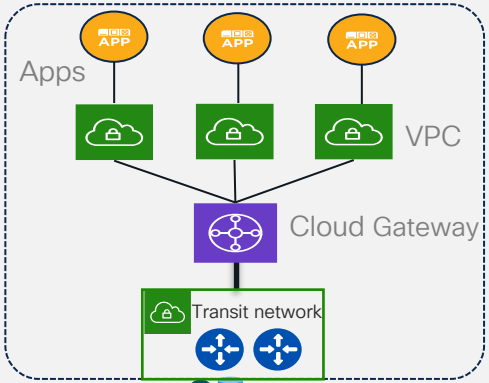
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Site-to-Cloud: Cloud Service Providers

Secure connectivity to Native Cloud Resources







Native IPSEC termination on CSP's

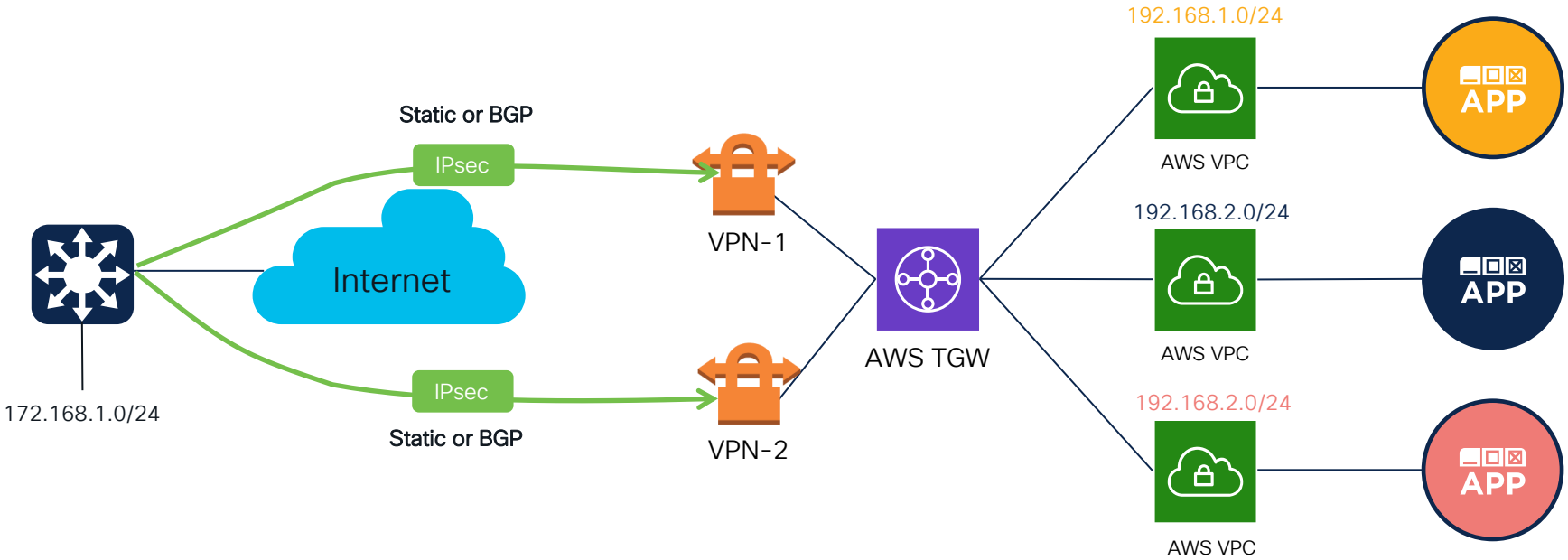
Static/BGP | Active/Backup | Active/Active

IPSEC termination on CSP's Transit Networks

Static/BGP | Active/Backup | Active/Active

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst 9000 – AWS Workflow



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella AWS

IKEv2

```
crypto ikev2 proposal aws_tgw
 encryption aes-cbc-128
 integrity sha1
 group 19 20 21
crypto ikev2 nat keepalive 20
crypto ikev2 dpd 10 5 periodic
```

IKEv2 Policy

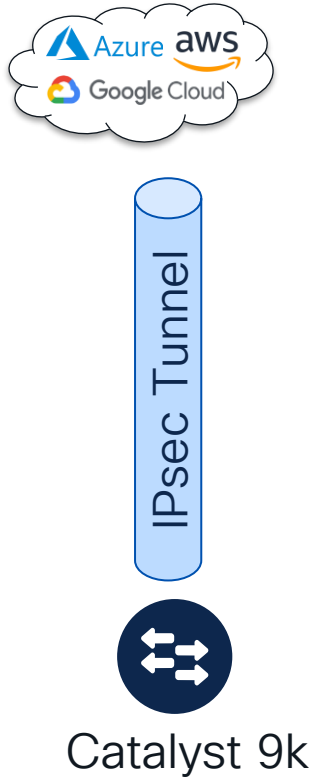
```
crypto ikev2 policy aws_tgw
 match fvrf any
 proposal aws_tgw
```

IKEv2 Keyring

```
crypto ikev2 keyring aws_tgw
 peer umbrella
  description ikev2_peer_52.8.92.5
  address 52.8.92.5
  pre-shared-key Cisco12345Cisco12345
```

IKEv2 Data Center Profile

```
crypto ikev2 profile aws_tgw
 match identity remote address 52.8.92.5 255.255.255.0
 identity local address 128.107.251.88
 authentication remote pre-share
 authentication local pre-share
 keyring local aws_tgw
 dpd 10 2 periodic
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec to Umbrella SIG and AWS

Transform Set

```
crypto ipsec transform-set aws_tgw esp-aes esp-sha-hmac
 mode tunnel
```

IPsec Profile

```
crypto ipsec profile aws_tgw
 set transform-set aws_tgw
 set ikev2-profile aws_tgw
```

Physical/Virtual Port

```
interface Vlan2
 no switchport
 ip address 128.107.251.122  255.255.255.0
 load-interval 30
```

Create IP in IP tunnel

```
interface Tunnel1
 ip address 169.254.16.102 255.255.255.252
 tunnel source Vlan2
 tunnel mode ipsec ipv4
 tunnel destination 52.8.92.5
 tunnel protection ipsec profile aws_tgw
```

Routes

```
ip route 0.0.0.0 0.0.0.0 Tunnel1
ip route 52.8.92.5 255.255.255.255 128.107.251.65
```

OR

Create IP in IP tunnel

```
router bgp 65000
 neighbor 169.254.16.101 remote-as 65001
 address-family ipv4
 network 192.168.1.0
 neighbor 169.254.16.101 activate
```



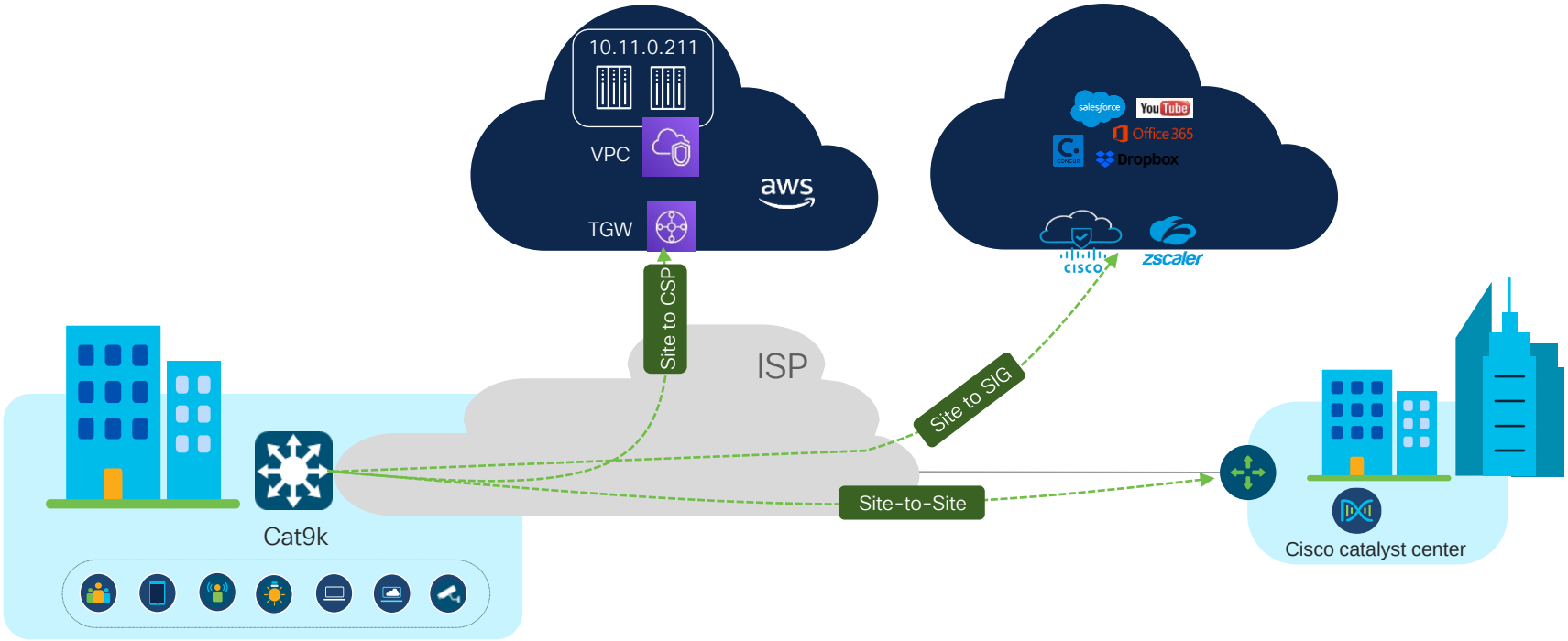
IPsec Tunnel



Catalyst 9k

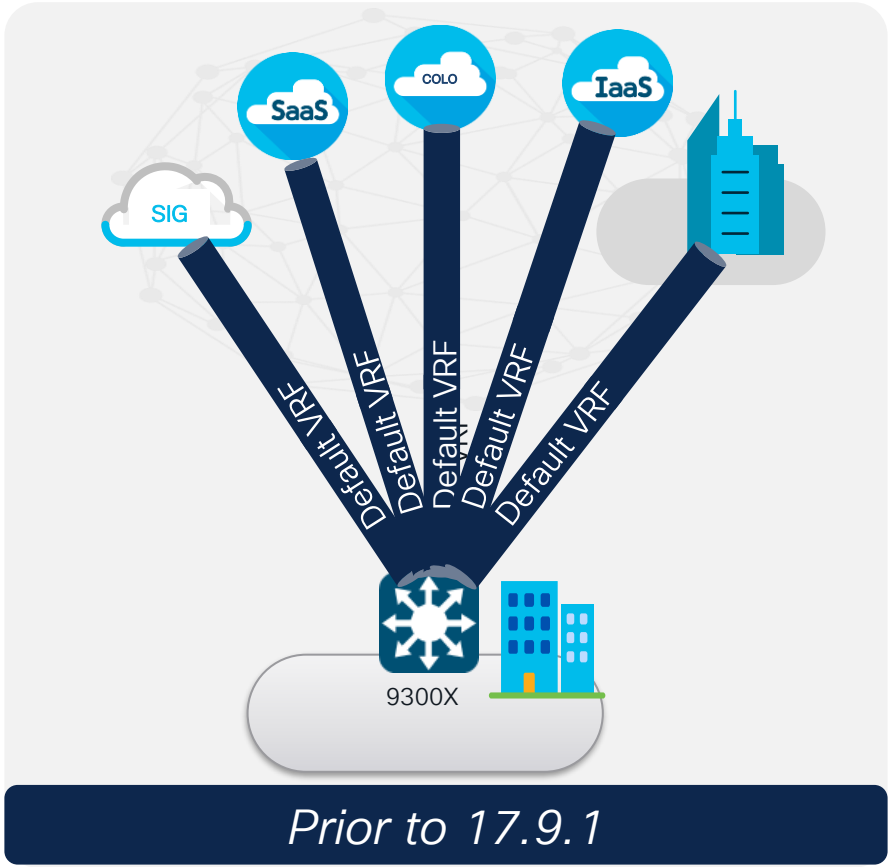
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cat9k – Secure Connectivity to Anywhere

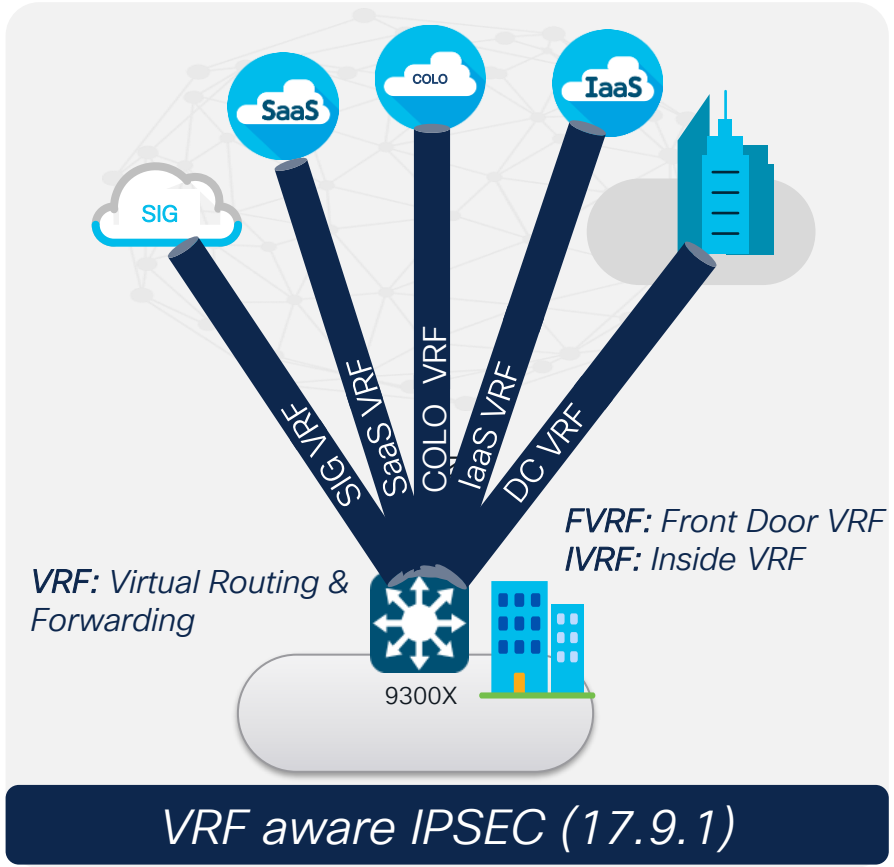


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

VRF Aware IPsec



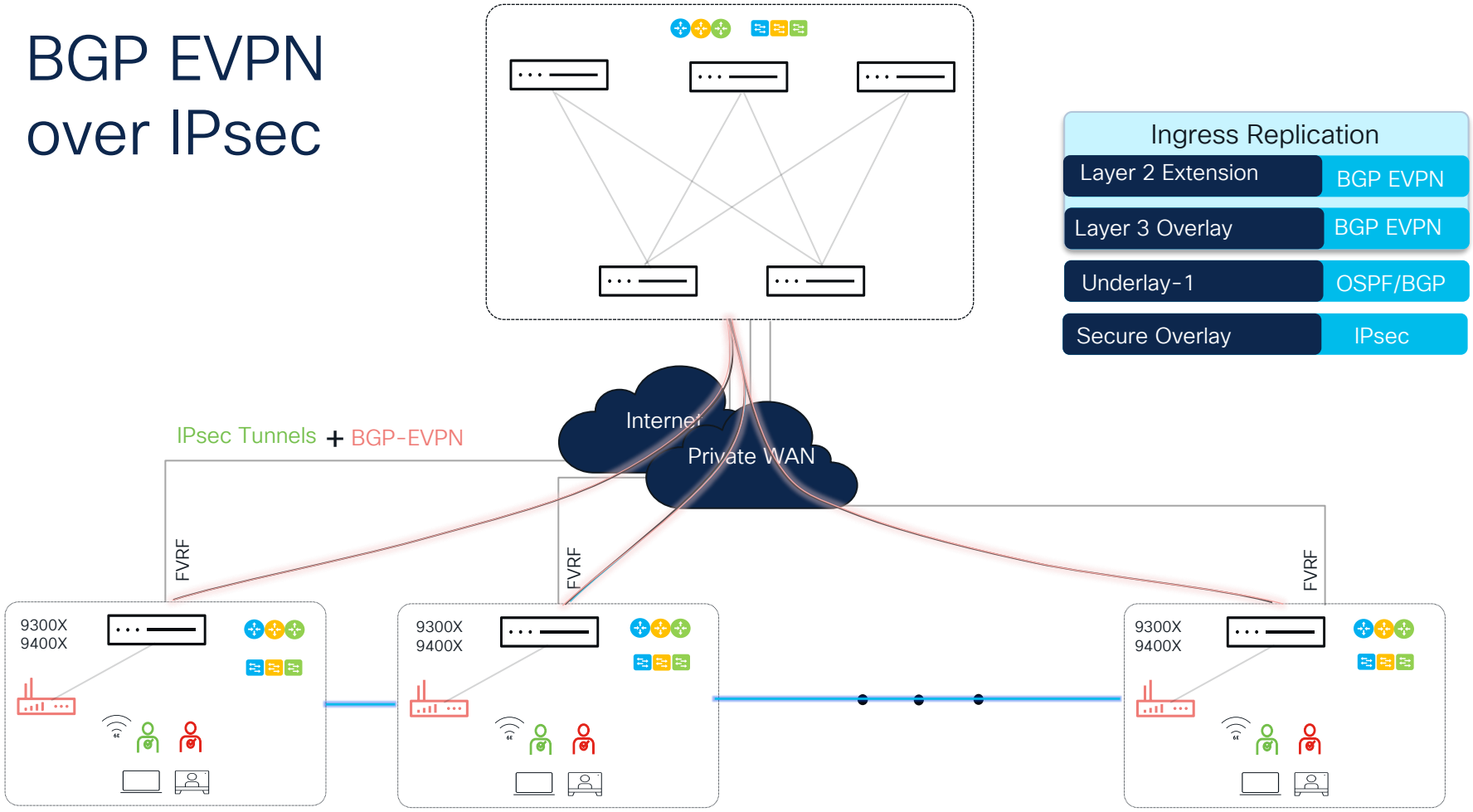
Prior to 17.9.1



VRF aware IPSEC (17.9.1)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BGP EVPN over IPsec



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst 9000 IPSEC – Automation & Monitoring

Flexible consumption options

Modes

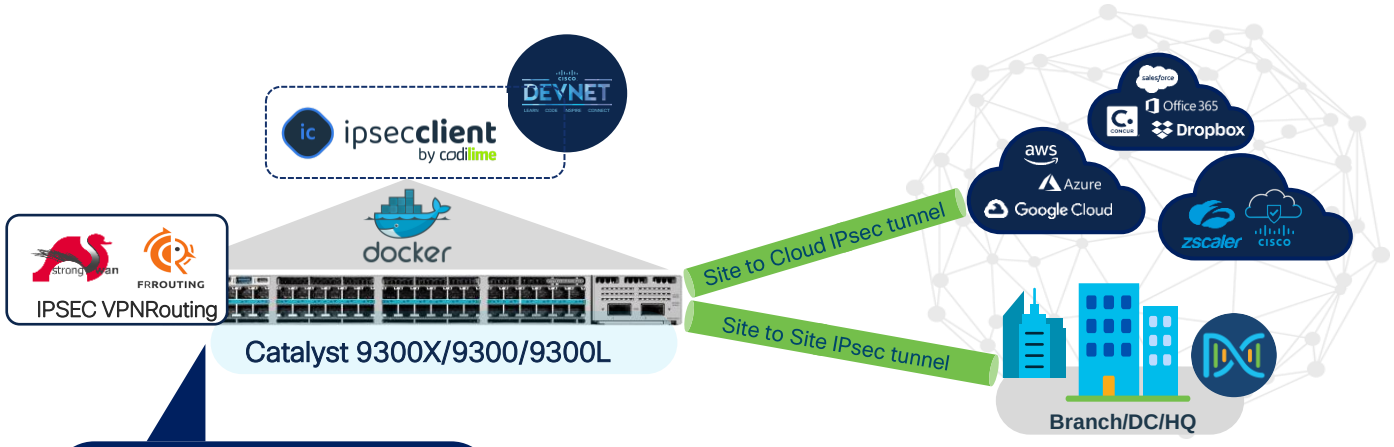
Turnkey with Cisco catalyst center (Beta)	DIY w/IOS XE (Shipping)	Ecosystem Integrators (Shipping)
Centralized management and monitoring Increased scalability	Distributed deployment using CLI/YANG APIs Flexible Consumption	Deployment via Ansible, Terraform, Chef etc. Seamless integration w/existing tools

Benefits

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Codilime: IPsec delivered via App-Hosting

Cisco IOS® XE 17.10
With Cisco DNA Advantage



App Resources

Memory (RAM)	: 409 MB
Disk (SSD)	: 10 MB
CPU	: 1480 units
CPU-percent	: 20 % of 1 core

Performance

~200Mbps Traffic Encryption

- IPsec VPN Application hosted on Cat9k
- Runs in Docker container
- Interactive Web UI for IPsec config
- SW IPsec - C9300/9300L
- HW & SW IPsec - C9300X
- Will be available on Cisco DEVNET

Security

- IPsec IKEv2
- Authentication using PSK or x509

Protocol Support

- VRF Aware
- NAT
- NAT-T

Automation

- YANG model with REST API

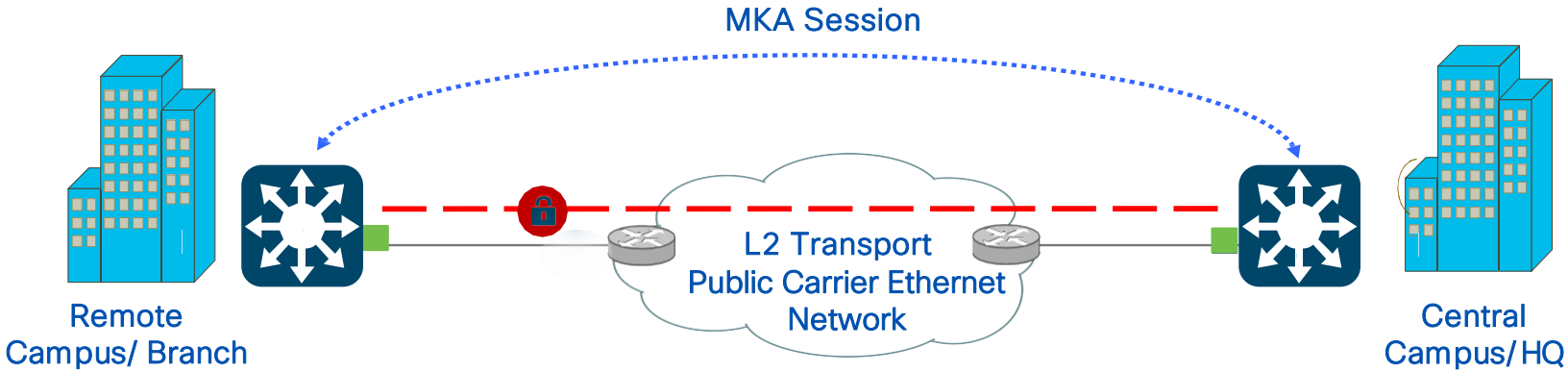
Interoperability

- AWS, GCP, Azure
- Cisco Umbrella, Zscaler
- C8K, ISR/ASR, Juniper

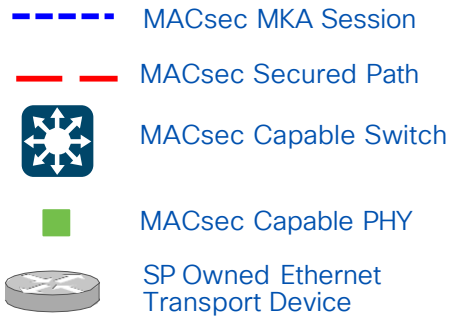
Available at Github

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

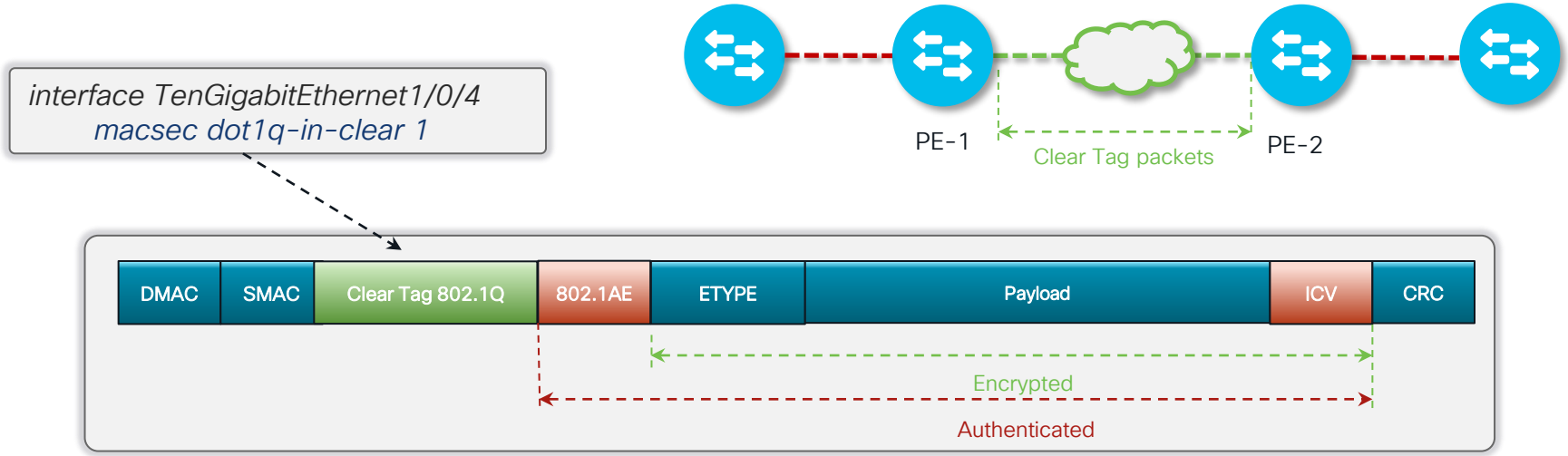
- AES-256 (AES/GCM) support
- Standards Based MKA key framework
  - (defined in 802.1X-2010) within Cisco security
- Ability to support 802.1Q tags in clear
  - Offset 802.1Q tags in clear before encryption
- Vital Network Features to Interoperate over Public Carrier Ethernet Providers
  - Ability to 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

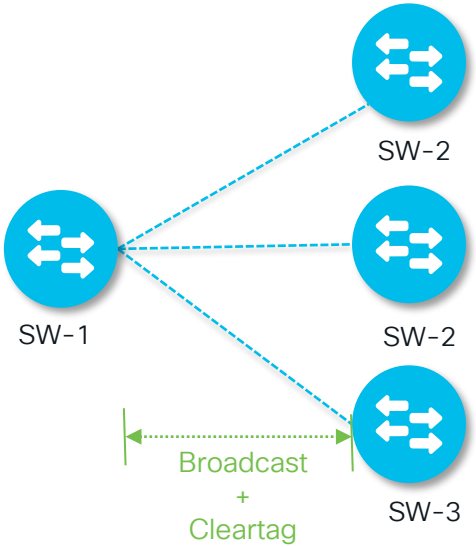


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

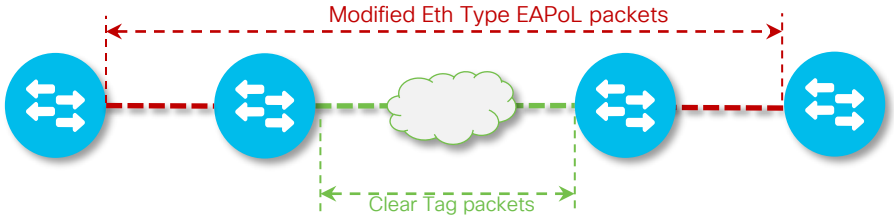
```
interface TenGigabitEthernet1/0/4
      eapol destination-address broadcast
      macsec dot1q-in-clear 1
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

MKA EAPoL EtherType Tuning

- Leverages a “well known” ether type value.
- By default, EAPoL EthType is 0x888E
- Can be used with or without “Clear Tag”

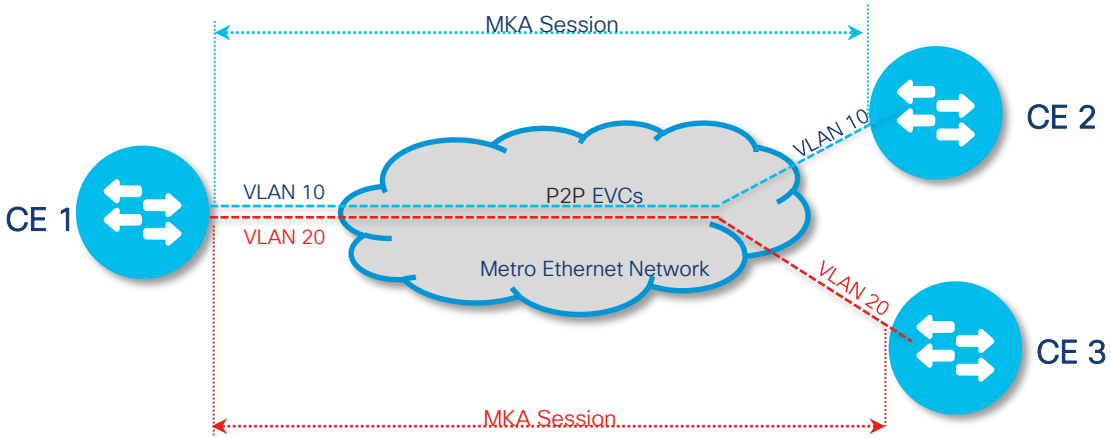



```
interface TenGigabitEthernet1/0/4
 eapol eth-type 876F
 macsec dot1q-in-clear 1
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



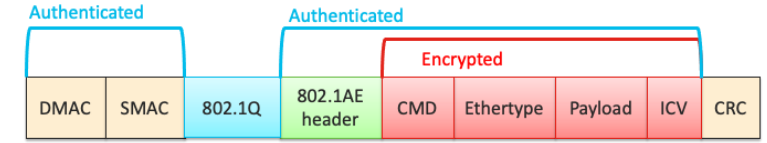
Security Associations **from CE 1**:

Tx: CE 1 → CE 2

CE 1 → CE 3

Rx: CE 2 → CE 1

CE 3 → CE 1

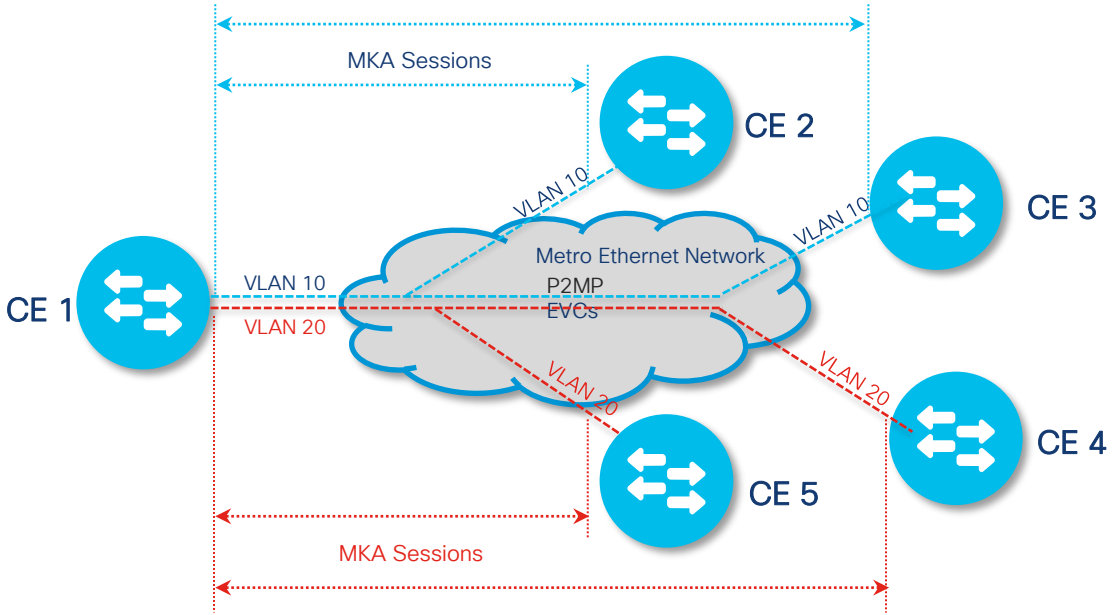


VLAN/Subinterface

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

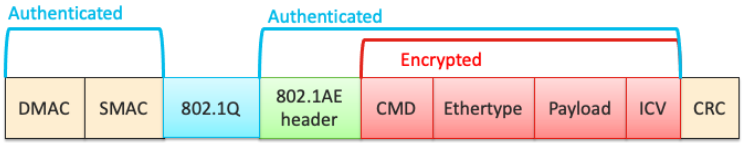
CE 4 → CE 1

CE 5 → CE 1

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

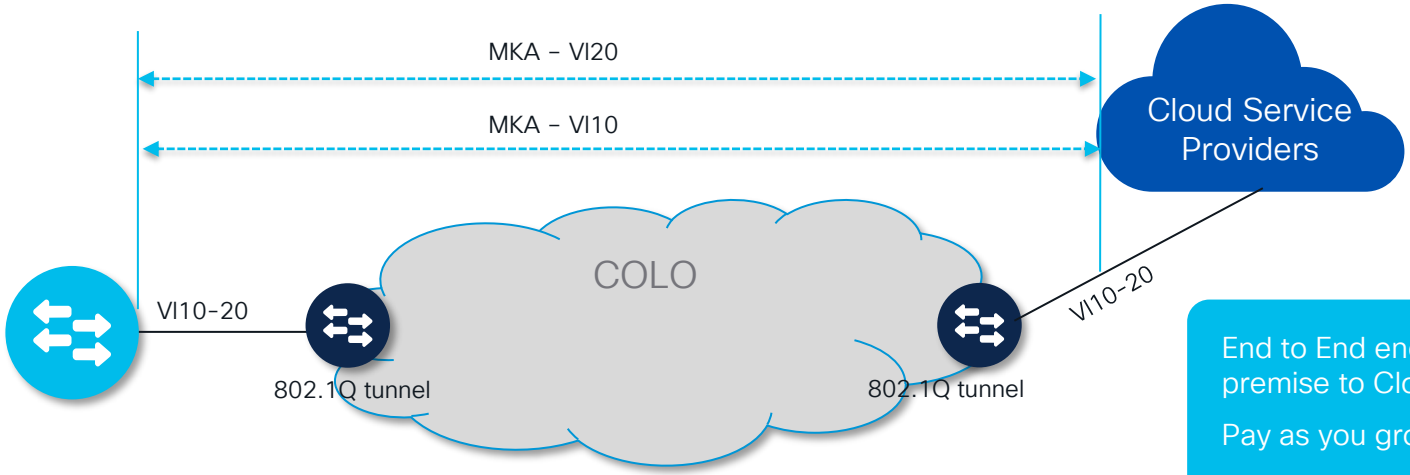
EAPoL DMAC is required to be Broadcast

VLAN/Subinterface



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deployment: Extending to Cloud Service Providers

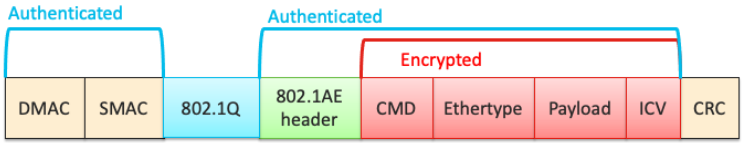


End to End encryption from On-premise to Cloud Infrastructure

Pay as you grow models

EAPoL DMAC is required to be Broadcast

VLAN/Subinterface

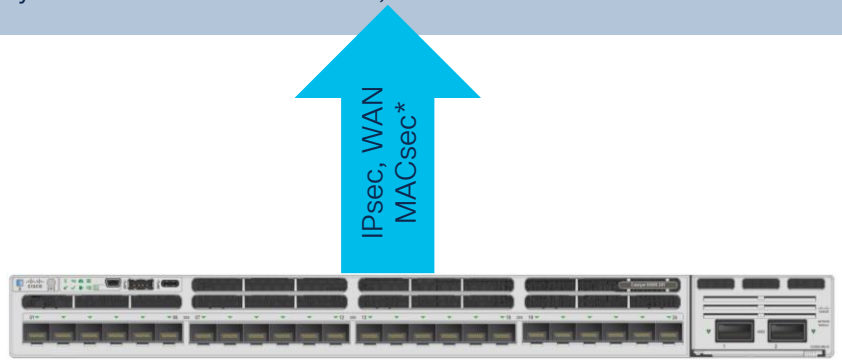


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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, 9400X,9500X and WAN MACsec on 9500X, 9600X.
- 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.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPsec & WAN MACsec Support and Scale

	IPsec	WAN MACsec	LAN MACsec
C9600X	HW Capable	✓	✓
C9500X	✓	✓	✓
C9300X	✓	HW Capable	✓
C9400X	✓	HW Capable	✓
C9200-C9600	–	–	✓

	9300X	9400X	9500X
IPv4	480	480	128
IPv6	240	240	128

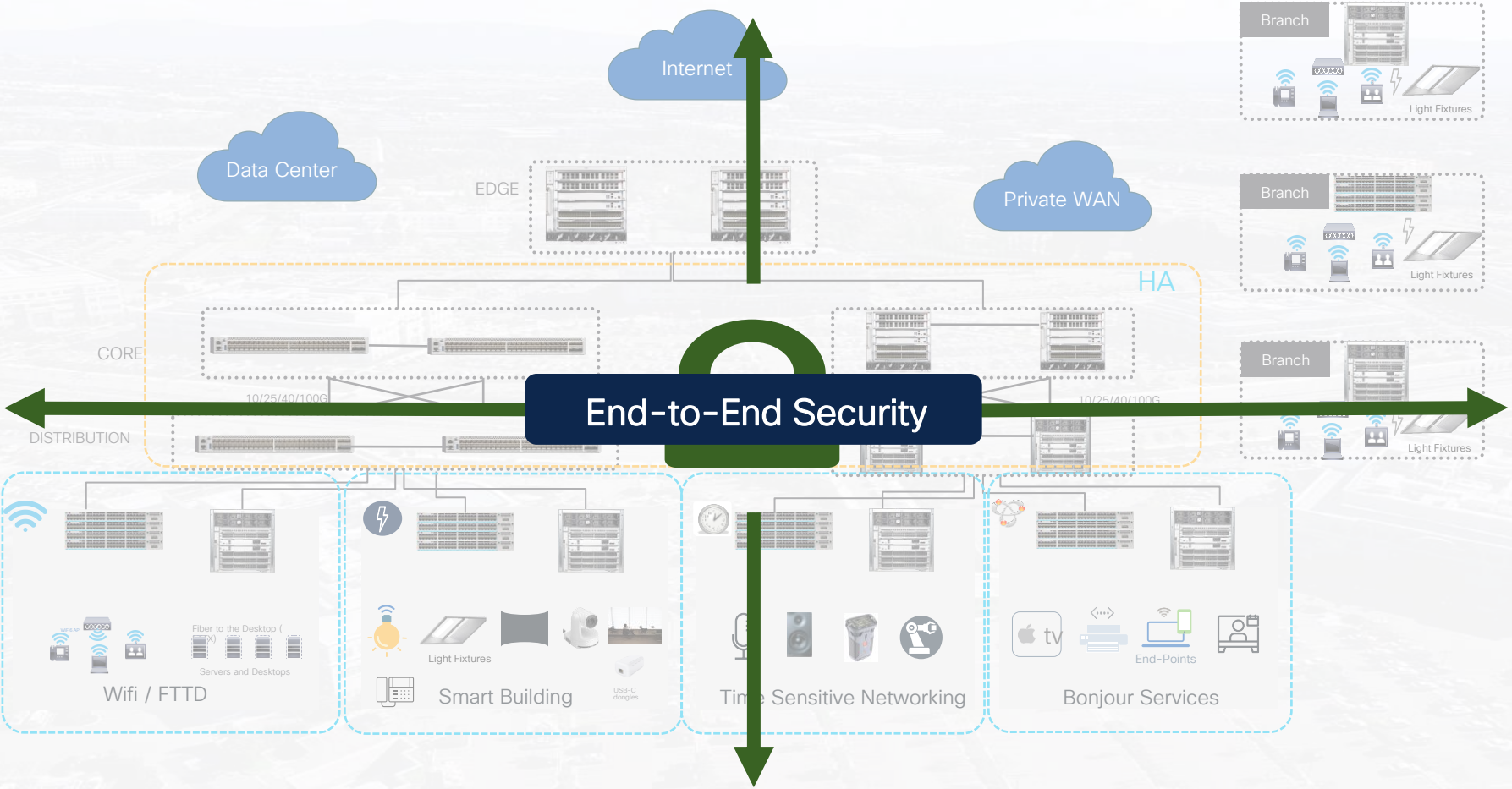
SCALE	C9600X	C9500X
WAN MACsec sessions	192	192

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public


Internet
Data Center
EDGE
Private WAN
Branch
Light Fixtures
Branch
Light Fixtures
Branch
Light Fixtures
HA
CORE
10/25/40/100G
10/25/40/100G
DISTRIBUTION
End-to-End Security
Fiber to the Desktop (
Servers and Desktops
Wifi / FTTD
Light Fixtures
USB-C dongles
Smart Building
Time Sensitive Networking
tv
End-Points
Bonjour Services


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go