

CISCO Live !

Inside Cisco 8000 Series Secure Routers: Architecture, Use Cases, and Innovation

Jason Yang
Principal Technical Marketing Engineer
www.linkedin.com/in/jy71428

BRKXAR-2027

Cisco Webex App

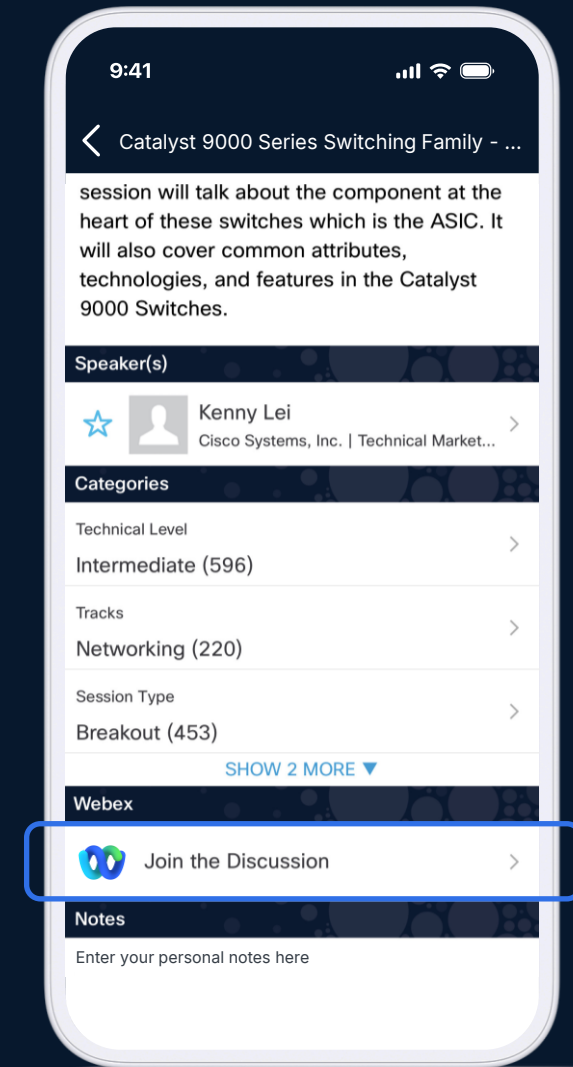
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2026.



<https://ciscolive.ciscoevents.com/ciscolivebot/BRKXAR-2027>

Agenda

1. What's new
2. Architecture
3. Product Innovation
4. Elevate Secure WAN use-cases
5. Operational Best Practice

Customer trends transforming the WAN edge

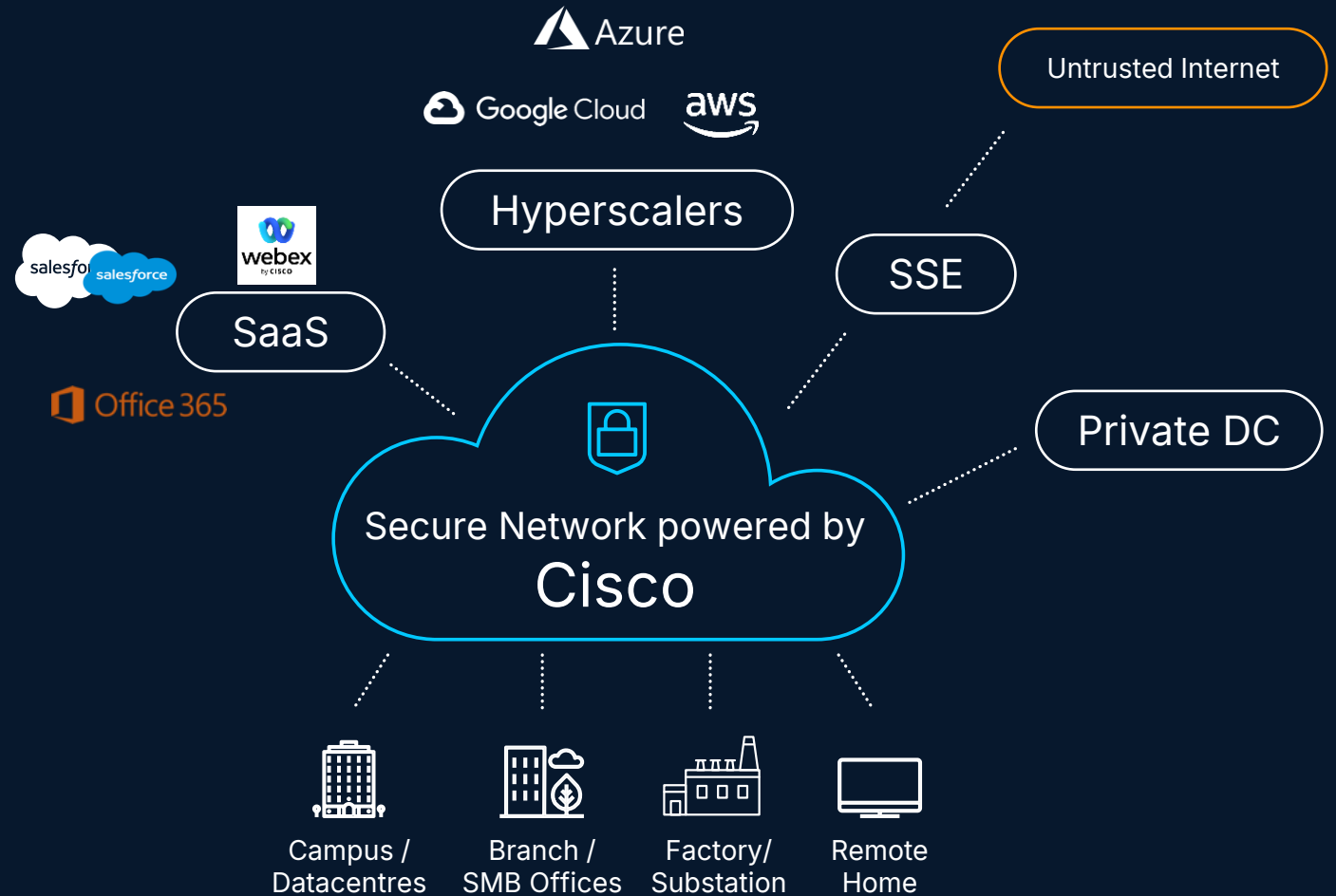
Multi-hybrid, neo, sovereign-cloud acceleration

Work from anywhere

Application/digital experience

Secure, internet-only branch

Simplify IT → centralized management distributed enforcement



Cisco 8000 Series Secure Routers

Connect Quantum-safe Secure WAN for every size location



**Cisco 8100 Series
Secure Routers**

Small Branch



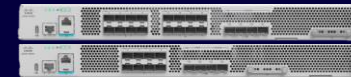
**Cisco 8200 Series
Secure Routers**

Medium Branch



**Cisco 8300 Series
Secure Routers**

Large Branch



**Cisco 8400 Series
Secure Routers**

Campus



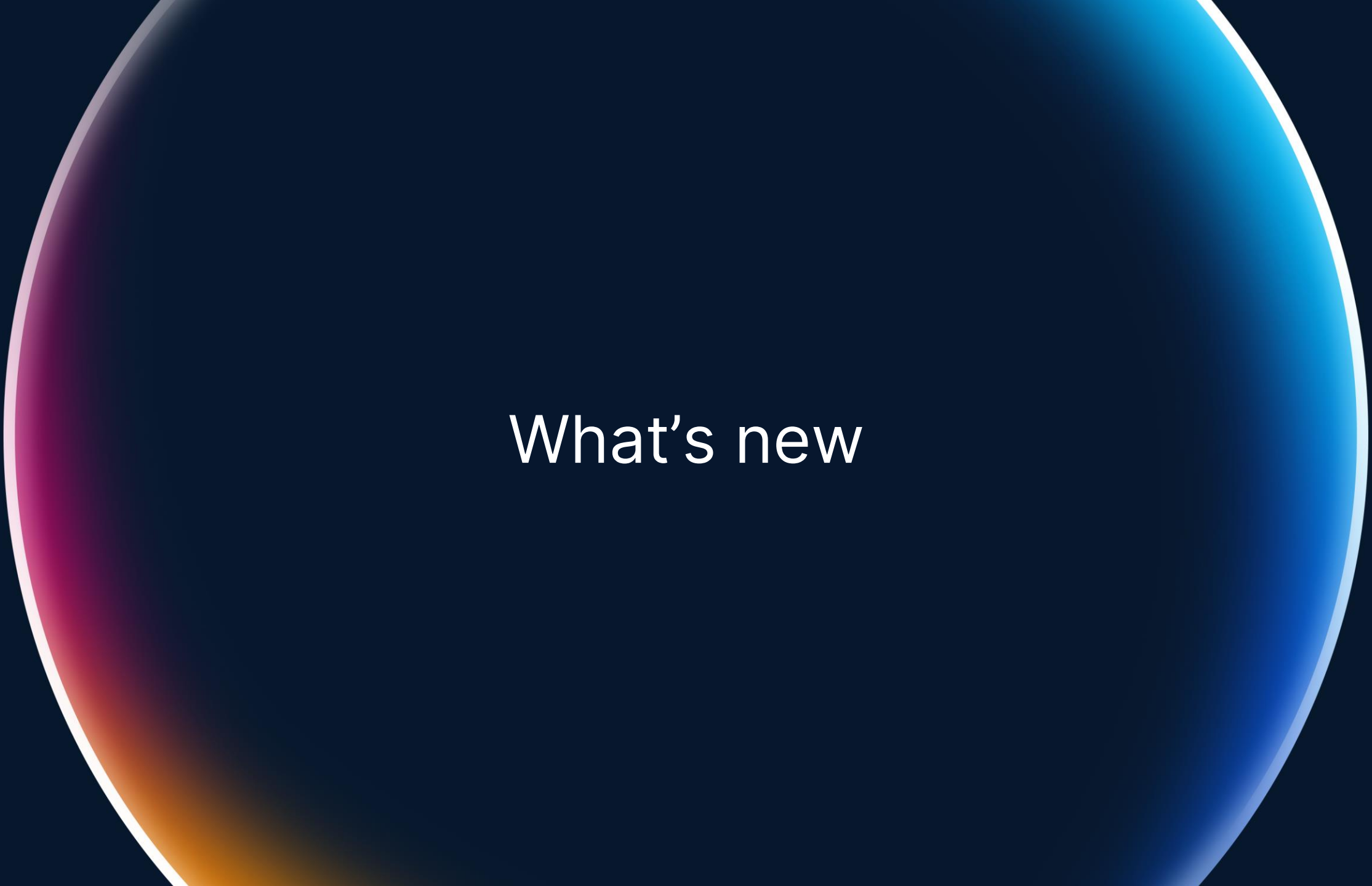
**Cisco 8500, 8600
Series Secure
Routers**

Data Center

Meet Cisco Cloud Control

The unified interface for AgenticOps





What's new

Cisco 8650 Secure Router

Post-Quantum Cryptography (PQC) Ready 100G Secure Router



Full-stack PQC

- NIST Compliant (FIPS-203) PQC IPsec VPN
- Quantum-safe MACsec (LAN/WAN) with EAP-TLS
- PQC SD-WAN
- PQC Secure Boot

- 6x 100/40G QSFP28
- 20x 10/1G SFP+
- Line-rate WAN MACsec on all ports
- 3RU

3rd Gen QFP



- High Performance:
 - 540 Gbps Forwarding
 - 220 Gbps IPsec
 - 82 Gbps SD-WAN
- High Scale:
 - 380K ACEs
 - 16M Routes
 - 32M NAT/FW sessions
 - 12K SD-WAN IPsec Tunnels

Expanding the Cisco 8200 Series Secure Routers

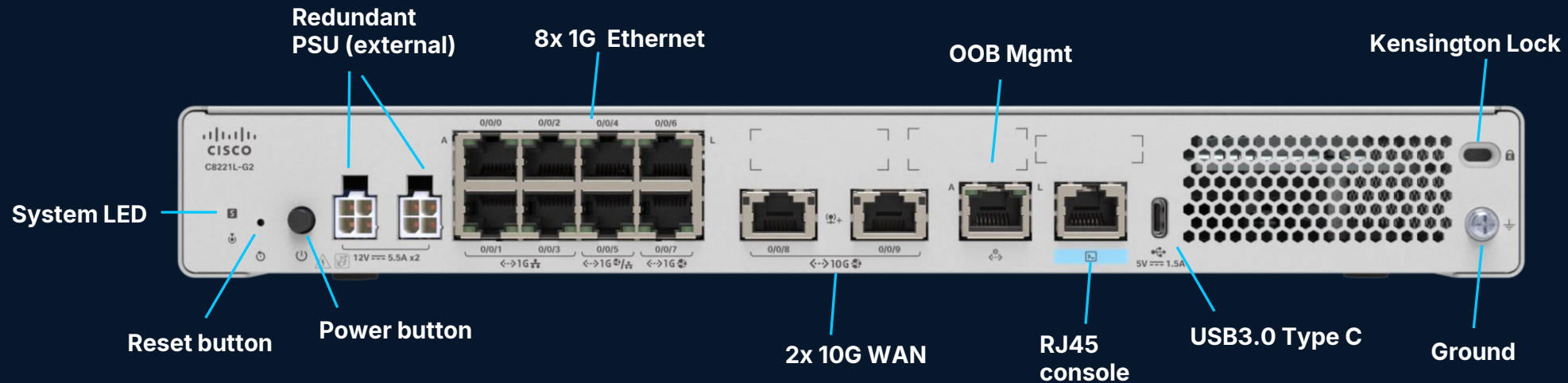
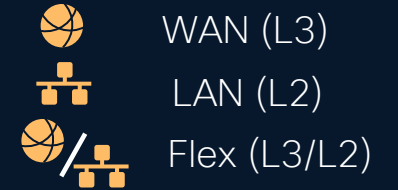
4 new variants



- SD-WAN + Threat Protection enterprise branch up to **2 Gbps** throughput performance
- Growing adoption of **10G WAN** (Copper & Fiber)
- Ethernet only
- **Dual PSU** (external)
- **PQC** IPsec/MACsec/SD-WAN
- **PQC** Secure Boot

Cisco 8221L-G2 Secure Router

2x 10G Copper WAN



19 Gbps Forwarding

5 Gbps IPsec

4 Gbps SD-WAN^[1]

1 Gbps Threat Protection^[2]

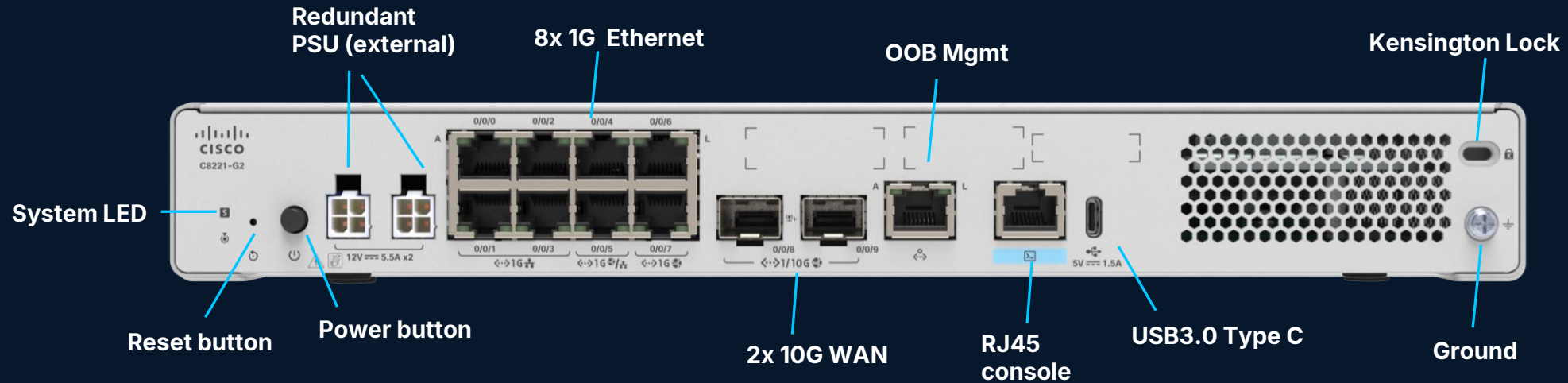
[1] SD-WAN feature combination: IPsec + QoS + Deep Packet Inspection + Flexible NetFlow

[2] Threat Protection: 100% DIA-NAT + App Aware FW + IPS + URLF + AMP

All numbers are interim, final numbers subject to change at FCS

Cisco 8221-G2 Secure Router

2x 10G Fiber WAN



19 Gbps Forwarding

5 Gbps IPsec

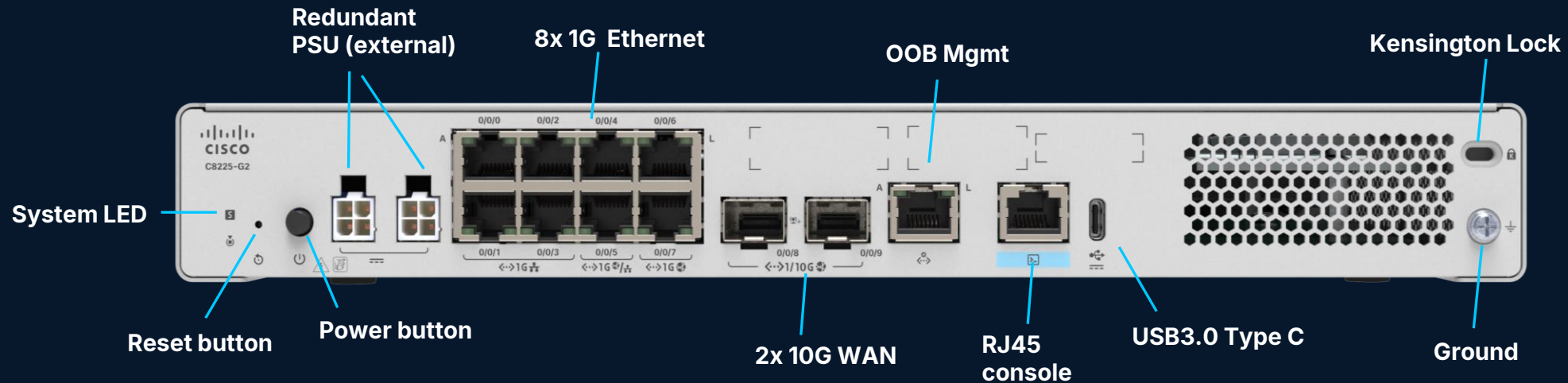
4 Gbps SD-WAN

1 Gbps Threat
Protection

All numbers are interim, final numbers subject to change at FCS

Cisco 8225-G2 Secure Router

2x 10G Fiber WAN w/ 2G Threat Protection



19 Gbps Forwarding

5 Gbps IPsec

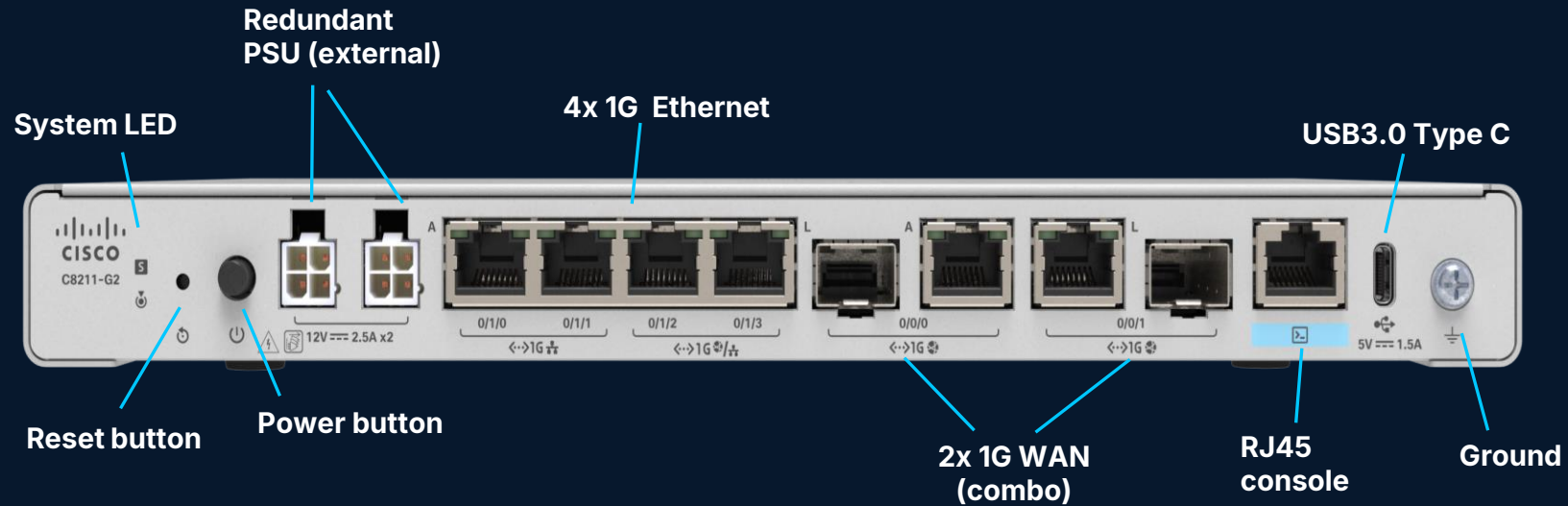
4 Gbps SD-WAN

2.2 Gbps Threat
Protection

All numbers are interim, final numbers subject to change at FCS

Cisco 8211-G2 Secure Router

2x 1G Fiber/Copper WAN



5.6 Gbps Forwarding

3 Gbps IPsec

2 Gbps SD-WAN

1 Gbps Threat
Protection

All numbers are interim, final numbers subject to change at FCS

Secure Router Node for Unified Edge



Secure Router Node •



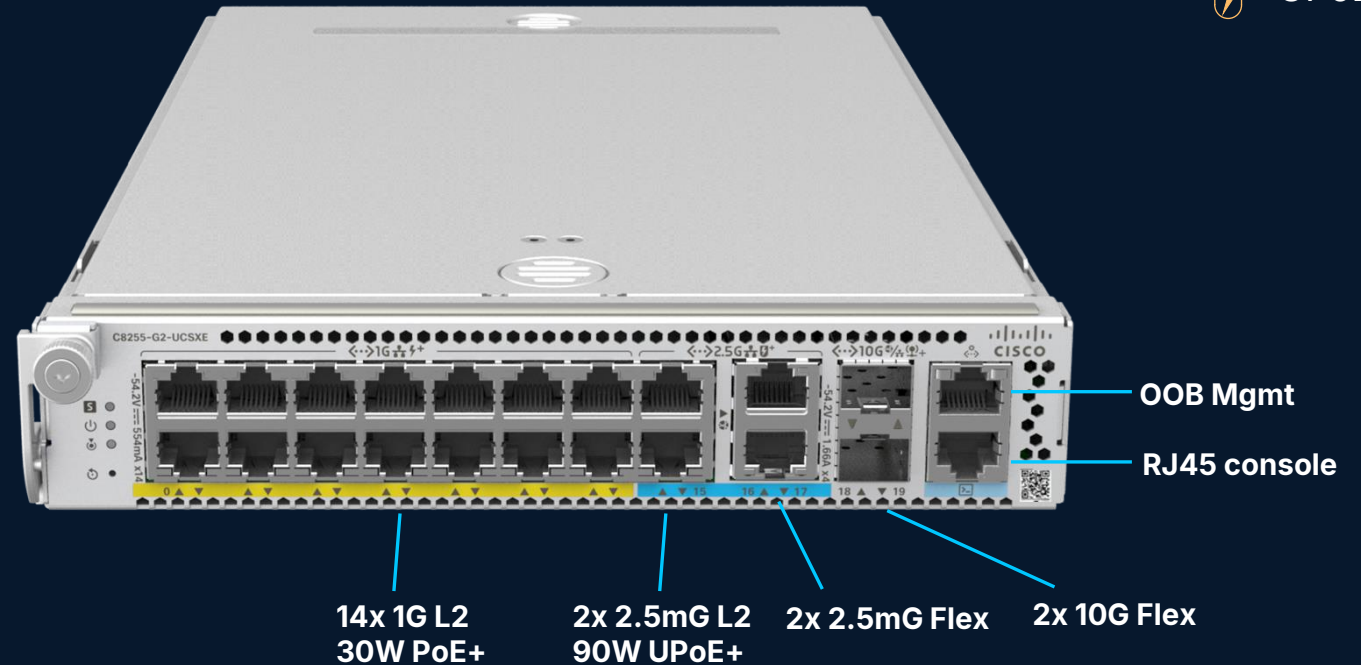
- Unified Edge Solution
 - Modular platform **converges** compute, LAN, WAN, and SASE
 - Enable deploying AI at the edge **securely** and **at scale**
- Unified Edge Network Node
 - Brings LAN, WAN, and SASE into the Unified Edge platform
 - 1U half-width Unified Edge node form factor
 - **Management plane integration** between Intersight and SD-WAN Manager
 - Delivers a "**One Cisco**" advantage with seamless integration across domains

Cisco 8200 Unified Edge Network Node

C8255-G2-UCSXE

⚡⁺ PoE⁺
⚡⁺ UPoE⁺

- 2x 25G backplane interface
- 360W PoE power budget in total
- PQC IPsec/MACsec/SD-WAN
- PQC Secure Boot
- Full Feature Parity with 8200 Secure Routers



19 Gbps Forwarding

5 Gbps IPsec

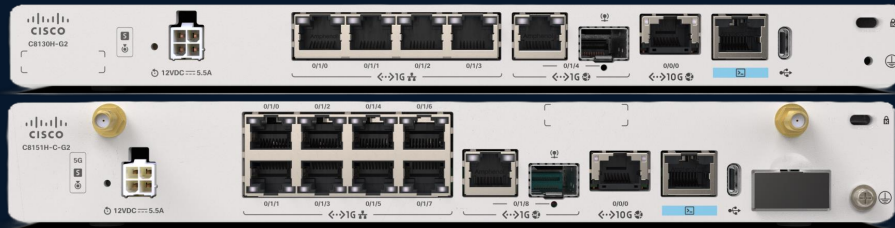
4 Gbps SD-WAN

2.2 Gbps Threat
Protection

All numbers are interim, final numbers subject to change at FCS

Expanding the Cisco 8100 Series Secure Routers

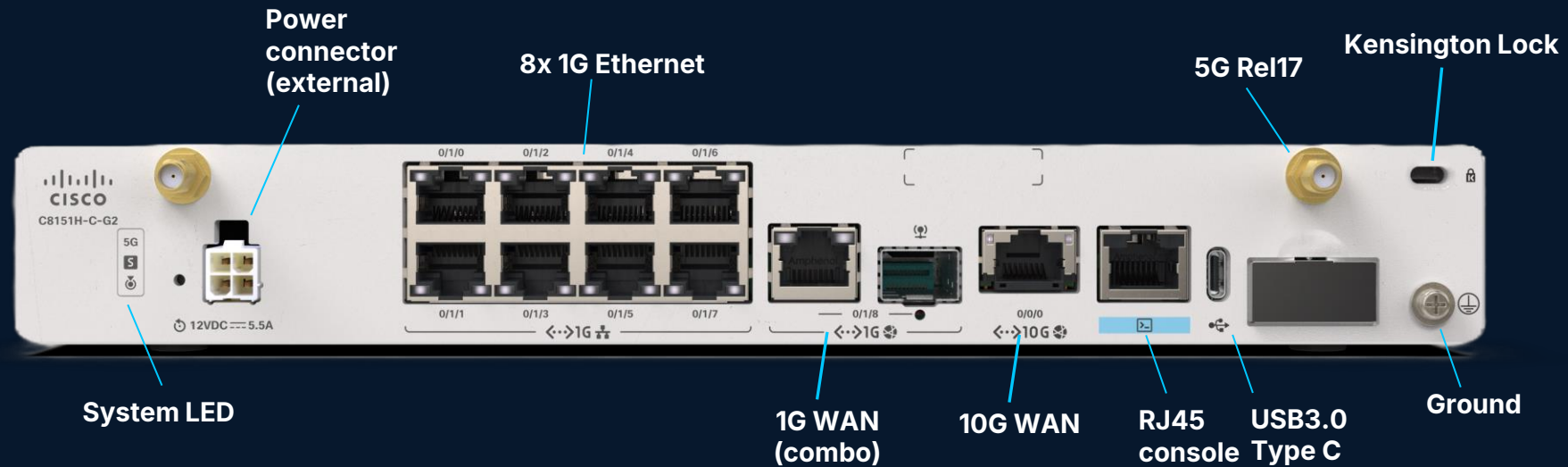
2 new variants



- Growing adoption of 10G Copper WAN
- Embedded 5G Rel 17 variant
- SD-WAN + Threat Protection enterprise branch with 1Gbps throughput
- PQC IPsec/SD-WAN
- PQC Secure Boot

Cisco 8151H-C-G2 Secure Router

10G Copper WAN



5.6 Gbps Forwarding

1.5 Gbps IPsec

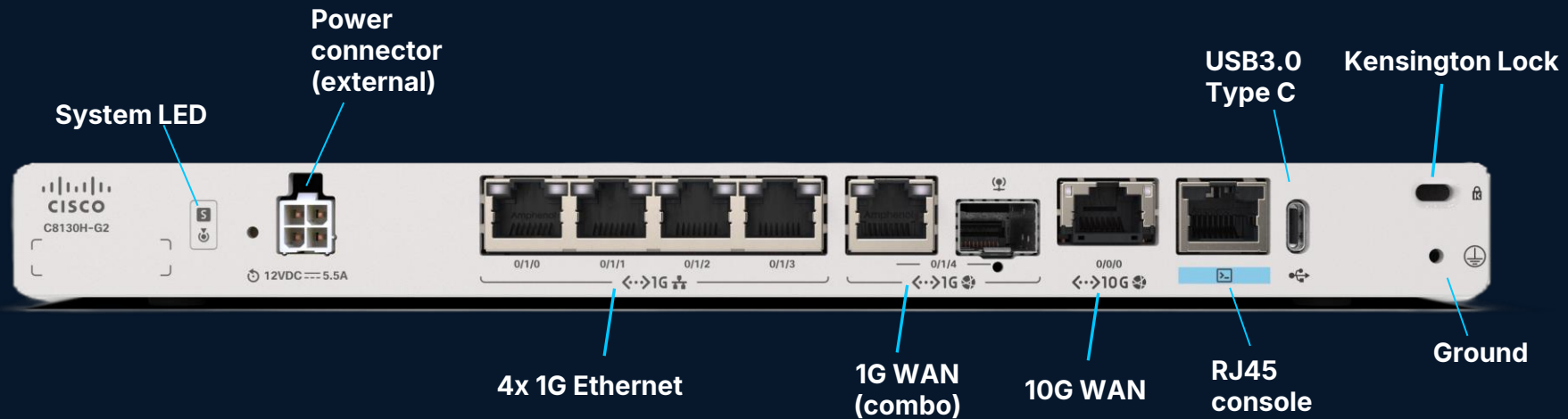
1 Gbps SD-WAN

1 Gbps Threat
Protection

All numbers are interim, final numbers subject to change at FCS

Cisco 8130H-G2 Secure Router

10G Copper WAN, Routing only



1.9 Gbps Forwarding

1.5 Gbps IPsec

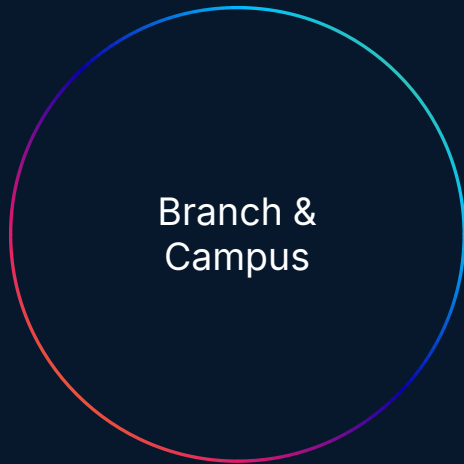
All numbers are interim, final numbers subject to change at FCS



Architecture

Secure Routers - Building Blocks

secure networking
processor



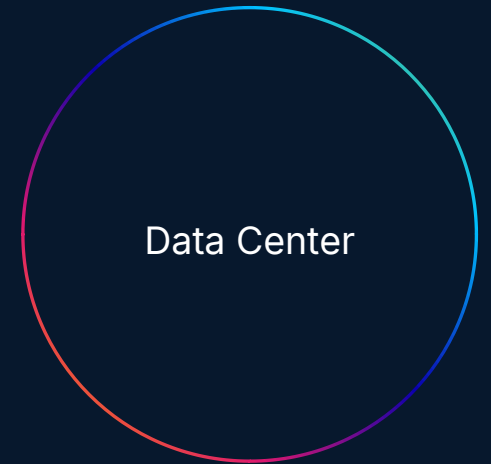
Security & Networking Convergence

Cisco
IOS XE



Programmability | On-prem & Cloud

Cisco Quantum
Flow Processor



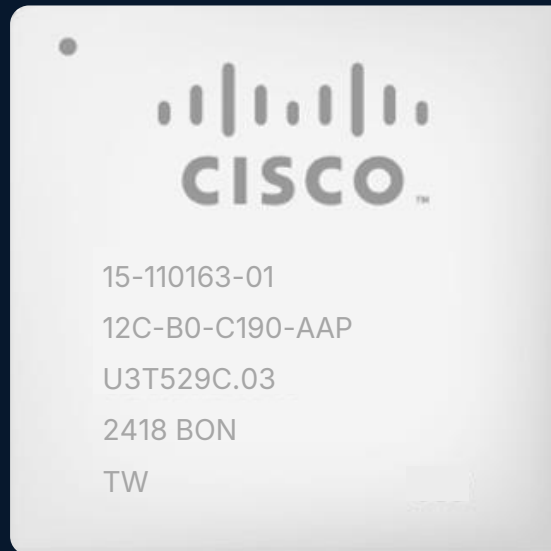
High Performance | High Scale ASIC

secure networking processor



Security

- Inline Crypto
- PQC ready crypto engine
- Cisco Secure Firewall acceleration
- AI/ML engine



Networking



- Integrated hardware accelerators
- Integrated Ethernet Controller – 1GE, mGig, 10GE, 25GE
- Performance defined Power
- Programmable uCode – protect IP, feature parity

Foster security and networking convergence

secure networking processor Architecture

Multi-core Parallel Processing

- High performance 64-bit processor
- Non-Strict Flow Based Distribution

Hardware Acceleration

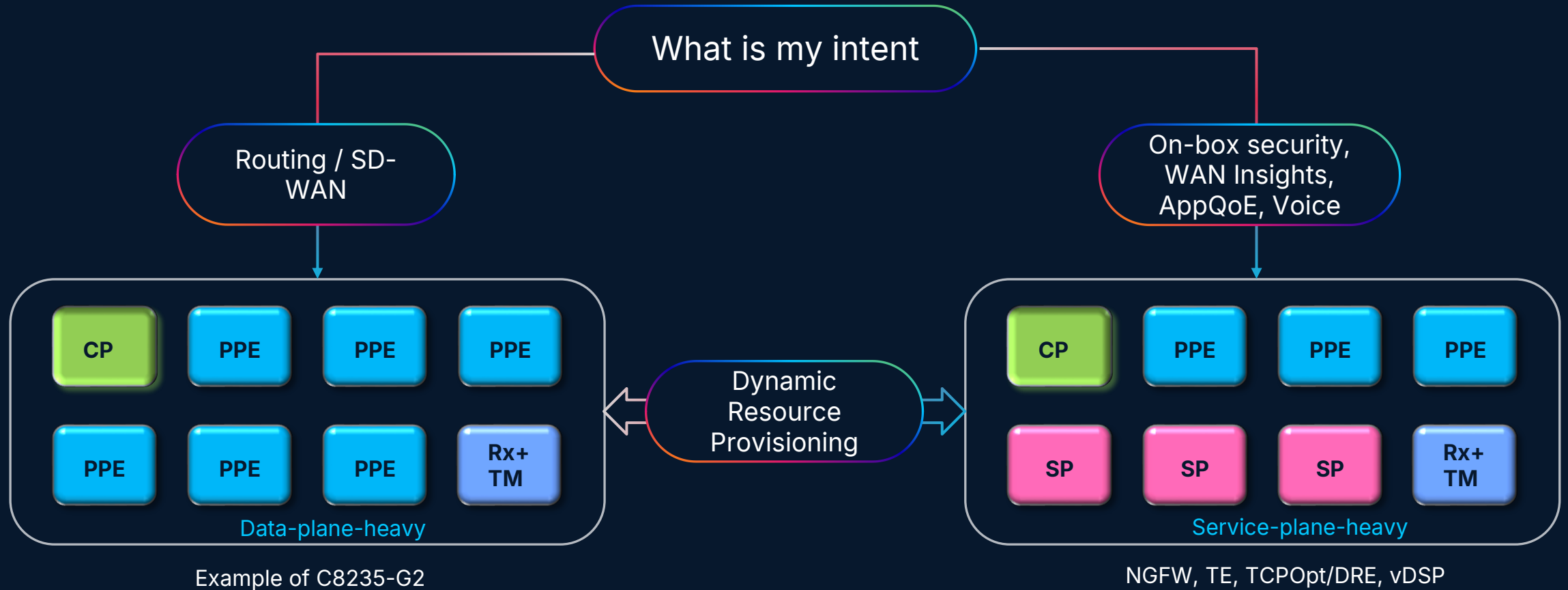
- HW packet distribution engine
- In-line Crypto engine
- Built-in AL/ML engine

System-on-chip

- Integrated Traffic Manager
- Integrated NIC
- Built-in Trust Anchor

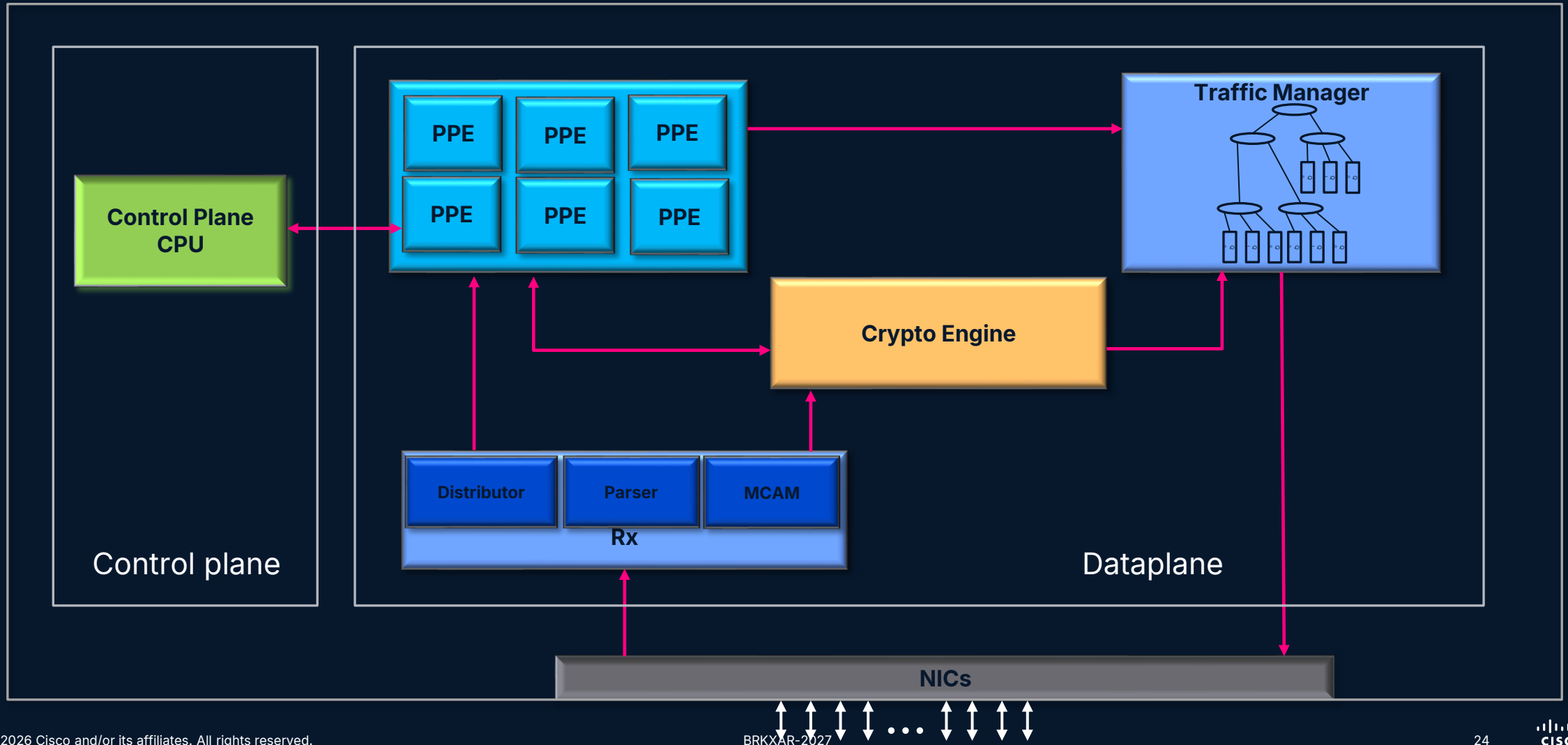


Dynamic Resource Provisioning

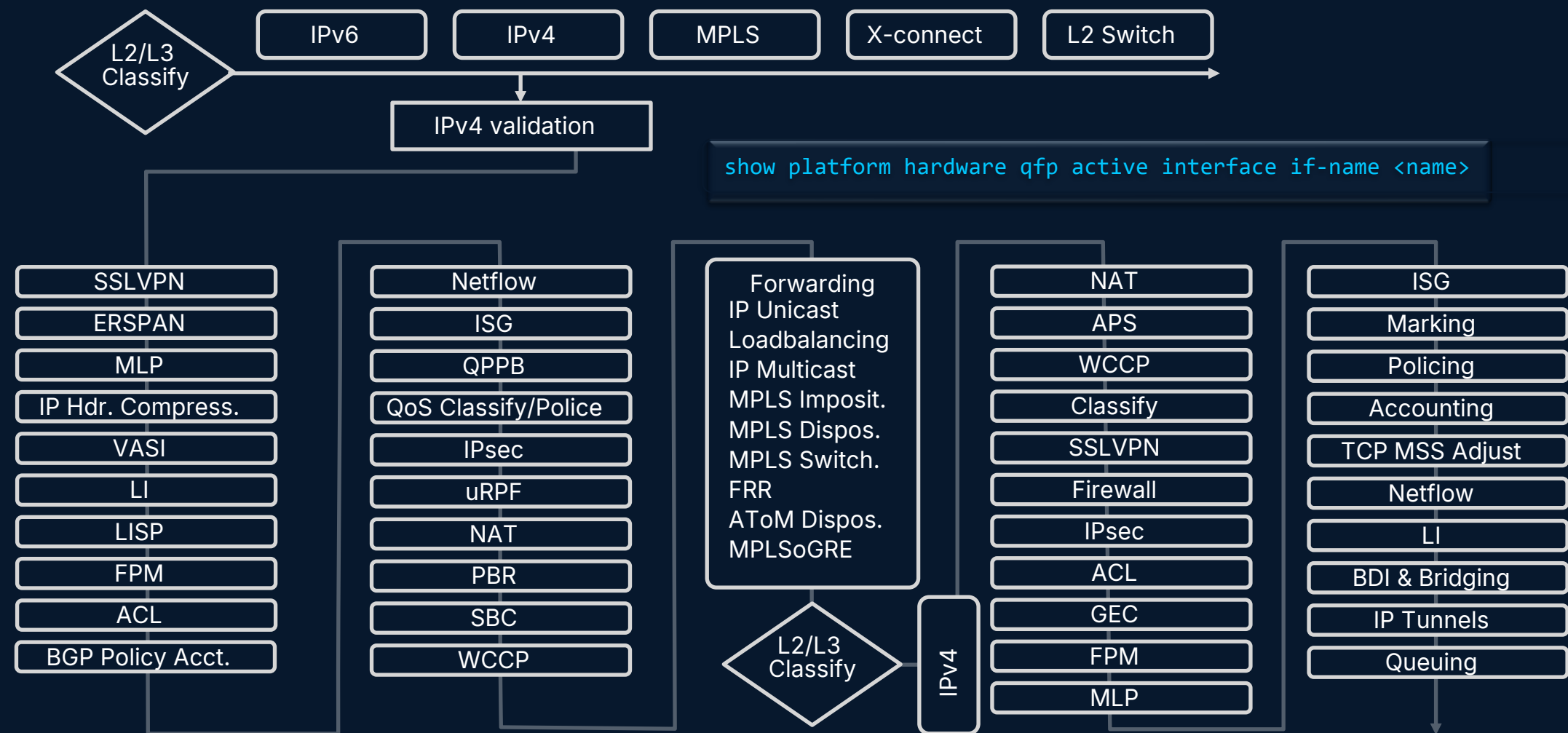


The Life of a Packet in Secure Router

Branch & Campus



Data Path: Feature Invocation Array (FIA)



QFP Architecture – 3rd Generation

Multi-threaded Parallel Processing

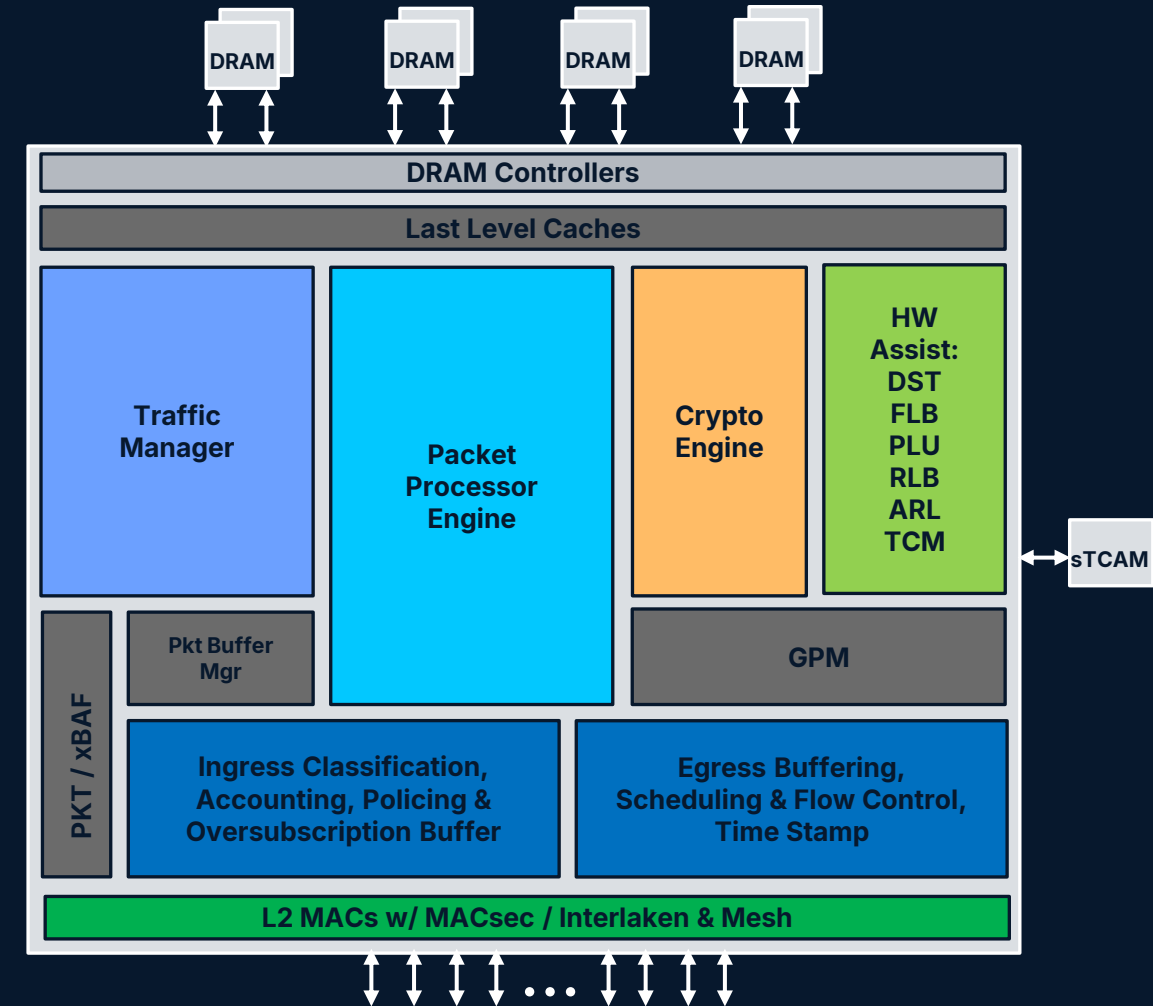
- 224 PPEs, 4 threads each → 896 threads
- Scalable Traffic Manager

Hardware Accelerated Crypto

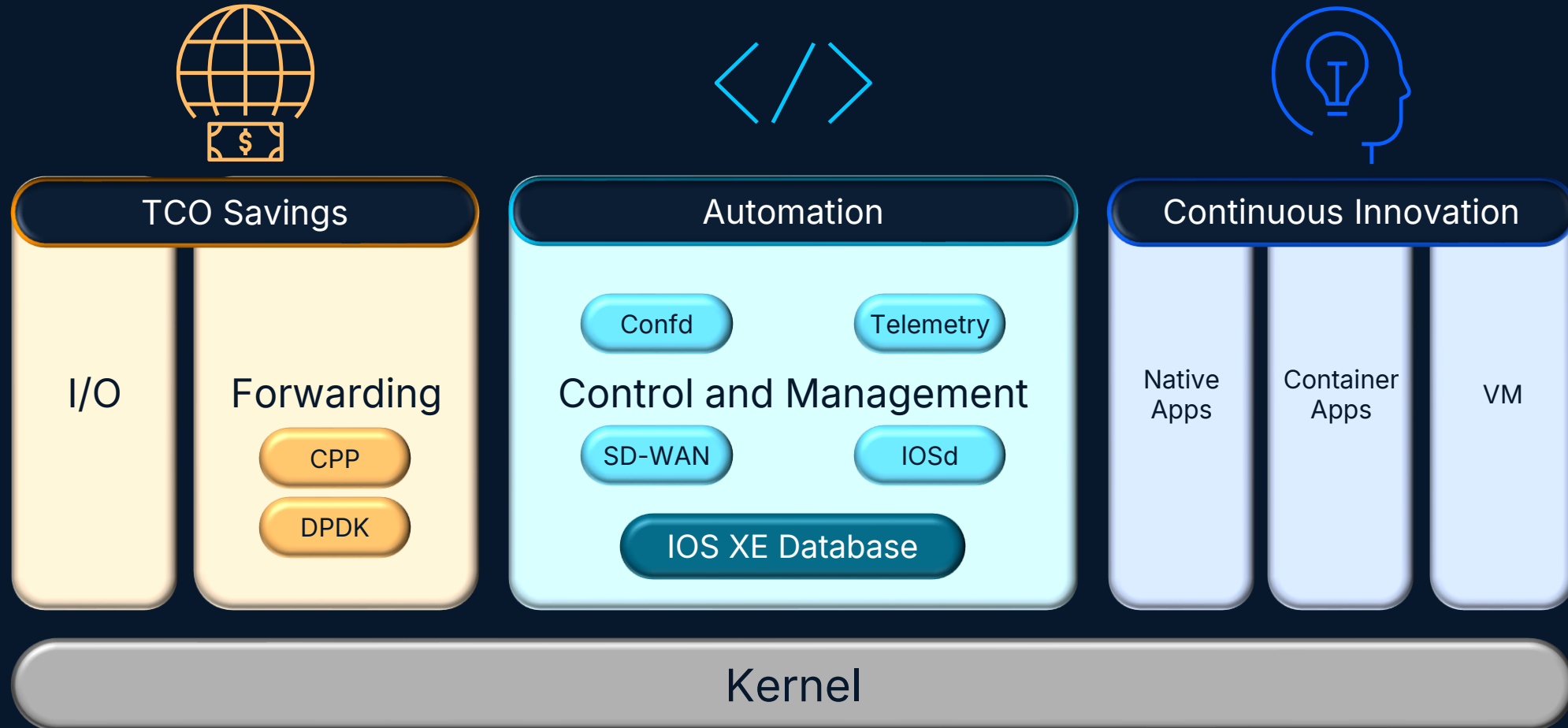
- 16 Crypto engines with dedicated resources
- Flow queues for complex stateful features

Integrated L2 MACs & Mesh

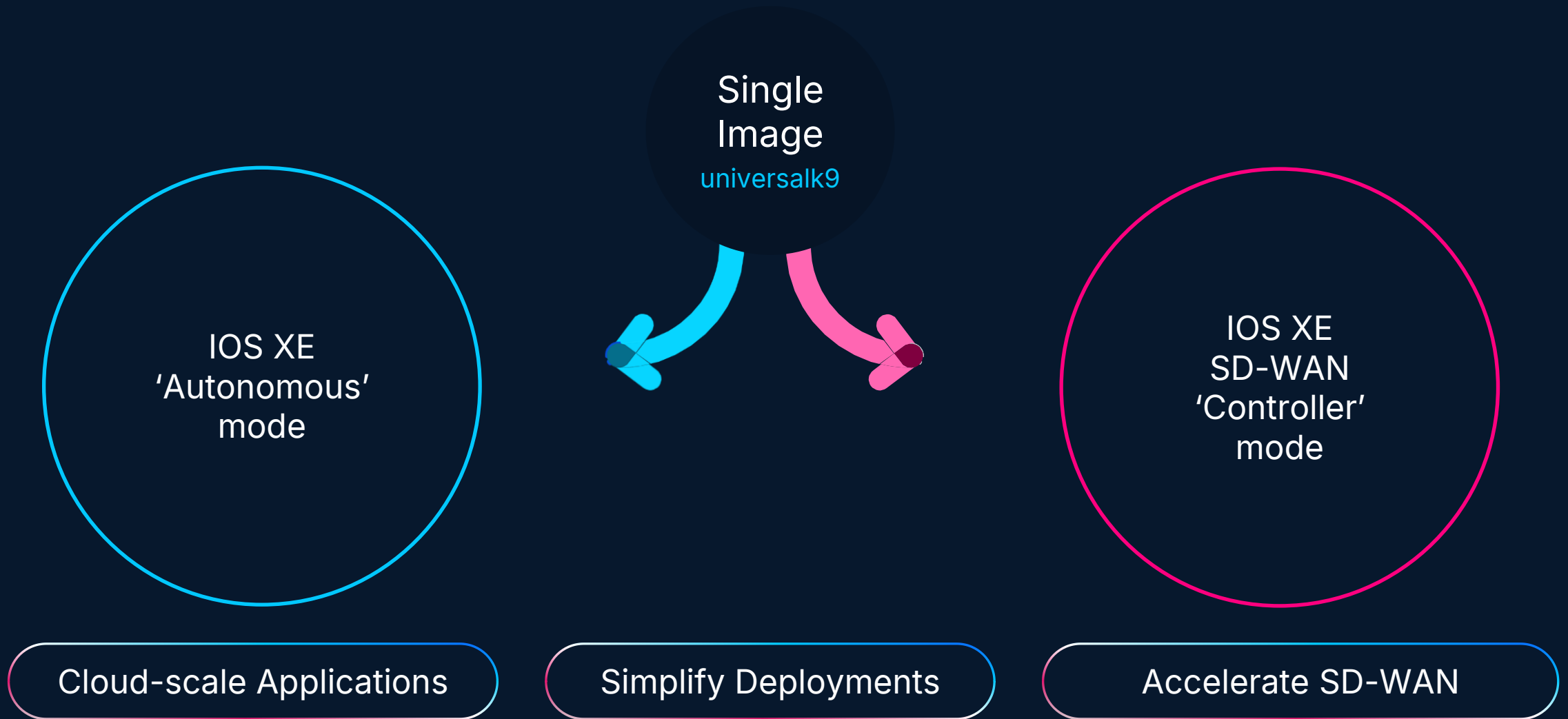
- max 240G of aggregated I/O
- Enable 4x QFP Cascading



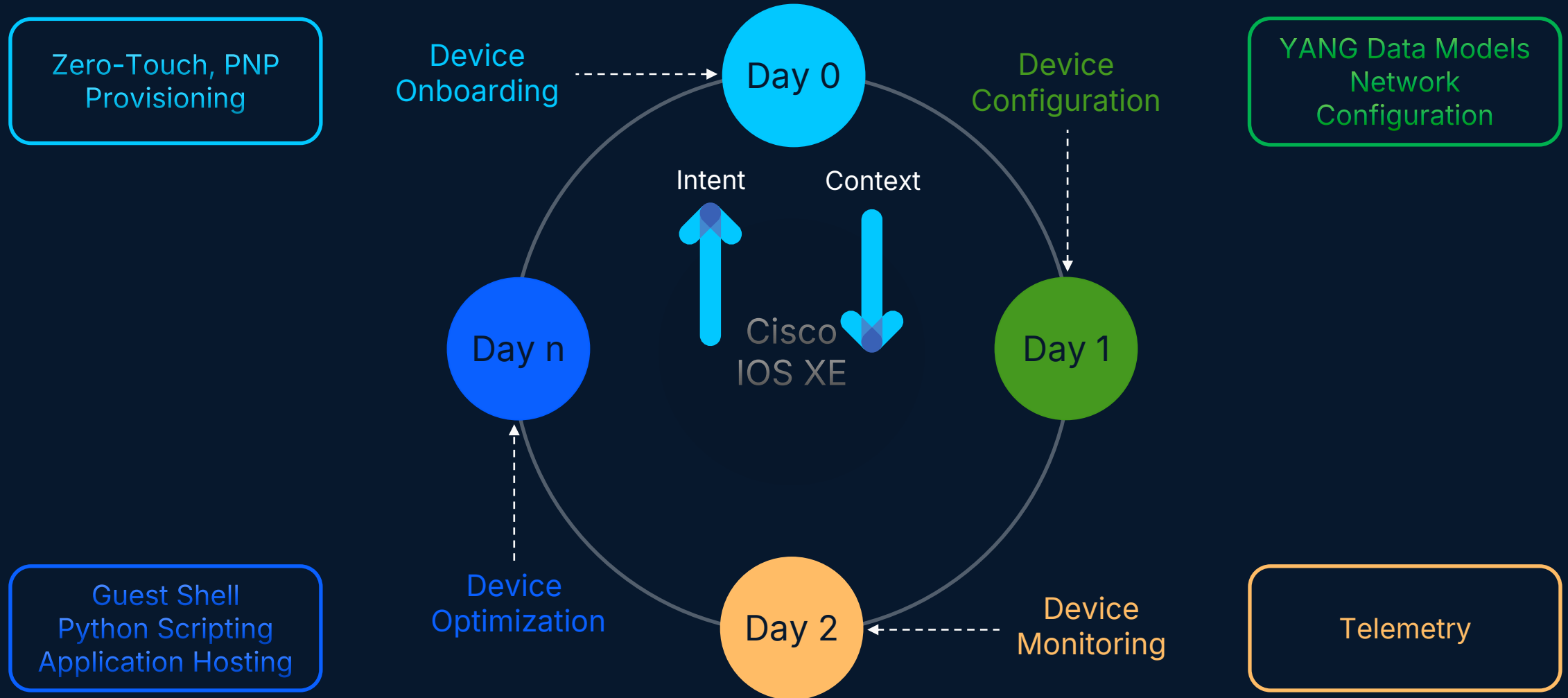
Open IOS XE — A Modern Operating System



Easy Operations with Single Image

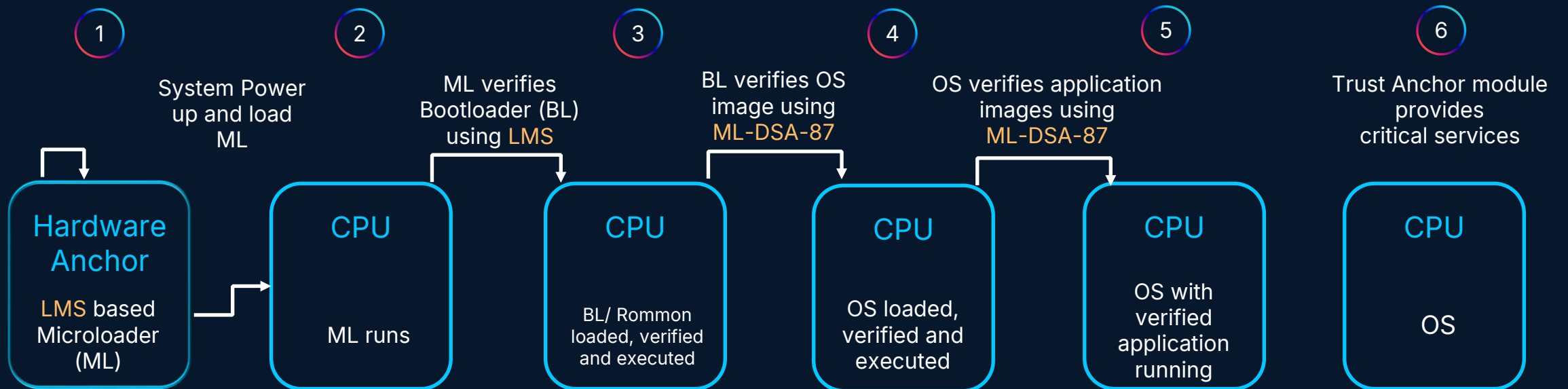


IOS XE Programmability



PQC Secure Boot on Secure Routers

Uplevel Trustworthy solution in post-quantum era

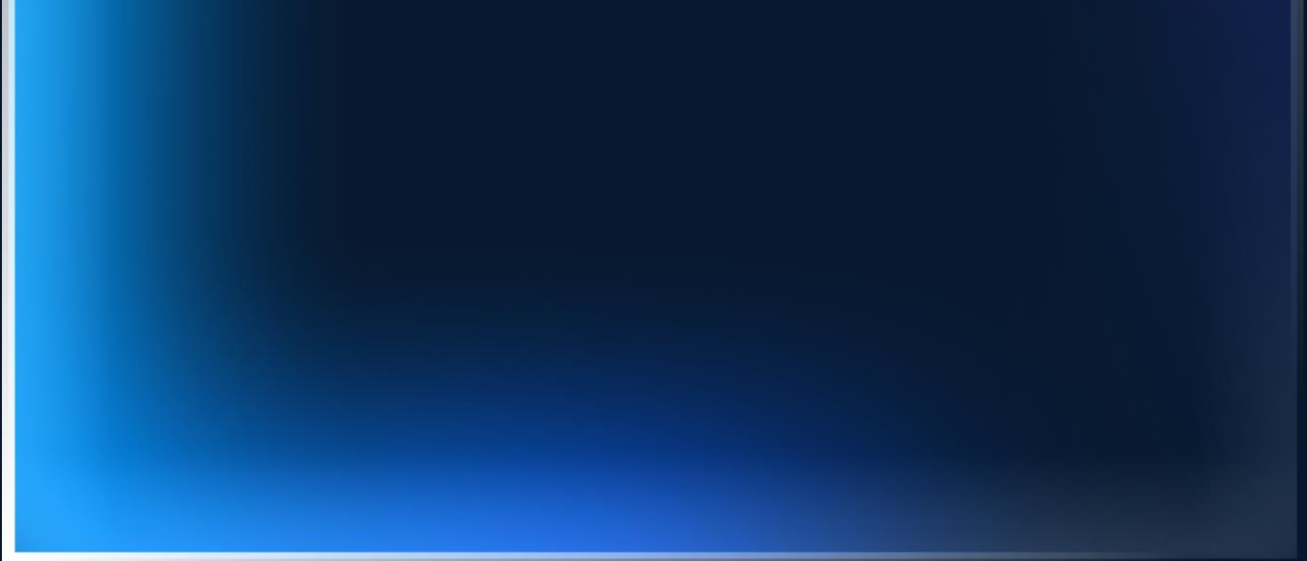


Leighton-Micali Signature (LMS) – RFC8554, NIST SP 800-208; ML-DSA-87 – Module lattice-based digital signature algorithm FIPS-204

Confidentiality

Integrity

Authenticity



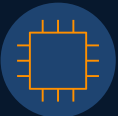
Product Innovations



The Power of Cisco 8000 Series Secure Routers

Hardware Innovations

Secure networking
processor



HW accelerated
Security & Networking

Fanless model



Small, medium,
large branch

25GE WAN



Campus Router

Secure boot



Post-Quantum Safe

Dying gasp



Small, medium,
large branch

mGig/10GE



Migration from
1GE

The Power of Cisco 8000 Series Secure Routers

Security Innovations

Consistent Security
Policy Construct



Built-in Secure
Firewall

NIST
Compliant PQC



IPsec/MACsec

Throughput
Improvement



10x IPsec,
6x Threat Protection

Line-rate MACsec



LAN/WAN MACsec
on all FPGE^[1]

Security AI/ML



Ready to offload
(8300/8400)

Tamper Detection

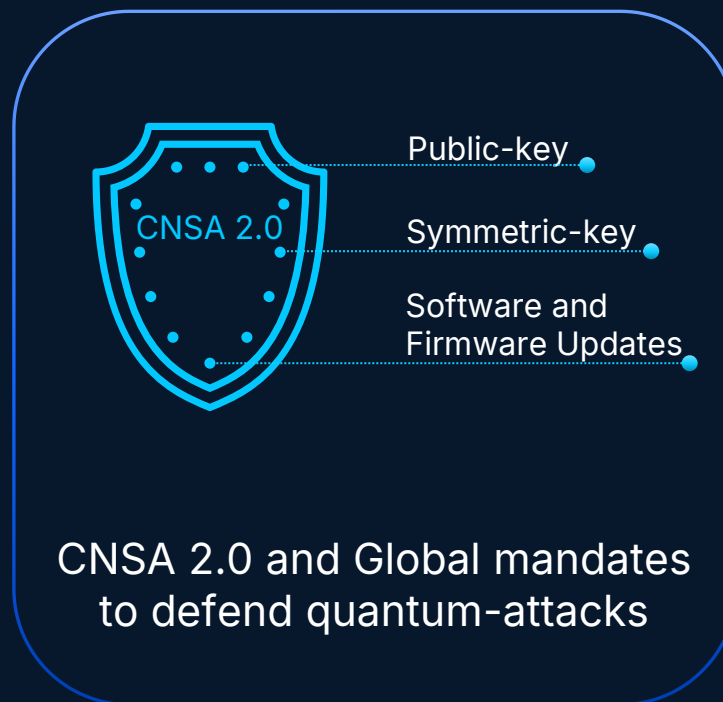


Physical (open chassis)
Intrusion Detection

[1] 8200 secure routers and onward

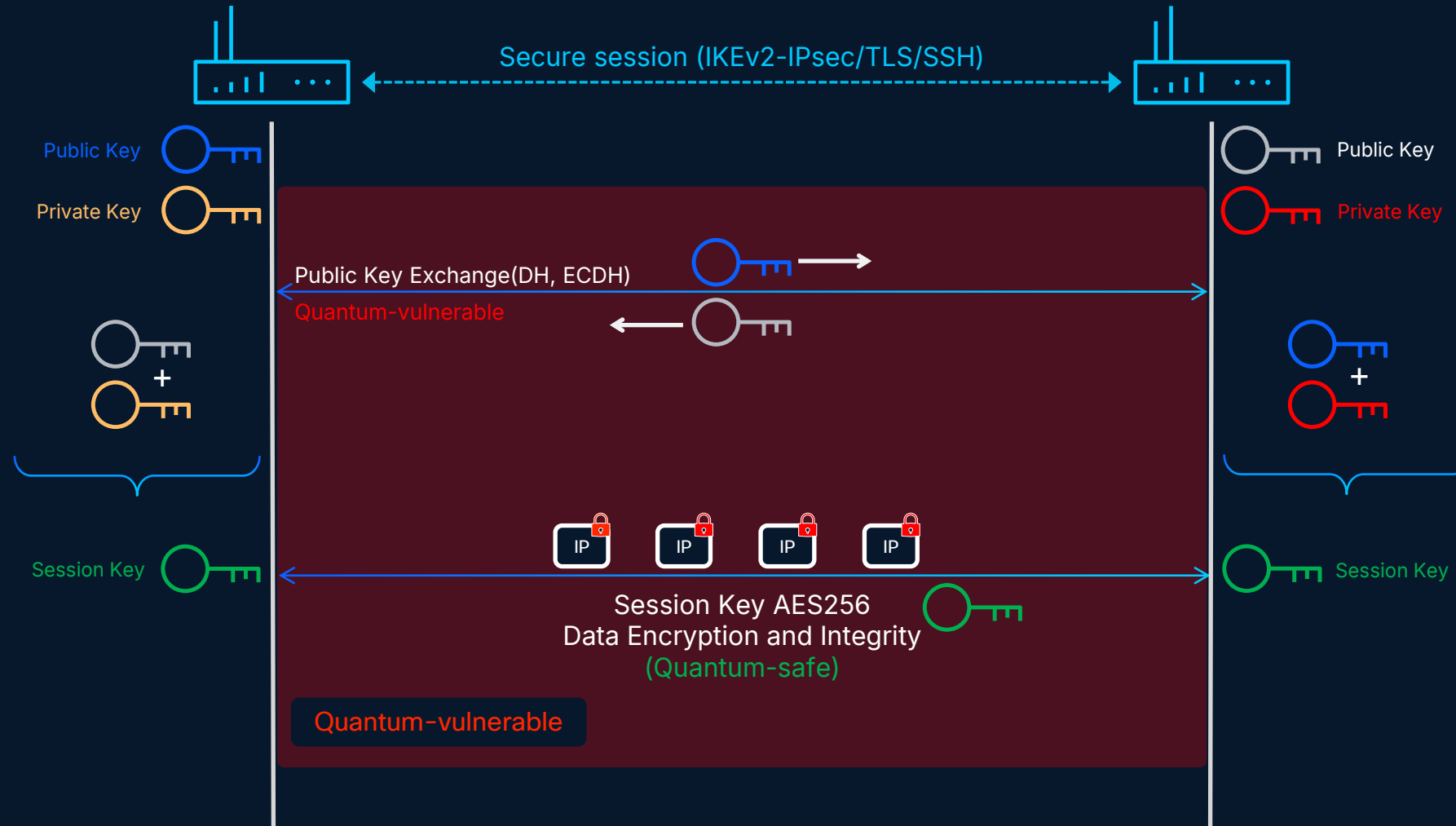
Securing Today to Prepare for a Quantum-safe Future

HNDL Attack, CNSA 2.0 and Timelines



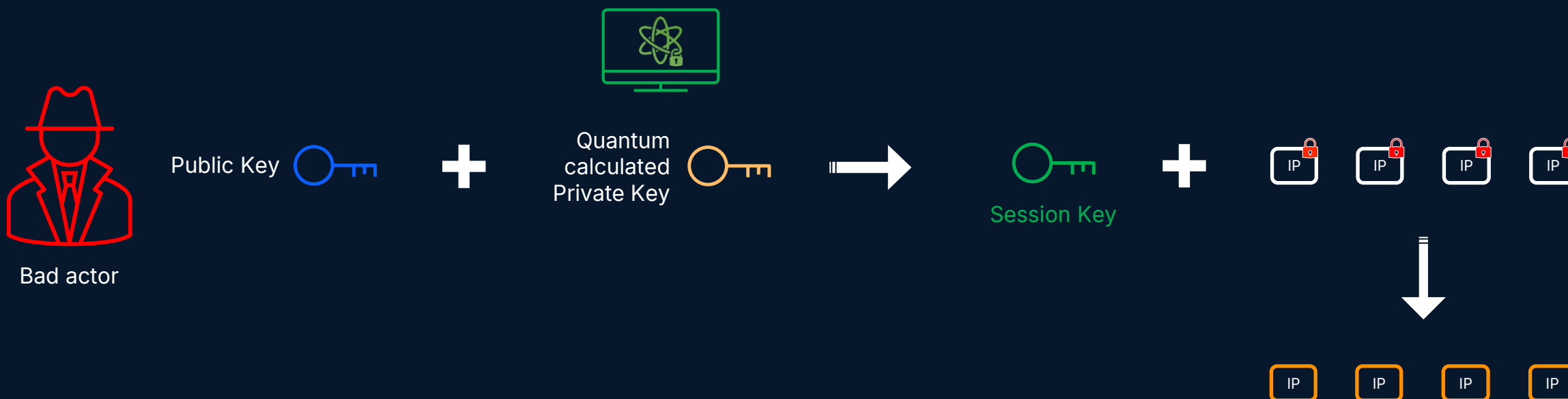
A 'Cryptographically Relevant Quantum Computer' (CRQC) could be used to **Break Current Encryption**.

Key Exchange phase is Quantum-vulnerable



'Harvest Now, Decrypt Later' (HN DL) attack

Attacker captures the key exchange phase and uses Quantum calculated Private Key to get Session Key!

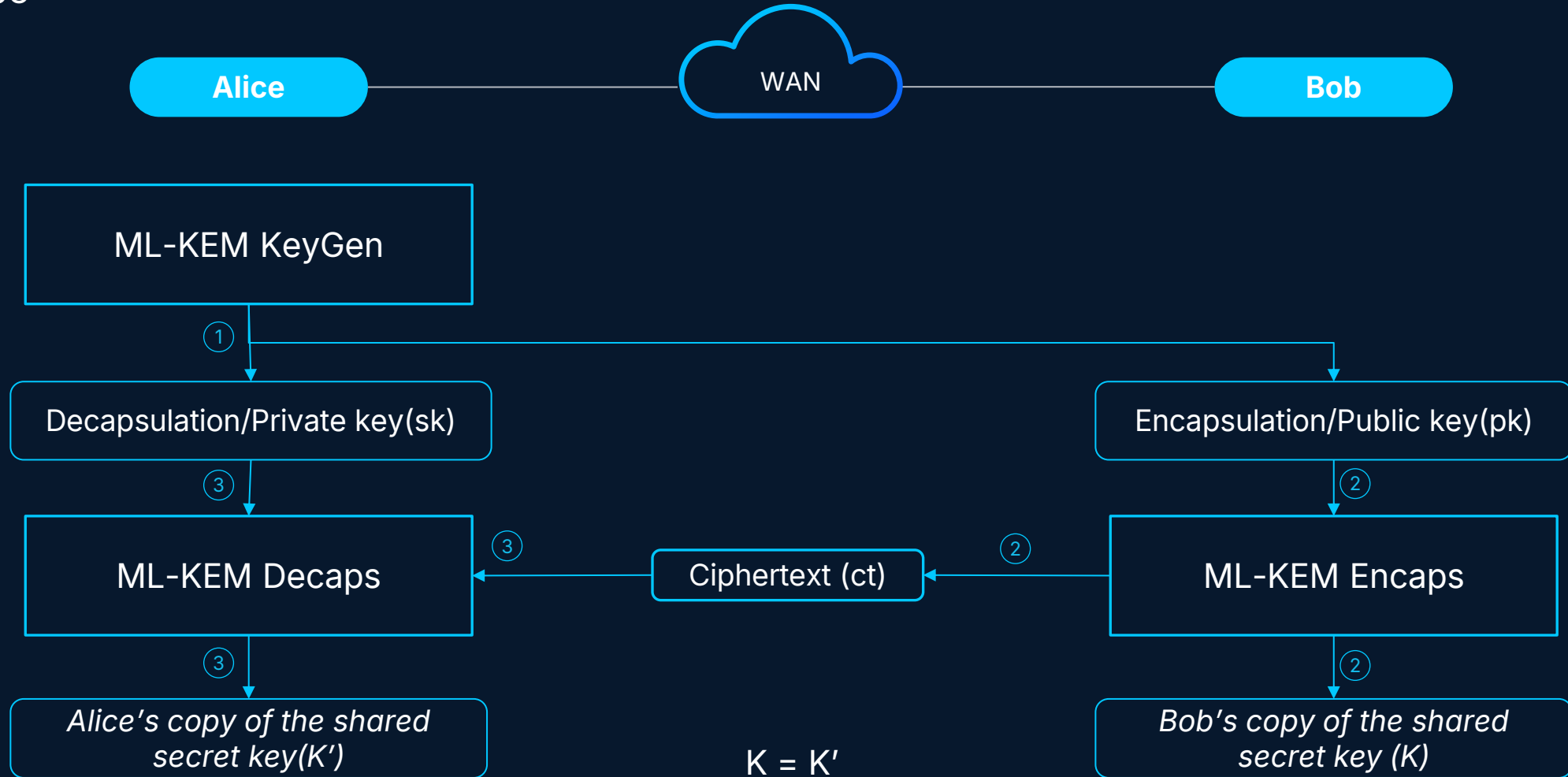


Public key cryptography is Quantum-vulnerable.

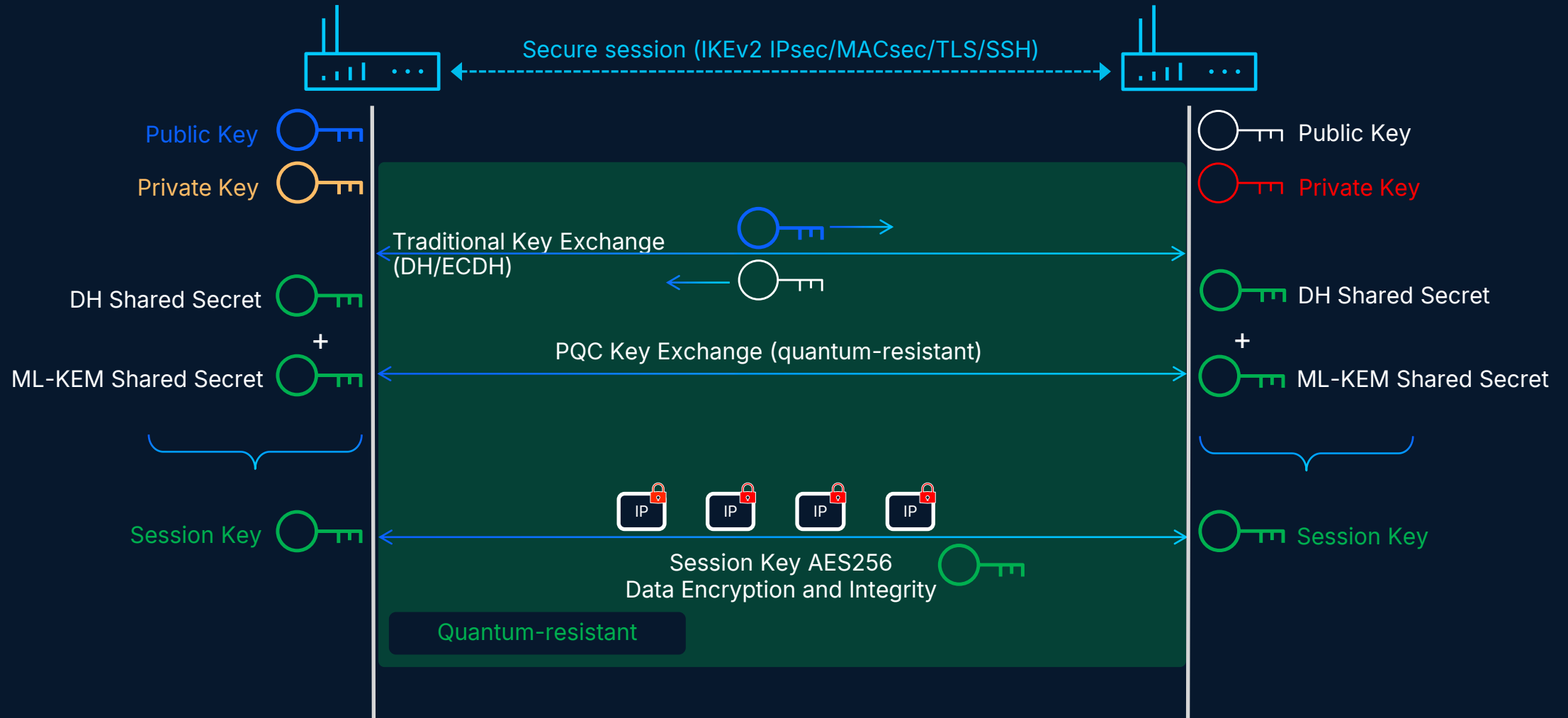
Module-Lattice-Based Key-Encapsulation Mechanism

FIPS 203

Key Establishment using ML-KEM



Key Exchange using PQC Algorithm



PQC Standards – Key Exchange

PQC Algorithm Standards - NIST

- FIPS-203 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

Protocol Extension Standards - IETF

- IKEv2
 - RFC-9370 – Multiple Key Exchanges in IKEv2
 - IETF Draft - PQ Hybrid Key Exchange with ML-KEM in IKEv2
- TLS & SSH
 - IETF Draft - Hybrid key exchange in TLS 1.3
 - IETF Draft - ML-KEM Post-Quantum Key Agreement for TLS 1.3
 - IETF Draft - PQ/T Hybrid Key Exchange with ML-KEM in SSH
 - IETF Draft - Module-Lattice Key Exchange in SSH

Secure WAN PQC Solutions

IKEv2
IPsec

DMVPN

FlexVPN,
IKEv2 CLB

MACsec
EAP-TLS

SSH

Config: PQC ML-KEM for IKEv2 IPsec

```
crypto ikev2 proposal ikev2proposal
  encryption aes-cbc-256
  integrity sha512
  group 21
  pqc mlkem768 optional
!
crypto ikev2 policy ikev2policy
  proposal ikev2proposal
!
crypto ikev2 keyring ikev2keyring
  peer HUB_PEER_KEYRING_NAME
  address [HUB_PUBLIC_IP]
  pre-shared-key Cisco@123
!
crypto ikev2 profile ikev2profile
  match identity remote address [HUB_PUBLIC_IP]
  authentication local pre-share
  authentication remote pre-share
  keyring local ikev2keyring
!
crypto ipsec transform-set tset1 esp-aes 256 esp-sha256-hmac
  mode tunnel
!
crypto ipsec profile ipsec_profile_vti
  set transform-set tset1
  set ikev2-profile ikev2profile
  set pfs
```

'optional' → non-strict
PQC enforcement

Verify: PQC ML-KEM for IKEv2 IPsec

Router# **show crypto ikev2 sa detailed**

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/ivrf	Status
4	<u>1.1.1.2/500</u>	<u>1.1.1.1/500</u>	none/none	READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK

PQC Key Exchange: ML-KEM-768

Life/Active Time: 86400/65905 sec

CE id: 0, Session-id: 1

Local spi: 828DC8848548B23C Remote spi: D77638A21E177EF0

Status Description: Negotiation done

Local id: 1.1.1.2

Remote id: 1.1.1.1

Local req msg id: 44 Remote req msg id: 0

Local next msg id: 44 Remote next msg id: 0

Local req queued: 44 Remote req queued: 0

Local window: 20 Remote window: 20

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Quantum-safe Encryption using PQC: ML-KEM-768

Dynamic Route Update: enabled

Extended Authentication not configured.

NAT-T is not detected

Cisco Trust Security SGT is disabled

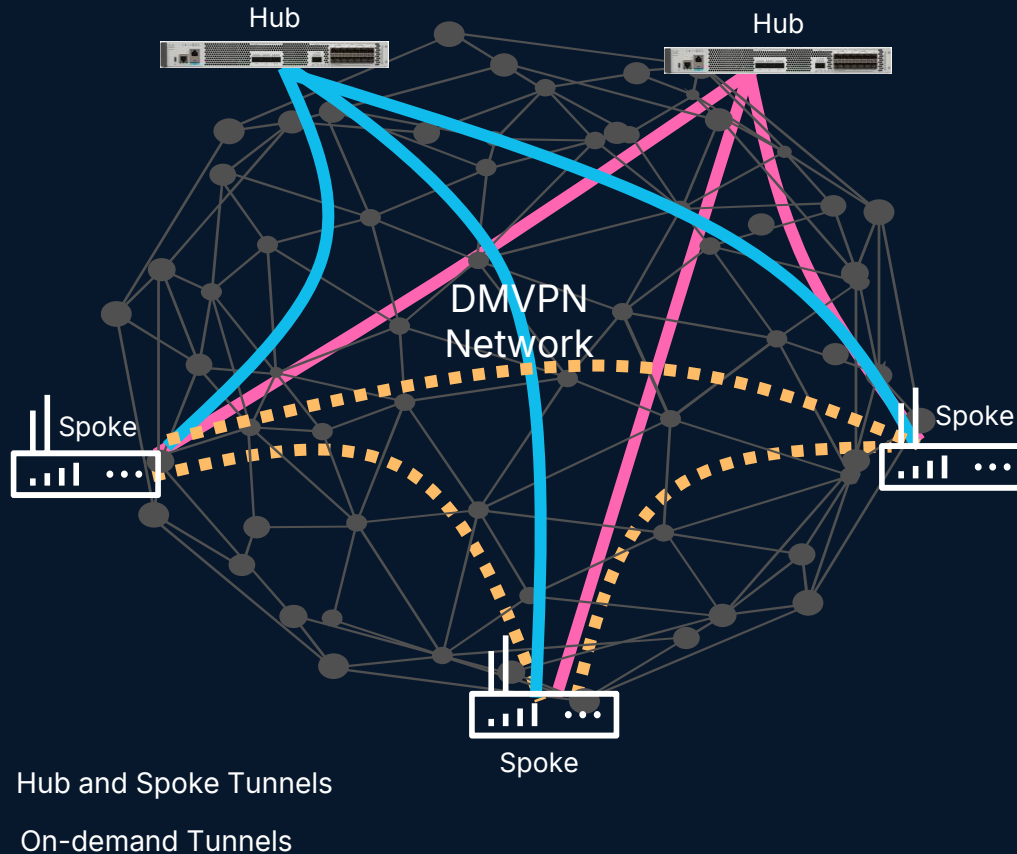
Initiator of SA : Yes

PEER TYPE: IOS-XE

ML-KEM
in use

PQC ML-KEM for DMVPN

DMVPN allows large scale IPsec VPNs deployment by combining mGRE, IPsec/IKEv2, and NHRP



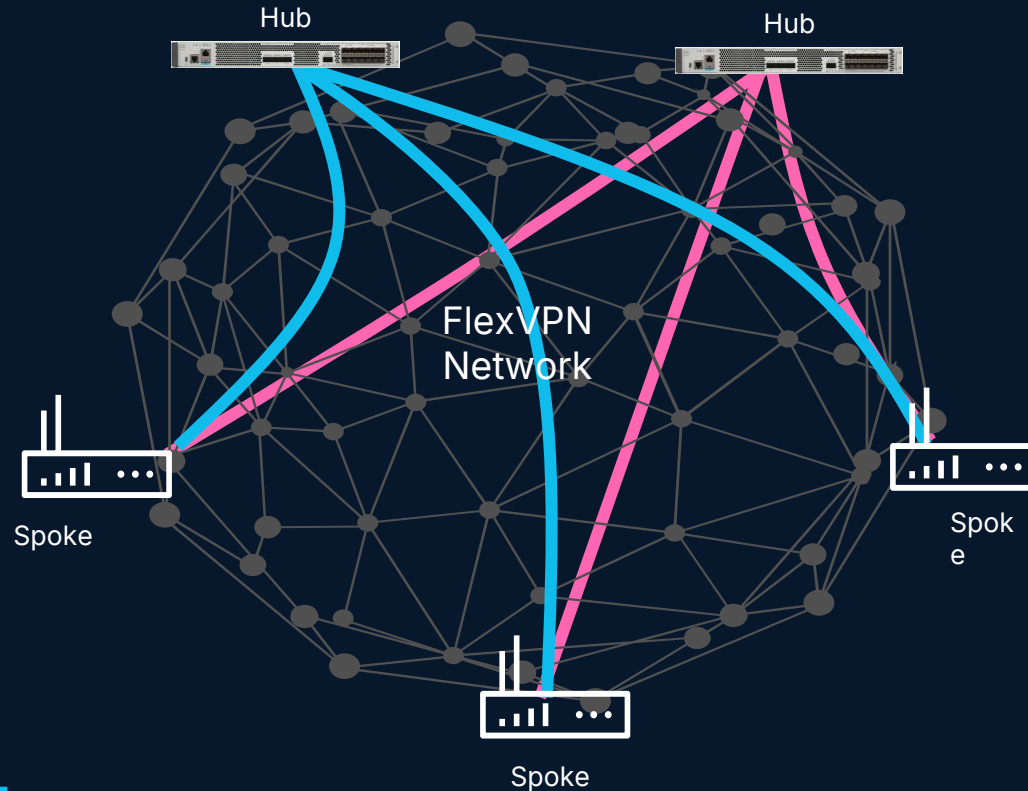
```
! Configure
crypto ikev2 proposal ikev2proposal
  encryption aes-cbc-256
  integrity sha512
  group 21
  pqc mlkem768 optional
!
crypto ikev2 policy ikev2policy
  proposal ikev2proposal
!

! Use show crypto ikev2 sa for verification
```

Same configuration
as IKEv2 IPsec

PQC ML-KEM for FlexVPN

FlexVPN is a standards-based framework to secure sites with IPsec



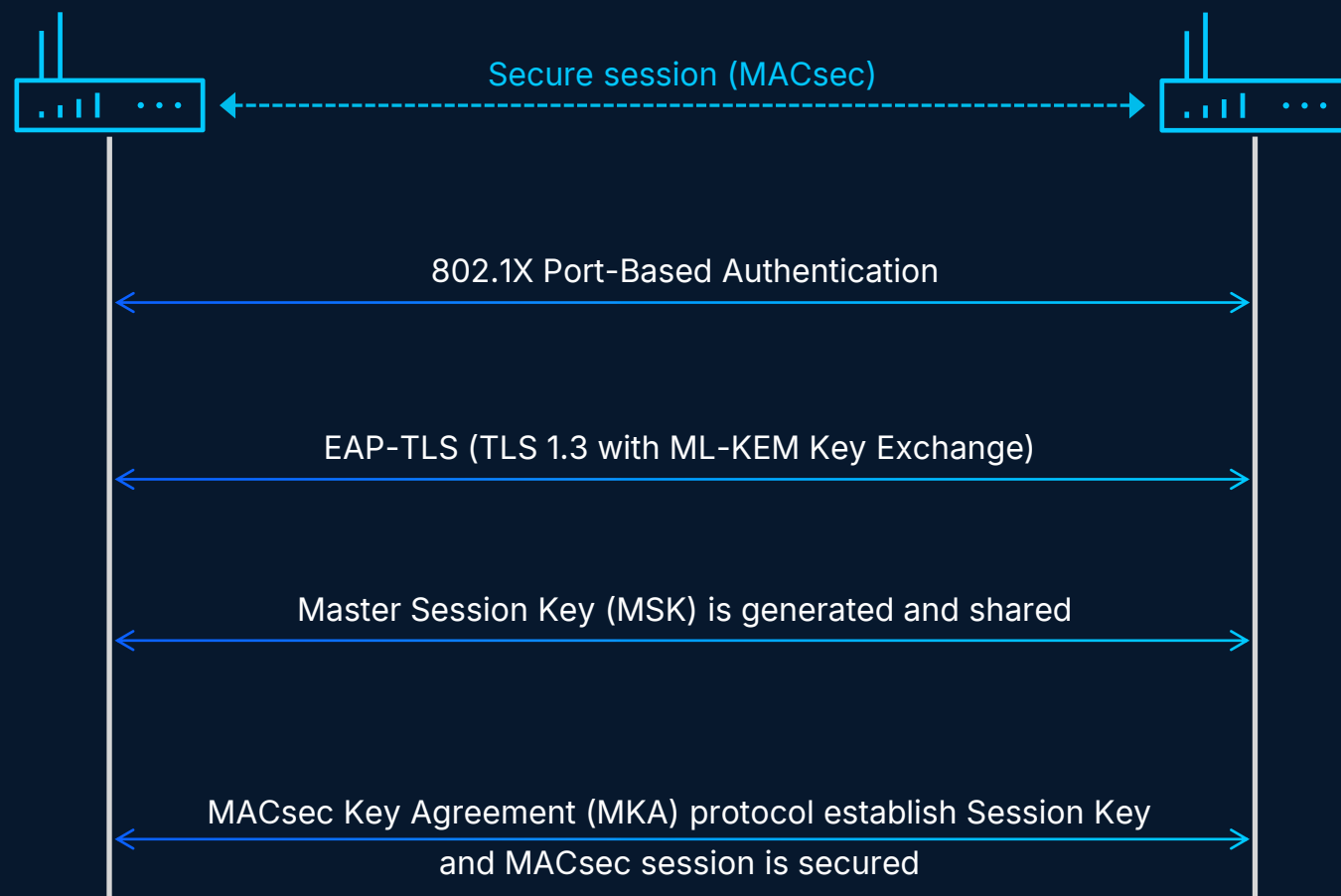
```
! Configure
crypto ikev2 proposal ikev2proposal
  encryption aes-cbc-256
  integrity sha512
  group 21
  pqc mlkem1024
!
crypto ikev2 policy ikev2policy
  proposal ikev2proposal
!

! Use show crypto ikev2 sa for verification
```

Same configuration
as IKEv2 IPsec

PQC ML-KEM for MACsec with EAP-TLS

Certificate-based MACsec encryption (RFC 9190)



Quantum-safe LAN/WAN MACsec with EAP-TLS

```
! Config
eap profile EAP-PROFILE
method tls
pki-trustpoint name
exit
dot1x credentials DOT1X-CREDS
username <username>
pki-trustpoint <name>
!
access-session tls-version all
!
access-session pqc-type pqc
!
interface <interface-id>
macsec
authentication periodic
authentication timer reauthenticate interval
access-session host-mode multi-domain
access-session closed
access-session port-control auto
dot1x pae both
dot1x credentials profile
dot1x authenticator eap profile <name>
dot1x supplicant eap profile <name>
service-policy type control subscriber <control-
policy name>
!
```

Enables PQC ML-KEM
algorithm for EAP-TLS

Router# **show dot1x interface Te0/1/1 detail**

```
Dot1x Info for TenGigabitEthernet0/1/1
PAE = BOTH

QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
EAP profile = EAP-PROFILE
Dot1x Info for
PAE = SUPPLICANT
StartPeriod = 30
AuthPeriod = 30
HeldPeriod = 60
MaxStart = 3
Credentials profile = DOT1X-CREDS
Dot1x Authenticator Client List

EAP Method = TLS
Supplicant = 78bc.1a60.d28a
Session ID = 0000000000000000C11F60339
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
Dot1x Supplicant Client List
```

PQC ML-KEM for SSH

```
ip ssh client algorithm kex <>
ip ssh server algorithm kex <>
```

ML-KEM selection
in KEX CLI

! New KEX config options:

```
mlkem768nistp256-sha256
mlkem1024nistp384-sha384
mlkem768x25519-sha256
```

```
Router# show ip ssh
SSH Enabled - version 2.0
```

<<< output removed for brevity >>>

```
KEX Algorithms:mlkem1024nistp384-
sha384,mlkem768nistp256-sha256,mlkem768x25519-
sha256
```

<<< output removed for brevity >>>

PQC for SD-WAN

Management Plane:

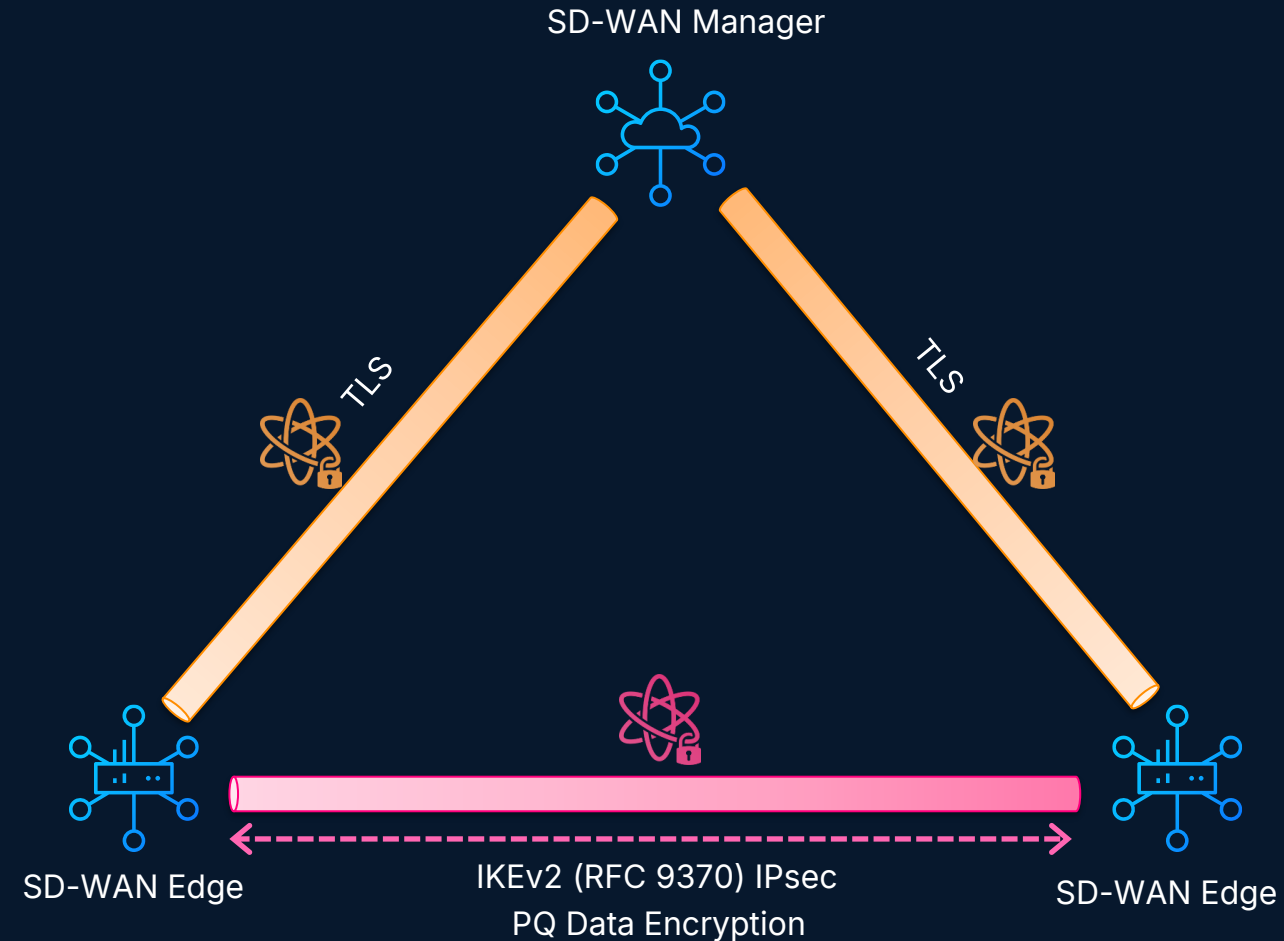
- Uses standards-based TLS
 - IETF draft - Hybrid key exchange in TLS 1.3
 - TLS with DH/ECDH + PQC(ML-KEM)

Control Plane

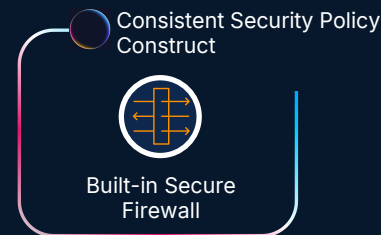
- Uses **standards-based** IKEv2/IPSec
 - RFC 9370 - Multiple Key Exchanges in IKEv2
 - IKEv2 with DH/ECDH + PQC(ML-KEM)

Data Plane

- Uses the same AES-GCM-256 cipher



Secure Firewall embedded in the Secure Routers



Management, Monitoring & Analytics



SD-WAN Manager



Cloud Control



Splunk

Next Generation Firewall



**L3 – L7 + Identity
FW**

Manage traffic traversing the branch



IPS/IDPS

Protect assets from bad actors



AMP

Protect against malware



Sandboxing

File Analysis using Threat Grid



URL-F

Filter Internet traffic



TLS Decryption

Traffic Decryption



SSE Ecosystem



Auto Tunnel + HA

Automatic IPsec tunnels to SSE – 8 Active / 8 Standby



Traffic Steering

App based traffic inspection and redirection to SSE



CASB

Govern access to cloud applications



FWaaS

Manage traffic to the internet



DLP

Protect sensitive data from unauthorized access



DNS/SWG

Protect web servers / applications

Proven Security Efficacy

99.23%

Intrusion Prevention
(IPS) Effectiveness

99.79%

Malware Detection
Rate

NetSec**✓**OPEN

Independent
Evaluation

Trusted
Organization

Deploy with
Confidence



[NetSecOpen Certification Report for 8375-E-G2 Secure Router](#)

[NetSecOpen Certification Report for 8235-G2 Secure Router](#)

Small Branch Portfolio

↑
Connectivity / Performance

Routing only

C8140-G2



5.6Gbps, 1.5Gbps, N/A

C8130H-G2
C8130-VAI/P-G2
C8130-G2



1.9Gbps, 1.5Gbps, N/A

Routing/SD-WAN

C8151H-C-G2
C8161-G2
C8151-G2
C8151-[CVAI/P]-G2



5.6Gbps, 1.5Gbps, 1Gbps

C8131-G2



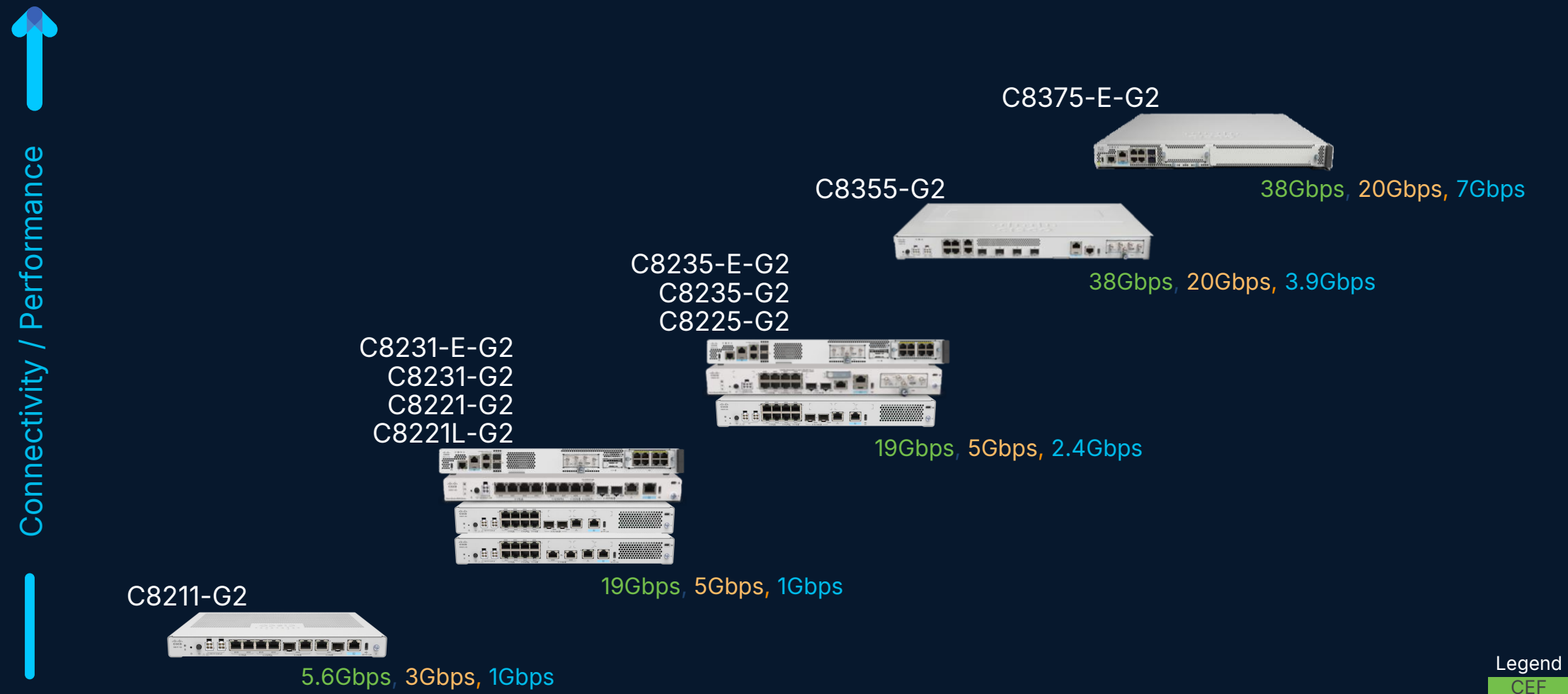
1.9Gbps, 1.5Gbps, 1Gbps

[1]Threat Protection: 100% DIA-NAT + App Aware FW + IPS + URLF + AMP

Legend

CEF
IPsec
TP ^[1]

Medium and Large Branch Portfolio



[1]Threat Protection: 100% DIA-NAT + App Aware FW + IPS + URLF + AMP

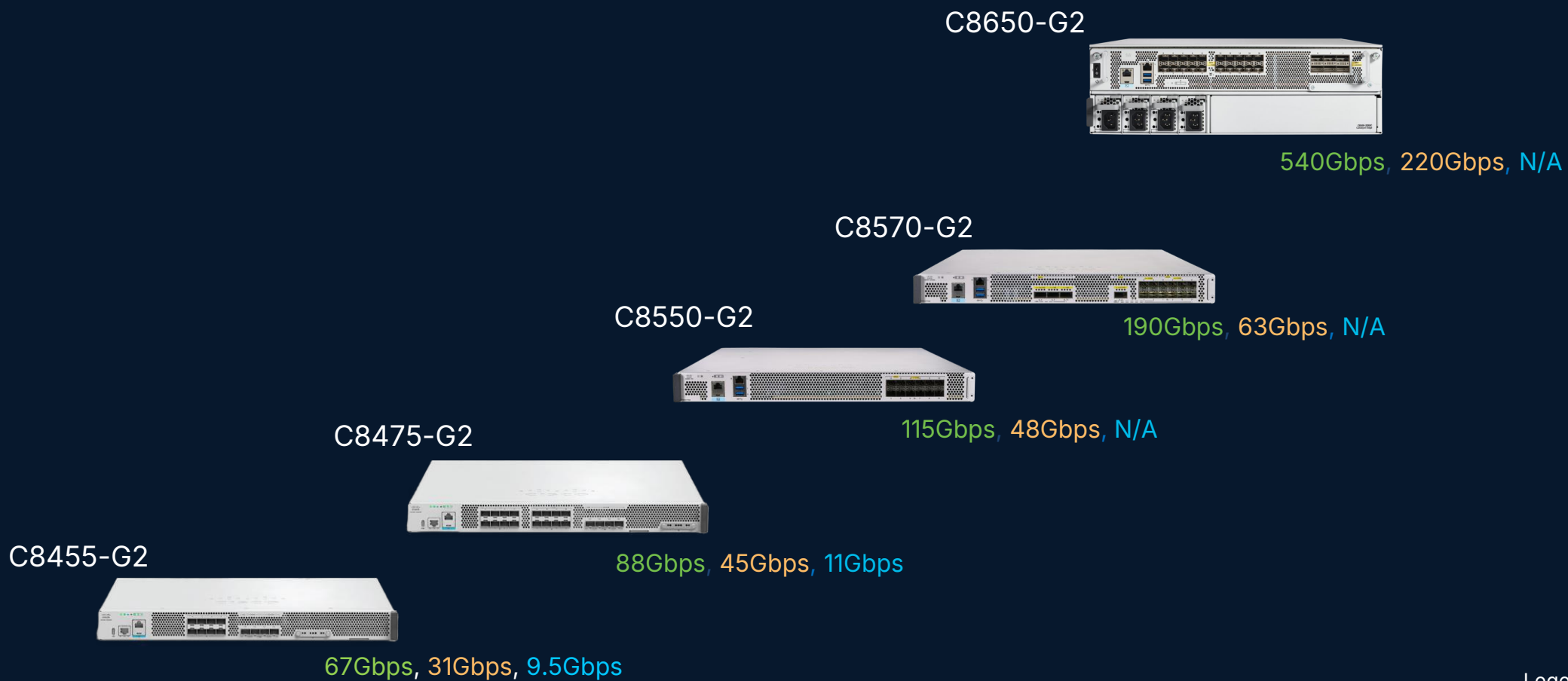
Legend

- CEF
- IPsec
- TP(1)

Campus and DC Portfolio



Connectivity / Performance



[1]Threat Protection: 100% DIA-NAT + App Aware FW + IPS + URLF + AMP

[1] Threat Protection: 100% DIA-NAT + ZBFW + IPS + URLF + AMP

© 2026 Cisco and/or its affiliates. All rights reserved.

BRKXAR-2027

Legend

CEF
IPsec
TP ^[1]



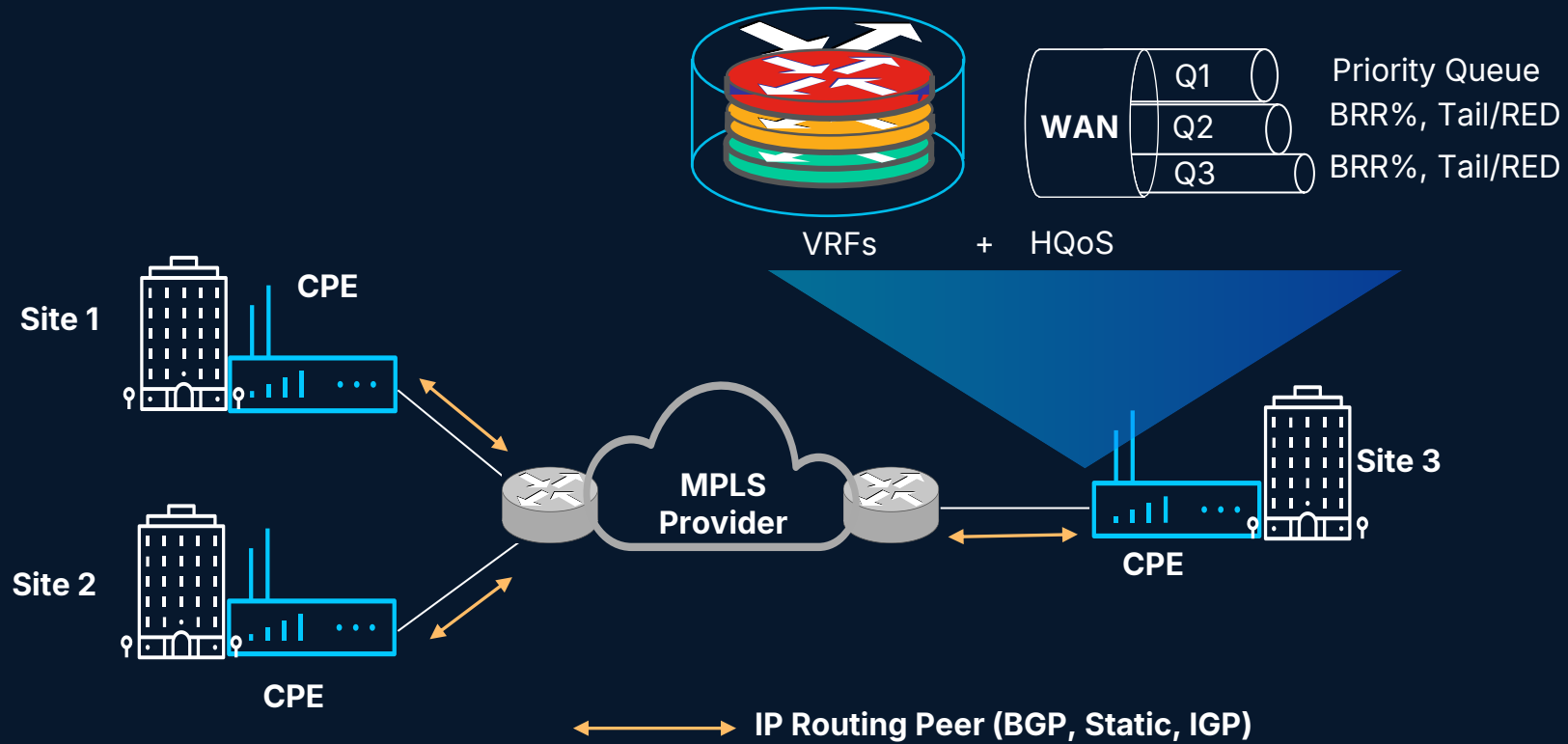


Elevate Secure WAN Use-cases

Primary Secure WAN Use Cases

1	MPLS CPE	CPE managed by enterprise or MSP, establish routing peering with MPLS provider PE for sites connectivity, provides VRF segmentation and QoS capabilities.
2	Overlay VPN	Enterprise want to have more control of their own network topology, build Overlay VPN on top of providers' transport network, typically in a Hub & Spoke topology with on-demand tunnels.
3	SD-WAN	Software-defined WAN to route the application to the best path to satisfy Application Aware Routing (AAR) policy.
4	Secure Branch DCA/DIA	Secure Branch direct cloud access (DCA) or direct Internet access(DIA) w/ Threat Protection (TP) using built-in Secure Firewall.
5	Secure Networks	Build highly resilient, secure and scalable network for Military protected core, Utility, Transportation & Govt agencies. It is typically deployed with Segment Routing solution.
6	Internet Gateway	BGP peering with multiple Internet service providers to learn full internet route table, provide resilient Internet access, network address translation and protect against Denial-of-Service Attack.
7	Cloud Edge	Connect on-prem sites at Colo or DC to multi-cloud via private, high-speed connections such as AWS DX, Azure ER, which are encrypted by IPsec or MACsec.

MPLS CPE

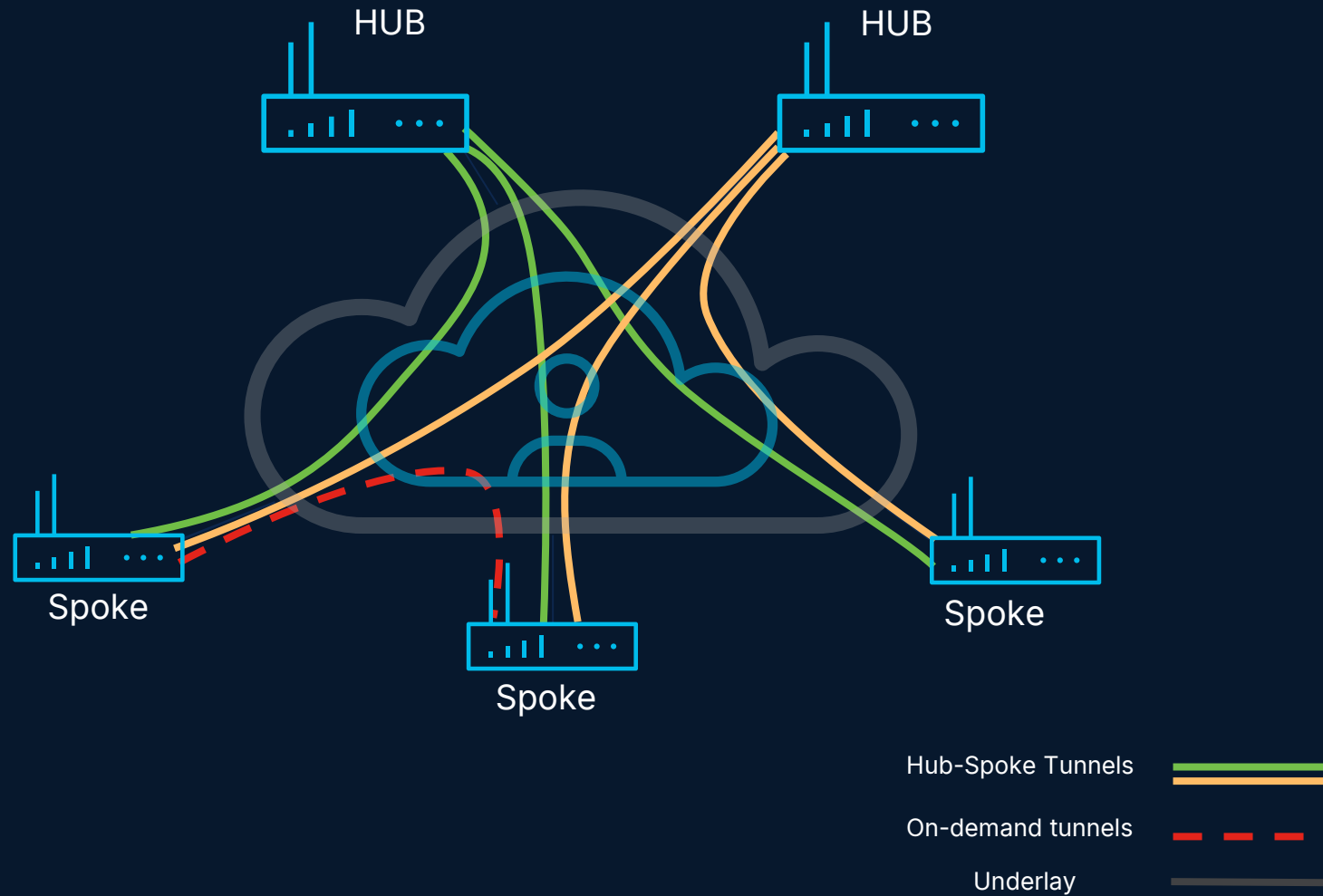


MPLS CPE - cont'd

Secure Routers	Why the Secure Routers are better*	VRF + HQoS Throughput @512B
8100	- Up to 2x faster 10GE Copper and XGSPON WAN	Up to 2.9Gbps
8200	- Up to 4x faster 10GE & mGig WAN	Up to 13.5Gbps
8300	- Up to 2x faster 4x 10GE & mGig connectivity	Up to 28Gbps
8400	- Up to 3x faster 25GE WAN	Up to 65Gbps
8500/8600	Continued perf excellence	Up to 420Gbps

* Better, faster than previous generation products
 8100 compared against ISR1K
 8200 compared against Catalyst 8200 Series
 8300 compared against Catalyst 8300 Series
 8400 compared against C8500L-8S4X
 8500 compared against C8500-12X, C8500-12X4QC
 8600 compared against C8500-20X6C

Overlay VPN



Overlay VPN – cont'd

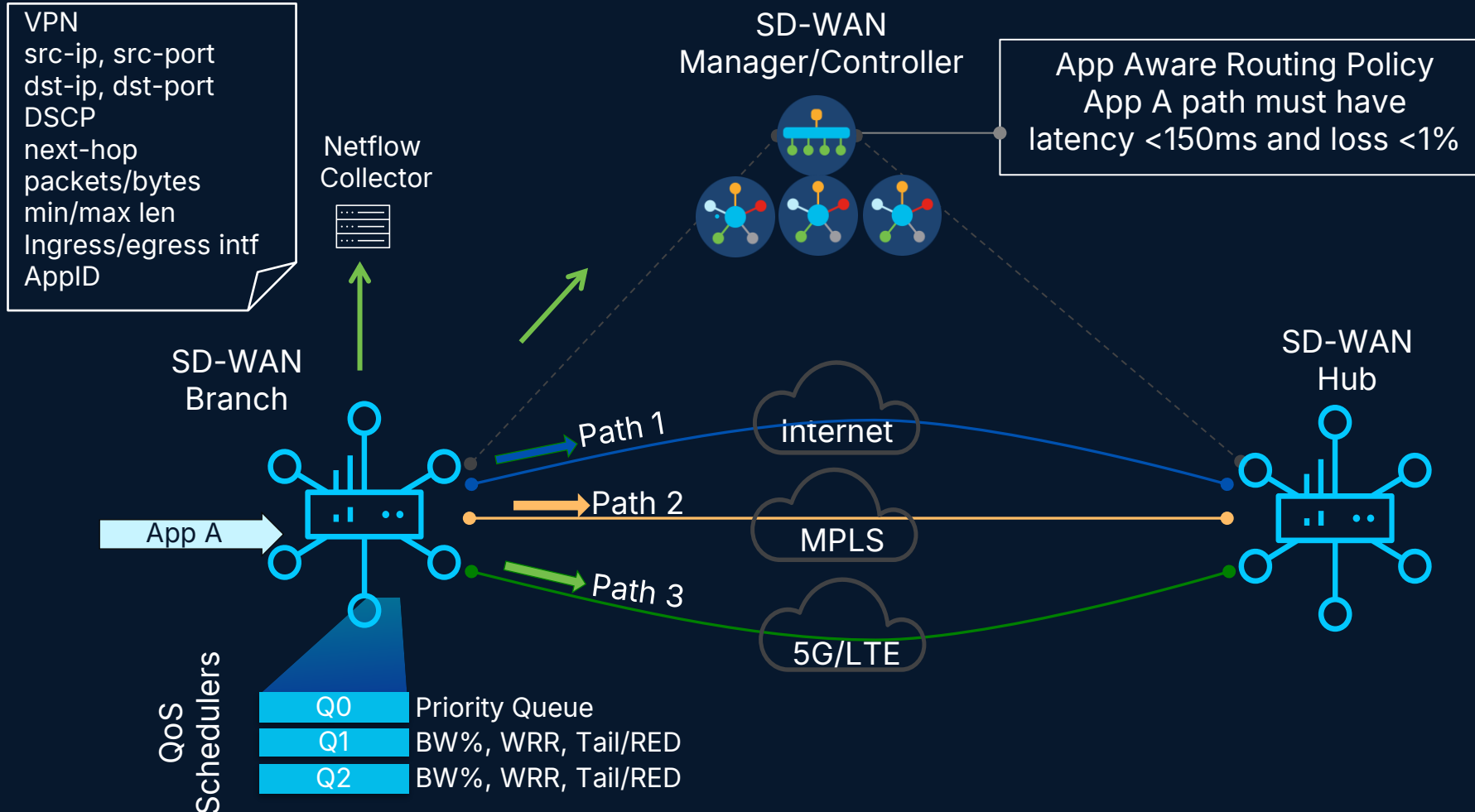


Secure Routers	Why the Secure Routers are better*	IPsec Throughput @512B
8100	• Up to 2x faster • 10GE Copper and XGSPON WAN	Up to 1.5Gbps
8200	• Up to 5x faster • 10GE & mGig WAN	Up to 5Gbps
8300	• Up to 10x faster • 4x 10GE & mGig connectivity	Up to 20Gbps
8400	• Up to 3x faster • 25GE WAN	Up to 45Gbps
8500/8600	• Continued perf excellence	Up to 220Gbps

* Better, faster than previous generation products

SD-WAN

Application Aware Routing (AAR)



SD-WAN – cont'd

Application Aware Routing (AAR)



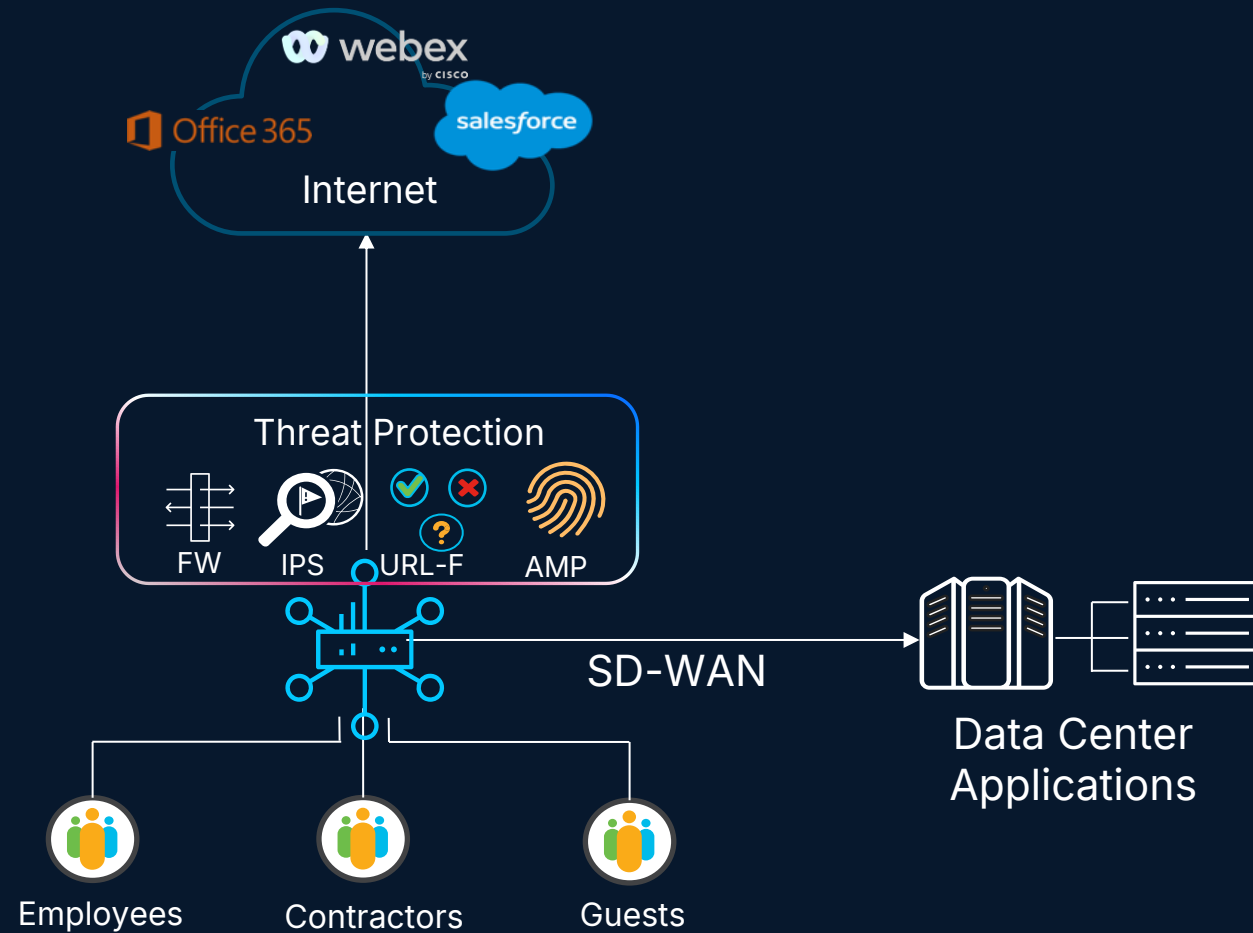
Secure Routers	Why the Secure Routers are better*	AAR ^[1] Throughput @512B
8100	• Up to 3x faster • 10GE Copper and XGSPON WAN	Up to 1Gbps
8200	• Up to 4x faster • 10GE & mGig WAN	Up to 4Gbps
8300	• Up to 4x faster • 4x 10GE & mGig connectivity	Up to 12Gbps
8400	• Up to 2x faster • 25GE WAN	Up to 20Gbps
8500/8600	• Continued perf excellence	Up to 82Gbps

* Better, faster than previous generation products

[1] App Aware Routing (AAR): IPsec+QoS+DPI+FNF

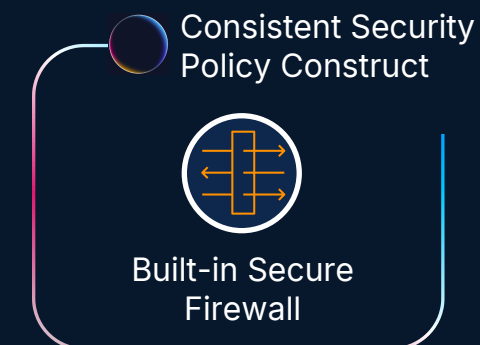
Secure Branch DCA/DIA

with Built-in Secure Firewall



Secure Branch DCA/DIA

Cisco 8000 Series Secure Routers - Miercom: Independent Analysis, Research and Reviews



Secure Routers	Why the Secure Routers are better*	TP ^[2] Throughput @EMIX	50% DIA-TP ^[3] Throughput @EMIX
8100	- Up to 6x faster - TLS Decryption^[1]	Up to 1Gbps	Up to 1Gbps
8200	Up to 2x faster	Up to 2.4Gbps	Up to 1.9Gbps
8300	Up to 3x faster	Up to 7Gbps	Up to 7Gbps
8400	Up to 3x faster	Up to 11Gbps	Up to 11Gbps

* Better, faster than previous generation products

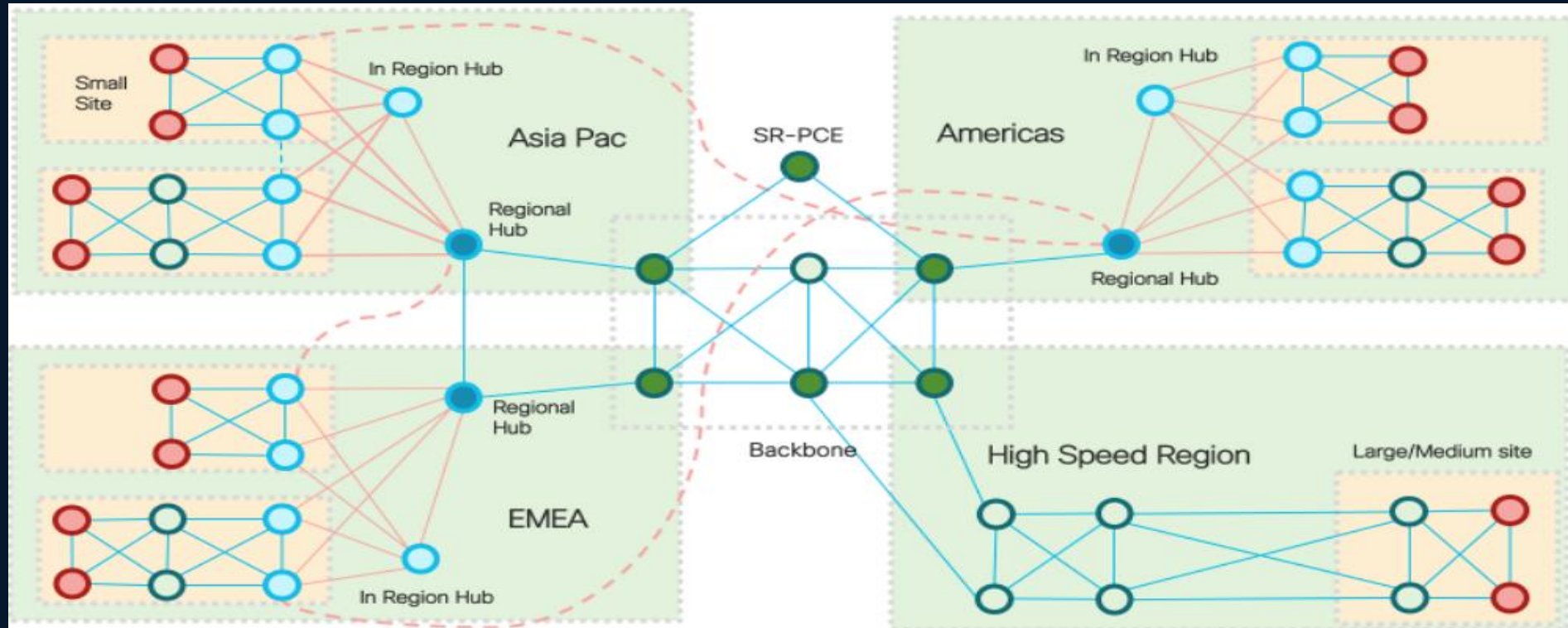
[1] TLS Decryption is new to small branch routers, already supported on previous gen medium/large branch and campus routers

[2] Threat Protection (TP): 100%DIA-NAT + App aware FW + IPS + URL-F + AMP

[3] 50% DIA-TP: IPsec + QoS + DPI + FNF + DIA-NAT50% + ZBFW + IPS + URL-F + AMP + TG

Secure Networks

Typically deployed with Segment Routing Solution



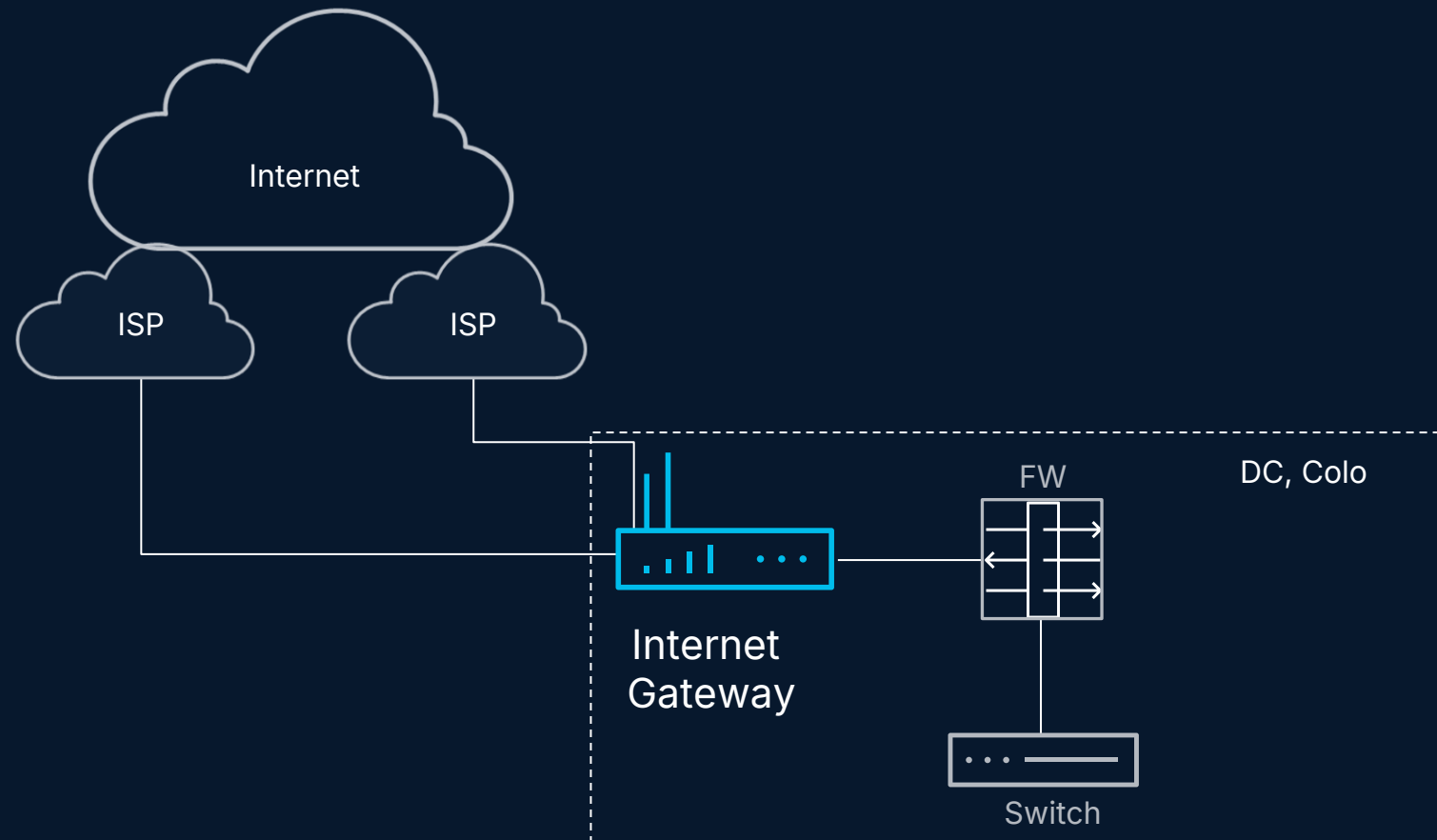
Secure Networks – cont'd

Secure Routers	Why the Secure Routers are better*	IPsec Throughput @512B
8100	Up to 2x faster	Up to 1.5Gbps
8200	- Up to 5x faster - WAN/LAN MACsec on all built-in ports^[1]	Up to 5Gbps
8300	- Up to 10x faster - WAN/LAN MACsec on all built-in ports^[1]	Up to 20Gbps
8400	- Up to 3x faster - Fast Reroute (<50msec convergence) - Ingress Classification (e2e QoS treatment)	Up to 45Gbps
8500/8600	Continued perf excellence	Up to 220Gbps

* Better, faster than previous generation products

[1] In previous gen branch routers WAN/LAN MACsec is only supported on 8300-2N2S-4T2X built-in 10GE ports, other models require specific NIM modules, it is fully supported in prev gen campus and DC routers.

Internet Gateway

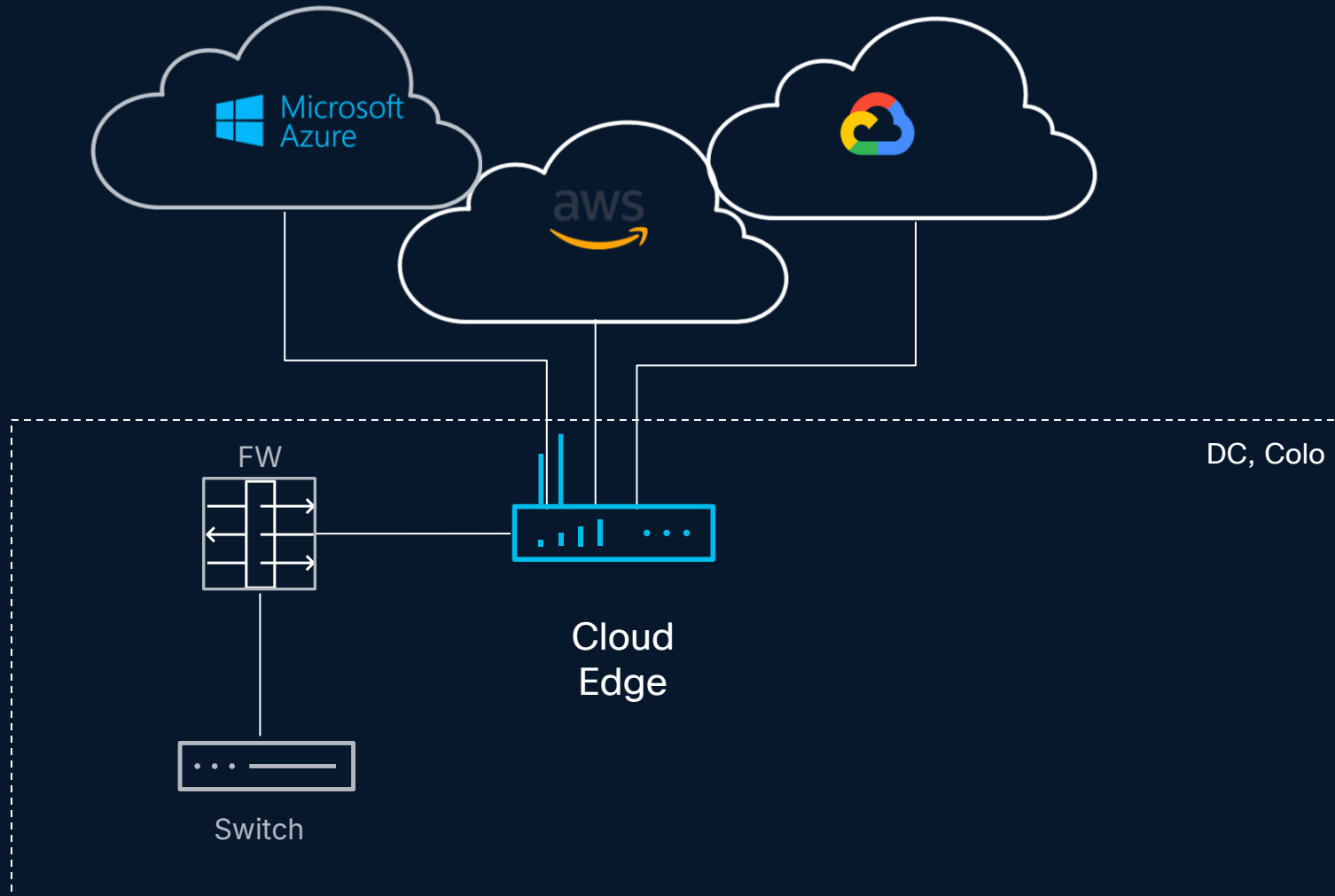


Internet Gateway – cont'd

Secure Routers	Why the Secure Routers are better*	NAT Throughput @512B
8300	• Up to 2x faster • 4x 10GE & mGig connectivity	Up to 26Gbps
8400	• Up to 2x faster • 25GE WAN • 2x NAT session scale (4M)	Up to 59Gbps
8500/8600	• Continued perf excellence • 2x BGP route scale (8M) on 8500	Up to 300Gbps

* Better, faster than previous generation products

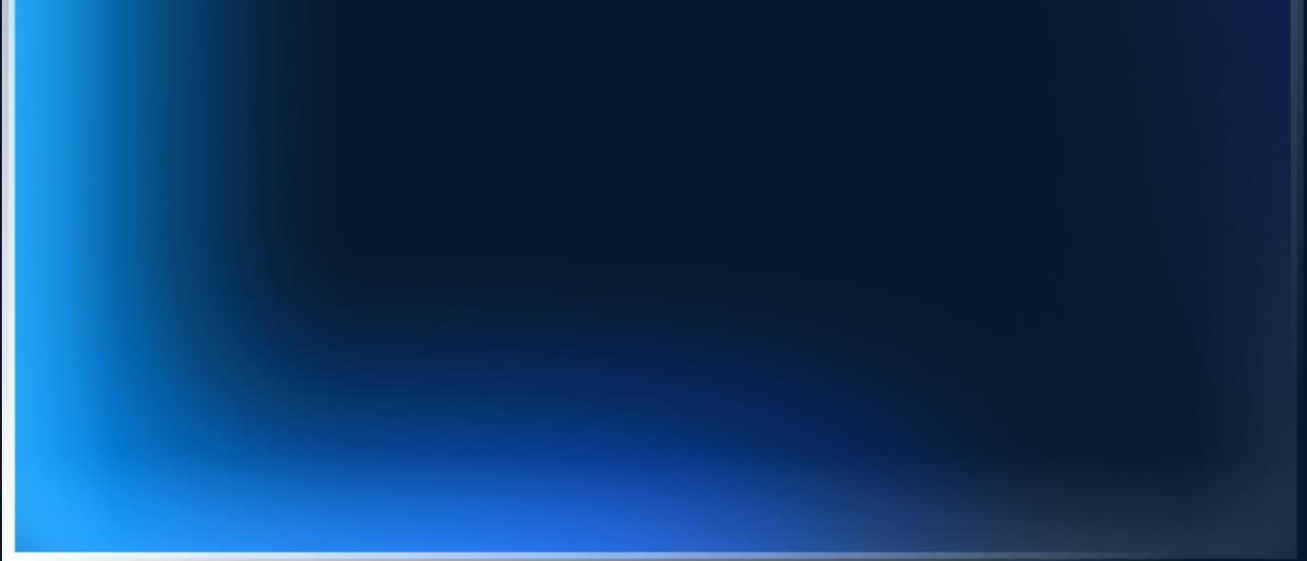
Cloud Edge



Cloud Edge – cont'd

Secure Routers	Why the Secure Routers are better*	IPsec Throughput @512B
8300	• Up to 10x faster • WAN/LAN MACsec on all built-in ports	Up to 20Gbps
8400	• Up to 3x faster	Up to 45Gbps
8500/8600	• Continued perf excellence	Up to 220Gbps

* Better, faster than previous generation products

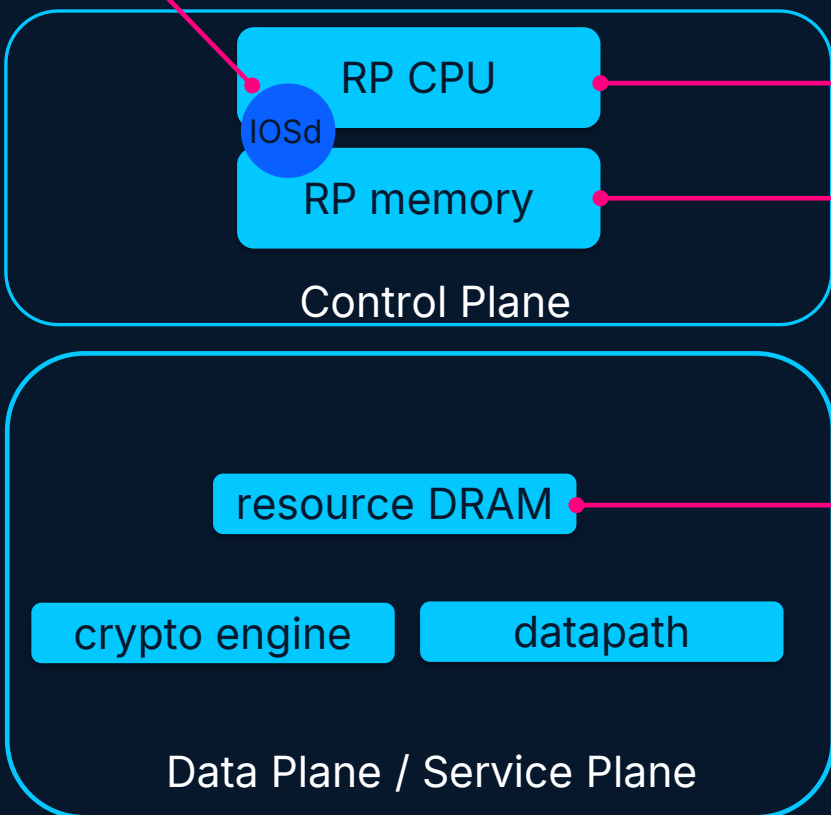


Operational Best Practices



Key System Resources to Monitor

show mem stat
show proc cpu sort



```
G2#show platform resources
```

```
**State Acronym: H - Healthy, W - Warning, C -
```

```
Critical
```

Resource	Usage	Max	Warning	Critical	State
RP0 (ok, active)					H
Control Processor	1.75%	100%	80%	90%	H
DRAM	3941MB(25%)	15755MB	88%	93%	H
ESP0(ok, active)					H
QFP					H
DRAM	48320KB(2%)	2326528KB	85%	95%	H

- Use CISCO-PROCESS-MIB to monitor CPU/Memory on RP
- Use CISCO-ENTITY-QFP-MIB to monitor QFP Memory

Mitigation Plan when run out of resources

Before upgrading platform/memory, customer can immediately take following actions to reduce system resources utilization:

- IOS/Control CPU Memory

1. Shutdown routing peers

```
neighbor {ip-address} shutdown graceful <seconds>
```

2. Reduce prefixes received from a peer

```
neighbor {ip-address} maximum-prefix <number of prefixes>
```

3. Turn off Software Redundancy

1. redundancy \ mode none

- QFP Resources DRAM

1. Reduce NAT max-entries:

```
ip nat translation max-entries <number of entries>; nat64 translation max-entries <number of entries>
```

2. Reduce FW session limit:

```
parameter-map type inspect global \ session total <count>
```

3. Reduce FNF cache limit:

```
flow monitor M1 \ cache entries <number of entries>
```

Datapath Utilization (1)

G2#show platform hardware qfp active datapath utilization summary

CPP 0:		5 secs	1 min	5 min	60 min
Input:	Total (pps)	2247717	1429213	1533059	212076
	(bps)	9134674616	5808330472	6230309296	861840936
Output:	Total (pps)	2247875	1430428	1532668	212095
	(bps)	9135341648	5813199336	6228747712	861932720
Processing: Load (pct)		99	61	67	9
Crypto/I/O					
RX: Load (pct)		0	0	0	0
TX: Load (pct)		41	26	28	5
Idle (pct)		58	73	71	94

Tip

bps/pps/8 = average
packet size in Bytes

Datapath Utilization (2)

G2#show platform hardware qfp active datapath infrastructure sw-cio

Core Utilization over preceding 5767441.1701 seconds

ID:	0	1	2	3	4	5	6	7	8	9	10	11	12	13
% PP:	0.71	0.15	0.16	0.18	0.16	0.17	0.17	0.17	0.16	0.16	0.17	0.16	0.00	0.00
% RX:	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
% TM:	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.40	1.59
% IDLE:	99.29	99.85	99.84	99.82	99.84	99.83	99.83	99.83	99.84	99.84	99.83	99.84	98.60	98.41

Crypto Engine Utilization

```
G2#show platform hardware crypto-device utilization
Past crypto device utilization:
utilizaition is for each crypto device, pkts are combined number.
 1 min (percentage) : 7%
    (decrypt pkt): 19744614
    (encrypt pkt): 35508495
 5 min (percentage) : 8%
    (decrypt pkt): 98761304
    (encrypt pkt): 177577353
15 min (percentage) : 7%
    (decrypt pkt): 292639607
    (encrypt pkt): 526899471
```

- CISCO-ENTITY-PERFORMANCE-MIB can monitor Crypto Engine Util

Secure Firewall System Resource Utilization

```
G2#sh platform software cpu alloc
```

```
CPU alloc information:
```

```
Control plane cpu alloc: 0-1
```

```
Data plane cpu alloc: 0,10-23
```

```
Service plane cpu alloc: 2-9
```

```
Template used: CLI-service_plane_heavy
```

```
G2#show processes cpu platform sorted | sec snort
20468 12655 451% 352% 248% S 2319156 snort3
```

```
G2#show utd engine standard status
```

```
Engine version : 1.14.16_SV3.1.81.0_XEmain
```

```
Profile : Cloud-High
```

```
System memory :
```

```
Usage : 5.8%
```

```
Status: Green
```

```
Number of engines : 6
```

```
Engine Running Health Reason
```

```
=====
```

```
Engine(#1): Yes Green None
```

```
Engine(#2): Yes Green None
```

```
Engine(#3): Yes Green None
```

```
Engine(#4): Yes Green None
```

```
Engine(#5): Yes Green None
```

```
Engine(#6): Yes Green None
```

```
=====
```

```
Overall system status: Green
```



Key Takeaways

Industry's most advanced Secure Router

Connect Secure WAN to every site

Cisco 8000 Series Secure Router



- **Secure Networking Processor** - Leapfrogs up to 10x higher throughput, AI-ready
- **Post-quantum Secure WAN** – Full-stack PQC
- **Advanced Security** – NGFW & SASE with 6x threat protection throughput
- **Operational Simplicity** – Managed by SD-WAN Manager and Cloud Control

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2027.



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



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



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



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

CISCO Live !

Thank you



