Quantum Safe Cryptography And Why You Need it

Andrew Benhase
Federal Architect, US Public Sector
@CyberSecOps

BRKSEC-2175

A Reference to “Quantum”... Many things to many people

Quantum Computer

A super powerful computer, based on quantum mechanics, allowing parallel processing and super fast execution of certain problems.

Quantum Networking

A global network that connects quantum computers **securely**, connecting multiple quantum processors for increased computational power and efficiency. This enhances complex problem solving, even in AI.

Quantum Cryptography

Post Quantum Cryptography

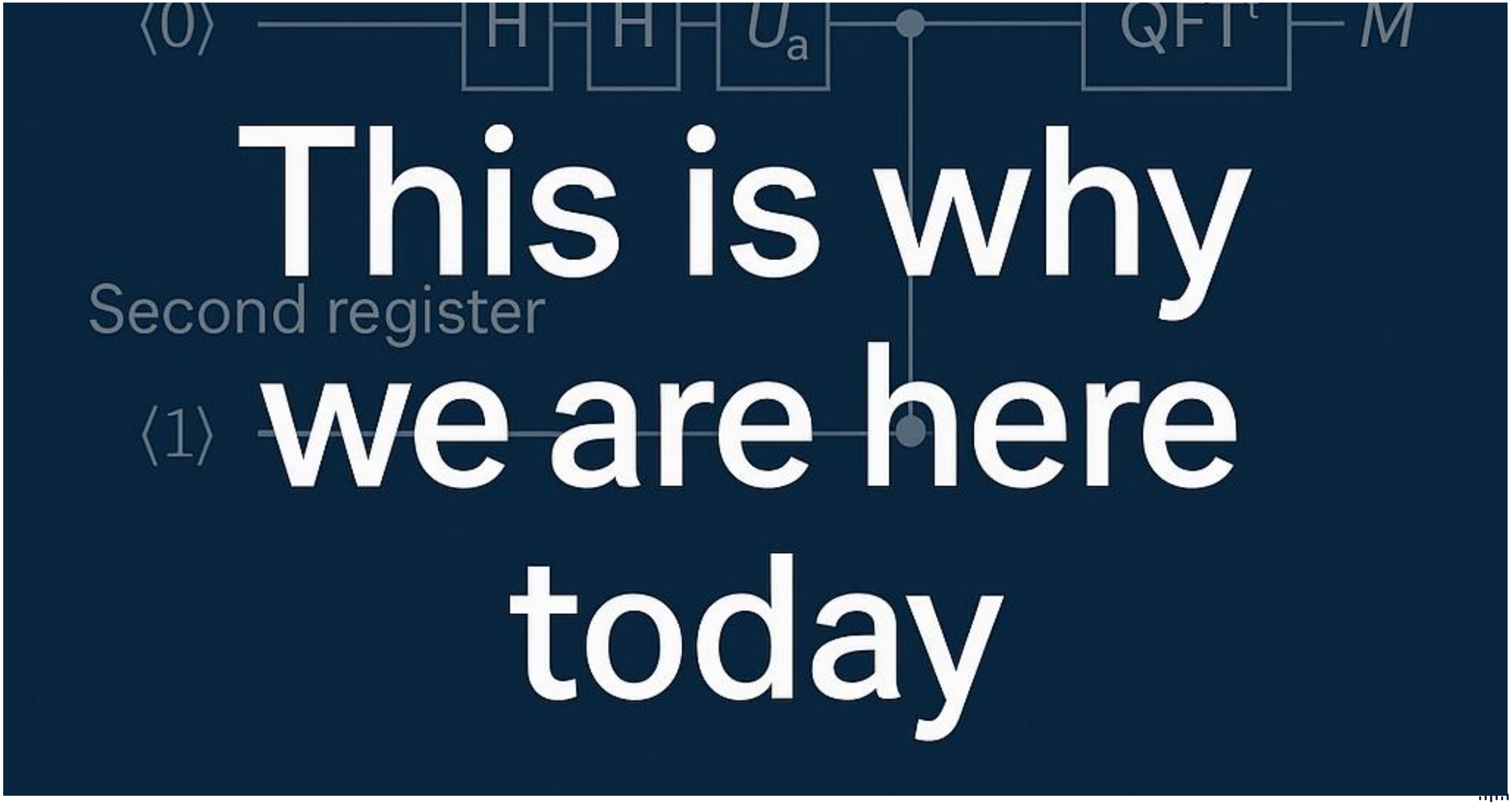
The cryptographic algorithms designed to be secure against quantum computer attacks unlike classical crypto (e.g., RSA, ECC).

Quantum Key Distribution

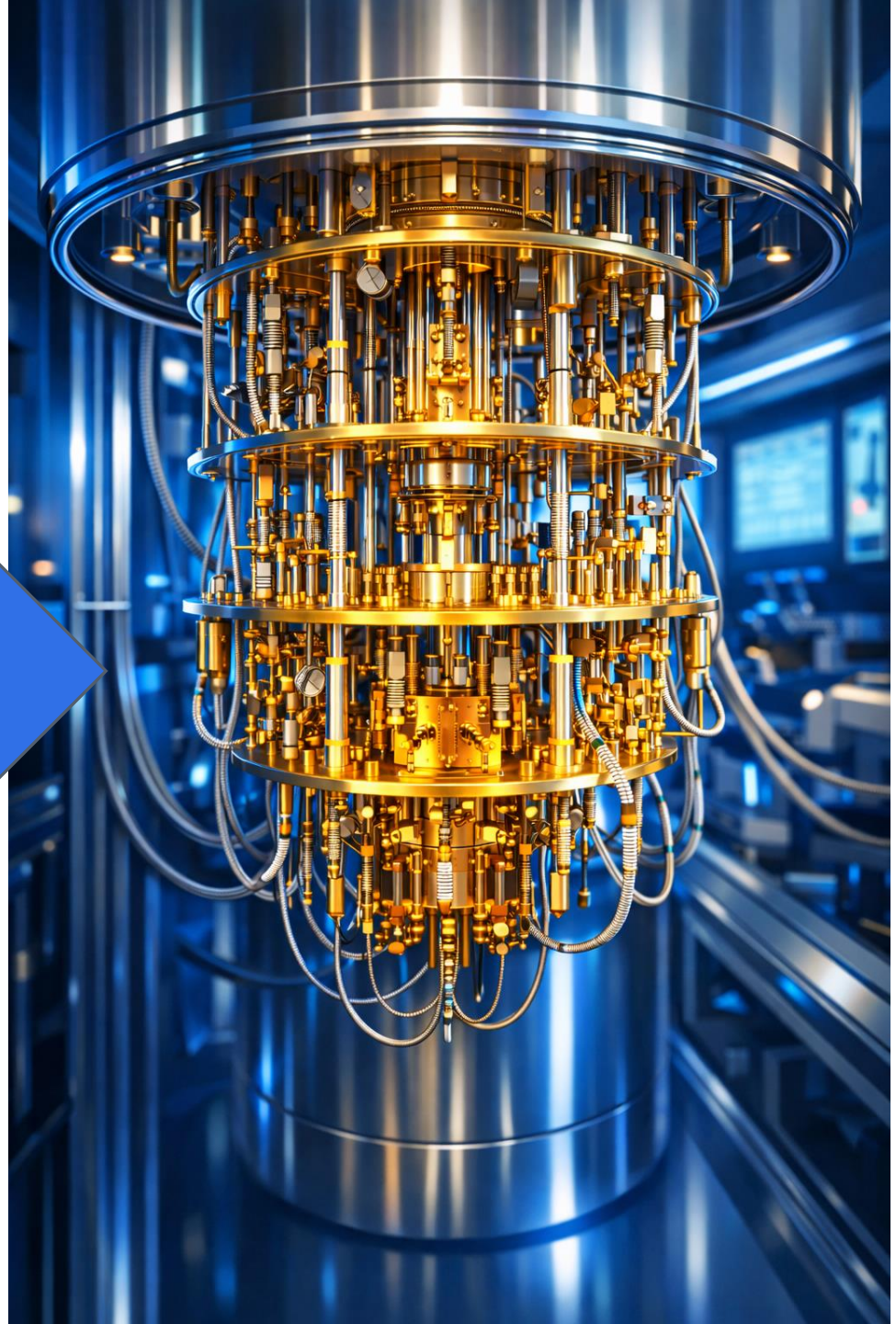
Uses quantum mechanics to securely exchange encryption keys between two or more elements.

Quantum Random Number Generation

The QRNG plays a critical role in quantum encryption, typically with QKD by ensuring the unpredictability of the cryptographic keys.



And because of this...



Quantum Baseline

Quantum Terminology

- Quantum Resistance – making it mathematically harder for a Quantum Computer
- Post Quantum Algorithms – set of CNSA 2.0 compliant algorithms that are deemed resistant to Quantum based attacks
- Quantum Safe – algorithm/capability set that has been determined to be resistant to Quantum based attacks
- ML-KEM – also known as “Kyber”
- ML-KEM 1024 – minimum modulus size for US Government
- PQ-TLS – Post Quantum TLS – point of introduction for post-quantum
- Cisco Cryptographic Provider 8.3 – entry point for PQ Algorithms for use internally at Cisco – released JAN 2025

What is the big problem here?

- A Quantum computer with sufficient Quantum Bit (Qubit) density could, assuming many other factors, present a capable platform for large prime factorization and potentially expose RSA based systems to cryptographic weakness
- Asymmetric exchange systems are potentially vulnerable
- Lays open the possibility that current RSA based crypto systems could become compromised over the next 10 years
- Quantum glide slope is targeted at full implementation of PQ Safe Algorithms in existing protocols by 2030

What is Quantum Resistance?

- QR to Cisco is IKEv2 Pre-Shared Key
- There was no analgous standard in IKEv2 RFC 5996 compared to IKEv1 RFC 2401 for Pre-Shared Keys
- IKEv2 Pre-Shared Keys is implemented in RFC 8784
- Provides for a symmetric key mix
- Defined as minimum standard for CNSA 1.0 (RFC 9206) for Quantum Resistance by the US Government
- We have minimum requirements for RFC 8784 in ASA and IOS-XE

What is Post Quantum?

- It means the implementation of FIPS 203,204,205 defined algorithm sets
- Integrated into either IKEv2 or TLS 1.3 or possibly Secure Shell
- Requires new version of RFC 9206 (CNSA 1.0) for CNSA 2.0 defined cipher suites
- Requires new version of RFC 5996 for PQ-IKEv2 (draft)
  - Example: https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/
- Requires new version of RFC 8446 for PQ-TLS 1.3 (draft)
  - Example: https://datatracker.ietf.org/doc/draft-connolly-tls-mlkem-key-agreement/
- Requires new version of RFC for PQ-SSHv2 (see above)

- Also see:
- https://www.ietf.org/id/draft-sfluhrer-cfrg-ml-kem-security-considerations-02.html

IKE / Cryptographic Evolution Timeline

- From RFC 2041 to RFC 9206

RFC 2041 – IKE Message Types (1996)

- Purpose: Early ISAKMP / IKEv1 Framework
  - Defined IKE message exchange formats
  - Introduced payload extensibility
  - Established Phase 1 / Phase 2 negotiation structure
  - Enabled early interoperable IPsec deployments

RFC 4306 – Internet Key Exchange Version 2 (2005)

- Purpose: Modern IPsec Foundation
  - Complete IKEv2 protocol redesign
  - Reduced message complexity
  - Integrated NAT traversal
  - Enhanced DoS protection
  - Simplified state handling
  - Enabled enterprise VPN and SD-WAN architectures

RFC 8784 – IKEv2 Multiple Key Exchanges (2020)

- Purpose: Enable Hybrid & Future Cryptographic Agility in IKEv2
  - Introduces support for multiple key exchanges within a single IKE_SA
  - Allows simultaneous classical and post-quantum key establishment
  - Maintains backward compatibility with RFC 4306
  - Foundational enabler for hybrid PQC IKE deployments
  - Critical precursor to CNSA 2.0 and post-quantum IPsec migration

RFC 9206 – CNSA Cryptographic Profile (2022)

- Purpose: High Assurance Government Crypto Profile
  - Aligns IKEv2 with NSA CNSA requirements
  - Defines mandatory strong algorithm selection
  - Eliminates legacy cryptography
  - Provides quantum-transition readiness
  - Mandated Algorithms: AES-256-GCM, SHA-384, ECDH P-384

Quantum Timelines

HISTORICAL TIMELINE

2015

CNSA 1.0 Publiined

Commercial National Security Algoritum Suite (CNSA 1.0)

2017

CNSSP No. 15

CNSA 1.0 Required for Classified Systems

2020

Quantum Risk Mitigation

Federal Quantum Readiness Guidance

2020

Quantum Risk Mitigation

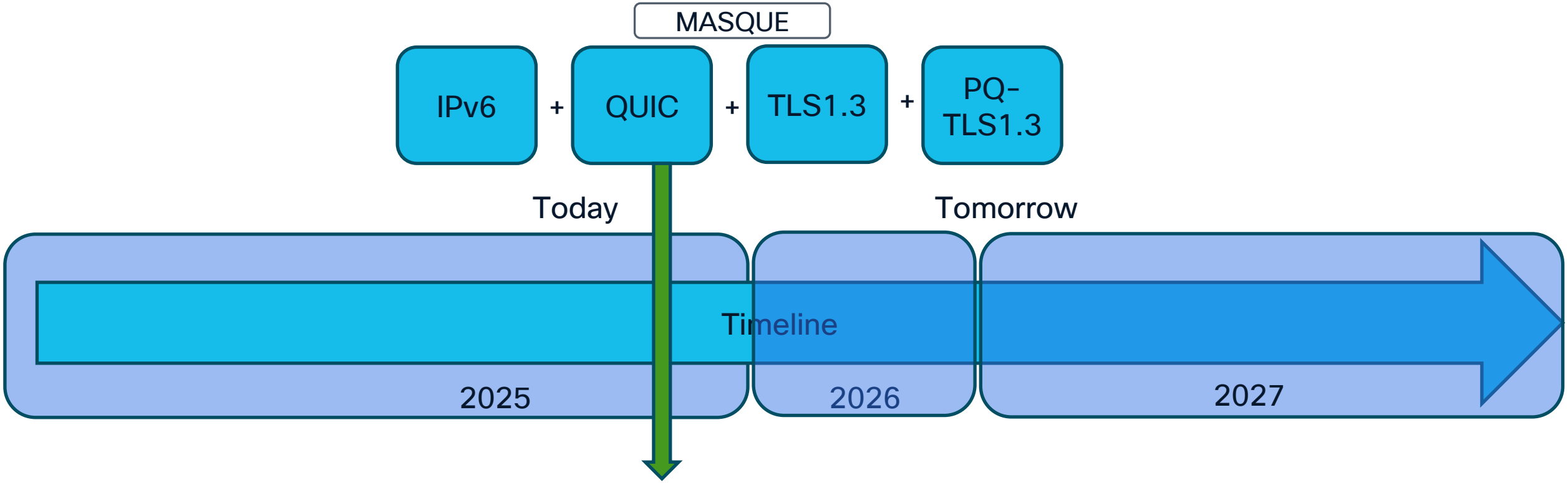
Federal Quantum Readiness Guidance

RFC 9206

RFC 9206 Issued

Guidelines on Hybrid PQC Key Establishment

Future Protocol Timeline



Browser dependent
Google already has a draft PQ-TLS1.3+QUIC implementation

CNSA 2.0 TIMELINE

2025

Transition

Adoption of CNSA 2.0 Algorithms

2027

Quantum Resistant Keys

Deployment of PQC Solutions

2029

Interoperability

Hybrid Cryptography Systems

2031

Full Migration

Complete Transition to CNSA 2.0

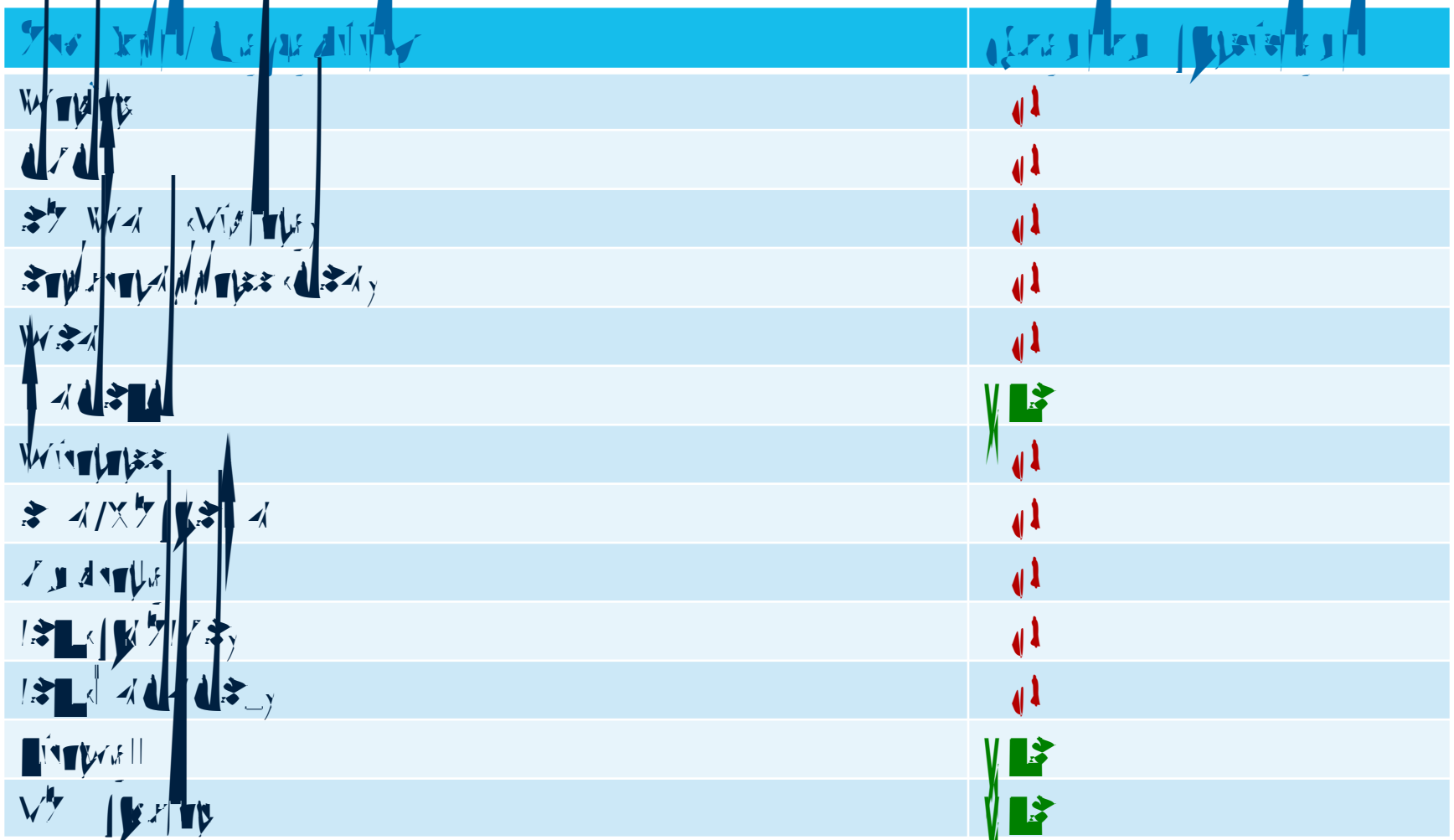
Beyond 2035

Post-Quantum Future

Advanced Quantum Technologies

Enough about time, tell me about the routers

Quantum Resistant Cisco Products



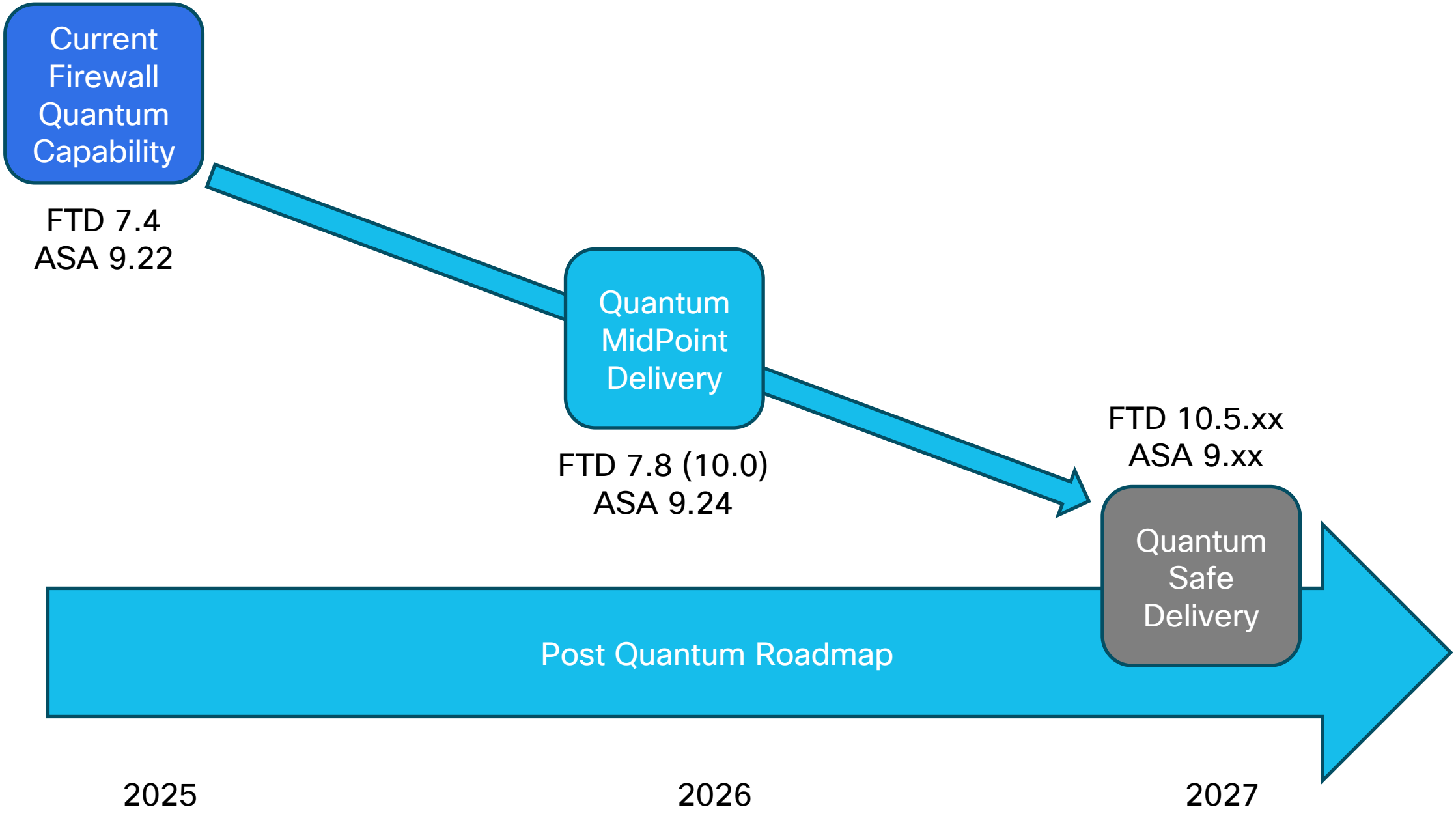
Quantum Resistant Cisco Products

Product / Capability	Quantum Resistant
Webex	NO
CUCM	NO
SD-WAN (Viptela)	NO
Secure Access (CSA)	NO
WSA	NO
MACSEC	YES
Wireless	NO
SNA/XDR/SMA	NO
Umbrella	NO
ISE (RADIUS)	NO
ISE (TACACS+)	NO
Firewall	YES
VPN Router	YES

Post-Quantum Cisco Products

Post-Quantum Cisco Products

Product / Capability	Post-Quantum
Webex	NO
CUCM	NO
SD-WAN (Viptela)	NO
Secure Access (CSA)	NO
WSA	NO
MACSEC	NO
Wireless	NO
SNA/XDR/SMA	NO
Umbrella	NO
ISE (RADIUS)	NO
ISE (TACACS+)	NO



Pre and Post Quantum Requirements

= Completed

= Underway

= Being Planned

All items are MANDATORY DELIVERY

- Support for RFC 9242+9370 for Site to Site VPN – ASA
- Support for RFC 8784+SKIP in ASA+FTD
- Support for RFC 9242+9370 for Site to Site VPN – FTD
- Support for RFC 9242+9370 for Remote Access VPN – ASA

- Support for RFC 9242+9370 for Remote Access VPN – FTD/FDM/FMC
- Support for Draft PQ-TLS 1.3 for IKEv2 Remote Access – ASA
- Support for Draft PQ-TLS 1.3 for IKEv2 Remote Access – FTD/FDM/FMC
- Support for ML-KEM-1024 for SSHv2 – ASA

- Support for ML-KEM-1024 for SSHv2 – FMC/FTD/FXOS
- Support for ML-KEM-1024 for SSHv2 – IOS-XE
- Support for Draft PQ-IKEv2 for Remote Access – ASA/FTD/FMC/FDM
- Support for TACACS+TLS1.3 Draft
  - Include PQ-TLS 1.3 as part of delivery

Currently shipping or 7.4-7.8 (10.0)

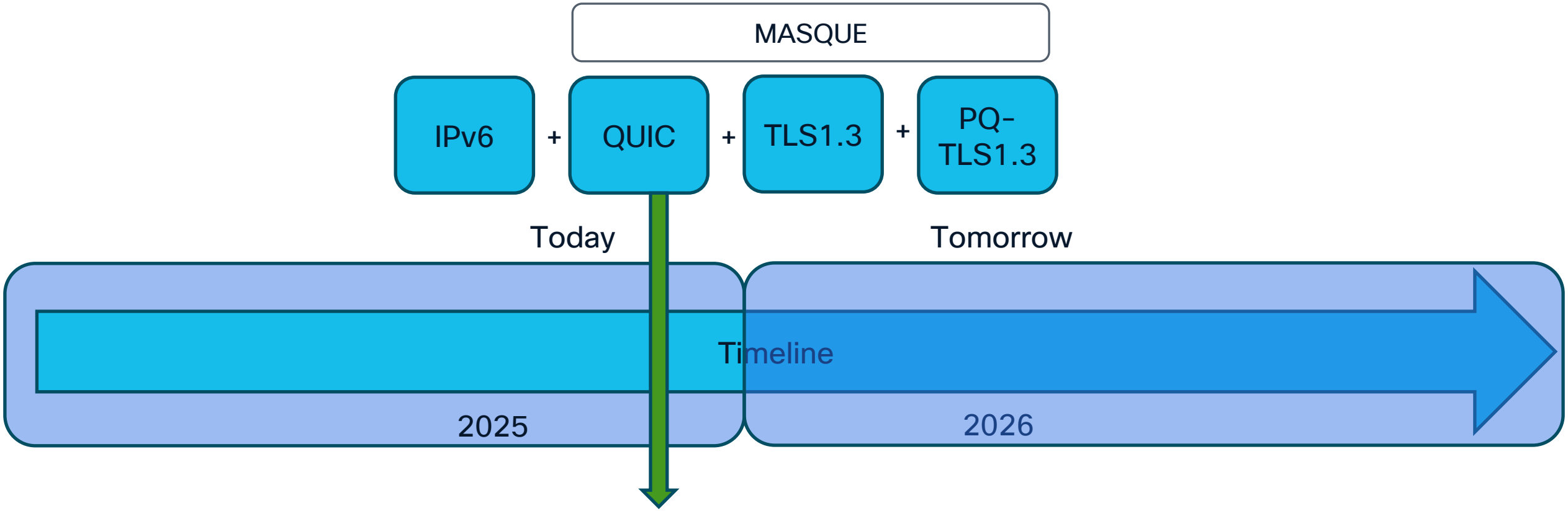
Must be committed for 10.0.10

PQ-Safe – includes SSH+TACACS+LMSS for firmware

cisco

My prediction for future protocols

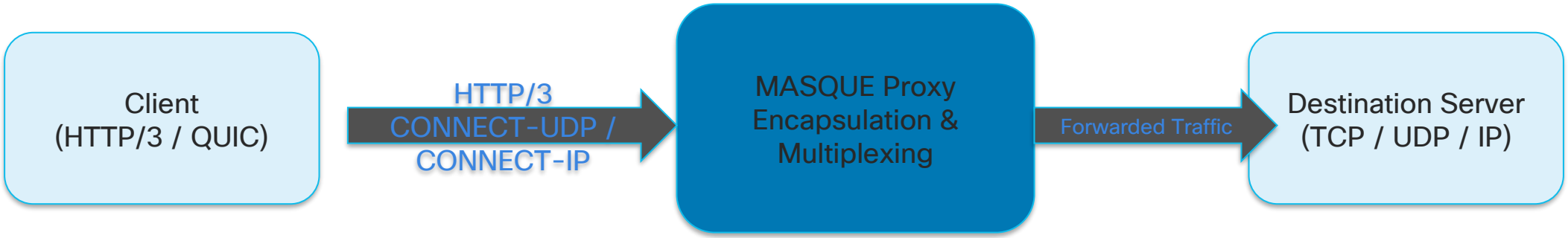
Future Protocol Timeline



Browser dependent
Google already has a draft PQ-TLS1.3+QUIC implementation

What is MASQUE you ask?

MASQUE Protocol Overview

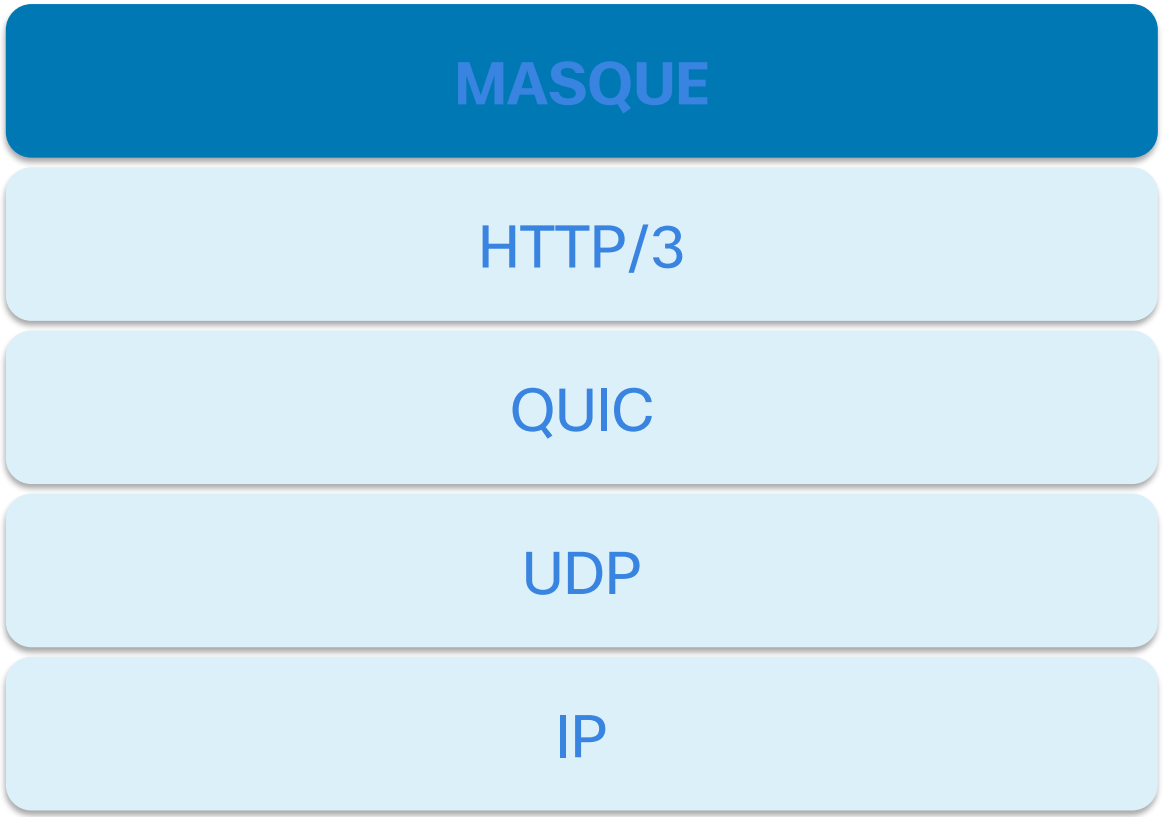


Key MASQUE Capabilities:

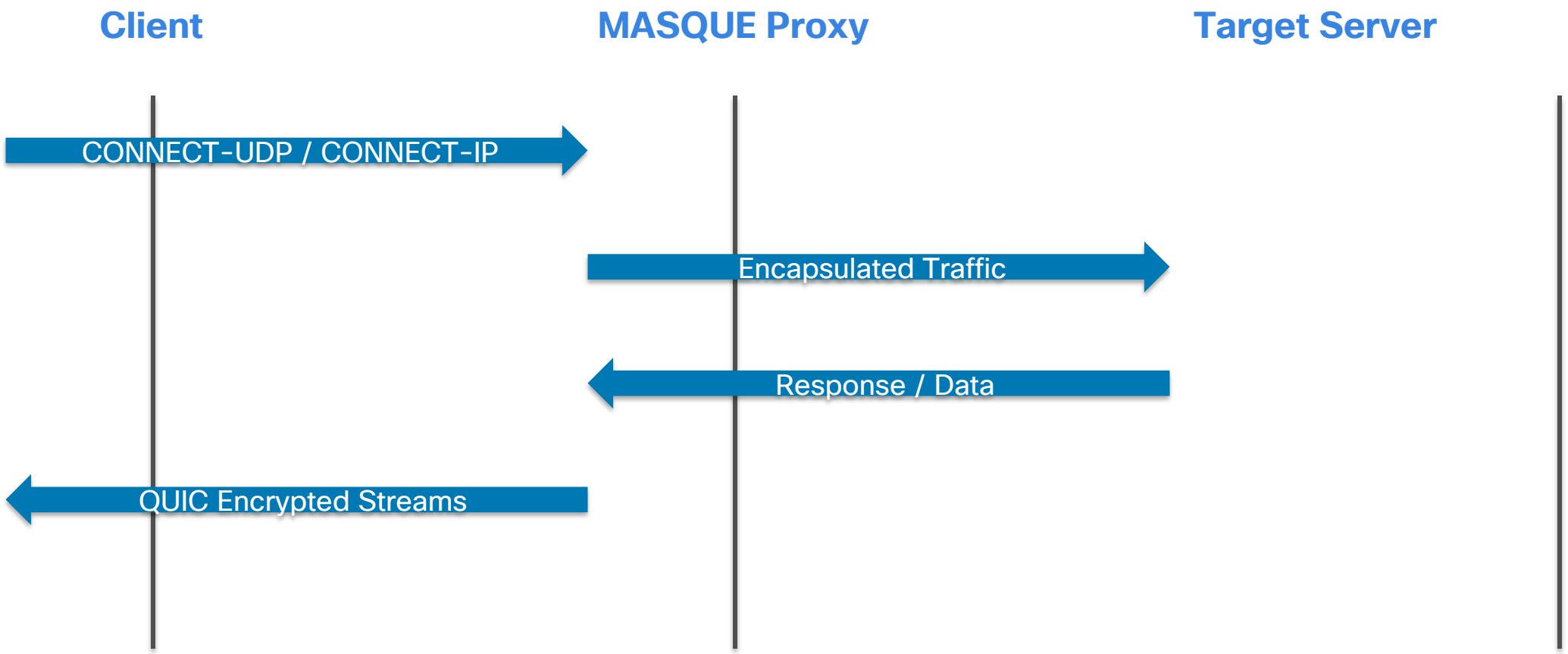
Tunnels arbitrary UDP, IP, and TCP over HTTP/3
Uses QUIC encryption and multiplexing
Supports VPN-like and proxy use cases
Improves performance and NAT traversal
Foundation for privacy and modern secure transport overlays

MASQUE Layered Protocol Stack

Application Tunneling Layer

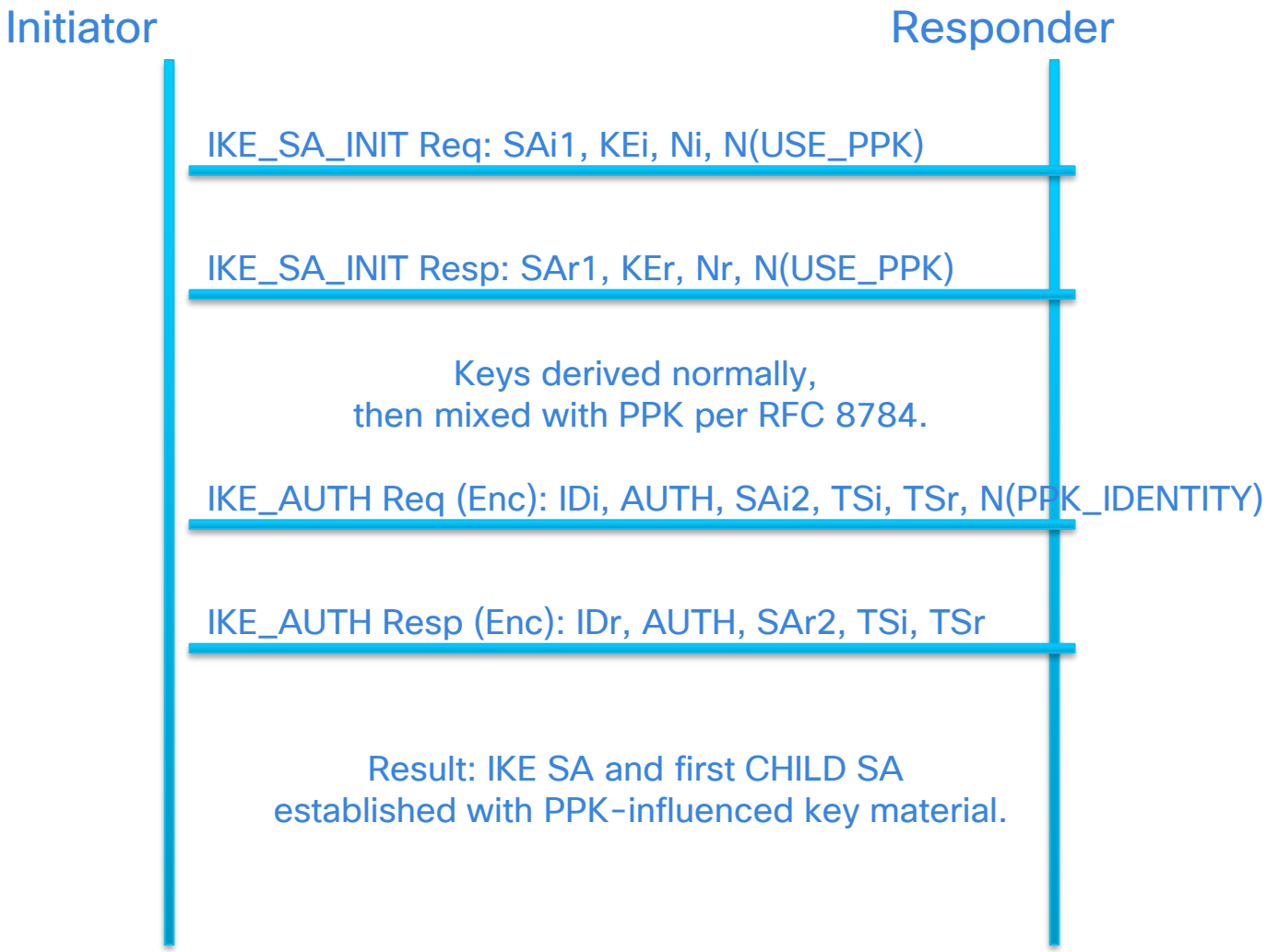


MASQUE Message Flow (Ladder Diagram)



Quantum Resistance

IKEv2 Exchange with PPK (RFC 8784)



Post-Quantum Roadmap

Post Quantum Strategic Plan

Crawl – Walk – Run Quantum Roadmap

Crawl

- Target early Quantum Resistant Solutions
- Leverage RFC 8784 for IKEv2/IPSEC
- Leverage MACSEC capabilities today
- SKIP Implementation mandatory for IPSec and MACSEC

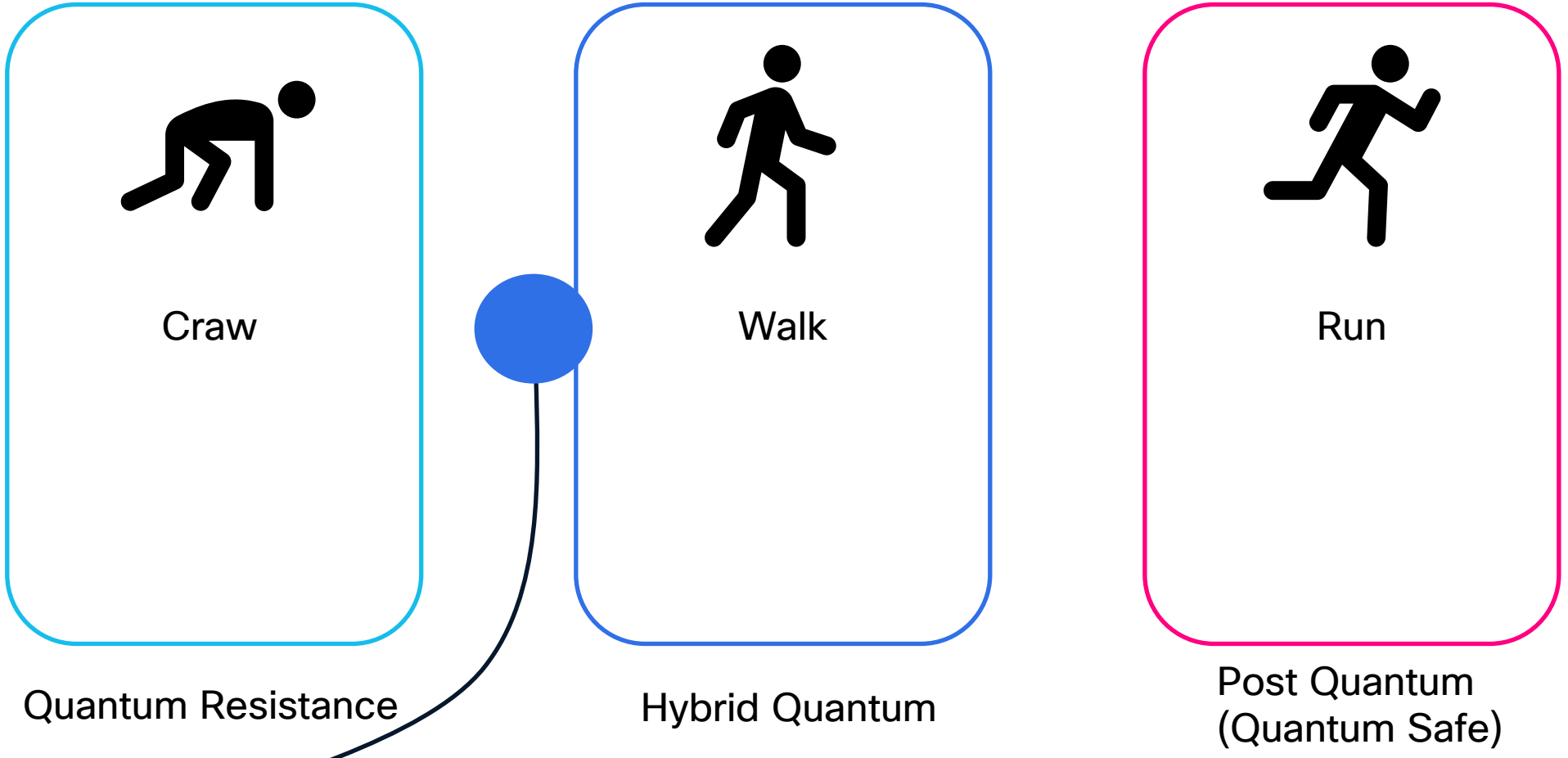
Walk

- Transition to early Post-Quantum
- All platforms must implement TLS 1.3
- FIPS-203 ML-KEM support in all platforms
- RFC 9242+9370 for IKEv2/IPSec
- Cisco SD-WAN (Viptela) to leverage TLS 1.3 + PQ

Run

- Full support for native Post-Quantum Cryptography
- All SSHv2 must use ML-KEM 1024
- Implement PQA into RADIUS, TACACS+, TLS1.3
- MACSEC MKA pre-standard work

Cisco Quantum Roadmap



Security Specific Tasks

Crawl

- Implement SKIP for ASA+FTD Builds
- Fully instrument RFC 8784_SKIP in ASDM, CLI, FDM, FMC

Walk

- Uplift all platforms to support CiscoSSL 8.3+
- Implement RFC 9370 in all products that support IPSec
- Fully instrument the above in ASDM, FDM, FMC, CLI

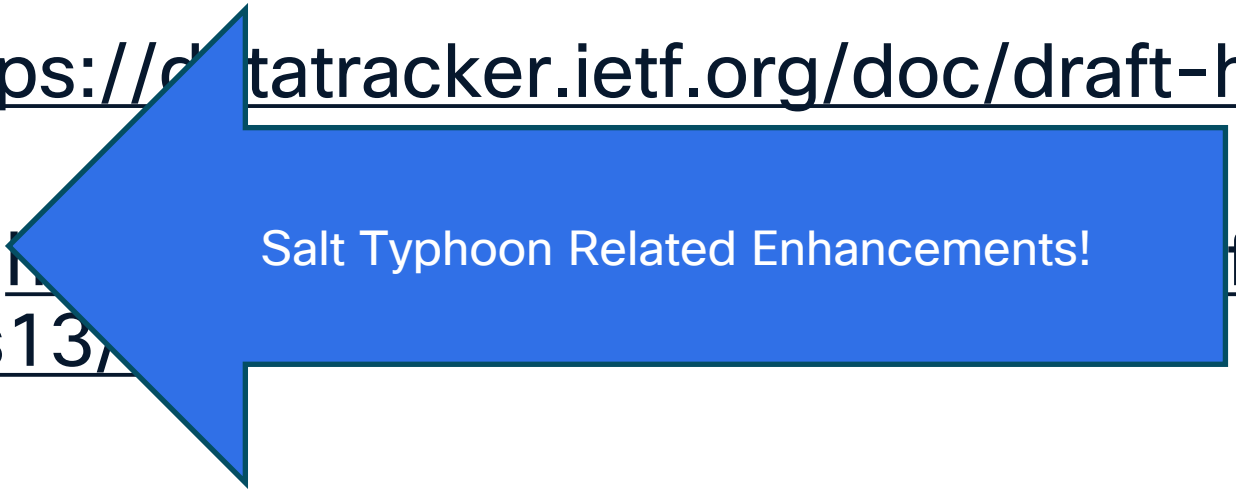
Run

- Post-Quantum Algorithm Support across all platforms for IKEv2, TLS1.3, SSH
- Target PQA for RADIUS, TACACS+

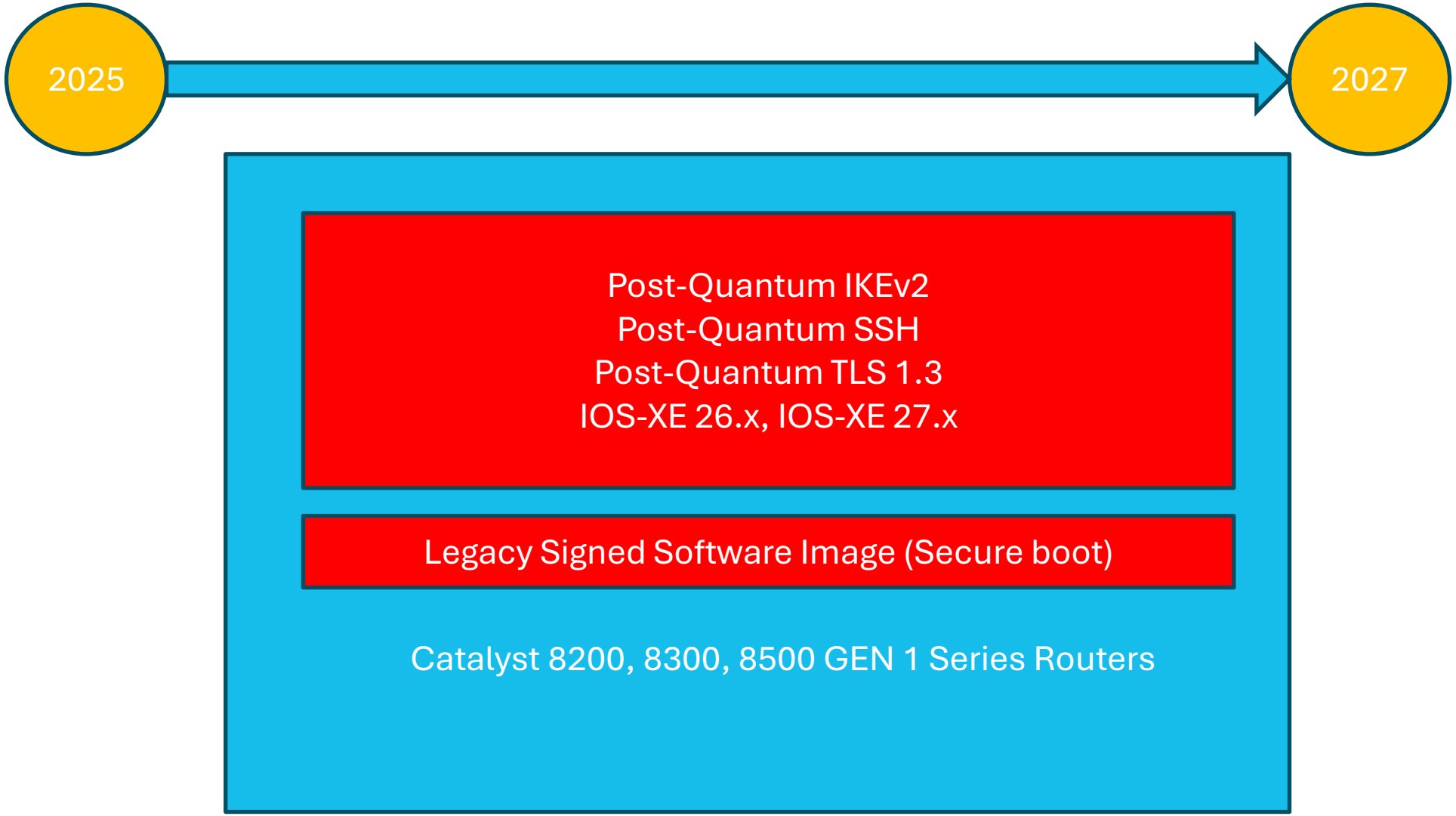
Post-Quantum Roadmap for IOS-XE

Supporting IETF RFCs

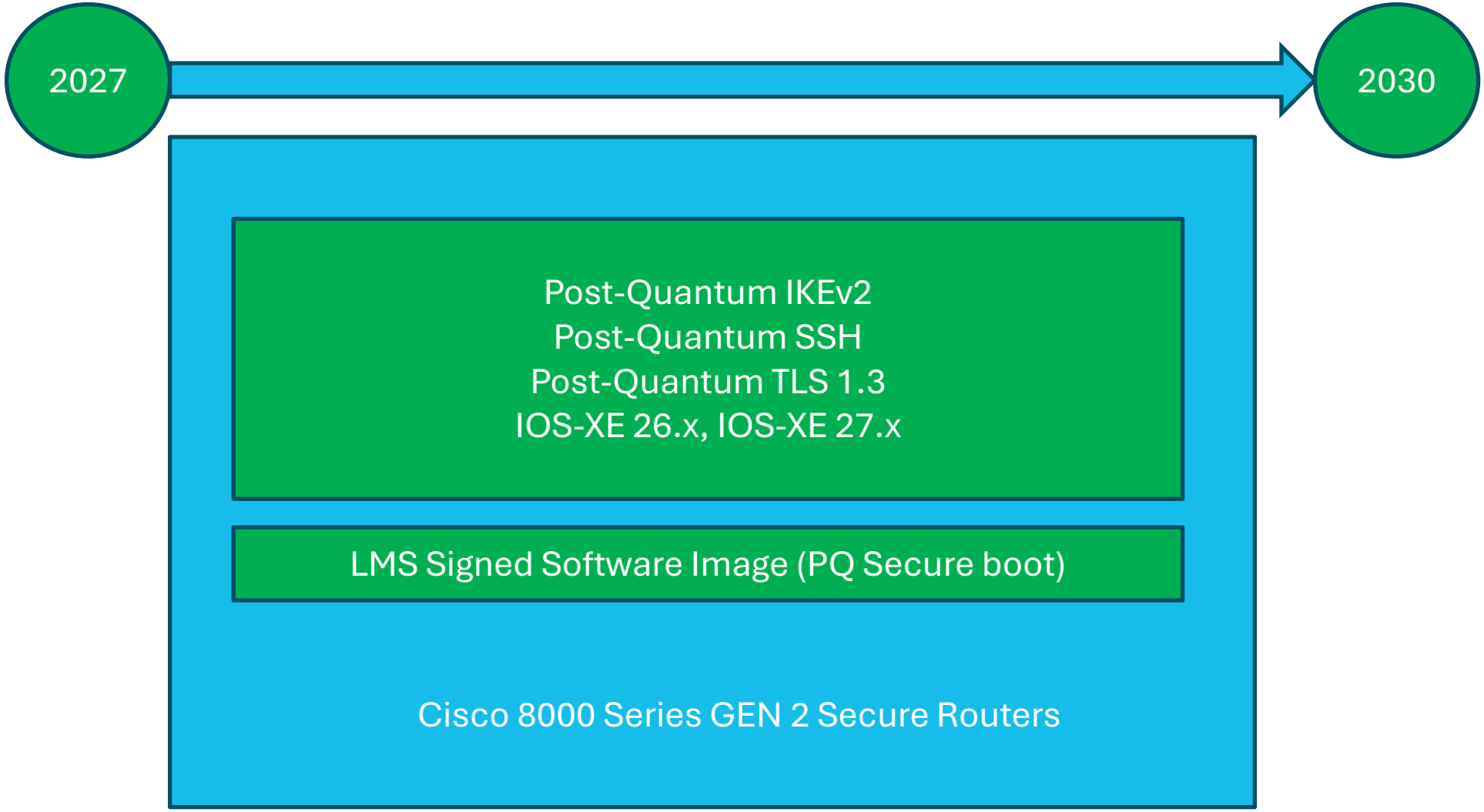
- IPSEC: https://datatracker.ietf.org/doc/draft-guthrie-cnsa2-ipsec-profile/
- TLS: https://datatracker.ietf.org/doc/draft-becker-cnsa2-tls-profile/01/
- SSH: https://datatracker.ietf.org/doc/draft-becker-cnsa2-ssh-profile/
- ML-KEM SSH - https://datatracker.ietf.org/doc/draft-harrison-mlkem-ssh/
- TACACS+TLS13 - https://datatracker.ietf.org/doc/draft-ietf-opsawg-tacacs-tls13/

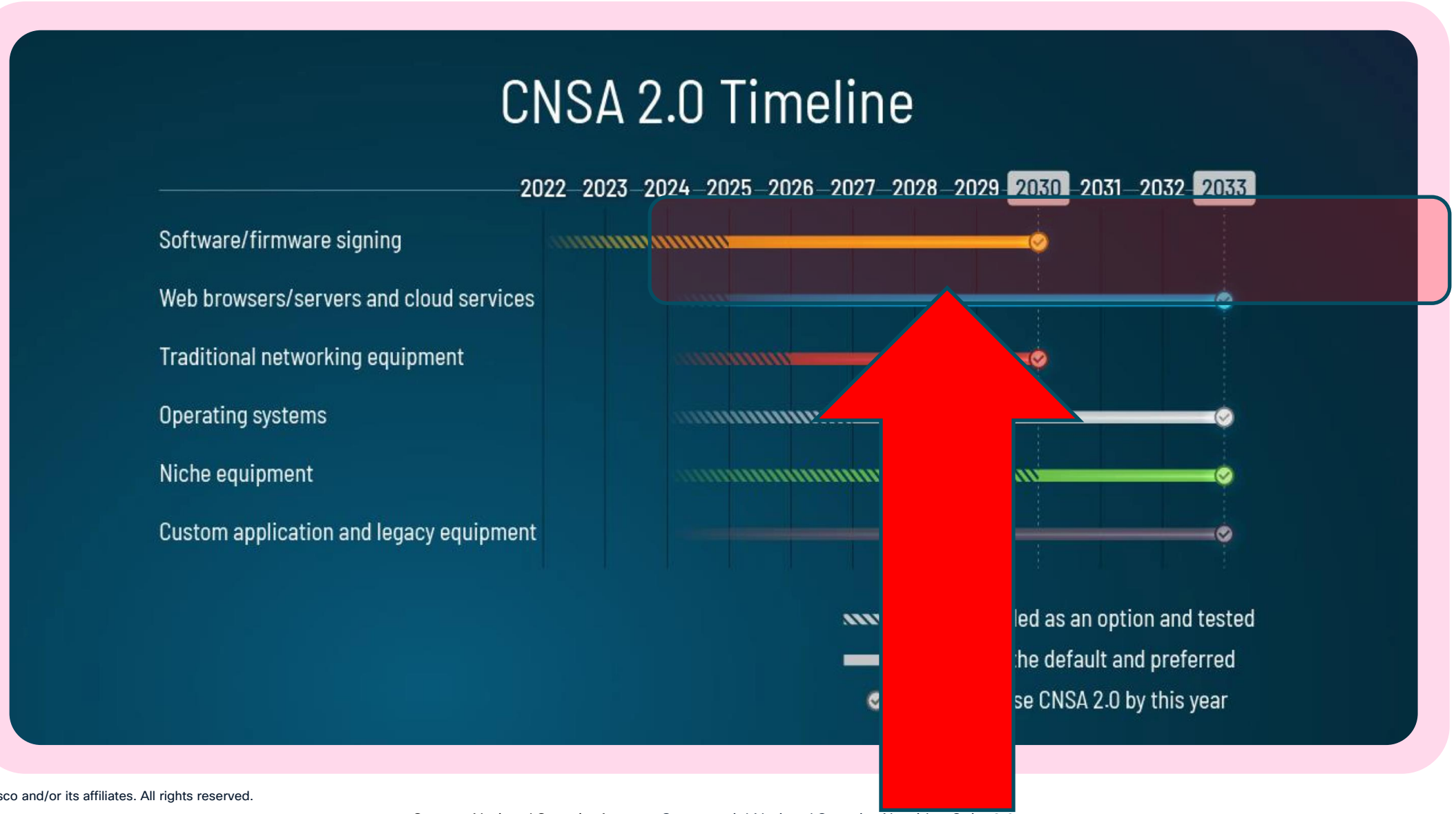


No Post Quantum in Gen 1 Routers



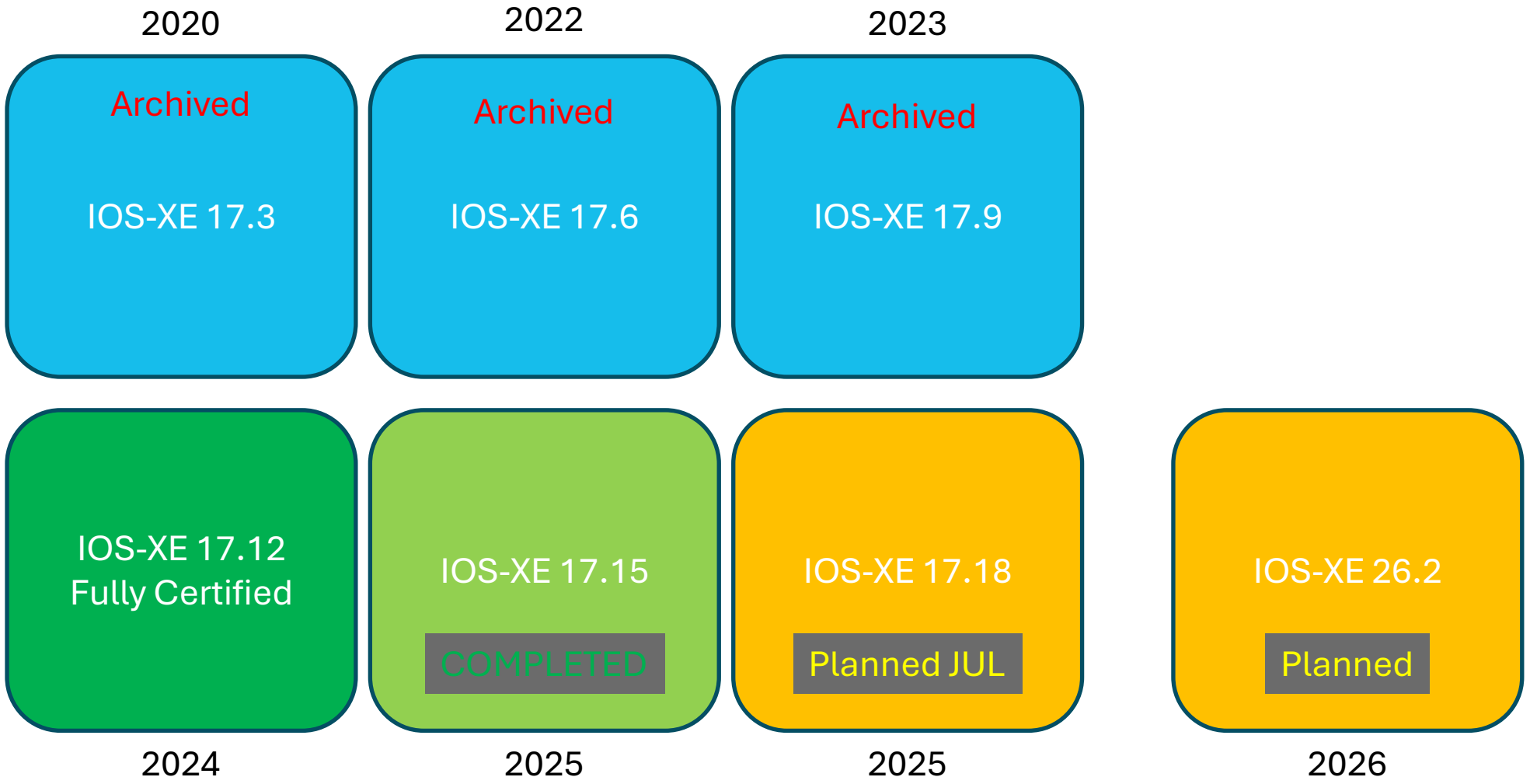
Post Quantum in Gen 2 Routers

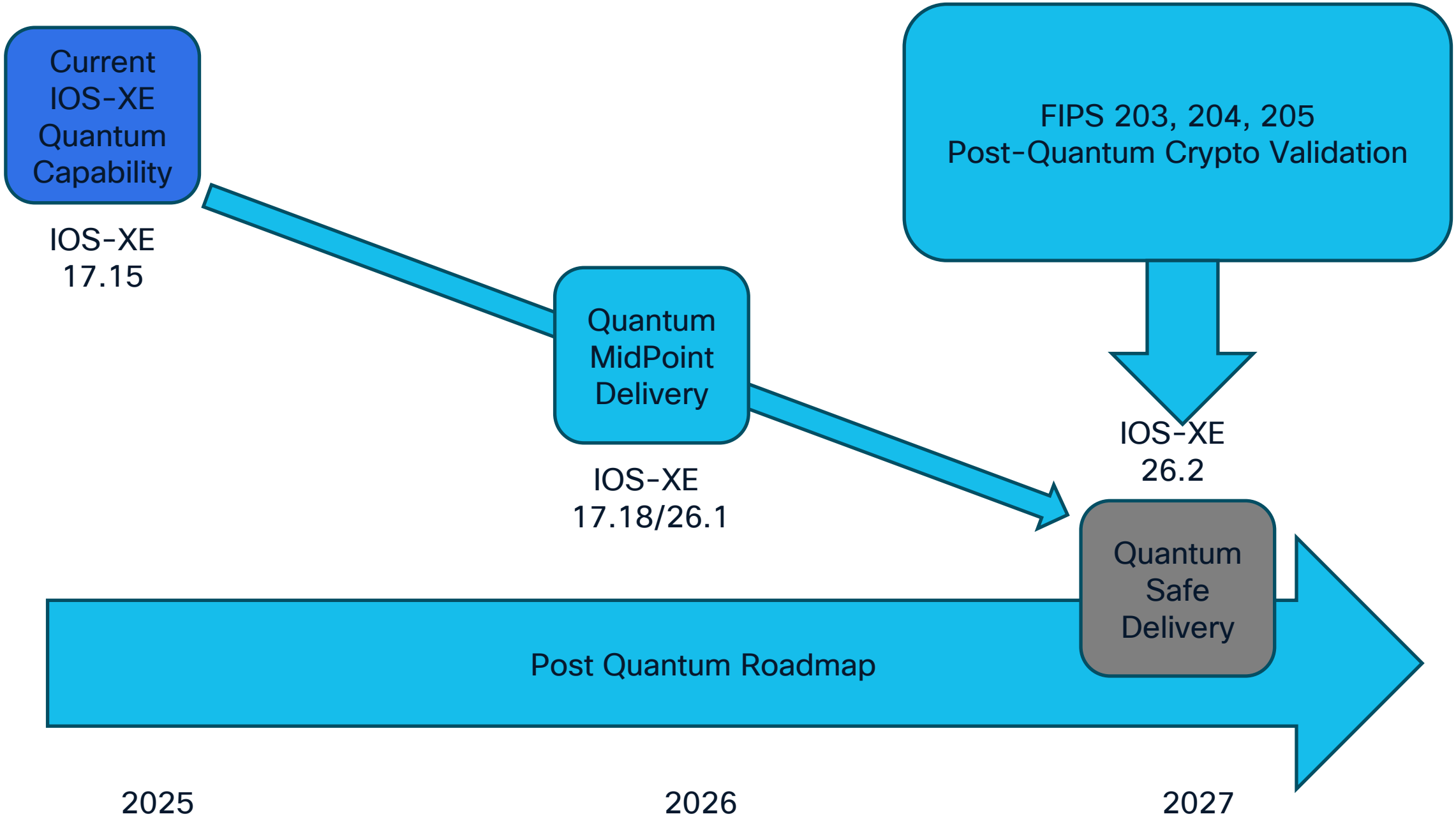


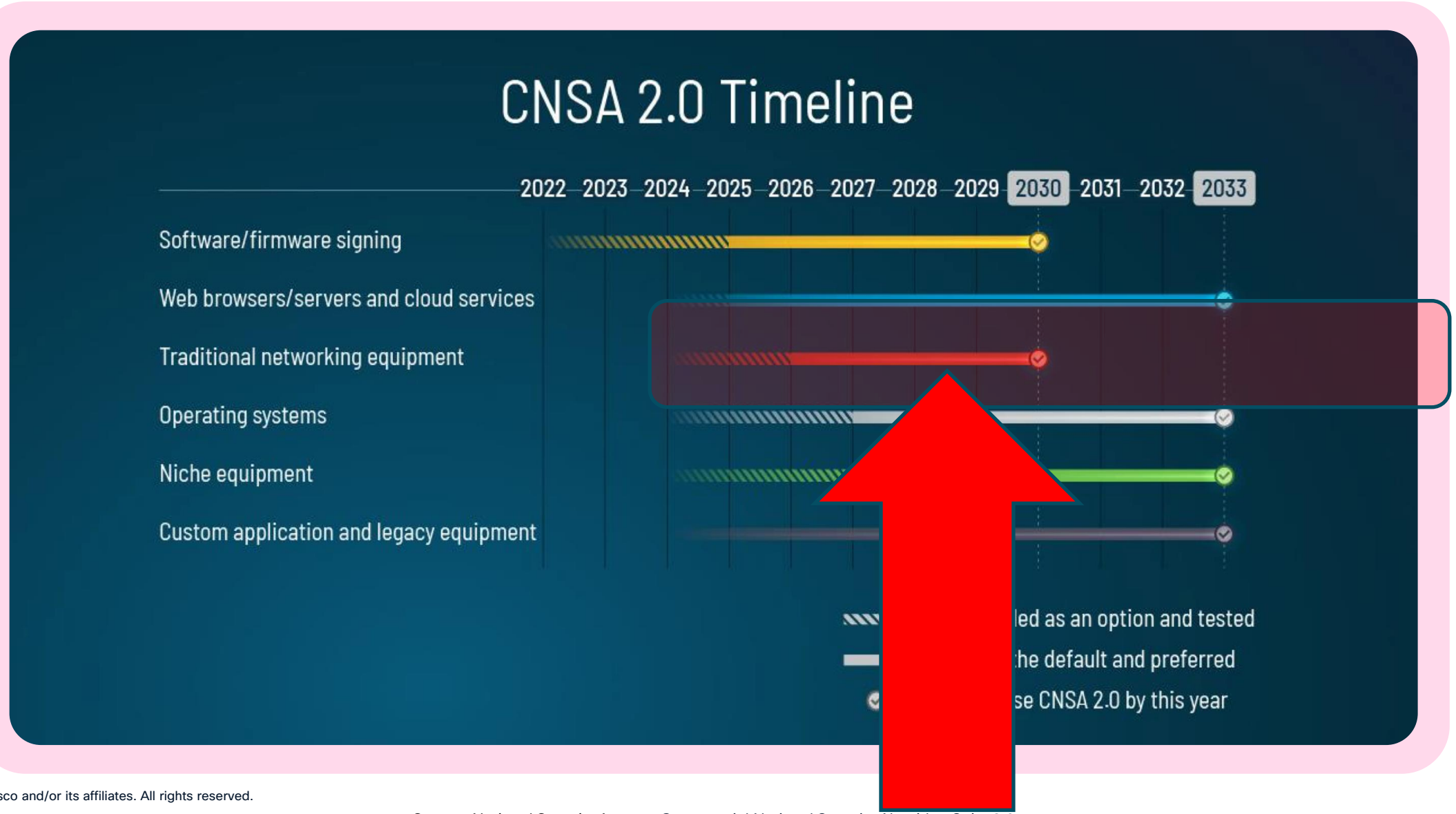


Source: National Security Agency, *Commercial National Security Algorithm Suite 2.0*

Constant Certification of IOS-XE





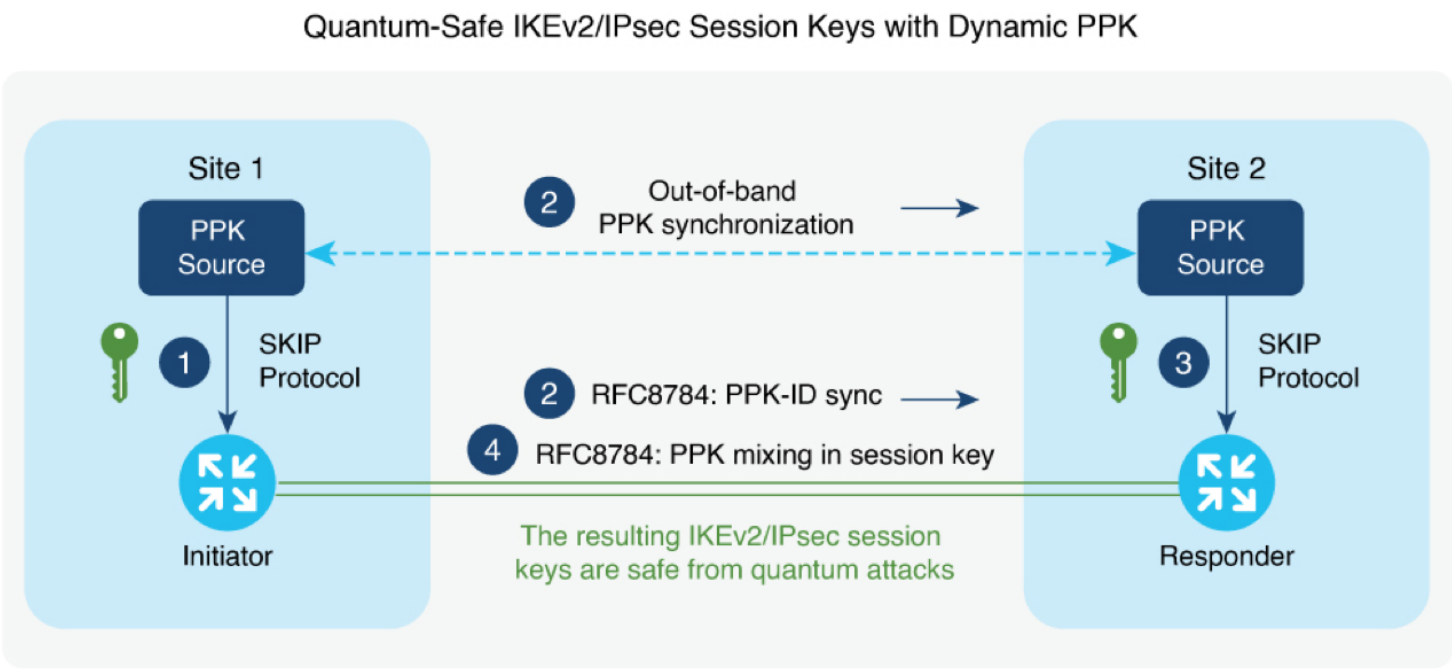


Source: National Security Agency, *Commercial National Security Algorithm Suite 2.0*

Quantum Key Distribution (QKD)

Quantum Key Distribution

- Today, Cisco supports SKIP in IOS-XE but no Security products
- https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.pdf



IETF Draft Submission for SKIP

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 7 March 2026

R. Singh, Ed.
C. Hill
Cisco Systems, Inc.
S. Kawaguchi
J. Lupo
QuSecure, Inc.
3 September 2025

Secure Key Integration Protocol (SKIP)
draft-cisco-skip-02

Abstract

This document specifies the Secure Key Integration Protocol (SKIP), a two-party protocol that allows a client to securely obtain a key from an independent Key Provider. SKIP enables network and security operators to provide quantum-resistant keys suitable for use with quantum-resistant cryptographic algorithms such as AES-256. It can also be used to provide an additional layer of security to an already quantum-resistant secure channel protocol for a defense-in-depth strategy, and/or enforce key management policies.

SKIP Info : https://datatracker.ietf.org/doc/html/draft-cisco-skip-02

Post-Quantum Encryption Solutions @Cisco...

What is real?

Foundation to Quantum Safe Network Encryption

IPSec / MACsec Support: IKEv2 and MKA extensions for quantum-resistant deployments (RFC 8784, MKA / EAP-TLS)

Management Plane Support: PQ TLS 1.3 using ML-KEM (SSH, TACACS), MACsec EAP-TLS 1.3, PQ SSH using IETF standard (PQC for TLS/SSH)

3rd Party Key Source Support: Secure Key Integration Protocol (SKIP) offers ability for network elements to leverage 3rd party Quantum Resistant key sources

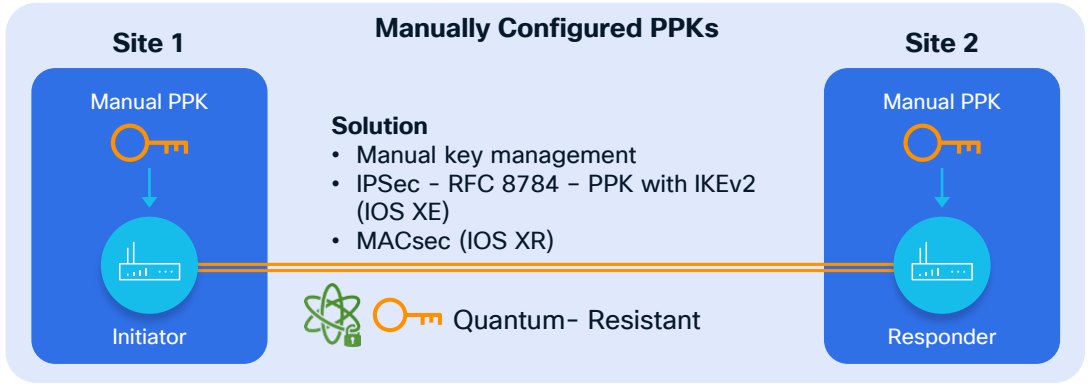
Integrate Evolving Open Standards: Open standards for existing protocols (IETF) and hybrid, encryption ciphers (NIST), Govt Guidelines (ASD / CNSA 2.0)

Quantum Resistant Solutions for IPSec & MACsec

Current Technology and Deployment Options

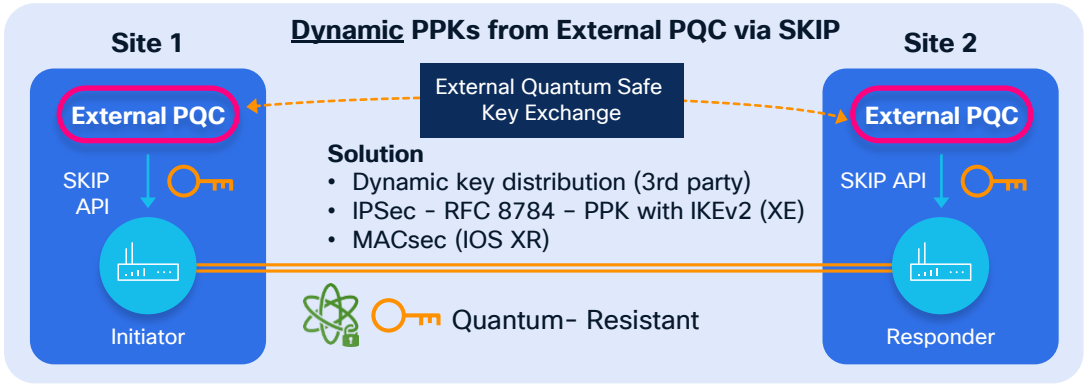
Quantum-Safe Encryption Options – Available Today

Manual Options



- Manual post-quantum pre-shared key mgmt.
- IPSec: Uses IKEv2 (IOS XE)
- MACsec (802.1AE): MKA extensions (IOS XR)

Dynamic Options



- PPK distribution through 3rd-party key source
- Secure Key Integration Protocol (SKIP) enabler
- Applies to HW or SW based key sources

Why it Matters: Begin early Post-quantum resistant implementations for the network (early mission-critical areas). Targets existing HNDL threats.

PPK = Postquantum Preshared Keys

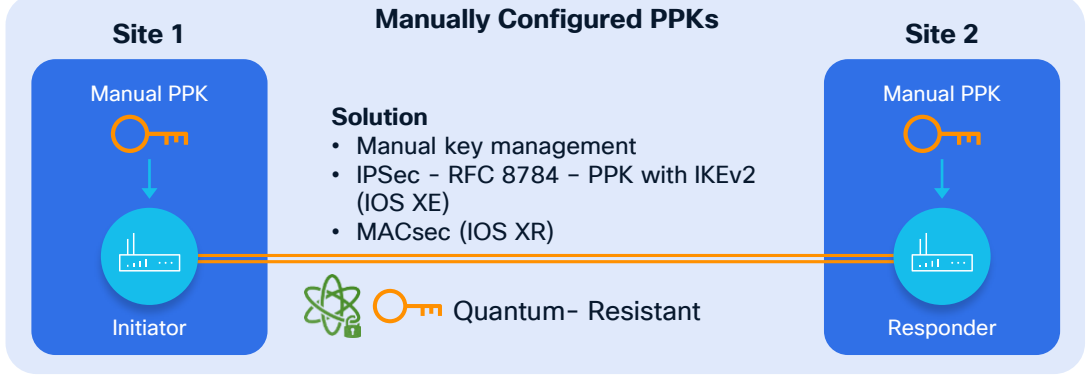
HNDL = Harvest Now, Decrypt Later

cisco

Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

Manual Options



Dynamic Options

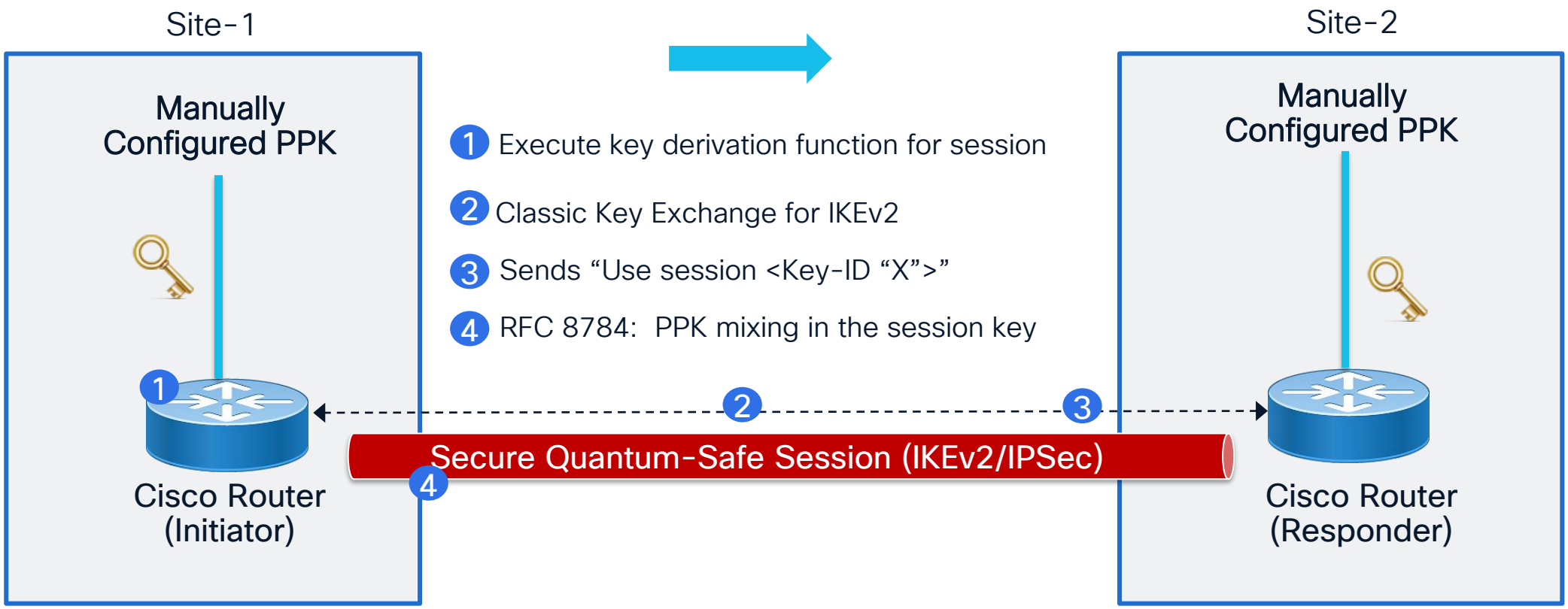
Dynamic Network Encryption Options:

- **IPSec:** RFC 8784 - PPK based IPsec encryption keys
- **MACsec:** PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

RFC 8784 with Quantum-Safe IKEv2/IPSec Session

Manual – Mixing Post-Quantum Pre-Shared Keys (PPK) in IKEv2 for Post-Quantum Security

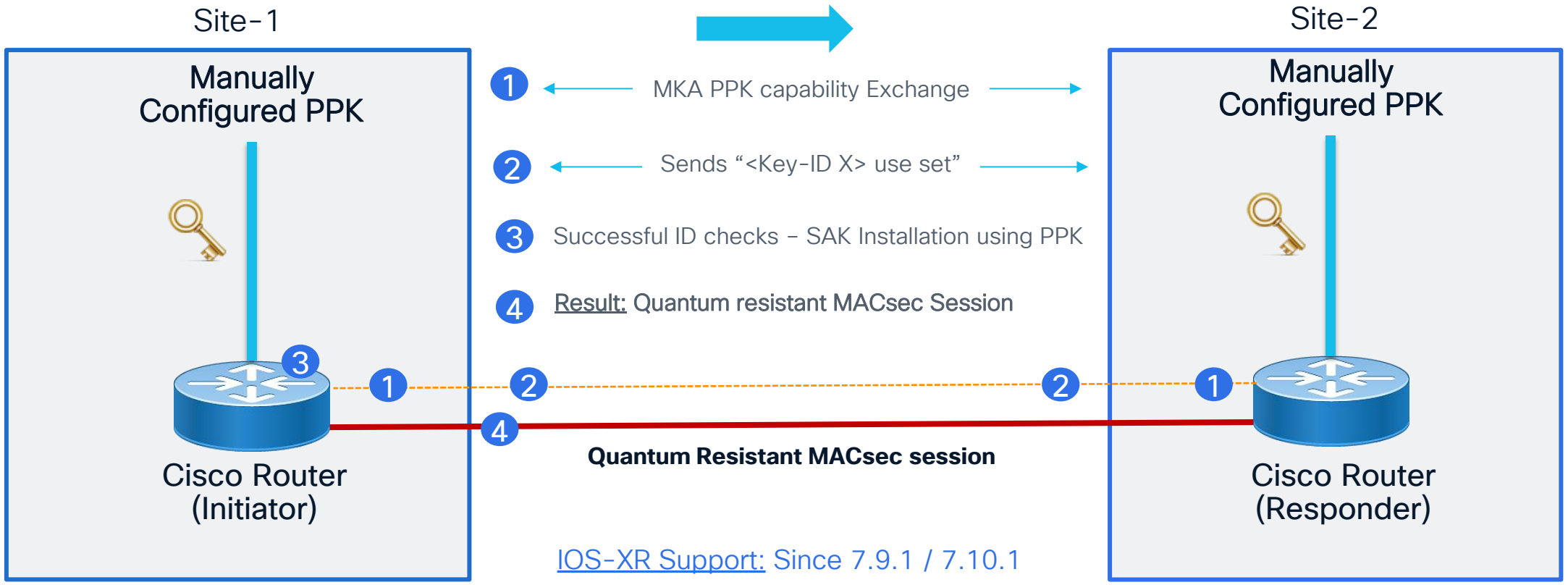


PQ PPK mix with DH is never transmitted over the wire (RFC 8784)

IOS-XE Support: Since 17.11.1a

Quantum-Safe MACsec with Preshared Keys

Example - Manual PPK for MACsec



- **Extensions to MKA are applied** to carry the PPK_ID as the SAK identifier (instead of the secret HW key)

NOTE: MACsec with symmetric keys not as vulnerable to quantum threats as asymmetric encryption (i.e. they do not leverage the same mathematical problems that are vulnerable to asymmetric keys)

“Bring your own key server… “

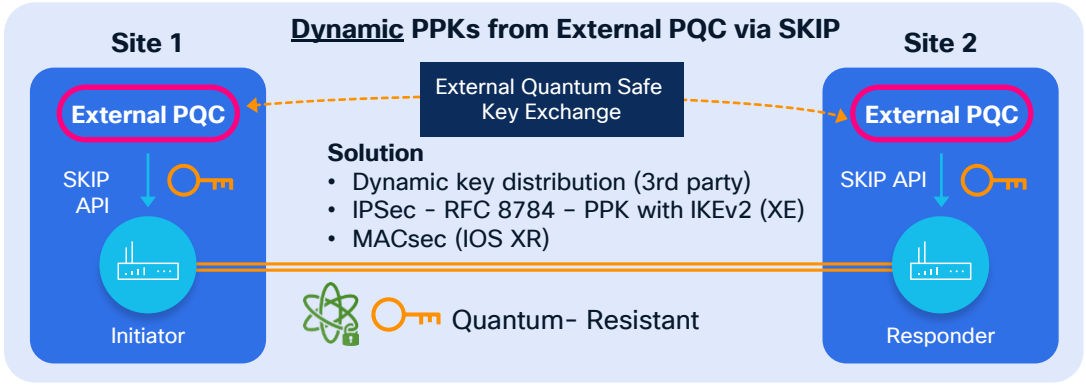
How To Import Post Quantum Keys to Cisco Devices via 3rd Party Key Sources

Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

Manual Options

Dynamic Options



- Dynamic quantum-safe key generation
- Automated key management
- Automated key refresh, entropy

Dynamic Network Encryption Options:

- **IPSec:** RFC 8784 – PPK based IPsec encryption keys
- **MACsec:** PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

Early IETF Draft Submission for SKIP

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 7 March 2026

R. Singh, Ed.
C. Hill
Cisco Systems, Inc.
S. Kawaguchi
J. Lupo
QuSecure, Inc.
3 September 2025

Secure Key Integration Protocol (SKIP)
draft-cisco-skip-02

Abstract

This document specifies the Secure Key Integration Protocol (SKIP), a two-party protocol that allows a client to securely obtain a key from an independent Key Provider. SKIP enables network and security operators to provide quantum-resistant keys suitable for use with quantum-resistant cryptographic algorithms such as AES-256. It can also be used to provide an additional layer of security to an already quantum-resistant secure channel protocol for a defense-in-depth strategy, and/or enforce key management policies.

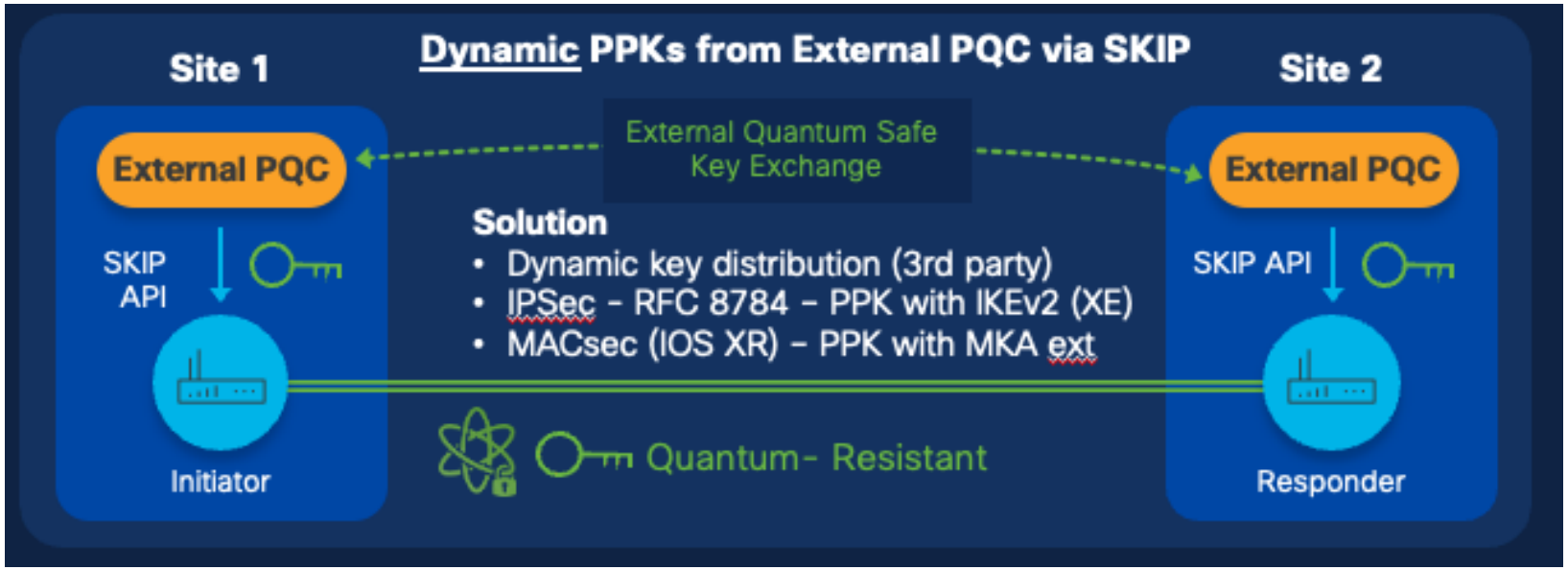
SKIP Info : https://datatracker.ietf.org/doc/html/draft-cisco-skip-02

Cisco Secure Key Integration Protocol (SKIP)

Leverage Existing Encryption with Post Quantum Security Methods

- Cisco developed the Secure Key Integration Protocol (SKIP) for 3rd party PQ key integration
- SKIP is a QR client/server framework (TLS 1.2 with PSK-DHE cipher suite

Why It Matters: SKIP allows 3rd-party "external" key vendors to distribute PQC keys to Cisco devices (PQC, QKD)



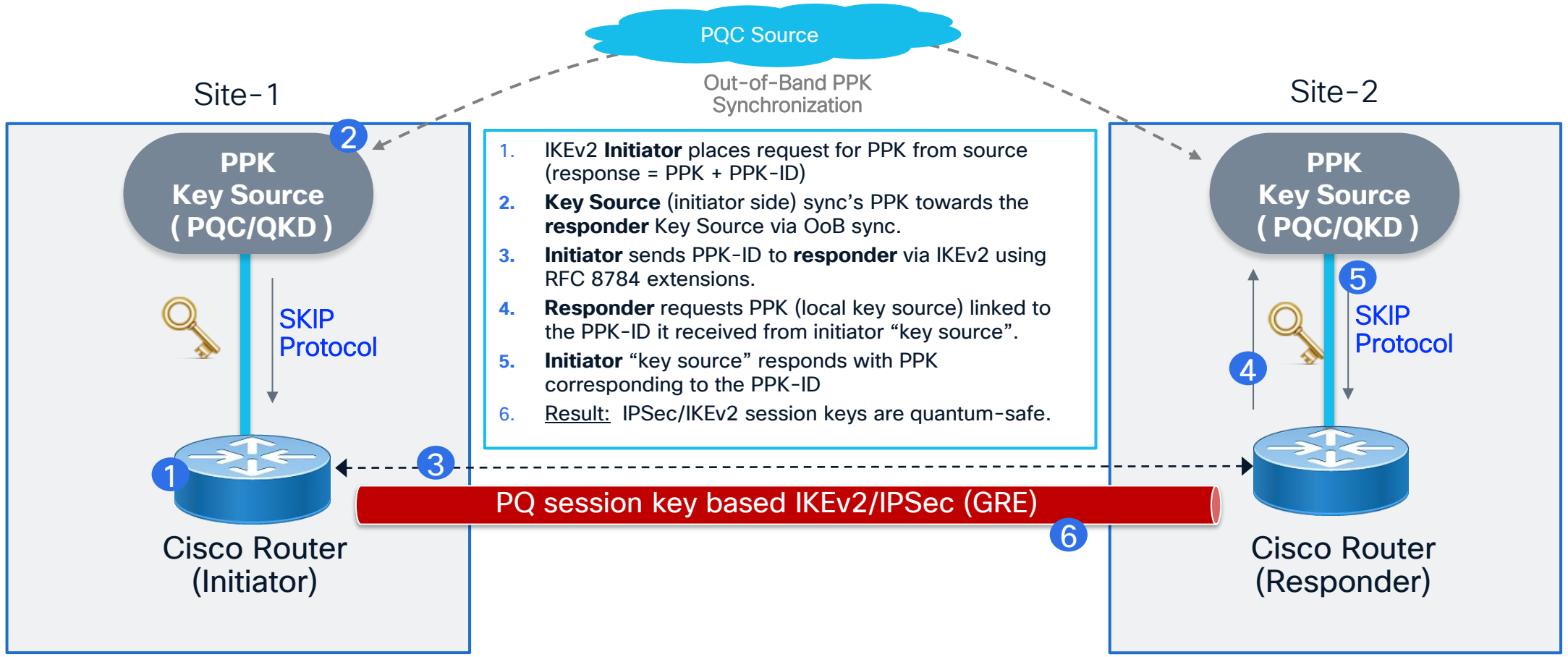
SKIP Info : https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html

Dynamic PPK with SKIP

IPSec/IKEv2
MACsec

RFC 8784 with Quantum-Safe IKEv2/IPSec Session

Dynamic PPK Example with SKIP



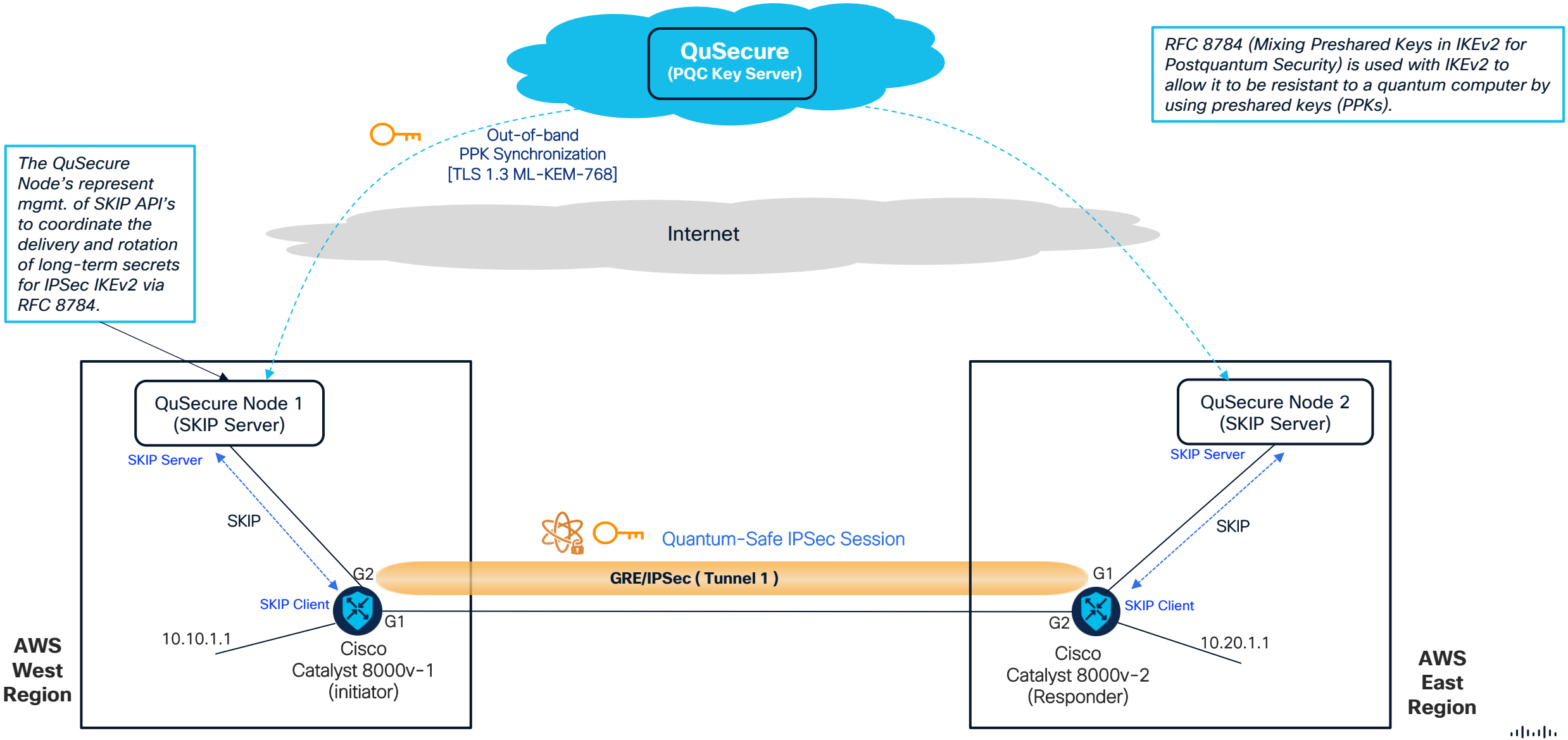
- PPK is never sent over the wire
- Only the PPK-ID is sent and over the OoB channel
- PPK Key Source is responsible for synchronization between both key sources
- SKIP protocol used between key source and routers

PPK = Postquantum Preshared Keys

IPSec/IKEv2 Quantum Safe Demo Using Dynamic PQ Preshared Keys

QuSecure

Demo: Cisco IOS-XE Catalyst 8000v using SKIP with 3rd Prty PQC (QuSecure)



cisco

SHOW Output

```
Cat8Kv_CPN_Ohio#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA


Tunnel-id Local                 Remote                fvrf/ivrf            Status
2         10.0.0.2/500          10.0.0.1/500          none/none            READY
      Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:20, Auth sign: PSK, Auth verify: PSK, QR
      Life/Active Time: 86400/2652 sec
      CE id: 0, Session-id: 44
      Local spi: CF0314EA311AF64A       Remote spi: 3052A8276D7F6FE8
      Status Description: Negotiation done
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      <<<<< Some output removed for brevity >>>>>
            Quantum-safe Encryption using Dynamic PPK
      Local Sys Id: Cat8Kv_CPN_Ohio  Remote Sys Id: Cat8Kv_CPN_Ashburn
      PEER TYPE: Other
```

Shows "Quantum Resistant"

Shows "Dynamic" PPK from External key source that is "quantum resistant" enabled

White Paper

Cisco Post-Quantum Demonstration w/ QuSecure

Engineering Quantum Resistance: An IPsec Case Study

Craig Hill[1], Scott Kawaguchi[2], and Joey Lupo[3]

[1]Distinguished Architect, Cisco Systems, Inc.
[2]Chief Architect, QuSecure, Inc.
[3]Product Security Architect, QuSecure, Inc.

Abstract

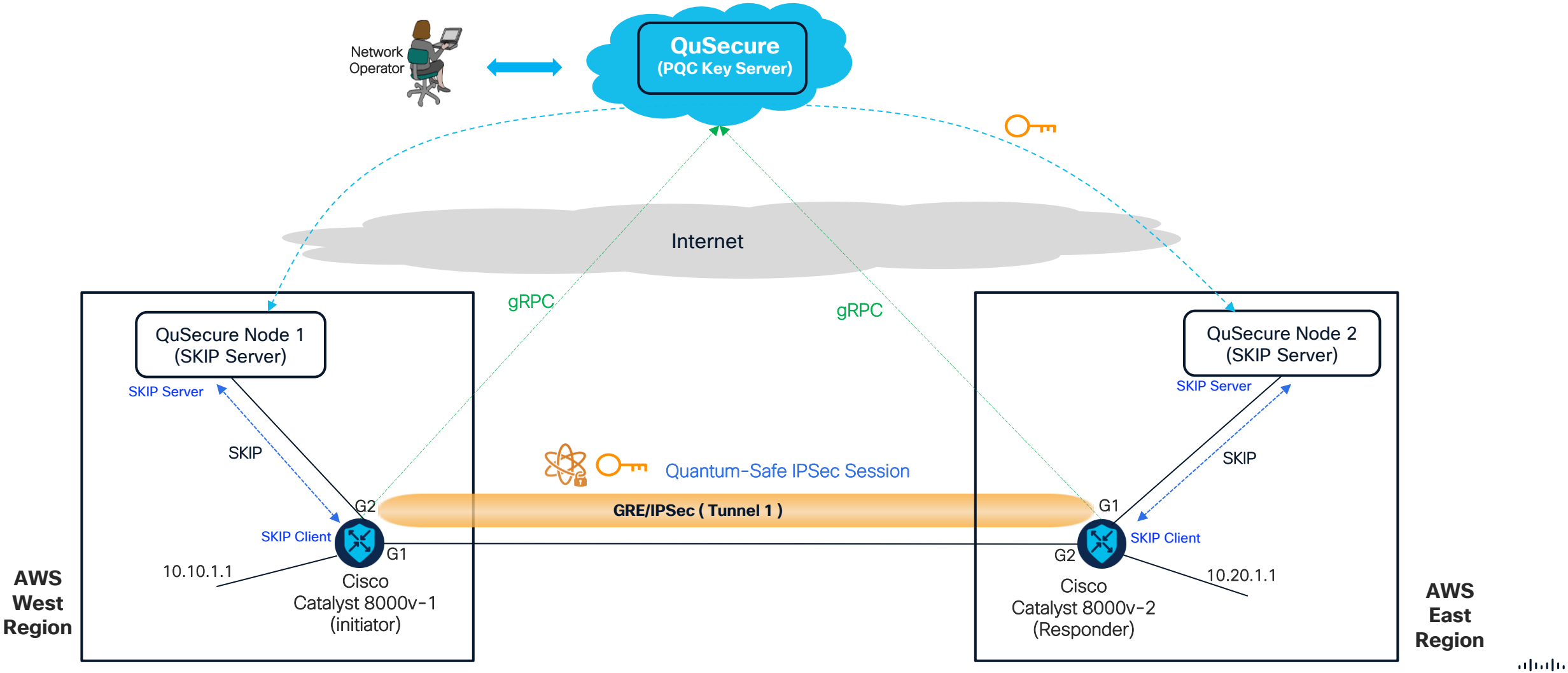
The urgency to meet the quantum threat to digital communications continues to intensify for organizations across the public and private sectors. Upgrading entire networks and applications to quantum resistance promises to be a monumental undertaking for all parties involved. The purpose of this paper is to highlight key principles for achieving quantum resistance in a timely and practical fashion. In particular, a migration strategy that emphasizes interoperability with existing protocols and systems can ease the burden on IT teams, minimize disruptions, limit infrastructure turnover, and improve security outcomes. We outline a solution blueprint for upgrading IPsec virtual private networks to quantum resistance that exemplifies this approach. Finally, we describe how Cisco and QuSecure recently demonstrated a proof-of-concept of this solution blueprint.

Link to Paper: https://www.qusecure.com/resources/ipsec-case-study-with-cisco-core-networking/

IPSec/IKEv2 Quantum Safe Demo Using Dynamic PQ Pre-shared Keys

QuSecure

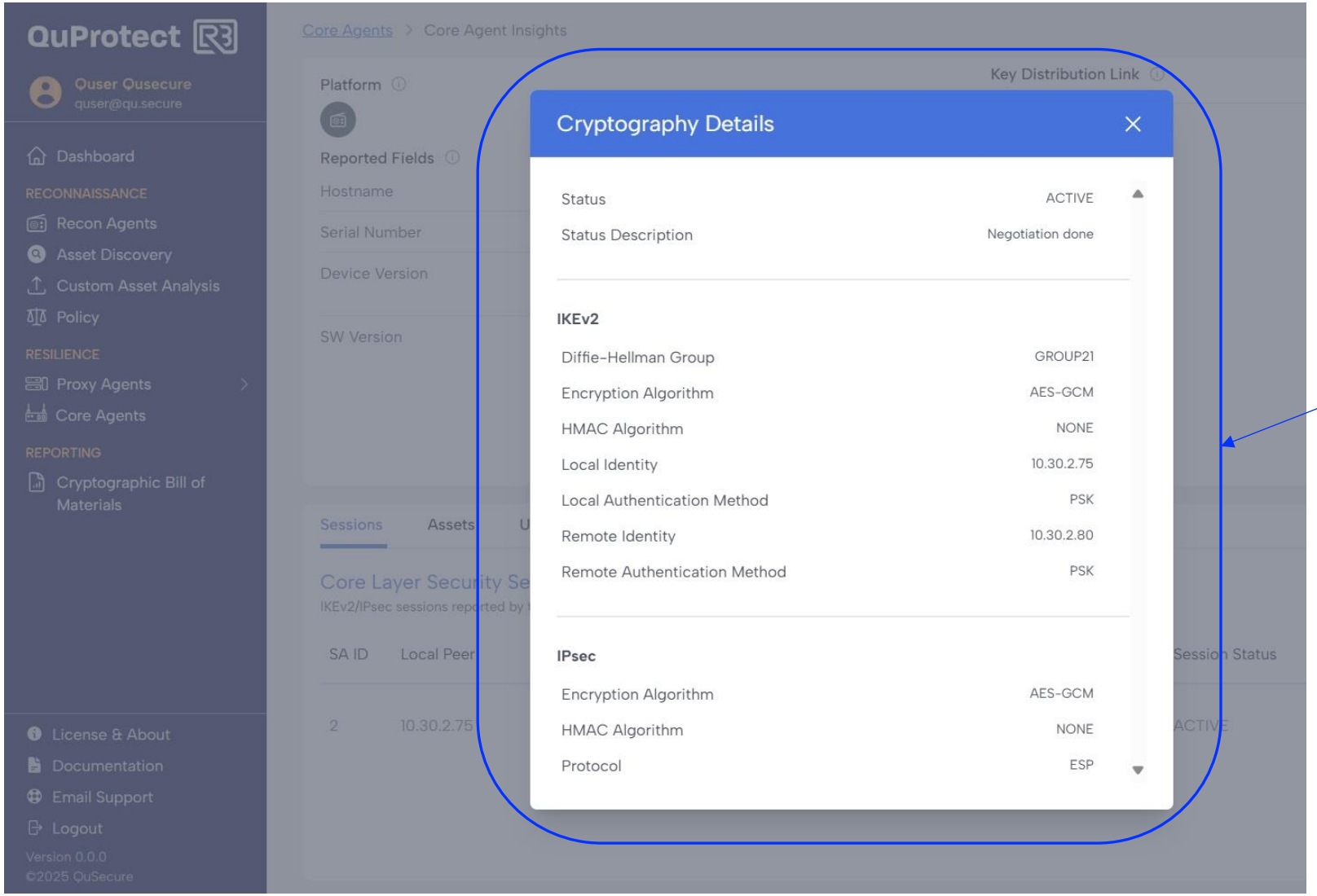
Leverage Operational YANG Models to Consolidate “Show” Ouput



cisco

QuSecure Screen Shots

QuSecure



Displays relevant data from:

“show crypto ikev2 session”

”show crypto ikev2 sa”

YANG Models Used:

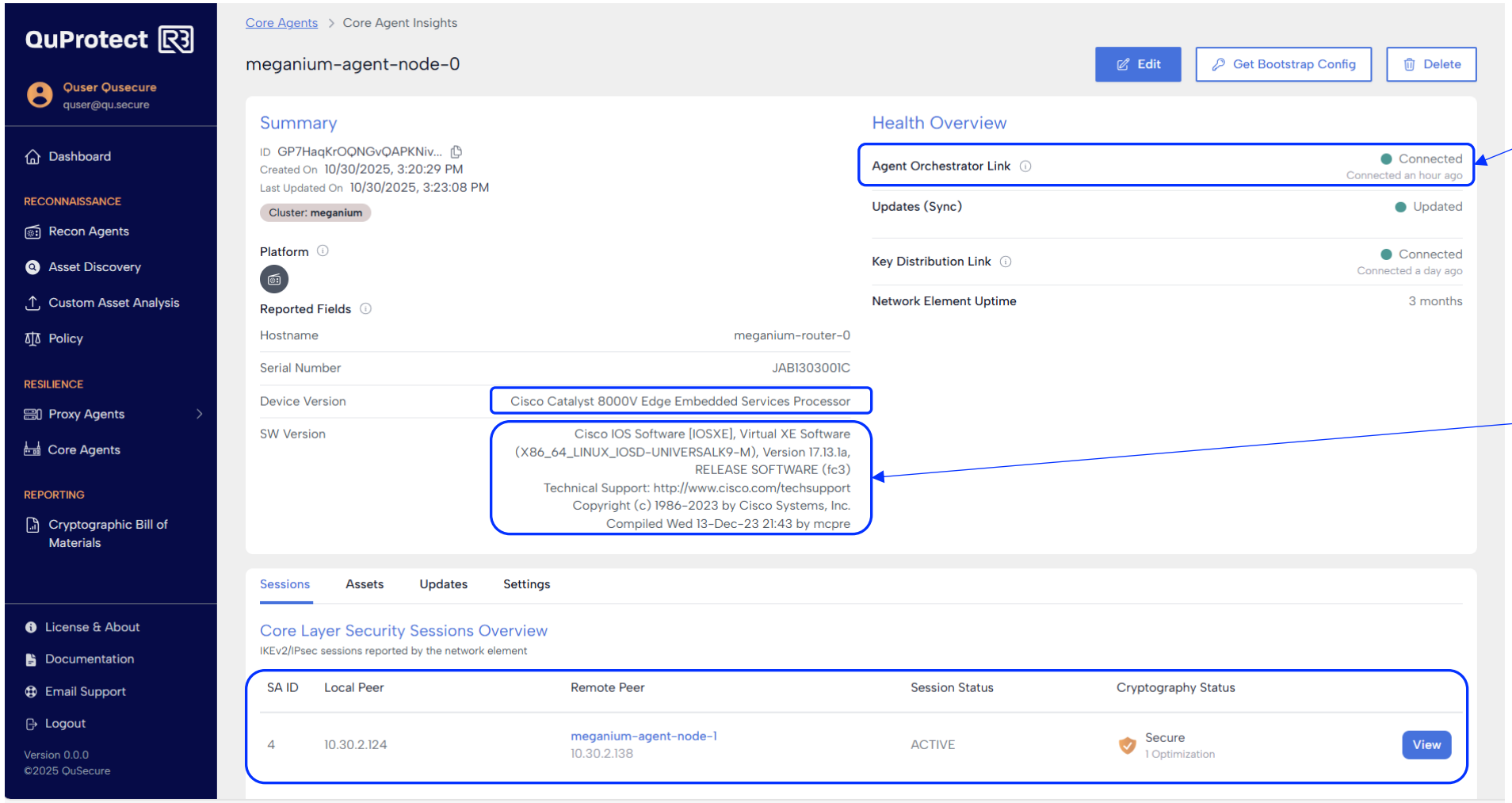
Cisco-IOS-XE-crypto-oper:crypto-oper-data/crypto-ikev2-sa

Cisco-IOS-XE-crypto-oper:crypto-oper-data/crypto-ikev2-sess-detail

cisco

QuSecure Screen Shots

QuSecure



Displays the SKIP link quality status

Displays relevant data from “show hardware”

Shows Remote Dynamic PQC Server (“quprotect-core” is the dynamic key server [QuSecure PQC])

YANG Models Used:

`Cisco-IOS-XE-device-hardware-oper:device-hardware-data`

cisco

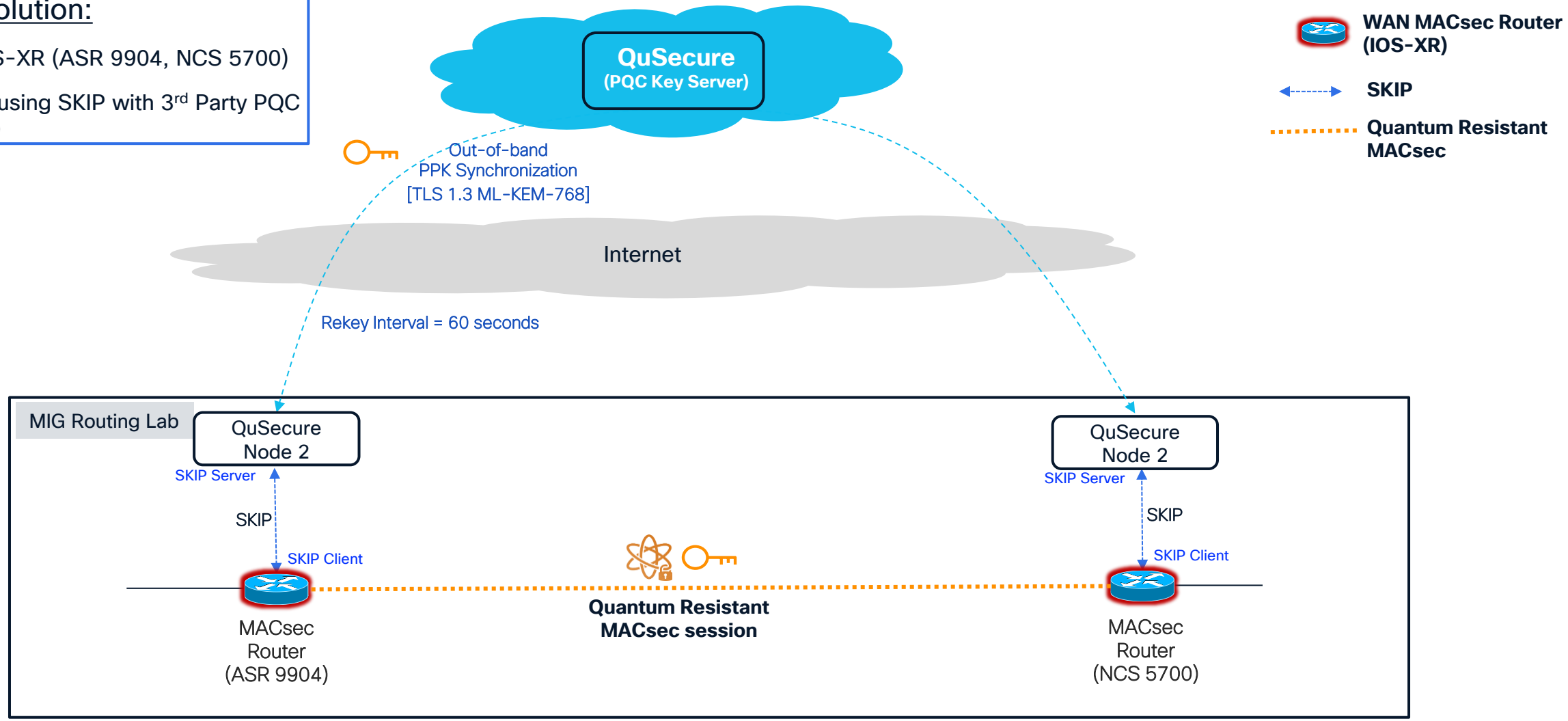
Post-Quantum IOS-XR

MACsec + SKIP using External Key Source

MACsec Quantum Safe Demo Using Dynamic Post Quantum Preshared Keys

Demo Solution:

- Cisco IOS-XR (ASR 9904, NCS 5700)
- MACsec using SKIP with 3rd Party PQC (QuSecure)



PPK = Postquantum Preshared Keys

SHOW Output

```
RP/0/RP0/CPU0:NCS-57B1# sh macsec mka int hun 0/0/0/3 detail

Thu Jun 13 20:02:39.839 UTC

Interface Name : HundredGigE0/0/0/3

    Interface Namestring     : HundredGigE0/0/0/3


    Interface MAC            : bc2c.e69a.9610

    Ethertype                : 888E

    EAPoL Destination Addr   : 0180.c200.0003


    MKA PSK Info

      Key Chain Name         : kc

      MKA Cipher Suite       : AES-256-CMAC

      CKN                    : 12 34

    MKA fallback_PSK Info

      fallback keychain Name : - NA -

    Policy                   : mp

    SKS Profile              : quprotect-core (Active)

    Traffic Status           : Protected
```

PPK based MACsec Key Distribution for MKA “enabled” with SKS profile on MACsec policy (Default = “OFF”)

MACsec Policy

```
!
macsec-policy mp
 ppk
  sks-profile quprotect-core
 !
 sak-rekey-interval seconds 60
!
sks profile quprotect-core type remote
 kme
  server hostname skip-poc-1 port 443
 !
!
```

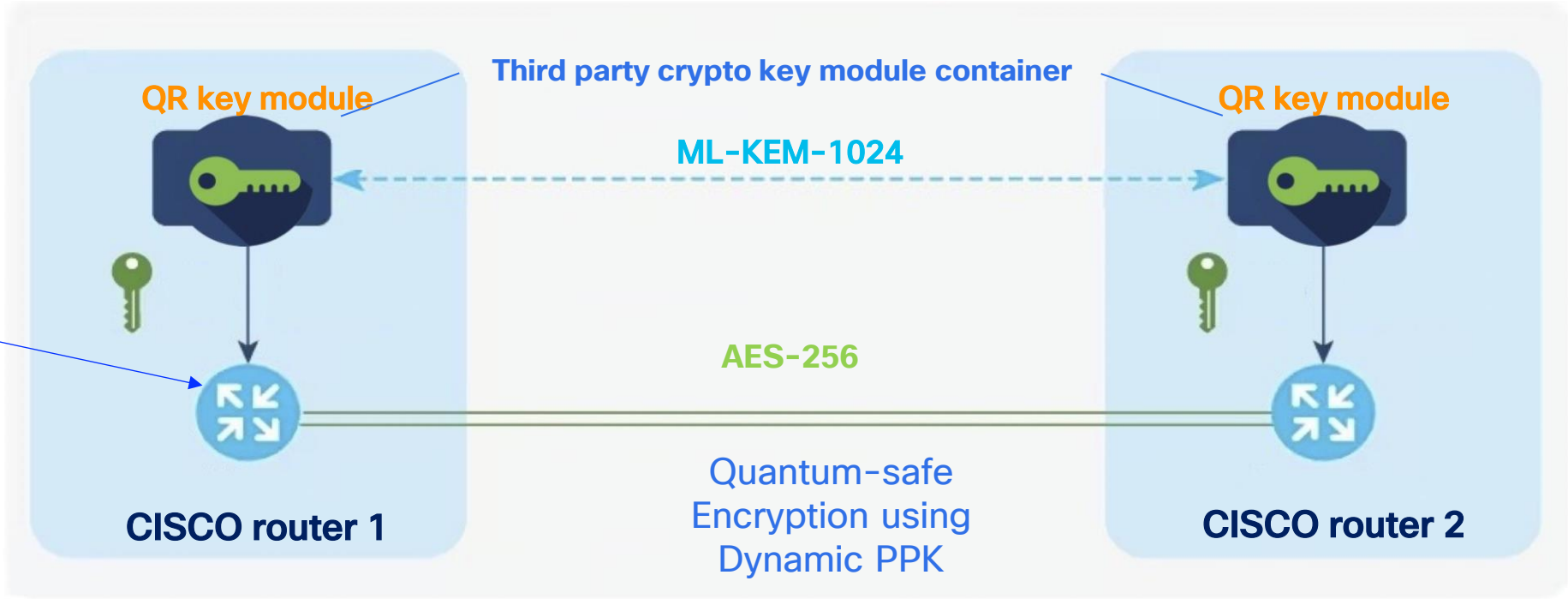
Shows Remote Dynamic PQC Server (“quprotect-core” is the dynamic key server [QuSecure PQC])

IPSec & MACsec Using Dynamic PPK

Quantum Xchange (Phio TX)™ Hosted on Cisco Router Platforms

QUANTUMXCHANGE

The “QR Key Module” is a hosted application in the Catalyst 8000 router.



- FIPS 203 ML-KEM-1024 validated
- Dynamic PPK – IPSec (RFC 8784), MACsec
- Catalyst 8000 w/ host App (IPsec verified)
- ASR 9000 & NCS 5K (MACsec verified)

- Maintains performance & Resiliency, Offers local PPK Keys hosted on platform, no additional dependencies or crypto key exposure
- Use Cases: applications where connection to external 3rd-party QR key servers are challenging (EX: tactical, mobile, non-terrestrial)

cisco

Transition To Native PQC Algorithms

Native PQC Method using quantum-safe algorithms

Solution Components:

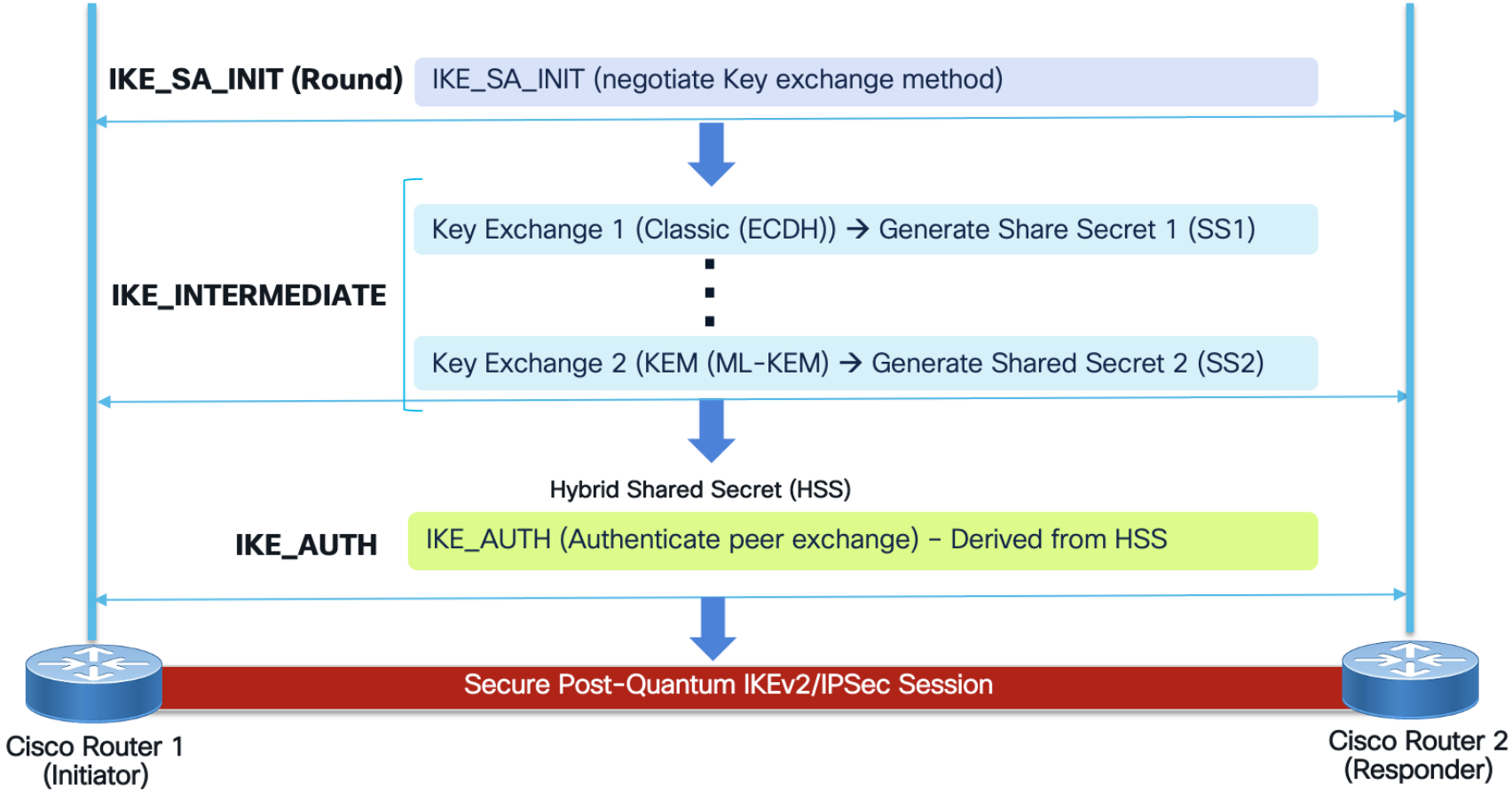
- RFC 9370 IKEv2 PQ Key Exchange
- Cisco SSL 8.3
- EAP-TLS PQ Key Exchange for MACsec

ML-KEM (CRYSTALS Kyber) – FIPS 203

- Module-Lattice-Based Key-Encapsulation Mechanism Standard

Quantum Resistant Encryption with RFC 9242 and RFC 9370

Support for Multiple Key Exchanges in IKEv2 for PQ with Hybrid

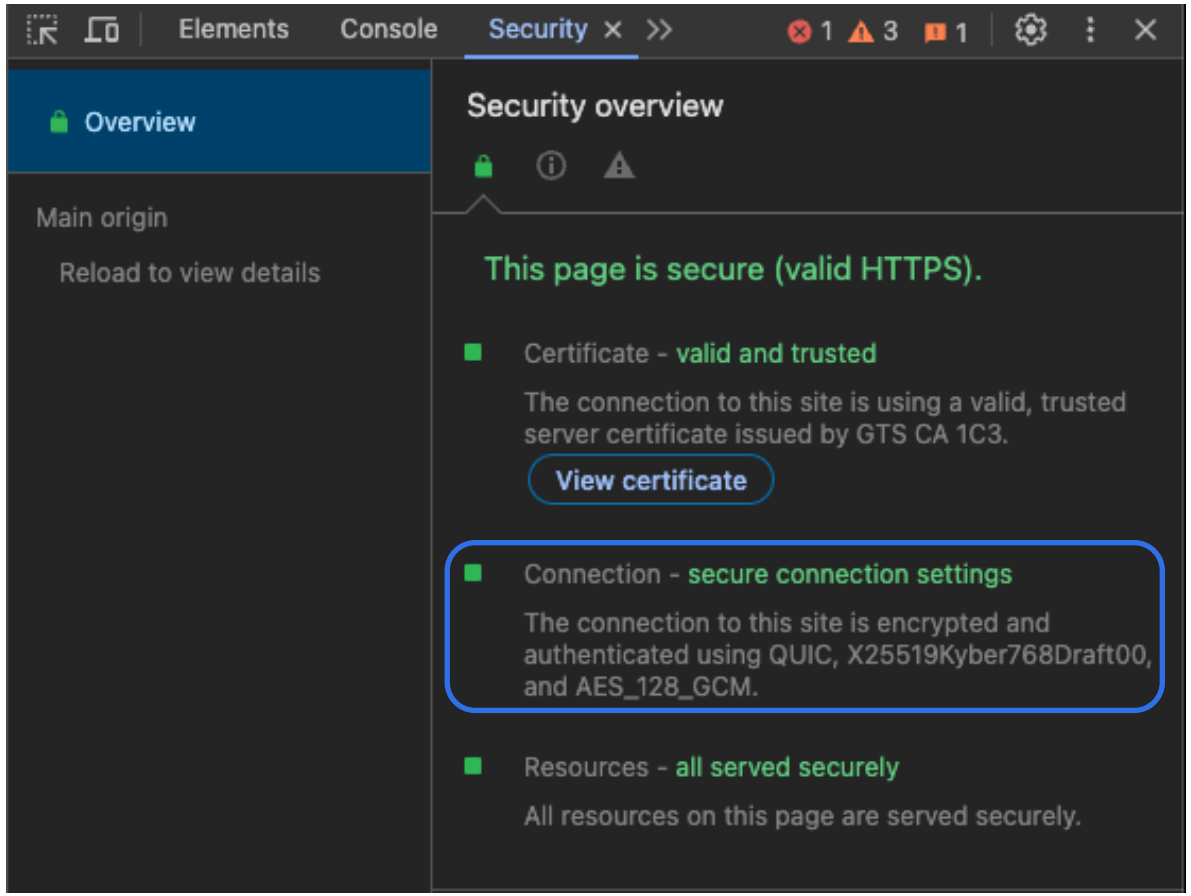


Transition Note per RFC 9370:

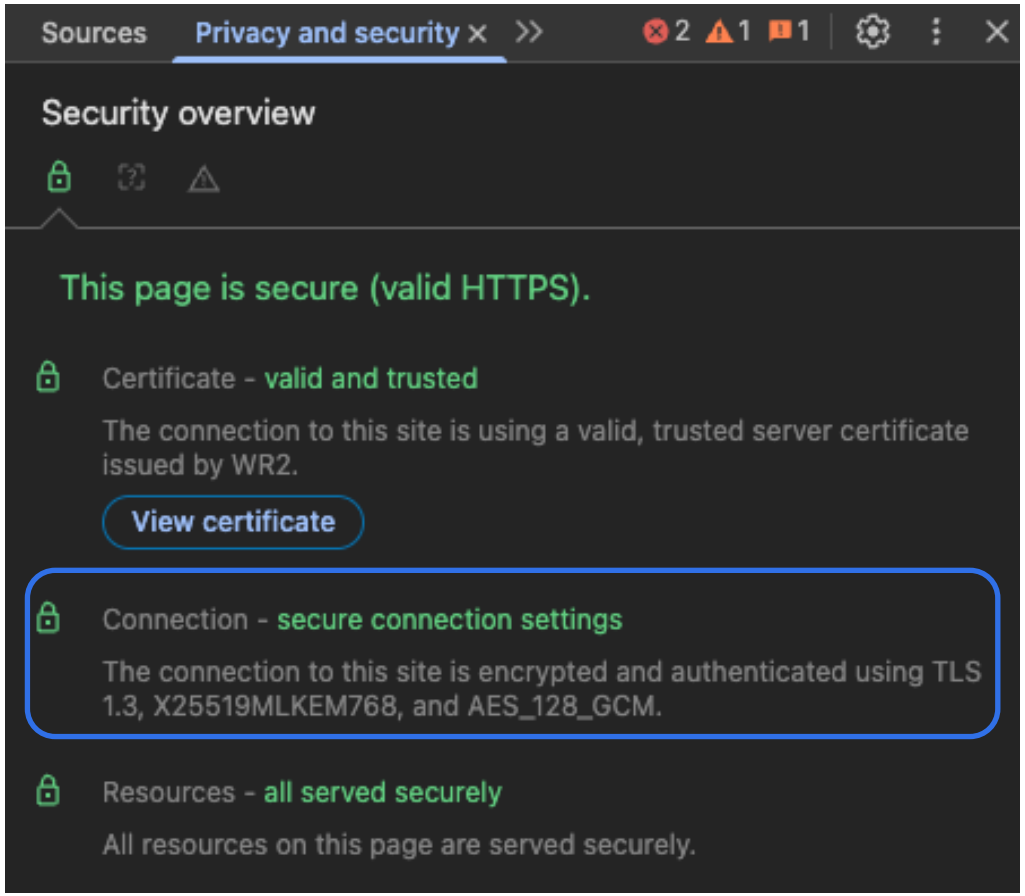
- *This is the approach long-term for IKEv2 support of PQ algorithms*
- *Short-term for IKEv2 quantum secure is PPK as specified in RFC8784*

Example: Hybrid TLS 1.3 on Chrome Web Browser

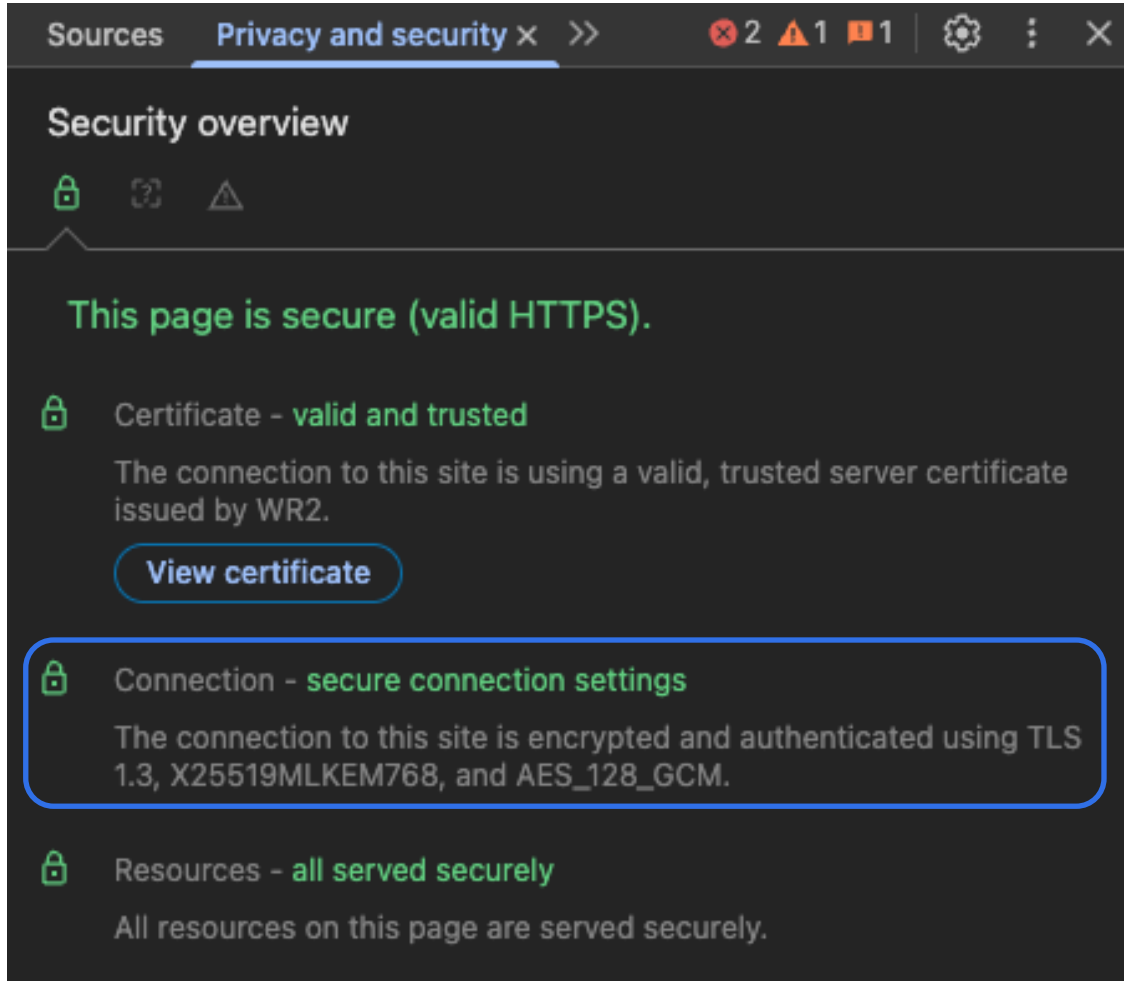
Pre NIST Standard



Post NIST Standard

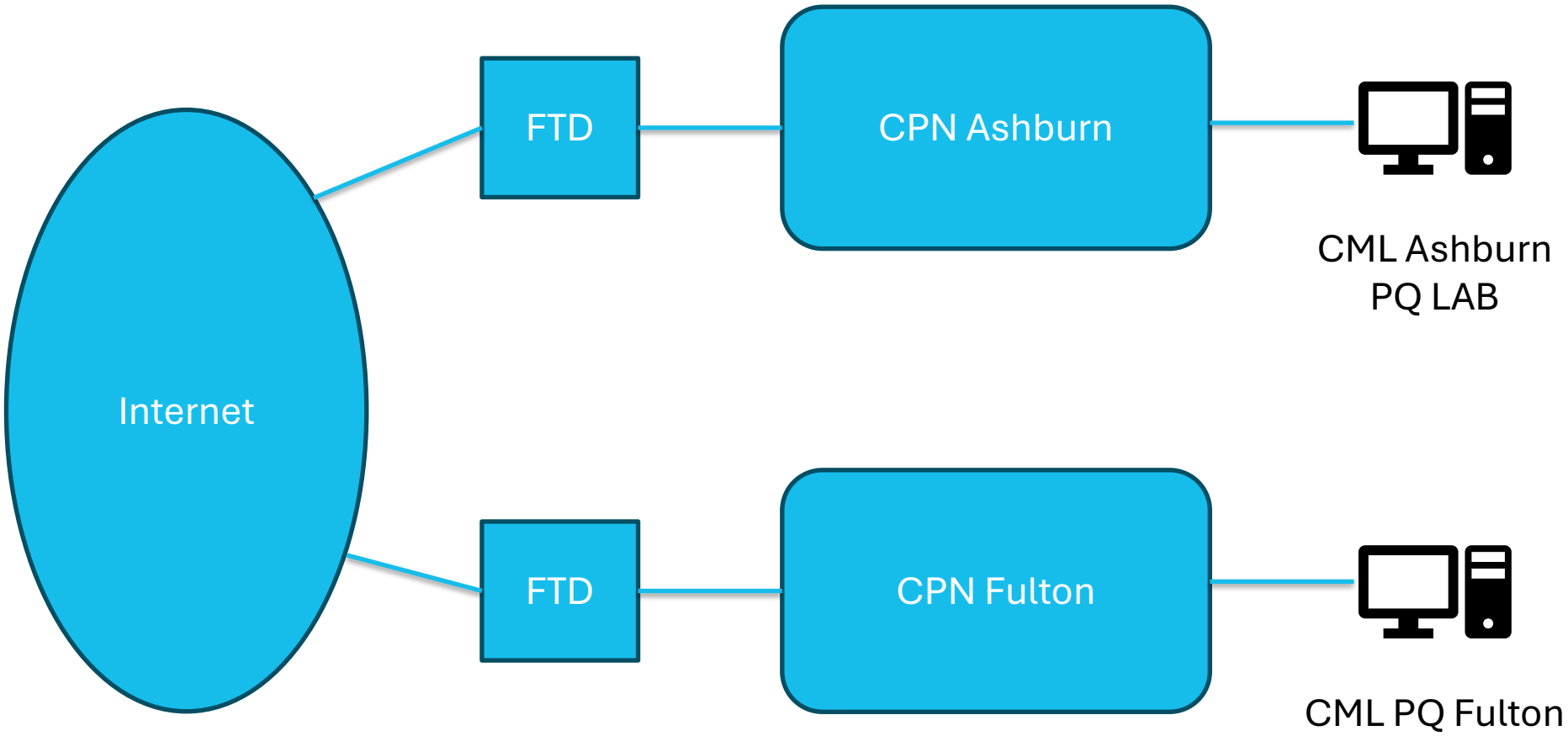


Example: Hybrid TLS 1.3 on Chrome Web Browser
(as of June 2, 2025)



- Google started post-quantum secure TLS encapsulation (AUG 2023)
- This shows successor to Kyber, using new ML-KEM standard for post-quantum key exchange
- Using X25519 in combination with ML-KEM, indicates “hybrid” key exchange for TLS 1.3
- Still early and some challenges with websites, applications and firewalls unable to crank back to classic cryptography

Post Quantum CML Lab



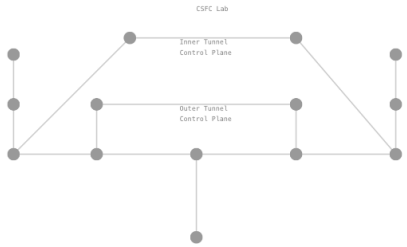
Cisco Modeling Labs | Dashboard

DASHBOARD | TOOLS | ABENHASE

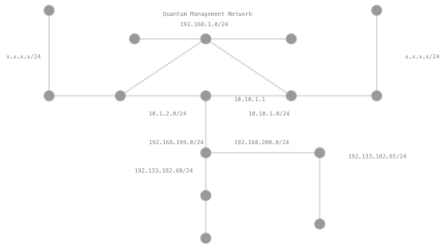
Show List | Show All

ADD | IMPORT

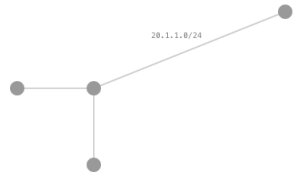
PQC Lab - Alpha



PQC Lab - Router Only ON

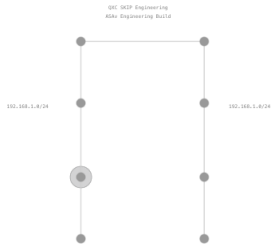


Joe Ciccone - QXC



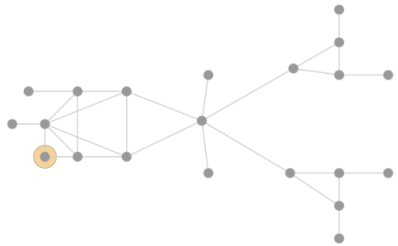
PhioTX Container Lab Space

SKIP Engineering - ASAv ON



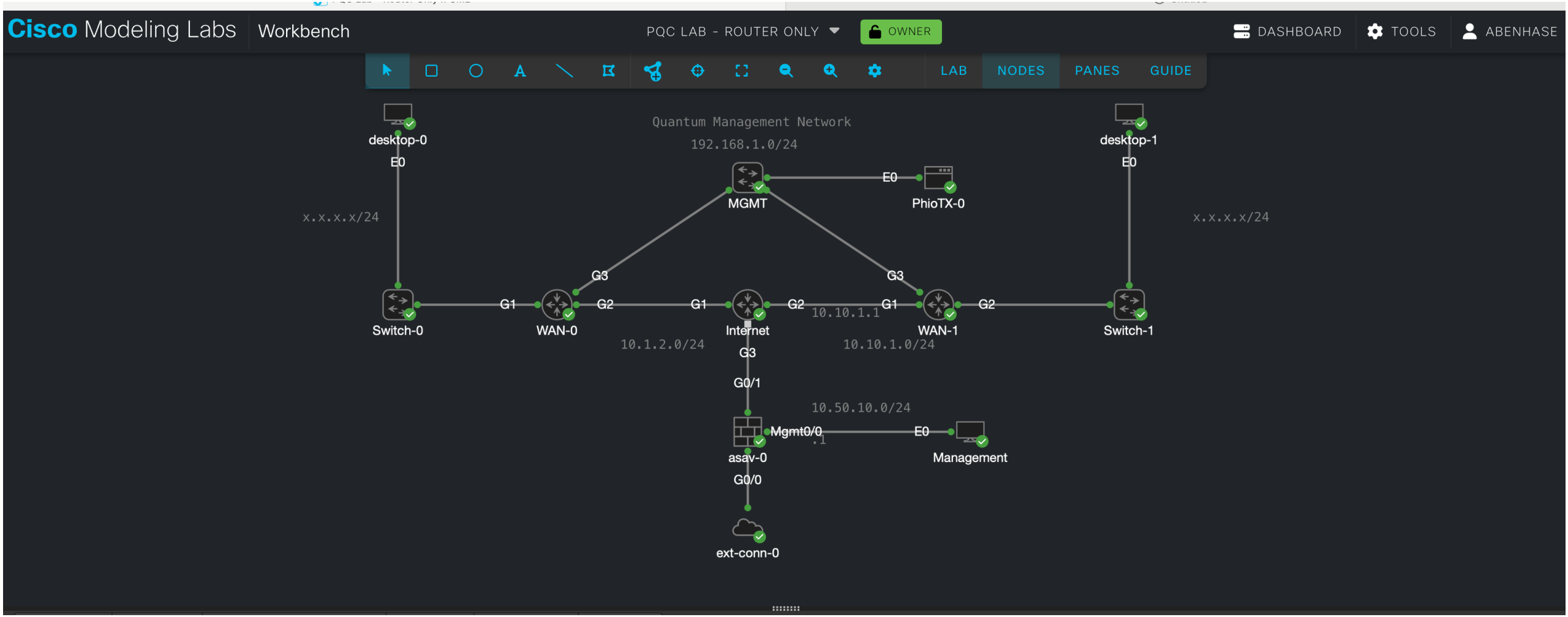
Protected Engineering Lab

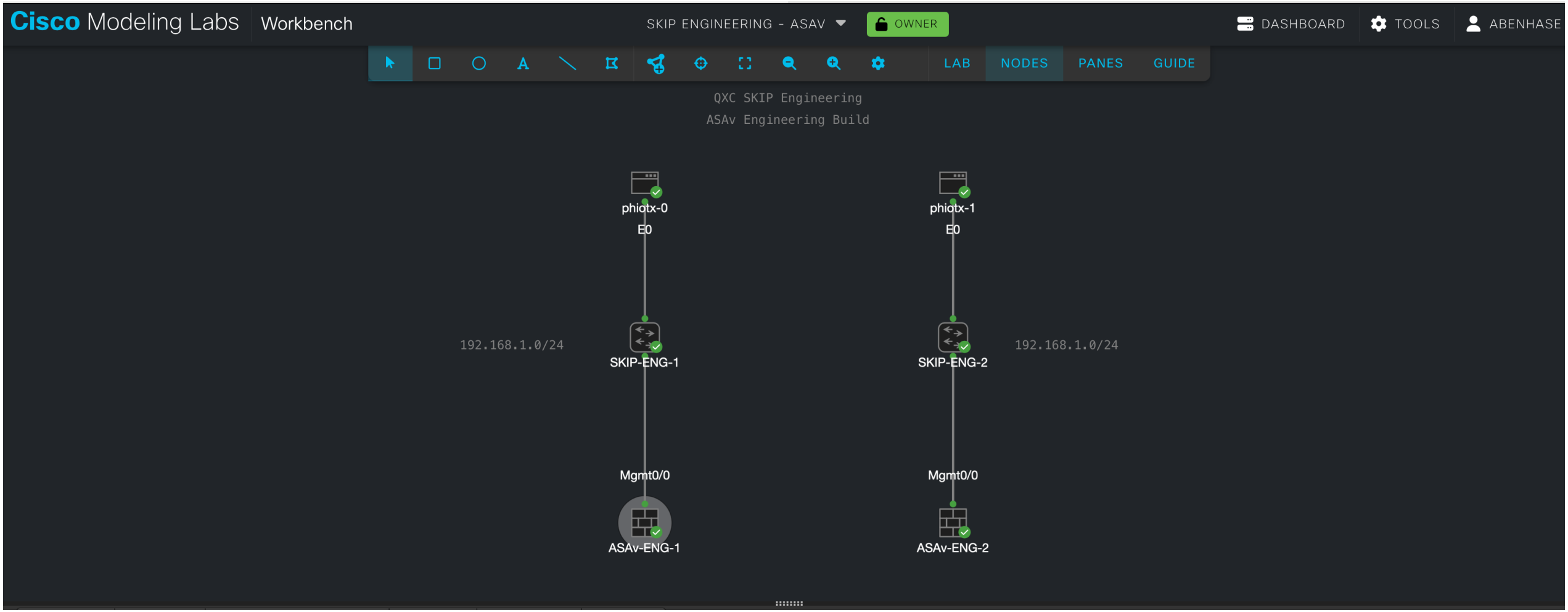
stevenca-mdd0



Lab at Tue 18:22 PM ON

cisco



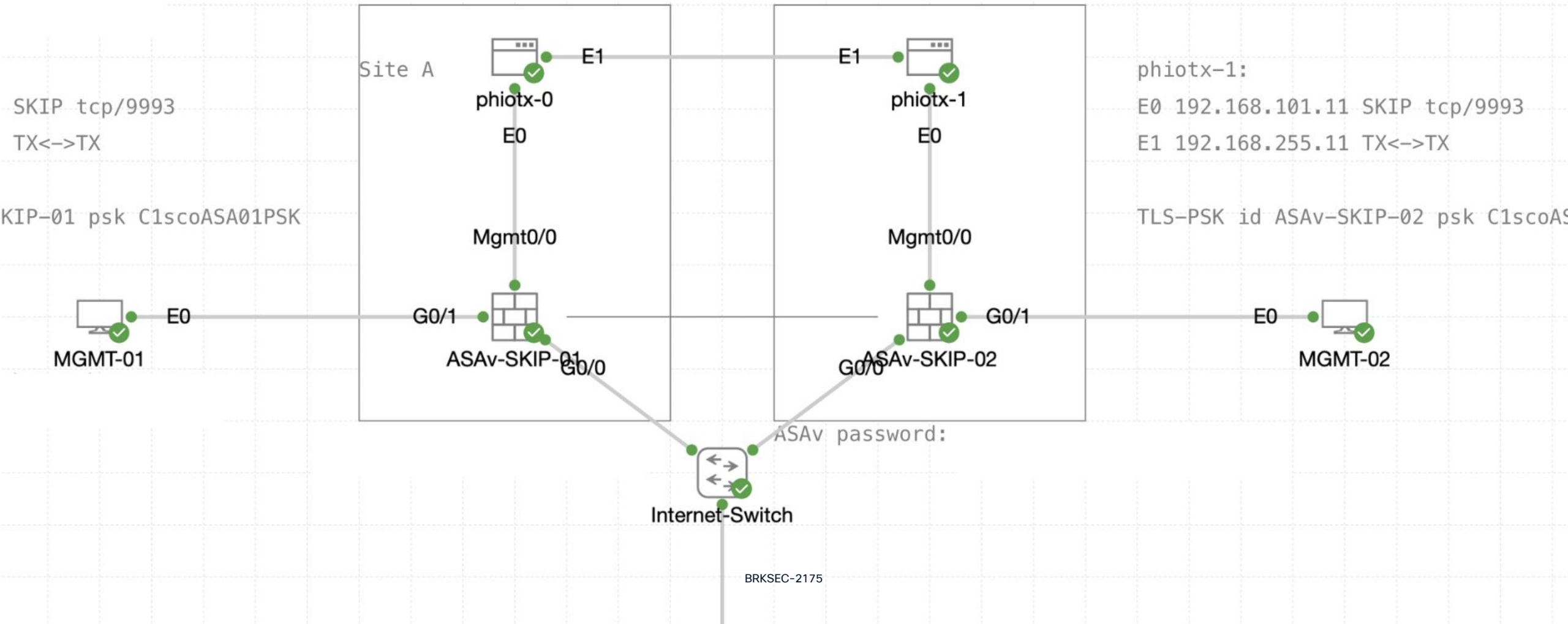


OS Workbench BANGALORE - SKIP ENGINEERING - QXC+ASAV ADMIN DASHBOARD TOOLS

LAB NODES PANES GUIDE

Bangalore SKIP Engineering with Quantum Exchange

TX Container:



SKIP tcp/9993
TX<->TX

KIP-01 psk C1scoASA01PSK

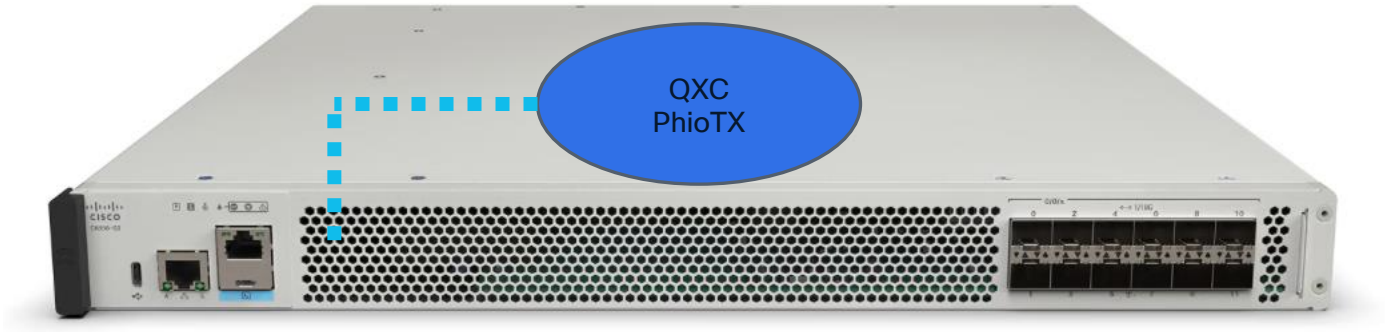
phiotx-1:
E0 192.168.101.11 SKIP tcp/9993
E1 192.168.255.11 TX<->TX

TLS-PSK id ASAv-SKIP-02 psk C1scoAS

ASAv password:

Why is this Quantum innovative?

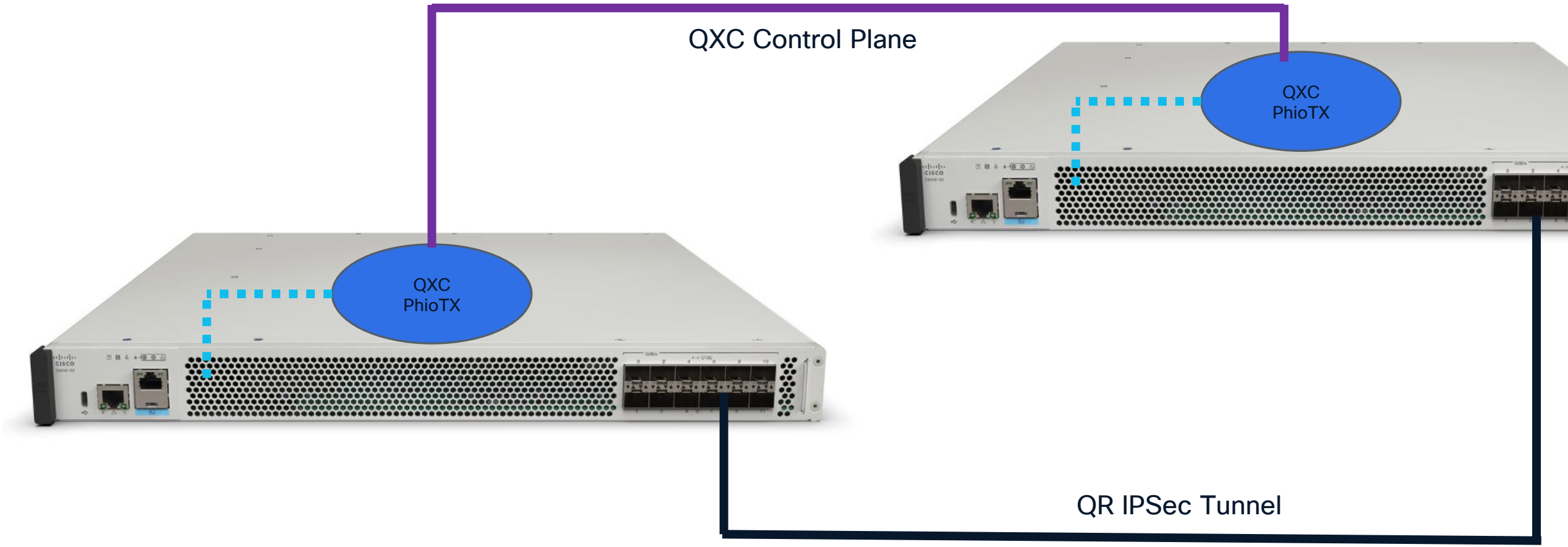
Running within the IOS-XE Memory Boundary is an embedded Key Server



Using the internal control plane, the PhioTX container communicates and rotates key_mat to the router

Control Plane Security insures protected communications to the opposing PhioTX container to synchronize

Why is this Quantum innovative?



References

References and Authored Documents

- Post Quantum Resistance – Case Study & Proof of Concept – Cisco / QuSecure (Hill, C., Lupo, J.)
  - Craig Hill will make available in ”Teams Room” (or email Craig @ crhill@cisco.com)
- Understanding Quantum-Safe Encryption on Cisco IOS XE Platforms
  - https://learningnetwork.cisco.com/s/article/understanding-quantum-safe-encryption-on-cisco-ios-xe-platforms
- Configuring Quantum-Safe IPSec Encryption using Postquantum Preshared Keys and using SKIP
  - https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html
- Configuring Quantum-Safe MACsec Encryption using SKIP
  - https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/710x/system-security/configuration/guide/b-system-security-cg-asr9000-710x/implementing-macsec-encryption.html
- Cisco Research – Cisco Quantum Lab
  - https://research.cisco.com/research-projects/quantum
- Cisco Live – On-Demand Library – **Search “quantum”**
- Cisco Session Key Server (SKS) in IOS XR
  - https://www.cisco.com/c/en/us/td/docs/optical/ncs1004/241x/configuration/guide/b-configuration-guide-ncs1004-r2411/m-sec-cfg-quantum-encryption-ppk.html
- MACsec White Paper (Hill, C., Orr, S.)
  - https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

Cisco Quantum Safe Crypto Capabilities

All Dates Subject to Change
(Does not include entire Cisco portfolio)

PQC Solution	Available Today	Future Roadmap
RFC8784 - Mixing Preshared Keys in IKEv2 for Post-quantum Security	PPK: Manual & SKIP • **IOS-XE 17.11+** - Cat8300, Cat8000v, ASR1K, ISR • **IOS-XE 17.12+** - Cat8500 PPK: Manual only • **ASA 7.3** (all ASA versions, not FTD)	Available now
RFC 9370/9242 – Multiple Key/Intermediate Exchanges IKEv2 Native PQC (FIPS 203)	• Planned – IOS XE, IOS XR, FXOS	**IOS-XE: CY-2026** Platforms: Catalyst 8000 Family (Others planned) **IOS-XE: 2H – CY-2026** Platforms: Catalyst 9000 Family
MACSEC	PPK: Cisco SKS & SKIP Support • **IOS-XR 7.9.1** - NCS540, NCS5500, NCS5700, 8000 • **IOS-XR 7.10.1** - ASR9000 PPK: Cisco SKIP Support • **NX-OS 10.4(3)F** – N9K-C93xx Fam (NX-OS specific HW)	**IOS-XE: CY-2026** Platforms: Catalyst 8000 Family – PQ EAP-TLS **IOS-XR: CY-2026** • Platforms MACsec Supported - PQ EAP-TLS
SD-WAN	• Planned – Future Committed	**IOS-XE: 2H - CY'26** Platforms: Cisco 8000 Secure Router
PQ TLS 1.3 (FIPS 203/ML-KEM)	• Planned – Future Committed Moving Forward with all platforms	**IOS-XE: CY-2026+** **OS-XR: CY-2026+**

Summary

- The transition to early quantum-safe network encryption is available now
- IPSec (RFC 8784 for IPSec) and MACsec (early MKA extensions) options exist today
- SKIP enables the use of external/3rd-party key servers to Cisco devices
- The transition to NIST native post-quantum encryption algorithms is underway
- Targets include IKEv2, TLS, SSH and will be leveraged by existing Cisco encryption solutions

Complete your session evaluations

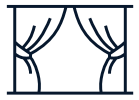
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

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

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

Contact me at: crhill@cisco.com, abenhase@cisco.com

Thank you

cisco Live !


CISCO