

Quantum Safe Cryptography And Why You Need it

cisco Live !

Andrew Benhase
Federal Architect, US Public Sector
@CyberSecOps

Craig Hill
Distinguished Solutions Engineer, US Public Sector
@netwrkr95

Cisco Webex App

Questions?

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

How

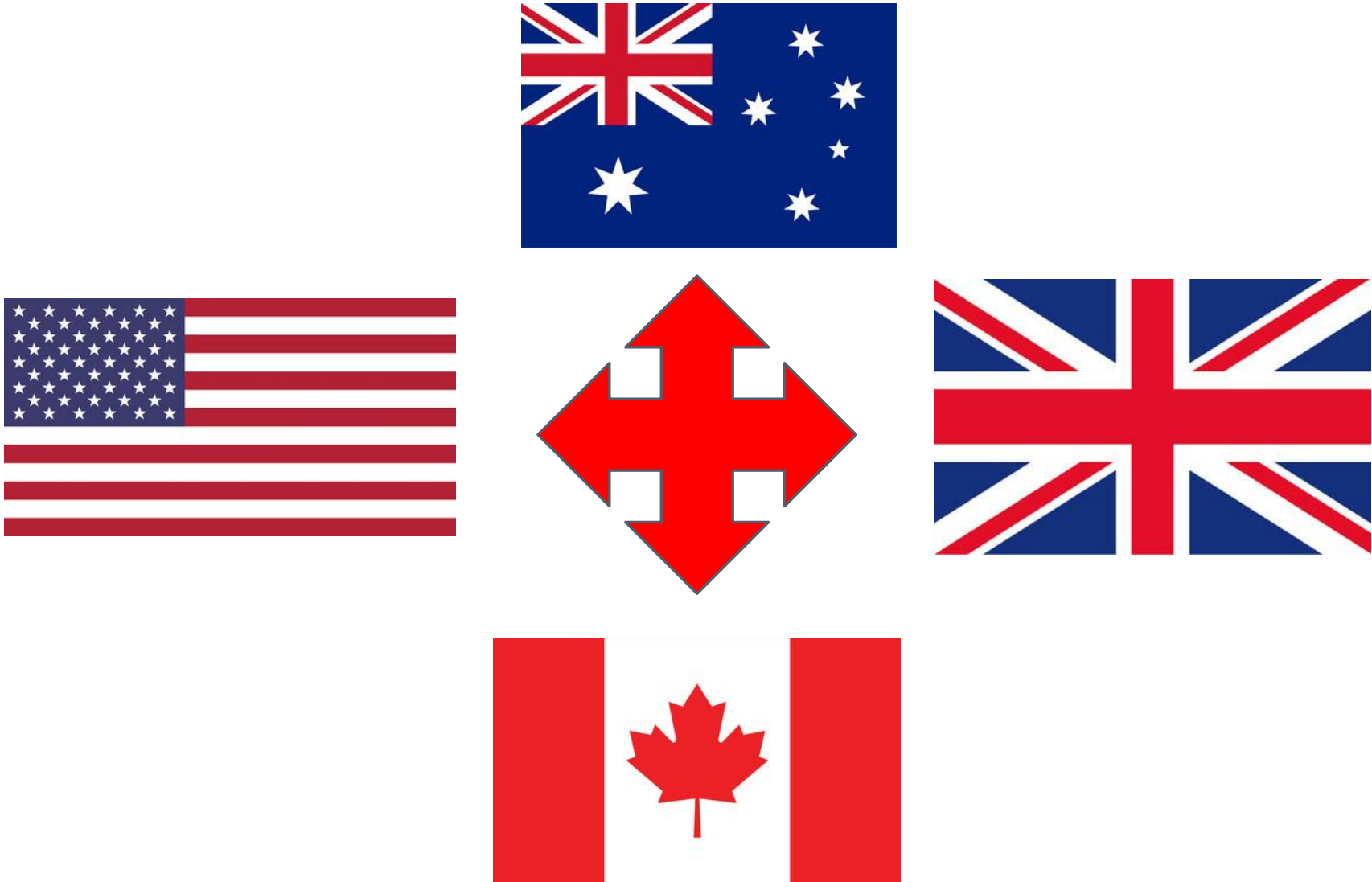
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2175>

About Nation State Cryptography



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.

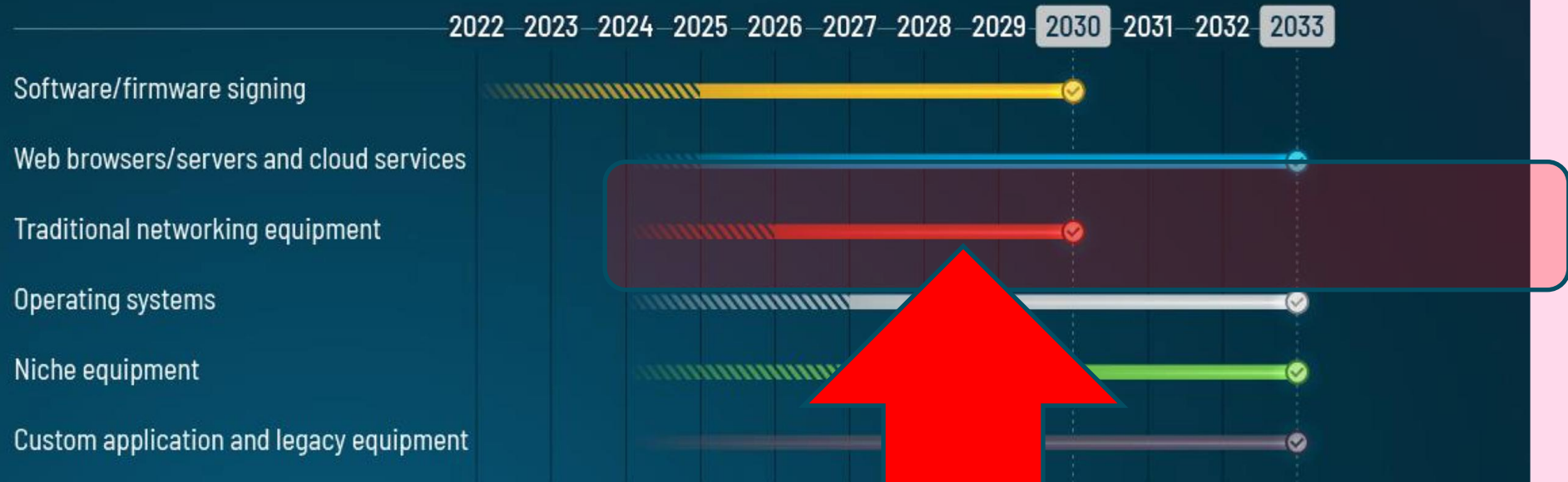
Quantum Random Number Generation

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



This is why
Second register
 $\langle 1 \rangle$ we are here
today

CNSA 2.0 Timeline



led as an option and tested
the default and preferred
se CNSA 2.0 by this year



↖ PRESIDENTIAL ACTIONS

SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144

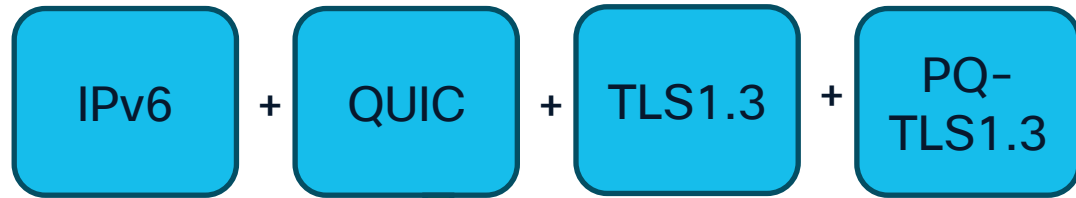
Executive Orders | June 6, 2025

More from the Executive Order – June 6, 2025...

(i) By December 1, 2025, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in consultation with the Director of the National Security Agency, shall release and thereafter regularly update a list of product categories in which products that support post-quantum cryptography (PQC) are widely available.

(ii) By December 1, 2025, to prepare for transition to PQC, the Director of the National Security Agency with respect to National Security Systems (NSS), and the Director of OMB with respect to non-NSS, shall each issue requirements for agencies to support, as soon as practicable, by January 2, 2030, Transport Layer Security protocol version 1.3 or a successor version.”;

Future Protocol Timeline



Today

Tomorrow

Timeline

2025

2026

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

US Government Direction on Quantum Safety

Current U.S. Government Direction

- US Government has provided clear direction for requirements on Quantum Resistance for protection of National Security Systems
 - (ref: NCSIP and NSM-10)
- Quantum Key Distribution is an open topic and lacks standards
- Not adopting ETSI-014
- Cisco SKIP should be an acceptable option (more on this later)
- All aspects of encryption should drive towards Quantum Resistance encryption options
- Site to Site VPN, VPN Client along with TLS stack implementations for control plane operations

US Department of Defense Mandate

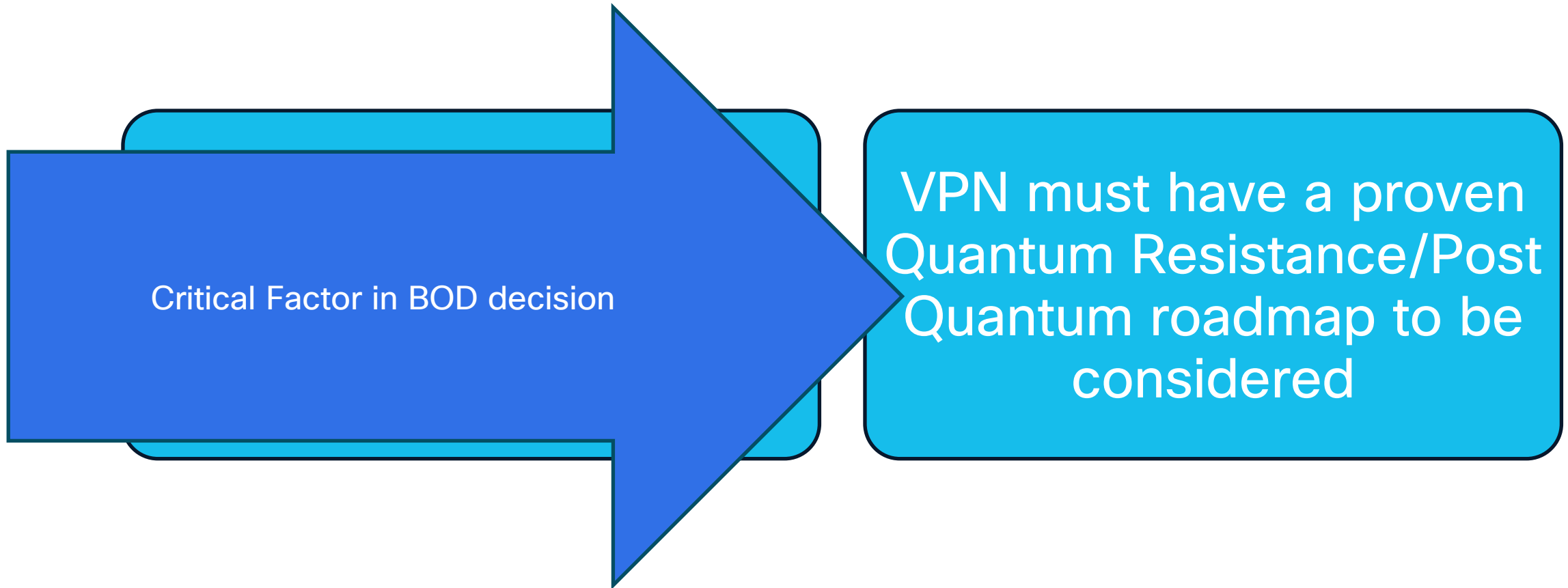
- October 2024 – DoD mandates use of Transport Security (TRANSEC) for all National Security Systems (NSS)
- Requires outer VPN tunnel for all NSS
- Funding was dropped JAN 2025
- Mandatory requirement for Outer VPN Tunnel across all NSS
- Also requires implementation of a standalone IDS outside of the VPN device
- Customers are currently planning for VPN + IDS
- VPN+IDS could be combined into a single offer

*Includes all FVEY Nations

BOD 2024-02 – TRANSEC

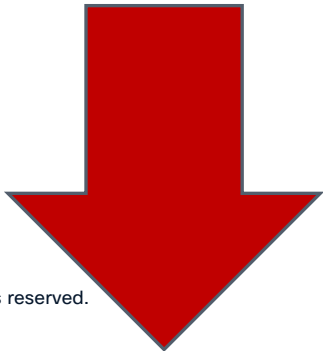
- October (MAY)2024 – DoD mandates use of Transport Security (TRANSEC) for all National Security Systems (NSS)
- Requires outer VPN tunnel for all NSS
- Funding was dropped JAN 2025
- Mandatory requirement for Outer VPN Tunnel across all NSS

Mandatory Requirements



Mandatory Requirements

VPN device must be a
NIAP approved device



VPN must have a proven
Quantum Resistance/Post
Quantum roadmap to be
considered

NIAP Evaluation (aka Common Criteria)

PRODUCT COMPLIANT LIST - 274

274

Product Compliant List

25

Products In Evaluation

1345

Archived Products

<< HIDE FILTER <<

Keyword Search

🔍

Filter Options

Technology Type

▼

Vendor

Cisco Systems, Inc. X ▼

Protection Profile

▼

Certifying Country

▼

Maintenance

All Products ▼

Product Status

CERTIFIED

IN EVALUATION

ARCHIVED

CLEAR FILTERS

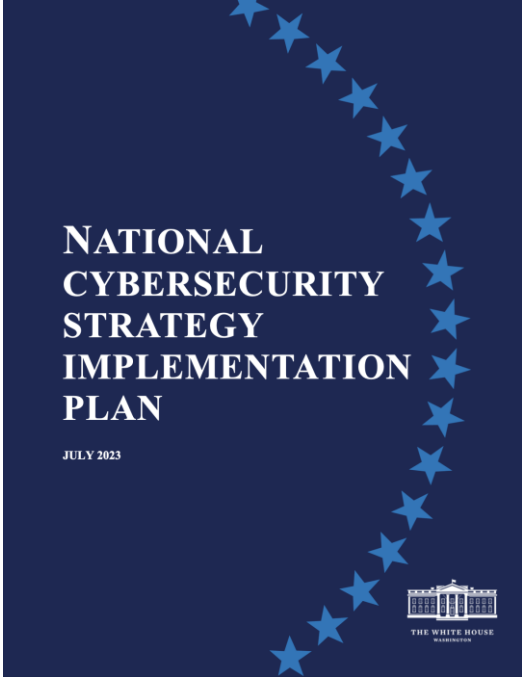
☰

🏠

📏

Showing: 40

VID	Vendor	Product	CCTL	Certification D...	Status	Conformance Claims	Assurance M
11643	Cisco Systems, Inc.	Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.15	Lightship Security	09/29/2025	Certified	<div>PKG_SSH_V1.0</div> <div>MOD_VPNGW_v1.3</div> <div>CPP_ND_V3.0E</div>	10/14/2025
11603	Cisco Systems, Inc.	Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15	Gossamer Security	09/29/2025	Certified	<div>PKG_SSH_V1.0</div> <div>MOD_MACSEC_V1.0</div> <div>CPP_ND_V3.0E</div>	10/03/2025
		Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K)	Lightship Security USA, Inc.	09/29/2025	Certified	<div>PKG_SSH_V1.0</div> <div>MOD_MACSEC_V1.0</div> <div>MOD_VPNGW_v</div>	09/29/2025



Strategic Objective 4.3: Prepare for Our Post-Quantum Future

Initiative Number: 4.3.1

Initiative Title: Implement National Security Memorandum-10

The Predicate

Initiative Description

The Office of Management and Budget and the National Manager for National Security Systems, in coordination with ONCD, will continue to prioritize implementation of National Security Memorandum-10 and transitioning vulnerable public networks and systems to quantum-resistant cryptography-based environments, focusing first on Federal information systems and NSS. OMB will work with NIST to develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

NCS Reference

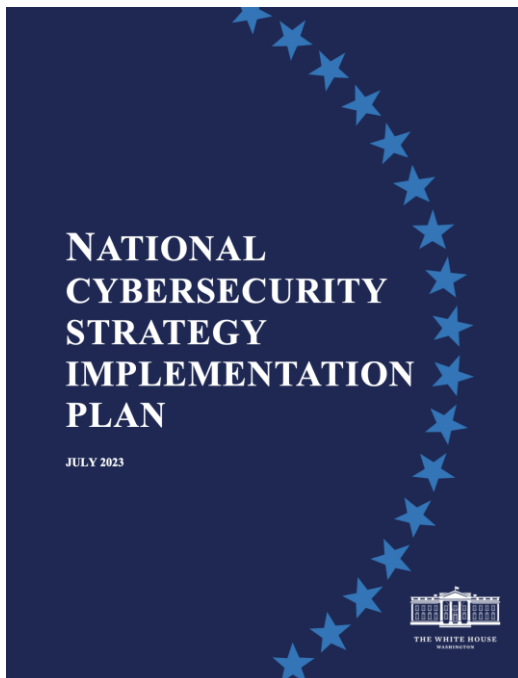
The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: OMB

Contributing Entities: NSA, ONCD

Completion Date: 1Q FY25

First Quarter, next year!



Initiative Number: 4.3.2

Initiative Title: Implement NSM-10 for National Security Systems (NSS)

Initiative Description

Implement the transition of NSS to quantum-resistant cryptography.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography (QRC)-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: NSA

Contributing Entities: DOD, ODNI

Completion Date: 3Q FY25

Initiative Number: 4.3.3

Initiative Title: Standardize, and support transition to, post-quantum cryptographic algorithms

Initiative Description

The National Institute of Standards and Technology will finalize its process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. New public-key cryptography standards will specify one or more additional unclassified, publicly-disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

NCS Reference

To balance the promotion and advancement of quantum computing against threats posted to digital systems, National Security Memorandum (NSM) 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes responsibilities and oversight to enable a timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography.

Responsible Agency: NIST

Completion Date: 1Q FY25

QR Mandatory

3rd Quarter, 2025

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 analogous 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-connelly-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>

What do we have for Firewalls today?

- ASA v9.20 (RFC 9242/9370-pre)
- ASA v9.18 (RFC 8784)

- No SKIP Support
- No FTD Support
- No FMC Support
- No FDM Support
- No PQ-SSH
- No PQ-TLS 1.3

- No AnyConnect Support for RFC 8784 or RFC 9370

What do we have for Routers today?

- RFC 8784 Support in IOS 17.11+
- SKIP Support in IOS 17.11+

- No PQ-SSH
- No PQ-IKEv2
- No PQ-TLS 1.3
- No RFC 9242/9370

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

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

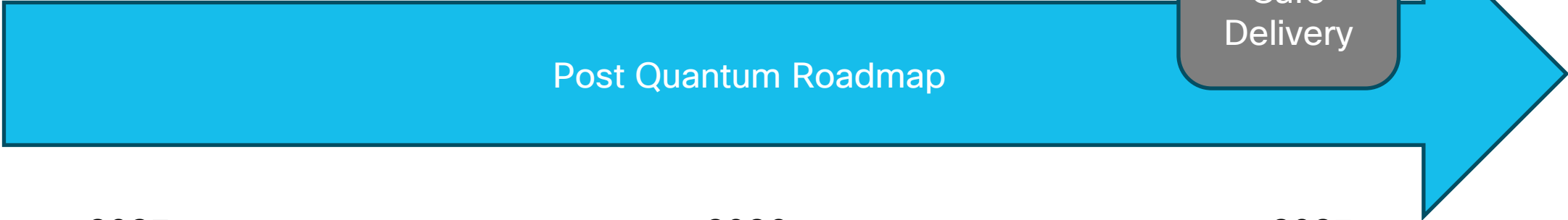
Current
Firewall
Quantum
Capability

FTD 7.4
ASA 9.22

Quantum
MidPoint
Delivery

FTD 7.8 (10.0)
ASA 9.24

FTD 10.5.xx
ASA 9.xx
Quantum
Safe
Delivery



Post Quantum Roadmap

2025

2026

2027

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

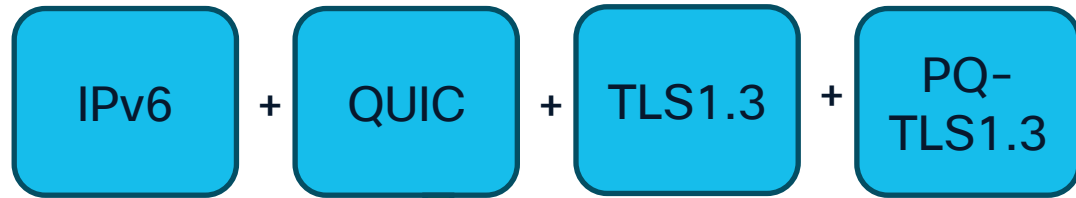
- Support for ML-KEM-1024 for SSHv2 – FMC/FTD/FXOS
- Support for ML-KEM-1024 for SSHv2 – IOS-XE
- Support for Draft PQ-IKEv2 for Remote Access – ASA/FTD/FMC/FDM
- Support for TACACS+TLS1.3 Draft
 - Include PQ-TLS 1.3 as part of delivery

Currently
shipping
or 7.4–7.8
(10.0)

Must be
committed
for
10.0.10

PQ-Safe –
includes
SSH+TACAC
S+LMSS for
firmware

Future Protocol Timeline



Today

Tomorrow

Timeline

2025

2026

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

Quantum Resistance Direction for Cisco

- Focus: ASA 9.21 and FTD 7.7
- Focus: IOS-XE 17.15

Overall Objective and Goal

- Moderate investment in Quantum Resistance technologies providing scalable solutions using Quantum Key Distribution
- Modest near term investment in Post-Quantum solutions watching closely at market directions
- Maintain Best-in-Class fully featured IKEv2/IPsec solution
- Provide an SDWAN Quantum Resistant option
- Provide US Government a cryptographically diverse solution between ASA/FTD and IOS-XE

Pathway to QR Minimum Viable Product

RFC 8784 Compliance for
IKEv2

Cisco SKIP integration for
Quantum Key Distribution

Near term focus on RFC
9242 and 9370

RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Establishes the ability to deposit a PPK between two devices and have IKEv2 use that key for security establishment

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

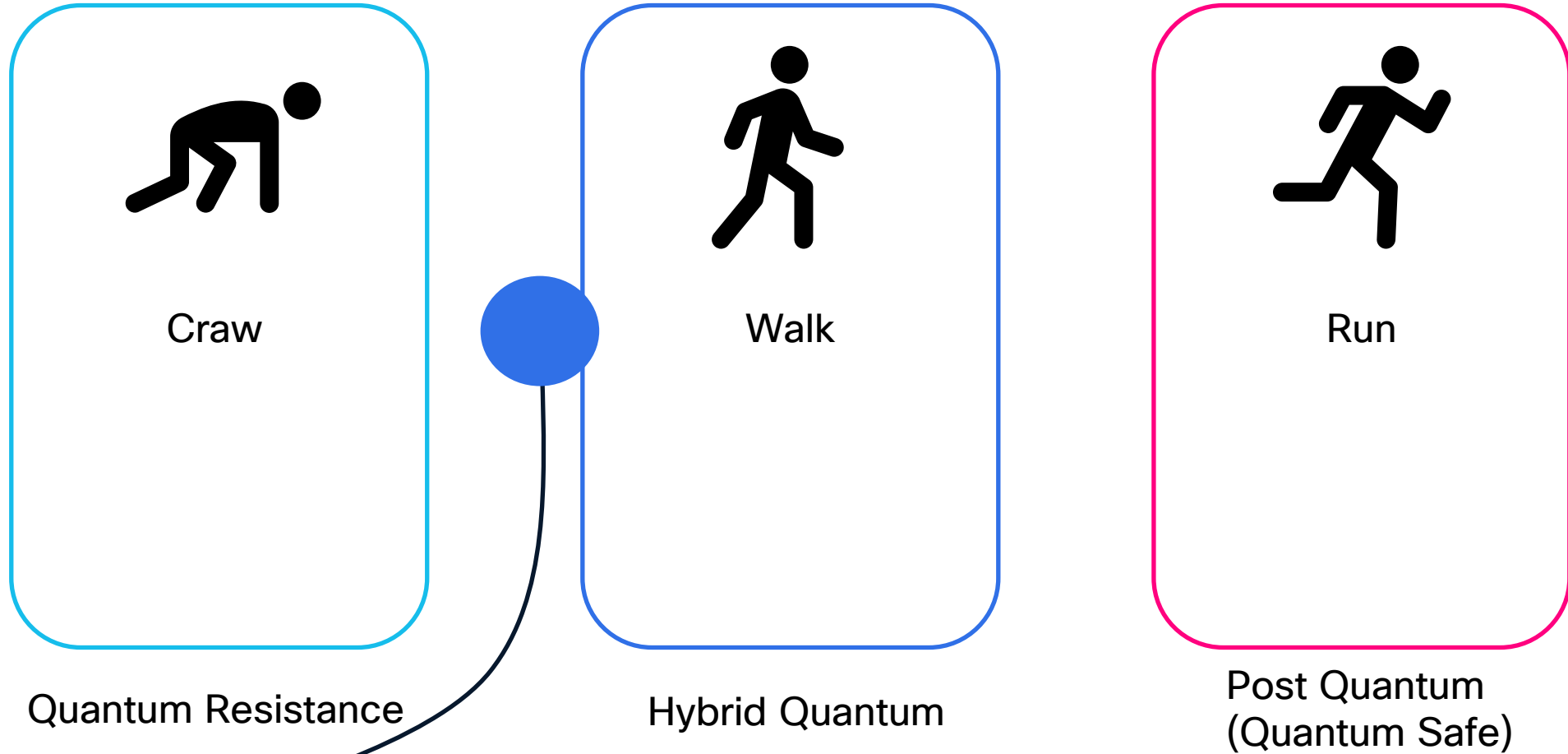


Run

- 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



We are here today

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+



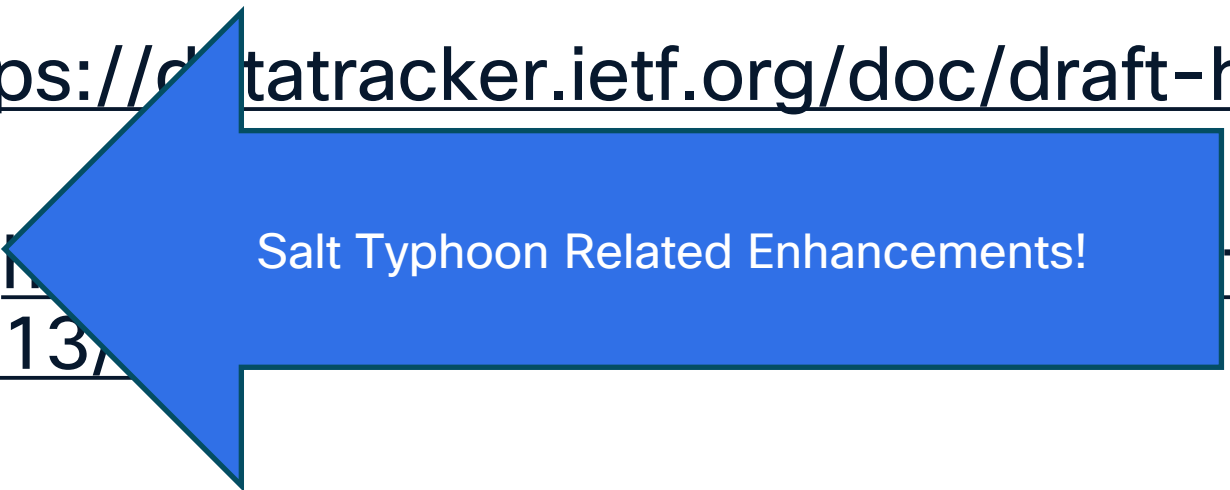
Post-Quantum Roadmap for IOS-XE

US Intelligence Community, US Department
of Defense, Five Eyes, NATO

Andrew Benhase

Supporting IETF RFCs

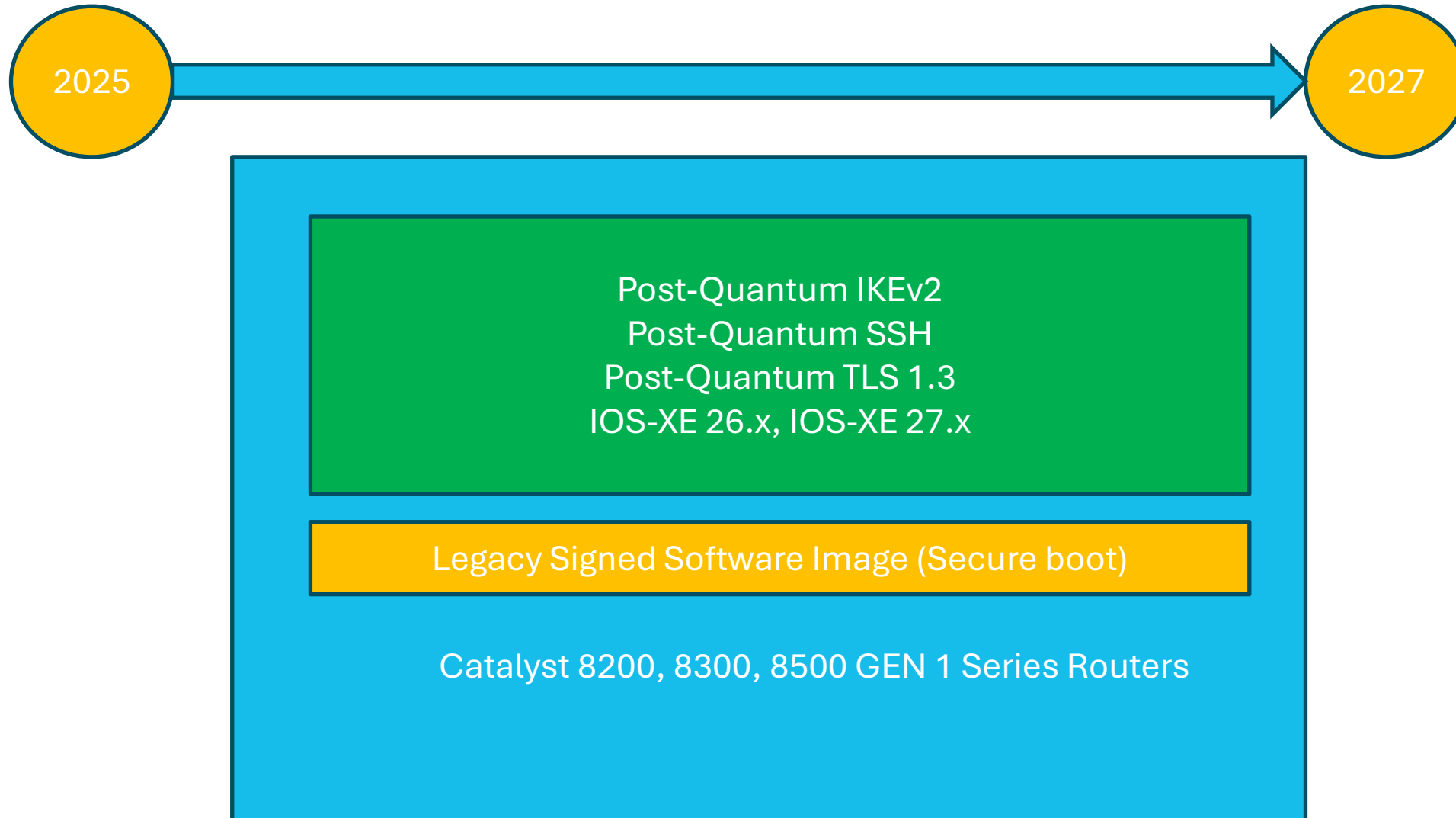
- IPSEC: <https://datatracker.ietf.org/doc/draft-guthrie-cnsa2-ipsec-profile/>
- TLS: <https://datatracker.ietf.org/doc/draft-becker-cnsa2-tls-profile/01/>
- SSH: <https://datatracker.ietf.org/doc/draft-becker-cnsa2-ssh-profile/>
- ML-KEM SSH - <https://datatracker.ietf.org/doc/draft-harrison-mlkem-ssh/>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



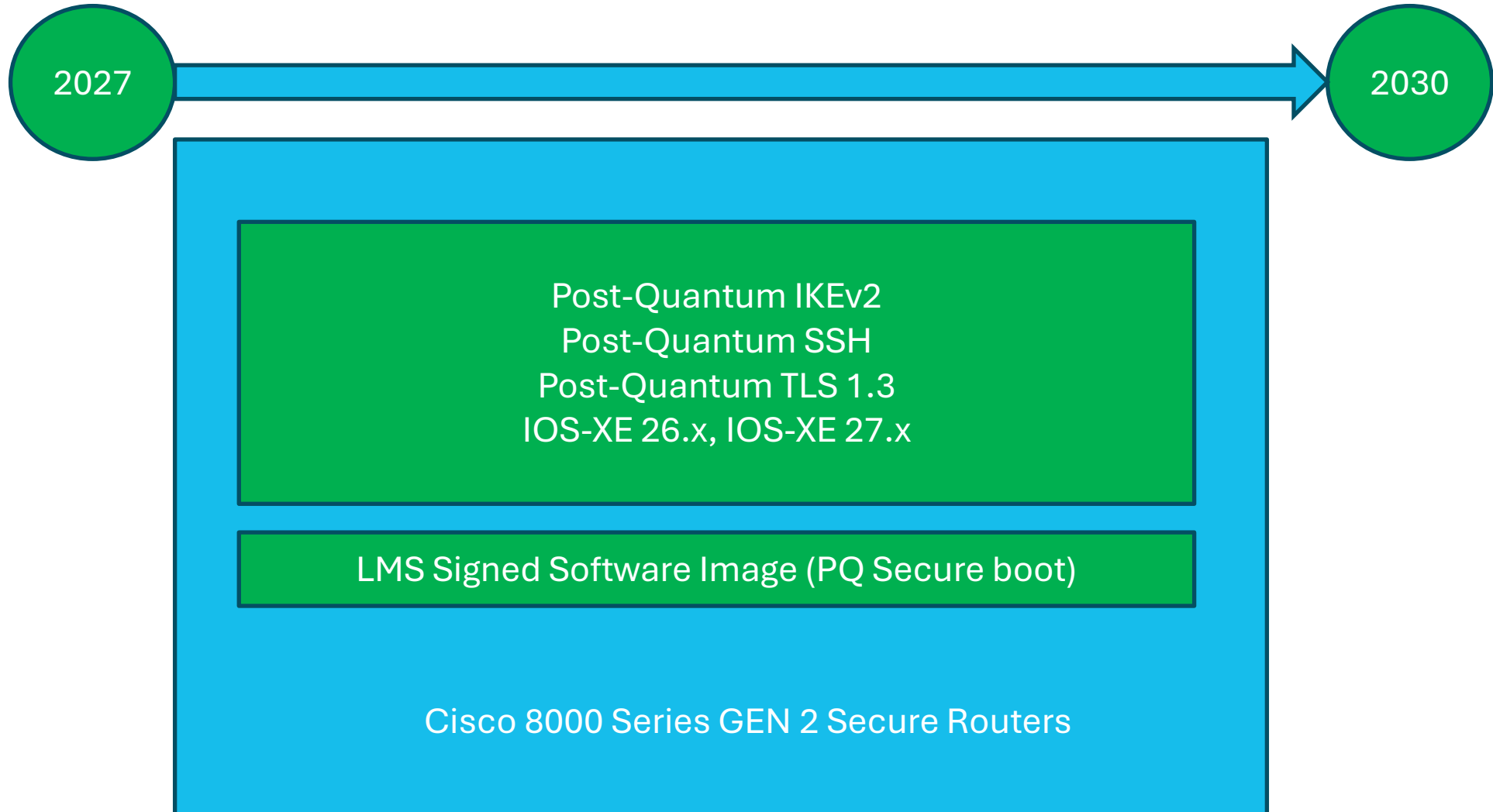
Salt Typhoon Related Enhancements!

[ft-ietf-opsawg-tacacs-tls13/](https://datatracker.ietf.org/doc/draft-ietf-opsawg-tacacs-tls13/)

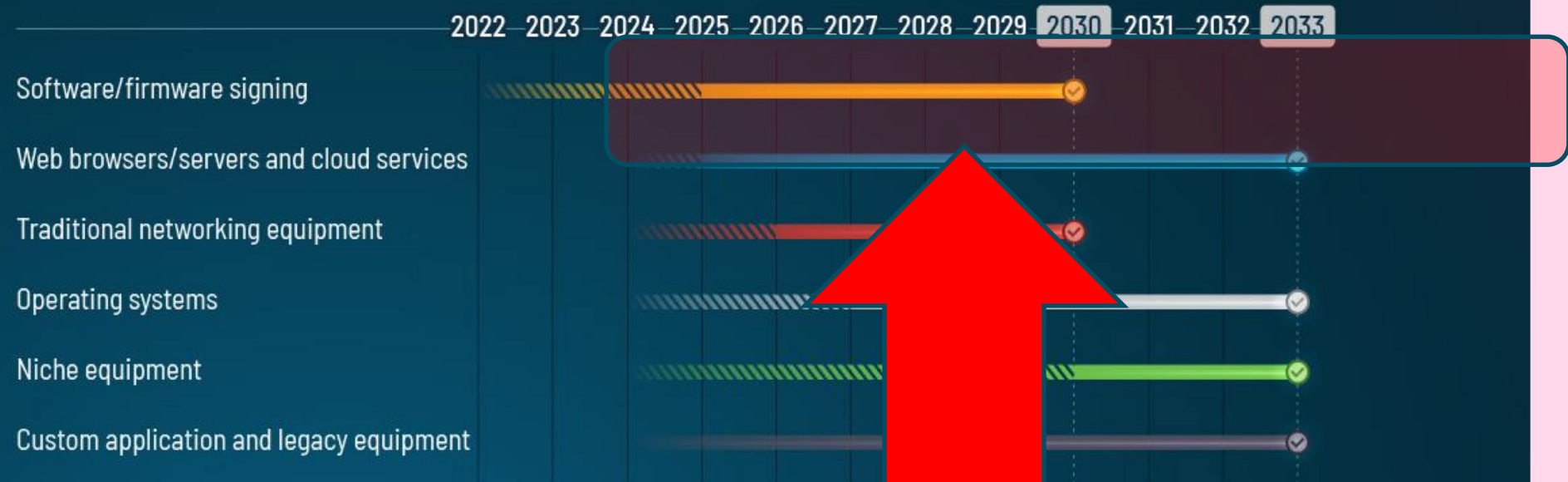
What is a Cat8k Hybrid Quantum Solution?



What is a Cisco 8000 Series Secure Routers Post Quantum Solution?

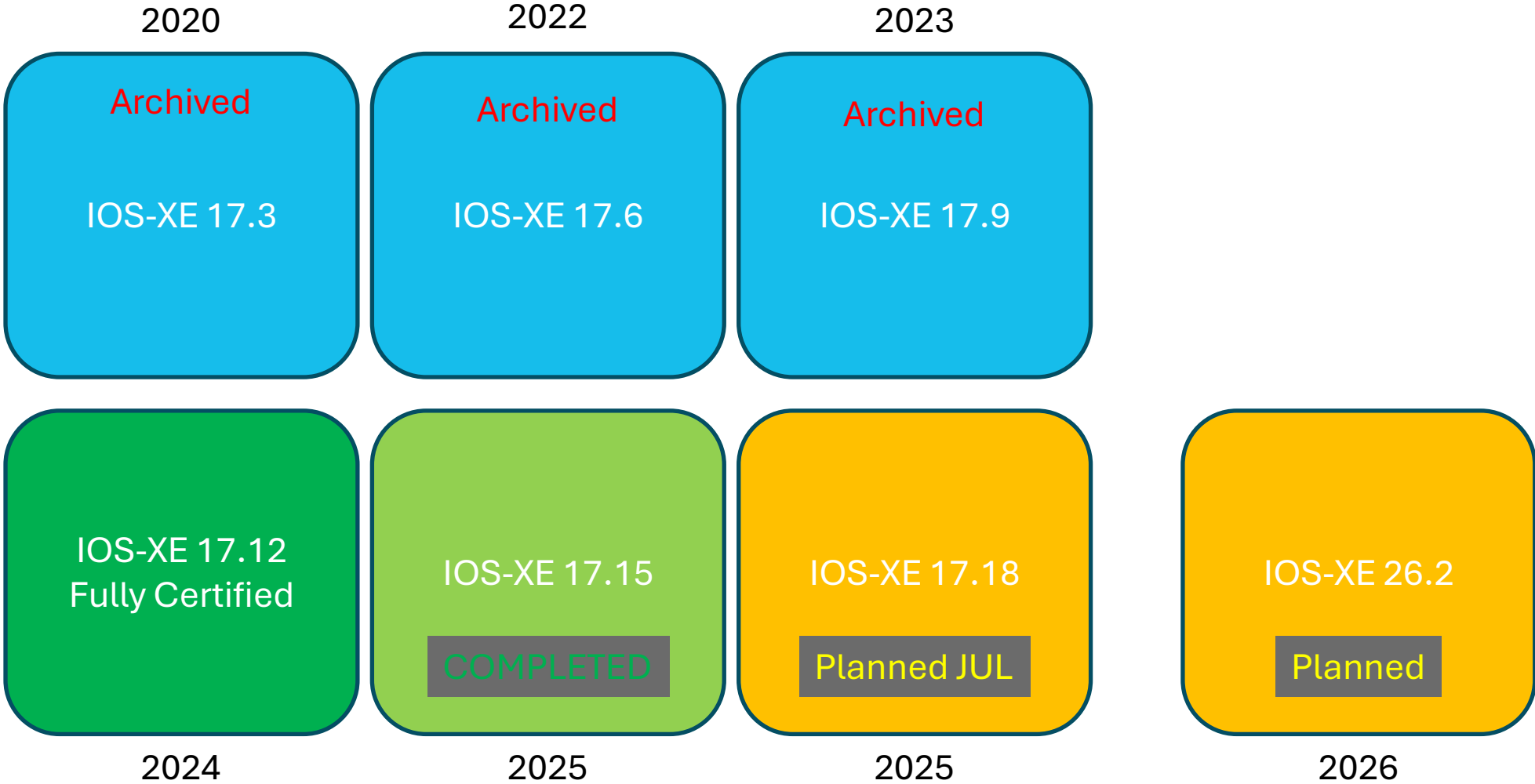


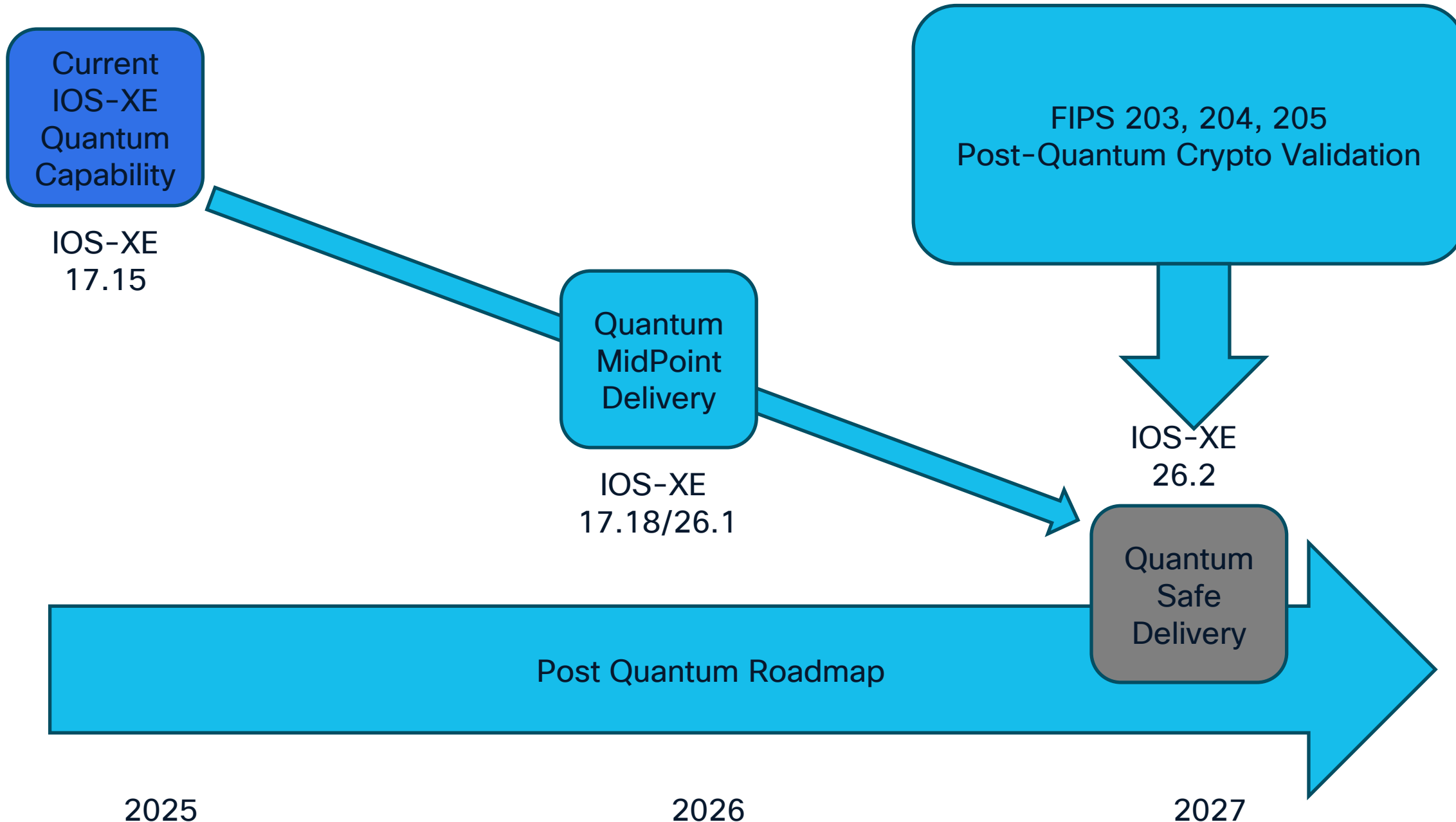
CNSA 2.0 Timeline



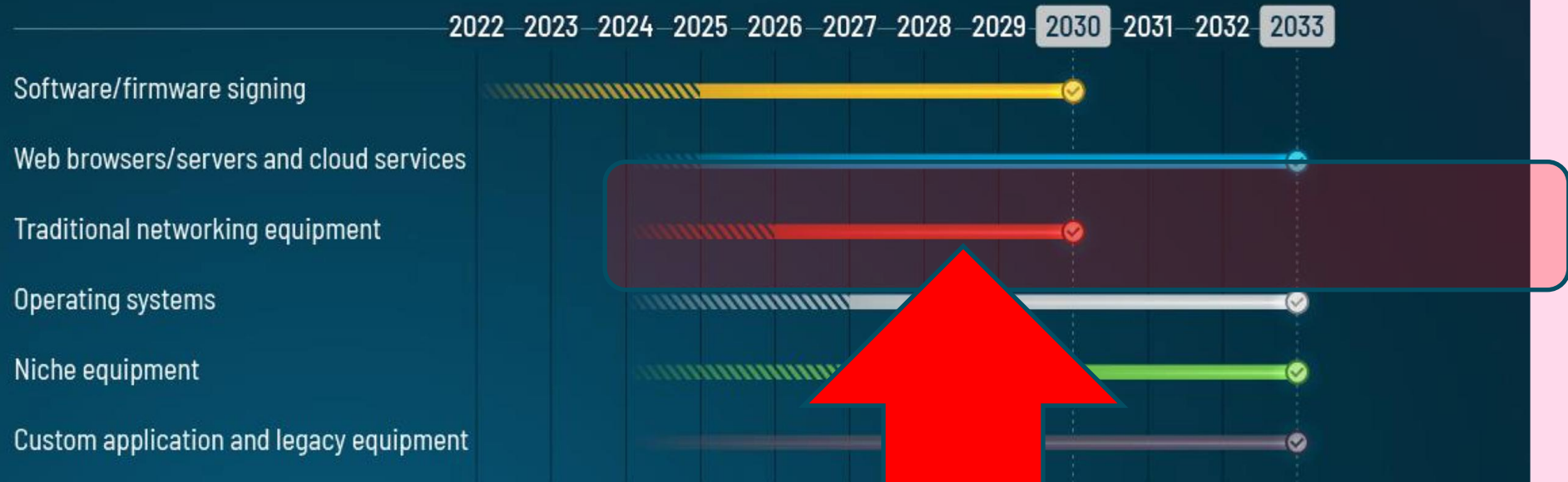
- Offered as an option and tested
- the default and preferred
- use CNSA 2.0 by this year

Constant Certification of IOS-XE





CNSA 2.0 Timeline



led as an option and tested
the default and preferred
se CNSA 2.0 by this year

Quantum Safe Cryptography And Why You Need it

cisco Live !

Andrew Benhase
Solutions Engineer, US Public Sector
@social

Craig Hill
Distinguished Solutions Engineer, US Public Sector
@netwrkr95

Post-Quantum Encryption Solutions @Cisco...

What is real?

Quantum Safe Cryptography And Why You Need it

cisco Live !

Andrew Benhase
Solutions Engineer, US Public Sector
@social

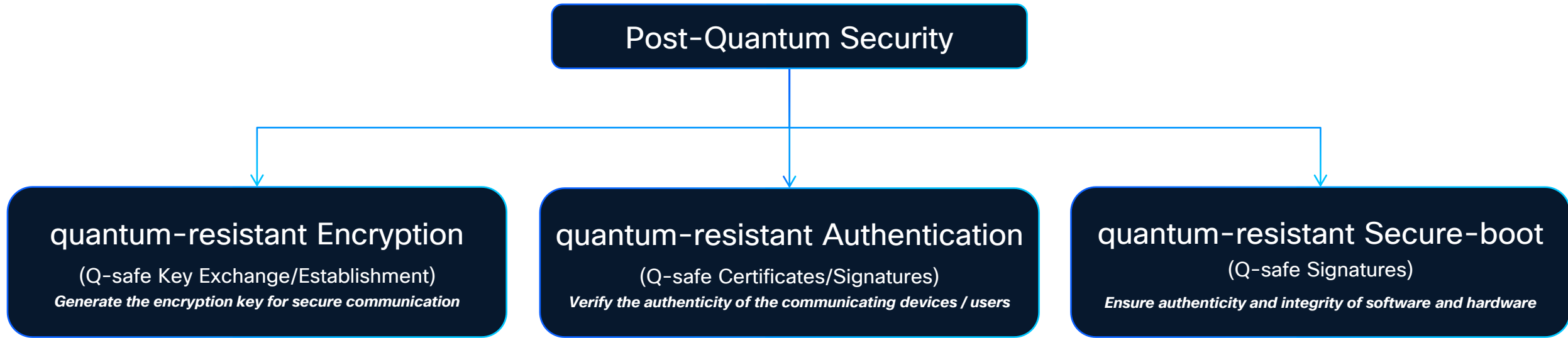
Craig Hill
Distinguished Solutions Engineer, US Public Sector
@netwrkr95

Post-Quantum Encryption Solutions @Cisco...

What is real?

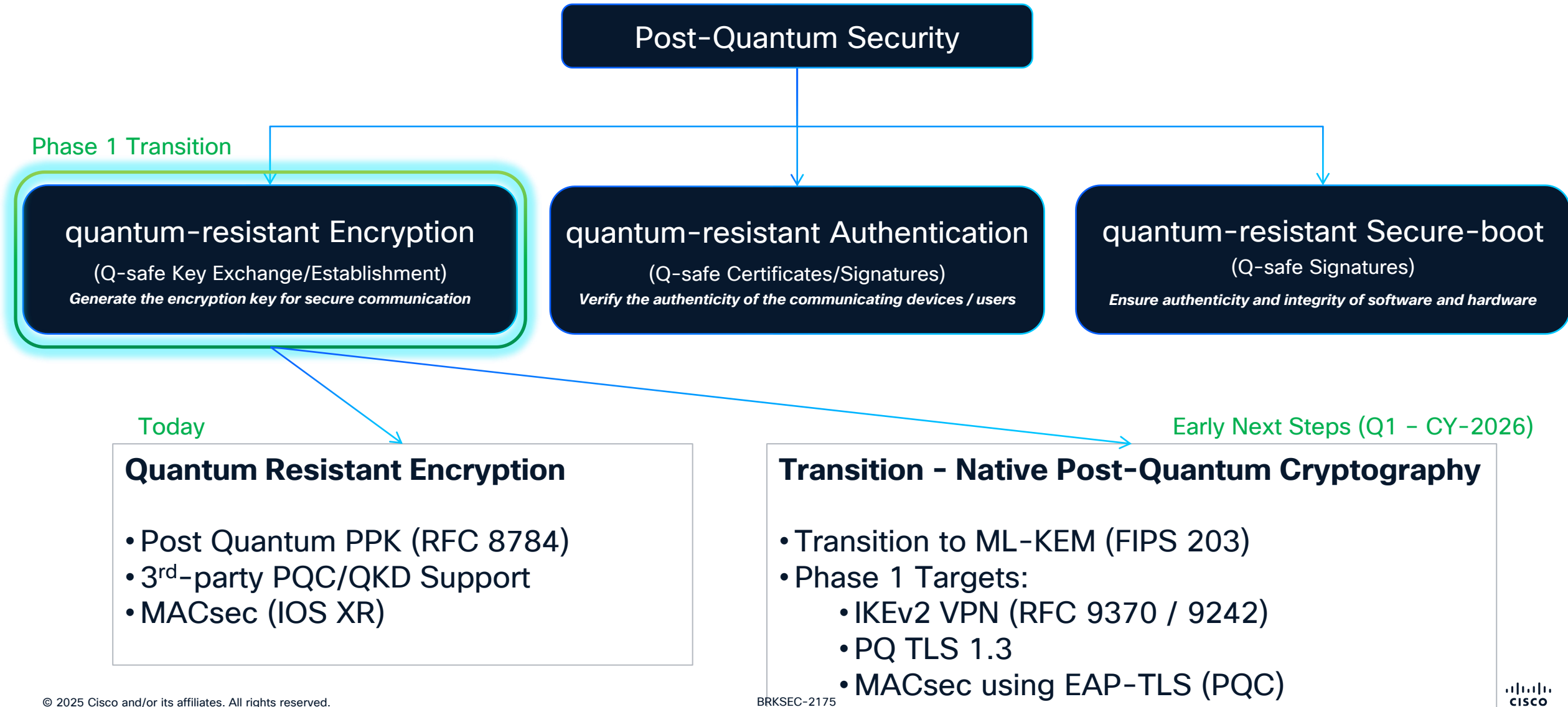
The Transition to Post-Quantum...

Post-Quantum 'Encryption + Authentication + Secure-boot'



The Transition to Post-Quantum...

Post-Quantum 'Encryption + Authentication + Secure-boot'



What is Real @ Cisco - Agenda

- 01 Foundational Components to a Quantum Resistant Architecture
- 02 Overview of the Currently Supported Quantum Resistant Solutions
- 03 Introduction on the Transition to Native PQC Algorithms
- 04 Preview of Supported Roadmaps
- 05 Summary / Reference Docs

What is Real @ Cisco - Agenda

- 01 Foundational Components to a Quantum Resistant Architecture
- 02 Overview of the Currently Supported Quantum Resistant Solutions
- 03 Introduction on the Transition to Native PQC Algorithms
- 04 Preview of Supported Roadmaps
- 05 Summary / Reference Docs

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

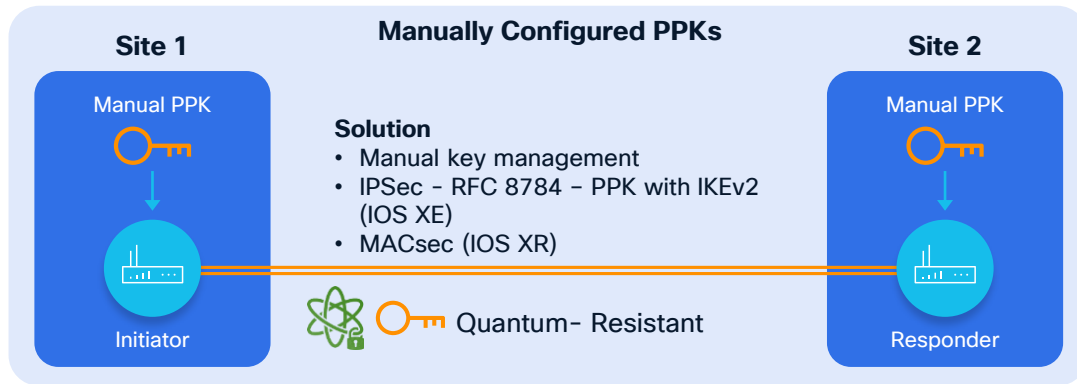
Integrate Evolving Open Standards: Open standards for existing protocols (IETF) and hybrid, encryption ciphers (NIST), Govt Guidelines (ASD / CNSA 2.0)

Quantum Resistant Solutions for IPSec & MACsec

Current Technology and Deployment Options

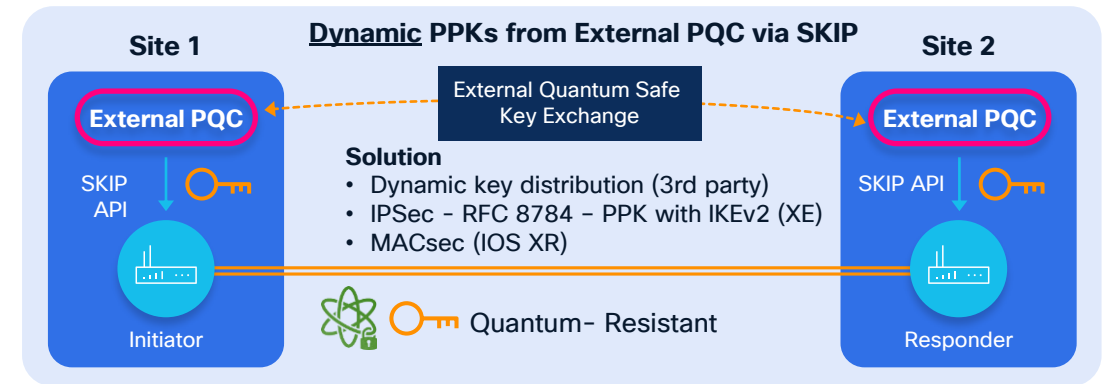
Quantum-Safe Encryption Options – Available Today

Manual Options



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

Dynamic Options



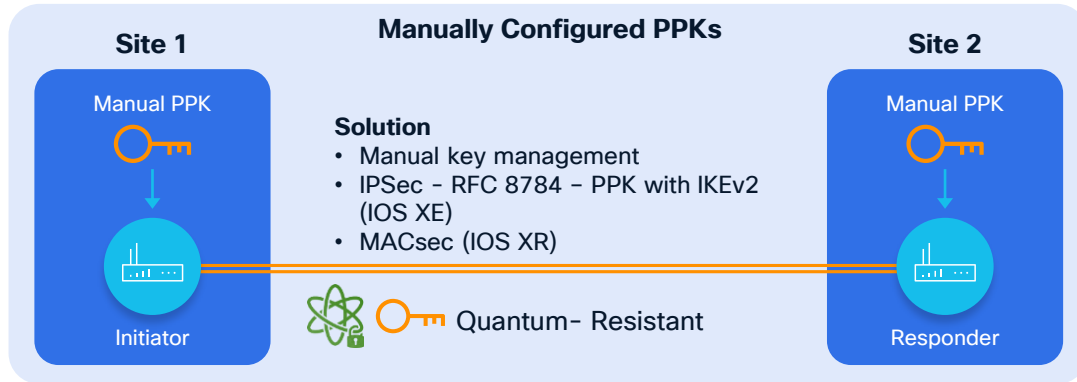
- PPK distribution through 3rd-party key source
- Secure Key Integration Protocol (SKIP) enabler
- Applies to HW or SW based key sources

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

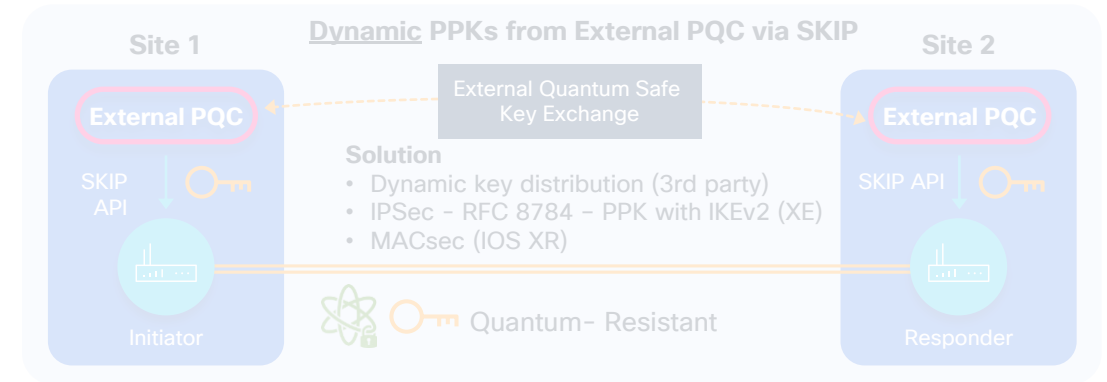
Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

Manual Options



Dynamic Options



Dynamic Network Encryption Options:

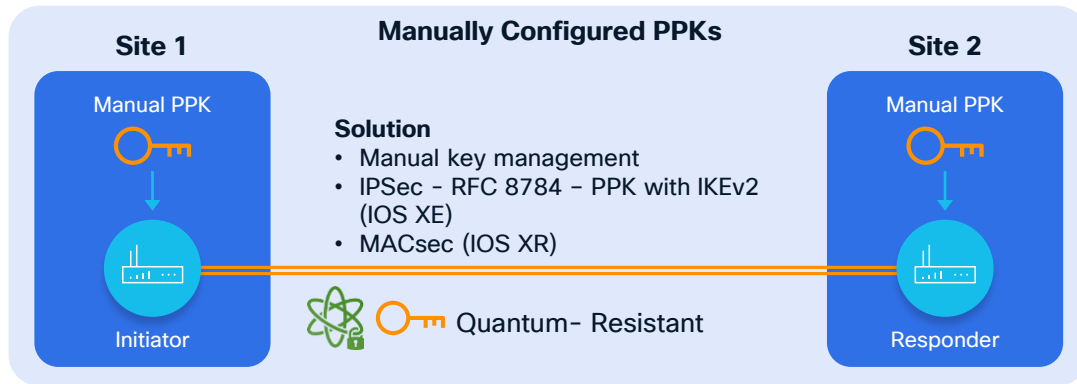
- **IPSec:** RFC 8784 - PPK based IPsec encryption keys
- **MACsec:** PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

Current Technology and Deployment Options

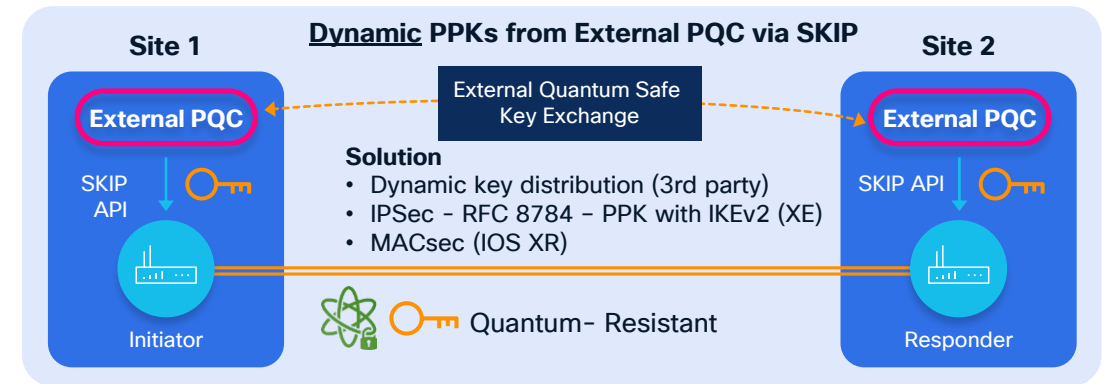
Quantum-Safe Encryption Options – Available Today

Manual Options



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

Dynamic Options



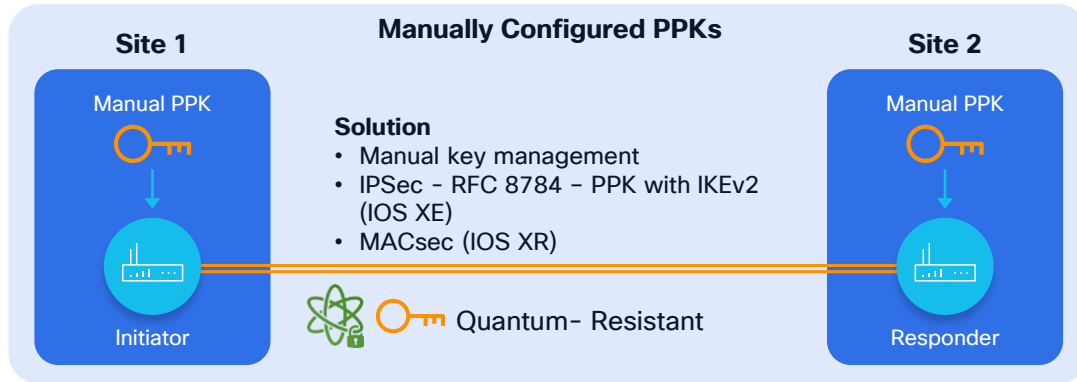
- PPK distribution through 3rd-party key source
- Secure Key Integration Protocol (SKIP) enabler
- Applies to HW or SW based key sources

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

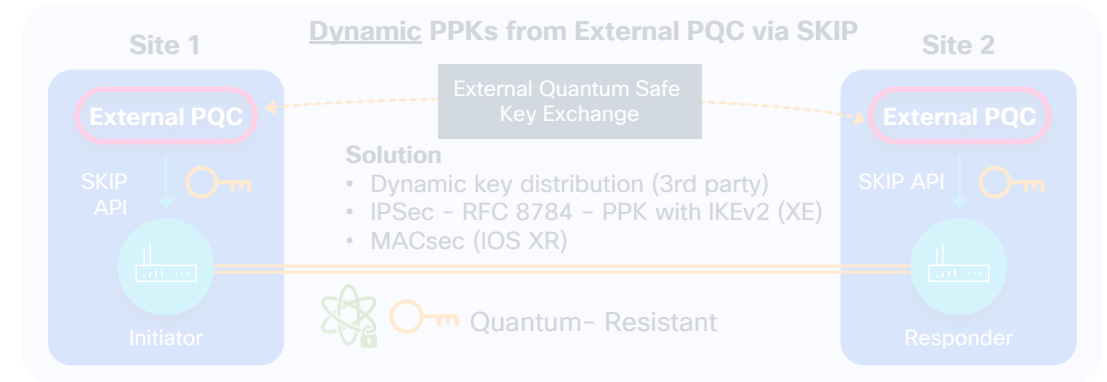
Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

Manual Options



Dynamic Options



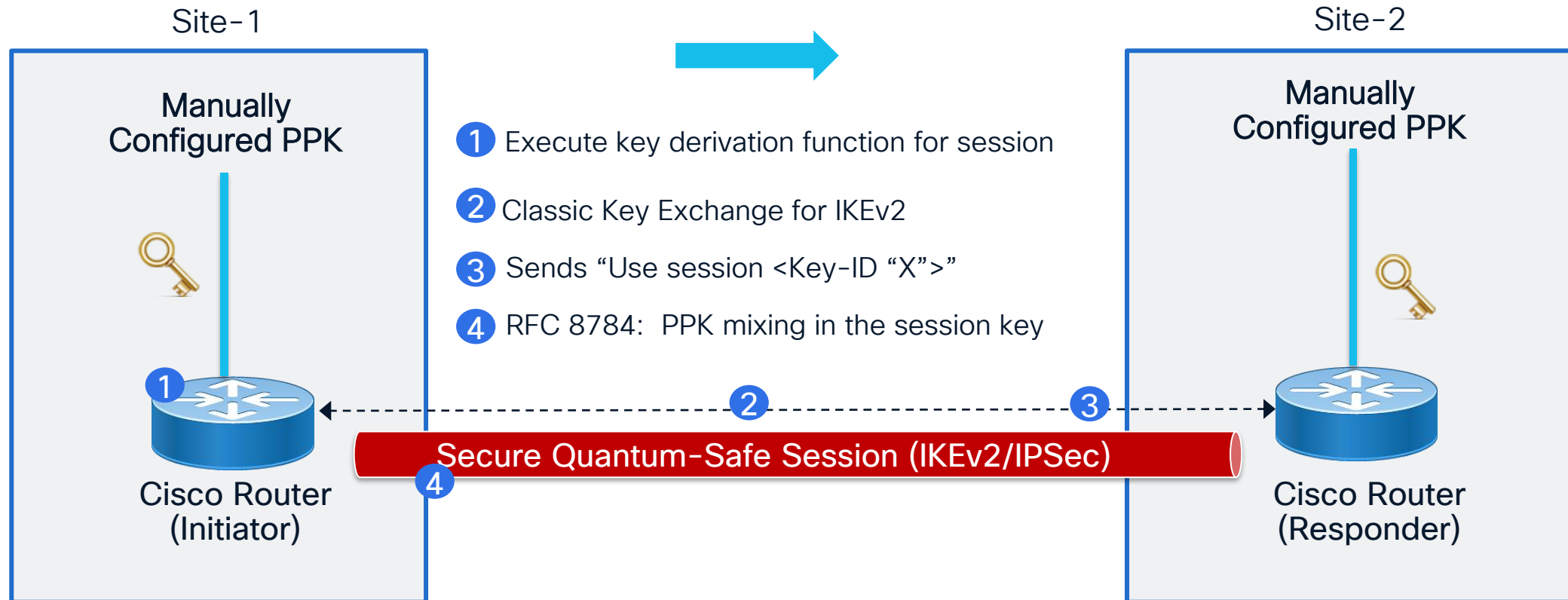
Dynamic Network Encryption Options:

- **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

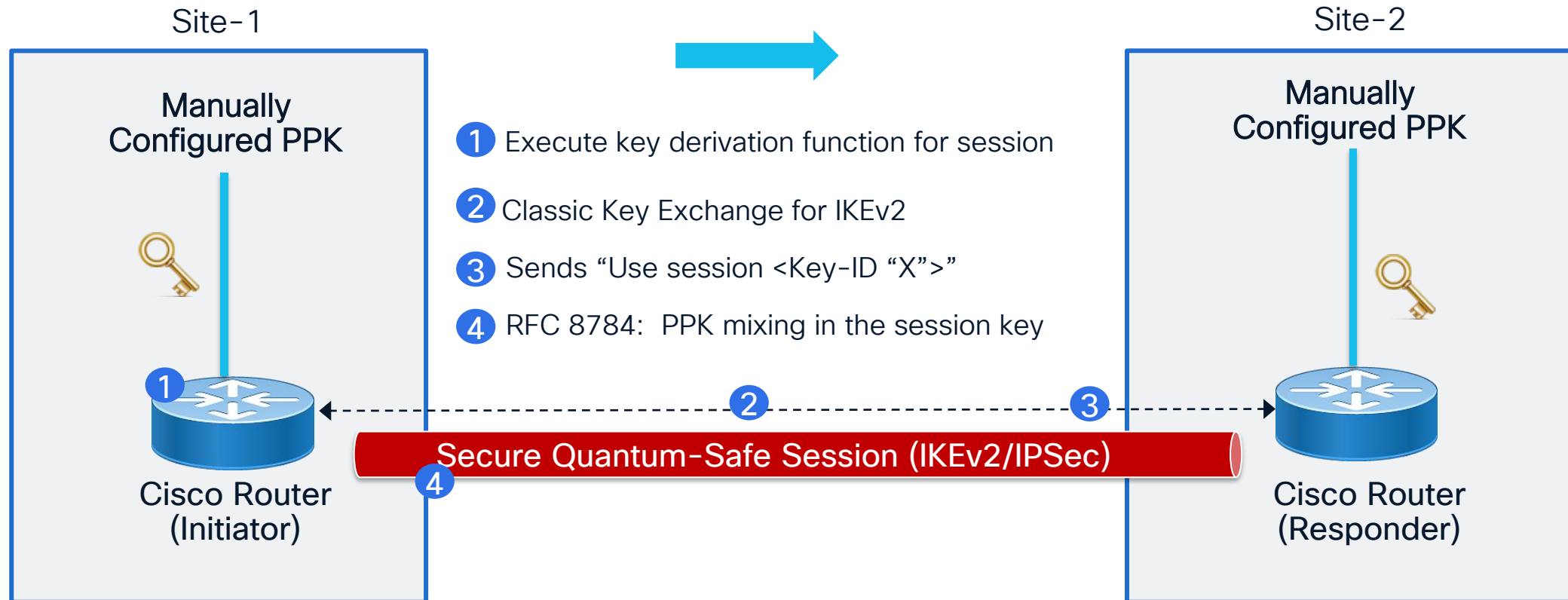


*PQ PPK mix with DH is never transmitted over the wire
(RFC 8784)*

[IOS-XE Support: Since 17.11.1a](#)

RFC 8784 with Quantum-Safe IKEv2/IPSec Session

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

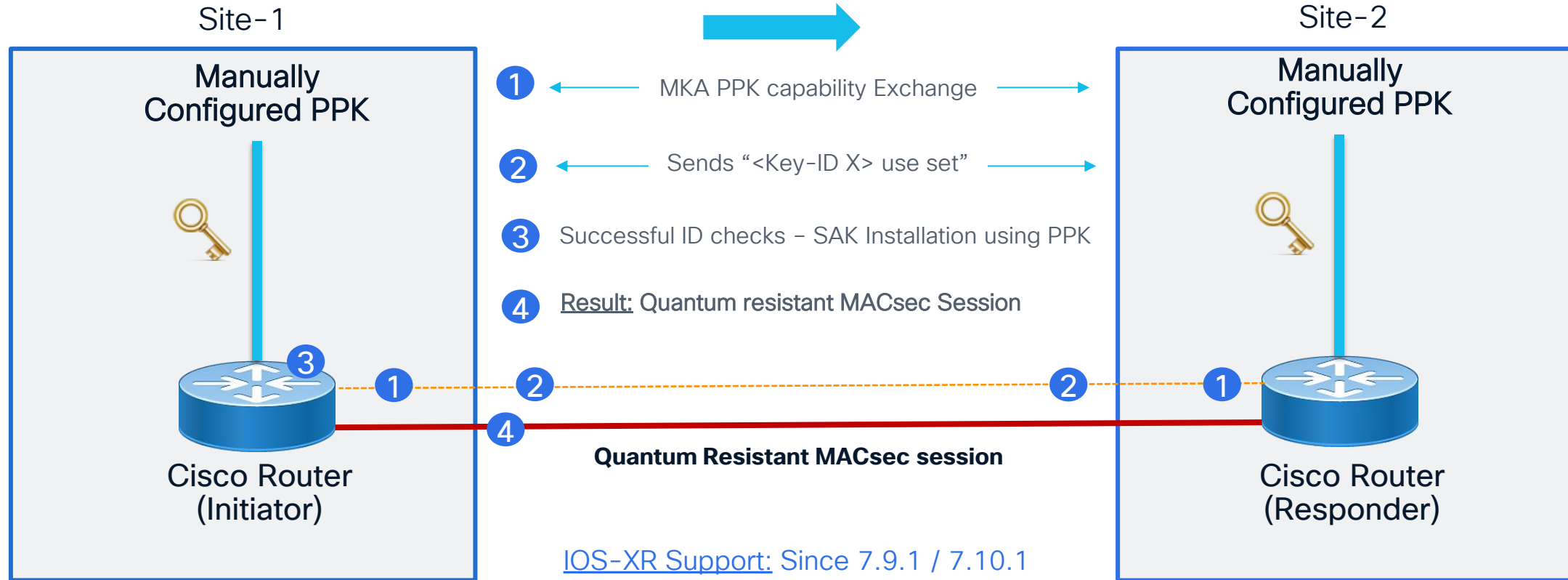


*PQ PPK mix with DH is never transmitted over the wire
(RFC 8784)*

[IOS-XE Support: Since 17.11.1a](#)

Quantum-Safe MACsec with Preshared Keys

Example - Manual PPK for MACsec

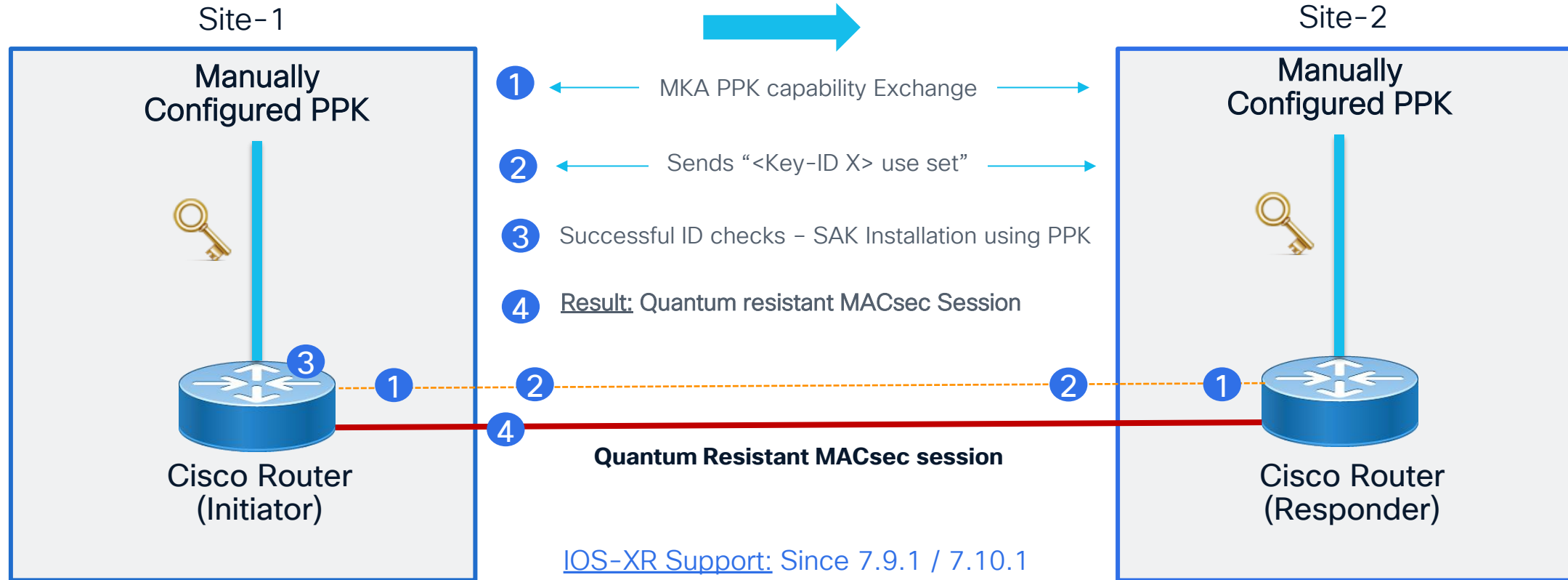


- **Extensions to MKA are applied** to carry the PPK_ID as the SAK identifier (instead of the secret HW key)

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)

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**

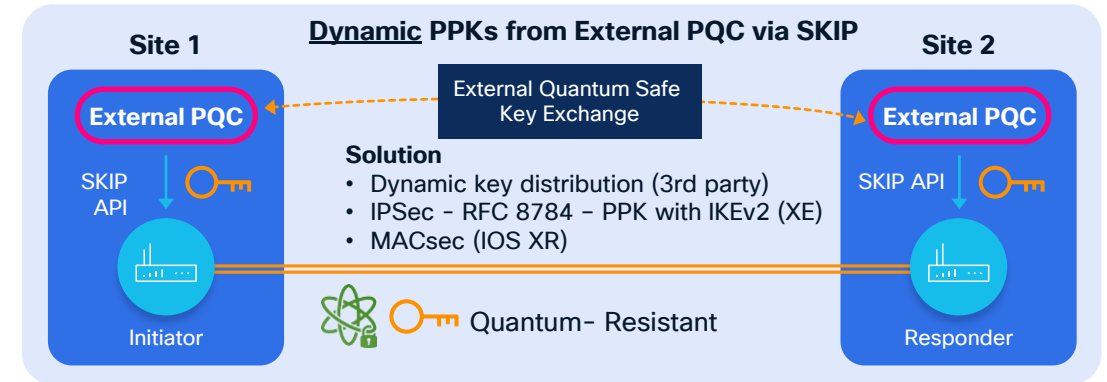
Current Technology and Deployment Options

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

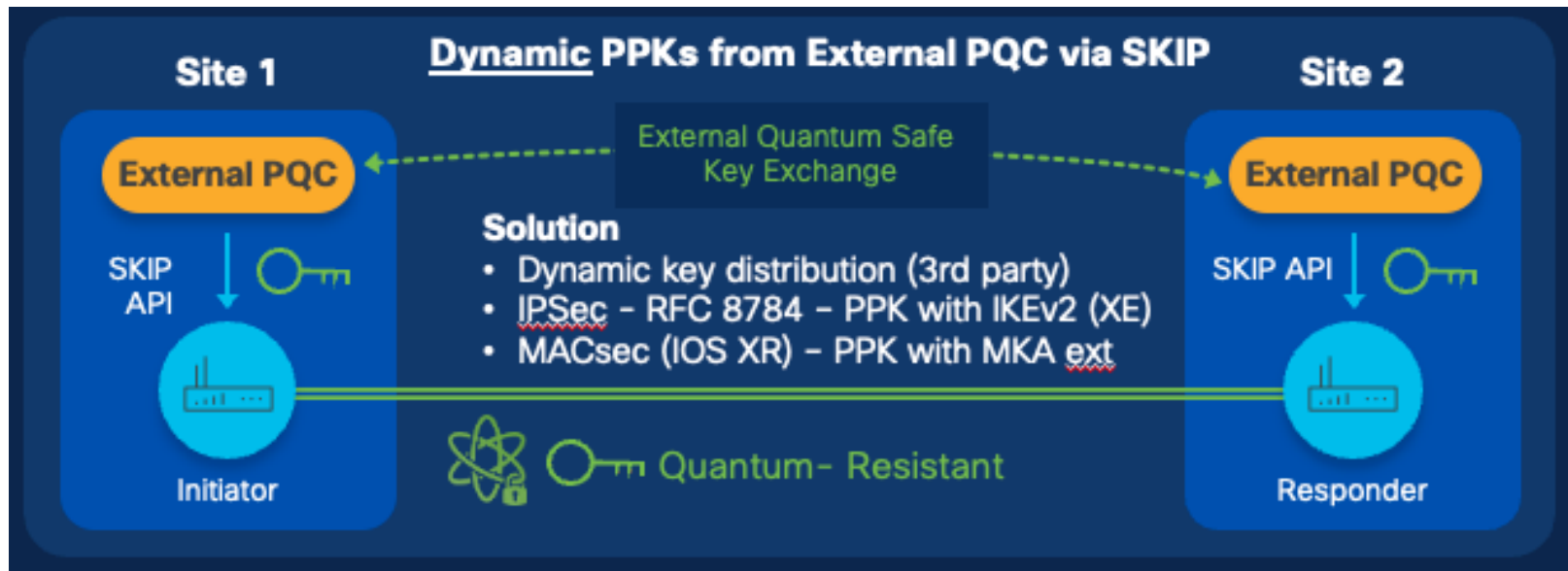
PPK = Postquantum Preshared Keys

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)



Early IETF Draft Submission for SKIP

Workgroup: Internet Engineering Task Force
Internet-Draft: draft-cisco-skip-01
Published: 2 March 2025
Intended Status: Informational
Expires: 3 September 2025

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

Secure Key Integration Protocol (SKIP)

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-01>

Post-Quantum Integration Using Dynamic PPK with SKIP

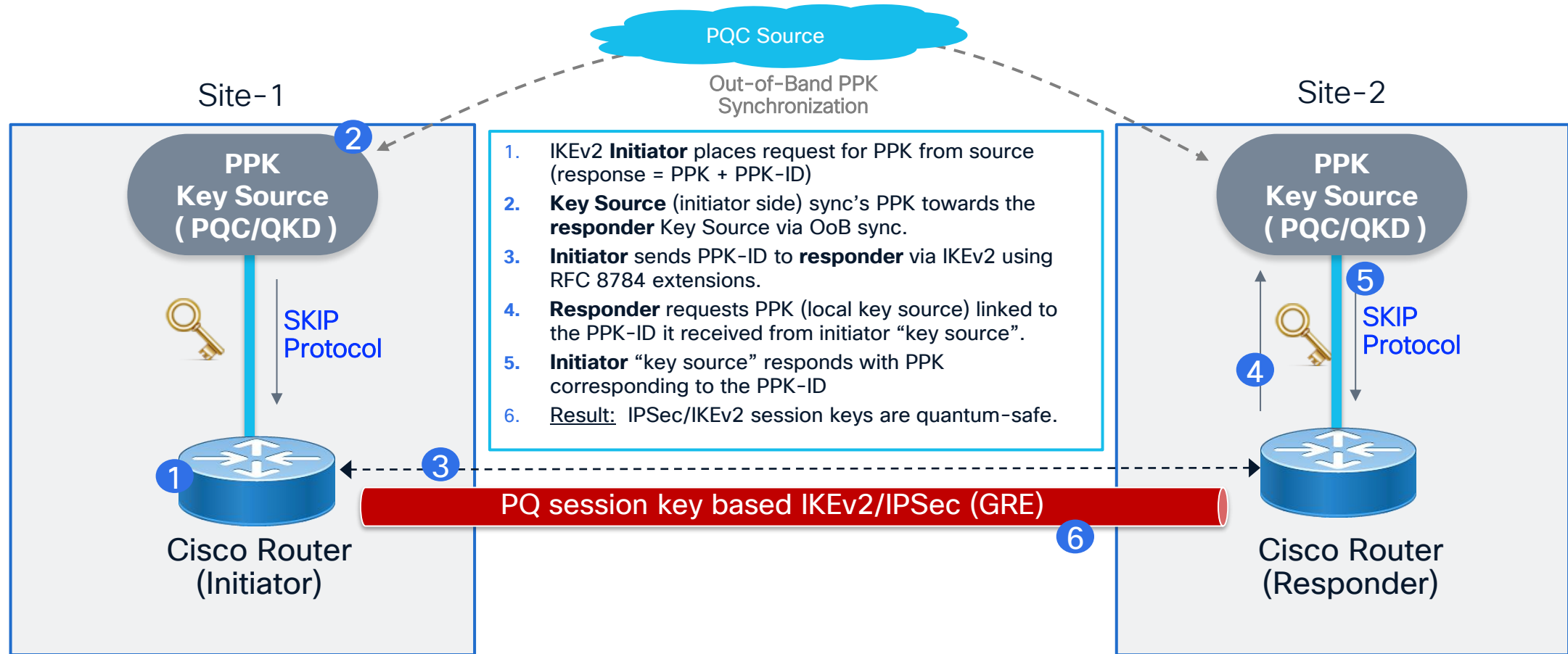
IPSec/IKEv2
MACsec

QuSecure



RFC 8784 with Quantum-Safe IKEv2/IPSec Session

Dynamic PPK Example with SKIP

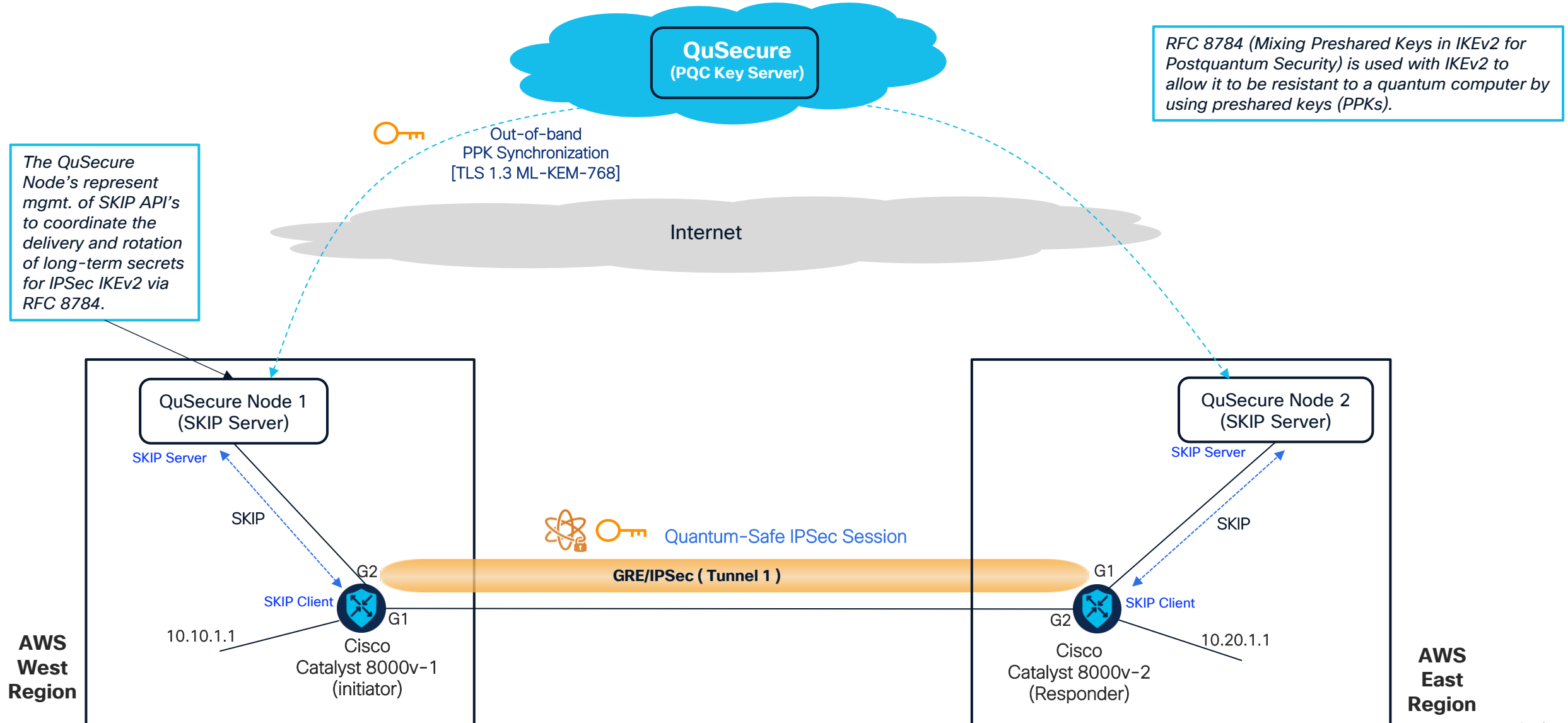


- PPK is never sent over the wire
- Only the PPK-ID is sent and over the OoB channel
- PPK Key Source is responsible for synchronization between both key sources
- SKIP protocol used between key source and routers

PPK = Postquantum Preshared Keys

IPSec/IKEv2 Quantum Safe Demo Using Dynamic PQ Preshared Keys

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



SHOW Output

Cat8Kv_CPN_Ohio#show crypto ikev2 sa detailed

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/f/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 Hill¹, Scott Kawaguchi², and Joey Lupo³

¹Distinguished Architect, Cisco Systems, Inc.

²Chief Architect, QuSecure, Inc.

³Product Security Architect, QuSecure, Inc.

© QuSecure, Inc, February, 2024

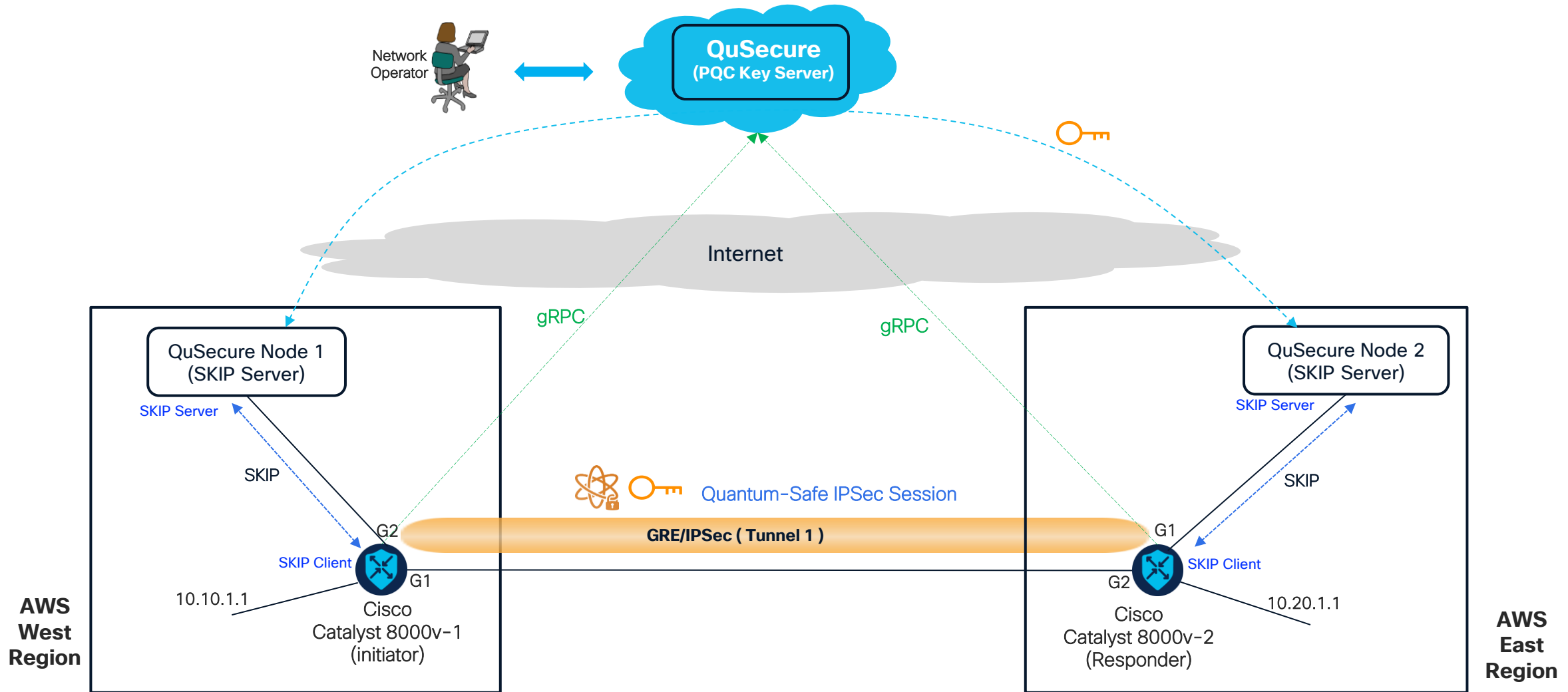
Abstract

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.

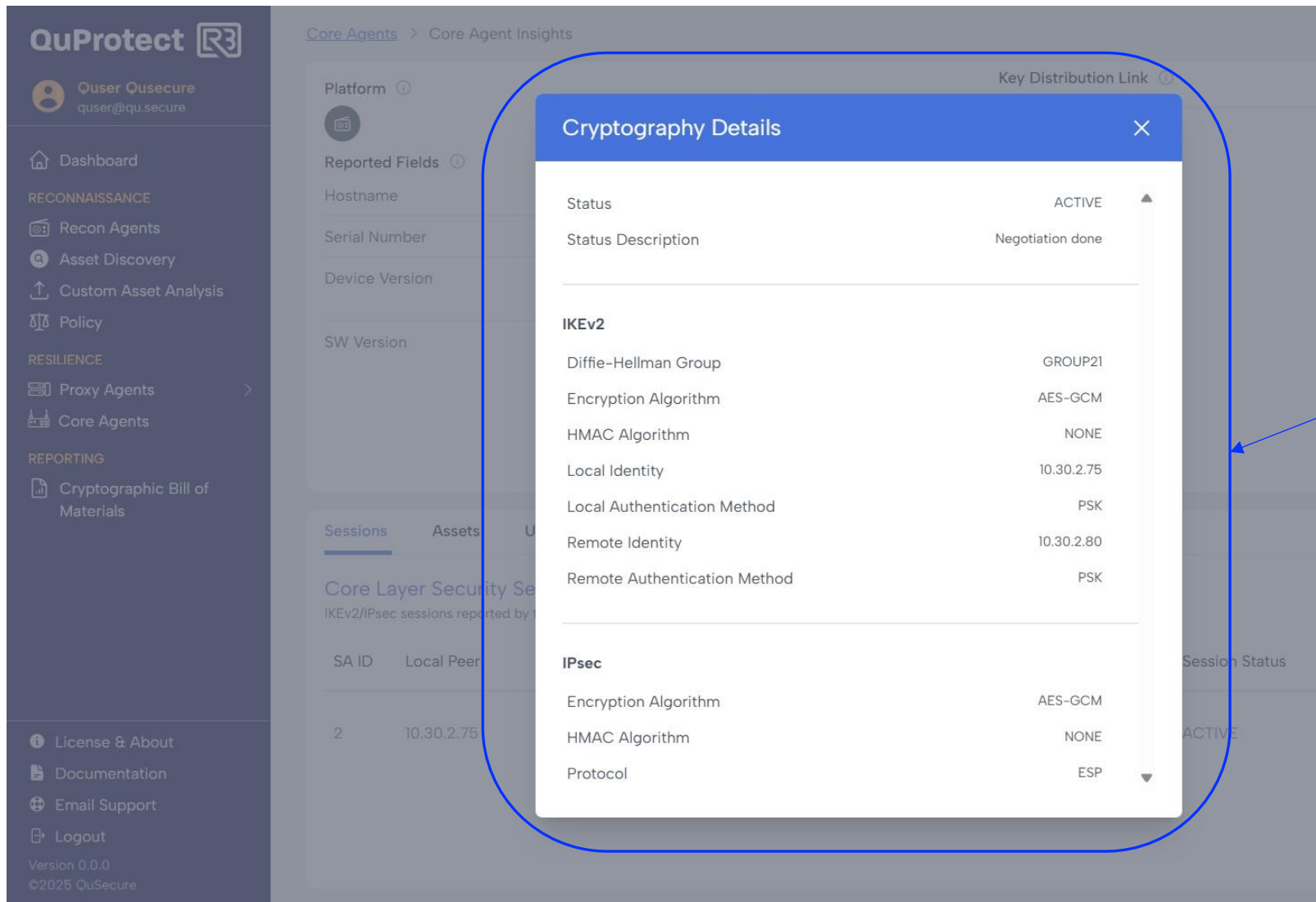
Link to Paper: <https://www.qusecure.com/resources/ipsec-case-study-with-cisco-core-networking/>

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

Leverage Operational YANG Models to Consolidate “Show” Ouput



QuSecure Screen Shots



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

QuSecure Screen Shots

QuProtect

User Ousecure

ouser@qu.secure

Dashboard

RECONNAISSANCE

Recon Agents

Asset Discovery

Custom Asset Analysis

Policy

RESILIENCE

Proxy Agents

Core Agents

REPORTING

Cryptographic Bill of Materials

License & About

Documentation

Email Support

Logout

Version 0.0.0

©2025 QuSecure

Core Agents

Core Agent Insights

meganium-agent-node-0

Edit

Get Bootstrap Config

Delete

Summary

ID GP7HaqKrOQNGvQAPKNiv...

Created On 10/30/2025, 3:20:29 PM

Last Updated On 10/30/2025, 3:23:08 PM

Cluster: meganium

Platform

Reported Fields

Hostname meganium-router-0

Serial Number JAB1303001C

Device Version Cisco Catalyst 8000V Edge Embedded Services Processor

SW Version Cisco IOS Software [IOSXE], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.13.1a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
Compiled Wed 13-Dec-23 21:43 by mcpre

Health Overview

Agent Orchestrator Link Connected
Connected an hour ago

Updates (Sync) Updated

Key Distribution Link Connected
Connected a day ago

Network Element Uptime 3 months

Sessions

Assets

Updates

Settings

Core Layer Security Sessions Overview

IKEv2/IPsec sessions reported by the network element

SA ID	Local Peer	Remote Peer	Session Status	Cryptography Status	
4	10.30.2.124	meganium-agent-node-1 10.30.2.138	ACTIVE	Secure 1 Optimization	View

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

Post-Quantum IOS-XR Demo Topology

MACsec + SKIP using External Key Source

Thanks to Lab Contributors:

Chennakesava Reddy Gaddam

Rakesh Kandula

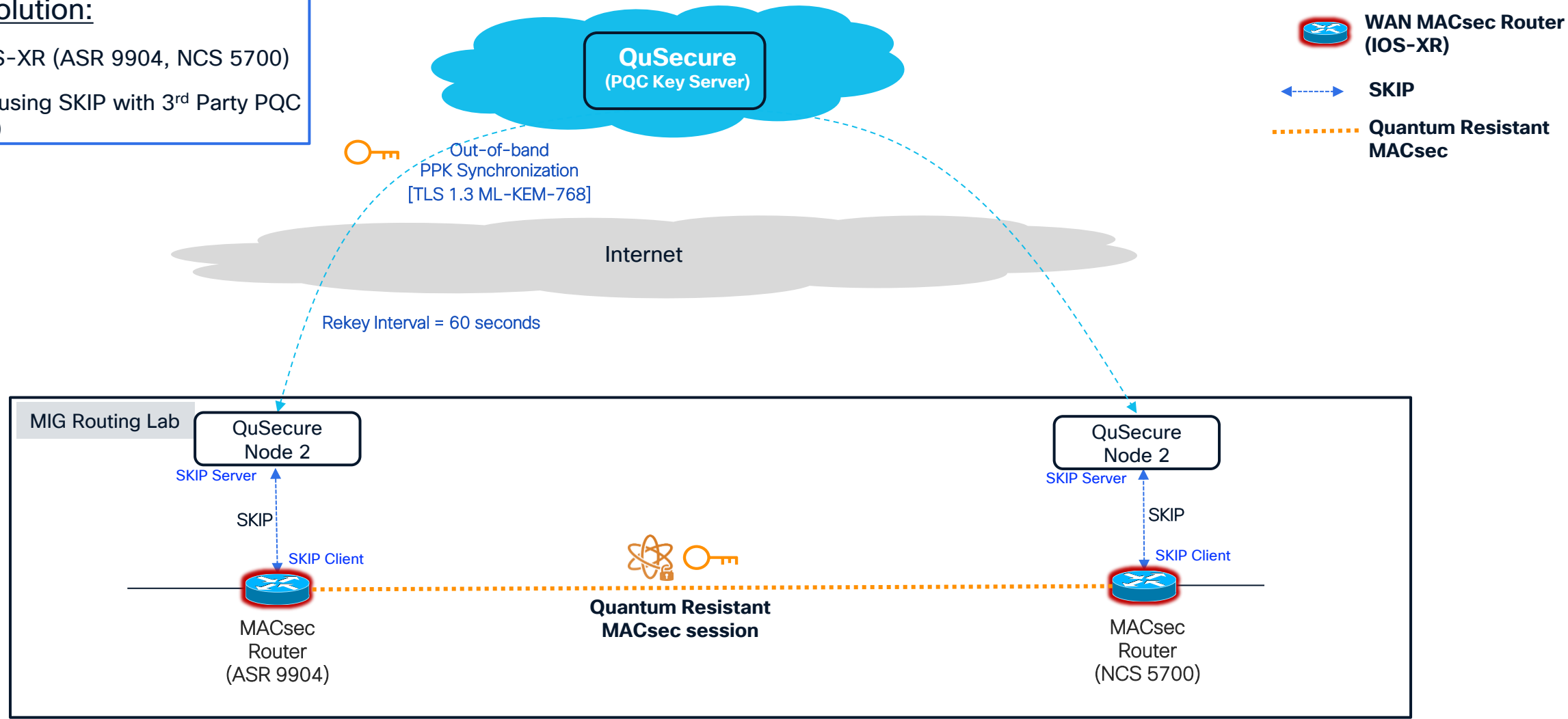
Joey Lupo (QuSecure)

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  
!  
!
```

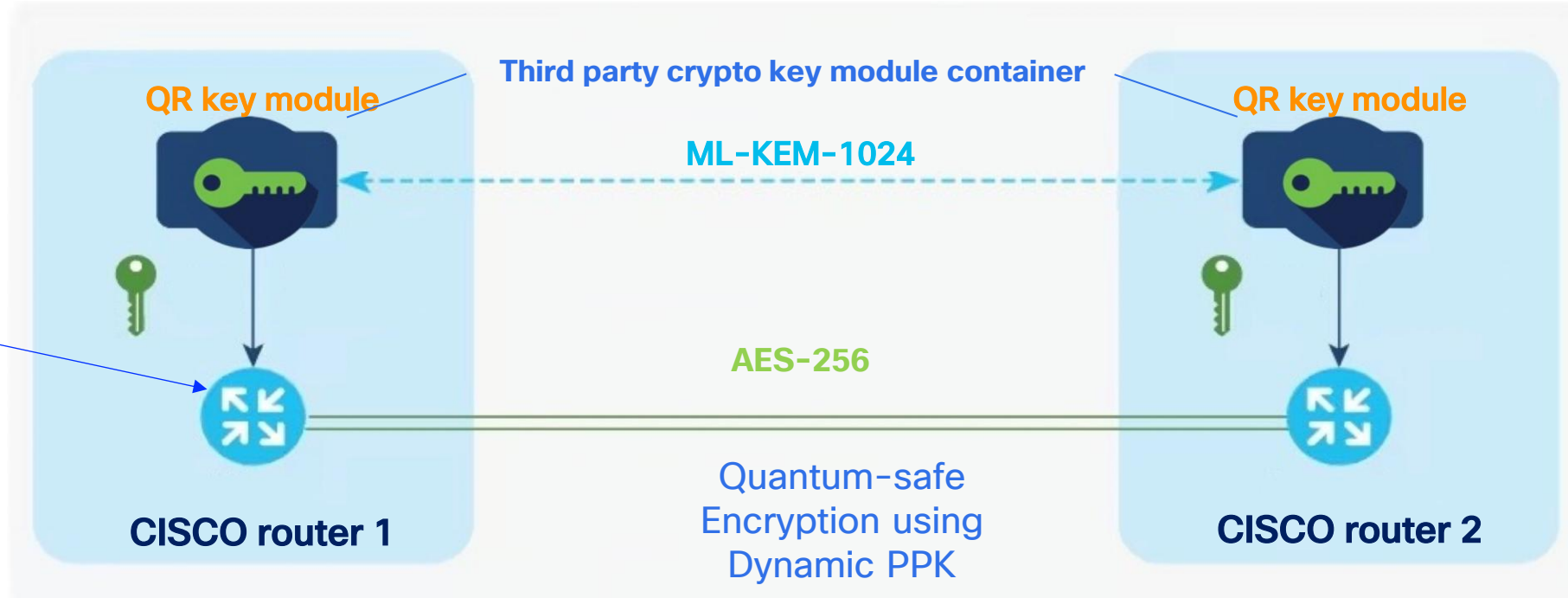
Shows Remote Dynamic PQC Server
(“quprotect-core” is the dynamic key
server [QuSecure PQC])

IPSec & MACsec Using Dynamic PPK

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



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

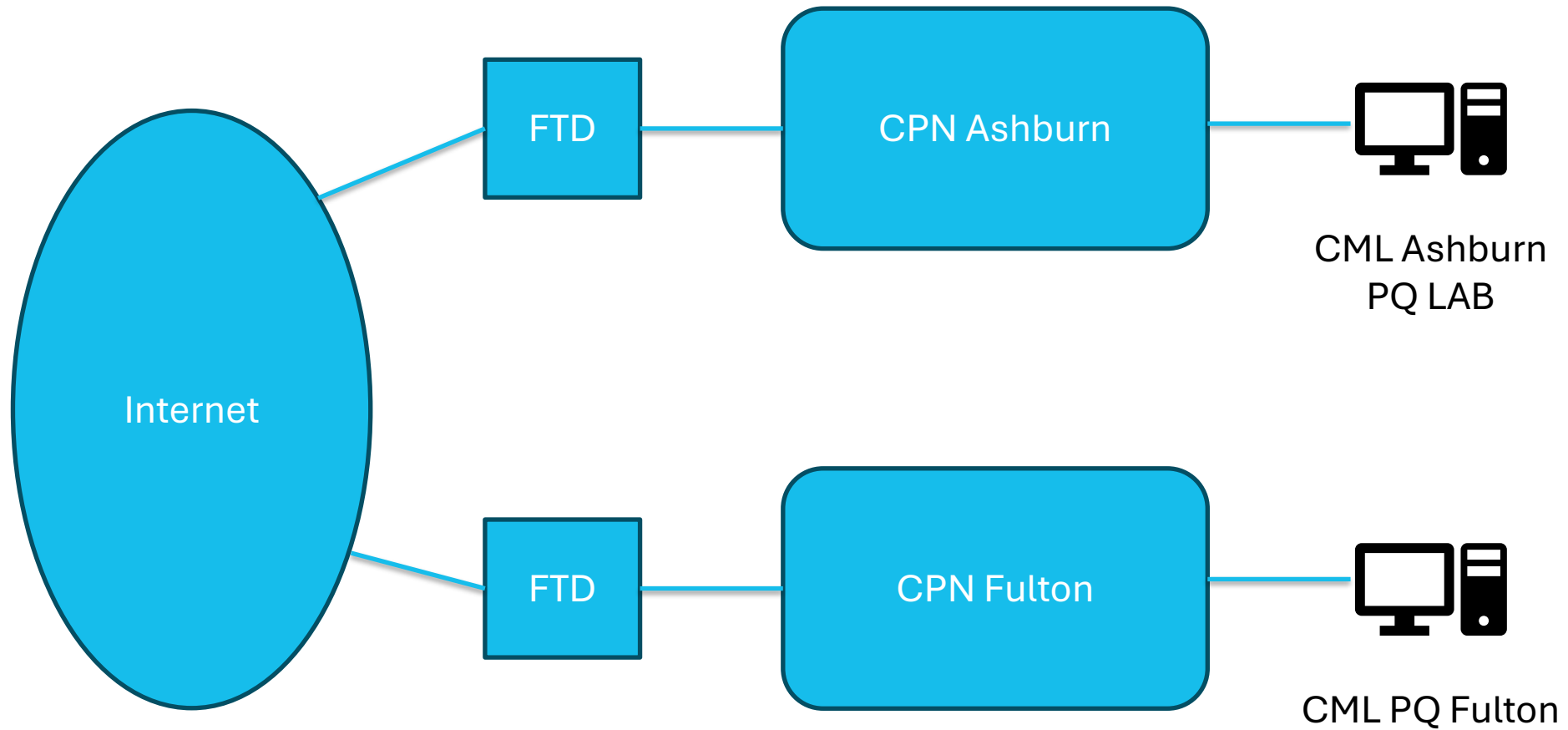


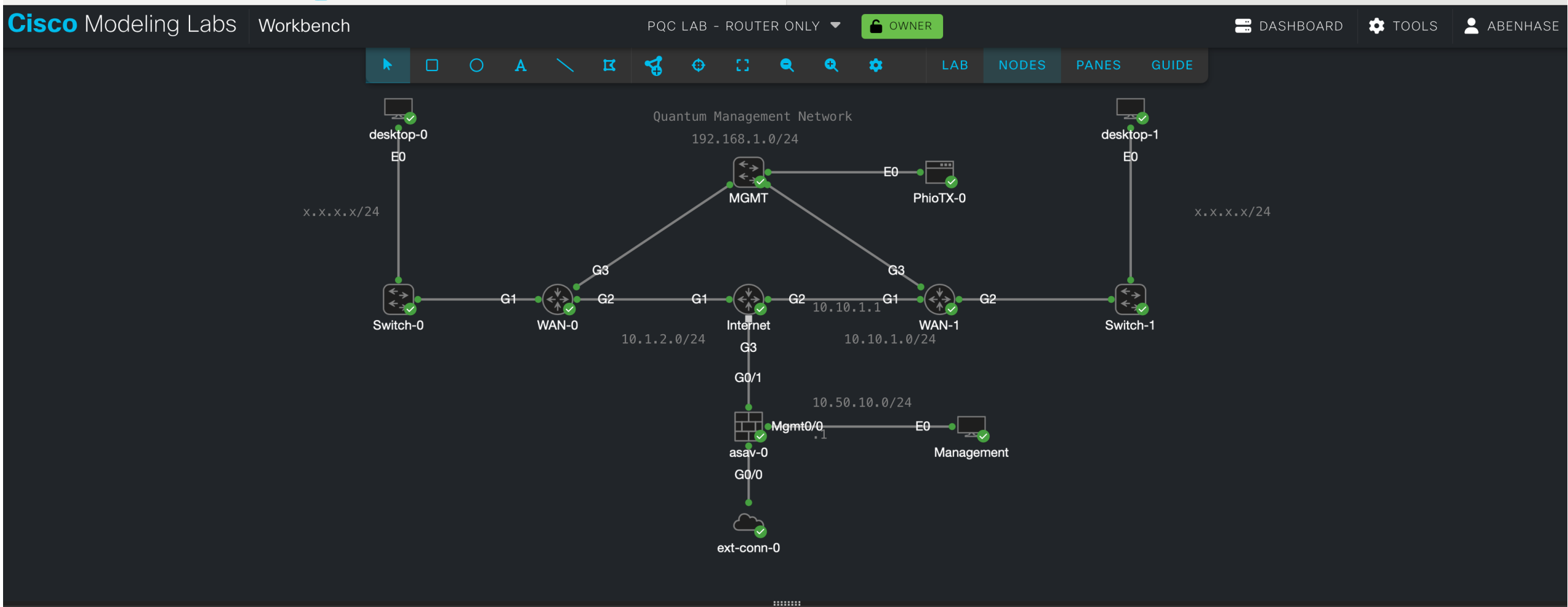
- FIPS 203 ML-KEM-1024 validated
- Dynamic PPK – IPSec (RFC 8784), MACsec
- Catalyst 8000 w/ host App (IPsec verified)
- ASR 9000 & NCS 5K (MACsec verified)

- 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)

Transition To Native PQC Algorithms

Cisco Post Quantum CML Lab





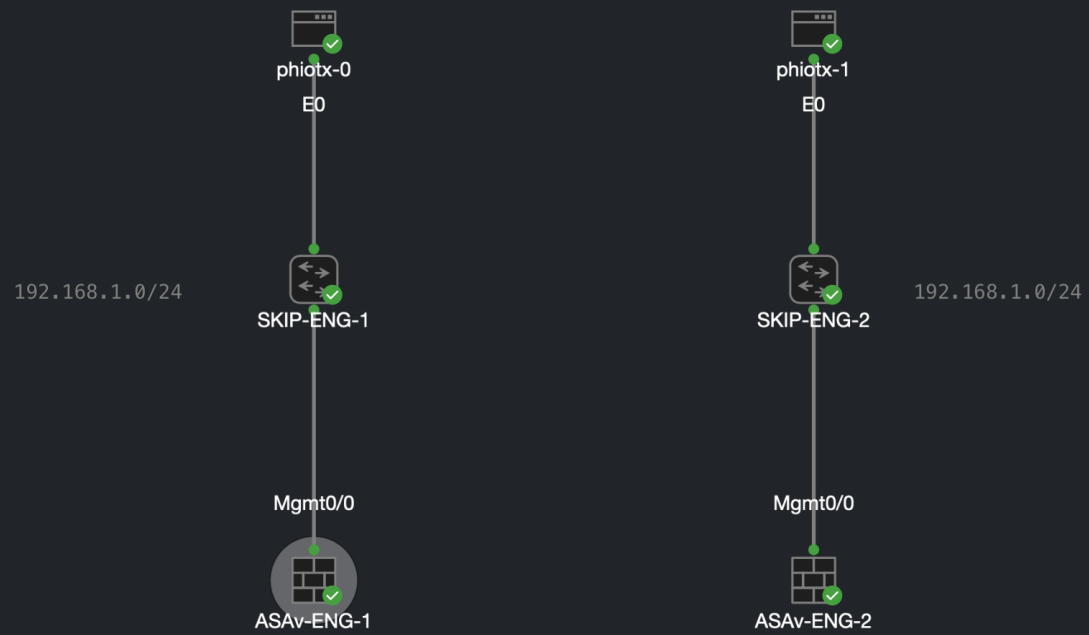
LAB

NODES

PANES

GUIDE

QXC SKIP Engineering
ASAv Engineering Build



Bangalore SKIP Engineering with Quantum Exchange

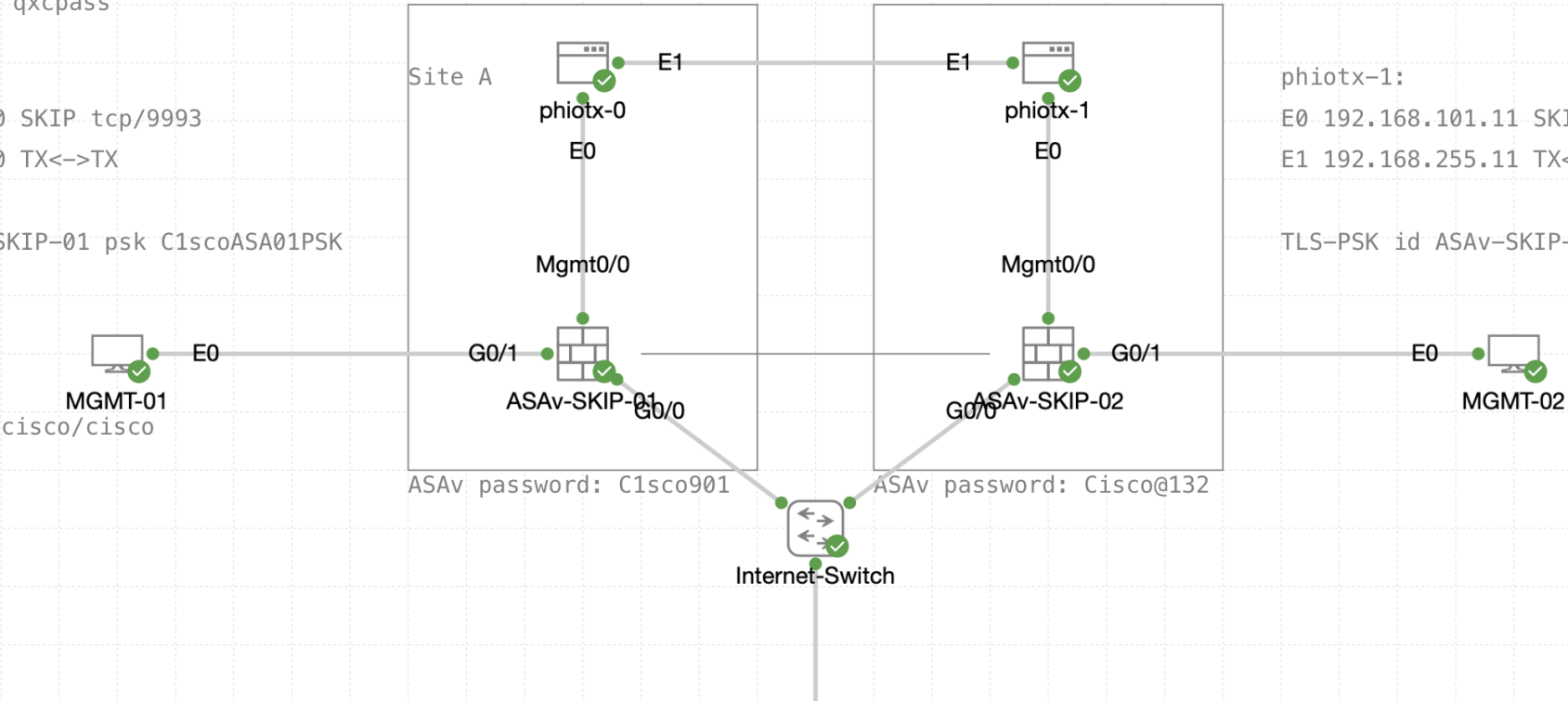
Phio TX Container:
qxc/"qxcpass"

phiotx-0:
E0 192.168.100.10 SKIP tcp/9993
E1 192.168.255.10 TX<->TX

TLS-PSK id ASAv-SKIP-01 psk C1scoASA01PSK

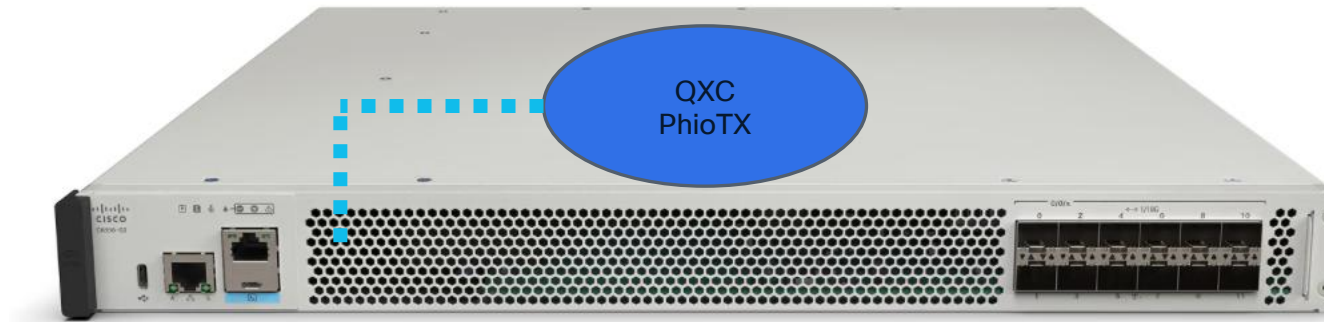
phiotx-1:
E0 192.168.101.11 SKIP tcp/9993
E1 192.168.255.11 TX<->TX

TLS-PSK id ASAv-SKIP-02 psk C1scoASA02PSK



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>

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 !

