Introduction to 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

BRKSEC-2175

Cisco Webex App

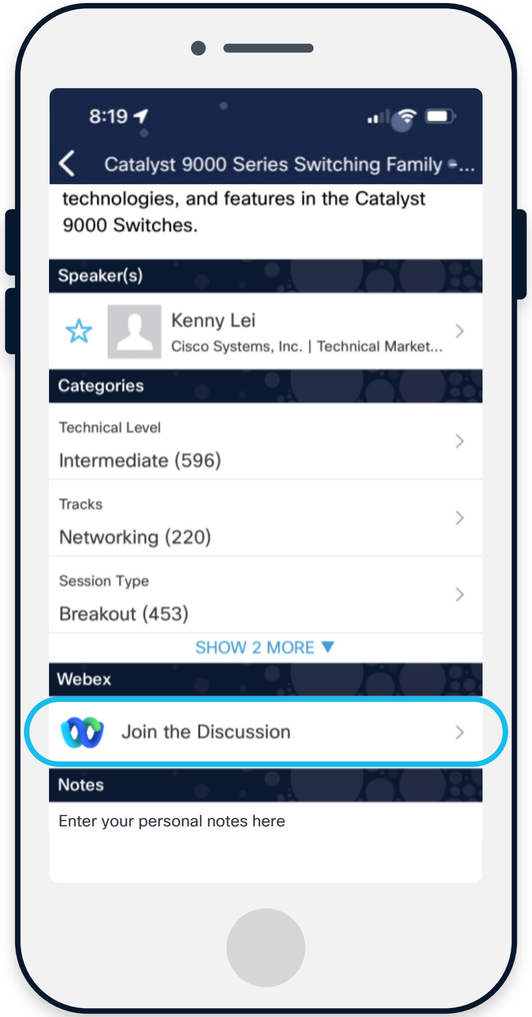
Questions?

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, 2025.



8:19

Catalyst 9000 Series Switching Family •...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

CLUS Quantum Strawman

BRKSEC-2175 Planning

cisco Live!

Agenda

01 Introduction

02 US Government Direction on Quantum Safety

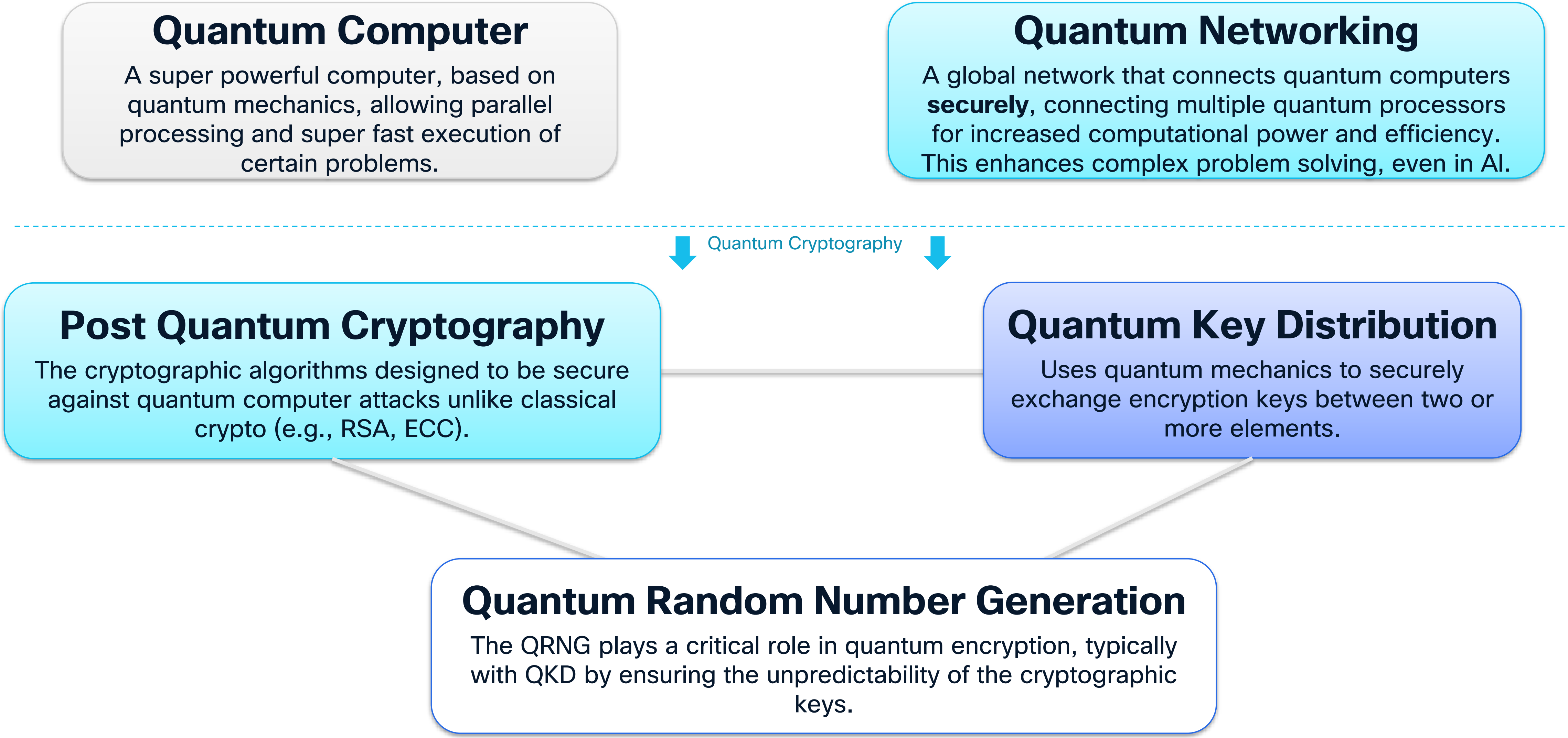
03 Crawl, Walk, Run Direction

04 What is Available Today @ Cisco?

05 Deployment Building Blocks

06 Quantum Resistant examples for IPSec, MACsec, 3rd-party Key Server Usage

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

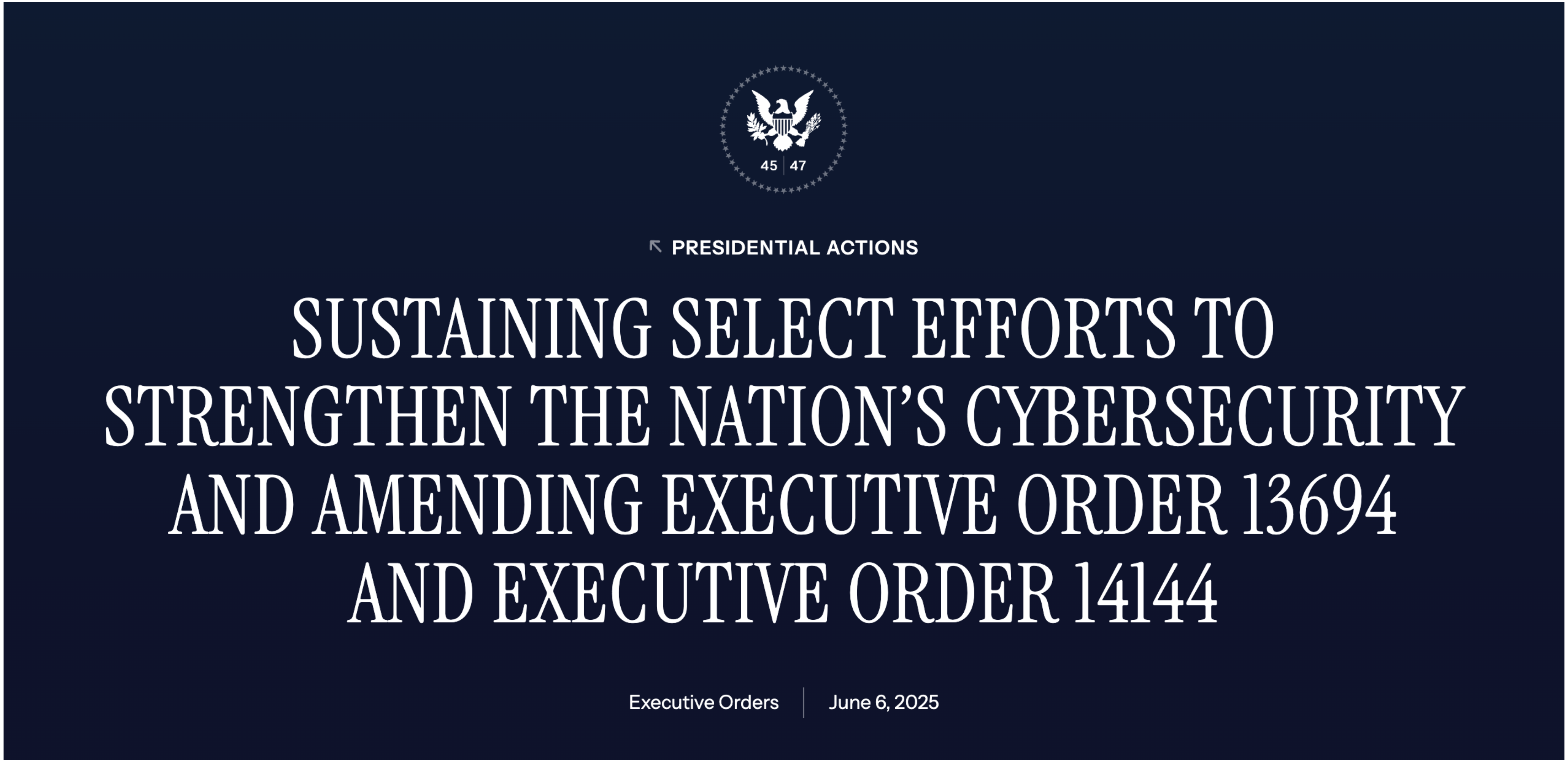
The cryptographic algorithms designed to be secure against quantum computer attacks unlike classical crypto (e.g., RSA, ECC).

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.

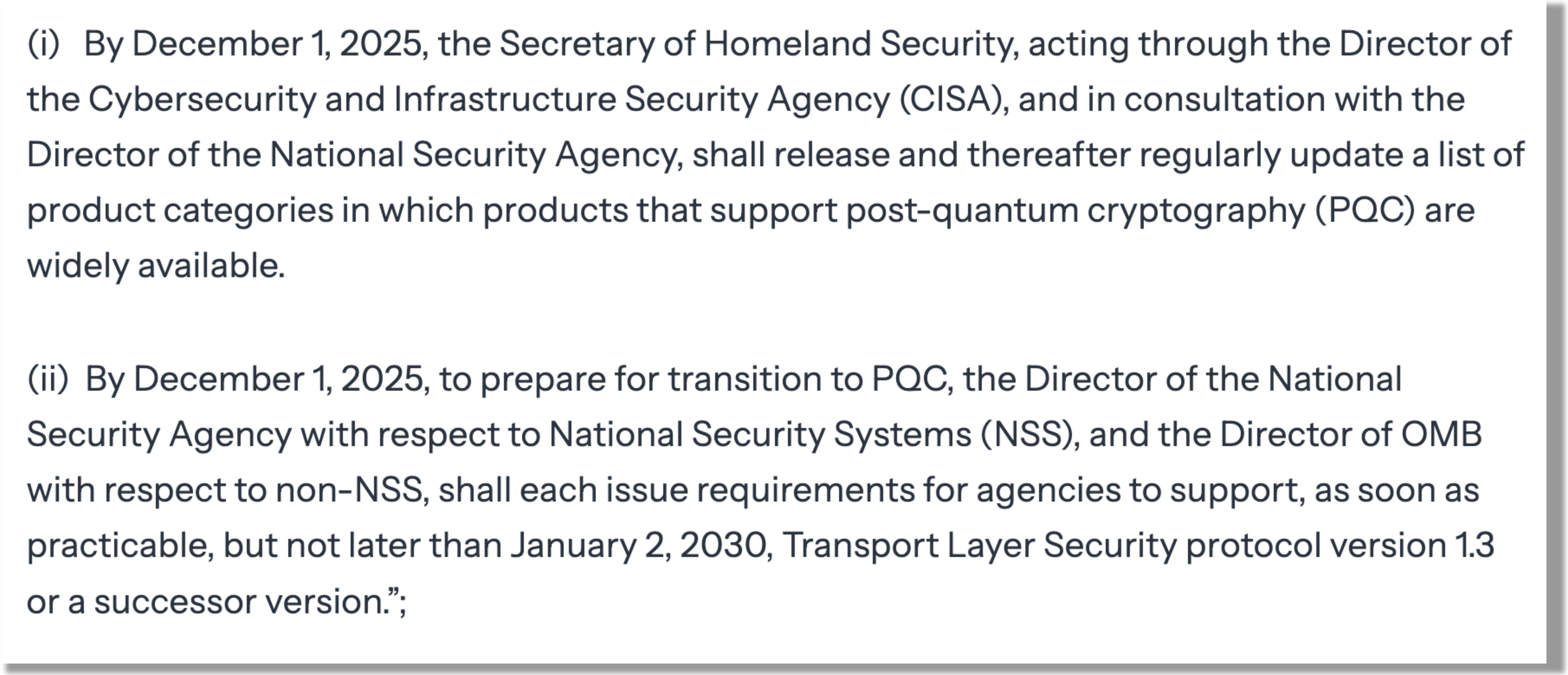


PRESIDENTIAL ACTIONS

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…



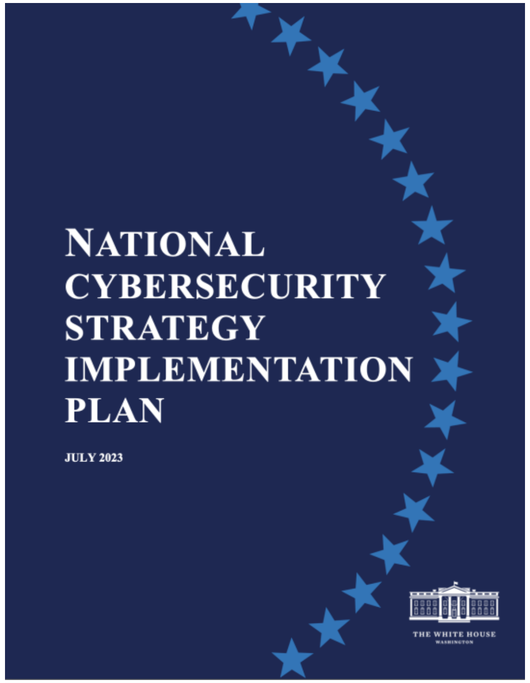
(i) By December 1, 2025, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in consultation with the Director of the National Security Agency, shall release and thereafter regularly update a list of product categories in 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, but not later than January 2, 2030, Transport Layer Security protocol version 1.3 or a successor version.”;

US Government Direction on Quantum Safety

Current U.S. Government Direction

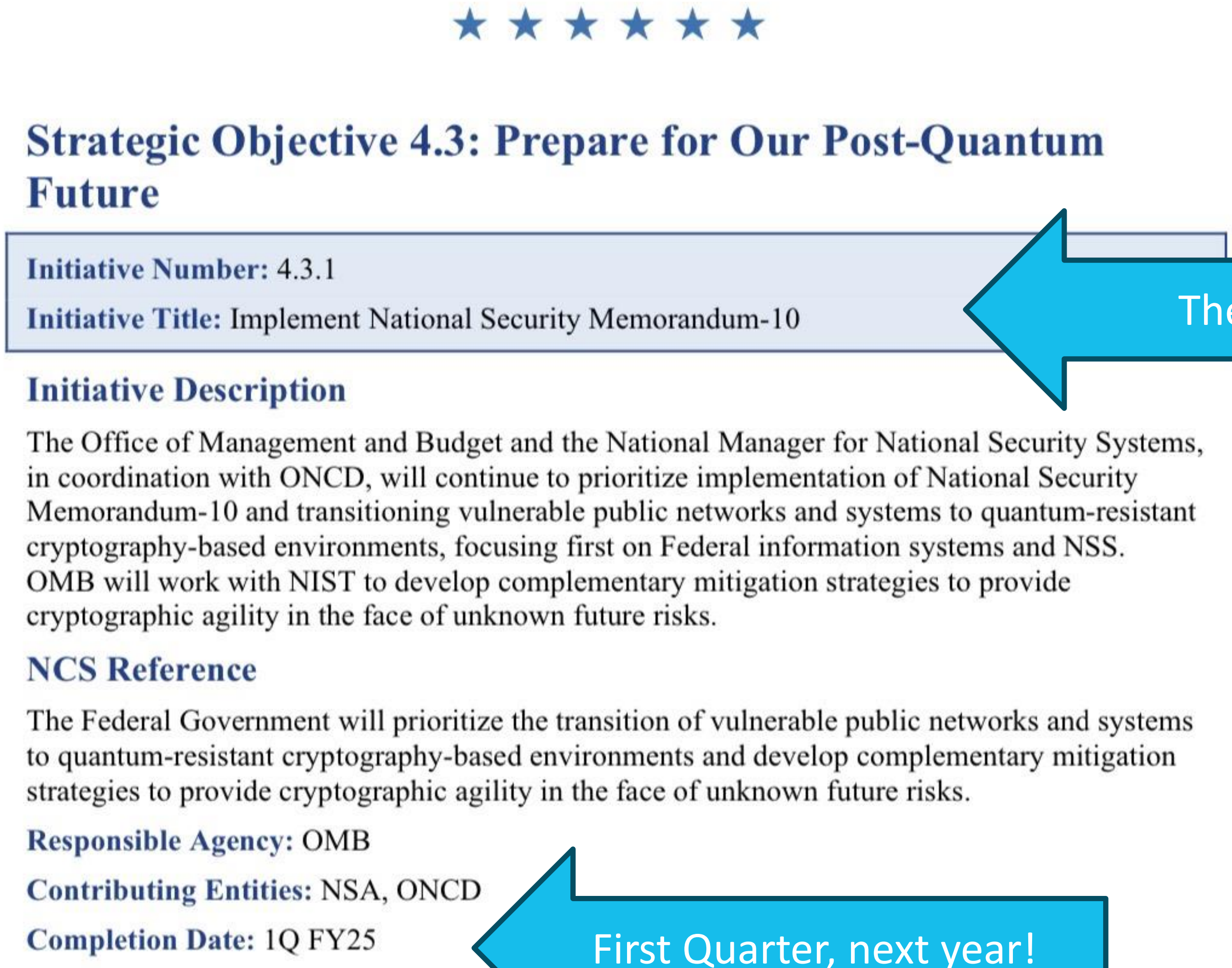
- US Government has provided clear direction for requirements on Quantum Resistance for protection of National Security Systems
  - (ref: NCSIP and NSM-10)
- Quantum Key Distribution is an open topic and lacks standards
- Cisco SKIP should be an acceptable interim option
- All aspects of encryption should drive towards Quantum Resistance encryption options
- Site to Site VPN, VPN Client along with TLS stack implementations for control plane operations



NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN

JULY 2023

THE WHITE HOUSE
WASHINGTON



★ ★ ★ ★ ★ ★

Strategic Objective 4.3: Prepare for Our Post-Quantum Future

Initiative Number: 4.3.1

Initiative Title: Implement National Security Memorandum-10

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.

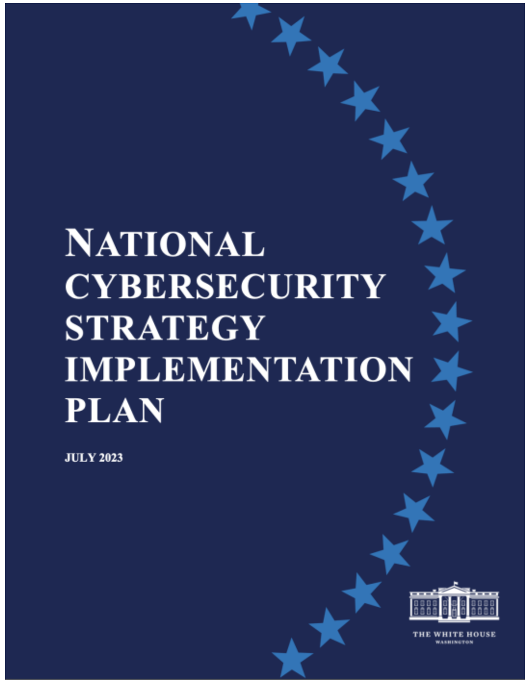
Responsible Agency: OMB

Contributing Entities: NSA, ONCD

Completion Date: 1Q FY25

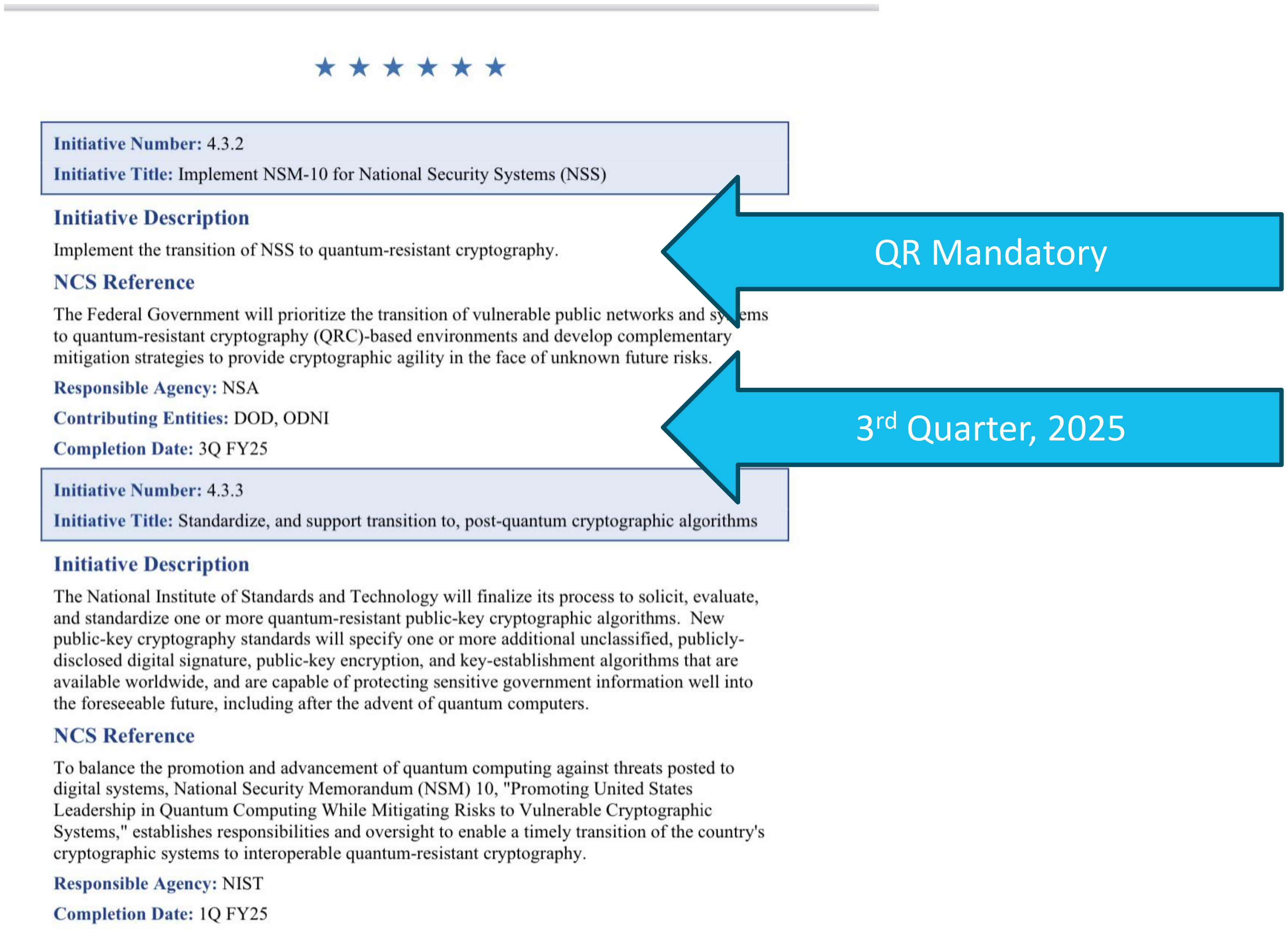
The Predicate

First Quarter, next year!



NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN

JULY 2023



★ ★ ★ ★ ★ ★

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

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

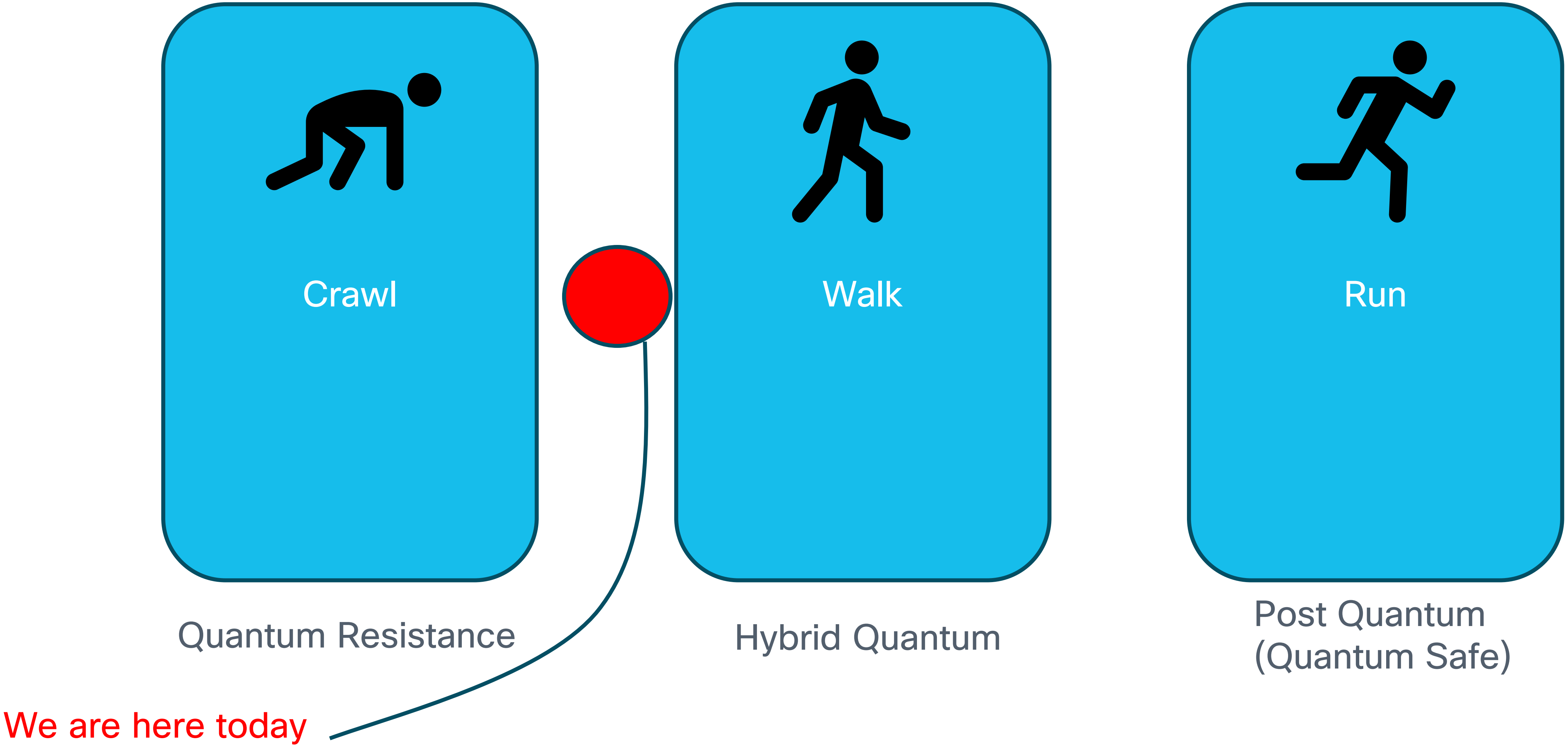
Run

- 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

Post-Quantum Roadmap

Post Quantum Strategic Plan

Cisco Quantum Roadmap



Crawl

Walk

Run

Quantum Resistance

Hybrid Quantum

Post Quantum
(Quantum Safe)

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+

Quantum Field Update

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

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

What products are Quantum Resistant?

• Is there a Quantum Resistant Webex?		NO
• Is there a Quantum Resistant CUCM	NO	
• Is there a Quantum Resistant SD-WAN (VIPTELA)		NO
• Is there a Quantum Resistant Secure Access (CSA)		NO
• Is there a Quantum Resistant WSA?	NO	
• Is there a Quantum Resistant MACSEC?		YES
• Is there a Quantum Resistant Wireless?		NO
• Is there a Quantum Resistant SNA/XDR/SMA	NO	
• Is there a Quantum Resistant Umbrella?		NO
• Is there a Quantum Resistant ISE (RADIUS)?		NO
• Is there a Quantum Resistant ISE (TACACS+)?	NO	
• Is there a Quantum Resistant Firewall?		YES
• Is there a Quantum Resistant VPN Router?		YES

What products are Post-Quantum Safe?

- Is there a Post-Quantum Webex? NO
- Is there a Post-Quantum CUCM NO
- Is there a Post-Quantum SD-WAN (VIPTELA) NO
- Is there a Post-Quantum Secure Access (CSA) NO
- Is there a Post-Quantum WSA? NO
- Is there a Post-Quantum MACSEC? NO
- Is there a Post-Quantum Wireless? NO
- Is there a Post-Quantum SNA/XDR/SMA NO
- Is there a Post-Quantum Umbrella? NO
- Is there a Post-Quantum ISE (RADIUS)? NO
- Is there a Post-Quantum ISE (TACACS+)? NO

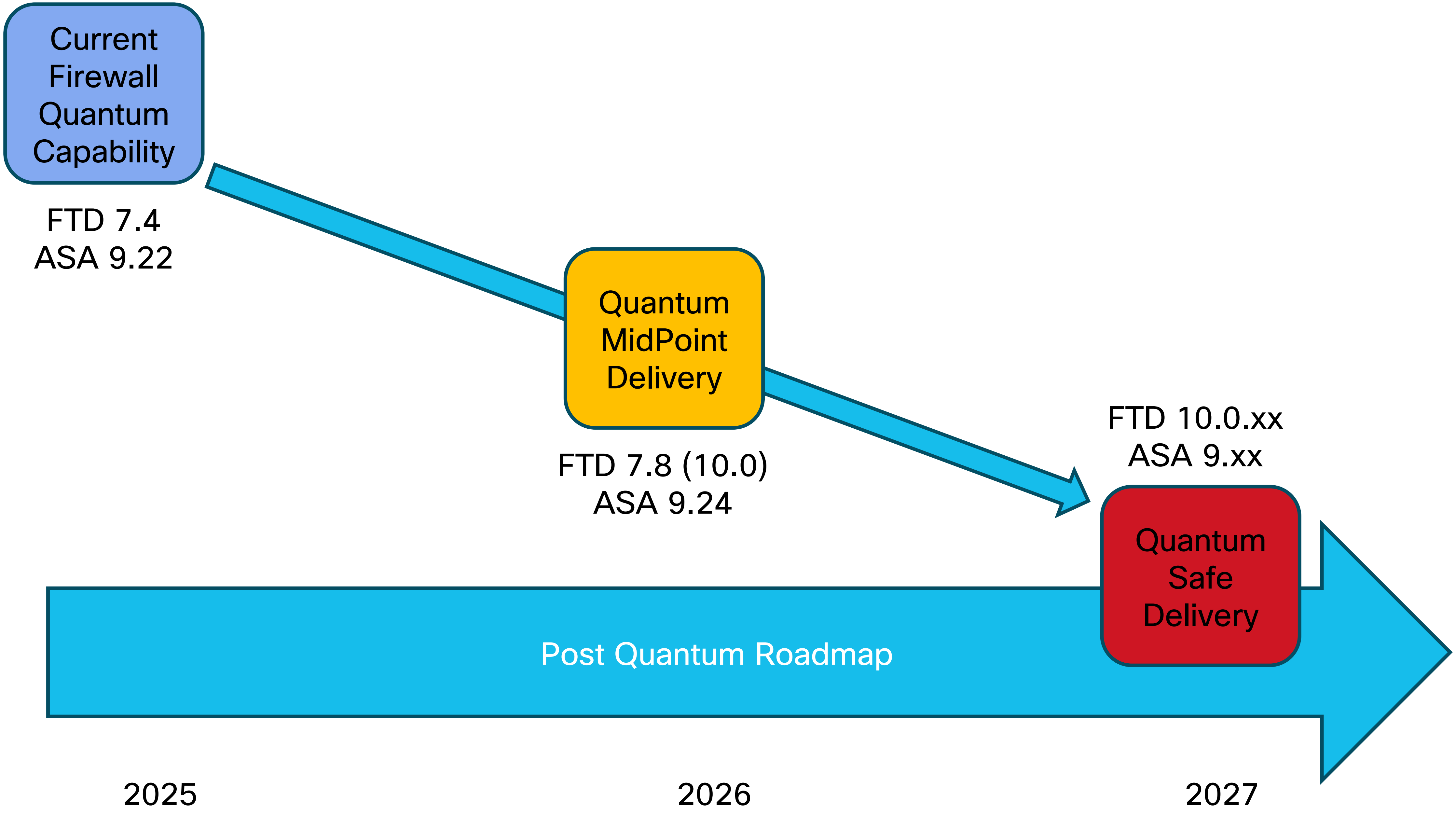
Practical Post-Quantum Roadmap

- Expect a 2027 Delivery timeframe for a Certified Product on core IOS Products
- Very limited to zero commitment from SBG Leadership on PQ
  - Meaning FIPS 203, 204, 205, CC, DODIN, CSfC

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



Current Firewall Quantum Capability

FTD 7.4
ASA 9.22

Quantum MidPoint Delivery

FTD 7.8 (10.0)
ASA 9.24

FTD 10.0.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

Currently shipping or 7.4-7.8 (10.0)

- 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

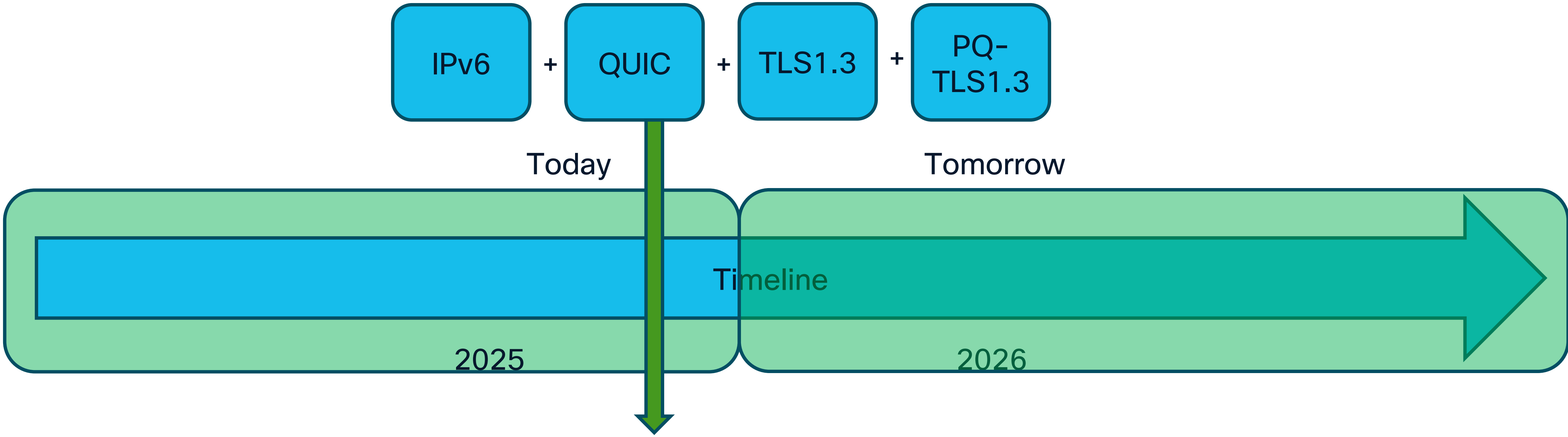
Must be committed for 10.0.10

- 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

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

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-tls13/19/



IPv6 + QUIC + TLS1.3 + PQ-TLS1.3

Today

Tomorrow

Timeline

2025

2026

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

Post-Quantum Roadmap for IOS-XE

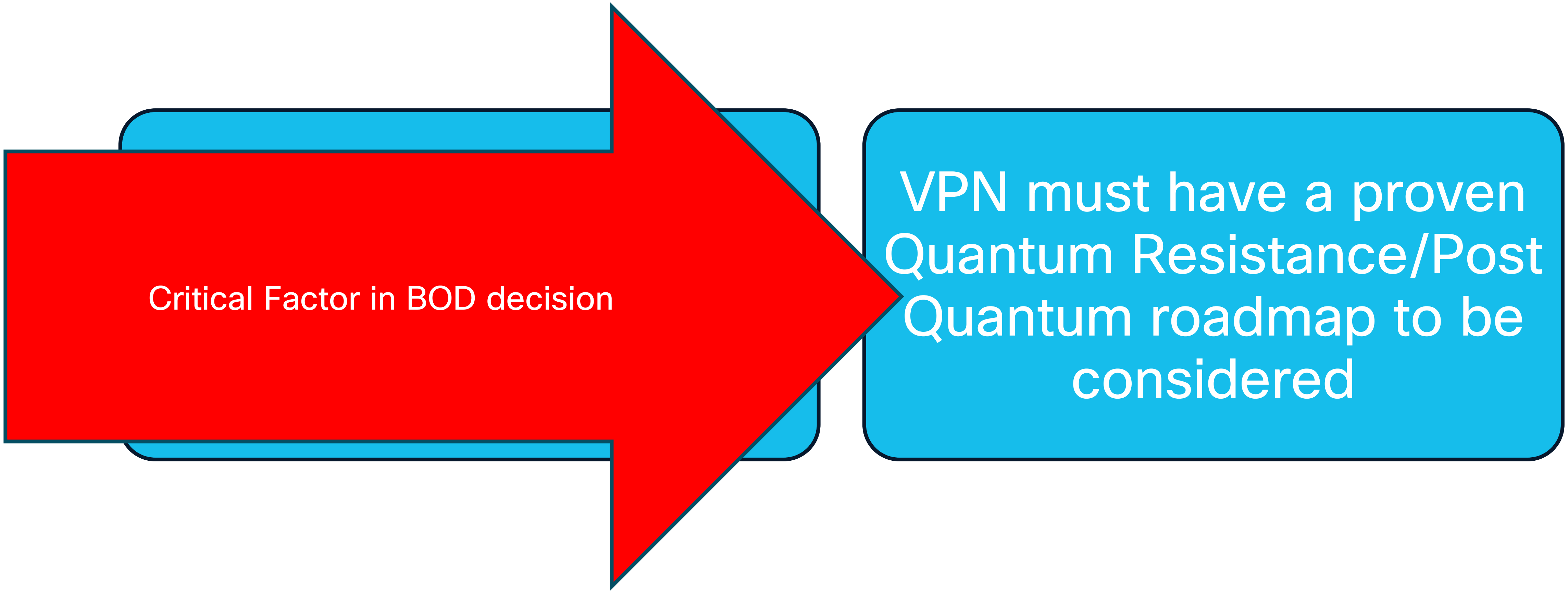
US Intelligence Community, US Department of Defense, Five Eyes, NATO

Andrew Benhase

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



Critical Factor in BOD decision

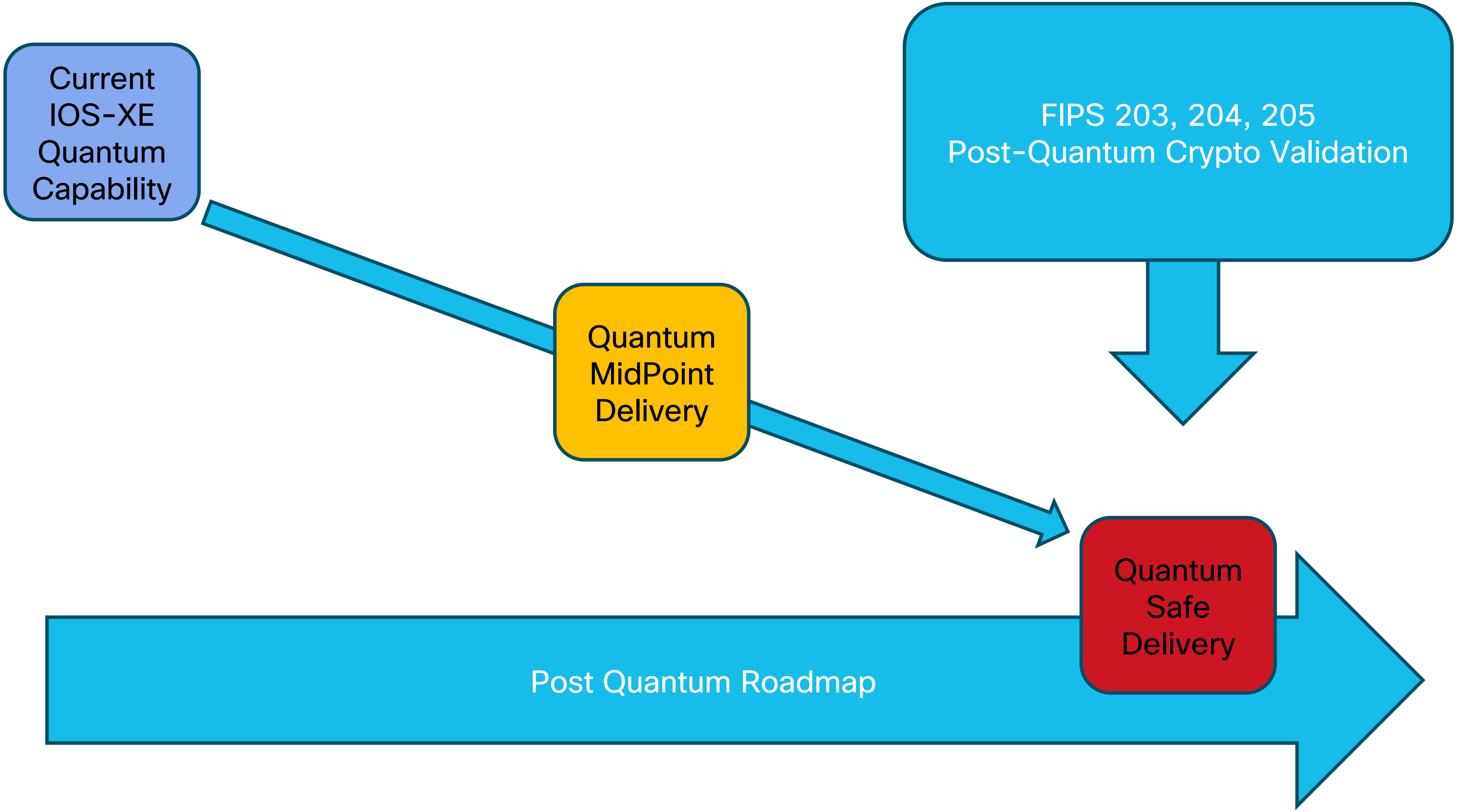
VPN must have a proven Quantum Resistance/Post Quantum roadmap to be considered

Cisco IOS-XE Post-Quantum Glide Slope

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-tls13/19/

Salt Typhoon Related Enhancements!



Current IOS-XE Quantum Capability

FIPS 203, 204, 205
Post-Quantum Crypto Validation

Quantum MidPoint Delivery

Quantum Safe Delivery

Post Quantum Roadmap

Pre and Post Quantum Requirements

- Strong Legacy supported for S2S+VTI, DMVPN, GET
- Support for RFC 8784+SKIP in IOS-XE
- Support for Third Party integration with SKIP for RFC 8784

Currently shipping in IOS-XE 17.12

- 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

Must be committed for 10.0.10

- Support for ML-KEM-1024 for SSHv2 – ASA
- Support for ML-KEM-1024 for SSHv2 – FMC/FTD/FXOS
- 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

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

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-tls13/19/

Quantum Resistance Direction for Cisco

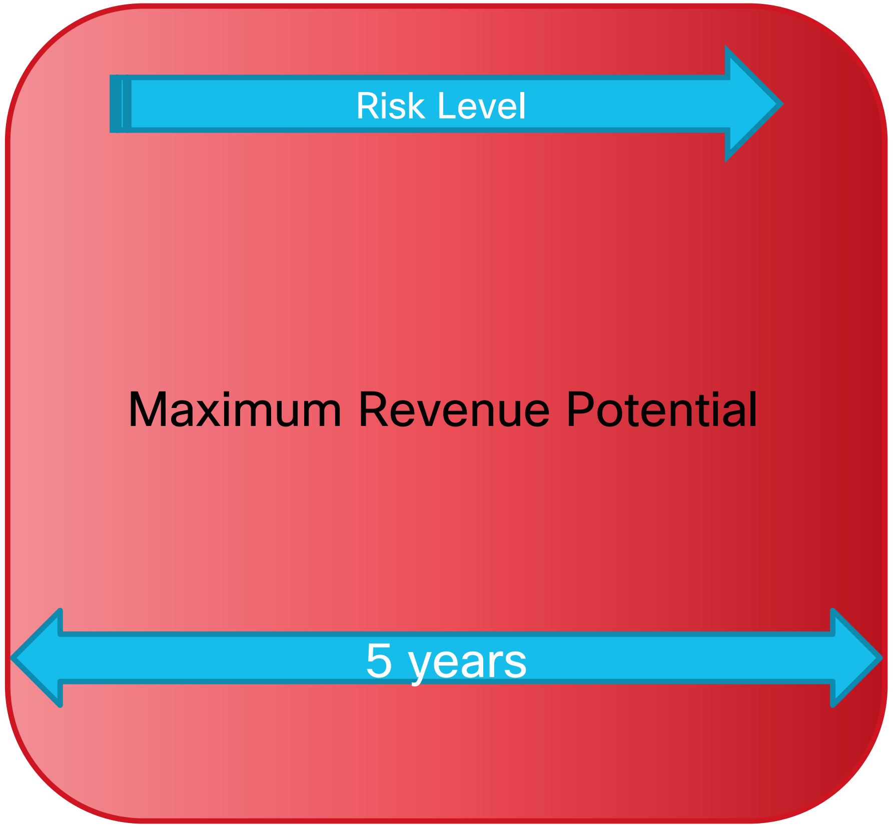
- Focus: ASA 9.21 and FTD 7.7
- Focus: IOS-XE 17.15

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

Quantum Crypto Market

Quantum Resistance Market

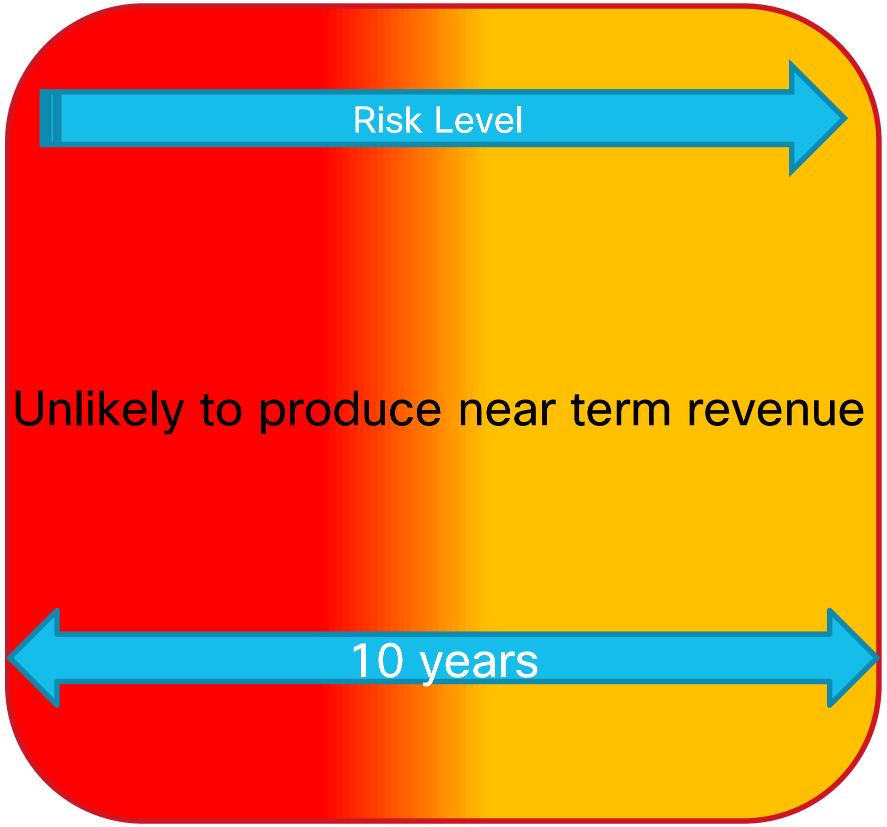


Well understood, existing market partnerships.

Current product development.

Requires near term Engineering investments.

Post-Quantum Market



10 year Roadmap, market not well understood.

Pure R&D, limited to no short-term revenue

Pathway to QR Minimum Viable Product

RFC 8784 Compliance for IKEv2

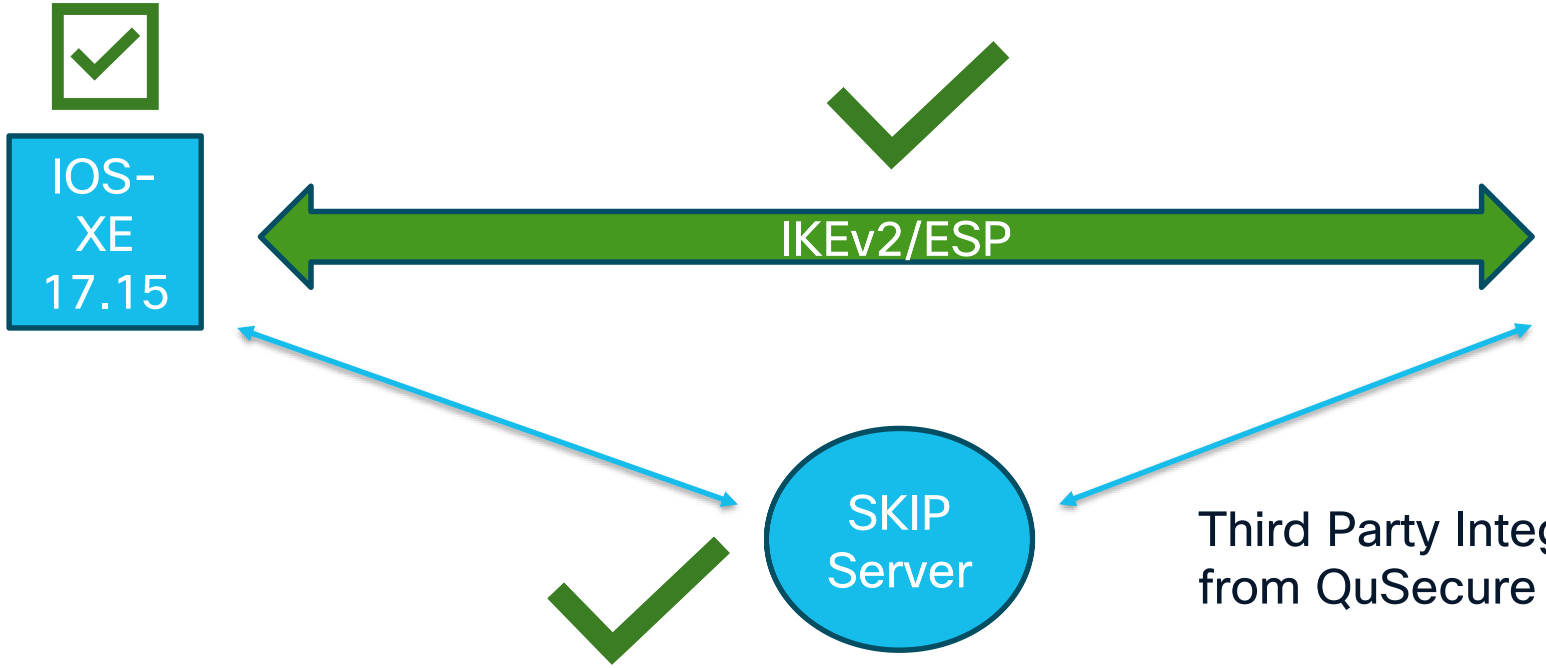
Cisco SKIP integration for Quantum Key Distribution

Near term focus on RFC 9242 and 9370

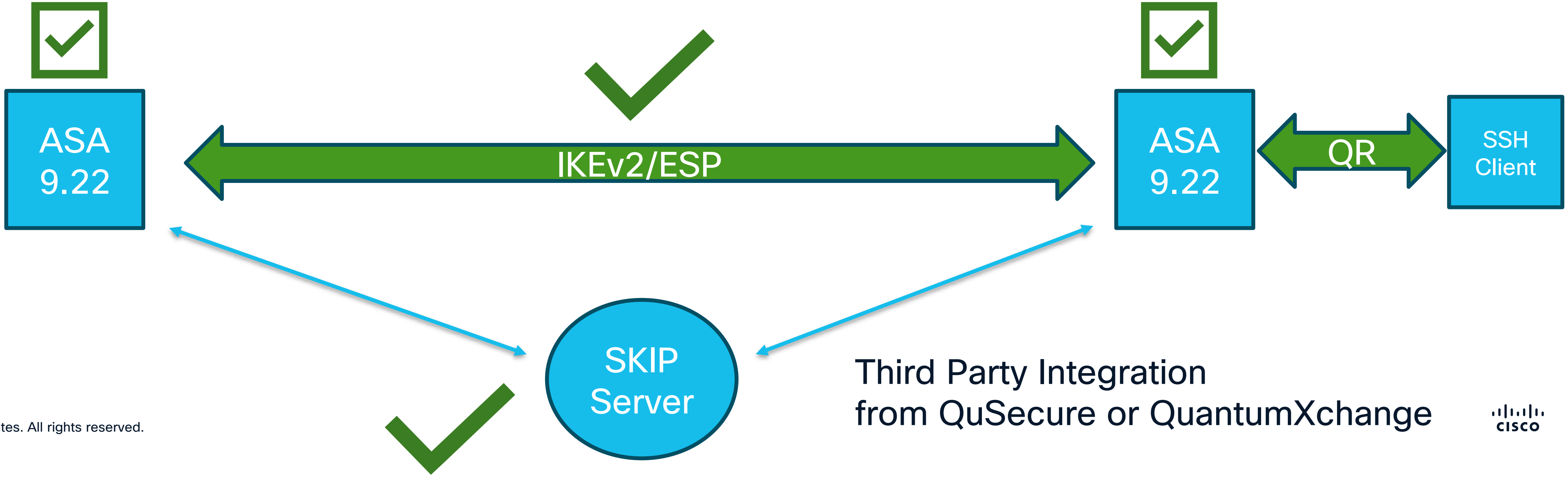
RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

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

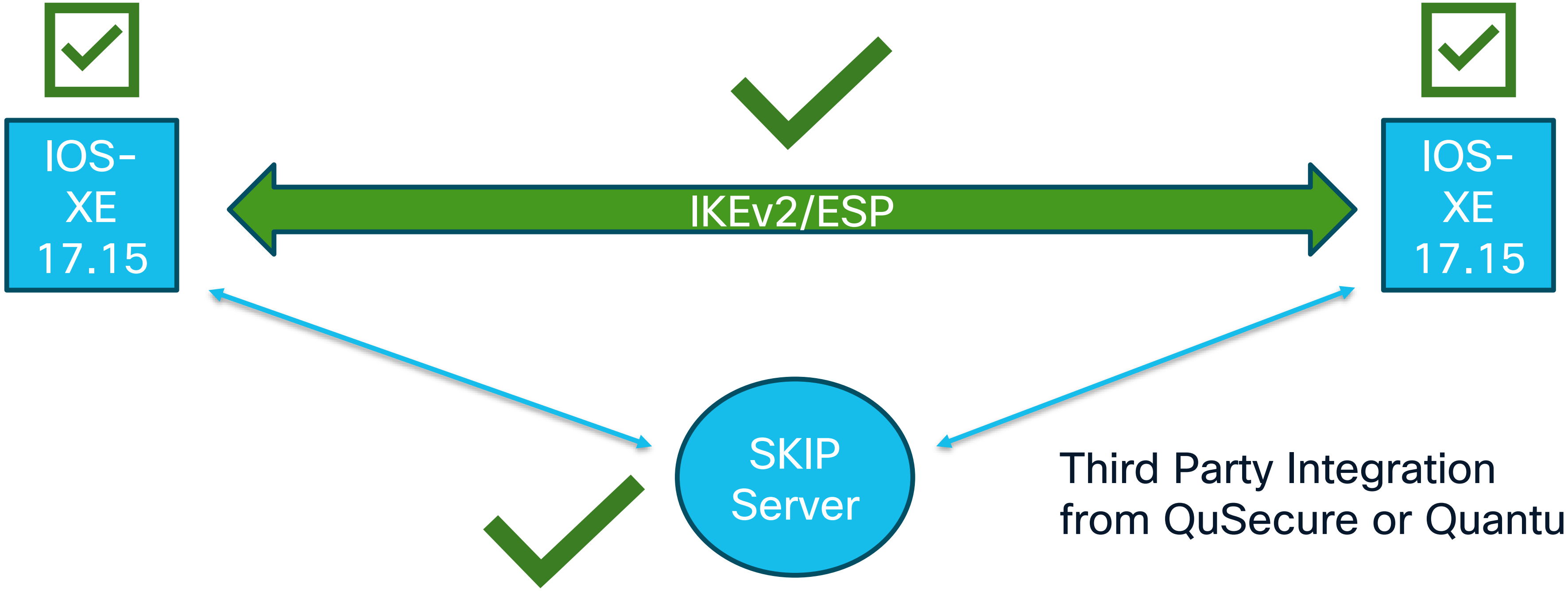
Desired QR Architecture



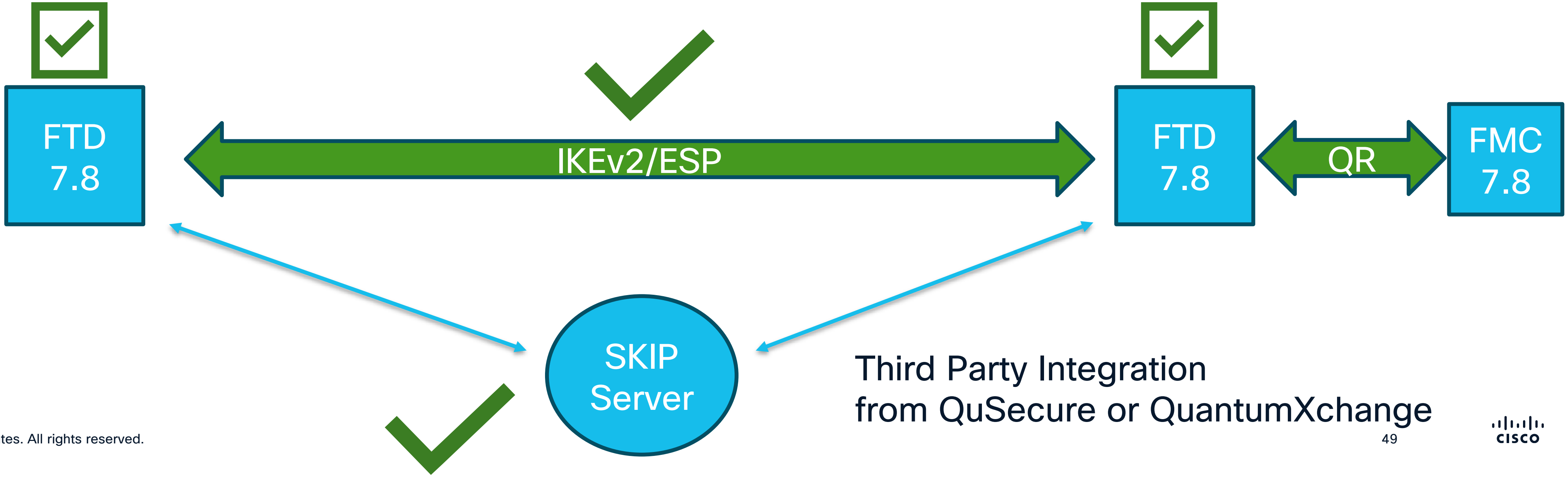
Third Party Integration
from QuSecure or QuantumXchange



Third Party Integration
from QuSecure or QuantumXchange



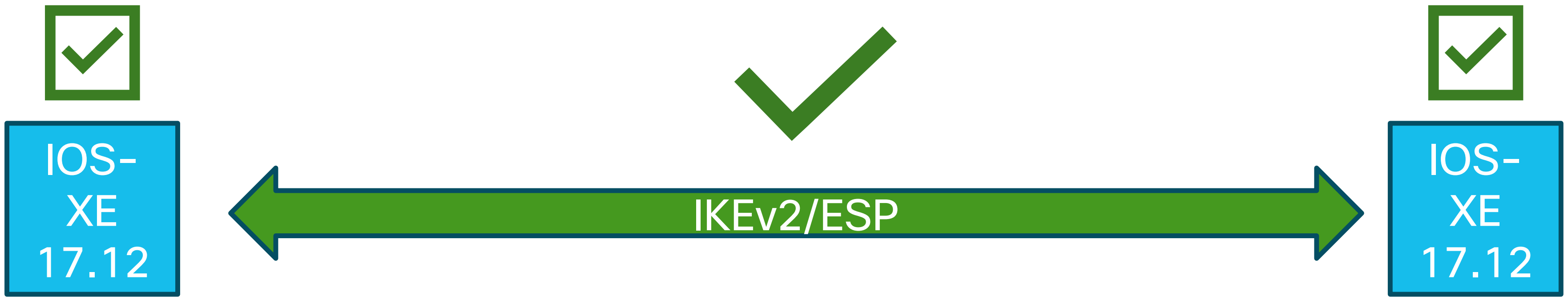
Third Party Integration
from QuSecure or QuantumXchange

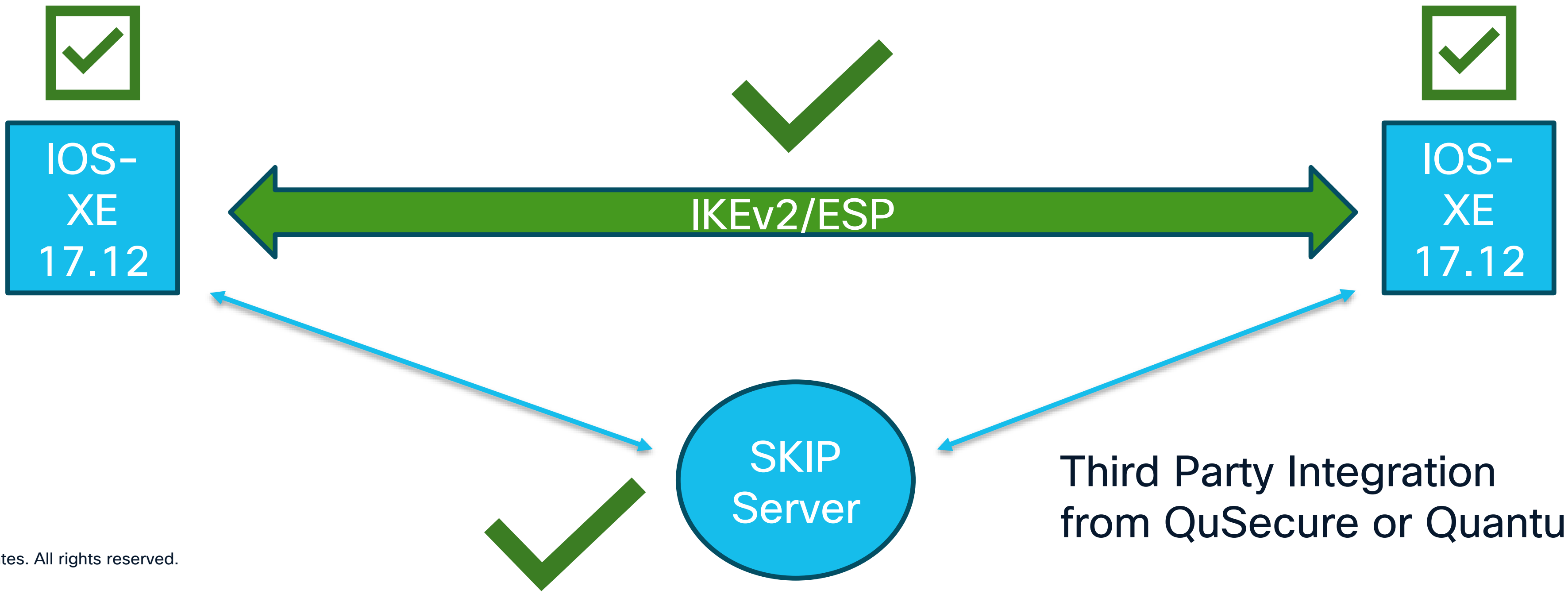


Third Party Integration
from QuSecure or QuantumXchange

Current Status of Products

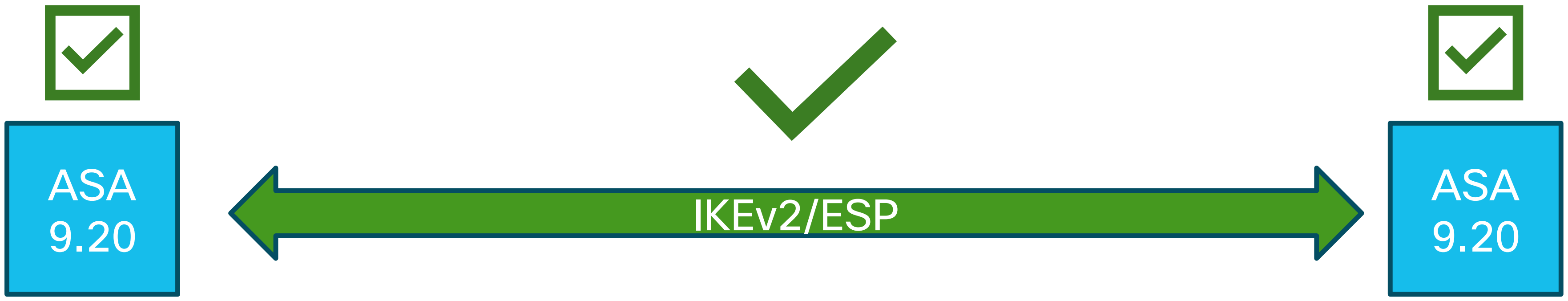
Catalyst Routers

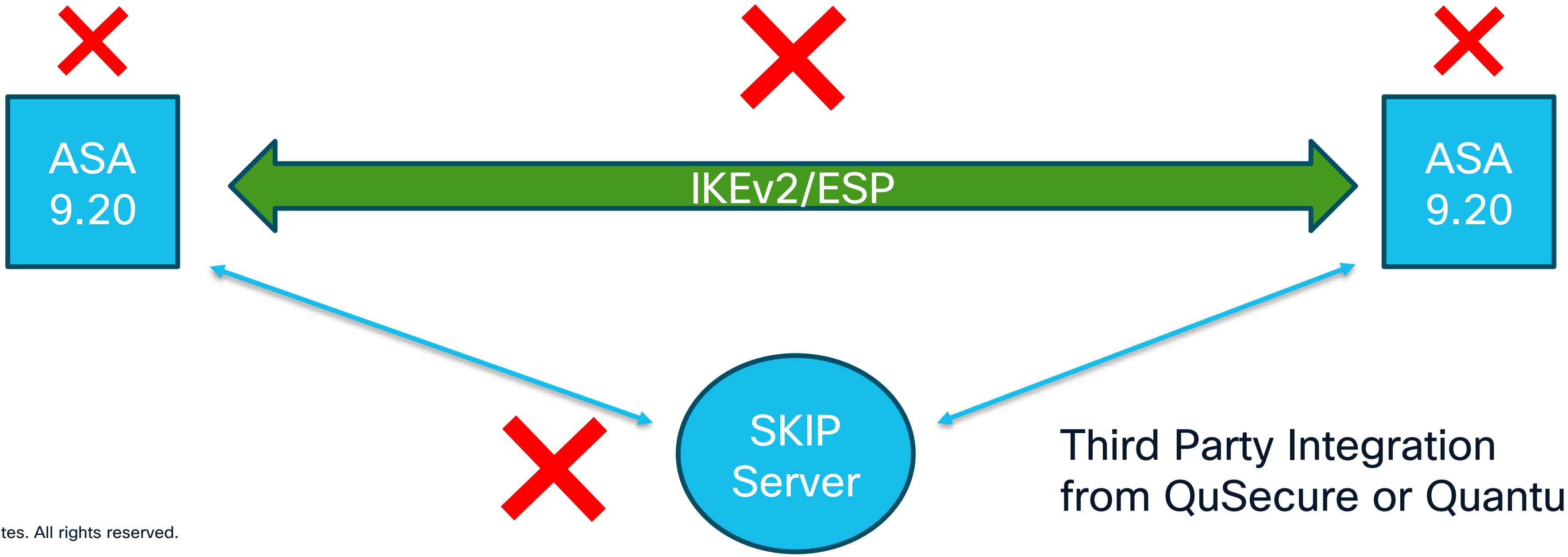




Third Party Integration
from QuSecure or QuantumXchange

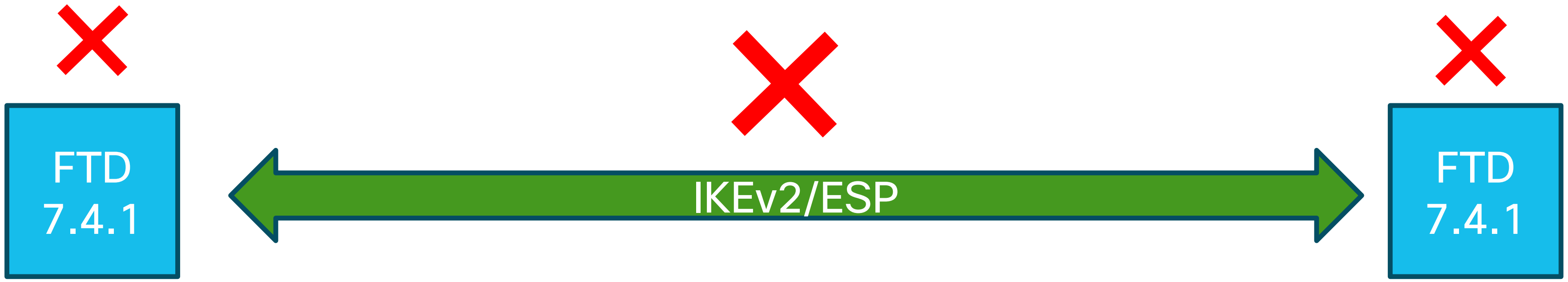
Firepower - ASA

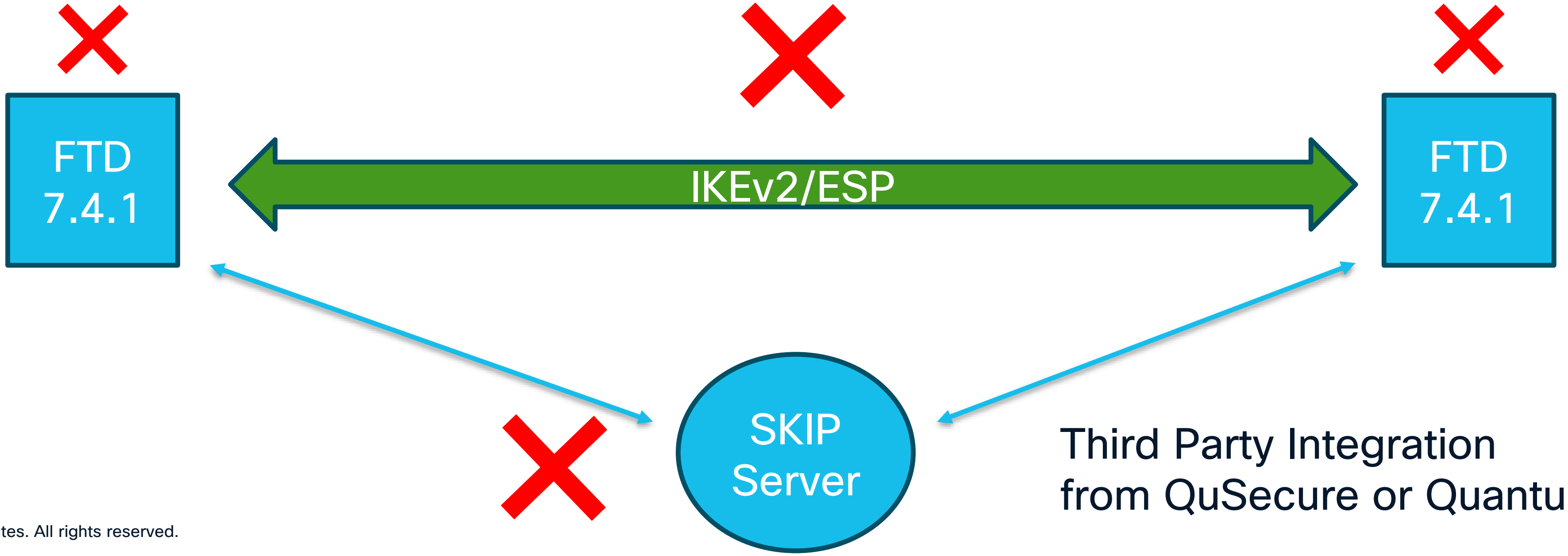




Third Party Integration
from QuSecure or QuantumXchange

Firepower - FTD

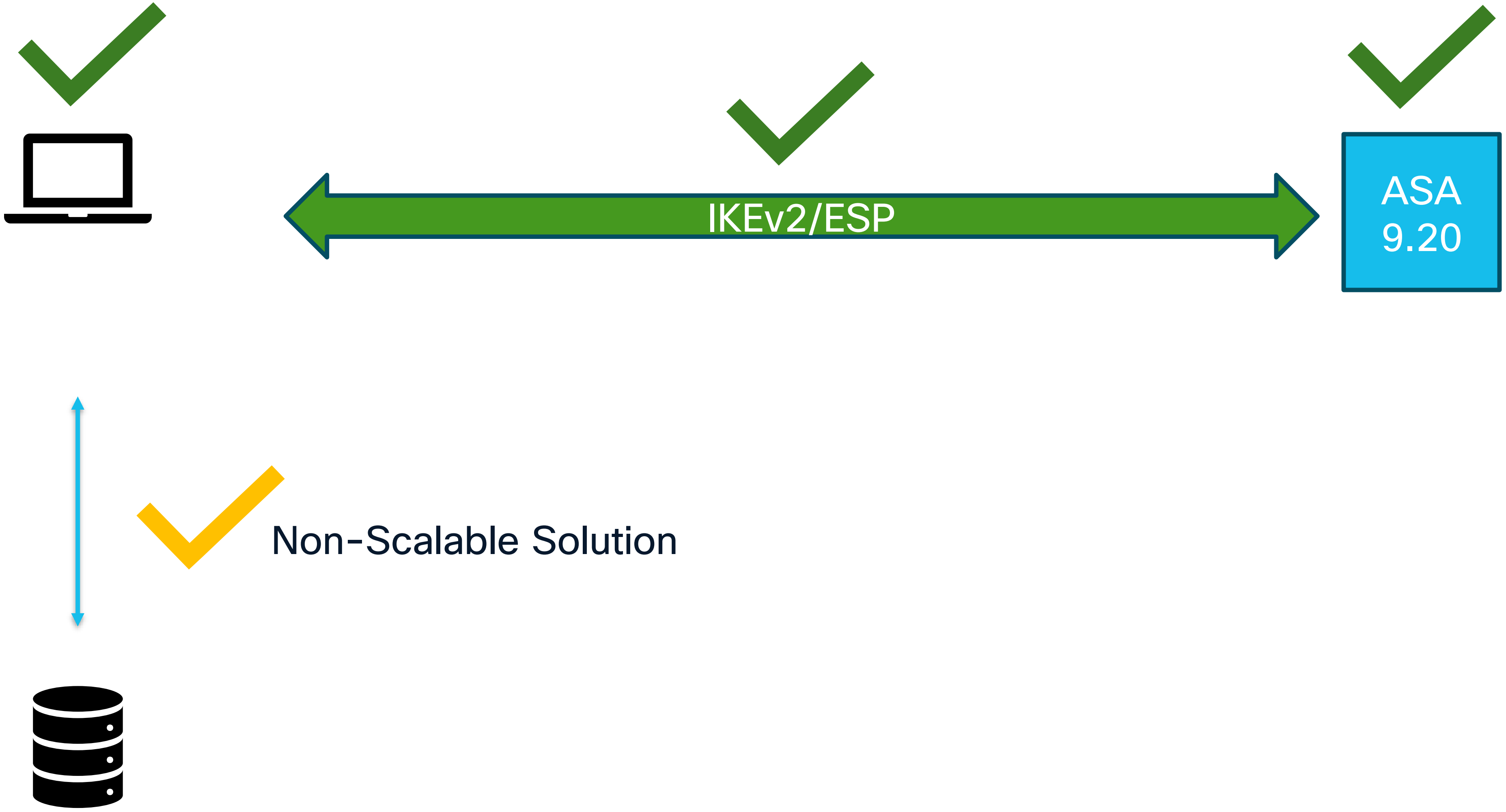




Third Party Integration
from QuSecure or QuantumXchange

FPR ASA + Secure Client

Cisco ASA Firewalls + Secure Client



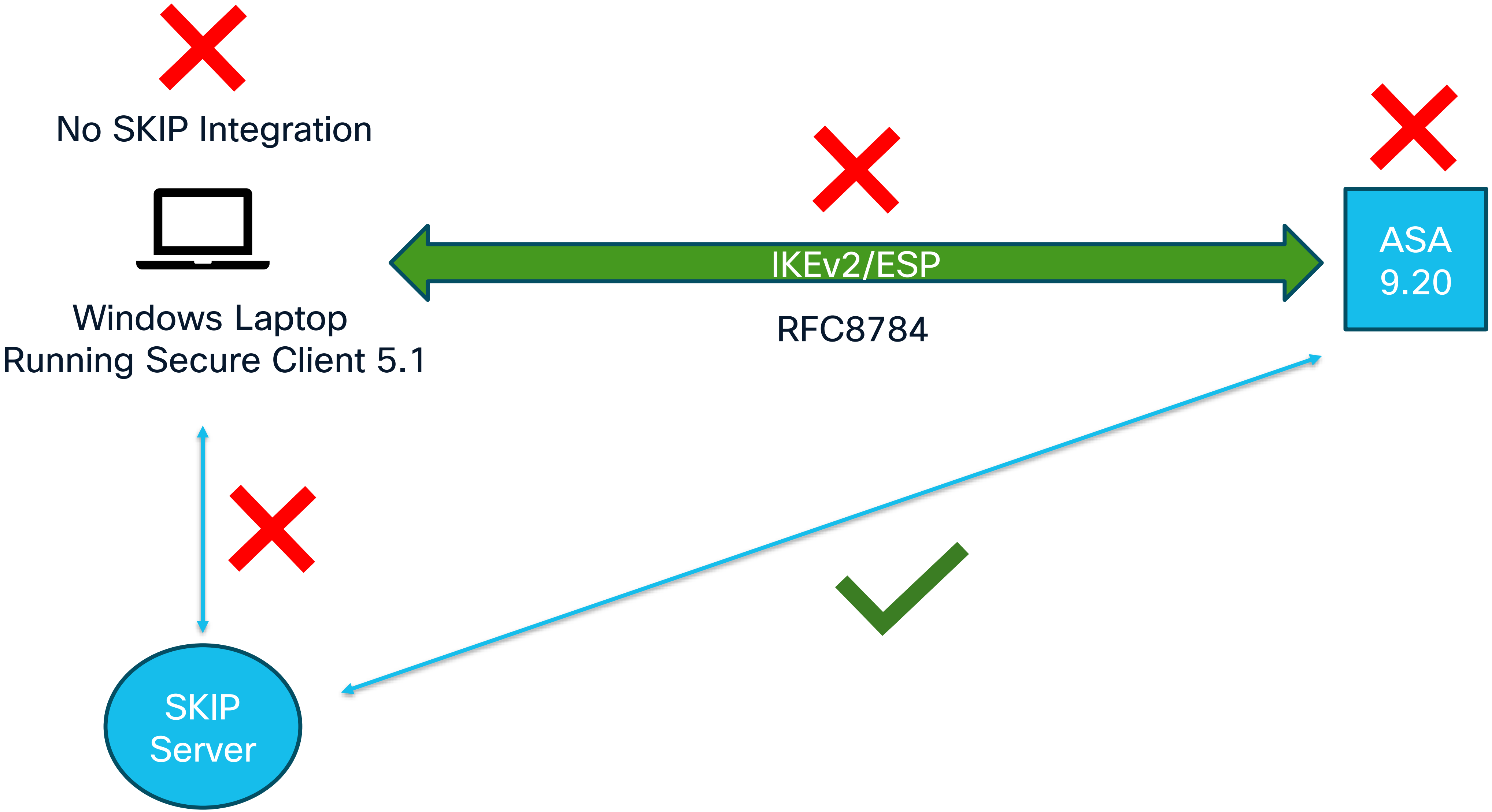
IKEv2/ESP

ASA
9.20

Non-Scalable Solution

FPR FTD + Secure Client

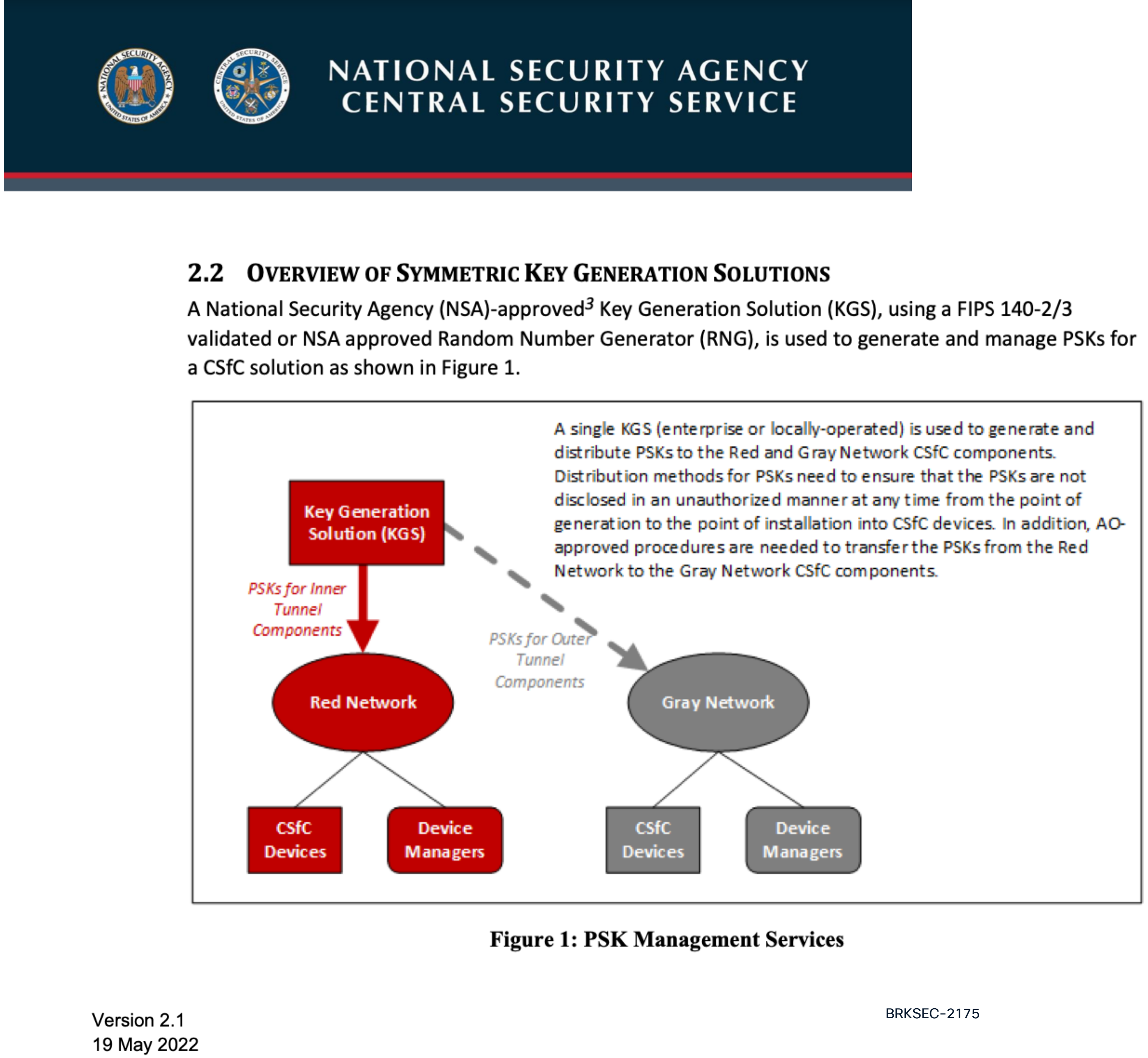
Cisco ASA Firewalls + Secure Client



Quantum Key Distribution (QKD)

Symmetric Key Options

- Symmetric Key Management Requirements Annex
- The Symmetric Key Management (KM) Requirements Annex Version 2.1, dated May 2022, has been approved by the Deputy National Manager (DNM) for National Security Systems. This annex defines additional requirements for implementing Symmetric KM capabilities defined in CSfC Capability Packages (CPs). It allows for the use of **Symmetric Pre-Shared Keys to provide quantum resistant cryptographic protection of classified information in properly configured, maintained and monitored CSfC solutions**. The updated version of this annex incorporates updated KGS product selection criteria, updated wording to improve and clarify PSK usage guidance, updated IPSec with RFC 8784-compliant implementations of IKE v2 PSK usage requirements, updated outer PSK classification requirement, and role-based personnel requirements. This document supersedes the SKM Requirements Annex Version 2.0.



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

2.2 Overview of Symmetric Key Generation Solutions

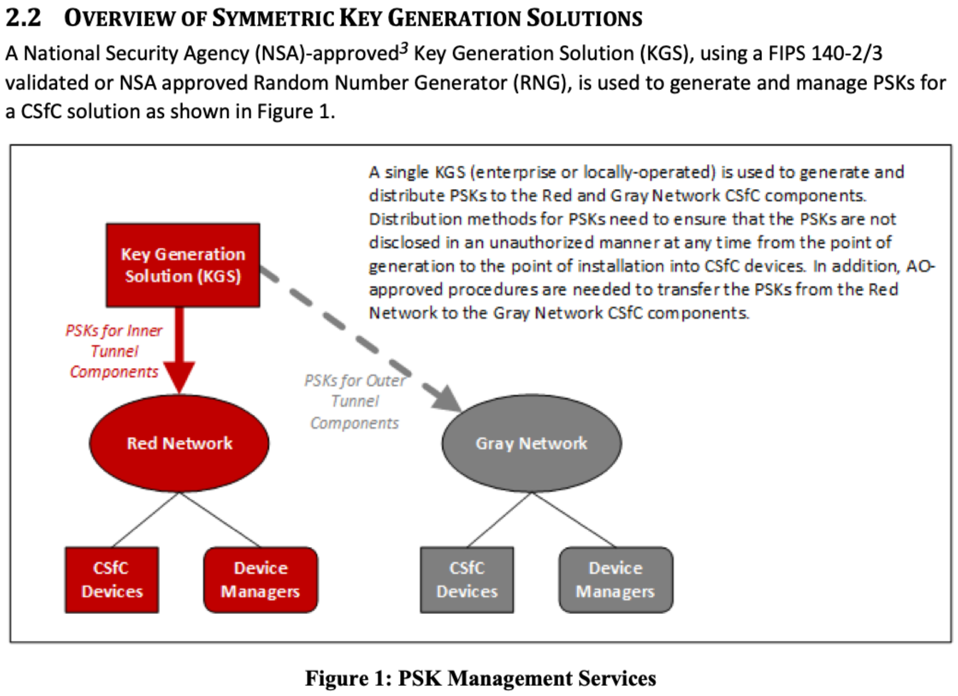
A National Security Agency (NSA)-approved[3] Key Generation Solution (KGS), using a FIPS 140-2/3 validated or NSA approved Random Number Generator (RNG), is used to generate and manage PSKs for a CSfC solution as shown in Figure 1.

A single KGS (enterprise or locally-operated) is used to generate and distribute PSKs to the Red and Gray Network CSfC components. Distribution methods for PSKs need to ensure that the PSKs are not disclosed in an unauthorized manner at any time from the point of generation to the point of installation into CSfC devices. In addition, AO-approved procedures are needed to transfer the PSKs from the Red Network to the Gray Network CSfC components.

Key Generation Solution (KGS)
PSKs for Inner Tunnel Components
PSKs for Outer Tunnel Components
Red Network
Gray Network
CSfC Devices
Device Managers
CSfC Devices
Device Managers

Figure 1: PSK Management Services

Version 2.1
19 May 2022



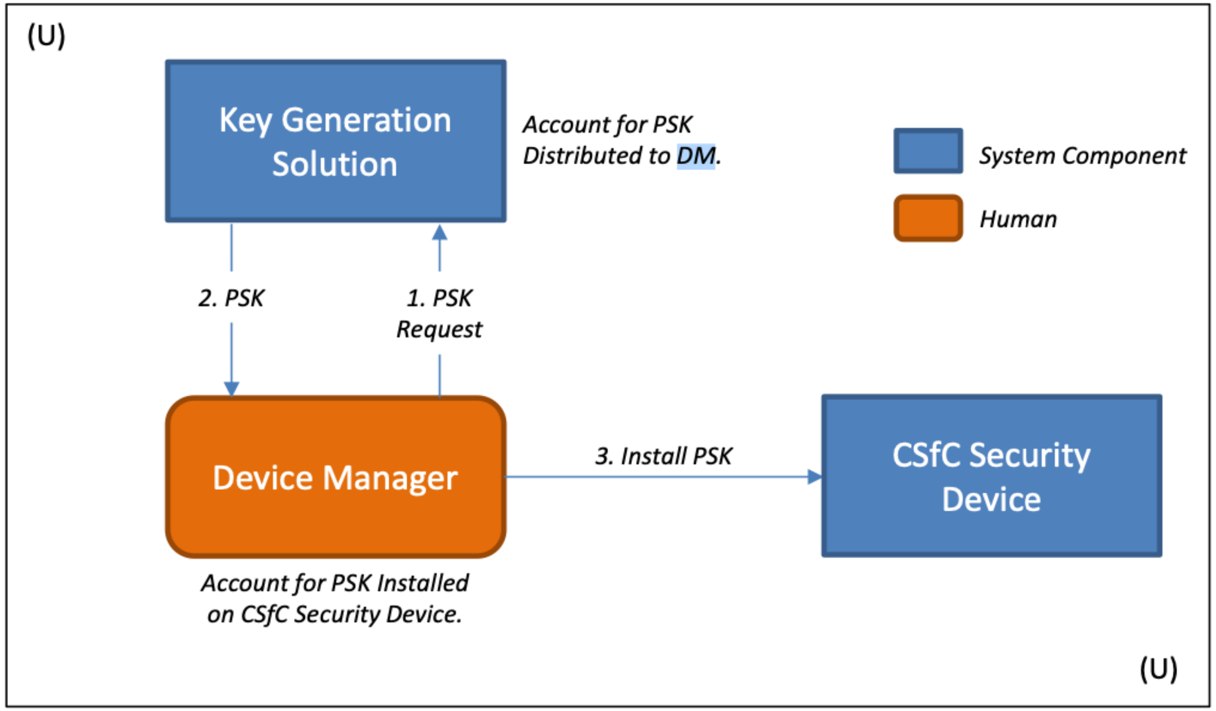
2.2 Overview of Symmetric Key Generation Solutions

A National Security Agency (NSA)-approved[3] Key Generation Solution (KGS), using a FIPS 140-2/3 validated or NSA approved Random Number Generator (RNG), is used to generate and manage PSKs for a CSfC solution as shown in Figure 1.

A single KGS (enterprise or locally-operated) is used to generate and distribute PSKs to the Red and Gray Network CSfC components. Distribution methods for PSKs need to ensure that the PSKs are not disclosed in an unauthorized manner at any time from the point of generation to the point of installation into CSfC devices. In addition, AO-approved procedures are needed to transfer the PSKs from the Red Network to the Gray Network CSfC components.

Key Generation Solution (KGS)
PSKs for Inner Tunnel Components
PSKs for Outer Tunnel Components
Red Network
Gray Network
CSfC Devices
Device Managers
CSfC Devices
Device Managers

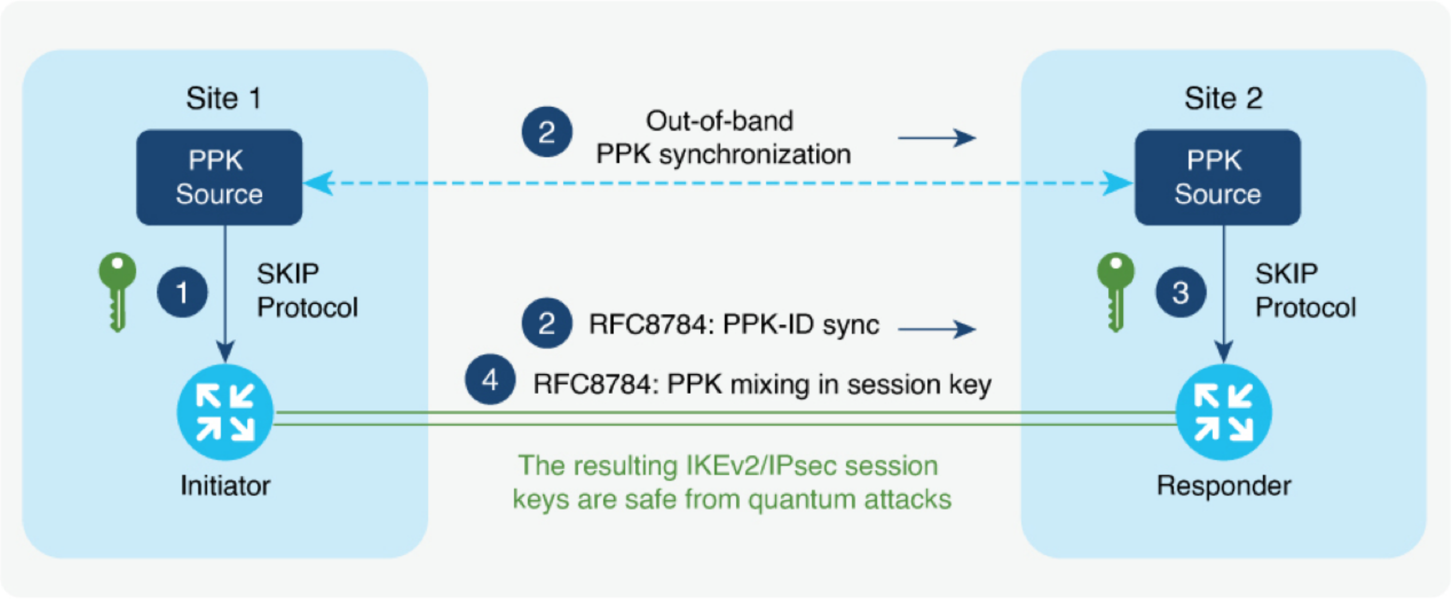
Figure 1: PSK Management Services



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

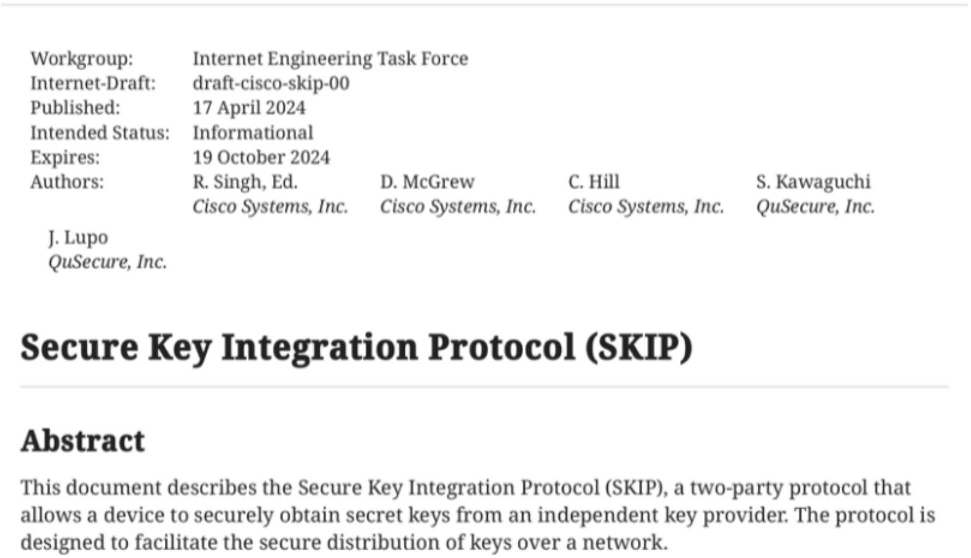
Quantum-Safe IKEv2/IPsec Session Keys with Dynamic PPK


Site 1
PPK Source
1
SKIP Protocol
Initiator
2
Out-of-band PPK synchronization
2
RFC8784: PPK-ID sync
4
RFC8784: PPK mixing in session key
The resulting IKEv2/IPsec session keys are safe from quantum attacks
Site 2
PPK Source
3
SKIP Protocol
Responder

SKIP vs ETSI-014

- ETSI-014
- https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

SKIP – IETF RFC

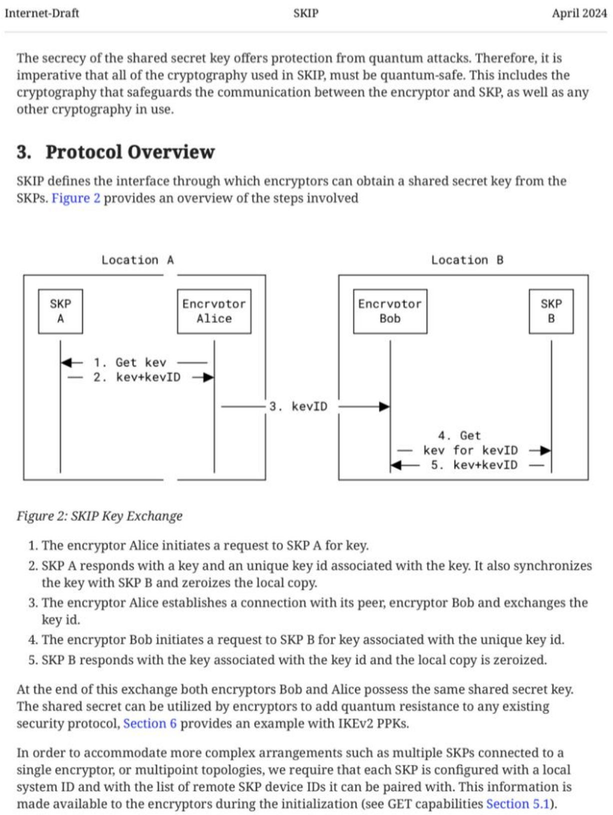


Workgroup: Internet Engineering Task Force
Internet-Draft: draft-cisco-skip-00
Published: 17 April 2024
Intended Status: Informational
Expires: 19 October 2024
Authors: R. Singh, Ed. *Cisco Systems, Inc.* D. McGrew *Cisco Systems, Inc.* C. Hill *Cisco Systems, Inc.* S. Kawaguchi *QuSecure, Inc.*
J. Lupo *QuSecure, Inc.*

Secure Key Integration Protocol (SKIP)

Abstract

This document describes the Secure Key Integration Protocol (SKIP), a two-party protocol that allows a device to securely obtain secret keys from an independent key provider. The protocol is designed to facilitate the secure distribution of keys over a network.



Internet-Draft SKIP April 2024

The secrecy of the shared secret key offers protection from quantum attacks. Therefore, it is imperative that all of the cryptography used in SKIP, must be quantum-safe. This includes the cryptography that safeguards the communication between the encryptor and SKP, as well as any other cryptography in use.

3. Protocol Overview

SKIP defines the interface through which encryptors can obtain a shared secret key from the SKPs. Figure 2 provides an overview of the steps involved

Figure 2: SKIP Key Exchange

1. The encryptor Alice initiates a request to SKP A for key.
2. SKP A responds with a key and an unique key id associated with the key. It also synchronizes the key with SKP B and zeroizes the local copy.
3. The encryptor Alice establishes a connection with its peer, encryptor Bob and exchanges the key id.
4. The encryptor Bob initiates a request to SKP B for key associated with the unique key id.
5. SKP B responds with the key associated with the key id and the local copy is zeroized.

At the end of this exchange both encryptors Bob and Alice possess the same shared secret key. The shared secret can be utilized by encryptors to add quantum resistance to any existing security protocol, Section 6 provides an example with IKEv2 PPKs.

In order to accommodate more complex arrangements such as multiple SKPs connected to a single encryptor, or multipoint topologies, we require that each SKP is configured with a local system ID and with the list of remote SKP device IDs it can be paired with. This information is made available to the encryptors during the initialization (see GET capabilities Section 5.1).

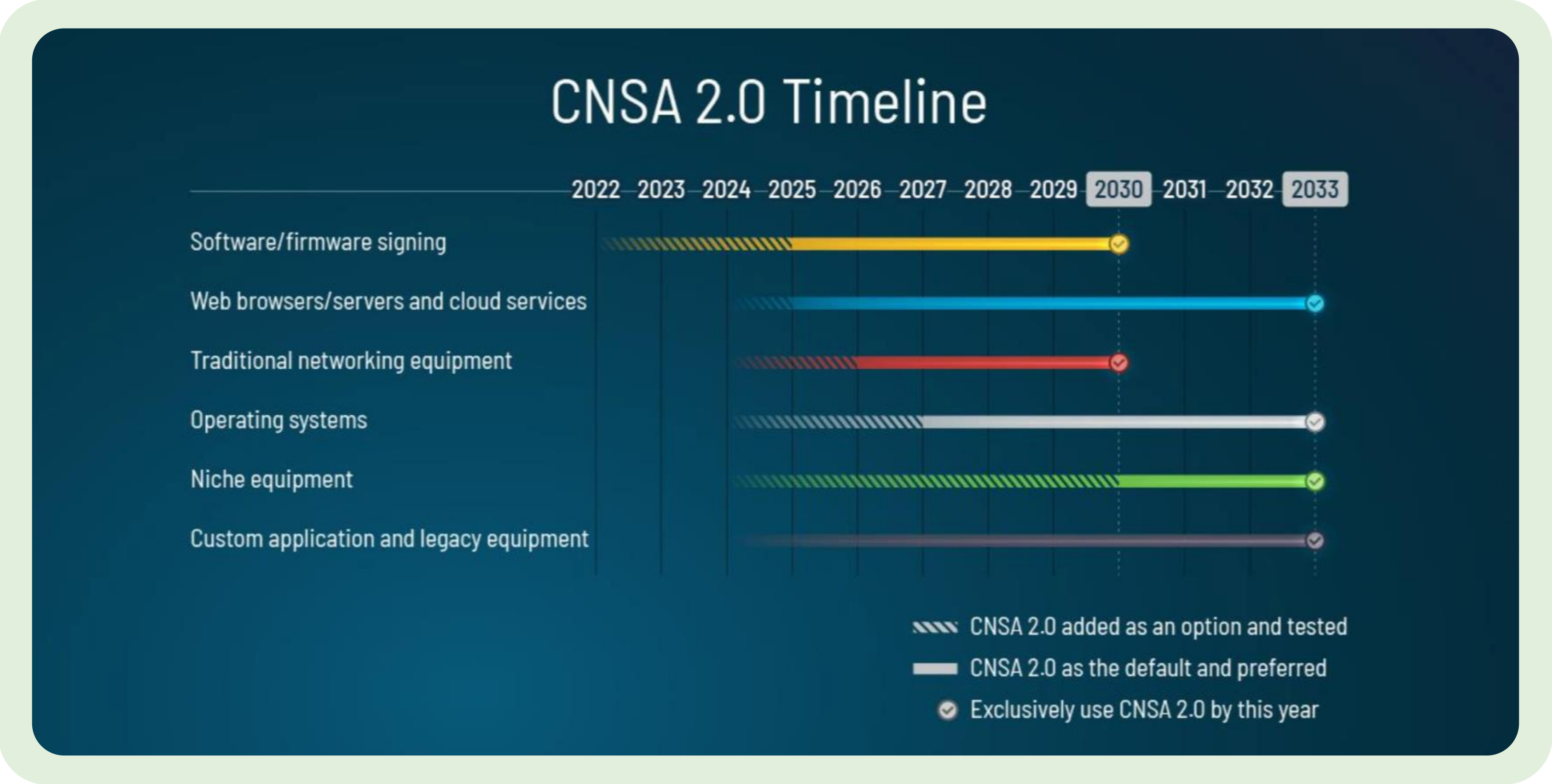
Forward Goals

Early Investments in Post Quantum Ciphers

- Focused investment in Post Quantum ciphers offers an ability to do some initial up front work to yield out year revenue

- Control Plane Post Quantum Security is a focus with low initial resistance

NSA | Commercial National Security Algorithm Suite 2.0



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

Secure Client PQ Roadmap

Secure Client Remote Access

HYBRID
- Phase 0: Multi-Round 9370 (r1 – legacy crypto, r2 - ML-KEM-1024)

HYBRID
- Phase 1: Single Round ML-KEM 1024 – RFC 9370

NATIVE
- Phase 2: Native IKEv2 ML-KEM 1024 – RFC unknown (2026)

NATIVE
- Phase 3: PQ-TLS 1.3 Integration – RFC unknown (2026)

Post-Quantum Encryption Solutions @Cisco...

What is real?

What is Real @ Cisco - Agenda

01 Foundation to Quantum Safe Network Encryption

02 Current Quantum Safe Deployment Options for IPSec and MACsec

03 “Bring your own key server…” What? How?

04 Testing Results for External Key Server Examples for IPSec / MACsec

05 Summary / Reference Docs

Foundation to Quantum Safe Network Encryption

IPSec Support: Mixing Preshared Keys in IKEv2 for early quantum-resistant deployments (RFC 8784)

MACsec Support: Leveraging existing Symmetric Key framework with MKA enhancements to provide quantum-resistant MACsec capabilities

Foundation to Quantum Safe Network Encryption

IPSec Support: Mixing Preshared Keys in IKEv2 for early quantum-resistant deployments (RFC 8784)

MACsec Support: Leveraging existing Symmetric Key framework with MKA enhancements to provide quantum-resistant MACsec capabilities

3rd Party Key Source Support: Using the open standard Secure Key Import Protocol (SKIP), offer the ability to dynamically distribute quantum safe keys to external Cisco devices

Foundation to Quantum Safe Network Encryption

IPSec Support: Mixing Preshared Keys in IKEv2 for early quantum-resistant deployments (RFC 8784)

MACsec Support: Leveraging existing Symmetric Key framework with MKA enhancements to provide quantum-resistant MACsec capabilities

3rd Party Key Source Support: Using the open standard Secure Key Import Protocol (SKIP), offer the ability to dynamically distribute quantum safe keys to external Cisco devices

Leverage Industry Standards: Support a combination of evolving open standards for Post-Quantum Cryptography, including NIST, IETF, ETSI and government standards (CNSA 2.0)

Network Encryption Use Cases (Govt & Enterprises)

Top Candidates Applications for Post Quantum Encryption? All of them ☺

IPSec (IP Transport)

- Point to point IP applications
- Backhaul to Hub/PoP/Colocation
- Tactical edge (LTE, 5G, LEO, SatCom)
- Colocation-to-Cloud
- Colocation-to-Colocation
- Inter-Cloud region (CSP global backbone)
- TRANSEC (Ext encryption obfuscation)
- * CSfC (inner / outer)

MACsec (Ethernet Transport)

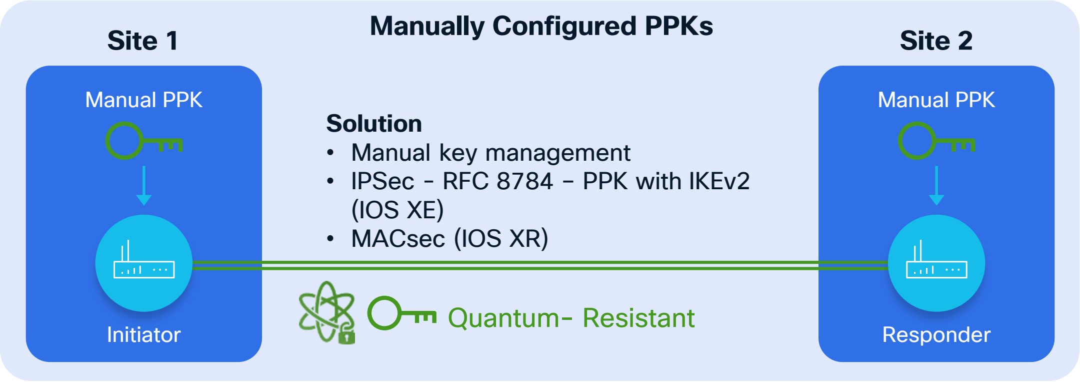
- High-speed data center interconnect (DCI)
- Core Backbone (ELINE) security (SR/SRv6)
- Secure PE to CE (L3 VPN service)
- Metro Ethernet Deployments
- *? Colocation-to-Cloud (Ex: AWS DirectConn)
- Colocation-to-Colocation (Equinix Fabric)
- Underlay optical / TRANSEC (External Encryptors)
- * CSfC (outer - high-speed)

*** CSfC - Commercial Solutions for Classified (unique to US Government)**

Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

Manual Options

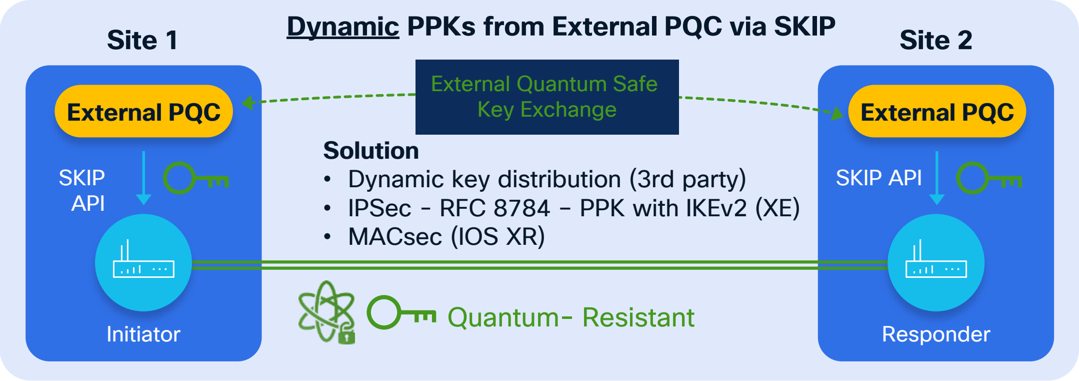


Manually Configured PPKs

Solution

- Manual key management
- IPSec – RFC 8784 – PPK with IKEv2 (IOS XE)
- MACsec (IOS XR)

Dynamic Options



Dynamic PPKs from External PQC via SKIP

Solution

- Dynamic key distribution (3rd party)
- IPSec – RFC 8784 – PPK with IKEv2 (XE)
- MACsec (IOS XR)

Network Encryption Options:

RFC 8784 – PPK based IPsec encryption keys

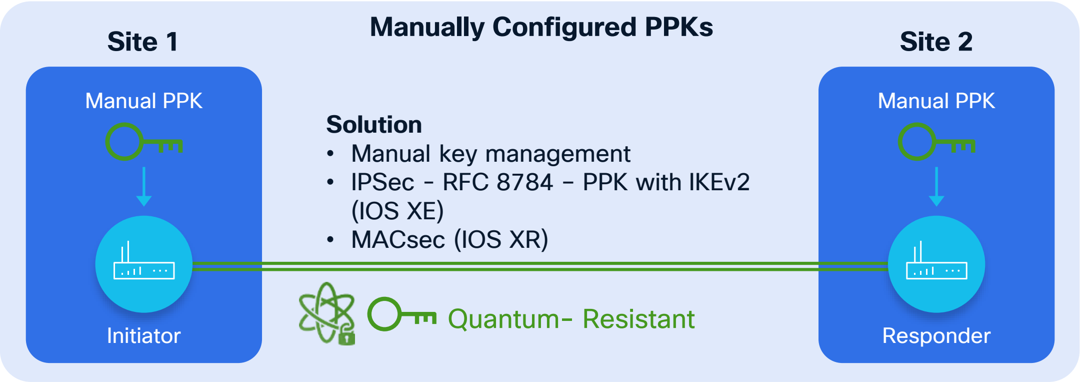
IEEE 802.1AE MACsec – PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

Current Technology and Deployment Options

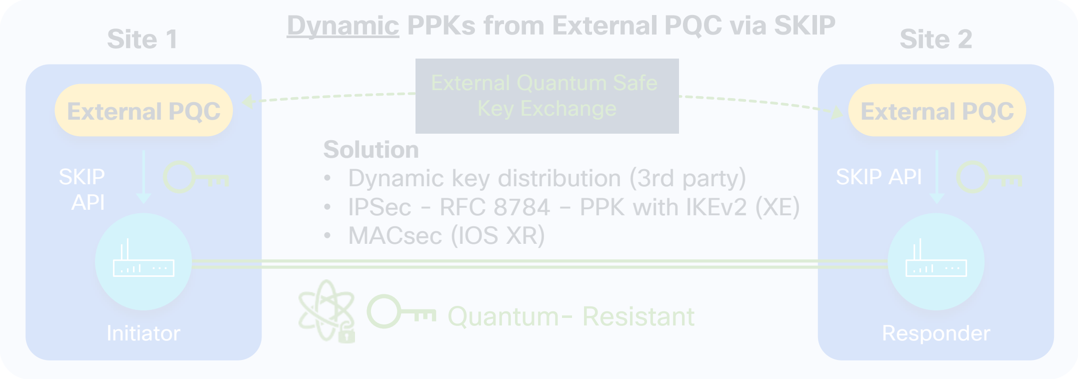
Quantum-Safe Encryption Options – Available Today

Manual Options



Solution
- Manual key management
- IPSec – RFC 8784 – PPK with IKEv2 (IOS XE)
- MACsec (IOS XR)

Dynamic Options



Solution
- Dynamic key distribution (3rd party)
- IPSec – RFC 8784 – PPK with IKEv2 (XE)
- MACsec (IOS XR)

Network Encryption Options:

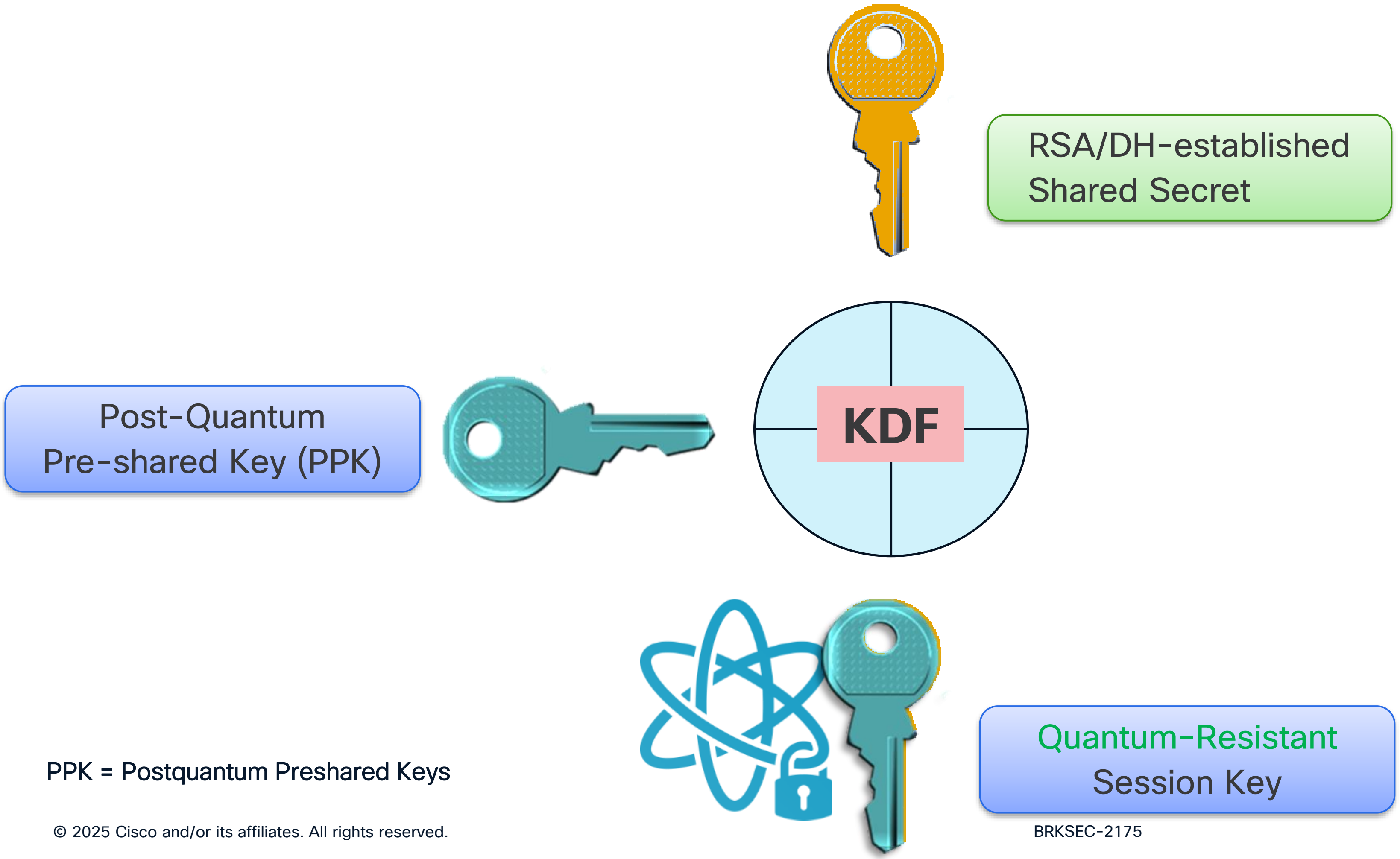
RFC 8784 – PPK based IPsec encryption keys

IEEE 802.1AE MACsec – PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

RFC 8784 : Quantum-Resistant Session Keys

RFC 8784: defines **negotiation of PPK capability**, **communication of PPK ID**, **mixing of PPK** as an additional input in the **session key derivation**, and optional fallback to a non-PPK-based session.



The general idea is an additional secret ***(sufficient entropy, Ps Random Func, encryption, auth)*** is added and shared between the initiator and the responder;

This secret is in addition to the authentication method that is already provided within IKEv2.

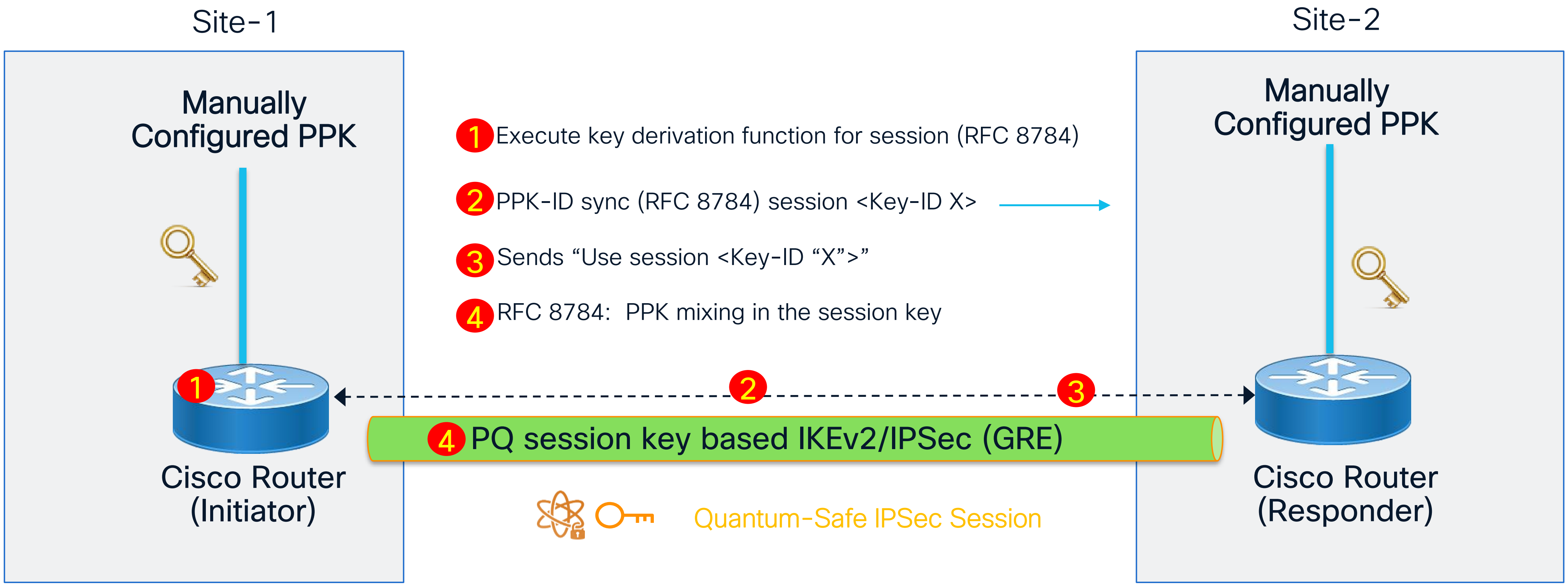
The secret is stirred into a value, which is used to generate the key material. The outcome secret provides a quantum resistance for the IPSec SA's and any subsequent IKE SA's, and the method allows both sides to detect a mismatch cleanly.

PPK = Postquantum Preshared Keys

RFC 8784 with Quantum-Safe IKEv2/IPSec Session

Manual PPK for IPSec - Example

RFC-8784 -Mixing Pre-shared Keys in IKEv2 for Post-Quantum Security



Site-1

Manually Configured PPK

Cisco Router (Initiator)

Site-2

Manually Configured PPK

Cisco Router (Responder)

1 Execute key derivation function for session (RFC 8784)

2 PPK-ID sync (RFC 8784) session <Key-ID X>

3 Sends "Use session <Key-ID "X">"

4 RFC 8784: PPK mixing in the session key

4 PQ session key based IKEv2/IPSec (GRE)

Quantum-Safe IPSec Session

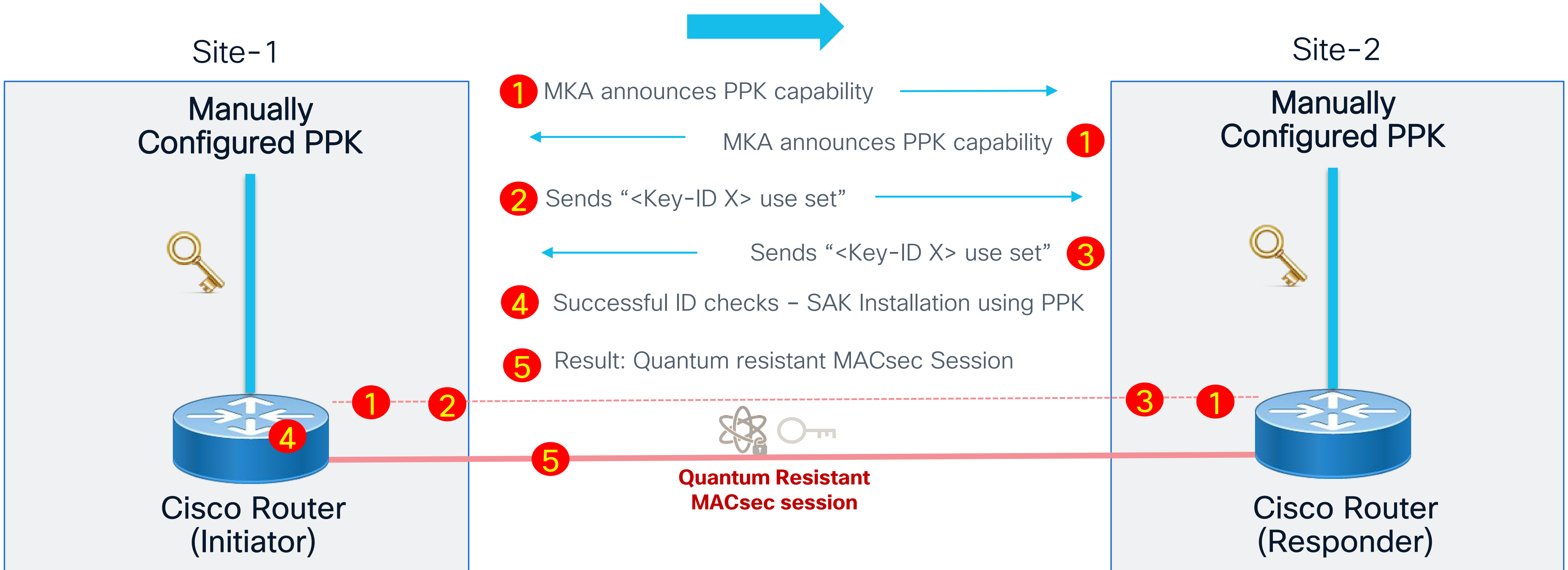
PQ PPK mix with DH is never transmitted (per RFC 8784)

IOS-XE Support: Since 17.11.1a

PPK = Postquantum Preshared Keys

Quantum-Safe MACsec with Preshared Keys

Example - Manual PPK for MACsec



1 MKA announces PPK capability →

← MKA announces PPK capability 1

2 Sends “<Key-ID X> use set” →

← Sends “<Key-ID X> use set” 3

4 Successful ID checks – SAK Installation using PPK

5 Result: Quantum resistant MACsec Session

IOS-XR Support: Since 7.9.1 / 7.10.1

- To support QR MACsec key distribution, extensions to MKA are applied to carry the PPK_ID as the SAK identifier (instead of the secret HW key)
- Symmetric key encryption, leveraged by MACsec algorithms (like AES) is considered to be quantum-safe
- MACsec with symmetric keys using AES is not as vulnerable to quantum threats as asymmetric encryption as they do not leverage the same mathematical problems that are vulnerable

“Bring your own key server… “

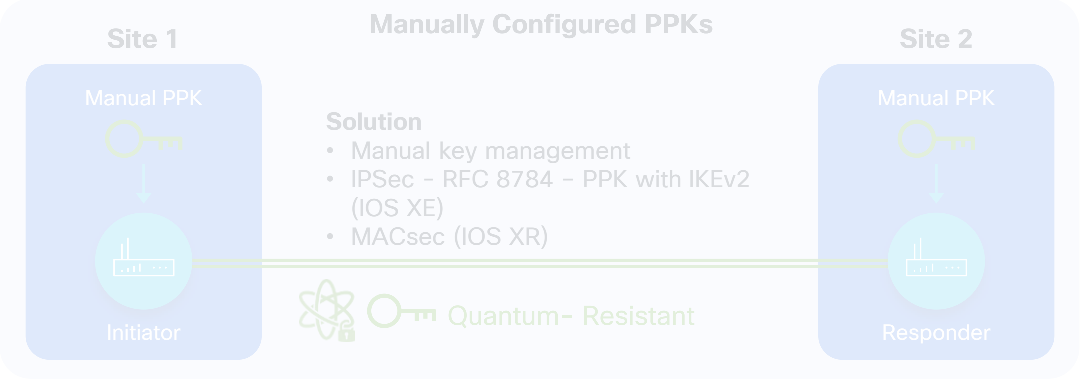
How To Import Post Quantum Keys to Cisco Devices via 3rd Party Key Sources

PPK = Postquantum Preshared Keys

Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today

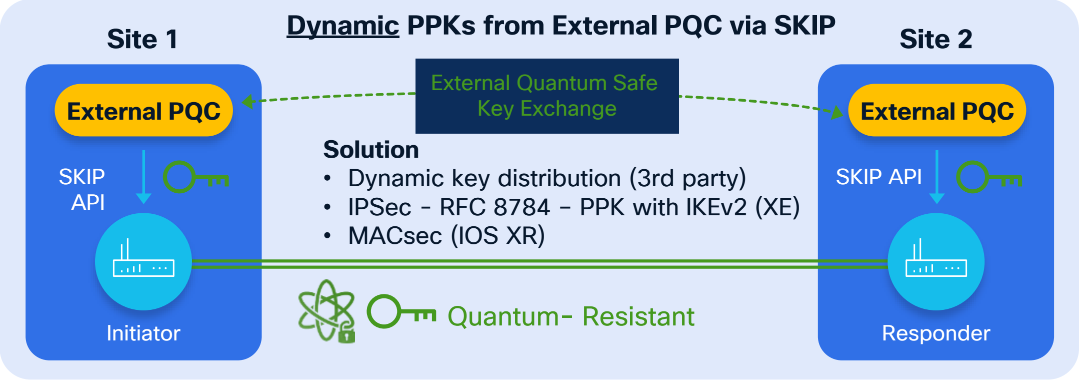
Manual Options



Solution

- Manual key management
- IPSec – RFC 8784 – PPK with IKEv2 (IOS XE)
- MACsec (IOS XR)

Dynamic Options



Solution

- Dynamic key distribution (3rd party)
- IPSec – RFC 8784 – PPK with IKEv2 (XE)
- MACsec (IOS XR)

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

Dynamic Network Encryption Options:

- RFC 8784 – PPK based IPsec encryption keys
- IEEE 802.1AE MACsec – PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

Cisco Secure Key Integration Protocol (SKIP)

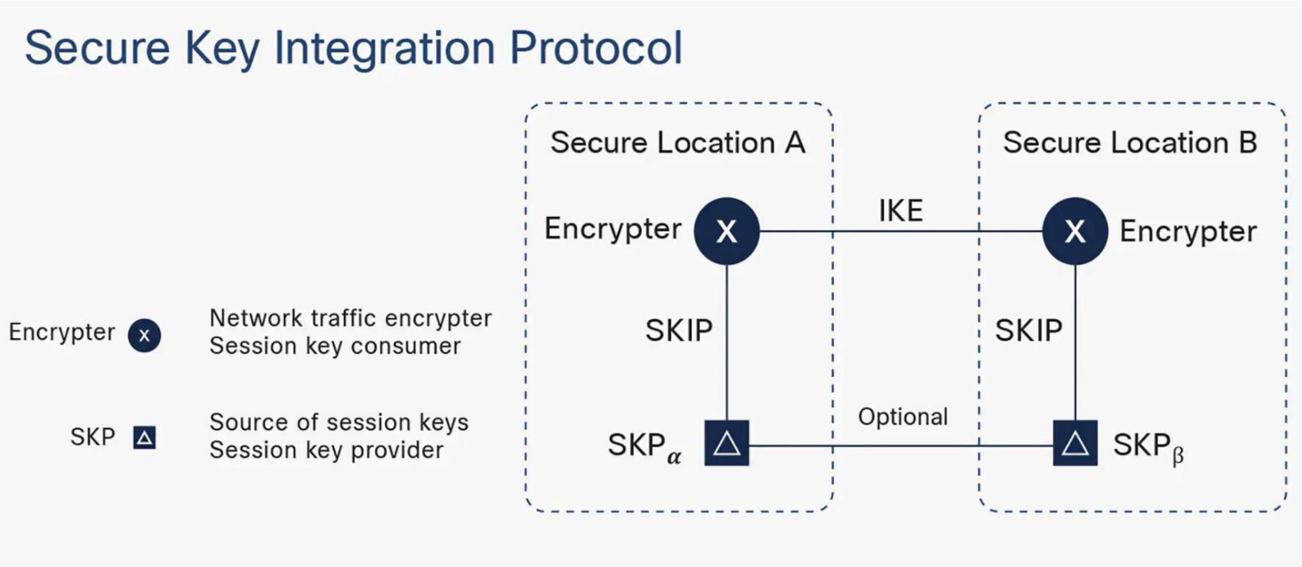
Leverage Existing Encryption with Post Quantum Security Methods

Cisco built a protocol called **Secure Key Integration Protocol (SKIP)**

SKIP uses TLS 1.2 with PSK-DHE cipher suite that makes the SKIP protocol quantum-safe

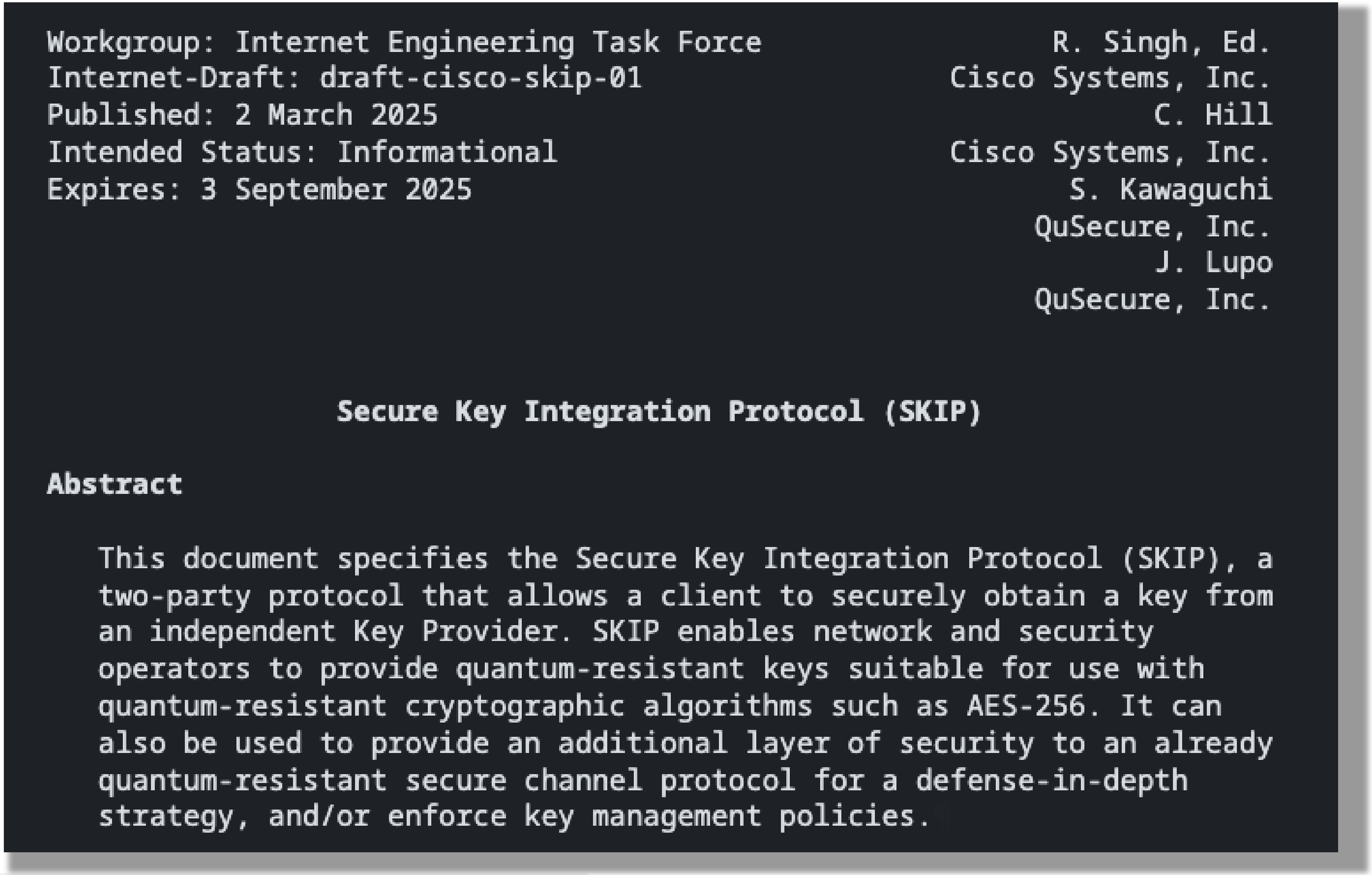
For a 3rd-party external key source to be SKIP compliant, it must (1) implement the Cisco SKIP protocol/API and (2) use an out-of-band synchronization mechanism to provide identical PPK to the two Cisco encryption devices.

SKIP allows an operator to leverage existing IPSec or MACsec and takes advantage of PQ external sources such as QKD, PQC, pre-shared keys, or other post-quantum-secure methods.



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

Early IETF Draft Submission for SKIP



```
Workgroup: Internet Engineering Task Force                  R. Singh, Ed.
Internet-Draft: draft-cisco-skip-01                   Cisco Systems, Inc.
Published: 2 March 2025                                           C. Hill
Intended Status: Informational                        Cisco Systems, Inc.
Expires: 3 September 2025                                    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

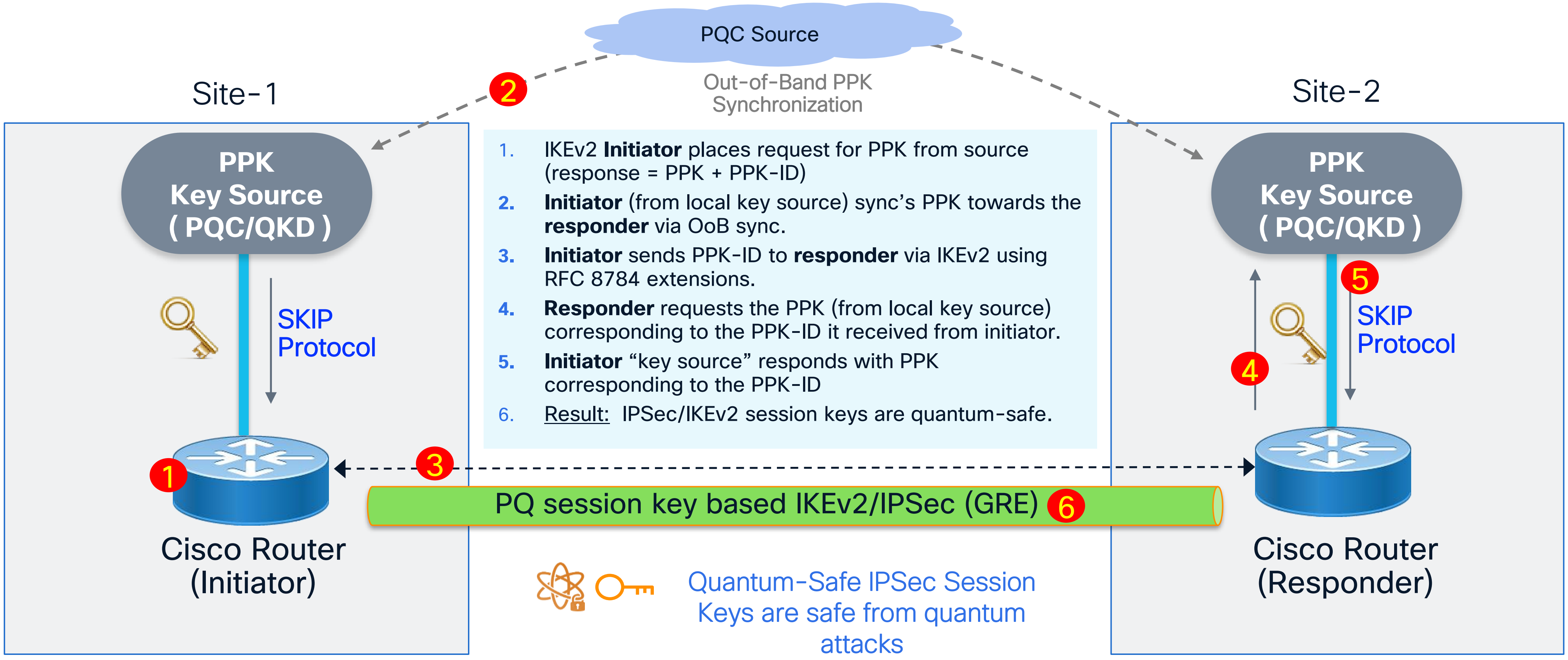
IPSec/IKEv2
MACsec

QuSecure

QUANTUMXCHANGE

RFC 8784 with Quantum-Safe IKEv2/IPSec Session

Dynamic PPK Example with SKIP


PQC Source
Out-of-Band PPK Synchronization
Site-1
Site-2
PPK Key Source (PQC/QKD)
PPK Key Source (PQC/QKD)
SKIP Protocol
SKIP Protocol
1
2
3
4
5
Cisco Router (Initiator)
Cisco Router (Responder)
PQ session key based IKEv2/IPSec (GRE) 6

1. IKEv2 **Initiator** places request for PPK from source (response = PPK + PPK-ID)
2. **Initiator** (from local key source) sync's PPK towards the **responder** via OoB sync.
3. **Initiator** sends PPK-ID to **responder** via IKEv2 using RFC 8784 extensions.
4. **Responder** requests the PPK (from local key source) corresponding to the PPK-ID it received from initiator.
5. **Initiator** "key source" responds with PPK corresponding to the PPK-ID
6. Result: IPSec/IKEv2 session keys are quantum-safe.

Quantum-Safe IPSec Session Keys are safe from quantum attacks

In RFC-8784, the PPK is never sent over the wire, only the PPK-ID that corresponds to that PPK (sync'ed over OoB channel).

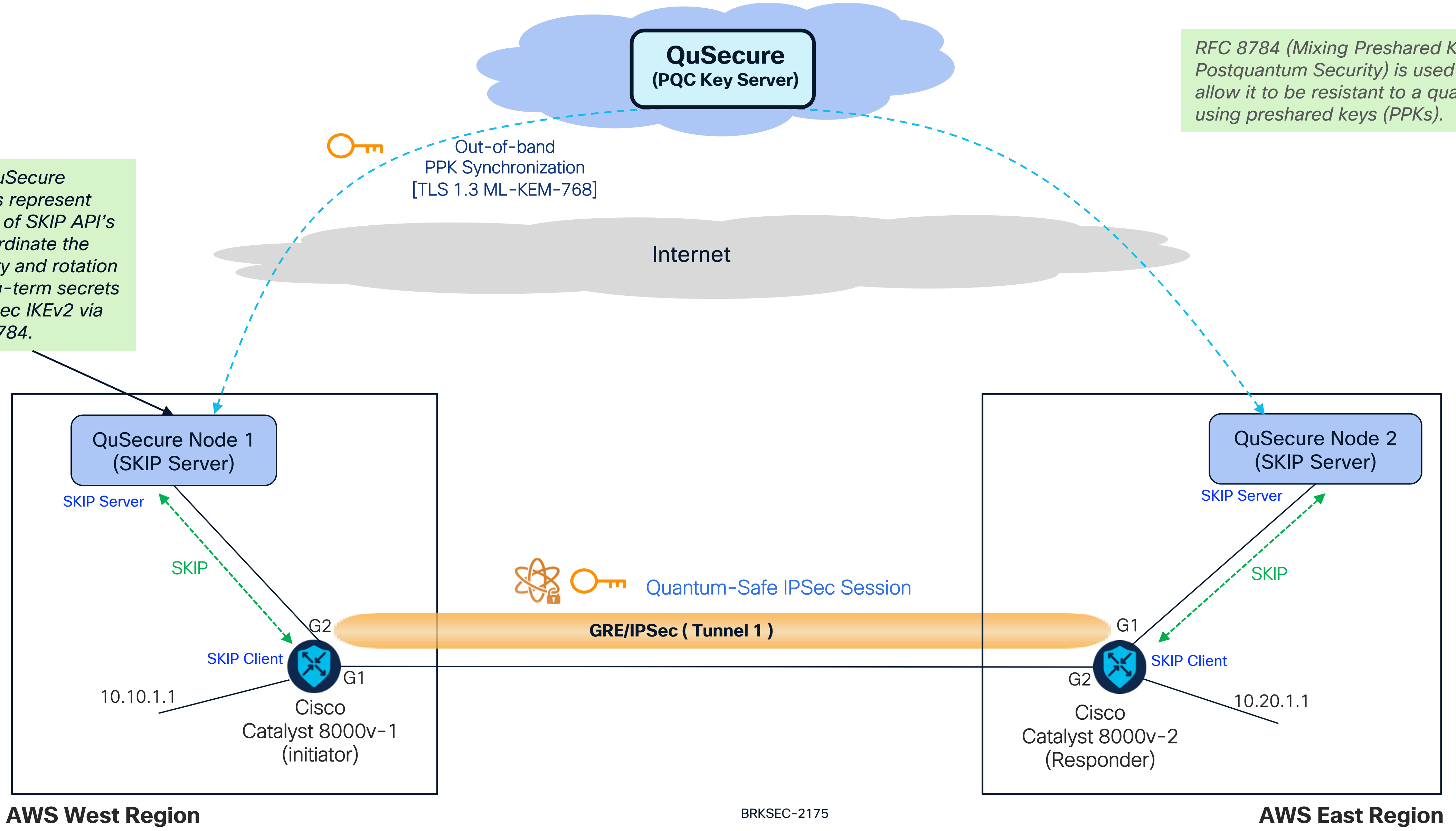
PPK = Postquantum Preshared Keys

IPSec/IKEv2 Quantum Safe Demo Using Dynamic PQ Preshared Keys

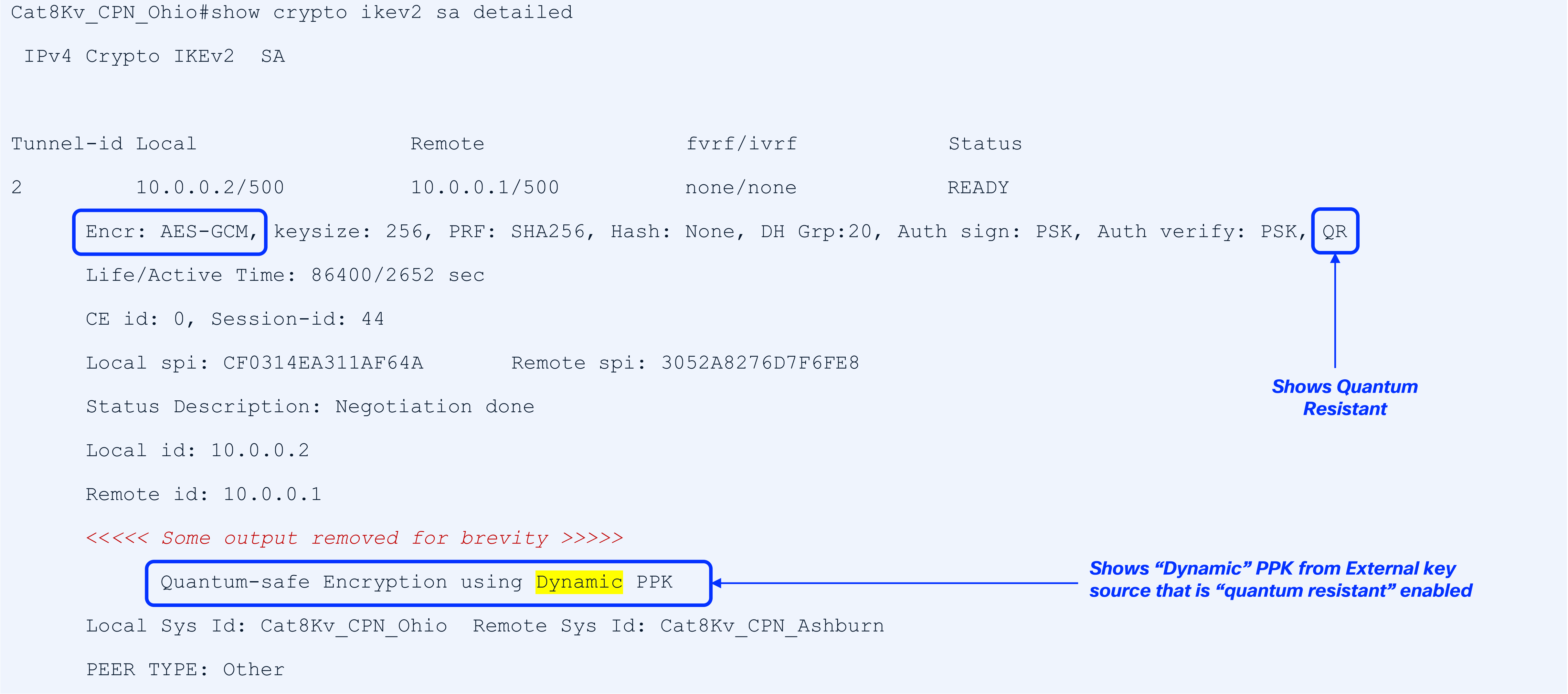
Demo: Cisco IOS-XE Catalyst 8000v using SKIP with 3rd Prty PQC (QuSecure)

RFC 8784 (Mixing Preshared Keys in IKEv2 for Postquantum Security) is used with IKEv2 to allow it to be resistant to a quantum computer by using preshared keys (PPKs).

The QuSecure Node's represent mgmt. of SKIP API's to coordinate the delivery and rotation of long-term secrets for IPSec IKEv2 via RFC 8784.



SHOW Output



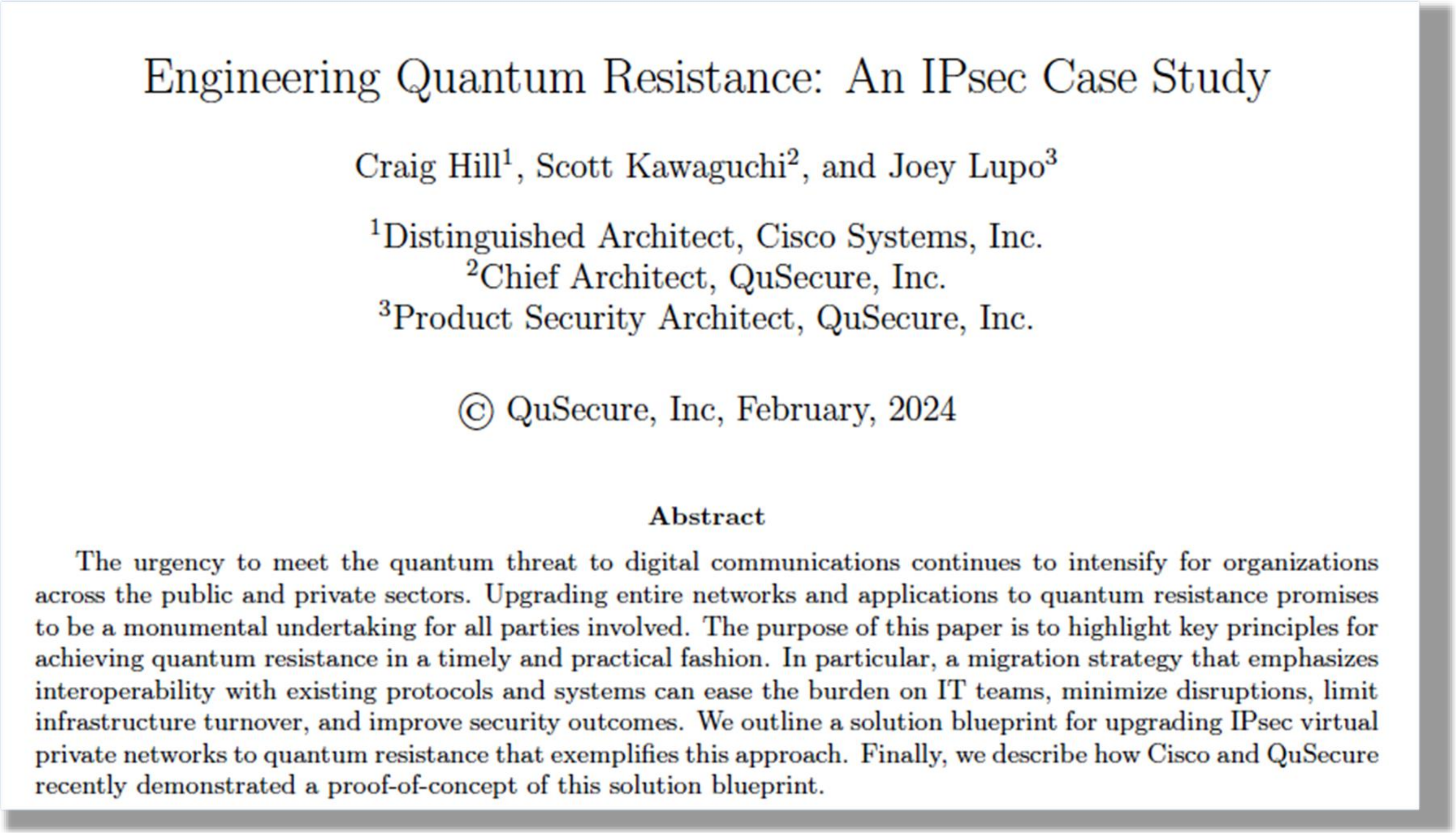
```
Cat8Kv_CPN_Ohio#show crypto ikev2 sa detailed

 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/

Post-Quantum IOS-XR Demo Topology

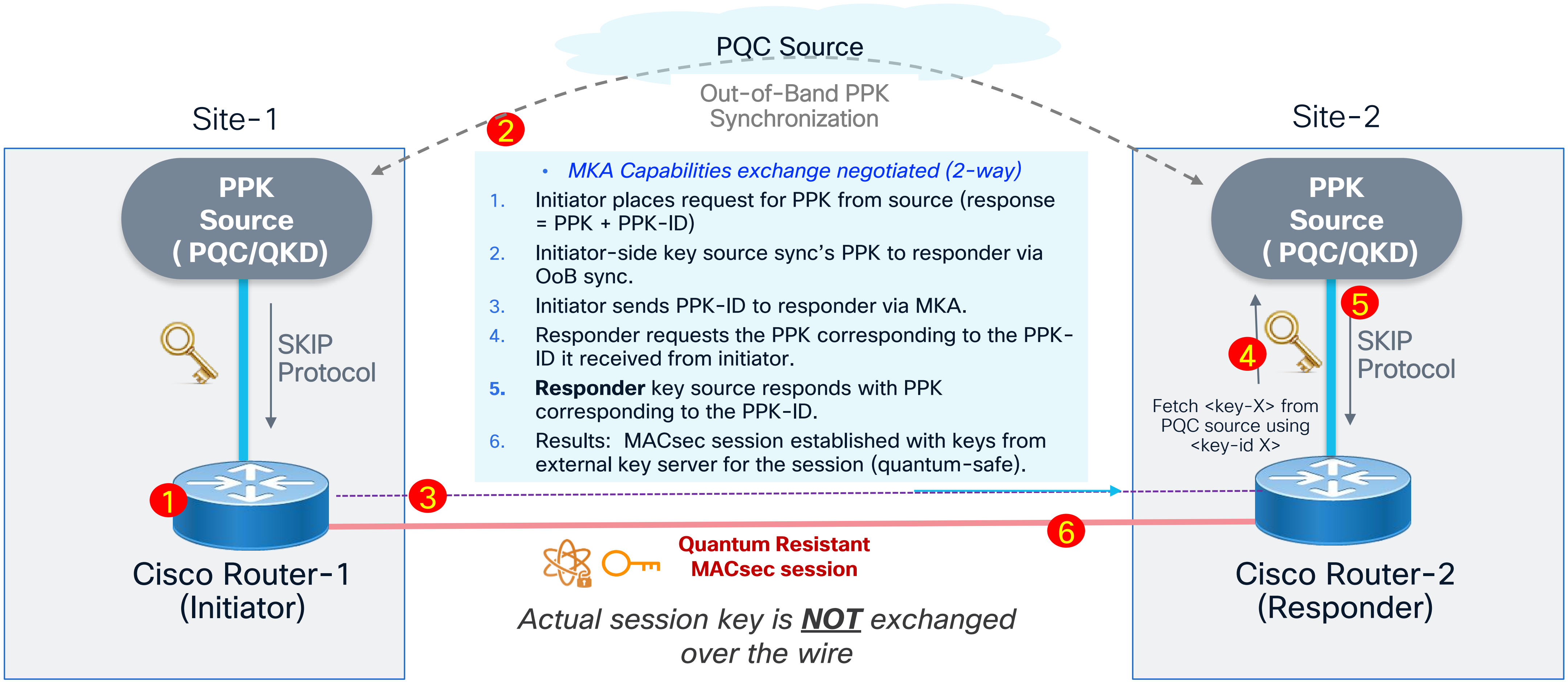
MACsec + SKIP using External Key Source

Thanks to Lab Contributors:

Chennakesava Reddy Gaddam
Rakesh Kandula
Joey Lupo (QuSecure)

Quantum-Safe MACsec with PQC Key Server

Using Dynamic PPK Example with SKIP


PQC Source
Out-of-Band PPK Synchronization
Site-1
Site-2
PPK Source (PQC/QKD)
SKIP Protocol
PPK Source (PQC/QKD)
SKIP Protocol
Fetch <key-X> from PQC source using <key-id X>
1
2
3
4
5
6
Cisco Router-1 (Initiator)
Cisco Router-2 (Responder)
Quantum Resistant MACsec session

- *MKA Capabilities exchange negotiated (2-way)*

1. Initiator places request for PPK from source (response = PPK + PPK-ID)
2. Initiator-side key source sync's PPK to responder via OoB sync.
3. Initiator sends PPK-ID to responder via MKA.
4. Responder requests the PPK corresponding to the PPK-ID it received from initiator.
5. **Responder** key source responds with PPK corresponding to the PPK-ID.
6. Results: MACsec session established with keys from external key server for the session (quantum-safe).

*Actual session key is **NOT** exchanged over the wire*

- Software-based key source (pre-standard) with Quantum safe key generation
- Not limited to distance limitations or additional HW
- Auto-key management, refresh, and entropy
- Supported from IOS-XR 7.9.1/17.10.1 release (platform dependent)

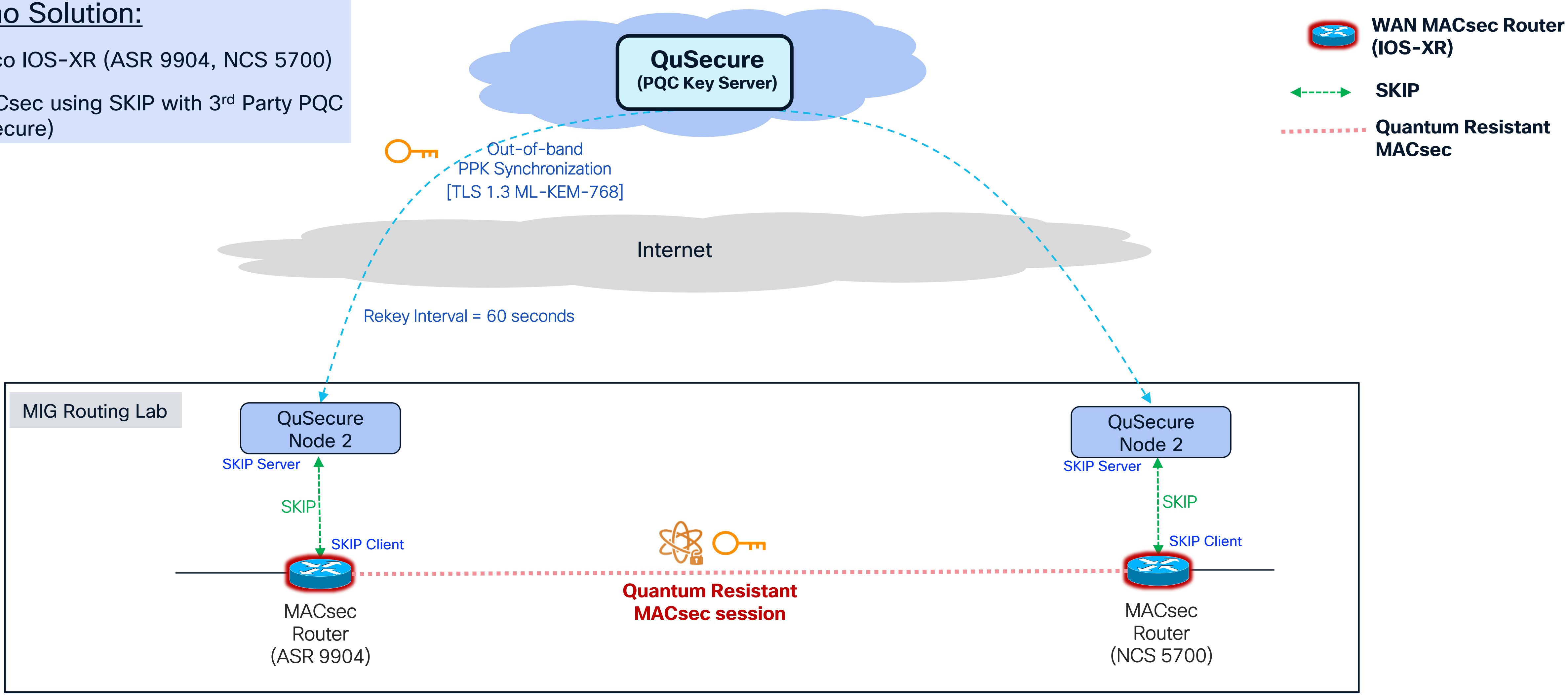
MKA Session

Blog Link: https://blogs.cisco.com/sp/safeguard-your-network-in-a-post-quantum-world

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
 !
!
```

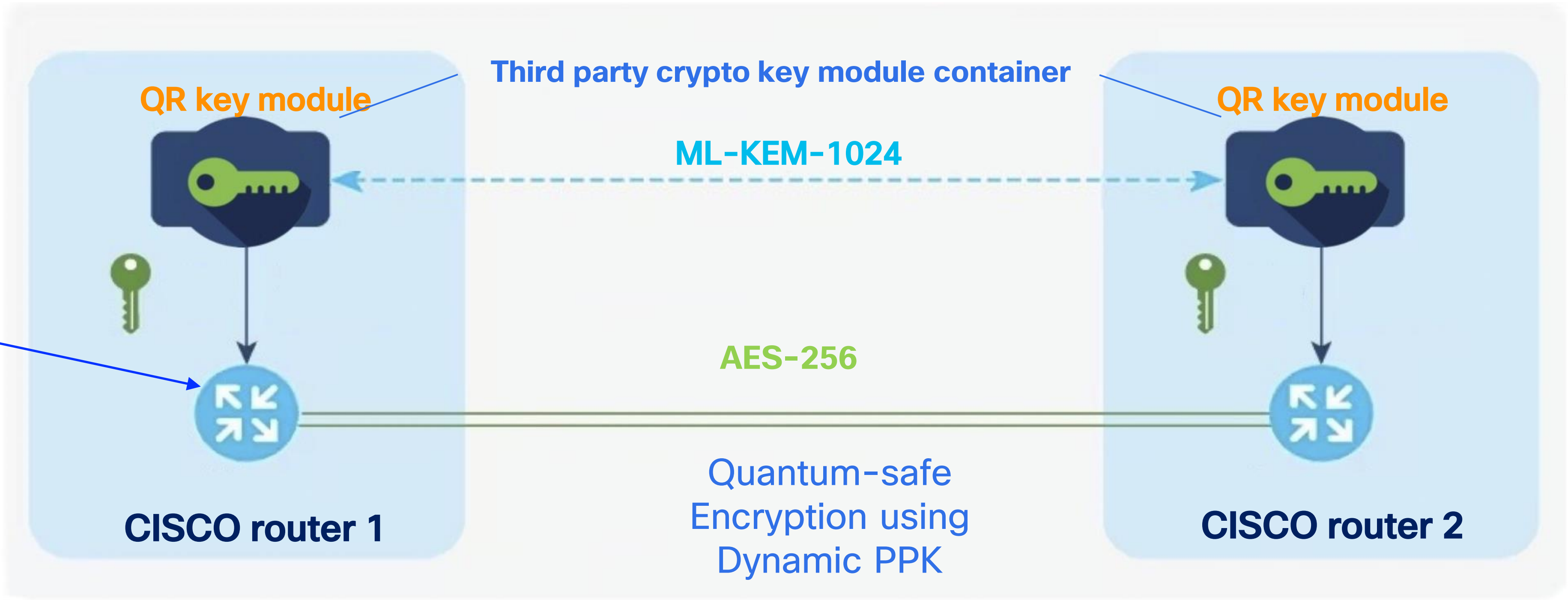
Shows Remote Dynamic PQC Server ("quprotect-core" is the dynamic key server [QuSecure PQC])

IPSec & MACsec Using Dynamic PPK

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

QUANTUM XCHANGE

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



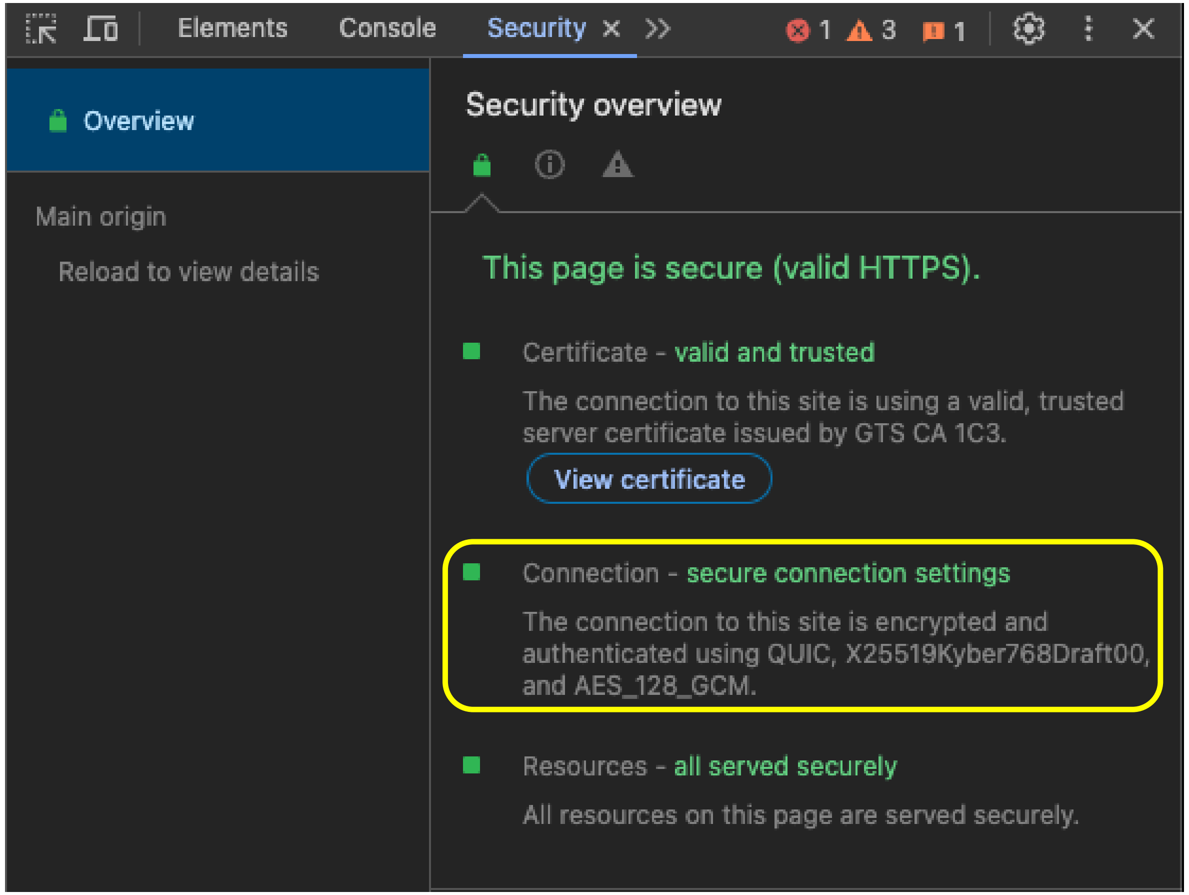
Third party crypto key module container
QR key module
QR key module
ML-KEM-1024
AES-256
CISCO router 1
Quantum-safe Encryption using Dynamic PPK
CISCO router 2

- 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)

Example: Hybrid TLS 1.3 on Chrome Web Browser

Pre NIST Standard



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by GTS CA 1C3.

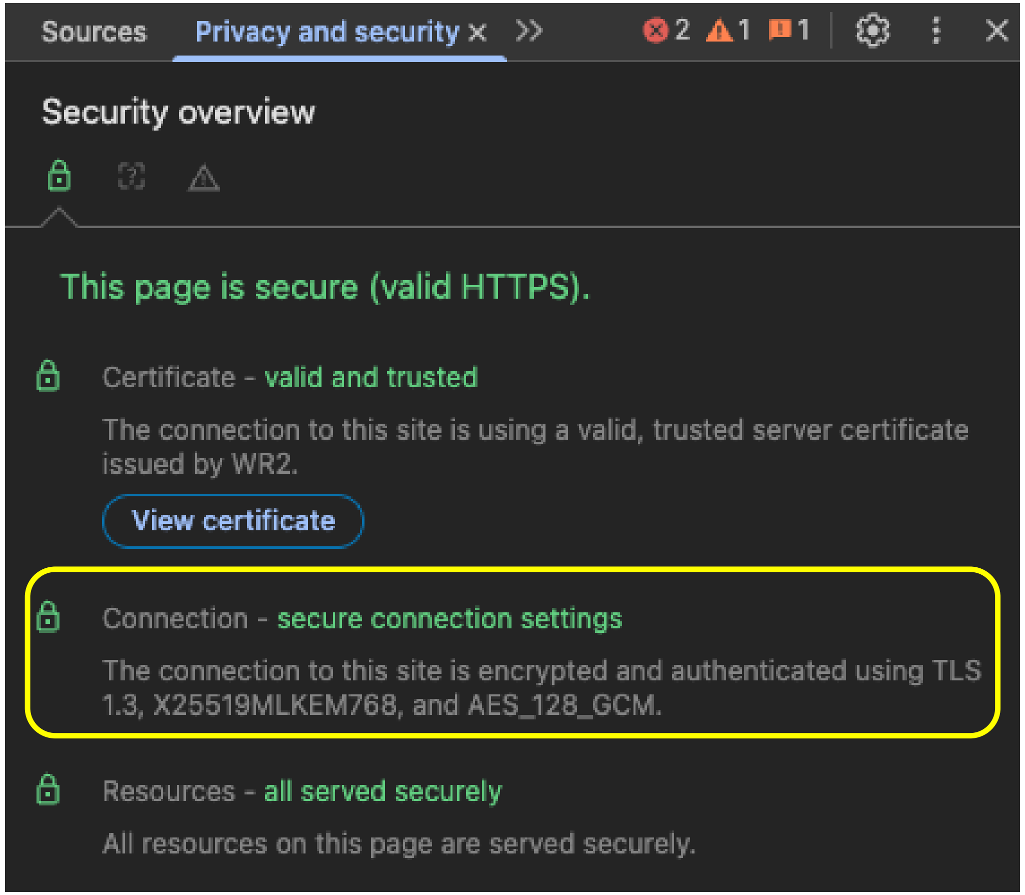
Connection - secure connection settings

The connection to this site is encrypted and authenticated using QUIC, X25519Kyber768Draft00, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

Post NIST Standard



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by WR2.

Connection - secure connection settings

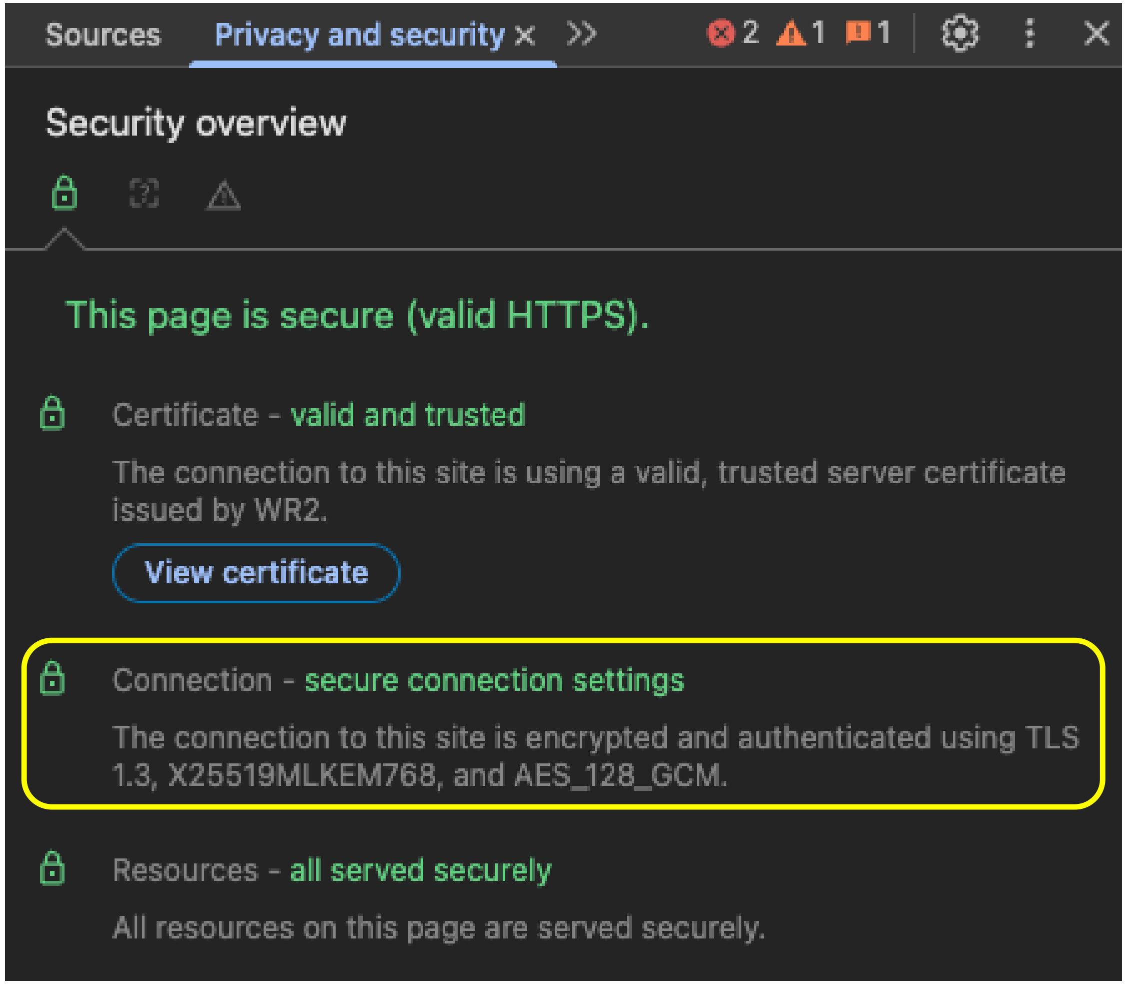
The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

Example: Hybrid TLS 1.3 on Chrome Web Browser

(as of June 2, 2025)



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by WR2.

View certificate

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

- 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

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

Session Summary

- US Government has provided clear direction for requirements on Quantum Resistance for protection of National Security Systems
- All aspects of encryption should drive towards Quantum Resistance encryption options
- The transition to early quantum-safe network encryption can begin now
- Cisco offers operators the ability to begin the post-quantum encryption offerings for IPSec (RFC 8784 for IPSec) and MACsec (early MKA extensions)
- SKIP enables the use of external/3rd-party key servers for those customers wanting to “Bring their own keys” and leverage external key population to Cisco devices
- Cisco will continue to drive encryption and network standards (IETF, NIST) for both new and existing (hybrid) transition methods
- Identify your company/agency top priority area to begin the transition

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 2026.

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

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

Thank you

CISCO Live!

cisco