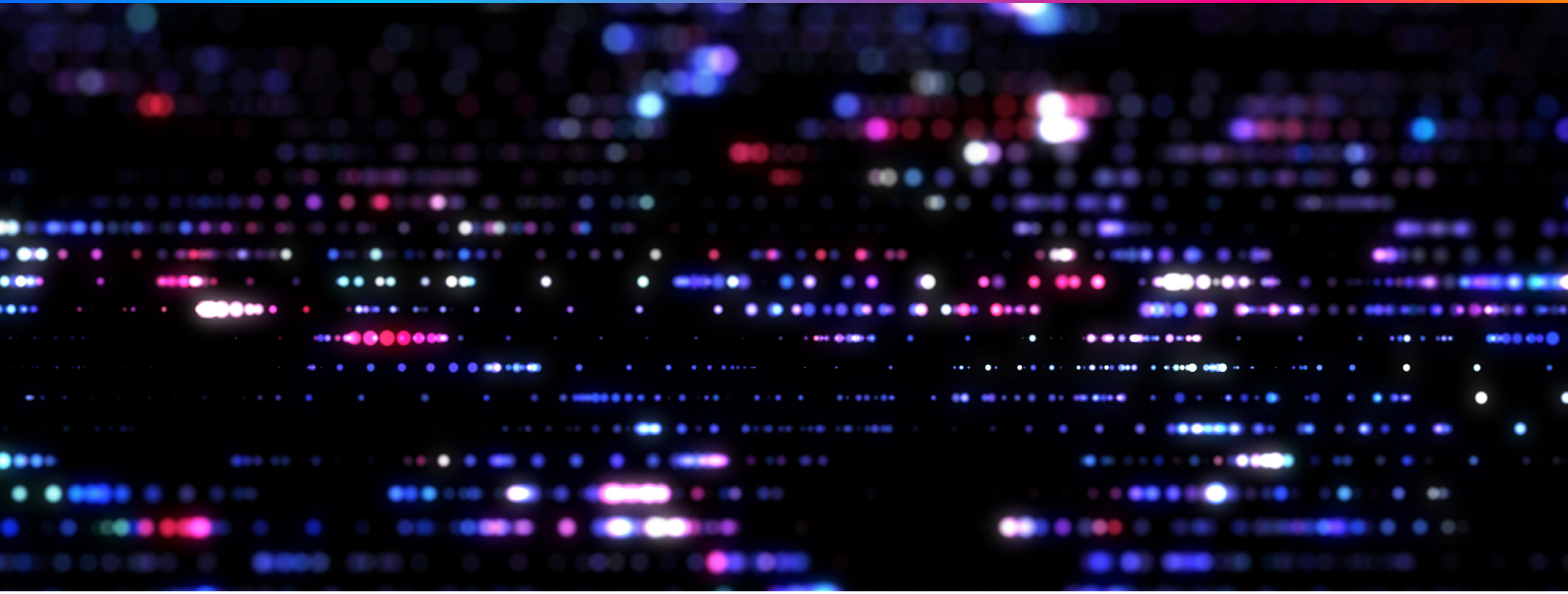


The Journey to Post-Quantum Cryptography in WAN Infrastructure

Why network modernization is the first step in post-quantum readiness

White paper Public

Executive summary

Your network never sleeps. Every second, critical data flows through your wide-area network (WAN) infrastructure–financial transactions, intellectual property, customer records, and strategic communications. This constant data movement makes the WAN the lifeblood of modern business operations, and one of the most critical assets to protect.

Today, virtually all enterprise WAN traffic is secured through cryptographic protocols like IPsec and MACsec. The advanced encryption standard (AES) and other symmetric encryption algorithms protecting this data are exceptionally strong. However, there's a critical vulnerability: these systems fundamentally depend on public key cryptography to establish and exchange secret keys that enable secure communications.

This dependency creates an urgent challenge. Quantum computing is advancing rapidly, and we are approaching "Q-Day"–the point at which cryptanalytically relevant quantum computers (CRQCs) will break current public key encryption in minutes. More concerning, adversaries are already executing harvest now, decrypt later (HNDL) attacks, in which they collect encrypted data today to decrypt once quantum computers become available.

This paper provides essential guidance to address this looming threat. We examine the specific risks posed by quantum computing and advocate for a WAN-first security approach–prioritizing your always-on network infrastructure where data constantly flows. We outline the post-quantum cryptography (PQC) algorithms standardized by national security agencies worldwide, describe evolving protocol requirements, and present architectural best practices for migrating to quantum-resistant security. The time to act is now, before your encrypted data becomes an open book.

Anticipating the quantum threat: Why your data is at risk

Imagine a scenario in the near future: A bank completes its annual audit. Systems are compliant and sensitive data is encrypted. Customers trust this protection.

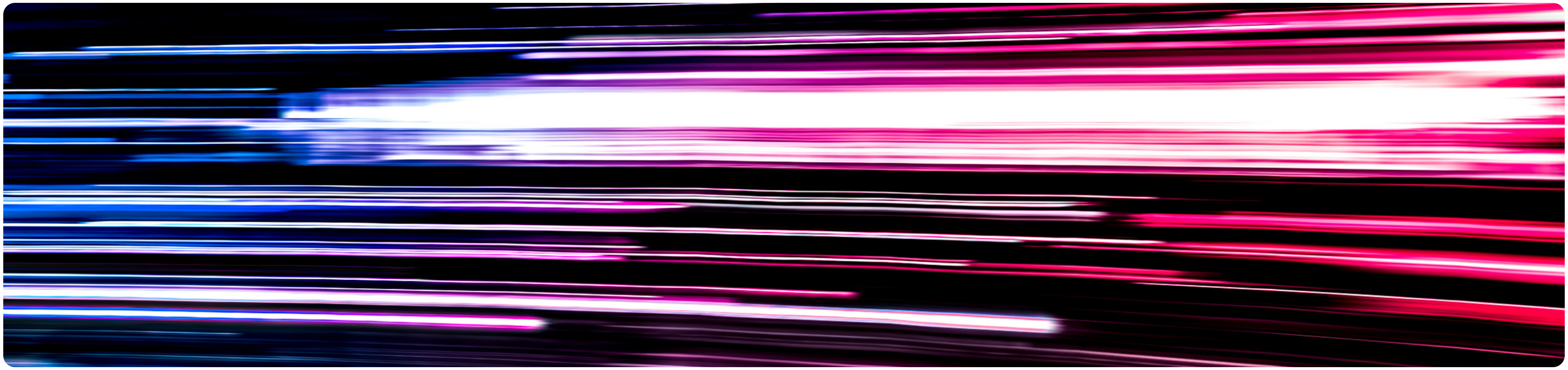
Yet an attacker has been quietly collecting encrypted data for years, anticipating the arrival of powerful quantum computers. When that day comes, the encryption that safeguards accounts and personal details is suddenly rendered useless. Transaction histories, account information, and private communications are exposed, leading to fraud, identity theft, and significant financial loss for millions.

The critical question for the bank—and for any organization—becomes, "Why weren't they prepared for the quantum era, despite clear industry warnings?"

According to the 2025 Cisco Cybersecurity Readiness Index, 31% of respondents ranked the network as the most challenging area to protect against cyberattacks—more than any other area.

New U.S. government regulations, including Federal Information Processing Standards (FIPS), Common Criteria, and the National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) program, are making PQC-certified encryption mandatory for national security systems by December 2031.

Amid rising traffic, the proliferation of AI applications, and increasingly complex threats, proactively securing the WAN with quantum-safe solutions is critical to network resilience—and the logical starting point for your quantum-safe journey.



Prioritizing PQC: Why the WAN is your quantum front line

Today's business-critical data flows seamlessly across data centers, branch offices, and cloud environments—often crossing the WAN, where sensitive information is most exposed in transit. These data flows depend on asymmetric cryptographic protections such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC). Quantum computers will be able to defeat these algorithms rapidly by compromising the mathematical foundations much faster than classic computers—making years of collected virtual private network (VPN) and transport layer security (TLS) traffic vulnerable to decryption.

Attacks like the one in the hypothetical scenario described earlier are classic HNDL attacks, where attackers simply apply the HNDL model at scale.

In anticipation of Q-Day, organizations worldwide are already advancing quantum chip designs and manipulating matter at the quantum level to accelerate CRQC development. On Q-Day, attackers could decrypt stored data and quickly reveal private keys, exposing sensitive information and triggering a global cybersecurity crisis.

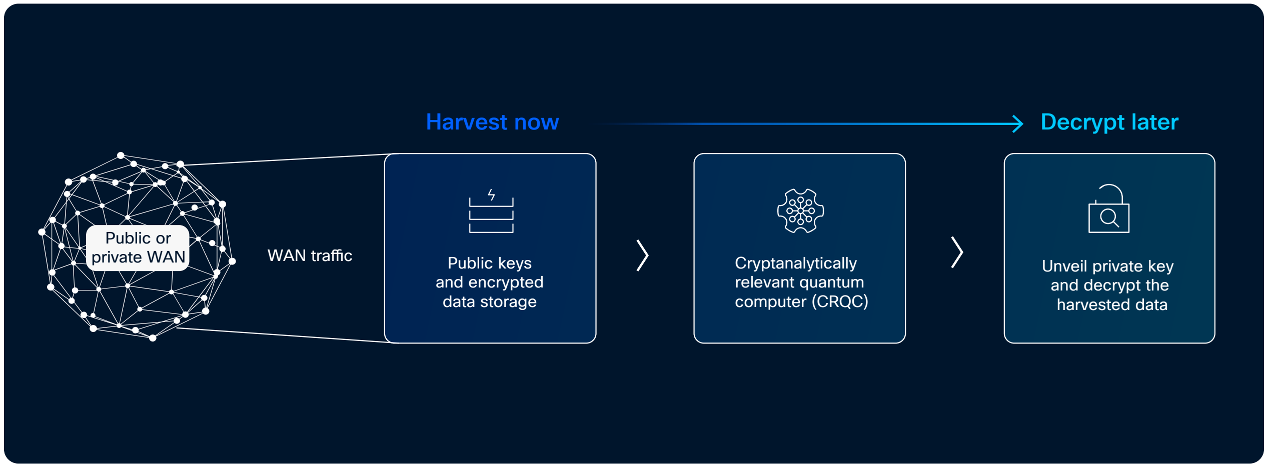

Harvest now
Decrypt later
Public or private WAN
WAN traffic
Public keys and encrypted data storage
Cryptanalytically relevant quantum computer (CRQC)
Unveil private key and decrypt the harvested data

Figure 1. A harvest now, decrypt later attack

Given how critical these WAN data flows are to business operations, PQC is now an urgent priority. Without it, organizations face risks such as data breaches, compromised digital certificates, forged digital signatures, and failures in secure key exchange and identity management.

Hardening the WAN must be the first step to protect sensitive data in a post-quantum world.

How to generate quantum-resistant encryption keys

Modern WAN security relies on IKEv2/IPsec implementations that combine symmetric and asymmetric cryptography. Symmetric algorithms (such as Triple Data Encryption Standard [3DES] and Advanced Encryption Standard [AES]) encrypt data-plane traffic due to their computational efficiency, high throughput, and scalability, with AES-256 offering robust, brute-force resistance.

Asymmetric cryptography using protocols like IKEv2 with RSA, Diffie-Hellman, and ECC securely establishes symmetric encryption keys through authentication and key exchange. However, these algorithms are central processing unit (CPU)-intensive due to complex mathematical operations, limiting their use to channel establishment rather than continuous data encryption.

Quantum computers with 1000 qubits using Shor's algorithm could break asymmetric algorithms within minutes, threatening the entire security foundation. Making asymmetric cryptography quantum resistant inherently protects dependent symmetric ciphers. Recognizing this threat, industry stakeholders and standards bodies have initiated quantum-resistant security development, leading to additional key material referred to as post-quantum pre-shared keys (PPKs) before formal quantum-safe algorithm standardization.

To protect data from quantum threats, use key generation methods that do not rely solely on asymmetric cryptography, but instead incorporate PPKs as well.

There are two methods:

1. Manually provision PPKs.
2. Use Cisco Secure Key Integration Protocol (SKIP) to import PPKs dynamically from external key sources such as quantum key distribution (QKD) systems.

Building on these PPK approaches, Cisco has invested in quantum-safe initiatives across both platforms and protocols, starting with quantum-safe hardware secure boot and the development of LDWM (2013) and LMS (2019) signature schemes. This work then extended into quantum-safe network transport protocols, particularly through the integration of QKD via SKIP (developed in 2017).

Today, quantum-safe transport security for IKEv2/IPsec VPNs, including FlexVPN (Static Virtual Tunnel Interface (SVTI) and Dynamic Virtual Tunnel Interface (DVTI)) and Dynamic Multipoint VPN (DMVPN), is addressed through two distinct PPK implementation methodologies. Both approaches rely on IKEv2 protocol extensions, specifically leveraging RFC 8784, which Cisco pioneered, to seamlessly integrate PPKs into existing key exchange mechanisms.

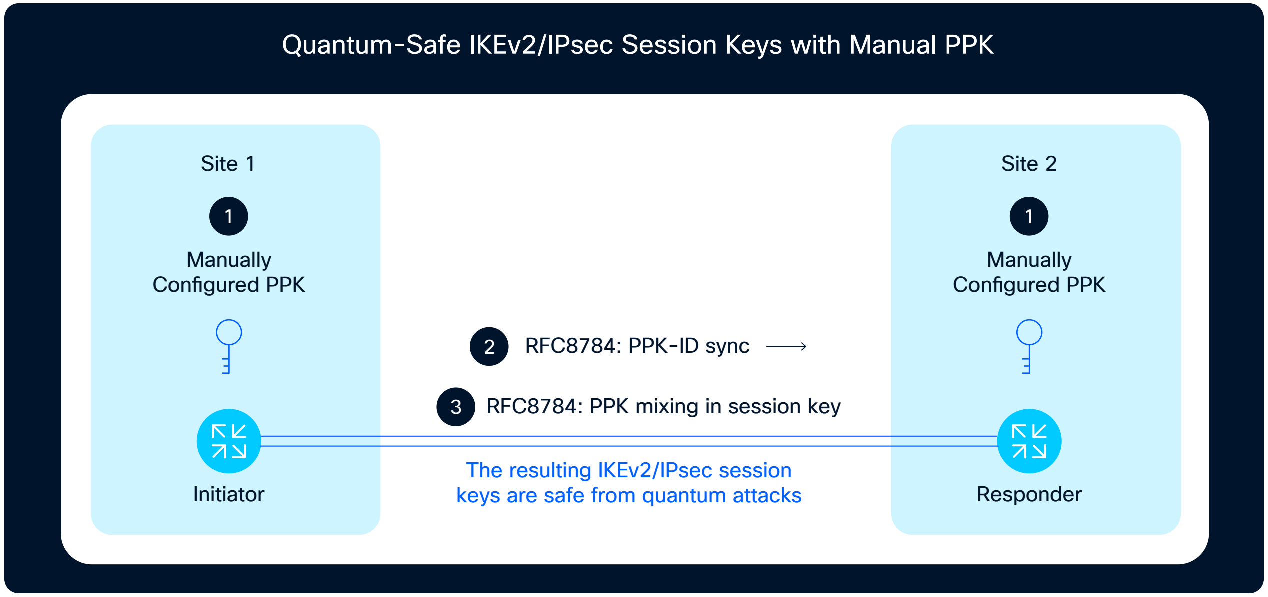

Quantum-Safe IKEv2/IPsec Session Keys with Manual PPK
Site 1
1
Manually Configured PPK
Initiator
Site 2
1
Manually Configured PPK
Responder
2 RFC8784: PPK-ID sync ⟶
3 RFC8784: PPK mixing in session key
The resulting IKEv2/IPsec session keys are safe from quantum attacks

Figure 2. Manual PPK

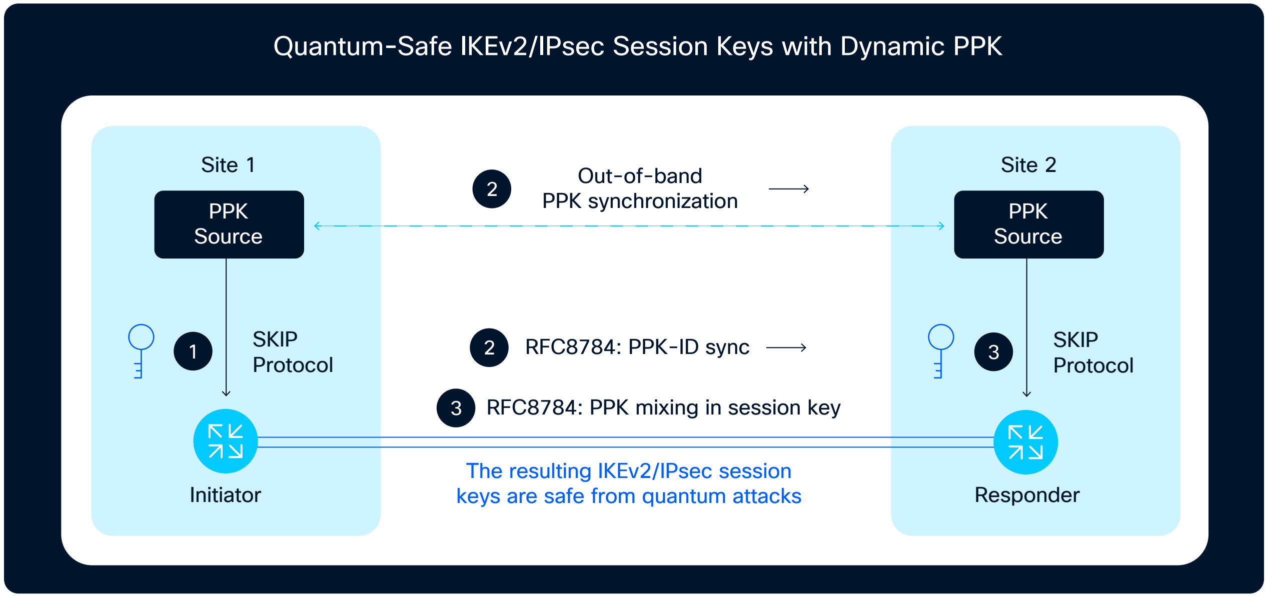

Quantum-Safe IKEv2/IPsec Session Keys with Dynamic PPK
Site 1
PPK Source
1
SKIP Protocol
Initiator
2 Out-of-band PPK synchronization ⟶
2 RFC8784: PPK-ID sync ⟶
3 RFC8784: PPK mixing in session key
The resulting IKEv2/IPsec session keys are safe from quantum attacks
Site 2
PPK Source
3
SKIP Protocol
Responder

Figure 3. Dynamic PPK with SKIP protocol

These methods create quantum-resistant session keys, effectively mitigating HNDL attacks on encrypted traffic, which we detail below.

A detailed configuration guide including both methods is available from Cisco.

Cisco supports PPK and RFC 8784 implementation to make all routing-mode transports VPNs, such as FlexVPN and DMVPN, quantum-safe on enterprise-grade branch and data center platforms, including Catalyst 8000 Edge, ISR 1000 Series (from IOS XE 17.12), and the latest generation of Cisco 8000 Series Secure platforms (from IOS XE 17.15).

Manual provisioning

Manual PPK provisioning requires administrators to configure a PPK on both IPsec peers. This is a simple and quick way to start for small deployments, but it does not scale well for large networks and increases key management complexity—placing a heavy burden on administrators. Manual key management increases the risk of weak keys and key exposure, especially if keys are not regularly rotated or if insecure distribution protocols are used. Human error or low-entropy keys can compromise the benefits of post-quantum security, making manual processes impractical for networks spanning thousands of sites.

Dynamic PPK using SKIP and QKD as external key source

SKIP addresses the limitations of manual PPK provisioning by enabling a dynamic, fresh PPK for every IKEv2 execution. Acting as a crucial bridge, SKIP connects PPK-augmented IKEv2 peers with an arbitrary, out-of-band PPK synchronization mechanism, such as a QKD source. This ensures that a unique, high-entropy key and key ID are ingested securely, which provides robust quantum resistance, thereby significantly enhancing encryption security and delivering robust quantum resistance. The protocol operates over HTTPS/TLS, allowing routers (encryptors) to securely fetch these dynamic PPKs from trusted key providers.

Operationally, an IKEv2 initiator requests a PPK and its corresponding ID from its local key provider. This PPK is then securely synchronized out-of-band to the responder's key provider. The initiator communicates only the PPK ID to the responder over IKEv2 (using RFC 8784 extensions)—never the actual key. The responder then uses this ID to retrieve the correct PPK from its own key provider. Both encryptors then mix this identical, unexposed PPK into the key derivation process. This method ensures the actual pre-shared key never traverses the wire, making captured traffic useless for HNDL, even by quantum computers.

Key considerations for QKD-based deployments

Organizations can explore quantum-safe WAN transport VPNs by integrating third-party QKD solutions with SKIP. However, this approach requires careful evaluation across multiple dimensions before deployment. Critical considerations include:

- **Vendor collaboration:** Select QKD vendors that are capable of integrating, testing, and qualifying their solution with Cisco networking infrastructure.
- **Scalability assessment:** Evaluate how the vendor's key synchronization techniques perform at scale for large enterprise deployments.
- **Cost-benefit analysis:** Assess total cost of ownership, including initial hardware investment and long-term management expenses.
- **Security responsibilities:** Clearly define security perimeters between the QKD vendor's components and Cisco devices in this two-box solution architecture.
- **Standards evolution:** Determine how the solution adapts to native PQC standards and maintains crypto agility.
- **Regulatory compliance:** Align with country-specific guidelines; for example, the NSA prohibits QKD solutions and Germany's federal cybersecurity authority, BSI, does not recommend them.

Cisco pioneered the development of the Secure Key Integration Protocol (SKIP) and RFC 8784.

SKIP is an API framework that enables acquiring quantum-safe keys from external key-source management systems such as quantum key distribution (QKD). Today, several QKD vendors in the market have implemented SKIP. RFC 8784 defines how to mix these post-quantum pre-shared keys (PPKs) into IKEv2 IPsec.

Emerging regulatory directives on quantum-safe algorithms

The quantum threat has prompted decisive government action. In 2022, the U.S. issued an executive order directing the National Institute of Standards and Technology (NIST) to establish quantum-resistant cryptographic standards for national security.

After six years of global research and collaboration, NIST standardized quantum-resistant algorithms. The NSA subsequently released Commercial National Security Algorithms Suite 2.0 (CNSA 2.0), mandating implementation timelines for all national security systems.

The CNSA 2.0 establishes a phased transition approach, enabling organizations to strategically plan, develop, and execute their quantum-safe migration.

Table 1: NIST post-quantum algorithms

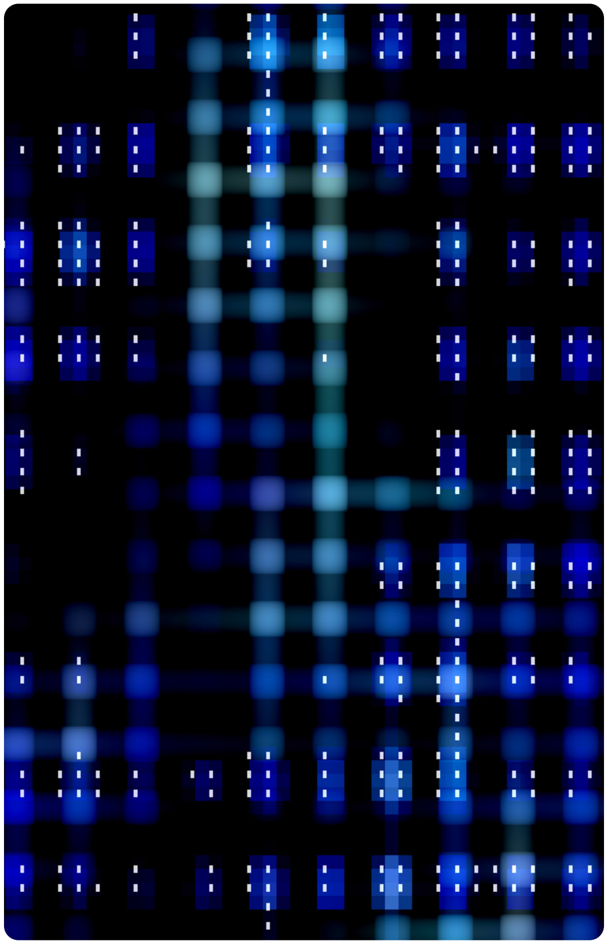
Algorithm	Function	Specification	Replaces
ML-KEM (formerly CRYSTALS-Kyber)	Key establishment	FIPS-203	DH, ECDH
ML-DSA (formerly CRYSTALS-Dilithium)	Authentication (digital signatures and certificates)	FIPS-204	RSA, ECDSA
LMS/ML-DSA-87 (Leighton-Micali Signature)	Digital signing of firmware and software	NIST SP 800-208	–

These standardized algorithms form the foundation for protecting critical infrastructure against quantum threats.

Countries worldwide were quick to follow up with their own directives around PQC standards and migration timelines. Below are some of the guidelines published by national security bodies worldwide:

- Australia: Stay ahead of the quantum threat with PQC
- Canada (CCCS): ITSM.40.00–roadmap for PQC migration
- United Kingdom (NCSC): PQC migration timelines
- India (TEC): TEC 910018:2025–migration to PQC

Embarking on PQC migration



PQC migration demands rigorous planning and execution. Success requires a structured approach across three critical dimensions:

Data sensitivity and classification

Begin by classifying data based on sensitivity and required protection duration. Distinguish between data in transit and data at rest—not all WAN segments carry highly sensitive information. This helps you prioritize resources by identifying which data requires protection against quantum threats.

Cryptographic assessment and agility

Conduct comprehensive network audits to assess readiness and identify risks before major upgrades. Perform cryptographic inventory discovery across on-premises, cloud, IaaS, and SaaS environments, documenting all management protocols, overlay VPNs, and cryptographic assets. Utilize tools like a Cryptographic Bill of Materials (CBoM) for thorough assessment.

Ensure crypto hygiene by following regulatory guidelines while maintaining crypto agility through swift adaptation to new standards with minimal disruption.

The latest generation of Cisco 8000 Series Secure Routers is engineered with inherent cryptographic agility, a foundational requirement for incorporating the specifications outlined in CNSA 2.0.

Some models of Cisco 8000 Series Secure Routers come with a secure networking processor capable of performing in-line crypto for IPsec and MACsec and providing the crypto agility required to support CNSA 2.0 quantum-safe standards as well as evolving Internet Engineering Task Force (IETF) protocols.

Best practices

Collaborate with vendors to verify hardware compatibility and plan refresh cycles. Monitor regulatory timelines, establish response teams, implement phased migration approaches, and select future-proof solutions supporting 10 to 15 years of cryptographic evolution.

Table 2: Steps to preparing for WAN PQC migration

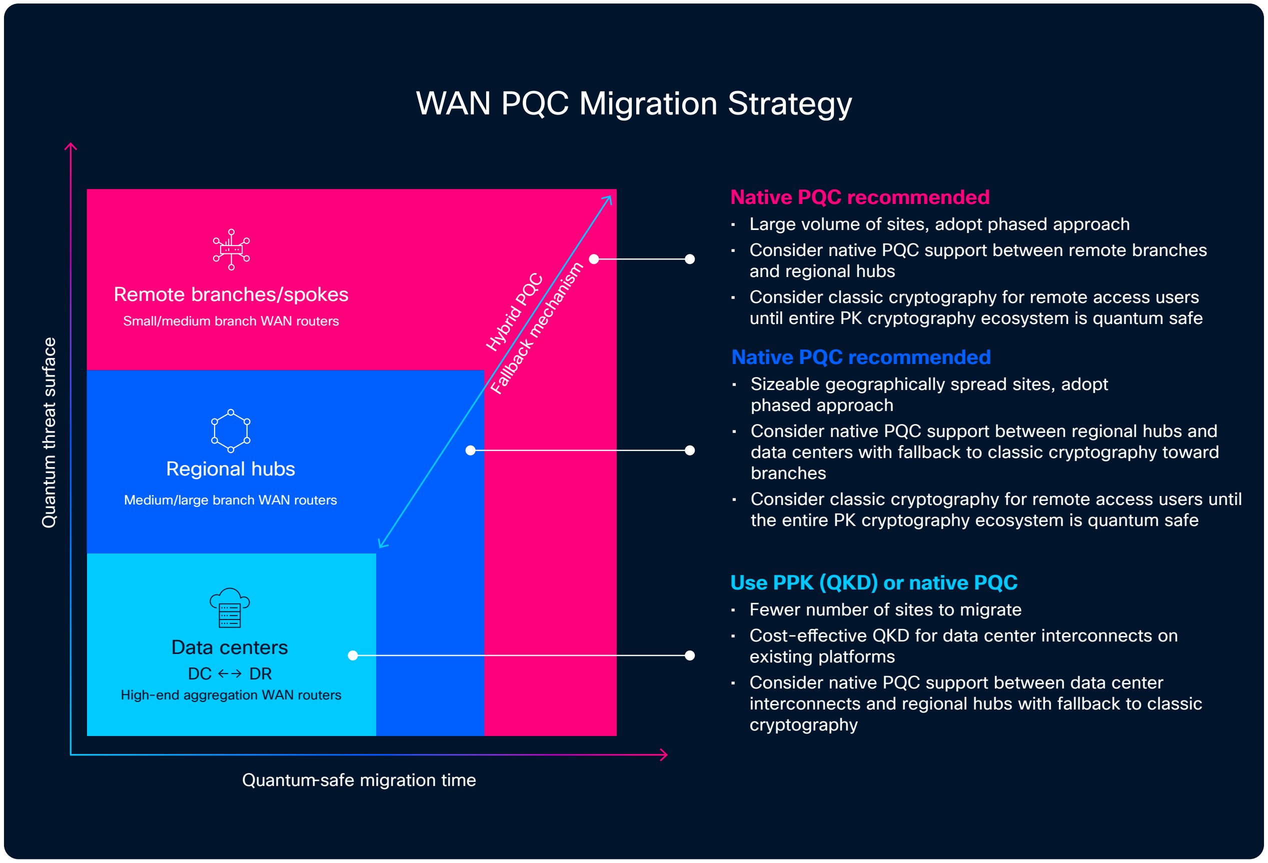
Educate	Assess and prioritize WAN cryptography	Research WAN PQC options	Develop a WAN PQC strategy	Execute the WAN PQC strategy	Monitor WAN PQC progress
Ensure IT, network security, and leadership teams comprehend the quantum threats and their impact on WAN infrastructure and data.	Inventory all cryptographic mechanisms in use across WAN devices and links. Identify which data and asymmetric encryption types are most vulnerable.	Evaluate PQC algorithms, hybrid solutions, and crypto agility for WAN environments–including the need for PQC-ready hardware upgrades.	Create a roadmap for integrating PQC into your WAN, focusing on crypto agility for seamless algorithm switching.	Adopt NIST-standardized PQC protocols, implement hybrid cryptographic schemes, and update WAN protocols (such as IKEv2/IPsec and TLS) to support PQC.	Track your WAN's PQC transition, stay informed on quantum hardware advancements, and align with evolving standards.

Adapt hybrid PQC for transport security

PQC migration requires a phased approach that ensures business continuity with defined outage thresholds and rollback strategies.

During transition, networks must support both PQC and traditional public key cryptography (PKC) concurrently. Implementing post-quantum/traditional hybrid schemes enables seamless interoperability between systems with varying security requirements, facilitating eventual migration to PQC-only environments.

Comprehensive testing and validation are critical. Migration plans must verify proper integration of PQC-capable software libraries into infrastructure systems and establish interoperability with PQC-based ecosystem services, including third-party identity providers and enterprise certificate authority (CA) servers. This phased methodology minimizes risk while maintaining operational continuity throughout the quantum-safe transition.


WAN PQC Migration Strategy
Quantum threat surface
Remote branches/spokes
Small/medium branch WAN routers
Regional hubs
Medium/large branch WAN routers
Data centers
DC <-> DR
High-end aggregation WAN routers
Hybrid PQC
Fallback mechanism
Quantum-safe migration time

Native PQC recommended

- Large volume of sites, adopt phased approach
- Consider native PQC support between remote branches and regional hubs
- Consider classic cryptography for remote access users until entire PK cryptography ecosystem is quantum safe

Native PQC recommended

- Sizeable geographically spread sites, adopt phased approach
- Consider native PQC support between regional hubs and data centers with fallback to classic cryptography toward branches
- Consider classic cryptography for remote access users until the entire PK cryptography ecosystem is quantum safe

Use PPK (QKD) or native PQC

- Fewer number of sites to migrate
- Cost-effective QKD for data center interconnects on existing platforms
- Consider native PQC support between data center interconnects and regional hubs with fallback to classic cryptography

Figure 4. Quantum migration timelines

When migrating large-scale secure WAN networks (DMVPN, SD-WAN) to PQC, evaluate network hierarchy and prioritize segments requiring immediate protection. Hardware assessments are also critical, as platform replacements face procurement delays and budget constraints.

Recommended inward-out migration strategy

Data center/ disaster recovery

Begin with four to eight hub nodes across data center/disaster recovery and cloud environments. While legacy ASR1K and Cisco Catalyst 8500 Series Edge Routers support only PPK solutions, newer Cisco 8500/8400 Series Secure Routers offer built-in PQC with PPK compatibility, ensuring future negotiation capabilities across regional hubs and spokes, superior to QKD-only approaches.

Regional hubs

These aggregation points connect regional branches and function as spokes to global data centers. Native PQC support is essential for eventual compliance across remote branches and across remote access users.

Remote branches

With hundreds to thousands of geographically distributed locations, native PQC ensures quantum-safe encryption and authentication at scale.

Remote access users

PQC-enabled VPN headends secure remote user traffic, though authentication requires quantum-safe certificate authorities and identity providers.

Third-party integrations

Cloud providers, middle-mile interconnects, and SSE solutions form the broader connectivity fabric for applications and users. Built-in PQC on Cisco 8000 Series Secure Routers extend comprehensive protection across on-premises, cloud, and remote-access environments.

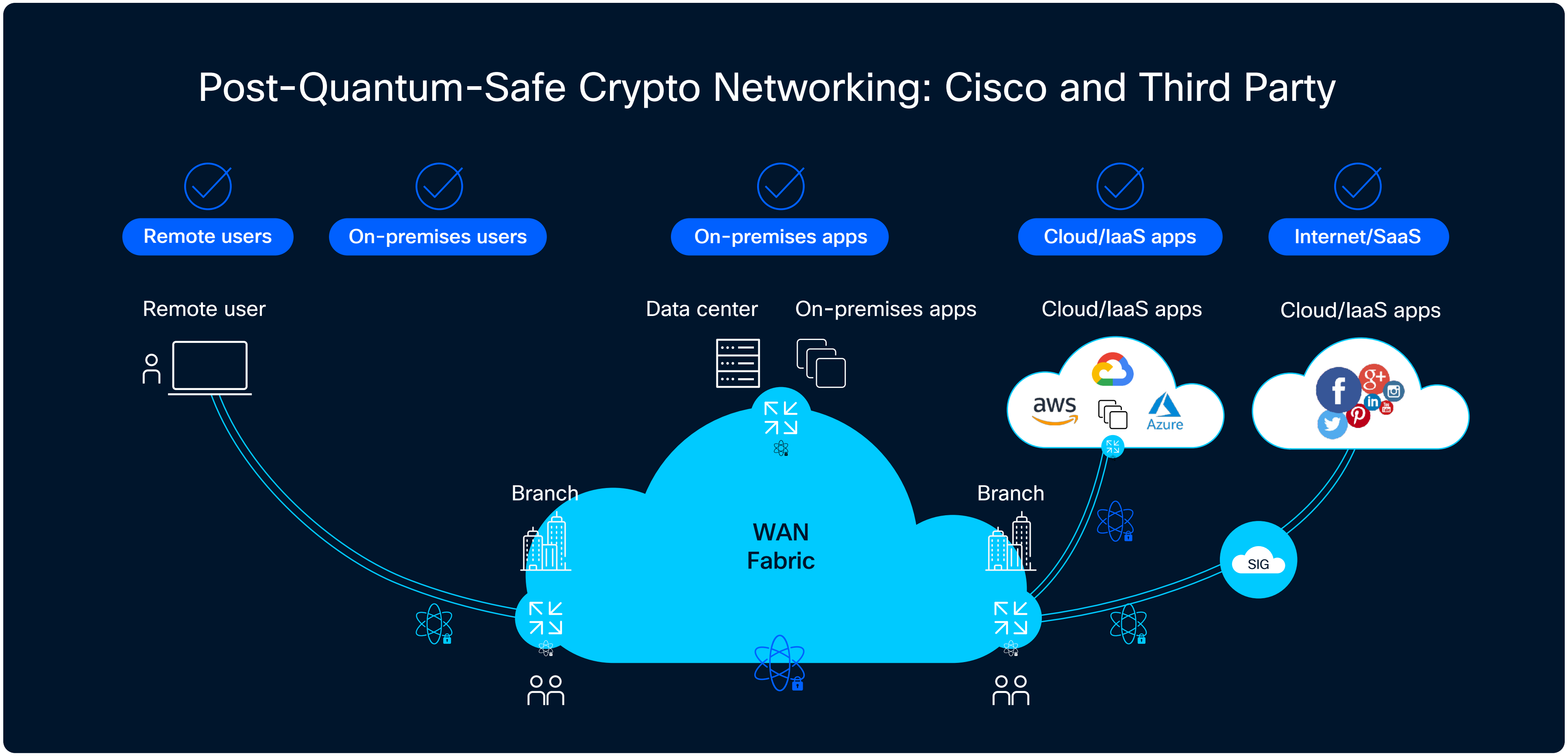


Figure 5. PQC ecosystem considerations and integrations

As you plan your PQC migration, consider third-party integrations to ensure secure communication between any endpoint, user, or application—on-premises, cloud, or remote. This approach offers flexibility to use legacy PPK solutions or move to PQC as your network allows, with the option to enforce PQC later. Since your network may include multiple cloud providers, middle-mile, and SSE interconnects, review their capabilities to make sure your WAN infrastructure PQC migration strategy aligns with their current and evolving post-quantum security support.

Using built-in PQC on the Cisco 8000 Series Secure Routers connecting with these integrations helps future-proof your PQC migration journey for the entire network across on-premises, cloud IaaS/SaaS, and remote-access users.

Charting your quantum security journey

The WAN remains the most critical point for business data in transit, making it the decisive battleground for defending against HNDL attacks. For optimal quantum-safe protection, organizations should prioritize building crypto agility directly into their WAN infrastructure. By leveraging native post-quantum cryptography (PQC) capabilities and exploring solutions such as Cisco 8000 Series Secure Routers, you can establish a foundation of resilience that extends across your entire network.

Cisco supports customers and partners at every stage of their quantum security journey, providing the expertise, technology, and solutions needed to build resilient, future-ready network security for the post-quantum era.

Get started with Cisco 8000 Series Secure Routers and begin your quantum-safe journey.