Quantum-Ready Migration Guide

Modernizing Mission-Critical Networks with Post Quantum Cryptography (PQC)

May 2026

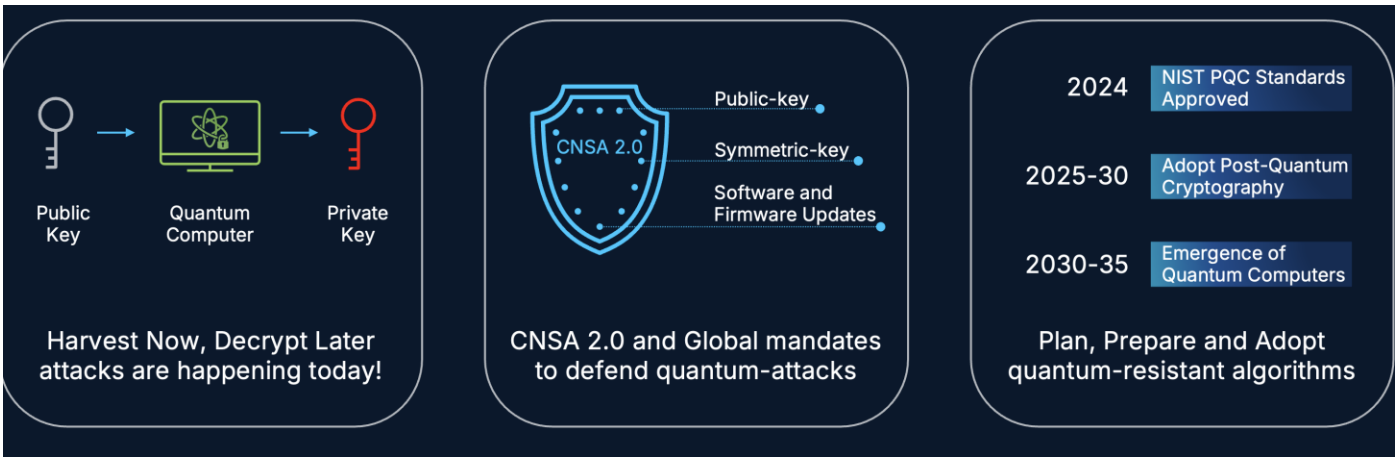
Executive summary

The global cybersecurity landscape has reached a critical window—the era of post-quantum transition. The emergence of cryptographically relevant quantum computers (CRQC) is no longer a distant theoretical milestone, but a definitive deadline for national security and enterprise data integrity. The core mission of this guide is clear: **Securing Today for Tomorrow.**

For mission-critical networks, the transition to Post-Quantum Cryptography (PQC) is a mandatory evolution driven by three critical realities:

- Harvest Now, Decrypt Later (HNDL): Adversaries are currently intercepting and archiving encrypted traffic with the intent to decrypt it once quantum capabilities mature. Attacks on today's data are happening now.
- Global Mandates (CNSA 2.0): Standard-setting bodies have issued clear mandates to defend against quantum-level threats across Public Keys, Symmetric Keys, and Software/Firmware Updates.
- The Strategic Adoption Window: With the emergence of functional quantum computers projected for the 2030–2035 horizon, the current decade is the essential period to Plan, Prepare, and Adopt quantum-resistant algorithms.

This guide provides the blueprint for migrating legacy infrastructures to a quantum-resilient posture using the Cisco 8000 Series Secure Routers. By implementing ML-KEM (FIPS 203) and hardware-rooted trust, organizations can ensure their current secure communications remain protected against the computational breakthroughs of the future.



Foundations of the quantum threat

The immediate crisis: "Harvest Now, Decrypt Later" (HNDL)

The most immediate and insidious threat is HNDL. Sophisticated adversaries are currently intercepting and archiving petabytes of encrypted traffic from high-value targets across global WAN links.

The Ticking Clock: While this data is unreadable today, it is effectively a "time capsule." Once a CRQC is operational, all archived datasets-containing decades of intellectual property, state secrets, and financial records-will be decrypted retroactively.

- The Lifecycle Risk: If your data has a shelf-life of 10+ years, it is already compromised if it is being sent over classical IPsec VPNs today. The decision to delay PQC implementation is a decision to forfeit the long-term confidentiality of your current communications.

The authentication collapse

Encryption protects confidentiality, but authentication protects identity. Current digital signatures (RSA/ECDSA) used for VPN tunnel establishment, BGP routing updates, and administrative access are vulnerable to Shor's Algorithm.

Identity Forgery: An attacker with a quantum computer can forge the digital signatures used to identify a network peer. This allows them to impersonate a trusted Hub, a management server, or an endpoint.

- Control Plane Hijacking: Once authentication is broken, an adversary can inject malicious routes into the routing table or establish "trusted" tunnels into the heart of the network, bypassing all perimeter defenses without triggering a single classical alarm.

The Insecure Boot and Supply Chain Threat

The quantum threat extends below the software layer to the very foundation of the device. If the boot process is not protected by quantum-resilient signatures, the entire hardware chain of trust is broken.

- Malware Injection: Attackers can inject malicious code during the boot sequence. This code operates at a level deeper than the Operating System, allowing it to remain invisible to standard security monitoring tools while providing persistent, elevated access.
- Counterfeit Hardware & Software: Without quantum-safe hardware-rooted trust, attackers can push "official" firmware updates that contain malicious payloads or insert counterfeit components into the supply chain that bypass traditional integrity checks.
- Persistent Backdoors: An adversary can establish a "Root of Trust" that belongs to them rather than the organization. This makes the device permanently compromised; no amount of software patching can remove a backdoor that is validated by a compromised boot sequence.

The hardware trust anchor: Cisco 8000 Series Secure Routers

To achieve true quantum resilience, security cannot be a mere software overlay; it must be anchored in the physical silicon. The Cisco 8000 Series Secure Routers represent a fundamental shift in network security architecture, moving beyond traditional defenses to a system that is inherently "Secure by Design."

Secure Network Processor (SNP): Hardware-integrated security

At the heart of the Cisco 8000 Series Secure Router is the Secure Network Processor (SNP). This specialized silicon is purpose-built to handle the heavy computational requirements of next-generation cryptography while maintaining high-performance routing.

- **Line-Rate PQC Acceleration:** The SNP provides the dedicated hardware engines required to process Post-Quantum Cryptography (PQC) algorithms without the performance "tax" typically associated with software-based encryption.
- **Unified Security Processing:** By integrating security functions directly into the packet-processing path, the SNP ensures that features like deep packet inspection and PQC-native encryption are executed at line rate.

Immutable Trust: Secure Boot and Hardware Root of Trust (RoT)

The integrity of a router is only as strong as its first instruction. The Cisco 8000 Series utilizes a Hardware Root of Trust (RoT) to ensure a completely untampered boot sequence.

- **Trust Anchor Module (TAM):** This dedicated hardware chip stores unique device identities and cryptographic keys in a secure, tamper-proof environment, isolated from the main processor and memory.
- **Multi-Stage Verification:** Before the operating system even begins to load, the hardware verifies the microcode and bootloader. Each subsequent stage of the boot process is cryptographically signed and verified against the TAM, creating an unbroken Chain of Trust.
- **Anti-Tamper Mechanisms:** If the device detects a hardware modification or a signature mismatch during boot, the SNP will halt the initialization process, preventing a compromised device from ever joining the production network.

Roadmap Alignment: The Path to Quantum Dominance

Cisco's commitment to PQC is reflected in the rapid delivery of standardized algorithms within the IOS-XE lifecycle.

IOS-XE 26.1.1 (Full-Stack PQC Enablement)

This release marks a major milestone in securing both the WAN and the LAN edge.

- **ML-KEM (FIPS 203):** Support for Module-Lattice-Based Key-Encapsulation Mechanism is enabled across the portfolio for **IPsec VPN** key exchange.
- **Quantum-Safe MACsec:** 26.1.1 introduces **PQC-resistant MACsec** using ML-KEM-based key exchange. This allows for quantum-safe encryption between the LAN switch and the Cisco 8000 Series Secure Router, ensuring the "first hop" of the data journey is protected against harvesting.
- **Hybrid Key Exchange:** To ensure maximum compatibility, this release supports hybrid modes—combining classical Diffie-Hellman/ECC with ML-KEM. This ensures that even if a flaw were discovered in a new PQC algorithm, the classical encryption remains as a fallback.

IOS-XE 26.2.1 (Hardened PQC Authentication)

This release expands from data confidentiality to **Control Plane Integrity**.

- **PQC Authentication:** Moving beyond RSA/ECC for tunnel authentication, this release will introduce quantum-safe digital signatures (such as ML-DSA) to verify the identity of the router itself.

- **Secure Boot Enhancements:** Further hardening of the boot sequence with quantum-resistant signatures, ensuring that the SNP-verified hardware remains protected against attackers armed with future quantum capabilities.

Quantum-safe WAN architectures

With the hardware foundation established, the architecture must transition to a modernized cryptographic stack. The shift to Post-Quantum Cryptography (PQC) is not a rip-and-replace of networking protocols, but a fundamental upgrade of the underlying mathematical primitives used to secure those protocols.

The PQC encryption stack: ML-KEM for IKEv2/IPsec

The transition centers on ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism). In the classical model, IKEv2 uses Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) to establish session keys. In a quantum-ready architecture, ML-KEM replaces or augments these methods.

- Hybrid Key Exchange (Recommended): To mitigate the risk of "early-adopter" vulnerabilities, Cisco 26.1.1 supports a hybrid approach. The session key is derived from both a classical ECDH exchange and an ML-KEM exchange. An attacker must break both algorithms to compromise the tunnel.
- Algorithm Efficiency: Despite the complexity of lattice-based math, the SNP in the Cisco 8000 Series ensures that ML-KEM key generation and encapsulation do not introduce significant latency to tunnel establishment.

Bringing PQC into today's WAN architectures:

Dynamic Multipoint VPN (DMVPN): Scalable PQC for mGRE

DMVPN remains the backbone of many mission-critical enterprise WANs. Bringing DMVPN into the quantum era involves upgrading the IKEv2 profiles that protect the mGRE tunnels.

- **mGRE Integration:** PQC is applied at the IKEv2 layer, ensuring that the Dynamic NHRP registrations and subsequent spoke-to-spoke tunnels are initiated with quantum-safe session keys.
- **Scalability:** The SNP handles the high volume of concurrent IKEv2 negotiations typical of large DMVPN Hubs, even with the increased packet size required for PQC key exchange.

FlexVPN: The Unified PQC Standard

FlexVPN is the natural home for PQC because it is built natively on **IKEv2**.

- **Standardization:** By using FlexVPN, organizations can apply a single, consistent PQC policy across Site-to-Site, Remote Access, and Hub-and-Spoke topologies.
- **Multi-Service PQC:** FlexVPN simplifies the deployment of ML-KEM by using a modular "Smart Default" configuration catalog, allowing for a rapid shift to quantum-safe standards across the entire fabric.

Classical point-to-point IPsec VPNs

For point-to-point tunnels connecting high-value data centers or secure enclaves, the migration involves a direct transition from legacy transform sets to PQC-native IKEv2 proposals.

- **Granular Control:** This architecture allows for the immediate enforcement of "PQC Required" policies on specific high-security links, ensuring that sensitive data is never transmitted using classical-only encryption.

Strategic Note: PQC Roadmap for SD-WAN

While this guide focuses on SD-Routing managed IOS-XE WAN architectures, it is important to note the transition path for Cisco SD-WAN. To achieve quantum resilience, the SD-WAN architecture is evolving from its current model of controller-based key distribution to a decentralized model.

- IKEv2 Integration: Future releases will introduce native IKEv2 support for data plane tunnels, replacing the distribution of keys via TLS/DTLS control channels.

- PQC Enablement: This shift to IKEv2 is a functional prerequisite, providing the standard framework necessary to negotiate ML-KEM key exchanges directly between Edge peers.
- Preparation: Organizations should prioritize the deployment of Cisco 8000 Series hardware today. This ensures that when the PQC-enabled software is released, the Secure Network Processor (SNP) is already in place to handle the post-quantum computational load without a hardware refresh.

LAN Edge Security (MACsec): Securing the "First Hop"

A common blind spot in PQC strategies is the internal LAN. If an adversary gains physical or logical access to the local access switch, they can harvest traffic before it ever reaches the WAN router.

- **PQC MACsec:** In IOS-XE 26.1.1, MACsec is enhanced with ML-KEM support. By implementing PQC MACsec between a PQC-capable LAN switch and the Cisco 8000 Series Secure Router, the "first hop" is secured against harvesting.
- **Defense in Depth:** This ensures a continuous quantum-safe envelope. Data is encrypted at Layer 2 (MACsec) across the LAN and re-encrypted at Layer 3 (IPsec) across the WAN, providing multi-layered protection against different harvest points.

Case study: migrating DMVPN to PQC ML-KEM IPsec

This section provides a technical blueprint for transitioning a production DMVPN environment to the Cisco 8000 Series Secure Router platform. The objective is to achieve a **Post-Quantum Cryptography (PQC)** state using **ML-KEM** while maintaining high availability and zero downtime for mission-critical traffic.

To accommodate varying risk tolerances and technical baselines, this guide outlines two primary migration paths:

- **Migration Option 1:** DMVPN Hub 'Hot Swap': A redundancy-based approach that replaces legacy Hubs with 8000 secure routers within the existing topology. This leverages the 'pqc optional' backwards-compatibility feature to allow a single Hub to service both legacy and PQC-migrated spokes simultaneously.
- **Migration Option 2:** Parallel Architecture: A greenfield approach where a new PQC-native 8000 series secure router Hub cluster is built alongside the legacy network. Spokes are migrated site-by-site to the new "Island," using a Network-to-Network Interface (NNI) to maintain reachability between the two environments.

Migration prerequisites

To execute the 'Hot Swap' migration, the legacy environment must satisfy specific baseline requirements to ensure seamless interoperability with the Cisco 8000 Series (G2).

- **IKEv2 Framework:** This migration path relies on the hybrid negotiation capabilities of IKEv2. If the legacy DMVPN network currently utilizes IKEv1, it **must** be modernized to IKEv2 prior to hardware replacement. Environments unable to perform this baseline upgrade should proceed with **Option 2**, which allows for a direct transition from IKEv1 to PQC-native IKEv2 on the new infrastructure.
- **TCP MSS Clamping:** To account for the increased overhead of PQC payloads and hybrid key exchanges, MSS clamping must be enforced to prevent performance-degrading fragmentation.
  - **Implementation:** Apply `ip tcp adjust-mss` 1360 on all Hub tunnel interfaces and Spoke LAN-facing interfaces.
- **IKEv2 Fragmentation:** Because ML-KEM public keys are significantly larger than classical ECDH keys, IKEv2 fragmentation must be enabled to ensure these larger payloads can transit MTU-constrained service provider networks without being dropped.
  - **Command:** crypto ikev2 fragmentation

Option 1: The 'Hot Swap' (DMVPN Hub Replacement)

This option is ideal for environments with constrained rack space where a rolling upgrade of the existing Hub redundancy pair is preferred.

Step 1. **Replace the hub:** Stage the new Secure Router DMVPN Hub with crypto configuration and "pqc optional". This allows the new Cisco 8000 (G2) Hub to negotiate PQC with migrated spokes while maintaining classical IKEv2 exchanges with legacy spokes.

The following code block includes Cisco's preferred crypto configuration for Mission Critical Network greenfield deployments.

```
crypto ikev2 proposal cni_ikev2_proposal
 pqc mlkem1024 optional
 encryption aes-gcm-256
 prf sha512
```

```
 group 21
!
crypto ikev2 policy cni_ikev2_policy
 proposal cni_ikev2_proposal
!
crypto ikev2 keyring ikev2keyring
 peer HUB-inet
  address 64.101.25.31
  pre-shared-key Cisco@123
 !
 peer ANY_SPOKE
  address 0.0.0.0 0.0.0.0
  pre-shared-key Cisco@123
!
crypto ikev2 profile ikev2profile
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2keyring
!
crypto ikev2 fragmentation mtu 1400
```

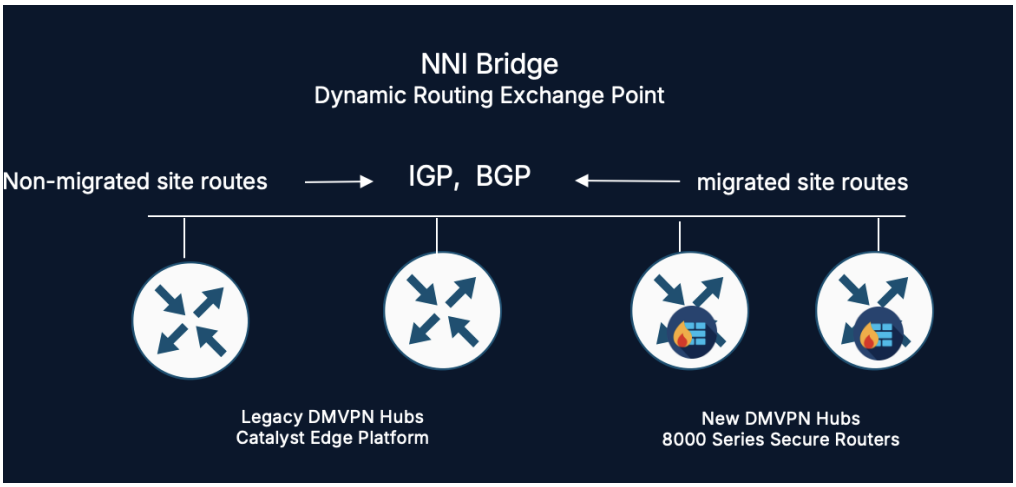
Step 2. Hub router replacement:

1. Drain traffic from the Primary Legacy Hub to the Secondary Hub by adjusting routing metrics.
2. Physically replace the Legacy Hub with the Cisco 8000 (G2).
3. Verify that legacy spokes re-establish tunnels using classical algorithms.
4. Restore traffic balance and repeat for the Secondary Hub.

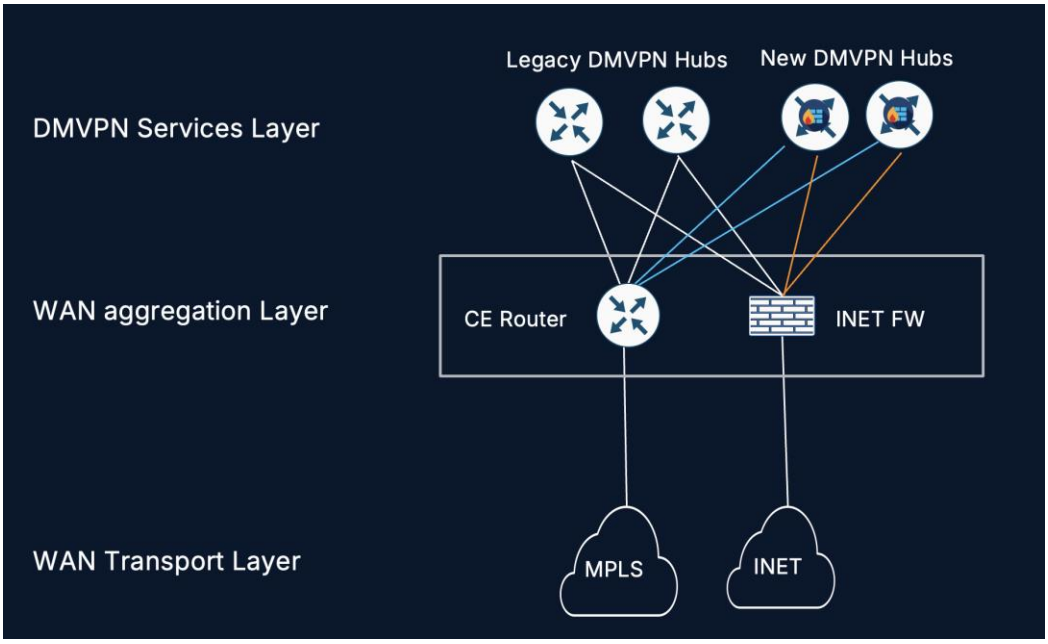
Option 2: Parallel architecture

This is the recommended path for risk-averse organizations. It involves building a "PQC Island" alongside the legacy network and migrating spokes site-by-site.

Step 1. The NNI bride: Establish a **Network-to-Network Interface (NNI)** between the Legacy Hub router cluster and the new Secure Router G2 Hub cluster. A routing protocol (e.g., BGP or EIGRP) used to exchange routes between migrated and non-migrated sites in order to allow communications during the course of the migration.



Step 2. **WAN transport sharing:** To ensure a seamless transition, the most effective method for sharing WAN circuits between legacy and new hub routers is to terminate both the DMVPN hubs and the transport circuits into an intermediate Layer 2 WAN transport layer. This architecture allows for a "clean-room" migration by enabling both hub generations to reside on the same physical circuit simultaneously, utilizing unique public IP addresses to build independent tunnel fabrics. By leveraging this intermediate switch, organizations can achieve a zero-impact migration where spokes are transitioned to the post-quantum cryptography (PQC) environment purely through configuration or edge hardware updates, maintaining a stable physical handoff at the data center throughout the process.



Step 3. **DMVPN spoke migration**: Once the new DMVPN Hub cluster is online and sharing the WAN transport, the spoke migration begins by replacing legacy routers at each site with Cisco 8000 (G2) platforms. These new spokes register directly to the PQC-enabled G2 Hub cluster using the modernized IKEv2 policy, establishing a quantum-safe "island" within the fabric. During this transitional phase, inter-site connectivity is maintained via the NNI bridge, allowing traffic from migrated PQC spokes to reach legacy destinations by transiting the G2 Hub and crossing into the legacy environment.

Implementation note: PQC MACsec integration

In both options, once the Cisco 8000 Secure Routers are in place, PQC MACsec should be enabled on the link(s) between the new hub router(s) and the internal LAN switches. This ensures that the migration doesn't just secure the WAN but provides a quantum-safe envelope from the very first hop in the branch.

Refer to the configuration guide on how to configure PQC MACsec on the Cisco Secure Routers https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_wan_macsec_MKA_support_enhancements.html

Feature	Option 1: Hot Swap	Option 2: Parallel Island
Risk Profile	Moderate (Modifies existing Hubs)	Lowest (Clean-room environment)
Legacy Impact	Minimal (Uses pqc optional)	Zero (Legacy network remains untouched)
Rollback	Revert Hub hardware/config	Re-home Spoke to Legacy Hub
Prerequisite	Redundant Hub infrastructure	Available WAN IP/Port for NNI

Centralized orchestration: Cisco SD-Routing

Managing a transition to Post-Quantum Cryptography (PQC) across hundreds or thousands of sites manually is prone to configuration drift and operational errors. Cisco SD-Routing via Catalyst Manager (formerly vManage) provides the centralized control plane necessary to orchestrate, push, and monitor quantum-safe configurations at scale.

Orchestration via Catalyst Manager

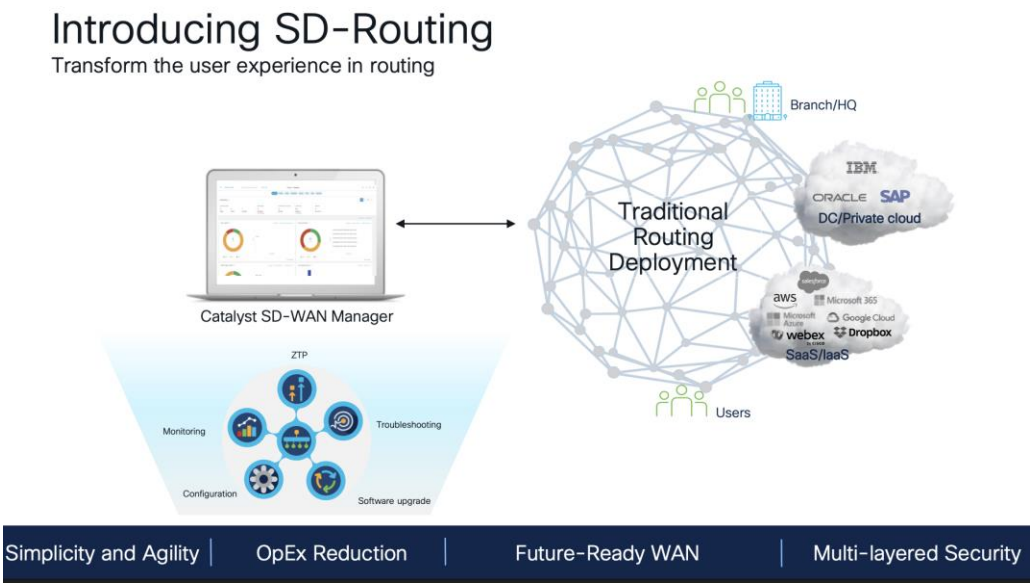
Catalyst Manager simplifies the complexity of PQC by abstracting the advanced CLI into manageable, reusable templates. This ensures that every router in the fleet adheres to the same mission-critical security standards.

- **Configuration Catalog Integration:** Cisco provides a pre-validated Configuration Catalog that includes recommended templates for IPsec and MACsec PQC profiles. These templates are pre-engineered to align with NIST and CNSA 2.0 standards, reducing the research burden on network engineering teams.
- **PQC Policy Enforcement:** Administrators can define global policies that determine the "PQC State" of the network. For example, a policy can be pushed to enforce pqc optional during the migration phase and then globally updated to pqc required once the legacy hardware has been decommissioned.
- **Automated ML-KEM Deployment:** Catalyst Manager automates the generation and distribution of IKEv2 proposals containing ML-KEM. This eliminates the risk of manual typos in complex cryptographic strings across large-scale DMVPN or FlexVPN deployments.

Real-time monitoring and visibility

Beyond configuration, SD-Routing provides deep visibility into the "Quantum Health" of the fabric.

- **Security Dashboards:** The Catalyst Manager dashboard provides a high-level view of which tunnels are currently operating in a quantum-safe state (ML-KEM) versus those still relying on classical encryption.
- **Crypto Audit Logs:** Detailed logs provide forensic evidence of IKEv2 negotiations, allowing engineers to verify that hybrid key exchanges are completing successfully across different transport providers.



Operational intelligence: Cisco IQ

As networks grow in complexity, **Cisco IQ** acts as the "Intelligence Engine" for the Quantum Ready Migration, providing value through both initial auditing and ongoing lifecycle management.

Discovery and risk audit

The first step in any PQC migration is gaining comprehensive landscape clarity through Cisco IQ, which acts as a powerful discovery and assessment engine. By analyzing platform-level features—such as trust anchors, secure boot, and secure storage—alongside the cryptographic agility and communication protocols of the management, control, and data planes, Cisco IQ identifies exactly which assets require hardware replacement, software upgrades, or specific feature activations to achieve a quantum-safe state. Beyond initial discovery, the platform continuously tracks the organization's progress against global mandates, ensuring the migration remains compliant with targets set by CNSA 2.0 and equivalent standards in the EU, UK, Canada, Australia, and Japan.

Ongoing operational monitoring and compliance

Future capabilities of Cisco IQ will include operational assurance roles, such as:

- **Compliance Measurement:** Cisco IQ continuously measures the network against industry mandates (such as FIPS 203). It generates automated compliance reports for stakeholders, proving that the mission-critical data remains within a quantum-safe envelope.
- **Configuration Drift Detection:** It proactively identifies any devices that have been manually rolled back to non-PQC states, ensuring that the security posture does not degrade over time.
- **Predictive Analytics:** By analyzing encrypted traffic health and SNP (Secure Network Processor) utilization, Cisco IQ can predict performance bottlenecks before they impact production traffic, ensuring the PQC "tax" remains invisible to the end-user.

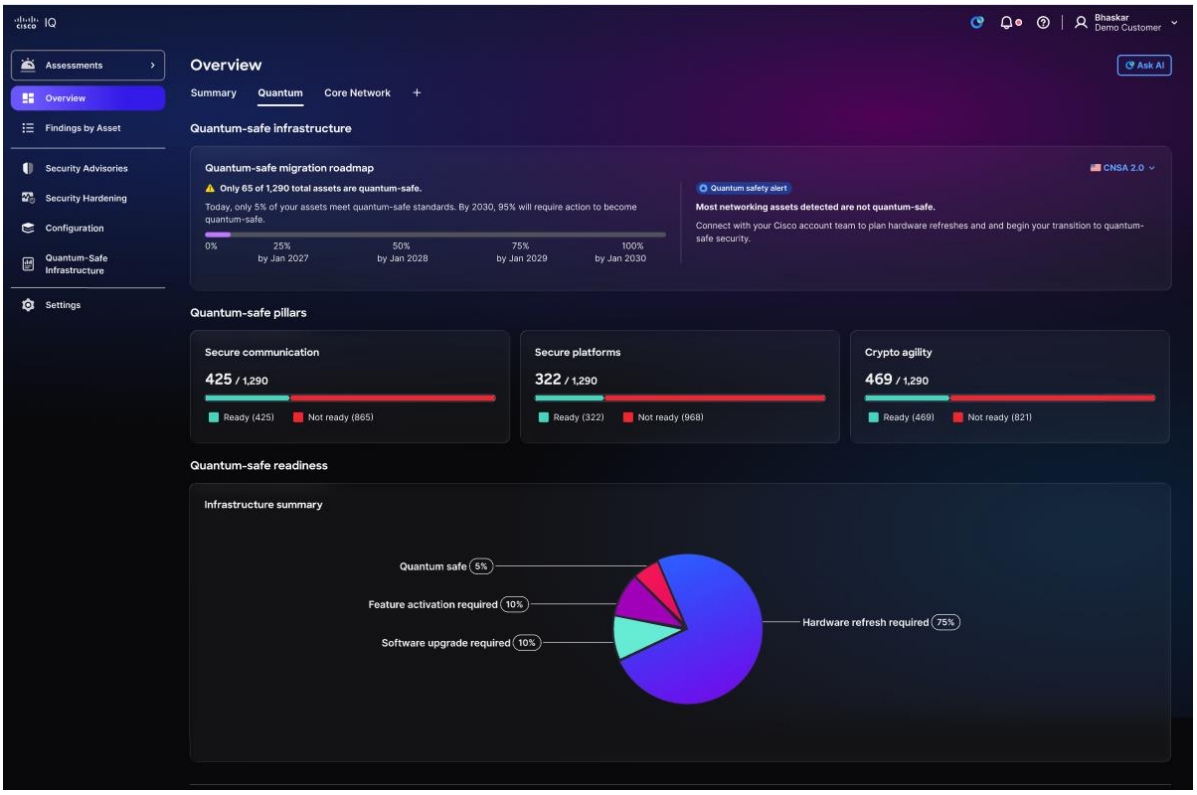


Figure 1. Cisco IQ Quantum-Safe readiness audit

Conclusion

The transition to a quantum-resilient network is an operational imperative that requires immediate and sustained action. By combining the Cisco 8000 Series Secure Router hardware with SD-Routing and Cisco IQ, organizations move from a reactive security posture to a proactive, quantum-resilient architecture.

As we look toward the 2030–2035 horizon, the security of our future data depends entirely on the discipline of our current adoption phase.

Securing Today for Tomorrow: Final Pillars

- **Defending Against HNDL:** The implementation of ML-KEM on the Cisco 8000 Series SNP provides immediate protection against the retroactive decryption of mission-critical traffic.
- **Compliance with Global Standards:** Adhering to NIST and CNSA mandates ensures that every layer of the stack—from asymmetric public keys to symmetric encryption and firmware updates—is hardened against quantum cryptanalysis.
- **A Disciplined Adoption Path:** Whether utilizing a Hot Swap or Parallel Island approach, this guide ensures that the transition to PQC standards is achieved with zero downtime and total operational transparency.

In the quantum era, a "secure network" is defined by its readiness. This guide provides the blueprint; the Cisco 8000 Series provides the platform. Together, they ensure that your organization's most sensitive data remains secure, both now and throughout the quantum evolution.