Post-Quantum Cryptography on Cisco 8000 Series Secure Routers

Introduction

Q: What is Post-Quantum Cryptography?

A: Post-quantum cryptography, or PQC, is designed to protect against future cyber attacks from quantum computers. Much of today's public-key cryptography relies on math problems that would take classical computers an impractically long time to solve. A sufficiently powerful quantum computer could solve those problems much faster, putting commonly used key exchange and digital signatures at risk.

This creates a significant risk where attackers can capture encrypted data now and potentially decrypt it later in a threat called "Harvest Now, Decrypt Later (HNDL)." PQC helps organizations start protecting sensitive data before that threat becomes a reality.

Q: If quantum computers don't exist today, why should I be concerned about post-quantum threats?

A: Because the immediate risk has already started. Attackers can capture your encrypted data today and store it to potentially decrypt later through HDNL.

Moving to PQC also takes time. You need to understand where vulnerable cryptography is used, prioritize sensitive data, and update your infrastructure over time. Starting now gives you time to plan the transition instead of rushing it later.

Q: What does PQC have to do with routing?

A: Your router sits at a critical point at the WAN edge, where data moves between branches, data centers, cloud environments, and the internet. As the WAN connects these distributed environments and carries sensitive data between them, it naturally becomes most important place to begin your PQC preparation. Those connections rely on cryptography to protect communications and authenticate trusted devices.

PQC helps prepare the WAN for quantum threat defense by strengthening how secure connections are established, how devices are authenticated, and how the router itself verifies trusted software.

© 2026 Cisco and/or its affiliates. All rights reserved.

Solution

Q: What network routers does Cisco offer to help me prepare for PQC?

A: Cisco® builds post-quantum capabilities into the hardware and software of secure networking infrastructure you use to connect branches, campuses, data centers, cloud environments, and other locations.

Cisco 8000 Series Secure Routers and Cisco IOS® XE protects your WAN in three ways:

1. **Quantum-safe encryption:** Helps protect how encryption keys are established for secure connections across your WAN.
2. **Quantum-safe authentication:** Uses post-quantum digital signatures to help verify that the devices you connect to are trusted.
3. **Quantum-safe Secure Boot:** Extends post-quantum protection to the router itself by establishing hardware and software root-of-trust every time the device boots up.

Together, these capabilities help protect your communications and hardware.

Exact support depends on the Secure Router model, software release, protocol, and deployment mode. Visit the Cisco 8000 Series Secure Router data sheets for specific details.

Q: Which PQC algorithms are supported on the Cisco 8000 Series Secure Routers?

A: Post-quantum cryptography uses algorithms designed to protect key establishment and digital signatures against future quantum attacks. Cisco uses post-quantum algorithms aligned with NIST standards:

- **ML-KEM (FIPS 203):** Helps establish quantum-safe encryption keys for secure communications, including supported IKEv2/IPsec VPN connections across the WAN.
- **ML-DSA (FIPS 204):** Provides quantum-safe digital signatures for authentication and software verification.
- **LMS (NIST SP 800-208):** Provides quantum-safe digital signatures used as part of Secure Boot.

This approach extends quantum protection beyond encryption to help address authentication and trust in the infrastructure itself.

Q: What PQC capabilities are supported on Cisco 8000 Series Secure Routers?

A: Cisco 8000 Series Secure Routers use post-quantum algorithms to apply PQC across secure encryption, authentication, and platform trust. This includes:

- **IKEv2 IPsec VPNs,** including supported Dynamic Multipoint VPN (DMVPN) and FlexVPN deployments
- **SD-WAN** data and control plane protection
- **LAN and WAN MACsec** on applicable platforms
- **SSH and TLS 1.3** for secure connections
- **Public Key Infrastructure (PKI) and authentication** using quantum-safe digital signatures
- **Secure Boot** capabilities including LMS signed ROMMON and ML-DSA signed IOS XE, to help verify trusted software from startup

© 2026 Cisco and/or its affiliates. All rights reserved.

These capabilities address comprehensive quantum-safe solution to protect your WAN connectivity at every layer of cryptography.

Visit the Cisco 8000 Series Secure Router webpage to learn more about the key feature and capabilities for each Secure Router.

Q: What protection is available to defend against HDNL attacks on legacy platforms?

A: PPK based implementation (RFC 8784) is available on Catalyst 8000 Series platforms for defending against HNDL.

Q: What is quantum-safe Secure Boot, and why does it matter?

A: Secure Boot helps your router verify that it starts with trusted Cisco software every time the device boots up. Quantum-safe Secure Boot extends the protection with LMS signed ROMMON and ML-DSA signed IOS XE verification and establishes secure chain of trust for quantum defense.

This means your PQC strategy can go beyond protecting data in transit to also help protect the integrity and authenticity of the infrastructure carrying it.

Q: How do Cisco Secure Routers support PQC for SD-WAN?

A: Cisco Secure Routers extend quantum-safe protection across the SD-WAN fabric. On supported platforms and Cisco IOS XE releases, ML-KEM strengthens key establishment using IKEv2 IPsec connections to protect data moving between SD-WAN sites.

PQC capabilities also extend to the SD-WAN control plane using TLS 1.3 based ML-KEM implementation to protect the connections used to manage and coordinate the fabric.

Q: How do Cisco Secure Routers support PQC for SASE?

A: Secure Access Service Edge (SASE) depends on secure connections between branch locations and cloud-delivered security services. Cisco 8000 Series Secure Routers apply PQC to IKEv2 IPsec VPN connections, including supported DMVPN and FlexVPN deployments. A hybrid key exchange combines post-quantum and classical cryptography to help protect the keys that establish these WAN connections against future quantum threats. This helps strengthen the secure connectivity that SASE relies on.

Q: Do I need Cisco 8000 Series Secure Routers to access all these PQC capabilities?

A: Yes, Cisco 8000 Series Secure Routers offer comprehensive PQC capabilities to address immediate defense against the HNDL threat and establish complete solution approach across quantum-safe encryption, authentication, and secure boot, helping you prepare your WAN infrastructure for the transition to PQC.

Q: Do I need an additional license to access PQC capabilities on the Cisco 8000 Series Secure Routers?

A: No. PQC solutions are expected to offer each layer of cryptography with updated algorithms. The associated PQC capabilities on the Cisco 8000 Series Secure Routers can be consumed using your existing essentials or advantage license configuration based on the use-case.

Please review the Cisco 8000 Series Secure Router Feature Matrix to learn about which features are available based on license type.

© 2026 Cisco and/or its affiliates. All rights reserved.

Q: Can Cisco Secure Routers help me prepare for government or industry PQC requirements?

A: Yes. Cisco Secure Routers use standards-based post-quantum algorithms such as ML-KEM (FIPS 203), ML-DSA (FIPS 204) and LMS (NIST SP 800-208) capabilities to help you prepare for evolving government and industry requirements, including CNSA 2.0 and associated IETF protocol standards as applicable.

Requirements and timelines vary by country and industry, so PQC-capable infrastructure should be part of a broader migration and compliance plan.

Q: How does PQC affect Secure Router performance?

A: Cisco Secure Routers are designed with hardware-accelerated cryptographic capabilities to support demanding security workloads.

Depending on the platform, they deliver IPsec performance ranging from up to 1.5 Gbps on the 8100 Series Secure Routers to up to 225 Gbps on the 8600 Series Secure Routers. Refer to respective data sheets for additional insights.

Zero throughput and tunnel scale impact is expected. Initial tunnel establishment can require some additional processing due to the post-quantum key exchange but the same scale is supported for a given platform.

Migration

Q: What is Cisco's approach to helping customers complete a PQC migration?

A: Cisco supports a hybrid approach to PQC migration, enabling you to introduce quantum-safe cryptography while continuing to use proven classical cryptography during the transition.

For supported use cases, Cisco combines traditional key exchange with post-quantum algorithms such as ML-KEM. This helps you strengthen protection against future quantum threats while migrating your WAN in phases, rather than changing your entire infrastructure at once. Cisco's approach also incorporates crypto-agility, so your cryptographic strategy can continue to evolve as the PQC landscape changes.

Q: What is crypto-agility, and why does it matter for PQC?

A: Crypto-agility is the ability to update and transition cryptographic algorithms as security standards and threats evolve.

Cisco 8000 Series Secure Routers give you infrastructure you can invest in today that is designed to adopt newer algorithms and standards as cryptography evolves. This helps you adopt new algorithms and requirements over time without treating PQC as a one-time migration.

Q: How do I know what areas of my network are not quantum ready?

A: Start by identifying where your network relies on quantum-vulnerable public-key cryptography, such as RSA and Elliptic-Curve Cryptography (ECC). Look across your encryption, key exchange, authentication, certificates, software, and network infrastructure to understand where these algorithms are still in use.

The Cisco IQ Quantum Readiness Assessment can help evaluate your environment, identify potential gaps, and prioritize where to begin your PQC migration.

Q: What happens if one router supports PQC and the other does not?

A: PQC-capable and non-PQC routers can coexist during your migration as you adopt ML-KEM hybrid PQC implementation. For supported configurations, PQC can be optional, allowing a router to establish a quantum-safe session with a PQC-capable peer while continuing to use classical cryptography with a peer that does not support PQC.

© 2026 Cisco and/or its affiliates. All rights reserved.

This gives you flexibility to migrate your WAN in phases without requiring every router to be upgraded at the same time. As you plan your PQC migration, work with your Cisco team or trusted experts to understand your current environment, prioritize critical connections, and build the right transition plan.

Q: Is PQC architecture agile to stay future proof?

A: Yes, the architecture is crypto agile. It is designed to accommodate evolving government mandates, standards, and protocols.

Q: How do I know if PQC is working on my routers?

A: Use the PQC verification steps in the Cisco 8000 Series Secure Routers configuration guide. These steps confirm that PQC is active in the session, not just configured on the router.



© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C67-6809214-00 11/26