Post-Quantum Cryptography Challenges and Opportunities

TECHNICAL WHITE PAPER

TABLE OF CONTENTS:

Executive Summary

The advent of quantum computing promises to revolutionize fields from materials science to pharmaceuticals. However, for the cybersecurity community, it presents a fundamental threat to the cryptographic foundations of the modern internet. Most current encryption standards—including RSA and Elliptic Curve Cryptography (ECC)—rely on mathematical problems that a Cryptographically Relevant Quantum Computer (CRQC), when available, could solve swiftly.

This white paper explores the technical implementation of Post-Quantum Cryptography (PQC), the immediate risks of "Harvest Now, Decrypt Later" (HNDL) attacks, and how organizations can leverage Zscaler's industry-first PQC capabilities to prepare for a quantum-secure future.

1. Understanding Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography refers to a new generation of cryptographic algorithms designed to be secure against both quantum and classical computers. Unlike current public-key algorithms that rely on the difficulty of integer factorization (RSA) or discrete logarithms (ECC), PQC is built upon mathematical problems that are currently believed to be intractable even for quantum systems.

Technical Implementation: How PQC Works

Most leading PQC algorithms, including those recently standardized by NIST (National Institute of Standards and Technology), fall into several categories:

- **Lattice-Based Cryptography:** Algorithms such as ML-KEM (formerly Kyber) and ML-DSA (formerly Dilithium) are based on the "Shortest Vector Problem" (SVP) in high-dimensional lattices. These are considered the most versatile for general-purpose encryption and digital signatures due to their relatively small key sizes and high performance.
- **Code-Based Cryptography:** Based on error-correcting codes, these algorithms (like Classic McEliece) have been studied for decades and are known for their high security, though they often require larger key sizes than lattice-based alternatives.
- **Hash-Based Signatures:** Algorithms like SLH-DSA (formerly SPHINCS+) provide stateful and stateless digital signatures based on the security of cryptographic hash functions (e.g., SHA-3). These are highly resistant to quantum attacks because they do not rely on structured mathematical groups.

Opportunities for the Modern Enterprise

PQC is not just a defensive necessity: it is an opportunity for crypto agility. By transitioning to PQC algorithms, organizations can:

- **Modernize Legacy Infrastructure:** Use the transition as a catalyst to phase out deprecated protocols and weak algorithms.
- **Enhance Data Longevity:** Protect intellectual property and sensitive records that must remain confidential for 20, 50, or even 100 years.
- **Gain a Competitive Advantage:** Demonstrating "quantum-ready" security builds trust with partners and customers who are increasingly aware of long-term data risks.

2. The Flipside: Quantum Risks and the HNDL Threat

The primary motivation for adopting PQC is the looming threat posed by quantum computers. While a CRQC capable of breaking 2048-bit RSA may still be several years away, the risks to data are active today. Moreover, parties that would build a CRQC may not announce it publicly, resulting in a long period of uncertainty about whether or not a CRQC already exists.

Shor's Algorithm and the End of Classical Public-Key Cryptography

In 1994, Peter Shor developed a quantum algorithm that can factorize large integers and solve discrete logarithms in polynomial time. This means that as soon as a sufficiently powerful quantum computer exists, almost all current asymmetric encryption used for key exchange (Diffie-Hellman) and digital signatures (ECDSA) will become obsolete. Additionally, newer and more efficient algorithms have also been proposed that pose a threat to asymmetric encryption methods.

"Harvest Now, Decrypt Later" (HNDL)

Adversaries—including nation-state actors—are currently practicing HNDL (you may also see "SNDL," an acronym for "store now, decrypt later," in articles or online forums discussing quantum threats): they are intercepting and storing massive amounts of encrypted traffic traversing the internet today. Their strategy is simple: even if they cannot read the data now, they will store it until a CRQC is available to decrypt it retrospectively.

This creates an immediate risk for any data with a long-term "secrecy requirement." If your organization's data (e.g., clinical trial results, national security secrets, or long-term financial plans) is captured today, it will be compromised shortly after a quantum computer is online.

3. Preparing for a Quantum Future: A Roadmap

Organizations cannot wait for the first CRQC to be publicly announced before they begin their transition. NIST and the CISA (Cybersecurity and Infrastructure Security Agency) recommend a multi-phased approach to quantum readiness.

Step 1: Inventory Protocol Information and the Cryptographic Stack

The first and most critical step is visibility. Organizations must inventory all systems, applications, and network services that use public-key cryptography.

- Identify where RSA and ECC are used for TLS, code signing, and identity management.
- Document the "confidentiality lifetime" of the data being protected.
- Inventory protocol information since legacy protocols such as TLS 1.2 are not compatible with PQC.

Step 2: Identify PQC-Ready Traffic

As software vendors begin to roll out PQC-capable clients (e.g., Google Chrome and Firefox browsers) and servers, your network will start seeing Hybrid Key Exchanges. These combine classical algorithms (like X25519) with PQC algorithms (like ML-KEM). Organizations need the ability to identify this traffic to ensure that their security stack is not inadvertently blocking or breaking it.

Step 3: Implement Crypto-Agility

Crypto-agility is the ability of a system to quickly switch between cryptographic algorithms without requiring a complete overhaul of the underlying infrastructure. Organizations should prioritize vendors and protocols that support modular algorithm updates.

4. How Zscaler Enables the PQC Transition

Zscaler has integrated PQC capabilities directly into the Zero Trust Exchange™ platform, allowing organizations to adopt quantum-safe security without disrupting their operations.

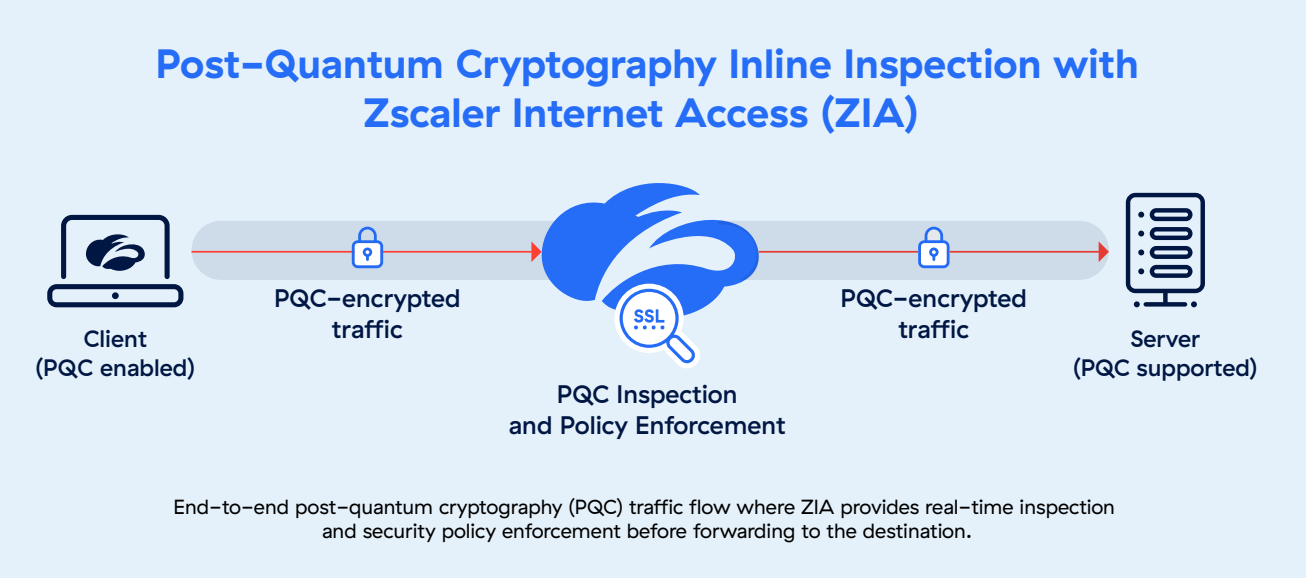
Industry-First PQC Traffic Inspection

Zscaler is the first Security Service Edge (SSE) provider to offer inline PQC traffic inspection as well as visibility via analytics reporting and logging.

- **Visibility:** Zscaler's PQC Visibility Report identifies which applications and users are already using PQC-capable clients as well as specifics around those transactions.
- **Security:** Zscaler can now decrypt, inspect, and re-encrypt TLS traffic using quantum-safe key exchange algorithms. This ensures that even as your traffic becomes quantum-resistant, it remains subject to the same deep content inspection, DLP, and threat prevention policies that Zscaler provides for classical traffic.

Zscaler performs real-time, deep inspection of PQC traffic, by leveraging the NIST-standardized ML-KEM (FIPS 203) standard for post-quantum key exchange. Just as we do for classical encryption, Zscaler unlocks complete visibility and protection for PQC sessions, all without impacting performance. Our implementation of hybrid PQC key exchange is compliant with the draft-ietf-tls-echde-mlkem proposed standard and is fully compatible with Chrome, Firefox, Safari and other widely deployed clients as well as servers.

ML-KEM is a post-quantum key establishment method that lets two parties create the same shared secret over an insecure network, without sending that secret directly—so an eavesdropper can record everything but still can't compute the secret. By implementing PQC traffic inspection with ML-KEM, Zscaler unlocks the visibility and protection that inline inspection of PQC sessions provides.



End-to-end post-quantum cryptography (PQC) traffic flow where ZIA provides real-time inspection and security policy enforcement before forwarding to the destination.

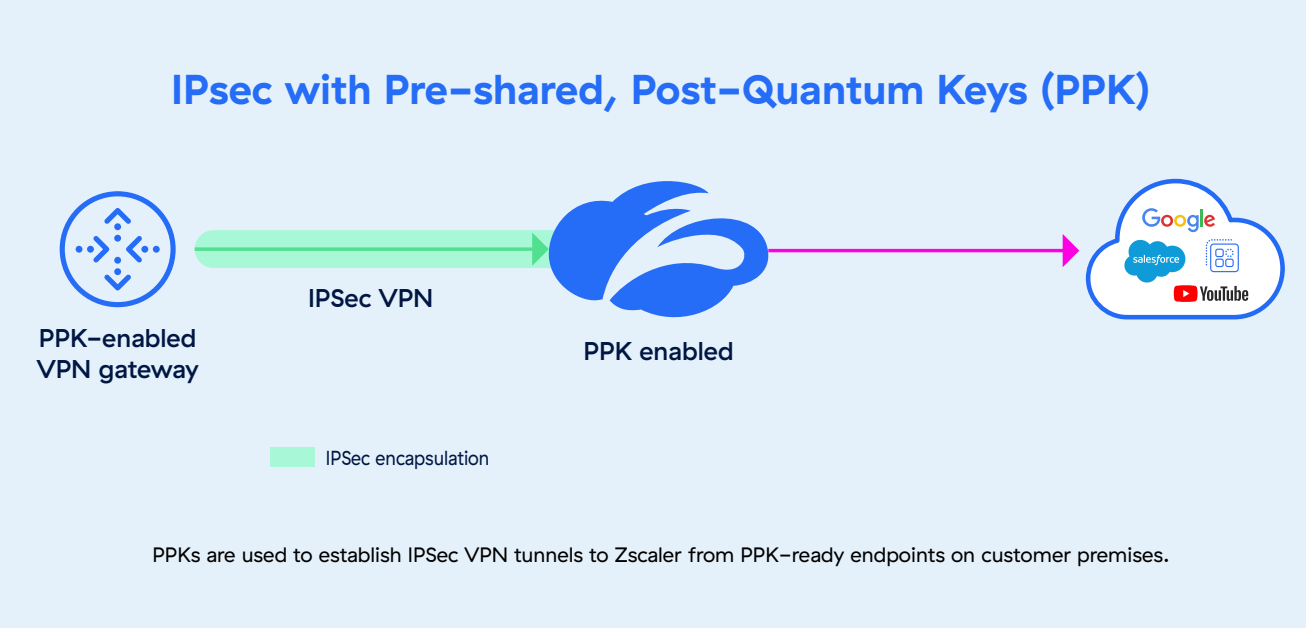
The Zscaler Zero Trust Exchange sits inline, and our cloud-native inspection engine seamlessly decrypts, scans and enforces security policy, and re-encrypts traffic before sending it onto its destination. Here's how our quantum-ready inspection process works:

- **Zscaler checks the TLS ClientHello message from the client:** If the client indicates TLS 1.3 support and includes a hybrid PQC supported TLS Group in its proposal, Zscaler Internet Access uses TLS 1.3 with a supported hybrid PQC key exchange group. This process is independent of server capabilities and allows PQC usage between client and ZIA even if the server does not support it. The supported TLS version and selected key exchange group is always logged so administrators can get valuable information about PQC support on the client side. Those same insights can help security and IT teams prioritize upgrading software that is not PQC ready.

- **Zscaler sends TLS ClientHello to the server on behalf of the client:** In the ClientHello message it indicates support for TLS 1.3 and includes all standard hybrid PQC TLS Groups in the offer. In the TLS protocol it is up to the server to choose from a supported list of key exchange algorithms. Zscaler Internet Access logs selected TLS version and cryptographic parameters for each session that allows administrators to understand the security posture and work with service providers to use PQC capabilities.
- **Zscaler performs traffic inspection and applies security policies:** all threat prevention, DLP and access control policies are applied transparently for the client and server without any configuration changes to current policies. This means Zscaler provides the same industry-leading threat detection and prevention to PQC sessions that Zscaler has applied to non-PQC traffic for years.

Securing IPsec VPN Tunnels with Pre-shared, Post-Quantum Keys (PPK)

While traditional IPsec VPNs are vulnerable to quantum attacks on their IKEv2 key exchanges, Zscaler has implemented Post-Quantum Pre-shared Keys as defined in RFC 8784.

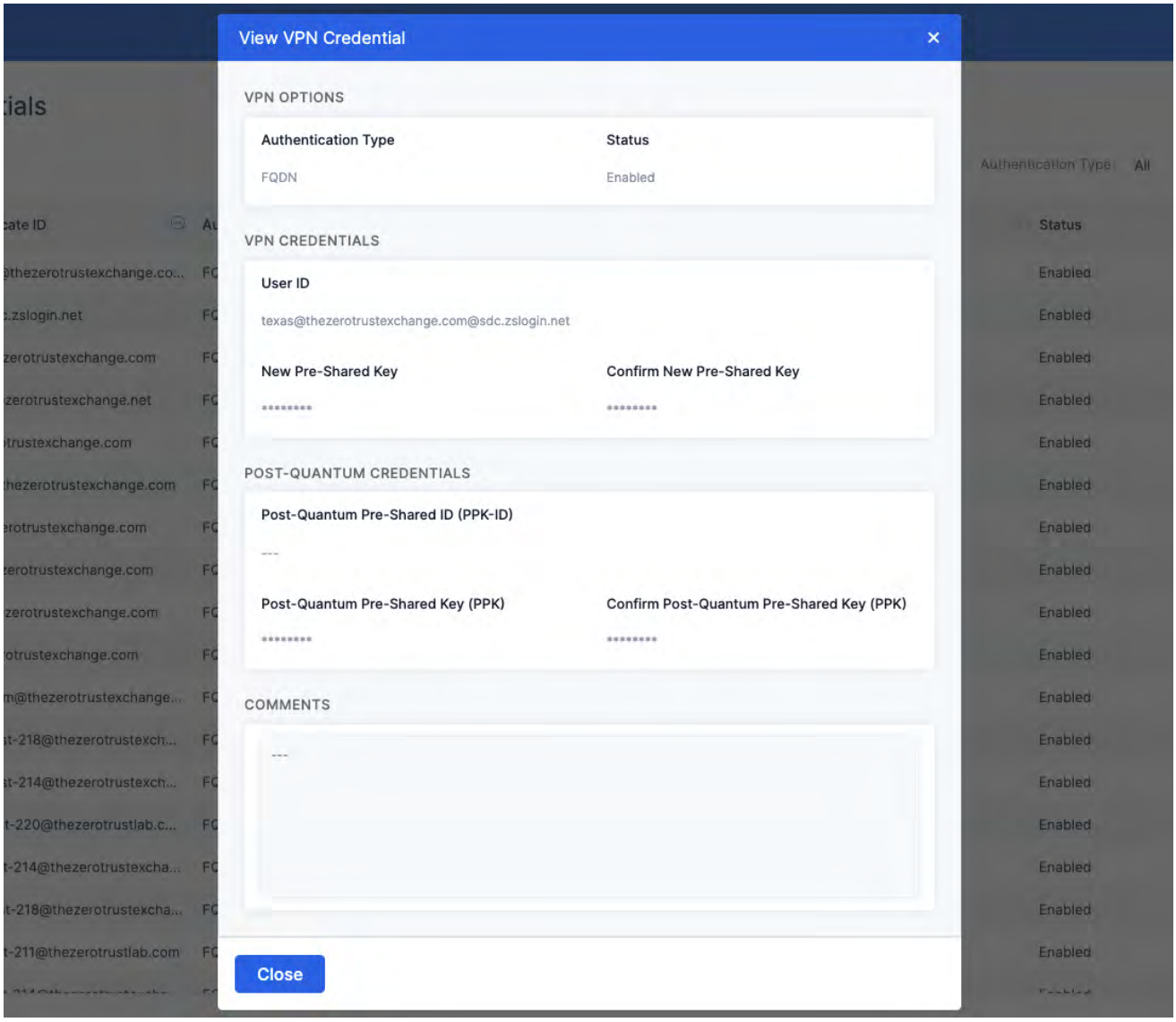


PPKs are used to establish IPSec VPN tunnels to Zscaler from PPK-ready endpoints on customer premises.

- PPK adds an additional layer of security by mixing a quantum-safe pre-shared key into the standard IKEv2 key derivation process.
- Even if an attacker uses a quantum computer to break the initial Diffie-Hellman exchange, they cannot derive the final session keys without the PPK. This provides an immediate, robust defense for branch-to-cloud and site-to-site connectivity.

How it works

- To counter the HNDL scenario, pre-shared post-quantum keys are generated outside of a VPN tunnel and then inserted at:
  - The client gateway
  - The PPK-enabled VPN gateway
  - And in the Zscaler Admin Portal as shown below:



- These PPK keys are used to create the keys that are used to encrypt the VPN tunnel traffic.
- This method protects the integrity of IKE Key derivation so that IPsec keys remain secure even if the Diffie-Hellman (DH/ECDH) exchange is later broken by a quantum computer.

Conclusion

The transition to Post-Quantum Cryptography is not an overnight task: it is a strategic migration that begins with visibility and ends with a resilient, crypto-agile architecture. By addressing the HNDL threat today and leveraging Zscaler's PQC inspection and IPsec tunnel security, organizations can ensure that their data remains secure in the quantum era and beyond.

Learn more about how Zscaler can be your trusted partner on your PQC transition journey: schedule a demo discussion today

zscaler™ | Act Fast. Stay Secure.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com