Post-Quantum Cryptography Inline Inspection

Decrypt and inspect quantum-encrypted traffic at scale, defend against “harvest now, decrypt later” attacks and meet compliance mandates

SOLUTION BRIEF

“Q Day” will be upon us by 2030 according to industry analysts: this is the day that a quantum computer will be able to break today’s public-key cryptography.

Representing the next generation in computing power, quantum computers use specialized technology—including hardware and algorithms that take advantage of the principles of quantum mechanics—to solve complex problems that our current “classical” computers or supercomputers can’t solve (or can’t solve quickly enough).

While the rise of quantum computing presents a transformative opportunity for innovation it will also introduce new challenges:

Defending Against Quantum Threats

When decryption by a quantum computer becomes available, threat actors will decrypt these stolen secrets, data and other sensitive information for further exploitation. Existing VPN tunnels are not quantum-safe either, exposing them to potential decryption by quantum computing in the future.

Meeting Compliance Mandates

Governments are requiring organizations to implement PQC because encrypted data has a long shelf life, the internet is globally interconnected, and crypto migrations can take years—so coordinated standards and timelines reduce systemic risk and transition cost. Because the internet and supply chains are globally interconnected, countries are collaborating to ensure interoperable, standards-based PQC adoption that avoids fragmentation, lowers transition cost, and supports regulation of critical sectors.

Bolstering Business Continuity

Keeping critical operations running through disruptions is central to business continuity—and the shift to quantum-resistant cryptography is a predictable, high-impact technology transition that could disrupt availability, trust, and compliance if handled reactively.

Current Cryptographic Algorithms will Become Vulnerable

Modern key exchange and digital signature mechanisms used in TLS, SSH and IPsec are vulnerable to attacks by forthcoming quantum computers. This represents a threat to traffic being transferred between devices and workloads today as attackers can capture traffic, store it and decrypt once quantum capability becomes available.

Achieve Deep PQC Traffic Inspection and Bolster Your Defenses

Zscaler Internet Access™ (ZIA™) can now provide real-time inspection of PQC traffic and security policy enforcement before forwarding requests to the destination. Unlike other vendors, Zscaler's cloud native solution provides visibility and the same level of threat protection regardless of the encryption algorithm applied to incoming traffic.

With Zscaler, organizations gain deep visibility into quantum-encrypted traffic without sacrificing performance or interoperability with other key IT assets in their compute environment. Just as done now with classical encryption algorithms, customers can make the transition to those that are quantum-safe without impacting their operations. With quantum-encrypted traffic inspection, Zscaler delivers:

Seamless inline inspection of PQC traffic at scale

By leveraging hybrid PQC key exchange, Zscaler performs full SSL/TLS decryption and deep content inspection on traffic initiated by clients or servers using post-quantum cryptography algorithms.

Deep visibility into PQC traffic for granular control

Recognize and negotiate hybrid PQC key-encapsulation mechanisms (KEM) in TLS 1.2. Auto-detect leading post-quantum KEM groups such Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) and Open Quantum Safe alongside classical elliptic curves. ML-KEM is the primary NIST standard for post-quantum key exchange finalized in August 2024 as FIPS 203.

Industry-leading performance and control

Retain high throughput and low latency regardless of whether classical or quantum-safe algorithms are applied to traffic traversing your environment.

Frictionless deployment

Apply existing zero trust access and threat prevention policies without changing configurations or policy criteria.

The Zscaler Quantum-Ready Inspection Solution

Zscaler now provides real-time, deep inspection of PQC traffic, 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.

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 key exchange 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 key exchange methods 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.

Post-Quantum Cryptography Inline Inspection with Zscaler Internet Access (ZIA)

Key Features

Inline SSL/TLS Inspection with ML-KEM

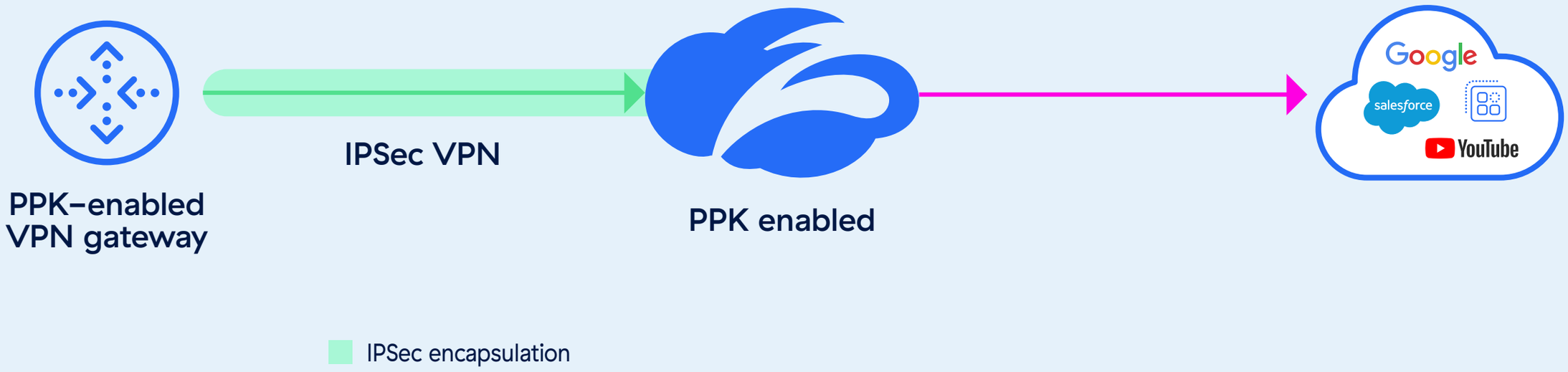
ML-KEM is a post-quantum key establishment method that lets two parties create the same shared secret over an insecure network, without sending that secret directly—so an eavesdropper can record everything but still can't compute the secret.

- By implementing PQC traffic inspection with ML-KEM, Zscaler unlocks the visibility and protection that inline inspection of PQC sessions provides.
- Recognize and negotiate hybrid PQC key-encapsulation mechanisms (KEM) in TLS 1.2.
- Auto-detect leading post-quantum KEM groups such ML-KEM and Open Quantum Safe alongside classical elliptic curves.

PQC IPSec with Pre-shared, Post-Quantum Keys (PPK)

- Establishes IPSec VPN tunnels to Zscaler from PPK ready endpoints on customer premises so organizations can employ PQC safe keys, safeguarding their traffic from threat actors.
- Provides a post-quantum risk-mitigation mode for IPsec without requiring full PQC algorithms in the key exchange.
- 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.

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



Benefits

- **Real-time decryption and deep content inspection on PQC-encrypted sessions** to provide superior detection and protection.
- **Leverage future-proof, secure VPN forwarding** to Zscaler
- **Prevents the decryption of captured VPN traffic later,** even when quantum computers become available.
- **Secures harvested data** since attackers need both the encrypted data and keys which RFC 8784 is designed to protect
- **Enables a practical, quantum-resistant transition** from classical to post-quantum cryptography that can be deployed today
- **Simplifies deployment** since existing cryptographic algorithms require no changes.
- **Rapid implementation** when both VPN endpoints support RFC 8784

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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

zscaler™

Act Fast.
Stay Secure.