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

AT-A-GLANCE

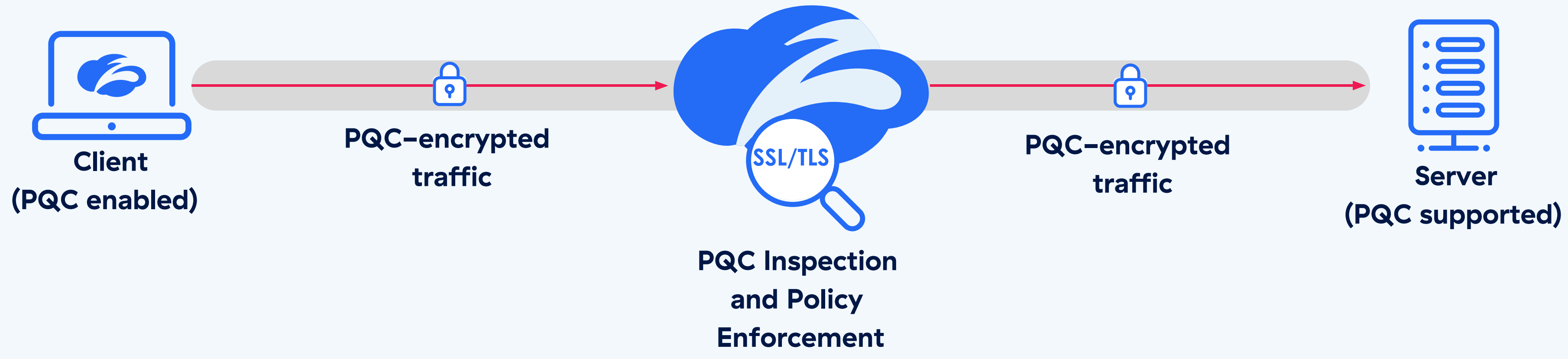
About Post-Quantum Cryptography Inline Inspection

“Q Day” is the day quantum computers will be able to break today’s public-key cryptography—and it could be here as soon as 2030 according to industry analysts.

Representing the next generation in computing power, quantum computing uses specialized technology to solve complex problems that our current “classical” computers can’t solve—or can’t solve quickly enough. But 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.

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.

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



PQC Inline Inspection Benefits

Seamless Inline Inspection of PQC Traffic at Scale

Leveraging hybrid PQC key exchange, 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 both pure and hybrid PQC key-encapsulation mechanisms (KEM) in TLS 1.2. Auto-detect 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.

Frictionless Deployment

Apply existing zero trust access and threat prevention policies without changing customer configurations.

Inline SSL/TLS Inspection with ML-KEM

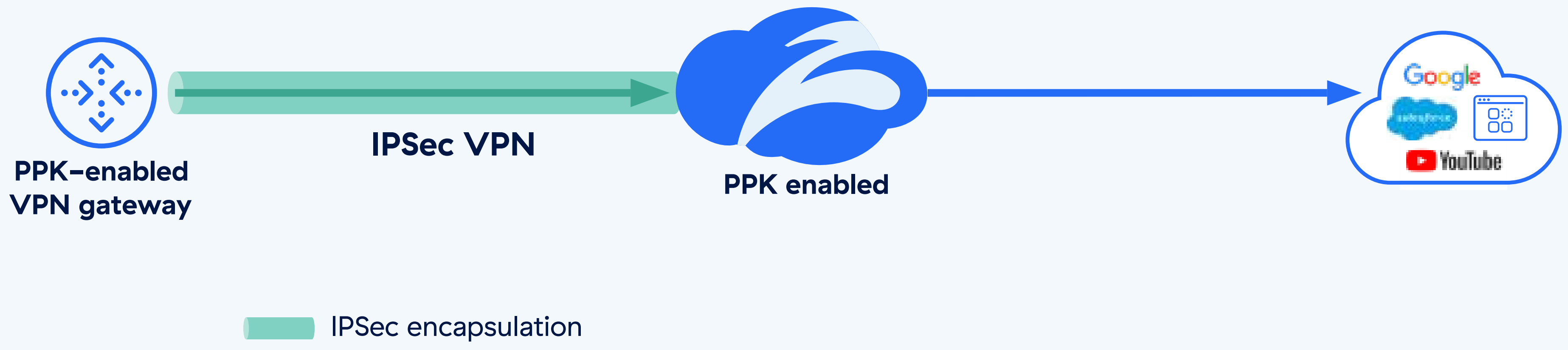
ML-KEM is a post-quantum key establishment method that lets two parties create the same shared secret over an insecure network, without sending that secret directly—so even if an eavesdropper captures data packets they still cannot compute the secret.

- Unlock the visibility and protection that inline inspection of PQC sessions with ML-KEM 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)



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

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**

Act Fast. Stay Secure.