Palo Alto Networks and Quantropi

Delivering a Quantum Secure IPsec VPN to Mitigate Harvest Now, Decrypt Later Attacks

Benefits of the Integration

- Implement a quantum entropy secured IPsec VPN with a much higher resistance to future quantum attacks.
- Quantum-safe IPsec VPN communications without cryptographic upgrades or any dependency on NIST PQC algorithm approval timelines.
- Encrypted communications remain secure even if a core key exchange is compromised—mitigating harvest now, decrypt later attacks.
- Easy-to-use browser extension generates PPKs with flexibility to configure directly in PAN-OS® or via Panorama®.

The Challenge

Organizations rely on site-to-site IPsec VPN security to protect critical data. However, bad actors are already storing encrypted communications today to decrypt in the future, using quantum computing or other advanced capabilities, such as "harvest now, decrypt later." IPsec VPNs are starting to incorporate new post-quantum algorithms to address this threat, but these alone aren't sufficient.

Although it will take time before fully approved, FIPS-validated software packages with post-quantum algorithms are available. Even so, the new algorithms won't have decades of vetting like classic algorithms in use today. If a major issue surfaces, there's only one standardized key encapsulation mechanism (ML-KEM) preventing a crypto-agile approach to simply switch algorithms.

Organizations need an immediate solution to protect critical data, one that isn't dependent on standards and FIPS timelines and also provides a defense-in-depth approach that doesn't rely solely on new algorithms.

The Solution

To quantum-secure an IPsec VPN, add post-quantum pre-shared keys (PPKs) to the configuration per the RFC 8784 standard, PPKs are shared out-of-band to VPN nodes. When a connection is initialized, PPKs are "mixed" with classic key material from the key exchange process and the mixed key is used to encrypt communications. Key mixing modifies the original key from the key exchange—so it isn't solely based on prime numbers—to protect against harvest now, decrypt later attacks based on Shor's algorithm.

Quantropi QiSpace SEQUR PPK Generator

The Quantropi QiSpace™ SEQUR PPK Generator is a browser extension available from major app stores including Chrome, Edge, and Firefox. The PPK Generator—powered by our global quantum entropy generation and distribution network—can generate PPKs between 16 bytes to 64 bytes in hex or Base64 format that are securely delivered to the browser using AES-256 payload encryption.

A PPK should be a strong random secret that can't be predicted algorithmically or by other advanced methods like machine learning. Therefore, the strongest PPKs need to be generated from truly random processes such as quantum phenomena in a quantum random number generator (QRNG). High-quality QRNG-based keys significantly lower the probability of a successful quantum-based attack.

Quantropi sources its quantum entropy from various industry-leading QRNG vendors for entropy diversity and validates entropy quality using a robust set of industry-standard statistical testing tools with audit reporting available.

Palo Alto Networks NGFWs

Palo Alto Networks Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection everywhere. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Quantropi

The Palo Alto Networks NGFW and Quantropi QiSpace SEQUR PPK Generator integration provides an elevated security posture by ensuring IPsec VPN traffic is secure against quantum and harvest now, decrypt later attacks. Layering the Quantropi RFC 8784-compliant solution provides protection without deploying post-quantum cryptography (PQC) algorithms.

The Quantropi PPK Generator integrates with Palo Alto Networks NGFWs to allow system administrators to add PPKs to IPsec VPN configurations. The PPK Generator can be accessed directly from the NGFW configuration screen with no rekeying or copy/pasting. Up to 10 unique PPKs can be configured for each IKE Gateway profile.

Use Case 1: Ensuring Compliance and Protecting Critical Data

Challenge

Regulatory compliance and/or internal policy requirements often require safeguarding critical data for long periods of time—in many cases, seven years or longer. Ensuring compliance with long-term data protection policies requires a mitigation for harvest now, decrypt later attacks. Attackers harvesting encrypted data today may have the ability to decrypt it before the end of this decade.

Solution

Palo Alto Networks NGFW, in combination with Quantropi's PPK Generator, protects IPsec VPN traffic against harvest now, decrypt later attacks and helps ensure compliance with long-term data protection requirements. This protection mixes in an out-of-band, quantum-generated PPK during the key exchange process.

The PPK itself is never transmitted over the connection—only the Key ID of the PPK is specified to identify the correct PPK to use in the key establishment. Adversaries listening on the connection can only harvest the classic key material and the PPK Key ID but not the PPK itself. Without the PPK component, the adversary can't reconstruct the key and decrypt data.

Use Case 2: Protecting Critical Data in Heterogeneous Environments

Challenge

Many IPsec VPN environments are heterogeneous with solutions from different vendors—and even involve connections across two or more organizations. However, these environments still require the same level of data security and need solutions that are compatible across vendors and easy to implement between organizations.

Solution

Palo Alto Networks NGFW supports industry standards, including RFC 8784 for post-quantum pre-shared key mixing. This enables quantum secure heterogeneous IPsec VPN connections with any vendor that supports the RFC 8784 standard.

Quantropi's PPK Generator is compatible with major firewall vendors and is available from the Chrome, Edge, or Firefox app stores. Using the PPK Generator, system administrators can create quantum-generated pre-shared keys that are securely delivered out-of-band to the browser. These PPKs can be configured on heterogeneous IPsec VPN endpoints in just a few minutes to create quantum secure connections across different vendor hardware and between organizations.

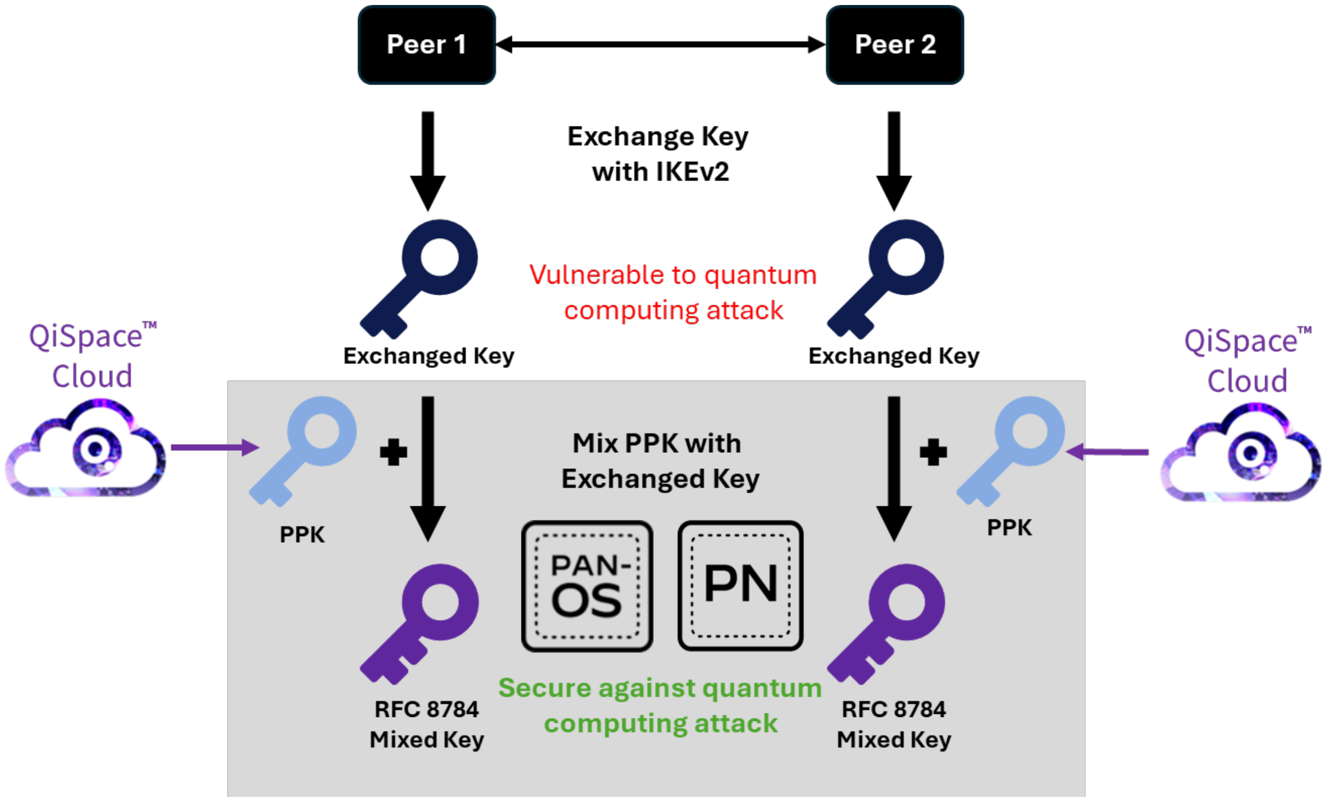

Figure 1: Post-quantum security for IPsec VPN

About Quantropi

Quantropi, Inc. is a Canadian cybersecurity company founded in 2018 that provides quantum secure cryptography to protect data and communications. Quantropi's QiSpace platform includes all three criteria for complete cryptographic integrity—Trust, Uncertainty, and Entropy (TrUE)—providing governments and organizations with quantum-secure cryptography to protect data, networks, and systems.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com