quantropi
Bring it on.

QiSpace SEQUR™ RFC 8784 PPK Generation for PAN-OS 11.1

QiSpace SEQUR™ supports the generation of Post-quantum Preshared Keys (PPKs) in compliance with RFC 8784 for any Palo Alto Networks Next Generation Firewall running PAN-OS 11.1 or greater.

What is RFC 8784?

IETF RFC 8784 "Mixing Preshared Keys in Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security" is a mechanism to create IKEv2 IPSec VPN connections that are resistant to quantum attacks. This is accomplished by adding PPKs using an out of band mechanism to each side of the VPN. The PPKs are then "mixed" with the classic key material from the Diffie-Hellman (DH) 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.

PPK mixing provides hardened security for the key exchange in two ways:

1. If the core key exchange process was compromised - by a quantum computer using Shor's algorithm, or any other unforeseen attack - the additional PPK component that is mixed in will still ensure the subsequent encryption remains secure.
2. An adversary, or man in the middle, listening on the connection to execute a "steal now, crack later" attack will only be able to harvest the classic DH key material and the PPK Key ID, but not the PPK itself. Without the PPK component, the adversary will not be able to reconstruct the key and decrypt the data.

RFC 8784 is an existing multi-vendor standard that is recommended by government agencies, including NIAP, the NSA, and the German Federal Office for Information Security. It is independent of the NIST PQC approval timelines and can be implemented today with no additional network resources consumed or significant latency added.

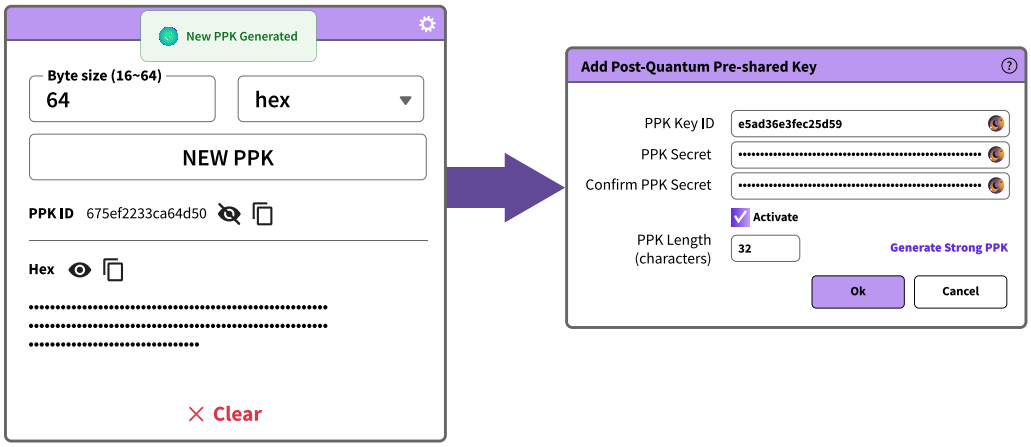
Using QRNG for PPKs

A PPK should be a strong, random secret not subject to a dictionary attack and is 32 Bytes / 256 bits of entropy or greater in length to meet the NIST Category 5 security level. PPKs that are created algorithmically, by definition, are not truly random and are subject to machine learning based attacks and varying levels of quality depending on the underlying device operating system. The optimal PPK should be truly random and produced by a quantum phenomenon in a quantum random number generator (QRNG).

Scan for a free PPK Trial

V02/2024.02.01

QiSpace SEQUR™ PPK Generator provides an easy-to-use web interface to generate a quantum-based PPK that can be copied into the PAN-OS 11.1 IKE Gateway configuration screen.



QiSpace SEQUR™ QRNG Differentiators

QiSpace SEQUR™ is a scalable and resilient hybrid SaaS solution providing a secure distribution network for strong entropy to any endpoint over existing IP networks. Quantropi has invested to create a sophisticated global QRNG generation and distribution network with several key differentiators.

- **Entropy Sovereignty:** With a global data center footprint, customers have complete ownership and control over where their entropy is generated and how it is stored and used. Details about QRNG key material and endpoint consumption is private and only known by the customer.
- **Multi-source QRNG Generation:** QiSpace™ hosts a multi-source portfolio of industry leading quantum random number generators to ensure entropy source diversity. Customers can specify a specific source, mix and match sources, or use sources randomly.
- **Quantum Secure Distribution:** QiSpace™ uses quantum secure symmetric encryption for transmissions to enable high-performance distribution, at gigabits per second, over existing internet infrastructure.
- **Entropy Expansion:** QiSpace™ provides platform resiliency against peak demand and flexibility for connection limited and offline endpoints.

For Pricing and Availability Contact:

Quantropi Inc.
1545 Carling Ave, Suite 620
Ottawa ON, K1Z 8P9 CANADA
+1 (613) 695-5711
www.quantropi.com

Scan for a free PPK Trial