paloalto TECHDOCS

Administración de Seguridad cuántica

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

July 23, 2024

Table of Contents

Conceptos de seguridad cuántica.....5

La amenaza de la computación cuántica.....6

Cómo RFC 8784 resiste las amenazas de computación cuántica..... 10

Cómo las RFC 9242 y RFC 9370 resisten las amenazas de la computación cuántica..... 12

Compatibilidad con funciones postcuánticas..... 15

Planificación y preparación de la migración postcuántica.....17

Prácticas recomendadas para resistir ataques postcuánticos..... 25

Más información sobre la seguridad poscuántica..... 29

Configurar redes VPN IKEv2 resistentes a la tecnología cuántica.....33

Configurar las VPN de tipo IKEv2 postcuántica con PPK RFC 8784..... 34

Configurar las VPN de tipo IKEv2 postcuántica con claves híbridas RFC 9242 y RFC 9370.....41

Ejemplo de configuración de RFC 8784 de IKEv2 Post-Quantum..... 48

Conceptos de seguridad cuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

Las ordenadores cuánticos amenazan la seguridad de la red y los datos. Cuando el desarrollo de la QC alcanza un estado de madurez que produce ordenadores cuánticos criptográficamente relevantes (CRQC), diseñados específicamente para romper el descifrado, muchos cifrados clásicos que se consideraban seguros ya no podrán evitar que los atacantes descifren sus datos. Esto significa que su infraestructura de clave pública (PKI) basada en criptografía clásica será vulnerable a ataques postcuánticos. La amenaza es inmediata, especialmente para los datos de larga duración, debido a los ataques Harvest Now, Decrypt Later, en los que los atacantes obtienen los datos cifrados y los almacenan hasta que tienen un CRQC que puede descifrar los datos.

La resistencia a ataques basados en la computación cuántica comienza con la mejora de la clave creada durante el intercambio de claves IKEv2 para salvaguardar sus VPN, y con la comprensión de su criptografía actual y criptografías postcuánticas (PQC). Las soluciones de Palo Alto Networks para resistir ataques cuánticos se basan en estándares abiertos que permiten y garantizan la interoperabilidad con otros equipos que cumplan con los estándares.

El primer paso es implementar RFC 8784 para crear VPN IKEv2 resistentes a la tecnología cuántica como se describe en este documento. Las VPN resistentes a la tecnología cuántica pueden evitar que los atacantes graben material clave cifrado crítico y evitar que descifren los datos incluso si roban con éxito los datos cifrados. RFC 8784 proporciona una transición resistente a la criptografía cuántica de la criptografía clásica actual de una manera directa que no requiere actualizaciones de criptografía y se considera la manera más fácil de introducir resistencia cuántica a sus comunicaciones VPN.

El segundo paso es implementar RFC 9370 por sí mismo o con RFC 8784 para crear VPNs IKEv2 resistentes a la informática cuántica usando múltiples mecanismos de intercambio de claves (KEM) que pueden combinar tecnologías KEM clásicas y PQC. Esta solución también se conoce como clave híbrida postcuántica IKEv2 y utiliza los nuevos algoritmos PQC de reemplazo que no son vulnerables a un ataque cuántico que utiliza el algoritmo de Shor.

En este capítulo se describen los controles de calidad, la amenaza que representan para la seguridad de sus datos, lo que puede hacer al respecto ahora mediante la creación de VPN IKEv2 resistentes a la cuántica y cómo planificar y prepararse para migrar a VPN y PQC posteriores a la cuántica.

- La amenaza de la computación cuántica
- Cómo RFC 8784 resiste las amenazas de computación cuántica
- Cómo las RFC 9242 y RFC 9370 resisten las amenazas de la computación cuántica
- Compatibilidad con funciones postcuánticas
- La amenaza de la computación cuántica
- Prácticas recomendadas para resistir ataques postcuánticos
- Más información sobre la seguridad poscuántica

La amenaza de la computación cuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

El cifrado de infraestructura de clave pública (PKI) y los mecanismos de intercambio de claves IKE utilizan ampliamente criptografías clásicas como Diffie-Hellman (DH), criptografía de curva elíptica (ECC) y curva elíptica Diffie-Hellman (ECDH). Es probable que las ordenadores cuánticos (QC) rompan estas tecnologías en los próximos 5 a 15 años posteriores a la estandarización del NIST de las primeras criptografías postcuánticas (PQC).

Las VPN de tipo IKEv2 postcuántica basadas en los estándares abiertos RFC 8784, RFC 9242y RFC 9370 resisten los ataques basados en la computación cuántica y los PQC. Con RFC 8784, en lugar de enviar el material de claves al par IKE en el protocolo de enlace de emparejamiento, los administradores configuran y comparten el material de claves por separado, fuera de banda. Si los atacantes roban los datos, no pueden descifrarlos porque no tienen el material clave. RFC 9370 añade siete rondas KEM opcionales adicionales a IKEv2 para permitir la creación de claves de cifrado híbridas formuladas con diferentes tipos de tecnologías KEM. Para romper la clave híbrida, todos los KEM utilizados para crear la clave tendrían que estar en peligro. Las soluciones de Palo Alto Networks para resistir ataques cuánticos se basan en estándares abiertos que permiten y garantizan la interoperabilidad con otros equipos que cumplan con los estándares.

El peligro más inmediato es Harvest Now, Decrypt Later. Aquí los atacantes roban datos (en reposo o en tránsito) que no pueden descifrar ahora y los almacenan hasta que un ordenador cuántico criptográficamente preparado (CRQC) pueda descifrarlos. Un CRQC es un control de calidad optimizado para usar algoritmos cuánticos para romper el cifrado en segundos en lugar de en los millones de años que necesitaría un superordenador clásico. Los datos con mayor riesgo son los datos de larga duración que seguirán siendo relevantes cuando los CRQC estén disponibles.

- ¿Qué es un ordenador cuántico?
- ¿Cómo afecta la amenaza cuántica a mi red?
- Qué hacer ahora para mitigar los ataques de recopilación

¿Qué es un ordenador cuántico?

Ordenadores cuánticos (QC) son básicamente la próxima generación de plataformas de supercomputación. Los QC utilizan las leyes de la mecánica cuántica para reducir en gran medida la cantidad de tiempo que se tarda en procesar datos y ejecutar algoritmos, incluidos los algoritmos que pueden romper el descifrado clásico. Las operaciones que tardarían cientos o miles de años en procesar en un ordenador clásico tardan segundos o incluso microsegundos en un ordenador cuántico. En lugar de basarse en bits clásicos (ceros y unos) que aumentan linealmente la potencia de un superordenador, los QC utilizan cúbits, que se basan en fotones polarizados (luz) y aumentan exponencialmente la potencia de procesamiento de un control de calidad.

Hay varias formas de crear cúbits y el método afecta a la calidad de los cúbits, es decir, a la eficiencia de los cúbits. Cuanto mayor sea la calidad de los cúbits, más rápido y eficaz será el control de calidad. Debido a su naturaleza cuántica, un cúbit representa dos estados a la vez y esos estados se pueden replicar a grandes distancias. Esto se debe a los efectos cuánticos de la superposición y el entrelazamiento:

- **Superposición**: un cúbit puede representar un uno y un cero al mismo tiempo. La combinación de cúbits da como resultado un aumento del número de estados que pueden representar los cúbits porque el número de estados aumenta a una velocidad de 2**n, donde "n" es el número de cúbits. Por lo tanto, dos cúbits pueden representar cuatro estados (2**2), tres cúbits pueden representar ocho estados (2**3), cuatro cúbits pueden representar 16 estados (2**4), etc.

  A medida que aumenta la densidad de cúbits (el número de cúbits que caben en un chip), el número de estados que pueden representar los cúbits combinados aumenta exponencialmente. Cuanto mayor sea la calidad de los cúbits, más se acercará el número combinado de cúbits a una verdadera escala exponencial. Los cúbits de baja calidad (ruidosos), cuando se combinan, no aumentan exponencialmente el número de estados, pero aún así aumentan significativamente el número de estados en comparación con un equipo informático clásico. A medida que mejora la calidad de los cúbits, los QC se acercan cada vez más a una verdadera escalada exponencial del número de estados representados.
- **Entrelazamiento**: el entrelazamiento es un enlace cuántico entre cúbits. Los cúbits entrelazados generan los mismos resultados al ejecutar el mismo algoritmo cuántico en ellos, sin importar dónde se encuentren, incluso si los cúbits están al otro lado del mundo. Por lo tanto, si ejecuta un algoritmo determinado en cúbits entrelazados que se encuentran en Bangalore (India) y Los Ángeles (Estados Unidos), los cúbits entrelazados en esas ubicaciones ofrecen el mismo resultado. Se desconoce el mecanismo exacto por el cual funciona el entrelazamiento cuántico.

Hay tres tipos de ordenadores cuánticos:

- **Quantum Annealers**: están disponibles hoy. Son los ordenadores cuánticos menos potentes con los casos de uso más limitados. Sin embargo, los atacantes pueden usarlos para factorizar grandes números utilizando algoritmos cuánticos, que es la forma de romper el cifrado asimétrico.
- **Simuladores cuánticos analógicos**: estos resuelven problemas de física que están más allá de la capacidad de las ordenadores clásicos, como la química cuántica, las ciencias de los materiales, los problemas de optimización, la factorización de grandes números, el muestreo y la dinámica cuántica.
- **Ordenador cuántico universal**: Estos son los QC más difíciles de construir porque requieren muchos cúbits físicos. Resuelven la gama más amplia de casos de uso y varias empresas apuntan a finales de esta década para comercializarlos. Cuando se desarrollen, estos son los equipos que serán CRQC.

Los ordenadores cuánticos crean un espacio multidimensional compuesto por muchos cúbits entrelazados en los que resolver problemas complejos. Por ejemplo, los ordenadores clásicos toman cada elemento de una base de datos, lo procesan y luego lo combinan con otros elementos después de procesar todos los elementos. Los ordenadores cuánticos crean un algoritmo que resuelve cada estado y resultado que está buscando. Pasan toda la base de datos a través del algoritmo simultáneamente, analizando los datos para cada resultado simultáneamente. Esto hace que los QC sean potencialmente millones de veces más rápidos que los ordenadores clásicos y es una de las razones por las que son excelentes para resolver problemas matemáticos complejos, como romper el cifrado.

¿Cómo afecta la amenaza cuántica a mi red?

El enorme aumento de la potencia de procesamiento y la velocidad de los ordenadores cuánticos amenaza con romper los métodos clásicos de cifrado de datos, lo que podría comprometer su infraestructura de clave pública (PKI).

La amenaza más inmediata son los ataques Harvest Now, Decrypt Later que roban sus datos cifrados con la intención de utilizar un CRQC para descifrarlos en el futuro. Una vez que los atacantes roban sus datos y el material de clave clásico, no hay forma de evitar que descifren los datos en el futuro mediante el uso de un CRQC. Si los datos robados siguen siendo válidos en ese momento, estos se verán comprometidos.

El cifrado asimétrico clásico se basa en números primos y se basa en la dificultad de factorizar números complejos para derivar esos números primos. Un algoritmo cuántico llamado Algoritmo de Shor puede factorizar números complejos y resolver problemas de logaritmos discretos. El algoritmo de Shor amenaza la seguridad de PKI, que se basa en dos números primos muy grandes para producir la clave. Sin embargo, el algoritmo de Shor no puede romper la seguridad de PKI en menos de millones de años usando un ordenador clásico. Sin los CRQC, el algoritmo de Shor no supone una amenaza. Sin embargo, dada la potencia de procesamiento de un CRQC, el algoritmo de Shor puede factorizar números complejos y descifrar el cifrado asimétrico clásico (como el material de intercambio de claves necesario para descifrar datos) en segundos o menos. Es por eso que los ataques Harvest Now, Decrypt Later son una amenaza inmediata.

Las consecuencias de romper el cifrado clásico incluyen comprometer la seguridad de las criptografías PKI clásicas que se consideraban seguras, como Diffie-Hellman (DH), Elliptic Curve Cryptography (ECC) y Elliptic Curve Diffie-Hellman (ECDH). El intercambio de claves corre el mayor riesgo y es por eso que debe configurar las VPN de tipo IKEv2 postcuántica para proteger el intercambio de claves.

Los certificados son la base de cómo dos puntos de conexión establecen confianza. Sin embargo, los CRQC también pueden comprometer RSA, que se utiliza para crear y proteger certificados digitales. Esto significa que los atacantes pueden robar o hacerse pasar por firmas digitales con un CRQC, por lo que el servidor al que cree que se está conectando podría ser en realidad el servidor de un atacante. La capacidad de hacer esto podría llegar tan pronto como en la próxima década.

Además, la gran potencia de procesamiento de fuerza bruta de los QC significa que el cifrado simétrico tampoco es seguro. Algoritmo de Grover es un algoritmo de búsqueda cuántico no estructurado, acelerado cuadráticamente, que encuentra la entrada única que produce un valor de salida determinado. El algoritmo de Grover se centra en la criptografía simétrica y las funciones hash. Básicamente, reduce a la mitad la fuerza criptográfica de los algoritmos AES, por lo que si utiliza el cifrado AES de 128 bits, el algoritmo de Grover lo reduce a la fuerza criptográfica del cifrado de 64 bits. Debido a que los ordenadores clásicos no tienen suficiente potencia de procesamiento, no pueden usar el algoritmo de Grover para romper el cifrado simétrico. Sin embargo, utilizando un ordenador cuántico, el algoritmo de Grover puede romper el cifrado AES de 128 bits.

Debido a la vulnerabilidad del cifrado AES de 128 bits frente al algoritmo de Grover, utilice el cifrado AES de 256 bits, que el algoritmo de Grover no podrá romper en un futuro cercano o a medio plazo.

Para ayudar a proteger las funciones hash, utilice SHA-384 como mínimo.

Las criptografías poscuánticas (PQC) están disponibles hoy en día y la mayoría de las personas expertas en seguridad pueden descargar y configurar PQC que no se pueden descifrar. Si permite PQC no autorizados en su red, un actor malintencionado interno podría introducir PQC en su red. Si eso sucede, no tendrá visibilidad del tráfico que utiliza un PQC ni de las amenazas en ese tráfico. Utilice las funciones de descifrado para detectar las PQC no autorizadas en su red y bloquear automáticamente el tráfico que utilizan dichas PQC.

Qué hacer ahora para mitigar los ataques de recopilación

Tome estas medidas ahora para resistir los ataques poscuánticos de Harvest Now, Decrypt Later. Revise sus conexiones VPN y refuércelas:

- Siga RFC 6379 para los *Conjuntos criptográficos Suite B para IPsec* para actualizar sus conexiones VPN a conjuntos de cifrado difíciles. Utilice Suite-B-GCM-256 y evite algoritmos AES de 128 bits más débiles, que son vulnerables al algoritmo de Grover.

- Actualice su CA a claves de tamaño RSA 4K para mitigar los ataques de fuerza bruta que pueden romper claves más pequeñas y migre su autenticación de certificado VPN a nuevos certificados.
- Actualice a tamaños de hash SHA de bits más altos como SHA-384 y SHA-512. Deje de usar hashes débiles como MD5 y SHA-1.
- Implemente RFC 8784 y/o RFC 9242 y RFC 9370 para crear VPN postcuánticas que resistan ataques cuánticos.

Además, revise sus conexiones SSL/TLS y refuércelas:

- Actualice las conexiones SSL/TLS a conjuntos de cifrado resistentes; use TLSv1.3 con cifrados de Perfect Forward Secrecy (PFS).
- Sesiones SSL/TLS de túnel en sesiones VPN endurecidas de cliente a servidor. Utilice una aplicación de escritorio postcuántica para soportar Proxy inverso.

Cómo RFC 8784 resiste las amenazas de computación cuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

El estándar RFC 8784, *Mezclar claves compartidas en protocolo de intercambio de claves de Internet versión 2 (IKEv2) para seguridad postcuántica*, le permite crear redes VPN IKEv2 que son resistentes a los ataques basados en ordenadores cuánticos (QC) y criptografías postcuánticas (PQC) en la actualidad.

La esencia de RFC 8784 es el intercambio estático de claves precompartidas postcuánticas (PPK PQ) fuera de banda, por separado del intercambio de claves IKE, y mezclar el material de la PPK PQ fuera de banda con el material de clave Diffie-Hellman (DH) clásico que se transmite en banda durante el intercambio de claves IKEv2. Esto mejora el intercambio de claves de dos maneras:

- Una clave DH y variantes de claves DH se basan en la dificultad de resolver el problema del registro discreto, como por ejemplo resolver para los números primos muy grandes en los que se basa DH. Sin embargo, con la llegada de los ordenadores cuánticos criptográficamente relevantes (CRQC), las claves DH se vuelven vulnerables a los ataques basados en el algoritmo de Shor. La implementación de RFC 8784 mejora la fuerza criptográfica de la clave porque la clave mixta ya no se basa únicamente en la dificultad de resolver el problema del registro discreto (por ejemplo, resolver números primos muy grandes), por lo que la clave mixta no es vulnerable al algoritmo de Shor
- Un fisgón, o desconocido, no puede recopilar todo el material clave para descifrarlo más tarde. La porción DH clásica de la clave se envía en el intercambio de claves entre pares de IKE, pero el PPK PQ que los pares de IKE mezclan con el material de clave DH nunca se transmite durante el intercambio de claves, o en la VPN después de que se haya establecido, por lo que incluso con la porción DH del material de clave, los atacantes no pueden descifrar los datos que atraviesan la VPN.

Los pares de IKEv2 saben qué PPK PQ usar en función de un Key ID. Cada PPK PQ consta de dos elementos, una KeyID y un secreto precompartido. El secreto precompartido es el material clave que comparte con el compañero de IKEv2 fuera de banda. Nunca se transmite en banda con el material de clave DH o con los datos después de establecer la VPN. En su lugar, el administrador de un par IKEv2 crea manualmente el secreto estático precompartido y lo comunica de forma segura, por ejemplo, por correo electrónico seguro o enviado desde Panorama, al administrador del otro par IKEv2. Cada administrador programa el secreto precompartido en su par, por lo que el secreto nunca se revela en la conexión IKE.

El ID de clave, que se transmite en banda durante el intercambio de claves, identifica el secreto precompartido en el par IKEv2. El par IKEv2 utiliza el ID de clave para buscar el secreto precompartido y lo mezcla con el material de clave DH para crear nuevo material de clave que no se basa en números primos y no se puede robar escuchando la comunicación.

Ambos pares IKEv2 deben usar exactamente el mismo ID de clave (KeyID) y secreto PPK PQ precompartido. Si los identificadores de clave y sus secretos precompartidos asociados no coinciden, la conexión se cancela. Si configura más de una PPK PQ, ambos pares de IKEv2 deben tener exactamente el mismo conjunto de identificadores de clave activos y secretos precompartidos. (Palo Alto Networks le permite configurar hasta diez PPK PQ activas, pero algunos proveedores permiten tan solo una PPK PQ, por lo que es importante entender las capacidades del par.

Este método basado en estándares proporciona una manera fácil de evitar que los atacantes escuchen la conexión e intercepten las claves, lo que permitiría a los atacantes descifrar los datos enviados en la VPN después de su establecimiento, al tiempo que garantiza la interoperabilidad con otros dispositivos que se adhieren al estándar. Los beneficios de RFC 8784 incluyen:

- Estándar aprobado con soporte para múltiples proveedores.
- No consume recursos de red adicionales y prácticamente no añade latencia.
- Compatible con versiones anteriores, por lo que puede usarlo en redes donde no todos los pares admiten IKEv2 y donde no controla todos los pares.
- La clave ya no se basa en primos y por lo tanto no es vulnerable al algoritmo de Shor.
- PPK PQ no se transmite, por lo que no se puede utilizar para descifrar los datos recopilados.
- Recomendado por agencias gubernamentales, incluidos NIAP, NSA, Oficina Federal de Seguridad de la Información de Alemania y muchos más en todo el mundo. Además, la creación de un secreto fuerte y aleatorio de 32 bytes o mayor longitud cumple con el nivel de seguridad NIST Categoría 5. Asegúrese de que el secreto es fuerte y aleatorio, no sigue un patrón y no está sujeto a ataques de diccionario.
- Puede crear capas de RFC 8784 con futuras capacidades basadas en estándares, como claves híbridas PQC.

Esto se suma a una adopción más rápida porque hay pocos cambios que hacer y no hay peligro de que se caigan las conexiones debido a la incompatibilidad. Sin embargo, RFC 8784 tiene algunas desventajas:

- La configuración manual de las PPK PQ estáticas no se escala bien en muchos sitios, aunque enviar las PPK PQ de Panorama a cortafuegos gestionados puede ayudar a mitigar el escalado.
- Todos los administradores de IKEv2 con los que se comparten las PPK PQ deben guardarlas de forma segura. Eso incluye no solo a los administradores internos de su empresa, sino también a los administradores de socios, proveedores y otros administradores externos con los que necesita relacionarse. El riesgo proviene de administradores que están escribiendo la PPK PQ y lo pierdan o lo roben o comprometan.
- Confiar en los seres humanos para crear secretos aleatorios largos y fuertes que resistan los ataques de diccionario y otros ataques podría ser todo un desafío. La implementación de Palo Alto Networks le permite generar automáticamente secretos largos, fuertes y hexadecimales en lugar de tener que crearlos usted mismo.

Las VPN IKEv2 basadas en RFC 8784 son el primer paso recomendado para una solución frente a los PQC y las amenazas postcuánticas. Después de que NIST estandarice los primeros PQC, otros métodos que pueden funcionar con RFC 8784 mejorarán la resistencia a amenazas cuánticas, como RFC 9242 y RFC 9370.

Cómo las RFC 9242 y RFC 9370 resisten las amenazas de la computación cuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.2 o posterior.

El estándar RFC 9242, *Intercambio de claves intermedio en el Protocolo de intercambio de claves de Internet 2 (IKEv2)*, permite que IKEv2 transfiera grandes cantidades de datos en el establecimiento de la Asociación de seguridad (SA) IKEv2 para admitir múltiples intercambios de claves PQC con tamaños de clave más grandes. El estándar RFC 9370, *Intercambios de claves múltiples en el Protocolo de intercambio de claves de Internet 2 (IKEv2)*, permite que se realicen múltiples intercambios de claves mientras se calcula un secreto compartido durante la configuración de SA.

En conjunto, estos dos estándares RFC le dan a IKEv2 la capacidad de crear claves híbridas utilizando mecanismos de intercambio de claves (KEM) clásicos y PQC para mitigar un ataque cuántico utilizando el algoritmo de Shor. Los nuevos PQC se basan en tecnologías matemáticas diferentes que no son vulnerables a los ataques clásicos o cuánticos conocidos, y estas incluyen:

- Enrejado
- Basado en código
- Basado en hash
- Clave simétrica
- Basado en isogenia
- Multivariable

El estándar RFC 9370 permite siete rondas de intercambio de claves adicionales, y estas pueden ser KEM clásicas o PQC, como ML-KEM, BIKE, HQC, Classic McEliese y otras, además del intercambio de claves predeterminado IKEv2 para un total de ocho rondas.

Para romper la clave híbrida, todas las tecnologías KEM utilizadas para crear la clave de cifrado deben caer ante una vulnerabilidad y verse comprometidas. Por ejemplo, para crear una clave híbrida que sea resistente tanto a las vulnerabilidades conocidas actuales como a las amenazas futuras de las ordenadores cuánticos (QC), las prácticas recomendadas recomiendan utilizar tanto claves clásicas como una o más claves PQC KEM que utilicen diferentes tecnologías matemáticas.

- Ronda KEM predeterminada: Grupo 21 de Diffie-Hellman (DH)
- Intercambio de claves adicional, ronda 1: ML-KEM-768 (CRYSTALS-Kyber-786)
- Intercambio de claves adicional, ronda 2: BIKE L3

En el ejemplo anterior, el clásico Grupo 21 de DH proporciona protección frente a los ataques precuánticos actuales. Al agregar dos rondas PQC KEM adicionales con ML-KEM-768 (en red) y BIKE-L3 (basada en código), una después de la otra, se crea una clave de cifrado basada en tres tecnologías KEM y brinda protección para futuros ataques utilizando el algoritmo de Shor. La adición de al menos dos PQC al intercambio de claves DH proporciona un mayor nivel de protección frente a un solo fallo de KEM y puede ayudar a resistir ataques cuánticos durante más tiempo. Además, el uso de KEM basados en diferentes

tipos de matemáticas puede proteger contra futuras vulnerabilidades, contra un tipo específico de PQC, como todos los PQC basados en tecnología de red.

La transición al mundo poscuántico, donde las PQC son el único mecanismo de intercambio de claves, llevará muchos años, ya que el sector necesita tiempo para validar los nuevos PQC y ganar confianza en sus capacidades de seguridad. Durante el período de transición, las claves híbridas basadas en RFC 9242 y RFC 9370 serán el estándar.

El proceso de normalización para aprobar nuevos PQC se realizará en fases, y el NIST aprobará grupos de PQC para cada ronda de aprobación. Dado que cada PQC tiene compensaciones en términos de rendimiento y seguridad, es necesario comprender cómo funciona cada uno para determinar qué tecnología es la más adecuada para los diferentes casos de uso de seguridad. Por ejemplo, Classic McEliece ha demostrado ser un PQC muy seguro a lo largo del tiempo, pero la desventaja de su alta seguridad son los grandes tamaños de clave que utiliza, lo que puede limitar el uso de Classic McEliece en las comunicaciones VPN y TLS.

Los gobiernos del mundo están recomendando un nivel de seguridad L3 o superior para brindar seguridad sólida y resistencia a futuros ataques informáticos cuánticos.

Durante el período de transición del cifrado clásico al cifrado poscuántico, se requerirá agilidad criptográfica para permitir el reemplazo rápido de cualquier PQC comprometido. La solución KEM postcuántica RFC 9242 y RFC 9370 de Palo Alto Networks proporciona un amplio conjunto de PQC para lograr agilidad criptográfica desde el principio, lo que permite a los clientes seleccionar y eliminar cualquier PQC compatible de la negociación de claves IKEv2 rápidamente, sin ninguna actualización de software o cambios en la red existente.

Los siguientes PQC son compatibles con PAN-OS IKEv2:

- ML-KEM (Kiber) 512, 768, 1024
- BIKE L1, L3, L5
- FrodoKEM 640-aes, 640-shake, 976-aes, 976-shake, 1344-aes, 1344-shake
- HQC 128, 192, 256
- NTRU-Prime sntrup761
- McEliece clásico 348864, 348864f

Los beneficios de RFC 9242 y RFC 9370 incluyen:

- Estándares aprobados con soporte multiproveedor.
- Alta escalabilidad con intercambio de claves dinámico en lugar de las PPK estáticas del RFC 8784.
- Soporte para una amplia gama de PQC KEM.
- La compatibilidad con versiones anteriores de IKEv2 permite una solución alternativa si el par no puede soportar las RFC.
- Las claves híbridas son más resistentes a algoritmo de Shor ya que se pueden utilizar diferentes tecnologías PQC juntas.
- Se pueden combinar con RFC 8784 para lograr defensa cuántica en profundidad y agilidad criptográfica.

Las desventajas de RFC 9242 y RFC 9370 incluyen:

- Es posible que las primeras listas estandarizadas de PQC no proporcionen suficientes PQC para lograr agilidad criptográfica al comienzo de la transición postcuántica.
- Es posible que se necesiten muchos años para que el nuevo PQC sea totalmente examinado y obtenga la confianza del sector.
- Varios KEM pueden añadir sobrecarga adicional y ralentizar el proceso de emparejamiento IKEv2.
- Los nuevos PQC KEM pueden provocar fragmentación debido a que los tamaños de clave y las cargas útiles de datos son mayores.
- No todos los dispositivos pueden actualizarse para admitir PQC KEM.
- El riesgo de ataques de denegación de servicio (DoS) puede aumentar con el intercambio de clave extendido durante IKE_INTERMEDIATE, debido al aumento de recursos necesarios antes de que el iniciador sea autenticado.
- Las claves híbridas están diseñadas para proteger frente a ataques de recopilación de datos donde la información cifrada se guarda y se descifra con un ordenador cuántico criptográficamente relevante (CRQC) en una fecha posterior. Los ataques que utilizan un ordenador cuántico en un ataque activo no se resuelven completamente con claves híbridas por las siguientes razones:
  - La autenticación todavía se realiza mediante métodos clásicos, ya sea algoritmos de clave precompartida o de firma digital. Las claves precompartidas deben ser largas y complejas para ser seguras después de la era cuántica, pero no son escalables. La autenticación con firmas digitales debe realizarse con una firma digital postcuántica.
  - Los PQC están diseñados para brindar resistencia a los ataques de recopilación y hasta que los CRQC estén disponibles, atacar la autenticidad de una conexión no importa porque no hay posibilidades de explotación ya que estas solo ocurren en el momento de la conexión.

Se recomienda utilizar VPN IKEv2 basadas en RFC 9242 y RFC 9370 para proteger las conexiones VPN frente a amenazas postcuánticas mediante el uso de claves híbridas basadas en múltiples tecnologías KEM. Con un conjunto amplio de PQC, se puede lograr agilidad criptográfica para protegerse contra los PQC comprometidos durante la transición a un mundo poscuántico.

Compatibilidad con funciones postcuánticas

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

El soporte para funciones y capacidades postcuánticas incluye RFC, alta disponibilidad y consideraciones de actualizaciones y cambios a versiones anteriores. Estamos en una etapa temprana del desarrollo de estándares y características postcuánticas, mientras naciones, proveedores y empresas luchan por encontrar la manera de defender sus datos de ataques postcuánticos. A medida que los estándares progresen y las plataformas de Palo Alto Networks los admitan, este tema se actualizará para indicar dichas compatibilidades.

- RFC compatibles e interoperabilidad
- Compatibilidad con HA
- Consideraciones sobre el cambio a versiones anteriores/posteriores

RFC compatibles e interoperabilidad

Los dispositivos de Palo Alto Networks son totalmente compatibles con los estándares abiertos RFC 8784, RFC 9242y RFC 9370 .

Los dispositivos de Palo Alto Networks interoperan con otros dispositivos que admiten los mismos estándares, aunque las implementaciones de algunos proveedores pueden diferir según la interpretación de los RFC. Por ejemplo, algunos proveedores podrían no ofrecer la posibilidad de configurar tantas claves precompartidas postcuánticas (PPK PQ) con RFC 8784 o podrían no admitir el amplio conjunto de PQC que Palo Alto Networks admite con RFC 9370.

Compatibilidad con HA

La alta disponibilidad (HA) para las VPN IKE es la misma que antes de la introducción de las funciones postcuánticas: Los túneles VPN continúan ejecutándose después de una conmutación por error, y los pares IKE se vuelven a sincronizar y actualizan las claves IKE tras una conmutación por error.

Consideraciones sobre el cambio a versiones anteriores/posteriores

Cuando se actualiza desde una versión que no admite las VPN de tipo IKEv2 postcuántica, la plataforma proporciona compatibilidad para las características y capacidades post-cuánticas.

Al degradar a una versión que admita las funciones postcuánticas que configuró, la configuración no se modifica y la seguridad VPN IKEv2 postcuántica permanece vigente.

Al cambiar a una versión anterior que no admite las funciones de VPN IKEv2 postcuánticas:

- Si no configuró las VPN de tipo IKEv2 postcuántica, el cambio a una versión anterior continúa de manera habitual y se eliminan las opciones de configuración de seguridad de la VPN IKEv2 post-cuánticas.
- Si configuró las VPN de tipo IKEv2 postcuántica, el cambio a una versión anterior se bloquea porque la versión degradada no admite las opciones de configuración post-cuánticas. Aparece un mensaje de advertencia cuando se bloquea la degradación que le notifica que debe eliminar la configuración

VPN IKEv2 posterior a la cuántica y seleccionar el cifrado que desea usar para la VPN después de la degradación.

Después de eliminar la configuración VPN IKEv2 postcuántica y seleccionar el cifrado, puede continuar con el cambio a la versión anterior.

Los archivos de logs conservan los registros postcuánticos después del cambio a la versión anterior, o degradación.

Planificación y preparación de la migración postcuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

Actualizar su red para resistir ataques postcuánticos requiere una planificación y preparación significativas porque, además de actualizar las redes VPN, necesita realizar la transición de conjuntos criptográficos clásicos a conjuntos criptográficos postcuánticos. Y no es solo un cambio de red y cortafuegos, sino también endpoints, aplicaciones, aplicaciones cliente, etc.; una migración completa de extremo a extremo. Es una gran inversión en tiempo, investigación y recursos. La magnitud de la inversión depende de su negocio y de su red. Sin embargo, el coste de la inversión es menor en comparación con el coste de un ataque que roba sus activos más valiosos, como datos financieros, código, datos de PII y otros datos potencialmente duraderos que son vulnerables a un ataque de Harvest Now, Decrypt Later.

Además, las agencias reguladoras, las agencias de seguridad nacional como la NSA, los gobiernos y las autoridades de normas como el NIST en todo el mundo requieren o requerirán que las agencias gubernamentales y también algunos sectores empresariales (incluidos potencialmente el transporte y la infraestructura crítica) se preparen y defiendan frente a las amenazas poscuánticas. Preparar la transición a un mundo postcuántico no es cuestión de si lo debería hacer, es cuestión de cuándo lo hará.

La pregunta es, *¿cuándo debería empezar la migración*?

El momento en que debe iniciar la migración depende de los requisitos de sus activos digitales, especialmente cuánto tiempo necesita proteger su privacidad, debido a los ataques Harvest Now, Decrypt Later, que registran datos cifrados, incluido el material de clave transmitido en el protocolo de acceso entre pares IKE y TLS, con la intención de descifrar los datos capturados cuando estén disponibles los ordenadores cuánticos (CRQC) criptográficamente relevantes. La pregunta clave es, ¿cuánto tiempo necesitan estar seguros sus datos? Si un atacante ya ha capturado datos confidenciales y esos datos siguen siendo válidos cuando los CRQC entran en juego, el atacante podrá descifrar los datos robados y actuar sobre su contenido. Los CRQC podrían estar disponibles en el próximo decenio.

Si su empresa es un objetivo potencial para los ataques de recopilación, cada día que pasa sin tomar medidas corre el riesgo de dar a los atacantes más información para descifrar más tarde. Cuanto antes tome medidas, antes evitará que los atacantes puedan descifrar en el futuro los datos recopilados ahora.

Históricamente, la mayoría de los esfuerzos anteriores para reemplazar los protocolos criptográficos, como la transición del cifrado 3DES a AES o el paso de las funciones hash SHA-1 a SHA-2, han tomado de 5 a 20 años después del desarrollo de los nuevos estándares. Eso incluye tiempo para investigar los nuevos protocolos en el mundo real. Después de que el NIST estandarice las criptografías postcuánticas (PQC), a pesar de que las PQC se han sometido a pruebas rigurosas, probablemente harán falta de 5 a 10 años de experiencia en el mundo real e intentos de descifrar las PQC antes de que podamos tener confianza en que las nuevas PQC sean realmente sólidas.

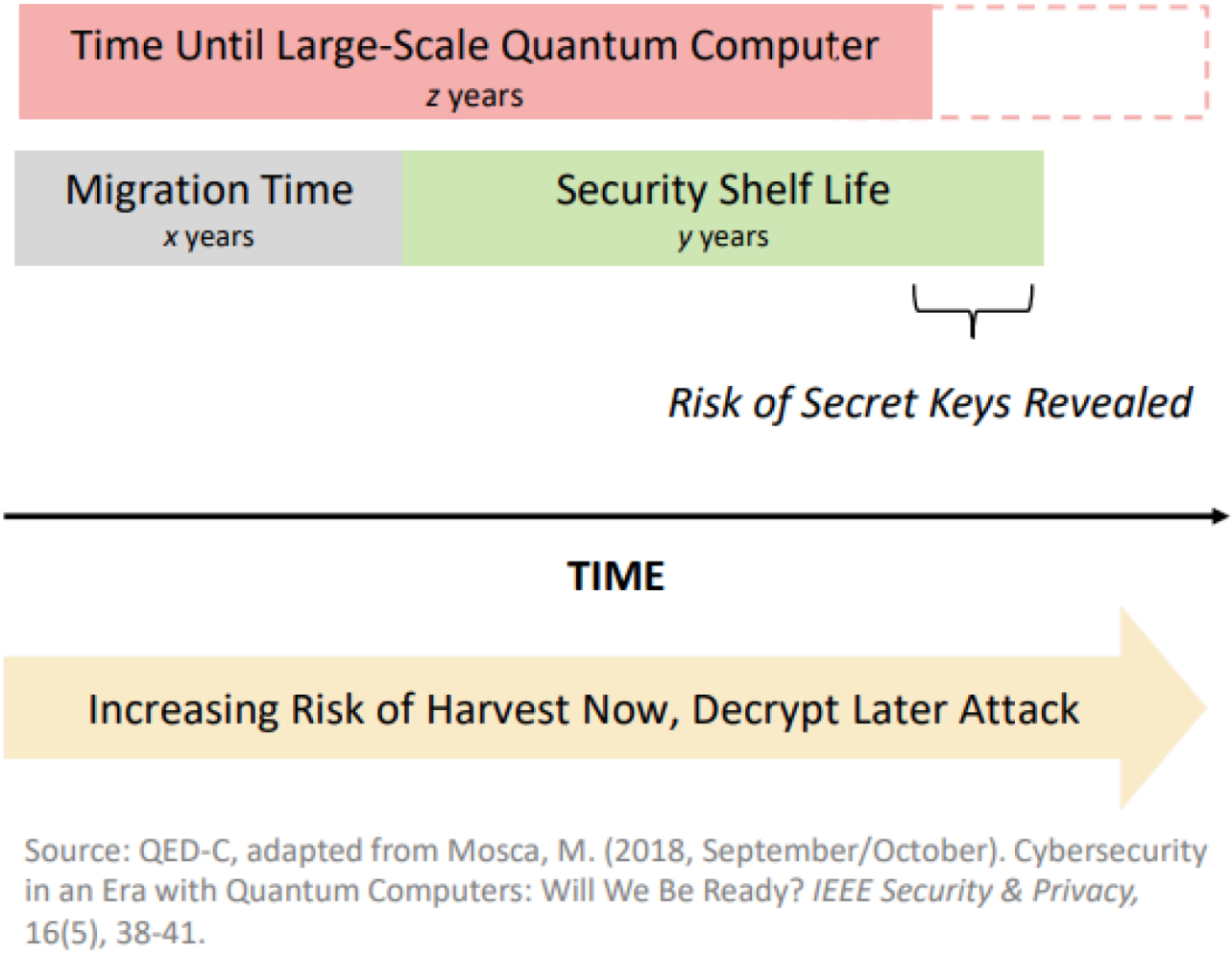
Los PQC son sustitutos de los algoritmos criptográficos clásicos y proporcionan resistencia cuántica para el intercambio de claves, el cifrado y las firmas digitales.

Para salvaguardar la transición del cifrado clásico a los nuevos PQC, la industria está adoptando claves híbridas. Las claves híbridas proporcionan una capa adicional de seguridad al crear la clave de cifrado con múltiples tecnologías de mecanismo de intercambio de claves (KEM). La práctica recomendada es usar un KEM clásico fuerte, como el Grupo 21 de Diffie-Hellman, y uno o más PQC. Si uno de los KEM PQC utilizados para crear la clave cae en una vulnerabilidad, los otros KEM aún protegen la clave. Las llaves híbridas son la mejor manera de avanzar hasta que los nuevos PQC obtengan suficiente experiencia en el mundo real para que la industria pueda confiar en su fuerza de seguridad.

Y los ataques de Harvest Now, Decrypt Later no son la única amenaza postcuántica. Los malos actores internos con conocimientos técnicos pueden descargar PQC de código abierto y mostrar sus propios servidores PQC o complementos de navegador en su red si no bloquea proactivamente los PQC no autorizados en su red.

A principios de la década de 2030, es probable que los datos protegidos con la criptografía clásica de hoy no estén protegidos de ataques postcuánticos. Por lo tanto, es importante entender cuánto tiempo necesita tener segura su información y estimar cuánto tiempo tardará en preparar y ejecutar su plan postcuántico. Cuanto antes comience, más fácil será mantener la calidad alta y los costes predecibles, además de evitar las prisas a medida que avanza en el proceso y aumentan las amenazas postcuánticas.

Una manera de pensar en la rapidez con la que empezar es utilizar un modelo Mosca, que presenta una línea de tiempo simple en la que se conectan sus estimaciones de tiempo para que pueda entender la urgencia de tomar medidas.



Source: QED-C, adapted from Mosca, M. (2018, September/October). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy,* 16(5), 38-41.

Este modelo de Mosca muestra cómo estimar la línea de tiempo hasta la vulnerabilidad postcuántica de sus activos y le ayuda a hacerse una idea de cuándo debería comenzar el viaje hacia la preparación postcuántica. El modelo compara su estimación del tiempo que tarda en migrar a la preparación postcuántica (*x*, que probablemente sea de al menos cinco años) más su estimación de la vida útil de sus datos (*y*, que es el período de tiempo desde que logra la preparación postcuántica hasta el momento en que la exposición de los datos ya no ponen en riesgo los datos) con el momento en que es probable que los CRQC estén disponibles (*z*).

La diferencia entre (*x* + *y*) y *z* muestra el tiempo que sus datos de larga duración corren el riesgo de exposición si se han recopilado o cuánto tiempo tiene de colchón antes de que sus datos de larga duración estén en riesgo. Esto le ayuda a entender cuánto tiempo tiene para empezar o si y va con retraso. Si (*x* + *y*) es mayor que *z*, la diferencia entre esas líneas de tiempo es el tiempo en que sus datos podrían estar expuestos si los atacantes los recopilaron en un ataque de Harvest Now, Decrypt Later que se muestra en la ilustración anterior como *Riesgo de claves secretas reveladas*.

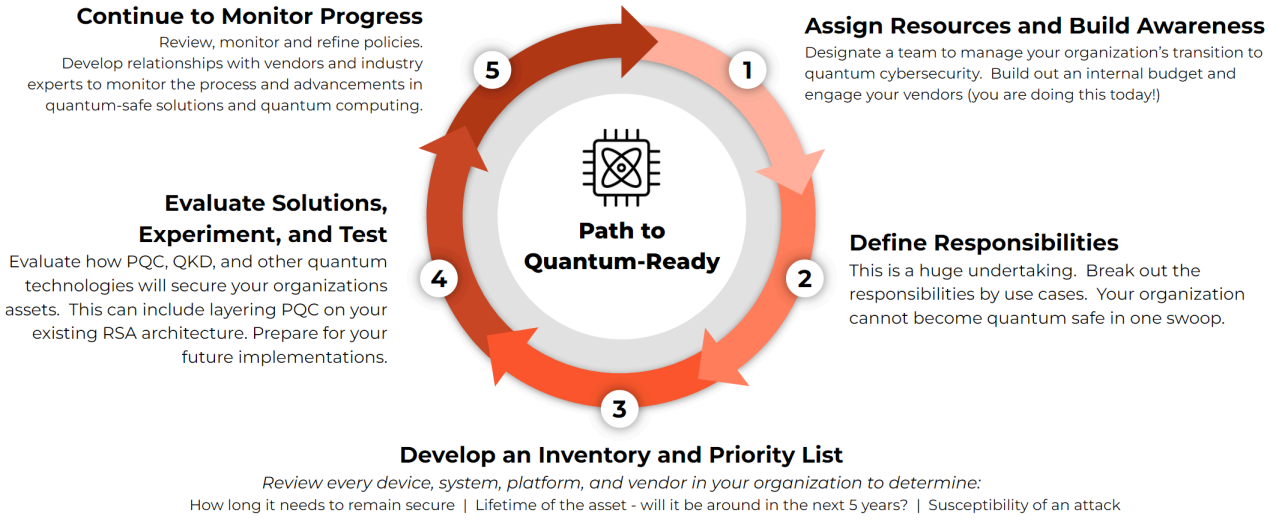
A medida que comienza la planificación de la transición, hay varias cosas que puede hacer de inmediato para fortalecer sus conexiones VPN existentes:

- Siga RFC 6379 para los *Conjuntos criptográficos Suite B para IPsec* para actualizar sus conexiones VPN a conjuntos de cifrado difíciles. Utilice Suite-B-GCM-256 y evite algoritmos AES de 128 bits más débiles, que son vulnerables al algoritmo de Grover.
- Actualice su CA a claves de tamaño RSA 4K para mitigar los ataques de fuerza bruta que pueden romper claves más pequeñas y migre su autenticación de certificado VPN a nuevos certificados.
- Actualice a tamaños de hash SHA de bits más altos como SHA-384 y SHA-512. Deje de usar hashes débiles como MD5 y SHA-1.
- Implemente RFC 8784 y/o RFC 9242 y RFC 9370 para crear VPN postcuánticas que resistan ataques cuánticos.

Además, revise sus conexiones SSL/TLS y refuércelas:

- Actualice las conexiones SSL/TLS a conjuntos de cifrado resistentes; use TLSv1.3 con cifrados de Perfect Forward Secrecy (PFS).
- Sesiones SSL/TLS de túnel en sesiones VPN endurecidas de cliente a servidor. Utilice una aplicación de escritorio postcuántica para soportar Proxy inverso.

Para iniciar la transición, el Consorcio de Desarrollo Económico Cuántico (QED-C) ha desarrollado un modelo para planificar y preparar la transición a la seguridad postcuántica que Palo Alto Networks ha adaptado a un modelo de cinco pasos para ayudarle a evaluar la preparación, el tiempo y los recursos de la migración.



Source: A guide to a quantum-safe organization, QED-C December 2021, July 2022

Las siguientes secciones describen cada paso del viaje hacia la preparación cuántica, para lo cual implementar RFC 8784 para crear VPNs IKEv2 resistentes a la tecnología cuántica es el primer paso:

- Asignar recursos y crear conciencia
- Definir responsabilidades
- Desarrollar un inventario de criptografía y una lista de prioridades
- Evalúe soluciones, experimentos y pruebas
- Continúe para supervisar el progreso

Asignar recursos y crear conciencia

Los objetivos de esta fase de planificación y preparación son identificar al equipo de transición, tener una idea de qué recursos necesita, involucrar a los proveedores para que entiendan sus planes de preparación postcuántica y comenzar a entender el coste que supone.

Las actualizaciones que crean resistencia a los ataques postcuánticos a menudo encajan con el trabajo que su departamento de TI ya está haciendo para modernizar la red.

1. Cree un equipo de gestión de proyectos dedicado a asumir la responsabilidad de desarrollar una estrategia postcuántica y una hoja de ruta de preparación cuántica para gestionar la transición. El equipo es responsable de la planificación de alto nivel. El equipo también identifica quién es responsable de las partes de la red que forman parte de la transición. Comience pronto y dese tiempo suficiente para un enfoque reflexivo y medido que le ayude a garantizar que la calidad siga siendo alta y los costes predecibles.
2. Desarrolle una comprensión de las tecnologías de seguridad cuántica y descubra cómo integrarlas en su entorno. Las VPN de tipo IKEv2 postcuántica (RFC 8784) son el primer paso para crear una red postcuántica segura, lo que puede hacer ahora sin afectar a su red. Además, todas las organizaciones tendrán que reemplazar sus algoritmos asimétricos existentes con los PQC resistentes a la computación cuántica. Para seguir los siguientes pasos, obtenga información sobre los PQC, las claves híbridas y los intercambios de múltiples claves (RFC 9370 y 9242). También aprenda sobre la agilidad criptográfica (usando múltiples PQC para que tenga la capacidad de cambiar fácil y rápidamente entre PQC si

un PQC se ve comprometido), distribución de claves cuánticas (QKD) y generadores de números aleatorios cuánticos (QRNG) para saber si estas medidas de seguridad están justificadas para proteger sus datos.

Investigue las tecnologías cuánticas e involucre a sus proveedores para comprender sus planes de preparación cuántica y cómo afecta eso a su negocio.

3. Involucrar a la comunidad de la empresa y desarrollar una comprensión de los niveles de preparación y conciencia de la Criptografía postcuántica y la tecnología. Crear conciencia en los equipos y líderes de equipo, y ayudarles a entender los cambios potenciales y por qué son necesarios. Por ejemplo, trabajar con los equipos de adquisiciones para incluir requisitos postcuánticos a fin de garantizar que los nuevos equipos y los nuevos programas informáticos sean compatibles con las CCP y estén preparados para el futuro.

   Inicie actividades de descubrimiento criptográfico (es posible que pueda aprovechar la documentación de auditoría) para obtener visibilidad e identificar la dependencia actual de la organización de las firmas digitales y las criptografías que son vulnerables a ataques post-cuánticos, como Diffie-Hellman (DH), criptografía de curva elíptica (ECC), curva elíptica Diffie-Hellman (ECDH), AES-128, cifrado RSA que es menor que 4K, etc.
4. Comience a trabajar en un presupuesto interno. Ajuste el presupuesto a medida que aprende más y formule la mejor solución para su negocio.

Definir responsabilidades

Averigüe quién es responsable de cada parte de la red, incluidas las redes, el cifrado de archivos y datos, las aplicaciones de software, los endpoints, IAM, los servidores de aplicaciones, etc. Asigne responsabilidades a los miembros del equipo en cada área y asegúrese de que entiendan la razón, urgencia y valor de la transición. Las vulnerabilidades postcuánticas afectan a todo el cifrado asimétrico existente. Los miembros del equipo deben entender que descubrir, categorizar y actualizar todo en la red de manera priorizada supondrá un esfuerzo significativo.

Desarrollar un inventario de criptografía y una lista de prioridades

Un inventario de criptografía es una lista completa de todo en su red: cada dispositivo, sistema, código, aplicación, plataforma y proveedor en su red, y la criptografía que cada uno utiliza, suites cibernéticas, versiones utilizadas para TLS, SSH y VPN, gestión de certificados, generación de claves de cifrado, tamaños de clave y almacenamiento de claves, etc. El inventario de criptografía debe ser exhaustivo porque las PQC representan una amenaza para toda la ruta de datos de extremo a extremo, incluidos los endpoints, las aplicaciones y los servidores de todo tipo. Esto significa que debe planificar una migración completa de extremo a extremo.

El inventario de criptografía no solo enumera los componentes, también proporciona información sobre cada componente, además de los componentes en sí y la criptografía que cada uno utiliza. Para cada componente, el inventario incluye quién lo usa, qué datos se almacenan en él, cómo se protegen y cómo se mueven los datos entre componentes. El objetivo es comprender los tipos de cifrado que se utilizan en su red, los datos que el cifrado protege, dónde se almacenan los datos, a dónde van los datos y todo sobre los dispositivos y usuarios involucrados. En resumen, un inventario completo de su criptografía de red y todo lo que afecta.

Sin un inventario de criptografía completo, no puede identificar todos los componentes afectados en su red, evaluar su riesgo o priorizar de manera efectiva qué actualizar primero.

Para crear su inventario de criptografía, investigue y documente el uso de criptografía (la TI y SecOps a menudo pueden ayudar con esto):

- Qué criptografía se utiliza: los cifrados criptográficos y protocolos en uso actual.
- Quién o qué usa cada cifrado y protocolo criptográfico.
- Dónde se utiliza la criptografía: qué datos, servidores, navegadores, VPN, aplicaciones remotas, etc., protege la criptografía. Identifique quién está utilizando los datos, qué partes de la red atraviesa y cómo se protegen de extremo a extremo.
- Clasificar por riesgo para cada elemento de la red.
- Determine la duración requerida de la privacidad de los datos y el final de la vida útil prevista para los datos, para ayudar a medir el riesgo de pérdida de datos por ataques de recopilación.

Incluya proveedores y socios en el inventario de criptografía. Por ejemplo, entreviste a proveedores para entender la criptografía utilizada en sus aplicaciones y cuán fuertes son las claves y cómo se generan. Identifique quién está utilizando los datos y cómo se protegen de extremo a extremo. No deje brechas que los atacantes puedan aprovechar en un ataque postcuántico.

Al crear su inventario de criptografía, es posible que pueda aprovechar el trabajo realizado para auditorías, mejoras de red, Zero Trust, etc.

Desarrollar su inventario de criptografía podría ser la parte más difícil de la transición. La buena noticia es que hacer el inventario genera conciencia que ayuda a las organizaciones a ser más seguras incluso antes de que se materialice una amenaza cuántica, porque el inventario identificará sistemas arcaicos y obsoletos.

Palo Alto Networks proporciona varias herramientas para ayudarle a realizar su inventario de criptografía

- Los logs de descifrado, tráfico y amenazas muestran qué protocolos criptográficos se ejecutan en su red, los dispositivos y usuarios de esos protocolos, etc.
- Las firmas de perfiles de protección frente a vulnerabilidades en la versión de contenido 8692 pueden detectar y alertar sobre el uso de PQC en los logs. Puede configurar perfiles de protección frente a vulnerabilidades para bloquear automáticamente los PQC no autorizados en su red, lo que es una práctica recomendada. (Haga las excepciones necesarias para las pruebas internas de PEN).
- Utilice el descifrado SSL para bloquear automáticamente los cifrados que el cortafuegos no puede descifrar.

Evalúe el riesgo de los elementos en su inventario de criptografía y determine sus opciones de seguridad para que pueda priorizar la migración:

- Comprenda sus datos y aplicaciones:
  - Identifique datos de alta prioridad y alta privacidad.
  - Clasifique los datos en función de la seguridad y el riesgo.
  - Asigne la duración de la privacidad (qué duración tienen los datos, cuánto tiempo serán válidos).
  - Comprenda cómo las aplicaciones protegen sus datos.
  - Sepa quién está utilizando los datos.
- Entienda sus endpoints.
  - ¿Dónde se almacenan los datos y cómo se protegen?
  - ¿Qué servidores alojan y sirven los datos?
  - ¿Qué dispositivos utilizan los usuarios para acceder a los datos?
  - ¿Cómo se protegen los endpoints?

- Entienda su red.
  - ¿Cómo se mueven los datos a través de la red?
  - ¿Qué dispositivos protegen los datos?
  - ¿Está involucrada la nube? ¿Cómo se aseguran los datos en la nube?
  - ¿Dónde están las áreas de red con mayor riesgo?
- Comprenda sus opciones de seguridad y dónde debe aplicar la mitigación postcuántica.
  - ¿Necesita migrar a protocolos más nuevos?
  - ¿Qué PQC debería usar y cuándo? (Preste atención a los estándares de NIST para PQC).
  - ¿Necesitará utilizar claves híbridas para proteger sus datos?
  - ¿Cómo garantizará la criptoagilidad (la capacidad de cambiar entre algoritmos criptográficos rápidamente en caso de que se descubran vulnerabilidades en un PQC).
  - ¿Necesitará usar QRNG o QKD?
  - ¿Cuándo necesita realizar la transición a certificados y autenticación postcuánticos?
  - ¿Las opciones satisfacen sus requisitos de cumplimiento normativo?

Cuando entienda su inventario de criptografía, analice los datos y establezca prioridades de migración basándose en ellos. Al establecer prioridades, tenga en cuenta la vida útil de los datos para defenderse frente a los ataques de recopilación, la ubicación y sensibilidad de los datos y cuán susceptibles son los datos a los ataques. Hoy en día, el intercambio de claves corre el mayor riesgo, por lo que implementar RFC 8784 y/o RFC 9242 y RFC 9370 para crear VPN resistentes a la tecnología cuántica es el primer trabajo.

Para establecer prioridades migratorias:

- Clasifique las tareas según el impacto empresarial. ¿Qué tan crítico es el activo para su negocio? ¿Cuánto tiempo necesitan los datos para ser seguros o privados? ¿Está el activo expuesto a un posible ataque de Harvest Now, Decrypt Later? Compare el valor de capital de los activos en riesgo con el coste estimado de una posible pérdida de datos debido a un ataque postcuántico.
- Migre primero las áreas de alto impacto.
- Defina las acciones correctivas.
- Establezca plazos y políticas de migración.
- Dedique recursos y financie actividades.

Evalúe soluciones, experimentos y pruebas

Con la información de su inventario de criptografía, desarrolle las políticas, planes de migración y planes de prueba para realizar la transición de su red, estar preparado para tecnología postcuántica y proteger sus datos. Incluya proveedores, socios y cualquier otra influencia externa en la seguridad de su red. Para desarrollar políticas de soluciones y planes de migración:

- Identifique los activos que necesita actualizar a PQC.

  Identifique qué tecnologías se requieren para cada nivel de prioridad y determine cómo encajan en la estrategia de migración.
- Cree un plan de transición que identifique los algoritmos más adecuados para proteger sus activos ahora y de cara al futuro, cuando reemplace o aumente los algoritmos clásicos con PQC.

- Desarrolle políticas de ciclo de vida de claves para reflejar el riesgo de claves de cifrado asimétricas y simétricas, especialmente para datos de larga duración que corren el riesgo de sufrir ataques de Harvest Now, Decrypt Later.
- Incluya la implementación de criptoagilidad en sus políticas y planes. La criptoagilidad garantiza que si un algoritmo (clásico o PQC) se ve comprometido, estará listo para pasar rápida y fácilmente a un algoritmo seguro.

Entienda que es una transición reflexiva, no una acción de destruir y reemplazar. Es probable que tenga que adoptar un enfoque híbrido y crear capas de PQC con algoritmos criptográficos clásicos para mejorar la seguridad antes de completar una transición completa a PQC.

Para probar planes y políticas, configure laboratorios de prueba de concepto para que pueda:

- Probar minuciosamente todos los componentes de PQC y la interoperabilidad entre dispositivos y aplicaciones.
- Comprender las diferencias de rendimiento y capacidad entre algoritmos clásicos y PQC. Los PQC tienen tamaños de clave y tamaños de firma digital más grandes que las criptografías clásicas, lo que resulta en tamaños de archivo cifrados más grandes que también podrían afectar la latencia.

  Pruebe la interoperabilidad PQC entre componentes y trate de maximizar la resistencia cuántica de extremo a extremo, no solo dentro de la organización, sino también entre partes externas. Identifique los algoritmos que tienen más sentido para cada caso de uso y cree un plan de transición para reemplazar las criptografías clásicas con PQC.
- Pruebe de extremo a extremo e incluya socios, proveedores y otras partes externas cuya preparación postcuántica podría afectar a su red. Algunos sistemas podrían necesitar actualizaciones para tener un rendimiento postcuántico aceptable.
- Identifique los componentes y activos incompatibles que necesita actualizar.

La experimentación también es otra forma de crear conciencia en su organización, al tiempo que responde preguntas y proporciona información sobre lo fácil o difícil que puede ser la transición. Busque experiencia externa si no tiene experiencia interna o no puede desarrollarla en un plazo razonable.

Continúe para supervisar el progreso

Supervise y evalúe de forma continua el progreso hacia un entorno resistente a la informática cuántica para ayudar a garantizar que la transición se mantenga en el plazo previsto y mitigar los riesgos de ataques de recopilación, o cosecha. Haga ajustes al plan y al personal involucrado según sea necesario. Además, trabaje con expertos para asegurarse de cubrir todas las bases y no dejar brechas que un atacante pueda explotar en un futuro ataque cuántico.

Prácticas recomendadas para resistir ataques postcuánticos

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

Hay muchas prácticas recomendadas que puede implementar ahora para defenderse de los ataques postcuánticos llevados a cabo por ordenadores cuánticos, incluida la defensa frente a ataques de Harvest Now, Decrypt Later. Los ataques Harvest Now, Decrypt Later capturan datos cifrados y material de intercambio de claves con la intención de usar ordenadores cuánticos criptográficamente relevantes (CRQC) para descifrar el material más tarde acelerando el algoritmo de Shor, que factoriza el material de la clave para encontrar los números primos grandes en los que se basa la clave de cifrado.

Estas prácticas recomendadas abarcan:

- Prácticas recomendadas para la Planificación de la transición postcuántica
- Prácticas recomendadas para la criptografía
- Prácticas recomendadas para la configuración de VPN

Prácticas recomendadas para la Planificación de la transición postcuántica

La transición de la criptografía clásica a la criptografía postcuántica puede tardar cinco años o incluso más. La planificación por sí sola puede tardar varios años. Cuente con la mejor ventaja:

- **Anticípese**: si su empresa tiene datos de larga duración y es un objetivo potencial de ataques de recopilación, cada día que pasa y no toma medidas, corre el riesgo de permitir que los atacantes recopilen más información para descifrarla más tarde. Cuanto antes tome medidas, antes impedirá que los atacantes recopilen datos para descifrarlos en el futuro.
- **Aprovechar recursos existentes**: cuando realice su criptoinventario, aproveche el trabajo que ya ha realizado para auditorías, Zero Trust, mejoras de red y otras actividades.
- **Educarse a sí mismo**: conozca la amenaza de la computación cuántica, la criptografía postcuántica (PQC), las tecnologías y métodos para fortalecer su red contra ataques cuánticos y los PQC nuevos y emergentes que puede usar para proteger su red. Aprenda de los mandatos gubernamentales, planes y legislaciones, RFC y otras fuentes de información.

Prácticas recomendadas para la criptografía

Aumente la fuerza de sus conjuntos criptográficos clásicos para hacer que sea más difícil para un atacante descifrar claves por fuerza bruta a medida que las ordenadores cuánticos se vuelven más rápidos y evolucionan en CRQC. Las ordenadores cuánticos que no son CRQC aún pueden ser lo suficientemente rápidos como para romper el cifrado más débil.

- Siga RFC 6379 para los *Conjuntos criptográficos Suite B para IPsec* para actualizar sus conexiones VPN a conjuntos de cifrado difíciles. Utilice Suite-B-GCM-256 y evite algoritmos AES de 128 bits más débiles, que son vulnerables al algoritmo de Grover.
- Actualice su CA a tamaños de clave RSA 4K para mitigar los ataques de fuerza bruta que pueden romper tamaños de clave más pequeños.
- Migre su autenticación de certificado VPN a nuevos certificados con tamaños de clave más grandes.

- Actualice a tamaños de hash SHA de bits más altos como SHA-384 y SHA-512. Deje de usar hashes débiles como MD5 y SHA-1.
- Actualice las conexiones SSL/TLS a conjuntos de cifrado resistentes; use TLSv1.3 con cifrados de Perfect Forward Secrecy (PFS).
- Sesiones SSL/TLS de túnel en sesiones VPN endurecidas de cliente a servidor.
- Configure sus perfiles de protección de vulnerabilidades para bloquear los PQC no autorizados para el tráfico que no descifre. Para el tráfico que descifra, utilice un perfil de descifrado para bloquear los PQC no autorizados (el perfil de descifrado solo permite los cifrados que habilita y el cortafuegos bloquea todos los demás cifrados). Los PQC no autorizados pueden indicar una filtración o un actor malintencionado interno que intenta usar los PQC para comprometer su red. Haga excepciones según sea necesario para sus equipos de pruebas PEN internos.

Prácticas recomendadas para la configuración de VPN

Cuando configure las VPN de tipo IKEv2 postcuántica, hágalas lo más resistentes posible a los ataques cuánticos:

- Implemente RFC 8784 para crear VPN IKEv2 que resistan ataques cuánticos.
- Implemente RFC 9242 y RFC 9370 para crear VPN IKEv2 que resistan ataques cuánticos.

> *RFC 8784 se puede utilizar con RFC 9242 y RFC 9370 para proporcionar una capa adicional de protección y esto puede cumplir con los requisitos de agilidad criptográfica.*

Prácticas recomendadas de RFC 8784:

- No utilice IKEv1. IKEv1 se considera un protocolo débil y no admite VPN postcuánticas. Si ambos pares de IKE son compatibles, actualice sus conexiones VPN a IKEv2 y seleccione el **IKEv2 only mode (Modo solo IKEv2)** cuando configure las puertas de enlace IKE [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** > **General**].
- Fije el **Negotiation Mode (Modo de negociación)** en **Mandatory (Obligatorio)** siempre que sepa que ambos pares admiten RFC 8784. El uso del modo **Mandatory (Obligatorio)** garantiza que la VPN resista los ataques postcuánticos y los atacantes no pueden cosechar los datos ahora y descifrarlos más tarde usando un algoritmo CRQC que ejecuta el algoritmo de Shor.

  > *El algoritmo de Shor puede descifrar el intercambio dinámico de claves en el protocolo de enlace IKEv2 que utiliza cifrado asimétrico, dada la suficiente potencia de procesamiento. Sin embargo, el algoritmo de Shor no puede descifrar el cifrado simétrico del túnel IPSec. Para proteger el cifrado IPSec simétrico, use AES-256 para protegerse contra el algoritmo de Grover y use los hashes y longitudes de clave más fuertes recomendados en la* sección anterior sobre prácticas recomendadas para la criptografía.

  Cuando utilice dispositivos externos, intente determinar si el dispositivo admite RFC 8784 y trabaje con el otro administrador para utilizar los mismos PPK PQ para la conexión, de modo que pueda utilizar el modo obligatorio.
- Especifique manualmente o genere automáticamente un secreto de PPK que tenga al menos 64 caracteres (32 bytes o 256 bits de entropía) de longitud para crear una clave fuerte. Puede especificar manualmente o generar automáticamente un **PPK Secret (Secreto de PPK)** de hasta 128 caracteres

(64 bytes, 512 bits de entropía). Cuanto más largo es el secreto de PPK, mayor es el número de bits de entropía, lo que hace que el secreto de PPK sea más difícil de descifrar.

El número de bits de entropía proporciona la mitad de ese número de bits de seguridad postcuántica. Por ejemplo, 256 bits de entropía proporcionan 128 bits de seguridad postcuántica y 512 bits de entropía proporcionan 256 bits de seguridad postcuántica. Un mínimo de 256 bits de entropía proporciona la seguridad equivalente a la Categoría 5, según se define en la Convocatoria de Propuestas de Criptografía Postcuántica del NIST. La sección Consideraciones de seguridad de RFC 8784 proporciona más detalles sobre la entropía y qué cantidad de entropía es suficiente.

El secreto de PPK solo se muestra en texto claro cuando lo configura o se genera automáticamente. Después de configurar o generar el secreto de PPK y navegar lejos de la pantalla que muestra el secreto en texto claro, nunca se muestra en texto claro de nuevo para ayudar a evitar comprometer la clave.

Copie el par KeyID y secreto de PPK y guárdalo de forma segura. Si no almacena la clave cuando la configura o genera, no puede recuperarla más tarde. (Puede eliminar la PPK PQ y configurar otra si es necesario).

Otras Prácticas recomendadas para gestionar las PPK PQ incluyen:

- Cree múltiples PPK PQ activos. El uso de varias teclas activas, no solo una, añade un elemento de aleatoriedad a la selección de teclas durante el intercambio de claves.
- de Asegúrese de que cada par IKEv2 tenga exactamente el mismo conjunto de PPK PQ activados (pares KeyID y secreto de PPK) para negociar el intercambio de claves.
- Si Panorama gestiona los pares, configure las PPK PQ y envíelos a cortafuegos gestionados para una configuración más fácil, rápida y automática.
- Si necesita comunicar la PPK PQ a otro administrador, utilice un método de comunicación criptográficamente seguro, como el correo electrónico cifrado.
- Almacene la cadena de secreto de PPK de forma segura. No lo guarde en notas adhesivas o en cualquier lugar donde administradores no autorizados puedan encontrarlo.

La NSA publica guías sobre cómo gestionar las claves precompartidas de forma segura, incluidas las claves cuánticas precompartidas RFC 8784.

Prácticas recomendadas de RFC 9242 y RFC 9370:

- No utilice IKEv1. IKEv1 se considera un protocolo débil y no admite VPN postcuánticas. Si ambos pares de IKE son compatibles, actualice sus conexiones VPN a IKEv2 y seleccione el **IKEv2 only mode (Modo solo IKEv2)** cuando configure las puertas de enlace IKE [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** > **General**].
- Cree la clave híbrida utilizando un KEM clásico fuerte, como Diffie-Hellman Group 20 y superior, y al menos un PQC en las rondas de KEM adicionales, como Kyber-768 (ML-KEM), cuando configure los perfiles criptográficos IKE [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto** > **General and Advanced Options (Opciones generales y avanzadas)**].
- Utilice solo PQC que tengan un nivel de seguridad de L3 o superior para obtener información confidencial. Cada PQC adicional añadido al proceso de creación de claves aumenta la capacidad de la clave para resistir un ataque cuántico, pero también añade latencia y capacidad al proceso de peering IKEv2. En general, añadir un nivel de seguridad L3 PQC agrega aproximadamente de 20 a 30 ms al

intercambio de claves IKEv2, y agregar un nivel de seguridad L5 PQC añade de 40 a 60 ms. Los PQC más fuertes que utilizan claves más grandes, como Classic McEliese, pueden añadir potencialmente más de 800 ms al intercambio de claves e introducir altos niveles de fragmentación. Familiarícese con los tamaños de clave PQC y las fortalezas de seguridad para seleccionar el mejor PQC para sus comunicaciones VPN.

- Coordine los PQC utilizados en cada ronda de negociación clave con el administrador que gestiona el dispositivo VPN homólogo. Cuando ambos dispositivos VPN a cada lado del túnel se configuran con los mismos PQC en cada ronda de negociación de claves opcional, los problemas de interoperabilidad se minimizan. Trata de llegar a un acuerdo sobre el PQC y su fortaleza de seguridad para garantizar que ambas partes estén configuradas con los mismos parámetros. Para cortafuegos gestionados bajo la misma organización, se pueden utilizar herramientas de gestión central para garantizar una configuración coherente y una selección de PQC en cada ronda de negociación de claves.
- Habilite la agilidad criptográfica para proteger sus datos durante la transición a un entorno PQC puro. La transición puede requerir de 5 a 10 años antes de que el sector confíe plenamente en los nuevos PQC.
  - Para las organizaciones que deben usar PQC estandarizados por NIST y aprobados por FIPS, la agilidad criptográfica se puede lograr habilitando RFC 8784 con RFC 9242 y RFC 9370. Si el PQC utilizado en la clave híbrida cae en una vulnerabilidad, la cadena PPK utilizada en RFC 8784 aún puede proporcionar resistencia cuántica para evitar un ataque de recopilación exitoso.
  - Para las organizaciones a las que se les permite usar PQC estandarizados y no estandarizados de NIST, la agilidad criptográfica se puede lograr usando al menos dos PQC con un KEM clásico fuerte, como Diffie-Hellman Group 21. Idealmente, los PQC KEM deberían utilizar diferentes tecnologías matemáticas, en las que un KEM se base en tecnología reticular y el otro en tecnología basada en código u otras tecnologías no reticulares. Opcionalmente, RFC 8784 también se puede habilitar con la clave híbrida para añadir una capa adicional de seguridad y extender la agilidad criptográfica.
- Reduzca el valor de vida útil de la clave de su valor predeterminado a un valor más bajo para facilitar un cambio de clave más rápido.
- Habilite IPSec para usar claves híbridas cuando configure los perfiles criptográficos IPSec [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Crypto IPSec)** > **General and Advanced Options (Opciones avanzadas y generales)**]. Ambos lados del túnel IPSec deben configurarse para utilizar el mismo PQC y la misma fuerza de seguridad en cada ronda de intercambio de claves adicional.

Más información sobre la seguridad poscuántica

La seguridad poscuántica, las tecnologías poscuánticas y las implementaciones poscuánticas recomendadas están en apenas empezando. A medida que planifica proteger sus activos en un mundo de computación poscuántica, es importante comprender todo lo que pueda sobre las tecnologías poscuánticas, las regulaciones y mandatos gubernamentales que afectan a su negocio, y cómo realizar la transición a las VPN y cifrados poscuánticos.

El gobierno de los Estados Unidos y los gobiernos de todo el mundo están creando planes para abordar la amenaza a la seguridad cuántica que representan las ordenadores cuánticos y la criptografía poscuántica. Además, organismos de normalización como el Instituto Nacional de Normas y Tecnología (NIST) y el Grupo de Trabajo de Ingeniería de Internet (IETF) están creando normas para las nuevas tecnologías poscuánticas y cómo implementarlas.

En este tema se proporcionan enlaces a información que le ayudarán a aumentar la comprensión, la preparación y la transición a la seguridad poscuántica en su empresa.

- Gobierno de los Estados Unidos
- Otros Gobiernos del Mundo
- RFC
- Tecnologías e información general

Gobierno de los Estados Unidos

Los gobiernos de muchas naciones están desarrollando planes, normas y leyes para abordar la amenaza de la computación cuántica y el advenimiento de la criptografía poscuántica. Los siguientes enlaces proporcionan información sobre cómo el gobierno de los Estados Unidos está abordando el tema, incluidos enlaces a información del Instituto Nacional de Estándares y Tecnología (NIST) y la Agencia de Seguridad Nacional (NSA). Consulte los sitios y organizaciones de seguridad de su gobierno local para averiguar cómo su gobierno está abordando la seguridad poscuántica.

- El NIST Post-Quantum Cryptography Resource Center proporciona información sobre la estandarización de la criptografía poscuántica y otros materiales.
- El National Cybersecurity Center of Excellence (NCCOE) del NIST *Migración a la criptografía poscuántica* Ofrece orientación para migrar a la criptografía poscuántica.
- *Los requisitos de gestión de claves simétricas Anexo V2.1* del Servicio de Seguridad Central de la NSA proporciona los requisitos de implementación para el uso de claves precompartidas para Commercial Solutions for Classified (CSfC).
- El Sitio web del Departamento de Seguridad Nacional para la criptografía poscuántica Incluye la hoja de ruta postcuántica del departamento y otros recursos.
- La Iniciativa de criptografía poscuántica de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) unifica los esfuerzos poscuánticos con otras agencias gubernamentales y socios de la industria para abordar las amenazas de la computación cuántica. El sitio también proporciona enlaces a más recursos de CISA, NIST y el Departamento de Seguridad Nacional.
- Para fomentar la migración de los sistemas de tecnología de la información del gobierno federal a la criptografía resistente a la tecnología cuántica, el presidente Biden firmó la Ley de Ciberseguridad de la computación cuántica (HR 7535).

- Memorándum Ejecutivo M-23-02, La *Migración a la criptografía poscuántica* de la Oficina Ejecutiva del Presidente proporciona orientación a las agencias de los Estados Unidos sobre el cumplimiento del Memorándum de Seguridad Nacional 10 (NSM-10), el *Memorándum de Seguridad Nacional sobre la promoción del liderazgo de los Estados Unidos en computación cuántica y la mitigación de riesgos para los sistemas criptográficos vulnerables*.

Otros Gobiernos del Mundo

Los siguientes enlaces proporcionan información sobre cómo varios gobiernos de todo el mundo están abordando el tema.

- La Oficina Federal para la Seguridad de la Información (BSI) de Alemania proporciona información sobre criptografía poscuántica, estrategias de migración, desarrollos y recomendaciones actuales, y otros materiales.
- El Gobierno del Reino Unido proporciona información sobre ordenadores y tecnologías cuánticas, amenaza de ordenadores cuánticos, estrategia cuántica nacional, distribución de claves cuánticas, generación de números aleatorios cuánticos y otros materiales.
- El Agencia Francesa de Ciberseguridad (ANSSI) proporciona información sobre la transición poscuántica, la distribución de claves cuánticas y otros materiales.
- El Servicio General de Inteligencia y Seguridad de los Países Bajos (AIVD) proporciona información sobre las amenazas de los ordenadores cuánticos, las estrategias y los pasos de la migración poscuántica, la distribución de claves cuánticas y otros materiales.
- La Agencia de la Unión Europea para la Ciberseguridad (ENISA) proporciona información sobre criptografía poscuántica, implementaciones híbridas, estrategias poscuánticas y otros materiales.
- La Autoridad Monetaria de Singapur proporciona información sobre los programas cuánticos y aborda los riesgos de ciberseguridad asociados con quantum.
- El Gobierno de Japón proporciona información sobre estrategias cuánticas, seguridad cuántica y migración a la tecnología cuántica.

RFC

Solicitudes de propuestas (RFC) describen los fundamentos técnicos de internet. Varias solicitudes de propuestas describen aspectos de la resistencia de IKEv2 a los ataques de ordenadores cuánticos:

- RFC 8784, *Combinación de claves previamente compartidas en el protocolo de intercambio de claves de Internet versión 2 (IKEv2) para la seguridad poscuántica*, describe el estándar para la extensión IKE que permite que IKEv2 sea resistente a los ataques de los equipos cuánticos. Cómo RFC 8784 resiste las amenazas de computación cuántica resume el efecto de RFC 8784 en su red.
- RFC 6379, *Conjuntos criptográficos Suite B para IPsec*, describe el algoritmo Suite-B-GCM-256 bits que se debería utilizar en lugar del cifrado AES-128 bits más débil. La eliminación de cifrados débiles como AES-128 ayuda a retrasar el tiempo en que el Algoritmo de Grover podría ser capaz de romper el cifrado simétrico.
- RFC 9370, *Múltiples intercambios de claves en el Protocolo de intercambio de claves de Internet versión 2 (IKEv2)*, describe cómo ampliar IKEv2 para permitir que varios intercambios de claves se mezclen para crear la clave de cifrado.
- RFC 9242, *Intercambio intermedio en el Protocolo de intercambio de claves de Internet versión 2 (IKEv2)*, define un mecanismo de intercambio intermedio que permite la transferencia de grandes cantidades de datos, como claves de cifrado basadas en múltiples intercambios de claves, en el

intercambio de claves inicial. Esto ayuda a evitar la fragmentación. (Algunos dispositivos no permiten la fragmentación).

- RFC 7383, *Fragmentación de mensajes del Protocolo de intercambio de claves de Internet versión 2 (IKEv2)*, permite que los mensajes IKE se fragmenten en el nivel IKE, lo que elimina los problemas causados por la fragmentación de IP. Sin embargo, RFC 7383 no funciona para el intercambio inicial. RFC 9242 ayuda a evitar la fragmentación en el intercambio inicial y RFC 7383 evita la fragmentación de IP en los mensajes IKEv2 posteriores.

Tecnologías e información general

Muchas organizaciones reconocen las amenazas potenciales que plantean los ordenadores cuánticos y las tecnologías que no representan ningún peligro cuando se ejecutan en ordenadores clásicos, pero representan un peligro potencialmente catastrófico cuando se ejecutan en un ordenador cuántico criptográficamente relevante (CRQC).

- El sitio liboqs de la organización Open Quantum Safesite es una biblioteca de código abierto en C para algoritmos criptográficos cuánticos seguros.
- El programa de la Fundación Linux, proyecto Alianza de Criptografía postcuántica, busca abordar los desafíos de seguridad criptográfica planteados por la computación cuántica mediante la producción de implementaciones de software de alta seguridad de algoritmos estandarizados.
- Algoritmo de Shor, este amenaza con romper muchos algoritmos clásicos de cifrado asimétrico que se utilizan hoy en día cuando se utilizan con un CRQC. El algoritmo de Shor factoriza números grandes y complejos para derivar los números primos que son la base del cifrado clásico y asimétrico.
- Algoritmo de Grover, este es un algoritmo de búsqueda no estructurado cuántico, acelerado cuadráticamente. Puede romper los algoritmos clásicos de cifrado simétrico a través de la fuerza bruta al reducir la fuerza criptográfica de los algoritmos AES y las funciones hash a la mitad cuando se usa con un CRQC.
- Harvest Now, Decrypt Later, los ataques de recopilación ahora y descifrar después son una amenaza activa en la actualidad. En los ataques Harvest Now, Decrypt Later, los atacantes roban datos que no pueden descifrar ahora y los almacenan hasta que un CRQC pueda descifrarlos. Estos ataques están teniendo lugar hoy en día y suponen una amenaza inmediata para los datos de larga duración.
- El artículo de la base de conocimientos de Quantum Inspire *¿Qué es un cúbit?* explica los bits cuánticos.
- El artículo de Deloitte *The Quantum Threat to Cryptography* (La amenaza cuántica para la criptografía) analiza las razones por las que debe comenzar su transición poscuántica lo antes posible, al igual que el artículo de Forbes *The Quantum Threat To Cryptography: Don't Panic, But Prepare Now* (La amenaza cuántica a la criptografía: que no cunda el pánico, pero prepárese ahora).
- La *Criptografía cuántica segura (QSC) de ETSI: Un Marco reproducible para migraciones cuánticas seguras* proporciona una buena plantilla para crear un plan de migración poscuántica.
- El *Plan de Economía Cuántica del Foro Económico Mundial* proporciona una hoja de ruta para desarrollar ecosistemas cuánticos de manera equitativa para permitir la transición a la economía cuántica.

Configurar redes VPN IKEv2 resistentes a la tecnología cuántica

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

Las VPN IKEv2 resistentes a la tecnología cuántica basadas en RFC 8784 y/o RFC 9242 y RFC 9370 evitan que los atacantes que intentan ejecutar ataques Harvest Now, Decrypt Later roben el material de clave criptográfica utilizado para cifrar datos en la VPN. Sin las claves criptográficas, los atacantes no pueden descifrar los datos recopilados posteriormente con un ordenador cuántico criptográficamente relevante. Incluso si los atacantes logran robar los datos cifrados, sin un ordenador cuántico criptográficamente relevante para descifrar el material clave, no pueden comprometer los datos recopilados porque no pueden descifrarlos sin la clave.

RFC 8784 proporciona una transición resistente a la tecnología cuántica desde la criptografía clásica actual a la criptografía poscuántica que puede implementar hoy mismo. RFC 8784 no requiere actualizaciones de criptografía, por lo que su implementación es sencilla y rápida siempre que ambos dispositivos VPN en cada lado del túnel puedan soportarlo.

RFC 9242 y RFC 9370 consumen más recursos que RFC 8784, pero proporcionan una capacidad de generación de claves dinámica basada en los nuevos algoritmos matemáticos PQC que no son vulnerables al algoritmo de Shor. Debido a que RFC 9242 y RFC 9370 requieren actualizaciones de criptografía, puede llevar más tiempo implementar la tecnología de clave híbrida, por lo que debe tener en cuenta la agilidad criptográfica.

Este capítulo le muestra cómo configurar las VPN de tipo IKEv2 postcuántica, incluido cómo configurar las VPN de tipo IKEv2 postcuántica en escenarios donde conoce al peer IKEv2 y sus capacidades y escenarios donde no controla al peer IKEv2 y no conoce sus capacidades.

- Configurar las VPN de tipo IKEv2 postcuántica con PPK RFC 8784 le muestra los pasos y las opciones de configuración de VPN IKEv2 postcuántica para proteger las comunicaciones VPN con claves precompartidas postcuánticas.
- Configurar las VPN de tipo IKEv2 postcuántica con claves híbridas RFC 9242 y RFC 9370 Le muestra los pasos de configuración y las opciones para asegurar las comunicaciones VPN con claves híbridas.
- Ejemplo de configuración de RFC 8784 de IKEv2 Post-Quantum Proporciona un ejemplo de una topología simple y cómo configurar el soporte de VPN IKEv2 postcuántico para la topología.

Además de configurar las VPN de tipo IKEv2 postcuántica basadas en RFC 8784, siga RFC 6379 para Conjuntos criptográficos Suite B para IPsec para actualizar sus conexiones VPN a suites de cifrado resistentes, actualice su CA a tamaños de clave RSA de 4K para mitigar ataques de fuerza bruta que pueden romper tamaños de clave más pequeños y migrar su autenticación de certificado VPN a nuevos certificados, además de actualizar a tamaños de hash SHA de bits más altos, como SHA-384 y SHA-512.

Configurar las VPN de tipo IKEv2 postcuántica con PPK RFC 8784

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

Las VPN de tipo IKEv2 postcuántica basadas en RFC 8784 funcionan transmitiendo un secreto previamente compartido por separado (fuera de banda) del intercambio de pares inicial (el intercambio IKE_SA_INIT). En lugar de transmitir el secreto previamente compartido en el intercambio de emparejamiento, que un atacante podría comprometer o recopilar ahora y descifrar más tarde, el intercambio de emparejamiento solo transmite un ID de clave. Un ID de clave y un secreto previamente compartido comprenden un par único denominado clave poscuántica precompartida (PPK PQ).

Cada par de IKEv2 utiliza el ID de clave para buscar el secreto previamente compartido, que se transmite de forma segura entre los administradores o se inserta mediante Panorama, y se almacena localmente en cada par IKEv2. La clave previamente compartida nunca forma parte del intercambio de emparejamiento y nunca atraviesa la VPN poscuántica, por lo que un atacante que utilice un ordenador cuántico no puede robarla, descifrarla y utilizarla para descifrar los datos recopilados de una VPN.

Ambos pares IKEv2 deben tener los mismos pares activos de ID de clave más secreto previamente precompartido para que, cuando los pares negocien la conexión, cada par pueda buscar el mismo ID de clave y recuperar el mismo secreto previamente compartido. Si el elemento del mismo nivel que responde no tiene un identificador de clave coincidente o si el secreto previamente compartido asociado con el identificador de clave difiere del iniciador, la conexión se anula.

Establecimiento del emparejamiento IKEv2 y un túnel IPSec *antes de configurar los componentes poscuánticos. Además, asegúrese de tener políticas de seguridad que permitan el tráfico IKEv2 e IPSec entre los cortafuegos y habiliten el registro.*

Para hacer que sus VPN IKEv2 sean resistentes a los ataques cuánticos:

STEP 1 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** y **Add (Añadir)** una nueva puerta de enlace.

STEP 2 | Configure los ajustes de la pestaña **General** y seleccione una de las siguientes opciones: **IKEv2 only mode (Modo solo IKEv2)** o **IKEv2 preferred mode (Modo preferido de IKEv2)** como la **Version (Versión)**.

En **IKEv2 only mode (Modo solo IKEv2)**, si el par no es compatible con IKEv2, el cortafuegos anula la conexión. En **IKEv2 preferred mode (Modo preferido de IKEv2)**, si el par no es compatible con IKEv2, el cortafuegos recurre a IKEv1. Sin embargo, la VPN debe negociar IKEv2 para usar las funciones de VPN poscuánticas, por lo que si el cortafuegos vuelve a IKEv1, esas funciones no están disponibles.

*IKEv1 se considera débil. Si ambos pares IKE son compatibles, actualice sus conexiones VPN a IKEv2 y seleccione **IKEv2 only mode (Modo solo IKEv2)** para garantizar niveles adecuados de seguridad y la capacidad de uso de las VPN PQ.*

STEP 3 | Seleccione **Advanced Options (Opciones avanzadas)** y configure las opciones no cuánticas.

Si seleccionó **IKEv2 preferred mode (Modo preferido de IKEv2)** como la **Version (Versión)**, hay pestañas para **IKEv1** y **IKEv2**; seleccione **IKEv2**. Si seleccionó **IKEv2 only mode (Modo solo IKEv2)** como la **Version (Versión)**, solo se muestran las opciones de IKEv2.

Seleccione **PQ PPK (PPK PQ)** (clave precompartida poscuántica) para configurar los elementos poscuánticos de su VPN IKEv2. [**General** le permite añadir un perfil de IKE Crypto y establecer la **Liveness Check (Comprobación de actividad)**].

STEP 4 | Deberá **Habilitar la clave precompartida poscuántica (PPK)** para habilitar el uso de funciones de resistencia poscuántica en la VPN. Esta opción está deshabilitada de manera predeterminada.

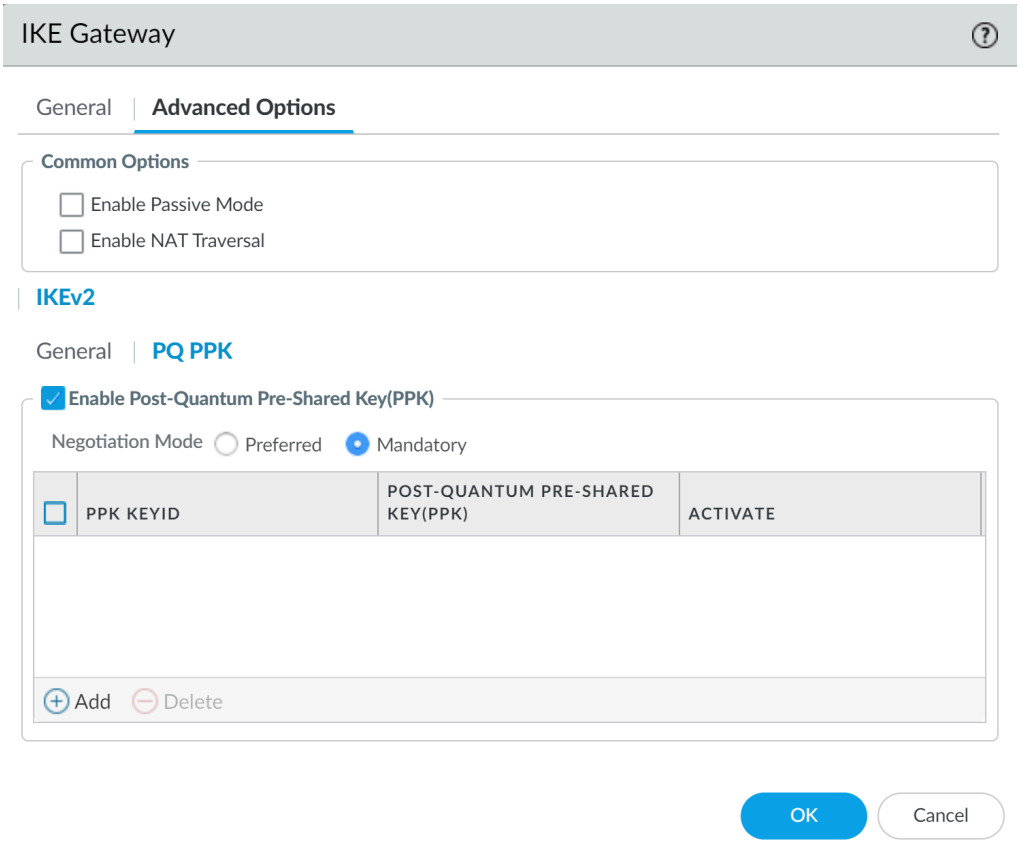
*Debe configurar y activar al menos una PPK PQ cuando **Habilita la clave precompartida poscuántica (PPK)** de modo que el cortafuegos tenga una PPK PQ para usar durante la negociación de IKEv2 y pueda admitir RFC 8784.*

STEP 5 | Establezca el parámetro **Negotiation Mode (Modo de negociación)** en **Preferred (Preferida)** o **Mandatory (Obligatorio)**.

- **Preferred (Preferido)**: cuando el cortafuegos negocia con el par, el cortafuegos primero intenta negociar mediante PPK PQ. Si el par no es compatible con RFC 8784, el cortafuegos recurre a un intercambio de claves clásico para la conexión. Si no sabe o no tiene control sobre si el par admite RFC 8784, el modo **Preferred (Preferido)** conserva la compatibilidad con versiones anteriores para garantizar que las conexiones retrocedan en lugar de eliminarse. **Preferred (Preferido)** es el modo predeterminado.
- **Mandatory (Obligatorio)**: cuando el cortafuegos negocia con el par, el par debe ser compatible con RFC 8784 PQ PPK. Si el par que responde no es compatible con RFC 8784, el cortafuegos anula la

conexión. Utilice el modo **Mandatory (Obligatorio)** cuando sabe que el par es compatible con RFC 8784 PQ PPK.

*Utilice el modo **Mandatory (Obligatorio)** cuando puede optar por la mejor seguridad.*



STEP 6 | Debe **Add (Añadir)** y **Activate (Activar)** hasta diez PPK PQ únicos.

Una PPK PQ consta de dos elementos emparejados: un KeyID de PPK y un secreto de PPK. El KeyID de PPK es una cadena única que identifica el secreto de PPK y puede ser cualquier cosa que desee con un máximo de 31 caracteres, como **`PPK-1`** o **`PPK súper fuerte`**. El secreto de PPK es la clave aleatoria previamente compartida que nunca se transmite a través de la VPN porque los administradores de ambos pares comparten la clave mediante un método de comunicación seguro y la configuran en los pares fuera de banda. El cortafuegos solo transmite el KeyID en la VPN de IKEv2 para que el par pueda buscar el secreto de PPK localmente.

El número de PPK PQ que puede definir depende de lo que pueda admitir el par IKE. Las implementaciones de algunos proveedores permiten menos de diez PPK PQ únicos; algunas

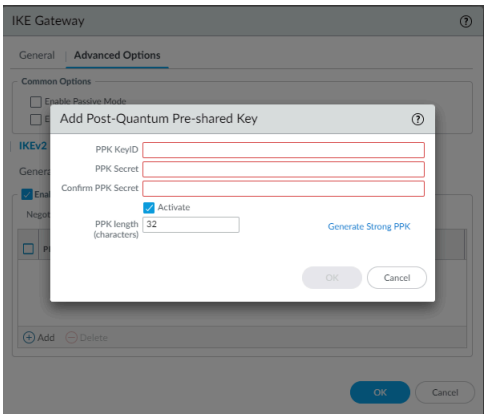
implementaciones incluso permiten solo uno. No defina más PPK PQ de los que puede admitir el par, ya que ambos pares deben tener exactamente las mismas PPK PQ disponibles.

Configure varias PPK PQ activas para los pares compatibles con varias PPK PQ. El cortafuegos elige aleatoriamente entre los PPK PQ activos, lo que añade un elemento de aleatoriedad a la negociación IKEv2.

La configuración de varias PPK PQ es más segura porque añade un elemento aleatorio a la selección de PPK PQ.

Puede crear el secreto de PPK manualmente o utilizar el cortafuegos para generar un secreto seguro para usted. Configure el secreto de PPK manualmente si desea generar la clave usted mismo o si recibe una PPK PQ del administrador de un par y necesita configurarla en su cortafuegos. Cuanto más largo es

el secreto de PPK, mayor es el número de bits de entropía, lo que hace que el secreto de PPK sea más difícil de descifrar.



Para configurar el secreto de PPK de forma manual, que puede especificar mediante caracteres ASCII:

1. Especifique una única **PPK KeyID (KeyID de PPK)** de hasta 31 caracteres.
2. Especifique una cadena de **PPK Secret (Secreto de PPK)** única y aleatoria. La cadena puede tener entre 32 y 128 caracteres (entre 16 y 64 bytes, lo que equivale a entre 128 y 512 bits de entropía).

   *Especifique un **PPK Secret (Secreto de PPK)** de al menos 64 caracteres (32 bytes o 256 bits de entropía) de longitud para crear una clave segura.*
3. Especifique exactamente la misma cadena en **Confirm PPK Secret (Confirmar secreto de PPK)**.

   Almacene el secreto de PPK de forma segura. de El secreto de PPK no se muestra en texto no cifrado, por lo que si no lo almacena ahora, no podrá recuperarlo más adelante. (Puede eliminar la PPK PQ y configurar otra si es necesario). Dado que el par IKEv2 debe tener la misma PPK PQ (KeyID más secreto de PPK), es posible que deba comunicar el secreto de PPK a otro administrador. Si es así, asegúrese de que el método de comunicación utilizado sea criptográficamente seguro y asegúrese de que el secreto de PPK esté almacenado de forma segura.

   La NSA publica guías sobre cómo gestionar las claves precompartidas de forma segura, incluidas las claves cuánticas precompartidas RFC 8784.
4. **Activate (Activar)** se selecciona de forma predeterminada para que el cortafuegos pueda usar el par KeyID de PPK y el secreto de PPK (el PPK PQ) para negociar con el par. Si no desea que el cortafuegos use este par KeyID de PPK y secreto de PPK al negociar con pares, desmarque **Activate (Activar)**.

   Por ejemplo, si configura un nuevo PPK PQ en un cortafuegos, es posible que desee desactivarlo hasta que el administrador del mismo nivel pueda añadir el mismo PPK PQ al mismo nivel para

evitar un error de conexión porque el iniciador usa un PPK PQ que aún no está instalado en el mismo nivel.

5. Haga clic en **OK (Aceptar)**. La pestaña **PQ PPK (PPK PQ)** muestra el ID de clave de PPK en texto no cifrado, oculta la clave previamente compartida y muestra el estado de activación de PPK PQ.

Para configurar el secreto de PPK mediante la generación automática de PPK segura del cortafuegos, que utiliza caracteres hexadecimales:

1. Especifique una única **PPK KeyID (KeyID de PPK)** de hasta 31 caracteres.
2. Establezca el parámetro **PPK length (characters) [Longitud de PPK (caracteres)]** a la longitud que desea generar para el **PPK Secret (Secreto de PPK)**. El valor predeterminado es de 32 caracteres (16 bytes).

   *Establezca la **PPK length (characters) [Longitud de PPK (caracteres)]** en al menos 64 caracteres (32 bytes o 256 bits de entropía) de longitud para generar una clave segura.*
3. Haga clic en **Generate Strong PPK (Generar PPK fuerte)**. El cortafuegos genera y muestra un secreto de PPK seguro de la longitud especificada en **PPK length (characters) [Longitud de PPK (caracteres)]**.

   Esta es la única vez que el secreto de PPK se muestra en texto no cifrado. Si no almacena el secreto de forma segura, no podrá recuperarlo. (Puede eliminar la PPK PQ y configurar otra si es necesario). Dado que el par IKEv2 debe tener la misma PPK PQ (KeyID más secreto de PPK), es posible que deba comunicar el secreto de PPK a otro administrador. Si es así, asegúrese de que el método de comunicación utilizado sea criptográficamente seguro y asegúrese de que el secreto de PPK esté almacenado de forma segura.

   Copie el secreto de PPK, haga clic en **OK (Aceptar)** y péguelo en los campos **PPK Secret (Secreto de PPK)** y **Confirm PPK Secret (Confirmar el secreto de PPK)**.
4. **Activate (Activar)** se selecciona de forma predeterminada para que el cortafuegos pueda usar el par KeyID de PPK y el secreto de PPK (el PPK PQ) para negociar con el par. Si no desea que el cortafuegos use este par KeyID de PPK y secreto de PPK al negociar con pares, desmarque **Activate (Activar)**.

   Por ejemplo, si configura un nuevo PPK PQ en un cortafuegos, es posible que desee desactivarlo hasta que el administrador del mismo nivel pueda añadir el mismo PPK PQ al mismo nivel para evitar un error de conexión porque el iniciador usa un PPK PQ que aún no está instalado en el mismo nivel.
5. Haga clic en **OK (Aceptar)**. La pestaña **PQ PPK (PPK PQ)** muestra el ID de clave de PPK en texto no cifrado, oculta la clave previamente compartida y muestra el estado de activación de PPK PQ.

STEP 7 | Haga clic en **OK (Aceptar)** para crear la VPN.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

El tema Ejemplo de configuración de RFC 8784 de IKEv2 Post-Quantum proporciona un ejemplo de una topología simple y cómo configurar la compatibilidad de VPN IKEv2 poscuántica para la topología.

STEP 9 | Si no es el administrador de ambos pares IKEv2, comunique de forma segura la PPK PQ (KeyID más secreto de PPK) al administrador del mismo nivel para la instalación en el mismo nivel. La comunicación y el almacenamiento seguros de PPK PQ son fundamentales para proteger sus datos.

Ambos pares IKEv2 deben tener los mismos ID de clave activos y los secretos previamente compartidos asociados para activar la conexión VPN poscuántica.

Configurar las VPN de tipo IKEv2 postcuántica con claves híbridas RFC 9242 y RFC 9370

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.2 o posterior.

Las VPN de tipo IKEv2 postcuántica basadas en RFC 9242 y RFC 9370 funcionan creando una clave híbrida utilizando dos o más mecanismos de intercambio de claves (KEM) en el intercambio de pares inicial (el intercambio IKE_SA_INIT). Las claves híbridas proporcionan resistencia cuántica al evitar que un KEM comprometido permita el ataque cuántico utilizando Harvest Now, Decrypt Later (HNDL) para conseguir su objetivo. Siempre y cuando todos los KEM utilizados para crear la clave híbrida no se vean comprometidos, los datos seguirán protegidos.

Como los estándares son todavía relativamente nuevos y cada proveedor puede tener diferentes interpretaciones del estándar para su implementación, mantener las configuraciones idénticas en ambos lados ayuda a mantener las cosas sencillas y permitir que el túnel VPN postcuántico tenga éxito. Para minimizar las posibilidades de interoperabilidad, asegúrese de que ambos lados del túnel VPN estén configurados con los mismos PQC y las fortalezas de seguridad en cada una de las rondas de negociación de claves opcionales. También compruebe la configuración de fragmentación IKEv2 en ambos lados para asegurarse de que están configurados correctamente.

Configure el emparejamiento IKEv2 y un túnel IPSec *antes de configurar sus componentes postcuánticos. Además, asegúrese de tener políticas de seguridad que permitan el tráfico IKEv2 e IPSec entre los cortafuegos y habiliten el registro.*

Para garantizar la protección de los datos durante largos períodos, se deben utilizar más de dos KEM y, además, se puede agregar defensa en profundidad habilitando tanto la clave precompartida a través de RFC 8784 como la clave híbrida a través de RFC 9242 y RFC 9370.

Para hacer que sus VPN IKEv2 sean resistentes a los ataques cuánticos:

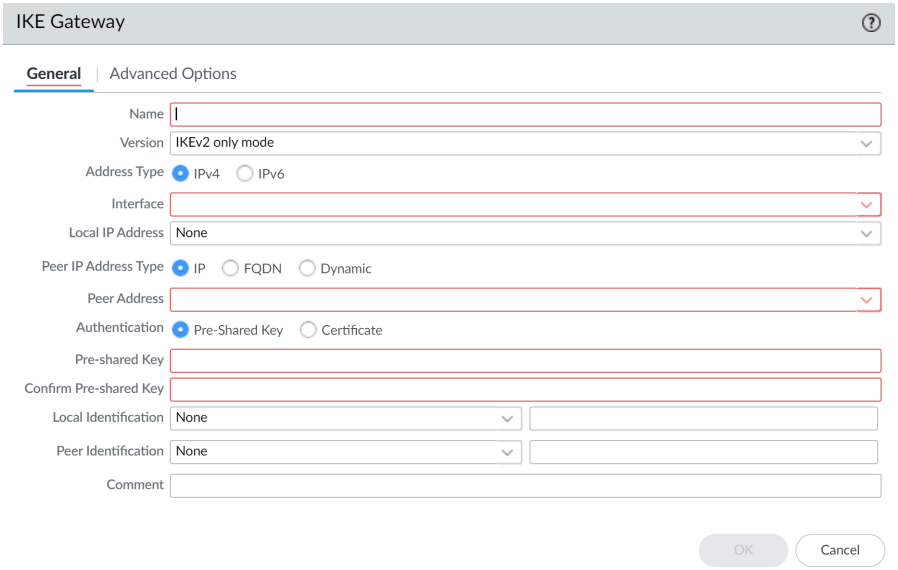
STEP 1 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** y **Add (Añadir)** una nueva puerta de enlace.

STEP 2 | Configure los ajustes **General (Generales)** y seleccione el **IKEv2 only mode (Solo modo IKEv2)** o el **IKEv2 preferred mode (Modo preferido IKEv2)** como la **Version (Versión)**.

En el **IKEv2 only mode (Modo solo IKEv2)**, si el par no admite IKEv2, el cortafuegos aborta la conexión. En **IKEv2 preferred mode (Modo preferido de IKEv2)**, si el par no es compatible con IKEv2, el cortafuegos recurre a IKEv1. Sin embargo, la VPN debe negociar IKEv2 para usar las

funciones de VPN postcuánticas, por lo que si el cortafuegos vuelve a IKEv1, esas funciones no están disponibles.

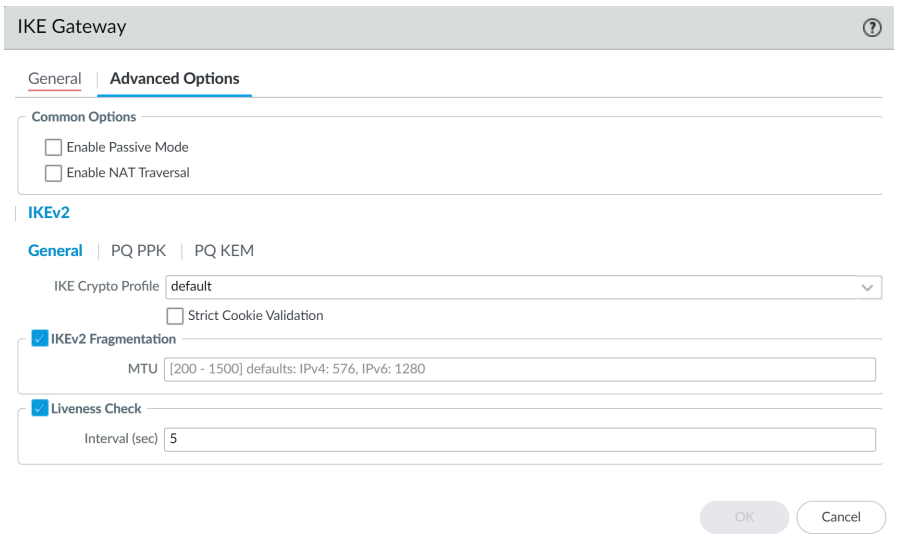
*IKEv1 se considera débil. Si ambos pares IKE son compatibles, actualice sus conexiones VPN a IKEv2 y seleccione **IKEv2 only mode (Modo solo IKEv2)** para garantizar niveles adecuados de seguridad y la capacidad de uso de las VPN PQ.*



STEP 3 | Seleccione **Advanced Options (Opciones avanzadas)** y configure las opciones no cuánticas. Seleccione **IKEv2** y configure la configuración **General**.

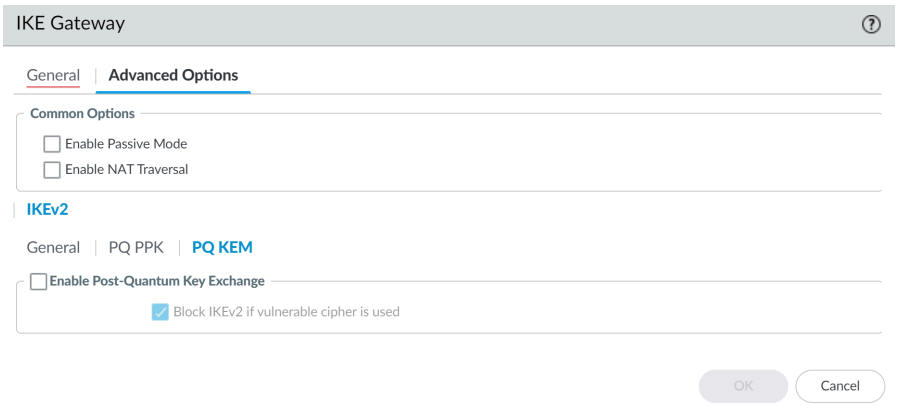
Generalmente le permite añadir un perfil criptográfico IKE, habilitar la **IKEv2 Fragmentation (Fragmentación IKEv2)** y establecer la **Liveness Check (Comprobación de actividad)**.

La fragmentación IKEv2 debe activarse cuando se utilizan los PQC KEM, ya que los tamaños de clave y las cargas útiles de datos son mayores. Ambos dispositivos de terminación VPN deben establecerse en los mismos valores de fragmentación.



STEP 4 | **Enable Post-Quantum Key Exchange (Habilitar el intercambio de claves poscuántico)** para que KEM de PQ habilite el uso de funciones de resistencia postcuántica en la VPN. Esta opción está deshabilitada de manera predeterminada.

Opcionalmente, habilite el **Block IKEv2 if vulnerable cipher is used (Bloquear IKEv2 si se utiliza un cifrado vulnerable)**. Si esta opción está activada, el cortafuegos bloquea todos los nuevos pares IKEv2 si detecta que se está utilizando un KEM vulnerable en el perfil criptográfico de IKE. Los túneles VPN existentes que surgieron de antemano pueden continuar.

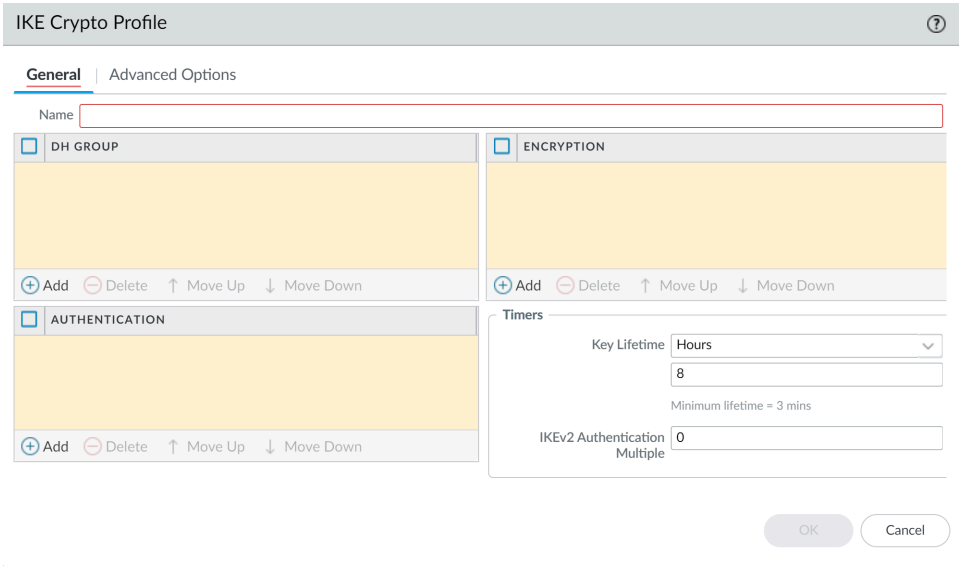


STEP 5 | Haga clic en **OK (Aceptar)** para crear la puerta de enlace de IKE.

STEP 6 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico de IKE)** y luego **Add (Añadir)** un nuevo perfil.

STEP 7 | Configure la configuración **General** y seleccione los componentes criptográficos (grupo DH, cifrado, autenticación, temporizadores) para el intercambio de claves IKEv2 predeterminado.

Seleccione una configuración de intercambio de claves clásica fuerte para aumentar la resistencia cuántica. Grupo DH 20 o superior, AES-256-GCM, y actualice las claves con más frecuencia utilizando la duración de la clave. Para regenerar completamente la clave a intervalos específicos, habilite el Múltiplo de autenticación IKEv2 estableciendo un valor superior a cero. La clave se regenera después de alcanzar el múltiplo de la Duración de la clave.



STEP 8 | Seleccione **Advanced Options (Opciones avanzadas)** y configure las rondas opcionales de **Post-Quantum IKEv2 Additional Key Exchange (Intercambio de claves adicionales de IKEv2 poscuántico)**.

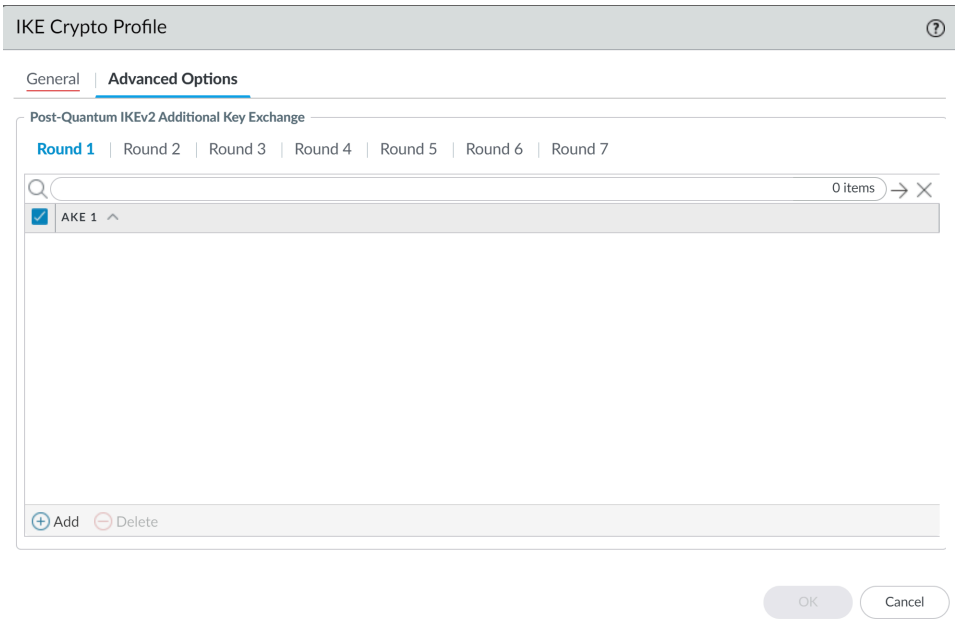
En la RFC 9370 se permite un máximo de siete **Additional Key Exchange Rounds (Rondas adicionales de intercambio de claves)** (ronda 1-7). Como mínimo, se requiere un PQC KEM para añadir resistencia cuántica. Añadir los PQC KEM adicionales aumenta aún más la resistencia cuántica, pero añade capacidad de negociación y aumenta el tamaño de los paquetes IKEv2.

RFC 9370 permite omitir rondas de intercambio de claves adicionales. Para las rondas omitidas, se pueden dejar en blanco o establecer en **None (Ninguno)**.

El orden de los PQC en la Ronda de intercambio de claves adicionales establece la preferencia. El PQC enumerado en la parte superior es preferente y se selecciona si el dispositivo de terminación VPN en el otro lado del túnel lo admite. Si desea negociar el PQC más fuerte que ambas partes puedan

apoyar, coloque el PQC de mayor nivel de seguridad en la parte superior de la lista en cada Ronda de intercambio de claves adicional.

Los dispositivos de terminación VPN en ambos lados del túnel deben configurarse con el mismo PQC y fuerza de seguridad para minimizar los problemas de interoperabilidad. Para proteger la información confidencial durante largos períodos de tiempo, seleccione un PQC con una fuerza de seguridad equivalente al nivel 3 o superior.

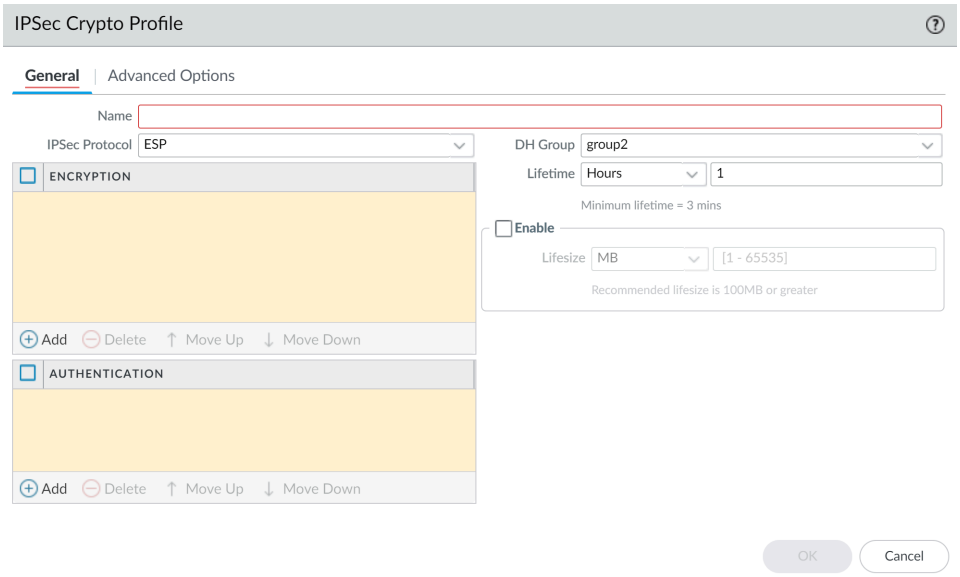


STEP 9 | Haga clic en **OK (Aceptar)** para crear el perfil criptográfico de IKE.

STEP 10 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico de IPSec)** y luego **Add (Añadir)** para añadir un nuevo perfil.

STEP 11 | Configure la configuración **General** y seleccione los componentes criptográficos para el protocolo IPSec ESP (encriptación, autenticación, grupo DH, vida útil).

Seleccione una configuración criptográfica clásica fuerte para elevar la resistencia cuántica. Grupo DH 20 o superior, AES-256-GCM, SHA384 o superior y actualice las claves con más frecuencia utilizando la duración de la clave.



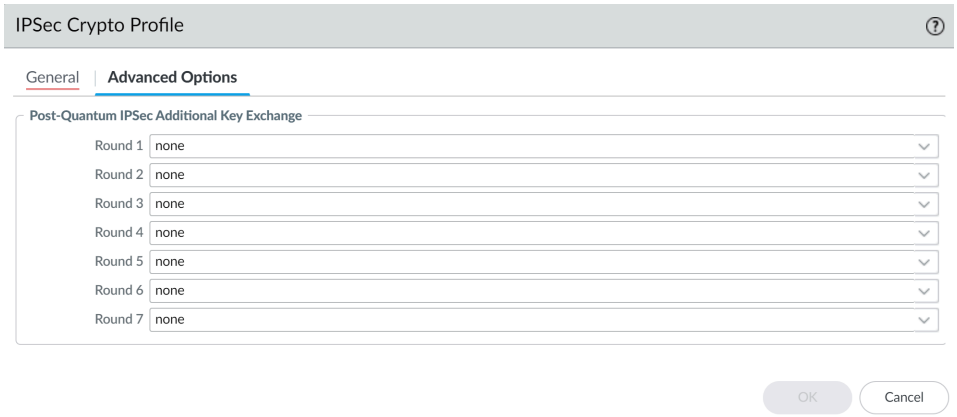
STEP 12 | Seleccione las **Advanced Options (Opciones avanzadas)** y configure las rondas opcionales de **Post-Quantum IPSec Additional Key Exchange (Intercambio de claves adicionales de IPSec poscuántico)**.

Se permite un máximo de siete **Additional Key Exchange Rounds (Rondas adicionales de intercambio de claves)** (ronda 1-7) y solo se permite un PQC KEM por ronda. Como mínimo, se requiere un PQC KEM para añadir resistencia cuántica. Añadir mecanismos de encapsulación de

claves (KEM) de PQC adicionales aumenta aún más la resistencia cuántica, pero añade sobrecarga de negociación y aumenta el tamaño de los paquetes de regeneración de IPSec.

Ambos lados del túnel IPSec deben configurarse con el mismo nivel de PQC y de seguridad en cada ronda de intercambio de claves adicional. Si hay un desajuste, la operación de regeneración de clave falla.

Para proteger la información confidencial durante largos períodos de tiempo, seleccione un PQC con una fuerza de seguridad equivalente al nivel 3 o superior.



STEP 13 | Haga clic en **OK (Aceptar)** para crear el Perfil criptográfico de IPSec.

STEP 14 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Si no es el administrador de ambos pares IKEv2, comunique la puerta de enlace IKEv2, el perfil criptográfico IKE y la información del perfil criptográfico IPSec al administrador del par para su instalación en su dispositivo homólogo.

Ejemplo de configuración de RFC 8784 de IKEv2 Post-Quantum

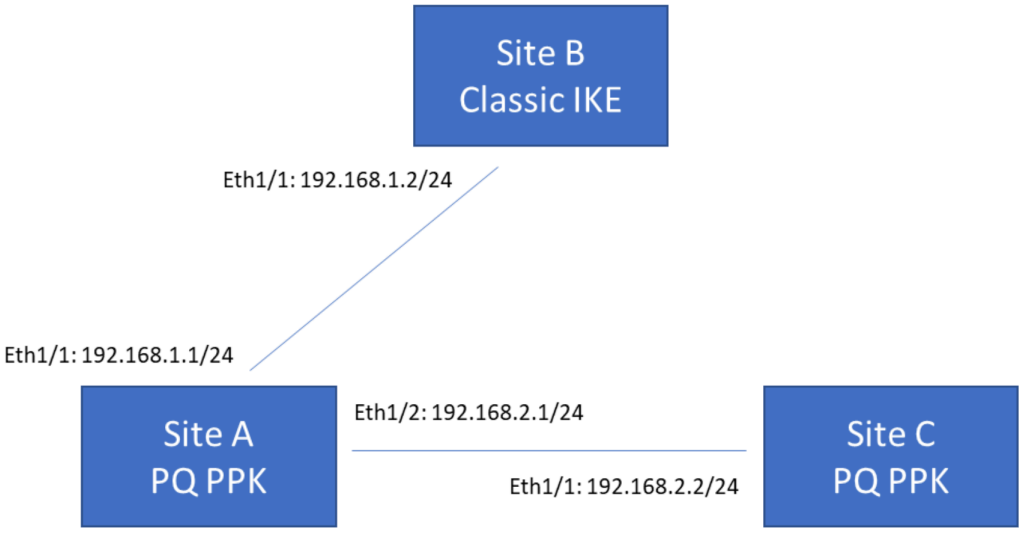
¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS	❑ PAN-OS 11.1 o posterior.

En este ejemplo se proporciona una topología y una configuración de VPN poscuántica IKEv2 básicas. Incluye dos sitios que admiten RFC 8784 (VPN poscuánticas que resisten los ataques de ordenadores cuánticos y criptografía cuántica) y un sitio que no es compatible con RFC 8784.

Cuando un cortafuegos que admite RFC 8784 se comunica con un cortafuegos que también admite RFC 8784, los dispositivos utilizan la configuración poscuántica. El intercambio de claves utiliza claves precompartidas poscuánticas (PPK PQ) que se comparten fuera de banda de la conexión, por lo que la PPK PQ nunca se expone durante el protocolo de enlace IKE. Los cortafuegos mezclan las PPK PQ con el material de clave clásico Diffie-Hellmann (DH) (que se transmite durante el protocolo de enlace IKE) para crear una clave que no se basa en números primos y, por lo tanto, no puede ser descifrada por Algoritmo de Shor. Esto permite a los cortafuegos crear una clave resistente a la cuántica para ayudar a protegerse frente a los ataques Harvest Now, Decrypt Later, en el que los atacantes roban datos que no pueden descifrar ahora y los almacenan hasta que puedan usar un ordenador cuántico criptográficamente relevante (CRQC) para descifrarlos.

Cuando un cortafuegos que admite RFC 8784 se comunica con un cortafuegos que no admite RFC 8784, el cortafuegos RFC 8784 puede recurrir al intercambio de claves DH clásico. Si eso sucede, los cortafuegos no se mezclan en un PPK PQ y solo usan el material de clave DH para crear la clave. Es importante comprender que el tráfico VPN en este caso es vulnerable a los ataques Harvest Now, Decrypt Later.

Esta topología de ejemplo simple consta de tres cortafuegos ubicados en diferentes sitios, conectados por VPN IKEv2. Dos de los cortafuegos admiten RFC 8784 y un cortafuegos no admite RFC 8784.



En este ejemplo:

- **Sitio A** es compatible con RFC 8784. Su conexión con el Sitio B es Eth1/1: 192.168.1.1/24 y su conexión al Sitio C es Eth1/2: 192.168.2.1/24. El sitio A requiere dos puertas de enlace IKEv2, una para conectarse con el sitio B y otra para conectarse con el sitio A.
- **Sitio B** solo es compatible con las VPN IKEv2 clásicas y no es compatible con RFC 8784. Su conexión con el Sitio A es Eth1/1: 192.168.1.2/24. El sitio B requiere una puerta de enlace IKEv2 para conectarse al sitio A. La configuración de la puerta de enlace IKEv2 del sitio B no incluye PPK PQ porque el sitio B no admite RFC 8784.
- **Sitio C** es compatible con RFC 8784. Su conexión con el Sitio A es Eth1/1: 192.168.2.2/24. El sitio C requiere una puerta de enlace IKEv2 para conectarse al sitio A.

Cada par VPN IKEv2 que admita RFC 8784 debe tener exactamente el mismo conjunto de PPK PQ (pares de cadenas KeyID más secreto de PPK) instalados y activados. La conexión se anula si el PPK PQ seleccionado no está disponible en ambos pares.

El KeyID identifica la cadena de secreto de PPK.

Los pares IKEv2 transmiten el KeyID durante el protocolo de enlace IKEv2, pero la cadena secreto de PPK se comparte fuera de banda y se instala en cada par por separado, ya sea insertada por Panorama o instalada manualmente. La cadena secreto de PPK nunca se envía en el protocolo de enlace ni se ve en el túnel IKEv2 resultante. En su lugar, los pares IKEv2 utilizan el KeyID para buscar localmente la cadena secreto de PPK y mezclarla con el material de la clave DH para producir la clave de cifrado poscuántica.

Para configurar las VPN de IKEv2 para la topología de ejemplo, vaya a **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)**:

STEP 1 | Configure las propiedades generales de la puerta de enlace VPN IKEv2 para los sitios A, B y C como lo haría con cualquier otra puerta de enlace de IKE.

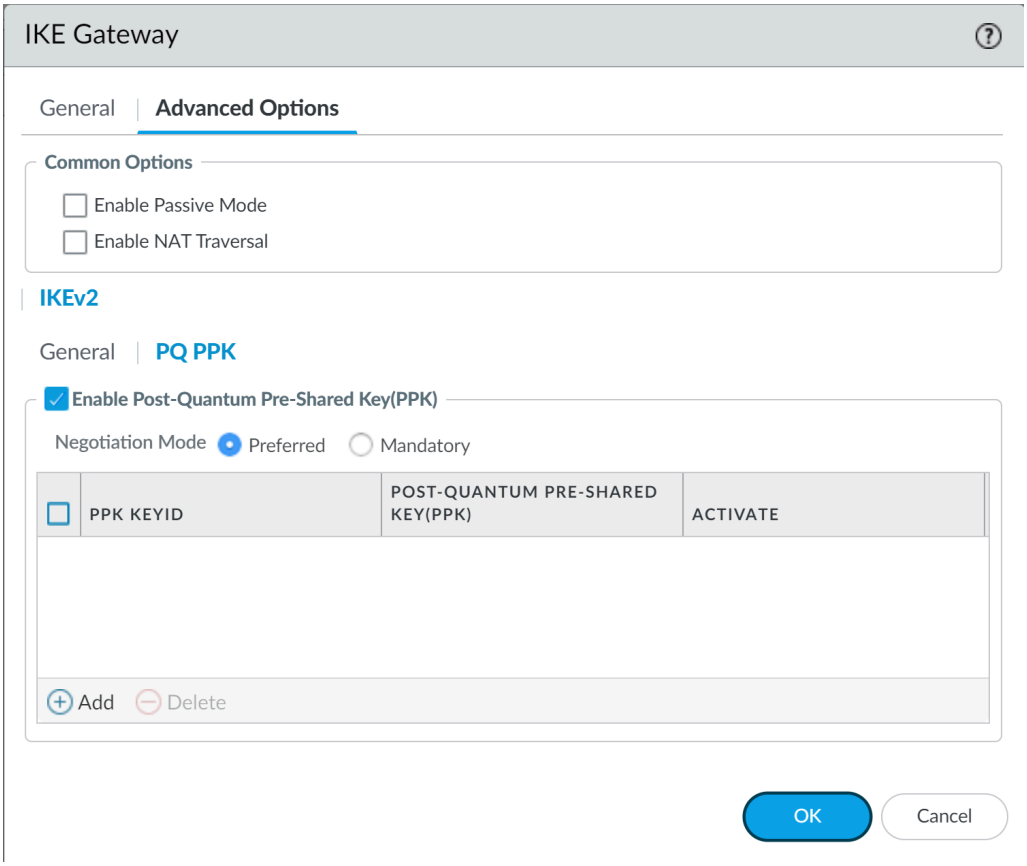
En la pestaña **General**, configure las direcciones, la autenticación y otra información general de la puerta de enlace de IKE. Establezca la **Version (Versión)** en **IKEv2 mode only (Solo el modo IKEv2)** para una mejor seguridad. IKEv1 se considera un protocolo débil y no es compatible con las VPN poscuánticas RFC 8784.

*La clave previamente compartida que configure en la pestaña**General** no es la clave precompartida postcuántica que resiste los ataques basados en cuántica. Esta se utiliza para la autenticación simétrica a través del túnel.*

STEP 2 | Configurar **Advanced Options (Opciones avanzadas)** comunes y generales como modo pasivo, NAT transversal y el perfil criptográfico de IKE para los tres sitios.

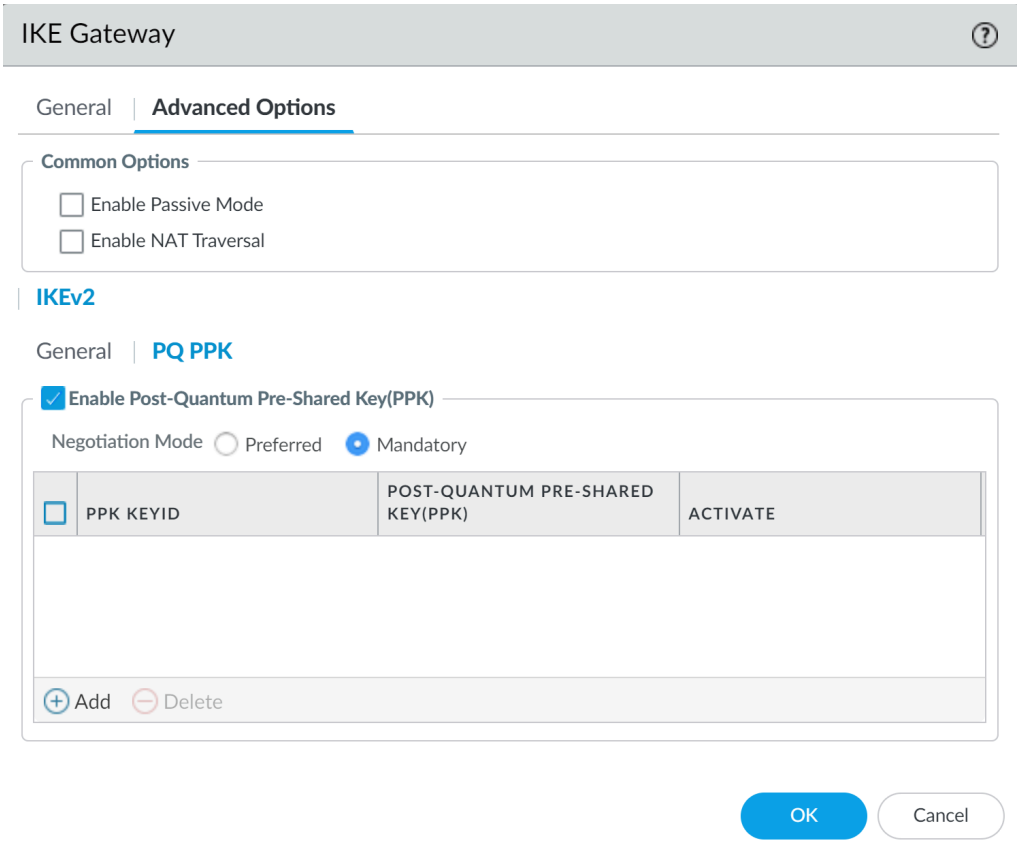
STEP 3 | En la pestaña **Advanced Options (Opciones avanzadas)** > **PQ PPK (PPL PQ)**, seleccione **Enable Post-Quantum Pre-Shared Key (PPK) [Habilitar clave postcuántica precompartida (PPK)]** para la VPN IKEv2 del sitio A al sitio C y en el sitio C VPN IKEv2 al sitio A.

Dado que el sitio B no admite RFC 8784, no es necesario **Enable Post-Quantum Pre-Shared Key (PPK) [Habilitar la clave precompartida poscuántica (PPK)]** en la configuración de puerta de enlace de IKE del sitio B o en la configuración de VPN de IKEv2 del sitio A al sitio B.



Cuando selecciona **Enable Post-Quantum Pre-Shared Key (PPK) [Habilitar la clave precompartida poscuántica (PPK)]**, el ajuste predeterminado de **Negotiation Mode (Modo de negociación)** es **Preferred (Preferido)**, lo que significa que las conexiones que no pueden admitir RFC 8784 recurren a la criptografía clásica. (En el modo **Mandatory (Obligatorio)**, si el par no es compatible con PPK PQ , el cortafuegos anula la conexión).

STEP 4 | Establezca el **Negotiation Mode (Modo de negociación)** en las VPN de IKEv2 del sitio A al sitio C y del sitio C al sitio A en **Mandatory (Obligatorio)**.



Usar **Mandatory (Obligatorio)** como el **Negotiation Mode (Modo de negociación)** garantiza que el sitio A y el sitio C siempre configuren VPN resistentes a la tecnología cuántica en lugar de las VPN clásicas cuando negocien túneles VPN. Use **Mandatory (Obligatorio)** cuando esté seguro de que los pares admiten RFC 8784. Si no está seguro, use el modo **Preferido** para que el cortafuegos pueda recurrir a las VPN IKEv2 clásicas si el par no es compatible con RFC 8784, por ejemplo, cuando se empareja con dispositivos fuera de la empresa que no controla.

STEP 5 | Configure PPK PQ activos para la conexión IKEv2 del sitio A al sitio C y para la conexión IKEv2 del sitio C al sitio A. Cuando el sitio A y el sitio C activan la conexión IKEv2, seleccionan entre estos

PPK PQ activos y mezclan el PPK PQ elegido con el material de la clave DH para crear una clave segura que no se base en números primos.

No hay ninguna configuración poscuántica para la comunicación del sitio A al sitio B o para la comunicación del sitio B al sitio A porque el sitio B no admite RFC 8784.

Los pares IKEv2 del sitio A y del sitio C deben tener la misma configuración exacta de PPK PQ activos.

- Si Panorama gestiona ambos pares IKEv2, puede crear la configuración en Panorama e insertarla en los cortafuegos gestionados.
- Si Panorama no gestiona ambos pares IKEv2 y diferentes administradores controlan los pares, comunique la PPK PQ al otro administrador de forma segura, como con correo electrónico cifrado, y almacene la clave de forma segura.

Puede asignar el nombre que desee al KeyID de cada PPK PQ. Puede configurar manualmente el secreto de PPK que empareje con el KeyID para cada PPK PQ o el cortafuegos puede generar un secreto de PPK seguro. En este ejemplo se muestra cómo utilizar ambos métodos.

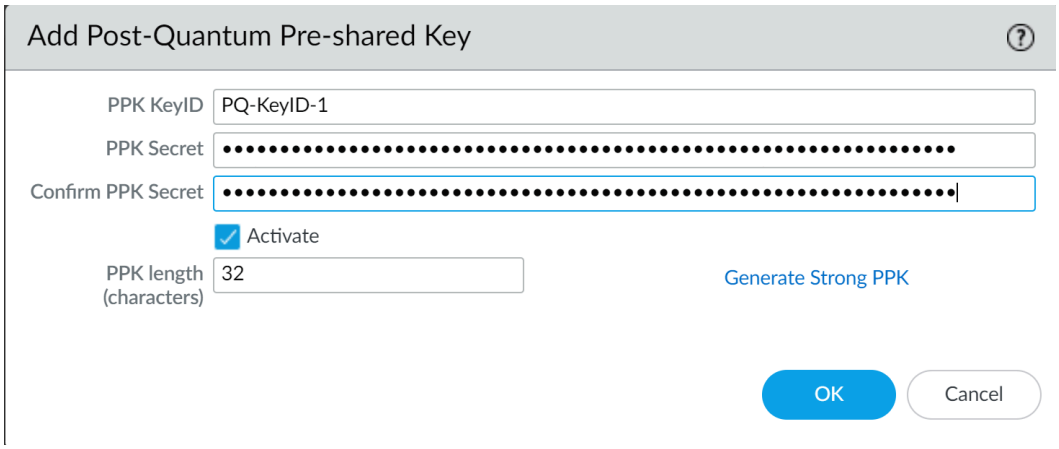
Para crear la PPK PQ con un secreto de PPK configurado manualmente:

1. Debe **Add (Añadir)** un PPK PQ.
2. En el cuadro de diálogo **Add Post-Quantum Pre-shared Key (Añadir clave precompartida postcuántica)**, introduzca el nombre de **PPK KeyID (KeyID de PPK)**. En este ejemplo, el nombre es **`PQ-KeyID-1`**.
3. Escriba (o copie y pegue de otra fuente) exactamente la misma cadena ASCII en **PPK KeyID (KeyID de PPK)** y seleccione **Confirm PPK Secret (Confirmar el secreto de PPK)**.

   Almacene la PPK PQ (el ID de clave y su secreto de PPK) de forma segura. En el caso de los secretos de PPK introducidos manualmente, el secreto nunca se muestra en texto no cifrado. Si pierde el secreto de PPK, no podrá recuperarlo. (Puede eliminar la PPK PQ y, a continuación, configurar una nuevo).

   Si el **PPK KeyID (KeyID de PPK)** y **Confirm PPK Secret (Confirmar el secreto de PPK)** no coinciden, el mensaje de error `Secreto de PPK y Confirmar que el secreto de PPK no coincide` aparece. Como práctica recomendada, especifique un secreto de PPK aleatorio que tenga al menos 64 caracteres (32 bytes o 256 bits de entropía) de longitud para crear una clave segura. De forma predeterminada, la nueva clave está activa. Si no desea utilizar la clave en la negociación entre pares de IKE, anule la selección **Activate (Activar)**. Si desactiva el PPK PQ en un par, también debe desactivarlo en el otro par. En el ejemplo siguiente

se muestra una clave segura de 64 caracteres (las claves introducidas manualmente nunca se muestran en texto no cifrado):



*El campo **PPK length (characters) [Longitud de PPK (caracteres)]** solo se aplica a las claves que el cortafuegos genera automáticamente. No controla la longitud de las cadenas de secreto de PPK configuradas manualmente.*

4. Haga clic en **OK (Aceptar)** para instalar el PPK PQ configurado manualmente.
5. Si Panorama gestiona ambos pares, puede crear la configuración en Panorama e insertarla en los cortafuegos gestionados. Si Panorama no gestiona ambos pares y un administrador diferente

controla el par VPN, comunica de forma segura la PPK PQ a ese administrador, quien lo instala en el par.

Para crear la PPK PQ con un secreto de PPK que genera el cortafuegos:

1. Debe **Add (Añadir)** un PPK PQ.
2. En el cuadro de diálogo **Add Post-Quantum Pre-shared Key (Añadir clave precompartida postcuántica)**, introduzca el nombre de **PPK KeyID (KeyID de PPK)**. En este ejemplo, el nombre es **`PQ-Key-ID-2`**.
3. Establezca la **PPK length (characters) [Longitud de PPK (caracteres)]** en al menos 64 caracteres (32 bytes o 256 bits de entropía) de longitud para crear una clave segura.
4. Haga clic en **Generate Strong PPK (Generar PPK fuerte)**.

   El cortafuegos genera un secreto de PPK hexadecimal aleatorio y seguro de la longitud configurada en **PPK length (characters) [Longitud de PPK (caracteres)]**.
5. Resalte y copie la cadena secreta de PPK.

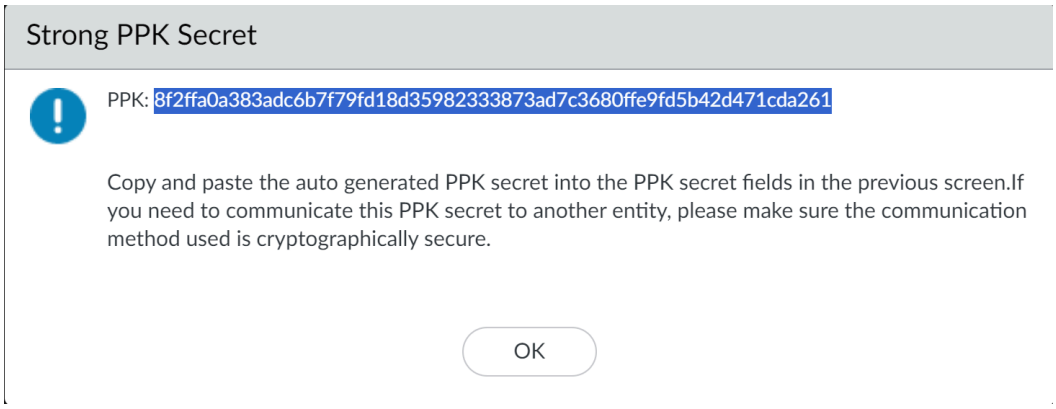
   Copie solo el secreto hexadecimal. No copie los caracteres `PPK:` iniciales. Por ejemplo, si el secreto generado se muestra como:

   `PPK:`
   `38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

   Solo copie:

   `38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

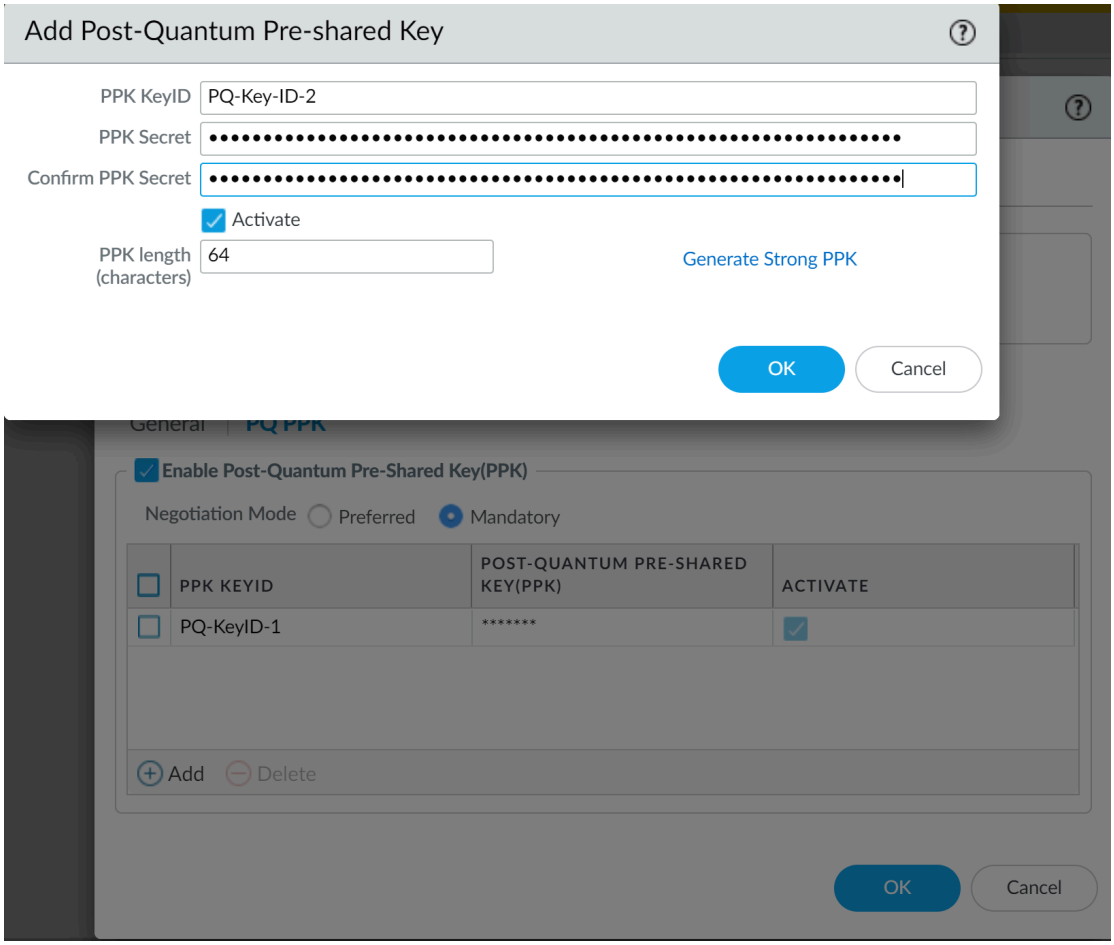
   El `PPK:` inicial no forma parte de la cadena secreta.



Almacene de forma segura el secreto de PPK copiado que generó el cortafuegos. Después de hacer clic en **OK (Aceptar)**, el cortafuegos nunca vuelve a mostrar el secreto de PPK en texto no

cifrado. Si no copia y almacena de forma segura el secreto de PPK ahora, no lo tendrá y deberá eliminar esta PPK PQ y configurar uno nuevo.

6. Con el secreto de PPK copiado aún en el portapapeles o disponible para copiar desde el almacenamiento seguro, haga clic en **OK (Aceptar)**. Si no copió el secreto de PPK, genere otro secreto de PPK seguro y asegúrese de copiarlo y almacenarlo de forma segura.
7. Pegue la cadena secreta de PPK copiada en ambos campos **PPK Secret (Secreto de PPK)** y **Confirm PPK Secret (Confirmar secreto de PPK)** en **Add Post-Quantum Pre-Shared Key (Añadir clave precompartida poscuántica**.

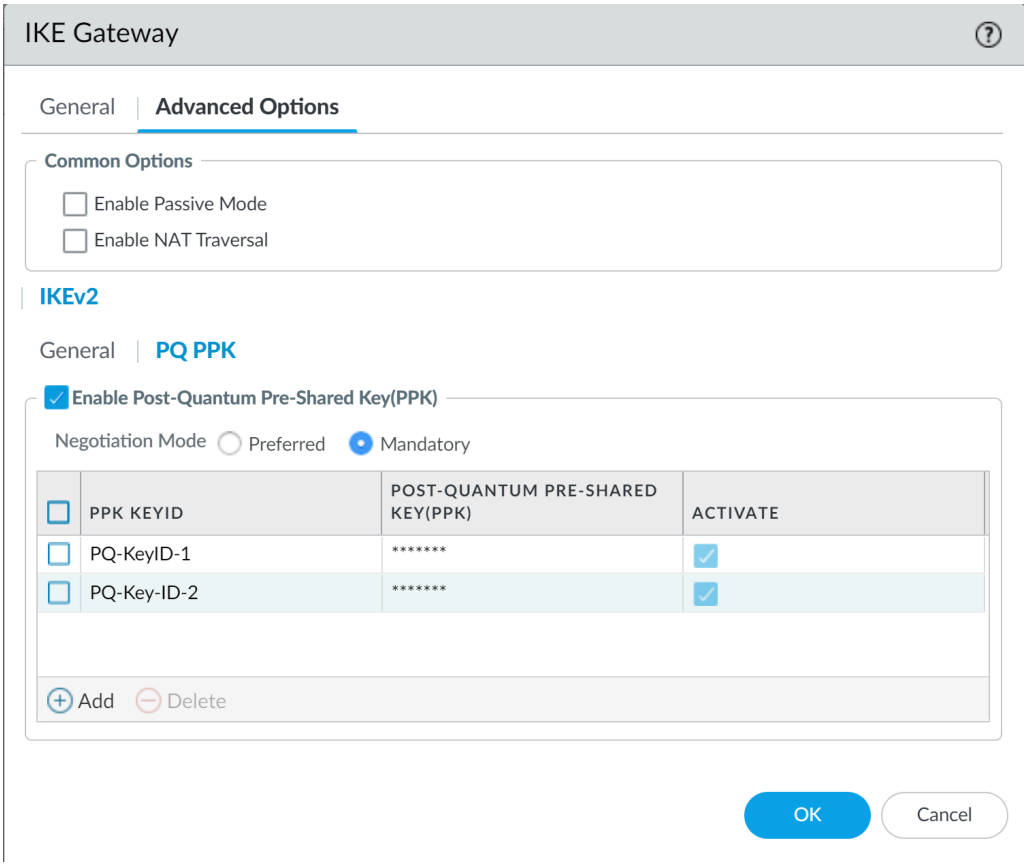


De forma predeterminada, la nueva clave está activa. Si no desea utilizar la clave en la negociación entre pares de IKE, anule la selección **Activate (Activar)**. Si desactiva el PPK PQ en un par, también debe desactivarlo en el otro par.

8. haga clic en **OK (Aceptar)** para instalar el PPK PQ generado por el cortafuegos.
9. Si Panorama gestiona ambos pares, puede crear la configuración en Panorama e insertarla en los cortafuegos gestionados. Si Panorama no gestiona ambos pares y un administrador diferente

controla el par VPN, comunica de forma segura la PPK PQ a ese administrador, quien lo instala en el par.

Para el sitio A y el sitio C, las dos PPK PQ creadas en este ejemplo se enumeran como PPK PQ activas en modo **Obligatorio**.



El secreto de PPK ahora está oculto y nunca se muestra en texto sin cifrar. Las VPN IKEv2 entre el sitio A y el sitio C ahora implementan RFC 8784 para resistir ataques cuánticos. Las VPN IKEv2 entre el sitio A y el sitio B siguen utilizando los intercambios de claves DH clásicos y siguen siendo vulnerables a los ataques Harvest Now, Decrypt Later.

Si el sitio B de este ejemplo se actualizara para admitir RFC 8784, seguiría el mismo proceso para actualizar las VPN IKEv2 del sitio A al sitio B y del sitio B al sitio A.

