paloalto TECHDOCS

Administration de la sécurité quantique

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

Concepts de sécurité quantum

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Les ordinateurs quantiques (QC) menacent la sécurité des réseaux et des données. Lorsque le développement des QC atteint un niveau de maturité permettant de produire des ordinateurs quantiques pertinents sur le plan cryptographique (CRQC), spécialement conçus pour casser le décryptage, de nombreux cryptogrammes classiques qui étaient considérés comme sûrs ne seront plus en mesure d'empêcher les attaquants de décrypter vos données. Cela signifie que votre infrastructure à clé publique (PKI) basée sur la cryptographie classique sera vulnérable aux attaques post-quantiques. La menace est immédiate, en particulier pour les données à longue durée de vie, en raison des attaques Harvest Now, Decrypt Later dans lesquelles les attaquants obtiennent les données cryptées et les stockent jusqu'à ce qu'ils disposent d'un CRQC capable de les décrypter.

La résistance aux attaques basées sur le calcul quantique commence par le renforcement de la clé créée lors de l'échange de clés IKEv2 afin de protéger vos VPN et par la compréhension de votre cryptographie actuelle et de vos cryptographies post-quantiques (PQC). Les solutions de Palo Alto Networks pour résister aux attaques quantiques sont basées sur des normes ouvertes afin de favoriser et d'assurer une interopérabilité avec d'autres équipements conformes aux normes.

La première étape consiste à mettre en œuvre la RFC 8784 pour créer des VPN IKEv2 résistants au quantique, comme décrit dans ce document. Les VPN résistants au quantique peuvent empêcher les attaquants d'enregistrer le matériel des clés cryptées essentielles et de décrypter les données même s'ils réussissent à voler les données cryptées. La RFC 8784 fournit une transition résistante au quantique par rapport à la cryptographie classique d'aujourd'hui d'une manière simple qui ne nécessite aucune mise à niveau de la cryptographie et est considérée comme le moyen le plus simple d'introduire une résistance quantique à vos communications VPN.

La deuxième étape consiste à mettre en œuvre la RFC 9370 seule ou avec la RFC 8784 pour créer des VPN IKEv2 résistants au quantique à l'aide de mécanismes d'échange de clés (KEM) multiples capables de combiner à la fois les technologies KEM classiques et PQC. Cette solution est également connue sous le nom de clé hybride post-quantique IKEv2 et elle utilise les nouveaux algorithmes PQC de remplacement qui ne sont pas vulnérables à une attaque quantique qui utilise l'algorithme de Shor.

Ce chapitre décrit les QC, la menace qu'ils représentent pour la sécurité des données, ce que vous pouvez faire dès maintenant en créant des VPN IKEv2 résistants aux technologies quantiques, et comment planifier et préparer la migration vers des VPN et des PQC post-quantiques.

La menace du calcul quantique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Les mécanismes de cryptage de l'infrastructure à clé publique (PKI) et d'échange de clés IKE utilisent largement des cryptographies classiques comme Diffie-Hellman (DH), la cryptographie à courbe elliptique (ECC) et l'échange de clés Diffie-Hellman basé sur les courbes elliptique (ECDH). Les ordinateurs quantiques (QC) sont susceptibles de casser ces technologies dans les 5 à 15 ans après la normalisation par le NIST des premières cryptographies post-quantiques (PQC).

Les VPN IKEv2 post-quantiques basés sur les normes ouvertes RFC 8784, RFC 9242 et RFC 9370 résistent aux attaques basées sur le calcul quantique et les PQC. Avec la RFC 8784, au lieu d'envoyer le matériel de la clé à l'homologue IKE lors de l'établissement de la connexion de couplage, les administrateurs configurent et partagent le matériel de la clé séparément, hors bande. Si les attaquants volent les données, ils ne peuvent pas les décrypter parce qu'ils n'ont pas le matériel de la clé. La RFC 9370 ajoute sept tours KEM supplémentaires facultatifs à IKEv2 pour permettre la création de clés de cryptage hybrides formulées avec différents types de technologies KEM. Pour décoder la clé hybride, tous les KEM utilisés pour créer la clé devraient être compromis. Les solutions de Palo Alto Networks pour résister aux attaques quantiques sont basées sur des normes ouvertes afin de favoriser et d'assurer une interopérabilité avec d'autres équipements conformes aux normes.

Le danger le plus immédiat réside dans les attaques Harvest Now, Decrypt Later, où les attaquants volent des données (au repos ou en transit) qu'ils ne peuvent pas décrypter maintenant et les stockent jusqu'à ce qu'un ordinateur quantique pertinent sur le plan cryptographique (CRQC) puisse les décrypter. Un CRQC est un QC optimisé pour utiliser des algorithmes quantiques afin de pouvoir casser le cryptage en quelques secondes au lieu d'avoir besoin des millions d'années d'un superordinateur classique. Les données les plus exposées au risque sont celles qui ont une longue durée de vie et qui seront encore pertinentes lorsque les CRQC seront disponibles.

- Qu'est-ce qu'un ordinateur quantique ?
- Comment la menace quantique affecte-t-elle mon réseau ?
- Que faire maintenant pour atténuer les attaques de récolte de données

Qu'est-ce qu'un ordinateur quantique ?

Les ordinateurs quantiques (QC) sont essentiellement la prochaine génération de plateformes de supercalcul. Les QC utilisent les lois de la mécanique quantique pour réduire considérablement le temps nécessaire pour traiter les données et exécuter des algorithmes, y compris des algorithmes capables de casser le décryptage classique. Les opérations qui prendraient des centaines ou des milliers d'années à un ordinateur classique ne prennent quelques secondes, voire quelques microsecondes, avec un QC Au lieu d'être basés sur des bits classiques (zéros et uns) qui augmentent la puissance d'un superordinateur de manière linéaire, les QC utilisent des qubits qui sont basés sur des photons polarisés (lumière) et qui augmentent exponentiellement la puissance de traitement d'un QC.

Il existe plusieurs façons de créer des qubits, mais la qualité et l'efficacité des qbits dépend de la méthode suivie. Plus la qualité des qubits est élevée, plus le QC est rapide et efficace. En raison de sa nature

quantique, un qubit représente deux états à la fois et ces états peuvent être répliqués sur de grandes distances. Cela est dû aux effets quantiques de la superposition et de l'intrication :

- **Superposition** : un qubit peut représenter à la fois un « un » et un zéro. La combinaison des qubits entraîne une augmentation du nombre d'états que les qubits peuvent représenter car le nombre d'états augmente à un rythme de 2**n, où « n » est le nombre de qubits. Ainsi, deux qubits peuvent représenter quatre états (2**2), trois qubits peuvent représenter huit états (2**3), quatre qubits peuvent représenter 16 états (2**4), etc.

  À mesure que la densité de qubits (le nombre de qubits qui tiennent sur une puce) augmente, le nombre d'états représentés par les qubits combinés augmente de manière exponentielle. Plus la qualité des qubits est bonne, plus le nombre combiné de qubits se rapproche d'une véritable échelle exponentielle. Lorsque des qubits de faible qualité (bruyants) sont combinés, ils n'augmentent pas le nombre d'états de façon exponentielle, mais ils l'augmentent quand même de façon significative par rapport à un ordinateur classique. À mesure que la qualité des qubits s'améliore, les QC se rapprochent de plus en plus d'une véritable escalade exponentielle du nombre d'états représentés.
- **Intrication** : l'intrication est une liaison quantique entre les qubits. Les qubits intriqués génèrent les mêmes résultats en exécutant le même algorithme quantique sur eux, peu importe où ils se trouvent, même si les qubits sont à l'autre bout du monde les uns des autres. Ainsi, si vous exécutez un algorithme particulier sur des qubits intriqués situés à Bangalore (Inde) et Los Angeles (États-Unis), les qubits intriqués dans ces emplacements donnent le même résultat. Le mécanisme exact par lequel l'intrication quantique fonctionne est inconnu.

Il existe trois types de QC :

- **Recuits quantiques** : ils sont disponibles dès aujourd'hui. Ce sont les QC les moins puissants avec les cas d'utilisation les plus étroits. Cependant, les attaquants peuvent les utiliser pour factoriser de grands nombres à l'aide d'algorithmes quantiques, ce qui permet de casser le cryptage asymétrique.
- **Simulateurs quantiques analogiques** : ils résolvent des problèmes de physique qui dépassent les capacités des ordinateurs classiques, tels que la chimie quantique, les sciences des matériaux, les problèmes d'optimisation, la factorisation de grands nombres, l'échantillonnage et la dynamique quantique.
- **Ordinateur quantique universel** : ce sont les QC les plus difficiles à construire parce qu'ils nécessitent de nombreux qubits physiques. Ils permettent de résoudre le plus grand nombre de cas d'utilisation et plusieurs entreprises prévoient de les commercialiser d'ici la fin de la décennie. Quand ils seront développés, ces ordinateurs seront des CRQC.

Les QC créent un espace multidimensionnel composé de nombreux qubits intriqués dans lesquels résoudre des problèmes complexes. Par exemple, les ordinateurs classiques prennent chaque élément d'une base de données, le traitent, puis le combinent avec d'autres éléments après avoir traité tous les éléments. Les QC créent un algorithme qui permet de résoudre chaque état et résultat que vous recherchez. Ils font passer toute la base de données dans l'algorithme de manière simultanée, en analysant simultanément les données pour chaque résultat. Cela rend les QC potentiellement des millions de fois plus rapides que les ordinateurs classiques et c'est l'une des raisons pour lesquelles ils sont excellents pour résoudre des problèmes mathématiques complexes, comme casser le cryptage.

Comment la menace quantique affecte-t-elle mon réseau ?

L'augmentation considérable de la puissance de traitement et de la vitesse des QC menace de remettre en cause les méthodes classiques de cryptage des données, ce qui pourrait compromettre votre infrastructure à clé publique (PKI).

La menace la plus immédiate réside dans les attaques « Harvest Now, Decrypt Later » qui volent vos données cryptées avec l'intention d'utiliser un CRQC pour les décrypter à l'avenir. Une fois que les attaquants volent vos données et le matériel de la clé classique, il n'y a aucun moyen de les empêcher de décrypter les données à l'avenir à l'aide d'un CRQC. Si les données volées sont toujours valides à ce moment-là, elles seront compromises.

Le cryptage asymétrique classique est basé sur les nombres premiers et repose sur la difficulté de factoriser des nombres complexes pour obtenir ces nombres premiers. Un algorithme quantique appelé algorithme de Shor peut factoriser des nombres complexes et résoudre les problèmes de logarithme discret. L'algorithme de Shor menace la sécurité de la PKI, qui est basée sur deux très grands nombres premiers pour produire la clé. Cependant, l'algorithme de Shor ne peut pas casser la sécurité de la PKI en moins de millions d'années en utilisant un ordinateur classique. Sans les CRQC, l'algorithme de Shor ne représentait pas une menace. Cependant, étant donné la puissance de traitement d'un CRQC, l'algorithme de Shor peut factoriser des nombres complexes et décoder le cryptage asymétrique classique (comme le matériel d'échange de clés nécessaire pour décrypter les données) en quelques secondes ou moins. C'est pourquoi les attaques de type « Harvest Now, Decrypt Later » sont une menace immédiate.

Les conséquences d'une rupture du cryptage classique incluent la compromission de la sécurité des cryptographies classiques de la PKI que l'on croyait sécurisées, telles que Diffie-Hellman (DH), la cryptographie à courbe elliptique (ECC) et l'échange de clés Diffie-Hellman basé sur les courbes elliptique (ECDH). L'échange de clés présente un grand risque et c'est pourquoi vous devez configurer des VPN IKEv2 post-quantiques afin de sécuriser l'échange de clés.

Les certificats sont à la base de l'établissement de la confiance entre deux terminaux. Cependant, les CRQC peuvent également compromettre le RSA, qui est utilisé pour créer et sécuriser des certificats numériques. Cela signifie que les attaquants peuvent voler ou usurper l'identité de signatures numériques avec un CRQC, de sorte que le serveur auquel vous pensez vous connecter pourrait être en fait le serveur d'un attaquant. La capacité d'agir de la sorte pourrait être disponible dès la prochaine décennie.

En outre, la puissance de traitement par force brute des QC signifie que le cryptage symétrique n'est pas sûr non plus. L'algorithme de Grover est un algorithme de recherche quantique non structurée, accéléré quadratiquement, qui trouve l'entrée unique qui produit une valeur de sortie particulière. L'algorithme de Grover cible la cryptographie symétrique et les fonctions de hachage. Il divise essentiellement par deux la puissance de cryptage des algorithmes AES. Ainsi, si vous utilisez un cryptage AES-128 bits, l'algorithme de Grover le réduit à un cryptage de 64 bits. Comme les ordinateurs classiques ne disposent pas d'une puissance de traitement suffisante, ils ne peuvent pas utiliser l'algorithme de Grover pour casser le cryptage symétrique. Cependant, lors de l'utilisation d'un QC, l'algorithme de Grover est capable de casser le cryptage AES-128 bits.

En raison de la vulnérabilité du cryptage AES-128 bits à l'algorithme de Grover, utilisez le cryptage AES-256 bits, que l'algorithme de Grover ne pourra pas casser à court ou à moyen terme.

Pour aider à protéger les fonctions de hachage, utilisez SHA-384 au minimum.

Les cryptographies post-quantiques (PQC) sont disponibles aujourd'hui et la plupart des personnes intéressées par la sécurité sont en mesure de télécharger et de configurer des PQC, qui ne peuvent pas être décryptés. Si vous autorisez la présence de PQC non autorisées sur votre réseau, un mauvais acteur interne pourrait introduire des PQC dans votre réseau. Si cela se produit, vous n'avez aucune visibilité sur le trafic qui utilise une PQC et aucune visibilité sur les menaces dans ce trafic. Utilisez les fonctionnalités de décryptage pour détecter les PQC non autorisées sur votre réseau et bloquer automatiquement le trafic qui utilise des PQC.

Que faire maintenant pour atténuer les attaques de récolte de données

Prenez ces mesures dès maintenant pour résister aux attaques post-quantiques de type « Harvest Now, Decrypt Later ». Examinez vos connexions VPN et renforcez-les :

- Conformez-vous à la RFC 6379 pour *Suites de chiffrement Suite B pour IPsec* pour mettre à niveau vos connexions VPN vers des suites de cryptage difficiles. Utilisez Suite-B-GCM-256 et évitez les algorithmes AES 128 bits plus faibles, qui sont vulnérables à l'algorithme de Grover.
- Mettez à niveau votre CA vers des tailles de clé RSA 4K pour atténuer les attaques par force brute capables de décoder des clés de plus petite taille et migrez votre authentification de certificat VPN vers de nouveaux certificats.
- Passez à des tailles de hachage SHA à bits plus élevés telles que SHA-384 et SHA-512. Cessez d'utiliser des hachages faibles tels que MD5 et SHA-1.
- Mettez en œuvre les RFC 8784 et/ou RFC 9242 et RFC 9370 pour créer des VPN post-quantiques résistants aux attaques quantiques.

En outre, vérifiez vos connexions SSL/TLS et renforcez-les :

- Mettez à niveau les connexions SSL/TLS vers des suites de cryptage difficiles; utilisez TLSv1.3 avec des cryptages Perfect Forward Secrecy (Confidentialité de transmission parfaite, PFS).
- Tunnelisez les sessions SSL/TLS dans des sessions VPN client à serveur renforcées. Utilisez une application de bureau post-quantique pour prendre en charge le proxy inverse.

Comment la RFC 8784 résiste aux menaces du calcul quantique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

La norme RFC 8784, *Mélange de clés pré-partagées dans le protocole d'échange de clés Internet, version 2 (IKEv2) pour la sécurité post-quantique*, vous permet de créer des VPN IKEv2 résistants aux attaques basées sur des ordinateurs quantiques (QC) et des cryptographies post-quantiques (PQC) aujourd'hui.

L'essence de la RFC 8784 consiste à échanger des clés pré-partagées post-quantiques (PPK PQ) statiques hors bande, séparément de l'échange de clés IKE, et à mélanger le matériel PPK PQ hors bande avec le matériel classique de la clé Diffie-Hellman (DH) qui est transmis en bande pendant l'échange de clés IKEv2. Cela renforce l'échange de clés de deux manières :

- Une clé DH et des variantes de clés DH reposent sur la difficulté de résoudre le problème de logarithme discret, comme la résolution des très grands nombres premiers sur lesquels DH est basé. Cependant, avec l'avènement des ordinateurs quantiques pertinents sur le plan cryptographique (CRQC), les clés DH deviennent vulnérables aux attaques basées sur l'algorithme de Short. La mise en œuvre de la RFC 8784 améliore la force cryptographique de la clé car la clé mixte n'est plus uniquement basée sur la difficulté de résoudre le problème de logarithme discret (par exemple, la résolution de très grands nombres premiers), de sorte que la clé mixte n'est pas vulnérable à l'algorithme de Shor
- Un écouteur ou un intercepteur, ne peut pas récolter tout le matériel de la clé pour le décrypter ultérieurement. La partie DH classique de la clé est envoyée dans l'échange de clés de couplage IKE, mais la PPK PQ que les homologues IKE mélangent avec le matériel de la clé DH n'est jamais transmise pendant l'échange de clés ou dans le VPN après son établissement, donc même avec la partie DH du matériel de la clé, les attaquants ne peuvent pas décrypter les données qui traversent le VPN.

Les homologues IKEv2 savent quel PPK PQ utiliser en fonction d'un ID de clé. Chaque PPK PQ se compose de deux éléments, un ID de clé et un secret pré-partagé. Le secret pré-partagé est le matériel de la clé que vous partagez avec l'homologue hors bande IKEv2. Il n'est jamais transmis en bande avec le matériel de la clé DH ou avec les données après l'établissement du VPN. Au lieu de cela, l'administrateur d'un homologue IKEv2 crée manuellement le secret pré-partagé statique et le communique de manière sécurisée à l'administrateur de l'autre homologue IKEv2, par exemple par messagerie sécurisée ou en le transmettant depuis Panorama. Chaque administrateur programme le secret pré-partagé dans son homologue, de sorte que le secret n'est jamais révélé dans la connexion IKE.

L'ID de clé, qui est transmis en bande lors de l'échange de clés, identifie le secret pré-partagé sur l'homologue IKEv2. L'homologue IKEv2 utilise l'ID de clé pour rechercher le secret pré-partagé et le mélange avec le matériel de la clé DH pour créer un nouveau matériel de clé qui n'est pas basé sur des nombres premiers et ne peut pas être volé par l'écoute clandestine de la communication.

Les deux homologues IKEv2 doivent utiliser exactement les mêmes paires d'ID de clé et de secret PPK pré-partagé. Si les ID de clé et leurs secrets pré-partagés associés ne correspondent pas, la connexion est abandonnée. Si vous configurez plus d'une PPK PQ, les deux homologues IKEv2 doivent avoir exactement le même ensemble d'ID de clé actifs et de secrets pré-partagés. (Palo Alto Networks vous permet de configurer jusqu'à dix PPK PQ actives, mais certains fournisseurs n'autorisent qu'une seule PPK PQ. Il est donc important de comprendre les capacités de votre homologue.

Cette méthode basée sur les normes fournit un moyen facile d'empêcher les attaquants d'écouter clandestinement la connexion et d'intercepter les clés, ce qui leur permettrait de décrypter les données envoyées dans le VPN après son établissement, tout en assurant l'interopérabilité avec d'autres périphériques conformes à la norme. Les avantages de la RFC 8784 comprennent :

- Une norme approuvée avec une prise en charge par plusieurs fournisseurs.
- Ne consomme aucune ressource réseau supplémentaire et n'ajoute pratiquement aucune latence.
- Rétrocompatible, de telle sorte que vous pouvez l'utiliser dans des réseaux où tous les homologues ne prennent pas en charge IKEv2 et où vous ne contrôlez pas tous les homologues.
- La clé n'est plus basée sur des nombres premiers et n'est donc pas vulnérable à l'algorithme de Shor.
- La PPK PQ n'est pas transmise, donc elle ne peut pas être utilisée pour décrypter les données récoltées.
- Recommandé par les agences gouvernementales, y compris le NIAP, la NSA, l'Office fédéral allemand de la sécurité de l'information, et bien d'autres à travers le monde. De plus, la création d'un secret fort et aléatoire de 32 octets ou plus respecte le niveau de sécurité de catégorie 5 du NIST. Veillez à ce que le secret soit fort et aléatoire, à ce qu'il ne suive pas un modèle et ne soit pas sujet aux attaques par dictionnaire.
- Vous pouvez superposer la RFC 8784 avec de futures capacités basées sur des normes telles que les clés hybrides PQC.

Cela permet une adoption plus rapide car les modifications à apporter sont minimes et il n'y a pas de danger d'abandonner des connexions en raison d'une incompatibilité. Cependant, la RFC 8784 présente quelques inconvénients :

- La configuration manuelle des PPK PQ statiques ne peut pas être bien mise à l'échelle pour de nombreux sites, bien que la transmission des PPK PQ depuis Panorama vers des pare-feu gérés puisse aider à atténuer la mise à l'échelle.
- Les PPK PQ doivent être conservées en toute sécurité par tous les administrateurs IKEv2 avec lesquels elles sont partagées. Cela inclut non seulement les administrateurs internes à votre entreprise, mais aussi les administrateurs des partenaires, des fournisseurs et d'autres administrateurs externes avec lesquels vous devez coupler. Le risque vient du fait que les administrateurs écrivent les PPK PQ et les perdent ou se les font voler ou compromettre.
- Il peut être difficile de compter sur les êtres humains pour créer des secrets aléatoires longs et forts qui résistent aux attaques par dictionnaire et autres attaques. La mise en œuvre de Palo Alto Networks vous permet de générer automatiquement de longs secrets hexadécimaux forts au lieu d'avoir à les créer vous-même.

Les VPN IKEv2 basés sur la RFC 8784 sont la première étape recommandée vers une solution contre les PQC et les menaces post-quantiques. Après la normalisation par le NIST des premières PQC, d'autres méthodes qui peuvent fonctionner avec la RFC 8784 amélioreront la résistance aux menaces quantiques, notamment la RFC 9242 et la RFC 9370.

Comment les RFC 9242 et 9370 résistent aux menaces du calcul quantique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.2 ou version ultérieure.

La norme RFC 9242, *Échange intermédiaire dans le protocole d'échange de clé Internet version 2 (IKEv2)*, permet à IKEv2 de transférer de grandes quantités de données dans l'établissement de la Security Association (association de sécurité – SA) IKEv2 pour prendre en charge des échanges de clés PQC multiples pour des tailles de clés plus importantes. La norme RFC 9370, *Échanges de clés multiples dans le protocole d'échange de clés Internet version 2 (IKEv2)*, permet d'effectuer des échanges de clés multiples tout en calculant un secret partagé lors de la configuration SA.

Ensemble, ces deux normes RFC donnent à IKEv2 la capacité de créer des clés hybrides en utilisant des mécanismes d'échange de clés (KEM) classiques et PQC pour atténuer une attaque quantique à l'aide de l'algorithme de Short. Les nouvelles PQC sont basées sur différentes technologies mathématiques qui ne sont pas vulnérables aux attaques classiques ou quantiques connues, notamment :

- Treillis
- Basé sur le code
- Basé sur le hachage
- Clé symétrique
- Basé sur l'isogénie
- Multivariable

La norme RFC 9370 permet d'avoir sept cycles d'échange de clés supplémentaires, qui peuvent être des KEM classiques ou PQC, tels que ML-KEM, BIKE, HQC, Classic McEliese, et d'autres, en plus de l'échange de clés par défaut IKEv2 pour un total de huit cycles.

Pour décoder la clé hybride, toutes les technologies KEM utilisées pour créer la clé de cryptage doivent succomber à une vulnérabilité et être compromises. Par exemple, pour créer une clé hybride résistante aux vulnérabilités d'ordinateur quantique (QC) connues aujourd'hui et aux menaces futures, les meilleures pratiques recommandent d'utiliser à la fois des KEM classiques et un ou plusieurs KEM de PQC qui utilisent différentes technologies mathématiques.

- Cycle KEM par défaut : Groupe Diffie-Hellman (DH) 21
- Échange de clés supplémentaire Cycle 1 : ML-KEM-768 (CRYSTALS-Kyber-786)
- Échange de clés supplémentaire Cycle 2 : BIKE L3

Dans l'exemple précédent, le groupe DH 21 classique fournit une protection pour les attaques préquantiques d'aujourd'hui. L'ajout de deux cycles de KEM PQC supplémentaires avec ML-KEM-768 (treillis) et BIKE-L3 (basé sur le code), l'un après l'autre, crée une clé de cryptage basée sur trois technologies KEM et fournit une protection pour les attaques futures à l'aide de l'algorithme de Shor. L'ajout d'au moins deux PQC à l'échange de clés DH offre un niveau de protection plus élevé contre une panne KEM unique et peut aider à résister aux attaques quantiques pendant une plus longue durée. En outre, l'utilisation de KEM basés sur différents types de mathématiques peut protéger contre les

vulnérabilités futures pour un type spécifique de PQC, comme toutes les PQC basées sur la technologie de treillis.

La transition vers le monde post-quantique où les PQC sont le seul mécanisme d'échange de clés prendra de nombreuses années car l'industrie a besoin de temps pour valider les nouvelles PQC et avoir confiance dans leurs capacités de sécurité. Pendant la période de transition, les clés hybrides basées sur les RFC 9242 et 9370 deviendront la norme.

Le processus d'approbation des nouvelles PQC par les normes se fera par étapes, avec des groupes d'approbation de PQC par le NIST pour chaque cycle d'approbation. Étant donné que chaque PQC présente des compromis en matière de performance et de sécurité, il est nécessaire d'acquérir une compréhension de la façon dont chaque PQC fonctionne pour déterminer la technologie la mieux adaptée aux différents cas d'utilisation de la sécurité. Par exemple, Classic McEliece a fait ses preuves comme une PQC très sécurisé au fil du temps, mais le compromis pour sa haute sécurité réside dans la grande taille des clés qu'il utilise, ce qui peut limiter l'utilisation de Classic McEliece dans les communications VPN et TLS.

Les gouvernements du monde recommandent un niveau de sécurité de L3 ou supérieur pour fournir une sécurité et une résistance fortes aux attaques futures d'informatique quantique.

Pendant la période de transition du cryptage classique au cryptage post-quantique, l'agilité cryptographique sera nécessaire pour permettre le remplacement rapide de toute PQC compromise. La solution de KEM post-quantique des RFC 9242 et 9370 de Palo Alto Networks fournit un large ensemble de PQC pour obtenir une agilité cryptographique dès le début, permettant aux clients de sélectionner et de supprimer rapidement toute PQC prise en charge de la négociation de clés IKEv2 sans mise à jour logicielle ou modification du réseau existant.

Les PQC suivantes sont prises en charge pour PAN-OS IKEv2 :

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

Les avantages des RFC 9242 et 9370 comprennent :

- Normes approuvées avec prise en charge par plusieurs fournisseurs.
- Évolutivité élevée avec échange dynamique de clés au lieu des PPK statiques de la RFC 8784.
- Prise en charge d'une large gamme de KEM de PQC.
- La rétrocompatibilité IKEv2 permet le repli si l'homologue est incapable de prendre en charge les RFC.
- Les clés hybrides sont plus résistantes à l'algorithme de Shor car différentes technologies PQC peuvent être utilisées ensemble.
- Possibilité de superposer avec la RFC 8784 pour une défense quantique en profondeur et une agilité cryptographique.

Les inconvénients des RFC 9242 et 9370 sont les suivants :

- Les premières listes PQC normalisées pourraient ne pas fournir suffisamment de PQC pour atteindre une agilité cryptographique au début de la transition PQ.
- La nouvelle PQC pourrait avoir besoin de nombreuses années pour être entièrement vérifiée et approuvée par l'industrie.
- Les KEM multiples peuvent ajouter des surcharges supplémentaires et ralentir le processus de couplage IKEv2.
- Les nouveaux KEM de PQC peuvent provoquer une fragmentation car les tailles de clés et les charges utiles de données sont plus importantes.
- Tous les périphériques ne peuvent pas être mis à niveau pour prendre en charge les KEM de PQC.
- Le risque d'attaque par déni de service (DoS) peut augmenter avec l'échange de clés étendu pendant l'IKE_INTERMEDIATE en raison de l'augmentation des ressources nécessaires avant l'authentification de l'initiateur.
- Les clés hybrides sont conçues pour protéger contre les attaques de récolte de données lorsque les informations chiffrées sont enregistrées et décryptées avec un ordinateur quantique pertinent sur le plan cryptographique (CRQC) à une date ultérieure. Les attaques utilisant un ordinateur quantique dans une attaque active ne sont pas complètement résolues avec des clés hybrides pour les raisons suivantes :
  - L'authentification est toujours effectuée à l'aide de méthodes classiques, soit des algorithmes de clé pré-partagée ou de signature numérique. Les clés pré-partagées doivent être longues et complexes pour être sécurisées post-quantiquement, mais elles ne sont pas évolutives. L'authentification à l'aide de signatures numériques doit être effectuée par une signature numérique post-quantique.
  - Les PQC sont conçues pour fournir une résistance aux attaques de récolte de données et tant que les CRQC ne sont pas disponibles, l'attaque contre l'authenticité d'une connexion importe peu car il n'y a pas de possibilité d'exploitation car celles-ci ne se produisent qu'au moment de la connexion.

Il est recommandé d'utiliser des VPN IKEv2 basés sur les RFC 9242 et 9370 pour sécuriser les connexions VPN contre les menaces post-quantiques à l'aide de clés hybrides basées sur des technologies KEM multiples. Avec un large ensemble de PQC, l'agilité cryptographique peut être obtenue pour se protéger contre les PQC compromis pendant la transition vers un monde post-quantique.

Prise en charge des fonctionnalités post-quantiques

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

La prise en charge des fonctionnalités et des capacités post-quantiques inclut les RFC, les HA, ainsi que des considérations relatives à la mise à niveau et à la rétrogradation. Le développement des normes et fonctionnalités post-quantiques en est encore à ses débuts, pendant que les nations, les fournisseurs et les entreprises cherchent à savoir comment défendre leurs données contre les attaques post-quantiques. Au fur et à mesure que les normes progressent et que les plateformes Palo Alto Networks les prennent en charge, cette rubrique sera mise à jour pour indiquer cette prise en charge.

- Prise en charge et interopérabilité des RFC
- Prise en charge HA
- Considérations relatives à la mise à niveau/rétrogradation

Prise en charge et interopérabilité des RFC

Les périphériques de Palo Alto Networks prennent entièrement en charge les normes ouvertes de la RFC 8784, la RFC 9242 et la RFC 9370.

Les périphériques de Palo Alto Networks interagissent avec d'autres périphériques qui prennent en charge les mêmes normes, bien que certaines implémentations de fournisseurs puissent différer en fonction de l'interprétation des RFC. Par exemple, certains fournisseurs peuvent ne pas offrir la possibilité de configurer autant de clés pré-partagées post-quantiques (PPK PQ) avec la RFC 8784 ou peuvent ne pas prendre en charge le large ensemble de PQC prises en charge par Palo Alto Networks avec la RFC 9370.

Prise en charge HA

La haute disponibilité (HA) pour les VPN IKE est la même qu'avant l'introduction des fonctionnalités post-quantiques : Les tunnels VPN continuent de s'exécuter après un basculement, et les homologues IKE se resynchronisent et actualisent les clés IKE après un basculement.

Considérations relatives à la mise à niveau/rétrogradation

Lorsque vous effectuez une mise à niveau à partir d'une version qui ne prend pas en charge les VPN IKEv2 post-quantiques, la plateforme prend en charge les fonctionnalités et capacités post-quantiques.

Lorsque vous passez à une version prenant en charge les fonctionnalités post-quantiques que vous avez configurées, la configuration n'est pas modifiée et la sécurité VPN IKEv2 post-quantique reste en place.

Lorsque vous rétrogradez vers une version qui ne prend pas en charge les fonctionnalités VPN IKEv2 post-quantiques :

- Si vous n'avez pas configuré les VPN IKEv2 post-quantiques, la rétrogradation se déroule comme d'habitude et les options de configuration de sécurité VPN IKEv2 post-quantiques sont supprimées.
- Si vous avez configuré des VPN IKEv2 post-quantiques, la rétrogradation est bloquée parce que la version de rétrogradation ne prend pas en charge les options de configuration post-quantiques. Un message d'avertissement s'affiche lorsque la rétrogradation est bloquée, vous demandant de supprimer

la configuration VPN IKEv2 post-quantique et de sélectionner le cryptogramme que vous souhaitez utiliser pour le VPN après la rétrogradation.

Après avoir supprimé la configuration VPN IKEv2 post-quantique et sélectionné le cryptogramme, vous pouvez procéder à la rétrogradation.

Les fichiers journaux conservent les journaux post-quantiques après la rétrogradation.

Planification et préparation de la migration post-quantique

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

La mise à niveau de votre réseau pour résister aux attaques post-quantiques exige une planification et une préparation importantes, car en plus d’un mise à niveau des VPN, vous devez passer de suites cryptographiques classiques à des suites cryptographiques post-quantiques. Et il ne s’agit pas seulement d’un changement de réseau et de pare-feu, mais également de terminaux, d’applications, d’applications clientes, etc. Une migration complète de bout en bout. Il s’agit d’un investissement important en matière de temps, de recherche et de ressources. L’importance de l’investissement est relative de votre entreprise et à votre réseau. Cependant, le coût de l’investissement est mineur par rapport au coût d’une attaque qui vole vos ressources les plus précieuses, notamment les données financières, le code, les données PII et d’autres données potentiellement à longue durée de vie qui sont vulnérables à une attaque Harvest Now, Decrypt Later.

En outre, les agences de réglementation, les agences de sécurité nationale telles que la NSA, les gouvernements et les autorités de normalisation telles que le NIST dans le monde entier exigent ou exigeront que les organismes publics et certains secteurs d’activité (y compris éventuellement les transports et les infrastructures critiques) se préparent et se défendent contre les menaces post-quantiques. La préparation de la transition vers un monde post-quantique n’est pas une question de savoir si vous devez le faire, mais quand vous le ferez.

La question qui se pose est donc la suivante : *Quand devez-vous commencer la migration* ?

Le moment de lancer la migration dépend des exigences de vos ressources numériques, en particulier de la durée de sécurisation de leur confidentialité, en raison des attaques Harvest Now, Decrypt Later, qui enregistrent des données cryptées, y compris le matériel de la clé transmis dans l’établissement de la connexion de couplage IKE et TLS, dans le but de décrypter les données capturées lorsque des ordinateurs quantiques pertinents sur le plan cryptographique (CRQC) deviennent disponibles. La question essentielle qui se pose, pendant combien de temps vos données doivent-elles être sécurisées ? Si un attaquant a déjà capturé des données sensibles et que ces données sont toujours valides lorsque les CRQC entrent en jeu, l’attaquant sera en mesure de décrypter les données volées et d’agir sur leur contenu. Les CRQC pourraient devenir disponibles dès la prochaine décennie.

Si votre entreprise est une cible potentielle d’attaques de récolte de données, chaque jour de retard dans l’adoption d mesures présente un risque de donner aux attaquants plus d’informations à décrypter par la suite. Plus tôt vous prenez des mesures, plus vous empêchez les attaquants d’être en mesure de décrypter des données récoltées à l’avenir.

Dans le passé, la plupart des efforts de remplacement des protocoles cryptographiques, notamment le passage du cryptage 3DES au cryptage AES ou le passage des fonctions de hachage SHA-1 à SHA-2, ont nécessité entre 5 et 20 ans après l’élaboration des nouvelles normes. Cela inclut le temps nécessaire pour valider les nouveaux protocoles dans le monde réel. Une fois que le NIST aura normalisé les cryptographies post-quantiques (PQC), et même si elles auront subi des tests rigoureux, il faudra probablement 5 à 10 ans d’expérience des PQC dans le monde réel et des tentatives de les décoder avant de s’assurer qu’elles sont vraiment solides.

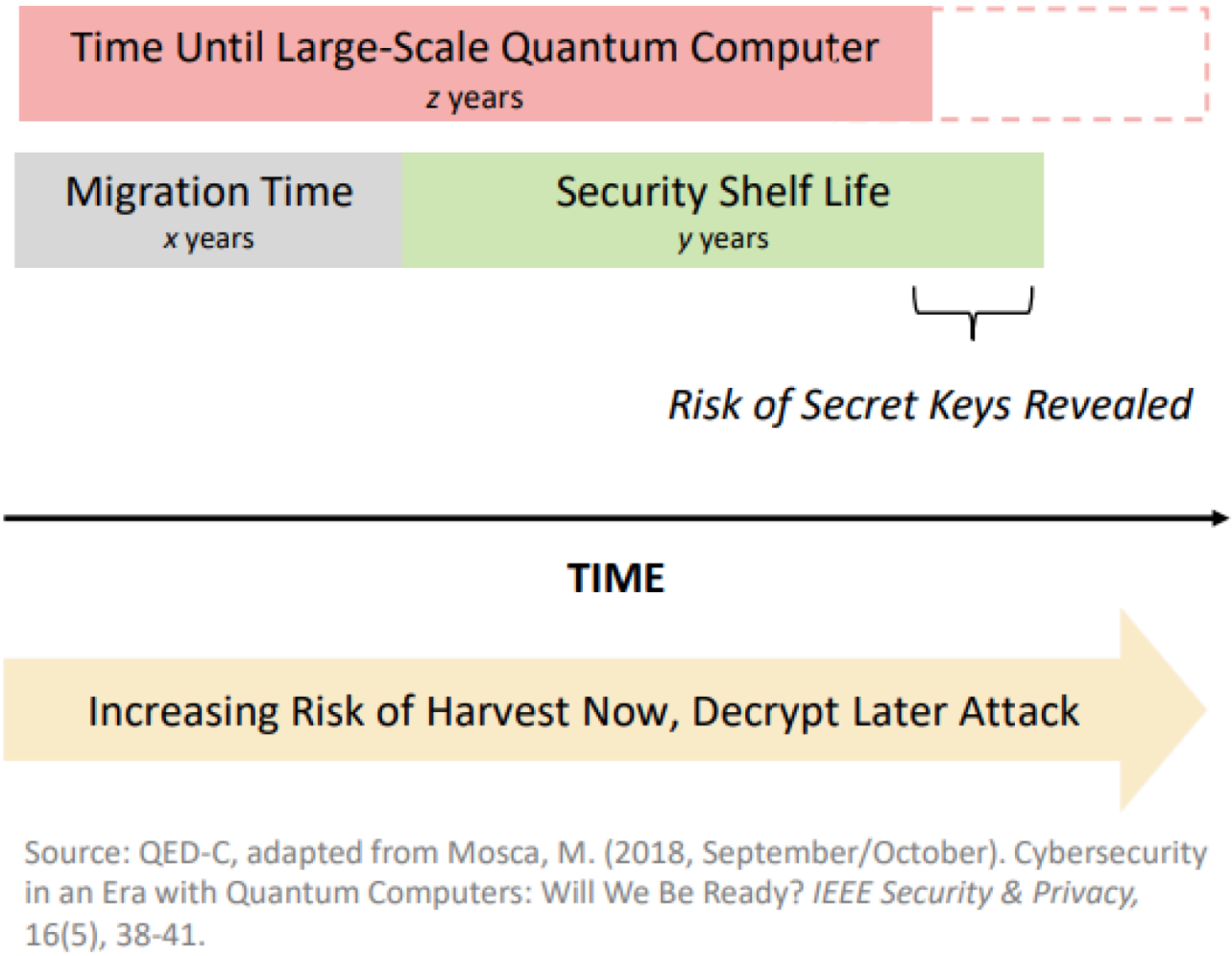
Les PQC remplacent les algorithmes cryptographiques classiques et fournissent une résistance quantique pour l'échange de clés, le cryptage et les signatures numériques.

Pour faciliter la transition du cryptage classique aux nouvelles PQC, l'industrie est en train d'adopter des clés hybrides. Les clés hybrides assurent une couche de sécurité supplémentaire en créant la clé de cryptage à l'aide de technologies de mécanisme d'échange de clés (KEM) multiple. La meilleure pratique consiste à utiliser un KEM classique fort, comme le groupe Diffie-Hellman 21, et une ou plusieurs PQC. Si l'un des KEM de PQC utilisés pour créer la clé succombe à une vulnérabilité, les autres KEM protègent toujours la clé. Les clés hybrides restent la meilleure solution jusqu'à ce que les nouvelles PQC gagnent suffisamment d'expérience dans le monde réel pour convaincre l'industrie de leur efficacité en matière de sécurité.

Et les attaques Harvest Now, Decrypt Later ne sont pas la seule menace post-quantique. Si vous ne bloquez pas les PQC non autorisées sur votre réseau de manière proactive, de mauvais acteurs internes techniquement compétents peuvent télécharger des PQC open-source et mettre en place leurs propres serveurs ou plug-ins de navigateur de PQC sur votre réseau.

D'ici le début des années 2030, il est probable que les données sécurisées à l'aide de la cryptographie classique d'aujourd'hui ne seront plus protégées contre les attaques post-quantiques. Il est donc important de comprendre pendant combien de temps vos données doivent être sécurisées et d'estimer le temps qu'il vous faudra pour préparer et exécuter votre plan post-quantique. Plus tôt vous commencez, plus il est facile de maintenir une qualité élevée et des coûts prévisibles, pour éviter de précipiter le processus à mesure que les menaces post-quantiques augmentent.

L'une des façons de déterminer le moment propice pour passer à l'action est d'utiliser le modèle de Mosca, qui présente un calendrier simple dans lequel vous inscrivez vos estimations de temps afin de comprendre l'urgence de prendre des mesures.



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.

Ce modèle Mosca explique comment estimer le calendrier de vulnérabilité post-quantique de vos ressources et vous aide à déterminer à quel moment vous devez commencer à vous préparer au post-quantique. Le modèle compare votre estimation du temps nécessaire pour migrer vers la préparation post-quantique (*x*, qui est susceptible d'être d'au moins cinq ans) et votre estimation de la durée de vie de vos données (*y*, qui est le temps écoulé entre l'achèvement de la préparation post-quantique et le moment où l'exposition des données ne compromet plus les données) par rapport au moment où les CRQC sont susceptibles d'être disponibles (*z*).

La différence entre (*x* + *y*) et *z* indique la durée pendant laquelle vos données à longue durée de vie risquent d'être exposées si elles ont été récoltées ou le temps dont vous disposez avant que vos données à longue durée de vie ne soient à risque. Cela vous aide à déterminer combien de temps vous avez avant de commencer et combien vous pourriez être en retard. Si (*x* + *y*) est supérieur à *z*, la différence entre ces chronologies désigne la durée pendant laquelle vos données risquent d'être exposées si elles étaient récoltées par des attaquants lors d'une attaque Harvest Now, Decrypt Later, indiquée dans l'illustration précédente intitulée *Révélation des risques des clés secrètes*.

Lorsque vous commencez à planifier la transition, plusieurs options immédiates s'offrent à vous pour renforcer vos connexions VPN existantes :

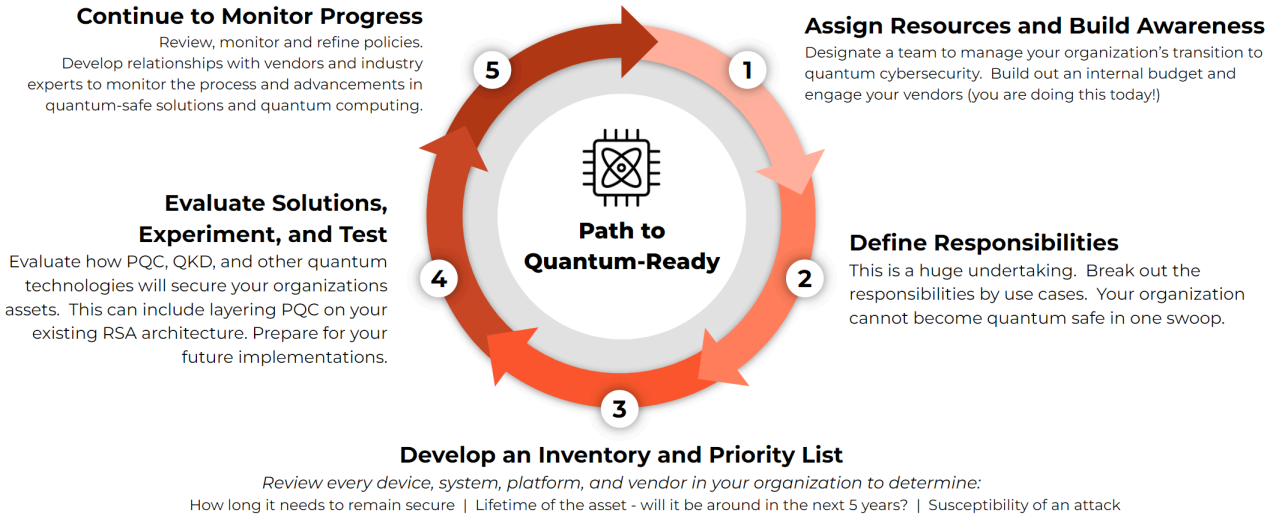
- Conformez-vous à la RFC 6379 pour *Suites de chiffrement Suite B pour IPsec* pour mettre à niveau vos connexions VPN vers des suites de cryptage difficiles. Utilisez Suite-B-GCM-256 et évitez les algorithmes AES 128 bits plus faibles, qui sont vulnérables à l'algorithme de Grover.

- Mettez à niveau votre CA vers des tailles de clé RSA 4K pour atténuer les attaques par force brute capables de décoder des clés de plus petite taille et migrez votre authentification de certificat VPN vers de nouveaux certificats.
- Passez à des tailles de hachage SHA à bits plus élevés telles que SHA-384 et SHA-512. Cessez d'utiliser des hachages faibles tels que MD5 et SHA-1.
- Mettez en œuvre les RFC 8784 et/ou RFC 9242 et RFC 9370 pour créer des VPN post-quantiques résistants aux attaques quantiques.

En outre, vérifiez vos connexions SSL/TLS et renforcez-les :

- Mettez à niveau les connexions SSL/TLS vers des suites de cryptage difficiles; utilisez TLSv1.3 avec des cryptages Perfect Forward Secrecy (Confidentialité de transmission parfaite, PFS).
- Tunnelisez les sessions SSL/TLS dans des sessions VPN client à serveur renforcées. Utilisez une application de bureau post-quantique pour prendre en charge le proxy inverse.

Pour amorcer la transition, le Quantum Economic Development Consortium (QED-C) a développé un modèle pour la planification et la préparation de la transition vers la sécurité post-quantique qui a été adapté par Palo Alto Networks en un modèle en cinq étapes qui vous aide à évaluer la préparation à la migration, le temps et les ressources.



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

Les sections suivantes décrivent chaque étape du parcours vers la préparation au quantique, où la mise en œuvre de la RFC 8784 pour créer des VPN IKEv2 résistants aux technologies quantiques représente la première étape :

- Attribuer des ressources et renforcer la sensibilisation
- Définir les responsabilités
- Élaborer un inventaire cryptographique et une liste de priorités
- Évaluer les solutions, expérimenter et tester
- Continuer à surveiller les progrès

Attribuer des ressources et renforcer la sensibilisation

Les objectifs de cette phase de planification et de préparation consistent à identifier l'équipe de transition, à déterminer les ressources nécessaires, à inciter les fournisseurs à comprendre leurs plans de préparation post-quantique et à commencer à appréhender les coûts impliqués.

Les mises à niveau qui renforcent la résistance aux attaques post-quantiques s'inscrivent souvent dans le cadre des travaux déjà lancés par votre service informatique pour moderniser le réseau.

1. Formez une équipe de gestion de projet dédiée pour assumer la responsabilité de l'élaboration d'une stratégie post-quantique et d'une feuille de route de préparation au quantique afin de gérer la transition. L'équipe est responsable de la planification de haut niveau. L'équipe détermine également les responsabilités vis-à-vis des parties du réseau qui font partie de la transition. Commencez tôt et donnez-vous suffisamment de temps pour adopter une approche réfléchie et mesurée afin de garantir le maintien d'une qualité élevée et de coûts prévisibles.
2. Développez une compréhension des technologies de sécurité quantique et trouvez un moyen de les intégrer dans votre environnement. Les VPN IKEv2 post-quantiques (RFC 8784) constituent la première étape de la création d'un réseau post-quantique sécurisé, ce que vous pouvez faire dès maintenant sans incidence sur votre réseau. En outre, toutes les organisations devront remplacer leurs algorithmes asymétriques existants par des PQC quantiques. Pour passer aux étapes suivantes, renseignez-vous sur les PQC, les clés hybrides et les échanges de clés multiples (RFC 9370 et 9242). Renseignez-vous également sur la crypto-agilité (utilisation de PQC multiples afin d'avoir la possibilité de passer facilement et rapidement d'une PQC à l'autre si une PQC est compromise), la distribution de clés quantiques (QKD) et les générateurs de nombres aléatoires quantiques (QRNG) pour savoir si ces mesures de sécurité sont justifiées pour protéger vos données.

   Effectuez des recherches sur les technologies quantiques et demandez à vos fournisseurs de comprendre leurs plans de préparation au quantique et leur incidence sur votre entreprise.
3. Mobilisez la communauté de l'entreprise et développez une compréhension de la PQC et des niveaux de sensibilisation et de préparation à la technologie. Sensibilisez les équipes et les chefs d'équipe et aidez-les à comprendre les changements potentiels et les raisons pour lesquelles ils sont nécessaires. Par exemple, travaillez avec les équipes d'approvisionnement pour inclure les exigences post-quantiques afin de garantir la compatibilité du nouveau matériel et des nouveaux logiciels avec les PQC et de pérenniser l'infrastructure.

   Lancez des activités de découverte cryptographique (vous pourriez tirer parti de la documentation d'audit) pour mieux comprendre et identifier la dépendance actuelle de l'organisation à l'égard des signatures numériques et des cryptographies vulnérables aux attaques post-quantiques, telles que Diffie-Hellman (DH), la cryptographie à courbe elliptique (ECC) et l'échange de clés Diffie-Hellman basé sur les courbes elliptique (ECDH), AES-128, le cryptage RSA inférieur à 4K, etc.
4. Commencez à préparer un budget interne. Ajustez le budget au fur et à mesure que vous en apprenez davantage et formulez la solution la mieux adaptée à votre entreprise.

Définir les responsabilités

Déterminez qui est responsable de chaque partie du réseau, y compris la mise en réseau, le cryptage des fichiers et des données, les applications logicielles, les terminaux, l'IAM, les serveurs d'applications, etc. Attribuez des responsabilités aux membres de l'équipe dans chaque domaine et veillez à ce qu'ils comprennent la raison, l'urgence et la valeur de la transition. Les vulnérabilités post-quantiques affectent l'ensemble du cryptage asymétrique existant. Les membres d'équipe doivent comprendre qu'il faudra

déployer des efforts considérables pour découvrir, catégoriser et mettre à niveau tout ce qui se trouve sur le réseau de manière hiérarchisée.

Élaborer un inventaire cryptographique et une liste de priorités

Un inventaire cryptographique est une liste complète de tous les éléments de votre réseau (chaque périphérique, système, code, application, plateforme et fournisseur de votre réseau) et de la cryptographie que chacun utilise (suites cybernétiques, versions utilisées pour TLS, SSH et VPN, gestion des certificats, génération de clés de cryptage, tailles de clés et stockage des clés, etc. L'inventaire cryptographique doit être complet, car les PQC représentent une menace pour l'ensemble du chemin de données de bout en bout, y compris les points de terminaux, les applications et les serveurs de tous types. Cela signifie que vous devez planifier une migration complète de bout en bout.

L'inventaire cryptographique ne se contente pas d'énumérer les composants, il fournit également des informations sur chaque composant en plus des composants et de la cryptographie utilisée par chacun d'eux. Pour chaque composant, l'inventaire indique son utilisation, les données qui y sont stockées, sa protection et le moyen de déplacement des données entre les composants. L'objectif est de comprendre les types de cryptage utilisés dans votre réseau, les données protégées par le cryptage, le lieu de stockage des données, leur destination, et tout ce qui concerne les périphériques et les utilisateurs concernés. En bref, un inventaire complet de la cryptographie de votre réseau et de tout ce qu'elle affecte.

Sans un inventaire cryptographique complet, vous ne pouvez pas identifier tous les composants affectés de votre réseau, évaluer leur niveau de risque ou hiérarchiser efficacement les éléments à mettre à niveau en premier.

Pour créer votre inventaire cryptographique, examinez et documentez l'utilisation de la cryptographie (les services informatique et SecOps peuvent souvent vous aider) :

- Quelles cryptographie est utilisée : les codes et protocoles cryptographiques actuellement utilisés.
- Qui utilise chaque code et protocole cryptographique.
- Où la cryptographie est utilisée : les données, serveurs, navigateurs, VPN, applications distantes, etc., protégés par la cryptographie. Identifiez les utilisateurs des données, les parties du réseau qu'elles traversent et la manière dont elles sont sécurisées de bout en bout.
- Catégorisez pour chaque élément du réseau selon le risque.
- Déterminez la durée de confidentialité des données requise et la fin de vie prévue des données afin d'évaluer le risque de perte de données à cause d'attaques de collecte.

Incluez les fournisseurs et les partenaires dans l'inventaire cryptographique. Par exemple, interrogez les fournisseurs pour comprendre la cryptographie utilisée dans leurs applications, la force des clés et la façon dont elles sont générées. Identifiez qui utilise les données et comment elles sont sécurisées de bout en bout. Ne laissez aucune lacune susceptible d'être exploitée par des attaquants dans une attaque post-quantique.

Lors de la création de votre inventaire cryptographique, vous pourriez tirer parti du travail effectué pour les audits, des améliorations du réseau, du Zero Trust, etc.

Le développement de votre inventaire cryptographique pourrait représenter la partie la plus difficile de la transition. La bonne nouvelle, c'est que l'inventaire permet de sensibiliser les organisations et de les aider à devenir plus sécurisées avant même qu'une menace quantique ne se concrétise, car l'inventaire permet d'identifier les systèmes archaïques et obsolètes.

Palo Alto Networks met à votre disposition plusieurs outils pour vous aider à faire votre inventaire cryptographique :

- Les journaux de décryptage, de trafic et de menaces révèlent les protocoles cryptographiques exécutés sur votre réseau, les périphériques et les utilisateurs de ces protocoles, etc.
- Les signatures de profil de protection contre les vulnérabilités dans la version de contenu 8692 peuvent détecter l'utilisation de PQC et générer des alertes dans les journaux à cet effet. Vous pouvez configurer des profils de protection contre les vulnérabilités pour bloquer automatiquement les PQC non approuvées sur votre réseau, ce qui est une bonne pratique. (Prévoyez les exceptions requises pour les tests PEN internes.)
- Utilisez le décryptage SSL pour bloquer automatiquement les cryptogrammes qui ne peuvent pas être décryptés par le pare-feu

Évaluez le risque des éléments de votre inventaire cryptographique et déterminez vos options de sécurité afin de pouvoir ensuite prioriser la migration :

- Comprendre vos données et vos applications :
  - Identifiez les données hautement prioritaires et à haute confidentialité.
  - Catégorisez les données en fonction de la sécurité et du risque.
  - Attribuez une durée de confidentialité (durée de vie des données, durée de validité).
  - Comprenez comment les applications sécurisent leurs données.
  - Sachez qui utilise les données.
- Comprenez vos terminaux.
  - Où les données sont-elles stockées et comment sont-elles protégées ?
  - Quels serveurs hébergent et servent les données ?
  - Quels périphériques les utilisateurs utilisent-ils pour accéder aux données ?
  - Comment les terminaux sont-ils sécurisés ?
- Comprenez votre réseau.
  - Comment les données se déplacent-elles dans le réseau ?
  - Quels périphériques protègent les données ?
  - Le cloud est-il impliqué ? Comment les données sont-elles sécurisées dans le cloud ?
  - Où se trouvent les zones de réseau à haut risque ?
- Comprenez vos options de sécurité et où vous devez appliquer l'atténuation post-quantique.
  - Avez-vous besoin de migrer vers des protocoles plus récents ?
  - Quelles PQC devriez-vous utiliser et quand ? (Faites attention aux normes du NIST pour les PQC.)
  - Aurez-vous besoin d'utiliser des clés hybrides pour sécuriser vos données ?
  - Comment allez-vous garantir la crypto-agilité (la capacité de passer rapidement d'un algorithme cryptographique à un autre en cas de découverte de vulnérabilités dans une PQC) ?
  - Aurez-vous besoin d'utiliser des QRNG ou des QKD ?
  - Quand devrez-vous passer aux certificats et à l'authentification post-quantique ?
  - Les options répondent-elles à vos exigences en matière de conformité ?

Lorsque vous comprenez votre inventaire cryptographique, analysez les données et définissez des priorités de migration en fonction de celles-ci. Lorsque vous établissez des priorités, tenez compte de la durée de vie

des données à défendre contre les attaques de récolte de données, de l'emplacement et de la sensibilité des données, ainsi que de la sensibilité des données aux attaques. Aujourd'hui, l'échange de clés pose le plus grand risque, c'est pourquoi la mise en œuvre de la RFC 8784 et/ou des RFC 9242 et 9370 pour créer des VPN résistants au quantique est la première priorité.

Pour définir les priorités de migration :

- Classez les tâches en fonction de leur impact sur l'entreprise. Dans quelle mesure l'actif est-il essentiel pour votre entreprise ? Combien de temps les données doivent-elles rester sécurisées ou privées : l'actif est-il exposé au risque d'une attaque Harvest Now, Decrypt Later ? Comparez la valeur en capital des ressources à risque à l'estimation du coût d'une perte de données future due à une attaque post-quantique.
- Migrez d'abord les zones à fort impact.
- Définissez des actions de correction.
- Établissez des calendriers et des politiques de migration.
- Consacrez des ressources et financez des activités.

Évaluer les solutions, expérimenter et tester

Utilisez les informations de votre inventaire cryptographique pour élaborer des politiques, des plans de migration et des plans de test afin de faire passer votre réseau à la préparation post-quantique et sécuriser vos données. Incluez les fournisseurs, les partenaires et toutes les autres influences externes sur la sécurité de votre réseau. Pour développer des politiques de solutions et des plans de migration :

- Identifiez les ressources dont vous avez besoin pour effectuer la mise à niveau vers des PQC.

  Identifiez les technologies requises pour chaque niveau de priorité et déterminez comment elles s'intègrent dans la stratégie de migration.
- Créez un plan de transition qui identifie les algorithmes les mieux adaptés pour protéger vos ressources à présent et à l'avenir, lorsque vous remplacerez ou renforcerez les algorithmes classiques par des PQC.
- Élaborez des politiques de cycle de vie pour les clés afin de tenir compte des risques liés aux clés de cryptage asymétriques et symétriques, en particulier pour les données à longue durée de vie susceptibles de subir des attaques de type Harvest Now, Decrypt Later.
- Incluez une mise en œuvre de la crypto-agilité dans vos politiques et plans. La crypto-agilité garantit la capacité de passer rapidement et facilement à un algorithme sécurisé en cas de compromission d'un algorithme (classique ou PQC).

Comprenez qu'il s'agit d'une transition réfléchie, et non d'un remplacement à la chaîne. Il est probable que vous devrez adopter une approche hybride et appliquer des couches de PQC avec des algorithmes cryptographiques classiques pour renforcer la sécurité avant de passer complètement aux PQC.

Pour tester les plans et les politiques, configurez des laboratoires de preuve de concept afin de pouvoir :

- Tester minutieusement tous les composants de la PQC et l'interopérabilité entre les périphériques et les applications.
- Comprendre les différences de performances et de capacité entre les algorithmes classiques et PQC. Les PQC ont des tailles de clé et de signature numérique plus grandes que les cryptographies classiques, ce qui entraîne des fichiers cryptés plus volumineux et pourrait également affecter la latence.

  Testez l'interopérabilité PQC entre les composants et essayez de maximiser la résistance quantique de bout en bout, non seulement au sein de l'organisation, mais aussi entre les parties externes. Identifiez

les algorithmes les plus pertinents pour chaque cas d’utilisation et créez un plan de transition pour remplacer les cryptographies classiques par des PQC.

- Effectuez des tests de bout en bout et incluez des partenaires, des fournisseurs et d’autres parties externes dont la préparation post-quantique pourrait affecter votre réseau. Certains systèmes pourraient nécessiter des mises à niveau pour avoir des performances post-quantiques acceptables.
- Identifiez les composants et les ressources incompatibles que vous devez mettre à niveau.

L’expérimentation est également un autre moyen de sensibiliser votre organisation tout en répondant aux questions et en fournissant des informations sur la facilité ou les difficultés de la transition. Recherchez une expertise externe si vous ne disposez pas d’une expertise interne ou si vous ne pouvez pas développer une expertise interne dans un délai raisonnable.

Continuer à surveiller les progrès

Surveillez et évaluez en permanence les progrès réalisés dans la mise en place d’un environnement résistant au quantique afin de garantir le respect du calendrier de transition et d’atténuer les risques d’attaques de récolte de données. Apportez des ajustements au plan et au personnel impliqué, le cas échéant. En outre, collaborez avec des experts pour vous assurer de couvrir toutes les bases et de ne laisser aucune lacune susceptible d’être exploitée par un pirate lors d’une future attaque quantique.

Meilleures pratiques pour résister aux attaques post-quantiques

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Il existe de nombreuses bonnes pratiques que vous pouvez mettre en œuvre dès maintenant pour vous défendre contre les attaques post-quantiques menées par des ordinateurs quantiques, notamment les attaques Harvest Now, Decrypt Later. Les attaques Harvest Now, Decrypt Later capturent des données cryptées et du matériel d'échange de clés avec l'intention d'utiliser des ordinateurs quantiques pertinents sur le plan cryptographique (CRQC) pour décrypter le matériel ultérieurement en accélérant l'algorithme de Short, qui prend en compte le matériel de la clé pour rechercher les grands nombres premiers sur lesquels la clé de cryptage est basée.

Ces meilleures pratiques couvrent :

- Meilleures pratiques de planification de la transition post-quantique
- Meilleures pratiques de cryptographie
- Bonnes pratiques de configuration de VPN

Meilleures pratiques de planification de la transition post-quantique

La transition de la cryptographie classique à la cryptographie post-quantique peut prendre cinq ans, voire plus. La planification seule peut prendre plusieurs années. Donnez-vous le meilleur avantage en procédant comme suit :

- **Commencer tôt** : si votre entreprise dispose de données à longue durée de vie et constitue une cible potentielle d'attaques de récolte de données, chaque jour de retard dans l'adoption de mesures présente un risque d'autoriser les attaquants à récolter plus d'informations pour les décrypter par la suite. Plus tôt vous prenez des mesures, plus vous empêchez les attaquants de récolter des données pour les décrypter à l'avenir.
- **Exploiter les ressources existantes** : lorsque vous effectuez votre inventaire cryptographique, tirez parti du travail que vous avez déjà effectué pour les audits, le Zero Trust, les améliorations réseau et d'autres activités.
- **Se renseigner** : renseignez-vous sur la menace de calcul quantique, la cryptographie post-quantique (PQC), les technologies et méthodes permettant de renforcer votre réseau contre les attaques quantiques et les PQC nouveaux et émergents que vous pouvez utiliser pour protéger votre réseau. Consultez les mandats, plans et lois du gouvernement, les RFC (Demandes de commentaires) et d'autres sources d'information.

Meilleures pratiques de cryptographie

Augmentez la puissance de vos suites cryptographiques classiques pour compliquer la tâche d'un attaquant qui cherche à décrypter les clés par force brute, car les ordinateurs quantiques deviennent de plus en plus rapides en évoluant vers des CRQC. Les ordinateurs quantiques qui ne sont pas des CRQC peuvent être encore assez rapides pour casser un cryptage plus faible.

- Conformez-vous à la RFC 6379 pour *Suites de chiffrement Suite B pour IPsec* pour mettre à niveau vos connexions VPN vers des suites de cryptage difficiles. Utilisez Suite-B-GCM-256 et évitez les algorithmes AES 128 bits plus faibles, qui sont vulnérables à l'algorithme de Grover.
- Mettez à niveau votre CA vers des tailles de clés RSA 4K pour atténuer les attaques par force brute capables de casser des tailles de clés plus petites.
- Migrez votre authentification de certificats VPN vers de nouveaux certificats dotés de tailles de clés plus grandes.
- Passez à des tailles de hachage SHA à bits plus élevés telles que SHA-384 et SHA-512. Cessez d'utiliser des hachages faibles tels que MD5 et SHA-1.
- Mettez à niveau les connexions SSL/TLS vers des suites de cryptage difficiles; utilisez TLSv1.3 avec des cryptages Perfect Forward Secrecy (Confidentialité de transmission parfaite, PFS).
- Tunnelisez les sessions SSL/TLS dans des sessions VPN client à serveur renforcées.
- Configurez vos profils de protection contre les vulnérabilités pour bloquer les PQC non autorisés pour le trafic que vous ne décryptez pas. Pour le trafic que vous décryptez, utilisez un profil de décryptage pour bloquer les PQC non autorisés (le profil de décryptage n'autorise que les cryptogrammes que vous activez et le pare-feu bloque tous les autres cryptogrammes). Les PQC non autorisés peuvent indiquer une faille ou un mauvais acteur interne tentant d'utiliser des PQC pour compromettre votre réseau. Prévoyez des exceptions au besoin pour vos équipes internes de test PEN.

Bonnes pratiques de configuration de VPN

Lorsque vous configurez des VPN IKEv2 post-quantiques, faites en sorte qu'ils soient aussi résistants que possible aux attaques quantiques :

- Mettez en œuvre la RFC 8784 pour créer des VPN IKEv2 résistants aux attaques quantiques.
- Mettez en œuvre les RFC 9242 et RFC 9370 pour créer des VPN IKEv2 résistants aux attaques quantiques.

> *La RFC 8784 peut être utilisée avec les RFC 9242 et 9370 pour fournir une couche de protection supplémentaire afin de répondre aux exigences d'agilité en matière de cryptographie.*

Meilleures pratiques de la RFC 8784 :

- N'utilisez pas le protocole IKEv1. IKEv1 est considéré comme un protocole faible qui ne prend pas en charge les VPN post-quantiques. Si la prise en charge peut être assurée par les deux homologues IKE, mettez à niveau vos connexions VPN vers IKEv2 et sélectionnez **IKEv2 only mode (Mode IKEv2 uniquement)** lorsque vous configurez les passerelles IKE (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** > **General (Général)**).
- Réglez le **Negotiation Mode (Mode de négociation)** sur **Mandatory (Obligatoire)** toutes les fois où vous savez que les deux homologues prennent en charge la RFC 8784. L'utilisation du mode **Mandatory (Obligatoire)** garantit la résistance du VPN aux attaques post-quantiques, ce qui rend les

attaquants incapables de récolter les données maintenant et de les décrypter ultérieurement à l'aide d'un CRQC exécutant l'algorithme de Shor.

L'algorithme de Shor peut décoder l'échange dynamique de clés dans l'établissement de la connexion IKEv2 qui utilise un cryptage asymétrique, avec suffisamment de puissance de traitement. Cependant, l'algorithme de Shor est incapable de décoder la cryptographie symétrique du tunnel IPSec. Pour protéger la cryptographie symétrique IPSec, utilisez AES-256 pour vous protéger contre l'algorithme de Grover ainsi que les hachages et longueurs de clés plus forts recommandés dans la section précédente sur les meilleures pratiques de cryptographie.

Lorsque vous effectuez un couplage avec des périphériques externes, essayez de vérifier si l'homologue prend en charge la RFC 8784 et travaillez avec l'autre administrateur pour utiliser les mêmes PPK (clé pré-partagée) PQ (post-quantique) pour la connexion afin de pouvoir utiliser le mode Obligatoire.

- Précisez manuellement ou générez automatiquement un secret PPK ayant une longueur d'au moins 64 caractères (32 octets ou 256 bits d'entropie) pour créer une clé forte. Vous pouvez spécifier un **PPK Secret (Secret PPK)** manuellement ou en générer automatiquement un d'une longueur allant jusqu'à 128 caractères (64 octets, 512 bits d'entropie). Plus le secret PPK est long, plus le nombre de bits d'entropie est important, ce qui rend le secret PPK plus difficile à décoder.

  Le nombre de bits d'entropie fournit la moitié de ce nombre de bits de sécurité post-quantique. Par exemple, 256 bits d'entropie fournissent 128 bits de sécurité post-quantique et 512 bits d'entropie fournissent 256 bits de sécurité post-quantique. Un minimum de 256 bits d'entropie fournit la sécurité équivalente à la catégorie 5 définie dans l'Appel à propositions sur la cryptographie post-quantique du NIST. La section Considérations de sécurité de la RFC 8784 fournit plus de détails sur l'entropie et la quantité d'entropie suffisante.

  Le secret PPK est affiché en clair uniquement lors de sa configuration ou génération automatique. Après avoir configuré ou généré le secret PPK et quitté l'écran qui affiche le secret en clair, celui-ci n'est plus jamais affiché en texte en clair pour contribuer à empêcher la compromission de la clé.

  Copiez le secret PPK et la paire d'ID de clé et stockez-le en toute sécurité. Si vous ne stockez pas la clé au moment de sa configuration ou de sa génération, vous ne pourrez pas la récupérer par la suite. (Vous pouvez supprimer la PPK PQ et en configurer une autre si nécessaire.)

  Voici d'autres bonnes pratiques pour manipuler les PPK PQ :

  - Créez plusieurs PPK PQ actives. L'utilisation de plusieurs clés actives, et non d'une seule, ajoute un élément aléatoire à la sélection des clés pendant l'échange de clés.
  - Vérifiez que chaque homologue IKEv2 a exactement le même ensemble de PPK PQ activées (paires d'ID de clé et de secret PPK) pour négocier l'échange de clés.
  - Si Panorama gère les homologues, configurez les PPK PQ et transmettez-les à des pare-feu gérés pour une configuration plus facile, plus rapide et plus automatique.
  - Si vous devez communiquer la PPK PQ à un autre administrateur, utilisez une méthode de communication cryptographiquement sécurisée comme la messagerie cryptée.

- Conservez la chaîne du secret PPK en toute sécurité. Ne la conservez pas sur des notes autocollantes ou dans un endroit où des administrateurs non autorisés pourraient la découvrir.

La NSA publie des conseils sur la manipulation des clés pré-partagées en toute sécurité, *notamment la RFC 8784 sur les clés pré-partagées quantiques.*

Meilleures pratiques des RFC 9242 et 9370 :

- N'utilisez pas le protocole IKEv1. IKEv1 est considéré comme un protocole faible qui ne prend pas en charge les VPN post-quantiques. Si la prise en charge peut être assurée par les deux homologues IKE, mettez à niveau vos connexions VPN vers IKEv2 et sélectionnez **IKEv2 only mode (Mode IKEv2 uniquement)** lorsque vous configurez les passerelles IKE (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** > **General (Général)**).
- Créez la clé hybride à l'aide d'un KEM (mécanisme d'encapsulation de clé) classique puissant, tel que le groupe Diffie-Hellman 20 et supérieur, et d'au moins une PQC (cryptographie post-quantique) dans les cycles KEM supplémentaires, tels que Kyber-768 (ML-KEM), lorsque vous configurez les profils crypto IKE (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)** > **General and Advanced Options (Options générales et avancées)**).
- Utilisez uniquement des PQC évaluées à un niveau de sécurité L3 ou plus pour les informations sensibles. Chaque PQC supplémentaire ajoutée au processus de création de clé augmente la capacité de la clé à résister à une attaque quantique, mais elle ajoute également de la latence et des surcharges au processus de couplage IKEv2. En général, l'ajout d'une PQC à niveau de sécurité L3 ajoute environ 20 à 30 ms à l'échange de clés IKEv2, et l'ajout d'une PQC à niveau de sécurité L5 ajoute 40 à 60 ms. Les PQC plus fortes qui utilisent des clés plus grandes, comme Classic McEliese, peuvent potentiellement ajouter plus de 800 ms à l'échange de clés et introduire des niveaux élevés de fragmentation. Familiarisez-vous avec les tailles de clés PQC et les forces de la sécurité pour sélectionner la meilleure PQC pour vos communications VPN.
- Coordonnez les PQC utilisées dans chaque cycle de négociation de clés avec l'administrateur qui gère le périphérique VPN homologue. Lorsque les deux périphériques VPN de chaque côté du tunnel sont configurés avec les mêmes PQC à chaque cycle de négociation de clés optionnel, les problèmes d'interopérabilité sont réduits. Essayez de vous entendre sur la PQC et sa force de sécurité pour garantir la configuration des deux parties avec les mêmes paramètres. Pour les pare-feu gérés par la même organisation, des outils de gestion centralisée peuvent être utilisés pour assurer une configuration et une sélection de PQC cohérentes à chaque cycle de négociation de clés.
- Activez l'agilité cryptographique pour protéger vos données pendant la transition vers un environnement de PQC pur. La transition peut prendre jusqu'à 5 à 10 ans avant que l'industrie ne fasse pleinement confiance aux nouvelles PQC.
  - Pour les organisations qui doivent utiliser des PQC normalisées par le NIST et approuvées par le FIPS, l'agilité cryptographique peut être obtenue en activant la RFC 8784 avec les RFC 9242 et 9370. Si la PQC utilisée dans la clé hybride succombe à une vulnérabilité, la chaîne PPK utilisée dans la RFC 8784 peut toujours fournir une résistance quantique pour empêcher une attaque de récolte de données réussie.
  - Pour les organisations autorisées à utiliser à la fois des PQC normalisées et non normalisées du NIST, l'agilité cryptographique peut être obtenue en utilisant au moins deux PQC avec un KEM classique fort, comme le groupe Diffie-Hellman 21. Idéalement, les KEM de PQC devraient utiliser des technologies mathématiques différentes où l'un des KEM est basé sur un treillis et l'autre sur des technologies basées sur du code ou d'autres technologies non-treillis. En option, la RFC 8784

peut également être activée avec la clé hybride pour ajouter une couche de sécurité supplémentaire et étendre l’agilité cryptographique.

- Réduisez la valeur de la durée de vie de la clé de sa valeur par défaut à une valeur inférieure pour faciliter une réinitialisation des clés plus rapide.
- Activez IPSec pour utiliser des clés hybrides lors de la configuration de profils crypto IPSec (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)** > **General and Advanced Options (Options générales et avancées)**). Les deux côtés du tunnel IPSec doivent être configurés pour utiliser la même PQC et la même force de sécurité à chaque cycle d’échange de clés supplémentaire.

En savoir plus sur la sécurité post-quantique

La sécurité, les technologies et les mises en œuvre post-quantiques recommandées en sont encore à leurs débuts. Lorsque vous planifiez de sécuriser vos ressources dans un monde de calcul post-quantique, il est important de comprendre autant que possible les technologies post-quantiques ainsi que les réglementations et mandats gouvernementaux qui affectent votre entreprise, et la manière de passer à des VPN et des cryptages post-quantiques.

Le gouvernement des États-Unis et les gouvernements du monde entier élaborent des plans pour faire face à la menace pour la sécurité représentée par les ordinateurs quantiques et la cryptographie post-quantique. En outre, des organismes de normalisation tels que le National Institute of Standards and Technology (NIST) et l'Internet Engineering Task Force (IETF) sont en train de créer des normes pour les nouvelles technologies post-quantiques et d'élaborer la manière de les mettre en œuvre.

Cette rubrique fournit des liens vers des informations qui vous aideront à mieux comprendre, préparer et passer à la sécurité post-quantique dans votre entreprise.

- Gouvernement des États-Unis
- Autres gouvernements dans le monde
- Les RFC
- Technologies et informations générales

Gouvernement des États-Unis

Les gouvernements de nombreux pays élaborent des plans, des mandats et des lois pour faire face à la menace de calcul quantique et à l'avènement de la cryptographie post-quantique. Les liens suivants fournissent des informations sur la façon dont le gouvernement des États-Unis aborde la question, ainsi que des liens vers des informations du National Institute of Standards and Technology (NIST) et de la National Security Agency (NSA). Consultez les sites et les organisations de sécurité de votre gouvernement local pour savoir comment votre gouvernement aborde la sécurité post-quantique.

- Le NIST Post-Quantum Cryptography Resource Center (Centre de ressources du NIST sur la cryptographie post-quantique) fournit des informations sur la normalisation de la cryptographie post-quantique et d'autres documents.
- La *Migration to Post-Quantum Cryptography (Migration vers la cryptographie post-quantique)* du National Cybersecurity Center of Excellence (Centre d'excellence de la cybersécurité nationale) (NCCOE) du NIST offre des conseils sur la migration vers la cryptographie post-quantique.
- *Les exigences relatives à la gestion symétrique des clés de l'Annexe V2.1* du Service central de sécurité de la NSA présente les exigences de mise en œuvre relatives à l'utilisation de clés pré-partagées pour les solutions commerciales classifiées (CSfC).
- Le site web du ministère de la Sécurité intérieure pour la cryptographie post-quantique comprend la feuille de route post-quantique du ministère et d'autres ressources.
- L'Initiative de cryptographie post-quantique de la Cybersecurity & Infrastructure Security Agency (CISA) unifie les efforts post-quantiques avec d'autres agences gouvernementales et partenaires de l'industrie pour faire face aux menaces du calcul quantique. Le site fournit également des liens vers d'autres ressources de la CISA, du NIST et du ministère de la Sécurité intérieure.

- Pour encourager la migration des systèmes informatiques du gouvernement fédéral vers la cryptographie résistante au quantique, le président Biden a signé le Quantum Computing Cybersecurity Act (HR 7535) (Loi relative à la sécurité liée au calcul quantique).
- Le mémorandum exécutif M-23-02, *Migrating to Post-Quantum Cryptography (Migration vers la cryptographie post-quantique)*, du Cabinet du Président donne des directives aux organismes américains sur la façon de se conformer au mémorandum sur la sécurité nationale 10 (NSM-10), *Mémorandum sur la sécurité nationale concernant la promotion du leadership des États-Unis du calcul quantique tout en atténuant les risques pour les systèmes cryptographiques vulnérables*.

Autres gouvernements dans le monde

Les liens suivants fournissent des informations sur la façon dont plusieurs gouvernements dans le monde s'attaquent à la question.

- L'Office fédéral allemand de la sécurité de l'information (BSI) fournit des informations sur la cryptographie post-quantique, les stratégies de migration, les développements actuels et des recommandations, et d'autres documents.
- Le Gouvernement du Royaume-Uni fournit des informations sur les ordinateurs et les technologies quantiques, la menace informatique quantique, la stratégie quantique nationale, la distribution des clés quantiques, la génération de nombres aléatoires quantiques et d'autres documents.
- L'Agence française de cybersécurité (ANSSI) fournit des informations sur la transition post-quantique, la distribution des clés quantiques et d'autres documents.
- Le Service général de renseignements et de sécurité (AIVD) des Pays-Bas fournit des informations sur les menaces informatiques quantiques, les stratégies et les étapes de migration post-quantique, la distribution des clés quantiques et d'autres documents.
- L'Agence de l'Union européenne pour la cybersécurité (ENISA) fournit des informations sur la cryptographie post-quantique, les mises en œuvre hybrides, les stratégies post-quantiques et d'autres documents.
- L'Autorité monétaire de Singapour fournit des informations sur les programmes quantiques et sur la lutte contre les risques de cybersécurité associés au quantique.
- Le Gouvernement japonais fournit des informations sur les stratégies quantiques, la sécurité quantique et la migration vers la technologie quantique.

Les RFC

Les demandes de propositions (RFC) décrivent les fondements techniques de l'Internet. Plusieurs RFC décrivent des aspects de la résistance IKEv2 aux attaques des ordinateurs quantiques :

- La RFC 8784, *Mélange de clés pré-partagées dans le protocole d'échange de clés Internet, version 2 (IKEv2) pour la sécurité post quantique*, décrit la norme pour l'extension IKE qui permet à IKEv2 d'être résistante aux attaques des ordinateurs quantiques. Comment la RFC 8784 résiste aux menaces du calcul quantique résume l'effet de la RFC 8784 sur votre réseau.
- La RFC 6379, *Suites de chiffrement Suite B pour IPsec*, décrit l'algorithme Suite-B-GCM-256 bits que vous devez utiliser au lieu du cryptage AES-128 bits plus faible. La suppression des cryptogrammes faibles tels que AES-128 contribue à retarder le moment où l'algorithme de Grover pourrait être capable de casser le cryptage symétrique.

- La RFC 9370, *Échanges de clés multiples dans le protocole d'échange de clé Internet version 2 (IKEv2)*, décrit la manière d'étendre IKEv2 pour permettre le mélange des échanges de clés multiples afin de créer la clé de cryptage.
- La RFC 9242, *Échange intermédiaire dans le protocole d'échange de clés Internet version 2 (IKEv2)*, définit un mécanisme d'échange intermédiaire qui permet le transfert de grandes quantités de données, telles que des clés de cryptage basées sur les échanges de clés multiples, dans l'échange de clés initial. Cela permet d'éviter la fragmentation. (Certains périphériques n'autorisent pas la fragmentation.)
- La RFC 7383, *Fragmentation du message du protocole Internet Key Exchange (échange de clés Internet) Version 2 (IKEv2)*, permet de fragmenter les messages IKE au niveau IKE, ce qui élimine les problèmes causés par la fragmentation IP. Cependant, la RFC 7383 ne fonctionne pas pour l'échange initial. La RFC 9242 permet d'éviter la fragmentation dans l'échange initial et la RFC 7383 évite la fragmentation IP dans les messages IKEv2 suivants.

Technologies et informations générales

De nombreuses organisations reconnaissent les menaces potentielles posées par les ordinateurs quantiques et par les technologies qui ne présentent aucun danger lorsqu'elles sont exécutées sur des ordinateurs classiques, mais qui présentent un danger potentiellement catastrophique lorsqu'elles sont exécutées sur un ordinateur quantique pertinent sur le plan cryptographique (CRQC).

- Le site liboqs de l'organisation Open Quantum Safe est une bibliothèque C open source pour les algorithmes cryptographiques sécurisés au niveau quantique.
- Le projet Alliance pour la cryptographie post-quantique de la Fondation Linux vise à relever les défis de sécurité cryptographique posés par l'informatique quantique en produisant des implémentations logicielles à haute assurance d'algorithmes normalisés.
- L'algorithme de Shor menace de casser de nombreux algorithmes classiques de cryptage asymétrique qui sont actuellement utilisés avec un CRQC. L'algorithme de Shor factorise de grands nombres complexes pour en tirer les nombres premiers qui constituent la base du cryptage asymétrique classique.
- L'algorithme de Grover est un algorithme de recherche quantique non structurée, accéléré quadratiquement. Il est capable de casser les algorithmes de cryptage symétrique classiques par la force brute en coupant de moitié la force cryptographique des algorithmes AES et des fonctions de hachage lorsqu'il est utilisé avec un CRQC.
- Les attaques Harvest Now, Decrypt Later sont une menace actuellement active. Dans les attaques Harvest Now, Decrypt Later, les attaquants volent des données qu'ils sont incapables de décrypter maintenant et les stockent jusqu'à ce qu'un CRQC puisse les décrypter. Ces attaques se déroulent aujourd'hui et constituent une menace immédiate pour les données à longue durée de vie.
- L'article de la base de connaissances Quantum Inspire *Qu'est-ce qu'un Qubit ?* explique les bits quantiques.
- L'article de Deloitte *The quantique Threat to Cryptography (La menace quantique à la cryptographie)* aborde les raisons pour lesquelles vous devriez commencer votre transition post-quantique dès que possible, tout comme l'article de Forbes *The Quantum Threat to Cryptography: Don't Panic, But Prepare Now (La menace quantique à la cryptographie : ne paniquez pas, mais préparez-vous dès aujourd'hui*.
- La publication *d'ETSI, Quantum-Safe Cryptography (QSC): A Repeatable Framework for Quantum-safe Migrations (La cryptographie sûre au niveau quantique : un cadre reproductible pour des migrations sûres au niveau quantique)* fournit un bon modèle pour créer un plan de migration post-quantique.

- Le *Plan directeur pour l’économie quantique du Forum économique mondial* fournit une feuille de route pour construire des écosystèmes quantiques de manière équitable afin de favoriser la transition vers l’économie quantique.

Configurer des VPN IKEv2 résistants au quantique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Les VPN IKEv2 résistants au quantique basés sur la RFC 8784 et/ou la RFC 9242 et la RFC 9370 empêchent les attaquants qui tentent d'exécuter des attaques Harvest Now, Decrypt Later de voler le matériel de la clé cryptographique utilisé pour crypter les données dans le VPN. Sans les clés cryptographiques, les attaquants ne peuvent pas décrypter ultérieurement les données récoltées à l'aide d'ordinateur quantique pertinent sur le plan cryptographique. Même si les attaquants réussissent à voler les données cryptées, ils seraient incapables de compromettre les données récoltées sans un ordinateur quantique pertinent sur le plan cryptographique qui leur permettrait de décrypter le matériau de la clé.

La RFC 8784 fournit une transition résistante au quantique de la cryptographie classique actuelle à la cryptographie post-quantique que vous pouvez mettre en œuvre aujourd'hui. La RFC 8784 ne nécessite pas de mise à niveau de la cryptographie, sa mise en œuvre est donc simple et rapide tant qu'elle peut être prise en charge par les deux périphériques VPN de chaque côté du tunnel.

Les RFC 9242 et 9370 sont plus gourmandes en ressources que la RFC 8784 mais fournissent une capacité de génération de clés dynamique basée sur les nouveaux algorithmes mathématiques de la PQC qui ne sont pas vulnérables à l'algorithme de Shor. Étant donné que les RFC 9242 et 9370 nécessitent des mises à niveau de la cryptographie, le déploiement de la technologie de clé hybride peut prendre plus de temps, ce qui nécessite de tenir compte de l'agilité cryptographique.

Ce chapitre vous montre comment configurer les VPN IKEv2 post-quantiques, y compris la manière de configurer les VPN IKEv2 post-quantiques dans des scénarios où vous connaissez l'homologue IKEv2 et ses capacités et des scénarios où vous ne contrôlez pas l'homologue IKEv2 et ne connaissez pas ses capacités.

- Configurer les VPN IKEv2 post-quantiques avec des PPK RFC 8784 vous indique les étapes et les options de configuration du VPN IKEv2 post-quantique pour sécuriser les communications VPN avec des clés pré-partagées post-quantiques.
- Configurer des VPN IKEv2 post-quantiques avec des clés hybrides des RFC 9242 et 9370 vous indique les étapes et les options de configuration pour sécuriser les communications VPN avec des clés hybrides.
- Exemple de configuration post-quantique IKEv2 de la RFC 8784 fournit un exemple de topologie simple et de la manière de configurer le support VPN IKEv2 post-quantique pour la topologie.

En plus de configurer les VPN IKEv2 post-quantiques basés sur la RFC 8784, conformez-vous à la RFC 6379 pour Suites de chiffrement Suite B pour IPsec pour mettre à niveau vos connexions VPN vers des suites de cryptage difficiles, mettre à niveau votre CA vers des tailles de clés RSA 4K afin d'atténuer les attaques par force brute capables de casser des tailles de clés plus petites et migrer l'authentification de votre certificat de VPN vers de nouveaux certificats, et mettre à niveau vers des tailles de hachage SHA à bits plus élevés, telles que SHA-384 et SHA-512.

Configurer les VPN IKEv2 post-quantiques avec des PPK RFC 8784

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Les VPN IKEv2 post-quantiques basés sur la RFC 8784 fonctionnent en transmettant un secret pré-partagé séparément (hors bande) de l'échange de couplage initial (l'échange IKE_SA_INIT). Au lieu de transmettre le secret pré-partagé dans l'échange de couplage, qu'un attaquant pourrait compromettre ou récolter maintenant et décrypter plus tard, l'échange de couplage ne transmet qu'un ID de clé. Un ID de clé et un secret pré-partagé comprennent une paire unique appelée clé pré-partagée post-quantique (PPK PQ).

Chaque homologue IKEv2 utilise l'ID de clé pour rechercher le secret pré-partagé, qui est transmis de manière sécurisée entre les administrateurs ou poussé par Panorama, et stocké localement sur chaque pair IKEv2. La clé pré-partagée ne fait jamais partie de l'échange de couplage et ne traverse jamais le VPN post-quantique, donc un attaquant utilisant un ordinateur quantique ne peut pas la voler, la décoder et l'utiliser pour décrypter les données récoltées à partir d'un VPN.

Les deux homologues IKEv2 doivent avoir les mêmes paires actives d'ID de clé en plus du secret pré-partagé afin que, lorsque les homologues négocient la connexion, chaque homologue puisse rechercher le même ID de clé et récupérer le même secret pré-partagé. Si l'homologue répondant ne dispose pas d'un ID de clé correspondant ou si le secret pré-partagé associé à l'ID de clé est différent de celui de l'initiateur, la connexion est abandonnée.

Configurez le couplage IKEv2 et un tunnel IPSec *avant de configurer vos composants post-quantiques. De plus, assurez-vous d'avoir des politiques de sécurité qui autorisent le trafic IKEv2 et IPSec entre les pare-feu et activent la journalisation.*

Pour rendre vos VPN IKEv2 résistants aux attaques quantiques :

STEP 1 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** et **Add (Ajouter)** une nouvelle passerelle.

STEP 2 | Configurez les paramètres de l'onglet **General (Général)** et sélectionnez le **IKEv2 only mode (Mode IKEv2 uniquement)** ou le **IKEv2 preferred mode (Mode IKEv2 préféré)** comme **Version**.

En **IKEv2 only mode (Mode IKEv2 uniquement)**, si l'homologue ne prend pas en charge IKEv2, le pare-feu abandonne la connexion. En **IKEv2 preferred mode (Mode IKEv2 préféré)**, si l'homologue ne prend pas en charge IKEv2, le pare-feu revient au mode IKEv1. Cependant, le VPN doit négocier IKEv2 pour utiliser les fonctionnalités VPN post-quantiques, donc si le pare-feu revient au mode IKEv1, ces fonctionnalités ne sont pas disponibles.

*IKEv1 est considéré comme étant faible. Si les deux homologues IKE peuvent le prendre en charge, mettez à niveau vos connexions VPN vers IKEv2 et sélectionnez **IKEv2 only mode (Mode IKEv2 uniquement)** pour garantir des niveaux de sécurité adéquats et la possibilité d'utiliser des VPN PQ.*

STEP 3 | Sélectionnez **Advanced Options (Options avancées)** et configurez les options non quantiques.

Si vous avez sélectionné **IKEv2 preferred mode (Mode KEv2 préféré)** comme **Version**, il y a des onglets pour **IKEv1** et **IKEv2** ; sélectionnez **IKEv2**. Si vous avez sélectionné **IKEv2 only mode (Mode IKEv2 uniquement)** comme **Version**, seules les options IKEv2 s'affichent.

Sélectionnez **PQ PPK (PPK PQ)** (clé pré-partagée post-quantique) pour configurer les éléments post-quantiques de votre VPN IKEv2. (**General (Général)** vous permet d'ajouter un profil crypto IKE et de définir la **Liveness Check (Vérification de l'activité)**.)

STEP 4 | **Enable Post-Quantum Pre-Shared Key (Activez la clé pré-partagée post-quantique) (PPK)** pour activer l'utilisation des fonctionnalités de résistance post-quantique sur le VPN. Cette option est désactivée par défaut.

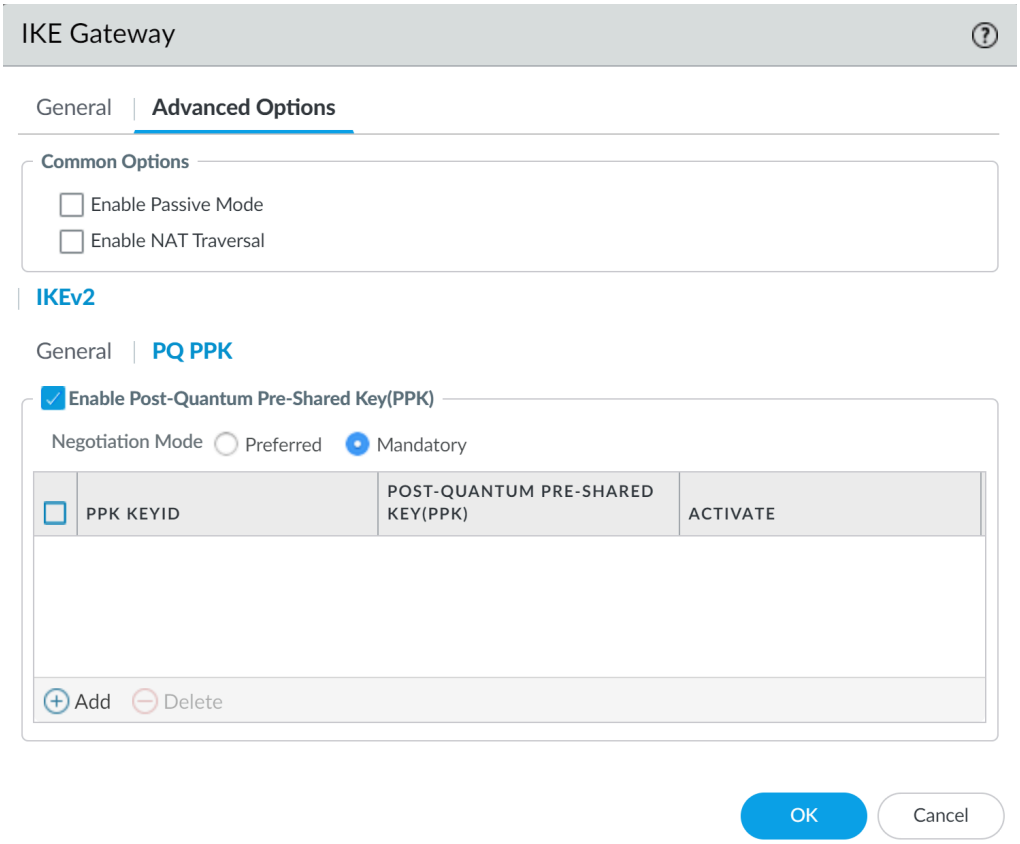
*Vous devez configurer et activer au moins une PPK PQ lorsque vous **Enable Post-Quantum Pre-Shared Key (Activez la clé pré-partagée post-quantique) (PPK)** afin que le pare-feu dispose d'une PPK PQ à utiliser pendant la négociation IKEv2 et puisse prendre en charge la RFC 8784.*

STEP 5 | Configurez le **Negotiation Mode (Mode de négociation)** sur **Preferred (Préféré)** ou **Mandatory (Obligatoire)**.

- **Preferred (Préféré)** : lorsque le pare-feu négocie avec l'homologue, le pare-feu tente d'abord de négocier à l'aide des PPK PQ. Si l'homologue ne prend pas en charge la RFC 8784, le pare-feu revient à un échange de clés classique pour la connexion. Si vous ne savez pas si l'homologue prend en charge la RFC 8784 ou si vous ne pouvez pas le contrôler, le mode **Preferred (Préféré)** préserve la compatibilité descendante pour garantir un retour des connexions au lieu de leur interruption. **Preferred (Préféré)** est le mode par défaut.
- **Mandatory (Obligatoire)** : lorsque le pare-feu négocie avec l'homologue, celui-ci doit prendre en charge les PPK PQ de la RFC 8784. Si l'homologue répondant ne prend pas en charge le RFC 8784,

le pare-feu abandonne la connexion. Utilisez le mode **Mandatory (Obligatoire)** lorsque vous savez que l'homologue prend en charge les PPK PQ de la RFC 8784.

*Utilisez le mode **Mandatory (Obligatoire)** quand vous le pouvez pour obtenir une meilleure sécurité.*



STEP 6 | Vous pouvez **Add (Ajouter)** et **Activate (Activer)** jusqu'à dix PPK PQ uniques.

Une PPK PQ se compose de deux éléments couplés : un ID de clé PPK et un secret PPK. L'ID de clé PPK est une chaîne unique qui identifie le secret PPK et peut être composée de n'importe quoi jusqu'à 31 caractères, comme **`PPK-1`** ou **`PPK super fort`**. Le secret PPK est la clé pré-partagée aléatoire qui n'est jamais transmise via le VPN parce que les administrateurs des deux homologues la partagent par une méthode de communication sécurisée et la configurent sur les homologues hors bande. Le pare-feu transmet uniquement l'ID de clé dans le VPN IKEv2 afin que l'homologue puisse rechercher le secret PPK au niveau local.

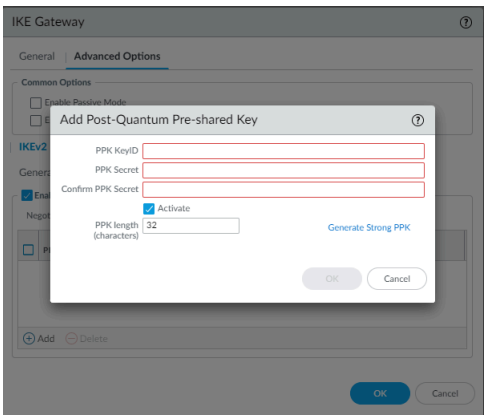
Le nombre de PPK PQ que vous pouvez définir dépend du nombre pouvant être pris en charge par l'homologue IKE. Certaines mises en œuvre de fournisseurs autorisent moins de dix PPK PQ uniques; et d'autres n'en autorisent qu'une seule. Ne définissez pas un nombre de PPK PQ supérieur à celui que

l'homologue peut prendre en charge car les deux homologues doivent avoir exactement les mêmes PPK PQ disponibles.

Configurez plusieurs PPK PQ actives pour les homologues qui prennent en charge plusieurs PPK PQ. Le pare-feu choisit de manière aléatoire parmi les PPK PQ actives, ce qui ajoute un élément aléatoire à la négociation IKEv2.

Une configuration de plusieurs PPK PQ est la plus sécurisée car elle ajoute un élément aléatoire à la sélection des PPK PQ.

Vous pouvez créer le secret PPK manuellement ou générer un secret fort sur le pare-feu. Configurez le secret PPK manuellement si vous souhaitez générer la clé vous-même ou si vous recevez un PPK PQ de l'administrateur d'un homologue et que vous devez le configurer sur votre pare-feu. Plus le secret PPK est long, plus le nombre de bits d'entropie est important, ce qui rend le secret PPK plus difficile à décoder.



Pour configurer le secret PPK manuellement, vous pouvez le spécifier à l'aide de caractères ASCII :

1. Spécifiez un **PPK KeyID (ID de clé PPK)** unique de 31 caractères maximum.
2. Spécifiez une chaîne de **PPK Secret (Secret PPK)** unique et aléatoire. La chaîne peut contenir de 32 à 128 caractères (16 à 64 octets, ce qui équivaut à 128 à 512 bits d'entropie).

   *Spécifiez un **PPK Secret (Secret PPK)** d'au moins 64 caractères (32 octets, ou 256 bits d'entropie) de longueur pour créer une clé forte.*
3. Spécifiez exactement la même chaîne dans **Confirm PPK Secret (Confirmer le secret PPK)**.

   Conservez le secret PPK en toute sécurité. Le secret PPK n'est pas affiché en clair, donc si vous ne le stockez pas maintenant, vous ne pourrez pas le récupérer par la suite. (Vous pouvez supprimer la PPK PQ et en configurer une autre si nécessaire.) Comme l'homologue IKEv2 doit avoir la même PPK PQ (ID de clé et secret PPK), vous devrez peut-être communiquer le secret PPK à un autre administrateur. Si c'est le cas, veillez à ce que la méthode de communication utilisée soit cryptographiquement sécurisée et que le secret PPK soit stocké en toute sécurité.

   La NSA publie des conseils sur la manipulation des clés pré-partagées en toute sécurité, notamment la RFC 8784 sur les clés pré-partagées quantiques.

4. **Activate (Activer)** est sélectionné par défaut afin que le pare-feu puisse utiliser la paire ID de clé PPK et secret PPK (la PPK PQ) pour négocier avec l'homologue. Si vous ne voulez pas que le pare-feu utilise cette paire d'ID de clé PPK et secret PPK lors de négociations avec des homologues, décochez **Activate (Activer)**.

   Par exemple, si vous configurez une nouvelle PPK PQ sur un pare-feu, vous pourriez devoir la désactiver jusqu'à ce que l'administrateur de l'homologue puisse ajouter la même PPK PQ à l'homologue pour éviter un échec de connexion parce que l'initiateur utilise une PPK PQ qui n'est pas encore installée sur l'homologue.
5. Cliquez sur **OK**. L'onglet **PQ PPK (PPK PQ)** affiche l'ID de clé PPK en clair, masque la clé pré-partagée et affiche l'état d'activation de la PPK PQ.

Pour configurer le secret PPK à l'aide de la génération PPK forte automatique du pare-feu, qui utilise des caractères hexadécimaux :

1. Spécifiez un **PPK KeyID (ID de clé PPK)** unique de 31 caractères maximum.
2. Définissez **PPK length (characters) (Longueur PPK (caractères))** sur la longueur que vous souhaitez générer pour le **PPK Secret (Secret PPK)**. La valeur par défaut est de 32 caractères (16 octets).

   *Configurez **PPK length (characters) (Longueur PPK (caractères))** sur une longueur d'au moins 64 caractères (32 octets, soit 256 bits d'entropie) pour générer une clé forte.*
3. Cliquez sur **Generate Strong PPK (Générer une PPK fort)**. Le pare-feu génère et affiche un secret PPK fort de la longueur spécifiée dans **PPK length (characters) (Longueur de la PPK (caractères))**.

   C'est la seule fois où le secret PPK est affiché en clair. Si vous ne stockez pas le secret en toute sécurité, vous ne pouvez pas le récupérer. (Vous pouvez supprimer la PPK PQ et en configurer une autre si nécessaire.) Comme l'homologue IKEv2 doit avoir la même PPK PQ (ID de clé et secret PPK), vous devrez peut-être communiquer le secret PPK à un autre administrateur. Si c'est le cas, veillez à ce que la méthode de communication utilisée soit cryptographiquement sécurisée et que le secret PPK soit stocké en toute sécurité.

   Copiez le secret PPK, cliquez sur **OK** et collez-le dans les champs **PPK Secret (Secret PPK)** et **Confirm PPK Secret (Confirmer le secret PK)**.
4. **Activate (Activer)** est sélectionné par défaut afin que le pare-feu puisse utiliser la paire ID de clé PPK et secret PPK (la PPK PQ) pour négocier avec l'homologue. Si vous ne voulez pas que le pare-feu utilise cette paire d'ID de clé PPK et secret PPK lors de négociations avec des homologues, décochez **Activate (Activer)**.

   Par exemple, si vous configurez une nouvelle PPK PQ sur un pare-feu, vous pourriez devoir la désactiver jusqu'à ce que l'administrateur de l'homologue puisse ajouter la même PPK PQ à l'homologue pour éviter un échec de connexion parce que l'initiateur utilise une PPK PQ qui n'est pas encore installée sur l'homologue.
5. Cliquez sur **OK**. L'onglet **PQ PPK (PPK PQ)** affiche l'ID de clé PPK en clair, masque la clé pré-partagée et affiche l'état d'activation de la PPK PQ.

STEP 7 | Cliquez sur **OK** pour créer le VPN.

STEP 8 | **Commit (Validez)** la configuration.

La rubrique Exemple de configuration post-quantique IKEv2 de la RFC 8784 *fournit un exemple de topologie simple et de la manière de configurer la prise en charge du VPN de l'IKEv2 post-quantique pour la topologie.*

STEP 9 | Si vous n'êtes pas l'administrateur des deux homologues IKEv2, communiquez la PPK PQ (ID de clé et secret PPK) à l'administrateur de l'homologue de manière sécurisée pour l'installer sur l'homologue. La communication et le stockage sécurisés de la PPK PQ sont essentiels pour sécuriser vos données.

Les deux homologues IKEv2 doivent avoir les mêmes ID de clé actifs et les mêmes secrets pré-partagés associés pour lancer la connexion VPN post-quantique.

Configurer des VPN IKEv2 post-quantiques avec des clés hybrides des RFC 9242 et 9370

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.2 ou version ultérieure.

Les VPN IKEv2 post-quantiques basés sur les RFC 9242 et 9370 fonctionnent en créant une clé hybride à l'aide de deux ou plusieurs mécanismes d'échange de clés (KEM) dans l'échange de couplage initial (l'échange IKE_SA_INIT). Les clés hybrides fournissent une résistance quantique en empêchant un KEM compromis de permettre la réussite d'une attaque quantique utilisant Harvest Now, Decrypt Later (HNDL). Tant que tous les KEM utilisés pour créer la clé hybride ne sont pas compromis, les données restent protégées.

Étant donné que les normes sont encore relativement récentes et que chaque fournisseur peut avoir des interprétations différentes de la mise en œuvre de la norme, la conservation des configurations identiques des deux côtés permet de simplifier les choses et de permettre le lancement réussi du tunnel VPN post-quantique. Pour minimiser les chances d'interopérabilité, assurez-vous de configurer les deux côtés du tunnel VPN avec les mêmes PQC et les mêmes niveaux de sécurité dans chacun des cycles de négociation de clés facultatifs. Vérifiez également les paramètres de fragmentation IKEv2 des deux côtés pour vérifier qu'ils sont correctement configurés.

Configurez le couplage IKEv2 et un tunnel IPSec *avant de configurer vos composants post-quantiques. De plus, assurez-vous d'avoir des politiques de sécurité qui autorisent le trafic IKEv2 et IPSec entre les pare-feu et activent la journalisation.*

Pour garantir la protection des données pendant de longues durées, il convient d'utiliser plus de deux KEM et vous pouvez ajouter une défense en profondeur supplémentaire en activant la clé pré-partagée via la RFC 8784 et la clé hybride via les RFC 9242 et 9370.

Pour rendre vos VPN IKEv2 résistants aux attaques quantiques :

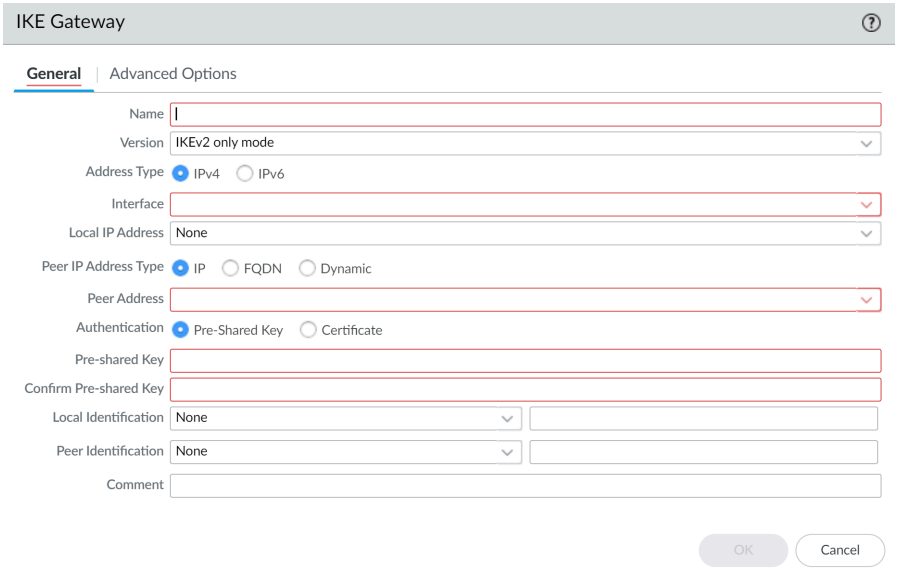
STEP 1 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** et **Add (Ajouter)** une nouvelle passerelle.

STEP 2 | Configurez les paramètres **General (Général)** et sélectionnez **IKEv2 only mode (Mode IKEv2 uniquement)** ou **IKEv2 preferred mode (Mode IKEv2 préféré)** comme **Version**.

En **IKEv2 only mode (Mode IKEv2 uniquement)**, si l'homologue ne prend pas en charge IKEv2, le pare-feu abandonne la connexion. En **IKEv2 preferred mode (Mode IKEv2 préféré)**, si l'homologue ne prend pas en charge IKEv2, le pare-feu revient au mode IKEv1. Cependant, le VPN doit négocier

IKEv2 pour utiliser les fonctionnalités VPN post-quantiques, donc si le pare-feu revient au mode IKEv1, ces fonctionnalités ne sont pas disponibles.

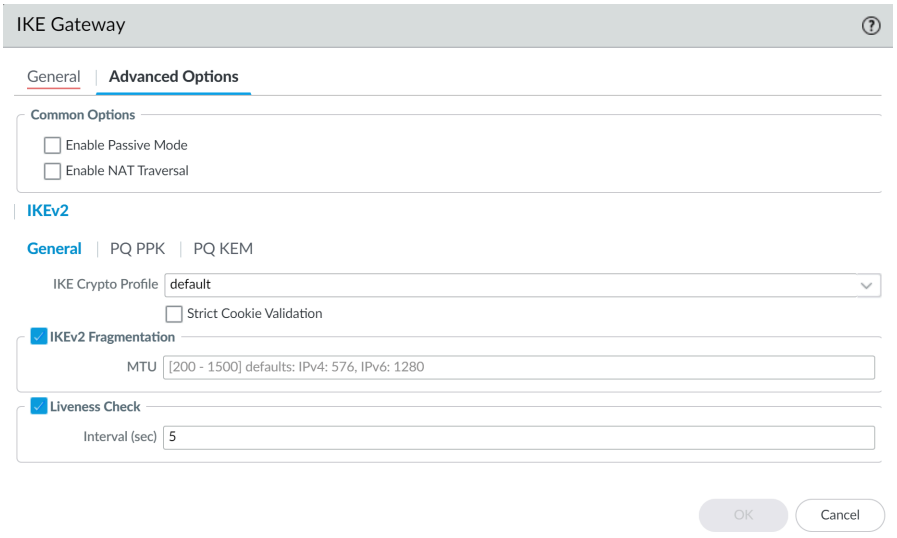
*IKEv1 est considéré comme étant faible. Si les deux homologues IKE peuvent le prendre en charge, mettez à niveau vos connexions VPN vers IKEv2 et sélectionnez **IKEv2 only mode (Mode IKEv2 uniquement)** pour garantir des niveaux de sécurité adéquats et la possibilité d'utiliser des VPN PQ.*



STEP 3 | Sélectionnez **Advanced Options (Options avancées)** et configurez les options non quantiques. Sélectionnez **IKEv2** et configurez les paramètres **General (Général)**.

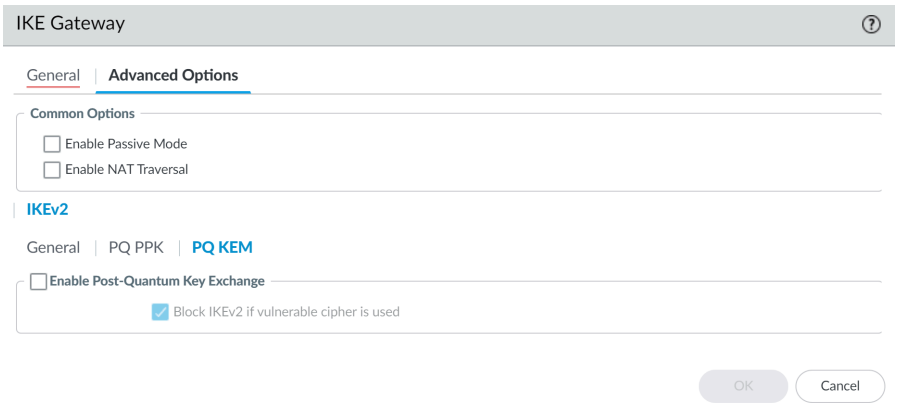
L'option Général vous permet d'ajouter un profil crypto IKE, d'activer **IKEv2 Fragmentation (Fragmentation IKEv2)** et de définir la **Liveness Check (Vérification de l'activité)**.

La fragmentation IKEv2 doit être activée lors de l'utilisation de KEM de PQC car les tailles de clé et les charges utiles de données sont plus importantes. Les deux périphériques de fin de VPN doivent être définis sur les mêmes valeurs de fragmentation.



STEP 4 | **Enable Post-Quantum Key Exchange (Activez l’échange de clés post-quantique)** pour KEM PQ pour activer l’utilisation des fonctionnalités de résistance post-quantique sur le VPN. Cette option est désactivée par défaut.

En option, activez **Block IKEv2 if vulnerable cipher is used (Bloquer IKEv2 si un cryptage vulnérable est utilisé)**. Si cette option est activée, le pare-feu bloque tous les nouveaux couplages IKEv2 s’il détecte l’utilisation d’un KEM vulnérable dans le profil crypto IKE. Les tunnels VPN existants déjà créés peuvent continuer.

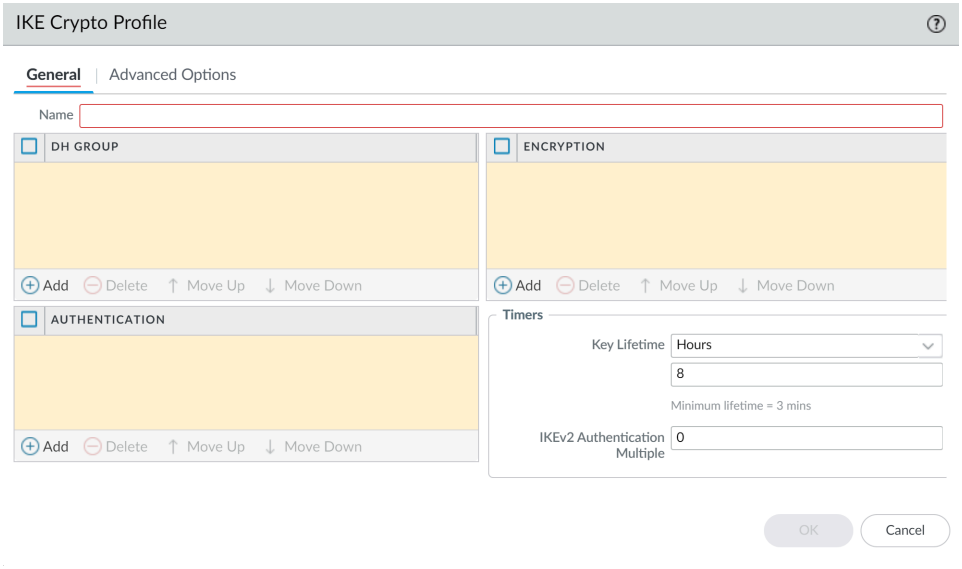


STEP 5 | Cliquez sur **OK** pour créer la passerelle IKE.

STEP 6 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)** puis **Add (Ajouter)** un nouveau profil.

STEP 7 | Configurez les paramètres **General (Général)** et sélectionnez les composants cryptographiques (groupe DH, cryptage, authentification, minuteries) pour l'échange de clés IKEv2 par défaut.

Sélectionnez une configuration d'échange de clés classique forte pour augmenter la résistance quantique : groupe DH 20 ou supérieur, AES-256-GCM et actualisez les clés plus fréquemment en utilisant la durée de vie de la clé. Pour régénérer la clé complètement à des intervalles spécifiques, activez l'authentification multiple IKEv2 en définissant une valeur supérieure à zéro. La clé est régénérée une fois que le multiple de la durée de vie de la clé est atteint.



STEP 8 | Sélectionnez les **Advanced Options (Options avancées)** et configurez les cycles **Post-Quantum IKEv2 Additional Key Exchange (Échange de clés supplémentaire post-quantique IKEv2)** facultatifs.

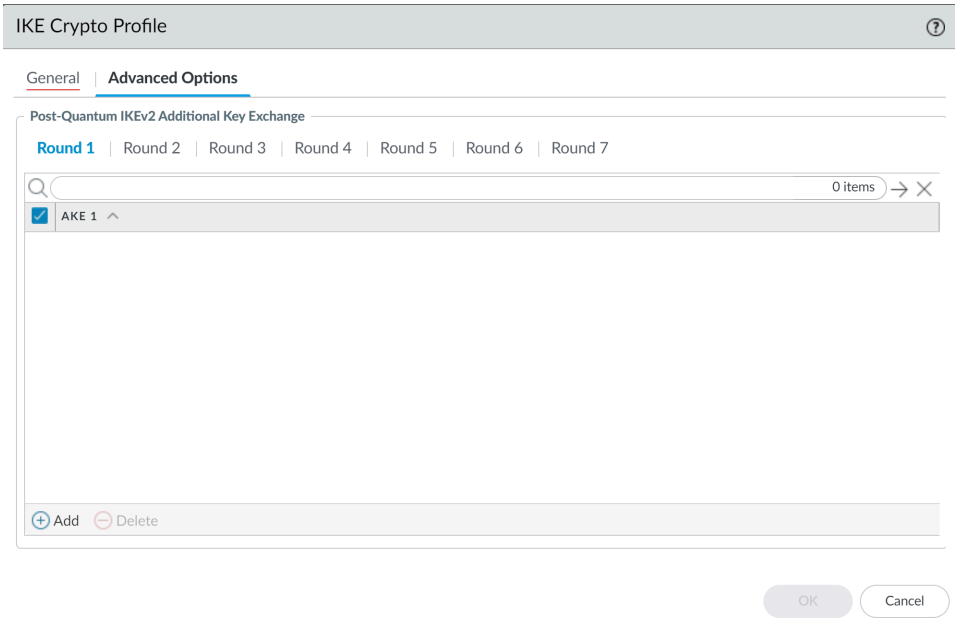
Un maximum de sept **Additional Key Exchange Rounds (Cycles d'échange de clés supplémentaires)** (cycles 1 à 7) sont autorisés dans la RFC 9370. Au minimum, un KEM PQC est nécessaire pour ajouter une résistance quantique. L'ajout de KEM de PQC supplémentaires augmente davantage la résistance quantique, mais ajoute une surcharge de négociation et augmente la taille des paquets IKEv2.

La RFC 9370 permet d'ignorer les cycles d'échange de clés supplémentaires. Les cycles ignorés peuvent être laissés vides ou être définis sur **None (Aucun)**.

L'ordre des PQC dans le cycle d'échange de clés supplémentaire définit la préférence. La PQC répertoriée en haut est préférée et est sélectionnée si elle est prise en charge par le périphérique de fin de VPN de l'autre côté du tunnel. Si vous souhaitez négocier la PQC la plus forte pouvant être prise en

charge par les deux parties, placez la PQC ayant le niveau de sécurité le plus élevé en haut de la liste dans chaque cycle d'échange de clés supplémentaire.

Les périphériques de fin de VPN des deux côtés du tunnel doivent être configurés avec la même PQC et le même niveau de sécurité afin de réduire les problèmes d'interopérabilité. Pour sécuriser les informations sensibles pendant de longues périodes, sélectionnez une PQC ayant une sécurité équivalente au niveau 3 ou supérieure.

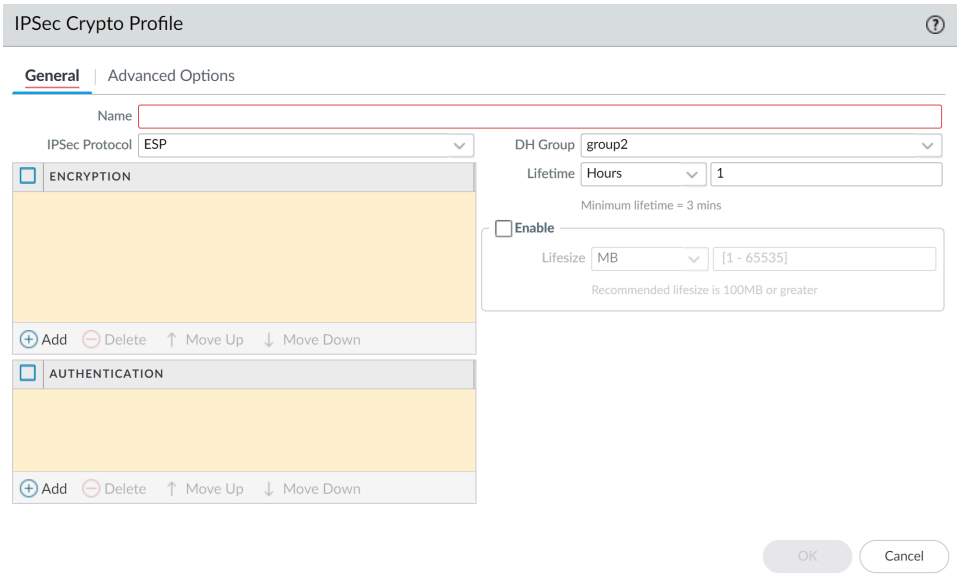


STEP 9 | Cliquez sur **OK** pour créer le profil crypto IKE.

STEP 10 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**, puis **Add (Ajouter)** un nouveau profil.

STEP 11 | Configurez les paramètres **General (Général)** et sélectionnez les composants cryptographiques du protocole ESP IPSec (cryptage, authentification, groupe DH, durée de vie).

Sélectionnez une configuration cryptographique classique forte pour augmenter la résistance quantique : Groupe DH 20 ou supérieur, AES-256-GCM, SHA384 ou supérieur et actualisez les clés plus fréquemment en utilisant la durée de vie de la clé.



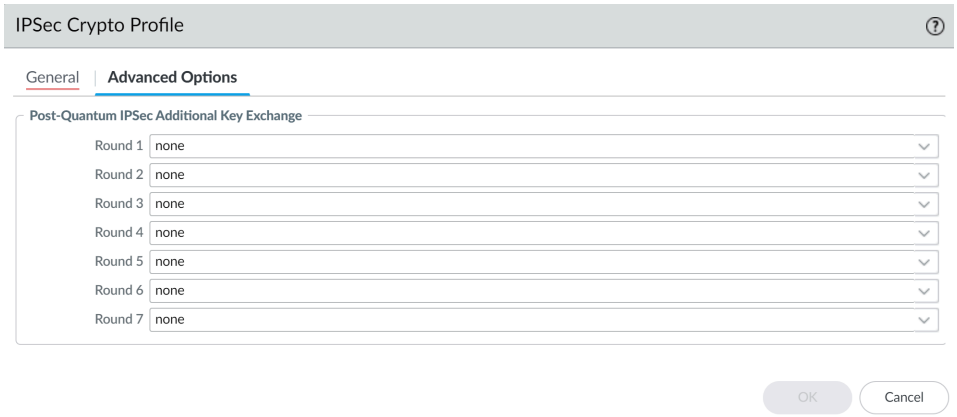
STEP 12 | Sélectionnez les **Advanced Options (Options avancées)** et configurez les cycles **Post-Quantum IPSec Additional Key Exchange (Échange de clés supplémentaire post-quantique IPSec)** facultatifs.

Un maximum de sept **Additional Key Exchange Rounds (Cycles d'échange de clés supplémentaires)** (cycles 1 à 7) sont autorisés et un seul KEM PQC est autorisé par cycle. Au minimum, un KEM PQC est nécessaire pour ajouter une résistance quantique. L'ajout de KEM de PQC

supplémentaires augmente davantage la résistance quantique, mais ajoute une surcharge de négociation et augmente la taille des paquets de changement de clé IPSec.

Les deux côtés du tunnel IPSec doivent être configurés avec la même PQC et le même niveau de force de sécurité à chaque cycle d'échange de clés supplémentaire. En cas d'incompatibilité, l'opération de changement de clé échoue.

Pour sécuriser les informations sensibles pendant de longues périodes, sélectionnez une PQC ayant une sécurité équivalente au niveau 3 ou supérieure.



STEP 13 | Cliquez sur **OK** pour créer le profil crypto IPSec.

STEP 14 | **Commit (Validez)** la configuration.

Si vous n'êtes pas l'administrateur des deux homologues IKEv2, communiquez les informations de la passerelle IKEv2, du profil crypto IKE et du profil crypto IPSec à l'administrateur de l'homologue pour l'installation sur son périphérique homologue.

Exemple de configuration post-quantique IKEv2 de la RFC 8784

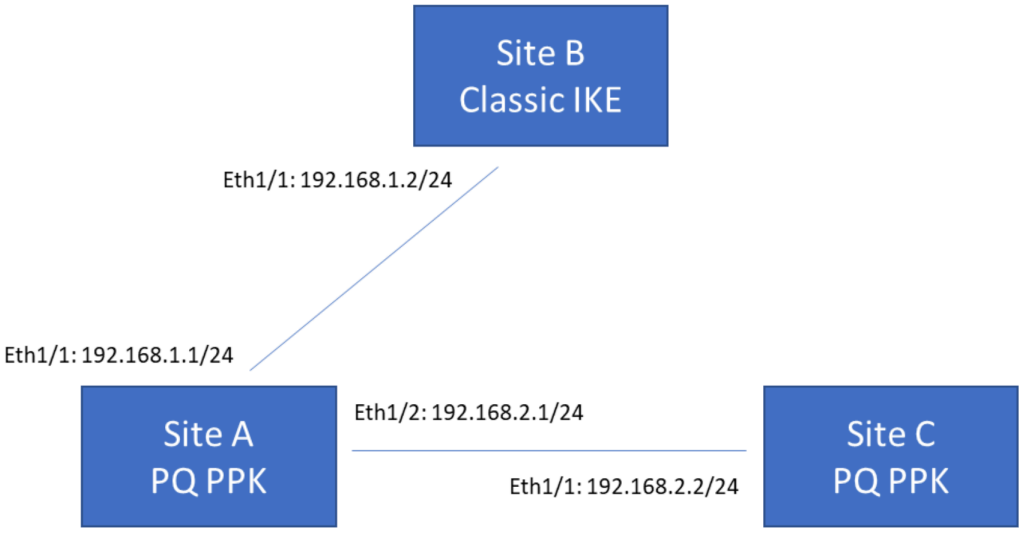
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	❑ PAN-OS 11.1 ou version ultérieure.

Cet exemple fournit une configuration et une topologie de VPN post-quantique IKEv2 de base. Il comprend deux sites qui prennent en charge la RFC 8784 (des VPN post-quantiques qui résistent aux attaques des ordinateurs quantiques et de la cryptographie quantique) et un site qui ne prend pas en charge la RFC 8784.

Lorsqu’un pare-feu qui prend en charge la RFC 8784 communique avec un pare-feu qui prend également en charge la RFC 8784, les périphériques utilisent la configuration post-quantique. L’échange de clés utilise des clés pré-partagées post-quantiques (PPK PQ) qui sont partagées hors bande à partir de la connexion, de sorte que la PPK PQ n’est jamais exposée lors de l’établissement de la connexion IKE. Les pare-feu mélangent la PPK PQ avec le matériel de la clé classique Diffie-Hellmann (DH) (qui est transmis lors de l’établissement de la connexion IKE) pour créer une clé qui n’est pas basée sur des nombres premiers et ne peut donc pas être décodée par l’algorithme de Shor. Cela permet aux pare-feu de créer une clé résistante au quantique pour se protéger contre une attaque Harvest Now, Decrypt Later dans laquelle les attaquants volent des données qu’ils ne peuvent pas décrypter maintenant et les stockent jusqu’à ce qu’ils puissent utiliser un ordinateur quantique pertinent sur le plan cryptographique (CRQC) pour les décrypter.

Lorsqu’un pare-feu qui prend en charge la RFC 8784 communique avec un pare-feu qui ne prend pas en charge la RFC 8784, le pare-feu prenant en charge la RFC 8784 peut revenir à l’échange de clés DH classique. Si cela se produit, les pare-feu ne se mélangent pas dans une PPK PQ et n’utilisent que le matériel de la clé DH pour créer la clé. Il est important de comprendre que, dans ce cas, le trafic VPN est vulnérable aux attaques Harvest Now, Decrypt Later.

Cet exemple simple de topologie se compose de trois pare-feu situés sur différents sites et connectés par des VPN IKEv2. Deux des pare-feu prennent en charge la RFC 8784 et un pare-feu ne prend pas en charge la RFC 8784.



Dans cet exemple :

- **Le site A** prend en charge la RFC 8784. Sa connexion au site B est Eth1/1 : 192.168.1.1/24 et sa connexion au site C est Eth1/2 : 192.168.2.1/24. Le site A doit avoir deux passerelles IKEv2, l'une pour se connecter au site B et l'autre pour se connecter au site A.
- **Le site B** ne prend en charge que les VPN IKEv2 classiques et ne prend pas en charge la RFC 8784. Sa connexion au site A est Eth1/1 : 192.168.1.2/24. Le site B doit avoir une passerelle IKEv2 pour se connecter au site A. La configuration de la passerelle IKEv2 du site B n'inclut pas les PPK PQ, car le site B ne prend pas en charge la RFC 8784.
- **Le site C** prend en charge la RFC 8784. Sa connexion au site A est Eth1/1 : 192.168.2.2/24. Le site C doit avoir une passerelle IKEv2 pour se connecter au site A.

Chaque homologue VPN IKEv2 qui prend en charge la RFC 8784 doit avoir exactement le même ensemble de PPK PQ (paires de chaînes d'ID de clé et de secret PPK) installé et activé. La connexion est abandonnée si la PPK PQ sélectionnée n'est pas disponible sur les deux homologues.

L'ID de clé identifie la chaîne du secret PPK.

Les homologues IKEv2 transmettent l'ID de clé lors de l'établissement de la connexion IKEv2, mais la chaîne du secret PPK est partagée hors bande et installée séparément sur chaque homologue, ou transmise par Panorama, ou installée manuellement. La chaîne du secret PPK n'est jamais envoyée dans l'établissement de la connexion ni affichée dans le tunnel IKEv2 résultant. Les homologues IKEv2 utilisent plutôt l'ID de clé pour rechercher localement la chaîne du secret PPK et la mélanger avec le matériel de la clé DH afin de générer la clé de cryptage post-quantique.

Pour configurer les VPN IKEv2 pour l'exemple de topologie, accédez à **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** :

STEP 1 | Configurez les propriétés générales de la passerelle VPN IKEv2 pour les sites A, B et C comme pour toute autre passerelle IKE.

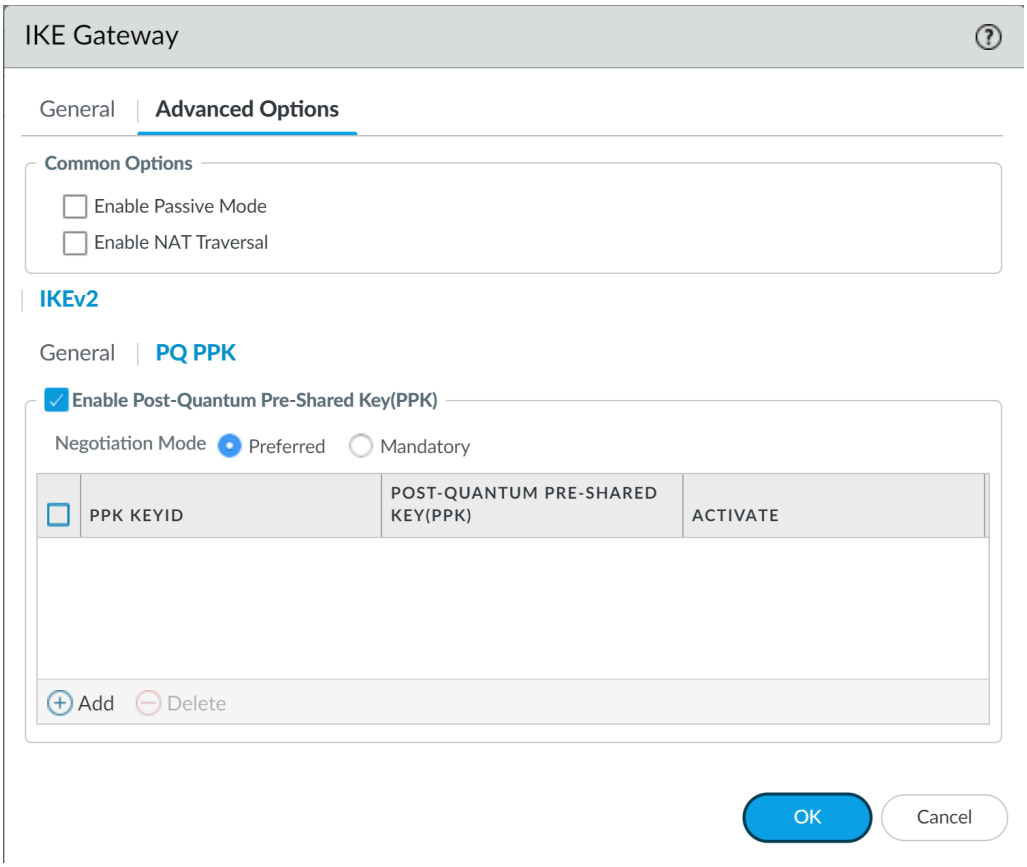
Dans l'onglet **General (Général)**, configurez les adresses, l'authentification et d'autres informations générales sur la passerelle IKE. Définissez la **Version** sur **IKEv2 mode only (Mode IKEv2 uniquement)** pour une sécurité optimale. IKEv1 est considéré comme un protocole faible qui ne prend pas en charge les VPN post-quantiques de la RFC 8784.

*La clé pré-partagée que vous configurez sur l'onglet **General (Général)** n'est pas la clé pré-partagée post-quantique qui résiste aux attaques quantiques. Celle-ci est utilisée pour l'authentification symétrique sur l'ensemble du tunnel.*

STEP 2 | Configurez des **Advanced Options (Options avancées)** communes et générales, notamment mode passif, parcours NAT et profil crypto IKE pour les trois sites.

STEP 3 | Dans l'onglet **Advanced Options (Options avancées)** > **PQ PPK (PPK PQ)**, **Enable Post-Quantum Pre-Shared Key (PPK) (Activer la clé pré-partagée post-quantique (PPK))** pour VPN IKEv2 du site A vers le site C et sur le VPN IKEv2 du site C vers le site A.

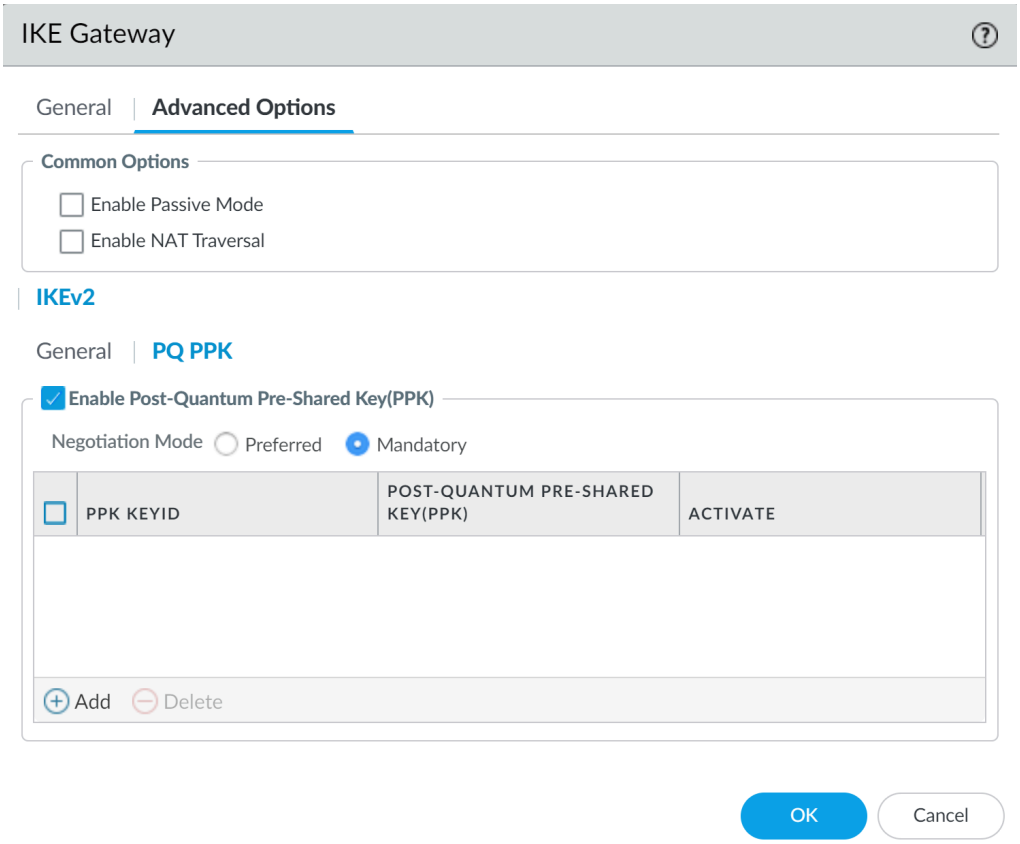
Étant donné que le site B ne prend pas en charge la RFC 8784, il n'est pas nécessaire de **Enable Post-Quantum Pre-Shared Key (PPK) (Activer la clé pré-partagée post-quantique (PPK))** dans la configuration de la passerelle IKE du site B ou dans la configuration du VPN IKEv2 du site A vers le site B.



Lorsque vous **Enable Post-Quantum Pre-Shared Key (PPK) (Activez la clé pré-partagée post-quantique (PPK))**, le paramètre par défaut du **Negotiation Mode (Mode de négociation)**

est **Preferred (Préféré)**, ce qui signifie que les connexions qui ne peuvent pas prendre en charge la RFC 8784 reviennent à la cryptographie classique. (En mode **Mandatory (Obligatoire)**, si l'homologue ne prend pas en charge les PPK PQ, le pare-feu abandonne la connexion.)

STEP 4 | Définissez le **Negotiation Mode (Mode de négociation)** dans les VPN IKEv2 du site A vers le site C et du site C vers le site A sur **Mandatory (Obligatoire)**.



L'utilisation de **Mandatory (Obligatoire)** comme **Negotiation Mode (Mode de négociation)** garantit que le site A et le site C configurent toujours des VPN résistants au quantique au lieu de VPN classiques lorsqu'ils négocient des tunnels VPN. Utilisez **Mandatory (Obligatoire)** lorsque vous êtes sûr que les homologues prennent en charge la RFC 8784. Si vous n'en êtes pas certain, utilisez **Preferred (Préféré)** afin que le pare-feu puisse revenir aux VPN IKEv2 classiques si l'homologue ne prend pas en charge la RFC 8784, comme, par exemple, lors d'un couplage avec des périphériques extérieurs à votre entreprise que vous ne contrôlez pas.

STEP 5 | Configurez les PPK PQ actives pour la connexion IKEv2 du site A au site C et pour la connexion IKEv2 du site C au site A. Lorsque le site A et le site C activent la connexion IKEv2, ils

sélectionnent parmi les PPK PQ actives et mélangent la PPK PQ choisie avec le matériel de la clé DH afin de créer une clé sécurisée qui n'est pas basée sur des nombres premiers.

Il n'existe pas de configuration post-quantique pour la communication du site A vers le site B ou du site B vers le site A, car le site B ne prend pas en charge la RFC 8784.

Les homologues IKEv2 du site A et du site C doivent avoir exactement la même configuration de PPK PQ actives.

- Si Panorama gère les deux homologues IKEv2, vous pouvez créer la configuration sur Panorama et la transmettre aux pare-feu gérés.
- Si Panorama ne gère pas les deux homologues IKEv2 et qu'ils sont contrôlés par des administrateurs différents, communiquez la PPK PQ à l'autre administrateur de manière sécurisée, comme par messagerie cryptée, et stockez la clé en toute sécurité.

Vous pouvez donner le nom de votre choix à chaque ID de clé de PPK PQ. Vous pouvez configurer le secret PPK que vous associez à l'ID de clé manuellement pour chaque PPK PQ, ou le pare-feu peut générer un secret PPK fort pour vous. Cet exemple vous montre la manière d'utiliser les deux méthodes.

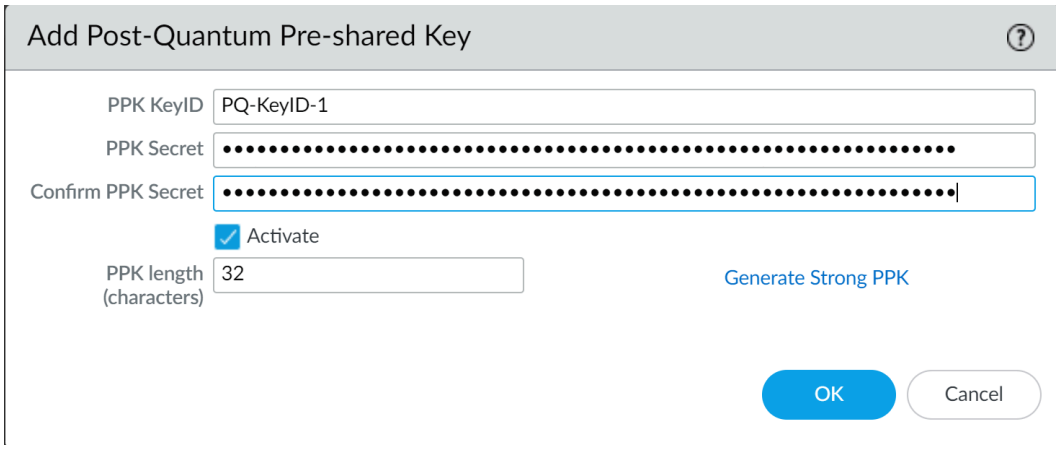
Pour créer la PPK PQ avec un secret PPK configuré manuellement :

1. **Add (Ajouter)** une PPK PQ.
2. Dans la boîte de dialogue **Add Post-Quantum Pre-shared Key (Ajouter une clé pré-partagée post-quantique)**, saisissez le nom de **PPK KeyID (ID de clé PPK)**. Dans cet exemple, le nom est **`PQ-KeyID-1`**.
3. Tapez (ou copiez-collez à partir d'une autre source) la même chaîne ASCII exactement dans **PPK KeyID (ID de clé PPK)**, puis **Confirm PPK Secret (Confirmer le secret PPK)**.

   Stockez la PPK PQ (l'ID de clé et son secret PPK) en toute sécurité. Pour les secrets PPK saisis manuellement, le secret n'est jamais affiché en texte en clair. Si vous perdez le secret PPK, vous ne pouvez pas le récupérer. (Vous pouvez supprimer la PPK PQ, puis en configurer une nouvelle.)

   Si les entrées **PPK KeyID (ID de clé PPK)** et **Confirm PPK Secret (Confirmer le secret PPK)** ne correspond pas, le message d'erreur `PPK Secret and Confirm PPK Secret Do Not Match (Le secret PPK et la confirmation du secret PPK ne correspondent pas)` s'affiche. Une bonne pratique recommande de spécifier un secret PPK aléatoire d'au moins 64 caractères (32 octets ou 256 bits d'entropie) pour créer une clé forte. Par défaut, la nouvelle clé est active. Si vous ne souhaitez pas utiliser la clé dans la négociation entre les homologues IKE, désélectionnez **Activate (Activer)**. Si vous désactivez la PPK PQ sur un homologue, vous devez également la désactiver sur l'autre homologue.

L’exemple suivant montre une clé forte de 64 caractères (les clés saisies manuellement ne sont jamais affichées en texte clair) :



*Le champ **PPK length (characters) (Longueur de la PPK (caractères))** ne s’applique qu’aux clés générées par le pare-feu pour vous. Il ne contrôle pas la longueur des chaînes de secret PPK configurées manuellement.*

4. Cliquez sur **OK** pour installer la PPK PQ configurée manuellement.
5. Si Panorama gère les deux homologues, vous pouvez créer la configuration sur Panorama et la transmettre vers les pare-feu gérés. Si Panorama ne gère pas les deux homologues et qu’un autre

administrateur contrôle l'homologue VPN, communiquez la PPK PQ de manière sécurisée à cet administrateur, qui l'installe sur l'homologue.

Pour créer la PPK PQ avec un secret PPK généré par le pare-feu :

1. **Add (Ajouter)** une PPK PQ.
2. Dans la boîte de dialogue **Add Post-Quantum Pre-shared Key (Ajouter une clé pré-partagée post-quantique)**, saisissez le nom de **PPK KeyID (ID de clé PPK)**. Dans cet exemple, le nom est **`PQ-Key-ID-2`**.
3. Configurez **PPK length (characters) (Longueur PPK (caractères))** sur une longueur d'au moins 64 caractères (32 octets, soit 256 bits d'entropie) pour créer une clé forte.
4. Cliquez sur **Generate Strong PPK (Générer une PPK fort)**.

   Le pare-feu génère un secret PPK hexadécimal aléatoire fort de la longueur configurée dans **PPK length (characters) (Longueur de la PPK (caractères))**.
5. Mettez la chaîne du secret PPK en surbrillance et copiez-la.

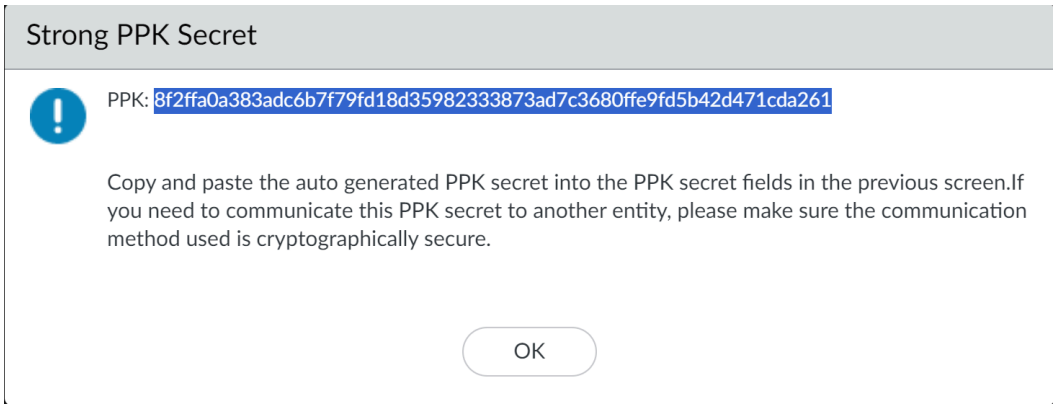
   Copiez uniquement le secret hexadécimal. Ne copiez pas la `PPK:` affichée au début. Par exemple, si le secret généré s'affiche sous la forme :

   `PPK:`
   `38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

   Vous ne copiez que :

   `38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

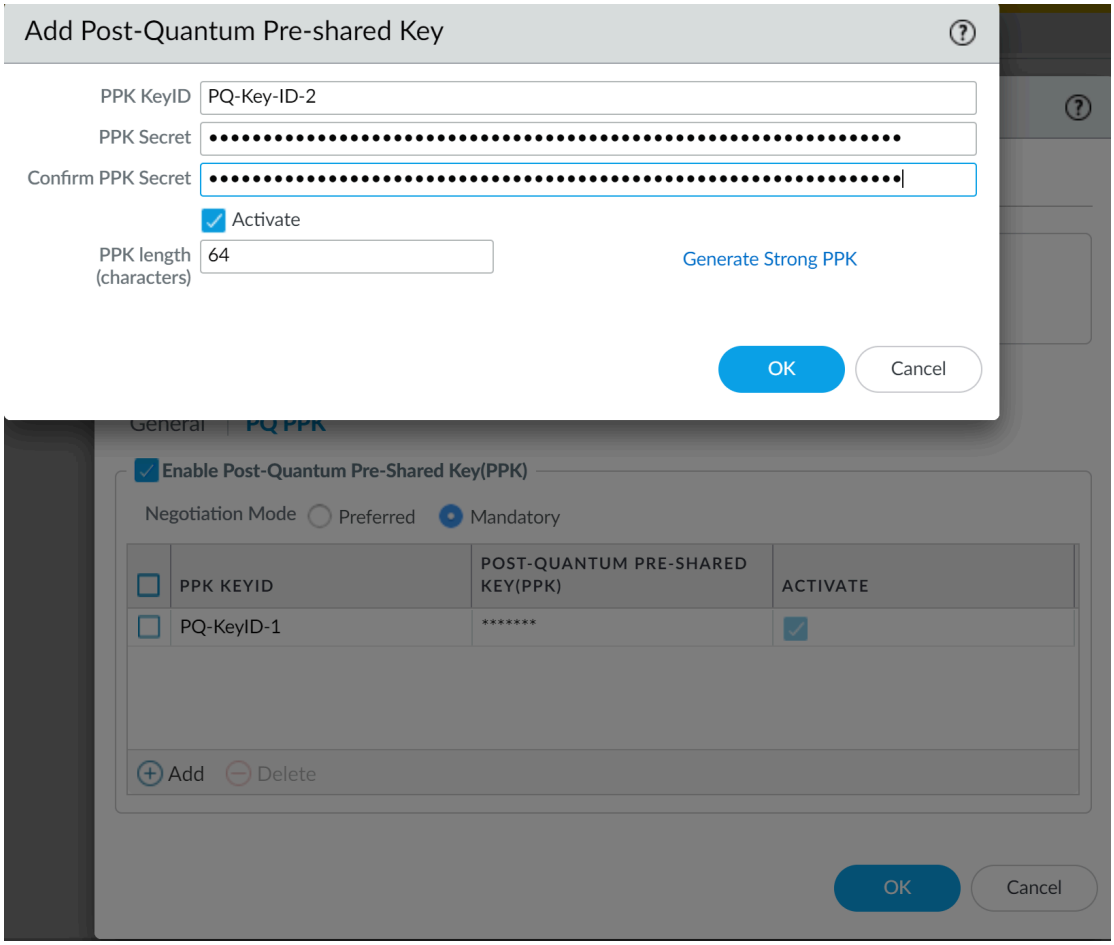
   La `PPK:` affichée au début ne fait pas partie de la chaîne du secret.



Stockez le secret PPK copié généré par le pare-feu en toute sécurité. Après avoir cliqué sur **OK**, le pare-feu n'affiche plus jamais le secret PPK en texte clair. Si vous ne copiez pas le secret PPK

et le stockez en toute sécurité dès maintenant, vous ne l'aurez pas et vous devrez supprimer cette PPK PQ et en configurer une nouvelle.

6. En ayant le secret PPK copié et présent dans votre presse-papiers ou disponible pour copie à partir d'un stockage sécurisé, cliquez sur **OK**. Si vous n'avez pas copié le secret PPK, générez un autre secret PPK fort et assurez-vous de le copier et de le stocker en toute sécurité.
7. Collez la chaîne du secret PPK copié dans les deux champs **PPK Secret (Secret PPK)** et **Confirm PPK Secret (Confirmer le secret PPK)** dans **Add Post-Quantum Pre-Shared Key (Ajouter une clé pré-partagée post-quantique)**.

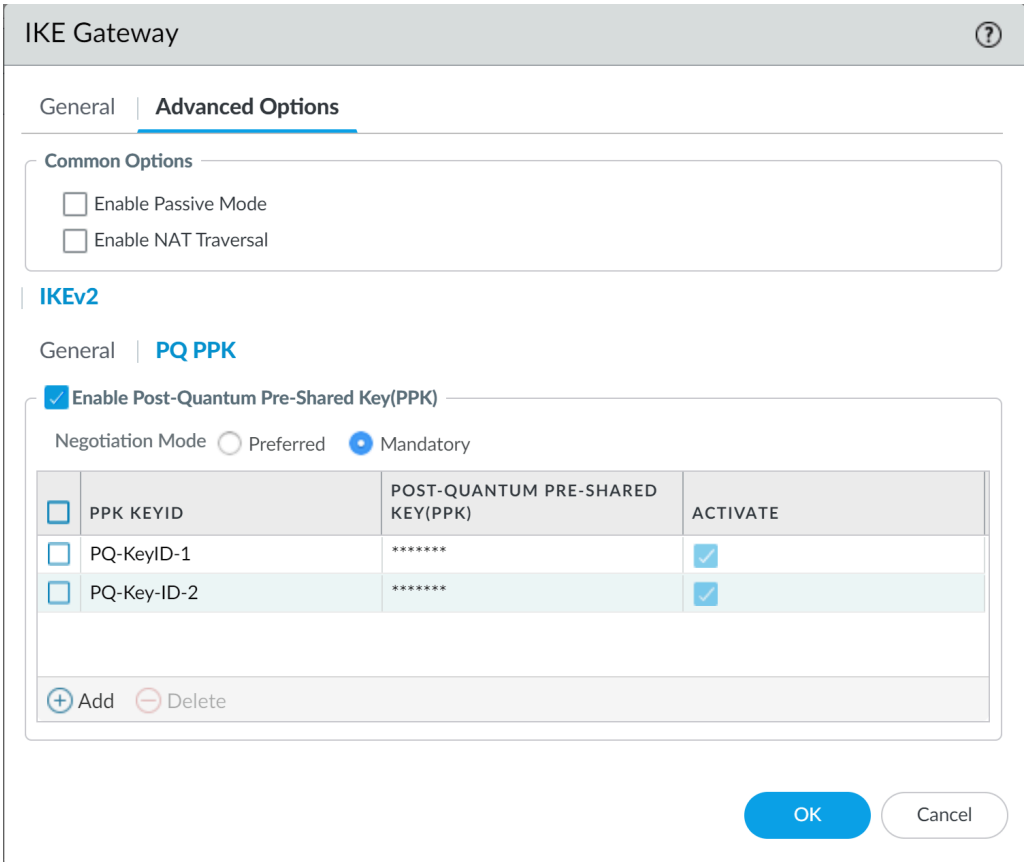


Par défaut, la nouvelle clé est active. Si vous ne souhaitez pas utiliser la clé dans la négociation entre les homologues IKE, désélectionnez **Activate (Activer)**. Si vous désactivez la PPK PQ sur un homologue, vous devez également la désactiver sur l'autre homologue.

8. Cliquez sur **OK** pour installer la PPK PQ générée par le pare-feu.
9. Si Panorama gère les deux homologues, vous pouvez créer la configuration sur Panorama et la transmettre vers les pare-feu gérés. Si Panorama ne gère pas les deux homologues et qu'un autre

administrateur contrôle l'homologue VPN, communiquez la PPK PQ de manière sécurisée à cet administrateur, qui l'installe sur l'homologue.

Pour le site A et le site C, les deux PPK PQ créées dans cet exemple sont répertoriées comme des PPK PQ actives en mode **Mandatory (Obligatoire)**.



Le secret PPK est désormais masqué et n'est jamais affiché en texte clair. Les VPN IKEv2 entre le site A et le site C mettent désormais en œuvre la RFC 8784 pour résister aux attaques quantiques. Les VPN IKEv2 entre le site A et le site B continuent d'utiliser des échanges de clés DH classiques et sont toujours vulnérables aux attaques Harvest Now, Decrypt Later.

Si le site B de cet exemple avait été mis à niveau pour prendre en charge la RFC 8784, vous devez suivre le même processus pour mettre à niveau les VPN IKEv2 du site A vers le site B et du site B vers le site A.

