paloalto
TECHDOCS

量子セキュリティ管理

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

量子セキュリティの概念

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

量子コンピューター(QC)は、ネットワークとデータのセキュリティを脅かしています。QC開発が成熟し、暗号に関連する量子コンピューター(CRQC)が生成され、復号化を解読するために設計された状態になると、安全と考えられていた多くの従来の暗号では、攻撃者がデータを復号化するのを防ぐことができなくなります。これは、従来の暗号化に基づく公開鍵基盤(PKI)がポスト量子攻撃に対して脆弱になることを意味します。この脅威は、特に長期間使用されるデータに差し迫っています。Harvest Now, Decrypt Later攻撃では、攻撃者は暗号化されたデータを取得し、データを復号化できるCRQCができるまで保存しておくからです。

量子コンピューティングに基づく攻撃に対する抵抗は、VPNを保護するためにIKEv2鍵交換中に作成された鍵を強化し、現在の暗号化とポスト量子暗号(PQC)を理解することから始まります。Palo Alto Networksの量子攻撃に対抗するソリューションは、オープン スタンダードに基づいており、その基準を満たす他の機器との相互運用性を確保しています。

最初のステップでは、このドキュメントで説明されているように、RFC 8784を実装して量子耐性IKEv2 VPNを作成します。量子耐性のあるVPNは、攻撃者が暗号化された重要な鍵材料を記録するのを防ぎ、暗号化されたデータを盗むことに成功した場合でもデータを復号化するのを防ぐことができます。RFC 8784は、今日の従来の暗号からの量子耐性への移行を、暗号のアップグレードを必要としない簡単な方法で提供し、VPN通信に量子耐性を導入する最も簡単な方法と考えられています。

2番目のステップでは、RFC 9370を単独で、またはRFC 8784と併用して実装し、従来のKEMテクノロジーとPQC KEMテクノロジーの両方を組み合わせることができる複数の鍵交換メカニズム(KEM)を使用して、量子耐性IKEv2 VPNを作成します。このソリューションは、IKEv2ポスト量子ハイブリッド キーとも呼ばれ、Shorのアルゴリズムを使用する量子攻撃に対して脆弱ではない新しい代替PQCアルゴリズムを使用します。

この章では、QC、QCがデータ セキュリティにもたらす脅威、量子耐性IKEv2 VPNを作成することで今すぐできること、およびポスト量子VPNとPQCへの移行を計画し、準備する方法について説明します。

- 量子コンピューティングの脅威
- RFC 8784が量子コンピューティングの脅威にどう抵抗するか
- RFC 9242とRFC 9370が量子コンピューティングの脅威にどのように対抗するか
- ポスト量子機能のサポート
- 量子コンピューティングの脅威

- ポスト量子攻撃に抵抗するためのベストプラクティス
- ポスト量子セキュリティの詳細

量子コンピューティングの脅威

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

公開鍵基盤(PKI)暗号化と IKE鍵交換メカニズムでは、Diffie-Hellman (DH)、楕円曲線暗号(ECC)、楕円曲線Diffie-Hellman (ECDH)などの従来の暗号が広く使用されています。量子コンピューター(QC)は、NISTが最初のポスト量子暗号(PQC)を標準化してから5〜15年以内にこれらのテクノロジーを破る可能性があります。

RFC 8784、RFC 9242、RFC 9370のオープンスタンダードに基づくポスト量子IKEv2 VPNは、量子コンピューティングやPQCに基づく攻撃に耐性があります。RFC 8784では、ピアリング ハンドシェイクで鍵材料をIKEピアに送信する代わりに、管理者は鍵材料をアウトオブバンドで個別に設定して共有します。攻撃者がデータを盗んだ場合、鍵材料がないため、データを復号化することはできません。RFC 9370では、IKEv2に7つのオプションのKEMラウンドが追加され、さまざまな種類のKEMテクノロジーで策定されたハイブリッド暗号化キーの作成が可能になりました。ハイブリッド キーを解読するには、キーの作成に使用されたすべてのKEMを侵害する必要があります。Palo Alto Networksの量子攻撃に対抗するソリューションは、オープン スタンダードに基づいており、その基準を満たす他の機器との相互運用性を確保しています。

最も差し迫った危険はHarvest Now, Decrypt Later攻撃です。この攻撃では、攻撃者が(保存中または転送中の)データを盗み、そのデータはすぐに解読することはできず、暗号に関連する量子コンピューター(CRQC)が解読できるようになるまで保存されます。CRQCは、量子アルゴリズムを使用して、従来のスーパーコンピューターでは数百万年かかるであろう暗号化の解読を数秒でできるように最適化されたQCです。最もリスクの高いデータは、CRQCが利用可能になったときにも依然として関連性がある長期間使用されるデータです。

- 量子コンピューターとは
- 量子の脅威はネットワークにどのような影響を与えますか?
- ハーベスティング攻撃を軽減するために今すべきこと

量子コンピューターとは

量子コンピューター(QC)は、本質的には次世代のスーパーコンピューティング プラットフォームです。QCは、量子力学の法則を使用して、データの処理とアルゴリズムの実行にかかる時間を大幅に短縮します。これには、従来の復号化を破る可能性のあるアルゴリズムも含まれます。従来のコンピューターでは処理に数百年または数千年かかる操作は、QCでは数秒あるいはマイクロ秒で処理できます。QCは、スーパーコンピューターの電力を線形に増加させる従来のビット(0と1)に基づくのではなく、偏光光子(光)に基づきQCの処理能力を指数関数的に増加させる量子ビットを使用してます。

量子ビットを作成する方法はいくつかあり、その方法は量子ビットの品質(量子ビットの効率)に影響します。量子ビットの品質が高いほど、QCはより速く、より効果的になります。量子ビットは、その量子的な性質により、一度に2つの状態を表し、それらの状態を長距離にわたって複製できます。これは、重ね合わせと量子もつれの量子効果によるものです。

- 重ね合わせ: 量子ビットは、1と0の両方を同時に表すことができます。量子ビットを組み合わせると、状態の数が2**nの割合で増加するため、量子ビットが表すことができる状態の数が増加します("n"は量子ビットの数)。したがって、2つの量子ビットは4つの状態(2**2)、3つの量子ビットは8つの状態(2**3)、4つの量子ビットは16の状態(2**4)を表すことができます。

  量子ビット密度(チップに収まる量子ビットの数)が増えると、結合された量子ビットが表すことができる状態の数が指数関数的に増加します。量子ビットの品質が優れているほど、結合された量子ビットの数は真の指数スケールに近づきます。低品質の(ノイズの多い)量子ビットを組み合わせても、状態の数は指数関数的に増加しませんが、それでも従来のコンピューターと比較して状態の数は大幅に増加します。量子ビットの品質が向上するにつれて、QCは、表現される状態の数の真の指数関数的なエスカレーションにますます近づいています。
- 量子もつれ: 量子もつれは、量子ビット間の量子結合です。もつれ量子ビットは、それがどこにあろうとも、たとえ互いに地球の裏側にある場合でも、同じ量子アルゴリズムを実行すると同じ結果が生成されます。そのため、バンガロール(インド)とロサンゼルス(米国)にあるもつれた量子ビットに対して特定のアルゴリズムを実行すると、それらの場所にあるもつれた量子ビットは同じ結果になります。量子もつれが機能する正確なメカニズムは不明です。

QCには3つのタイプがあります。

- 量子アニーラ: これらは今日利用可能です。これらは最も能力の低いQCで、使用例も最も限られています。しかし、攻撃者はそれらを使用して量子アルゴリズムで大量の数値を因数分解することができ、これが非対称暗号化を破る方法となります。
- アナログ量子シミュレーター: 量子化学、材料科学、最適化問題、大数因数分解、サンプリング、量子力学など、従来のコンプーターの能力を超えた物理問題を解きます。
- ユニバーサル量子コンピューター: これらは、多くの物理量子ビットを必要とするため、構築が最も難しいQCです。これらは幅広い用途に対応しており、複数の企業が10年後の実用化を目指しています。開発された場合、これらはCRQCになるコンピューターです。

QCは、複雑な問題を解決するために、多くのもつれた量子ビットで構成される多次元空間を作成します。たとえば、従来のコンピューターは、データベースの各要素を取得して処理し、すべての要素を処理した後で他の要素と組み合わせます。QCは、あなたが求めるあらゆる状態と結果を導き出すアルゴリズムを作成します。データベース全体を同時にアルゴリズムに通し、すべての結果のデータを同時に分析します。これにより、QCは従来のコンピューターよりも数百万倍高速になる可能性があり、暗号化の解読などの複雑な数学的問題を解決するのに優れている理由の1つです。

量子の脅威はネットワークにどのような影響を与えますか?

QCの処理能力と速度の大幅な向上は、データを暗号化するための従来の方法を破る恐れがあり、公開鍵基盤(PKI)を危険にさらす可能性があります。

最も差し迫った脅威は、暗号化されたデータを盗み、将来CRQCを使用して復号化することを目的としたHarvest Now, Decrypt Later攻撃です。攻撃者がデータや従来の鍵材料を盗むと、将来的にCRQCを使用してデータを復号化するのを阻止する方法はありません。盗まれたデータがその時点でまだ有効である場合、そのデータは侵害されます。

従来の非対称暗号化は素数に基づいており、それらの素数を導出するために複素数を因数分解することの難しさに依存しています。Shorのアルゴリズムという量子アルゴリズムは、複素数を因数分解し、離散対数の問題を解くことができます。Shorのアルゴリズムは、鍵を生成するために2つの非常に大きな素数に基づくPKIセキュリティを脅かします。ただし、Shorのアルゴリズムは、従来のコンピューターを使用して数百万年以内にPKIセキュリティを破ることはできません。CRQCがなければ、Shorのアルゴリズムは脅威ではありませんでした。しかし、CRQCの処理能力を考えると、Shorのアルゴリズムは複素数を因数分解し、従来の非対称暗号化(データの復号化に必要な鍵交換材料など)を数秒以下で解読することができます。これが、Harvest Now, Decrypt Later攻撃が差し迫った脅威である理由です。

従来の暗号化が破られると、Diffie-Hellman (DH)、楕円曲線暗号(ECC)、楕円曲線Diffie-Hellman (ECDH)など、安全であると考えられていた従来のPKI暗号のセキュリティが損なわれます。鍵交換は最もリスクが高いため、鍵交換を保護するためにポスト量子IKEv2 VPNを設定する必要があります。

証明書は、2つのエンドポイントが信頼を確立する方法の基盤となっています。ただし、CRQCは、デジタル証明書の作成と保護に使用されるRSAを危険にさらす可能性もあります。つまり、攻撃者はCRQCを使用してデジタル署名を盗んだり、なりすましたりできるため、接続していると思っていたサーバーが実際には攻撃者のサーバーである可能性があります。これができるようになるのは、早ければ今後10年以内になるかもしれません。

さらに、QCの純粋な力ずくの処理能力は、対称暗号化も安全ではないことを意味します。Groverのアルゴリズムは、特定の出力値を生成する一意の入力を見つける、量子の2次加速非構造化探索アルゴリズムです。Groverのアルゴリズムは、対称暗号化とハッシュ関数を対象としています。基本的にAESアルゴリズムの暗号化強度が半分になるため、AES-128ビット暗号化を使用すると、Groverのアルゴリズムはそれを64ビット暗号化の暗号化強度に落とします。従来のコンピューターには十分な処理能力がないため、Groverのアルゴリズムを使用して対称暗号化を解くことはできません。ただし、QCを使用すると、GroverのアルゴリズムはAES-128ビット暗号化を破ることができます。

*AES-128*ビット暗号化は*Grover*のアルゴリズムに対して脆弱であるため、*AES-256*ビット暗号化を使用してください。これは、*Grover*のアルゴリズムでは近い将来または中期的未来に破ることはできません。

ハッシュ関数を保護するために、少なくとも*SHA-384*を使用してください。

ポスト量子暗号(PQC)は現在利用可能であり、セキュリティに精通した人であれば、復号化できないPQCをダウンロードして設定できます。ネットワーク上で不正なPQCを許可すると、内部の

悪意のある人物がネットワークにPQCを持ち込む可能性があります。その場合、PQCを使用するトラフィックは可視化されず、そのトラフィックの脅威も可視化されません。復号化機能を使用して、ネットワーク上の不正なPQCを検出し、PQCを使用するトラフィックを自動的にブロックします。

ハーベスティング攻撃を軽減するために今すべきこと

ポスト量子の「Harvest Now, Decrypt Later」攻撃に抵抗するために、今すぐこれらの行動を取りましょう。VPN接続を見直し、強化します。

- VPN接続をタフな暗号スイートにアップグレードするには、RFC 6379 (*IPsec*のための*Suite B*暗号スイート)に従ってください。Suite-B-GCM-256を使用して、Groverのアルゴリズムに脆弱な128ビットのAESアルゴリズムを回避します。
- CAを4K RSAキー サイズにアップグレードすることで、より小さいキー サイズを破る総当たり攻撃を軽減し、VPN証明書の認証を新しい証明書に移行します。
- SHA-384やSHA-512などの上位ビットのSHAハッシュ サイズにアップグレードします。MD5やSHA-1などの弱いハッシュの使用を中止します。
- RFC 8784とRFC 9242およびRFC 9370を実装して、量子攻撃に抵抗するポスト量子VPNを構築します。

さらに、SSL/TLS接続を見直して強化します。

- SSL/TLS接続をタフな暗号スイートにアップグレードし、PFS (Perfect Forward Secrecy)暗号とともにTLSv1.3を使用します。
- 強化されたクライアント/サーバ間のVPNセッションでSSL/TLSセッションをトンネリングします。リバース プロキシをサポートするには、ポスト量子デスクトップ アプリケーションを使用します。

RFC 8784が量子コンピューティングの脅威にどう抵抗するか

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

RFC 8784標準である「ポスト量子セキュリティのための*Internet Key Exchange*プロトコル バージョン*2 (IKEv2)*での事前共有キーの混合」によって、今日、量子コンピューター(QC)およびポスト量子暗号(PQC)に基づく攻撃に耐性のあるIKEv2 VPNを作成することができます。

RFC 8784の本質は、IKE鍵交換とは別に帯域外で静的ポスト量子事前共有鍵(PQ PPK)を交換し、帯域外のPQ PPK材料をIKEv2鍵交換時に帯域内で伝送される従来のDiffie-Hellman (DH)鍵材料と混合することです。これにより、次の2つの方法で鍵交換が強化されます。

- DH鍵とその変形は、DHの基底となる非常に大きな素数に対する解法など、離散対数問題を解く難しさに依存しています。しかし、暗号に関連する量子コンピューター(CRQC)の登場により、DH鍵はShorのアルゴリズムに基づく攻撃に対して脆弱になります。RFC 8784を実装することで、混合鍵が離散対数問題(例えば、非常に大きな素数に対する解法)の解法の難しさだけに基づいていないため、鍵の暗号強度が強化され、混合鍵はShorのアルゴリズムに対して脆弱ではありません。
- 聞き手、つまり中間者は、後で復号化する鍵材料をすべて収集することはできません。鍵の従来のDH部分はIKEピアリング鍵交換で送信されますが、IKEピアがDH鍵材料と混合するPQ PPKは鍵交換中や確立後のVPNでは決して送信されないため、鍵材料のDH部分を使用しても、攻撃者はVPNを通過するデータを復号化できません。

IKEv2ピアは、Key IDに基づいて使用するPQ PPKを認識します。各PQ PPKは、KeyID と事前共有秘密の2つの要素で構成されます。事前共有秘密鍵は、IKEv2ピアと帯域外で共有する鍵材料です。DH鍵材料やVPN確立後のデータと一緒に帯域内で伝送されることはありません。代わりに、一方のIKEv2ピアの管理者が手動で静的な事前共有秘密を作成し、セキュアな電子メールやPanoramaからのプッシュなどにより、もう一方のIKEv2ピアの管理者に安全に伝達します。各管理者は、事前共有秘密をピアにプログラムするため、IKE接続で秘密が公開されることはありません。

鍵交換時に帯域内で送信される鍵IDは、IKEv2ピア上の事前共有秘密を識別します。IKEv2ピアは、鍵IDを使用して事前共有秘密を検索し、DH鍵材料と混合して、素数に基づかない新しい鍵材料を作成します。また、通信を盗聴しても盗み出すことはできません。

両方の*IKEv2*ピアは、まったく同じ鍵*ID*と事前共有秘密*PPK*のペアを使用する必要があります。鍵*ID*と関連する事前共有秘密が一致しない場合、接続は中断されます。複数の*PQ PPK*を設定する場合、両方の*IKEv2*ピアのアクティブな鍵*ID*と事前共有秘密のセットがまったく同じである必要があります。*(Palo Alto Networks*では最大*10*個のアクティブな*PQ PPK*を設定できますが、ベンダーによっては最低*1*個の*PQ PPK*しか設定できないため、ピアの機能を理解することが重要です。

この標準ベースの方法は、攻撃者が接続を盗聴し、VPN接続が確立された後にVPNで送信されるデータを攻撃者が解読できるようにする鍵を傍受するのを防ぐ簡単な方法を提供します。また、標準に準拠した他のデバイスとの相互運用性も確保できます。RFC 8784の利点は次のとおりです。

- マルチベンダー対応の標準規格として承認されています。
- 余分なネットワーク リソースを消費せず、遅延も実質発生しません。
- 下位互換性があるため、IKEv2をサポートしていないピアがある場合や、制御していないピアがあるネットワークで使用できます。
- 鍵はもはや素数に基づいておらず、Shorのアルゴリズムに対して脆弱ではありません。
- PQ PPKは送信されないので、収集されたデータの復号には使用できません。
- NIAP、NSA、ドイツ連邦情報セキュリティ局など、世界中の政府機関が推奨しています。さらに、長さが32バイト以上の強力なランダム秘密を作成すると、NISTカテゴリー5のセキュリティ レベルを満たします。秘密が強固でランダムであること、パターンに従っていないこと、辞書攻撃を受けないことを保証します。
- PQCハイブリッド キーなどの将来の標準ベースの機能を使用してRFC 8784をレイヤ化できます。

これにより、変更がほとんどなく、互換性がないために接続が切断される危険性がないため、導入が迅速化されます。ただし、RFC 8784にはいくつかの欠点があります。

- 静的なPQ PPKを手動で設定しても多くのサイトではうまくスケーリングできませんが、PQ PPKをPanoramaから管理対象ファイアウォールにプッシュすることでスケーリングを緩和できます。
- PQ PPKは、共有されているすべてのIKEv2管理者が安全に保管する必要があります。これには、社内の管理者だけでなく、パートナーやベンダーの管理者など、ピアリングが必要な社外の管理者も含まれます。リスクは、管理者がPQ PPKを書き留めて紛失したり、盗難や漏洩に遭ったりすることで生じます。
- 辞書攻撃やその他の攻撃に抵抗する、長くて強力なランダム秘密を作成するのを人間に頼るのは、難しいかもしれません。Palo Alto Networksの実装により、長い強力な16進数の秘密情報を自動生成できます。自分で作成する必要はありません。

RFC 8784ベースのIKEv2 VPNは、PQCとポスト量子脅威に対するソリューションの推奨される第一ステップです。NISTが最初のPQCを標準化した後、RFC 8784と連携できるRFC 9242やRFC 9370などの他の手法を使用すると、量子脅威に対する耐性を強化できます。

RFC 9242とRFC 9370が量子コンピューティングの脅威にどのように対抗するか

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.2以降

RFC 9242標準である「*Internet Key Exchange*プロトコル *2 (IKEv2)*の中間鍵交換」によって、IKEv2はIKEv2 Security Association (SA)の確立時に大量のデータを転送して、より大きなキー サイズを持つ複数のPQC鍵交換をサポートできます。RFC 9370標準である「*Internet Key Exchange*プロトコル *2 (IKEv2)*での複数の鍵交換」によって、SAのセットアップ中に共有シークレットを計算しながら、複数の鍵交換を行うことができます。

これら2つのRFC標準を組み合わせることで、IKEv2は、従来の鍵交換メカニズム(KEM)とPQC鍵交換メカニズム(KEM)の両方を使用してハイブリッド キーを作成し、Shorのアルゴリズムを使用して量子攻撃を緩和します。この新しいPQCは、既知の従来の攻撃や量子攻撃に対して脆弱ではないさまざまな数学的技術に基づいており、これらには次のものが含まれます。

- 格子
- コードベース
- ハッシュベース
- 対称キー
- アイソジェニーベース
- 多変数

RFC 9370標準では、さらに7つの鍵交換ラウンドが許可されており、これらはML-KEM、BIKE、HQC、Classic McElieseなどの従来のKEMまたはPQC KEMであり、IKEv2のデフォルト鍵交換に加えて、合計8つのラウンドとなります。

ハイブリッド キーを解読するには、暗号化キーの作成に使用されたすべてのKEMテクノロジーが脆弱性に陥り、侵害されなければなりません。たとえば、現在の既知の脆弱性と将来の量子コンピューター(QC)の脅威の両方に対して耐性を持つハイブリッド キーを作成するには、ベストプラクティスでは、従来のKEMと、異なる数学的技術を使用する1つ以上のPQC KEMの両方を使用することをお勧めします。

- デフォルトのKEMラウンド:Diffie-Hellman (DH)グループ21
- 追加の鍵交換ラウンド1:ML-KEM-768 (CRYSTALS-Kyber-786)
- 追加の鍵交換ラウンド2:BIKE-L3

前の例では、従来のDHグループ21が今日のプレ量子攻撃に対する保護を提供します。ML-KEM-768 (格子)とBIKE-L3(コードベース)の2つのPQC KEMラウンドを順々に追加すると、3つ

のKEMテクノロジーに基づく暗号化キーが作成され、Shorのアルゴリズムを使用した将来の攻撃に対する保護が提供されます。DH鍵交換に少なくとも2つのPQCを追加すると、1つのKEM障害に対する保護レベルが向上し、量子攻撃に長期間抵抗できます。さらに、さまざまな種類の数学に基づくKEMを使用すると、格子技術に基づくすべてのPQCなど、特定のタイプのPQCに対する将来の脆弱性から保護できます。

PQCが唯一の鍵交換メカニズムであるポスト量子世界への移行は、業界が新しいPQCを検証し、そのセキュリティ能力に確信を持つための時間を必要とするため、何年もかかるでしょう。移行期間中は、RFC9242とRFC 9370に基づくハイブリッド キーが標準になります。

新しいPQCを承認するための標準プロセスは段階的に行われ、NISTは承認ラウンドごとにPQCのグループを承認します。各PQCにはパフォーマンスとセキュリティのトレードオフがあるため、各PQCのパフォーマンスを理解するには、さまざまなセキュリティ ユース ケースに最適なテクノロジーを決定する必要があります。たとえば、Classic McElieceは時間の経過とともに非常に安全なPQCであることが証明されましたが、その高いセキュリティのトレードオフは、使用するキー サイズが大きいため、VPNおよびTLS通信でのClassic McElieceの使用が制限される可能性があることです。

世界の政府は、将来の量子コンピューター攻撃に対する強力なセキュリティと耐性を提供するために、*L3*以上のセキュリティ レベルを推奨しています。

従来の暗号化からポスト量子暗号化への移行期間中は、侵害されたPQCを迅速に置き換えることができるうように、暗号化の俊敏性が必要になります。Palo Alto NetworksのRFC 9242およびRFC 9370ポスト量子KEMソリューションは、暗号化の俊敏性を最初から実現するための広範なPQCを提供し、お客様はソフトウェアの更新や既存のネットワークの変更なしに、サポートされているPQCをIKEv2キー ネゴシエーションから迅速に選択して削除することができます。

PAN-OS IKEv2では、次のPQCがサポートされています。

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

RFC 9242とRFC 9370の利点は次のとおりです。

- マルチベンダーをサポートする承認された標準。
- RFC 8784の静的PPKの代わりに動的鍵交換による高いスケーラビリティ。
- 幅広いPQC KEMのサポート。
- IKEv2の下位互換性により、ピアがRFCをサポートできない場合のフォールバックが可能になります。

- ハイブリッド キーは、異なるPQCテクノロジーを一緒に使用できるため、Shorのアルゴリズムに対してより耐性があります。
- RFC 8784と階層化して、量子多層防御と暗号化の俊敏性を実現できます。

RFC 9242とRFC 9370の欠点は次のとおりです。

- 初期のPQC標準化リストでは、PQ移行の開始時に暗号化の俊敏性を実現するのに十分なPQCが提供されない場合があります。
- 新しいPQCは、業界から入念に審査され、信頼されるまでに何年もかかる場合があります。
- 複数のKEMを使用すると、オーバーヘッドが追加され、IKEv2ピアリング プロセスが遅くなる可能性があります。
- 新しいPQC KEMは、キー サイズとデータ ペイロードが大きくなるため、フラグメンテーションを引き起こす可能性があります。
- すべてのデバイスをアップグレードしてPQC KEMをサポートできるわけではありません。
- サービス拒否(DoS)攻撃のリスクは、イニシエータが認証される前に必要なリソースが増加するため、IKE_INTERMEDIATE中の拡張鍵交換によって増加する可能性があります。
- ハイブリッド キーは、暗号化された情報が保存され、後日暗号に関連する量子コンピューター(CRQC)で復号化されるハーベスティング攻撃から保護するように設計されています。アクティブな攻撃で量子コンピューターを使用した攻撃は、次の理由により、ハイブリッド キーでは完全には解決されません。
  - 認証は、事前共有鍵またはデジタル署名アルゴリズムのいずれかの従来の方法を使用して実行されます。事前共有鍵は、ポスト量子セキュリティを確保するために長くて複雑である必要がありますが、スケーラブルではありません。デジタル署名による認証は、ポスト量子デジタル署名を使用して実行する必要があります。
  - PQCは、ハーベスティング攻撃に対する耐性を提供するように設計されており、CRQCが利用可能になるまでは、接続の信頼性を攻撃しても意味がありません。なぜなら、攻撃は接続時にのみ発生するため、悪用の可能性がないためです。

RFC 9242およびRFC 9370ベースのIKEv2 VPNを使用して、複数のKEMテクノロジーに基づくハイブリッド キーを使用して、ポスト量子の脅威からVPN接続を保護することをお勧めします。PQCの広範なセットにより、暗号の俊敏性を実現し、ポスト量子世界への移行中に侵害されたPQCから保護することができます。

ポスト量子機能のサポート

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

ポスト量子機能のサポートには、RFC、HA、およびアップグレードとダウングレードの考慮事項が含まれます。国、ベンダー、企業がポスト量子攻撃からデータを保護する方法を模索しているため、ポスト量子の規格と機能の開発は初期段階にあります。規格が進歩し、Palo Alto Networksのプラットフォームがサポートするようになると、このトピックは更新され、そのサポートが示されます。

- サポートされるRFCと相互運用性
- HAのサポート
- アップグレードおよびダウングレードに関する考慮事項

サポートされる**RFC**と相互運用性

Palo Alto Networksのデバイスは、RFC 8784、RFC 9242、およびRFC 9370オープン スタンダードを完全にサポートしています。

Palo Alto Networksのデバイスは、同じ規格をサポートする他のデバイスと相互運用できます。ただし、RFCの解釈に基づいて、一部のベンダーの実装が異なる場合があります。たとえば、ベンダーによっては、RFC 8784で設定できるポスト量子事前共有鍵(PQ PPK)の数が制限されていたり、Palo Alto NetworksがRFC 9370でサポートしている広範なPQCのセットをサポートしていなかったりする場合があります。

HAのサポート

IKE VPNの高可用性(HA)は、ポスト量子機能が導入される前と同じです。VPNトンネルはフェイルオーバー後も実行され続け、IKEピアはフェイルオーバー後にIKEキーを再同期および更新します。

アップグレードおよびダウングレードに関する考慮事項

ポスト量子IKEv2 VPNをサポートしていないバージョンからアップグレードする場合、プラットフォームはポスト量子の機能をサポートします。

設定したポスト量子機能をサポートするバージョンにダウングレードする場合、設定は変更されず、ポスト量子IKEv2 VPNセキュリティは維持されます。

ポスト量子のIKEv2 VPN機能をサポートしていないバージョンにダウングレードすると、次のようになります。

- ポスト量子IKEv2 VPNを設定していない場合、ダウングレードは通常通り進行し、ポスト量子IKEv2 VPNのセキュリティ設定オプションは削除されます。
- ポスト量子IKEv2 VPNを設定した場合、ダウングレード バージョンはポスト量子設定オプションをサポートしていないため、ダウングレードはブロックされます。ダウングレードがブロックされると警告メッセージが表示され、ポスト量子IKEv2 VPN設定を削除し、ダウングレード後にVPNに使用する暗号を選択するように通知されます。

  ポスト量子IKEv2 VPN設定を削除し、暗号を選択したら、ダウングレードを続行できます。

ログ ファイルには、ダウングレード後のポスト量子のログが保持されます。

ポスト量子の移行計画と準備

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

ポスト量子攻撃に抵抗するようにネットワークをアップグレードするには、VPNのアップグレードに加えて、従来の暗号スイートからポスト量子暗号スイートへの移行が必要になるため、かなりの計画と準備が必要です。また、ネットワークやファイアウォールの変更だけでなく、エンドポイント、アプリケーション、クライアント アプリケーションなど、エンドツーエンドの完全な移行が必要です。時間、研究、リソースに多大な投資が必要です。投資の規模は、ビジネスとネットワークによって異なります。しかし、財務データ、コード、PIIデータ、その他の長期間使用される可能性のあるデータなど、Harvest Now, Decrypt Later攻撃に脆弱な最も貴重な資産を盗む攻撃のコストと比較すると、投資コストはわずかなものです。

さらに、世界中の規制機関、NSAなどの国家安全保障機関、政府、NISTなどの標準化機関は、政府機関や一部のビジネス部門(輸送機関や重要インフラを含む可能性がある)に対して、ポスト量子の脅威に対する準備と防御を義務付けているか、また今後義務付けることを予定しています。ポスト量子の世界への移行を準備することは、実行すべきかどうかの問題ではなく、いつ実行するかの問題なのです。

問題はいつ移行を開始すべきかということです。

移行を開始するタイミングは、デジタル資産の要件、特にプライバシーを保護する必要がある期間によって異なります。なぜなら、IKEとTLSピアリング ハンドシェイクで送信される鍵材料を含む暗号化されたデータを記録するHarvest Now, Decrypt Later攻撃は、暗号に関連する量子コンピューター(CRQC)が利用可能になったときに収集したデータを復号化することを目的としているためです。重要な問題は、データのセキュリティをどの程度確保する必要があるかということです。攻撃者が機密データをすでに取得しており、CRXCが機能した時点でそのデータがまだ有効だった場合、攻撃者は盗まれたデータを解読し、その内容に基づいて行動することができます。CRQCは早ければ今後10年で利用可能になる可能性があります。

企業がハーベスト攻撃の標的になり得る場合、対策を先延ばしにする日数だけ、攻撃者が後で解読する情報をより多く収集できるリスクが高まります。早期に対処すればするほど、攻撃者が収集したデータを将来的に解読することを早期に阻止できます。

歴史的には、3DESからAES暗号化への移行やSHA-1からSHA-2ハッシュ関数への移行など、暗号プロトコルを置き換えるための過去の取り組みのほとんどは、新しい標準の開発から5〜20年かかっています。これには、現実世界で新しいプロトコルを吟味する時間も含まれます。NISTがポスト量子暗号(PQC)を標準化した後、PQCが厳格なテストを経たとしても、新しいPQCが本当に堅牢であるという確信が得られるまでには、実世界での経験と、PQCの解読の試行に5〜10年の時間が必要でしょう。

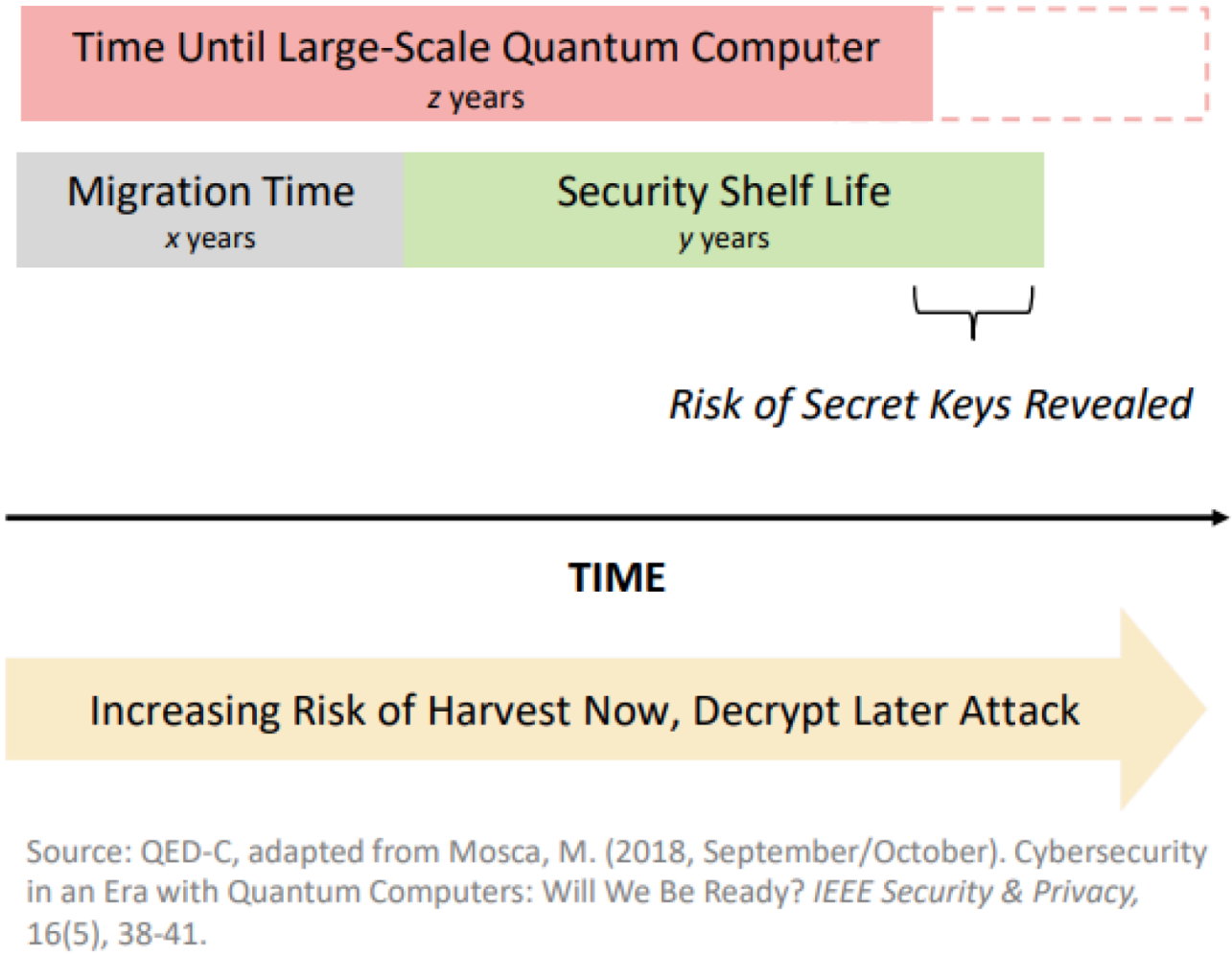
*PQC*は従来の暗号アルゴリズムを置き換えるもので、鍵交換、暗号化、デジタル署名に量子耐性を提供します。

従来の暗号化から新しいPQCへの移行を保護するために、業界ではハイブリッド キーの採用が進んでいます。ハイブリッド キーは、複数の鍵交換メカニズム(KEM)テクノロジーで暗号化キーを作成することで、セキュリティをさらに強化します。ベストプラクティスは、Diffie-Hellmanグループ21などの強力な従来のKEMと、1つまたは複数のPQCを使用することです。キーの作成に使用されたPQC KEMの1つが脆弱性に該当した場合でも、他のKEMが引き続きキーを保護します。新しいPQCが実世界での十分な経験を得て、業界がセキュリティ強度に確信を持つようになるまでは、ハイブリッド キーが前進するための最善の方法となります。

また、Harvest Now, Decrypt Later攻撃はポスト量子の脅威だけではありません。ネットワーク上の不正なPQCをプロアクティブにブロックしなければ、技術に精通した悪意のある人物がオープンソースのPQCをダウンロードし、ネットワーク内に独自のPQCサーバーやブラウザ プラグインを持ち出す可能性があります。

2030年代初頭までに、今日の従来の暗号技術で保護されているデータがポスト量子攻撃から保護されなくなると見られます。そのため、データのセキュリティ保護が必要な期間を理解し、ポスト量子の計画の準備と実行にかかる時間を見積もることが重要です。開始が早ければ早いほど、予測した品質とコストを保ちやすくなり、ポスト量子の脅威が増加しても、プロセスを急いで進めなくてよくなります。

いつ開始するべきか検討する1つの方法は、モスカモデルを使用することです。モスカモデルは、簡単なタイムラインを提示し、そこに時間の見積もりを挿入することで、行動を起こす緊急度を把握できます。



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.

このモスカモデルは、資産のポスト量子脆弱性へのタイムラインを推定する方法を示し、ポスト量子対応プロセスをいつ開始すべきか把握するのに役立ちます。このモデルでは、ポスト量子対応に移行するのにかかる時間の推定値(*x*、おそらく少なくとも5年)に、データの存続期間の推定値(*y*、ポスト量子対応を達成してから、データが暴露してもデータが侵害されなくなるまでの時間)を足したものと、CRCが利用可能になるであろう時間(*z*)を比較します。

(*x* + *y*)と*z*の差は、長期間使用されるデータが取得された場合にデータが漏洩するリスクがある時間、または長期間使用されるデータが危険にさらされるまでにどれだけの時間の余裕があるかを示します。これにより、開始までにどのくらいの時間があるか、またはどのくらい遅れる可能性があるかを把握できます。(*x* + *y*)が*z*より大きい場合、それらのタイムラインの違いは、前述の図で「秘密鍵が漏洩されるリスク」として示されている、攻撃者がデータを「Harvest Now, Decrypt Later」攻撃で収集した場合にデータが漏洩する可能性がある時間です。

移行計画を開始するにあたり、既存のVPN接続を強化するためにすぐに実行できることがいくつかあります。

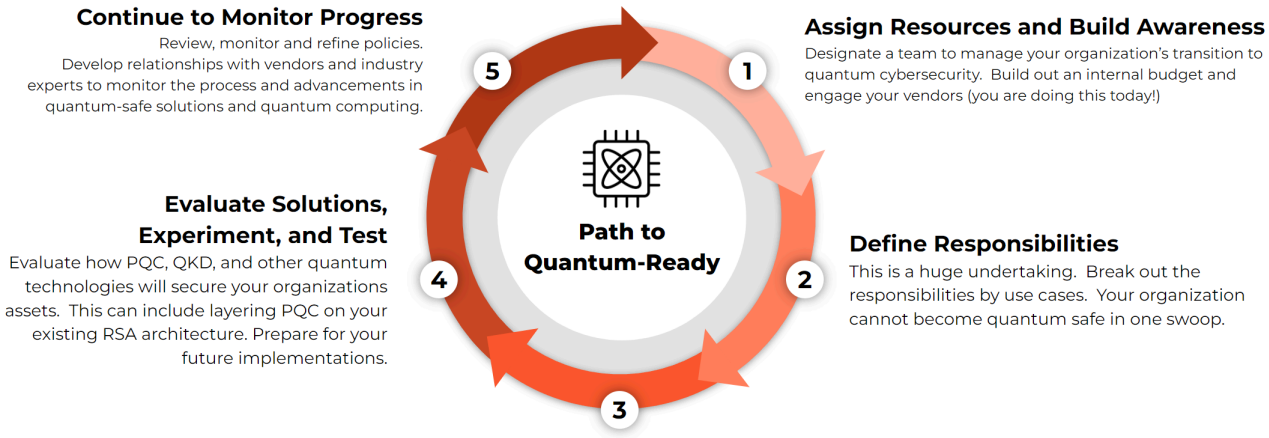
- VPN接続をタフな暗号スイートにアップグレードするには、RFC 6379 (*IPsec*のための*Suite B*暗号スイート)に従ってください。Suite-B-GCM-256を使用して、Groverのアルゴリズムに脆弱な128ビットのAESアルゴリズムを回避します。

- CAを4K RSAキー サイズにアップグレードすることで、より小さいキー サイズを破る総当たり攻撃を軽減し、VPN証明書の認証を新しい証明書に移行します。
- SHA-384やSHA-512などの上位ビットのSHAハッシュ サイズにアップグレードします。MD5やSHA-1などの弱いハッシュの使用を中止します。
- RFC 8784とRFC 9242およびRFC 9370を実装して、量子攻撃に抵抗するポスト量子VPNを構築します。

さらに、SSL/TLS接続を見直して強化します。

- SSL/TLS接続をタフな暗号スイートにアップグレードし、PFS (Perfect Forward Secrecy)暗号とともにTLSv1.3を使用します。
- 強化されたクライアント/サーバ間のVPNセッションでSSL/TLSセッションをトンネリングします。リバース プロキシをサポートするには、ポスト量子デスクトップ アプリケーションを使用します。

移行を開始するにあたり、量子経済開発コンソーシアム（QED-C）はポスト量子セキュリティへの移行を計画および準備するためのモデルを開発しました。Palo Alto Networksは、それを移行準備、時間、リソースを評価するのに役立つ5段階のモデルに適応させました。



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

次の項では、量子対応プロセスの各ステップについて説明します。RFC 8784を実装して量子耐性のあるIKEv2 VPNを構築することが最初のステップです。

- リソースの割り当てと認識の構築
- 責任の定義
- 暗号インベントリと優先度リストの作成
- ソリューションの評価、実験、テスト
- 継続した進捗状況の監視

リソースの割り当てと認識の構築

計画と準備の段階における目標は、移行チームを特定し、必要なリソースを把握し、ベンダーを関与させてポスト量子対応計画を把握し、それに伴うコストを把握することです。

ポスト量子の攻撃に対する耐性を構築するアップグレードは、多くの場合、*IT*部門がネットワークの近代化のためにすでに行っている作業と関係しています。

1. 移行を管理するためのポスト量子戦略と量子対応ロードマップの策定に責任を持つ、専門のプロジェクト管理チームを結成します。チームは、ハイレベルなプランニングを担当します。チームはまた、移行の一部であるネットワークの部分の責任者を特定します。早い段階で開始し、十分な時間をとって、熟慮された測定されたアプローチを行うことにより、品質を高く維持し、予測したコストを保つことができます。
2. 量子セキュリティ技術について理解し、環境に統合する方法を理解します。ポスト量子IKEv2 VPN (RFC 8784)は、セキュアなポスト量子ネットワークを構築するための最初のステップです。ネットワークに影響を与えることなく、今すぐ実行できます。さらに、すべての組織は既存の非対称アルゴリズムを耐量子PQCに置き換える必要があります。次のステップに進むには、PQC、ハイブリッド キー、および複数の鍵交換(RFC 9370および9242)について学習します。また、暗号の俊敏性(複数のPQCを使用して、PQCが漏洩した場合にPQCを簡単かつ迅速に切り替えられるようにする)、量子鍵配布(QKD)、量子乱数ジェネレーター(QRNG)についても学び、これらのセキュリティ対策がデータ保護に妥当であるかどうかを確認します。

   量子技術を研究し、ベンダーを巻き込んでベンダーの量子対応計画とそれが自身のビジネスにどのような影響を与えるかを把握します。
3. 企業のコミュニティに参加し、PQCとテクノロジーに対する認識と準備レベルについての理解を深めます。チームやチームリーダーの意識を高め、変化の可能性と変化が必要な理由を理解できるようにします。たとえば、調達チームと協力して、新しいハードウェアとソフトウェアがPQCと互換性があることを確認し、インフラストラクチャの将来性を保証するポスト量子の要件を含めます。

   暗号検出アクティビティを開始して(監査ドキュメントを活用できる可能性があります)、Diffie-Hellman (DH)、楕円曲線暗号(ECC)、楕円曲線Diffie-Hellman (ECDH)、AES-128、4K未満のRSA暗号化など、ポスト量子攻撃に脆弱なデジタル署名と暗号に依存している組織の現状を可視化し、識別します。
4. 社内予算の手配を開始します。詳細を把握しながら予算を調整し、自身のビジネスに最適なソリューションを策定します。

責任の定義

ネットワーク、ファイルおよびデータの暗号化、ソフトウェア アプリケーション、エンドポイント、IAM、アプリケーション サーバーなど、ネットワークの各部分の責任者を確認します。各エリアのチーム メンバーに責任を割り当て、移行の理由、緊急性、価値を理解していることを確認します。ポスト量子の脆弱性は、既存の非対称暗号化すべてに影響します。チーム・メンバーは、ネットワーク内のすべてのものを優先的に検出、分類、アップグレードするには多大な努力が必要であることを理解する必要があります。

暗号インベントリと優先度リストの作成

暗号インベントリとは、ネットワーク内のすべてのデバイス、システム、コード、アプリケーション、プラットフォーム、ベンダー、およびそれぞれが使用する暗号方式(サイバー スイート、TLS、SSH、VPNに使用されるバージョン、証明書管理、暗号化キー生成、キー サイズ、キー ストレージなど)に関する包括的なリストです。PQCはあらゆるタイプのエンドポイント、アプリケーション、サーバーを含むエンドツーエンドのデータパス全体に脅威を与えるため、暗号インベントリは包括的にする必要があります。つまり、完全なエンドツーエンドの移行を計画する必要があります。

暗号インベントリにはコンポーネントが単にリストされているだけではなく、各コンポーネントに関する情報、コンポーネント自体とそれぞれが使用する暗号に関する情報も提供されます。コンポーネントごとに、インベントリには、誰がそれを使用し、どのデータがその中に格納され、どのように保護され、データがコンポーネント間でどのように移動するかが含まれます。その目的は、ネットワークで使用されている暗号化の種類、暗号化によって保護されるデータ、データの格納場所、データの送信先、および関係するデバイスとユーザーに関するすべてを理解することです。要するに、ネットワーク暗号とその暗号が影響するすべてのものの包括的なインベントリです。

包括的な暗号インベントリがなければ、ネットワーク内の影響を受けるすべてのコンポーネントを特定したり、そのリスクを評価したり、最初にアップグレードするコンポーネントに効果的に優先順位を付けることはできません。

暗号インベントリを作成するには、暗号の使用状況を調査して文書化します(IT部門やSecOpsと協力して行うことが多い)。

- どのような暗号が使用されているか: 現在使用されている暗号暗号とプロトコル。
- 各暗号および暗号プロトコルを使用している人または物。
- 暗号が使用される場所: 暗号が保護するデータ、サーバー、ブラウザ、VPN、リモート アプリなど。誰がデータを使用しているか、データがネットワークのどの部分を通過するか、エンドツーエンドでどのように保護されているかを特定します。
- ネットワーク要素ごとにリスクで分類します。
- ハーベスティング攻撃によるデータ損失のリスクを把握するために、データに必要なデータ プライバシー期間と予測される使用期間を決定します。

暗号インベントリにベンダーとパートナーを含めます。たとえば、ベンダーに聞き取りを行って、アプリケーションで使用されている暗号方式や、鍵の強度と生成方法を把握します。誰がデータを使用しているか、エンドツーエンドでどのようにデータが保護されているかを特定します。攻撃者がポスト量子攻撃で活用できる隙間を残さないようにします。

暗号インベントリを作成する際、監査、ネットワーク強化、ゼロトラストなどのために行われた作業を活用できる可能性があります。

暗号インベントリの開発は、移行の最も困難な部分かもしれません。幸いなことに、インベントリを取得することで、量子の脅威が現実のものとなる前から、組織のセキュリティ強化に役立つ認識が芽生えます。インベントリによって、初期の古いシステムも特定されるからです。

Palo Alto Networksでは、暗号インベントリの取得に役立ついくつかのツールを提供しています。

- 復号化、トラフィック、および脅威ログには、ネットワーク上で実行される暗号プロトコル、それらのプロトコルのデバイスとユーザーなどが表示されます。
- コンテンツ リリース8692の脆弱性防御プロファイル シグネチャは、PQCの使用状況をログで検出して警告することができます。脆弱性防御プロファイルを設定して、ネットワーク上で非認可のPQCを自動的にブロックできます。これがベストプラクティスです。(社内PENテストに必要な例外を設けること。)
- SSL復号化機能を使って、ファイアウォールが復号化できない暗号を自動的にブロックします。

暗号インベントリ内のアイテムのリスクを評価し、移行の優先順位付けができるようにセキュリティ オプションを決定します。

- データとアプリケーションを理解する:
  - 優先度の高いデータとプライバシーの高いデータを特定します。
  - セキュリティとリスクに基づいてデータを分類します。
  - プライバシー期間(データの存続期間、有効期間)を割り当てます。
  - アプリケーションがどのようにデータを保護するかを理解します。
  - 誰がデータを使用しているかを把握します。
- エンドポイントを理解する。
  - データはどこに保存され、どのように保護されるか。
  - どのサーバーがデータをホストし、サービスを提供するか。
  - ユーザーがデータにアクセスするときにどのデバイスを使用するか。
  - エンドポイントのセキュリティはどのように確保されているか。
- ネットワークを理解する。
  - データはネットワーク上をどのように移動するか。
  - データを保護するのはどのデバイスか。
  - クラウドは関係しているか。クラウド上のデータはどのように保護されているか。
  - リスクの高いネットワーク領域はどこか。

- セキュリティ オプションと、ポスト量子の緩和を適用する必要がある箇所を理解する。
  - 新しいプロトコルに移行する必要があるか。
  - どのPQCをいつ使うべきか。(NIST PQC規格に注意。)
  - データを保護するためにハイブリッド キーを使用する必要があるか。
  - 暗号の俊敏性(PQCに脆弱性が発見された場合に暗号アルゴリズムを迅速に切り替える機能)をどう確保するか。
  - QRNGやQKDを使う必要があるか。
  - ポスト量子証明書と認証への移行が必要になるのはいつか。
  - 選択がコンプライアンス要件を満たしているか。

暗号インベントリを把握したら、データを分析し、それに基づいて移行の優先順位を設定します。優先順位を設定する場合は、ハーベスティング攻撃から防御するためのデータの有効期間、データの場所と機密性、およびデータの攻撃の受けやすさを考慮します。現在、鍵交換は最もリスクが高い状態にあるため、RFC 8784やRFC 9242およびRFC 9370を実装して量子耐性VPNを構築することが最優先事項です。

移行の優先順位を設定するには:

- ビジネスへの影響別にタスクをランク付けします。資産がビジネスにとってどの程度重要か。データのセキュリティ保護やプライベート保護が必要な期間はどのくらいか。資産がHarvest Now, Decrypt Later攻撃による危険にさらされているか。リスク資産の資本価値と、ポスト量子攻撃に対する将来のデータ損失の推定コストを比較します。
- 影響の大きい領域から移行します。
- 修復アクションを定義します。
- 移行スケジュールとポリシーを設定します。
- リソースと資金活動に取り組みます。

ソリューションの評価、実験、テスト

暗号インベントリの情報を使用して、ポリシー、移行計画、およびテスト計画を作成し、ネットワークをポスト量子対応に移行し、データを保護します。ベンダー、パートナー、およびネットワーク セキュリティに対するその他の外部の影響を含めます。ソリューション ポリシーと移行計画を作成するには:

- PQCにアップグレードする必要がある資産を特定します。

  各優先度レベルに必要なテクノロジーを特定し、移行戦略にどのように適合するかを判断します。
- 従来のアルゴリズムをPQCに置き換えたり、強化したりする際に、現在および将来の資産保護に最適なアルゴリズムを特定する移行計画を作成します。

- 非対称暗号化キーと対称暗号化キーのリスクを反映するために、鍵ライフサイクル ポリシーを策定します。特に、Harvest Now, Decrypt Later攻撃によるリスクにさらされている長期間使用されるデータに対して有効です。
- ポリシーと計画に暗号の俊敏性の実装を含めます。暗号の俊敏性により、アルゴリズム(従来またはPQC)が侵害された場合でも、迅速かつ簡単に安全なアルゴリズムに移行できます。

やみくもな総入れ替えではなく、十分に検討された移行であることを理解してください。PQCへの完全な移行を完了する前に、ハイブリッド アプローチを採用し、従来の暗号アルゴリズムでPQCを階層化してセキュリティを強化する必要があると考えられます。

計画とポリシーをテストするには、概念実証ラボを設定して、次のことを行います。

- すべてのPQCコンポーネントとデバイスとアプリケーション間の相互運用性を十分にテストします。
- 従来のアルゴリズムとPQCアルゴリズムのパフォーマンスと容量の違いを理解します。PQCは、従来の暗号よりもキー サイズとデジタル署名のサイズが大きいため、暗号化されたファイルのサイズが大きくなり、遅延にも影響する可能性があります。

  コンポーネント間のPQC相互運用性をテストし、組織内だけでなく、外部関係者間でもエンドツーエンドの量子耐性を最大限に高めるようにしてください。各ユースケースに最も適したアルゴリズムを特定し、従来の暗号をPQCに置き換えるための移行計画を作成します。
- エンドツーエンドでテストし、ポスト量子への対応がネットワークに影響を与える可能性のあるパートナー、ベンダー、およびその他の外部関係者を含めます。システムによっては、ポスト量子のパフォーマンスを許容するにはアップグレードが必要な場合があります。
- 互換性のないコンポーネントとアップグレードが必要な資産を特定します。

実験は、組織内で意識を高めると同時に、質問に答えたり、移行がいかに簡単か、または困難かについての情報を提供する手段でもあります。社内に専門家がいない場合や、適切な期間内に社内で専門家を育成できない場合は、外部の専門家に意見を求めます。

継続した進捗状況の監視

量子耐性環境に向けた進捗状況を継続的に監視および評価し、移行が予定通りに進行していることを確認し、ハーベスト攻撃のリスクが軽減されるようにします。必要に応じて、計画と関係する人員を調整します。さらに、専門家と協力して、あらゆる可能性を考慮し、攻撃者が将来の量子攻撃で悪用できる隙間を残さないようにします。

ポスト量子攻撃に抵抗するためのベストプラクティス

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

量子コンピューターによって実行されるポスト量子攻撃に対する防御には、Harvest Now, Decrypt Later攻撃に対する防御など、今すぐ実装できる多くのベストプラクティスがあります。Harvest Now, Decrypt Later攻撃は、暗号化キーのベースとなる大きな素数を見つけるための鍵材料を要因とするShorのアルゴリズムを高速化することで、暗号に関連する量子コンピューター(CRQC)を使用して後で材料を解読することを意図して、暗号化されたデータと鍵交換材料をキャプチャします。

次のベストプラクティスについて説明します。

- ポスト量子移行計画のベストプラクティス
- 暗号化のベストプラクティス
- VPN設定のベストプラクティス

ポスト量子移行計画のベストプラクティス

従来の暗号からポスト量子暗号への移行には、5年あるいはそれ以上かかることがあります。計画だけで数年かかることもあります。次の方法で、最大のメリットを得ましょう。

- 早期開始: 企業が長期間使用されるデータを保持しており、ハーベスティング攻撃の標的となりうる場合、対策を先延ばしにする日数だけ、攻撃者が後で解読する情報をより多く収集できるリスクが高まります。早期に対処すればするほど、攻撃者が将来的に解読するデータを収集するのを早期に阻止できます。
- 既存のリソースの活用: 暗号インベントリを取得する際には、監査、ゼロトラスト、ネットワークの強化、その他の活動のためにすでに行った作業を活用します。
- 自己啓発: 量子コンピューティングの脅威、ポスト量子暗号(PQC)、量子攻撃からネットワークを強化するテクノロジーと方法、およびネットワークを保護するために使用できる新しいPQCについて学びます。政府の命令、計画、法律、RFC、その他の情報ソースから学びます。

暗号化のベストプラクティス

CRQCに進化するにつれて量子コンピューターが高速かつ高速になるため、従来の暗号スイートの強度を高めて、攻撃者による総当たり解読キーをより困難にします。CRQCではない量子コンピューターでも、より弱い暗号を解読するには十分な速度である可能性があります。

- VPN接続をタフな暗号スイートにアップグレードするには、RFC 6379 (*IPsec*の*Suite B*暗号スイート)に従ってください。Suite-B-GCM-256を使用し、Groverのアルゴリズムに脆弱な128ビットAESアルゴリズムのような弱いものは避けるべきです。
- CAを4K RSAキー サイズにアップグレードして、より小さいキー サイズを突破する総当たり攻撃を軽減します。
- VPN証明書認証を、より大きなキー サイズの新しい証明書に移行します。
- SHA-384やSHA-512などの上位ビットのSHAハッシュ サイズにアップグレードします。MD5やSHA-1などの弱いハッシュの使用を中止します。
- SSL/TLS接続をタフな暗号スイートにアップグレードし、PFS (Perfect Forward Secrecy)暗号とともにTLSv1.3を使用します。
- 強化されたクライアント/サーバ間のVPNセッションでSSL/TLSセッションをトンネリングします。
- 復号化しないトラフィックに対して非認可のPQCをブロックするように脆弱性防御プロファイルを設定します。復号化するトラフィックの場合、復号プロファイルを使用して、認可されていないPQCをブロックします(復号プロファイルは、有効にした暗号だけを許可し、ファイアウォールは他のすべての暗号をブロックします)。認可されていないPQCは、侵害または内部の悪意のある人物がPQCを使用してネットワークを危険にさらそうとしたことを示している可能性があります。必要に応じて、社内のPENテスト チームのために例外を設けます。

VPN設定のベストプラクティス

ポスト量子IKEv2 VPNを設定する場合は、量子攻撃に対してできるだけ耐性を持たせるようにします。

- RFC 8784を実装して、量子攻撃に耐性のあるIKEv2 VPNを構築します。
- RFC 9242およびRFC 9370を実装して、量子攻撃に耐性のあるIKEv2 VPNを構築します。

> *RFC 8784*を*RFC 9242*および*RFC 9370*と併用することで、保護レイヤを追加でき、暗号の俊敏性要件を満たすことができます。

RFC 8784のベストプラクティス**:**

- IKEv1は使用しないでください。IKEv1は脆弱なプロトコルと考えられており、ポスト量子VPNをサポートしていません。両方のIKEピアがサポートできる場合は、VPN接続をIKEv2にアップグレードし、IKEゲートウェイを設定する際に**IKEv2**専用モードを選択してください(**[Network (**ネットワーク**)]** > **[Network Profiles (**ネットワーク プロファイル**)]** > **[IKE Gateways (IKE**ゲートウェイ**)]** > **[General (**全般**)]**)。
- 両方のピアがRFC 8784をサポートしていることがわかっている場合は、**[Negotiation Mode (**ネゴシエーション モード**)]**を**[Mandatory (**必須**)]**に設定します。**[Mandatory (**必須**)]**モードを使用すると、VPNがポスト量子攻撃に抵抗し、攻撃者がデータをすぐに収集することができ

ず、Shorのアルゴリズムを実行しているCRQCを使用して後で復号化することができなくなります。

*Shor*のアルゴリズムは、十分な処理能力があれば、非対称暗号化を使用する*IKEv2*ハンドシェイクの動的鍵交換を解読できます。しかし、*Shor*のアルゴリズムでは*IPSec*トンネル対称暗号化を解読できません。対称*IPSec*暗号化を保護するには、*AES-256*を使用して*Grover*のアルゴリズムから保護し、前のセクションの暗号化のベストプラクティスで推奨されているより強力なハッシュとキー長を使用します。

外部デバイスとのピアリングを行う場合は、ピアがRFC 8784をサポートしているかどうかを確認し、他の管理者と協力して同じPQ PPKを接続に使用して、[Mandatory (必須)]モードを使用できるようにします。

- 64文字以上(32バイト、つまり256ビットのエントロピー)のPPKシークレットを手動で指定または自動生成して、強力なキーを作成します。最大128文字(64バイト、512ビットのエントロピー)の**PPK**シークレットを手動で指定したり、自動生成したりできます。PPKシークレットが長いほどエントロピー ビット数が多くなり、PPKシークレットが解読されにくくなります。

  エントロピー ビット数は、ポスト量子セキュリティの半分のビット数を提供します。例えば、256ビットのエントロピーは128ビットのポスト量子セキュリティを提供し、512ビットのエントロピーは256ビットのポスト量子セキュリティを提供します。最小256ビットのエントロピーは、NIST Post-Quantum Cryptography Call for Proposalsで定義されているカテゴリ5相当のセキュリティを提供します。RFC 8784の「セキュリティ上の考慮事項」の項に、エントロピーの詳細と、エントロピーの十分な量について示されています。

  *PPK*シークレットは、設定または自動生成したときにだけ平文で表示されます。*PPK*シークレットを設定または生成し、シークレットが平文で表示される画面から移動した後は、鍵の漏洩を防ぐため、*2*度とシークレッが平文で表示されることはありません。

  *PPK*シークレットと*KeyID*のペアをコピーし、安全に保管してください。キーを設定または生成するときにキーを保管しないと、後でキーを取得できません。*(PQ PPK*を削除して、必要に応じて別の*PPK*を設定できます*)*。

  PQ PPKを処理するためのその他のベストプラクティスには、次のものがあります。

  - アクティブなPQ PPKを複数作成します。1つだけではなく複数のアクティブなキーを使用すると、鍵交換時の鍵選択にランダム性の要素が加わります。
  - 各IKEv2ピアが、鍵交換をネゴシエートするために、アクティブ化されたPQ PPK (KeyIDとPPKシークレットのペア)のまったく同じセットを持っていることを確認します。

- Panoramaがピアを管理する場合は、PQ PPKを設定し、管理対象ファイアウォールにプッシュすることで、より簡単かつ迅速かつ自動的に構成できます。
- PQ PPKを他の管理者に伝える必要がある場合は、暗号化メールなど暗号で保護された通信方法を使用してください。
- PPKシークレット文字列を安全に保存します。付箋紙や、権限のない管理者が発見するような場所に保管しないでください。

*NSA*は、*RFC 8784*量子事前共有鍵を含む事前共有鍵を安全に扱うためのガイダンスを公開しています。

RFC 9242および**RFC 9370**のベストプラクティス**:**

- IKEv1は使用しないでください。IKEv1は脆弱なプロトコルと考えられており、ポスト量子VPNをサポートしていません。両方のIKEピアがサポートできる場合は、VPN接続をIKEv2にアップグレードし、IKEゲートウェイを設定する際に**IKEv2**専用モードを選択してください(**[Network (**ネットワーク**)]** > **[Network Profiles (**ネットワーク プロファイル**)]** > **[IKE Gateways (IKE**ゲートウェイ**)]** > **[General (**全般**)]**)。
- IKE暗号プロファイルを設定する場合、Diffie-Hellman Group 20以上のような強力な従来のKEMと、Kyber-768 (ML-KEM)のような追加のKEMラウンドで少なくとも1つのPQCを使用してハイブリッド キーを作成します(**[Network (**ネットワーク**)]** > **[Network Profiles (**ネットワーク プロファイル**)]** > **[IKE Crypto (IKE**暗号**)]** > **[General and Advanced Options (**一般オプションと詳細オプション**)]**)。
- 機密情報については、セキュリティ強度レベルがL3以上と評価されたPQCのみを使用します。鍵作成プロセスにPQCが追加されるたびに、鍵の量子攻撃に対する耐性は高まりますが、IKEv2ピアリング プロセスに遅延とオーバーヘッドが追加されます。一般に、セキュリティ レベルL3 PQCを追加すると、IKEv2鍵交換に約20～30ミリ秒、セキュリティ レベルL5 PQCを追加すると40～60ミリ秒が追加されます。Classic McElieseなど、より大きな鍵を使用する強力なPQCでは、鍵交換に800ミリ秒以上が追加され、高レベルのフラグメンテーションが発生する可能性があります。PQCキーのサイズとセキュリティの強度を十分に理解して、VPN通信に最適なPQCを選択します。
- 各キー ネゴシエーション ラウンドで使用されるPQCを、ピアVPNデバイスを管理する管理者と調整します。トンネルの両側にある両方のVPNデバイスに、オプションのキー ネゴシエーション ラウンドごとに同じPQCが設定されている場合、相互運用性の問題は最小限に抑えられます。PQCとそのセキュリティ強度について合意し、両側が同じパラメータで設定されていることを確認するようにしてください。同じ組織で管理されているファイアウォールの場合、中央管理ツールを使用して、各キー ネゴシエーション ラウンドで一貫した設定とPQCの選択を行うことができます。
- 暗号の俊敏性を有効にし、ピュアなPQC環境への移行時にデータを保護します。業界が新しいPQCを完全に信頼するまでには、移行には5年から10年もかかる可能性があります。
  - NISTによって標準化され、FIPSによって承認されたPQCを使用しなければならない組織の場合、RFC 9242とRFC 9370とともにRFC 8784を有効にすることで、暗号の俊敏性を実現で

きます。ハイブリッド キーで使用されるPQCが脆弱性に陥った場合でも、RFC 8784で使用されるPPK文字列は引き続き量子耐性を提供し、ハーベスト攻撃の成功を防ぐことができます。

  - NIST標準化PQCと非標準化PQCの両方を使用することを許可されている組織では、Diffie-Hellman Group 21のように、強力な従来のKEMを備えた少なくとも2つのPQCを使用することで、暗号の俊敏性を達成できます。PQC KEMは、理想的には、1つのKEMが格子に基づいており、もう1つのKEMがコードベースまたはその他の非格子技術に基づいている、異なる数学的技術を使用している必要があります。オプションとして、RFC 8784をハイブリッド キーで有効にして、セキュリティ層を追加し、暗号の俊敏性を拡張することもできます。

- キーの再生成を高速化するために、キーのライフタイム値をデフォルト値から小さい値に減らします。
- IPSec暗号プロファイルを設定する際は、ハイブリッド キーを使用するようにIPSecを有効にします(**[Network (**ネットワーク**)]** > **[Network Profiles (**ネットワーク プロファイル**)]** > **[IPSec Crypto (IPSec**暗号**)]** > **[General and Advanced Options (**一般オプションと詳細オプション**)]**)。IPSecトンネルの両側は、追加の鍵交換ラウンドごとに同じPQCとセキュリティ強度を使用するように設定する必要があります。

ポスト量子セキュリティの詳細

ポスト量子セキュリティ、ポスト量子技術、および推奨されるポスト量子実装は、初期段階にあります。ポスト量子コンピューティングの世界で資産を保護する計画を立てる際には、ポスト量子技術、ビジネスに影響を与える政府の規制と義務、およびポスト量子VPNと暗号への移行方法についてできるだけ多くのことを理解することが重要です。

米国政府と世界中の政府は、量子コンピューターとポスト量子暗号によってもたらされる量子セキュリティの脅威に対処するための計画を作成しています。さらに、米国国立標準技術研究所(NIST)やインターネット技術特別調査委員会(IETF)などの標準化団体は、新しいポスト量子技術とその実装方法に関する標準を作成しています。

このトピックでは、ビジネスにおけるポスト量子セキュリティへの理解、準備、移行を促進するのに役立つ情報へのリンクを提供します。

- 米国政府
- 他の世界の政府
- RFC
- テクノロジーと一般情報

米国政府

多くの国の政府は、量子コンピューティングの脅威とポスト量子暗号の出現に対処するための計画、義務、および法律を策定しています。次のリンクは、米国国立標準技術研究所(NIST)および国家安全保障局(NSA)からの情報へのリンクを含む、米国政府による問題への対処方法に関する情報を提供します。地方自治体のセキュリティ サイトや組織をチェックして、政府がポスト量子セキュリティにどのように取り組んでいるかを確認してください。

- NISTのポスト量子暗号リソース センターでは、ポスト量子暗号の標準化などに関する情報を提供しています。
- NISTのNational Cybersecurity Center of Excellence (NCCOE)による「ポスト量子暗号への移行」では、ポスト量子暗号への移行に関するガイダンスを提供しています。
- 対称鍵管理要件付録*V2.1* (NSAの中央セキュリティ サービス発行)では、Commercial Solutions for Classified (CSfC)の事前共有鍵の使用に関する実装要件を提供しています。
- 国土安全保障省のポスト量子暗号に関するウェブサイトには、省のポスト量子ロードマップとその他のリソースが含まれています。
- ポスト量子暗号イニシアティブ(サイバーセキュリティー社会基盤安全保障庁(CISA)発行)では、量子コンピューティングの脅威に対処するために、他の政府機関や業界パートナーとのポスト量子の取り組みを統合しています。このサイトでは、CISA、NIST、および国土安全保障省のその他のリソースへのリンクも提供しています。
- 連邦政府の情報技術システムの量子耐性暗号への移行を促進するために、バイデン大統領は量子コンピューティング サイバーセキュリティ法(HR 7535)に署名しました。

- 大統領府から発出された大統領令M-23-02「ポスト量子暗号への移行」では、米国の機関が国家安全保障覚書第10号(NSM-10)「量子コンピューティングにおける米国のリーダーシップを促進しつつ、脆弱な暗号システムへのリスクを軽減するための国家安全保障覚書」を遵守するための指針を示しています。

他の世界の政府

次のリンクは、世界中のいくつかの政府がこの問題にどのように取り組んでいるかについての情報を提供します。

- ドイツ連邦情報セキュリティ局(BSI)は、ポスト量子暗号、移行戦略、現在の開発と推奨事項、およびその他の資料に関する情報を提供しています。
- イギリス政府は、量子コンピューターと技術、量子コンピューターの脅威、国家量子戦略、量子鍵配布、量子乱数生成、およびその他の資料に関する情報を提供しています。
- フランス サイバーセキュリティ庁(ANSSI)は、ポスト量子遷移、量子鍵配布、およびその他の材料に関する情報を提供しています。
- オランダ総合情報安全保障局(AIVD)は、量子コンピューターの脅威、ポスト量子移行の戦略と手順、量子鍵配布、およびその他の資料に関する情報を提供しています。
- 欧州ネットワーク・情報セキュリティ機関(ENISA)は、ポスト量子暗号、ハイブリッド実装、ポスト量子戦略、およびその他の資料に関する情報を提供しています。
- シンガポール金融管理局は、量子プログラムと、量子に関連するサイバーセキュリティ リスクへの対処に関する情報を提供しています。
- 日本政府は、量子戦略、量子セキュリティ、および量子テクノロジーへの移行に関する情報を提供しています。

RFC

提案依頼書(RFC)は、インターネットの技術的基盤を説明しています。いくつかのRFCでは、量子コンピューターからの攻撃に対するIKEv2の耐性の側面が説明されています。

- RFC 8784「ポスト量子セキュリティのための*Internet Key Exchange*プロトコル バージョン*2 (IKEv2)*での事前共有キーの混合」では、IKEv2が量子コンピューターからの攻撃に耐性を持つようにするIKE拡張機能の標準について説明しています。RFC 8784が量子コンピューティングの脅威にどう抵抗するかでは、ネットワークにおけるRFC 8784の影響をまとめています。
- RFC 6379「*IPsec*のための*Suite B*暗号スイート」では、脆弱なAES-128ビット暗号化の代わりに使用するべきSuite-B-GCM-256ビット アルゴリズムについて説明しています。AES-128などの脆弱な暗号を排除することは、Groverのアルゴリズムが対称暗号を破ることができるようになる時期を遅らせるのに役立ちます。
- RFC 9370「*Internet Key Exchange*プロトコル バージョン*2 (IKEv2)*における複数の鍵交換」では、IKEv2を拡張して複数の鍵交換を混在させて暗号化キーを作成する方法について説明しています。

- RFC 9242「*Internet Key Exchange*プロトコル バージョン*2 (IKEv2)*における中間交換」では、初期鍵交換で大量のデータ(複数の鍵交換に基づく暗号化キーなど)の転送を可能にする中間交換メカニズムを定義しています。これにより、フラグメンテーションを回避できます。(一部のデバイスではフラグメンテーションが許可されていません。
- RFC 7383「*Internet Key Exchange*プロトコル バージョン*2 (IKEv2)*メッセージのフラグメンテーション」を使用すると、IKEメッセージをIKEレベルでフラグメント化できるため、IPフラグメンテーションによる問題が解消されます。ただし、RFC 7383は最初の交換では機能しません。RFC 9242は初期交換でのフラグメンテーションを回避するのに役立ち、RFC 7383は後続のIKEv2メッセージでのIPフラグメンテーションを回避します。

テクノロジーと一般情報

多くの組織は、量子コンピューターや、従来のコンピューターで実行すれば危険ではないが、暗号に関連する量子コンピューター(CRQC)で実行すると壊滅的な危険をもたらす可能性のあるテクノロジーによってもたらされる潜在的な脅威を認識しています。

- Open Quantum Safe組織のliboqsサイトは、耐量子暗号アルゴリズムのためのオープンソースのCライブラリです。
- The Linux Foundationのポスト量子暗号アライアンス プロジェクトは、標準化されたアルゴリズムの高保証ソフトウェア実装を作成することにより、量子コンピューティングによってもたらされる暗号化セキュリティの課題に対処しようとしています。
- ShorのアルゴリズムをCRQCと一緒に使用した場合、今日使用されている多くの従来の非対称暗号化アルゴリズムが破られる恐れがあります。Shorのアルゴリズムは、大きな複素数を因数分解して、従来の非対称暗号化の基礎となる素数を導き出します。
- Groverのアルゴリズムは、量子の二次的に高速化された非構造化探索アルゴリズムです。CRQCで使用すると、AESアルゴリズムとハッシュ関数の暗号化強度を半分に減らすことで、総当たり攻撃によって従来の対称暗号化アルゴリズムを破ることができます。
- Harvest Now, Decrypt Later攻撃は現在アクティブな脅威です。Harvest Now, Decrypt Later攻撃では、攻撃者は今すぐは解読できないデータを盗み、CRQCが復号化できるようになるまで保存します。これらの攻撃は今日も発生しており、長期間使用されるデータに差し迫った脅威となっています。
- Quantum Inspireのナレッジ ベース記事「量子ビットとは?」では、量子ビットについて説明しています。
- Deloitteの記事「暗号に対する量子の脅威」では、できるだけ早くポスト量子移行を開始すべき理由について説明しており、Forbesの記事「暗号に対する量子の脅威: 慌てずに、今すぐ備えましょう」にも同様の説明があります。
- *ETSI*の「耐量子暗号*(QSC: Quantum-Safe Cryptography)*:耐量子移行のための反復可能なフレームワーク」では、ポスト量子移行計画を作成するための優れたテンプレートを提供しています。
- 世界経済フォーラムの「量子経済ブループリント」では、量子経済への移行を可能にするために、公平な方法で量子エコシステムを構築するためのロードマップを提供しています。

耐量子IKEv2 VPNの設定

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

RFC 8784および/またはRFC 9242およびRFC 9370に基づく量子耐性IKEv2 VPNは、Harvest Now, Decrypt Later攻撃を実行しようとする攻撃者が、VPN内のデータを暗号化するために使用される暗号化鍵材料を盗むことを防ぎます。暗号化キーがなければ、攻撃者は後で暗号に関連する量子コンピューターを使用して収集したデータを復号化することはできません。たとえ攻撃者が暗号化されたデータを盗むことに成功したとしても、暗号に関連する量子コンピューターがなければ鍵材料を復号化できず、鍵がなければデータを復号化できないため、収集したデータを侵害することはできません。

RFC 8784は、今日の従来の暗号化から、今日実装できるポスト量子暗号化への量子耐性のある移行を提供します。RFC 8784では暗号化のアップグレードは必要ないため、トンネルの両側にある両方のVPNデバイスが対応している限り、実装は簡単かつ高速です。

RFC 9242とRFC 9370はRFC 8784よりも多くのリソースを消費しますが、Shorのアルゴリズムに対して脆弱ではない新しいPQC数学アルゴリズムに基づく動的なキー生成機能を提供します。RFC 9242およびRFC 9370では暗号化のアップグレードが必要なため、ハイブリッド キー テクノロジーの導入には時間がかかる可能性があり、暗号化の俊敏性を考慮する必要があります。

この章では、IKEv2ピアとその機能がわかっているシナリオと、IKEv2ピアを制御できずその機能がわからないシナリオでポスト量子IKEv2 VPNを設定する方法など、ポスト量子IKEv2 VPNを設定する方法について説明します。

- RFC 8784 PPKを使用したポスト量子IKEv2 VPNの設定に、ポスト量子事前共有鍵を使用してVPN通信を保護するためポスト量子IKEv2 VPN構成手順とオプションを示します。
- RFC 9242およびRFC 9370ハイブリッド キーを使用してポスト量子IKEv2 VPNを構成するに、ハイブリッド キーを使用してVPN通信を保護するための構成手順とオプションを示します。
- ポスト量子IKEv2 RFC 8784の設定例に、単純なトポロジの例と、そのトポロジに対してポスト量子IKEv2 VPNサポートを構成する方法を示します。

*RFC 8784*に基づいてポスト量子*IKEv2 VPN*を構成することに加えて、RFC 6379の*IPsec*のための*Suite B*暗号スイートに従って、*VPN*接続を強力な暗号スイートにアップグレードし、*CA*を*4K RSA*キー サイズにアップグレードして、小さいキー サイズを破る総当たり攻撃を軽減し、*VPN*証明書認証を新しい証明書に移行し、*SHA-384*や*SHA-512*などの高ビット*SHA*ハッシュ サイズにアップグレードします。

RFC 8784 PPKを使用したポスト量子IKEv2 VPNの設定

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

RFC 8784に基づくポスト量子IKEv2 VPNは、事前共有秘密を最初のピアリング交換(IKE__SA__INIT Exchange)とは別に(アウトオブバンドで)送信することによって動作します。攻撃者が今侵害または収集し、後で解読することが可能になるピアリング交換で事前共有秘密を送信するのではなく、ピアリング交換は鍵 IDを送信するだけです。鍵IDと事前共有秘密鍵は、ポスト量子事前共有鍵(PQ PPK)と呼ばれる一意のペアを構成します。

各IKEv2ピアは、Key IDを使用して事前共有秘密を検索します。この秘密は、管理者間で安全に送信されるか、Panoramaによってプッシュされ、各IKEv2ピアにローカルに保存されます。事前共有鍵はピアリング交換の一部になることはなく、ポスト量子VPNを通過することもないため、量子コンピューターを使用している攻撃者がそれを盗み、解読し、VPNから収集したデータを復号化するために使用することはできません。

ピアが接続をネゴシエートするときに、各ピアが同じ鍵IDを検索して同じ事前共有秘密を取得できるように、両方のIKEv2ピアは、鍵IDと事前共有秘密の同じアクティブ ペアを持っている必要があります。応答するピアが一致する鍵IDを持っていない場合、または鍵IDに関連付けられた事前共有秘密が発信側と異なる場合、接続は中断されます。ポスト量子コンポーネントを設定する前に、

IKEv2ピアリングとIPSecトンネルをセットアップします。さらに、ファイアウォール間の*IKEv2*および*IPSec*トラフィックを許可し、ロギングを有効にするセキュリティ ポリシーがあることを確認します。

IKEv2 VPNを量子攻撃に耐性のあるものにするには、次の手順を実行します。

STEP 1 | **[Network (ネットワーク)]** > **[Network Profiles (ネットワーク プロファイル)]** > **[IKE Gateways (IKEゲートウェイ)]**を選択し、新しいゲートウェイを追加します。

STEP 2 | ［**General (全般)**］タブの設定を行い、［**Version (バージョン)**］として**[IKEv2 only mode (IKEv2専用モード)]**または**[IKEv2 preferred mode (IKEv2優先モード)]**を選択します。

[IKEv2 only mode (IKEv2専用モード)]では、ピアがIKEv2をサポートしていない場合、ファイアウォールは接続を中止します。**[IKEv2 preferred mode (IKEv2優先モード)]**では、ピアがIKEv2をサポートしていない場合、ファイアウォールはIKEv1にフォールバックします。ただし、VPNはポスト量子のVPN機能を使用するためIKEv2をネゴシエートする必要があるた

め、ファイアウォールがIKEv1にフォールバックすると、それらの機能は利用できなくなります。

*IKEv1*は弱いと考えられています。両方の*IKE*ピアがサポートできる場合は、*VPN*接続を*IKEv2*にアップグレードし、***[IKEv2 only mode (IKEv2*専用モード*)]***を選択して、適切なレベルのセキュリティと*PQ VPN*を使用できることを確認します。

STEP 3 | **[Advanced Options (**詳細オプション**)]**を選択し、非量子オプションを設定します。

［**Version (**バージョン**)**］で**[IKEv2 preferred mode (IKEv2**優先モード**)]**を選択した場合は、**[IKEv1]**と**[IKEv2]**のタブがあります。［**IKEv2**］を選択します。［**Version (**バージョン**)**］で**[IKEv2 only mode (IKEv2**専用モード**)]**を選択した場合は、IKEv2オプションのみが表示されます。

IKEv2 VPNのポスト量子要素を設定するには、**[PQ PPK] (**ポスト量子事前共有鍵**)**を選択します。(［**General (**全般**)]**では、IKE暗号プロファイルの追加とライブネス チェックの設定が可能です)。

STEP 4 | **[Enable Post-Quantum Pre-Shared Key (PPK) (**ポスト量子事前共有鍵**(PPK)**を有効にする**)]**を有効にして、VPNでポスト量子抵抗機能を使用できるようにします。このオプションはデフォルトでは無効になっています。

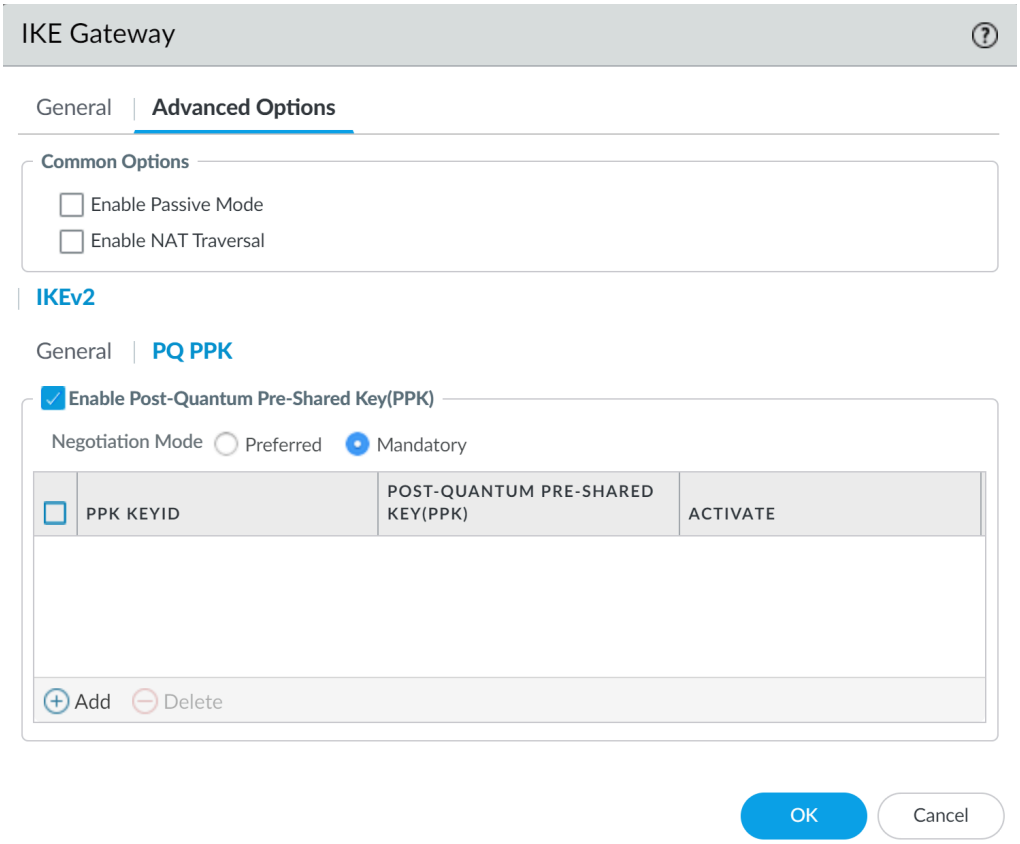
*IKEv2*ネゴシエーション中に使用する*PQ PPK*がファイアウォールにあり、*RFC 8784*をサポートできるように、***[Enable Post-Quantum Pre-Shared Key (PPK) (***ポスト量子事前共有鍵***(PPK)***を有効にする***)]***を有効にする場合は、少なくとも*1*つの*PQ PPK*を設定してアクティブにする必要があります。

STEP 5 | **[Negotiation Mode (**ネゴシエーションモード**)]**を**[Preferred (**優先**)]**または**[Mandatory (**必須**)]**に設定します。

- **[Preferred (**優先**)]**: ファイアウォールがピアとネゴシエートするとき、ファイアウォールはまずPQ PPKを使用してネゴシエートを試みます。ピアがRFC 8784をサポートしていない場合、ファイアウォールは接続のための従来の鍵交換にフォールバックします。ピアがRFC 8784をサポートするかどうかがわからない、または制御できない場合、**[Preferred (**優先**)]**モードでは下位互換性が維持され、接続がドロップされる代わりにフォールバックされます。**[Preferred (**優先**)]**モードがデフォルト モードです。
- **[Mandatory (**必須**)]**: ファイアウォールがピアとネゴシエートする場合、ピアはRFC 8784 PQ PPKをサポートする必要があります。応答側のピアがRFC 8784をサポートしていない

場合、ファイアウォールは接続を中止します。ピアがRFC 8784 PQ PPKをサポートしていることがわかっている場合は、**[Mandatory (必須)]**モードを使用します。

最適なセキュリティを確保するには、可能な場合は***[Mandatory (必須)]***モードを使用してください。



STEP 6 | 最大10個の固有のPQ PPKを追加してアクティブ化します。

PQ PPKは、PPK KeyIDとPPKシークレットの2つのペア要素で構成されます。PPK KeyIDはPPKシークレットを識別する一意の文字列で、**PPK-1**や**Super Strong PPK**など、31文字以内の任意の文字を指定できます。PPKシークレットはランダムな事前共有鍵であり、両方のピアの管理者が安全な通信方法を使用して鍵を共有し、ピアにアウトオブバンドで設定するため、VPNを通じて転送されることはありません。ファイアウォールは、ピアがローカルでPPKシークレットを検索できるように、IKEv2 VPNでKeyIDのみを送信します。

定義できるPQ PPKの数は、IKEピアがサポートできる内容によって異なります。ベンダーの実装によっては、一意のPQ PPkを10個未満しか許可されない場合があります。実装によって

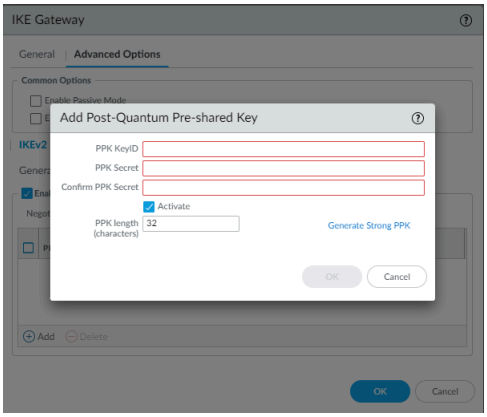
は1個しか許可されていない場合もあります。ピアがサポートできる数を超えるPQ PPKを定義しないでください。両方のピアがまったく同じPQ PPKを使用できる必要があるためです。

複数の*PQ PPK*をサポートするピアに対して、複数のアクティブな*PQ PPK*を設定します。ファイアウォールはアクティブな*PQ PPK*からランダムに選択するので、*IKEv2*ネゴシエーションにランダム性の要素が追加されます。

複数のPQ PPKを設定すると、PQ PPKの選択にランダムな要素が追加されるため、最も安全です。

PPKシークレットを手動で作成することも、ファイアウォールを使用して強力なシークレットを生成することもできます。自分で鍵を生成する場合、またはピアの管理者からPQ PPKを受け取り、ファイアウォールで設定する必要がある場合は、PPKシークレットを手動で設定

します。PPKシークレットが長いほどエントロピー ビット数が多くなり、PPKシークレットが解読されにくくなります。



ASCII文字を使用して指定できるPPKシークレットを手動で設定するには、次の手順を実行します。

1. 一意の**PPK KeyID**を31文字以内で指定します。
2. 一意でランダムな**PPK**シークレット文字列を指定します。文字列は32-128文字(16-64バイト、128-512ビットのエントロピーに相当)からなります。

   *64*文字以上*(32*バイト、つまり*256*ビットのエントロピー*)*の***PPK***シークレットを指定して、強力なキーを作成します。
3. **[Confirm PPK Secret (PPK**シークレットの確認**)]**にまったく同じ文字列を指定します。

   *PPK*シークレットを安全に保管します。*PPK*シークレットは平文で表示されないので、今保存しないと後で取り出すことができません。*(PQ PPK*を削除して、必要に応じて別の*PPK*を設定できます*)*。*IKEv2*ピアは同じ*PQ PPK(KeyID*と*PPK*シークレット*)*を持つ必要があるため、*PPK*シークレットを別の管理者に伝える必要がある場合があります。その場合は、使用する通信方式が暗号学的に安全であることを確認し、*PPK*シークレットが安全に保存されていることを確認します。

   *NSA*は、*RFC 8784*量子事前共有鍵を含む事前共有鍵を安全に扱うためのガイダンスを公開しています。
4. ファイアウォールがPPK KeyIDとPPKシークレットのペア(PQ PPK)を使用してピアとネゴシエートできるように、デフォルトで**[Activate (**アクティブ**)]**が選択されています。ピアと

ネゴシエートするときにファイアウォールでこのPPK KeyIDとPPKシークレットのペアを使用しないようにするには、**[Activate (アクティブ)]**のチェックを外します。

たとえば、ファイアウォールで新しいPQ PPKを設定する場合、イニシエータがまだピアにインストールされていないPQ PPKを使用するため、ピアの管理者がピアに同じPQ PPKを追加できるまで非アクティブにすることができます。

5. **OK** をクリックします。**[PQ PPK]**タブには、PPK KeyIDが平文で表示され、事前共有鍵が非表示になり、PQ PPKのアクティベート状態が表示されます。

ファイアウォールの強力なPPK自動生成(16進文字を使用)を使用してPPKシークレットを構成するには、次の手順を実行します。

1. 一意の**PPK KeyID**を31文字以内で指定します。
2. **[PPK length (characters) (PPK**長**(**文字数**)]**を**PPK**シークレット用に生成する長さに設定します。デフォルトは32文字(16バイト)です。

   ***[PPK length (characters) (PPK**長**(**文字数**)]**を*64*文字以上*(32*バイト、つまり*256*ビットのエントロピー*)*に設定して、強力な鍵を生成します。
3. **[Generate Strong PPK (**強力な**PPK**を生成する**)]**をクリックします。ファイアウォールは、**[PPK length (characters) (PPK**長**(**文字数**)]**で指定された長さの強力なPPKシークレットを生成し、表示します。

   *PPK*シークレットが平文で表示されるのはこの時だけです。シークレットを安全に保管しないと、シークレットを取り出すことができません。*(PQ PPK*を削除して、必要に応じて別の*PPK*を設定できます*)*。*IKEv2*ピアは同じ*PQ PPK(KeyID*と*PPK*シークレット*)*を持つ必要があるため、*PPK*シークレットを別の管理者に伝える必要がある場合があります。その場合は、使用する通信方式が暗号学的に安全であることを確認し、*PPK*シークレットが安全に保存されていることを確認します。

   PPKシークレットをコピーして**[OK]**をクリックし、**[PPK Secret (PPK**シークレット**)]**フィールドと**[Confirm PPK Secret (PPK**シークレットの確認**)]**フィールドにペーストします。
4. ファイアウォールがPPK KeyIDとPPKシークレットのペア(PQ PPK)を使用してピアとネゴシエートできるように、デフォルトで**[Activate (アクティブ)]**が選択されています。ピアとネゴシエートするときにファイアウォールでこのPPK KeyIDとPPKシークレットのペアを使用しないようにするには、**[Activate (アクティブ)]**のチェックを外します。

   たとえば、ファイアウォールで新しいPQ PPKを設定する場合、イニシエータがまだピアにインストールされていないPQ PPKを使用するため、ピアの管理者がピアに同じPQ PPKを追加できるまで非アクティブにすることができます。
5. **OK** をクリックします。**[PQ PPK]**タブには、PPK KeyIDが平文で表示され、事前共有鍵が非表示になり、PQ PPKのアクティベート状態が表示されます。

STEP 7 | **[OK]**をクリックしてVPNを作成します。

STEP 8 | 設定を **Commit**（コミット）します。

ポスト量子IKEv2 RFC 8784の設定例のトピックでは、単純なトポロジの例と、トポロジのポスト量子*IKEv2 VPN*サポートを構成する方法について説明します。

STEP 9 | 両方のIKEv2ピアの管理者でない場合は、PQ PPK (KeyIDとPPKシークレット)をピアの管理者に安全に伝達し、ピアにインストールしてもらいます。PQ PPKの安全な通信とストレージは、データの安全性を確保するために重要です。

ポスト量子*VPN*接続を起動するには、両方の*IKEv2*ピアが同じアクティブな鍵*ID*と関連する事前共有秘密を持っている必要があります。

RFC 9242およびRFC 9370ハイブリッド キーを使用してポスト量子IKEv2 VPNを構成する

どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.2以降

RFC 9242およびRFC 9370に基づくポスト量子IKEv2 VPNは、初期ピアリング交換(IKE_SA_INIT交換)で2つ以上の鍵交換メカニズム(KEM)を使用してハイブリッド キーを作成することで機能します。ハイブリッド キーは、侵害されたKEMが Harvest Now, Decrypt Later (HNDL) を使用した量子攻撃を成功させることを防ぐことで、量子耐性を実現します。ハイブリッド キーの作成に使用されるすべてのKEMが侵害されない限り、データは保護されたままになります。

標準はまだ比較的新しいため、各ベンダーが実装に関して標準を異なる解釈で示す可能性があります。そのため、両側で構成を同一に保つことで、物事をシンプルに保ち、ポスト量子VPNトンネルを正常に構築できるようになります。相互運用性の可能性を最小限に抑えるには、オプションのキー ネゴシエーション ラウンドごとに、VPNトンネルの両側で同じPQCとセキュリティ強度が構成されていることを確認します。また、両側のIKEv2フラグメンテーション設定をチェックして、正しく設定されていることを確認します。

ポスト量子コンポーネントを構成する前に、IKEv2ピアリングとIPSecトンネルを設定します。さらに、ファイアウォール間の*IKEv2*および*IPSec*トラフィックを許可し、ロギングを有効にするセキュリティ ポリシーがあることを確認します。

データが長期間保護されるようにするには、2つ以上のKEMを使用する必要があります。また、RFC 8784による事前共有鍵とRFC 9242およびRFC 9370によるハイブリッド キーの両方を有効にすることで、さらに多層防御を追加できます。

IKEv2 VPNを量子攻撃に耐性のあるものにするには、次の手順を実行します。

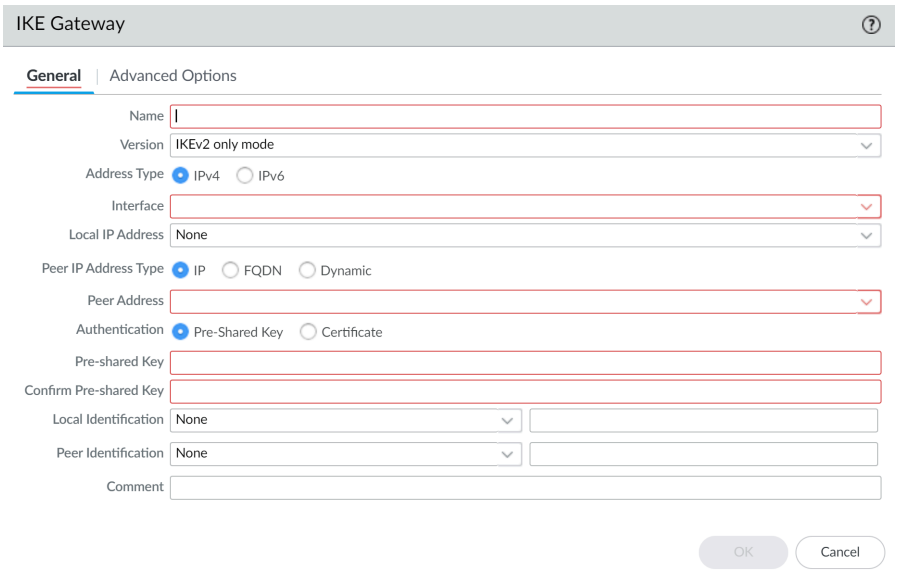
STEP 1 | **[Network (ネットワーク)]** > **[Network Profiles (ネットワーク プロファイル)]** > **[IKE Gateways (IKEゲートウェイ)]**を選択し、新しいゲートウェイを追加します。

STEP 2 | **[General (全般)]**設定を構成し、**[Version (バージョン)]**として**[IKEv2 only mode (IKEv2専用モード)]**または**[IKEv2 preferred mode (IKEv2優先モード)]**のいずれかを選択します。

[IKEv2 only mode (IKEv2専用モード)]では、ピアがIKEv2をサポートしていない場合、ファイアウォールは接続を中止します。**[IKEv2 preferred mode (IKEv2優先モード)]**では、ピアがIKEv2をサポートしていない場合、ファイアウォールはIKEv1にフォールバックします。た

だし、VPNはポスト量子VPN機能を使用するためにIKEv2をネゴシエートする必要があるため、ファイアウォールがIKEv1にフォールバックすると、それらの機能は使用できません。

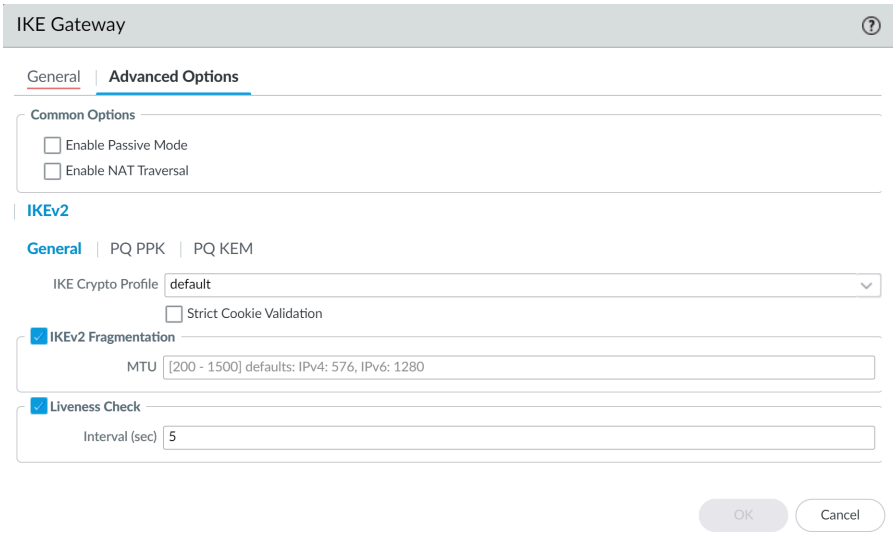
*IKEv1*は弱いと考えられています。両方の*IKE*ピアがサポートできる場合は、*VPN*接続を*IKEv2*にアップグレードし、***[IKEv2 only mode (IKEv2**専用モード**)]***を選択して、適切なレベルのセキュリティと*PQ VPN*を使用できることを確認します。



STEP 3 | **[Advanced Options (詳細オプション)]**を選択し、非量子オプションを設定します。**[IKEv2]**を選択し、**[General (全般)]**設定を構成します。

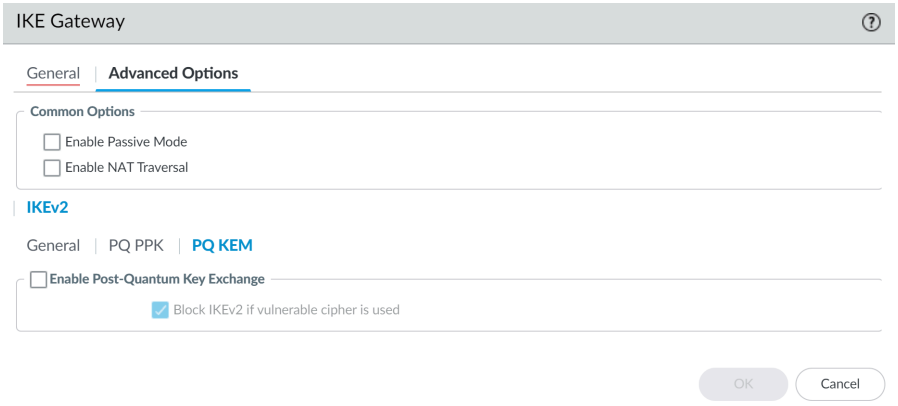
[General (全般)]では、IKE暗号プロファイルを追加し、**[IKEv2 Fragmentation (IKEv2フラグメンテーション)]**を有効にし、**[Liveness Check (ライブネス チェック)]**を設定できます。

キー サイズとデータ ペイロードが大きくなるため、PQC KEMを使用する場合はIKEv2フラグメンテーションを有効にする必要があります。両方のVPN終端デバイスを同じフラグメンテーション値に設定する必要があります。



STEP 4 | PQ KEMの**[Enable Post-Quantum Key Exchange (ポスト量子鍵交換を有効にする)]**を有効にして、VPNでポスト量子抵抗機能を使用できるようにします。このオプションはデフォルトでは無効になっています。

オプションで、**[Block IKEv2 if vulnerable cipher is used (脆弱な暗号が使用されている場合は**IKEv2をブロックする**)]**を有効にします。このオプションを有効にすると、ファイアウォールは、IKE暗号プロファイルで脆弱なKEMが使用されていることを検出すると、すべての新しいIKEv2ピアリングをブロックします。以前に確立された既存のVPNトンネルは継続できます。

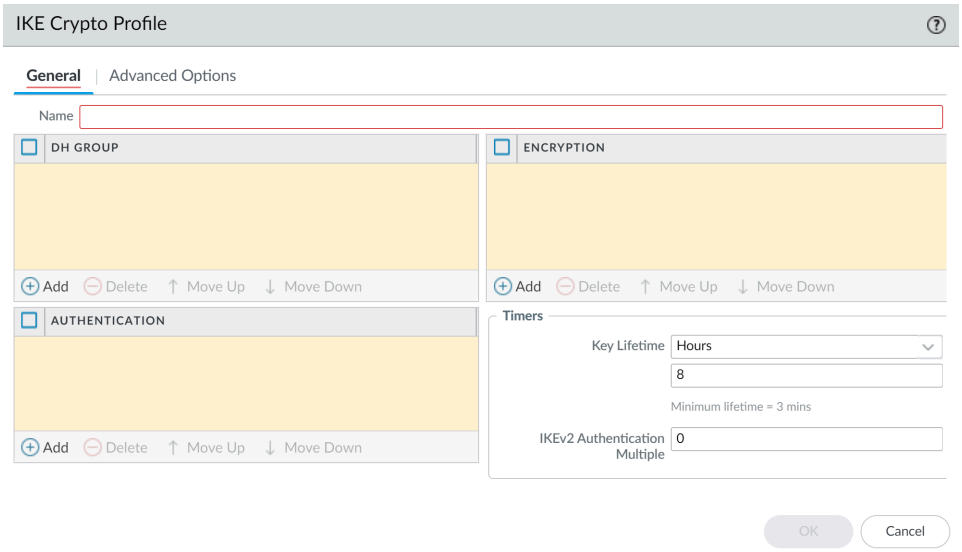


STEP 5 | **[OK]** をクリックしてIKEゲートウェイを作成します。

STEP 6 | **[Network (ネットワーク)]** > **[Network Profiles (ネットワーク プロファイル)]** > **[IKE Crypto (IKE暗号)]**を選択し、新しいプロファイルを追加します。

STEP 7 | **[General (全般)]**設定を構成し、デフォルトのIKEv2鍵交換の暗号化コンポーネント(DHグループ、暗号化、認証、タイマー)を選択します。

量子耐性を高めるために、強力な従来の鍵交換構成を選択します。*DH*グループ*20*以上、*AES-256-GCM*、およびキーの有効期間を使用してキーをより頻繁に更新します。特定の間隔でキーを完全に再生成するには、ゼロより大きい値を設定して*IKEv2*認証倍数を有効にします。キーの有効期間の倍数に達すると、キーは再生成されます。



STEP 8 | **[Advanced Options (詳細オプション)]**を選択し、オプションの**[Post-Quantum IKEv2 Additional Key Exchange (ポスト量子IKEv2追加鍵交換)]**ラウンドを構成します。

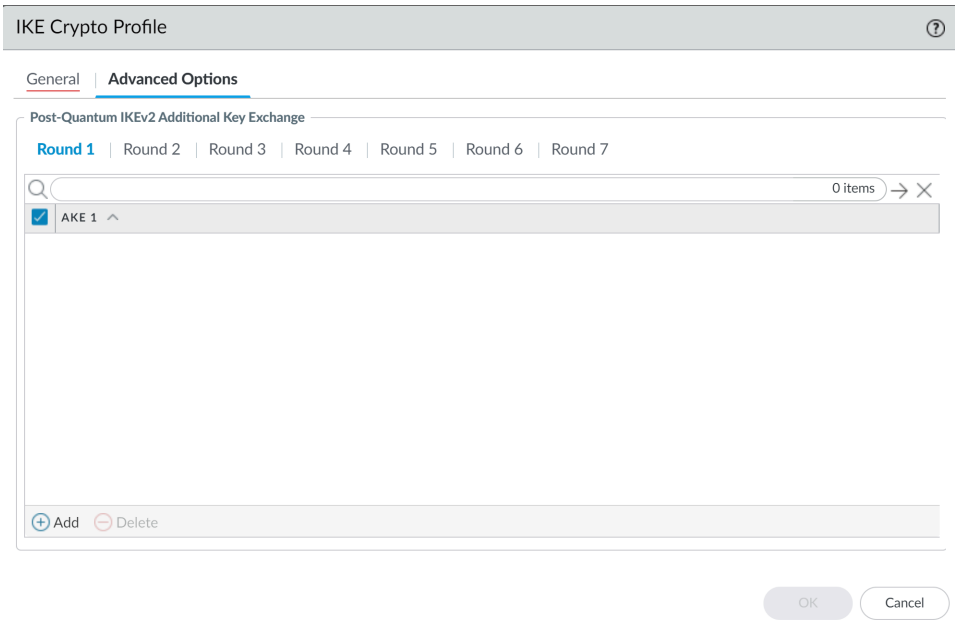
RFC 9370では、最大7つの追加鍵交換ラウンド(ラウンド1～7)が許可されます。量子耐性を追加するには、少なくとも1つのPQC KEMが必要です。PQC KEMを追加すると量子耐性がさらに高まりますが、ネゴシエーションのオーバーヘッドが追加され、IKEv2パケットのサイズが増加します。

RFC 9370では、追加の鍵交換ラウンドをスキップできます。スキップされたラウンドの場合は、空白のままにするか、**[None (なし)]**に設定できます。

追加鍵交換ラウンドのPQCの順序によって優先順位が設定されます。一番上にリストされているPQCが優先され、トンネルの反対側のVPN終端デバイスがそれをサポートしている場合

に選択されます。両側がサポートできる最も強力なPQCをネゴシエートする場合は、各追加鍵交換ラウンドで、最もセキュリティ レベルの高いPQCをリストの先頭に配置します。

相互運用性の問題を最小限に抑えるには、トンネルの両側にある*VPN*終端デバイスを同じ*PQC*とセキュリティ強度に設定する必要があります。機密情報を長期にわたって保護するには、レベル*3*以上のセキュリティ強度を持つ*PQC*を選択してください。

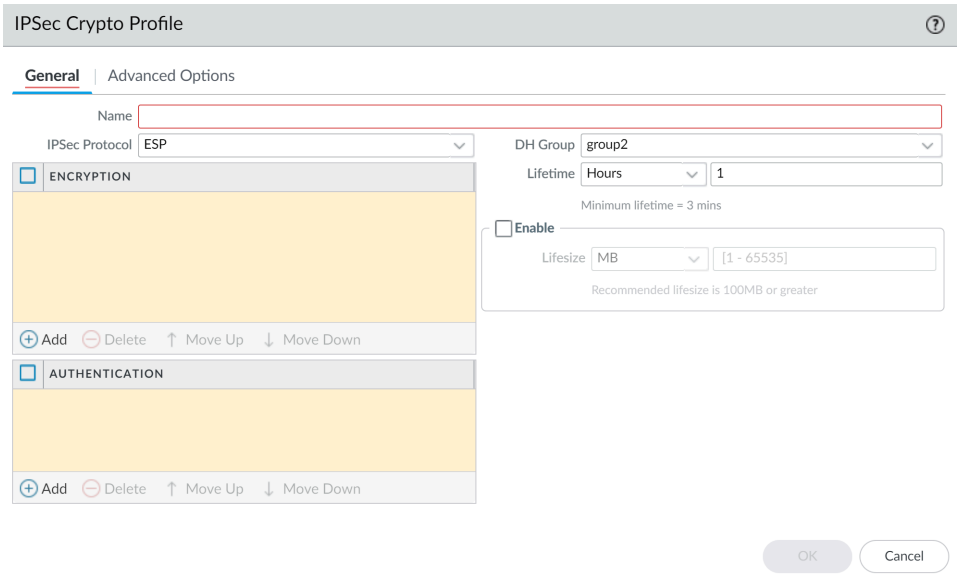


STEP 9 | **[OK]**をクリックしてIKE暗号プロファイルを作成します。

STEP 10 | **[Network (ネットワーク)]** > **[Network Profiles (ネットワーク プロファイル)]** > **[IPSec Crypto (IPSec暗号)]**を選択し、新しいプロファイルを追加します。

STEP 11 | **[General (全般)]**設定を構成し、IPSec ESPプロトコルの暗号化コンポーネント(暗号化、認証、DHグループ、有効期間)を選択します。

量子耐性を高めるために、強力な従来の暗号化構成を選択します。*DH*グループ*20*以上、*AES-256-GCM*、*SHA384*以上、およびキーの有効期間を使用してキーをより頻繁に更新します。



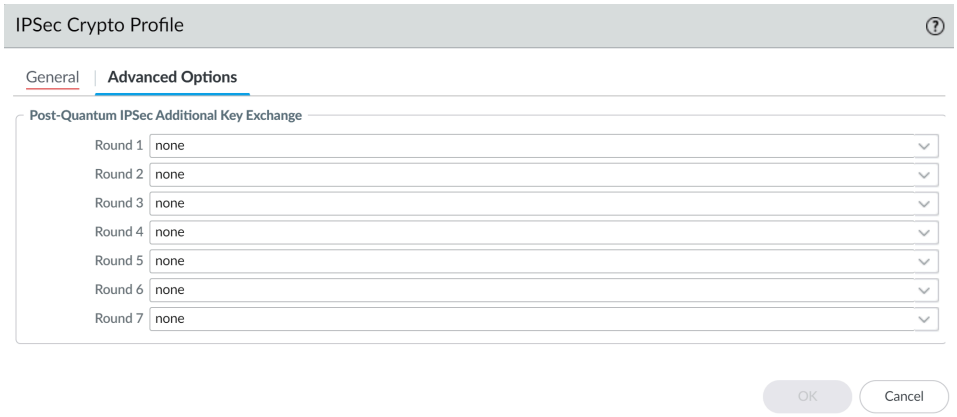
STEP 12 | **[Advanced Options (詳細オプション)]**を選択し、オプションの**[Post-Quantum IPSec Additional Key Exchange (ポスト量子IPSec追加鍵交換)]**ラウンドを構成します。

最大7つの追加鍵交換ラウンド(ラウンド1～7)が許可され、ラウンドごとに1つのPQC KEMのみが許可されます。量子耐性を追加するには、少なくとも1つのPQC KEMが必要です。PQC

KEMを追加すると量子耐性がさらに高まりますが、ネゴシエーションのオーバーヘッドが追加され、IPSec鍵更新パケットのサイズが増加します。

IPSecトンネルの両側は、各追加鍵交換ラウンドで同じPQCとセキュリティ強度レベルで構成する必要があります。不一致がある場合、鍵更新操作は失敗します。

機密情報を長期にわたって保護するには、レベル3以上のセキュリティ強度を持つ*PQC*を選択してください。



STEP 13 | **[OK]**をクリックしてIPSec暗号化プロファイルを作成します。

STEP 14 | 設定を **Commit**（コミット）します。

両方の*IKEv2*ピアの管理者でない場合は、*IKEv2*ゲートウェイ、*IKE*暗号プロファイル、および*IPSec*暗号プロファイル情報をピアの管理者に伝え、ピアデバイスにインストールしてもらいます。

ポスト量子IKEv2 RFC 8784の設定例

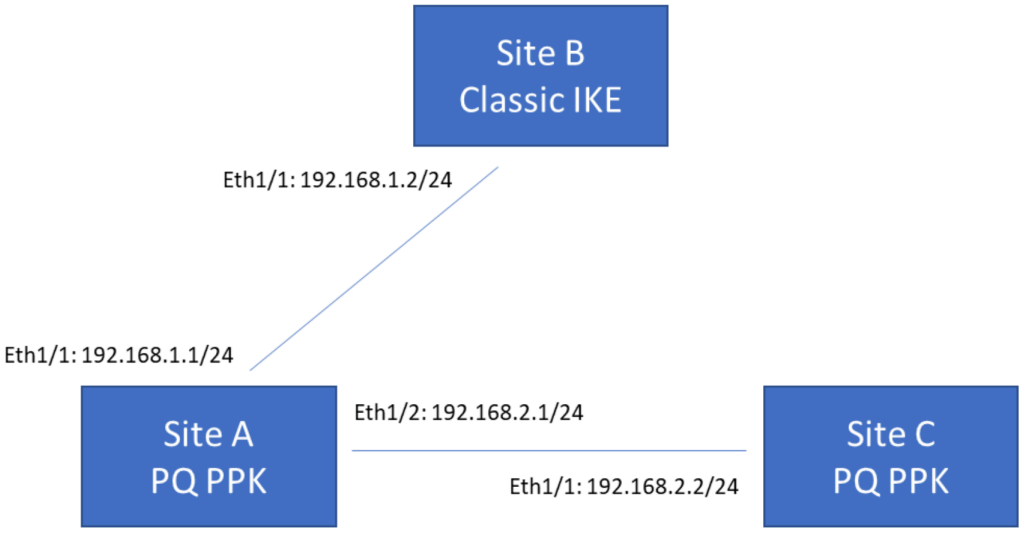
どこで使用できますか?	何が必要ですか?
• PAN-OS	❑ PAN-OS 11.1以降。

この例では、IKEv2ポスト量子VPNの基本的な設定とトポロジを示します。RFC 8784(量子コンピューターや量子暗号からの攻撃に抵抗するポスト量子VPN)をサポートしている2つのサイトと、RFC 8784をサポートしていない1つのサイトが含まれています。

RFC 8784をサポートするファイアウォールがRFC 8784をサポートするファイアウォールと通信する場合、デバイスはポスト量子設定を使用します。鍵交換では、接続からアウトオブバンドで共有されるポスト量子事前共有鍵(PQ PPK)が使用されるため、IKEハンドシェイク中にPQ PPKが公開されることはありません。ファイアウォールは、PQ PPKと従来のDiffie-Hellmann (DH)鍵材料を混合して(IKEハンドシェイク中に送信される)、素数に基づかない鍵を作成するため、Shorのアルゴリズムでは解読できません。これにより、ファイアウォールは量子耐性のある鍵を作成し、攻撃者が今すぐには解読できないデータを盗み出し、暗号に関連する量子コンピューター(CRQC)が解読できるまで保存しておくというHarvest Now, Decrypt Later攻撃から保護することができます。

RFC 8784をサポートするファイアウォールがRFC 8784をサポートしないファイアウォールと通信する場合、RFC 8784ファイアウォールは従来のDH鍵交換にフォールバックできます。その場合、ファイアウォールはPQ PPKを混在させず、DH鍵材料のみを使用して鍵を作成します。この場合のVPNトラフィックは、Harvest Now, Decrypt Later攻撃に対して脆弱であることを理解することが重要です。

この単純なトポロジ例は、IKEv2 VPNによって接続された、異なるサイトに配置された3つのファイアウォールで構成されています。そのうち2つのファイアウォールはRFC 8784をサポートし、1つのファイアウォールはRFC 8784をサポートしていません。



この例では:

- サイト**A**はRFC 8784をサポートしています。サイトBへの接続はEth1/1:192.168.1.1/24であり、サイトCへの接続はEth1/2:192.168.2.1/24です。サイトAには2つのIKEv2ゲートウェイが必要です。1つはサイトBと接続するためのゲートウェイで、もう1つはサイトAと接続するためのゲートウェイです。
- サイト**B**は従来のIKEv2 VPNのみをサポートしており、RFC 8784をサポートしていません。サイトAへの接続はEth1/1:192.168.1.2/24です。サイトBでは、サイトAに接続するためにIKEv2ゲートウェイが1つ必要です。サイトBはRFC 8784をサポートしていないため、IKEv2ゲートウェイ構成にはPQ PPKが含まれていません。
- サイト**C**はRFC 8784をサポートしています。サイトAへの接続はEth1/1:192.168.2.2/24です。サイトCでは、サイトAに接続するためのIKEv2ゲートウェイが1つ必要です。

*RFC 8784*をサポートする各*IKEv2 VPN*ピアは、まったく同じ*PQ PPK*のセット*(KeyID*と*PPK*シークレット文字列のペア*)*がインストールされ、アクティブ化されている必要があります。選択した*PQ PPK*が両方のピアで使用できない場合、接続は中断されます。

*KeyID*は*PPK*シークレット文字列を識別します。

*IKEv2*ピアは*IKEv2*ハンドシェイク中に*KeyID*を送信しますが、*PPK*シークレット文字列はアウトオブバンドで共有され、*Panorama*によってプッシュされるか、または手動でインストールされるかによって、各ピアに別々にインストールされます。*PPK*シークレット文字列はハンドシェイクで送信されず、結果の*IKEv2*トンネルでも表示されません。代わりに、*IKEv2*ピアは*KeyID*を使用して*PPK*シークレット文字列をローカルで検索し、*DH*鍵材料と混合してポスト量子暗号キーを生成します。

トポロジ例のIKEv2 VPNを設定するには、**[Network (ネットワーク)]** > **[Network Profiles (ネットワーク プロファイル)]** > **[IKE Gateways (IKEゲートウェイ)]**に移動します。

STEP 1 | 他のIKEゲートウェイと同様に、サイトA、B、CのIKEv2 VPNゲートウェイの一般プロパティを設定します。

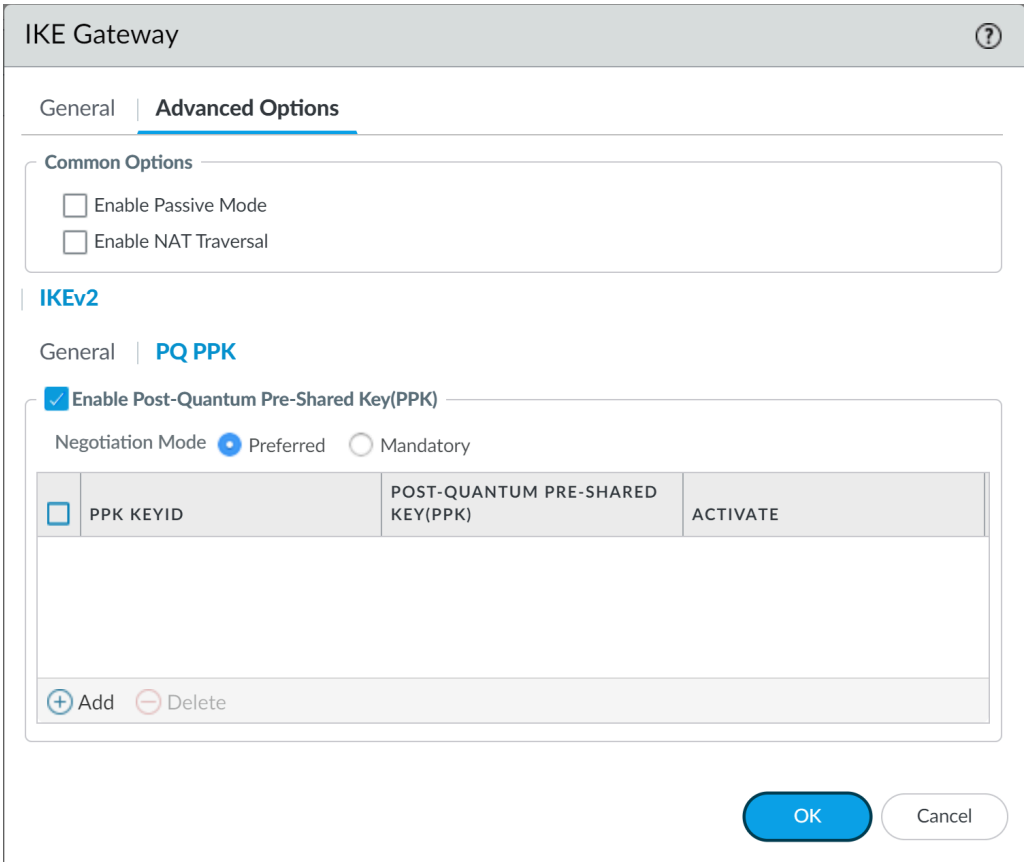
[General (全般)]タブで、アドレス、認証、およびその他の一般的なIKEゲートウェイ情報を設定します。最適なセキュリティを確保するために、**[Version (バージョン)]**を**[IKEv2 mode only (IKEv2モードのみ)]**に設定します。IKEv1は脆弱なプロトコルと見なされ、RFC 8784ポスト量子VPNをサポートしません。

[General (全般)]タブで設定する事前共有鍵は、量子ベースの攻撃に抵抗するポスト量子の事前共有鍵ではありません。トンネル全体での対称認証に使用されます。

STEP 2 | パッシブモード、NATトラバーサル、IKE暗号プロファイルなど、3つのサイトすべてに共通で一般的な詳細オプションを設定します。

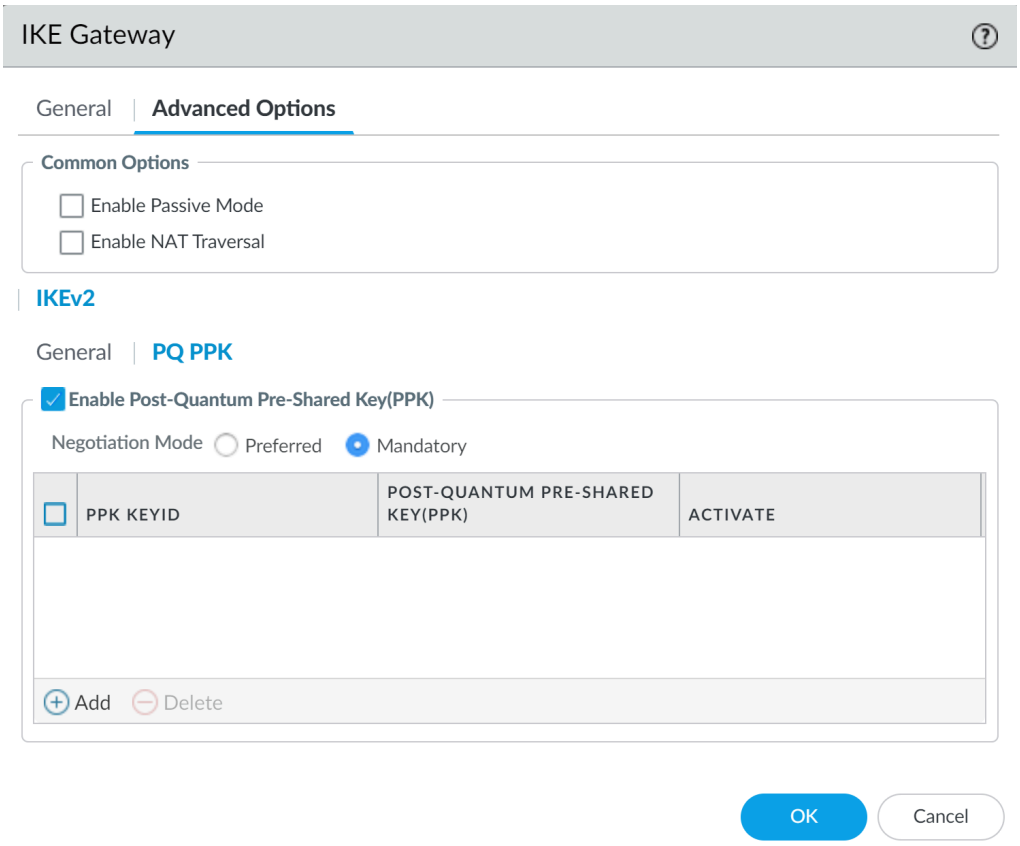
STEP 3 | **[Advanced Options (詳細オプション)]** > **[PQ PPK]**タブで、サイトAのIKEv2 VPNからサイトCに対し、およびサイトCのIKEv2 VPNからサイトAに対する、**[Enable Post-Quantum Pre-Shared Key (PPK) (ポスト量子事前共有鍵(PPK)を有効にする)]**をオンにします。

サイトBはRFC 8784をサポートしていないため、サイトBのIKEゲートウェイ設定やサイトAのIKEv2 VPNからサイトBへの設定に対し**[Enable Post-Quantum Pre-Shared Key (PPK) (ポスト量子事前共有鍵(PPK)を有効にする)]**をオンにする必要はありません。



[Enable Post-Quantum Pre-Shared Key (PPK) (ポスト量子事前共有鍵(PPK)を有効にする)]をオンにすると、**[Negotiation Mode (ネゴシエーションモード)]**のデフォルト設定は**[Preferred (優先)]**となり、RFC 8784をサポートできない接続は従来の暗号方式にフォールバックされます。(**[Mandatory (必須)]**モードでは、ピアがPQ PPKをサポートしていない場合、ファイアウォールは接続を中止します)。

STEP 4 | サイトAからサイトC、およびサイトCからサイトAのIKEv2 VPNの**[Negotiation Mode (ネゴシエーションモード)]**を**[Mandatory (必須)]**に設定します。



[Negotiation Mode (ネゴシエーションモード)]を**[Mandatory (必須)]**に設定すると、サイトAとサイトCがVPNトンネルをネゴシエートするときに、従来のVPNではなく常に量子耐性VPNが設定されます。ピアがRFC 8784をサポートしていることが確実な場合は、**[Mandatory (必須)]**を使用します。確信が持てない場合は、**[Preferred (優先)]**モードを使用して、ピアがRFC 8784をサポートしていない場合、たとえば、自分が管理していない社外のデバイスとピア接続する場合などに、ファイアウォールが従来のIKEv2 VPNにフォールバックできるようにします。

STEP 5 | サイトAからサイトCへのIKEv2接続およびサイトCからサイトAへのIKEv2接続にアクティブなPQ PPKを設定します。サイトAとサイトCがIKEv2接続を確立する際、これらのアク

ティブなPQ PPKから選択し、選択したPQ PPKをDH鍵材料と混合して、素数に基づかない安全なキーを作成します。

サイト*A*からサイト*B*への通信、またはサイト*B*からサイト*A*への通信には、サイト*B*が*RFC 8784*をサポートしていないため、ポスト量子設定はありません。

サイトAとサイトCの両方のIKEv2ピアは、アクティブなPQ PPKの設定が完全に一致している必要があります。

- Panoramaが両方のIKEv2ピアを管理している場合、Panorama上で設定を作成し、管理対象ファイアウォールにプッシュすることができます。
- PanoramaがIKEv2ピアの両方を管理しておらず、異なる管理者がピアを管理している場合は、暗号化メールなど安全な方法でPQ PPKを他方の管理者に伝え、鍵を安全に保管してください。

各PQ PPKのKeyIDには任意の名前を付けることができます。PQ PPKごとにKeyIDとペアにするPPKシークレットを手動で設定することも、ファイアウォールが強力なPPKシークレットを生成することもできます。この例では、両方の方法を使用する方法を示します。

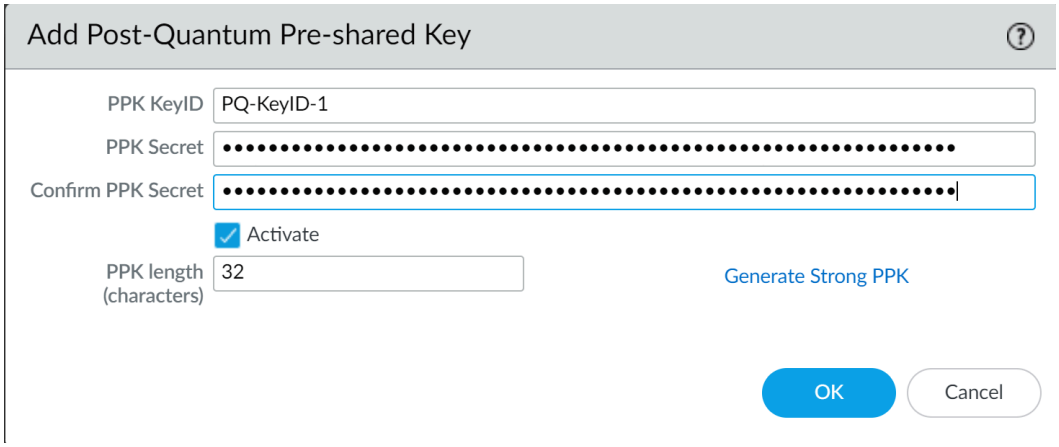
手動で構成したPPKシークレットを使用してPQ PPKを作成するには、次の手順を実行します。

1. PQ PPKを追加します。
2. **[Add Post-Quantum Pre-shared Key (**ポスト量子事前共有鍵の追加**)]**ダイアログで、**PPK KeyID**名を入力します。この例では、名前は**`PQ-KeyID-1`**です。
3. **[PPK KeyID]**と**[Confirm PPK Secret (PPK**シークレットの確認**)]**にまったく同じASCII文字列を入力(または別のソースからコピーして貼り付け)します。

   *PQ PPK (KeyID*とその*PPK*シークレット*)*を安全に保管します。手動で入力された*PPK*シークレットの場合、シークレットが平文で示されることはありません。*PPK*シークレットを紛失すると、復元できなくなります。*(PQ PPK*を削除してから、新しい*PPK*を設定できます*)*。

   [PPK KeyID]と**[Confirm PPK Secret (PPK**シークレットの確認**)]**が一致しない場合、`PPK Secret and Confirm PPK Secret Do Not Match (PPK`シークレットと`PPK`シークレットの確認が一致しません) というエラーメッセージが表示されます。ベストプラクティスとして、少なくとも64文字(32バイト、つまり256ビットのエントロピー)の長さのランダムなPPKシークレットを指定して、強力な鍵を作成します。デフォルトでは、新しいキーがアクティブになります。IKEピア間のネゴシエーションでキーを使用しない場合は、［**Activate (**アクティベート**)**］を選択解除します。一方のピアでPQ PPKを非アクティブにした場合は、もう一方のピアでも非アクティブにする必

要があります。次の例は、64文字の強力なキーを示しています(手動で入力したキーが平文で表示されることはありません)。



[PPK length (characters) (PPK**長**(**文字数**)]フィールドは、ファイアウォールが生成したキーにのみ適用されます。手動で設定された*PPK*シークレット文字列の長さは制御しません。

4. **[OK]**をクリックして、手動で設定したPQ PPKをインストールします。
5. Panoramaが両方のピアを管理している場合、Panorama上で設定を作成し、管理対象ファイアウォールにプッシュすることができます。Panoramaが両方のピアを管理しておら

ず、別の管理者がVPNピアを管理している場合、PQ PPKをその管理者に安全に伝達し、PQ PPKをピアにインストールしてもらいます。

ファイアウォールが生成するPPKシークレットを使用してPQ PPKを作成するには、次の手順を実行します。

1. PQ PPKを追加します。
2. **[Add Post-Quantum Pre-shared Key (**ポスト量子事前共有鍵の追加**)]**ダイアログで、**PPK KeyID**名を入力します。この例では、名前は**PQ-Key-ID-2**です。
3. **[PPK length (characters) (PPK**長**(**文字数**)]**を64文字以上(32バイト、つまり256ビットのエントロピー)に設定して、強力なキーを作成します。
4. **[Generate Strong PPK (**強力な**PPK**を生成する**)]**をクリックします。

   ファイアウォールは、**[PPK length (characters) (PPK**長**(**文字数**)]**で設定された長さの強力なランダムな16進数のPPKシークレットを生成します。
5. PPKシークレット文字列をハイライトしてコピーします。

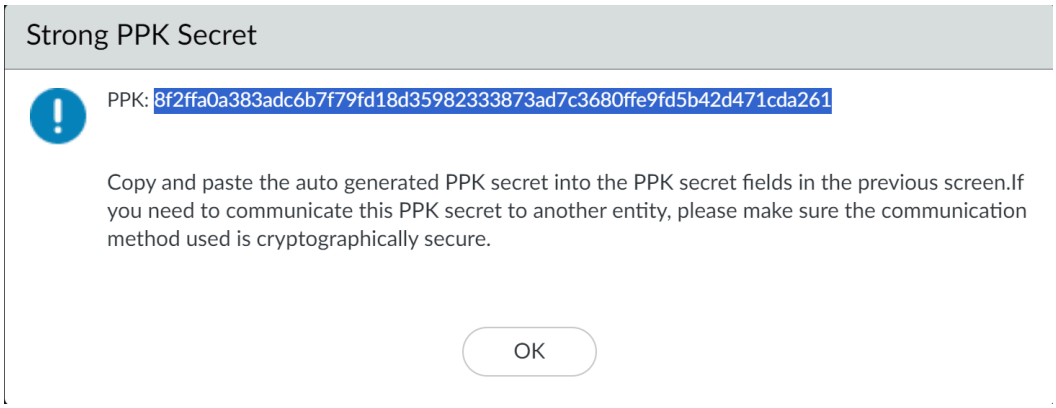
   *16*進数のシークレットだけをコピーします。先頭の*PPK:*文字はコピーしないでください。たとえば、以下のシークレットが生成された場合:

   PPK:38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d

   コピーするのは以下の部分のみです:

   38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d

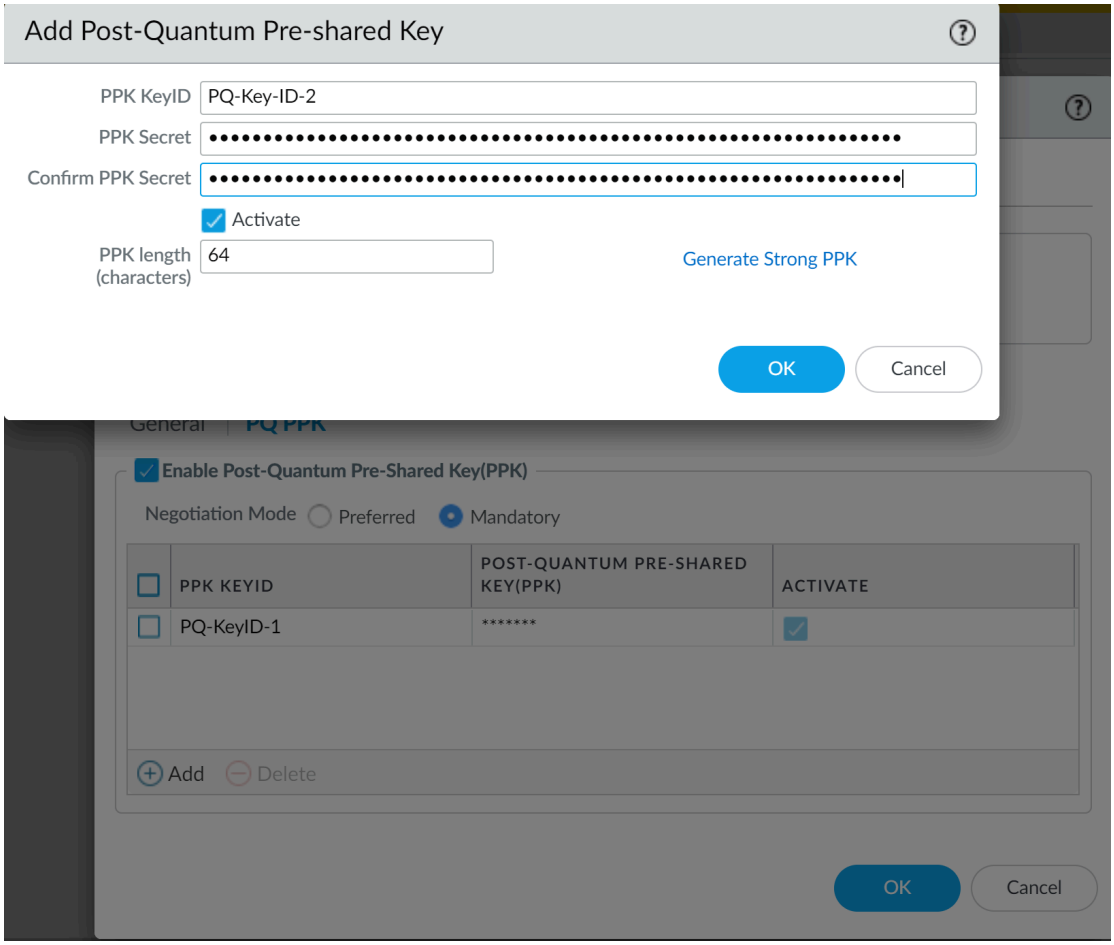
   先頭の*PPK:*はシークレット文字列の一部ではありません。



コピーしたファイアウォールが生成したPPKシークレットを安全に保管します。［**OK**］をクリックすると、PPKシークレットは二度と平文で表示されません。こ

こでPPKシークレットをコピーして安全に保管しないと、PPKシークレットがわからなくなり、このPQ PPKを削除して新しく設定しなければならなくなります。

6. コピーしたPPKシークレットがクリップボードに残っているか、セキュア ストレージからコピーできる状態で、**[OK]**をクリックします。PPKシークレットをコピーしなかった場合は、別の強力なPPKシークレットを生成し、必ずコピーして安全に保管してください。
7. コピーしたPPKシークレット文字列を、**[Add Post-Quantum Pre-Shared Key (**ポスト量子事前共有鍵の追加**)]**の**[PPK Secret (PPK**シークレット**)]**フィールドと**[Confirm PPK Secret (PPK**シークレットの確認**)]**フィールドの両方に貼り付けます。

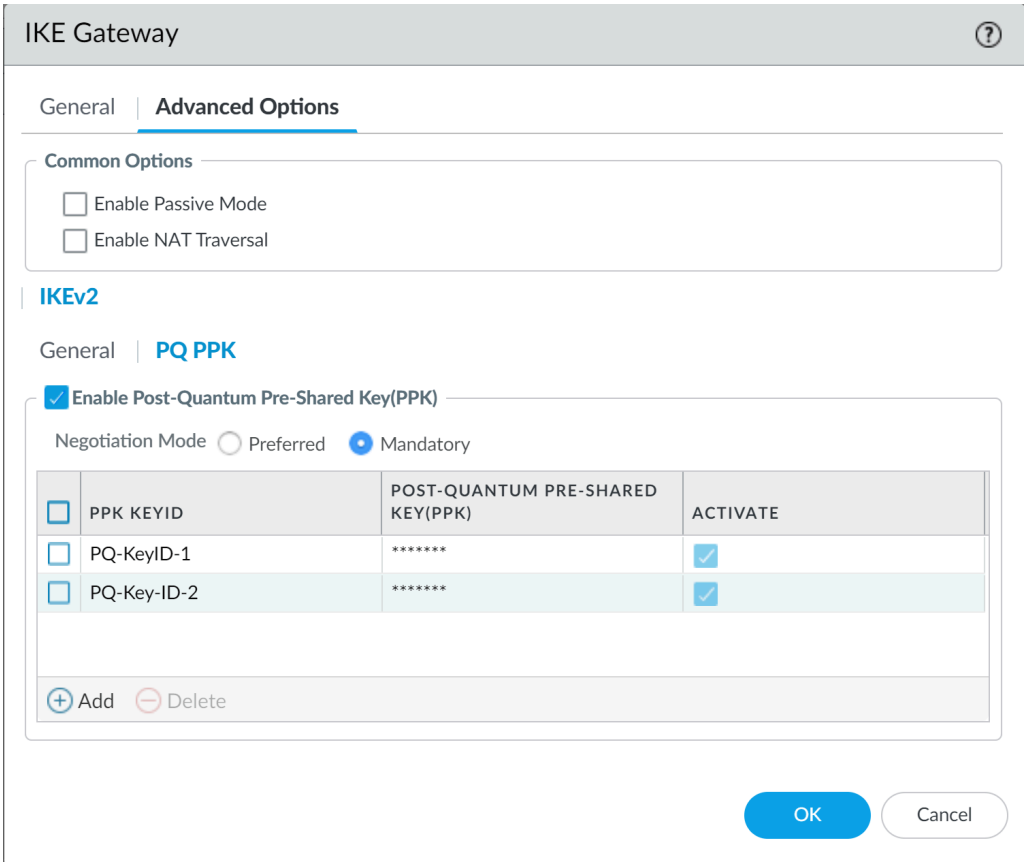


デフォルトでは、新しいキーがアクティブになります。IKEピア間のネゴシエーションでキーを使用しない場合は、［**Activate (**アクティベート**)**］を選択解除します。一方のピアでPQ PPKを非アクティブにした場合は、もう一方のピアでも非アクティブにする必要があります。

8. **[OK]**をクリックして、ファイアウォールで生成されたPQ PPKをインストールします。
9. Panoramaが両方のピアを管理している場合、Panorama上で設定を作成し、管理対象ファイアウォールにプッシュすることができます。Panoramaが両方のピアを管理しておら

ず、別の管理者がVPNピアを管理している場合、PQ PPKをその管理者に安全に伝達し、PQ PPKをピアにインストールしてもらいます。

サイトAとサイトCの場合、この例で作成された2つのPQ PPKは、**[Mandatory (必須)]**モードでアクティブなPQ PPKとしてリストされます。



PPKシークレットは非表示になり、平文では表示されなくなります。サイトAとサイトCの間のIKEv2 VPNが、量子攻撃に抵抗するためにRFC 8784を実装するようになりました。サイトAとサイトBの間のIKEv2 VPNは、引き続き従来のDH鍵交換を使用しており、依然としてHarvest Now, Decrypt Later攻撃に対して脆弱です。

この例のサイトBがRFC 8784をサポートするようにアップグレードされた場合、同じプロセスに従ってサイトAとサイトBの間、およびサイトBとサイトAの間のIKEv2 VPNをアップグレードします。