paloalto TECHDOCS

量子安全管理

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

量子安全概念..5

量子计算威胁..6

RFC 8784 如何抵御量子计算威胁..9

RFC 9242 和 RFC 9370 如何抵抗量子计算威胁...11

支持后量子功能...14

后量子迁移规划与准备..16

抵抗后量子攻击的最佳实践..23

进一步了解后量子安全性..27

配置量子抵抗 IKEv2 VPN... 31

使用 RFC 8784 PPK 配置后量子 IKEv2 VPN..32

使用 RFC 9242 和 RFC 9370 混合密钥配置后量子 IKEv2 VPN.....................................38

后量子 IKEv 2 RFC 8784 配置示例.. 45

量子安全概念

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

量子计算机 (QC) 会对网络和数据安全造成威胁。如果 QC 开发达到成熟状态，产生专门为破解解密而开发的加密相关量子计算机 (CRQC)，许多被认为安全的经典密码将不再能够阻止攻击者解密您的数据。这意味着基于经典加密的公钥基础设施 (PKI) 将容易受到后量子攻击。这种威胁是即时的，特别是对于长期数据，因为存在"先采集，后解密"攻击，攻击者会获取加密数据并将其存储，直到他们拥有可以解密数据的 CRQC。

抵抗基于量子计算的攻击首先要增强 IKEv2 密钥交换期间创建的密钥以保护您的 VPN，并了解您当前的加密和后量子加密 (PQC)。Palo Alto Networks 所采用的抵抗量子攻击的解决方案是基于开放标准，以实现并确保与其他符合标准的设备的互操作性。

第一步是实施 RFC 8784 来创建量子抵抗 IKEv2 VPN，如本文档所述。量子抵抗 VPN 可以阻止攻击者记录关键加密密钥材料，即使攻击者成功窃取加密数据，也无法解密数据。RFC 8784 以一种直接方式从当今传统加密技术过渡到量子抵抗，不需要加密技术升级，这是向您的 VPN 通信引入量子抵抗能力的最简单方法。

第二步是单独实现 RFC 9370 或者与 RFC 8784 一起实现来创建量子抵抗 IKEv2 VPN，这种 VPN 采用了可结合经典和 PQC KEM 技术的多种密钥交换机制 (KEM)。这种解决方案也称为 IKEv2 后量子混合密钥，使用新的替代 PQC 算法，该算法可以抵御使用 Shor 算法的量子攻击。

本章介绍了 QC、QC 对您的数据安全构成的威胁、您现在可以通过创建量子抵抗 IKEv2 VPN 采取的措施，以及如何规划和准备迁移到后量子 VPN 和 PQC。

- 量子计算威胁
- RFC 8784 如何抵御量子计算威胁
- RFC 9242 和 RFC 9370 如何抵抗量子计算威胁
- 支持后量子功能
- 量子计算威胁
- 抵抗后量子攻击的最佳实践
- 进一步了解后量子安全性

量子计算威胁

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

公钥基础设施 (PKI) 加密和 IKE 密钥交换机制广泛使用 Diffie-Hellman (DH)、椭圆曲线加密 (ECC) 和椭圆曲线 Diffie-Hellman (ECDH) 等经典加密技术。量子计算机 (QC) 可能会在 NIST 对第一个后量子加密 (PQC) 进行标准化后的 5 到 15 年内破解这些技术。

基于 RFC 8784、RFC 9242和 RFC 9370 开放标准的后量子 IKEv2 VPN 可抵抗基于量子计算和 PQC 的攻击。使用 RFC 8784 时，管理员无需在对等握手期间将密钥材料发送给 IKE 对等方，而是单独配置和共享带外密钥材料。攻击者即使窃取了数据也无法解密数据，因为他们没有密钥材料。RFC 9370 向 IKEv2 增加了额外 7 轮可选 KEM，支持创建使用不同类型 KEM 技术制定的混合加密密钥。要破解混合密钥，需要破解用于创建密钥的所有 KEM。Palo Alto Networks 所采用的抵抗量子攻击的解决方案是基于开放标准，以实现并确保与其他符合标准的设备的互操作性。

最迫切危险是“先采集，后解密”攻击，攻击者会窃取他们现在无法解密的数据（静态或传输中）并将数据存储起来，直到加密相关的量子计算机 (CRQC) 可以解密这些数据。CRQC 是一种 QC，针对使用量子算法进行了优化，CRQC 可在几秒钟内破解加密，而传统超级计算机则需要数百万年时间。风险最高的数据是长期数据，这些数据在 CRQC 问世时仍有价值。

- 什么是量子计算机？
- 量子威胁对我的网络有何影响？
- 现在如何缓解采集式攻击

什么是量子计算机？

量子计算机 (QC) 本质上是下一代超级计算平台。QC 利用量子力学定律大大减少了处理数据和运行算法（包括可以破解经典解密的算法）所需的时间。传统计算机需要数百年或数千年才能完成的操作，QC 只需要几秒钟甚至几微秒。QC 并非基于经典的位（0 和 1，线性增加超级计算机能力），而是使用 量子比特，量子比特基于偏振光子（光），可呈指数提高 QC 的处理能力。

有几种方法可以创建量子比特，该方法会影响量子比特的质量，即量子比特的效率。量子比特的质量越高，QC 就越快速、越高效。由于量子比特的量子性质，一个量子比特一次表示两种状态，并且这些状态可以远距离复制。这是由于叠加和纠缠的量子效应：

- 叠加：一个量子比特可以同时表示 1 和 0。组合量子比特会导致量子比特可以表示的状态数增加，因为状态数以 2**n 的速率增加，其中“n”是量子比特数。因此，两个量子比特可以表示 4 个状态 （2**2），3 个量子比特可以表示 8 个状态 （2**3），4 个量子比特可以表示 16 个状态 （2**4），依此类推。

  随着量子比特密度（适合芯片的量子比特数）的增加，组合量子比特可以表示的状态数也会呈指数级增加。量子比特的质量越好，量子比特的总数量就越接近真正的指数尺度。如果组合了

低质量（嘈杂）量子比特，则不会以指数方式增加状态数，但与经典计算机相比，仍会显著增加状态数。随着量子比特质量的提高，QC 越来越接近所代表状态数量的真正指数级增长。

- 纠缠：纠缠是量子比特之间的量子键。通过对纠缠量子比特运行同一个量子比特算法，无论它们位于何处（那怕量子比特彼此相距半个地球），都会生成相同结果。因此，如果对位于班加罗尔（印度）和洛杉矶（美国）的纠缠量子比特运行特定算法，则这些位置的纠缠量子比特会产生相同结果。量子纠缠工作的确切机制尚不清楚。

QC 分为三种类型：

- 量子退火器：目前已经可用。这是功能最弱的 QC，用例最为狭窄。但是，攻击者可以使用量子退火器，利用量子算法来对大数字进行分解，这就是破解非对称加密的方法。
- 模拟量子仿真器：这些仿真器解决了经典计算机无法解决的物理问题，例如量子化学、材料科学、优化问题、大数因式分解、采样和量子动力学。
- 通用量子计算机：这些是最难构建的 QC，因为它们需要许多物理量子比特。通用量子计算机解决了最广泛的用例，有几家公司的目标是在 2030 年前将其商业化。在通用量子计算机开发出来后，便将成为 CRQC。

QC 创建了一个由许多纠缠量子比特组成的多维空间，用于解决复杂问题。例如，经典计算机获取数据库的每个元素，对其进行处理，然后在处理完所有元素后将其与其他元素组合。QC 创建了一个算法，可以求解您正在寻找的每种状态和结果。QC 同时将整个数据库传递给算法，而且同时分析每个结果的数据。这使得 QC 可能比传统计算机快数百万倍，这也是它们擅长解决复杂数学问题（例如破解加密）的原因之一。

量子威胁对我的网络有何影响？

QC 的处理能力和速度大大提高，可能会破坏传统的数据加密方法，这可能会损害您的公钥基础设施（即 PKI）。

最直接的威胁是“先采集，后解密”攻击，这些攻击会窃取您的加密数据，目的是将来使用 CRQC 对其进行解密。一旦攻击者窃取了您的数据和经典密钥材料，就无法阻止他们将来使用 CRQC 解密数据。如果被窃数据到那时仍然有效，则会泄露。

经典非对称加密是基于质数，并依赖于分解复杂数字来推导这些质数的难度。名为 Shor 算法的量子算法可以分解复杂数字并解决离散对数问题。Shor 的算法威胁到 PKI 安全，PKI 是基于两个非常大的质数来生成密钥。不过如果使用经典计算机，Shor 算法破解 PKI 安全性的时间要超过一百万年。如果没有 CRQC，Shor 算法就不会构成威胁。但是，鉴于 CRQC 的处理能力，Shor 算法可以在几秒钟或更短的时间内分解复杂数字并破解经典的非对称加密（例如解密数据所需的密钥交换材料）。这就是为什么“先采集，后解密”是一个直接威胁。

破解经典加密的后果包括：损害被认为安全的经典 PKI 加密的安全性，例如 Diffie-Hellman (DH)、椭圆曲线加密 (ECC) 和椭圆曲线 Diffie-Hellman (ECDH)。密钥交换面临最大的风险，这就是为什么您需要配置后量子 IKEv2 VPN 来保护密钥交换。

证书从来都是两个端点建立信任的基础。但 CRQC 也可能破坏 RSA，而 RSA 用于创建和保护数字证书。这意味着攻击者可以使用 CRQC 窃取或冒充数字签名，这样一来，您认为要连接的服务器实际上可能是攻击者的服务器。最快在未来十年可能就能做到。

此外，QC 的纯粹暴力处理能力意味着对称加密也不安全。Grover 算法是一种量子二次加速非结构化搜索算法，用于查找生成特定输出值的唯一输入。Grover 算法以对称加密和哈希函数为目标。Grover 算法基本上会将 AES 算法的加密强度减半，因此如果您使用 AES-128 位加密，Grover 算法会将其降低到 64 位加密的加密强度。因为传统计算机没有足够的处理能力，所以无法使用 Grover 算法来破解对称加密。但如果使用 QC，则 Grover 算法可以破解 AES-128 位加密。

由于 *AES-128* 位加密容易受到 *Grover* 算法的影响，因此请使用 *AES-256* 位加密，*Grover* 算法在近期或中期将无法破解 *AES-256* 位加密。

为帮助保护哈希函数，请至少使用 *SHA-384*。

后量子加密 (PQC) 现已可用，大多数精通安全的行业人士都可以下载和设置 PQC，PQC 无法被解密。如果您在网络上允许未经授权的 PQC，则怀有恶意的内部人员可能会将 PQC 引入您的网络。如果发生这种情况，您将无法查看使用 PQC 的流量，也无法查看该流量中的威胁。使用解密功能检测网络上未经授权的 PQC，并自动阻止使用 PQC 的流量。

现在如何缓解采集式攻击

立即采取这些行动来抵抗后量子“先采集，后解密”攻击检查您的 VPN 连接并加以强化：

- 按照 *IPsec* 的 *Suite B* 加密套件的 RFC 6379，将您的 VPN 连接升级到强密码套件。使用 Suite-B-GCM-256 并避免使用较弱的 128 位 AES 算法，因为这些算法容易遭受 Grover 算法的攻击。
- 将您的 CA 升级到 4K RSA 密钥大小以缓解暴力攻击（暴力攻击可以攻破小于 4K 的密钥大小），并将您的 VPN 证书认证迁移到新证书。
- 升级到更高位数的 SHA 哈希大小，例如 SHA-384 和 SHA-512。停止使用 MD5 和 SHA-1 等弱哈希值。
- 实施 RFC 8784 和/或 RFC 9242 和 RFC 9370 来创建抵抗量子攻击的后量子 VPN。

此外，请检查您的 SSL/TLS 连接并加以强化：

- 将 SSL/TLS 连接升级到强密码套件；使用支持完全正向保密 (PFS) 密码的 TLSv1.3。
- 在强化的客户端到服务器 VPN 会话中隧道化 SSL/TLS 会话。使用后量子桌面应用程序支持反向代理。

RFC 8784 如何抵御量子计算威胁

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

通过 RFC 8784 标准“在互联网密钥交换协议版本 *2*（简称 *IKEv2*）中混合预共享密钥以实现后量子安全”，您可以创建 IKEv2 VPN，从而能够抵抗当今基于量子计算机 (QC) 和后量子密码 (PQC) 的攻击。

RFC 8784 的本质是在带外交换静态后量子预共享密钥 (PQ PPK)，与 IKE 密钥交换分开，并将带外 PQ PPK 材料与在 IKEv2 密钥交换期间在带内传输的经典 Diffie-Hellman (DH) 密钥材料混合。这从两个方面增强了密钥交换：

- DH 密钥及其变体依赖于解决离散对数问题的难度，例如求解 DH 所基于的超大质数。然而，随着加密相关量子计算机 (CRQC) 的出现，DH 密钥在基于 Shor 算法的攻击面前变得脆弱。实施 RFC 8784 可增强密钥的加密强度，因为混合密钥不再仅仅基于解决离散对数问题的难度（例如，求解超大质数），因此混合密钥很难被 Shor 算法攻破
- 监听者或中间人无法进行“先收集所有密钥材料，然后再解密”这样的操作。密钥的传统 DH 部分在 IKE 对等密钥交换过程中发送，但 IKE 对等方与 DH 密钥材料混合的 PQ PPK 绝不会在密钥交换期间传输，也绝不会在 VPN 中传输（在建立 VPN 之后），因此即使与密钥材料的 DH 部分一起发送，攻击者也无法解密穿过 VPN 的数据。

IKEv2 对等方会根据密钥 ID 而知晓使用哪个 PQ PPK。每个 PQ PPK 由两个元素组成：一个 KeyID 和一个预共享机密。预共享机密是您与带外 IKEv2 对等方共享的密钥材料。预共享机密永远不会与 DH 密钥材料一起传输，也永远不会与数据一起传输（建立 VPN 之后）。相反，一个 IKEv2 对等方的管理员要手动创建静态预共享机密，然后通过安全方式（例如通过安全电子邮件或从 Panorama 推送）将静态预共享机密传达给另一个 IKEv2 对等方的管理员。每个管理员都将预共享机密编写到其对等方的程序中，因此密钥永远不会在 IKE 连接中泄露。

密钥 ID 在密钥交换期间在带内传输，用于标识 IKEv2 对等方上的预共享机密。IKEv2 对等方使用密钥 ID 来查找预共享机密，并将其与 DH 密钥材料混合来创建新的密钥材料，该密钥材料并非基于质数，也无法通过窃听通信来窃取。

两个 *IKEv2* 对等方必须使用完全相同的密钥 *ID* 和预共享机密 *PQ PPK* 对。如果密钥 *ID* 及其关联的预共享机密不匹配，则连接会中止。如果配置多个 *PQ PPK*，则两个 *IKEv2* 对等方必须具有完全相同的一组活动密钥 *ID* 和预共享机密。（*Palo Alto Networks* 允许您配置最多十个活动 *PQ PPK*，但某些供应商只允许配置一个 *PQ PPK*，因此请务必了解对等方的能力，这一点非常重要。

这种基于标准的方法提供了一种简单的方法来阻止攻击者窃听连接和拦截密钥（如果攻击者的窃听和拦截成功，便能够在 VPN 建立之后解密通过 VPN 发送的数据），同时还能确保实现与遵守标准的其他设备的互操作性。RFC 8784 的优点包括：

- 标准已获得批准并得到多个供应商的支持。

- 不消耗额外的网络资源，几乎不会增加延迟。
- 向后兼容，因此即使在并非所有对等方都支持 IKEv2 的网络中也能使用，而且在您无法控制所有对等方的情况下也能使用。
- 密钥不再基于质数，因此不易被 Shor 算法攻破。
- 不会传输 PQ PPK，也就无法将其用于解密采集的数据。
- NIAP、NSA、德国联邦信息安全局等全球许多政府机构推荐。此外，创建长度为 32 字节或更大的强随机密钥也符合 NIST 第 5 类安全级别。确保机密强大且随机，不遵循任何模式，并且不会被字典攻击攻破。
- 您可以将 RFC 8784 与未来基于标准的功能（例如 PQC 混合密钥）进行分层。

这意味着可以更快地采用，因为只需进行很少更改，也不存在因不兼容而导致连接中断的危险。但 RFC 8784 也有一些缺点：

- 虽然将 PQ PPK 从 Panorama 推送到托管防火墙可以帮助缓解扩展问题，但如果站点数量很多的话，手动配置静态 PQ PPK 的扩展性并不好。
- 与之共享了 PQ PPK 的所有 IKEv2 管理员都必须安全保管 PQ PPK。这不仅包括您公司内部的管理员，还包括合作伙伴、供应商的管理员以及您需要与之建立对等关系的其他外部管理员。如果管理员写下 PQ PPK 而后又将其丢失或者被盗或被泄露，则会产生风险。
- 要想依靠人类来创建强大的长随机机密来抵御字典攻击和其他攻击，目前可能还很难做到。实施 Palo Alto Networks 后，您便能够自动生成强壮的长十六进制机密，而不必自己创建。

要解决 PQC 和后量子威胁，建议首先建立基于 RFC 8784 的 IKEv2 VPN。在 NIST 标准化第一个 PQC 之后，其他可以与 RFC 8784 配合使用的方法将增强对量子威胁的抵抗能力，例如 RFC 9242 和 RFC 9370。

RFC 9242 和 RFC 9370 如何抵抗量子计算威胁

在何处可以使用？	需要提供什么？
• PAN-OS	☐ PAN-OS 11.2 或更高版本：

RFC 9242 标准“互联网密钥交换协议 *2*（简称 *IKEv2*）中的中间密钥交换”使 IKEv2 能够在建立的 IKEv2 安全关联（简称 SA）中传输大量数据，以支持具有更大密钥大小的多个 PQC 密钥交换。RFC 9370 标准“互联网密钥交换协议 *2*（简称 *IKEv2*）中的多次密钥交换”允许在 SA 设置期间计算共享密钥的同时进行多次密钥交换。

在这两个 RFC 标准的共同作用下，IKEv2 能够使用经典和 PQC 密钥交换机制（简称 KEM）创建混合密钥，从而使用 Shor 算法缓解量子攻击。新的 PQC 基于不同的数学技术，已知的经典或量子攻击均无法将其攻破，采用的新技术包括：

- 格
- 基于代码
- 基于哈希
- 对称密钥
- 基于同源
- 多变体

RFC 9370 标准允许进行额外七轮密钥交换，这些轮次可以是经典或 PQC KEM，例如 ML-KEM、BIKE、HQC、Classic mcEliese 等，此外还有总共八轮的 IKEv2 默认密钥交换。

要破解混合密钥，用于创建加密密钥的所有 KEM 技术都必须出现漏洞并遭到破坏。例如，要创建能够抵御当今已知漏洞和未来量子计算机 (QC) 威胁的混合密钥，最佳实践建议同时采用经典密钥以及一个或多个使用不同数学技术的 PQC KEM。

- 默认 KEM 轮次：Diffie-Hellman (DH) Group 21
- 第一轮额外密钥交换：ML-KEM-768 (CRYSTALS-Kyber-786)
- 第二轮额外密钥交换：BIKE L3

在前面的示例中，经典 DH Group 21 为当今的前量子攻击提供了保护。依次添加两轮采用 ML-KEM-768（格）和 BIKE-L3（基于代码）的 PQC KEM，基于三种 KEM 技术创建加密密钥，并防范以后使用 Shor 算法发起的攻击。在 DH 密钥交换中添加至少两个 PQC 可以在更大程度上防止单一 KEM 失效，并且可以帮助在更长时间内抵抗量子攻击。此外，使用基于不同类型数学的 KEM 可以防止未来出现针对特定类型 PQC 的漏洞，例如基于格技术的所有 PQC。

需要多年时间才能过渡到以 PQC 为唯一关键交换机制的后量子世界，因为行业需要时间来验证新的 PQC 并获得对其安全能力的信心。在过渡期间，基于 RFC 9242 和 RFC 9370 的混合密钥将成为标准。

批准新 PQC 的标准流程将分为多个阶段，NIST 将批准每轮批准的 PQC 组。由于每个 PQC 都需要权衡性能与安全性，因此我们需要了解每个 PQC 的性能，以确定哪种技术最适合不同的安全用例。例如，随着时间的推移，经典 McEliece 已证明自身是一款非常安全的 PQC，但其高安全性的代价是使用的密钥大小，这可能会限制经典 McEliece 在 VPN 和 TLS 通信中的使用。

世界各国政府建议安全级别为 *L3* 或更高，以提供强大的安全性并抵御未来的量子计算机攻击。

在从经典加密到后量子加密的过渡期间，将需要密码敏捷性，才能快速替换任何受影响的 PQC。Palo Alto Networks RFC 9242 和 RFC 9370 后量子 KEM 解决方案提供了一套广泛 PQC，可从一开始就实现加密灵活性，使客户能够快速从 IKEv2 密钥协商中选择和移除任何支持的 PQC，无需对现有网络进行任何软件更新或更改。

PAN-OS IKEv2 支持以下 PQC：

- 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
- 经典 Mceliece 348864、348864f

RFC 9242 和 RFC 9370 的优势包括：

- 标准已获得批准并得到多个供应商的支持。
- 以动态密钥交换代替 RFC 8784 的静态 PPK，从而实现了高可扩展性。
- 支持各种 PQC KEM。
- IKEv2 具有向后兼容性，可在对等方无法支持 RFC 时进行回退。
- 混合密钥对 Shor 算法的抵抗力更强，因为不同的 PQC 技术可以一起使用。
- 可以使用 RFC 8784 进行分层，以实现量子深度防御和加密敏捷性。

RFC 9242 和 RFC 9370 的缺点包括：

- 早期的 PQC 标准化列表可能无法提供足够的 PQC，无法在 PQ 过渡开始时实现加密灵活性。
- 新的 PQC 可能需要很多年才能通过业界的严格审查并获得业界信任。
- 多个 KEM 会增加额外的开销并减慢 IKEv2 对等互连过程。
- 随着密钥大小和数据负载的增加，新的 PQC KEM 可能会导致碎片化。
- 并非所有设备都可以升级到支持 PQC KEM。
- 在 IKE_INTERMEDIATE 期间进行扩展密钥交换时，拒绝服务 (DoS) 攻击的风险可能会增加，这是因为在对发起者进行身份验证之前所需的资源增加。

- 混合密钥旨在防范收集攻击，即先保存加密信息，之后再使用加密相关量子计算机 (CRQC) 来解密加密信息。由于以下原因，混合密钥无法完全解决在主动攻击中使用量子计算机的攻击：
    - 仍使用传统方法执行身份验证，包括预共享密钥或数字签名算法。预共享密钥必须长且复杂以保证后量子安全，但预共享密钥不可扩展。使用数字签名的身份验证必须使用后量子数字签名执行。
    - PQC 旨在抵抗收集攻击，在 CRQC 问世之前，攻击连接的真实性并不重要，原因在于无法实现漏洞利用（因为这些攻击只发生在连接时）。

建议使用基于 RFC 9242 和 RFC 9370 的 IKEv2 VPN，以使用基于多种 KEM 技术的混合密钥，从而让 VPN 连接抵抗后量子威胁。利用一组广泛 PQC，可以实现加密灵活性，以防在向后量子世界过渡期间 PQC 受到损害。

支持后量子功能

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

对后量子特性和功能的支持包括 RFC、HA 以及升级和降级注意事项。后量子标准和功能的开发还处于早期阶段，同时国家、供应商和企业都在努力解决如何保护其数据免受后量子攻击的问题。随着标准的进步以及 Palo Alto Networks 平台对这些标准的支持，本主题也将更新以表明支持。

- 支持的 RFC 和互操作性
- HA 支持
- 升级和降级注意事项

支持的 **RFC** 和互操作性

Palo Alto Networks 设备完全支持 RFC 8784、RFC 9242 和 RFC 9370 开放标准。

Palo Alto Networks 设备可与支持相同标准的其他设备进行互操作，尽管某些供应商的实现方式可能会由于对 RFC 的理解而不同。例如，某些供应商可能不具备以下能力：使用 RFC 8784 配置尽可能多的后量子预共享密钥 (PQ PPK)，或者他们无法像 Palo Alto Networks 那样能够通过 RFC 9370 如此广泛的 PQC。

HA 支持

IKE VPN 的高可用性 (HA) 与引入后量子功能之前相同：VPN 隧道在故障转移后继续运行，IKE 对等方在故障转移后重新同步并刷新 IKE 密钥。

升级和降级注意事项

从不支持后量子 IKEv2 VPN 的版本升级时，该平台将提供对后量子特性和功能的支持。

降级到支持您配置的后量子功能的版本时，配置不会更改，并且后量子 IKEv2 VPN 安全性仍然存在。

降级到不支持后量子 IKEv2 VPN 功能的版本时：

- 如果没有配置后量子 IKEv2 VPN，则降级将照常进行，并且后量子 IKEv2 VPN 安全配置选项将被移除。
- 如果配置了后量子 IKEv2 VPN，则降级将被阻止，因为降级版本不支持后量子配置选项。降级被阻止时，会显示一条警告消息，通知您移除后量子 IKEv2 VPN 配置，并选择降级后要用于 VPN 的密码。

  移除后量子 IKEv2 VPN 配置并选择密码后，您可以继续进行降级。

在降级后，日志文件将保留后量子日志。

后量子迁移规划与准备

在何处可以使用？	需要提供什么？
• PAN-OS	☐ PAN-OS 11.1 或更高版本：

升级您的网络以抵抗后量子攻击需要大量的规划和准备，因为除了升级 VPN 之外，您还需要从传统加密套件过渡到后量子加密套件。这不仅仅是网络和防火墙的变化，还包括端点、应用程序、客户端应用程序等，是一套完整的端到端迁移。这需要投入大量的时间、研究和资源。需要多少投资取决于您的业务和网络。但是，较之于窃取您的最有价值资产（如财务数据、代码、PII 数据和其他可能长期存在且容易受到 “先采集，后解密” 攻击的数据）的攻击所造成的损失，这笔投资费用微不足道。

此外，世界各地的监管机构、国家安全机构（如 NSA）、政府和标准管理机构（如 NIST）都要求或即将要求政府机构以及一些商业部门（可能包括交通和关键基础设施）为后量子威胁做好准备并加以防御。准备过渡到后量子世界不是“应不应该做”的问题，而是“什么时候开始”的问题。

问题是您应该何时开始迁移？

何时开始迁移取决于您的数字资产的要求，尤其是需要保护其隐私多长时间，因为“先采集，后解密”攻击会记录加密数据，包括在 IKE 和 TLS 对等握手中传输的密钥材料，目的是在加密相关量子计算机 (CRQC) 问世时解密捕获的数据。关键问题是，您的数据需要保护多长时间？如果攻击者已经捕获了敏感数据，并且在 CRQC 投入使用时该数据仍然有效，则攻击者将能够解密被盗数据并对其内容采取行动。CRQC 最快有望在下一个十年问世。

如果您的公司是数据收集攻击的潜在目标，那么哪怕是晚一天采取行动，都会面临让攻击者日后能够解谜更多信息的风险。越早采取行动，就能越早阻止攻击者在未来解密所收集的数据。

从历史上看，过去大多数替代加密协议的努力都要在新标准制定后 5 到 20 年的时间才能完成，例如从 3DES 过渡到 AES 加密或从 SHA-1 过渡到 SHA-2 哈希函数。这包括在真实环境中严格审查新协议的时间。在 NIST 标准化后量子加密 (PQC) 之后，即使 PQC 已经经过了严格的测试，我们可能需要 5 到 10 年的实际经验和尝试破解 PQC，然后我们才能相信新的 PQC 确实坚固。

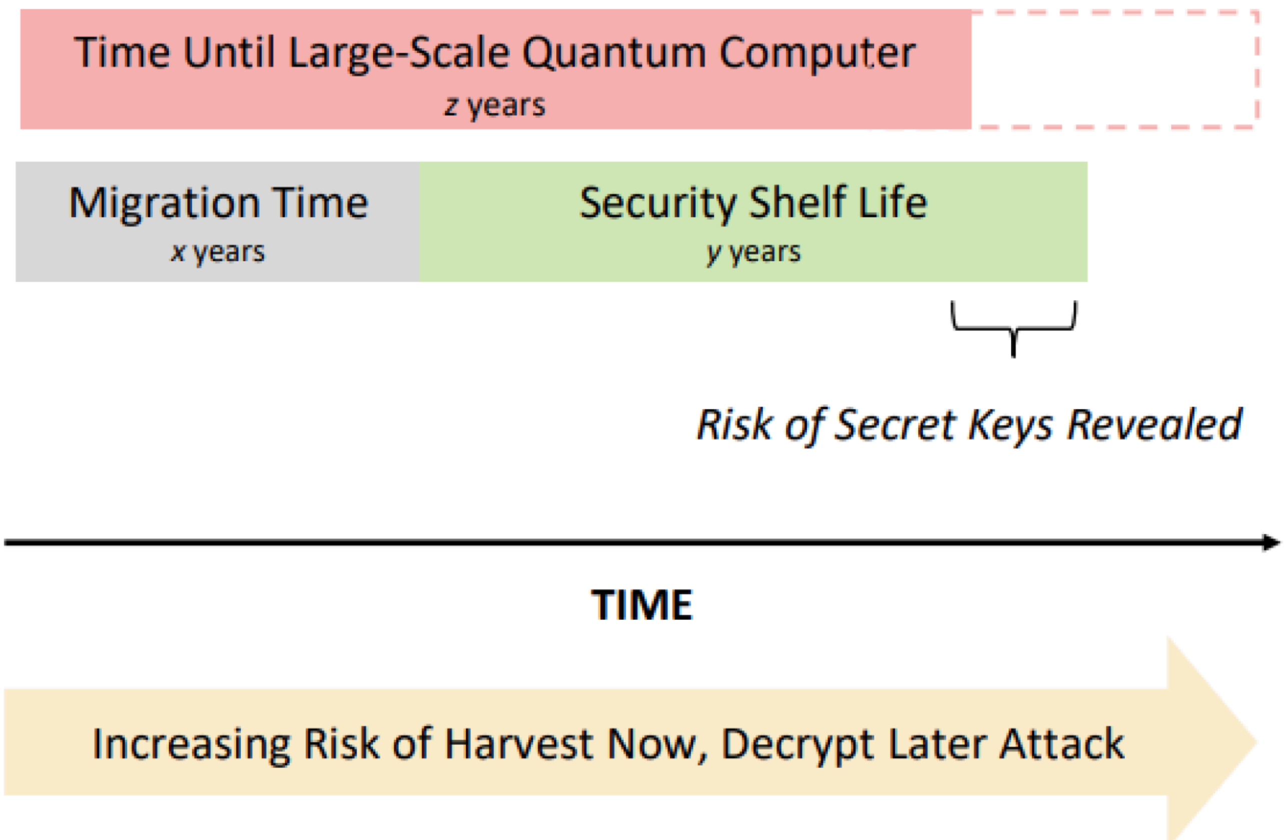
PQC 是传统加密算法的替代方法，为密钥交换、加密和数字签名提供量子抵抗能力。

为了保障从传统加密向新 PQC 的过渡，业界正在采用混合密钥。混合密钥通过使用多密钥交换机制 (KEM) 技术创建加密密钥，从而提供额外的安全性。最佳做法是使用强大的经典 KEM（例如 Diffie-Hellman Group 21）以及一个或多个 PQC。如果用于创建密钥的其中一个 PQC KEM 出现漏洞，其他 KEM 仍然可以保护该密钥。在新 PQC 获得足够的实际经验以使业界对其安全实力充满信心之前，混合密钥是最稳妥的方法。

而且“先采集，后解密”攻击也不是唯一的后量子威胁。如果您不主动阻止网络上未经授权的 PQC，怀有恶意的内部技术高手可以下载开源 PQC 并在您的网络中启动他们自己的 PQC 服务器或浏览器插件。

预计到本世纪 30 年代初期，使用当今经典密码技术保护的数据很可能无法抵抗后量子攻击。因此，请务必了解您的数据需要在多长时间内保证安全以及估算您准备和执行后量子计划需要多长时间，这一点非常重要。越早开始，就越容易保持高质量和可预测成本，也能避免在后量子威胁增大时仓促完成整个过程。

要考虑何时开始，可以采用 Mosca 模型，该模型提供了一个简单的时间表，您可以在其中插入估计时间，以便了解采取行动的紧迫性。



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.

Mosca 模型展示了如何估计您的资产对于后量子脆弱性严重程度的时间表，并帮助您了解可以在多久之后开始量子准备流程该模型将您对迁移到后量子准备就绪状态所需时间估算（*x*，可能至少为五年）加上您对数据寿命的估算（*y*，即从您实现后量子准备就绪到暴露数据不再损害数据的时间长度）与 CRQC 可能问世的时间 (*z*) 进行比较。

(*x*+*y*) 和 *z* 之间的差异显示了您的长期数据在被收集后面临泄露风险的时间，或者您的长期数据在面临风险之前有多少时间缓冲。这可以帮助您了解您需要多少时间开始或可能晚多久。如果 (*x*+*y*)

大于 z，则这些时间线之间的差异表示如果攻击者在“先采集，后解密”攻击中采集了您的数据，您的数据可能泄露的时间，如上图中所示的“机密泄露风险”。

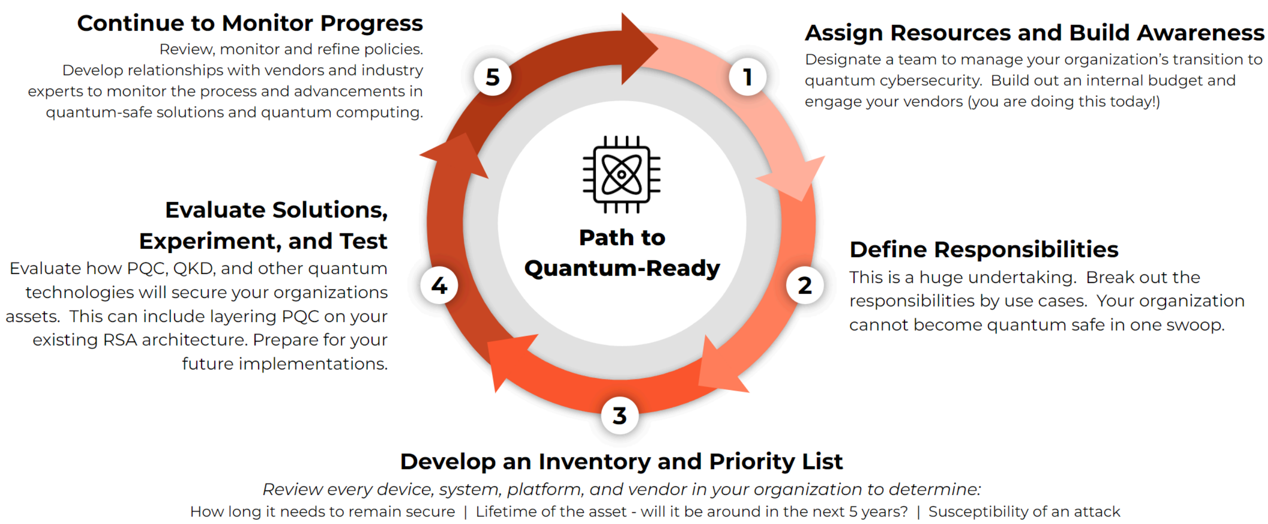
在您开始过渡规划时，您可以立即采取以下几项措施来强化现有的 VPN 连接：

- 按照 *IPsec* 的 *Suite B* 加密套件的 RFC 6379，将您的 VPN 连接升级到强密码套件。使用 Suite-B-GCM-256 并避免使用较弱的 128 位 AES 算法，因为这些算法容易遭受 Grover 算法的攻击。
- 将您的 CA 升级到 4K RSA 密钥大小以缓解暴力攻击（暴力攻击可以攻破小于 4K 的密钥大小），并将您的 VPN 证书认证迁移到新证书。
- 升级到更高位数的 SHA 哈希大小，例如 SHA-384 和 SHA-512。停止使用 MD5 和 SHA-1 等弱哈希值。
- 实施 RFC 8784 和/或 RFC 9242 和 RFC 9370 来创建抵抗量子攻击的后量子 VPN。

此外，请检查您的 SSL/TLS 连接并加以强化：

- 将 SSL/TLS 连接升级到强密码套件；使用支持完全正向保密 (PFS) 密码的 TLSv1.3。
- 在强化的客户端到服务器 VPN 会话中隧道化 SSL/TLS 会话。使用后量子桌面应用程序支持反向代理。

为了开始过渡，量子经济发展联盟 (QED-C) 开发了一个模型，用于规划和准备向后量子安全过渡，Palo Alto Networks 已将其改编为五步模型，以帮助您评估迁移准备工作、时间和资源。



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

以下各节描述了向量子过渡的准备过程的每个步骤，其中第一步是实施 RFC 8784 来创建量子抵抗 IKEv2 VPN：

- 分配资源并建立意识
- 定义职责
- 制定加密清单和优先级列表
- 评估解决方案、实验和测试

- 继续监测进展

分配资源并建立意识

在规划和准备的这一阶段，目标是确定过渡团队，了解所需的资源，接洽供应商以了解他们的后量子准备计划，并开始了解所涉及的成本。

抵抗后量子攻击的升级通常与您的 *IT* 部门为实现网络现代化而已经进行的工作相吻合。

1. 组建专门的项目管理团队，负责制定后量子战略和量子准备路线图来管理过渡。该团队负责高层规划。该团队还将确定过渡所隶属网络的负责人。尽早开始，留出足够时间采取深思熟虑、慎重的方法，帮助确保保持较高质量水平并且成本保持可预测。
2. 了解量子安全技术，并弄清楚如何将其集成到您的环境中。要创建安全后量子网络，第一步是后量子 IKEv2 VPN (RFC 8784)，您现在可以执行此操作而不会对网络造成影响。此外，所有组织都需要用量子安全的 PQC 取代其现有的非对称算法。要采取下一步措施，请了解 PQC、混合密钥和多次密钥交换（RFC9370 和 9242）。还要了解加密敏捷性（使用多个 PQC，如果其中一个 PQC 被破坏，您能够在 PQC 之间轻松快速地切换）、量子密钥分发 (QKD) 和量子随机数生成器 (QRNG)，以了解是否能证明这些安全措施可以保护您的数据。

   研究量子技术并与您的供应商接洽，以了解他们的量子准备计划以及这对您的业务有何影响。
3. 参与企业社区并了解 PQC 和技术意识和准备水平。提高团队和团队领导的意识，帮助他们理解潜在变更以及为什么需要进行这些变更。例如，与采购团队合作，在采购时纳入后量子要求，以确保新的硬件和软件与 PQC 兼容并确保基础设施面向未来。

   启动加密发现活动（您可能能够利用审计文档），以了解并识别组织目前对数字签名和加密（易受后量子攻击）的依赖程度，例如 Diffie-Hellman (DH)、椭圆曲线密码 (ECC)、椭圆曲线 Diffie-Hellman (ECDH)、AES-128、小于 4K 的 RSA 加密等等。
4. 开始内部预算制定工作。随着您的深入了解，调整预算并制定适合您的业务的最佳解决方案。

定义职责

确定网络的每个部分的负责人，包括网络、文件和数据加密、软件应用程序、端点、IAM、应用程序服务器等。为每个领域的团队成员分配职责，确保他们了解过渡的原因、紧迫性和价值。后量子漏洞将影响所有现有的非对称加密。团队成员应该明白，以优先方式发现、分类和升级网络中的所有功能需要付出巨大的努力。

制定加密清单和优先级列表

加密清单是网络中的所有组件的综合列表（即网络中的每个设备、系统、代码、应用程序、平台和供应商），以及每个使用的加密技术（即网络套件、用于 TLS、SSH 和 VPN 的版本、证书管理、加密密钥生成、密钥大小和密钥存储等）。加密清单需要全面，因为 PQC 对整个端到端数据路径构成威胁，包括所有类型的端点、应用程序和服务器。这意味着您需要规划完整的端到端迁移。

加密清单不仅列出组件，还提供每个组件的信息以及组件本身和每个组件使用的加密技术。对于每个组件，清单包括使用者、其中存储的数据、保护方式以及数据在组件之间移动方式。目标是了解

网络中使用的加密类型、加密保护的数据、数据的存储位置、数据的去向以及所涉及的设备和用户的所有信息。简而言之，全面盘点您的网络加密以及造成的任何影响。

如果没有全面的加密清单，您就无法识别网络中所有受影响的组件、评估其风险，或有效确定升级的优先顺序。

要创建加密库存，请调查并记录加密使用情况（IT 部门和安全运营 (SecOps) 部门通常可以提供帮助）：

- 使用的加密方法：当前使用的加密密码和协议。
- 什么人或什么对象使用每个密码和加密协议。
- 加密的使用场合：加密保护哪些数据、服务器、浏览器、VPN、远程应用程序等。确定谁在使用数据、数据经过网络的哪些部分以及如何实现端到端的安全保护。
- 根据每个网络元素的风险进行分类。
- 确定所需的数据隐私期限和数据的预期寿命，以帮助衡量因收集攻击而丢失数据的风险。

将供应商和合作伙伴纳入加密库存。例如，采访供应商以了解他们的应用程序中使用的加密技术、密钥的强度和生成方式。确定谁在使用数据以及如何端到端地保护数据。切勿留下攻击者可以在后量子攻击中利用的漏洞。

创建加密库存时，您也许能够利用在审计、网络增强、零信任等方面已完成的工作。

开发加密库存可能是过渡过程中最困难的部分。好消息是，库存可以提高意识，帮助组织在量子威胁出现之前提高安全性，因为库存可以识别出陈旧和过时的系统。

Palo Alto Networks 提供了多种工具来帮助您获取加密库存：

- 解密、流量和威胁日志显示您的网络上运行哪些加密协议、这些协议的设备和用户等等。
- 内容版本 8692 中的漏洞保护配置文件签名可以检测日志中的 PQC 使用情况并发出警报。您可以配置漏洞保护配置文件来自动阻止网络上未经批准的 PQC，这是最佳实践。（必要时，对内部 PEN 测试做出例外。）
- 使用 SSL 解密自动阻止防火墙无法解密的密码。

评估加密库存中各项的风险并确定您的安全选项，以便您可以确定迁移的优先顺序：

- 了解您的数据和应用程序：
  - 识别高优先级和高隐私数据。
  - 根据安全性和风险对数据进行分类。
  - 分配隐私期限（数据寿命和有效期）。
  - 了解应用程序如何保护其数据。
  - 知道谁在使用数据。

- 了解您的端点。
  - 数据存储位置以及保护方式
  - 哪些服务器托管和提供数据？
  - 用户使用来访问数据的设备
  - 保护端点的方式
- 了解您的网络。
  - 数据在网络中移动方式
  - 保护数据的设备
  - 是否涉及云？如何在云端保护数据？
  - 有哪些网络高风险区域？
- 了解您的安全选项以及需要在哪些区域应用后量子缓解措施。
  - 您需要迁移到更新的协议吗？
  - 您应该在何时使用哪种 PQC？（注意 NIST PQC 标准。）
  - 您是否需要使用混合密钥来保护您的数据？
  - 您将如何确保加密灵活性（如果在 PQC 中发现漏洞，能够快速在加密算法之间切换）。
  - 您需要使用 QRNG 或 QKD 吗？
  - 何时需要过渡到后量子证书和身份验证？
  - 这些选项是否满足您的合规性要求？

在您了解了自己的加密库存时，请分析数据并根据分析结果设置迁移优先顺序。在设定优先顺序时，请考虑数据的生命周期以防御收集攻击、数据的位置和敏感度以及数据易受攻击的程度。如今，密钥交换的风险最高，因此首要任务是实施 RFC 8784 和/或 RFC 9242 和 RFC 9370 来创建量子抵抗 VPN。

要设置迁移优先顺序：

- 根据业务影响对任务进行排名。该资产对您的业务的重要性。数据需要保持安全或私密的时间长度：资产是否会面临“先采集，后解密”攻击的风险？将风险资产的资本价值与后量子攻击造成的未来数据丢失的预计成本进行比较。
- 首先迁移影响较大的区域。
- 定义补救措施。
- 设定迁移时间表和策略。
- 投入资源和资金活动。

评估解决方案、实验和测试

利用您的加密库存中的信息，制定策略、迁移计划和测试计划，以将您的网络过渡到后量子准备就绪并保护您的数据。包括供应商、合作伙伴以及对您的网络安全产生影响的任何其他外部因素。制定解决方案策略和迁移计划：

- 确定您需要升级到 PQC 的资产。

  识别每个优先级别所需的技术并确定它们如何适应迁移策略。
- 创建一个过渡计划，确定现在以及将来您用 PQC 替换或增强传统算法时最适合保护您的资产的算法。
- 制定密钥生命周期策略来反映非对称和对称加密密钥的风险，特别是对于容易受到“先采集，后解密”攻击的长期数据。
- 在您的策略和计划中包括实施加密敏捷性。加密敏捷性确保在算法（经典或 PQC）受到威胁的情况下，您可以快速轻松地转向安全算法。

请务必明白，这是一个经过深思熟虑的过渡，而不是把一切推倒重来那样的“焦土政策”。在完全过渡到 PQC 之前，您可能需要采用混合方法并将 PQC 与传统加密算法分层以增强安全性。

为了测试计划和策略，请设置概念验证实验室，以是下以下目的：

- 彻底测试所有 PQC 组件以及设备和应用程序之间的互操作性。
- 了解经典算法和 PQC 算法之间在性能和能力方面的差异。与经典加密技术相比，PQC 的密钥和数字签名更大，这会导致加密文件的大小增大，也可能影响延迟。

  测试组件之间的 PQC 互操作性，并尝试最大化端到端量子抵抗力，不仅在组织内部中，还包括在外部各方之间。确定最适合每个用例的算法，并制定用 PQC 取代传统加密技术的过渡计划。
- 进行端到端测试，并包括合作伙伴、供应商和其他外部方，他们的后量子就绪情况可能会影响您的网络。某些系统可能需要升级才能获得可接受的后量子性能。
- 识别需要升级的不兼容组件和资产。

实验也是在组织内培养意识的另一种方式，同时可以回答问题，并提供有关转变的难易程度或挑战性的信息。如果您没有内部专业知识或无法在合理的时间范围内培养内部专业知识，请寻求外部专业知识。

继续监测进展

持续监控和评估形成量子抵抗环境的进展，以帮助确保过渡按计划进行，并降低收集攻击的风险。根据需要对计划和涉及的人员进行调整。此外，与专家合作还可以帮助确保您覆盖所有基础，并且不会留下攻击者可以在未来的量子攻击中利用的任何漏洞。

抵抗后量子攻击的最佳实践

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

您现在可以实施很多最佳实践来防御量子计算机进行的后量子攻击，包括防御“先收集，后解密”攻击。“先收集，后解密”攻击会捕获加密数据和密钥交换材料，目的是稍后使用加密相关量子计算机 (CRQC) 通过加速 Shor 算法来解密这些材料，Shor 算法可将密钥材料进行因数分解，以找出加密密钥所基于的大质数。

这些最佳实践包括：

- 后量子过渡规划最佳实践
- 加密最佳实践
- VPN 配置最佳实践

后量子过渡规划最佳实践

从古典加密转变为后量子加密可能需要五年甚至更长时间。单是规划就可能要花费几年时间。要想在最大程度上占据优势，请采取以下措施：

- 尽早开始：如果您的公司数据需要长期保存并且可能是收集攻击目标，那么哪怕是晚一天采取行动，都会面临让攻击者“先收集，后解密”的攻击得逞的风险。越早采取行动，就能越早阻止攻击者发起的“先收集，后解密”攻击。
- 利用现有资源：在获取加密库存后，请利用您已在审计、零信任、网络增强和其他活动方面已经完成的工作。
- 自学：了解量子计算威胁、后量子加密 (PQC)、强化可抵御量子攻击的网络的技术和方法以及可用于保护网络的新兴 PQC。从政府法令、规律、法律、征求意见稿 (RFC) 以及其他信息来源学习。

加密最佳实践

随着量子计算机进化为 CRQC，其速度越来越快，因此需提高经典加密套件的强度，提高攻击者暴力破解密钥的难度。非 CRQC 的量子计算机的速度可能就足以破解较弱的加密。

- 按照 *IPsec* 的 *Suite B* 加密套件的 RFC 6379，将您的 VPN 连接升级到强密码套件。使用 Suite-B-GCM-256 并避免使用较弱的 128 位 AES 算法，因为这些算法容易遭受 Grover 算法的攻击。
- 将您的 CA 升级到 4K RSA 密钥大小以缓解暴力攻击（暴力攻击可以攻破小于 4K 的密钥大小）。
- 将您的 VPN 证书认证迁移到具有更大密钥大小的新证书。
- 升级到更高位数的 SHA 哈希大小，例如 SHA-384 和 SHA-512。停止使用 MD5 和 SHA-1 等弱哈希值。

- 将 SSL/TLS 连接升级到强密码套件；使用支持完全正向保密 (PFS) 密码的 TLSv1.3。
- 在强化的客户端到服务器 VPN 会话中隧道化 SSL/TLS 会话。
- 配置您的漏洞防护配置文件，以针对未解密的流量阻止未经批准的 PQC。对于您解密的流量，使用解密配置文件来阻止未经批准的 PQC（解密配置文件仅允许您启用的密码，而防火墙会阻止所有其他密码）。未经批准的 PQC 表明可能存在违规行为或内部不良行为者可能试图使用 PQC 来破坏您的网络。根据需要为内部 PEN 测试团队做出例外处理。

VPN 配置最佳实践

配置后量子 IKEv2 VPN 时，尽可能使其能够抵量子抵抗攻击：

- 实现 RFC 8784 来创建可抵抗量子攻击的 IKEv2 VPN。
- 实现 RFC 9242 和 RFC 9370 来创建可抵抗量子攻击的IKEv2 VPN。

RFC 8784 可与 *RFC 9242* 和 *RFC 9370* 一起使用以提供额外的保护层，这样便可以满足加密灵活性要求。

RFC 8784 最佳实践：

- 切勿使用 IKEv1。IKEv1 被认为是一种弱协议，不支持后量子 VPN。如果两个 IKE 对等设备都可以支持后量子 VPN，请将您的 VPN 连接升级到 IKEv2，并在配置 IKE 网关（**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关） > **General**（常规））时选择 **IKEv2 only mode**（仅 **IKEv2** 模式）。
- 如果您已知道两个对等设备均支持 RFC 8784，请将 **Negotiation Mode**（协商模式）设置为 **Mandatory**（强制）。使用 **Mandatory**（强制）模式可确保 VPN 能够抵抗后量子攻击，攻击者也无法使用运行 Shor 算法的 CRQC 来发起“先收集，后解密”。

  只要有足够的处理能力，*Shor* 算法就可以破解 *IKEv2* 握手中使用非对称加密的动态密钥交换。然而 *Shor* 算法无法破解 *IPSec* 隧道对称加密。为了保护对称 *IPSec* 加密，请使用 *AES-256* 来防御 *Grover* 算法，并使用上一节加密最佳实践中推荐的更强哈希值和密钥长度。

  与外部设备对等连接时，尝试确定对等设备是否支持 RFC 8784，并与其他管理员合作以将同一个 PQ PPK 用于连接，以便您可以使用强制模式。
- 手动指定或自动生成一个 PPK 机密，其长度至少为 64 个字符（32 个字节或 256 位熵）以创建强密钥。您可以手动指定或自动生成最大长度为 128 个字符（64 字节，512 位熵）的 **PPK** 机密。PPK 机密越长，熵位数越多，PPK 机密的破解也就更难。

  熵位数提供的安全性是后量子位数的一半。例如，256 位熵可提供 128 位后量子安全性，512 位熵可提供 256 位后量子安全性。要提供与 NIST 后量子加密提案征集中所定义的第 5 类相同的安

全性，至少需要 256 位的熵。RFC 8784 的安全注意事项章节详细介绍了熵的概念以及多少位的熵才够用。

仅当 *PPK* 机密是由您配置或自动生成时才会以明文显示。在您配置或生成 *PPK* 机密并离开以明文显示机密的屏幕后，该机密再也不会以明文显示，这样有助于防止密钥泄露。

请复制 *PPK* 机密/*KeyID* 对并妥善存储。如果您在配置或生成密钥后没有存储，那么以后无法检索。（如有必要，可以删除 *PQ PPK* 并配置另一个。）

处理 PQ PPK 的其他最佳实践包括：

- 创建多个活动的 PQ PPK。使用多个活动密钥（而非仅使用一个）能为密钥交换期间的密钥选择增加了随机性。
- 确保每个 IKEv2 对等设备都有完全相同的一组激活 PQ PPK（KeyID 加 PPK 机密对）来协商密钥交换。
- 如果由 Panorama 管理对等设备，请配置 PQ PPK 并将其推送至托管防火墙，以让配置更轻松、更快捷、更加自动化。
- 如果您需要将 PQ PPK 传达给另一位管理员，请使用加密安全通信方法，例如加密电子邮件。
- 请安全存储 PPK 机密字符串。请勿将其写在便签上或是任何未经授权的管理员可能发现的地方。

NSA 发布了有关如何安全处理预共享密钥的指南，包括 *RFC 8784* 量子预共享密钥。

RFC 9242 和 **RFC 9370** 最佳实践：

- 切勿使用 IKEv1。IKEv1 被认为是一种弱协议，不支持后量子 VPN。如果两个 IKE 对等设备都可以支持后量子 VPN，请将您的 VPN 连接升级到 IKEv2，并在配置 IKE 网关（**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关） > **General**（常规））时选择 **IKEv2 only mode**（仅 **IKEv2** 模式）。
- 在配置 IKE 加密配置文件（**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密） > **General and Advanced Options**（常规选项和高级选项））时，请使用强经典 KEM（例如 Diffie-Hellman Group 20 及以上）以及其他 KEM 轮次中的至少一个 PQC（例如 Kyber-768 (ML-KEM)）创建混合密钥。
- 对于敏感信息，只能使用安全强度级别为 L3 或更高的 PQC。在密钥创建过程中添加的每个额外 PQC 都会提高密钥抵抗量子攻击的能力，但也会增加 IKEv2 对等连接过程的延迟和开销。一般来说，添加安全级别 L3 PQC 会使 IKEv2 密钥交换延长约 20 到 30 毫秒，而添加安全级别 L5 PQC 会使 IKEv2 密钥交换延长约 40 到 60 毫秒。更强的 PQC（其使用的密钥也更大，例如 Classic McEliese）可能会让密钥交换延长 800 多毫秒，并引入高度的碎片化。熟悉 PQC 密钥大小和安全强度，以便为您的 VPN 通信选择最佳 PQC。
- 与负责管理对等 VPN 设备的管理员协调每轮密钥协商中使用的 PQC。当隧道两侧的 VPN 设备在每轮可选密钥协商中都配置为相同 PQC 时，会最大程度上减少互操作性问题。尝试就 PQC

及其安全强度达成一致，以确保双方配置的参数相同。若防火墙是由同一个组织管理，则可以使用中央管理工具来确保在每一轮密钥协商中配置和PQC选择一致。

- 在过渡到纯 PQC 环境期间，请启用加密灵活性来保护您的数据。可能需要 5 到 10 年的过渡时间才能让行业完全信任新的 PQC。
  - 若组织必须使用由 NIST 标准化且经 FIPS 批准的 PQC，可以通过启用 RFC 8784 与 RFC 9242 和 RFC 9370 来实现加密灵活性。如果混合密钥中使用的 PQC 出现漏洞，RFC 8784 中使用的 PPK 字符串仍然可以提供量子抵抗，以防止收集攻击成功。
  - 若组织允许同时使用 NIST 标准化和非标准化 PQC，则可以使用至少两个具有强经典 KEM 的 PQC（例如 Diffie-Hellman Group 21）来实现加密灵活性。理想情况下，PQC KEM 应该使用不同的数学技术，其中一个 KEM 基于格，另一个 KEM 则是基于代码或其他非格技术。或者，还可以使用混合密钥启用 RFC 8784，以增加额外的安全性并扩展加密灵活性。
- 将密钥生存期值从其默认值降低为更低的值，以便于更快地重新生成密钥。
- 在配置 IPSec 加密配置文件（**Network**（网络） > **Network Profiles**（网络配置文件） > **IPSec Crypto**（**IPSec** 加密） > **General and Advanced Options**（常规选项和高级选项））时启用 IPSec 以使用混合密钥。IPSec 隧道的两侧必须配置为在每一轮附加密钥交换中使用相同 PQC 和安全强度。

进一步了解后量子安全性

后量子安全、后量子技术和推荐的后量子实现尚处于起步阶段。如果您有打算在后量子计算世界中保护您的资产，请务必尽可能详细了解后量子技术、影响您业务的政府法规和规定，以及如何过渡到后量子 VPN 和密码。

美国政府以及世界各国政府正在制定计划，以应对量子计算机和后量子加密构成的量子安全威胁。此外，美国国家标准与技术研究院 (NIST) 和互联网工程任务组 (IETF) 等标准机构正在为新的后量子技术及其实施方式制定标准。

本主题提供了一些参考信息的链接，可帮助您更深入地了解、准备后量子安全性并在业务中过渡到后量子安全性。

- 美国政府
- 全球各地的其他政府
- RFC
- 技术和一般信息

美国政府

许多国家的政府正在制定计划、授权和法律，以应对量子计算威胁和后量子加密的出现。以下链接提供了有关美国政府如何解决该问题的参考信息，包括美国国家标准与技术研究院 (NIST) 和美国国家安全局 (NSA) 提供的参考信息的链接。查看当地政府的安全站点和组织，了解您的政府如何实现后量子安全。

- NIST 后量子加密资源中心提供有关后量子加密标准化和其他材料的信息。
- NIST 下属的美国国家网络安全卓越中心（简称 NCCOE）迁移到后量子加密提供迁移到后量子加密的指南。
- NSA 下属的中央安全局发布的对称密钥管理要求附录 *V2.1* 提供对涉密商业解决方案（简称 CSfC）使用预共享密钥的实施要求。
- 美国国土安全部后量子加密网站包括该部门的后量子路线图和其他资源。
- 美国网络安全和基础设施安全局（简称 CISA）发布的后量子加密计划与其他政府机构和行业合作伙伴合作推动后量子工作，以应对量子计算威胁。该网站还提供了 CISA、NIST 和美国国土安全部发布的更多资源的链接。
- 为了鼓励美国联邦政府信息技术系统迁移到量子抵抗加密技术，拜登总统签署了量子计算网络安全法案 (HR 7535)。
- 美国总统执行办公室发布的执行备忘录 M-23-02和迁移到后量子加密为美国各机构就遵守国家安全备忘录 10 (NSM-10)、关于促进美国在量子计算领域的领导地位，同时降低易受攻击加密系统的风险的国家安全备忘录提供了指引。

全球各地的其他政府

以下链接提供了有关全球多个政府如何应对此问题的信息。

- 德国联邦信息安全局 (BSI) 提供有关后量子加密、迁移策略、当前发展和建议以及其他材料的信息。
- 英国政府提供有关量子计算机和技术、量子计算机威胁、国家量子战略、量子密钥分发、量子随机数生成和其他材料的信息。
- 法国网络安全局 (ANSSI) 提供有关后量子转换、量子密钥分发和其他材料的信息。
- 荷兰情报和安全总局 (AIVD) 提供有关量子计算机威胁、后量子迁移策略和步骤、量子密钥分发和其他材料的信息。
- 欧盟网络安全局 (ENISA) 提供有关后量子加密、混合实现、后量子策略和其他材料的信息。
- 新加坡金融管理局提供有关量子计划和解决与量子相关的网络安全风险的信息。
- 日本政府提供有关量子策略、量子安全性和迁移到量子技术的信息。

RFC

征求意见稿 (RFC) 介绍了 Internet 的技术基础。几个 RFC 介绍了 IKEv2 抵抗量子计算机攻击的各个方面：

- RFC 8784 "在 *Internet* 密钥交换协议版本 *2 (IKEv2)* 中混合预共享密钥以实现后量子安全性" 介绍了 IKE 扩展的标准，这一扩展使 IKEv2 能够抵抗来自量子计算机的攻击。RFC 8784 如何抵御量子计算威胁总结了 RFC 8784 对您的网络的影响。
- RFC 6379 "适用于 *IPsec* 的 *Suite B* 加密套件" 介绍了您应该使用 Suite-B-GCM-256 位算法，以取代较弱的 AES-128 位加密。取缔 AES-128 等弱密码有助于延迟 Grover 算法 可能破解对称加密的时间。
- RFC 9370 "互联网密钥交换协议版本 *2 (IKEv2)* 中的多次密钥交换" 介绍了如何扩展 IKEv2 以允许混合多次密钥交换，从而创建加密密钥。
- RFC 9242 "互联网密钥交换协议版本 *2 (IKEv2)* 中的中间交换" 定义了一种中间交换机制，该机制允许在初始密钥交换中传输大量数据，例如基于多个密钥交换的加密密钥。这有助于避免碎片。（某些设备不允许碎片。）
- RFC 7383"*Internet* 密钥交换协议版本 *2 (IKEv2)* 消息分片" 允许在 IKE 级别对 IKE 消息进行分段，从而消除 IP 分段导致的问题。但 RFC 7383 不适用于初始交换。RFC 9242 有助于避免初始交换中出现碎片，RFC 7383 可避免后续 IKEv2 消息中的 IP 碎片。

技术和一般信息

许多组织已经认识到量子计算机和相关技术带来的潜在威胁，这些技术在经典计算机上运行时不会造成危险，但在加密相关量子计算机 (CRQC) 上运行时可能会造成灾难性危险。

- Open Quantum Safe 组织的 liboqs 站点是一个量子安全加密算法的开源 C 库。
- Linux 基金会的后量子加密联盟项目通过生成标准化算法的高可靠性软件实现来寻求解决量子计算带来的加密安全挑战。
- Shor 算法与 CRQC 一起使用时，可能会攻破当今使用的许多经典非对称加密算法。Shor 的算法将很大的复杂数字进行分解，以得出质数，这些质数是经典非对称加密的基础。

- Grover 算法是一种量子二次加速非结构化搜索算法。Grover 算法与 CRQC 一起使用时，可以通过暴力破解经典的对称加密算法，将 AES 算法和哈希函数的加密强度降低一半。
- 先采集，后解密攻击是当前盛行的威胁。在“先采集，后解密”攻击中，攻击者会窃取了他们现在无法解密的数据并将其存储起来，直到 CRQC 可以解密。这些攻击眼下就在发生，这对长期数据构成直接威胁。
- Quantum Inspire 知识库文章什么是量子比特解释量子比特的概念。
- Deloitte 文章量子对于加密的威胁讨论了您为何应该尽快开始过渡到后量子，福布斯文章量子对于加密的威胁：不要惊慌，现在就做好准备也探讨这方面。
- *ETSI* 量子安全加密 *(QSC)*：量子安全迁移的可重复框架为创建后量子迁移计划提供了一个不错的模板。
- 世界经济论坛量子经济蓝图提供了以公平方式构建量子生态系统的路线图，以实现向量子经济过渡。

配置量子抵抗 IKEv2 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.1 或更高版本：

量子抵抗 IKEv2 VPN 是基于 RFC 8784 和/或 RFC 9242 和 RFC 9370，可阻止试图发起“先收集，后解密”攻击的攻击者窃取用于加密 VPN 中数据的加密密钥材料。如果没有加密密钥，攻击者以后就无法使用加密相关量子计算机来解密收集的数据。即使攻击者成功窃取了加密的数据，如果没有加密相关量子计算机来解密密钥材料，他们也无法损害收集的数据，因为他们没有密钥就无法解密这些数据。

RFC 8784 提供了量子抵抗过渡功能，可让您从目前的经典加密过渡到目前可以实现的后量子加密。RFC 8784 不需要加密升级，因此只要隧道两端的两台 VPN 设备都能支持，其就能简单快速地实现。

与 RFC 8784 相比，RFC 9242和RFC 9370的资源密集度更高，但提供了基于新的 PQC 数学算法的动态密钥生成能力，并且可以抵御 Shor 算法的攻击。由于 RFC 9242 和 RFC 9370 需要加密升级，因此部署混合密钥技术可能需要更长时间，因此您需要考虑加密灵活性。

本章向您介绍如何配置后量子 IKEv2 VPN，包括分别在以下两种情况下如何配置后量子 IKEv2 VPN：您了解 IKEv2 对等方及其功能；您无法控制 IKEv2 对等方也不知道其功能。

- 使用 RFC 8784 PPK 配置后量子 IKEv2 VPN演示了使用后量子预共享密钥保护 VPN 通信的后量子 IKEv2 VPN 配置步骤和选项。
- 使用 RFC 9242 和 RFC 9370 混合密钥配置后量子 IKEv2 VPN演示了使用混合密钥保护 VPN 通信的配置步骤和选项。
- 后量子 IKEv 2 RFC 8784 配置示例提供了一个简单的拓扑示例，并介绍了如何为该拓扑配置后量子 IKEv2 VPN 支持。

除了配置基于 *RFC 8784* 的后量子 *IKEv2 VPN* 外，请按照适用于 *IPsec* 的 *B* 加密套件的 RFC 6379，将您的 *VPN* 连接升级到强密码套件，将您的 *CA* 升级到 *4K RSA* 密钥大小以缓解暴力攻击（暴力攻击可能会攻破较小密钥大小），将您的 *VPN* 证书身份验证迁移到新证书的暴力攻击，并升级到更高位的*SHA*哈希大小，例如 *SHA-384* 和 *SHA-512*。

使用 RFC 8784 PPK 配置后量子 IKEv2 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	☐ PAN-OS 11.1 或更高版本：

基于 RFC 8784 的后量子 IKEv2 VPN 的工作原理如下：在初始对等交换（IKE_SA_INIT 交换）中单独（带外）传输预共享机密。对等交换仅传输密钥 ID，而不会传输预共享机密，在后一种情况下，攻击者可以进行破坏或是“先收集，后解密”。密钥 ID 和预共享机密组成一个唯一的对，称为后量子预共享密钥 (PQ PPK)。

每个 IKEv2 对等方使用密钥 ID 来查找预共享机密，该机密在管理员之间安全传输（或由 Panorama 推送），并在每个 IKEv2 对等上以本地方式存储。在对等交换过程中，绝不会交换预共享密钥，而且预共享密钥也绝不会穿过后量子 VPN，因此使用量子计算机的攻击者无法窃取和破解预共享密钥，也无法用它来解密从 VPN 收集的数据。

两个 IKEv2 对等方必须具有相同且成对的活动密钥 ID 与预共享密钥，这样当对等协商连接时，每个对等方都可以查找相同的密钥 ID 并检索相同的预共享密机密。如果响应对等方没有匹配的密钥 ID，或者与密钥 ID 关联的预共享机器与发起方不同，则连接将中止。

在配置后量子组件之前，先设置 IKEv2 对等和 IPSec 隧道。此外，还要确保您的安全策略允许防火墙之间的 *IKEv2* 和 *IPSec* 流量并启用日志记录。

要让您的 IKEv2 VPN 能够抵抗量子攻击，请采取以下步骤：

STEP 1 | 选择 **Network**（网络） > 网络配置文件（**Network Profiles**） > **IKE** 网关（**IKE Gateways**），然后选择 **Add**（添加）以添加新网关。

STEP 2 | 配置 **General**（常规）选项卡设置，然后针对 **Version**（版本）选择 **IKEv2 only mode**（仅 **IKEv2**模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式）。

在仅 **IKEv2**模式下，如果对等方不支持 IKEv2，防火墙将中止连接。在**IKEv2** 首选模式下，如果对等方不支持 IKEv2，防火墙将回退到 IKEv1。但 VPN 必须协商 IKEv2 才能使用后量子 VPN 功能，因此如果防火墙回退到 IKEv1，则后量子 VPN 功能将不可用。

IKEv1 被认为比较弱。如果两个 *IKE* 对等方都能支持 *IKEv1*，请将您的 *VPN* 连接升级到 *IKEv2* 并选择 ***IKEv2 only mode***（仅 ***IKEv2***模式）以确保安全级别足够且能够使用 *PQ VPN*。

STEP 3 | 选择 **Advanced Options**（高级选项）并配置非量子选项。

如果对 **Version**（版本）选择 **IKEv2 preferred mode**（**IKEv2** 首选模式），则会出现 **IKEv1** 和 **IKEv2**选项卡；请选择 **IKEv2**。如果对 **Version**（版本）选择 **IKEv2 only mode**（仅 **IKEv2** 模式），则仅显示 IKEv2 选项。

选择 **PQ PPK**（后量子预共享密钥）来配置 IKEv2 VPN 的后量子元素。（**General**（常规）可用于添加 IKE 加密配置文件以及设置 **Liveness Check**（活性检查）。）

STEP 4 | 启用后量子预共享密钥 **(PPK)** 以在 VPN 上使用后量子抵抗功能。该选项在默认情况下已禁用。

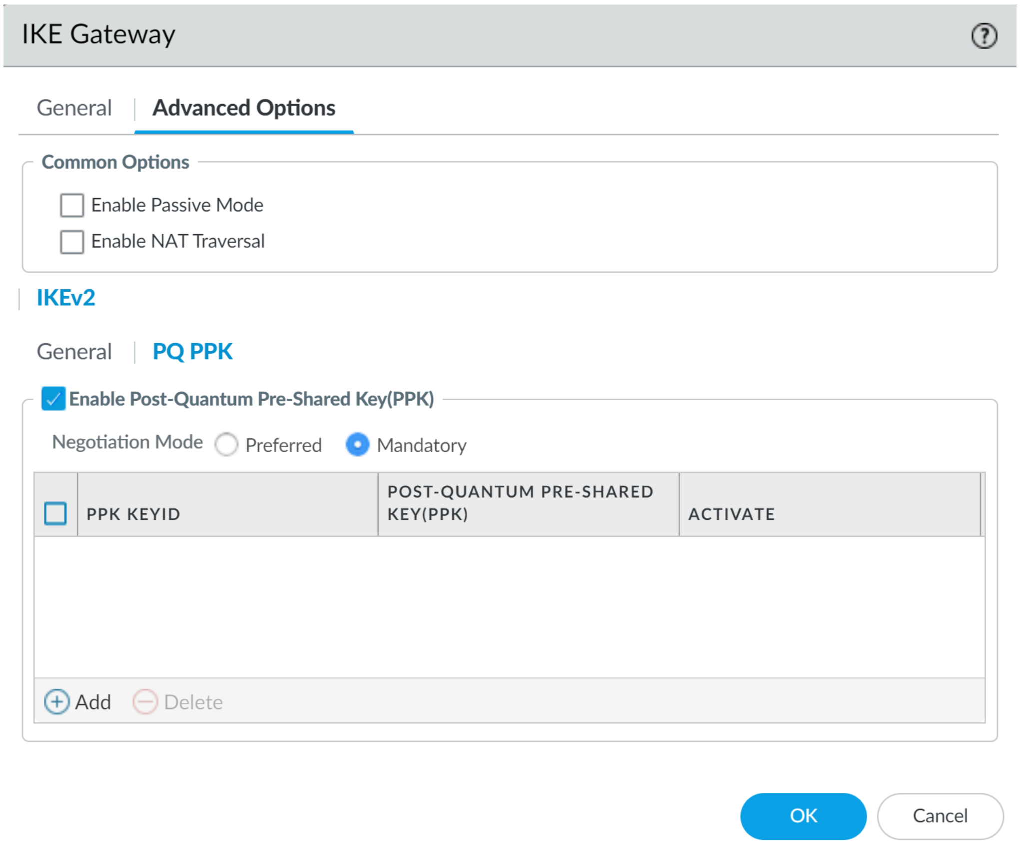
> 启用后量子预共享密钥 ***(PPK)*** 时必须配置并激活至少一个 *PQ PPK*，以确保防火墙在 *IKEv2* 协商期间有一个 *PQ PPK* 可用，并且可以支持 *RFC 8784*。

STEP 5 | 将 **Negotiation Mode**（协商模式）设置为 **Preferred**（首选）或 **Mandatory**（强制）。

- **Preferred**（首选）：当防火墙与对等方协商时，防火墙首先尝试使用 PQ PPK 进行协商。如果对等方不支持 RFC 8784，防火墙将回退到传统密钥交换以进行连接。如果您不知道或无法控制对等方是否支持 RFC 8784，**Preferred**（首选）模式将保留向后兼容性以确保连接能够回退，而不会断开。默认模式为 **Preferred**（首选）。

- **Mandatory**（强制）：当防火墙与对等方协商时，对等方必须支持 RFC 8784 PQ PPK。如果响应对等方不支持 RFC 8784，则防火墙将中止连接。如果您知道对等方支持 RFC 8784 PQ PPK，则使用 **Mandatory**（强制）模式。

为获得最佳安全性，请尽可能使用 ***Mandatory***（强制）模式。



STEP 6 | 添加并激活最多十个唯一 PQ PPK。

一个 PQ PPK 由两个成对元素组成：PPK KeyID 和 PPK 机密。PPK KeyID 是一个用于标识 PPK 机密的唯一字符串，可以是任意长度，最多 31 个字符，例如 **`PPK-1`** 或 **`Super Strong PPK`**。PPK 机密是随机预共享密钥，从不通过 VPN 传输，因为对等方双方的管理员都使用安

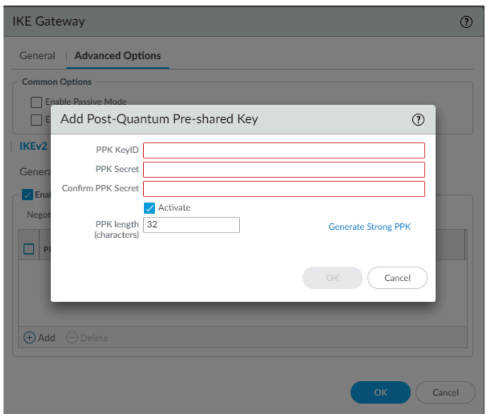
全通信方法来共享密钥，并在带外对等方上配置 PPK 机密。防火墙仅在 IKEv2 VPN 中传输 KeyID，以便对等方可以在本地查找 PPK 机密。

您可以定义的 PQ PPK 数量取决于 IKE 对等方可以支持的数量。一些供应商的实现方式允许少于十个唯一的 PQ PPK；一些实现方式甚至只允许一个。切勿定义超过对等方可以支持的 PQ PPK 数量，因为两个对等方的可用 PQ PPK 数量必须完全相同。

为支持多个 *PQ PPK* 的对等方配置多个活动 *PQ PPK*。防火墙从活动 *PQ PPK* 中随机选择，这为 *IKEv2* 协商增加了随机性元素。

配置多个 PQ PPK 是最安全的，因为这为 PQ PPK 选择增加了随机元素。

您可以手动创建 PPK 密钥，也可以使用防火墙为您生成强密钥。如果您想自己生成密钥，或者您从对等方的管理员那里获得了 PQ PPK 并且需要在防火墙上进行配置，请手动配置 PPK 密钥。PPK 机密越长，熵位数越多，PPK 机密的破解也就更难。



要手动配置 PPK 密钥，您可以使用 ASCII 字符指定：

1. 指定一个唯一 **PPK KeyID**，最多 31 个字符。
2. 指定一个唯一随机 **PPK** 机密字符串。该字符串可以是 32 到 128 个字符（16 到 64 个字节，相当于 128 到 512 位熵）。

   要创建强密钥，请指定长度至少为 *64* 个字符（*32* 个字节或 *256* 位熵）的 ***PPK*** 密钥。
3. 在 **Confirm PPK Secret**（确认 **PPK** 机密）中指定完全相同的字符串。

   安全存储 *PPK* 机密。*PPK* 机密不会以明文显示，因此如果您现在不存储，以后便无法再检索。（如有必要，可以删除 *PQ PPK* 并配置另一个。）由于 *IKEv2* 对等方必须具有相同 *PQ PPK*（*KeyID* 加 *PPK* 机密），因此您可能需要将 *PPK* 密钥传达给另一个管理员。如果需要传达，请确保所使用的通信方法是加密安全的，并确保 *PPK* 密钥已安全存储。

   NSA 发布了有关如何安全处理预共享密钥的指南，包括 *RFC 8784* 量子预共享密钥。

4. 默认选择 **Activate**（激活），以便防火墙可以使用 PPK KeyID/PPK 机密对 (PQ PPK) 与对方进行协商。如果您不希望防火墙在与对端协商时使用此 PPK KeyID/PPK 机密对，请取消选中 **Activate**（激活）。

   例如，如果您在防火墙上配置了新的 PQ PPK，则可能需要将其停用，直到对等方的管理员可以将相同 PQ PPK 添加到对等方，以避免由于发起者使用尚未在对等方上安装的 PQ PPK 而导致连接失败。

5. 单击 **OK**（确定）。**PQ PPK** 选项卡以明文显示PPK KeyID，隐藏预共享密钥，并显示PQ PPK 的激活状态。

要使用防火墙的自动强 PPK 生成（使用十六进制字符）配置 PPK 密钥：

1. 指定一个唯一 **PPK KeyID**，最多 31 个字符。
2. 将 **PPK length (characters)**（**PPK** 长度（字符））设置为您想要为 **PPK** 机密生成的长度。默认值为 32 个字符（16 个字节）。

   要生成强密钥，请将 ***PPK length (characters)***（***PPK*** 长度（字符））设置为至少 *64* 个字符（*32* 字节或 *256* 位熵）。

3. 单击 **Generate Strong PPK**（生成强 **PPK**）。防火墙将生成并显示一个强 PPK 密钥，其长度如 **PPK length (characters)**（**PPK** 长度（字符））中所指定。

   这是唯一一次以明文显示 *PPK* 机密。如果您此时没有安全地存储机密，以后便再也无法检索。（如有必要，可以删除 *PQ PPK* 并配置另一个。）由于 *IKEv2* 对等方必须具有相同 *PQ PPK*（*KeyID* 加 *PPK* 机密），因此您可能需要将 *PPK* 密钥传达给另一个管理员。如果需要传达，请确保所使用的通信方法是加密安全的，并确保 *PPK* 密钥已安全存储。

   复制 PPK 机密，单击 **OK**（确定），然后将其粘贴到 **PPK Secret**（**PPK** 机密）和 **Confirm PPK Secret**（确认 **PPK** 密钥）字段中。

4. 默认选择 **Activate**（激活），以便防火墙可以使用 PPK KeyID/PPK 机密对 (PQ PPK) 与对方进行协商。如果您不希望防火墙在与对端协商时使用此 PPK KeyID/PPK 机密对，请取消选中 **Activate**（激活）。

   例如，如果您在防火墙上配置了新的 PQ PPK，则可能需要将其停用，直到对等方的管理员可以将相同 PQ PPK 添加到对等方，以避免由于发起者使用尚未在对等方上安装的 PQ PPK 而导致连接失败。

5. 单击 **OK**（确定）。**PQ PPK** 选项卡以明文显示PPK KeyID，隐藏预共享密钥，并显示PQ PPK 的激活状态。

STEP 7 | 单击 **OK**（确定）以创建 VPN。

STEP 8 | **Commit**（提交）配置。

后量子 IKEv 2 RFC 8784 配置示例主题提供了一个简单拓扑的示例，并介绍了如何为该拓扑配置后量子 *IKEv2 VPN* 支持。

STEP 9 | 如果您不是双方 IKEv2 对等方的管理员，请将 PQ PPK（KeyID 加 PPK 机密）安全地传达给对等方的管理员，以便在对等方上进行安装。安全的 PQ PPK 通信和存储对于保护您的数据至关重要。

> 两个 *IKEv2* 对等方的活动密钥 *ID* 和相关预共享机密必须相同才能建立后量子 *VPN* 连接。

使用 RFC 9242 和 RFC 9370 混合密钥配置后量子 IKEv2 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	❑ PAN-OS 11.2 或更高版本：

基于 RFC 9242 和 RFC 9370 的后量子 IKEv2 VPN 的工作原理如下：在初始对等交换（IKE_SA_INIT 交换）中使用两个或多个密钥交换机制 (KEM) 创建混合密钥来工作。混合密钥可防止受损的 KEM 允许使用“先收集，后解密”（简称 HNDL）的量子攻击成功，从而提供量子抗性。只要用于创建混合密钥的所有 KEM 均未受到破坏，数据就会仍然受到保护。

由于该标准仍然相对较新，并且每个供应商对其实施的标准可能有不同的理解，因此保持双方的配置相同将有助于简化操作并使后量子 VPN 隧道成功建立。为最大限度减少互操作性的可能性，请确保 VPN 隧道两侧在每轮可选的密钥协商中配置相同的 PQC 和安全强度。还请检查双方的 IKEv2 分段设置，确保配置正确。

请在配置后量子组件之前设置 IKEv2 对等和 IPSec 隧道。此外，还要确保您的安全策略允许防火墙之间的 *IKEv2* 和 *IPSec* 流量并启用日志记录。

为了确保数据长期受到保护，应使用两个以上的 KEM，并且可同时启用预共享密钥（通过 RFC 8784）和混合密钥（通过 RFC 9242 和 RFC 9370）来进一步增加纵深防御。

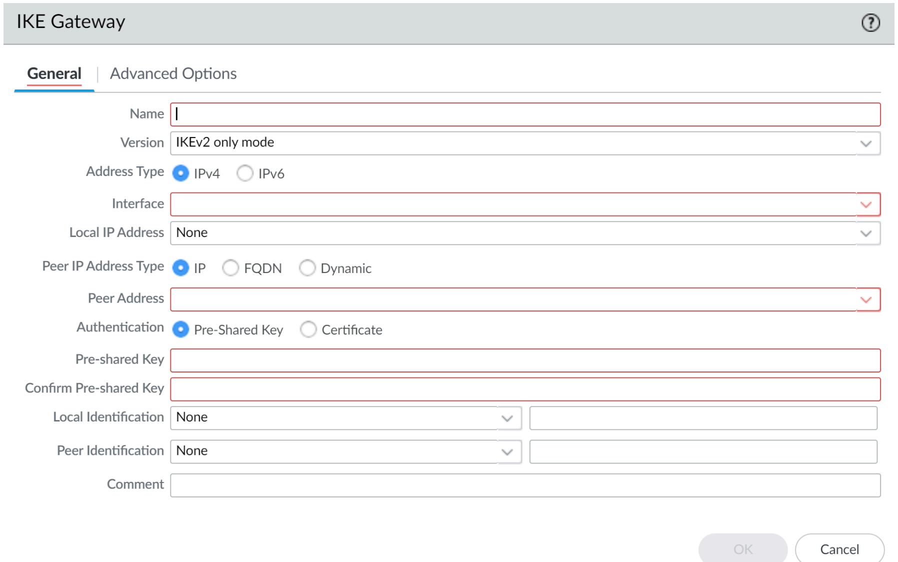
要让您的 IKEv2 VPN 能够抵抗量子攻击，请采取以下步骤：

STEP 1 | 选择 **Network**（网络） > 网络配置文件（**Network Profiles**） > **IKE** 网关（**IKE Gateways**），然后选择 **Add**（添加）以添加新网关。

STEP 2 | 配置 **General**（常规）设置，然后针对 **Version**（版本）选择 **IKEv2 only mode**（仅 **IKEv2**模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式）。

在仅 **IKEv2**模式下，如果对等方不支持 IKEv2，防火墙将中止连接。在 **IKEv2** 首选模式下，如果对等方不支持 IKEv2，防火墙将回退到 IKEv1。但 VPN 必须协商 IKEv2 才能使用后量子 VPN 功能，因此如果防火墙回退到 IKEv1，则后量子 VPN 功能将不可用。

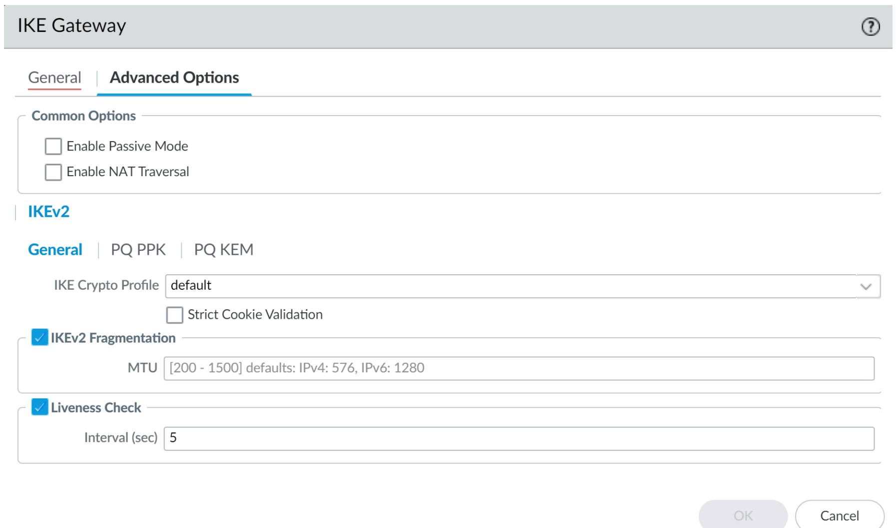
IKEv1 被认为比较弱。如果两个 *IKE* 对等方都能支持 *IKEv1*，请将您的 *VPN* 连接升级到 *IKEv2* 并选择 ***IKEv2 only mode***（仅 ***IKEv2***模式）以确保安全级别足够且能够使用 *PQ VPN*。



STEP 3 | 选择 **Advanced Options**（高级选项）并配置非量子选项。选择 **IKEv2** 并配置 **General**（常规）设置。

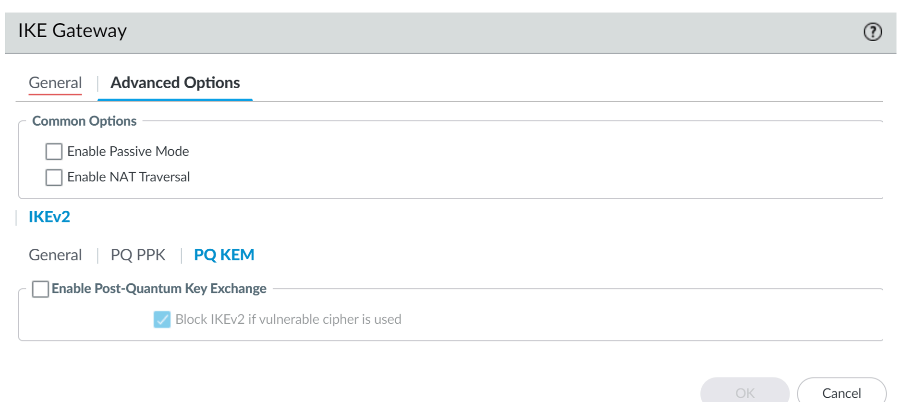
General（常规）设置可用于添加 IKE 加密配置文件、启用 **IKEv2 Fragmentation**（**IKEv2** 分段）选项以及设置 **Liveness Check**（活性检查）选项。

使用 PQC KEM 时应启用“IKEv2 Fragmentation（IKEv2 分段）”选项，因为密钥大小和数据负载都比较大。两个 VPN 终端设备都应设置为相同的片段值。



STEP 4 | 为 PQ KEM 启用后量子密钥交换，以在 VPN 上使用后量子抵抗功能。该选项在默认情况下已禁用。

或者启用 **Block IKEv2 if vulnerable cipher is used**（如果使用易受攻击的密码，则阻止 **IKEv2**）选项。如果启用此选项，则当防火墙检测到 IKE 加密配置文件中使用了易受攻击的 KEM 时，防火墙会阻止所有新的 IKEv2 对等连接。之前建立的现有 VPN 隧道可以继续生效。

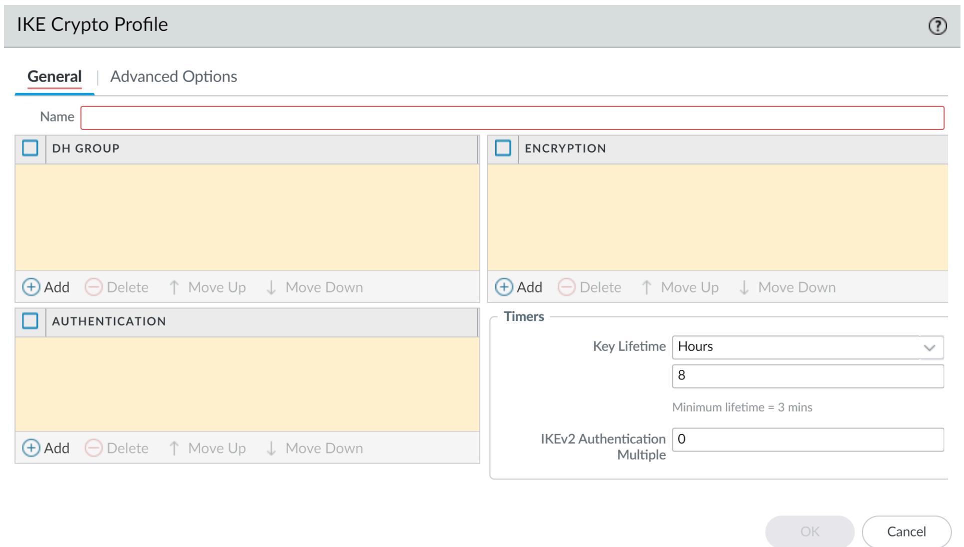


STEP 5 | 单击 **OK**（确定）以创建 IKE 网关。

STEP 6 | 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密），然后选择 **Add**（添加）以添加新配置文件。

STEP 7 | 配置 **General**（常规）设置并选择默认 IKEv2 密钥交换的加密组件（DH Group、加密、身份验证、计时器）。

选择经典强密钥交换配置来提高量子抵抗能力。*DH Group 20* 或更高、*AES-256-GCM*，并使用密钥生存期来提高密钥刷新频率。要以特定时间间隔完全重新生成密钥，请启用 *"IKEv2 Authentication Multiple*（*IKEv2* 身份验证倍数）*"*（将该选项的值设置为大于零）。达到密钥生存期的倍数后，将重新生成密钥。



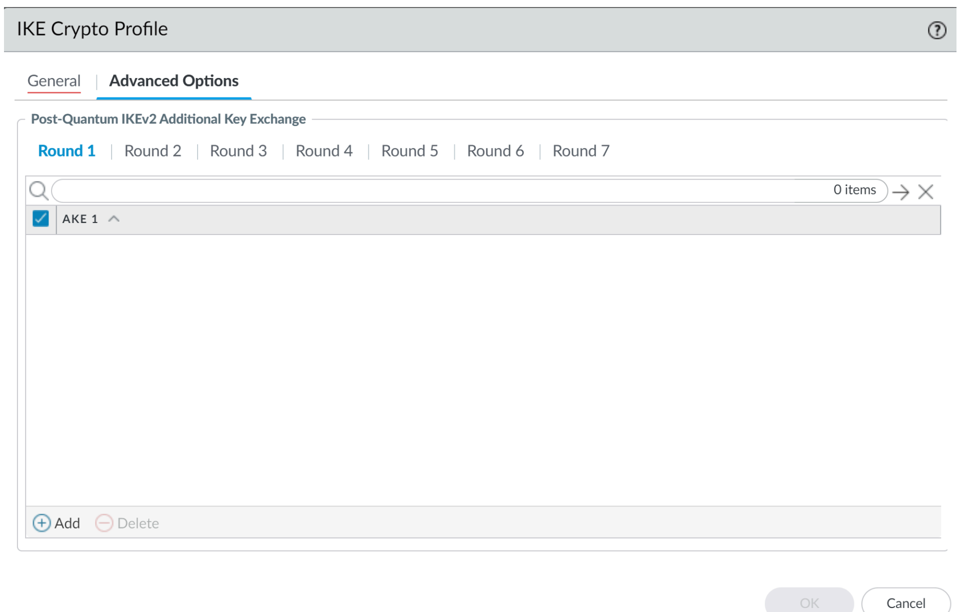
STEP 8 | 选择 **Advanced Options**（高级选项）并配置可选参数 **Post-Quantum IKEv2 Additional Key Exchange**（后量子 **IKEv2** 附加密钥交换）的轮次。

RFC 9370 允许最多七轮附加密钥交换（第 1 轮到第 7 轮）。至少需要一个 PQC KEM 来增加量子抗性。添加更多 PQC KEM 可进一步提高量子抗性，但会增加协商开销并增加 IKEv2 数据包的大小。

RFC 9370 允许跳过额外的密钥交换轮次。对于跳过的轮次，可以将其留空或设置为 **None**（无）。

附加密钥交换轮次中的 PQC 顺序设置了首选 PQC。首选顶部列出的 PQC，如果隧道另一端的 VPN 终端设备支持，则会选择该 PQC。如果您想要协商双方都能支持的最强 PQC，请在每个附加密钥交换轮次中，将最高安全级别 PQC 放在列表顶部。

隧道两侧的 VPN 终端设备应配置为相同的 PQC 和安全强度，以最大限度减少互操作性问题。为了长期保护敏感信息的安全，请选择安全强度相当于 3 级或更高的 PQC。

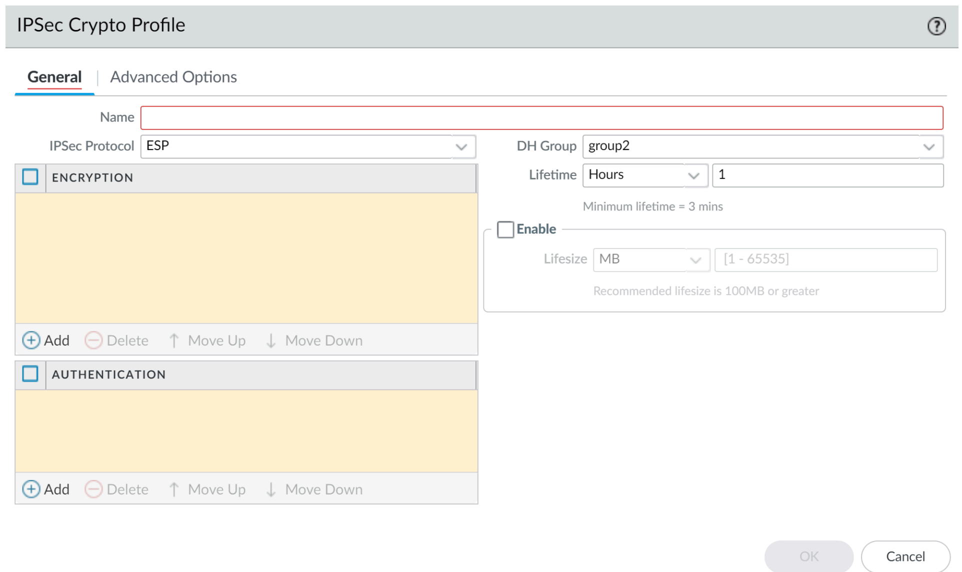


STEP 9 | 单击 **OK**（确定）以创建 IKE 加密配置文件。

STEP 10 | 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密），然后选择 **Add**（添加）以添加新配置文件。

STEP 11 | 配置 **General**（常规）设置并选择 IPSec ESP 协议的加密组件（加密、身份验证、DH Group、生命周期）。

> 选择经典强加密配置来提高量子抵抗能力。*DH Group 20* 或更高、*AES-256-GCM*、*SHA384* 或更高，并使用密钥生存期来提高密钥刷新频率。

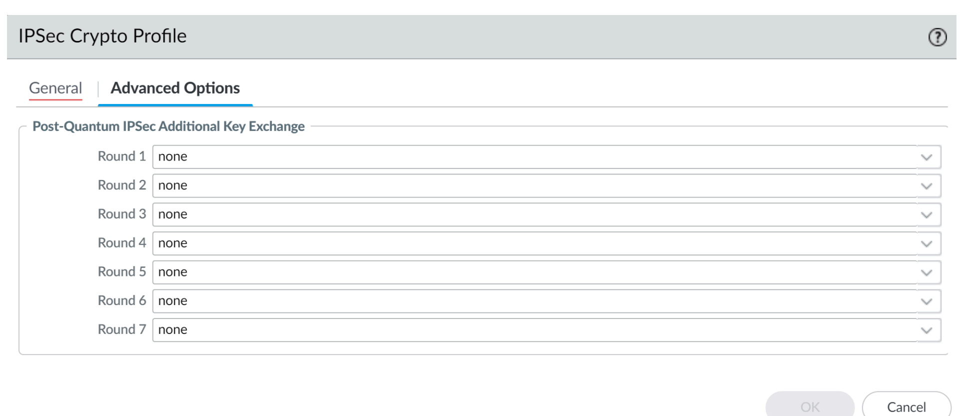


STEP 12 | 选择 **Advanced Options**（高级选项）并配置可选参数 **Post-Quantum IPSec Additional Key Exchange**（后量子 **IPSec** 附加密钥交换）的轮次。

最多允许七轮附加密钥交换（第 1 轮到第 7 轮），并且每轮仅允许一个 QC KEM。至少需要一个 PQC KEM 来增加量子抗性。添加更多 PQC KEM 可进一步提高量子抗性，但会增加协商开销并增加 IPSec 密钥更新数据包的大小。

在每个附加密钥交换轮次中，IPSec 隧道的两侧都必须配置相同的 PQC 和安全强度级别。如果存在不匹配项，密钥更新操作将失败。

> 为了长期保护敏感信息的安全，请选择安全强度相当于 *3* 级或更高的 *PQC*。



STEP 13 | 单击 **OK**（确定）以创建 IPSec 加密配置文件。

STEP 14 | **Commit**（提交）配置。

> 如果您不是双方 *IKEv2* 对等方的管理员，请将 *IKEv2* 网关、*IKE* 加密配置文件和 *IPSec* 加密配置文件信息传达给对等方的管理员，以便在其对等设备上进行安装。

后量子 IKEv 2 RFC 8784 配置示例

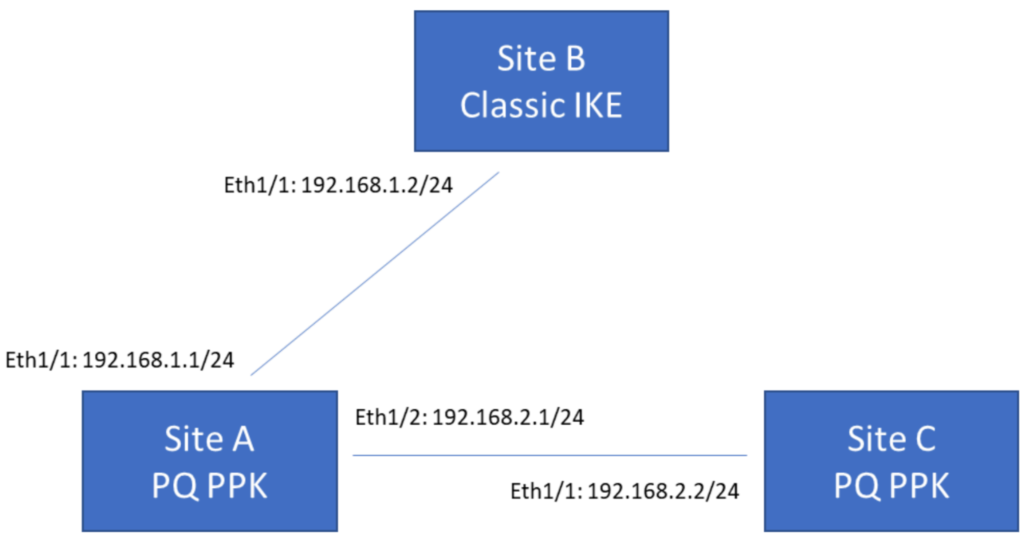
在何处可以使用？	需要提供什么？
• PAN-OS	☐ PAN-OS 11.1 或更高版本：

此示例提供了基本的 IKEv2 后量子 VPN 配置和拓扑。此示例包括两个支持 RFC 8784 的站点（后量子 VPN，可抵抗量子计算机和量子加密攻击）和一个不支持 RFC 8784 的站点。

当支持 RFC 8784 的防火墙与同样支持 RFC 8784 的防火墙通信时，设备将使用后量子配置。密钥交换使用从连接带外共享的后量子预共享密钥 (PQ PPK)，因此在 IKE 握手期间不会暴露 PQ PPK。防火墙将 PQ PPK 与经典 Diffie-Hellmann (DH) 密钥材料（在 IKE 握手期间传输）混合来创建一个不基于质数的密钥，因此无法被 Shor 算法破解。这使得防火墙能够创建一个量子抵抗密钥，以帮助抵御 "先采集，后解密" 攻击，在这种攻击中，攻击者窃取他们现在无法解密的数据并将其存储，等到他们可以使用加密相关量子计算机 (CRQC) 进行解密的时候再进行解密。

当支持 RFC 8784 的防火墙与不支持 RFC 8784 的防火墙通信时，RFC 8784 防火墙可以回退到经典 DH 密钥交换。如果发生这种情况，防火墙不会混合 PQ PPK，而是只使用 DH 密钥材料来创建密钥。请务必注意，在这种情况下，VPN 流量容易受到 "先采集，后解密" 攻击。

这个简单拓扑示例由位于不同站点的三个防火墙组成，这三个防火墙通过 IKEv2 VPN 连接。其中两个防火墙支持 RFC 8784，一个防火墙不支持 RFC 8784。



在该举例中：

- 站点 **A** 支持 RFC 8784。站点 A 与站点 B 的连接为 Eth 1/1：192.168.1.1/24 及其与站点 C 的连接为 Eth 1/2：192.168.2.1/24。站点 A 需要两个 IKEv2 网关，一个连接站点 B，另一个连接站点 A。

- 站点 **B** 仅支持经典 IKEv2 VPN，不支持 RFC 8784。它与站点 A 的连接为 Eth 1/1：192.168.1.2/24。站点 B 需要一个 IKEv2 网关才能连接到站点 A。站点 B 的 IKEv2 网关配置不包括 PQ PPK，因为站点 B 不支持 RFC 8784。
- 站点 **C** 支持 RFC 8784。它与站点 A 的连接为 Eth 1/1：192.168.2.2/24。站点 C 需要一个 IKEv2 网关才能连接到站点 A。

> 每个支持 *RFC 8784* 的 *IKEv2 VPN* 对等方必须安装和激活完全相同的*PQ PPK* 集（*KeyID* 加 *PPK* 机密字符串对）。如果选定的 *PQ PPK* 在两个对等方上都不可用，则连接将中止。
>
> *KeyID* 用于标识 *PPK* 机密字符串。
>
> *IKEv2* 对等方在 *IKEv2* 握手期间传输 *KeyID*，但 *PPK* 机密字符串是带外共享的，并单独安装在每个对等方上，由 *Panorama* 推送或由用户手动安装。*PPK* 机密字符串永远不会在握手期间发送，也无法在产生的 *IKEv2* 隧道中查看。*IKEv2* 对等方而是会使用 *KeyID* 在本地查找 *PPK* 机密字符串，并将其与 *DH* 密钥材料混合以产生后量子加密密钥。

要为示例拓扑配置 IKEv2 VPN，请导航到**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（IKE 网关）：

STEP 1 | 像配置任何其他 IKE 网关一样，为站点 A、B、C 配置 IKEv2 VPN 网关常规属性。

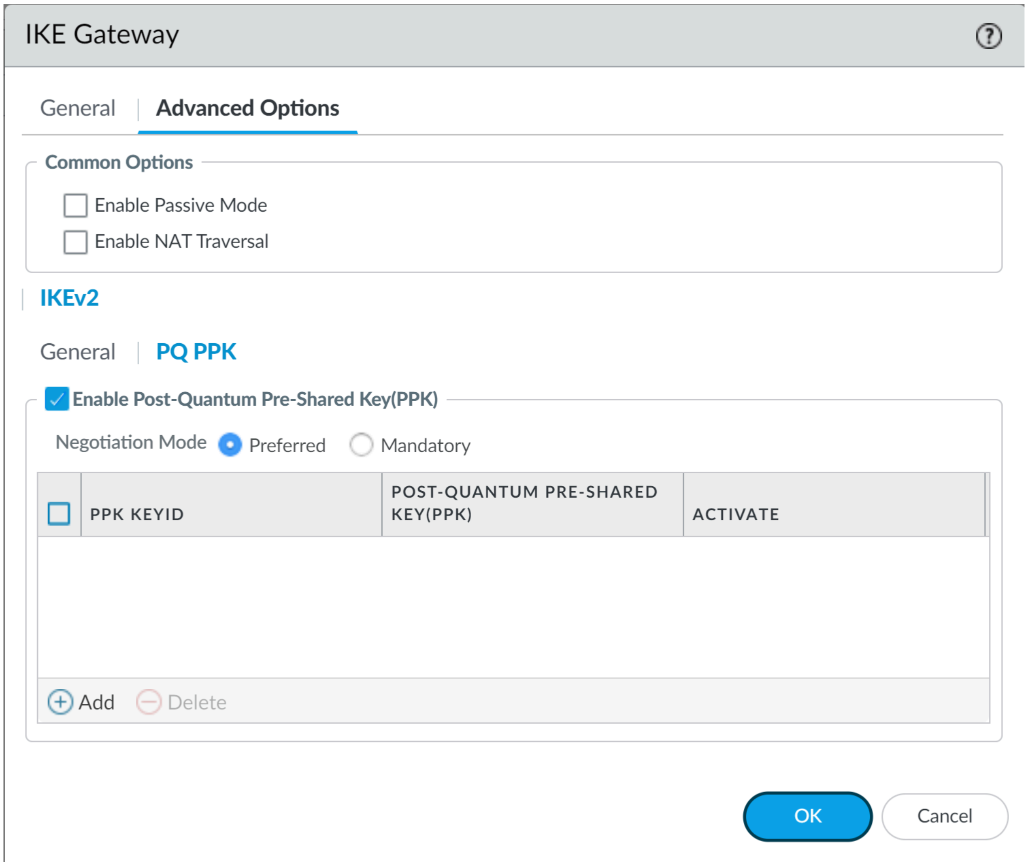
在 **General**（常规）选项卡中，配置地址、身份验证和其他常规 IKE 网关信息。将 **Version**（版本）设置为 **IKEv2 mode only**（仅 **IKEv2** 模式）以实现最佳安全性。IKEv1 被认为是一个弱协议，不支持 RFC 8784 后量子 VPN。

> 在 ***General***（常规）选项卡上配置的预共享密钥并非抵抗基于量子的攻击的后量子预共享密钥。该预共享密钥用于跨隧道的对称身份验证。

STEP 2 | 为所有三个站点配置通用选项和常规高级选项，如被动模式、NAT 遍历和 IKE 加密配置文件。

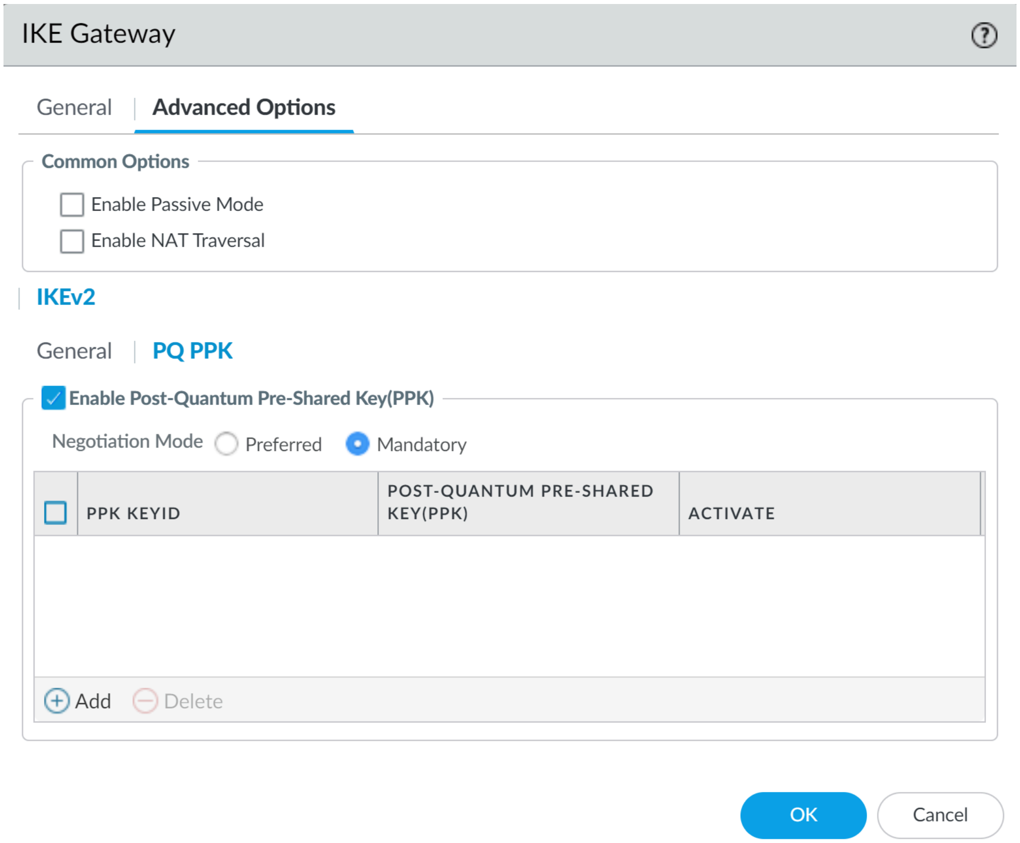
STEP 3 | 在 **Advanced Options**（高级选项） > **PQ PPK**选项卡上，为站点 A 到站点 C 的 IKEv2 VPN 和站点 C 到站点 A 的 IKEv2 VPN 选择 **Enable Post-Quantum Pre-Shared Key (PPK)**（启用后量子预共享密钥 **(PPK)**）。

由于站点 B 不支持 RFC 8784，因此您不需要在站点 B 的 IKE 网关配置或站点 A 到站点 B 的 IKEv2 VPN 配置中选择 **Enable Post-Quantum Pre-Shared Key (PPK)**（启用后量子预共享密钥 **(PPK)**）。



选择了 **Enable Post-Quantum Pre-Shared Key (PPK)**（启用后量子预共享密钥 **(PPK)**）时，**Negotiation Mode**（协商模式）的默认设置为 **Preferred**（首选），这意味着不支持 RFC 8784 的连接将回退到使用经典加密。(在 **Mandatory**（强制）模式下，如果对等方不支持 PQ PPK，防火墙将中止连接。）

STEP 4 | 在站点 A 到站点 C 以及站点 C 到站点 A 的 IKEv2 VPN 中，将 **Negotiation Mode**（协商模式）设置为 **Mandatory**（强制）。



将 **Negotiation Mode**（协商模式）设为 **Mandatory**（强制）可确保站点 A 和站点 C 在协商 VPN 隧道时始终设置量子抵抗 VPN，而不是传统 VPN。如果确定对等点是否支持 RFC 8784，请使用 **Mandatory**（强制）。如果不确定，请使用 **Preferred**（首选）模式，这样在对等方不支持 RFC 8784 的情况下（例如，您与您无法控制的企业外部设备进行对等连接时），防火墙可以回退到经典 IKEv2 VPN。

STEP 5 | 为站点 A 到站点 C 的 IKEv2 连接和站点 C 到站点 A 的 IKEv2 连接配置活动 PQ PPK。当站点 A 和站点 C 建立 IKEv2 连接时，这两个站点从这些活动 PQ PPK 中进行选择，并将所选 PQ PPK 与 DH 密钥材料混合，以创建并非基于质数的安全密钥。

> *由于站点 B 不支持 RFC 8784，因此站点 A 到站点 B 的通信或站点 B 到站点 A 的通信没有后量子配置。*

站点 A 和站点 C 的 IKEv2 对等方必须具有完全相同的活动 PQ PPK 配置。

- 如果 Panorama 管理两个 IKEv2 对等方，则可以在 Panorama 上创建配置并将其推送到托管防火墙。
- 如果 Panorama 未同时管理 IKEv2 对等方，并且对等方是由其他管理员控制，请以安全方式（如加密电子邮件）将 PQ PPK 传达给其他管理员，并安全地存储密钥。

可以为每个 PQ PPK 指定任意名称的 KeyID。您可以手动配置与每个 PQ PPK 的 KeyID 配对的 PPK 机密，也可以由防火墙为您生成一个强 PPK 机密。以下示例展示了如何使用这两种方法。

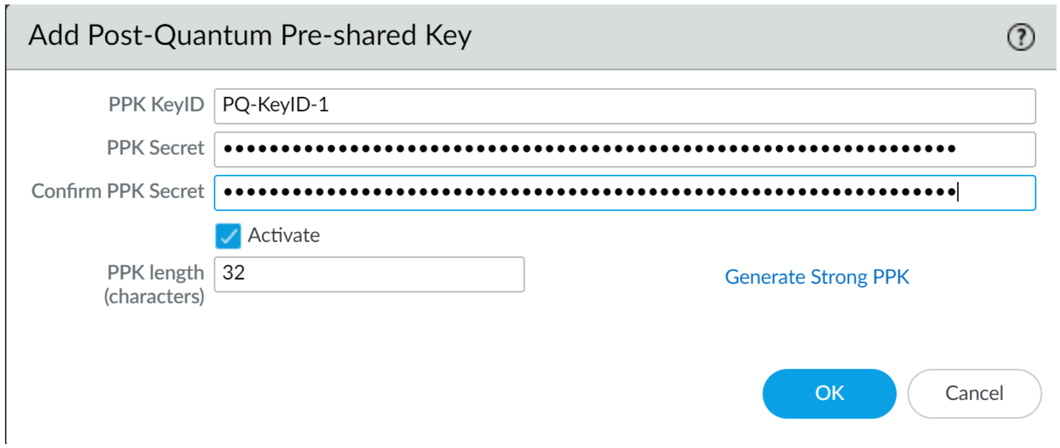
要使用手动配置的 PPK 机密创建 PQ PPK，请执行以下操作：

1. 添加 PQ PPK。
2. 在 **Add Post-Quantum Pre-shared Key**（添加后量子预共享密钥）对话框中，输入 **PPK KeyID** 名称。在本例中，名称为 **`PQ-KeyID-1`**。
3. 在 **PPK KeyID** 和 **Confirm PPK Secret**（确认 **PPK** 机密）中键入（或从其他来源复制并粘贴）完全相同的 ASCII 字符串。

   > *安全存储 PQ PPK（KeyID 及其 PPK 机密）。若手动输入 PPK 机密，机密永远不会以明文显示。如果丢失 PPK 机密，便无法恢复。(可以删除 PQ PPK，然后配置一个新的。）*

   如果 **PPK KeyID** 和 **Confirm PPK Secret**（确认 **PPK** 机密）不匹配，则出现错误消息 `PPK Secret and Confirm PPK Secret Do Not Match`（“PPK 机密”与“确认 PPK 机密”不匹配）。作为最佳实践，请指定一个长度至少为 64 个字符（32 字节或 256 位熵）的随机 PPK 机密来创建强密钥。默认情况下，新密钥处于活动状态。如果不想在 IKE 对等方之间的协商中使用密钥，请取消选择 **Activate**（激活）。如果在一个对等

方上停用 PQ PPK，则必须在另一个对等方上也停用。下面的示例显示了一个 64 个字符的强密钥（手动输入的密钥永远不会以明文显示）：



> ***PPK length (characters)***（***PPK*** 长度（字符））字段仅适用于防火墙为您生成的密钥。该字段无法控制手动配置的 *PPK* 机密字符串的长度。

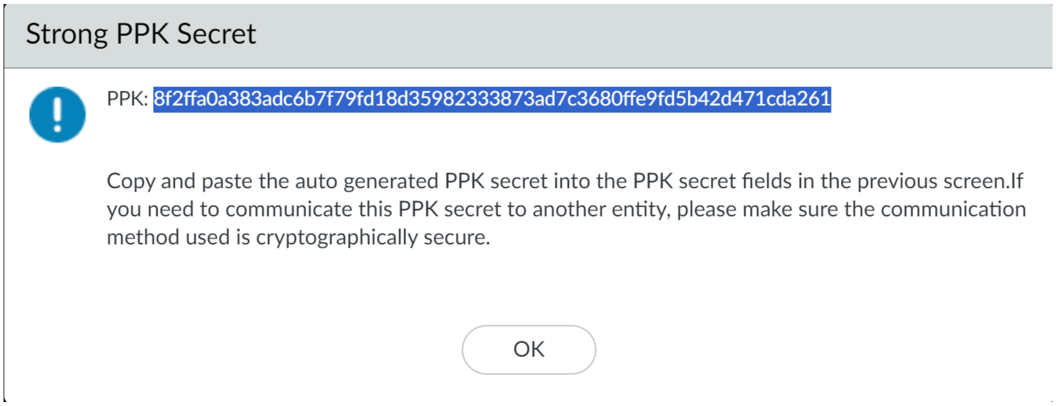
4. 单击 **OK**（确定）以安装手动配置的 PQ PPK。
5. 如果 Panorama 管理两个对等方，您可以在 Panorama 上创建配置并将其推送到托管防火墙。如果 Panorama 未同时管理两个对等方，并且另一个管理员控制 VPN 对等方，您可以将 PQ PPK 安全地传达给该管理员，由该管理员将 PQ PPK 安装在对等方上。

要使用防火墙生成的 PPK 机密创建 PQ PPK，请执行以下操作：

1. 添加 PQ PPK。
2. 在 **Add Post-Quantum Pre-shared Key**（添加后量子预共享密钥）对话框中，输入 **PPK KeyID** 名称。在本例中，名称为 **`PQ-Key-ID-2`**。
3. 要创建强密钥，请将 **PPK length (characters)**（**PPK** 长度（字符））设置为至少 64 个字符（32 字节或 256 位熵）。
4. 单击 **Generate Strong PPK**（生成强 **PPK**）。

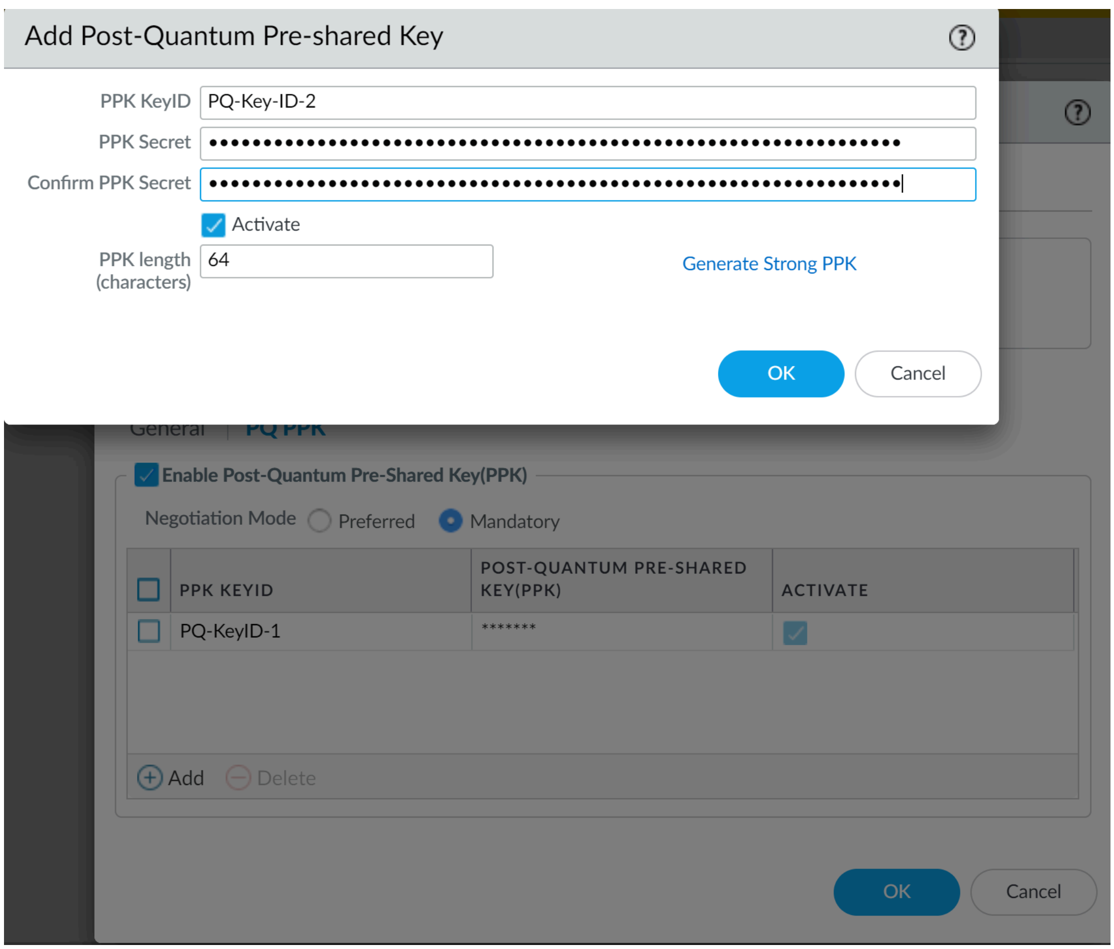
   防火墙生成一个随机的强十六进制 PPK 机密，其长度如 **PPK length (characters)**（**PPK** 长度（字符））中所配置。
5. 突出显示并复制 PPK 机密字符串。

> 仅复制十六进制机密。请勿复制 *PPK:* 字符。例如，如果生成的机密显示为：
>
> *`PPK:38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`*
>
> 只需复制：
>
> *`38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`*
>
> 前导字符 *PPK:* 不属于机密字符串。



存储复制的 PPK 机密（由防火墙以安全方式生成）。单击 **OK**（确定）后，防火墙将不再以明文形式显示 PPK 机密。如果现在不复制并安全地存储 PPK 密钥，便会丢失，并且需要删除此 PQ PPK 再配置一个新的。

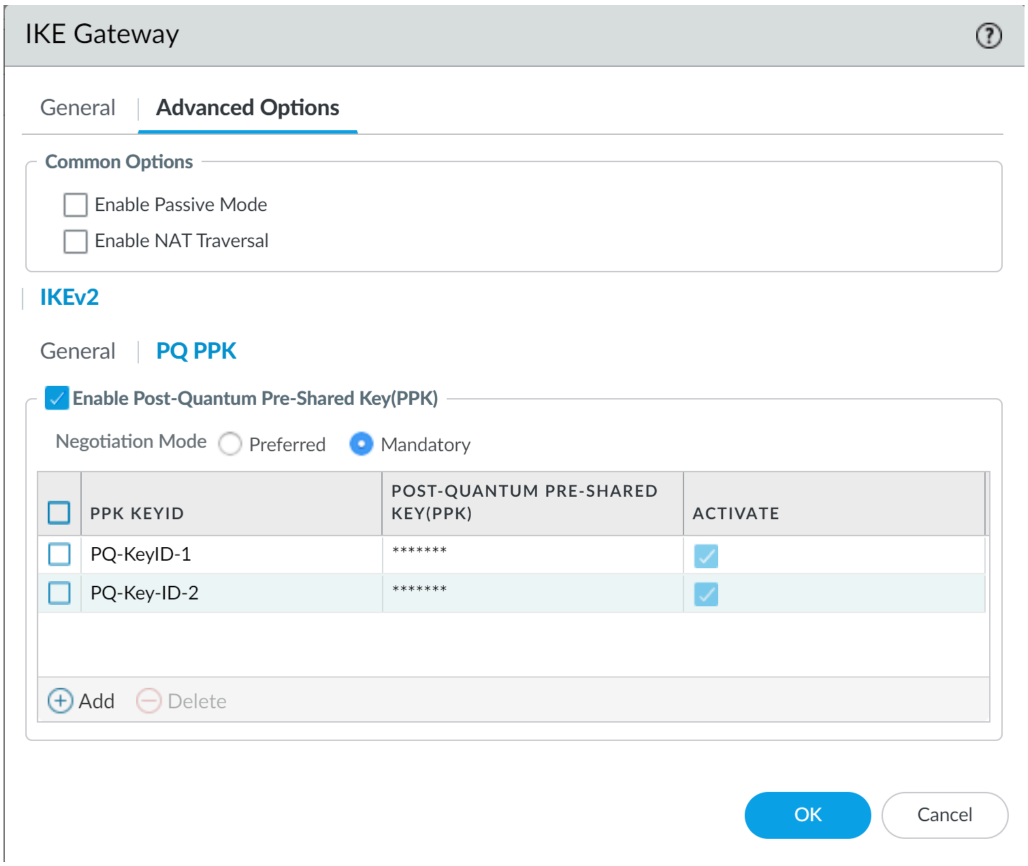
6. 当复制的 PPK 机密仍在剪贴板中或可从安全存储中复制时，单击 **OK**（确定）。如果您没有复制 PPK 机密，请生成另一个强 PPK 机密，并确保复制且安全地存储。
7. 将复制的 PPK 机密字符串粘贴到 **Add Post-Quantum Pre-Shared Key**（添加后量子预共享密钥）中的 **PPK Secret**（**PPK** 机密）和 **Confirm PPK Secret**（确认**PPK**机密）字段中。



默认情况下，新密钥处于活动状态。如果不想在 IKE 对等方之间的协商中使用密钥，请取消选择 **Activate**（激活）。如果在一个对等方上停用 PQ PPK，则必须在另一个对等方上也停用。

8. 单击 **OK**（确定）以安装防火墙生成的 PQ PPK。
9. 如果 Panorama 管理两个对等方，您可以在 Panorama 上创建配置并将其推送到托管防火墙。如果 Panorama 未同时管理两个对等方，并且另一个管理员控制 VPN 对等方，您可以将 PQ PPK 安全地传达给该管理员，由该管理员将 PQ PPK 安装在对等方上。

对于站点 A 和站点 C，在此示例中创建的两个 PQ PPK 在强制模式下列为活动 PQ PPK。



PPK 机密现在是隐藏的，永远不会以明文显示。站点 A 和站点 C 之间的 IKEv2 VPN 现在实施 RFC 8784 以抵抗量子攻击。站点 A 和站点 B 之间的 IKEv2 VPN 继续使用经典的 DH 密钥交换，并且仍然容易受到“先采集，后解密”的攻击。

如果此示例中的站点 B 已升级为支持 RFC 8784，您可以按照相同过程将站点 A 升级到站点 B，并将站点 B 升级到站点 A 的 IKEv2 VPN。