paloalto TECHDOCS

量子安全性管理

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

量子安全性概念 5

量子運算威脅 6

RFC 8784 如何抵抗量子運算威脅 9

RFC 9242 和 RFC 9370 如何抵抗量子運算威脅 11

支援後量子特性 14

後量子移轉規劃與準備 15

抵抗後量子攻擊的最佳做法 22

深入瞭解後量子安全性 26

設定抗量子 **IKEv2 VPN** **29**

使用 RFC 8784 PPK 設定後量子 IKEv2 VPN 30

使用 RFC 9242 和 RFC 9370 混合金鑰設定後量子 IKEv2 VPN 36

後量子 IKEv2 RFC 8784 設定範例 42

量子安全性概念

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

量子電腦 (QC) 威脅網路和資料安全。當 QC 發展至成熟狀態，可生產出專門用於破解解密的攸關加密量子電腦 (CRQC) 時，許多過去被認為安全的經典密碼將再也無法阻止攻擊者解密您的資料。這意味著基於經典密碼編譯的公用金鑰基礎結構 (PKI) 將容易受到後量子攻擊。威脅是立即的，特別是對於長期存活的資料，因為存在現在收集，日後解密攻擊，其中攻擊者會取得加密資料並將其保存，直到他們擁有可以解密資料的 CRQC 為止。

抵抗基於量子運算的攻擊首先要增強 IKEv2 金鑰交換期間建立的金鑰，以保護您的 VPN，並瞭解您目前的密碼編譯和後量子密碼編譯 (PQC)。Palo Alto Networks 抵抗量子攻擊的解決方案是以開放標準為基礎，來實現並確保能與符合標準的其他裝置互通。

第一步是實作 RFC 8784 以建立抗量子 IKEv2 VPN，如本文件所述。抗量子 VPN 可以防止攻擊者記錄關鍵的加密金鑰材料，並防止他們解密資料，即使他們成功竊取了加密的資料。RFC 8784 提供一種簡單的方式可從當今的經典密碼編譯轉移至具有量子抵抗力，此方式不需要升級密碼，且被認為是在 VPN 通訊中引入量子抵抗力的最簡單方式。

第二步是單獨實作 RFC 9370 或與 RFC 8784 一起實作，以使用可結合經典 KEM 技術和 PQC KEM 技術的多種金鑰交換機制 (KEM)，來建立抗量子 IKEv2 VPN。該解決方案也稱為 IKEv2 後量子混合金鑰，並使用新的替代 PQC 演算法，該演算法不易受到使用 Shor 演算法的量子攻擊。

本章介紹 QC、它們對資料安全的威脅、您現在可以透過建立抗量子 IKEv2 VPN 來做些什麼，以及如何規劃和準備移轉到後量子 VPN 和 PQC。

- 量子運算威脅
- RFC 8784 如何抵抗量子運算威脅
- RFC 9242 和 RFC 9370 如何抵抗量子運算威脅
- 支援後量子特性
- 量子運算威脅
- 抵抗後量子攻擊的最佳做法
- 深入瞭解後量子安全性

量子運算威脅

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

公用金鑰基礎結構 (PKI) 加密和 IKE 金鑰交換機制廣泛使用 Diffie-Hellman (DH)、橢圓曲線密碼編譯 (ECC) 和橢圓曲線 Diffie-Hellman (ECDH) 等經典密碼編譯。量子電腦 (QC) 可能會在 NIST 對第一個後量子密碼編譯 (PQC) 進行標準化後的 5-15 年內破解這些技術。

基於 RFC 8784、RFC 9242 和 RFC 9370 開放標準的後量子 IKEv2 VPN 可抵抗基於量子運算和 PQC 的攻擊。使用 RFC 8784 時，管理員不是在對等交握中將金鑰材料傳送到 IKE 對等體，而是單獨頻外設定和共用金鑰材料。如果攻擊者竊取資料，他們無法解密資料，因為他們沒有金鑰材料。RFC 9370 對 IKEv2 新增了額外 7 輪的選用 KEM 輪次，以允許建立使用不同類型的 KEM 技術制定的混合加密金鑰。若要破解混合金鑰，必須入侵用於建立該金鑰的所有 KEM。Palo Alto Networks 抵抗量子攻擊的解決方案是以開放標準為基礎，來實現並確保能與符合標準的其他裝置互通。

最立即的危險是現在收集，日後解密攻擊，攻擊者會竊取他們現在無法解密的資料（靜止或傳輸中）並將其保存起來，直到攻關加密的量子電腦 (CRQC) 可以解密為止。CRQC 是一種 QC，針對使用量子演算法進行最佳化，能在數秒內破解加密，而不是經典超級電腦需要數百萬年的時間才能破解。風險最高的資料是長期存活的資料，當 CRQC 可供使用時，這些資料仍然具有相關性。

- 什麼是量子電腦？
- Quantum 威脅對我的網路有何影響？
- 現在如何緩解收集攻擊

什麼是量子電腦？

量子電腦 (QC) 本質上是次世代的超級運算平台。QC 利用量子力學定律大幅減少處理資料和執行演算法（包括可以破解經典解密的演算法）所需的時間。經典電腦需花費數百年或數千年才能完成的作業，QC 只需要幾秒鐘甚至幾微秒就能完成。QC 不是基於讓超級電腦能力線性成長的經典位元（0 和 1），而是使用基於偏振光子（光）的量子位元，能讓 QC 的處理能力呈指數性成長。

有幾種方法可以建立量子位元，該方法會影響量子位元的品質，亦即量子位元的效率。量子位元的品質越高，QC 就越快、越有效。量子位元因為其量子性質，可以同時表示兩種狀態，且可以遠距離複製這些狀態。這是由於量子的疊加與糾纏效應：

- 疊加—量子位元可以同時表示 1 和 0。組合的量子位元讓量子位元可以表示的狀態數量增加，因為狀態數量以 2**n 的速率增加，其中“n”是量子位元數量。因此，兩個量子位元可以表示 4 個狀態 (2**2)，3 個量子位元可以表示 8 個狀態 (2**3)，4 個量子位元可以表示 16 個狀態 (2**4)，依此類推。

  隨著量子位元密度（晶片上可容納的量子位元數量）的增加，組合後的量子位元可以表示的狀態數量會呈指數性增加。量子位元的品質越好，量子位元的組合數量就越接近真正的指數規模。低品質（雜訊）的量子位元在組合後，所增加的狀態數量不會呈指數級增長，但與經典電

腦相比，仍然會顯著增加狀態數量。隨著量子位元品質的提升，QC 所表示的狀態數量就越來越接近真正的指數級增長。

- 糾纏—糾纏是量子位元之間的量子鍵。糾纏量子位元會透過對其執行相同的量子演算法產生相同的結果，無論它們位於何處，即使量子位元彼此相距半個地球。因此，如果您在位於邦加羅爾（印度）和洛杉磯（美國）的糾纏量子位元上執行特定的演算法，則這些位置的糾纏量子位元會產生相同的結果。量子糾纏運作的確切機制尚不清楚。

QC 分為三種類型：

- 量子退火—當今可用的類型，是能力最弱的，使用案例最窄的 QC。但是，攻擊者可以透過使用量子演算法來利用這種類型進行大數的因式分解，這就是破解非對稱加密的方法。
- 類比量子模擬器—這種模擬器解決了經典電腦無法解決的物理問題，例如量子化學、材料科學、最佳化問題、大數因式分解、採樣和量子動力學。
- 通用量子電腦—這些是最難建構的 QC，因為需要許多物理量子位元。其解決的使用案例最為廣泛，有幾家公司的目標是在這個十年結束時將其商業化。這類電腦開發出來時，將成為 CRQC。

QC 建立了一個由許多糾纏量子位元組成的多維空間，用於解決複雜的問題。例如，經典電腦擷取資料庫的每個元素，加以處理，然後在處理完所有元素後將其與其他元素組合。QC 建立一個演算法，可以解決您正在尋找的每種狀態和結果。它們同時通過演算法傳遞整個資料庫，並同時分析每個結果的資料。這使得 QC 可能比經典電腦快數百萬倍，這也是它們擅長解決複雜數學問題（例如破解加密）的原因之一。

Quantum 威脅對我的網路有何影響？

QC 的處理能力和速度大幅提高，可能會破壞經典的資料加密方法，而危害您的公用金鑰基礎結構 (PKI)。

最直接的威脅是「現在收集，日後解密」攻擊，這些攻擊會竊取您的加密資料，目的是未來使用 CRQC 將其解密。一旦攻擊者竊取了您的資料和經典金鑰材料，就無法阻止他們未來使用 CRQC 解密資料。如果被竊取的資料當時仍然有效，資料便會洩漏。

經典非對稱加密是基於質數，並依賴因式分解複數導出這些質數的難度。一個名為 Shor 演算法的量子演算法可以因式分解複數並解決離散對數問題。Shor 演算法威脅到 PKI 安全性，此安全性基於兩個非常大的質數來產生金鑰。然而，Shor 演算法使用經典電腦的話，無法在不到數百萬年的時間破解 PKI 安全性。如果沒有 CRQC，Shor 演算法就不會構成威脅。但是，因為 CRQC 的處理能力，Shor 演算法可以在數秒或更短的時間內將複數因式分解，並破解經典的非對稱加密（例如解密資料所需的金鑰交換材料）。這就是為什麼「現在收集，日後解密」攻擊是一個直接的威脅。

破解經典加密的後果包括危害被認為安全的經典 PKI 密碼編譯（例如 Diffie-Hellman (DH)、橢圓曲線密碼編譯 (ECC) 和橢圓曲線 Diffie-Hellman (ECDH)）其安全性。金鑰交換面臨最大的風險，這就是為什麼您需要設定後量子 IKEv2 VPN 來保護金鑰交換。

憑證一直是兩個端點建立信任的基礎。但是，CRQC 也可能危害 RSA；RSA 用於建立和保護數位憑證。這意味著攻擊者可以使用 CRQC 竊取或仿冒數位特徵碼，因此您認為正在連線的伺服器實際上可能是攻擊者的伺服器。最快在未來十年內就會具備這種能力。

此外，QC 的純粹暴力密碼破解意味著對稱加密也不安全。Grover 演算法是一種量子二次方加速非結構化搜尋演算法，用於尋找產生特定輸出值的唯一輸入。Grover 演算法以對稱密碼編譯和雜湊函數為目標。它基本上將 AES 演算法的密碼強度減半，因此如果您使用 AES-128 位元加密，Grover 演算法會將其降低到 64 位加密的密碼強度。因為經典電腦沒有足夠的處理能力，所以無法使用 Grover 演算法來破解對稱加密。但是，使用 QC，Grover 演算法便可以破解 AES-128 位加密。

由於 *AES-128* 位加密容易遭到 *Grover* 演算法破解，因此請使用 *Grover* 演算法在近期或中期無法破解的 *AES-256* 位加密。

為了幫助保護雜湊函數，請至少使用 *SHA-384*。

後量子密碼編譯 (PQC) 現今已可用，大多數精通安全性的人都可以下載和設定無法解密的 PQC。如果您在網路上允許未經授權的 PQC，則內部不良行為者可能會將 PQC 引入您的網路。如果發生這種情況，您將無法查看使用 PQC 的流量，也無法查看該流量中的威脅。使用解密功能可偵測網路上未經授權的 PQC，並自動封鎖使用 PQC 的流量。

現在如何緩解收集攻擊

立即採取這些動作來抵抗後量子「現在收集，日後解密」攻擊。檢查您的 VPN 連線並加以強化：

- 遵循 RFC 6379《*IPsec* 的套件 *B* 加密套件》，將您的 VPN 連線升級成嚴格的密碼套件。使用 Suite-B-GCM-256 並避免使用較弱的 128 位元 AES 演算法，這些演算法容易受到 Grover 演算法的攻擊。
- 將您的 CA 升級到 4K RSA 金鑰大小，以減輕會破壞較小金鑰大小的暴力密碼破解，並將您的 VPN 憑證驗證轉移到新憑證。
- 升級至更高位元的 SHA 雜湊大小，例如 SHA-384 和 SHA-512。停止使用如 MD5 和 SHA-1 等弱式雜湊。
- 實作 RFC 8784 和/或 RFC 9242 和 RFC 9370 以建立可抵抗量子攻擊的後量子 VPN。

此外，檢查您的 SSL/TLS 連線並加以強化：

- 將 SSL/TLS 連線升級為嚴格的密碼套件；將 TLSv1.3 與完美轉送密碼 (PFS) 的密碼結合使用。
- 在強化的用戶端到伺服器 VPN 工作階段中，建立 SSL/TLS 工作階段通道。使用後量子桌面應用程式來支援反向 Proxy。

RFC 8784 如何抵抗量子運算威脅

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

RFC 8784 標準《在網際網路金鑰交換通訊協定版本 *2 (IKEv2)* 中混合預先共用金鑰以實現後量子安全性》，讓您能夠建立 IKEv2 VPN 來抵抗當今基於量子電腦 (QC) 和後量子密碼編譯 (PQC) 的攻擊。

RFC 8784 的本質是與 IKE 金鑰交換分開地在頻外交換靜態後量子預先共用金鑰 (PQ PPK)，並將頻外的 PQ PPK 材料與於 IKEv2 金鑰交換期間在頻內傳輸的 Diffie-Hellman (DH) 金鑰材料混合。這透過兩種方式增強金鑰交換：

- DH 金鑰和 DH 金鑰的變體憑藉的是解決離散對數問題有難度，例如解決 DH 所基於的質數非常大。然而，隨著攸關加密的量子電腦 (CRQC) 出現，DH 金鑰變得容易受到基於 Shor 演算法的攻擊。實作 RFC 8784 增強了金鑰的加密強度，因為混合金鑰不再僅基於解決離散對數問題的難度（例如，解決非常大的質數），因此混合金鑰不易受到 Shor 演算法的影響
- 接聽程式（或是中間人）無法取得所有金鑰材料以供日後解密。金鑰的經典 DH 部分會在 IKE 對等金鑰交換中傳送，但 IKE 對等體與 DH 金鑰材料混合的 PQ PPK 絕不會在金鑰交換期間或在建立VPN 後於 VPN 中傳輸，因此攻擊者即使使用金鑰材料的 DH 部分，也無法解密周遊 VPN 的資料。

IKEv2 對等體會根據金鑰 ID 知道要使用哪個 PQ PPK。每個 PQ PPK 皆包含兩個元素：KeyID 和預先共用密碼。預先共用密碼是您在頻外與 IKEv2 對等體共用的金鑰材料。它絕對不會與 DH 金鑰材料或在建立 VPN 後與資料一起在頻內傳輸。相反地，一個 IKEv2 對等體的管理員會手動建立靜態預先共用密碼，並安全地將其傳達給另一個 IKEv2 對等體的管理員，例如透過安全電子郵件或從 Panorama 推送。每個管理員都將預先共用密碼以程式寫到其對等體中，因此該密碼絕對不會在 IKE 連線中洩漏。

金鑰 ID 在金鑰交換期間於頻內傳輸，用於識別 IKEv2 對等體上的預先共用密碼。IKEv2 對等體使用金鑰 ID 來尋找預先共用密碼，並將其與 DH 金鑰材料混合，以建立不基於質數且無法透過竊聽通訊來竊取的新金鑰資料。

兩個 *IKEv2* 對等體必須使用完全相同的金鑰 *ID* 和預先共用密碼 *PQ PPK* 配對。如果金鑰 *ID* 及其相關聯的預先共用密碼不相符，則會中止連線。如果您設定多個 *PQ PPK*，則兩個 *IKEv2* 對等體必須具有一組完全相同的作用中金鑰 *ID* 和預先共用密碼。（*Palo Alto Networks* 允許您設定最多 *10* 個作用中 *PQ PPK*，但某些廠商只允許設定 *1* 個 *PQ PPK*，因此瞭解對等體的能力非常重要。）

這種基於標準的方法提供了一種簡單的方法，來防止攻擊者竊聽連線並攔截金鑰（這讓攻擊者能夠在 VPN 建立後解密於 VPN 中傳送的資料），同時還確保能夠與遵守標準的其他裝置互通。RFC 8784 的優點包括：

- 具有多個廠商支援的經核准標準。

- 不會消耗額外的網路資源，而且延遲時間幾乎不增加。
- 回溯相容，因此您可以在並非所有對等體都支援 IKEv2 且您無法控制所有對等體的網路中使用它。
- 金鑰不再基於質數，因此不易受到 Shor 演算法的影響。
- 不會傳輸 PQ PPK，因此不能用於解密所收集的資料。
- 受到 NIAP、NSA、德國聯邦資訊安全辦公室等全球許多政府機構的推薦。此外，建立長度為 32 位元組或更長的強式隨機密碼符合 NIST Category 5 安全性層級。確保密碼是強大且隨機的、不遵循模式，且不會受到字典攻擊。
- 您可以將 RFC 8784 與基於標準的未來功能（例如 PQC 混合金鑰）分層。

這可以加快採用的速度，因為幾乎不需要進行任何更改，而且不存在由於不相容而導致連線中斷的危險。然而，RFC 8784 有一些缺點：

- 儘管將 PQ PPK 從 Panorama 推送到受管理的防火牆有助於減緩擴展，但手動設定靜態 PQ PPK 對於許多網站而言無法很好地擴展。
- PQ PPK 必須由共用它的所有 IKEv2 管理員安全地保存。這不僅包括您公司內部的管理員，還包括合作夥伴、廠商的管理員，以及您需要對等互連的其他外部管理員。風險來自於管理員寫下 PQ PPK 後卻使其遺失、遭竊或外洩。
- 要依靠人類建立長而強大的隨機密碼來抵抗字典攻擊和其他攻擊，可能具有挑戰性。實作 Palo Alto Networks 能夠讓您自動產生長且強大的十六進位密碼，您不必自己建立。

基於 RFC 8784 的 IKEv2 VPN 是針對解決 PQC 和後量子威脅建議的第一步。在 NIST 標準化第一批 PQC 後，可以與 RFC 8784 配合使用的其他方法將增強對量子威脅的抵抗力，例如 RFC 9242 和 RFC 9370。

RFC 9242 和 RFC 9370 如何抵抗量子運算威脅

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.2 或更新版本。

RFC 9242 標準「網際網路金鑰交換通訊協定 *2 (IKEv2)* 中的中繼金鑰交換」讓 IKEv2 能夠在 IKEv2 安全性關聯 (SA) 建立中傳輸大量資料，以支援其金鑰大小更大的多個 PQC 金鑰交換。RFC 9370 標準「網際網路金鑰交換通訊協定 *2 (IKEv2)* 中的多個金鑰交換」允許在 SA 設定期間計算共用密碼時，進行多個金鑰交換。

這兩個 RFC 標準一起讓 IKEv2 能夠使用經典和 PQC 金鑰交換機制 (KEM) 建立混合金鑰，以減緩使用 Shor 演算法的量子攻擊。新的 PQC 基於不同的數學技術，不易受到已知的經典或量子攻擊，其中包括：

- 晶格
- 基於程式碼
- 基於雜湊
- 對稱金鑰
- 基於同源性
- 多變數

RFC 9370 標準允許有額外七次的金鑰交換輪次，這些輪次可以是經典或 PQC KEM，例如 ML-KEM、BIKE、HQC、Classic McEliese 等，此外還有總共 8 輪次的 IKEv2 預設金鑰交換。

若要破解混合金鑰，用於建立加密金鑰的所有 KEM 技術都必須有弱點並受到危害。例如，要建立一個能夠抵抗當今已知弱點和未來量子電腦 (QC) 威脅的混合金鑰，最佳做法建議使用經典 KEM 和一或多個使用不同數學技術的 PQC KEM。

- 預設 KEM 輪次：Diffie-Hellman (DH) 群組 21
- 第 1 輪次的額外金鑰交換：ML-KEM-768 (CRYSTALS-Kyber-786)
- 第 2 輪次的額外金鑰交換：BIKE-L3

在前面的範例中，經典的 DH 群組 21 針對當今的前量子攻擊提供了防護。透過 ML-KEM-768（晶格）和 BIKE-L3（基於代碼）新增額外兩輪次的 PQC KEM，可依序建立基於三種 KEM 技術的加密金鑰，並使用 Shor 演算法針對未來的攻擊提供防護。在 DH 金鑰交換中新增至少兩個 PQC，可針對單一 KEM 故障提供更高層級的防護，並有助於更長期抵抗量子攻擊。此外，使用基於不同類型數學的 KEM 可以防止未來容易遭受特定類型 PQC（例如基於晶格技術的所有 PQC）的入侵

轉移至 PQC 是唯一金鑰交換機制的後量子世界將需要很多年的時間，因為產業需要時間來驗證新的 PQC 並對其安全能力建立信心。在轉移期間，基於 RFC 9242 和 RFC 9370 的混合金鑰將成為標準。

核准新 PQC 的標準程序將分階段進行，NIST 在每一輪次的核准中都會核准 PQC 群組。由於每個 PQC 都要權衡效能和安全性，因此需要瞭解每個 PQC 的執行方式，以確定不同的安全性使用案例最適合哪一種技術。例如，Classic McEliece 隨著時間已證明自己是非常安全的 PQC，但其高安全的代價是所使用金鑰的大小很大，這會限制 Classic McEliece 在 VPN 和 TLS 通訊中的使用。

全球各國政府建議採用 *L3* 或以上的安全性層級，以提供強大的安全性並抵抗未來的量子電腦攻擊。

在從經典加密轉移至後量子加密的過渡期間，需要具有加密靈活性，以允許快速更換任何受損的 PQC。Palo Alto Networks RFC 9242 和RFC 9370 後量子 KEM 解決方案提供了一組廣泛的PQC，可從一開始就實現加密靈活性，允許客戶快速從 IKEv2 金鑰交涉中選取和刪除任何支援的 PQC，而無需更新任何的軟體或變更現有的網路。

PAN-OS IKEv2 支援以下 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
- Classic McEliece 348864、348864f

RFC 9242 和 RFC 9370 的優點包括：

- 多廠商支援的已核准標準。
- 透過動態金鑰交換實現高可擴展性，而不是透過 RFC 8784 的靜態 PPK。
- 支援廣泛的 PQC KEM。
- 如果對等體不支援 RFC，則 IKEv2 回溯相容性允許回退。
- 混合金鑰更能抵抗 Shor 演算法，因為不同的 PQC 技術可以一起使用。
- 可與 RFC 8784 分層，以實現量子深度防禦和加密靈活性。

RFC 9242 和 RFC 9370 的缺點包括：

- 早期的 PQC 標準化清單可能無法提供足夠的 PQC，以在 PQ 轉移開始時實現加密靈活性。
- 新的 PQC 可能需要很多年才能得到行業的充分審查和信任。
- 多個 KEM 會增加額外的開銷並減緩 IKEv2 對等互連的過程。
- 由於金鑰大小和資料有效負載較大，新的 PQC KEM 可能會導致分段。
- 並非所有的裝置都可以升級以支援 PQC KEM。
- 由於驗證起始者之前所需的資源增加，因此在 IKE_INTERMEDIATE 期間，延伸的金鑰交換可能會增加拒絕服務 (DoS) 攻擊的風險。

- 混合金鑰旨在防禦收集攻擊，在此攻擊中，攸關加密的量子電腦 (CRQC) 會儲存加密的資訊並於日後解密。在主動攻擊中使用量子電腦進行的攻擊無法透過混合金鑰完全解決，原因如下：
  - 仍然使用經典方法（預先共用金鑰或數位特徵碼演算法）進行驗證。預先共用金鑰必須又長又複雜，才能保證後量子安全，但它們不可擴展。使用數位特徵碼的驗證必須使用後量子數位特徵碼來執行。
  - PQC 旨在提供對收集攻擊的抵抗力，在 CRQC 可用之前，攻擊連線的真實性並不重要，因為不存在被利用的可能性，原因是這些攻擊僅發生在連線時。

建議您使用基於 RFC 9242 和 RFC 9370 的 IKEv2 VPN，透過使用基於多種 KEM 技術的混合金鑰，來保護 VPN 連線免受後量子威脅。透過廣泛的 PQC，可以實現加密靈活性，以在轉移至後量子世界的過渡期間防禦遭入侵的 PQC。

支援後量子特性

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

後量子功能和能力的支援包括 RFC、HA 以及升級和降級考量事項。現在正處於後量子標準和功能發展的早期階段，各國、廠商和企業都在努力設法保護其資料免受後量子攻擊。隨著標準的進展和 Palo Alto Networks 平台的支援，本主題將更新以說明該支援。

- 支援的 RFC 和互通性
- HA 支援
- 升級和降級考量事項

支援的 **RFC** 和互通性

Palo Alto Networks 裝置完全支援 RFC 8784、RFC 9242 和 RFC 9370 開放標準。

Palo Alto Networks 裝置可與支援相同標準的其他裝置互通，儘管某些廠商的實作可能會因 RFC 的解釋而有所不同。例如，某些廠商可能無法提供功能以使用 RFC 8784 盡量設定後量子預先共用金鑰 (PQ PPK)，或者他們可能不支援 Palo Alto Networks 透過 RFC 9370 支援的廣泛 PQC。

HA 支援

IKE VPN 的高可用性 (HA) 與引入後量子功能之前相同：VPN 通道在容錯移轉後會繼續執行，且 IKE 對等體在容錯移轉後會重新同步化和重新整理 IKE 金鑰。

升級和降級考量事項

當您從不支援後量子 IKEv2 VPN 的版本升級時，平台會提供對後量子功能和能力的支援。

當您降級到支援您所設定後量子功能的版本時，設定不會變更，且後量子 IKEv2 VPN 安全性仍然存在。

當您降級到不支援後量子 IKEv2 VPN 功能的版本時：

- 如果您未設定後量子 IKEv2 VPN，降級會照常進行，且後量子 IKEv2 VPN 安全性設定選項將會刪除。
- 如果您已設定後量子 IKEv2 VPN，則會阻止降級，因為降級後的版本不支援後量子設定選項。當降級遭阻止時，會出現警告訊息，通知您移除後量子 IKEv2 VPN 設定，並選擇降級後要用於 VPN 的密碼。

  移除後量子 IKEv2 VPN 設定並選取密碼後，您可以繼續降級。

日誌檔案會保留降級後的後量子日誌。

後量子移轉規劃與準備

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

升級網路以抵抗後量子攻擊需要大量的規劃和準備，因為除了升級 VPN 之外，您還需要將經典加密套件轉移到後量子加密套件。這不僅要改變網路和防火牆，端點、應用程式、用戶端應用程式等也要進行完整的端對端移轉。這要大量投資在時間、研究和資源上。投資所需的規模取決於您的業務和網路。然而，與竊取您最有價值資產（例如財務資料、程式碼、PII 資料和其他容易受到現在收集，日後解密攻擊的潛在長期存活資料）的攻擊成本相比，投資成本很小。

此外，世界各地的監管機構、國家安全機構（例如 NSA）、政府和標準機關（例如 NIST）都要求或將要求政府機構以及一些商業部門（可能包括運輸和關鍵基礎設施）做好準備及防禦後量子威脅。準備轉移至後量子世界不是您是否應該做的問題，而是您何時做的問題。

那麼問題來了，什麼時候開始移轉呢？

何時應開始移轉取決於您的數位資產需求，尤其是因為「現在收集，日後解密」攻擊之故需要保護其隱私多久的時間，這類攻擊會記錄加密的資料，包括在 IKE 和 TLS 對等交握中傳輸的金鑰材料，目的是在攸關加密的量子電腦 (CRQC) 可用時解密擷取的資料。關鍵問題是，您的資料需要保護多久？如果攻擊者已經獲取敏感資料，且在 CRQC 發揮作用時該資料仍然有效，則攻擊者將能夠解密竊取的資料，並對其內容採取行動。CRQC 最快可能在下一個十年內推出。

如果您的公司是收集攻擊的潛在目標，那麼每延遲採取行動一天，就多一份風險讓攻擊者能夠收集更多資訊以供日後解密。越早採取行動，就能越早阻止攻擊者未來解密所收集的資料。

從歷史上看，過去大多數取代加密通訊協定的努力，例如從 3DES 轉移到 AES 加密，或從 SHA-1 轉移至 SHA-2 雜湊函數，都是在新標準制定後 5 到 20 年的時間完成的。這包括在現實世界中審查新通訊協定的時間。在 NIST 標準化後量子密碼編譯 (PQC) 後，即使 PQC 已經歷嚴格的測試，但可能需要 5 到 10 年在現實世界的實際經驗及破解 PQC 的嘗試，才能確信新的 PQC 是真正可靠的。

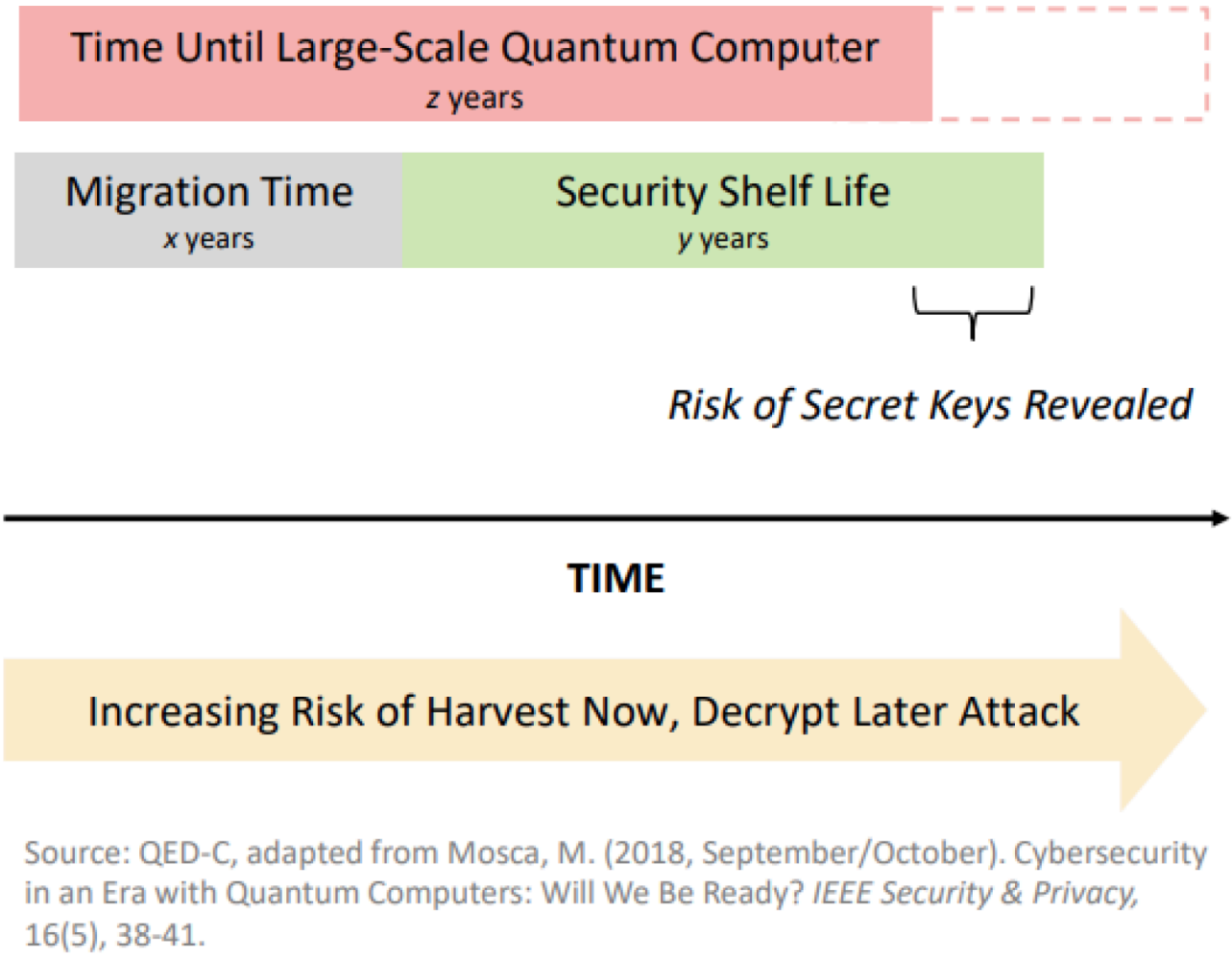
PQC 取代了經典密碼演算法，並為金鑰交換、加密和數位特徵碼提供量子抵抗力。

為了保障從經典加密轉移到新 PQC，業界採用混合金鑰。混合金鑰透過使用多種金鑰交換機制 (KEM) 技術建立加密金鑰，提供額外的安全層。最佳做法是使用強大的經典 KEM（例如 Diffie-Hellman Group 21）和一個或多個 PQC。如果用於建立金鑰的 PQC KEM 之一有弱點，其他 KEM 仍會保護該金鑰。在新 PQC 獲得足夠的實際經驗，能使業界對其安全強度充滿信心之前，混合金鑰是最好的前進方向。

「現在收集，日後解密」攻擊並不是唯一的後量子威脅。如果您不主動封鎖網路上未經授權的 PQC，內部精通技術的不良行為者便可以下載開放原始碼的 PQC，並在您的網路中啟動其 PQC 伺服器或瀏覽器外掛程式。

到 2030 年代初期，使用當今經典密碼編譯保護的資料很可能無法抵抗後量子攻擊。因此，請務必瞭解需要保護您資料多久的時間，並估計準備和執行後量子計劃需要多長時間的時間。越早開始，就越容易維持高品質和成本可預測，並避免隨著後量子威脅的增加而倉促完成整個過程。

考慮多久開始的一種方法是使用 Mosca 模型，它提供了一個簡單的時間軸，您可以在其中插入時間估計，以便您瞭解採取行動的緊迫性。



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.

這個 Mosca 模型展示如何估計資產後量子弱點的時間軸，並幫助您瞭解何時開始進行後量子準備。該模型會將您對移轉到後量子準備狀態所需時間的估計（*x*，可能至少五年），以及您對資料存活時間的估計（*y*，這是從您達成後量子準備狀態的時間，到就算暴露資料也不再會危害資料的時間），與 CRQC 可能可供使用的時間 (*z*) 進行比較。

(*x*+*y*) 和 *z* 之間的差異顯示了長期存活資料如果被收集後會有暴露風險的時間，或在長期資料有風險之前您有多少緩衝時間。這可以幫助您瞭解需要多長的時間開始或可能會延遲多久的時間。如果 (*x*+*y*) 大於 *z*，則這些時間軸之間的差異是如果攻擊者已透過「現在收集，日後解密」攻擊獲取您的資料，該資料可能會暴露的時間，如上圖中密碼金鑰洩漏風險所示。

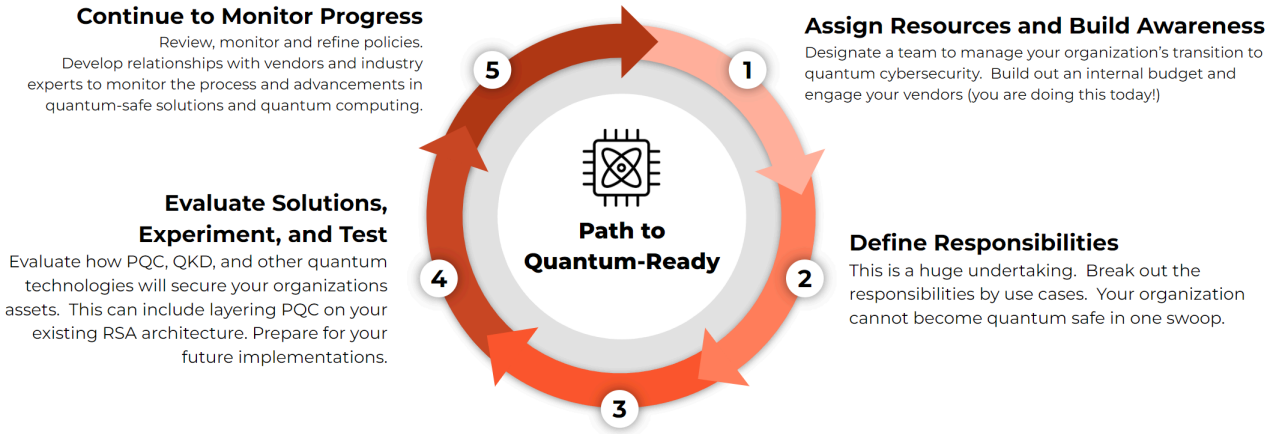
當您開始轉移規劃時，您可以立即執行以下幾項操作來強化現有 VPN 連線：

- 遵循 RFC 6379《*IPsec* 的套件 *B* 加密套件》，將您的 VPN 連線升級成嚴格的密碼套件。使用 Suite-B-GCM-256 並避免使用較弱的 128 位元 AES 演算法，這些演算法容易受到 Grover 演算法的攻擊。
- 將您的 CA 升級到 4K RSA 金鑰大小，以減輕會破壞較小金鑰大小的暴力密碼破解，並將您的 VPN 憑證驗證轉移到新憑證。
- 升級至更高位元的 SHA 雜湊大小，例如 SHA-384 和 SHA-512。停止使用如 MD5 和 SHA-1 等弱式雜湊。
- 實作 RFC 8784 和/或 RFC 9242 和 RFC 9370 以建立可抵抗量子攻擊的後量子 VPN。

此外，檢查您的 SSL/TLS 連線並加以強化：

- 將 SSL/TLS 連線升級為嚴格的密碼套件；將 TLSv1.3 與完美轉送密碼 (PFS) 的密碼結合使用。
- 在強化的用戶端到伺服器 VPN 工作階段中，建立 SSL/TLS 工作階段通道。使用後量子桌面應用程式來支援反向 Proxy。

為了開始轉移，量子經濟發展聯盟 (QED-C) 開發了一個模型用於規劃和準備轉移至後量子安全性，Palo Alto Networks 已將該模型改編為五個步驟模型，以幫助您評估移轉準備、時間和資源。



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

以下幾段說明量子準備過程的每個步驟，第一步是實作 RFC 8784 以建立抗量子 IKEv2 VPN：

- 分配資源並建立意識
- 定義職責
- 制定密碼詳細目錄和優先順序清單
- 評估解決方案、試驗和測試
- 繼續監控進展

分配資源並建立意識

此規劃和準備階段的目標是確定轉移團隊，瞭解您需要哪些資源，讓廠商瞭解他們的後量子準備計劃，並開始瞭解涉及的成本。

為建立對後量子攻擊的抵抗力所進行的升級，通常與您的 *IT* 部門已經為實現網路現代化所做的工作吻合。

1. 組成專責的專案管理團隊，負責制定後量子策略和量子準備藍圖以管理轉移過程。該團隊負責高層規劃。此外該團隊還確定誰負責轉移過程中的網路部分。儘早開始，讓自己有足夠的時間採取經深思熟慮、謹慎的方法，以幫助確保能保持高品質且成本維持可預測。
2. 瞭解量子安全性技術，並理解要如何整合到您的環境中。後量子 IKEv2 VPN (RFC 8784) 是建立安全後量子網路的第一步，您現在可以在不影響網路的情況下執行這一步。此外，所有組織都需要用量子安全 PQC 取代現有的非對稱演算法。若要採取後續步驟，請瞭解 PQC、混合金鑰和多重金鑰交換（RFC 9370 和 9242）。亦請瞭解密碼靈活性（使用多個 PQC，以便在 PQC 受到危害時您能夠輕鬆快速地在 PQC 之間切換）、量子金鑰分配 (QKD) 和量子亂數產生器 (QRNG)，以瞭解是否能證明這些安全措施能夠保護您的資料。

   研究量子技術並讓您的廠商瞭解他們的量子準備計劃以及這對您的業務有何影響。
3. 讓企業社群參與，並深入瞭解 PQC 及技術意識和準備程度。培養團隊和團隊領導者的意識，幫助他們知道潛在的變化以及為什麼需要這些變化。例如，與採購團隊合作納入後量子需求，以確保新的硬體和軟體與 PQC 相容且基礎設施防過時。

   發起密碼探索活動（您或許能夠利用稽核文件），來瞭解並找出組織目前依賴哪些易受後量子攻擊的數位特徵碼和密碼編譯，例如 Diffie-Hellman (DH)、橢圓曲線密碼編譯 (ECC)、橢圓曲線 Diffie-Hellman (ECDH)、AES-128、小於 4K 的 RSA 加密等。
4. 開始編列內部預算。隨著您深入瞭解來調整預算，並制定適合您業務的最佳解決方案。

定義職責

找出網路每個部分的負責人，包括網路、檔案和資料加密、軟體應用程式、端點、IAM、應用程式伺服器等。將職責分配給每個領域的團隊成員，並確保他們瞭解轉移的原因、急迫性和價值。後量子弱點會影響所有現有的非對稱加密。團隊成員應該明白，依優先順序探索、分類和升級網路中的所有一切，需要付出巨大的努力。

制定密碼詳細目錄和優先順序清單

密碼詳細目錄是網路中所有一切的完整清單—網路中的每個裝置、系統、程式碼、應用程式、平台和廠商，以及各自使用的密碼編譯—網路套件、用於 TLS、SSH 和 VPN 的版本、憑證管理、加密金鑰產生、金鑰大小和金鑰儲存空間等。密碼詳細目錄必須是全方位的，因為 PQC 對整個端對端資料路徑（包括所有類型的端點、應用程式和伺服器）構成威脅。這意味著您需要規劃完整的端對端移轉。

密碼詳細目錄不僅列出元件，除了元件本身和每個元件使用的密碼編譯之外，還提供每個元件的相關資訊。對於每個元件，詳細目錄中包含誰使用該元件、元件中儲存了哪些資料、如何保護元件，以及資料如何在元件之間移動。目標是瞭解網路中使用的加密類型、加密保護的資料、資料的儲存

位置、資料的去向，與所涉及裝置和使用者的所有資訊。簡言之，這是有關網路密碼編譯及其影響所有一切的完整詳細目錄。

如果沒有全面的密碼編譯詳細目錄，您就無法識別網路中所有受影響的元件、評估其風險，或有效地確定首先升級的優先順序。

若要建立密碼詳細目錄，請調查並記錄密碼使用情況（I.T. 和 SecOps 通常可以幫助解決此情況）：

- 使用什麼密碼編譯—目前使用的密碼和通訊協定。
- 誰或什麼使用每個密碼和密碼通訊協定。
- 密碼使用位置—密碼保護的資料、伺服器、瀏覽器、VPN、遠端應用程式等。確定誰在使用資料、資料周遊網路的哪些部分，以及如何端對端保護資料。
- 按每個網路元素的風險進行分類。
- 確定所需的資料隱私權持續時間和資料的預期生命週期，以協助評估因收集攻擊而遺失資料的風險。

將廠商和合作夥伴納入密碼詳細目錄。例如，訪問廠商以瞭解其應用程式中使用的密碼編譯，與金鑰的強度及其產生方式。確定誰在使用資料以及如何端對端保護資料。不要留下可讓攻擊者在後量子攻擊中利用的漏洞。

在建立密碼詳細目錄時，您也許能夠利用稽核、網路增強、零信任等方面所進行的工作。

開發您的密碼詳細目錄可能是轉移中最困難的部分。好消息是，詳細目錄可以培養意識，甚至幫助組織在量子威脅出現之前變得更加安全，因為詳細目錄可以識別陳舊和過時的系統。

Palo Alto Networks 提供多種工具來幫助您取得密碼詳細目錄：

- 解密、流量和威脅日誌顯示網路上執行的加密通訊協定、這些通訊協定適用的裝置和使用者等。
- 內容版本 8692 中的弱點保護設定檔特徵碼可以偵測日誌中的 PQC 使用情況並發出警示。您可以設定弱點保護設定檔，以自動封鎖網路上未經認可的 PQC，這是最佳做法。（為內部 PEN 測試制定所需的例外情況。）
- 使用 SSL 解密自動封鎖防火牆無法解密的密碼。

評估密碼詳細目錄中項目的風險並確定安全選項，以便您可以安排移轉的優先順序：

- 瞭解您的數據和應用程式：
  - 識別高優先順序和高隱私的資料。
  - 根據安全性和風險分類資料。
  - 指派隱私權持續時間（資料的存活時間有多長，有效時間就有多長）。
  - 瞭解應用程式如何保護其資料。
  - 知道誰在使用資料。

- 瞭解您的端點。
  - 資料儲存在何處以及如何保護？
  - 哪些伺服器託管和提供資料？
  - 使用者使用什麼裝置來存取資料？
  - 如何保護端點？
- 認識您的網路。
  - 資料如何透過網路移動？
  - 哪些裝置保護資料？
  - 是否涉及雲端？如何保護雲端中的資料？
  - 哪些網路區域是高風險的？
- 瞭解您的安全性選項及需要在何處套用後量子緩解措施。
  - 您需要移轉到更新的通訊協定嗎？
  - 您應該使用哪些 PQC 以及何時使用？（注意 NIST PQC 標準。）
  - 您需要使用混合金鑰來保護您的資料嗎？
  - 如何確保具有密碼靈活性（能夠在 PQC 中發現弱點時快速切換密碼演算法）。
  - 您需要使用 QRNG 或 QKD 嗎？
  - 什麼時候需要轉移到後量子憑證和驗證？
  - 這些選項是否符合您的合規性需求？

當您瞭解您的密碼詳細目錄時，請分析資料並根據資料設定移轉優先順序。設定優先順序時，請考量防禦收集攻擊的資料生命週期、資料的位置和敏感度，以及資料易受攻擊的程度。如今，金鑰交換面臨最高的風險，因此實作 RFC 8784 和/或 RFC 9242 和 RFC 9370 來建立抗量子 VPN 是首要工作。

若要設定移轉優先順序：

- 依業務影響對任務進行排名。該資產對您的業務有多重要？需要保護資料的安全或隱私多久的時間—資產是否面臨「現在收集，日後解密」的風險？將風險資產的資本價值與估計未來因後量子攻擊所造成遺失資料的成本進行比較
- 首先移轉受影響高的區域。
- 定義補救措施。
- 設定移轉時間軸和政策。
- 投入資源並資助活動。

評估解決方案、試驗和測試

利用密碼詳細目錄中的資訊制定政策、移轉計劃和測試計劃，以將您的網路轉移至後量子準備狀態，並保護您的資料。包含廠商、合作夥伴及對網路安全性的任何其他外部影響。制定解決方案政策和移轉計劃：

- 識別必須升級到 PQC 的資產。

  確定每個優先順序層級需要哪些技術，並判定技術對移轉策略適配程度。
- 建立一個轉移計劃，其中確定當您以 PQC 取代或增強經典演算法時，在目前和日後最適合保護您資產的演算法。
- 制定金鑰生命週期策略以反映非對稱和對稱加密金鑰的風險，特別是對於面臨「現在收集，日後解密」攻擊風險的長期存活資料。
- 在您的政策和計劃中納入實作密碼靈活性。密碼靈活性可確保如果演算法（經典或 PQC）受到危害，您可以快速輕鬆地轉向安全的演算法。

請明白，這是一個深思熟慮的轉移，而不是焦土式的推倒重來。在完全轉移到 PQC 完成之前，您可能需要採用混合方法，並將 PQC 與經典加密演算法結合，以增強安全性。

若要測試計劃和政策，請建立概念驗證實驗室，以便您可以：

- 徹底測試所有 PQC 元件及裝置和應用程式之間的互通性。
- 瞭解經典演算法和 PQC 演算法之間的效能和功能差異。與經典密碼編譯相比，PQC 具有更大的金鑰大小和數位特徵碼大小，這會導致加密後的檔案大小更大，也可能影響延遲。

  測試元件之間的 PQC 互通性，並嘗試最大化端對端量子抵抗力，不僅是在組織內部，還有在外部各方之間。找出對每個使用案例最有意義的演算法，並建立一個轉移計劃以用 PQC 取代經典密碼編譯。
- 進行端到端測試，並包含合作夥伴、廠商和其他其後量子準備情況可能會影響您網路的外部各方。某些系統可能需要升級，才能具有可接受的後量子效能。
- 確定需要升級的不相容元件和資產。

實驗也是在組織中培養意識的另一種方法，同時也回答有關轉移難易度的問題並提供相關資訊。如果您沒有內部專業知識或無法在合理的時間內培養內部專業知識，請尋求外部專家意見。

繼續監控進展

持續監控和評估抗量子環境的進展，以幫助確保轉移能按表進行，並降低收集攻擊的風險。視需要對計劃和涉及的人員進行調整。此外，與專家合作以協助確保您能涵蓋所有的基礎，不會留下攻擊者在未來量子攻擊中可利用的漏洞。

抵抗後量子攻擊的最佳做法

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

現在您可以實作許多最佳做法來防禦由量子電腦發動的後量子攻擊，包括防禦現在收集，日後解密攻擊。「現在收集，日後解密」攻擊會擷取加密資料和金鑰交換材料，其目的是之後使用攸關加密的量子電腦 (CRQC) 透過加速Shor 演算法來解密該材料，該演算法會將金鑰材料進行因式分解，以找到加密金鑰所基於的大質數。

這些最佳做法包括：

- 後量子轉移規劃最佳做法
- 密碼編譯最佳做法
- VPN 設定最佳做法

後量子轉移規劃最佳做法

從經典密碼編譯轉移至後量子密碼編譯，可能需要五年甚至更長的時間。僅規劃就可能需要數年時間。請透過以下方式讓自己取得最大優勢：

- 儘早開始—如果您的公司擁有長期存活的資料，而且是收集攻擊的潛在目標，那麼每延遲採取行動一天，就多一份風險讓攻擊者能夠收集更多資訊以供日後解密。越早採取行動，就能越早阻止攻擊者收集資料以供未來解密。
- 利用現有資源—當您取得 密碼詳細目錄時，請利用您已經為稽核、零信任、網路增強和其他活動完成的工作。
- 自我教育—瞭解量子運算威脅、後量子密碼編譯 (PQC)、強化網路抵禦量子攻擊的技術和方法，以及可用於保護網路的全新與新興 PQC。熟悉政府命令、計劃、法律、RFC 和其他資訊來源。

密碼編譯最佳做法

隨著量子電腦演變成 CRQC 而變得越來越快，應提高經典加密套件的強度，使攻擊者更難以暴力破解方式將金鑰解密。不是 CRQC 的量子電腦速度可能仍然夠快，足以破解較弱的加密。

- 遵循 RFC 6379《*IPsec* 的套件 *B* 加密套件》，將您的 VPN 連線升級成嚴格的密碼套件。使用 Suite-B-GCM-256 並避免使用較弱的 128 位元 AES 演算法，這些演算法容易受到 Grover 演算法的攻擊。
- 將您的 CA 升級到 4K RSA 金鑰大小，以減輕可能破壞較小金鑰大小的暴力密碼攻擊。
- 將您的 VPN 憑證驗證移轉到金鑰大小更大的新憑證。
- 升級至更高位元的 SHA 雜湊大小，例如 SHA-384 和 SHA-512。停止使用如 MD5 和 SHA-1 等弱式雜湊。

- 將 SSL/TLS 連線升級為嚴格的密碼套件；將 TLSv1.3 與完美轉送密碼 (PFS) 的密碼結合使用。
- 在強化的用戶端到伺服器 VPN 工作階段中，建立 SSL/TLS 工作階段通道。
- 設定您的弱點保護設定檔，以針對您未解密的流量封鎖未認可的 PQC。對於您解密的流量，請使用解密設定檔封鎖未認可的 PQC（解密設定檔僅允許您啟用的密碼，防火牆會封鎖所有其他密碼）。未認可的 PQC 表示可能有違規或內部不良的行為者試圖使用 PQC 危害您的網路。視需要為您的內部 PEN 測試團隊設定例外狀況。

VPN 設定最佳做法

設定後量子 IKEv2 VPN 時，請使其儘可能地抵抗量子攻擊：

- 實作 RFC 8784 以建立可抵抗量子攻擊的 IKEv2 VPN。
- 實作 RFC 9242 和 RFC 9370 以建立可抵抗量子攻擊的 IKEv2 VPN。

> *RFC 8784* 可與 *RFC 9242* 和 *RFC 9370* 搭使用，以提供額外一層的保護層，並可以滿足加密靈活性的需求。

RFC 8784 最佳做法：

- 不要使用 IKEv1。IKEv1 被認為是弱式通訊協定，不支援後量子 VPN。如果兩個 IKE 對等體皆可以支援，請將您的 VPN 連線升級到 IKEv2，並在設定 IKE 閘道時（**Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道） > **General**（一般）），選取 **IKEv2 only mode**（僅 **IKEv2** 模式）。
- 只要您知道兩個對等體皆支援 RFC 8784，請將 **Negotiation Mode**（交涉模式）設定為 **Mandatory**（強制）。使用 **Mandatory**（強制）模式可確保 VPN 能夠抵抗後量子攻擊，且攻擊者無法立即收集資料並於日後使用執行 Shor 演算法的 CRQC 解密資料。

  > 如果有足夠的處理能力，*Shor* 演算法便可以在使用非對稱加密的 *IKEv2* 交握中破解動態金鑰交換。然而，*Shor* 演算法無法破解 *IPSec* 通道對稱加密。若要保護對稱 *IPSec* 加密，請使用 *AES-256* 來防範 *Grover* 演算法，並使用上一節密碼編譯最佳作法中建議的更強雜湊和金鑰長度。

  與外部裝置進行對等互連時，請嘗試確定該對等體是否支援 RFC 8784，並與其他管理員合作使用相同的 PQ PPK 進行連線，以便您可以使用強制模式。
- 手動指定或自動產生 PPK 密碼，長度至少為 64 個字元（32 位元組或 256 位元熵），以建立強式金鑰。您可以手動指定或自動產生最長 128 個字元（64 位元組，512 位元熵）的 **PPK Secret**（**PPK** 密碼）。PPK 密碼越長，熵位數便越多，這使得 PPK 密碼更難破解。

  熵位元數提供後量子安全性一半的位元數。例如，256 位元熵提供 128 位元的後量子安全性，512 位元熵提供 256 位元的後量子安全性。至少 256 位元熵可提供相當於 NIST 後量子密碼

編譯提案徵集中定義的 Category 5 安全性。RFC 8784 的安全注意事項部分提供有關熵以及有多少熵就足夠的更多詳細資訊。

只有在您設定或自動產生 *PPK* 密碼時，該密碼才會以純文字顯示。設定或產生 *PPK* 密碼並離開以純文字顯示密碼的畫面後，該密碼將不再以純文字形式顯示，以協助防止金鑰洩漏。

複製 *PPK* 密碼和 *KeyID* 配對並安全地保存。如果您在設定或產生金鑰時未儲存金鑰，則以後無法擷取該金鑰。（如果需要，您可以刪除 *PQ PPK* 並再設定另一個。）

處理 PQ PPK 的其他最佳做法包括：

- 建立多個作用中 PQ PPK。使用多個作用中金鑰（而不僅僅是一個）可以為金鑰交換期間的金鑰選擇增加隨機元素。
- 確保每個 IKEv2 對等體皆具有完全相同的一組已啟動 PQ PPK（KeyID 加 PPK 密碼配對），來交涉金鑰交換。
- 如果 Panorama 管理對等體，請設定 PQ PPK 並將其推送到管理的防火牆，以便更輕鬆、更快速且更自動地進行設定。
- 如果您需要將 PQ PPK 傳達給其他管理員，請使用加密的安全通訊方法，例如加密的電子郵件。
- 安全地儲存 PPK 密碼字串。請勿將其保留在便利貼上或未經授權的管理員可能會發現的任何地方。

NSA 發佈了預先共用金鑰安全處理方式指引，包括 *RFC 8784* 量子預先共用金鑰。

RFC 9242 與 **RFC 9370** 最佳做法：

- 不要使用 IKEv1。IKEv1 被認為是弱式通訊協定，不支援後量子 VPN。如果兩個 IKE 對等體皆可以支援，請將您的 VPN 連線升級到 IKEv2，並在設定 IKE 閘道時（**Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道） > **General**（一般）），選取 **IKEv2 only mode**（僅 **IKEv2** 模式）。
- 當您設定 IKE 密碼設定檔時（**Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼） > **General and Advanced Options**（一般與進階選項）），使用強式經典 KEM（例如 Diffie-Hellman Group 20 和以上）建立混合金鑰，並在額外的 KEM 輪次中，例如 Kyber-768 (ML-KEM)，建立至少一個 PQC。
- 對於敏感資訊，僅使用安全性強度層級為 L3 或更高層級的 PQC。新增至金鑰建立程序中的每個額外 PQC 都會增強金鑰抵抗量子攻擊的能力，但也會增加 IKEv2 對等互連程序的延遲和開銷。一般而言，新增安全性層級 L3 PQC 會使 IKEv2 金鑰交換增加約 20 到 30 毫秒，而新增安全性層級 L5 PQC 則會增加 40 到 60 毫秒。使用較大金鑰的更強式 PQC（例如 Classic McEliese）可能會增加超過 800 毫秒的金鑰交換時間，並引起高度分散。熟悉 PQC 金鑰大小和安全性強度，以便為您的 VPN 通訊選取最佳的 PQC。
- 與管理對等 VPN 裝置的管理員協調每個金鑰交涉輪次中使用的 PQC。當在每個選用金鑰交涉輪次中，以相同的 PQC 設定位於通道兩端的兩個 VPN 裝置時，可以最大限度地減少互通性問

題。嘗試將 PQC 及其安全性強度達成一致，以確保雙方皆設有相同的參數。對於同一個組織下管理的防火牆，可以使用中央管理工具來確保每個金鑰交涉輪次有一致的設定和 PQC 選擇。

- 啟用加密靈活性，以在轉移到純 PQC 環境期間保護您的資料。此轉移可能需要長達 5 到 10 年的時間，業界才會完全信任新的 PQC。
  - 對於必須使用由 NIST 標準化並經 FIPS 核准的 PQC 的組織，可以透過啟用 RFC 8784 以及 RFC 9242 和 RFC 9370，來達成加密靈活性。如果混合金鑰中使用的 PQC 有弱點，則 RFC 8784 中使用的 PPK 字串仍然可以提供量子抵抗，以防止收集攻擊成功。
  - 對於獲允許同時使用 NIST 標準化和非標準化 PQC 的組織，可以透過使用至少兩個具有強式經典 KEM 的 PQC（例如 Diffie-Hellman Group 21），來達成加密靈活性。理想情況下，PQC KEM 應使用不同的數學技術，其中一個 KEM 以晶格為基礎，另一個則以代碼或其他非晶格技術為基礎。或者，還可以使用混合金鑰啟用 RFC 8784，以增加額外一層的安全並擴展加密靈活性。
- 將金鑰生命週期值從預設值減少到較低的值，可促使加速重設金鑰。
- 設定 IPSec 密碼設定檔時，啟用 IPSec 以使用混合金鑰（**Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼） > **General and Advanced Options**（一般與進階選項））。IPSec 通道的兩端必須設定為在每個額外的金鑰交換輪次中使用相同的 PQC 和安全性強度。

深入瞭解後量子安全性

後量子安全性、後量子技術和建議的後量子實作尚處於起步階段。當您計劃在後量子運算的世界中保護您的資產時，請務必盡量地瞭解會影響您業務的後量子技術、政府規章和命令，以及如何轉移到後量子 VPN 和密碼。

美國政府和世界各國政府正在制定計劃，以因應量子電腦和後量子密碼編譯帶來的量子安全性威脅。此外，美國國家標準暨技術研究院 (NIST) 和網際網路工程任務組 (IETF) 等標準機構正在為新的後量子技術及其實作方式制定標準。

本主題提供資訊連結，幫助您加深對業務中後量子安全性的理解、準備和轉移。

- 美國政府
- 全球其他政府
- RFC
- 技術和一般資訊

美國政府

許多國家的政府正在制定計劃、命令和法規，來因應量子運算威脅和後量子密碼編譯出現。以下連結提供有關美國政府如何解決該問題的資訊，包括美國國家標準暨技術研究院 (NIST) 和美國國家安全局 (NSA) 的資訊連結。查看當地政府的安全性網站和組織，以瞭解您的政府如何實現後量子安全性。

- NIST 後量子密碼編譯資源中心提供有關後量子密碼編譯標準化和其他材料的資訊。
- NIST 國家網路安全卓越中心 (NCCOE) 移轉至後量子密碼編譯提供移轉到後量子密碼編譯的指引。
- NSA 中央安全署的對稱金鑰管理需求附件 *V2.1* 提供將預先共用金鑰用於商業解決方案 (CSfC) 的實作需求。
- 美國國土安全部後量子密碼編譯網站包含該部門的後量子藍圖和其他資源。
- 網路安全暨基礎設施安全局 (CISA) 的後量子密碼編譯倡議將其他政府機構和產業合作夥伴聯合進行後量子工作，以因應量子運算威脅。該網站還提供 CISA、NIST 和美國國土安全部中更多資源的連結。
- 為了鼓勵將聯邦政府資訊技術系統移轉到抗量子密碼編譯，拜登總統簽署了量子運算網路安全法案 (HR 7535)。
- 美國總統行政辦公室發布的執行備忘錄 M-23-02《移轉至後量子密碼編譯》，為美國機構遵循國家安全備忘錄 10 (NSM-10)《促進美國量子運算領域地位並降低易受攻擊之密碼系統風險國家安全備忘錄》提供指引。

全球其他政府

以下連結提供有關世界各地政府如何處理該問題的資訊。

- 德國聯邦資訊安全辦公室 (BSI) 提供有關後量子密碼編譯、移轉策略、目前發展和建議，以及其他材料的相關資訊。
- 英國政府提供有關量子電腦與技術、量子電腦威脅、國家量子策略、量子金鑰分配、量子亂數產生和其他材料的資訊。
- 法國網路安全局 (ANSSI) 提供有關後量子轉移、量子金鑰分配和其他材料的資訊。
- 荷蘭情報與安全總局 (AIVD) 提供有關量子電腦威脅、後量子移轉策略與步驟、量子金鑰分配和其他材料的資訊。
- 歐盟網路安全局 (ENISA) 提供有關後量子密碼編譯、混合實作、後量子策略和其他材料的資訊。
- 新加坡金融管理局提供有關量子計劃及解決與量子相關網路安全風險的資訊。
- 日本政府提供有關量子策略、量子安全性和移轉至量子技術的資訊。

RFC

提案需求書 (RFC) 描述網際網路的技術基礎。一些 RFC 描述 IKEv2 抵抗量子電腦攻擊的各個層面：

- RFC 8784《在網際網路金鑰交換通訊協定版本 *2 (IKEv2)* 中混合預先共用金鑰以實現後量子安全性》描述 IKE 延伸模組標準，該標準使 IKEv2 能夠抵抗來自量子電腦的攻擊。RFC 8784 如何抵抗量子運算威脅 總結 RFC 8784 在您網路中的影響。
- RFC 6379《*IPsec* 的套件 *B* 加密套件》描述您應該使用的 Suite-B-GCM-256 位元演算法，而不是較弱的 AES-128 位元加密。移除 AES-128 等弱式密碼有助於延遲 Grover 演算法破解對稱加密的時間。
- RFC 9370《網際網路金鑰交換通訊協定版本 *2 (IKEv2)* 中的多個金鑰交換》描述如何延伸 IKEv2 以允許混合多個金鑰交換來建立加密金鑰。
- RFC 9242《網際網路金鑰交換通訊協定版本 *2 (IKEv2)* 中的中繼交換》定義一種中繼交換機制，該機制能夠在初始金鑰交換中傳輸大量資料，例如基於多個金鑰交換的加密金鑰。這有助於避免分段。（某些裝置不允許分段。）
- RFC 7383《網際網路金鑰交換通訊協定版本 *2 (IKEv2)* 訊息分段》允許在 IKE 層級對 IKE 訊息進行分段，從而消除因 IP 分段造成的問題。但是，RFC 7383 不適用於初始交換。RFC 9242 有助於避免初始交換中的分段，RFC 7383 可避免後續 IKEv2 訊息中的 IP 分段。

技術和一般資訊

許多組織認識到量子電腦和某些技術所帶來的潛在威脅，這些技術在經典電腦上執行時不會造成危險，但在攸關加密的量子電腦 (CRQC) 上執行時可能會造成災難性的危險

- Open Quantum Safe 組織的 liboqs 網站是一個量子安全加密演算法的開放原始碼 C 函數庫。
- Linux 基金會的後量子密碼學聯盟專案旨於透過生產標準化演算法的高安全性軟體實作，來解決量子運算帶來的加密安全性挑戰。
- 當與 CRQC 一起使用時，Shor 演算法可能會破壞當今使用的許多經典非對稱加密演算法。Shor 演算法會將大的複數分解為質數，這些質數是經典非對稱加密的基礎。

- Grover 演算法是一種量子二次方加速非結構化搜尋演算法。與 CRQC 一起使用時，可以透過暴力密碼破解將 AES 演算法和雜湊函數的加密強度減半，來破壞經典對稱加密演算法。
- 現在收集，日後解密攻擊是目前活躍的威脅。在「現在收集，日後解密」攻擊中，攻擊者會竊取他們現在無法解密的資料，並將其保存起來，直到 CRQC 可以將其解密為止。今日，這些攻擊正在發生中，並對長期存活的資料構成直接威脅。
- Quantum Inspire 知識庫文章「什麼是量子位元？）解釋量子位元。
- Deloitte 文章「密碼編譯的量子威脅）」討論您為什麼應儘快開始進行後量子轉移的原因，Forbes 文章「密碼編譯的量子威脅：不要驚慌，但現在就做好準備」中也有相同的討論。
- *ETSI* 量子安全密碼編譯 *(QSC)*：量子安全移轉的可重複架構」為建立後量子移轉計劃提供了一個很好的範本。
- 世界經濟論壇量子經濟藍圖提供以公平方式建構量子生態系統，以轉移至量子經濟的藍圖。

設定抗量子 IKEv2 VPN

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

基於 RFC 8784 和/或 RFC 9242 與 RFC 9370 的抗量子 IKEv2 VPN 可防止嘗試執行「現在收集，日後解密」攻擊的攻擊者竊取用於加密 VPN 中資料的加密金鑰材料。如果沒有加密金鑰，攻擊者日後便不能使用攸關加密的量子電腦解密所收集的資料。即使攻擊者成功竊取加密的資料，但沒有攸關加密的量子電腦來解密金鑰材料，他們也無法入侵收集的資料，因為沒有金鑰，他們便無法將其解密。

RFC 8784 可供將量子抵抗力從現今的經典密碼編譯轉移到您現在就可以實作的後量子密碼編譯。RFC 8784 不需要密碼編譯升級，因此只要通道兩端的 VPN 裝置皆支援它，就能簡單快速地加以實作。

RFC 9242 和 RFC 9370 比 RFC 8784 更耗費資源，但所提供的動態金鑰產生功能是採用不易受 Shor 演算法攻擊的新 PQC 數學演算法。由於 RFC 9242 和 RFC 9370 需要密碼編譯升級，因此部署混合金鑰技術可能需要更長時間，所以您需要考慮加密靈活性。

本章向您展示如何設定後量子 IKEv2 VPN，包括如何在您知道 IKEv2 對等體及其功能的情況下，以及不控制 IKEv2 對等體且不知道其功能的情況下，設定後量子 IKEv2 VPN。

- 使用 RFC 8784 PPK 設定後量子 IKEv2 VPN 向您展示後量子 IKEv2 VPN 設定步驟和選項，以使用後量子預先共用金鑰來保護 VPN 通訊。
- 使用 RFC 9242 和 RFC 9370 混合金鑰設定後量子 IKEv2 VPN 向您展示使用混合金鑰保護 VPN 通訊的設定步驟與選項。
- 後量子 IKEv2 RFC 8784 設定範例 提供了一個簡單拓撲範例，以及如何為該拓撲設定後量子 IKEv2 VPN 支援。

除了根據 *RFC 8784* 設定後量子 *IKEv2 VPN* 之外，請遵循 RFC 6379《*IPsec* 的套件 *B* 加密套件》，將 *VPN* 連線升級為嚴格的密碼套件，將 *CA* 升級為 *4K RSA* 金鑰大小，以減緩會破壞較小金鑰大小的暴力密碼破解攻擊，亦將 *VPN* 憑證驗證移轉到新憑證，並升級到較高位元的 *SHA* 雜湊大小，如 *SHA-384* 和 *SHA-512*。

使用 RFC 8784 PPK 設定後量子 IKEv2 VPN

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

基於 RFC 8784 的後量子 IKEv2 VPN 透過從初始對等交換（IKE_SA_INIT 交換）單獨（頻外）傳輸預先共用金鑰來運作。對等交換不會在對等交換中傳輸預先共用金鑰（攻擊者會現在入侵或收集金鑰，日後再解密），而只會傳輸金鑰 ID。金鑰 ID 和預先共用金鑰組成唯一的配對，稱為後量子預先共用金鑰 (PQ PPK)。

每個 IKEv2 對等體會使用金鑰 ID 來查閱預先共用金鑰，該金鑰會在管理員之間安全地傳輸或由 Panorama 推送，並儲存在每個 IKEv2 對等體的本機上。預先共用金鑰永遠不是對等交換的一部分，也永遠不會周遊後量子 VPN，因此使用量子電腦的攻擊者無法竊取、破解並使用該金鑰來解密從 VPN 收集的資料。

兩個 IKEv2 對等體必須具有相同的作用中金鑰 ID 與預先共用金鑰配對，以便在對等體交涉連線時，每個對等體都可以查閱相同的金鑰 ID，並擷取相同的預先共用金鑰。如果回應的對等體沒有符合的金鑰 ID，或與金鑰 ID 相關聯的預先共用金鑰和起始者的不同，則連線會中止。

先設定 IKEv2 對等互連與 IPSec 通道，再設定後量子元件。此外，請確保您的安全性政策允許防火牆之間的 *IKEv2* 和 *IPSec* 流量，並啟用日誌記錄。

若要讓您的 IKEv2 VPN 抵抗量子攻擊：

STEP 1 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），然後 **Add**（新增）新閘道。

STEP 2 | 設定 **General**（一般）頁籤設定，並選取 **IKEv2 only mode**（僅 **IKEv2** 模式） 或 **IKEv2 preferred mode**（**IKEv2** 慣用模式）作為**Version**（版本）。

在 **IKEv2 only mode**（僅 **IKEv2** 模式）下，如果對等體不支援 IKEv2，防火牆會中止連線。在 **IKEv2 preferred mode**（**IKEv2** 慣用模式）下，如果對等體不支援 IKEv2，防火牆會退回到 IKEv1。但是，VPN 必須交涉 IKEv2 才能使用後量子 VPN 功能，因此如果防火牆回退到 IKEv1，這些功能將不可用。

IKEv1 被認為是弱式的。如果兩個 *IKE* 對等體皆可以支援，請將您的 *VPN* 連線升級到 *IKEv2*，並選取 ***IKEv2 only mode***（僅 ***IKEv2*** 模式），以確保有足夠的安全性層級和使用 *PQ VPN* 的能力。

STEP 3 | 選取 **Advanced Options**（進階選項），然後設定非量子選項。

如果您選取了 **IKEv2 preferred mode**（**IKEv2** 慣用模式）作為 **Version**（版本），則會有 **IKEv1** 和 **IKEv2** 的頁籤；請選取 **IKEv2**。如果您選取 **IKEv2 only mode**（僅 **IKEv2** 模式）作為 **Version**（版本），則只有 IKEv2 選項會顯示。

選取 **PQ PPK**（後量子預先共用金鑰）以設定 IKEv2 VPN 的後量子元素。（**General**（一般）可讓您新增 IKE 密碼設定檔及設定 **Liveness Check**（活性檢查）。）

STEP 4 | **Enable Post-Quantum Pre-Shared Key (PPK)**（啟用後量子預先共用金鑰 **(PPK)**）以允許在 VPN 上使用後量子抵抗功能。此選項預設為停用。

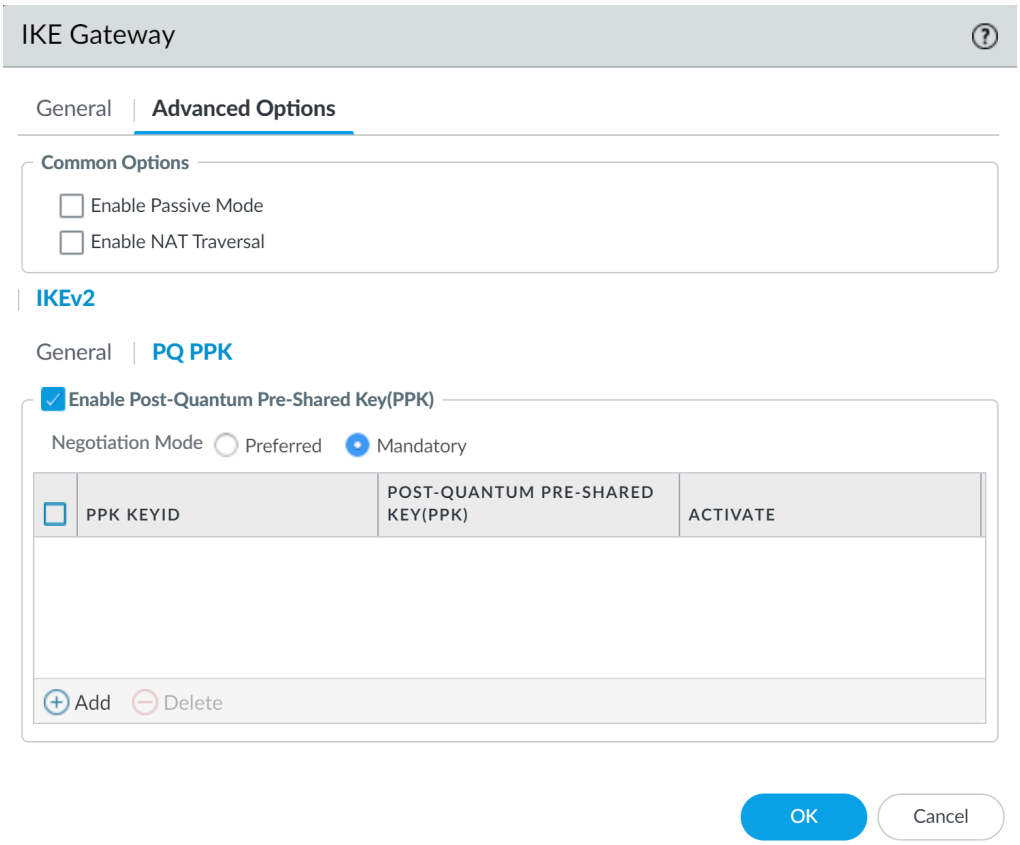
當您 ***Enable Post-Quantum Pre-Shared Key (PPK)***（啟用後量子預先共用金鑰 ***(PPK)***）時，必須設定並啟動至少一個 *PQ PPK*，以便防火牆具有可在 *IKEv2* 交涉期間使用的 *PQ PPK* 並支援 *RFC 8784*。

STEP 5 | 將 **Negotiation Mode**（交涉模式）設為 **Preferred**（慣用）或 **Mandatory**（強制）。

- **Preferred**（慣用）—當防火牆與對等體交涉時，防火牆會先嘗試使用 PQ PPK 進行交涉。如果對等體不支援 RFC 8784，防火牆會回退到經典的金鑰交換來進行連線。如果您不知道或無法控制對等體是否支援 RFC 8784，則 **Preferred**（慣用）模式會保留回溯相容性，以確保連線會回退而不是中斷。**Preferred**（慣用）是預設模式。

- **Mandatory**（強制）—當防火牆與對等體交涉時，對等體必須支援 RFC 8784 PQ PPK。如果回應的對等體不支援 RFC 8784，則防火牆會中止連線。當您知道對等體支援 RFC 8784 PQ PPK 時，請使用 **Mandatory**（強制）模式。

為了獲得最佳安全性，請儘可能使用 ***Mandatory***（強制）模式。



STEP 6 | **Add**（新增）並 **Activate**（啟動）最多十個唯一 PQ PPK。

PQ PPK 由兩個成對元素組成：PPK KeyID 和 PPK 密碼。PPK KeyID 是可識別 PPK 密碼的唯一字串，可以是最多 31 個字元的任何字串，例如 **`PPK-1`** 或 **`Super Strong PPK`**。PPK 密碼是隨機的預先共用金鑰，永遠不會透過 VPN 傳輸，因為兩個對等體的管理員皆使用安全的通訊方

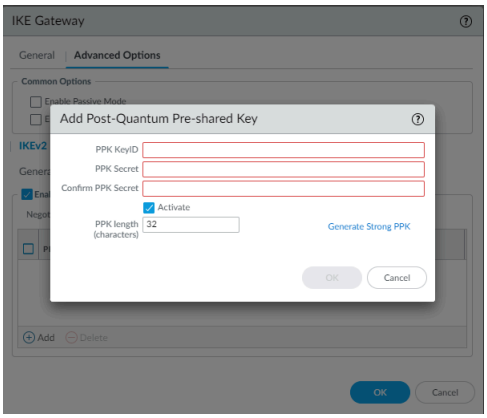
法共用金鑰，並將其設定在頻外的對等體上。防火牆僅在 IKEv2 VPN 中傳輸 KeyID，以便對等體可以在本機查閱 PPK 密碼。

您可以定義的 PQ PPK 數量取決於 IKE 對等體可以支援的項目。一些廠商的實作允許不到 10 個的唯一 PQ PPK；有些實作甚至只允許一個。不要定義多於對等體可以支援的 PQ PPK，因為兩個對等體必須具有完全相同的可用 PQ PPK。

為支援多個 *PQ PPK* 的對等體設定多個作用中 *PQ PPK*。防火牆會從作用中 *PQ PPK* 之中隨機選擇，這為 *IKEv2* 交涉新增隨機性元素。

設定多個 PQ PPK 是最安全的，因為它為 PQ PPK 選擇新增隨機元素。

您可以手動建立 PPK 密碼，或使用防火牆為您產生強式密碼。如果您想自行產生金鑰或從對等體的管理員收到 PQ PPK，並需要設定在防火牆上，請手動設定 PPK 密碼。PPK 密碼越長，熵位數便越多，這使得 PPK 密碼更難破解。



若要手動設定 PPK 密碼，您可以使用 ASCII 字元指定：

1. 指定最多 31 個字元的唯一 **PPK KeyID**。
2. 指定一個唯一、隨機的 **PPK Secret**（**PPK** 密碼）字串。該字串可以是 32-128 個字元長（16-64 個位元組，相當於 128-512 位元熵）。

   指定長度至少為 *64* 個字元（*32* 位元組，或 *256* 位元熵）的 ***PPK Secret***（***PPK*** 密碼），以建立強式金鑰。
3. 在 **Confirm PPK Secret**（確認 **PPK** 密碼）中指定完全相同的字串。

   安全地儲存 *PPK* 密碼。*PPK* 密碼不會以純文字顯示，因此如果您現在不儲存該密碼，以後便無法擷取它。（如果需要，您可以刪除 *PQ PPK* 並再設定另一個。）由於 *IKEv2* 對等體必須具有相同的 *PQ PPK*（*KeyID* 加上 *PPK* 密碼），因此您可能需要將 *PPK* 密碼傳達給其他管理員。若是如此，請確保所使用的通訊方法是以加密方式保護的，並確保安全地保存 *PPK* 密碼。

   NSA 發佈了預先共用金鑰安全處理方式指引，包括 *RFC 8784* 量子預先共用金鑰。

4. **Activate**（啟動）預設為已選取，讓防火牆可以使用 PPK KeyID 和 PPK 密碼配對 (PQ PPK) 與對等體交涉。如果您不希望防火牆在與對等體交涉時使用此 PPK KeyID 和 PPK 密碼配對，請取消勾選 **Activate**（啟動）。

   例如，如果您在防火牆上設定新的 PQ PPK，您可能會想要將其停用，直到對等體的管理員可以將相同的 PQ PPK 新增到對等體，以避免連線失敗為止，因為起始者使用的 PQ PPK 尚未安裝在對等體上。

5. 按一下 **OK**（確定）。**PQ PPK** 頁籤以純文字顯示 PPK KeyID，隱藏預先共用金鑰，並顯示 PQ PPK 的啟動狀態。

若要使用防火牆的自動產生強式 PPK 功能（使用十六進位字元）設定 PPK 密碼：

1. 指定最多 31 個字元的唯一 **PPK KeyID**。
2. 將 **PPK length (characters)**（**PPK** 長度（字元））設為您想要為 **PPK Secret**（**PPK** 密碼）產生的長度。預設值為 32 個字元（16 位元組）。

   將 ***PPK length (characters)***（***PPK*** 長度（字元））設為至少 *64* 個字元（*32* 位元組或 *256* 位元熵），以產生強式金鑰。

3. 按一下 **Generate Strong PPK**（產生強式 **PPK**）。防火牆會產生並顯示 **PPK length (characters)**（**PPK** 長度（字元））中指定長度的強式 PPK 密碼。

   這是 *PPK* 密碼唯一一次以純文字顯示。如果您未安全地保存該密碼，便無法擷取它。（如果需要，您可以刪除 *PQ PPK* 並再設定另一個。）由於 *IKEv2* 對等體必須具有相同的 *PQ PPK*（*KeyID* 加上 *PPK* 密碼），因此您可能需要將 *PPK* 密碼傳達給其他管理員。若是如此，請確保所使用的通訊方法是以加密方式保護的，並確保安全地保存 *PPK* 密碼。

   複製 PPK 密碼，按一下 **OK**（確定），然後貼到 **PPK Secret**（**PPK** 密碼）和**Confirm PPK Secret**（確認 **PPK** 密碼）欄位。

4. **Activate**（啟動）預設為已選取，讓防火牆可以使用 PPK KeyID 和 PPK 密碼配對 (PQ PPK) 與對等體交涉。如果您不希望防火牆在與對等體交涉時使用此 PPK KeyID 和 PPK 密碼配對，請取消勾選 **Activate**（啟動）。

   例如，如果您在防火牆上設定新的 PQ PPK，您可能會想要將其停用，直到對等體的管理員可以將相同的 PQ PPK 新增到對等體，以避免連線失敗為止，因為起始者使用的 PQ PPK 尚未安裝在對等體上。

5. 按一下 **OK**（確定）。**PQ PPK** 頁籤以純文字顯示 PPK KeyID，隱藏預先共用金鑰，並顯示 PQ PPK 的啟動狀態。

STEP 7 | 按一下 **OK**（確定）以建立 VPN。

STEP 8 | **Commit**（提交）組態。

此後量子 IKEv2 RFC 8784 設定範例主題提供了一個簡單拓撲範例，以及如何為該拓撲設定後量子 *IKEv2 VPN* 支援。

STEP 9 | 如果您不是兩個 IKEv2 對等體的管理員，請將 PQ PPK（KeyID 加上 PPK 密碼）安全地傳達給對等體的管理員，以便安裝在對等體上。安全地傳達與保存 PQ PPK 對於保護資料安全至關重要。

兩個 *IKEv2* 對等體必須具有相同的作用中 *Key ID* 和相關聯的預先共用金鑰，才能建立後量子 *VPN* 連線。

使用 RFC 9242 和 RFC 9370 混合金鑰設定後量子 IKEv2 VPN

這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.2 或更新版本。

基於 RFC 9242 和 RFC 9370 的後量子 IKEv2 VPN 其工作原理是，在初始對等交換（IKE_SA_INIT 交換）中使用兩個或多個金鑰交換機制 (KEM) 建立混合金鑰。混合金鑰透過防止受危害的 KEM 允許使用「現在收集，日後解密」(HNDL) 進行的量子攻擊得逞，進而提供抵抗量子的能力。只要用於建立混合金鑰的所有 KEM 不被洩漏，資料仍然受到保護。

由於這些標準相對上仍較新，並且每個廠商對其實作的標準可能有不同的解釋，因此保持雙方有相同的設定有助於讓事情變得簡單，並使後量子 VPN 通道能夠成功建立。為了最大程度地減少互通性的機會，請確保 在每輪次的選用金鑰交涉中，皆以相同的 PQC 和安全性強度設定 VPN 通道的兩端。另請檢查兩端的 IKEv2 分段設定，以確保其設定正確。

先設定 IKEv2 對等互連與 IPSec 通道，再設定後量子元件。此外，請確保您的安全性政策允許防火牆之間的 *IKEv2* 和 *IPSec* 流量，並啟用日誌記錄。

為了確保資料長期受到保護，應使用兩個以上的 KEM，且您可以透過 RFC 8784 啟用預先共用金鑰，並透過 RFC 9242 和 RFC 9370 啟用混合金鑰，來進一步新增深度防禦。

若要讓您的 IKEv2 VPN 抵抗量子攻擊：

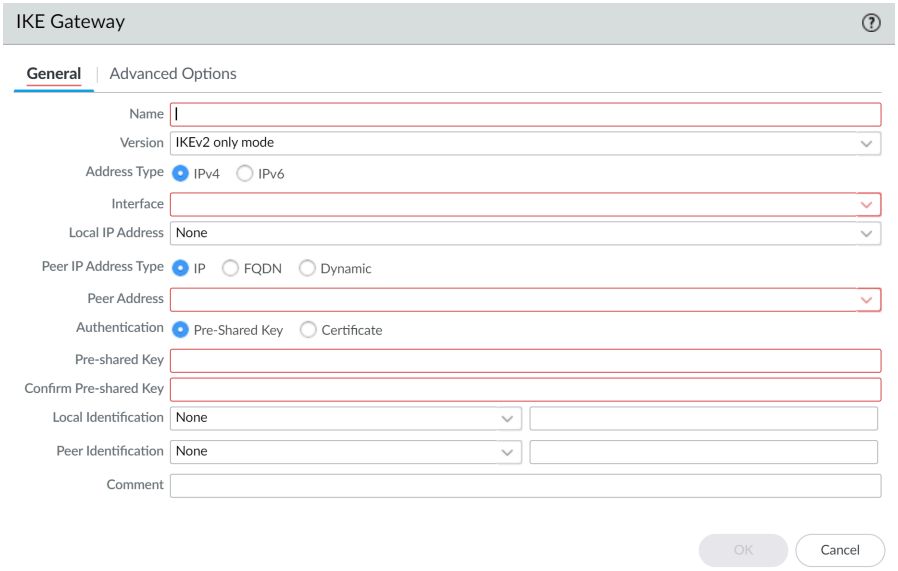
STEP 1 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），然後 **Add**（新增）新閘道。

STEP 2 | 設定 **General**（一般）設定，並選取 **IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 慣用模式）作為 **Version**（版本）。

在 **IKEv2 only mode**（僅 **IKEv2** 模式）下，如果對等體不支援 IKEv2，防火牆會中止連線。
在 **IKEv2 preferred mode**（**IKEv2** 慣用模式）下，如果對等體不支援 IKEv2，防火牆會退回

到 IKEv1。但是，VPN 必須交涉 IKEv2 才能使用後量子 VPN 功能，因此如果防火牆回退到 IKEv1，這些功能將不可用。

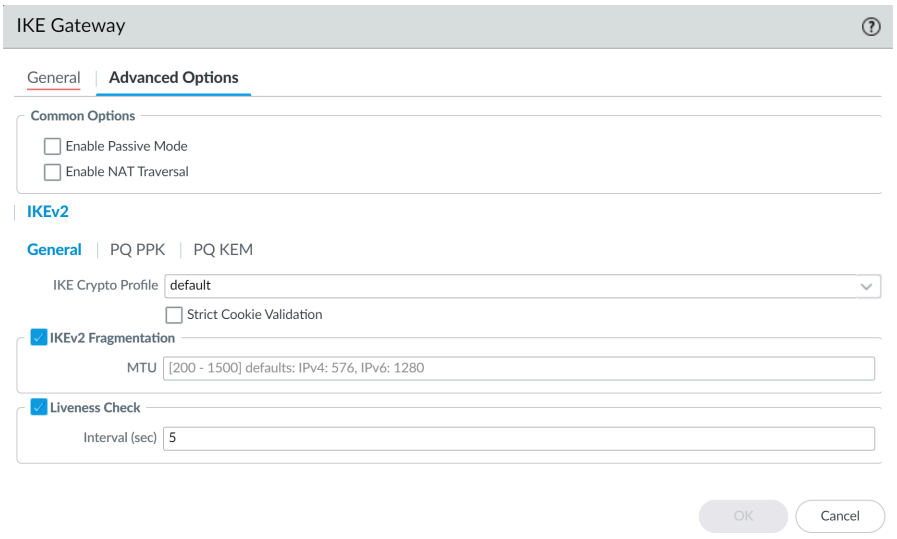
IKEv1 被認為是弱式的。如果兩個 *IKE* 對等體皆可以支援，請將您的 *VPN* 連線升級到 *IKEv2*，並選取 ***IKEv2 only mode***（僅 ***IKEv2*** 模式），以確保有足夠的安全性層級和使用 *PQ VPN* 的能力。



STEP 3 | 選取 **Advanced Options**（進階選項），然後設定非量子選項。選取 **IKEv2**，並設定 **General**（一般）設定。

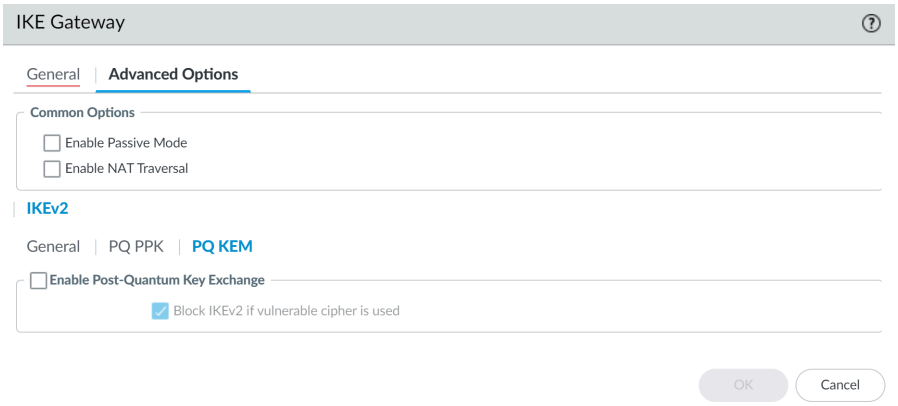
[General（一般）] 可讓您新增 IKE 密碼設定檔、啟用 **IKEv2 Fragmentation**（**IKEv2** 分段），以及設定 **Liveness Check**（活性檢查）。

使用 PQC KEM 時應啟用 [IKEv2 Fragmentation（IKEv2 分段）]，因為金鑰大小和資料有效負載較大。兩個 VPN 終端裝置應設定為相同的分段值。



STEP 4 | 針對 PQ KEM **Enable Post-Quantum Key Exchange**（啟用後量子金鑰交換），以允許在 VPN 上使用後量子抵抗功能。此選項預設為停用。

或者，啟用 **Block IKEv2 if vulnerable cipher is used**（如果使用易受攻擊的密碼，則封鎖 **IKEv2**）。當此選項已啟用時，如果防火牆偵測到 IKE 密碼設定檔中正在使用易受攻擊的 KEM，則會封鎖所有新的 IKEv2 對等互連。先前建立的現有 VPN 通道可以繼續。

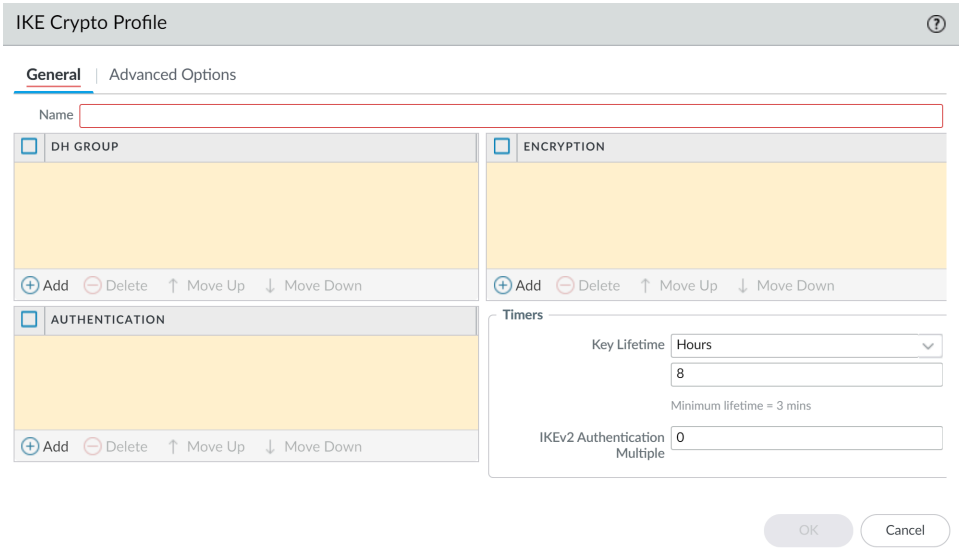


STEP 5 | 按一下 **OK**（確定）以建立 IKE 閘道。

STEP 6 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼），然後選取 **Add**（新增）新的設定檔。

STEP 7 | 設定 **General**（一般）設定，然後選取預設 IKEv2 金鑰交換的加密元件（DH 群組、加密、驗證、計時器）。

選取強大的經典金鑰交換設定，以提高量子抵抗性。*DH Group 20* 或以上、*AES-256-GCM*，並使用金鑰生命週期更頻繁地重新整理金鑰。若要按特定間隔完全重新產生金鑰，請透過設定大於零的值來啟用 *IKEv2* 驗證倍數。達到金鑰生命週期的倍數後，將重新產生金鑰。



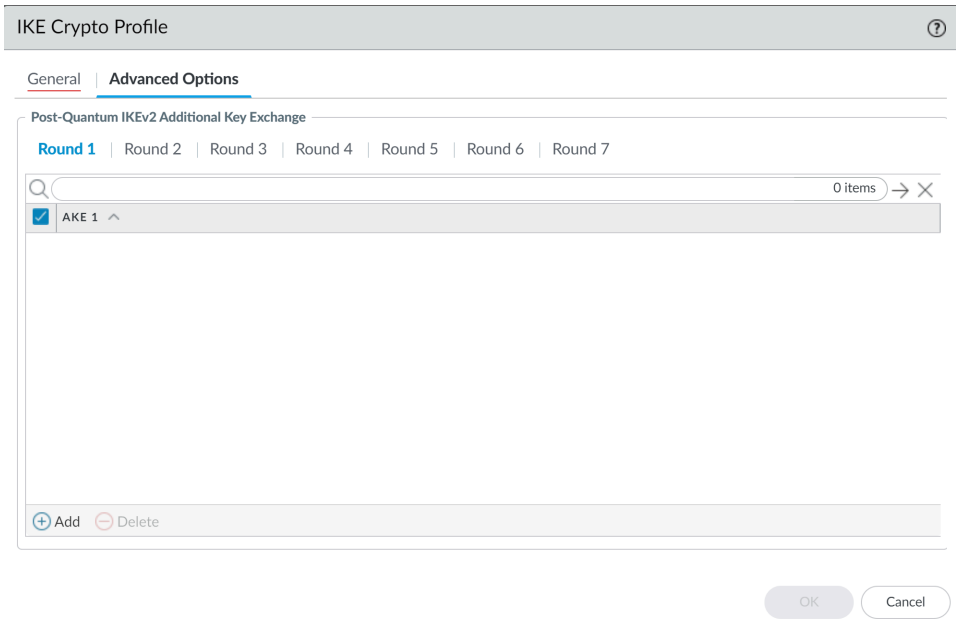
STEP 8 | 選取 **Advanced Options**（進階選項），然後設定選用的 **Post-Quantum IKEv2 Additional Key Exchange**（後量子 **IKEv2** 額外金鑰交換）輪次。

在 RFC 9370 中允許最多七次的 **Additional Key Exchange Rounds**（額外金鑰交換輪次）（第 1-7 輪）。至少需要一個 PQC KEM 來增加量子抵抗力。增加額外的 PQC KEM 會進一步提高量子阻力，但會提高交涉開銷並增加 IKEv2 封包的大小。

RFC 9370 允許略過額外的金鑰交換輪次。對於略過的輪次，會保留空白或設定為 **None**（無）。

在 [Additional Key Exchange Round（額外金鑰交換輪次）] 中的 PQC 順序會設定偏好設定。頂端列出的 PQC 是慣用的，如果通道另一端的 VPN 終端裝置支援它，就會選取該 PQC。如果您想交涉兩端皆支援的最強 PQC，請將安全層級最高的 PQC 置於每個額外金鑰交換輪次清單的頂部。

通道兩端的 *VPN* 終端裝置應設定為相同的 *PQC* 和安全性強度，以最大限度減少互通性問題。若要長期保護敏感訊息，請選取安全性強度相當於 *3* 級或更高層級的 *PQC*。

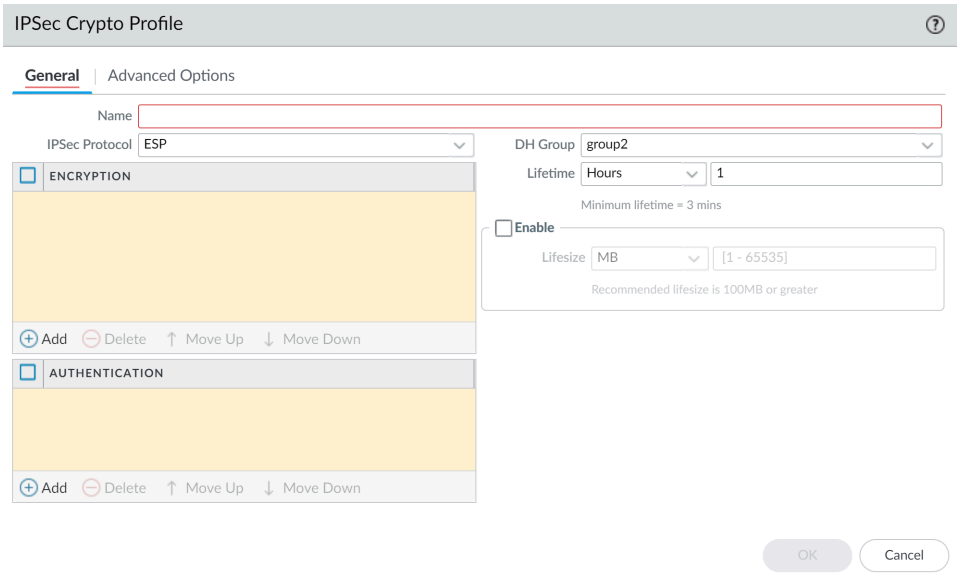


STEP 9 | 按一下 **OK**（確定）以建立 IKE 密碼設定檔。

STEP 10 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼），然後選取 **Add**（新增）新的設定檔。

STEP 11 | 設定 **General**（一般）設定，並為 IPSec ESP 通訊協定（加密、驗證、DH 群組、生命週期）選取加密元件。

選取強式經典加密設定來提高量子抵抗力。*DH Group 20* 或以上、*AES-256-GCM*、*SHA384* 或以上，並使用金鑰生命週期更頻繁地重新整理金鑰。

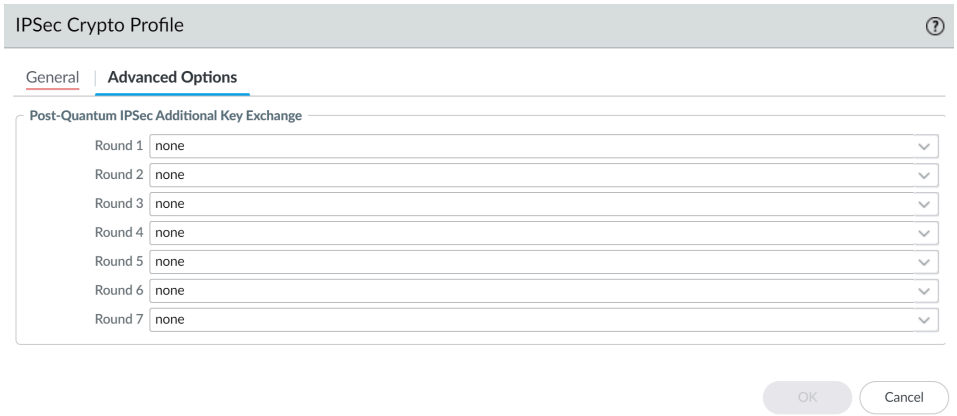


STEP 12 | 選取 **Advanced Options**（進階選項），然後設定選用的 **Post-Quantum IPSec Additional Key Exchange**（後量子 **IPSec** 額外金鑰交換）輪次。

允許最多七次的 **Additional Key Exchange Rounds**（額外金鑰交換輪次）（第 1-7 輪），每一輪次僅允許一個 PQC KEM。至少需要一個 PQC KEM 來增加量子抵抗力。增加額外的 PQC KEM 會進一步提高量子阻力，但會提高交涉開銷並增加 IPSec 重設金鑰封包的大小。

在每個額外的金鑰交換輪次中必須使用相同的 PQC 和安全性強度層級設定 IPSec 通道的兩端。如果不相符，則重設金鑰作業會失敗。

若要長期保護敏感訊息，請選取安全性強度相當於 *3* 級或更高層級的 *PQC*。



STEP 13 | 按一下 **OK**（確定）以建立 IPSec 密碼設定檔。

STEP 14 | **Commit**（提交）組態。

如果您不是兩個 *IKEv2* 對等體的管理員，請將 *IKEv2* 閘道、*IKE* 密碼設定檔和 *IPSec* 密碼設定檔資訊傳達給對等體的管理員，以便安裝在其對等裝置上。

後量子 IKEv2 RFC 8784 設定範例

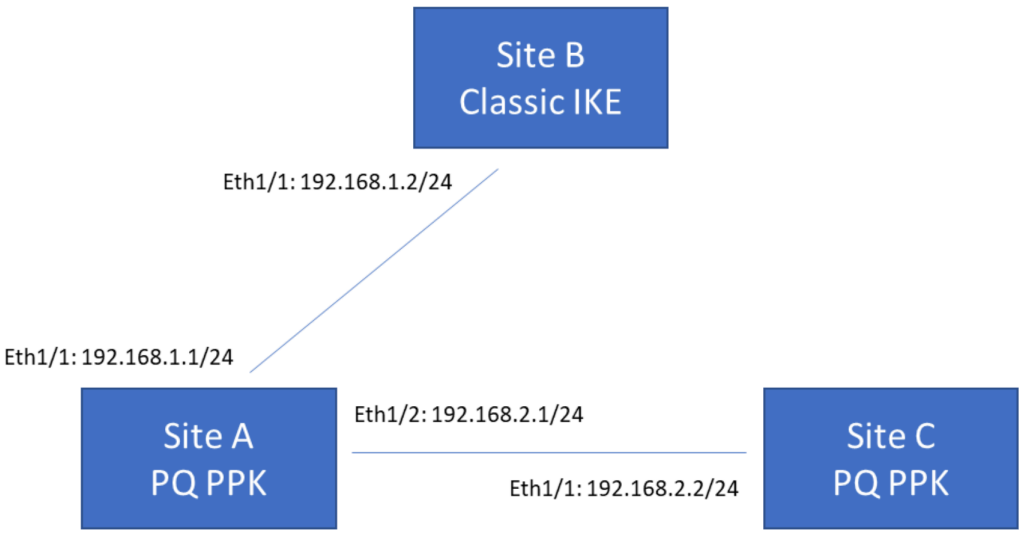
這可在何處使用？	我需要哪些內容？
• PAN-OS	❑ PAN-OS 11.1 或更新版本。

此範例提供基本的 IKEv2 後量子 VPN 設定和拓撲。它包括兩個支援 RFC 8784（抵抗量子電腦和量子密碼編譯攻擊的後量子 VPN）的站點，和一個不支援 RFC 8784 的站點。

當支援 RFC 8784 的防火牆與也支援 RFC 8784 的防火牆通訊時，裝置會使用後量子設定。金鑰交換使用從連線中頻外共用的後量子預先共用金鑰 (PQ PPK)，因此 PQ PPK 在 IKE 交握期間永遠不會暴露。防火牆將 PQ PPK 與經典的 Diffie-Hellmann (DH) 金鑰材料（在 IKE 交握期間傳輸）混合，以建立不基於質數的金鑰，因此無法被 Shor 演算法破解。這使得防火牆能夠建立抗量子的金鑰，以幫助防止現在收集，日後解密攻擊，在這種攻擊中，攻擊者會竊取他們現在無法解密的資料並將其保存起來，直到他們可以使用攸關加密的量子電腦 (CRQC) 解密為止。

當支援 RFC 8784 的防火牆與不支援 RFC 8784 的防火牆進行通訊時，RFC 8784 防火牆可以回退到經典 DH 金鑰交換。如果發生這種情況，防火牆不會混合 PQ PPK ，而僅使用 DH 金鑰材質來建立金鑰。重要的是要瞭解，在這種情況下， VPN 流量容易受到「現在收集，日後解密」攻擊。

此簡單範例拓撲由位於不同站點的三個防火牆組成，並透過 IKEv2 VPN 連線。其中兩個防火牆支援 RFC 8784，一個防火牆不支援 RFC 8784。



在本範例中：

- 站點 **A** 支援 RFC 8784。它與站點 B 的連線是 Eth1/1：192.168.1.1/24，與站點 C 的連線是 Eth1/2：192.168.2.1/24。站點 A 需要兩個 IKEv2 閘道，一個用於與站點 B 連線，另一個用於與站點 A 連線。

- 站點 **B** 僅支援經典 IKEv2 VPN，不支援 RFC 8784。它與站點 A 的連線是 Eth1/1：192.168.1.2/24。站點 B 需要一個 IKEv2 閘道才能連線到站點 A。站點 B 的 IKEv2 閘道設定不包括 PQ PPK，因為站點 B 不支援 RFC 8784。
- 站點 **C** 支援 RFC 8784。它與站點 A 的連線是 Eth1/1：192.168.2.2/24。站點 C 需要一個 IKEv2 閘道來連線到站台 A。

每個支援 *RFC 8784* 的 *IKEv2 VPN* 對等體必須安裝並啟動一組完全相同的 *PQ PPK*（*KeyID* 加上 *PPK* 密碼字串配對）。如果所選 *PQ PPK* 在兩個對等體上均不可用，便會中止連線。

KeyID 會識別 *PPK* 密碼字串。

IKEv2 對等體會在 *IKEv2* 交握期間傳輸 *KeyID*，但 *PPK* 密碼字串會在頻外共用並單獨安裝在每個對等體上（由 *Panorama* 推送或手動安裝）。*PPK* 密碼字串永遠不會在交握中傳送，也不會在產生的 *IKEv2* 通道中看到。相反的，*IKEv2* 對等體使用 *KeyID* 在本機查閱 *PPK* 密碼字串，並將其與 *DH* 金鑰材料混合以產生後量子加密金鑰。

若要為範例拓撲設定 IKEv2 VPN，請導覽至 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）：

STEP 1 | 像設定任何其他 IKE 閘道一樣，設定站點 A、B 和 C 的 IKEv2 VPN 閘道一般屬性。

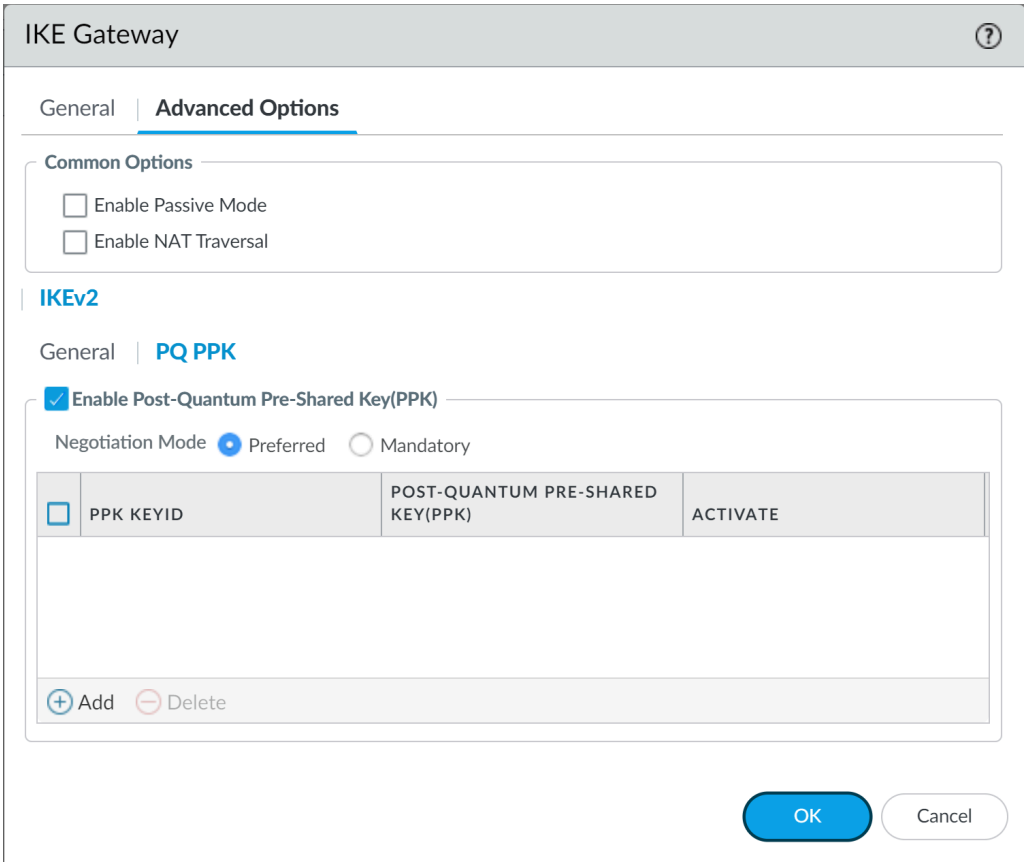
在 **General**（一般）頁籤中，設定位址、驗證與其他一般 IKE 閘道資訊。將 **Version**（版本）設為 **IKEv2 mode only**（僅 **IKEv2** 模式）以獲得最佳安全性。IKEv1 被認為是弱式通訊協定，不支援 RFC 8784 後量子 VPN。

您在 ***General***（一般）頁籤上設定的預先共用金鑰不是會抵抗基於量子之攻擊的後量子預先共用金鑰。它用於跨通道的對稱驗證。

STEP 2 | 為所有三個網站設定常見和一般的 **Advanced Options**（進階選項），例如被動模式、NAT 周遊和 IKE 密碼設定檔。

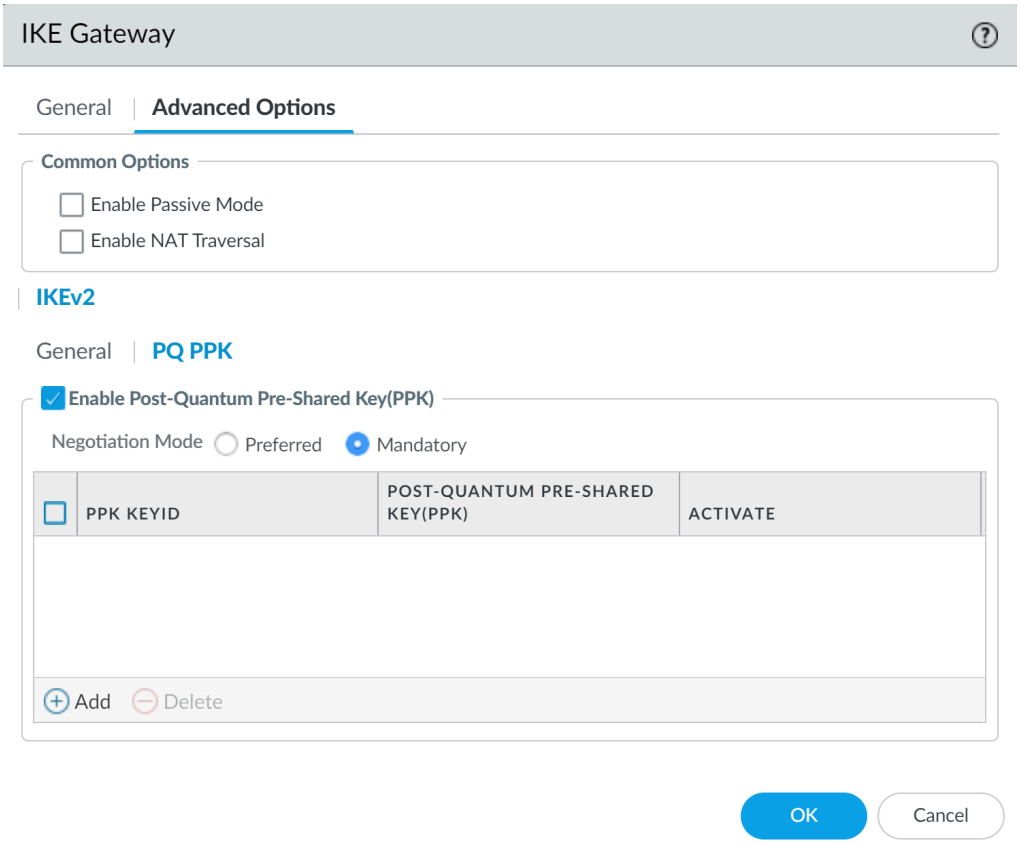
STEP 3 | 在 **Advanced Options**（進階選項）> **PQ PPK** 頁籤上，針對站點 A IKEv2 VPN 到站點 C 及站點 C IKEv2 VPN 到站點 A **Enable Post-Quantum Pre-Shared Key (PPK)**（啟用後量子預先共用金鑰 **(PPK)**）。

由於站點 B 不支援 RFC 8784，因此您無需在站點 B IKE 閘道設定或在站點 A IKEv2 VPN 到站點 B 設定中 **Enable Post-Quantum Pre-Shared Key (PPK)**（啟用後量子預先共用金鑰 **(PPK)**）。



當您 **Enable Post-Quantum Pre-Shared Key (PPK)**（啟用後量子預先共用金鑰 **(PPK)**）後，**Negotiation Mode**（交涉模式）預設設定為 **Preferred**（慣用），這表示無法支援 RFC 8784 的連線會回退使用經典密碼編譯。（在 **Mandatory**（強制）模式下，如果對等體不支援 PQ PPK，防火牆便會中止連線。）

STEP 4 | 將站點 A 到站點 C 和站點 C 到站點 A IKEv2 VPN 中的 **Negotiation Mode**（交涉模式）設為 **Mandatory**（強制）。



使用 **Mandatory**（強制）作為 **Negotiation Mode**（交涉模式），可確保站點 A 和站點 C 在交涉 VPN 通道時，一律設定抗量子的 VPN，而非經典 VPN。當您確定對等體支援 RFC 8784 時，請使用 **Mandatory**（強制）。如果您不確定，請使用 **Preferred**（慣用）模式，以便在對等體不支援 RFC 8784 時（例如，當您與企業外部不受您控制的裝置進行對等互連時），防火牆可以回退到經典 IKEv2 VPN。

STEP 5 | 為站點 A 到站點 C 的 IKEv2 連線以及站點 C 到站點 A 的 IKEv2 連線設定作用中 PQ PPK。當站點 A 和站點 C 啟動 IKEv2 連線時，它們會從這些作用中 PQ PPK 之間進行選擇，並將所選的 PQ PPK 與 DH 金鑰材料混合，以建立不基於質數的安全性金鑰。

站點 *A* 到站點 *B* 的通訊或站點 *B* 到站點 *A* 的通訊沒有後量子設定，因為站點 *B* 不支援 *RFC 8784*。

站點 A 和站點 C IKEv2 對等體必須具有完全相同的作用中 PQ PPK 設定。

- 如果 Panorama 管理兩個 IKEv2 對等體，您可以在 Panorama 上建立設定，並將其推送到受管理的防火牆。
- 如果 Panorama 不管理兩個 IKEv2 對等體，且由不同的管理員控制對等體，則請以安全的方式（例如加密電子郵件）將 PQ PPK 傳達給另一位管理員，並安全地保存金鑰。

您可以為每個 PQ PPK 的 KeyID 指定任何您想要的名稱。您可以手動為每個 PQ PPK 設定您要與 KeyID 配對的 PPK 密碼，或者防火牆可以為您產生強式 PPK 密碼。此範例向您展示如何使用這兩種方法。

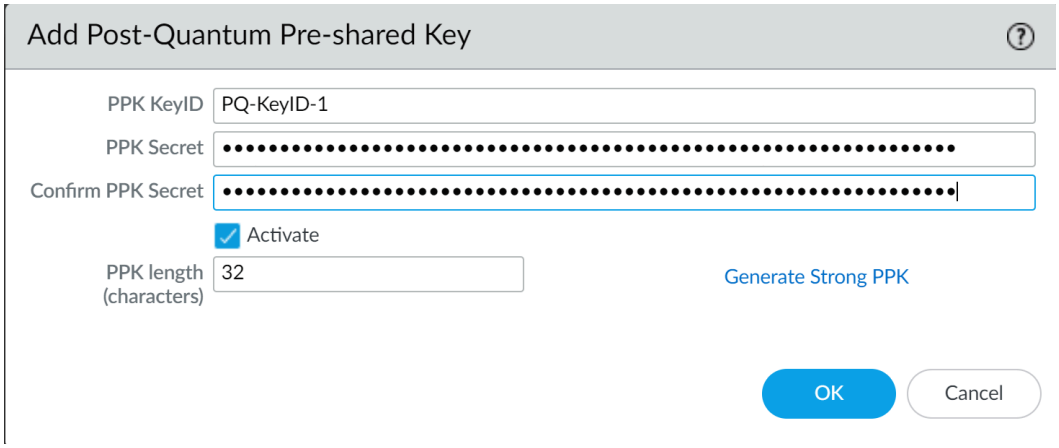
若要使用手動設定的 PPK 密碼建立 PQ PPK：

1. **Add**（新增） PQ PPK。
2. 在 **Add Post-Quantum Pre-shared Key**（新增後量子預先共用金鑰）對話方塊中，輸入 **PPK KeyID** 名稱。在此範例中，名稱為 **`PQ-KeyID-1`**。
3. 在 **PPK KeyID** 中輸入完全相同的 ASCII 字串（或從其他來源複製並貼上），然後 **Confirm PPK Secret**（確認 **PPK** 密碼）。

   安全地儲存 *PQ PPK*（*KeyID* 及其 *PPK* 密碼）。對於手動輸入的 *PPK* 密碼，該密碼永遠不會以純文字顯示。*PPK* 密碼一旦遺失，便無法復原。（您可以刪除 *PQ PPK*，然後設定新的 *PQ PPK*。）

   如果 **PPK KeyID** 和 **Confirm PPK Secret**（確認 **PPK** 密碼）不相符，則會出現錯誤訊息 `PPK Secret and Confirm PPK Secret Do Not Match`（`PPK` 密碼和確認 `PPK` 密碼不相符）。最佳做法是指定長度至少為 64 個字元（32 位元組或 256 位元熵）的隨機 PPK 金鑰來建立強式金鑰。新金鑰預設處於作用中狀態。如果您不想在 IKE 對等體之間的交涉中使用該金鑰，請取消選取 **Activate**（啟動）。如果您在一個對等體上停用

PQ PPK，則您也必須在另一個對等體上停用它。以下範例顯示一個 64 字元長的強式金鑰（手動輸入的金鑰永遠不會以純文字顯示）：



PPK length (characters)（***PPK*** 長度（字元數））欄位僅適用於防火牆為您產生的金鑰。它不會控制手動設定的 *PPK* 密碼字串長度。

4. 按一下 **OK**（確定）安裝手動設定的 PQ PPK。
5. 如果 Panorama 管理這兩個對等體，您可以在 Panorama 上建立設定，並將其推送到受管理的防火牆。如果 Panorama 不管理這兩個對等點，且 VPN 對等體由不同的管理員控制，您可以將 PQ PPK 以安全的方式傳達給那位將其安裝在對等體上的管理員。

若要使用防火牆產生的 PPK 密碼建立 PQ PPK：

1. **Add**（新增） PQ PPK。
2. 在 **Add Post-Quantum Pre-shared Key**（新增後量子預先共用金鑰）對話方塊中，輸入 **PPK KeyID** 名稱。在此範例中，名稱為 **`PQ-Key-ID-2`**。
3. 將 **PPK length (characters)**（**PPK** 長度（字元數））設定為至少 64 個字元（32 位元組或 256 位元熵），以建立強式金鑰。
4. 按一下 **Generate Strong PPK**（產生強式 **PPK**）。

   防火牆會產生一個強式的隨機十六進位 PPK 金鑰，其長度在 **PPK length (characters)**（**PPK** 長度（字元數））中設定。
5. 反白顯示並複製 PPK 密碼字串。

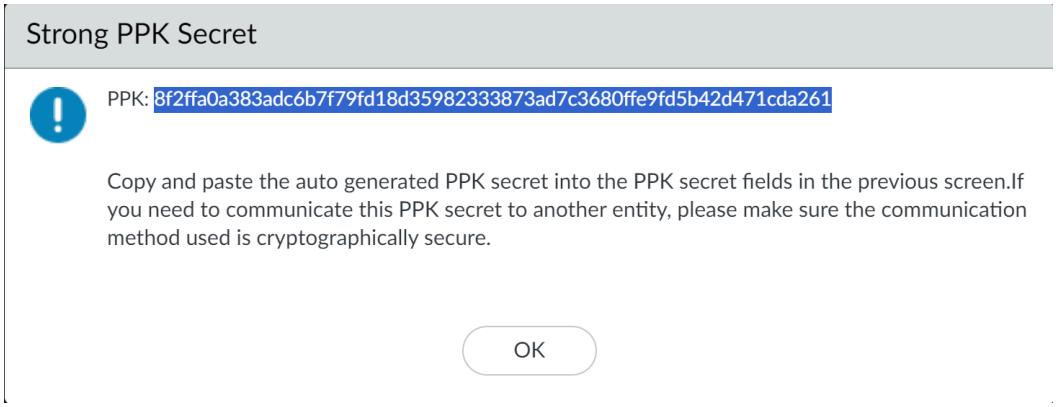
僅複製十六進位密碼。不要複製前置 *`PPK:`* 字元。例如，如果產生的 *PPK* 為：

`PPK:38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

您只需複製：

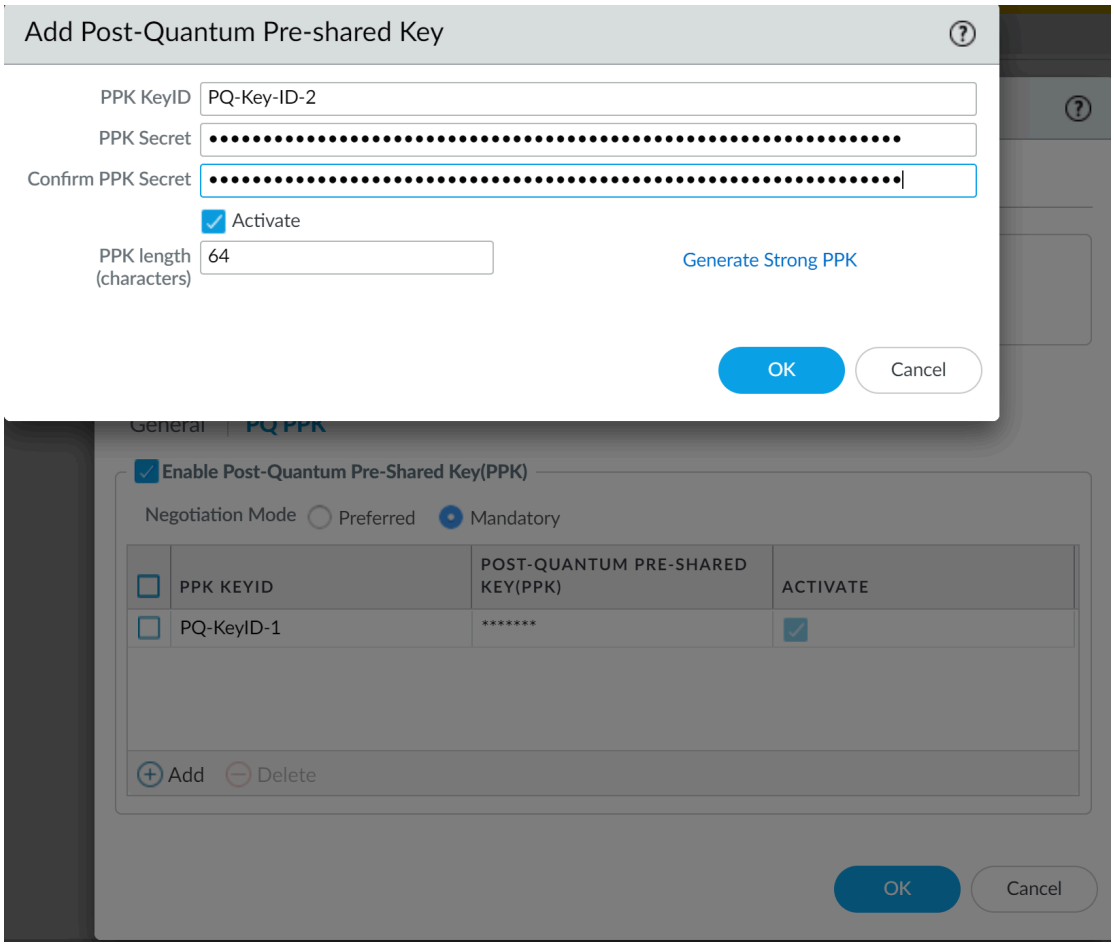
`38bcc7f9bd477885541ba0f12b93eb1b8e8ab772ccac1a891802a3abfe132b5d`

前置 *`PPK:`* 不是密碼字串的一部分。



安全地保存由防火牆產生的複製 PPK 密碼。按一下 **OK**（確定）後，防火牆再也不會以純文字顯示 PPK 密碼。如果您現在未複製並安全地保存 PPK 密碼，您將不會擁有該密碼，且需要刪除此 PQ PPK 並設定新的。

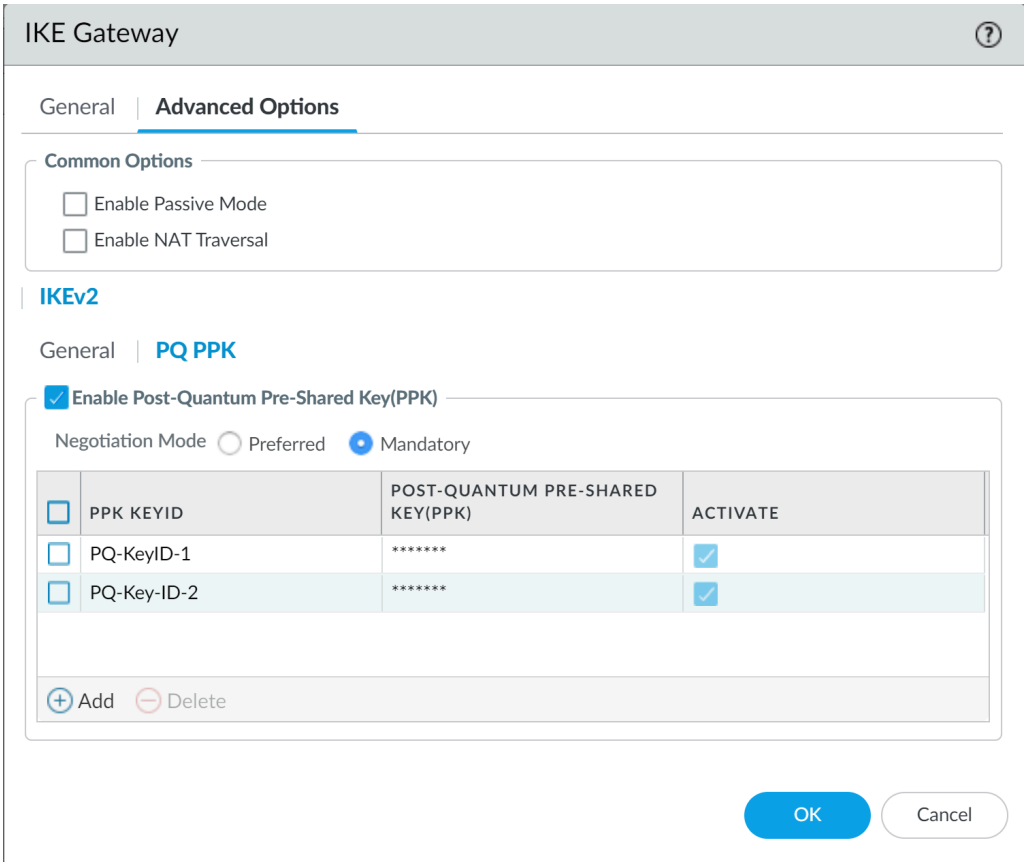
6. 當複製的 PPK 密碼仍在剪貼簿上或可從安全的儲存空間中複製時，按一下 **OK**（確定）。如果您沒有複製 PPK 密碼，請產生另一個強式 PPK 密碼，並確保複製並安全地儲存它。
7. 將複製的 PPK 密碼字串貼到 **Add Post-Quantum Pre-Shared Key**（新增後量子預先共用金鑰）中的 **PPK Secret**（**PPK** 密碼）和 **Confirm PPK Secret**（確認 **PPK** 密碼）欄位。



新金鑰預設處於作用中狀態。如果您不想在 IKE 對等體之間的交涉中使用該金鑰，請取消選取 **Activate**（啟動）。如果您在一個對等體上停用 PQ PPK，則您也必須在另一個對等體上停用它。

8. 按一下 **OK**（確定）安裝防火牆產生的 PQ PPK。
9. 如果 Panorama 管理這兩個對等體，您可以在 Panorama 上建立設定，並將其推送到受管理的防火牆。如果 Panorama 不管理這兩個對等點，且 VPN 對等體由不同的管理員控制，您可以將 PQ PPK 以安全的方式傳達給那位將其安裝在對等體上的管理員。

對於站點 A 和站點 C，本範例中建立的兩個 PQ PPK 在 **Mandatory**（強制）模式中列為作用中的 PQ PPK。



PPK 密碼現已隱藏，且永遠不會以純文字形式顯示。站台 A 和站台 C 之間的 IKEv2 VPN 現在實作 RFC 8784 以抵抗量子攻擊。站點 A 和站點 B 之間的 IKEv2 VPN 繼續使用經典的 DH 金鑰交換，且仍然容易受到「現在收集，日後解密」攻擊。

如果本範例中的站點 B 已升級為支援 RFC 8784，您可依照相同的程序將站點 A 升級至站點 B，並將站點 B 升級至站點 A IKEv2 VPN。