paloalto TECHDOCS

IPSec VPN 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

June 9, 2023

Table of Contents

IPSec VPN 基礎知識

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

virtual private network（虛擬私人網路 - VPN）可讓使用者和系統透過公共網路安全連線來建立通道，就像它們是透過區域網路 (LAN) 連線一樣。若要設定 VPN 通道，您必須有一對能夠互相驗證的裝置，並會加密彼此之間的資訊流量。這對裝置可以是一對 Palo Alto Networks 防火牆，或是 Palo Alto Networks 防火牆搭配其他廠商具備 VPN 功能的裝置。

了解 VPN 的基本概念：

- IPSec VPN
- IPSec 通道模式
- IPSec VPN 類型
- IPSec VPN 通道
- VPN 部署
- VPN 的網際網路金鑰交換 (IKE)

IPSec VPN

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

IPSec VPN 可透過公用網路基礎結構（例如網際網路）提供私人且安全的 IP 通訊。利用這項技術，不同地理區域的不同網站或使用者可以透過網路進行通訊，從而安全地使用其資源。IPSec 提供資料機密性和完整性，包括驗證、完整性檢查和加密。

IPSec VPN 是兩種常見的 VPN 通訊協定之一，或是用於建立 VPN 連線的標準集。在 IP 層上，IPSec 提供整個網路（而不僅僅是單一裝置）的安全遠端存取。

IPSec VPN 有兩種類型：

- 通道模式
- 傳輸方式

IPSec 和 **VPN** 之間的區別

IP 安全性 **(IPSec)**	**VPN**
為 IP 主機提供針對 IP 網路上傳送的資料進行加密和驗證的方法。	使用加密來隱藏 VPN 用戶端和伺服器之間傳送的所有資料。
透過使用 IPSec，擁有 IP 位址的實體可以建立安全通道。	許多類型的 VPN 通訊協定都會提供不同等級的安全性和其他功能。VPN 產業中最常用的通道通訊協定是點對點通道通訊協定 (PPTP)、第二層通道通訊協定 (L2TP) 或 IPSec、安全通訊端通道通訊協定 (SSTP) 和 OpenVPN。

IPSec 通道模式

這可在何處使用？	我需要什麼？
• Prisma Access（Prisma Access 尚不支援 IPSec 通道傳輸模式） • PAN-OS	無需授權

IPSec 標準定義了兩種不同的 IPSec 操作模式：通道模式和傳輸模式。傳輸模式和通道模式之間的主要區別在於套用政策規則的位置。雖然在通道模式下，原始封包會封裝在另一個 IP 標頭中，但在任一模式下，封包都可以透過驗證標頭 (AH) 和/或封裝安全有效負載 (ESP) 來加以保護。

- *AH* 不能與 *NAT* 一起使用，因為完整性是透過使用 *IP* 標頭的某些欄位來計算的。原因是 *AH* 在雜湊型訊息驗證碼 *(HMAC)* 計算中包含外部 *IP* 標頭，這會導致 *NAT* 將其破壞。
- *IPSec* 傳輸模式用於端對端通訊，例如用戶端和伺服器之間，或工作站和閘道之間（如果閘道被視為主機）。從工作站到伺服器的加密 *Telnet* 或遠端桌面工作階段就是個好例子。
- *PAN-OS®* 預設支援通道模式，而傳輸模式是從 *PAN-OS 11.0* 版開始引入的支援。

IPSec VPN 類型

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

站台對站台（或閘道到閘道）VPN 和遠端存取（用戶端到站台）VPN 是兩種不同類型的 VPN。用戶端對站台 VPN 代表單一使用者連線，而站台對站台 VPN 則會處理整個網路之間的遠端連線。

在站台對站台 VPN 中，IPSec 安全方法會用來建立從一個客戶網路到客戶遠端站台的加密通道。Palo Alto Networks VPN 通道也可以在合作夥伴之間使用。

站台對站台 VPN 不允許使用多個端點。

在遠端存取 VPN 中，各個端點都會連線到私人網路，以遠端存取該私人網路的服務和資源。遠端存取 VPN 最適合企業和家庭用戶，因為其允許多個端點。

IPSec VPN 通道

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

建立 IPSec 通道的程序會先從建立加密和受保護的準備通道開始，然後從該安全通道內與 IPSec 通道的加密金鑰和參數交涉。

VPN 交涉分成兩個已定義的階段進行：階段一和階段二。階段一的主要目的是設定安全的加密通道，讓兩個對等方可以透過該通道進行交涉。當階段一成功完成時，對等方會迅速進入階段二進行談判。

如果通道介面所在的區域與流量將起始或離開的區域不同，請定義政策規則以允許流量從來源區域流向包含通道介面的區域。在通道介面上設定 IP 位址是選用項目。如果您打算通過通道介面執行動態路由通訊協定，則需要此 IP 位址。

雖然 IPSec 包含許多元件技術並提供多個加密選項，但基本操作包括以下五個主要程序：

- 相關流量或隨選—IPSec 通道政策規則和路由表會決定哪種類型的流量會被視為「相關」或被「隨選」擷取，而因此受到保護。如何實作 PAN-OS VPN 安全性政策取決於裝置平台。存取清單會解釋 IPSec 政策規則，以確定哪些流量將受到 IPSec 的保護。

  僅當有相關流量流向通道時，IPSec 通道才會啟動。若要手動啟動通道，請參閱使用 CLI 對站台對站台 VPN 問題進行疑難排解，檢查通道狀態及清除通道。
- **IKE** 階段 **1**—IKE 是與 IPSec 搭配使用的金鑰管理通訊協定標準。IKE 會對 IPSec 工作階段中的每個對等進行驗證、自動交涉兩個層級的 SA，並處理分成兩個階段（階段 1 和階段 2）完成的工作階段金鑰交換。

  IKE 階段 1 的主要目的是對 IPSec 對等進行驗證，並在對等之間建立安全通道。
- **IKE** 階段 **2**—IKE 會在對等方之間與更嚴格的 security association（安全性關聯 - SA）參數交涉。
- **IPSec** 資料傳輸—符合條件的資料會在 IPSec 對等之間傳輸。資訊會根據用於定義相關流量的方法，透過 IPSec 工作階段進行交換。封包會使用 IPSec SA 中指定的任何加密在 IPSec 對上進行加密和解密。

- **IPSec** 通道工作階段終止—IPSec 工作階段可能會因為下列原因而終止：流量結束且 IPSec SA 已刪除，或者 SA 因為任一 SA 存留時間設定而逾時。SA 逾時可能會在指定的秒數或指定的位元數通過連線之後發生。

  當 SA 終止時，金鑰將被捨棄，這會需要 IKE 執行新的階段二，可能的話，一個交涉一個新階段。您可以在目前 SA 過期之前建立新的 SA，從而保持不間斷的資料流。

  IPSec 工作階段可透過刪除或逾時來終止。

Palo Alto Networks 新世代防火牆上的 **IPSec** 通道政策規則實作

封裝封包以便在網路上安全傳輸是透過 IPsec 通訊協定完成的。例如，在站台對站台 VPN 的情況下，網路中的來源主機會傳輸 IP 封包。該封包到達網路邊緣時，就會與 VPN 閘道聯絡。與該網路對應的 VPN 閘道會對私人 IP 封包進行加密，並通過 ESP 通道將其轉送到下一個網路邊緣的對等 VPN 閘道，該閘道會解密封包並將其傳送到目的地主機。

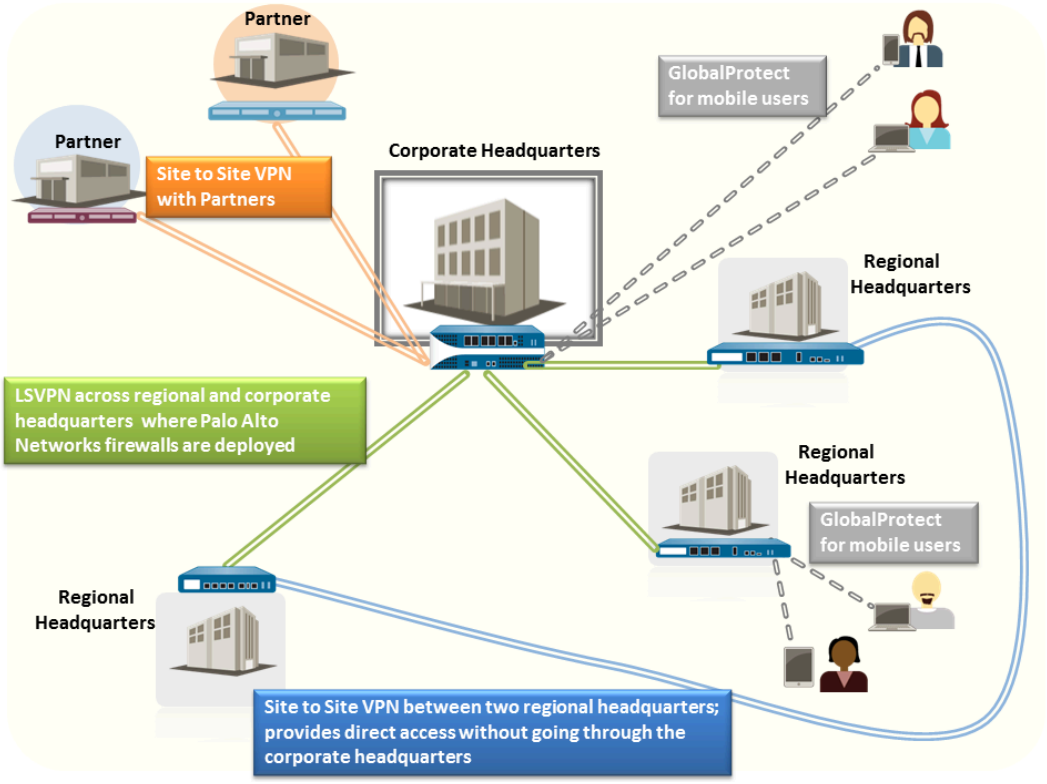
策略型 VPN 具有特定的安全規則、政策規則或存取清單（例如來源位址、目的地位址和連接埠），這些都是為了允許相關流量通過 IPSec 通道而設定。這些規則會在快速模式（或 IPSec 階段 2）期間受到參照，並在第一則或第二則訊息中作為 Proxy ID 交換。如果 Palo Alto Networks 防火牆未設定 Proxy ID 設定，防火牆將使用預設值設定 Proxy ID (source ip = 0.0.0.0/0, destination ip = 0.0.0.0/0, application:any)，並在快速模式的第一則或第二則訊息期間與對等方交換。

VPN 部署

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

Palo Alto Networks 防火牆支援下列 VPN 部署：

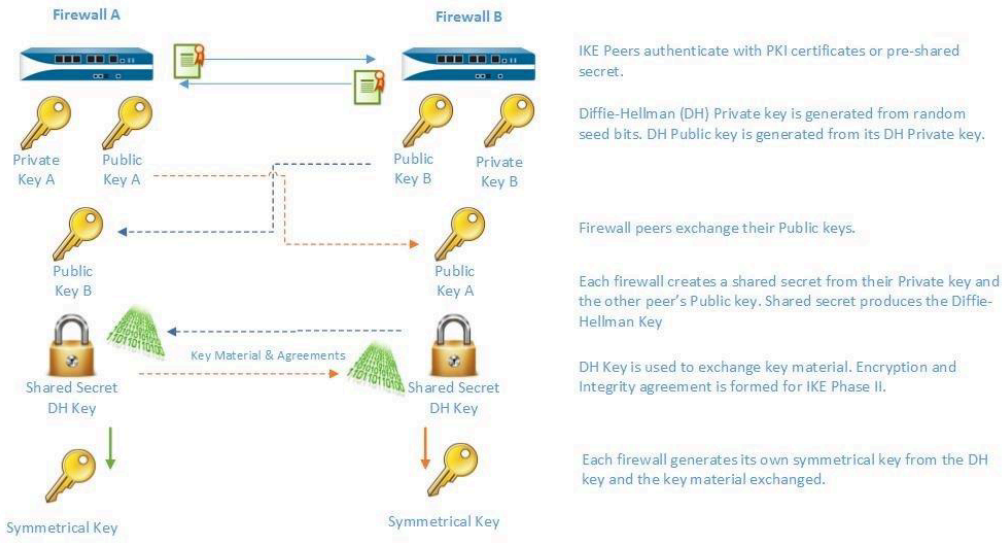
- 站台對站台 **VPN**—一種簡單的 VPN，可連接中央站台與遠端站台，或可連接中心點與軸輻式 VPN，讓中央站台與多個遠端站台連接。防火牆會使用網際網路通訊協定安全性 (IPSec) 通訊協定集為兩個站台間的流量設定安全通道。請參閱站點對站點 VPN 概覽。
- 遠端使用者對站台 **VPN**—此解決方案使用 GlobalProtect 代理程式，讓遠端使用者能夠透過防火牆建立安全連線。此解決方案使用 SSL 與 IPSec 在使用者與站台之間建立安全連線。請參閱《GlobalProtect 管理者指南》。
- 大規模 **VPN**— Palo Alto Networks GlobalProtect 大規模 VPN (LSVPN) 提供經過簡化的機制，能夠提供可調式中心點與軸輻式 VPN，最多可含 1,024 個衛星辦公室。此解決方案需要在中心點與每一個軸輻點上部署 Palo Alto Networks 防火牆。它使用憑證進行裝置驗證，使用 SSL 讓所有元件之間有安全的通訊，並使用 IPSec 保護資料。請參閱大規模 VPN (LSVPN)。
- 遠端站台 **VPN**—遠端站台會使用 IPSec 通道來保護遠端網路位置中的使用者和裝置安全。此外，受到 GlobalProtect 保護的行動裝置使用者和遠端站台的使用者可以使用 IPSec 通道（用於服務連線或 ZTNA 連接器）或 GRE 通道（用於 Colo-Connect 連線）來存取私人應用程式。



VPN 的網際網路金鑰交換 (IKE)

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IKE 程序允許通道兩端的 VPN 對等使用互相同意的金鑰或憑證與加密方法將封包加密與解密。IKE 程序分成兩個階段：IKE 階段 1 和 IKE 階段 2。每個階段皆使用以密碼設定檔—IKE 密碼設定檔與 IPSec 密碼設定檔—定義的金鑰與演算法，IKE 交涉的結果是 security association（安全性關聯 - SA）。SA 是一組互相同意的金鑰與演算法，VPN 對等雙方用於允許整個 VPN 通道的資料流量。下圖說明用於設定 VPN 通道的金鑰交換程序：



IKE 閘道

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

Palo Alto Networks 防火牆或啟動並終止兩個網路間 VPN 連線的防火牆與安全性裝置，可稱為 IKE 閘道。若要設定 VPN 通道並在 IKE 閘道之間傳送流量，則每個對等必須有 IP 位址—靜態或動態—或 FQDN。VPN 對等使用預先共用的金鑰或憑證彼此互相驗證。

對等也必須交涉模式—主要或積極—以設定 IKE 階段 1 中的 VPN 通道與 SA 存留時間。主要模式可保護對等的識別，而且更安全，因為設定通道時會交換更多的封包。如果兩個對等皆支援，則主要模式則為 IKE 交涉的建議模式。加強模式會使用較少的封包設定 VPN 通道，因此速度較快，但設定 VPN 通道的安全選項較少。

如需設定詳細資料，請參閱 設定 IKE 閘道。

IKE 階段 1

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

在此階段中，防火牆使用在 IKE 閘道組態和 IKE 密碼設定檔中定義的參數互相驗證，並設定安全控制通道。IKE 階段支援使用預先共用金鑰或數位憑證（使用公開金鑰基礎結構，PKI）互相驗證 VPN 對等。預先共用金鑰是保護小型網路的簡單解決方案，因為小型網路不需要支援 PKI 基礎結構。對於需要更強驗證安全性的大型網路或實作而言，數位憑證更為方便。

使用憑證時，請確定兩個閘道對等皆信任簽發憑證的 CA，憑證鏈結中憑證的最大長度為 5 以下。在 IKE 區段啟用的狀況下，防火牆最多可使用憑證鏈中最多五個憑證重新組合 IKE 訊息，並成功建立 VPN 通道。

IKE 密碼設定檔會定義下列在 IKE SA 交涉中使用的選項：

- 用於產生 IKE 對稱金鑰的 Diffie-Hellman (DH) 群組。

  Diffie-Hellman 演算法使用一方的私密金鑰及另一方的公開金鑰來建立共用金鑰，亦即由 VPN 通道對等雙方共用的加密金鑰。防火牆上支援的 DH 群組有：

群組編號	位元組數
群組 1	768 位元
群組 2	1,024 位元（預設值）
群組 5	1,536 位元
群組 14	2,048 位元
群組 15	（PAN-OS 10.2.0 和更新版本）3072 位元模指數群組
群組 16	（PAN-OS 10.2.0 和更新版本）4096 位元模指數群組
群組 19	256 位元橢圓曲線群組
群組 20	384 位元橢圓曲線群組
群組 21	（PAN-OS 10.2.0 和更新版本）512 位元隨機橢圓曲線群組

- 驗證演算法—sha1、sha 256、sha 384、sha 512 或 md5。

- 加密演算法—aes-256-gcm、aes-128-gcm、3des、aes-128-cbc、aes-192-cbc、aes-256-cbc 或 des。

  - *PAN-OS 10.0.3* 及更新版本支援 *aes-256-gcm* 和 *aes-128-gcm* 演算法。
  - *PAN-OS 10.1.0* 及更早版本支援 *des* 加密演算法。

IKE 階段 2

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

保護與驗證通道後，會進一步保護階段 2 中的通道，以在網路之間傳輸資料。IKE 階段 2 會使用在程序的階段 1 及 IPSec 密碼設定檔中建立的金鑰，這些金鑰會定義在 IKE 階段 2 中用於 SA 的 IPSec 密碼設定檔與金鑰。

IPSec 會使用下列通訊協定啟用安全通訊：

- 封裝安全有效負載 (ESP)—允許您加密整個 IP 封包，並驗證來源與資料完整性。ESP 要求您加密與驗證封包時，您可以透過將加密選項設為 (空值)，來選擇僅加密或僅驗證；不鼓勵使用加密但不進行驗證。
- 驗證標頭 (AH)—驗證封包來源與資料完整性。AH 不會加密資料承載，且不適用於資料隱私很重要的部署。AH 常用於主要考量為驗證對等合法性且資料隱私為非必要時。

表 **1:** 支援的 **IPSec** 驗證與加密演算法

ESP	**AH**
支援的 **Diffie Hellman (DH)** 交換選項	

- 群組 1—768 位元
- 群組 2—1024 位元（預設值）
- 群組 5—1536 位元
- 群組 14—2048 位元
- （PAN-OS 10.2.0 和更新版本）群組 15—3072 位元模指數群組
- （PAN-OS 10.2.0 和更新版本）群組 16—4096 位元模指數群組
- 群組 19—256 位元橢圓曲線群組
- 群組 20—384 位元橢圓曲線群組
- （PAN-OS 10.2.0 和更新版本）群組 21—512 位元隨機橢圓曲線群組
- 無 pfs—依預設會啟用完整轉送密碼，這表示會在 IKE 階段 2 中使用前述其中一個群組產生新的 DH 金鑰。此金鑰獨立於在 IKE 階段 1 中交換的金鑰以外，並且可提供更好的資料傳輸

ESP	AH
安全性。如果您選取「無 pfs」，在階段 1 中建立的 DH 金鑰將不會更新，且 IPSec SA 交涉會使用單一金鑰。VPN 對等雙方必須同時為 PFS 啟用或停用。	
支援加密演算法	
• des	（PAN-OS 10.1.0 及更早版本）資料加密標準 (DES)，安全強度為 56 位元。
• 3des	安全性長度為 112 位元的三重資料加密標準 (3DES)。
• aes-128-cbc	使用安全性長度為 128 位元之加密區塊鏈結 (CBC) 的進階加密標準 (AES)。
• aes-192-cbc	使用安全性長度為 192 位元之 CBC 的 AES。
• aes-256-cbc	使用安全性長度為 256 位元之 CBC 的 AES。
• aes-128-ccm	使用安全性長度為 128 位元之 CBC-MAC (CCM) 計數器的 AES。
• aes-128-gcm	使用安全性長度為 128 位元之伽羅瓦計數器模式 (GCM) 的 AES。
• aes-256-gcm	使用安全性長度為 256 位元之 GCM 的 AES。
支援驗證演算法	
• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

保護 **IPSec VPN** 通道的方法（**IKE** 階段 **2**）

IPSec VPN 通道可使用手動金鑰或自動金鑰予以保護。此外，IPSec 組態選項包括金鑰協議的 Diffie-Hellman 群組、加密演算法與訊息驗證的雜湊。

- 手動金鑰—手動金鑰通常用於 Palo Alto Networks 防火牆使用舊有裝置建立 VPN 通道時，或者您想要減少產生工作階段金鑰的負荷。如果使用手動金鑰，則必須在雙方對等建立相同的金鑰。

  不建議使用手動金鑰建立 VPN 通道，因為在對等方之間轉送金鑰資訊時可能會洩漏工作階段金鑰；如果金鑰遭到洩漏，便再也無法安全地傳輸資料。
- 自動金鑰—自動金鑰允許您自動產生金鑰，以根據在 IPSec 密碼設定檔中定義的演算法設定與維護 IPSec 通道。

IKEv2

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IPSec VPN 閘道會使用 IKEv1 或 IKEv2 來交涉 IKE 安全性關聯 (SA) 和 IPSec 通道。IKEv2 可於 RFC 5996 中定義。

不同於使用階段 1 SA 和階段 2 SA 的 IKEv1，IKEv2 使用的是封裝安全有效負載 (ESP) 或驗證標頭 (AH) 的子 SA，這是以 IKE SA 設定的。

如果您在位於兩個閘道之間的設備上執行 NAT，則必須在兩個閘道上都啟用 NAT 周遊 (NAT-T)。閘道只能看見 NAT 裝置的公用（可全域路由傳送）IP 位址。

IKEv2 提供下列優於 IKEv1 的好處：

- 通道端點只需交換較少的訊息即可建立通道。IKEv2 使用四個訊息；IKEv1 使用九個訊息（在主要模式中）或六個訊息（在加強模式中）。
- 內建的 NAT-T 功能可改善廠商之間的相容性。
- 內建的健康度檢查可在通道失效時自動加以重新建立。活性檢查取代了 IKEv1 中使用的「無效對等偵測」。
- 支援流量選取器（每個交換一個）。流量選取器可在 IKE 交涉中用來控制哪個流量可存取通道。
- 支援雜湊與 URL 憑證交換，以減少分散的狀況。
- 透過改良的對等驗證，能夠在 DoS 攻擊之後復原。額外的半開啟 SA 可觸發 Cookie 驗證。

在設定 IKEv2 之前，您應熟悉下列概念：

- 活性檢查
- Cookie 啟用臨界值和嚴格 Cookie 驗證
- 流量選取器
- 雜湊與 URL 憑證交換
- SA 金鑰的存留時間和重新驗證間隔

在設定 IKE 閘道之後，如果您選擇 IKEv2，請根據您的環境需求，執行下列與 IKEv2 有關的選用工作：

- 匯出憑證讓對等使用雜湊與 URL 加以存取
- 匯出憑證供 IKEv2 閘道驗證使用
- 變更 IKEv2 的金鑰存留時間或驗證層級
- 變更 IKEv2 的 Cookie 啟用臨界值
- 設定 IKEv2 流量選取器

活性檢查

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IKEv2 的活性檢查類似於無效對等偵測 (DPD)，後者是 IKEv1 用來判斷對等是否仍可用的方法。

在 IKEv2 中，活性檢查可使用由閘道依據可設定的間隔（預設為 5 秒）傳送至對等的任何 IKEv2 封包傳輸或空資訊訊息來執行。如有需要，寄件者最多可嘗試重新傳輸 10 次。如果沒有回應，寄件者會關閉並刪除 IKE_SA 與對應的 CHILD_SA。寄件者會重新開始寄出另一個 IKE_SA_INIT 訊息。

Cookie 啟用臨界值和嚴格 Cookie 驗證

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

對於 IKEv2 一律會啟用 Cookie 驗證；這有助於防止半 SA DoS 攻擊。您可以設定會觸發 Cookie 驗證之半開放 SA 的全域臨界值數。您也可以設定個別的 IKE 閘道，使其為每個新的 IKEv2 SA 強制執行 Cookie 驗證。

- **Cookie Activation Threshold**（**Cookie** 啟用臨界值）是一項全域 VPN 工作階段設定，可限制同時的半開啟 IKE SA 數目（預設值為 500）。當半開啟的 IKE SA 數目超過 **Cookie Activation Threshold**（**Cookie** 啟用臨界值）時，回應程式會要求一個 Cookie，且啟動者必須回應一個包含 Cookie 的 IKE_SA_INIT 以驗證連線。若 Cookie 驗證成功，則可以啟動另一個 SA。若值為零，表示 Cookie 驗證一律開啟。

  在啟動者傳回 Cookie 前，回應者將不會維護啟動者的狀態，也不會執行 Diffie-Hellman 金鑰交換。IKEv2 Cookie 驗證可緩解會嘗試致使許多連線半開啟的 DoS 攻擊。

  Cookie Activation Threshold（**Cookie** 啟用臨界值）必須低於 **Maximum Half Opened SA**（半開啟 **SA** 上限）設定。如果您 變更 IKEv2 的 Cookie 啟用臨界值 至較高的數值（例如 65534），且 **Maximum Half Opened SA**（半開啟 SA 上限）設定仍維持在預設值 65535，則 Cookie 驗證會停用。

- 如果您想要為閘道所接收的每個新的 IKEv2 SA 執行 Cookie 驗證，無論全域臨界值為何，您可以啟用 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）。**Strict Cookie Validation**（嚴格 **Cookie** 驗證）只會影響正在設定的 IKE 閘道，且預設為停用。如果 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）停用，系統會使用 **Cookie Activation Threshold**（**Cookie** 啟用臨界值）來判定是否需要某個 Cookie。

流量選取器

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

在 IKEv1 中，具有路由型 VPN 的防火牆必須使用本機和遠端 Proxy ID，以設定 IPSec 通道。每個對等都會比較其 Proxy ID 與它在封包中接收到的 ID，以成功交涉 IKE 階段 2。IKE 階段 2 與交涉 SA 以設定 IPSec 通道的程序有關。（如需 Proxy ID 的詳細資訊，請參閱隧道接口。）

在 IKEv2 中，您可以 設定 IKEv2 流量選取器，這是在 IKE 交涉期間所使用的網路流量元件。流量選取器可在 CHILD_SA（通道建立）階段 2 期間用來設定通道，以及決定哪些流量可通過通道。兩個 IKE 閘道對等必須互相交涉，並一致同意其流量選取器；否則，其中一方會縮小其位址範圍以達成協議。一個 IKE 連線可以有多個通道；例如，您可以將不同的通道指派給每個部門，以隔離其流量。流量的區隔可讓 QoS 之類的功能得以實作。

IPv4 和 IPv6 的流量選取器包括：

- 來源 **IP** 位址—網路首碼、位址範圍、特定主機或萬用字元。
- 目的地 **IP** 位址—網路首碼、位址範圍、特定主機或萬用字元。
- 通訊協定—一個傳輸通訊協定，例如 TCP 或 UDP。
- 來源連接埠—送出封包的連接埠。
- 目的地連接埠—封包預定要送達的連接埠。

在 IKE 交涉期間，可能會有用於不同網路和通訊協定的多個流量選取器。例如，啟動者可能會指出它要將 TCP 封包從 172.168.0.0/16 透過通道傳送至其對等，並以 198.5.0.0/16 作為目標。它也要將 UDP 封包從 172.17.0.0/16 透過相同的通道傳送至相同的閘道，並以 0.0.0.0（任何網路）作為目標。對等閘道必須同意這些流量選取器，以得知應有的預期。

一個閘道開始交涉時所使用的流量選取器，是比另一個閘道的 IP 位址更為特定的 IP 位址，是有可能發生的情況。

- 例如，閘道 A 提供的來源 IP 位址為 172.16.0.0/16，目的地 IP 位址為 192.16.0.0/16。但閘道 B 設定了 0.0.0.0（任何來源）作為來源 IP 位址，並以 0.0.0.0（任何目的地）作為目的地 IP 位址。因此，閘道 # 將其來源 IP 位址縮小為 192.16.0.0/16，並將目的地位址縮小為 172.16.0.0/16。據此，縮小範圍以接納閘道 A 的位址，兩個閘道的流量選取器得以達成協議。
- 如果閘道 B（設定的來源 IP 位址為 0.0.0.0）是啟動者而非回應者，則閘道 A 將會以其較特定的 IP 位址回應，而閘道 B 將會縮小其位址以達成協議。

雜湊與 URL 憑證交換

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IKEv2 支援「雜湊與 URL 憑證交換」，這是在 IKEv2 交涉 SA 期間所使用的功能。您會將憑證儲存在 URL 所指定的 HTTP 伺服器上。對等會根據接收到的伺服器 URL，從伺服器提取憑證。雜湊可用來檢查憑證的內容是否有效。因此，兩個對等將會與 HTTP CA 交換憑證，而不是互相交換。

「雜湊與 URL」的雜湊部分可減少訊息大小，因此「雜湊與 URL」可說是能夠在 IKE 交涉期間降低封包分散可能性的方式之一。對等會接收它所預期的憑證和雜湊，因此 IKE 階段 1 驗證了對等。減少分散的狀況有助於防止 DoS 攻擊。

在設定 IKE 閘道時，您可以選取 **HTTP Certificate Exchange**（**HTTP** 憑證交換）並輸入 **Certificate URL**（憑證 **URL**），以啟用「雜湊與 URL」憑證交換。此外，對等方也必須使用「雜湊與 URL」憑證交換，交換才能成功。如果對等方無法使用「雜湊與 URL」，則 X.509 憑證的交換方式將會類似於在 IKEv1 中的交換。

如果您啟用「雜湊與 URL」憑證交換，您必須將憑證匯出至憑證伺服器（如果已不在那裡）。匯出憑證時，檔案格式應為 **Binary Encoded Certificate (DER)**（二進位編碼憑證 **(DER)**）。請參閱匯出憑證讓對等使用雜湊與 URL 加以存取。

SA 金鑰的存留時間和重新驗證間隔

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IKEv2 中有兩個 IKE 密碼設定檔值 **Key Lifetime**（金鑰存留時間）和 **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數），可控制 IKEv2 IKE SA 的建立。金鑰存留時間是交涉的 IKE SA 金鑰有效的時間長度。在金鑰存留時間到期之前，必須重設 SA 金鑰，否則在到期時，SA 必須開始新的 IKEv2 IKE SA 金鑰重設。預設值是 8 小時。

重新驗證間隔衍生自 **Key Lifetime**（金鑰存留時間）與 **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數）的乘積。驗證倍數預設為 0，這會停用重新驗證功能。

驗證倍數的範圍為 0-50。因此，舉例來說，如何您將驗證倍數設定為 20，系統將會在每次經過 20 次金鑰重設時（也就是每 160 小時）執行重新驗證。這表示，在閘道必須向 IKE 重新驗證以從頭重新建立 IKE SA 之前，閘道有 160 小時可以執行子 SA 建立。

在 IKEv2 中，啟動者和回應者閘道各有其本身的金鑰存留期間值，而金鑰存留期間較短的閘道，將會是要求為 SA 重設金鑰的閘道。

開始使用 IPSec VPN（站台對站台）

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

VPN 連線能讓您在兩個以上站台之間安全地存取資訊。為了能夠安全存取資源並提供可靠的連線，VPN 連線需要下列元件：IKE 閘道、通道介面、通道監控、用於 VPN 的 Internet Key Exchange（網際網路金鑰交換 - IKE）和 IKEv2。

在規劃 IPSec VPN 通道設定之前，請務必了解：

- 隧道接口
- 通道監控器
- IPSec VPN 的 Proxy ID

站台對站台 VPN 概覽

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

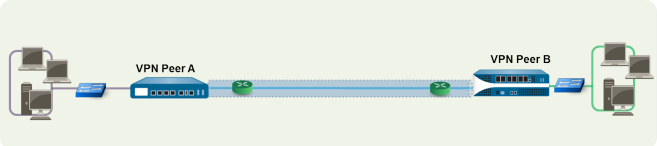
允許您將兩個區域網路 (LAN) 連接的 VPN 連線稱做站台對站台 VPN。您可以設定以路由為基礎的 VPN，以連接兩個站台的 Palo Alto Networks 防火牆，或將 Palo Alto Networks 防火牆與其他位置的協力廠商安全性裝置連接。防火牆也可以與以協力廠商原則為基礎的 VPN 裝置交互操作；Palo Alto Networks 防火牆支援以路由為基礎的 VPN。

Palo Alto Networks 防火牆會設定以路由為基礎的 VPN，在此防火牆會根據目的地 IP 位址來決定路由。如果流量透過 VPN 通道路由到特定目的地，會將其作為 VPN 流量處理。

網際網路通訊協定安全性 (IPSec) 通訊協定集可用於為 VPN 流量設定安全通道，並保護 TCP/IP 封包中的資訊 (如果通道類型為 ESP 則加密)。IP 封包 (標頭與承載) 會內嵌於另一個 IP 承載中，會套用新的標頭並隨後透過 IPSec 通道傳送此標頭。新標頭中的來源 IP 位址是本地 VPN 對等的 IP 位址，目的地 IP 位址是通道遠端處 VPN 對等的 IP 位址。當封包到達遠端 VPN 對等 (通道遠端的防火牆)，會移除外部標頭，原始封包會傳送至其目的地。

為了設定 VPN 通道，首先必須驗證對等。成功驗證後，對等會交涉加密機制與演算法，來保護通訊安全。網際網路金鑰交換 (IKE) 程序用於驗證 VPN 對等，IPSec 安全性關聯 (SA) 則會在通道的每一端定義，以保護 VPN 通訊安全。IKE 使用數位憑證或預先共用的金鑰及 Diffie Hellman 金鑰為 IPSec 通道設定 SA。SA 會指定安全傳輸所需的所有參數—包括安全性參數索引 (SPI)、安全性通訊協定、加密金鑰及目的地 IP 位址—加密、資料驗證、資料完整性及端點驗證。

下圖顯示兩個站台之間的 VPN 通道。當 VPN 對等 A 保護的用戶端需要位於另一個站台的伺服器內容時，VPN 對等 A 會對 VPN 對等 B 的連線啟動要求。如果安全性原則允許連線，VPN 對等 A 會使用 IKE 密碼設定檔參數（IKE 階段 1）建立安全連線並驗證 VPN 對等 B。接著，VPN 對等 A 會使用 IPSec 密碼設定檔來定義 IKE 階段 2 參數，以允許在兩個站台之間安全傳輸資料。



隧道接口

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

若要設定 VPN 通道，各端的 Layer 3 介面均必須具有邏輯通道介面，防火牆才能連線並建立 VPN 通道。通道介面是邏輯（虛擬）介面，用於在兩個端點之間傳遞流量。若您設定了任何 Proxy ID，則該 Proxy ID 將計入任何 IPSec 通道容量。

通道介面必須屬於安全性區域才能套用政策規則，且必須指派給虛擬路由器才能使用現有的路由基礎結構。確定通道介面與實體介面指派給同一個虛擬路由器，讓防火牆可執行路由查閱，並決定要使用的適當通道。

一般而言，附加通道介面的 Layer 3 介面屬於外部區域，例如不信任區域。雖然通道介面可以與實體介面位在同一個安全性區域中，但為了增加安全性與更好的可見度，您可以為通道介面另外建立一個區域。如果您為通道介面另外建立的區域為 VPN 區域，則必須建立安全性原則才能讓流量在 VPN 區域與信任區域之間流動。

若要在站台之間路由流量，通道介面不需要 IP 位址。如果您想要啟用通道監控，或者使用動態路由通訊協定在整個通道間路由流量，則只需要 IP 位址。有了動態路由，通道 IP 位址會作為將流量路由至 VPN 通道的下一個躍點 IP 位址。

如果您正在設定 Palo Alto Networks 防火牆，且其中的 VPN 對等執行以原則為基礎的 VPN，當設定 IPSec 通道時，您必須設定本機與遠端 Proxy ID。各對等均會與設定於對等上的 Proxy-ID 進行比較，在封包中必須收到 Proxy-ID，IKE 階段 2 交涉才能成功。如果需要多個通道，請為每個通道介面設定唯一的 Proxy ID；通道介面最多可以有 250 個 Proxy ID。每個 Proxy ID 會計入防火牆的 IPSec VPN 通道容量中，通道容量會隨著防火牆型號而異。

如需設定詳細資料，請參閱設定 IPSec 通道。

通道監控器

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

對於 VPN 通道而言，您可以在整個通道中檢查目的地 IP 位址的連線。防火牆的網路監控設定檔可讓您以指定的輪詢間隔驗證對目的地 IP 位址或下一個躍點的連線 (使用 ICMP)，並指定失敗時存取所監控 IP 位址的動作。

如果目的地 IP 位址無法連線，您可以設定防火牆等待通道復原，或設定自動容錯移轉至另一個通道。無論是哪種方式，防火牆都會產生系統日誌來提醒您通道失敗，並重新交涉 IPSec 金鑰以加速復原。

如需設定詳細資料，請參閱監控您的 IPSec VPN 通道。

IPSec VPN 的 Proxy ID

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

Proxy 身分識別或 Proxy ID 是指屬於 IPSec VPN 的一組流量，其受限於將在對等方之間交涉的 SA（或交涉成功後的設定）。

其允許識別並引導流量：

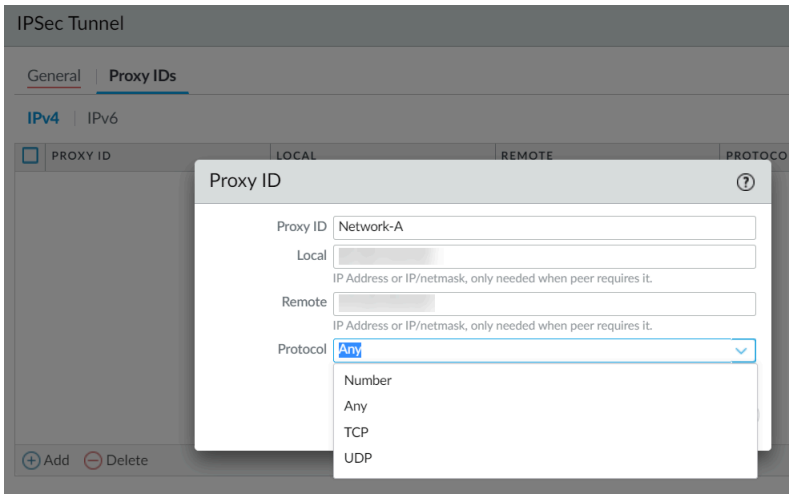
- 到適當的通道，其中在共用相同 IKE 閘道的相同兩個對等方之間有多個通道共存。
- 允許具有不同參數的唯一 SA 和共用 SA 共存。

在相同的兩個對等方之間設定 *VPN* 通道的設定中，使用 *Proxy ID*。

Proxy ID 有助於識別哪些流量屬於特定 IPSec VPN。這可讓作業系統安裝適當的掛鉤，來引導與 Proxy ID（客戶端 ID）中來源位址和目的地位址相符的流量，並將其引導至相符的 IPSec SA，或引導 VPN 進出相符的 IPSec SA。

設定代理 **ID**

Palo Alto Networks 是其他幾家使用 Proxy ID 的廠商之一。下圖顯示了 Palo Alto Networks Proxy ID 的視窗及其選項。



選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道） > **Proxy IDs**（**Proxy ID**）。輸入 Proxy ID 名稱、本機 IP 位址、遠端 IP 位址（如果對等方需要），以及通訊協定類型及其本機和遠端連接埠號碼。

每個 *Proxy ID* 都會被視為一個 *VPN* 通道，因此會計入防火牆的 *IPSec VPN* 通道容量。例如，*PA-3020* 的站台對站台 *IPSec VPN* 通道上限為 *1000*、*PA-2050* 的上限為 *100* 及 *PA-200* 的上限為 *25*。

Proxy ID 的行為與 IKE 版本不同：

- **IKEv1**—Palo Alto Networks 裝置僅支援 Proxy ID 完全相符。如果對等方的 Proxy ID 不相符，則 VPN 將無法正常運作。
- **IKEv2**—當兩個 VPN 閘道上的 Proxy ID 設定不同時，支援流量選取器縮小範圍。

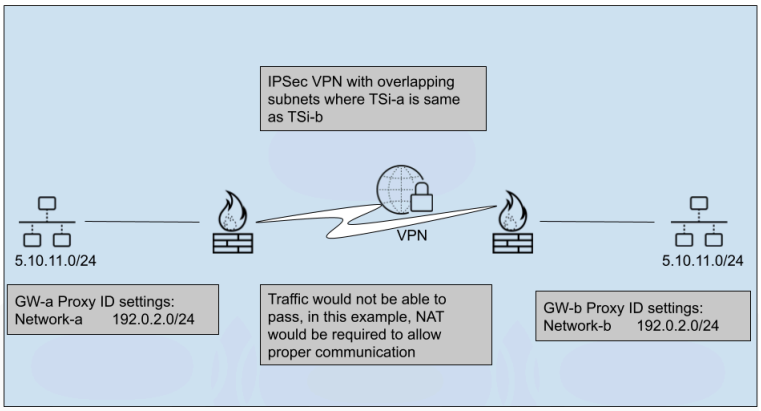
使用 **Proxy ID**

以下範例示範兩個 VPN 閘道：A 和 B。

IKE 交涉由 VPN GW-az 啟動，i=啟動者，r=回應者。VPN GW-a 會定義流量選取器 TSi-a/TSr-，而 VPN GW-b 會指定流量選取器 TSi-b/TSr-b。TSr-a 與 TSr-b 相同，因此可以忽略，但 TSi-a 也可以與 TSi-b 不同。

在此情況下，流量無法透過 VPN 通道路由，因為通道兩側存在相同的網路。

然而，如下圖所示，解決此問題的唯一方法是讓兩個對等閘道建立 NAT，以將新的唯一網路子網路轉換為內部網絡，否則其中一端必須更改子網路 IP。



這樣一來，兩端的所有流量都將發送至新的 NAT 位址，而不是其他類似的網路。兩個閘道都必須執行 NAT 才能正常運作，也才能消除哪個網路位於哪一端的任何困惑。

為 **Palo Alto Networks** 防火牆設定 **IPSec VPN**

如果通道的另一端是第三方 VPN 裝置，或是非 PAN-OS 防火牆，則您需要指定相符的本機 Proxy ID 和遠端 Proxy ID：通常是本機和遠端 LAN 子網路。

設定 IPSec 通道 Proxy ID 以針對經過 NAT 的流量識別本機和遠端 IP 網路時，必須使用 NAT 後的 IP 網路資訊設定 IPSec 通道的 Proxy ID 設定。原因是 Proxy ID 資訊會定義 IPSec 組態兩端上允許通過通道的網路。

規劃您的 IPSec VPN 通道設定

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

在設定 IPSec 通道之前，請務必決定以下要素並成功規劃 IPSec 通道設定。

STEP 1 | 決定 **VPN** 的類型：站台對站台或遠端存取

站台對站台 VPN 允許使用 IPSec 安全方法建立從一個客戶網路到客戶遠端站台的加密通道。但是，遠端存取 VPN 允許個人使用者連線到私人網路以存取其服務和資源。

STEP 2 | 為您的 **VPN** 選取安全方法

在站台對站台 VPN 中，IPSec 安全方法會用來建立從一個客戶網路到客戶遠端站台的加密通道。

在遠端存取 VPN 中，個人使用者會連線到私人網路。

STEP 3 | 決定 **VPN** 用戶端

站台對站台 VPN 不需要在每個用戶端上進行設定。遠端存取 VPN 可能需要或可能不需要在每個用戶端上進行設定。

STEP 4 | 決定 **VPN** 通道設定

站台對站台 VPN 不會要求每個使用者啟動 VPN 通道設定。遠端存取 VPN 會要求每個遠端存取使用者啟動 VPN 通道設定。

STEP 5 | 決定安全技術

站台對站台 VPN 支援 IPSec 技術，而遠端存取 VPN 支援 SSL 和 IPSec 技術。

STEP 6 | 決定您是否希望 **VPN** 上有一個或多個使用者

站台對站台 VPN 不允許多個使用者；但是遠端存取 VPN 允許多個使用者。

設定 IPSec VPN 通道（站台對站台）

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

若要設定站台對站台 VPN：

- 確定已正確設定乙太網路介面、虛擬路由器與區域。如需詳細資訊，請參閱設定介面及區域。
- 建立您的通道介面。理想狀況是將通道介面放置在不同的區域中，以便進入通道的流量可使用不同的政策規則。
- 設定靜態路由或指派路由通訊協定，以將流量重新導向至 VPN 通道。若要支援動態路由 (支援 OSPF、BGP、RIP)，您必須將 IP 位址指派給通道介面。
- 定義 IKE 閘道，藉以在 VPN 通道兩端的對等之間建立通訊；此外也定義密碼設定檔，此設定檔會為用於在 IKEv1 階段 1 中設定 VPN 通道的識別、驗證與加密等功能指定通訊協定與演算法。請參閱設定 IKE 閘道以及定義 IKE 密碼設定檔。
- 設定建立在 VPN 通道之間傳輸資料所用 IPSec 連線所需的參數；請參閱設定 IPSec 通道。對於 IKEv1 階段 2，請參閱定義 IPSec 密碼設定檔。
- （選用）指定防火牆監控 IPSec 通道的方式。請參閱監控您的 IPSec VPN 通道。
- 定義安全性政策以篩選及檢查流量。

如果安全性規則庫的結束處有拒絕規則，除非有另外允許，否則會封鎖區域內流量。允許 *IKE* 和 *IPsec* 應用程式的規則必須包含在拒絕規則之前。

如果您的 *VPN* 流量要通過（而非來源於或終止於）*PA-7000* 系列或 *PA-5200* 系列防火牆，則設定雙向安全性政策，以允許兩個方向上的 *ESP* 或 *AH* 流量。

完成這些工作之後，通道便已準備好可供使用了。系統會根據路由表中的目的地路由，正確自動路由目的地為政策規則中所定義區域/位址的流量，並將此類流量作為 VPN 流量處理。關於站台對站台 VPN 的範例，請參閱站台對站台 VPN 設定範例。

設定 IKE 閘道

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

若要設定 VPN 通道，VPN 對等或閘道必須使用預先共用金鑰或數位憑證互相驗證，並建立安全通道，以交涉用於保護每一端主機之間流量的 IPSec 安全性關聯 (SA)。

STEP 1 | 選取 IKE 閘道。

1. 選取 **Network**（網路）> **Network Profiles**（網路設定檔）> **IKE Gateways**（**IKE** 閘道），**Add**（新增）閘道，並輸入閘道 **Name**（名稱）（**General**（一般）頁籤）。
2. 將 **Version**（版本）設定為 **IKEv1 only mode**（僅 **IKEv1** 模式）、**IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（偏好 **IKEv2** 模式）。IKE 閘道會在此處指定的模式下開始與其對等交涉。如果您選取 **IKEv2 preferred mode**（偏好 **IKEv2** 模式），在遠端對等支援 IKEv2 的情況下，兩個對等會使用 IKEv2，否則將會使用 IKEv1。

   您所選取的 **Version**（版本）也會決定您可在 **Advanced Options**（進階選項）頁籤上設定的選項。

STEP 2 | 建立通道（閘道）的本機端點。

1. 選取 **Address Type**（位址類型）：**IPv4** 或 **IPv6**。
2. 在本機閘道所在的防火牆上，選取實體傳出 **Interface**（介面）。
3. 從 **Local IP Address**（本機 **IP** 位址）清單中，選取 VPN 連線將用作端點的 IP 位址；這是面向防火牆上可公開路由的 IP 位址的對外介面。

STEP 3 | 在通道（閘道）的遠端建立對等。

對於 **Peer IP Address Type**（對等 **IP** 位址類型），選取下列一項並輸入對等對應的資訊：

- **IP**—輸入 **Peer Address**（對等位址）（IPv4 或 IPv6 位址），或輸入作為 IPv4 或 IPv6 位址的位址物件。
- **FQDN**—輸入 **Peer Address**（對等位址）（FQDN 字串或使用 FQDN 字串的位址物件）。如果 FQDN 或 FQDN 位址物件解析超過一個 IP 位址，則防火牆會選取下列來自符合 IKE 閘道的位址類型（IPv4 或 IPv6）位址集中的偏好位址：
  - 如果沒有任何交涉的 IKE 安全性關聯 (SA)，則偏好的位址為帶有最小值的 IP 位址。
  - 如果 IKE 閘道使用傳回位址組中的位址，則防火牆會選取該位址（無論它是否為集合中的最小位址）。
  - 如果 IKE 閘道使用傳回位址集以外的位址，則防火牆會選取新位址，該位址是集合中的最小位址。
- **Dynamic**（動態）—如果對等 IP 位址或 FQDN 值未知，請選取 **Dynamic**（動態），以便對等啟動交涉。

使用 *FQDN* 或 *FQDN* 位址物件減少在環境中的問題，在該環境中對等會受制於動態 *IP* 位址變更（並因此需要您重新設定此 *IKE* 閘道對等位址）。

STEP 4 | 指定如何驗證對等。

選取 **Authentication**（驗證）方法：**Pre-Shared Key**（預先共用金鑰）或 **Certificate**（憑證）。如果您選擇預先共用金鑰，則繼續執行下一步。如果選取憑證，則跳至步驟 6，設定基於憑證的驗證。

STEP 5 | 設定預先共用金鑰。

1. 輸入 **Pre-shared Key**（預先共用金鑰），這是用於通道驗證的安全性金鑰。將值重新輸入 **Confirm Pre-shared Key**（確認預先共用金鑰）中。最多使用 255 個 ASCII 或非 ASCII 字元。

   產生字典攻擊難以破解的金鑰；可視需要使用預先共用金鑰。

2. 針對 **Local Identification**（本機識別），從下列類型中選擇，然後輸入您所決定的值：**FQDN (hostname)**（**FQDN**（主機名稱））、**IP address**（**IP** 位址）、**KEYID (binary format ID string in HEX)**（**KEYID**（十六進位的二進位格式 **ID** 字串））以及 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址））。本機識別會定義本機閘道的格式和識別。如果您未指定值，將使用本機 IP 位址作為本機識別值。
3. 針對 **Peer Identification**（對等識別），從下列類型中選擇，然後輸入您所決定的值：**FQDN (hostname)**（**FQDN**（主機名稱））、**IP address**（**IP** 位址）、**KEYID (binary format ID string in HEX)**（**KEYID**（十六進位的二進位格式 **ID** 字串））以及 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址））。對等識別會定義對等閘道的格式和識別。如果您未指定值，將使用對等 IP 位址作為對等識別值。
4. 繼續執行步驟 7（設定閘道的進階選項）。

STEP 6 | 設定憑證式驗證。

如果您選取了 **Certificate**（憑證），作為對通道另一端的對等閘道進行驗證的方法，請執行此程序中的其餘步驟。

1. 選取已在防火牆上的 **Local Certificate**（本機憑證）、**Import**（匯入）憑證，或 **Generate**（產生）新憑證。
   - 若需 **Import**（匯入）憑證，先匯入憑證供 IKEv2 閘道驗證使用，然後回到此工作。
   - 如果您想要 **Generate**（產生）新憑證，請先在防火牆上產生憑證，然後回到這項工作。
2. （選用）啟用（選取）**HTTP Certificate Exchange**（**HTTP** 憑證交換）以設定雜湊與 URL（僅限 IKEv2）。針對 HTTP 憑證交換，輸入 **Certificate URL**（憑證 **URL**）。如需詳細資訊，請參閱雜湊與 URL 憑證交換。
3. 選取 **Local Identification**（本機識別）類型—**Distinguished Name (Subject), FQDN (hostname)**（辨別名稱（主旨）、**FQDN**（主機名稱））、**IP address**（**IP** 位址）或 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址）），然後輸入值。本機識別會定義本機閘道的格式和識別。
4. 選取 **Peer Identification**（對等識別）類型—**Distinguished Name (Subject), FQDN (hostname)**（辨別名稱（主旨）、**FQDN**（主機名稱））、**IP address**（**IP** 位址）或 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址）），然後輸入值。對等識別會定義對等閘道的格式和識別。
5. 指定 **Peer ID Check**（對等 **ID** 檢查）的類型：
   - **Exact**（完全符合）—確保本機設定和對等 IKE ID 承載完全相符。
   - **Wildcard**（萬用字元）—讓對等識別比對出萬用字元 **(*)** 之前的每個相符字元。萬用字元之後的字元不需要符合。
6. （選用）如果即使對等識別不符合憑證中的對等識別，也仍然想要允許成功的 IKE SA，請 **Permit peer identification and certificate payload identification mismatch**（容許對等識別與憑證承載識別不相符）。
7. 選擇 **Certificate Profile**（憑證設定檔）。憑證設定檔包含關於如何驗證對等閘道的資訊。
8. （選用）若要嚴格控制金鑰的使用方式，請 **Enable strict validation of peer’s extended key use**（對對等的擴充金鑰使用方法啟用嚴格驗證）。

STEP 7 | 設定閘道的進階選項。

1. （選用）若要指定防火牆僅回應 IKE 連線請求而絕不會啟動連線，請在「通用選項」（**Advanced Options**（進階選項））中選取 **Enable Passive Mode**（啟用被動模式）。
2. 如果您有裝置在閘道之間執行 NAT，請 **Enable NAT Traversal**（啟用 **NAT** 周遊），在 IKE 與 UDP 通訊協定上使用 UDP 封裝，使這些通訊協定能通過中繼 NAT 裝置。
3. 若您之前已在步驟 1 中設定 **IKEv1 only mode**（僅 **IKEv1** 模式），則在 IKEv1 頁籤上：
   - 選取 **Exchange Mode**（交換模式）：**auto**（自動）、**aggressive**（加強） 或**main**（主要）。當將防火牆設定為使用 **auto**（自動）交換模式時，它可以接受 **main**（主要）模

式與 **aggressive**（加強）模式交涉要求；但若可能，它會在 **main**（主要）模式下啟動交換。

如果您未將交換模式設為 ***auto***（自動），則必須將對等雙方設為相同的交換模式，才能讓每個對等接受交涉要求。

- 從 **IKE Crypto Profile**（**IKE** 加密設定檔）清單中選取現有的設定檔或保留預設設定檔。若有必要，您可定義 IKE 加密設定檔。
- （僅適用於使用憑證式驗證，以及交換模式未設為加強模式的情況）按一下 **Enable Fragmentation**（啟用分散），讓防火牆能操作 IKE 分散功能。
- 按一下 **Dead Peer Detection**（無效對等偵測），然後輸入 **Interval**（間隔）（範圍為 2 至 100 秒）。對於 **Retry**（重試），請指定在斷開與 IKE 對等的連線之前的重試次數（範圍為 2 到 100）。無效對等偵測功能會識別非使用中或無法使用的 IKE 對等，做法是將 IKE 階段 1通知承載傳送至對等，並等待通知。

4. 如果您在步驟 1 中設定了 **IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（偏好 **IKEv2** 模式），則在 IKEv2 頁籤上：
   - 選取 **IKE Crypto Profile**（**IKE** 加密設定檔），這會設定 IKE 階段 1 選項，例如 DH 群組、雜湊演算法和 ESP 驗證。關於 IKE 密碼設定檔的相關資訊，請參閱 IKE 階段 1。
   - （選用）啟用 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）Cookie 啟用臨界值和嚴格 Cookie 驗證。
   - （選用）若要讓閘道將訊息要求傳送至其閘道對等以要求回應，請 **Enable Liveness Check**（啟用活性檢查），然後輸入 **Interval (sec)**（間隔（秒））（預設值為 5）。如有需要，啟動者可嘗試活性檢查至多 10 次。如果沒有回應，啟動者會關閉並刪除 IKE_SA 與 CHILD_SA。啟動者會重新開始寄出另一個 IKE_SA_INIT。

STEP 8 | 按一下 **OK**（確定）並 **Commit**（交付）變更。

匯出憑證讓對等使用雜湊與 URL 加以存取

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

IKEv2 支援以 雜湊與 URL 憑證交換 作為方法，讓位於通道遠端的對等可從您匯出憑證所在的伺服器擷取憑證。執行這項工作，將您的憑證匯出至該伺服器。您必須已使用 **Device**（裝置） > **Certificate Management**（憑證管理）建立憑證。

STEP 1 | 選取 **Device**（裝置） > **Certificates**（憑證），如果您的平台支援多個虛擬系統，您可以選取適當的虛擬系統作為 **Location**（位置）。

STEP 2 | 在 **Device Certificates**（裝置憑證）頁籤上，選取要 **Export**（匯出）至伺服器的憑證。

憑證的狀態應為有效，而不是已過期。防火牆並不會阻止您匯出無效憑證。

STEP 3 | 針對 **File Format**（檔案格式），選取 **Binary Encoded Certificate (DER)**（二進位編碼憑證 **(DER)**）。

STEP 4 | 將 **Export private key**（匯出私密金鑰）保留為清除。使用「雜湊與 URL」時不一定需要匯出私密金鑰。

STEP 5 | 按一下 **OK**（確定）。

匯出憑證供 IKEv2 閘道驗證使用

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您要驗證 IKEv2 閘道的對等方，但您未在防火牆上使用本機憑證，而想要從他處匯入憑證，請執行此工作。

這項工作假設您已選取 **Network**（網路） > **IKE Gateways**（**IKE** 閘道）、新增閘道，並已針對 **Local Certificate**（本機憑證）按一下 **Import**（匯入）。

STEP 1 | 匯入憑證。

1. 選取 **Network**（網路） > **IKE Gateways**（**IKE** 閘道），**Add**（新增）閘道，然後，在 **General**（一般）頁籤上，針對 **Authentication**（驗證）選取 **Certificate**（憑證）。針對 **Local Certificate**（本機憑證），按一下 **Import**（匯入）。
2. 在匯入憑證視窗中，輸入您所匯入之憑證的 **Certificate Name**（憑證名稱）。
3. 如果要在多個虛擬系統之間共用此憑證，請選取 **Shared**（共用）。
4. 針對 **Certificate File**（憑證檔案），**Browse**（瀏覽）至憑證檔案。按一下檔案名稱，然後按 **Open**（開啟），以填入 **Certificate File**（憑證檔案）欄位。
5. 對於 **File Format**（檔案格式），請選取下列其中一項：
   - **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—包含憑證，但不包含金鑰。這是純文字。
   - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—包含憑證與金鑰。
6. 如果私密金鑰位於與憑證檔案不同的檔案中，請選取 **Import private key**（匯入私密金鑰）。金鑰是選用的，但有下列例外：
   - 如果將 **File Format**（檔案格式）設為 **PEM**，則匯入金鑰。按一下 **Browse**（瀏覽）並導覽至要匯入的金鑰檔案，以輸入 **Key file**（金鑰檔案）。
   - 輸入 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼）。
7. 按一下 **OK**（確定）。

STEP 2 | 繼續下一項工作。

步驟設定憑證式驗證。

變更 IKEv2 的金鑰存留時間或驗證層級

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

此工作是選用的；IKEv2 IKE SA 金鑰重設存留時間的預設值為 8 小時。IKEv2 驗證倍數的預設值為 0，表示重新驗證功能停用。詳細資訊，請參閱 SA 金鑰的存留時間和重新驗證間隔。

若要變更預設值，請執行下列工作。先決條件是 IKE 密碼設定檔已存在。

STEP 1 | 變更 IKE 密碼設定檔的金鑰存留時間或驗證層級。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**，然後套用至本機閘道的 IKE Crypto 設定檔。
2. 針對 **Key Lifetime**（金鑰存留時間），選取單位（**Seconds**（秒）、**Minutes**（分鐘）、**Hours**（小時）或 **Days**（天）），然後輸入一個值。最短為 3 分鐘。
3. 針對 **IKE Authentication Multiple**（**IKE** 驗證倍數）輸入一個值，此值會與存留時間相乘，以決定重新驗證間隔。

STEP 2 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

變更 IKEv2 的 Cookie 啟用臨界值

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您想要讓防火牆使用不同於預設值（達到 500 個半開啟的 SA 工作階段之後需要 Cookie 驗證）的臨界值，請執行下列工作。關於 Cookie 驗證的詳細資訊，請參閱 Cookie 啟用臨界值和嚴格 Cookie 驗證。

STEP 1 | 變更 Cookie 啟用臨界值。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 VPN Session Settings（VPN 工作階段設定）。針對 **Cookie Activation Threshold**（**Cookie** 啟用臨界值），輸入回應者向啟動者要求 Cookie 之前所允許的半開啟 SA 數目上限（範圍為 0-65535；預設值為 500）。
2. 按一下 **OK**（確定）。

STEP 2 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

設定 IKEv2 流量選取器

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

在 IKEv2 中，您可以設定流量選取器，這是在 IKE 交涉期間所使用的網路流量元件。流量選取器可在 CHILD_SA（通道建立）階段 2 期間用來設定通道，以及決定哪些流量可通過通道。兩個 IKE 閘道對等必須互相交涉，並一致同意其流量選取器；否則，其中一方會縮小其位址範圍以達成

協議。一個 IKE 連線可以有多個通道；例如，您可以將不同的通道指派給每個部門，以隔離其流量。流量的區隔可讓 QoS 之類的功能得以實作。使用下列工作流程，設定流量選取器。

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道） > **Proxy IDs**（**Proxy ID**）。

STEP 2 | 選取 **IPv4** 或 **IPv6** 頁籤。

STEP 3 | 按一下 **Add**（新增），然後在 **Proxy ID** 欄位中輸入 **Name**（名稱）。

STEP 4 | 在 **Local**（本機）欄位中，輸入 **Source IP Address**（來源 **IP** 位址）。

STEP 5 | 在 **Remote**（遠端）欄位中，輸入 **Destination IP Address**（目的地 **IP** 位址）。

STEP 6 | 在 **Protocol**（通訊協定）欄位中，選取傳輸通訊協定（**TCP** 或 **UDP**）。

STEP 7 | 按一下 **OK**（確定）。

定義密碼設定檔

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

密碼設定檔會指定用於在兩個 IKE 對等之間進行驗證和/或加密的密碼，以及金鑰的存留時間。每個重新交涉之間的時段稱做存留時間；當指定時間過期時，防火牆將重新交涉一組新的金鑰。

為了保護整個 VPN 通道的通訊，防火牆需要 IKE 與 IPSec 密碼設定檔分別完成 IKE 階段 1 與階段 2 交涉。防火牆包括已可供使用的預設 IKE 密碼設定檔與預設 IPSec 密碼設定檔。

- 定義 IKE 密碼設定檔
- 定義 IPSec 密碼設定檔

定義 IKE 密碼設定檔

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

IKE 密碼設定檔用於設定在 IKE 階段 1 中交換金鑰程序所使用的加密與驗證演算法，並用於設定金鑰存留時間，亦即金鑰的有效時間。若要呼叫該設定檔，您必須將它附加到 IKE 閘道組態。

當將 *IKE* 閘道的 ***Peer IP Address Type***（對等 ***IP*** 位址類型）設定為 ***Dynamic***（動態）且套用了 *IKEv1* 主要模式或 *IKEv2* 時，在同一介面或本機 *IP* 位址上設定的所有 *IKE* 閘道必須使用相同的密碼設定檔。如果閘道上的密碼設定檔相同，即使初始連線可能在不同的閘道上開始，連線仍會在交換預先共用金鑰或憑證和對等 *ID* 時，轉移到正確的閘道。

無論您的 VPN 對等是否來自同一廠商，VPN 對等都必須設定相同的 IKE 參數，才能執行成功的 IKE 交涉。

需要符合以下參數才能成功進行 IKE 交涉：

- 用於金鑰交換的 DH 群組
- 加密演算法
- 驗證演算法：

例如，如果您已將 VPN 對等 1 的 DH 群組設定為 **group20**、將驗證設定為 **sha384**，以及將加密設定為 **aes-256-gcm**。然後，要與之建立 IPSec 通道的 VPN 對等 2 也應設定相同的值。

- PAN-OS 10.1 和更新版本與 Prisma Access（Panorama 管理）
- #unique_39

定義 IPSec 密碼設定檔

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

IPSec 密碼設定檔會在 IKE 階段 2 中叫用。它會指定當使用自動金鑰 IKE 為 IKE SA 自動產生金鑰時，如何保護通道內資料的安全。

無論您的 VPN 對等是否來自同一廠商，VPN 對等都必須設定相同的 IPSec 參數，才能執行成功的 IPSec 交涉。

當下列參數在 VPN 對等服務之間相符時，IPsec 交涉就會成功：

- IPSec 通訊協定（ESP 或 AH）
- 用於金鑰交換的 DH 群組（或 PFS）
- 加密演算法
- 驗證演算法：

例如，如果您已將 VPN 對等 1 的 IPSec 通訊協定設定為 **ESP**、將 DH 群組設定為 **group20**、將驗證設定為 **sha384**，以及將加密設定為 **aes-256-gcm**。然後，要與之建立 IPSec 通道的 VPN 對等 2 也應設定完全相同的值。

依預設，IPsec 通道上會啟用完美轉送密碼 (PFS)，用於產生更隨機的金鑰。PFS 可這麼做的方式是，在 IPSec SA 交涉期間執行其他金鑰交換來產生新的共用密碼，並將其合併到新的 IPSec SA 金鑰中。設定 PFS 時，請確保兩個 VPN 對等都具有相同的 PFS 設定。IPSec SA 交涉中的任何失敗都會導致無法建立 IPSec 通道。

- PAN-OS 10.1 和更新版本與 Prisma Access（Panorama 管理）
- Prisma Access（雲端管理）

設定 IPSec 通道

這可在何處使用？	我需要什麼？
• Prisma Access（Prisma Access 尚不支援 IPSec 通道傳輸模式） • PAN-OS	無需授權

IPSec 是一套用於保護對等之間通訊的通訊協定。在 IPSec 中，您可以配置各種設定，例如加密和驗證演算法以及安全性關聯逾時。IPSec 模式（通道模式或傳輸模式）就是這樣一種設定。

在設定 IPSec 通道時，您現在可以選取 IPSec 模式作為通道，或選取傳輸模式以建立安全連線。即您可以選擇在通道模式或傳輸模式中對封包進行加密或驗證。PAN-OS® 預設支援通道模式，可在資料（IP 封包）穿過通道時對其進行驗證或加密。從 PAN-OS 11.0.0 開始，您可以使用運輸模式。

通道和傳輸模式之間的差異

通道模式	傳輸方式
加密整個封包，包括 IP 標頭。加密後的封包中會新增一個新的 IP 標頭。	僅加密有效負載，同時保留原始 IP 標頭。
通道監控使用通道介面 IP 位址。	通道監控自動使用實體介面的 IP 位址（閘道介面 IP 位址），忽略通道介面 IP 位址。
支援雙重封裝。	不支援雙重封裝。
此模式通常用於站點到站點通訊。	此模式通常用於主機到主機通訊。

設定 IPSec 通道（通道模式）

這可在何處使用？	我需要什麼？
• Prisma Access • PAN-OS	無需授權

IPSec 通道設定允許您在資料於通道中周遊時驗證和/或加密資料 (IP 封包)。

如果您正在設定防火牆搭配使用支援以政策為基礎 VPN 的對等，您必須定義 Proxy ID。支援以政策為基礎 VPN 的裝置，使用特定的安全性規則/政策或存取清單（來源位址、目的地位址與連接埠）來允許您所要的流量通過 IPSec 通道。在快速模式或 IKE 階段 2 交涉期間會參照這些規則，並

會在程序的第一或第二個訊息中作為 Proxy ID 交換這些規則。因此，如果您正在設定防火牆搭配以政策為基礎的 VPN 對等使用，為了讓階段 2 交涉能夠成功，您必須定義 Proxy ID，讓對等雙方的設定相同。如果未設定 Proxy ID，由於防火牆支援以路由為基礎的 VPN，因此作為 Proxy ID 的預設值為 source ip:0.0.0.0/0，destination ip:0.0.0.0/0 且 application: any；當與對等交換這些值時，會造成無法設定 VPN 連線。

要成功建立 IPSec 通道，IKE 和 IPSec 交涉都應該要成功：

- 只有當兩個 VPN 對等交換相同的已設定 IKE 參數時，IKE 交涉才會成功。
- 只有當兩個 VPN 對等交換相同的已設定 IPSec 參數時，IPSec 交涉才會成功。
- PAN-OS 10.1 和更新版本
- #unique_43
- #unique_44

設定 IPSec 通道（傳輸模式）

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

傳輸模式是從 PAN-OS 11.0.0 版本開始使用的新模式，支援：

- 僅 IPv4 位址。
- 僅裝安全有效負載 (ESP) 通訊協定。
- 僅限 IKEv2。
- 用於 Diffie-Hellman (DH) 群組的 DH-group 20 和 PFS。
- 在 GCM 模式下僅支援具有 256 位元金鑰的 AES。

您可以根據您的網路需求選擇 IPSec 模式：

- 如果要加密新世代防火牆和通道端點之間交換的管理平面通訊協定（例如 BGP）封包，則您必須設定 IPSec 傳輸模式。傳輸模式使您能夠使用最穩健的通訊協定加密控制流量（例如路由通訊協定和訊號訊息）。使用傳輸模式，您可以加密屬於防火牆 IP 位址的點對點流量。
- 如果要加密新世代防火牆和通道端點之間交換的資料平面，則您必須設定 IPSec 通道模式。

啟用傳輸模式之前要記住的要點：

- 啟用 NAT-T 時無法選擇傳輸模式。
- 您無法在環回介面上將 IKE 閘道設定為使用傳輸模式的 IPSec 通道。
- IPSec 傳輸模式不會使用 Proxy ID 設定進行交涉。因此，您無法在傳輸模式下設定 Proxy ID。如果您嘗試透過任何其他方法設定 Proxy ID，其將自動替換為 0.0.0.0/0。
- 您只能將傳輸模式與 **auto-key** 金鑰交換一起使用。

- 如果您設定沒有 IPSec 通道的 IKE 閘道，預設情況下 IKE 會交涉通道模式子安全性關聯 (SA)。
- 在沒有 GRE 封裝的 IPSec 傳輸模式下，請勿透過關聯的通道介面路由使用者流量。在實體介面（例如乙太網路 1/1）而不是通道介面上設定控制通訊協定（例如 BGP 對等工作階段）。BGP 路由的 IPSec 通道模式適用於通道介面，而 BGP 路由的 IPSec 傳輸模式僅適用於實體介面。
- 預設情況下，IPSec 通道會以 **Tunnel**（通道）模式運作。
- 您應該在 **Transport**（傳輸）模式下啟用 **Add GRE Encapsulation**（新增 **GRE** 封裝）以封裝多點傳送封包。

由於 PAN-OS 10.2 及更早版本不支援傳輸模式，因此如果降級至之前的任何版本都會導致相容性問題。在降級之前，您必須手動移除任何傳輸模式通道或切換到通道模式。否則，降級將導致故障。

- PAN-OS 11.0 和更新版本

監控您的 IPSec VPN 通道

這可在何處使用？	我需要什麼？
• PAN-OS	無須授權

若要提供不中斷 VPN 服務，您可以使用防火牆上的無效對等偵測功能及通道監控功能。您也可以監控通道狀態。以下幾節將監控工作進行說明：

- 定義通道監控設定檔
- 檢視通道狀態

為了便於進行疑難排解，您可以啟用/停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道。

定義通道監控設定檔

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

通道監控設定檔可讓您驗證 VPN 對等之間的連線；您可以設定通道介面每隔指定間隔即偵測目的地 IP 位址，並指定如果整個通道通訊中斷時應採取的動作。

STEP 1 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Monitor**（監控）。預設通道監控設定檔可供使用。

STEP 2 | 按一下 **Add**（新增），然後輸入設定檔的 **Name**（名稱）。

STEP 3 | 選取無法連線目的地 IP 位址時要執行的 **Action**（動作）。

- 等待復原—防火牆等待通道復原。防火牆會繼續使用路由決策中的通道介面，如同通道仍然運作中。
- 容錯移轉—如果有可用路徑，強制流量進入備用路徑。防火牆會停用通道介面，並因此停用路由表中任何使用該介面的路由器。

無論是哪一種狀況，防火牆都會嘗試交涉新的 IPSec 金鑰來加速復原。

STEP 4 | 指定觸發指定的動作 **Interval (sec)**（間隔（秒））與 **Threshold**（臨界值）。

- **Threshold**（臨界值）指定了在採取指定動作之前，要等待的活動訊號數（範圍為 2-100；預設值為 5）。
- **Interval (sec)**（間隔（秒））指定活動訊號之間的時間（單位為秒；範圍為 2-10；預設值為 3）。

STEP 5 | 將監控設定檔附加至 IPSec 通道組態。請參閱啟用通道監控。

檢視通道狀態

這可在何處使用？	我需要什麼？
• PAN-OS • Cloud Management	❑ 無需授權 ❑ NGFW Premium 授權的 AIOps

通道狀態會告知您是否已建立有效的 IKE 階段 1 與階段 2 SA，以及通道介面是否有運作且可供傳遞流量。

由於通道介面是邏輯介面，所以無法指示實體連結狀態。因此，您必須啟用通道監控，讓通道介面能夠驗證對 IP 位址的連線，並判定路徑是否仍能使用。如果 IP 位址無法連線，防火牆會等待通道復原或容錯移轉。發生容錯移轉時，現有的通道會被卸除，然後觸發路由變更以設定新的通道並將流量重新導向。

- PAN-OS
- 雲端管理

檢視 IPSec VPN 通道狀態

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。

STEP 2 | 檢視**Tunnel Status**（通道狀態）。

- 綠色表示有效的 IPSec SA 通道。
- 紅色表示 IPSec SA 無法使用或已過期。

STEP 3 | 檢視 **IKE Gateway Status**（**IKE** 閘道狀態）。

- 綠色表示有效的 IKE 階段 1 SA。
- 紅色表示 IKE 階段 1 SA 無法使用或已過期。

STEP 4 | 檢視 **Tunnel Interface Status**（通道介面狀態）。

- 綠色表示通道介面有運作。
- 紅色表示由於已啟用通道監控，且狀態為關閉，因此通道介面已關閉。

若要疑難排解尚未運作的 VPN 通道，請參閱判讀 VPN 錯誤訊息。

檢視 IPSec VPN 通道狀態

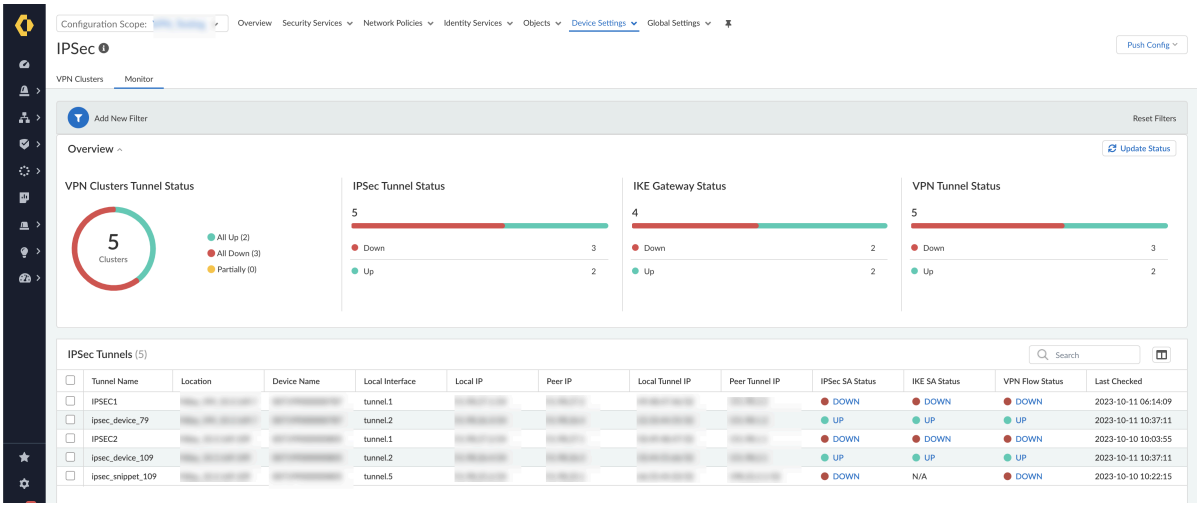
STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（裝置設定） > **IPSec Tunnels**（**IPSec** 通道），然後選取 **Monitor**（監控）。

STEP 3 | 選取 **Configuration Scope**（設定範圍）以檢視 IPSec VPN 通道狀態。您可以從 **Folders**（資料夾）中選取資料夾或防火牆來監控您在防火牆上建立的 IPSec VPN 通道：

- 若要檢視所有防火牆上的 IPSec 通道狀態，請選取 **All Firewalls**（所有防火牆）資料夾。
- 若要檢視與資料夾關聯的防火牆群組的 IPSec 通道狀態，請選取特定資料夾。
- 若要檢視特定防火牆上 IPSec 通道的狀態，請選取該防火牆。

- 如果您使用 *AutoVPN* 建立 *VPN* 叢集，則無法監控這些防火牆的 *IPSec* 通道狀態。
- 您只能監控內部部署防火牆，無法監控 *Prisma Access* 管理的元件。
- 在全域和指令碼片段層級上禁用監控。因此，您可以在全域或指令碼片段設定範圍內建立 *IPSec* 通道，但只能在資料夾或防火牆層級上監控 *IPSec* 通道。



STEP 4 | 檢視 **VPN Cluster Tunnel Status**（**VPN** 叢集通道狀態），這會以圖形方式顯示已啟動的通道數量、已關閉的通道數量以及部分啟動的通道數量。

STEP 5 | 檢視 **IPSec Tunnels**（**IPSec** 通道）中的 **IPSec SA Status**（**IPSec SA** 狀態）。

- 綠色（**UP**（啟動））表示有效的 IPSec SA 通道。選取 **UP**（啟動）可檢視 IPSec 通道的詳細資訊。
- 紅色（**DOWN**（關閉））表示 IPSec SA 不可用或已過期。選取 **DOWN**（關閉)可檢視用來解釋失敗原因的詳細資訊。

STEP 6 | 檢視 **IPSec Tunnels**（**IPSec** 通道）中的 **IKE SA Status**（**IKE SA** 狀態）。

- 綠色（**UP**（啟動））表示有效的 IKE 階段 1 SA。選取 **UP**（啟動）可檢視 IKE 閘道的詳細資訊。
- 紅色（**DOWN**（關閉））表示 IKE 階段 1 SA 不可用或已過期。選取 **DOWN**（關閉**)**可檢視用來解釋失敗原因的詳細資訊。

STEP 7 | 檢視 **VPN Flow Status**（**VPN** 流量狀態）以取得 **IPSec Tunnels**（**IPSec** 通道）中 VPN 流量資訊。

- 綠色（**UP**（啟動**)**）表示 IPSec 通道已啟動。選取 **UP**（啟動）可檢視 VPN 流量的詳細資訊。
- 紅色（**DOWN**（關閉**)**）表示 IPSec 通道已關閉。選取 **DOWN**（關閉**)**可檢視用來解釋失敗原因的詳細資訊。

STEP 8 | 選取 **Add New Filter**（新增篩選），然後選取欄位以檢視以所選欄位為依據的結果。例如，透過從清單中選取 **Device Name**（裝置名稱）來 **Add New Filter**（新增篩選），以檢視所選裝置的 IPSec 通道狀態。

選取 **Reset Filters**（重設篩選**)**Reset Filters來刪除一個或多個篩選。

STEP 9 | 選取 **Update Status**（更新狀態）以更新該等級（防火牆、資料夾或所有防火牆）中存在的所有 IPSec 通道監控資料。

啟用、停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

您可以啟用、停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道，以便進行疑難排解。

- 啟用或停用 IKE 閘道或 IPSec 通道
- 重新整理或重新啟動 IKE 閘道或 IPSec 通道

啟用或停用 IKE 閘道或 IPSec 通道

這可在何處使用？	我需要什麼？
• PAN-OS	無須授權

啟用或停用 IKE 閘道或 IPSec 通道，以便進行疑難排解。

啟用或停用 IKE 閘道。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），然後選取您要啟用或停用的閘道。
2. 在畫面底部按一下 **Enable**（啟用）或 **Disable**（停用）。

啟用或停用 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後選取您要啟用或停用的通道。
2. 在畫面底部按一下 **Enable**（啟用）或 **Disable**（停用）。

重新整理或重新啟動 IKE 閘道或 IPSec 通道

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

您可以重新整理或重新啟動 IKE 閘道或 IPSec 通道。IKE 閘道和 IPSec 通道的重新整理與重新啟動行為如下：

階段	重新整理	重新啟動
IKE 閘道（IKE 階段 1）	更新所選 IKE 閘道的螢幕統計資料。 相當於在 CLI 中發出第二個 `show` 命令 (在初始 `show` 命令之後)。	重新啟動選取的 IKE 閘道。 **IKEv2**:也會重新啟動任何相關聯的子 IPSec 安全性關聯 (SA)。 **IKEv1**:不會重新啟動相關聯的 IPSec SA。 重新啟動會中斷所有現有的工作階段。 相當於在 CLI 中發出 **`clear`**、**`test`**、**`show`** 命令序列。
IPSec 通道（IKE 階段 2）	更新所選 IPSec 通道的螢幕統計資料。 相當於在 CLI 中發出第二個 `show` 命令 (在初始 `show` 命令之後)。	重新啟動 IPSec 通道。 重新啟動會中斷所有現有的工作階段。 相當於在 CLI 中發出 **`clear`**、**`test`**、**`show`** 命令序列。

請注意，重新啟動 IKE 閘道的結果視乎於是 IKEv1 還是 IKEv2。

重新整理或重新啟動 IKE 閘道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後為您要重新整理或重新啟動的閘道選取通道。
2. 在該通道的列中，按一下狀態欄下方的 **IKE Info**（**IKE** 資訊）。
3. 在 IKE 資訊畫面底部，按一下您要的動作：
   - 重新整理—更新畫面上的統計資料。
   - 重新啟動—清除 SA，在 IKE 交涉重新開始且通道重新建立之前捨棄流量。

重新整理或重新啟動 IPSec 通道。

由於您使用通道監控器來監控通道狀態，或使用外部網路監控器來監控透過 IPSec 通道的網路連線狀態，因此您可能會判斷通道需要重新整理或重新啟動。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後選取您要重新整理或重新啟動的通道。
2. 在該通道的列中，按一下狀態欄下方的 **Tunnel Info**（通道資訊）。
3. 在通道資訊畫面底部，按一下您要的動作：
   - 重新整理—更新螢幕統計資料。
   - 重新啟動—清除 SA，在 IKE 交涉重新開始且通道重新建立之前捨棄流量。

站台對站台 VPN 設定範例

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

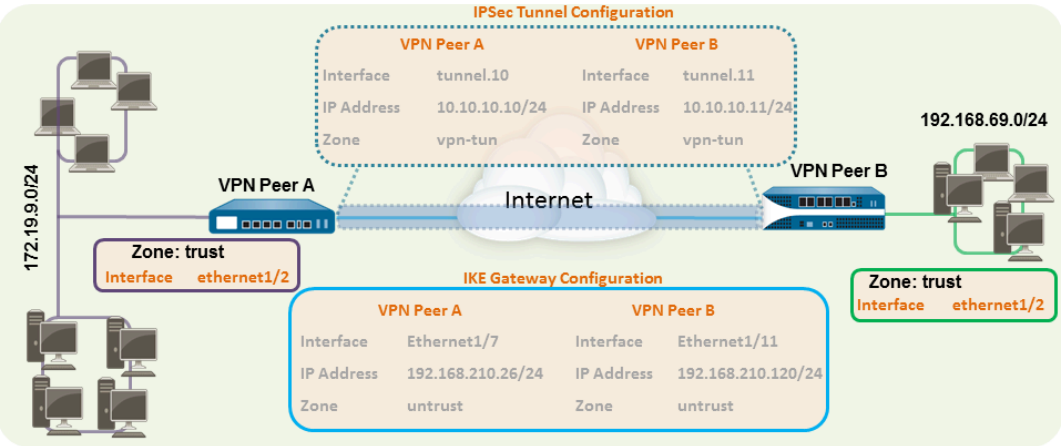
以下幾節提供設定某些常用 VPN 部署的說明：

- 含靜態路由的站台對站台 VPN
- 含 OSPF 的站台對站台 VPN
- 含靜態與動態路由的站台對站台 VPN

含靜態路由的站台對站台 VPN

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

以下範例顯示使用靜態路由的兩個站台之間的 VPN 連線。在沒有動態路由的狀況下，VPN 對等 A 與 VPN 對等 B 上的通道介面不需要 IP 位址，因為防火牆會自動使用通道介面作為在站台之間路由流量的下一個躍點。但是為了啟用通道監控，已將靜態 IP 位址指派給每個通道介面。



STEP 1 | 設定 Layer 3 介面。

此介面用於 IKE 階段 1 通道。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—192.168.210.26/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—192.168.210.120/24

STEP 2 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.1**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱）（例如 *vpn-tun*），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. （選用）若要將 IP 位址指定至通道介面，請選取 **IPv4** 或 **IPv6** 頁籤，按一下 [IP] 區段中按一下**Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩。

   在使用靜態路由的狀況下，通道介面不需要 IP 位址。對於目的地為指定子網路/IP 位址的流量，通道介面不會自動變成下一個躍點。如果您想要啟用通道監控，請考慮新增 IP 位址。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.10
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—172.19.9.2/24

   VPN 對等 B 的組態為：
   - 介面—tunnel.11
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—192.168.69.2/24

STEP 3 | 設定虛擬路由器上對目的地子網路的靜態路由。

1. 選取 **Network**（網路） > **Virtual Router**（虛擬路由器），然後按一下您在前一步中定義的路由器。
2. 選取靜態路由，按一下新增，然後輸入新路由以存取通道另一端的子網路。

   在此範例中，VPN 對等 A 的組態為：

   - 目的地—192.168.69.0/24
   - **Interface**（介面）—tunnel.10

   VPN 對等 B 的組態為：

   - **Destination**（目的地）—172.19.9.0/24
   - 介面—tunnel.11

STEP 4 | 設定密碼設定檔（IKE 密碼設定檔適用於階段 1，IPSec 密碼設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼）。在此範例中，我們使用預設設定檔。

STEP 5 | 設定 IKE 閘道。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - 介面—ethernet1/7
   - 本機 **IP** 位址—192.168.210.26/24
   - 對等 **IP** 類型/位址—靜態/192.168.210.120
   - 預先共用金鑰—輸入值
   - 本機識別—請注意，這表示將使用本機 IP 位址作為本機識別值。
   - VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 本機 **IP** 位址—192.168.210.120/24
   - 對等 **IP** 類型/位址—靜態/192.168.210.26
   - 先共用金鑰—輸入與對等 A 相同的值
   - 本機識別—無
3. 選取進階階段 **1** 選項，然後選取您先前建立用於 IKE 階段 1 的 IKE 加密設定檔。

STEP 6 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.10
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto Profile**（**IPSec** 密碼設定檔）—選取在步驟 4 中定義的 IPSec 密碼設定檔。

   VPN 對等 B 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.11
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto Profile**（**IPSec** 密碼設定檔）—選取在步驟 4 中定義的 IPSec 密碼設定檔。
3. （選用）選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要偵測的目的地 IP 位址以驗證連線。一般而言，會為 VPN 對等使用通道介面 IP 位址。
4. （選用）若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 7 | 建立要允許站台（子網路）之間流量的政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

STEP 8 | 提交任何擱置中的組態變更。

按一下 **Commit**（交付）。

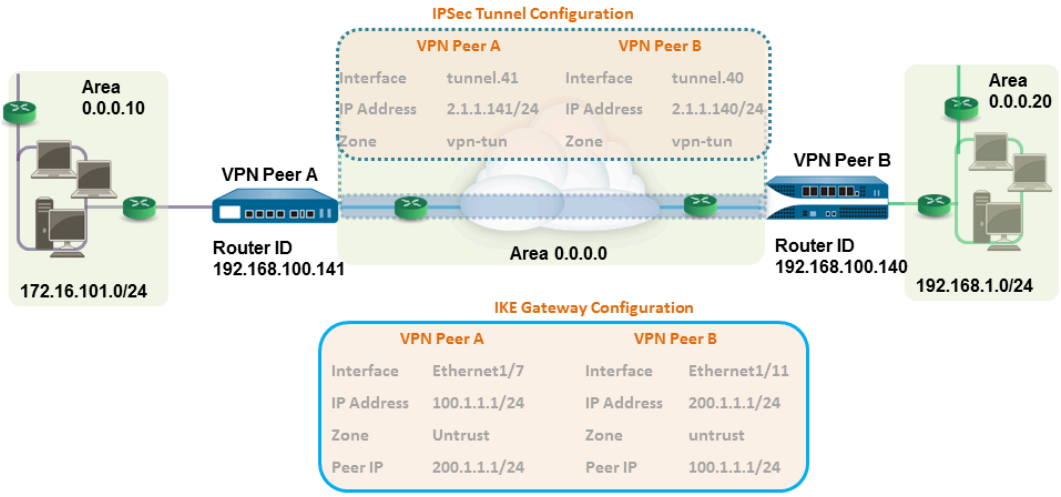
STEP 9 | 測試 VPN 連線。

另請參閱 檢視通道狀態。

含 OSPF 的站台對站台 VPN

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

在此範例中，每個站台會使用 OSPF 進行動態路由流量。系統會靜態指派每個 VPN 對等上的通道 IP 位址，並作為兩個站台之間路由流量時的下一個躍點。



STEP 1 | 在每個防火牆上設定 Layer 3 介面。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）清單中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）清單中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—100.1.1.1/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—200.1.1.1/24

STEP 2 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.11**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱）（例如 vpn-tun），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. 將 IP 位址指派給通道介面，選取 **IPv4** 或 **IPv6** 頁籤，按一下 IP 區段的 **Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩/首碼，例如 172.19.9.2/24。

   此 IP 位址將作為將流量路由至通道的下一個躍點 IP 位址，也可用於監控通道狀態。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.41
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.141/24

   VPN 對等 B 的組態為：
   - **Interface**（介面）—tunnel.40
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.140/24

STEP 3 | 設定密碼設定檔（IKE 密碼設定檔適用於階段 1，IPSec 密碼設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼）。在此範例中，我們使用預設設定檔。

STEP 4 | 在虛擬路由器上設定 OSPF 設定，並在防火牆上附加含適當介面的 OSPF 區域。

如需防火牆上可用 OSPF 選項的詳細資訊，請參閱設定 OSPF。

當有兩個以上的 OSPF 路由器需要交換路由資訊時，請使用 (廣播) 作為連結類型。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取預設路由器或新增路由器。
2. 選取 **OSPF**（適用於 IPv4）或 **OSPFv3**（適用於 Ipv6），然後選取 **Enable**（啟用）。
3. 在此範例中，VPN 對等 A 的 OSPF 組態為：
   - **Router ID**（路由器 **ID**）：192.168.100.141
   - **Area ID**（區域 **ID**）：0.0.0.0，指派給 tunnel.1 介面，連結類型為：p2p
   - **Area ID**（區域 **ID**）：0.0.0.10，指派給 Ethernet1/1 介面，連結類型為：廣播

   VPN 對等 B 的 OSPF 組態為：
   - **Router ID**（路由器 **ID**）：192.168.100.140
   - **Area ID**（區域 **ID**）：0.0.0.0，指派給 tunnel.1 介面，連結類型為：p2p
   - **Area ID**（區域 **ID**）：0.0.0.20，指派給 Ethernet1/15 介面，連結類型為：廣播

STEP 5 | 設定 IKE 閘道。

此範例在 VPN 對等雙方使用靜態 IP 位址。一般而言，總公司會使用靜態設定的 IP 位址，分公司則使用動態設定的 IP 位址；動態 IP 位址並不適用於設定穩定服務，例如 VPN。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 本地 **IP** 位址—100.1.1.1/24
   - 對等 **IP** 位址—200.1.1.1/24
   - 預先共用金鑰—輸入值

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - **Local IP address**（本機 **IP** 位址）—200.1.1.1/24
   - **Peer IP address**（對等 **IP** 位址）—100.1.1.1/24
   - 先共用金鑰—輸入與對等 A 相同的值
3. 選取您先前建立用於 IKE 階段 1 的 IKE 密碼設定檔。

STEP 6 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.41
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。

   VPN 對等 B 的組態為：

   - 通道介面—tunnel.40
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。
3. 選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要 ping 的目的地 IP 位址以驗證連線。
4. 若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 7 | 建立要允許站台（子網路）之間流量的政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

STEP 8 | 使用 CLI 確認 OSPF 相鄰項與路由。

確認兩個防火牆都能看見彼此為完整狀態的網路芳鄰。亦確認 VPN 對等通道介面的 IP 位址與 OSPF 路由器 ID。在每個 VPN 對等上使用下列 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
    admin@FW-B> show routing route type ospf

    flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
           Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


    VIRTUAL ROUTER: vr1 (id 1)
      ==========
    destination             nexthop             metric flags      age   interface
    2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
    172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
    192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
    total routes shown: 3
```

STEP 9 | 測試 VPN 連線。

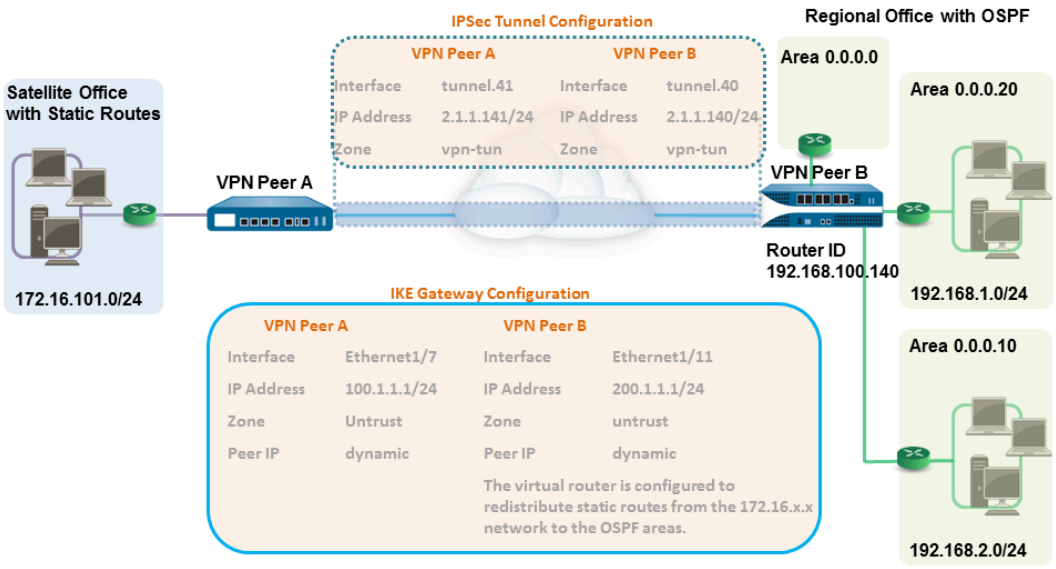
請參閱設定通道連線以及 檢視通道狀態。

含靜態與動態路由的站台對站台 VPN

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

在此範例中，一個站台使用靜態路由，另一個站台使用 OSPF。當兩個位置之間的路由通訊協定不相同時，則必須以靜態 IP 位置設定每個防火牆上的通道介面。因此，為了能交換路由資訊，必須以重新散佈設定檔設定靜態與動態路由程序皆參與的防火牆。設定重新散佈設定檔時，請讓虛擬路由器重新散佈及篩選通訊協定之間的路由—靜態路由、連線的路由及主機—從靜態自發系統到 OSPF 自發系統。若無此重新散佈設定檔，則每個通訊協定會獨自運作，不會與在相同虛擬路由器上執行的其他通訊協定交換任何路由資訊。

在此範例中，衛星辦公室有靜態路由，且所有目的地為 192.168.x.x 網路的流量會路由至 tunnel.41。VPN 對等 B 的虛擬路由器會同時參與靜態和動態路由程序，並用重新散佈設定檔設定，以便將靜態路由傳播 (匯出) 至 OSPF 自發系統。



STEP 1 | 在每個防火牆上設定 Layer 3 介面。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—100.1.1.1/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—200.1.1.1/24

STEP 2 | 設定密碼設定檔（IKE 密碼設定檔適用於階段 1，IPSec 密碼設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼）。在此範例中，我們使用預設設定檔。

STEP 3 | 設定 IKE 閘道。

使用預先共用金鑰時，在設定 IKE 階段 1 通道時若要新增驗證監督，您可以設定（本地識別）與（對等識別）屬性，以及在 IKE 交涉程序中比對的對應值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - 介面—ethernet1/7
   - 本地 **IP** 位址—100.1.1.1/24
   - 對等 **IP** 類型—動態
   - 預先共用金鑰—輸入值
   - 本機識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱)），然後輸入 VPN 對等 A 的值。
   - 對等識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱)），然後輸入 VPN 對等 B 的值

   VPN 對等 B 的組態為：

   - 介面—ethernet1/11
   - **Local IP address**（本機 **IP** 位址）—200.1.1.1/24
   - 對等 **IP** 位址—動態
   - 先共用金鑰—輸入與對等 A 相同的值
   - 本機識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱）），然後輸入 VPN 對等 B 的值
   - 對等識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱）），然後輸入 VPN 對等 A 的值
3. 選取您先前建立用於 IKE 階段 1 的 IKE 密碼設定檔。

STEP 4 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.41**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱）（例如 *vpn-tun*），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. 將 IP 位址指派給通道介面，選取 **IPv4** 或 **IPv6** 頁籤，按一下 IP 區段的 **Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩/首碼，例如 172.19.9.2/24。

   此 IP 位址將用於將流量路由至通道及監控通道狀態。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.41
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.141/24

   VPN 對等 B 的組態為：
   - **Interface**（介面）—tunnel.42
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.140/24

STEP 5 | 指定將流量路由至 192.168.x.x 網路上目的地的介面。

1. 在 VPN 對等 A 上，選取虛擬路由器。
2. 選取 **Static Routes**（靜態路由），再按一下 **Add**（新增），將 tunnel.41 新增為用於路由流量的 **Interface**（介面），並以 192.168.x.x　網路為 **Destination**（目的地）。

STEP 6 | 在虛擬路由器上設定靜態路由與 OSPF 設定，並在防火牆上附加含適當介面的 OSPF 區域。

1. 在 VPN 對等體 B 上，選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取預設路由器或新增路由器。
2. 選取 **Static Routes**（靜態路由），然後按一下 **Add**（新增）將通道 IP 位址新增為 172.168.x.x. 網路中流量的下一個躍點。

   指派所需的路由公制；使用的值愈小，在轉送表格中路由選擇的優先順序愈高。
3. 選取 **OSPF**（適用於 IPv4）或 **OSPFv3**（適用於 Ipv6），然後選取 **Enable**（啟用）。
4. 在此範例中，VPN 對等 # 的 OSPF 組態為：
   - 路由器 ID：192.168.100.140
   - 區域 ID：0.0.0.0，指派給 Ethernet1/12 介面，連結類型為：廣播
   - 區域 ID：0.0.0.10，指派給 Ethernet1/1 介面，連結類型為：廣播
   - 區域 ID：0.0.0.20，指派給 Ethernet1/15 介面，連結類型為：廣播

STEP 7 | 建立重新散佈設定檔，用於將靜態路由插入到 OSPF 自發系統。

1. 在 VPN 對等 B 建立重新散佈設定檔。
   1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取上述使用的路由器。
   2. 選取 **Redistribution Profiles**（重新散佈設定檔），然後按一下 **Add**（新增）。
   3. 輸入設定檔名稱，選取 **Redist**（重新散佈），然後指派 **Priority**（優先順序）值。如果您設定了多個設定檔，第一個會比對優先順序值最小的設定檔。
   4. 將 **Source Type**（來源類型）設為 **static**（靜態），然後按一下 **OK**（確定）。將使用步驟 6 中所定義的靜態路由進行重新散佈。
2. 將靜態路由插入到 OSPF 系統中。
   1. 選取 **OSPF** > **Export Rules**（匯出規則）（適用於 IPv4）或 **OSPFv3** > **Export Rules**（匯出規則）（適用於 IPv6）。
   2. 按一下 **Add**（新增），然後選取您建立的重新散佈設定檔。
   3. 選取將外部路由帶入 OSPF 系統中的方式。預設選項為 **Ext2**，僅使用外部公制計算路由總成本。若內部與外部 OSPF 公制都要使用，請使用 **Ext1**。
   4. 為插入到 OSPF 系統中的路由指派 **Metric**（公制）（成本值）。此選項可讓您在插入的路由進入 OSPF 系統時變更其公制。
   5. 按一下 **OK**（確定）。

STEP 8 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.41
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。

   VPN 對等 B 的組態為：

   - 通道介面—tunnel.40
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。
3. 選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要 ping 的目的地 IP 位址以驗證連線。
4. 若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 9 | 建立要允許站台（子網路）之間流量的政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

STEP 10 | 使用 CLI 確認 OSPF 相鄰項與路由。

確認兩個防火牆都能看見彼此為完整狀態的網路芳鄰。亦確認 VPN 對等通道介面的 IP 位址與 OSPF 路由器 ID。在每個 VPN 對等上使用下列 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

以下為每個 VPN 對等的輸出範例。

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | 測試 VPN 連線。

請參閱設定通道連線以及 檢視通道狀態。

疑難排解

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

本章分享測試 VPN 連線和解釋 VPN 錯誤訊息（若有遇到）的工作。使用 CLI 命令監控站台對站台 VPN 連線並進行疑難排解。

- 針對您的 IPsec VPN 通道連線進行疑難排解
- 使用 CLI 對站台對站台 IPSec VPN 通道問題進行疑難排解

針對您的 IPsec VPN 通道連線進行疑難排解

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

測試您的 IPSec VPN 連線並對其進行疑難排解除，以實現最佳效能：

- 測試 VPN 連線
- 判讀 VPN 錯誤訊息

測試 VPN 連線

這可在何處使用？	我需要什麼？
• PAN-OS	無須授權

執行此工作以測試 VPN 連線。

STEP 1 | ping 通道另一端的主機或使用下列 CLI 命令啟動 IKE 階段 1：

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 輸入下列命令，測試是否已設定 IKE 階段 1：

```
show vpn ike-sa gateway <gateway_name>
```

檢查輸出中是否顯示 security association（安全性關聯 - SA）。如果沒有，則檢閱系統日誌訊息以判讀失敗原因。

STEP 3 | ping 通道另一端的主機或使用下列 CLI 命令啟動 IKE 階段 2：

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | 輸入下列命令，測試是否已設定 IKE 階段 2：

```
show vpn ipsec-sa tunnel <tunnel_name>
```

檢查輸出中是否顯示 security association（安全性關聯 - SA）。如果沒有，則檢閱系統日誌訊息以判讀失敗原因。

STEP 5 | 若要檢視 VPN 流量資訊，請使用下列命令：

```
show vpn flow total tunnels configured:            1 filter - type
 IPSec, state any total IPSec tunnel configured:       1 total
 IPSec tunnel shown:                1 name                    id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

判讀 VPN 錯誤訊息

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

下表列出系統日誌中記錄的常見 VPN 錯誤訊息。

表 **2: VPN** 問題的系統日誌錯誤訊息

如果錯誤如下：	請嘗試：

`IKE phase-1 negotiation is failed as initiator, main mode.Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`
或
`IKE phase 1 negotiation is failed.Couldn’ t find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]`
	• 確認 IKE 閘道組態中每個 VPN 對等的公開 IP 位址皆正確。
	• 確認可 ping 到 IP 位址，且路由問題不會造成連線失敗。

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x(500) to y.y.y.y(500), ignored...`
或
`IKE phase-1 negotiation is failed.Unable to process peer’ s SA payload.`
	檢查 IKE 密碼設定檔組態，確認雙方的提案有共同的加密、驗證及 DH 群組提案。

`pfs group mismatched:my:2peer:0` 或	檢查 IPSec Crypto 設定檔組態以確認：

如果錯誤如下：	請嘗試：
`IKE phase-2 negotiation failed when processing SA payload.No suitable proposal found in peer' s SA payload.`	• VPN 對等雙方的 PFS 為啟用或停用 • 每個對等提案的 DH 群組至少有一個共用的 DH 群組
`IKE phase-2 negotiation failed when processing Proxy ID.Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.`	某一端的 VPN 對等使用的是基於政策的 VPN。您必須在 Palo Alto Networks 防火牆上設定 Proxy ID。請參閱建立 Proxy ID 以識別 VPN 對等。
提交錯誤：已達到通道介面 `tunnel.x` 多重綁定限制 `(xx)`。	您一定是已達到防火牆支援的 Proxy ID 上限。在建立 IPSec 通道之前，請檢查防火牆可支援的 Proxy ID 上限。 在您為 VPN 對等設定 Proxy ID 之前，建議您先檢查防火牆可支援的 Proxy ID 上限。如果您想要實作的 IPSec VPN 通道需要的 Proxy ID 數量超過防火牆支援的數量上限，請依照下列步驟操作： • 使用相同的階段 1 和階段 2 組態來設定另一個通道。 • 對 Proxy ID 的 IP 位址使用 SuperNet。例如，不要使用 10.1.0.0/16、10.2.0.0/16，而是使用 SuperNet 將範圍設定到 10.0.0.0/8，以避免多個項目
`Proxy ID` 不相符	Proxy ID 不符將導致無法建立站台對站台的 IPSec VPN 通道。因此，在兩個 VPN 對等上設定相同的 Proxy ID 即可成功建立站台對站台的 IPSec VPN 通道。 例如：在站台對站台的 IPSec 通道設定中，如果一個 VPN 對等設定了網路遮罩為 /32 的 IP 位址，而遠端 VPN 對等體設定了相同的 IP 位址，但網路遮罩是不同的 /16，則將導致 VPN 通道建立失敗。

如果錯誤如下：	請嘗試：
	其他防火牆廠商的 *Proxy ID* 稱為存取清單或存取控制清單 *(ACL)*。 VPN 對等中的 Proxy ID 應該是彼此的精確鏡像（即相反），但不是相符。 VPN 對等用於建立 IPSec VPN 通道的 Proxy ID 組態範例： 如果 VPN 防火牆 1 設定 192.0.2.0/24 作為本機 ID，並設定 192.0.2.25/24 作為對等 ID。則 VPN 防火牆 2 必須設定 192.0.2.25/24 作為本機 ID，並設定 192.0.2.0/24 作為對等 ID。

使用 CLI 對站台對站台 VPN 問題進行疑難排解

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

使用下列 CLI 命令對階段 1 和階段 2 站台到站台 VPN 問題進行疑難排解：

- 顯示命令
- 清除命令
- 測試命令
- 偵錯命令

顯示命令

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您想要...	使用...
• 顯示所有 VPN 通道的基本統計資料	`> show running tunnel flow info`
• 顯示指定閘道的 IKE SA	`> show vpn ike-sa gateway <gateway> | match <x.x.x.x/Y>`
• 顯示指定通道的 IKE SA	`> show vpn ike-sa tunnel <tunnel>`
• 顯示 IPSec 計數器	`> show vpn flow`
• 顯示所有 IPSec 閘道清單及其設定	`> show vpn gateway`
• 顯示 IKE 階段 1 SA	`> show vpn ike-sa`

如果您想要...	使用...
• 顯示 IKE 階段 2 SA	`> show vpn ipsec-sa`
• 顯示自動金鑰 IPSec 通道組態清單	`> show vpn tunnel`

清除命令

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您想要...	使用...
• 刪除指定閘道的 IKEv1 IKE SA	`> clear vpn ike-sa gateway <gateway>`
• 刪除指定通道的 IKEv1 IKE SA	`> clear vpn ike-sa tunnel <tunnel>`
• 刪除指定通道的 IKEv1 IPSec SA	`> clear vpn ipsec-sa tunnel <tunnel>`

測試命令

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您想要...	使用...
• 啟動與指定閘道的 IKE 交涉	`> test vpn ike-sa gateway <gateway>`
• 為指定通道啟動 IPSec 交涉	`> test vpn ipsec-sa tunnel <tunnel>`

偵錯命令

這可在何處使用？	我需要什麼？
• PAN-OS	無需授權

如果您想要...	使用...
• 開啟偵錯以檢視詳細的記錄和狀態	`> debug ike global on debug less mp-log ikemgr.log debug ike stat`
• packet capture（封包擷取 - pcap），用於檢視和擷取主要、積極和快速的模式交涉。	`> debug ike pcap on view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap`
• 關閉偵錯	`> debug ike pcap off`