使用Palo Alto防火牆配置安全訪問

目錄

簡介

本文檔介紹如何使用Palo Alto防火牆配置安全訪問。

必要條件

- 設定使用者啟動設定
- ZTNA SSO身份驗證配置
- 配置遠端訪問VPN安全訪問

需求

思科建議您瞭解以下主題：

- Palo Alto 11.x版防火牆
- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA
- 無客戶端ZTNA

採用元件

本文檔中的資訊基於：

- Palo Alto 11.x版防火牆

- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

安全訪問- Palo Alto

思科設計了安全訪問，可保護並提供對內部和基於雲的私有應用的訪問。它還保護從網路到Internet的連線。這透過實施多種安全方法和層來實現，所有這些方法都旨在保護透過雲訪問資訊時

所需的資訊。

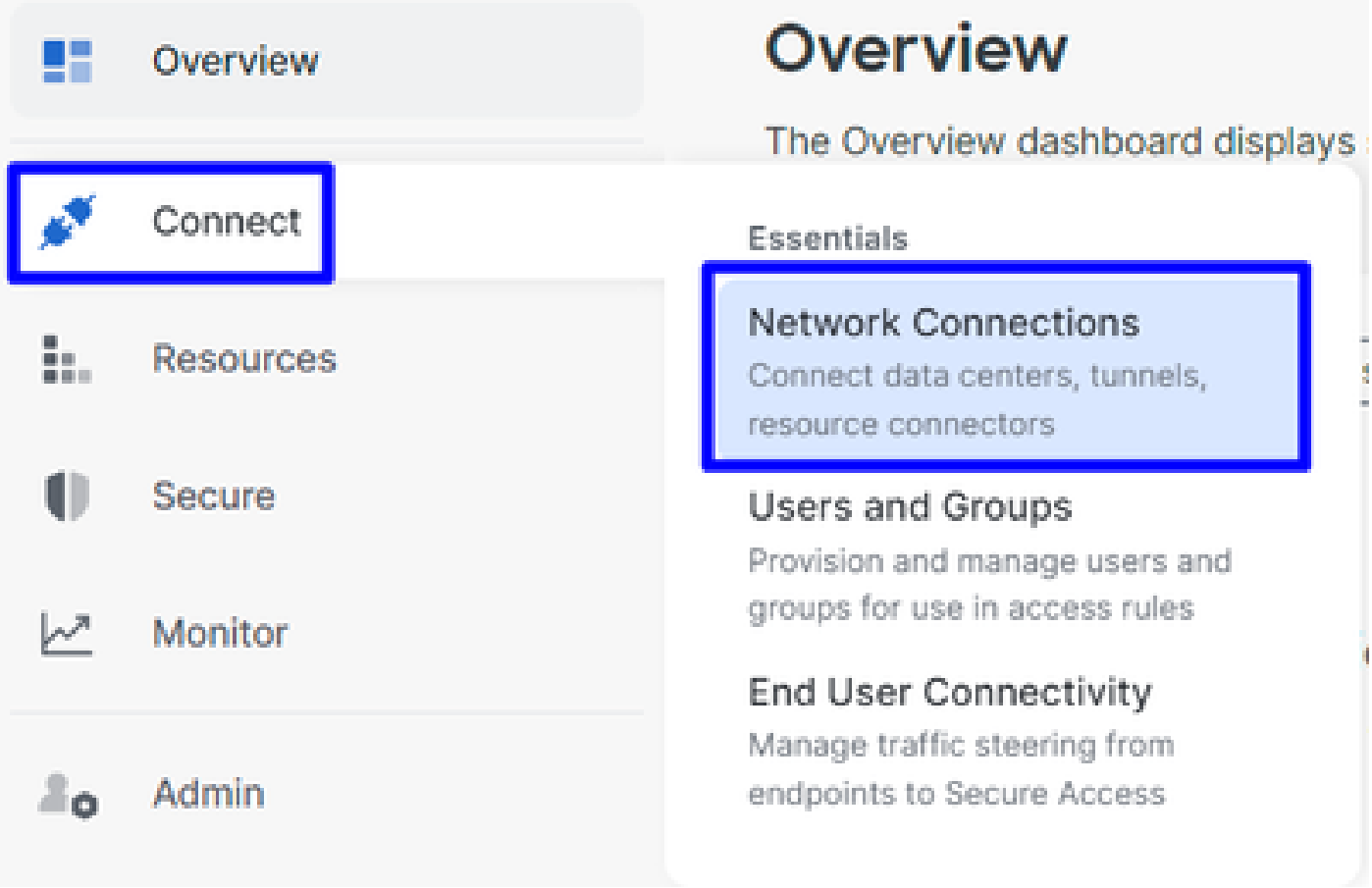
設定

在安全訪問上配置VPN

導航到[安全訪問](#)的管理面板。

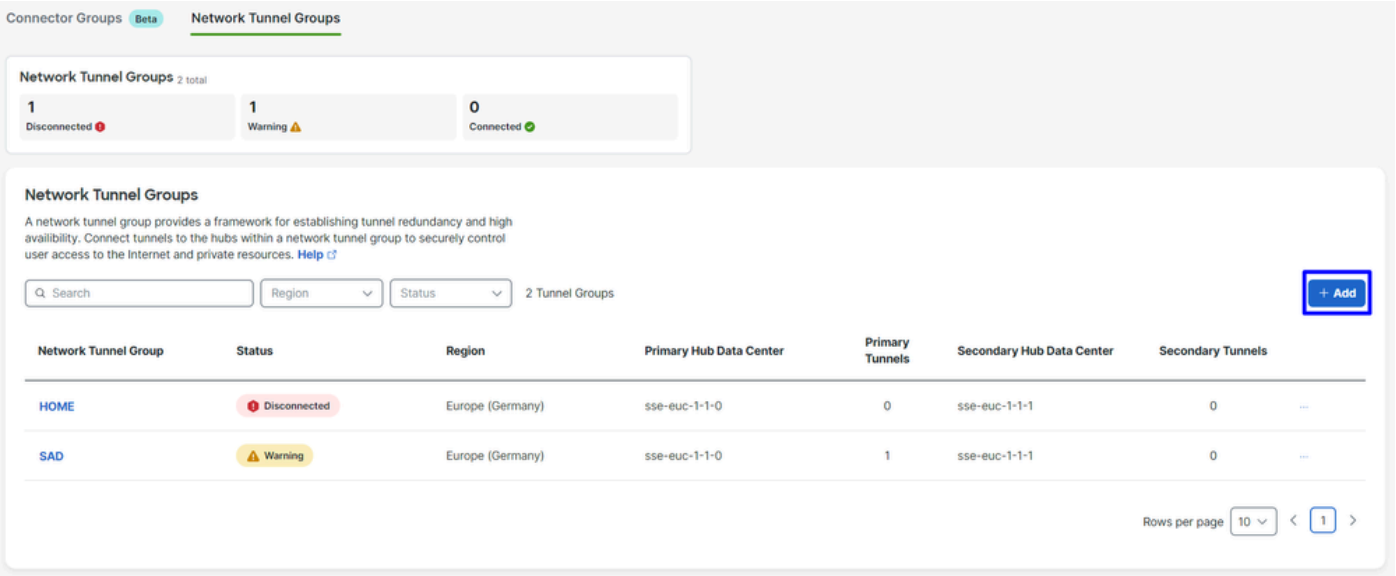
安全存取-首頁

- 按一下 Connect > Network Connections



安全訪問-網路連線

- 在Network Tunnel Groups下，按一下 + Add



安全訪問-網路隧道組

- 配置Tunnel Group Name、Region和 Device Type
- 按一下 **Next**

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Palo Alto

Region

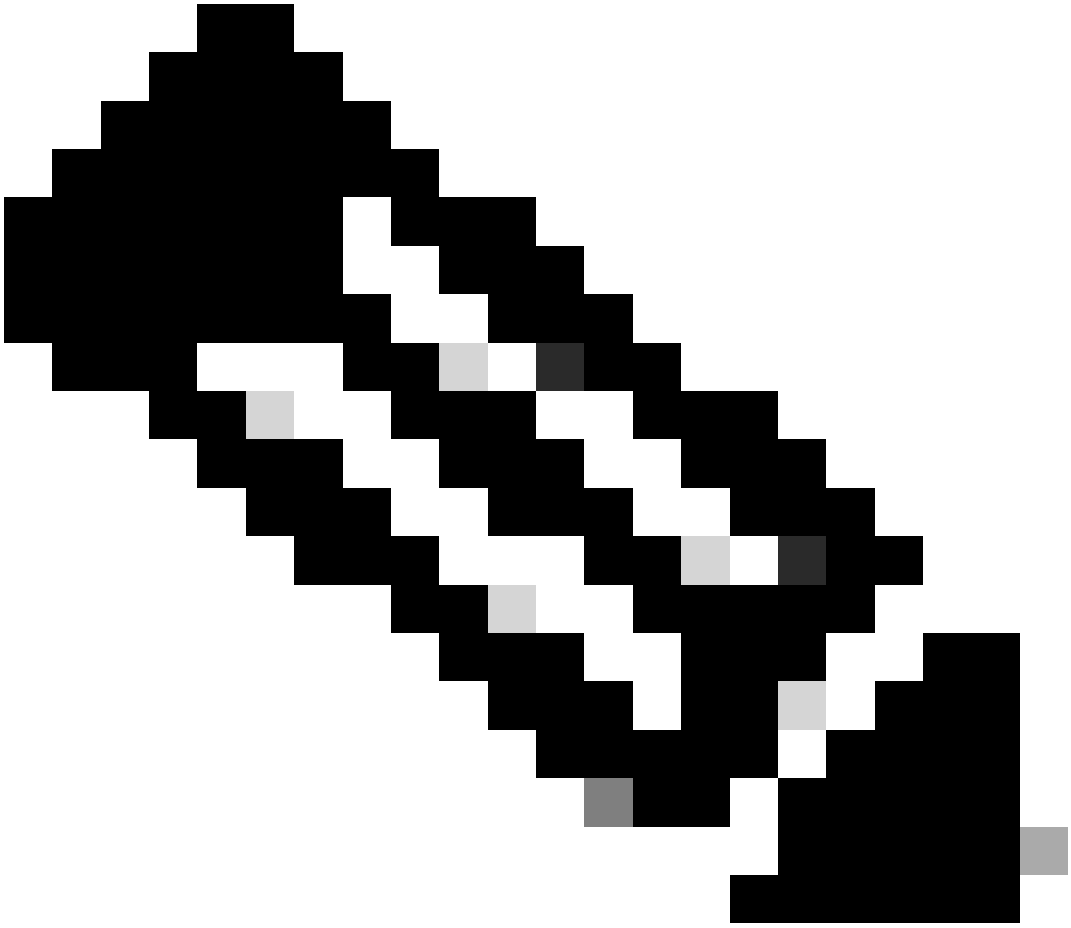
Europe (Germany)

Device Type

Other

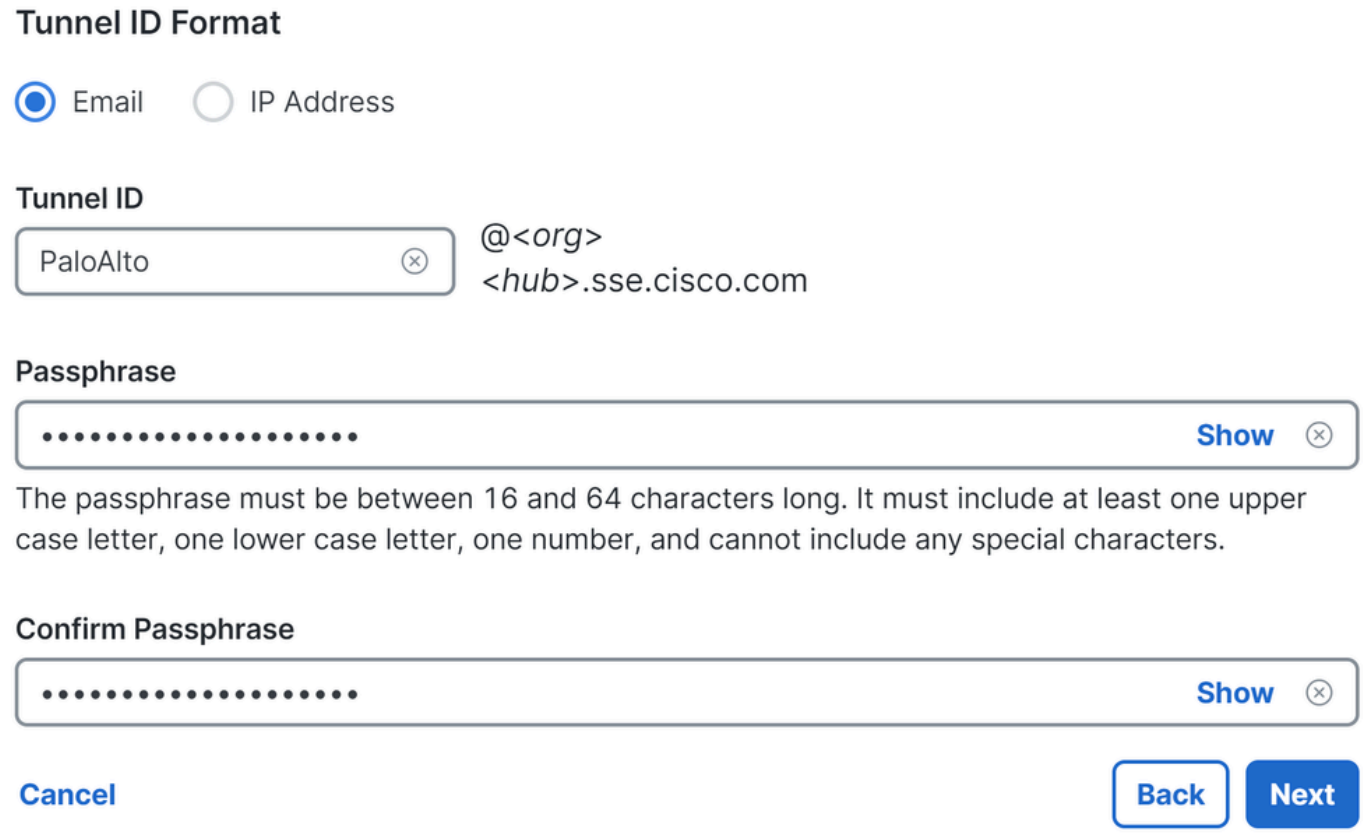
Cancel

Next

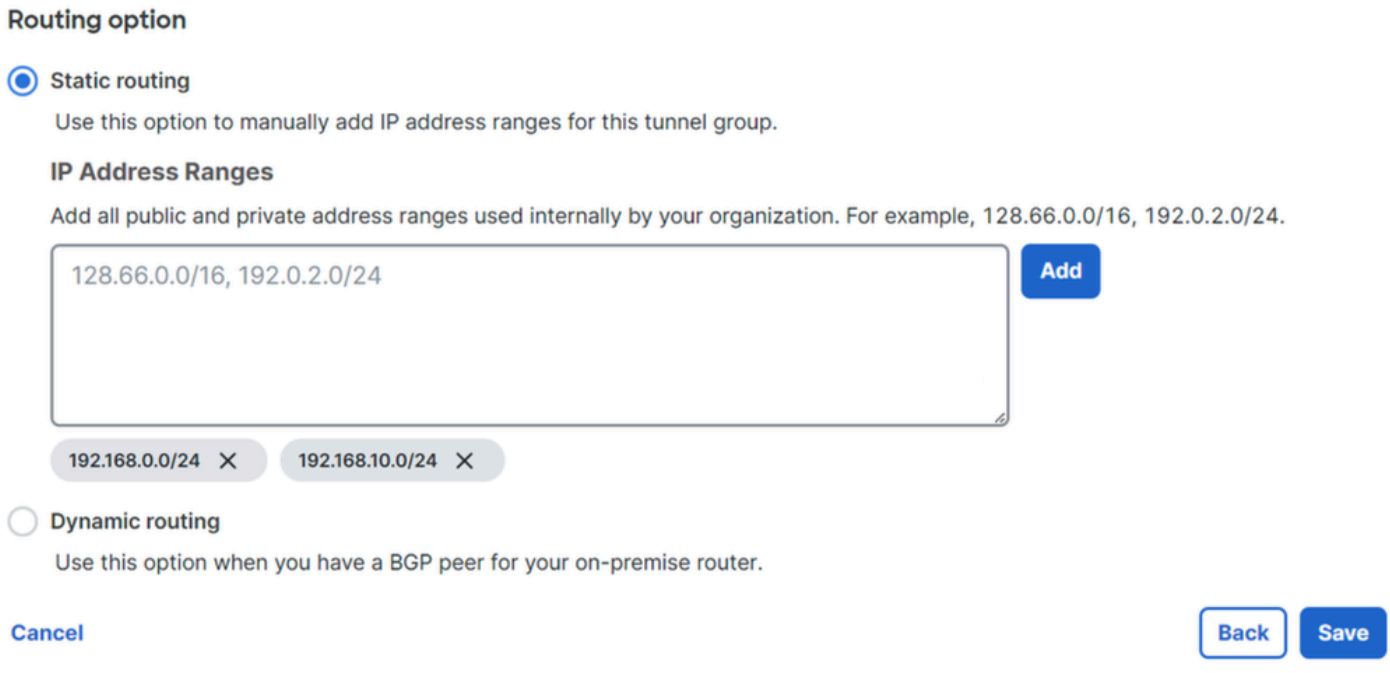


附註：選擇最接近防火牆位置的區域。

- 配置Tunnel ID Format和 Passphrase
- 按一下 Next



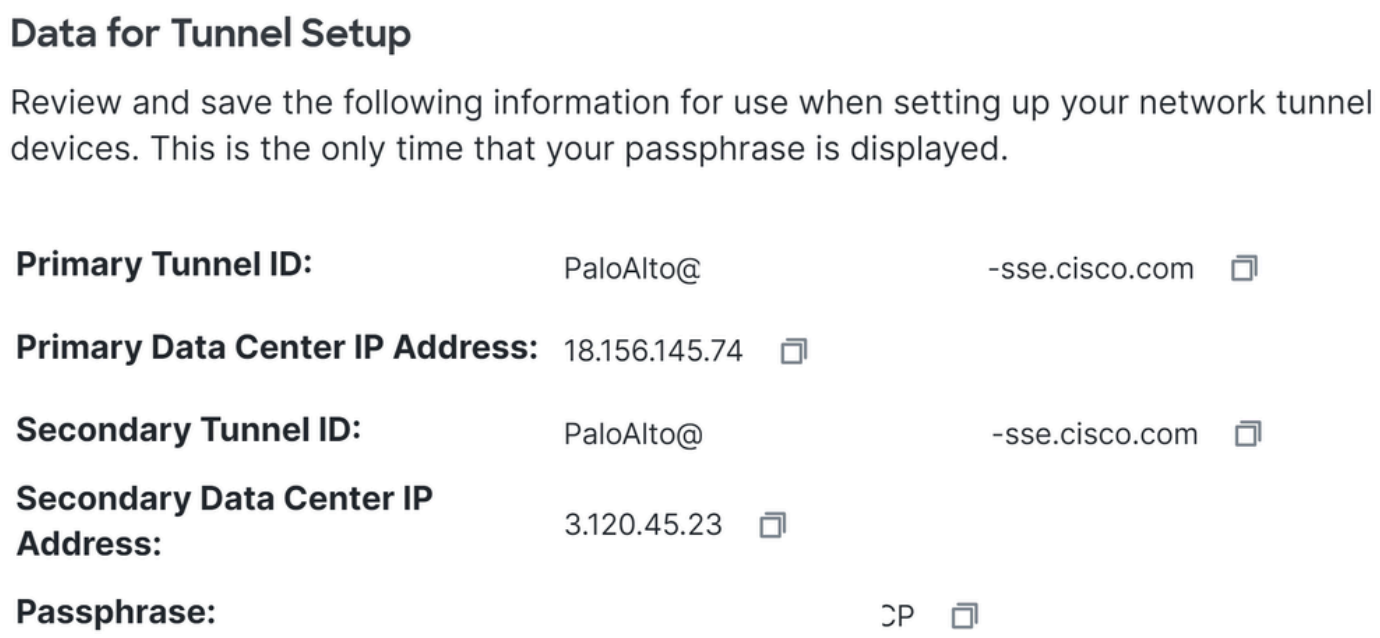
- 配置已在網路上配置且希望透過安全訪問傳輸流量的IP地址範圍或主機
- 按一下 **Save**



安全訪問-隧道組-路由選項

按一下顯示**Save** 的隧道資訊後，請儲存該資訊以用於下一步**Configure the tunnel on Palo Alto**。

通道資料

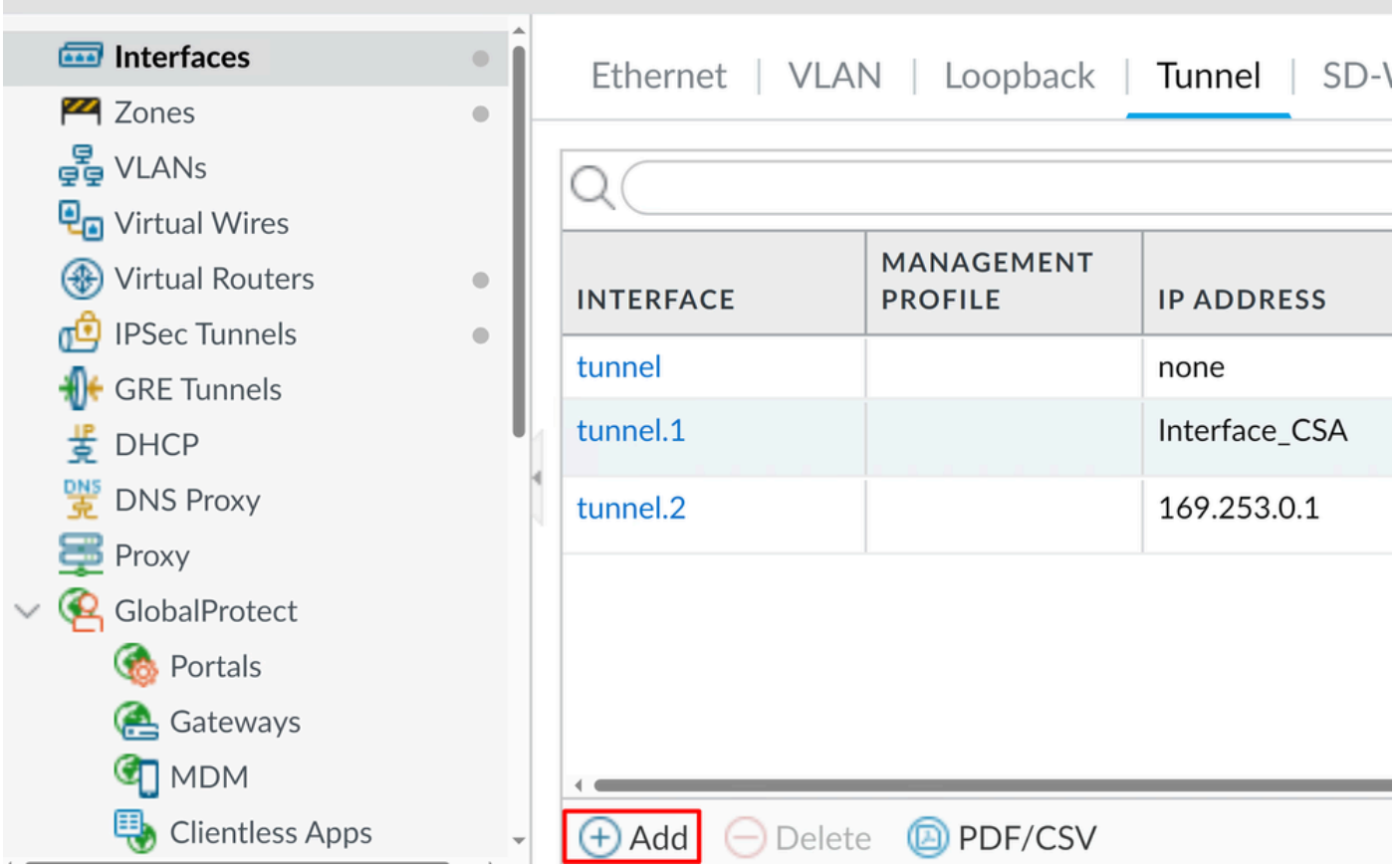


在Palo Alto上配置隧道

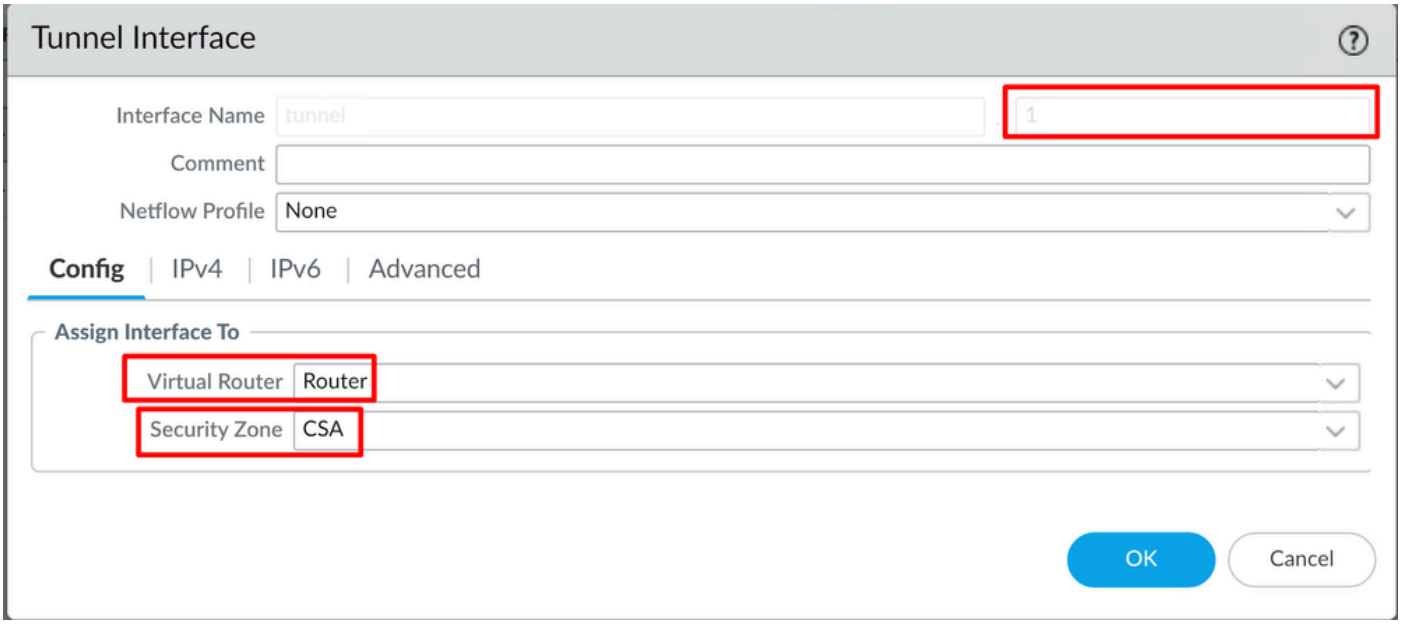
配置隧道介面

導航至Palo Alto Dashboard。

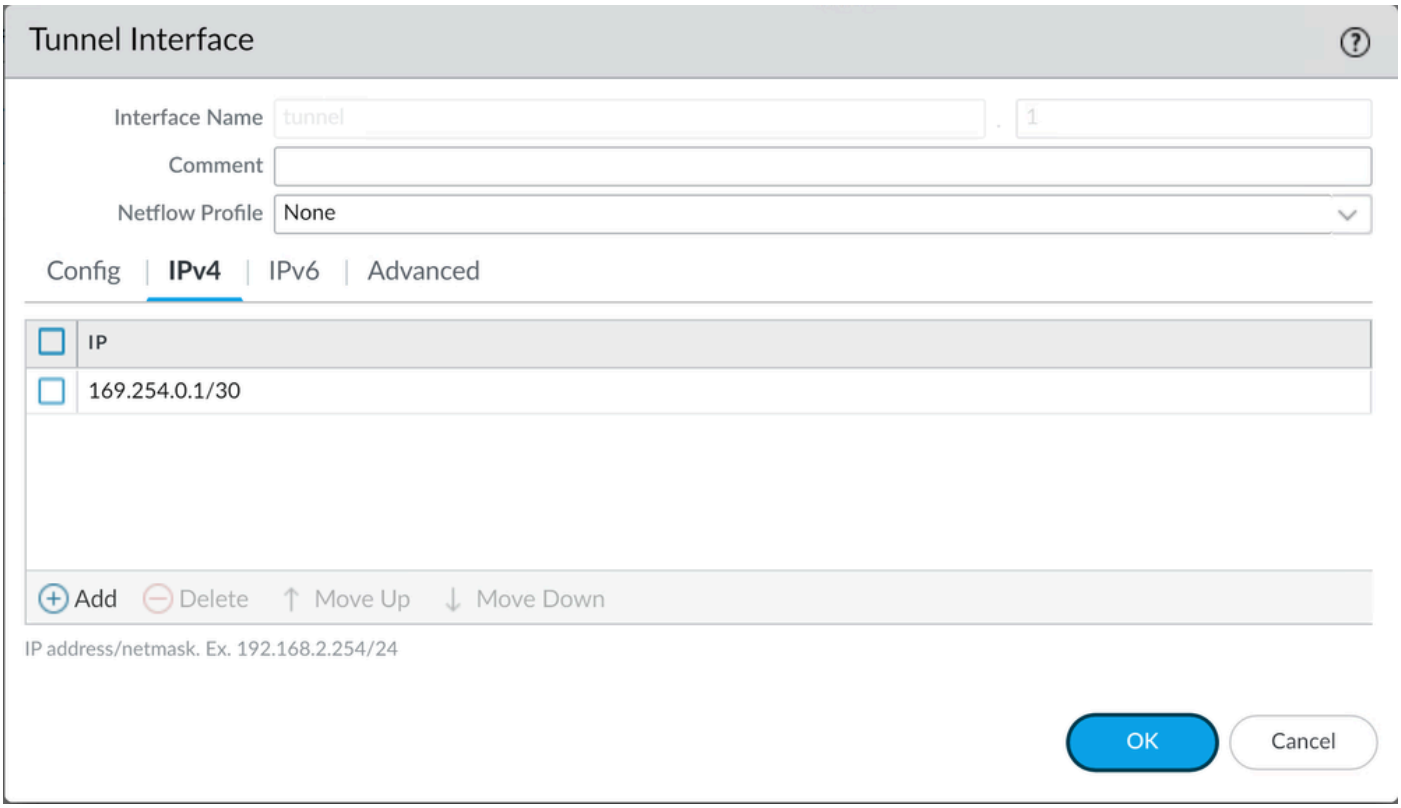
- Network > Interfaces > Tunnel
- Click Add



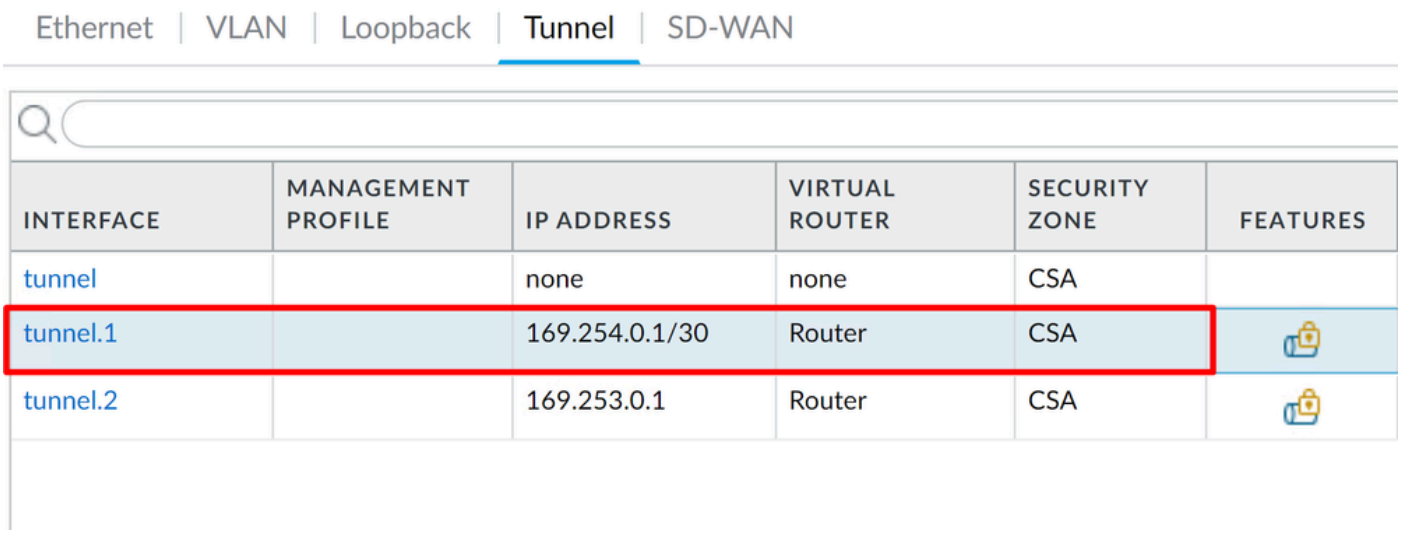
- 在Config下，配置Virtual Router、Security Zone並將Suffix Number



- 在IPv4下，配置一個不可路由的IP。例如，您可以使用 169.254.0.1/30
- 按一下OK



之後，您可以設定以下類似設定：

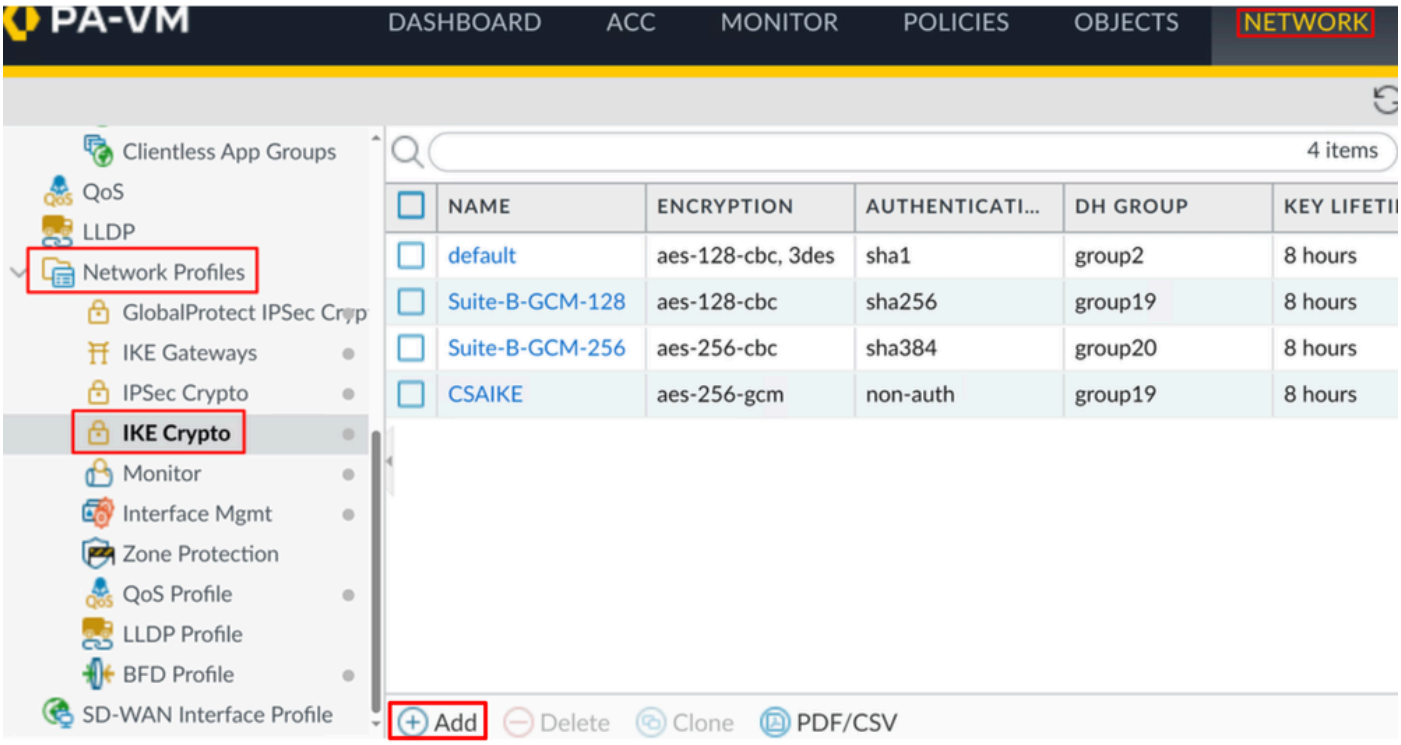


如果已按照如下方式配置該配置，您可以點選**Commit** 儲存配置，然後繼續下一步Configure IKE Crypto Profile。

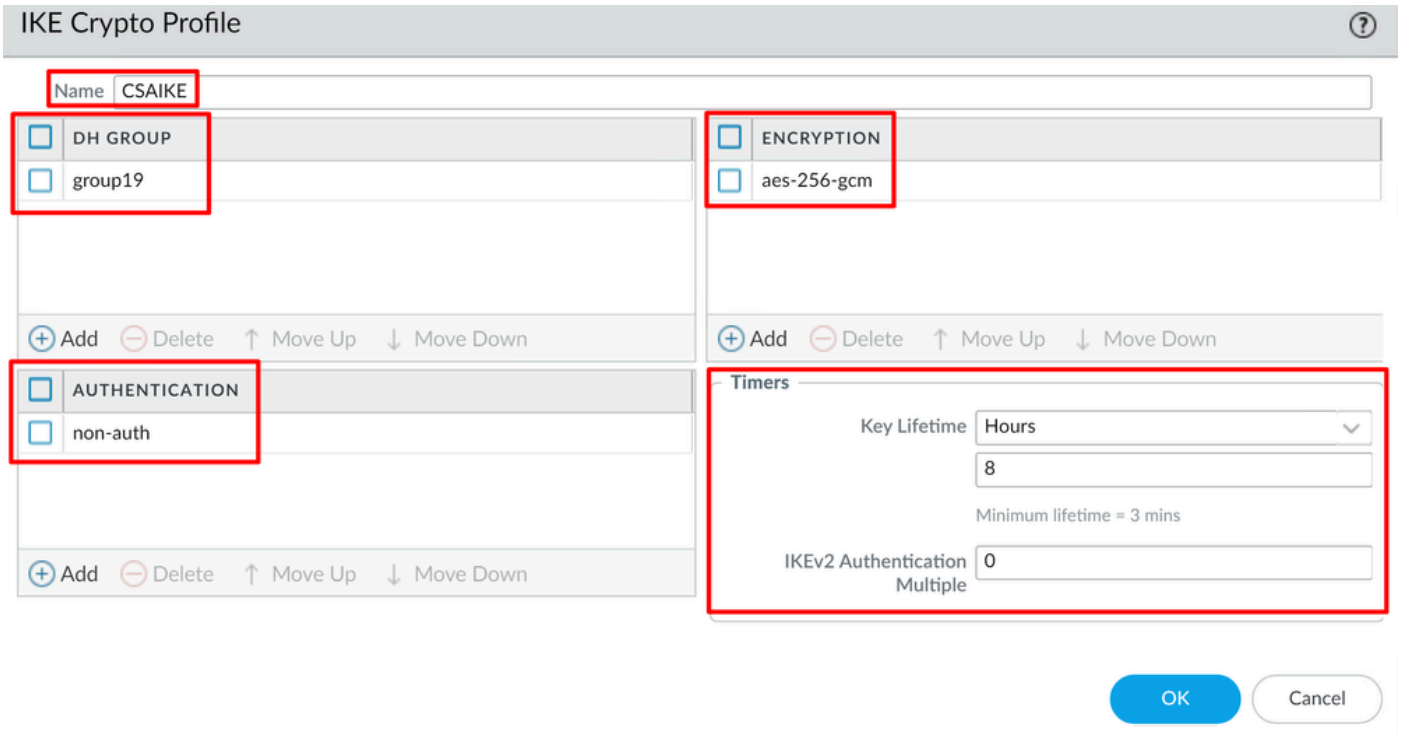
配置IKE加密配置檔案

要配置加密配置檔案，請導航到：

- Network > Network Profile > IKE Crypto
- 按一下Add



- 配置下一個引數：
  - **Name**：配置標識配置檔案的名稱。
    - **DH GROUP**：組19
    - **AUTHENTICATION**：非身份驗證
    - **ENCRYPTION**： aes-256-gcm
    - Timers
      - Key Lifetime：8小時
        - **IKEv2 Authentication**:0
- 完成所有配置後，按一下 **OK**

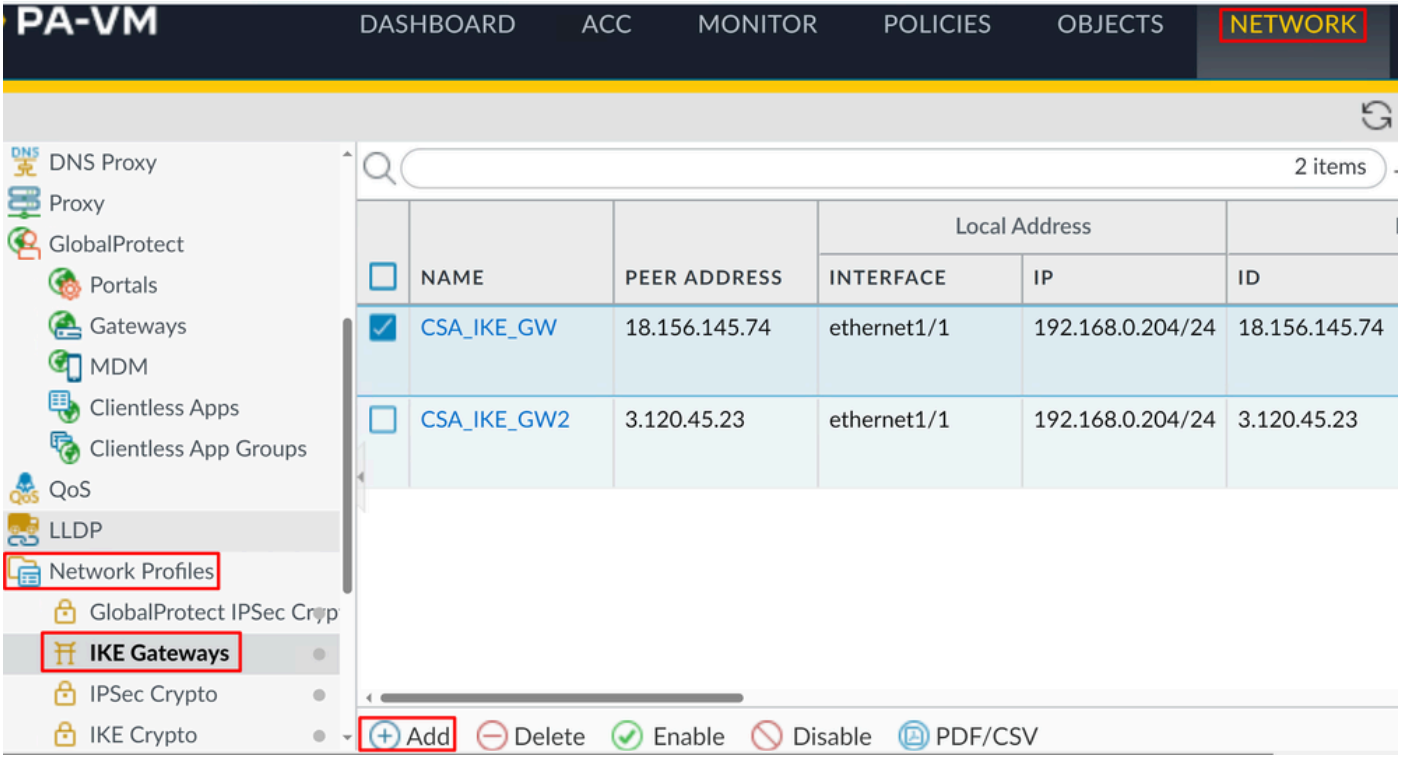


如果已按照如下方式配置該配置，可以點選**Commit** 儲存配置，然後繼續下一步， Configure IKE Gateways.

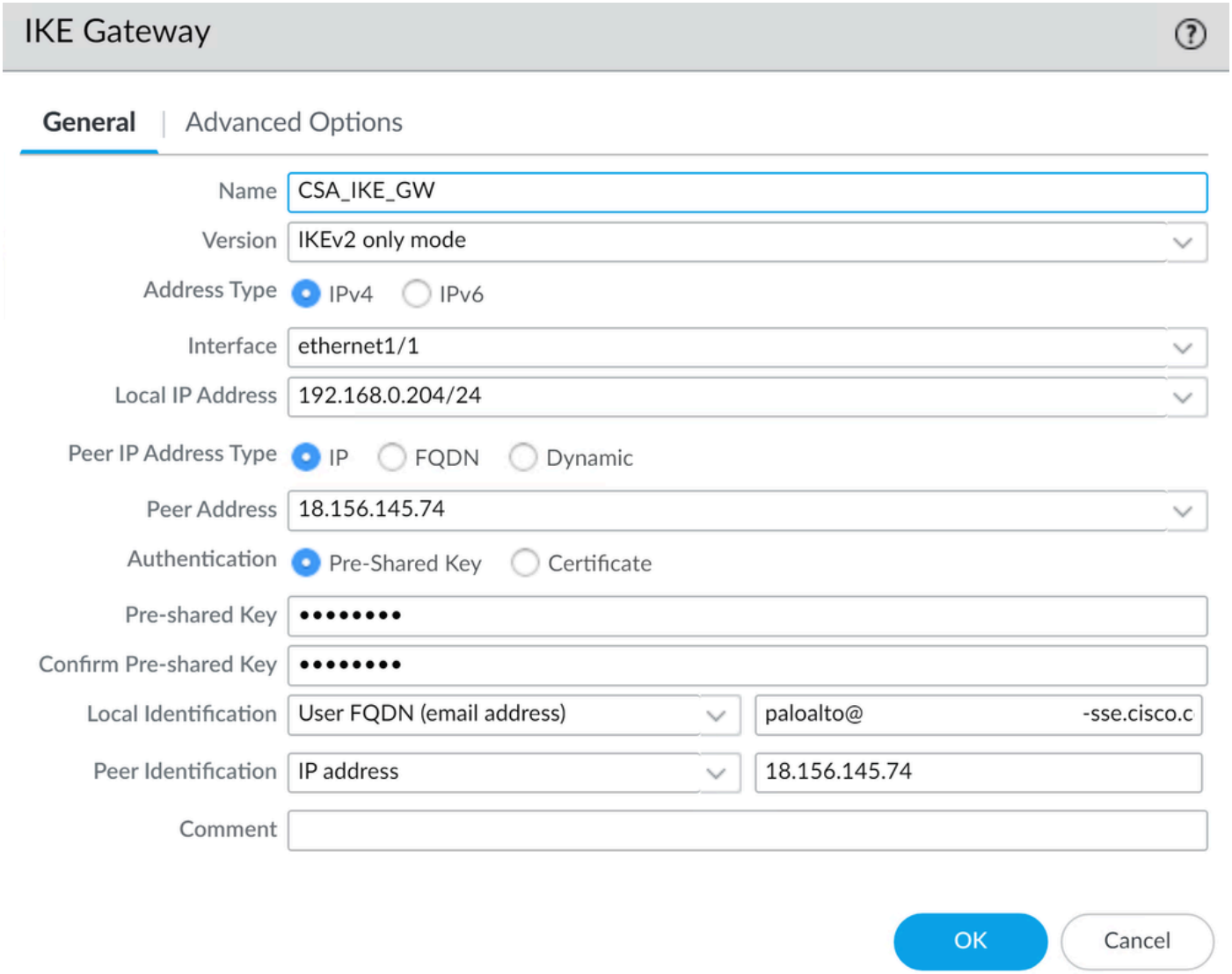
配置IKE網關

配置IKE網關

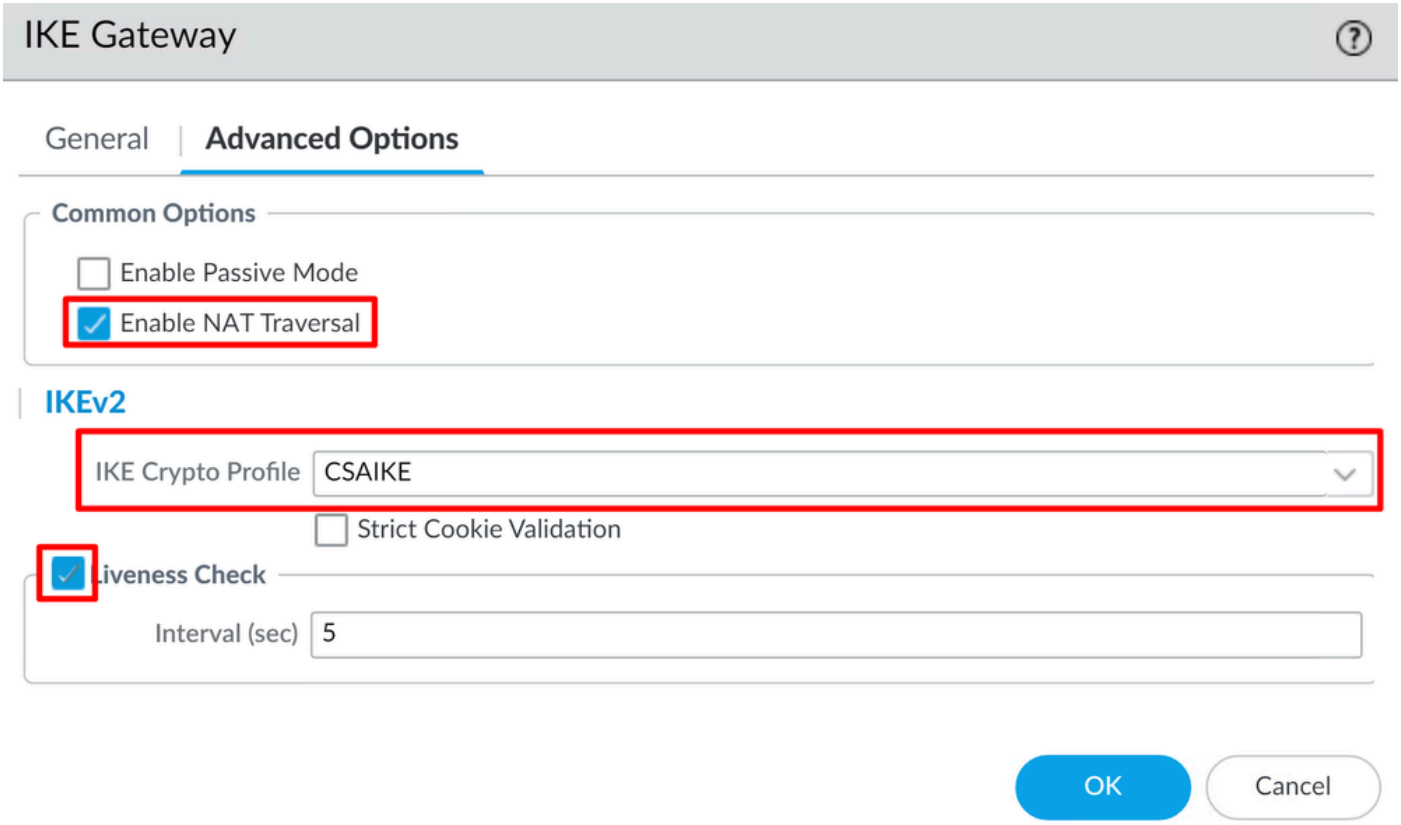
- Network > Network Profile > IKE Gateways
- 按一下Add



- 配置下一個引數：
  - Name：配置用於標識Ike網關的名稱。
    - **Version** ：僅IKEv2模式
    - Address Type ： IPv4
    - **Interface** ：選擇您的Internet WAN介面。
    - Local IP Address：選擇您的Internet WAN介面的IP。
    - **Peer IP Address Type** :IP
    - Peer Address：使用隧道資料步驟中指定的Primary IP Datacenter IP AddressIP。
    - Authentication：預共用金鑰
    - Pre-shared Key ：使用步驟Tunnel Data中給出的 **passphrase** 命令。
    - **Confirm Pre-shared Key** ：使用步驟Tunnel Data中給出的 **passphrase** 命令。
    - **Local Identification** ：選擇**User FQDN (Email address)** 並使用步驟Tunnel Data中給出的**Primary Tunnel ID** 命令。
    - **Peer Identification** ：選IP Address擇並使用Primary IP Datacenter IP Address。



- 按一下Advanced Options
    - **Enable NAT Traversal**
        - 在步驟Configure IKE Crypto Profile中選擇**IKE Crypto Profile** 建立的
        - 標示核取方塊 **Liveness Check**
        - 按一下 **OK**

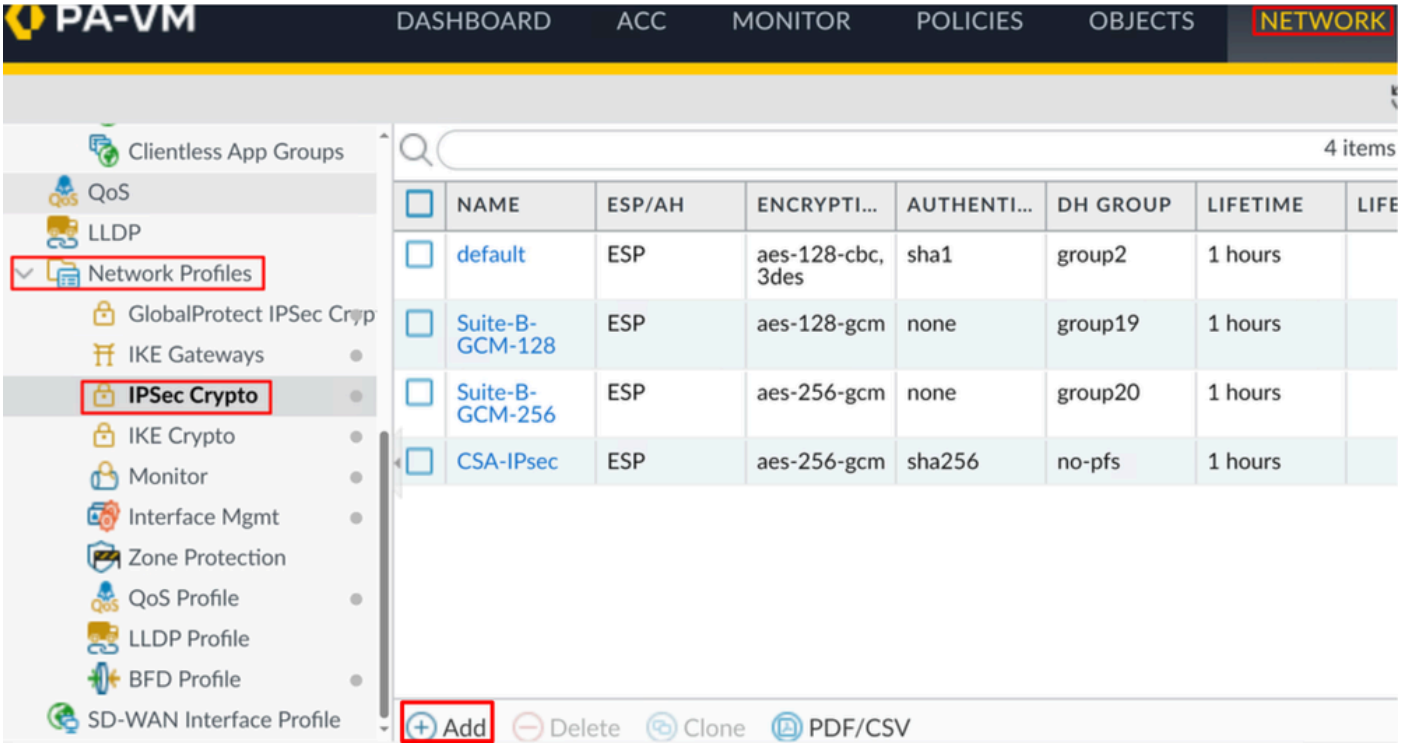


如果已按照如下方式配置該配置，可以點選**Commit** 儲存配置，然後繼續下一步， Configure IPSEC Crypto.

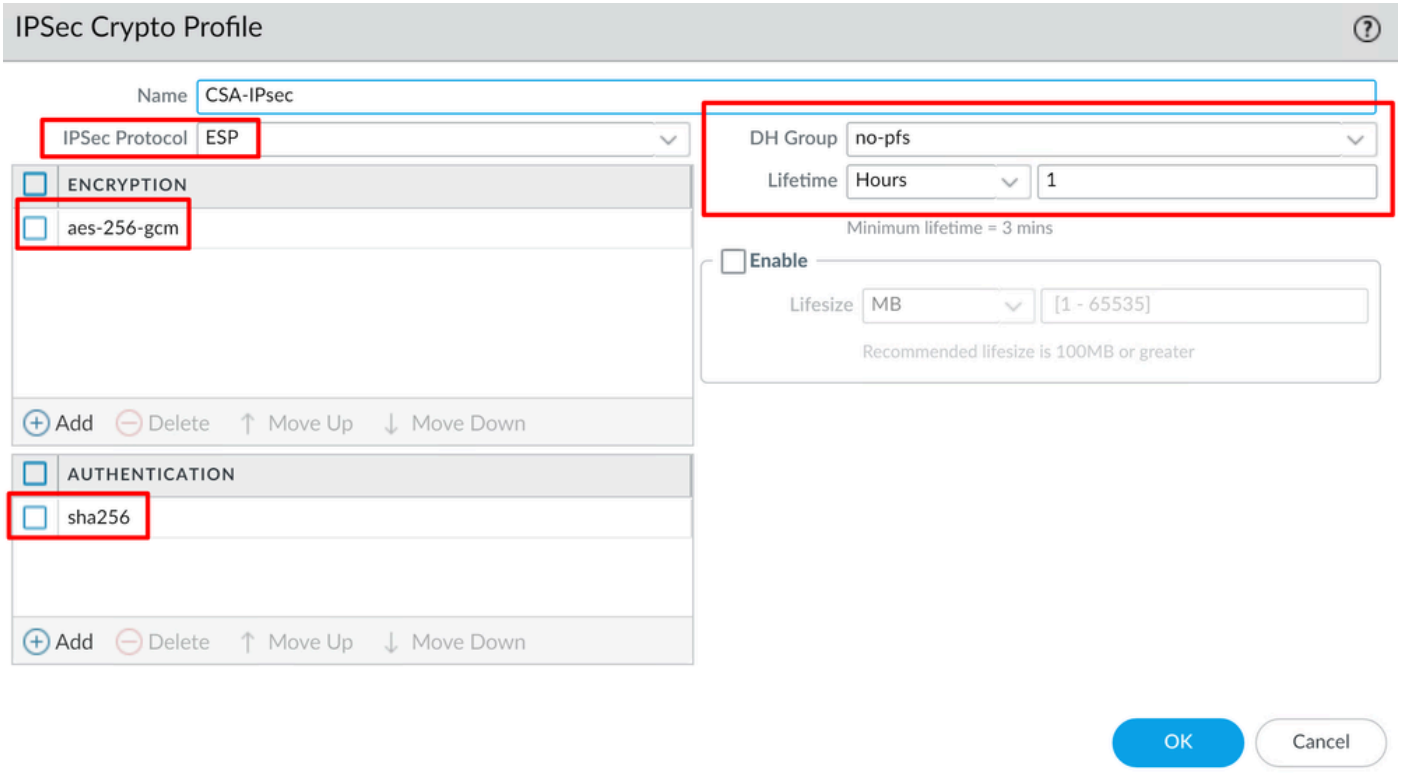
配置IPSEC加密配置檔案

要配置IKE網關，請導航至 Network > Network Profile > IPSEC Crypto

- 按一下Add



- 配置下一個引數：
  - **Name**：使用名稱標識安全訪問IPsec配置檔案
    - IPSec Protocol：ESP
    - **ENCRYPTION**： aes-256-gcm
    - DH Group：無pfs，1小時
- 按一下 OK

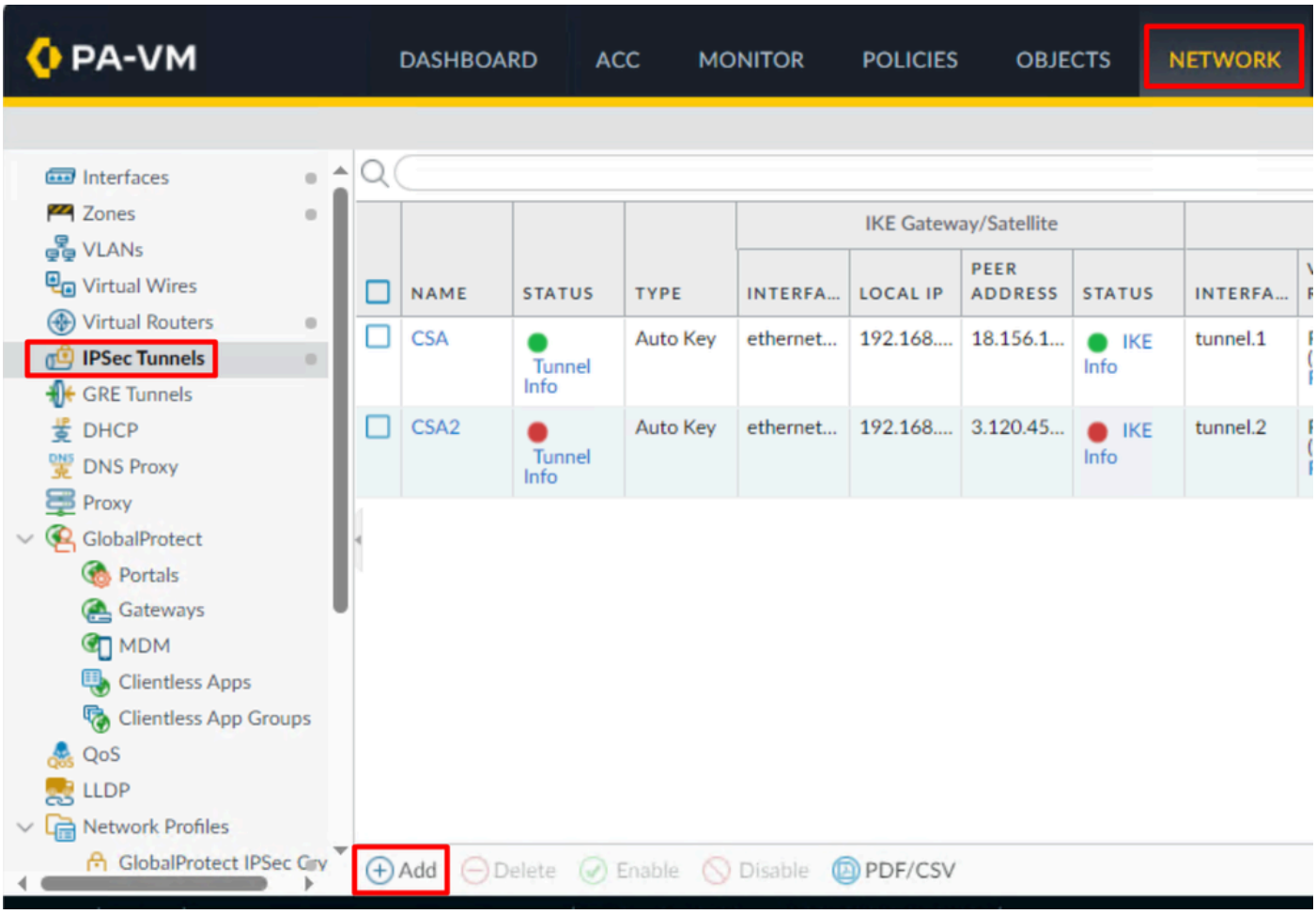


如果已按照如下方式配置該配置，可以點選**Commit** 儲存配置，然後繼續下一步， Configure IPSec Tunnels.

配置IPSec隧道

要配置**IPSec Tunnels**，請導航到Network > IPSec Tunnels。

- 按一下 Add



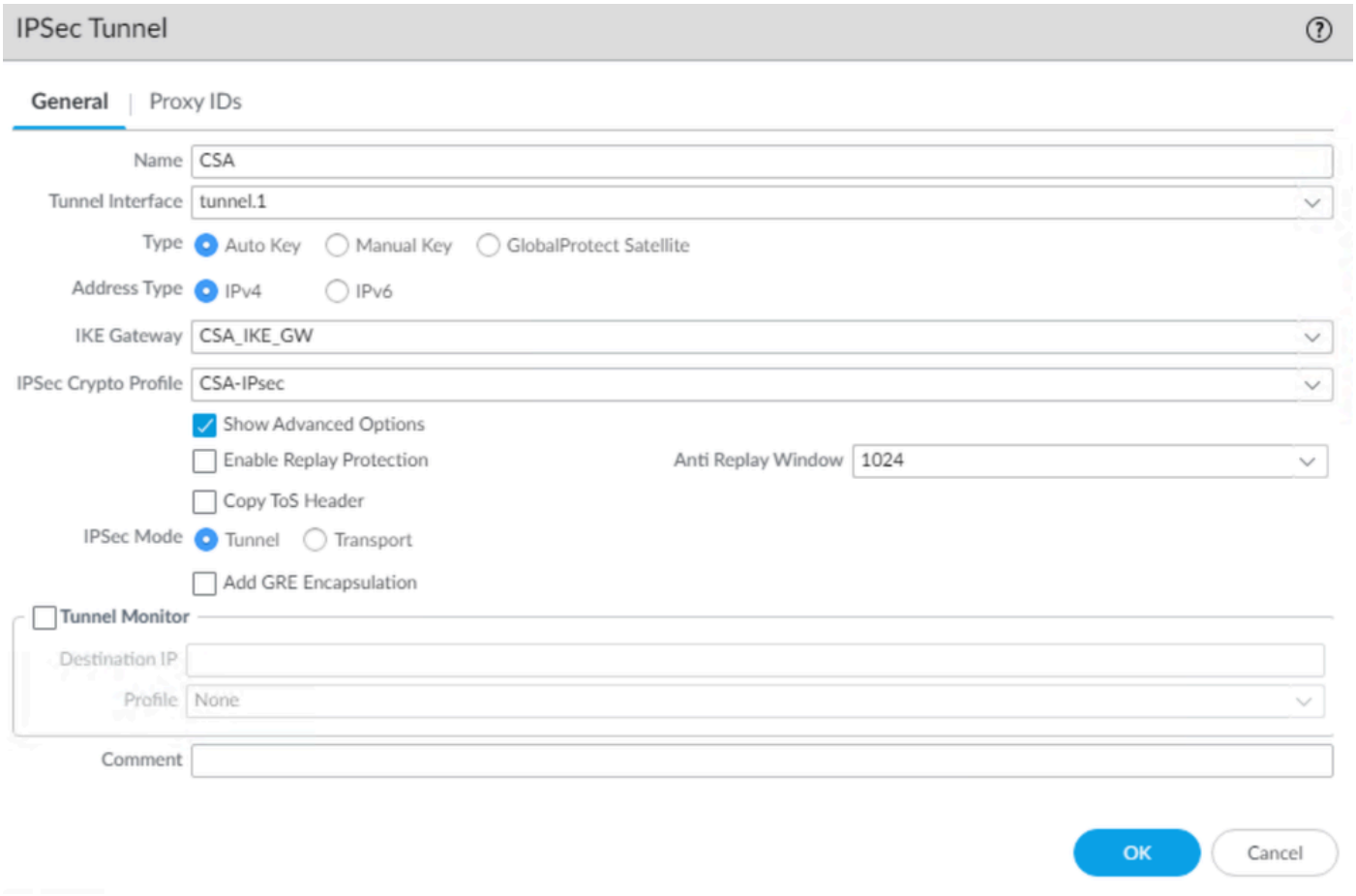
- 配置下一個引數：

  - **Name**：使用名稱標識安全訪問隧道

    - **Tunnel Interface**：選擇在步驟配置隧道介面上配置的隧道介面。
    - **Type**：自動金鑰
    - **Address Type**： IPv4
    - **IKE Gateways**：在配置IKE網關步驟中選擇已配置的IKE網關。
    - **IPsec Crypto Profile**：選擇在步驟配置IPSEC加密配置檔案中配置的IKE網關
    - 標示核取方塊 **Advanced Options**

      - **IPSec Mode Tunnel**：選擇隧道。

- 按一下 OK

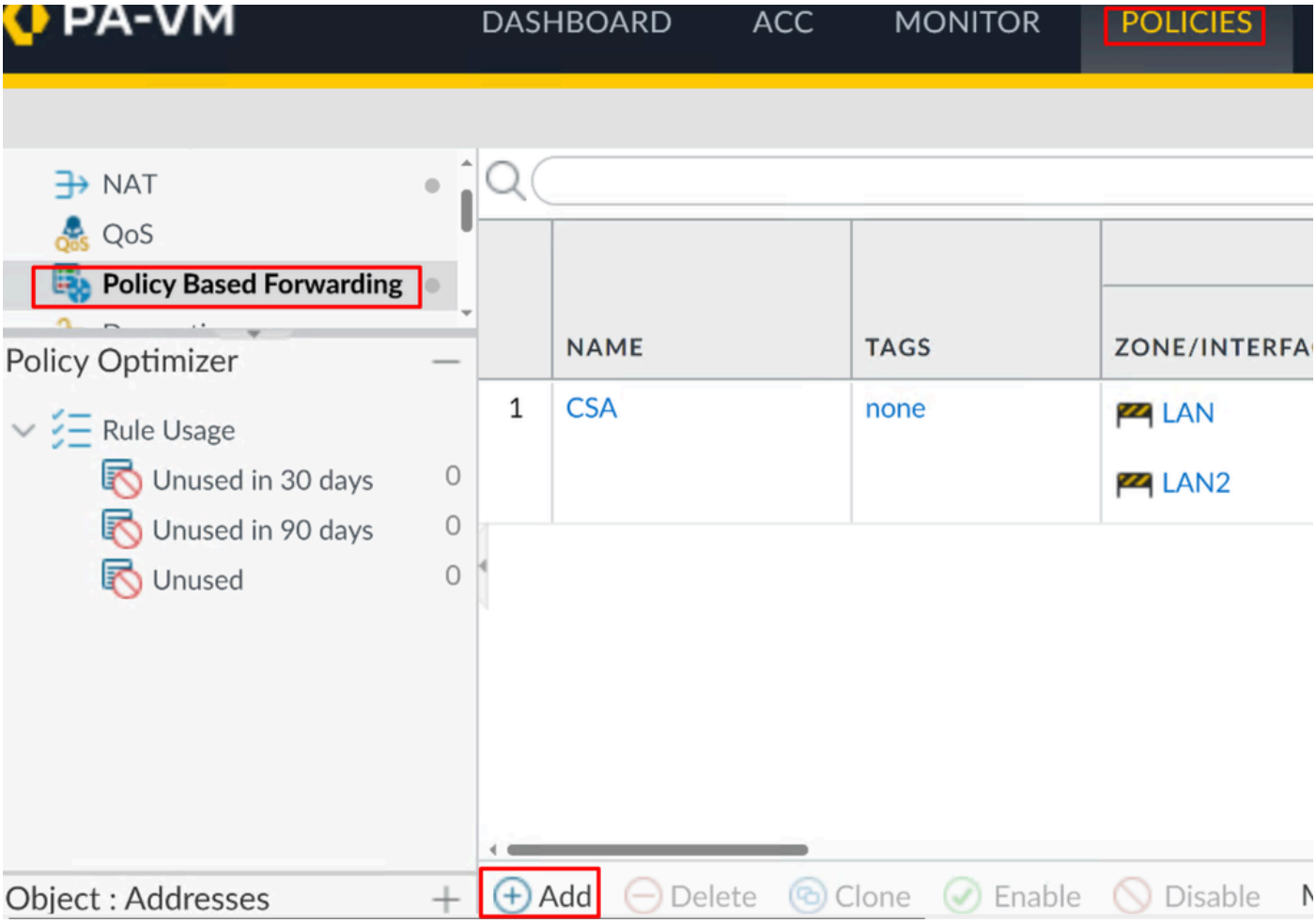


現在已成功建立您的VPN，您可以繼續執行 **Configure Policy Based Forwarding**步驟。

配置基於策略的轉發

要配置 Policy Based Forwarding，**請導航到** Policies > Policy Based Forwarding.

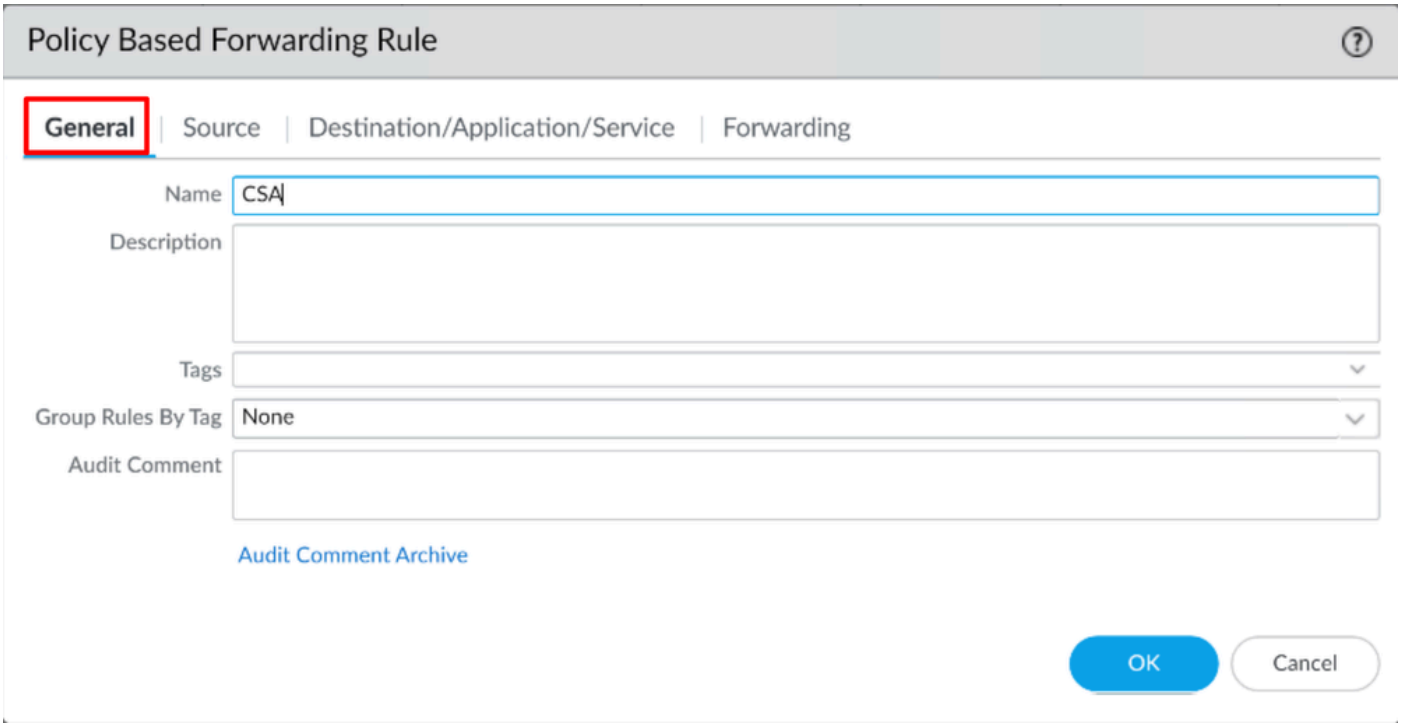
- 按一下 Add

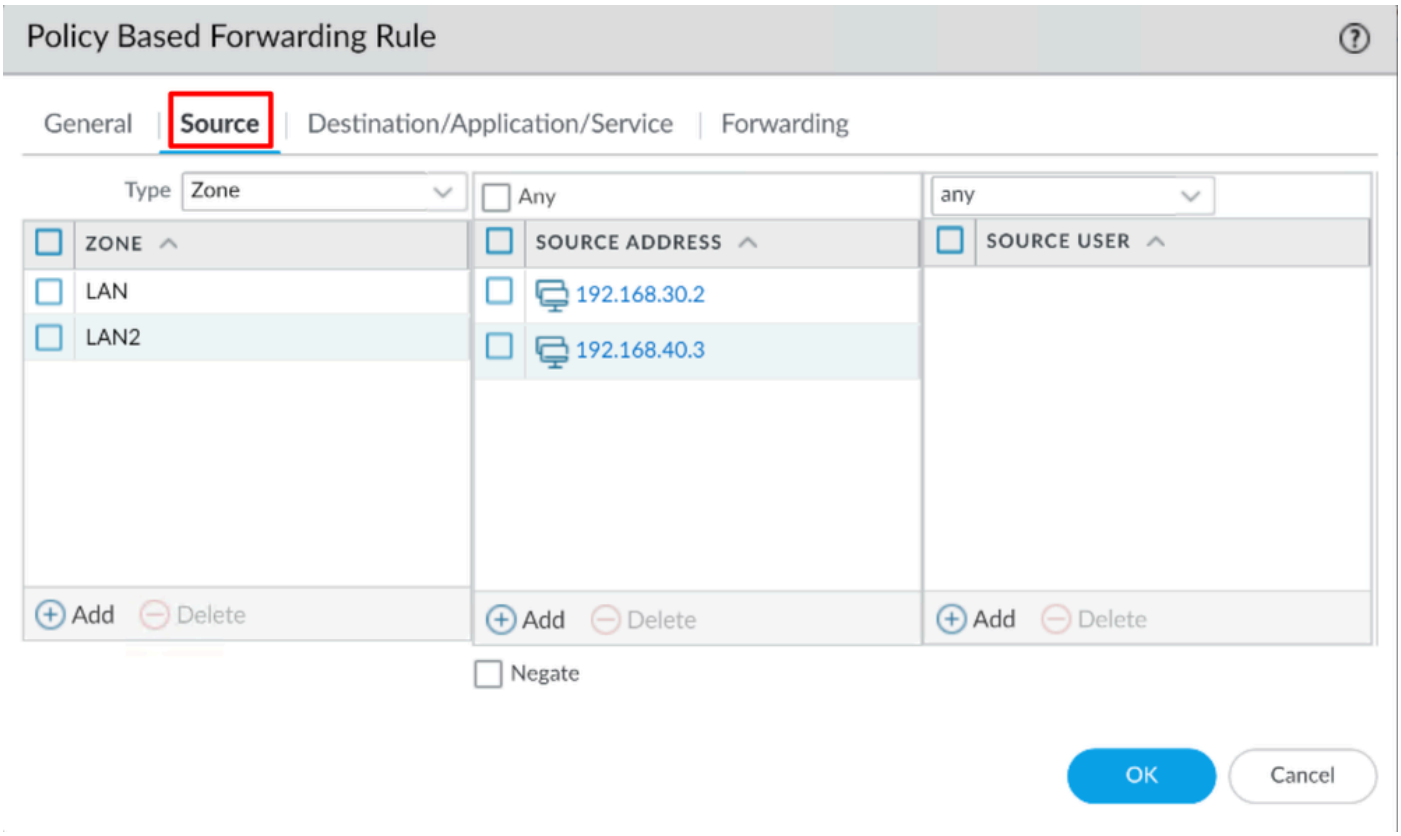


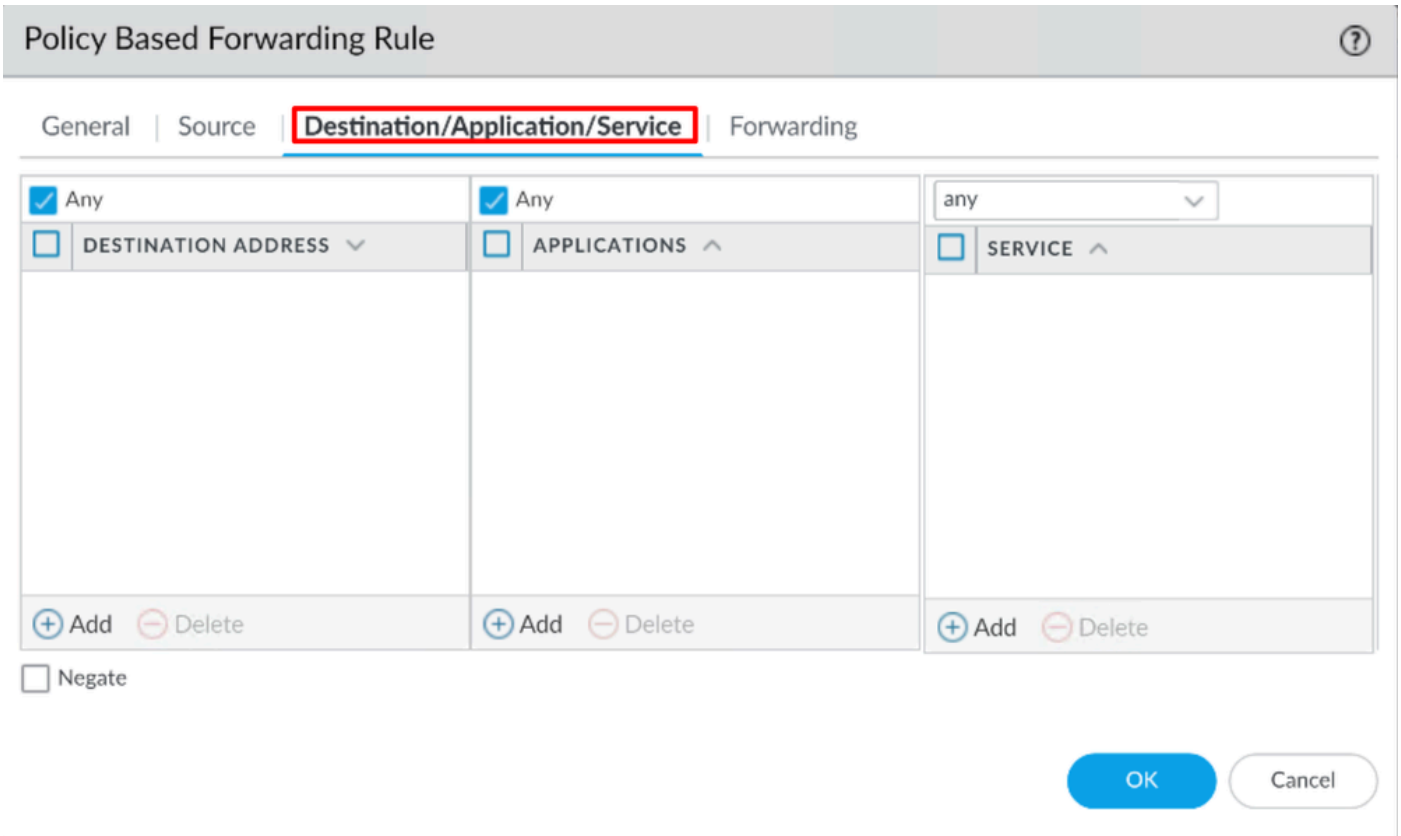
- 配置下一個引數：
  - General
    - **Name**：使用名稱標識安全訪問、策略基礎轉發（按源路由）
- Source
  - **Zone**：選擇您計畫根據源路由流量的區域
    - **Source Address**：配置要用作源的主機或網路。
    - Source Users：配置要路由流量的使用者（僅在適用時）

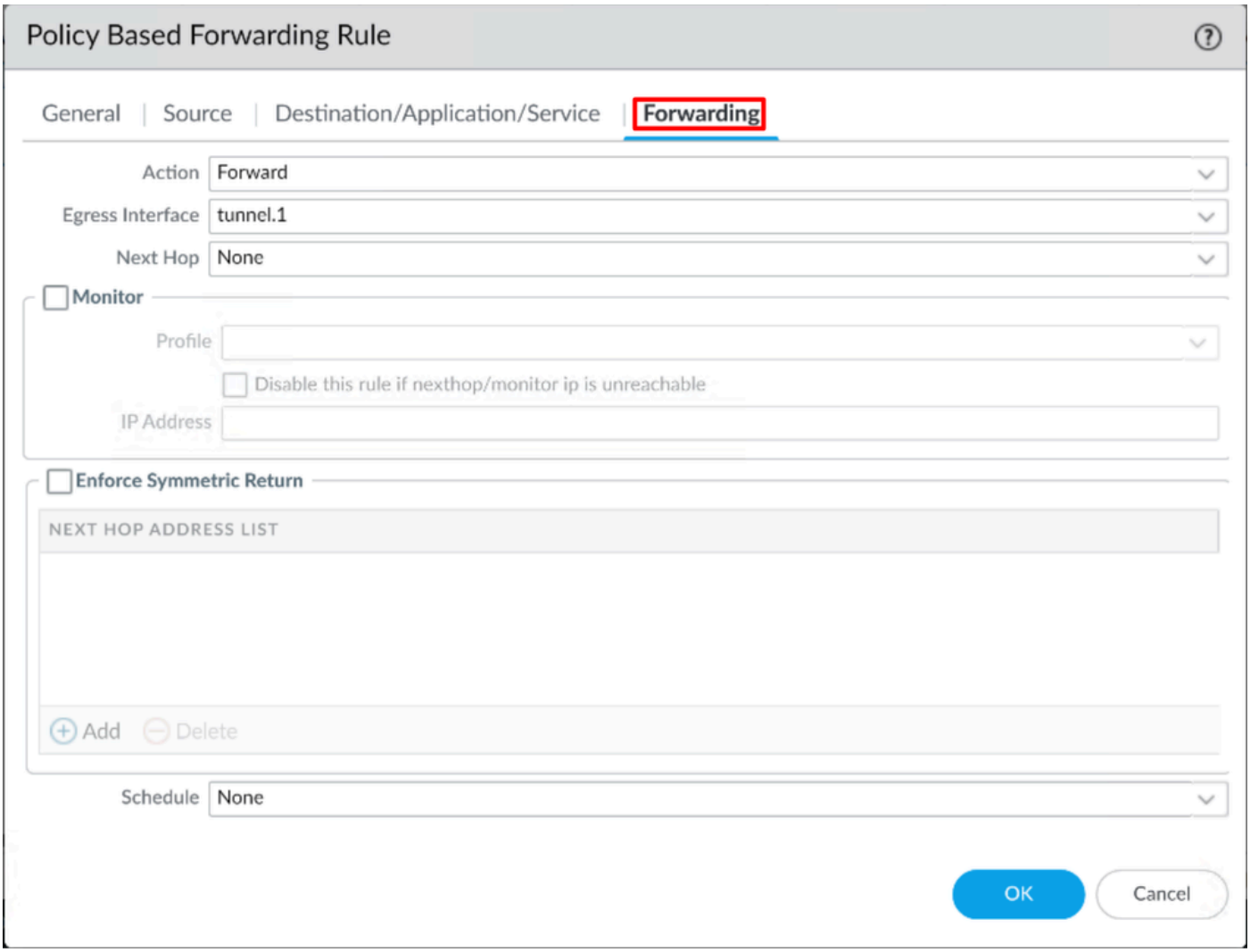
- Destination/Application/Service
  - Destination Address：您可以將其保留為Any，也可以指定安全訪問(100.64.0.0/10)的地址範圍
- Forwarding
  - **Action**：轉發
    - **Egress Interface**：選擇在步驟配置隧道介面上配置的隧道介面。
    - **Next Hop**:無

- 按一下OK，然後 Commit




Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Type
Zone
Any
any
ZONE
SOURCE ADDRESS
SOURCE USER
LAN
LAN2
192.168.30.2
192.168.40.3
Add
Delete
Add
Delete
Add
Delete
Negate
OK
Cancel


Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Any
Any
any
DESTINATION ADDRESS
APPLICATIONS
SERVICE
Add
Delete
Add
Delete
Add
Delete
Negate
OK
Cancel



現在，您已在Palo Alto上配置所有內容；配置路由後，即可建立隧道，您需要繼續在Secure Access Dashboard上配置RA-VPN、基於瀏覽器的ZTA或客戶端基礎ZTA。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。