使用Palo Alto防火墙配置安全访问

目录

简介

本文档介绍如何使用Palo Alto防火墙配置安全访问。

先决条件

- 配置用户调配
- ZTNA SSO身份验证配置
- 配置远程访问VPN安全访问

要求

Cisco 建议您了解以下主题：

- Palo Alto 11.x版本防火墙
- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA
- 无客户端ZTNA

使用的组件

本文档中的信息基于：

- Palo Alto 11.x版本防火墙

- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全访问- Palo Alto

思科设计了安全访问(Secure Access)，用于保护和提供对内部和基于云的私有应用的访问。它还可以保护从网络到Internet的连接。这通过实施多种安全方法和层来实现，所有这些方法都旨在保护通

过云访问信息时所需的信息。

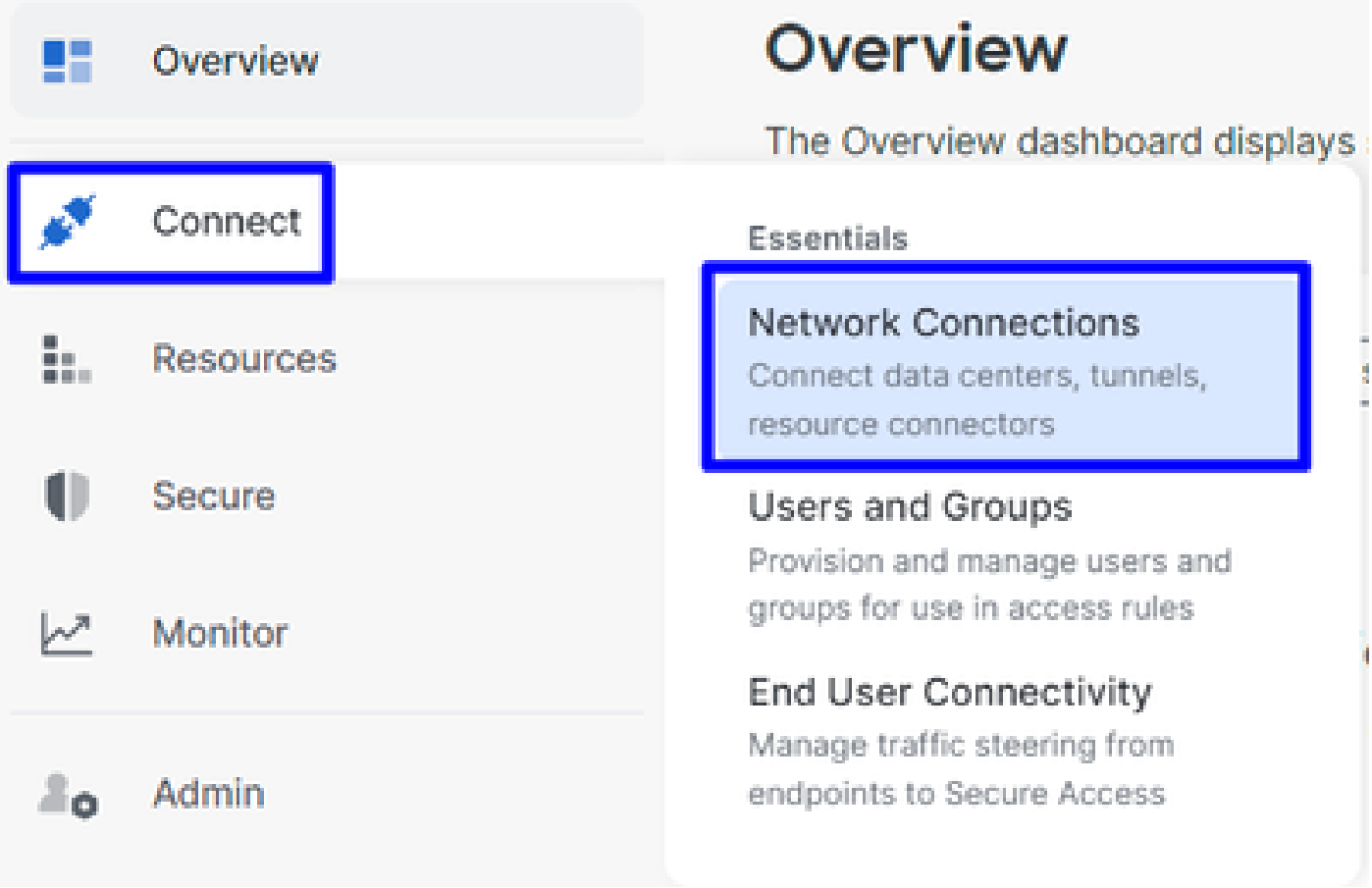
配置

在安全访问中配置VPN

导航到[安全访问]的管理面板。

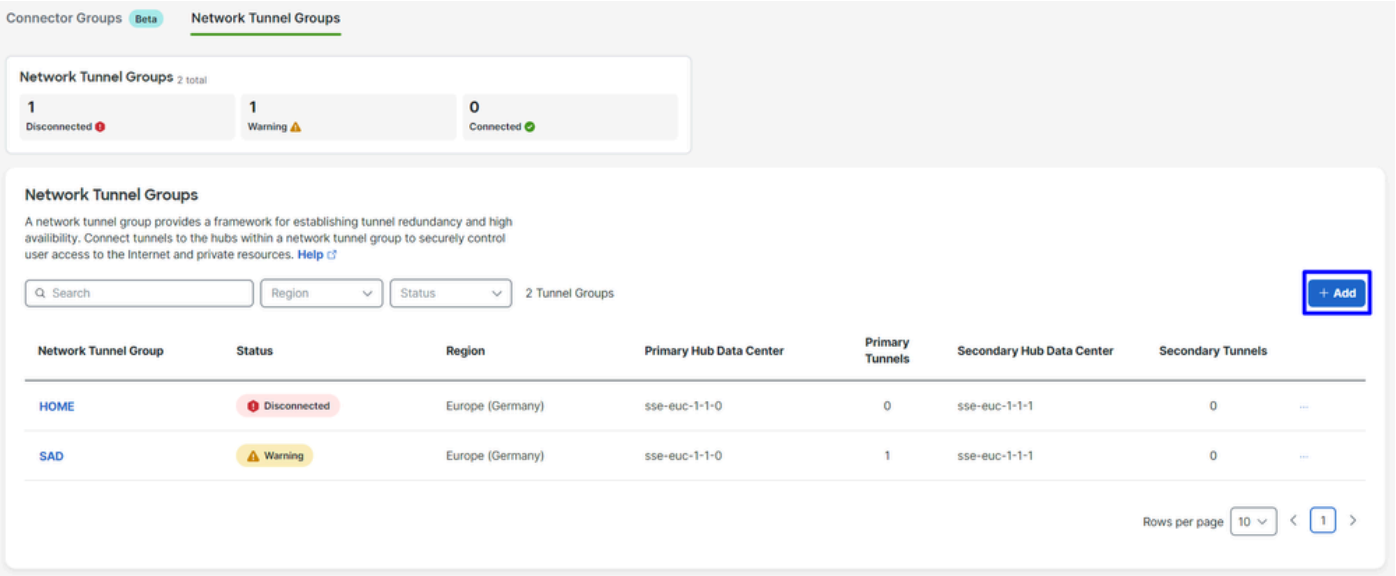
安全访问-主页

- 点击 Connect > Network Connections



安全访问-网络连接

- 在Network Tunnel Groups下单击 + Add



安全访问-网络隧道组

- 配置Tunnel Group Name、Region和 Device Type
- 点击 **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

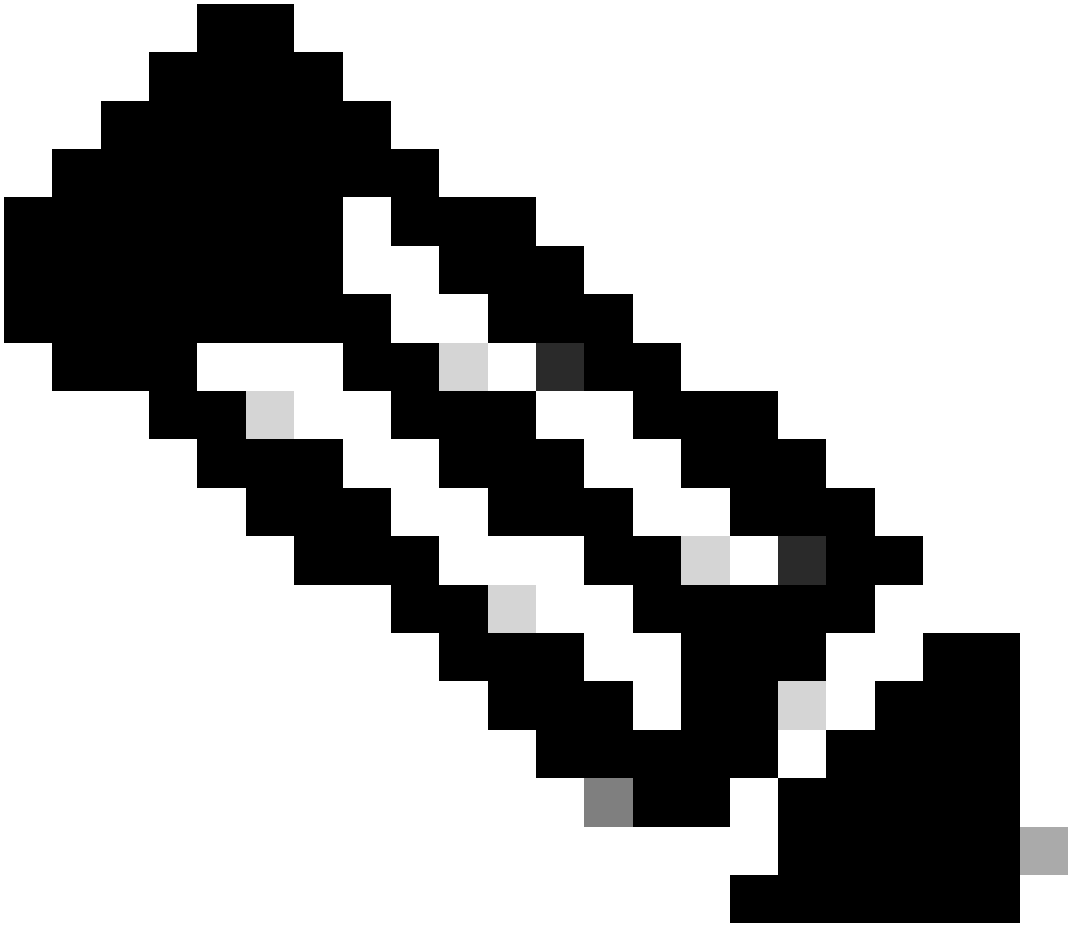
Europe (Germany)

Device Type

Other

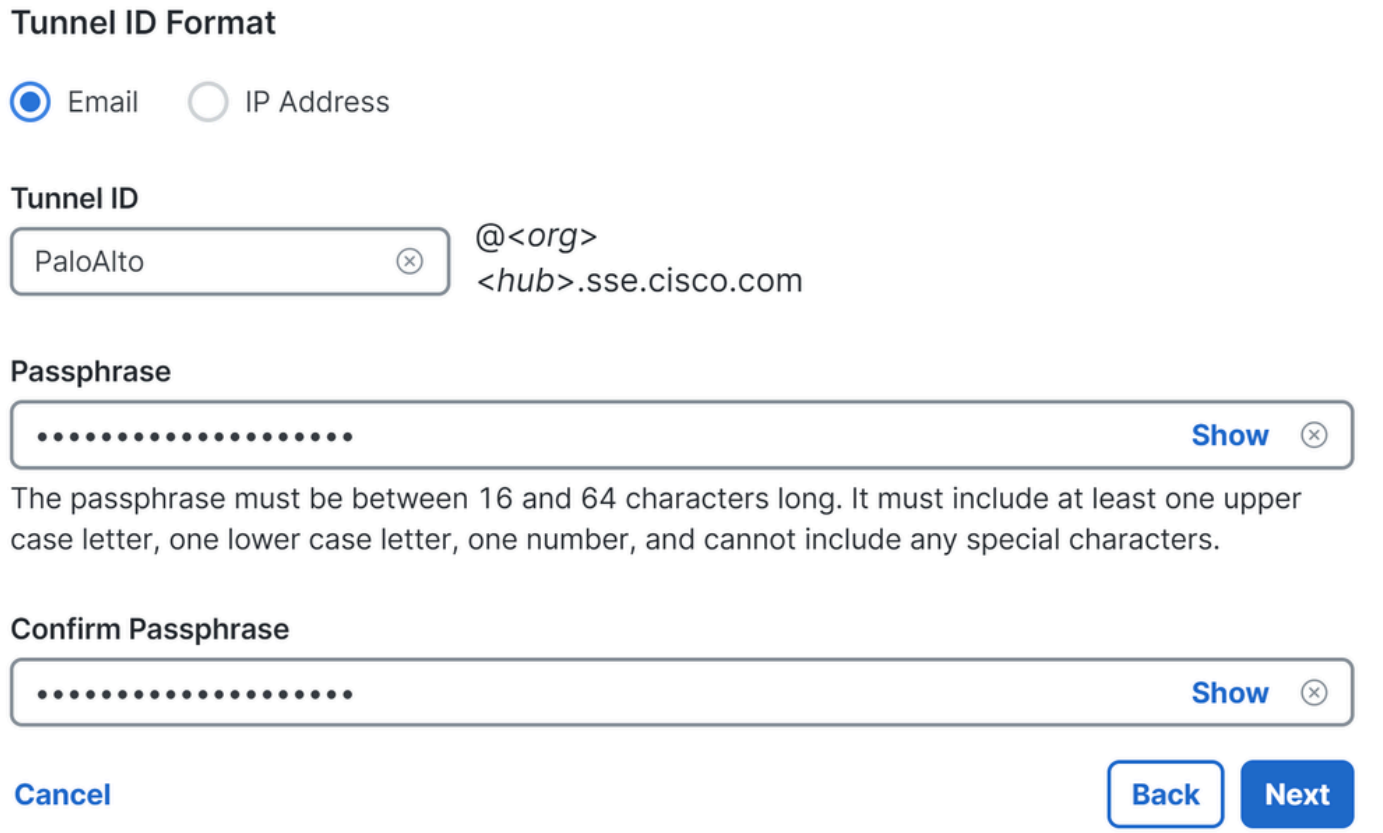
Cancel

Next

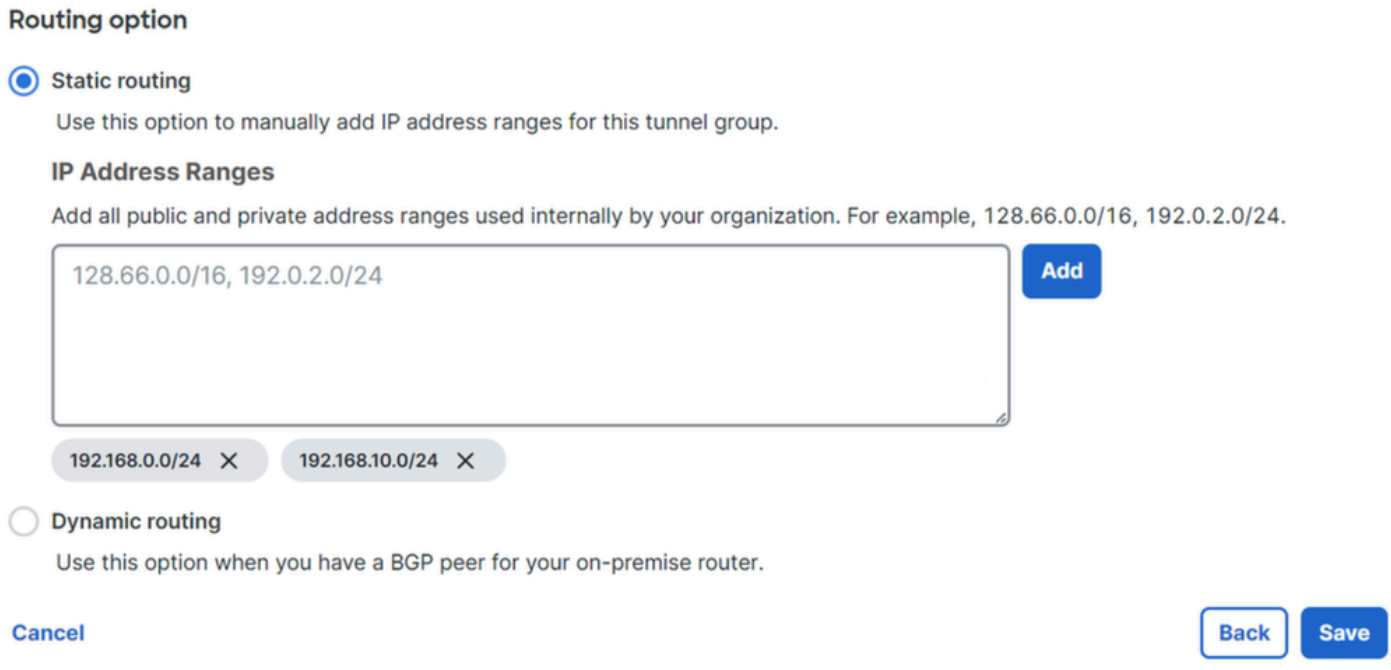


注意：选择距离防火墙位置最近的区域。

- 在路由器上配置Tunnel ID Format Passphrase
- 点击 Next



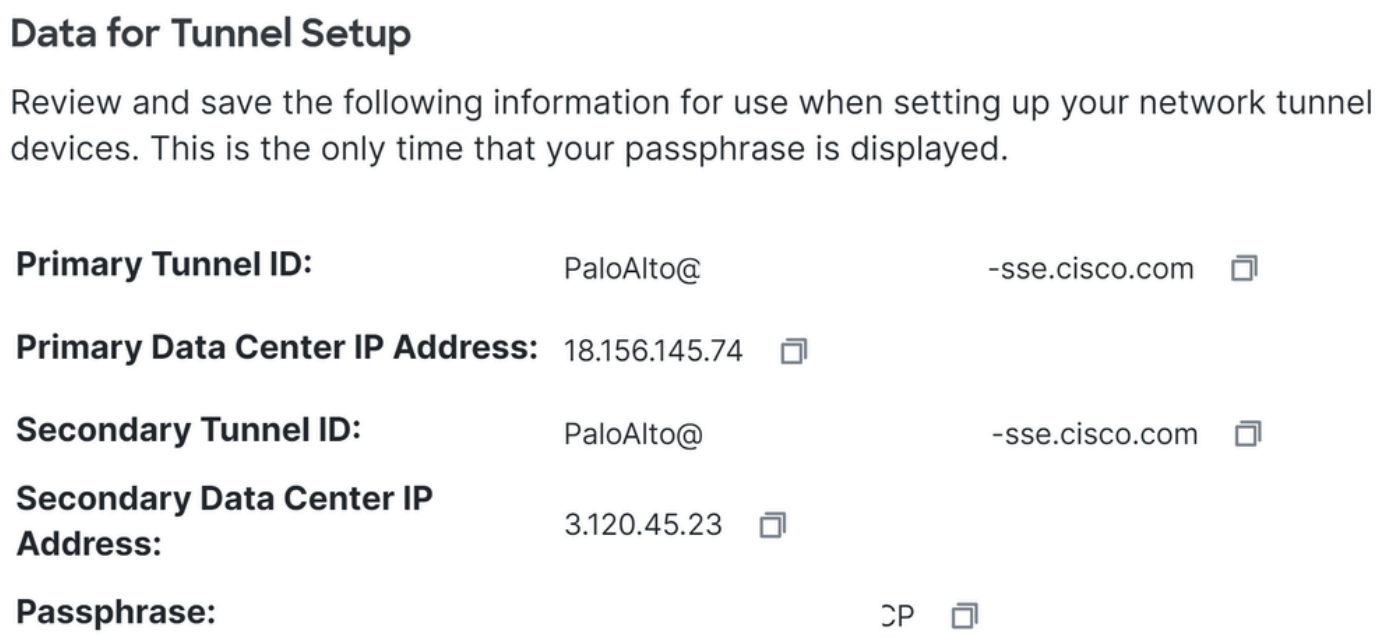
- 配置已在网络上配置并要通过安全访问传递流量的IP地址范围或主机
- 点击 **Save**



安全访问-隧道组-路由选项

单击显示的**Save** 有关隧道的信息后，请保存该信息，以便执行下一步**Configure the tunnel on Palo Alto**。

隧道数据

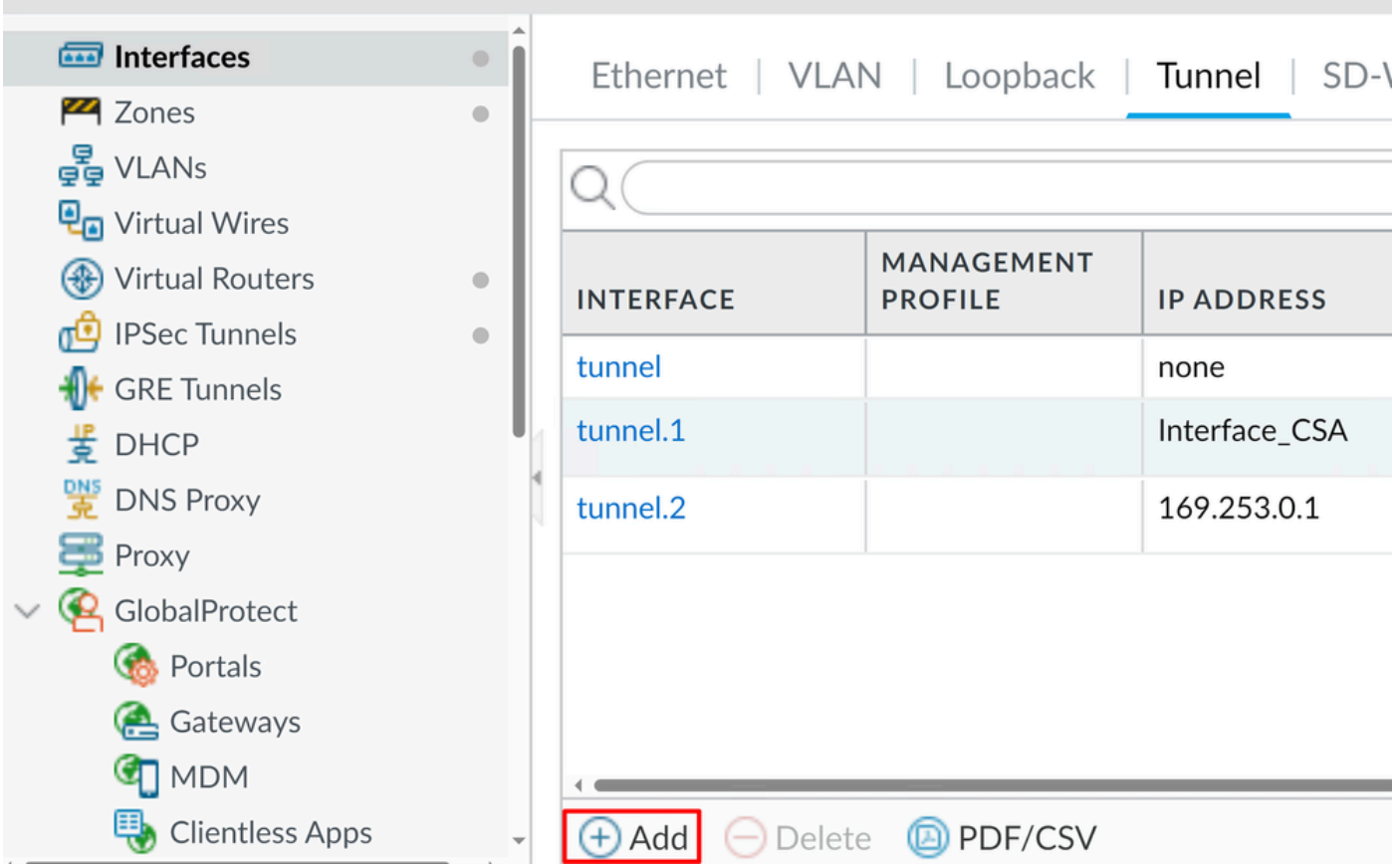


在Palo Alto上配置隧道

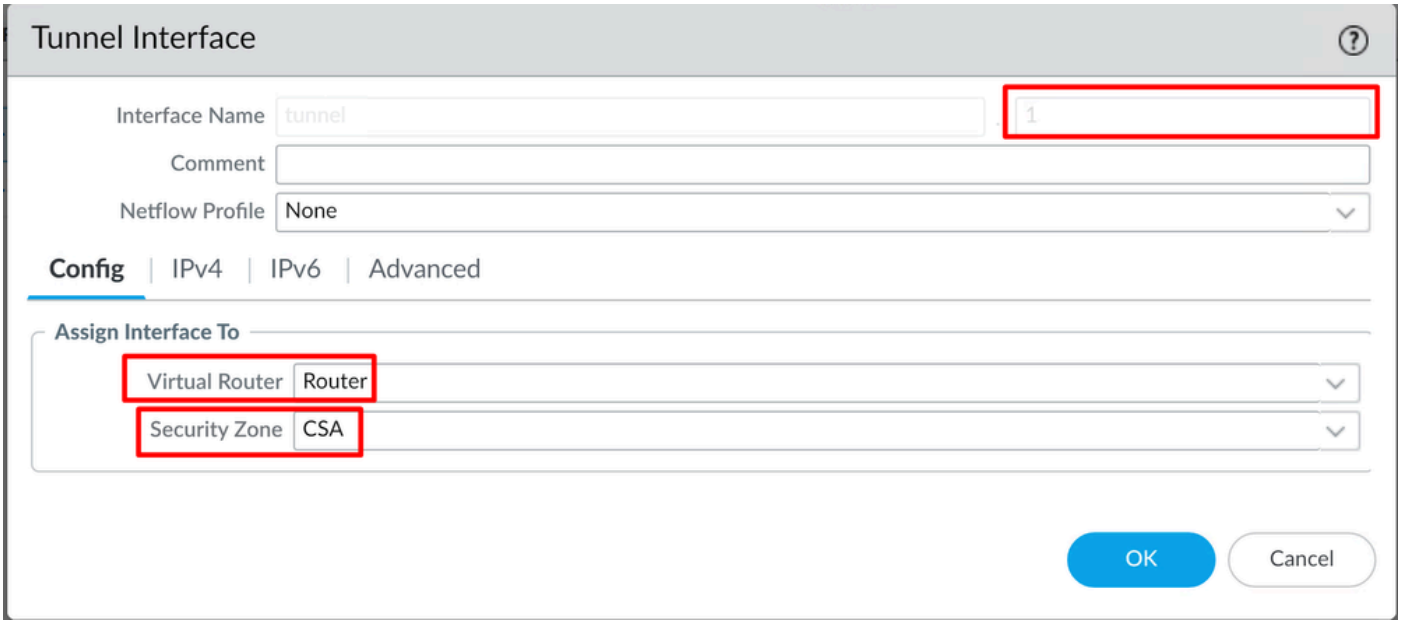
配置隧道接口

导航至Palo Alto Dashboard。

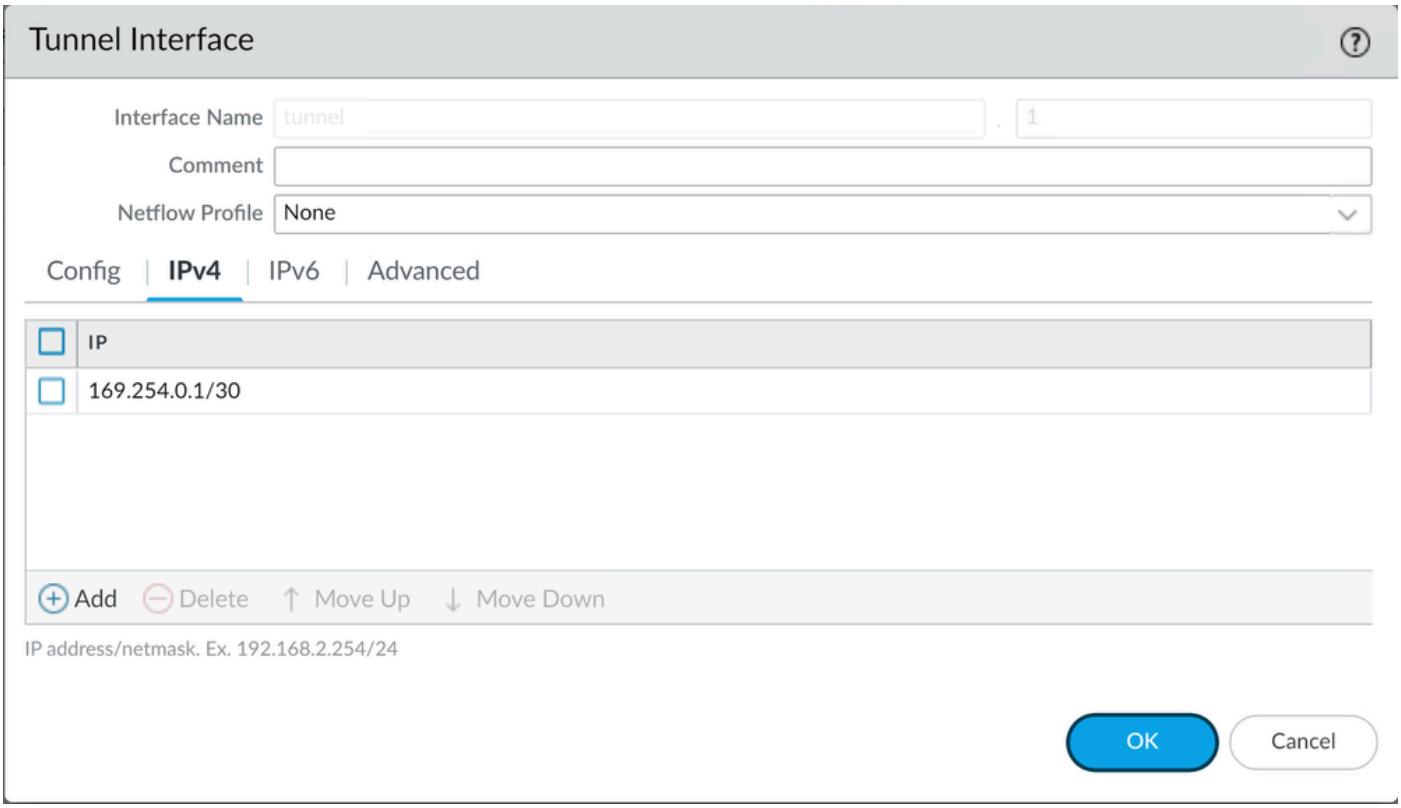
- Network > Interfaces > Tunnel
- Click Add



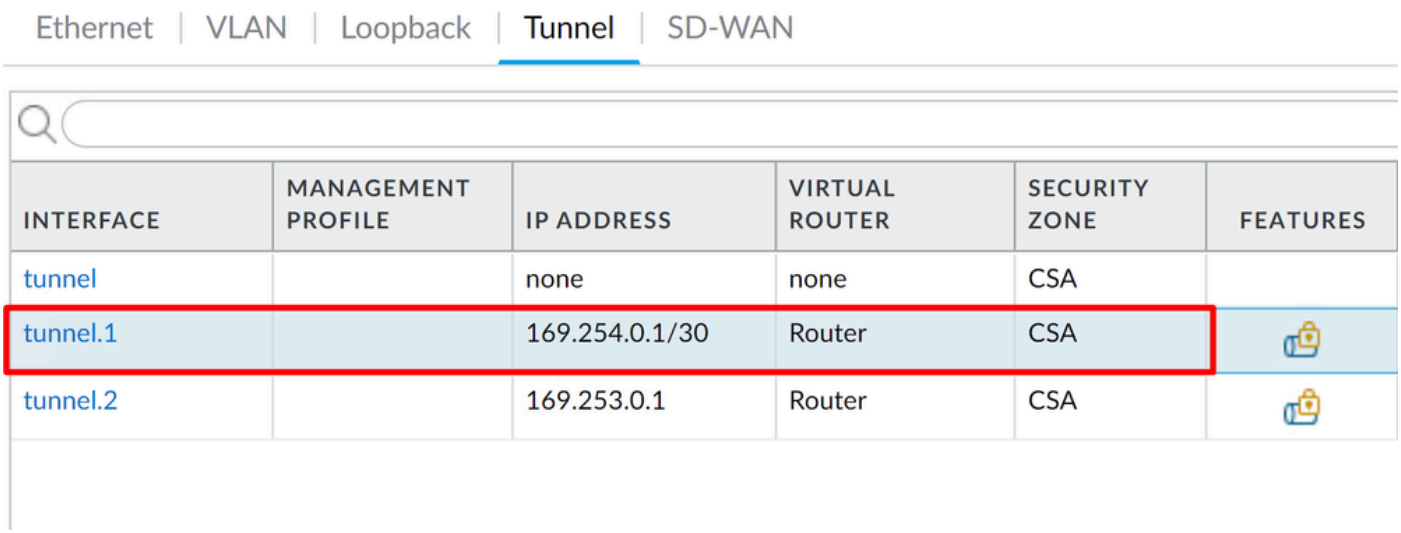
- 在Config菜单下，配置Virtual Router、Security Zone并指定Suffix Number



- 在IPv4下，配置不可路由的IP。例如，您可以使用 169.254.0.1/30
- 点击OK



之后，您可以配置如下内容：

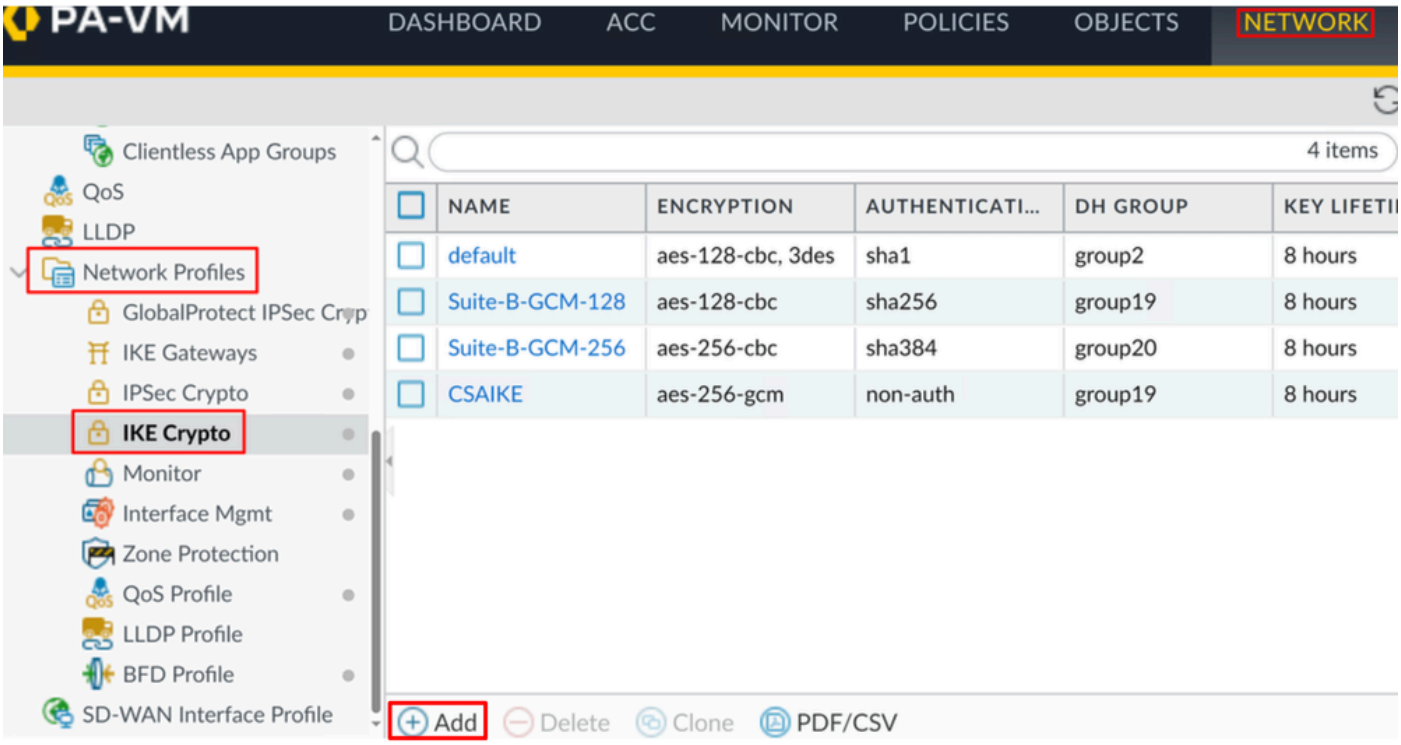


如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续执行下一步Configure IKE Crypto Profile。

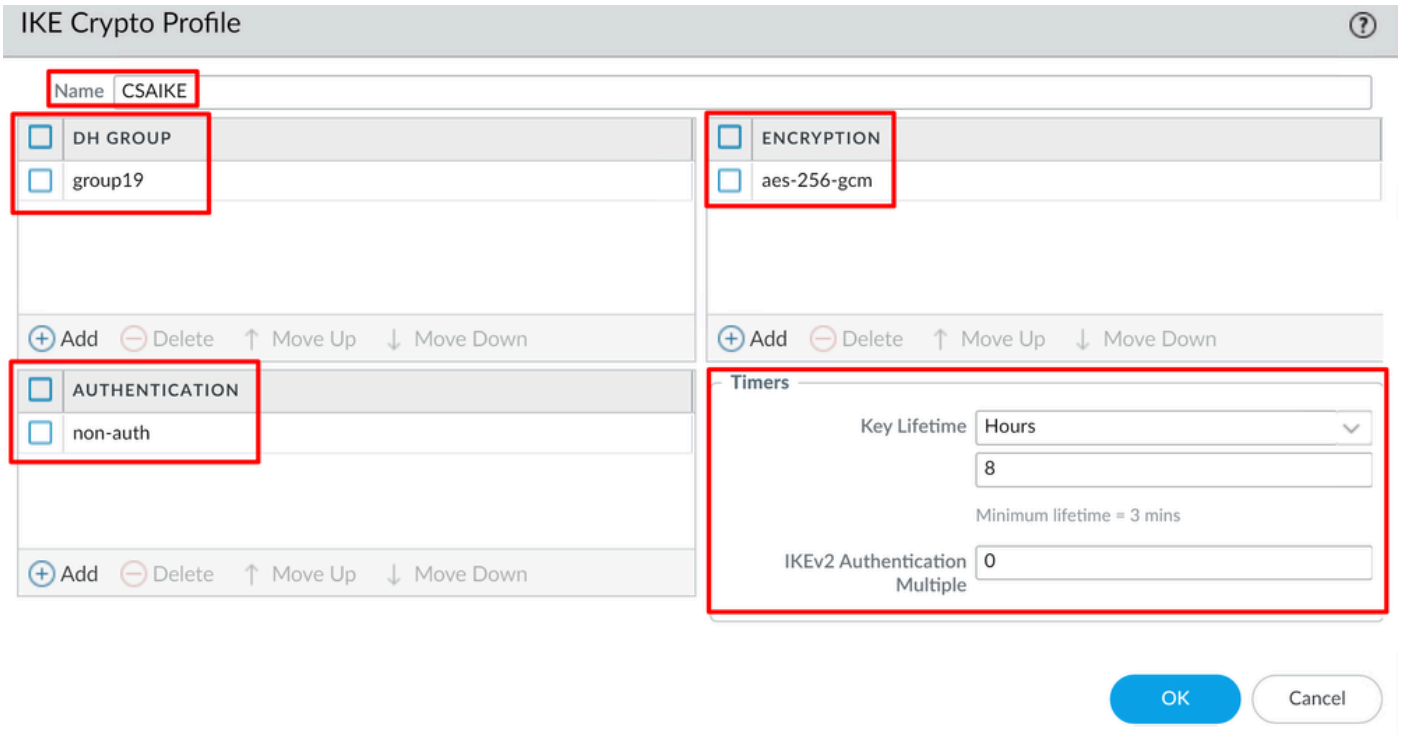
配置IKE加密配置文件

要配置加密配置文件，请导航至：

- Network > Network Profile > IKE Crypto
- 点击Add



- 配置以下参数：
  - **Name**：配置名称以标识配置文件。
    - **DH GROUP**：组19
    - **AUTHENTICATION**：非身份验证
    - **ENCRYPTION**：aes-256-gcm
    - Timers
      - Key Lifetime:8 小时
        - **IKEv2 Authentication**:0
- 完成所有配置后，单击 **OK**

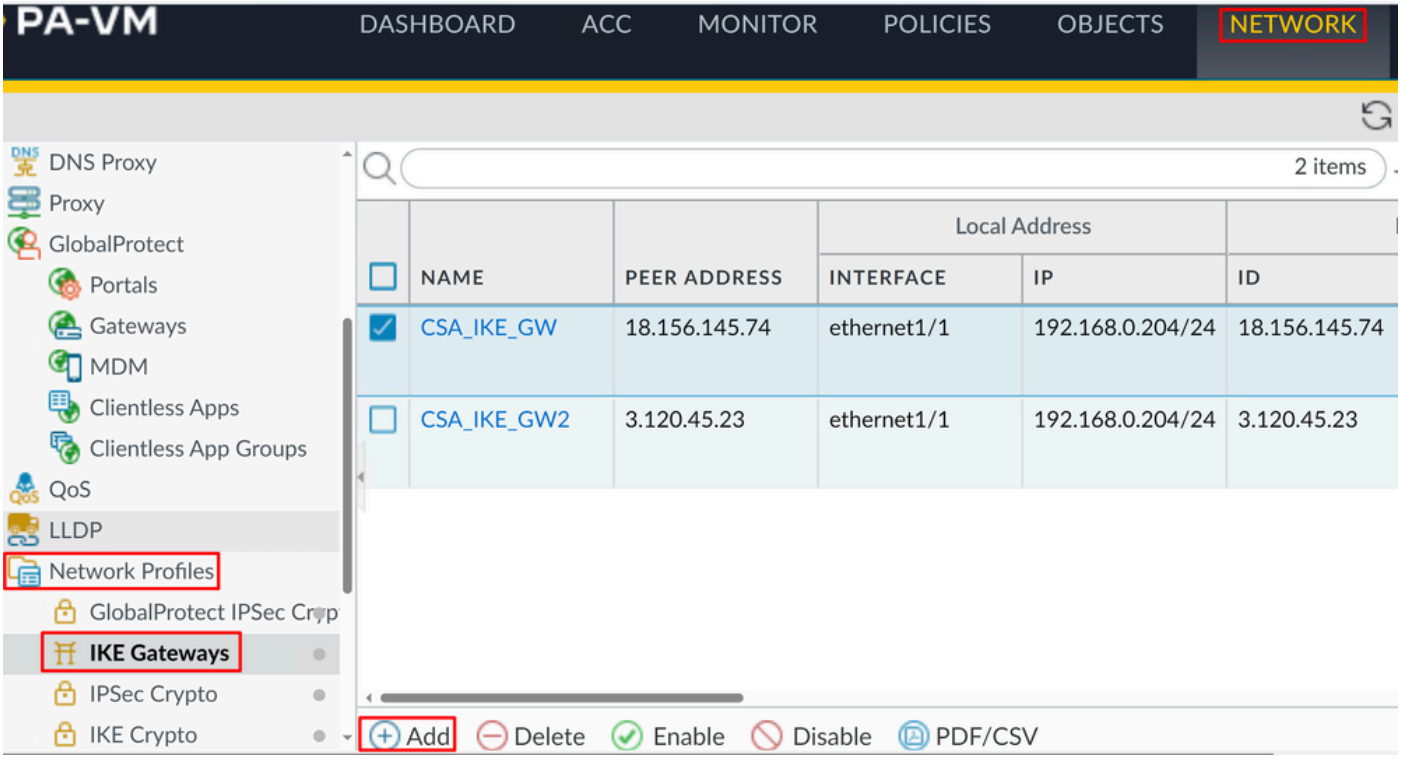


如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续下一步， Configure IKE Gateways.

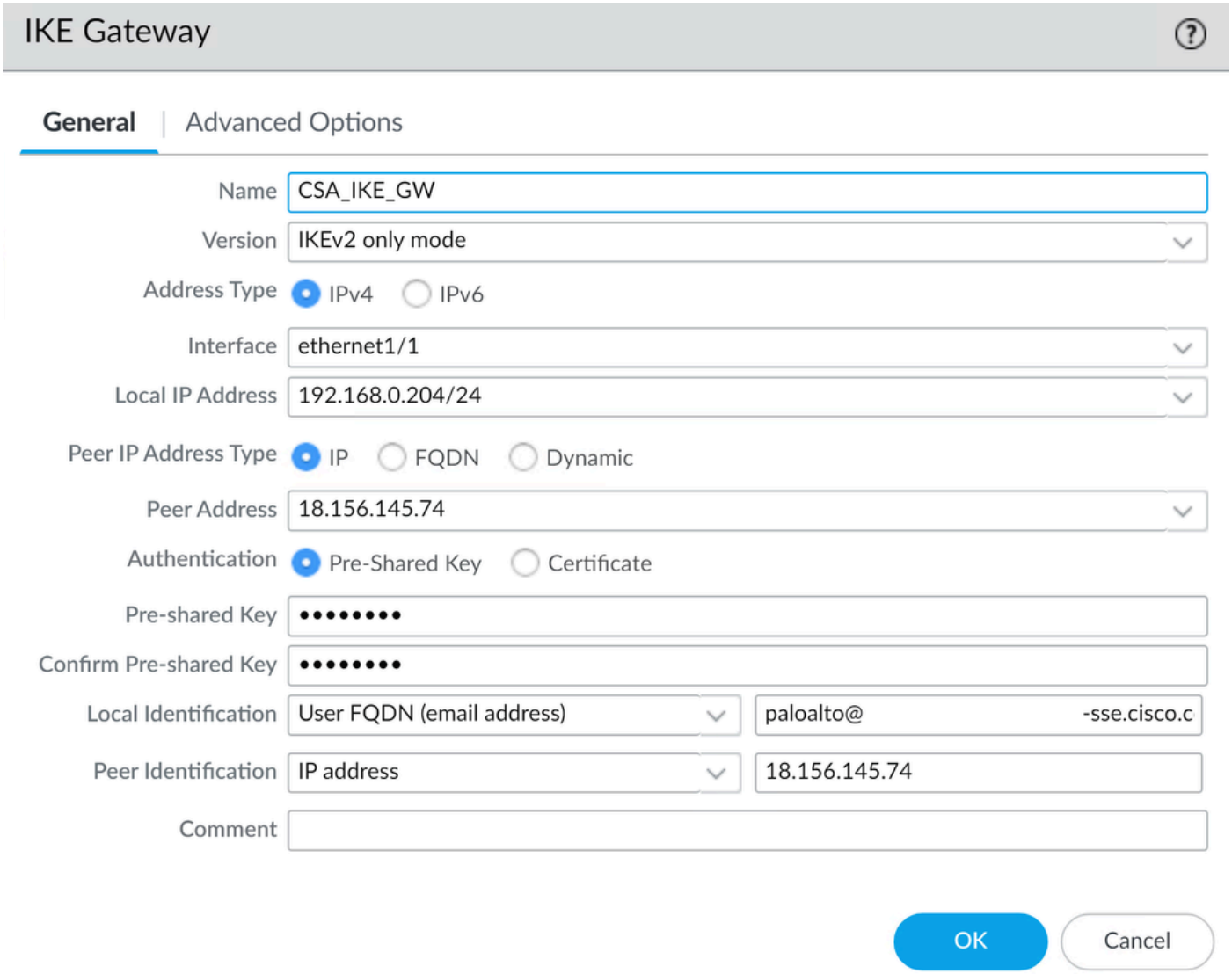
配置IKE网关

配置IKE网关

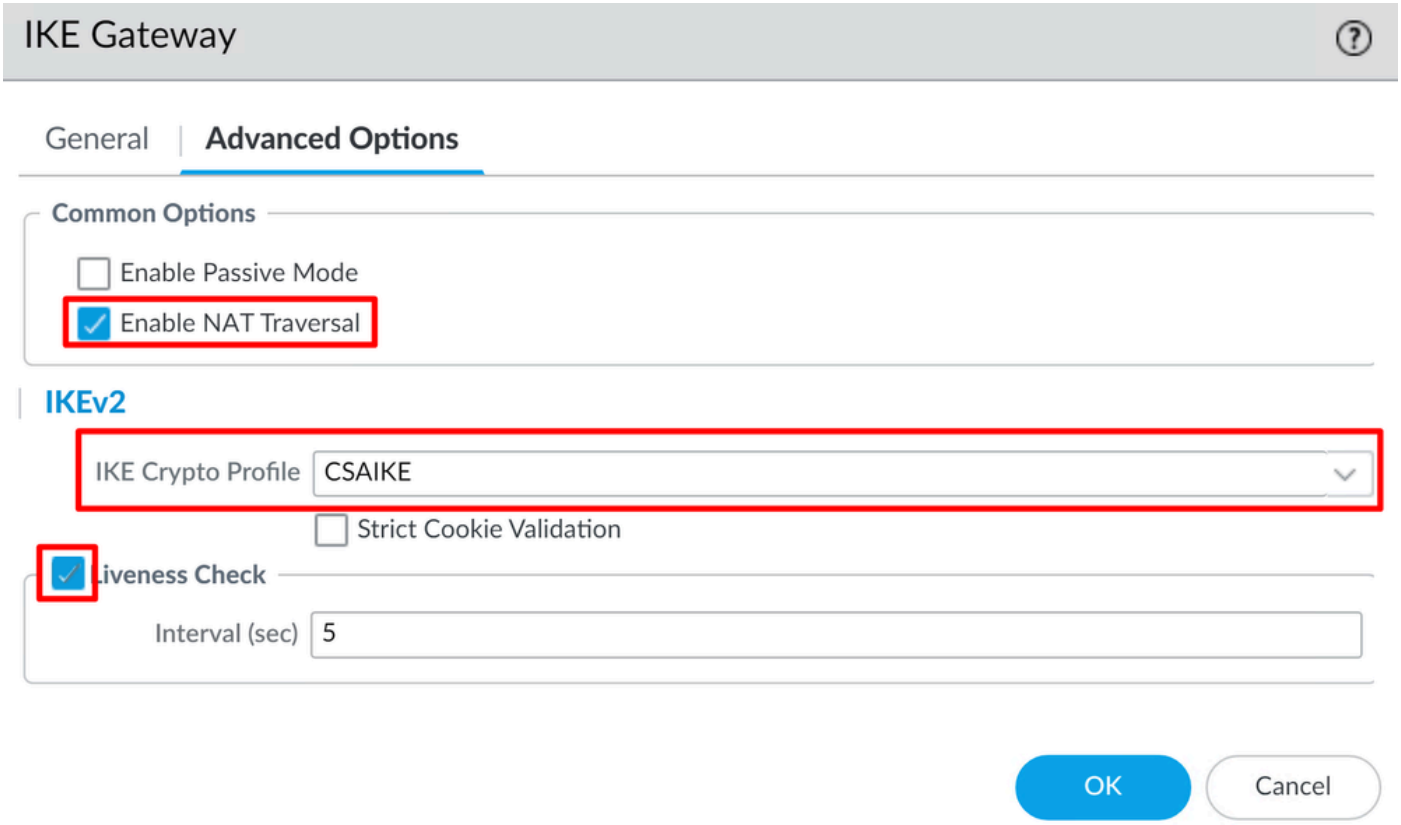
- Network > Network Profile > IKE Gateways
- 点击Add



- 配置以下参数：
    - Name：配置用于标识Ike网关的名称。
        - **Version** ：仅IKEv2模式
        - Address Type ： IPv4
        - **Interface** ：选择您的Internet WAN接口。
        - Local IP Address：选择您的Internet WAN接口的IP。
        - **Peer IP Address Type** :IP
        - Peer Address：使用隧道数据步骤中给定的Primary IP Datacenter IP AddressIP。
        - Authentication:预共享密钥
        - Pre-shared Key ：使用步骤隧道数据中给定 **passphrase** 的。
        - **Confirm Pre-shared Key** ：使用步骤隧道数据中给定 **passphrase** 的。
        - **Local Identification** ：选择**User FQDN (Email address)** 并使用步骤Tunnel Data中给定**Primary Tunnel ID** 的参数。
        - **Peer Identification** ：选IP Address择并使用Primary IP Datacenter IP Address。



- 点击Advanced Options
  - **Enable NAT Traversal**
    - 选择在步骤Configure IKE Crypto Profile上创**IKE Crypto Profile** 建的
    - 选中复选框 **Liveness Check**
    - 点击 **OK**

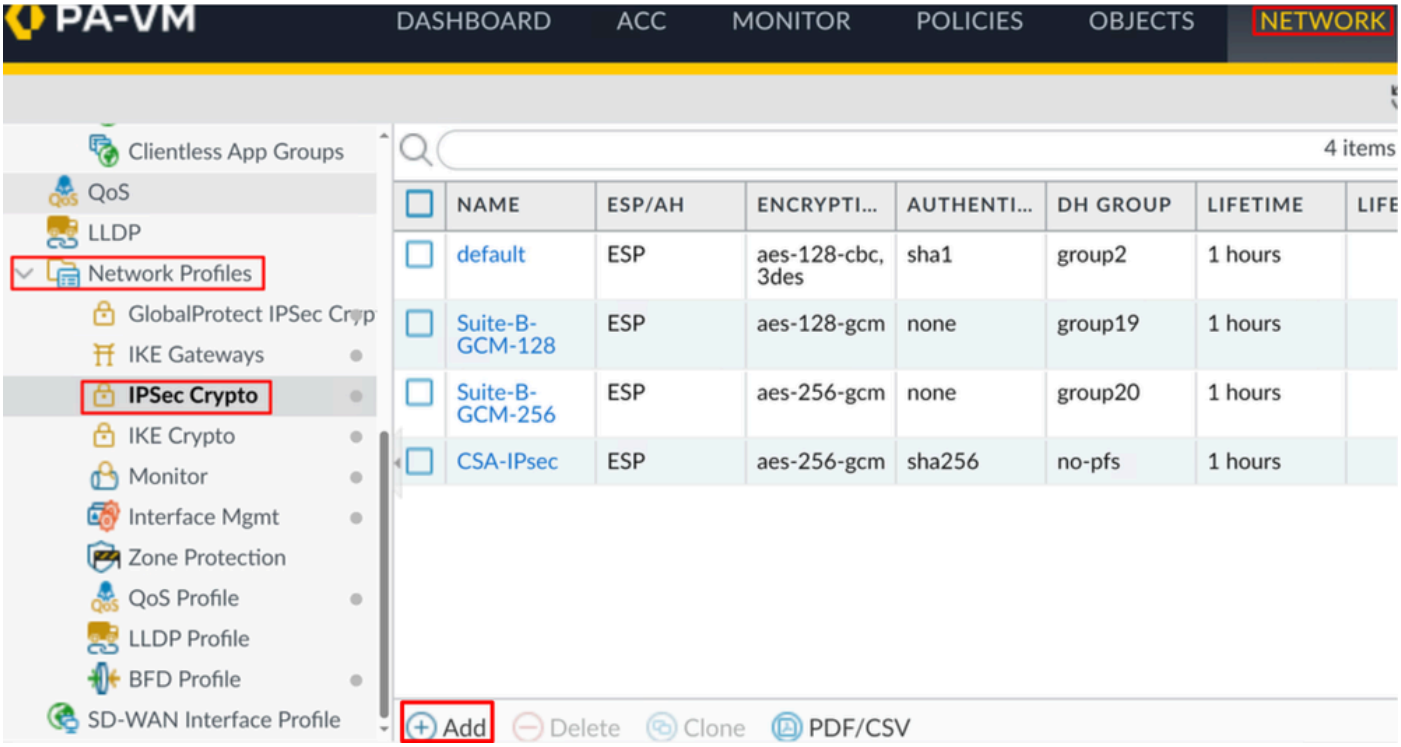


如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续下一步， Configure IPSEC Crypto.

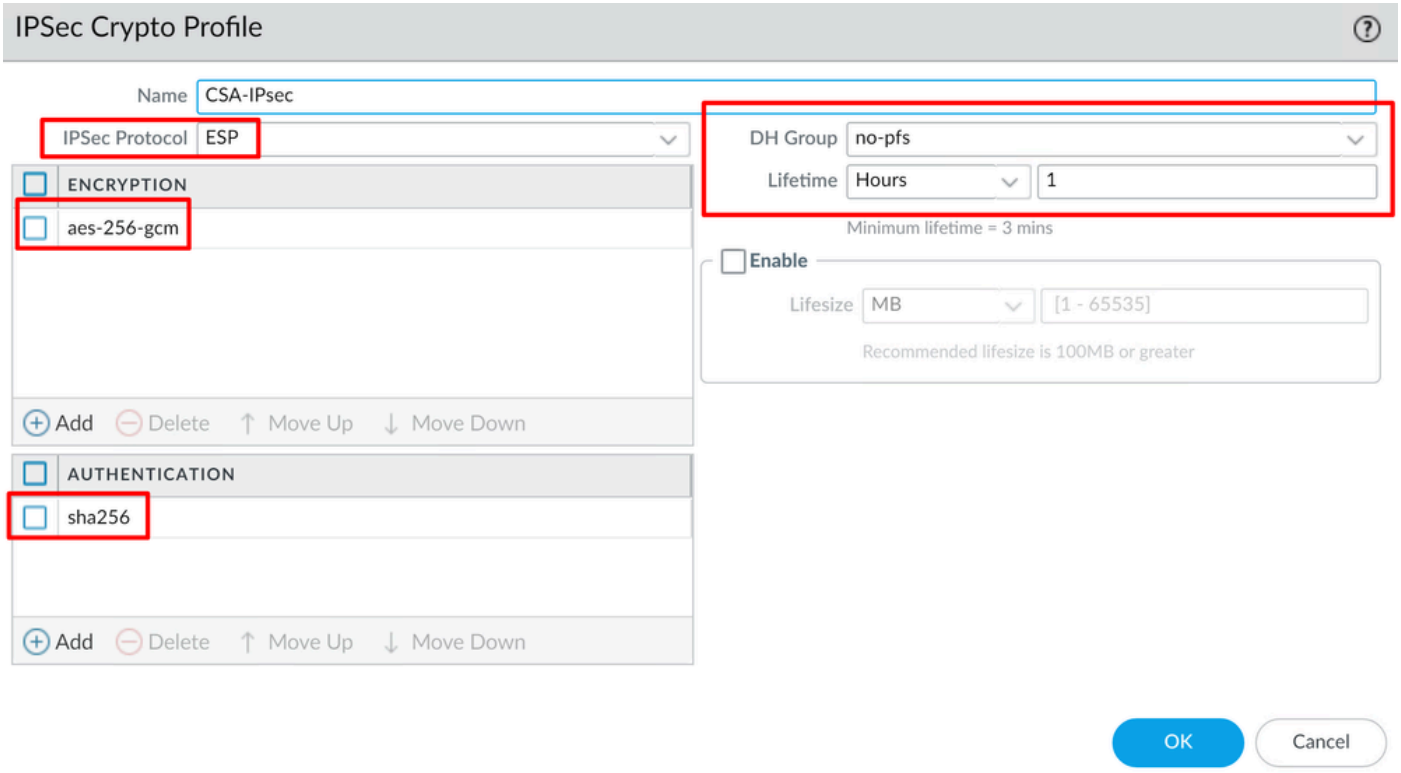
配置IPSEC加密配置文件

要配置IKE网关，请导航至 Network > Network Profile > IPSEC Crypto

- 点击Add



- 配置以下参数：
  - **Name**：使用名称标识安全访问IPsec配置文件
    - IPSec Protocol：ESP
    - **ENCRYPTION**：aes-256-gcm
    - DH Group：无pfs，1小时
- 点击 OK

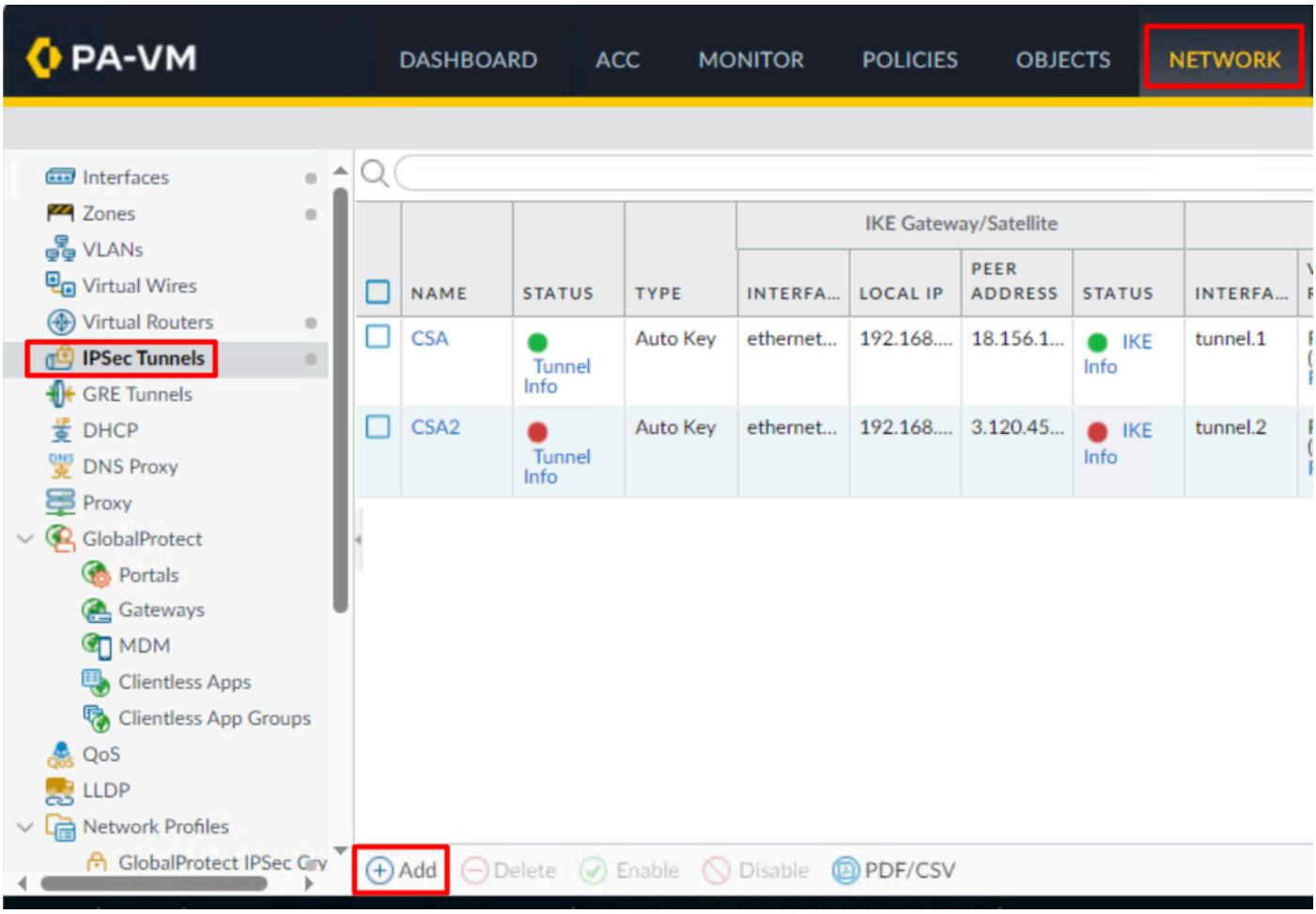


如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续下一步， Configure IPSec Tunnels.

配置IPSec隧道

要配置**IPSec Tunnels**，请导航到Network > IPSec Tunnels。

- 点击 Add



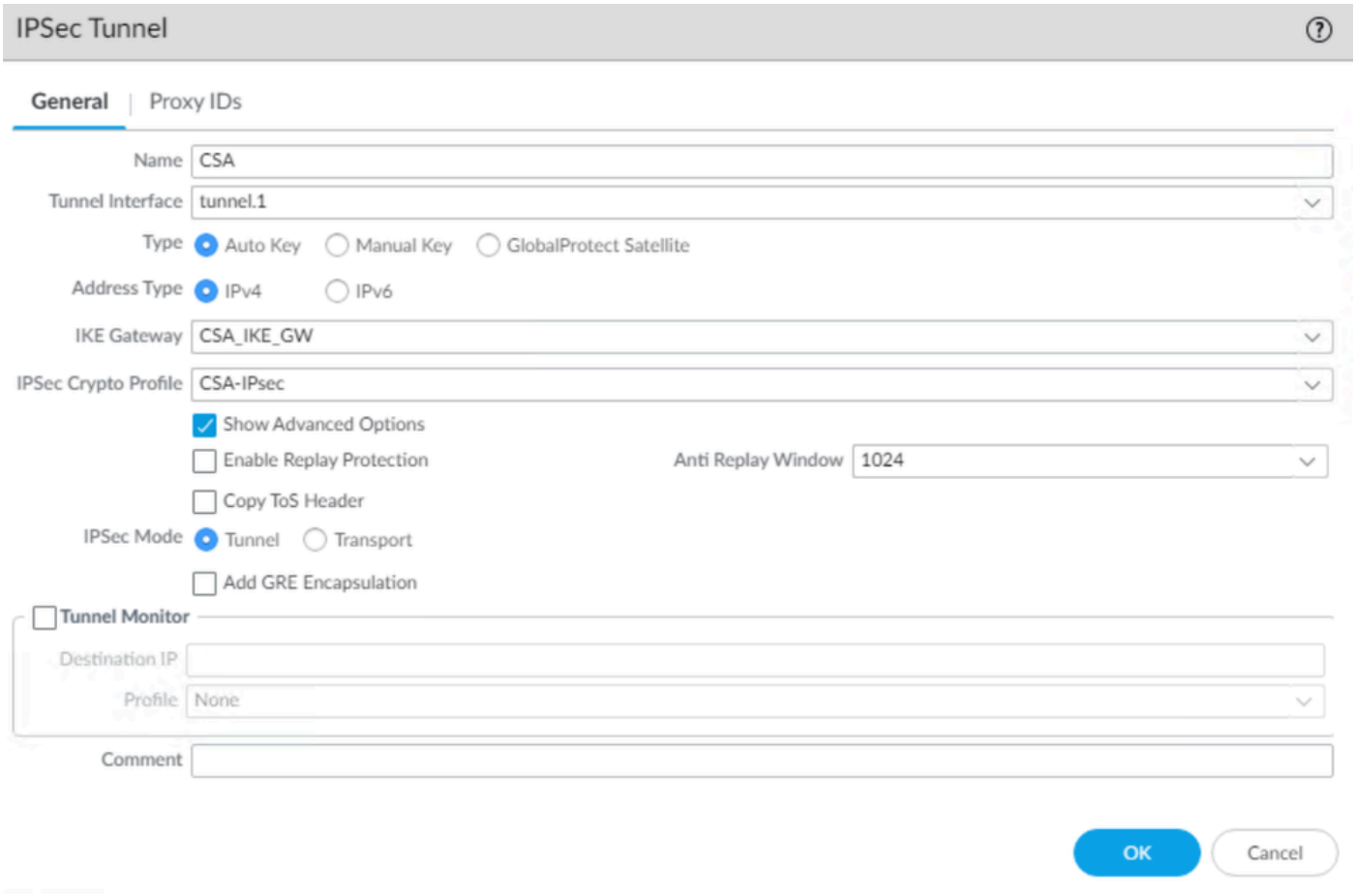
- 配置以下参数：

  - **Name**：使用名称标识安全访问隧道

    - **Tunnel Interface**：选择在配置隧道接口这一步中配置的隧道接口。
    - **Type**：自动密钥
    - **Address Type**： IPv4
    - **IKE Gateways**：选择在Configure IKE Gateways步骤中配置的IKE网关。
    - **IPsec Crypto Profile**：选择在配置IPSEC加密配置文件步骤中配置的IKE网关
    - 选中复选框 **Advanced Options**

      - **IPSec Mode Tunnel**：选择隧道。

- 点击 OK

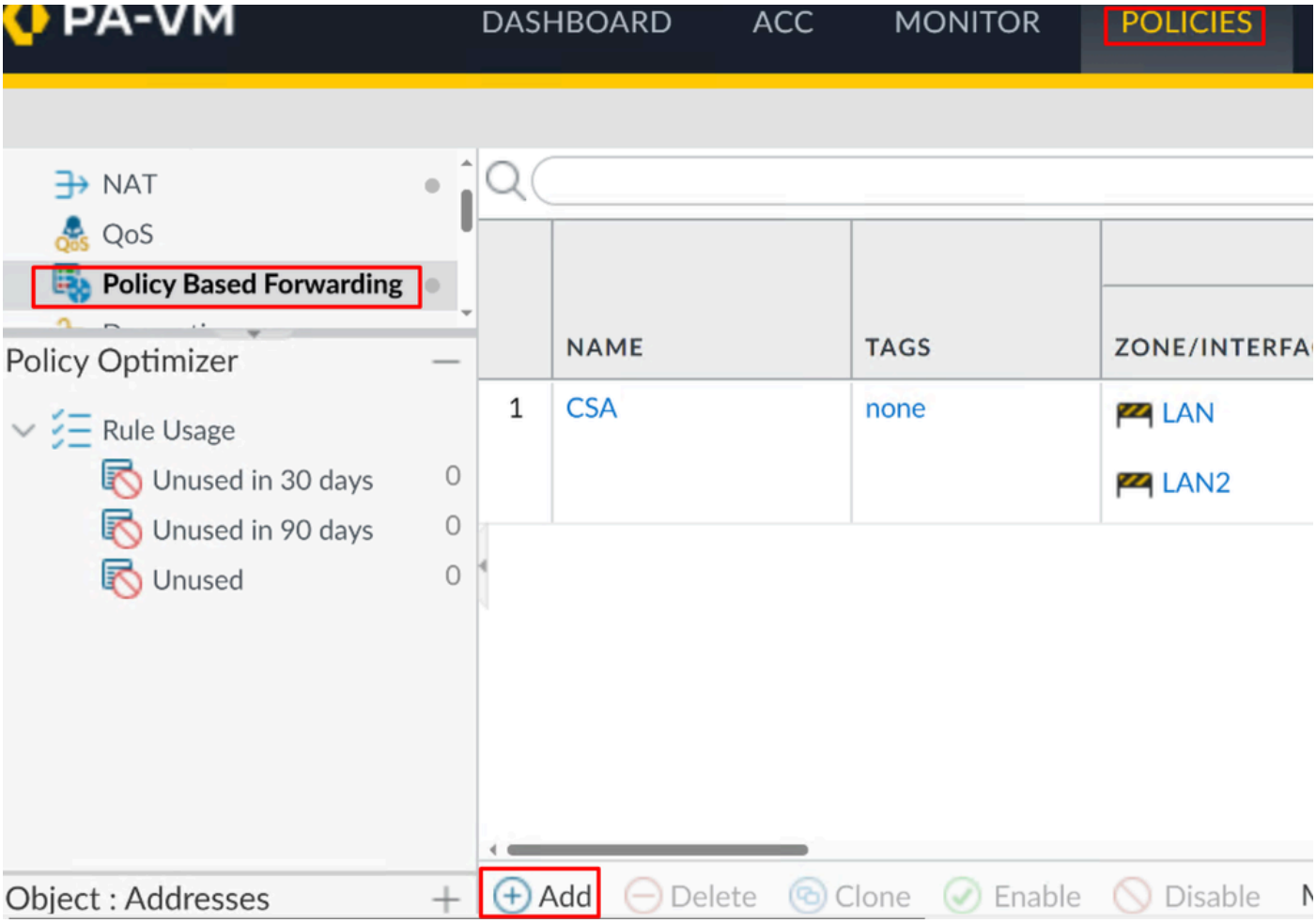


现在您的VPN已成功创建，您可以继续执行步骤 **Configure Policy Based Forwarding**。

配置基于策略的转发

要配置 Policy Based Forwarding，请导航到 Policies > Policy Based Forwarding.

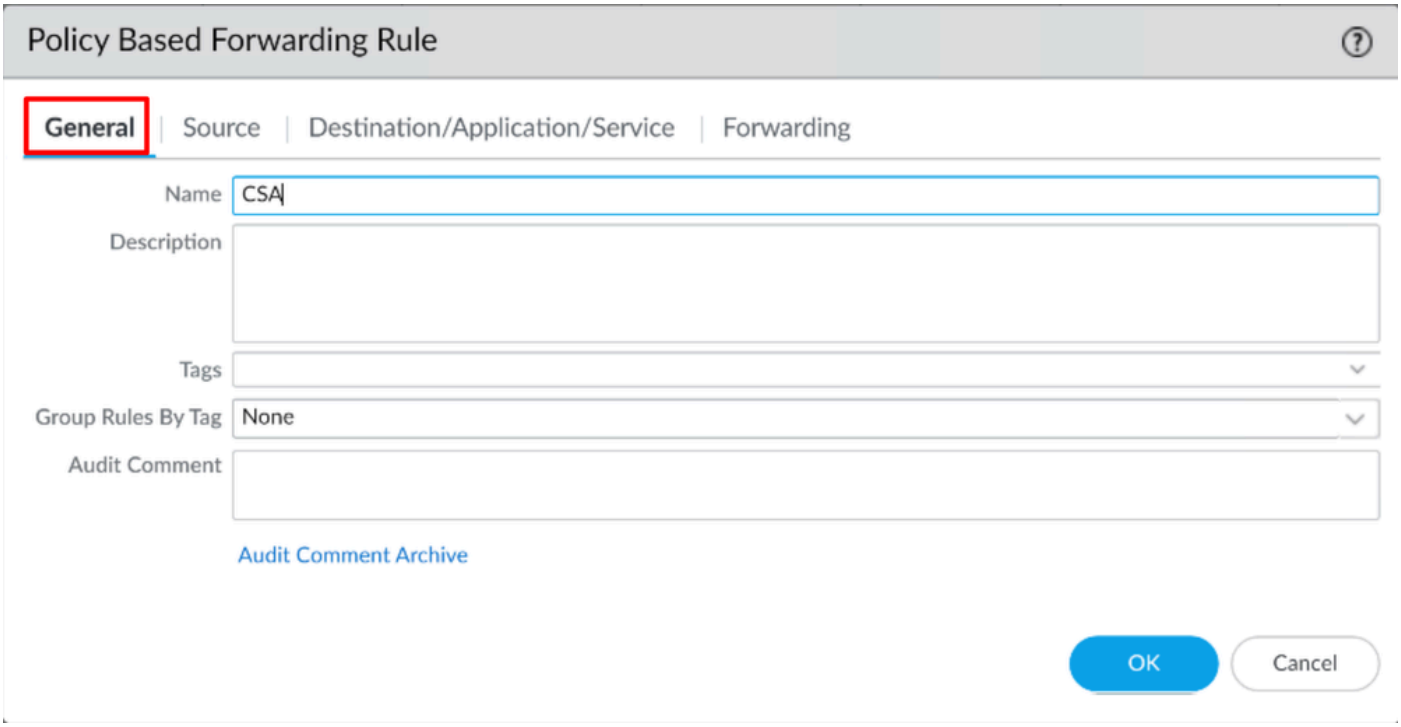
- 点击 Add

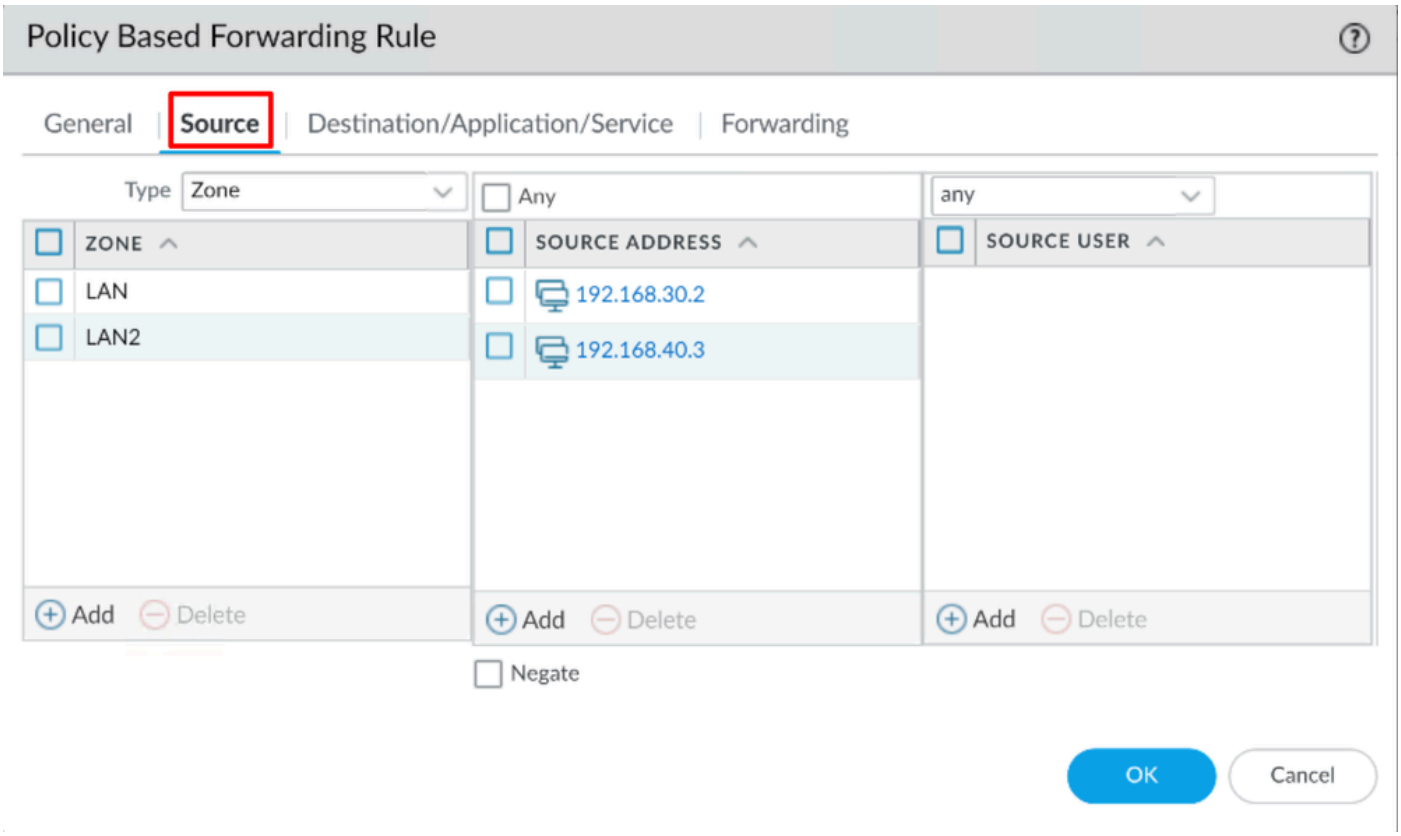


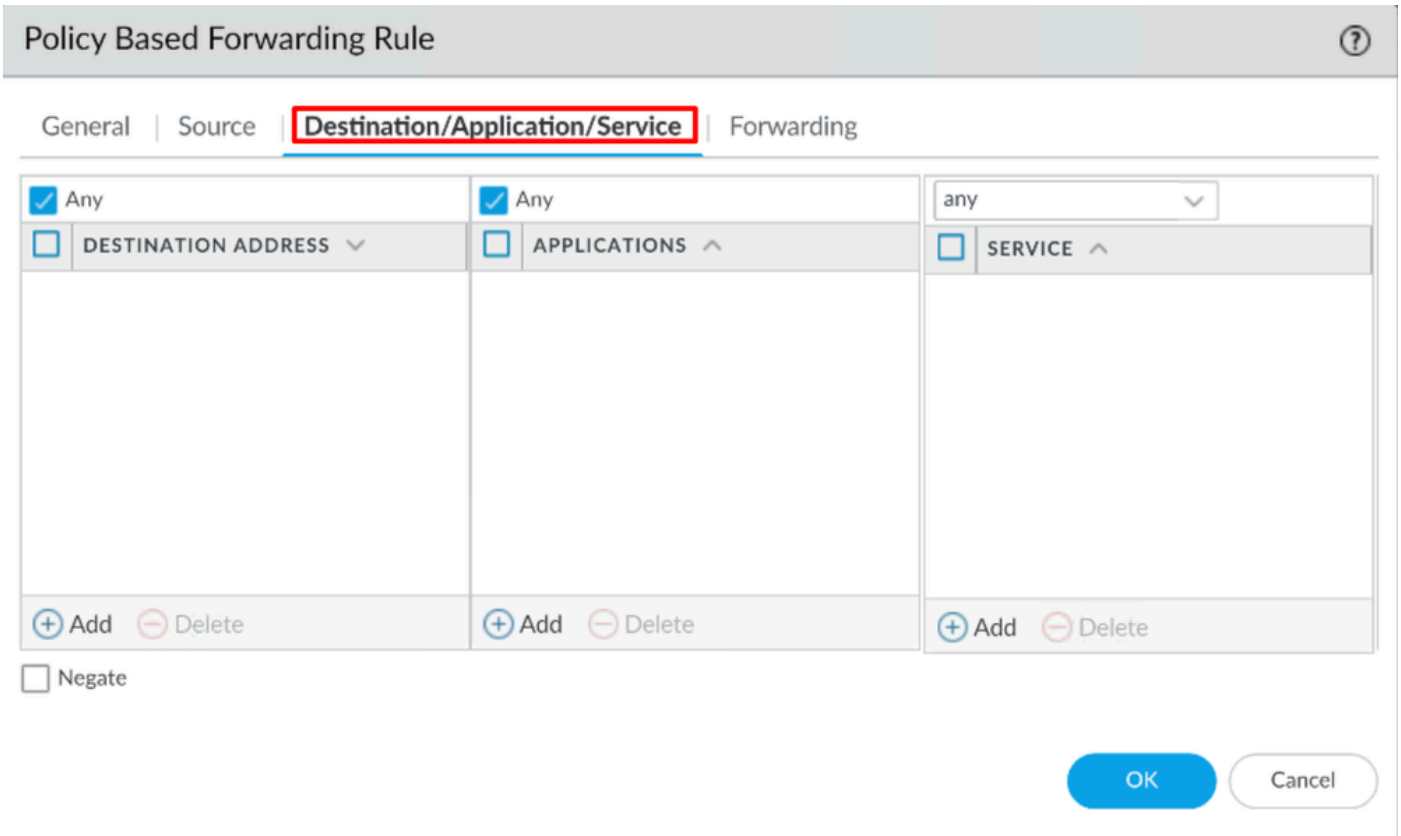
- 配置以下参数：
  - General
    - **Name**：使用名称标识安全访问、策略基础转发（按来源路由）
  - Source
    - **Zone**：选择您计划根据源路由流量的区域
      - **Source Address**：配置要用作源的一个或多个主机。
      - Source Users：配置要路由流量的用户（如果适用）

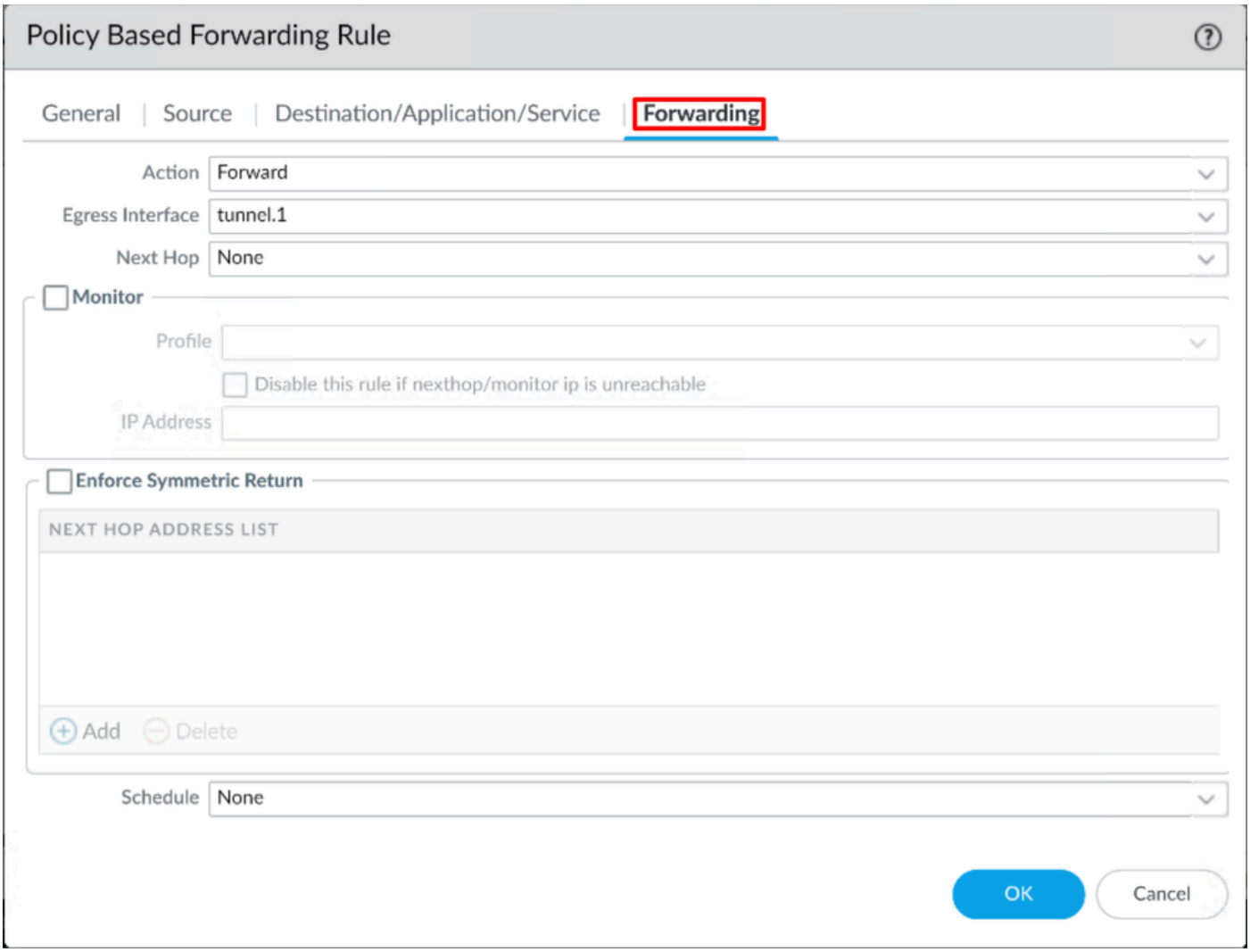
- Destination/Application/Service
    - Destination Address：您可以将其保留为Any，也可以指定安全访问(100.64.0.0/10)的地址范围
- Forwarding
    - **Action**：转发
        - **Egress Interface**：选择在配置隧道接口这一步中配置的隧道接口。
        - **Next Hop**:无

- 点击OK，然后 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



现在，您已在Palo Alto上配置所有内容；配置路由后，可以建立隧道，您需要继续在Secure Access Dashboard上配置RA-VPN、基于浏览器的ZTA或客户端基础ZTA。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。