使用Palo Alto防火墙配置安全访问

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 在安全访问中配置VPN
- 在Palo Alto上配置隧道
  - 配置IPSEC加密配置文件
  - 配置IPSec隧道
  - 配置基于策略的转发

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：

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

使用的组件

本文档中的信息基于：

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

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。这是通过实施多种安全方法和层来实现的，所有这些方法均旨在保护通过云访问信息时的安全。

配置

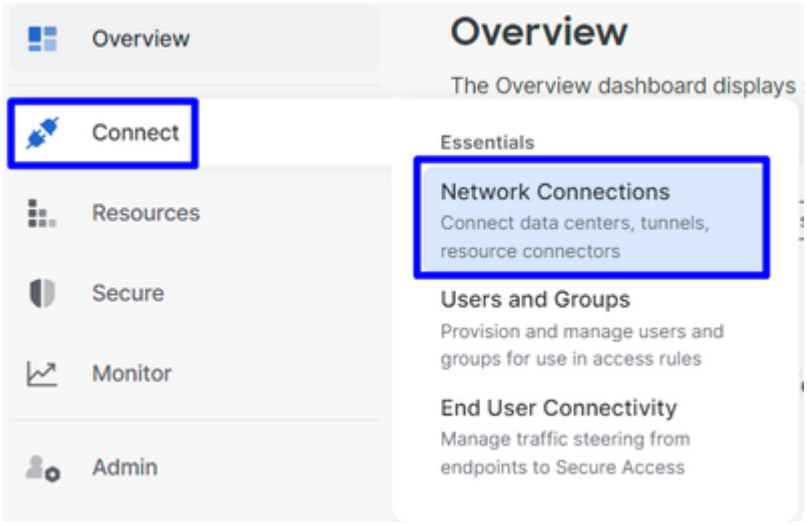
在安全访问中配置VPN

1.导航到Secure Access的管理面板。



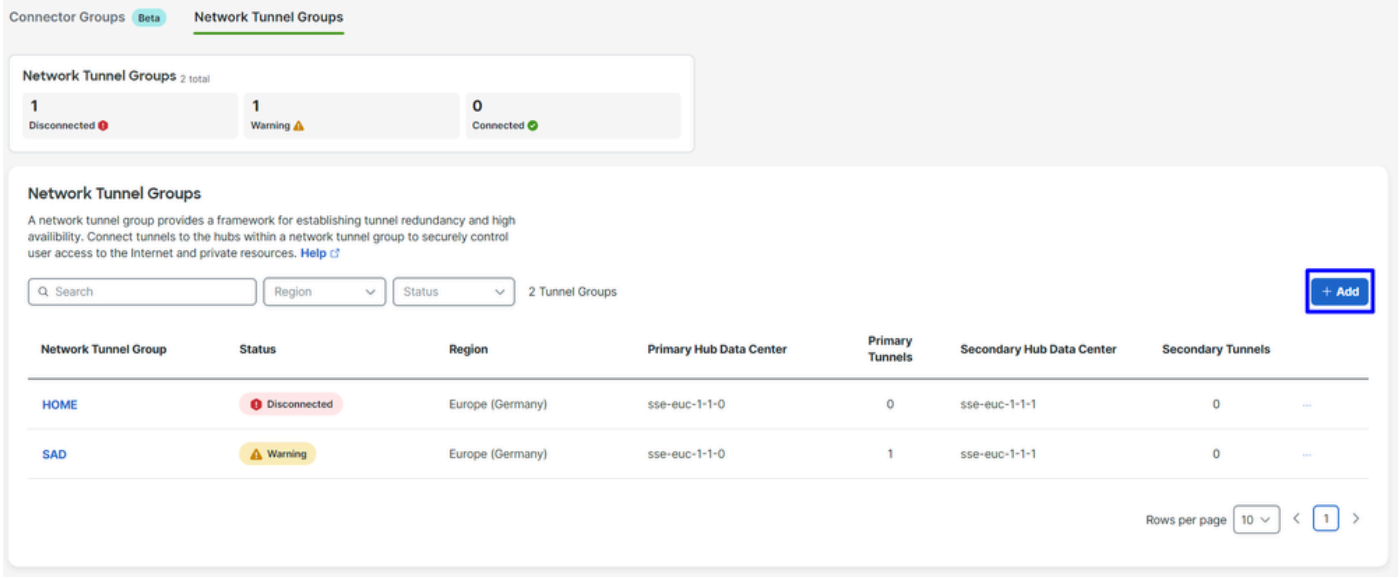
安全访问 — 主页

2.单击连接 > 网络连接。



安全访问 — 网络连接

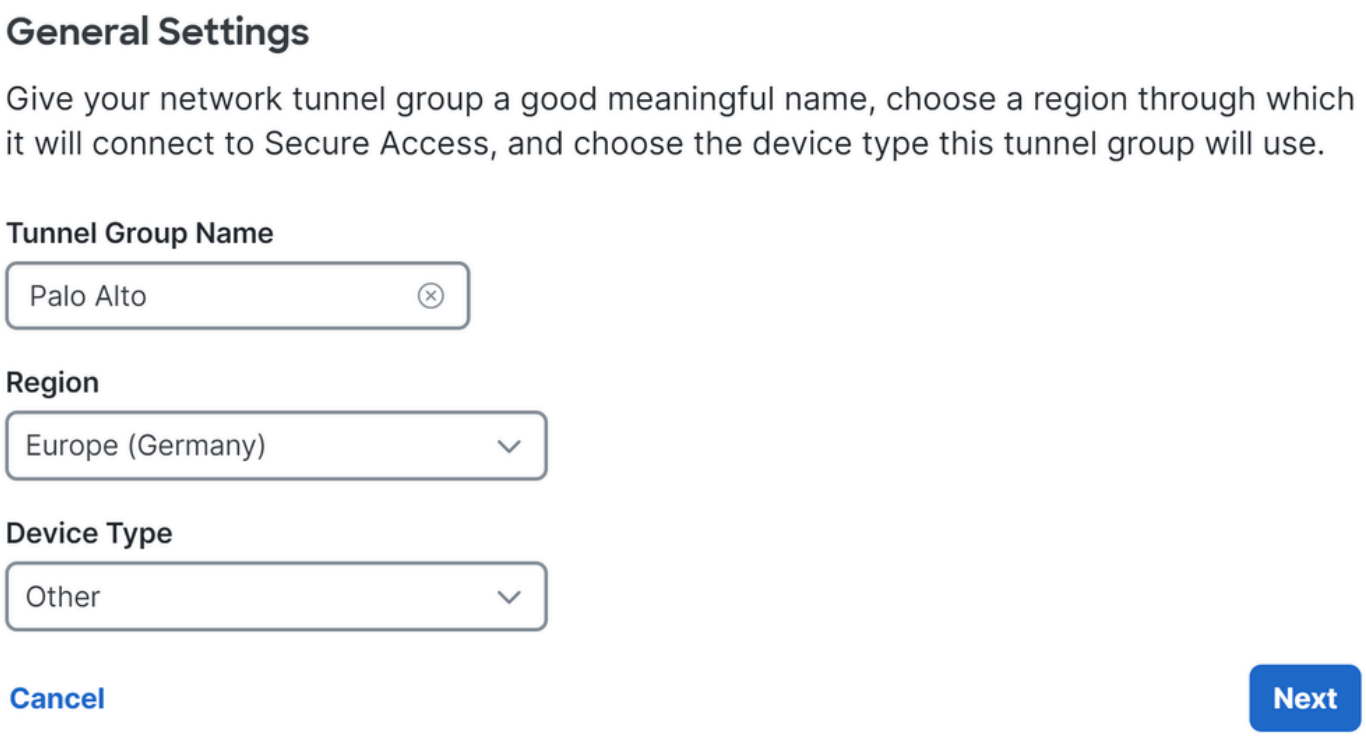
3.在Network Tunnel Groups下，单击+Add。



安全访问 — 网络隧道组

4.配置隧道组名称、区域和设备类型。

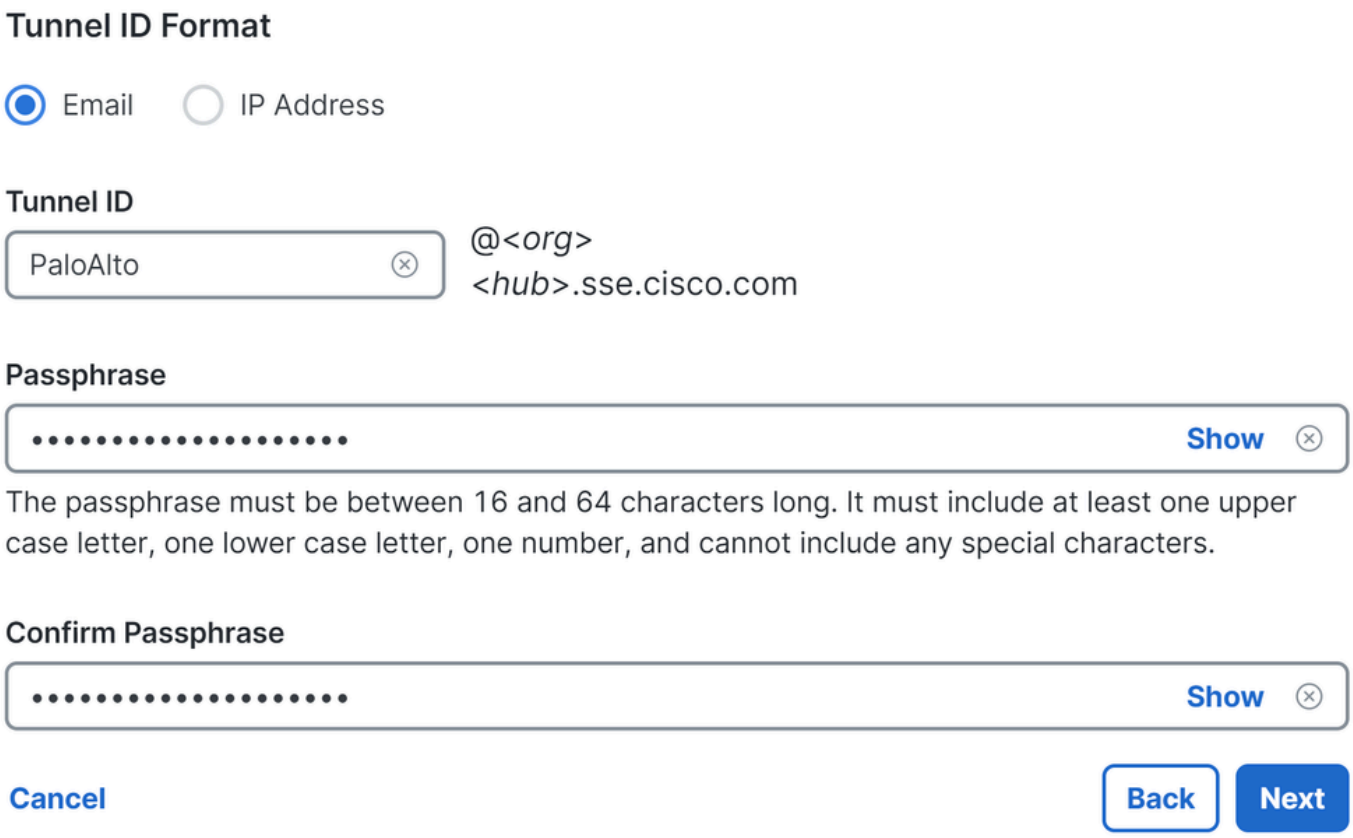
5.单击下一步。



注意：选择距离防火墙位置最近的区域。

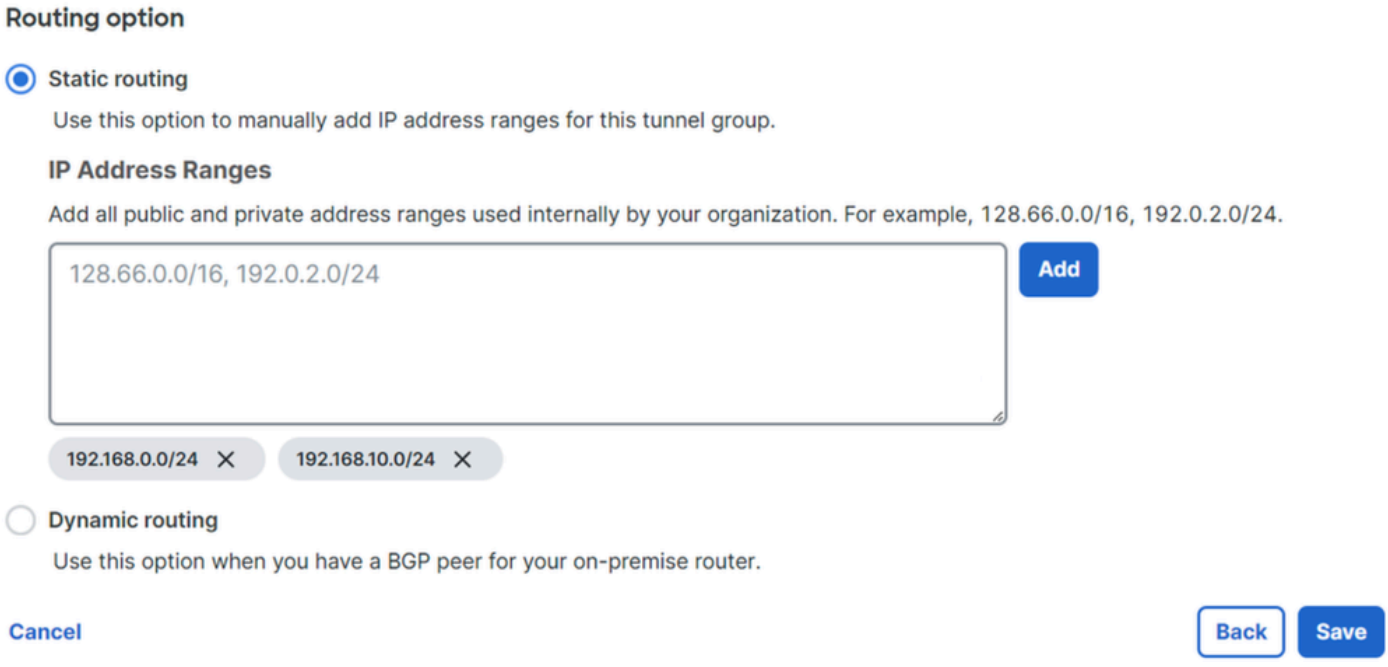
6.配置隧道ID格式和口令。

7.单击下一步。



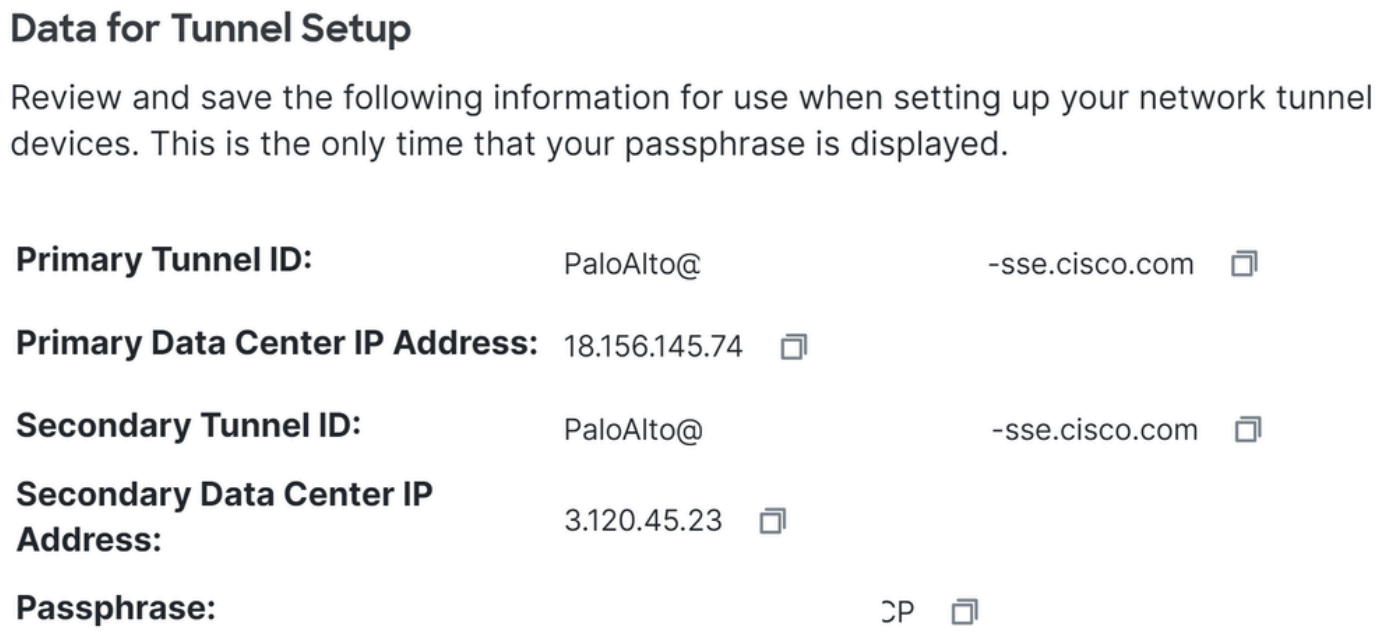
8.配置网络上配置的IP地址范围或主机，并希望通过安全访问传递流量。

9.单击保存。



10.单击Save后，将显示隧道信息，请保存此信息以供下一步操作；在Palo Alto上配置隧道。

隧道数据



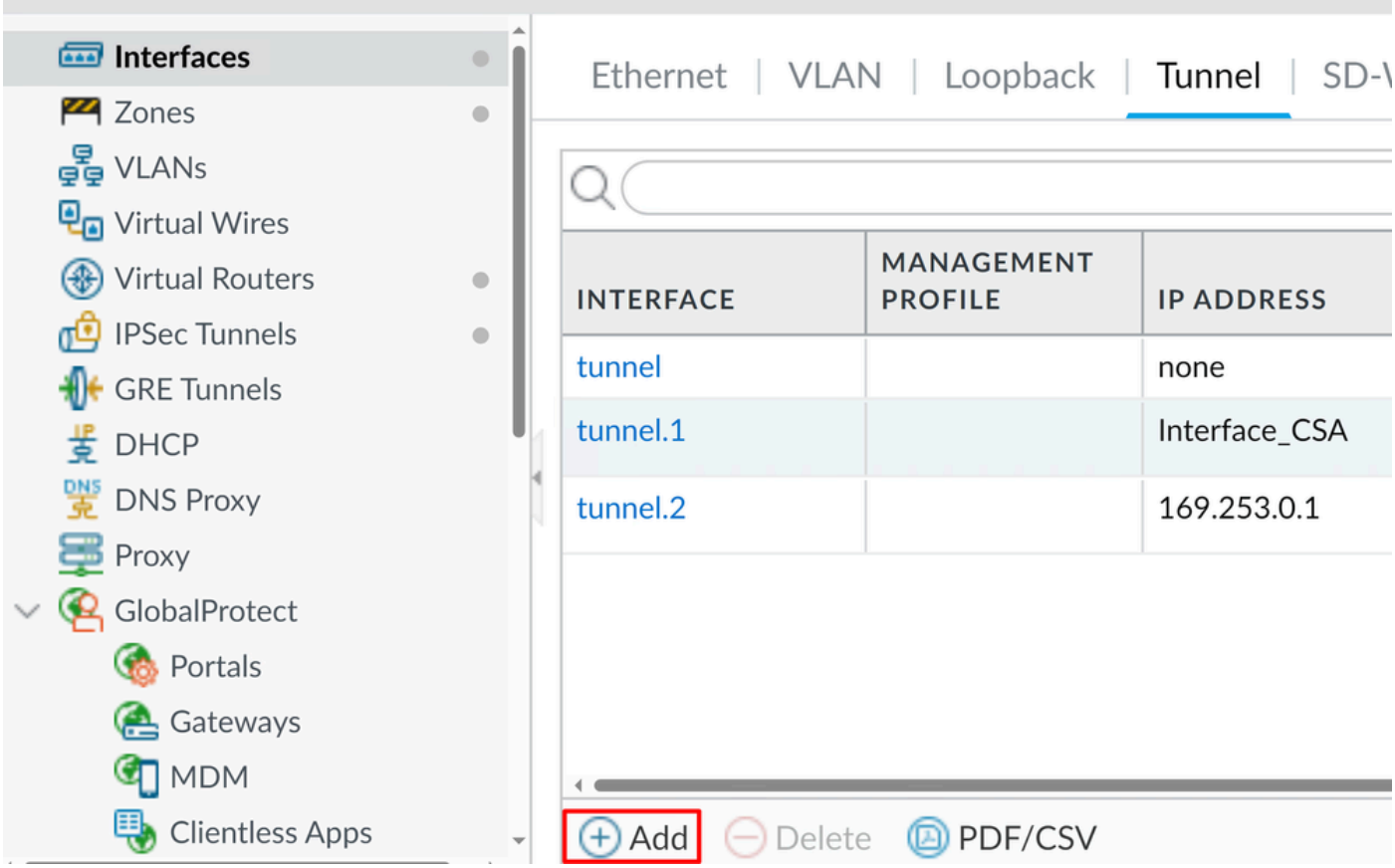
在Palo Alto上配置隧道

配置隧道接口

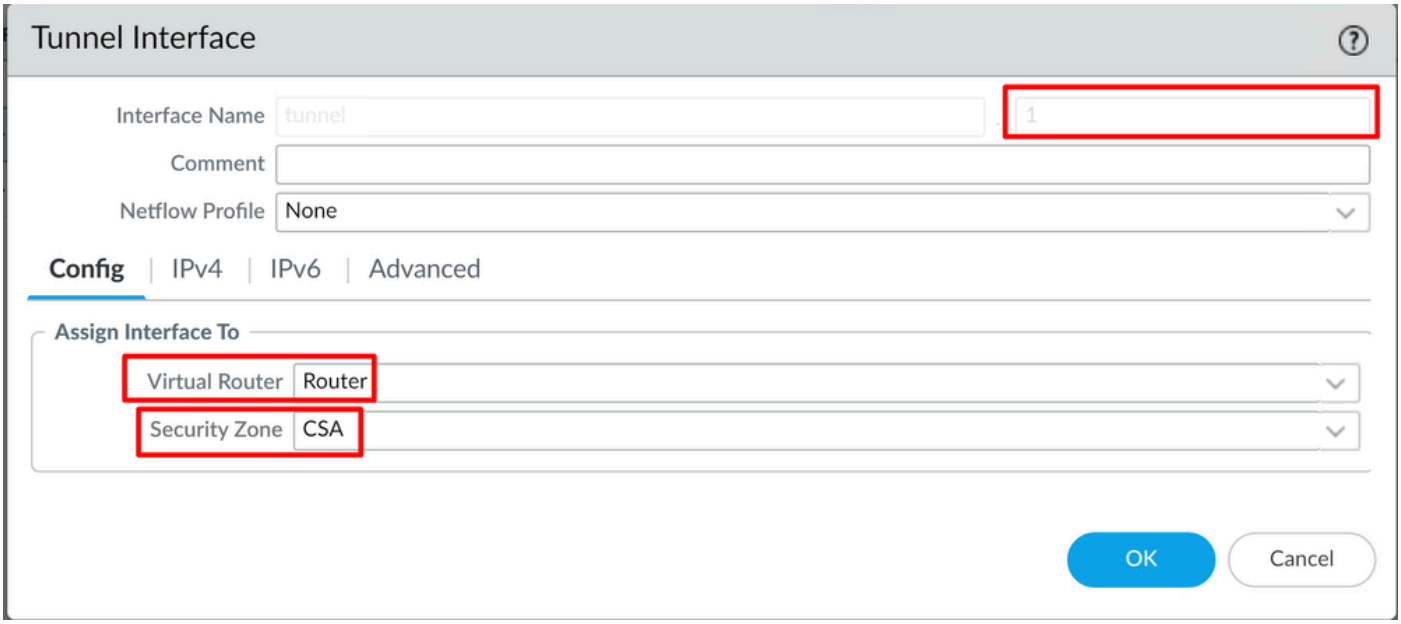
导航至Palo Alto Dashboard。

1. Network > Interfaces > Tunnel。

2.单击Add。

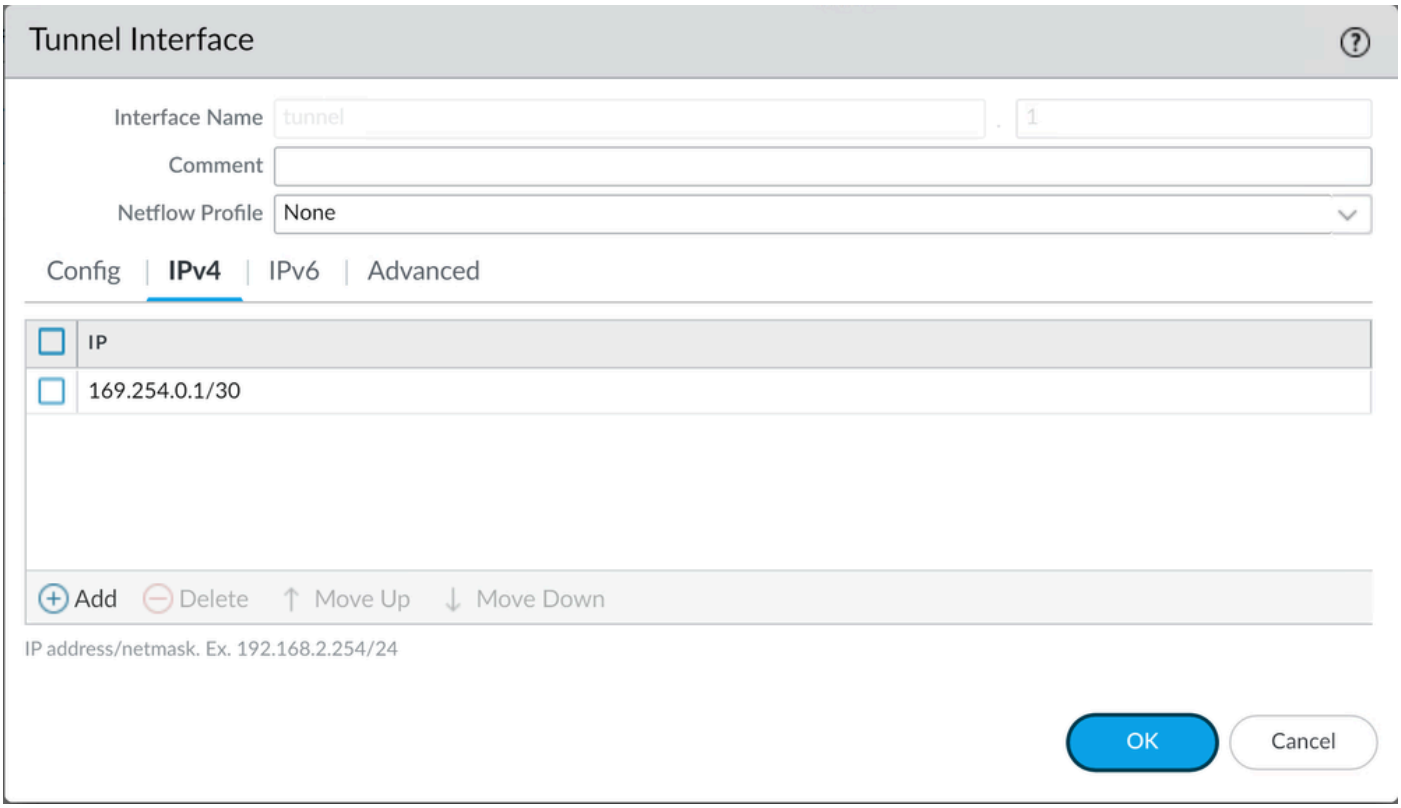


3.在Config菜单下，配置Virtual Router、Security Zone，并分配后缀编号。

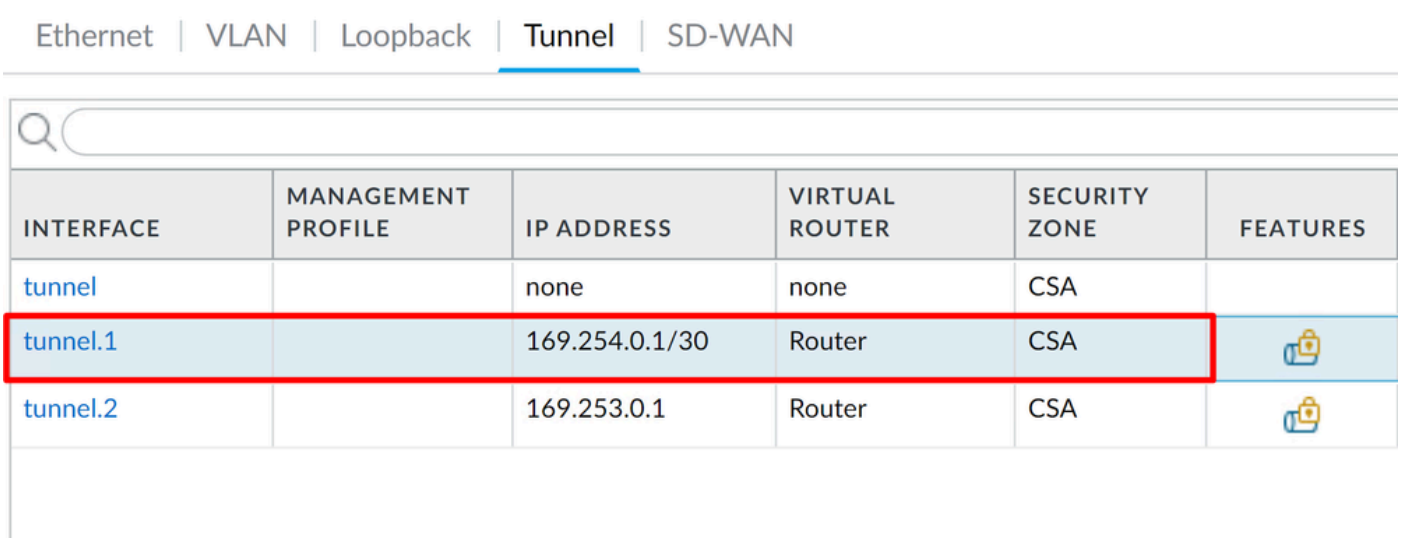


4.在IPv4下，配置不可路由的IP。例如，您可以使用169.254.0.1/30。

5.单击确定。



6.之后，您可以配置如下内容：



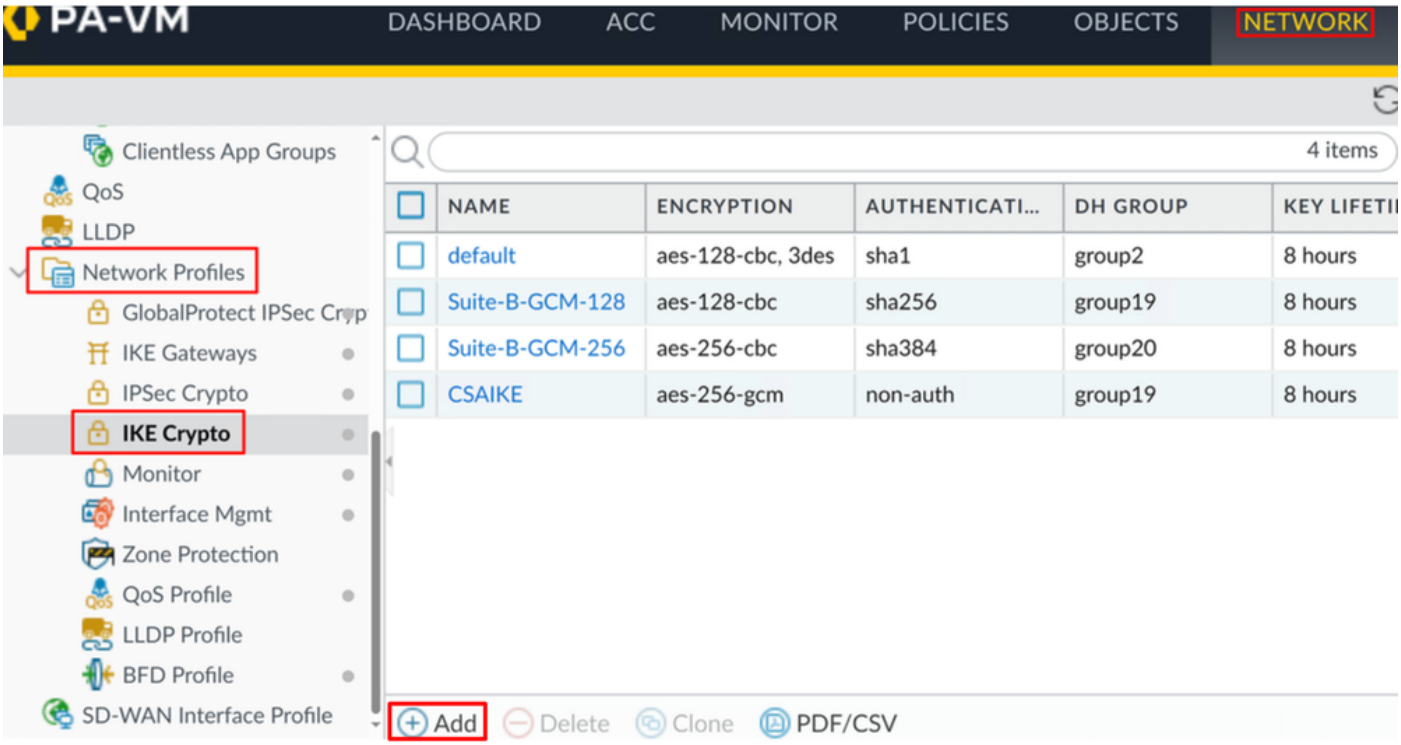
7.如果已按此方式进行配置，请点击提交以保存配置，然后继续执行下一步；配置IKE加密配置文件。

配置IKE加密配置文件

要配置加密配置文件，请导航至：

1. Network > Network Profile > IKE加密。

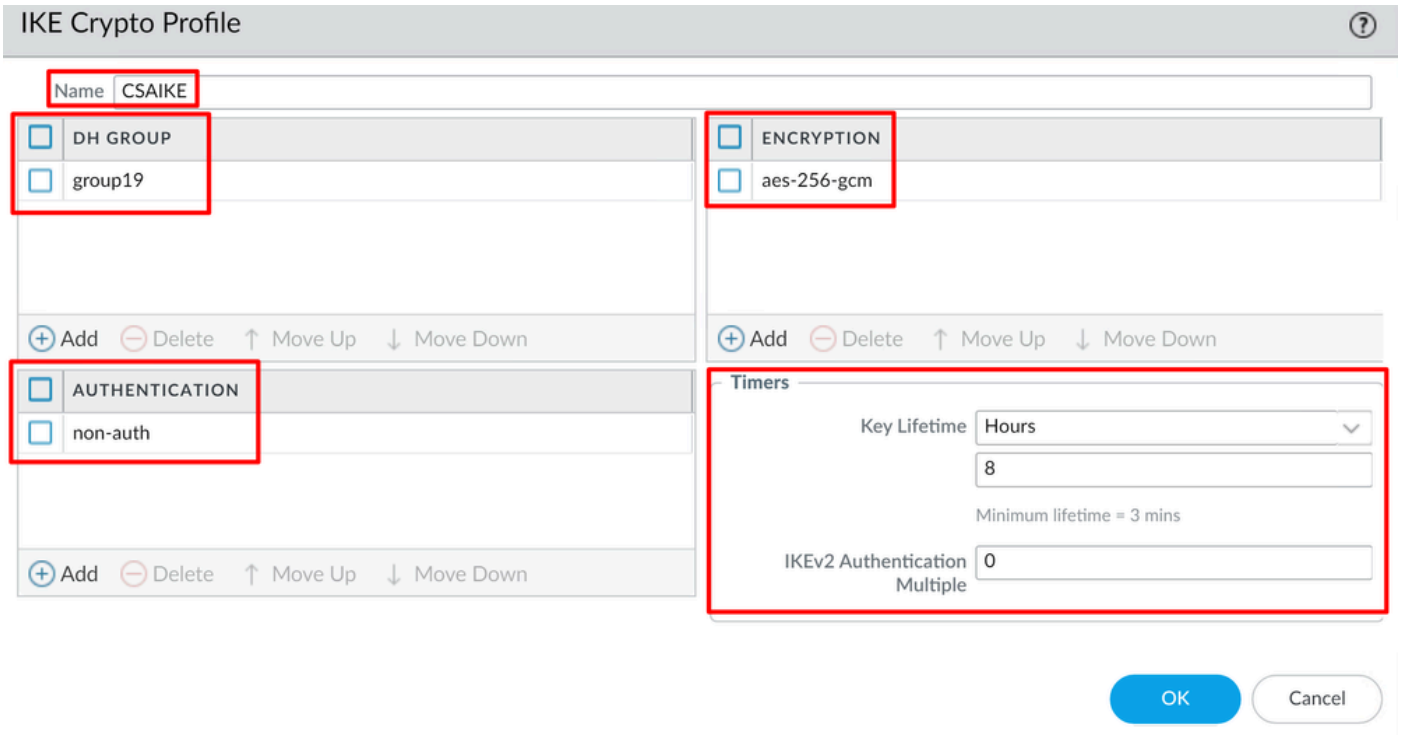
2.单击Add。



3.配置以下参数：

- 名称：配置名称以标识配置文件。
- DH GROUP：组19
- 身份验证:非身份验证
- 加密 :aes-256-gcm
- 计时器:
  - 密钥生命期:8 小时
  - IKEv2身份验证:0

4.完成所有配置后，单击OK。



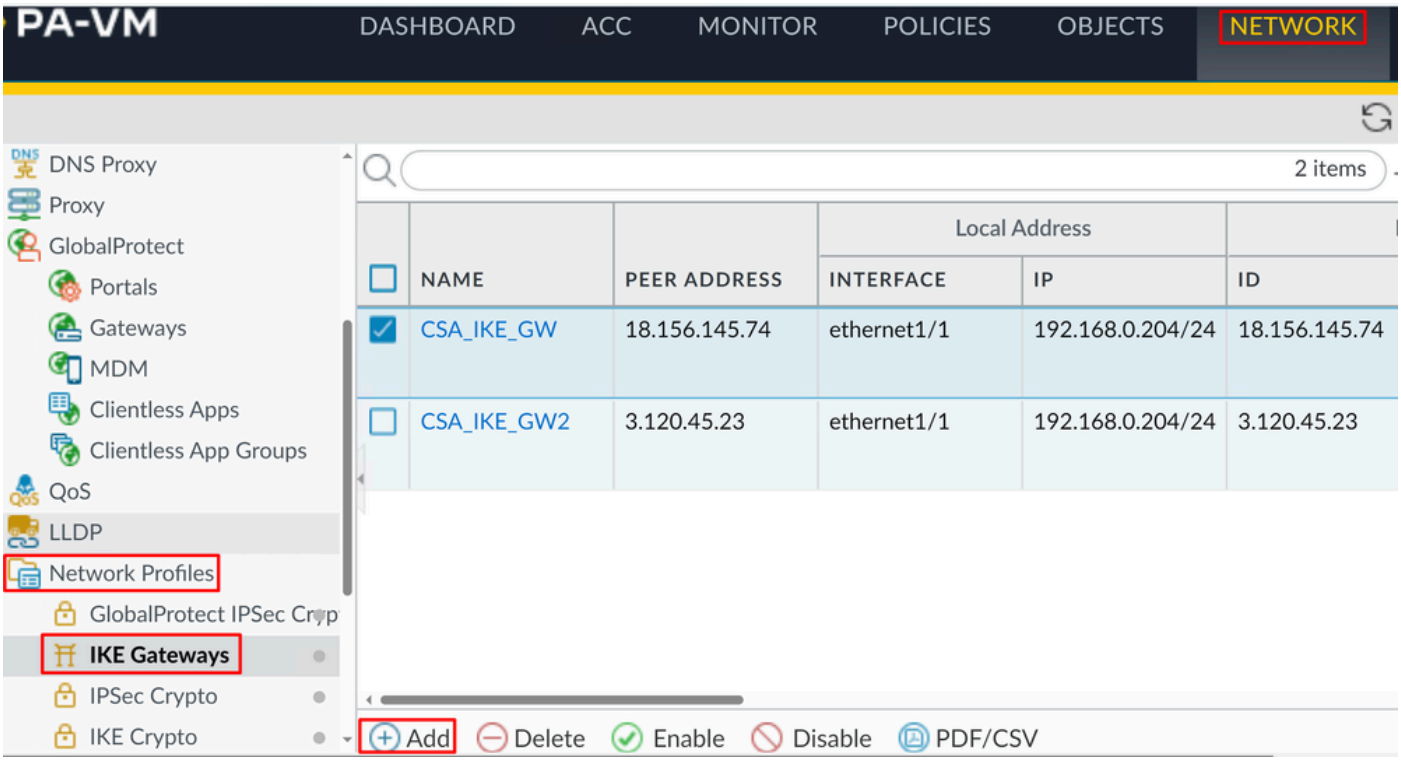
5.如果已按此方式进行配置，请单击Commit保存配置，然后继续下一步；配置IKE网关。

配置IKE网关

配置IKE网关

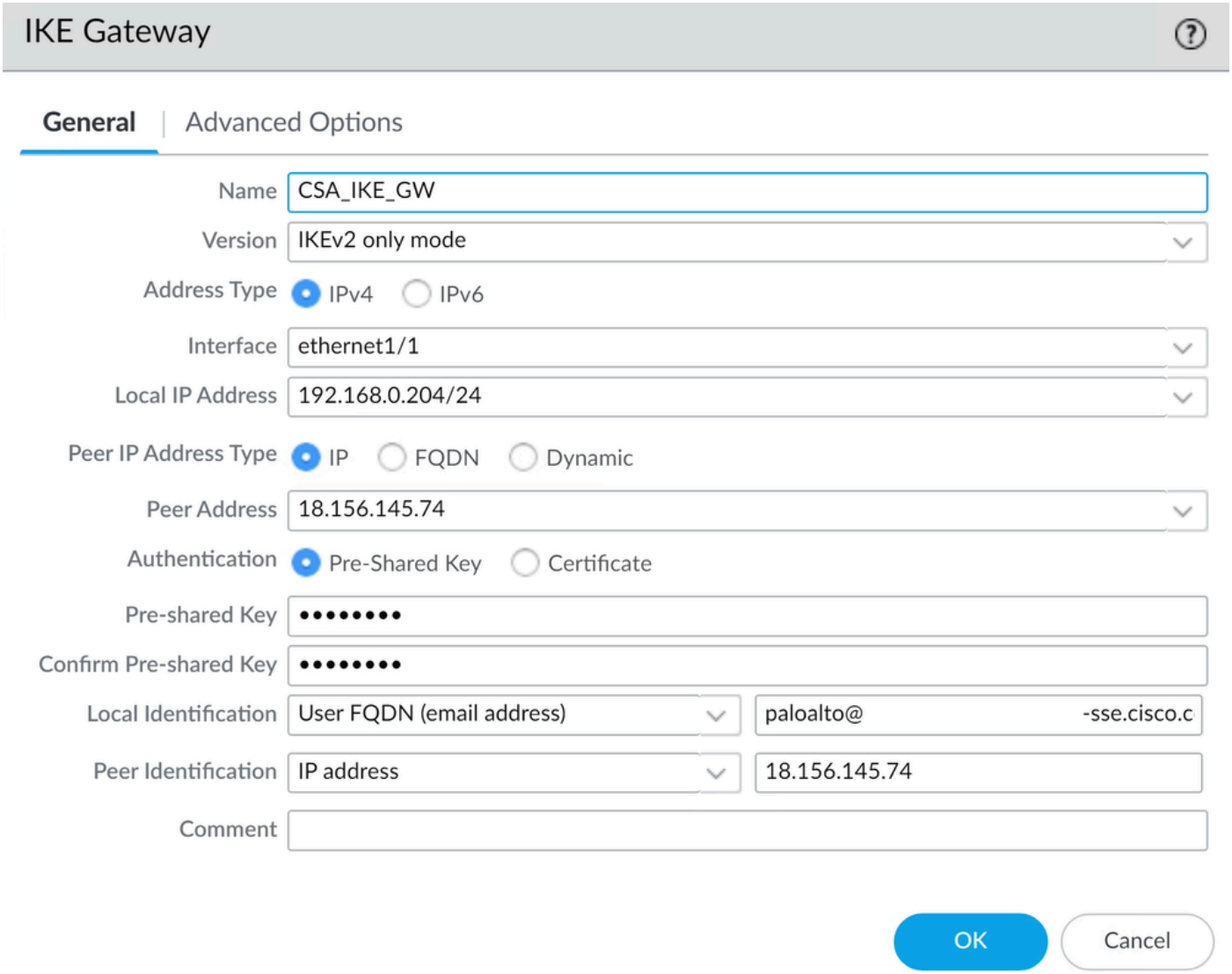
1. Network > Network Profile > IKE Gateways。

2.单击Add。



3.配置以下参数：

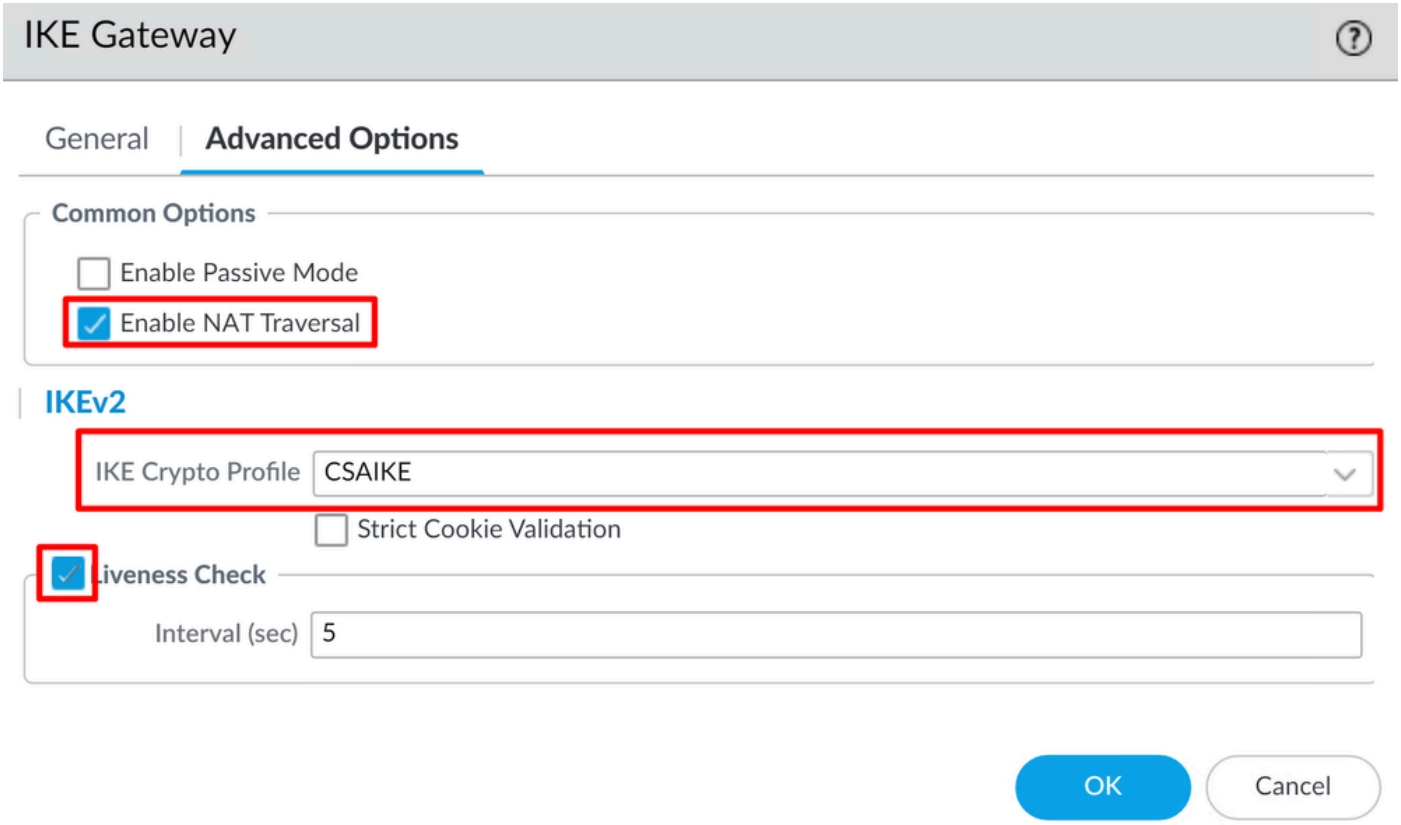
- 名称：配置用于标识Ike网关的名称
- 版本:仅IKEv2模式
- 地址类型:IPv4
- 接口:选择您的互联网WAN接口
- 本地 IP 地址:选择您的互联网WAN接口的IP
- 对等IP地址类型:IP
- 对等体地址:使用Tunnel Data步骤中给出的主IP数据中心IP地址的IP
- 身份验证:预共享密钥
- 预共享密钥:使用Tunnel Data步骤中给出的口令
- 确认预共享密钥:使用Tunnel Data步骤中给出的口令
- 本地标识:选择User FQDN(Email address)，并使用步骤Tunnel Data中给定的主隧道ID
- 对等体标识:选择IP Address并使用Primary IP Datacenter IP Address



4.单击Advanced Options。

- 启用NAT穿越
- 选择在步骤Configure IKE Crypto Profile中创建的IKE Crypto Profile
- 选中“活动检查”复选框

5.单击确定。

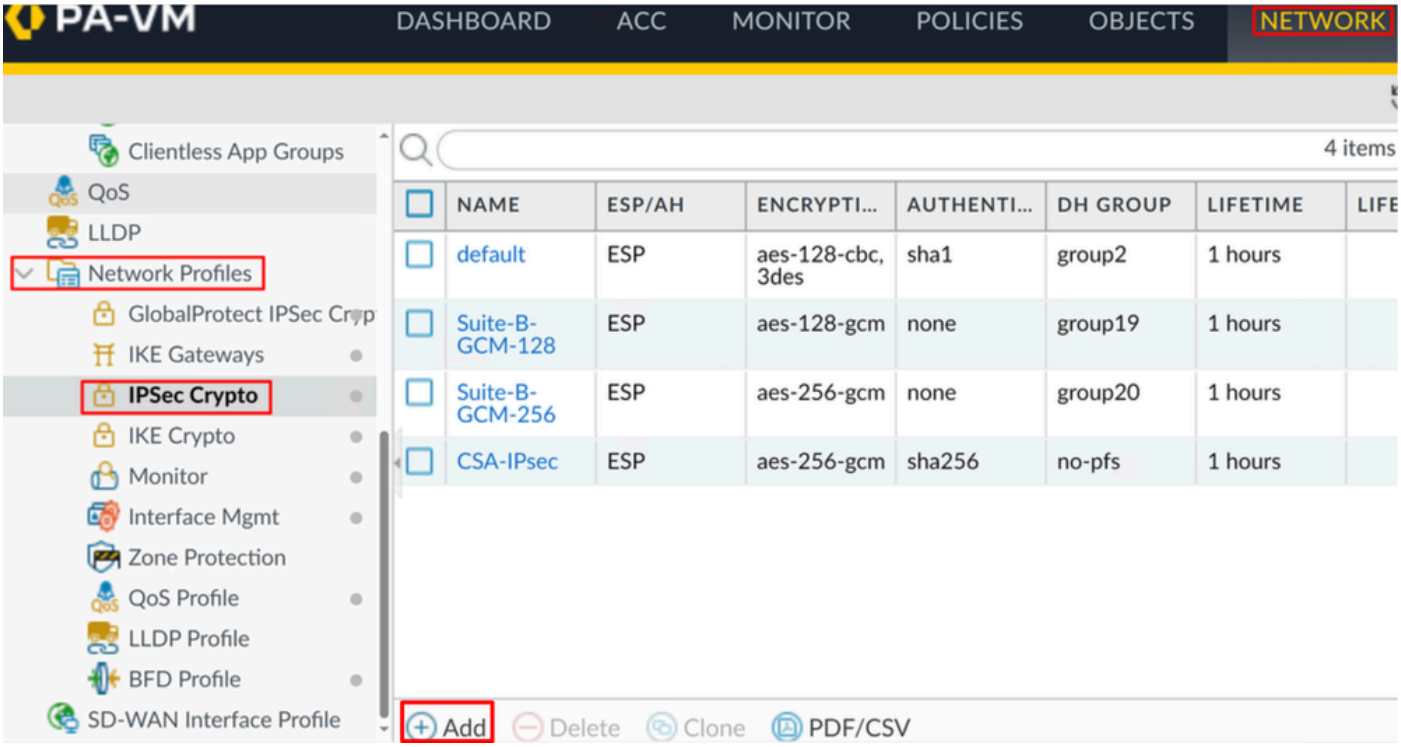


6.如果已按此方式进行配置，请单击Commit以保存配置，然后继续下一步Configure IPSEC Crypto Profile。

配置IPSEC加密配置文件

1.要配置IKE网关，请导航到Network > Network Profile > IPSEC加密。

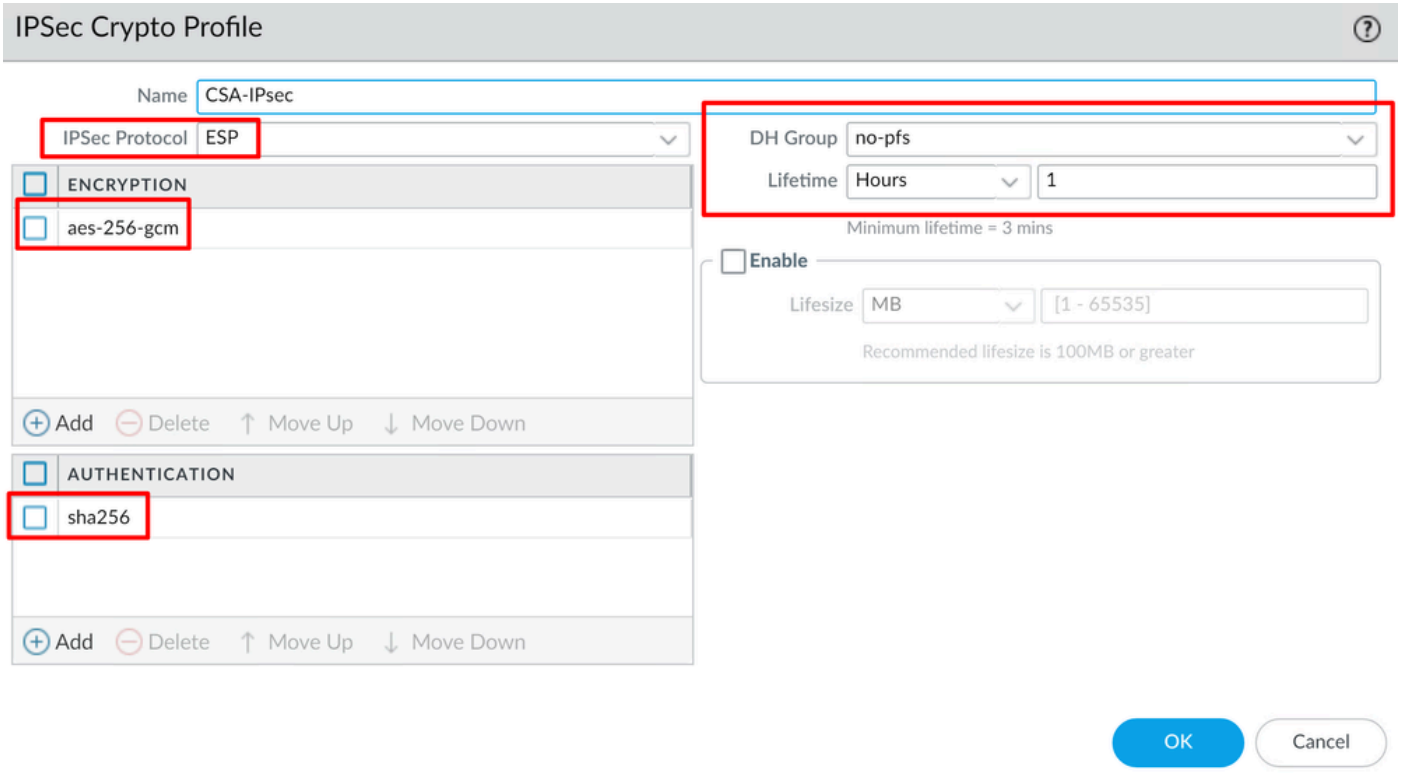
2.单击Add。



3.配置以下参数：

- 名称：使用名称标识安全访问IPsec配置文件
- IPsec 协议:ESP
- 加密 :aes-256-gcm
- DH Group：no-pfs， 1小时

4.单击确定。

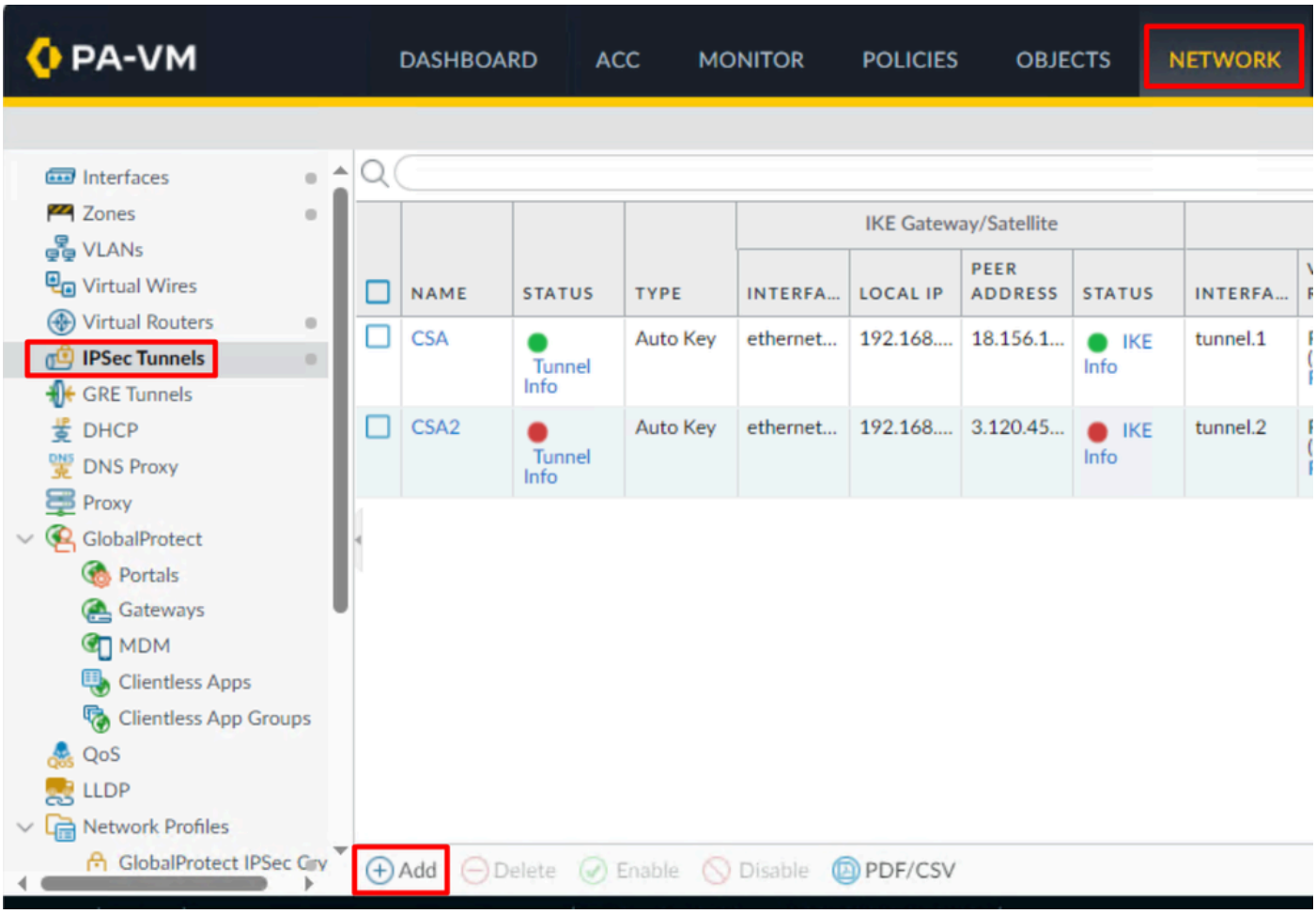


5.如果已按此方式进行配置，请单击Commit保存配置，然后继续下一步；配置IPSec隧道。

配置IPSec隧道

1.要配置IPSec Tunnels，请导航到Network > IPSec Tunnels。

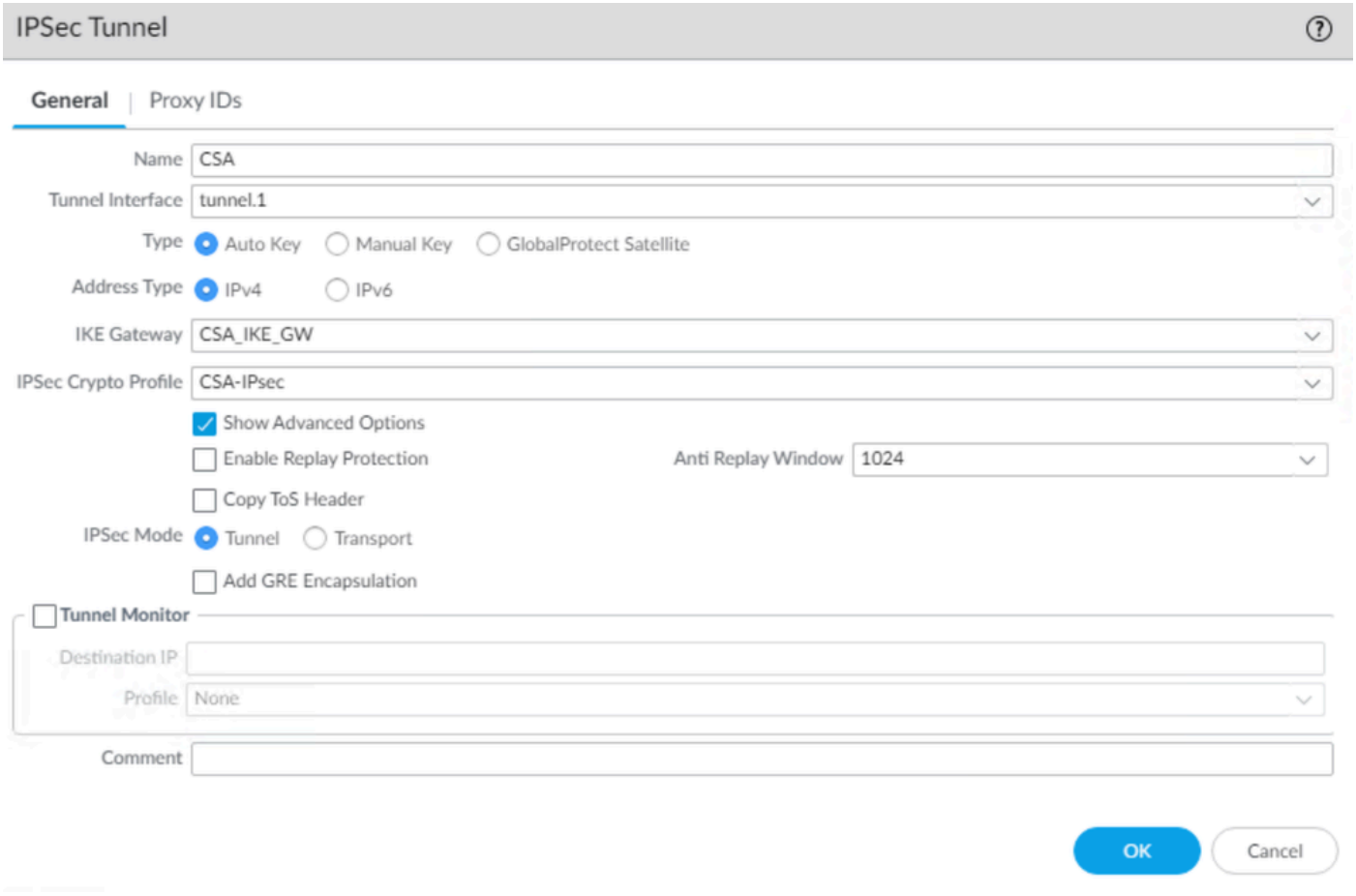
2.单击Add。



3.配置以下参数：

- 名称：使用名称来标识安全访问隧道
- 通道接口:选择步骤中配置的隧道接口，配置隧道接口
- type：自动密钥
- 地址类型:IPv4
- IKE网关:选择在步骤配置IKE网关上配置的IKE网关
- IPsec加密配置文件:选择在步骤配置IPSEC加密配置文件上配置的IKE网关
- 选中“高级选项”复选框
    - IPSec模式隧道:选择隧道

4.单击确定。



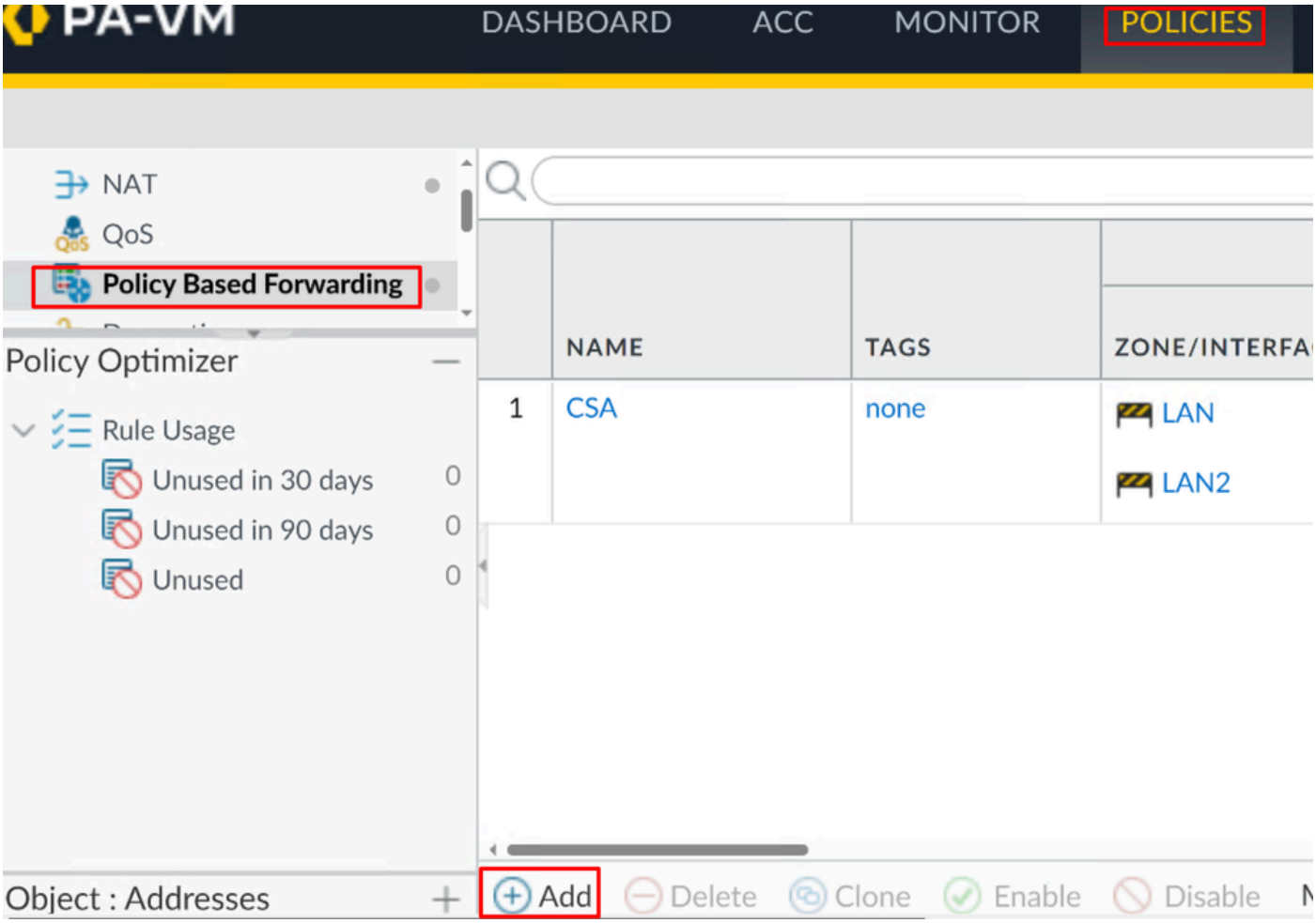
⚠ 警告：代理ID不受支持，请避免在具有安全访问的Palo Alto IPSEC隧道中使用代理ID进行任何配置。

现在您的VPN已成功创建，您可以继续执行此步骤；配置基于策略的转发。

配置基于策略的转发

1.要配置基于策略的转发，请导航到策略 > 基于策略的转发。

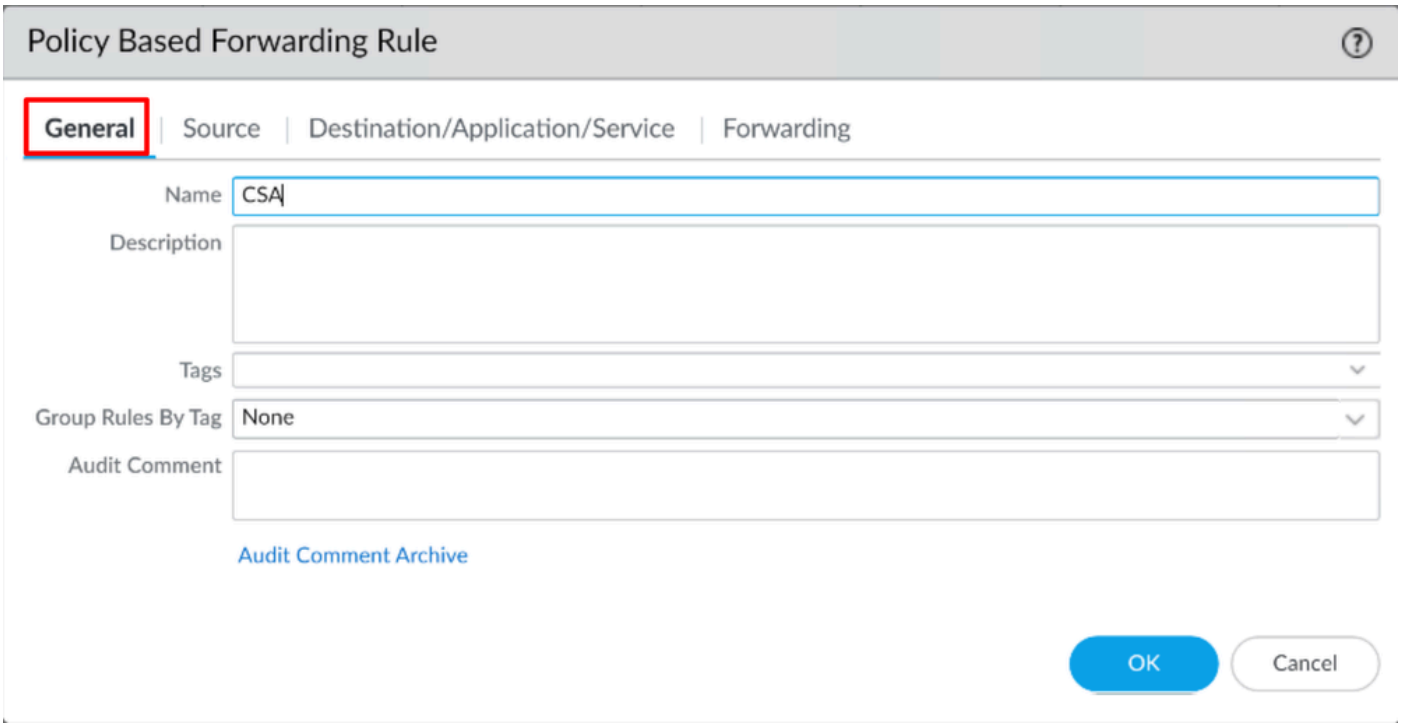
2.单击Add。

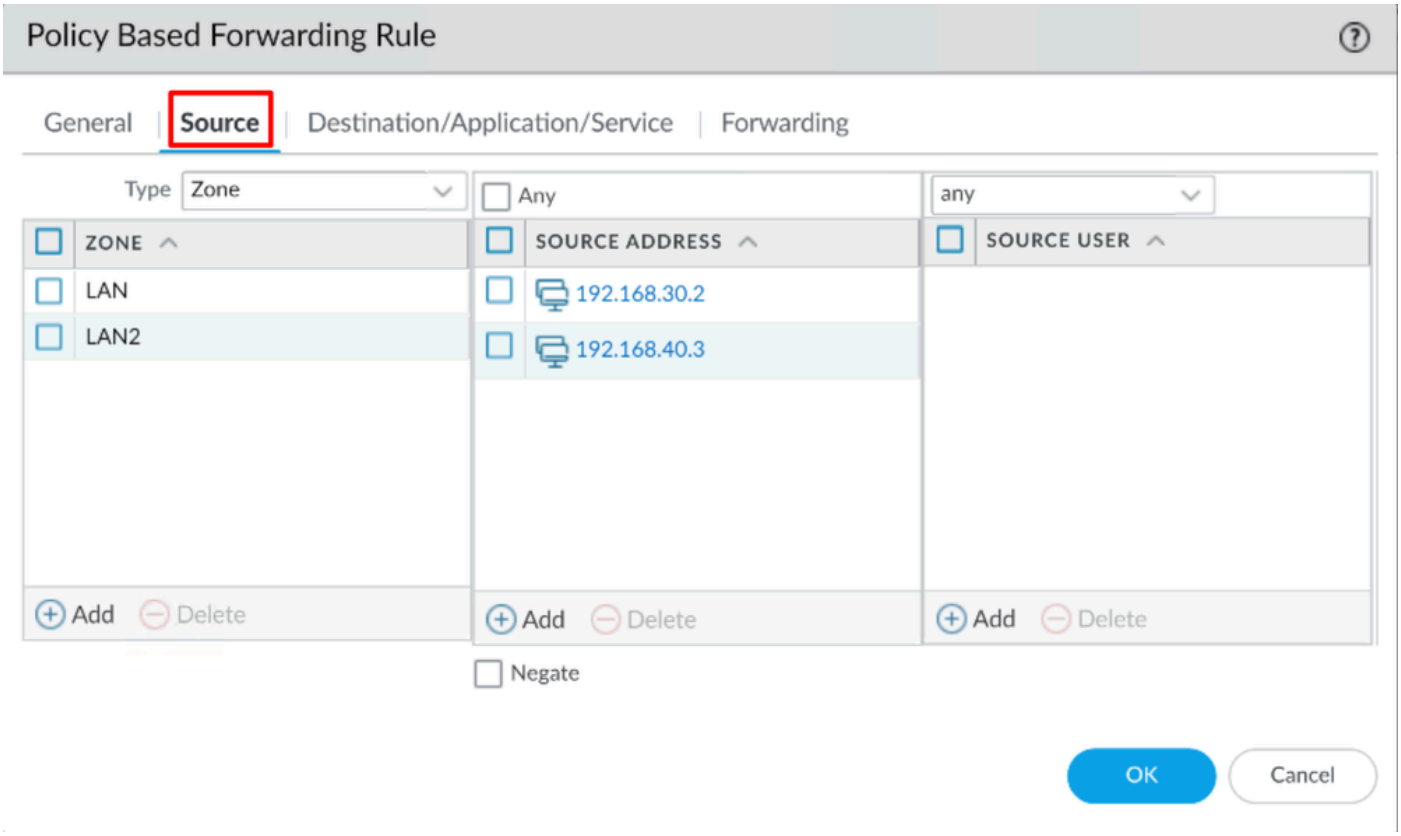


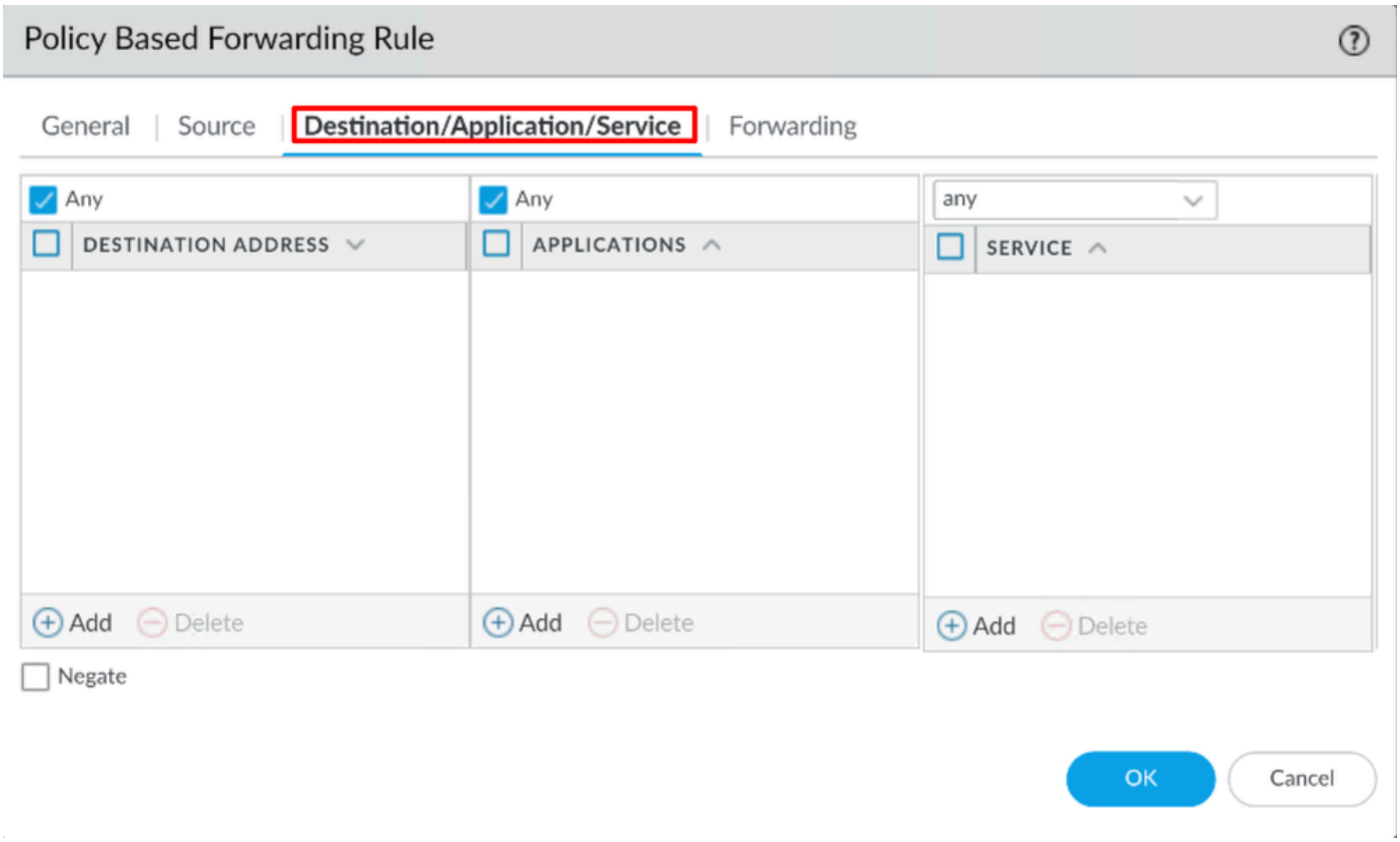
3.配置以下参数：

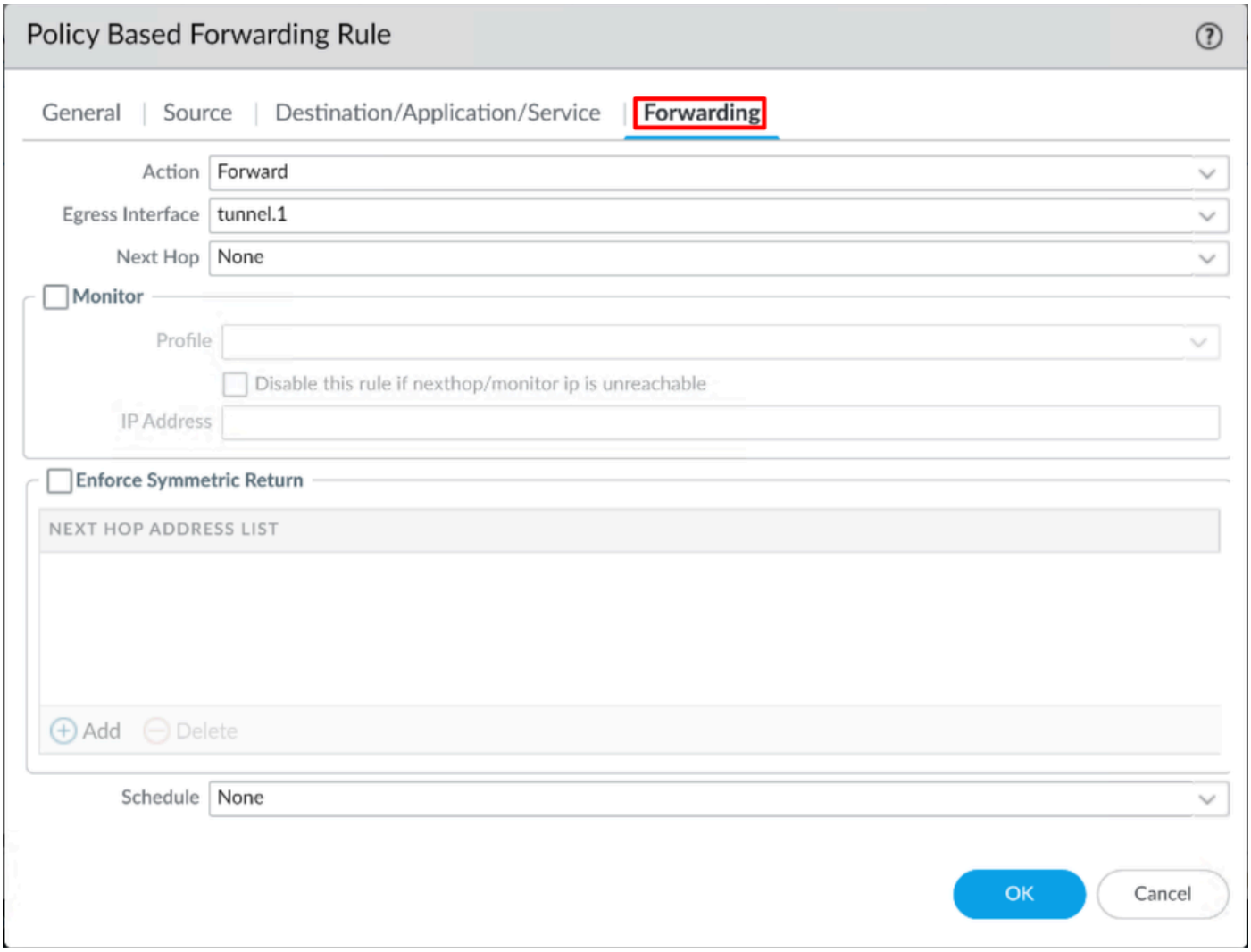
- 常规
  - 名称：使用名称标识安全访问和策略基本转发（按来源路由）
- 来源
  - 区域:选择您计划根据源路由流量的区域
  - 源地址：配置要用作源的主机或网络
  - 源用户:配置要将流量路由到的用户（如果适用）
- 目标/应用/服务
  - 目的地址：您可以保留为Any，或指定安全访问的地址范围(100.64.0.0/10)
- 转发
  - 操作：转发
  - Egress 接口:选择在步骤Configure the tunnel interface中配置的隧道接口。
  - 下一跳：无

4.单击OK和Commit。


Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Name
CSA
Description
Tags
Group Rules By Tag
None
Audit Comment
Audit Comment Archive
OK
Cancel


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


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


Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Action
Forward
Egress Interface
tunnel.1
Next Hop
None
Monitor
Profile
Disable this rule if nexthop/monitor ip is unreachable
IP Address
Enforce Symmetric Return
NEXT HOP ADDRESS LIST
Add
Delete
Schedule
None
OK
Cancel

现在，一切都在Palo Alto上进行了配置。配置路由后，可以建立隧道。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）。