Configuración del acceso seguro con el firewall de Palo Alto

Contenido

Introducción

Este documento describe cómo configurar Secure Access con el Firewall de Palo Alto.

Prerequisites

- Configurar aprovisionamiento de usuarios
- Configuración de Autenticación SSO de ZTNA
- Configurar acceso seguro VPN de acceso remoto

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall de la versión 11.x de Palo Alto
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

Componentes Utilizados

La información de este documento se basa en:

- Firewall de la versión 11.x de Palo Alto
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco ha diseñado Secure Access para proteger y proporcionar acceso a aplicaciones privadas, tanto in situ como basadas en la nube. También protege la conexión de la red a Internet. Esto se consigue mediante la implementación de varios métodos y capas de seguridad, todo ello con el objetivo de preservar la información a medida que acceden a ella a través de la nube.

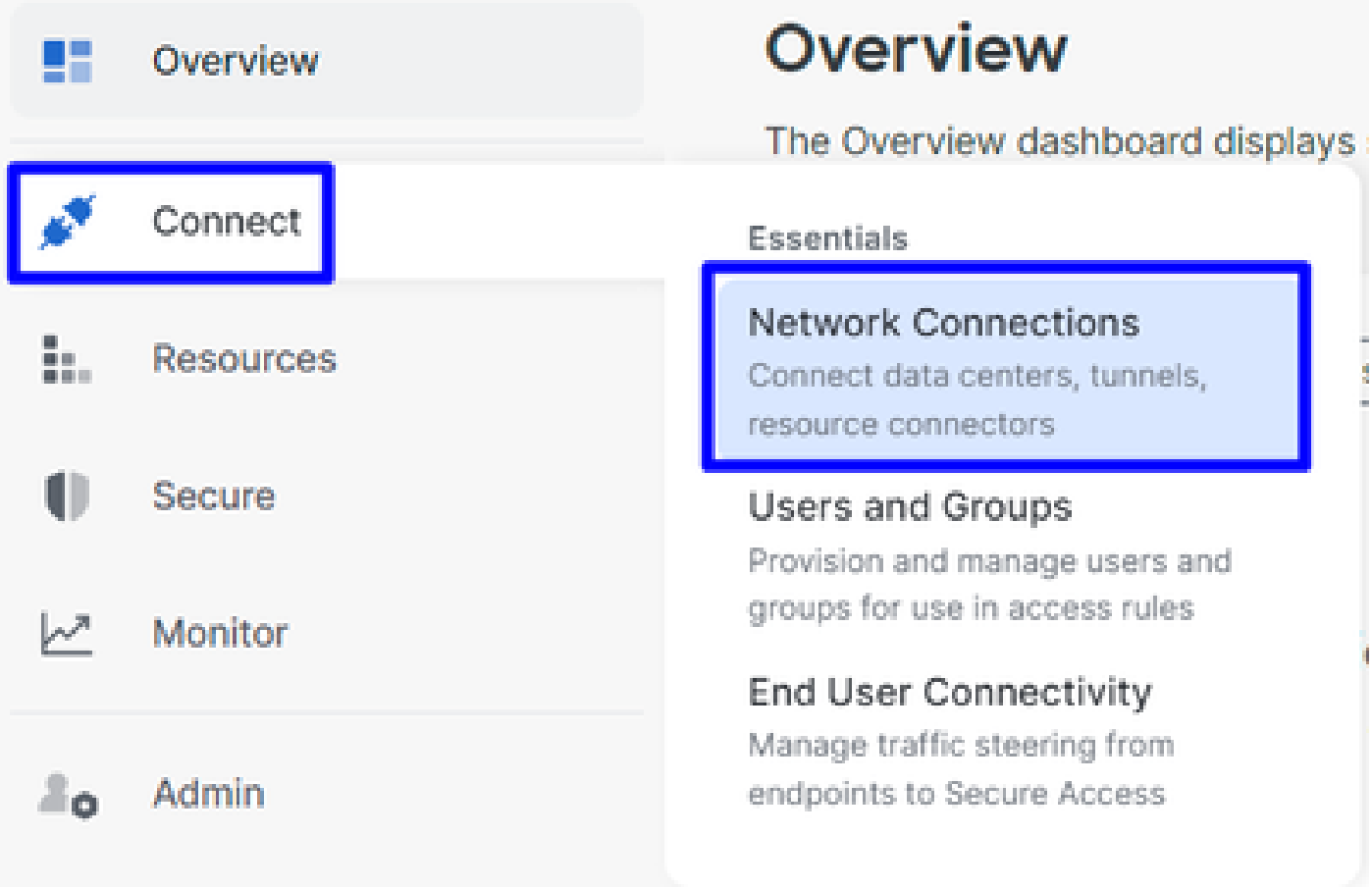
Configurar

Configuración de la VPN en Secure Access

Vaya al panel de administración de Secure Access.

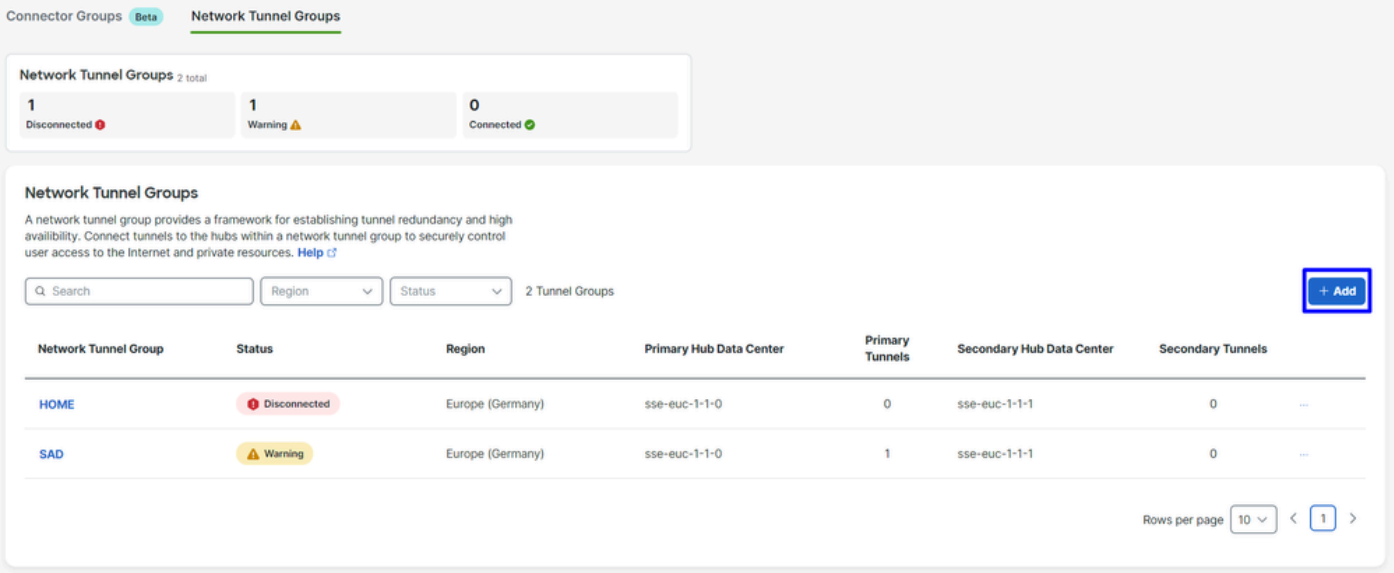
Acceso seguro - Página principal

- Haga clic en Connect > Network Connections



Acceso seguro - Conexiones de red

- En Network Tunnel Groups haga clic en + Add



Acceso seguro - Grupos de túnel de red

- Configurar Tunnel Group Name, Regiony Device Type
- Haga clic en **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

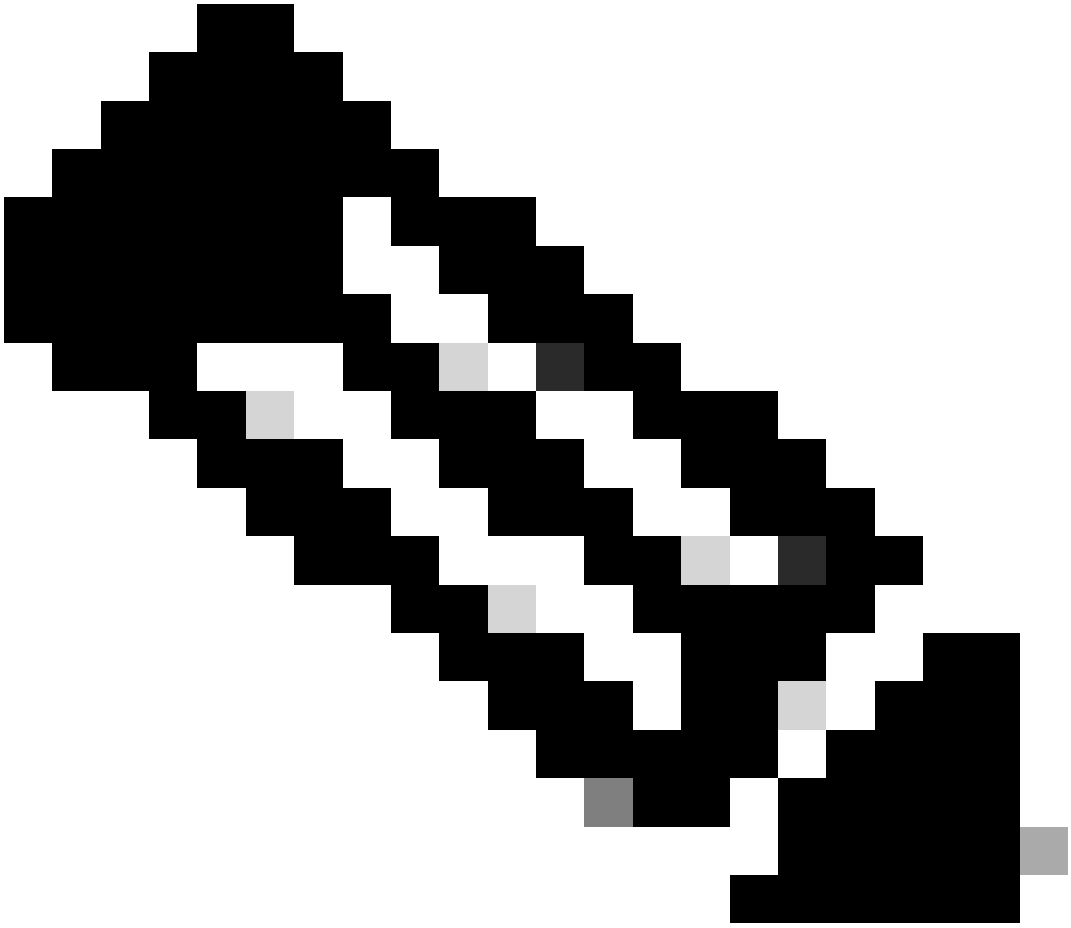
Europe (Germany)

Device Type

Other

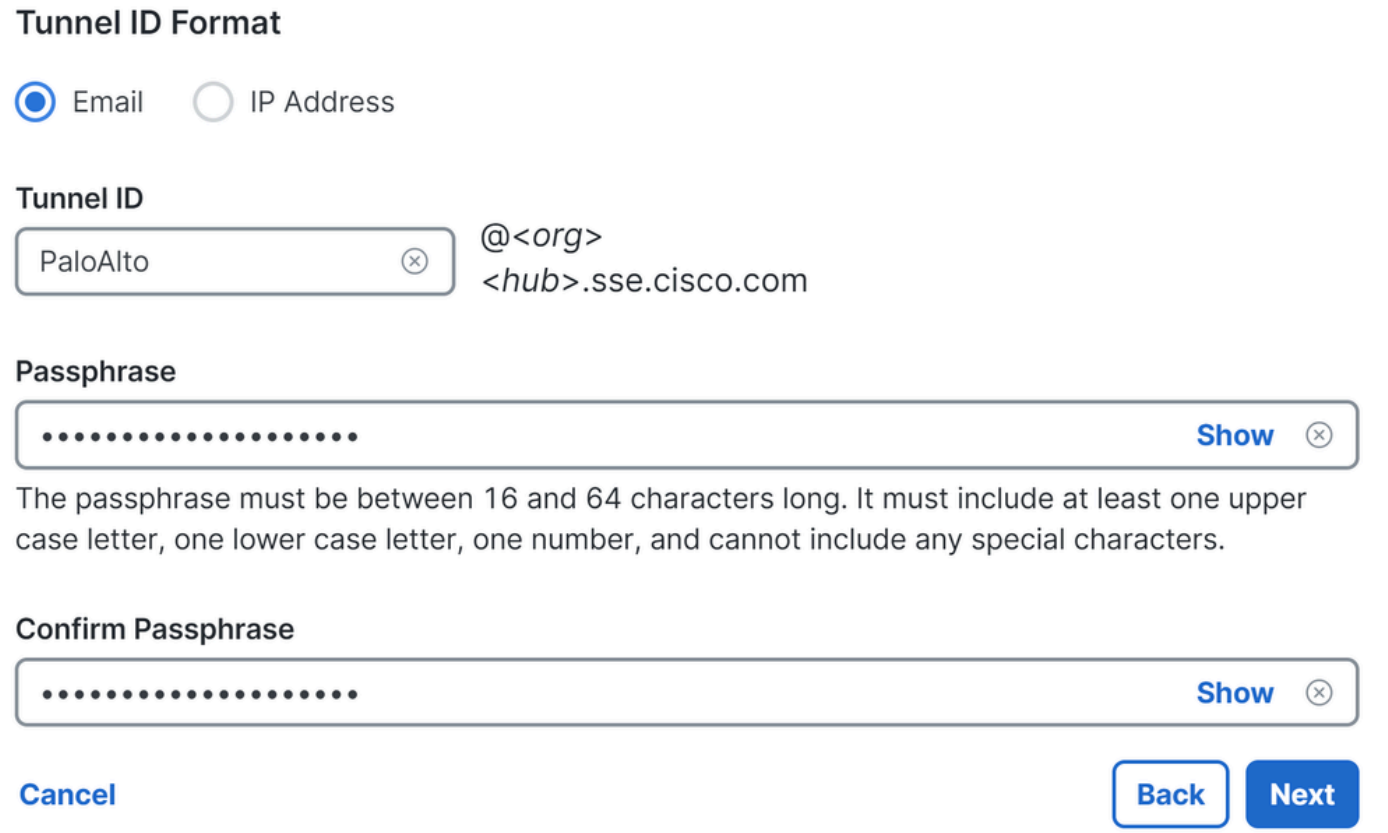
Cancel

Next



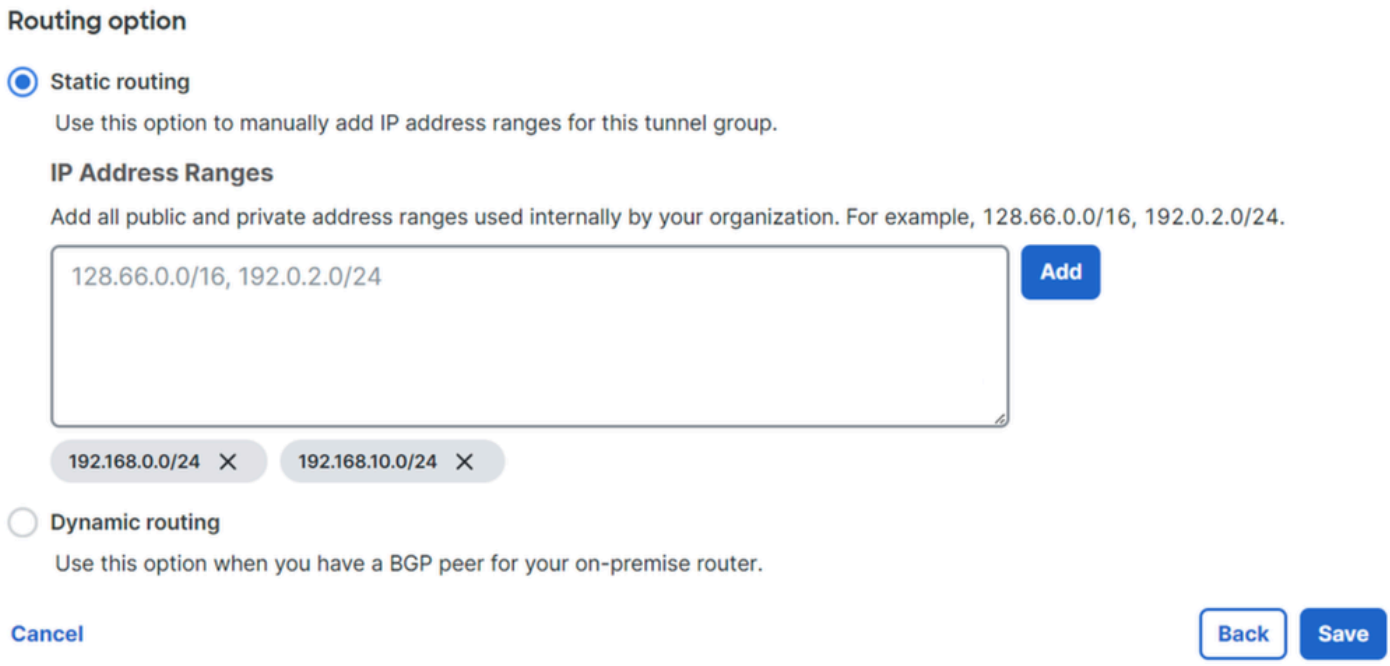
Nota: Seleccione la región más cercana a la ubicación del firewall.

- Configure el Tunnel ID Format y Passphrase
- Haga clic en Next



- Configure los rangos de direcciones IP o los hosts que ha configurado en la red y que desea que el tráfico pase a través de Secure Access

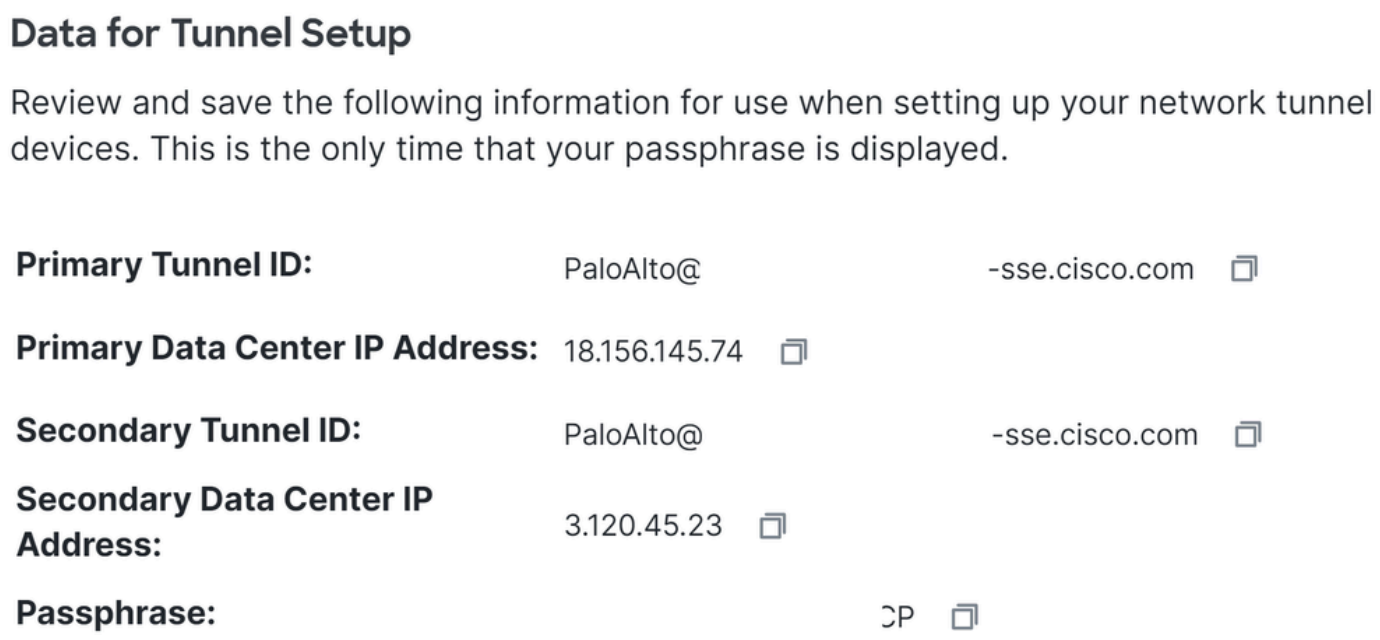
- Haga clic en **Save**



Acceso seguro - Grupos de túnel - Opciones de routing

Después de hacer clic en **Save** la información sobre el túnel se muestra, guarde esa información para el siguiente paso, **Configure the tunnel on Palo Alto**.

Datos del túnel

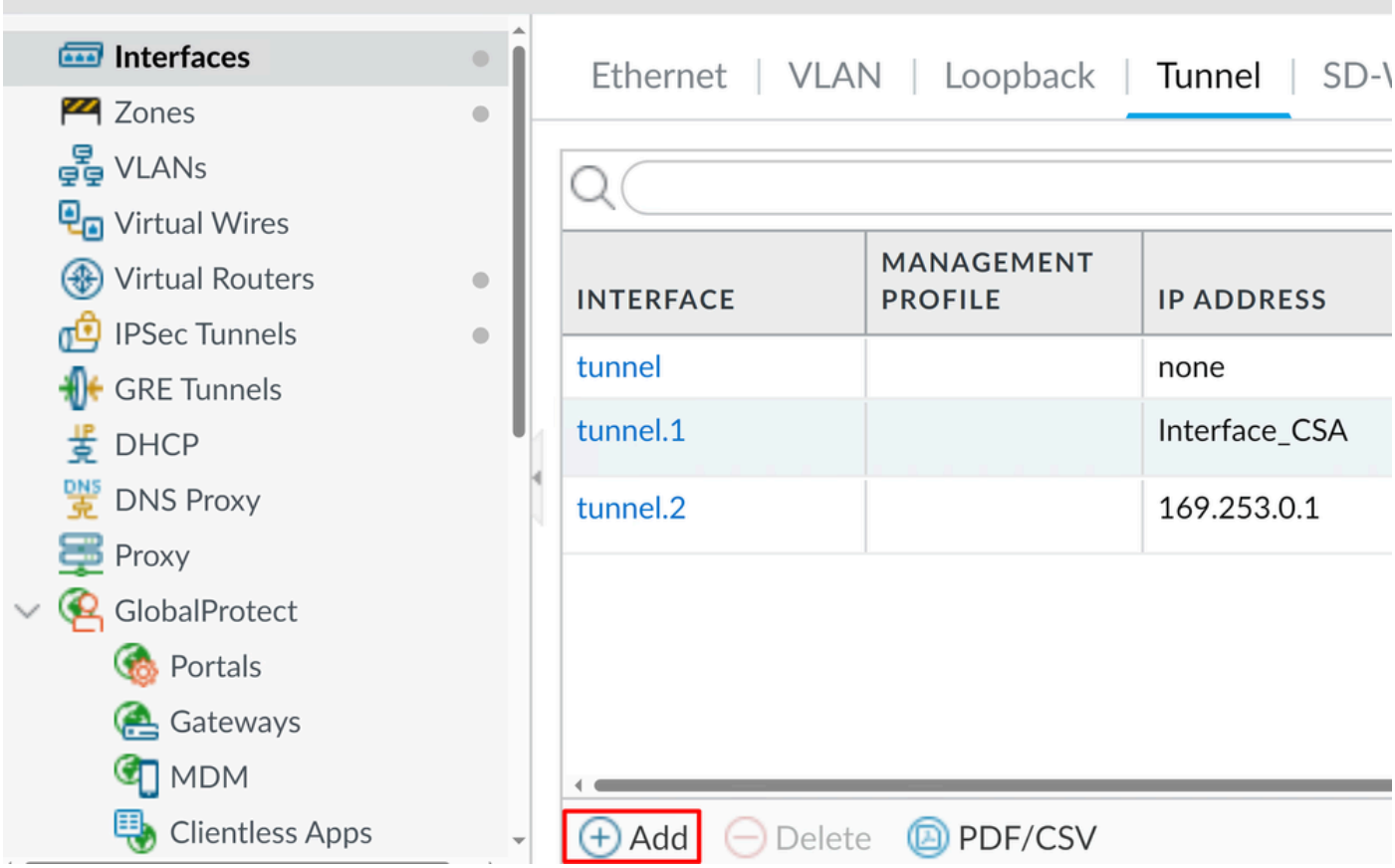


Configuración del túnel en Palo Alto

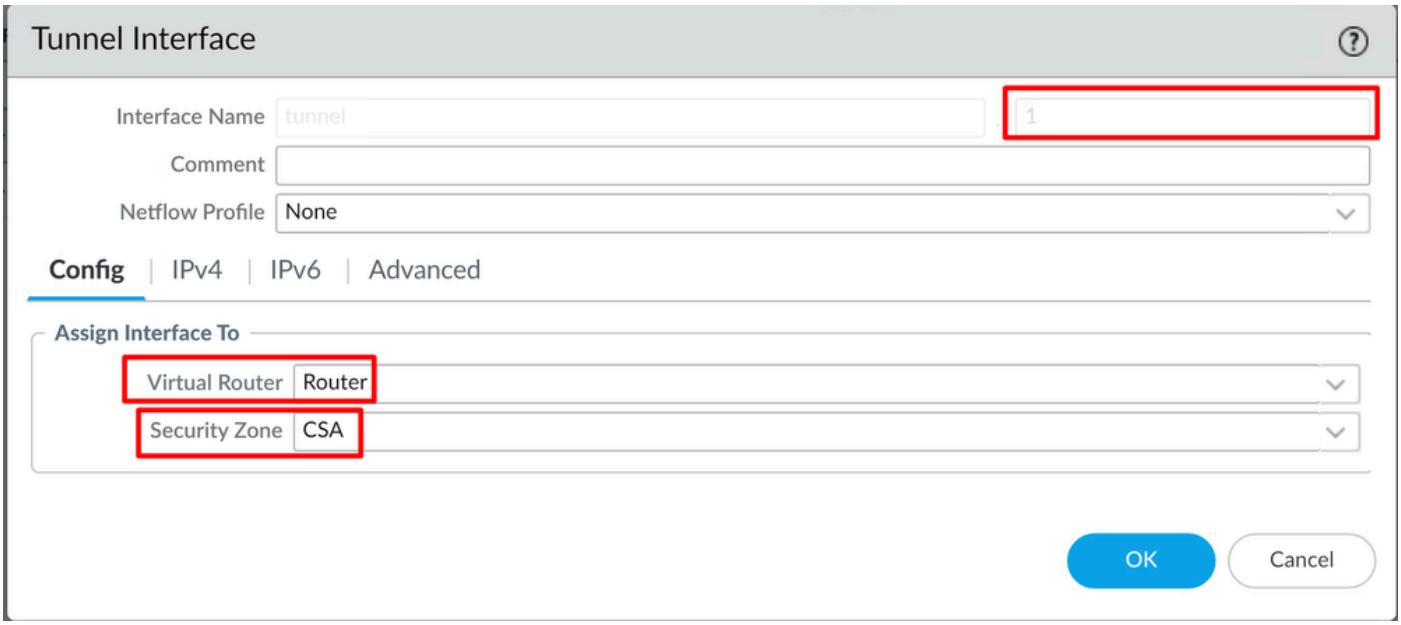
Configuración de la interfaz de túnel

Vaya al panel de Palo Alto.

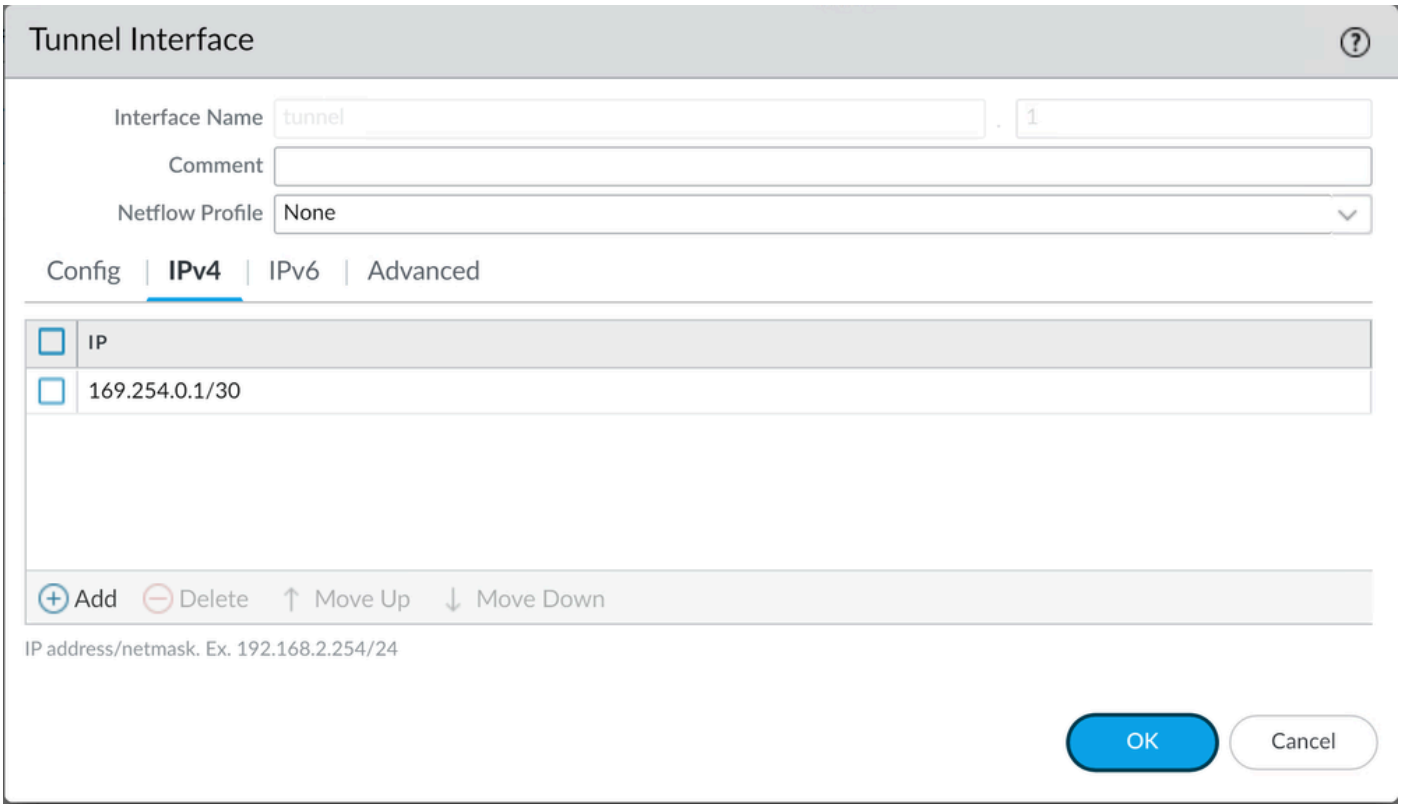
- Network > Interfaces > Tunnel
- Click Add



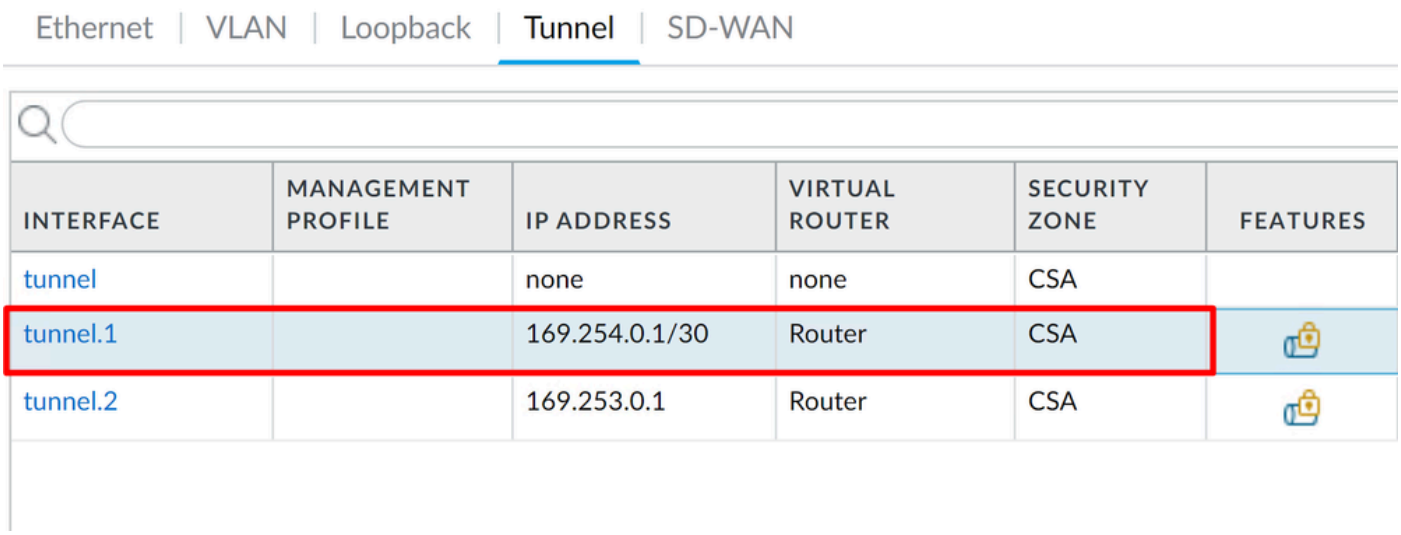
- En Config menú, configure el Virtual Router, Security Zone y asigne unSuffix Number



- En IPv4, configure una dirección IP no enrutable. Por ejemplo, puede utilizar 169.254.0.1/30
- Haga clic enOK



Después de eso, puede tener algo como esto configurado:

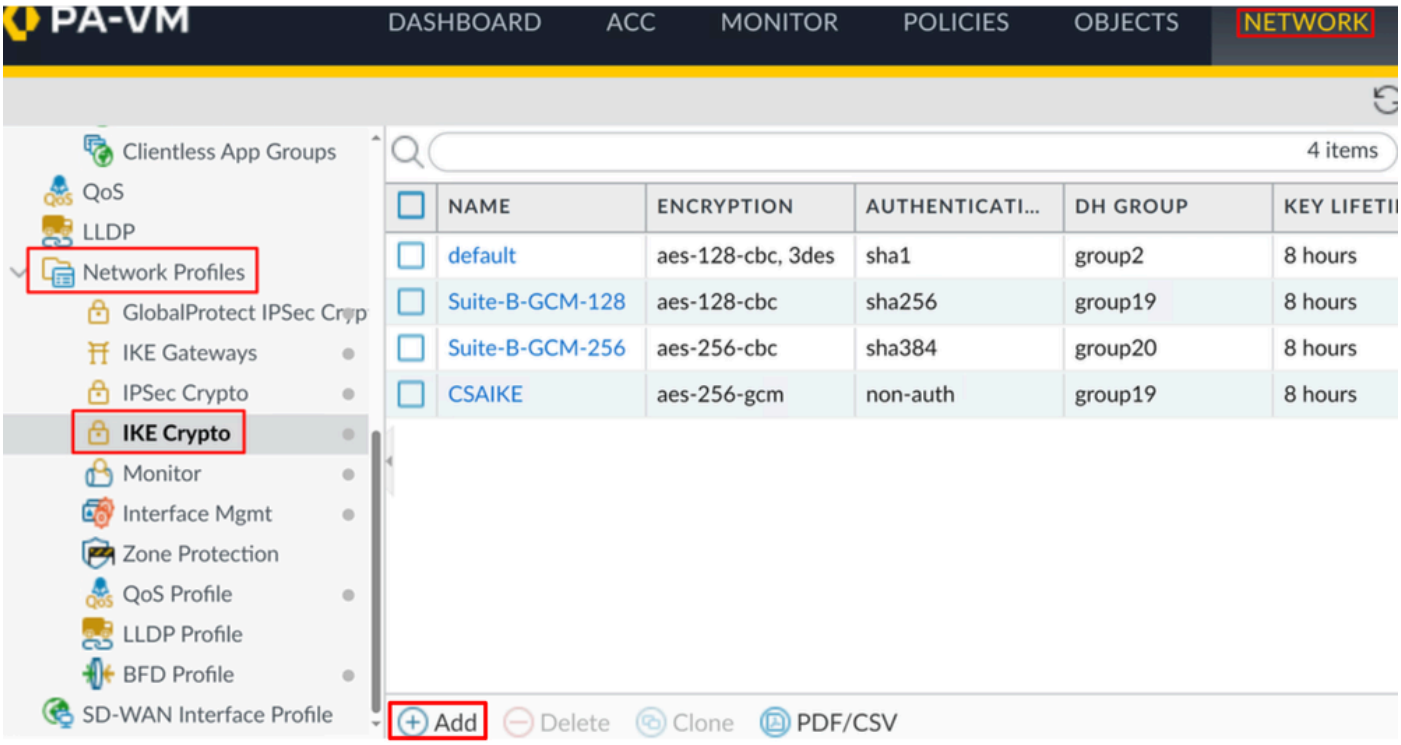


Si la tiene así configurada, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso, Configure IKE Crypto Profile.

Configurar perfil criptográfico IKE

Para configurar el perfil criptográfico, vaya a:

- Network > Network Profile > IKE Crypto
- Haga clic enAdd



- Configure los siguientes parámetros:

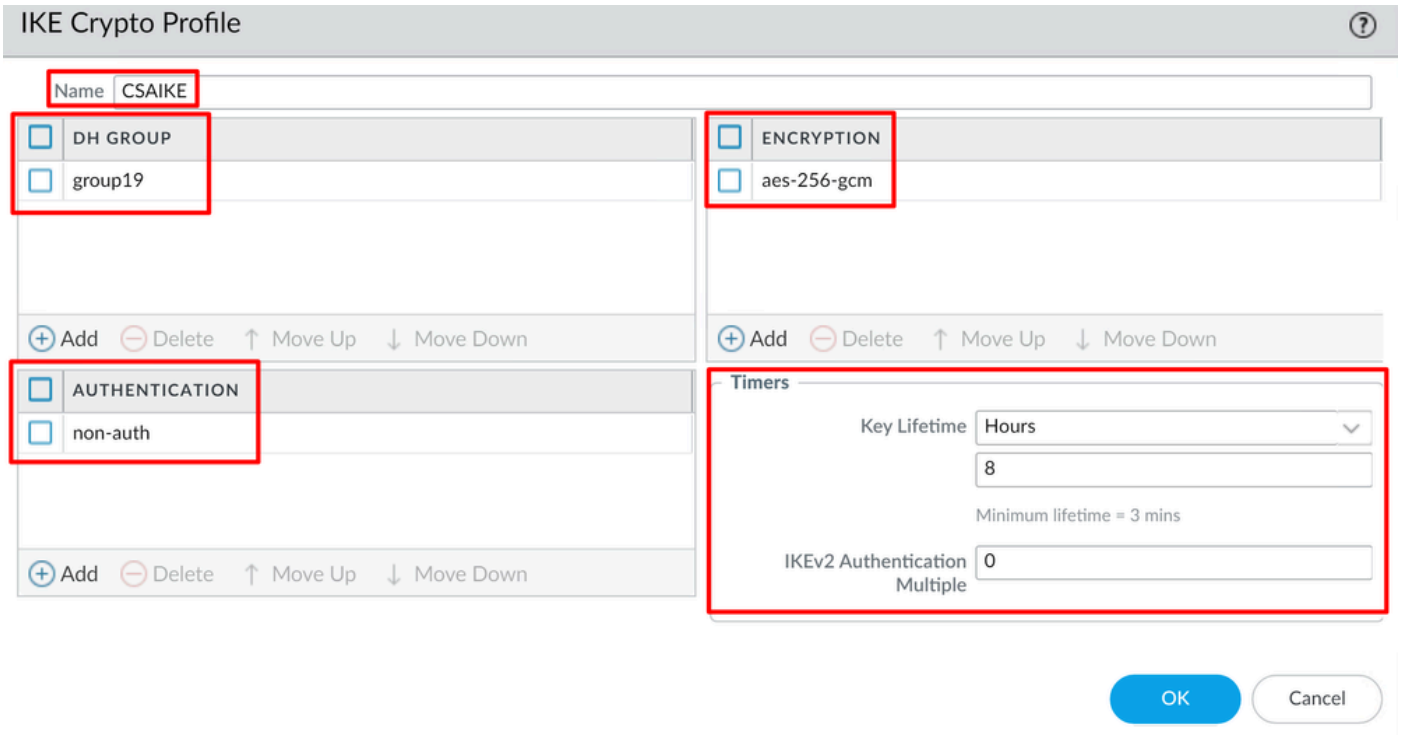
  - **Name**: configure un nombre para identificar el perfil.

    - **DH GROUP**: grupo19
    - **AUTHENTICATION**: sin autenticación
    - **ENCRYPTION**: aes-256-gcm
    - Timers

      - Key Lifetime: 8 horas

        - **IKEv2 Authentication**:0

- Una vez configurado todo, haga clic en **OK**

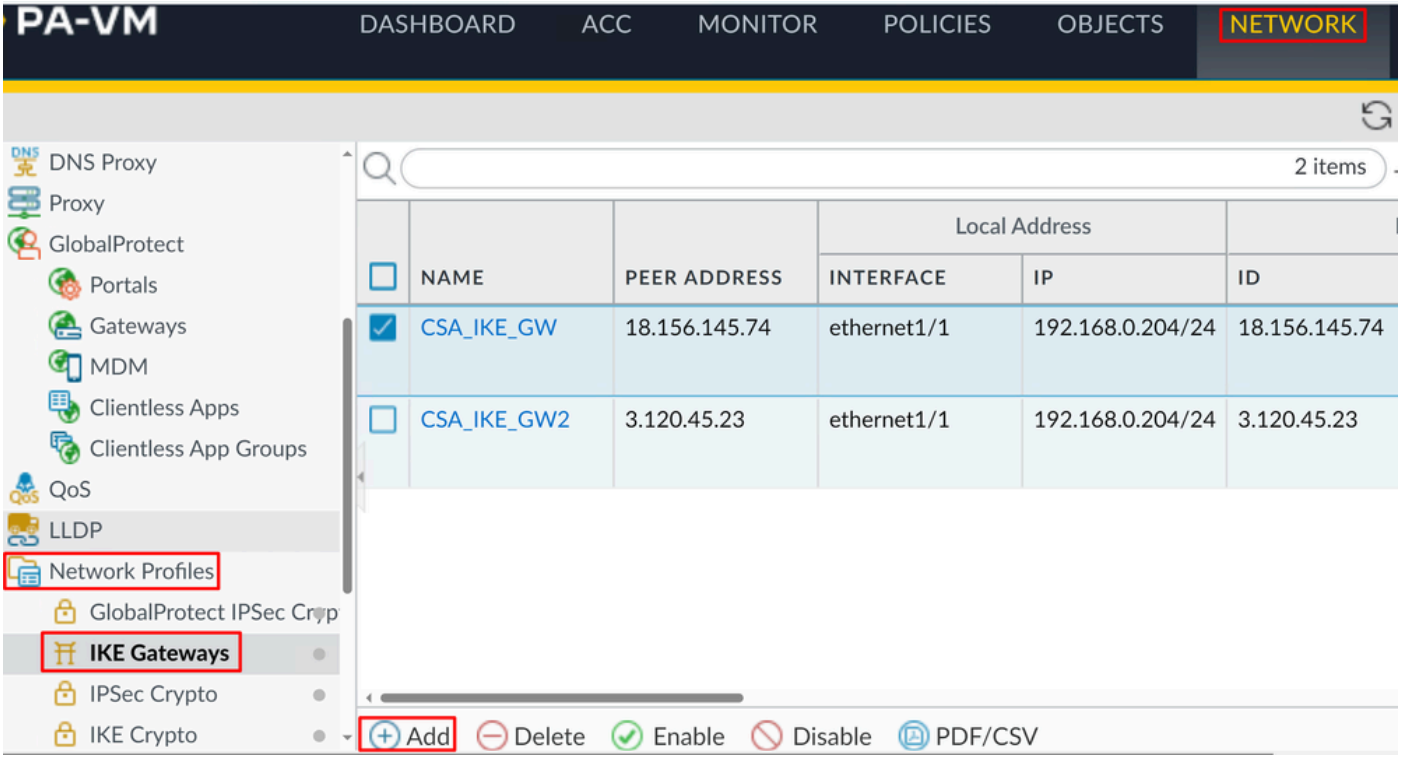


Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IKE Gateways.

Configuración de gateways IKE

Para configurar puertas de enlace IKE

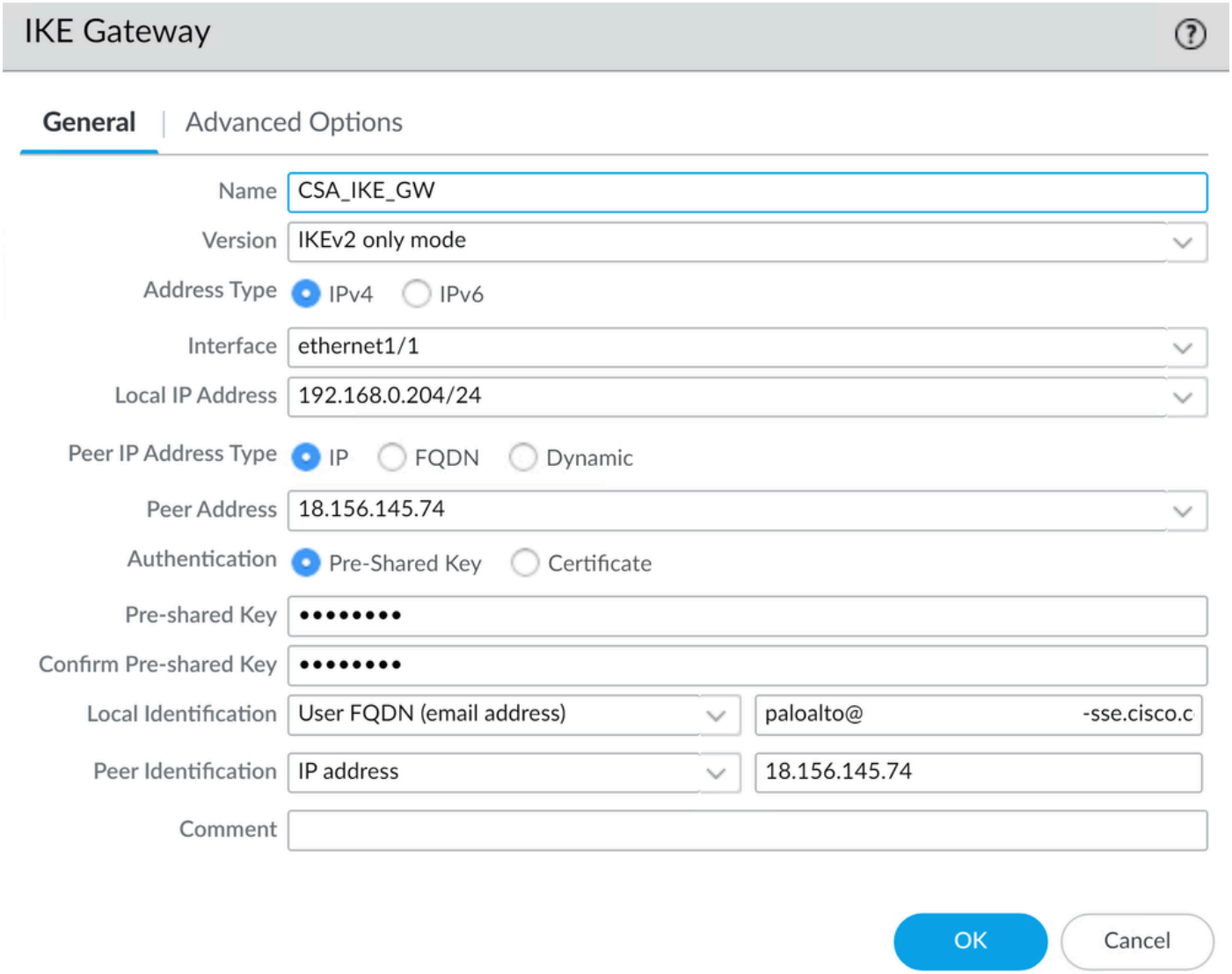
- Network > Network Profile > IKE Gateways
- Haga clic enAdd



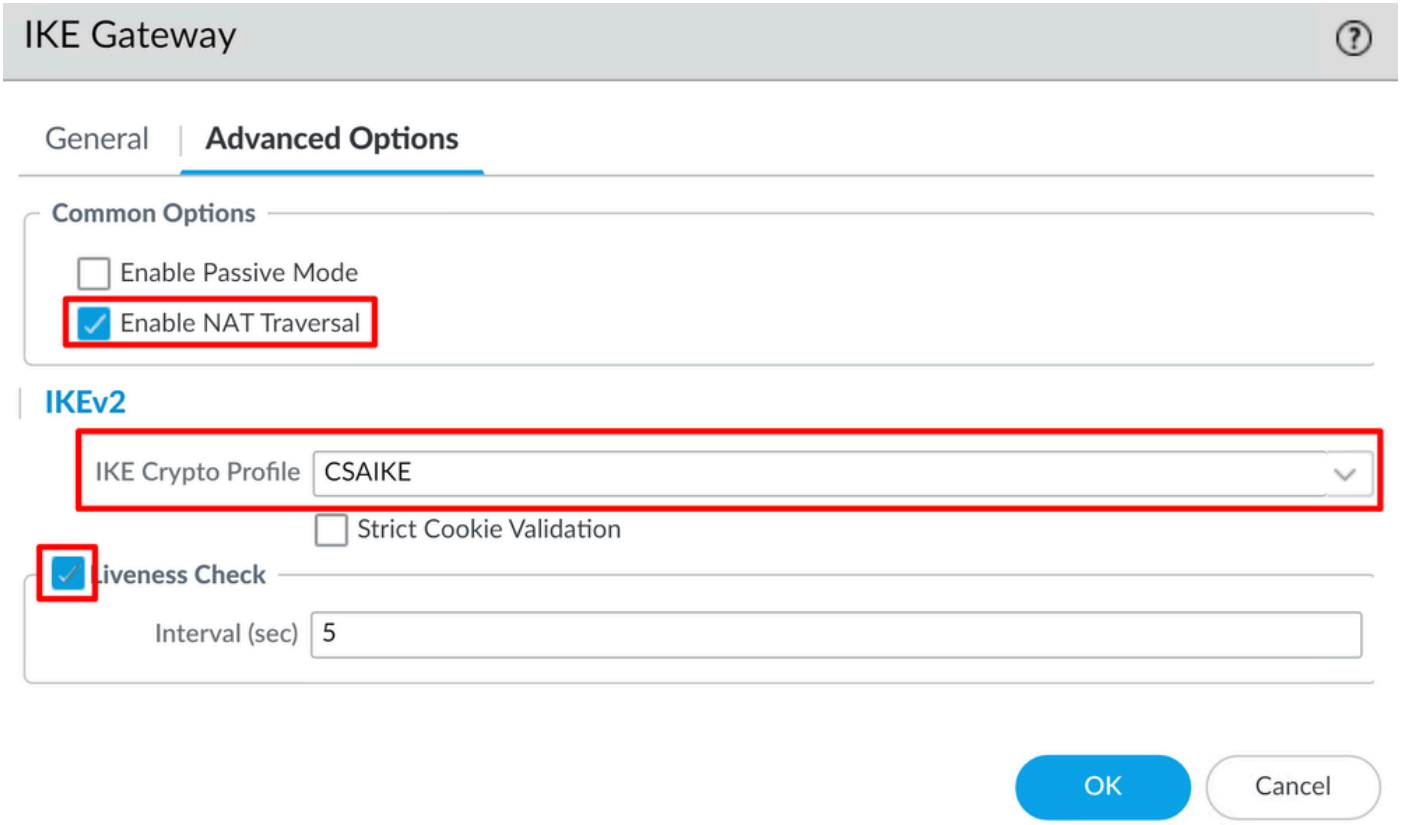
- Configure los siguientes parámetros:

    - Name: configure un nombre para identificar las puertas de enlace Ike.

        - **Version** : modo solo IKEv2
        - Address Type :IPv4
        - **Interface** : seleccione la interfaz WAN de Internet.
        - Local IP Address: seleccione la IP de la interfaz WAN de Internet.
        - **Peer IP Address Type** :IP
        - Peer Address: Utilice la dirección IP de Primary IP Datacenter IP Address, indicada en el paso Tunnel Data.
        - Authentication: clave precompartida
        - Pre-shared Key : Utilice el **passphrase** especificado en el paso Tunnel Data.
        - **Confirm Pre-shared Key** : Utilice el **passphrase** especificado en el paso Tunnel Data.
        - **Local Identification** : Elija **User FQDN (Email address)** y utilice el **Primary Tunnel ID** dato del paso, Tunnel Data.
        - **Peer Identification** : IP AddressElija y utilice el Primary IP Datacenter IP Address.



- Haga clic enAdvanced Options
    - **Enable NAT Traversal**
        - Seleccione el perfil **IKE Crypto Profile** creado en el paso Configure IKE Crypto Profile
        - Marque la casilla de verificación de **Liveness Check**
        - Haga clic en **OK**

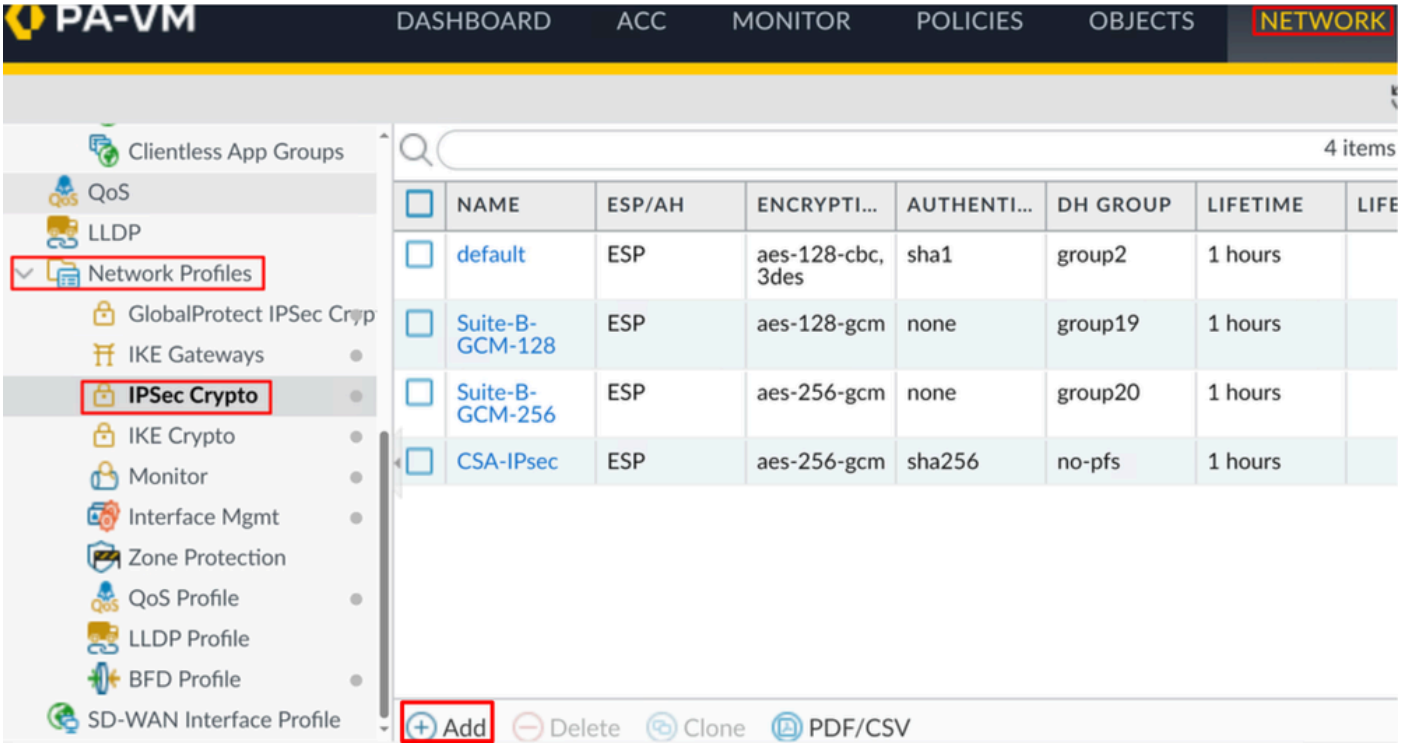


Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IPSEC Crypto.

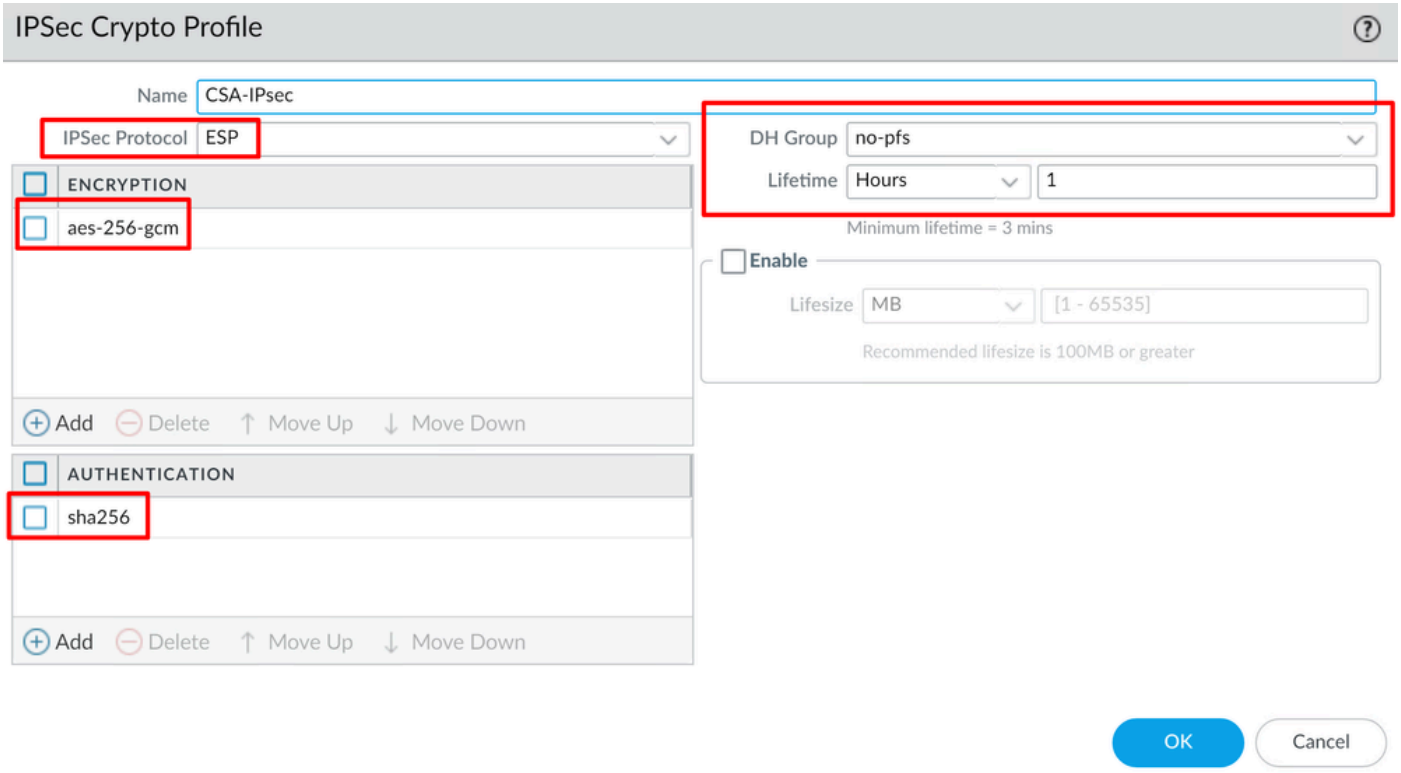
Configurar perfil criptográfico IPSEC

Para configurar puertas de enlace IKE, vaya a Network > Network Profile > IPSEC Crypto

- Haga clic enAdd



- Configure los siguientes parámetros:
    - **Name**: utilice un nombre para identificar el perfil IPSec de acceso seguro
        - IPSec Protocol: ESP
        - **ENCRYPTION**: aes-256-gcm
        - DH Group: no-pfs, 1 hora
- Haga clic en OK

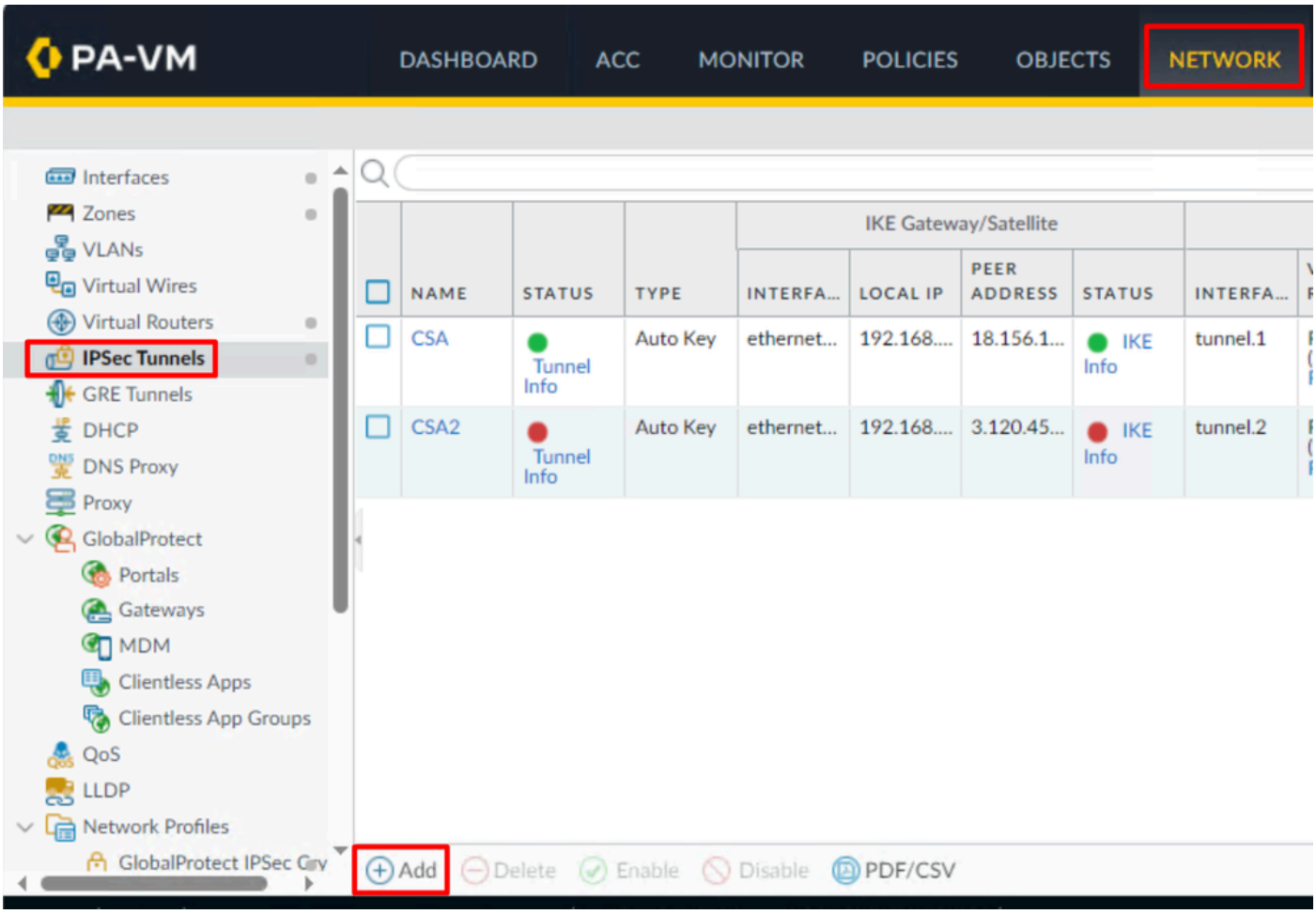


Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IPSec Tunnels.

Configuración de túneles IPSec

Para configurar **IPSec Tunnels**, vaya a Network > IPSec Tunnels.

- Haga clic en Add



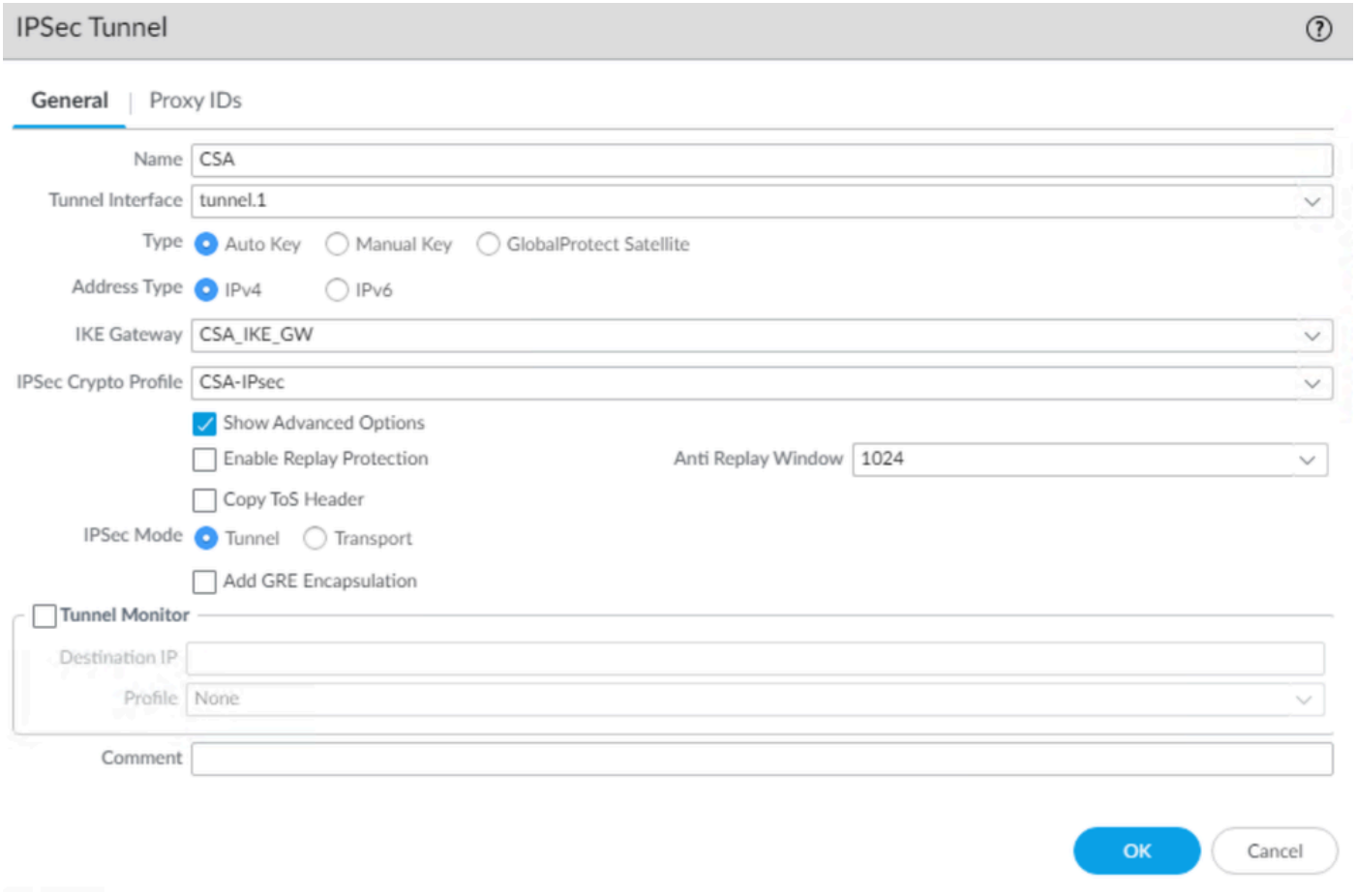
- Configure los siguientes parámetros:

  - **Name**: utilice un nombre para identificar el túnel de acceso seguro

    - **Tunnel Interface**: Seleccione la interfaz de túnel configurada en el paso Configurar la interfaz de túnel.
    - **Type**: Clave automática
    - **Address Type**:IPv4
    - **IKE Gateways**: Seleccione las puertas de enlace IKE configuradas en el paso Configure IKE Gateways.
    - **IPsec Crypto Profile**: Seleccione las puertas de enlace IKE configuradas en el paso Configure IPSEC Crypto Profile
    - Marque la casilla de verificación de **Advanced Options**

      - **IPSec Mode Tunnel**: seleccione Túnel.

- Haga clic en OK

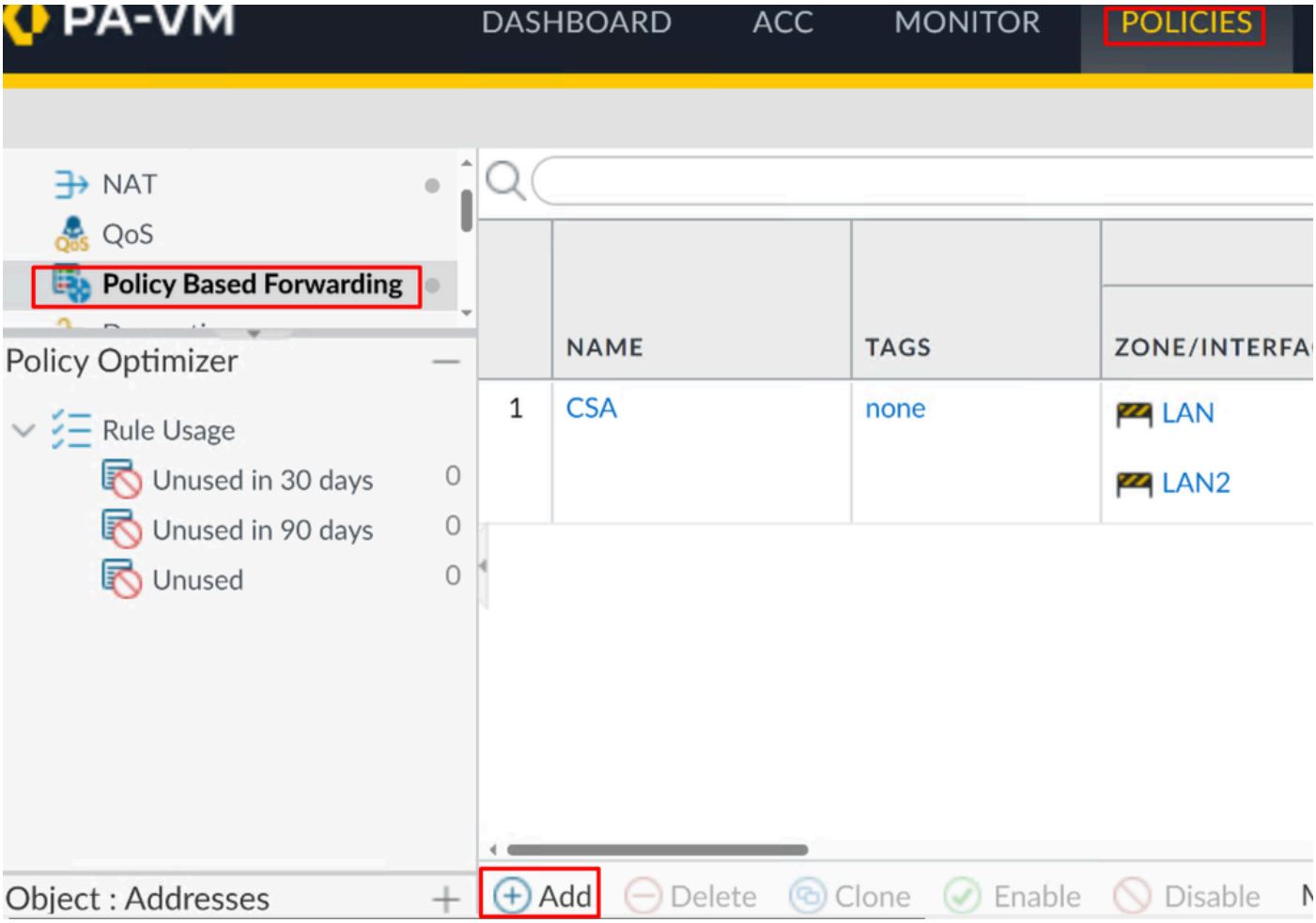


Ahora que la VPN se ha creado correctamente, puede continuar con el paso **Configure Policy Based Forwarding**.

Configurar el reenvío basado en políticas

Para configurar **Policy Based Forwarding**, vaya a Policies > Policy Based Forwarding.

- Haga clic en Add



- Configure los siguientes parámetros:
    - General
        - **Name**: utilice un nombre para identificar el acceso seguro, el reenvío de base de políticas (routing por origen)
- Source
    - **Zone**: seleccione las zonas desde las que tiene planes para enrutar el tráfico en función del origen
        - **Source Address**: configure el host o las redes que desea utilizar como origen.
        - Source Users: configure los usuarios a los que desea enrutar el tráfico (sólo si procede).

- Destination/Application/Service

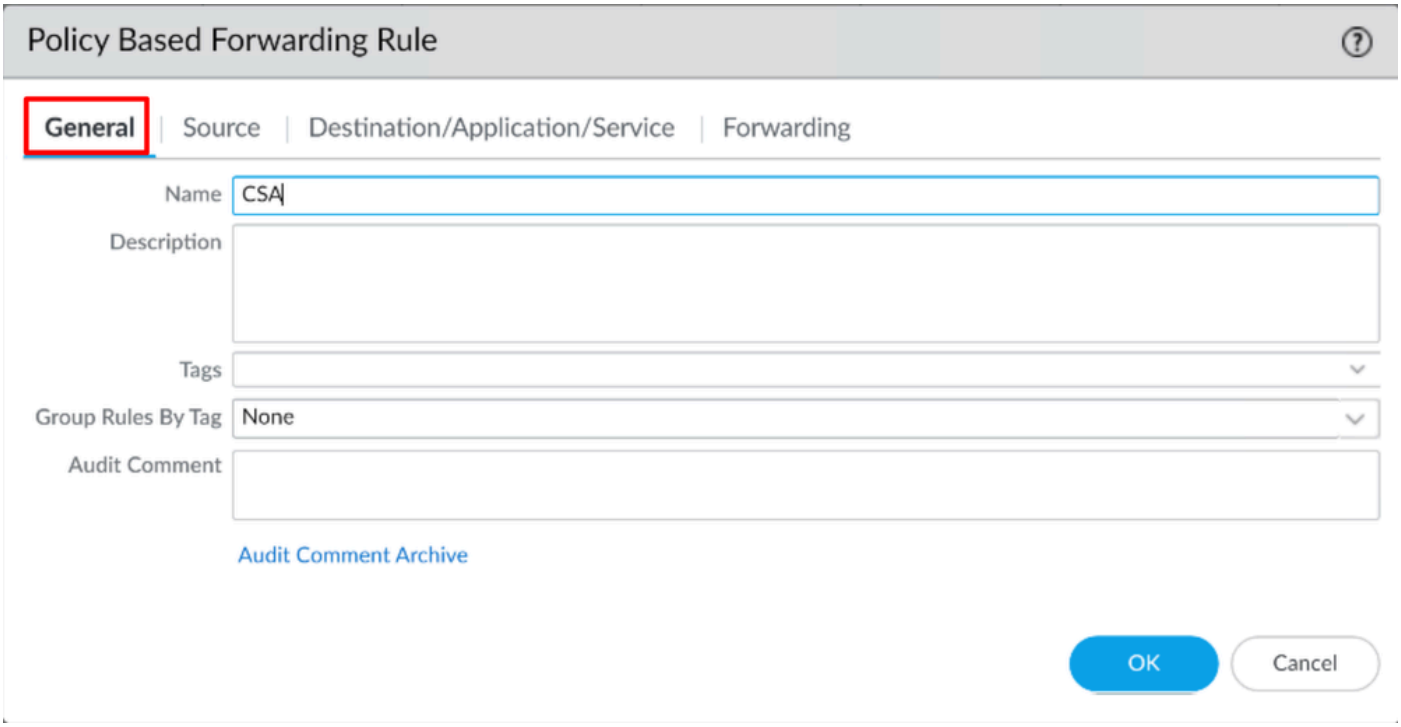
  - Destination Address: puede dejarlo como Any (Cualquiera) o puede especificar los intervalos de direcciones de Secure Access (100.64.0.0/10)

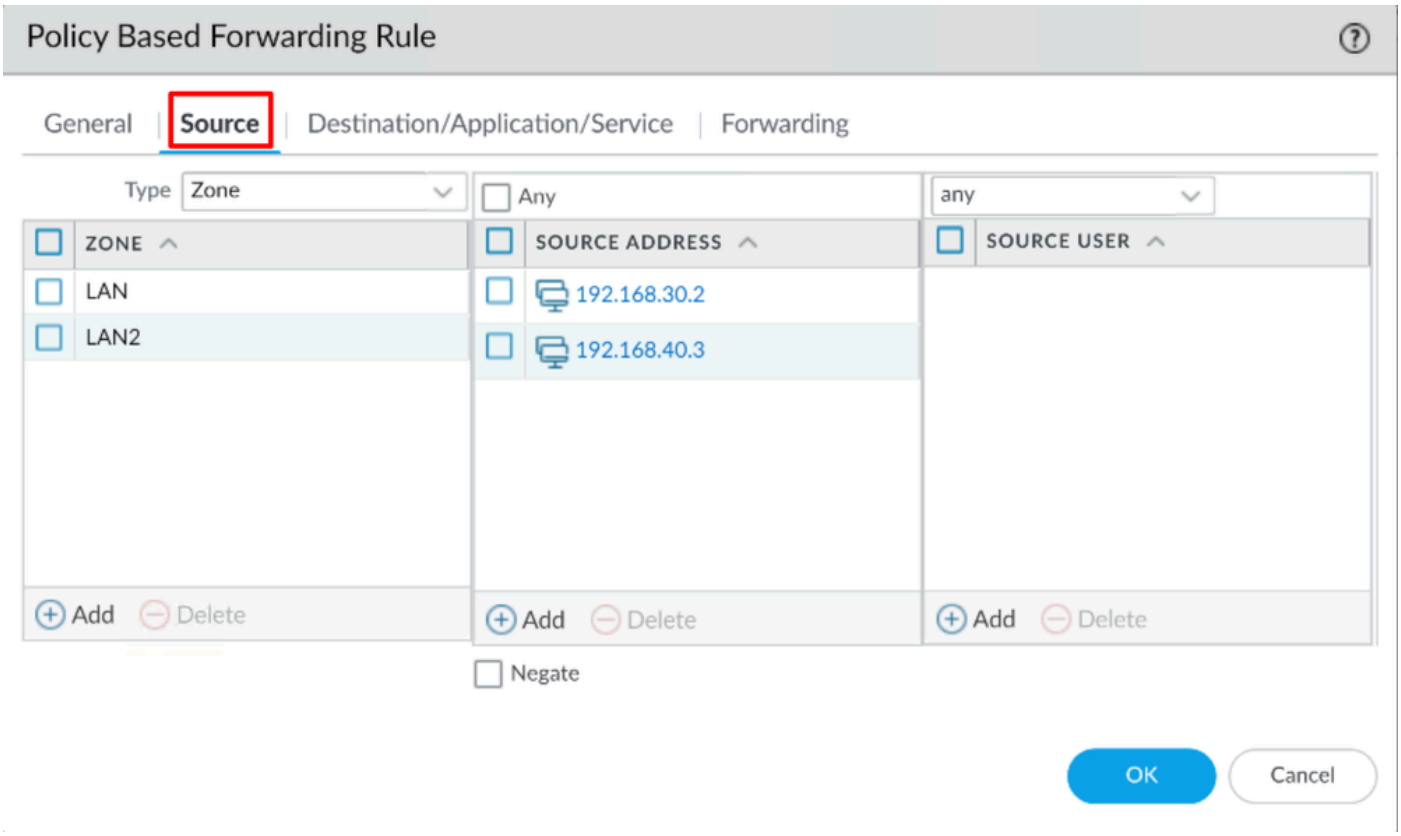
- Forwarding

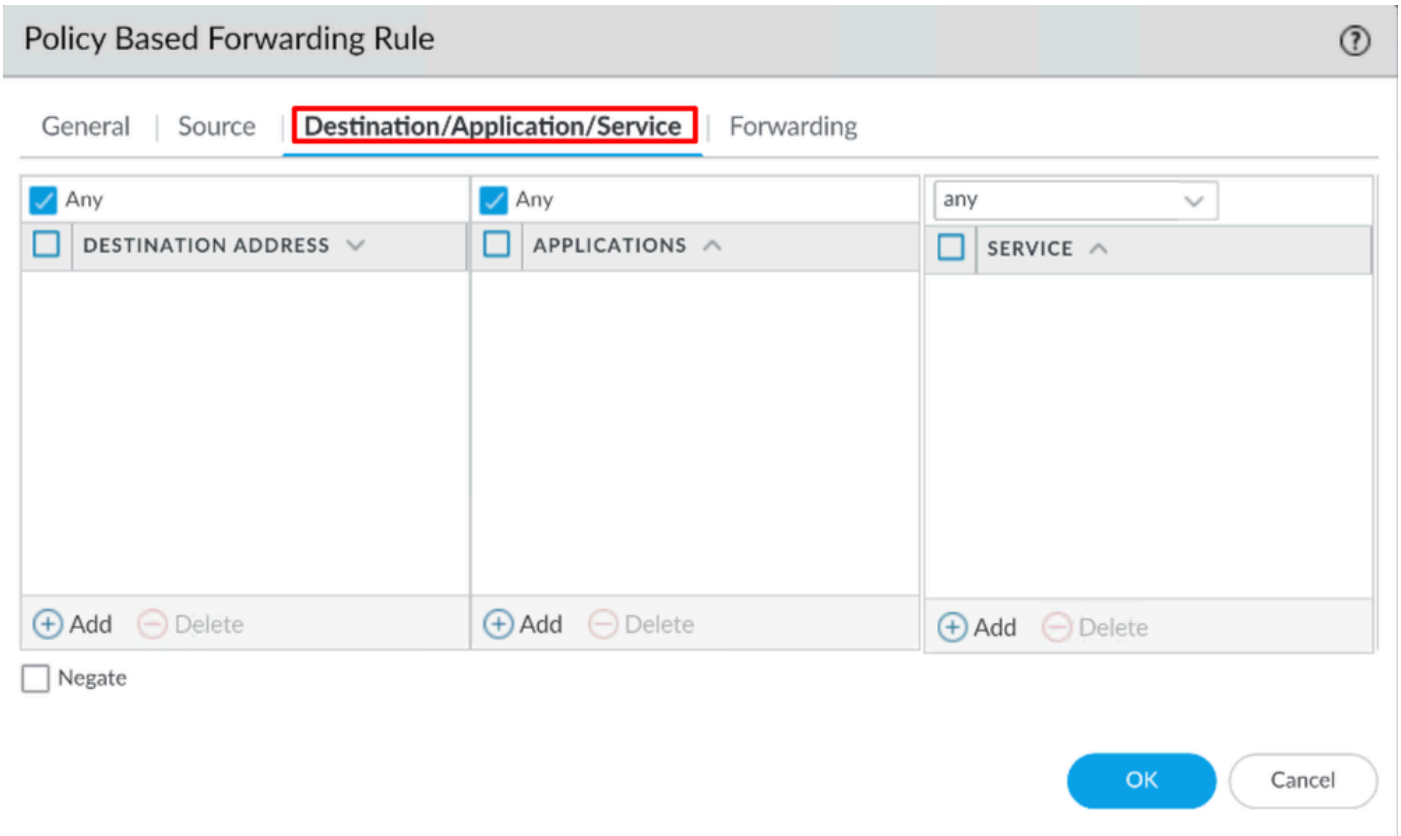
  - **Action**:Reenvío

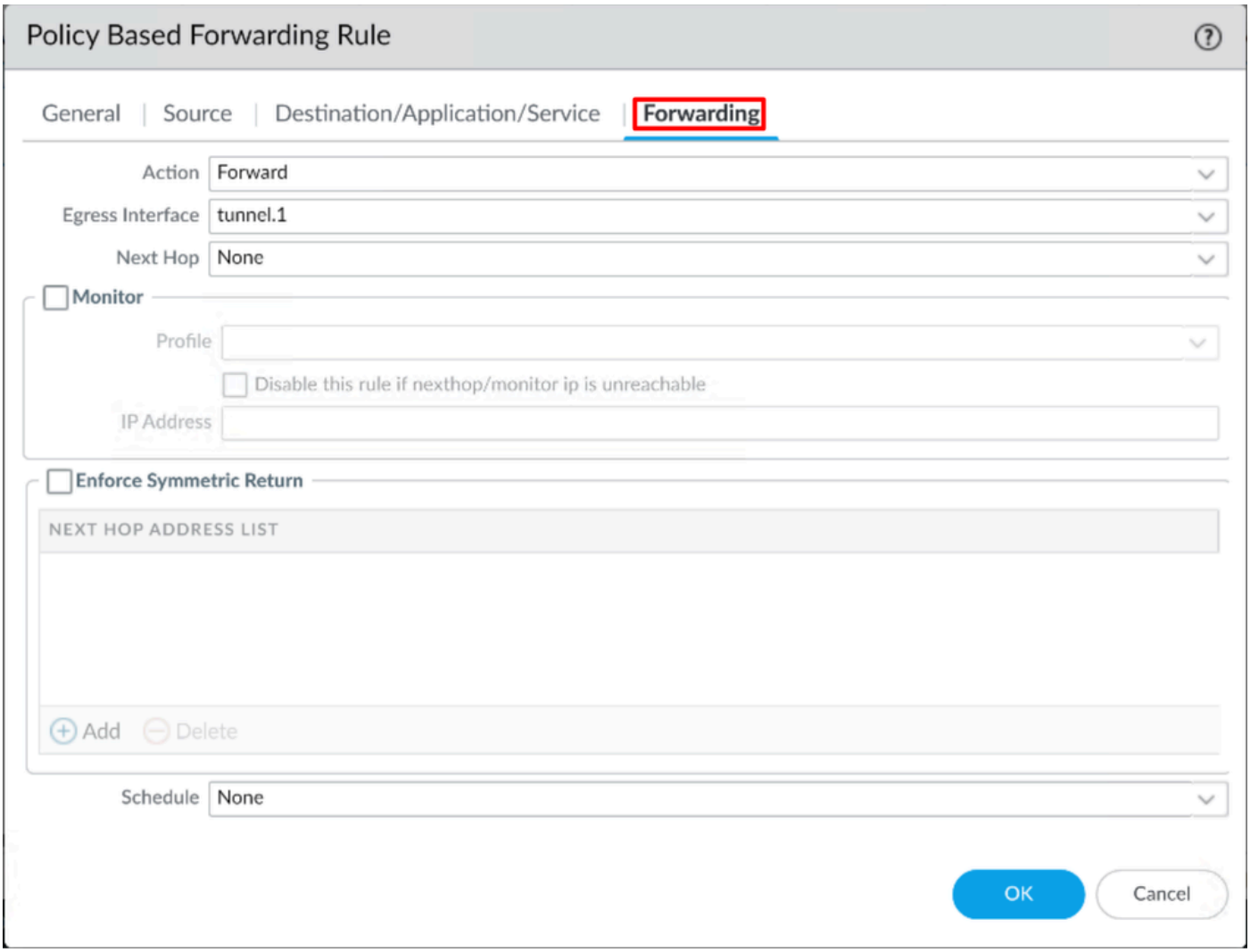
    - **Egress Interface**: Seleccione la interfaz de túnel configurada en el paso Configurar la interfaz de túnel.
    - **Next Hop**:Ninguno

- HagaOK clic y 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



Ahora tiene todo configurado en Palo Alto; después de configurar la ruta, se puede establecer el túnel y debe continuar configurando RA-VPN, ZTA basado en navegador o ZTA base de cliente en el panel de acceso seguro.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).