Configure o acesso seguro com o firewall Palo Alto

Contents

Introdução

Este documento descreve como configurar o acesso seguro com o firewall Palo Alto.

Pré-requisitos

- Configurar Provisionamento de Usuário
- Configuração de Autenticação ZTNA SSO
- Configurar o acesso seguro da VPN de acesso remoto

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall da versão Palo Alto 11.x
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

Componentes Utilizados

As informações neste documento são baseadas em:

- Firewall da versão Palo Alto 11.x
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Cisco projetou o Secure Access para proteger e fornecer acesso a aplicativos privados, no local e baseados em nuvem. Ele também protege a conexão da rede à Internet. Isso é obtido por meio da implementação de vários métodos e camadas de segurança, todos voltados para preservar as informações à medida que elas são acessadas pela nuvem.

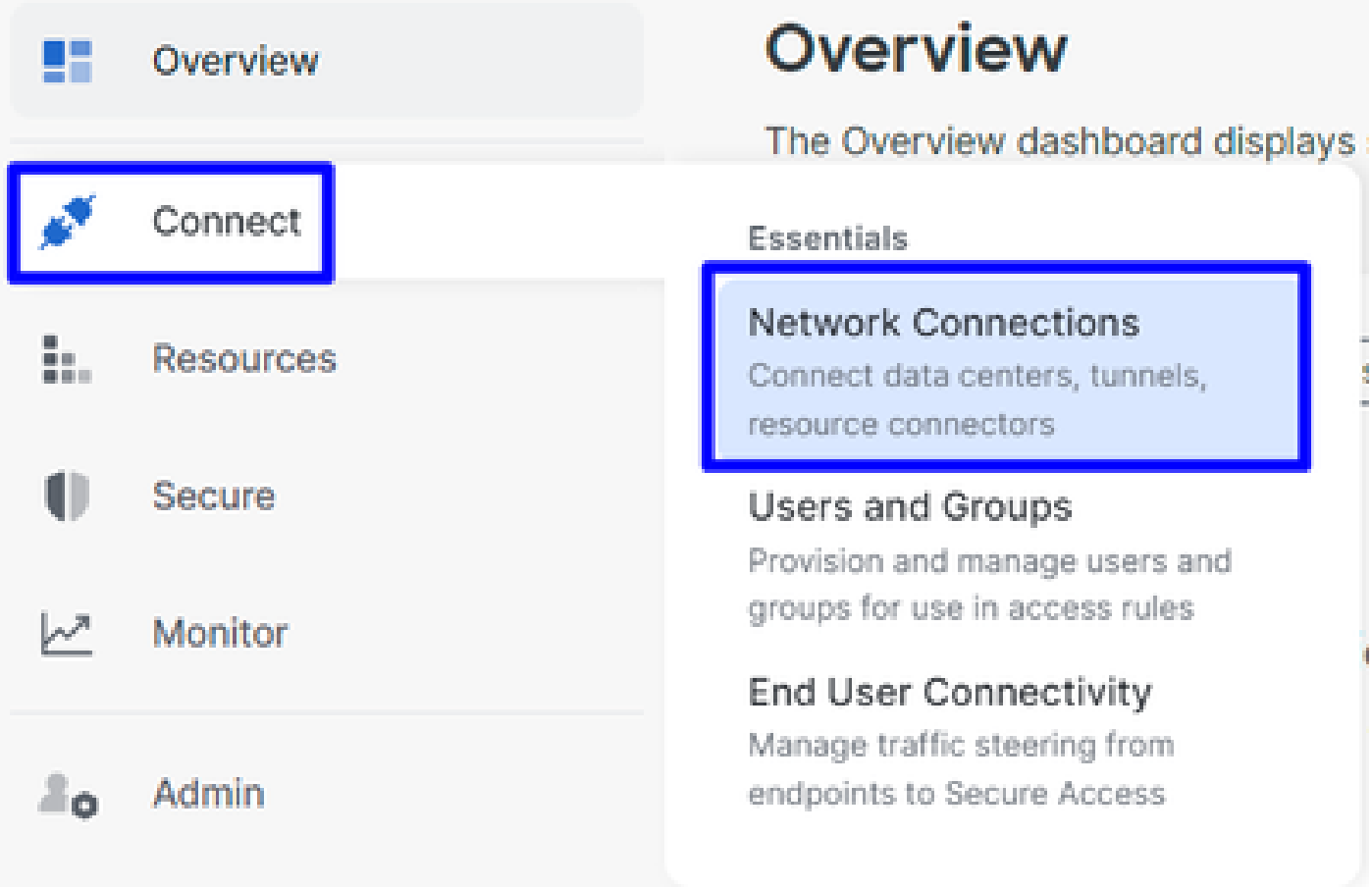
Configurar

Configurar a VPN no acesso seguro

Navegue até o painel de administração do Secure Access.

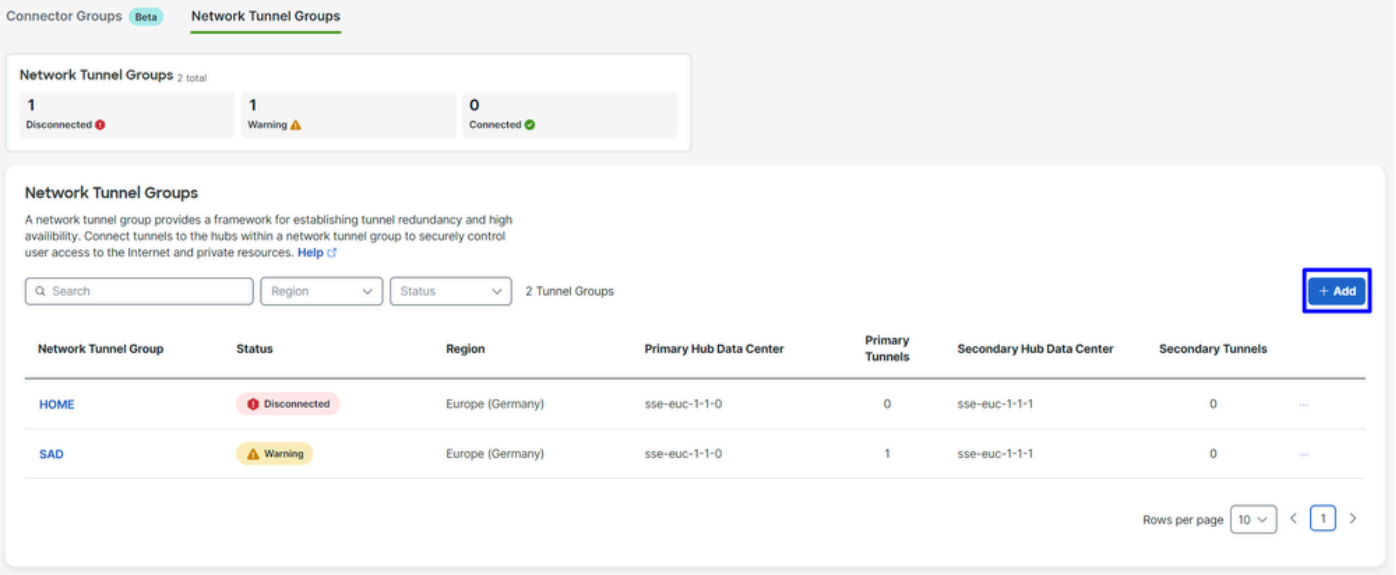
Acesso seguro - Página principal

- Clique em Connect > Network Connections



Acesso seguro - Conexões de rede

- Em Network Tunnel Groups clique em + Add



Acesso seguro - Grupos de túnel de rede

- Configure Tunnel Group Name, Region e Device Type
- Clique em **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

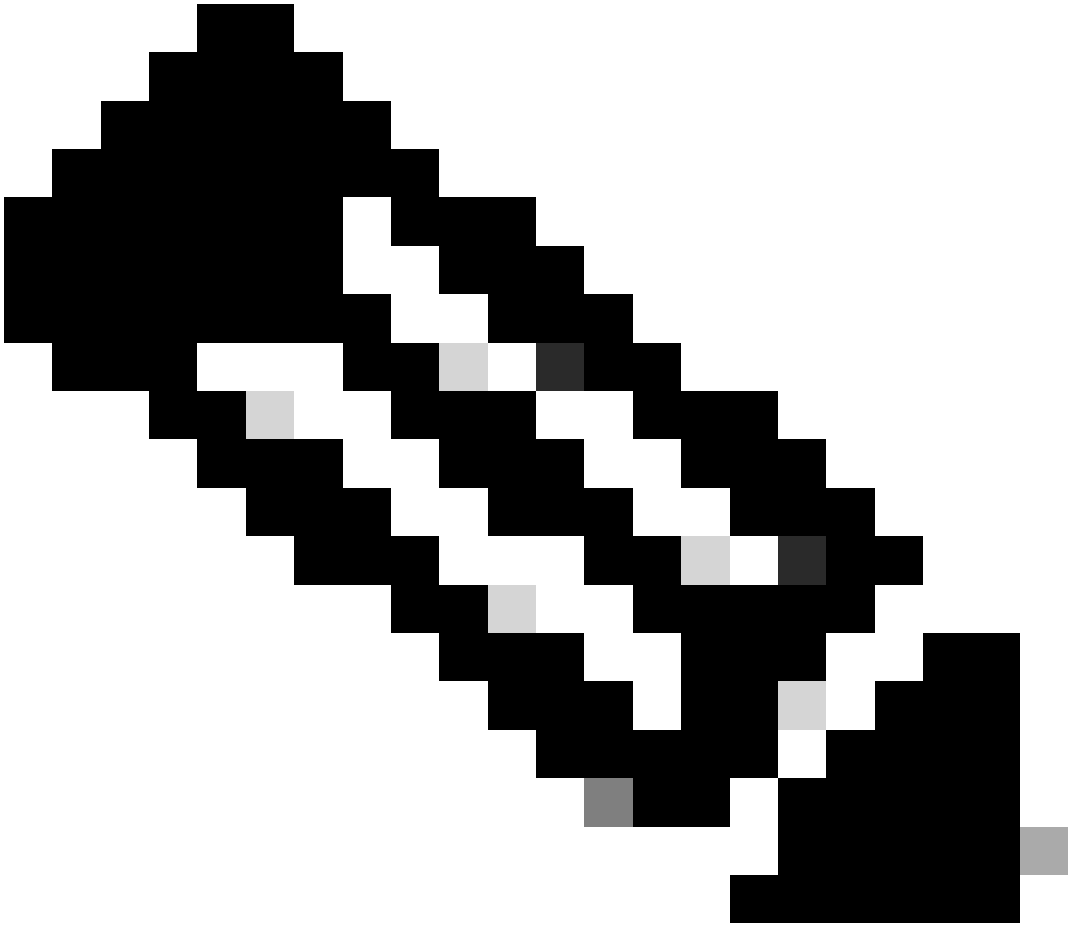
Europe (Germany)

Device Type

Other

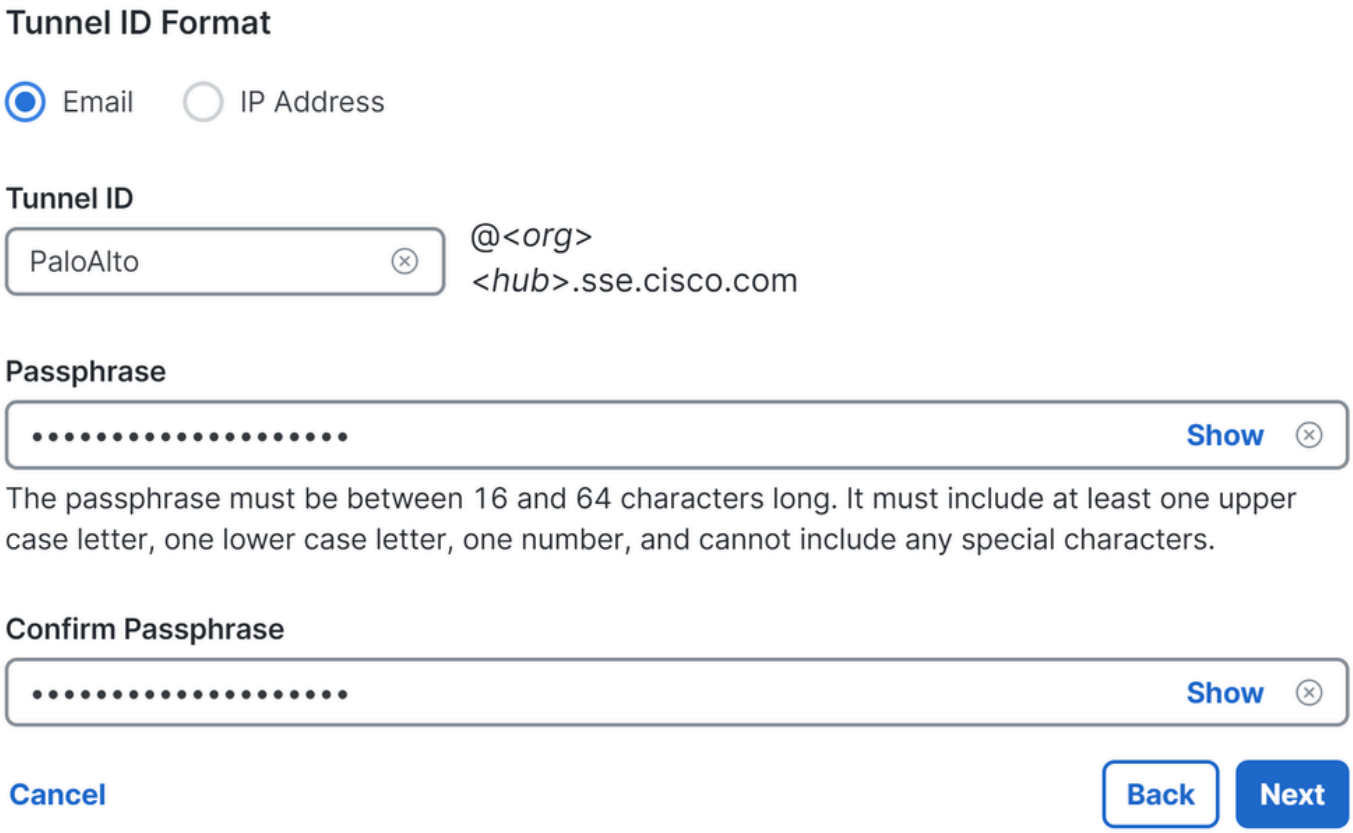
Cancel

Next

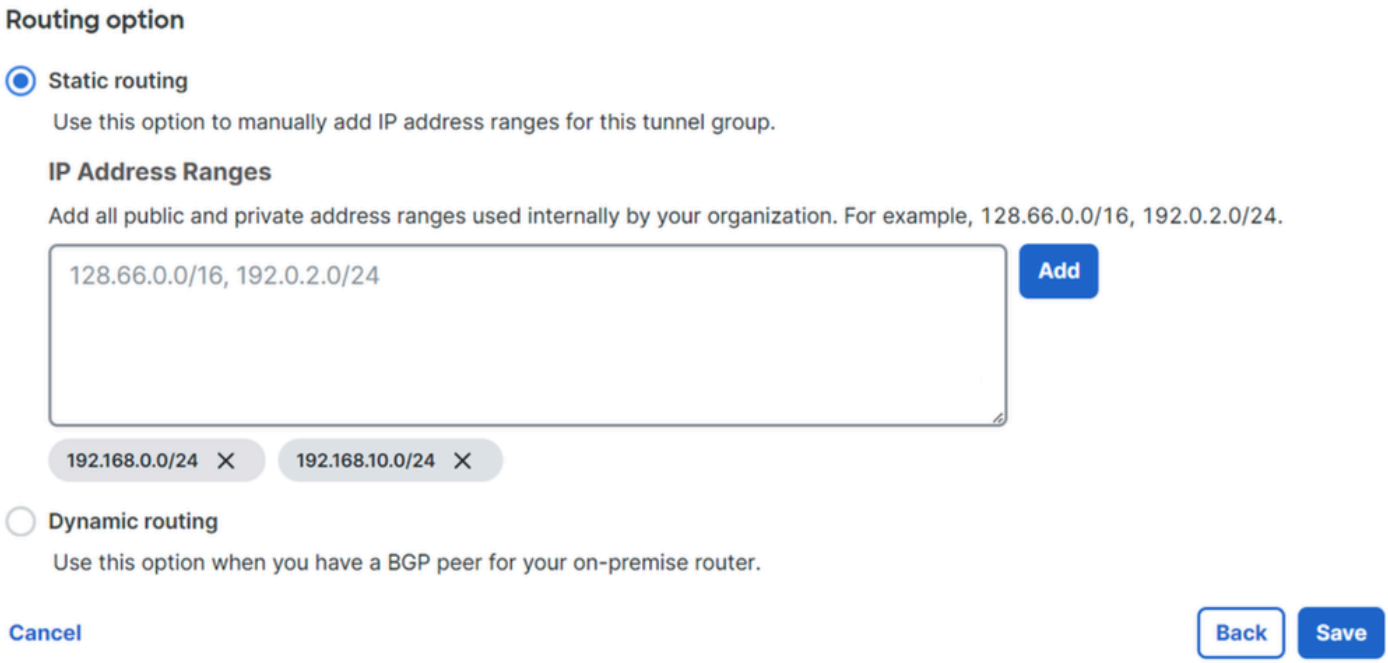


Observação: escolha a região mais próxima ao local do firewall.

- Configure o Tunnel ID Format e Passphrase
- Clique em Next



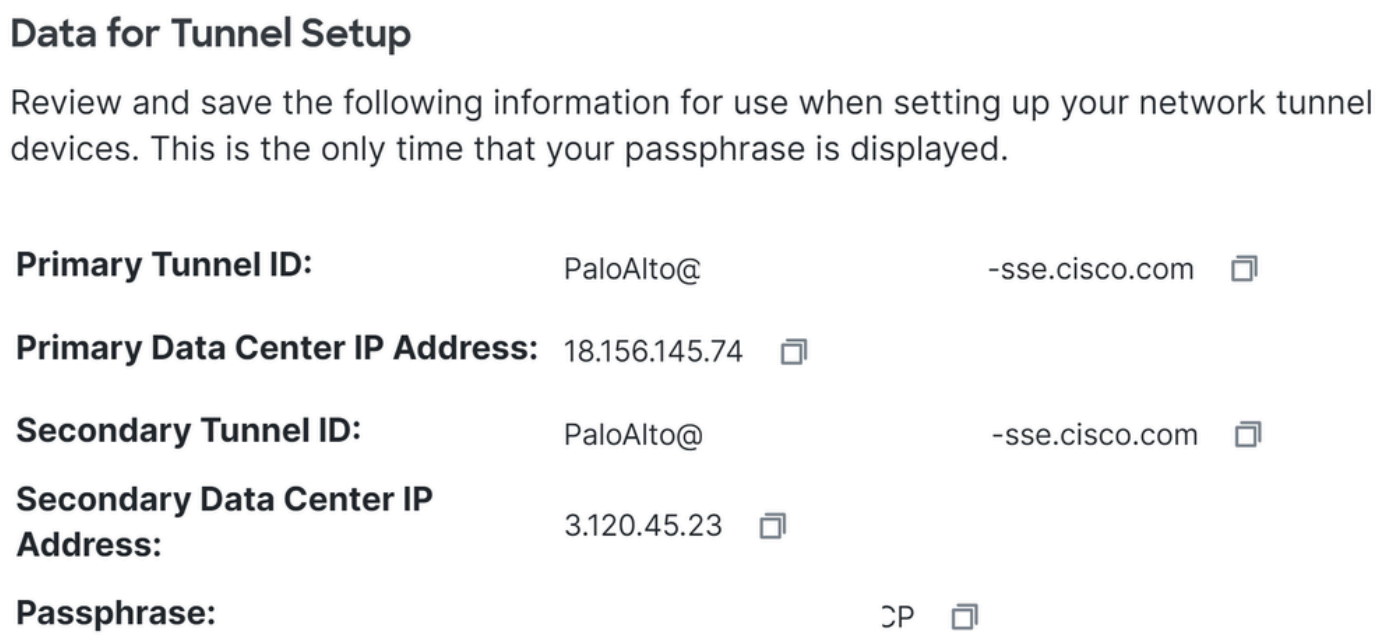
- Configure os intervalos de endereços IP ou hosts que você configurou na sua rede e deseja passar o tráfego pelo Secure Access
- Clique em **Save**



Acesso seguro - Grupos de túneis - Opções de roteamento

Depois de clicar nas informações sobre **Save** o túnel que são exibidas, salve essas informações para a próxima etapa, **Configure the tunnel on Palo Alto**.

Dados do túnel

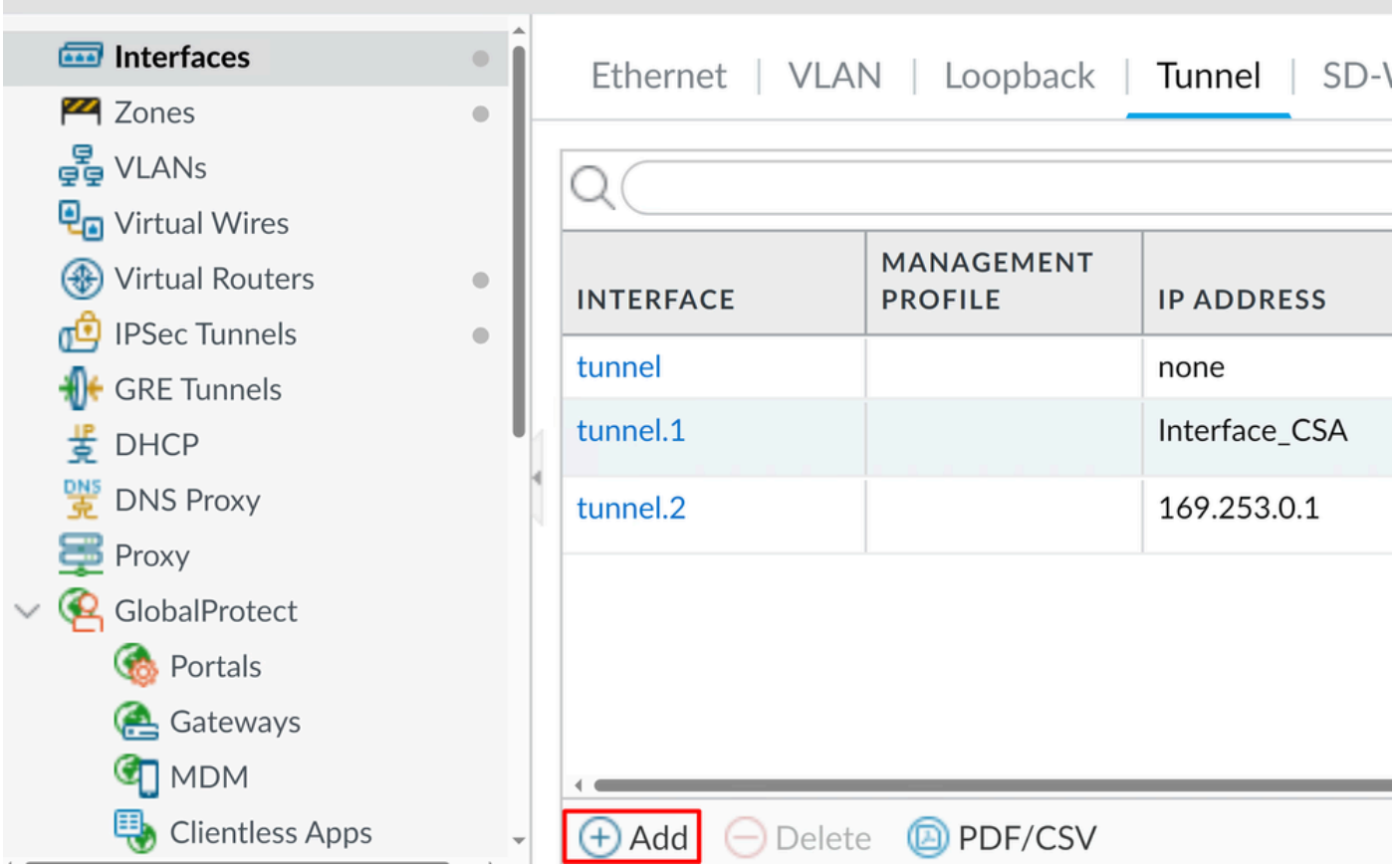


Configurar o túnel em Palo Alto

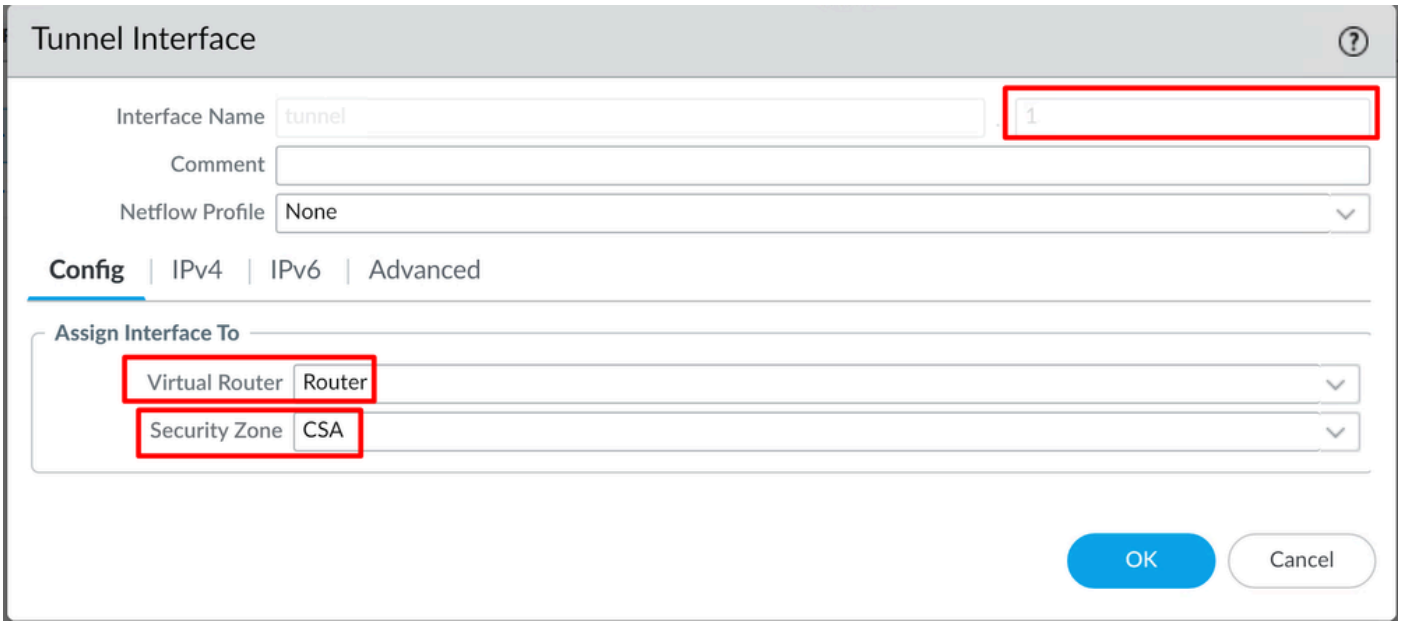
Configurar a interface do túnel

Navegue até o Painel Palo Alto.

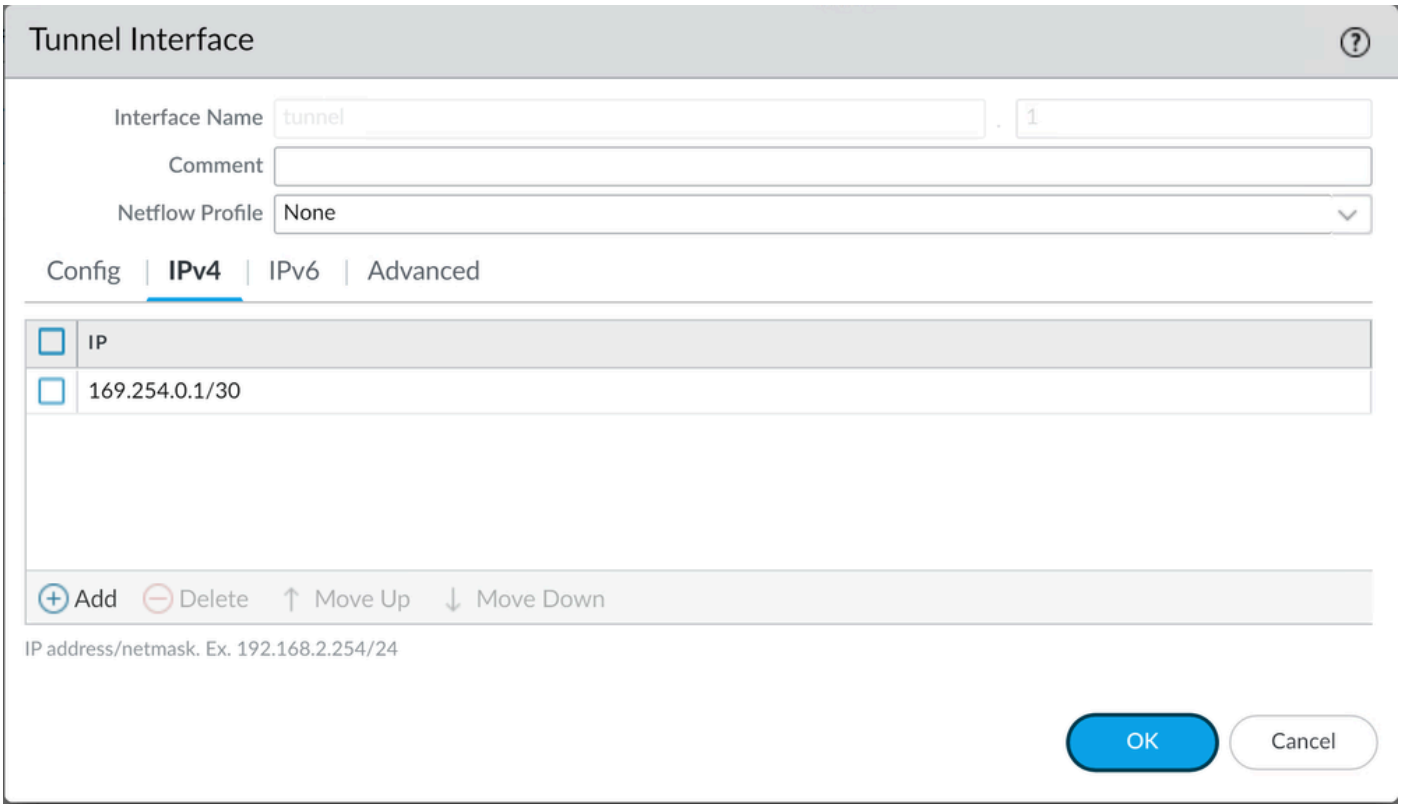
- Network > Interfaces > Tunnel
- Click Add



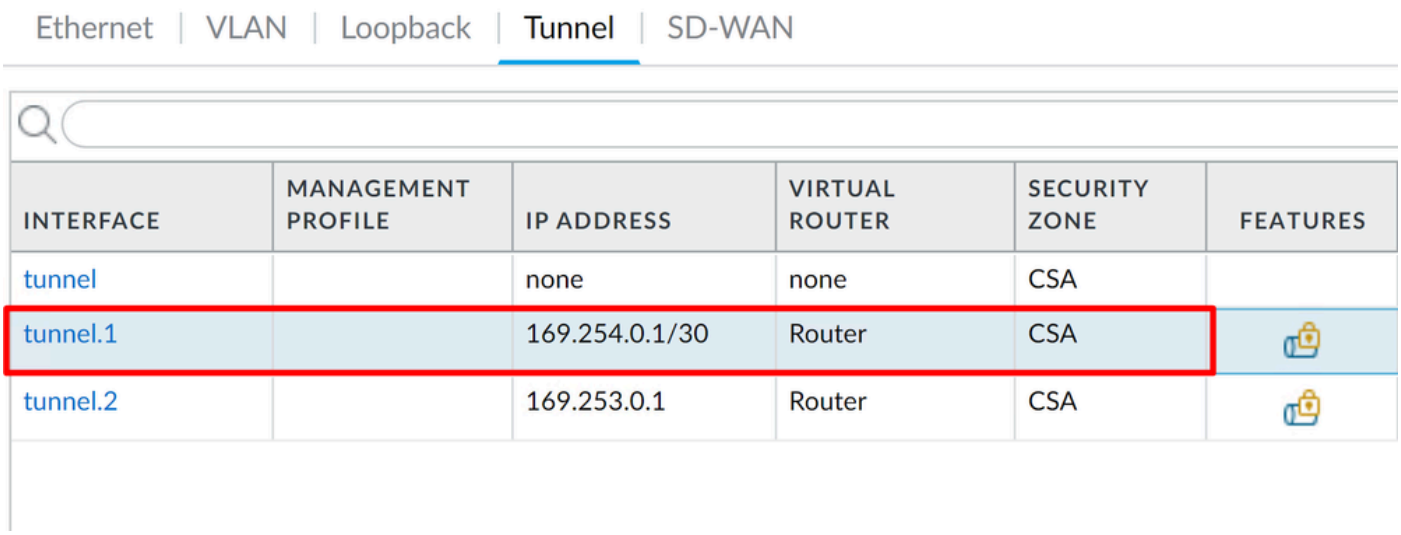
- No menuConfig, configure o Virtual Router, Security Zone e atribua umSuffix Number



- Em IPv4, configure um IP não roteável. Por exemplo, você pode usar 169.254.0.1/30
- Clique emOK



Depois disso, você pode ter algo assim configurado:

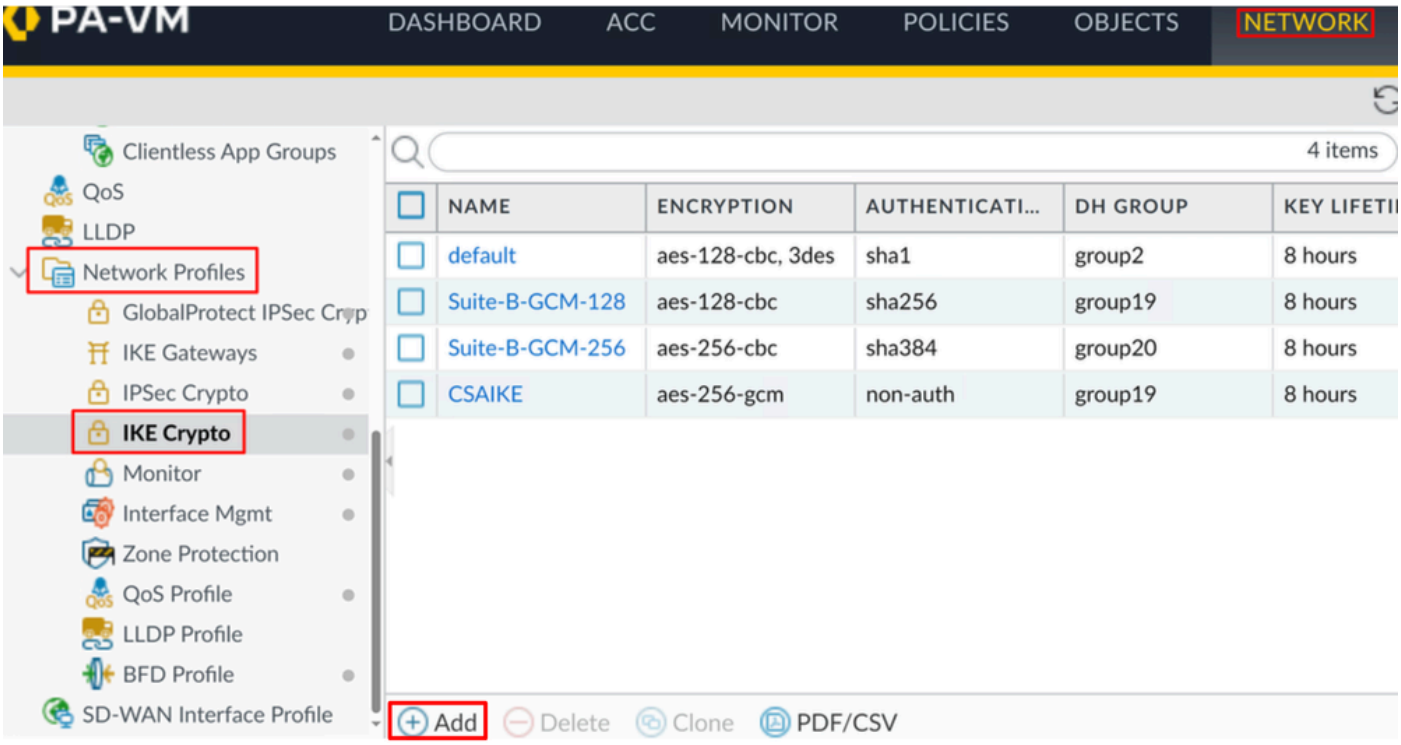


Se tiver configurado dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IKE Crypto Profile.

Configurar perfil de criptografia IKE

Para configurar o perfil de criptografia, navegue até:

- Network > Network Profile > IKE Crypto
- Clique emAdd



- Configure os próximos parâmetros:

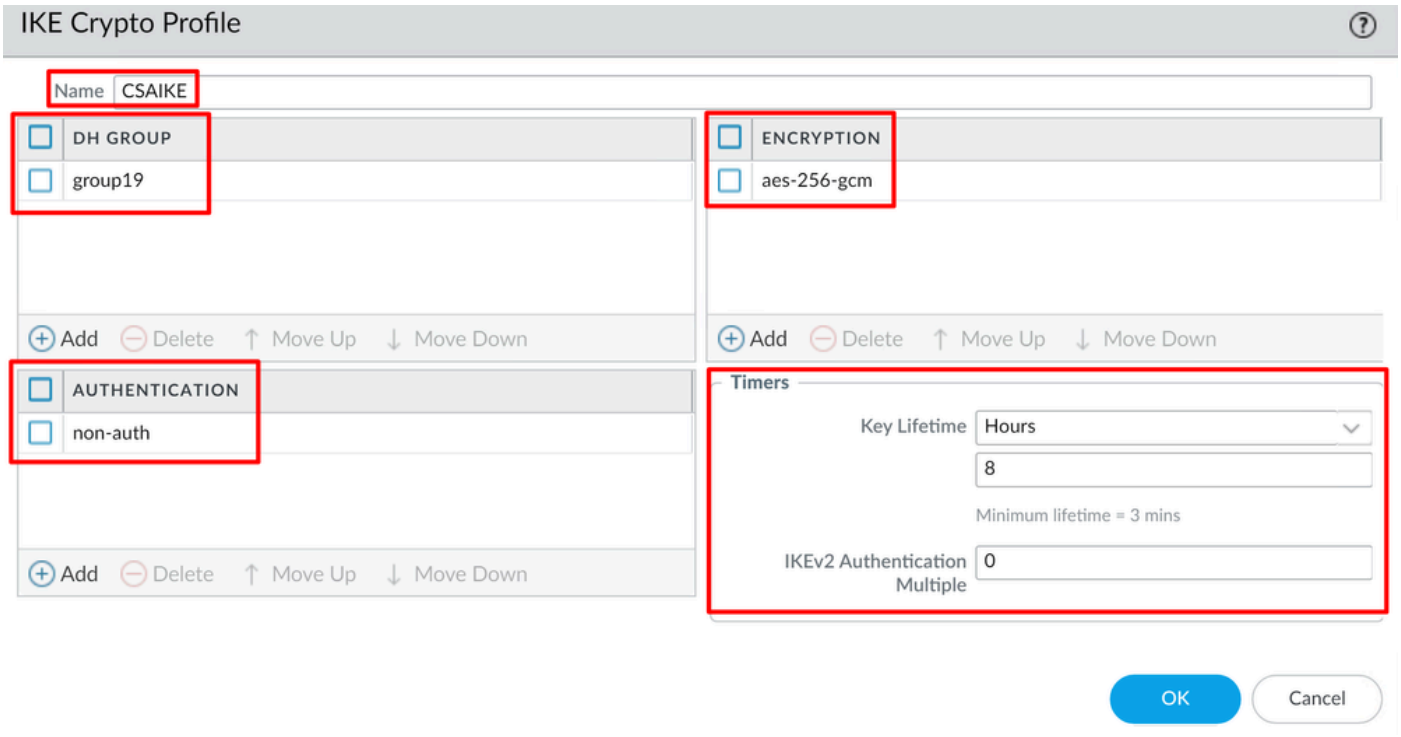
  - **Name**: Configure um nome para identificar o perfil.

    - **DH GROUP**: grupo19
    - **AUTHENTICATION**: não-autenticação
    - **ENCRYPTION**: aes-256-gcm
    - Timers

      - Key Lifetime: 8 horas

        - **IKEv2 Authentication**:0

- Após ter tudo configurado, clique em **OK**

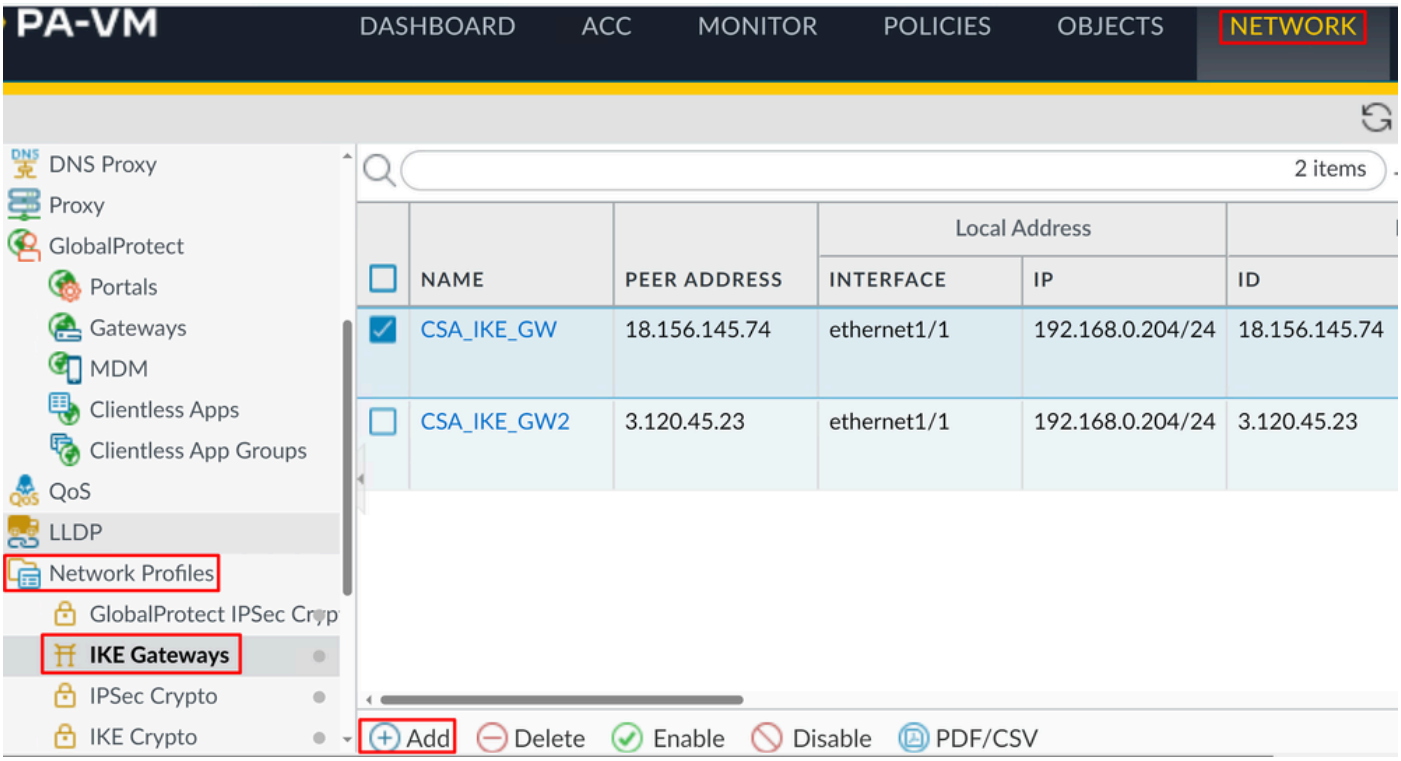


Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IKE Gateways.

Configurar gateways IKE

Para configurar gateways IKE

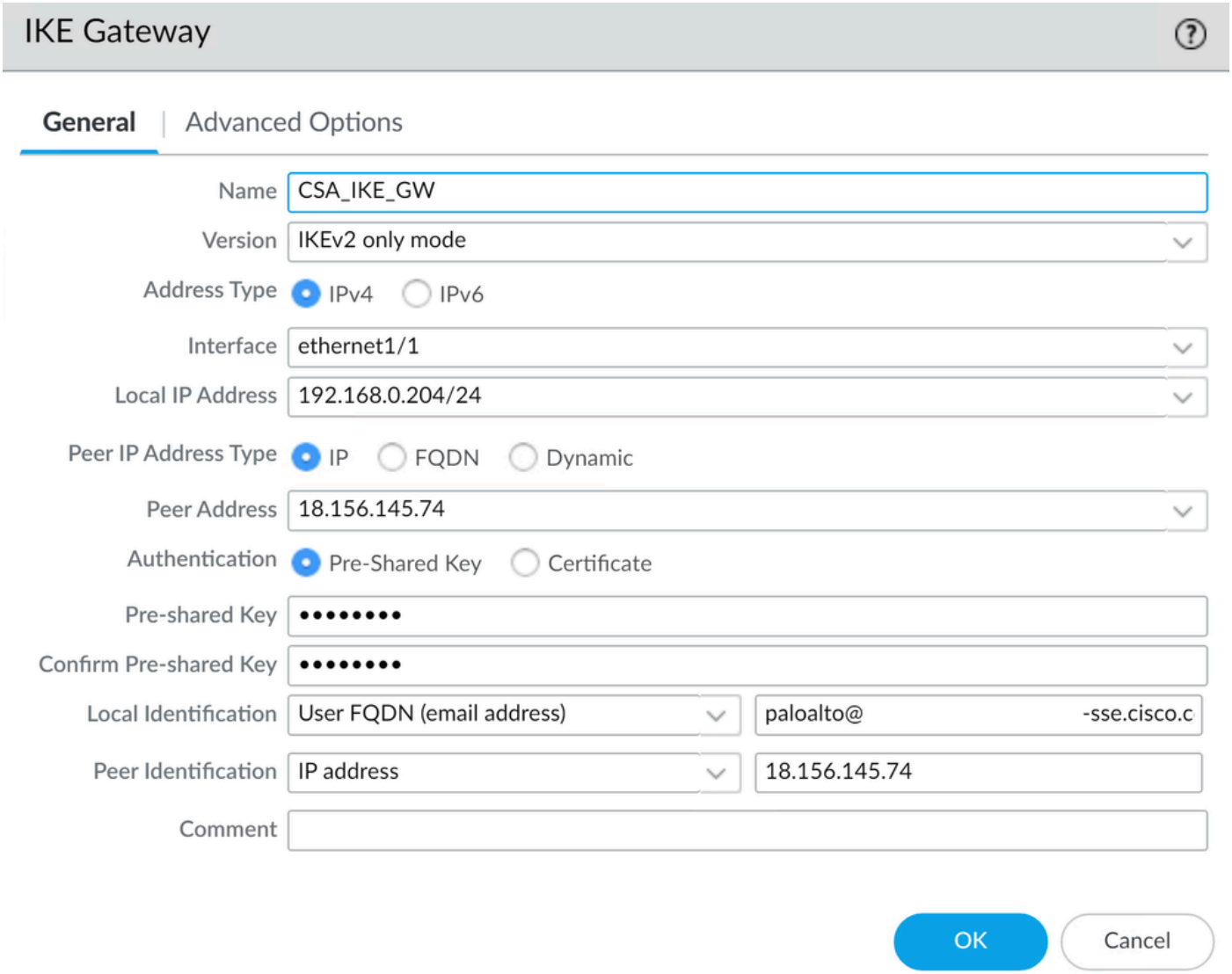
- Network > Network Profile > IKE Gateways
- Clique emAdd



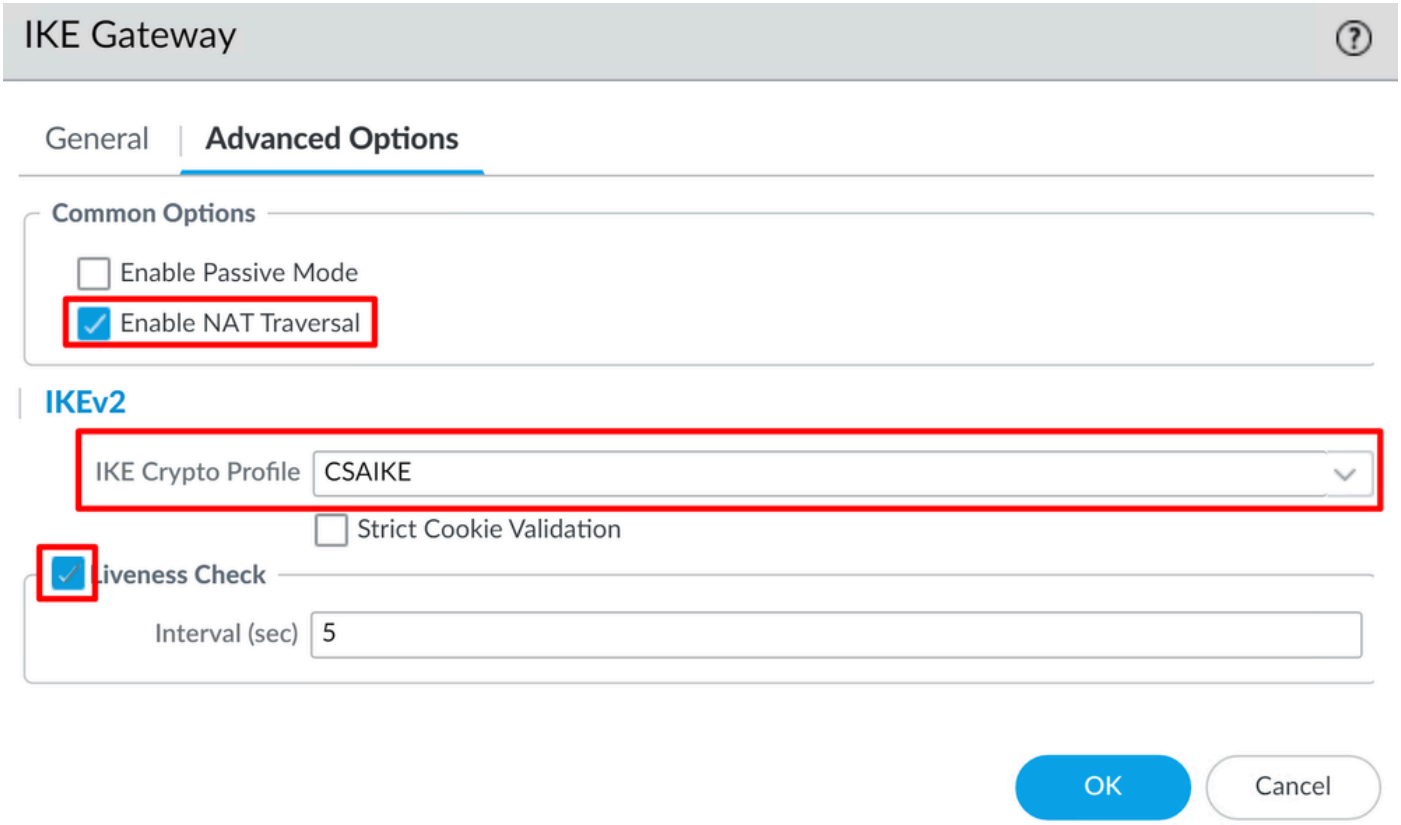
- Configure os próximos parâmetros:

  - Name: Configure um nome para identificar os Gateways Ike.

    - **Version** : modo somente IKEv2
    - Address Type :IPv4
    - **Interface** : selecione sua interface WAN da Internet.
    - Local IP Address: selecione o IP da interface WAN da Internet.
    - **Peer IP Address Type** :IP
    - Peer Address: Use o IP of Primary IP Datacenter IP Address, fornecido na etapa Tunnel Data.
    - Authentication: Chave pré-compartilhada
    - Pre-shared Key : Use o valor **passphrase** fornecido na etapa Tunnel Data.
    - **Confirm Pre-shared Key** : Use o valor **passphrase** fornecido na etapa Tunnel Data.
    - **Local Identification** : Escolha **User FQDN (Email address)** e use o **Primary Tunnel ID** dado na etapa, Dados do túnel.
    - **Peer Identification** : IP AddressEscolha e use o Primary IP Datacenter IP Address.



- Clique emAdvanced Options
    - **Enable NAT Traversal**
        - Selecione o **IKE Crypto Profile** criado na etapa, Configurar perfil de criptografia IKE
        - Marcar a caixa de seleção para **Liveness Check**
        - Clique em **OK**

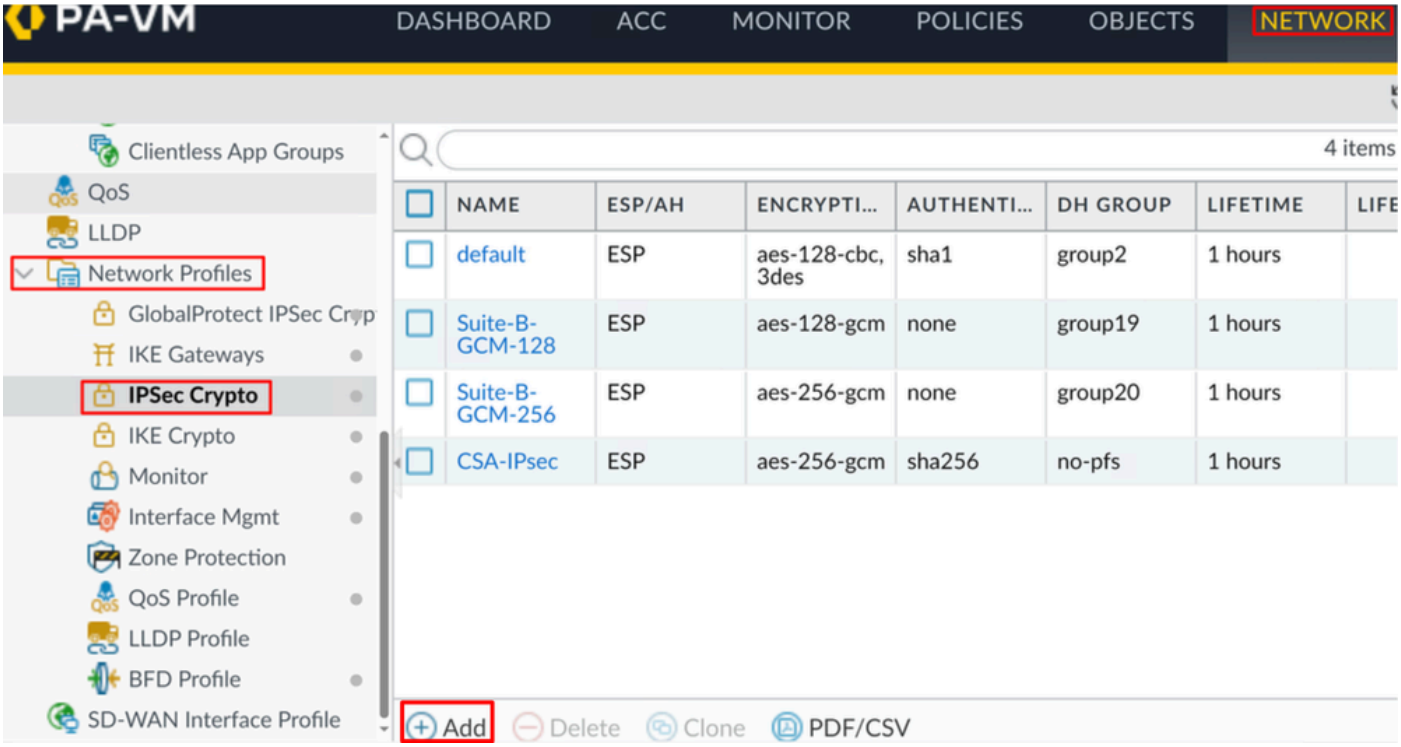


Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IPSEC Crypto.

Configurar perfil de criptografia IPSEC

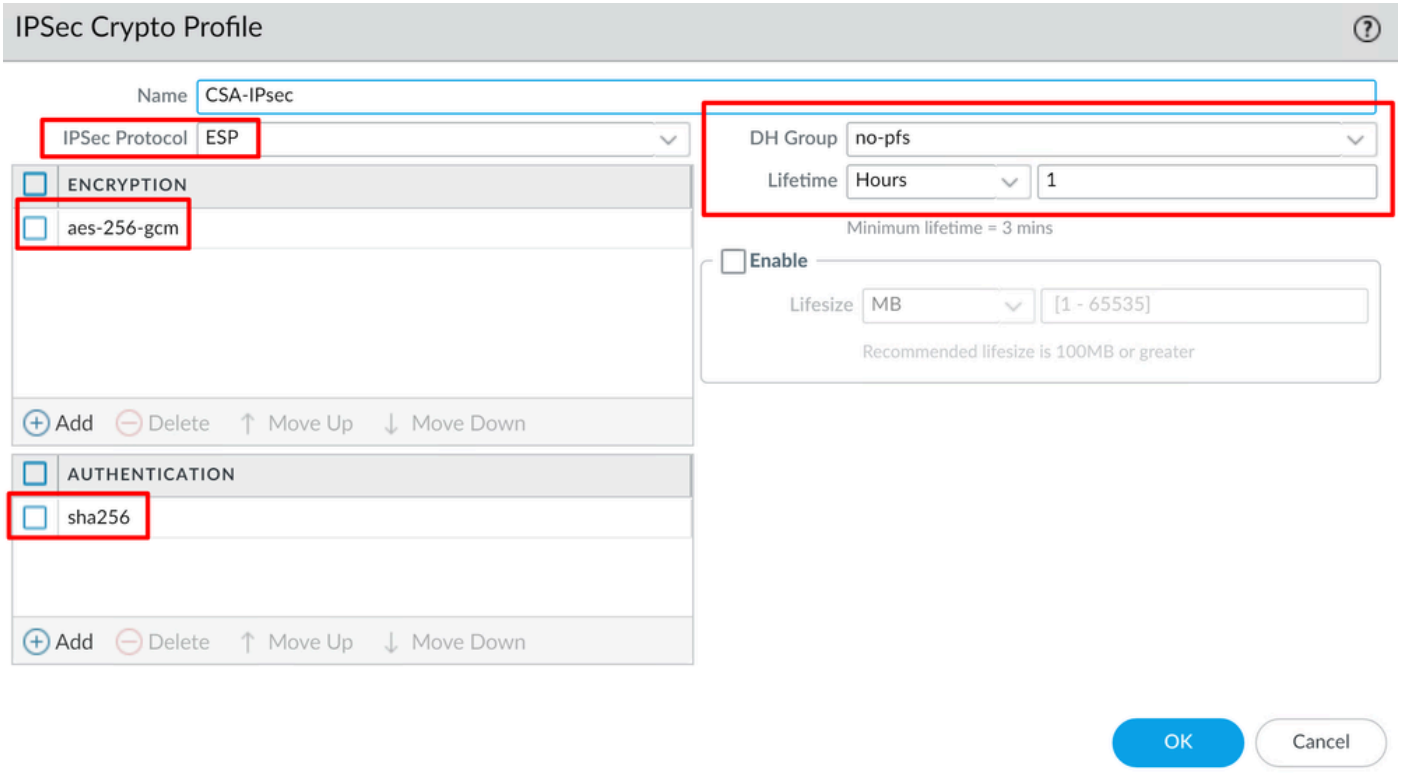
Para configurar os gateways IKE, navegue até Network > Network Profile > IPSEC Crypto

- Clique emAdd



- Configure os próximos parâmetros:
    - **Name**: use um nome para identificar o perfil IPsec de acesso seguro
        - IPSec Protocol: ESP
        - **ENCRYPTION**: aes-256-gcm
        - DH Group: no-pfs, 1 hora

- Clique em OK

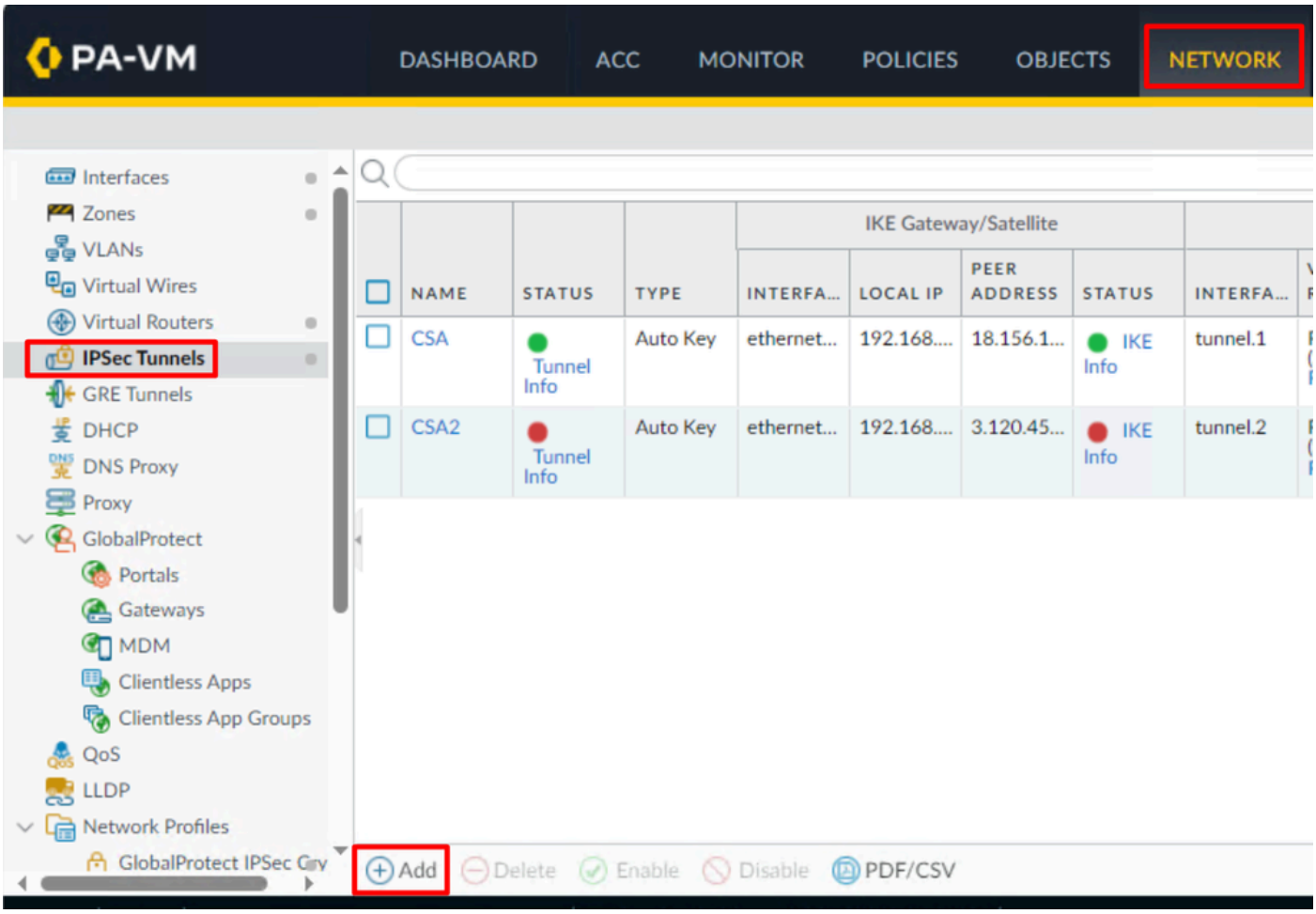


Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IPSec Tunnels.

Configurar túneis IPSec

Para configurar **IPSec Tunnels**, navegue até Network > IPSec Tunnels.

- Clique em Add



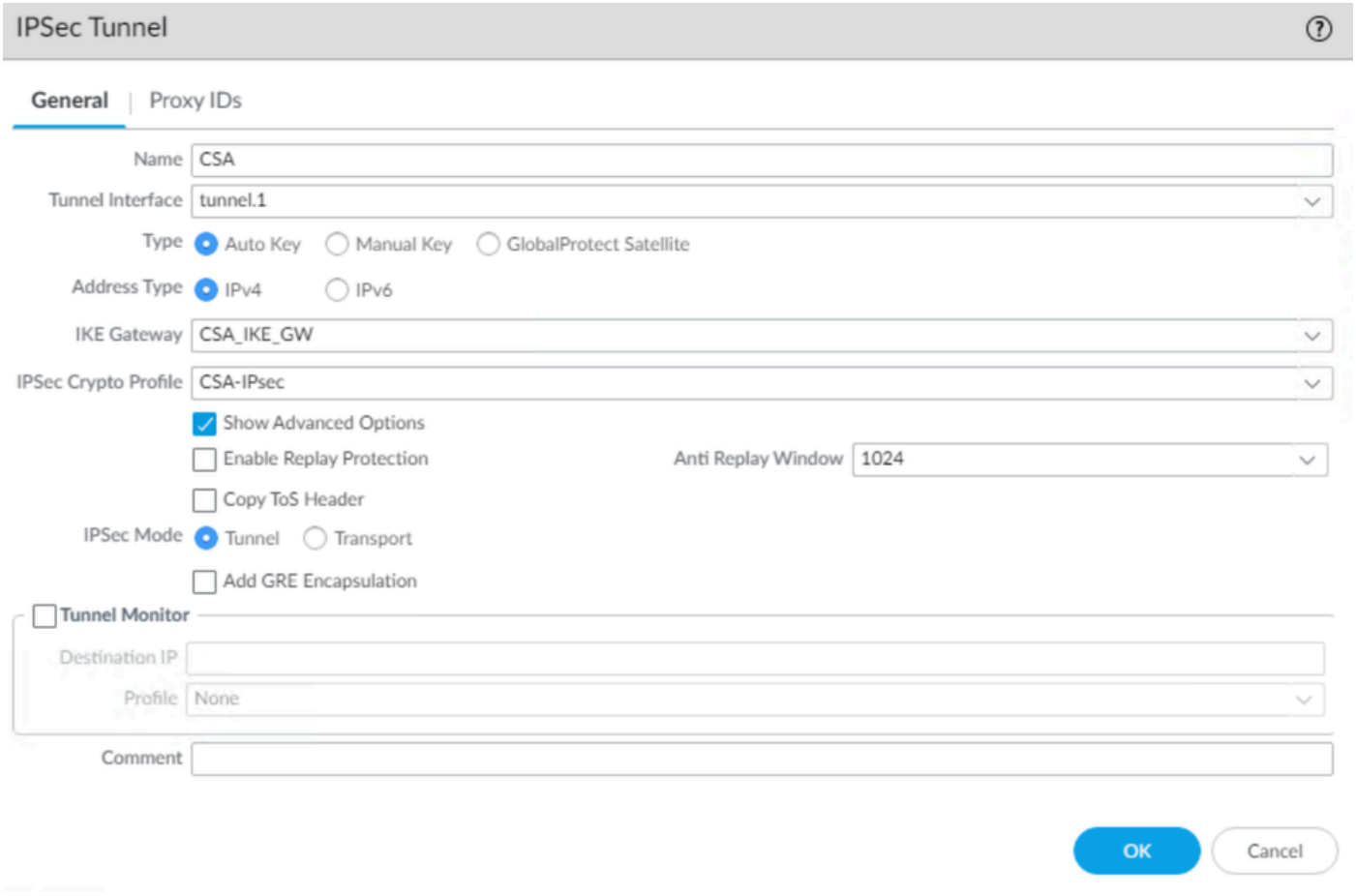
- Configure os próximos parâmetros:

  - **Name**: use um nome para identificar o túnel de acesso seguro

    - **Tunnel Interface**: Escolha a interface de túnel configurada na etapa, Configure a interface de túnel.
    - **Type**: Chave automática
    - **Address Type**:IPv4
    - **IKE Gateways**: Escolha os gateways IKE configurados na etapa, Configurar gateways IKE.
    - **IPsec Crypto Profile**: Escolha os gateways IKE configurados na etapa, Configurar perfil de criptografia IPSEC
    - Marcar a caixa de seleção para **Advanced Options**

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

- Clique em OK

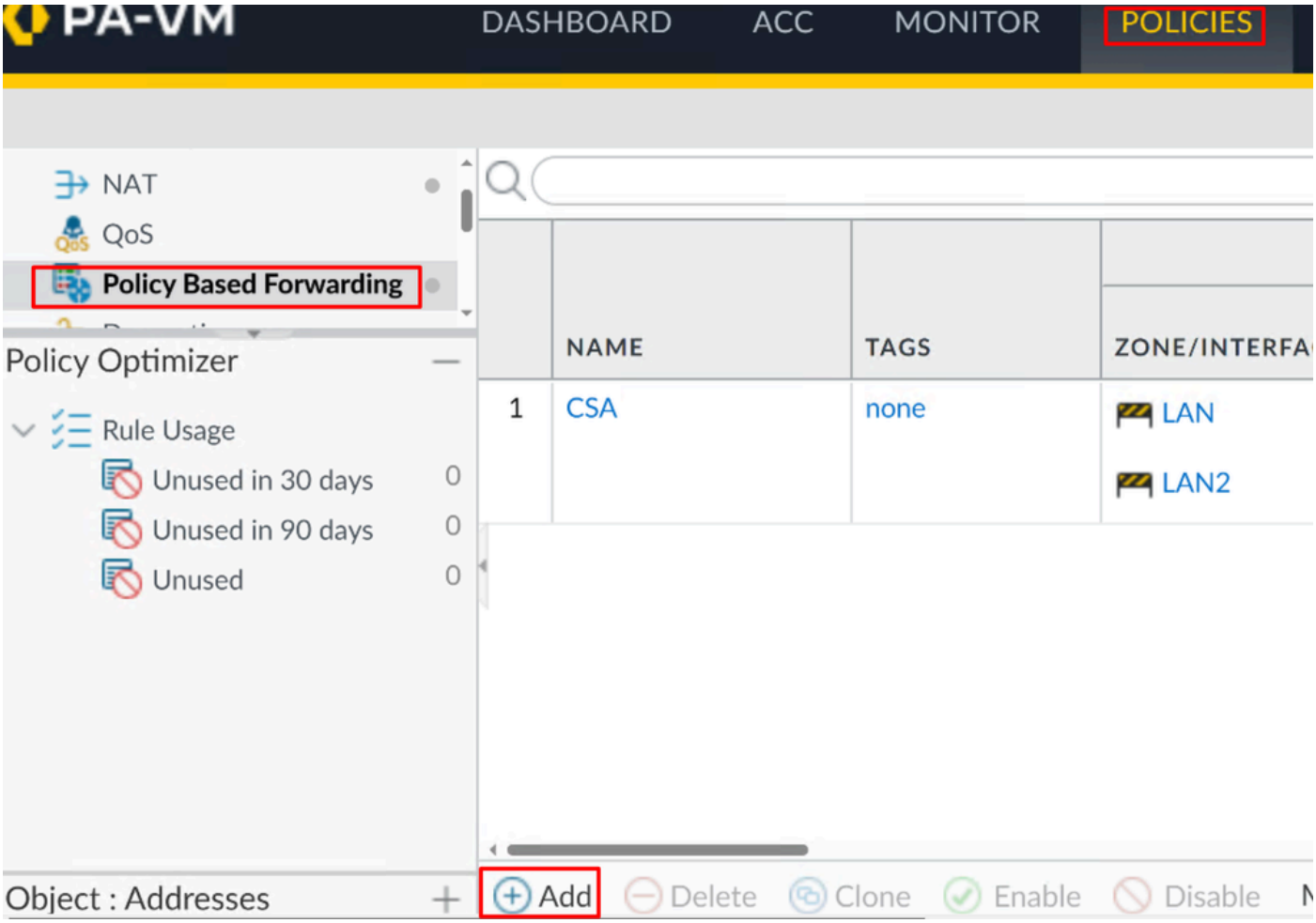


Agora que sua VPN foi criada com êxito, você pode prosseguir com a etapa, **Configure Policy Based Forwarding**.

Configurar Encaminhamento Baseado em Política

Para configurar **Policy Based Forwarding**, navegue até Policies > Policy Based Forwarding.

- Clique em Add



- Configure os próximos parâmetros:
  - General
    - **Name**: use um nome para identificar o acesso seguro, encaminhamento de base de política (roteamento por origem)
- Source
  - **Zone**: selecione as Zonas de onde você tem planos para rotear o tráfego com base na origem
    - **Source Address**: configure o host ou as redes que você deseja usar como origem.
    - Source Users: configure os usuários para os quais deseja rotear o tráfego (somente se aplicável)

- Destination/Application/Service

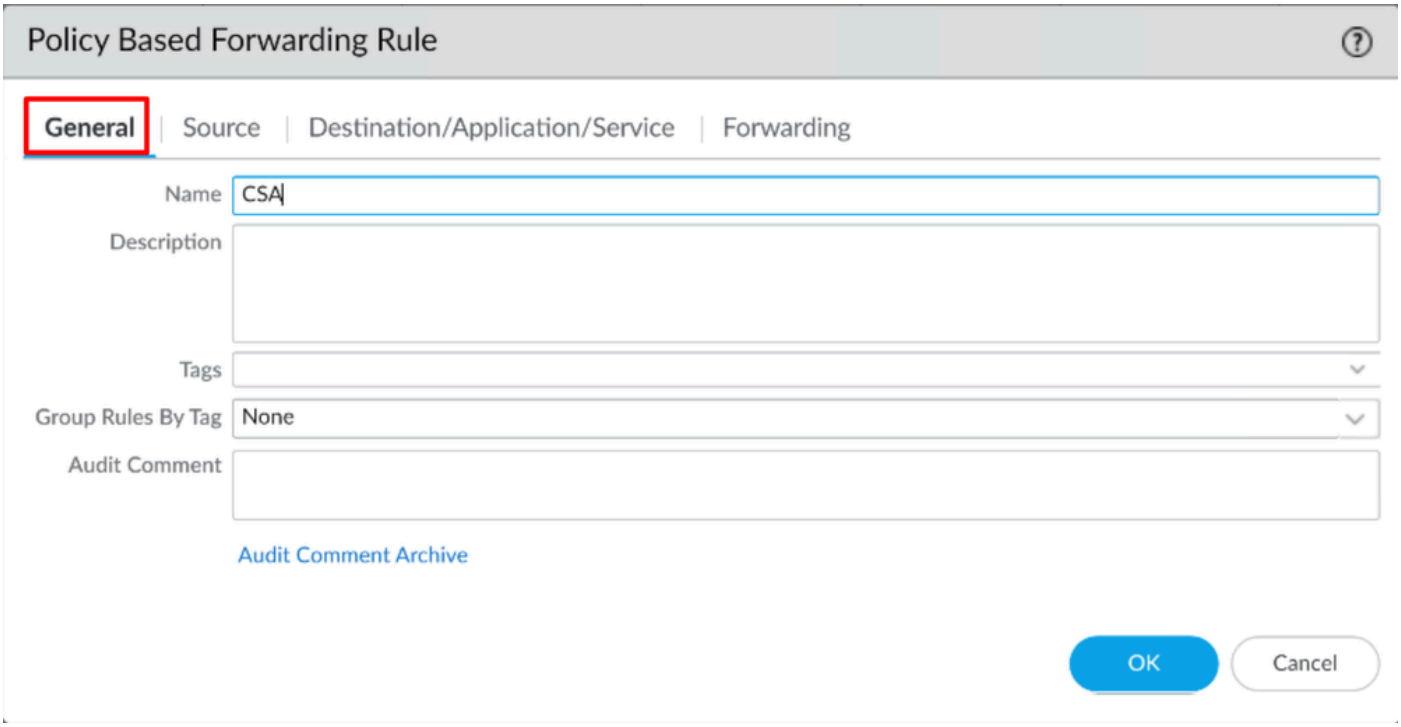
  - Destination Address: Você pode deixá-lo como Qualquer ou pode especificar os intervalos de endereços de Acesso seguro (100.64.0.0/10)

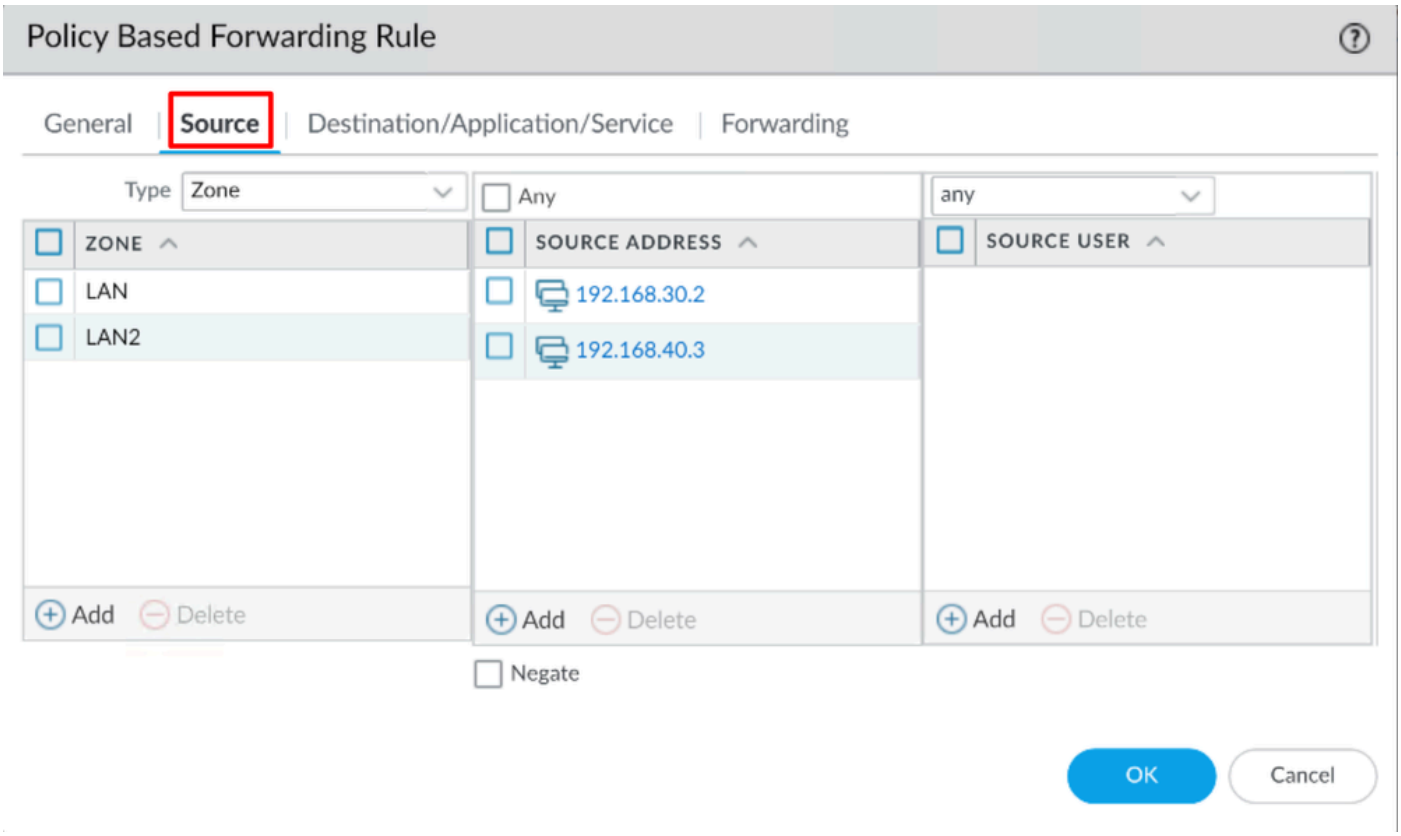
- Forwarding

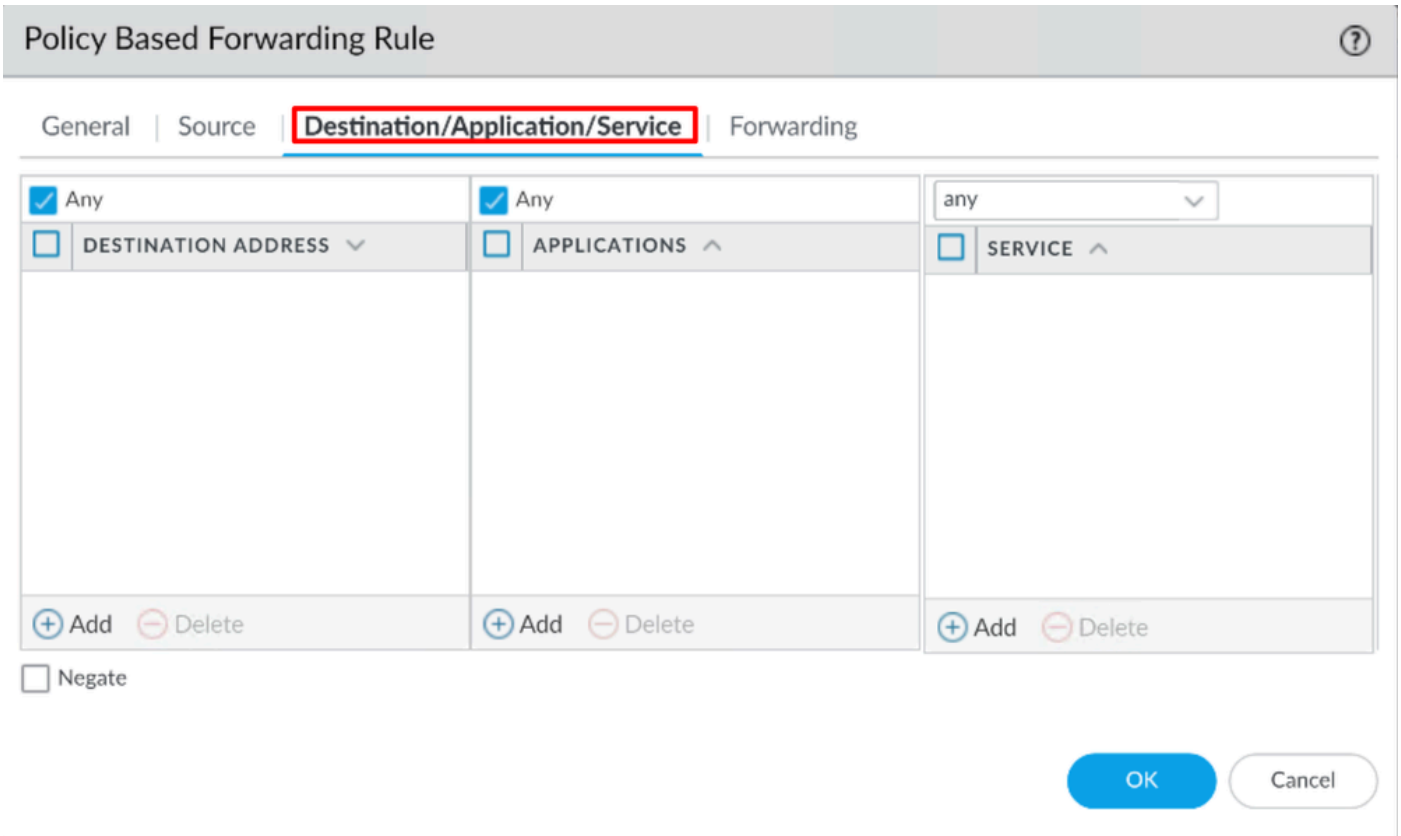
  - **Action**:Encaminhar

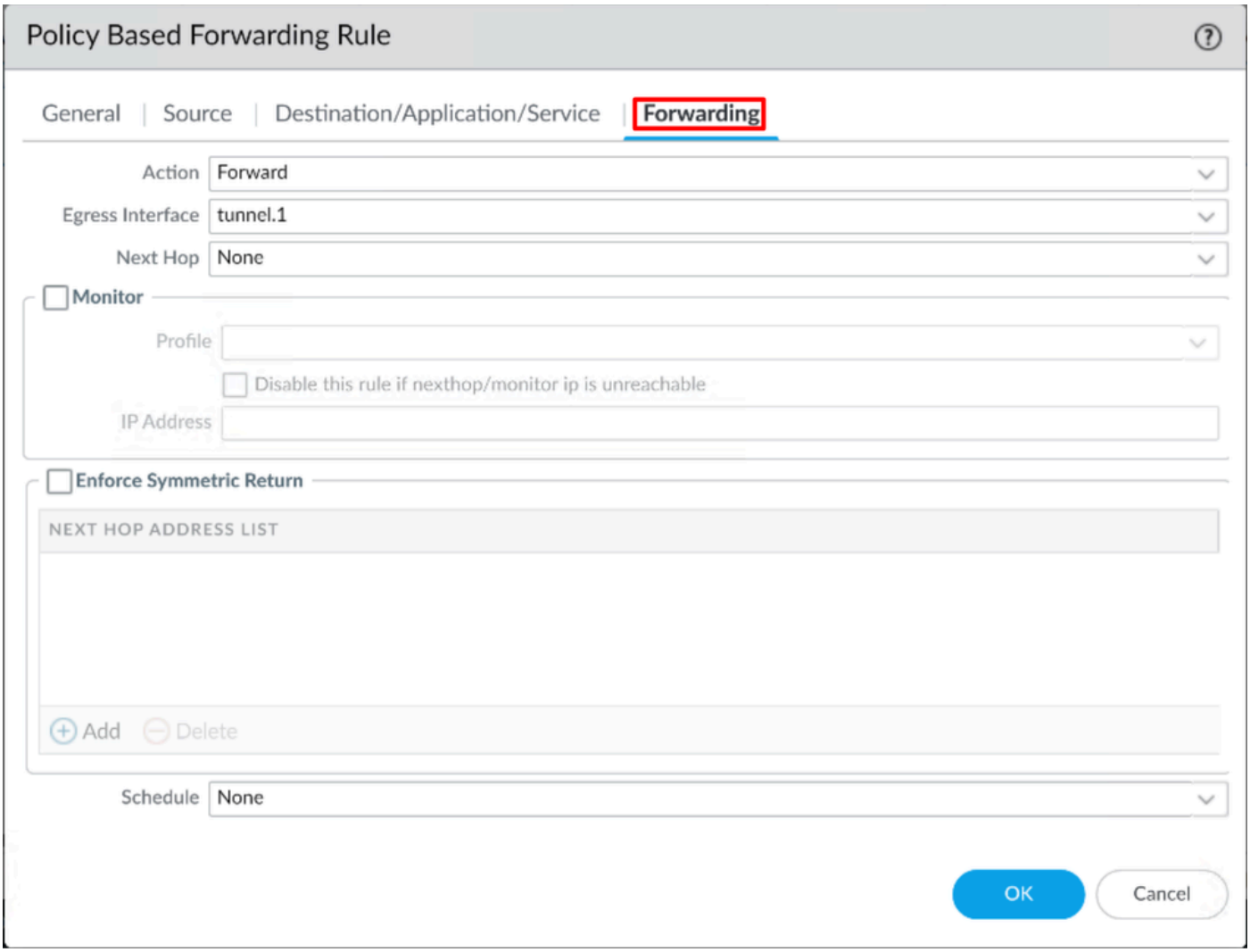
    - **Egress Interface**: Escolha a interface de túnel configurada na etapa, Configure a interface de túnel.
    - **Next Hop**:Nenhum

- CliqueOK em e 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



Agora você tem tudo configurado em Palo Alto; depois de configurar a rota, o túnel pode ser estabelecido e você precisa continuar configurando o RA-VPN, o ZTA baseado em navegador ou o ZTA base do cliente no painel de acesso seguro.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.