Sicheren Zugriff mit Palo Alto Firewall konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit der Palo Alto Firewall konfigurieren.

Voraussetzungen

- Konfiguration der Benutzerbereitstellung
- Konfiguration der ZTNA SSO-Authentifizierung
- Konfigurieren des sicheren Remotezugriff-VPN

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Palo Alto 11.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Palo Alto 11.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco hat Secure Access entwickelt, um den Zugriff auf private Anwendungen vor Ort und in der Cloud zu schützen. Außerdem wird die Verbindung vom Netzwerk zum Internet gesichert. Dies wird durch die Implementierung mehrerer Sicherheitsmethoden und -ebenen erreicht, die alle darauf abzielen, die Informationen beim Zugriff über die Cloud zu erhalten.

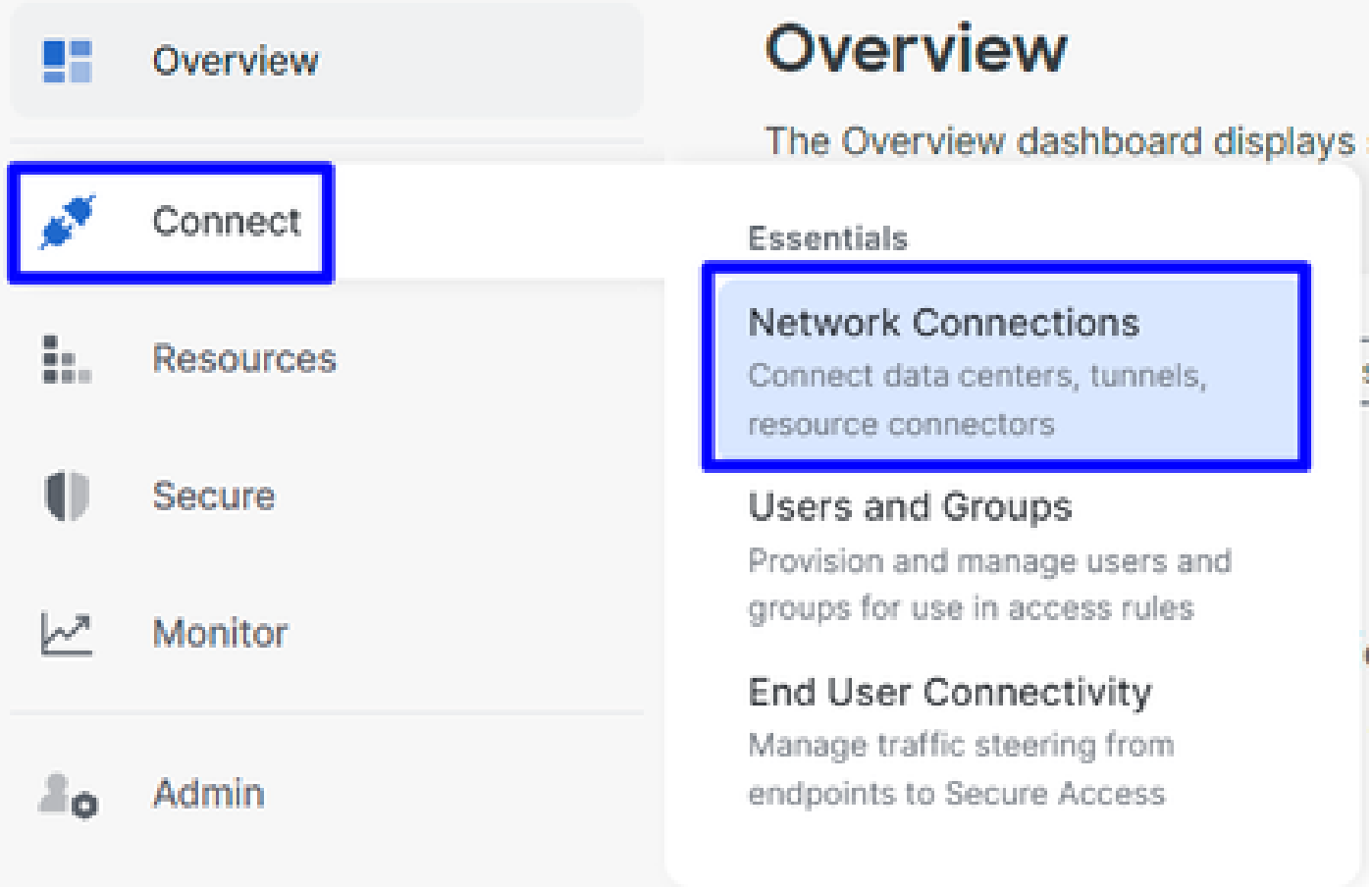
Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

Navigieren Sie zum Admin-Bereich von Secure Access.

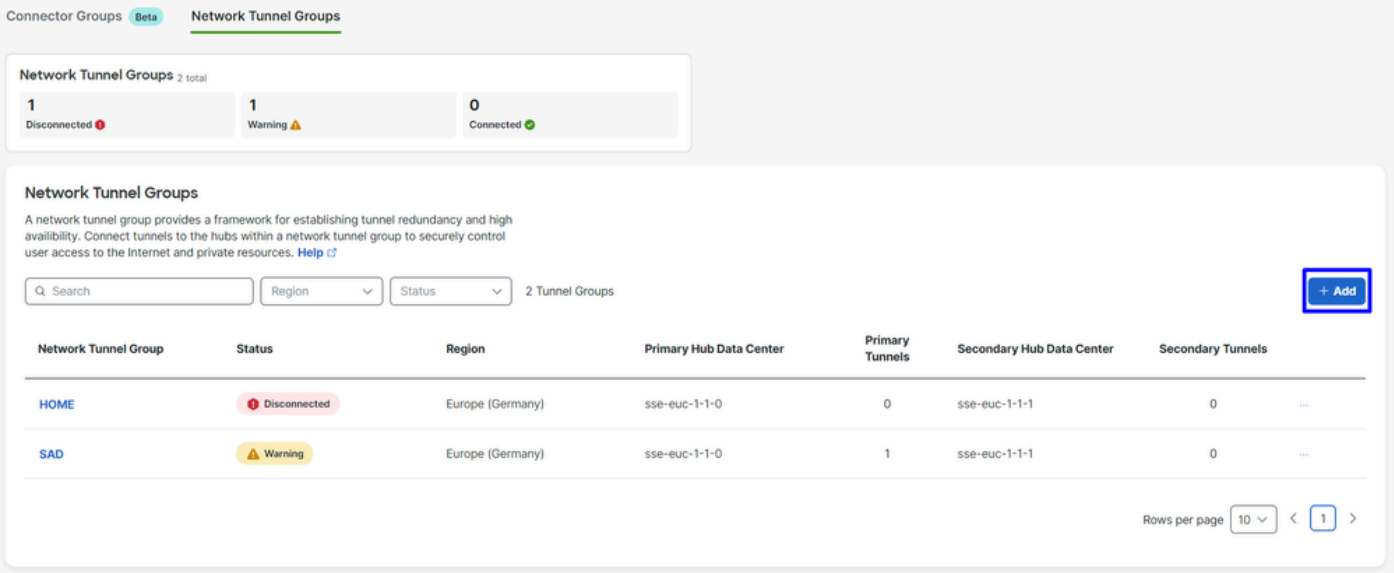
Sicherer Zugriff - Hauptseite

- Klicken Sie Connect > Network Connections



Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Network Tunnel Groups auf + Add



Sicherer Zugriff - Netzwerk-Tunnelgruppen

- Konfiguration Tunnel Group Name Region und Device Type
- Klicken Sie auf **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

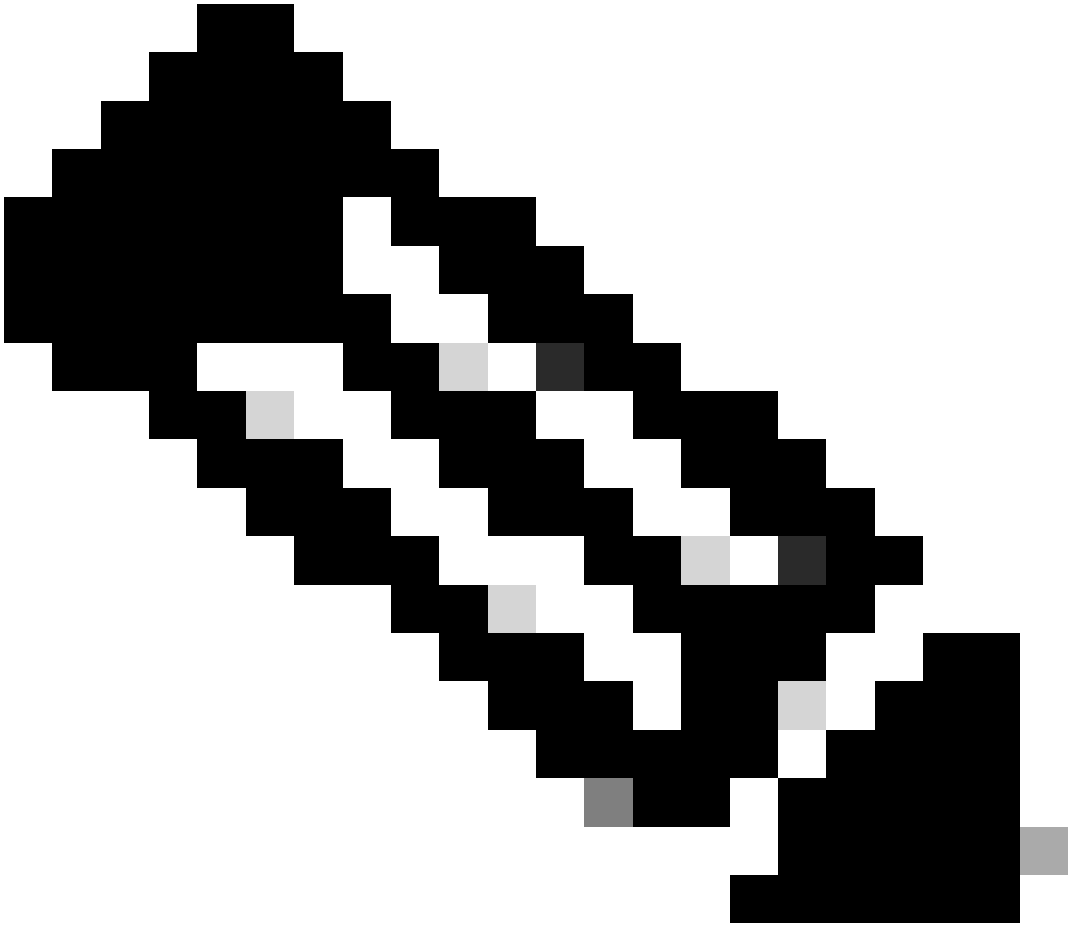
Europe (Germany)

Device Type

Other

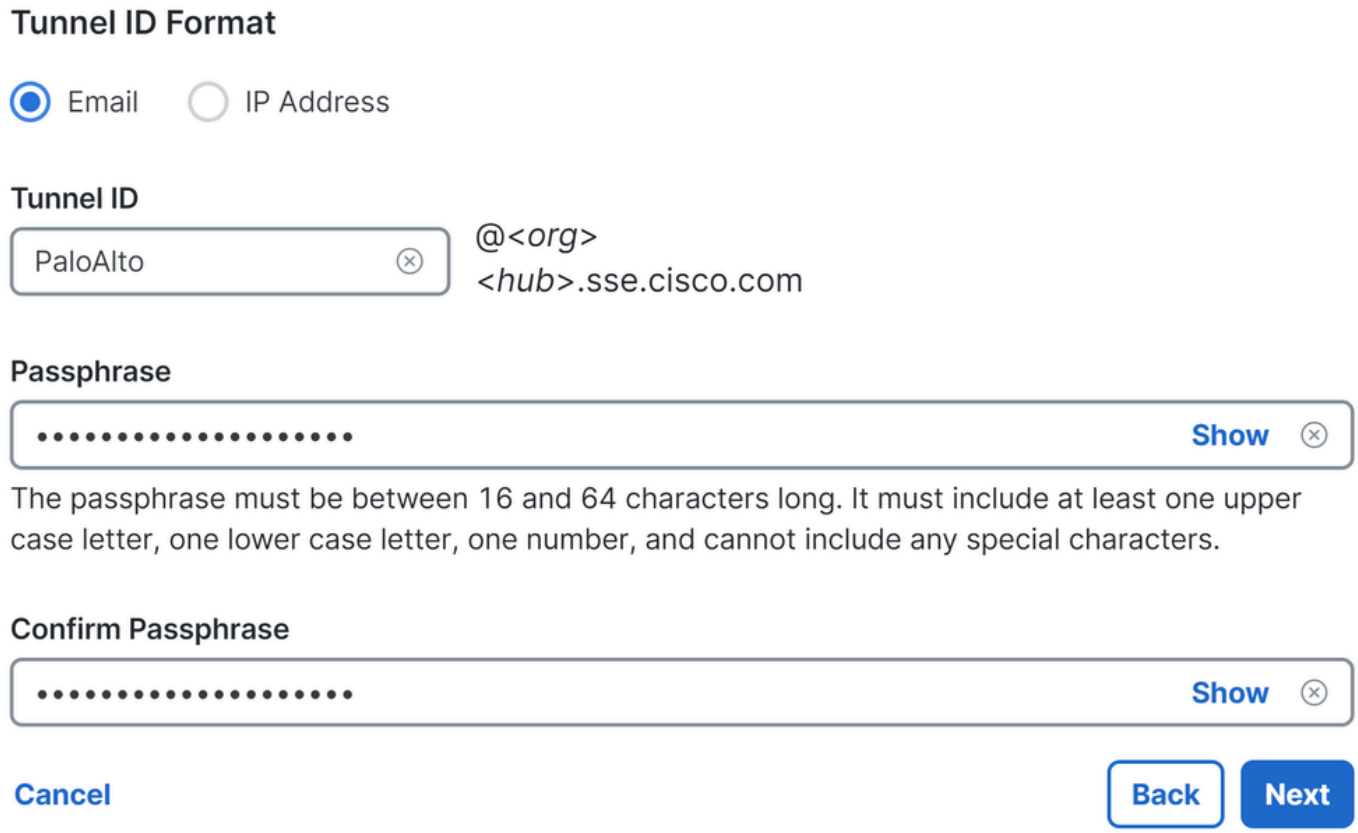
Cancel

Next



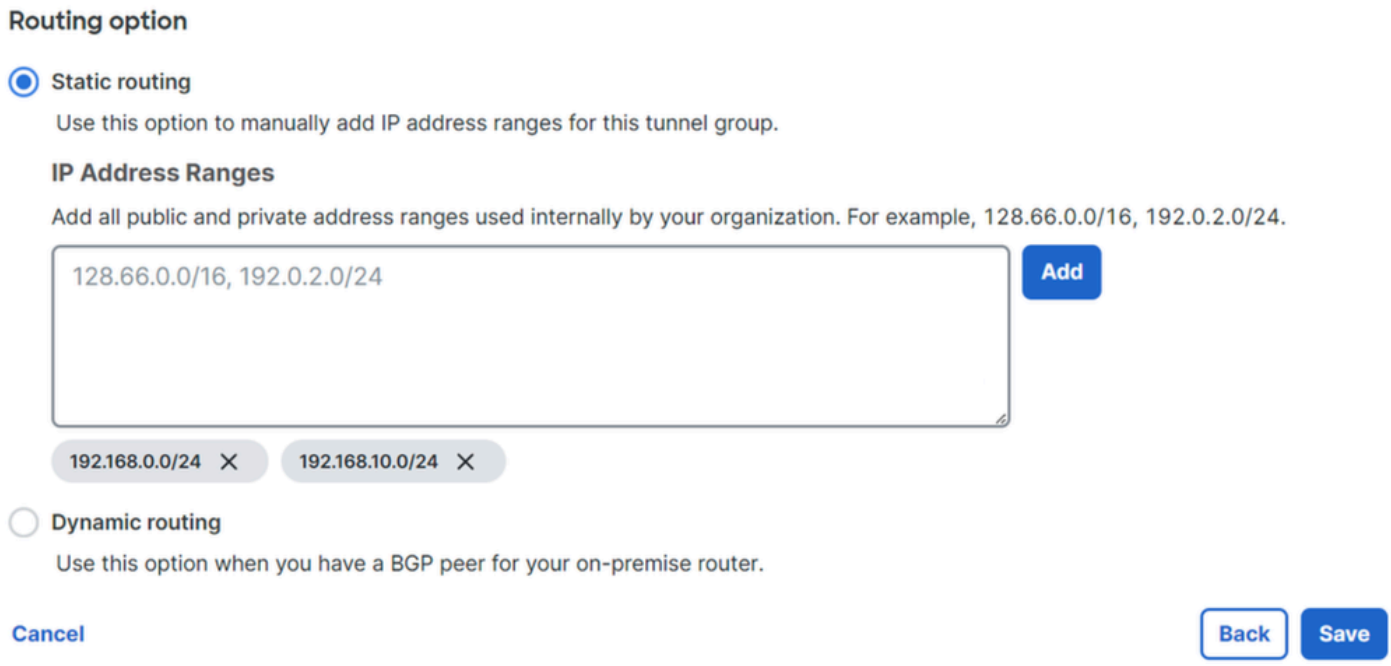
Hinweis: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten ist.

- Konfigurieren Sie die Tunnel ID Format und Passphrase
- Klicken Sie auf Next



- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über sicheren Zugriff weiter.

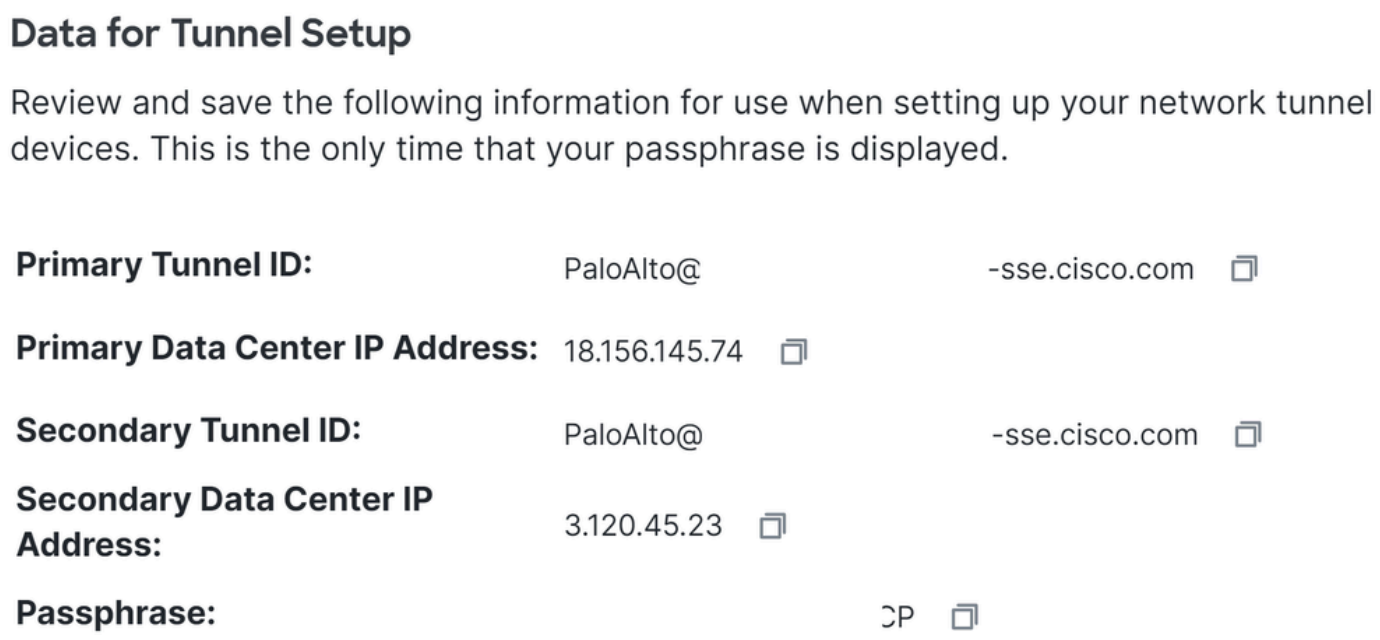
- Klicken Sie auf **Save**



Sicherer Zugriff - Tunnelgruppen - Routing-Optionen

Nachdem Sie auf **Save** die Informationen über den Tunnel wird angezeigt, speichern Sie diese Informationen für den nächsten Schritt, **Configure the tunnel on Palo Alto**.

Tunneldaten

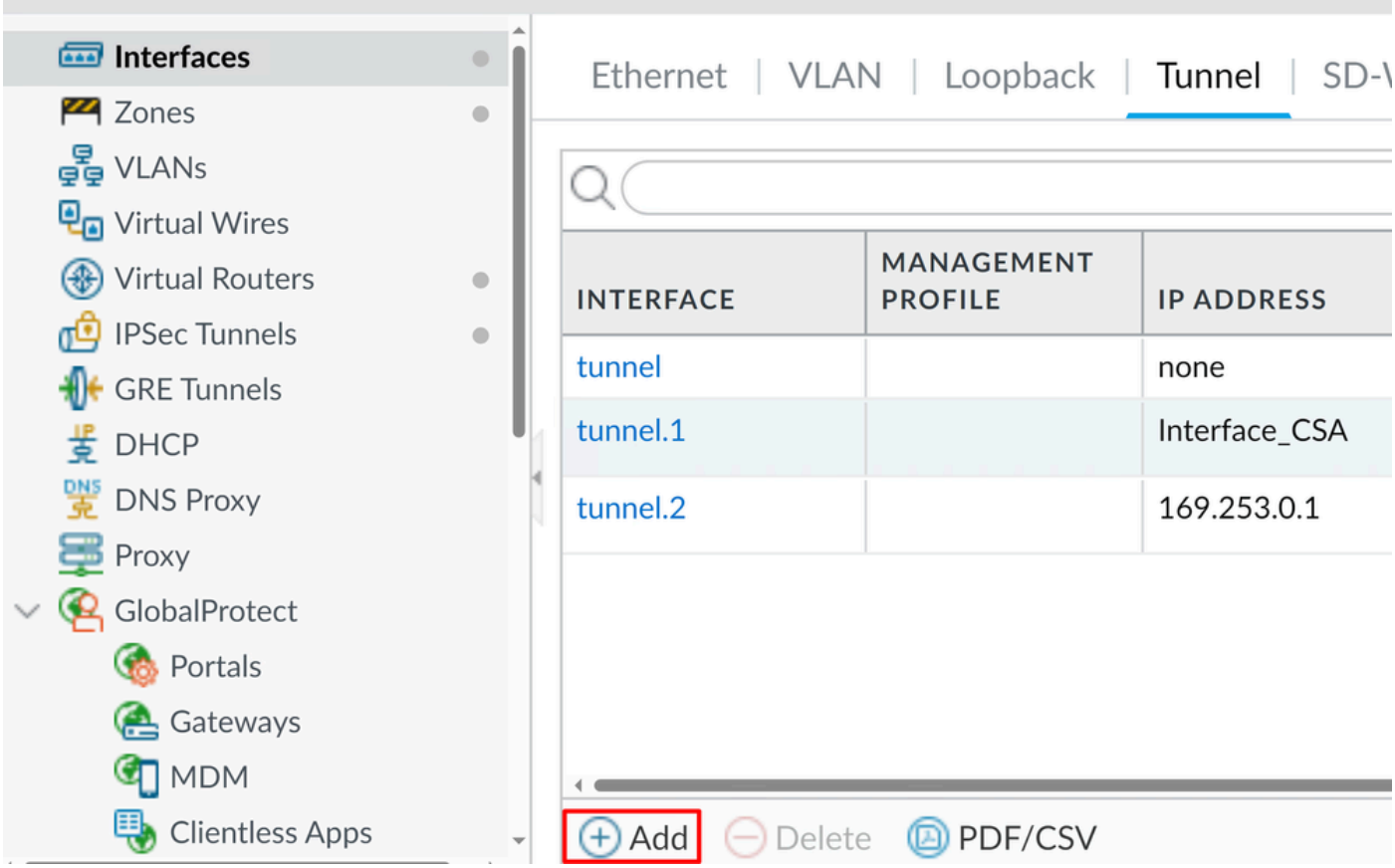


Konfigurieren Sie den Tunnel auf Palo Alto

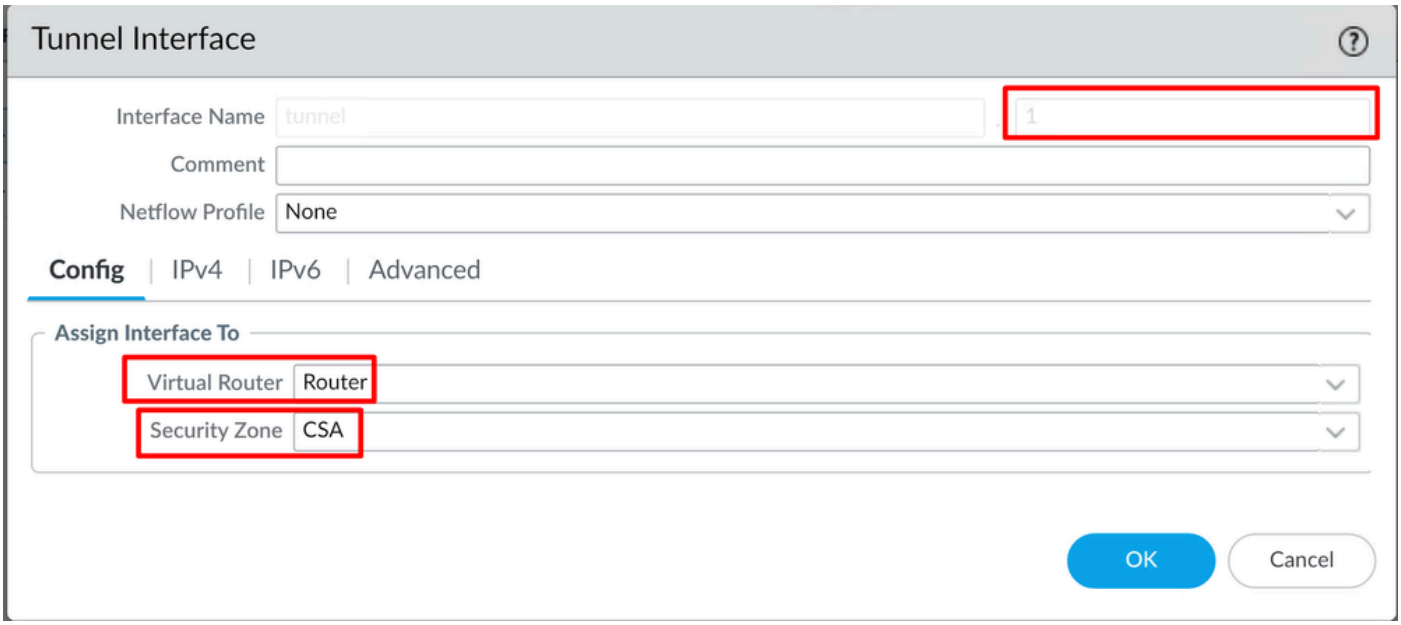
Konfigurieren der Tunnelschnittstelle

Navigieren Sie zum Palo Alto Dashboard.

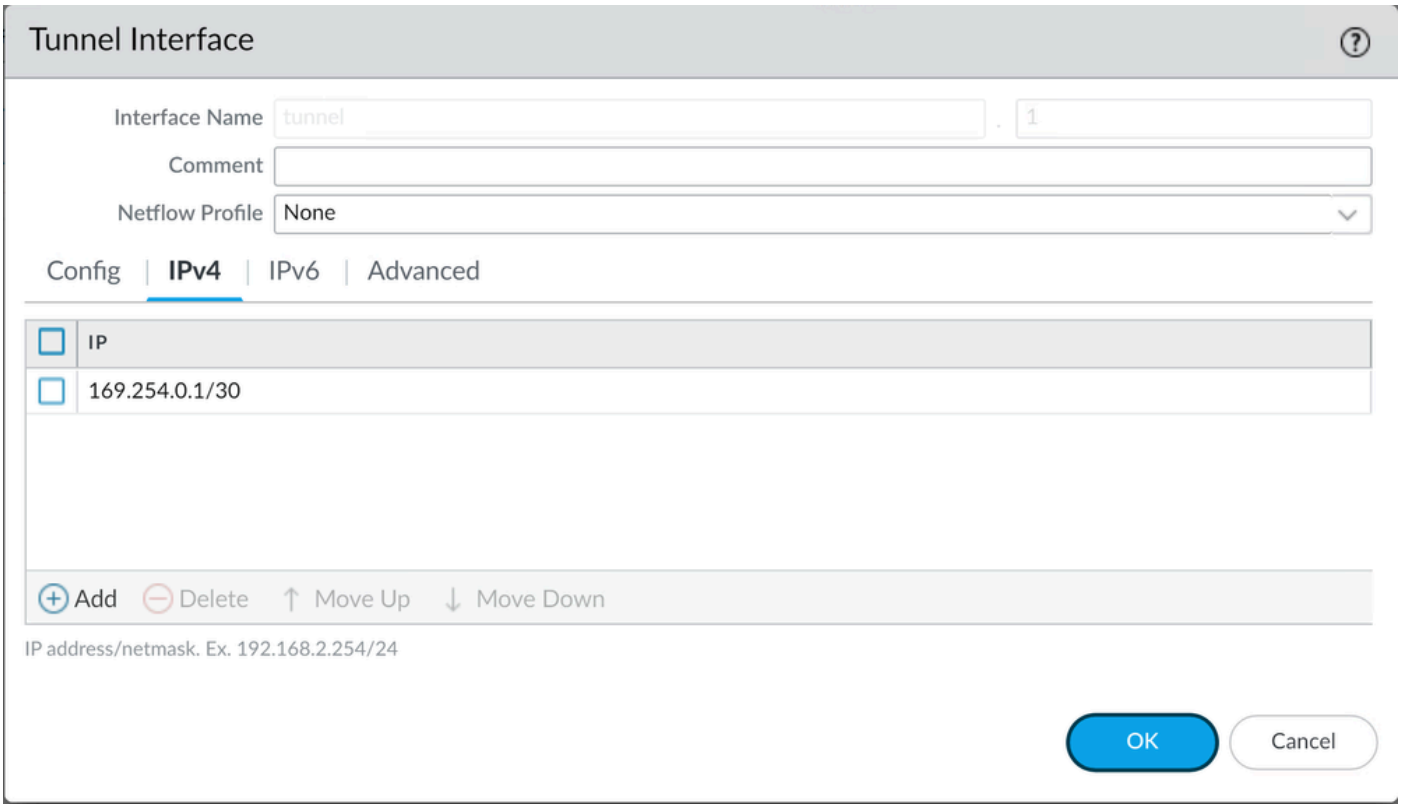
- Network > Interfaces > Tunnel
- Click Add



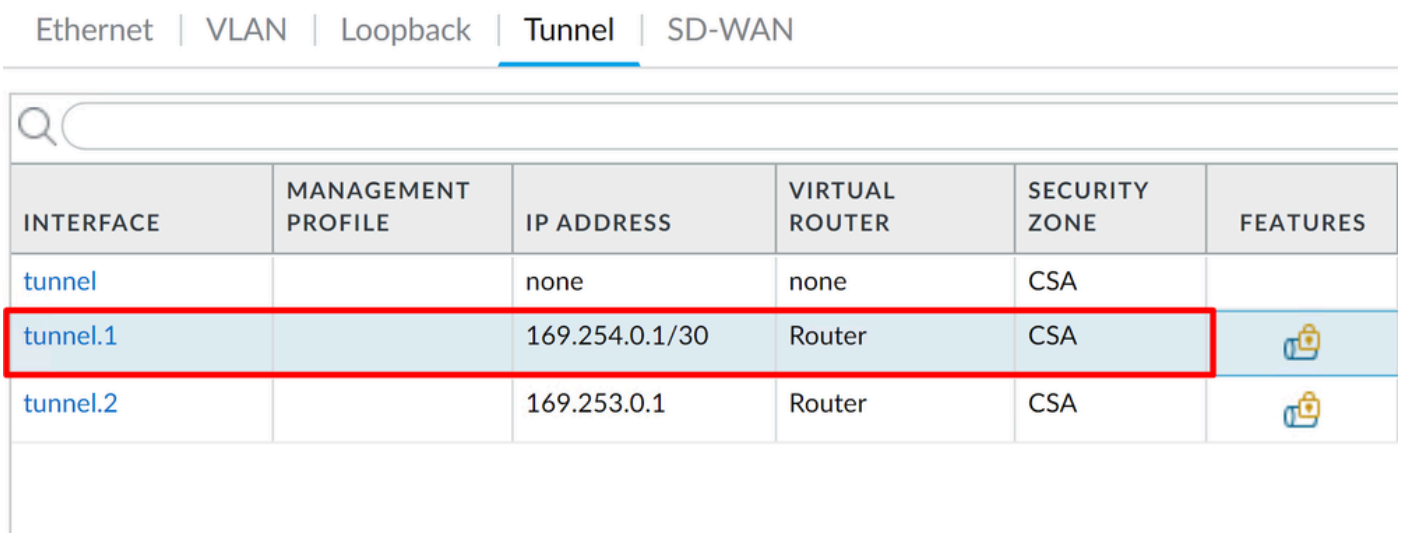
- Konfigurieren SieConfig im Menü die Virtual Router, Security Zone und weisen SieSuffix Number



- Konfigurieren Sie unter IPv4 eine nicht routbare IP-Adresse. Sie können z. B. 169.254.0.1/30
- Klicken Sie auf OK



Danach können Sie etwas wie das hier konfigurieren lassen:

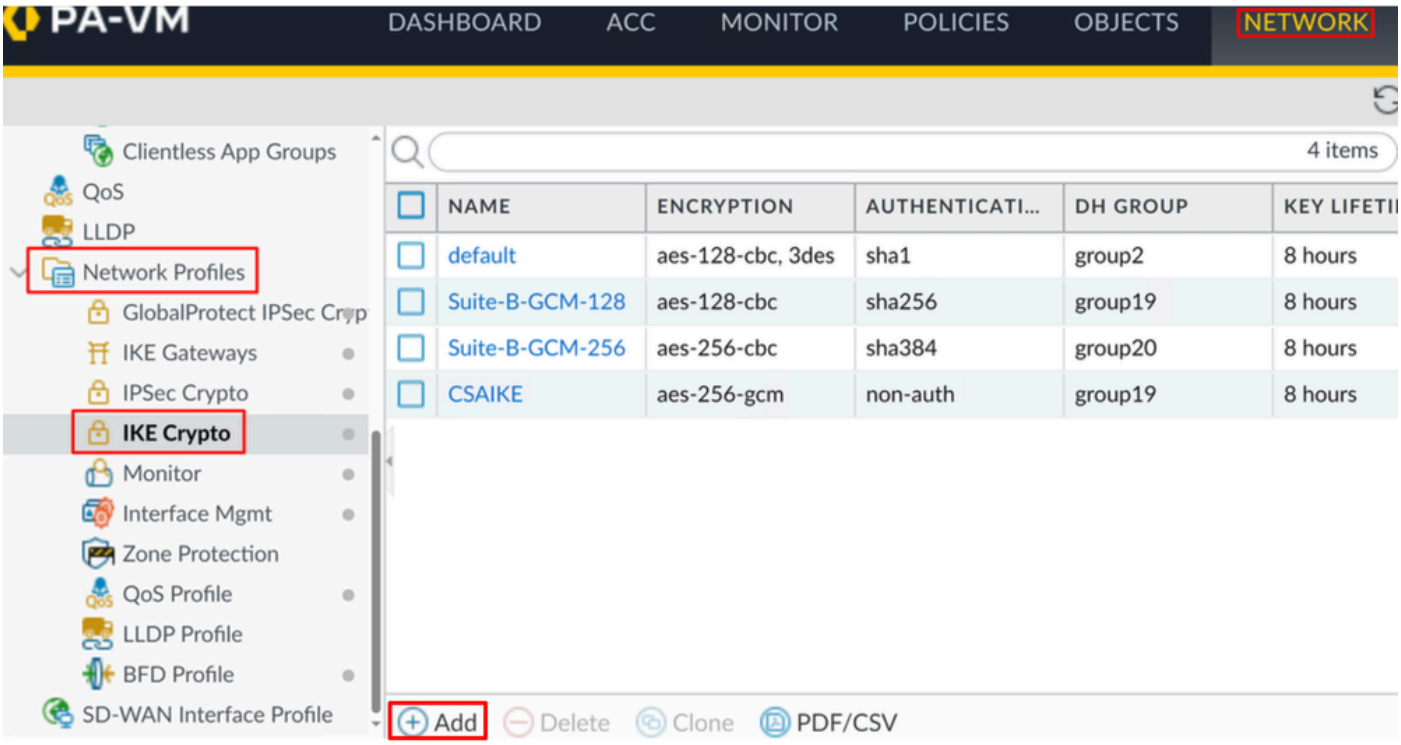


Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahrenConfigure IKE Crypto Profile.

IKE-Verschlüsselungsprofil konfigurieren

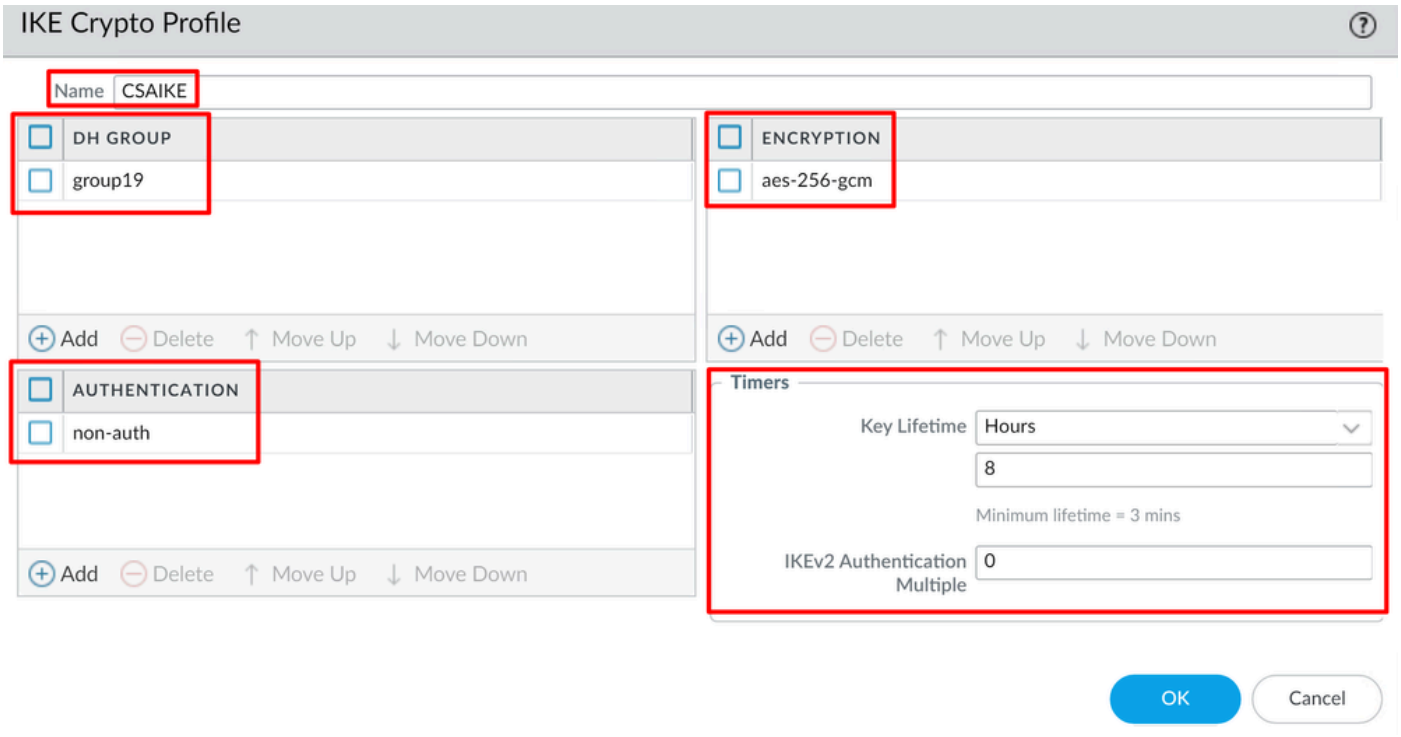
Um das Kryptografieprofil zu konfigurieren, navigieren Sie zu:

- Network > Network Profile > IKE Crypto
- Klicken Sie auf Add



- Konfigurieren Sie die folgenden Parameter:
    - **Name**: Konfigurieren Sie einen Namen zur Identifizierung des Profils.
        - **DH GROUP**: Gruppe19
        - **AUTHENTICATION**: nicht authentifiziert
        - **ENCRYPTION**: aes-256-gcm
        - Timers
            - Key Lifetime: 8 Stunden
                - **IKEv2 Authentication**:0

- Nachdem Sie alle Einstellungen konfiguriert haben, klicken Sie auf **OK**

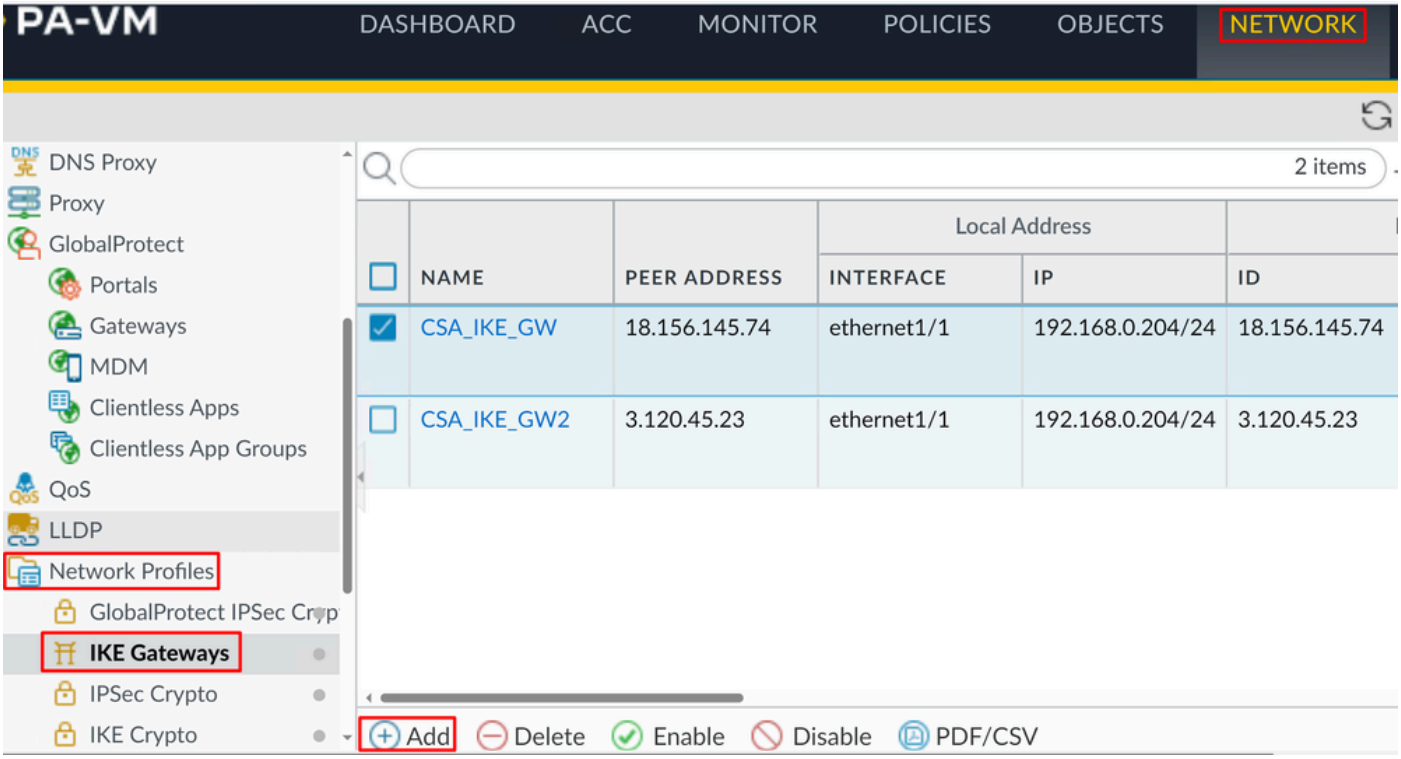


Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IKE Gateways.

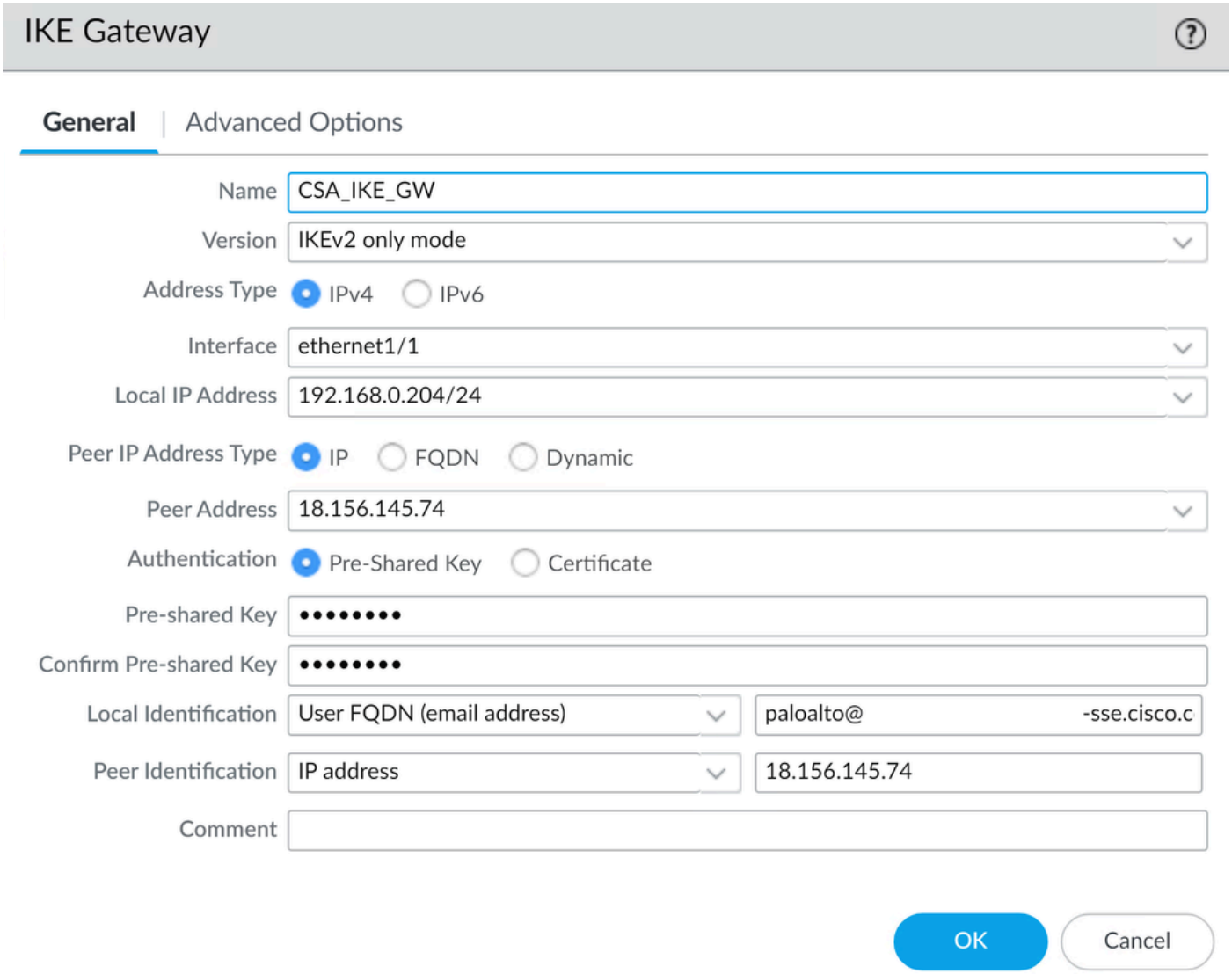
Konfigurieren von IKE-Gateways

IKE-Gateways konfigurieren

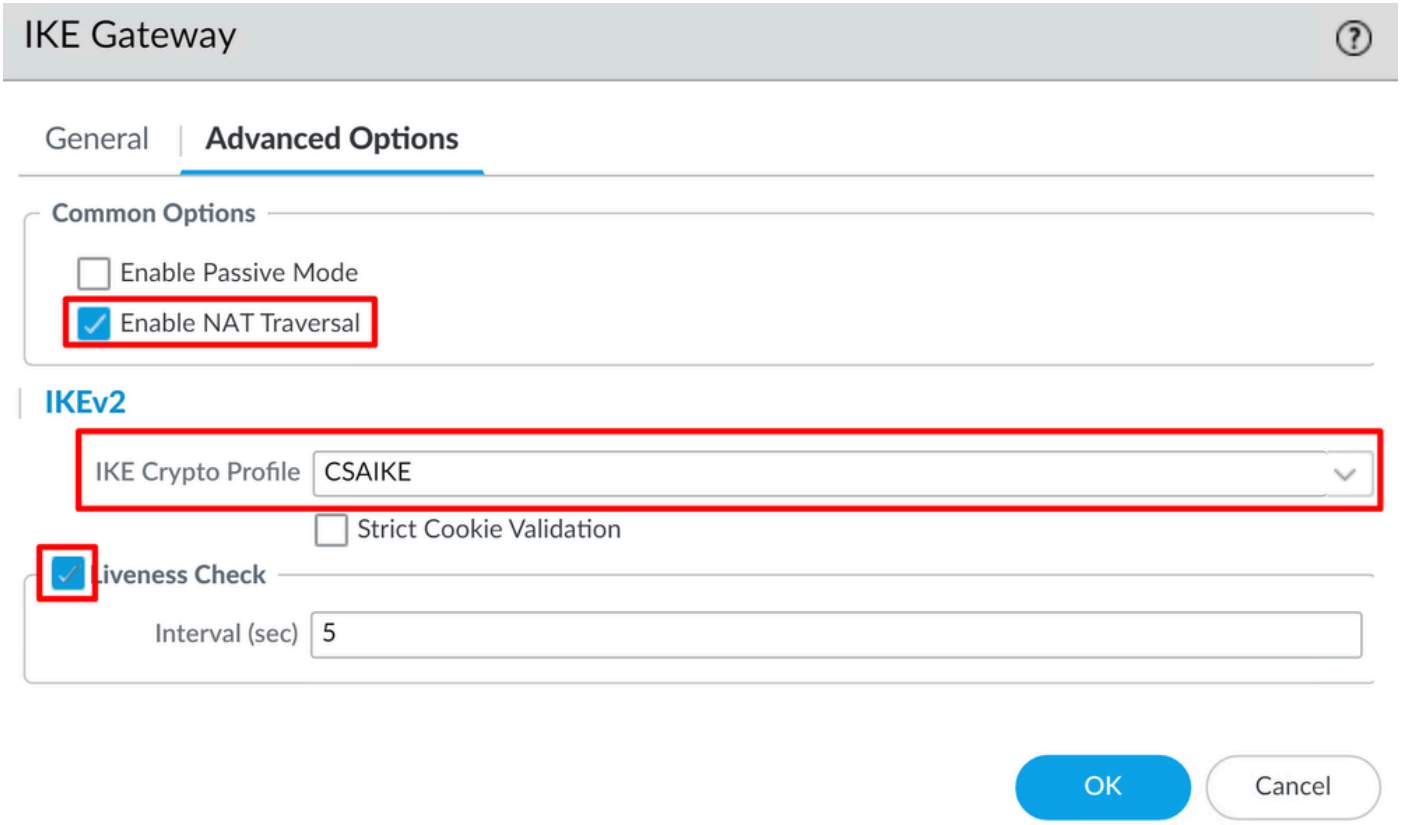
- Network > Network Profile > IKE Gateways
- Klicken Sie auf Add



- Konfigurieren Sie die folgenden Parameter:
    - Name: Konfigurieren Sie einen Namen, um die IKE-Gateways zu identifizieren.
        - **Version** : Nur IKEv2-Modus
        - Address Type :IPv4
        - **Interface** : Wählen Sie Ihre Internet-WAN-Schnittstelle aus.
        - Local IP Address: Wählen Sie die IP-Adresse Ihrer Internet-WAN-Schnittstelle aus.
        - **Peer IP Address Type** :IP
        - Peer Address: Verwenden Sie die IP-Adresse von Primary IP Datacenter IP Address, die im Schritt Tunneldaten angegeben ist.
        - Authentication: Vorläufiger gemeinsamer Schlüssel
        - Pre-shared Key : Verwenden Sie die im Schritt Tunneldaten **passphrase** angegebenen Daten.
        - **Confirm Pre-shared Key** : Verwenden Sie die im Schritt Tunneldaten **passphrase** angegebenen Daten.
        - **Local Identification** : Wählen Sie **User FQDN (Email address)** und verwenden Sie die **Primary Tunnel ID** im Schritt, Tunnel Data.
        - **Peer Identification** : IP AddressWählen und verwenden Sie den Primary IP Datacenter IP Address.



- Klicken Sie auf Advanced Options
    - **Enable NAT Traversal**
        - Wählen Sie die aus dem Schritt IKE-Verschlüsselungsprofil konfigurieren **IKE Crypto Profile** erstellte aus.
        - Aktivieren Sie das Kontrollkästchen für **Liveness Check**
        - Klicken Sie auf **OK**

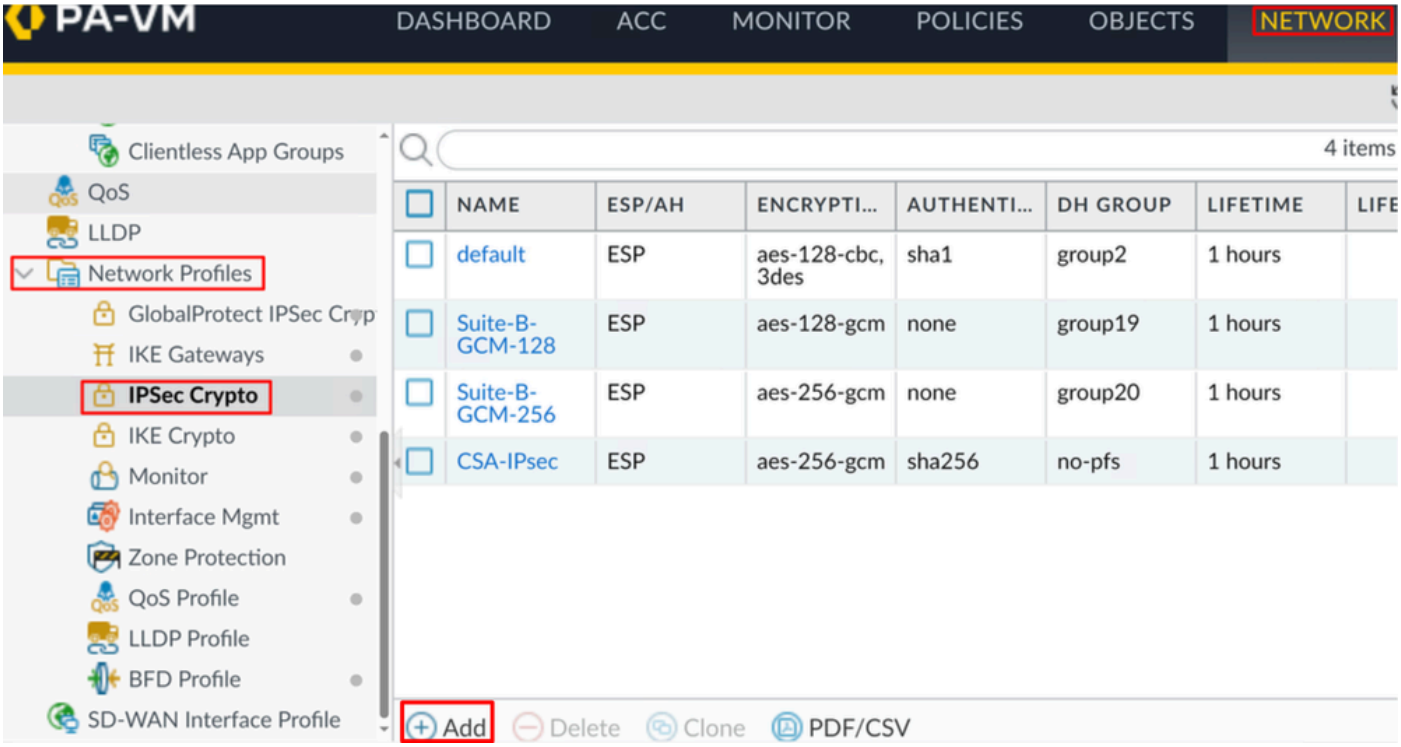


Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IPSEC Crypto.

IPSEC-Verschlüsselungsprofil konfigurieren

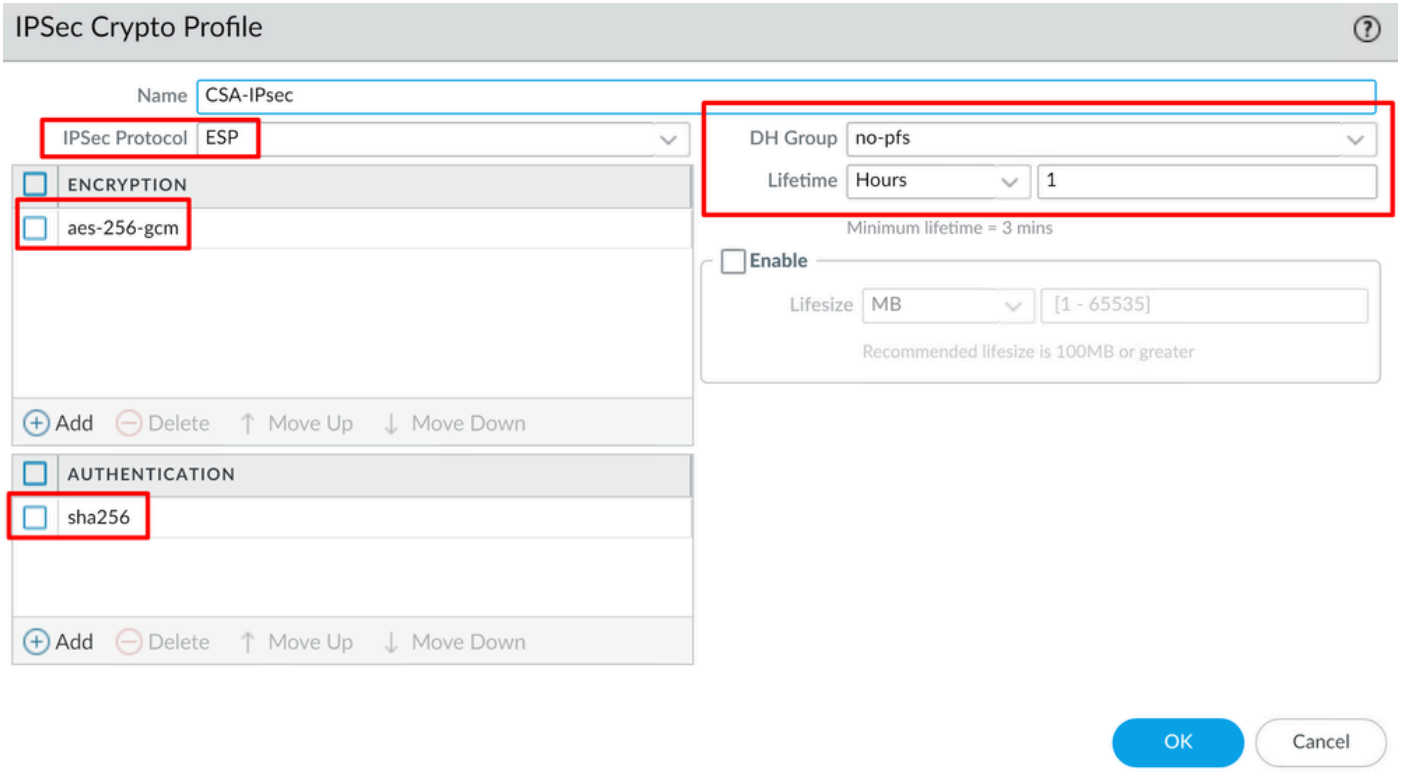
Zum Konfigurieren von IKE-Gateways navigieren Sie zu Network > Network Profile > IPSEC Crypto

- Klicken Sie auf Add



- Konfigurieren Sie die folgenden Parameter:
    - **Name**: Verwenden Sie einen Namen, um das IPsec-Profil für sicheren Zugriff zu identifizieren.
        - IPSec Protocol: ESP
        - **ENCRYPTION**: aes-256-gcm
        - DH Group: no-pfs, 1 Stunde

- Klicken Sie auf OK

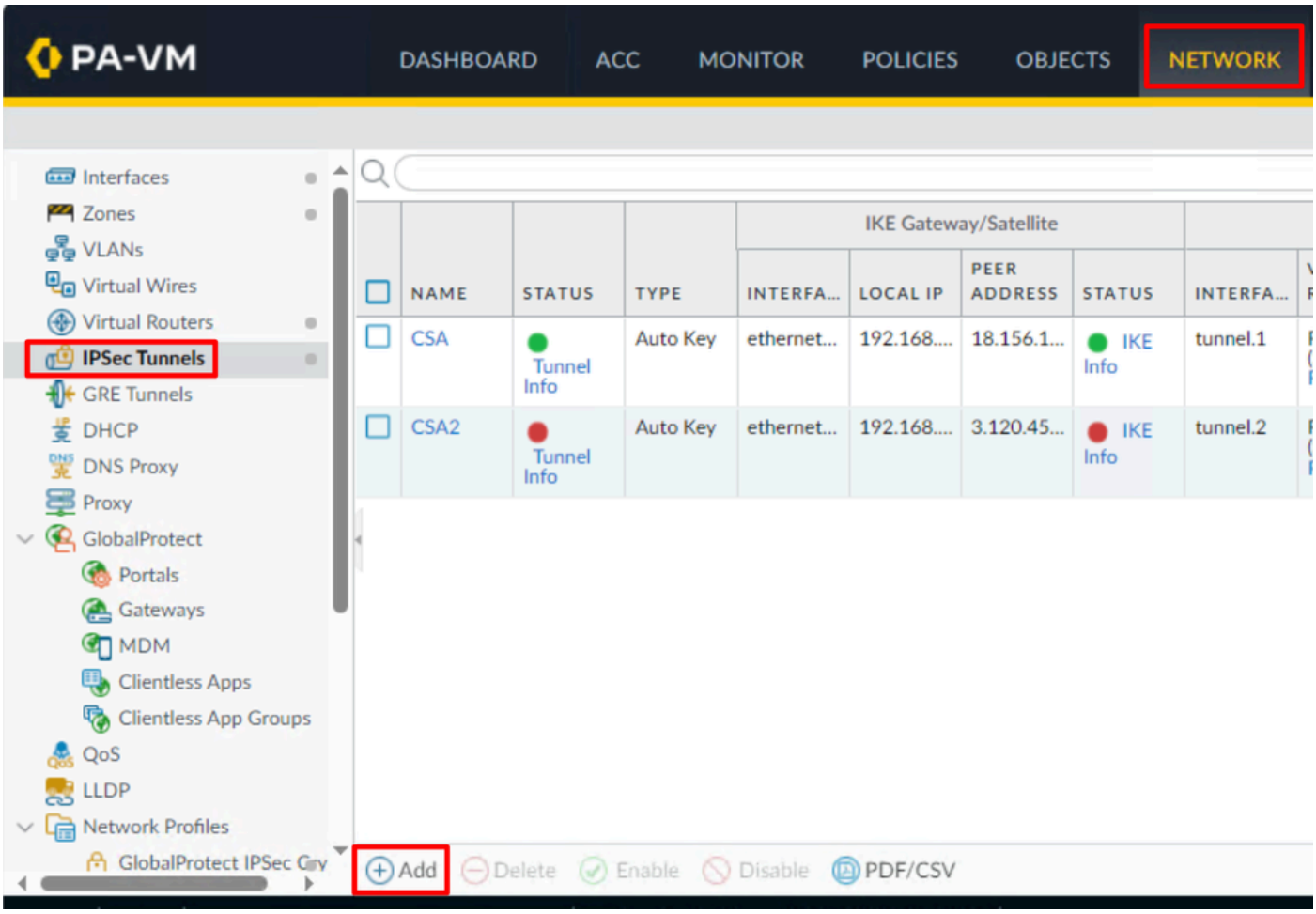


Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IPSec Tunnels.

Konfigurieren von IPSec-Tunneln

Navigieren Sie zum Konfigurieren **IPSec Tunnels**zu Network > IPSec Tunnels.

- Klicken Sie auf Add



- Konfigurieren Sie die folgenden Parameter:

  - **Name**: Verwenden Sie einen Namen, um den sicheren Zugriffstunnel zu identifizieren.

  - **Tunnel Interface**: Wählen Sie die Tunnelschnittstelle, die im Schritt konfiguriert wurde, Konfigurieren Sie die Tunnelschnittstelle.

  - **Type**: Auto-Taste

  - **Address Type**:IPv4

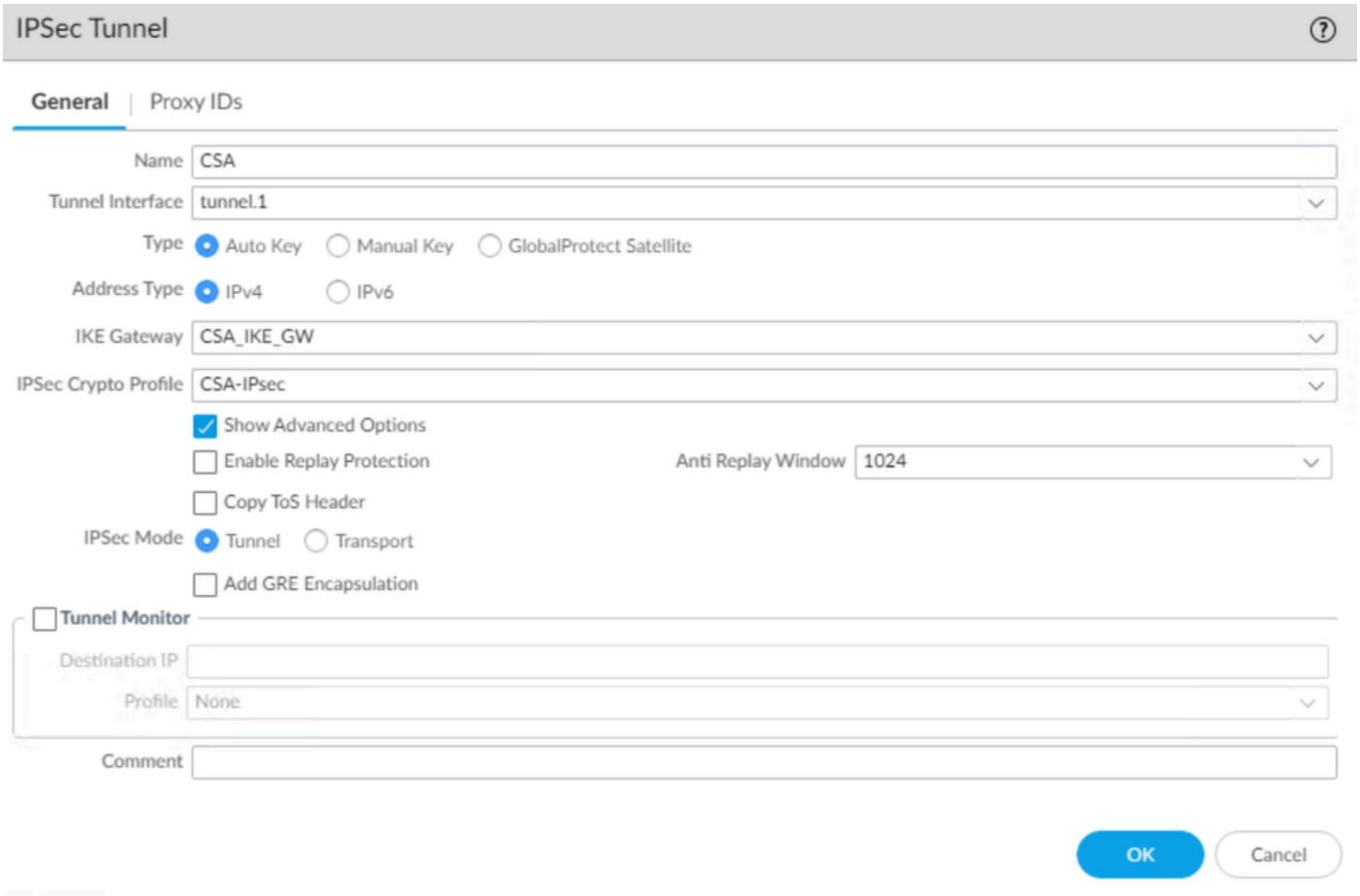
  - **IKE Gateways**: Wählen Sie die IKE-Gateways aus, die im Schritt konfiguriert wurden, Konfigurieren Sie IKE-Gateways.

  - **IPsec Crypto Profile**: Wählen Sie die IKE-Gateways aus, die auf dem Schritt konfiguriert wurden, und konfigurieren Sie das IPSEC-Kryptoprofil.

  - Aktivieren Sie das Kontrollkästchen für **Advanced Options**

    - **IPSec Mode Tunnel**: Wählen Sie Tunnel aus.

- Klicken Sie auf OK

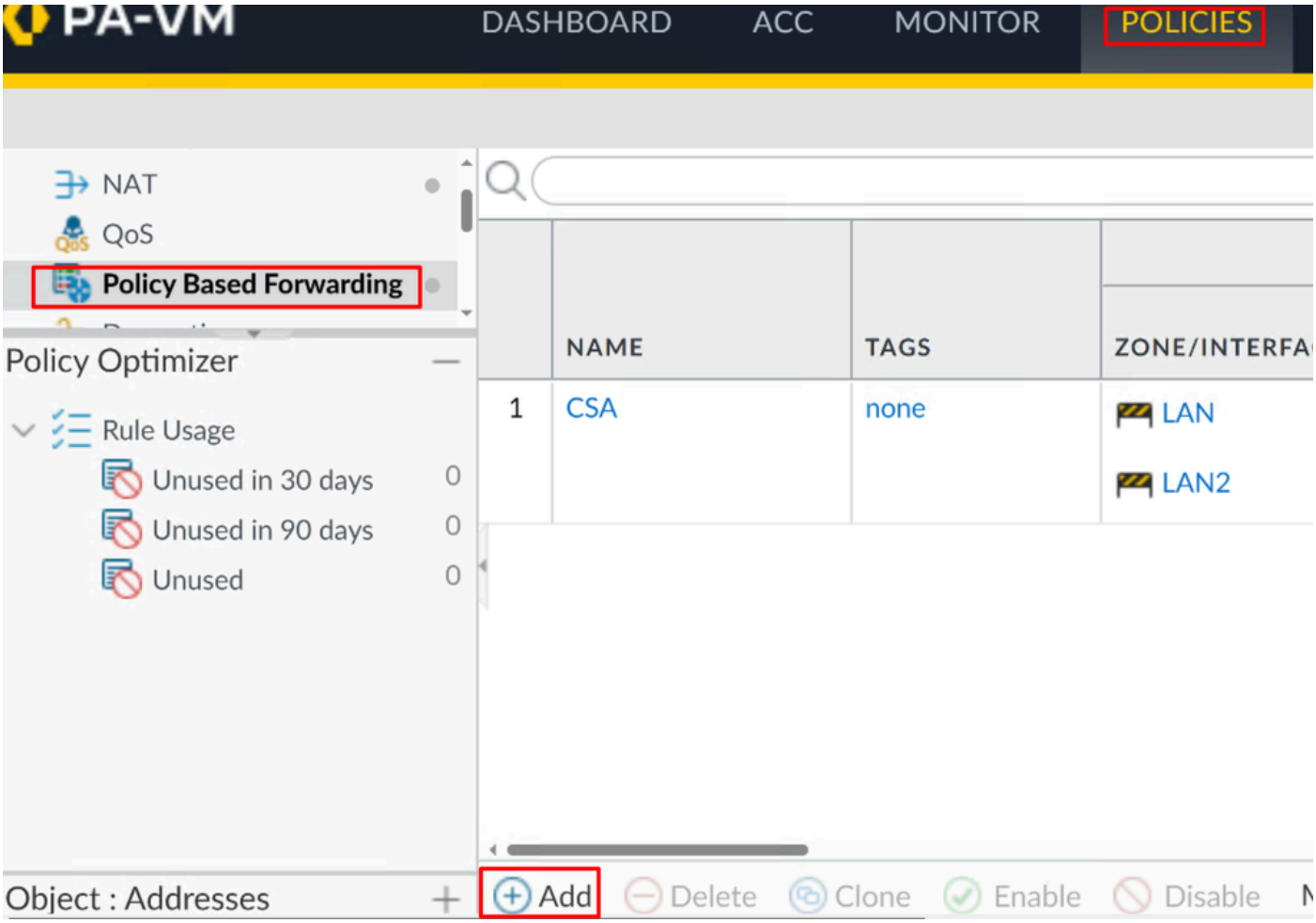


Nachdem Ihr VPN erfolgreich erstellt wurde, können Sie mit dem Schritt fortfahren **Configure Policy Based Forwarding**.

Richtlinienbasierte Weiterleitung konfigurieren

Navigieren Sie zum Konfigurieren **Policy Based Forwarding**zu Policies > Policy Based Forwarding.

- Klicken Sie auf Add

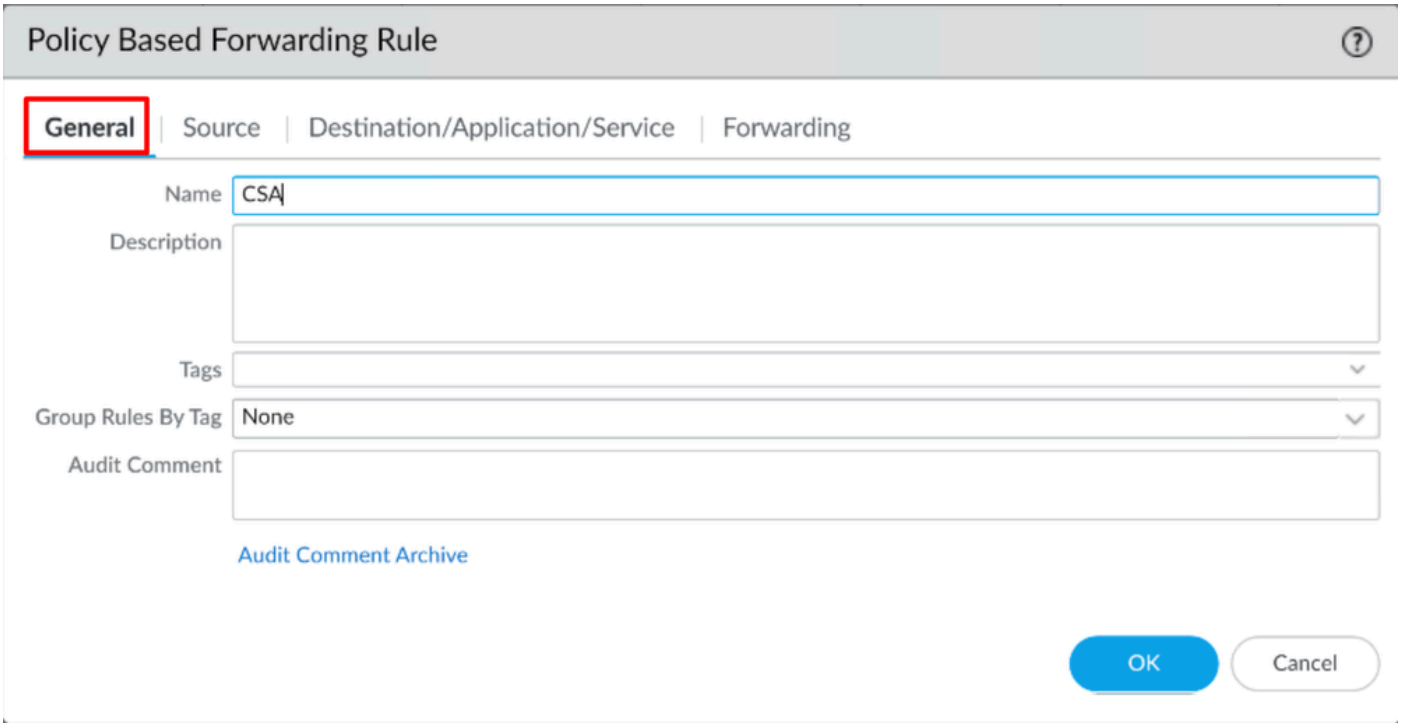


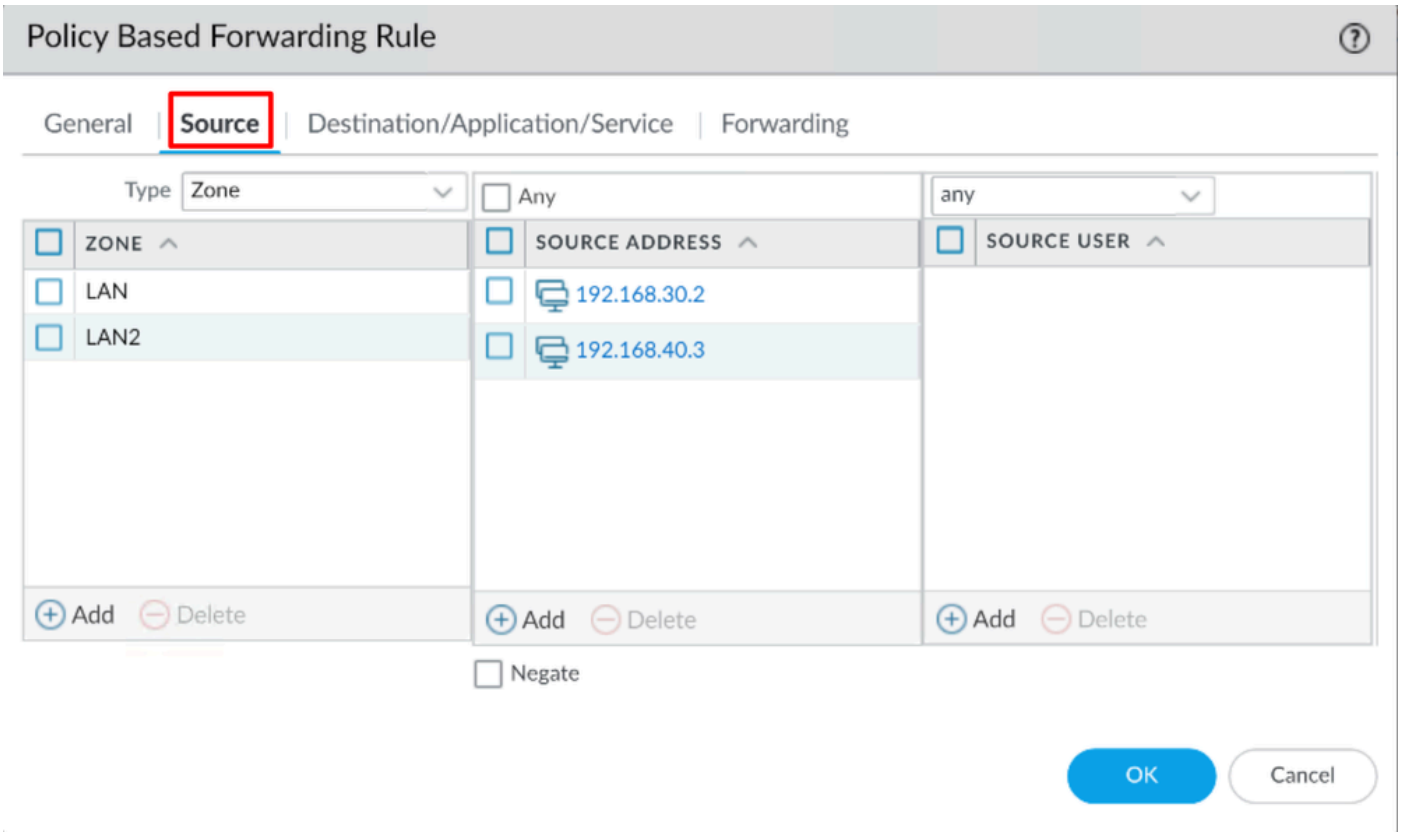
- Konfigurieren Sie die folgenden Parameter:
  - General
    - **Name**: Verwenden Sie einen Namen, um den sicheren Zugriff zu identifizieren, Policy Base Forwarding (Routing nach Ursprung)

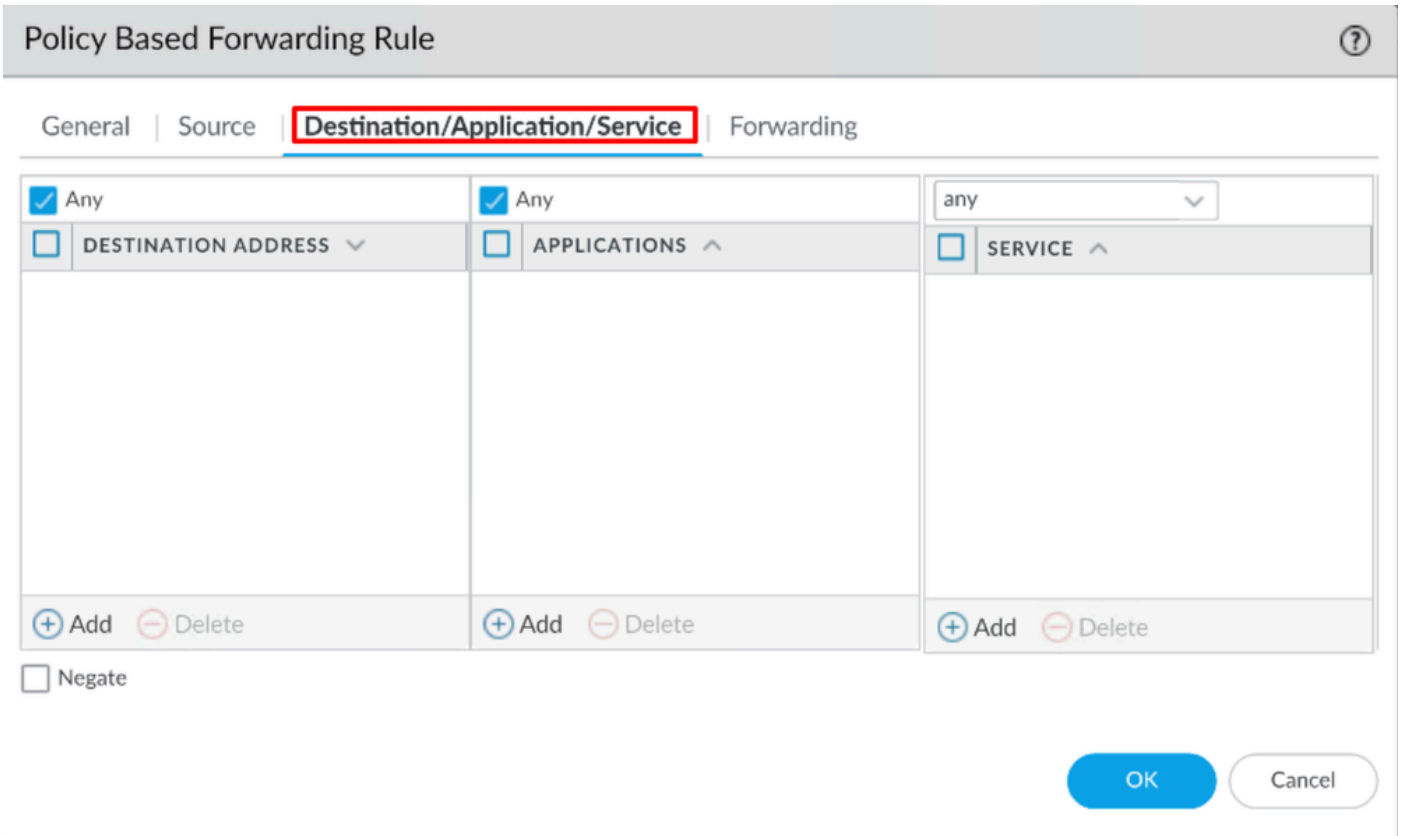
- Source
  - **Zone**: Wählen Sie die Zonen aus, in denen Sie den Datenverkehr basierend auf dem Ursprung weiterleiten möchten.
    - **Source Address**: Konfigurieren Sie den Host oder die Netzwerke, die Sie als Quelle verwenden möchten.
    - Source Users: Konfigurieren Sie die Benutzer, die den Datenverkehr weiterleiten sollen (nur falls zutreffend).

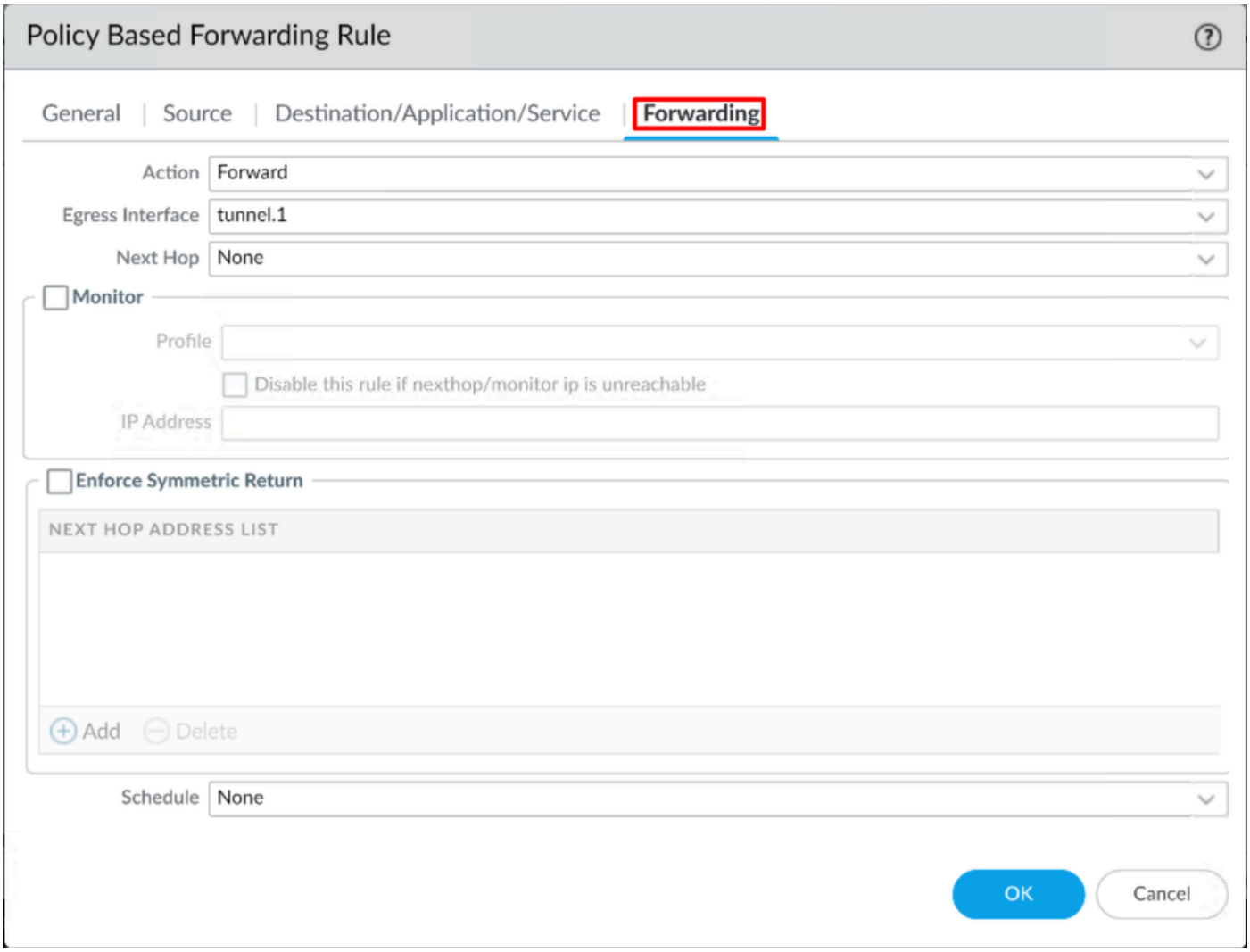
- Destination/Application/Service
    - Destination Address: Sie können es als Any (Beliebig) belassen oder die Adressbereiche von Secure Access (100.64.0.0/10) angeben.
- Forwarding
    - **Action**: Weiterleiten
        - **Egress Interface**: Wählen Sie die Tunnelschnittstelle, die im Schritt konfiguriert wurde, Konfigurieren Sie die Tunnelschnittstelle.
        - **Next Hop**:None

- KlickenOK und 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



Jetzt haben Sie alles auf Palo Alto konfiguriert. Nachdem Sie die Route konfiguriert haben, kann der Tunnel eingerichtet werden, und Sie müssen die Konfiguration des RA-VPN, der browserbasierten ZTA oder der Client Base ZTA auf dem Secure Access Dashboard fortsetzen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.