Palo Altoファイアウォールを使用したセキュアアクセスの設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

設定

- セキュアアクセスでのVPNの設定
  - トンネルデータ
- Palo Altoでのトンネルの設定
  - トンネルインターフェイスの設定
  - IKE暗号化プロファイルの設定
  - IKEゲートウェイの設定
  - IPSEC暗号化プロファイルの設定
  - IPSecトンネルの設定
  - ポリシーベースの転送の設定

はじめに

このドキュメントでは、Palo Altoファイアウォールを使用してセキュアアクセスを設定する方法について説明します。

前提条件

- ユーザプロビジョニングの設定
- ZTNA SSO認証設定
- リモートアクセスVPNセキュアアクセスの設定

要件

次の項目に関する知識があることが推奨されます。

- Palo Alto 11.xバージョンのファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Palo Alto 11.xバージョンのファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

シスコは、プライベートアプリケーション（オンプレミスとクラウドベースの両方）を保護し、アクセスを提供するセキュアなアクセスを設計しました。また、ネットワークからインターネットへの接続も保護します。これは、複数のセキュリティ方式とレイヤの実装によって実現されます。すべての目的は、クラウド経由でアクセスする情報を保持することです。

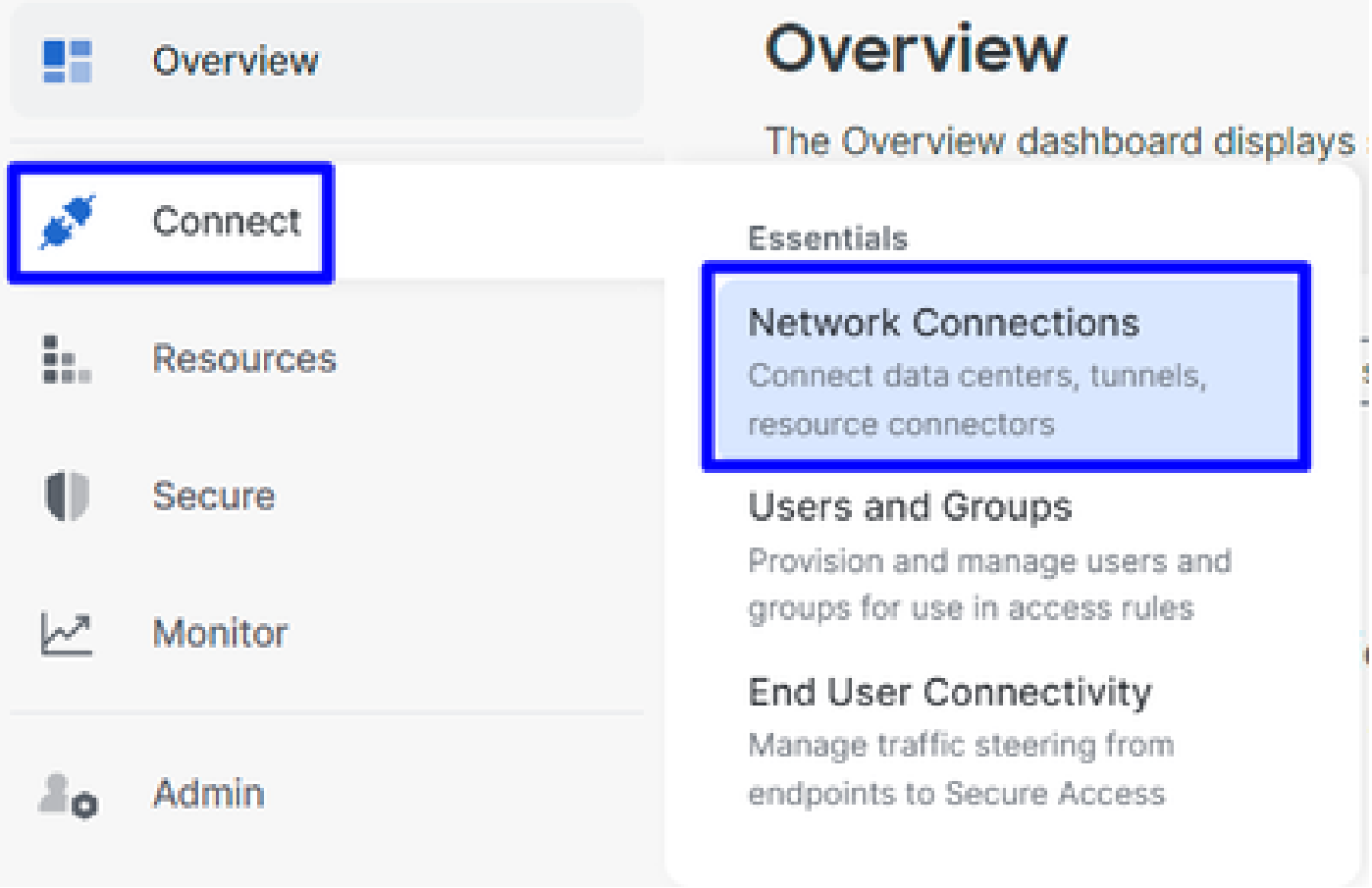
設定

セキュアアクセスでのVPNの設定

Secure Accessの管理パネルに移動します。

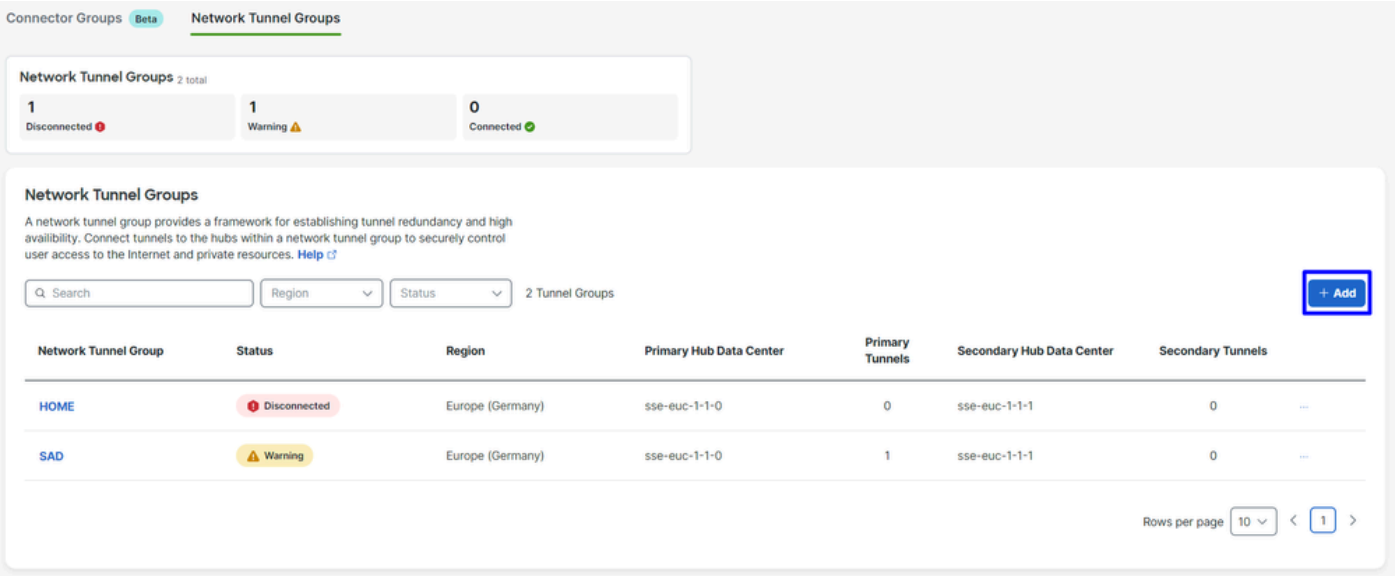
セキュアアクセス – メインページ

- クリック Connect > Network Connections



セキュアアクセス – ネットワーク接続

- 「Network Tunnel Groups」で、 + Add



セキュアアクセス – ネットワークトンネルグループ

- Tunnel Group Name、Regionの設定 Device Type
- クリック **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

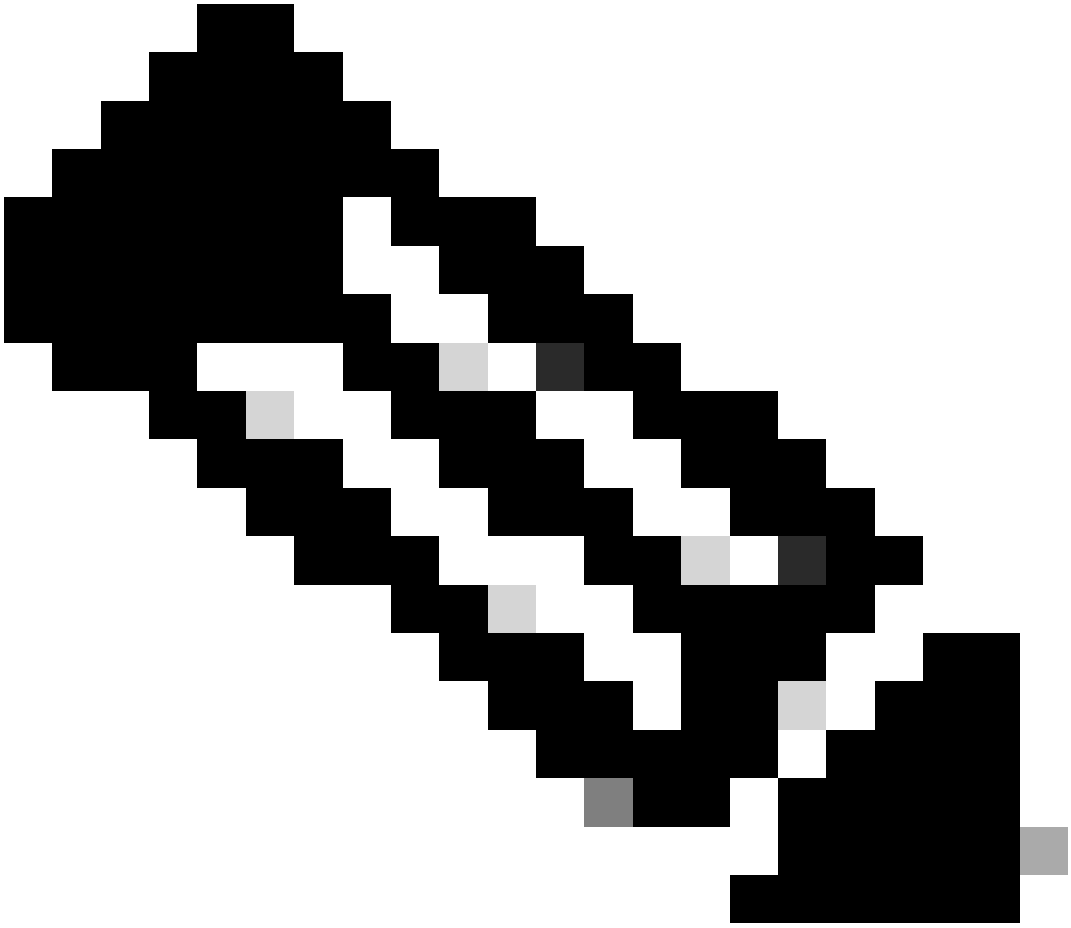
Europe (Germany)

Device Type

Other

Cancel

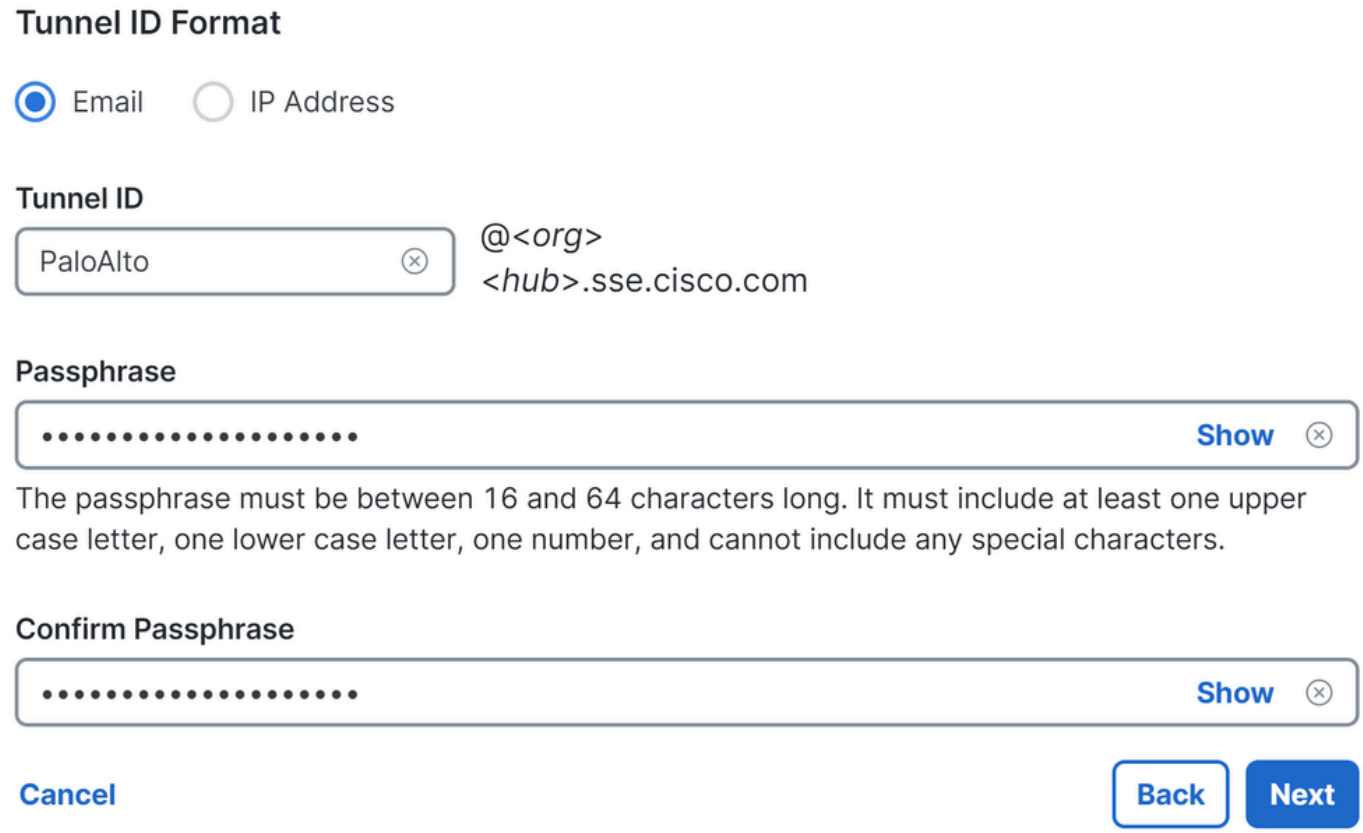
Next



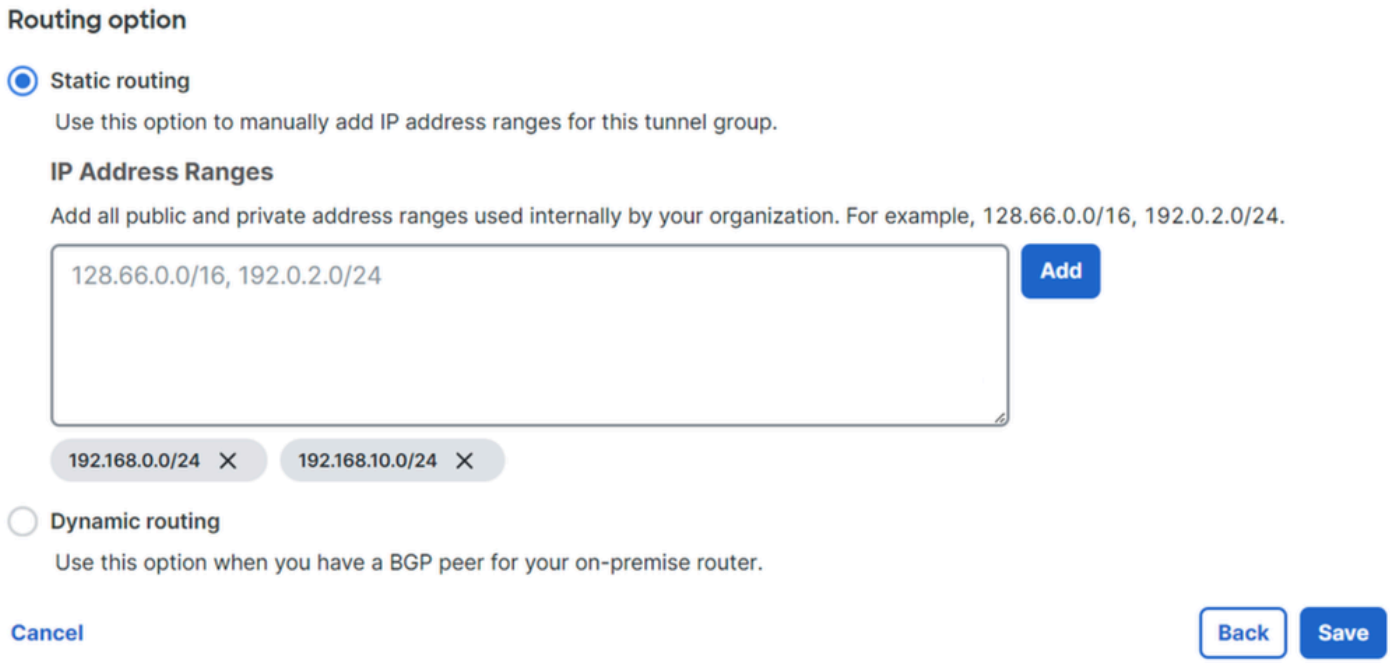
注：ファイアウォールの場所に最も近い地域を選択します。

Tunnel ID Format

- コマンドと Passphrase
- クリック Next



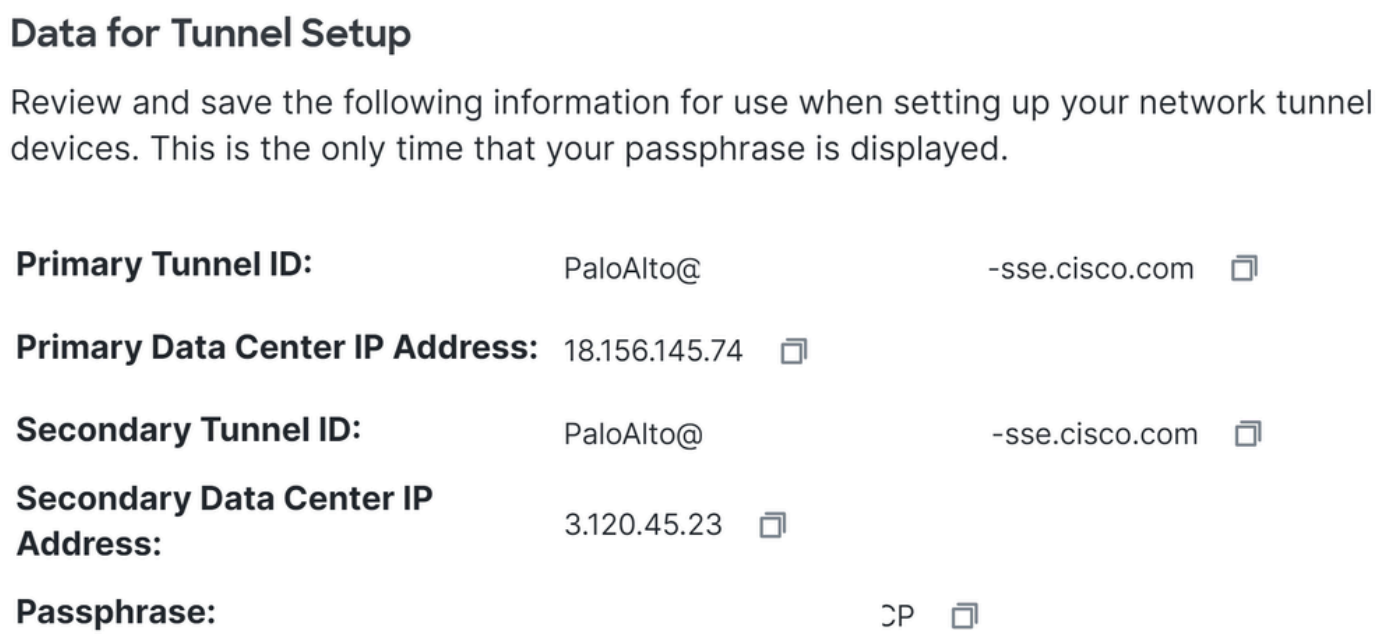
- ネットワークで設定したIPアドレス範囲またはホストを設定し、トラフィックをセキュアアクセス経由で通過させる
- クリック **Save**



セキュアアクセス – トンネルグループ – ルーティングオプション

トンネルに関す**Save** る情報をクリックして表示した後、次の手順**Configure the tunnel on Palo Alto**でその情報を保存してください。

トンネルデータ

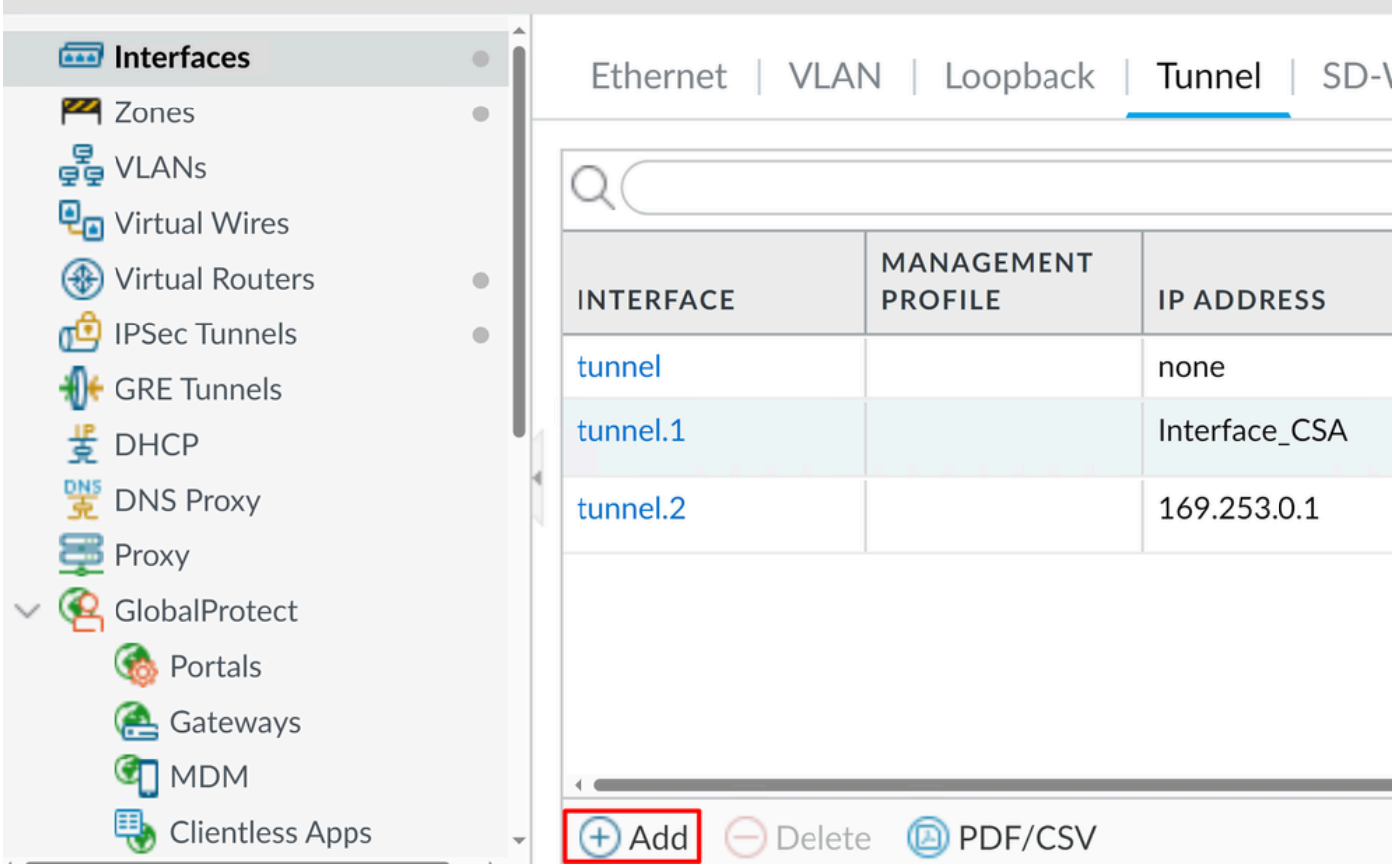


Palo Altoでのトンネルの設定

トンネルインターフェイスの設定

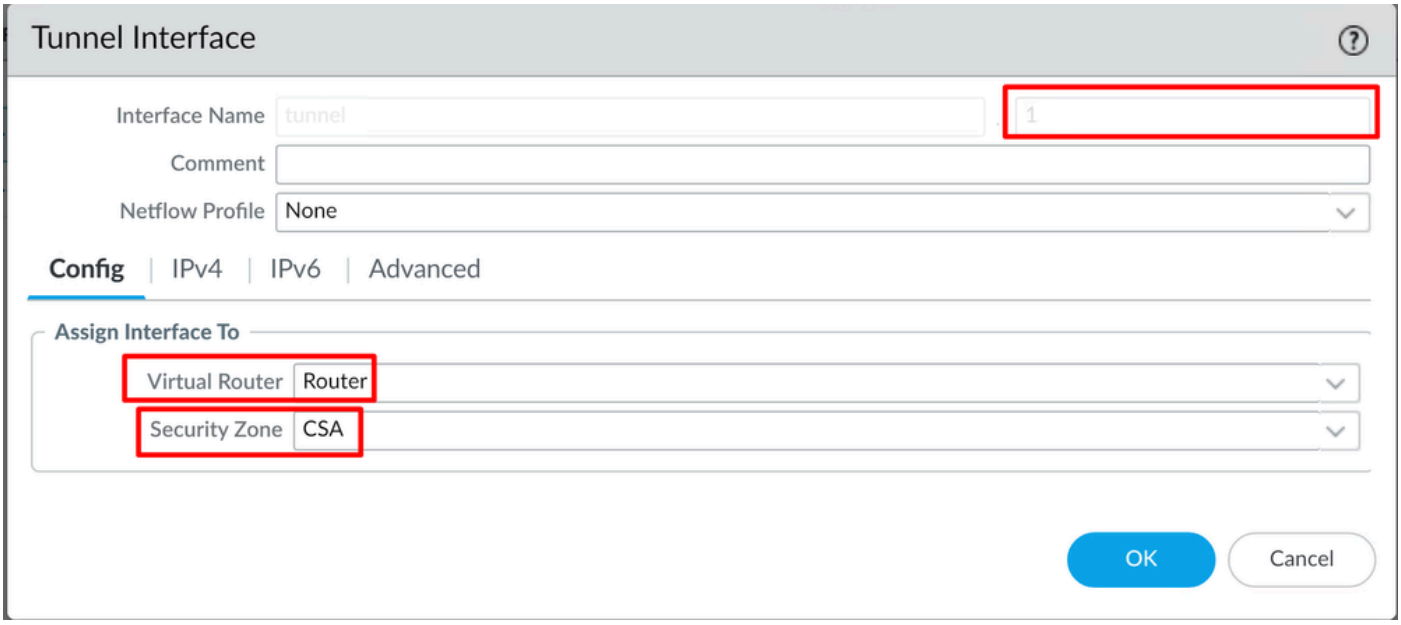
Palo Altoダッシュボードに移動します。

- Network > Interfaces > Tunnel
- Click Add

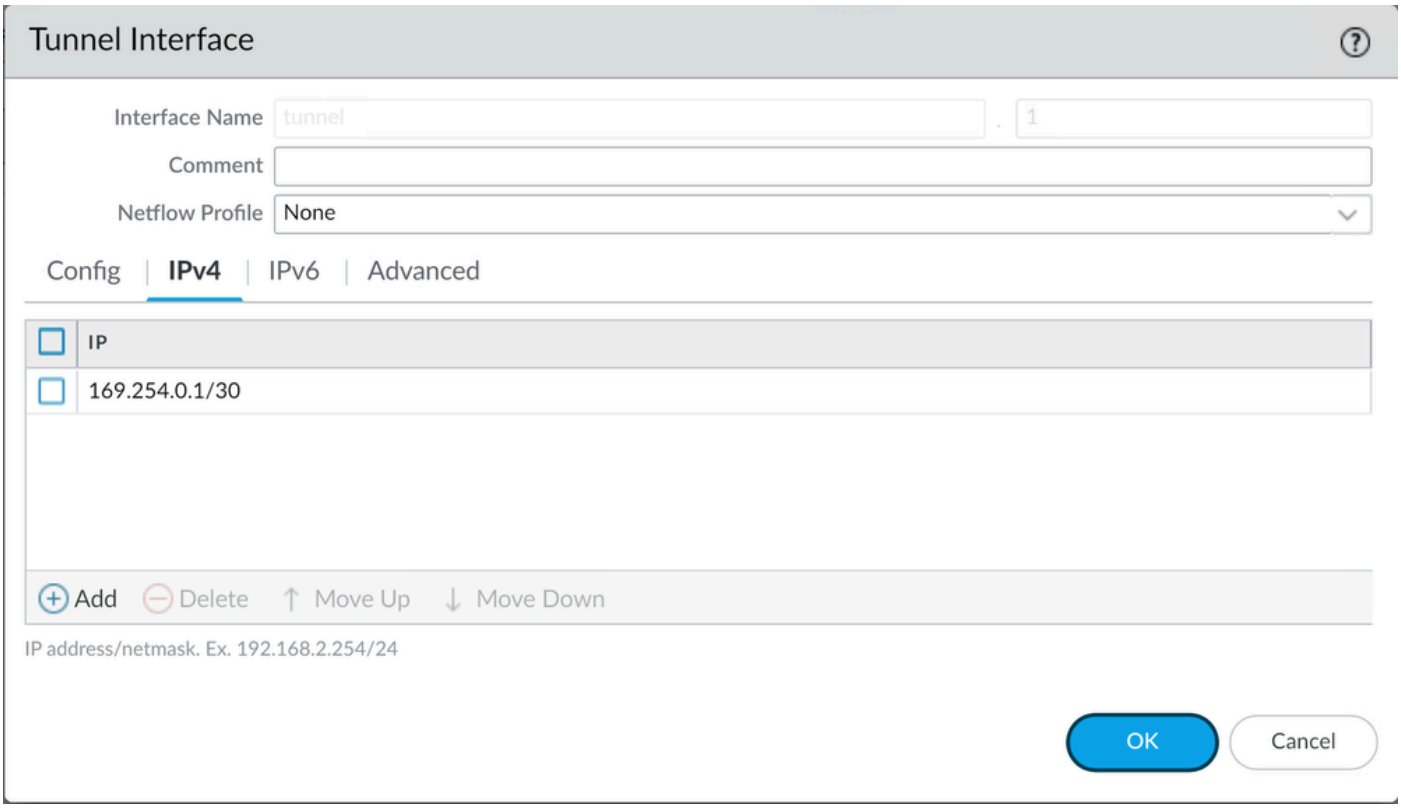


- Configメニューで Virtual Router、Security Zoneを設定し、Suffix Number

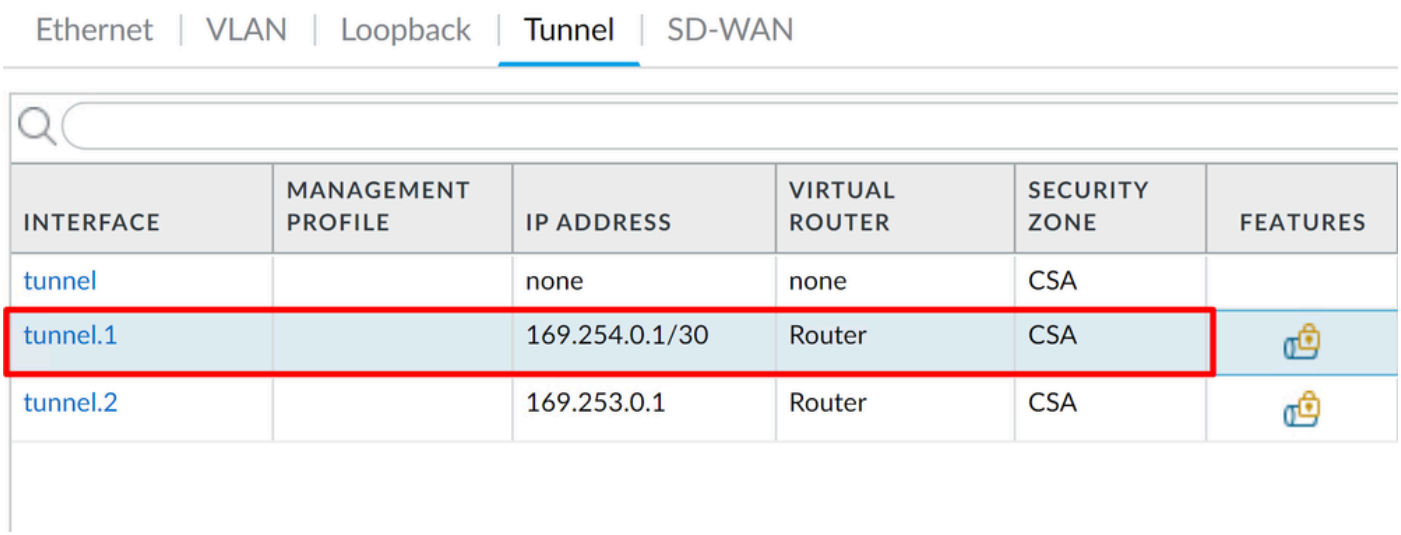
IPv4



- の下で、ルーティング不能IPを設定します。たとえば、 169.254.0.1/30
- クリックOK



その後、次のように設定できます。

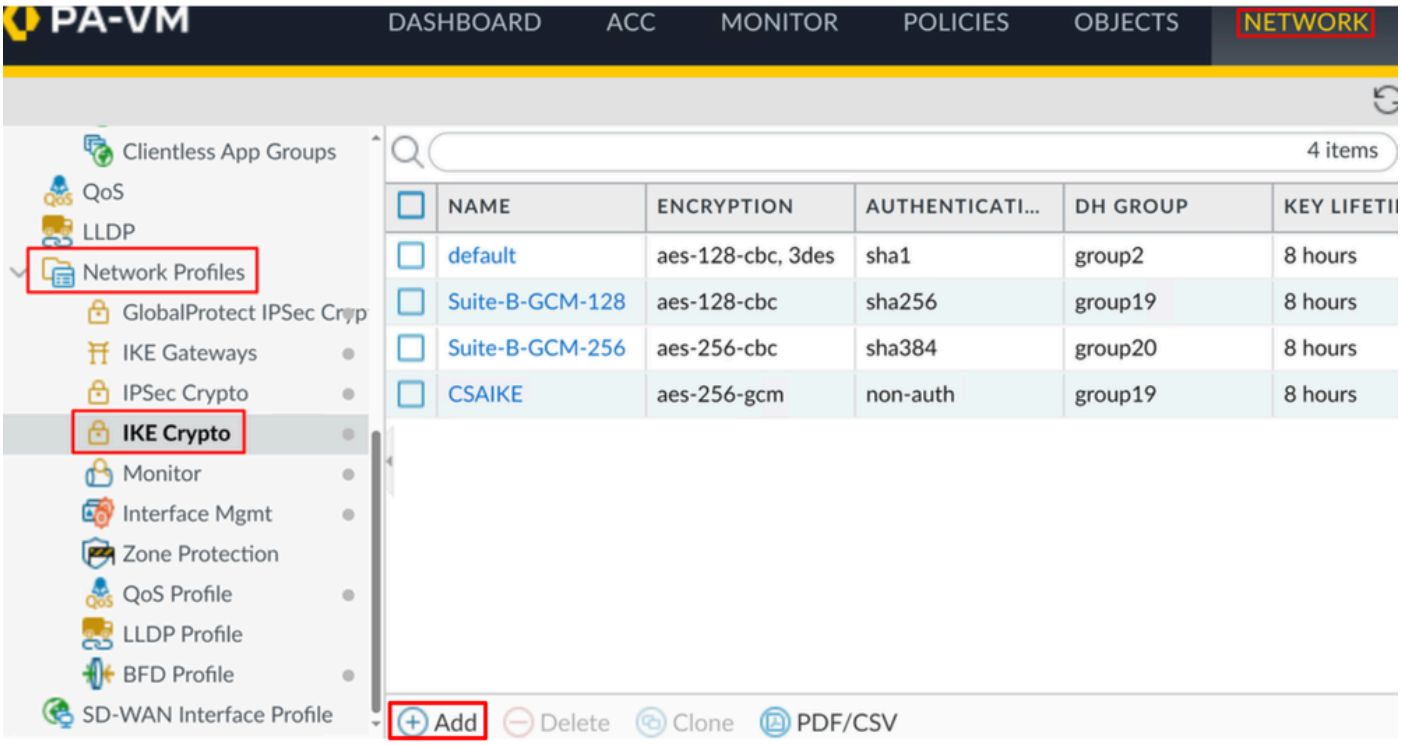


このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップConfigure IKE Crypto Profileに進みます。

IKE暗号化プロファイルの設定

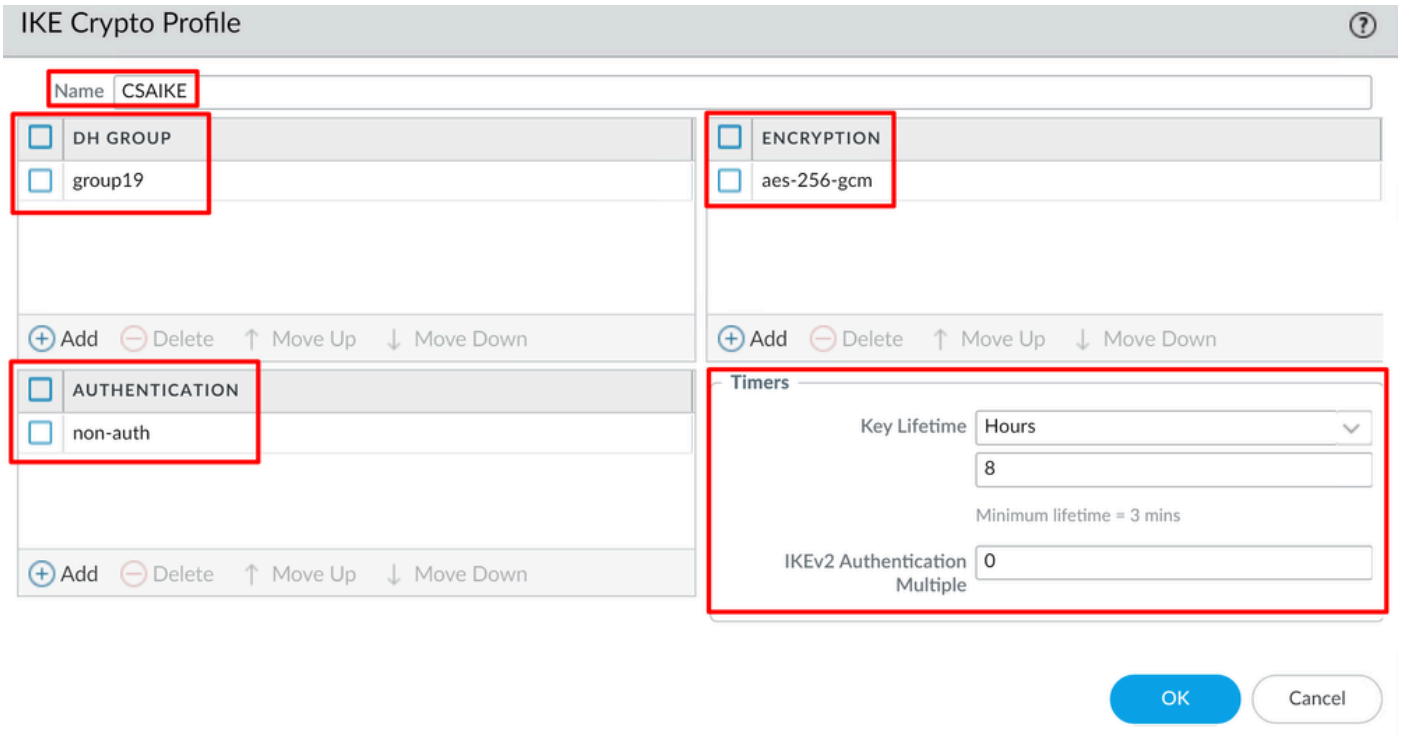
暗号化プロファイルを設定するには、次の場所に移動します。

- Network > Network Profile > IKE Crypto
- クリックAdd



- 次のパラメータを設定します。
    - **Name**：プロファイルを識別するための名前を設定します。
        - **DH GROUP**：グループ19
        - **AUTHENTICATION**：非認証
        - **ENCRYPTION**: aes-256-gcm
        - Timers
            - Key Lifetime:8 時間
                - **IKEv2 Authentication**:0

- すべての設定が完了したら、 **OK**

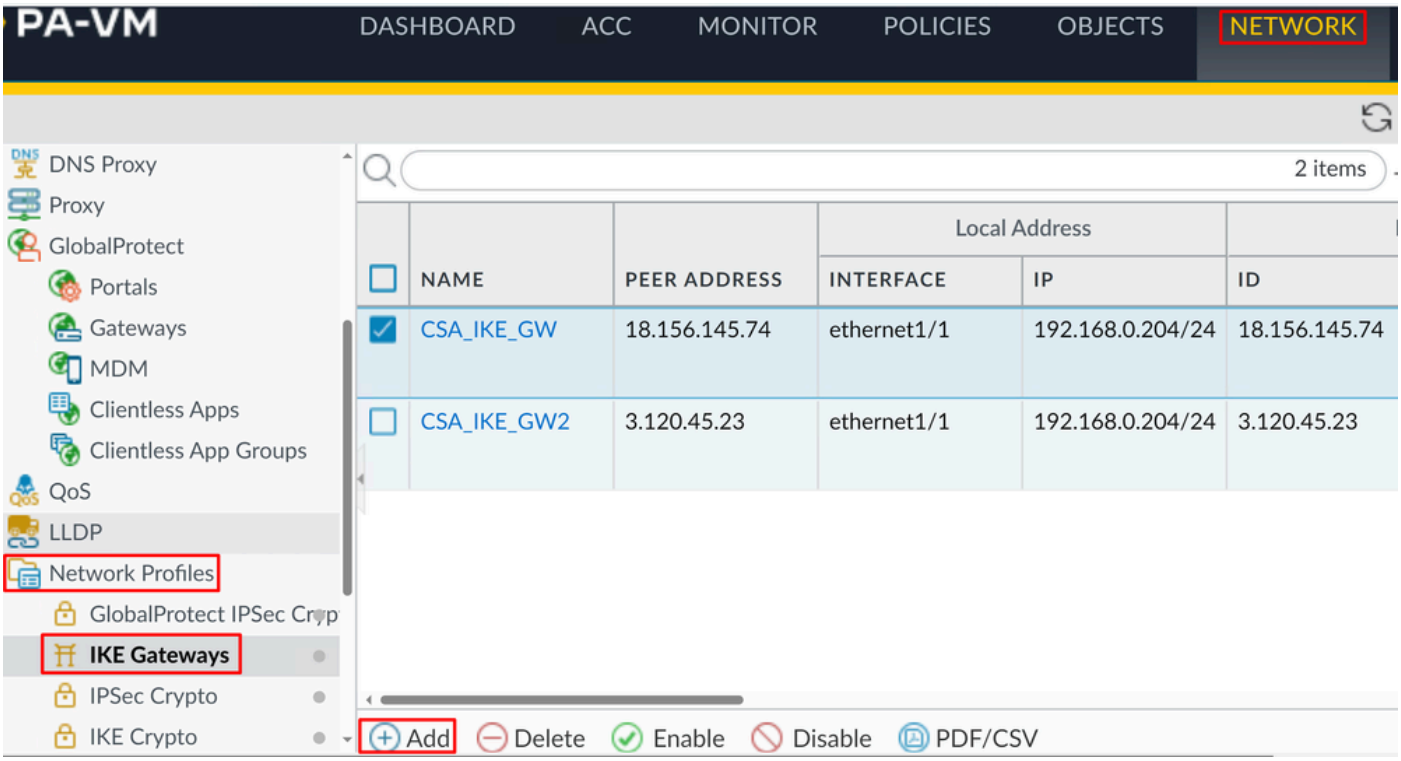


このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。 Configure IKE Gateways.

IKEゲートウェイの設定

IKEゲートウェイを設定するには

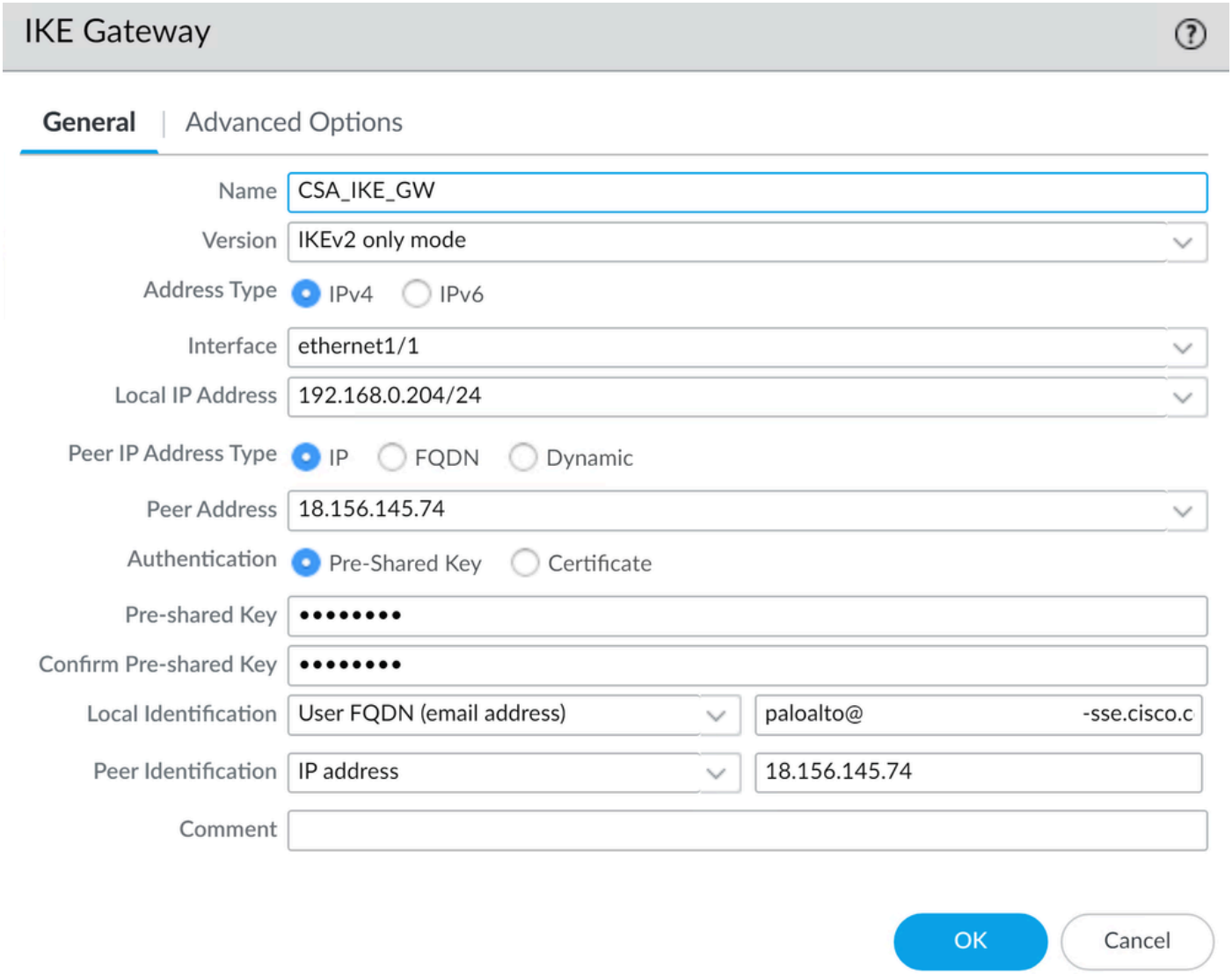
- Network > Network Profile > IKE Gateways
- クリックAdd



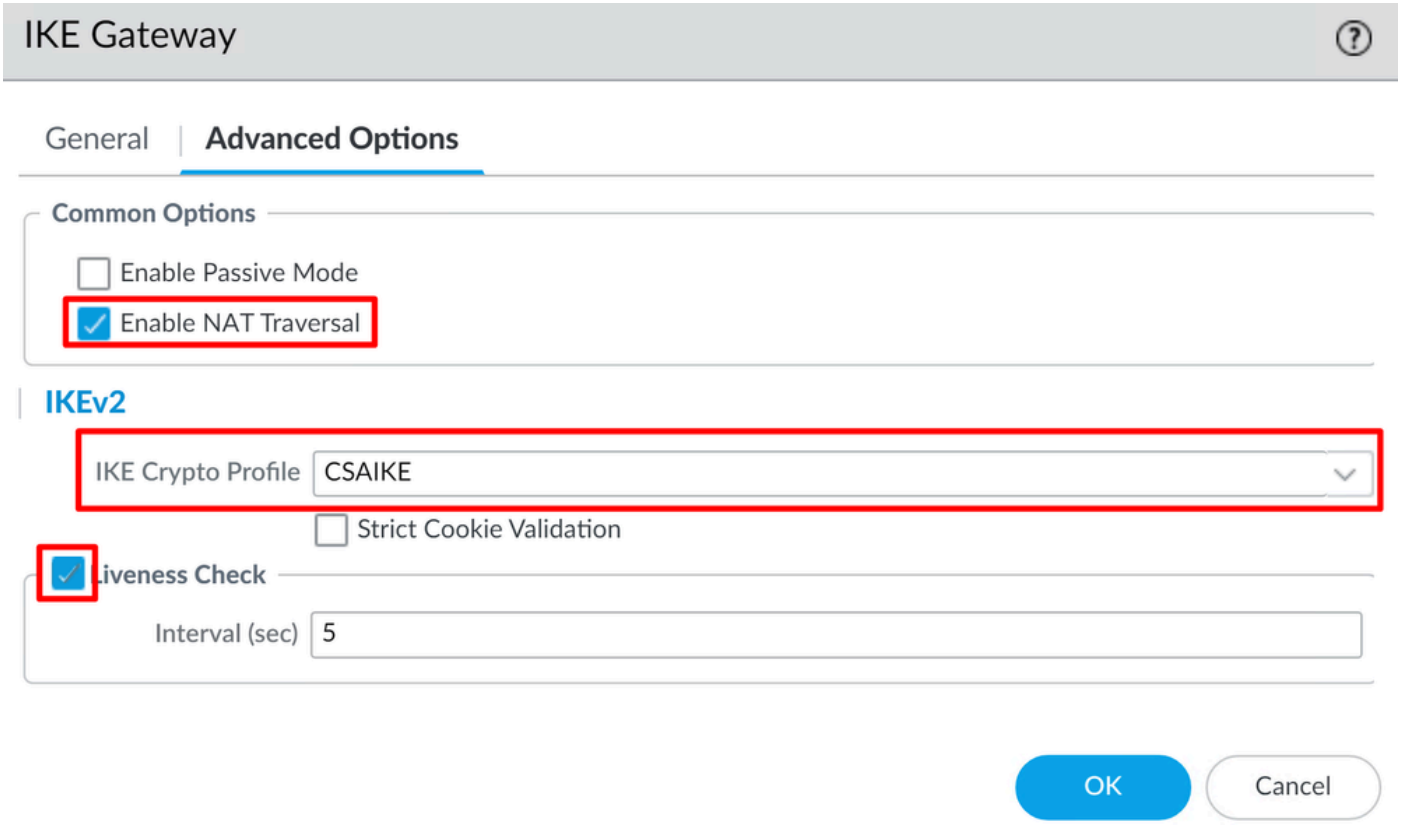
- 次のパラメータを設定します。

  - Name:Ikeゲートウェイを識別するための名前を設定します。

    - **Version** : IKEv2専用モード
    - Address Type : IPv4
    - **Interface** ：インターネットWANインターフェイスを選択します。
    - Local IP Address：インターネットWANインターフェイスのIPを選択します。
    - **Peer IP Address Type** :IP
    - Peer Address:手順「Tunnel Data」で指定したPrimary IP Datacenter IP AddressのIPを使用します。
    - Authentication:Pre-Shared Key
    - Pre-shared Key : Tunnel Dataの手順で指定した **passphrase** を使用します。
    - **Confirm Pre-shared Key** : Tunnel Dataの手順で指定した **passphrase** を使用します。
    - **Local Identification** ：を選択**User FQDN (Email address)** し、手順「Tunnel Data」で指定した**Primary Tunnel ID** を使用します。
    - **Peer Identification** : IP Addressを選択してPrimary IP Datacenter IP Addressを使用します。



- クリックAdvanced Options
    - **Enable NAT Traversal**
        - ステップConfigure IKE Crypto Profileで作**IKE Crypto Profile** 成した
        - チェックボックスをオンにする **Liveness Check**
        - クリック **OK**

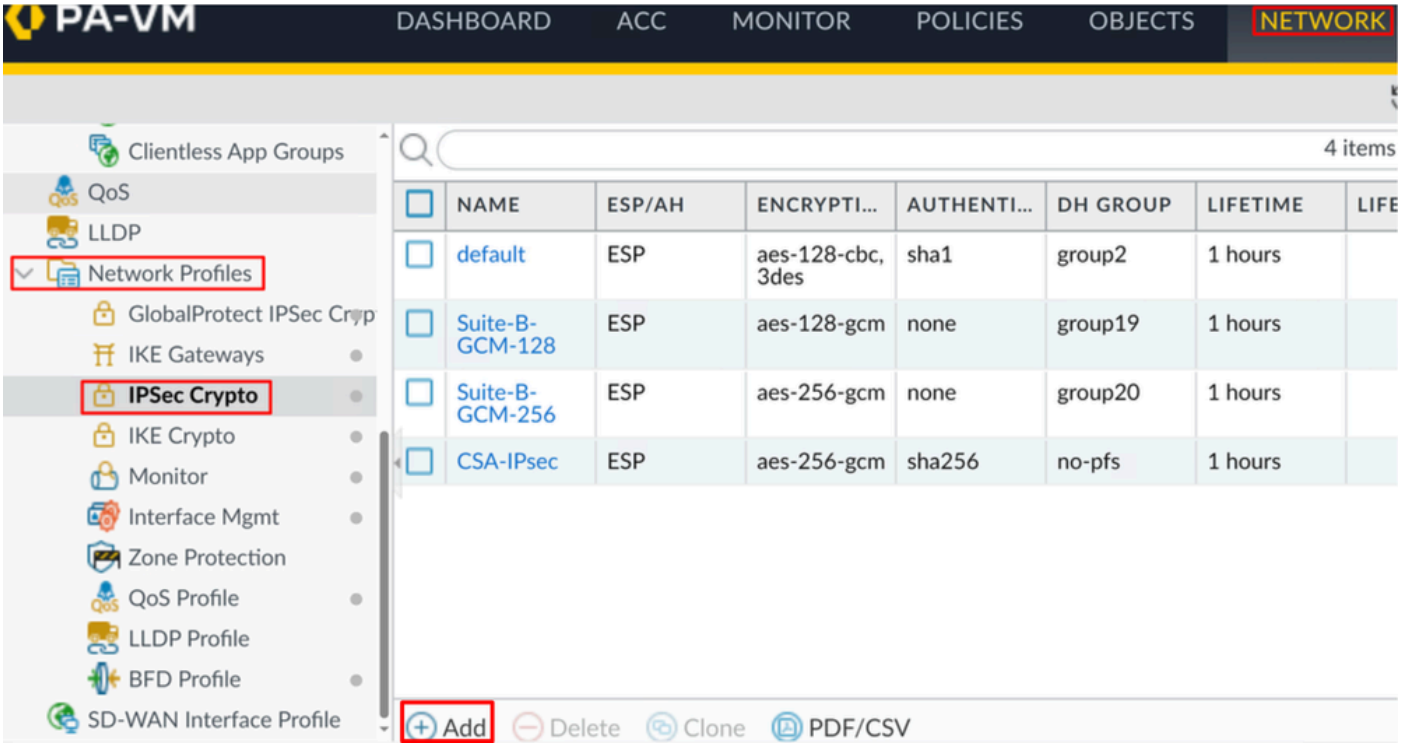


このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。 Configure IPSEC Crypto.

IPSEC暗号化プロファイルの設定

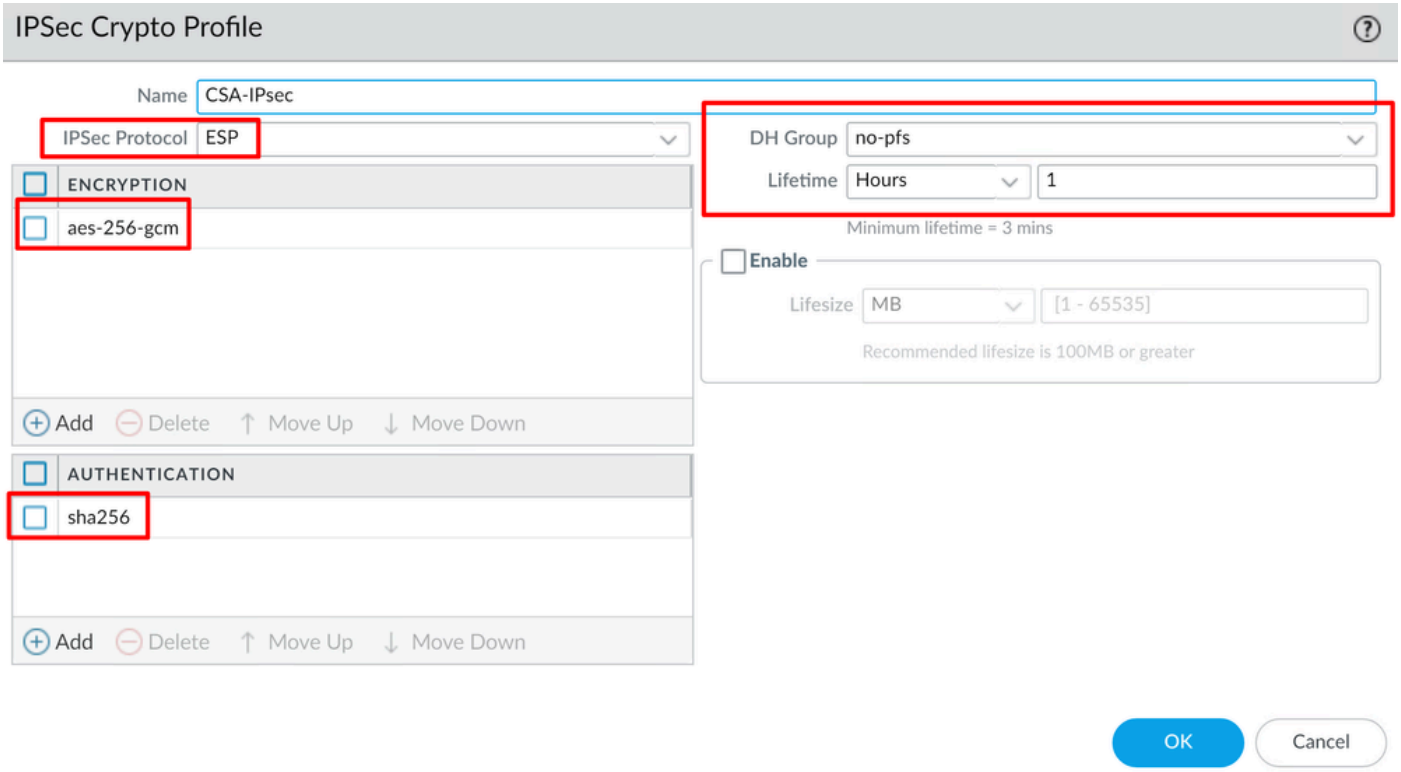
IKEゲートウェイを設定するには、 Network > Network Profile > IPSEC Crypto

- クリックAdd



- 次のパラメータを設定します。
    - **Name**：名前を使用してセキュアアクセスIPsecプロファイルを識別します。
        - IPSec Protocol:ESP
        - **ENCRYPTION**: aes-256-gcm
        - DH Group: pfsなし、1時間

- クリック OK

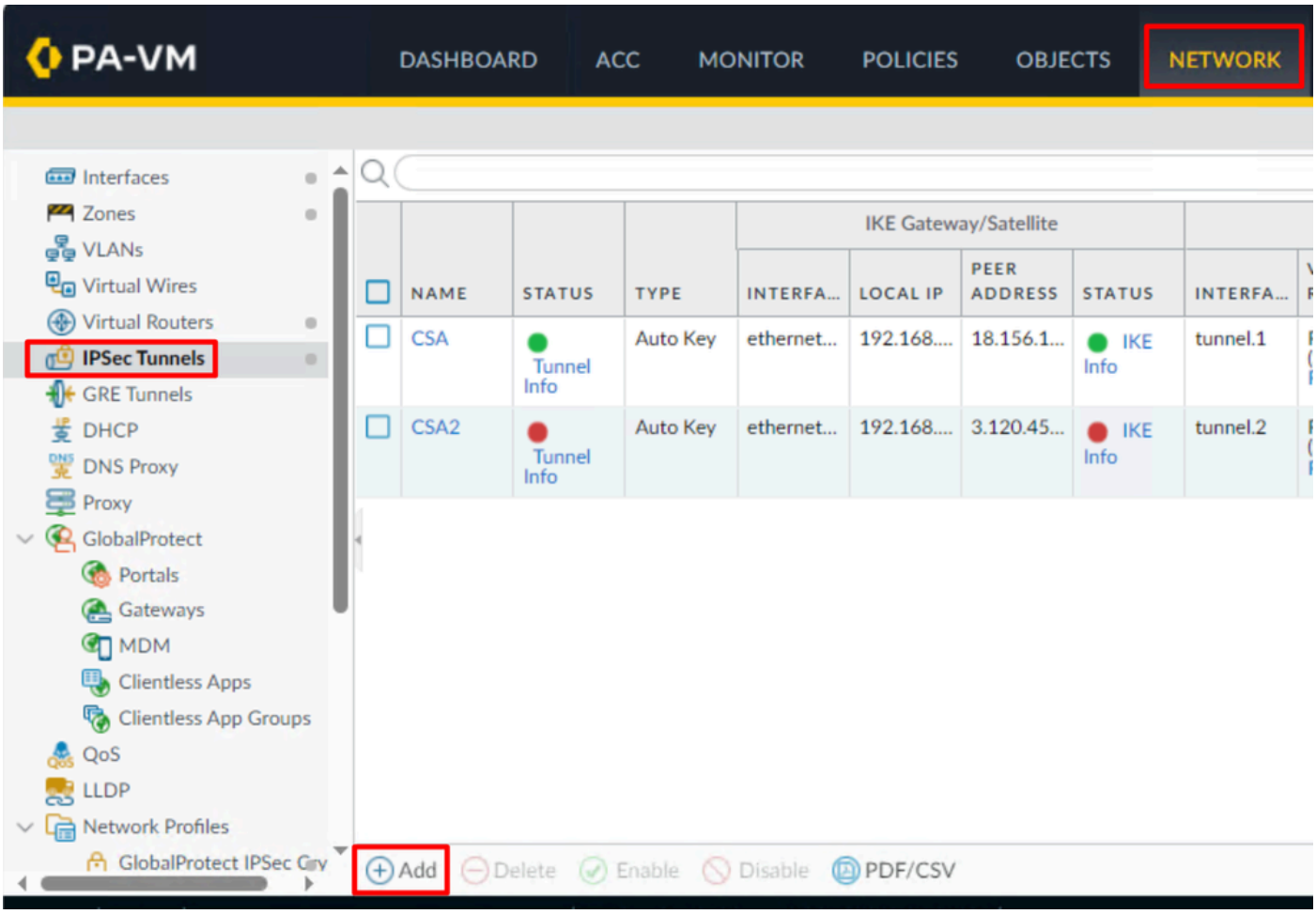


このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。 Configure IPSec Tunnels.

IPSecトンネルの設定

IPSec Tunnelsを設定するには、Network > IPSec Tunnelsに移動します。

- クリック Add



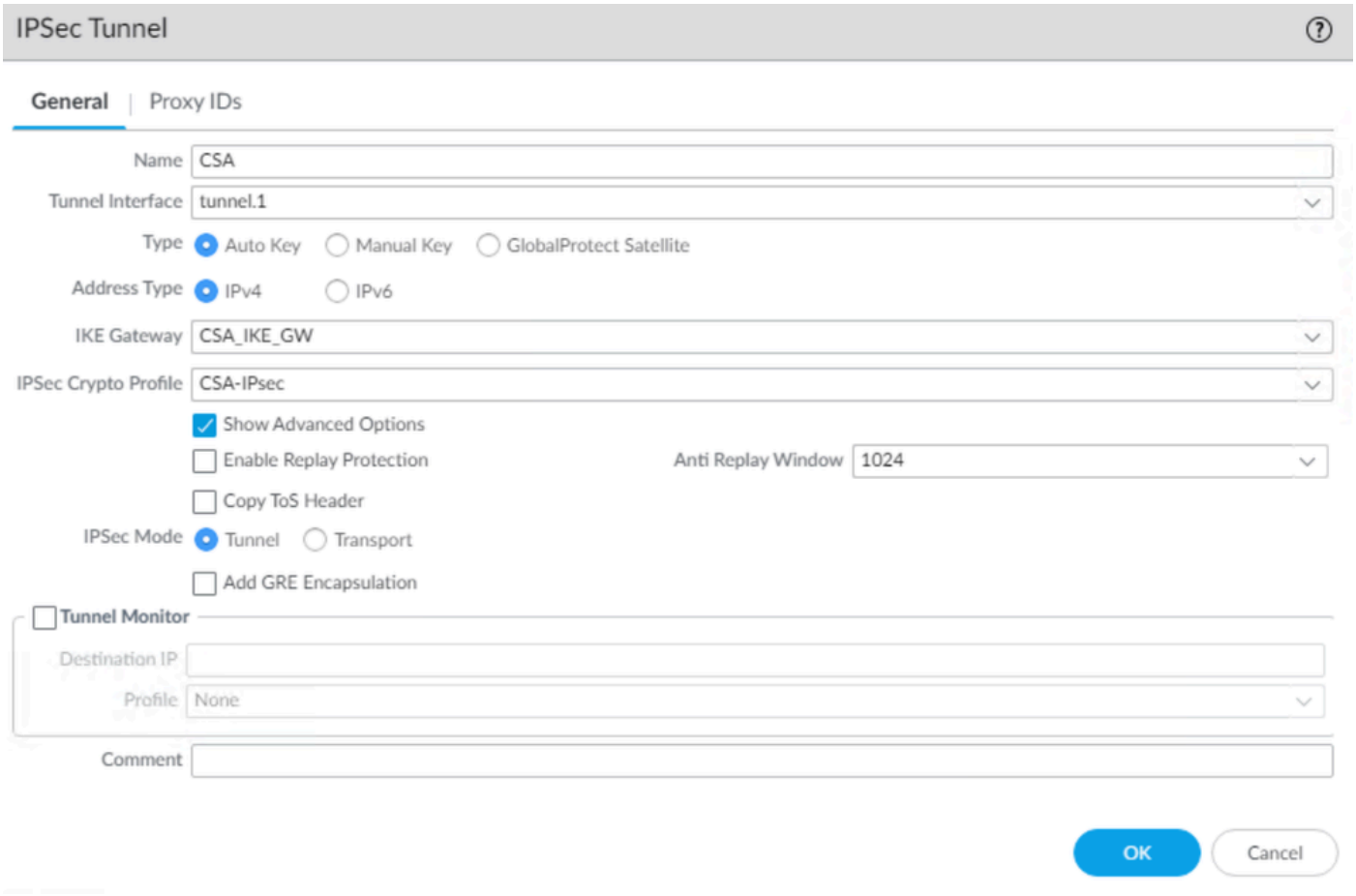
- 次のパラメータを設定します。

  - **Name**：セキュアアクセストンネルを識別する名前を使用します。

    - **Tunnel Interface**：ステップConfigure the tunnel interfaceで設定したトンネルインターフェイスを選択します。
    - **Type**：オートキー
    - **Address Type**: IPv4
    - **IKE Gateways**：ステップ「IKEゲートウェイの設定」で設定したIKEゲートウェイを選択します。
    - **IPsec Crypto Profile**：ステップConfigure IPSEC Crypto Profileで設定したIKEゲートウェイを選択します。
    - チェックボックスをオンにする **Advanced Options**

      - **IPSec Mode Tunnel**:Tunnelを選択します。

- クリック OK

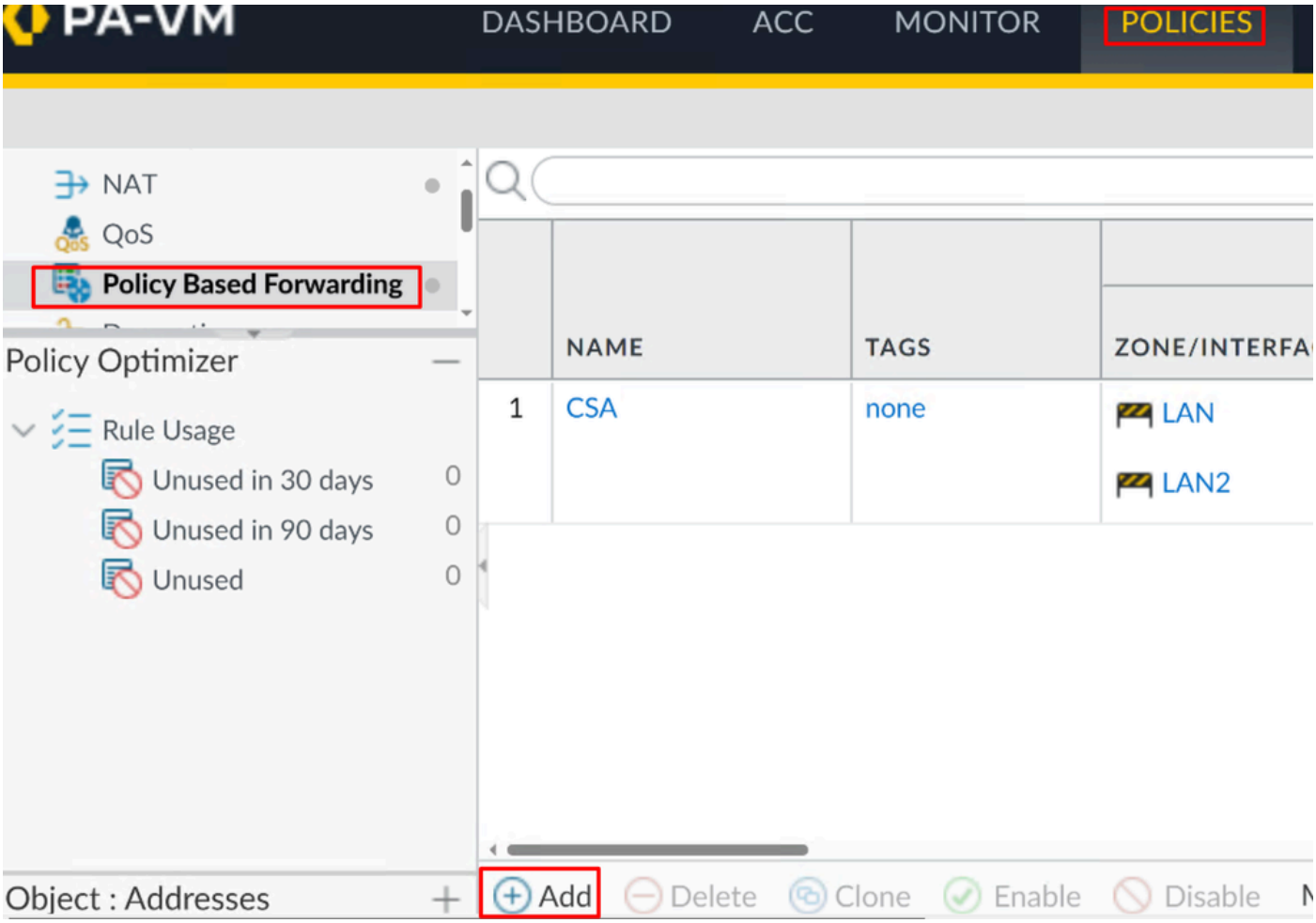


VPNが正常に作成されたら、 **Configure Policy Based Forwarding**の手順に進みます。

ポリシーベースの転送の設定

Policy Based Forwardingを設定するには、 Policies > Policy Based Forwarding.

- クリック Add

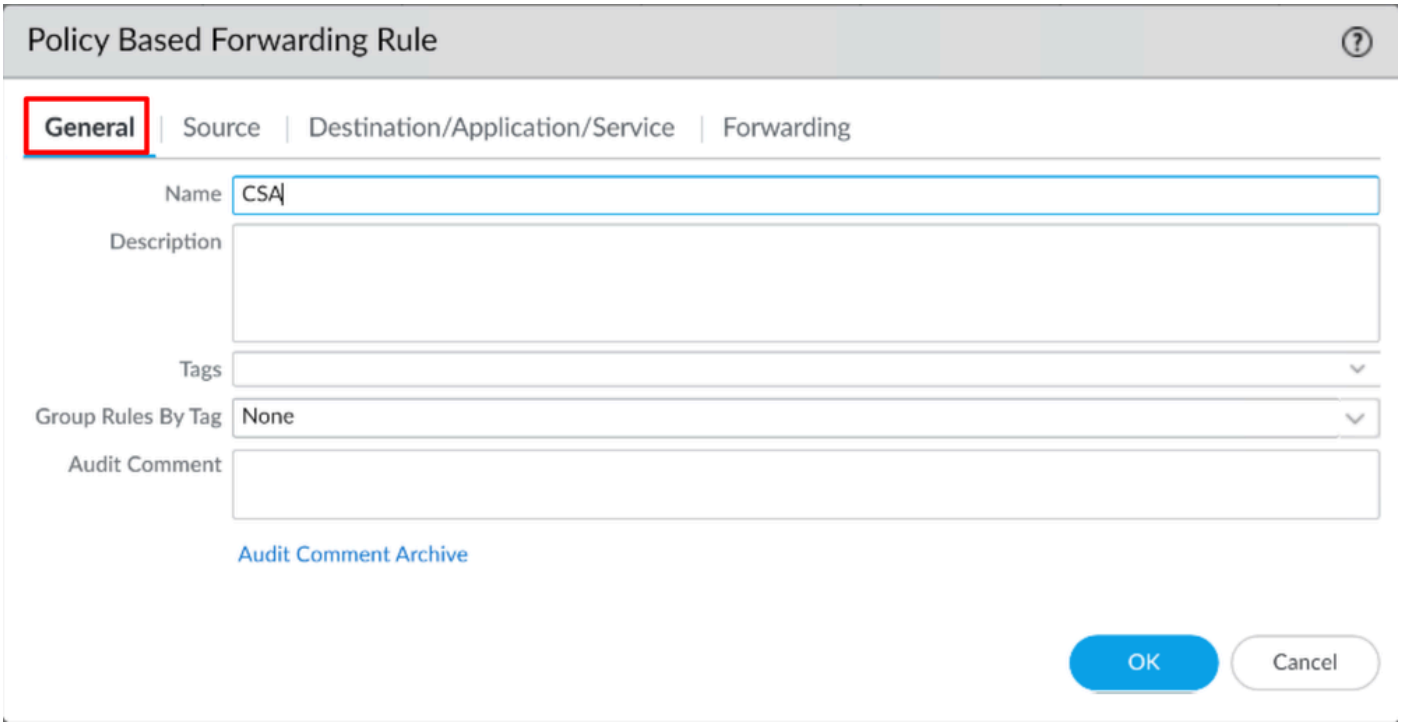


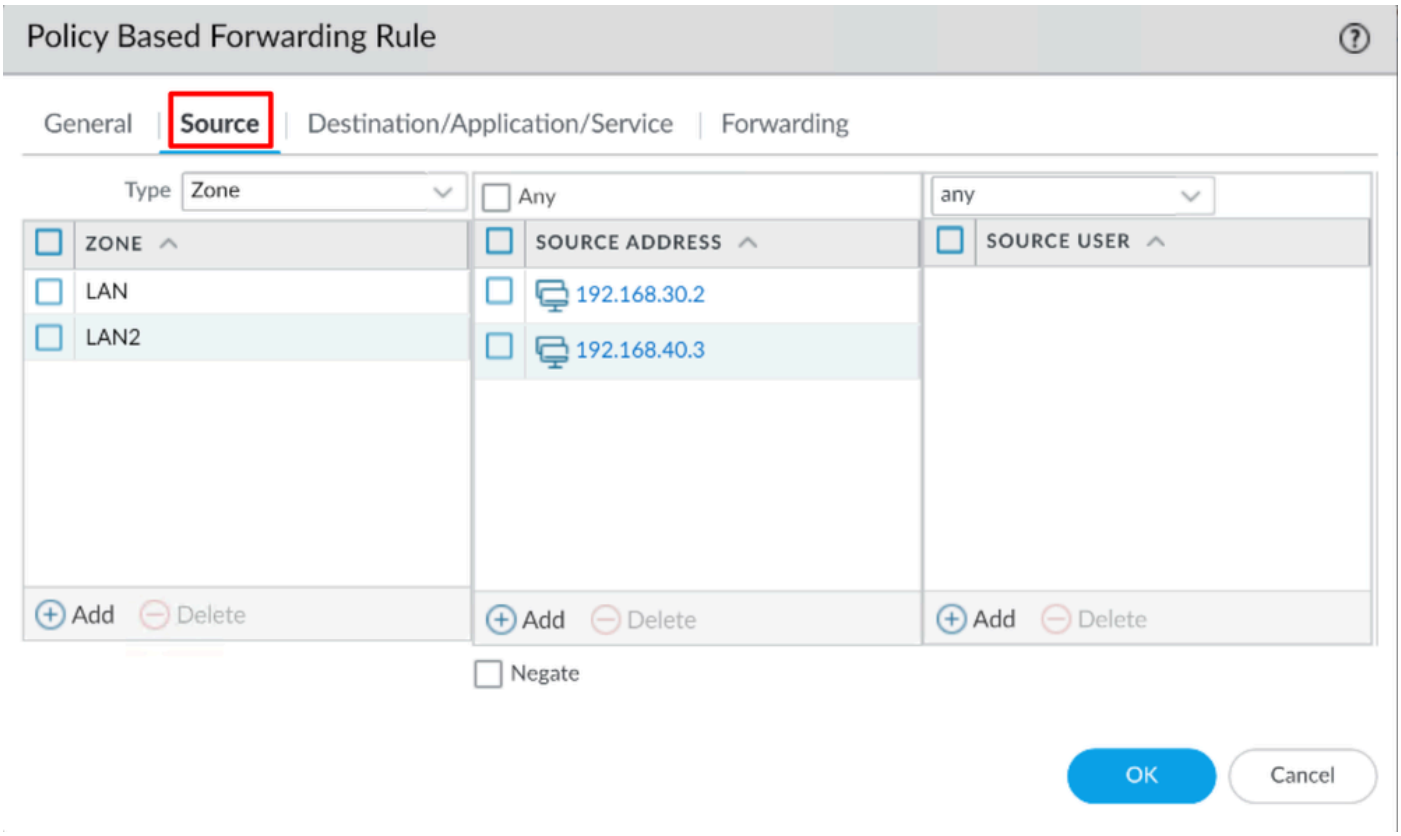
- 次のパラメータを設定します。
  - General
    - **Name**：名前を使用して、セキュアアクセス、ポリシーベース転送（発信元によるルーティング）を識別します。
- Source
  - **Zone**：送信元に基づいてトラフィックをルーティングする計画があるゾーンを選択します。
    - **Source Address**：送信元として使用する1つまたは複数のホストを設定します。
    - Source Users：トラフィックをルーティングするユーザを設定します（該当する場合のみ）。

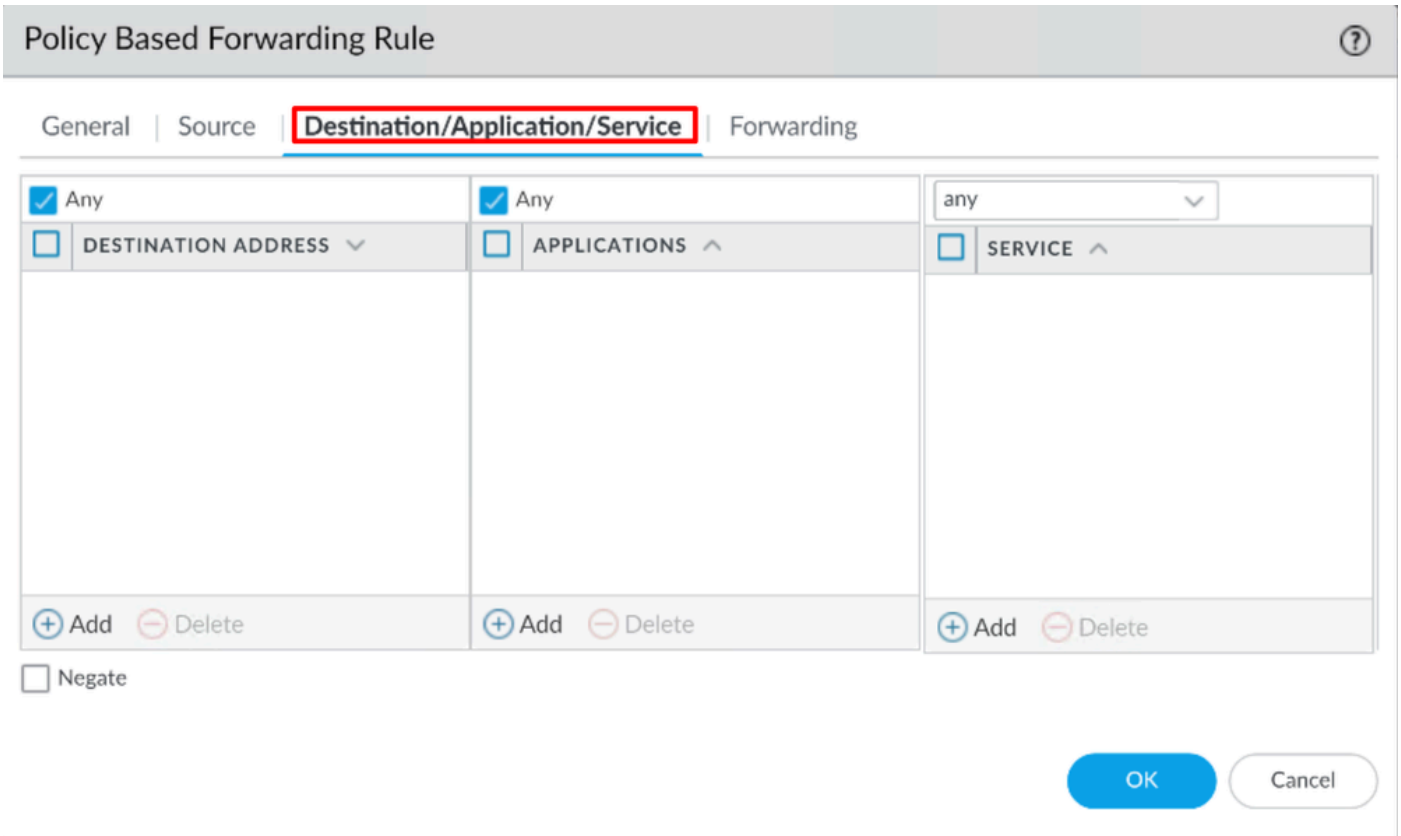
- Destination/Application/Service
    - Destination Address：これをAnyのままにしておくか、セキュアアクセス(100.64.0.0/10)のアドレス範囲を指定できます。
- Forwarding
    - **Action**:転送
        - **Egress Interface**：ステップConfigure the tunnel interfaceで設定したトンネルインターフェイスを選択します。
        - **Next Hop**:None

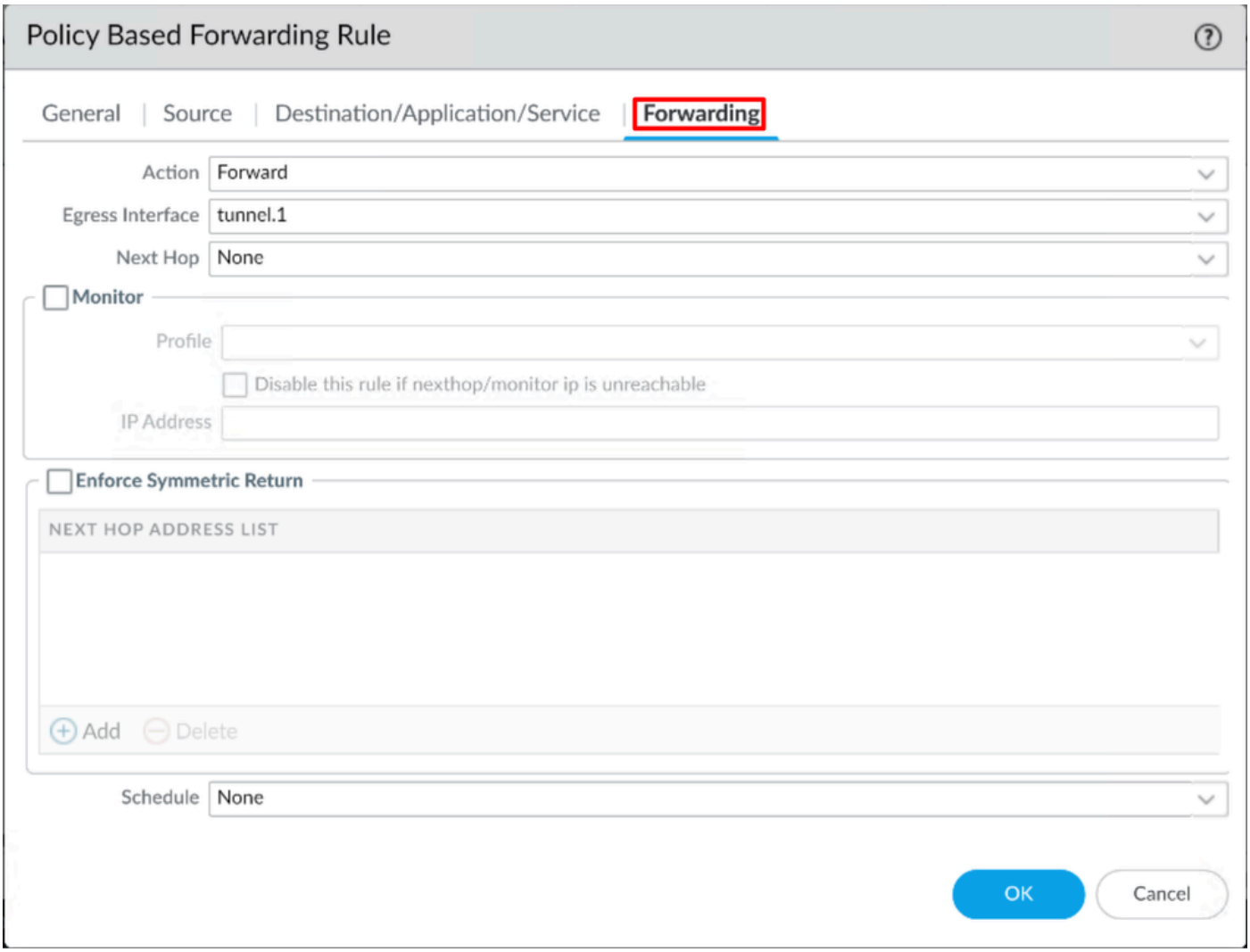
        OK

- をクリックし、 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



これで、Palo Altoですべての設定が完了しました。ルートの設定後にトンネルを確立できるため、引き続きSecure Access DashboardでRA-VPN、Browser-Based ZTA、またはClient Base ZTAを設定する必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。