Configurer un accès sécurisé avec le pare-feu Palo Alto

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Configurer le VPN sur un accès sécurisé
  - Configuration du tunnel sur Palo Alto
    - Configurer le profil de chiffrement IPSEC
    - Configuration des tunnels IPSec
    - Configurer le transfert basé sur des stratégies

Introduction

Ce document décrit comment configurer l'accès sécurisé avec Palo Alto Firewall.

Conditions préalables

- Configurer le provisionnement utilisateur
- Configuration de l'authentification ZTNA SSO
- Configuration de l'accès sécurisé VPN à distance

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé
- ZTNA sans client
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- Pare-feu de version Palo Alto 11.x

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- Pare-feu de version Palo Alto 11.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales



Accès sécurisé - Palo Alto

Cisco a conçu Secure Access pour protéger et fournir un accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles y accèdent via le cloud.

Configurer

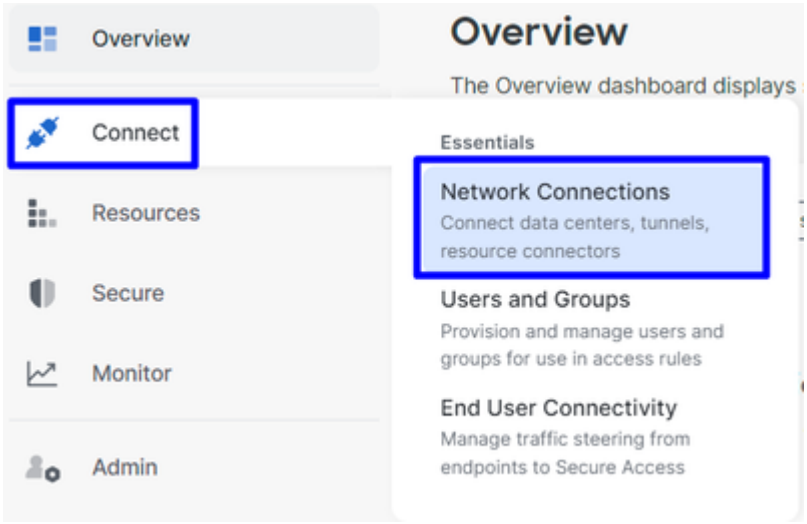
Configurer le VPN sur un accès sécurisé

1. Accédez au panneau d'administration de Secure Access.



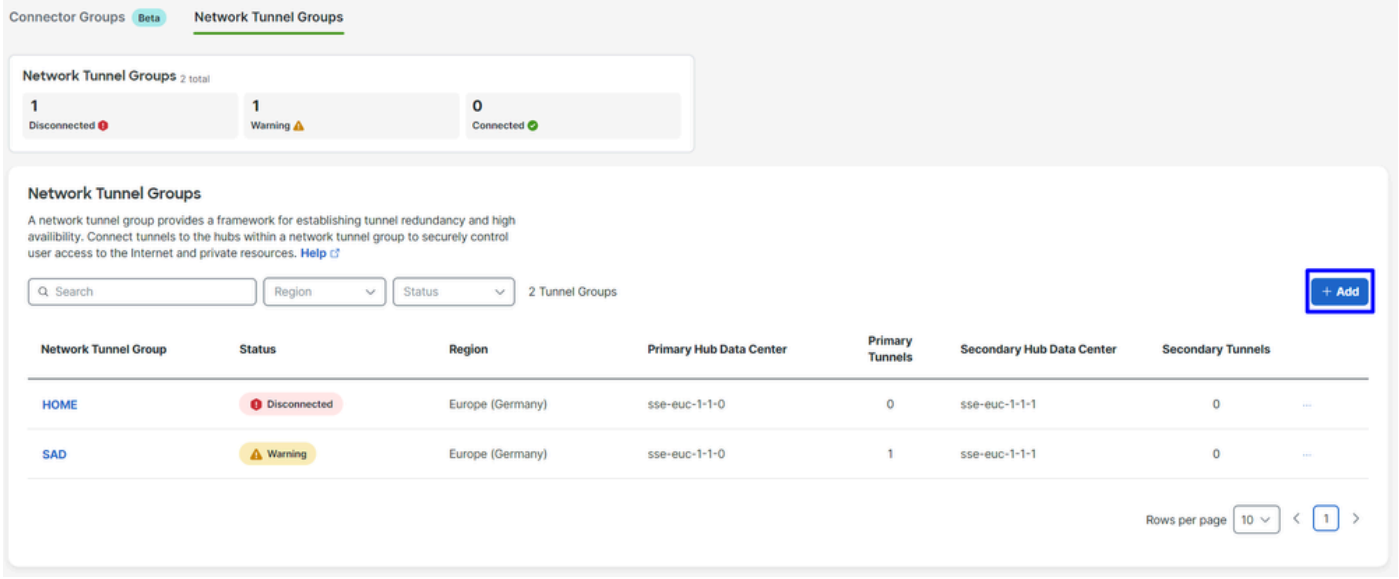
Accès sécurisé - Page principale

2. Cliquez sur Connect > Network Connections.



Accès sécurisé - Connexions réseau

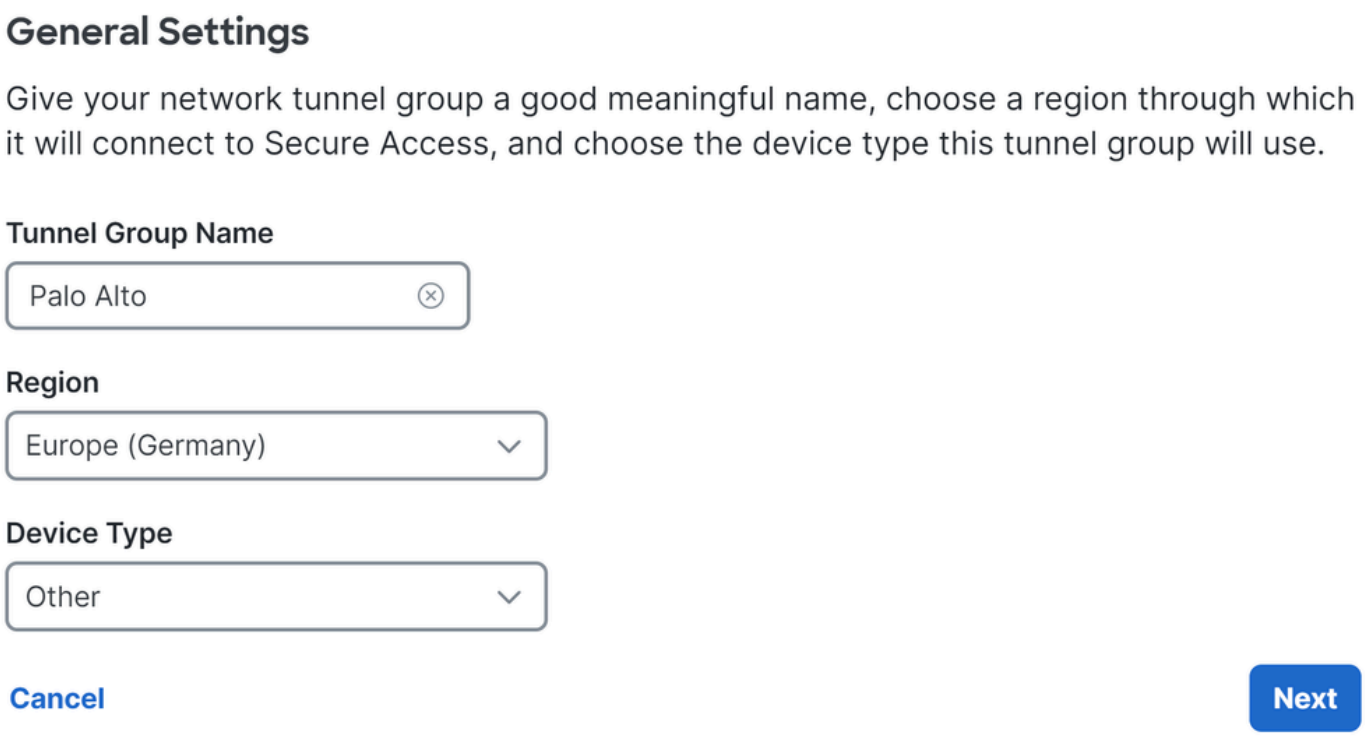
3. Sous Network Tunnel Groups, cliquez sur +Add.



Accès sécurisé - Groupes de tunnels réseau

4. Configurez le nom du groupe de tunnels, la région et le type de périphérique.

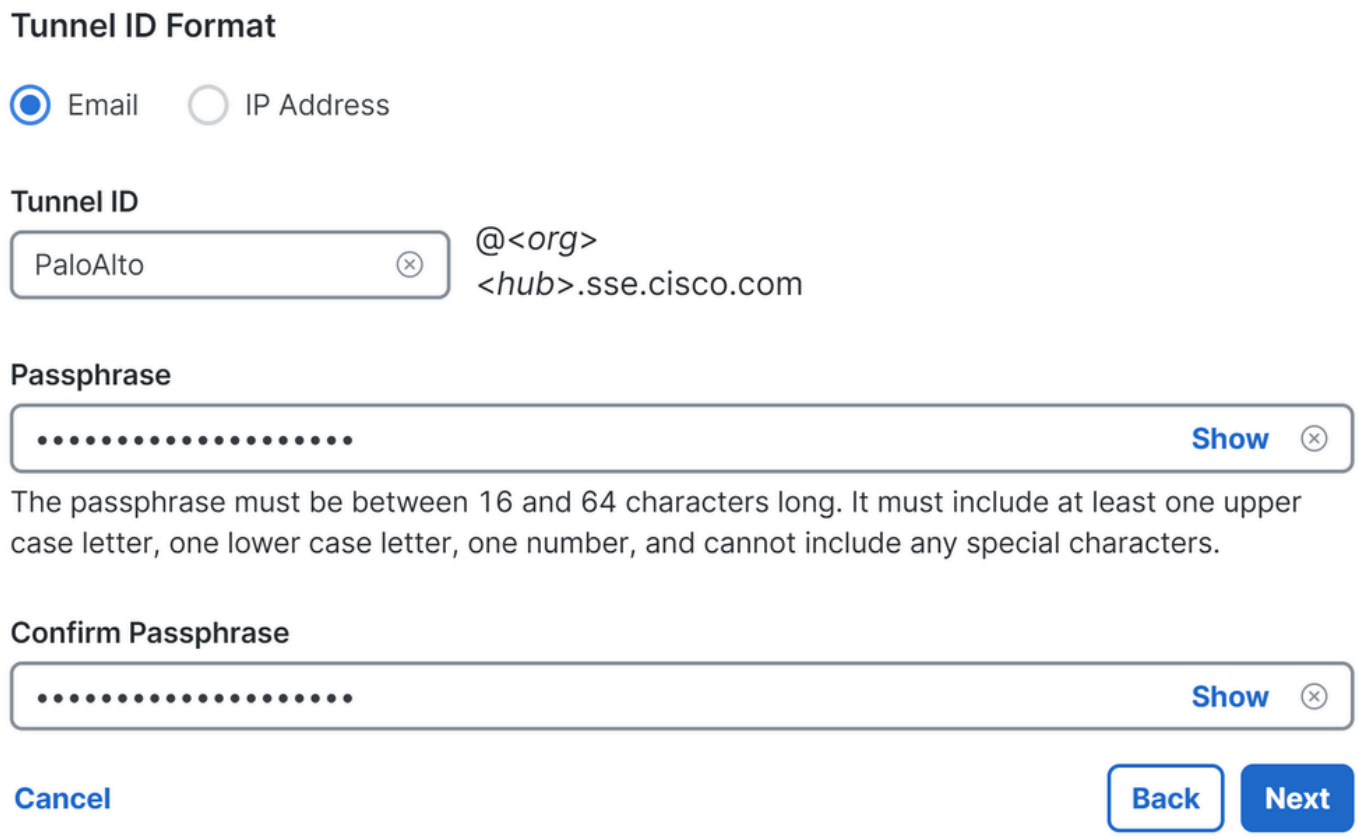
5. Cliquez sur Suivant.



Remarque : Sélectionnez la région la plus proche de l'emplacement de votre pare-feu.

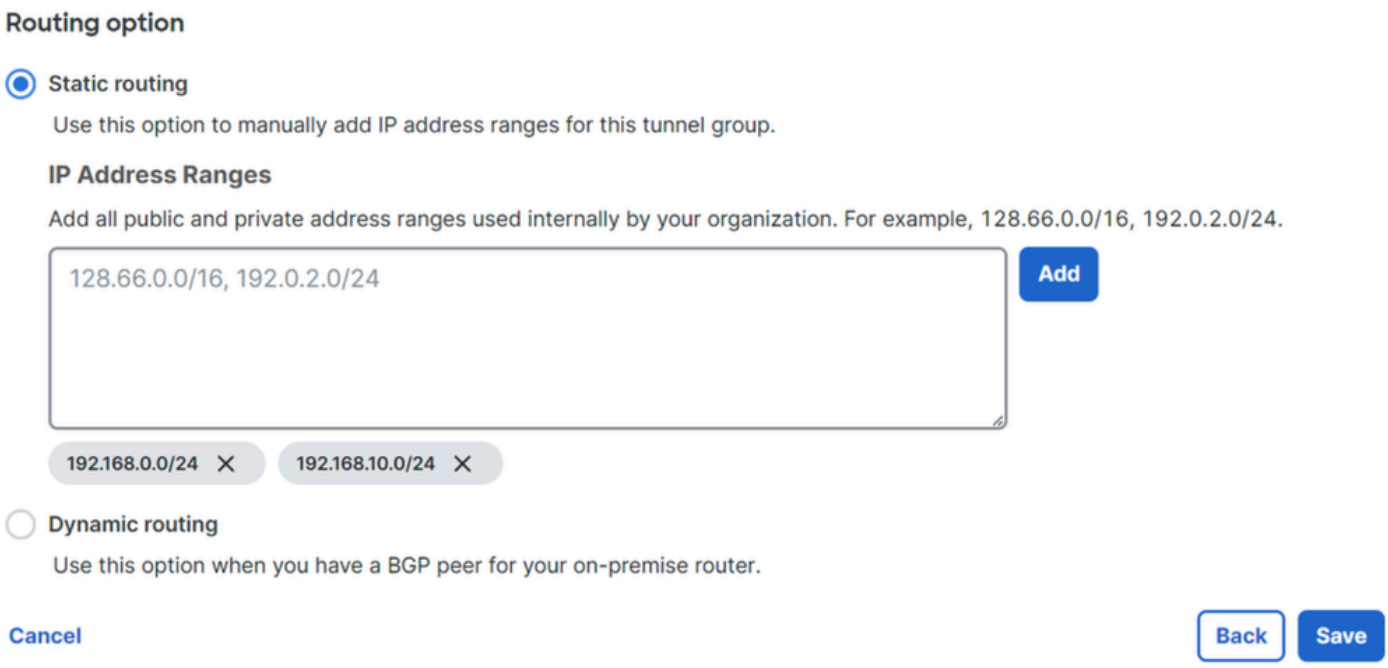
6. Configurez le format d'ID de tunnel et la phrase de passe.

7. Cliquez sur Suivant.



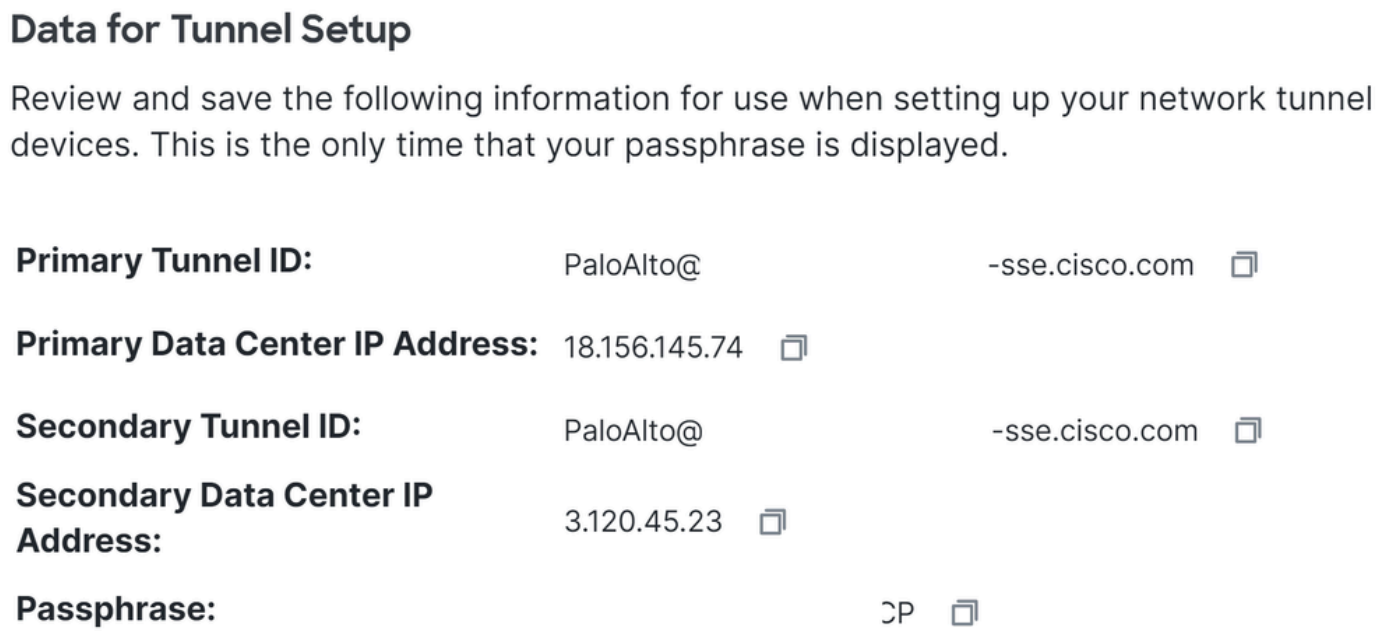
8. Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez acheminer le trafic via l'accès sécurisé.

9. Cliquez sur Enregistrer.



10. Après avoir cliqué sur Enregistrer, les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante ; Configurez le tunnel sur Palo Alto.

Données du tunnel



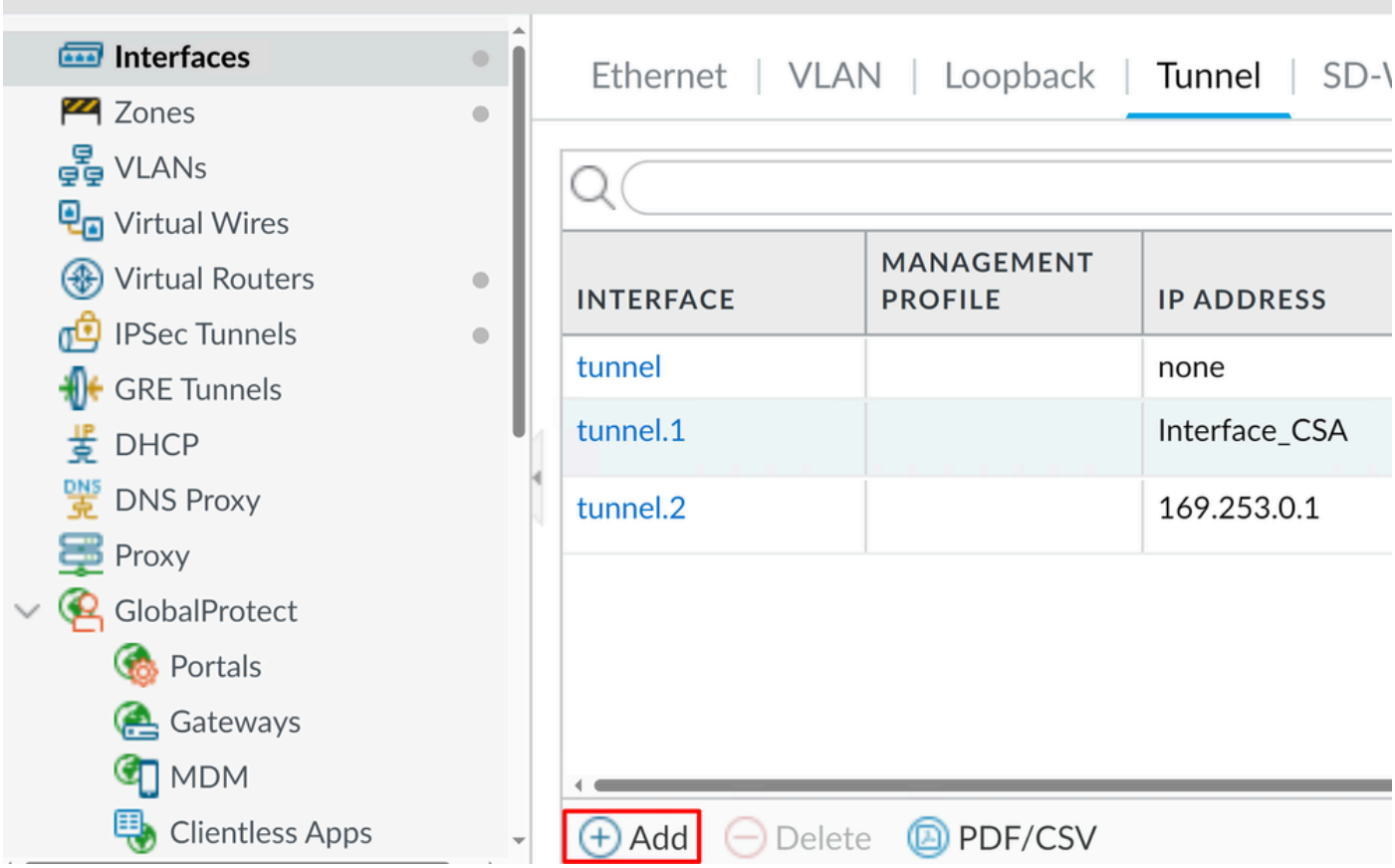
Configuration du tunnel sur Palo Alto

Configuration de l'interface du tunnel

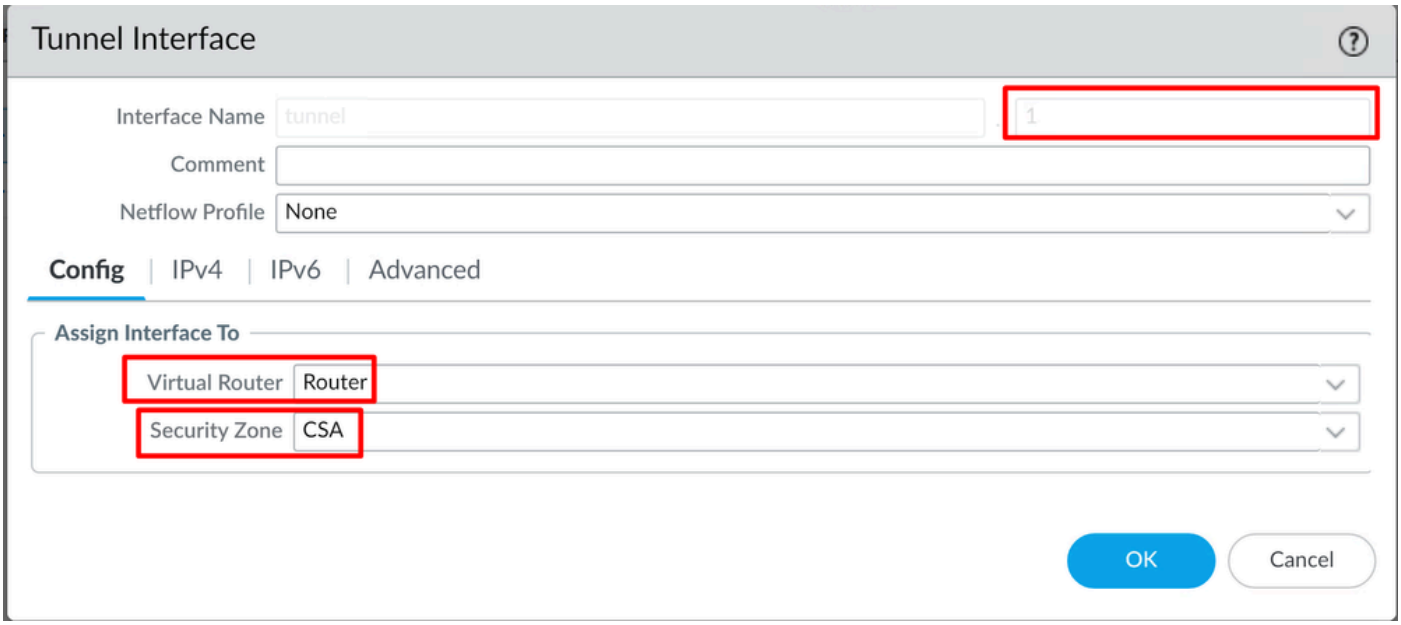
Accédez au tableau de bord Palo Alto.

1. Réseau > Interfaces > Tunnel.

2. Cliquez sur Ajouter.

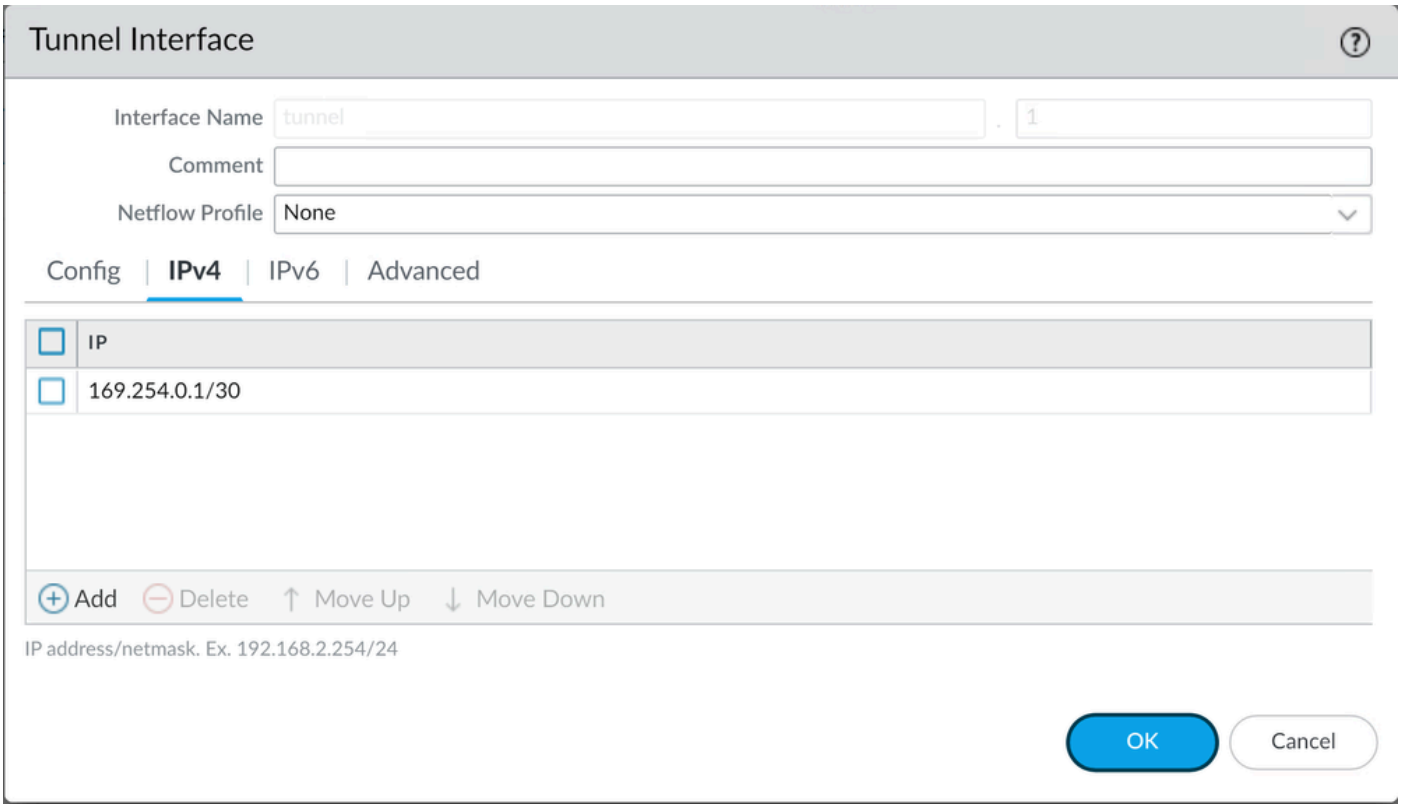


3. Dans le menu Config, configurez le routeur virtuel, la zone de sécurité et attribuez un numéro de suffixe.

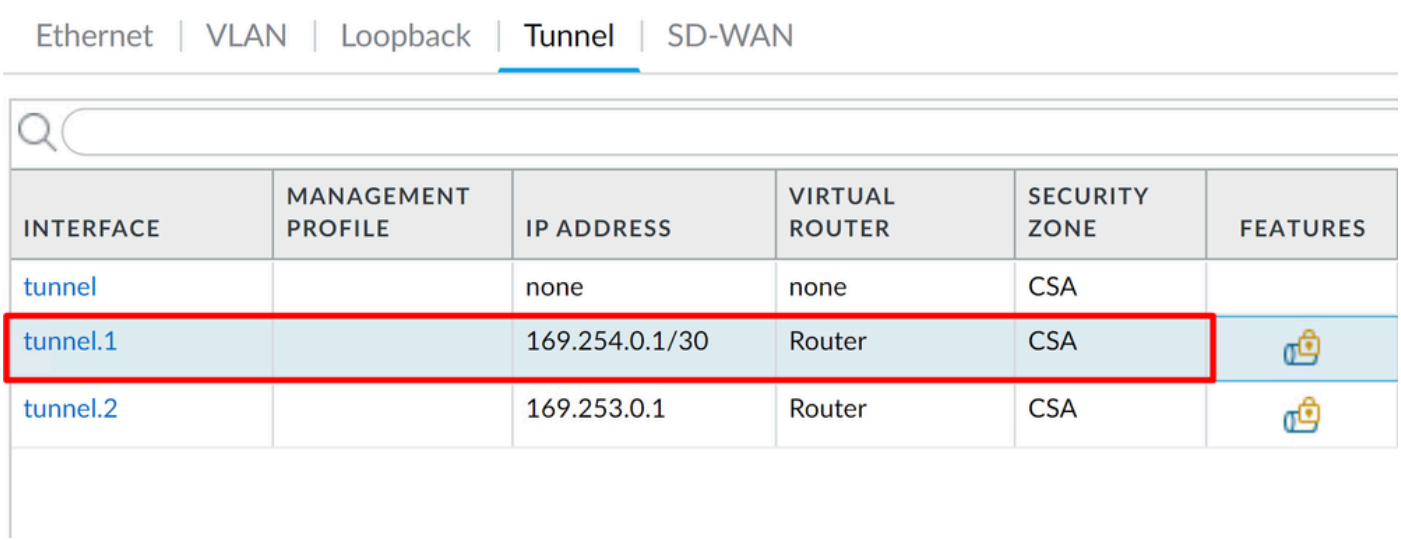


4. Sous IPv4, configurez une adresse IP non routable. Par exemple, vous pouvez utiliser 169.254.0.1/30.

5. Cliquez sur OK.



6. Après cela, vous pouvez avoir quelque chose comme ceci configuré :



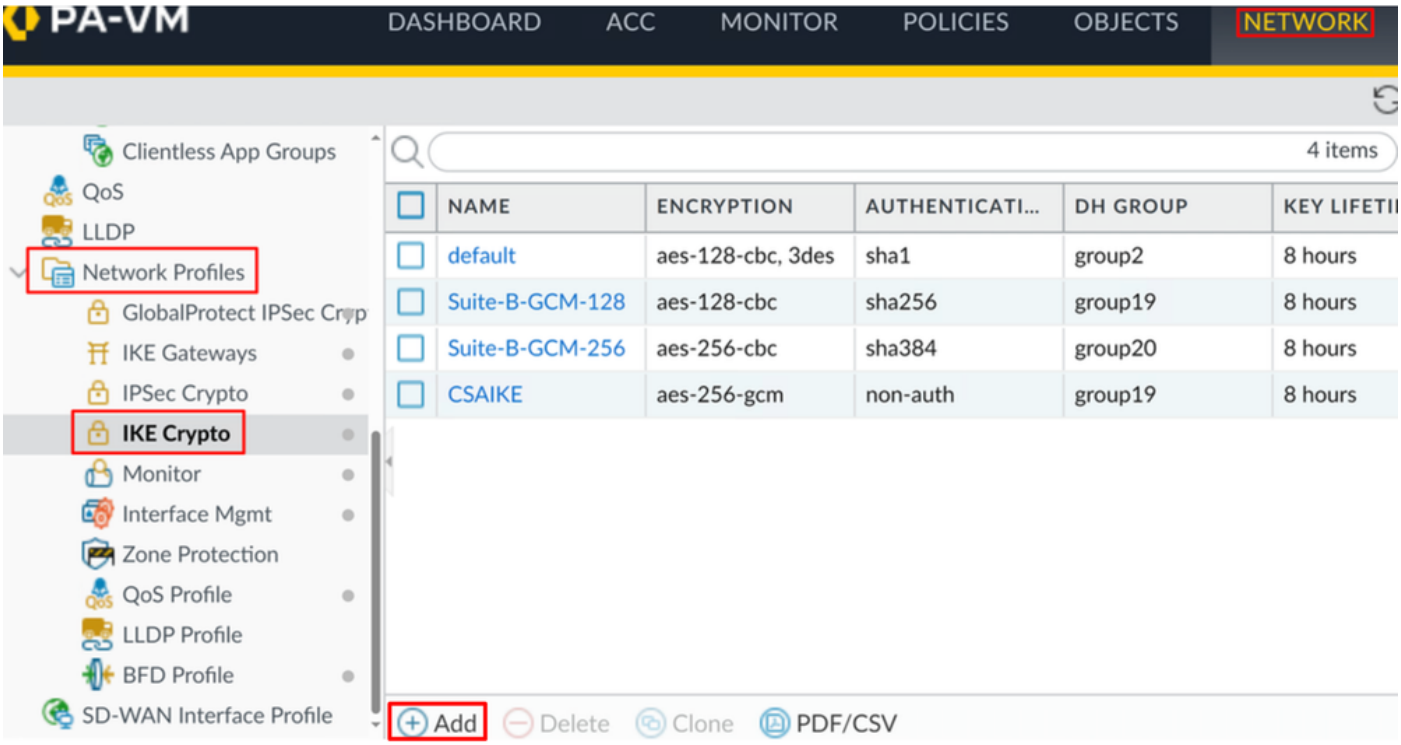
7. Si vous l'avez configuré comme ceci, cliquez sur Commit pour enregistrer votre configuration et continuer avec l'étape suivante ; Configurez le profil de chiffrement IKE.

Configuration du profil de chiffrement IKE

Pour configurer le profil de chiffrement, accédez à :

1. Réseau > Profil réseau > IKE Crypto.

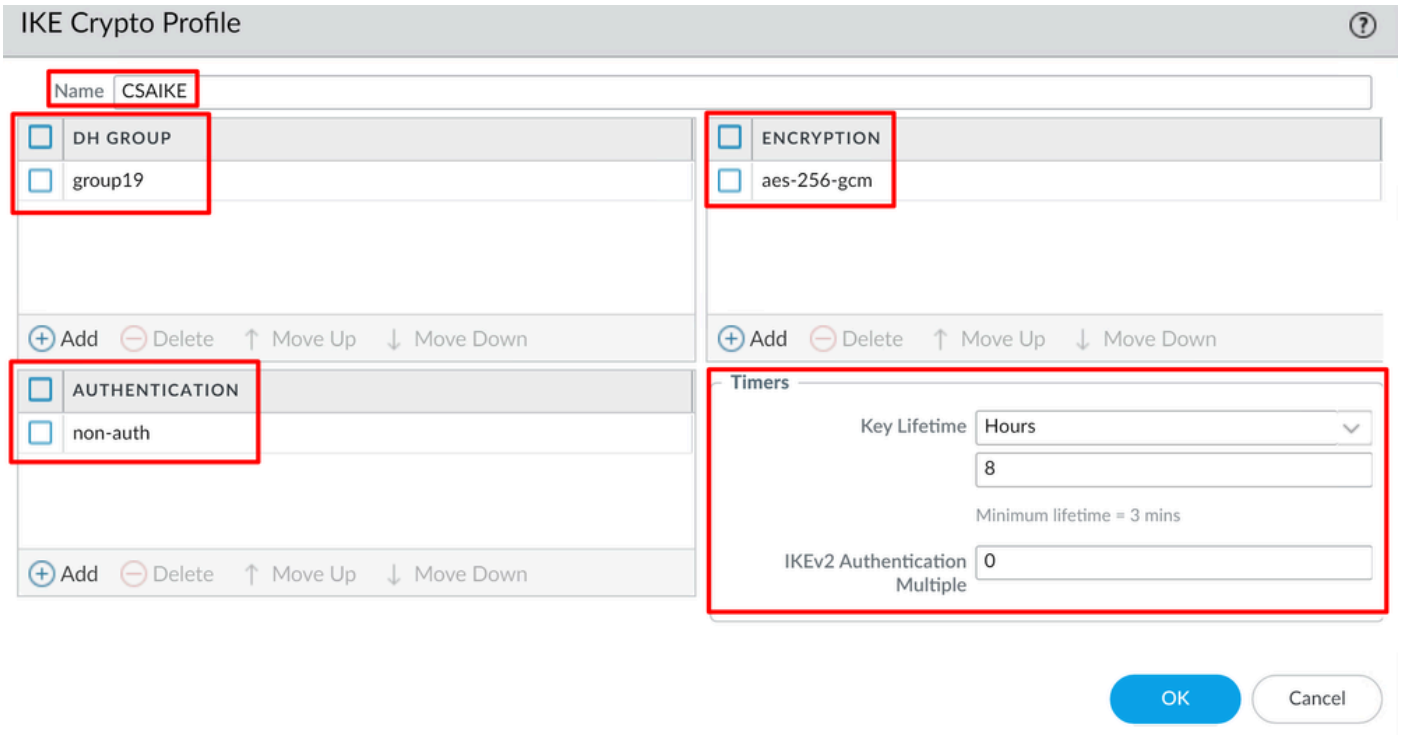
2. Cliquez sur Ajouter.



3. Configurez les paramètres suivants :

- Name : Configurez un nom pour identifier le profil.
- GROUPE DH : groupe19
- AUTHENTIFICATION: non-authentification
- CRYPTAGE : aes-256-gcm
- Minuteurs :
  - Durée de vie des clés : 8 heures
  - Authentification IKEv2 : 0

4. Une fois que tout est configuré, cliquez sur OK.



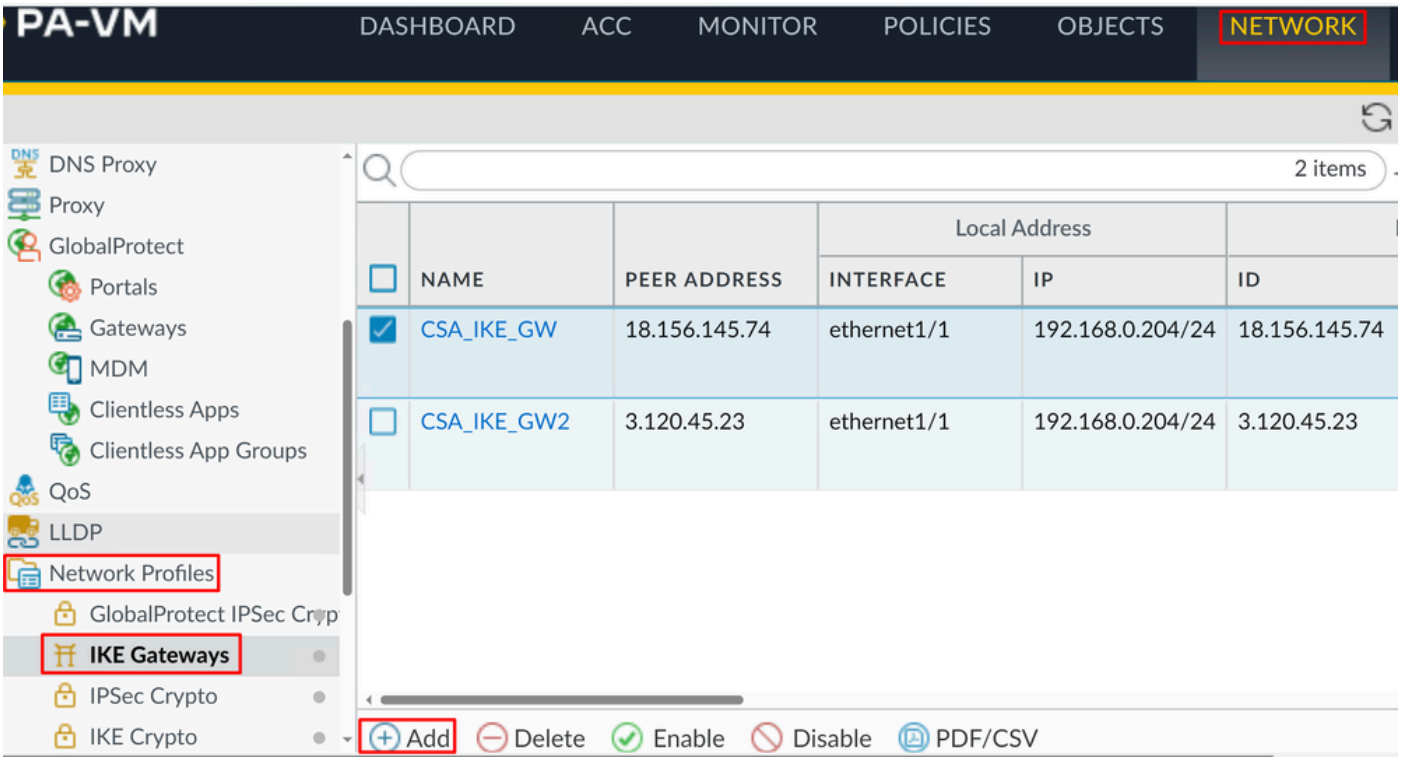
5. Si vous l'avez configuré comme ceci, cliquez sur Commit pour enregistrer votre configuration et continuer avec l'étape suivante ; Configurez les passerelles IKE.

Configuration des passerelles IKE

Pour configurer des passerelles IKE

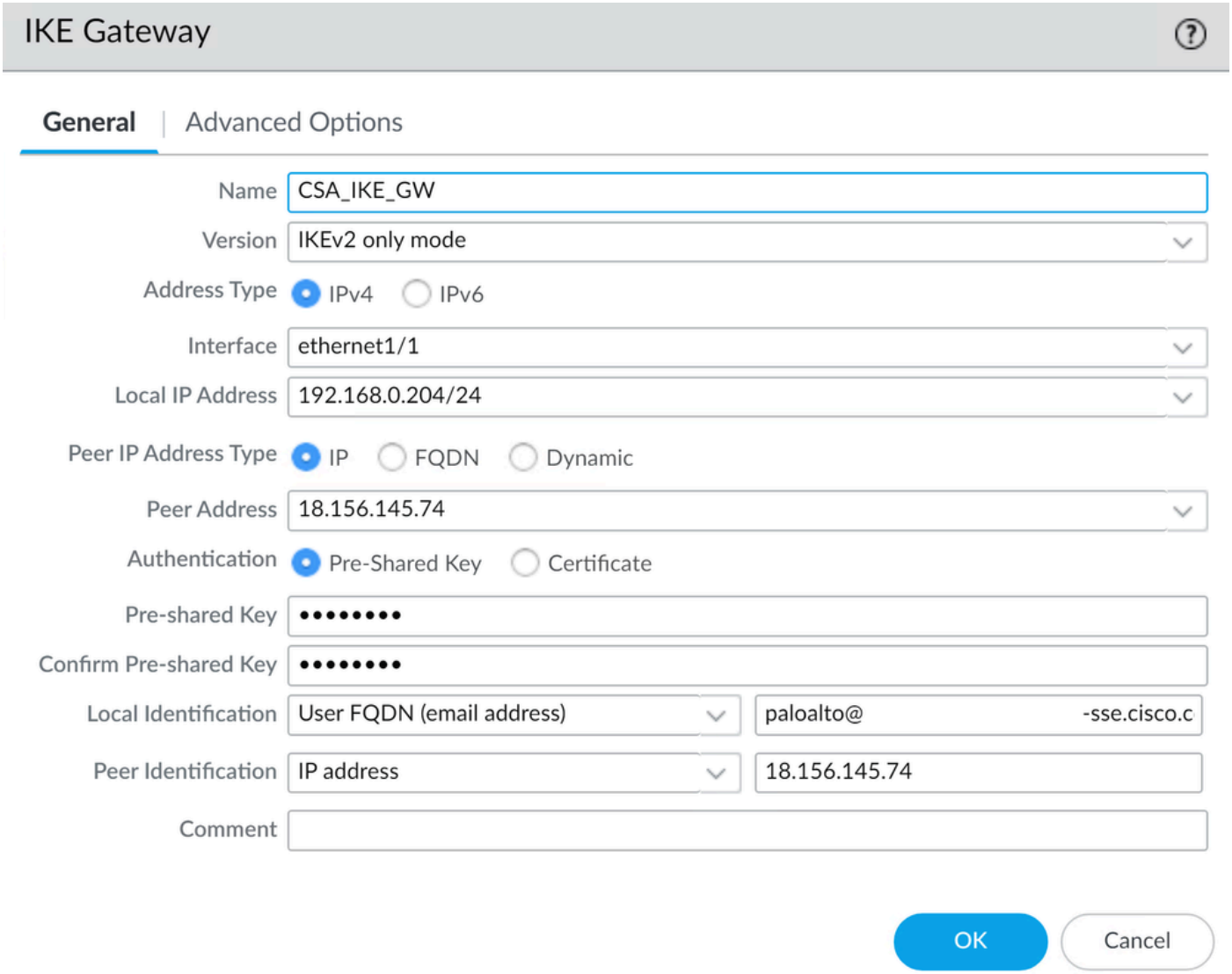
1. Réseau > Profil réseau > Passerelles IKE.

2. Cliquez sur Ajouter.



3. Configurez les paramètres suivants :

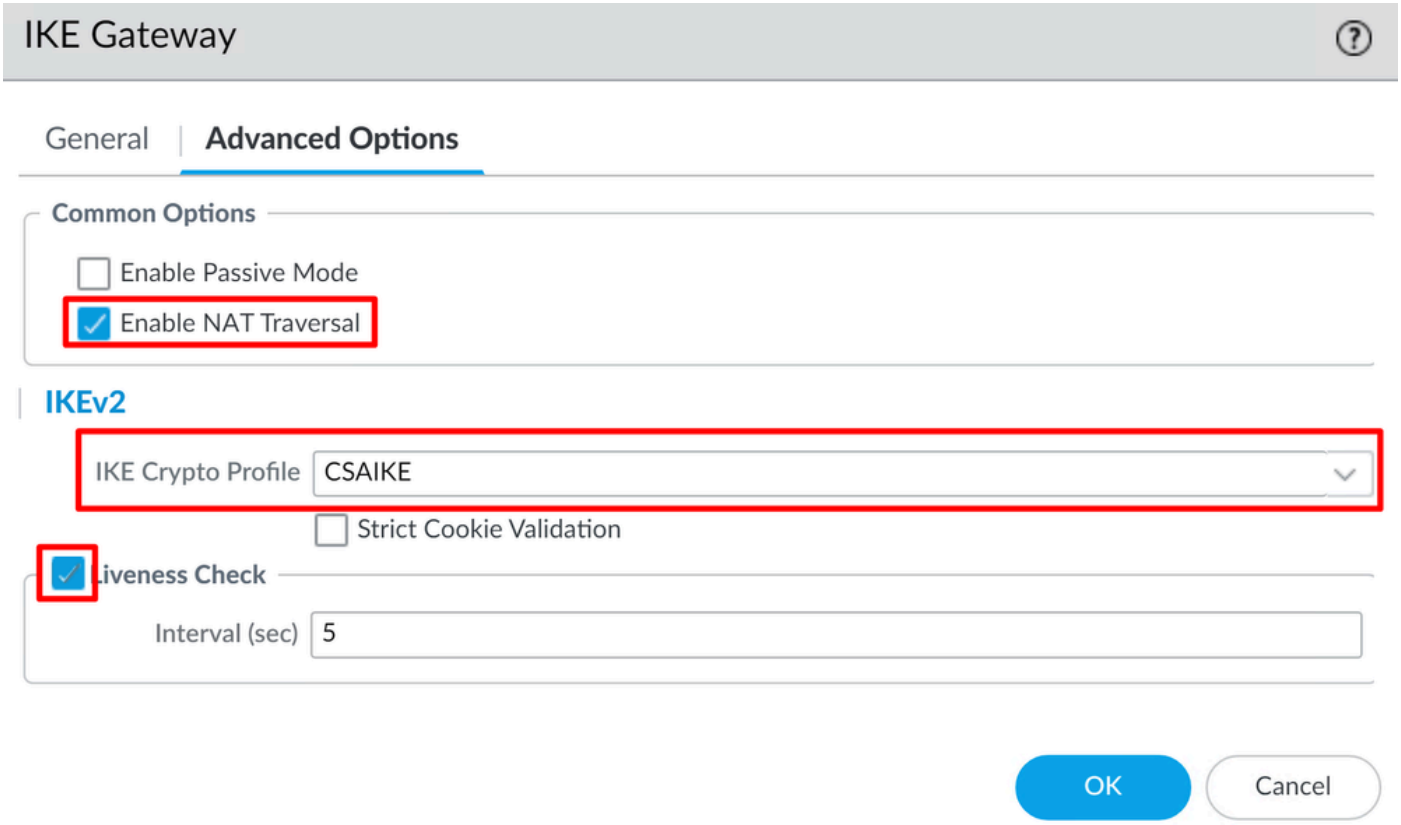
- Name : Configurez un nom pour identifier les passerelles Ike
- Version : Mode IKEv2 uniquement
- Type d'adresse : IPv4
- Interface: Sélectionnez votre interface WAN Internet
- Adresse IP locale : Sélectionnez l'adresse IP de votre interface WAN Internet
- Type d'adresse IP homologue : IP
- Adresse homologue : Utilisez l'adresse IP du data center IP principal, donnée dans l'étape Données de tunnel
- Authentification: Clé pré-partagée
- Clé pré-partagée : Utilisez la phrase de passe donnée dans l'étape Données de tunnel
- Confirmer la clé pré-partagée : Utilisez la phrase de passe donnée dans l'étape Données de tunnel
- Identification locale : Choisissez User FQDN (Email address) et utilisez l'ID de tunnel principal donné à l'étape, Tunnel Data
- Identification des homologues : Choisissez IP Address et utilisez l'adresse IP principale du data center



4. Cliquez sur Options avancées.

- Activer la traversée NAT
- Sélectionnez le profil de chiffrement IKE créé à l'étape Configurer le profil de chiffrement IKE
- Cochez la case Vérification de l'activité

5. Cliquez sur OK.

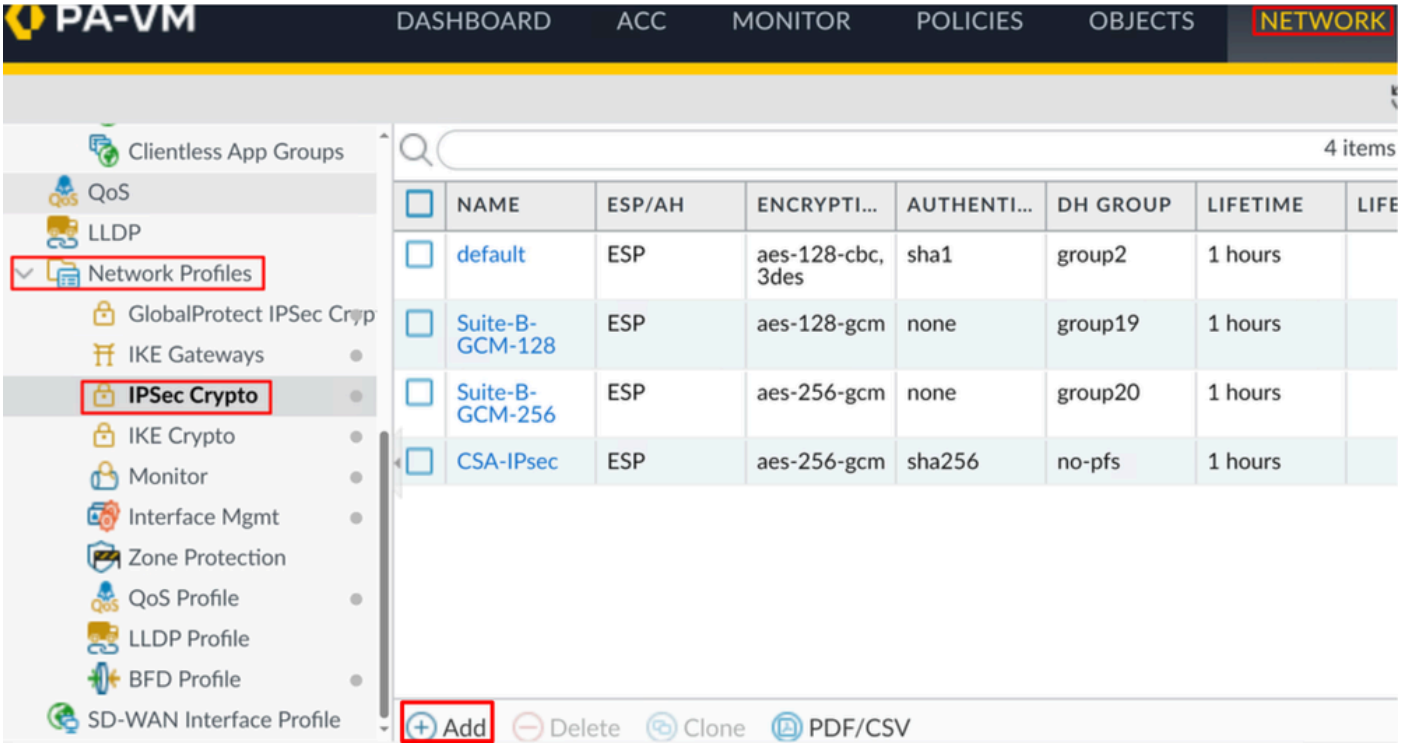


6. Si vous l'avez configuré comme ceci, cliquez sur Commit pour enregistrer votre configuration et continuer avec l'étape suivante, Configure IPSEC Crypto Profile.

Configurer le profil de chiffrement IPSEC

1. Pour configurer les passerelles IKE, accédez à Network > Network Profile > IPSEC Crypto.

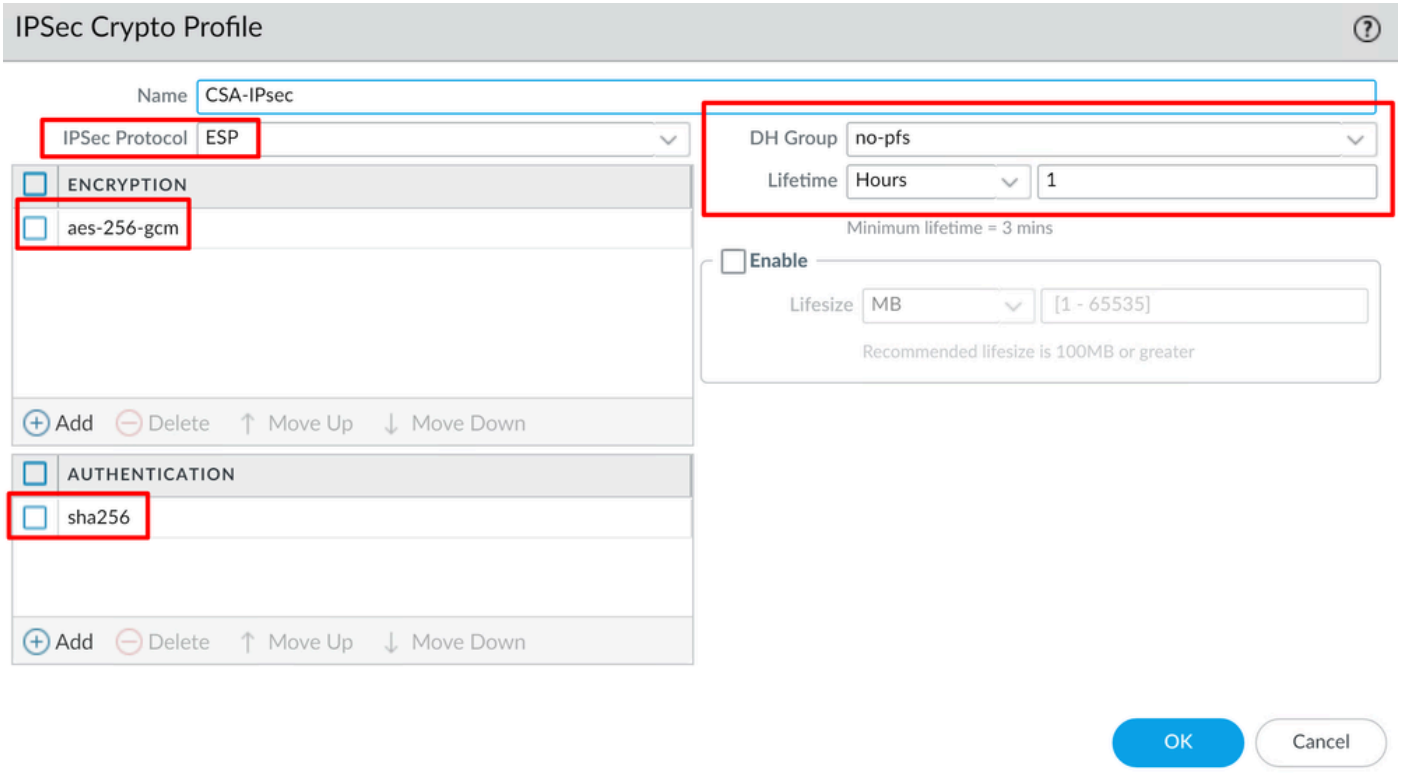
2. Cliquez sur Ajouter.



3. Configurez les paramètres suivants :

- Name : Utilisez un nom pour identifier le profil IPsec d'accès sécurisé
- Protocole IPSec : ESP
- CRYPTAGE : aes-256-gcm
- Groupe DH : sans pfs, 1 heure

4. Cliquez sur OK.

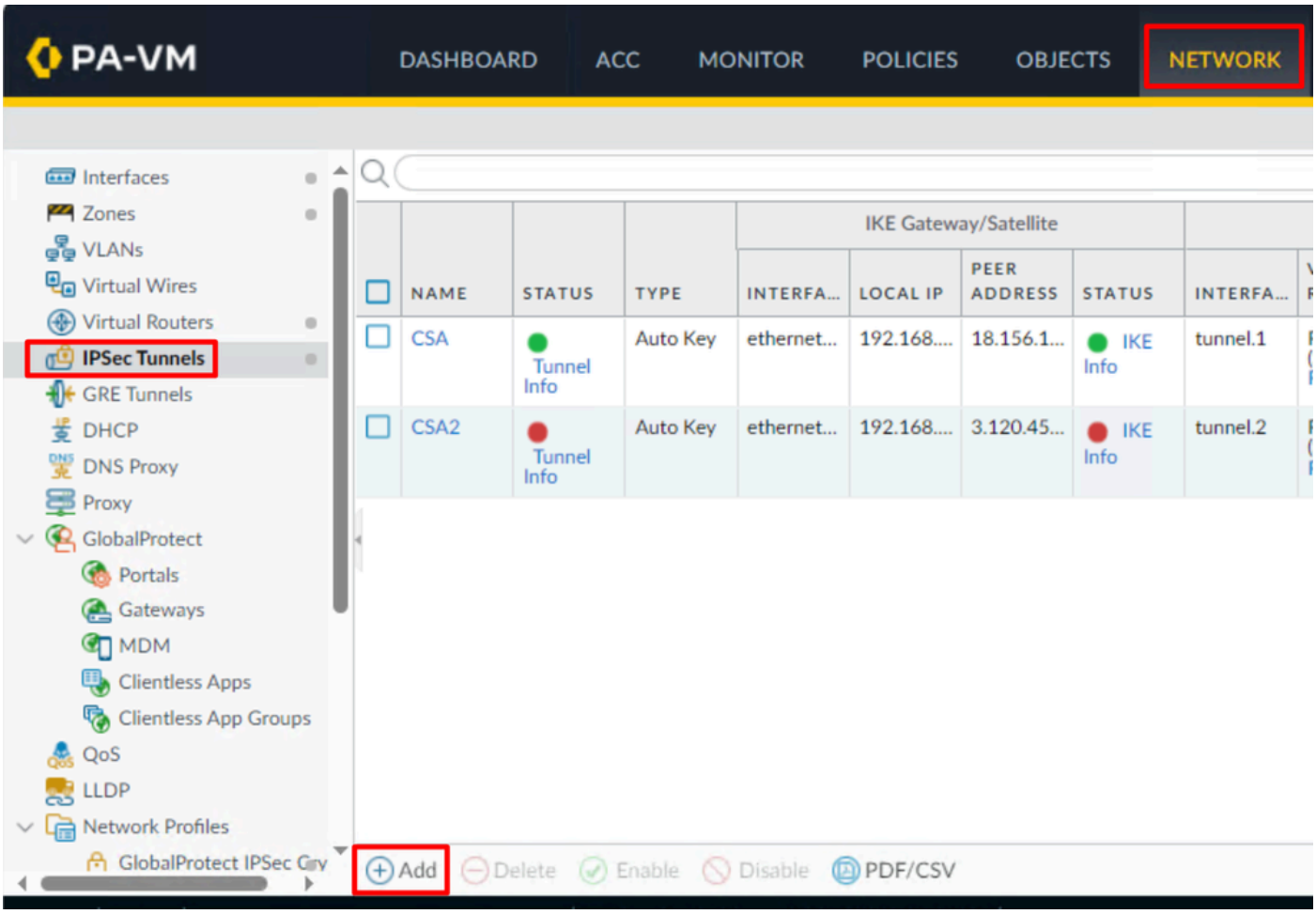


5. Si vous l'avez configuré comme ceci, cliquez sur Commit pour enregistrer votre configuration et continuer avec l'étape suivante ; Configurez les tunnels IPSec.

Configuration des tunnels IPSec

1. Pour configurer les tunnels IPSec, accédez à Réseau > Tunnels IPSec.

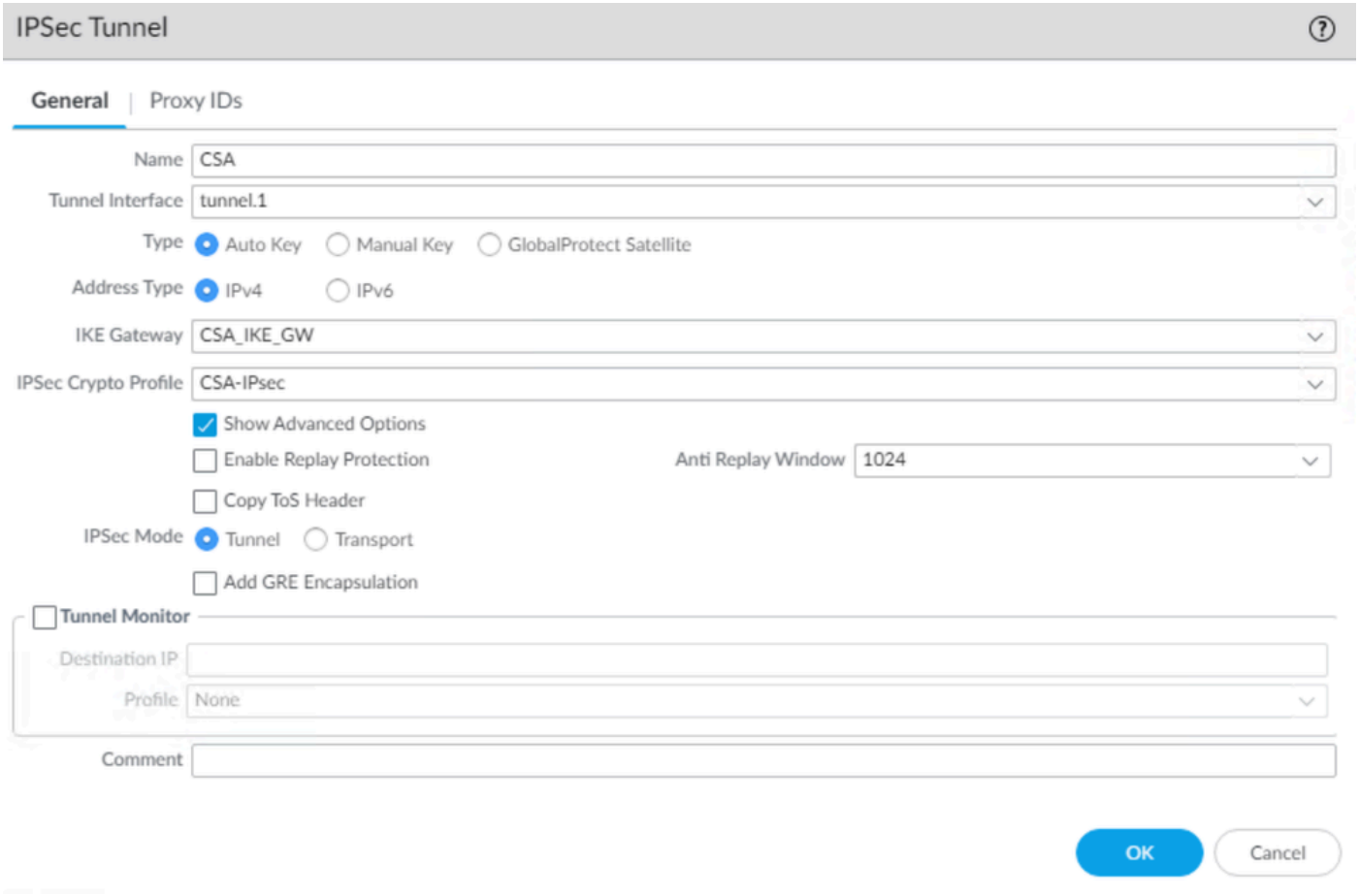
2. Cliquez sur Ajouter.



3. Configurez les paramètres suivants :

- Name : Utilisez un nom pour identifier le tunnel Secure Access
- Interface de tunnel : Choisissez l'interface de tunnel configurée à l'étape, Configurer l'interface de tunnel
- type : Clé automatique
- Type d'adresse : IPv4
- Passerelles IKE : Sélectionnez les passerelles IKE configurées à l'étape Configurer les passerelles IKE
- Profil de chiffrement IPsec : Sélectionnez les passerelles IKE configurées à l'étape Configurer le profil de chiffrement IPSEC
- Cochez la case Options avancées
    - Tunnel en mode IPSec : Choisir un tunnel

4. Cliquez sur OK.



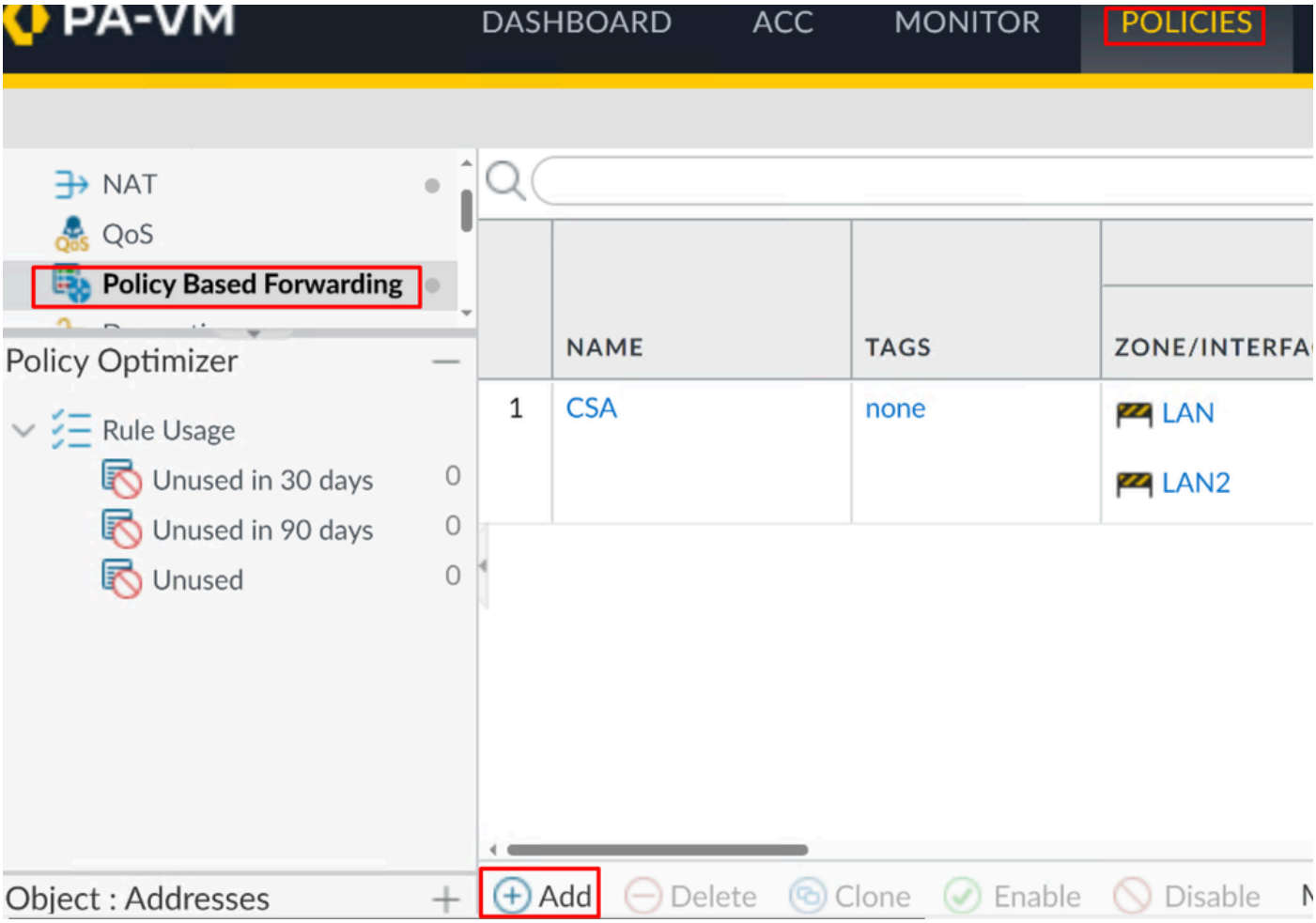
⚠ Mise en garde : Les ID de proxy ne sont pas pris en charge. Évitez toute configuration avec un ID de proxy dans les tunnels Palo Alto IPSEC avec accès sécurisé.

Maintenant que votre VPN a été créé avec succès, vous pouvez poursuivre l'étape ; Configurez le transfert basé sur des stratégies.

Configurer le transfert basé sur des stratégies

1. Pour configurer le transfert basé sur des stratégies, accédez à Stratégies > Transfert basé sur des stratégies.

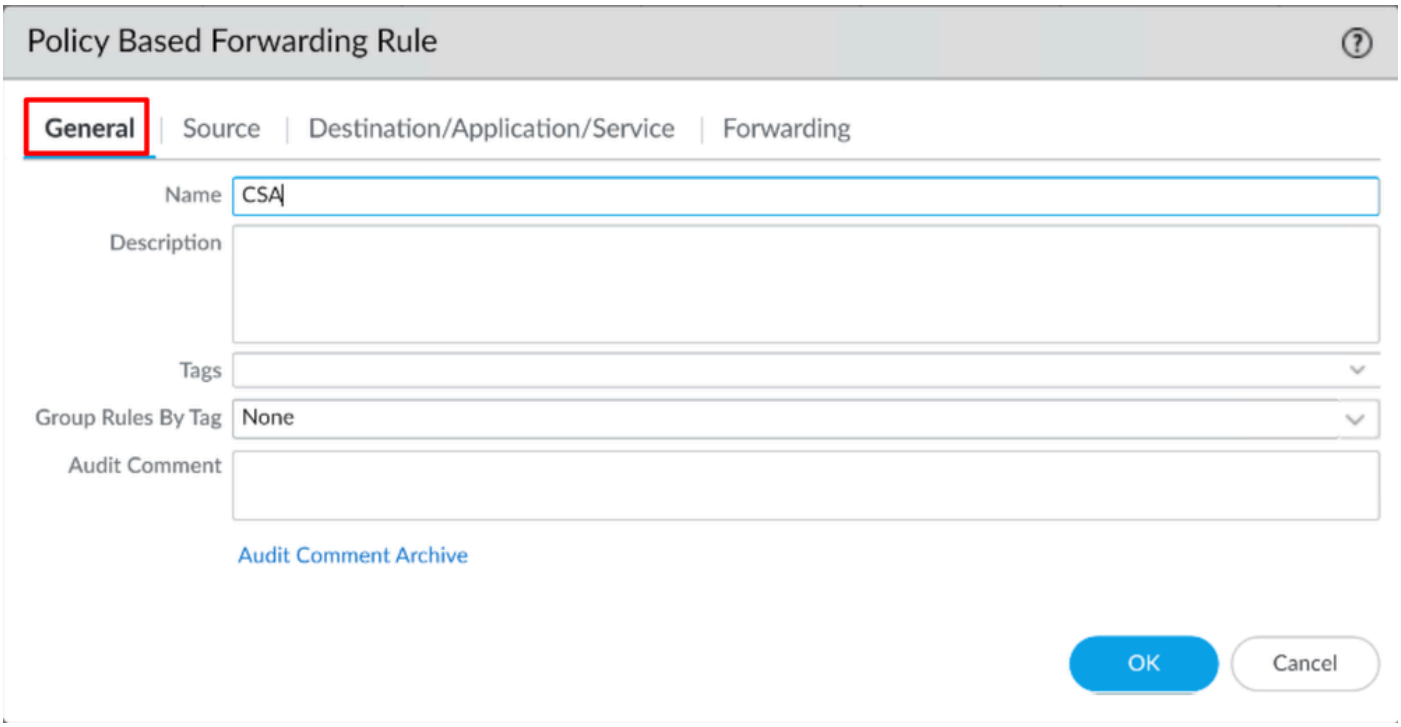
2. Cliquez sur Ajouter.

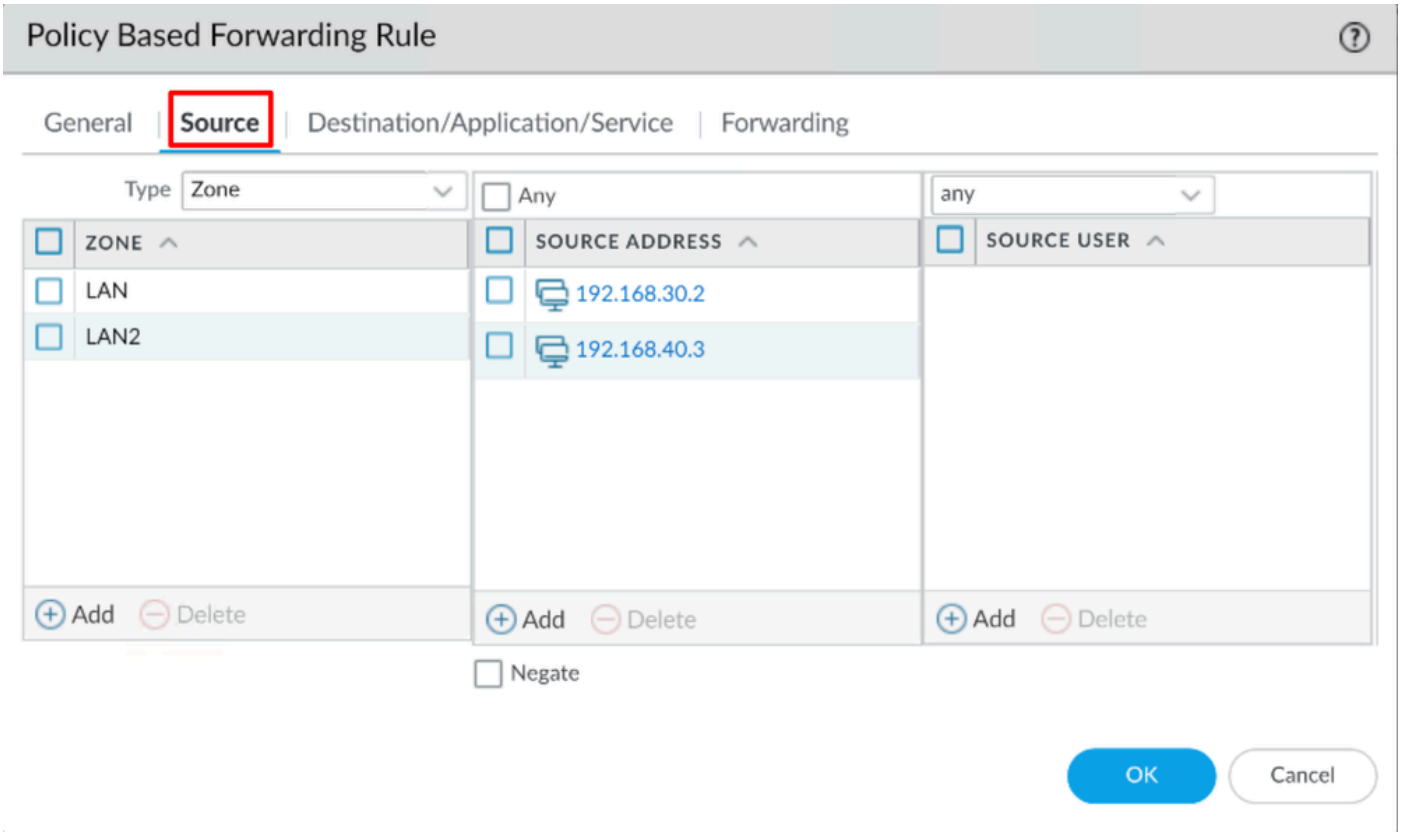


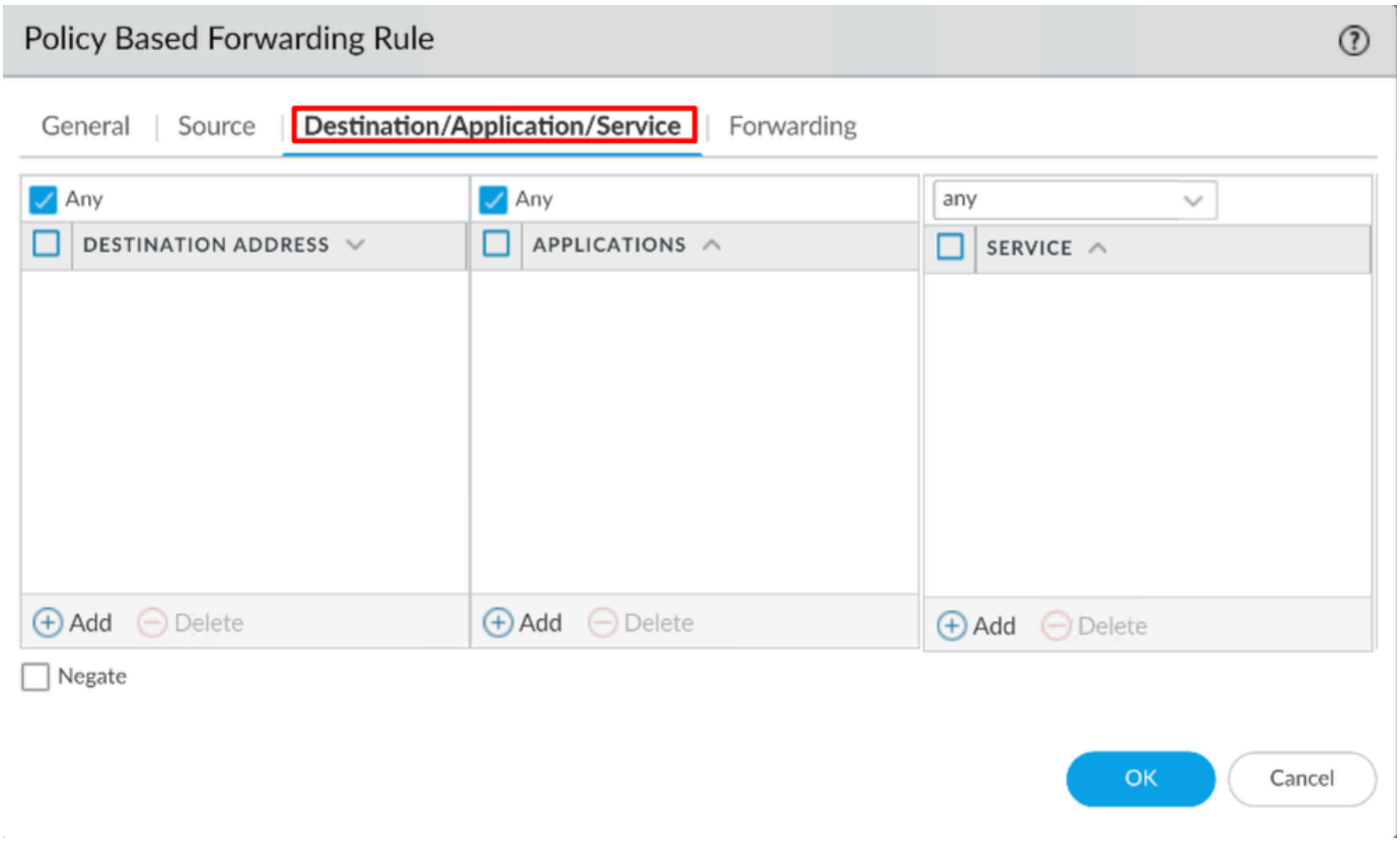
3. Configurez les paramètres suivants :

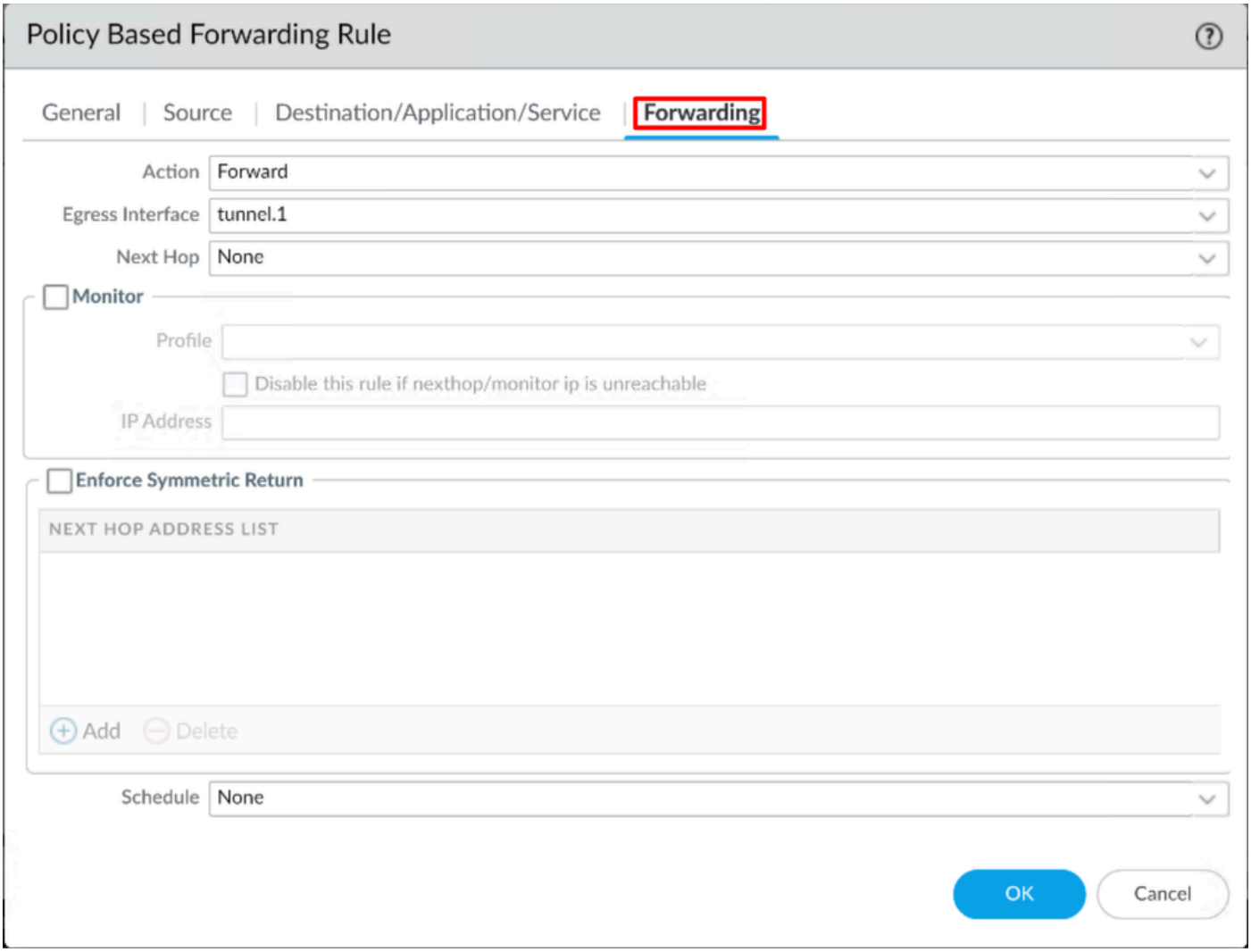
- Généralités
  - Name : Utilisez un nom pour identifier l'accès sécurisé et le transfert de la base de politiques (routage par origine)
- Source
  - Zone(s) : Sélectionnez la ou les zones où vous prévoyez d'acheminer le trafic en fonction de l'origine
  - Adresse source: Configurez le ou les hôtes que vous souhaitez utiliser comme source
  - Utilisateurs source : Configurez les utilisateurs vers lesquels acheminer le trafic (le cas échéant)
- Destination/Application/Service
  - adresse de destination: Vous pouvez laisser la valeur Any ou spécifier les plages d'adresses de l'accès sécurisé (100.64.0.0/10)
- Transmettre
  - Action : Transférer
  - Interface de sortie : Choisissez l'interface de tunnel configurée à l'étape, Configurer l'interface de tunnel.
  - Saut suivant : Aucune

4. Cliquez sur OK et sur Valider.


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

Maintenant tout est configuré sur Palo Alto. Une fois la route configurée, le tunnel peut être établi. Poursuivez la configuration de RA-VPN, ZTA basé sur navigateur ou ZTA de base client sur le tableau de bord d'accès sécurisé.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.