Configure Secure Access with Palo Alto Firewall

Contents

Introduction

This document describes how to configure Secure Access with Palo Alto Firewall.

Prerequisites

- Configure User Provisioning
- ZTNA SSO Authentication Configuration
- Configure Remote Access VPN Secure Access

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on:

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

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

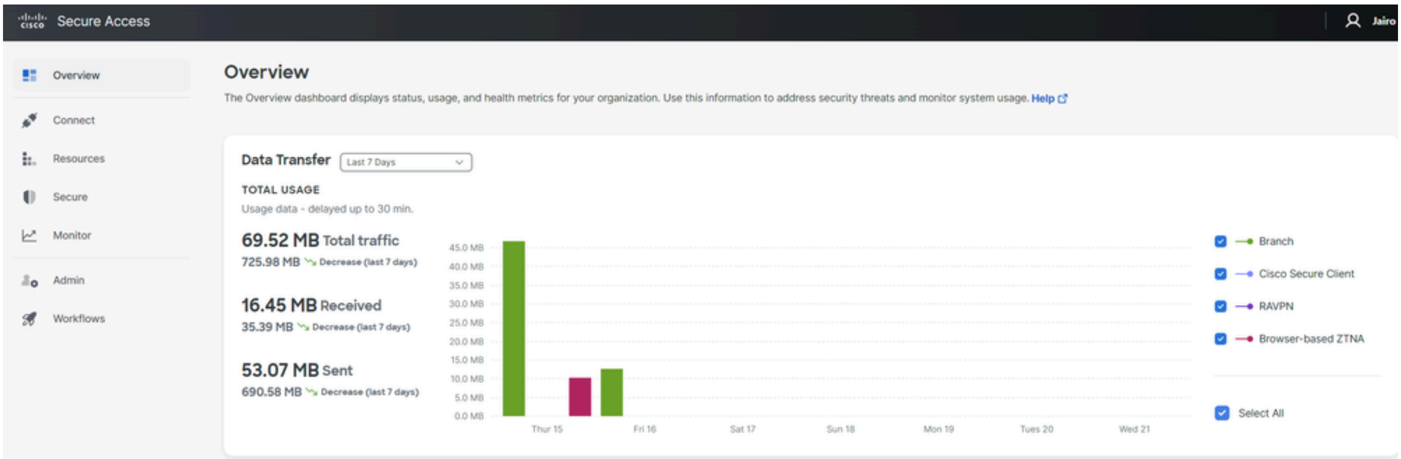
Secure Access - Palo Alto

Cisco has designed Secure Access to protect and provide access to private applications, both on-premise and cloud-based. It also safeguards the connection from the network to the internet. This is achieved through the implementation of multiple security methods and layers, all aimed at preserving the information as they access it via the cloud.

Configure

Configure the VPN on Secure Access

Navigate to the admin panel of Secure Access.



Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

TOTAL USAGE

Usage data - delayed up to 30 min.

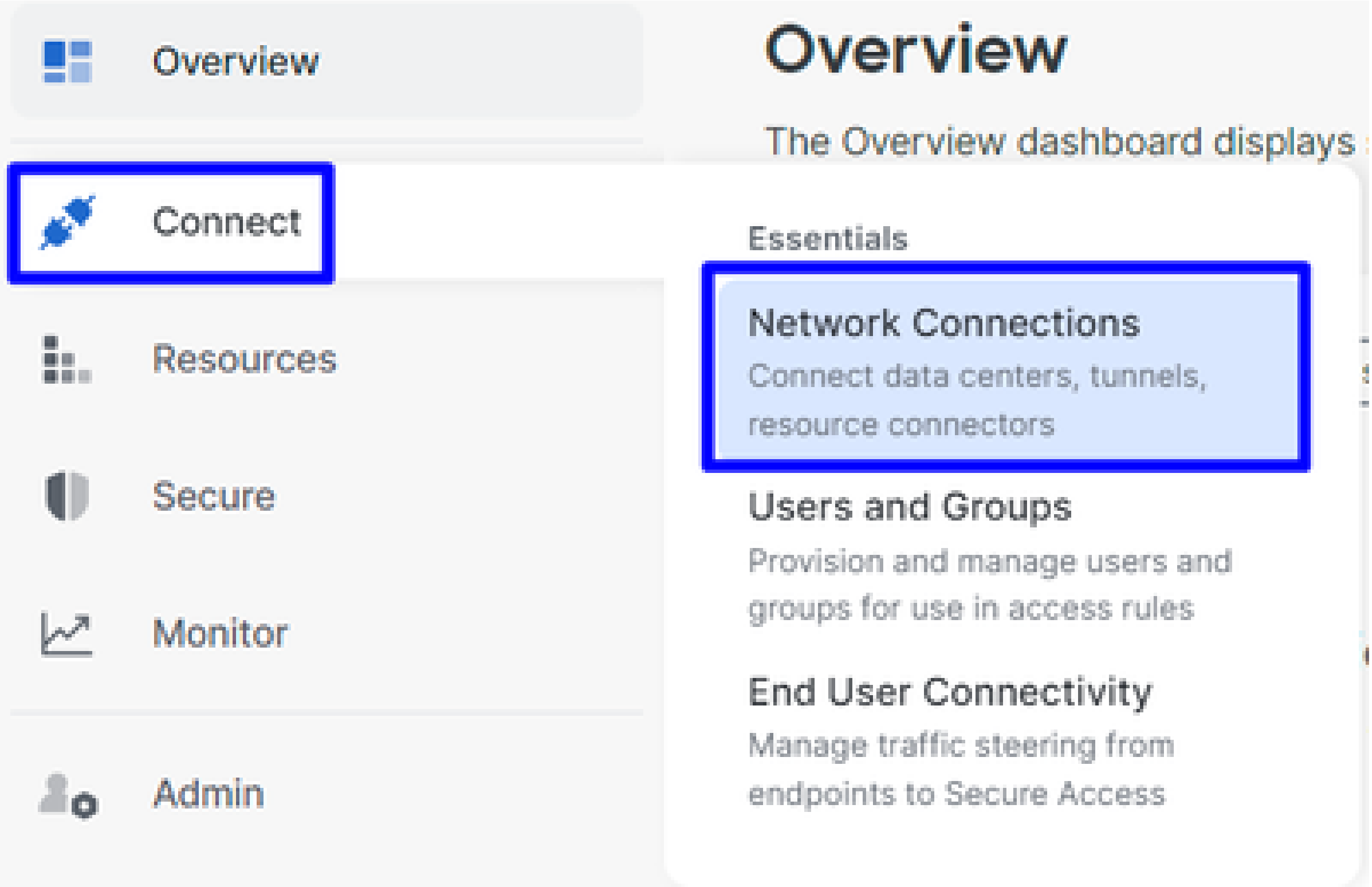
69.52 MB Total traffic
725.98 MB Decrease (last 7 days)

16.45 MB Received
35.39 MB Decrease (last 7 days)

53.07 MB Sent
690.58 MB Decrease (last 7 days)

Secure Access - Main Page

- Click on Connect > Network Connections



The Overview dashboard displays

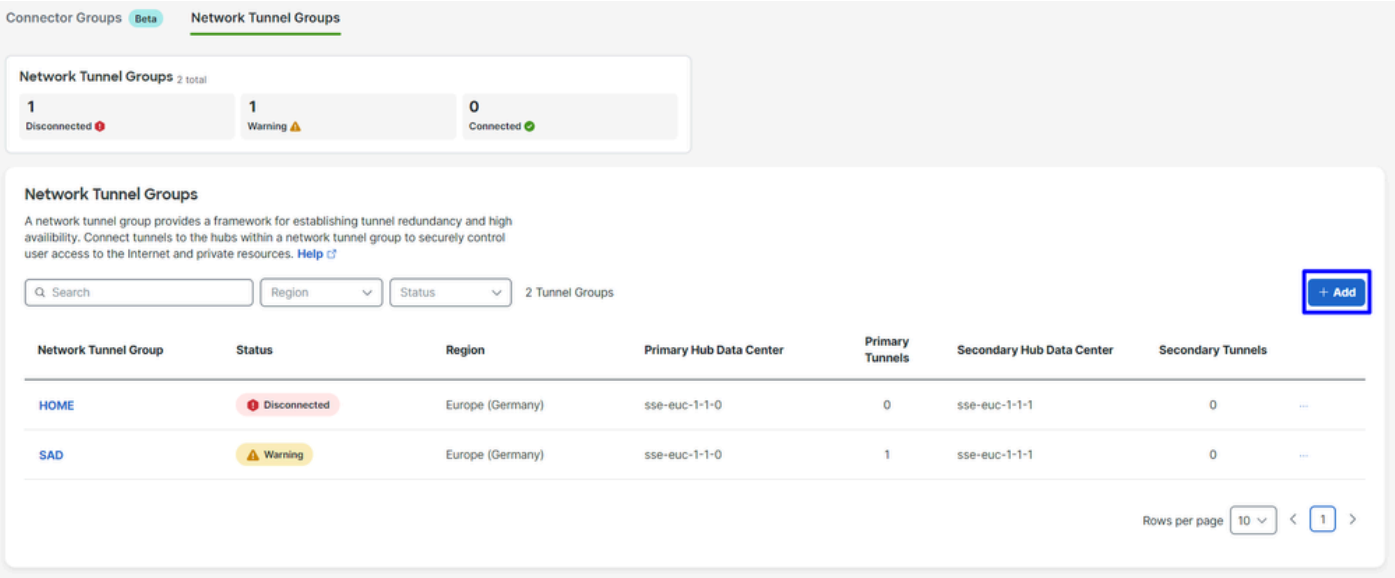
Connect data centers, tunnels, resource connectors

Provision and manage users and groups for use in access rules

Manage traffic steering from endpoints to Secure Access

Secure Access - Network Connections

- Under Network Tunnel Groups click on + Add



Connector Groups Beta

Network Tunnel Groups

Network Tunnel Groups 2 total

1 Disconnected

1 Warning

0 Connected

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

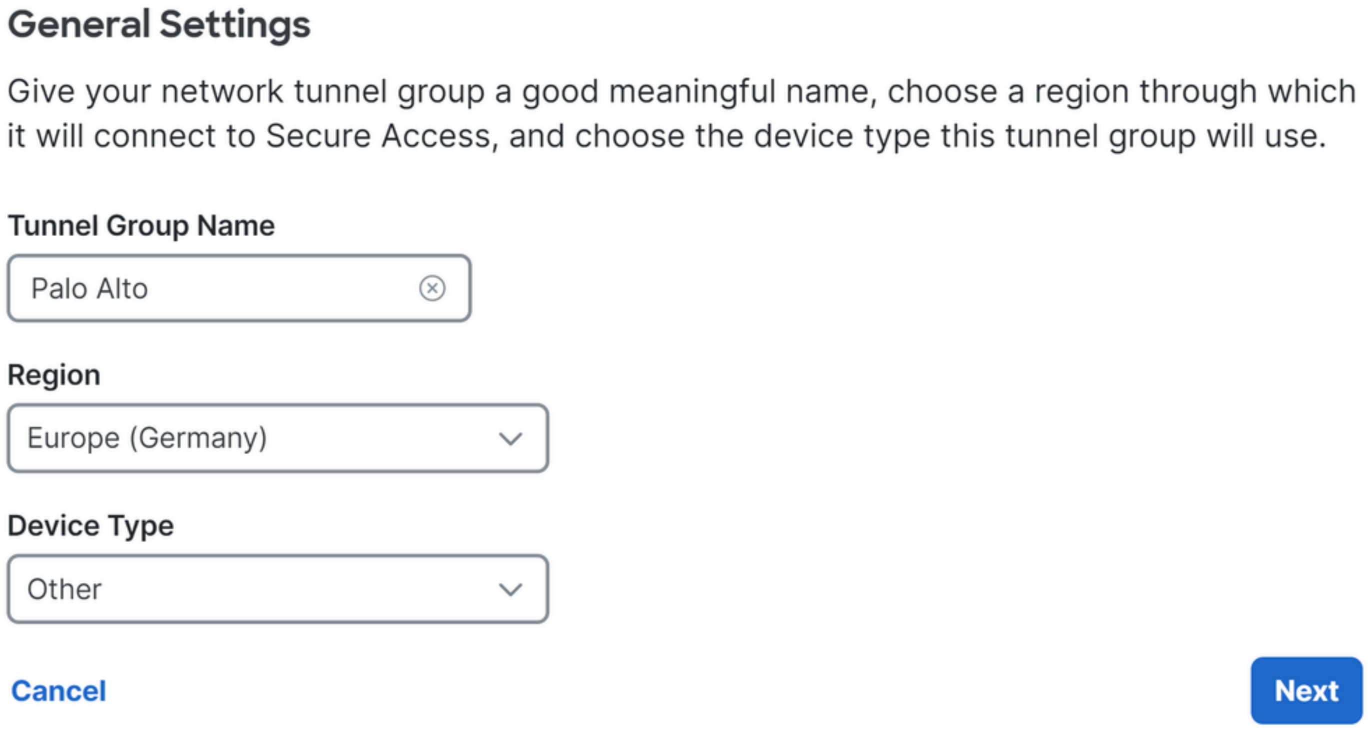
2 Tunnel Groups

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
HOME	Disconnected	Europe (Germany)	sse-euc-1-1-0	0	sse-euc-1-1-1	0
SAD	Warning	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1	0

Rows per page 10 1

Secure Access - Network Tunnel Groups

- Configure Tunnel Group Name, Region and Device Type
- Click **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.

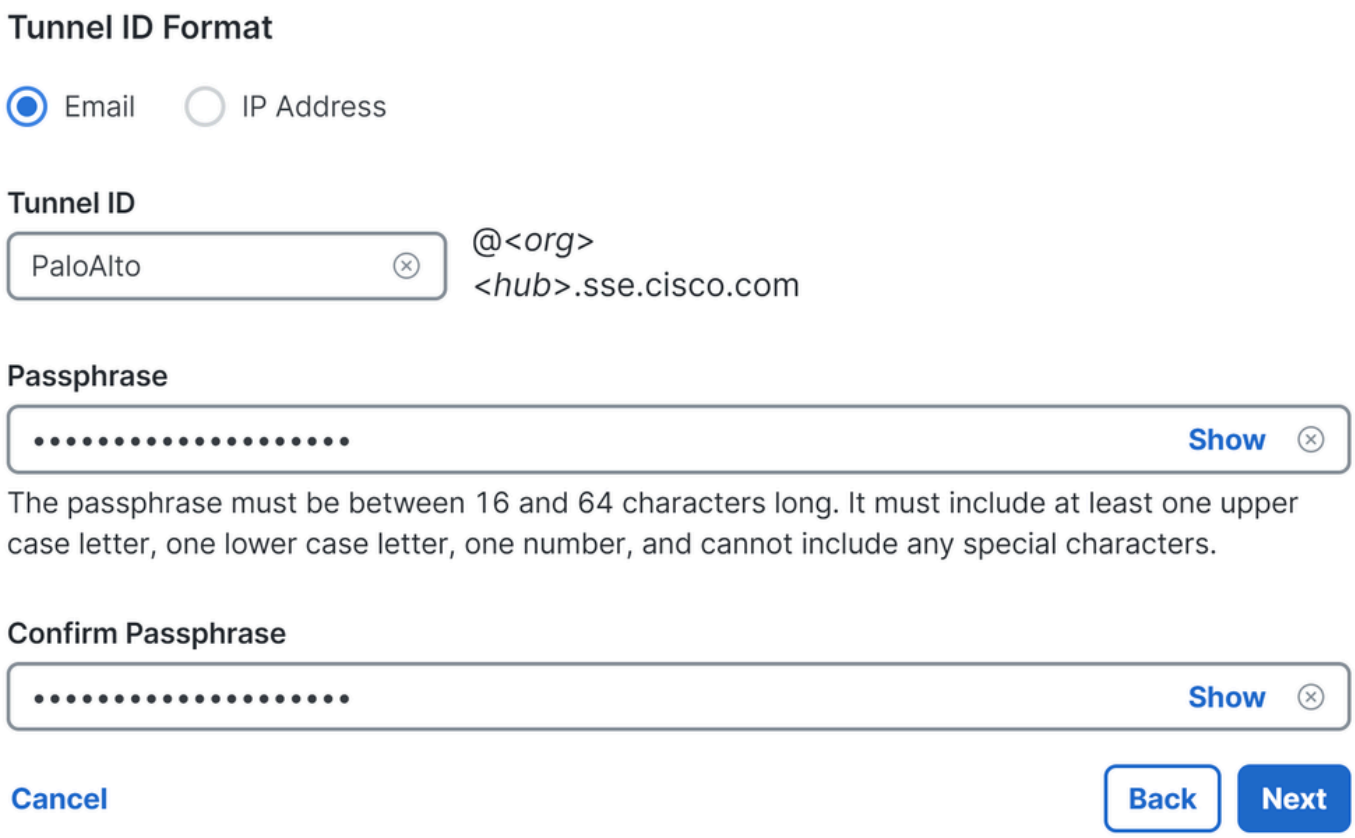
Tunnel Group Name: Palo Alto

Region: Europe (Germany)

Device Type: Other

Note: Choose the region nearest to the location of your firewall.

- Configure the Tunnel ID Format and Passphrase
- Click Next



Tunnel ID Format

● Email ○ IP Address

Tunnel ID

PaloAlto @<org><hub>.sse.cisco.com

Passphrase

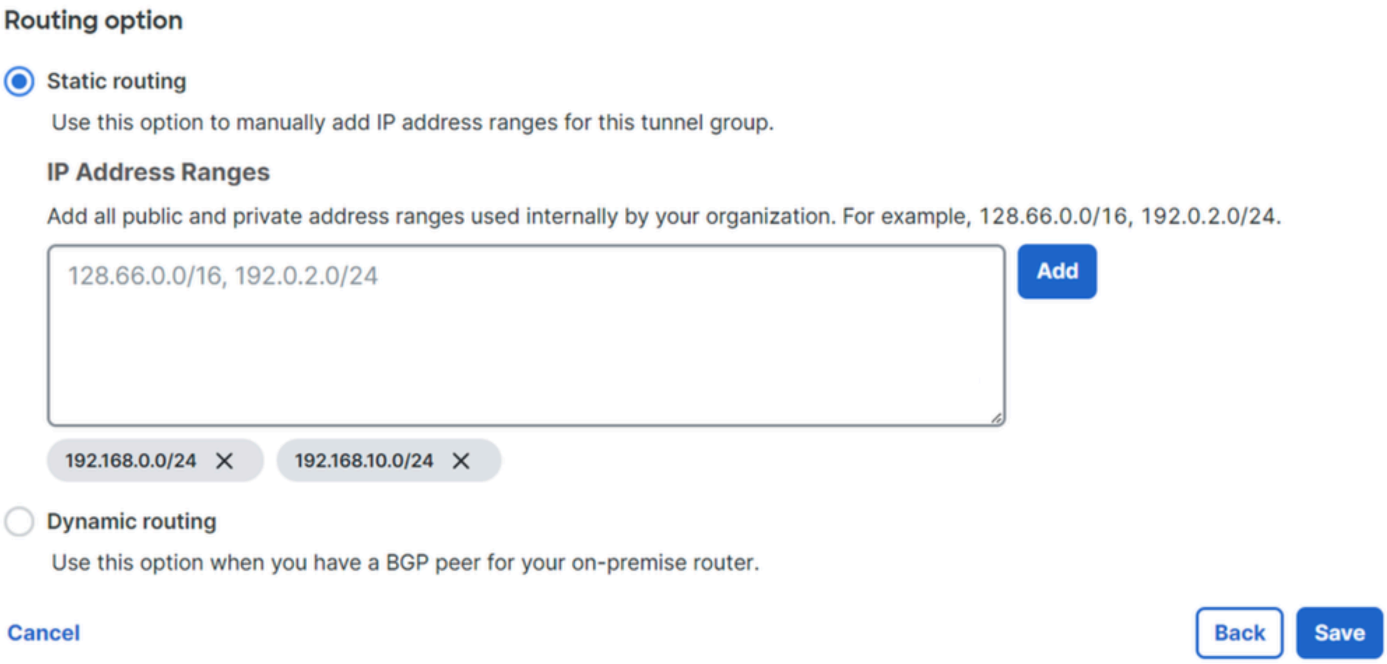
•••••••••••••••••••• Show

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

•••••••••••••••••••• Show

- Configure the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access
- Click **Save**



Routing option

● Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24

192.168.0.0/24 ✕ 192.168.10.0/24 ✕

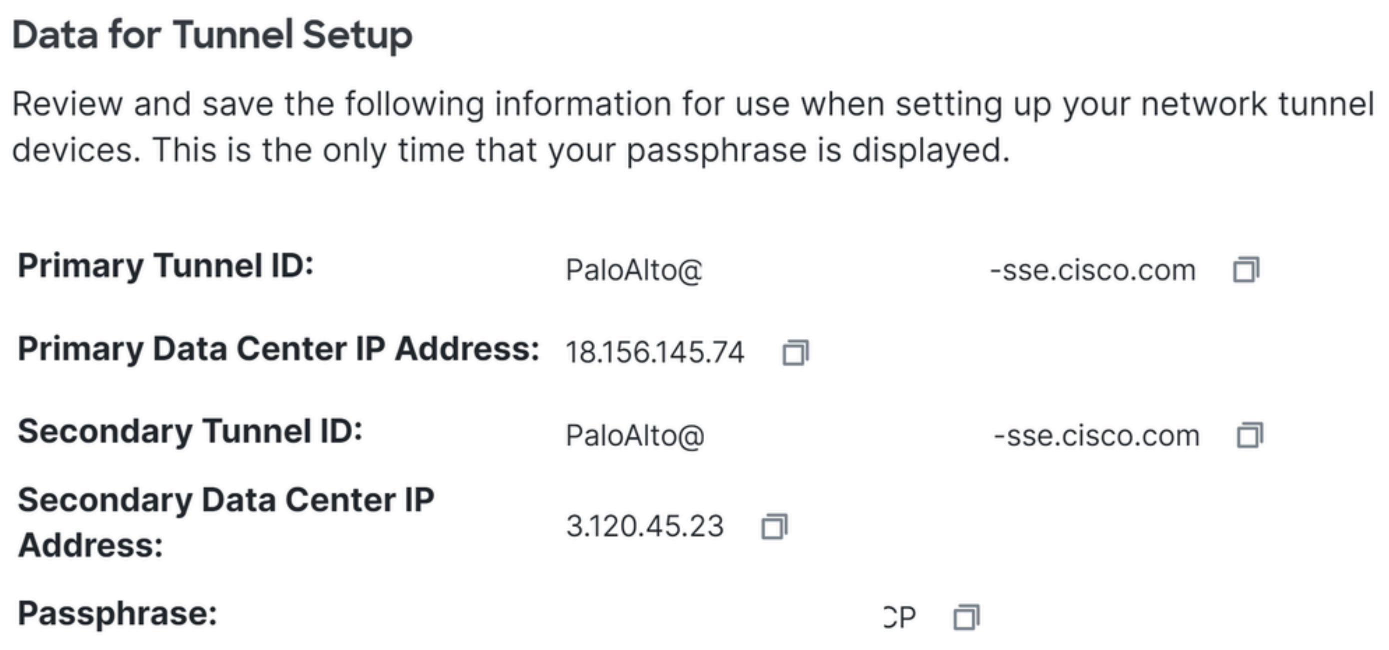
○ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Secure Access - Tunnel Groups - Routing Options

After you click on **Save** the information about the tunnel gets displayed, please save that information for the next step, **Configure the tunnel on Palo Alto.**

Tunnel Data



Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

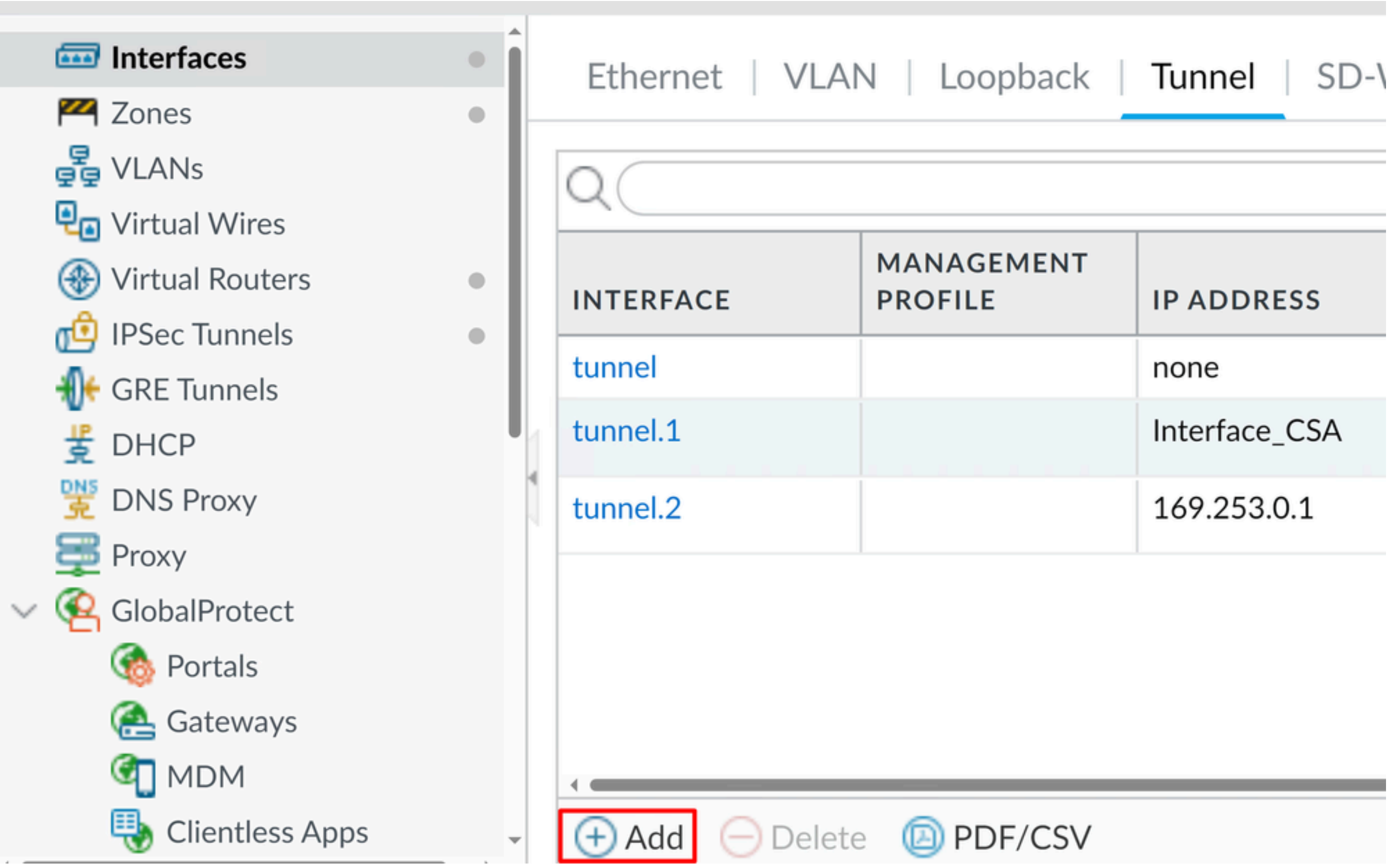
Primary Tunnel ID:	PaloAlto@ -sse.cisco.com
Primary Data Center IP Address:	18.156.145.74
Secondary Tunnel ID:	PaloAlto@ -sse.cisco.com
Secondary Data Center IP Address:	3.120.45.23
Passphrase:	CP

Configure the tunnel on Palo Alto

Configure the Tunnel Interface

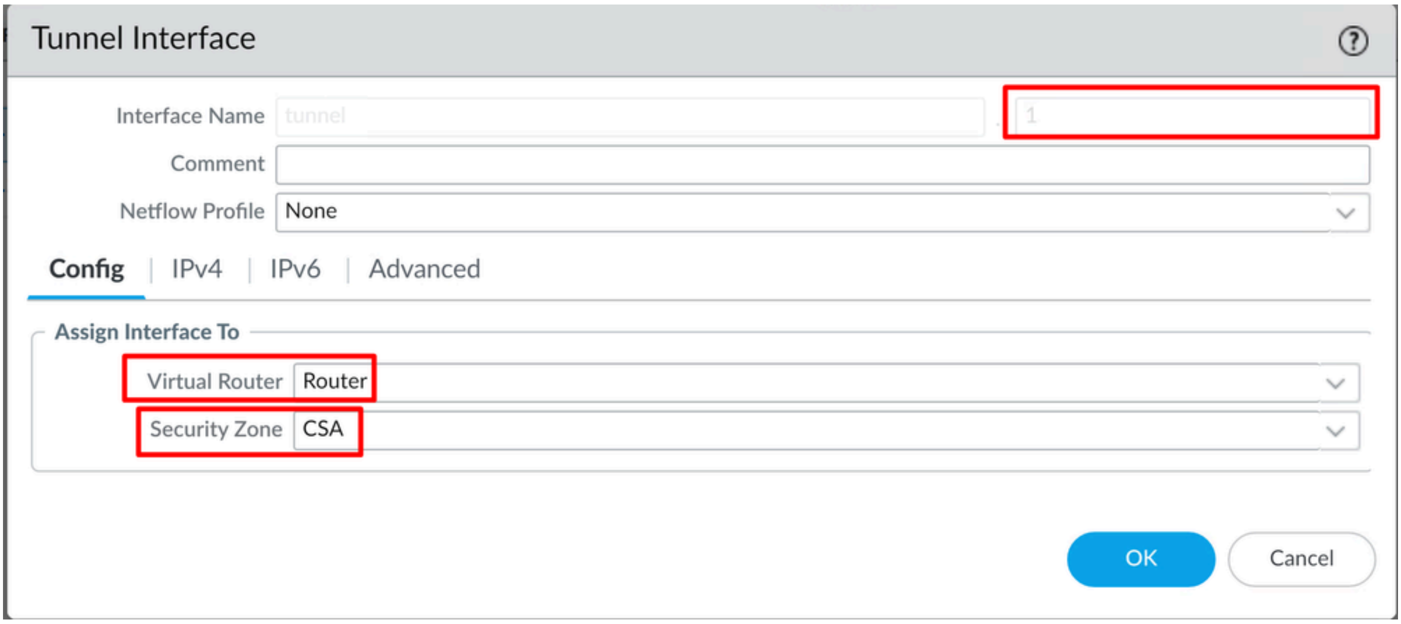
Navigate to the Palo Alto Dashboard.

- Network > Interfaces > Tunnel
- Click Add



INTERFACE	MANAGEMENT PROFILE	IP ADDRESS
tunnel		none
tunnel.1		Interface_CSA
tunnel.2		169.253.0.1

- Under Config menu, configure the Virtual Router, Security Zone, and assign aSuffix Number



Tunnel Interface

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

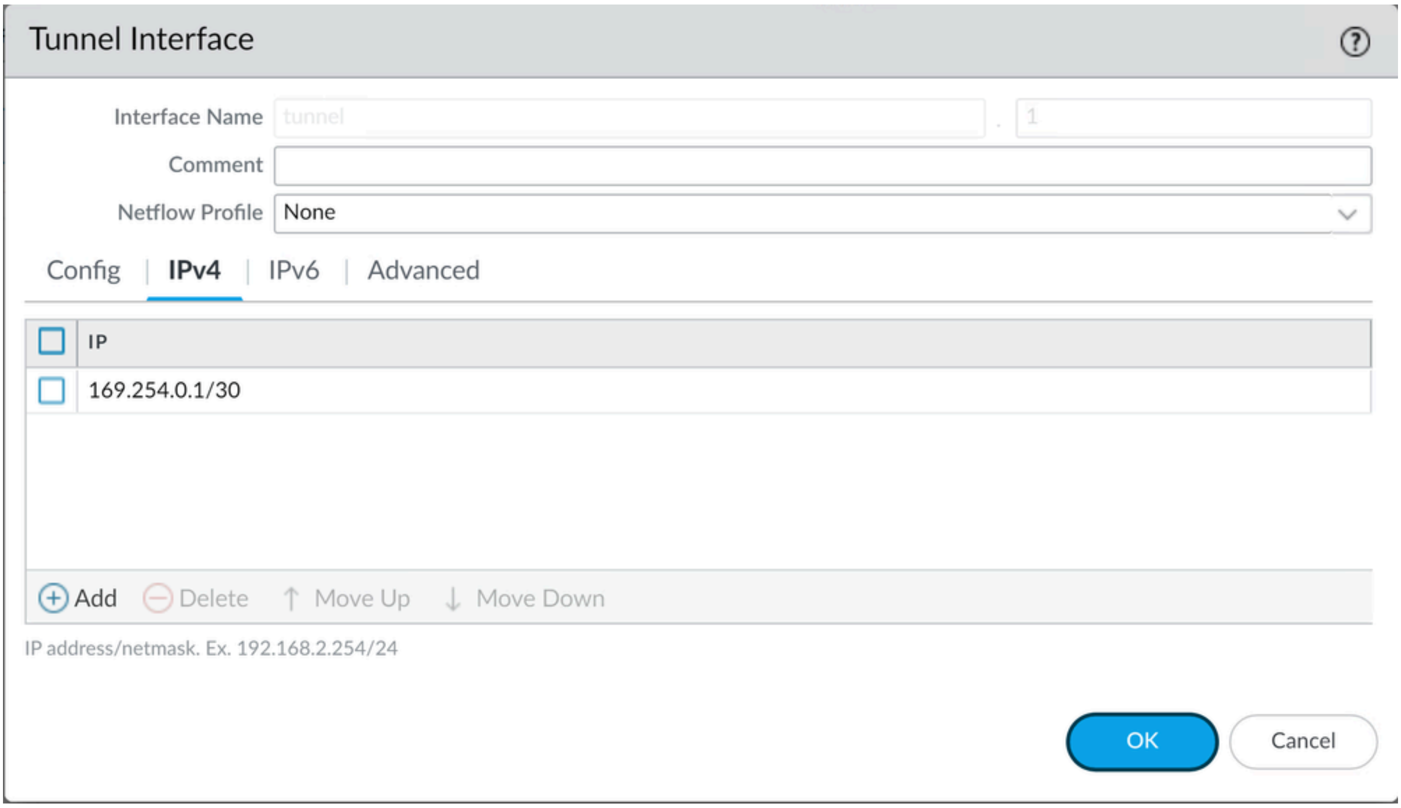
Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: Router

Security Zone: CSA

- Under IPv4, configure a non-routable IP. For example, you can use 169.254.0.1/30
- ClickOK



Tunnel Interface

Interface Name: tunnel . 1

Comment:

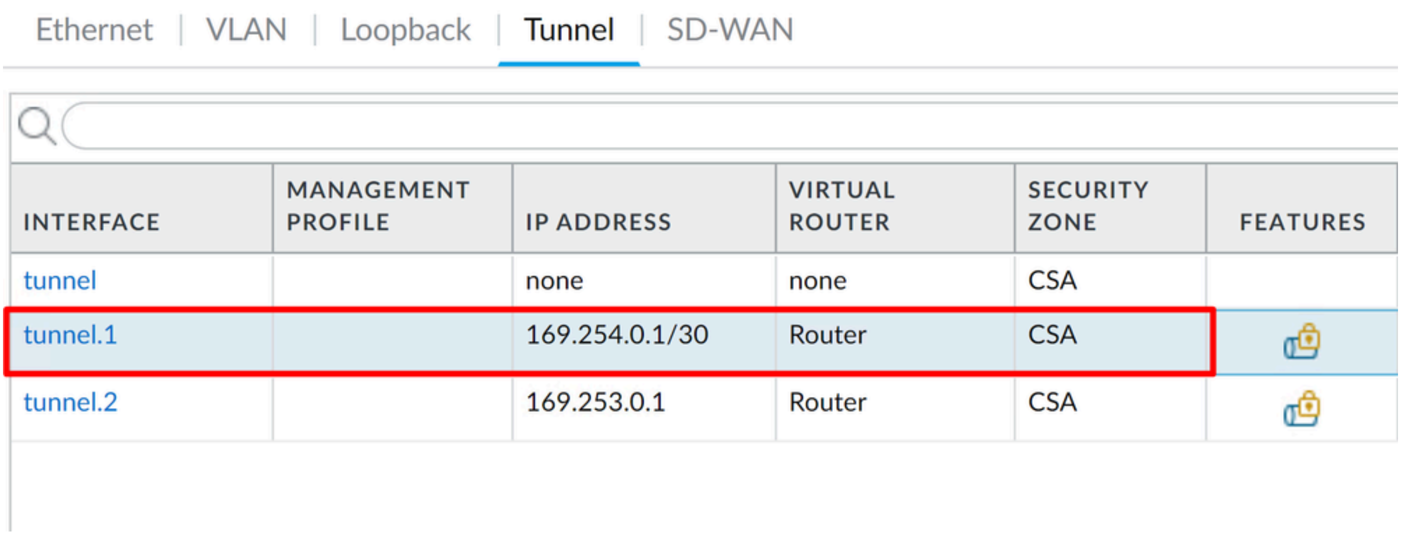
Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

□	IP
□	169.254.0.1/30

IP address/netmask. Ex. 192.168.2.254/24

After that, you can have something like this configured:



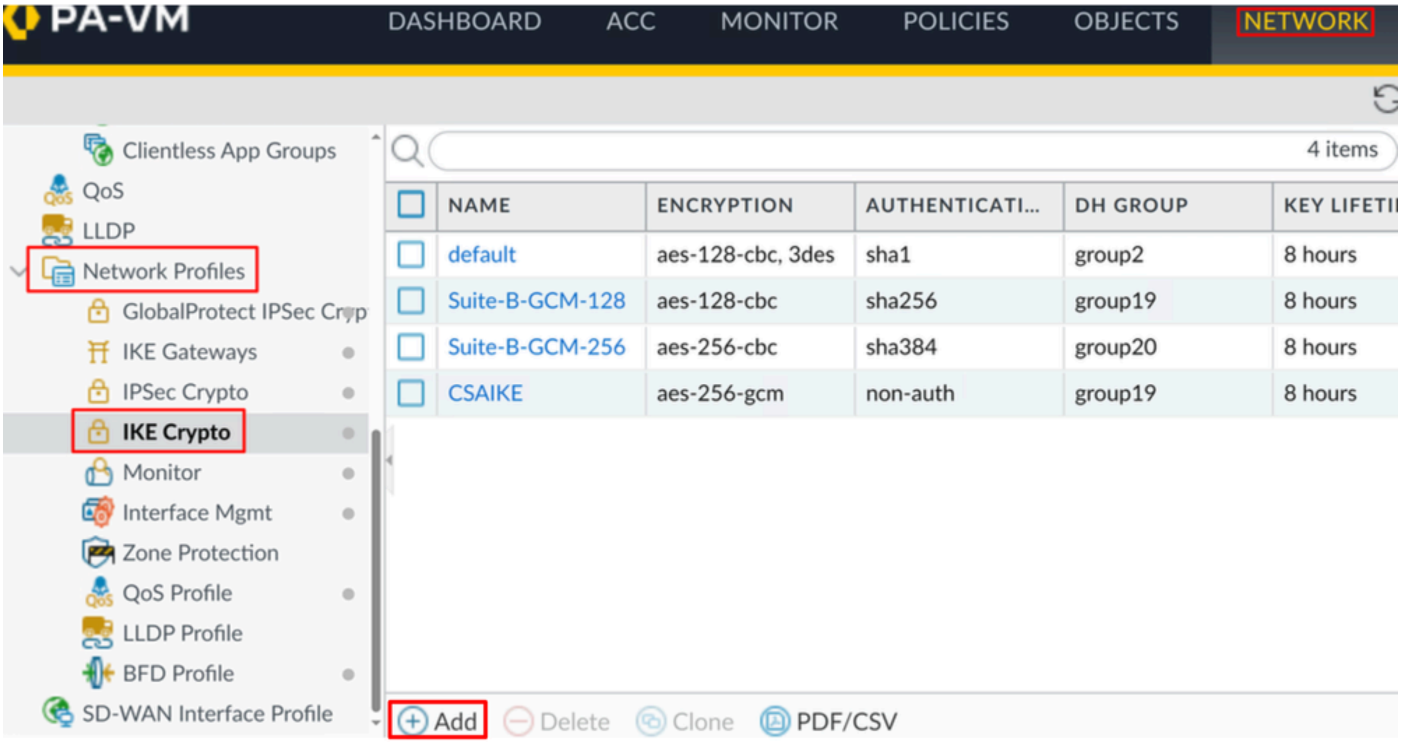
INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES
tunnel		none	none	CSA	
tunnel.1		169.254.0.1/30	Router	CSA	
tunnel.2		169.253.0.1	Router	CSA	

If you have it configured like this, you can click on **Commit** to save the configuration and continue with the next step, Configure IKE Crypto Profile.

Configure IKE Crypto Profile

To configure the crypto profile, navigate to:

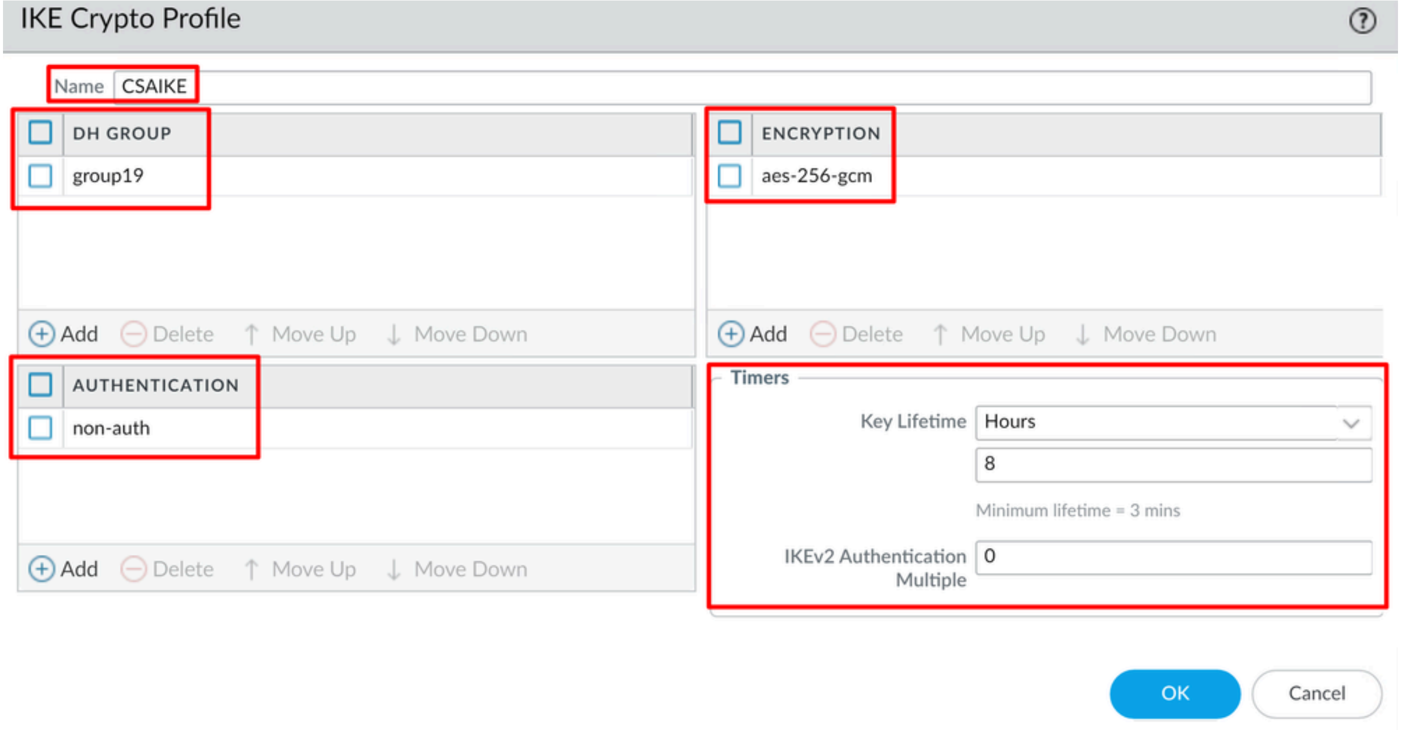
- Network > Network Profile > IKE Crypto
- ClickAdd



□	NAME	ENCRYPTION	AUTHENTICATI...	DH GROUP	KEY LIFETI
□	default	aes-128-cbc, 3des	sha1	group2	8 hours
□	Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
□	Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours
□	CSAIKE	aes-256-gcm	non-auth	group19	8 hours

- Configure the next parameters:
  - **Name**: Configure a name to identify the profile.
  - **DH GROUP**: group19
  - **AUTHENTICATION**: non-auth
  - **ENCRYPTION**: aes-256-gcm
  - Timers
    - Key Lifetime: 8 Hours

    - **IKEv2 Authentication**: 0
- After you have everything configured, click **OK**



IKE Crypto Profile

Name: CSAIKE

□	DH GROUP
□	group19

□	ENCRYPTION
□	aes-256-gcm

□	AUTHENTICATION
□	non-auth

Timers

Key Lifetime: Hours

8

Minimum lifetime = 3 mins

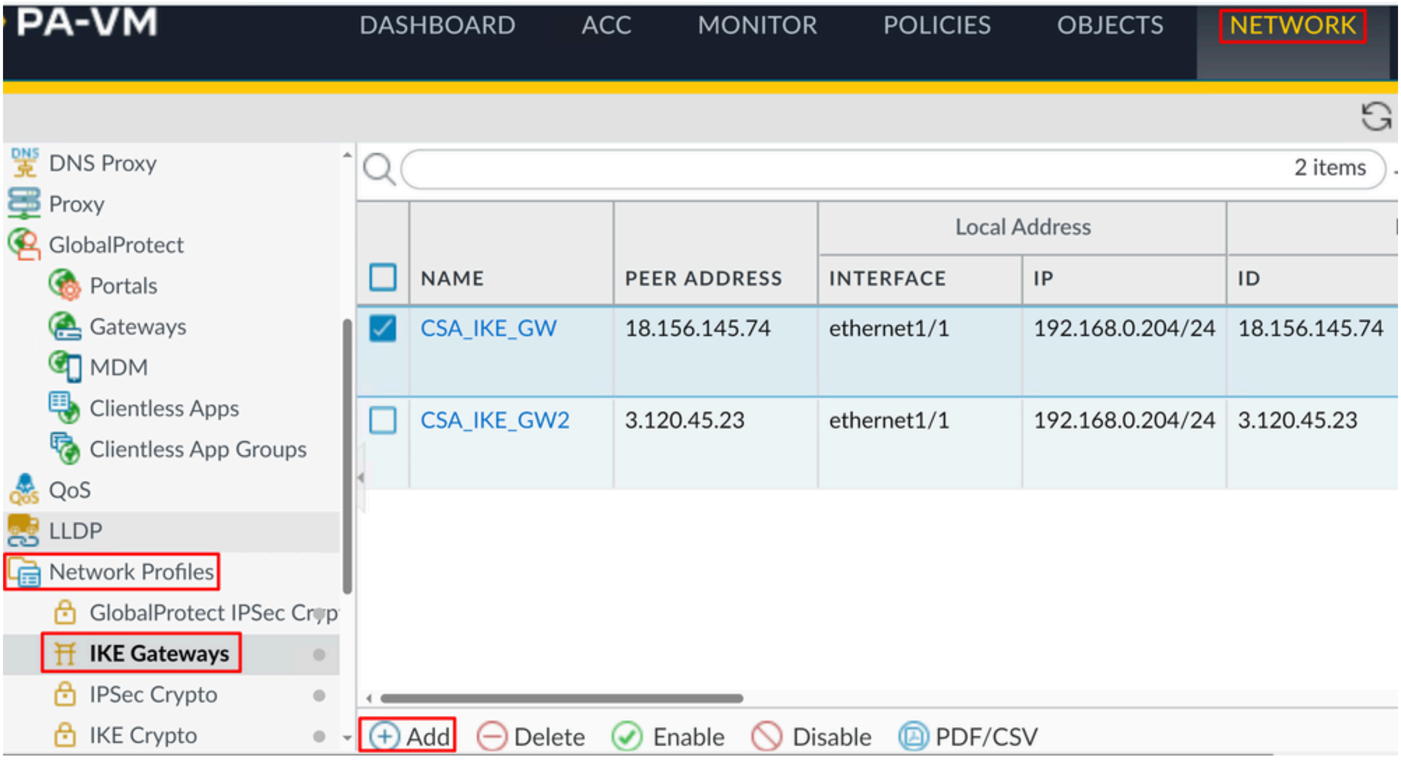
IKEv2 Authentication Multiple: 0

If you have it configured like this, you can click on **Commit** to save the configuration and continue with the next step, Configure IKE Gateways.

Configure IKE Gateways

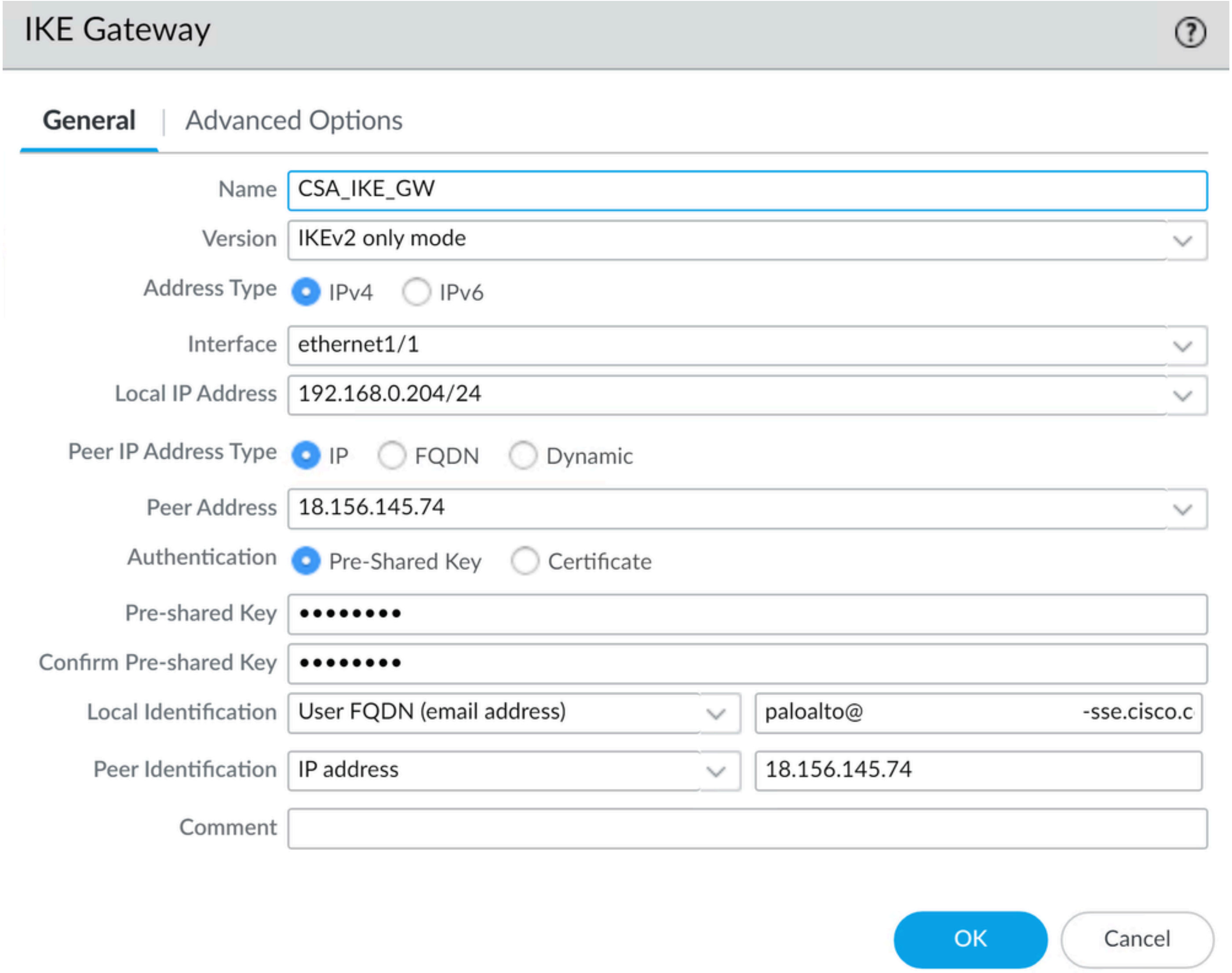
To configure IKE Gateways

- Network > Network Profile > IKE Gateways
- ClickAdd



			Local Address		
☐	NAME	PEER ADDRESS	INTERFACE	IP	ID
☑	CSA_IKE_GW	18.156.145.74	ethernet1/1	192.168.0.204/24	18.156.145.74
☐	CSA_IKE_GW2	3.120.45.23	ethernet1/1	192.168.0.204/24	3.120.45.23

- Configure the next parameters:
  - Name: Configure a name to identify the Ike Gateways.
  - **Version** : IKEv2 only mode
  - Address Type : IPv4
  - **Interface** : Select your Internet WAN interface.
  - Local IP Address: Select the IP of your Internet WAN Interface.
  - **Peer IP Address Type** : IP
  - Peer Address: Use the IP of Primary IP Datacenter IP Address, given in the step Tunnel Data.
  - Authentication: Pre-Shared Key
  - Pre-shared Key : Use the **passphrase** given in the step Tunnel Data.
  - **Confirm Pre-shared Key** : Use the **passphrase** given in the step Tunnel Data.
  - **Local Identification** : Choose **User FQDN (Email address)** and use the **Primary Tunnel ID** given in the step, Tunnel Data.
  - **Peer Identification** : ChooseIP Addressand use the Primary IP Datacenter IP Address.

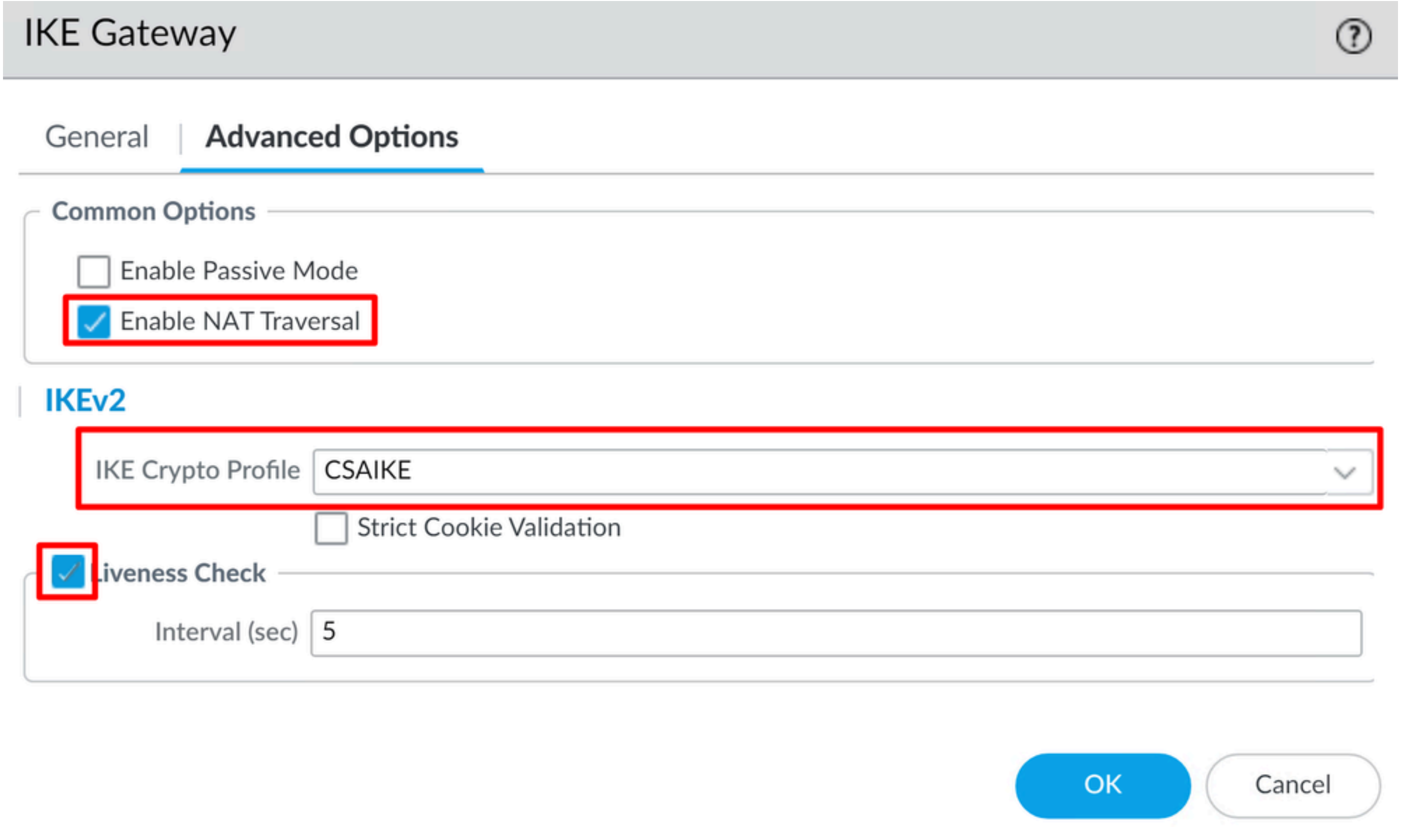


IKE Gateway

General | Advanced Options

Name	CSA_IKE_GW
Version	IKEv2 only mode
Address Type	● IPv4 ○ IPv6
Interface	ethernet1/1
Local IP Address	192.168.0.204/24
Peer IP Address Type	● IP ○ FQDN ○ Dynamic
Peer Address	18.156.145.74
Authentication	● Pre-Shared Key ○ Certificate
Pre-shared Key	••••••••
Confirm Pre-shared Key	••••••••
Local Identification	User FQDN (email address) paloalto@ -sse.cisco.c
Peer Identification	IP address 18.156.145.74
Comment	

- ClickAdvanced Options
  - **Enable NAT Traversal**
  - Select the **IKE Crypto Profile** created on the step, Configure IKE Crypto Profile
  - Mark the checkbox for **Liveness Check**
  - Click **OK**



IKE Gateway

General | **Advanced Options**

Common Options

□ Enable Passive Mode

☑ Enable NAT Traversal

IKEv2

IKE Crypto Profile: CSAIKE

□ Strict Cookie Validation

☑ Liveness Check

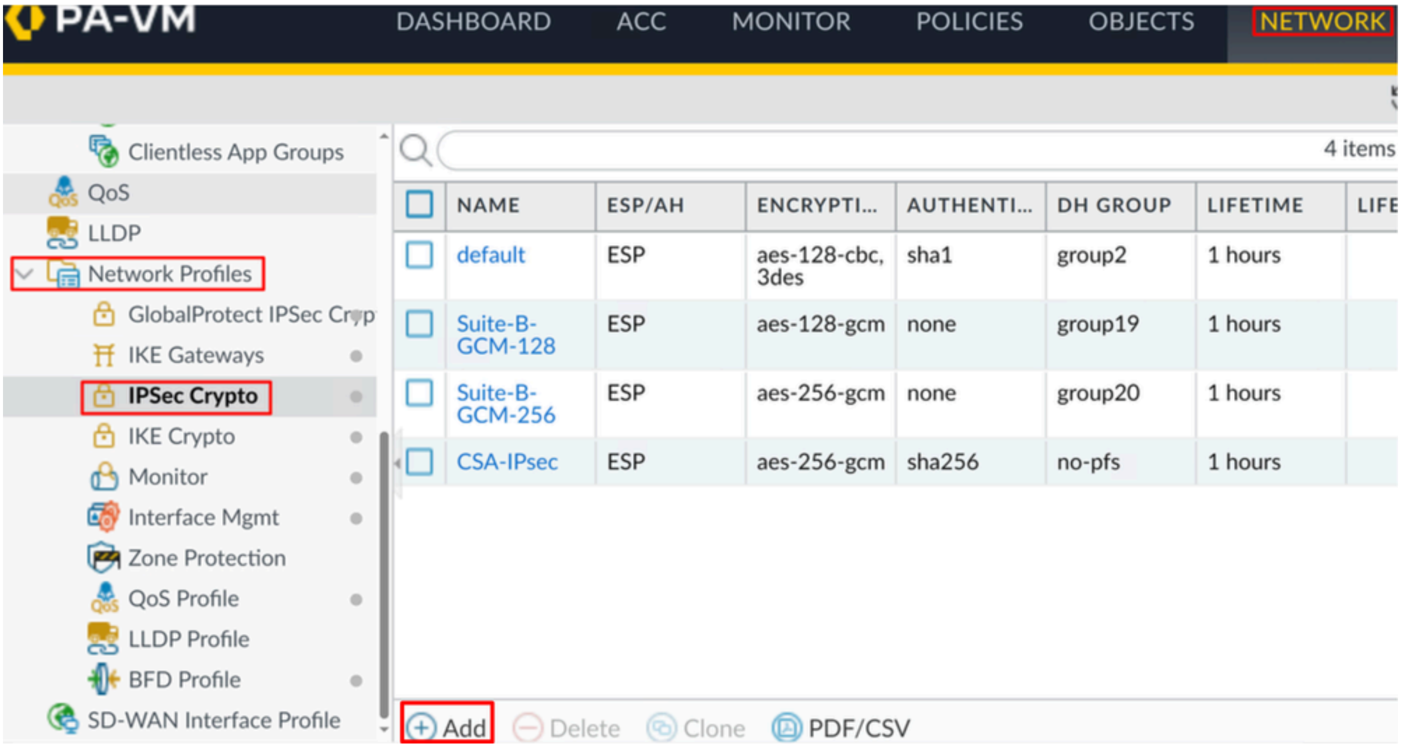
Interval (sec): 5

If you have it configured like this, you can click on **Commit** to save the configuration and continue with the next step, Configure IPSEC Crypto.

Configure IPSEC Crypto Profile

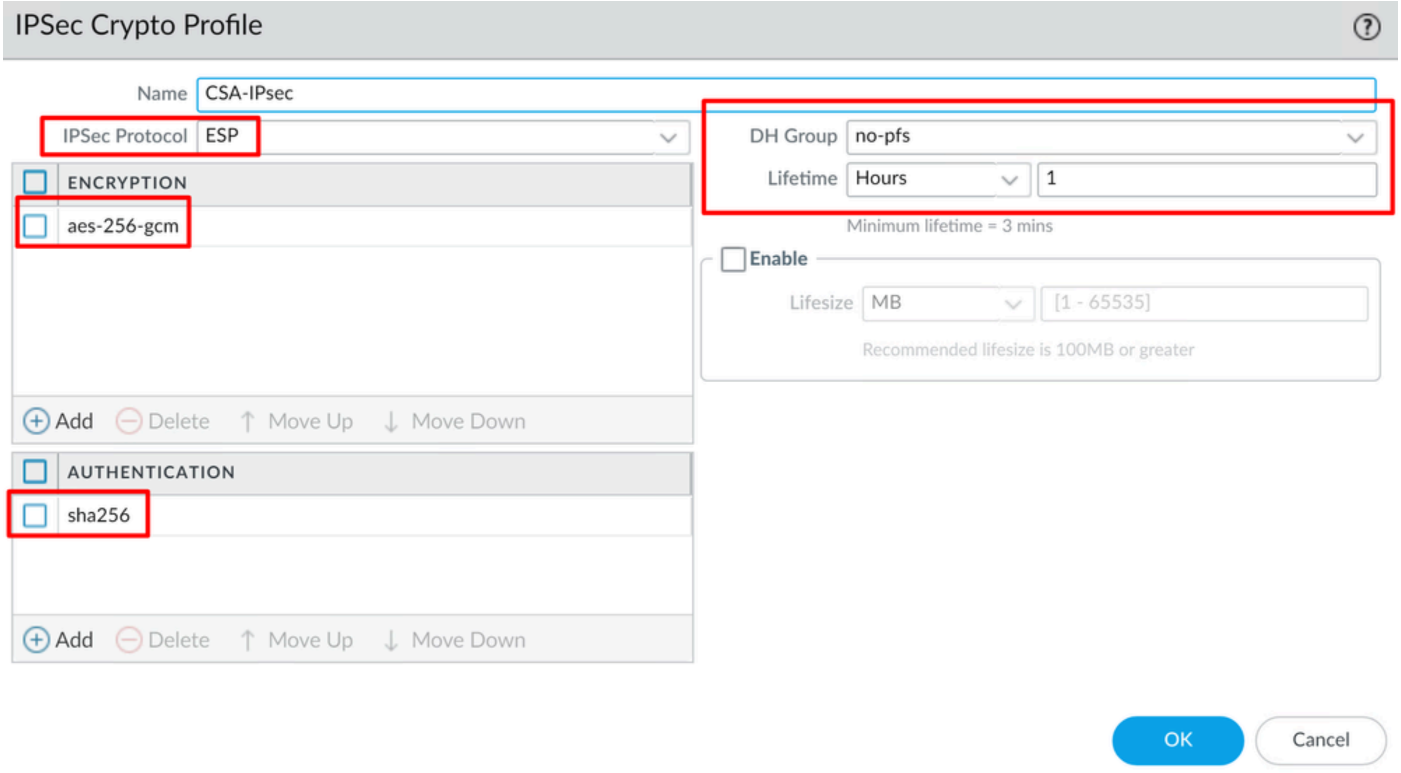
To configure IKE Gateways, Navigate to Network > Network Profile > IPSEC Crypto

- ClickAdd



NAME	ESP/AH	ENCRYPTI...	AUTHENTI...	DH GROUP	LIFETIME	LIFE
default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	
CSA-IPsec	ESP	aes-256-gcm	sha256	no-pfs	1 hours	

- Configure the next parameters:
  - **Name**: Use a name to identify the Secure Access IPsec Profile
  - IPSec Protocol: ESP
  - **ENCRYPTION**: aes-256-gcm
  - DH Group: no-pfs, 1 Hour
- Click OK



IPSec Crypto Profile

Name: CSA-IPsec

IPSec Protocol: ESP

□ ENCRYPTION

□ aes-256-gcm

□ AUTHENTICATION

□ sha256

DH Group: no-pfs

Lifetime: Hours 1

Minimum lifetime = 3 mins

□ Enable

Lifesize: MB [1 - 65535]

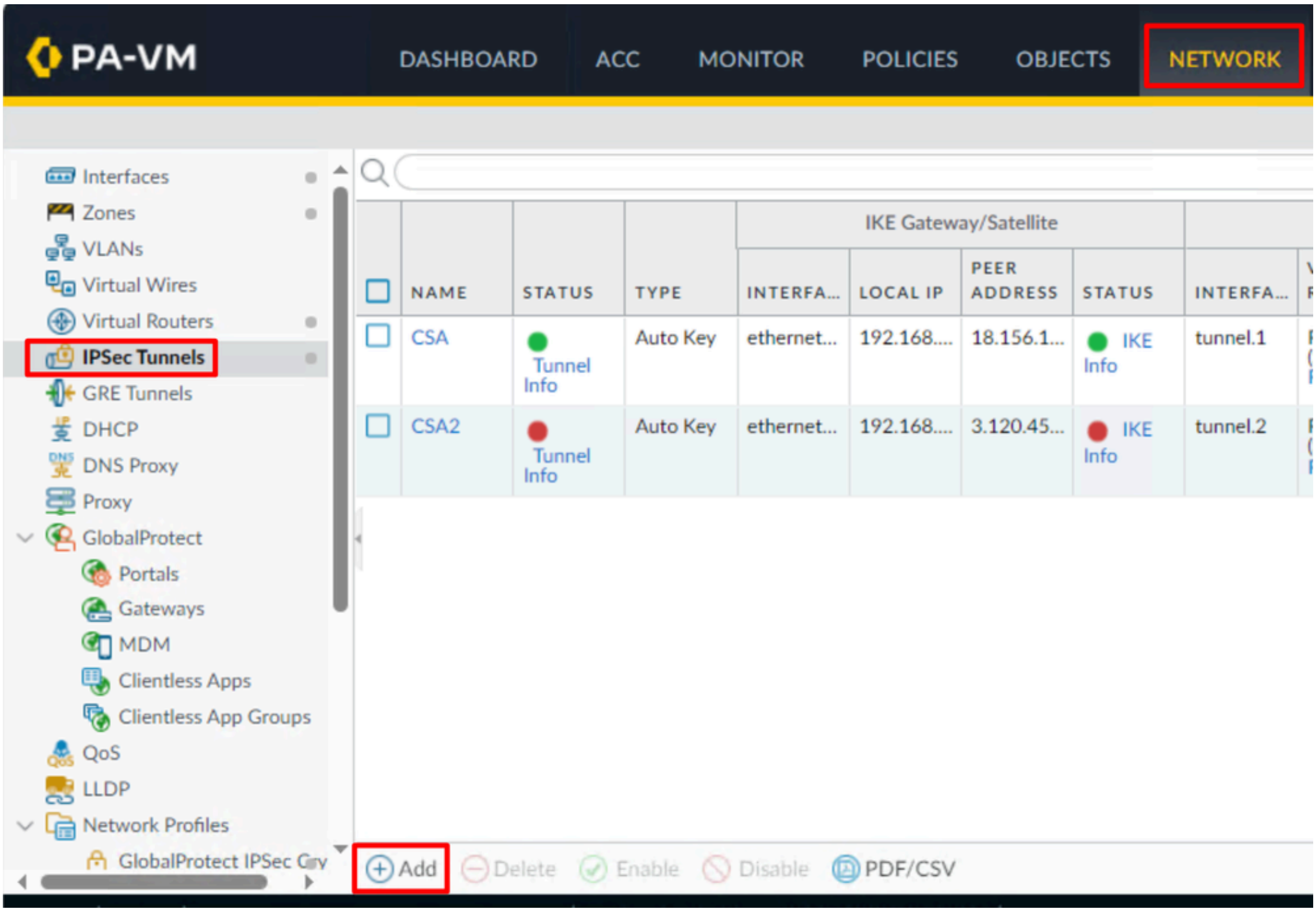
Recommended lifesize is 100MB or greater

If you have it configured like this, you can click on **Commit** to save the configuration and continue with the next step, Configure IPSec Tunnels.

Configure IPSec Tunnels

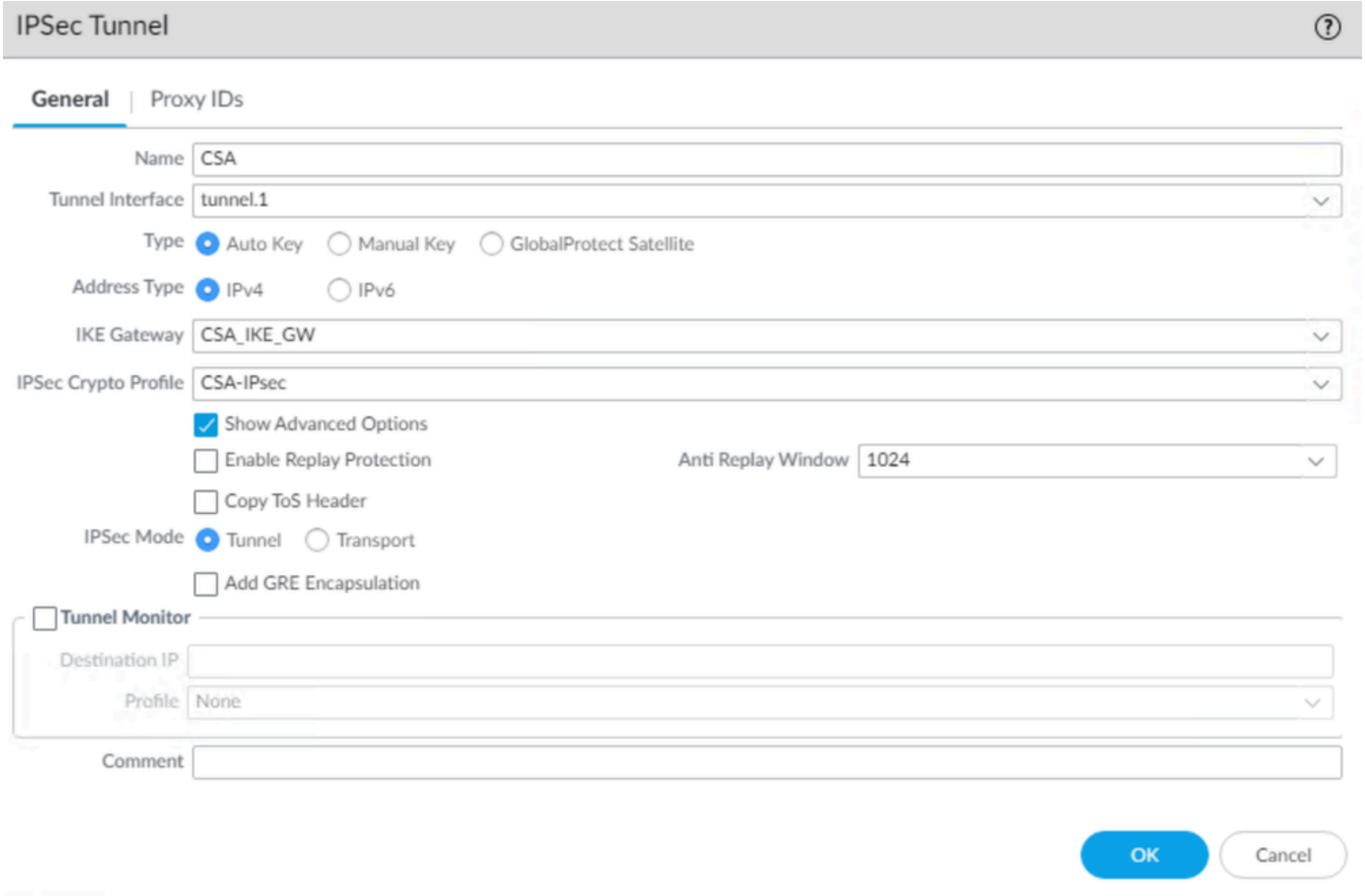
To configure **IPSec Tunnels**, navigate to Network > IPSec Tunnels.

- Click Add



				IKE Gateway/Satellite				
☐	NAME	STATUS	TYPE	INTERFA...	LOCAL IP	PEER ADDRESS	STATUS	INTERFA...
☐	CSA	● Tunnel Info	Auto Key	ethernet...	192.168....	18.156.1...	● IKE Info	tunnel.1
☐	CSA2	● Tunnel Info	Auto Key	ethernet...	192.168....	3.120.45...	● IKE Info	tunnel.2

- Configure the next parameters:
  - **Name**: Use a name to identify the Secure Access tunnel
  - **Tunnel Interface**: Choose the tunnel interface configured on the step, Configure the tunnel interface.
  - **Type**: Auto Key
  - **Address Type**: IPv4
  - **IKE Gateways**: Choose the IKE Gateways configured on the step, Configure IKE Gateways.
  - **IPsec Crypto Profile**: Choose the IKE Gateways configured on the step, Configure IPSEC Crypto Profile
  - Mark the checkbox for **Advanced Options**
    - **IPSec Mode Tunnel**: Choose Tunnel.
- Click OK



Name: CSA

Tunnel Interface: tunnel.1

Type: ● Auto Key ○ Manual Key ○ GlobalProtect Satellite

Address Type: ● IPv4 ○ IPv6

IKE Gateway: CSA_IKE_GW

IPSec Crypto Profile: CSA-IPsec

☑ Show Advanced Options

□ Enable Replay Protection   Anti Replay Window: 1024

□ Copy ToS Header

IPSec Mode: ● Tunnel ○ Transport

□ Add GRE Encapsulation

□ Tunnel Monitor

Destination IP:

Profile: None

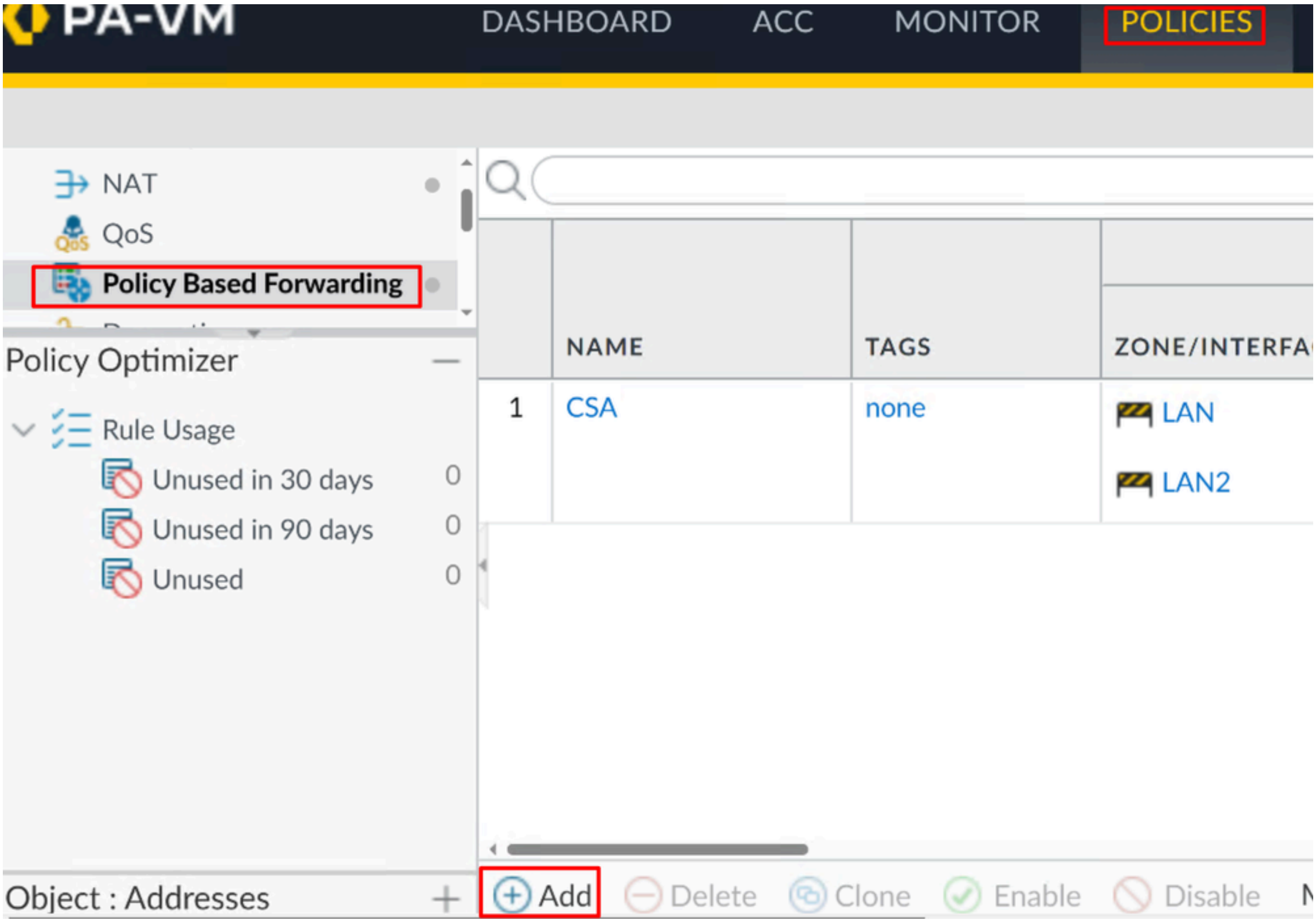
Comment:

Now your VPN is successfully created, you can proceed with the step, **Configure Policy Based Forwarding.**

Configure Policy Based Forwarding

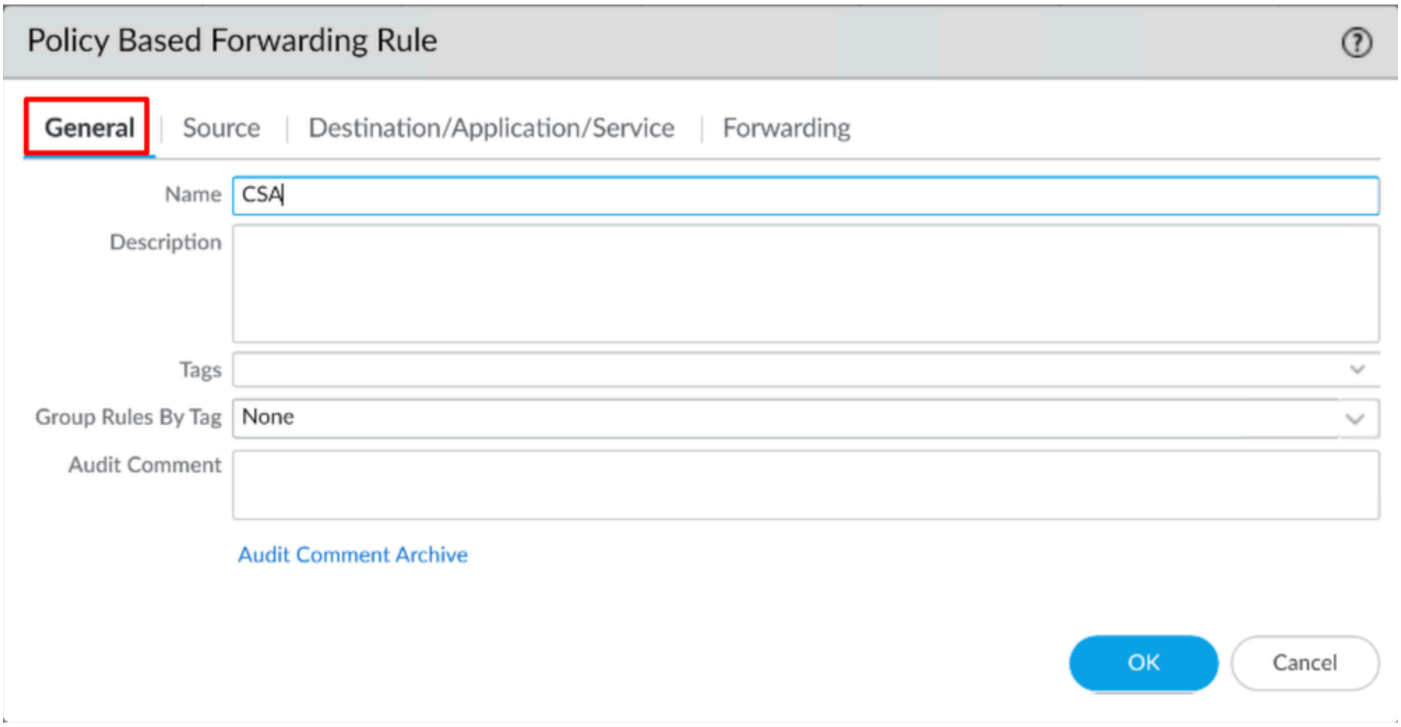
To configure **Policy Based Forwarding**, navigate to Policies > Policy Based Forwarding.

- Click Add



	NAME	TAGS	ZONE/INTERFA
1	CSA	none	LAN LAN2

- Configure the next parameters:
  - General
    - **Name**: Use a name to identify the Secure Access, Policy Base Forwarding (Routing by origin)
  - Source
    - **Zone**: Select the Zones from where you have plans to route the traffic based on the origin
    - **Source Address**: Configure the host or networks that you want to use as a source.
    - Source Users: Configure the users that you want to route the traffic (Only if applicable)
  - Destination/Application/Service
    - Destination Address: You can leave it as Any, or you can specify the ranges of addresses of Secure Access (100.64.0.0/10)
  - Forwarding
    - **Action**: Forward
    - **Egress Interface**: Choose the tunnel interface configured on the step, Configure the tunnel interface.
    - **Next Hop**: None
- ClickOK and Commit



Policy Based Forwarding Rule

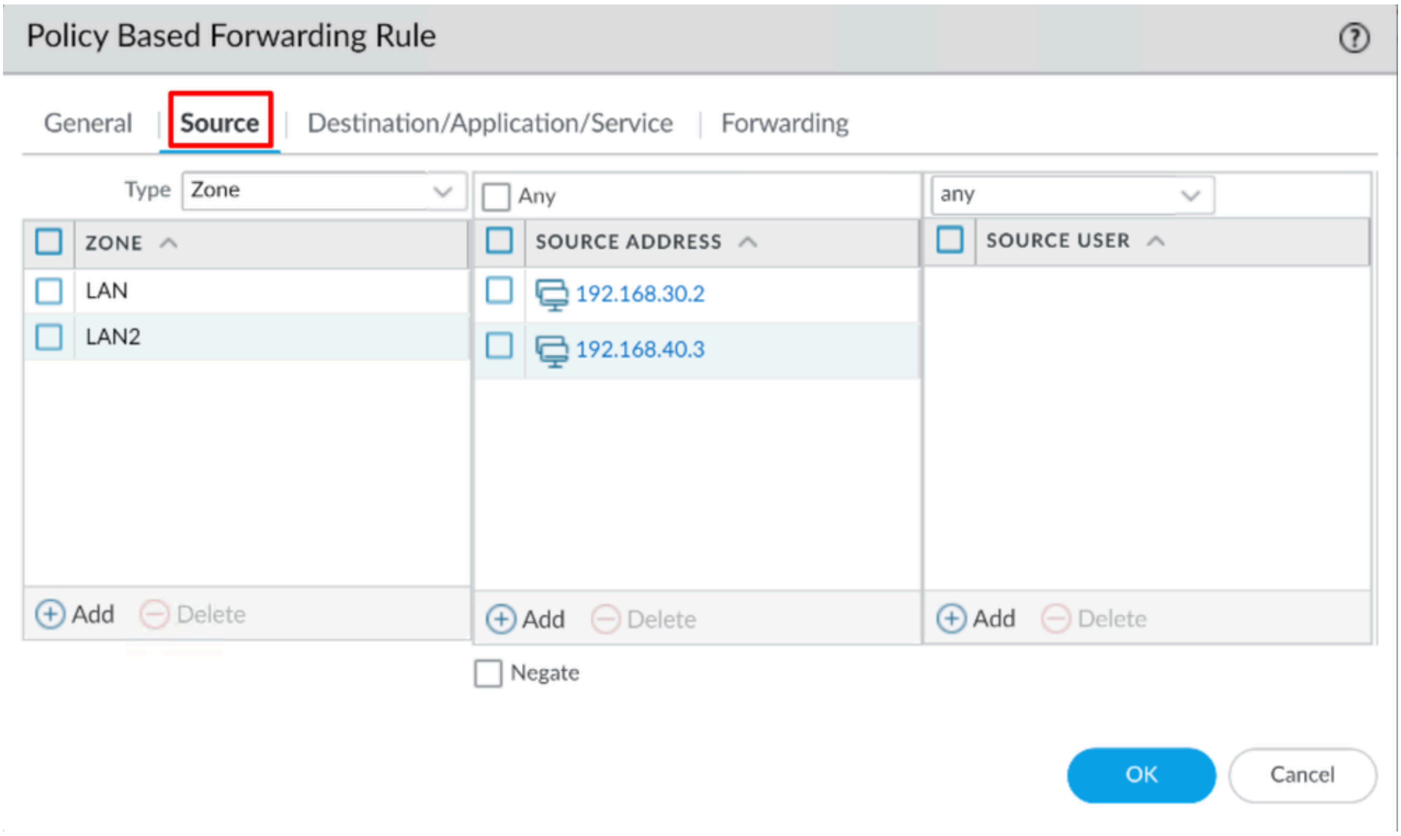
Name: CSA

Description:

Tags:

Group Rules By Tag: None

Audit Comment:



Policy Based Forwarding Rule

Type: Zone

□	ZONE
□	LAN
□	LAN2

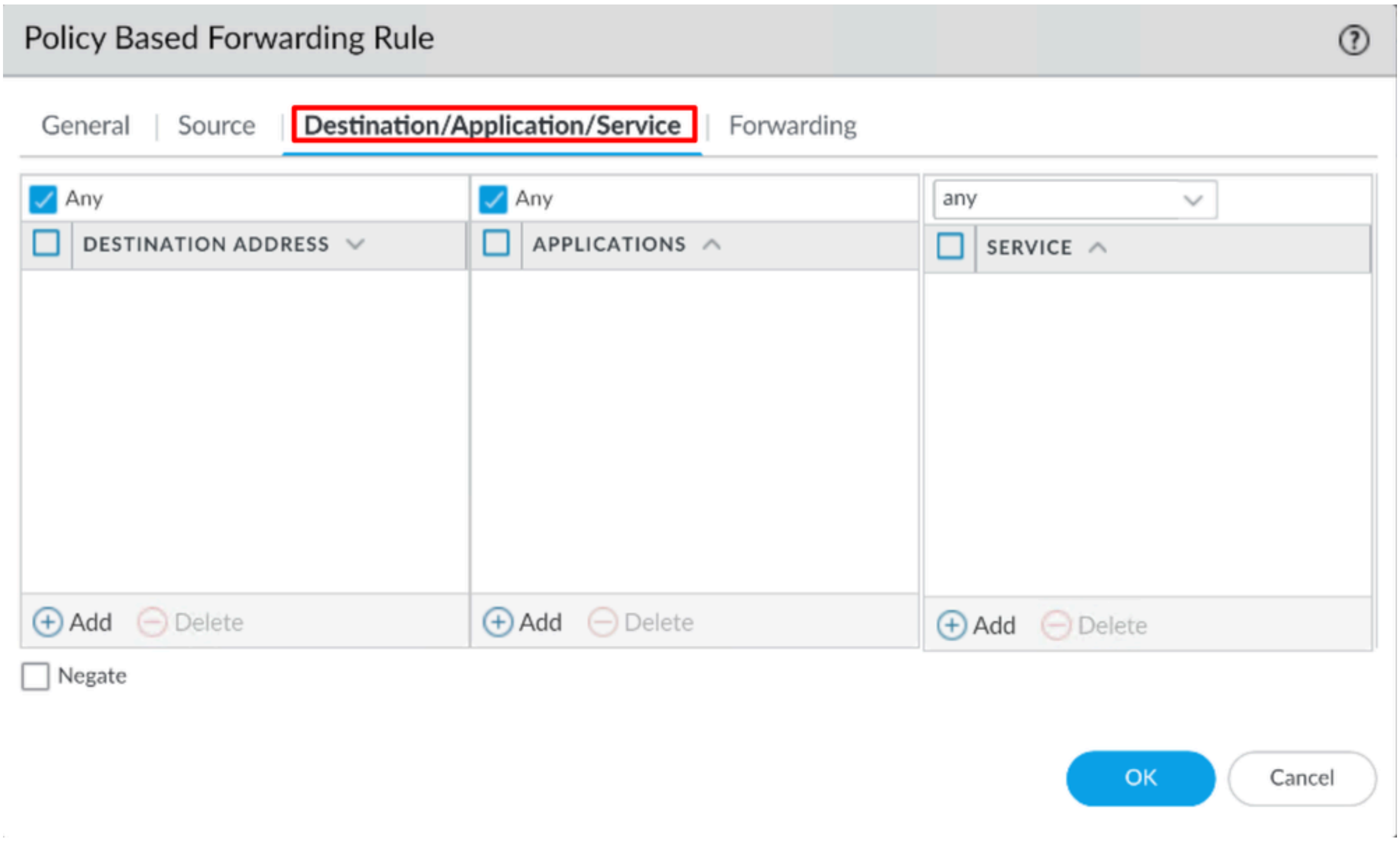
□ Any

□	SOURCE ADDRESS
□	192.168.30.2
□	192.168.40.3

any

□	SOURCE USER

□ Negate



Policy Based Forwarding Rule

General | Source | **Destination/Application/Service** | Forwarding

☑ Any

□ DESTINATION ADDRESS

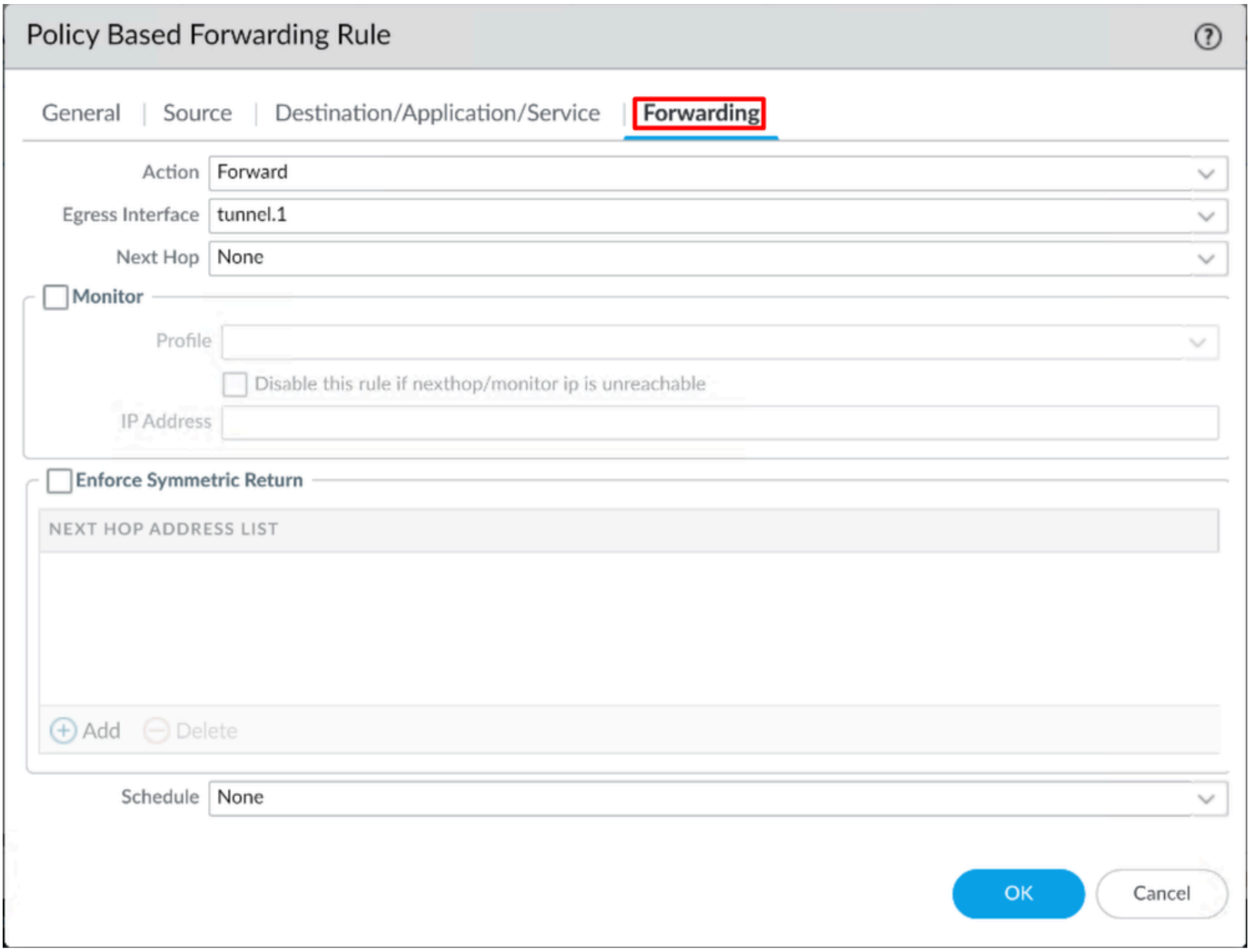
☑ Any

□ APPLICATIONS

any

□ SERVICE

□ Negate



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

Schedule: None

Now you have everything configured on Palo Alto; after you configure the route, the tunnel can be established, and you need to continue configuring the RA-VPN, Browser-Based ZTA, or Client Base ZTA on Secure Access Dashboard.