Windows VPN Client

Palo Alto 2.0.4 Configuration Guide

Latest update: 22 April 2022
Document reference number: 20220422_CG_Palo_Alto_EN_1.0

www.thegreenbow.com

All the information provided is subject to modifications at any time and without notice.

Despite our utmost care and attention in producing this document and its regular updates, errors may have been introduced in the information provided. If you notice any issues, please feel free to contact us and let us know. We will make the necessary changes.

Table of contents

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2022-04-22	All	Initial draft	AL, BB

1 Introduction

1.1 Purpose of document

This configuration guide describes how to configure version 6.8 of TheGreenBow Windows Enterprise VPN Client to establish VPN connections with version 2.0.4 of the Palo Alto firewall.

1.2 Software versions used

We used the following software versions to draft this document:

- Palo Alto version 2.0.4
- TheGreenBow Windows Enterprise VPN Client version 6.86.015

The instructions contained in this configuration guide should also work with newer versions of the Palo Alto firewall and TheGreenBow Windows Enterprise VPN Client.

2 Configuring the Palo Alto firewall

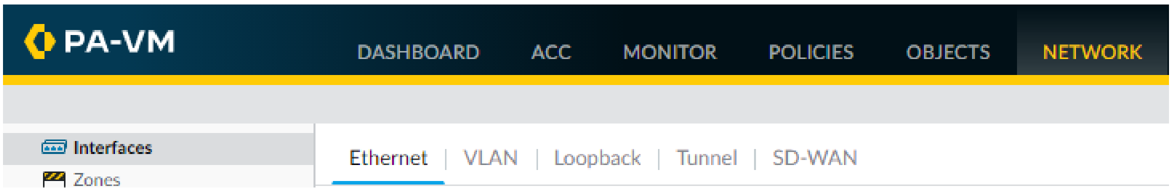
This section describes how to configure your Palo Alto firewall.

2.1 Configuring Network/Interfaces

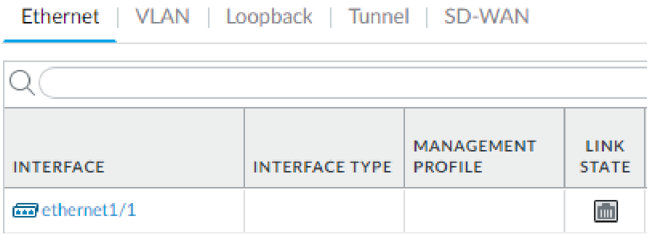
2.1.1 Configuring trusted physical interface (LAN)

Once you are connected, proceed as follows to configure trusted physical interfaces:

1. From the top menu, select **NETWORK**.



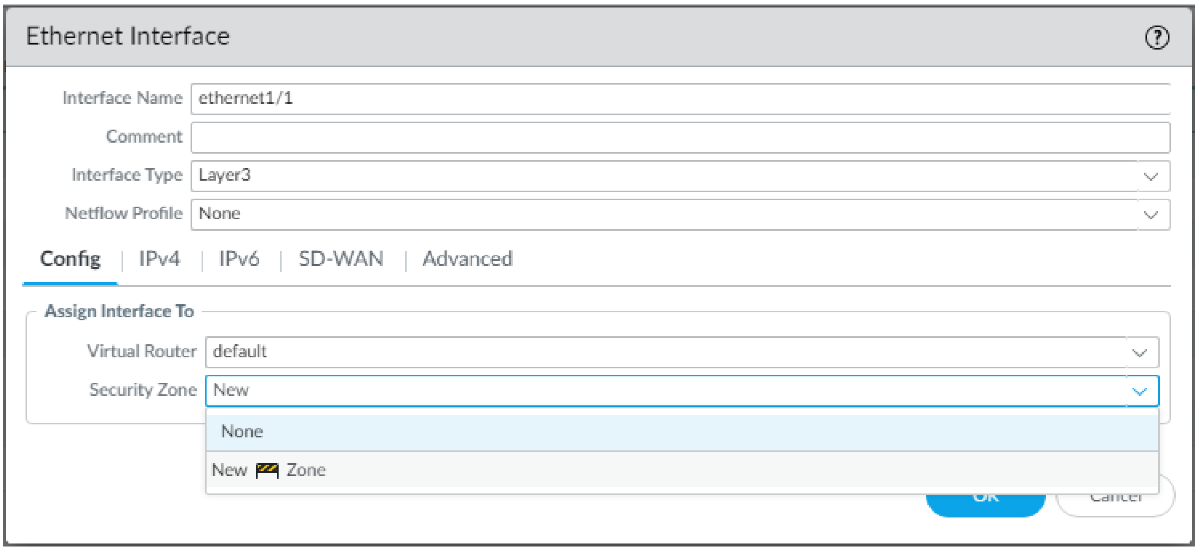
2. From the left menu, select **Interfaces**.
3. Then, click the **Ethernet** tab.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE
ethernet1/1			▦

4. On the **Ethernet** tab, click **ethernet1/1**.

The **Ethernet Interface** window is displayed:



Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

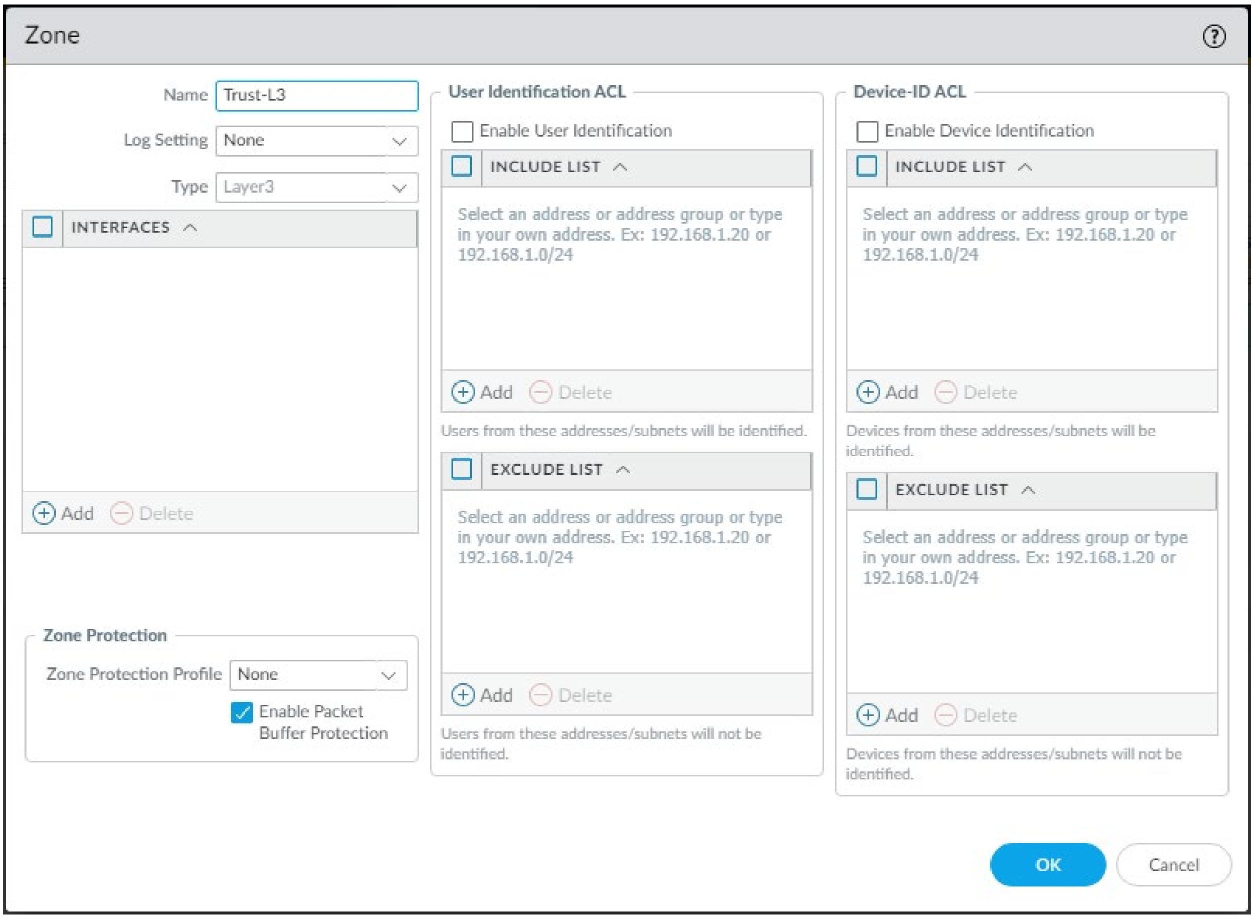
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: New

5. In the **Interface Type** drop-down list, select **Layer3**.
6. In the **Virtual Router** drop-down list, select **Default**.
7. In the **Security Zone** drop-down list, select **New Zone**. The **Zone** window is displayed:



Zone

Name: Trust-L3

Log Setting: None

Type: Layer3

□ INTERFACES

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identification ACL

□ Enable User Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Device-ID ACL

□ Enable Device Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

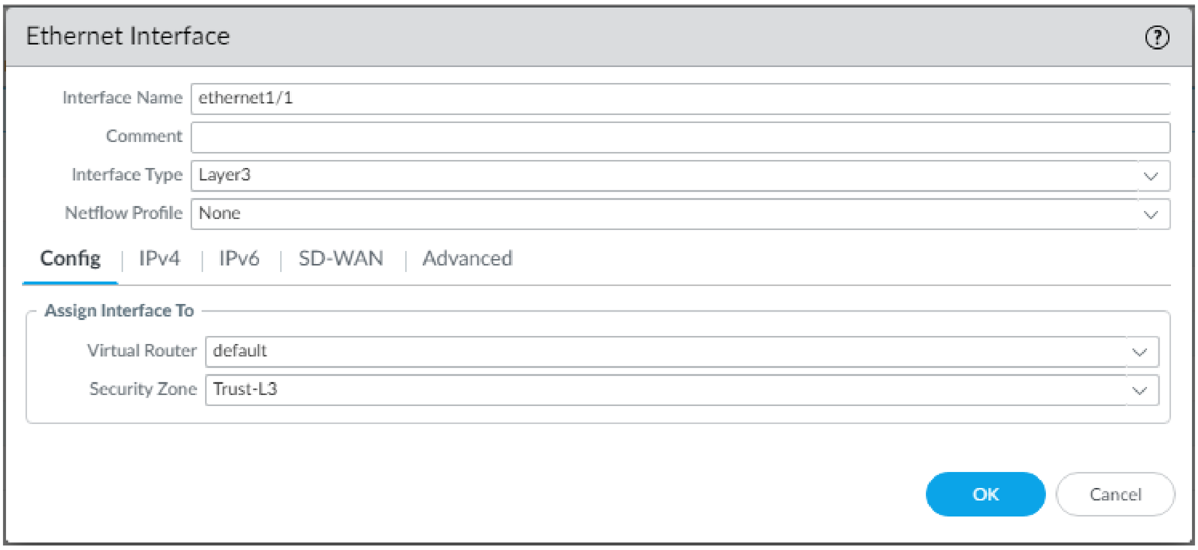
Devices from these addresses/subnets will be identified.

□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will not be identified.

8. In the **Name** field, enter `Trust-L3`, and then click **OK**. The **Security Zone** drop-down list is filled in automatically.



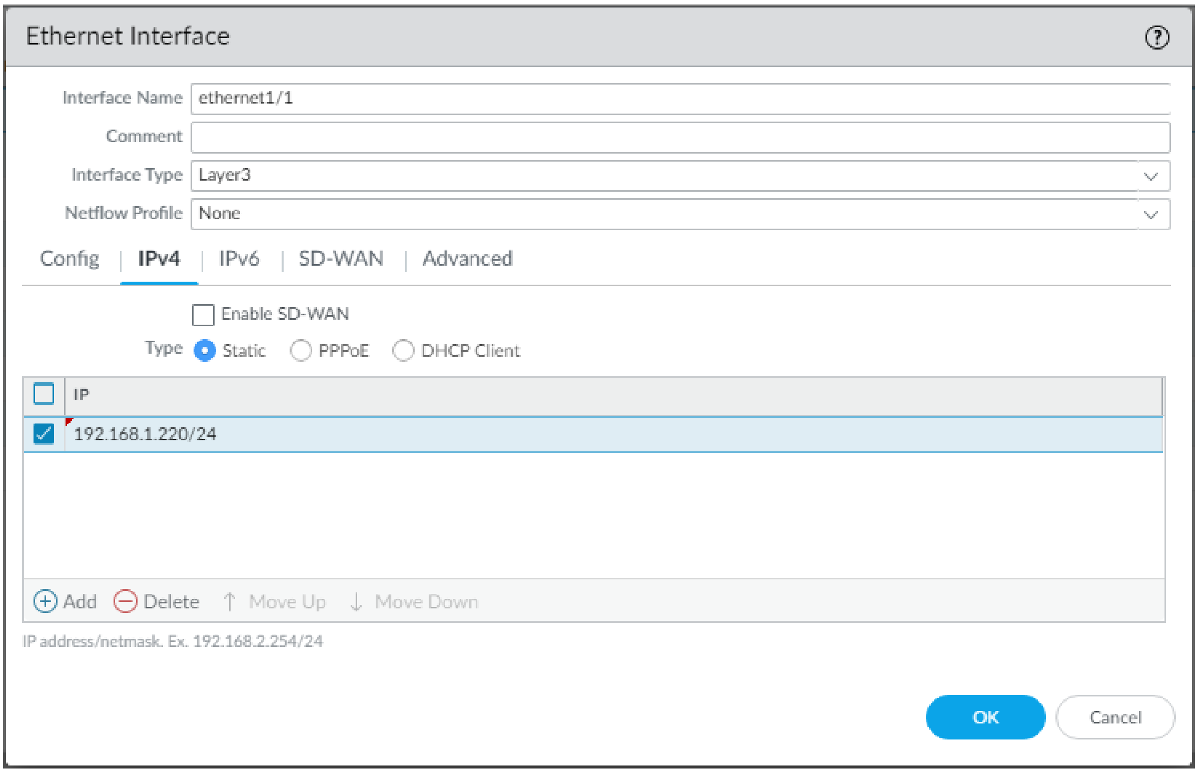
Ethernet Interface

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None

Assign Interface To

Virtual Router	default
Security Zone	Trust-L3

9. Click the **IPv4** tab, then click **Add** and enter the value `192.168.1.220/24`.



Ethernet Interface

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None

□ Enable SD-WAN

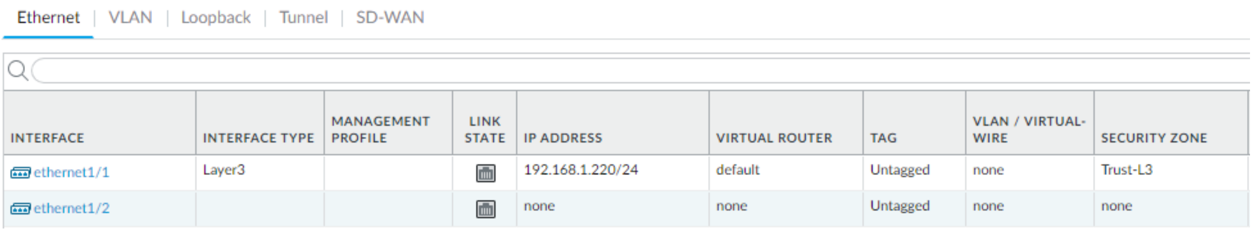
Type ● Static ○ PPPoE ○ DHCP Client

□	IP
☑	192.168.1.220/24

IP address/netmask. Ex. 192.168.2.254/24

10. Click **OK**.

You should now see the trusted interface properly configured as follows:



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3			192.168.1.220/24	default	Untagged	none	Trust-L3
ethernet1/2				none	none	Untagged	none	none

Security Zone can be found under **NETWORK** > **Zones**.

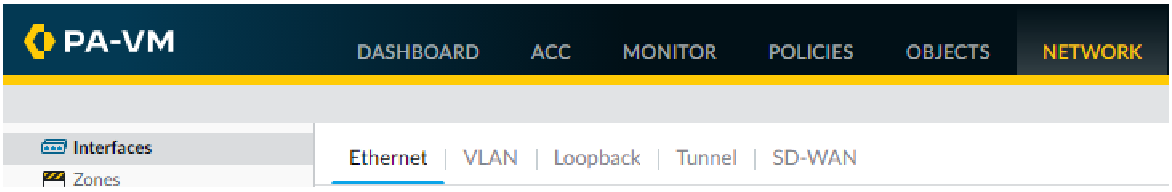
Repeat the above steps as many times as necessary to configure additional trusted physical interfaces.

You have successfully configured trusted physical interfaces. Proceed with configuring untrusted physical interfaces, as described in the next section.

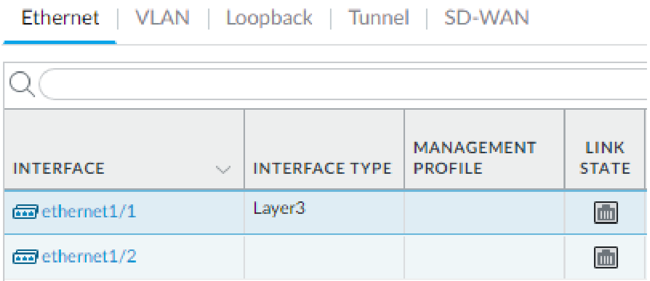
2.1.2 Configuring untrusted physical interfaces (WAN)

Proceed as follows to configure untrusted physical interfaces:

1. From the top menu, select **NETWORK**.



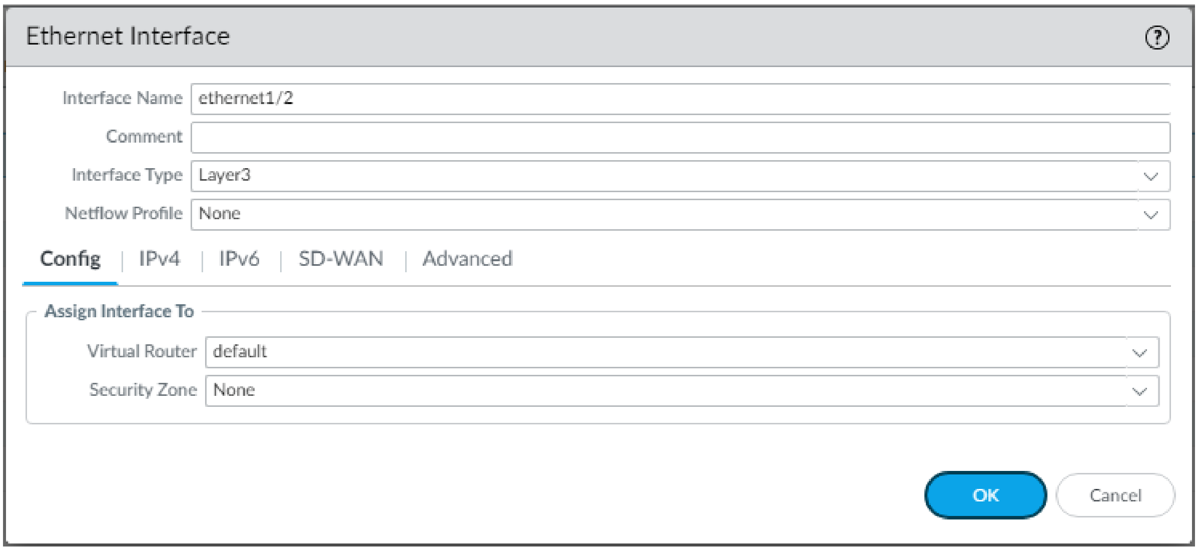
2. From the left menu, select **Interfaces**.
3. Then, click the **Ethernet** tab.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE
ethernet1/1	Layer3		
ethernet1/2			

4. Click **ethernet1/2**.

The **Ethernet Interface** window is displayed:



Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

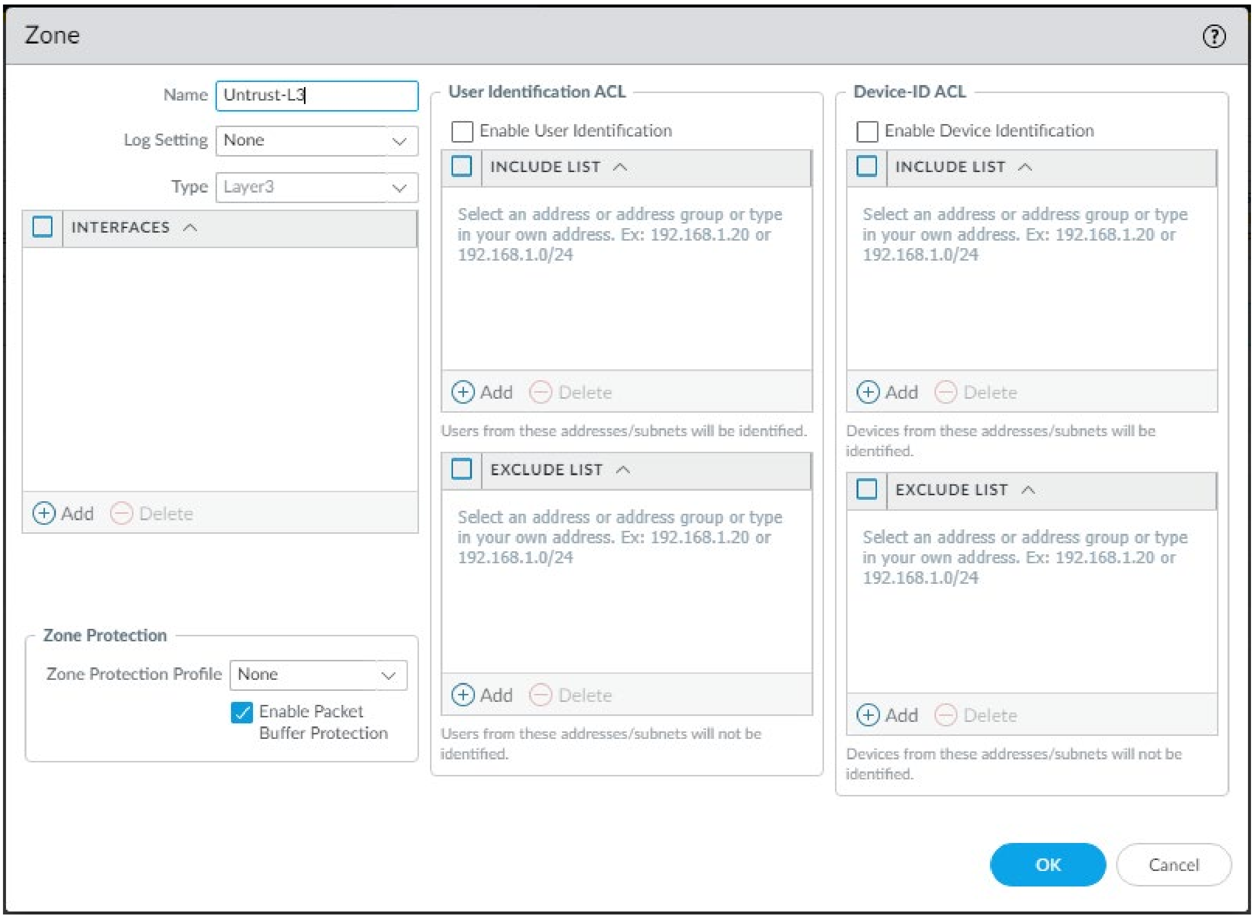
Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: None

5. In the **Interface Type** drop-down list, select **Layer3**.
6. In the **Virtual Router** drop-down list, select **Default**.
7. In the **Security Zone** drop-down list, select **New Zone**. The **Zone** window is displayed:



Zone

Name: Untrust-L3

Log Setting: None

Type: Layer3

□ INTERFACES

⊕ Add ⊖ Delete

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identification ACL

□ Enable User Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

⊕ Add ⊖ Delete

Users from these addresses/subnets will be identified.

□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

⊕ Add ⊖ Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

□ Enable Device Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

⊕ Add ⊖ Delete

Devices from these addresses/subnets will be identified.

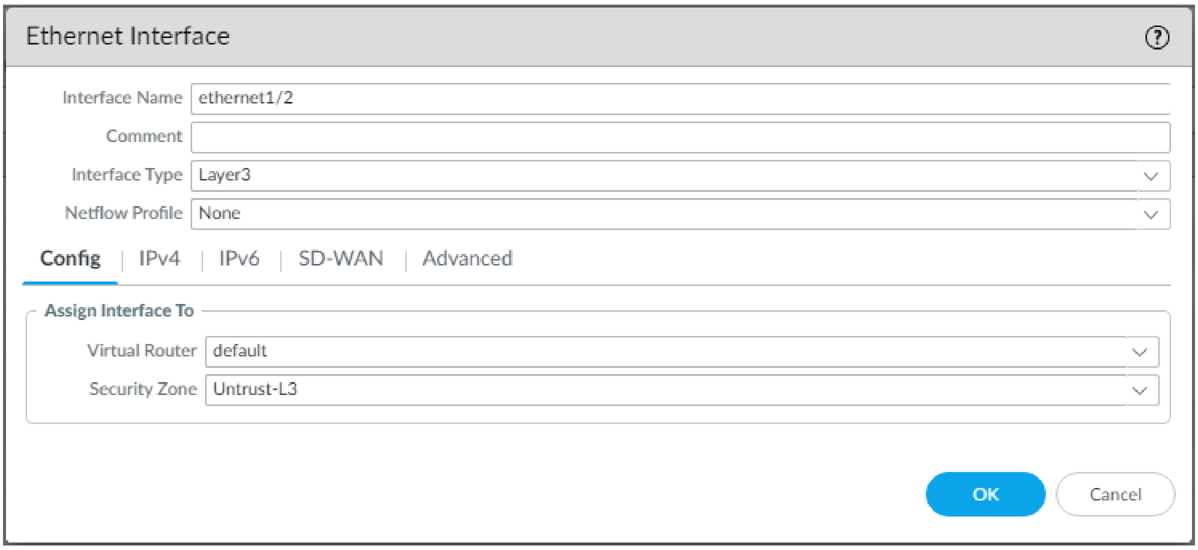
□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

⊕ Add ⊖ Delete

Devices from these addresses/subnets will not be identified.

8. In the **Name** field, enter `Untrust-L3`, and then click **OK**. The **Security Zone** drop-down list is filled in automatically.



Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

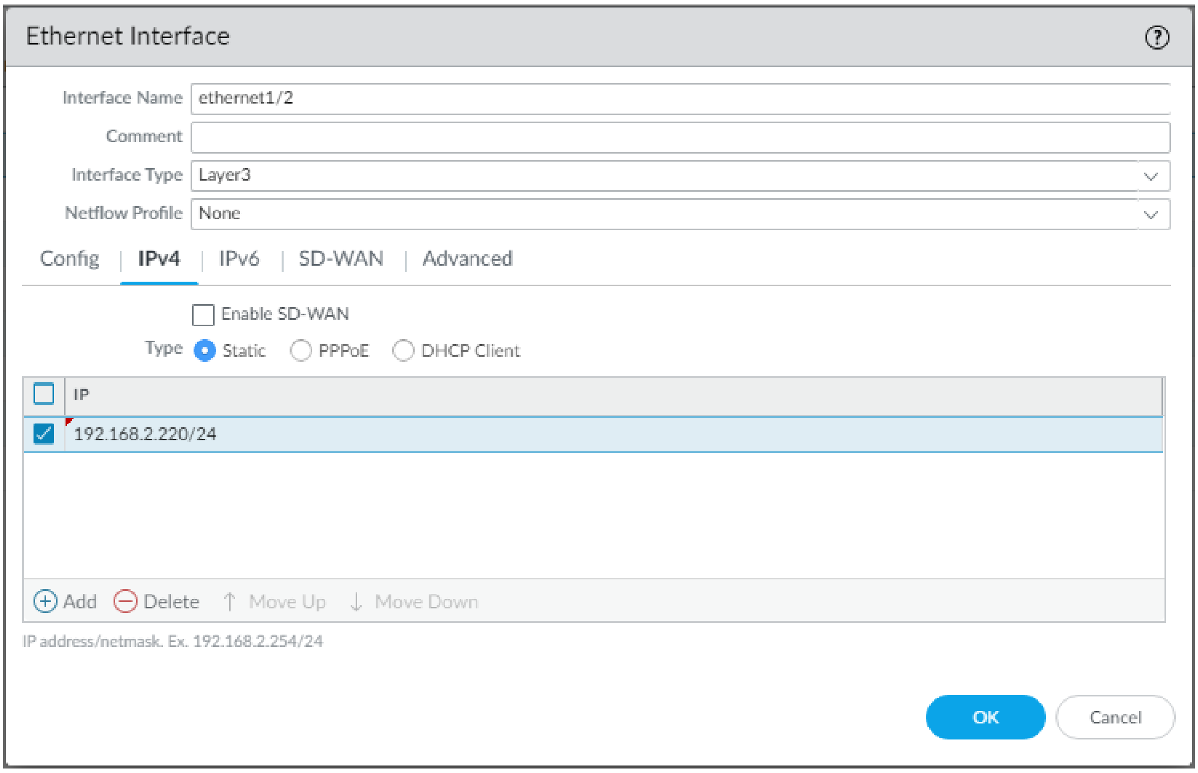
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: Untrust-L3

9. Click the **IPv4** tab, then click **Add** and enter the value `192.168.2.220/24`.



Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

□ Enable SD-WAN

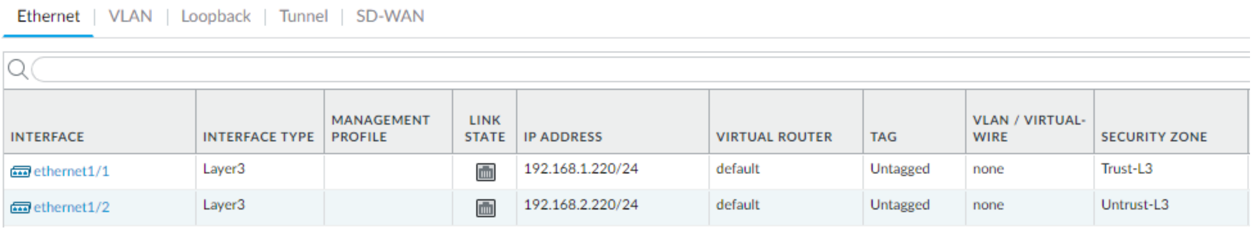
Type ● Static ○ PPPoE ○ DHCP Client

□	IP
☑	192.168.2.220/24

IP address/netmask. Ex. 192.168.2.254/24

10. Click **OK**.

You should now see the untrusted interface properly configured as follows:



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3		▦	192.168.1.220/24	default	Untagged	none	Trust-L3
ethernet1/2	Layer3		▦	192.168.2.220/24	default	Untagged	none	Untrust-L3

Security Zone can be found under **NETWORK** > **Zones**.

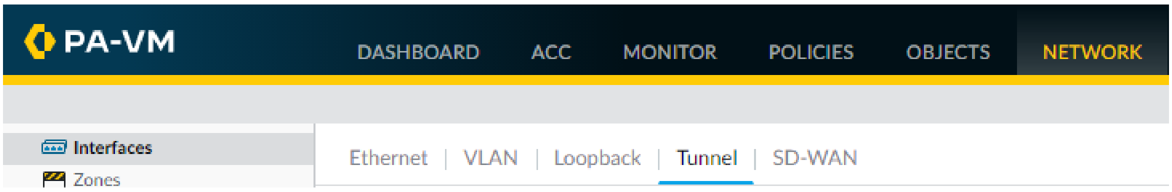
Repeat the above steps as many times as necessary to configure additional untrusted physical interfaces.

You have successfully configured untrusted physical interfaces. Proceed with configuring the virtual interface for the VPN tunnel, as described in the next section.

2.1.3 Configuring the virtual interface for the VPN tunnel

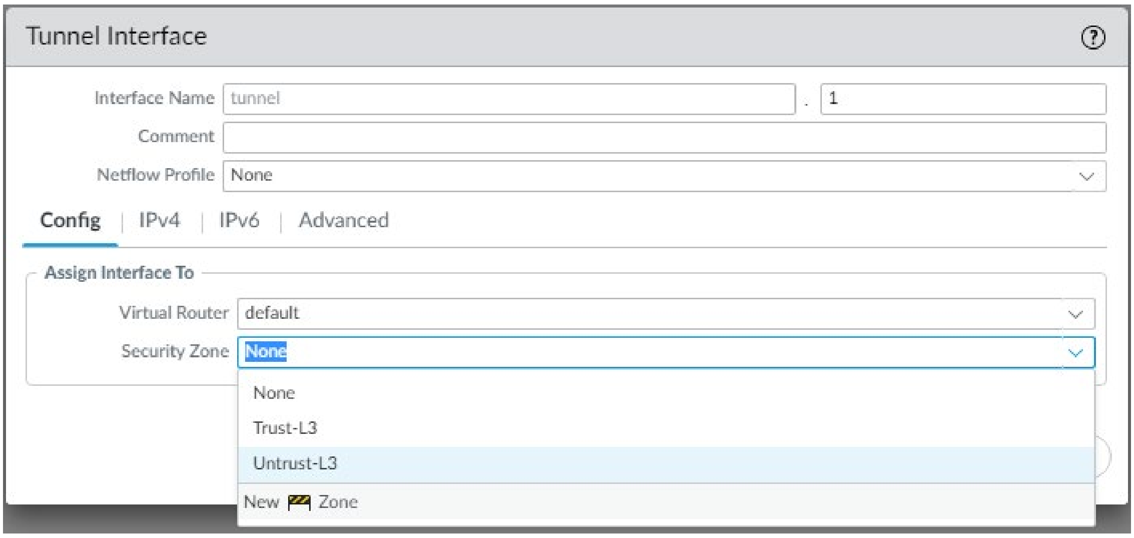
To configure the virtual interface for the VPN tunnel proceed as follows:

1. From the top menu, select **NETWORK**.



2. From the left menu, select **Interfaces**.
3. Then, click the **Tunnel** tab.
4. Click **Add**.

The **Tunnel Interface** window is displayed:



Tunnel Interface

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

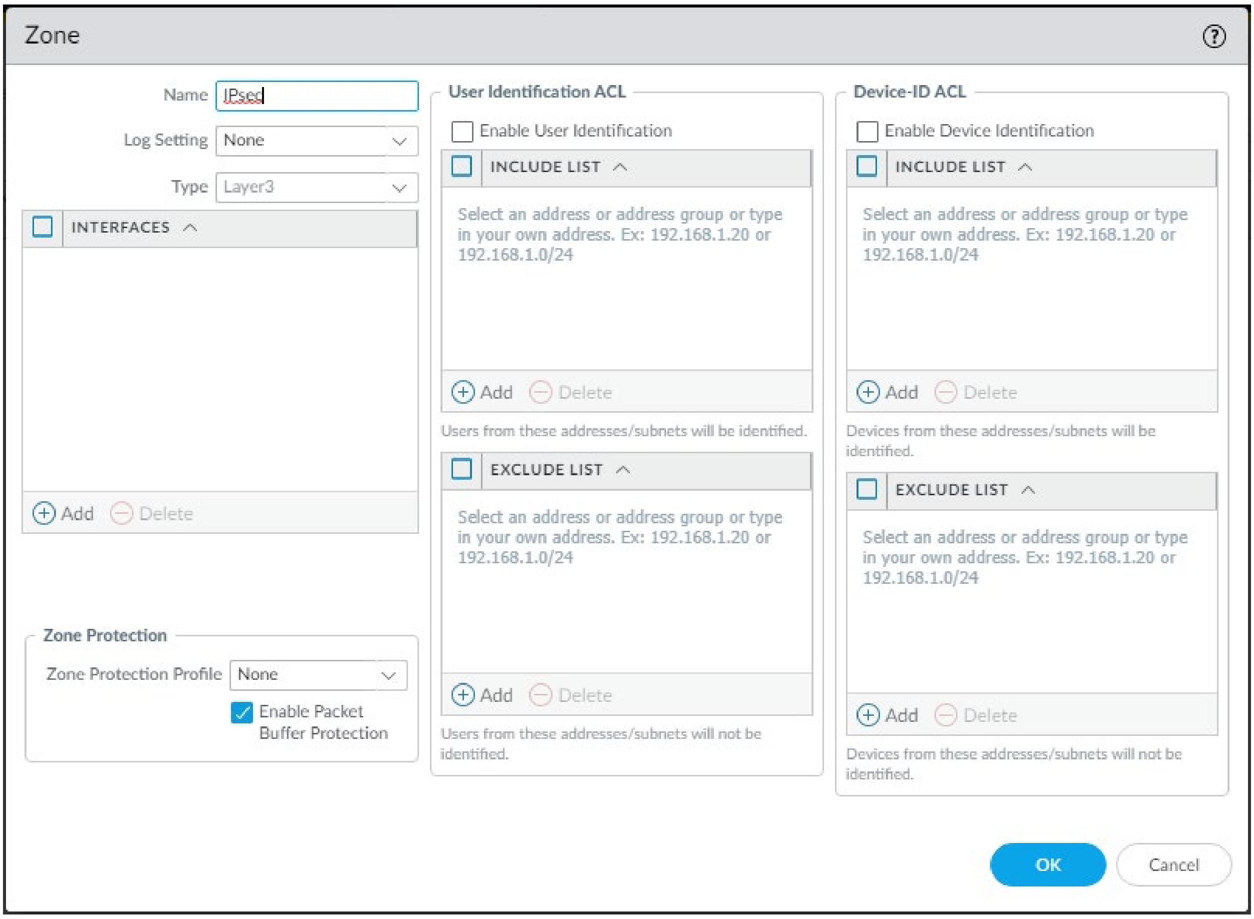
Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: None

5. In the **Interface Name** field, enter the value `1`.
6. In the **Virtual Router** drop-down list, select **Default**.
7. In the **Security Zone** drop-down list, select **New Zone**. The **Zone** window is displayed:



Zone

Name: IPsec

Log Setting: None

Type: Layer3

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identification ACL

□ Enable User Identification

INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete

Users from these addresses/subnets will be identified.

EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

□ Enable Device Identification

INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete

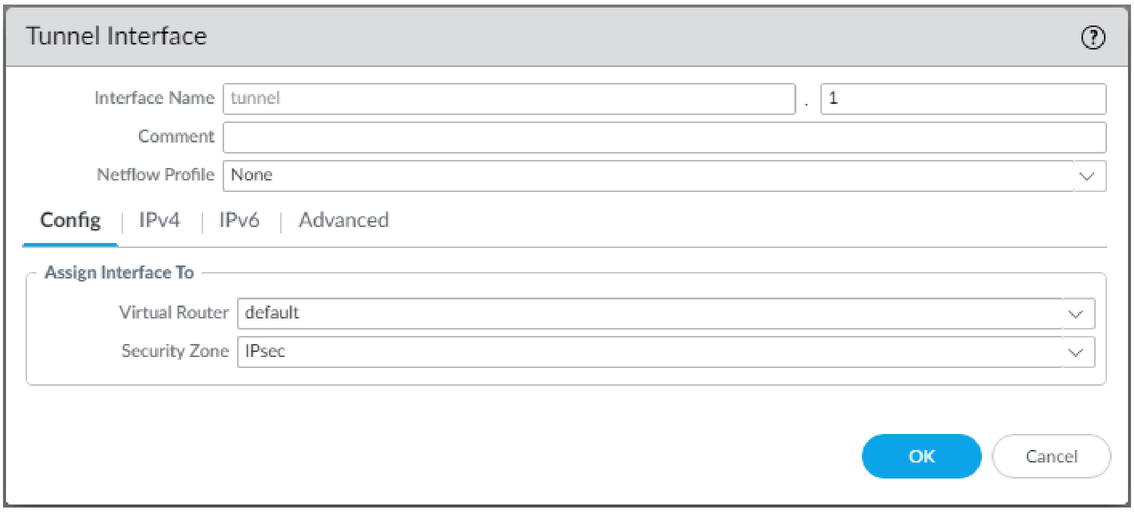
Devices from these addresses/subnets will be identified.

EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete

Devices from these addresses/subnets will not be identified.

8. In the **Name** field, enter `IPsec`, and then click **OK**.

The **Security Zone** drop-down list is filled in automatically.



Tunnel Interface

Interface Name: tunnel . 1

Comment:

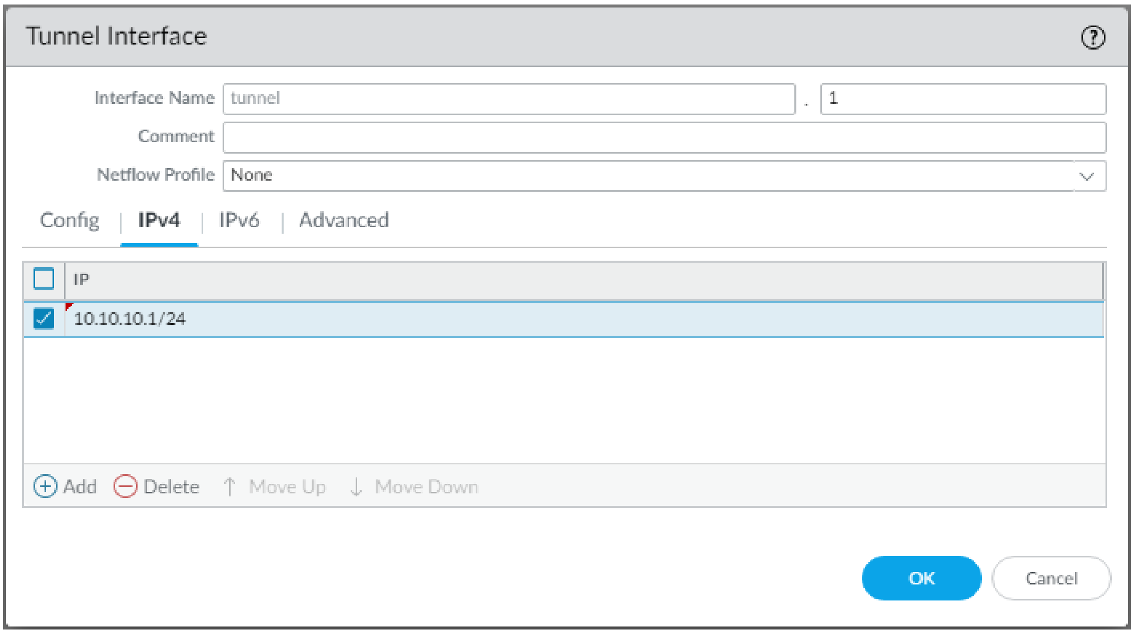
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: IPsec

9. Click the **IPv4** tab, then click **Add** and enter the value `10.10.10.1/24`.



Tunnel Interface

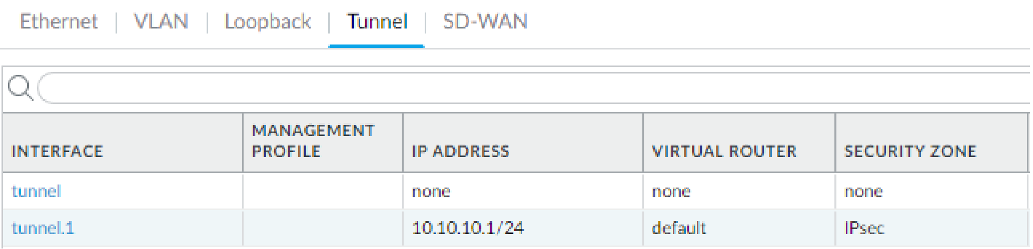
Interface Name: tunnel . 1

Comment:

Netflow Profile: None

□	IP
☑	10.10.10.1/24

10. Click **OK**. You should now see the trusted interface properly configured as follows:

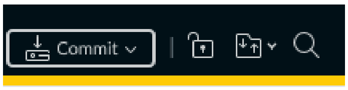


INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE
tunnel		none	none	none
tunnel.1		10.10.10.1/24	default	IPsec

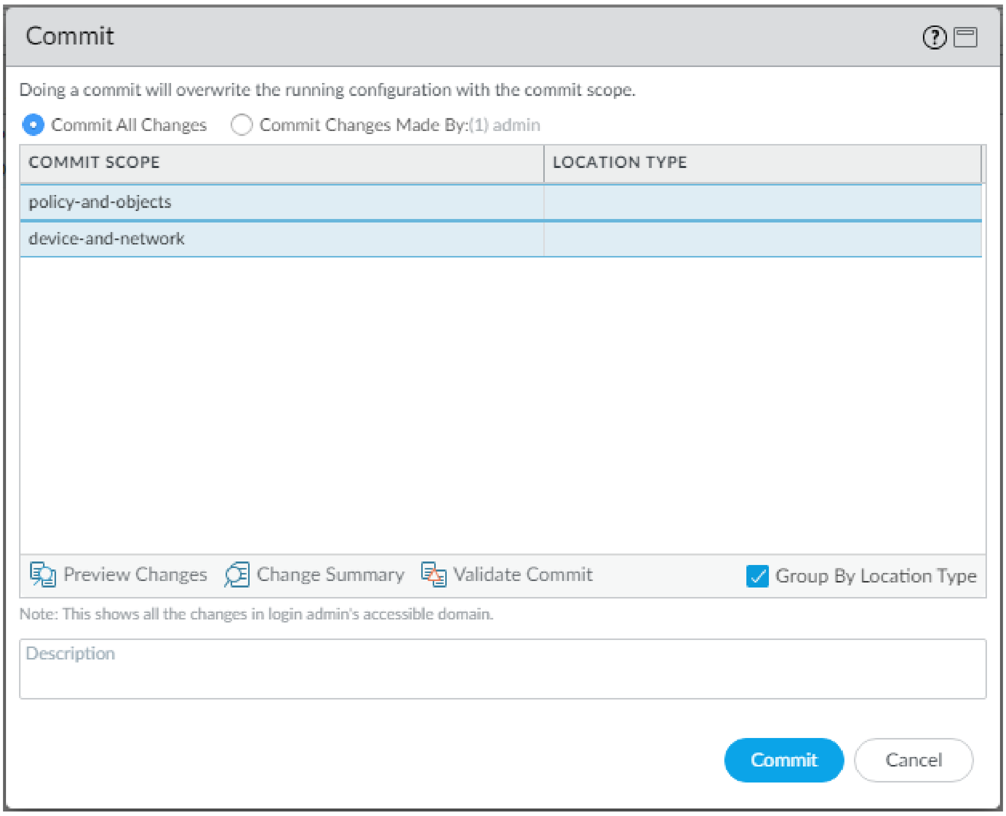
This IP address will be used as the virtual IP on TheGreenBow VPN Client in traffic selector.

Security Zone can be found under **NETWORK** > **Zones**.

11. Click **Commit** at the top right to apply the configuration.



The **Commit** window is displayed:



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

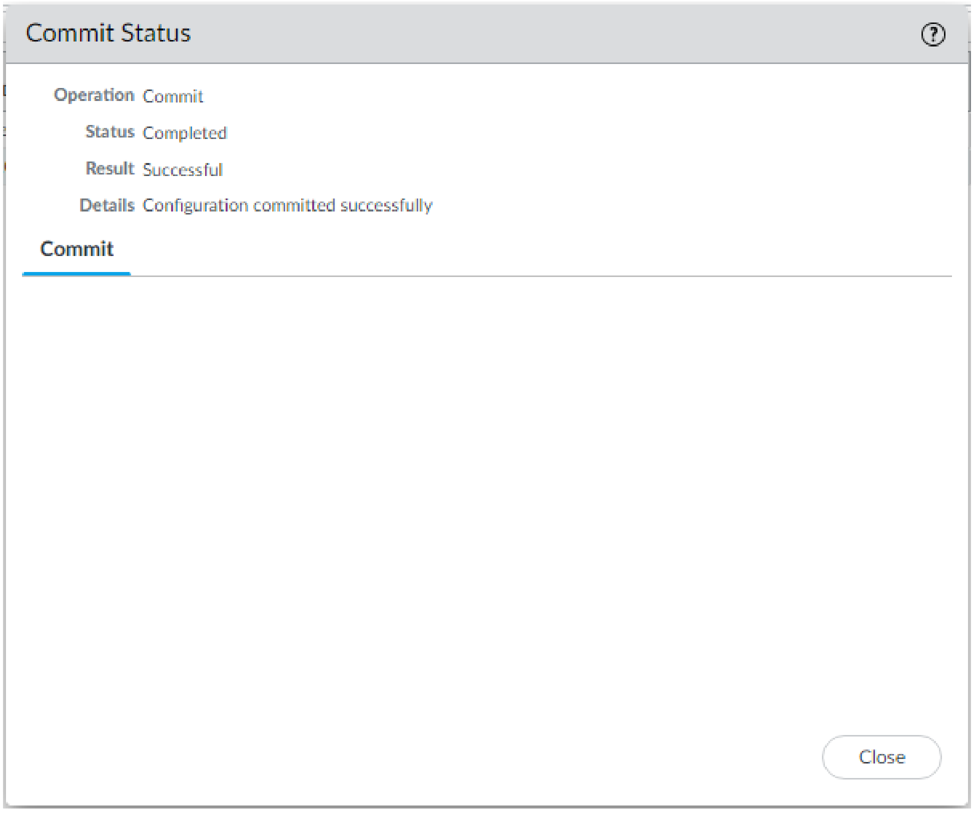
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
device-and-network	

Note: This shows all the changes in login admin's accessible domain.

Description

12. Click **Commit** to apply the changes.

The **Commit Status** window is displayed:



Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

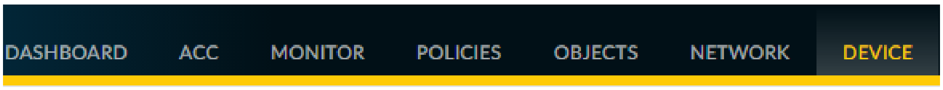
13. Click **Close**.

You have successfully configured the virtual interface for the VPN tunnel. Proceed with creating certificates, as described in the next section.

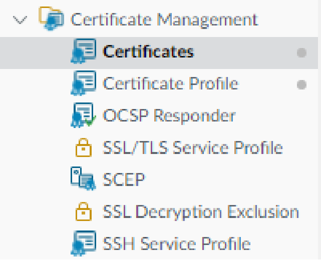
2.2 Creating certificates

To create the required certificates, follow the steps below:

1. From the top menu, select **DEVICE**.



2. Then, choose **Certificate Management** > **Certificates**.

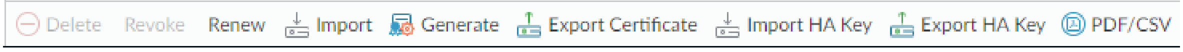


3. Follow the instructions below to create a set consisting of a Root Authority (CA), a User Identity, and a Server Identity.

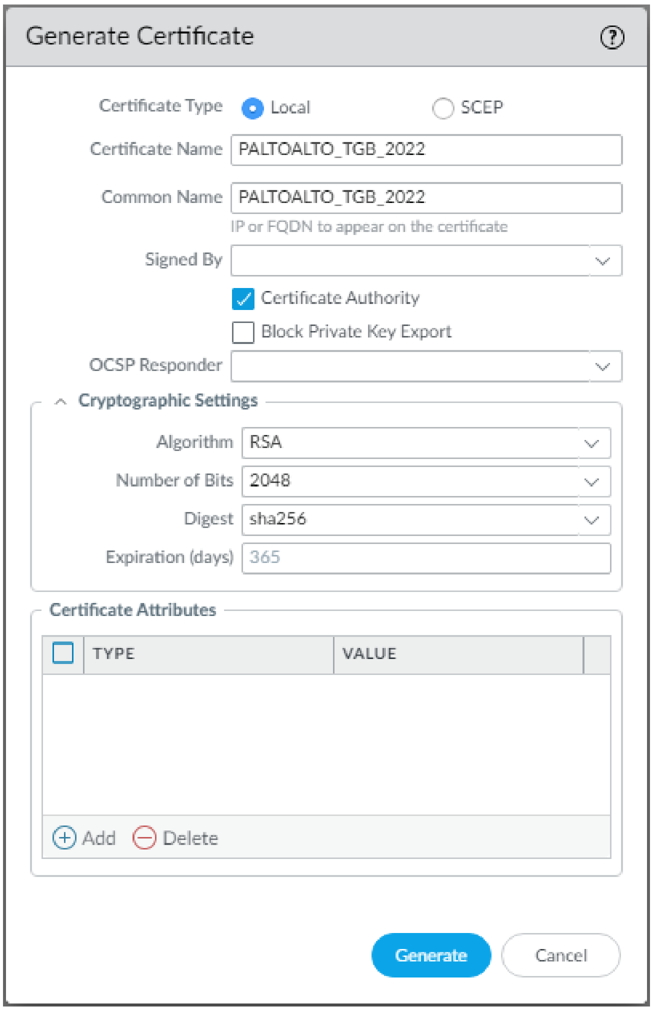
2.2.1 Creating a Root Authority

To create a Root Authority, proceed as follows:

1. Click **Generate** in the lower menu bar.



The **Generate Certificate** window is displayed:



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name PALTOALTO_TGB_2022

Common Name PALTOALTO_TGB_2022

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

□ Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm RSA

Number of Bits 2048

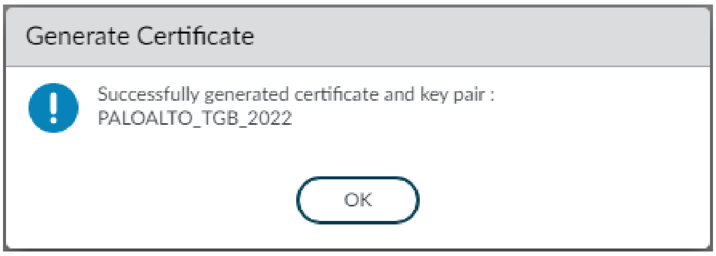
Digest sha256

Expiration (days) 365

Certificate Attributes

□	TYPE	VALUE

2. In the **Certificate Name** and **Common Name** fields, enter the value `PALOALTO_TGB_2022`.
3. Check the **Certificate Authority** box.
4. Click **Generate**. A confirmation prompt is displayed:

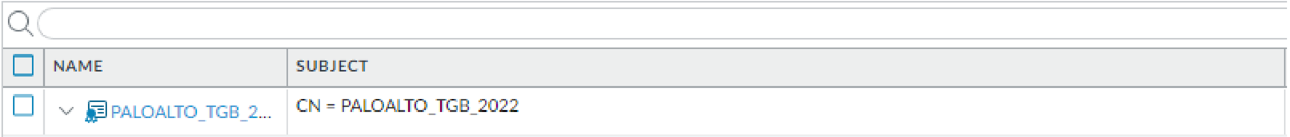


Generate Certificate

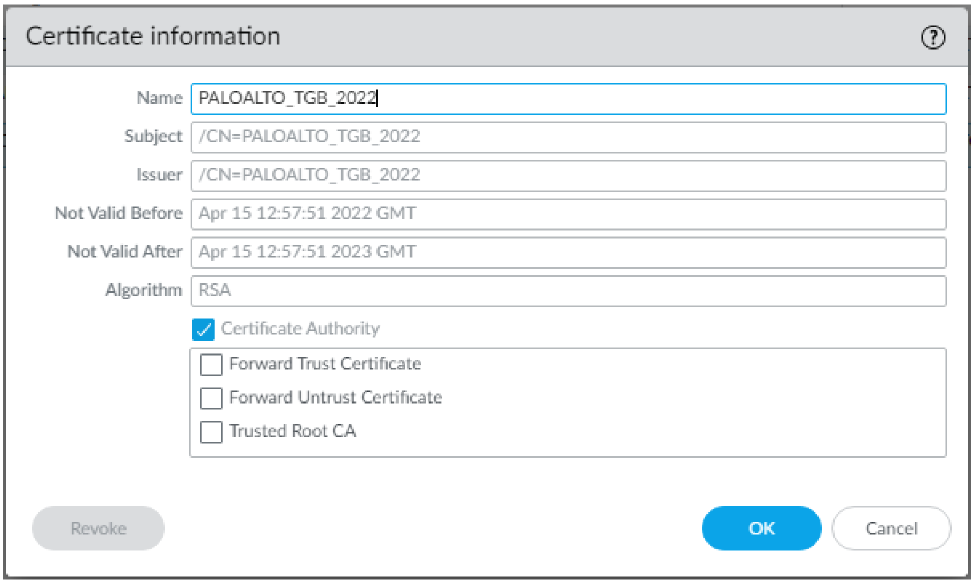
Successfully generated certificate and key pair :
PALOALTO_TGB_2022

5. Click **OK**.

   The summary should appear as follows:



□	NAME	SUBJECT
□	PALOALTO_TGB_2...	CN = PALOALTO_TGB_2022



Certificate information

Name	PALOALTO_TGB_2022
Subject	/CN=PALOALTO_TGB_2022
Issuer	/CN=PALOALTO_TGB_2022
Not Valid Before	Apr 15 12:57:51 2022 GMT
Not Valid After	Apr 15 12:57:51 2023 GMT
Algorithm	RSA

☑ Certificate Authority

□ Forward Trust Certificate

□ Forward Untrust Certificate

□ Trusted Root CA

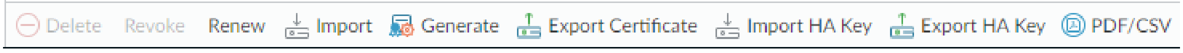
6. Click **OK**.

You have successfully created a Root Authority. Proceed with creating a User Identity, as described in the next section.

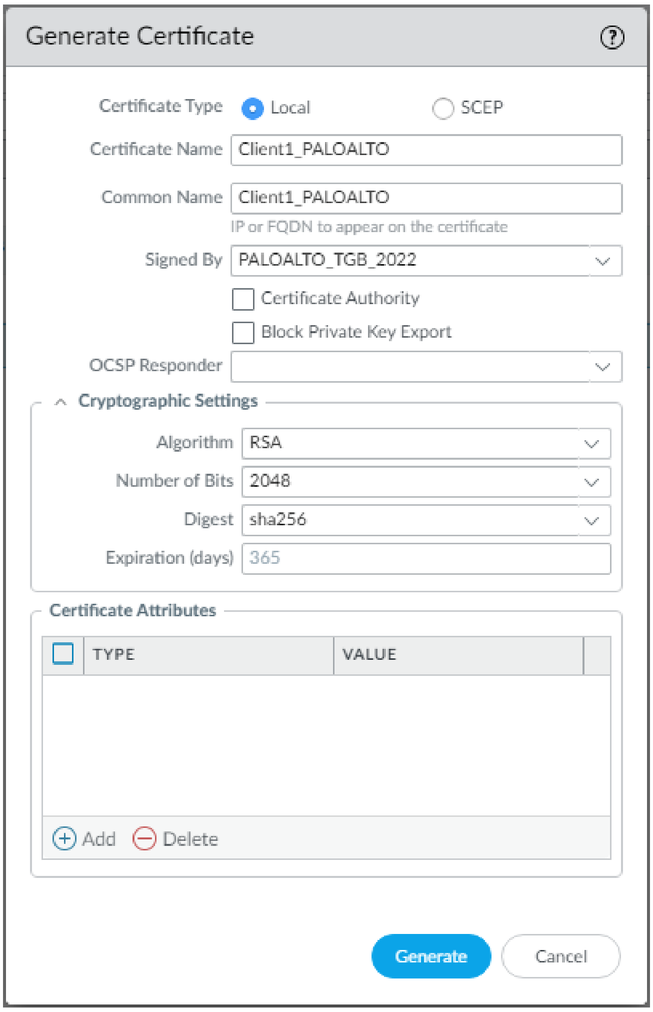
2.2.2 Creating a User Identity

To create a User Identity, proceed as follows:

1. Click **Generate** in the lower menu bar.



The **Generate Certificate** window is displayed:



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name Client1_PALOALTO

Common Name Client1_PALOALTO

IP or FQDN to appear on the certificate

Signed By PALOALTO_TGB_2022

□ Certificate Authority

□ Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm RSA

Number of Bits 2048

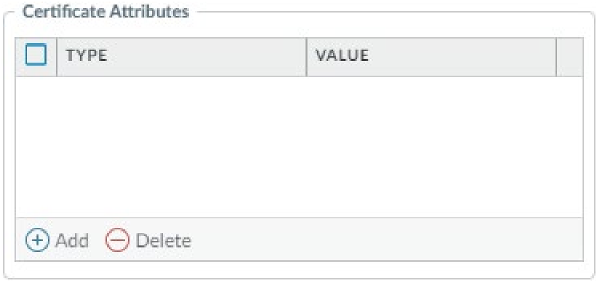
Digest sha256

Expiration (days) 365

Certificate Attributes

□	TYPE	VALUE

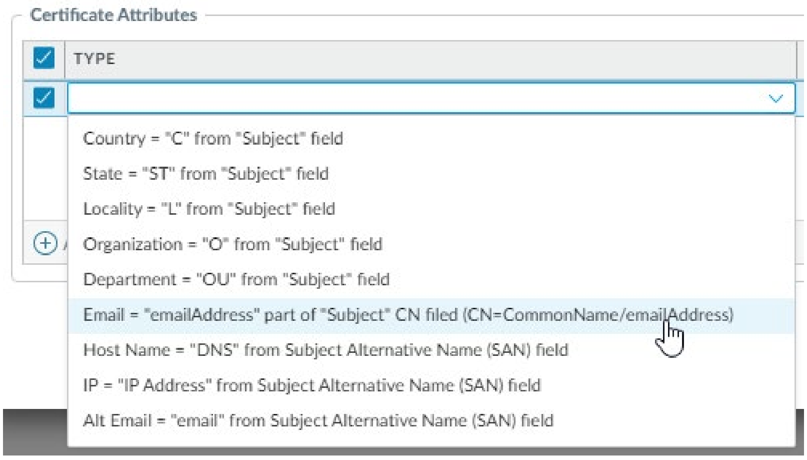
2. In the **Certificate Name** and **Common Name** fields, enter the value `Client1_PALOALTO`.
3. In the **Signed By** drop-down list, select the value **PALOALTO_TGB_2022**.
4. In the **Certificate Attributes** box, click **Add**.



Certificate Attributes

□	TYPE	VALUE

5. Select **TYPE** and choose the value **Email**.



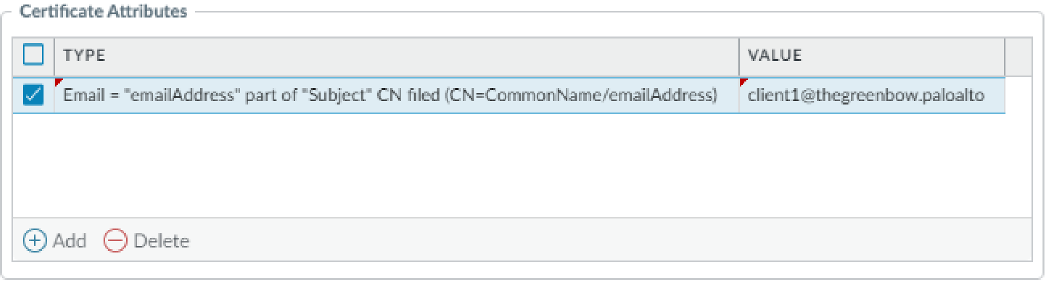
Certificate Attributes

☑ TYPE

☑

- Country = "C" from "Subject" field
- State = "ST" from "Subject" field
- Locality = "L" from "Subject" field
- Organization = "O" from "Subject" field
- Department = "OU" from "Subject" field
- Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailAddress)
- Host Name = "DNS" from Subject Alternative Name (SAN) field
- IP = "IP Address" from Subject Alternative Name (SAN) field
- Alt Email = "email" from Subject Alternative Name (SAN) field

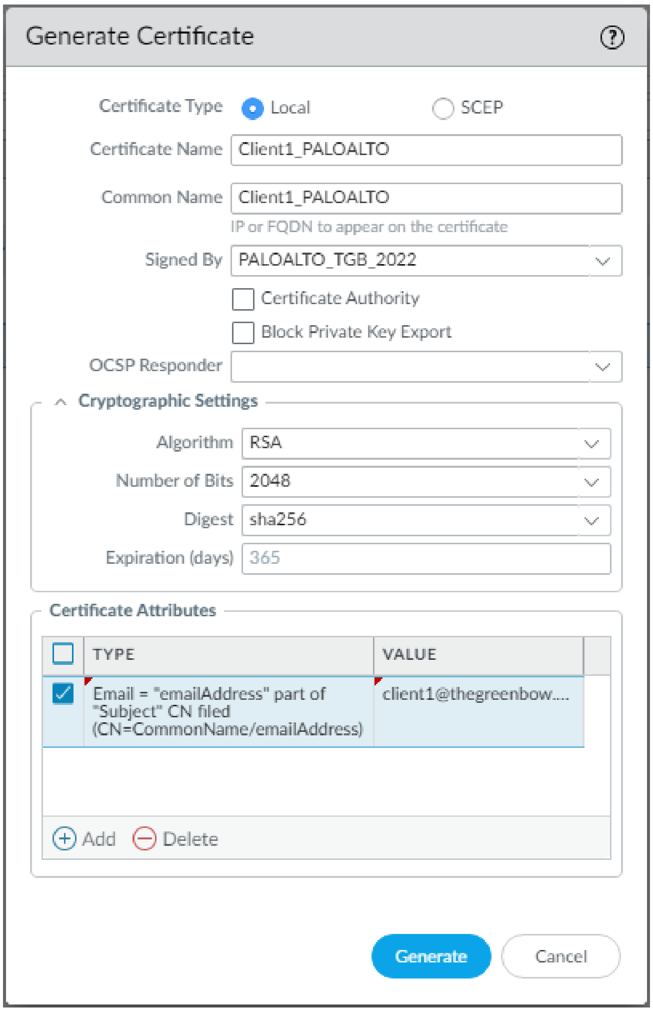
6. Define the relevant value for email from the VPN Client: `client1@thegreenbow.paloalto`.



Certificate Attributes

□	TYPE	VALUE
☑	Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailAddress)	client1@thegreenbow.paloalto

The summary should appear as follows:



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: Client1_PALOALTO

Common Name: Client1_PALOALTO

IP or FQDN to appear on the certificate

Signed By: PALOALTO_TGB_2022

□ Certificate Authority

□ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

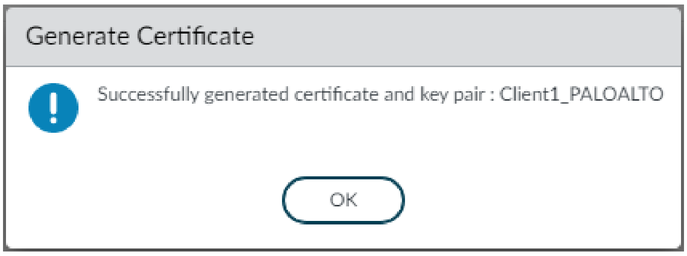
Digest: sha256

Expiration (days): 365

Certificate Attributes

□	TYPE	VALUE
☑	Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailAddress)	client1@thegreenbow....

7. Click **Generate**. A confirmation prompt is displayed:

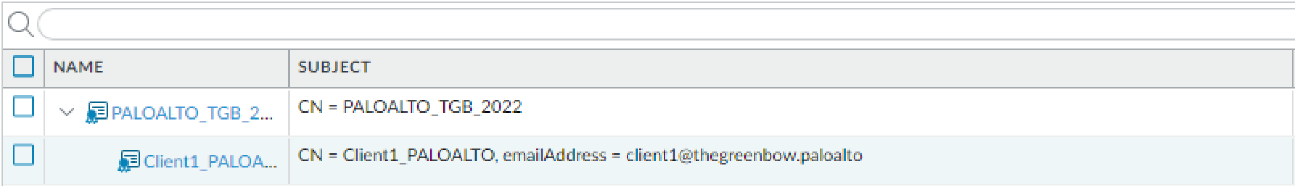


Generate Certificate

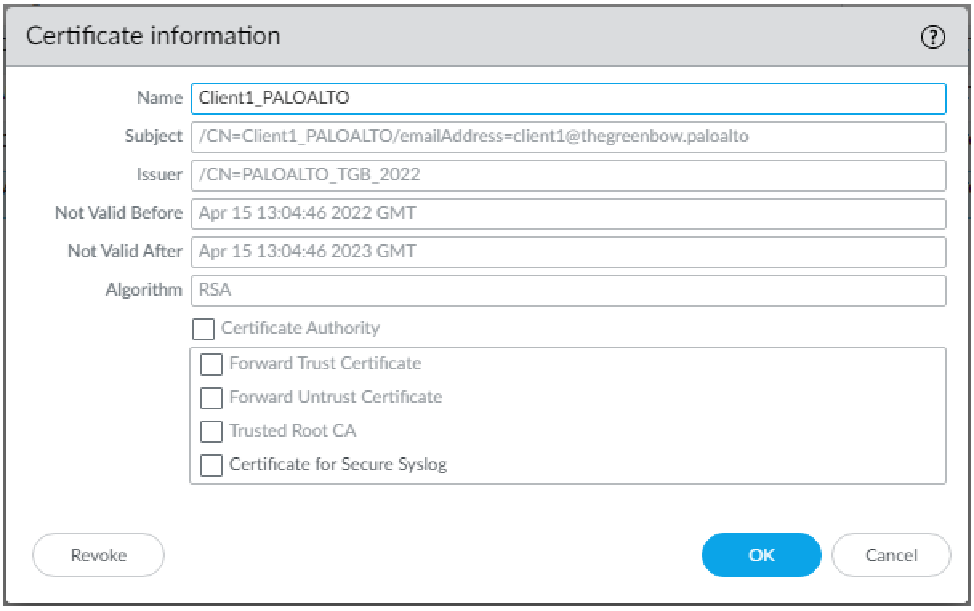
Successfully generated certificate and key pair : Client1_PALOALTO

8. Click **OK**.

The summary should appear as follows:



□	NAME	SUBJECT
□	PALOALTO_TGB_2...	CN = PALOALTO_TGB_2022
□	Client1_PALOA...	CN = Client1_PALOALTO, emailAddress = client1@thegreenbow.paloalto



Certificate information

Name: Client1_PALOALTO

Subject: /CN=Client1_PALOALTO/emailAddress=client1@thegreenbow.paloalto

Issuer: /CN=PALOALTO_TGB_2022

Not Valid Before: Apr 15 13:04:46 2022 GMT

Not Valid After: Apr 15 13:04:46 2023 GMT

Algorithm: RSA

□ Certificate Authority

□ Forward Trust Certificate

□ Forward Untrust Certificate

□ Trusted Root CA

□ Certificate for Secure Syslog

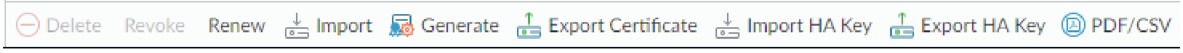
9. Click **OK**.

You have successfully created a User Identity. Proceed with creating a Server Identity, as described in the next section.

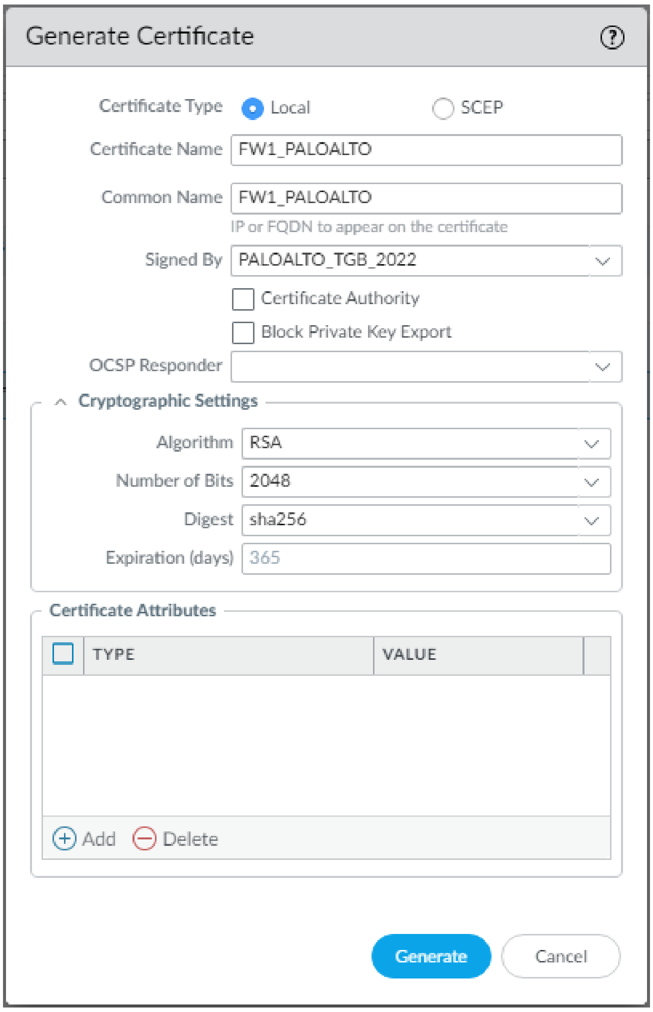
2.2.3 Creating a Server Identity

To create a Server Identity, proceed as follows:

1. Click **Generate** in the lower menu bar.



The **Generate Certificate** window is displayed:



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: FW1_PALOALTO

Common Name: FW1_PALOALTO

IP or FQDN to appear on the certificate

Signed By: PALOALTO_TGB_2022

□ Certificate Authority

□ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

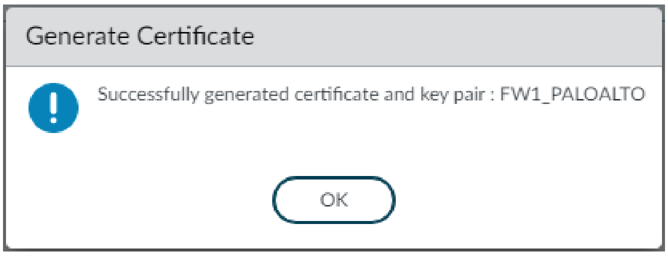
Digest: sha256

Expiration (days): 365

Certificate Attributes

□	TYPE	VALUE

2. In the **Certificate Name** and **Common Name** fields, enter the value `FW1_PALOALTO`.
3. In the **Signed By** drop-down list, select the value **PALOALTO_TGB_2022**.
4. Fill in the **Cryptographic settings** with relevant values.
5. Click **Generate**. A confirmation prompt is displayed:

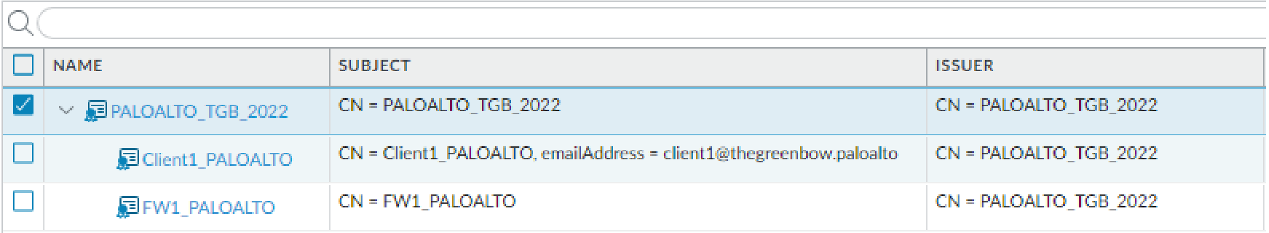


Generate Certificate

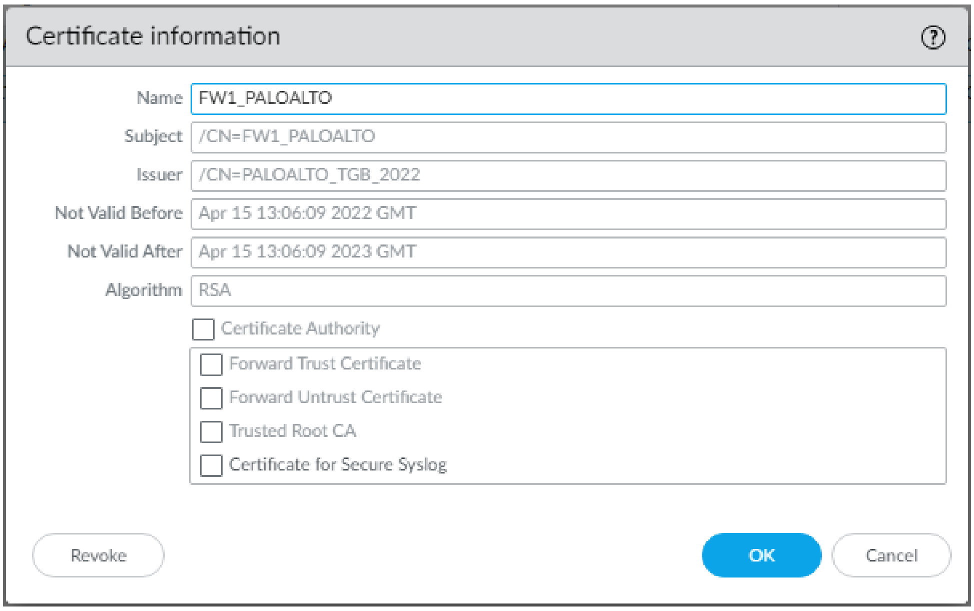
Successfully generated certificate and key pair : FW1_PALOALTO

6. Click **OK**.

The summary should appear as follows:



☐	NAME	SUBJECT	ISSUER
☑	PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022
☐	Client1_PALOALTO	CN = Client1_PALOALTO, emailAddress = client1@thegreenbow.paloalto	CN = PALOALTO_TGB_2022
☐	FW1_PALOALTO	CN = FW1_PALOALTO	CN = PALOALTO_TGB_2022



Certificate information

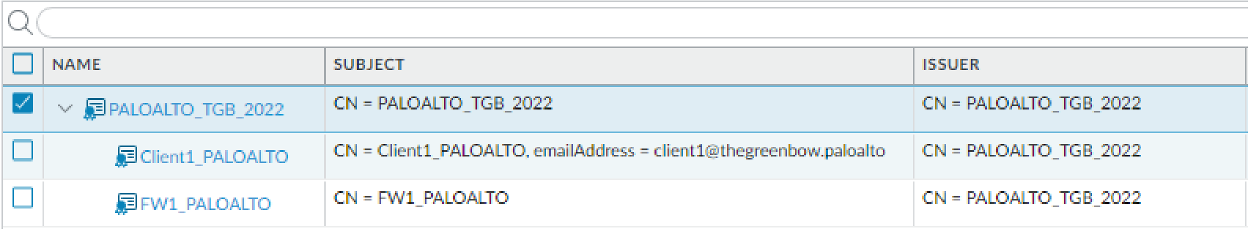
Name: FW1_PALOALTO
Subject: /CN=FW1_PALOALTO
Issuer: /CN=PALOALTO_TGB_2022
Not Valid Before: Apr 15 13:06:09 2022 GMT
Not Valid After: Apr 15 13:06:09 2023 GMT
Algorithm: RSA

☐ Certificate Authority
☐ Forward Trust Certificate
☐ Forward Untrust Certificate
☐ Trusted Root CA
☐ Certificate for Secure Syslog

7. Click **OK**.

You should now see the following in the **Device Certificates** list:

- A Root Authority (e.g. **PALOALTO_TGB_2022**) containing the following two items:
  - A User Identity (e.g. **Client1_PALOALTO**)
  - A Server Identity (e.g. **FW1_PALOALTO**)



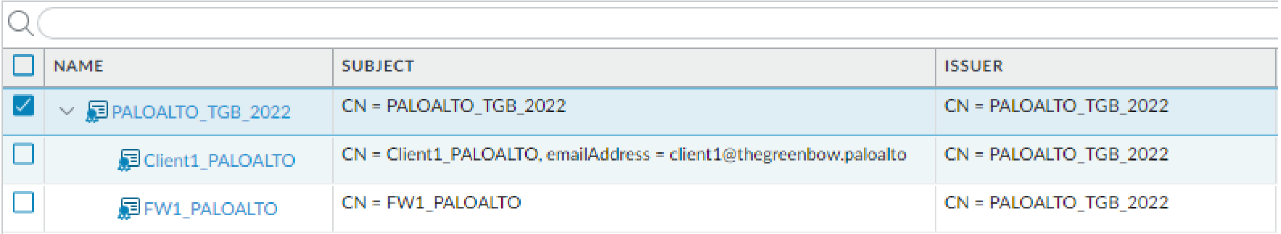
☐	NAME	SUBJECT	ISSUER
☑	PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022
☐	Client1_PALOALTO	CN = Client1_PALOALTO, emailAddress = client1@thegreenbow.paloalto	CN = PALOALTO_TGB_2022
☐	FW1_PALOALTO	CN = FW1_PALOALTO	CN = PALOALTO_TGB_2022

You have successfully created the required certificates. Proceed with exporting them, as described in the next section.

2.2.4 Exporting certificates

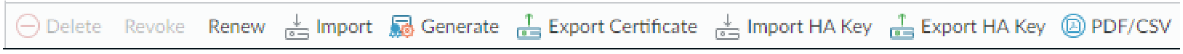
To export certificates, proceed as follows:

1. Start by downloading the Root Authority. To do so, check the box corresponding to the Root Authority you just created (e.g. **PALOALTO_TGB_2022**).

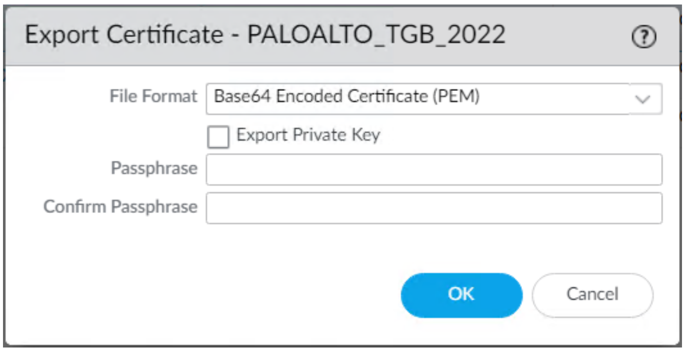


□	NAME	SUBJECT	ISSUER
☑	PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022
□	Client1_PALOALTO	CN = Client1_PALOALTO, emailAddress = client1@thegreenbow.paloalto	CN = PALOALTO_TGB_2022
□	FW1_PALOALTO	CN = FW1_PALOALTO	CN = PALOALTO_TGB_2022

2. Click **Export Certificate** in the lower menu bar.



The **Export Certificate** dialog box is displayed:



Export Certificate - PALOALTO_TGB_2022

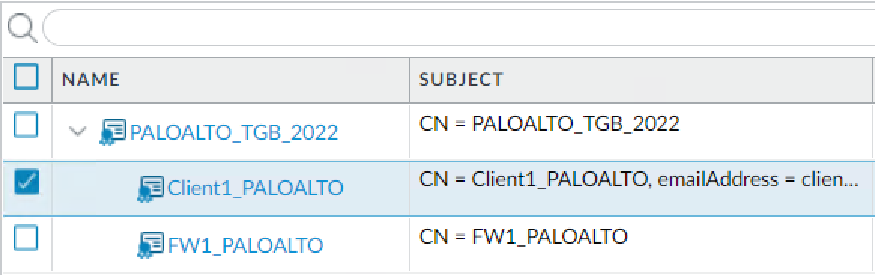
File Format: Base64 Encoded Certificate (PEM)

□ Export Private Key

Passphrase:

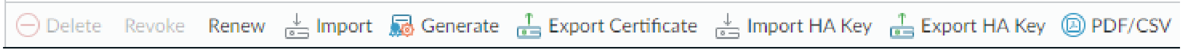
Confirm Passphrase:

3. In the **File Format** drop-down list, select the extension **Binary Encoded Certificate (PEM)**.
4. Click **OK**.
5. Now, download the User Identity. To do so, check the box corresponding to the User Identity you just created (e.g. **Client1_PALOALTO**).

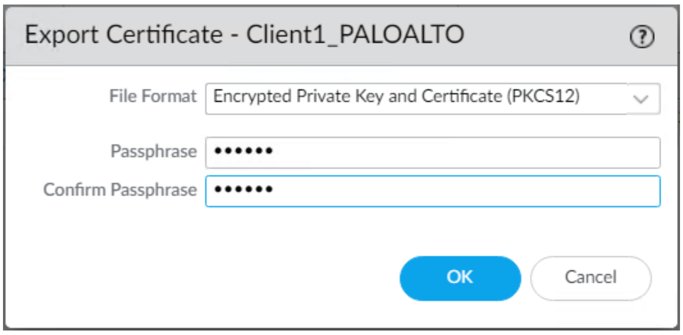


□	NAME	SUBJECT
□	PALOALTO_TGB_2022	CN = PALOALTO_TGB_2022
☑	Client1_PALOALTO	CN = Client1_PALOALTO, emailAddress = clien...
□	FW1_PALOALTO	CN = FW1_PALOALTO

6. Click **Export Certificate** in the lower menu bar.



The **Export Certificate** dialog box is displayed:


Export Certificate - Client1_PALOALTO

File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase: ••••••

Confirm Passphrase: ••••••

7. In the **File Format** drop-down list, select the extension **Encrypted Private Key and Certificate (PKCS12)**.
8. Set and confirm a passphrase.
9. Click **OK**.

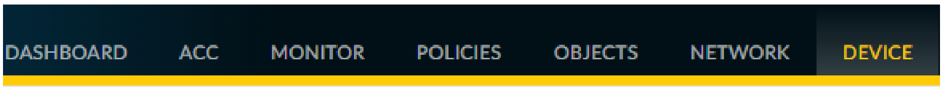
> You will later need to import this P12 file into the VPN Client using the passphrase that you just set.

You have successfully exported the required certificates. Proceed with creating a certificate profile, as described in the next section.

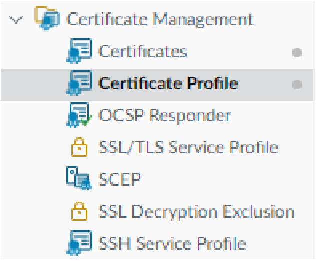
2.3 Creating a Certificate Profile

To create the required certificate profile, follow the steps below:

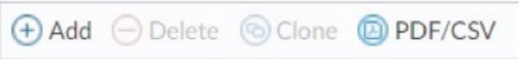
1. From the top menu, select **DEVICE**.



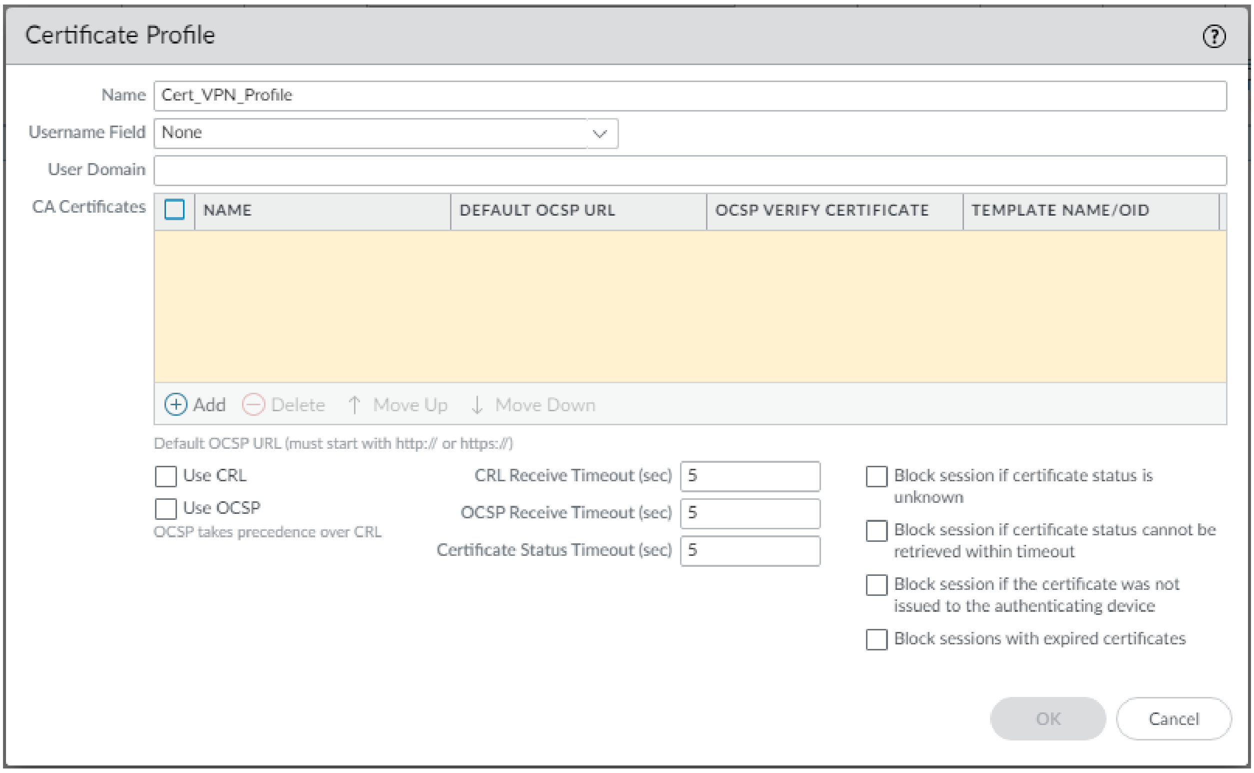
2. Then, choose **Certificate Management** > **Certificate Profile**.



3. Click **Add** in the lower menu bar.



The **Certificate Profile** window is displayed:


Certificate Profile

Name: Cert_VPN_Profile

Username Field: None

User Domain:

CA Certificates:

□	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID

Default OCSP URL (must start with http:// or https://)

□ Use CRL

□ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

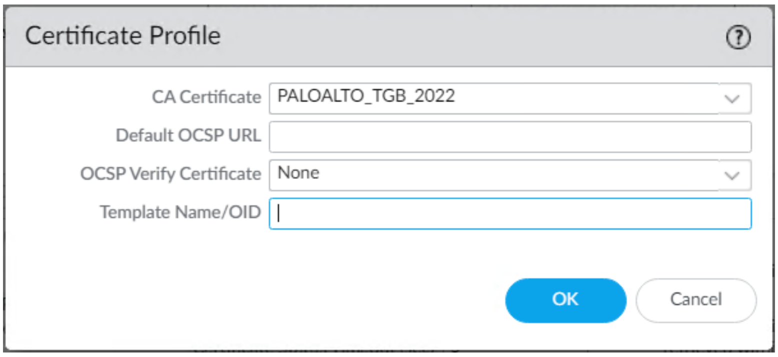
□ Block session if certificate status is unknown

□ Block session if certificate status cannot be retrieved within timeout

□ Block session if the certificate was not issued to the authenticating device

□ Block sessions with expired certificates

4. In the **Name** field, enter `Cert_VPN_profile`.
5. In the **CA Certificates** box, click **Add**. The **Certificate Profile** dialog box is displayed:


Certificate Profile

CA Certificate: PALOALTO_TGB_2022

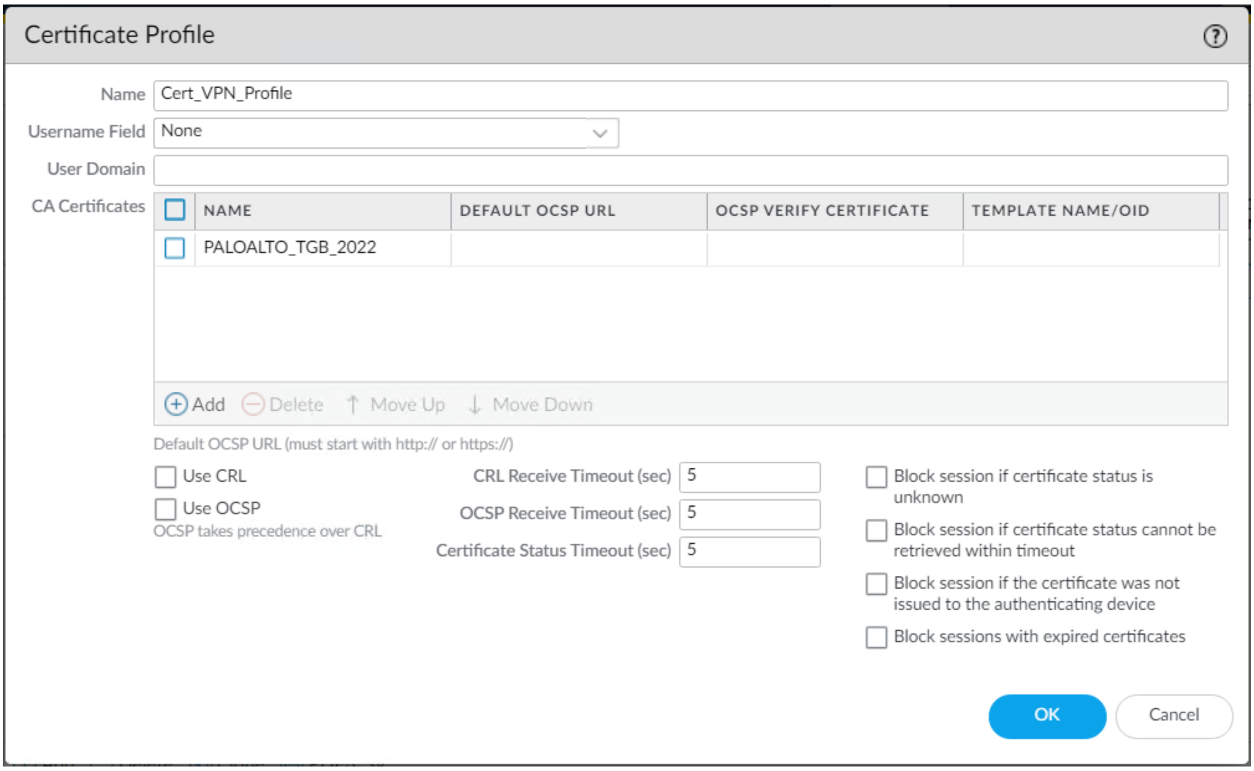
Default OCSP URL:

OCSP Verify Certificate: None

Template Name/OID:

6. In the **CA Certificate** drop-down list, select **PALOALTO_TGB_2022**.
7. Click **OK**.

The CA Certificate has been added to the Certificate Profile:



Certificate Profile

Name	Cert_VPN_Profile
Username Field	None
User Domain	

CA Certificates

□	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
□	PALOALTO_TGB_2022			

Default OCSP URL (must start with http:// or https://)

□ Use CRL

□ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec) 5

OCSP Receive Timeout (sec) 5

Certificate Status Timeout (sec) 5

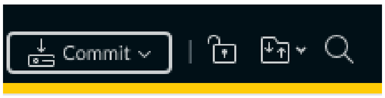
□ Block session if certificate status is unknown

□ Block session if certificate status cannot be retrieved within timeout

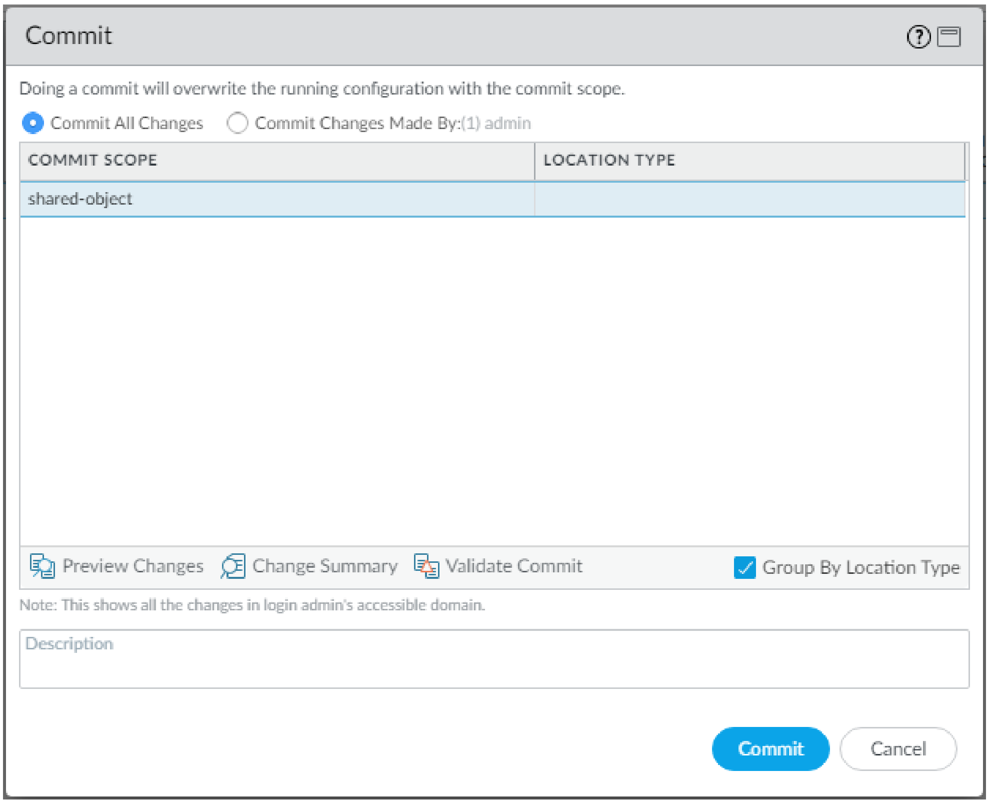
□ Block session if the certificate was not issued to the authenticating device

□ Block sessions with expired certificates

8. Click **OK**.
9. Click **Commit** at the top right to apply the configuration.



The **Commit** window is displayed:



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

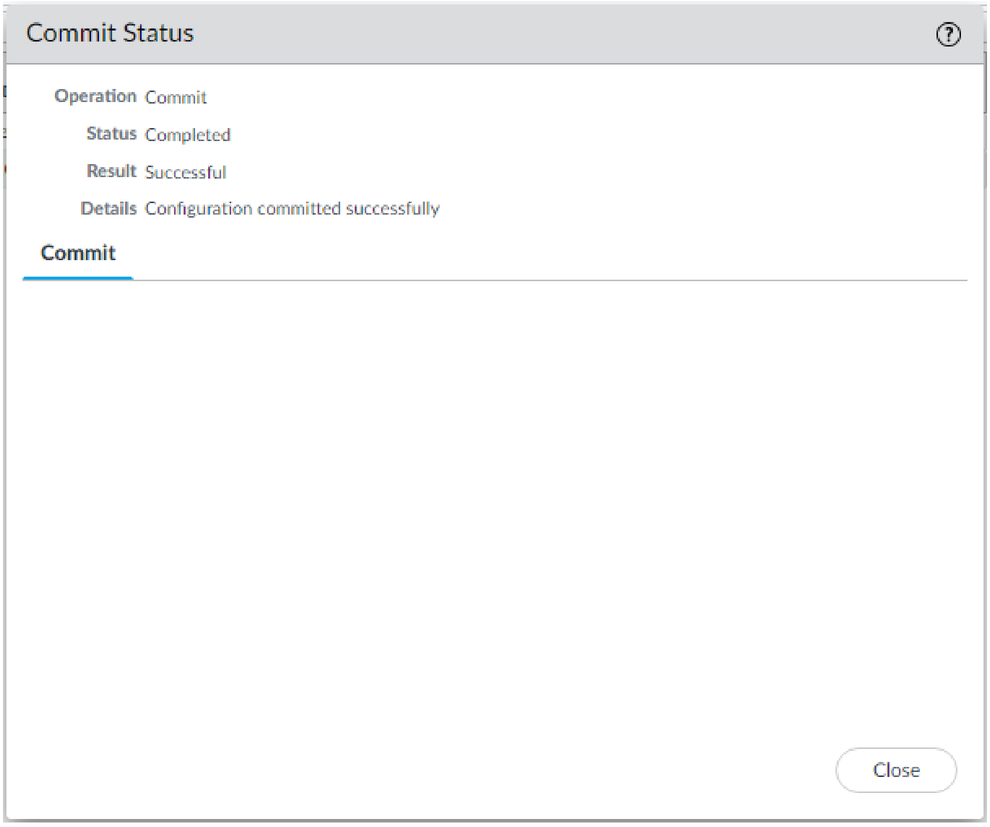
COMMIT SCOPE	LOCATION TYPE
shared-object	

☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

10. Click **Commit** to apply your changes.

The **Commit Status** window is displayed:



Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

11. Click **Close**.

You have successfully created a Certificate Profile. Proceed with generating VPN encryption profiles, as described in the next section.

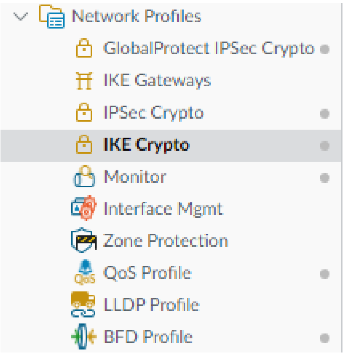
2.4 VPN encryption profiles

2.4.1 IKE profile

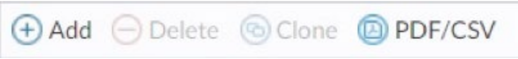
To generate the IKE VPN encryption profile, proceed as follows:

1. From the top menu, select **NETWORK**.

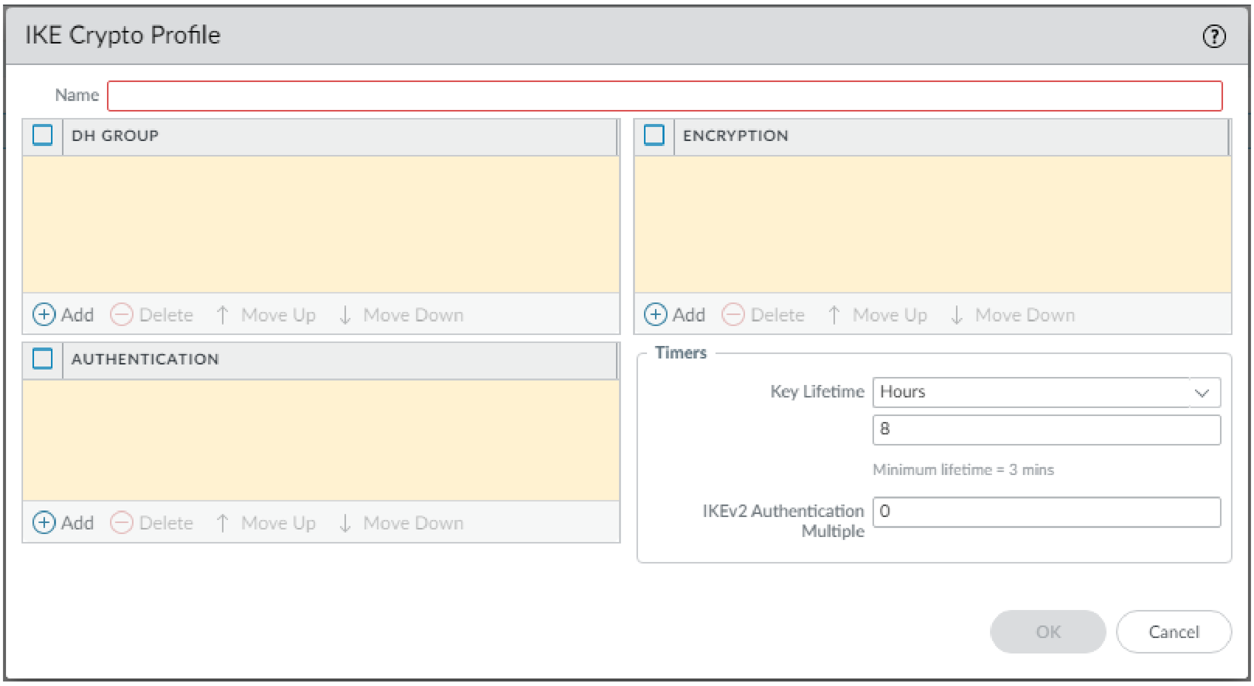
2. Then, choose **Network Profiles** > **IKE Crypto**.



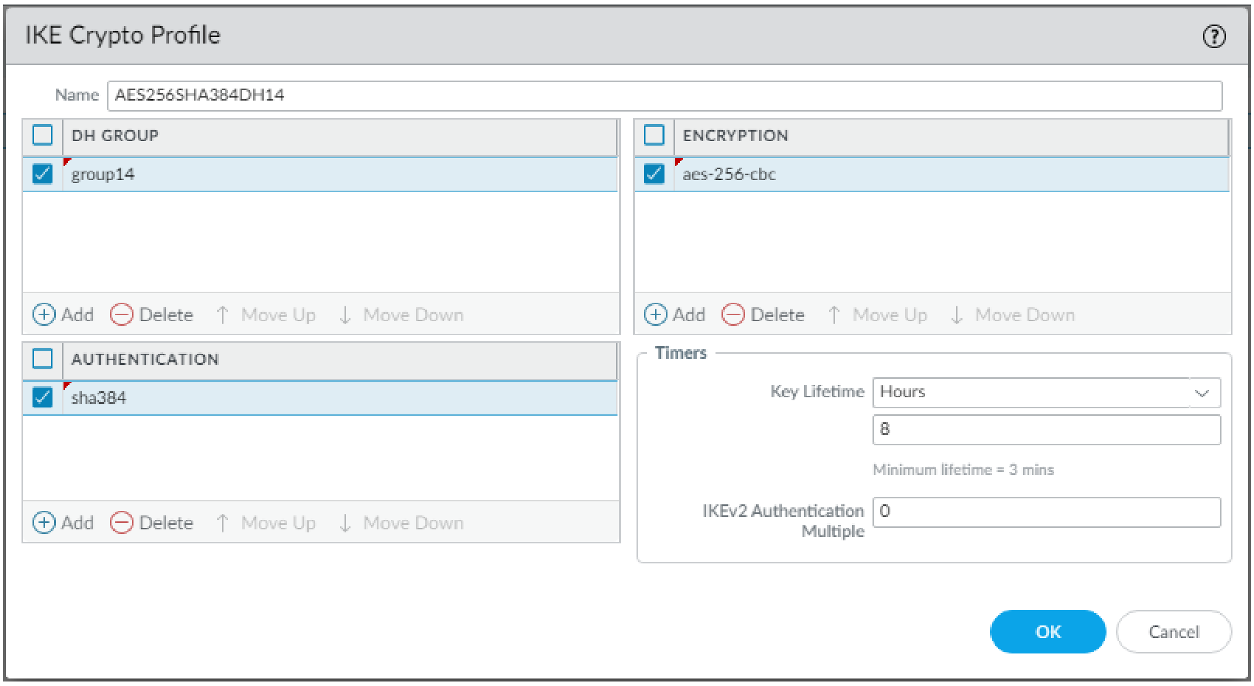
3. Click **Add** in the lower menu bar.



The **IKE Crypto Profile** window is displayed:



4. In the **Name** field, enter the value `AES256SHA384DH14`.
5. In the **DH GROUP** box, click **Add**, and then select the value **group14**.
6. In the **AUTHENTICATION** box, click **Add**, and the select the value **sha384**.
7. In the **ENCRYPTION** box, click **Add**, and the select the value **aes-256-cbc**.



IKE Crypto Profile

Name: AES256SHA384DH14

☐	DH GROUP
☑	group14

☐	ENCRYPTION
☑	aes-256-cbc

☐	AUTHENTICATION
☑	sha384

Timers

Key Lifetime: Hours

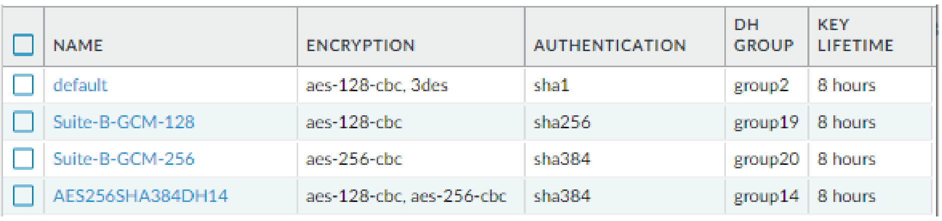
8

Minimum lifetime = 3 mins

IKEv2 Authentication Multiple: 0

8. Click **OK** to proceed with generating the IKE profile as described in the next section below.

   The summary should appear as follows:



☐	NAME	ENCRYPTION	AUTHENTICATION	DH GROUP	KEY LIFETIME
☐	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
☐	AES256SHA384DH14	aes-128-cbc, aes-256-cbc	sha384	group14	8 hours

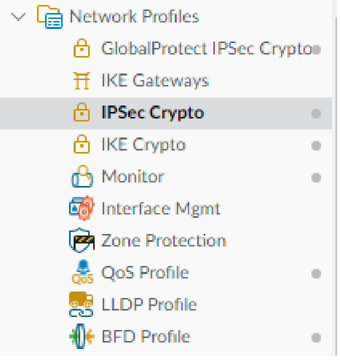
You have successfully generated an IKE VPN encryption profile. Proceed with generating a Child SA VPN encryption profile, as described in the next section.

2.4.2 VPN encryption profiles: Child SA profile

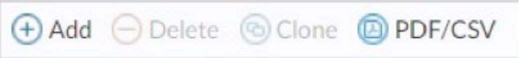
To generate the Child SA VPN encryption profile, proceed as follows:

1. From the top menu, select **NETWORK**.

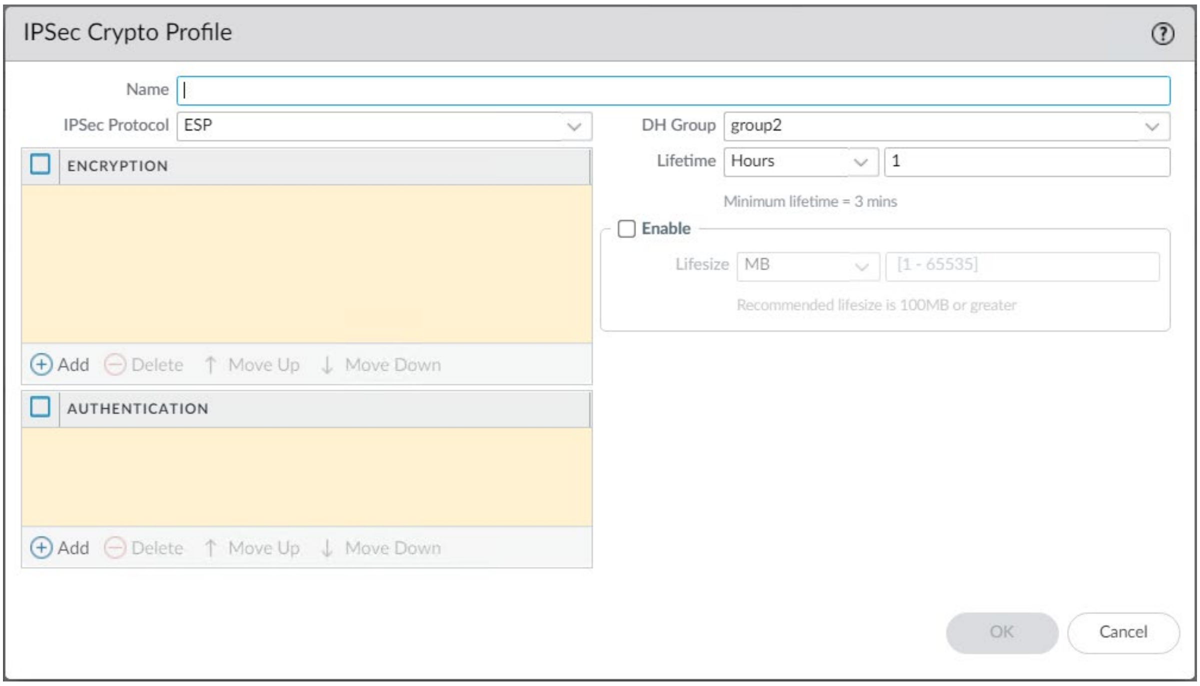
2. Then, choose **Network Profiles** > **IPSec Crypto**.



3. Click **Add** in the lower menu bar.



The **IPSec Crypto Profile** window is displayed:



Name |

IPSec Protocol ESP

DH Group group2

Lifetime Hours 1

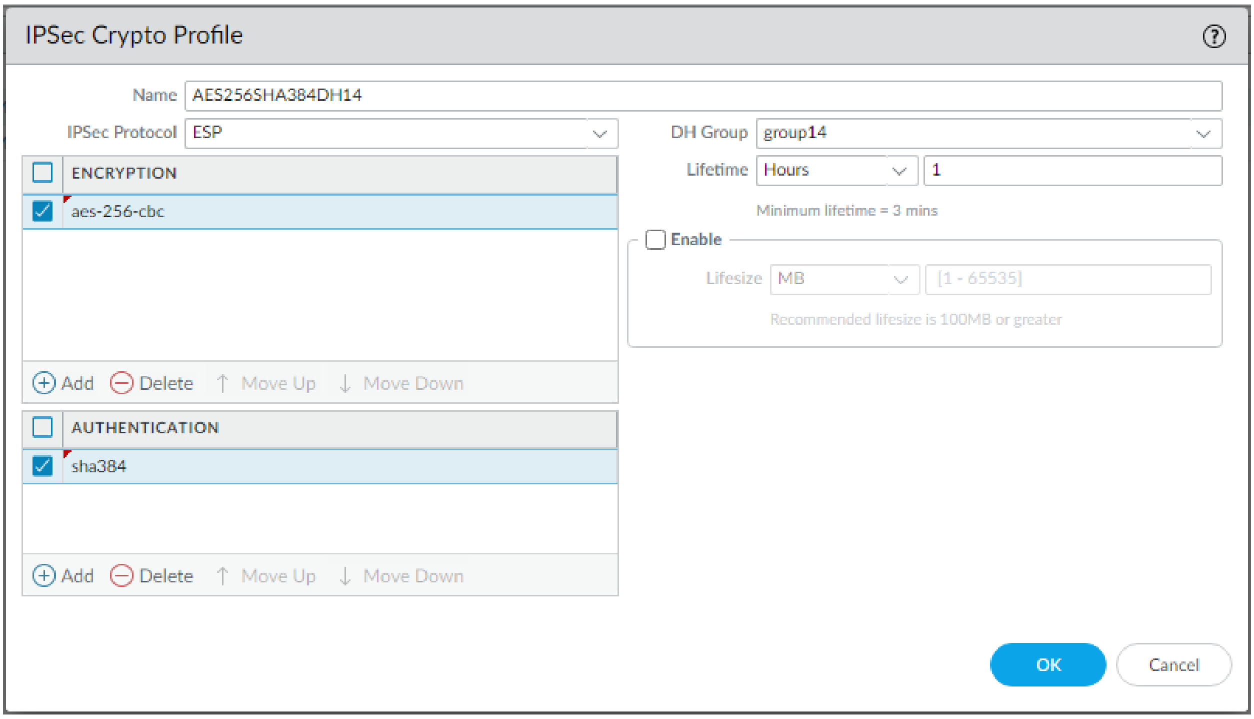
Minimum lifetime = 3 mins

□ Enable

Lifesize MB [1 - 65535]

Recommended lifesize is 100MB or greater

4. In the **Name** field, enter the value `AES256SHA384DH14`.
5. In the **ENCRYPTION** box, click **Add**, and the select the value **aes-256-cbc**.
6. In the **AUTHENTICATION** box, click **Add**, and the select the value **sha384**.
7. In the **DH GROUP** box, click **Add**, and then select the value **group14**.



IPSec Crypto Profile

Name: AES256SHA384DH14

IPSec Protocol: ESP

DH Group: group14

Lifetime: Hours 1

Minimum lifetime = 3 mins

□ Enable

Lifesize: MB [1 - 65535]

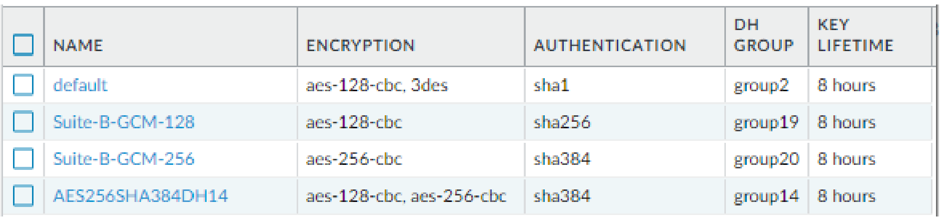
Recommended lifesize is 100MB or greater

□	ENCRYPTION
☑	aes-256-cbc

□	AUTHENTICATION
☑	sha384

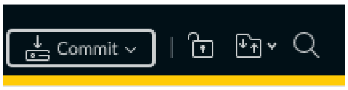
8. Click **OK** to proceed with generating the IKE profile as described in the next section below.

   The summary should appear as follows:

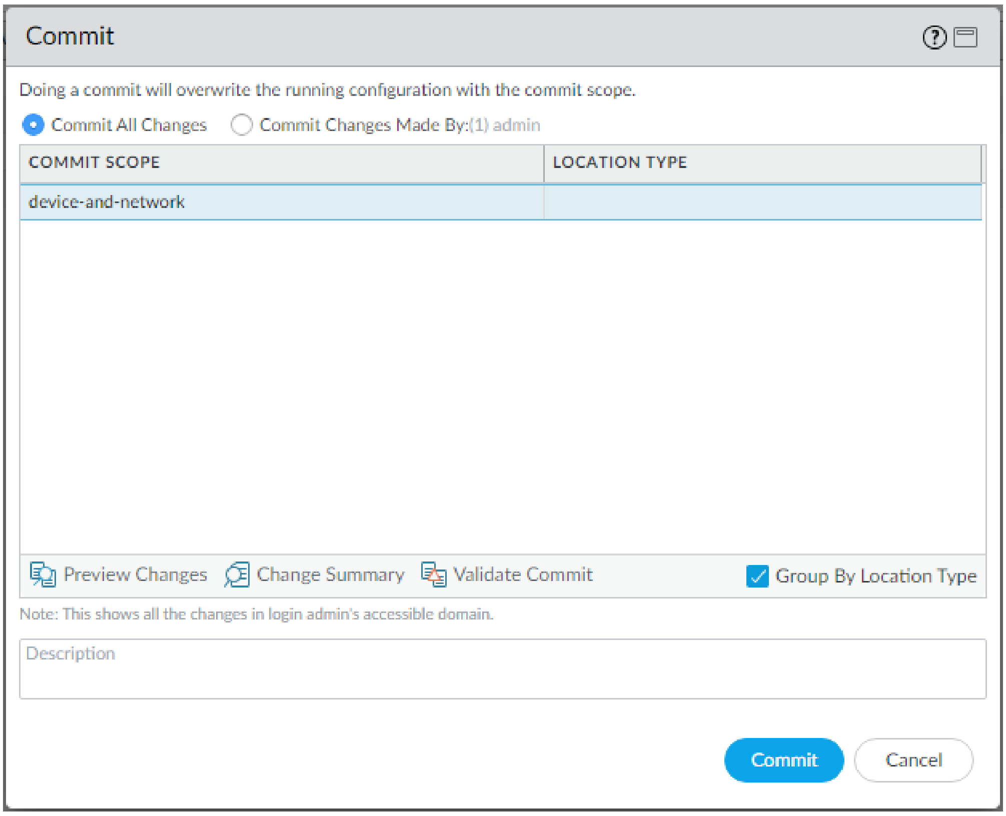


□	NAME	ENCRYPTION	AUTHENTICATION	DH GROUP	KEY LIFETIME
□	default	aes-128-cbc, 3des	sha1	group2	8 hours
□	Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
□	Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours
□	AES256SHA384DH14	aes-128-cbc, aes-256-cbc	sha384	group14	8 hours

9. Click **Commit** to apply the configuration.



The **Commit** window is displayed:



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
device-and-network	

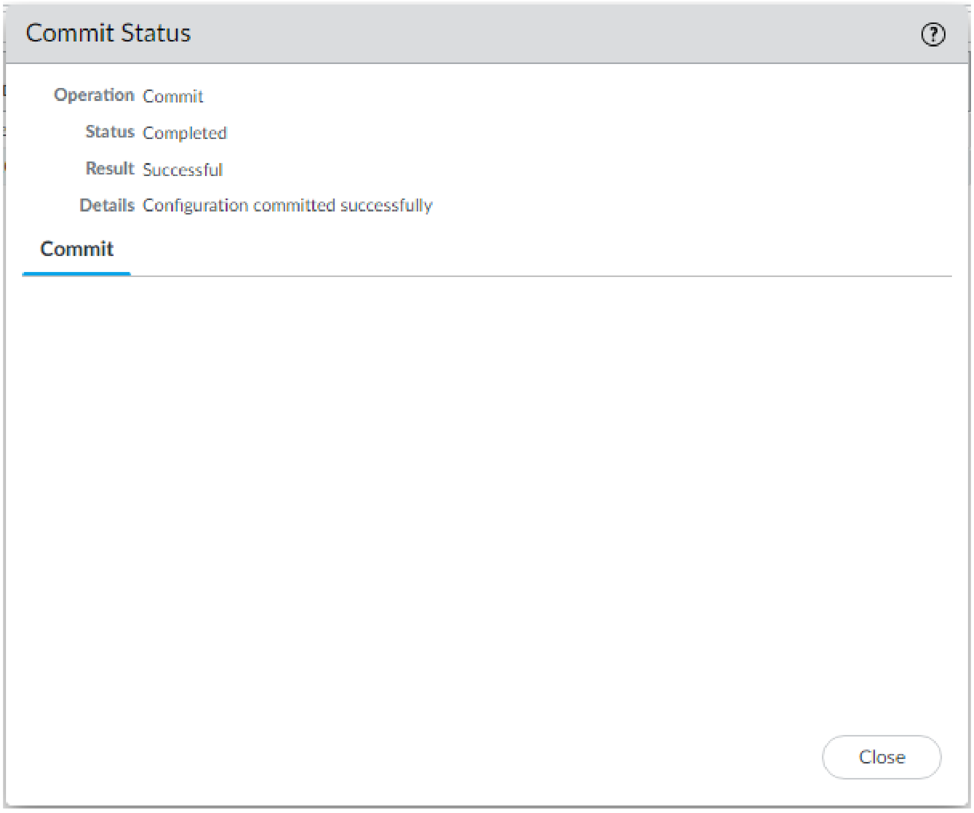
☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

10. Click **Commit** to apply your changes.

The **Commit Status** window is displayed:



Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

11. Click **Close**.

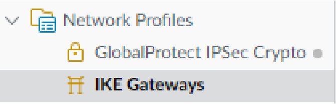
You have successfully generated a Child SA VPN encryption profile. Proceed with creating an IKE Auth for the VPN tunnel, as described in the next section.

2.5 VPN tunnel: IKE Gateways

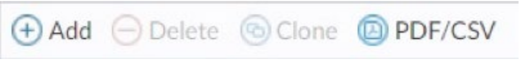
To create an IKE Auth for the VPN tunnel, proceed as follows:

1. From the top menu, select **NETWORK**.

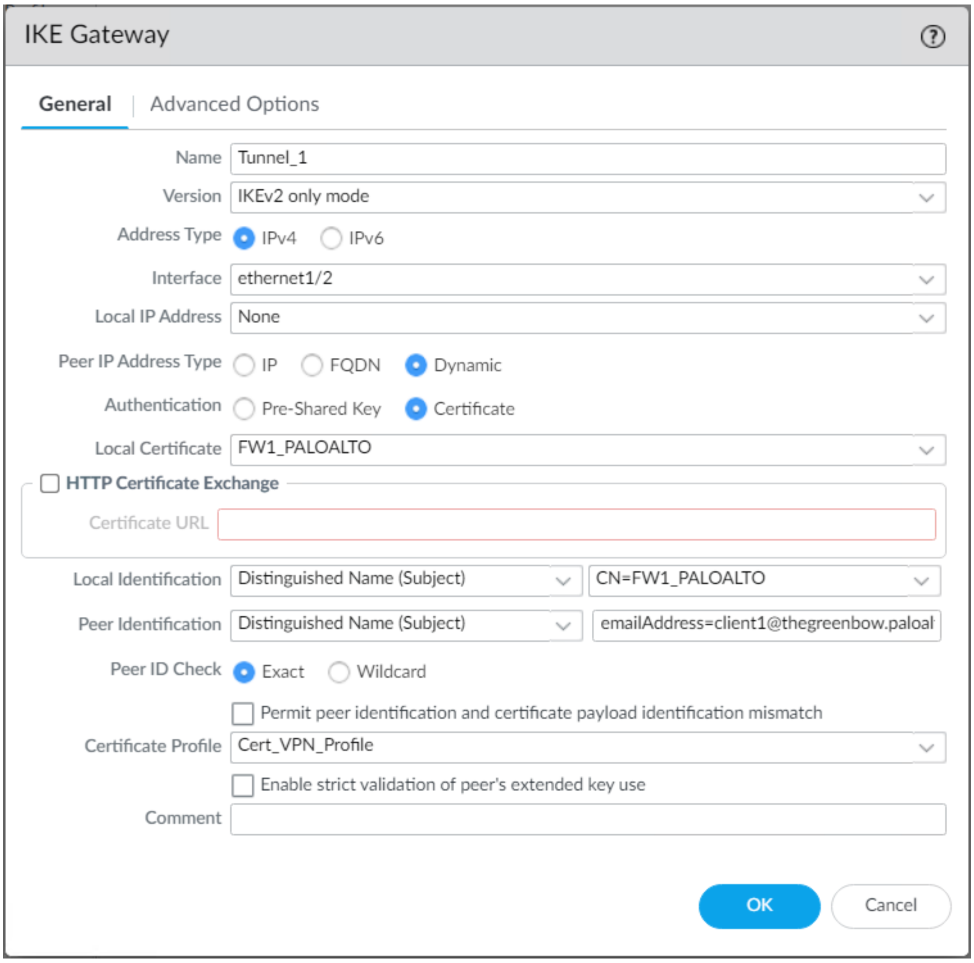
2. Then, choose **Network Profiles** > **IKE Gateways.**



3. Click **Add** in the lower menu bar.



The **IKE Gateway** window is displayed:



IKE Gateway

General | Advanced Options

Name: Tunnel_1

Version: IKEv2 only mode

Address Type: ● IPv4 ○ IPv6

Interface: ethernet1/2

Local IP Address: None

Peer IP Address Type: ○ IP ○ FQDN ● Dynamic

Authentication: ○ Pre-Shared Key ● Certificate

Local Certificate: FW1_PALOALTO

□ HTTP Certificate Exchange

Certificate URL:

Local Identification: Distinguished Name (Subject) CN=FW1_PALOALTO

Peer Identification: Distinguished Name (Subject) emailAddress=client1@thegreenbow.paloal

Peer ID Check: ● Exact ○ Wildcard

□ Permit peer identification and certificate payload identification mismatch

Certificate Profile: Cert_VPN_Profile

□ Enable strict validation of peer's extended key use

Comment:

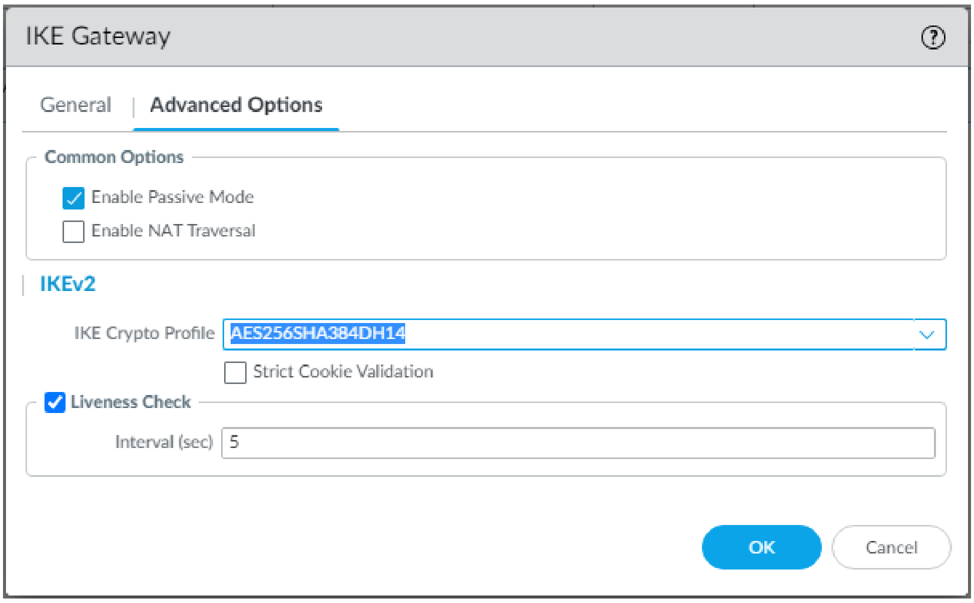
OK Cancel

4. In the **Name** field enter `Tunnel_1`.
5. In the **Version** drop-down list, select **IKEv2 only mode**.
6. In the **Interface** drop-down list, select **ethernet1/2**.
7. Under **Peer IP Address Type**, select **Dynamic**.
8. Under **Authentication**, select **Certificate**.
9. In the **Local Certificate** drop-down list, select **FW1_PALOALTO** (Server Identity).
10. In the **Local Identification** drop-down list, select **Distinguished Name (Subject)**. The corresponding value **CN=FW1_PALOALTO** (subject of the certificate from Server Identity) should be selected automatically. Select it, if this is not the case.
11. In the **Peer Identification** drop-down list, select **Distinguished Name (Subject)** and the corresponding value **emailAddress=client1@thegreenbow.paloalto,CN=Client1_PALOALTO** (subject of the certificate from User Identity).

12. In the **Certificate Profile** drop-down list, select **Cert_VPN_Profile**.

    The window should now appear as in the above screenshot.

13. Click the Advanced Options tab.



IKE Gateway

General | Advanced Options

Common Options

☑ Enable Passive Mode

□ Enable NAT Traversal

IKEv2

IKE Crypto Profile: AES256SHA384DH14

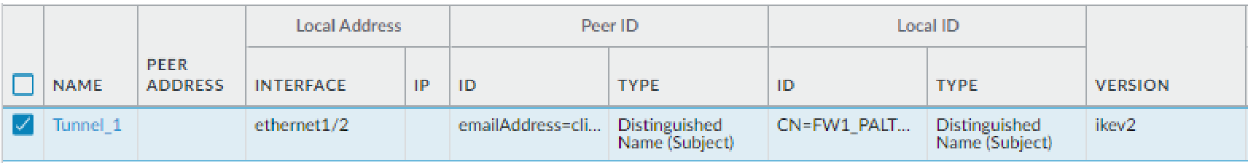
□ Strict Cookie Validation

☑ Liveness Check

Interval (sec): 5

14. In the IKE Crypto Profile drop-down list, select **AES256SHA384DH14**.
15. Click **OK**.

    You have successfully added the IKE Gateway named Tunnel_1.



			Local Address		Peer ID		Local ID		
□	NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION
☑	Tunnel_1		ethernet1/2		emailAddress=cli...	Distinguished Name (Subject)	CN=FW1_PALT...	Distinguished Name (Subject)	ikev2

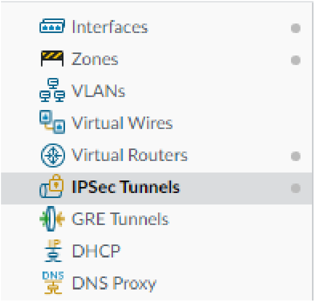
You have successfully created an IKE Auth for the VPN tunnel. Proceed with creating an IPsec tunnel for the VPN tunnel, as described in the next section.

2.6 VPN tunnel: IPsec Tunnels

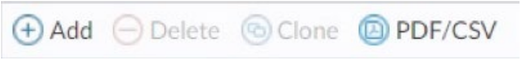
To create an IPsec tunnel for the VPN tunnel (corresponds to a Child SA in the Windows Enterprise VPN Client), proceed as follows:

1. From the top menu, select **NETWORK**.

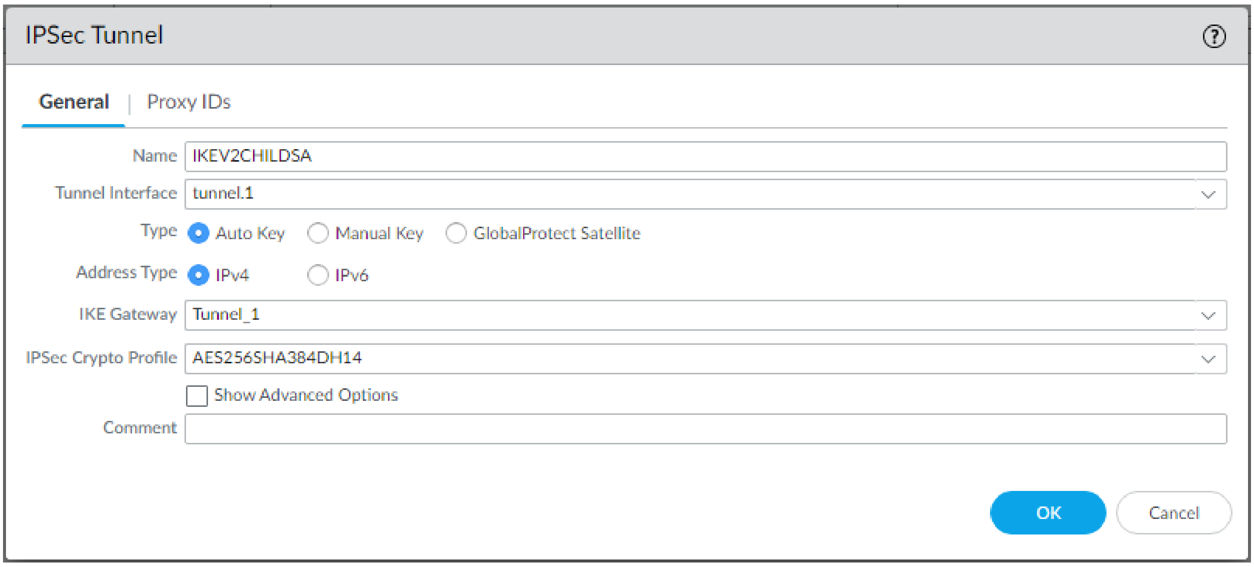
2. Then, choose **Network Profiles** > **IPSec Tunnels**.



3. Click **Add** in the lower menu bar.



The **IPSec Tunnel** window is displayed:



IPSec Tunnel

General | Proxy IDs

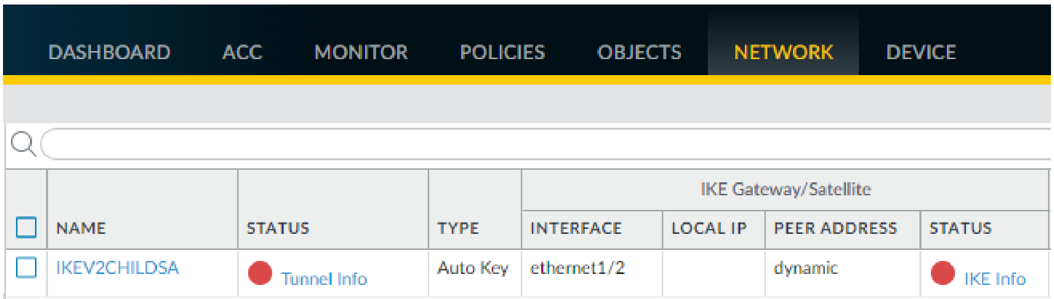
Name	IKEV2CHILDSA
Tunnel Interface	tunnel.1
Type	● Auto Key ○ Manual Key ○ GlobalProtect Satellite
Address Type	● IPv4 ○ IPv6
IKE Gateway	Tunnel_1
IPSec Crypto Profile	AES256SHA384DH14
	□ Show Advanced Options
Comment	

4. In the **Name** field enter `IKEV2CHILDSA`.
5. In the **Tunnel Interface** drop-down list, select **tunnel.1**.
6. Under **Type**, select **Auto Key**.
7. Under **Address Type**, select **IPv4**.
8. In the **IKE Gateway** drop-down list, select **Tunnel_1**.
9. In the **IPSec Crypto Profile** drop-down list, select **AES256SHA384DH14**.

   The window should now appear as in the above screenshot.

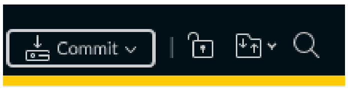
10. Click **OK**.

    You have successfully added the IPSec Tunnel named IKEV2CHILDSA.

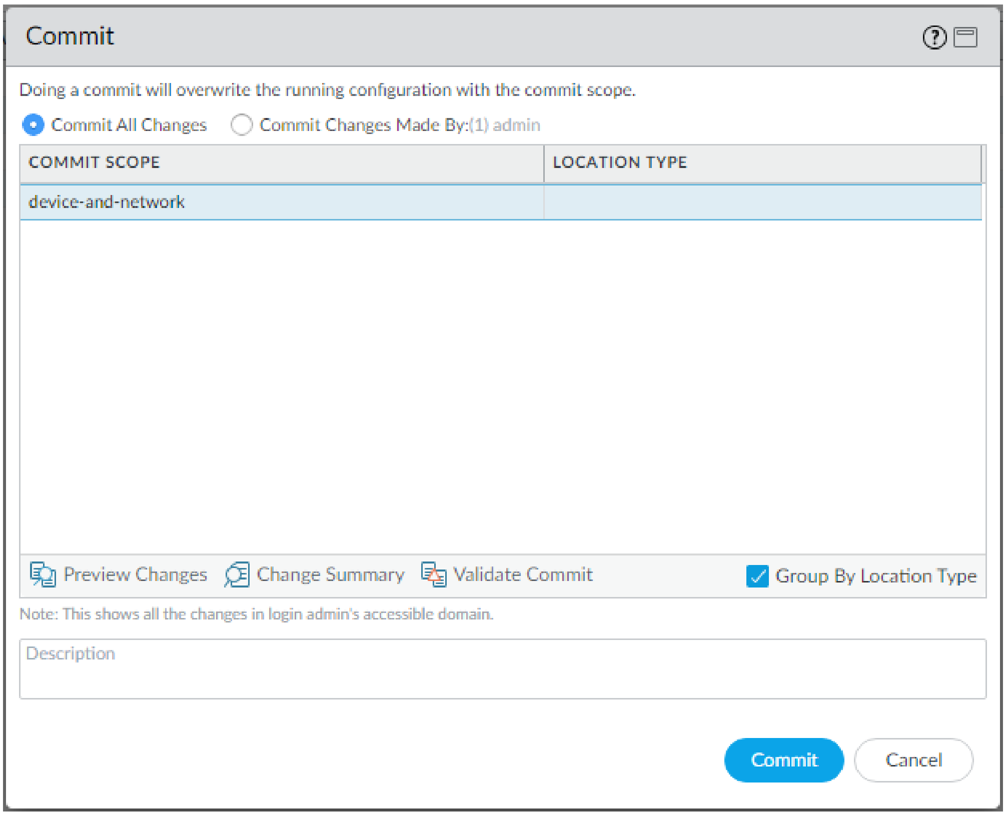


☐	NAME	STATUS	TYPE	IKE Gateway/Satellite			
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS
☐	IKEV2CHILDSA	● Tunnel Info	Auto Key	ethernet1/2		dynamic	● IKE Info

11. Click **Commit** at the top right to apply the configuration.



The **Commit** window is displayed:



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
device-and-network	

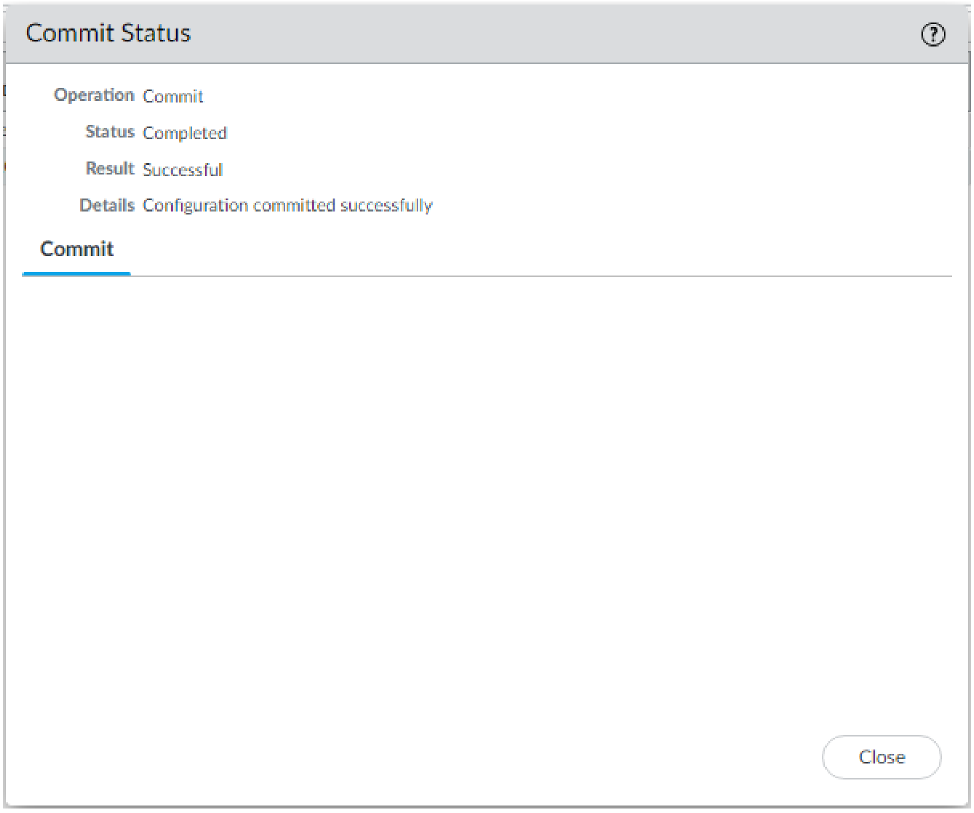
☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

12. Click **Commit** to apply your changes.

The **Commit Status** window is displayed:



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

13. Click **Close**.

You have successfully created an IPsec tunnel for the VPN tunnel. To complete the configuration of your Palo Alto firewall, you may want to define filtering rules, as described in the next section.

2.7 Filtering rules

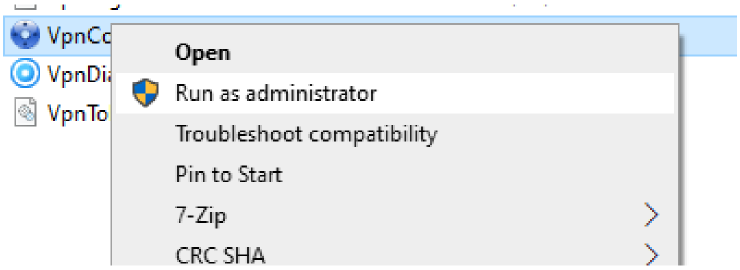
Where appropriate, integrate the filtering rules to allow IPsec traffic through the configured Palo Alto network interfaces (refer to Palo Alto documentation).

3 Configuring TheGreenBow VPN Client

This section describes how to configure TheGreenBow's Windows Enterprise VPN Client so that you may connect it to a Palo Alto firewall set up according to the instructions in the previous chapter.

3.1 Launching the VPN Client

By default, only administrators can access the Windows Enterprise VPN Client's **Configuration Panel**. Therefore, right-click **vpnconf.exe** in the **File Explorer** and select **Run as administrator**.



3.2 Creating a new IKE Auth

Configure the Windows Enterprise VPN Client as described below.

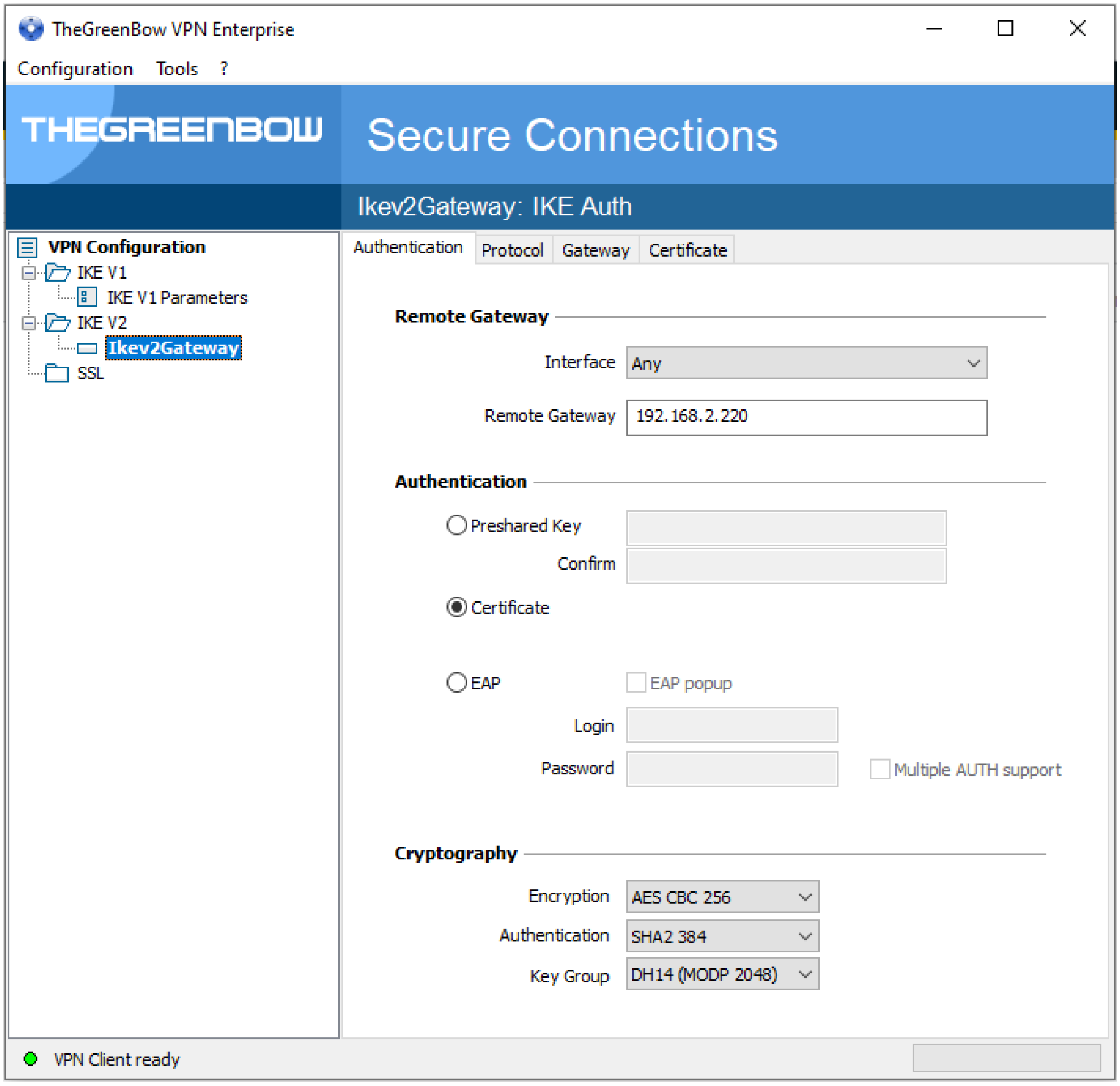
Start by creating a new IKEv2 IKE Auth. To do so, right-click the IKE v2 branch of the VPN configuration tree and select **New IKE Auth**.

3.2.1 Authentication tab

Select the **Authentication** tab and enter the following parameters:

- Interface: Any
- Remote Gateway: the IP address of the Palo Alto firewall in your network
- Authentication: certificate
- Cryptography:
  - Encryption: AES GCM 256
  - Authentication: SHA2 384
  - Key Group: DH14

You should now see the following screen:



Remote Gateway

Interface: Any

Remote Gateway: 192.168.2.220

Authentication

○ Preshared Key

Confirm

● Certificate

○ EAP □ EAP popup

Login

Password □ Multiple AUTH support

Cryptography

Encryption: AES CBC 256

Authentication: SHA2 384

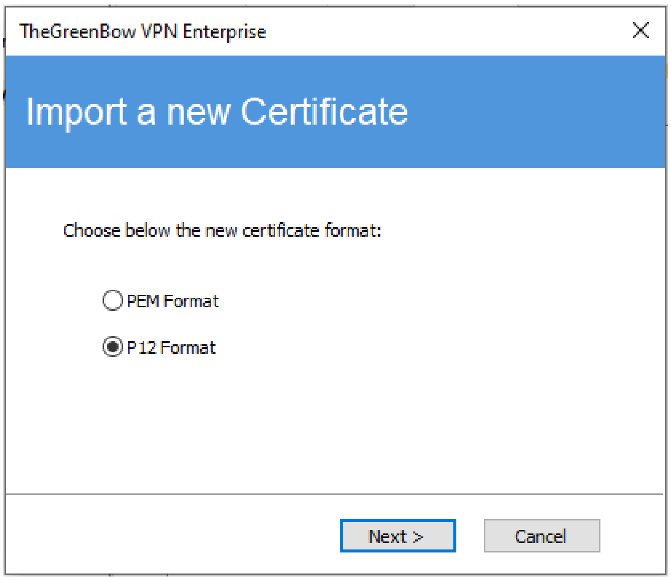
Key Group: DH14 (MODP 2048)

VPN Client ready

3.2.2 Certificate tab

To import the user certificate, proceed as follows:

1. Select the **Certificate** tab.
2. Click **Import Certificate...**


TheGreenBow VPN Enterprise

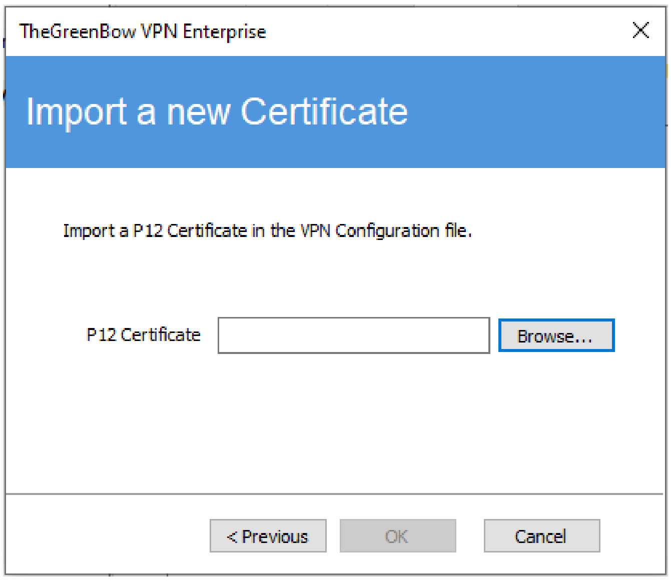
Import a new Certificate

Choose below the new certificate format:

○ PEM Format

● P12 Format

3. Select **P12 Format**.
4. Click **Next >**.


TheGreenBow VPN Enterprise

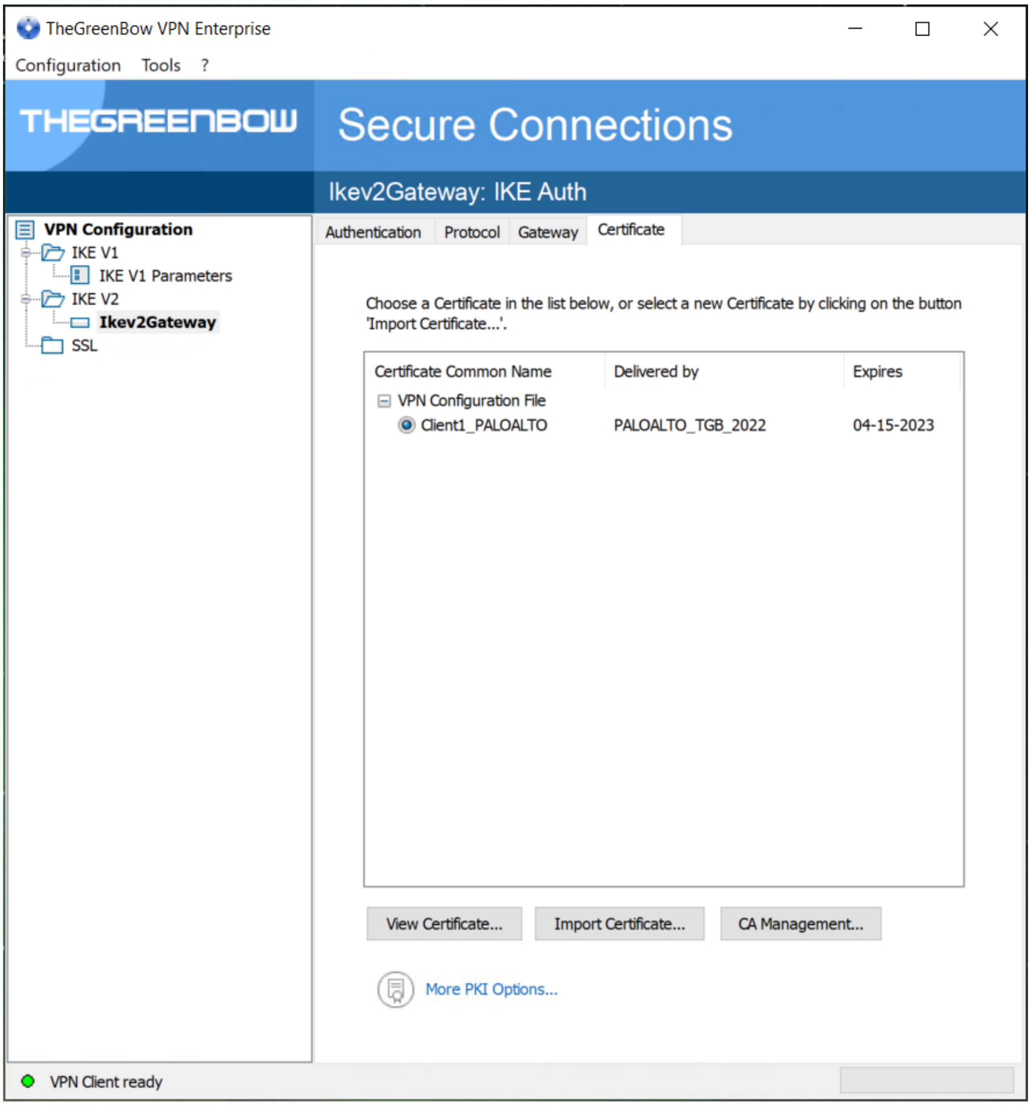
Import a new Certificate

Import a P12 Certificate in the VPN Configuration file.

P12 Certificate

5. Click **Browse...**
6. Select the User Identity that you have previously downloaded from the Palo Alto firewall (e.g. **cert_Client1_PALOALTO.p12**).
7. Enter the password when prompted.
8. Click **OK**.

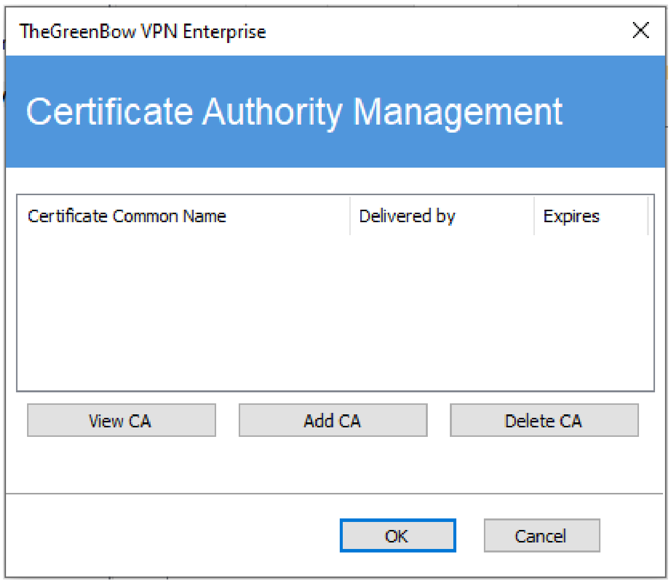
You should now see the following screen:



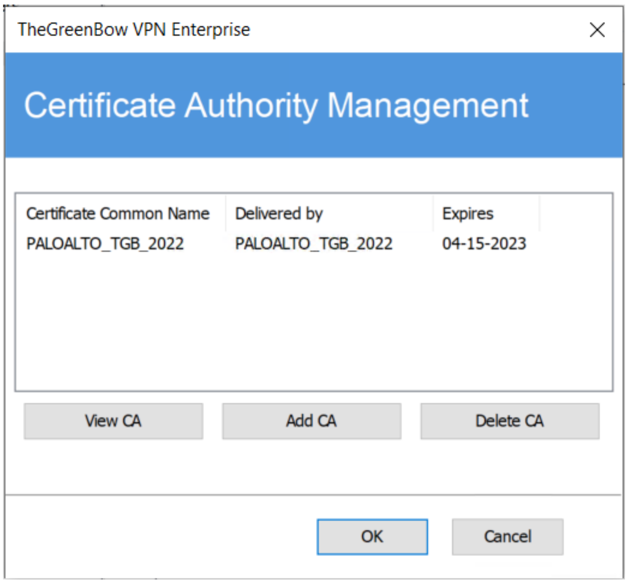
Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.

Certificate Common Name	Delivered by	Expires
⊟ VPN Configuration File		
● Client1_PALOALTO	PALOALTO_TGB_2022	04-15-2023

9. Click **CA Management**



10. Click **Add CA**
11. Select **DER format**.
12. Click **Next >**.
13. Click **Browse…**
14. Select the Certificate Authority that you have previously downloaded from the Palo Alto firewall (e.g. **cert_PALOALTO_TGB_2022.der**).
15. Click **OK**.

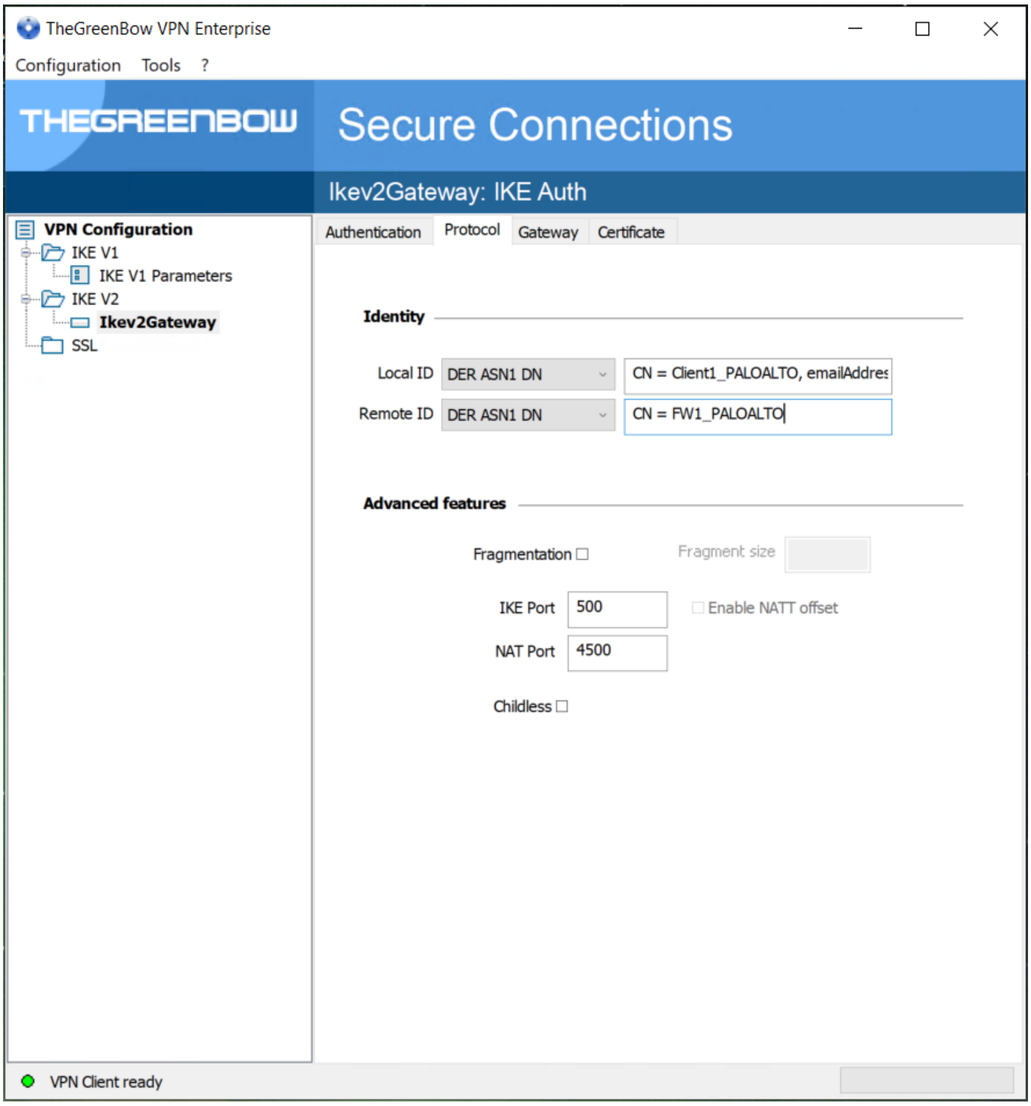


Certificate Common Name	Delivered by	Expires
PALOALTO_TGB_2022	PALOALTO_TGB_2022	04-15-2023

16. Click **OK**.

3.2.3 Protocol tab

Set the following additional parameters in the **Protocol** tab:



Local ID: DER ASN1 DN — CN = Client1_PALOALTO, emailAddres

Remote ID: DER ASN1 DN — CN = FW1_PALOALTO

Fragmentation □

IKE Port: 500

□ Enable NATT offset

NAT Port: 4500

Childless □

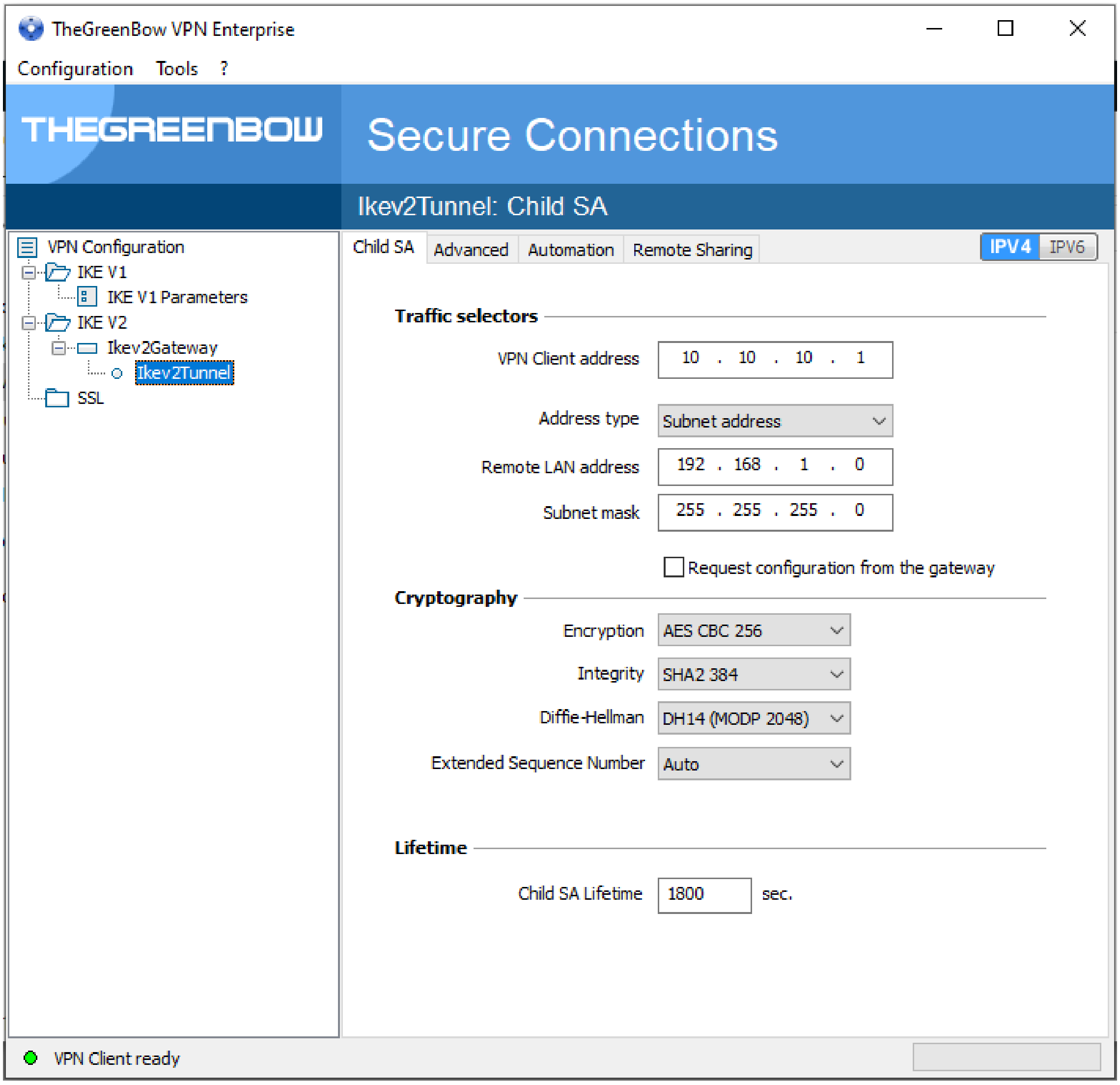
The **Local ID** `DER ASN1 DN` will be automatically updated with the subject from the imported certificate (see below).

The **Remote ID** must be of type `DER ASN1 DN` and contain the same value as the **Local ID** field on the Palo Alto firewall:

```
CN = FW1_PALOALTO
```

3.3 Creating a new Child SA

To configure the Windows Enterprise VPN Client for a Child SA, proceed as shown in the following screenshot:



Traffic selectors

VPN Client address: 10 . 10 . 10 . 1

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

□ Request configuration from the gateway

Cryptography

Encryption: AES CBC 256

Integrity: SHA2 384

Diffie-Hellman: DH14 (MODP 2048)

Extended Sequence Number: Auto

Lifetime

Child SA Lifetime: 1800 sec.

1. Uncheck the **Request configuration from the gateway** box and configure the **Traffic selectors**.
2. Under **Cryptography**, select the following values:
   - Encryption: AES GCM 256
   - Authentication: SHA2 384
   - Key Group: DH14
   - Extended Sequence Number: Auto

3.4 Saving the configuration

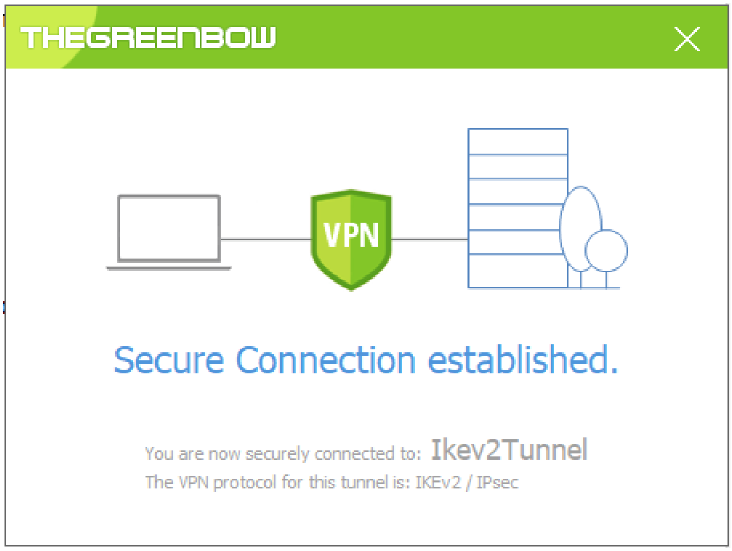
In the Windows Enterprise VPN Client, from the **Configuration** menu, select **Save** to account for all the changes you have made to your VPN configuration.

3.5 Opening the VPN connection

Once both the Palo Alto firewall and TheGreenBow Windows Enterprise VPN Client have been configured as described above, you are ready to open VPN connections.

Double-click your Child SA tunnel name or click **Open** in the **Connection Panel** to open a tunnel.

A green icon appears next to the Child SA when the connection is established successfully.



Secure Connection established.

You are now securely connected to: Ikev2Tunnel
The VPN protocol for this tunnel is: IKEv2 / IPsec

4 Troubleshooting

4.1 VPN Client

If the VPN connection cannot be established, check the Console log in TheGreenBow's VPN Client to determine whether any of the messages displayed match one of the messages described in the following sections.

4.1.1 NO_PROPOSAL_CHOSEN

If you encounter a `NO_PROPOSAL_CHOSEN` error, you might have incorrectly configured the Phase 1 [IKE Auth]. Make sure the encryption algorithms are the same at both ends of the VPN connection.

```
20XX0913 16:08:53:387 TIKEV2_Tunnel SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)]
[KE][VID][N(FRAGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR][N(NO_PROPOSAL_CHOSEN)]
```

4.1.2 AUTHENTICATION_FAILED

If you encounter an `AUTHENTICATION_FAILED` error, this means that the certificate sent by the VPN Client does not match what the firewall is expecting. Make sure the VPN Client's user certificate is correctly configured on the firewall.

```
20XX0913 16:15:22:032 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][N(AUTHENTICATION_FAILED)]
20XX0913 16:15:22:032 TIKEV2_Tunnel Remote endpoint sends error
AUTHENTICATION_FAILED
```

4.1.3 No user certificate available for the connection

Make sure the user certificate has been correctly imported to the VPN Client.

```
20XX0913 16:18:07:491 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_
IP)][CERTREQ][N(FRAGMENTATION_SUPPORTED)][N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:18:07:491 TIKEV2_Tunnel IKE SA I-SPI 8D4467C52C91C316 R-SPI
9DF0F0E4A91F8867
20XX0913 16:18:07:491 TIKEV2_Tunnel No user certificate available for the
connexion
20XX0913 16:18:07:491 TIKEV2_Tunnel Connection aborted.
```

4.1.4 Remote IDr rejected

The `Remote ID` type or value sent by the firewall does not match what the VPN Client is expecting (see **Protocol** tab). Configure the Remote ID type and value in the VPN Client according to the firewall's **Local ID**.

```
20180913 16:24:32:087 TIKEV2_Tunnel ID types do not match. Expecting
ID_RFC822_ADDR. Receiving ID_DER_ASN1_DN
20180913 16:24:32:087 TIKEV2_Tunnel Remote IDr rejected
```

4.1.5 FAILED_CP_REQUIRED

If you encounter a `FAILED_CP_REQUIRED` error, it means that the firewall is configured to use CP (Configuration Payload) mode, but not the VPN Client. In the Windows Enterprise VPN Client, go to **Traffic selectors** and enable **Request configuration from the gateway**.

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPT
ABLE)]
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error
FAILED_CP_REQUIRED
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a
configuration request from the client
```

5 Contact

5.1 Information

All the information on TheGreenBow products is available on our website: https://thegreenbow.com/.

5.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

5.3 Support

There are several pages related to the software's technical support on our website:

Online help

https://www.thegreenbow.com/en/support/online-support/

FAQ

https://www.thegreenbow.com/en/frequently-asked-questions/

Contact form

Technical support can be reached using the form on our website at the following address: https://www.thegreenbow.com/en/support/online-support/technical-support/.

Protect your connections
in any situation

14, rue Auber
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com