



## **PALO ALTO NETWORKS EDU-210**



### **Lab 11: Site-to-Site VPN**

**Document Version: 2020-06-26**

Copyright © 2020 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Theoretical Lab Topology.....	4
Lab Settings .....	5
11 Site-to-Site VPN.....	6
11.0 Load Lab Configuration.....	6
11.1 Configure the Tunnel Interface .....	9
11.2 Configure the IKE Gateway .....	11
11.3 Create an IPsec Crypto Profile.....	13
11.4 Configure the IPsec Tunnel.....	14
11.5 Test Connectivity .....	17

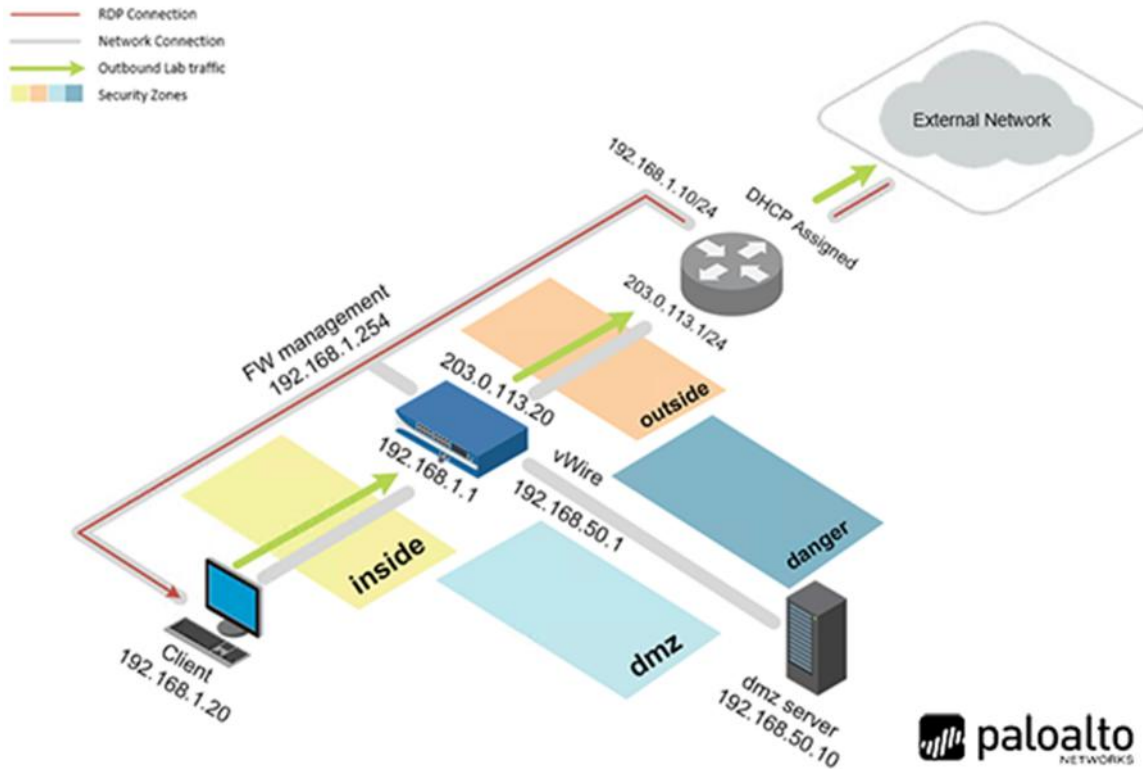
## Introduction

With the success of the Palo Alto Networks firewall at the corporate offices, the Board has approved the security team to establish Palo Alto Networks firewalls in our other locations and offices. To allow those branches to securely communicate with the corporate offices, we will implement site-to-site IPsec VPN tunnels and policies.

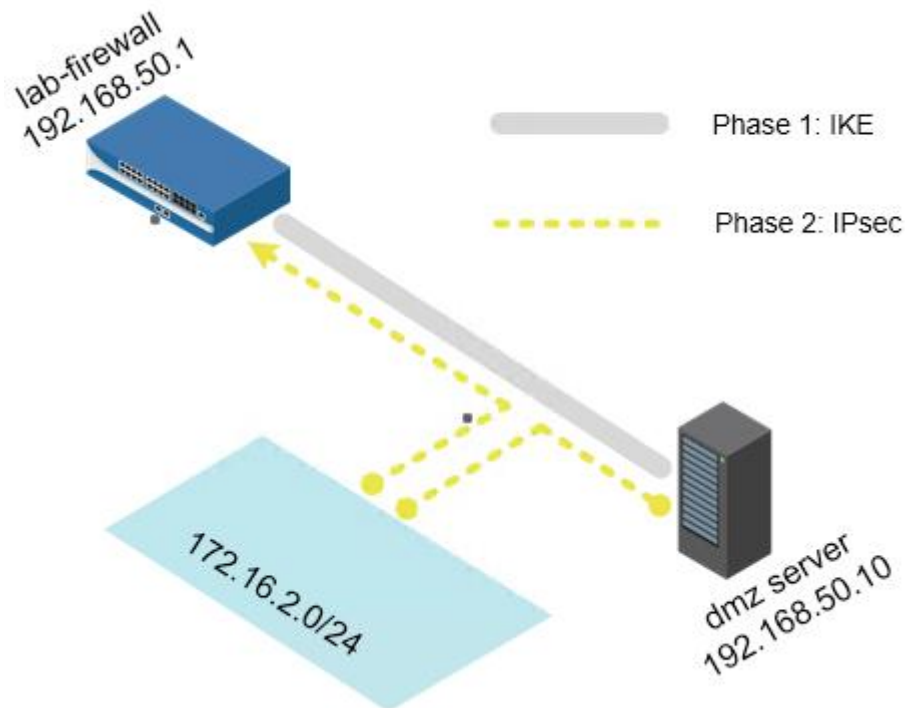
## Objectives

- ) Create and configure a tunnel interface to use in the site-to-site VPN connection
- ) Configure the IKE gateway and IKE Crypto Profile
- ) Configure the IPsec Crypto Profile and IPsec tunnel
- ) Test connectivity

## Lab Topology



## Theoretical Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
Firewall	192.168.1.254	admin	Train1ng\$

## 11 Site-to-Site VPN

### 11.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as **lab-user** using the password **Train1ng\$**.



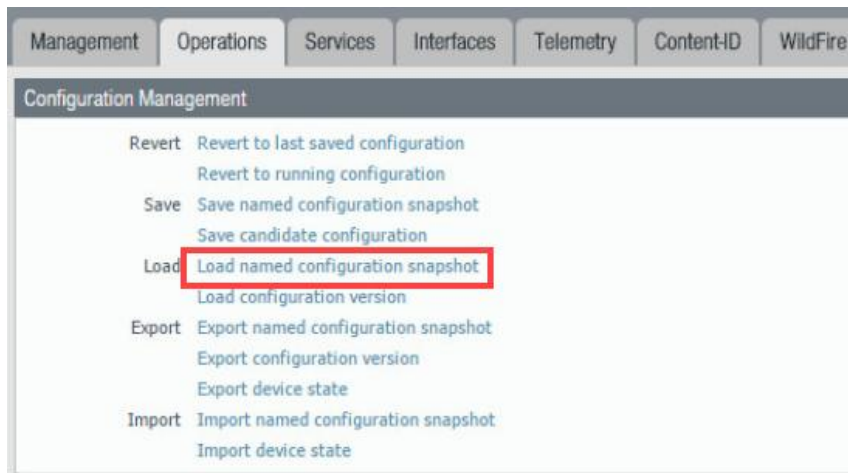
3. Launch the **Chromium Web Browser** and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	Train1ng\$

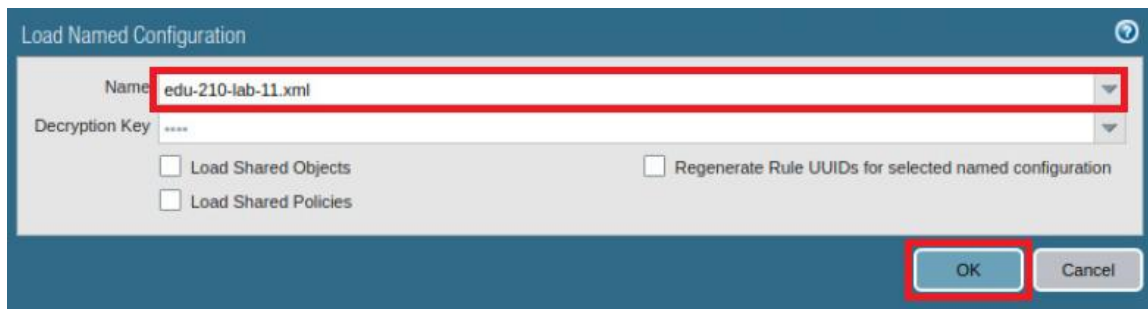
6. In the web interface, select **Device > Setup > Operations**.



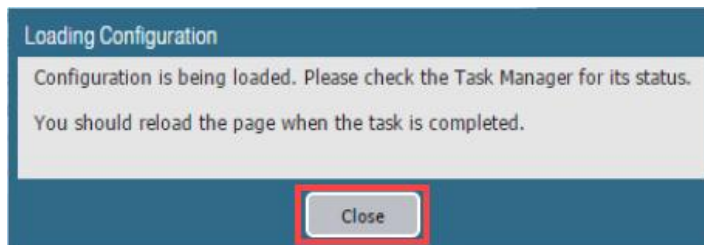
7. Click **Load named configuration snapshot**:



8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-011.xml**. Click **OK**.



9. Click **Close**.

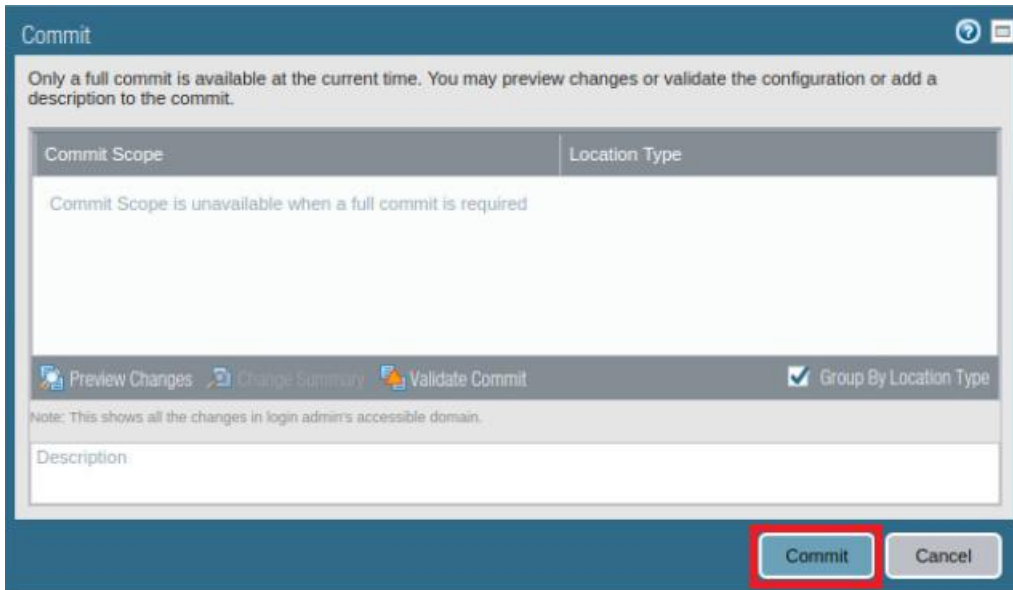


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

10. Click the **Commit** link at the top-right of the web interface.

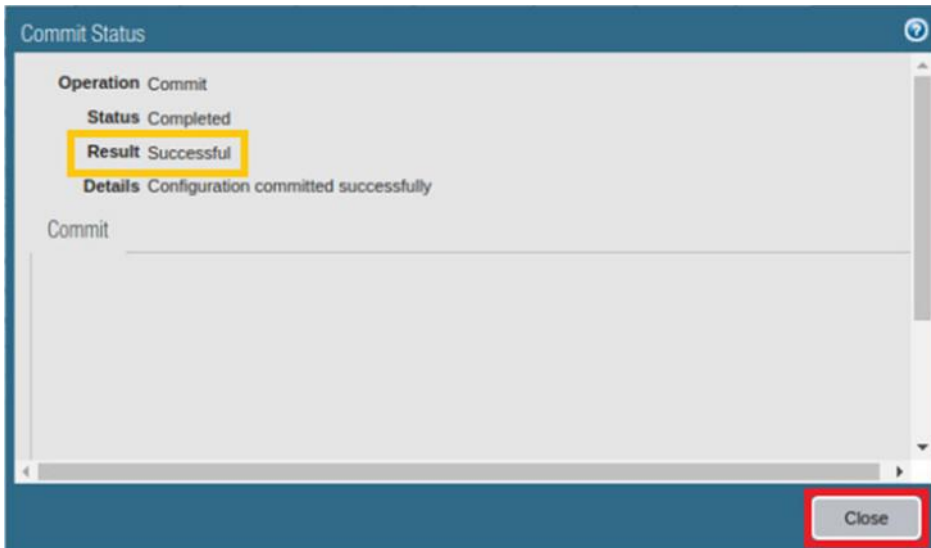


11. Click **Commit** and wait until the commit process is complete.



The image shows a 'Commit' dialog box with a blue header. Below the header, a message states: 'Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.' The dialog is divided into two main sections: 'Commit Scope' and 'Location Type'. The 'Commit Scope' section contains a message: 'Commit Scope is unavailable when a full commit is required'. Below these sections is a toolbar with three icons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of the toolbar is a checkbox labeled 'Group By Location Type' which is checked. Below the toolbar is a text area labeled 'Description'. At the bottom right of the dialog are two buttons: 'Commit' and 'Cancel'. The 'Commit' button is highlighted with a red rectangle.

12. Once completed successfully, click **Close** to continue.



The image shows a 'Commit Status' dialog box with a blue header. Below the header, the 'Operation' is listed as 'Commit'. The 'Status' is 'Completed'. The 'Result' is 'Successful', which is highlighted with a yellow rectangle. The 'Details' section shows 'Configuration committed successfully'. Below this is a large text area labeled 'Commit'. At the bottom right of the dialog is a button labeled 'Close', which is highlighted with a red rectangle.

13. Leave the firewall web interface open to continue with the next task.



## 11.1 Configure the Tunnel Interface

1. In the web interface, navigate to **Network > Interfaces > Tunnel**.

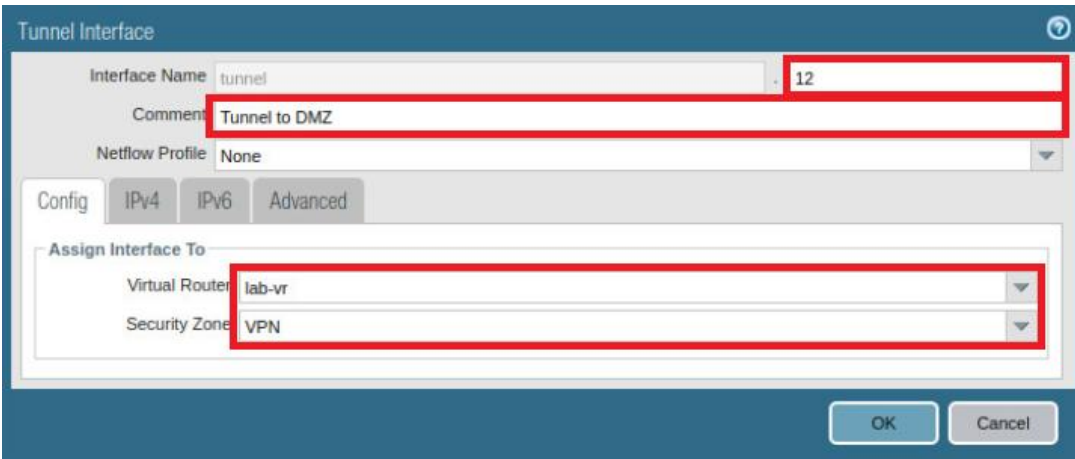


2. Click **Add** to configure a tunnel interface.



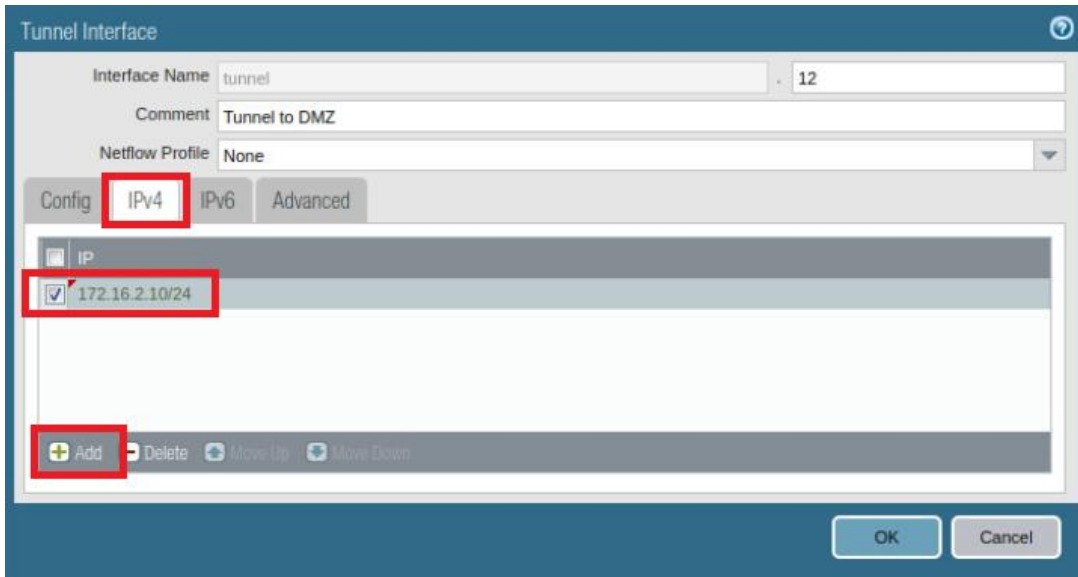
3. In the *Tunnel Interface* window, configure the following.

Parameter	Value
Interface Name	Type 12
Comment	Type Tunnel1 to DMZ
Virtual Router	Select <b>lab-vr</b> from the dropdown list
Security Zone	Create and assign a new Layer 3 zone named <b>VPN</b>



4. In the *Tunnel Interface* window, click the **IPv4** tab and configure the following.

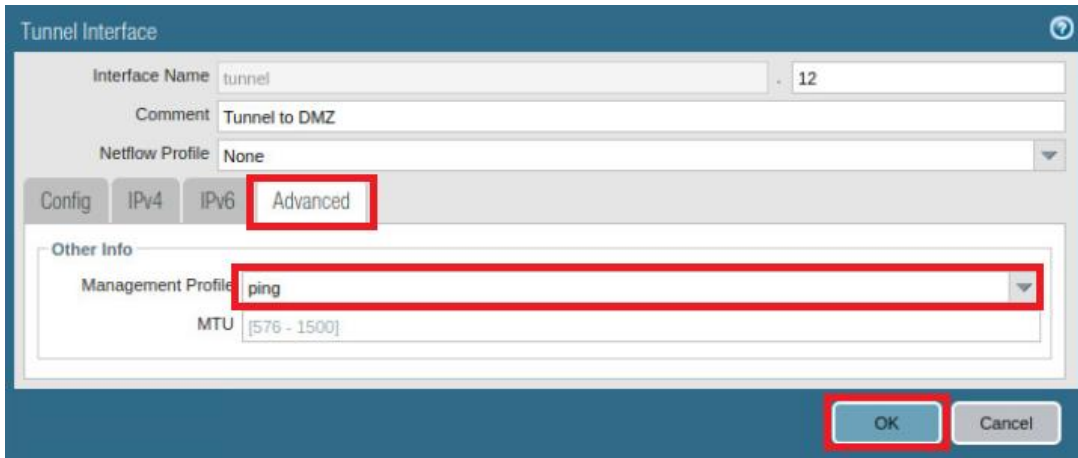
Parameter	Value
IP	Click <b>Add</b> and type <b>172.16.2.10/24</b>



The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' is 'tunnel' and the 'Comment' is 'Tunnel to DMZ'. The 'Netflow Profile' is set to 'None'. The 'IPv4' tab is selected. In the 'IP' section, the address '172.16.2.10/24' is listed with a checkmark. The 'Add' button is highlighted with a red box.

5. In the *Tunnel Interface* window, click the **Advanced** tab and configure the following. Once finished, click **OK**.

Parameter	Value
Management Profile	Select <b>ping</b> from the dropdown list

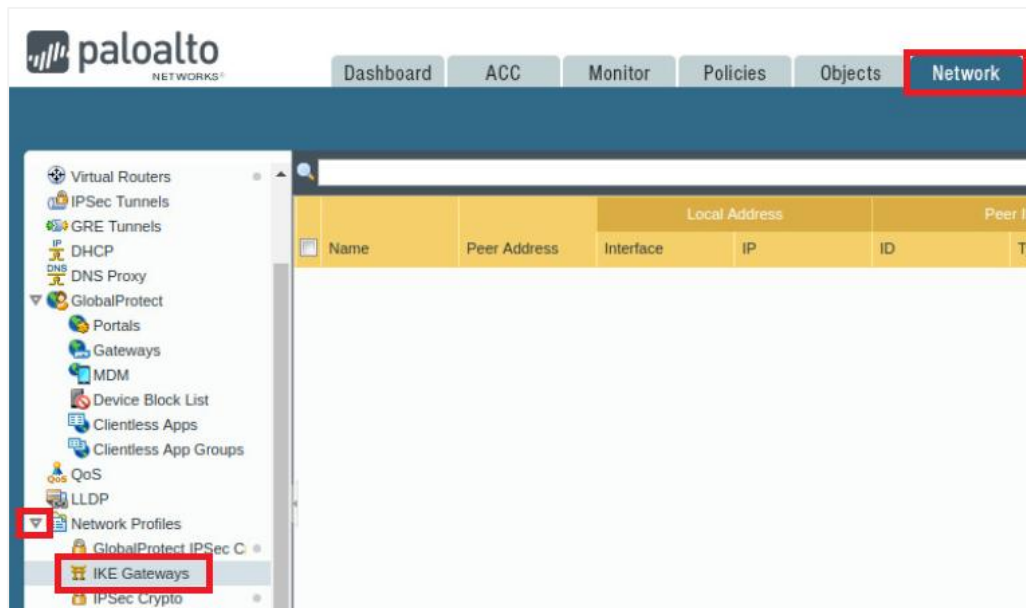


The screenshot shows the 'Tunnel Interface' configuration window with the 'Advanced' tab selected. The 'Management Profile' dropdown is set to 'ping'. The 'OK' button is highlighted with a red box.

6. Leave the firewall web interface open to continue with the next task.

## 11.2 Configure the IKE Gateway

1. In the web interface, navigate to **Network > Network Profiles > IKE Gateways**.

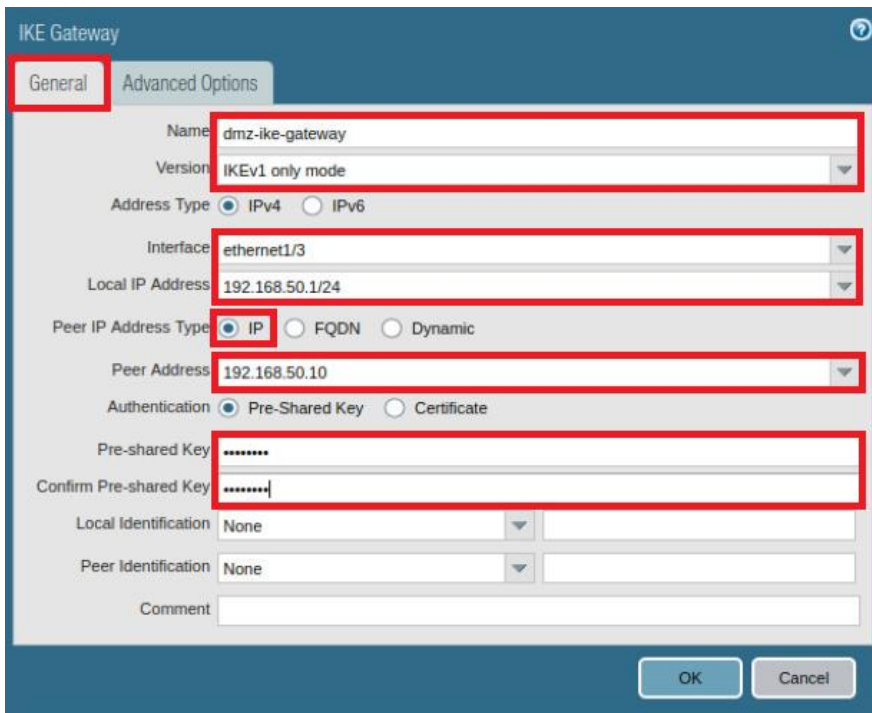


2. Click **Add** to create the IKE gateway.



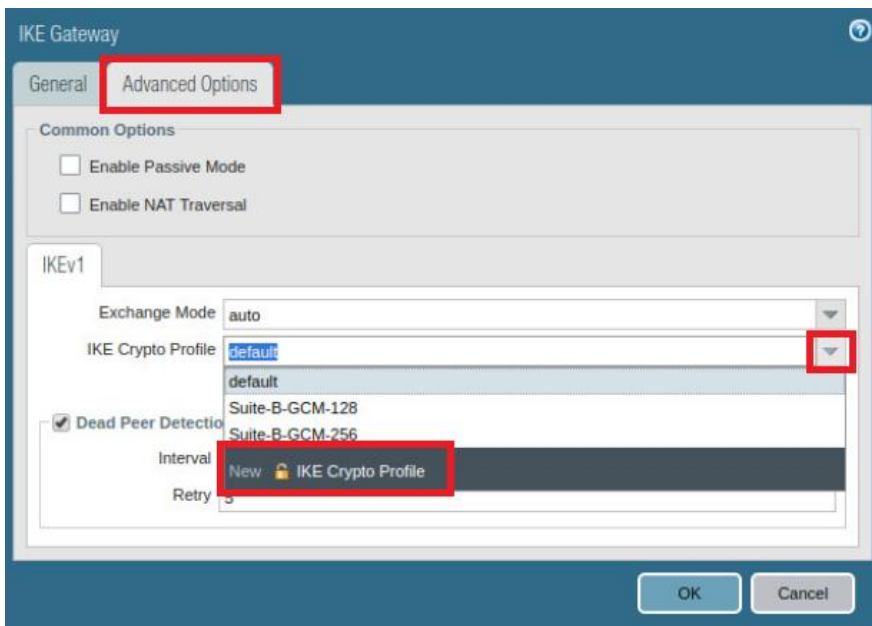
3. In the **General** tab of *IKE Gateway* window, configure the following.

Parameter	Value
Name	Type <b>dmz-ike-gateway</b>
Version	Verify that <b>IKEv1 only mode</b> is selected
Interface	Select <b>ethernet1/3</b> from the dropdown list
Local IP Address	Select <b>192.168.50.1/24</b> from the dropdown list
Peer IP Address Type	Verify that the <b>IP</b> radio button is selected
Peer Address	Type <b>192.168.50.10</b>
Pre-shared Key	Type <b>pa1oa1to</b>



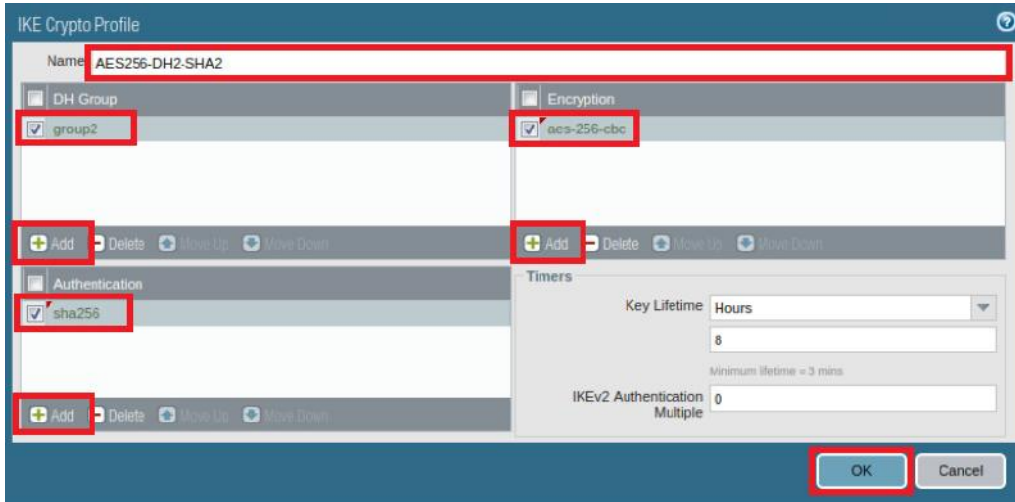
4. In the *IKE Gateway* window, click the **Advanced Options** tab. On the *IKEv1* subtab, configure the following.

Parameter	Value
IKE Crypto Profile	Select <b>New IKE Crypto Profile</b>



- Notice the *IKE Crypto Profile* window appears. Configure the following. Once finished, click **OK**.

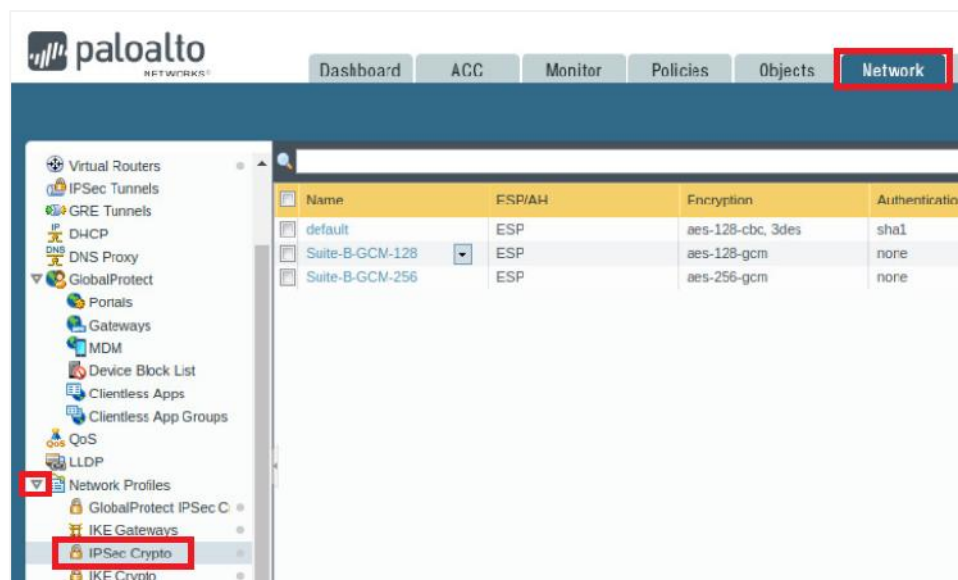
Parameter	Value
Name	Type AES256-DH2-SHA2
DH Group	Click <b>Add</b> and select <b>Group 2</b> from the dropdown list
Authentication	Click <b>Add</b> and select <b>sha256</b> from the dropdown list
Encryption	Click <b>Add</b> and select <b>aes-256-cbc</b> from the dropdown list



- Back on the *IKE Gateway* window, click **OK**.
- Leave the firewall web interface open to continue with the next task

### 11.3 Create an IPSec Crypto Profile

- In the web interface, navigate to **Network > Network Profiles > IPSec Crypto**.

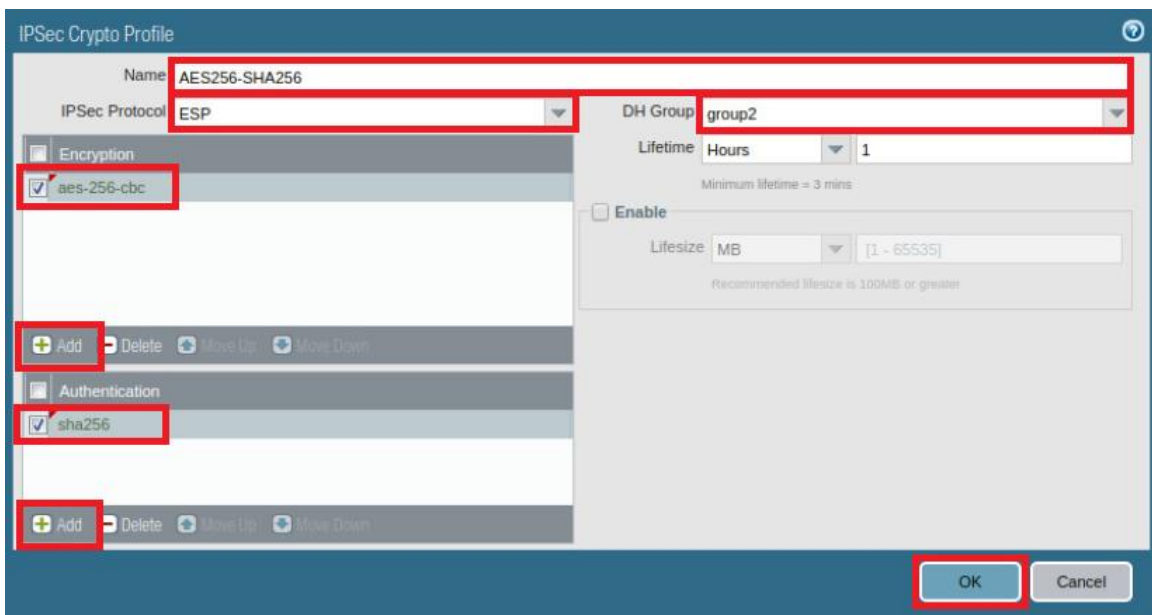


- Click **Add** to open the *IPSec Crypto Profile* configuration window.



- In the *IPSec Crypto Profile* window, configure the following. Once finished, click **OK**.

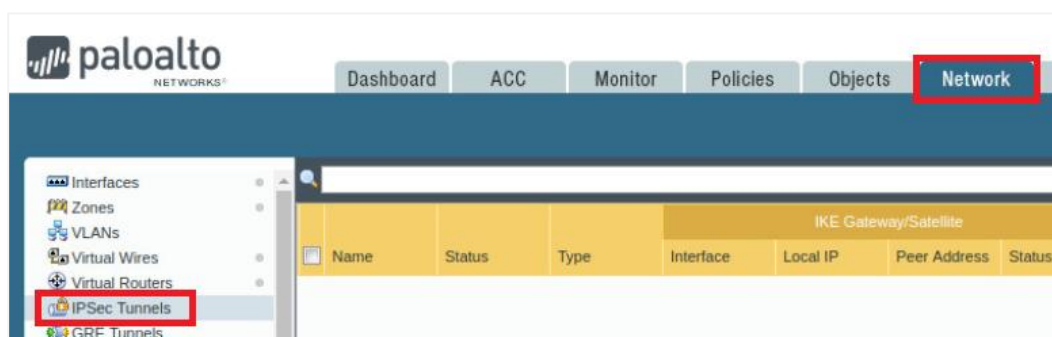
Parameter	Value
Name	Type AES256-SHA256
IPSec Protocol	Verify that <b>ESP</b> is selected
Encryption	Click <b>Add</b> and select <b>aes-256-cbc</b> from the dropdown list
Authentication	Click <b>Add</b> and select <b>sha256</b> from the dropdown list
DH Groups	Verify that <b>group2</b> is selected



- Leave the firewall web interface open to continue with the next task.

## 11.4 Configure the IPSec Tunnel

- In the web interface, navigate to **Network > IPSec Tunnels**.

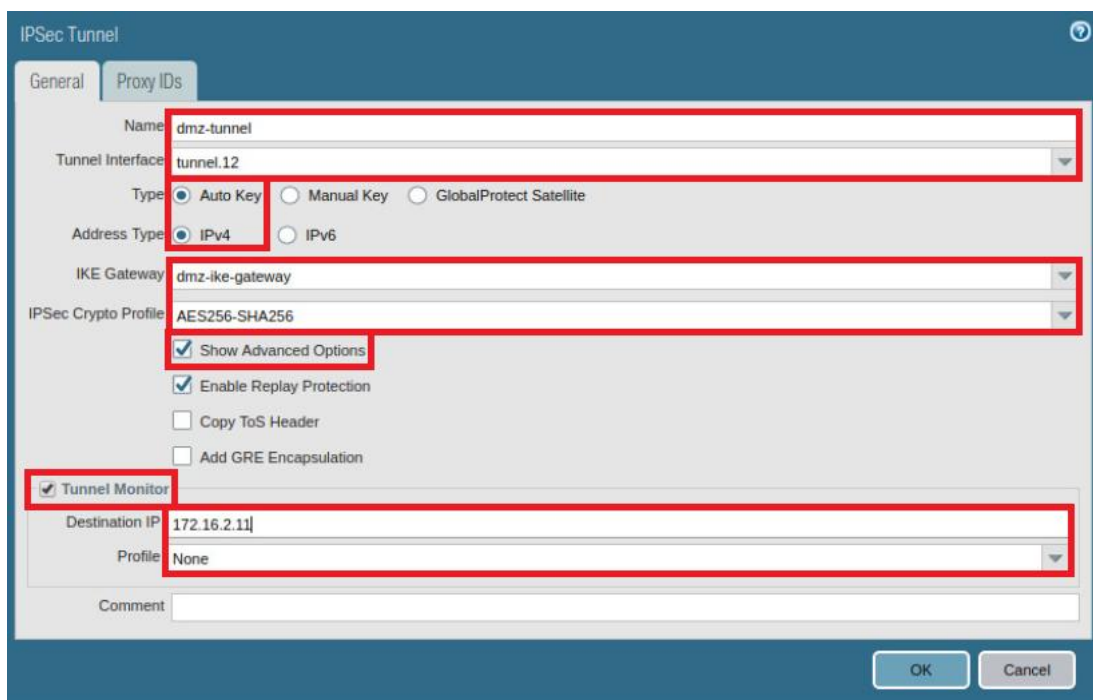


- Click **Add** to define the IPsec tunnel.



- In the *IPSec Tunnel* window, while on the *General* tab, configure the following.

Parameter	Value
Name	Type <b>dmz-tunnel1</b>
Tunnel Interface	Select <b>tunnel.12</b> from the dropdown list
Type	Verify that the <b>Auto Key</b> radio button is selected
Address Type	Verify that the <b>IPv4</b> radio button is selected
IKE Gateway	Select <b>dmz-ike-gateway</b> from the dropdown list
IPSec Crypto Profile	Select <b>AES256-SHA256</b> from the dropdown list
Show Advanced Options	Select the checkbox
Tunnel Monitor	Select the checkbox
Destination IP	Type <b>172.16.2.11</b>
Profile	Verify that <b>None</b> is selected



IPSec Tunnel

General Proxy IDs

Name: dmz-tunnel

Tunnel Interface: tunnel.12

Type: ☒ Auto Key ☐ Manual Key ☐ GlobalProtect Satellite

Address Type: ☒ IPv4 ☐ IPv6

IKE Gateway: dmz-ike-gateway

IPSec Crypto Profile: AES256-SHA256

☒ Show Advanced Options

☒ Enable Replay Protection

☐ Copy ToS Header

☐ Add GRE Encapsulation

☒ Tunnel Monitor

Destination IP: 172.16.2.11

Profile: None

Comment:

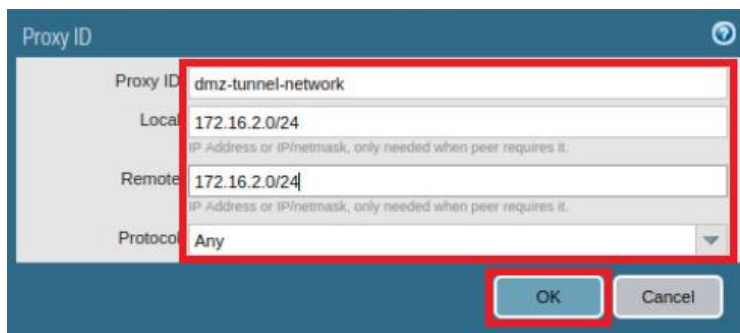
OK Cancel

- In the *IPSec Tunnel* window, click the **Proxy IDs** tab and then click **Add**.



- In the *Proxy ID* window, configure the following. Once finished, click **OK**.

Parameter	Value
Proxy ID	Type <b>dmz-tunnel-network</b>
Local	Type <b>172.16.2.0/24</b>
Remote	Type <b>172.16.2.0/24</b>
Protocol	Verify that <b>Any</b> is selected



- Back on the *IPSec Tunnel* window, click **OK**.
- Verify that a new IPSec tunnel should appear in the list.

Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface				
			Interface	Local IP	Peer Address	Status	Interface	Virtual Router	Virtual System	Secu... Zone	Sta...
dmz-tunnel	 Tunnel Info	Auto Key	ethernet1/3	192.168.50.1/24	192.168.50.10	 IKE Info	tunnel.12	lab-vr (Show Routes)	vsys1	VPN	

- Commit** all changes.
- Leave the firewall web interface open to continue with the next task.

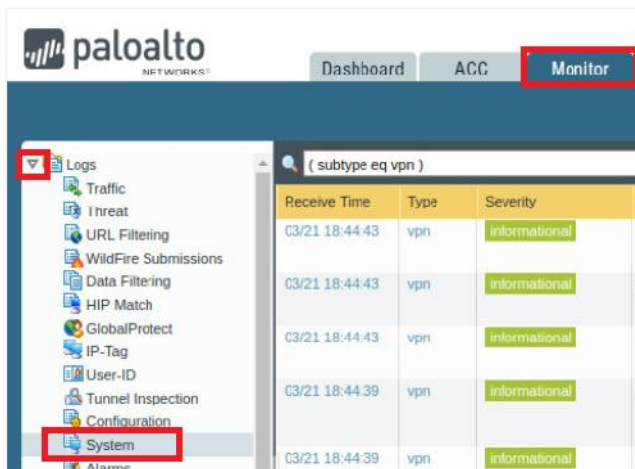


## 11.5 Test Connectivity

- After committing changes, refresh the *IPSec Tunnels* page. The *Status* column indicator should now be green, which means that the VPN tunnel is connected.

Name	Status	Type	IKE Gateway/Satellite			Status	Tunnel Interface				
			Interface	Local IP	Peer Address		Interface	Virtual Router	Virtual System	S...	Status
dmz-tunnel	 Tunnel Info	Auto Key	ethernet1/3	192.168.50.1/24	192.168.50.10	 IKE Info	tunnel.12	lab-vr (Show Routes)	vsys1	V...	

- Navigate to **Monitor > Logs > System**.



- Review the VPN log entries.

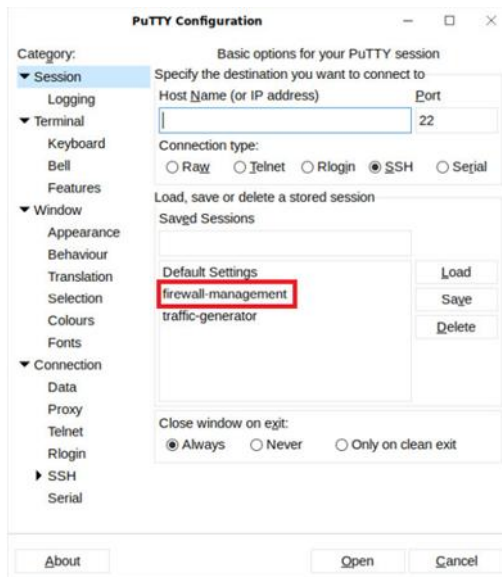
Receive Time	Type	Severity	Event	Object	Description
03/21 18:45:44	vpn	informational	ipsec-key-install	dmz-tunnel:dmz-tunnel-network	IPSec key installed. Installed SA: 192.168.50.1[500]-192.168.50.10[500] SPI:0xDDF1DD46/0x70D709CA lifetime 3600 Sec lifetime unlimited.
03/21 18:45:44	vpn	informational	ike-nego-p2-succ	dmz-tunnel:dmz-tunnel-network	IKE phase-2 negotiation is succeeded as initiator, quick mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x745A8B60, SPI:0xDDF1DD46/0x70D709CA.
03/21 18:45:44	vpn	informational	ike-nego-p2-start	dmz-tunnel:dmz-tunnel-network	IKE phase-2 negotiation is started as initiator, quick mode. Initiated SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x745A8B60.
03/21 18:44:43	vpn	informational	ike-nego-p1-delete	dmz-ike-gateway	IKE phase-1 SA is deleted SA: 192.168.50.1[500]-192.168.50.10[500] cookie:3b455879489d4024:f55a15eacb980429.
03/21 18:44:43	vpn	informational	ike-send-p1-delete	dmz-ike-gateway	IKE protocol phase-1 SA delete message sent to peer, cookie:3b455879489d4024:f55a15eacb980429.
03/21 18:44:43	vpn	informational	ike-nego-p1-expire	dmz-ike-gateway	IKE phase-1 SA is expired SA: 192.168.50.1[500]-192.168.50.10[500] cookie:3b455879489d4024:f55a15eacb980429.
03/21 18:44:39	vpn	informational	ipsec-key-install	dmz-tunnel:dmz-tunnel-network	IPSec key installed. Installed SA: 192.168.50.1[500]-192.168.50.10[500] SPI:0xCD34CC88/0xF4BDBA9D lifetime 3600 Sec lifetime unlimited.
03/21 18:44:39	vpn	informational	ike-nego-p2-succ	dmz-tunnel:dmz-tunnel-network	IKE phase-2 negotiation is succeeded as initiator, quick mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x86BB9A8D, SPI:0xCD34CC88/0xF4BDBA9D.



If you see messages related to “*pre-shared key mismatch*”, go back to your **IKE Gateways** web interface under **Network Profiles**, click on **dmz-ike-gateway**, and re-type `paltoalto` in both *Pre-shared Key* text fields. Click **OK** and **commit** all changes.



4. On the Windows desktop, double-click the **PuTTY** icon.
5. In the *PuTTY Configuration* window, double-click **firewall-management**.



6. When prompted for credentials, log in as **admin** with the password **Train1ng\$**.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 27 21:11:02 2020

Number of failed attempts since last successful login: 0

admin@firewall-a> █
```

7. After the VPN tunnel is connected, type the following CLI commands and observe the output.

```
admin@firewall-a> show vpn ike-sa
```

```
IKEv1 phase-1 SAs
GwID/client IP  Peer-Address      Gateway Name      Role Mode Algorithm      Established      Expiration      V  ST  Xt  Phase2
-----
4              192.168.50.10      dmz-ike-gateway   Resp Main PSK/ DH2/A256/SHA256  Mar.21 18:43:43  Mar.22 02:43:43  v1 13 1  6

Show IKEv1 IKE SA: Total 1 gateways found, 1 ike sa found.

IKEv1 phase-2 SAs
Gateway Name      TnID      Tunnel      GwID/IP      Role Algorithm      SPI(in)  SPI(out)  MsgID      ST  Xt
-----
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 9D74DC2C 1173FEEC 5CDDA8B5 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 E69F1865 65918FB8 2C09ED40 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 FE182F90 E82B44A7 AADD6782 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 DDF1DD46 70D709CA 745A8B60 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 CD34CC88 F4BDB49D 86BB9A8D 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Resp ESP/ DH2/tun1/SHA2 9DC4CC08 A6964930 B8F78551 9  1
dmz-ike-gateway   7         dmz-tunnel:dmz-tunnel- 4      Init ESP/ DH2/tun1/SHA2 D71B3714 8BFEAAB6 9A19D69A 9  1

Show IKEv1 phase2 SA: Total 1 gateways found, 7 ike sa found.

There is no IKEv2 SA found.
```

```
admin@firewall-a> show vpn ipsec-sa tunnel dmz-tunnel:dmz-tunnel-network
```

```
admin@firewall-a> show vpn ipsec-sa tunnel dmz-tunnel:dmz-tunnel-network

GwID/client IP  TnID  Peer-Address      Tunnel(Gateway)      Algorithm      SPI(in)  SPI(out)  life(Sec/KB)      remain-time(Sec)
-----
4              7     192.168.50.10      dmz-tunnel:dmz-tunnel-network(dmz-ike-gateway)  ESP/A256/SHA256  8B3F9CBA 41D0A2CE 3600/Unlimited      3582

Show IPsec SA: Total 1 tunnels found, 1 ipsec sa found.
```

```
admin@firewall-a> show vpn flow name dmz-tunnel:dmz-tunnel-network
```

```
admin@firewall-a> show vpn flow name dmz-tunnel:dmz-tunnel-network

tunnel  dmz-tunnel:dmz-tunnel-network
id:      7
type:    IPSec
gateway id: 4
local ip: 192.168.50.1
peer ip:  192.168.50.10
inner interface: tunnel.12
outer interface: ethernet1/3
state:    active
session:  1122
tunnel mtu: 1424
soft lifetime: 3494
hard lifetime: 3600
lifetime remain: 3535 sec
lifesize remain: N/A
latest rekey: 6 seconds ago
monitor:   on
  monitor status: down
  monitor dest: 172.16.2.11
  monitor interval: 3 seconds
  monitor threshold: 5 probe losses
  monitor bitmap: 00000
  monitor packets sent: 171
  monitor packets rcv: 0
  monitor packets seen: 0
  monitor packets reply: 0
en/decap context: 9
local spi: 8B3F9CBA
remote spi: 41D0A2CE
key type:  auto key
protocol:  ESP
auth algorithm: SHA256
enc algorithm: AES256
```

```
admin@firewall-a> show running tunnel flow
```

```
admin@firewall-a> show running tunnel flow

total tunnels configured:          1
filter - type any, state any

total IPSec tunnel configured:    1
total IPSec tunnel shown:         1

id   name                               state  monitor local-ip           peer-ip           tunnel-i/f
--   ---                               -----
7    dmz-tunnel;dmz-tunnel-network active  down   192.168.50.1       192.168.50.10    tunnel.12

total SSL-VPN tunnel configured:  0
total SSL-VPN tunnel shown:       0

total GlobalProtect-Gateway tunnel shown:  0

total GlobalProtect-site-to-site tunnel shown:  0
```

8. The lab is now complete; you may end the reservation.