# PALO ALTO NETWORKS EDU-210

# Lab 11: Site-to-Site VPN

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

# Contents



## Introduction

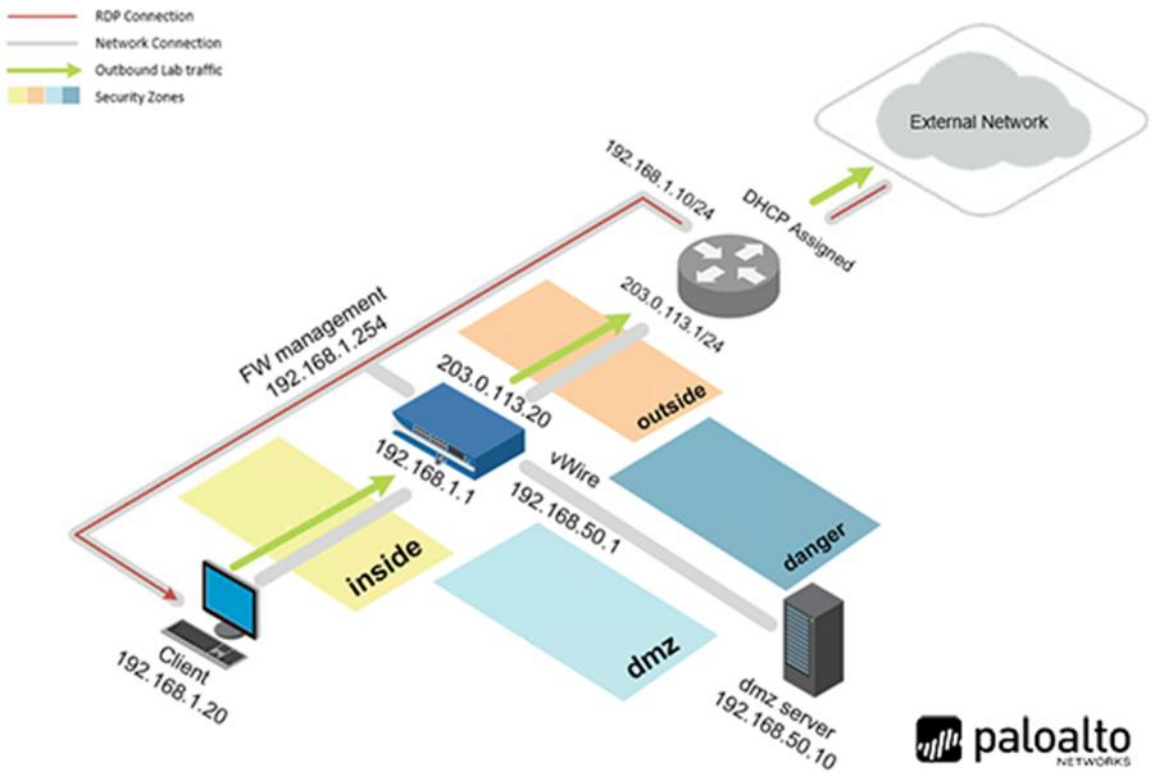
With the success of the Palo Alto Networks firewall at the corporate offices, the Board has approved the security team to establish Palo Alto Networks firewalls in our other locations and offices. To allow those branches to securely communicate with the corporate offices, we will implement site-to-site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

## Objectives

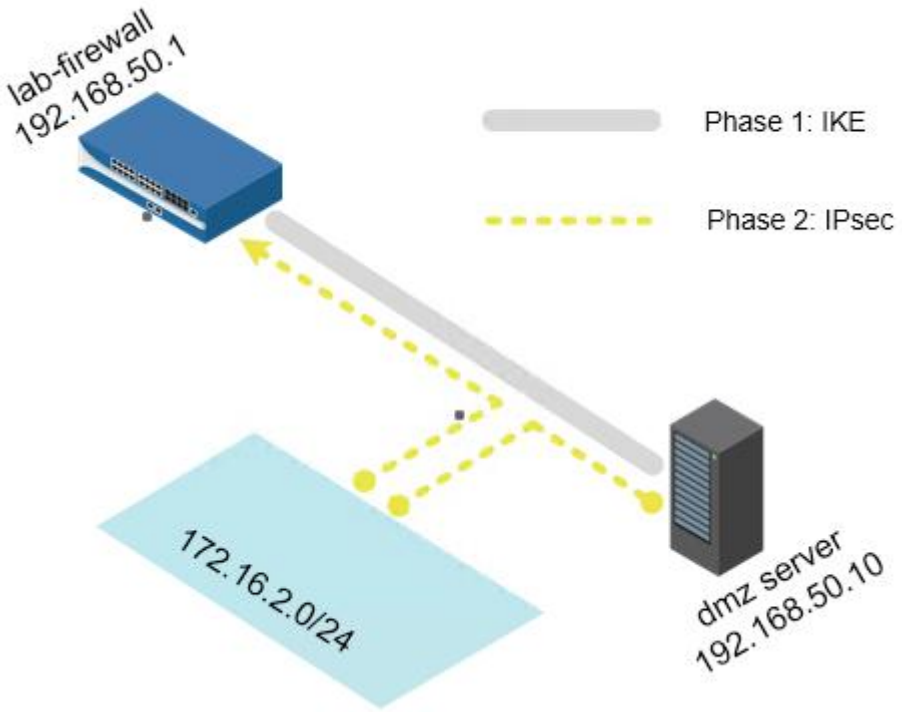
- Create and configure a tunnel interface to use in the site-to-site VPN connection
- Configure the IKE gateway and IKE Crypto Profile
- Configure the IPSec Crypto Profile and IPsec tunnel
- Test connectivity

## 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$`.

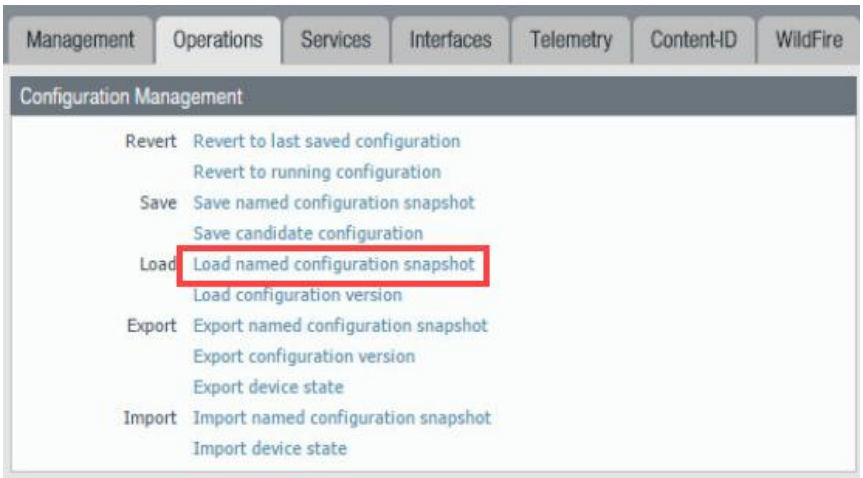

3. Launch the **Chromium Web Browser** and connect to `https://192.168.1.254.`
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

| Parameter | Value |
|---|---|
| Name | `admin` |
| Password | `Train1ng$` |

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

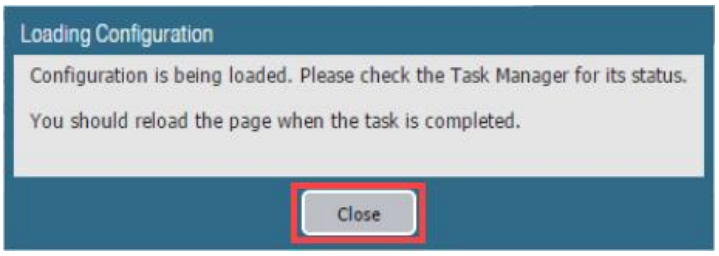

  

7. Click **Load named configuration snapshot**:




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


9. Click **Close**.

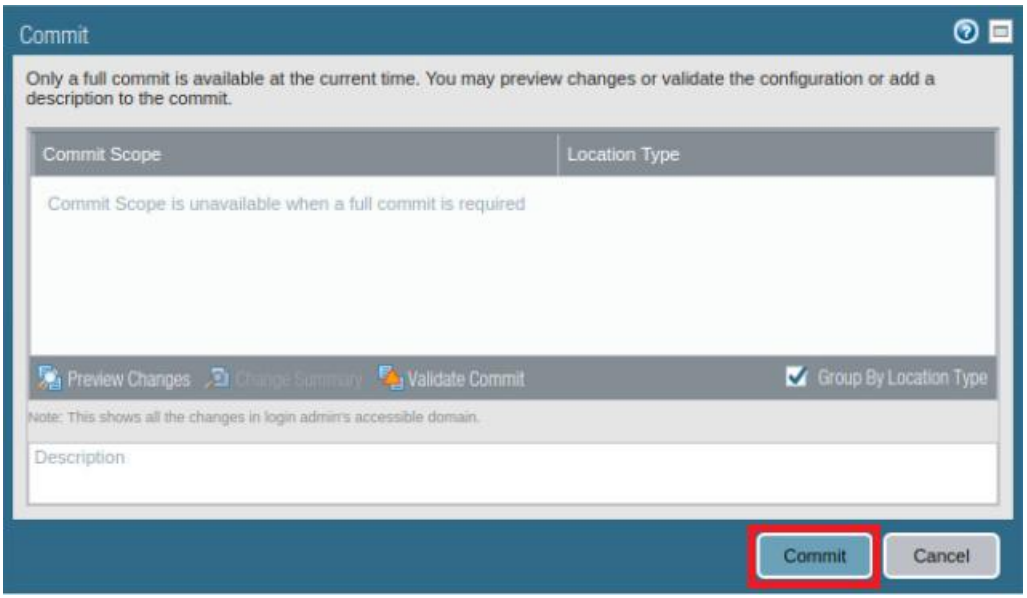



The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

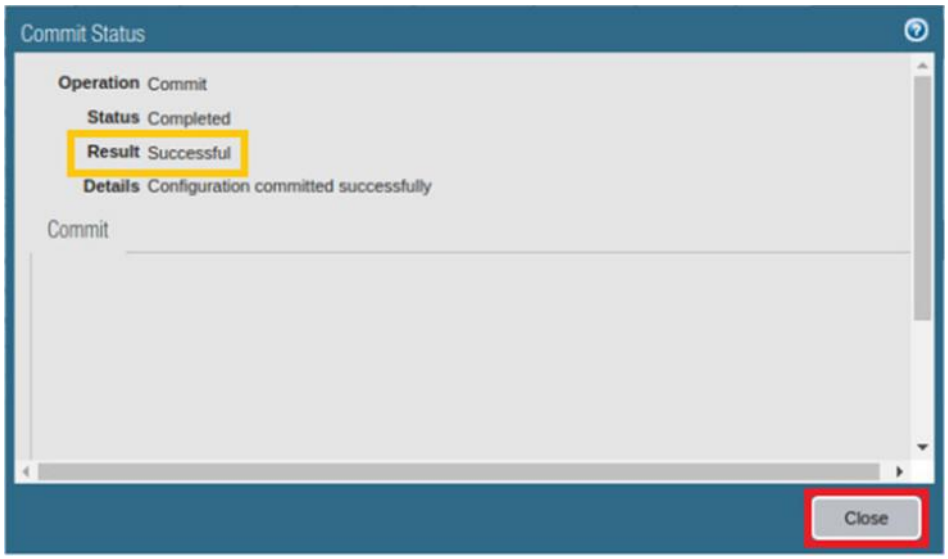
10. Click the **Commit** link at the top-right of the web interface.

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




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




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

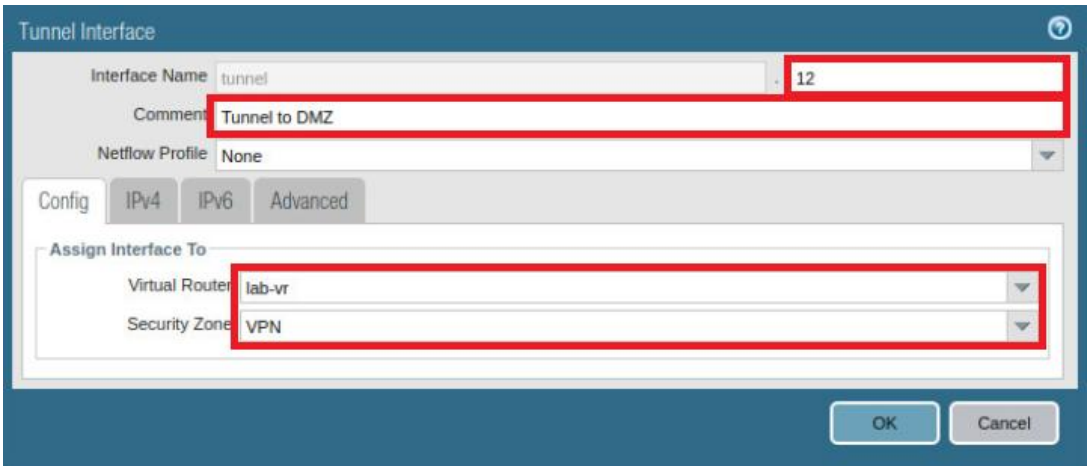
## 11.1 Configure the Tunnel Interface

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.

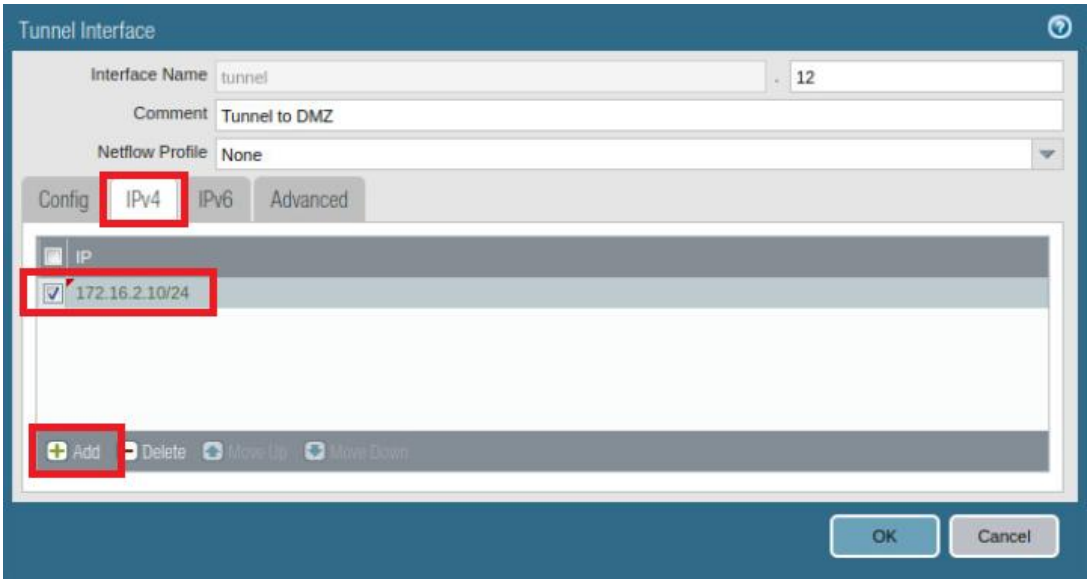
| Parameter | Value |
|---|---|
| Interface Name | Type **12** |
| Comment | Type `Tunnel to DMZ` |
| Virtual Router | Select **lab-vr** from the dropdown list |
| Security Zone | Create and assign a new Layer 3 zone named **VPN** |



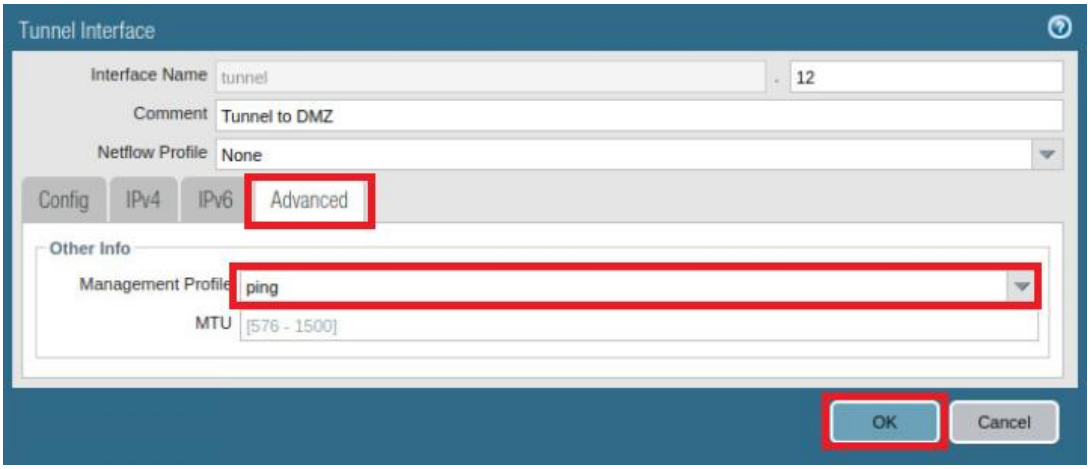
4. In the *Tunnel Interface* window, click the **IPv4** tab and configure the following.

| Parameter | Value |
|---|---|
| IP | Click **Add** and type `172.16.2.10/24` |




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

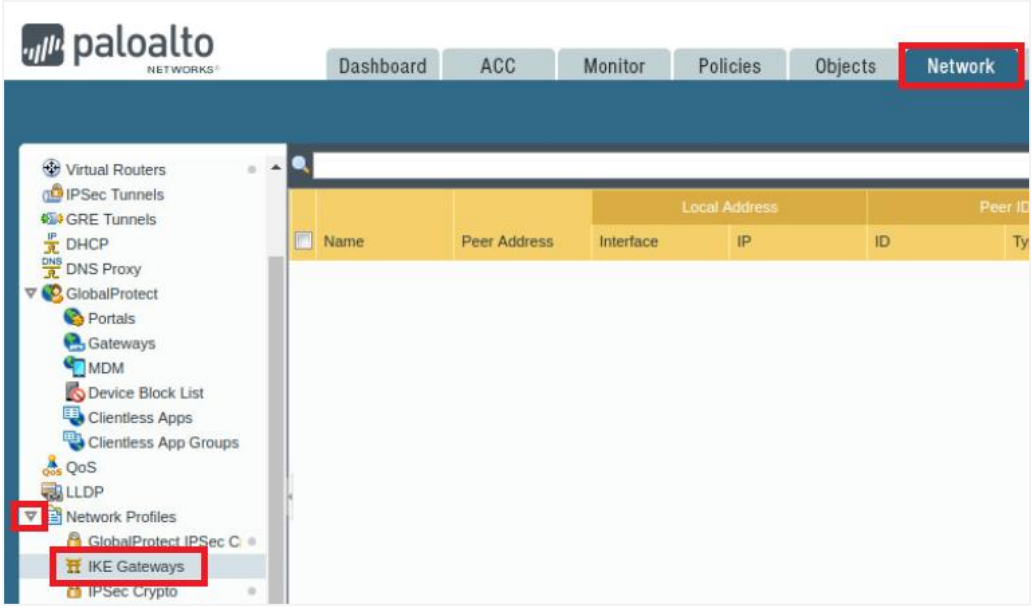
| Parameter | Value |
|---|---|
| Management Profile | Select **ping** from the dropdown list |



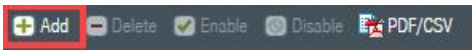

6. Leave the firewall web interface open to continue with the next task.

## 11.2 Configure the IKE Gateway

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



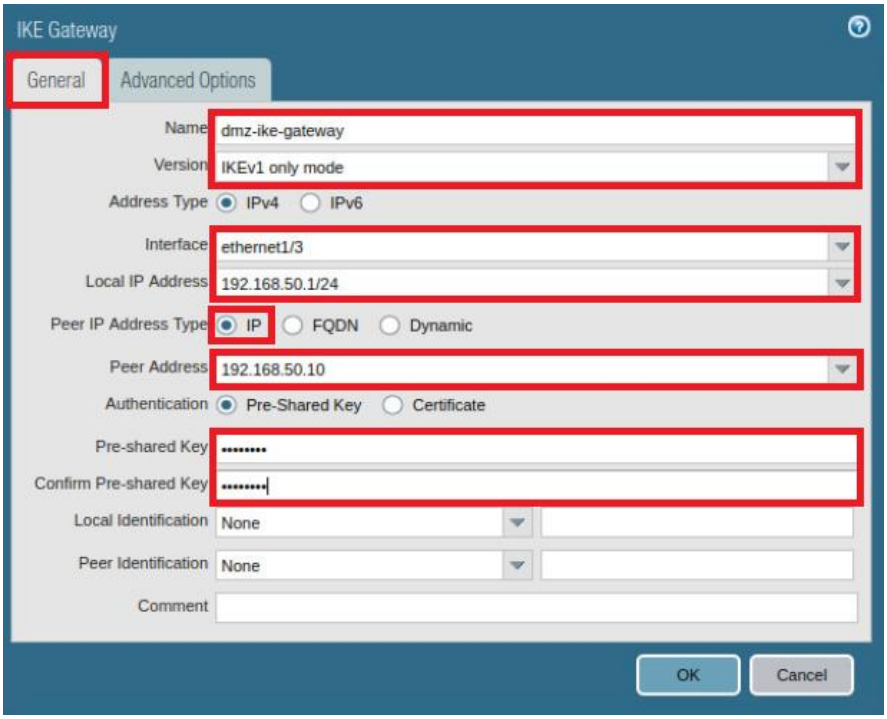

2. Click **Add** to create the IKE gateway.




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

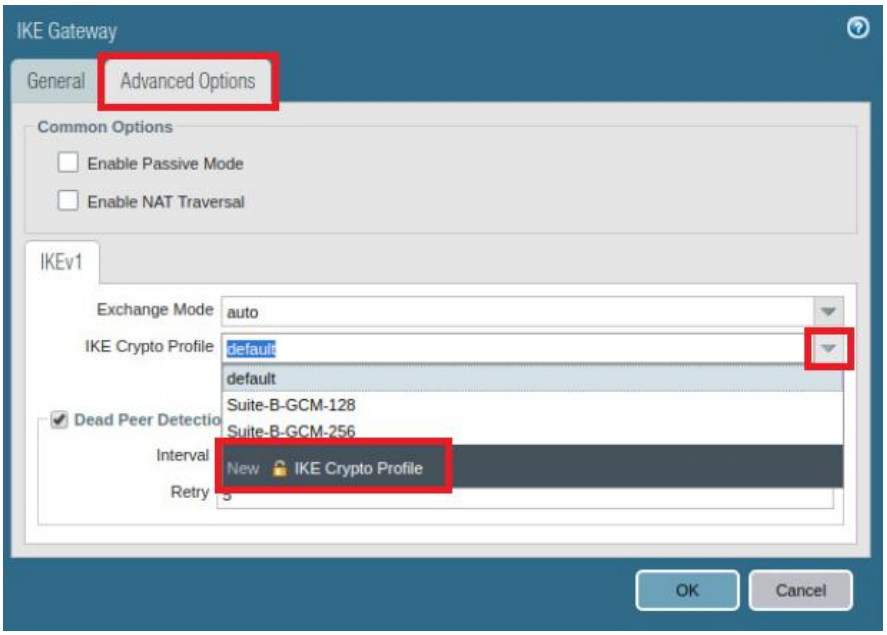
| Parameter | Value |
|---|---|
| Name | Type `dmz-ike-gateway` |
| Version | Verify that **IKEv1 only mode** is selected |
| Interface | Select **ethernet1/3** from the dropdown list |
| Local IP Address | Select **192.168.50.1/24** from the dropdown list |
| Peer IP Address Type | Verify that the **IP**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




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

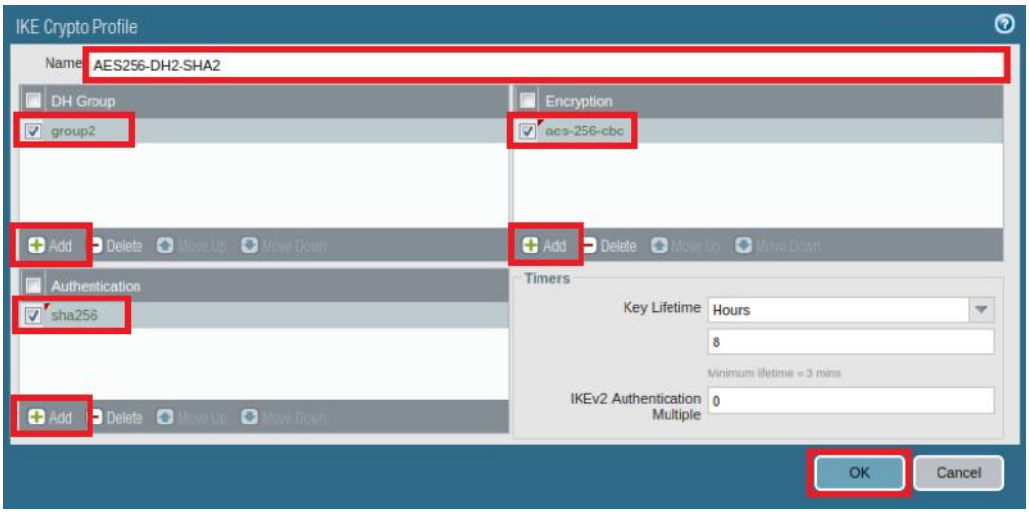
| Parameter | Value |
|---|---|
| IKE Crypto Profile | Select **New IKE Crypto Profile** |



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

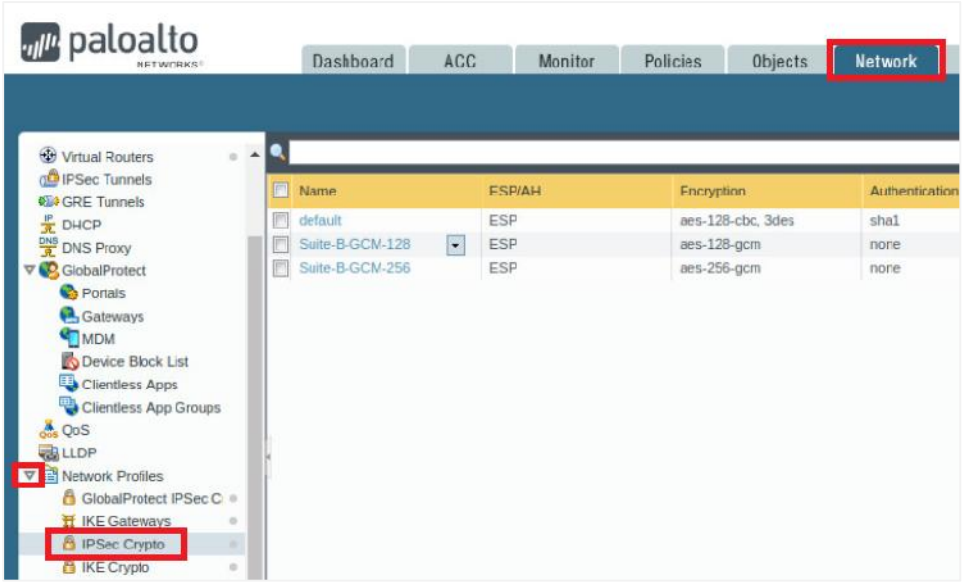
| Parameter | Value |
|---|---|
| Name | Type **AES256-DH2-SHA2** |
| DH Group | Click **Add** and select **Group 2** from the dropdown list |
| Authentication | Click **Add** and select **sha256** from the dropdown list |
| Encryption | Click **Add** and select **aes-256-cbc** from the dropdown list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




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

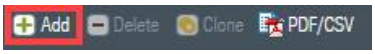
## 11.3 Create an IPSec Crypto Profile

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



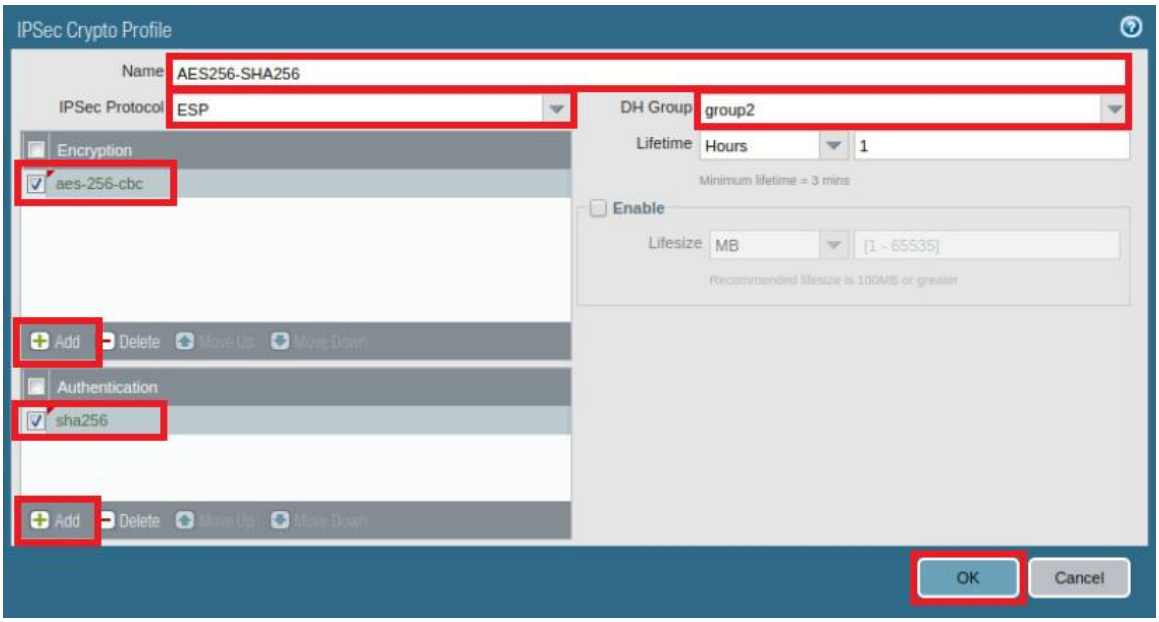

  

2. Click **Add** to open the *IPSec Crypto Profile* configuration window.




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

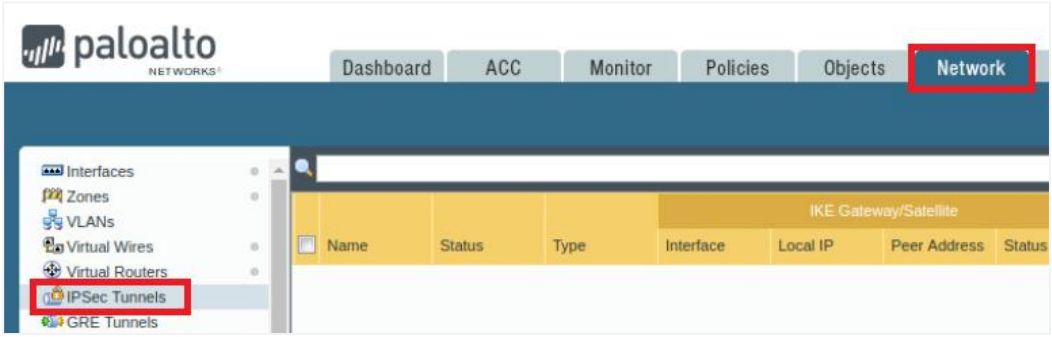
| Parameter | Value |
|---|---|
| Name | Type **AES256-SHA256** |
| IPSec Protocol | Verify that **ESP** is selected |
| Encryption | Click **Add** and select **aes-256-cbc** from the dropdown list |
| Authentication | Click **Add** and select **sha256** from the dropdown list |
| DH Groups | Verify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




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

## 11.4 Configure the IPsec Tunnel

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

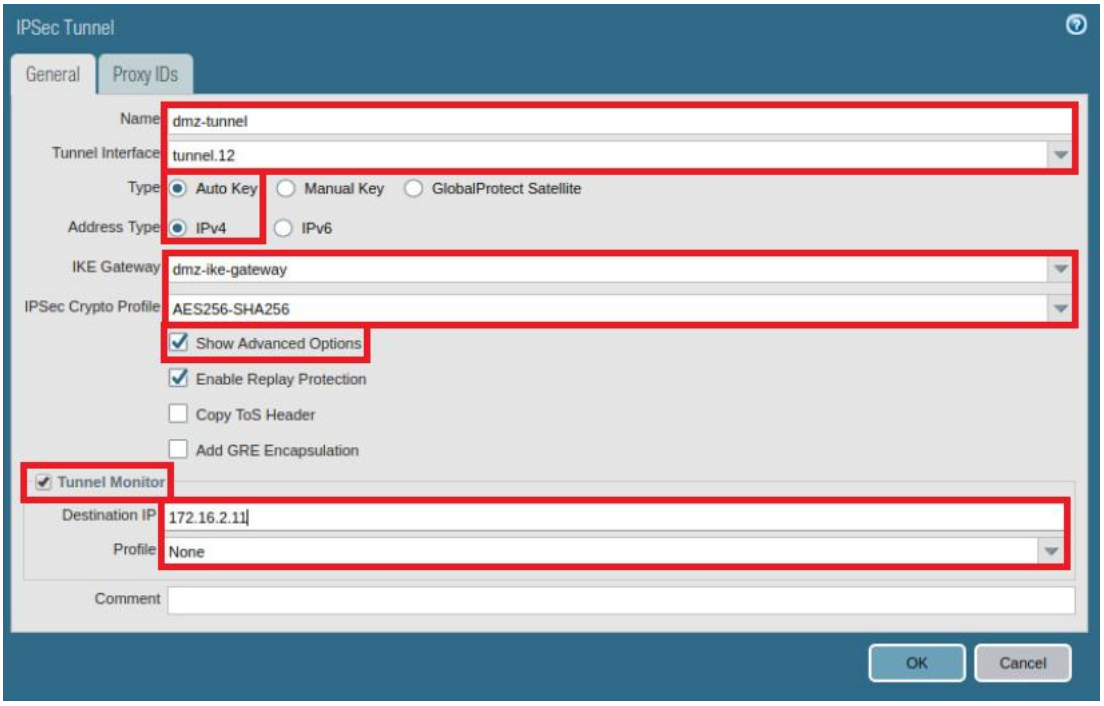


2. Click **Add** to define the IPsec tunnel.


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

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

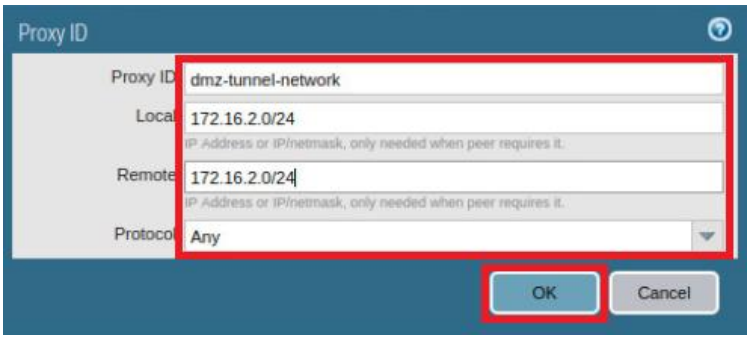


4. In the *IPSec Tunnel* window, click the **Proxy IDs** tab and then click **Add**.


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

| Parameter | Value |
|---|---|
| Proxy ID | Type `dmz-tunnel-network` |
| Local | Type `172.16.2.0/24` |
| Remote | Type `172.16.2.0/24` |
| Protocol | Verify that **Any** is selected |




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


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

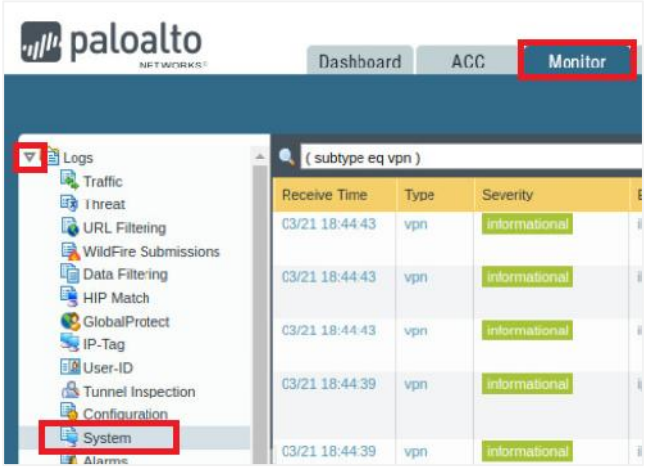
  

## 11.5 Test Connectivity

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

| | | | | IKE Gateway/Satellite | | | | Tunnel Interface | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Name | Status | Type | Interface | Local IP | Peer Address | Status | Interface | Virtual Router | Virtual System | S.. Z.. | 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... | |

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




3. Review the VPN log entries.

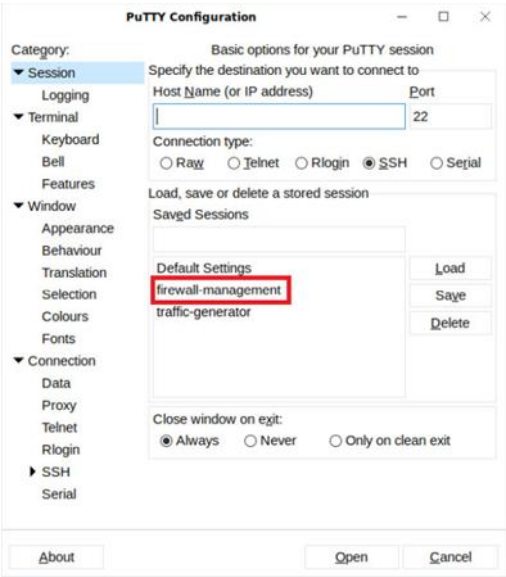
| Receive Time | Type | Severity | Event | Object | Description |
|---|---|---|---|---|---|
| 03/21 18:45:44 | vpn | informational | ipsec-key-install | dmz-tunnel:dmz-tunnel-network | IPSec key installed. Installed SA: 192.168.50.1[500]-192.168.50.10[500] SPI:0xDDF1DD46/0x70D709CA lifetime 3600 Sec lifesize 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 lifesize 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. |

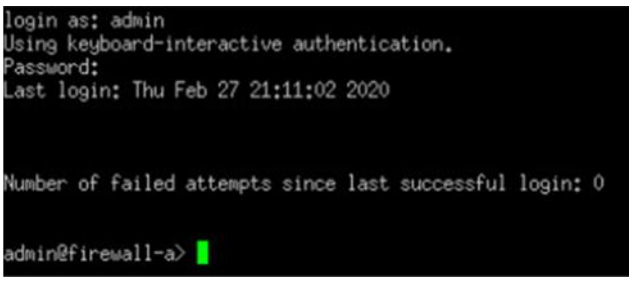
If you see messages related to "*pre-shared key mismatch*", go back to your **IKE Gateways** web interface under **Network Profiles**, click on **dmz-ike-gateway**, and re-type **`paloalto`** in both *Pre-shared Key* text fields. Click **OK** and **commit** all changes.

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$`**.



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/tunl/SHA2 9D74DC2C 1173FEEC 5CDDEAB5 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Init ESP/ DH2/tunl/SHA2 E69F1865 65918FB8 2C09EDA0 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Init ESP/ DH2/tunl/SHA2 FE182F90 E82B44A7 AADD6782 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Init ESP/ DH2/tunl/SHA2 DDF1DD46 70D709CA 745A8B60 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Init ESP/ DH2/tunl/SHA2 CD34CC88 F4BDBA9D 86BB9A8D 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Resp ESP/ DH2/tunl/SHA2 9DC4CC08 A6964930 B8F78551 9  1
dmz-ike-gateway       7       dmz-tunnel:dmz-tunnel- 4              Init ESP/ DH2/tunl/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 recv: 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.