PALO ALTO NETWORKS EDU-210

Lab 11: Site-to-Site VPN

Document Version: 2017-09-29

Contents

Introduction 3
Objectives 3
Lab Topology 4
Lab Settings 5
11 Lab: Site-to-Site VPN 6
11.1 Load Lab Configuration 6
11.2 Configure the Tunnel Interface 7
11.3 Configure the IKE Gateway 9
11.4 Create an IPSec Crypto Profile 12
11.5 Configure the IPsec Tunnel 14
11.6 Test Connectivity 17

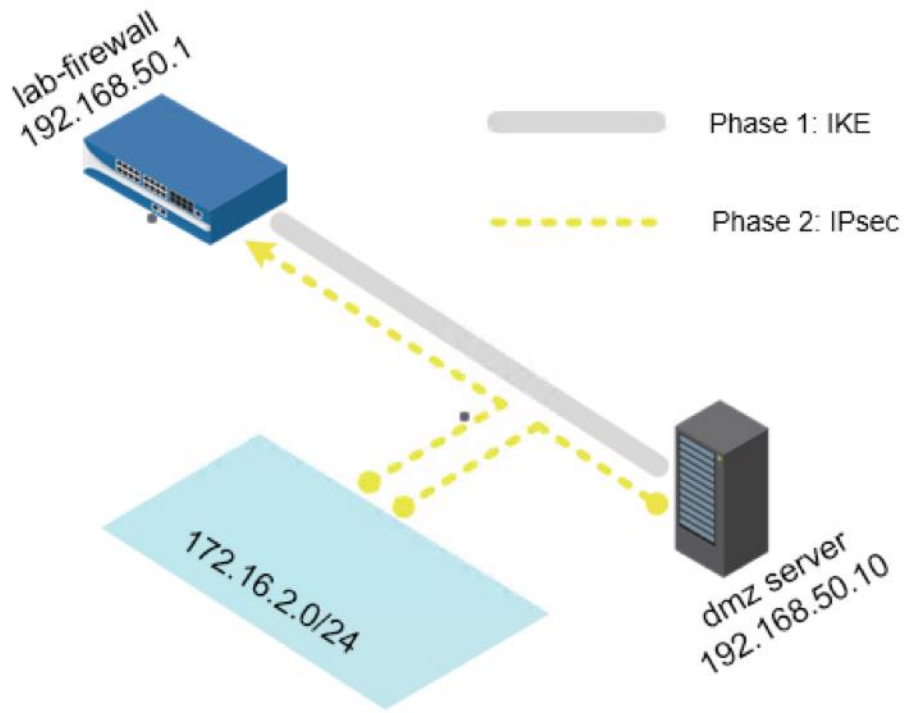
Introduction

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 locations and offices. To allow those branches to securely communicate with the office 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



Lab Settings

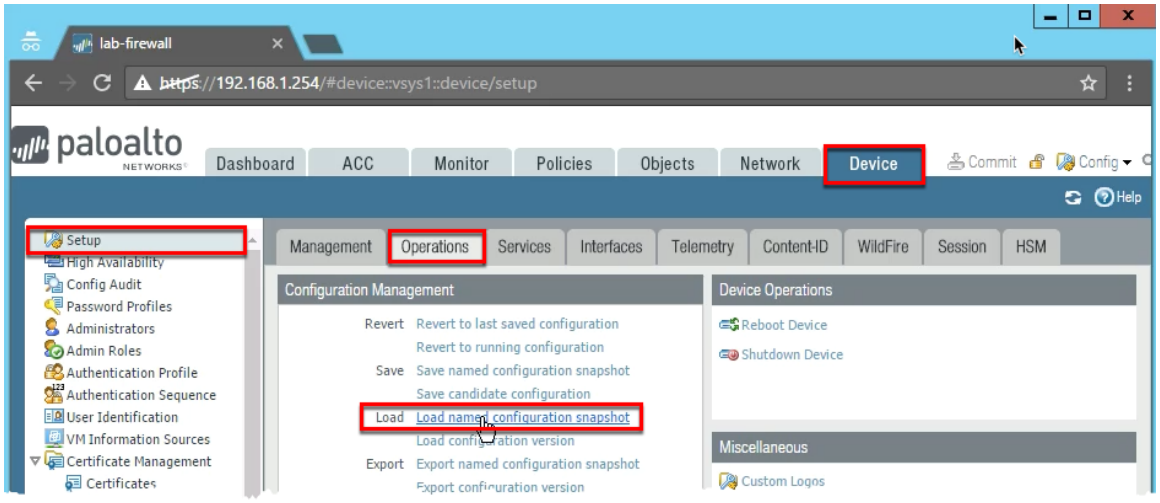
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

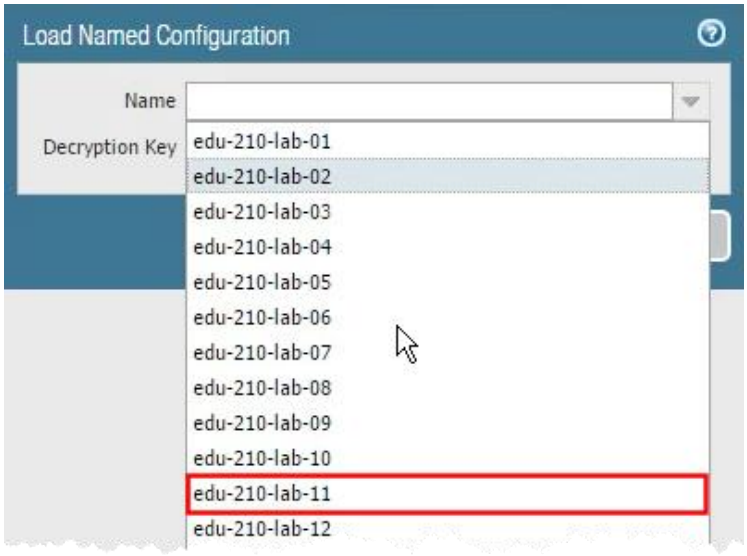
11 Lab: Site-to-Site VPN

11.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



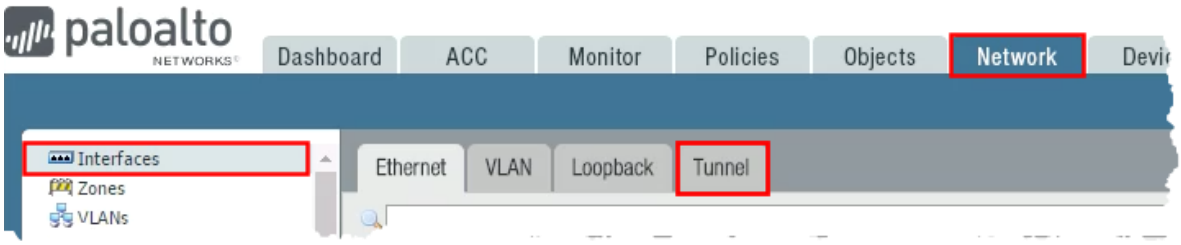
3. Select **edu-210-lab-11** and click **OK**.



4. Click **Close**.
5. **Commit** all changes.

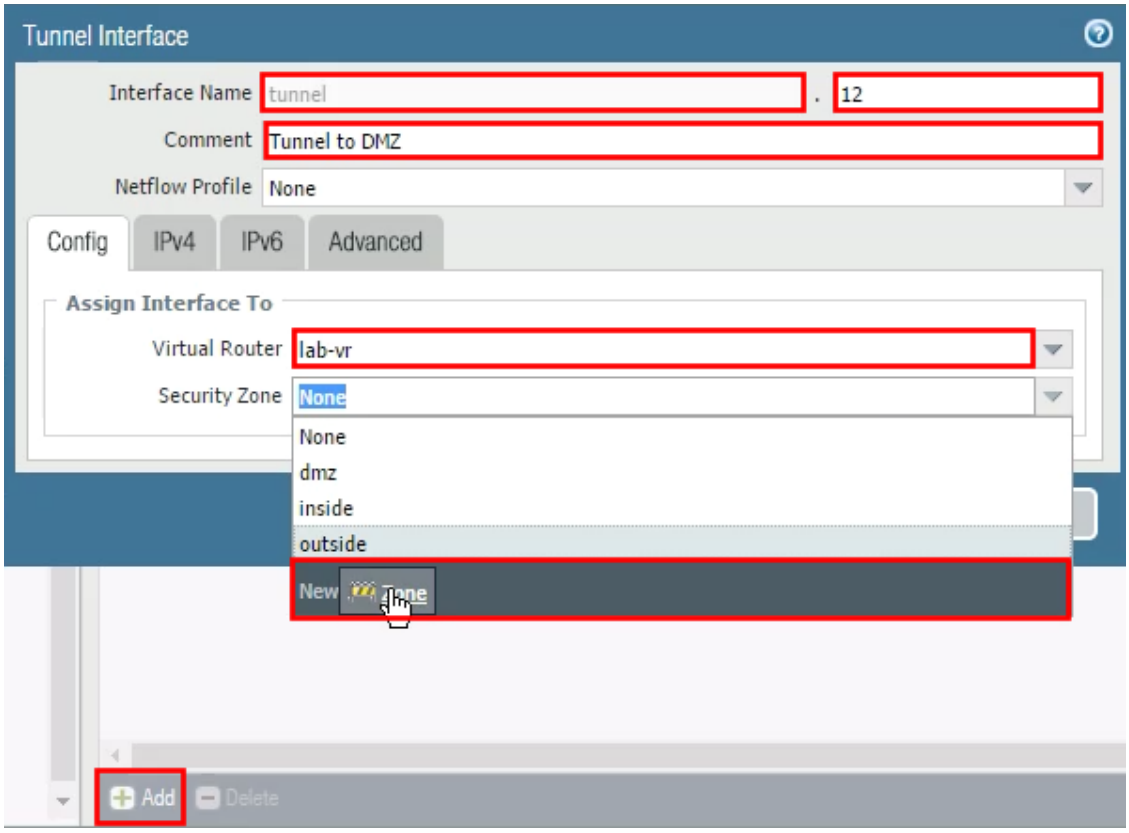
11.1 Configure the Tunnel Interface

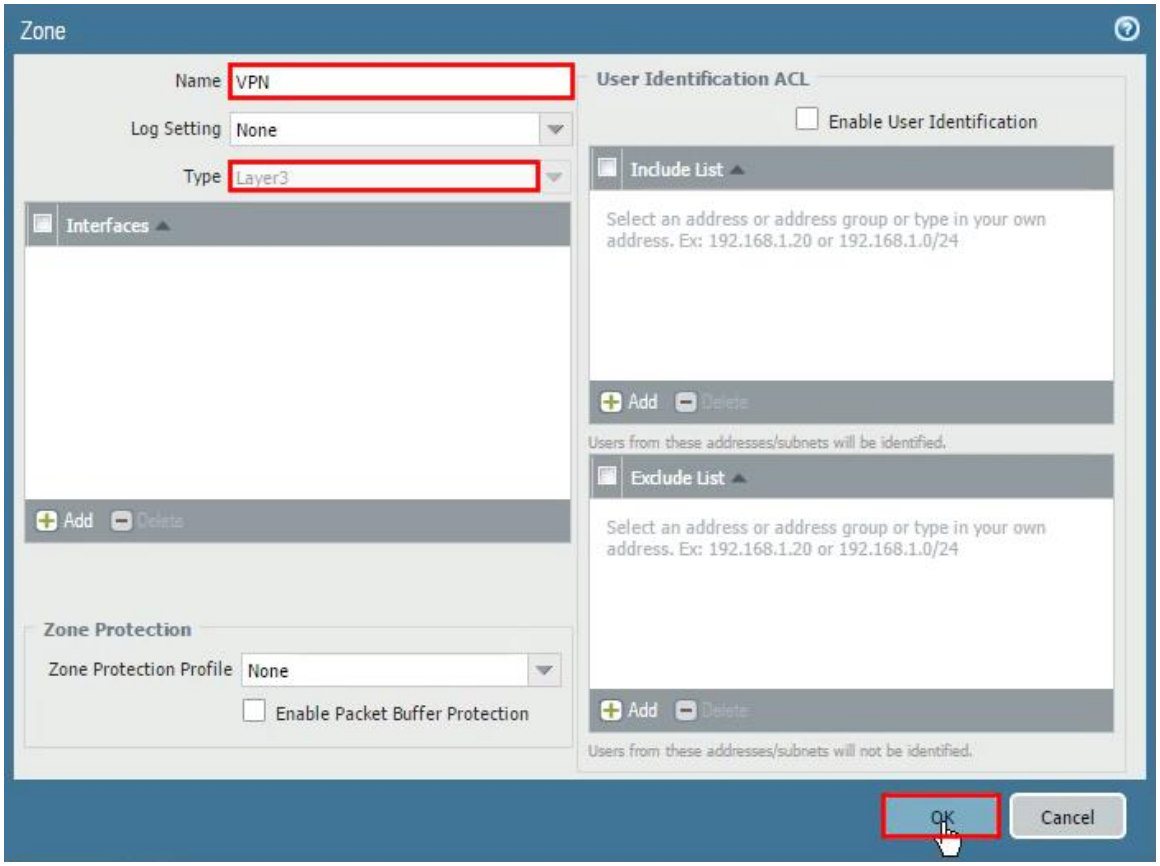
1. In the **WebUI select Network > Interfaces**.
2. Click the **Tunnel** tab.



3. Click **Add** to configure a tunnel interface:

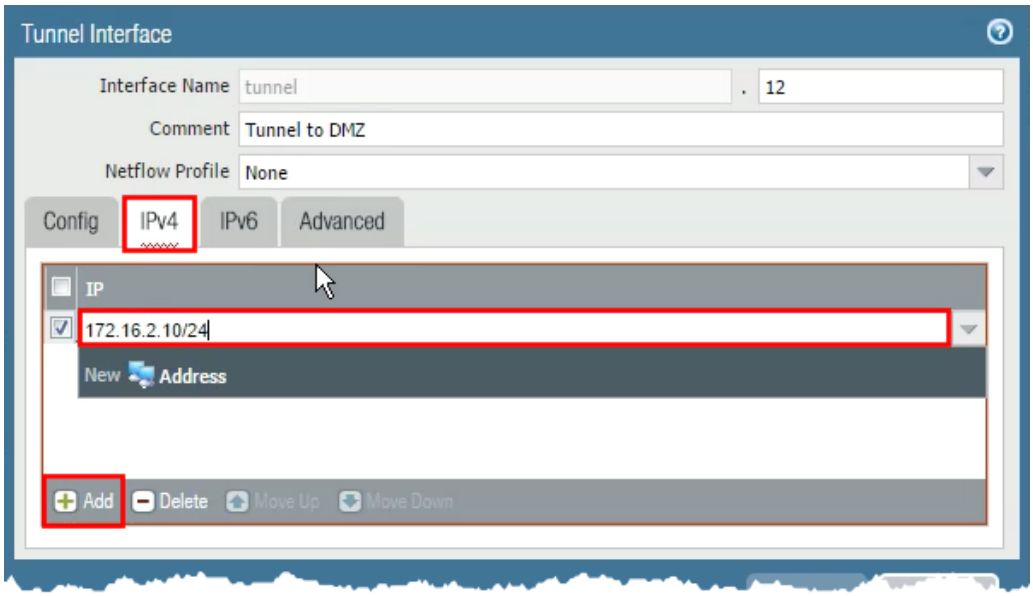
Parameter	Value
Interface Name	In the text box to the right of tunnel, enter `12`
Comment	`Tunnel to DMZ`
Virtual Router	**lab-vr**
Security Zone	Create and assign a new Layer 3 zone named `VPN`





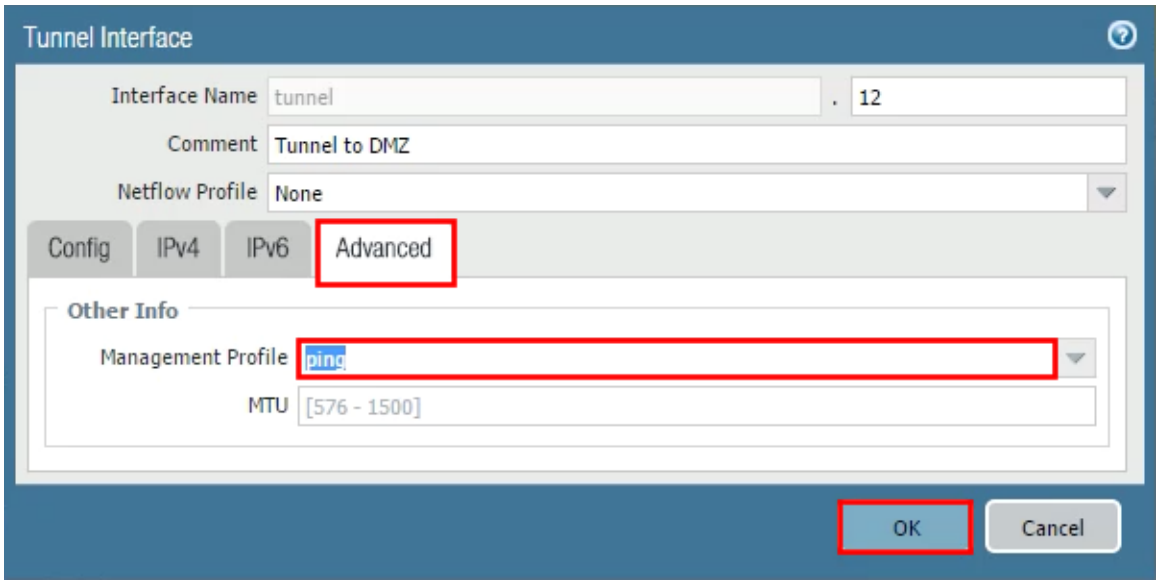
4. Click the **IPv4** tab and configure the following:

Parameter	Value
IP	172.16.2.10/24



5. Click the **Advanced** tab and configure the following:

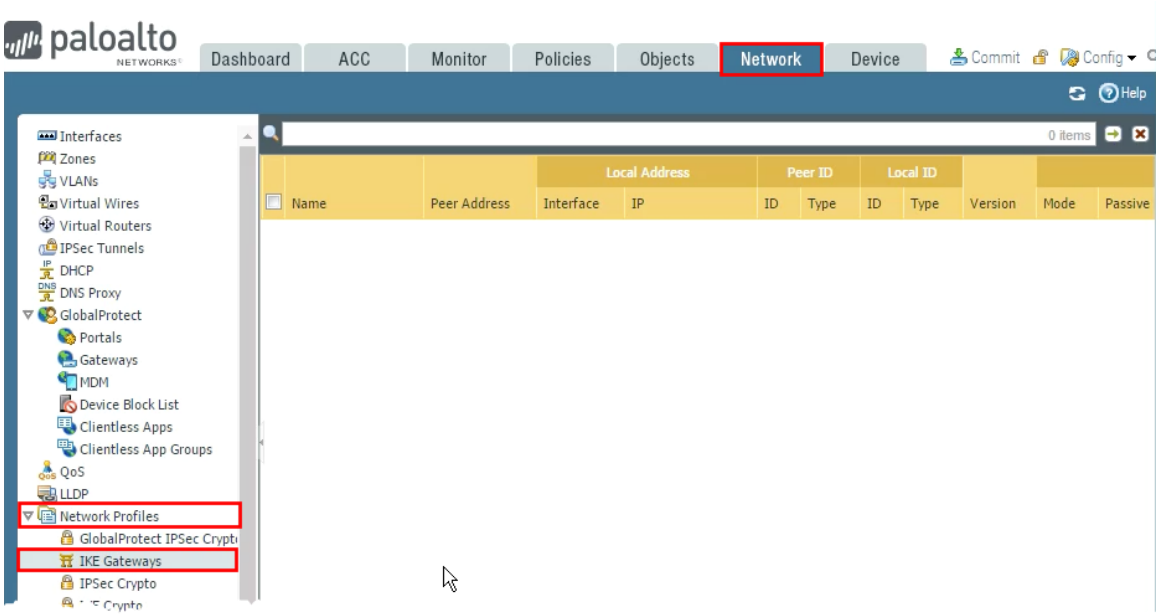
Parameter	Value
Management Profile	**ping**



6. Click **OK** to close the Tunnel Interface configuration window.

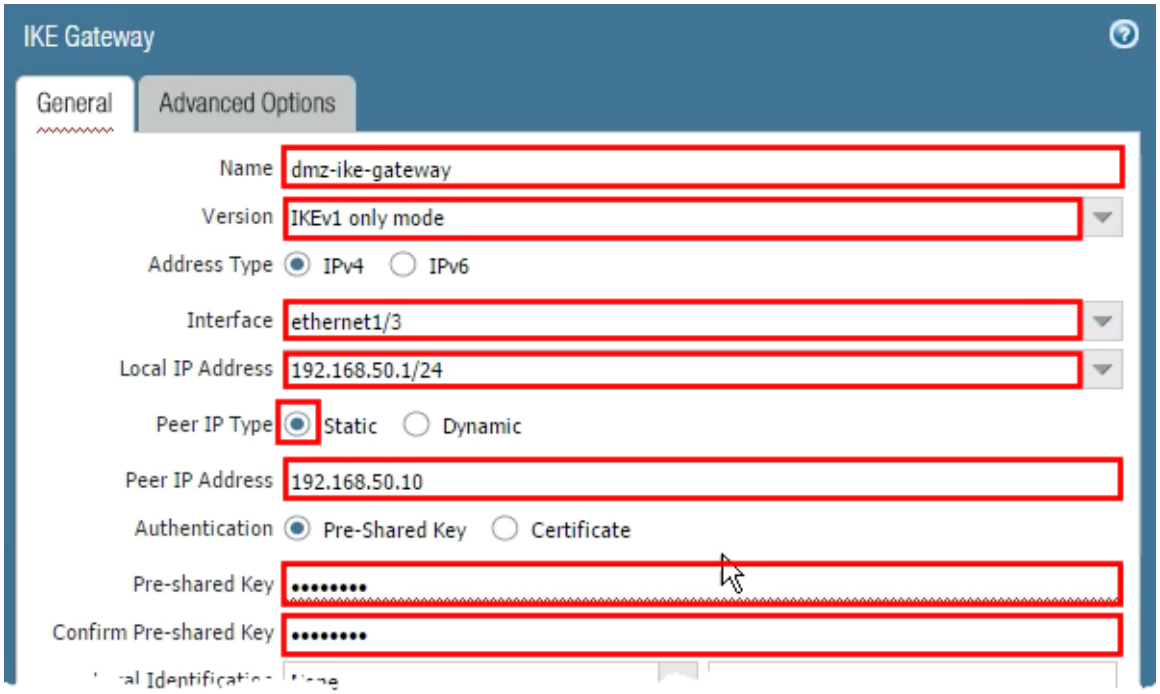
11.2 Configure the IKE Gateway

1. Select **Network > Network Profiles > IKE Gateways**.



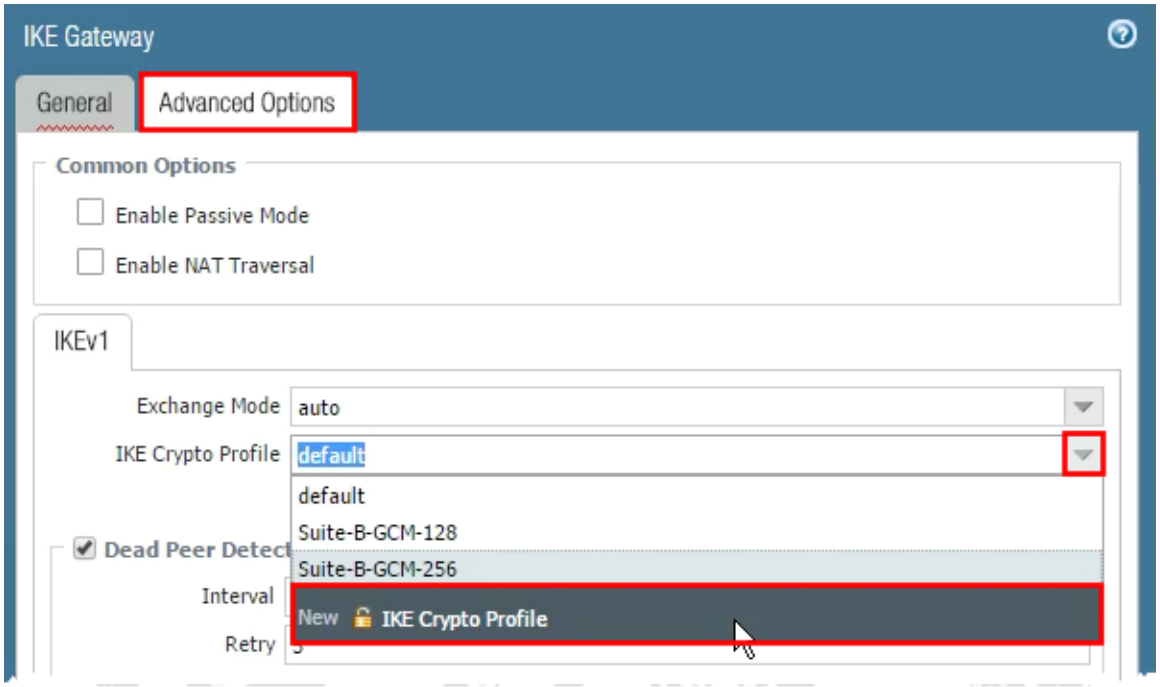
2. Click **Add** to create the IKE gateway and configure the following:

Parameter	Value
Name	`dmz-ike-gateway`
Version	**IKEv1 only mode**
Interface	**ethernet1/3**
Local IP Address	Select **192.168.50.1/24**
Peer Type	**static**
Peer IP Address	`192.168.50.10`
Pre-shared Key	`paloalto`



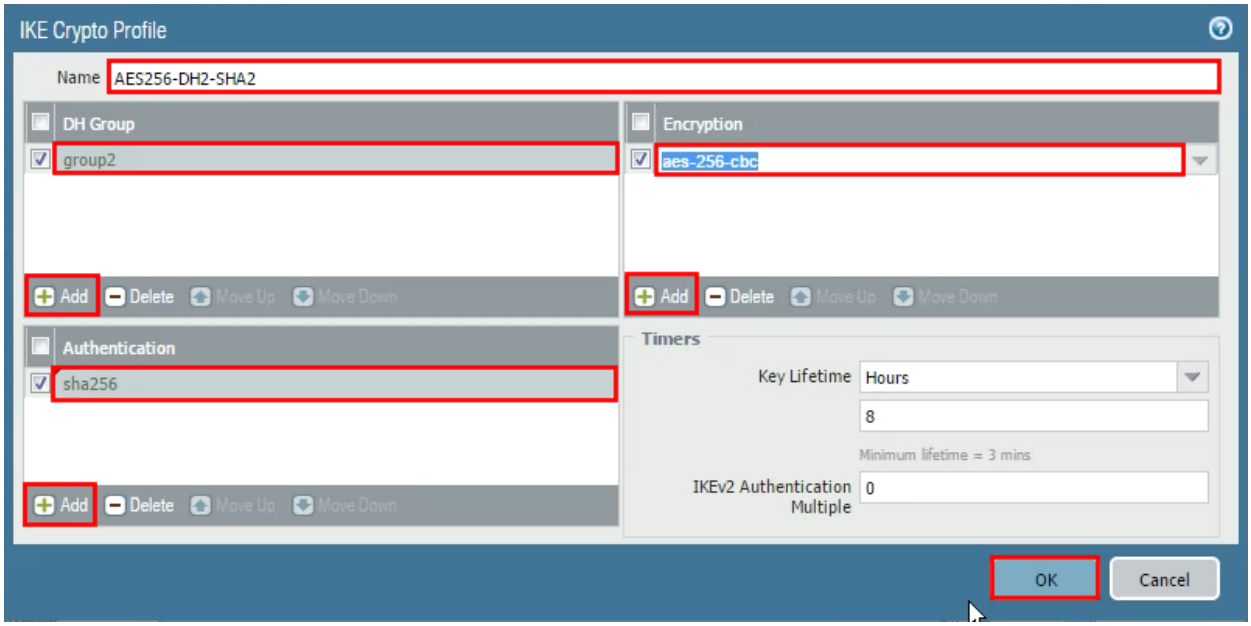
3. Click the **Advanced Options** tab.
4. On the IKEv1 subtab configure the following:

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



5. Configure the following:

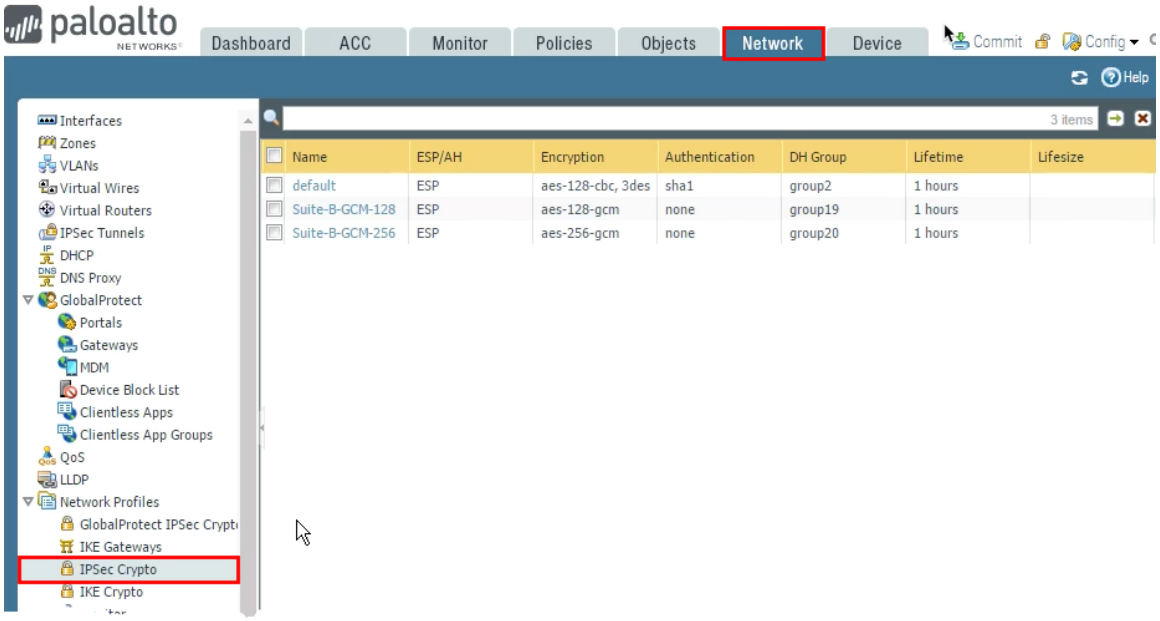
Parameter	Value
Name	AES256-DH2-SHA2
DH Group	Add **Group 2**
Authentication	Add **sha256**
Encryption	Add **aes-256-cbc**



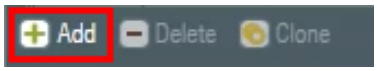
6. Click **OK** twice to close the IKE Crypto Profile and the IKE Gateway window.

11.3 Create an IPSec Crypto Profile

1. In the WebUI select **Network > Network Profiles > IPSec Crypto**.

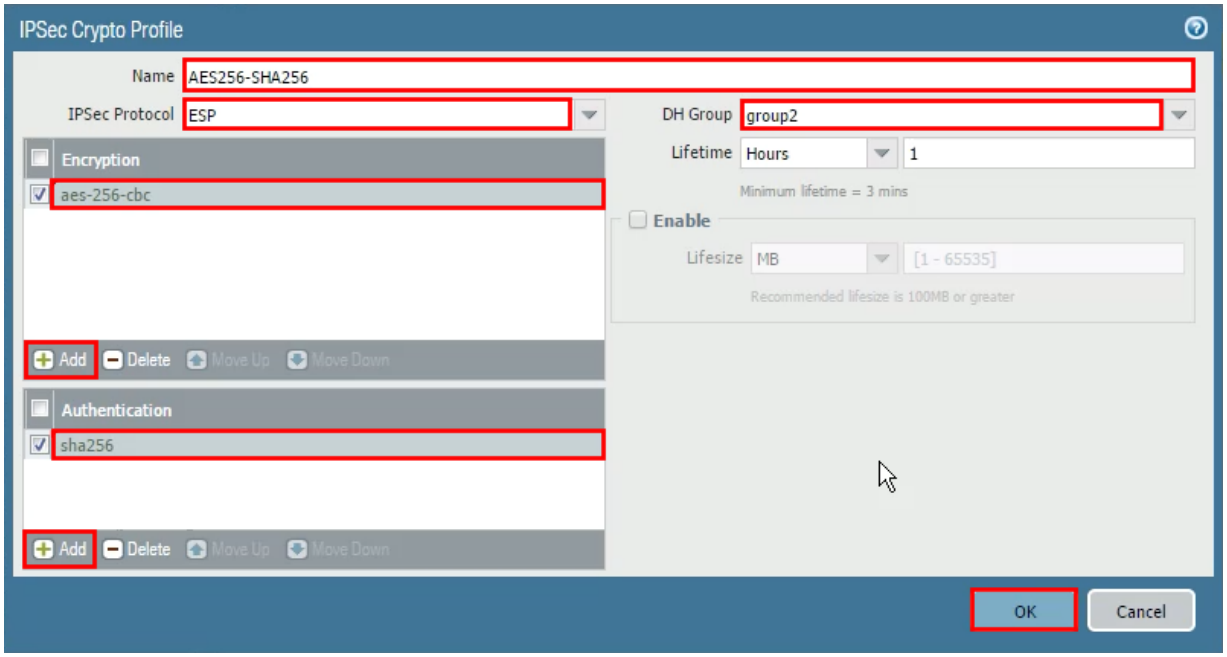


2. Click **Add** to open the IPSec Crypto Profile configuration window.



3. Configure the following:

Parameter	Value
Name	AES256-SHA256
IPSec Protocol	**ESP**
Encryption	Add **aes-256-cbc**
Authentication	Add **sha256**
DH Groups	Select **group2**

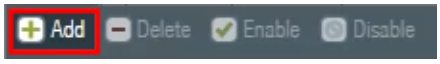


4. Click **OK** to close the IPSec Crypto Profile configuration window.

11.4 Configure the IPsec Tunnel

1. In the WebUI select **Network > IPSec Tunnels**.

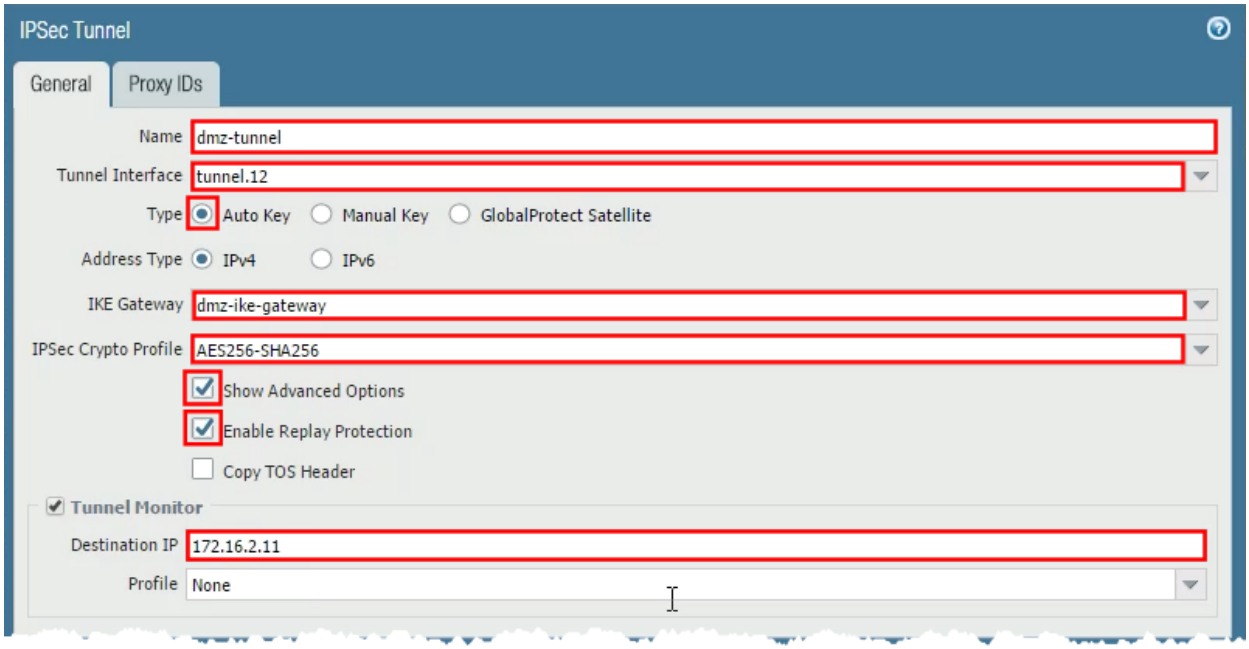
2. Click **Add** to define the IPsec tunnel.



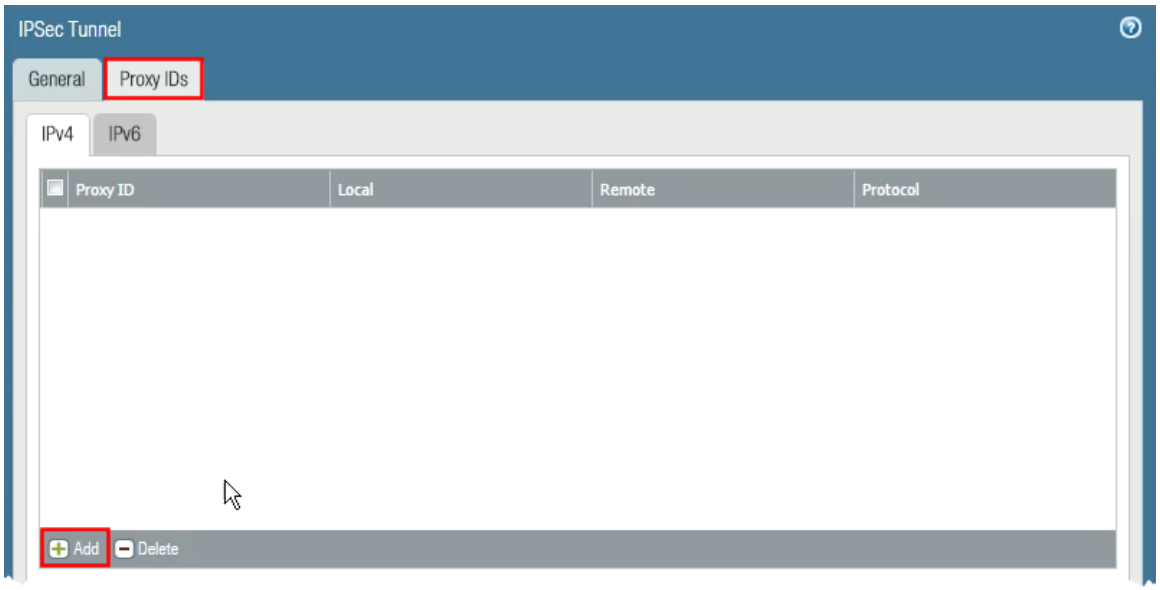
3. On the **General** tab:

Parameter	Value
Name	`dmz-tunnel`
Tunnel Interface	**tunnel.12**
Type	**Auto Key**
IKE Gateway	**dmz-ike-gateway**

Parameter	Value
IPSec Crypto Profile	**AES256-SHA256**
Show Advanced Options	Select the check box
Tunnel Monitor	Select the check box
Destination IP	`172.16.2.11`



4. Click the **Proxy IDs** tab.



5. Click **Add** and configure the following:

Parameter	Value
Proxy ID	dmz-tunnel-network
Local	172.16.2.0/24
Remote	172.16.2.0/24

6. Click **OK** twice to close the Proxy IDs and IPsec Tunnel windows:

7. **Commit** all changes.

11.5 Test Connectivity

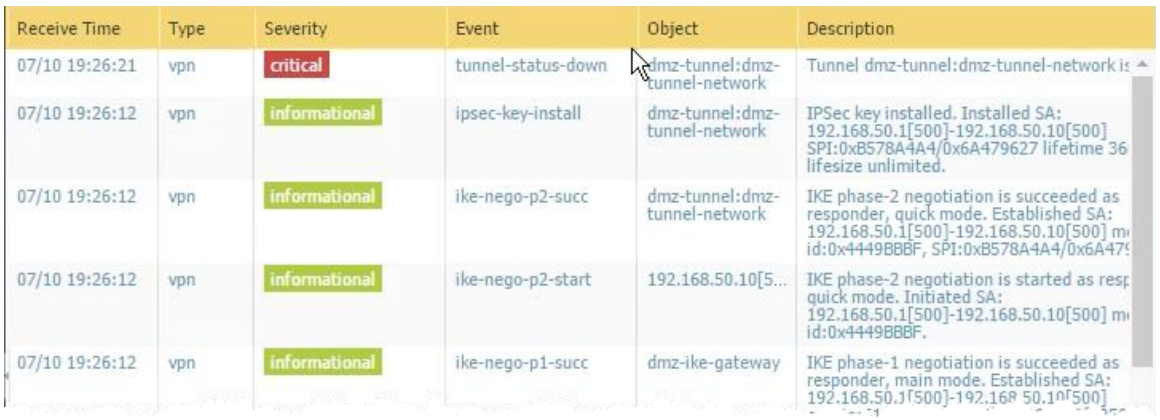
1. Select **Network > IPSec Tunnels**.

   Notice that the Status column indicator on the VPN tunnel might be red.

2. Refresh the Network > IPSec Tunnels page. The Status column indicator is now green:

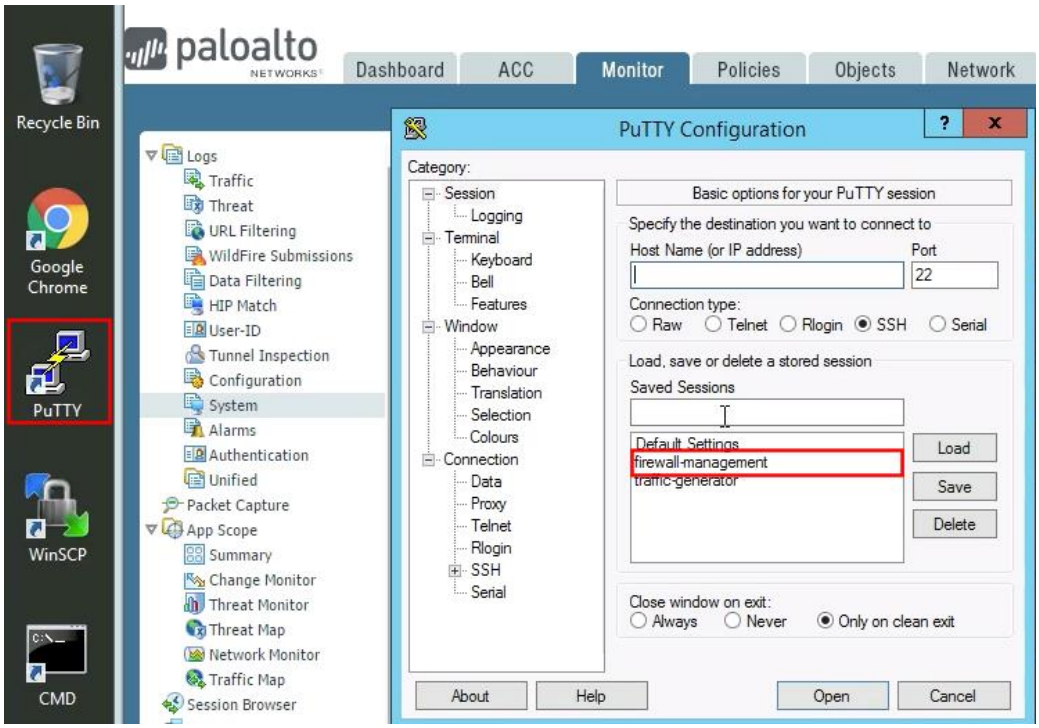
3. Select **Monitor > Logs > System**.

4. Review the VPN log entries:



Receive Time	Type	Severity	Event	Object	Description
07/10 19:26:21	vpn	critical	tunnel-status-down	dmz-tunnel:dmz-tunnel-network	Tunnel dmz-tunnel:dmz-tunnel-network is
07/10 19:26:12	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:0xB578A4A4/0x6A479627 lifetime 36 lifesize unlimited.
07/10 19:26:12	vpn	informational	ike-nego-p2-succ	dmz-tunnel:dmz-tunnel-network	IKE phase-2 negotiation is succeeded as responder, quick mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] m id:0x4449BBBF, SPI:0xB578A4A4/0x6A47
07/10 19:26:12	vpn	informational	ike-nego-p2-start	192.168.50.10[5...	IKE phase-2 negotiation is started as resp quick mode. Initiated SA: 192.168.50.1[500]-192.168.50.10[500] m id:0x4449BBBF.
07/10 19:26:12	vpn	informational	ike-nego-p1-succ	dmz-ike-gateway	IKE phase-1 negotiation is succeeded as responder, main mode. Established SA: 192.168.50.1[500]-192.168.50.10[500]

5. On the Windows desktop, launch **PuTTY**, double-click **firewall-management**, and log in to the firewall.




```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Sun Jul  9 04:48:18 2017 from 192.168.1.21

Number of failed attempts since last successful login: 0
```

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

```
show vpn ike-sa
```

```
admin@lab-firewall> 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  Jul.10 19:26:12 Jul.11 03:26:12
 v1 13 1  2

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 A75A3852 B03C125E 2DF67E22 9
 1
dmz-ike-gateway        7        dmz-tunnel:dmz-tunnel- 4                Resp ESP/ DH2/tunl/SHA2 B578A4A4 6A479627 4449BBBF 9
 1
dmz-ike-gateway        7        dmz-tunnel:dmz-tunnel- 4                Init ESP/ DH2/tunl/SHA2 DB0CBB5A C44B0279 B87A7B99 9
 1

Show IKEv1 phase2 SA: Total 1 gateways found. 3 ike sa found.


There is no IKEv2 SA found.

~
~
```

```
show vpn ipsec-sa tunnel dmz-tunnel:dmz-tunnel-network
```

```
admin@lab-firewall> 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)
--------------  ----   ------------           ---------------                                ---------          -------  ----
---- ------------
4               7      192.168.50.10          dmz-tunnel:dmz-tunnel-network(dmz-ike-gateway) ESP/A256/SHA256    B211E598 72B4
017E 3564/0

Show IPSec SA: Total 1 tunnels found. 1 ipsec sa found.
```

```
show vpn flow name dmz-tunnel:dmz-tunnel-network
```

```
admin@lab-firewall> 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:                989
        tunnel mtu:             1424
        soft lifetime:          3562
        hard lifetime:          3600
        lifetime remain:        3558 sec
        lifesize remain:        N/A
        latest rekey:           2 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: 63
          monitor packets recv: 0
          monitor packets seen: 0
          monitor packets reply:0
        en/decap context:       6
        local spi:              9134F574
        remote spi:             B7B8E733
        key type:               auto key
        protocol:               ESP
        auth algorithm:         SHA256
        enc  algorithm:         AES256
        proxy-id:
          local ip:             172.16.2.0/24
          remote ip:            172.16.2.0/24
          protocol:             0
          local port:           0
          remote port:          0
        anti replay check:      no
        copy tos:               no
        authentication errors:  0
lines 1-43
```

```
show running tunnel flow
```

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

```
total tunnels configured:                                   2
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:                            1
total SSL-VPN tunnel shown:                                 0


total GlobalProtect-Gateway tunnel shown:                   1

id    name                  local-i/f         local-ip                    tunnel-i/f
--    ----                  ---------         --------                    ----------
1     gp-ext-gateway-N      ethernet1/1       203.0.113.20                tunnel.11

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


admin@lab-firewall>
```

Stop. This is the end of the Site-to-Site VPN lab.

