



PALO ALTO NETWORKS EDU-210

Lab 11: Site-to-Site VPN

Document Version: 2017-09-29

Copyright © 2017 Network Development Group, Inc.
www.netdevgroup.com

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

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

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

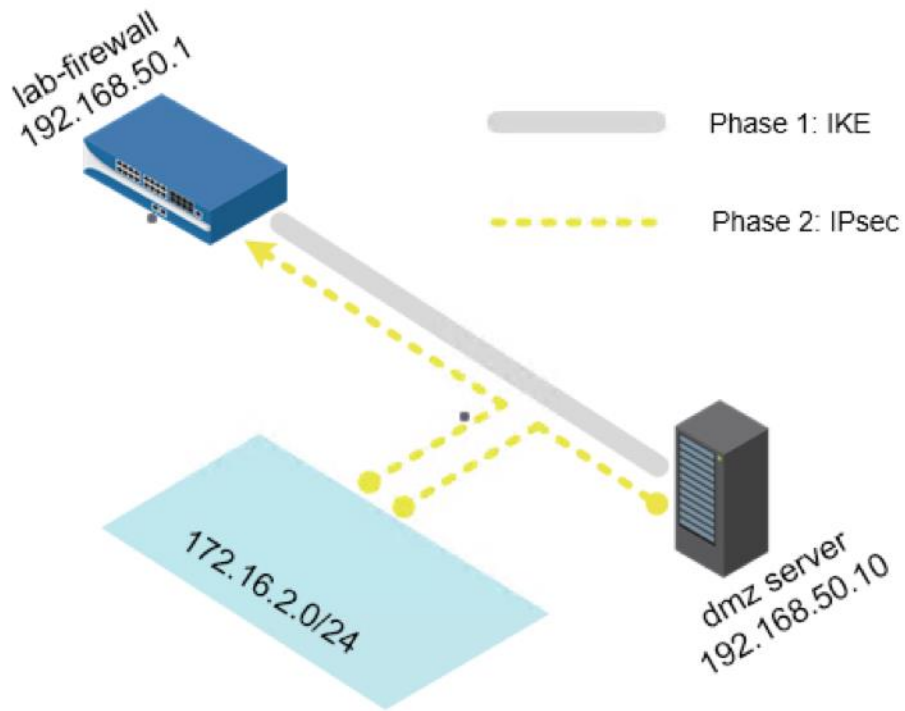
Introduction

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

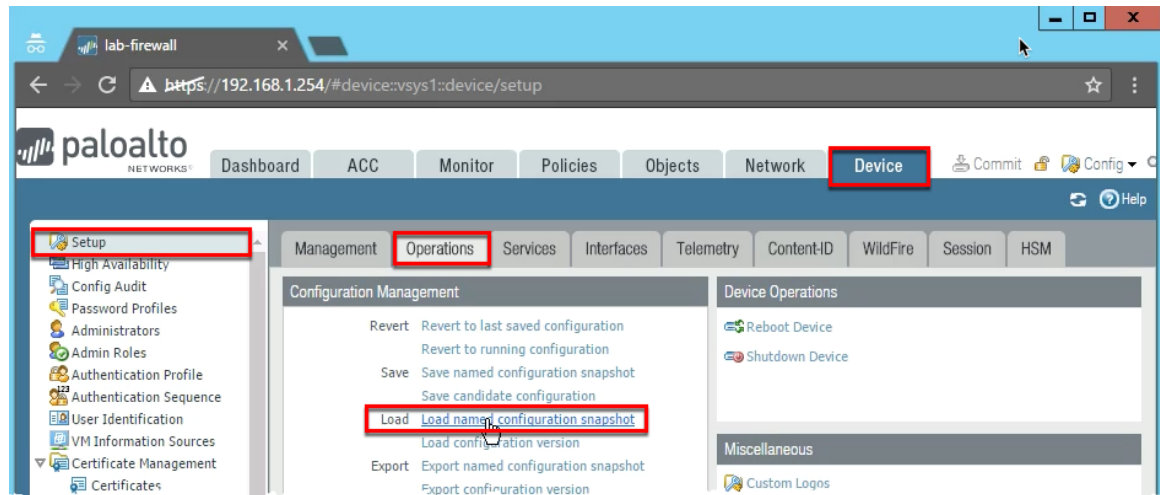
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

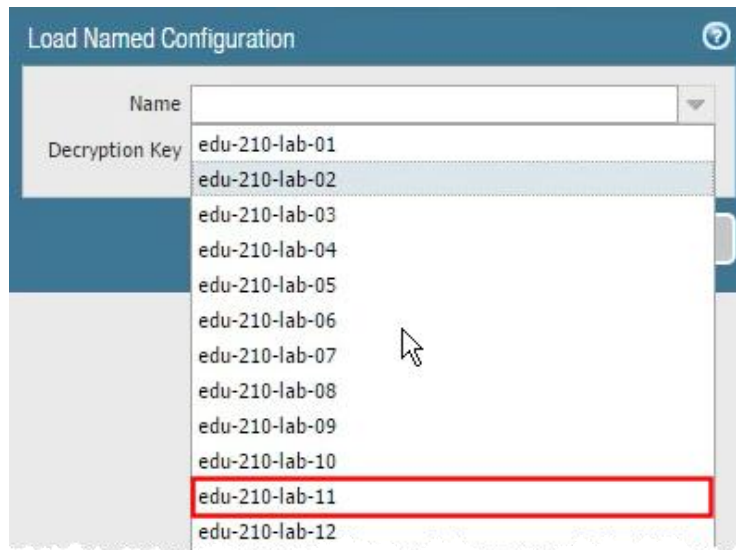
11 Lab: Site-to-Site VPN

11.0 Load Lab Configuration

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



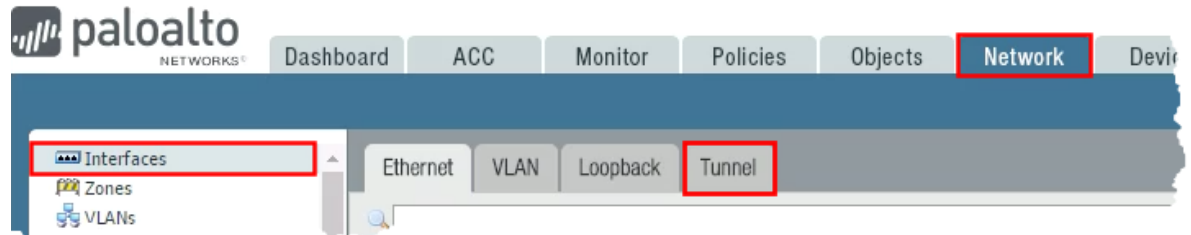
3. Select **edu-210-lab-11** and click **OK**.



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

Tunnel Interface

Interface Name: tunnel . 12

Comment: Tunnel to DMZ

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: lab-vr

Security Zone: None

None
dmz
inside
outside
New [icon] none

+ Add - Delete

Zone

Name: VPN

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

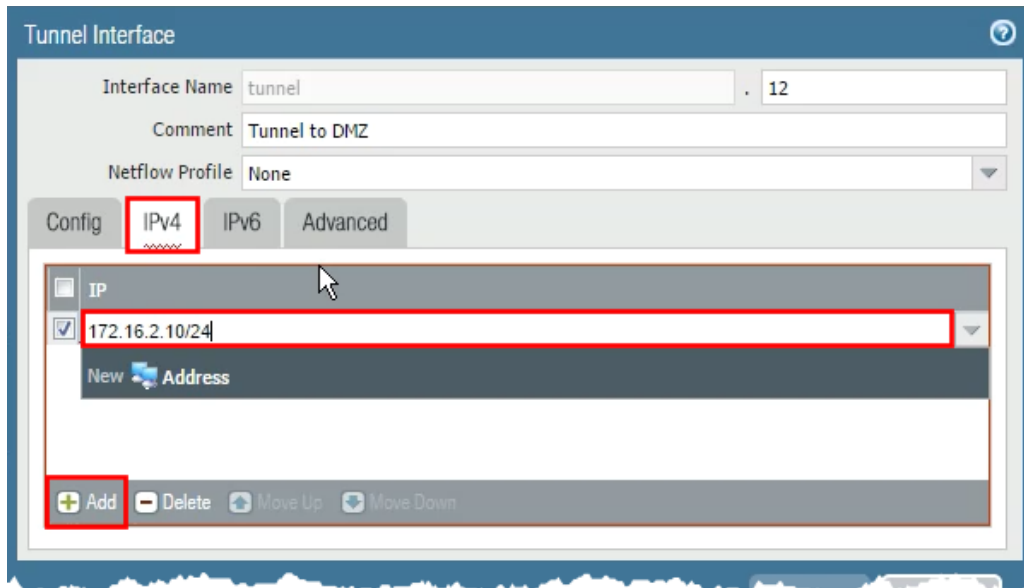
+ Add - Delete

Users from these addresses/subnets will not be identified.

OK Cancel

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

Parameter	Value
IP	172.16.2.10/24



Tunnel Interface

Interface Name: tunnel . 12

Comment: Tunnel to DMZ

Netflow Profile: None

Config IPv4 IPv6 Advanced

IP

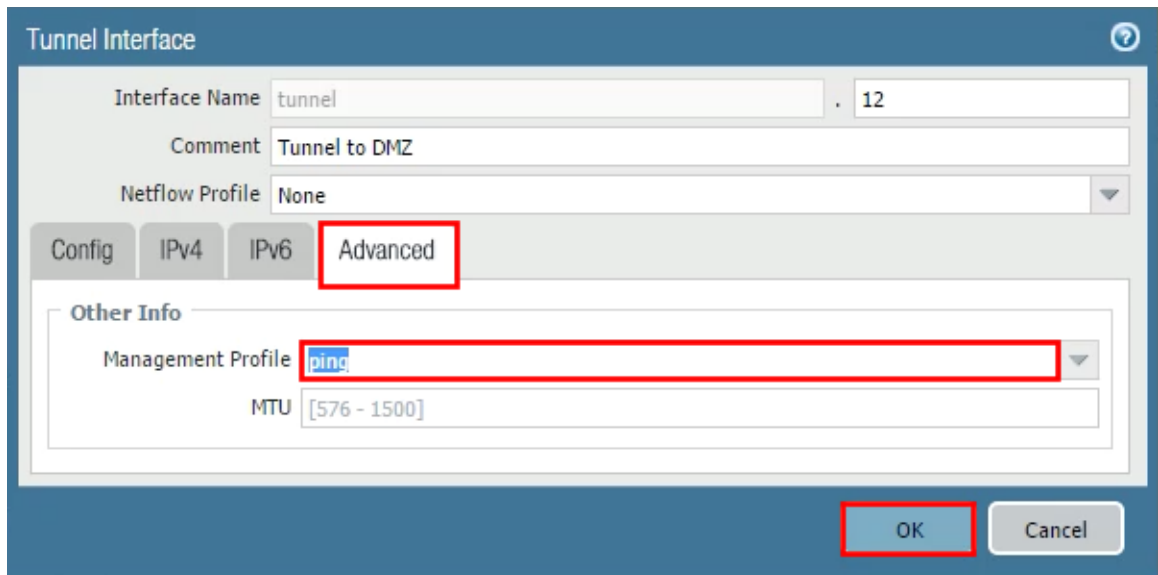
172.16.2.10/24

New Address

Add Delete Move Up Move Down

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

Parameter	Value
Management Profile	ping



Tunnel Interface

Interface Name: tunnel . 12

Comment: Tunnel to DMZ

Netflow Profile: None

Config IPv4 IPv6 Advanced

Other Info

Management Profile: ping

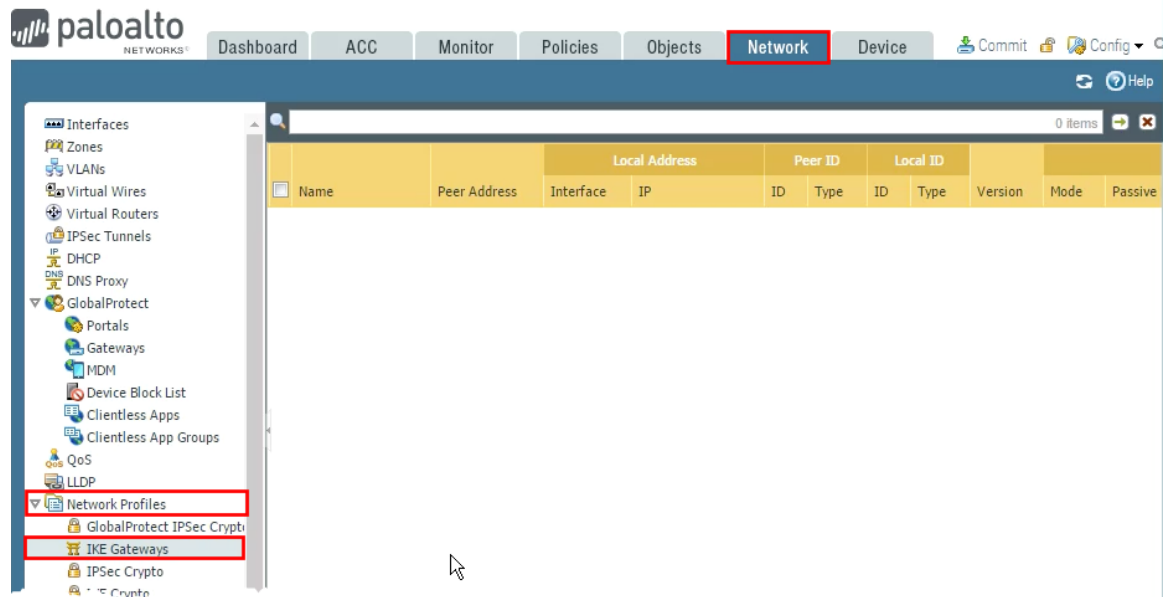
MTU: [576 - 1500]

OK Cancel

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

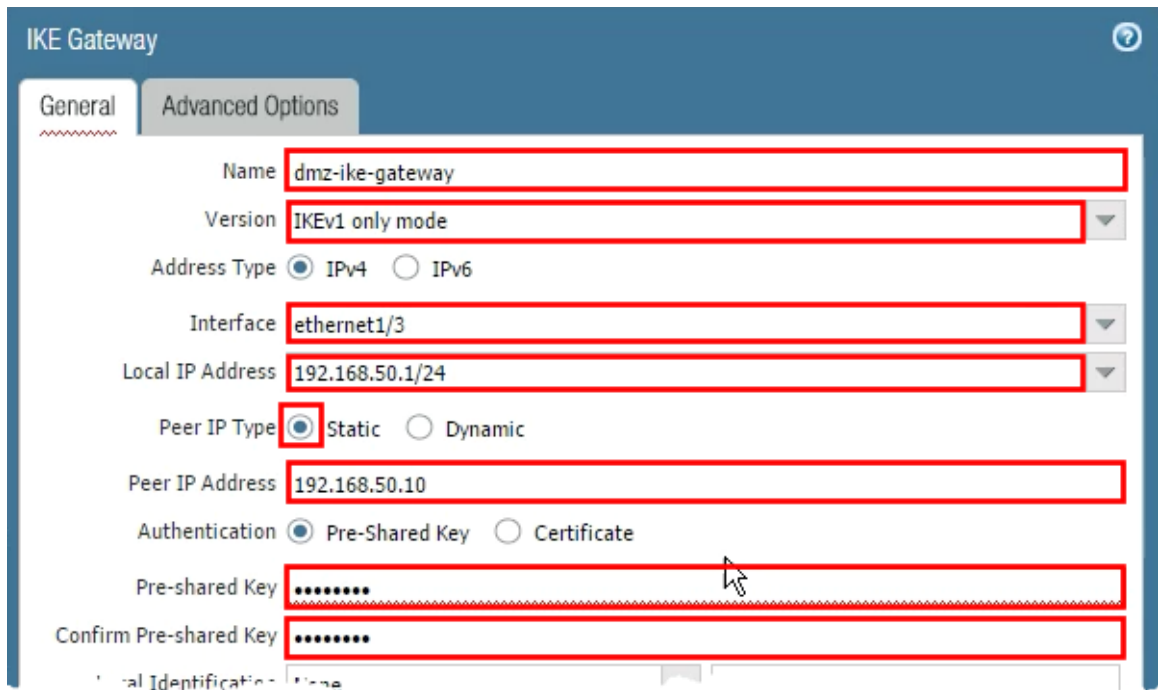
11.2 Configure the IKE Gateway

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



IKE Gateway

General | Advanced Options

Name: dmz-ike-gateway

Version: IKEv1 only mode

Address Type: ☒ IPv4 ☐ IPv6

Interface: ethernet1/3

Local IP Address: 192.168.50.1/24

Peer IP Type: ☒ Static ☐ Dynamic

Peer IP Address: 192.168.50.10

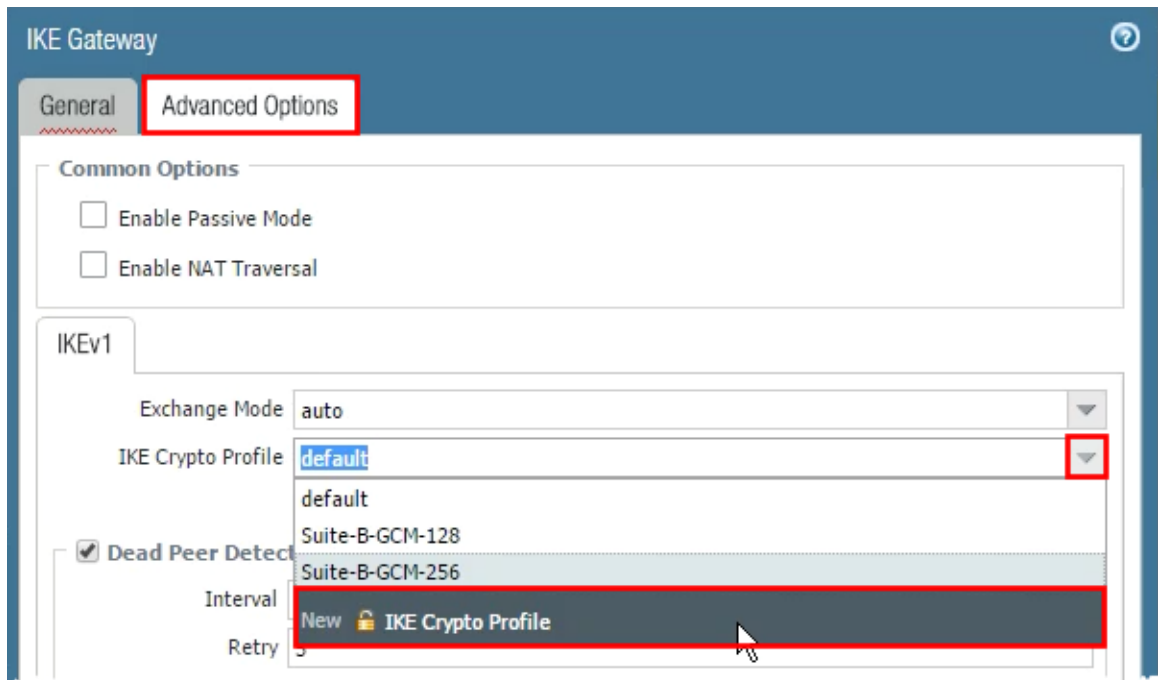
Authentication: ☒ Pre-Shared Key ☐ Certificate

Pre-shared Key:

Confirm Pre-shared Key:

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

Parameter	Value
IKE Crypto Profile	Select New IKE Crypto Profile



IKE Gateway

General | **Advanced Options**

Common Options

☐ Enable Passive Mode

☐ Enable NAT Traversal

IKEv1


Exchange Mode: auto

IKE Crypto Profile: default

☒ Dead Peer Detection

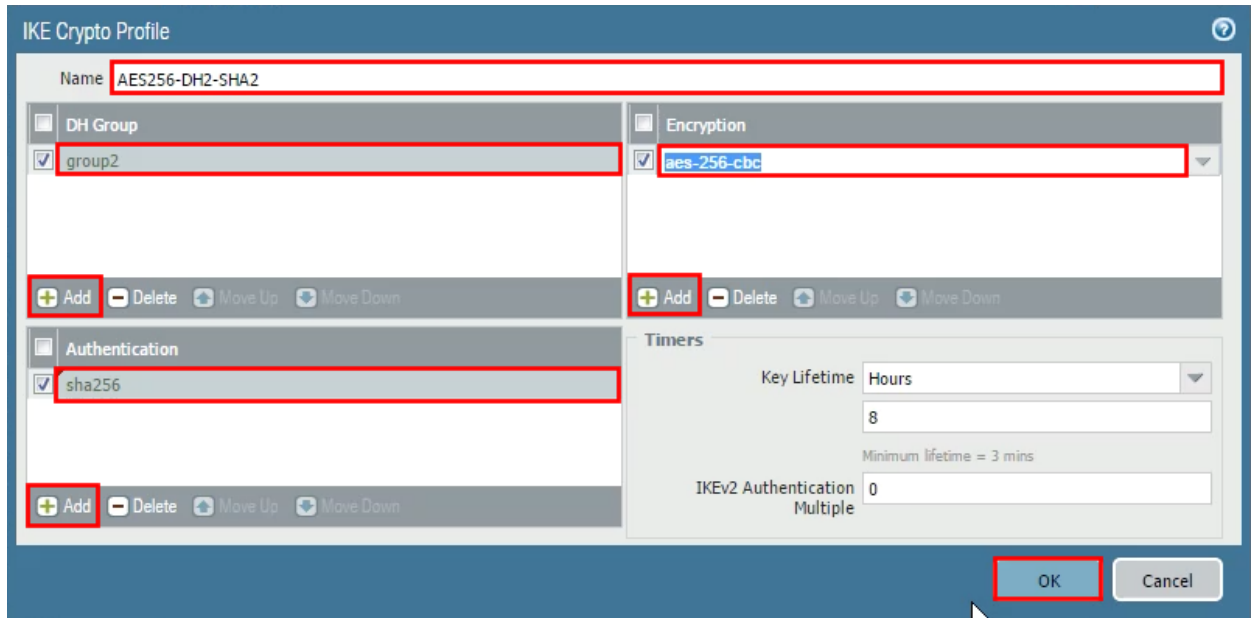
Interval: Suite-B-GCM-128

Retry: Suite-B-GCM-256

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

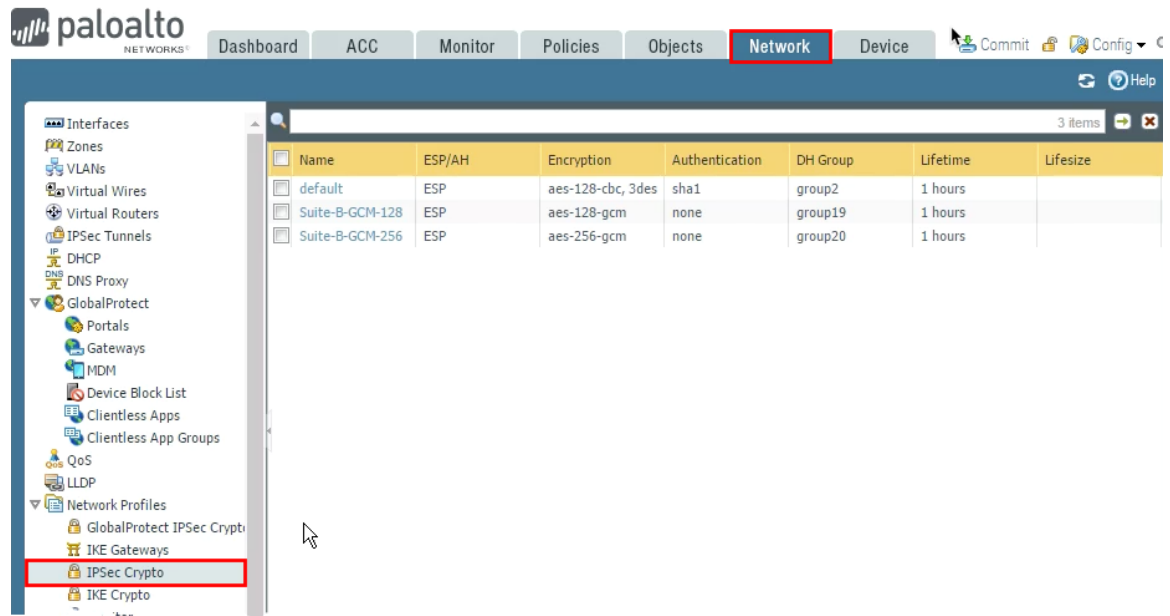


The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' field is 'AES256-DH2-SHA2'. The 'DH Group' section has 'group2' selected. The 'Encryption' section has 'aes-256-cbc' selected. The 'Authentication' section has 'sha256' selected. The 'Timers' section shows 'Key Lifetime' as 8 hours and 'IKEv2 Authentication Multiple' as 0. The 'OK' button is highlighted.

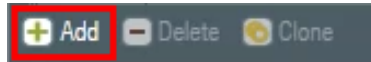
6. Click **OK** twice to close the IKE Crypto Profile and the IKE Gateway window.

11.3 Create an IPSec Crypto Profile

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

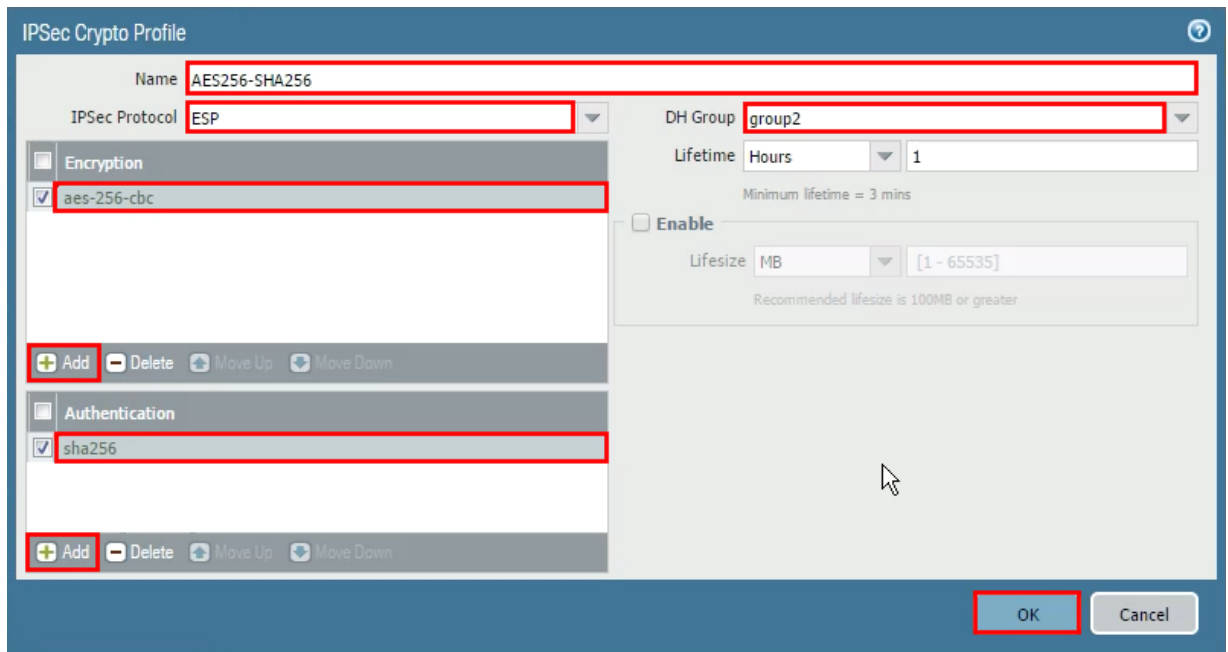


- Click **Add** to open the IPSec Crypto Profile configuration window.



- Configure the following:

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

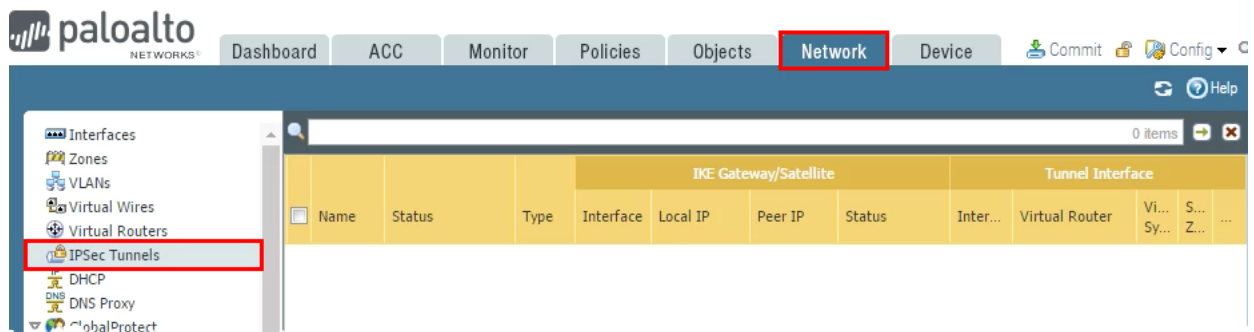


The screenshot shows the 'IPSec Crypto Profile' configuration window. The 'Name' field is set to 'AES256-SHA256'. The 'IPSec Protocol' is set to 'ESP'. The 'DH Group' is set to 'group2'. The 'Lifetime' is set to 'Hours' with a value of '1'. The 'Encryption' section has 'aes-256-cbc' selected. The 'Authentication' section has 'sha256' selected. The 'Enable' checkbox is unchecked. The 'Lifsize' is set to 'MB' with a range of '[1 - 65535]'. The 'OK' button is highlighted with a red box.

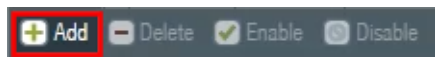
- Click **OK** to close the IPSec Crypto Profile configuration window.

11.4 Configure the IPSec Tunnel

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



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



- 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

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

☒ Tunnel Monitor

Destination IP: 172.16.2.11

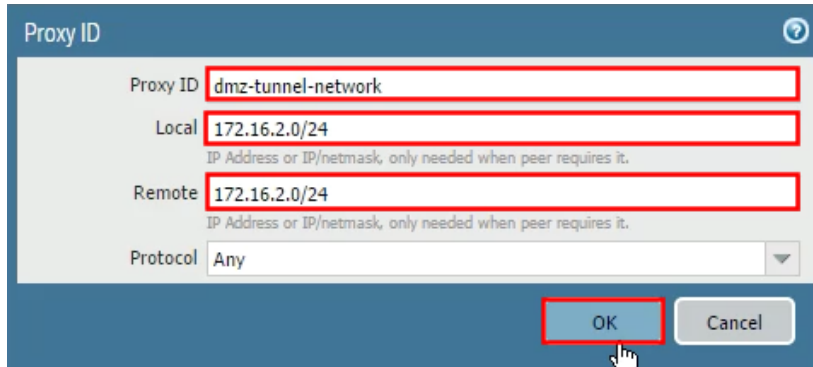
Profile: None

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

The screenshot shows the 'IPsec Tunnel' configuration window. The 'Proxy IDs' tab is selected and highlighted with a red box. Below the tabs, there are two sub-tabs: 'IPv4' and 'IPv6'. The 'IPv4' sub-tab is active, displaying a table with the following columns: 'Proxy ID', 'Local', 'Remote', and 'Protocol'. The table is currently empty. At the bottom left, there are two buttons: 'Add' (with a plus icon) and 'Delete' (with a minus icon). The 'Add' button is highlighted with a red box. A mouse cursor is visible over the 'Add' button.

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



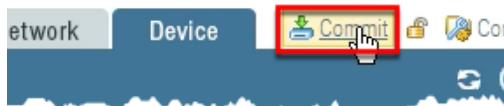
Proxy ID configuration dialog box. The fields are: Proxy ID (dmz-tunnel-network), Local (172.16.2.0/24), Remote (172.16.2.0/24), and Protocol (Any). The OK button is highlighted with a red box and a mouse cursor.

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



	Name	Status	Type	IKE Gateway/Satellite			Tunnel Interface				
				Interface	Local IP	Peer IP	Status	Inter...	Virtual Router	Vi... Sy...	S... Z...
<input type="checkbox"/>	dmz-tunnel	 Tunnel Info	Auto Key	ethern...	192.168.50...	192.168....	 IKE Info	tunn...	lab-vr (Show Routes)	vs...	...

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**.

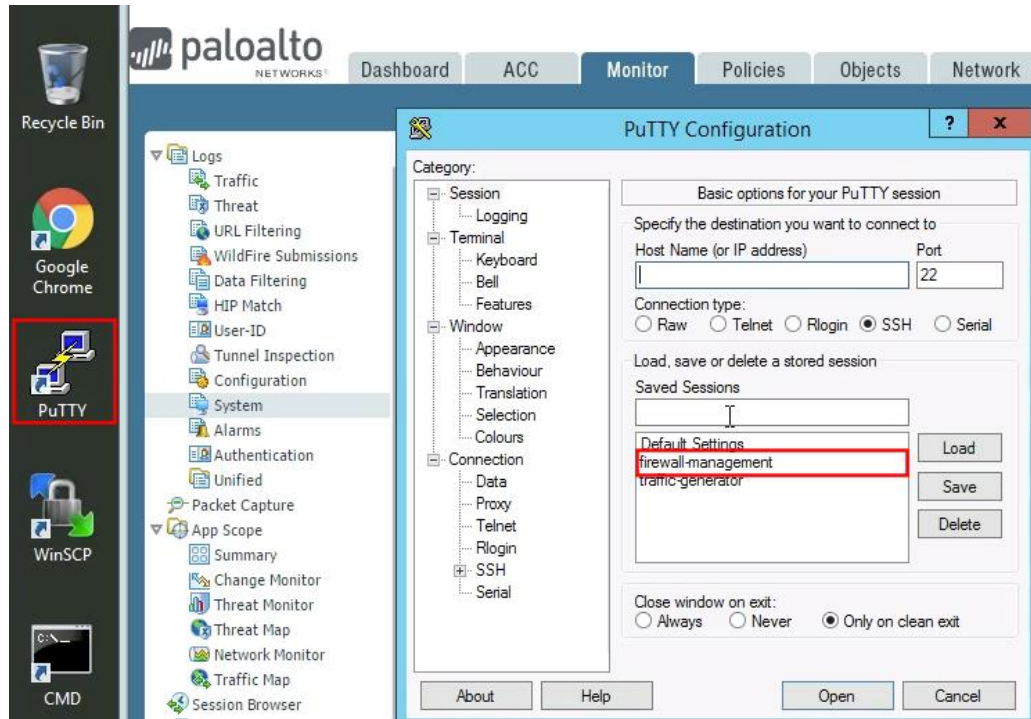


Receive Time	Type	Severity
07/10 19:26:21	vpn	 critical
07/10 19:26:12	vpn	 informational
07/10 19:26:12	vpn	 informational
07/10 19:26:12	vpn	 informational

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 lifeseize 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:0x444988BF, SPI:0xB578A4A4/0x6A479627
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:0x444988BF.
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]

- 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
```

- 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
I

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
-----
dmz-ike-gateway 7 dmz-tunnel:dmz-tunnel- 4 Init ESP/ DH2/tun1/SHA2 A75A3852 B03C125E 2DF67E22 9
1
dmz-ike-gateway 7 dmz-tunnel:dmz-tunnel- 4 Resp ESP/ DH2/tun1/SHA2 B578A4A4 6A479627 4449BBBF 9
1
dmz-ike-gateway 7 dmz-tunnel:dmz-tunnel- 4 Init ESP/ DH2/tun1/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 72B4017E 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 rcv: 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.