

PALO ALTO FIREWALL SITE TO SITE VPN LAB



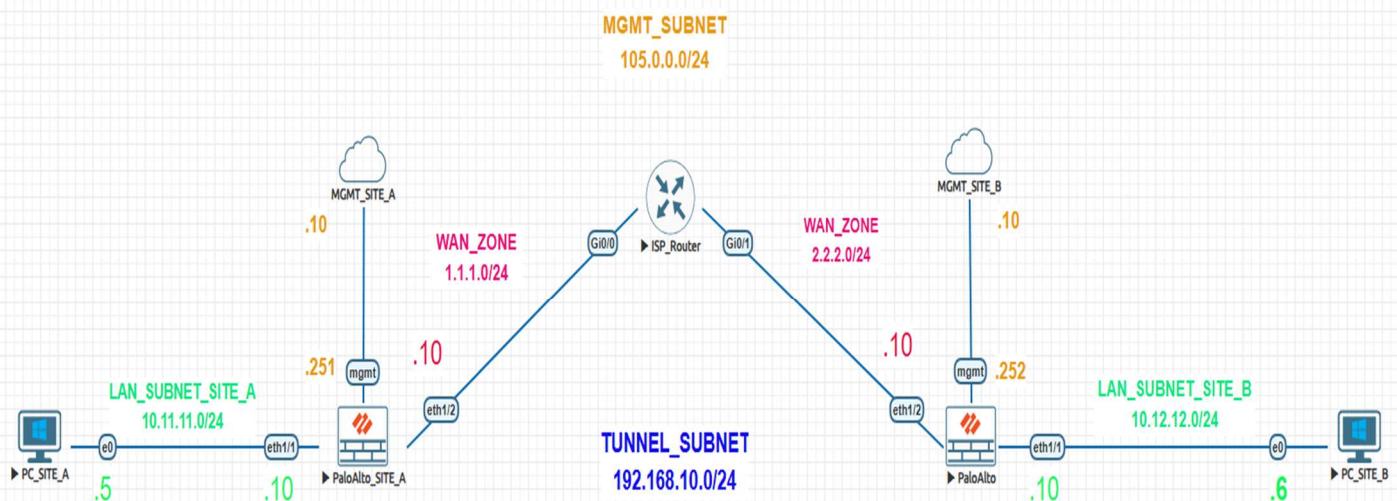
FOLLOW ME ON LINKEDIN FOR MORE SUCH CONTENTS



[linkedin.com/in/imkumarabhishek](https://www.linkedin.com/in/imkumarabhishek)

TOPOLOGY

PALO ALTO SITE TO SITE VPN LAB



Network topology of Site-to-Site VPN between Palo Alto Firewalls

Detailed Description (for documentation):

This diagram should display two Palo Alto Firewalls (Site A and Site B) connected through the Internet (Public Network). Each firewall should connect to a LAN network with one PC.

- Site A Firewall WAN IP: **105.0.0.251**
- Site B Firewall WAN IP: **105.0.0.252**
- Site A LAN: **192.168.1.0/24**
- Site B LAN: **192.168.2.0/24**
- Label tunnel interface tunnel.1 between both sites.
Optionally, show “IKE Phase 1” and “IPSec Phase 2” across the WAN link.

INITIAL CONFIGURATIONS

=====

PaloAlto_SITE_A - Setup Guide

=====

STEP 1: Login with Default Credentials

```
login: admin      (Default username)  
password: admin   (Default password)
```

STEP 2: Change Admin Password

```
Enter old password: admin      (Current password)  
Enter new password: Ab@12345    (New strong password)  
Confirm password: Ab@12345     (Confirm new password)
```

STEP 3: Enter Configuration Mode

```
> configure          (Enter configuration mode)
```

STEP 4: Remove DHCP Client Mode

```
# delete deviceconfig system type dhcp-client           (Remove DHCP if previously enabled)
```

STEP 5: Set Static IP Address

```
# set deviceconfig system ip-address 105.0.0.251 netmask 255.255.255.0      (Assign static IP and subnet mask)
```

STEP 6: Commit Changes

```
# commit            (Apply and save config)
```

STEP 7: Exit Configuration Mode

```
# exit              (Return to operational prompt)
```

STEP 8: Verify Interface Settings

```
> show interface management    (View current IP, MAC, status, etc.)
```

=====

After setup, access GUI at:

<https://105.0.0.251>

=====

=====

PaloAlto_SITE_B - Setup Guide

=====

STEP 1: Login with Default Credentials

login: admin (Default username)
password: admin (Default password)

STEP 2: Change Admin Password

Enter old password: admin (Current password)
Enter new password: Ab@12345 (New strong password)
Confirm password: Ab@12345 (Confirm new password)

STEP 3: Enter Configuration Mode

> configure (Enter configuration mode)

STEP 4: Remove DHCP Client Mode

delete deviceconfig system type dhcp-client (Remove DHCP if previously enabled)

STEP 5: Set Static IP Address

set deviceconfig system ip-address 105.0.0.252 netmask 255.255.255.0 (Assign static IP and subnet mask)

STEP 6: Commit Changes

commit (Apply and save config)

STEP 7: Exit Configuration Mode

exit (Return to operational prompt)

STEP 8: Verify Interface Settings

> show interface management
(View current IP, MAC, status, etc.)

=====

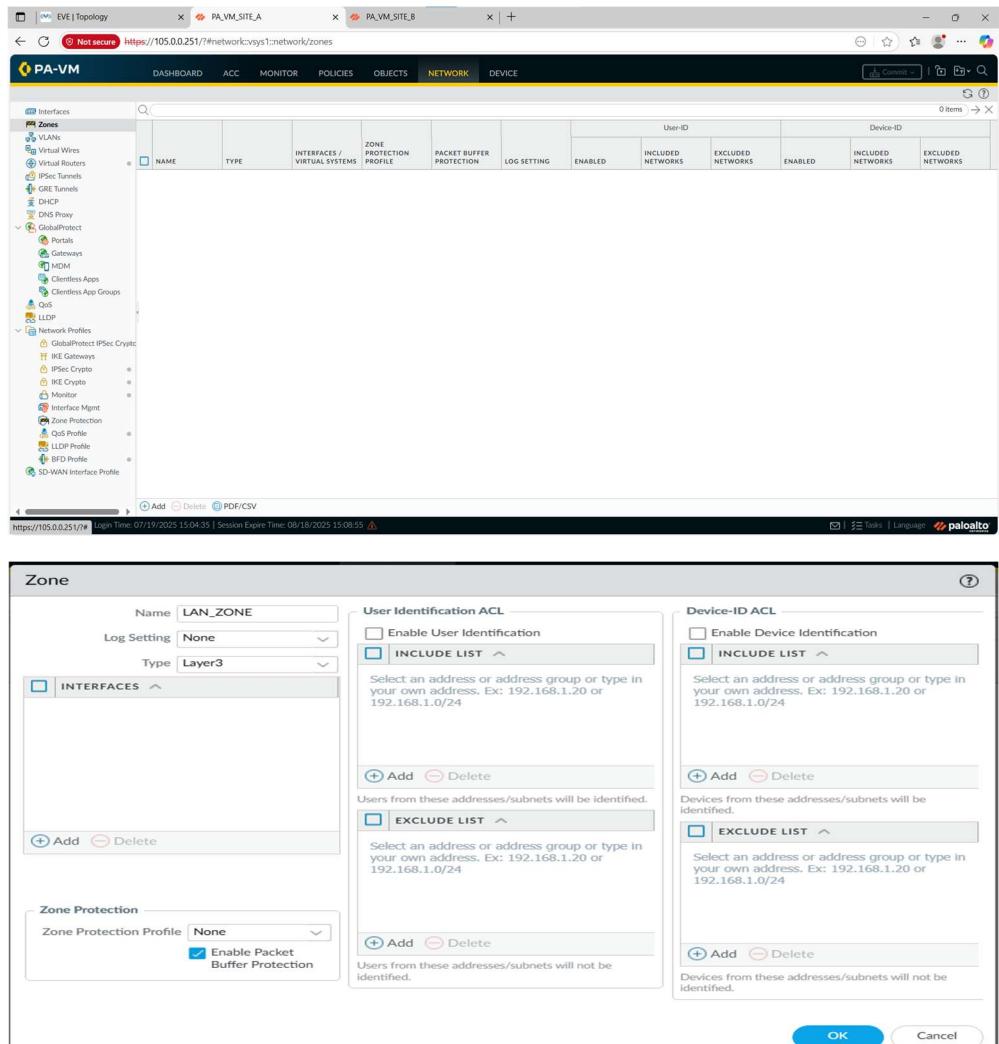
After setup, access GUI at:

<https://105.0.0.252>

=====

1. To Create Zone

Go to network >zone>add



The screenshot shows the Palo Alto Networks interface with the following details:

- Zone Creation Dialog:**
 - Name:** LAN_ZONE
 - Type:** Layer3
 - Log Setting:** None
 - Zone Protection Profile:** None (with Enable Packet Buffer Protection selected)
 - User Identification ACL:** Includes an for Enable User Identification and an for INCLUDE LIST. It also contains two 'Add' and 'Delete' buttons for address/subnet entries.
 - Device-ID ACL:** Includes an for Enable Device Identification and an for INCLUDE LIST. It also contains two 'Add' and 'Delete' buttons for address/subnet entries.
- OK and Cancel Buttons:** Located at the bottom right of the dialog.
- Network Zones Table:** Shows the newly created LAN_ZONE and another entry (WAN_ZONE) in the list.
- Page Header:** Shows tabs like DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, and a search bar.
- Page Footer:** Shows session information (Last Login Time: 07/19/2025 15:04:35, Session Expire Time: 08/18/2025 15:08:55), admin user, and a Palo Alto Networks logo.

2. To Create Tags

Go to objects>tag>add

NAME	LOCATION	COLOR	COMMENTS
Sanctioned	Predefined	Olive	
empty	Predefined	Lime	
<input checked="" type="checkbox"/> LAN_TAG			

Tag

Name:	<input type="text" value="WAN_TAG"/>
Color:	<input type="color" value="#c00000"/>
Comments:	<input type="text"/>

NAME	LOCATION	COLOR	COMMENTS
Sanctioned	Predefined	Olive	
empty	Predefined	Lime	
<input checked="" type="checkbox"/> LAN_TAG			
<input checked="" type="checkbox"/> WAN_TAG		Maroon	

3. To create objects for ip address

Objects > Addresses > Add

The screenshots illustrate the process of creating two IP address objects: LAN_INT_IP and WAN_INT_IP.

Screenshot 1: Object Creation Step 1

The first screenshot shows the 'Add' dialog for creating a new object. The 'Name' field is set to 'LAN_INT_IP', the 'Type' is selected as 'IP Netmask', and the value is '10.11.11.10/24'. A tag 'LAN_TAG' is assigned to the object.

Name	Type	Address	Tags
LAN_INT_IP	IP Netmask	10.11.11.10/24	LAN_TAG

Screenshot 2: Object Creation Step 2

The second screenshot shows the 'Add' dialog for creating another IP address object. The 'Name' field is set to 'WAN_INT_IP', the 'Type' is selected as 'IP Netmask', and the value is '1.1.10/24'. A tag 'WAN_TAG' is assigned to the object.

Name	Type	Address	Tags
WAN_INT_IP	IP Netmask	1.1.10/24	WAN_TAG

Screenshot 3: Object Creation Step 3

The third screenshot shows the final state of the 'Addresses' table. It lists the two newly created objects: 'LAN_INT_IP' and 'WAN_INT_IP'. Each object is associated with its respective IP address and tag.

Name	Location	Type	Address	Tags
LAN_INT_IP		IP Netmask	10.11.11.10/24	LAN_TAG
WAN_INT_IP		IP Netmask	1.1.10/24	WAN_TAG

4. To create interface management profile (to enable particular services for given interface)

Network >network profile >interface Mgmt

The screenshot shows the Palo Alto Networks PA-VM interface management profile configuration screen. The left sidebar lists various network objects like Zones, VLANs, Virtual Wires, and Network Profiles. The main area displays a table for Interface Management Profiles:

Name	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	USER-ID SYSLOG LISTENER-SSL	USER-ID SYSLOG LISTENER-UDP	PERMITTED IP ADDRESSES
LAN_PROFILE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								
WAN_PROFILES	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								

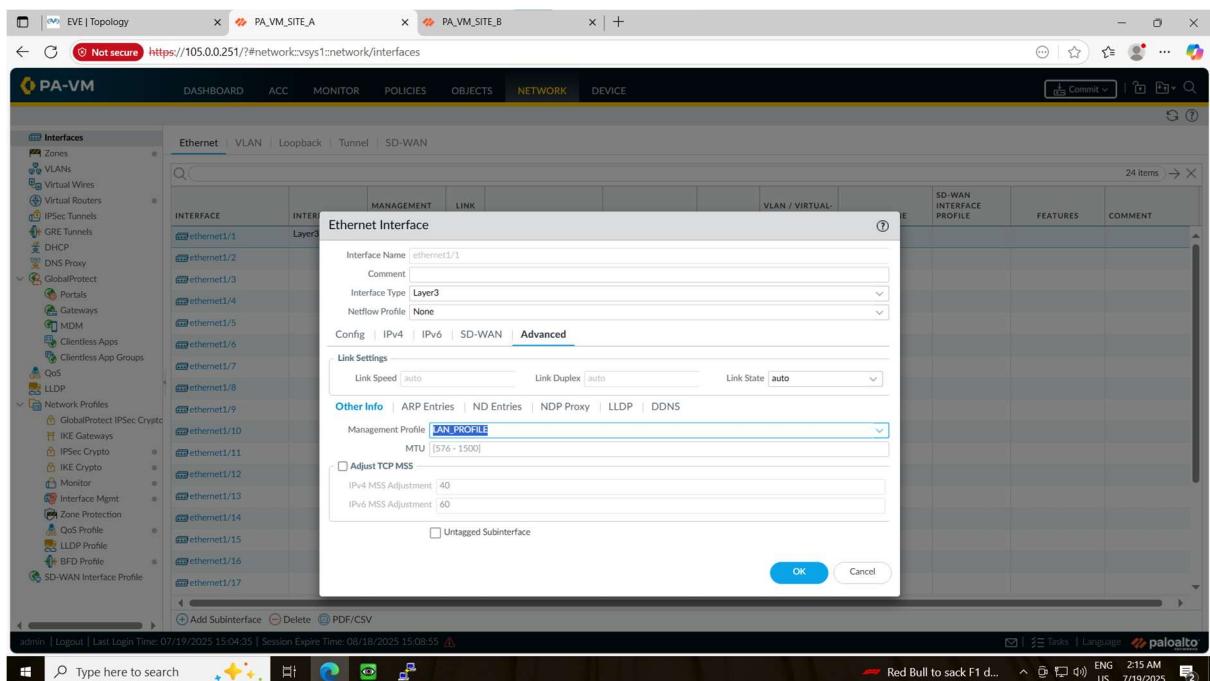
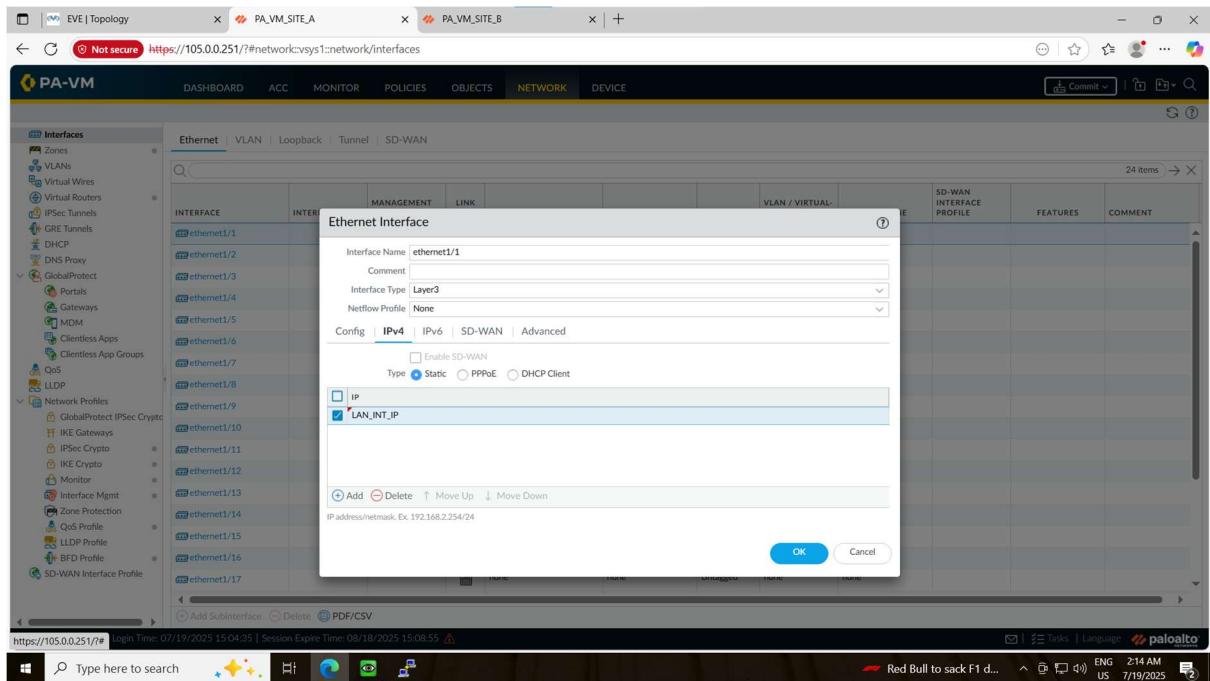
A modal window titled "Interface Management Profile" is open, showing the configuration for the LAN_PROFILE. It includes sections for "Administrative Management Services" (HTTP, HTTPS, Telnet, SSH) and "Network Services" (Ping, HTTP OCSP, SNMP, Response Pages, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP). Below the modal is a note about permitted IP addresses: "Ex: IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:1231::1 or 2001:db8:1231::/64". Buttons for "OK" and "Cancel" are at the bottom of the modal.

5. Assigning all above configuration to interface

Network>interfaces>select interface

The screenshot shows the PA-VM interface configuration page. The left sidebar contains navigation links for Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles. The main content area displays a table titled "Interfaces" with 24 items. The columns are: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, IP ADDRESS, VIRTUAL ROUTER, TAG, VLAN / VIRTUAL-WIRE, SECURITY ZONE, SD-WAN INTERFACE PROFILE, FEATURES, and COMMENT. The table lists interfaces from ethernet1/1 to ethernet1/17, each with "none" values across most columns.

The screenshot shows the PA-VM interface configuration page with the "Ethernet Interface" dialog box open over the list of interfaces. The dialog box has fields for Interface Name (set to "ethernet1/1"), Comment (empty), Interface Type (set to "Layer3"), and Netflow Profile (empty). It also has tabs for Config (selected), IPv4, IPv6, SD-WAN, and Advanced. Below these tabs is a section titled "Assign Interface To" with dropdown menus for Virtual Router (set to "default") and Security Zone (set to "LAN_ZONE"). At the bottom right of the dialog box are "OK" and "Cancel" buttons.



Apply commit for saving all changes

Check reachability from pc to firewall interface in same subnet

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\user>firewall.cpl
C:\Users\user>ncpa.cpl
Recycle C:\Users\user>ping 10.11.11.10
Pinging 10.11.11.10 with 32 bytes of data:
Reply from 10.11.11.10: bytes=32 time=6ms TTL=64
Reply from 10.11.11.10: bytes=32 time=2ms TTL=64
Reply from 10.11.11.10: bytes=32 time=2ms TTL=64
Contrary from 10.11.11.10: bytes=32 time=2ms TTL=64

Ping statistics for 10.11.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\Users\user>

```

6. For public reachability from site a to b create default routing

Network>virtual routers>add

The screenshot shows the Palo Alto Networks VM interface. The left sidebar contains navigation links for Zones, VLANs, Virtual Wires, and Virtual Routers. Under Virtual Routers, there is a sub-menu for GlobalProtect, Network Profiles, and SD-WAN Interface Profile. The main pane displays a table with columns: NAME, INTERFACES, CONFIGURATION, RIP, OSPF, OSPFv3, BGP, MULTICAST, and RUNTIME STATS. A single row is selected for the 'default' router, which has 'ethernet1/1' and 'ethernet1/2' listed under INTERFACES. The configuration status is shown as 'ECMP status: Disabled'. At the bottom of the main pane, there are buttons for Add, Delete, and PDF/CSV.

This screenshot shows the configuration of the 'default' virtual router. A modal dialog box is open, titled 'Virtual Router - default'. It is specifically configured for 'IPv4'. The 'Static Routes' tab is selected. The table header includes columns for NAME, DESTINA..., INTERFACE, TYPE, VALUE, ADMIN DISTANCE, METRIC, BFD, and ROUTE TABLE. There are currently 0 items in the route table. At the bottom of the dialog, there are buttons for Add, Delete, and Clone, along with OK and Cancel buttons.

The screenshot shows the Palo Alto Networks VM interface. In the center, a modal window is open for configuring a static route. The route is named 'WAN_ISP_ROUTE' and is set to destination '0.0.0.0'. The 'Interface' dropdown is set to 'None'. Under 'Next Hop', there is an 'IP Address' field containing '1.1.1.2'. The 'Admin Distance' is set to '10 - 240' and the 'Metric' is set to '10'. The 'Route Table' is set to 'Unicast' and the 'BFD Profile' is set to 'Disable BFD'. Below the main configuration, there is a 'Path Monitoring' section with a table for monitoring ping intervals. The table has columns for NAME, ENABLE, SOURCE IP, DESTINATION IP, PING INTERVAL(SEC), and PING COUNT. There are 'Add' and 'Delete' buttons at the bottom of the table. The 'OK' button is highlighted in blue.

NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

The screenshot shows the list of routes in the Palo Alto Networks VM interface. There is one entry for the default route, which is configured to use interface 'ethernet1/1' and has 'Static Routes: 1' listed under 'CONFIGURATION'. The 'ethernet1/2' interface is listed as having 'ECMP status: Disabled'.

NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
default	ethernet1/1	Static Routes: 1						More Runtime Stats
	ethernet1/2	ECMP status: Disabled						

Check reachability from site A to site b

```
admin@PA_VM_SITE_A# run ping source 1.1.1.10 host 2.2.2.10
PING 2.2.2.10 (2.2.2.10) from 1.1.1.10 : 56(84) bytes of data.
64 bytes from 2.2.2.10: icmp_seq=1 ttl=63 time=31.9 ms
64 bytes from 2.2.2.10: icmp_seq=2 ttl=63 time=5.83 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=63 time=7.28 ms
64 bytes from 2.2.2.10: icmp_seq=4 ttl=63 time=4.87 ms
64 bytes from 2.2.2.10: icmp_seq=5 ttl=63 time=4.95 ms
64 bytes from 2.2.2.10: icmp_seq=6 ttl=63 time=5.67 ms
^C
--- 2.2.2.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 4.872/10.092/31.933/9.799 ms
[edit]
admin@PA_VM_SITE_A#
```

7. VPN Configurations (Phase 1)

Step 1:

Network>network profile>IKE Crypto>

The screenshot shows the Palo Alto Networks interface with the URL <https://105.0.0.251/#/network/network-profiles/ike-crypto>. The left sidebar navigation includes: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, Network Profiles (GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto), Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, and SD-WAN Interface Profile. The main content area displays a table of IKE Crypto profiles:

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

At the bottom of the table are buttons for Add, Delete, Clone, PDF/CSV, and Commit.

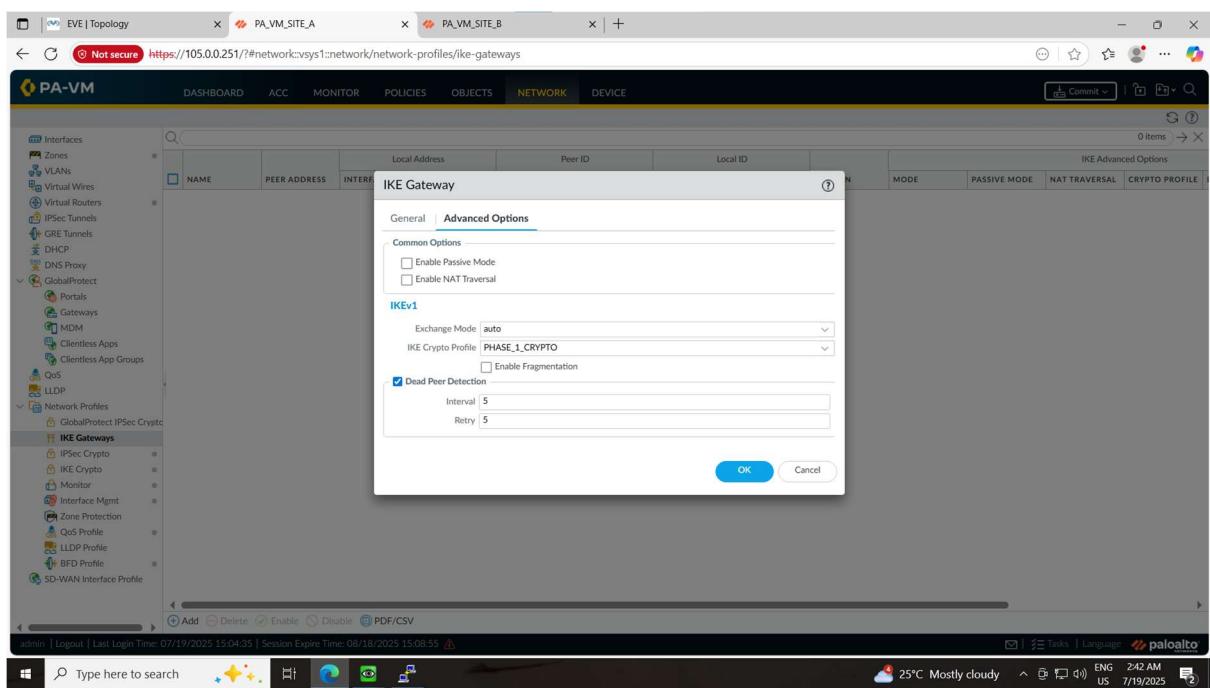
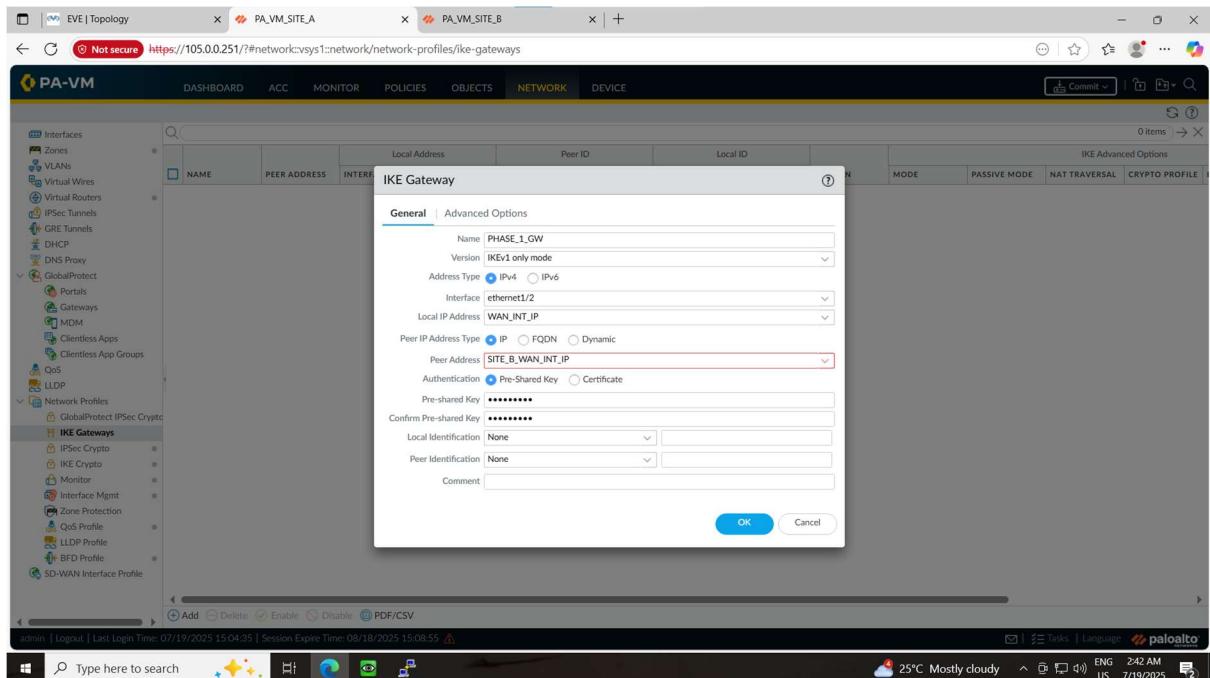
The screenshot shows the same Palo Alto Networks interface as above, but with a modal dialog box open over the table. The dialog is titled "IKE Crypto Profile" and contains fields for "Name": "PHASE_1_CRYPTO". Under "DH GROUP", "group5" and "group14" are selected. Under "ENCRYPTION", "aes-128-cbc" and "aes-192-cbc" are selected. Under "AUTHENTICATION", "sha1" and "sha256" are selected. Under "Timers", "Key Lifetime" is set to "Hours" with a value of "24", and "IKEv2 Authentication" is set to "Multiple". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Step 2:

Network>network profile>IKE Gateways

The screenshot shows the Palo Alto Networks GlobalProtect interface. The left sidebar navigation includes: Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, and Network Profiles (IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, SD-WAN Interface Profile). The main content area displays a table for 'IKE Gateways' with columns: NAME, PEER ADDRESS, INTERFACE, IP, ID, TYPE, Local ID, ID, TYPE, VERSION, MODE, PASSIVE MODE, NAT TRAVERSAL, and CRYPTO PROFILE. A search bar at the top of the table allows filtering by 'NAME'. Below the table are buttons for 'Add', 'Delete', 'Enable', 'Disable', and 'PDF/CSV'. The bottom status bar shows the URL as https://105.0.0.251/#, login time as 07/19/2025 15:04:35, session expire time as 08/18/2025 15:08:55, and the user as paloalto.

This screenshot shows the same interface as above, but with a modal dialog box open over the table. The dialog is titled 'Address' and contains fields for 'Name' (set to SITE_B_WAN_INT_IP) and 'Type' (set to IP Netmask, with value 2.2.2.10). There is also a 'Description' field and a 'Tags' dropdown. A 'Resolve' button is visible next to the Type dropdown. The background table shows a single row for 'IKE Gateway' with the name 'PHASE_1_GW'. The bottom status bar remains the same as in the previous screenshot.



The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar contains navigation links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The main pane displays the 'IKE Advanced Options' table with one item listed:

NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION	MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE
PHASE_1_GW	SITE_B_WAN_L...	ethernet1/2	WAN_INT_IP					ikev1	auto	<input type="checkbox"/>	<input type="checkbox"/>	PHASE_1_CRY...

Below the table are buttons for Add, Delete, Enable, Disable, and PDF/CSV. The bottom of the screen shows a taskbar with system information: Last Login Time: 07/19/2025 15:04:35, Session Expire Time: 08/18/2025 15:08:55, admin, Logout, 25°C Mostly cloudy, ENG US, 2:43 AM, 7/19/2025.

8. VPN Configurations (Phase 2)

Step 1:

Network>network>profile>IPsec Crypto

The screenshot shows the Palo Alto Networks interface with the URL <https://105.0.0.251/#network?vsys1:network/network-profiles/ipsec-crypto>. The left sidebar navigation includes: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps), Clientless App Groups, QoS, LLDP, Network Profiles (GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, SD-WAN Interface Profile). The main content area displays a table of IPsec Crypto profiles:

NAME	ESP/AH	ENCRYPTION	AUTHENTICATION	DH GROUP	LIFETIME	LIFESIZE
default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	

At the bottom of the page, there are buttons for Add, Delete, Clone, PDF/CSV, and a note: "https://105.0.0.251/#" Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55". The status bar at the bottom right shows: 25°C Mostly cloudy, ENG US, 2:45 AM, 7/19/2025.

The screenshot shows the Palo Alto Networks interface with the URL <https://105.0.0.251/#network?vsys1:network/network-profiles/ipsec-crypto>. The left sidebar navigation is identical to the previous screenshot. The main content area shows a modal dialog for creating a new IPsec Crypto Profile named "PHASE_2_CRYPTO". The configuration fields are as follows:

- Name: PHASE_2_CRYPTO
- IPSec Protocol: ESP
- DH Group: group5
- Encryption: aes-128-cbc
- Lifetime: Hours (set to 1)
- Enable checkbox is unchecked
- Lifesize: MB (set to 1 - 65535)
- Minimum lifetime = 3 mins
- Buttons: OK and Cancel

At the bottom of the page, there are buttons for Add, Delete, Clone, PDF/CSV, and a note: "https://105.0.0.251/#" admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55". The status bar at the bottom right shows: 25°C Mostly cloudy, ENG US, 2:45 AM, 7/19/2025.

Not secure https://105.0.0.251/?#network:vsys1:network/network-profiles/ipsec-crypto

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Interfaces Zones VLANs Virtual Wires Virtual Routers GRE Tunnels DHCP DNS Proxy GlobalProtect Portals Gateways MDM Clientless Apps Clientless App Groups QoS LLDP Network Profiles GlobalProtect IPsec Crypto IKE Gateways IPsec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection QoS Profile LLDP Profile BFD Profile SD-WAN Interface Profile

NAME	ESP/AH	ENCRYPTION	AUTHENTICATION	DH GROUP	LIFETIME	LIFESIZE
default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	
PHASE_2_CRYPTO	ESP	aes-128-cbc	sha1	group5	1 hours	

Add Delete Clone PDF/CSV

admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55

Tasks Language paloalto

25°C Mostly cloudy ENG 2:45 AM US 7/19/2025

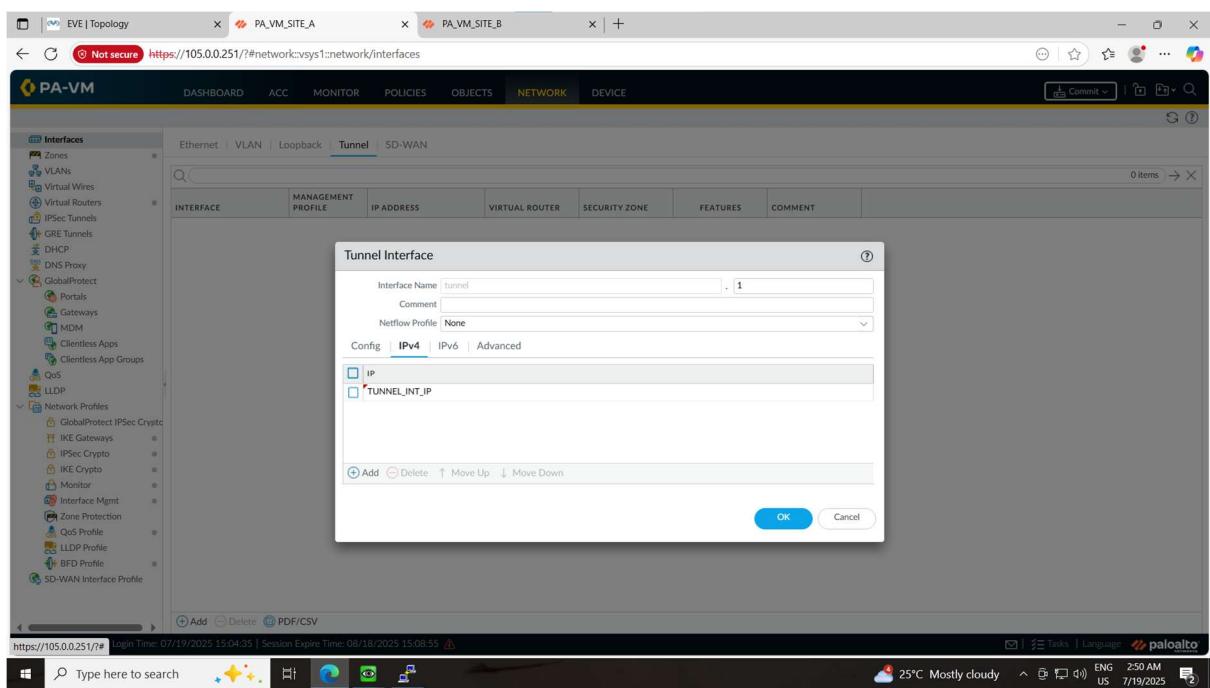
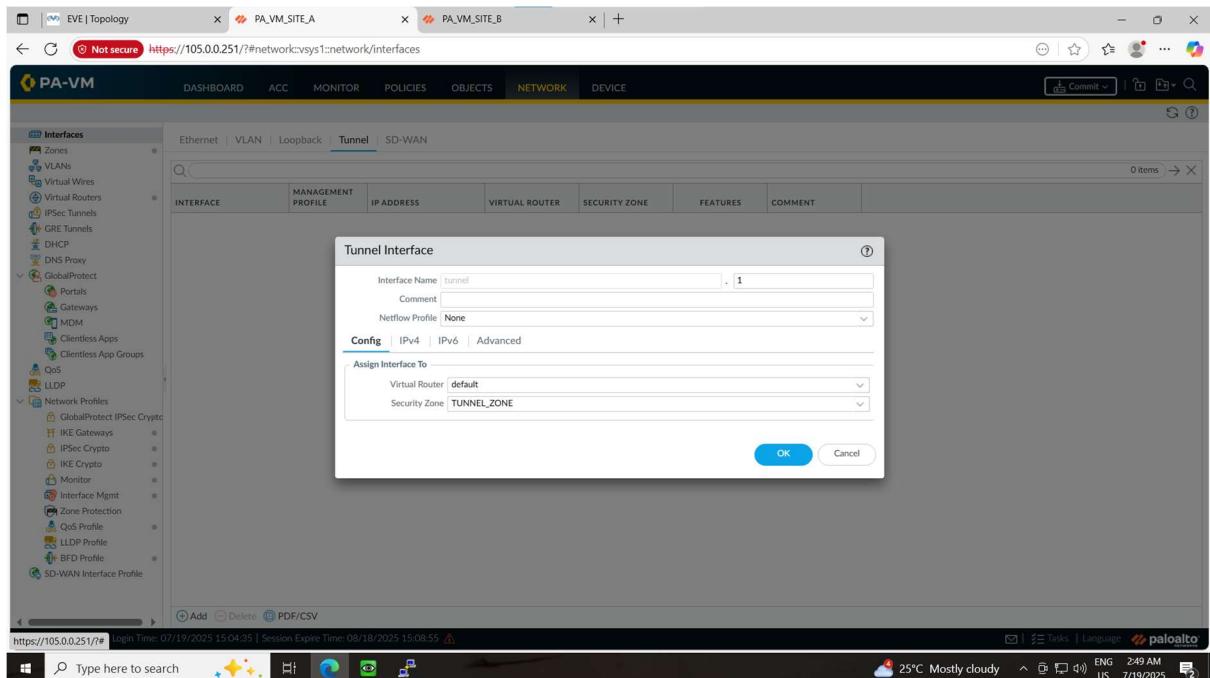
Step:2

To create tunnel

Network>interfaces>tunnel>add

The screenshot shows the Palo Alto Networks interface. The left sidebar has a tree view with 'Interfaces' expanded, showing options like Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, and Network Profiles (GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile). The main content area is titled 'Tunnel' and shows a table with columns: INTERFACE, MANAGEMENT PROFILE, IP ADDRESS, VIRTUAL ROUTER, SECURITY ZONE, FEATURES, and COMMENT. There are no items listed. At the bottom, there are 'Add', 'Delete', and 'PDF/CSV' buttons.

The screenshot shows the Palo Alto Networks interface with the Zone configuration dialog open. The dialog has fields for 'Name' (set to 'TUNNEL_ZONE'), 'Log Setting' (None), and 'Type' (Layer3). Under 'INTERFACES', there are 'INCLUDE LIST' and 'EXCLUDE LIST' sections. Under 'Zone Protection', there is an option for 'Enable Packet Buffer Protection'. On the right, there are sections for 'User Identification ACL' (with 'Enable User Identification' and 'INCLUDE LIST' checked) and 'Device-ID ACL' (with 'Enable Device Identification' and 'INCLUDE LIST' checked). Both sections have sub-sections for 'SELECT AN ADDRESS OR ADDRESS GROUP' and 'EXCLUDE LIST'. At the bottom, there are 'OK' and 'Cancel' buttons.



The screenshot shows a web-based interface for managing network configurations on a Palo Alto Networks device. The main navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The current view is under the NETWORK tab, specifically in the TUNNEL section.

In the center, there is a table titled "Tunnel Interface" with columns for INTERFACE, MANAGEMENT PROFILE, IP ADDRESS, VIRTUAL ROUTER, SECURITY ZONE, FEATURES, and COMMENT. A modal dialog box is open over the table, titled "Tunnel Interface". It contains fields for "Interface Name" (set to "tun0"), "Comment" (empty), and "Netflow Profile" (set to "None"). Below these are tabs for "Config", "IPv4", "IPv6", and "Advanced" (which is selected). Under "Other Info", it shows "Management Profile" set to "TUNNEL_PROFILE" and "MTU" set to "[576 - 1500]". At the bottom of the dialog are "OK" and "Cancel" buttons.

The left sidebar lists various network components and profiles, including Zones, VLANs, Virtual Wires, Virtual Routers, GRE Tunnels, IPSec Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, Network Profiles (GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile), and SD-WAN Interface Profile.

The bottom of the screen shows a taskbar with a search bar, system icons, and a weather widget indicating "25°C Mostly cloudy". It also displays the session information: "admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55".

Step 3:

Network>IPsec Tunnels> Add

Commit changes and try to ping

```
admin@PA-VM>
admin@PA-VM> ping source 192.168.10.1 host 192.168.10.2
PING 192.168.10.2 (192.168.10.2) from 192.168.10.1 : 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=17.7 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=7.71 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=64 time=8.89 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=64 time=7.18 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=64 time=11.0 ms
```

If it can ping, then your tunnel status will turn from red to green

As follows:

NAME	STATUS	TYPE	IKE Gateway/Satellite			Tunnel Interface				COMMENT	
			INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM		SECURITY ZONE
IPSEC_PHASE_2	Tunnel Info	Auto Key	ethernet1/2	WAN_INT_IP	SITE_B_WAN_I...	IKE Info	tunnel.1	Default (Show Routes)	vsys1	TUNNEL_ZONE	Green

The screenshot shows the Palo Alto Networks Management UI. The left sidebar has a tree view with 'IPSec Tunnels' selected. The main area displays a table of tunnels. One entry is highlighted with a green status indicator. The bottom of the screen shows a taskbar with the Windows Start button, a search bar, and various icons.

9. Create static routing for site A Lan to site b Lan communication

Network>virtual router>default>Static routes> add

The screenshot shows the Palo Alto VM interface with the following details:

- Top Bar:** EVE | Topology, PA_VM_SITE_A, PA_VM_SITE_B, Not secure, https://105.0.0.251/#network:vsys1:network/virtual-routers.
- Left Sidebar:** Interfaces, VLANs, Virtual Wires, Virtual Routers (selected), IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles.
- Middle Panel:** Shows a table for "Virtual Router - default" under "Router Settings" for "IPv4". It lists two static routes:

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
WANISP...	0.0.0.0/0	ip-address	1.1.1.2	default	10	None	unicast	
TUNNEL...	10.12.12...	ip-address	192.168.1...	default	10	None	unicast	
- Bottom Bar:** Add, Delete, PDF/CSV, admin, Logout, Last Login Time: 07/19/2025 15:04:35, Session Expire Time: 08/18/2025 15:08:55, 25°C Mostly cloudy, 3:24 AM, ENG US, 7/19/2025.

10. Create policy for communication

The screenshot shows the Palo Alto VM interface with the following details:

- Top Bar:** EVE | Topology, PA_VM_SITE_A, PA_VM_SITE_B, Not secure, https://105.0.0.251/#policies:vsys1:policies/security-rulebase.
- Left Sidebar:** Security (selected), NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, SD-WAN.
- Middle Panel:** Shows a table for "Security" rules:

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	
2 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	
- Bottom Bar:** Object : Addresses, Add, Delete, Clone, Override, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, View Rulebase as Groups, Reset Rule Hit Counter, Group, Test Policy Match, admin, Logout, Last Login Time: 07/19/2025 15:04:35, Session Expire Time: 08/18/2025 15:08:55, 25°C Mostly cloudy, 3:24 AM, ENG US, 7/19/2025.

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Security Policy Rule

NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS			
TUNNEL											

General **Source** Destination Application Service/URL Category Actions

Name: TUNNEL
Rule Type: universal (default)
Description:
Tags:
Group Rules By Tag: None
Audit Comment:
Audit Comment Archive:

OK Cancel

Object : Addresses + Add Delete Close Overrides Report Events Difficult Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy Match Activate Windows

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Security Policy Rule

NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS			
TUNNEL											

General **Source** **Destination** Application Service/URL Category Actions

Any SOURCE ZONE LAN_ZONE TUNNEL_ZONE

Add Delete Add Delete Add Delete Add Delete Negate OK Cancel

Object : Addresses + Add Delete Close Overrides Report Events Difficult Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy Match Activate Windows

Security Policy Rule

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Security Policy Rule				any								Allow

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
TUNNEL	none	universal	LAN_ZONE	any	any	any	LAN_ZONE	any	any	any	application-...	Allow
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Now commit all changes

REPEAT THE SAME STEPS FROM 1-10 ON PALOALTO VM SITE_B DEVICE

Now you will be able to ping from site A pc to site B pc

The screenshot shows a Windows Command Prompt window titled "QEMU (Win4)" running on a host machine. The window displays the output of several ping commands. The first command, "ping 10.12.12.6", shows four request timed out errors. The second command, "ping statistics for 10.12.12.6", shows four packets sent, zero received, and four lost (100% loss). The third command, "ping 10.12.12.6", shows four replies from 10.12.12.6 with varying times (56ms, 11ms, 9ms, 11ms) and TTLs (126). The fourth command, "ping statistics for 10.12.12.6", shows four packets sent, four received, and zero lost (0% loss), with approximate round trip times of 9ms, 56ms, and an average of 21ms. The Command Prompt window has a sidebar on the left labeled "TYPE" with categories "universal", "intrazone", and "interzone". The bottom right corner of the window shows the date and time as 3/29/2025 and 5:12 PM.

```
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 13ms, Average = 7ms  
C:\Users\user>ping 10.12.12.6  
Pinging 10.12.12.6 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Ping statistics for 10.12.12.6:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\Users\user>  
C:\Users\user>ping 10.12.12.6  
Pinging 10.12.12.6 with 32 bytes of data:  
Reply from 10.12.12.6: bytes=32 time=56ms TTL=126  
Reply from 10.12.12.6: bytes=32 time=11ms TTL=126  
Reply from 10.12.12.6: bytes=32 time=9ms TTL=126  
Reply from 10.12.12.6: bytes=32 time=11ms TTL=126  
Ping statistics for 10.12.12.6:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 9ms, Maximum = 56ms, Average = 21ms  
C:\Users\user>
```