

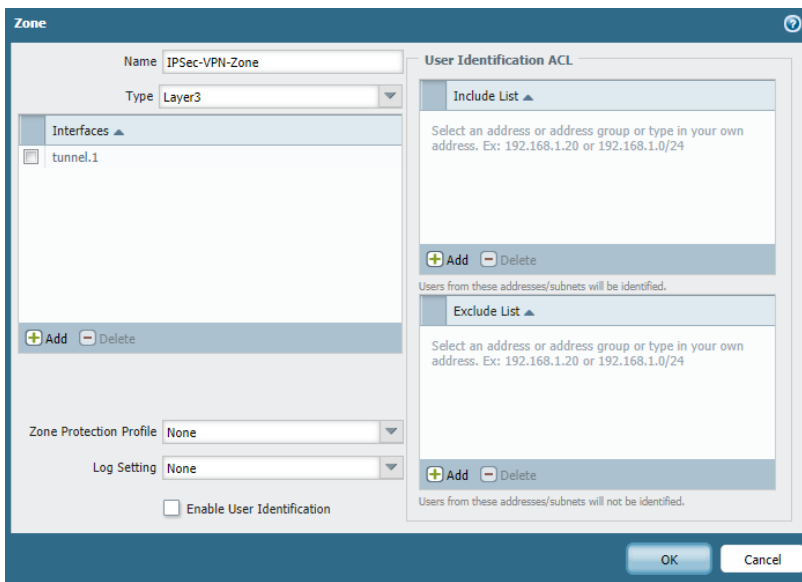
IP Address: 192.168.110.0/24  
 Default Gateway: 192.168.110.1  
 Subnet mask: 255.255.255.0

IP Address: 10.10.10.0/24  
 Default Gateway: 10.10.10.1  
 Subnet mask: 255.255.255.0

| Palo Alto Network Firewall |                  |
|----------------------------|------------------|
| Eth1/3 – Outside (WAN)     | 98.174.158.92    |
| Eth1/4 – Inside (LAN)      | 192.168.110.1    |
| Tunnel Interface           | tunnel.1         |
| Local Network              | 192.168.110.0/24 |
| Remote Network             | 10.10.10.0/24    |
| WTI Network                |                  |
| ppp0 – Cell (i2gold)       | 166.130.84.115   |
| Eth0 – Inside (LAN)        | 10.10.10.1       |
| Tunnel Name                | tunnel.1         |
| Local Network              | 10.10.10.0/24    |
| Remote Network             | 192.168.110.0/24 |

1. Creating a security zone on Palo Alto Firewall

First, we need to create a separate security zone on Palo Alto Firewall. In order to configure the security zone, you need to go **Network >> Zones >> Add**. Here, you need to provide the Name for the Security Zone. You can provide any name as per your convenience.



## 2. Creating a tunnel interface on Palo Alto Firewall

You need to define a separate virtual tunnel interface for IPsec Tunnel. To define the tunnel interface, Go to **Network >> Interfaces >> Tunnel**. Select the **Virtual Router**, an *IPsec-VR* in my case. Also, in **Security Zone** field, you need to select the security zone as defined in Step 1.

Interface Name: **tunnel.1**

Virtual Router: **IPSec-VR**

Security Zone: **IPSec-VPN-Zone**

The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' is 'tunnel.1'. The 'Netflow Profile' is set to 'None'. The 'Management Profile' is 'Outside'. The 'MTU' is set to '[576 - 1500]'. Under 'Assign Interface To', the 'Virtual Router' is 'IPSec-VR' and the 'Security Zone' is 'IPSec-VPN-Zone'. There are 'OK' and 'Cancel' buttons at the bottom right.

## 3. Defining IKE Crypto Profile [Phase 1 of IPsec Tunnel]

Now, you need to define Phase 1 of the IPsec Tunnel. You need to go **Network >> Network Profiles >> IKE Crypto >> Add**.

Name: **WTI\_IKECrypto**

DH Group: **group14**

Encryption: **aes256**

Authentication: **sha256**

Lifetime: **8 Hours**

The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' is 'WTI\_IKECrypto'. The 'DH Group' is 'group14'. The 'Encryption' is 'aes256'. The 'Authentication' is 'sha256'. The 'Lifetime' is set to 'Hours' and '8'. There are 'OK' and 'Cancel' buttons at the bottom right.

#### 4. Defining the IPsec Crypto Profile [Phase 2 of IPsec Tunnel]

Now, you need to define Phase 2 of the IPsec Tunnel. You need to go **Network >> Network Profiles >> IPsec Crypto >> Add**.

Name: **WTI\_IPSECcrypto**

IPsec Protocol: **ESP**

Encryption: **aes256**

Authentication: **sha256**

DH Group: **group14**

Lifetime: **1 Hours**

The screenshot shows the 'IPsec Crypto Profile' configuration window. The 'Name' field is set to 'WTI\_IPSECcrypto'. The 'IPsec Protocol' is set to 'ESP'. The 'DH Group' is set to 'group14'. The 'Lifetime' is set to 'Hours' and '1'. The 'Lifesize' is set to 'MB' and '[1 - 65535]'. There are two sections for configuration: 'Encryption' and 'Authentication'. The 'Encryption' section has a list with 'aes256' selected. The 'Authentication' section has a list with 'sha256' selected. Below each list are buttons for '+ Add', '- Delete', 'Move Up', and 'Move Down'. At the bottom right are 'OK' and 'Cancel' buttons.

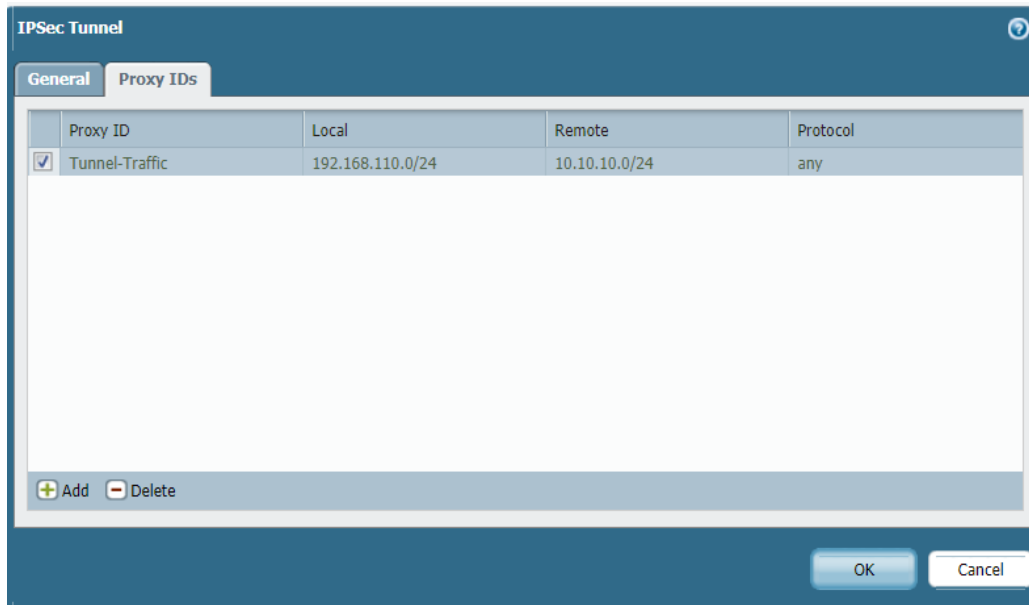
#### 5. Defining the IKE Gateway Profile

Now, you need to go **Network >> Network Profiles >> IKE Gateways >> Add**. In **General** Tab, You need to define the name of the IKE Gateway Profile. In Interface field, you need to define your Internet-facing Interface, in my case, Ethernet 1/3, which has **98.174.158.92** IP Address. Select Peer Type as **Static**. Define the Peer IP Address, in my case **166.130.84.115 (i2gold Cell)**. Select the Authentication Method, i.e. Pre Shared Key or Certificate. In this scenario, I'm using the Pre-shared Key as **WTI949**. Define the Local and Peer IP address in the **Local Identification** and **Peer Identification** field and select IKE Crypto Profile as **WTI\_IKECrypto**.

## 6. Creating the IPsec Tunnel

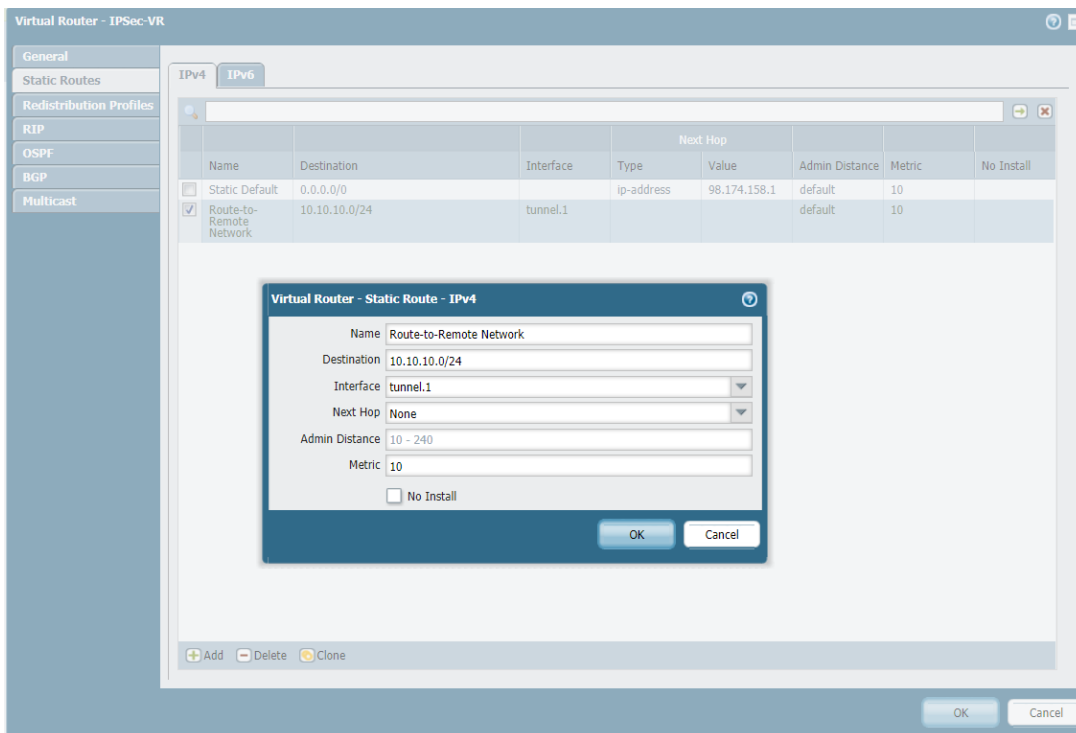
We have defined IKE Gateway and IPsec Crypto profile for our IPsec Tunnel. Now, we have to define the IPsec Tunnel. Go to **Network >> IPsec Tunnels >> Add**.

Go to the Proxy IDs Tab, and define Local and Remote Networks. In this scenario, I'm using 192.168.110.0/24 and 10.10.10.0/24 in LAN Networks.



## 7. Configuring Route for Peer end Private Network

Now, you need to provide a static route for Peer end Private Network. Just go to **Network >> Virtual Routers >> Default >> Static Routes >> Add**. Select the Name for this Route and define the destination network for this route, i.e. 10.10.10.0/24 in this example.



## 8. Creating the Security Policy for IPSec Tunnel Traffic.

Now, you need to create a security profile that allows the traffic from VPN Zone to Trust Zone. You need to Go **Policies >> Security >> Add** to define a new Policy.

### Security Policy overview

| Name                     | Tag  | Source         |                                 |      |             | Destination    |                                 | Application | Service | Action | Profile | Options |
|--------------------------|------|----------------|---------------------------------|------|-------------|----------------|---------------------------------|-------------|---------|--------|---------|---------|
|                          |      | Zone           | Address                         | User | HIP Profile | Zone           | Address                         |             |         |        |         |         |
| allow-ike-ipsec          | none | Outside        | 166.130.84.115<br>98.174.158.92 | any  | any         | Outside        | 116.130.84.115<br>98.174.158.92 | any         | any     | ✓      | none    |         |
| allow-tunnel-traffic-in  | none | IPSec-VPN-Z... | 10.10.10.0/24                   | any  | any         | Inside         | 192.168.110.0/24                | any         | any     | ✓      | none    |         |
| allow-tunnel-traffic-out | none | Inside         | 192.168.110.0/24                | any  | any         | IPSec-VPN-Z... | 10.10.10.0/24                   | any         | any     | ✓      | none    |         |
| Inside To Outside        | none | Inside         | any                             | any  | any         | Outside        | any                             | any         | any     | ✓      | none    |         |

## 1. Creating NAT to allow Inside (LAN) access Internet.

### NAT overview

| Name              | Tag  | Original Packet |                  |                       |                |                     |         | Translated Packet                                      |                         |
|-------------------|------|-----------------|------------------|-----------------------|----------------|---------------------|---------|--|-------------------------|
|                   |      | Source Zone     | Destination Zone | Destination Interface | Source Address | Destination Address | Service | Source Translation                                     | Destination Translation |
| Inside To Outside | none | Inside          | Outside          | any                   | any            | any                 | any     | dynamic-ip-and-port<br>ethernet1/3<br>98.174.158.92/24 | none                    |

We finished the configuration of the IPSec tunnel in the Palo Alto firewall. Now, we will configure the IPSec tunnel in WTI unit

WTI IPsec Setting

| IPSEC_CLIENT VPN DETAILS [tunnel.1]                  |   |
|--|---|
| Enable:  | <input type="checkbox"/> On <input type="button" value="v"/>                                      |
| Tunnel Name:   | <input type="text" value="tunnel.1"/>   |
| Security:  | <input type="text" value="Pre-shared Secret (Static Key File)"/> <input type="button" value="v"/> |
| Authentication Type:                                 | <input type="text" value="ESP"/> <input type="button" value="v"/>                                 |
| Left Address:  | <input type="text" value="166.130.84.115"/> #Cell (i2gold) Unit address                           |
| Left ID:   | <input type="text" value="166.130.84.115"/> #IKEID Sent by Cell (i2gold)                          |
| Left Subnet:   | <input type="text" value="10.10.10.0/24"/> #Subnet Local Network behind WTI                       |
| Right Address:                                       | <input type="text" value="98.174.158.92"/> #Palo Alto outside address                             |
| Right ID:  | <input type="text" value="98.174.158.92"/> #IKEID Sent by Palo Alto                               |
| Right Subnet:  | <input type="text" value="192.168.110.0/24"/> #Subnet Local Network behind Palo Alto              |
| Tunnel Options:                                      | <input type="checkbox"/> (Show Options)   |
| Option 1:  | <input type="text" value="keyexchange"/> <input type="text" value="ikev1"/>                       |
| Option 2:  | <input type="text" value="ike"/> <input type="text" value="aes256-sha256-modp2048"/>              |
| Option 3:  | <input type="text" value="esp"/> <input type="text" value="aes256-sha256-modp2048"/>              |
| Pre-Shared Key                                       | <input type="text" value="WTI949"/>   |
| <input type="button" value="Change VPN Parameters"/> |   |

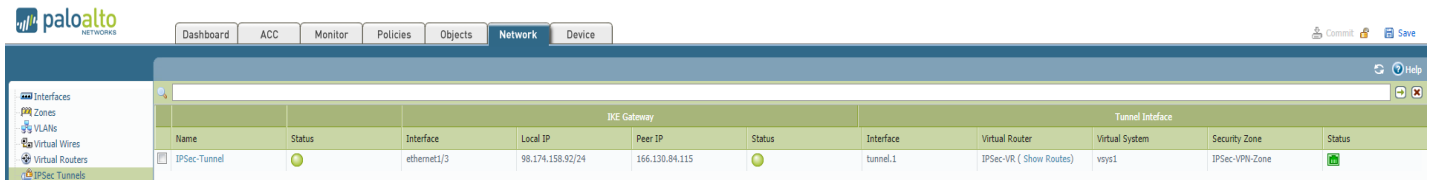
## Set IPTABLES on Eth0

In this Example:

- ppp0 is Cell (i2gold)
- Eth0 is inside (LAN)

1. `iptables -A INPUT -i eth0 -j ACCEPT #Allow traffic from the LAN side`
2. `iptables -A INPUT -i ppp0 -j ACCEPT #Always accept loopback traffic`
3. `iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT #Allow established connections`
4. `iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE #Masquerade`
5. `iptables -A FORWARD -i ppp0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT #Forwarding`
6. `iptables -A FORWARD -i eth0 -o ppp0 -j ACCEPT #Allow outgoing connections from the LAN side`
7. `iptables -t nat -I POSTROUTING 1 -m policy --pol ipsec --dir out -j ACCEPT #NAT IPsec Traffic`

## Monitoring VPN Session in Palo Alto



The screenshot shows the Palo Alto Networks management console interface. The navigation menu on the left includes Interfaces, Zones, VLAGs, Virtual Wires, Virtual Routers, and IPsec Tunnels. The main content area displays a table of VPN sessions under the 'Network' tab.

|              |                                      | IKE Gateway |                  |                | Tunnel Interface                     |           |                         |                |                |                                      |
|--------------|--------------------------------------|-------------|------------------|----------------|--------------------------------------|-----------|-------------------------|----------------|----------------|--------------------------------------|
| Name         | Status                               | Interface   | Local IP         | Peer IP        | Status                               | Interface | Virtual Router          | Virtual System | Security Zone  | Status                               |
| IPsec-Tunnel | <span style="color: green;">●</span> | ethernet1/3 | 98.174.158.82/24 | 166.130.84.115 | <span style="color: green;">●</span> | tunnel.1  | IPSec-VR ( Show Routes) | vsys1          | IPSec-VPN-Zone | <span style="color: green;">●</span> |

## Monitoring VPN Session in WTI

```
CPM> /bash ipsec status
Security Associations <1 up, 0 connecting>:
tunnel.1[1]: ESTABLISHED 2 minutes ago, 166.130.84.115[166.130.84.115]..98.174.158.92[98.174.158.92]
tunnel.1[1]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c117e769_i b0b96ce9_o
tunnel.1[1]: 10.10.10.0/24 == 192.168.110.0/24
```