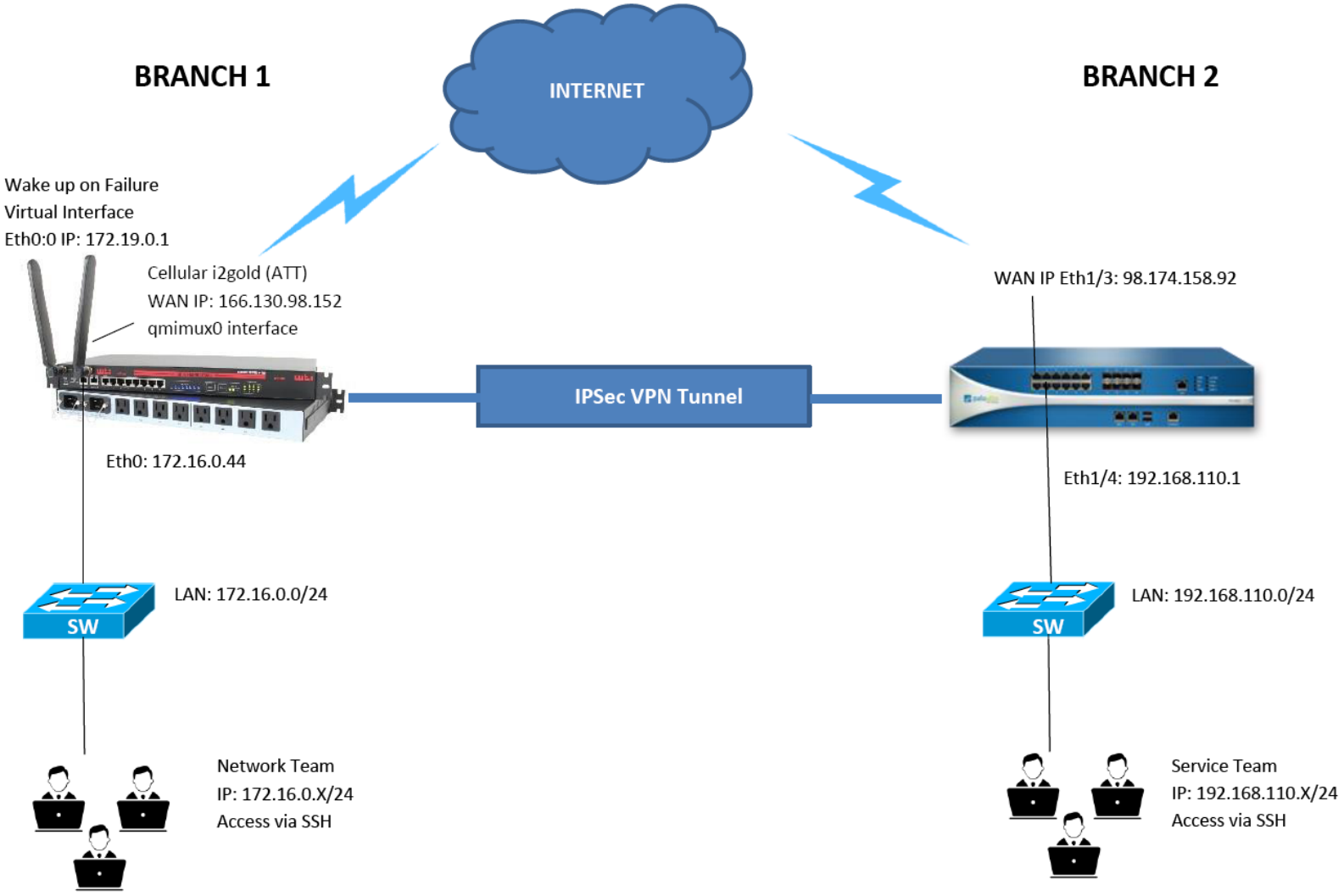
IPSec VPN Wake up on failure Cellular with Palo Alto



In this scenario, the Network Team in Branch1 lost connection and can't access the WTI unit via SSH from their LAN network to perform a daily configuration and update. The service team needs to access the attached devices from Branch 2. They can get access using the "wake-on failure" feature. The WTI unit has detected the LAN failure and has turned on the cell interface. The cell interface can be accessed securely because of an IPSec VPN Tunnel that has been established between the WTI and Palo Alto's IPSEC server.

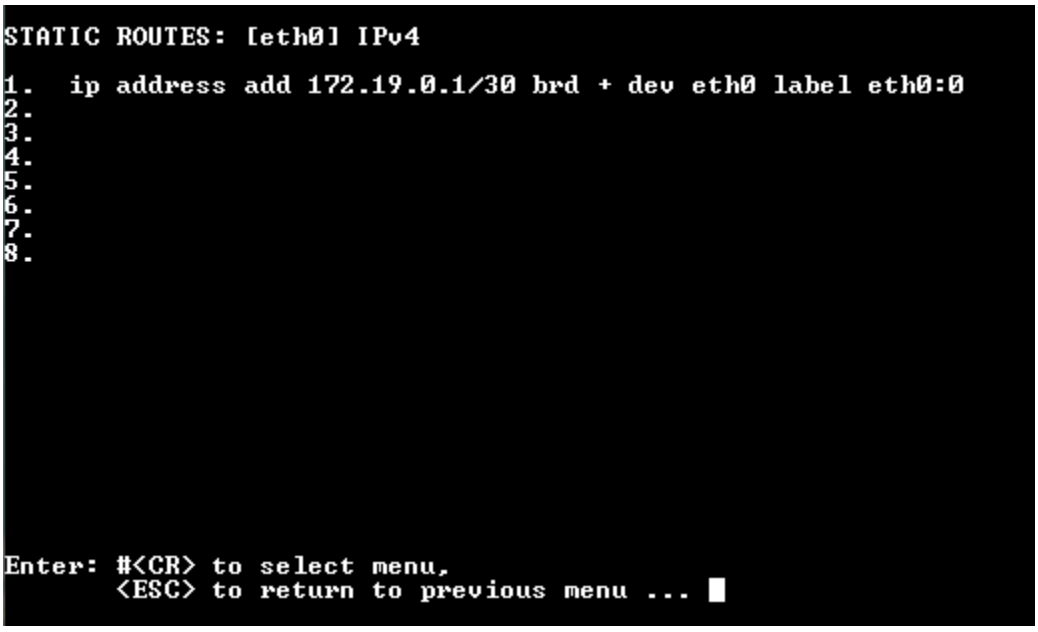
Setup configuration requirements:

WTI Network	
qmimux0 or ppp0 – Cell (i2gold)	166.130.98.152
Eth0:0 – Virtual Interface Wakeup on Failure	172.19.0.1/30
Eth0 – Inside (LAN)	172.16.0.44
Local Network (LAN)	172.16.0.0/24
Remote Network (Peer)	192.168.110.0/24
Palo Alto Network	
Eth1/3 – Outside (WAN)	98.174.158.92
Eth1/4 – Inside (LAN)	192.168.110.1
Tunnel Interface name	tunnel.1
Local Network (LAN)	192.168.110.0/24
Remote Network (Peer WOF Virtual Network)	172.19.0.0/30

Create Eth0:0 Virtual IP Interface for Wakeup on Failure

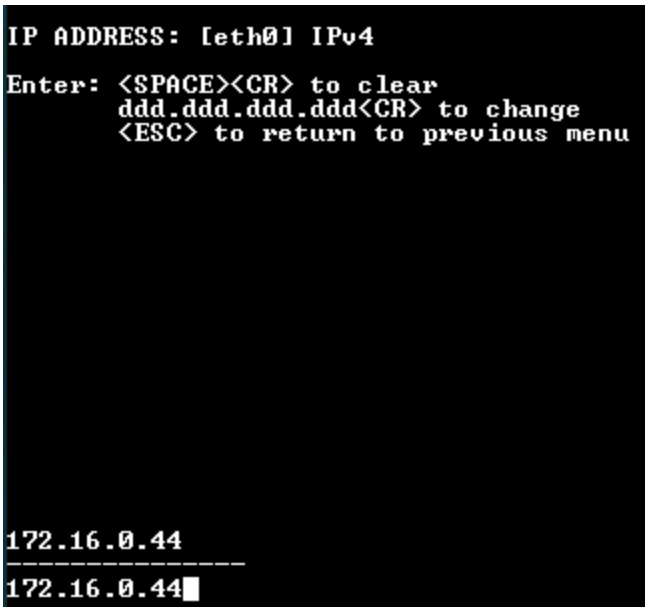
To create an Eth0:0 virtual IP Interface from WTI CLI, type /N and hit enter then select 6 for Static Route and enter the command mentioned below to create a virtual IP interface and assign an IP Address to it. In this example, we use IP Address 172.19.0.1 as our IPSec VPN wakeup on failure and assign it to the eth0:0 interface.

ip address add 172.19.0.1/30 brd + dev eth0 label eth0:0



Assign (LAN) IP Address on Eth0

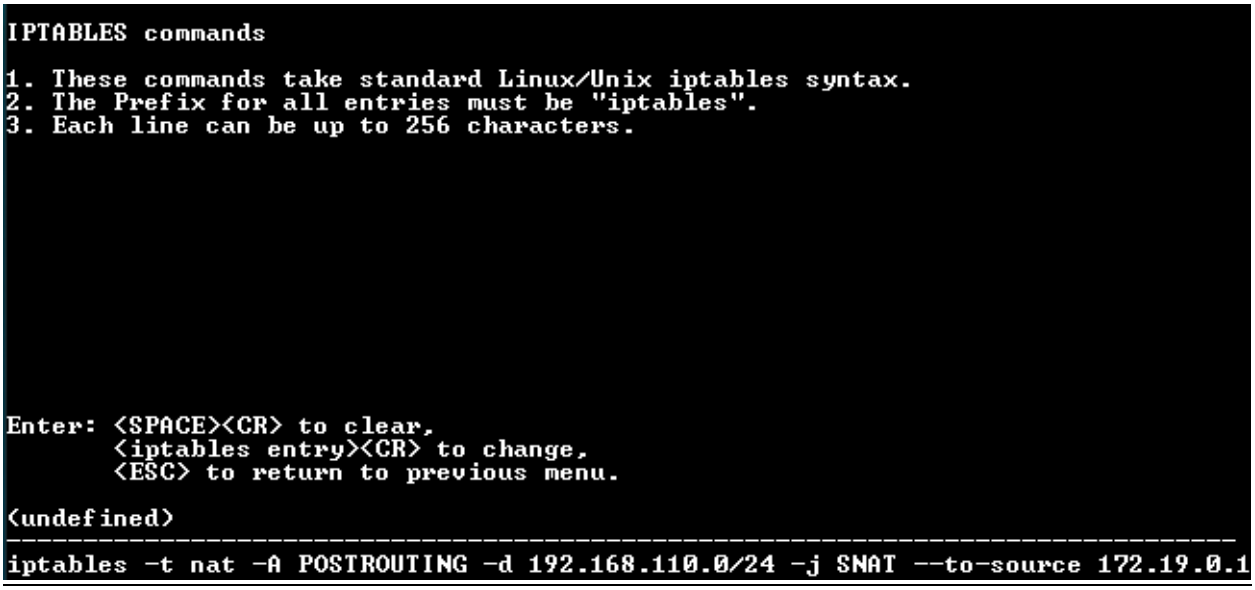
At the WTI CLI, type /N and hit enter then select 1 for IP Address and enter an IP Address as 172.16.0.44 then hit enter.



Create a NAT in IP TABLES

type /N and hit enter then select 5 for IP Tables enter the command mentioned below to allow remote peer (LAN) to access.

iptables -t nat -A POSTROUTING -d 192.168.110.0/24 -j SNAT --to-source 172.19.0.1



Enable Wakeup on Failure from Cell interface

To configure WTI cell wakeup on Failure from WTI CLI, type /cell and hit enter select 4 for wakeup on Failure.

1. Enable:	**Enabled**	
2. Interface to Monitor	**eth0**	(LAN interface)
3. Primary Address/Host to Ping	**172.19.0.1**	(virtual IP Address)
8. Auto Discovery	**On**	
12. Re-enable Wakeup on Failure	**Yes**	

The other parameters will be as default setting as below:

```
WAKEUP ON FAILURE:

The Wakeup On Failure feature allows a WTI unit with a cellular modem to put
its modem in a non connected sleep state, with its wired ethernet port(s)
acting as the unit's primary network interfaces. The modem will only wakeup
when certain failure conditions are detected on specified wired ethernet ports.

1.  Enable:                          Enabled
2.  Interface to Monitor:            eth0
3.  Primary Address/Host to Ping:    172.19.0.1
4.  Secondary Address/Host to Ping: (undefined)
5.  Ping Interval:                   60 Sec
6.  Interval after Failed Ping:      10 Sec
7.  Consecutive Failures:            05
8.  Auto Recovery:                   On
9.  Ethernet Default Gateway Port:   eth0
10. Ethernet Default Gateway Addr:  (undefined)
11. Sleep Mode:                      Attach
12. Re-enable Wakeup on Failure
13. Ping Test


Enter: #<CR> to change,
       <ESC> to return to previous menu ...
```

Configure WTI IPSEC VPN

To configure or setup IPSec VPN from WTI CLI, type /vpn and hit enter. Select 1 IPsec (Site-To-Site) to create a tunnel connection.

1. Enable:	**On**	
2. Tunnel Name:	**tunnel.1**	
3. Security:	**Pre-shared Secret (Static Key File)**	
4. Authentication Type:	**ESP**	
5. Left Address:	**166.130.98.152**	#WTI (Cell i2Gold) IP Address
6. Left ID:	**166.130.98.152**	#WTI (Cell i2Gold) IP Address
7. Left Subnet:	**172.19.0.1/30**	#Virtual LAN Subnet Wakeup on Failure
8. Right Address:	**98.174.158.92**	#Palo Alto WAN IP Address
9. Right ID:	**98.174.158.92**	#Palo Alto WAN IP Address
10. Right Subnet:	**192.168.110.0/24**	#Palo Alto LAN Subnet
11. Force Encaps:	**Off**	
12. Pre-shared Key:	**(Defined)**	#(Enter your pre-share key)
13. Tunnel Option	**(Defined)**	

Below 1-4 are the Tunnel options parameter setup

1. **keyexchange**

   Parameter: **keyexchange**

   Value: **ikev1**

```
1.    Parameter:            keyexchange
2.    Value:                ikev1
```

2. **Ike**

   Parameter: **ike**

   Value: **aes256-sha256-modp2048**

```
1.    Parameter:            ike
2.    Value:                aes256-sha256-modp2048
```

3. **esp**

   Parameter: **esp**

   Value: **aes256-sha256-modp2048**

```
1.    Parameter:            esp
2.    Value:                aes256-sha256-modp2048
```

4. **auto** #auto start VPN session

   Parameter: **auto**

   Value: **start**

```
1.    Parameter:            auto
2.    Value:                start
```

14 and 15 leave as default setting. Below is the overview of IPSec configuration.

```
IPSEC CLIENT VPN ASSOCIATED DETAILS: [tunnel.1] IPv4/IPv6

1.    Enable:               On
2.    Tunnel Name:          tunnel.1
3.    Security:             Pre-shared Secret (Static Key File)
4.    Authentication Type:  ESP
5.    Left Address:         166.130.98.152
6.    Left ID:              166.130.98.152
7.    Left Subnet :         172.19.0.1/30
8.    Right Address:        98.174.158.92
9.    Right ID:             98.174.158.92
10.   Right Subnet:         192.168.110.0/24
11.   Force Encaps:         Off
12.   Pre-Shared Key:       (defined)
13.   Tunnel Options:       (defined)
14.   Associated Menu:      (default)
15.   EAP User Menu:        (undefined)
16.   Runtime Status:



Enter: #<CR> to change,
       <ESC> to exit and save configuration ...
```

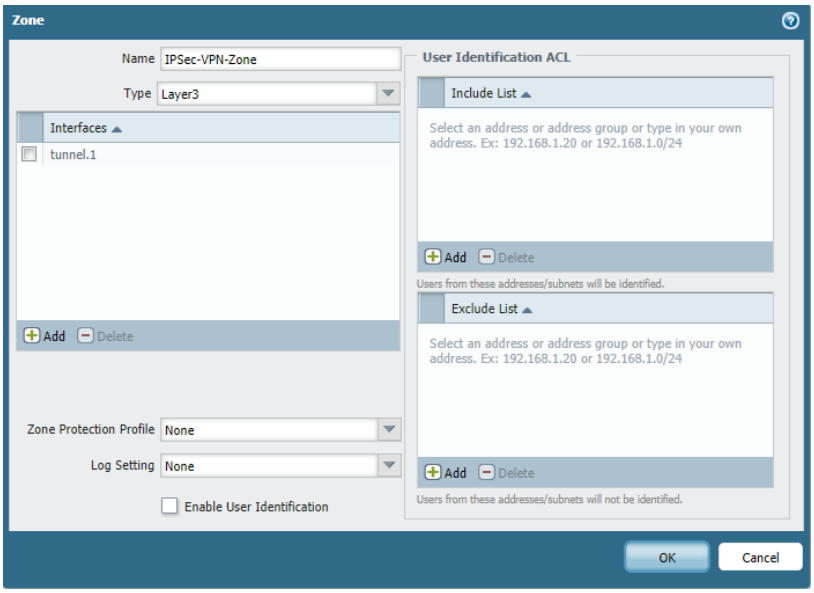
To verify if the virtual interface created by running the command below from WTI CLI

To check he VPN connection from WTI CLI
/bash ipsec status
/bash ipsec statusall

Palo Alto Setup Configuration

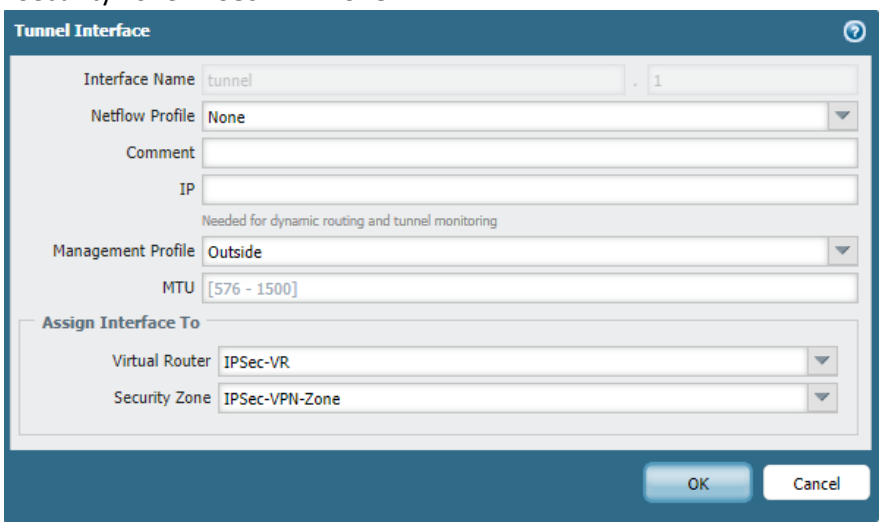
1. Creating a security zone on Palo Alto Firewall

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



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.

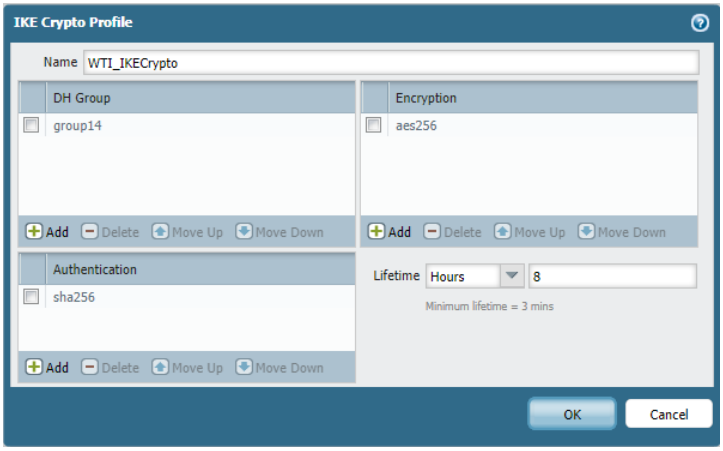
Interface Name: **tunnel.1**
Virtual Router: **IPSec-VR**
Security Zone: **IPSec-VPN-Zone**



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**.

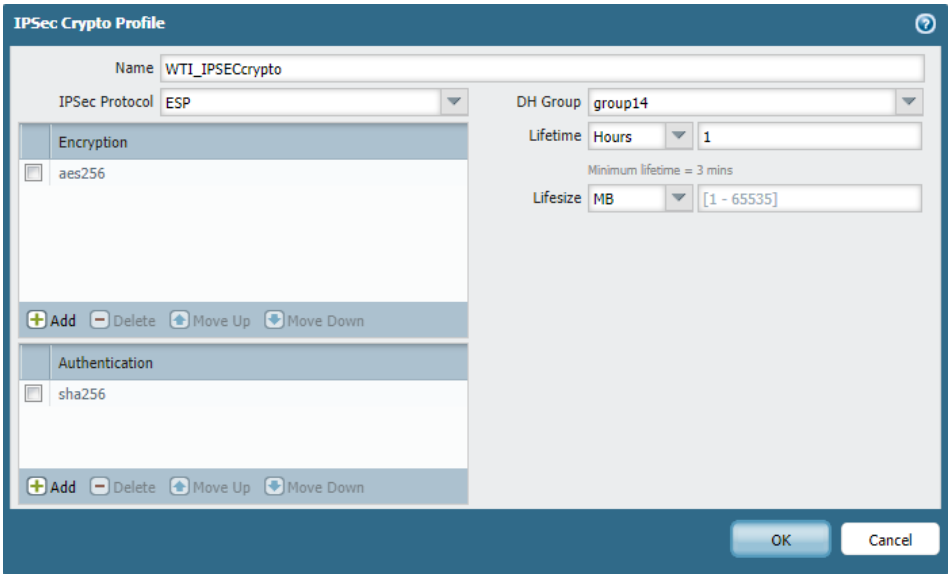
Name: **WTI_IKECrypto**
DH Group: **group14**
Encryption: **aes256**
Authentication: **sha256**
Lifetime: **8 Hours**



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

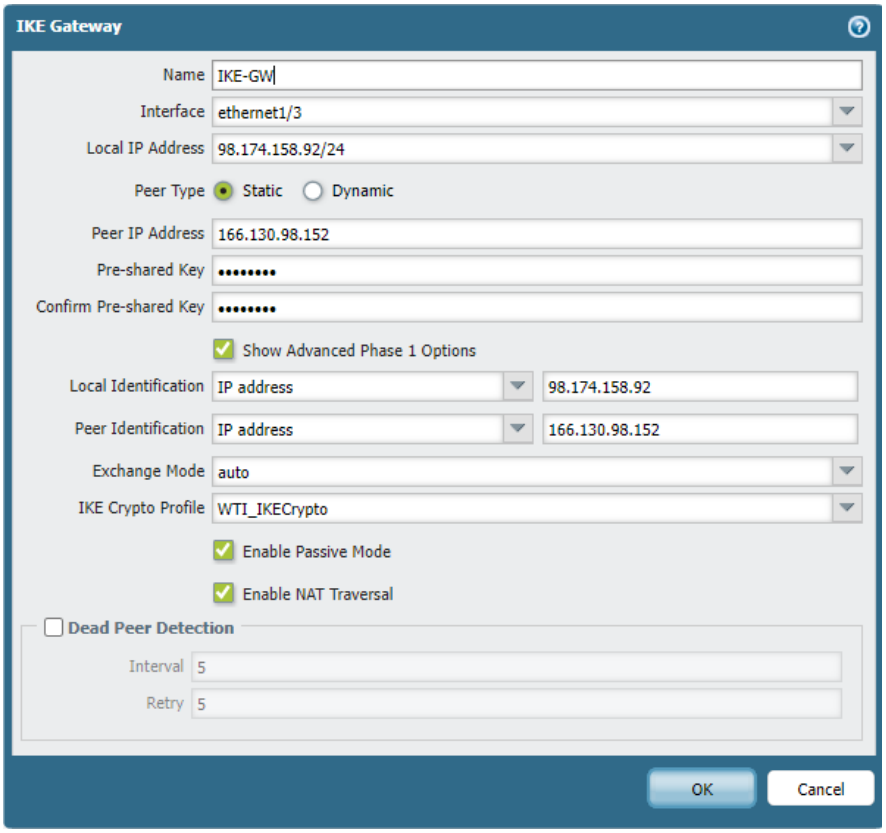
Now, you need to define Phase 2 of the IPSec Tunnel. You need to go **Network** >> **Network Profiles** >> **IPSec Crypto** >> **Add**.

Name: **WTI_IPSECcrypto**
IPSec Protocol: **ESP**
Encryption: **aes256**
Authentication: **sha256**
DH Group: **group14**
Lifetime: **1 Hours**



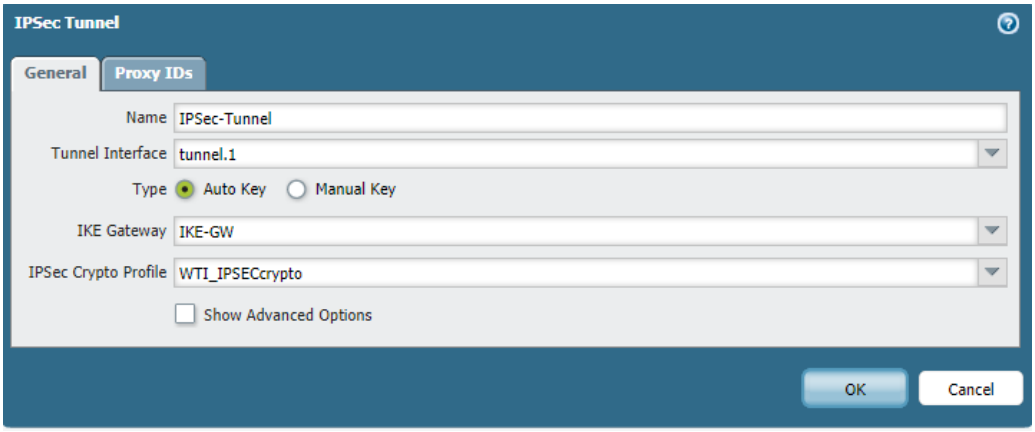
5. Defining the IKE Gateway Profile

Now, you need to go to **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 this example, IP Address of Ethernet 1/3 is **98.174.158.92**. Select Peer Type as **Static**. Define the Peer IP Address, in this example**,166.130.98.152 (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**.

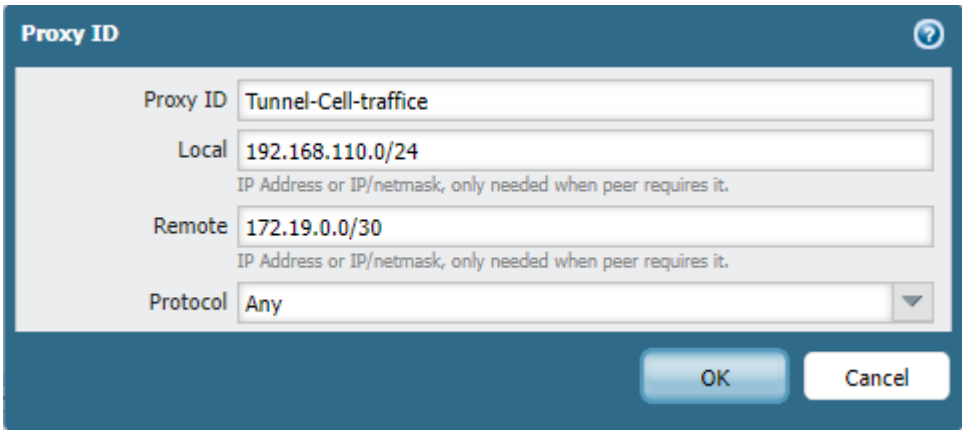


6. Creating the IPSec Tunnel

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

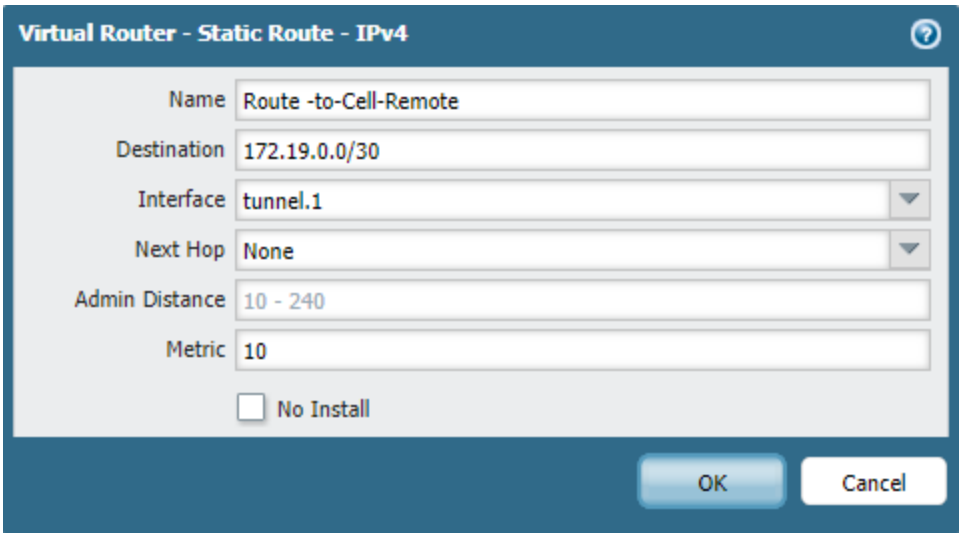


Go to the Proxy ID Tab and define Local and Remote Networks. In this scenario, Local Network is 192.168.110.0/24 and Remote Network is 172.19.0.0/30.



7. Configuring Route for Peer end Private Network

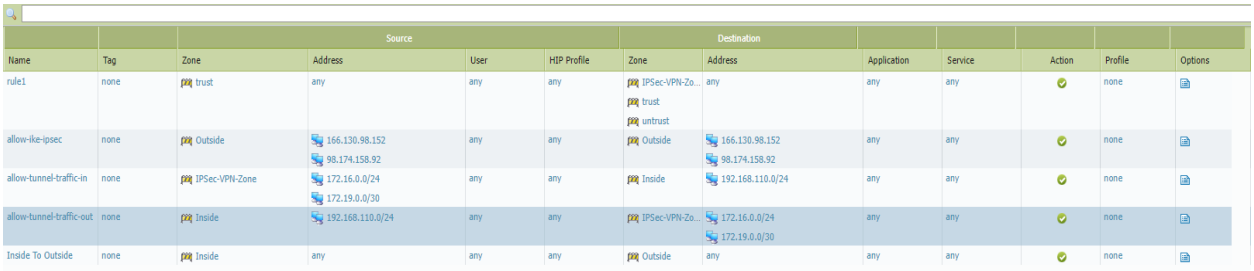
Now, you need to provide a static route for Peer end Private Network. Go to **Network** >> **Virtual Routers** >> **Default** >> **Static Routes** >> **Add**. Select the Name for this Route and define the destination network for this route, in this example 172.19.0.0/30.



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

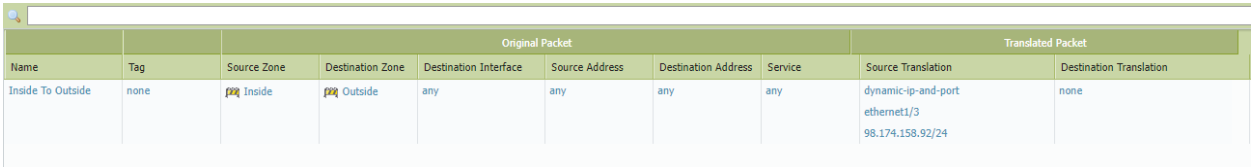


		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
rule1	none	trust	any	any	any	IPSec-VPN-Zo... trust untrust	any	any	any	✓	none	
allow-ike-ipsec	none	Outside	166.130.98.152 98.174.158.92	any	any	Outside	166.130.98.152 98.174.158.92	any	any	✓	none	
allow-tunnel-traffic-in	none	IPSec-VPN-Zone	172.16.0.0/24 172.19.0.0/30	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-Zo...	172.16.0.0/24 172.19.0.0/30	any	any	✓	none	
Inside To Outside	none	Inside	any	any	any	Outside	any	any	any	✓	none	

9. Creating NAT to allow Inside (LAN) access Internet.

Now, you need to create a NAT that allow inside LAN access Internet. You need to go to **Policies** >> **NAT** >> **Add** to define a new NAT.

NAT overview



		Original Packet						Translated Packet	
Name	Tag	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 ethernet1/3 98.174.158.92/24	none

10. Check VPN connection in Palo Alto

Go to **Network** >> **IPSec Tunnel**