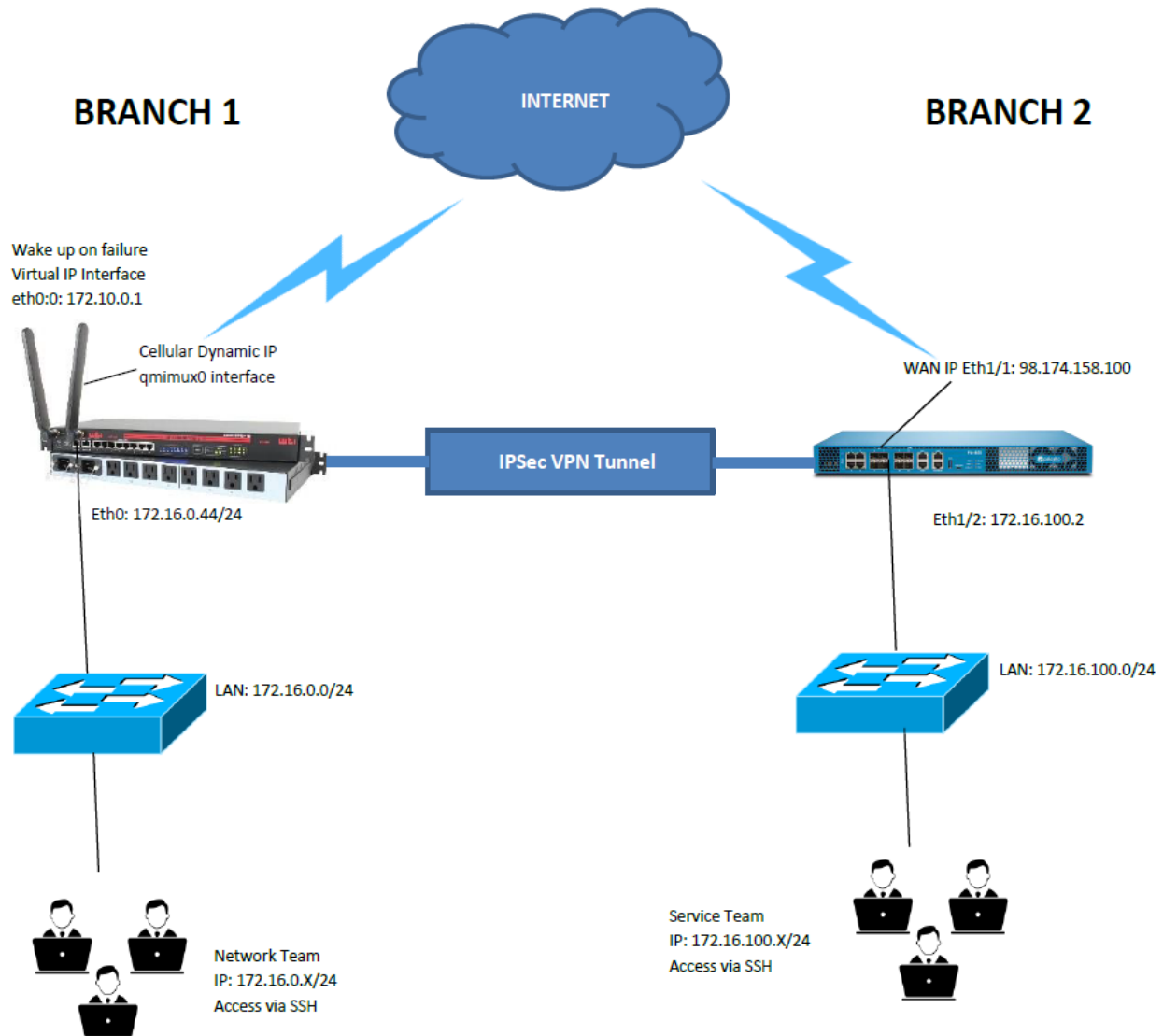


## Palo Alto to WTI IPsec VPN tunnel with Wakeup on Failure using %cell as left address

(Please note that this configuration is compatible with the latest firmware version, v8.07, which introduces several new features related to IPsec VPN)



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 – Cell Interface	Cell Dynamic IP
eth0:0 – Virtual Interface	172.10.0.1/30
Eth0 – Inside (LAN)	172.16.0.44
Local Network (LAN)	172.16.0.0/24
Remote Network (Peer)	172.16.100.0/24
Palo Alto Network	
Eth1/1 – Outside (WAN)	98.174.158.100
Eth1/2 – Inside (LAN)	172.16.100.2
Tunnel Interface name	PaloAlto-WI-Cell-Dynamic IP
Local Network (LAN)	172.16.100.0/24
Remote Network (Peer Virtual Network)	172.10.0.0/30

### Configure WTI IPSEC VPN

To configure or setup IPsec VPN from WTI WebGUI, go to the Configuration menu and navigate to the VPN Options. Expand the menu and select IPsec (Client Site-to Site). Please refer to the screenshot below for the configuration.

### Create eth0:0 Virtual IP Interface from VPN IPsec script under left up/down section available from Web GUI only

To create an eth0:0 virtual IP Interface from WTI Web GUI, go to configuration >> VPN option >> IPsec (Client Site-To-Site) >> select Tunnel Name >> Left Up/Down copy or paste the script as below. For this example, we assigned virtual ip address as 172.10.0.1/30.

```
#!/bin/bash
```

```
case "$PLUTO_VERB" in
```

```
  up-client)
```

```
    # Create Virtual Interface eth0:0
```

```
    ip address add 172.10.0.1/30 brd + dev eth0 label eth0:0
```

```
    /bin/wtinwcon sendwebrestart
```

```
    ;;
```

```
  down-client)
```

```
    # Remove Virtual Interface eth0:0
```

```
    ip address del 172.10.0.1/30 dev eth0:0
```

```
    ;;
```

```
esac
```



Site ID: MyTestUnit

HOME
STATUS +
CONTROL +
METERING +
CONFIGURATION -
GENERAL PARAMETERS +
SERIAL PORT CONFIGURATION
NETWORK CONFIGURATION +
CELLULAR CONFIGURATION +
USER CONFIGURATION
VPN OPTIONS -
IPsec (Client Site-To-Site)
OpenVPN (Client Site-To-Site)
IPsec (Server Site-To-Site)
PING NO ANSWER CONFIGURATION
ALARM CONFIGURATION
TELEMETRY OPTIONS +
DOWNLOAD UNIT CONFIGURATION
FIRMWARE
TEST
LOGOUT

IPSEC_CLIENT VPN DETAILS [PALOALTO-WTI-Cell-DynamicIP]	
Enable:	<input type="checkbox"/> On
Tunnel Name:	<input type="text" value="PALOALTO-WTI-Cell-DynamicIP"/>
Security:	<input type="text" value="Pre-shared Secret (Static Key File)"/>
Authentication Type:	<input type="text" value="ESP"/>
Left Address:	<input type="text" value="%cell"/>
Left ID:	<input type="text" value="WTI"/>
Left Subnet:	<input type="text" value="172.10.0.1/30"/>
Left Up/Down:	<input checked="" type="checkbox"/> (Show Left Up/Down)
	<pre>#!/bin/bash case "\$PLUTO_VERSION" in   up-client)     # Add Virtual Interface IP     ip address add 172.10.0.1/30 brd + dev eth0 label eth0:0     /bin/wtinwcon sendwebrestart</pre>
Right Address:	<input type="text" value="98.174.158.100"/>
Right ID:	<input type="text" value="98.174.158.100"/>
Right Subnet:	<input type="text" value="172.16.100.0/24"/>
Force Endcaps:	<input type="checkbox"/> On
Right Up/Down:	<input type="checkbox"/> (Show Right Up/Down)
Tunnel Options:	<input type="checkbox"/> (Show Options)
Option 1:	<input type="text" value="keyexchange"/> <input type="text" value="ikev2"/>
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!"/>
Option 4:	<input type="text" value="auto"/> <input type="text" value="start"/>
Associated Options:	Port: <input type="text" value="Default"/> ASSOCIATED IP: <input type="text"/>
EAP Users:	<input type="checkbox"/> (Show EAP Users)
Pre-Shared Key	<input type="text" value="WTI949"/>
<input type="button" value="Change VPN Parameters"/>	

**Note:** Use the static IP as the left address for the static IP address on the Cell interface. Alternatively, use %any for the left address to allow the VPN tunnel from any interface (eth0 or cell).

## Create a NAT in IP TABLES to allow WTI device to ping 172.16.100.0/24 network


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 172.16.100.0/24 -j SNAT --to-source 172.10.0.0
```

## Enable access to the WTI WebGUI using Virtual IP Address from Eth0

To access the unit via the WebGUI using a virtual IP address, please enter the virtual IP address as the "Listen Address" in the Web Access.

On WTI WebGUI, go to Configuration menu and navigate to Network Configuration and expand the Web menu. Enter an IP Address as 172.10.0.1 as Listen address.

 Site ID: MyTestUnit

<b>HOME</b>	<b>Web Access [eth0] IPv4/IPv6</b>
<b>STATUS</b> +	HTTP Access: <input type="checkbox"/> On
<b>CONTROL</b> +	HTTP Port: <input type="text" value="80"/>
<b>METERING</b> +	HTTPS Access: <input type="checkbox"/> On
<b>CONFIGURATION</b> -	HTTPS Port: <input type="text" value="443"/>
GENERAL PARAMETERS +	Harden Web Security: <input type="text" value="High"/>
SERIAL PORT CONFIGURATION	TLS Mode: <input type="text" value="TLSv1.1/TLSv1.2"/>
NETWORK CONFIGURATION -	HSTS Policy: <input type="checkbox"/> Off
IPV4 -	
eth0 -	
Shared Network Parameters	Trace Method: <input type="checkbox"/> Off
Network Parameters	OCSP Stapling: <input type="checkbox"/> Off
DHCP Server	Web Terminal: <input type="checkbox"/> On
IP Tables	Inactivity Timeout: <input type="text" value="0"/> In Minutes (0 is disabled)
Static Route	
DNS +	
Negotiation	
Web -	
Web Access	
SSL Certificates	
Import Wildcard Certs	
Syslog +	
SNMP Parameters	
SNMP Traps	
LDAP	
TACACS	
RADIUS	

Ⓢ Listen Address: ☐ (Show Listen Addresses)

Listen Address 1:

Change Web Parameters

## Enable Wakeup on Failure from Cell interface

To configure WTI cell wakeup on Failure from WTI WebGUI, go to Cell Configuration and click on Wakeup on failure. Please replace the Ping Address/Host 1 with the IP address you want to monitor from the Eth0 interface.



Site ID: MyTestUnit

<b>HOME</b>	
<b>STATUS</b> +	
<b>CONTROL</b> +	
<b>METERING</b> +	
<b>CONFIGURATION</b> -	
GENERAL PARAMETERS +	
SERIAL PORT CONFIGURATION	
NETWORK CONFIGURATION +	
CELLULAR CONFIGURATION -	
IPV4 -	
Cellular Parameters	
Cellular Usage Parameters	
Network Parameters	
Static Route	
DDNS	
Web +	
SNMP Parameters	
Ping Access	
Wakeup on Failure	
IP Passthrough	
USER CONFIGURATION	
VPN OPTIONS +	
PING NO ANSWER CONFIGURATION	
ALARM CONFIGURATION	
TELEMETRY OPTIONS +	
DOWNLOAD UNIT CONFIGURATION	
FIRMWARE	
TEST	
<b>LOGOUT</b>	

### Wakeup on Failure

The Wakeup On Failure feature allows a WTI unit to put an interface into sleep state, with the Ethernet port(s) acting as the unit's primary or secondary network interfaces. The interface will be in awake mode when it detects the failure on the specified Ethernet ports.

NETWORK	STATUS	PRIORITY	ALARM	GATEWAY
eth0	active	primary	no	default
eth1	---	---	no	
cell	asleep	last	no	

Enable:

On

②Interface to Monitor:

eth0

②Ping Address/Host 1:

192.168.100.2

②Ping Address/Host 2:

②Ping Interval:

5

(5-3600 Sec)

②Interval After Failed Ping:

5

(5-3600 Sec)

②Consecutive Failures:

3

(3-60)

②Single Ping Address Fail:

Disabled

②Autorecovery:

On

②Preferred Ethernet Default Gateway Port:

eth0

(NOT USED)

②Cell Tower Sleep Mode:

Detach

②Manual Recovery

Ping Wakeup on Failure Hosts

Change Wakeup on Failure

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

To check the VPN connection from WTI CLI

**/bash ipsec status**

**/bash ipsec statusall**

```
REM> /bash ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.14, Linux 5.4.0, armv7l):
  uptime: 8 seconds, since Dec 20 09:12:50 2024
  malloc: shrk 667648, mmap 0, used 423064, free 244584
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aes des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs12 pgp dnskey
  --default stroke vici updown eap-identity eap-mschapv2 xauth-generic counters
Listening IP addresses:
  172.10.0.1
  166.130.98.152
Connections:
PALOALTO-WTI-Cell-DynamicIP: 166.130.98.152...98.174.158.100 IKEv2, dpddelay=30s
PALOALTO-WTI-Cell-DynamicIP: local: [WTI] uses pre-shared key authentication
PALOALTO-WTI-Cell-DynamicIP: remote: [98.174.158.100] uses pre-shared key authentication
PALOALTO-WTI-Cell-DynamicIP: child: 172.10.0.0/30 == 172.16.100.0/24 TUNNEL, dpdaction=start
Security Associations (1 up, 0 connecting):
PALOALTO-WTI-Cell-DynamicIP[1]: ESTABLISHED 7 seconds ago, 166.130.98.152[WTI]..98.174.158.100[98.174.158.100]
PALOALTO-WTI-Cell-DynamicIP[1]: IKEv2 SPIs: 72b4d11038ab21b8_i* 68214bc8e661049b_r, pre-shared key reauthentication in 54 minutes
PALOALTO-WTI-Cell-DynamicIP[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
PALOALTO-WTI-Cell-DynamicIP[1]: INSTALLED TUNNEL, reqid 1, ESP in UDP SPIs: ca376add_i c97a257b_o
PALOALTO-WTI-Cell-DynamicIP[1]: AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
PALOALTO-WTI-Cell-DynamicIP[1]: 172.10.0.0/30 == 172.16.100.0/24
```

## 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.

The screenshot shows the 'Zone' configuration window in the Palo Alto Firewall GUI. The 'Name' field is set to 'IPSec-VPN-Zone' and the 'Type' is set to 'Layer3'. Under the 'Interfaces' section, 'tunnel.1' is listed. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is also 'None'. There is an unchecked checkbox for 'Enable User Identification'. On the right, the 'User Identification ACL' section has two lists: 'Include List' and 'Exclude List', both currently empty. At the bottom are 'OK' and 'Cancel' buttons.

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'. There are empty fields for 'Comment' and 'IP'. The 'Management Profile' is set to 'Outside' and the 'MTU' is set to '[576 - 1500]'. Under the 'Assign Interface To' section, the 'Virtual Router' is set to 'IPSec-VR' and the 'Security Zone' is set to 'IPSec-VPN-Zone'. At the bottom are 'OK' and 'Cancel' buttons.

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

The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' field is set to 'WTI\_IKECryptd'. There are three main sections: 'DH Group' with 'group14' selected, 'Encryption' with 'aes-256-cbc' selected, and 'Authentication' with 'sha256' selected. Each section has 'Add', 'Delete', 'Move Up', and 'Move Down' buttons. To the right, the 'Timers' section shows 'Key Lifetime' set to 'Hours' with a value of '8' and a note 'Minimum lifetime = 3 mins'. Below that, 'IKEv2 Authentication' is set to 'Multiple' with a value of '0'. At the bottom right are 'OK' and 'Cancel' buttons.

#### 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**.

The screenshot shows the 'IPsec Crypto Profile' configuration window. The 'Name' field is set to 'WTI\_IPSECryptd'. The 'IPsec Protocol' is set to 'ESP'. There are two main sections: 'Encryption' with 'aes-256-cbc' selected and 'Authentication' with 'sha256' selected. Each section has 'Add', 'Delete', 'Move Up', and 'Move Down' buttons. To the right, the 'DH Group' is set to 'group14', 'Lifetime' is set to 'Hours' with a value of '1' and a note 'Minimum lifetime = 3 mins'. Below that, the 'Enable' checkbox is unchecked, 'Lifesize' is set to 'MB' with a value of '[1 - 65535]' and a note 'Recommended lifesize is 100MB or greater'. At the bottom right are 'OK' and 'Cancel' buttons.



## 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 1/1 is **98.174.158.100**. Select Peer Type as **Dynamic**. Select the Authentication Method, i.e. Pre-shared Key or Certificate. In this scenario, I'm using the Pre-shared Key as **WTI949**. In the **Local Identification** select IP Address. **Peer Identification** as FQDN (hostname) and select IKE Crypto Profile as **WTI\_IKECrypto**.

The screenshot shows the 'IKE Gateway' configuration window with the 'General' tab selected. The configuration fields are as follows:

- Name:** WTI-Cell-DynamicIP
- Version:** IKEv2 only mode
- Address Type:** IPv4 (selected), IPv6
- Interface:** ethernet1/1
- Local IP Address:** 98.174.158.100/24
- Peer IP Address Type:** IP, FQDN, Dynamic (selected)
- Authentication:** Pre-Shared Key (selected), Certificate
- Pre-shared Key:** [Redacted]
- Confirm Pre-shared Key:** [Redacted]
- Local Identification:** IP address (selected), 98.174.158.100
- Peer Identification:** FQDN (hostname) (selected), WTI
- Comment:** [Empty]

At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the 'IKE Gateway' configuration window with the 'Advanced Options' tab selected. Under 'Common Options', 'Enable Passive Mode' and 'Enable NAT Traversal' are checked. The 'IKEv2' section is expanded, showing 'IKE Crypto Profile' set to 'WTI\_IKECrypto', 'Strict Cookie Validation' is unchecked, 'Liveness Check' is checked, and the 'Interval (sec)' is set to 5. 'OK' and 'Cancel' buttons are at the bottom right.

**IKE Gateway**

General Advanced Options

Common Options

- ☒ Enable Passive Mode
- ☒ Enable NAT Traversal

IKEv2

IKE Crypto Profile: WTI\_IKECrypto

☐ Strict Cookie Validation

☒ Liveness Check

Interval (sec): 5

OK Cancel

## 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**.

The screenshot shows the 'IPSec Tunnel' configuration window with the 'General' tab selected. The 'Name' field contains 'WTI-Cell-DynamicIP'. 'Tunnel Interface' is set to 'tunnel.1'. 'Type' is set to 'Auto Key'. 'Address Type' is set to 'IPv4'. 'IKE Gateway' is set to 'WTI-Cell-DynamicIP'. 'IPSec Crypto Profile' is set to 'WTI\_IPSECrypto'. 'Show Advanced Options' is unchecked. A 'Comment' field is empty. 'OK' and 'Cancel' buttons are at the bottom right.

**IPSec Tunnel**

General Proxy IDs

Name: WTI-Cell-DynamicIP

Tunnel Interface: tunnel.1

Type: ☒ Auto Key ☐ Manual Key ☐ GlobalProtect Satellite

Address Type: ☒ IPv4 ☐ IPv6

IKE Gateway: WTI-Cell-DynamicIP

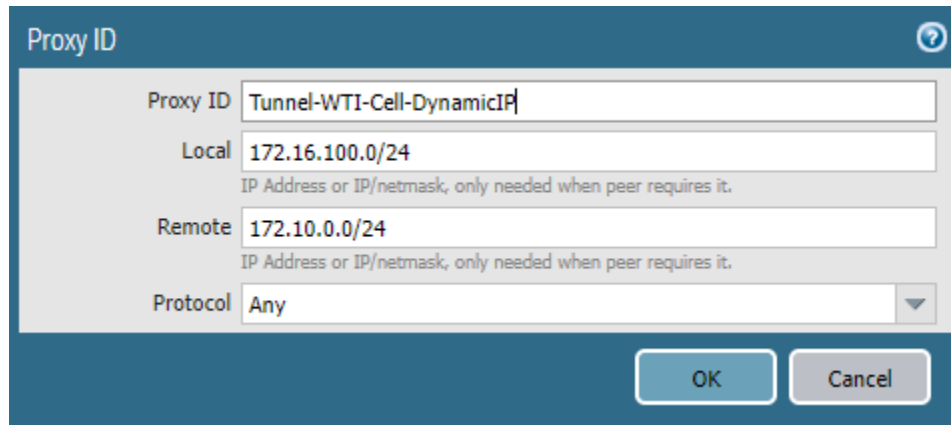
IPSec Crypto Profile: WTI\_IPSECrypto

☐ Show Advanced Options

Comment:

OK Cancel

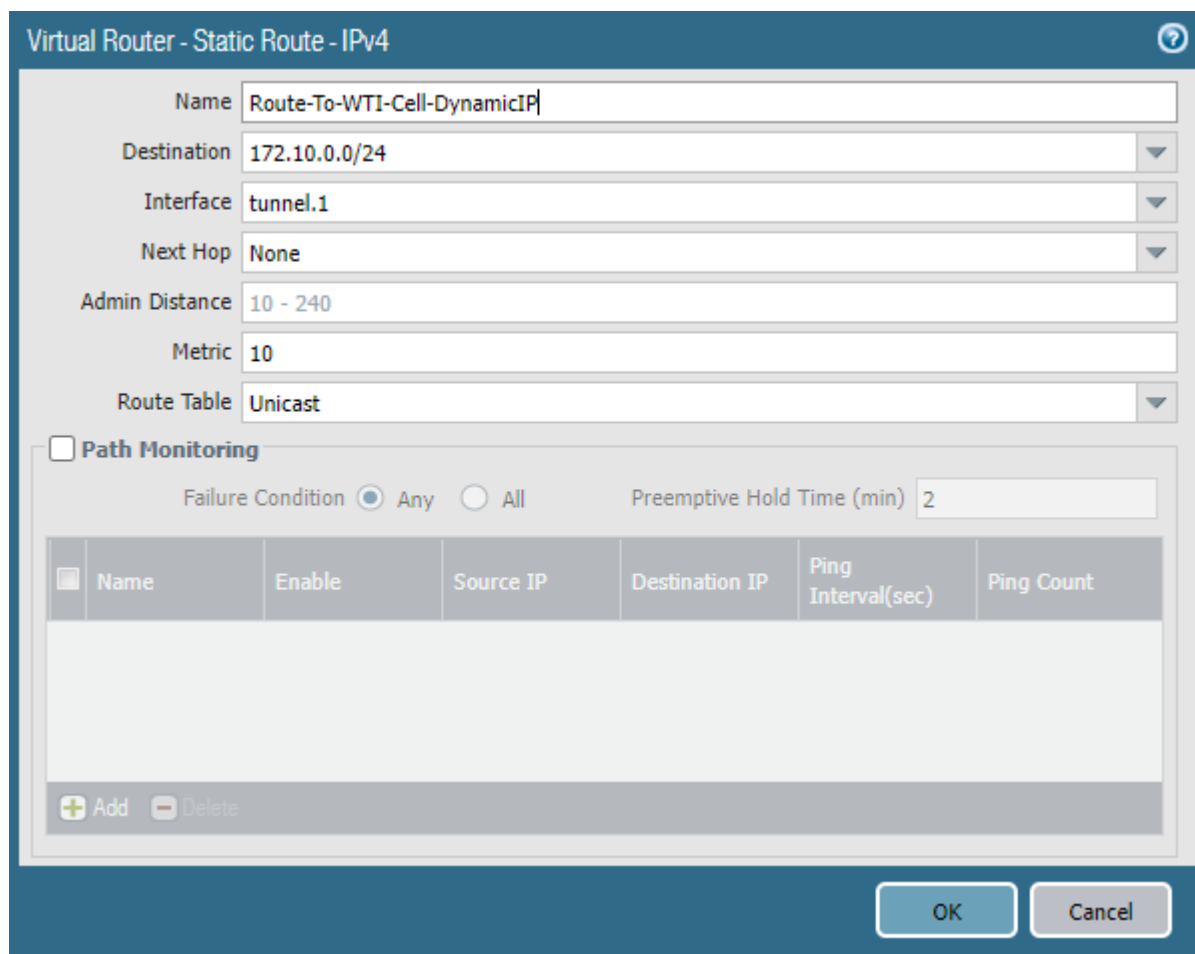
Go to the Proxy ID Tab and define Local and Remote Networks. In this scenario, Local Network is 172.16.100.0/24 and Remote Network is 172.10.0.0/24.



The Proxy ID configuration window has a title bar with a question mark icon. It contains four input fields: 'Proxy ID' with the text 'Tunnel-WTI-Cell-DynamicIP', 'Local' with '172.16.100.0/24', 'Remote' with '172.10.0.0/24', and 'Protocol' with a dropdown menu set to 'Any'. Below the 'Local' and 'Remote' fields is a small grey box with the text 'IP Address or IP/netmask, only needed when peer requires it.' At the bottom right are 'OK' and 'Cancel' buttons.

## 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 172.10.0.0/24.



The Virtual Router - Static Route - IPv4 configuration window has a title bar with a question mark icon. It contains several input fields: 'Name' with 'Route-To-WTI-Cell-DynamicIP', 'Destination' with '172.10.0.0/24', 'Interface' with 'tunnel.1', 'Next Hop' with 'None', 'Admin Distance' with '10 - 240', 'Metric' with '10', and 'Route Table' with 'Unicast'. Below these is a 'Path Monitoring' section with a checkbox, 'Failure Condition' with radio buttons for 'Any' (selected) and 'All', and 'Preemptive Hold Time (min)' with '2'. At the bottom are 'OK' and 'Cancel' buttons.

	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

## 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	Tags	Type	Source				Destination		Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	Allow
2	Inside To Outside	none	universal	LAN-Inside	any	any	any	WAN-Outside	any	any	any	Allow
3	Allow-Tunnel-VPN-Ins...	none	universal	IPSec-VPN-Z...	172.10.0.0/30 172.16.100.0/24 172.19.0.0/30	any	any	LAN-Inside	172.16.100.0/24	any	any	Allow
4	Allow-Tunnel-VPN-Ou...	none	universal	LAN-Inside	172.16.100.0/24	any	any	IPSec-VPN-Z...	172.10.0.0/30 172.16.100.0/24 172.19.0.0/30	any	any	Allow

## 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

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 ethernet1/3 98.174.158.92/24	none

## 10. Check VPN connection in Palo Alto

Go to **Network >> IPSec Tunnel**

WTT-Cell-DynamicIP	Tunnel Info	Auto Key	ethernet1/1	98.174.158.100/24	dynamic	IKE Info	tunnel.1	VirtualRoute (Show Routes)	vsys1	IPSec-VPN-Zone	
--------------------	-------------	----------	-------------	-------------------	---------	----------	----------	----------------------------	-------	----------------	--