



# PAN-OS VPN Configuration:

---

## *Configuring IPSec VPN between PAN-OS & Check Point Edge / Safe @Office*

April 2011

Jon Farkas  
Palo Alto Networks  
232 E. Java Dr.  
Sunnyvale, CA 94089  
408.738.7700  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

## Table of Contents:

Introduction.....	2
Configuration on Palo Alto Networks device:.....	2
Configuration on UTM-1 Edge:.....	6
Verifying that the tunnel is up:.....	10

## Introduction


This document outlines the basic steps involved in establishing a tunnel between a Palo Alto Networks (PAN) and a Check Point UTM-1 Edge. The UTM-1 Edge might also be referred to as VPN-1 Edge, SofaWare, or Safe@Office appliances. All of the named Check Point devices run SofaWare’s Embedded NGX code. The firmware versions used in this document are:

- PAN-OS version 4.0.1
- SofaWare Embedded NGX version 8.0.42

\*Note that this document is not relevant to Check Point VPN-1 running on Secure Platform, Nokia IPSO appliances, Solaris or Windows.

## Configuration on Palo Alto Networks device:

- Navigate to the Network tab > IKE Gateways (click “New”):

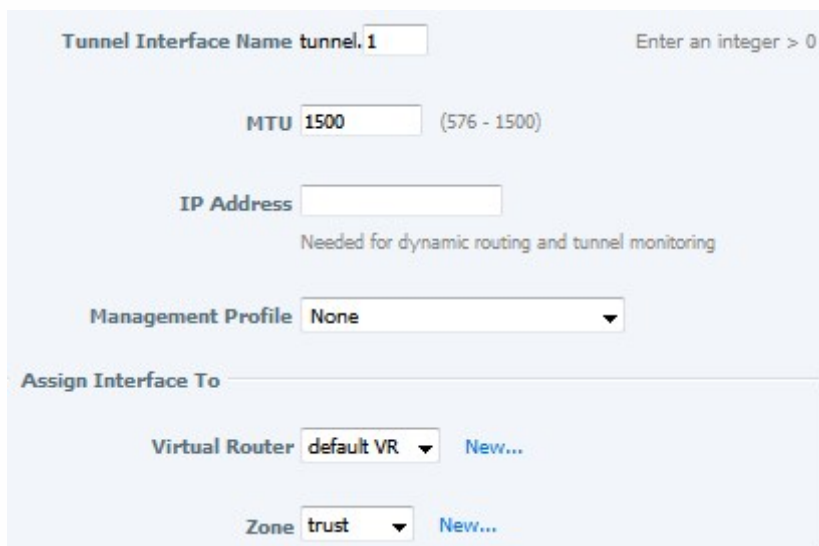


The screenshot shows the configuration form for an IKE Gateway. The fields are as follows:

- IKE Gateway:** UTM-1 Edge
- Local IP Address:** ethernet1/8 (dropdown), IP: [redacted].11 (dropdown)
- Peer IP Address:** [redacted].14 (dropdown),  Dynamic (checkbox), with a note: "Select 'Dynamic' or enter a Peer IP Address"
- Pre-shared Key:** [redacted]
- Confirm Pre-shared Key:** [redacted]

- Enter Remote IKE Gateway name, Local interface and IP, remote Gateway IP, & Pre-Shared Key

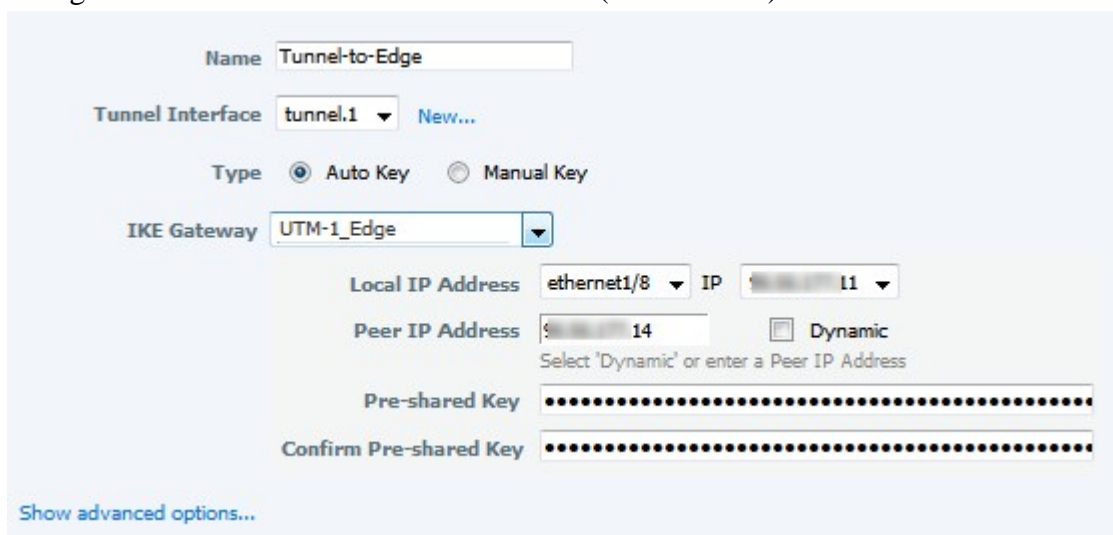
- Navigate to the Network tab > Interfaces, at the bottom of the page choose to create a new Tunnel Interface:



The screenshot shows the configuration page for a new Tunnel Interface. The fields are as follows:

- Tunnel Interface Name:** tunnel.1 (with a note: Enter an integer > 0)
- MTU:** 1500 (with a range of 576 - 1500)
- IP Address:** (empty field, with a note: Needed for dynamic routing and tunnel monitoring)
- Management Profile:** None (dropdown menu)
- Assign Interface To:**
  - Virtual Router:** default VR (dropdown menu, with a "New..." link)
  - Zone:** trust (dropdown menu, with a "New..." link)

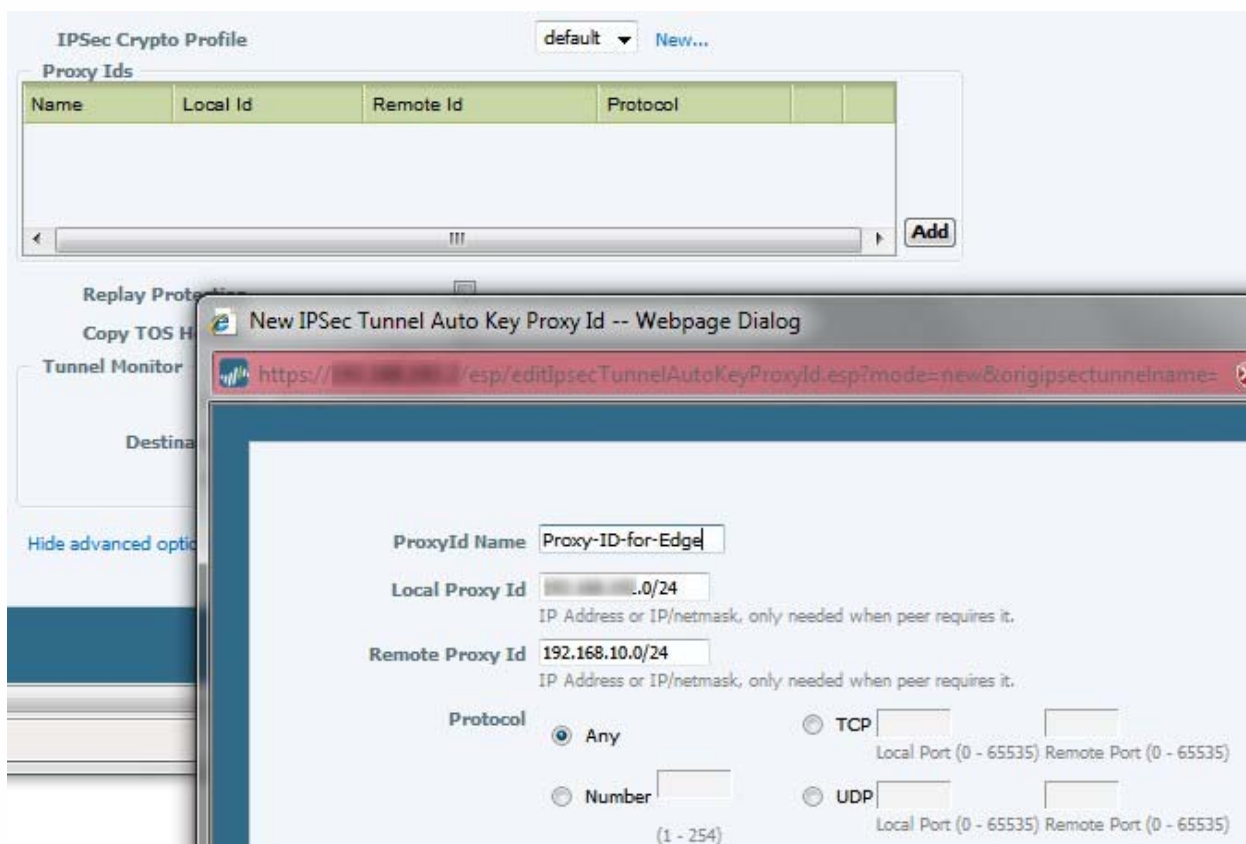
- Navigate to the Network tab > IPsec Tunnels (click “New”):



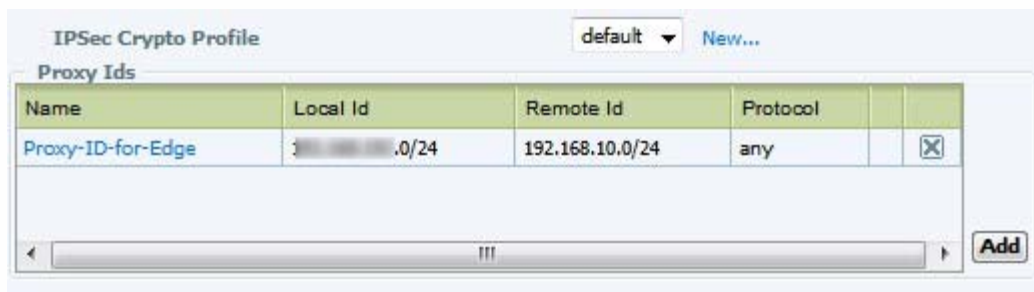
The screenshot shows the configuration page for a new IPsec Tunnel. The fields are as follows:

- Name:** Tunnel-to-Edge
- Tunnel Interface:** tunnel.1 (dropdown menu, with a "New..." link)
- Type:** Auto Key (radio button selected), Manual Key (radio button unselected)
- IKE Gateway:** UTM-1\_Edge (dropdown menu)
- Local IP Address:** ethernet1/8 (dropdown menu), IP: 11 (dropdown menu)
- Peer IP Address:** 14 (text field), Dynamic (checkbox unselected). Note: Select 'Dynamic' or enter a Peer IP Address
- Pre-shared Key:** (password field with dots)
- Confirm Pre-shared Key:** (password field with dots)
- Show advanced options...** (link)

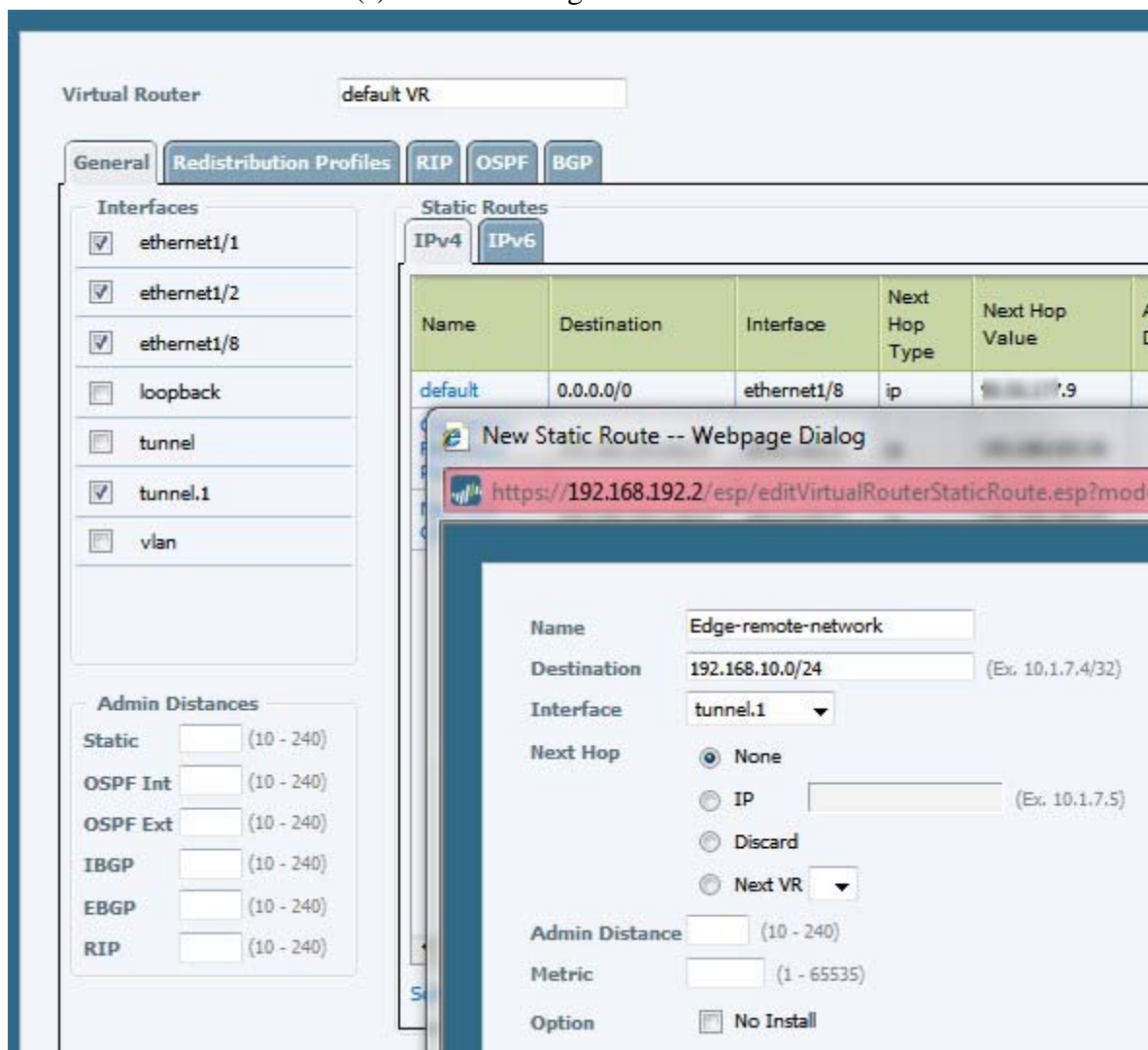
- Enter a name, choose the tunnel interface (above), and choose the IKE gateway (above), all other fields are populated automatically
- Click “Show advanced options” and enter local and remote proxy ID’s:



Click OK:



- Navigate to the Network tab > Virtual Routers. Open the appropriate VR, and add a static route to the network(s) behind the Edge device:



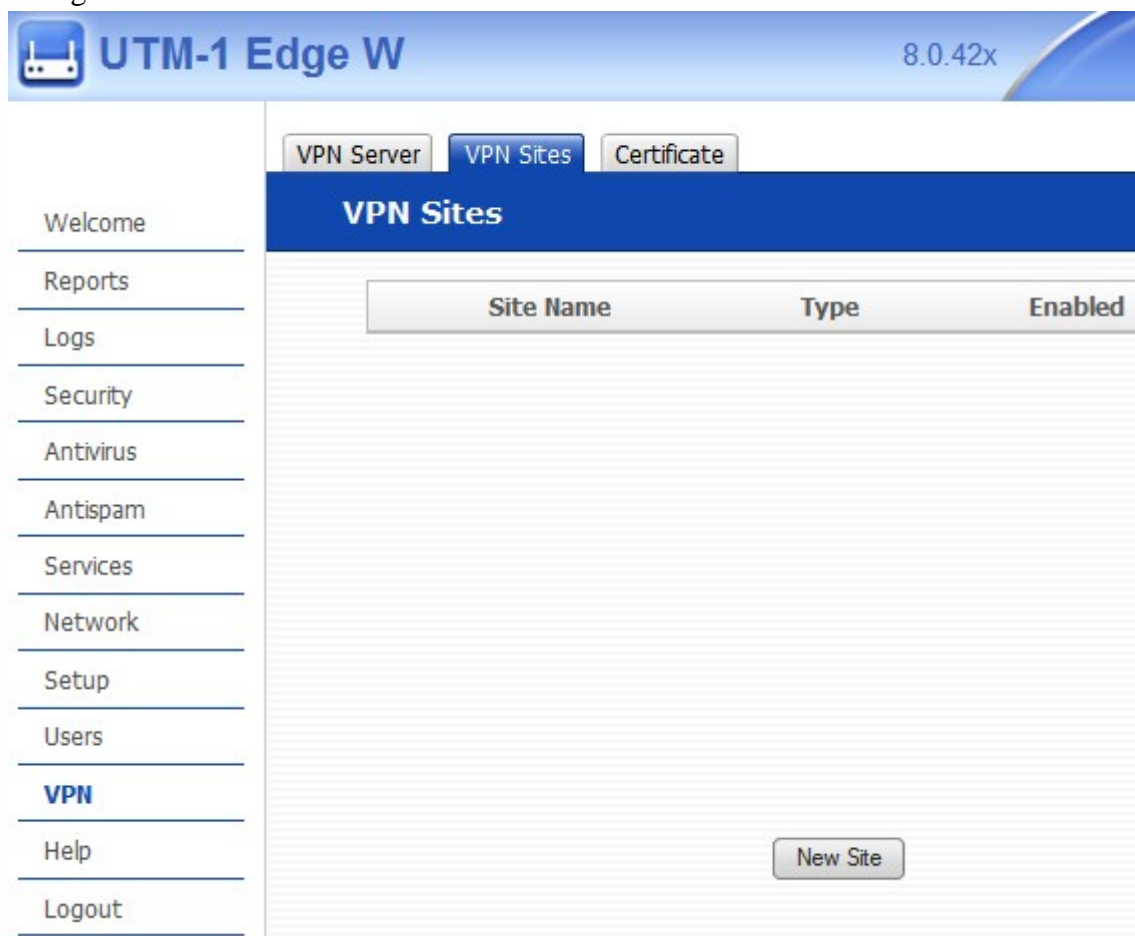
- Be sure that the interface is the tunnel interface from above, and next hop is "None"
- Navigate to the Policies tab > Security. Add new rules to allow IKE/IPSec traffic between the gateways, and desired traffic inside the tunnel:

Name	T...	Source				Destination				Application	Service	Action	Profile	Opti...
		Zone	Address	User	HIP Pr...	Zone	Address							
VPN-to-Edge Tunnel Setup	n...	untr...	Edge	any	any	untrust	PA-500			ike	any	✓	none	
			PA-500				Edge			ipsec				
VPN to Edge	test	trust	LAN	any	any	trust	192.168.10.0/24			any	any	✓	none	

- Commit the changes

**Configuration on UTM-1 Edge:**

- Navigate to VPN > VPN Sites:



The screenshot shows the configuration interface for a Palo Alto Networks UTM-1 Edge W device. The top navigation bar includes "VPN Server", "VPN Sites" (selected), and "Certificate". The main content area is titled "VPN Sites" and features a table with the following headers: "Site Name", "Type", and "Enabled". The table is currently empty. A "New Site" button is located at the bottom right of the table area. On the left side, a navigation menu lists various system functions, with "VPN" highlighted in blue.

- Click "New Site"

- Choose Site-to-Site VPN in the Wizard:



**UTM-1 Edge VPN Site Wizard**

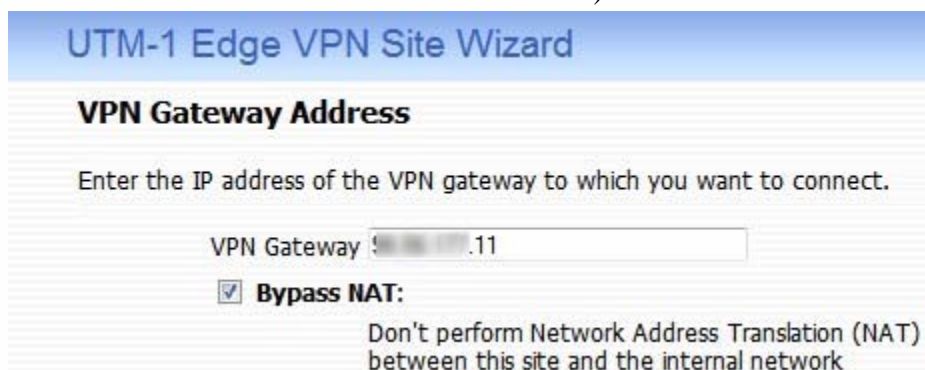
**Welcome to the VPN Site Wizard**

Using this wizard, you can create a connection to a VPN (Virtual Private Network) site. Select the type of site to establish:

- Remote Access VPN:**  
Allows a user to establish remote access sessions to another network.
- Site-to-Site VPN:**  
Establishes a permanent secure link between your network and a remote network.

To continue, click **Next**.

- Enter the IP of the Palo Alto Networks device (must be the same IP configured on the Palo Alto Networks as the Local IP above):



**UTM-1 Edge VPN Site Wizard**

**VPN Gateway Address**

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway : 10.10.10.11

**Bypass NAT:**  
Don't perform Network Address Translation (NAT) between this site and the internal network

- Specify VPN configuration:

### UTM-1 Edge VPN Site Wizard

#### VPN Network Configuration

How do you want to obtain the VPN network configuration?

To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

- Download Configuration:**  
Obtain the network configuration by downloading it from the site.
- Specify Configuration:**  
Enter the network configuration manually.
- Route All Traffic:**  
All network traffic will be routed via this site (Including Internet traffic)
- Route Based VPN:**  
Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.

- Enter the IP Subnet(s) behind the Palo Alto Networks device:

### UTM-1 Edge VPN Site Wizard

#### VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.	1 . . . .0	255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

- Choose Authentication method of Shared Secret:

### UTM-1 Edge VPN Site Wizard

#### Authentication Method

Select the authentication method used by this VPN site.

- Shared Secret**
- Certificate**



- Enter the pre-shared key configured on the Palo Alto Networks device:

UTM-1 Edge VPN Site Wizard

### Authentication

Please enter the Shared Secret:

Use Shared Secret

- Set “Security Methods” Phase 1 and Phase 2 to Automatic:

UTM-1 Edge VPN Site Wizard

### Security Methods

Select the security and integrity methods for this site, or select “Automatic” to automatically select the best security methods supported by the site.

[▼ Show Advanced Settings](#)

**Phase 1**  
Security Methods

**Phase 2**  
Security Methods

- Allow the tunnel to connect:

UTM-1 Edge VPN Site Wizard

### Connect

Try to Connect to the VPN Gateway  
Using the credentials you provided. Any existing tunnels will be terminated.

- Give the VPN site a name:

UTM-1 Edge VPN Site Wizard

### Site Name

You have successfully defined the VPN site.  
Please enter a name for this site:

Site Name

**Keep this site alive**  
This site will be connected even if there is no network traffic.

- Make sure to check “Keep this site alive”

## Verifying that the tunnel is up:

The following steps can be used to verify that the tunnel is established:

- Send a ping from each side to the other (if allowed by policies):

```
Pinging 192.168.10.22 with 32 bytes of data:
Reply from 192.168.10.22: bytes=32 time=50ms TTL=126
Reply from 192.168.10.22: bytes=32 time=46ms TTL=126
Reply from 192.168.10.22: bytes=32 time=46ms TTL=126
Reply from 192.168.10.22: bytes=32 time=46ms TTL=126

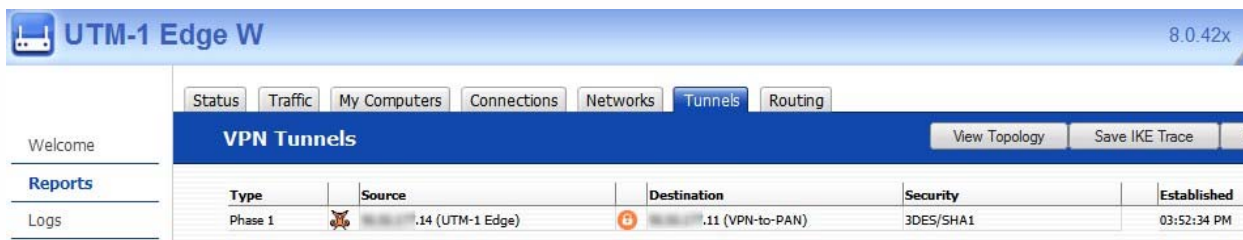
Ping statistics for 192.168.10.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 50ms, Average = 47ms
```

- On the Palo Alto Networks device, navigate to the Network Tab > IPsec Tunnels:

IKE Gateway						Tunnel Interface				
Name	Status	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Security Zone	Status	
Tunnel-to-Edge		ethernet1/8	192.168.11.29	192.168.11.14		tunnel.1	default VR (Show Routes)	trust		

- Verify that the lights are green for both Phase 1 and Phase 2 status

- On the UTM-1 Edge, navigate to the Reports > Tunnels tab and verify that the tunnel is established:



The screenshot shows the 'VPN Tunnels' page on a Palo Alto Networks UTM-1 Edge W device. The page title is 'UTM-1 Edge W' with version '8.0.42x'. The navigation tabs include Status, Traffic, My Computers, Connections, Networks, Tunnels (selected), and Routing. The main content area shows a table of VPN tunnels.

Type	Source	Destination	Security	Established
Phase 1	192.168.11.14 (UTM-1 Edge)	192.168.11.11 (VPN-to-PAN)	3DES/SHA1	03:52:34 PM