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

Table of Contents:

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

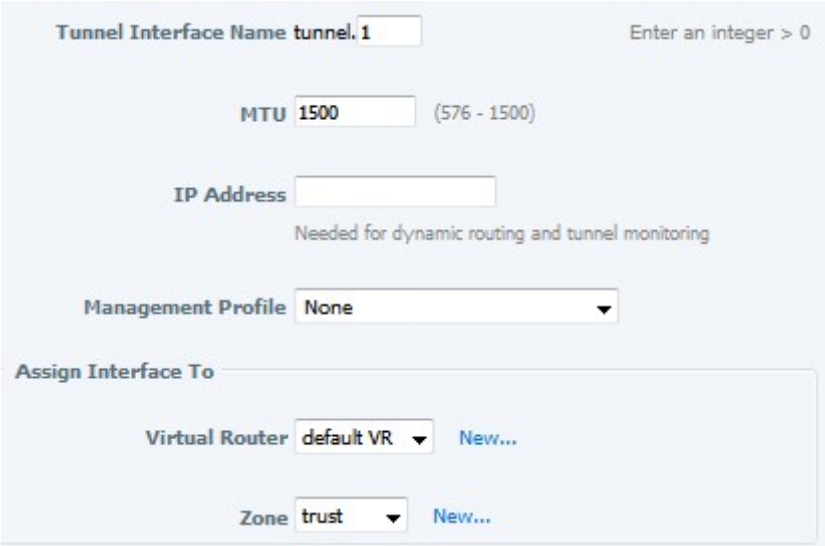
*Note that this document is not relevant to Check Point VPN-1 runing on Secure Platform, Nokia IPSO appliances, Solaris or Windows.

Configuration on Palo Alto Networks device:

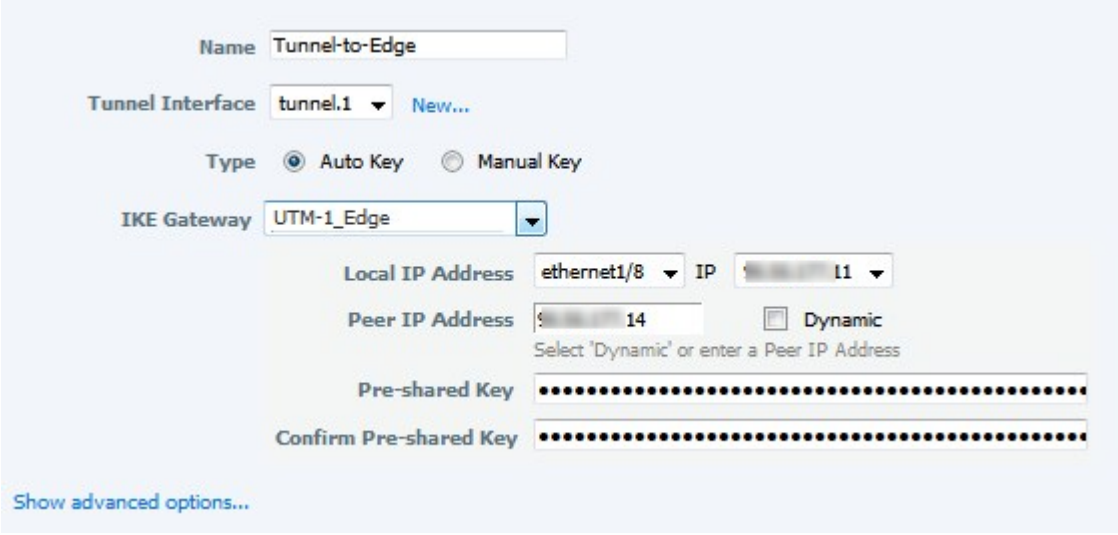
- Navigate to the Network tab > IKE Gateways (click "New"):

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

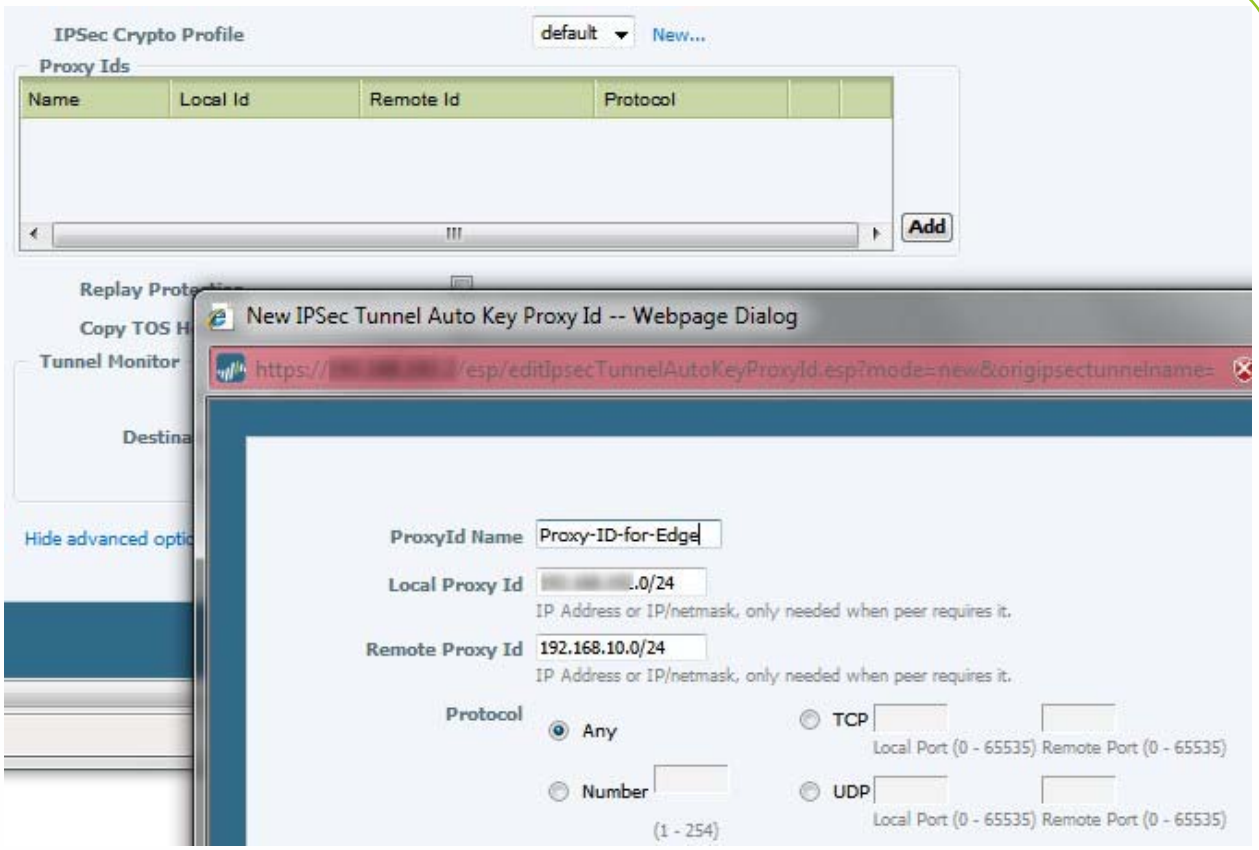
- Navigate to the Network tab > Interfaces, at the bottom of the page choose to create a new Tunnel Interface:



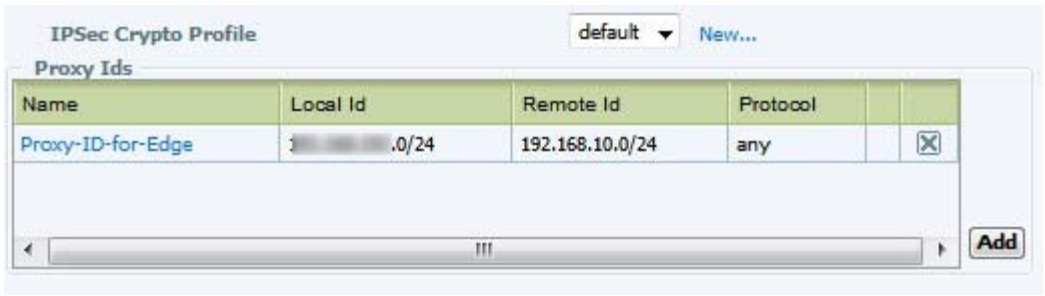
- Navigate to the Network tab > IPSec Tunnels (click "New"):



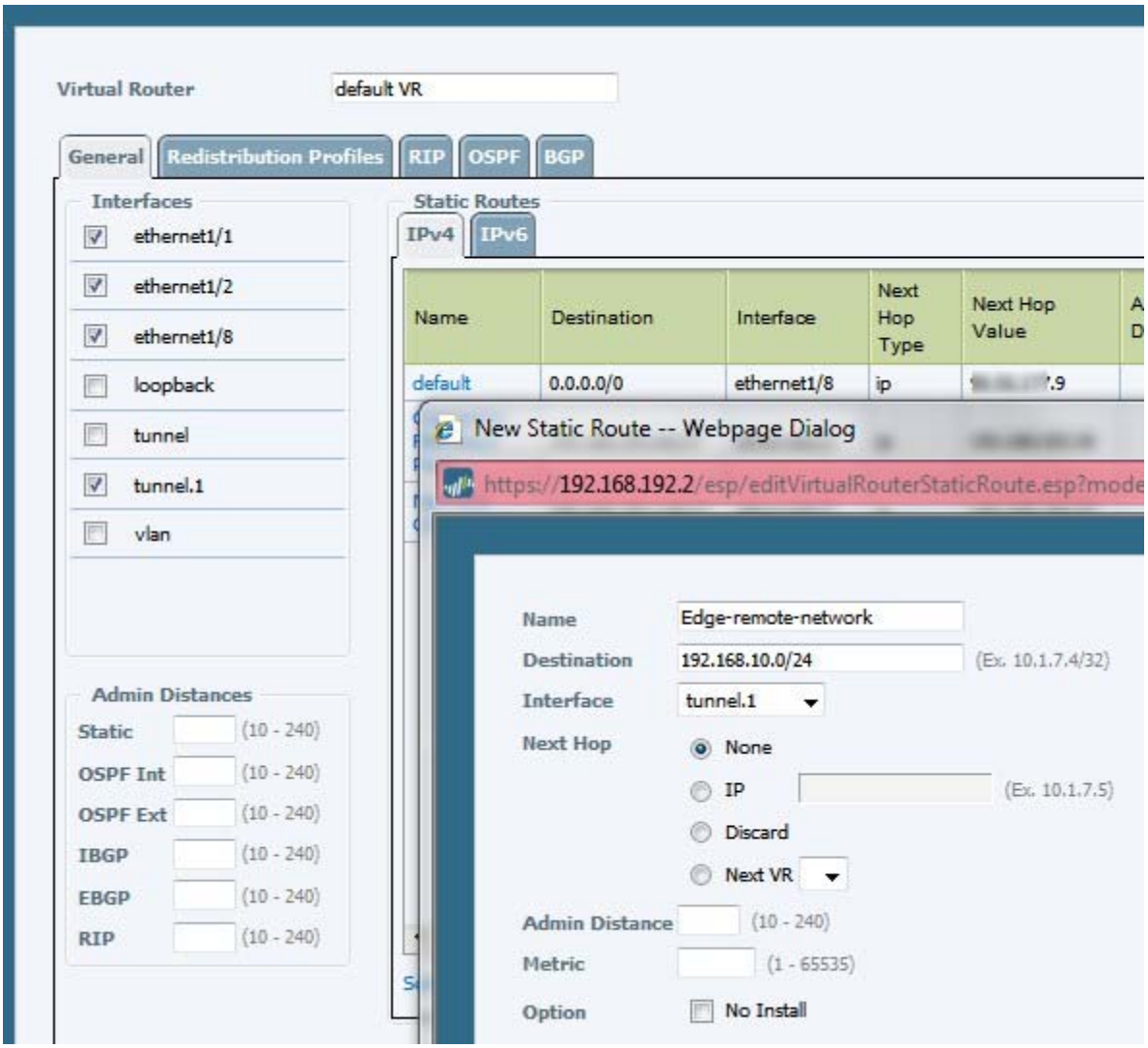
  - Enter a name, choose the tunnel interface (above), and choose the IKE gateway (above), all other fields are populated automatically
- Click "Show advanced options" and enter local and remote proxy ID's:



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"

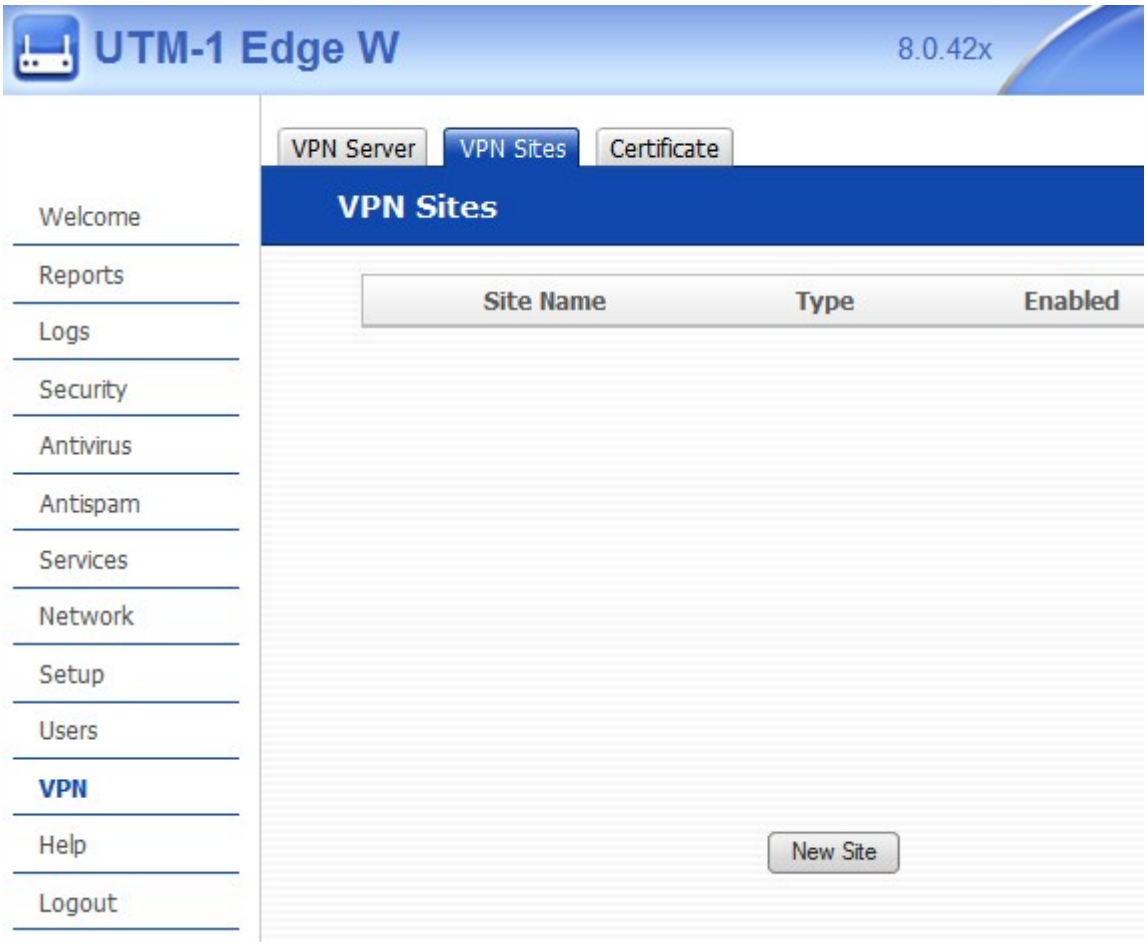
- Navigate to the Policies tab > Security. Add new rules to allow IKE/IPSec traffic between the gateways, and desired traffic inside the tunnel:

		Source				Destination						
Name	T...	Zone	Address	User	HIP Pr...	Zone	Address	Application	Service	Action	Profile	Optic
VPN-to-Edge Tunnel Setup	n...	untr...	Edge PA-500	any	any	untrust	PA-500 Edge	ike ipsec	any	✓	none	
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:

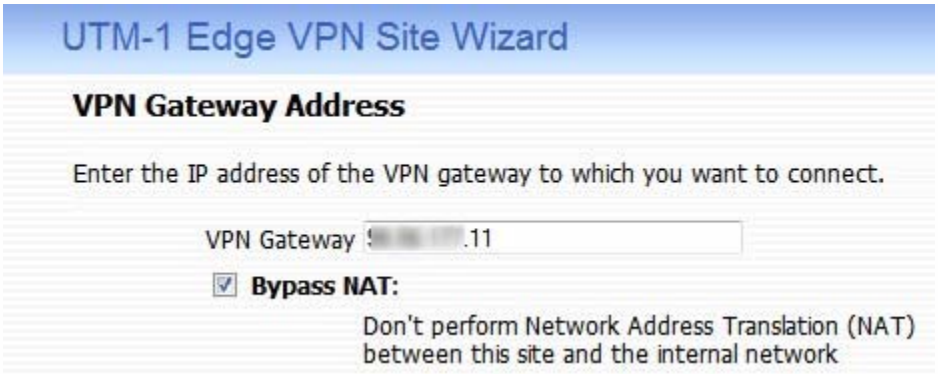
- Navigate to VPN > VPN Sites:



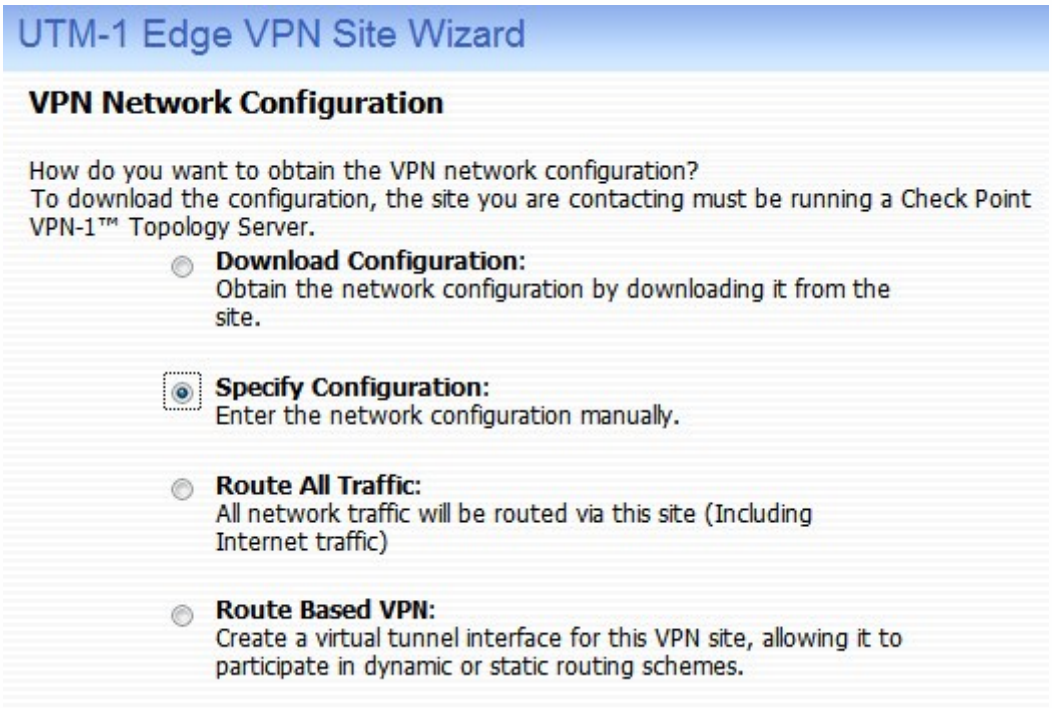
- Click “New Site”

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

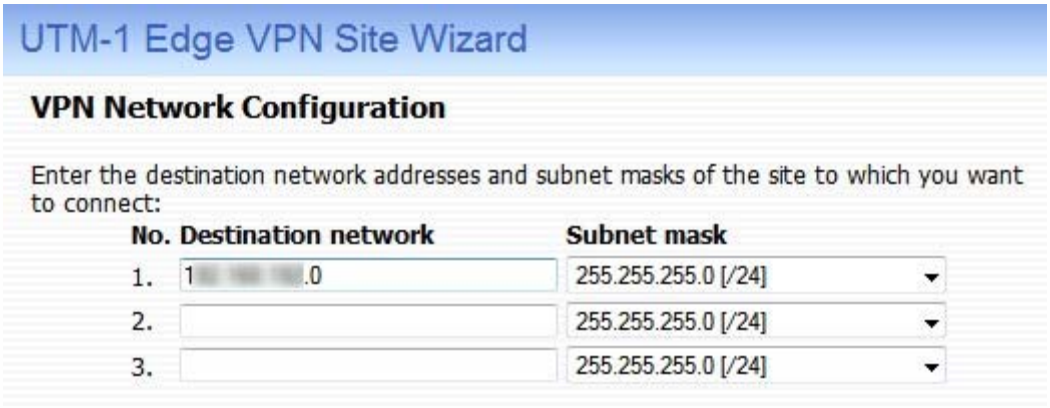
- Enter the IP of the Palo Alto Networks device (must be the same IP configured on the Palo Alto Networks as the Local IP above):



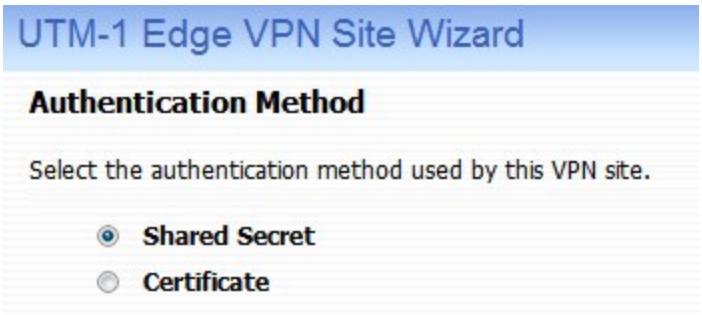
- Specify VPN configuration:



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



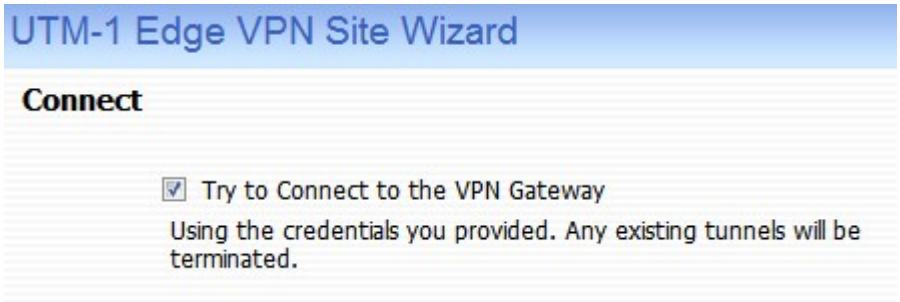
- Choose Authentication method of Shared Secret:



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

- Set "Security Methods" Phase 1 and Phase 2 to Automatic:

- Allow the tunnel to connect:



- Give the VPN site a name:

  - 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:

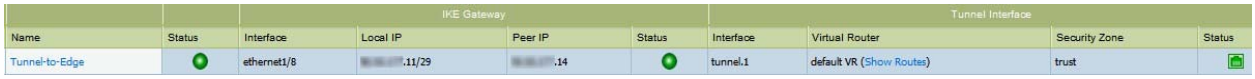
- Send a ping from each side to the other (if allowed by policies):

```
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:



  - 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: