EdgeMAX - L2TP Server

July 02, 2015 11:18

Overview

Readers will learn how to configure the EdgeRouter to act as an L2TP (Layer-2 Tunnel Protocol) server for remote access.

Note: These instructions assume that *eth0* is your WAN (Internet) connection. Early in the configuration, a specific command should be used in case you receive a DHCP-assigned IP address from your Internet service provider, while a separate command should be used if you receive a static IP address from your Internet service provider.

Steps

Access the router's command line interface. You can do this using the CLI button while inside the Web UI or by using an SSH program such as PuTTY. PuTTY is generally quicker, as it allows easy copying and pasting (copy in Windows, paste using the right mouse button).

Note: Commands that start with a pound (#) are explanatory comments that you do not need to enter.

The steps follow below:

#Enter configuration mode.

```
configure
```

#Define the interface ipsec will use for internet connections (eth0 in this example).

```
set vpn ipsec ipsec-interfaces interface eth0
```

#Enable NAT traversal (this is mandatory).

```
set vpn ipsec nat-traversal enable
```

#Set the allowed subnet (allowing all subnets).

```
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
```

#Show the ipsec configuration.

```
show vpn ipsec
```

DHCP ONLY: If you obtain your IP address from your internet service provider via DHCP, use this

command:

```
set vpn l2tp remote-access dhcp-interface eth0
```

STATIC IP ONLY: If you have a static IP address and do NOT obtain your IP address from your

internet service provider via DHCP, then use this command instead of the one above:

```
set vpn l2tp remote-access outside-address STATICIP
```

Replace "STATICIP" in the command above with your actual static IP address!

#Set up the pool of IP addresses that remote VPN connections will assume.

In this case we make 10 addresses available (from.101 to .110) on subnet #192.168.100.0/24.

You can also issue IP addresses used in your subnet, but make sure that

They do not overlap with IP addresses issued by your DHCP Server or used by

other devices on your network.

```
set vpn l2tp remote-access client-ip-pool start 192.168.100.101
set vpn l2tp remote-access client-ip-pool stop 192.168.100.110
```

#Set the IPsec authentication mode to pre-shared secret.

```
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared
-secret
```

#Set the pre-shared secret (replace "secret phrase" with your desired passphrase)

```
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secr
et "secret phrase"
```

#Set the L2TP remote access authentication mode to local.

```
set vpn l2tp remote-access authentication mode local
```

#Set theL2TP remote access username and password.

#Replace testuser with your desired username and testpassword with your desired password.

#Repeat this line as needed.

```
set vpn l2tp remote-access authentication local-users username testuser
password testpassword
```

#Set the MTU

```
set vpn l2tp remote-access mtu 1492
```

#Set DNS Servers:

```
set vpn l2tp remote-access dns-servers server-1 8.8.8.8
set vpn l2tp remote-access dns-servers server-2 8.8.4.4
```

#Commit the change.

```
commit
```

#Show the l2tp remote access configuration.

```
show vpn l2tp remote-access
```

#Save the settings

```
save
```

#Open the required ports and protocol using the Web UI.

#Access the Web UI.

Click on the "Security Tab" (in earlier versions of the firmware) or the "Firewall/NAT" tab and then "Firewall Policies" (in firmware version 1.5).

Find the "WAN_LOCAL" rule (or whatever you called the rule that controls access to the router), and click "Actions" to the right of it.

Select "Edit Ruleset" from the pull-down.

Add a new rule somewhere before you drop invalid packets as follows:

Basic Tab:

- Description: Allow L2TP
- Check Enable.
- Action: Accept.
- Protocol: Either UDP (1.5) or Choose a protocol by name: udp (earlier versions)

Destination Tab:

- Port: 500,1701,4500

#Click Save.

Add a new rule somewhere after the previous rule as follows:

Basic Tab:

- Description: Allow ESP
- Check Enable.
- Action: Accept.
- Protocol: Either enter a procotol number 50 or Choose a protocol by name: esp

#Click Save.

Thanks Advocate99!

Was this article helpful? 0 out of 0 found this helpful

Give Feedback

Don’t see what you are looking for? Get advice for UniFi from our Community or Submit a Help Ticket.

EDGEMAX COMMUNITY

SUBMIT A REQUEST