Ubiquiti
MDS 3rd Party Integration

CONTENTS

INTRODUCTION

Congratulations on your sale of MyDigitalShield, using the option to configure existing device(s) to use tunneling protocol.

This guide is written specifically for the **Ubiquiti EdgeRouter X**. It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

This guide documents configuration of the Ubiquiti EdgeRouter gateway using SSH software to connect to the gateway.

ASSUMPTIONS

- This guide was developed to provide configuration information of the Ubiquiti gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The Ubiquiti EdgeRouterModel has been upgraded to firmware version v1.9.1
- This guide is NOT intended to be a full configuration guide for the Ubiquiti EdgeRouter.
- Responsibility for the management of the Ubiquiti gateway is not assumed by MyDigitalShield.
- The user of this guide is familiar with the operation of the EdgeRouter and is able to navigate using GUI and CLI.
- The partner is aware that the router will be **ERASED** and reset to factory default.
  DO NOT USE THIS DOCUMENT IF LOCAL CONFIG NEEDS TO BE PRESERVED.

WHAT YOU WILL NEED

- An SSH software (e.g. Putty, SSH Secureshell, etc.)*
- The local public IP address/subnet.
- The local public IP GW address (your customer's default gateway address).
- Local LAN network/subnet.
- The MDS Cloud IP address assigned to you.
- VTI Tunnel IP (Provided by MDS).
- The following IP address information:

*Putty can be downloaded here
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

In this document, the term "Local" refers to a configuration or IP address at your customer's site. "Cloud" refers to the MyDigitalShield node.

1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides.
2. **Local Public GW:** The gateway IP address provided by the customer's ISP.
3. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
4. **Cloud Public IP:** This is the address assigned to you by MyDigitalShield. It is the remote IP address at the MDS Node that the IPSEC tunnel will terminate on.
5. **Local IPSEC VTI IP:** This is the local side of the tunnel provided by MDS
6. **Cloud IPSEC VTI IP:** This is the Cloud side of the tunnel provided by MDS

Fill in the middle column of the following table for reference throughout this guide. To map IP addresses throughout this guide, values in the “Reference Sample” column are used.

Network	IP	Reference Sample
Local Public IP: (x.x.x.x/mask)		71.194.9.231/23
Local Public GW (x.x.x.x)		71.194.8.1
Local LAN Network (x.x.x.x/mask)		192.168.1.0/24
Cloud Public IP (x.x.x.x)		216.21.158.211
Local IPSEC VTI IP (x.x.x.x)		10.10.10.1
Cloud IPSEC VTI IP (x.x.x.x)		10.10.10.2

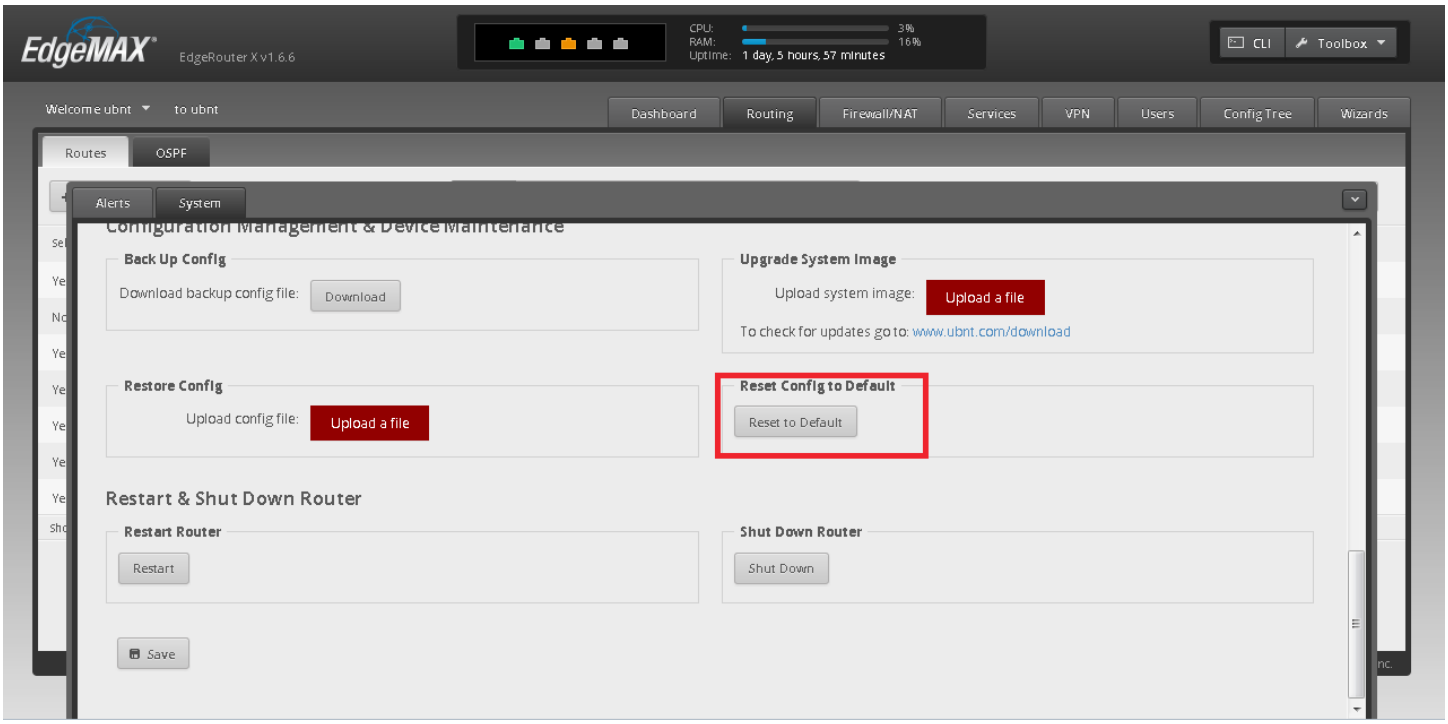
RESET THE CONFIGURATION

WARNING: THIS WILL ERASE THE CURRENT CONFIGURATION IN THE EDGEROUTER

Login to the GUI by accessing the local subnet defined in the EdgeRouter. For example, if the subnet is 192.168.40.0/24, the usual local router IP is 192.168.40.1.

Click **System** then scroll to the bottom

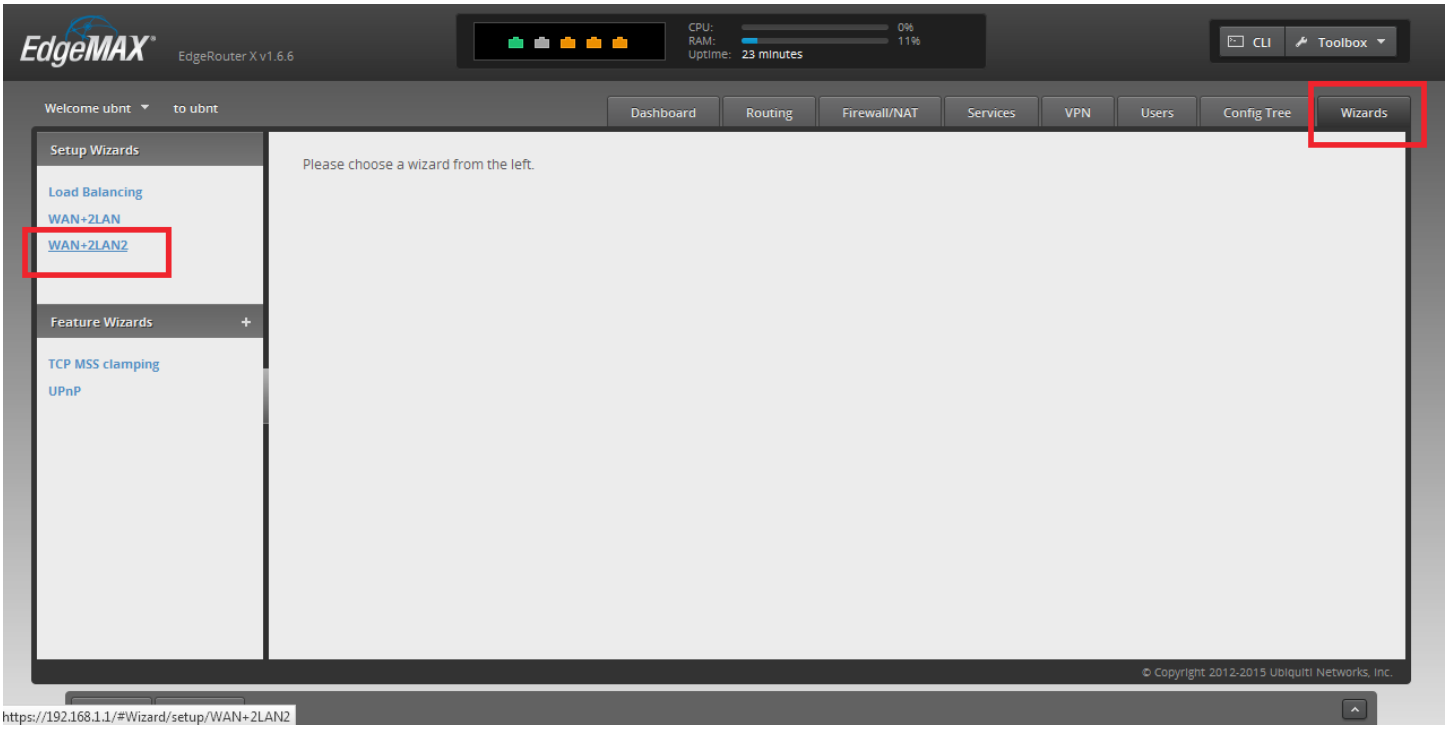
Click “**Reset to Default**”



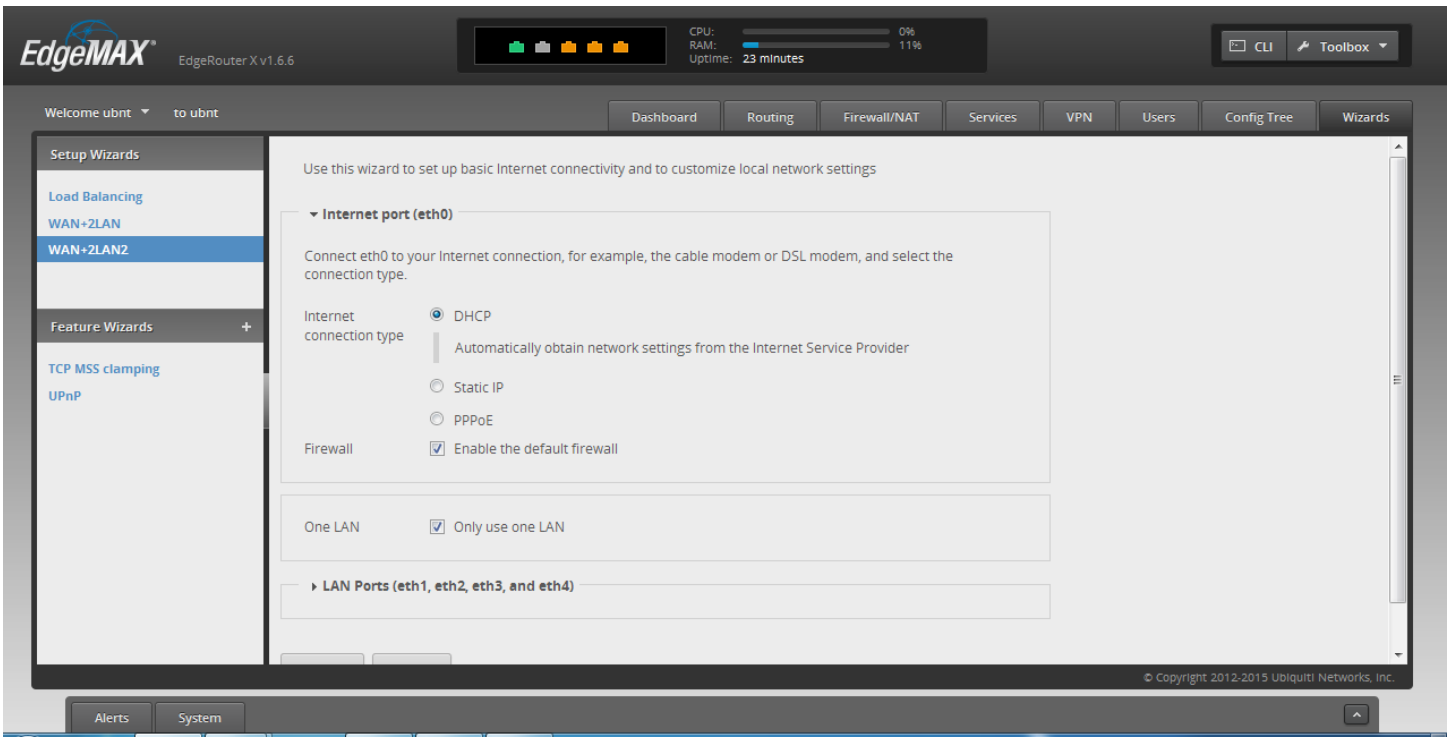
The router will reboot once the configuration has been set to default. The initial IP configuration will be set to 192.168.1.0/24 and ETH0 will be 192.168.1.1.

SET WAN AND LAN CONFIGURATION

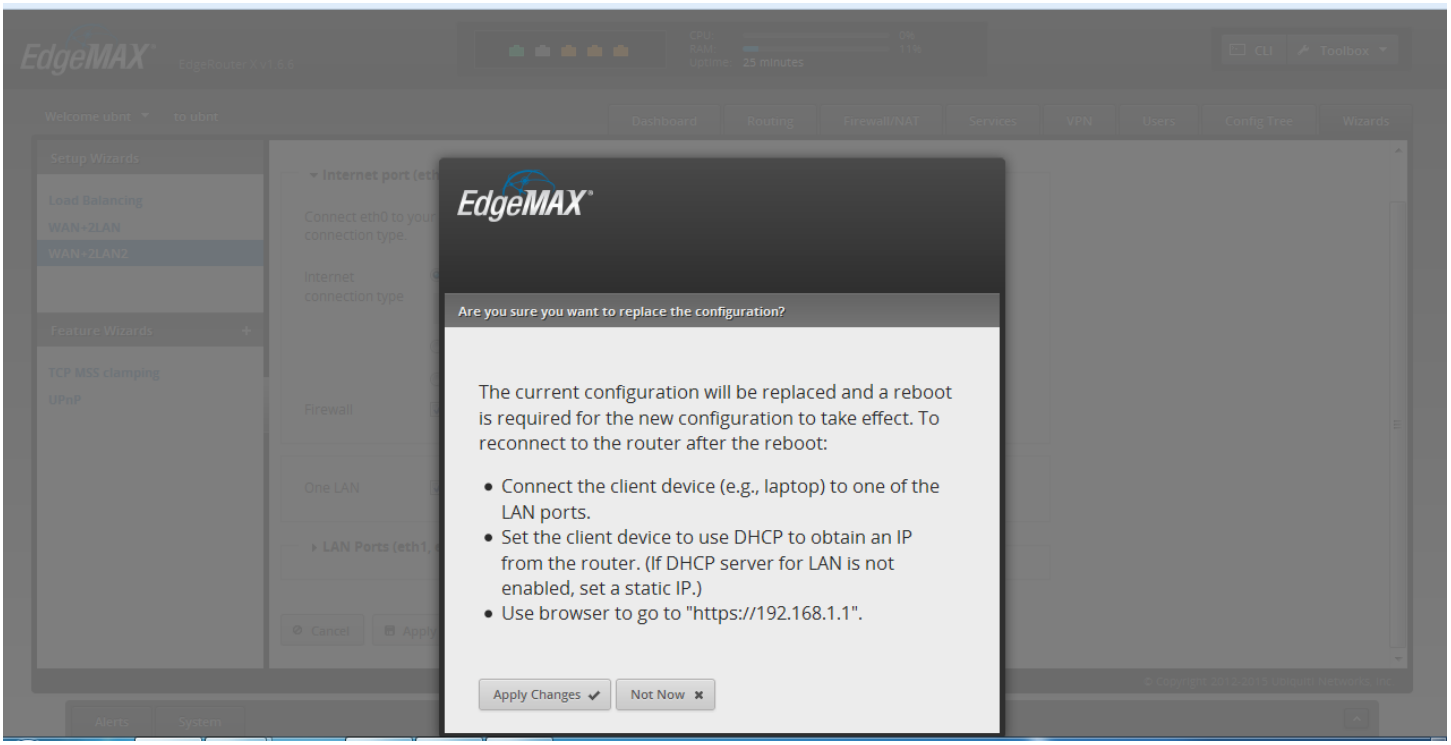
Log back in to the router at 192.168.1.1. Click the **Wizards** tab and then select **WAN+2LAN2.**



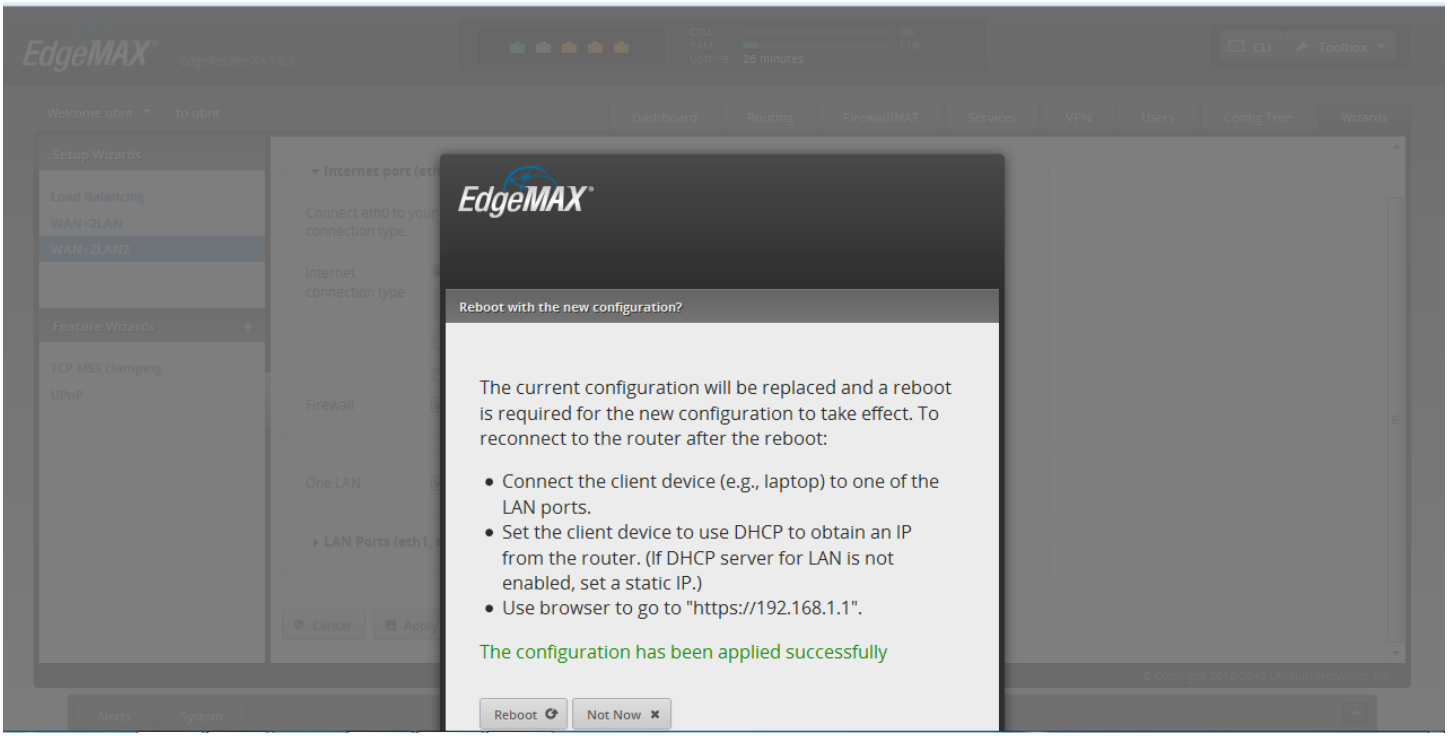
Click **Next**



Click **Apply Changes**



Click **Reboot**. Once the router is back up, eth0 will be dedicated for Internet port and eth1 to eth4 will be in switch mode. The default subnet of the switch will be 192.168.1.0/24.



CUSTOMIZE IPSEC CONFIGURATION

To begin customization, connect to your EdgeRouter with PuTty and run the following command:

```
ubnt@ubnt:~$
ubnt@ubnt:~$ configure
[edit]
ubnt@ubnt#
```

Reference this table again to fill in the correct addresses

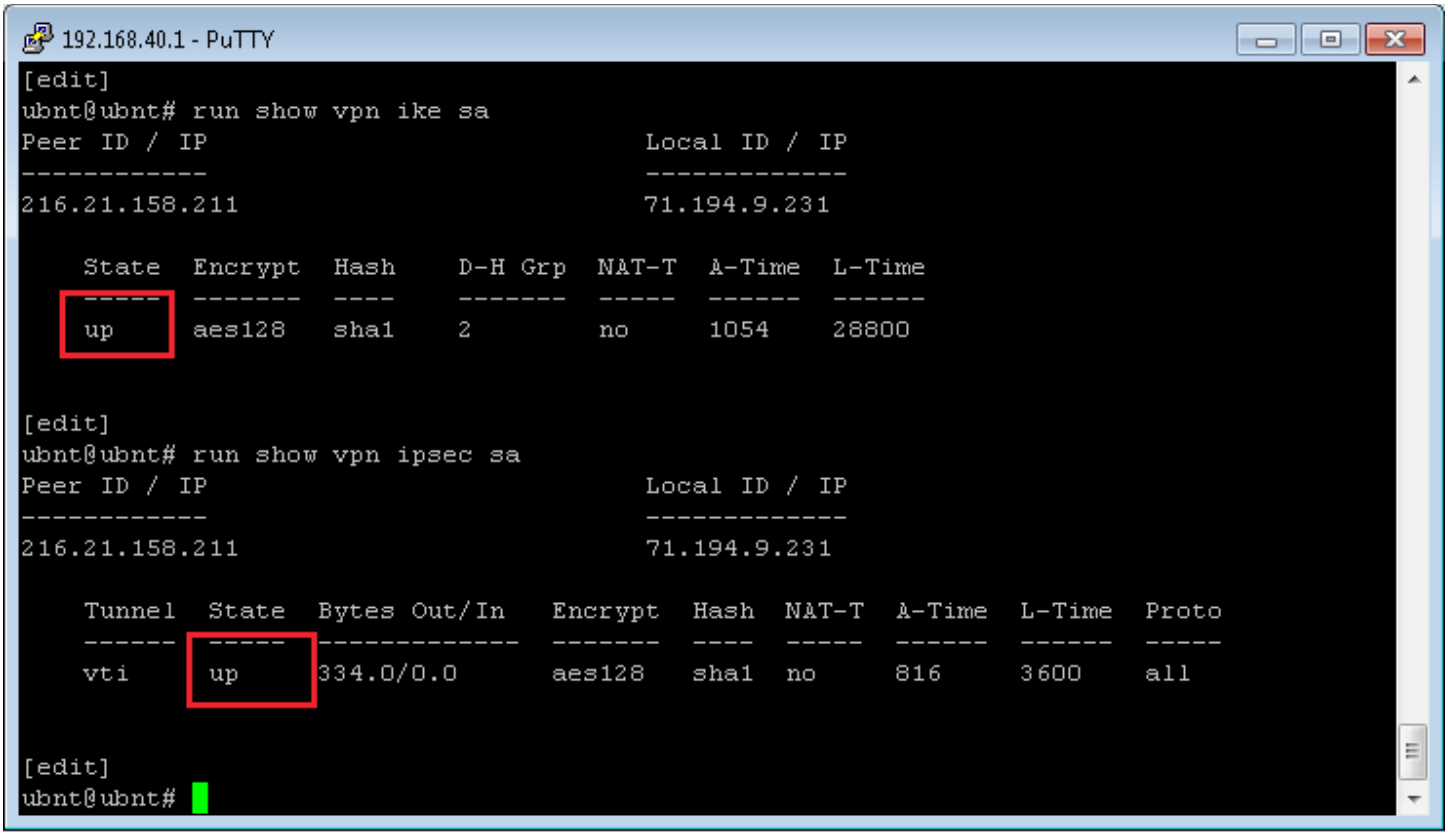
Network	IP	Reference Sample
Local Public IP: (x.x.x.x/mask)		71.194.9.231/23
Local Public GW (x.x.x.x)		71.194.8.1
Local LAN Network (x.x.x.x/mask)		192.168.1.0/24
Cloud Public IP (x.x.x.x)		216.21.158.211
MDS IPSEC VTI IP (x.x.x.x)		10.10.10.1
Cloud IPSEC VTI IP (x.x.x.x)		10.10.10.2
Pre-Shared Secret		XXXXXXXX

Paste this **CLI** configuration in putty ensuring you have modified the correct IP address values shown below in red to reflect your local configuration.

```
set interfaces vti vti0 address 10.10.10.1/30
set interfaces vti vti0 mtu 1436
set protocols static interface-route 0.0.0.0/0 next-hop-interface vti0
set protocols static route 0.0.0.0/0 next-hop 71.194.8.1 distance 20
set protocols static route 216.21.158.211/32 next-hop 71.194.8.1 distance 10
set vpn ipsec auto-firewall-nat-exclude enable
set vpn ipsec esp-group noPFS compression disable
set vpn ipsec esp-group noPFS lifetime 3600
set vpn ipsec esp-group noPFS mode tunnel
set vpn ipsec esp-group noPFS pfs disable
set vpn ipsec esp-group noPFS proposal 1 encryption aes128
set vpn ipsec esp-group noPFS proposal 1 hash sha1
set vpn ipsec ike-group IKE1 key-exchange ikev1
set vpn ipsec ike-group IKE1 lifetime 28800
set vpn ipsec ike-group IKE1 proposal 1 dh-group 2
set vpn ipsec ike-group IKE1 proposal 1 encryption aes128
set vpn ipsec ike-group IKE1 proposal 1 hash sha1
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn ipsec nat-traversal enable
set vpn ipsec site-to-site peer 216.21.158.211 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 216.21.158.211 authentication pre-shared-secret XXXXXXX
set vpn ipsec site-to-site peer 216.21.158.211 connection-type initiate
set vpn ipsec site-to-site peer 216.21.158.211 ike-group IKE1
set vpn ipsec site-to-site peer 216.21.158.211 local-address 71.194.9.231
set vpn ipsec site-to-site peer 216.21.158.211 vti bind vti0
set vpn ipsec site-to-site peer 216.21.158.211 vti esp-group noPFS
set system offload hwnat enable
set system offload ipsec enable
commit
save
exit
```

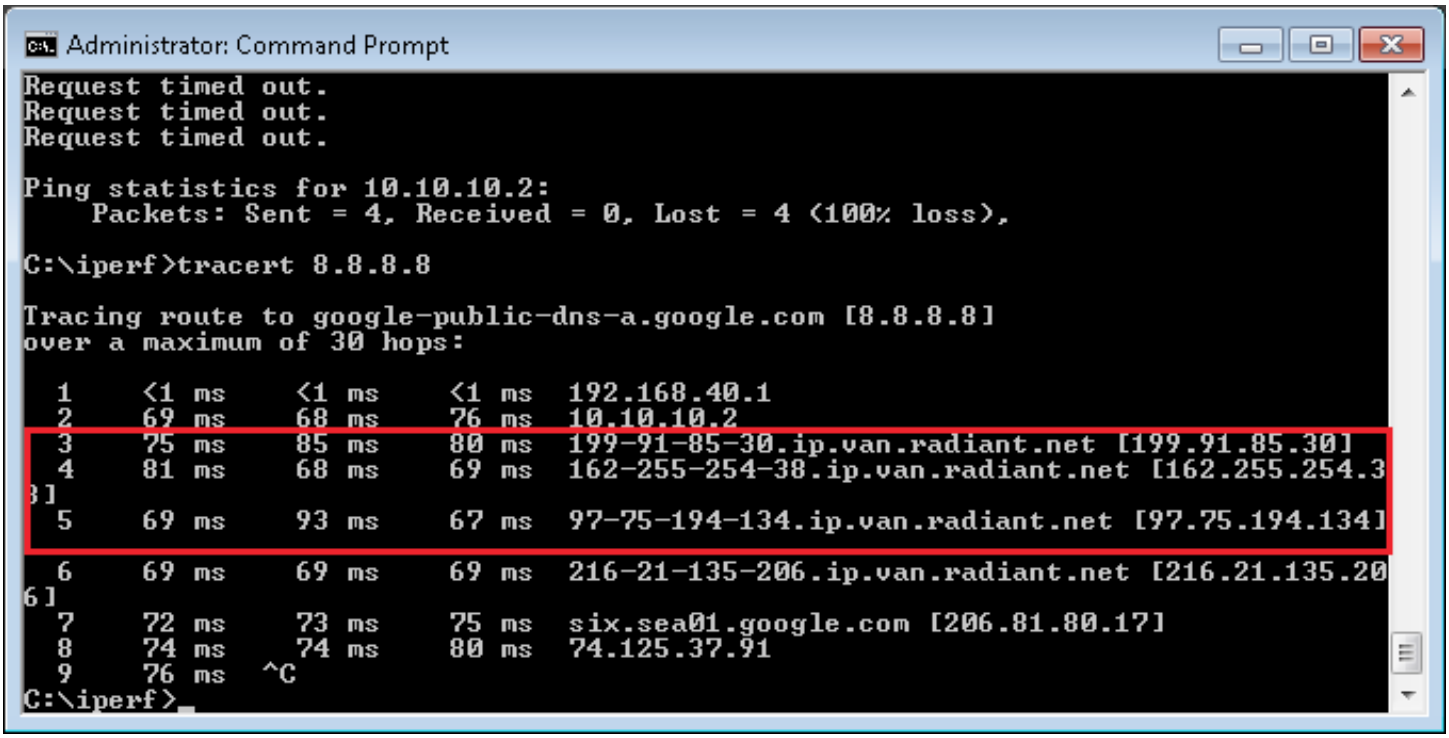
SHOW IPSEC TUNNEL STATUS

The ‘run show vpn ike sa’ shows Phase 1 status. The ‘run show vpn ipsec sa’ shows Phase 2 status. If the state for both phases are up this means that ipsec tunnel is up.



VALIDATE TRAFFIC VIA MDS NODE

Running traceroute to a known public IP address (8.8.8.8) will prove that traffic is traversing to the tunnel.



VALIDATE MDS WEB BLOCK

Download a benign AV string by going here:

http://www.eicar.org/download/eicar.com

NOTES

If you plan on using MDS based SSL-VPN please check with MDS support to help you configure your Ubiquiti with an extra static route that is necessary to enable MDS based SSL-VPN interoperability