AN-300-RT-4L2W NETWORK ROUTER
MDS 3RD PARTY INTEGRATION

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 Araknis AN-300-RT-4L2W. 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 Araknis gateway.

Assumptions

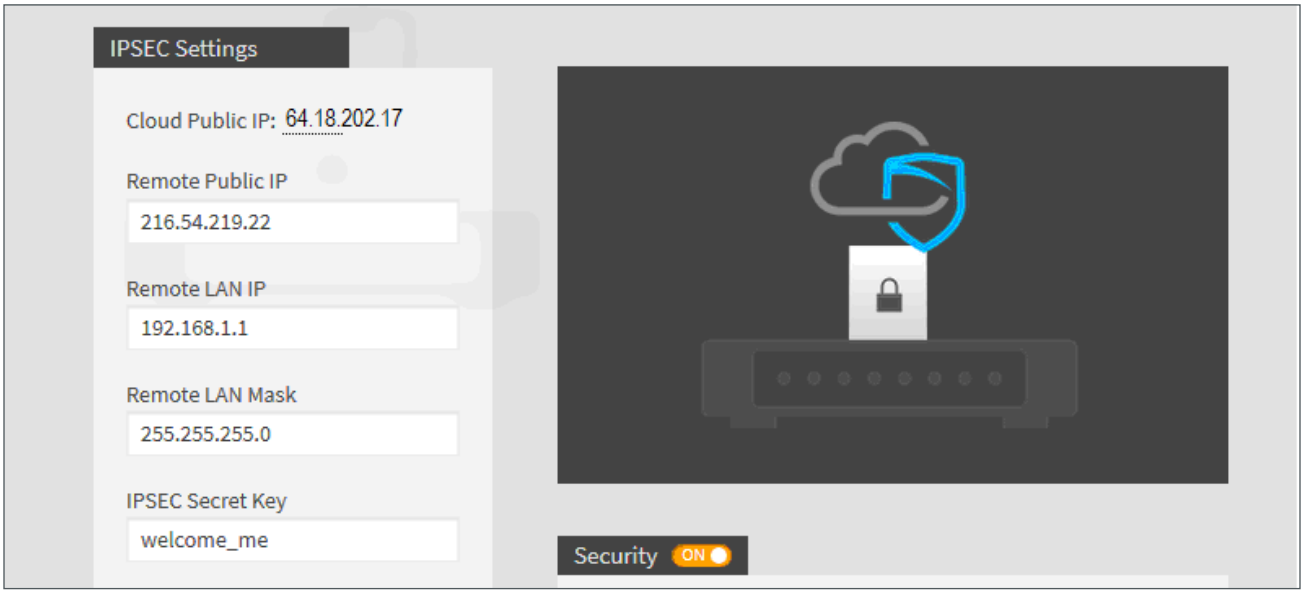
- This guide was developed to provide configuration information of the Araknis gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Araknis AN-300 v1.0.4.7.
- This guide is NOT intended to be a full configuration guide for the Araknis gateway.
- Responsibility for the management of the Araknis gateway is not assumed by MyDigitalShield.
- Proceeding to this guide means that the order has been placed in the MyDigitalShield portal.

What You Will Need

The following IP address information:

- 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 during order and activation.
- Preshared key that was defined during setup on the portal.

Please reference the sample configuration from the MDS portal:



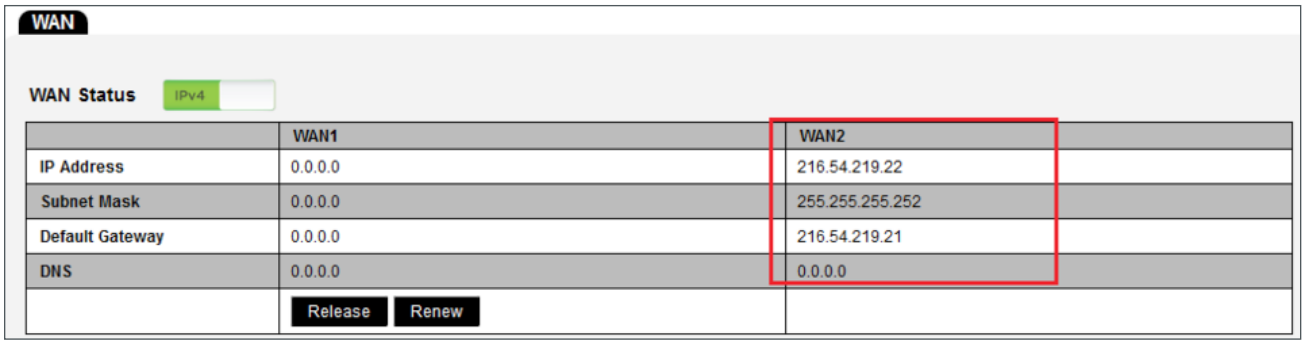
- **Local Public IP –** The local Public IP address/subnet mask that your customer's ISP provides.
- **Local Public GW –** The gateway IP address provided by the customer's ISP.
- **Local LAN Network –** This is the network address that is being used on your customer's LAN.
- **Cloud Public IP –** This 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.

Fill in the middle column of the following table for reference in later sections of this guide. To map IP addresses that are used in this guide, values in the "Reference Sample" column are used.

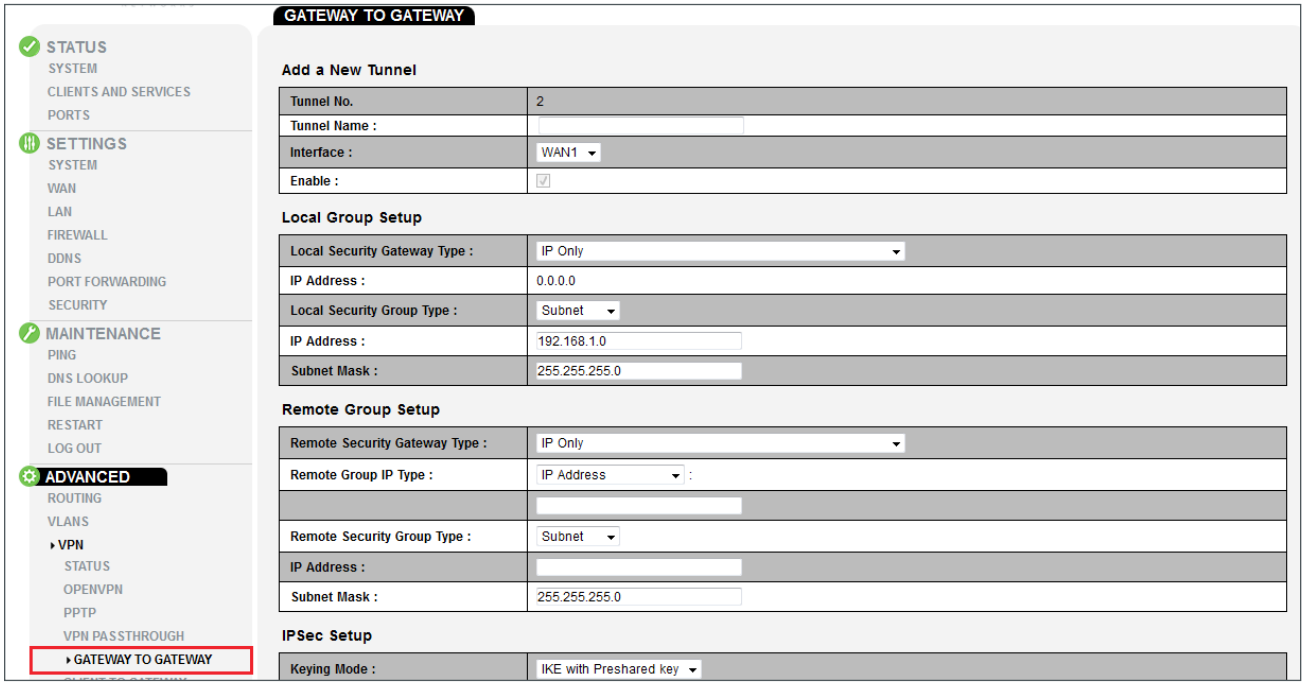
Network	IP	Reference Sample
Local Public IP: (x.x.x.x/mask)		216.54.219.22
Local Public GW (x.x.x.x)		216.54.219.21
Local LAN Network (x.x.x.x/mask)		192.168.1.0/24
Cloud Public IP (x.x.x.x)		64.18.202.17

IPSEC Configuration

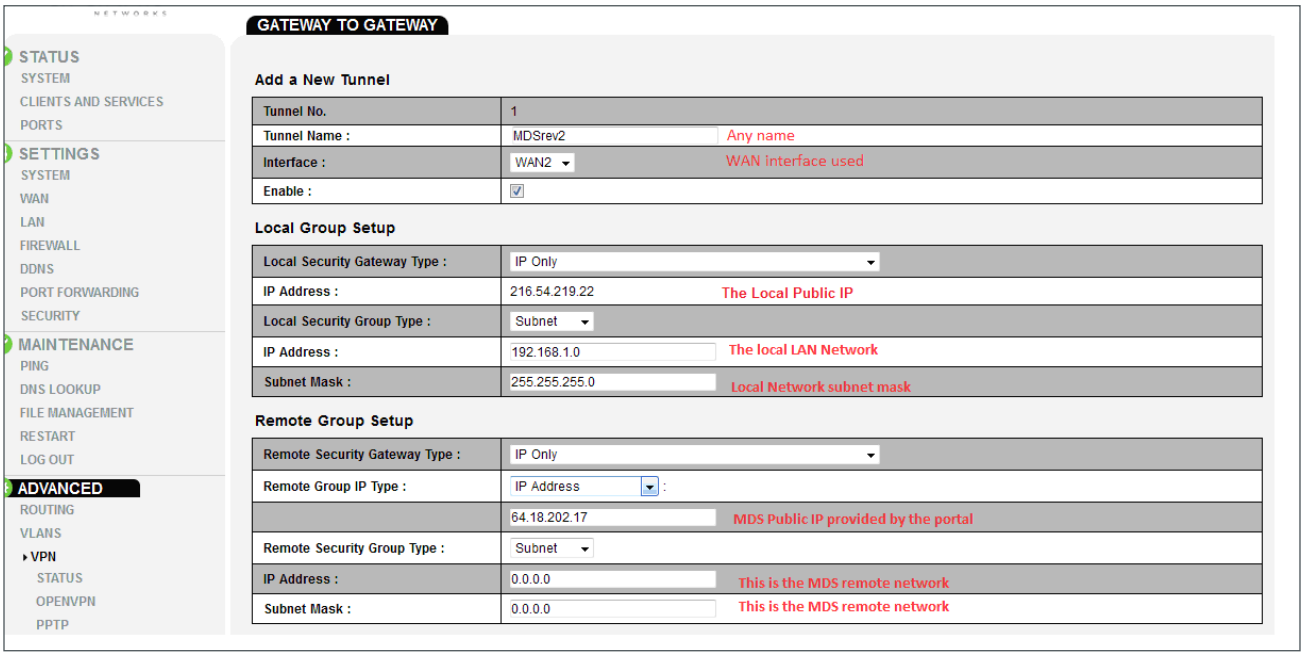
1. Log into the Araknis gateway – **Username:** araknis **Password:** araknis
   You can find your Local Public IP and subnet by going to the Settings > WAN section:



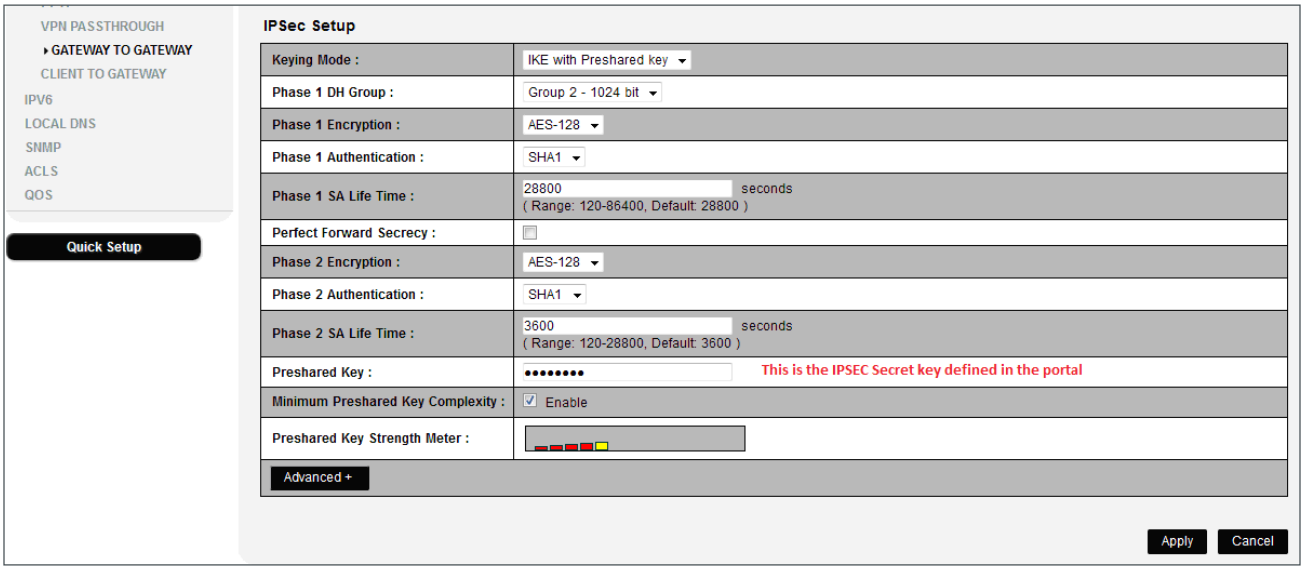
2. Record your local IP information. Then, from the left side menu, click Advanced -> VPN -> Gateway to Gateway to add a new tunnel



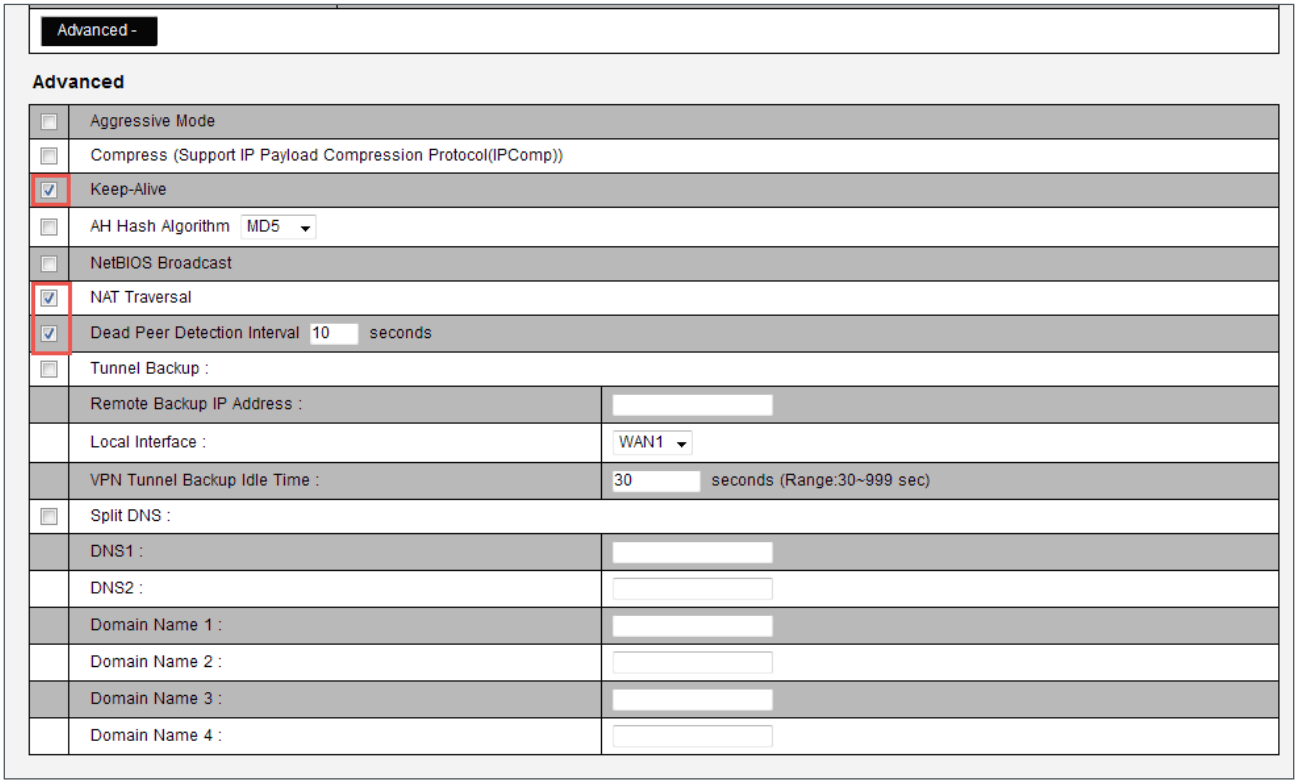
3. Fill in the appropriate fields depicted in the screenshot below:



4. Scroll down and fill in the IPSEC setup. Copy all the fields from the screenshot. Enter the Preshared key defined in the portal.

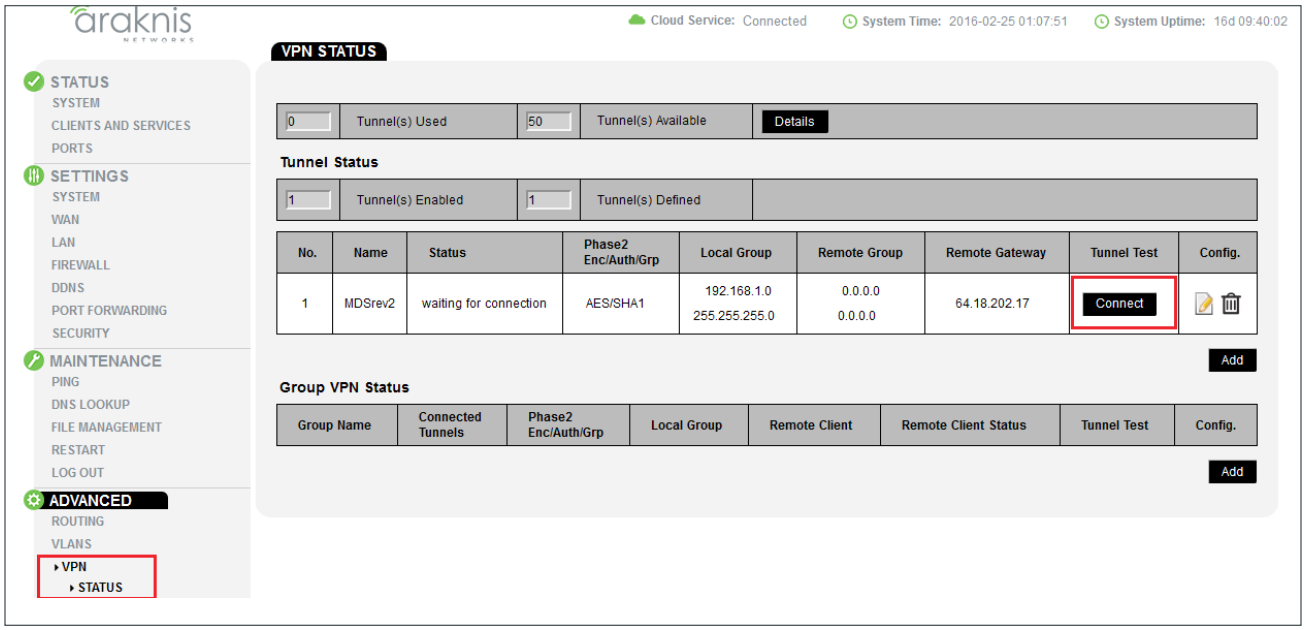


5. Click the Advanced button to expand the Advanced Section. Make sure that the highlighted items in the screenshot are checked, then click Apply.

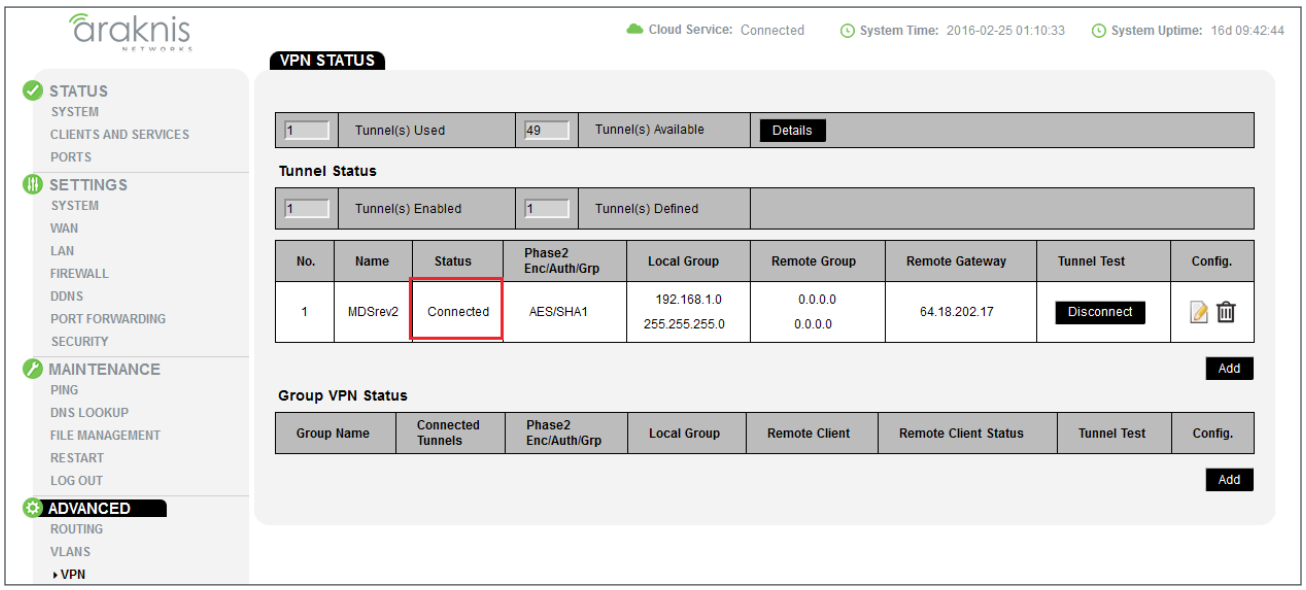


Initiating IPSEC Connection

1. On the left side menu, click VPN -> Status. At this point, the tunnel is not up. Click Connect under Tunnel Test to initiate the connection.

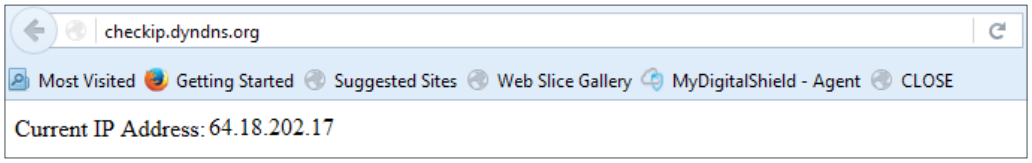


2. The tunnel is up when the Status changes to “Connected”.



Validate Traffic to MDS

From a local computer that is connected in the local subnet, open up the browser and go to checkip.dyndns.org. The Public IP should reflect the MDS node.



Validate MDS Web Block

Access EICAR AV download page:

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

Congratulations!

Your Araknis firewall is now enhanced with the protection of MyDigitalShield Clean Internet!

You can adjust your filtering settings via the MDS Cloud Manager at **https://mdsmanager.com**

For more info on Araknis products, hardware support, and to purchase additional Araknis products go to **http://onaisle8.com**