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

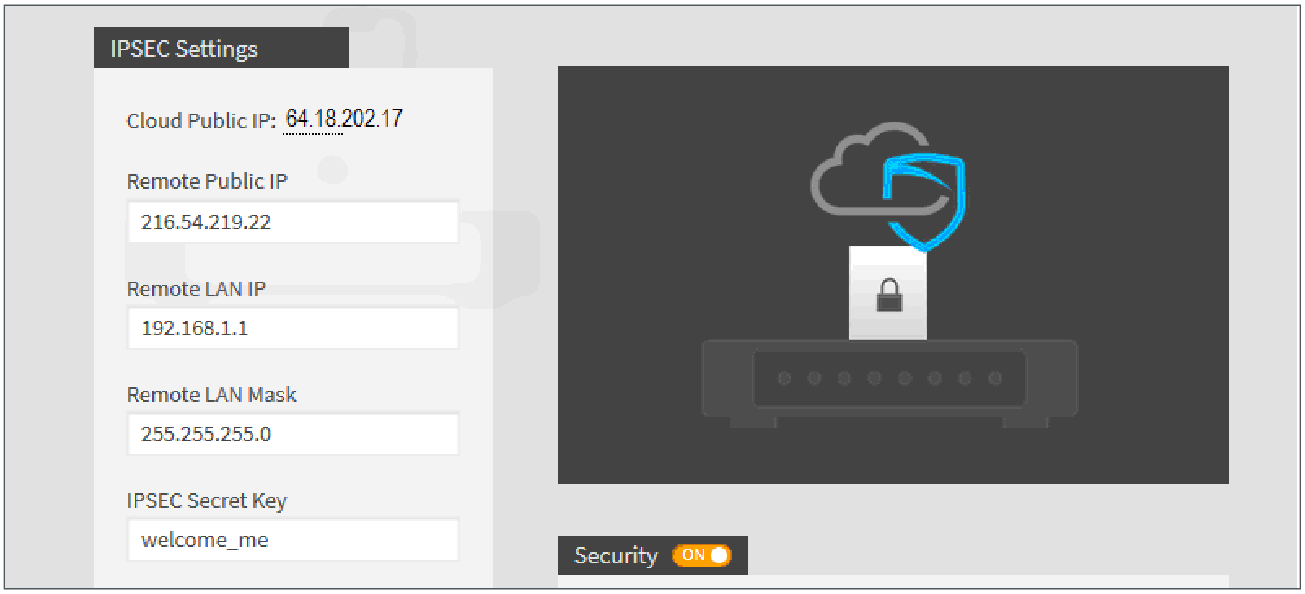
- This guide was developed to provide configuration information of the Araknis gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Araknis AN-300 v1.0.4.7.
- This guide is NOT intended to be a full configuration guide for the Araknis gateway.
- 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:



IPSEC Settings

Cloud Public IP: 64.18.202.17

Remote Public IP: 216.54.219.22

Remote LAN IP: 192.168.1.1

Remote LAN Mask: 255.255.255.0

IPSEC Secret Key: welcome_me

Security ON

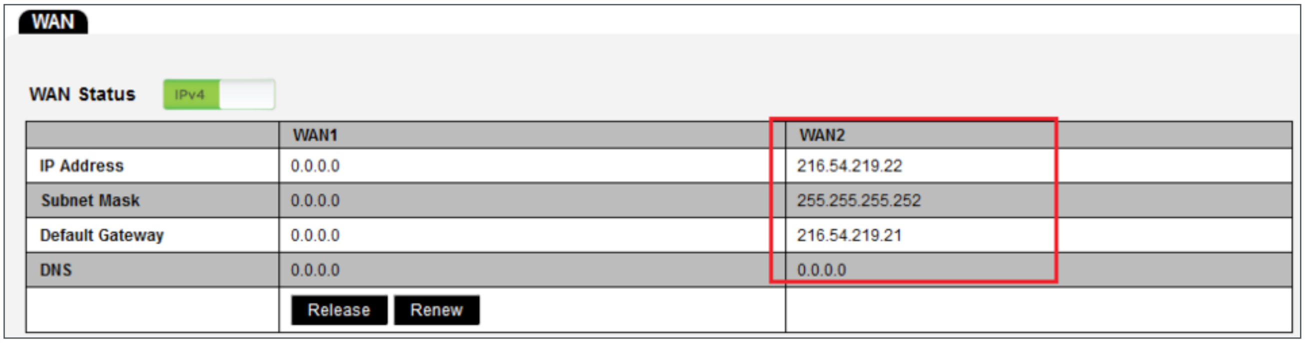
- **Local Public IP –** The local Public IP address/subnet mask that your customer's ISP provides.
- **Local Public GW –** The gateway IP address provided by the customer's ISP.
- **Local LAN Network –** This is the network address that is being used on your customer's LAN.
- **Cloud Public IP –** This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

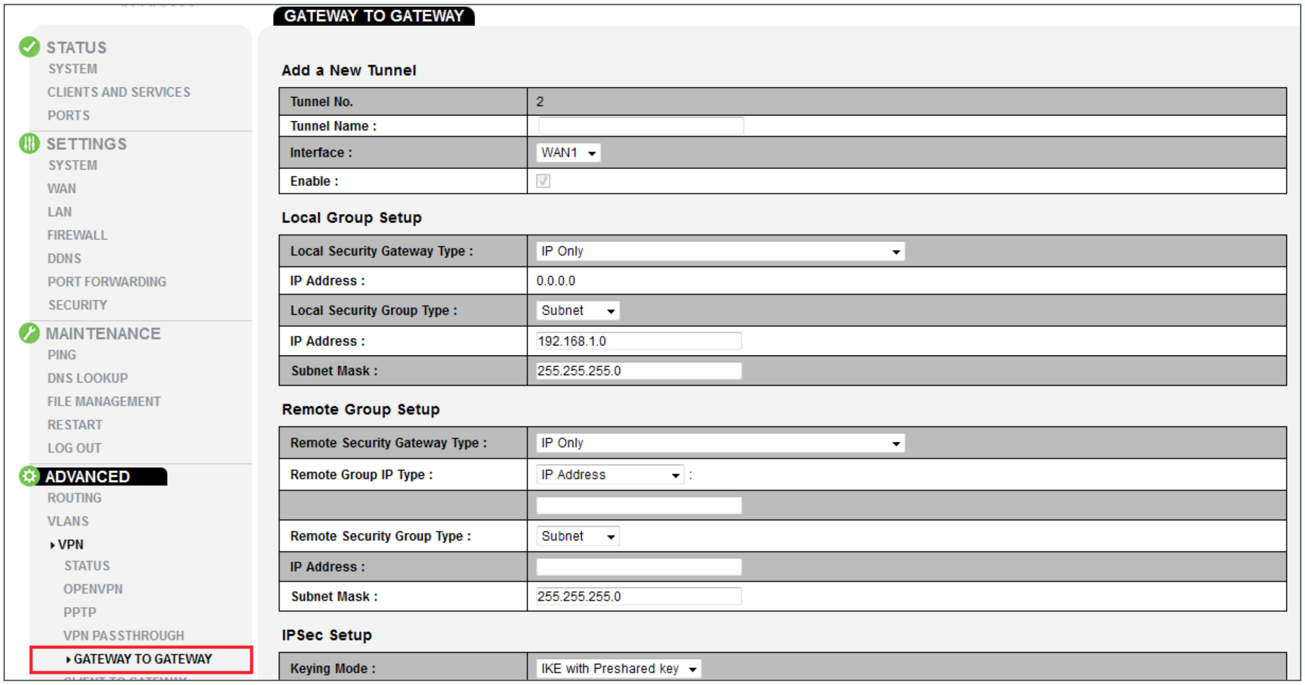


WAN

WAN Status IPv4

	WAN1	WAN2
IP Address	0.0.0.0	216.54.219.22
Subnet Mask	0.0.0.0	255.255.255.252
Default Gateway	0.0.0.0	216.54.219.21
DNS	0.0.0.0	0.0.0.0
	Release Renew	

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



GATEWAY TO GATEWAY

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	0.0.0.0
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

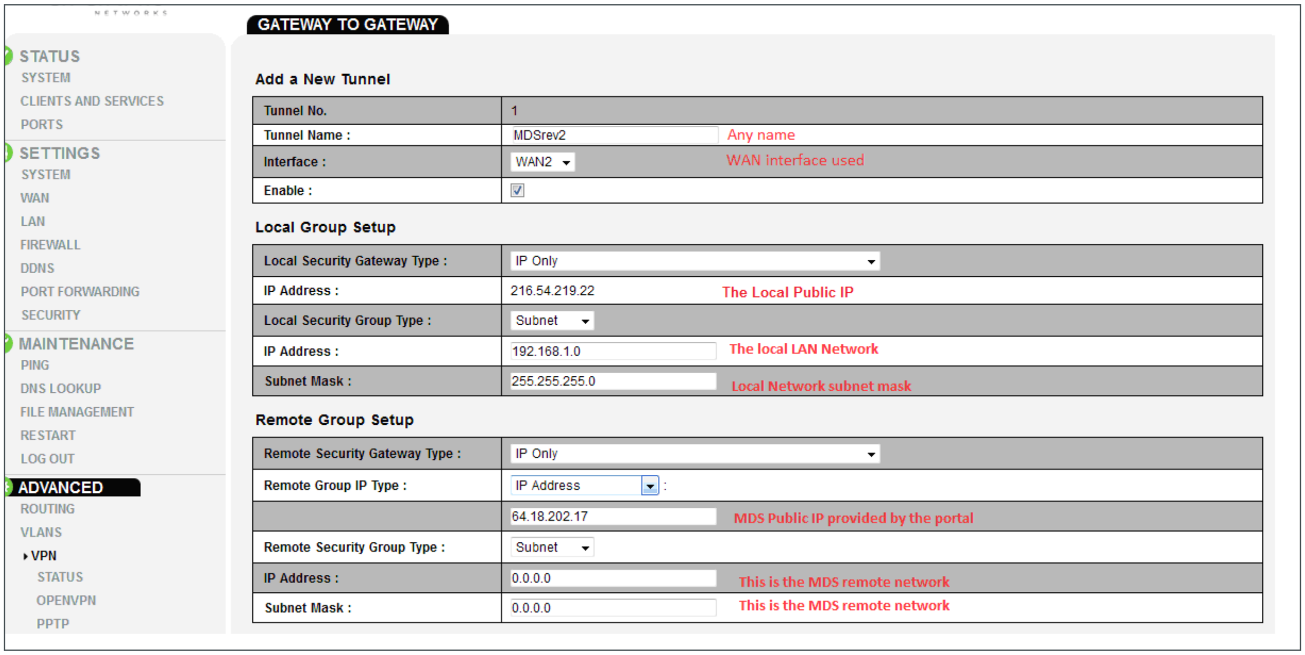
Remote Group Setup

Remote Security Gateway Type :	IP Only
Remote Group IP Type :	IP Address :
Remote Security Group Type :	Subnet
IP Address :	
Subnet Mask :	255.255.255.0

IPSec Setup

Keying Mode :	IKE with Preshared key

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



GATEWAY TO GATEWAY

Add a New Tunnel

Tunnel No.	1	
Tunnel Name :	MDSrev2	Any name
Interface :	WAN2	WAN interface used
Enable :	☑	

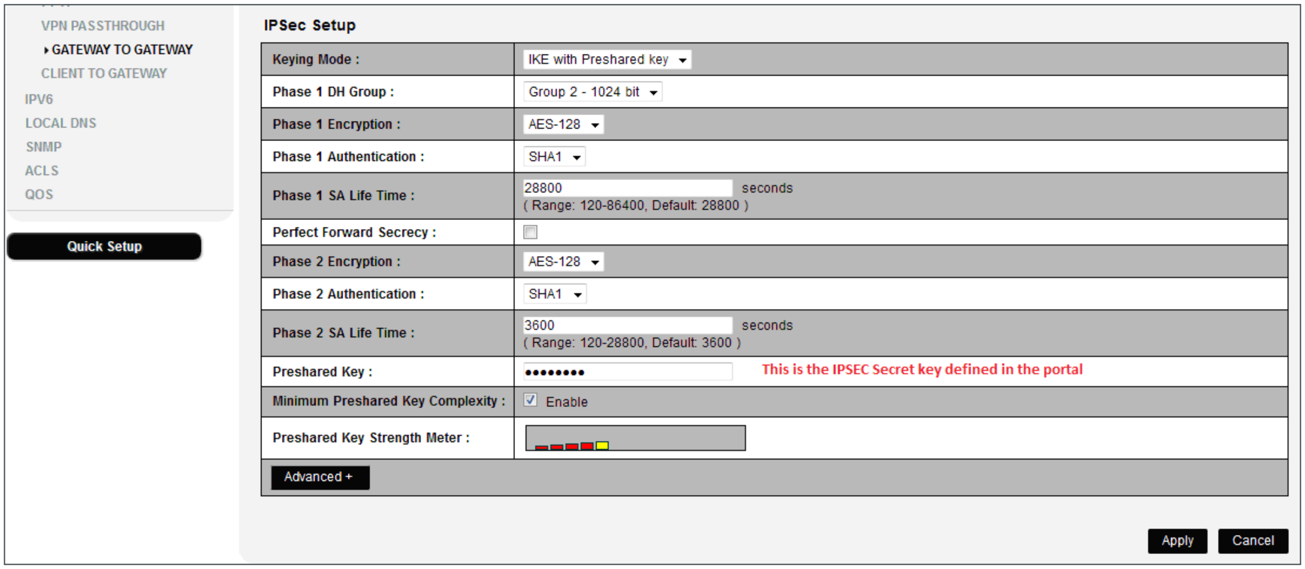
Local Group Setup

Local Security Gateway Type :	IP Only	
IP Address :	216.54.219.22	The Local Public IP
Local Security Group Type :	Subnet	
IP Address :	192.168.1.0	The local LAN Network
Subnet Mask :	255.255.255.0	Local Network subnet mask

Remote Group Setup

Remote Security Gateway Type :	IP Only	
Remote Group IP Type :	IP Address :	
	64.18.202.17	MDS Public IP provided by the portal
Remote Security Group Type :	Subnet	
IP Address :	0.0.0.0	This is the MDS remote network
Subnet Mask :	0.0.0.0	This is the MDS remote network

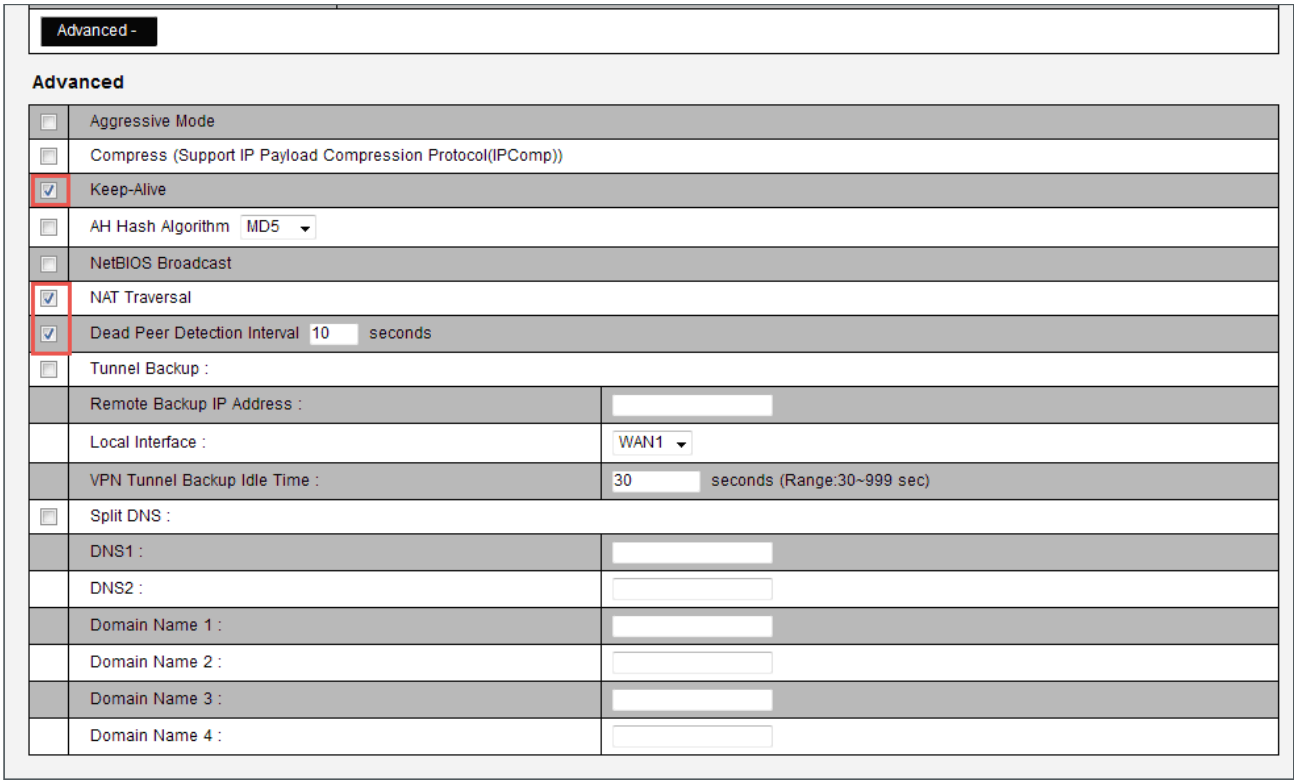
4. Scroll down and fill in the IPSEC setup. Copy all the fields from the screenshot. Enter the Preshared key defined in the portal.



IPSec Setup

Keying Mode :	IKE with Preshared key	
Phase 1 DH Group :	Group 2 - 1024 bit	
Phase 1 Encryption :	AES-128	
Phase 1 Authentication :	SHA1	
Phase 1 SA Life Time :	28800 seconds (Range: 120-86400, Default: 28800)	
Perfect Forward Secrecy :	□	
Phase 2 Encryption :	AES-128	
Phase 2 Authentication :	SHA1	
Phase 2 SA Life Time :	3600 seconds (Range: 120-28800, Default: 3600)	
Preshared Key :	••••••••	This is the IPSEC Secret key defined in the portal
Minimum Preshared Key Complexity :	☑ Enable	
Preshared Key Strength Meter :		

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

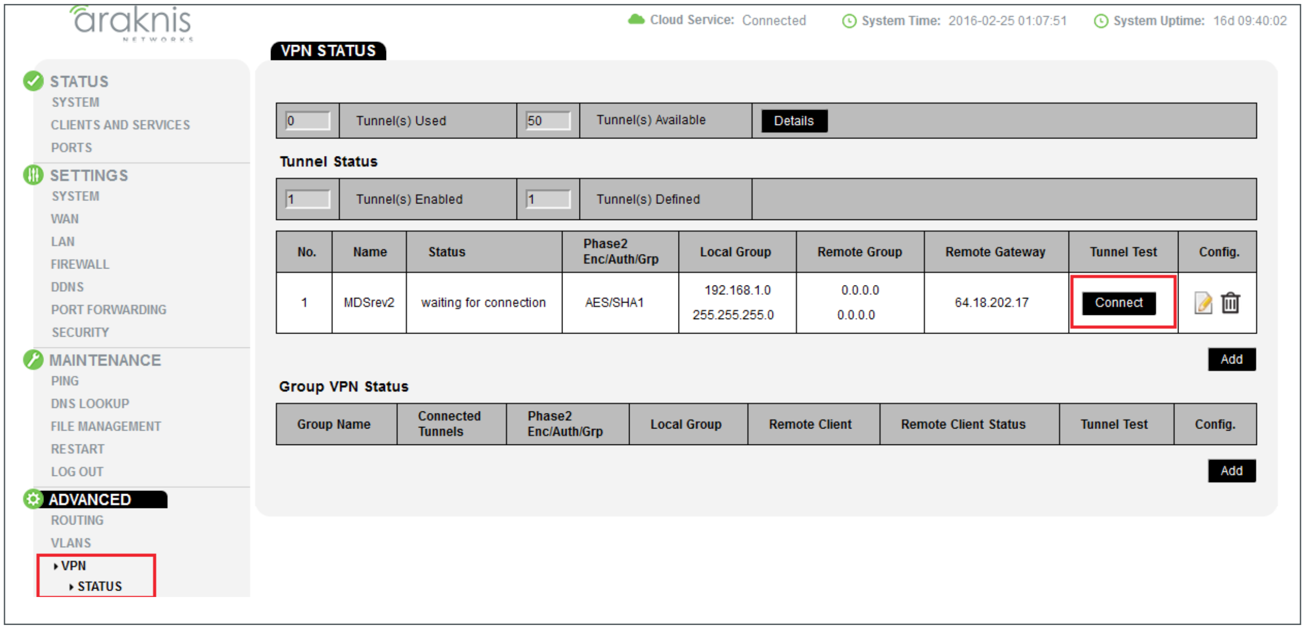


Advanced

☐	Aggressive Mode	
☐	Compress (Support IP Payload Compression Protocol(IPComp))	
☑	Keep-Alive	
☐	AH Hash Algorithm MD5	
☐	NetBIOS Broadcast	
☑	NAT Traversal	
☑	Dead Peer Detection Interval 10 seconds	
☐	Tunnel Backup :	
	Remote Backup IP Address :	
	Local Interface :	WAN1
	VPN Tunnel Backup Idle Time :	30 seconds (Range:30~999 sec)
☐	Split DNS :	
	DNS1 :	
	DNS2 :	
	Domain Name 1 :	
	Domain Name 2 :	
	Domain Name 3 :	
	Domain Name 4 :	

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.



Cloud Service: Connected System Time: 2016-02-25 01:07:51 System Uptime: 16d 09:40:02

VPN STATUS

0	Tunnel(s) Used	50	Tunnel(s) Available

Tunnel Status

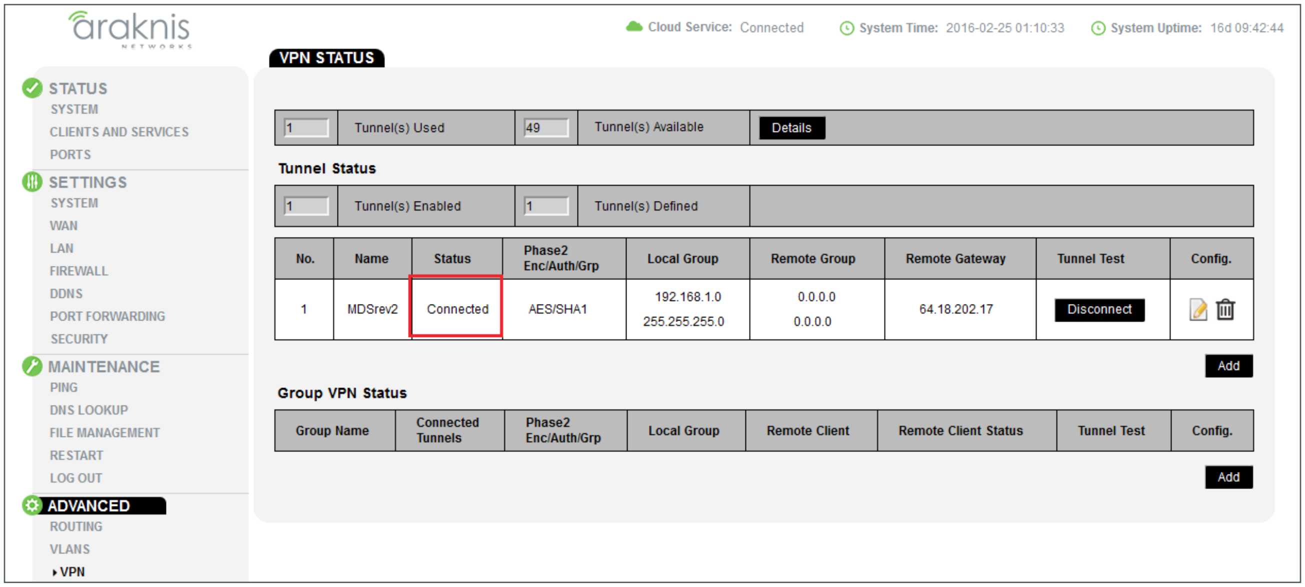
1	Tunnel(s) Enabled	1	Tunnel(s) Defined

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	MDSrev2	waiting for connection	AES/SHA1	192.168.1.0 255.255.255.0	0.0.0.0 0.0.0.0	64.18.202.17	Connect	

Group VPN Status

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.

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



Cloud Service: Connected System Time: 2016-02-25 01:10:33 System Uptime: 16d 09:42:44

VPN STATUS

1	Tunnel(s) Used	49	Tunnel(s) Available

Tunnel Status

1	Tunnel(s) Enabled	1	Tunnel(s) Defined

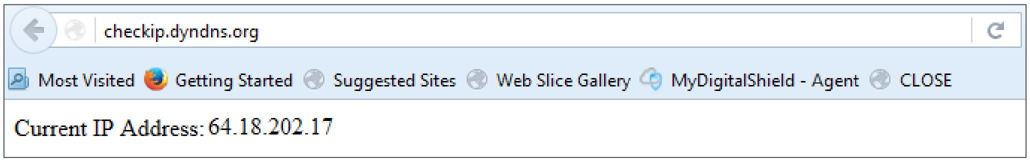
No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	MDSrev2	Connected	AES/SHA1	192.168.1.0 255.255.255.0	0.0.0.0 0.0.0.0	64.18.202.17	Disconnect	

Group VPN Status

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.

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.

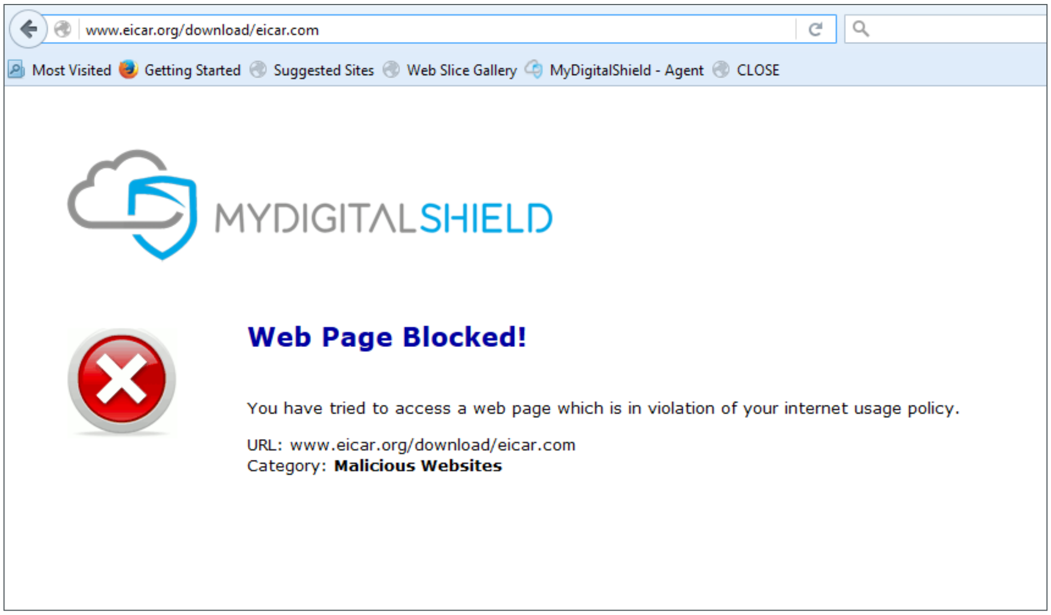


Current IP Address: 64.18.202.17

Validate MDS Web Block

Access EICAR AV download page:

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



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: www.eicar.org/download/eicar.com
Category: **Malicious Websites**

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**