Fortigate
MDS BYOG Integration Guide

CONTENTS

INTRODUCTION

Congratulations on your sale of MyDigitalShield using the BYOG option.

This guide is written specifically for the **Fortigate (FortiOS 5.2)** It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

ASSUMPTIONS

- This guide was developed to provide configuration information of the Fortigate running FortiOS 5.2 specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Fortigate FortiOS 5.2.4
- This guide is NOT intended to be a full configuration guide for the Fortigate gateway
- It is assumed that an Internet port and Lan port are configured and operational.
- Responsibility of the management of the Fortigate gateway is not assumed by MyDigitalShield.
- Proceeding to this guide means that the order has been placed in the MyDigitalShield portal.

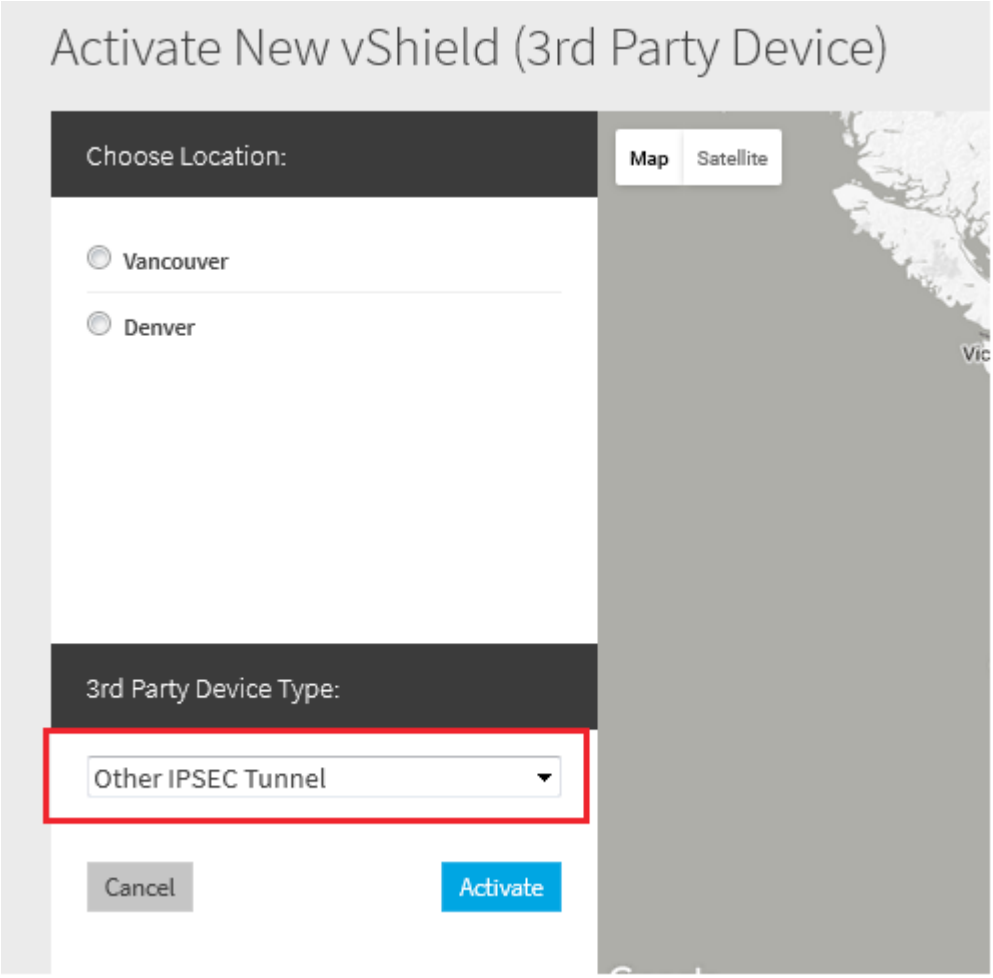
WHAT YOU WILL NEED

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.

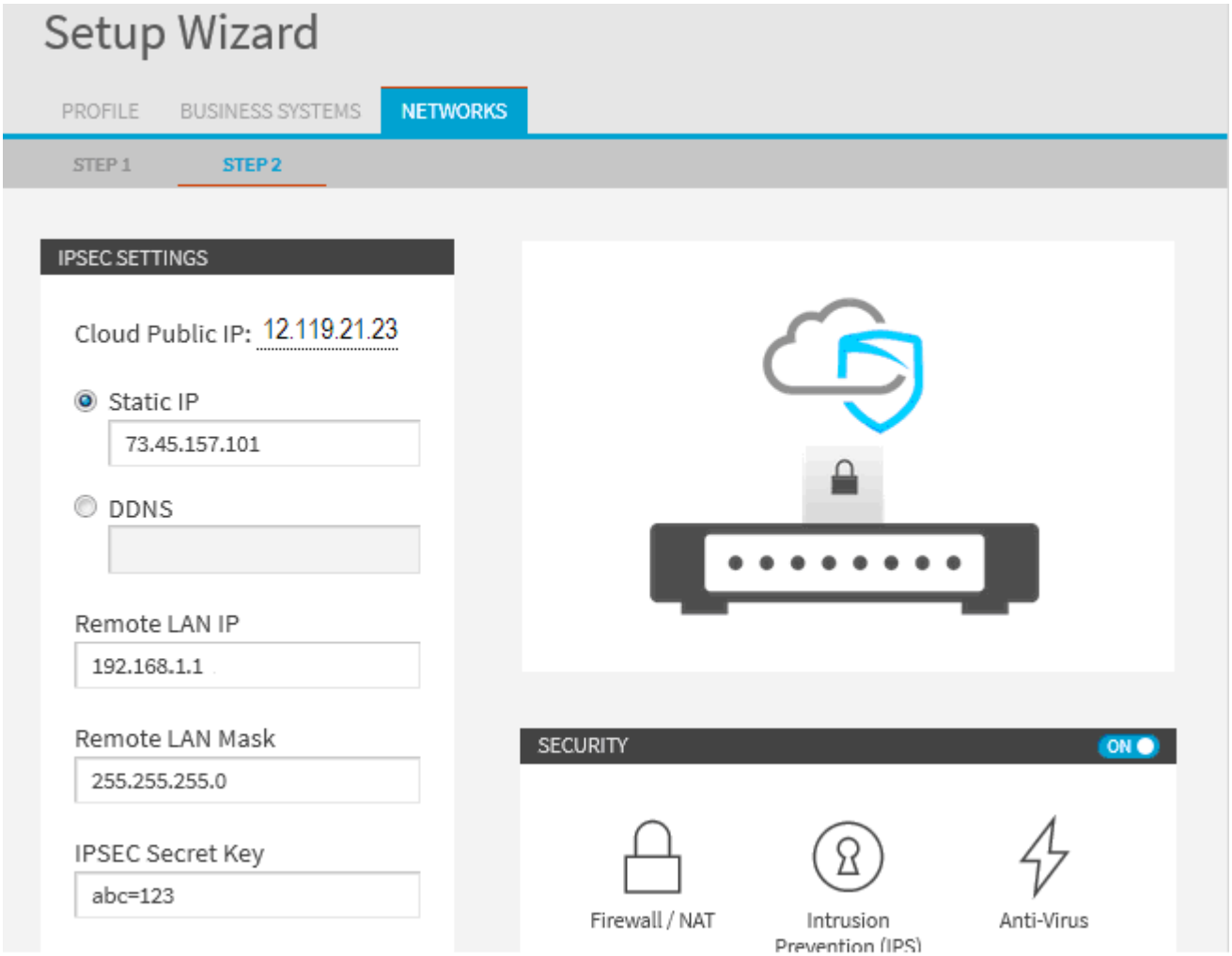
ACTIVATION PROCESS

Please select the “Other IPSEC Tunnel” during activation



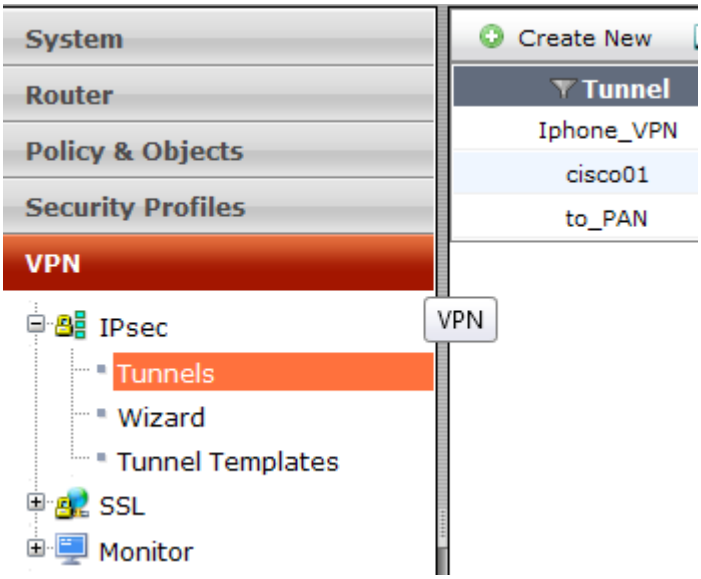
Setup Process from the Portal

Please reference the sample configuration from the MDS portal

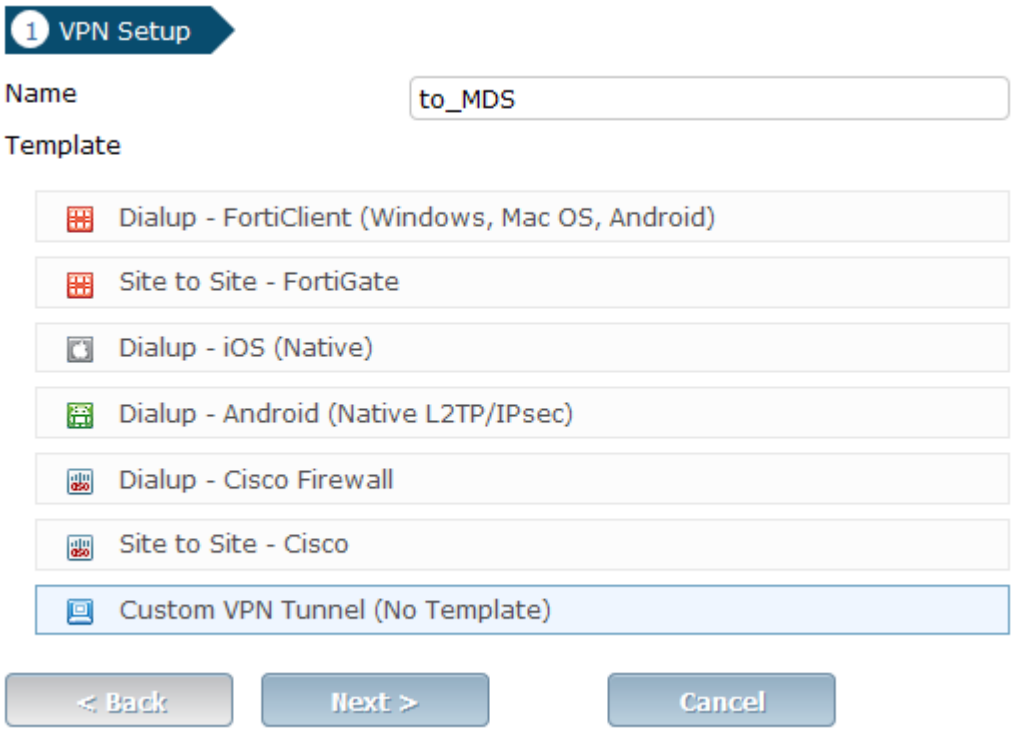


IPSEC CONFIGURATION

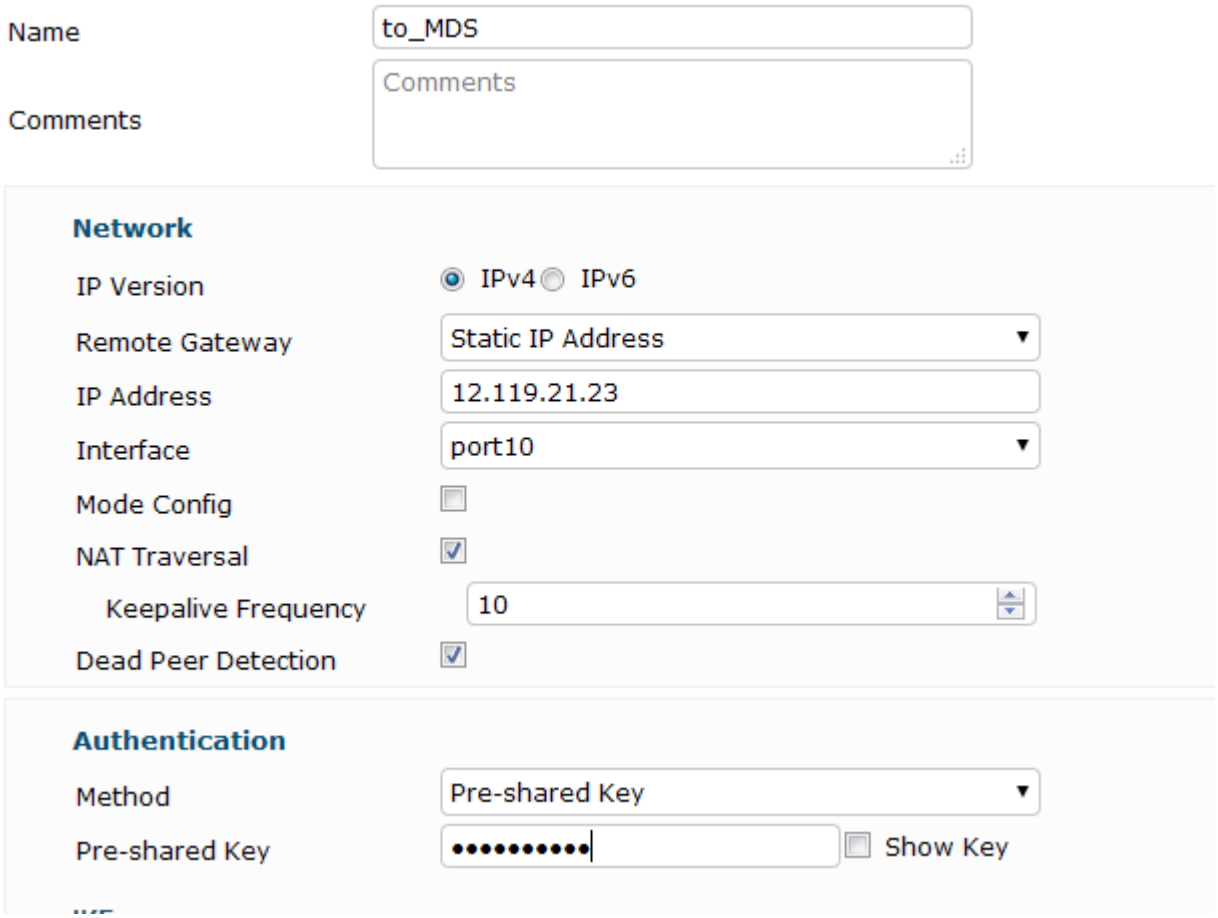
From the Fortigate UI, go to **VPN > IPsec > Tunnels**. Click Create **New**.



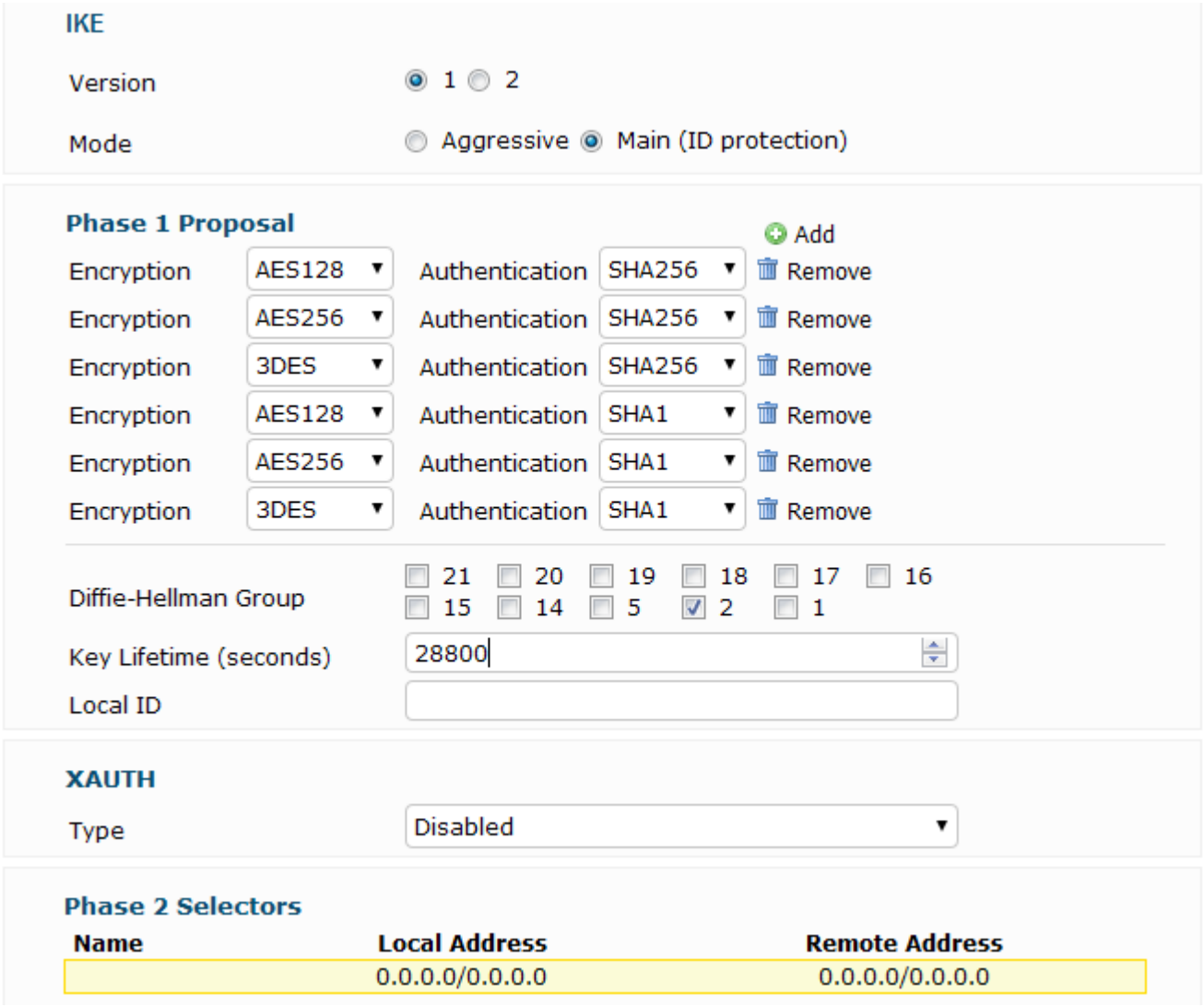
Type the tunnel name and select Custom VPN tunnel. Then click **Next**.



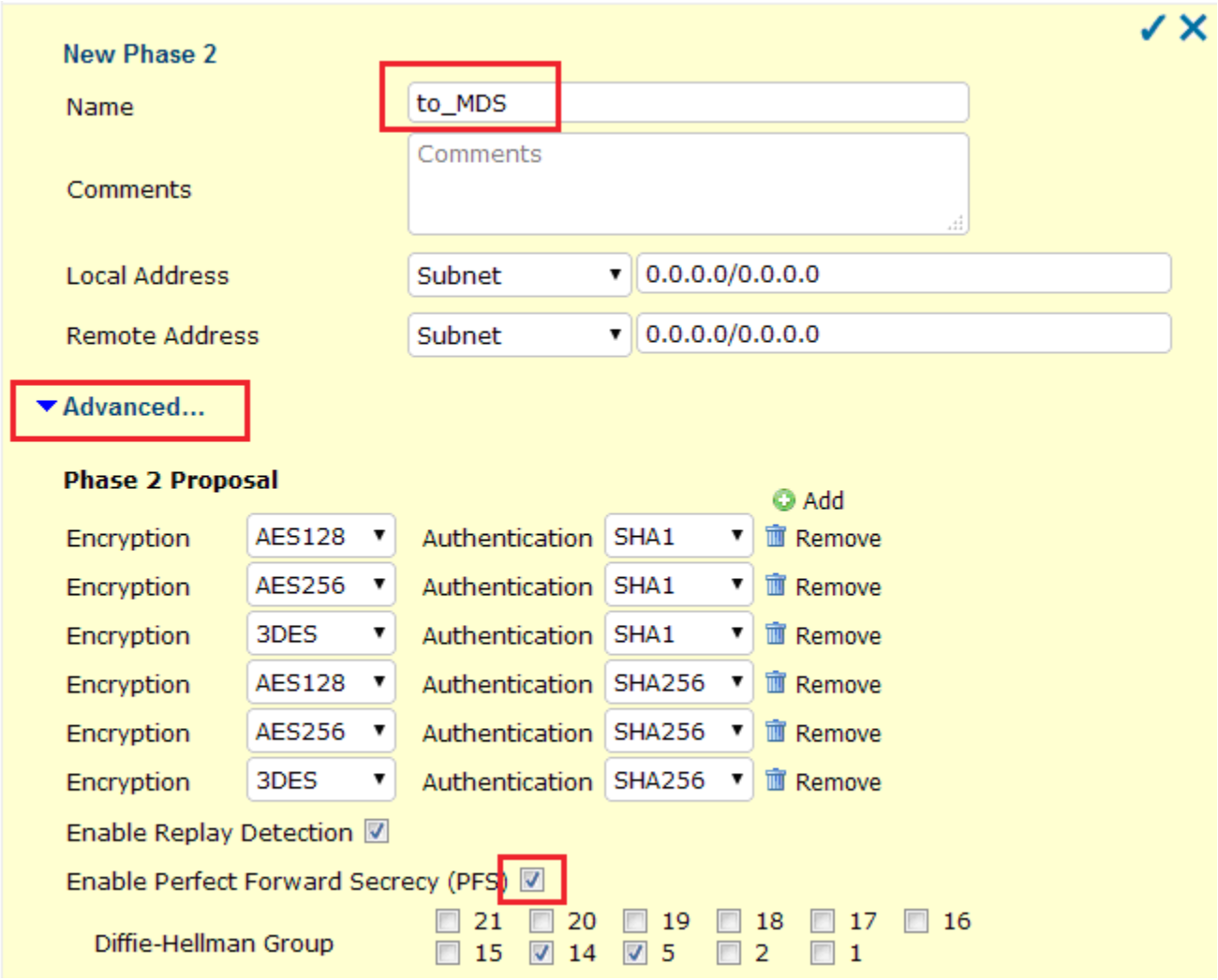
In the next step, set the remote gateway ip address (the Cloud Public IP in the MDS Cloud Manager). In this example, it is 12.119.21.23. Select the interface where the ipsec tunnel will terminate. In this example, port10 is being used. Set a secure Pre-Shared key (IPSEC Secret Key), which you entered in the portal.



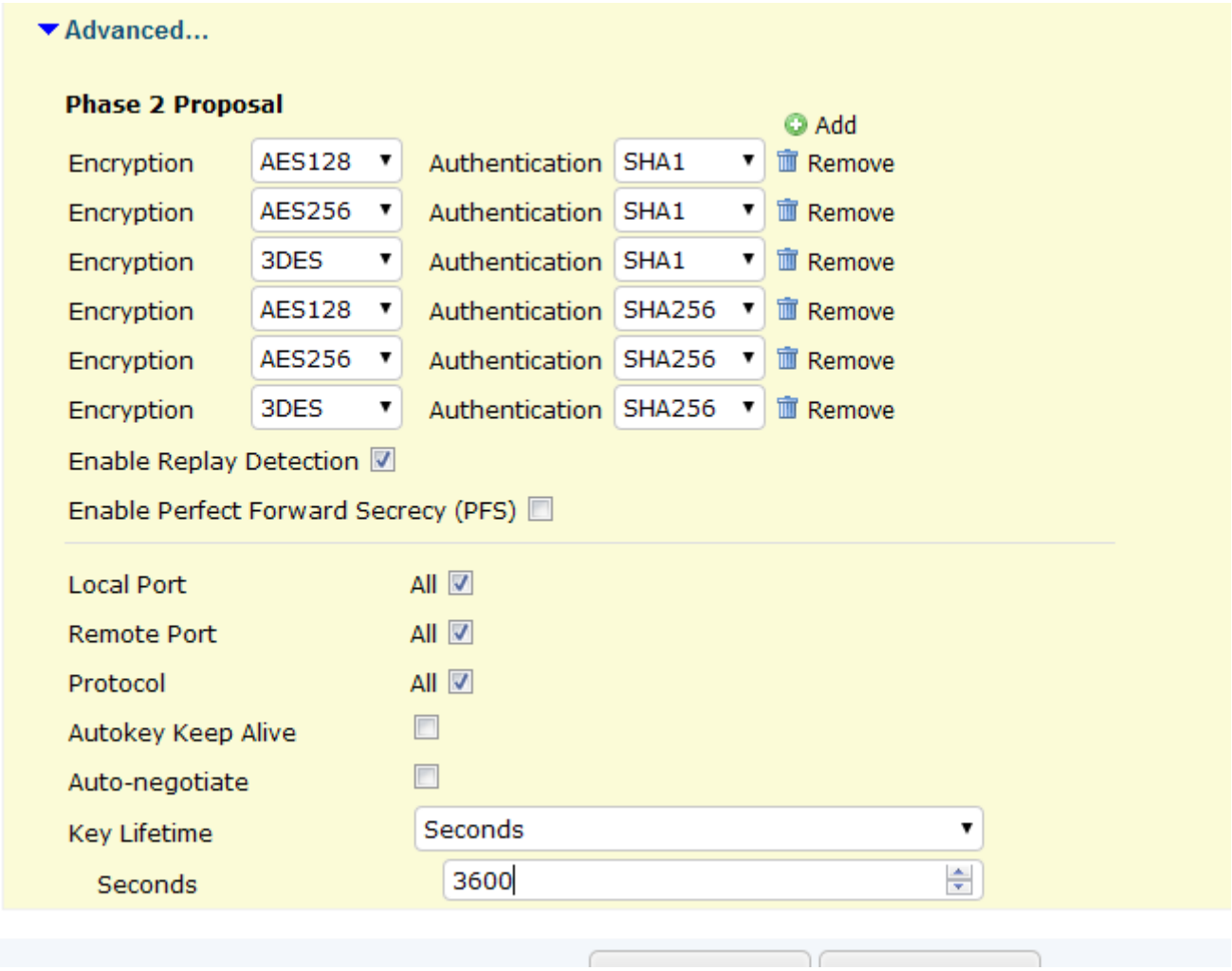
Enter selections as shown below:



Enter a Phase name (example “to_MDS”). Expand Advanced arrow. Untick “Enable Perfect Forward Secrecy (PFS).”

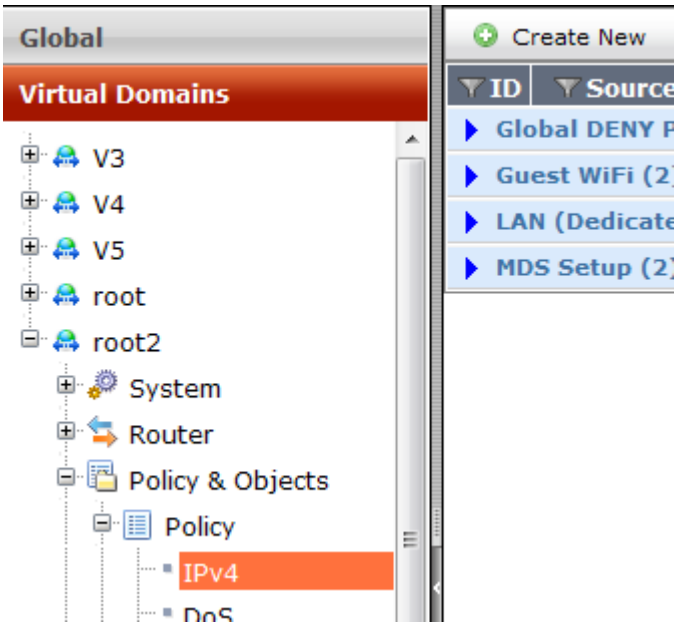


Set the Key Lifetime to **3600 seconds**



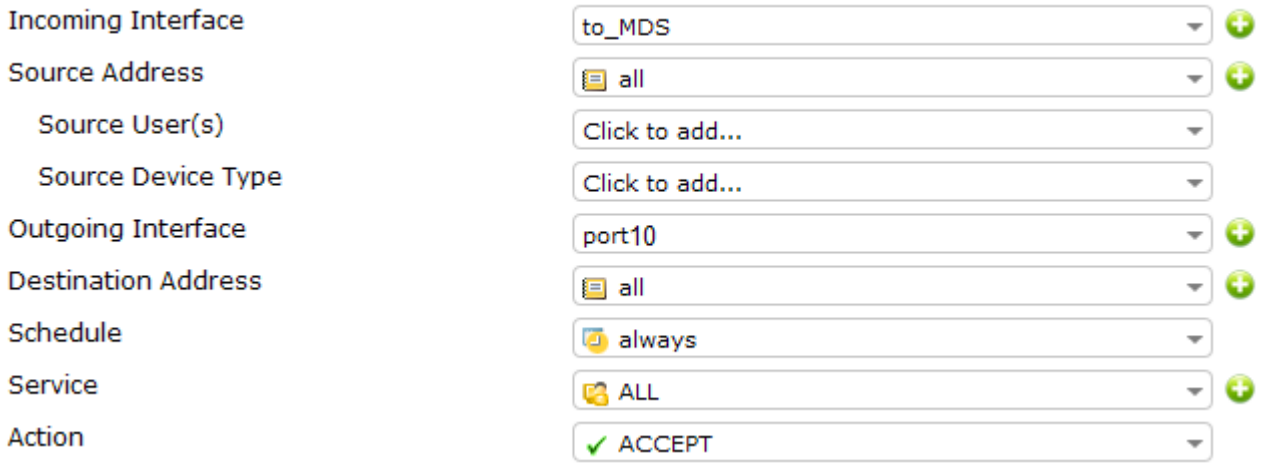
CREATE FIREWALL POLICY

Select Policy & Objects > Policy > IPv4. Click **Create New** to create a new Firewall policy

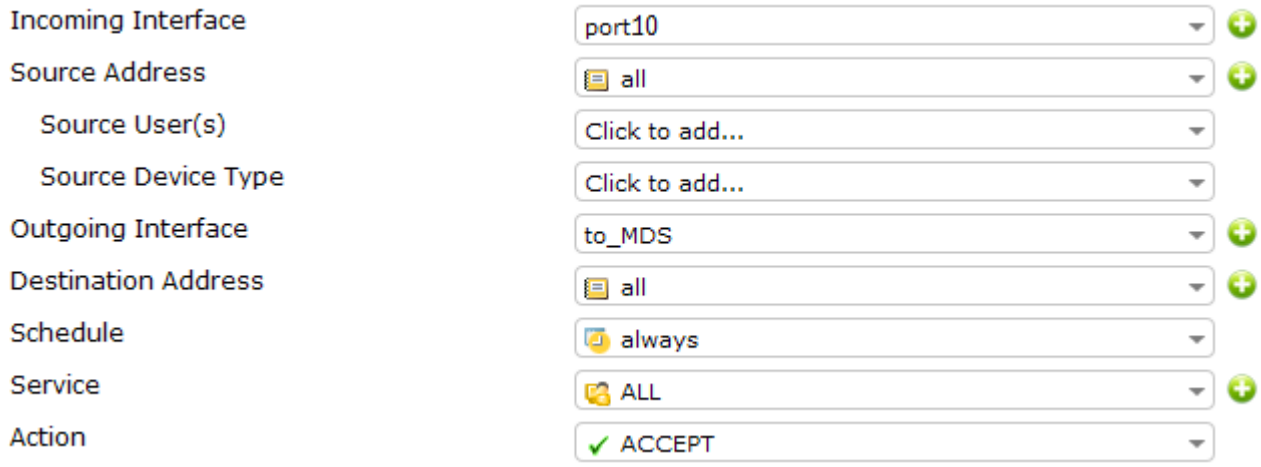


Two policies are required for each direction – Outbound and Inbound.

Outbound Policy (No NAT)



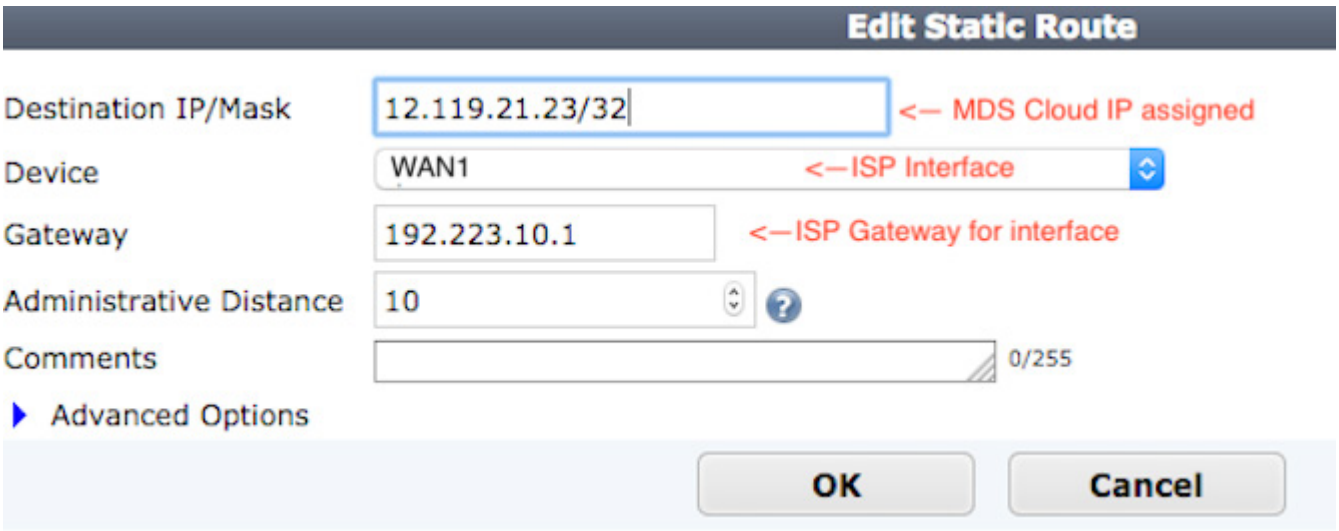
Inbound Policy (No NAT)



Create static route to the tunnel

Go to **Router > Static > Static Routes.** Click **Create New**

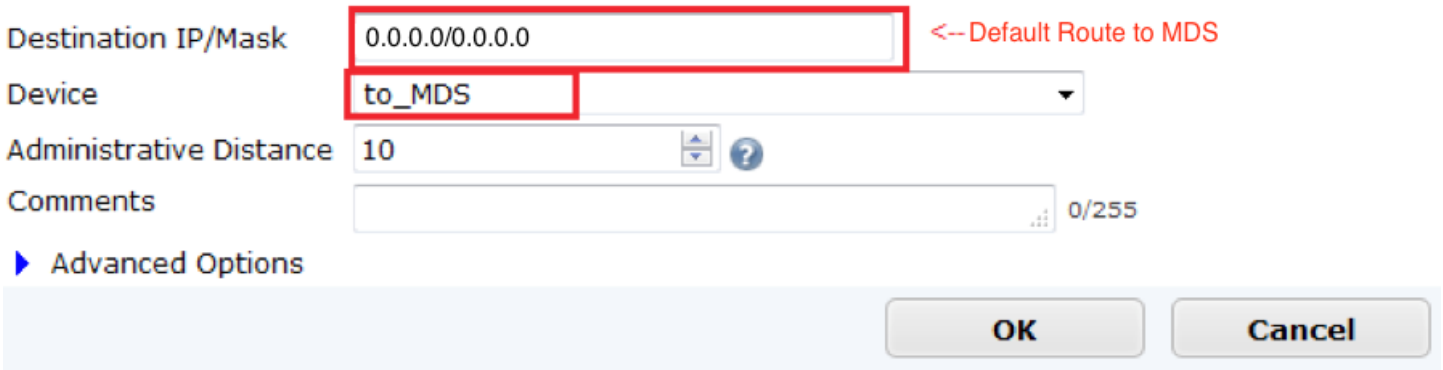
NOTE: Is is required to allow tunnel termination traffic to not be routed through internet.
NOTE: IF MANAGING REMOTELY we also recommend adding /32 for your public IP that your using to access this Fortigate using WAN interface and ISP assigned gateway same as below.



Create Default Route route to MDS via the tunnel

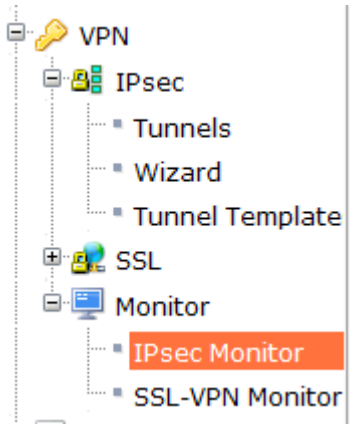
Go to **Router > Static > Static Routes.** Click **Create New**

NOTE: Make sure the administrative distance to MDS is lower than the WAN interface otherwise traffic will continue routing out WAN interface only and not tunnel



Bring the tunnel up:

Go to **VPN > Monitor > IPsec Monitor**

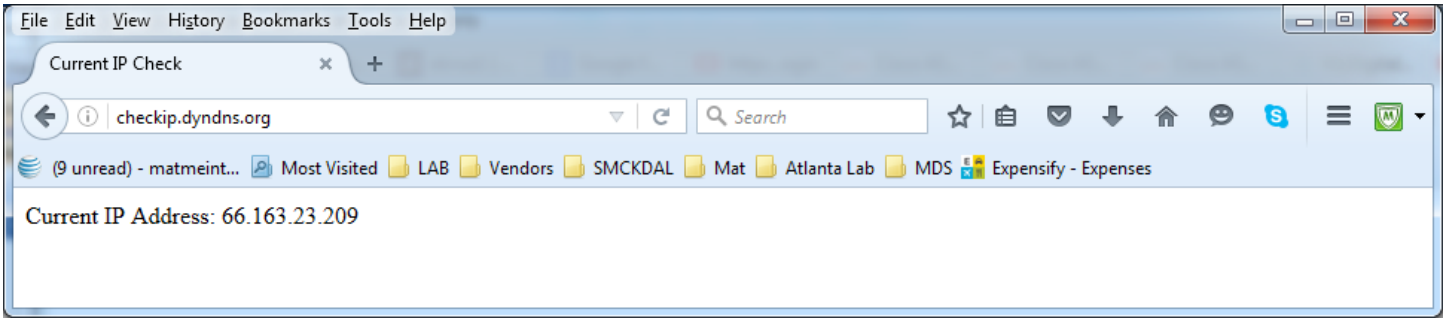


Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selectors
to_MDS	Custom - Static IP or Dynamic DNS	12.119.21.23		Down			to_MDS
meraki	Custom - Sta	73.72.183.23		Up	14.37 MB	177.25 MB	meraki
to_aisle8	Custom - Sta	1.2.3.4		Down			to_aisle8

Reset Statistics
Bring Up
Bring Down

VALIDATE TRAFFIC TO MDS

From a local computer that is connected in the local subnet, open up a 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