



Fortigate
MDS BYOG Integration Guide

CONTENTS

Introduction	3
Assumptions	3
What You Will Need	4
Activation Process	5
IPSEC Configuration	7
Create Firewall Policy	13
Validate Traffic to MDS	17
Validate MDS Web Block	18

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

Activate New vShield (3rd Party Device)

Choose Location:

Vancouver

Denver

Map Satellite

3rd Party Device Type:

Other IPSEC Tunnel

Cancel Activate

Setup Process from the Portal

Please reference the sample configuration from the MDS portal

Setup Wizard

PROFILE BUSINESS SYSTEMS NETWORKS

STEP 1 STEP 2

IPSEC SETTINGS

Cloud Public IP: 12.119.21.23


Static IP
73.45.157.101

DDNS

Remote LAN IP
192.168.1.1

Remote LAN Mask
255.255.255.0

IPSEC Secret Key
abc=123



SECURITY ON

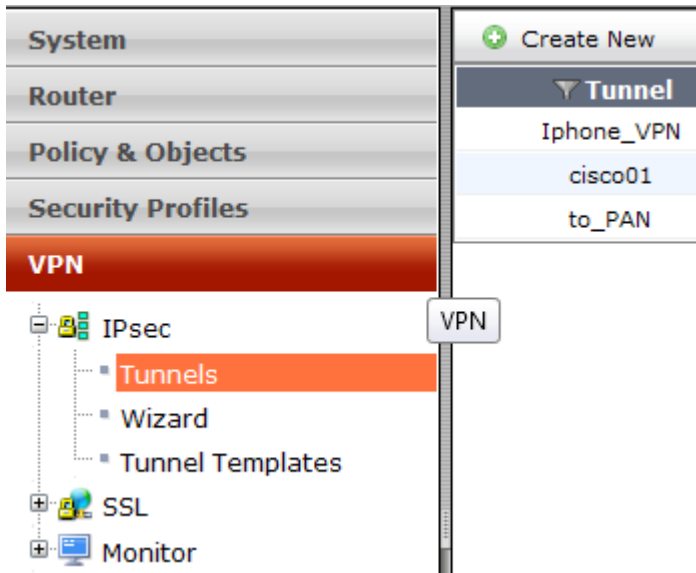
Firewall / NAT

Intrusion Prevention (IPS)

Anti-Virus

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**.

1 VPN Setup


Name


to_MDS


Template


 Dialup - FortiClient (Windows, Mac OS, Android)


 Site to Site - FortiGate

 Dialup - iOS (Native)

 Dialup - Android (Native L2TP/IPsec)

 Dialup - Cisco Firewall

 Site to Site - Cisco

 Custom VPN Tunnel (No Template)

< Back

Next >

Cancel

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.

Name

Comments

Network

IP Version IPv4 IPv6

Remote Gateway

IP Address

Interface

Mode Config

NAT Traversal

Keepalive Frequency

Dead Peer Detection

Authentication

Method

Pre-shared Key Show Key

Enter selections as shown below:

IKE

Version 1 2

Mode Aggressive Main (ID protection)

Phase 1 Proposal + Add

Encryption	AES128 ▼	Authentication	SHA256 ▼	Remove
Encryption	AES256 ▼	Authentication	SHA256 ▼	Remove
Encryption	3DES ▼	Authentication	SHA256 ▼	Remove
Encryption	AES128 ▼	Authentication	SHA1 ▼	Remove
Encryption	AES256 ▼	Authentication	SHA1 ▼	Remove
Encryption	3DES ▼	Authentication	SHA1 ▼	Remove

Diffie-Hellman Group 21 20 19 18 17 16
 15 14 5 2 1

Key Lifetime (seconds)

Local ID

XAUTH

Type

Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

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

New Phase 2 ✓ ✕

Name

Comments

Local Address

Remote Address

▼ Advanced...

Phase 2 Proposal + Add

Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="Remove"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="Remove"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="Remove"/>
Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="Remove"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="Remove"/>
Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="Remove"/>

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Set the Key Lifetime to 3600 seconds

▼ **Advanced...**

Phase 2 Proposal + Add

Encryption	AES128 ▼	Authentication	SHA1 ▼	Remove
Encryption	AES256 ▼	Authentication	SHA1 ▼	Remove
Encryption	3DES ▼	Authentication	SHA1 ▼	Remove
Encryption	AES128 ▼	Authentication	SHA256 ▼	Remove
Encryption	AES256 ▼	Authentication	SHA256 ▼	Remove
Encryption	3DES ▼	Authentication	SHA256 ▼	Remove

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Local Port All

Remote Port All

Protocol All

Autokey Keep Alive

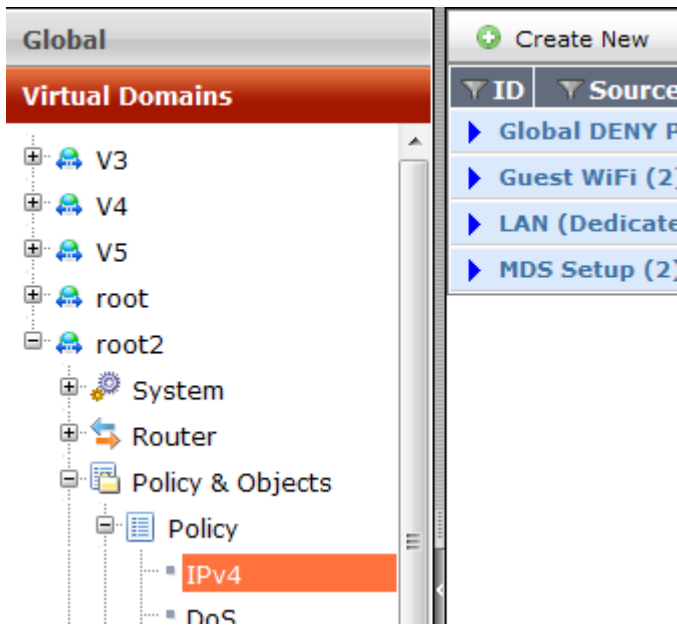
Auto-negotiate

Key Lifetime Seconds ▼

Seconds 3600

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)

Incoming Interface	to_MDS	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	port10	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Inbound Policy (No NAT)

Incoming Interface	port10	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	to_MDS	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Create static route to the tunnel

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

NOTE: It 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 you are using to access this Fortigate using WAN interface and ISP assigned gateway same as below.

Edit Static Route

Destination IP/Mask	<input type="text" value="12.119.21.23/32"/>	<-- MDS Cloud IP assigned
Device	<input type="text" value="WAN1"/>	<-- ISP Interface
Gateway	<input type="text" value="192.223.10.1"/>	<-- ISP Gateway for interface
Administrative Distance	<input type="text" value="10"/>	?
Comments	<input type="text"/>	0/255

▶ Advanced Options

Create Default Route route to MDS via the tunnel

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

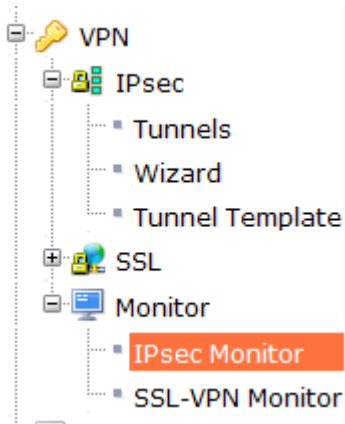
NOTE: Make sure the administrative distance to MDS is lower than the WAN interface otherwise traffic will continue routing out WAN interface only and not tunnel

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>	<-- Default Route to MDS
Device	<input type="text" value="to_MDS"/>	
Administrative Distance	<input type="text" value="10"/>	?
Comments	<input type="text"/>	0/255

▶ Advanced Options

Bring the tunnel up:

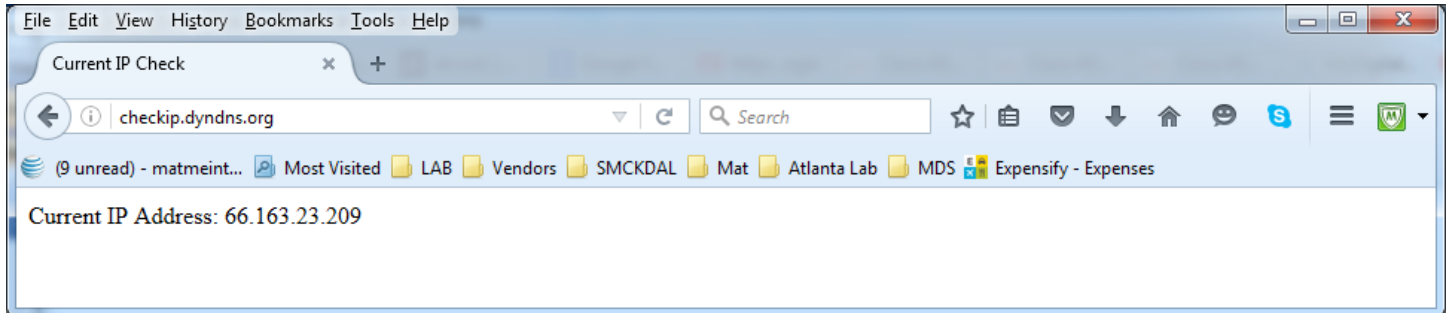
Go to VPN > Monitor > IPsec Monitor



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 - Static IP	73.72.183.23		Up	14.37 MB	177.25 MB	meraki
to_aisle8	Custom - Static IP	1.2.3.4		Down			to_aisle8

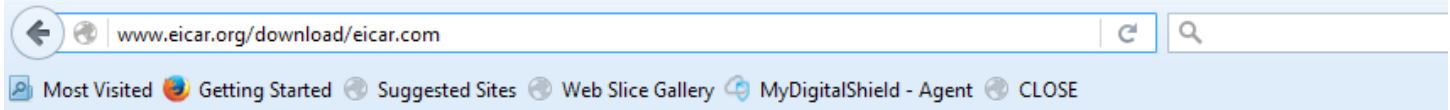
VALIDATE TRAFFIC TO MDS

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>



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**