

# Fortigate MyDigitalShield BYOG Integration Guide

## Introduction

Congratulations on your sale of MyDigitalShield using the BYOG option.

This guide is written specifically for the **Fortigate (FortiOS 5.4)** 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 5.4.1
- 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

3rd Party Device Type:

Other IPSEC Tunnel

Cancel Activate

Map Satellite

Vic

## 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

DDNS

Remote LAN IP

Remote LAN Mask

IPSEC Secret Key



#### SECURITY ON

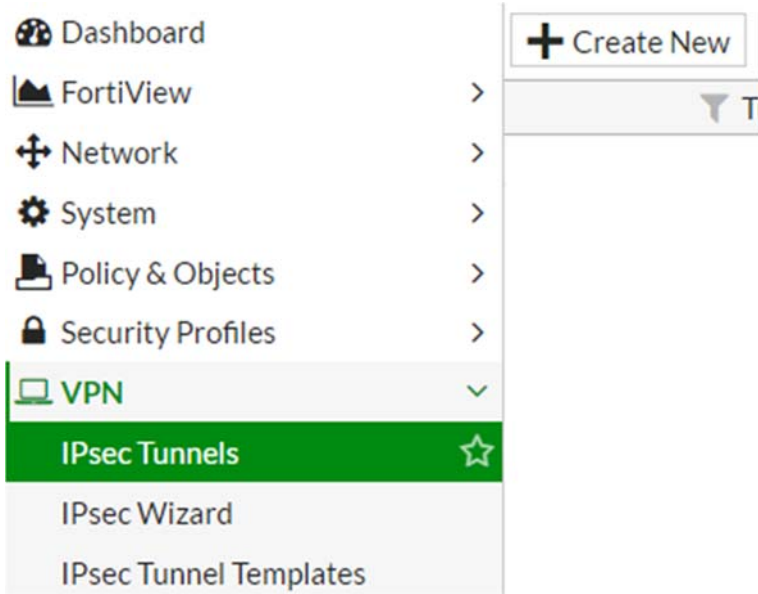
Firewall / NAT

Intrusion Prevention (IPS)

Anti-Virus

# IPSEC Configuration

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



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

### VPN Creation Wizard

**1 VPN Setup**

Name

Template Type

< 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 12.119.12.13. Select the interface where the ipsec tunnel will terminate. In this example, wan1 is being used. Set a secure Pre-Shared key which you entered in the portal.

### Edit VPN Tunnel

Name

Comments

#### Network

IP Version

Remote Gateway

IP Address

Interface

Mode Config

NAT Traversal

Keepalive Frequency

Dead Peer Detection

Set a secure Pre-Shared key which you entered in the portal.

**Authentication** ✓ ↺

Method

Pre-shared Key

**IKE**

Version

Mode

Enter selections as below:

**Phase 1 Proposal**  ✓ ↺

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

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

Key Lifetime (seconds)

Local ID

**XAUTH** ✓ ↺

Type

Enter a Phase name (example "to\_MDS"). Expand Advanced arrow. **Untick** "Enable Perfect Forward Security (PFS)." Set the Key Lifetime to **3600 seconds**

**Phase 2 Selectors**

Name	Local Address	Remote Address	
to_MDS	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	

**Edit Phase 2**

Name

Comments

Local Address Subnet

Remote Address Subnet

**Phase 2 Proposal**

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

Enable Replay Detection

Enable Perfect Forward Security (PFS)

Local Port All

Remote Port All

Protocol All

Auto-negotiate

Autokey Keep Alive

Key Lifetime

Seconds



## Create Firewall Policy







The screenshot shows the FortiGate configuration menu. The 'Policy & Objects' section is expanded, and 'IPv4 Policy' is selected. A sub-menu is visible, showing a '+ Create New' button and a table with a 'Seq.#' header and several policy entries: 'internal - to\_M', 'internal - wan', 'to\_MDS - inter', and 'Implicit (5 - 5)'.

Seq.#	
	+ internal - to_M
	+ internal - wan
	+ to_MDS - inter
	+ Implicit (5 - 5)

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

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







Outbound Policy (No NAT)

Name	outboundMDS
Incoming Interface	 internal ▼
Outgoing Interface	 to_MDS ▼
Source	 all ✕
Destination Address	 all ✕
Schedule	 always ▼
Service	 ALL ✕
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

NAT

Inbound Policy (No NAT)

Name	incomingMDS
Incoming Interface	 to_MDS ▼
Outgoing Interface	 internal ▼
Source	 all ✕
Destination Address	 all ✕
Schedule	 always ▼
Service	 ALL ✕
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

NAT

## Create static route to the tunnel

Go to Network > Routing > and click Create New under Static Routes.

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.

### New Static Route

Destination	<input type="text" value="12.119.21.23/32"/> <b>Subnet</b> <input type="text" value=""/> <b>Named Address</b> <input type="text" value=""/> <b>Internet Service</b>
	<small>&lt;-- MDS Cloud IP assigned</small>
Device	<input type="text" value="WAN (wan1)"/> <b>WAN (wan1)</b> <small>&lt;--ISP Interface</small>
Gateway	<input type="text" value="192.223.10.1"/> <small>&lt;-- ISP Gateway for interface</small>
Administrative Distance	<input type="text" value="10"/>
Comments	<input type="text" value=""/> <small>0/255</small>
Status	<input checked="" type="checkbox"/> <b>Enabled</b> <input type="checkbox"/> <b>Disabled</b>
<input type="checkbox"/> <b>Advanced Options</b>	
Priority	<input type="text" value="0"/>

## 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

### New Static Route

Destination Subnet Named Address Internet Service  
0.0.0.0/0

Device MDS

Administrative Distance ⓘ 10

Comments 0/255

Status Enabled Disabled

**Advanced Options**

Priority ⓘ 0

## Bring the tunnel up

## Go to Monitor > IPsec Monitor

The screenshot shows the FortiView IPsec Monitor interface. The left sidebar contains a navigation menu with 'Monitor' expanded and 'IPsec Monitor' selected. The main area displays a table of IPsec tunnels. The 'MDS' tunnel is highlighted in yellow and shows a status of 'Up'. A context menu is open over the 'MDS' row, showing options: 'Reset Statistics', 'Bring Up', and 'Bring Down'.

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selectors
MDS	Custom			Up	357.86 MB	77.52 MB	MDS