



**Sophos**  
**UTM MDS BYOG Integration Guide**

# CONTENTS

Introduction	3
Assumptions	3
What You Will Need	4
Configure the Gateway	6
Verification of IPSEC Tunnel	11
Validate traffic to MDS	11

# INTRODUCTION

Congratulations on your sale of MyDigitalShield using the BYOG option.

This guide is written specifically for the **Sophos UTM**. It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

## ASSUMPTIONS

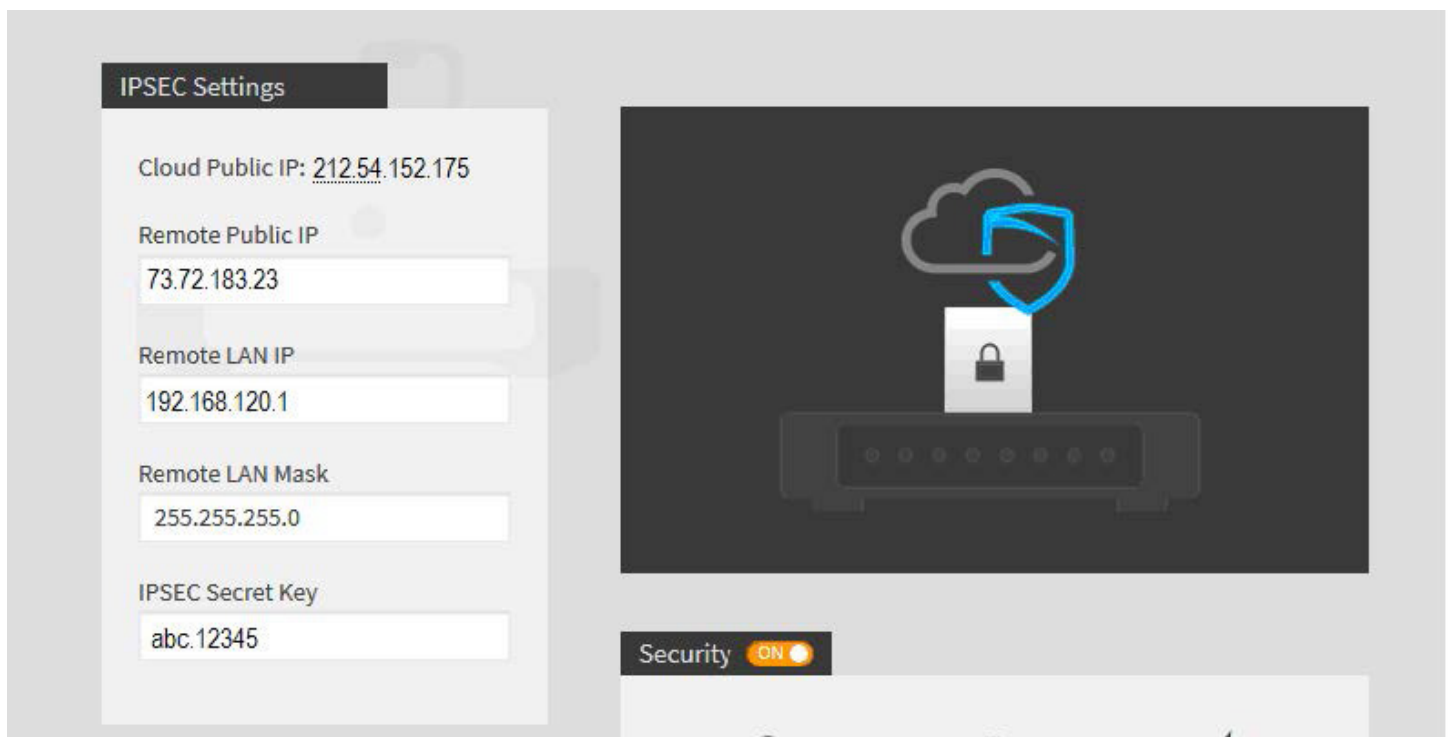
- This guide was developed to provide configuration information of the Sophos UTM gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Sophos UTM Version 9.400-9.
- This guide is NOT intended to be a full configuration guide for the Sophos gateway.
- It is assumed that an Internet port and LAN port are configured and operational.
- Responsibility of the management of the Sophos UTM 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:

- Local Public IP address/subnet.
- Local Public GW address (your customer's default gateway address).
- Local LAN Network/subnet.
- Cloud Public 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.



1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides. You can find this address following the instructions in the IPSEC Configuration section below.
2. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
3. **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 throughout this guide. To map IP addresses throughout this guide, values in the “Reference Sample” column are used.

<b>Network</b>	<b>IP</b>	<b>Reference Sample</b>
Local Public IP: (x.x.x.x/mask)		73.72.183.23/23
Local LAN Network (x.x.x.x/mask)		192.168.120.0/24
Cloud Public IP (x.x.x.x)		212.54.152.175

# CONFIGURE THE GATEWAY

In the left tabs on the main page expand **Site-to-Site VPN** and select **IPsec**. Select the **Policies** tab and click **New IPsec Policy**.

The screenshot shows the IPsec configuration interface. On the left is a navigation menu with categories like Dashboard, Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, and Site-to-site VPN. Under Site-to-site VPN, 'IPsec' is selected and highlighted with a red box. The main content area has a top navigation bar with tabs: Connections, Remote Gatew..., Policies (highlighted with a red box), Local RSA Key, Advanced, and Debug. Below this is a '+ New IPsec Policy...' button (also highlighted with a red box) and a search field with a 'Find' button. The main area displays a table of existing policies, sorted by Name asc. Each policy row includes an 'Action' column with checkboxes for Edit, Delete, and Clone, and a description of the policy settings.

Action	Sort by:	Name asc
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		<b>AES-256 PFS</b> Compression off, not using strict policy. IKE Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		<b>Microsoft Windows</b> Compression off, not using strict policy. IKE Settings: 3DES / SHA1 / Group 14: MODP 2048 Lifetime: 28800 seconds IPsec Settings: 3DES / MD5 / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		<b>Novell BorderManager</b> Compression off, using strict policy. IKE Settings: 3DES / SHA1 / Group 2: MODP 1024 Lifetime: 14400 seconds IPsec Settings: 3DES / MD5 / Group 2: MODP 1024 Lifetime: 3600 seconds
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		<b>TripleDES</b> Compression off, not using strict policy. IKE Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: 3DES / MD5 / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		<b>TripleDES PFS</b> Compression off, not using strict policy. IKE Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<input type="checkbox"/> Edit		<b>fgat</b>

Use the settings from the sample screenshot below:

### Add IPsec Policy ✕

---

Name:

---

IKE encryption algorithm:  ▼

IKE authentication algorithm:  ▼

IKE SA lifetime:

IKE DH group:  ▼

---

IPsec encryption algorithm:  ▼

IPsec authentication algorithm:  ▼

IPsec SA lifetime:

IPsec PFS group:  ▼

---

Strict policy:

Compression:

---

Comment:

---

Select the **Advanced** Tab. Enable **Dead Peer Detection** and **NAT Traversal**. Make sure to click **Apply** to save the configuration.

Connections Remote Gatew... Policies Local RSA Key **Advanced** Debug

Local X509 Certificate

Local X509 Cert  Please select the default local X509 certificate used for IPsec connections.

**Apply**

Preshared Key Settings

VPN ID type:  Specify the VPN ID that is used by PSK connections here. When the VPN ID is empty, the system will automatically use the interface IP address as the VPN ID.

VPN ID:

Enable probing of preshared keys Activate probing if you need to use different PSKs for your IPsec connections in respond-only mode.

**Apply**

Dead Peer Detection (DPD)

**Use Dead Peer Detection** When this option is activated, the system will try to detect dead (offline) remote systems.

**Apply**

NAT Traversal (NAT-T)

**Use NAT traversal** With NAT Traversal, IPsec traffic can pass upstream systems that use Network Address Translation (NAT).

NAT traversal keepalive:  seconds

**Apply**

Select the **Remote Gateway** tab and click **New Remote Gateway**.

Connections **Remote Gatew...** Policies Local RSA Key Advanced Debug

**+ New Remote Gateway...**  Find << >>

Display:  1-1 of 1

Action	Sort by: Name asc
<input type="checkbox"/> Edit	any-hack  dev-fgat
<input checked="" type="checkbox"/> Delete	VPN ID is IP Address, authenticated via Preshared key.
<input type="checkbox"/> Clone	



Fill in the IPV4 field with the **Cloud Public IP** address.

The screenshot shows the Mikrotik WinBox interface. At the top, there are tabs for 'Connections', 'Remote Gatew...', 'Policies', and 'Local RSA Key'. Below the tabs is a '+ New Remote Gateway...' button. The main area is divided into two windows:

- Edit Remote Gateway:** This window is for editing a gateway named 'MDS-Node'. It has fields for 'Name', 'Gateway type' (set to 'Initiate connection'), 'Gateway' (set to 'GW1'), 'Authentication type' (set to 'Preshared key'), 'Key', 'Repeat', 'VPN ID type' (set to 'IP address'), 'VPN ID (optional)', 'Remote networks' (with a list containing 'Any'), and 'Comment'. There are 'Save' and 'Cancel' buttons at the bottom.
- Add Network Definition:** This window is for adding a new network definition. It has fields for 'Name' (set to 'GW1'), 'Type' (set to 'Host'), and 'IPv4 address' (set to '212.54.152.175'). It also has expandable sections for 'DHCP Settings', 'DNS Settings', and 'Advanced', and a 'Comment' field. There are 'Save' and 'Cancel' buttons at the bottom.

Red boxes highlight the '+' icon in the 'Gateway' field of the 'Edit Remote Gateway' window and the '+' icon in the 'Remote networks' list. Another red box highlights the 'Any' network in the 'Networks (CTRL+Z)' dropdown menu.

Select the **Connections** tab then click **New IPsec Connection**.

The screenshot shows the Mikrotik WinBox interface with the 'Connections' tab selected. At the top, there are tabs for 'Connections', 'Remote Gatew...', 'Policies', 'Local RSA Key', 'Advanced', and 'Debug'. Below the tabs is a '+ New IPsec Connection...' button, which is highlighted with a red box. There is also a search bar with a 'Find' button and navigation arrows. Below the search bar is an 'Open Live Log' button. At the bottom, there is a table of connections with columns for 'Action', 'Name', and 'Status'. The table shows one connection named 'fgat' with status 'WAN' and 'any-hack'. There are 'Edit', 'Delete', and 'Clone' buttons for each connection.

Fill in the appropriate field then click **Save**.

**Connections** Remote Gatew... Policies

**+ New IPsec Connection...**

**Open Live Log**

**Edit IPsec Connection** ✕

Name:

Remote gateway:  ▼

Local interface:  ▼

Policy:  ▼

**Local Networks** 📁 +

Local Network			
DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND

Automatic firewall rules

Strict routing

Bind tunnel to local interface

Comment:

**✓ Save**

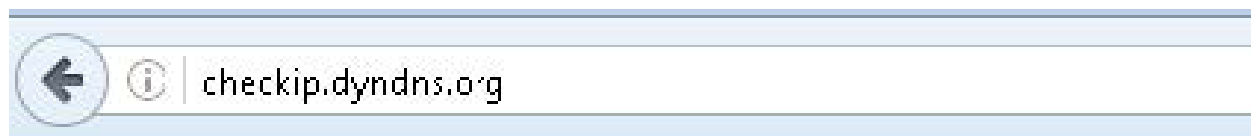
**✕ Cancel**

# VERIFICATION OF IPSEC TUNNEL

The screenshot shows a network management dashboard with a search bar at the top left. The main navigation menu on the left includes: Dashboard, Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, and Site-to-site VPN. Under Site-to-site VPN, there are sub-items: Amazon VPC, IPsec, and SSL. The main content area is titled "Site-to-site VPN Tunnel Status" and displays a green checkmark icon next to "MDS-IPsec" with the text "[1 of 1 IPsec SAs established]".

## VALIDATE TRAFFIC TO MDS

From a local computer that is connected to the local subnet, open up the browser and go to [checkip.dyndns.org](http://checkip.dyndns.org). The Public IP should reflect the MDS node.



Current IP Address: 212.54.152.175

Access a gambling site. For example, try [gamblingsites.org](http://gamblingsites.org).



## Web Page Blocked!

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

URL: [www.gamblingsites.org/](http://www.gamblingsites.org/)

Category: Gambling

✖

Proceed

Go Back