

**SOPHOS**

Security made simple.



# Pocket Guide

Establish IPsec VPN Connection  
Between Sophos XG Firewall and  
Fortigate with IKEv2

Product: Sophos XG Firewall

## Contents

<b>Overview</b> .....	<b>3</b>
<b>Prerequisite</b> .....	<b>3</b>
<b>Network Diagram</b> .....	<b>3</b>
<b>Configuration</b> .....	<b>4</b>
Fortigate.....	4
Create IPsec Phases and Tunnels.....	4
Configure Phase 1 Parameters .....	5
Configure Phase 2 Parameters .....	6
Create Static Route for VPN Tunnel.....	7
Create Firewall Policies.....	8
Sophos XG Firewall.....	10
Create IPsec Connection.....	10
Create Firewall Rule.....	11
Enable IPsec Connection.....	13
Verify VPN Tunnel Status on Fortigate Appliance .....	14
<b>Result</b> .....	<b>15</b>
<b>Copyright Notice</b> .....	<b>16</b>

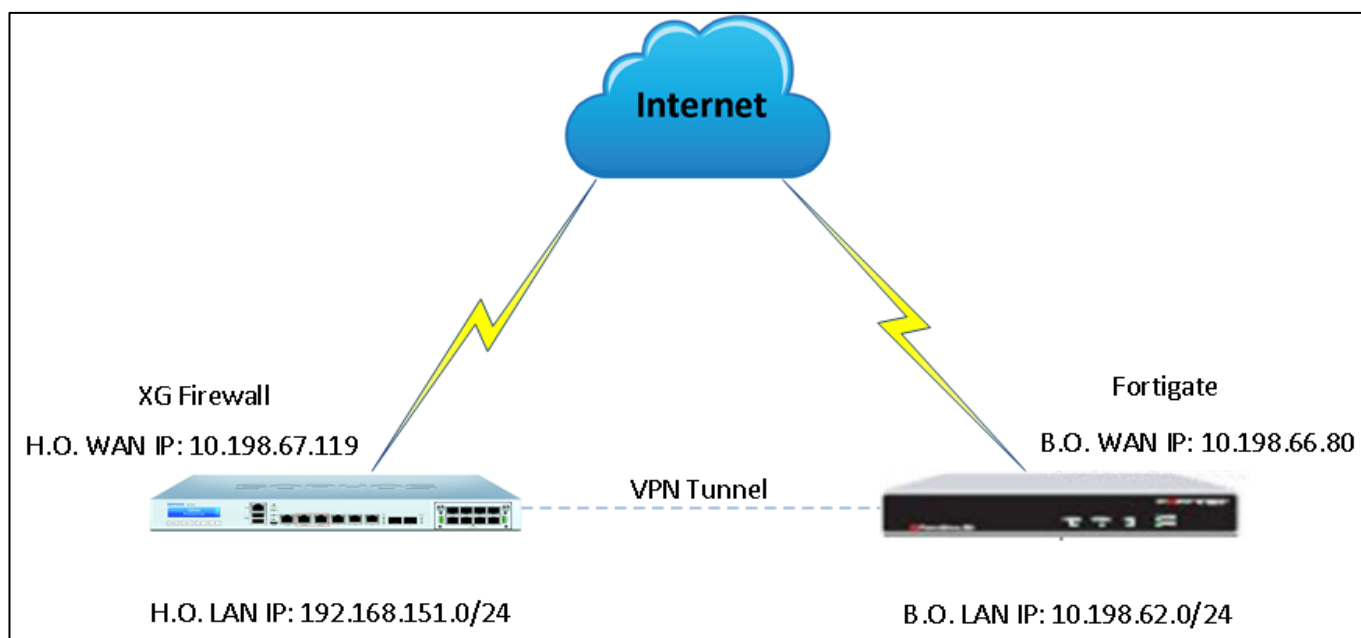
## Overview

This guide describes how to set up a site-to-site IPsec VPN connection between Sophos XG Firewall and Fortigate appliance using preshared key to authenticate VPN peers.

## Prerequisite

You must have read-write permissions on the SFOS Admin Console and the Fortigate Web Admin Console for the relevant features.

## Network Diagram



## Configuration

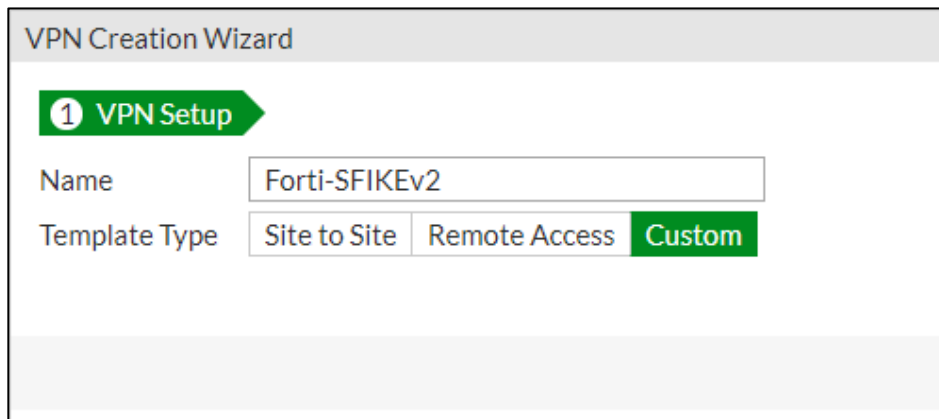
### Fortigate

#### Create IPsec Phases and Tunnels

- Go to **VPN > IPsec Tunnels** and click **Create New**.



- Under **VPN Setup**, enter a **Name**.
- Set **Template Type** to **Custom**.

A screenshot of the 'VPN Creation Wizard' interface. The title is 'VPN Creation Wizard'. Below the title is a progress indicator '1 VPN Setup' with a green arrow. There are two input fields: 'Name' with the value 'Forti-SFIKEv2' and 'Template Type' with three radio buttons: 'Site to Site', 'Remote Access', and 'Custom'. The 'Custom' radio button is selected and highlighted in green.

Click **Next**.

- Under **Network**, set **IP Version** to **IPv4**.
- Set **Remote Gateway** to **Static IP Address**.
- For **IP Address**, enter the WAN IP address of XG Firewall. [example: 10.198.67.119]
- Set **Interface** to the WAN interface. [example: CE vlan (wan2)]
- Set **NAT Traversal** to **Disable** and **Dead Peer Detection** to **On Demand**.
- Under **Authentication**, set **Method** to **Pre-shared Key**.
- Enter **Pre-shared Key**.
- In **IKE**, set **Version** to **2**.

- Under Peer Options, set Accept Types to Any peer ID.

The screenshot shows the configuration page for a peer. It is divided into two main sections: Network and Authentication. In the Network section, IP Version is set to IPv4, Remote Gateway is Static IP Address, IP Address is 10.198.67.119, Interface is CE vlan (wan2), Mode Config is disabled, NAT Traversal is Disabled, and Dead Peer Detection is On Demand. In the Authentication section, Method is Pre-shared Key, and the key is masked with dots. Under the IKE section, Version is set to 2. Under the Peer Options section, Accept Types is set to Any peer ID.

### Configure Phase 1 Parameters

- Set Encryption to AES256 and Authentication to SHA512.
- Click Add and set Encryption to AES256 and Authentication to SHA384.
- For Diffie-Hellman Groups, select 16, 19 and 21.
- For Key Lifetime (seconds), enter 5400.

The screenshot shows the configuration for Phase 1 Proposals. There is an 'Add' button. Two proposals are listed: the first has Encryption AES256 and Authentication SHA512; the second has Encryption AES256 and Authentication SHA384. Under Diffie-Hellman Groups, checkboxes for 21, 19, and 16 are checked. Key Lifetime (seconds) is set to 5400. Local ID is empty.

### Configure Phase 2 Parameters

- Under **Phase 2 Selectors**, enter a **Name**.
- Set **Local Address** to **Subnet** and enter the LAN IP address of Fortigate appliance. (example: 10.198.62.0/24).
- Set **Remote Address** to **Subnet** and enter the LAN IP address of XG Firewall. (example: 192.168.151.0/24).
- Click to expand the **Advanced** section.
- Under **Phase 2 Proposal**, set **Encryption** to **AES256** and **Authentication** to **SHA512**.
- Click **Add** and set **Encryption** to **AES256** and **Authentication** to **SHA384**.
- Select **Enable Replay Detection** and **Enable Perfect Forward Secrecy (PFS)**.
- For **Diffie-Hellman Group**, select **16, 19** and **21**.
- For **Local Port**, **Remote Port** and **Protocol**, select **All**.
- Select **Auto-negotiate**.
- Set **Key Lifetime** to **Seconds** and enter **3600** in **Seconds**.

**Phase 2 Selectors**

Name	Local Address	Remote Address
Forti-SFIKEv2	10.198.62.0/24	192.168.151.0/24

**New Phase 2**

Name: Forti-SFIKEv2

Comments: Comments

Local Address: Subnet 10.198.62.0/24

Remote Address: Subnet 192.168.151.0/24

**Advanced...**

**Phase 2 Proposal** + Add

Encryption: AES256 Authentication: SHA512 ✕

Encryption: AES256 Authentication: SHA384 ✕

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

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

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

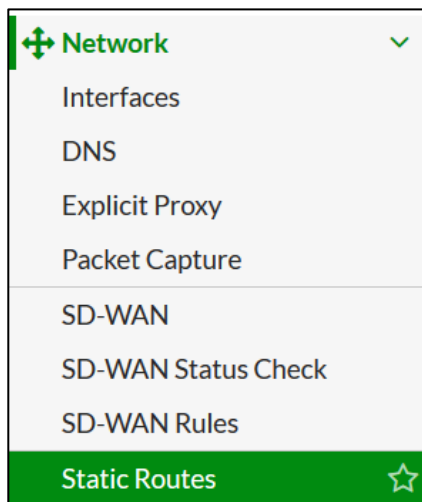
Key Lifetime: Seconds

Seconds: 3600


Click **OK**.

### Create Static Route for VPN Tunnel

- Go to **Network > Static Routes** and click **Create New**.



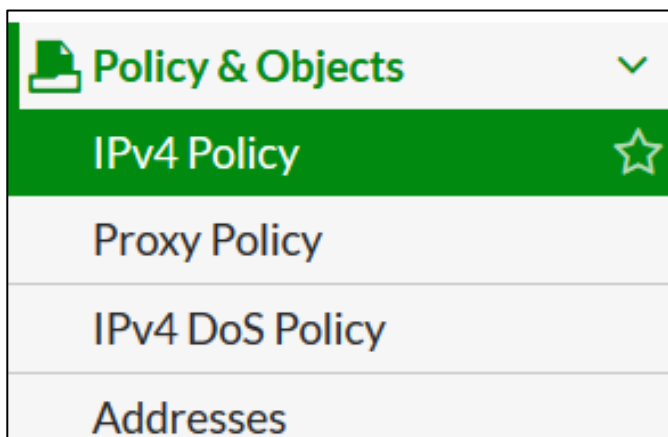
- For **Destination**, select **Subnet** and enter the LAN IP address of XG Firewall. (example: 192.168.151.0/24).
- Set **Device** to the IPsec tunnel you have created. (example: Forti-SFIKEv2)
- For **Administrative Distance**, enter **10**.
- Set **Status** to **Enabled**.

Destination	<b>Subnet</b>   Named Address   Internet Service
	192.168.151.0/24
Device	Forti-SFIKEv2
Administrative Distance 	10
Comments	<input type="text"/> 0/255
Status	<b>Enabled</b>   Disabled

Click **OK**.

### Create Firewall Policies

- Go to **Policy & Objects > IPv4 Policy** and click **Create New**.













- Enter a **Name**.
- Set **Incoming Interface** to the LAN interface of Fortigate appliance. (example: Forti-SFIKEv2)
- Set **Outgoing Interface** to the IPsec tunnel you have created. (example: vlan680 (port1))
- For **Source**, **Destination** and **Service**, select **all**.
- Set **Schedule** to **always**.

Name ⓘ	Sophos to Fortinet
Incoming Interface	Forti-SFIKEv2
Outgoing Interface	vlan680 (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Similarly, create another firewall policy for traffic from XG Firewall to Fortigate appliance.



Name 	Sophos to Fortinet
Incoming Interface	 Forti_To_Sophos ▼
Outgoing Interface	 vlan680 (port1) ▼
Source	 all  +
Destination	 all  +
Schedule	 always ▼
Service	 ALL  +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Note: Turn off **NAT** if you do not wish to use NAT-T in VPN Profile.

Click **OK**.

Firewall / Network Options	
NAT	<input type="checkbox"/>

## Sophos XG Firewall

### Create IPsec Connection

- Go to **Configure > VPN > IPsec Connections** and click **Add**.
- Under **General Settings**, enter a **Name**.
- Set **IP Version** to **IPv4**, **Connection Type** to **Site-to-Site** and **Gateway Type** to **Respond Only**.
- Select **Activate on Save**.

The screenshot shows the 'General Settings' configuration page for an IPsec connection. The 'Name' field contains 'Sophos\_To\_Fortinet'. The 'IP Version' is set to 'IPv4' with radio buttons. The 'Connection Type' is set to 'Site-to-Site'. The 'Gateway Type' is set to 'Respond Only'. The 'Activate on Save' checkbox is checked. There is also a 'Description' text area.

- Under **Encryption**, set **Policy** to **IKEv2**.
- Set **Authentication Type** to **Preshared Key**, enter **Preshared Key** and **Repeat Preshared Key**.

The screenshot shows the 'Encryption' configuration page. The 'Policy' is set to 'IKEv2'. The 'Authentication Type' is set to 'Preshared Key'. Below this, there are two text input fields for 'Preshared Key' and 'Repeat Preshared Key', both containing masked characters (dots). A 'Cancel' button is visible at the bottom.

- Under **Gateway Settings – Local Gateway**, set **Listening Interface** to the WAN IP address of XG Firewall (example: PortE1.690 – 10.198.67.119) and set **Local Subnet** to **LAN**.

- Under **Gateway Settings – Remote Gateway**, set **Gateway Address** to the WAN IP address of Fortigate appliance (example: 10.198.66.80) and set **Remote Subnet** to **Forti\_LAN**.

- Under **Advanced**, set **User Authentication Mode** to **None**.

### Create Firewall Rule

- Go to **Protect > Firewall** and click **Add Firewall Rule**.

- Enter a **Rule Name**.
- For **Source Zones**, select **LAN** and for **Destination Zones**, select **VPN**.
- Under **Identity**, clear the **Match known users** check box.

The screenshot shows the configuration for a firewall rule named "LAN-VPN". The rule position is set to "Bottom". The action is set to "Accept". The source zone is "LAN", source networks and devices are "Any", and it is active "All the Time". The destination zone is "VPN", destination networks are "Any", and services are "Any". The "Match known users" checkbox is checked.

- Similarly, create a firewall rule for VPN to LAN traffic.

The screenshot shows the configuration for a firewall rule named "VPN-LAN". The rule position is set to "Bottom". The action is set to "Accept". The source zone is "VPN", source networks and devices are "Any", and it is active "All the Time". The destination zone is "LAN", destination networks are "Any", and services are "Any". The "Match known users" checkbox is checked.

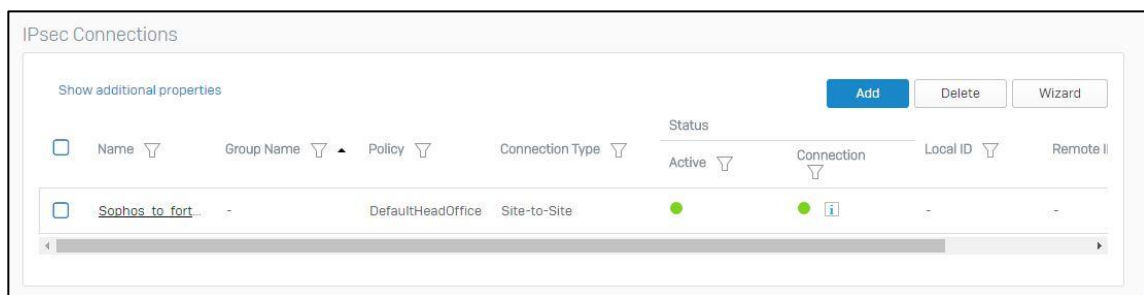
- Select **Log Firewall Traffic**.



Click **Save**.

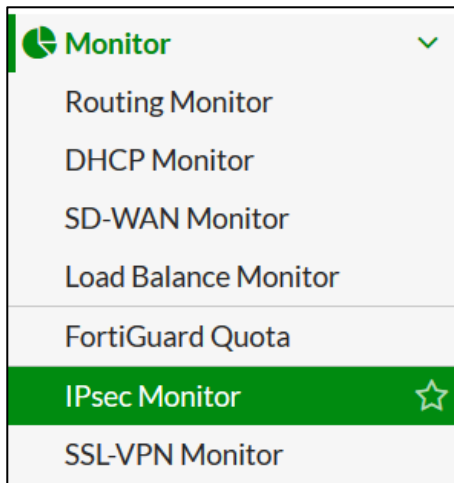
## Enable IPsec Connection

- Go to **Configure > VPN > IPsec Connections**.
- Under **Status**, click **Active** and **Connection** to activate the connection.



## Verify VPN Tunnel Status on Fortigate Appliance

Go to Monitor > IPsec Monitor



Tunnel details are displayed. If Status is **Down**, select the tunnel and click **Bring Up** to initiate tunnel.

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 1
Forti-SFIKEv2	Custom	10.198.67.119		Up	1.10 MB	11.04 MB	Forti-SFIKEv2

## **Result**

You have established an IPsec VPN connection between XG Firewall and Fortigate appliance.

## **Copyright Notice**

Copyright 2016-2017 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.