

**SOPHOS**

Security made simple.



# Pocket Guide

Establish IPsec VPN Connection  
Between Sophos XG Firewall and  
Fortigate with IKEv1

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>

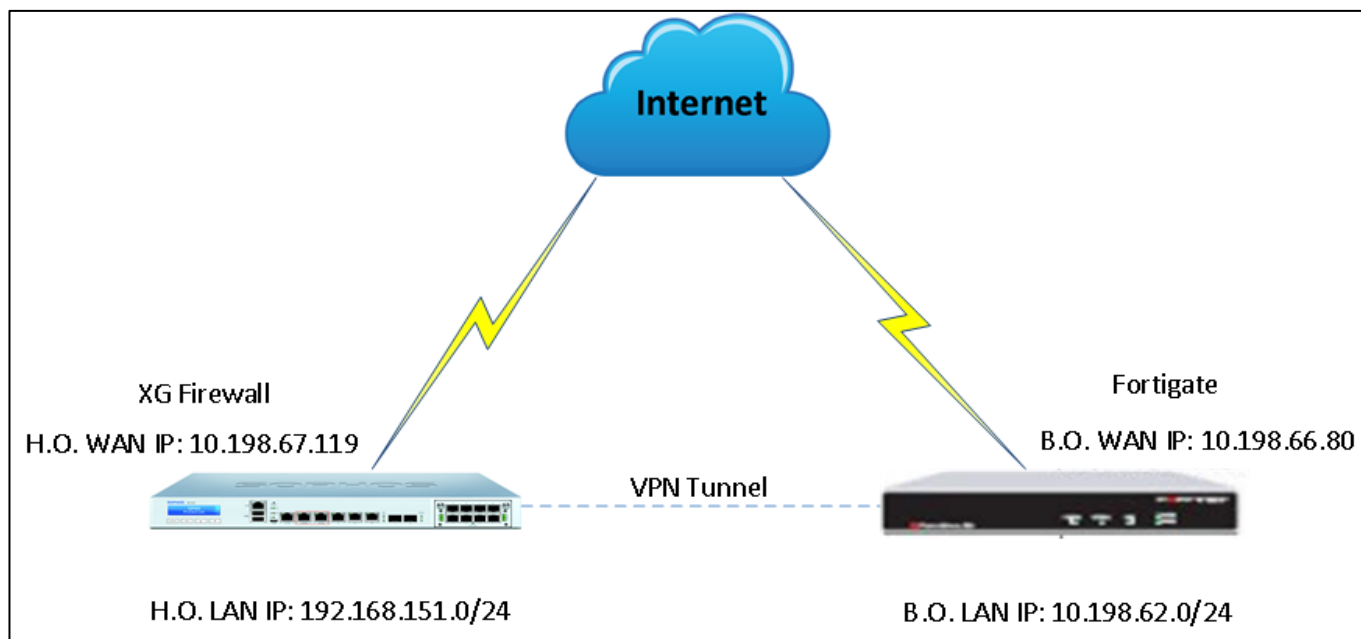
## Overview

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

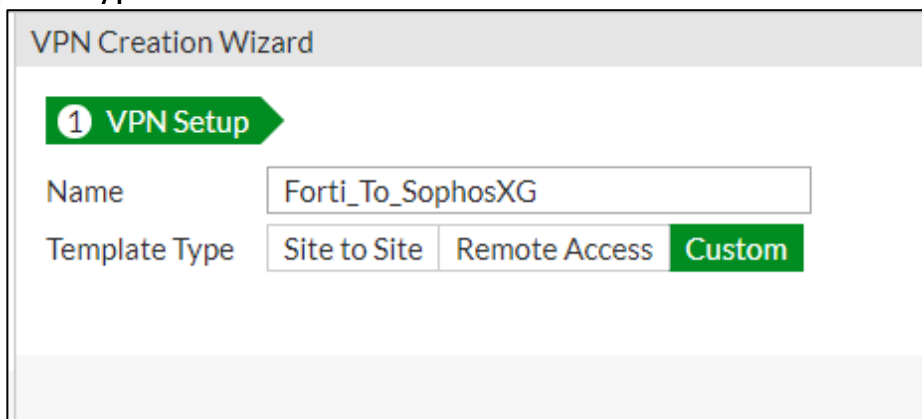
### Fortigate

#### Create IPsec Phases and Tunnels

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



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

A screenshot of the 'VPN Creation Wizard' in Fortigate. The first step, 'VPN Setup', is highlighted with a green arrow and the number 1. Below the step indicator, there is a text input field for 'Name' containing 'Forti\_To\_SophosXG'. Underneath, there are three radio button options for 'Template Type': 'Site to Site', 'Remote Access', and 'Custom'. The 'Custom' option 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**.
- Set **Version** to **1**, and **Mode** to **Main (ID protection)**.

Network	
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Remote Gateway	Static IP Address
IP Address	10.198.67.119
Interface	CE vlan (wan2)
Mode Config	<input type="checkbox"/>
NAT Traversal	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="radio"/> Forced
Dead Peer Detection	<input type="radio"/> Disable <input type="radio"/> On Idle <input checked="" type="radio"/> On Demand
Authentication	
Method	Pre-shared Key
Pre-shared Key	.....
IKE	
Version	<input checked="" type="radio"/> 1 <input type="radio"/> 2
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)

### Configure Phase 1 Parameters

- Set Encryption to AES256, and Authentication to SHA256.
- Click Add and set Encryption to AES256 and Authentication to SHA1.
- Enable 14, 15 and 16 in Diffie-Hellman Groups.
- Enter 12600 in Key Lifetime (seconds).
- Under XAUTH, set Type to Disabled.

Phase 1 Proposal	<input type="button" value="+ Add"/>		
Encryption	AES256	Authentication	SHA256 <input type="button" value="X"/>
Encryption	AES256	Authentication	SHA1 <input type="button" value="X"/>
Diffie-Hellman Groups	<input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1		
Key Lifetime (seconds)	12600		
Local ID			
XAUTH <input type="button" value="Edit"/>			
Type : Disabled			

### Configure Phase 2 Parameters

- Under **Phase 2 Selectors**, enter a **Name**.
- Set **Local Address** to **Subnet** and enter the LAN IP address of the Fortigate appliance. (example: 10.198.62.0/255.255.255.0)
- Set **Remote Address** to **Subnet** and enter the LAN IP address of XG Firewall. (example: 192.168.151.0/255.255.255.0)
- 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 **SHA256**.
- Select **Enable Replay Detection** and **Enable Perfect Forward Secrecy (PFS)**.
- Enable **14, 15** and **16** in **Diffie-Hellman Group**.
- For **Local Port**, **Remote Port** and **Protocol**, select **All**.
- Select **Auto-negotiate**.
- Set **Key Lifetime** to **Seconds** and enter **5400** in **Seconds**.

The screenshot shows the configuration interface for Phase 2 Selectors and Phase 2 Proposal. The Phase 2 Selectors section includes a table with columns for Name, Local Address, and Remote Address. The Phase 2 Proposal section includes fields for Name, Comments, Local Address, Remote Address, Encryption, Authentication, Enable Replay Detection, Enable Perfect Forward Secrecy (PFS), Diffie-Hellman Group, Local Port, Remote Port, Protocol, Auto-negotiate, Autokey Keep Alive, Key Lifetime, and Seconds.

Phase 2 Selectors		
Name	Local Address	Remote Address
Forti_To_SophosXG_Phase2	10.198.62.0/255.255.255.0	192.168.151.0/255.255.255.0

**Edit Phase 2**

Name: Forti\_To\_SophosXG\_Phase2

Comments: Comments

Local Address: Subnet, 10.198.62.0/255.255.255.0

Remote Address: Subnet, 192.168.151.0/255.255.255.0

**Advanced...**

**Phase 2 Proposal** Add

Encryption: AES256, Authentication: SHA512

Encryption: AES256, Authentication: SHA256

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:

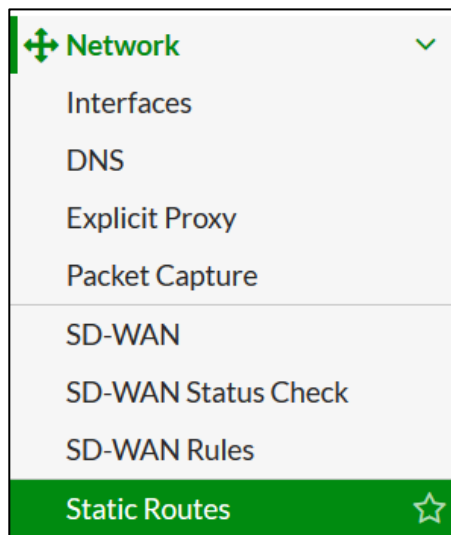
Key Lifetime: Seconds

Seconds: 5400


Click **OK**.

### Create Static Route for VPN Tunnel

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



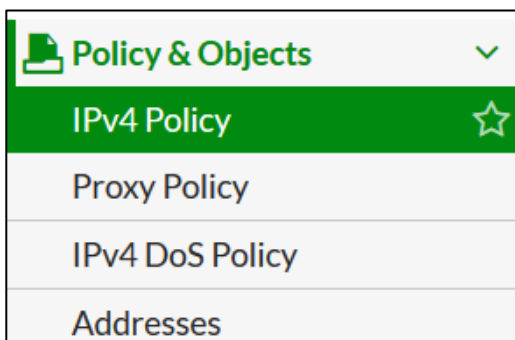
- For **Destination**, select **Subnet** and enter the LAN IP address of XG Firewall. (example: 192.168.151.0/24)
- Set **Device** to the IPsec tunnel you have created. (example: Forti\_To\_Sophos)
- For **Administrative Distance**, enter **10**.
- Set **Status** to **Enabled**.

Destination	<b>Subnet</b>   Named Address   Internet Service
	192.168.151.0/24
Device	Forti_To_Sophos
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 the Fortigate appliance. (example: vlan680 (port1))
- Set **Outgoing Interface** to the IPsec tunnel you have created. (example: Forti\_To\_Sophos)
- For **Source**, **Destination** and **Service**, select **all**.
- Set **Schedule** to **always**.

Name ⓘ	Forti to Sophos
Incoming Interface	vlan680 (port1) ▼
Outgoing Interface	Forti_To_Sophos ▼
Source	all [X] +
Destination	all [X] +
Schedule	always ▼
Service	ALL [X] +
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 	<input type="text" value="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**.
- In **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. The 'Name' field contains 'Sophos\_To\_Fortinet'. The 'IP Version' section has 'IPv4' selected with a radio button. The 'Connection Type' dropdown is set to 'Site-to-Site'. The 'Gateway Type' dropdown is set to 'Respond Only'. There is a checked checkbox for 'Activate on Save'.

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

The screenshot shows the 'Encryption' configuration page. The 'Policy' dropdown is set to 'DefaultHeadOffice'. The 'Authentication Type' dropdown is set to 'Preshared Key'. Below it, there are two text input fields: 'Preshared Key' and 'Repeat Preshared Key', both containing a series of dots to represent masked text.

- 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**.
- In **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**.

The screenshot shows the 'Gateway Settings' configuration page. It is divided into two columns: 'Local Gateway' and 'Remote Gateway'.  
Local Gateway settings include:  
- Listening Interface: PortE1.690 - 10.198.67.119  
- Local ID: Select Local ID  
- Local ID: (empty field)  
- Local Subnet: LAN  
- Add New Item button  
Remote Gateway settings include:  
- Gateway Address: 10.198.66.80  
- Remote ID: Select Remote ID  
- Remote ID: (empty field)  
- Remote Subnet: Forti\_LAN  
- Add New Item button  
At the bottom, there is a checkbox for 'Network Address Translation (NAT)' which is unchecked. Below it is a note: 'Subnets which can be selected here, must be first created under "Hosts and Services".'

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

The screenshot shows the 'Advanced' settings section. The 'User Authentication Mode' is set to 'None' (selected with a radio button). Other options are 'As Client' and 'As Server'. There is an unchecked checkbox for 'Disconnect when idle'. Below that, the 'Idle session time interval' is set to '120' seconds.

#### 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.

# Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv1

The screenshot shows the configuration for a firewall rule named "LAN-VPN". The rule is positioned at the bottom. The action is set to "Accept". The source is configured with "Source Zones" set to "LAN", "Source Networks and Devices" set to "Any", and "During Scheduled Time" set to "All the Time". The destination is configured with "Destination Zones" set to "VPN", "Destination Networks" set to "Any", and "Services" set to "Any". The identity is set to "Match known users".

- Similarly. Create a firewall rule for traffic from VPN to LAN.

The screenshot shows the configuration for a firewall rule named "VPN-LAN". The rule is positioned at the bottom. The action is set to "Accept". The source is configured with "Source Zones" set to "VPN", "Source Networks and Devices" set to "Any", and "During Scheduled Time" set to "All the Time". The destination is configured with "Destination Zones" set to "LAN", "Destination Networks" set to "Any", and "Services" set to "Any". The identity is set to "Match known users".

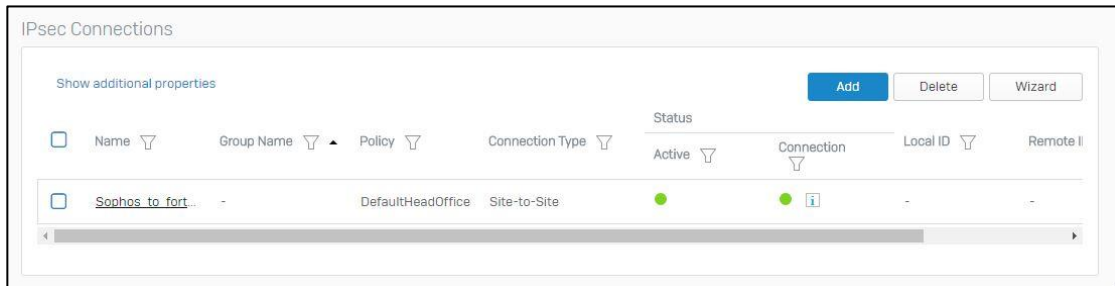
- Select Log Firewall Traffic.

The screenshot shows the "Log Traffic" configuration panel. The checkbox for "Log Firewall Traffic" is checked.

Click **Save**.

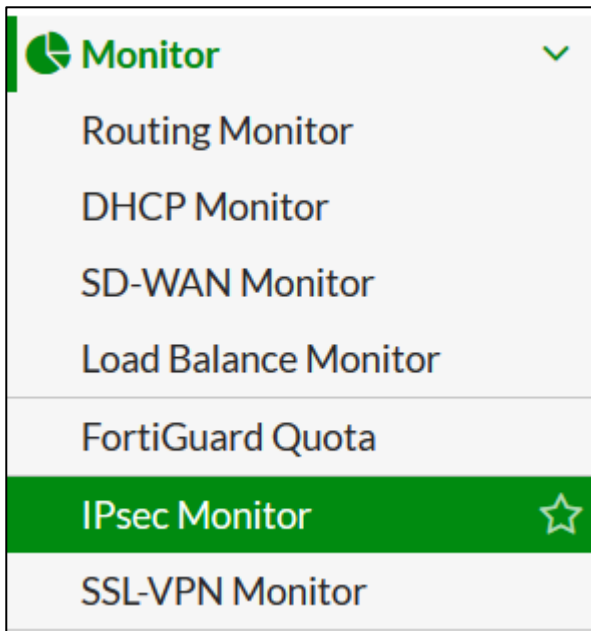
## Enable IPsec Connection

- 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 the 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_To-Sophos	Custom	10.198.67.119		Up	26.34 kB	319.11 kB	Forti_To-Sophos

## **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.