Pocket Guide

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

Product: Sophos XG Firewall
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv2

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.

Click Next.

- 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.
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv2

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

![Network Configuration](image)

**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.
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.
Click OK.

**Create Static Route for VPN Tunnel**

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

  ![Static Routes](image)

- 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.

  ![Static Route Configuration](image)

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.

Similarly, create another firewall policy for traffic from XG Firewall to Fortigate appliance.
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv2

<table>
<thead>
<tr>
<th>Name</th>
<th>Sophos to Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Interface</td>
<td>Forti_To_Sophos</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>vlan680 (port1)</td>
</tr>
<tr>
<td>Source</td>
<td>all</td>
</tr>
<tr>
<td>Destination</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ALL</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

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

Click OK.
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv2

**Sophos XG Firewall**

**Create IPsecConnection**

- 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.

![General Settings](image)

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

![Encryption](image)

- 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.

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

• Select Log Firewall Traffic.
Log Traffic

- 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.
**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.