Pocket Guide

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

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

Contents

Overview........................................................................................................................................3
Prerequisite...................................................................................................................................3
Network Diagram.........................................................................................................................3
Configuration...............................................................................................................................4
  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
Result..........................................................................................................................................15
Copyright Notice.......................................................................................................................16
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv1

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

![Network Diagram]

- **Internet**
- **XG Firewall**
  - H.O. WAN IP: 10.198.67.119
  - H.O. LAN IP: 192.168.151.0/24
- **Fortigate**
  - B.O. WAN IP: 10.198.66.80
  - B.O. LAN IP: 10.198.62.0/24
- **VPN Tunnel**
Configuration

Fortigate

Create IPsec Phases and Tunnels

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

![VPN Tunnels Menu]

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

![VPN Creation Wizard]

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.
- Set Version to 1, and Mode to Main [ID protection].
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv1

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

**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.**

![Phase 2 Selectors Configuration](image)

---

**Phase 2 Selectors**

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Address</th>
<th>Remote Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forti.ToSophosXG.Phase2</strong></td>
<td>10.198.62.0/255.255.25</td>
<td>192.168.151.0/255.255.0</td>
</tr>
</tbody>
</table>

**Advanced**

- **Encryption**: AES256
- **Authentication**: SHA512

**Enable**

- **Replay Detection**: Yes
- **Perfect Forward Secrecy (PFS)**: Yes
- **Diffie-Hellman Group**: 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
- **Local Port**: All
- **Remote Port**: All
- **Protocol**: All
- **Auto-negotiate**: Yes
- **Autokey Keep Alive**: Yes
- **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**.

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.

Similarly, create another firewall policy for traffic from XG Firewall to Fortigate appliance.
<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><img src="https://example.com" alt="ACCEPT" />, <img src="https://example.com" alt="DENY" />, <img src="https://example.com" alt="LEARN" /></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 IKEv1

**Sophos XG Firewall**

**Create IPsecConnection**

- 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.

![General Settings](image)

- Under Encryption, set Policy to DefaultHeadOffice.
- 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.
- 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.
• 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.
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv1

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

- 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

![IPsec Monitor]

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

![Tunnel Status]
Establish IPsec VPN Connection between Sophos XG Firewall and Fortigate with IKEv1

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.