Pocket Guide

Configure Site-to-Site IPsec VPN between Sophos XG Firewall and Sophos UTM

Product: Sophos XG Firewall
Configure Site-to-Site IPsec VPN between Sophos XG Firewall and Sophos UTM

Contents
Overview........................................................................................................................................3
Prerequisites......................................................................................................................................3
Network Diagram.............................................................................................................................3
Configuration on XG Firewall...........................................................................................................4
Add Local and Remote LAN...............................................................................................................4
Create IPsec VPN Connection...........................................................................................................5
Create a Firewall Rule to Allow VPN Traffic....................................................................................7
Configuration on SG Firewall...........................................................................................................8
Create Network Definitions................................................................................................................8
Create Remote Gateway....................................................................................................................9
Create IPsec Policy............................................................................................................................11
Create IPsec Connection....................................................................................................................11
Result................................................................................................................................................13
Copyright Notice...............................................................................................................................14
Configure Site-to-Site IPsec VPN between Sophos XG Firewall and Sophos UTM

**Overview**
This guide describes how to configure site-to-site IPsec VPN connection using a preshared key between Sophos XG Firewall and Sophos UTM [SG Series Firewall]. The configuration is applicable to the following versions:
- Sophos XG Firewall: Version 16.5 or later
- Sophos UTM (SG Series): Version 9.5 or later

**Prerequisites**
You must have read-write permissions on the SFOS Admin Console and UTM WebAdmin Console for the relevant features.

**Network Diagram**
**Configuration on XG Firewall**

Log in to the SFOS Admin Console.

**Add Local and Remote LAN**

- Go to **System > Hosts and Services > IP Host** and click **Add**.
- Enter the **Name**.
- Select the **IP Family** and set **Type** to **Network**.
- Enter the **IP Address** of local LAN.

![Add IP Host](image)

Repeat the steps to add the remote LAN.

![Add IP Host](image)

Click **Save**.
Create IPsec VPN Connection

- Go to Configure > VPN > IPsec Connections and click Add.

**General Settings**
- Enter the Name.
- Set Connection Type to Site-to-Site.
- Select the Policy that you wish to apply to the connection (we have applied a policy named DefaultHeadOffice).
- Set Action on VPN Restart to Respond Only. The connection will remain ready to respond to an incoming request.

![General Settings](image)

**Authentication Details**
- Set Authentication Type to Preshared Key. You must share the key with the remote peer.
- Enter and confirm Preshared Key.

**Endpoints Details**
- For Local, select the local WAN port.
- For Remote, enter the IP address or domain name.

![Authentication Details](image)
Network Details

- Add the local and remote network details created in Add Local and Remote LAN.

Click Save.
The IPsec connection appears on Configure > VPN > IPsec Connections. To activate the connection, click the red button under Status [Active].
Create a Firewall Rule to Allow VPN Traffic

- Go to Protect > Firewall. Click +Add Firewall Rule and click **User/Network Rule**.
- Enter the Rule Name.
- Set Source Zones to LAN and Source Networks and Devices to HO_XG_LOCAL.
- Set Destination Zones to VPN and Destination Networks to BO_UTM_REMOTE.

Create another firewall rule to allow inbound VPN traffic. Reverse the settings of Source and Destination & Services in the previous firewall rule.
**Configuration on SG Firewall**

Log in to the UTM WebAdmin Console.

**Create Network Definitions**

- Go to Definitions & Users > Network Definitions and click New Network Definition. To create a remote gateway IP object.
- Enter a Name.
- Set Type to Host.
- Enter the IPv4 address of the remote peer.

![Edit Network Definition](image)

To create a remote and local LAN object

- Enter a Name.
- Set Type to Network.
- Enter the LAN IPv4 address and Netmask.
Create Remote Gateway

- Go to Site-to-Site VPN > IPsec > Remote Gateways and select +New Remote Gateway.
- Set Gateway type to Initiate connection. Remote office will initiate the connection and local office will respond to the request since we had set the XG Firewall to ‘Respond only’.
- For Gateway, select the network definition created for the remote gateway IP object. It applies the public IP address of the XG Firewall.
- Set Authentication type to Preshared key. Enter the Key and Repeat the key.
- Set VPN ID type to IP address.
- For Remote networks, enter the subnets that will have access to the IPsec tunnel.
Click Save.
Create IPsec Policy

- Go to **Site-to-Site VPN > IPsec > Policies** and click **+New IPsec Policy**.
- Create a new IPsec policy similar to XG Firewall’s ‘DefaultHeadOffice’ policy.

![New IPsec Policy](image)

Create IPsec Connection

- Go to **Site-to-Site VPN > IPsec > Connections** and click **+New IPsec Connection**.
- Select the Remote gateway created in **Create Remote Gateway**.
- Set Local Interface to WAN.

Note: Local interface should be the gateway used to establish the IPsec connection. It is usually the WAN interface.

- Select the **IPsec Policy** created in the previous step.
- Select the **Local Networks** that will have access to the IPsec tunnel.
- Select **Automatic firewall rules**. If you do not select this, you need to create firewall rules manually to allow traffic between remote subnets.
Go to Site-to-site VPN and check Site-to-site VPN Tunnel Status:

- Green: Tunnel has been created.
- Red: There has been an error.
Configure Site-to-Site IPsec VPN between Sophos XG Firewall and Sophos UTM

**Result**

You have configured Site-to-Site IPsec VPN connection between Sophos XG Firewall and Sophos UTM.
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.