Pocket Guide

Configure Site-to-Site IPsec Tunnel using Preshared Key between two Sophos XG Firewalls

Product: Sophos XG Firewall
Configure Site to Site IPsec Tunnel using Preshared Key between two Sophos XG Firewall

Contents

Scenario ................................................................................................................................................. 3
Prerequisites .......................................................................................................................................... 3
Site A Configuration ............................................................................................................................. 3
   Step 1: Create IPsec Connection ....................................................................................................... 4
   Step 2: Activate Connection ............................................................................................................ 5
Site B Configuration ............................................................................................................................. 6
   Step 1: Create IPsec Connection ....................................................................................................... 6
   Step 2: Activate and Establish Connection ..................................................................................... 7
Result .................................................................................................................................................... 7
Copyright Notice .................................................................................................................................. 8
Scenario

This guide describes a configuration example to demonstrate how to set up a site-to-site IPsec VPN connection between Site A and Site B using a preshared key to authenticate VPN peers.

The example helps you control the Internet traffic of the branch (remote) office through the firewall deployed in the head office.

Prerequisites

- You must have read-write permissions for the relevant features on the SF-OS Admin Console for both the Sophos XG Firewall devices.

Site A Configuration

Log in to the SF-OS Admin Console.
Step 1: Create IPsec Connection

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

- Set Connection Type to SitetoSite.
- Set Policy to DefaultHeadOffice.
- Set Action on VPN Restart to Respond Only.
- Set Authentication Type to Preshared Key and enter the preshared key. This preshared key must be entered in the Site B device too.
- For Local, enter the IP address of Site A; for Remote, enter the IP address of Site B.
- For Local Subnet, select the LAN subnet range of Site A; for the Remote LAN Network, select the LAN subnet range of Site B.

Click Save.
Step 2: Activate Connection

You are automatically taken to Configure > VPN > IPsec Connections.

To activate the connection, click below Status (Active) and Status (Connection).

You have completed Site A configuration.
Site B Configuration
Log in to the SF-OS Admin Console.

Step 1: Create IPsec Connection
Go to Configure > VPN > IPsec Connections and click Add.
- Set Connection Type to SiteToSite.
- Set Policy to DefaultBranchOffice.
- Set Action on VPN Restart to Initiate.
- Set Authentication Type to Preshared Key and enter the preshared key entered in the Site A device.
- For Local, enter the IP address of Site B; for Remote, enter the IP address of Site A.
- For Local Subnet, select the LAN subnet range of Site B; for Remote LAN Network, select the LAN subnet range of Site A.

Click Save.
Step 2: Activate and Establish Connection

You are automatically taken to Configure > VPN > IPSec Connections.

To activate the connection, click below Status [Active] and Status [Connection].

You have completed Site B configuration. If the tunnel is successfully established status is shown in green.

Result

The above configuration establishes an IPSec connection between the two sites.

Note:

1. Make sure that you have configured Network Policies [Protect > Firewall] to allow LAN to VPN and VPN to LAN traffic.

2. In a head office-branch office setup, usually the branch office acts as the tunnel initiator and the head office acts as the responder for the following reasons:
   - The head office cannot initiate the connection since the branch office and other remote sites have dynamic IPs.
   - Retrying connections to multiple branch offices can place a load on the head office. Hence, it is a good practice for the branch office to retry the connection.
Copyright Notice

Copyright 2015-2016 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.