Pocket Guide

Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

Product: Sophos XG Firewall
Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

Contents

Overview ..................................................................................................................................... 3
Prerequisites .............................................................................................................................. 3
Network Diagram ....................................................................................................................... 3
Configuration .............................................................................................................................4
  Palo Alto ..................................................................................................................................................................................... 4
    Create Tunnel Interface ................................................................................................................................................... 4
    Configure IKE Gateway: Phase 1 Parameters .................................................................................................................... 4
    Configure IPsec Phase 2 Parameters ...................................................................................................................................... 6
    Define Monitor Profile .................................................................................................................................................... 7
  Configure IPsec VPN Tunnel .......................................................................................................................... 7
  Create Route for VPN Traffic ........................................................................................................................................ 8
  Define Firewall Rule to allow VPN Traffic ............................................................................................................. 9
Sophos XG Firewall .............................................................................................................................................................. 10
  Create IPsec VPN Policy for Phase 1 and Phase 2 .............................................................................................. 10
  Configure IPsec Connection ........................................................................................................................................ 11
  Activate IPsec Connection ........................................................................................................................................ 13
  Create LAN-VPN Firewall Rules .................................................................................................................................. 13
Result ....................................................................................................................................... 14
Copyright Notice ...................................................................................................................... 15
Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

Overview
This guide describes how to set up a site-to-site IPsec VPN connection between Sophos XG Firewall and Palo Alto Firewall using a pre-shared key to authenticate VPN peers.

Prerequisites
- You must have read-write permissions on the SFOS Admin Console and the Palo Alto Web Admin Console for the relevant features.
- Palo Alto firewall must have at least two interfaces in Layer 3 mode.

Network Diagram
Configuration

Palo Alto Firewall

Create Tunnel Interface

- Go to Network > Interface > Tunnel and click Add.
- Enter Interface Name.
- Select existing Virtual Router.
- For Security Zone, select layer 3 internal zone from which traffic will originate.

Configure IKE Gateway: Phase 1 Parameters

- Go to Network Profiles > IKE Crypto > PA_IKE Crypto.
- In IKE Crypto Profile, add group5 to DH Group, aes-256-cbc to Encryption and sha1 to Authentication.
- Enter Seconds in Key Lifetime and 28800 as Lifetime.
- Set IKEv2 Authentication Multiple to 0.
Click **OK**.

To add **PA_IKE_Crypto** profile to IKE gateway:

- Go to **Network > IKE Gateway > General** and create a new gateway.
- Enter **Name**.
- Set **Version** to **IKEv1 only mode**.
- Set **Address Type** to **IPv4**.
- Set **Interface** to **ethernet1/2**, and **Local IP Address** to **10.198.66.86**.
- Set **Peer IP Type** to **Static**.
- For **Peer IP Address**, enter **10.198.67.249**.
- Set **Authentication** to **Pre-Shared Key**.

Click **OK**.

- Go to **Network > IKE Gateway > Advanced Options**.
- Under **Common Options**, select **Enable Passive Mode**, since Palo Alto will act as the responder for the IPsec connection.
- Under **IKEv1**, set **Exchange Mode** to **main**, and **IKE Crypto Profile** to **PA_IKE_Crypto**, which you have created.
- Select **Dead Peer Detection**. Set **Interval** and **Retry** to **5**.

Click **OK**.
Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

Configure IPsec Phase 2 Parameters

- Go to **Network > IPsec Crypto** and create a profile.
- Enter **Name**.
- Set **IPSec Protocol** to ESP, and **DH Group** to no-pfs.
- Add **aes-256-cbc** and **aes-256-gcm** to **Encryption**.
- Add **sha1** to **Authentication**.
- Set **Lifetime** to **Hours** and enter **1**.

Click OK.
Define Monitor Profile

- Go to Network Profile > Monitor Profile.
- Enter Name.
- Set Action to Wait Recover.
- Enter the following values:
  - Interval (sec): 3
  - Threshold: 5

Click OK.

Configure IPSec VPN Tunnel

- Go to Network > IPSec Tunnel > General.
- Enter Name.
- Select Tunnel Interface you have created in Create Tunnel Interface.
- Set Type to Auto Key, and Address Type to IPv4.
- Set IKE Gateway to PA_IKE, and IPSec Crypto Profile to PA_IPSEC_Crypto, which you have created.
- Select Show Advanced Options and Enable Replay Protection.

Click OK.
To Add Proxy ID:

Go to Network > IPSec Tunnel > Proxy IDs and configure the local and remote subnets for Head Office (HO) and Branch Office (BO).

Create Route for VPN Traffic

- Go to Virtual Router > Static Route > IPv4.
- Enter Name.
- For Destination, enter 172.16.16.0/24.
- Set Interface to tunnel.1, and Next Hop to None.
- For Metric, enter 10.
- Set Route Table to Unicast.
Click **OK**.

- Add tunnel interface in **Virtual Router**.

Create a Firewall Rule to allow VPN Traffic

- Go to **Policies > Security** and create a firewall rule.
Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

**Sophos XG Firewall**

Create IPsec VPN Policy for Phase 1 and Phase 2

- Go to Configure > VPN > IPsec Profiles and click Add.
- Enter Name.
- Set Key exchange to IKEv2 and Authentication Mode to Main Mode.
- Set Key Negotiation Tries to 0.
- Select Allow Re-keying.
- Under Phase 1, set Key Life to 28800, Re-key Margin to 120 and Randomize Re-Keying Margin by to 100.
- Set DH Group (Key Group) to 7 selected.
- Set Encryption to AES256 and Authentication to SHA1.

- Under Phase 2, set PFS Group (DH Group) to Same as Phase-1, and Key Life to 3600.
- Set Encryption to AES256 and Authentication to SHA1.
- Under Dead Peer Detection, set Check Peer After Every to 30 seconds and Wait for Response Up to as 120 seconds.
- Set When Peer Unreachable to Re-initiate.
Click **Save**.

You have created the following IPsec VPN policy.

![IPsec VPN Configuration](image)

**Configure IPsec Connection**

- Go to **Configure > VPN > IPsec Connections** and click **Add**.
- Under **General Settings**, enter **Name**.
- For **IP Version**, select **IPv4**.
- Select **Activate on Save**.
- Set **Connection Type** to **Site-to-Site** and **Gateway Type** to **Initiate the Connection**.
- Under **Encryption**, set **Policy** to **XG_IPsec Policy**, which you have created.
- Set **Authentication Type** to **Preshared Key**. Enter and repeat **Preshared key**.
• Under **Gateway Settings** > **Local Gateway**, set **Listening Interface** to **PortB** – 10.198.67.249 and **Local ID** to **Select Local ID**.
• Under **Local Subnet**, add **XG_Network**.
• Under **Remote Gateway**, set **Gateway Address** to 10.198.66.86 and **Remote ID** to **Select Remote ID**.
• Under **Remote Subnet**, add **Palo_Alto Network**.

Click **Save**.
Establish IPsec VPN Connection between Sophos XG and Palo Alto Firewall

Activate IPsec Connection

- Go to Configure > VPN > IPsec Connections.
- Under Status, click Active and Connection to activate and establish connection.

![IPsec Connections table]

Create LAN-VPN Firewall Rules

Create LAN to VPN and VPN to LAN firewall rules to allow traffic through the VPN tunnel.

![LAN to VPN firewall rule]

![VPN to LAN firewall rule]
**Result**

You have established an IPsec VPN connection between XG Firewall and Palo Alto Firewall.
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.