Pocket Guide

Establish IPsec Connection between Sophos XG Firewall and Check Point

Product: Sophos XG Firewall
Contents

Overview ......................................................................................................................................................... 3
Prerequisites .................................................................................................................................................. 3
Configuration .............................................................................................................................................. 4
  Checkpoint .............................................................................................................................................. 4
    Create a Checkpoint Gateway Network Object ...................................................................................... 4
    Configure Interoperable Device ............................................................................................................. 8
  Create a new VPN Community .................................................................................................................... 9
  Define a topology for VPN Community ..................................................................................................... 14
  Access Control Policy ............................................................................................................................... 15
Sophos XG Firewall .................................................................................................................................... 16
  Create IPSec Profile ................................................................................................................................. 16
  Create Network Object ............................................................................................................................ 17
  Create an IPSec Connection ....................................................................................................................... 17
  Create Firewall Policy .............................................................................................................................. 19
  Activate Tunnel ....................................................................................................................................... 19
Result ............................................................................................................................................................ 20
Copyright Notice ............................................................................................................................................ 21
Establish IPSec Connection between Sophos XG Firewall and Check Point

Overview
This guide describes how to establish a site-to-site IPsec VPN between Sophos XG Firewall and Check Point firewall.

In this scenario, the Check Point gateway is deployed as Peer A and the XG Firewall gateway as Peer B.
The following external IP addresses have been assigned:
- Peer A Gateway: 10.198.66.79
- Peer B Gateway: 10.198.66.115

Prerequisites
- You must have read-write permissions on the SFOS Admin Console for the relevant features.
- You must have Check Point SmartDashBoard R77.30.
**Configuration**

**Check Point**

Log in to the Check Point gateway.

Create a Check Point Gateway Network Object

- Go to Firewall > Network Objects > Check Point and right-click.
- Go to Check Point > Host...
- In General Properties, enter Name.
- For IPv4 Address, enter 10.198.66.79.
- Under Platform, set Hardware to 5000 Appliances, Version to R77.30 and OS to Gaia.
- Under Network Security, select IPSec VPN.
• You can retrieve Topology automatically or manually:
  o **Automatic**: Go to Check Point > Host... > General Properties > Topology. Click Get and click Interfaces with Topology.

  ![Topology Interface](image)

  o **Manual**: Go to Check Point > Host... > General Properties. Click New...
    ▪ In Interface Properties, under General, enter the **Name**.
    ▪ Enter the external network details:
      o **IP Address**: 10.198.66.79
      o **Netmask**: 255.255.254.0
    ▪ Under Topology, select **External** (leads out to the Internet). Under Anti-Spoofing select **Perform Anti-Spoofing based on interface topology**. Anti-Spoofing action is set to **Prevent**.
- Enter the internal network details:
  - IP Address: 192.168.150.150
  - Netmask: 255.255.255.0
- Under Topology, select Internal [leads to the local network]. Select Network defined by the interface IP and Net Mask.
Click OK.
Note: Configure the topology based on the Ethernet interfaces.

- **Under VPN Domain, select Manually defined.** We have selected CP_LAN as the internal network behind the Peer A gateway.

Note: Select All IPAddresses behind Gateway are based on Topology information if you want all networks behind CP firewall to participate in VPN.
Configure Interoperaeable Device

Configure an Interoperable Device to represent the third-party VPN gateway. The public IP address of Peer B gateway is 10.198.66.115.

- Right-click Network Objects and click Interoperable Device.

- Enter the Name.
- For IPv4 Address, enter 10.198.66.115.
Create a New VPN Community

- Go to IPSec VPN. Click New and click Star Community.

- Under General, enter the Name. In this scenario, we have entered S2S to stand for Site-to-Site.

- Under Center Gateways, Add Peer A (Checkpoint Firewall).
• Under Satellite Gateways, Add Peer B (XG Firewall).

• Under Encryption, make sure that the Encryption Method matches the agreed upon configurations. We have selected IKEv1 for IPv4 and IKEv2 for IPv6.
Establish IPSec Connection between Sophos XG Firewall and Check Point

- Under Encryption Suite, select Custom. Click Custom Encryption, and select the required Custom Encryption Suite Properties.

- Select Tunnel Management. Under Permanent Tunnels, select Set Permanent Tunnels.
- Select On all tunnels of specific Gateways and click Select Gateways.
• Under **Community Members**, select the gateways and **Add** them to **Selected Gateways**.

• Under **Advanced Settings**, select the required settings.

**VPN Routing**
Establish IPSec Connection between Sophos XG Firewall and Check Point

Shared Secret

Note: This is a pre-arranged code that you must securely share with the peer gateway administrator. (Based on the option selected in Satellite Gateway while creating IPsec VPN communities.)

Advanced VPN Properties
Under NAT, select Disable NAT inside the VPN community.

![Image of Advanced VPN Properties screen]

Define a Topology for VPN Community

- Go to Network Objects > Interoperable Device.

- Go to Topology. Under VPN Domain, select Manually defined.
Establish IPSec Connection between Sophos XG Firewall and Check Point

- Add XG_LAN.

Note: XG_LAN is the network behind Peer B gateway.

Access Control Policy

Create a policy to allow traffic of S2S VPN Community only.
- Go to Rule Base, Firewall > Policy.
- To add the VPN access rule, right-click the rule number.
- Select Add Rule > Above.
- Select Only connections encrypted in specific VPN Communities option and click add.
- Select the S2S VPN community.

Click OK.

Note:- To allow VPN traffic, add the relevant rules to the firewall rule base.

Install policy on the Gateway.
Establish IPSec Connection between Sophos XG Firewall and Check Point

**Sophos XG Firewall**

Log in to SFOS Admin Console.

**Create IPsec Profile**

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

Note: The XG Firewall parameters must match the parameters you have defined in Check Point Firewall.

![IPsec Profile Configuration](image)

<table>
<thead>
<tr>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

- **Allow Re-keying:** Enable
- **Key Negotiation Tries:** 0<br>Set to unlimited number of negotiation tries
- **Authentication Mode:** Preshared Key Mode
- **Pass Data in Compressed Format:** Enable

**Phase 1**

- **Algorithm:** AES256
- **Encryption:** CFB
- **Authentication:** MD5

- **DH (group Key Group):** 1 (DH-1024, DH-1120, DH-1536, DH-1920, DH-2400, DH-2700, DH-3000)
- **Key Life:** 600 seconds
- **Re-key Margin:** 0 seconds
- **Dead Peer Detection:** Enable

**Phase 2**

- **Algorithm:** AES256
- **Encryption:** CFB
- **Authentication:** MD5

- **PFS (group DH Group):** None
- **Key Life:** 3600 seconds
Establish IPSec Connection between Sophos XG Firewall and Check Point

**Create Network Object**

Go to System > Hosts and Services > IP Host and click Add.

Similarly, create a Network Object for networks behind the Check Point Gateway.

**Create an IPsec Connection**

- Go to Configure > VPN > IPsec Connections and click Add.
- For Name, enter S2S.
- Set Connection Type to Site-to-Site.
- Set Policy to XGCP [Created in Create IPsec Profile].
- Set Action on VPN Restart to Respond Only.
- For Authentication Type, select Preshared Key and use the shared key, which was created in Check Point Firewall.
Establish IPSec Connection between Sophos XG Firewall and Check Point

- For IP Family, select IPv4.
- Set Local Subnet to XG LAN.
- For Remote LAN Network, add Checkpoint LAN.

- For User Authentication Mode select Disabled.
- Set Protocol to All.
Establish IPSec Connection between Sophos XG Firewall and Check Point

Create Firewall Policy

- Go to Protect > Firewall > Add Firewall Rule > User / Network Rule.
- Create firewall rules to allow LAN to VPN and VPN to LAN traffic.

Activate Tunnel

- Go to Configure > VPN > IPsec Connections and click Active.
- Click Connection to activate the tunnel.
Result

You have established IPsec connection between XG Firewall and Check Point 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.