Integration Guide: Sophos XG

This article describes how to establish a Site-To-Site IPSec VPN connection between Sophos XG and the SonicWall network.

- Configuring an IPSec tunnel at the Management Platform
- Configuring at the Sophos XG Interface

Please follow the steps below:

Configuring an IPSec tunnel at the Management Platform

1. Go to the Gateway in your network from which you want to create the tunnel to Sophos XG.

2. Select the three-dotted menu (...) and select Add Tunnel.
3. Select **IPSec Site-2-Site Tunnel** and select **Continue**.

**General Settings**

Enter the General settings:
**Name:** Set the name for the Tunnel.

**Shared Secret:** Enter the same Shared secret you set in Sophos XG.

**Public IP and Remote ID:** Enter the Sophos XG VPN Gateway Public IP address. In Gateway Proposal Subnets, select *Any or Specific Subnet.*

In **Remote Gateway Proposal Subnets** enter the Sophos XG subnet/s.

### Advanced Settings

1. Enter the Advanced settings:

   - **IKE Version:** V1, V2
   - **IKE Lifetime:** 8h
- IKE Version: V1
- IKE Lifetime: 8h
- Tunnel Lifetime: 1h
- Dead Peer Detection Delay: 10s
- Dead Peer Detection Timeout: 30s
- Encryption (Phase 1): aes256
- Encryption (Phase 2): aes256
- Integrity (Phase 1): sha1
- Integrity (Phase 2): sha1
- Diffie-Hellman Groups (Phase 1): 2
- Diffie-Hellman Groups (Phase 1): 2

2. Select Add Tunnel.

Configuring at the Sophos XG Interface

1. Go to the Sophos XG interface and add a local and remote LAN.
2. Go to Hosts and Services > IP Host and select Add to create the local LAN.
3. Go to Hosts and Services > IP Host and select Add to create the LAN.
4. Create an IPsec VPN connection.
5. Go to VPN > IPsec Connections and select Wizard.
6. Give it a name and description.
7. Click **Start** to follow the wizard.

8. Select **Site To Site** as a connection type and select **Head Office**.
9. Set the Authentication Type to preshared key.

![VPN connection wizard]

**Preshared key**
Authenticate IPSec endpoints by using the secret key to both the endpoints

**Digital certificate**
Authenticate IPSec endpoints by exchanging certificates (either self-signed or issued by a certificate authority)

**RSA key**
Authenticate IPSec endpoints using RSA keys. Local RSA key can be regenerated from CLI console. Refer to the console guide for more details

![VPN connection wizard]

10. In the Local Subnet field, choose the local LAN created earlier.

![VPN connection wizard]
11. In the **Remote Subnet** field, choose the remote LAN created earlier.

12. In the **User Authentication Mode** field, choose **Disabled**.

13. Review the IPSec connection summary and click **Finish**.

14. Click the **Status** (Active) to activate the connection.

15. Add two firewall rules allowing VPN traffic. Go to **Firewall** and click **+Add Firewall Rule**.

16. Create two user/network rules as shown below.

   **First Rule:**
Click Save.

Second Rule:

SonicWall Cloud Edge ZTNA Integration Guide
SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.
About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Cloud Edge ZTNA Integration Guide
Updated - October 2020

Copyright © 2020 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates’ products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement


Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to “SonicWall Inc.”, to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035