Integration Guide: WatchGuard

This article describes how to configure a VPN tunnel on the WatchGuard devices using the management interface.

- Configuring an IPSec tunnel on the Management Platform
- Configuring the tunnel on the WatchGuard Management Interface
- Making sure the tunnel is up

Please follow the steps below:

Configuring an IPSec tunnel on the Management Platform

1. Under Network, in the Management Portal on the left side, select the name of the network in which you’d like to set the tunnel.
2. Locate the desired gateway, and select the three-dotted menu (...).

3. Select Add Tunnel and then IPSec Site-2-Site Tunnel.
4. Select **IPSec Site-2-Site Tunnel**. The following window displays:

5. In the **General Settings** section fill in the following information:
- **Name**: Choose whatever name you find suitable for the tunnel.
- **Shared Secret**: Insert a string of your own or use **Generate**.
- **Public IP**: Insert the public IP of the firewall (you can copy it from the Fireware Web UI URL).
- **Remote IP**: Insert the public IP of the firewall (same address as above).
- **Gateway Proposal Subnets**: by default, this should be set to 10.255.0.0/16.
- **Remote Gateway Proposal Subnets**: 0.0.0.0/0 or specify according to your customized settings.

In the **Advanced Settings** section fill in the following information:

- **Diffie-Hellman Groups (Phase 1)**: 2
- **Diffie-Hellman Groups (Phase 2)**: 2

Leave the rest of the fields with the default values (as shown in the attached image).

**Configuring the tunnel on the WatchGuard Management Interface**

1. **Open Fireware Web UI**.
2. In the left panel, select **VPN**, then **Branch Office VPN**.
3. Under **Gateways** select **ADD**. The following window will open (make sure that you're in the **General Settings** tab):
4. Under Gateway Name fill in an indicative name of your own choice.

5. Select Use Pre-Shared Key and insert the Shared Secret you selected or generated while defining the tunnel in the Management Platform.

6. Under Gateway Endpoint select ADD.

7. Fill in the following information:

   - Local Gateway
     - External Interface: External
     - Interface IP Address: Primary Interface IP Address

   - Remote Gateway
     - Static IP Address and enter your gateway IP.
     - Select By IP Address and enter your gateway IP.

   - Advanced
     - Select Specify a different pre-shared key for each gateway endpoint and enter the Shared Secret.
Leave the rest of the fields with the default values.

8. Go to the **Phase 1 Settings** tab and fill in the following information:

- **Version**: IKEv1
- **Mode**: Main
- **NAT Traversal**: Check
- **Keep-alive Interval**: 20 seconds
- **IKE Keep-alive**: Check
- **Message Interval**: 30 seconds
- **Max failures**: 5
- **Dead Peer Detection (RFC3706)**: Check
- **Traffic idle timeout**: 20 seconds
- **Max retries**: 5

9. Go to the **Transform Settings** and select **ADD**. Fill in the following information:

- **Authentication**: SHA2-256
- **Encryption**: AES(256-bit)
- **SA Life**: 24 hours
- **Key Group**: Diffie-Hellman Group 2

10. Go back to the **Branch Office VPN** page. Under **Tunnel** select **ADD**.

- **Name**: Fill in an indicative name of your choice.
- **Gateway**: Choose the gateway that you have just created.

11. Go to the **Addresses** tab and select **ADD**.

- **Local IP**: Any (0.0.0.0/0)
- **Remote IP**: Network IPv4; 10.255.0.0/16 (or the customized subnet you entered while creating your network).
- **Direction**: bi-directional
Leave the rest of the fields with default values (including the NAT tab).

12. Go to the **Phase 2 Settings**
13. Check **Enable Perfect Forward Secrecy** and select Diffie-Hellman Group 2.
14. Under **IPSec Proposals** choose ESP-AES256-SHA256 then select ADD.
15. Select **Save** (no need to customize the settings in the Multicast Settings tab).

**Making sure the tunnel is up**

At the **Fireware Web UI**, go to **System Status -> VPN Statistics -> Branch Office VPN**. If the tunnel is active, the line will appear at the table as shown below:

If you experience a different result, make sure you carefully went through all the steps; however, in case the issue persists please contact our **support team**.

**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](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

1) NOTE: A NOTE icon indicates supporting information.
2) IMPORTANT: An IMPORTANT icon indicates supporting information.
3) 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 Secure Access Integration Guide
Updated - December 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