Integration Guide: FortiGate

This article describes how to configure the VPN tunnels on the FortiGate devices using the Management Platform. Please follow the steps below:

Configuring an IPSec tunnel at 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**.

![Add Tunnel](image)

**Choose template type:**

- **IPSec Site-2-Site Tunnel**
  
  Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.

- **WireGuard Connector**
  
  Interconnect cloud AWS/Azure/GCP/other DC with easy to use connector.

5. Select **Continue**. The following window displays:

![IPSec Site-2-Site Tunnel](image)

**General Settings**

- **Name**:
  
  Enter name

- **Shared Secret**:
  
  Enter shared secret

- **Public IP**:
  
  Enter public IP

- **Remote ID**:
  
  Enter remote ID

**Perimeter Gateway Proposal Subnets**

- **Any (0.0.0.0/0)**

- **10.248.0.0/16**

**Remote Gateway Proposal Subnets**

- **Any (0.0.0.0/0)**

**Advanced Settings**

- **IKE Version**
  
  V1

- **IKE Lifetime**
  
  8h
6. 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 FortiGate device.
   - **Remote ID**: Insert the remote ID of the FortiGate device.
   - **Gateway Proposal Subnets**: by default, this should be set to 10.255.0.0/16.
   - **Remote Gateway Proposal Subnets**: click "Specified Subnets" and specify according to your local LAN Subnets.

![Advanced Settings](image)

7. At the **Advanced Settings** section complete the following information:
   - **Diffie-Hellman Groups (Phase 1)**: 21
   - **Diffie-Hellman Groups (Phase 2)**: 21

   Leave the rest of the fields with the default values (as shown in the attached image).
Configuring the tunnel at the FortiGate Management Interface

1. Open the FortiGate Management Interface.
2. In the left panel, select VPN, then IPsec Tunnels, and select Create New.
3. In the VPN Creation Wizard window set the Name to any name you desire, the Template Type to General tab, and select Next.
4. Fill in the following information:

   - **Network Section:**
     - **IP Version:** IPv4
     - **Remote Gateway:** Static IP Address
     - **IP Address:** Insert the public IP of the location server
     - **Interface:** select your WAN interface
     - **Mode Config:** unchecked
     - **NAT Traversal:** Disable
     - **Dead Peer Detection:** On-Demand

   - **Authentication section:**
- **Method:** Pre-shared Key
- **Pre-shared Key:** Insert the Shared Key you chose in Step 1
- **IKE Version:** 2
- **Mode:** Main (ID protection)

**Phase 1 Proposal section:**
- **Encryption:** AES256
- **Authentication:** SHA256
- **Diffie-Hellman Group:** 21
- **Key Lifetime (seconds):** 28800
- **Local ID:** leave blank
- **XAUTH Section:** leave disabled

**Phase 2 Selectors (+Advanced) section:**
- **Name:** Your choice
- **Local Address:** Your Local network Subnet
- **Remote Address:** Network Subnet, Usually: 10.255.0.0/255.255.0.0
- **Enable Replay Detection:** Checked
- **Enable Perfect Forward Secrecy (PFS):** Checked
- **“Diffie-Hellman Group:** 21
- **Encryption:** AES256
- **Authentication:** SHA256
- **Local Port:** Checked
- **Remote Port:** Checked
- **Protocol:** Checked
- **Key Lifetime:** Seconds
- **Seconds:** 43200

**Configuring firewall and static routing**

It is necessary to add static routes from the subnet (10.255.0.0/16) to the local network and from the local network to the subnet (10.255.0.0/16) to the local network through the VPN tunnel gateway.
1. Go to Network -> Routing -> Static Routes -> Create new -> Route.

   ![Static Routes Table]

   - **Destination**: 10.255.0.0/16
   - **Device**: 10.255.0.0/16
   - **Administrative Distance**: 10
   - **Status**: Enabled
   - **Priority**: 0

2. Set **Destination** to 10.255.0.0/16 and the **Device**: Any other name you chose for the tunnel.

3. Select **OK**. It is necessary to add firewall rules to allow traffic from the subnet (10.255.0.0/16) to your local network or services you desire.


5. Fill in the following information.
   - **Name**: Your choice
   - **Incoming Interface**: Interface name
   - **Outgoing Interface**: Your local network object
   - **Source**: All
   - **Destination**: All
   - **Schedule**: Always
• **Service:** All
• **NAT:** Disabled

If any additional settings appear, leave them in their default status.

6. Select **OK.**

**Make sure the tunnel is up**

At the FortiGate Management Interface, go to **VPN -> IPSec Tunnels.** If the tunnel is up the line will appear in the table:

| Perimeter 01 | wan2 (Hot) | Custom | 1 connections | 3 |

If you experience different results, 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](https://community.sonicwall.com/technology-and-support).
- View video tutorials
- Access [https://mysonicwall.com](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](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