Integration Guide: Cisco Meraki

This article describes how to configure the Site-To-Site VPN tunnel to SonicWall from the Cisco Meraki device using the Management Platform. You must replace the example values in the procedures with the values that are provided in the configuration file.

- Adding a new VPN site
- Editing firewall rules

Please follow the steps below:

Adding a new VPN site

1. Go to the **Non-Meraki VPN peers** section in **Security Appliance** > **Configure** > **Site-to-site VPN** page.
2. Select **Add a peer** and enter the following information:

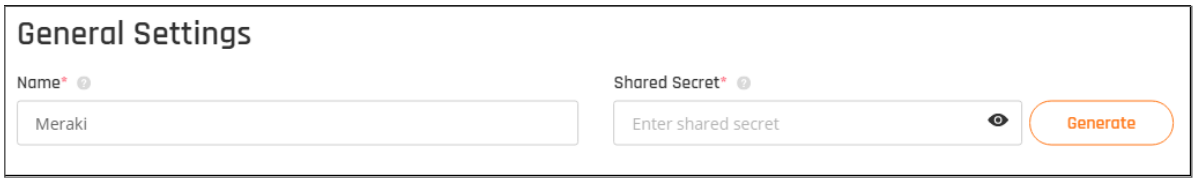
- A name for the remote device or VPN tunnel: Your choice
- The public IP address of the remote device: **Public IP Address of the Gateway**
- The subnets behind the third-party device that you wish to connect to over the VPN: **10.255.0.0/16**
- The IPsec policy to use: Select **Custom** and enter the following information:

Phase 1:

- **Encryption:** Select **AES-256** encryption
- **Authentication:** Select *SHA1* authentication
- **Diffie-Hellman group:** Select between Diffie-Hellman (DH) groups 5
- **Lifetime (seconds):** 28800

Phase 2:

- **Encryption:** Select AES-256 encryption
- **Authentication:** Select SHA1 authentication
- **PFS group:** Select group 5 to enable PFS using that Diffie Hellman group.
- **Lifetime (seconds):** 3600
- The preshared secret key (PSK): Enter the PSK you created in the interface.



- Meraki uses IKEv1, please set accordingly on the Tunnel interface

Editing firewall rules

You can add firewall rules to control what traffic is allowed to pass through the tunnel.
These rules will apply to inbound and/or outbound VPN traffic from all MX appliances in the Organization that participate in site-to-site VPN.

To create a firewall rule, select **Add a rule** in the Site-to-site firewall section on the **Security Appliance > Configure > Site-to-site VPN** page. These rules are configured in the same manner as the Layer 3 firewall rules.
You can add firewall rules to allow traffic from the subnet (10.255.0.0/16) to your local network or services if you desire.

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 - September 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

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

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