Integration Guide: UniFi USG

This article describes how to configure the VPN tunnels on the UniFi - USG devices using the Management Platform.

- Configuring an IPSec tunnel at the Management Portal
- Configuring the tunnel at the UniFi-USG Management Interface
- Configuring a firewall and static routing

Please follow the steps below:

**Configuring an IPSec tunnel at the Management Portal**

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**: Enter a string of your own or use Generate.
- **Public IP**: Enter the public IP of the UniFi USG device.
- **Remote IP**: Enter the public IP of the UniFi USG 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_url)

6. In 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 image below).
Configuring the tunnel at the UniFi - USG Management Interface

1. Open the UniFi - USG management interface.
2. In the left panel, select Networks, then select Create New Network:

3. Select Site to Site VPN > Manual IPsec and fill in with the following information:
   - Enable this Site-to-Site VPN
   - Remote Subnets: Enter the subnet (by default it's 10.255.0.0/16).
   - Peer IP: Enter the public IP of the location server.
   - Local WAN IP: Enter the public IP of the UniFi SCG.
• **Pre-shared key:** Enter the Shared Key you chose on the Management Platform.

4. In the **Advanced Options** fill in the following information:
   - **Key Exchange Version:** IKEv2
   - **Encryption:** AES-256
   - **Hash:** SHA1
   - **DH Group:** 21
   - **PFS:** Enable
   - **Dynamic Routing:** Disable

**Configuring a 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. Also, it's necessary
to create firewall rules to allow this traffic.

1. Go to Routing & Firewall > Static Routes > Create New Route.
   - Choose a name.
   - Enable the route.
   - Enter the subnet (by default it's 10.255.0.0/16) in Destination Network.
   - Make sure to choose the interface you created in the previous section.
2. Create a firewall rule that allows traffic from the subnet to the LAN Network.
CREATE NEW RULE

Name
Enabled
ON
Rule Applied
Before predefined rules
Action
Drop
Reject
Accept
IPv4 Protocol
All
TCP
UDP
TCP and UDP
ICMP
Choose a protocol by name
AH
Enter a protocol number
0

ADVANCED

Logging
Enable logging
States
New
Established
Invalid
Related
IPsec
Don’t match on IPsec packets
Match inbound IPsec packets
Match inbound non-IPsec packets

SOURCE

Source Type
Address/Port Group
Network
IP Address
IPv4 Address Group
perimeter81
CREATE IPV4 ADDRESS GROUP
Port Group
Any
CREATE PORT GROUP
MAC Address

DESTINATION

Destination Type
Address/Port Group
Network
IP Address
Network
LAN
IPv4 Subnet
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](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