Integration Guide: Palo Alto

This article describes how to establish a Site-To-Site IPSec VPN connection between your Palo Alto FW and the network.

- Configuring the tunnel in the Palo Alto WebGUI
- Configuring the tunnel in the Management Platform

Please follow the steps below:

Configuring the tunnel in the Palo Alto WebGUI

1. Open the Palo Alto WebGUI, and select the Network tab.
2. Select Interfaces and open the Tunnel tab.
3. Click Add.

4. Assign the parameters according to the following:
   - **Virtual Router:** Select the virtual router you would like your tunnel interface to reside in.
   - **Security Zone:** Configure a new zone for the tunnel interface for more granular control of traffic ingress/egressing the tunnel. If the tunnel interface is in a zone different from the zone where the traffic will originate or depart, then a policy is required to allow the traffic to flow from the source zone to the SonicWall Cloud Edge ZTNA Integration Guide
zone containing the tunnel interface.

5. Open the **Network** tab.
6. Select **Network Profiles** and go to **IKE Crypto**.
7. Click **Add** (at the bottom of the page) and define the IKE Crypto profile (IKEv1 Phase-1) parameters.

   ![IKE Crypto Profile]

   - **Name**: Choose an indicative name of your own choice.
   - **DH Group**: 14
   - **Encryption**: aes-256-cbc
   - **Authentication**: sha256
   - **Key Lifetime**: 8 Hours
   - **IKEv2 Authentication Multiple**: 0

8. Open the **Network** tab. Select **Network Profiles** and go to **IKE Gateway**.

9. Select **Add** and fill in the following information:

   - **Name**: Choose an indicative name of your own choice
   - **Version**: IKEv1
   - **Address Type**: IPv4
   - **Interface**: The external interface connected to the internet
   - **Local IP Address**: Choose the external IP address
   - **Peer IP Address Type**: IP
   - **Peer Address**: Enter your gateway IP
- **Authentication**: Pre-Shared Key
- **Pre-Shared Key**: Enter a string of your own choice containing lower-case characters, upper-case characters, and a number. Please write down this value as you will use it to configure the tunnel and the Management Platform as well.
- **Local Identification**: None (the gateway will use the local IP as the local identification value)
- **Peer Identification**: None (the gateway will use the peer IP as the peer identification value)

10. Open the **Network** tab. Select **Network Profiles** and go to **IPSec Crypto**.
11. Select **Add** and fill in the following information:

   ![IPSec Crypto Profile](image)

   - **Name**: Phase2
   - **IPSec Protocol**: ESP
   - **DH Group**: 14
   - **Encryption**: aes-256-gcm
   - **Lifetime**: 1 hour
   - **Authentication**: sha256

12. Open the **Network** tab. Select **IPSec Tunnels**, then **Add** and fill in the following information:

   ![IPSec Tunnel](image)
- **Name**: Choose the name of your own choice
- **Tunnel Interface**: Choose the appropriate interface
- **Type**: Auto Key
- **Address Type**: IPv4
- **IKE Gateway**: Choose the gateway that was defined earlier
- **IPSec Crypto Profile**: Choose the profile that was defined earlier

13. Open the **Network** tab.
14. Select **Virtual Routers**, then select **Static Routes** and click **Add**. Fill in the following information:

![Virtual Router: Static Route - IPv4](image)

- **Name**: Choose an indicative name of your own choice
- **Destination**: Your subnet (if such an object does not exist yet make sure to define it)
- **Interface**: Choose the appropriate interface
- **Next Hop**: None
- **Metric**: 10
- **Route Table**: Unicast
- **BFD Profile**: Disable BFD

15. Open the **Policies** tab and select **Security**.

![Policy Table](image)
By default, IKE negotiation and IPSec/ESP packets are allowed.

16. If you see somewhat differently or if you wish to have more granular traffic control, select **ADD**, and create an appropriate rule.

### Configuring the tunnel in the Management Platform

1. Enter the Management Platform.
2. Under the **Networks** tab in the left menu, select the name of the network in which you’d like to set the tunnel.
3. Locate the desired gateway, select the three-dotted menu (…).
4. Select **Add Tunnel** and then **IPSec Site-2-Site Tunnel**.

5. Fill in the following information:
   - **Name**: Specify an indicative name
   - **Public IP**: Insert the external IP you receive from your ISP.
   - **Remote ID**: Insert the FW’s external Interface IP. This can be found in Palo Alto WebGUI under **Network /Interfaces /Ethernet**.

**NOTE:** Remote ID and Public IP will be identical if your FW is connected directly to the internet.

   - **Shared Secret**: Insert the same **Pre-Shared Key** that you inserted in Palo Alto WebGUI.
   - **Gateway Proposal Subnets**: The default value is 10.255.0.0/16. If you have multiple tunnels to the same gateway make sure the adjust the range accordingly to avoid overlap.
**Remote Gateway Proposal Subnets**: Specify the subnet that you defined as a local IP address configuring the IKE Gateway at the PA portal.

6. At the **Advanced Settings** section fill in the following information:

   - **IKE Version**: 1
   - **IKE Lifetime**: 8h
   - **Tunnel Lifetime**: 1h
   - **Dead Peer Detection Delay**: 10s
   - **Dead Peer Detection Timeout**: 30s
   - **Encryption (Phase 1)**: aes256
   - **Encrption (Phase 2)**: aes256
   - **Integrity (Phase 1)**: sha256
   - **Integrity (Phase 1)**: sha256
   - **Diffie-Hellman Groups (Phase 1)**: 14
   - **Diffie-Hellman Groups (Phase 2)**: 14

---

**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

| 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


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