Integration Guide: Check Point

This article describes how to configure a Check Point firewall using the Checkpoint Smart Console. The example values should be replaced with your actual values found within your Management Platform.

Please follow the steps below.

- Creating a gateway object at the Check Point Smart Console
- Creating a VPN Star community
- Additional settings at the Check Point Smart Console
- Adding the gateway IP and remote subnet
- Configuring the tunnel at the Management Platform

Creating a gateway object at the Check Point Smart Console

1. Open the Check Point Smart Console.
2. Go to Security Policies.
3. Add Gateway as an object as shown in the image below. Please make sure you have your gateway IP (which can be found in the Network tab in your Management Platform).
Creating a VPN Star community

1. Create a new **Star Community**.

![Image of creating a new Star Community]

2. Fill in the following information:
   - Specify an **Object Name** of your own choice.
   - Add your gateway as **Center Gateway**.
   - Add your external Firewall IP as **Satellite Gateways**.

![Image of Star Community with configurations]
3. Go to **Shared Secret**.
4. Add a **Shared Secret** and write it down as it will also be used in configuring the tunnel at the Management Platform. Please note: Check Point recommends choosing a shared secret that contains at least 20 characters.

5. Go to **Encryption** and set **IKE Security**. Note that you'll need to set these exact preferences while configuring the tunnel at the Management Platform.
6. Go to **Tunnel Management**.
7. Set VPN Tunnel Sharing to **One VPN tunnel per Gateway pair**.

8. Important: The remote subnets you defined need to match exactly to the remote subnets entered within the other side (if additional subnets are added, it can cause the tunnels to break from time to time).

9. Select **OK**.

### Additional settings at the Check Point Smart Console

1. Under Check Point firewall policy, add a rule for any to any, in and out to 10.255.0.0/16 (this may vary if you did not set the default subnet during network creation).
2. Create a Network group with All local networks to be trusted with the VPN tunnels.
Adding the gateway IP and remote subnet

1. Open the object you created.
2. Go to Topology.
3. Select New at the top.
4. Under the General tab, fill in Name, IP Address, and Net Mask.
5. Add remote subnet 10.255.0.0 as IP Address.
6. Add "255.255.0.0" as Net Mask.
7. Open the **Topology** tab. Select **Network defined by the interface IP and Net Mask**.

![Interface Properties](image)

8. Select **OK**.
9. Go to **Topology**.
10. Select **New** at the top.
11. Under the **General** tab, fill in **Name**, **IP Address**, and **Net Mask**.
12. Add gateway IP `xxx.xxx.xxx.xxx` as **IP Address**.
13. Add “255.255.255.255” as **Net Mask**.
14. Open the **Topology** tab. Select **External (leads out to the internet)**.
15. Select **OK**.
16. Publish and **Install Policy**.
Configuring the tunnel at the Management Platform

1. Open your Management Platform and go to the **Networks** tab.

![SonicWall Management Platform Network Tab](image)

2. Go to the gateway in your network from which you want to create the tunnel to Azure, select the three-dotted menu (...) beside it, and select **Add Tunnel**.

3. Select IPSec Site-2-Site Tunnel and select **Continue**.

4. Fill in the following information:
   - **Name**: Choose an indicative name of your own choice
   - **Shared Secret**: Enter the same Shared secret you set in the Check Point Interface
   - **Public IP**: Enter the Check Point public IP
   - **Remote ID**: Enter the Check Point public IP
   - **Gateway Proposal Subnets**: Select any or specify according to your needs
   - **Remote Gateway Proposal Subnets**: Enter the Check Point internal subnet(s)
   - Fill in the **Advanced Settings** parameters according to your Check Point settings

5. Select **Add Tunnel**.

**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
• 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 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