Integration Guide: Edgemax

This article describes how to configure a VPN tunnel on the Edgemax device using the management interface.

- Configuring SonicWall Site-to-Site with Edgemax Device
- Configuring the Edgemax Device

Please follow the steps below:

Configuring SonicWall Site-To-Site with Edgemax Device

1. Go to the Gateway in your network from which you want to create the tunnel to Edgemax.
2. Select the three-dotted menu (…) and select **Add Tunnel**

Add Tunnel

Choose the type of tunnel between your gateway and resources. *[Learn More]*

**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.

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

Enter the General settings:

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

#### General Settings

- **Name**: Set the name for the Tunnel.
- **Shared Secret**: Put the same Shared secret you set in Edgemax.
- **Public IP** and **Remote ID**: enter Edgemax VPN Gateway Public IP address.
- In **Gateway Proposal Subnets** select **Any** or **Specific Subnet**.
- In **Remote Gateway Proposal Subnets** put your Edgemax subnet/s.

---

**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) Specified Subnets

#### Advanced Settings

- **IKE Version**: V1 V2
- **IKE Lifetime**: 8h

---

SonicWall Cloud Edge ZTNA Integration Guide
Advanced Settings

Enter the Advanced settings:

- **IKE Version**: V1
- **IKE Lifetime**: 8h
- **Tunnel Lifetime**: 1h
- **Dead Peer Detection Delay**: 15s
- **Dead Peer Detection Timeout**: 30s
- **Encryption (Phase 1)**: aes256
- **Encryption (Phase 2)**: aes256
- **Integrity (Phase 1)**: sha1
- **Integrity (Phase 2)**: sha1
- **Diffie-Hellman Groups (Phase 1)**: 2
- **Diffie-Hellman Groups (Phase 2)**: 2

4. Select Add Tunnel.

Configuring the Edgemax device

1. On the Edgemax router go to the CLI and enter configuration mode.
2. Enable the `auto-firewall-nat-exclude` feature which automatically creates the IPsec firewall/NAT policies in the iptables firewall.

   ```
   set vpn ipsec auto-firewall-nat-exclude enable
   ```
3. **Create IKE / Phase 1 (P1) Security Associations (SAs).**

   set vpn ipsec ike-group FOO0 lifetime 28800  
   set vpn ipsec ike-group FOO0 proposal 1 dh-group 14  
   set vpn ipsec ike-group FOO0 proposal 1 encryption aes128  
   set vpn ipsec ike-group FOO0 proposal 1 hash sha1  
   set vpn ipsec ike-group FOO0 dead-peer-detection interval 15  
   set vpn ipsec ike-group FOO0 dead-peer-detection timeout 30  

4. **Create the ESP / Phase 2 (P2) SAs and enable Perfect Forward Secrecy (PFS).**

   set vpn ipsec esp-group FOO0 lifetime 3600  
   set vpn ipsec esp-group FOO0 pfs enable  
   set vpn ipsec esp-group FOO0 proposal 1 encryption aes128  
   set vpn ipsec esp-group FOO0 proposal 1 hash sha1  

5. **Define the remote peering address (replace <secret> with your desired passphrase and <Your Gateway IP> with the Gateway IP you got from the connector).**

   set vpn ipsec site-to-site peer <Your Gateway IP> authentication mode pre-shared-secret  
   set vpn ipsec site-to-site peer <Your Gateway IP> authentication pre-shared-secret <secret>  
   set vpn ipsec site-to-site peer <Your Gateway IP> description ipsec  
   set vpn ipsec site-to-site peer <Your Gateway IP> local-address <Your Edgerouter WAN IP>  

6. **Link the SAs created above to the remote peer and bind the VPN to a virtual tunnel interface (vti0).**

   set vpn ipsec site-to-site peer <Your Gateway IP> ike-group FOO0  
   set vpn ipsec site-to-site peer <Your Gateway IP> vti bind vti0  
   set vpn ipsec site-to-site peer <Your Gateway IP> vti esp-group FOO0  

7. **Configure the virtual tunnel interface (vti0) and assign it an IP address (this is just an internal IP address for the Virtual Tunnel Interface - IP can be anything that you do not use on any of your sites)**

   set interfaces vti vti0 address 192.168.20.20/32  

8. **Create a static route for the subnet (in this case the default 10.255.0.0/16)**

   set protocols static interface-route 10.255.0.0/16 next-hop-interface vti0  

9. **Commit the changes and save the configuration.**

   commit ; save  

10. **Go back to the GUI, click VPN -> site to site connection.**

11. **Verify that the peer associated with the Gateway IP you got from the connector has:**

    - **Remote subnet:** 10.255.0.0/16 (or the local gateway that you selected)
    - **Local subnet:** All the subnet range (CIDR) of your LAN devices
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.

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