Integration Guide: Sophos XG

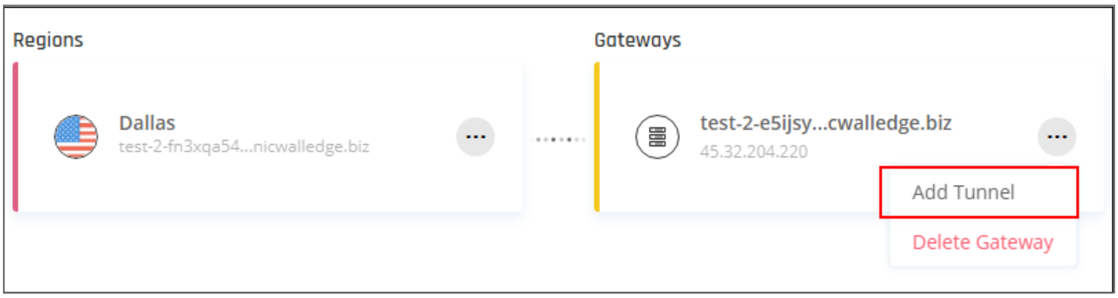
This article describes how to establish a Site-To-Site IPSec VPN connection between Sophos XG and the SonicWall network.

- Configuring an IPSec tunnel at the Management Platform
- Configuring at the Sophos XG Interface

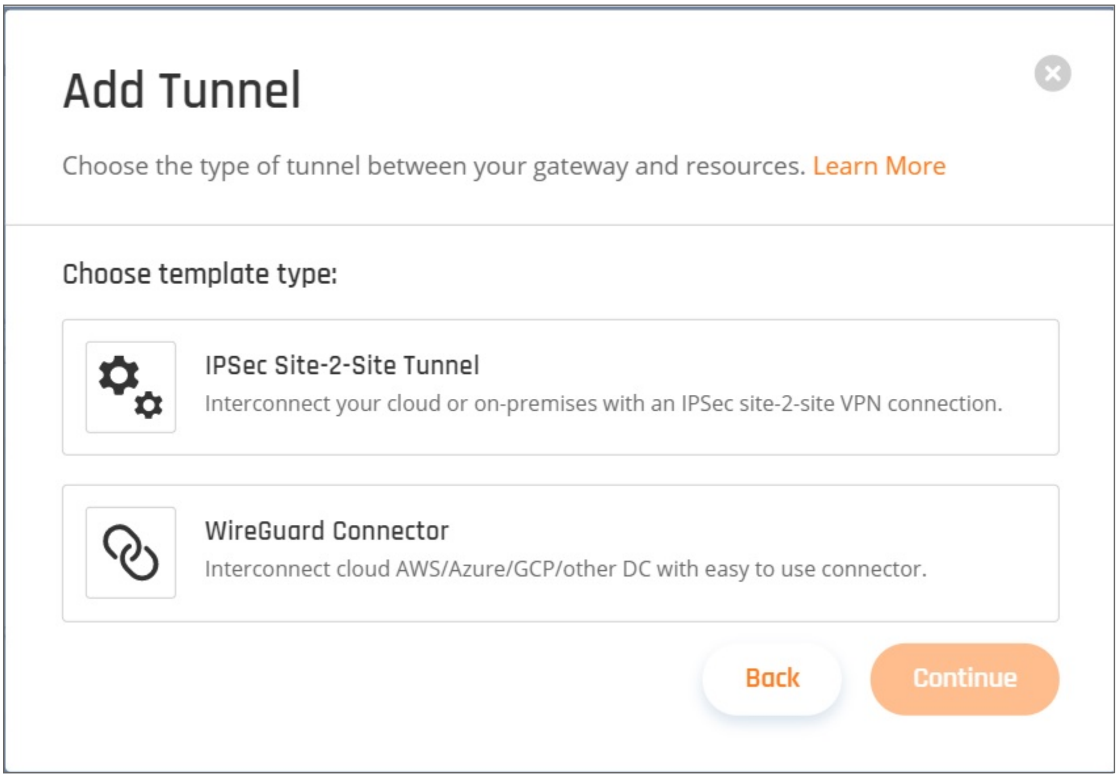
Please follow the steps below:

Configuring an IPSec tunnel at the Management Platform

1. Go to the Gateway in your network from which you want to create the tunnel to Sophos XG.


Regions
Gateways
Dallas
test-2-fn3xqa54...nicwalledge.biz
test-2-e5ijsy...cwalledge.biz
45.32.204.220
Add Tunnel
Delete Gateway

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:

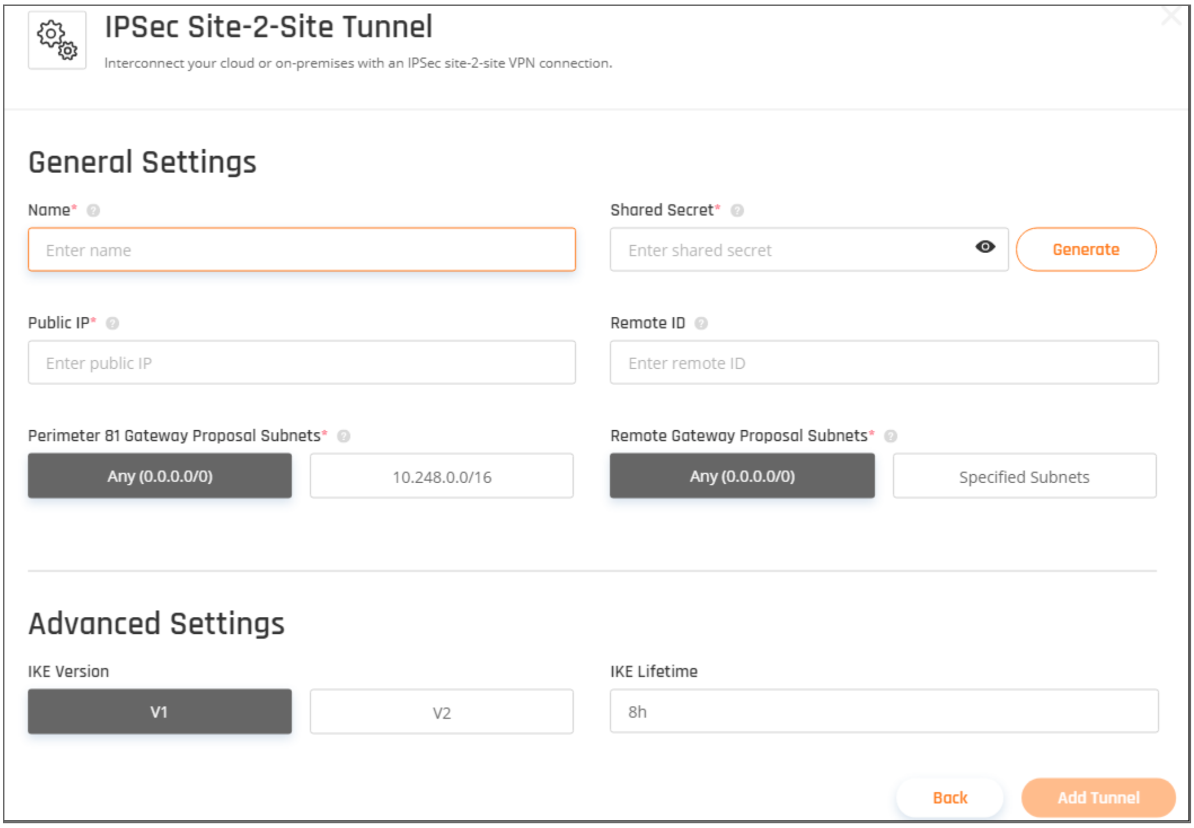
IPSec Site-2-Site Tunnel
Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.

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*: Enter name

Shared Secret*: Enter shared secret

Public IP*: Enter public IP

Remote ID: Enter remote ID

Perimeter 81 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

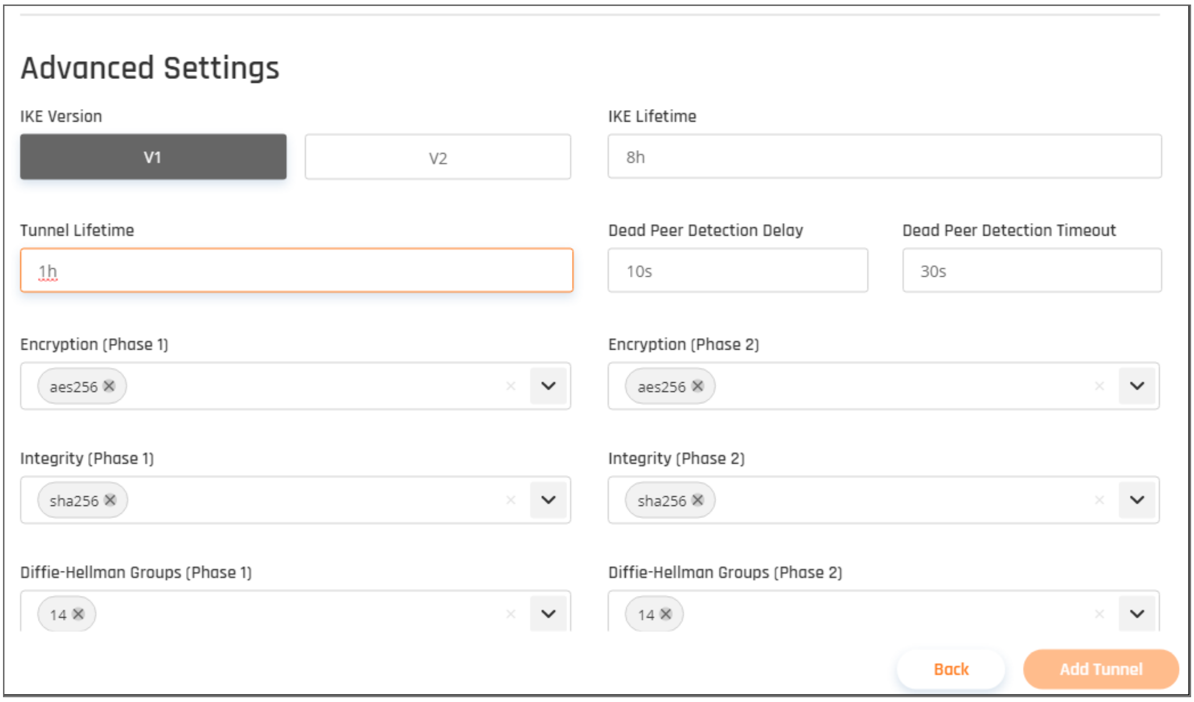
IKE Version: V1 | V2

IKE Lifetime: 8h

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

Advanced Settings

1. Enter the Advanced settings:


Advanced Settings

IKE Version: V1 | V2

IKE Lifetime: 8h

Tunnel Lifetime: 1h

Dead Peer Detection Delay: 10s

Dead Peer Detection Timeout: 30s

Encryption (Phase 1): aes256

Encryption (Phase 2): aes256

Integrity (Phase 1): sha256

Integrity (Phase 2): sha256

Diffie-Hellman Groups (Phase 1): 14

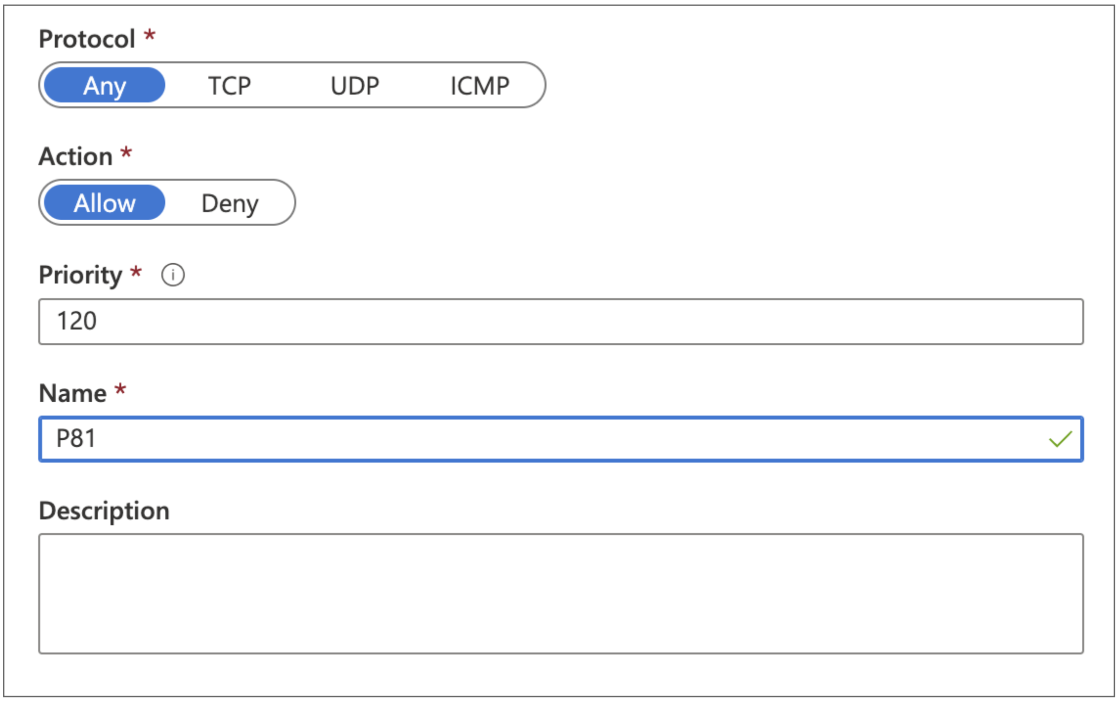
Diffie-Hellman Groups (Phase 2): 14

- **IKE Version:** V1
- **IKE Lifetime:** 8h
- **Tunnel Lifetime:** 1h
- **Dead Peer Detection Delay:** 10s
- **Dead Peer Detection Timeout:** 30s
- **Encryption (Phase 1):** aes256
- **Encryption (Phase 2):** aes256
- **Integrity (Phase 1):** sha1
- **Integrity (Phase 2):** sha1
- **Deffie-Hellman Groups (Phase 1):** 2
- **Deffie-Hellman Groups (Phase 1):** 2

2. Select **Add Tunnel**.

Configuring at the Sophos XG Interface

1. Go to the Sophos XG interface and add a local and remote LAN.
2. Go to Hosts and Services > IP Host and select **Add** to create the local LAN.
3. Go to Hosts and Services > IP Host and select **Add** to create the LAN
4. Create an IPsec VPN connection.
5. Go to VPN > IPsec Connections and select **Wizard**.



Protocol *

Action *

Priority *

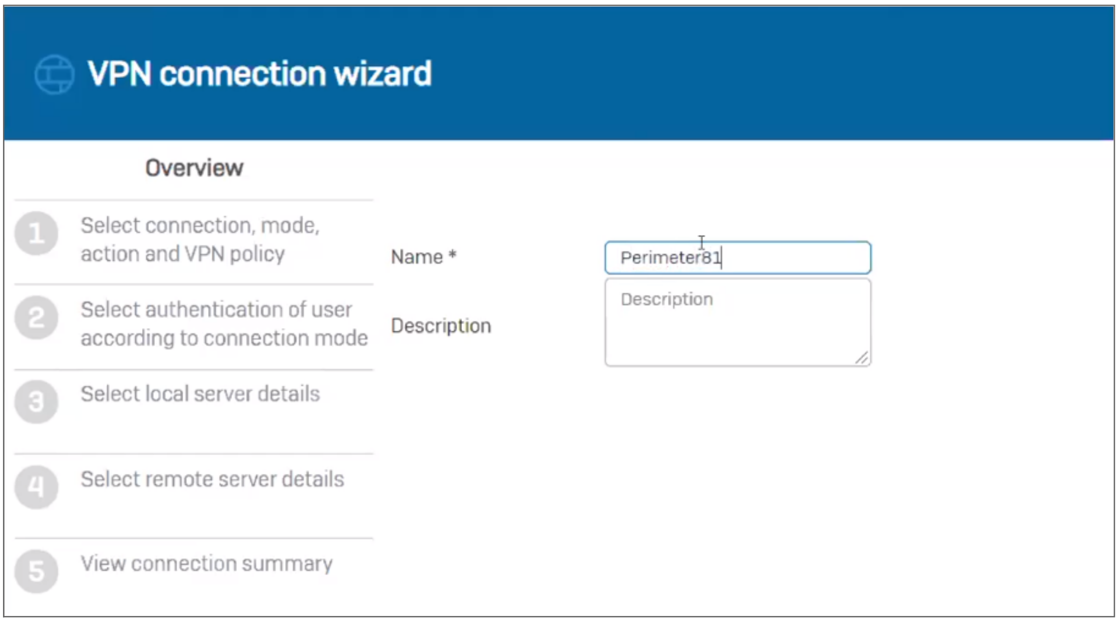
120

Name *

P81

Description

6. Give it a name and description.



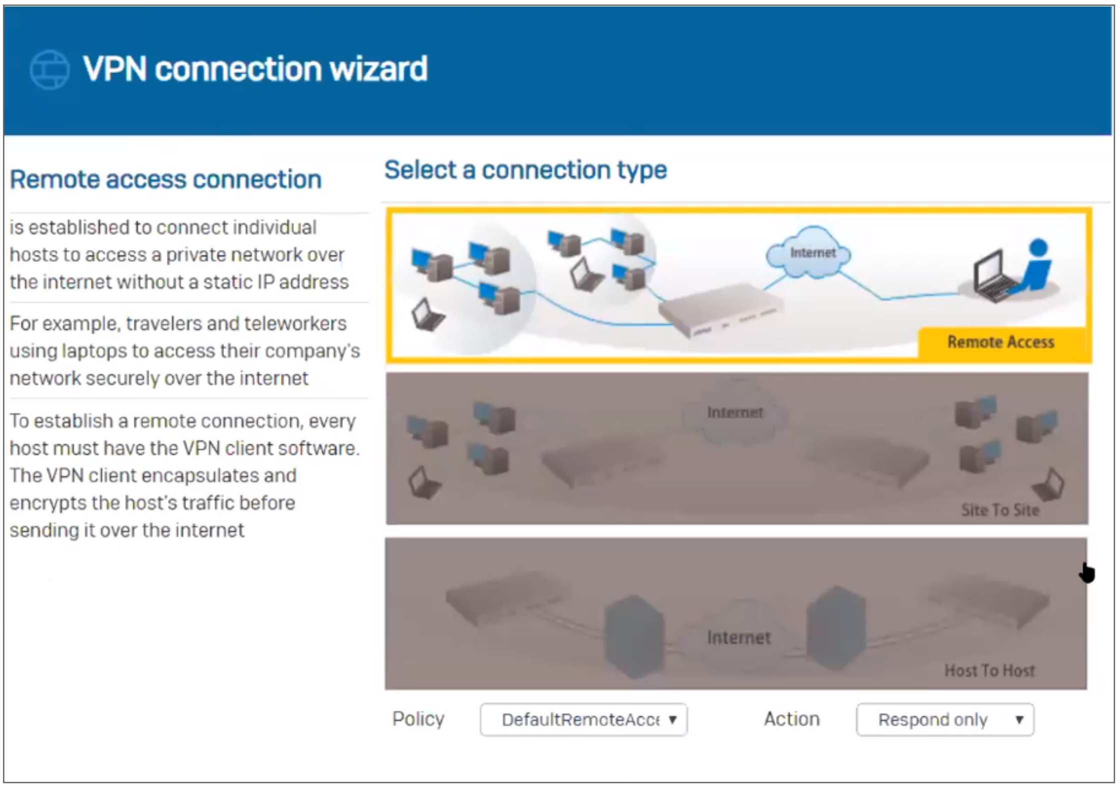
VPN connection wizard

Overview
1 Select connection, mode, action and VPN policy
2 Select authentication of user according to connection mode
3 Select local server details
4 Select remote server details
5 View connection summary

Name * Perimeter81

Description

7. Click **Start** to follow the wizard.



VPN connection wizard

Remote access connection

is established to connect individual hosts to access a private network over the internet without a static IP address

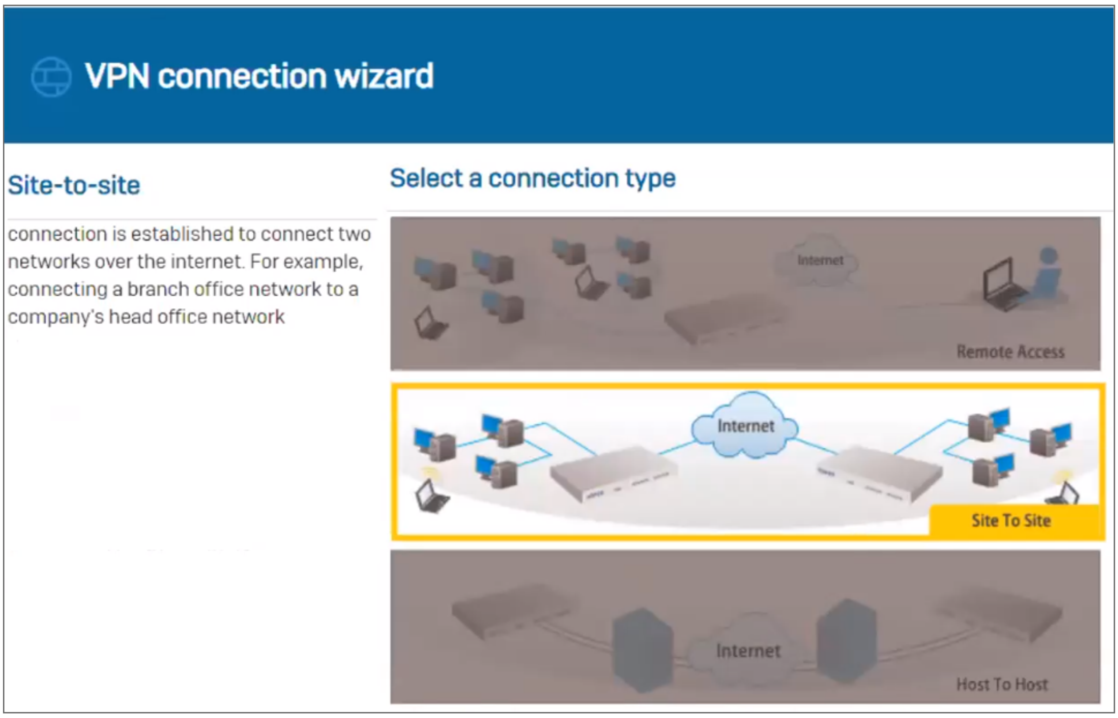
For example, travelers and teleworkers using laptops to access their company's network securely over the internet

To establish a remote connection, every host must have the VPN client software. The VPN client encapsulates and encrypts the host's traffic before sending it over the internet

Select a connection type

Policy DefaultRemoteAcce ▾ Action Respond only ▾

8. Select **Site To Site** as a connection type and select **Head Office**.



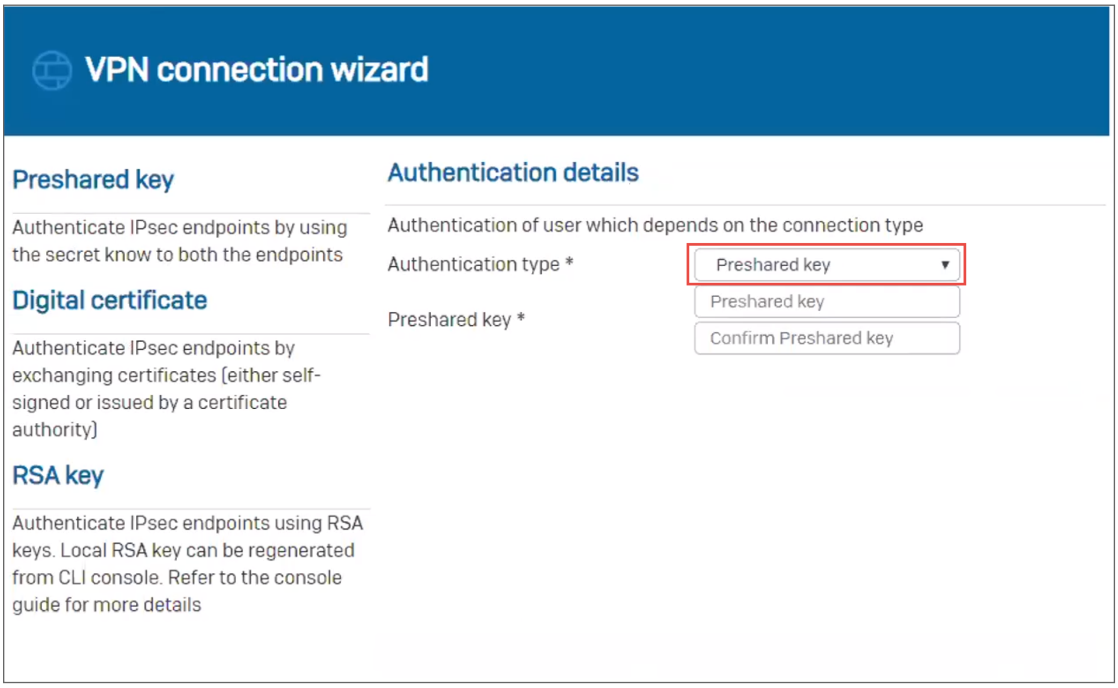
VPN connection wizard

Site-to-site

connection is established to connect two networks over the internet. For example, connecting a branch office network to a company's head office network

Select a connection type

9. Set the **Authentication Type** to **preshared** key.



VPN connection wizard

Preshared key

Authenticate IPsec endpoints by using the secret know to both the endpoints

Digital certificate

Authenticate IPsec endpoints by exchanging certificates (either self-signed or issued by a certificate authority)

RSA key

Authenticate IPsec endpoints using RSA keys. Local RSA key can be regenerated from CLI console. Refer to the console guide for more details

Authentication details

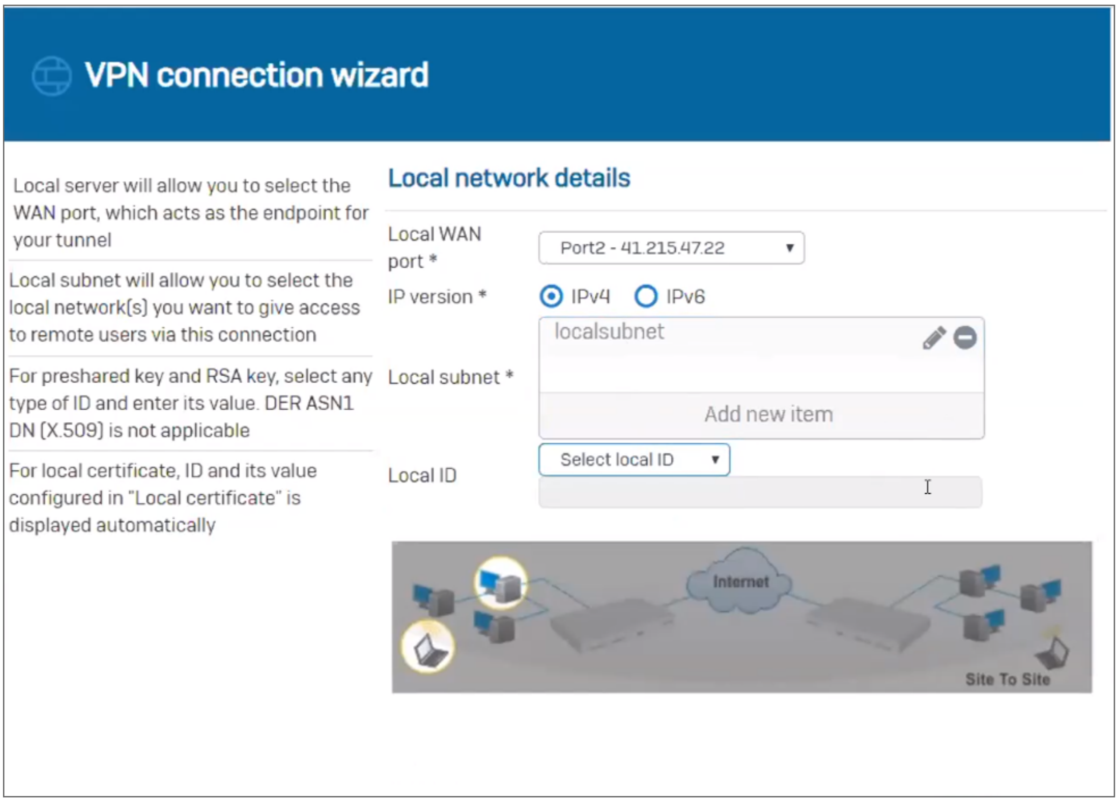
Authentication of user which depends on the connection type

Authentication type * Preshared key ▾

Preshared key * Preshared key

Confirm Preshared key

10. In the **Local Subnet** field, choose the local LAN created earlier.



VPN connection wizard

Local server will allow you to select the WAN port, which acts as the endpoint for your tunnel

Local subnet will allow you to select the local network(s) you want to give access to remote users via this connection

For preshared key and RSA key, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable

For local certificate, ID and its value configured in "Local certificate" is displayed automatically

Local network details

Local WAN port * Port2 - 41.215.47.22 ▾

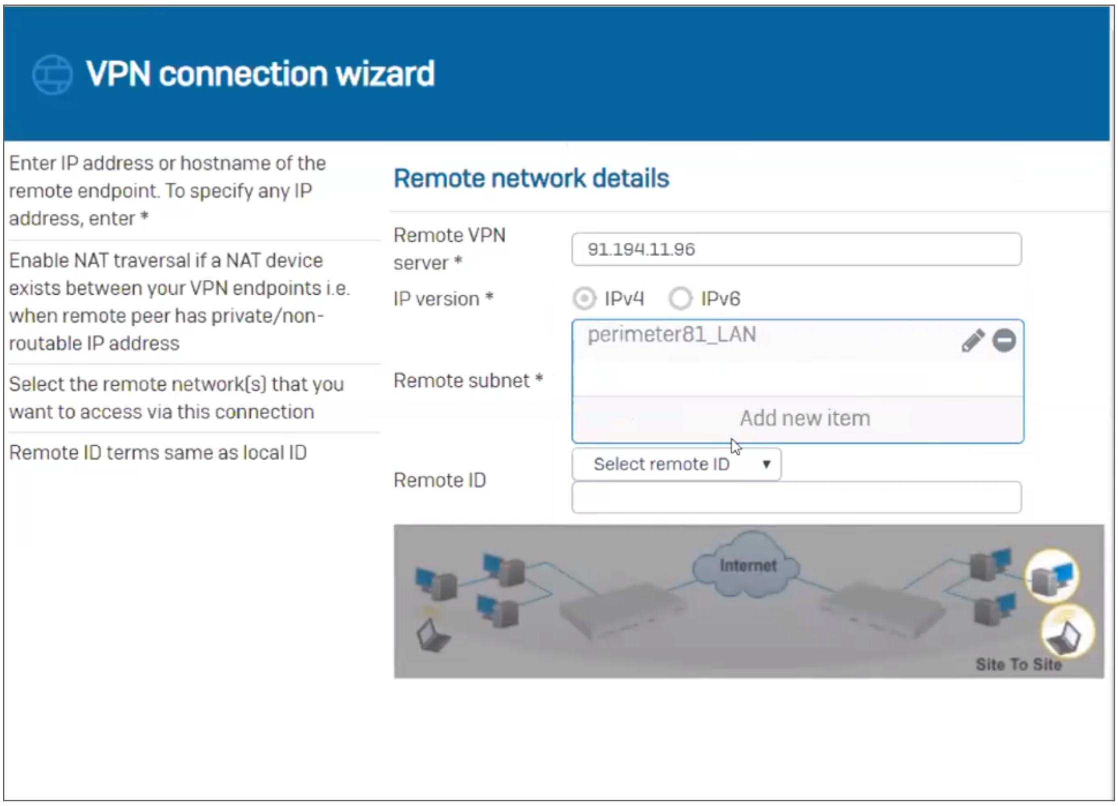
IP version * ● IPv4 ○ IPv6

Local subnet * localsubnet

Add new item

Local ID Select local ID ▾

11. In the **Remote Subnet** field, choose the remote LAN created earlier.



VPN connection wizard

Enter IP address or hostname of the remote endpoint. To specify any IP address, enter *

Enable NAT traversal if a NAT device exists between your VPN endpoints i.e. when remote peer has private/non-routable IP address

Select the remote network(s) that you want to access via this connection

Remote ID terms same as local ID

Remote network details

Remote VPN server * 91.194.11.96

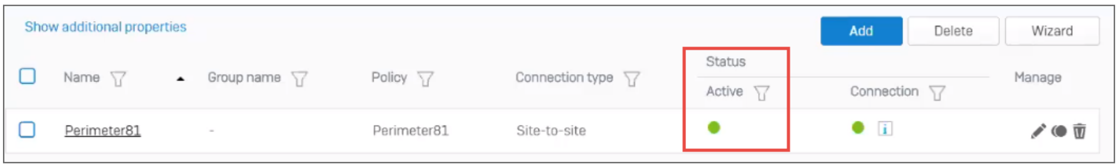
IP version * ○ IPv4 ○ IPv6

Remote subnet * perimeter81_LAN

Add new item

Remote ID Select remote ID ▾

12. In the **User Authentication Mode** field, choose **Disabled**.
13. Review the IPsec connection summary and click **Finish**.
14. Click the **Status** (Active) to activate the connection.

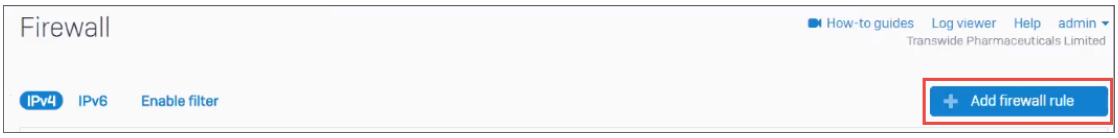


Show additional properties

Add Delete Wizard

□	Name	Group name	Policy	Connection type	Status Active	Connection	Manage
□	Perimeter81	-	Perimeter81	Site-to-site	●	● ℹ	

15. Add two firewall rules allowing VPN traffic. Go to **Firewall** and click **+Add Firewall Rule**.



Firewall

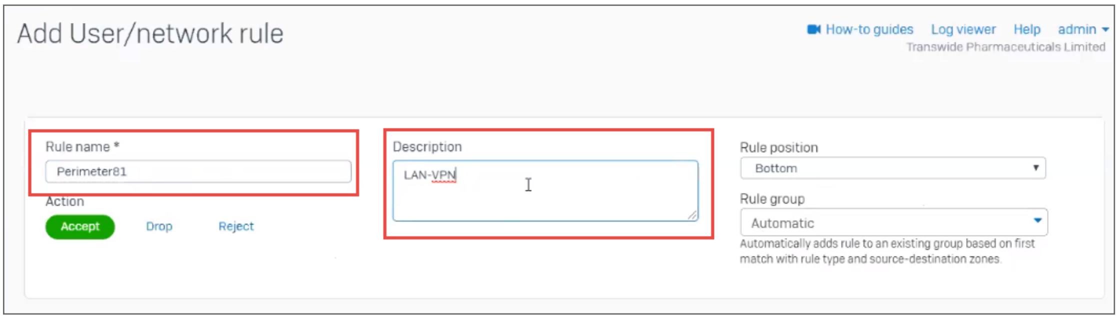
How-to guides Log viewer Help admin ▾
Transwide Pharmaceuticals Limited

IPv4 IPv6 Enable filter

+ Add firewall rule

16. Create two user/network rules as shown below.

First Rule:


Add User/network rule

Rule name *: Perimeter81

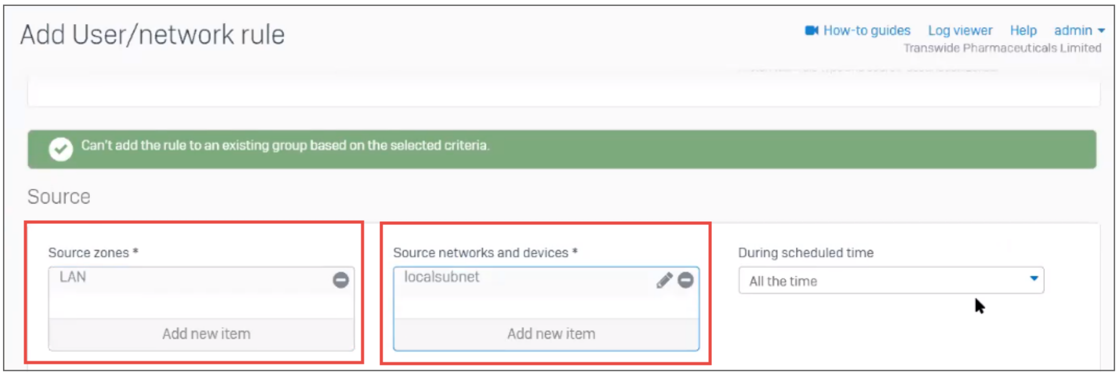
Description: LAN-VPN

Rule position: Bottom

Rule group: Automatic

Automatically adds rule to an existing group based on first match with rule type and source-destination zones.

Action: Accept | Drop | Reject


Add User/network rule

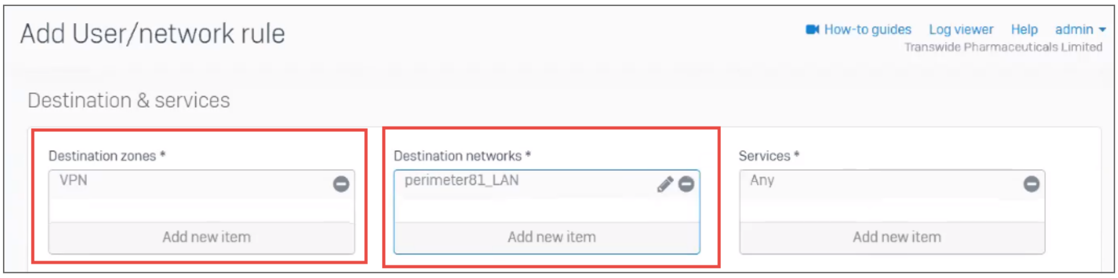
Can't add the rule to an existing group based on the selected criteria.

Source

Source zones *: LAN

Source networks and devices *: localsubnet

During scheduled time: All the time


Add User/network rule

Destination & services

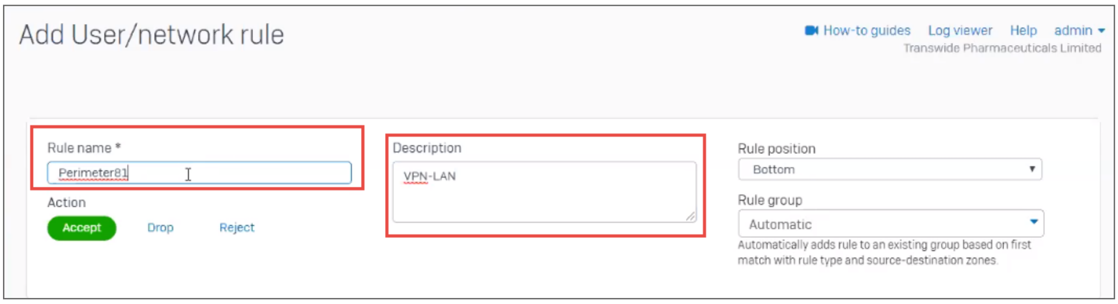
Destination zones *: VPN

Destination networks *: perimeter81_LAN

Services *: Any

Click **Save**.

Second Rule:


Add User/network rule

Rule name *: Perimeter81

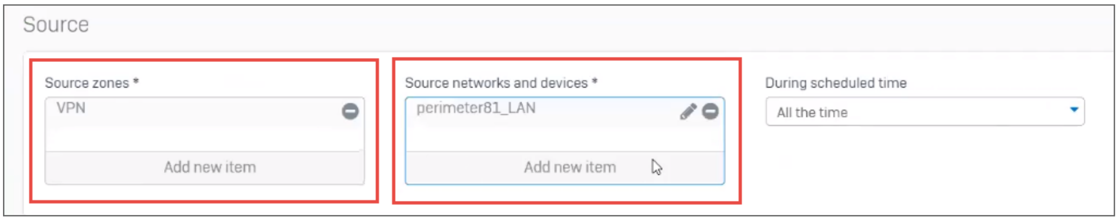
Description: VPN-LAN

Rule position: Bottom

Rule group: Automatic

Automatically adds rule to an existing group based on first match with rule type and source-destination zones.

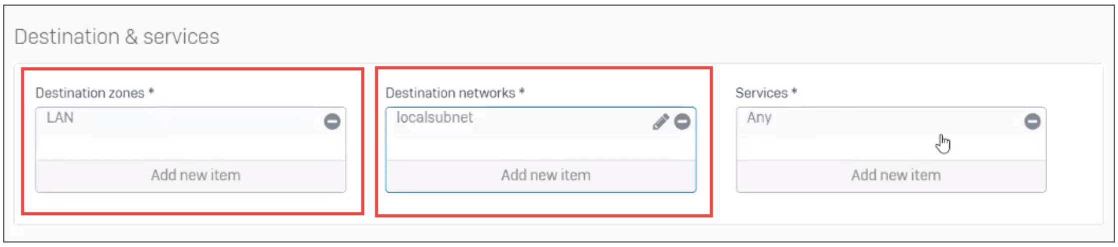
Action: Accept | Drop | Reject


Source

Source zones *: VPN

Source networks and devices *: perimeter81_LAN

During scheduled time: All the time


Destination & services

Destination zones *
LAN

Destination networks *
localsubnet

Services *
Any

Click **Save**.

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

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