RG-WALL 1600-Z-S Cloud-Managed Firewall

IPsec VPN Typical Configuration Examples

Document version: V1.2
Date: August 28, 2024

Copyright

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Official website of Ruijie Reyee: https://reyee.ruijie.com/
- Online support center: https://reyee.ruijie.com/en-global/support
- Case portal: https://www.ruijie.com/support/caseportal
- Community: https://community.ruijienetworks.com/portal.php
- Live chat: https://networks.s5.udesk.cn/im_client/?web_plugin_id=1296&language=en-us

Conventions

1. GUI Symbols

GUI Symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

✓ **Specification**

An alert that contains a description of product or version support.

3. Notes

This document describes the features and use methods of the product and provides a guide for users to configure and use it in the trial stage.

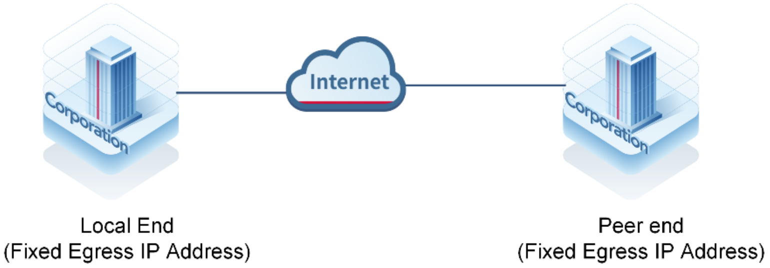
Contents

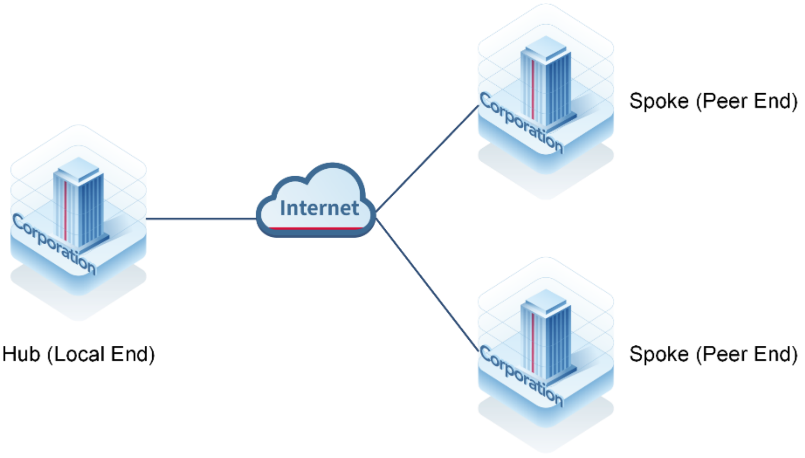
1 Overview

Internet Protocol Security (IPsec) is a protocol suite for establishing secure connections over public networks. The objective of IPsec is to provide security services for network layer traffic in IPv4 and IPv6 formats. Typically, IPsec is used to provide Virtual Private Network (VPN) services between two sites or between remote users and enterprise networks.

IPsec is an open protocol suite consisting of multiple protocols, including security protocols Authentication Header (AH). Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE), as well as authentication and encryption algorithms. The AH and ESP protocols provide security services, and the IKE protocol enables key exchange.

IPsec VPN applies to the following scenarios.

Scenario	Description
Site-to-Site	The peer device has a fixed IP address, and the local device is typically located at one end of a tunnel or a spoke site on a hub-spoke network.  Corporation Internet Corporation Local End (Fixed Egress IP Address) Peer end (Fixed Egress IP Address) Key configurations: ● Configure the address or domain name of the peer. ● Configure interesting traffic that is symmetric to that of the peer. ● Configure the same pre-shared key as that of the peer. ● Configure the same IKE and IPsec parameters as those of the peer. ● Select IKE main mode or IKE aggressive mode for negotiation.

Scenario	Description
Site-to-Multisite	The peer device does not have a fixed IP address, and the local device is typically a hub site on a hub-spoke network.  Corporation Internet Hub (Local End) Spoke (Peer End) Spoke (Peer End) Key configurations: ● Configure any-to-any interesting traffic. ● Enable IPsec Reverse Route Injection (RRI). ● Select IKE auto mode for negotiation.

2 Configuration Examples of Site-to-Site IPsec VPN

2.1 Applicable Products and Versions

Table 2-1 Products and Versions

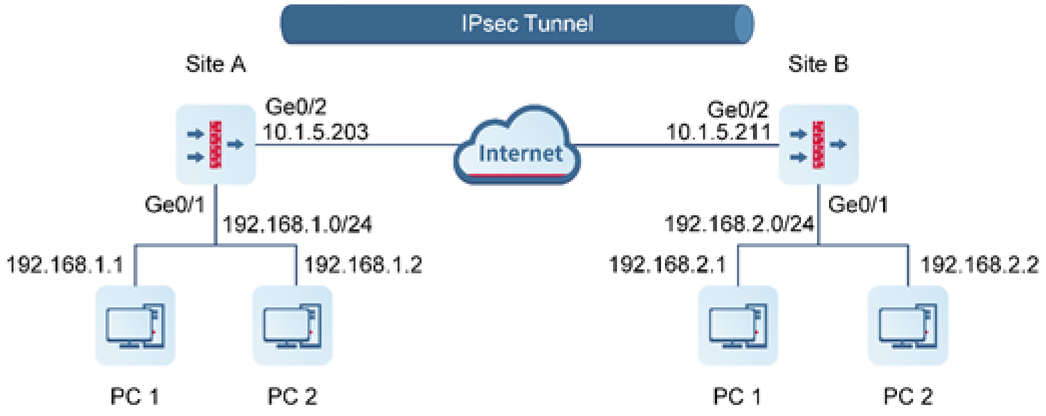
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

2.2 Service Demands

As shown in Figure 2-1, Site A and Site B at both ends have fixed public IP addresses. A site-to-site IPsec VPN tunnel needs to be established between the LANs of the two sites to achieve secure mutual access.

The authentication mode should be pre-shared key, and the encapsulation mode should be the tunnel mode. In this way, both ends can initiate connections.

Figure 2-1 Site-to-Site Networking



2.3 Restrictions and Guidelines

- Currently, the RG-WALL 1600-Z series firewall supports only the IPsec IKEv1 protocol for pre-shared key authentication and ESP tunnel mode for encapsulation.

2.4 Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following point during configuration:

- The IP addresses of Site A and Site B are fixed.

2.5 Procedure

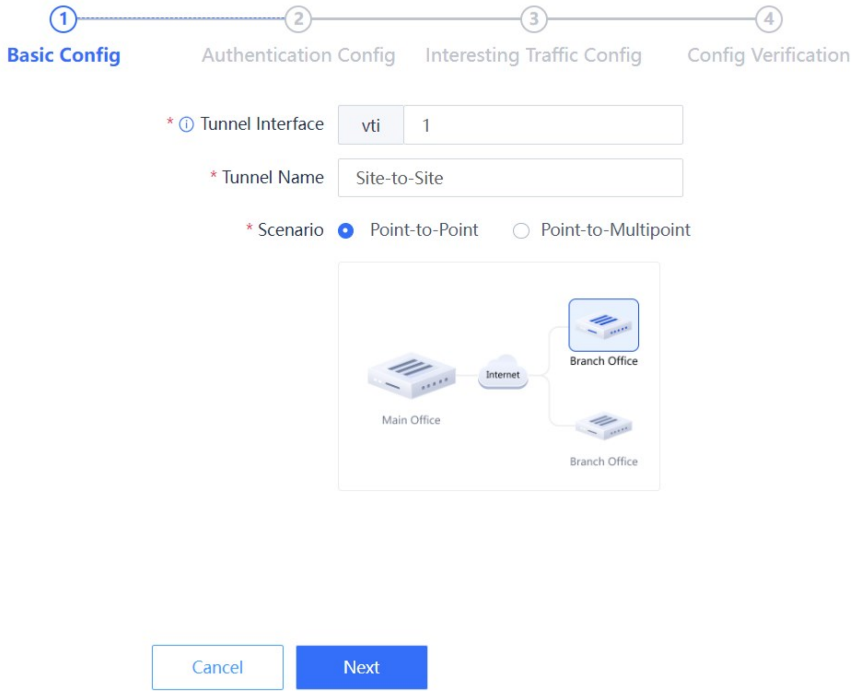
2.5.1 Using a Configuration Wizard

1. Configuring Site A

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 1

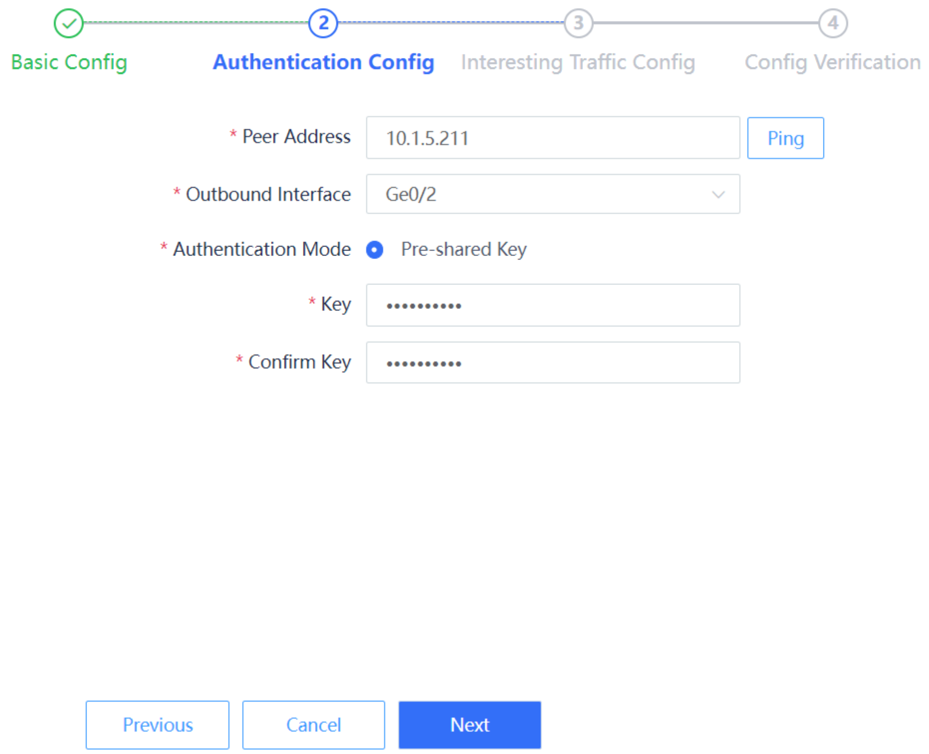
* Tunnel Name: Site-to-Site

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.



* Peer Address: 10.1.5.211

* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

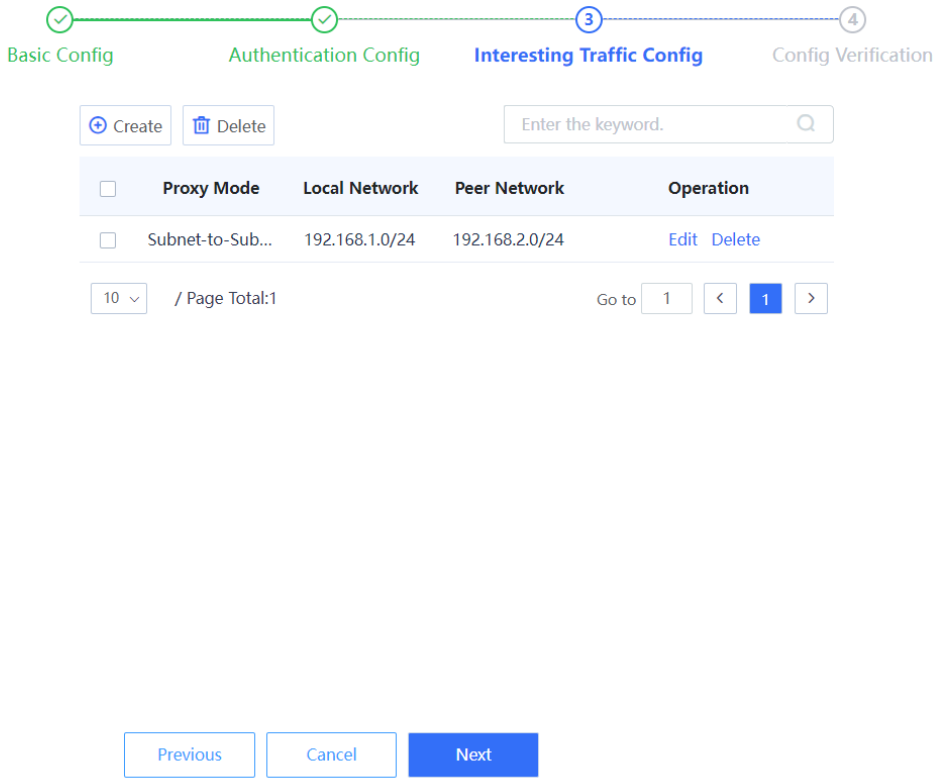
* Key: ••••••••••

* Confirm Key: ••••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

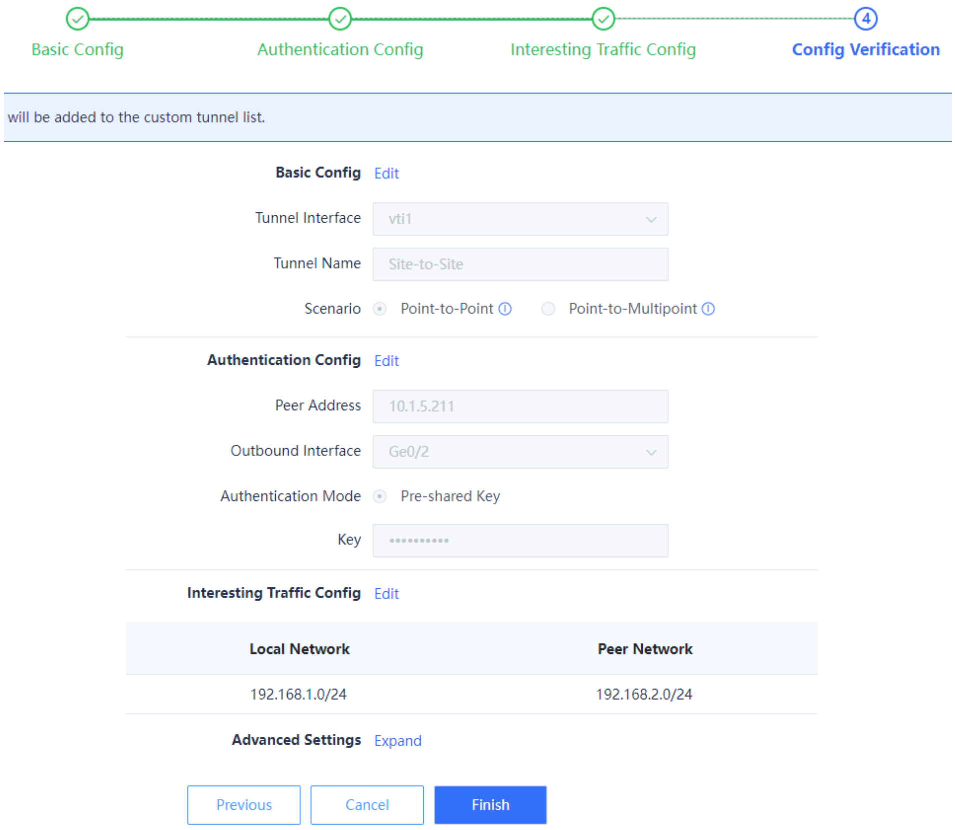


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Sub...	192.168.1.0/24	192.168.2.0/24	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti1

Tunnel Name: Site-to-Site

Scenario: ● Point-to-Point ○ Point-to-Multipoint

Authentication Config Edit

Peer Address: 10.1.5.211

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: ••••••••••

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

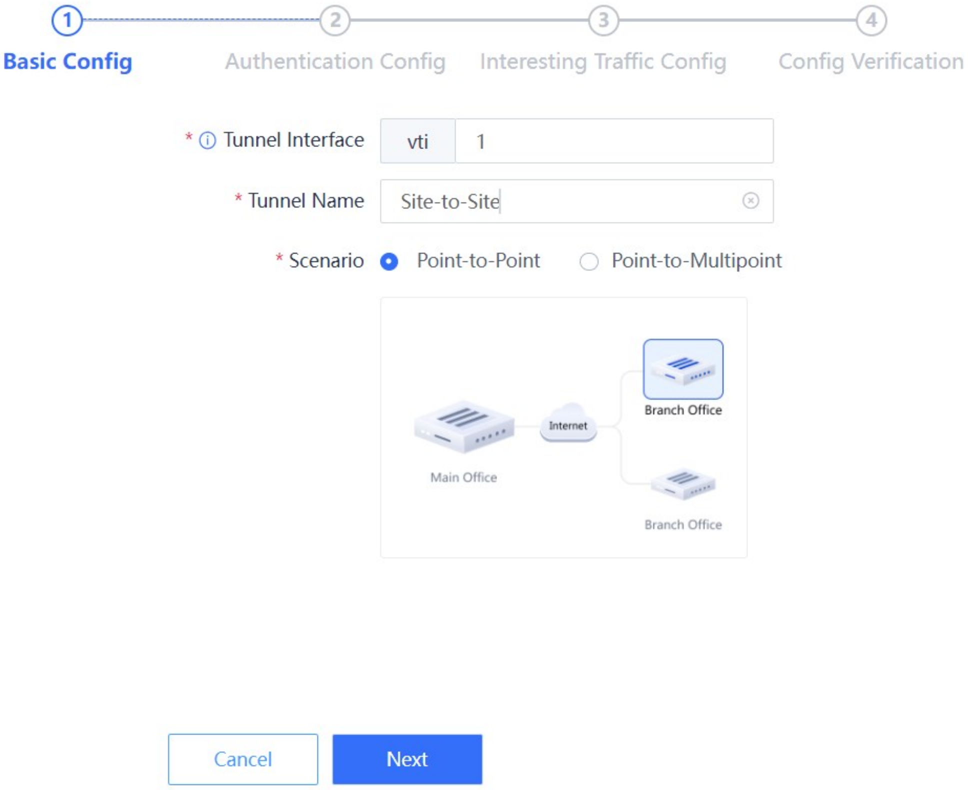
Advanced Settings Expand

2. Configuring Site B

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



* ⓘ Tunnel Interface: vti 1

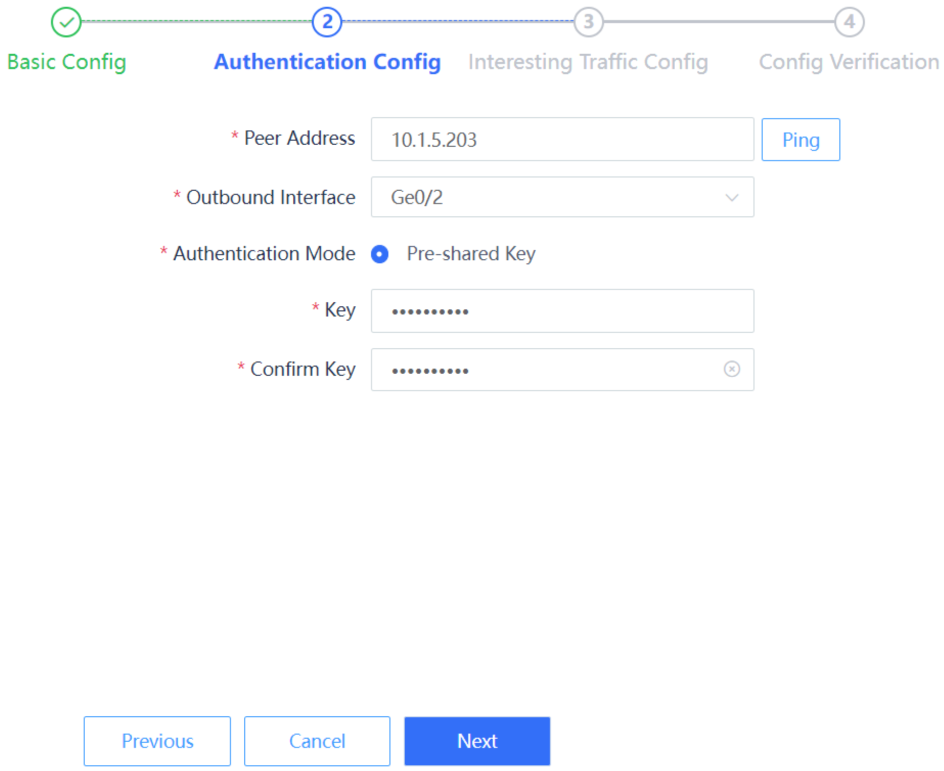
* Tunnel Name: Site-to-Site

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.



* Peer Address: 10.1.5.203

* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

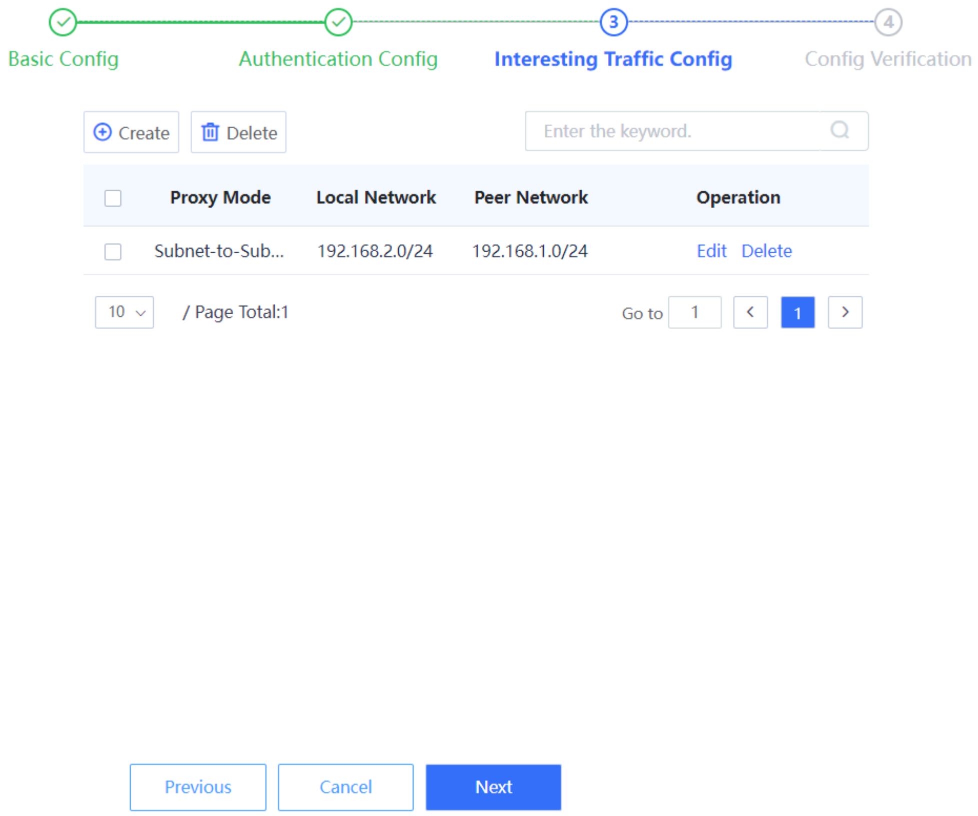
* Key: ••••••••••

* Confirm Key: ••••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

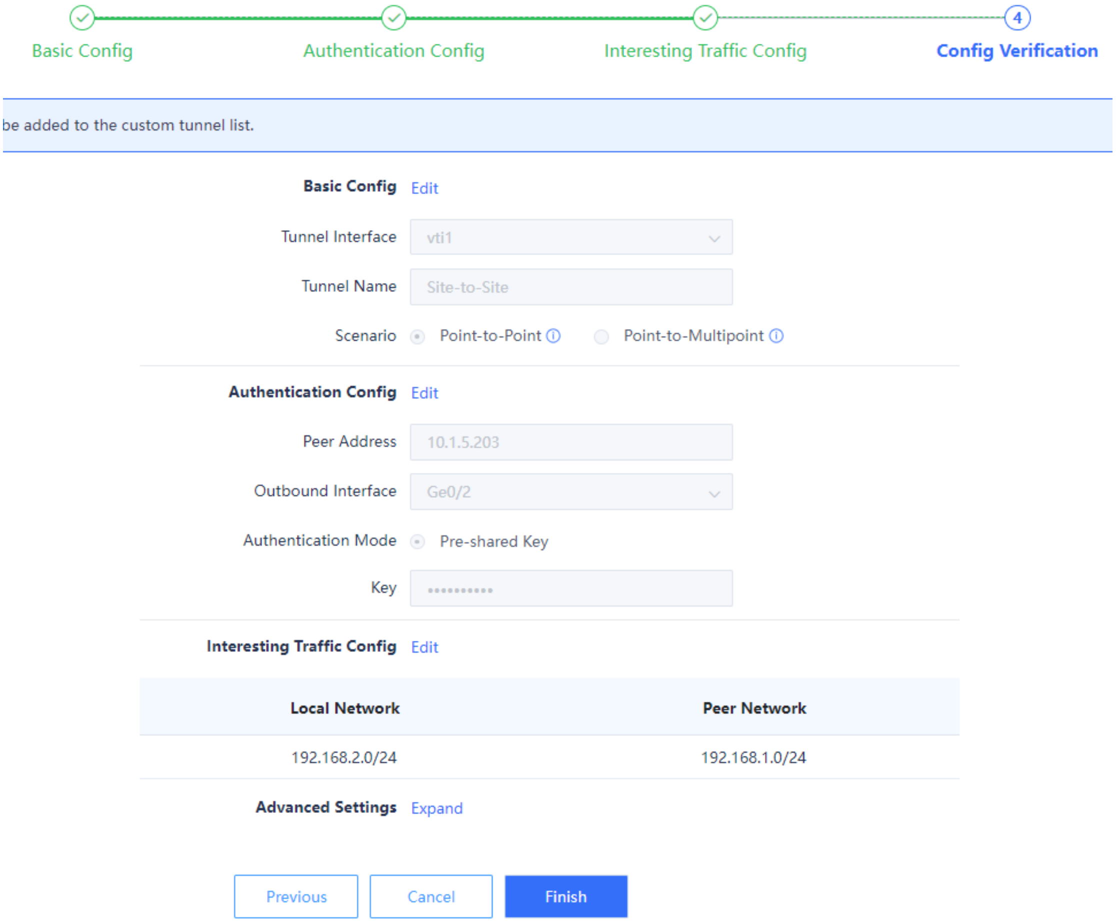


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Sub...	192.168.2.0/24	192.168.1.0/24	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti1

Tunnel Name: Site-to-Site

Scenario: ● Point-to-Point ○ Point-to-Multipoint

Authentication Config Edit

Peer Address: 10.1.5.203

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: ••••••••••

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.2.0/24	192.168.1.0/24

Advanced Settings Expand

2.5.2 Manually Configuring a Tunnel

1. Configuring Site A

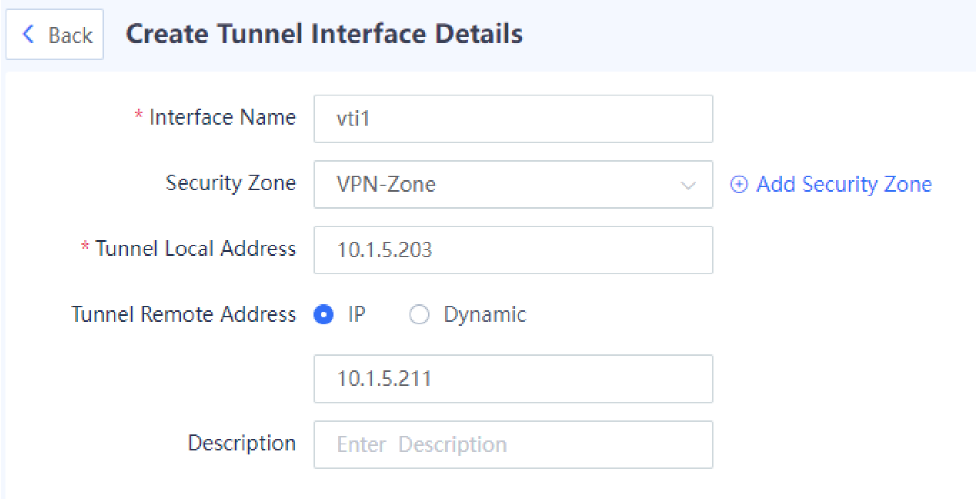
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **vti1**.
- Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
- Set **Tunnel Remote Address** to the default outbound interface address of Site B: 10.1.5.211.



< Back **Create Tunnel Interface Details**

* Interface Name: vti1

Security Zone: VPN-Zone

* Tunnel Local Address: 10.1.5.203

Tunnel Remote Address: ● IP ○ Dynamic

10.1.5.211

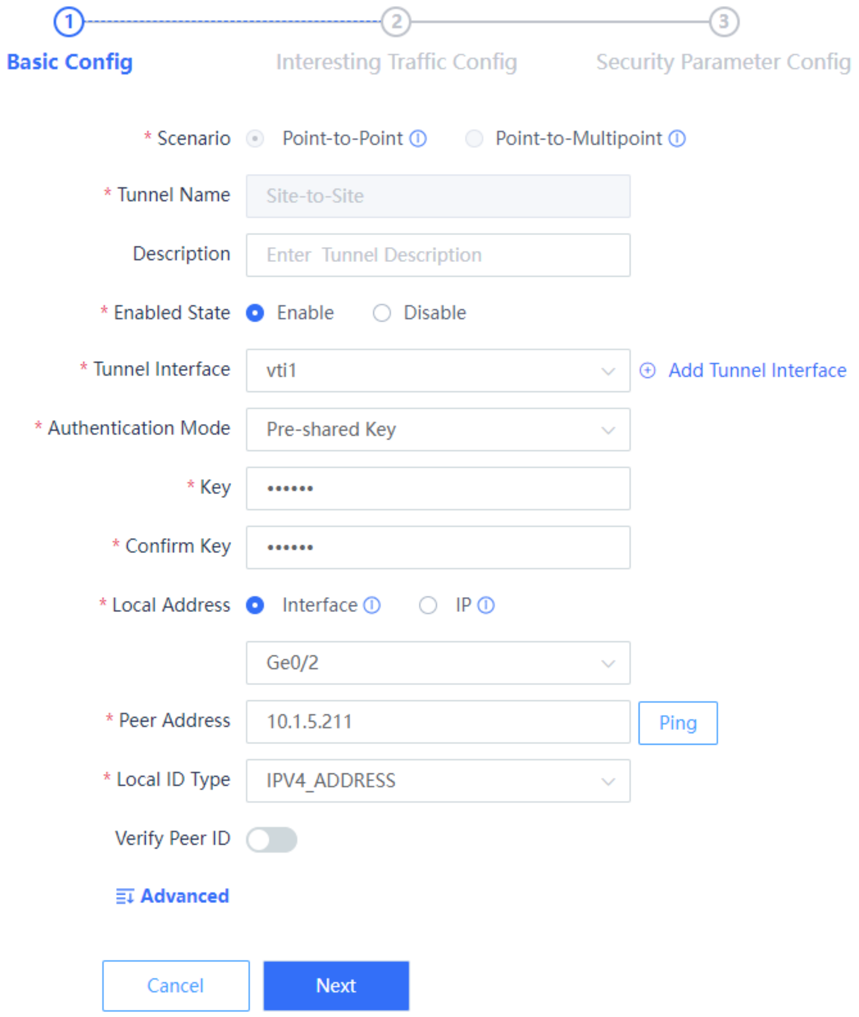
Description: Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **Site-to-Site**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **vti1**. Set **Local Address** to interface Ge0/2, and **Peer Address** to 10.1.5.211.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.



* Scenario ● Point-to-Point ○ Point-to-Multipoint

* Tunnel Name: Site-to-Site

Description: Enter Tunnel Description

* Enabled State ● Enable ○ Disable

* Tunnel Interface: vti1 — Add Tunnel Interface

* Authentication Mode: Pre-shared Key

* Key: ••••••

* Confirm Key: ••••••

* Local Address ● Interface ○ IP

Ge0/2

* Peer Address: 10.1.5.211 Ping

* Local ID Type: IPV4_ADDRESS

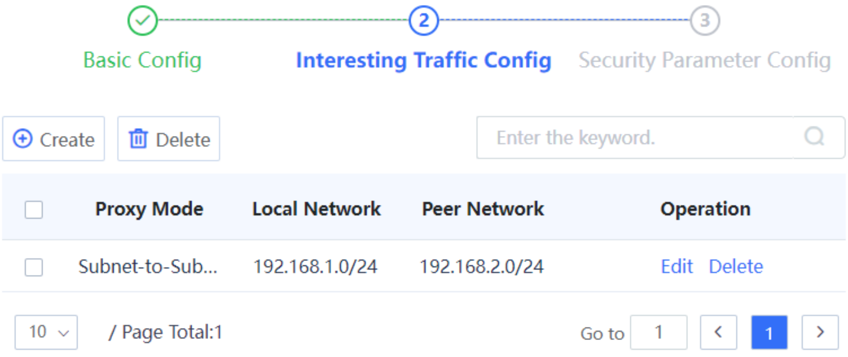
Verify Peer ID: ○

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set **Local Network** to 192.168.1.0/24 and **Peer Network** to 192.168.2.0/24.



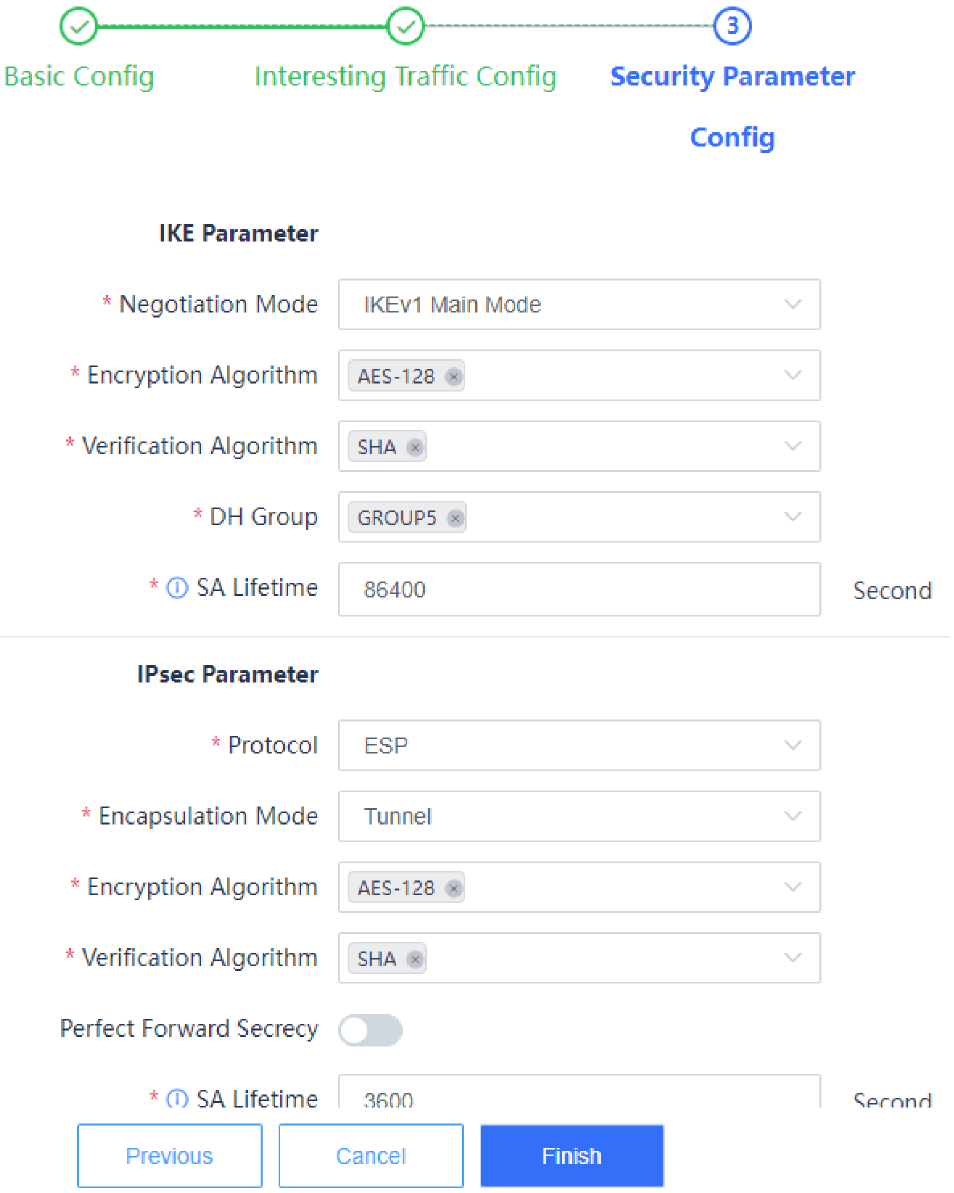
□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Sub...	192.168.1.0/24	192.168.2.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode: IKEv1 Main Mode
* Encryption Algorithm: AES-128
* Verification Algorithm: SHA
* DH Group: GROUP5
* SA Lifetime: 86400 Second

IPsec Parameter

* Protocol: ESP
* Encapsulation Mode: Tunnel
* Encryption Algorithm: AES-128
* Verification Algorithm: SHA

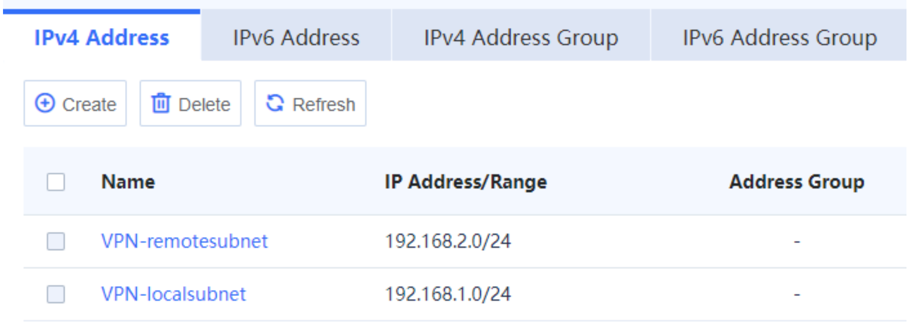
Perfect Forward Secrecy: ○

* SA Lifetime: 3600 Second

Click **Finish** to complete the configuration for the IPsec tunnel.

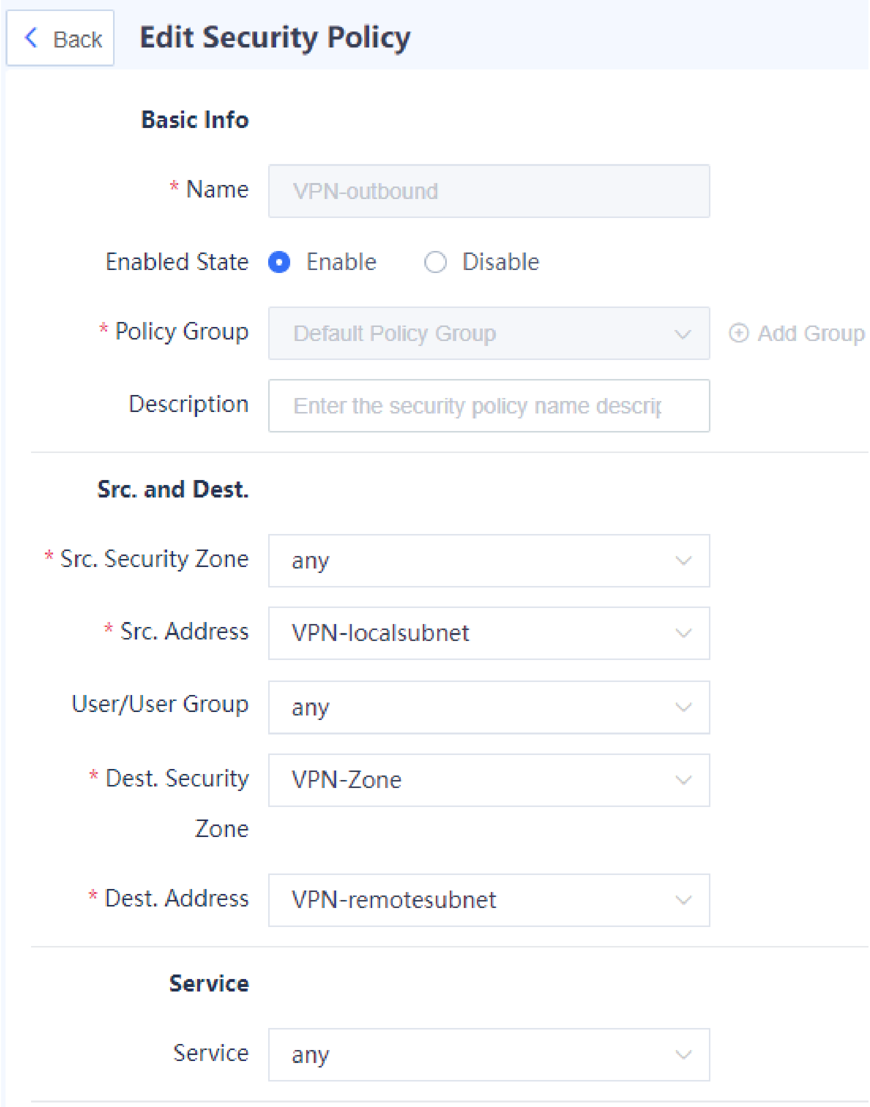
(3) Create security policies.

a Choose **Object** > **Address** > **IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.1.0/24 and peer network 192.168.2.0/24 of the interesting traffic separately.



□	Name	IP Address/Range	Address Group
□	VPN-remotesubnet	192.168.2.0/24	-
□	VPN-localsubnet	192.168.1.0/24	-

b Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.



Edit Security Policy

Basic Info

* Name: VPN-outbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: any

* Src. Address: VPN-localsubnet

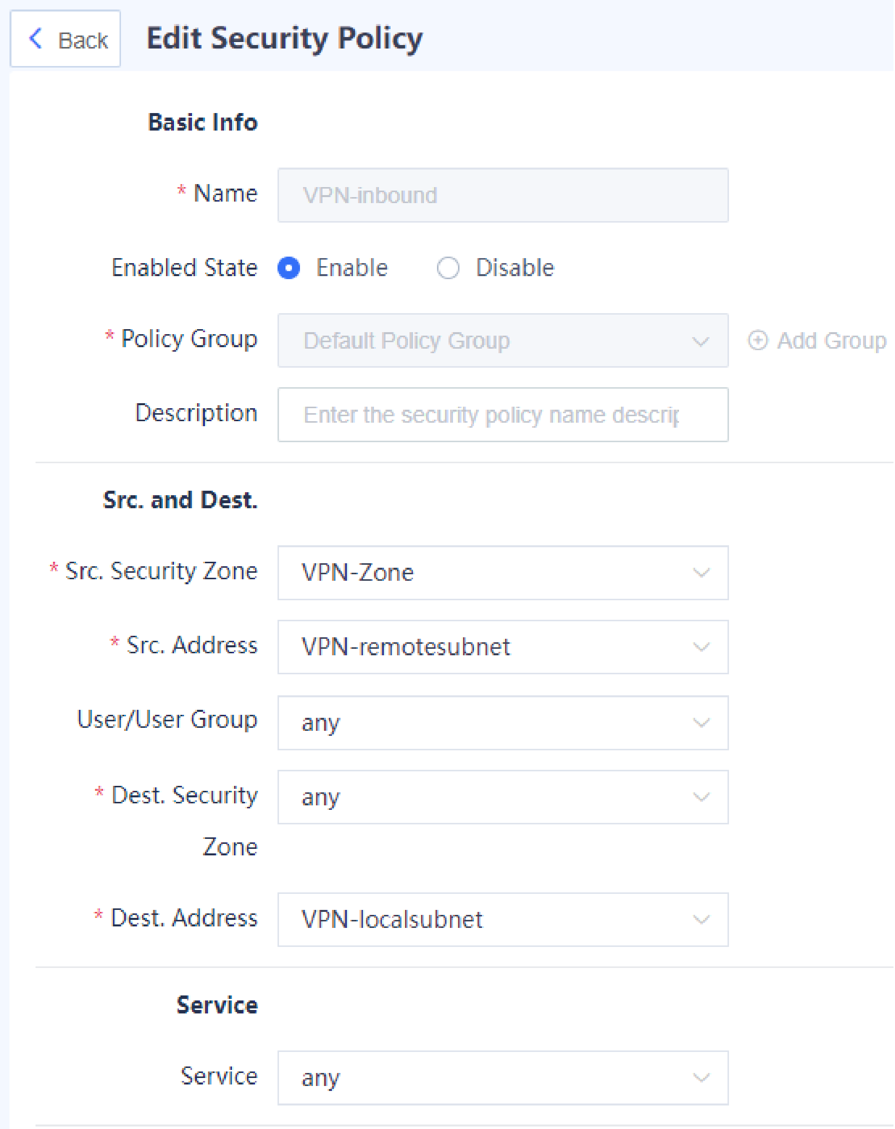
User/User Group: any

* Dest. Security Zone: VPN-Zone

* Dest. Address: VPN-remotesubnet

Service

Service: any



< Back **Edit Security Policy**

Basic Info

* Name: VPN-inbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: VPN-Zone

* Src. Address: VPN-remotesubnet

User/User Group: any

* Dest. Security Zone: any

* Dest. Address: VPN-localsubnet

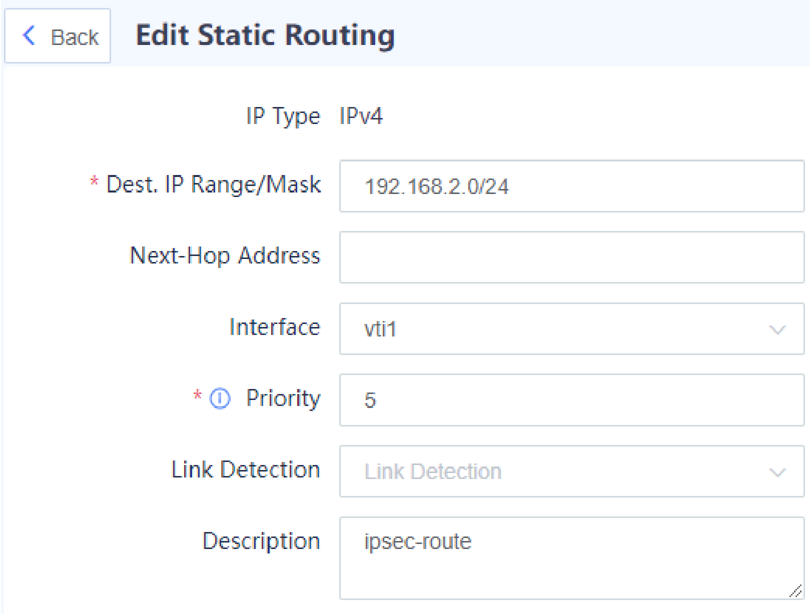
Service

Service: any

(4) Configure a static route.

a Choose **Network** > **Routing** > **Static Routing** > **IPv4**.

b Click **Create** and create a static route to the peer protected subnet of the VPN.



Back **Edit Static Routing**

IP Type IPv4

* Dest. IP Range/Mask 192.168.2.0/24

Next-Hop Address

Interface vti1

* ⓘ Priority 5

Link Detection Link Detection

Description ipsec-route

2. Configuring Site B

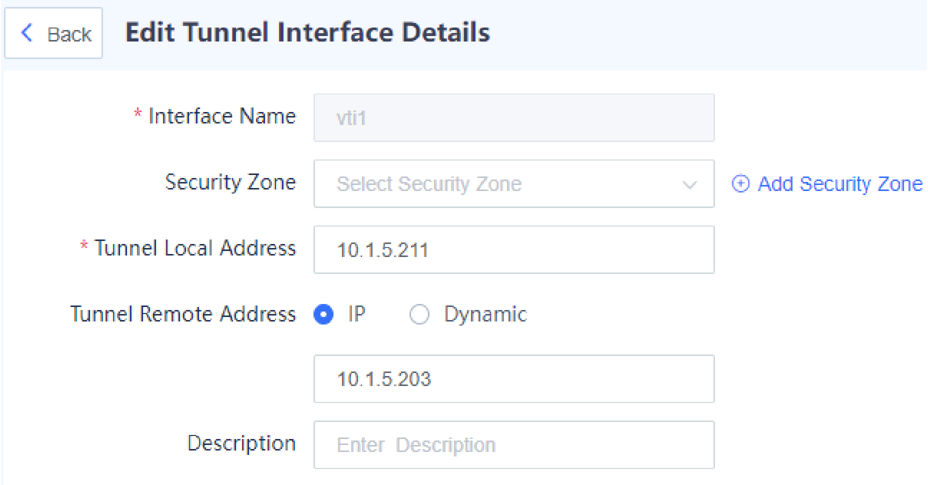
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **vti1**.
- Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of Site B: 10.1.5.211.
- Set **Tunnel Remote Address** to the default outbound interface address of Site A: 10.1.5.203.



Back **Edit Tunnel Interface Details**

* Interface Name vti1

Security Zone Select Security Zone ⊕ Add Security Zone

* Tunnel Local Address 10.1.5.211

Tunnel Remote Address ● IP ○ Dynamic

10.1.5.203

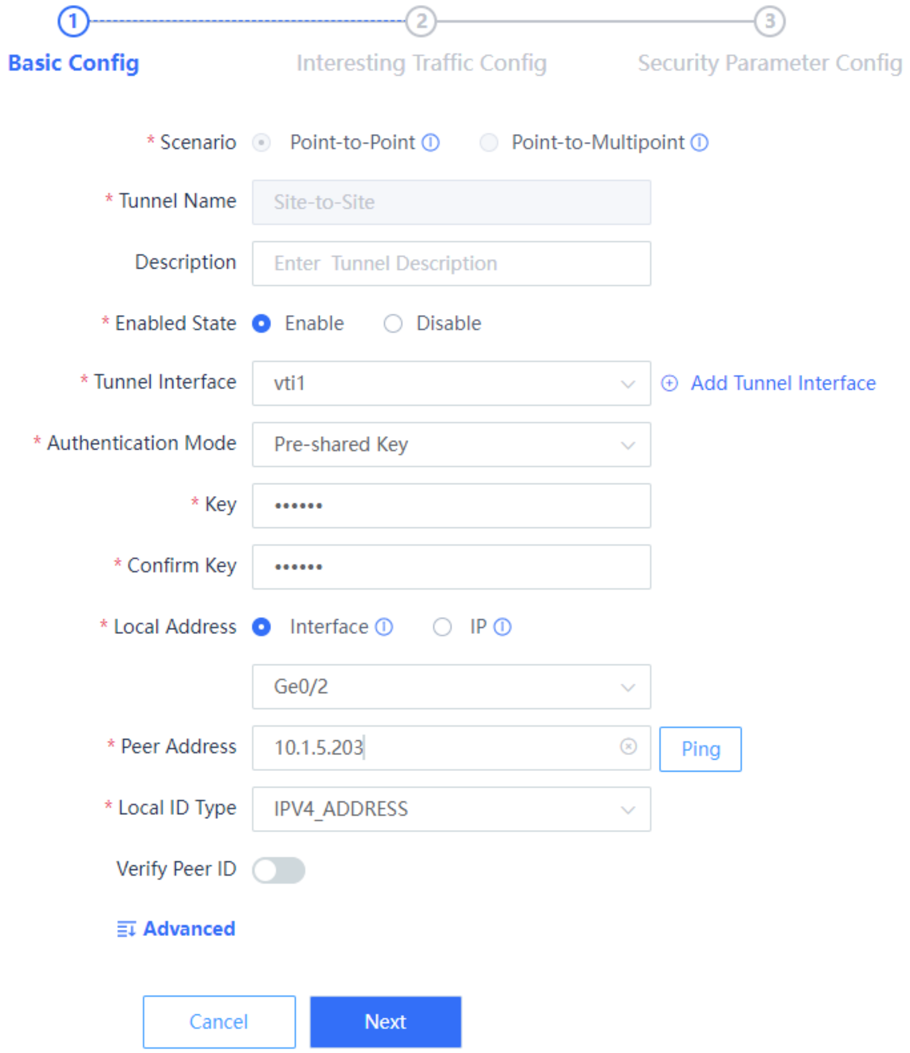
Description Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **Site-to-Site**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **vti1**. Set **Local Address** to interface Ge0/2, and **Peer Address** to 10.1.5.203.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.



* Scenario ● Point-to-Point ○ Point-to-Multipoint

* Tunnel Name: Site-to-Site

Description: Enter Tunnel Description

* Enabled State ● Enable ○ Disable

* Tunnel Interface: vti1

* Authentication Mode: Pre-shared Key

* Key: ••••••

* Confirm Key: ••••••

* Local Address ● Interface ○ IP

Ge0/2

* Peer Address: 10.1.5.203

* Local ID Type: IPV4_ADDRESS

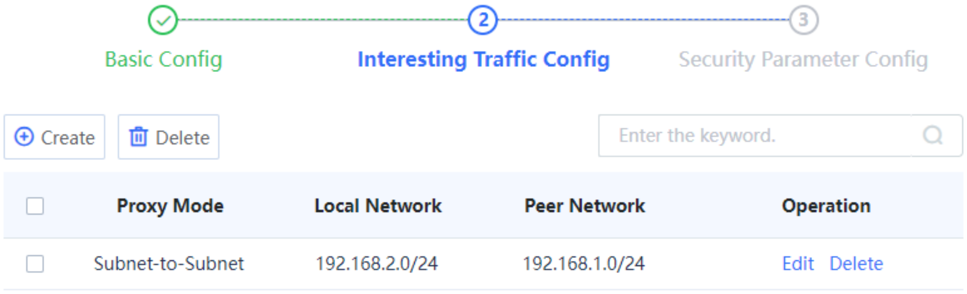
Verify Peer ID

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set **Local Network** to 192.168.2.0/24 and **Peer Network** to 192.168.1.0/24.



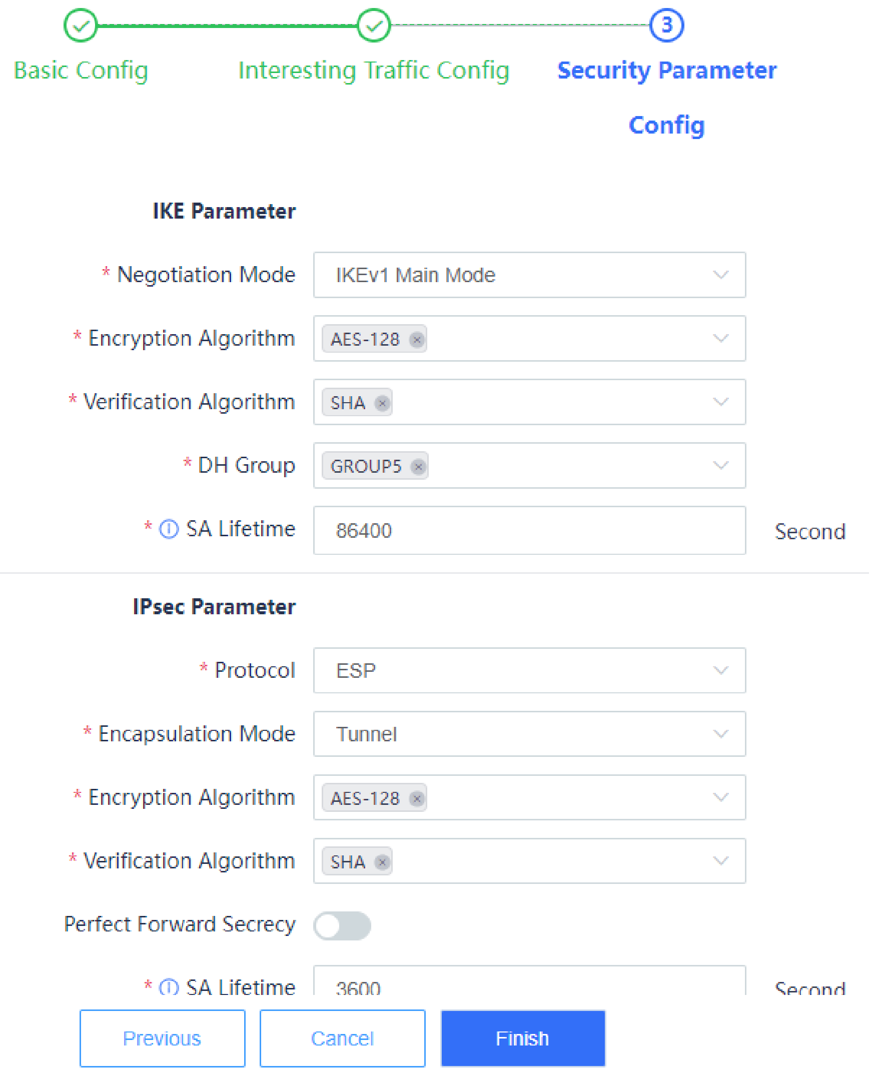
□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	192.168.2.0/24	192.168.1.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode: IKEv1 Main Mode

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 86400 Second

IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

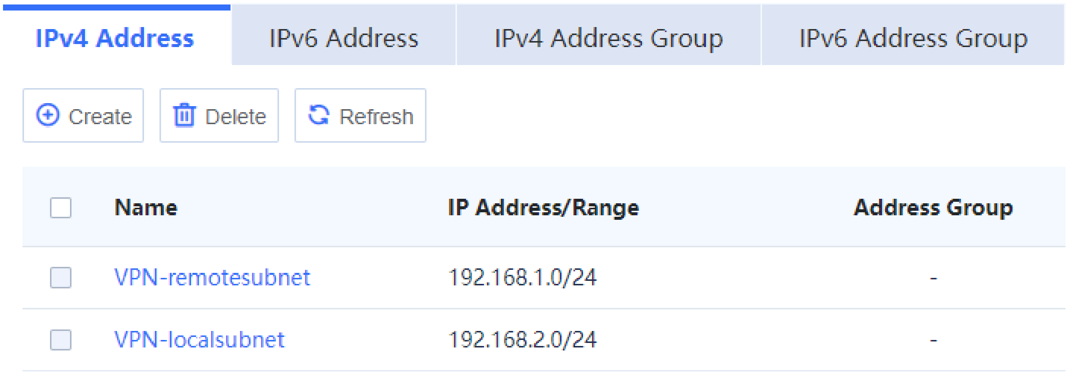
Perfect Forward Secrecy: ○

* SA Lifetime: 3600 Second

Click **Finish** to complete the configuration for the IPsec tunnel.

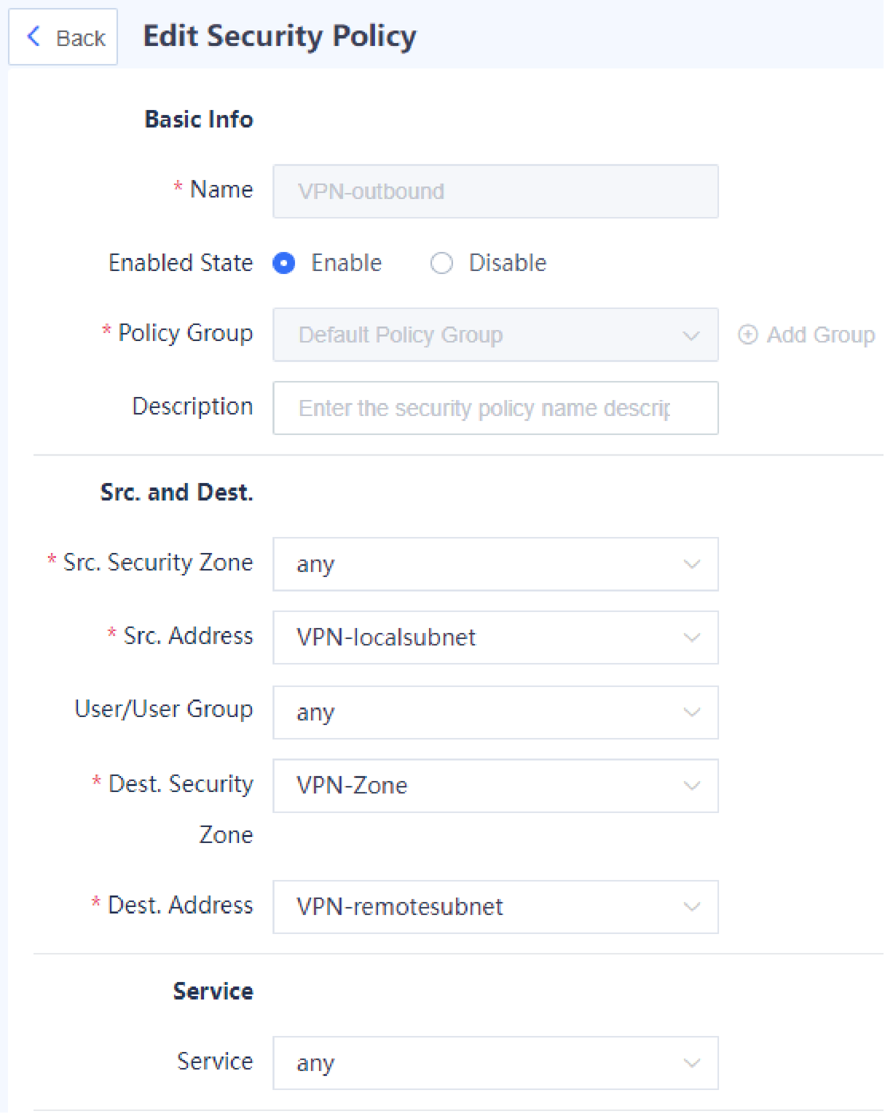
(3) Create security policies.

a Choose **Object** > **Address** > **IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.2.0/24 and peer network 192.168.1.0/24 of the interesting traffic separately.



□	Name	IP Address/Range	Address Group
□	VPN-remotesubnet	192.168.1.0/24	-
□	VPN-localsubnet	192.168.2.0/24	-

b Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.



Edit Security Policy

Basic Info

* Name: VPN-outbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: any

* Src. Address: VPN-localsubnet

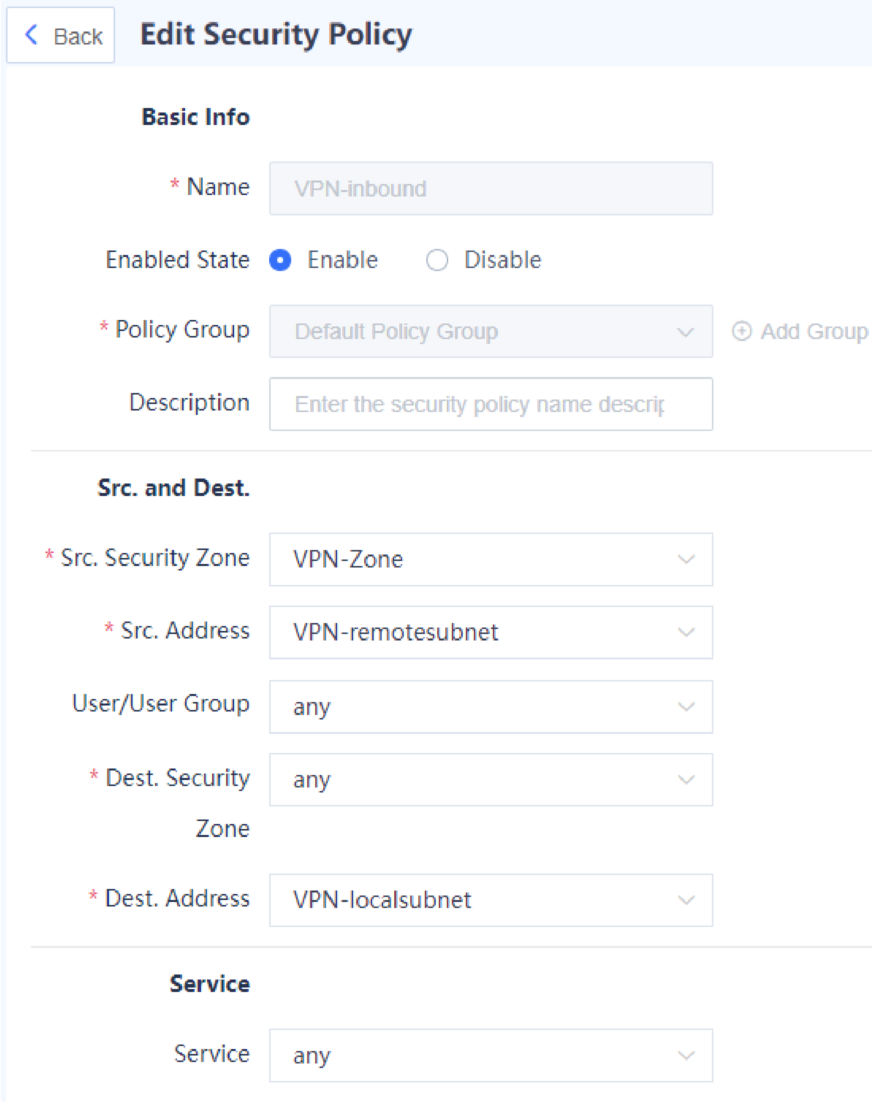
User/User Group: any

* Dest. Security Zone: VPN-Zone

* Dest. Address: VPN-remotesubnet

Service

Service: any



< Back **Edit Security Policy**

Basic Info

* Name: VPN-inbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: VPN-Zone

* Src. Address: VPN-remotesubnet

User/User Group: any

* Dest. Security Zone: any

* Dest. Address: VPN-localsubnet

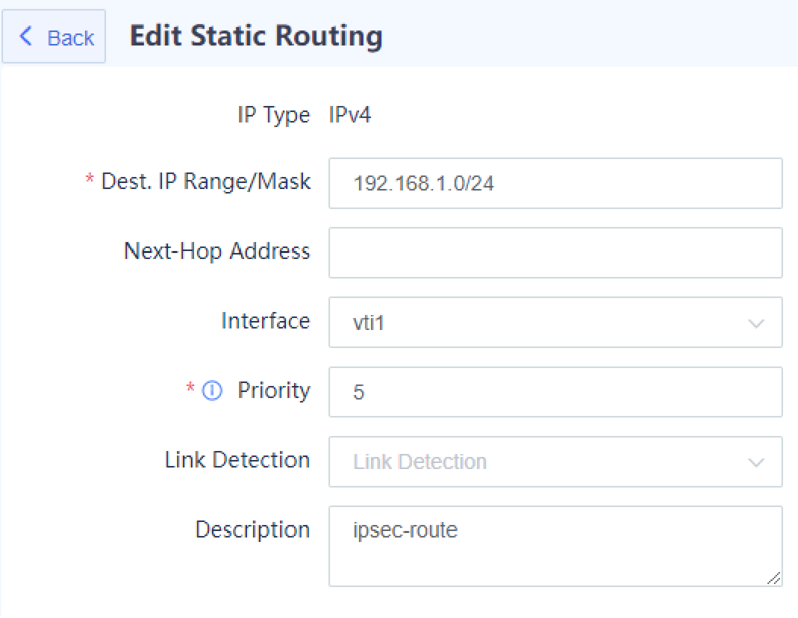
Service

Service: any

(4) Configure a static route.

a Choose **Network** > **Routing** > **Static Routing** > **IPv4**.

b Click **Create** and create a static route to the peer protected subnet of the VPN.



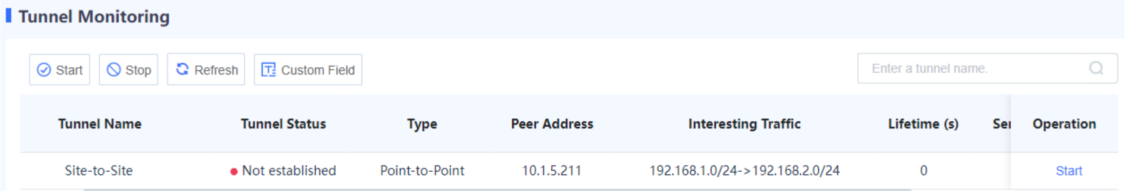
Edit Static Routing

IP Type	IPv4
* Dest. IP Range/Mask	192.168.1.0/24
Next-Hop Address	
Interface	vti1
* Priority	5
Link Detection	Link Detection
Description	ipsec-route

2.6 Verification

2.6.1 Verifying Configuration of Site A

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.

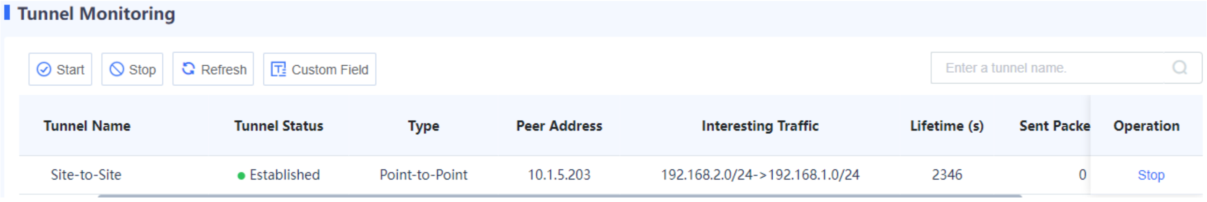


Tunnel Monitoring

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Se	Operation
Site-to-Site	● Not established	Point-to-Point	10.1.5.211	192.168.1.0/24->192.168.2.0/24	0		Start

2.6.2 Verifying Configuration of Site B

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.



Tunnel Monitoring

Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packe	Operation
Site-to-Site	● Established	Point-to-Point	10.1.5.203	192.168.2.0/24->192.168.1.0/24	2346	0	Stop

3 Configuration Examples of Site-to-Site IPsec VPN (Interconnection with Fortinet Firewall)

3.1 Applicable Products and Versions

Table 3-1 Products and Versions

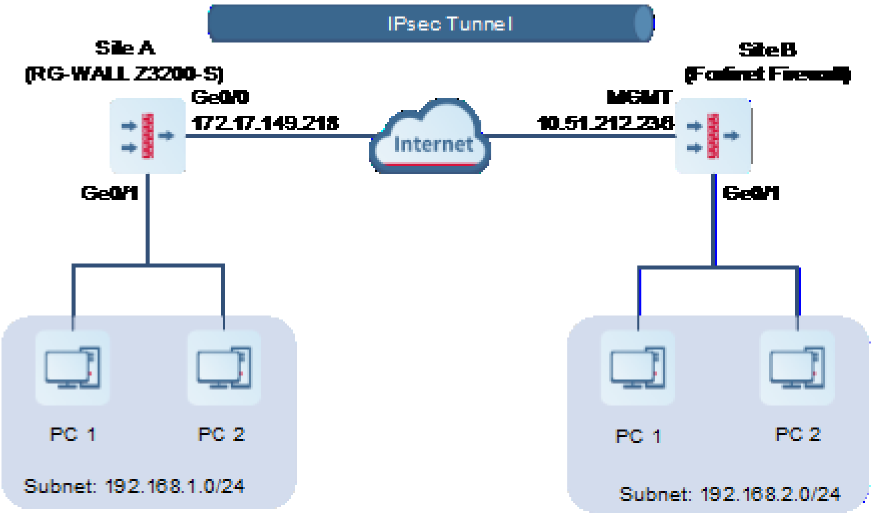
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later
Firewall	FortiGate 100F	FortiOS 7.2.4 Build 1396 (Feature)

3.2 Service Demands

As shown in Figure 3-1, Site A (RG-WALL Z3200-S) and Site B (Fortinet firewall) at both ends have fixed public IP addresses. A site-to-site IPsec VPN tunnel needs to be established between the LANs of the two sites to achieve secure mutual access.

The authentication mode should be pre-shared key, and the encapsulation mode should be the tunnel mode. In this way, both ends can initiate connections.

Figure 3-1 Site-to-Site Networking



3.3 Restrictions and Guidelines

Currently, the IPsec VPN function of the RG-WALL 1600-Z series firewall supports only the IKEv1 protocol for pre-shared key authentication and ESP tunnel mode for encapsulation.

3.4 Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- Ensure that the IP addresses of Site A and Site B are fixed.

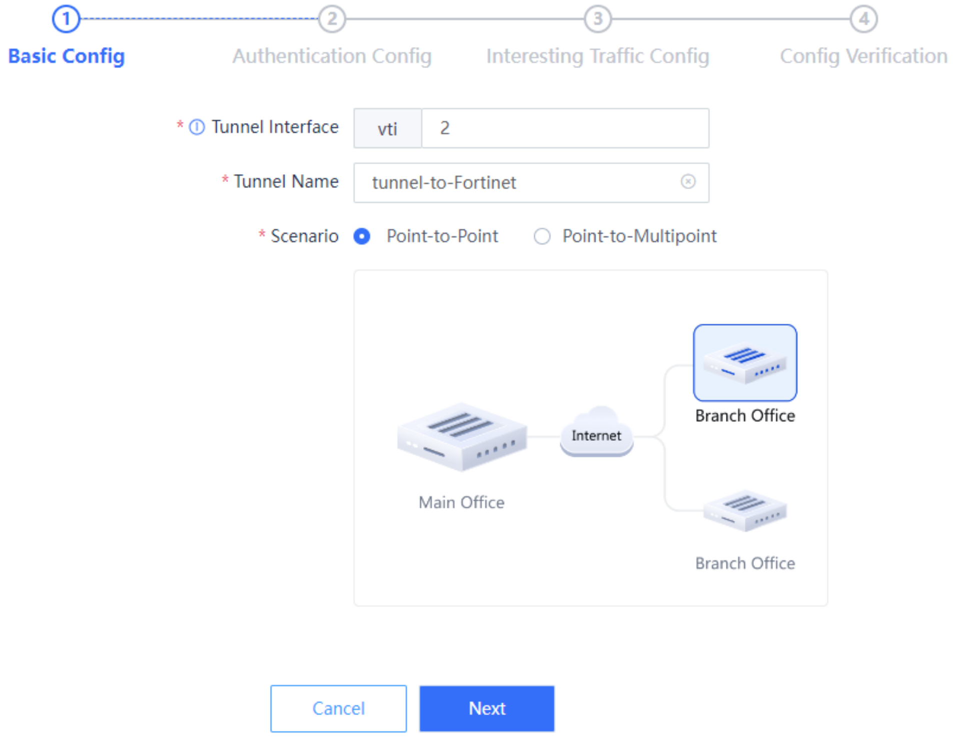
3.5 Procedure

3.5.1 Configuring Site A (RG-WALL 1600-Z3200-S)

1. Basic Configuration

(1) Log in to the RG-WALL 1600-Z3200-S firewall and choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 2

* Tunnel Name: tunnel-to-Fortinet

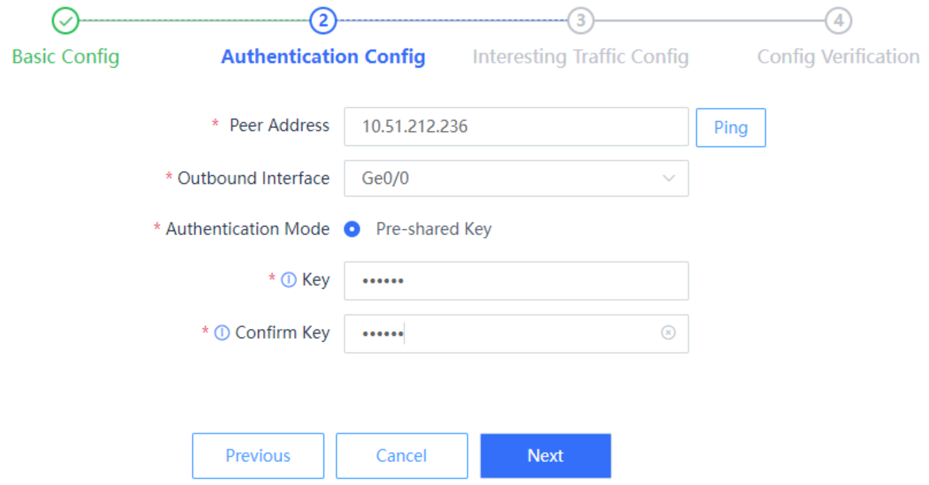
* Scenario: ● Point-to-Point ○ Point-to-Multipoint

(3) After completing the configuration, click **Next**.

2. Authentication Configuration

(1) Configure parameters as follows:

- Set the peer address to the IP address of the Fortinet firewall's WAN interface (10.51.212.236).
- Set the outbound interface to that of the local device (Ge0/0).
- Set the authentication mode to pre-shared key, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



* Peer Address: 10.51.212.236

* Outbound Interface: Ge0/0

* Authentication Mode: ● Pre-shared Key

* Key: ••••••

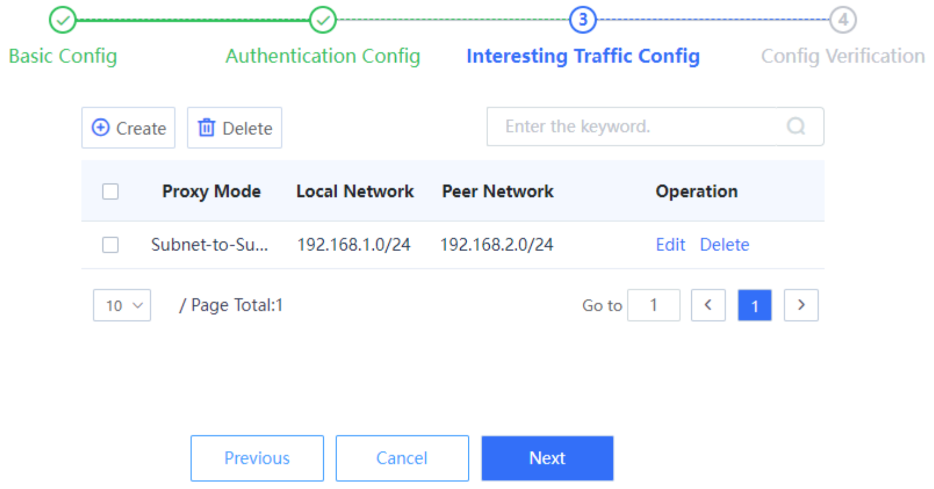
* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Interesting Traffic Configuration

(1) Click **Create**. Configure parameters for interesting traffic as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set the local network to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.
- Set the peer network to the subnet 192.168.2.0/24 of the Fortinet firewall.

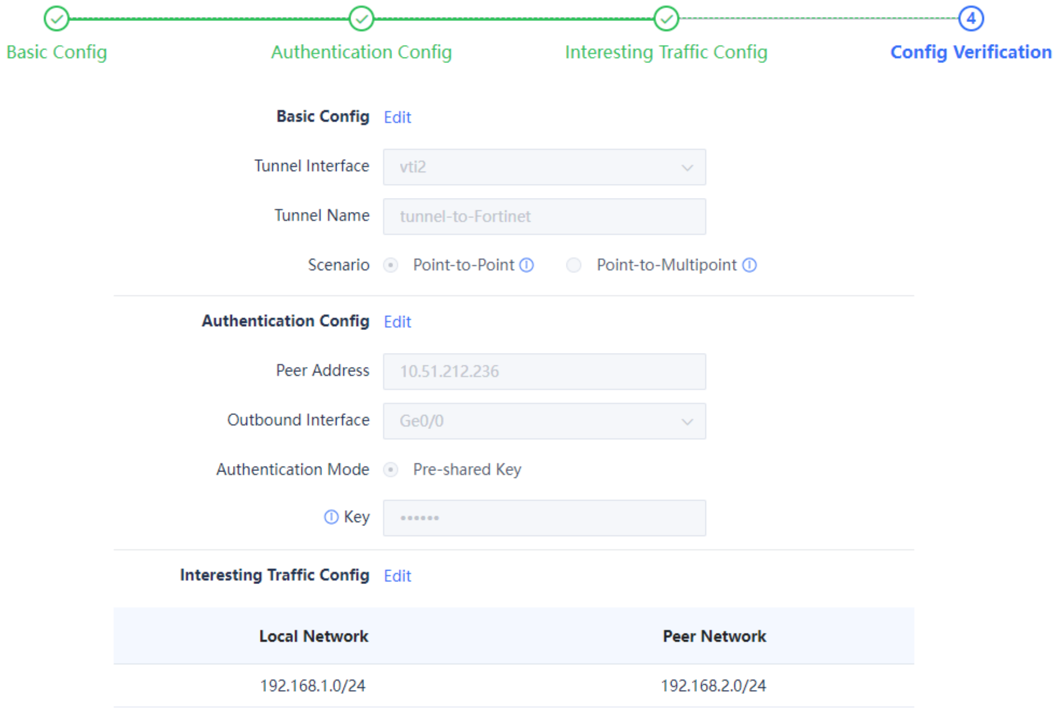


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Su...	192.168.1.0/24	192.168.2.0/24	Edit Delete

(2) After completing the configuration, click **Next**.

4. Verification

(1) Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.



Basic Config Edit

Tunnel Interface: vti2

Tunnel Name: tunnel-to-Fortinet

Scenario: ● Point-to-Point ⓘ ○ Point-to-Multipoint ⓘ

Authentication Config Edit

Peer Address: 10.51.212.236

Outbound Interface: Ge0/0

Authentication Mode: ● Pre-shared Key

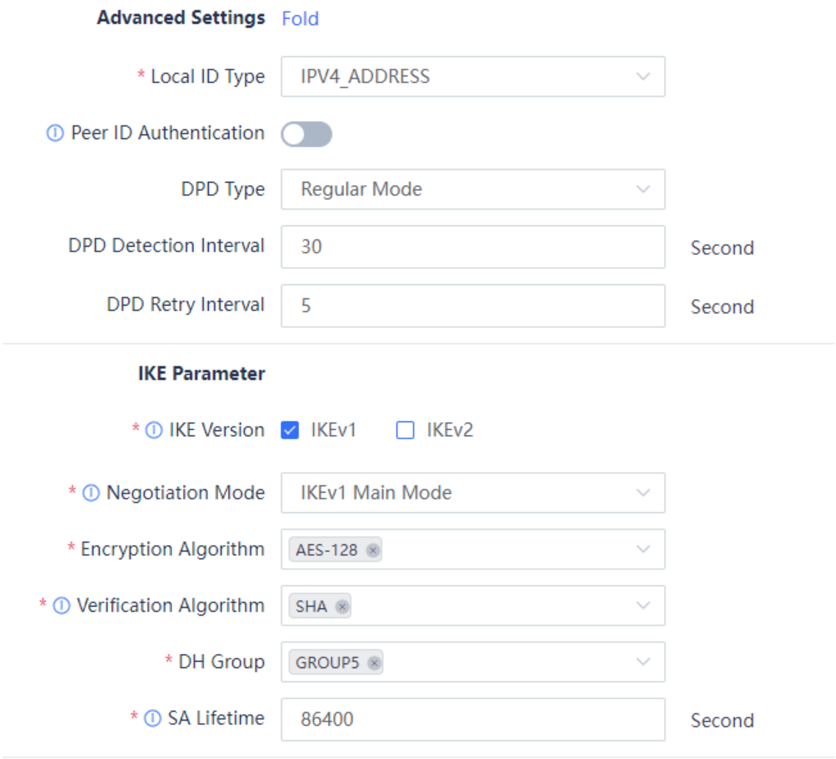
ⓘ Key: ••••••

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

(2) Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.

- IKE parameters:
  - Set **IKE Version** to **IKEv1**.
  - Set **Negotiation Mode** to **IKEv1 Main Mode**.
  - Set **Encryption Algorithm** to **AES-128**.
  - Set **Verification Algorithm** to **SHA**.
  - Set **DH Group** to **GROUP5**.



Advanced Settings Fold

* Local ID Type: IPV4_ADDRESS

Peer ID Authentication: off

DPD Type: Regular Mode

DPD Detection Interval: 30 Second

DPD Retry Interval: 5 Second

IKE Parameter

* IKE Version: ☑ IKEv1 □ IKEv2

* Negotiation Mode: IKEv1 Main Mode

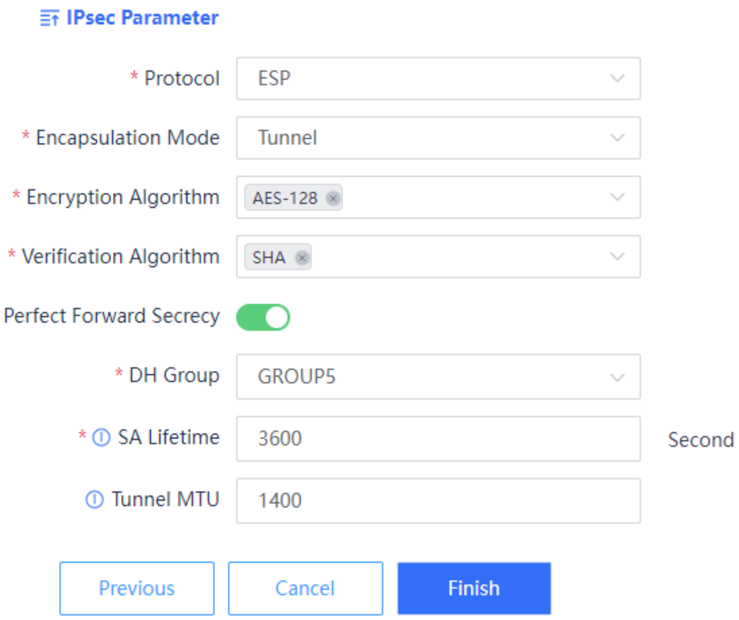
* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 86400 Second

- IPsec parameters:
  - Set **Encryption Algorithm** to **AES-128**.
  - Set **Verification Algorithm** to **SHA**.
  - Enable **Perfect Forward Secrecy**.
  - Set **DH Group** to **GROUP5**.



IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

Perfect Forward Secrecy: on

* DH Group: GROUP5

* SA Lifetime: 3600 Second

Tunnel MTU: 1400

(3) After verifying the configuration, click **Finish**.

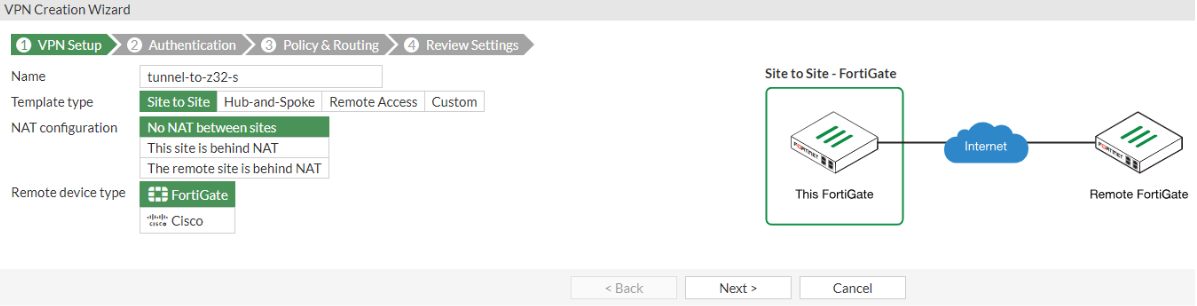
3.5.2 Configuring Site B (Fortinet Firewall)

1. VPN Setup

(1) Log in to the Fortinet firewall and choose **VPN** > **IPsec Wizard**. The configuration wizard page is displayed.

(2) Configure parameters as follows:

- Set **Template type** to **Site to Site**.
- Set **NAT configuration** to **No NAT between sites**.
- For the device type, use the default configuration.



VPN Creation Wizard

Name: tunnel-to-z32-s

Template type: **Site to Site** | Hub-and-Spoke | Remote Access | Custom

NAT configuration: **No NAT between sites** | This site is behind NAT | The remote site is behind NAT

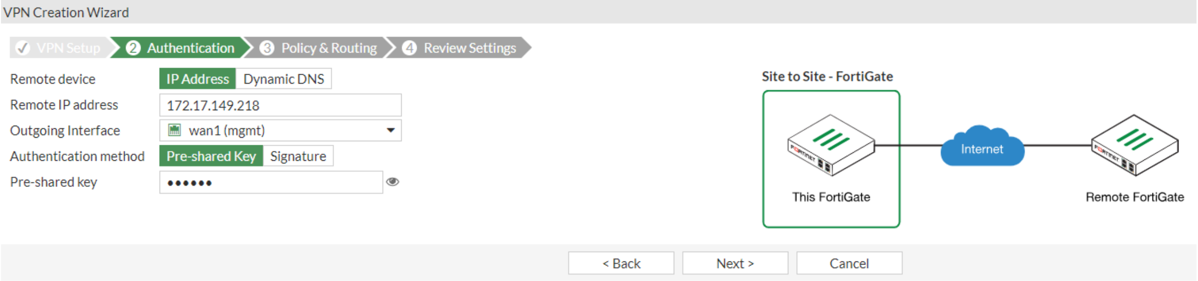
Remote device type: **FortiGate** | Cisco

(3) After completing the configuration, click **Next**.

2. Authentication Configuration

(1) Configure parameters as follows:

- Set **Remote device** to **IP Address**.
- Set **Remote IP address** to the IP address of the RG-WALL Z3200-S (172.17.149.218).
- Set **Outgoing interface** to that of the local device: **wan1(mgmt)**.
- Set **Authentication method** to **Pre-shared Key**, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



VPN Creation Wizard

Remote device: **IP Address** | Dynamic DNS

Remote IP address: 172.17.149.218

Outgoing Interface: wan1 (mgmt)

Authentication method: **Pre-shared Key** | Signature

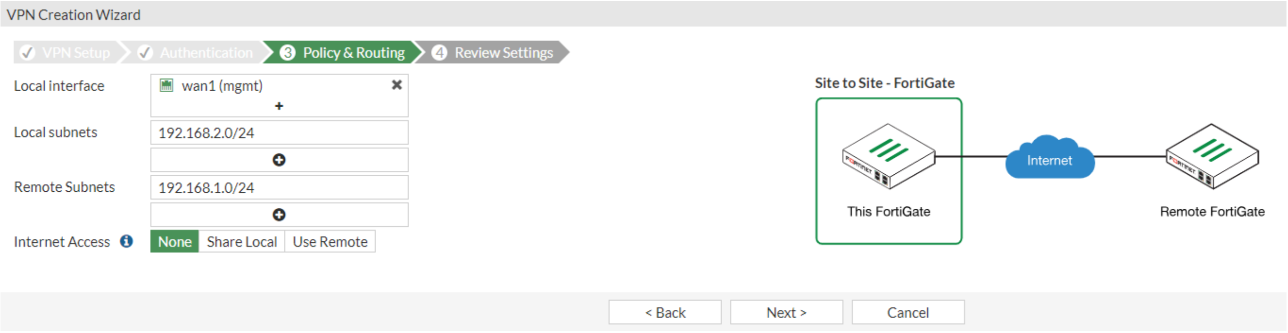
Pre-shared key: ••••••

(2) After completing the configuration, click **Next**.

3. Policy and Route Configuration

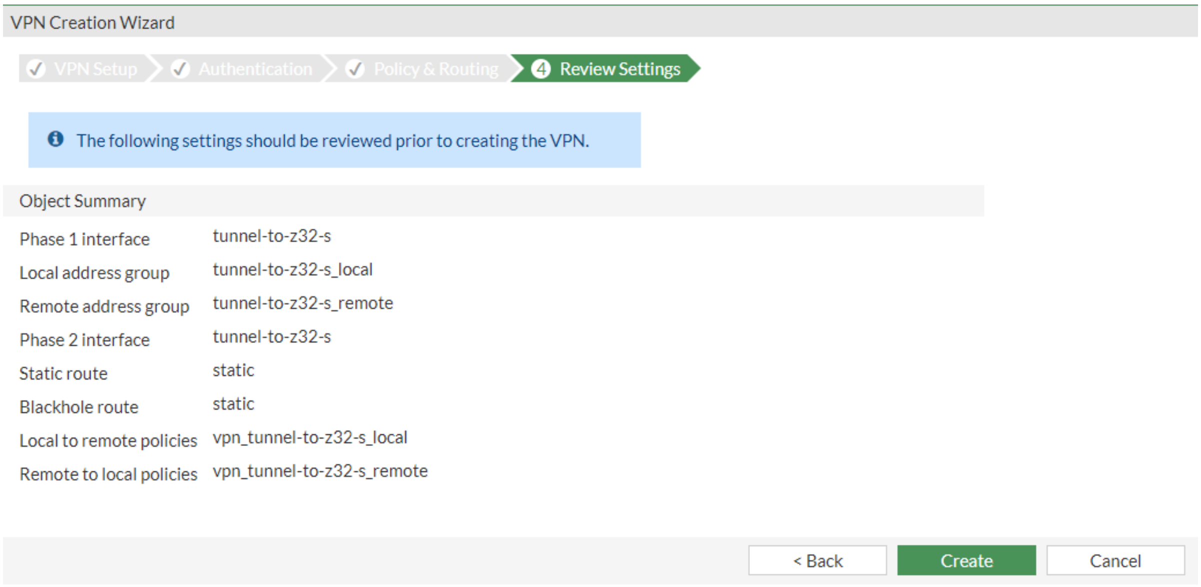
(1) Configure policy and route parameters as follows:

- Set **Local interface** to the outbound interface **wan1(mgmt)** of the local device.
- Set **Local subnets** to the subnet 192.168.2.0/24 of the Fortinet firewall.
- Set **Remote subnets** to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.



Local interface	wan1 (mgmt)
Local subnets	192.168.2.0/24
Remote Subnets	192.168.1.0/24
Internet Access	[✓ None] Share Local Use Remote

(2) After completing the configuration, click **Next**. The **Review Settings** page is displayed.



The following settings should be reviewed prior to creating the VPN.

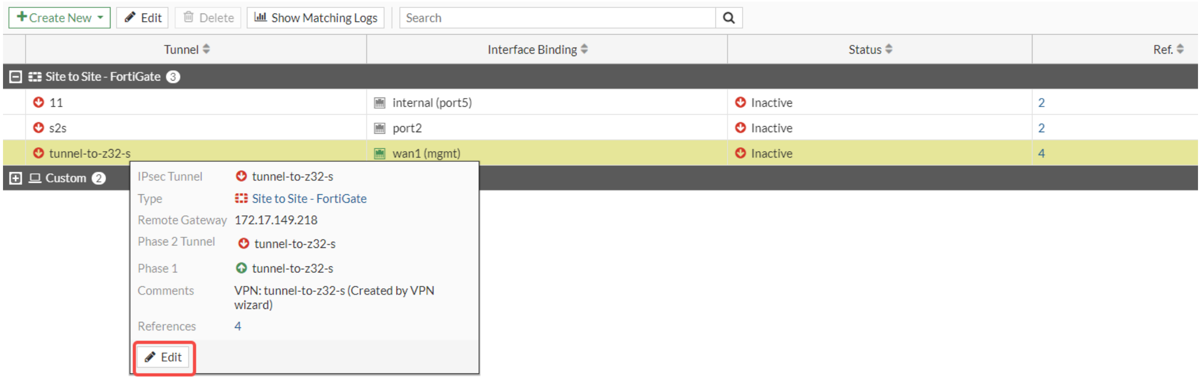
Object Summary

Phase 1 interface	tunnel-to-z32-s
Local address group	tunnel-to-z32-s_local
Remote address group	tunnel-to-z32-s_remote
Phase 2 interface	tunnel-to-z32-s
Static route	static
Blackhole route	static
Local to remote policies	vpn_tunnel-to-z32-s_local
Remote to local policies	vpn_tunnel-to-z32-s_remote

(3) After verifying the configuration, click **Create**.

4. VPN Authentication Configuration

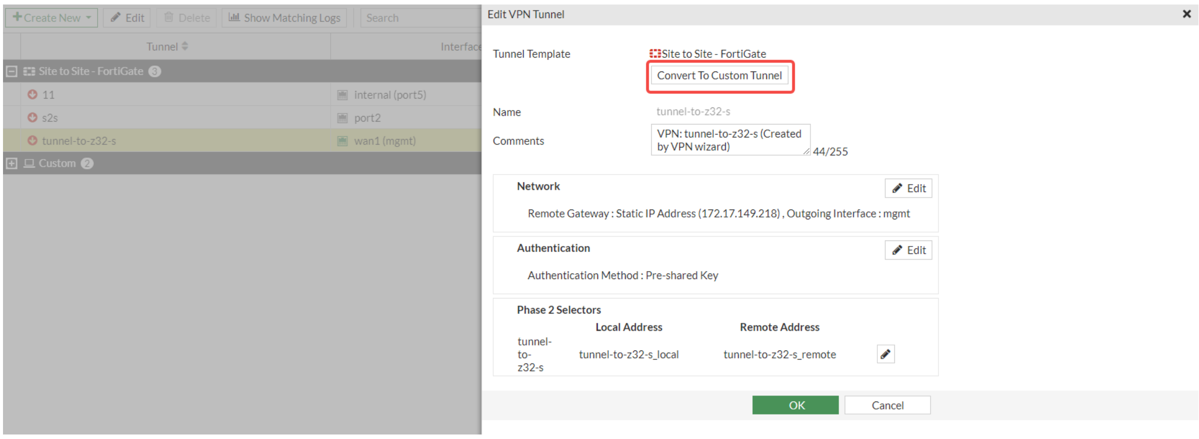
(1) Choose **VPN** > **IPsec Tunnels**. The IPsec tunnel page is displayed.



Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 3			
11	internal (port5)	Inactive	2
s2s	port2	Inactive	2
tunnel-to-z32-s	wan1 (mgmt)	Inactive	4
Custom 2			

IPsec Tunnel	tunnel-to-z32-s
Type	Site to Site - FortiGate
Remote Gateway	172.17.149.218
Phase 2 Tunnel	tunnel-to-z32-s
Phase 1	tunnel-to-z32-s
Comments	VPN: tunnel-to-z32-s (Created by VPN wizard)
References	4

(2) Select the tunnel created in the previous step, and click **Edit**. In the dialog box that is displayed, click **Convert To Custom Tunnel**.



Tunnel Template: Site to Site - FortiGate

Name: tunnel-to-z32-s

Comments: VPN: tunnel-to-z32-s (Created by VPN wizard) 44/255

Network

Remote Gateway : Static IP Address (172.17.149.218) , Outgoing Interface : mgmt

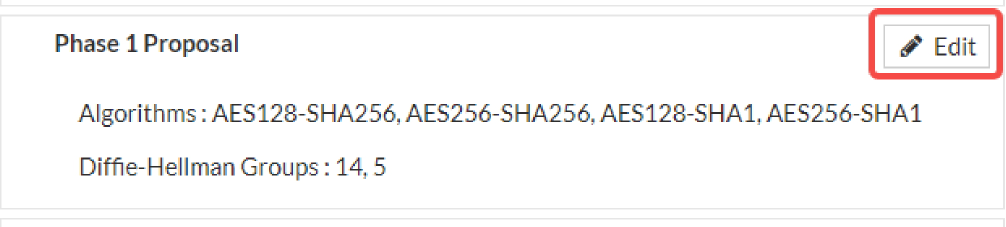
Authentication

Authentication Method : Pre-shared Key

Phase 2 Selectors

	Local Address	Remote Address
tunnel-to-z32-s	tunnel-to-z32-s_local	tunnel-to-z32-s_remote

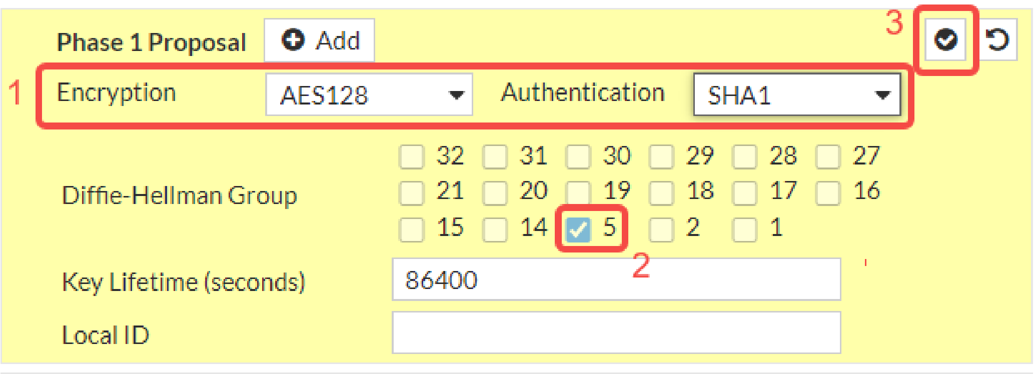
(3) Click **Edit** in the **Phase 1 Proposal** area and modify the authentication parameters according to the following figure.



Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1

Diffie-Hellman Groups : 14, 5

- Set **Encryption** to **AES128**.
- Set **Authentication** to **SHA1**.
- Set **Diffie-Hellman Group** to 5.
- Use the default configuration for the other parameters.



Encryption: AES128

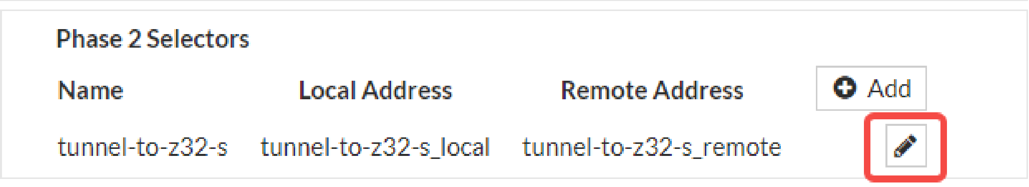
Authentication: SHA1

Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1

Key Lifetime (seconds): 86400

Local ID:

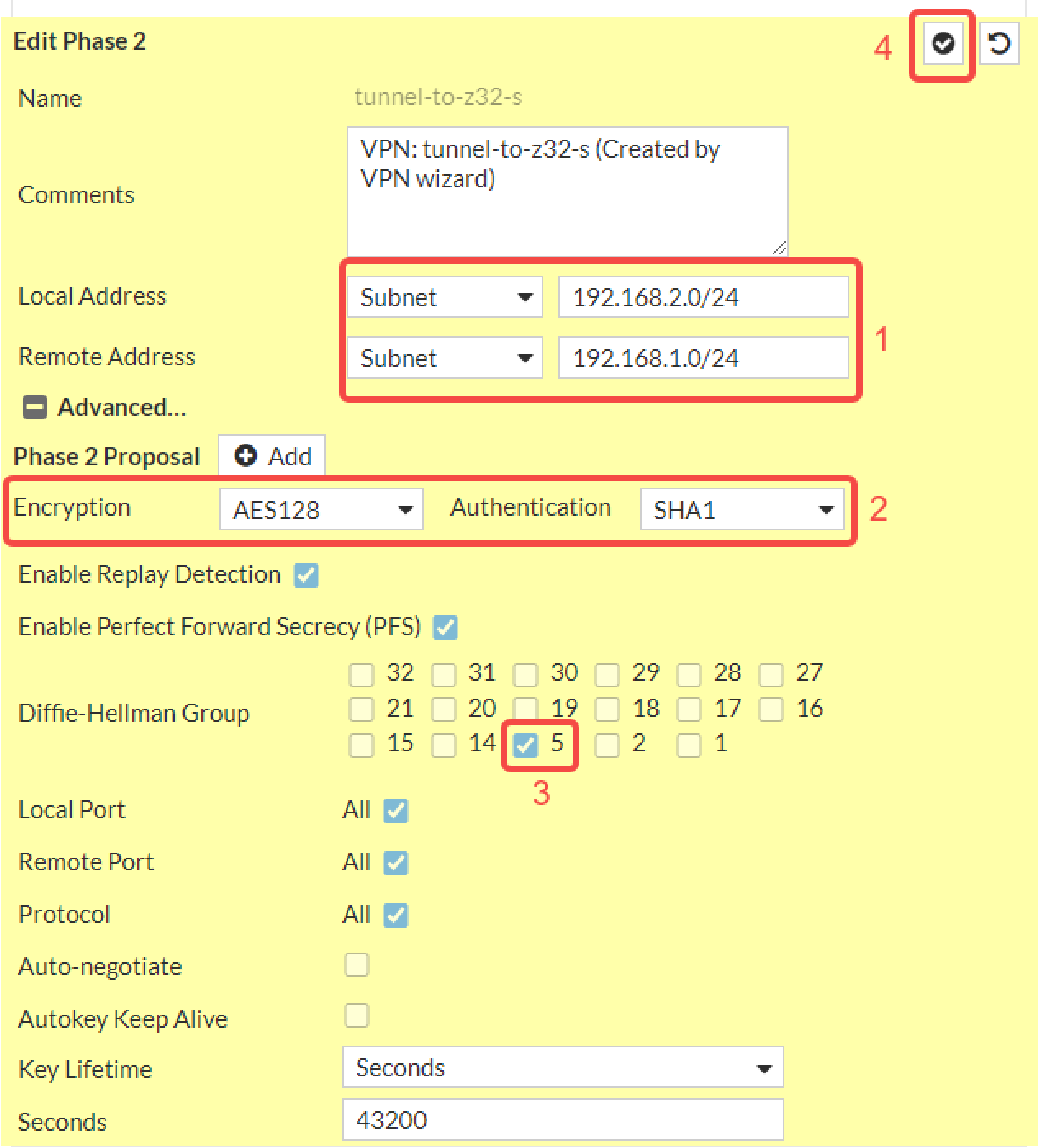
(4) Click the edit icon in the **Phase 2 Proposal** area and modify the authentication parameters according to the following figure.



Phase 2 Selectors

Name	Local Address	Remote Address
tunnel-to-z32-s	tunnel-to-z32-s_local	tunnel-to-z32-s_remote

- Set **Local Address** to the subnet 192.168.2.0/24 of the Fortinet firewall.
- Set **Remote Address** to the subnet 192.168.1.0/24 of the RG-WALL Z3200-S.
- Set **Encryption** to **AES128**.
- Set **Authentication** to **SHA1**.
- Set **Diffie-Hellman Group** to 5.
- Use the default configuration for the other parameters.



Edit Phase 2

Name: tunnel-to-z32-s

Comments: VPN: tunnel-to-z32-s (Created by VPN wizard)

Local Address: Subnet 192.168.2.0/24

Remote Address: Subnet 192.168.1.0/24

Advanced...

Phase 2 Proposal

Encryption: AES128 Authentication: SHA1

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1

Local Port: All ☑

Remote Port: All ☑

Protocol: All ☑

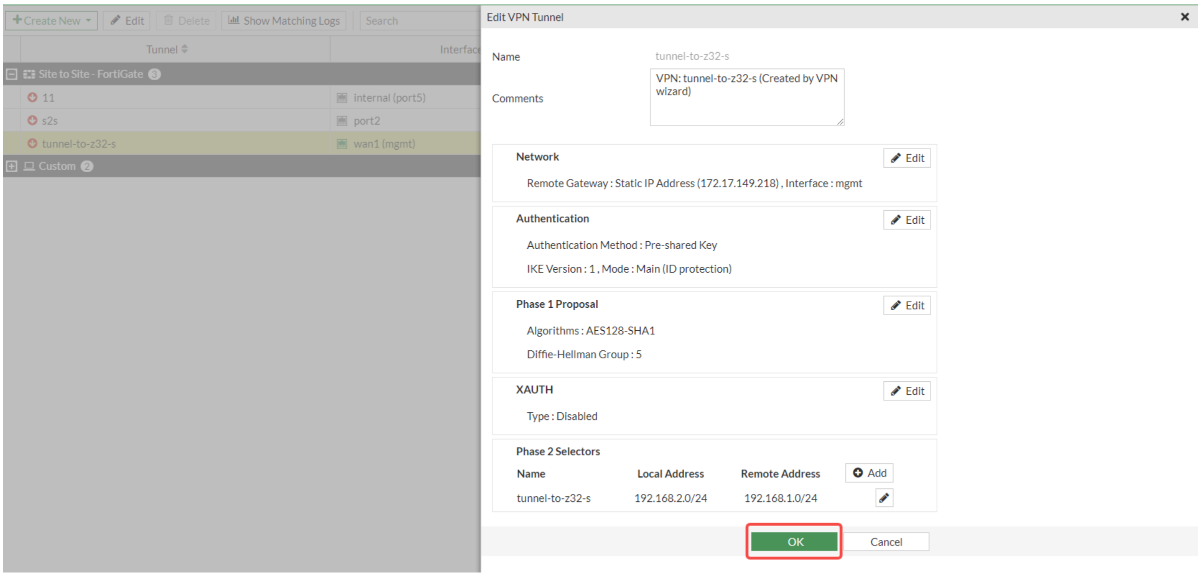
Auto-negotiate □

Autokey Keep Alive □

Key Lifetime: Seconds

Seconds: 43200

(5) After completing the modification, click **OK**.



Tunnel	Interface
Site to Site - FortiGate 3	
11	internal (port5)
s2s	port2
tunnel-to-z32-s	wan1 (mgmt)
Custom 2	

Name: tunnel-to-z32-s

Comments: VPN: tunnel-to-z32-s (Created by VPN wizard)

Network

Remote Gateway : Static IP Address (172.17.149.218) , Interface : mgmt

Authentication

Authentication Method : Pre-shared Key

IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal

Algorithms : AES128-SHA1

Diffie-Hellman Group : 5

XAUTH

Type : Disabled

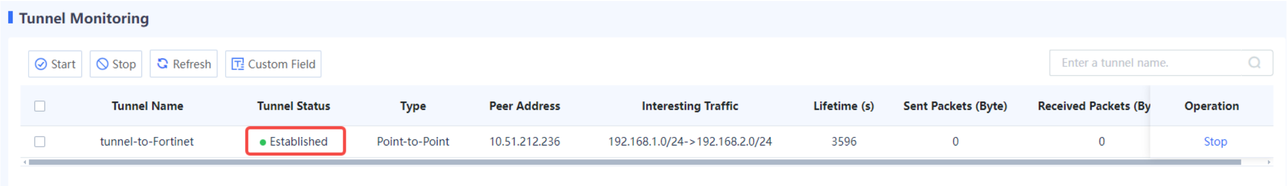
Phase 2 Selectors

Name	Local Address	Remote Address
tunnel-to-z32-s	192.168.2.0/24	192.168.1.0/24

3.6 Verification

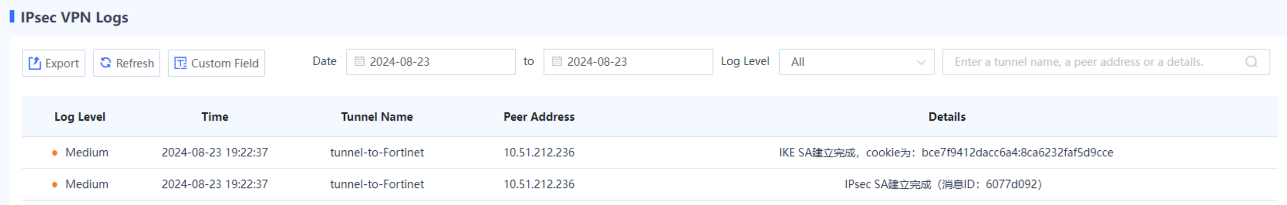
3.6.1 Verifying Configuration of Site A (RG-WALL Z3200-S)

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. Verify that the tunnel status is **Established**.



☐	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Received Packets (By	Operation
☐	tunnel-to-Fortinet	● Established	Point-to-Point	10.51.212.236	192.168.1.0/24->192.168.2.0/24	3596	0	0	Stop

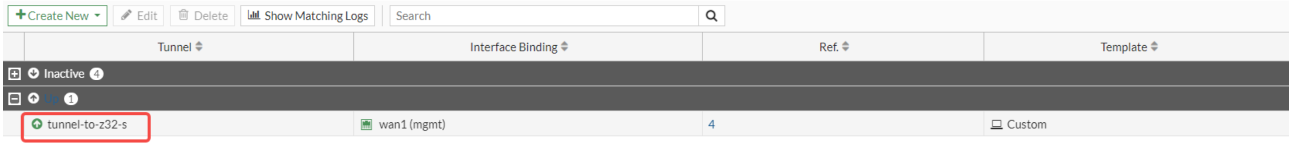
- Choose **Monitor** > **Log Monitoring** > **IPsec VPN Log**. Check IPsec tunnel negotiation logs.



Log Level	Time	Tunnel Name	Peer Address	Details
● Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IKE SA建立完成，cookie为：bce7f9412dacc6a4:8ca6232faf5d9cce
● Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IPsec SA建立完成（消息ID：6077d092）

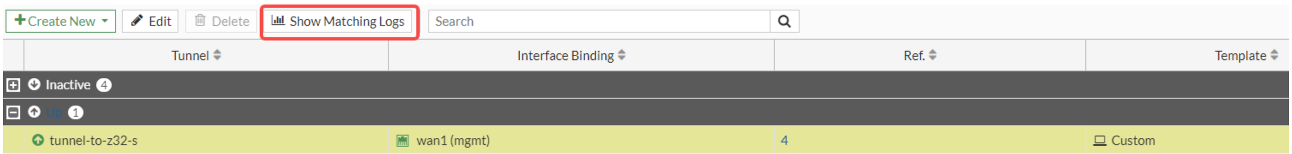
3.6.2 Verifying Configuration of Site B (Fortinet Firewall)

- Choose **VPN** > **IPsec Tunnels**. Verify that the tunnel status is established.

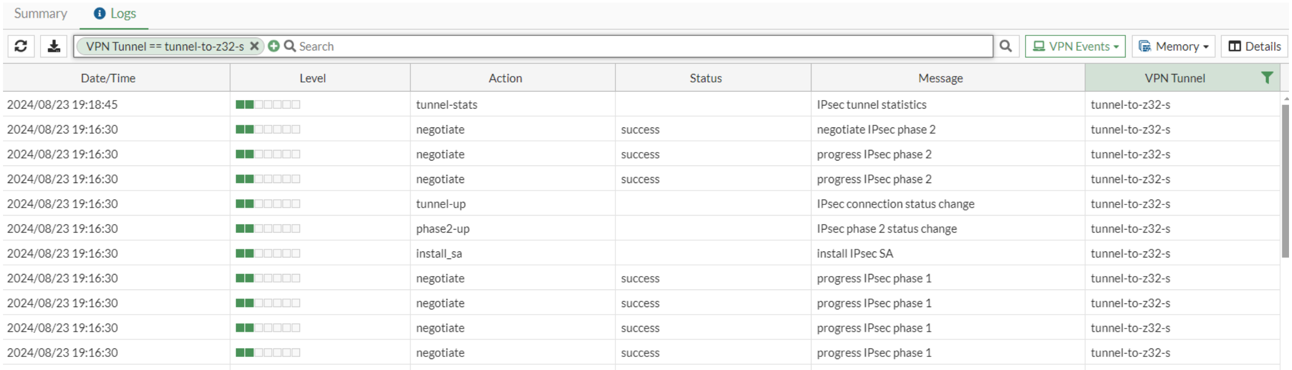


Tunnel	Interface Binding	Ref.	Template
Inactive 4			
Up 1			
tunnel-to-z32-s	wan1 (mgmt)	4	Custom

- Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.



Tunnel	Interface Binding	Ref.	Template
⊞ Inactive 4			
⊟ Up 1			
tunnel-to-z32-s	wan1 (mgmt)	4	Custom



Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/08/23 19:18:45	■■□□□□□	tunnel-stats		IPsec tunnel statistics	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	negotiate IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 2	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	tunnel-up		IPsec connection status change	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	phase2-up		IPsec phase 2 status change	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	install_sa		install IPsec SA	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s
2024/08/23 19:16:30	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-z32-s

4 Configuration Examples of Site-to-Multisite IPsec VPN

4.1 Applicable Products and Versions

Table 4-1 Products and Versions

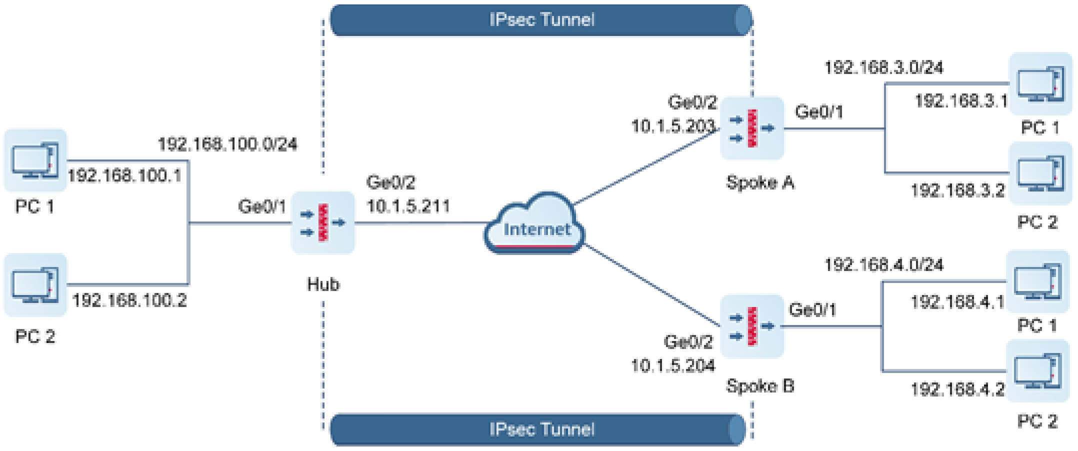
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

4.2 Service Demands

In a site-to-site scenario, a pre-shared key needs to be specified for each peer. When defining an IPsec policy, you also need to specify the IP address or domain name of the peer. As the number of peers increases, duplicate configurations also increase, making maintenance difficult. In addition, if a peer does not have a fixed IP address, the IPsec tunnel cannot be established.

To solve the preceding problems, a site-to-multisite solution is proposed, as shown in Figure 4-1. In a site-to-multisite scenario, the hub site needs to establish tunnels with multiple spoke sites. All the spoke sites use the same pre-shared key as the hub site. The hub site does not initiate connections. Instead, the spoke sites initiate connections to establish IPsec tunnels.

Figure 4-1 Site-to-Multisite Networking



4.3 Restrictions and Guidelines

- Currently, if the RG-WALL 1600-Z series firewall acts as a hub site on an IPsec VPN, all spoke sites must use the same pre-shared key to negotiate with the hub site.

- The following describes how to configure Spoke A. The configuration for Spoke B is similar.

4.4 Prerequisites

You have completed basic network configurations for Site A and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- The IP address of the hub site is fixed.
- All spoke sites can obtain the pre-shared key configured on the hub site in out-of-band (OOB) mode.

4.5 Procedure

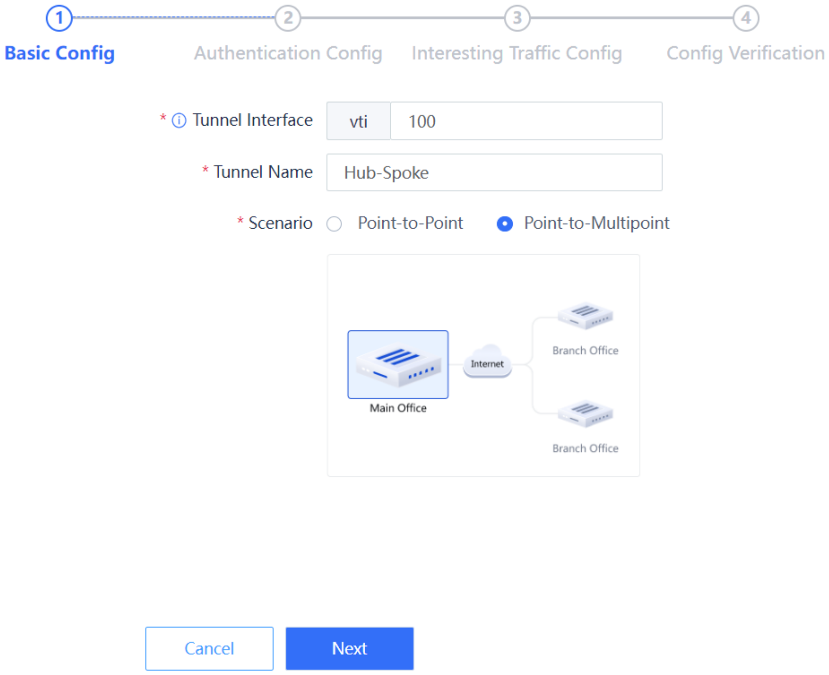
4.5.1 Using a Configuration Wizard

1. Configuring the Hub Site

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Site-to-Multisite**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 100

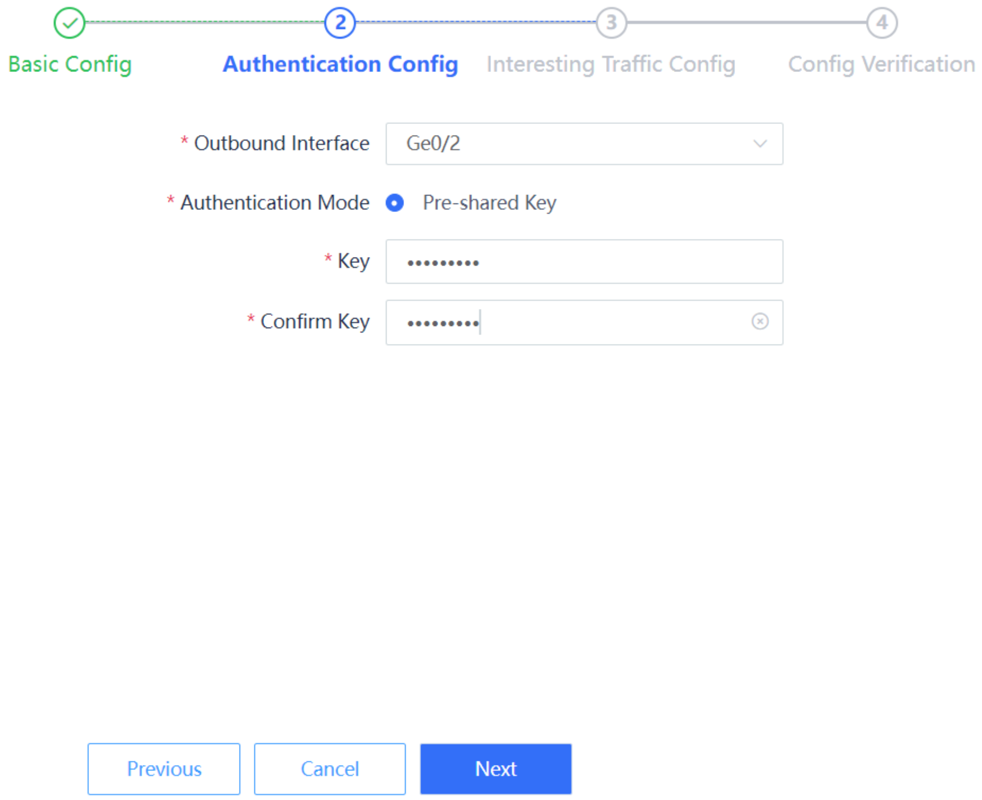
* Tunnel Name: Hub-Spoke

* Scenario: ○ Point-to-Point ● Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.



* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

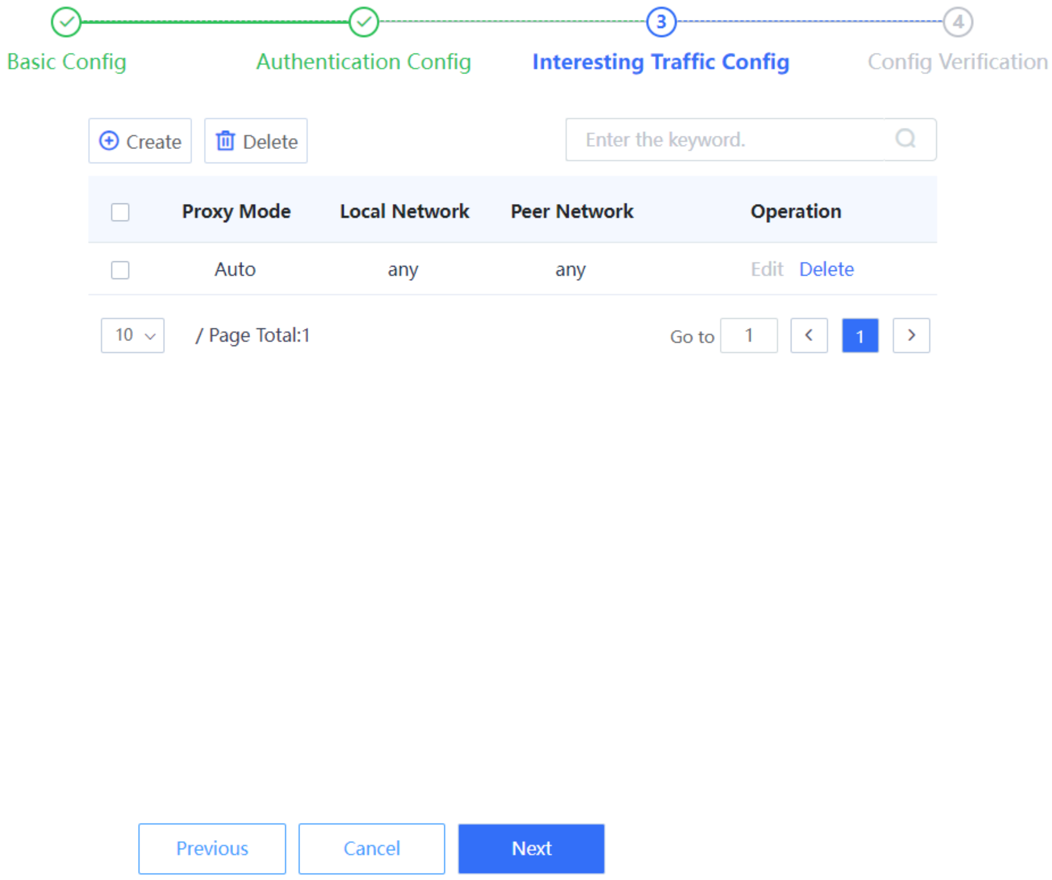
* Key: •••••••••

* Confirm Key: •••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

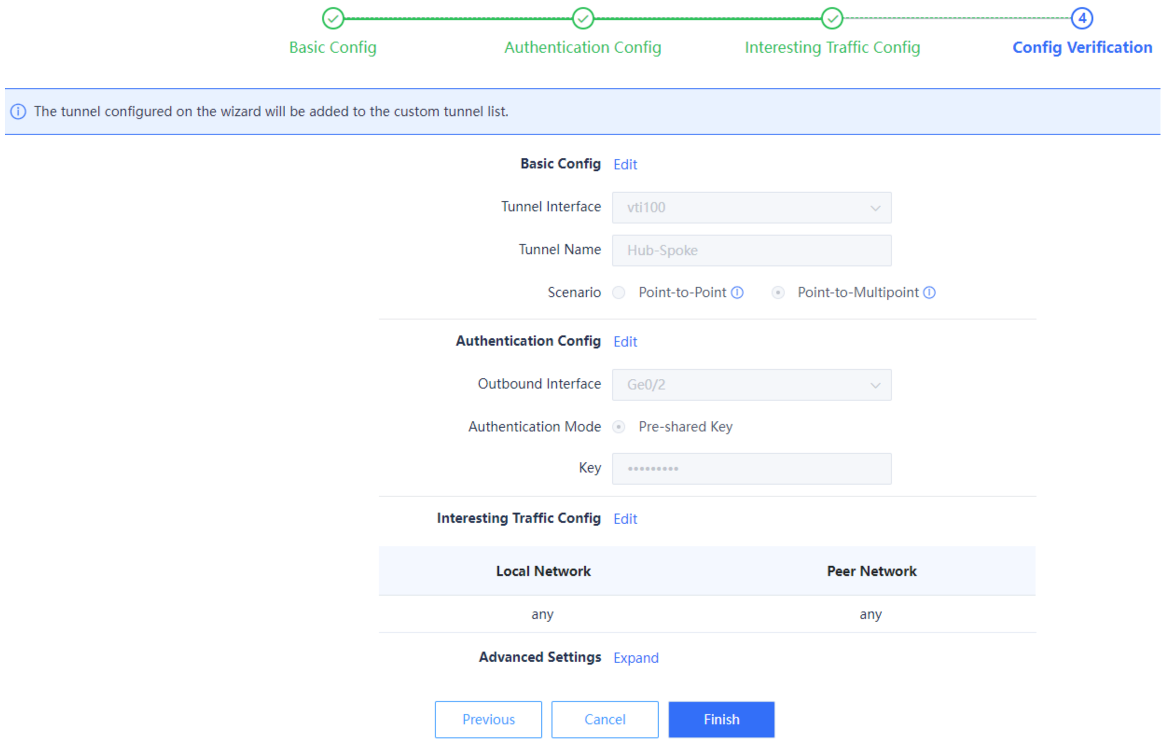


□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



ⓘ The tunnel configured on the wizard will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti100

Tunnel Name: Hub-Spoke

Scenario: ○ Point-to-Point ⓘ ● Point-to-Multipoint ⓘ

Authentication Config Edit

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: ·········

Interesting Traffic Config Edit

Local Network	Peer Network
any	any

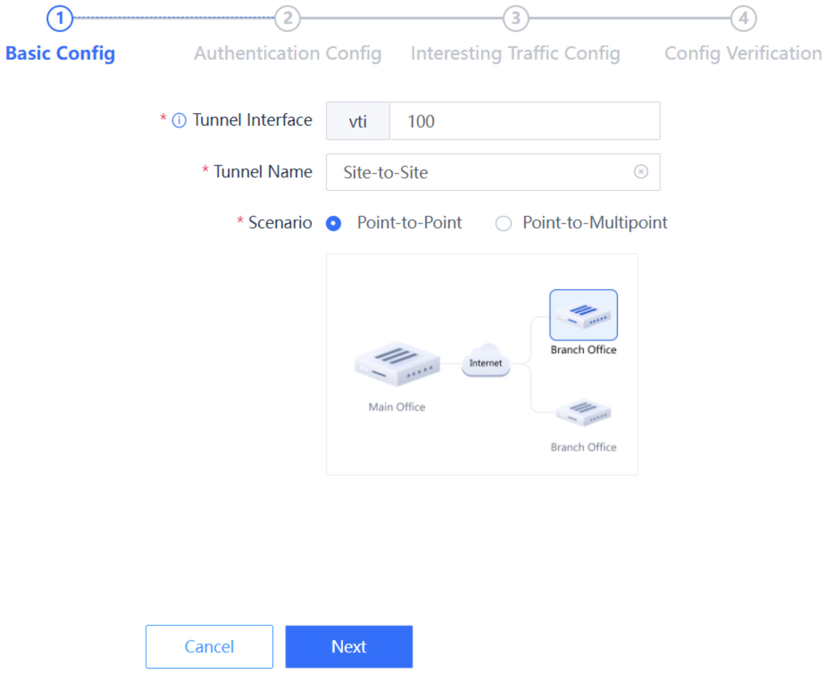
Advanced Settings Expand

2. Configuring Spoke A

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



* ⓘ Tunnel Interface: vti 100

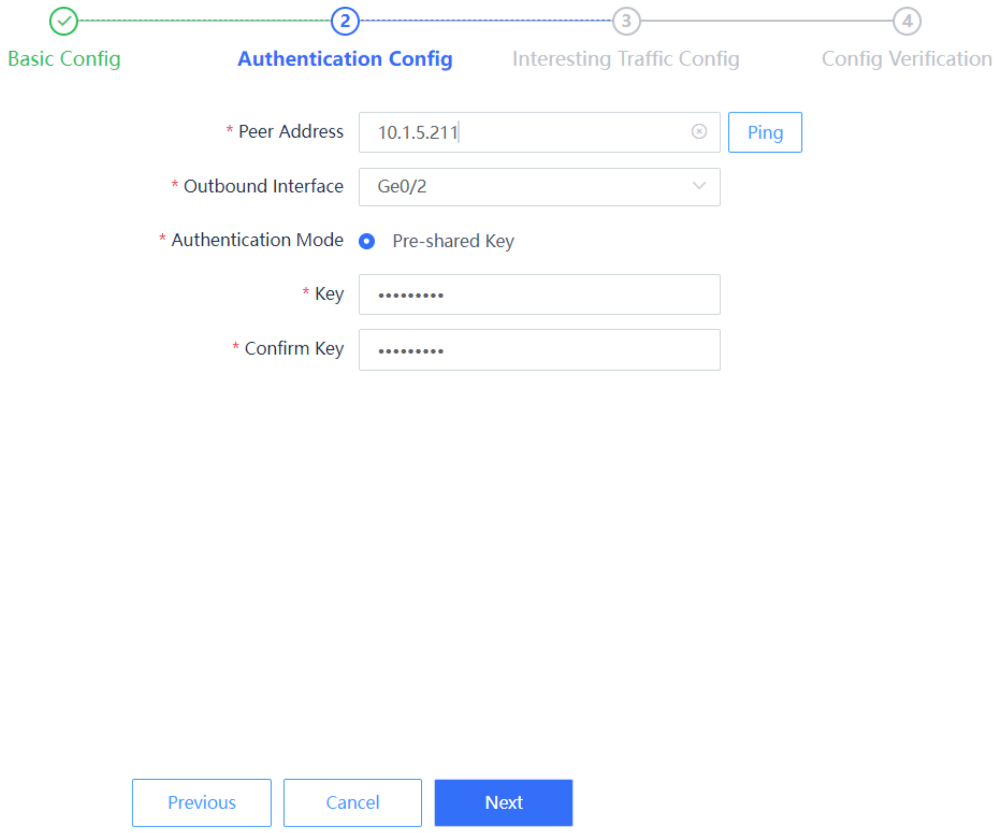
* Tunnel Name: Site-to-Site

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.

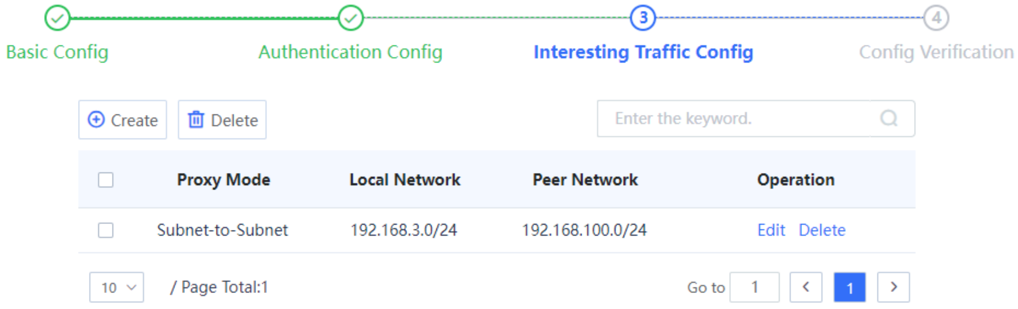


* Peer Address: 10.1.5.211
* Outbound Interface: Ge0/2
* Authentication Mode: ● Pre-shared Key
* Key: •••••••••
* Confirm Key: •••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

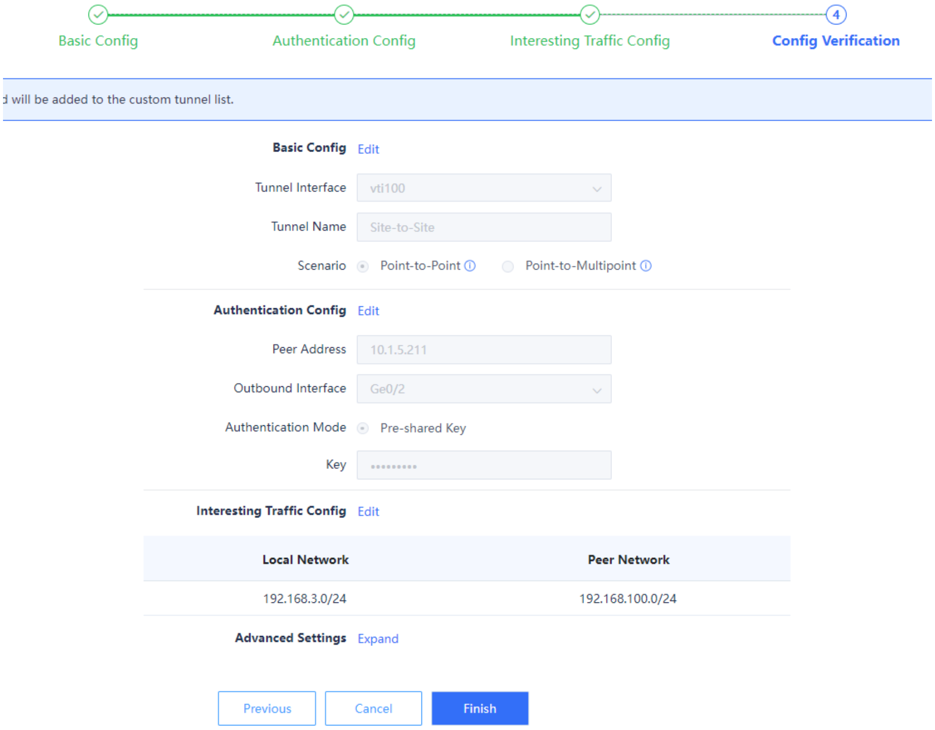


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



d will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti100

Tunnel Name: Site-to-Site

Scenario: ● Point-to-Point ○ Point-to-Multipoint

Authentication Config Edit

Peer Address: 10.1.5.211

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: •••••••••

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.3.0/24	192.168.100.0/24

Advanced Settings Expand

4.5.2 Manually Configuring a Tunnel

1. Configuring the Hub Site

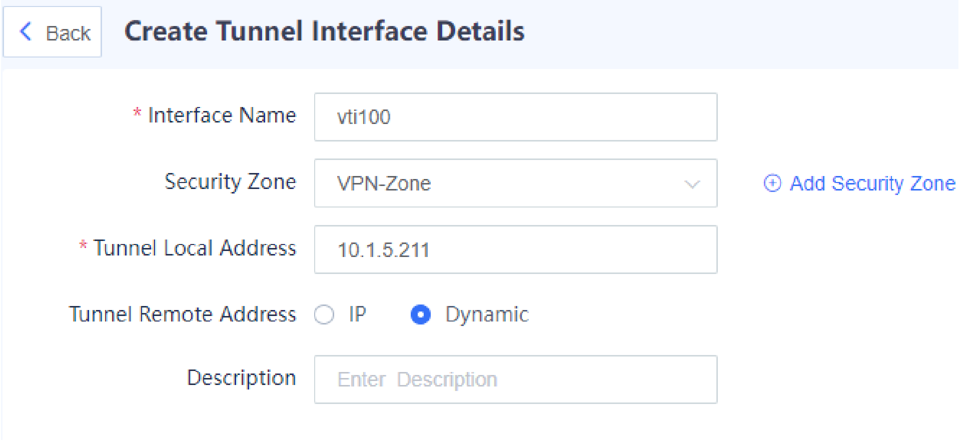
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **vti100**.
- Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of the hub site: 10.1.5.211.
- Set **Tunnel Remote Address** to **Dynamic**.


< Back **Create Tunnel Interface Details**

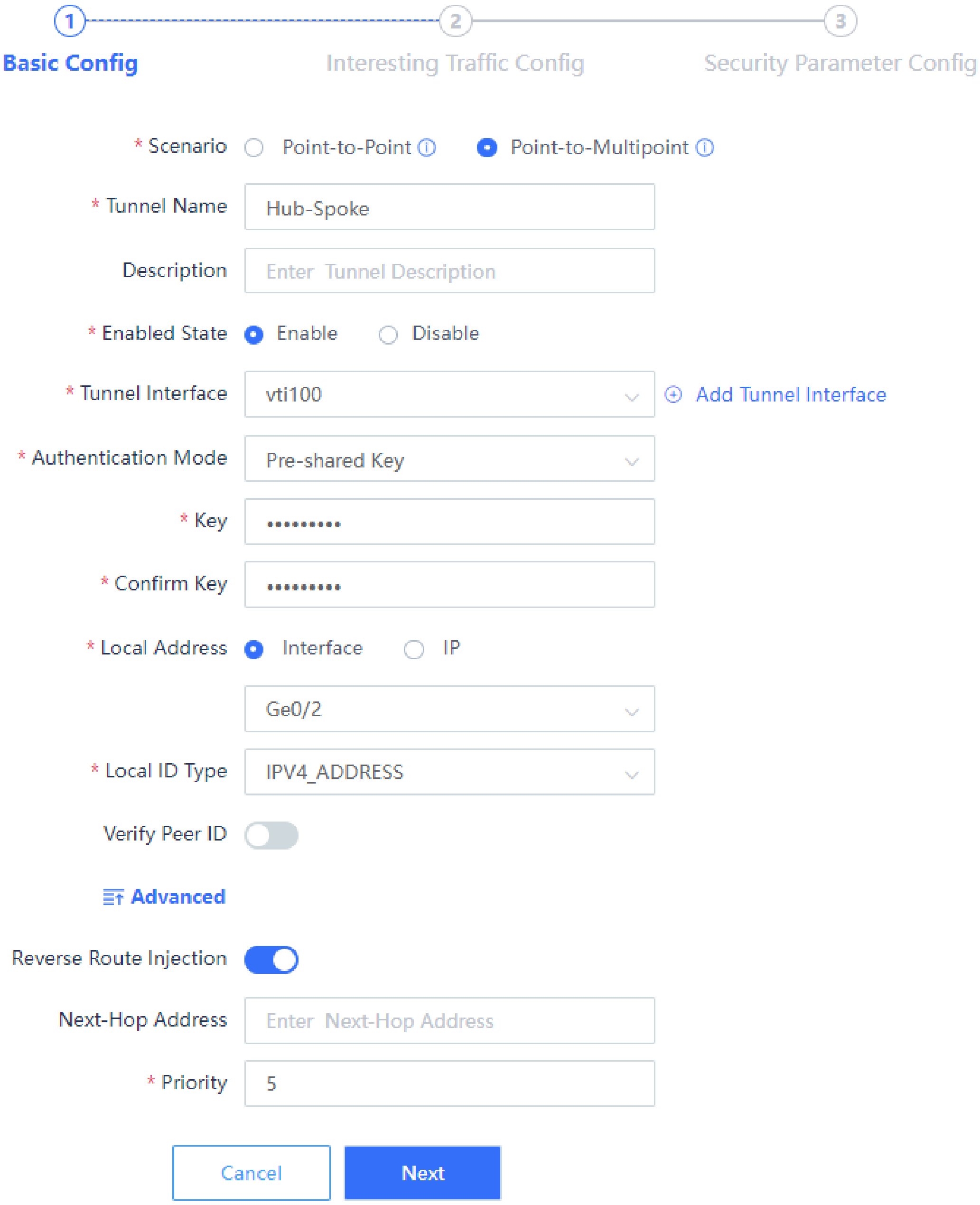
* Interface Name	vti100
Security Zone	VPN-Zone
* Tunnel Local Address	10.1.5.211
Tunnel Remote Address	○ IP ● Dynamic
Description	Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **Hub-Spoke**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **vti100**.
- Set **Local Address** to **interface Ge0/2**.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- Toggle on **Reverse Route Injection** for the hub site. For **Priority**, use the default value 5. Do not configure **Next-Hop Address**.



* Scenario ○ Point-to-Point ● Point-to-Multipoint

* Tunnel Name: Hub-Spoke

Description: Enter Tunnel Description

* Enabled State ● Enable ○ Disable

* Tunnel Interface: vti100

* Authentication Mode: Pre-shared Key

* Key: ••••••••••

* Confirm Key: ••••••••••

* Local Address ● Interface ○ IP

Ge0/2

* Local ID Type: IPV4_ADDRESS

Verify Peer ID: off

Reverse Route Injection: on

Next-Hop Address: Enter Next-Hop Address

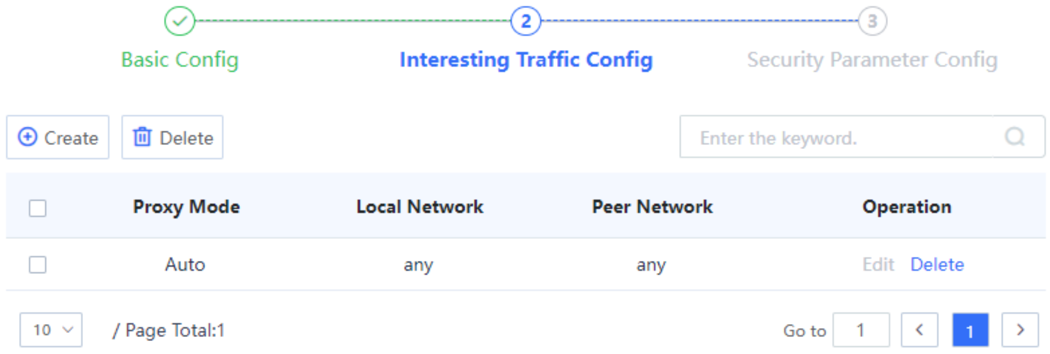
* Priority: 5

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

o Set **Proxy Mode** to **Auto**.



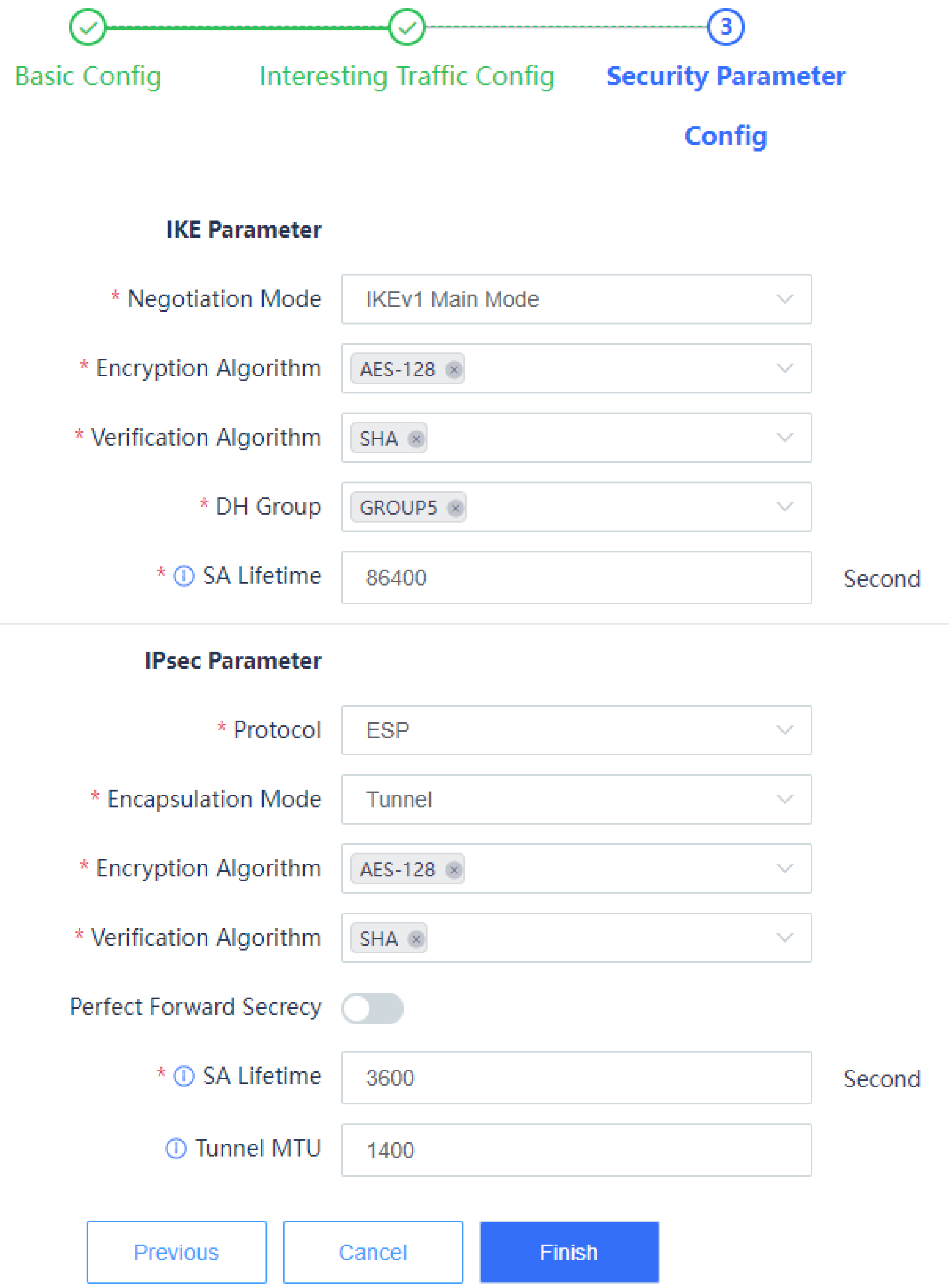
□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode: IKEv1 Main Mode

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 86400 Second

IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

Perfect Forward Secrecy: Off

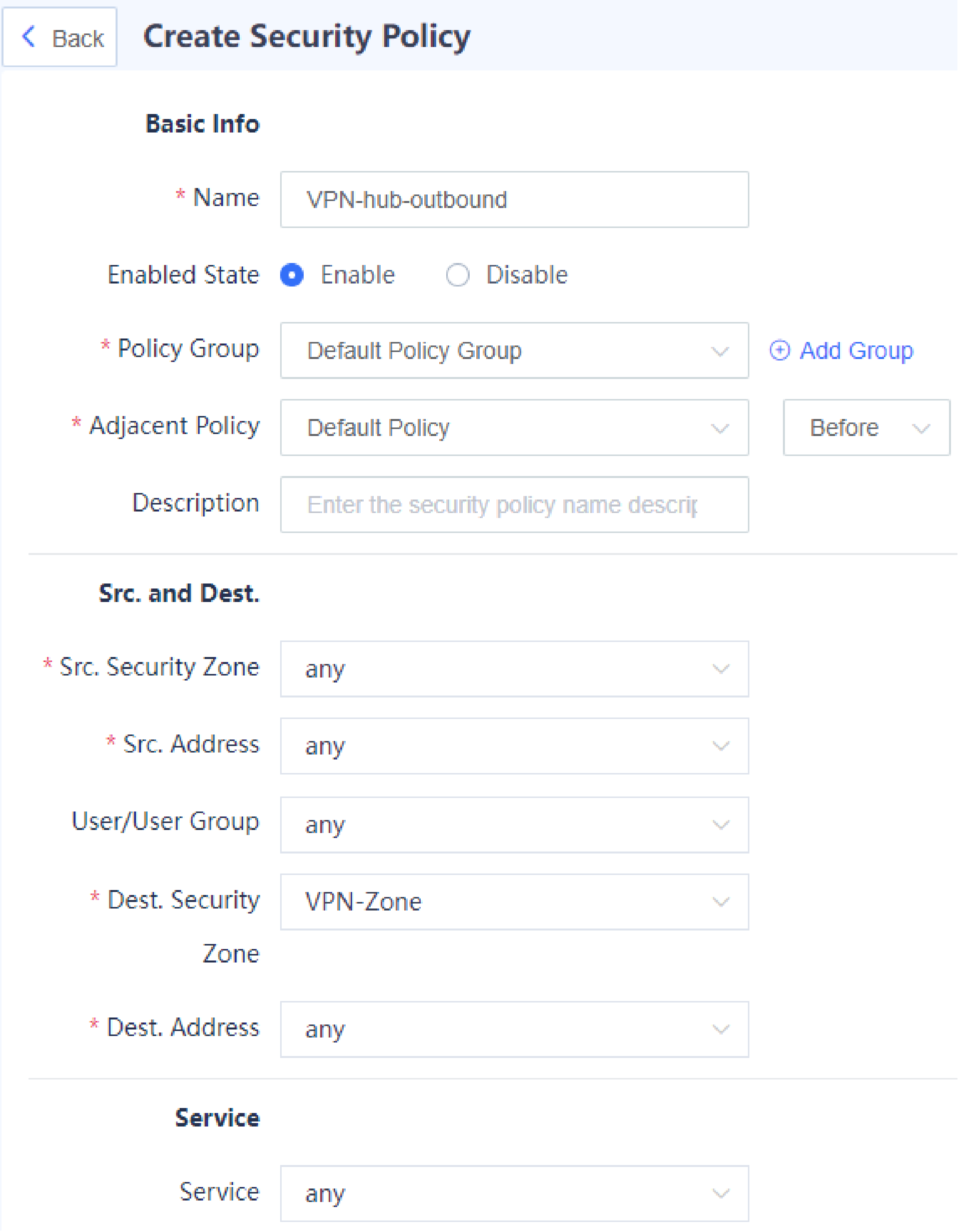
* SA Lifetime: 3600 Second

Tunnel MTU: 1400

Click **Finish** to complete the IPsec tunnel configuration for the hub site.

(3) Create security policies.

a Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-hub-outbound** and inbound security policy **VPN-hub-inbound** separately.



< Back **Create Security Policy**

Basic Info

* Name: VPN-hub-outbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

* Adjacent Policy: Default Policy, Before

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: any

* Src. Address: any

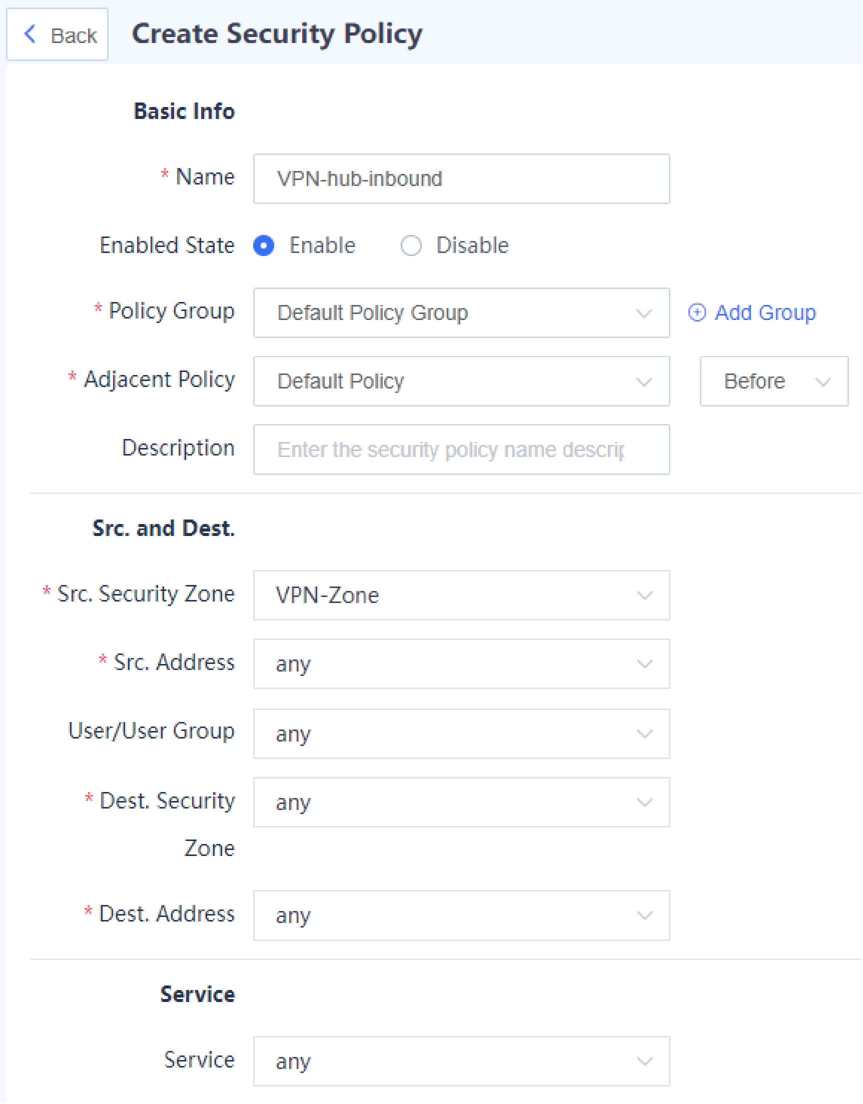
User/User Group: any

* Dest. Security Zone: VPN-Zone

* Dest. Address: any

Service

Service: any



Create Security Policy

Basic Info

* Name	VPN-hub-inbound
Enabled State	● Enable ○ Disable
* Policy Group	Default Policy Group ⊕ Add Group
* Adjacent Policy	Default Policy Before
Description	Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone	VPN-Zone
* Src. Address	any
User/User Group	any
* Dest. Security Zone	any
* Dest. Address	any

Service

Service	any

2. Configuring Spoke A

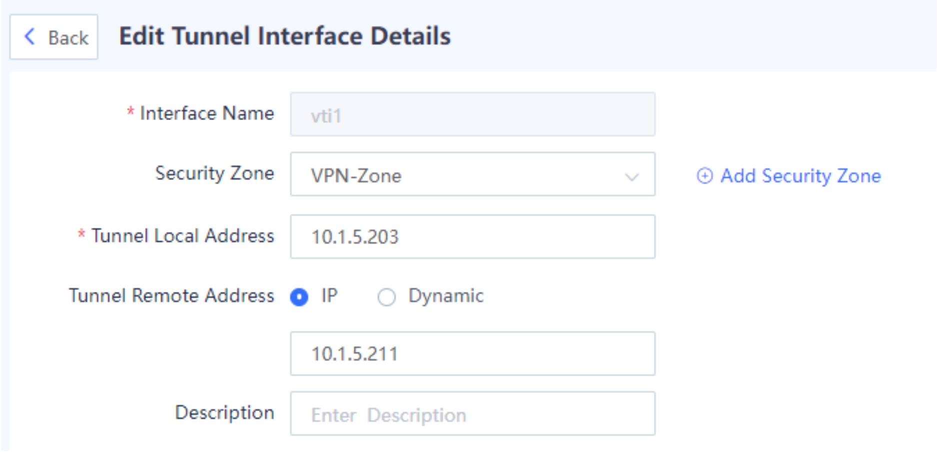
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **vti1**.
- Add security zone VPN-Zone and set **Security Zone** to **VPN-Zone** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
- Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 10.1.5.211.



< Back **Edit Tunnel Interface Details**

* Interface Name: vti1

Security Zone: VPN-Zone ⊕ Add Security Zone

* Tunnel Local Address: 10.1.5.203

Tunnel Remote Address: ● IP ○ Dynamic

10.1.5.211

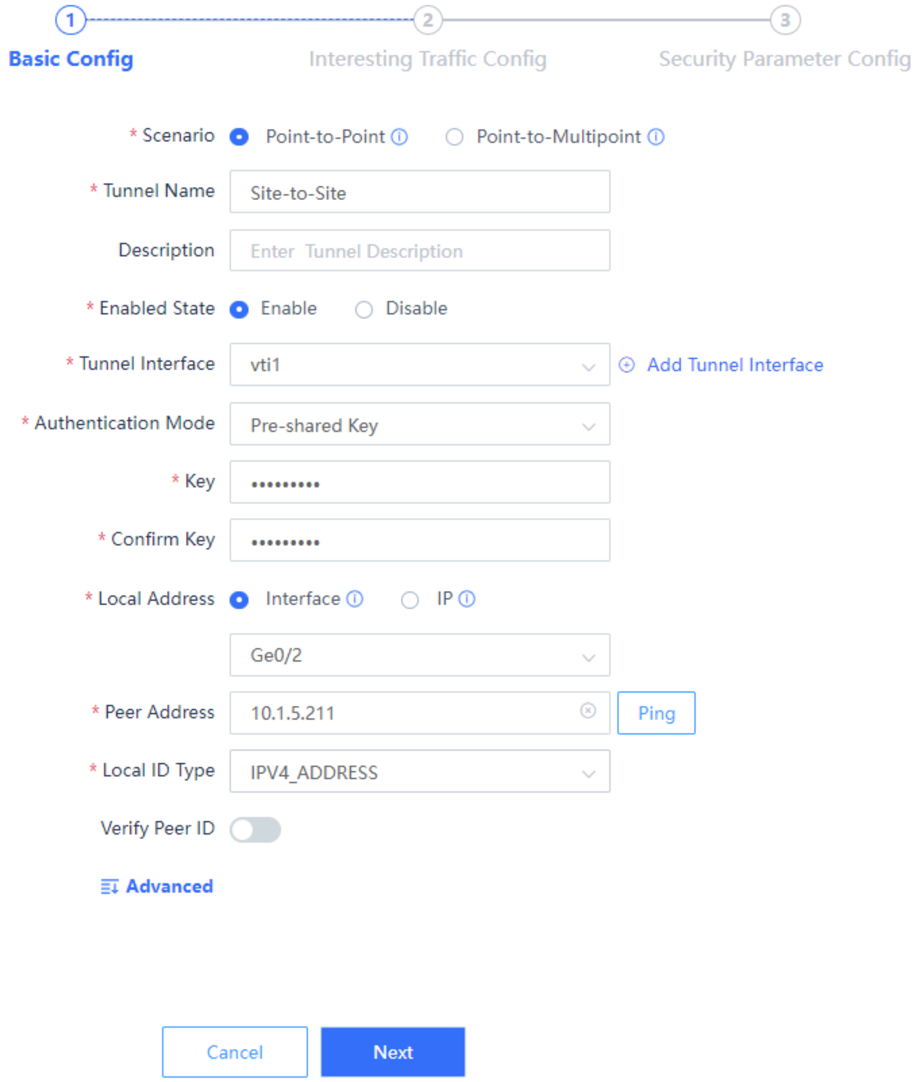
Description: Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **Site-to-Site**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **vti1**. Set **Local Address** to **interface Ge0/2**, and **Peer Address** to 10.1.5.211.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.



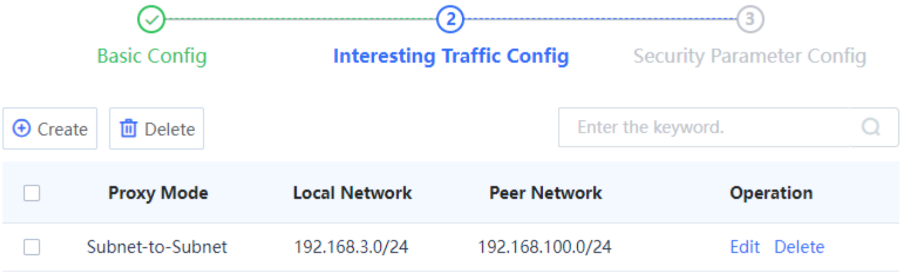
* Scenario: ● Point-to-Point ○ Point-to-Multipoint
* Tunnel Name: Site-to-Site
Description: Enter Tunnel Description
* Enabled State: ● Enable ○ Disable
* Tunnel Interface: vti1
* Authentication Mode: Pre-shared Key
* Key: •••••••••
* Confirm Key: •••••••••
* Local Address: ● Interface ○ IP
Ge0/2
* Peer Address: 10.1.5.211
* Local ID Type: IPV4_ADDRESS
Verify Peer ID: off

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set **Local Network** to 192.168.3.0/24 and **Peer Network** to 192.168.100.0/24.



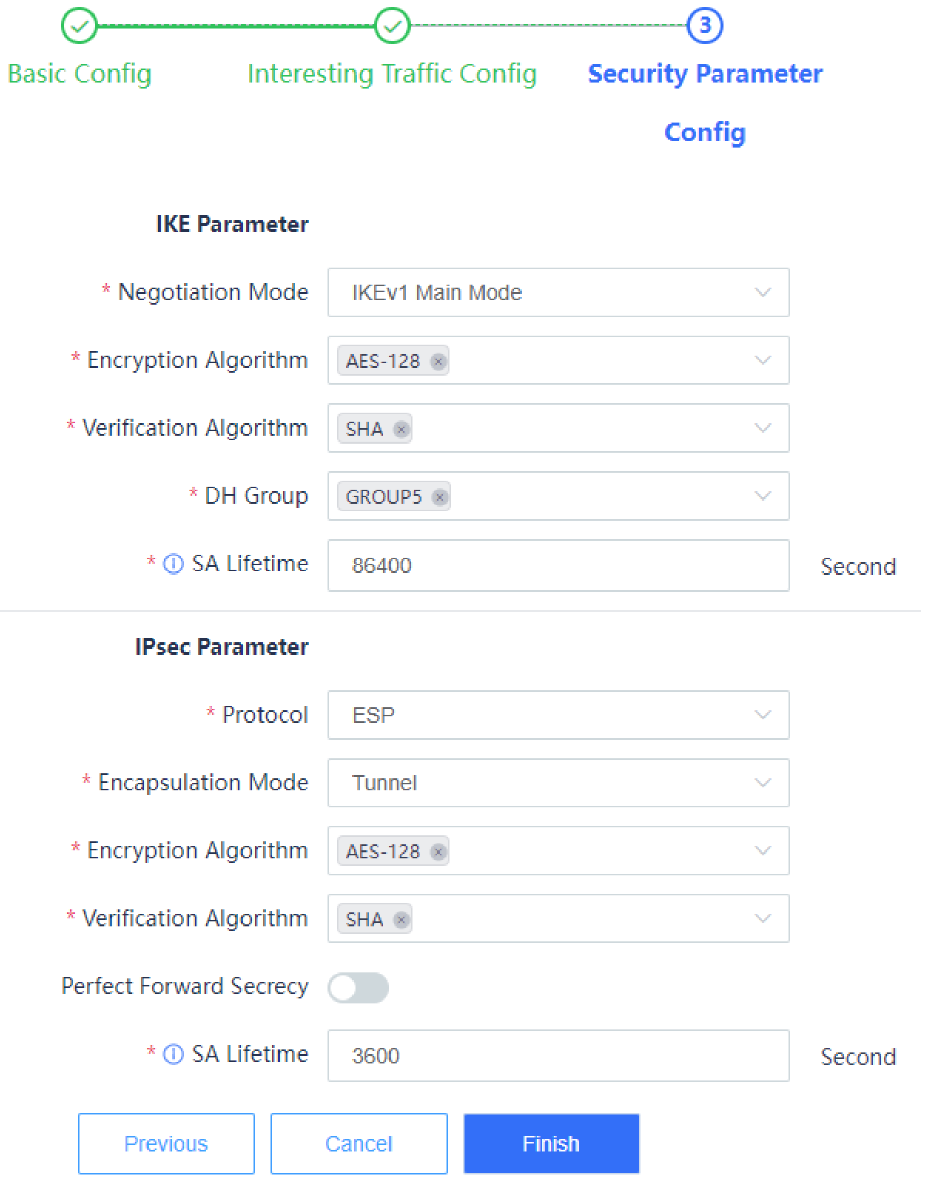
□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Main Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 86400 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 3600 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode: IKEv1 Main Mode
* Encryption Algorithm: AES-128
* Verification Algorithm: SHA
* DH Group: GROUP5
* SA Lifetime: 86400 Second

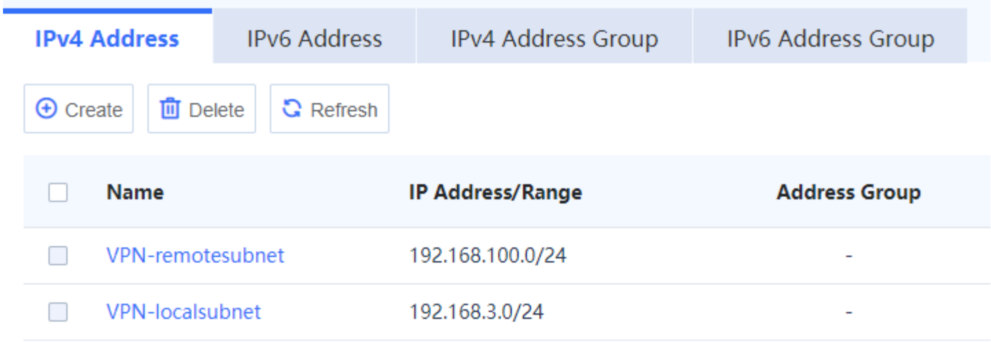
IPsec Parameter

* Protocol: ESP
* Encapsulation Mode: Tunnel
* Encryption Algorithm: AES-128
* Verification Algorithm: SHA
Perfect Forward Secrecy: ○
* SA Lifetime: 3600 Second

Click **Finish** to complete the configuration for the IPsec tunnel.

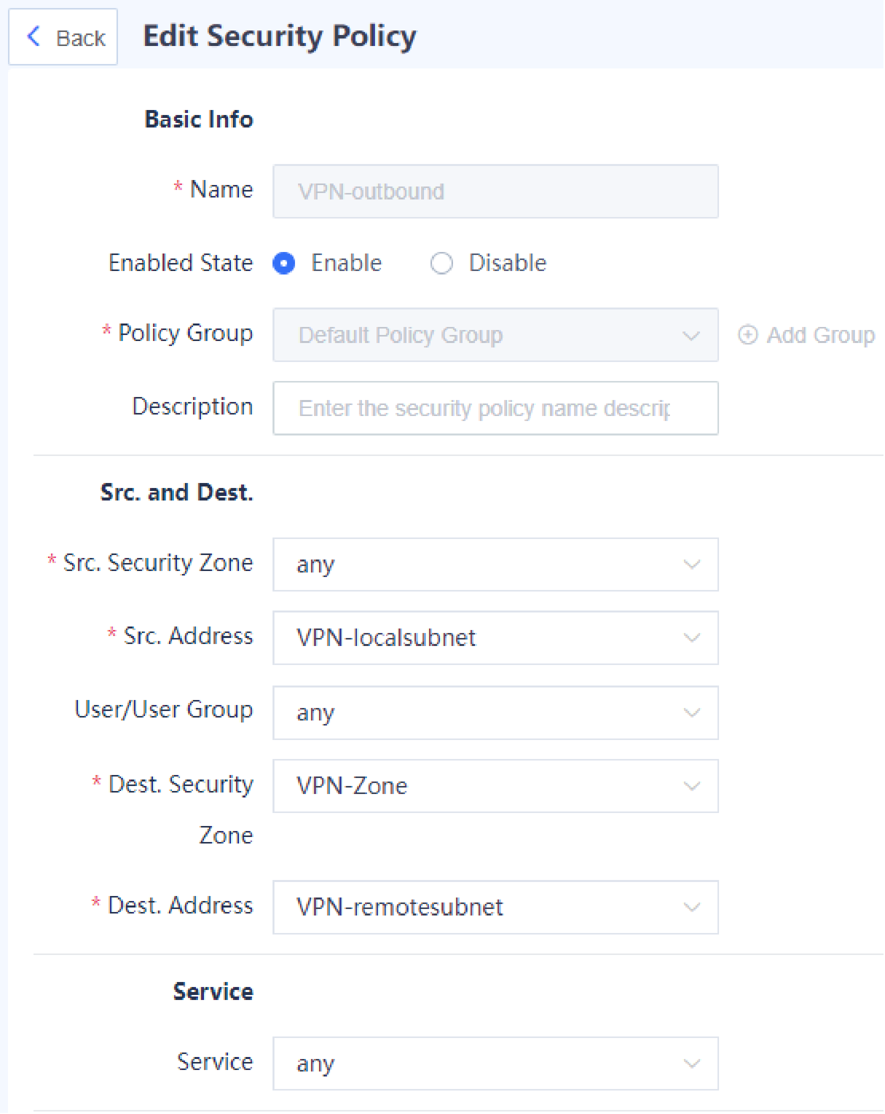
(3) Create security policies.

a Choose **Object** > **Address** > **IPv4 Address**. On the page that is displayed, click **Create** and create two address objects for local network 192.168.3.0/24 and peer network 192.168.100.0/24 of the interesting traffic separately.



□	Name	IP Address/Range	Address Group
□	VPN-remotesubnet	192.168.100.0/24	-
□	VPN-localsubnet	192.168.3.0/24	-

b Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create** and create outbound security policy **VPN-outbound** and inbound security policy **VPN-inbound** separately.



Basic Info

* Name: VPN-outbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: any

* Src. Address: VPN-localsubnet

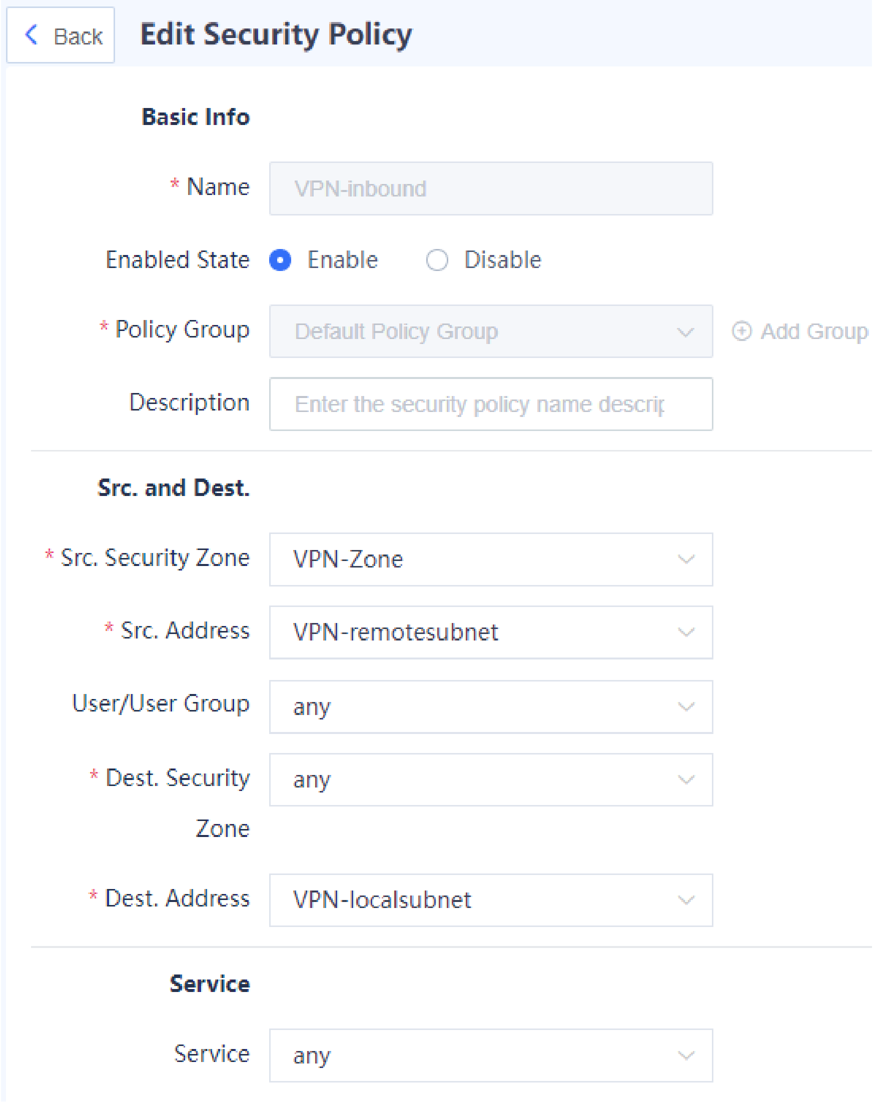
User/User Group: any

* Dest. Security Zone: VPN-Zone

* Dest. Address: VPN-remotesubnet

Service

Service: any



Basic Info

* Name: VPN-inbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: VPN-Zone

* Src. Address: VPN-remotesubnet

User/User Group: any

* Dest. Security Zone: any

* Dest. Address: VPN-localsubnet

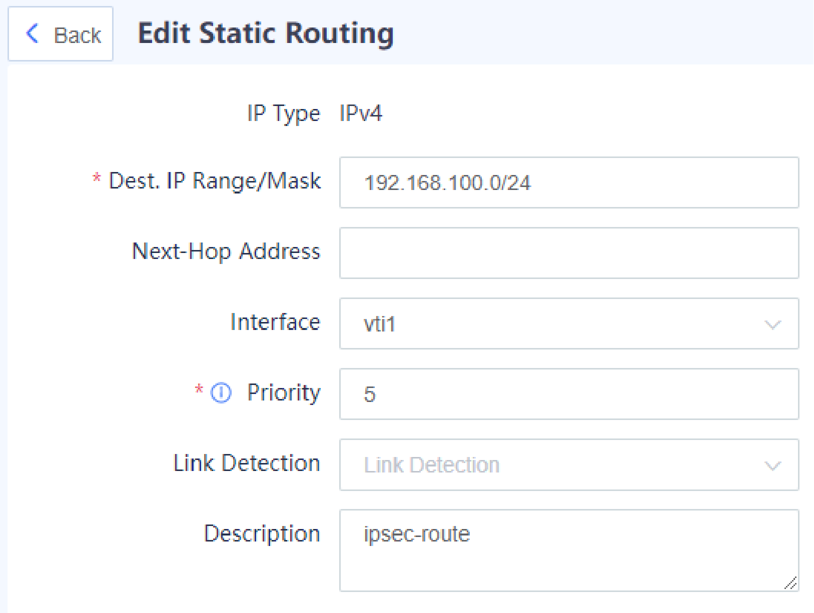
Service

Service: any

(4) Configure a static route.

a Choose **Network** > **Routing** > **Static Routing** > **IPv4**.

b Click **Create** and create a static route to the peer protected subnet of the VPN.



Edit Static Routing

IP Type IPv4

* Dest. IP Range/Mask 192.168.100.0/24

Next-Hop Address

Interface vti1

* Priority 5

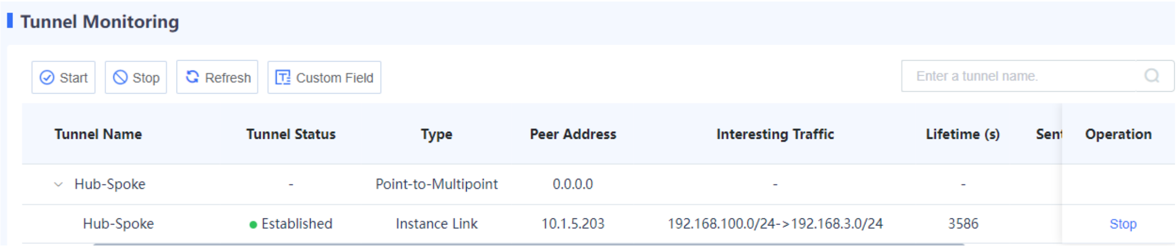
Link Detection Link Detection

Description ipsec-route

4.6 Verification

4.6.1 Verifying Configuration of the Hub Site

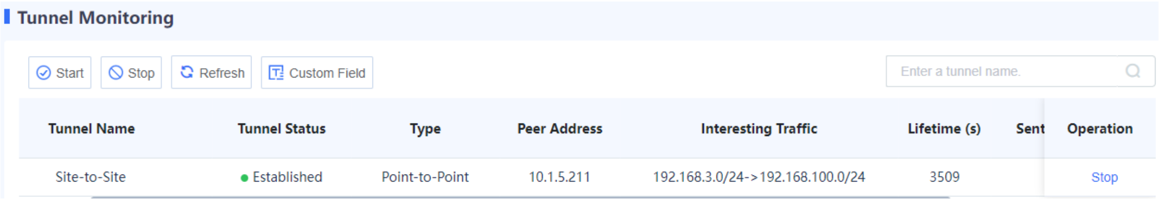
- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.



Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sen	Operation
Hub-Spoke	-	Point-to-Multipoint	0.0.0.0	-	-		
Hub-Spoke	● Established	Instance Link	10.1.5.203	192.168.100.0/24->192.168.3.0/24	3586		Stop

4.6.2 Verifying Configuration of Spoke A

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.



Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent	Operation
Site-to-Site	● Established	Point-to-Point	10.1.5.211	192.168.3.0/24->192.168.100.0/24	3509		Stop

5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall)

5.1 Applicable Products and Versions

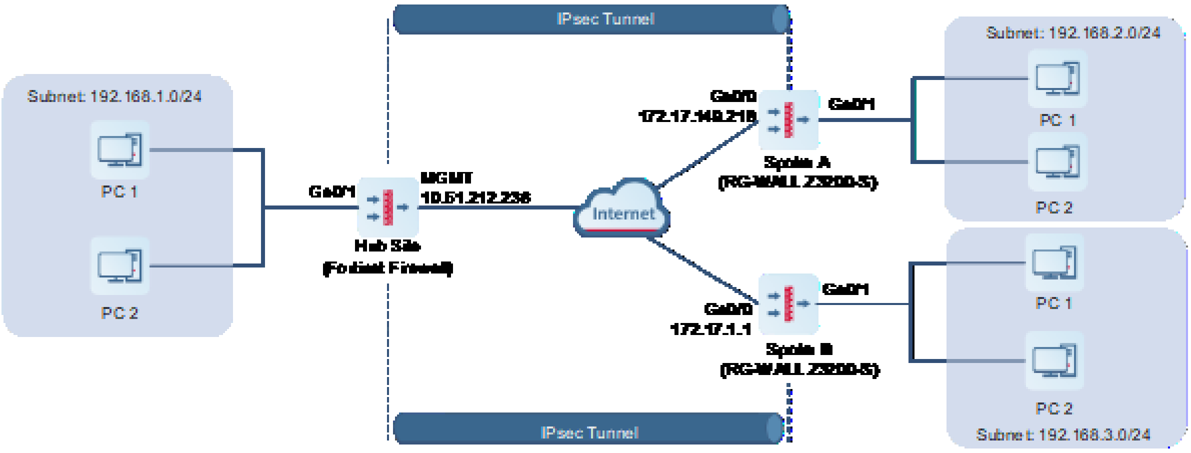
Table 5-1 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R8 or later
Firewall	FortiGate 100F	FortiOS 7.2.4 Build 1396 (Feature)

5.2 Service Demands

As shown in Figure 5-1, in a site-to-multisite scenario, the Fortinet firewall acts as the hub site, and multiple RG-WALL Z3200-S firewalls act as spoke sites. In a site-to-multisite scenario, the hub site needs to establish tunnels with multiple spoke sites. All the spoke sites use the same pre-shared key as the hub site. The hub site does not initiate connections. Instead, the spoke sites initiate connections to establish IPsec tunnels.

Figure 5-1 Site-to-Multisite Networking



5.3 Restrictions and Guidelines

- If the Fortinet FortiGate 100F series firewall acts as a hub site on an IPsec VPN, all spoke sites must use the same pre-shared key to negotiate with the hub site.
- The following describes how to configure Spoke A. The configuration for Spoke B is similar.

5.4 Prerequisites

You have completed basic network configurations for the hub site, Site A, and Site B, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- Ensure that the IP address of the hub site is fixed.
- All spoke sites obtain the pre-shared key configured on the hub site in OOB mode.

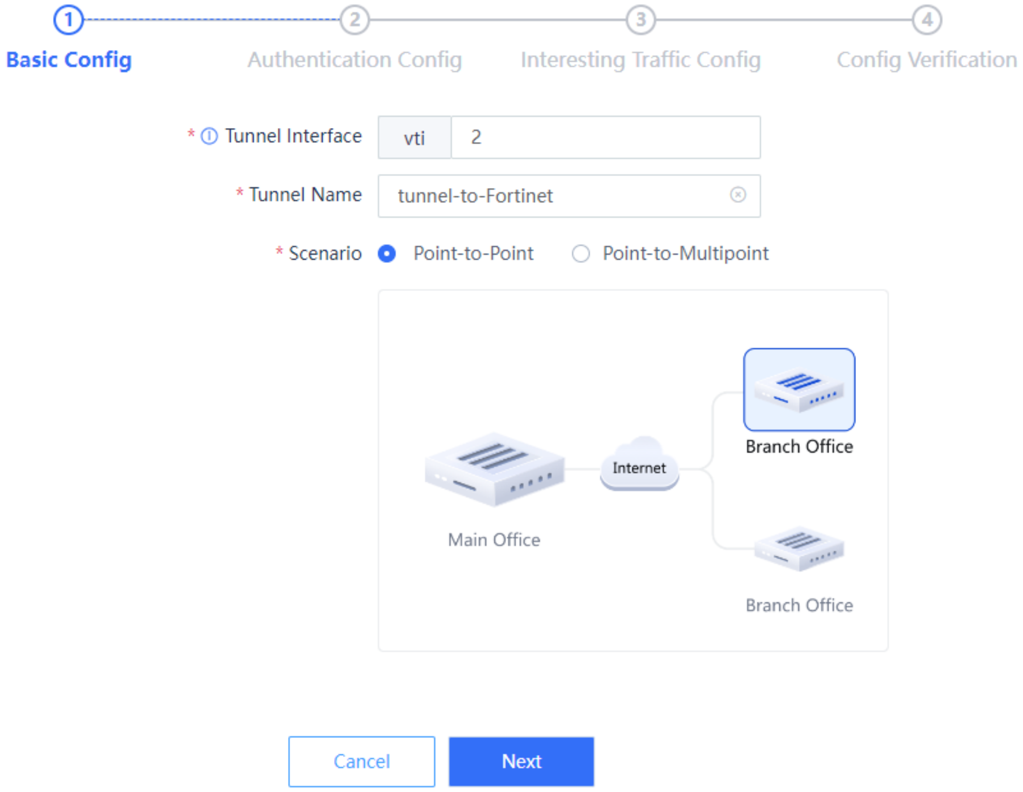
5.5 Procedure

5.5.1 Configuring Spoke A (RG-WALL Z3200-S)

1. **Basic Configuration**

(1) Log in to the RG-WALL Z3200-S firewall and choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 2

* Tunnel Name: tunnel-to-Fortinet

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

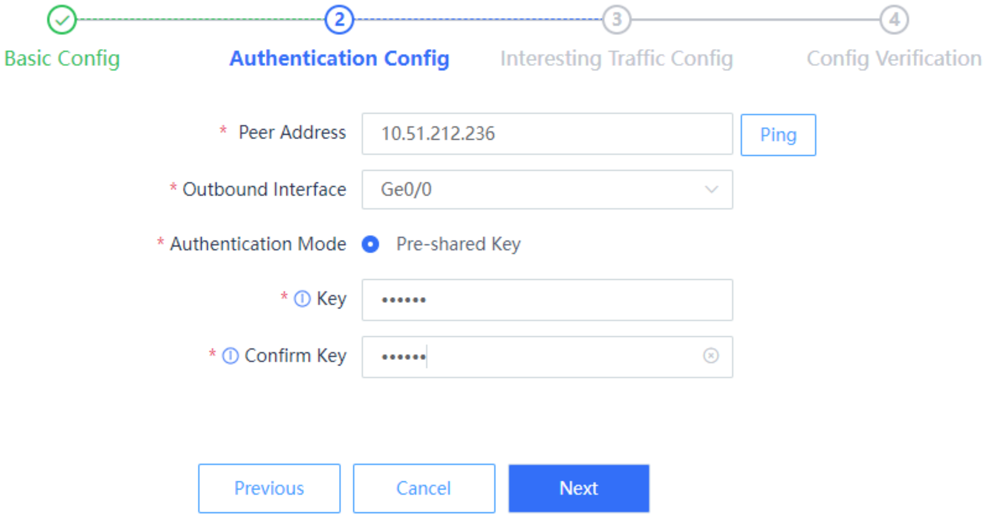
(3) After completing the configuration, click **Next**.

2. **Authentication Configuration**

(1) Configure parameters as follows:

- Set the peer address to the IP address of the Fortinet firewall's WAN interface (10.51.212.236).
- Set the outbound interface to that of the local device (Ge0/0).
- Set the authentication mode to pre-shared key, and set the key to 123123. The pre-shared keys on both ends

of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



* Peer Address: 10.51.212.236

* Outbound Interface: Ge0/0

* Authentication Mode: ● Pre-shared Key

* Key: ••••••

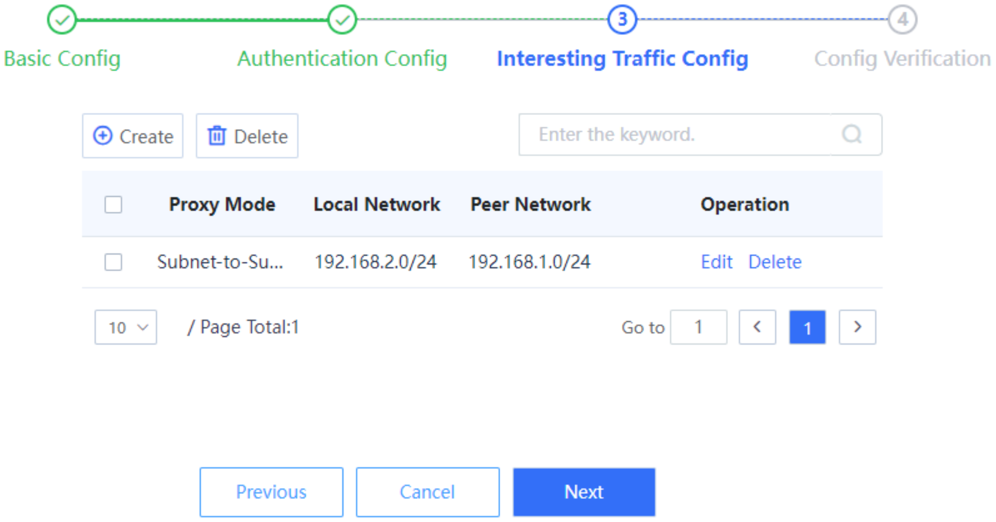
* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Interesting Traffic Configuration

(1) Click **Create**. Configure parameters for interesting traffic according to the following figure.

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set the local network to the subnet 192.168.2.0/24 of the RG-WALL Z3200-S.
- Set the peer network to the subnet 192.168.1.0/24 of the Fortinet firewall.

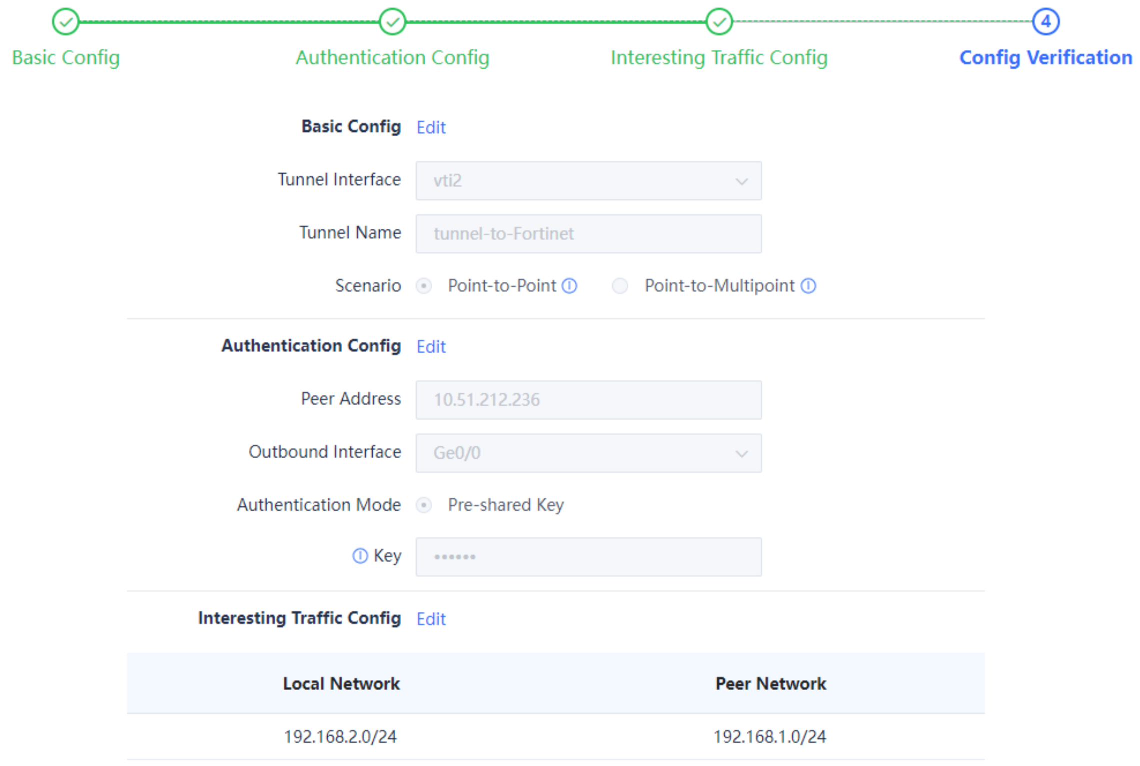


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Su...	192.168.2.0/24	192.168.1.0/24	Edit Delete

(2) After completing the configuration, click **Next**.

4. Verification

(1) Verify that the basic configuration, authentication configuration, and interesting traffic configuration are correct.



Basic Config Edit

Tunnel Interface: vti2

Tunnel Name: tunnel-to-Fortinet

Scenario: ● Point-to-Point ○ Point-to-Multipoint

Authentication Config Edit

Peer Address: 10.51.212.236

Outbound Interface: Ge0/0

Authentication Mode: ● Pre-shared Key

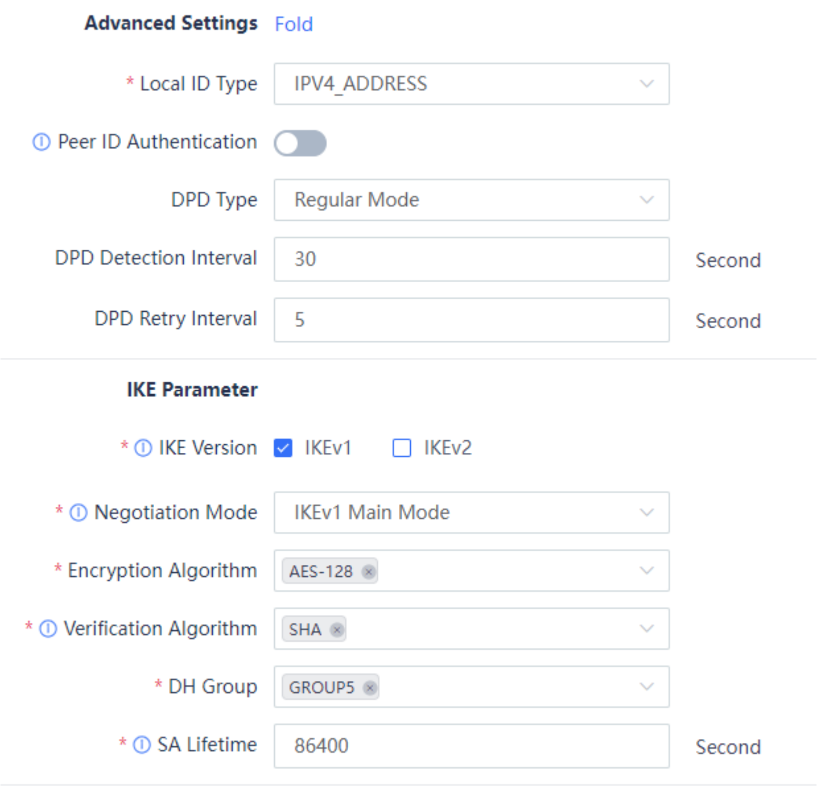
Key: ••••••

Interesting Traffic Config Edit

Local Network	Peer Network
192.168.2.0/24	192.168.1.0/24

(2) Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.

- IKE parameters:
  - Set **IKE Version** to **IKEv1**.
  - Set **Negotiation Mode** to **IKEv1 Main Mode**.
  - Set **Encryption Algorithm** to **AES-128**.
  - Set **Verification Algorithm** to **SHA**.
  - Set **DH Group** to **GROUP5**.



Advanced Settings Fold

* Local ID Type: IPV4_ADDRESS

Peer ID Authentication: ○ (off)

DPD Type: Regular Mode

DPD Detection Interval: 30 Second

DPD Retry Interval: 5 Second

IKE Parameter

* IKE Version: ☑ IKEv1 □ IKEv2

* Negotiation Mode: IKEv1 Main Mode

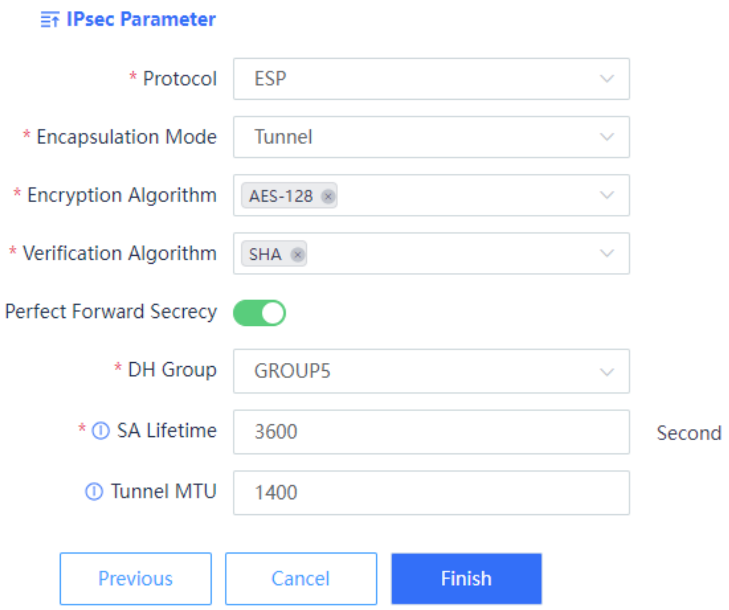
* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 86400 Second

- IPsec parameters:
  - Set **Encryption Algorithm** to **AES-128**.
  - Set **Verification Algorithm** to **SHA**.
  - Enable **Perfect Forward Secrecy**.
  - Set **DH Group** to **GROUP5**.



IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

Perfect Forward Secrecy: ● (on)

* DH Group: GROUP5

* SA Lifetime: 3600 Second

Tunnel MTU: 1400

5.5.2 Configuring Spoke B (RG-WALL Z3200-S)

The configuration steps are the same as those of Spoke A and are not described here.

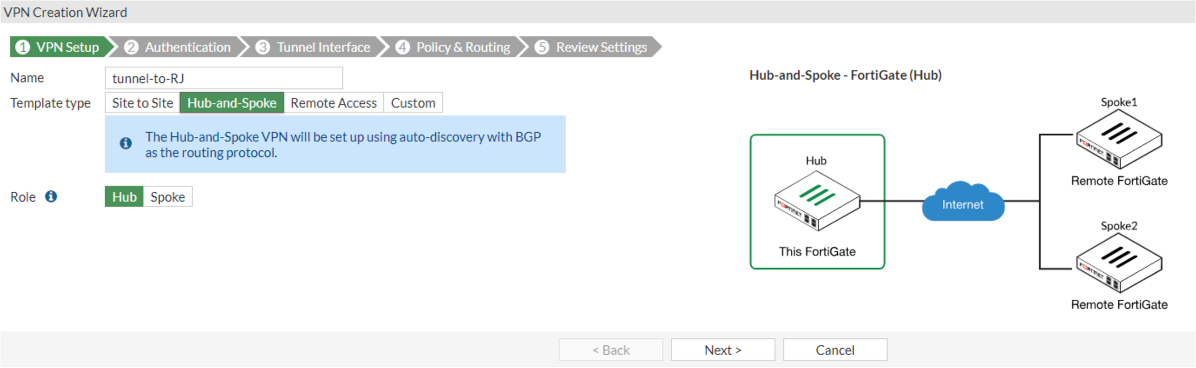
5.5.3 Configuring the Hub Site (Fortinet Firewall)

1. VPN Setup

(1) Log in to the Fortinet firewall and choose **VPN** > **IPsec Wizard**. The configuration wizard page is displayed.

(2) Configure parameters as follows:

- Set **Template type** to **Hub-and-Spoke**.
- Select **Role** to **Hub**.



VPN Creation Wizard

Name: tunnel-to-RJ

Template type: Site to Site | Hub-and-Spoke | Remote Access | Custom (Hub-and-Spoke selected)

The Hub-and-Spoke VPN will be set up using auto-discovery with BGP as the routing protocol.

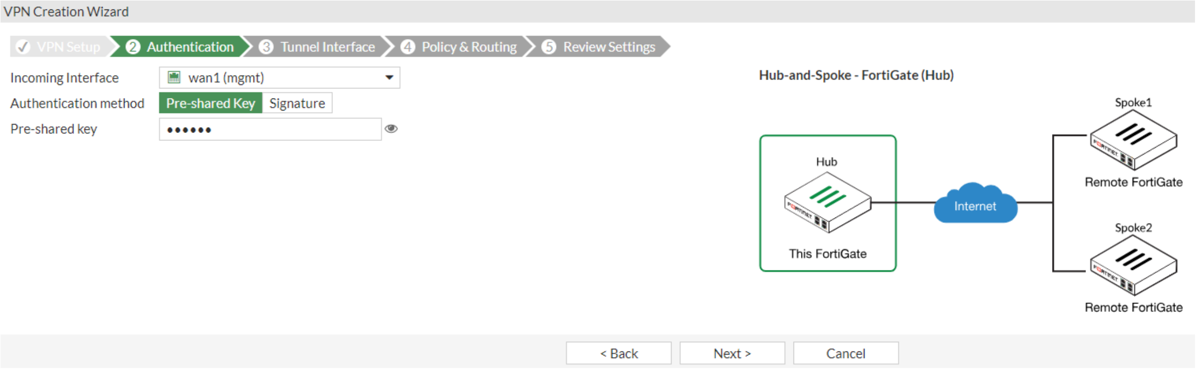
Role: Hub | Spoke (Hub selected)

(3) After completing the configuration, click **Next**.

2. Authentication Configuration

(1) Configure parameters as follows:

- Set **Incoming interface** to the WAN interface of the local device: **wan1(mgmt)**.
- Set **Authentication method** to **Pre-shared Key**, and set the key to 123123. The pre-shared keys on both ends of an IPsec VPN tunnel must be the same. Otherwise, the tunnel cannot be established.



VPN Creation Wizard

Incoming Interface: wan1 (mgmt)

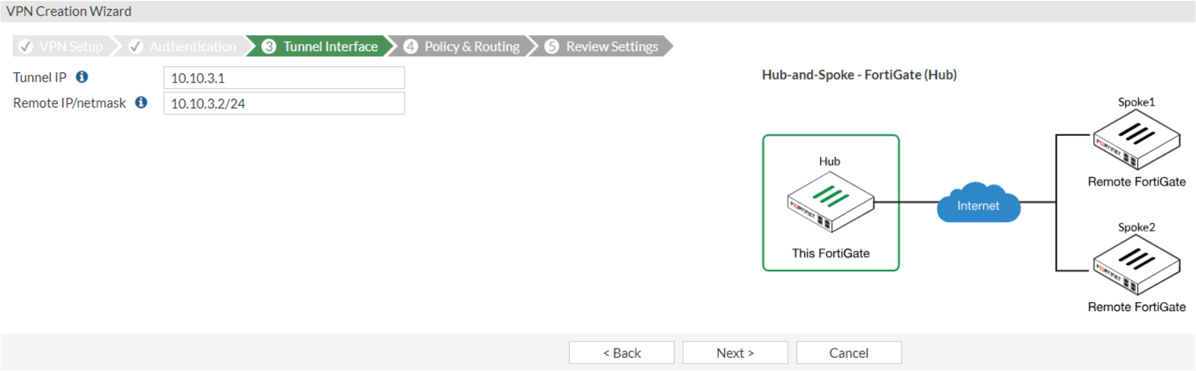
Authentication method: Pre-shared Key | Signature (Pre-shared Key selected)

Pre-shared key: ••••••

(2) After completing the configuration, click **Next**.

3. Tunnel Interface Configuration

Use the default configuration for parameters on this page and click **Next**.



VPN Creation Wizard

✓ VPN Setup ✓ Authentication 3 Tunnel Interface 4 Policy & Routing 5 Review Settings

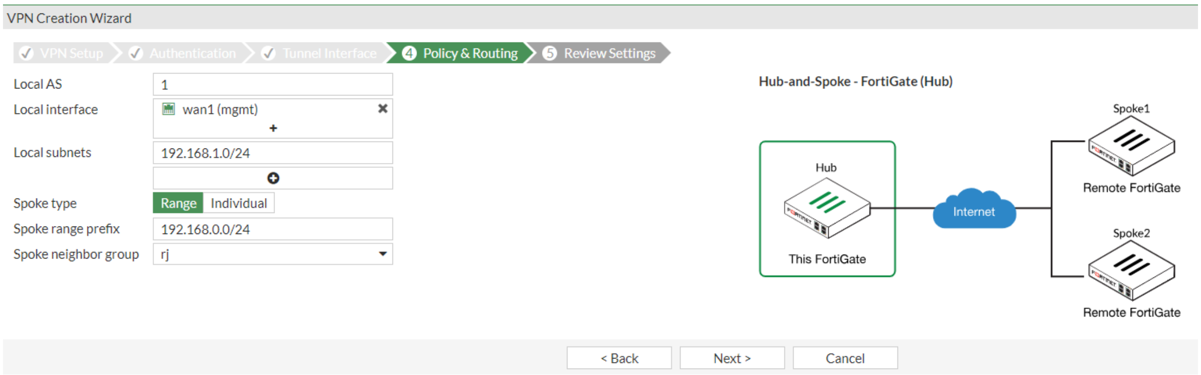
Tunnel IP: 10.10.3.1

Remote IP/netmask: 10.10.3.2/24

4. Policy and Route Configuration

(1) Configure policy and route parameters as follows:

- Set **Local AS** to 1.
- Set **Local interface** to **wan1(mgmt)** of the local device.
- Set **Local subnets** to the subnet 192.168.1.0/24 of the Fortinet firewall.
- Set **Spoke type** to **Range**.
- Set the **Spoke range prefix** to the subnet range 192.168.0.0/16 of the spoke sites.
- For **Spoke neighbor group**, click **Create**. Set **Name** and **Remote AS** as required, and select the local WAN interface **wan1(mgmt)** as the interface.



VPN Creation Wizard

✓ VPN Setup ✓ Authentication ✓ Tunnel Interface 4 Policy & Routing 5 Review Settings

Local AS: 1

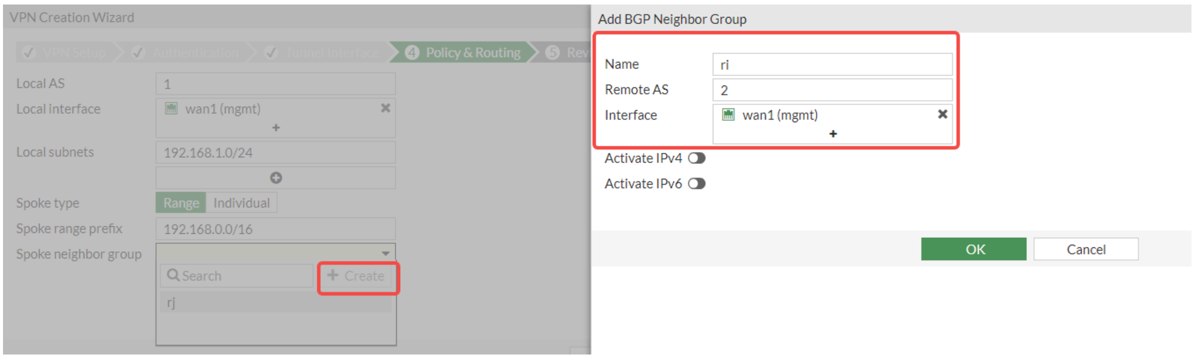
Local interface: wan1 (mgmt)

Local subnets: 192.168.1.0/24

Spoke type: Range | Individual

Spoke range prefix: 192.168.0.0/24

Spoke neighbor group: rj



VPN Creation Wizard

Local AS: 1

Local interface: wan1 (mgmt)

Local subnets: 192.168.1.0/24

Spoke type: Range | Individual

Spoke range prefix: 192.168.0.0/16

Spoke neighbor group: rj

Add BGP Neighbor Group

Name: ri

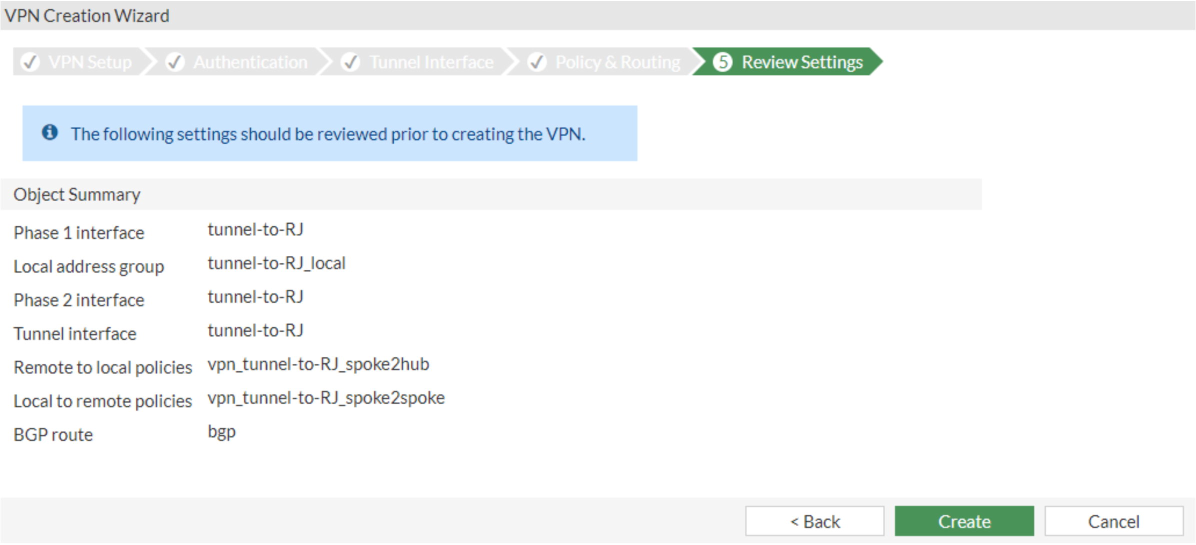
Remote AS: 2

Interface: wan1 (mgmt)

Activate IPv4

Activate IPv6

(2) After completing the configuration, click **Next**. The **Review Settings** page is displayed.



The following settings should be reviewed prior to creating the VPN.

Object Summary

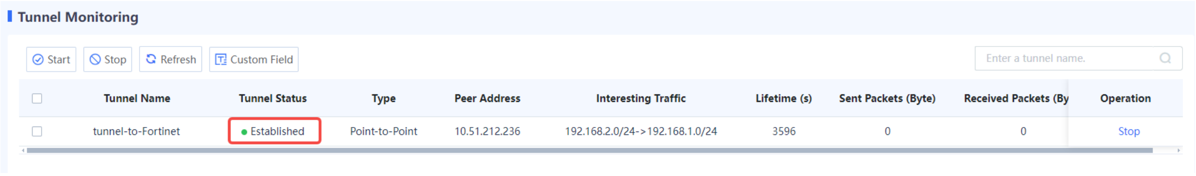
Phase 1 interface	tunnel-to-RJ
Local address group	tunnel-to-RJ_local
Phase 2 interface	tunnel-to-RJ
Tunnel interface	tunnel-to-RJ
Remote to local policies	vpn_tunnel-to-RJ_spoke2hub
Local to remote policies	vpn_tunnel-to-RJ_spoke2spoke
BGP route	bgp

(3) After verifying the configuration, click **Create**.

5.6 Verification

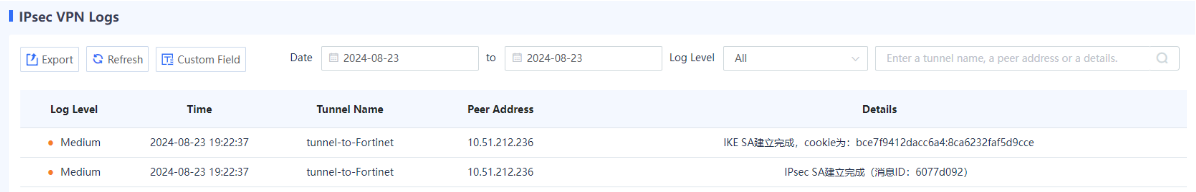
5.6.1 Verifying Configuration of Spoke Sites (Spoke A as an Example)

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. Verify that the tunnel status is **Established**.



□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Received Packets (By	Operation
□	tunnel-to-Fortinet	● Established	Point-to-Point	10.51.212.236	192.168.2.0/24->192.168.1.0/24	3596	0	0	Stop

- Choose **Monitor** > **Log Monitoring** > **IPsec VPN Log**. Check IPsec tunnel negotiation logs.

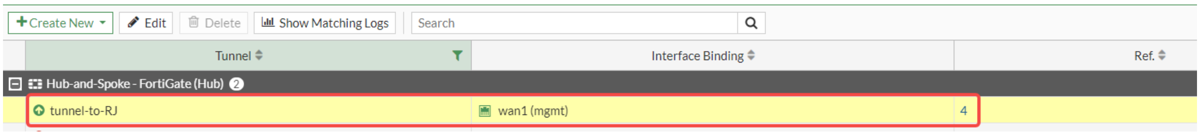


Date 2024-08-23 to 2024-08-23 Log Level All

Log Level	Time	Tunnel Name	Peer Address	Details
● Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IKE SA建立完成，cookie为：bce7f9412dacc6a4:8ca6232faf5d9cce
● Medium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IPsec SA建立完成（消息ID：6077d092）

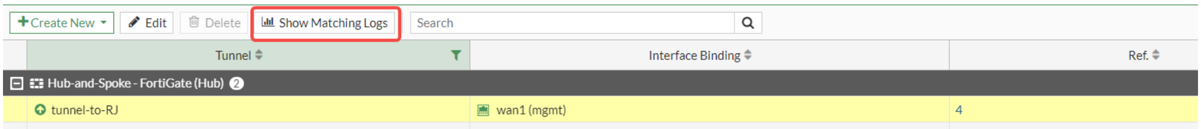
5.6.2 Verifying Configuration of the Hub Site (Fortinet Firewall)

- Choose **VPN** > **IPsec Tunnels**. Verify that the tunnel status is established.

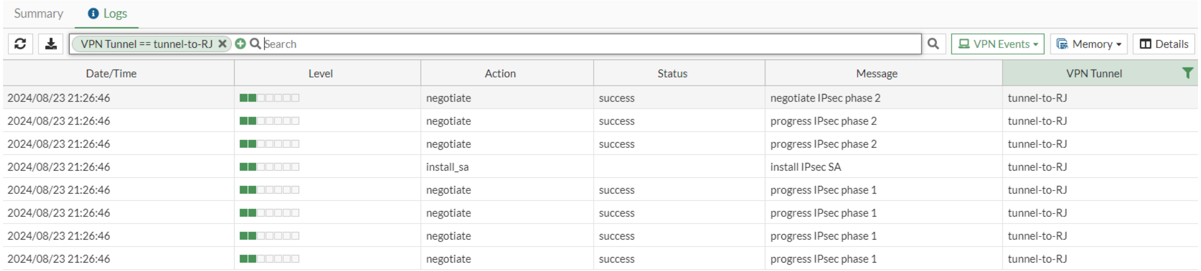


Tunnel	Interface Binding	Ref.
Hub-and-Spoke - FortiGate (Hub) 2		
tunnel-to-RJ	wan1 (mgmt)	4

- Select the IPsec tunnel and click **Show Matching Logs** to view IPsec tunnel negotiation logs.



Tunnel	Interface Binding	Ref.
Hub-and-Spoke - FortiGate (Hub) 2		
tunnel-to-RJ	wan1 (mgmt)	4



Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/08/23 21:26:46	■■□□□□□	negotiate	success	negotiate IPsec phase 2	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 2	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 2	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	install_sa		install IPsec SA	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-RJ
2024/08/23 21:26:46	■■□□□□□	negotiate	success	progress IPsec phase 1	tunnel-to-RJ

6 Configuration Examples of IPsec VPN with NAT Traversal

6.1 Applicable Products and Versions

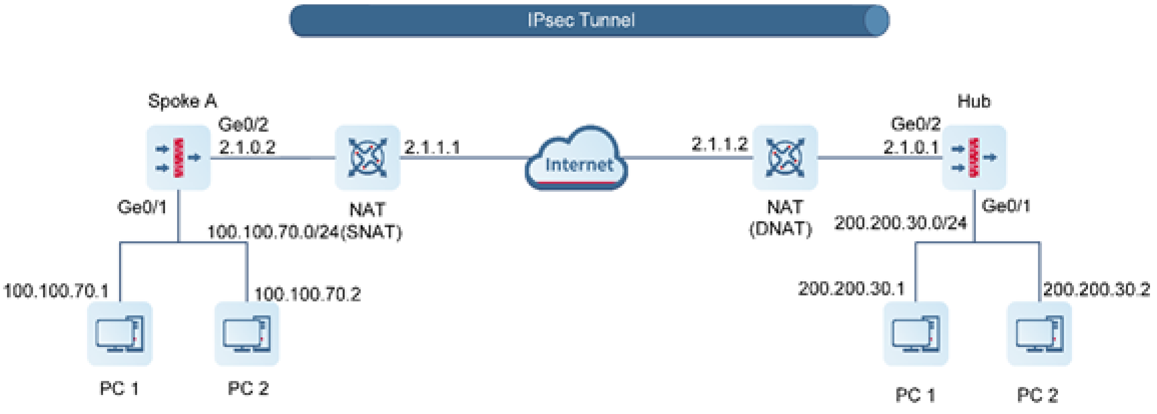
Table 6-1 Products and Versions

Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R6 or later

6.2 Service Demands

In a scenario of IPsec VPN with NAT traversal, static NAT (SNAT) needs to be deployed for Spoke A to initiate a connection with the hub site, and dynamic NAT (DNAT) needs to be deployed for the hub site. Figure 6-1 shows the typical networking diagram.

Figure 6-1 Networking of IPsec VPN with NAT Traversal



6.3 Restrictions and Guidelines

- In IPsec, the default port that supports NAT traversal is UDP port 4500. A custom port is not supported.

6.4 Prerequisites

You have completed basic network configurations, including interface IP address and routing information on routers and servers.

6.5 Procedure

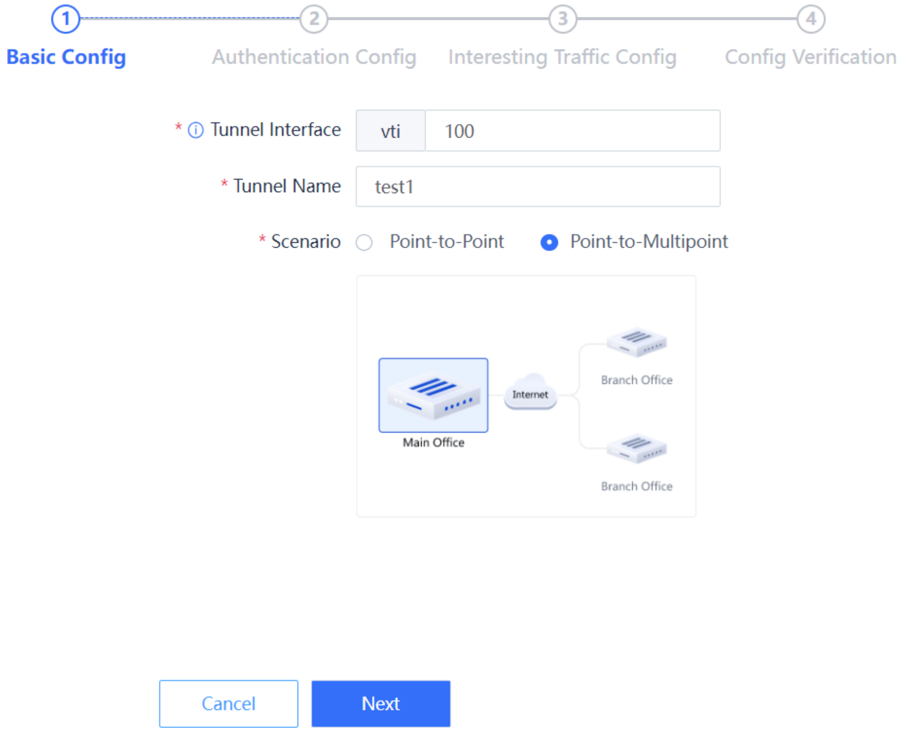
6.5.1 Using a Configuration Wizard

1. Configuring the Hub Site

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Site-to-Multisite**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 100

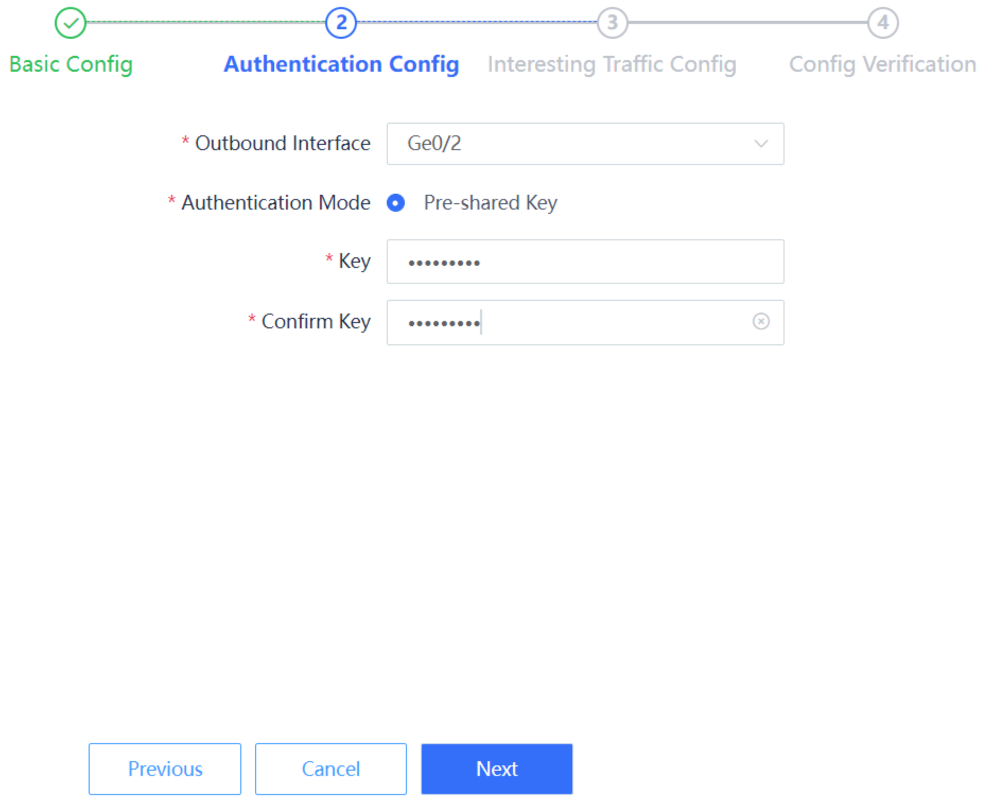
* Tunnel Name: test1

* Scenario: ○ Point-to-Point ● Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.



* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

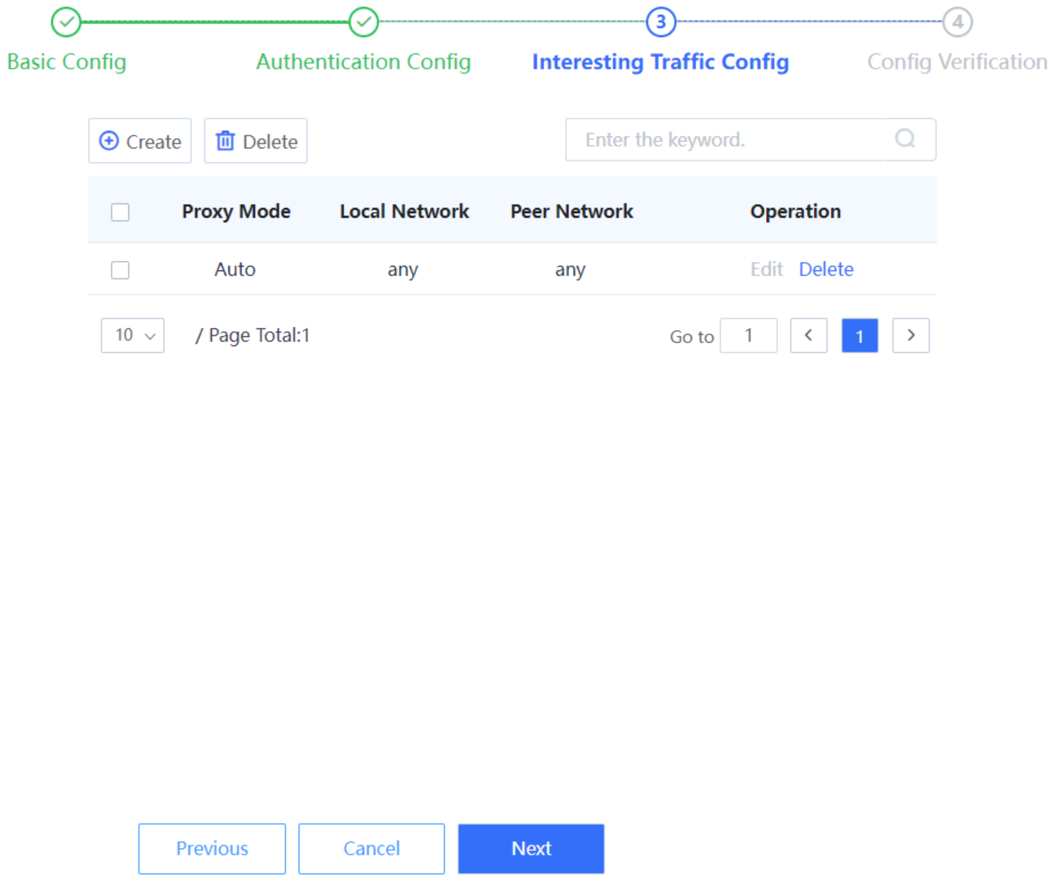
* Key: •••••••••

* Confirm Key: •••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

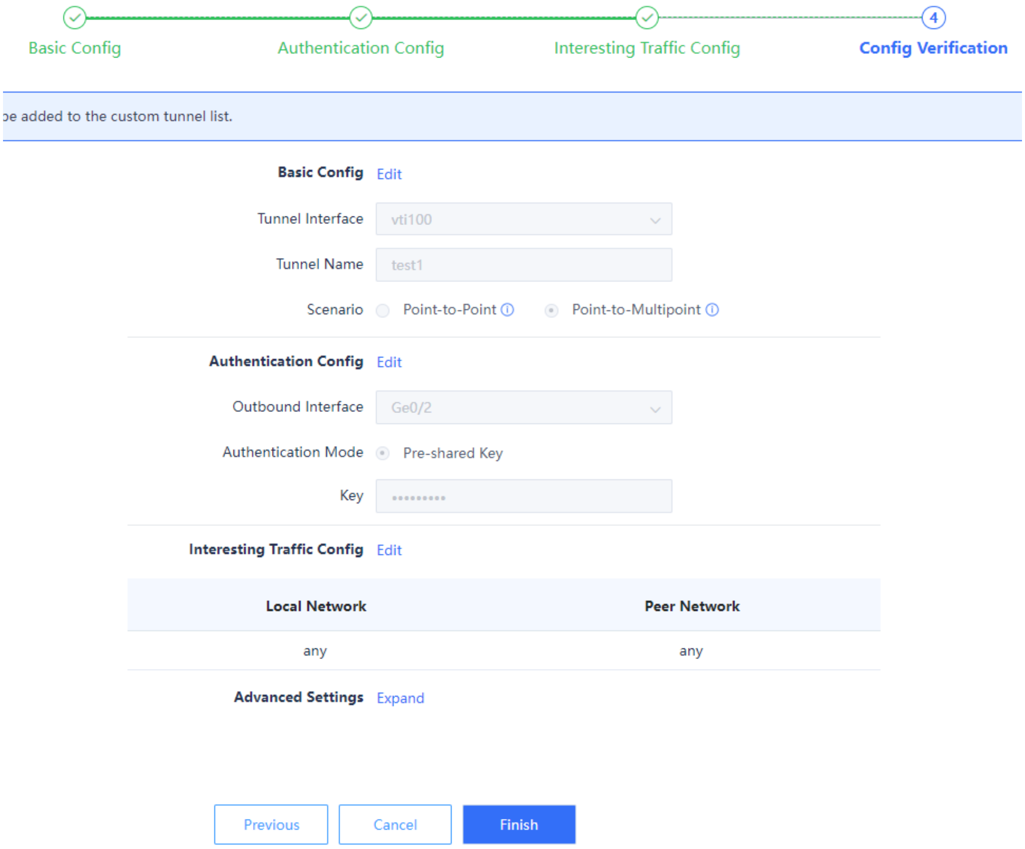


□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



pe added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti100

Tunnel Name: test1

Scenario: ○ Point-to-Point ⓘ ● Point-to-Multipoint ⓘ

Authentication Config Edit

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: •••••••••

Interesting Traffic Config Edit

Local Network	Peer Network
any	any

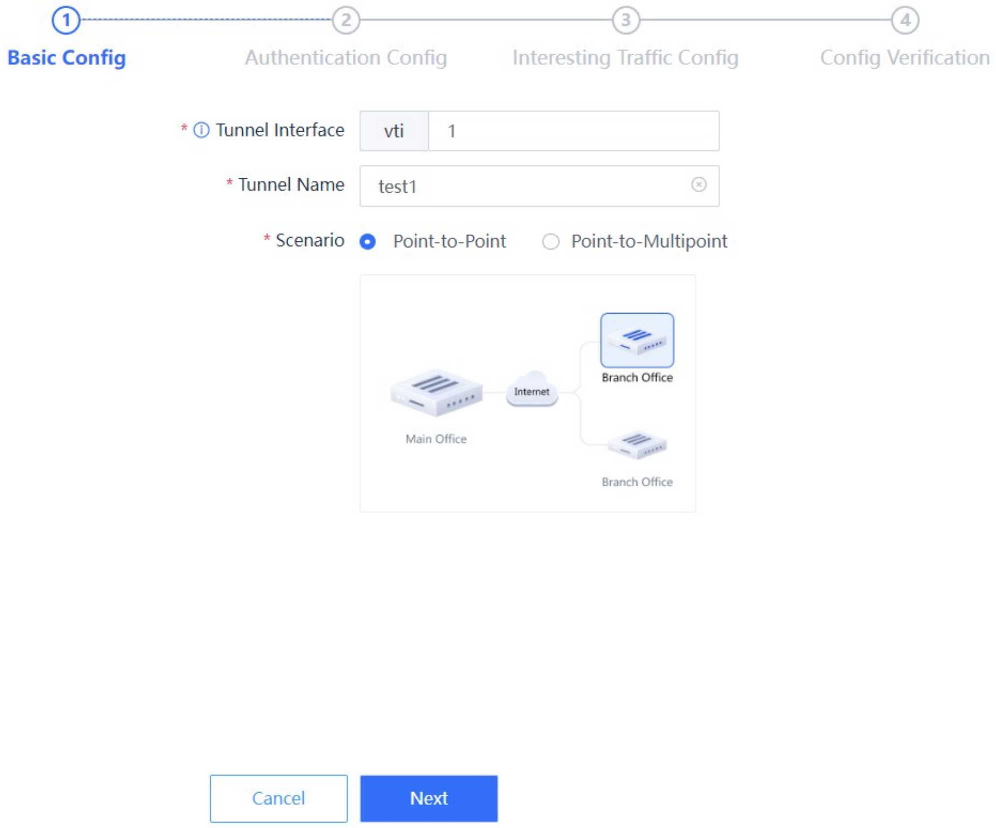
Advanced Settings Expand

2. Configuring Spoke A

(1) Perform basic configuration.

a Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

b Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



1 Basic Config — 2 Authentication Config — 3 Interesting Traffic Config — 4 Config Verification

* ⓘ Tunnel Interface: vti 1

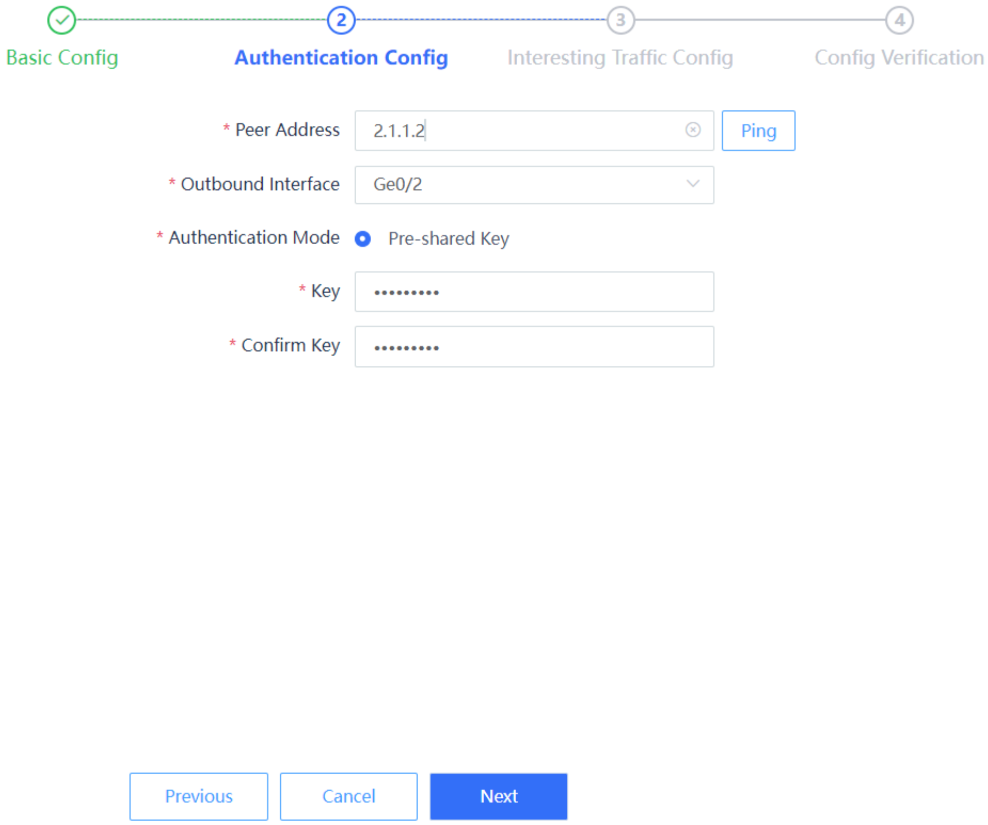
* Tunnel Name: test1

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

c After completing the configuration, click **Next**.

(2) Configure authentication.

a Configure parameters according to the following figure.



* Peer Address: 2.1.1.2

* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

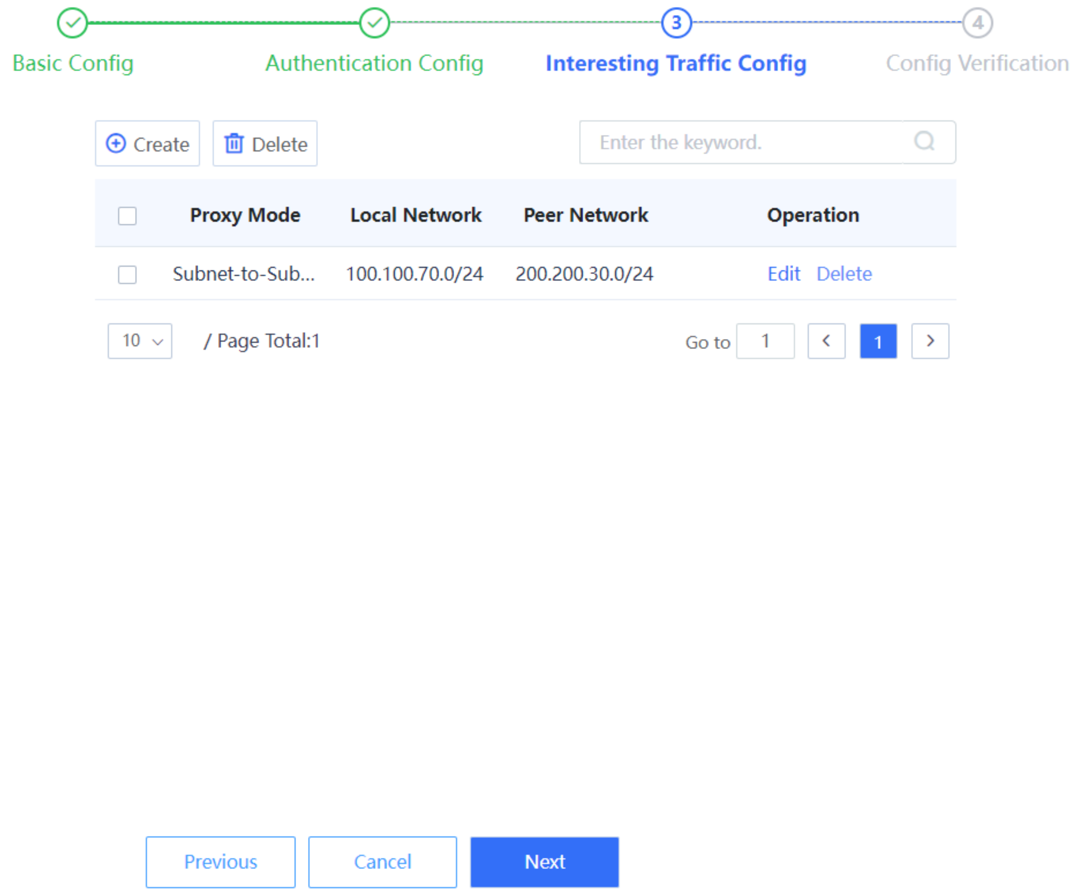
* Key: •••••••••

* Confirm Key: •••••••••

b After completing the configuration, click **Next**.

(3) Configure interesting traffic.

a Click **Create**. Configure parameters for interesting traffic according to the following figure.

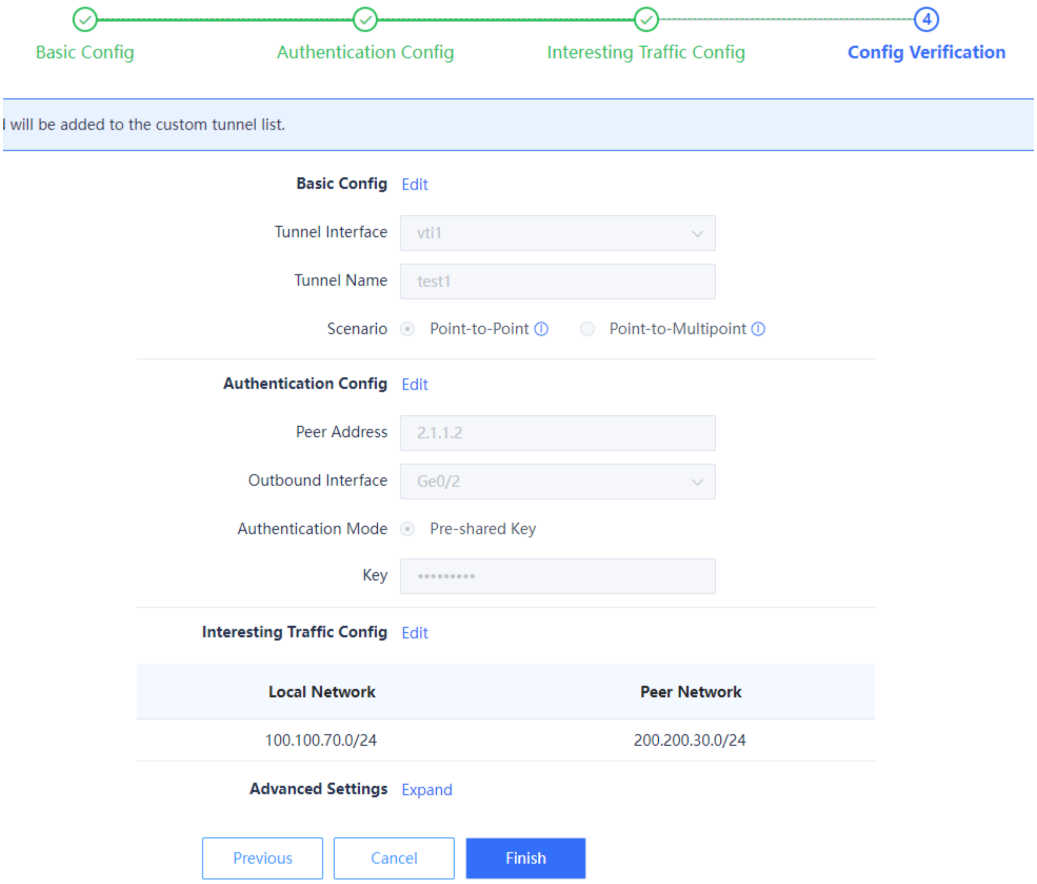


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Sub...	100.100.70.0/24	200.200.30.0/24	Edit Delete

b After completing the configuration, click **Next**.

(4) Verify configuration.

a After verifying the configuration, click **Finish**.



l will be added to the custom tunnel list.

Basic Config

Tunnel Interface: vti1

Tunnel Name: test1

Scenario: ● Point-to-Point ○ Point-to-Multipoint

Authentication Config

Peer Address: 2.1.1.2

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: •••••••••

Interesting Traffic Config

Local Network	Peer Network
100.100.70.0/24	200.200.30.0/24

Advanced Settings

6.5.2 Manually Configuring a Tunnel

1. Configuring the Hub Site

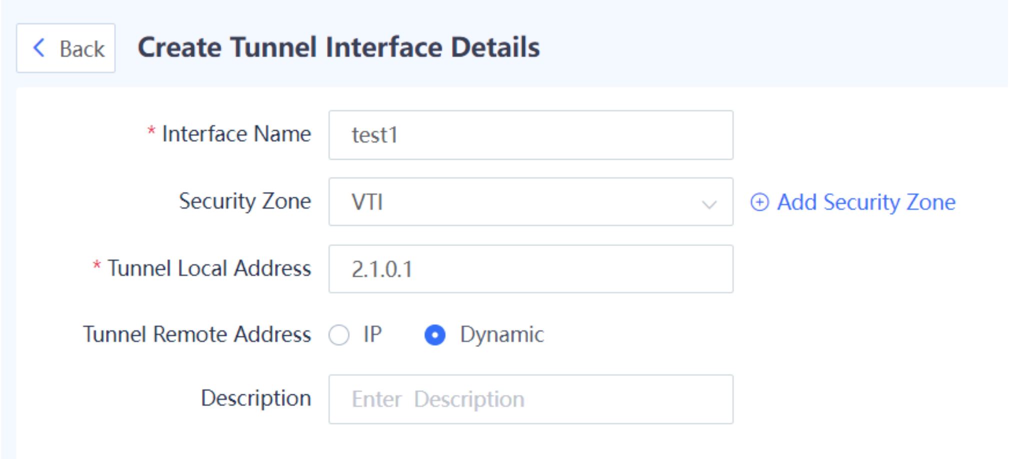
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **test1**.
- Add security zone **VTI** and set **Security Zone** to **VTI** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of the hub site: 2.1.0.1. Set **Tunnel Remote Address** to **Dynamic**.



* Interface Name: test1

Security Zone: VTI

* Tunnel Local Address: 2.1.0.1

Tunnel Remote Address: ○ IP ● Dynamic

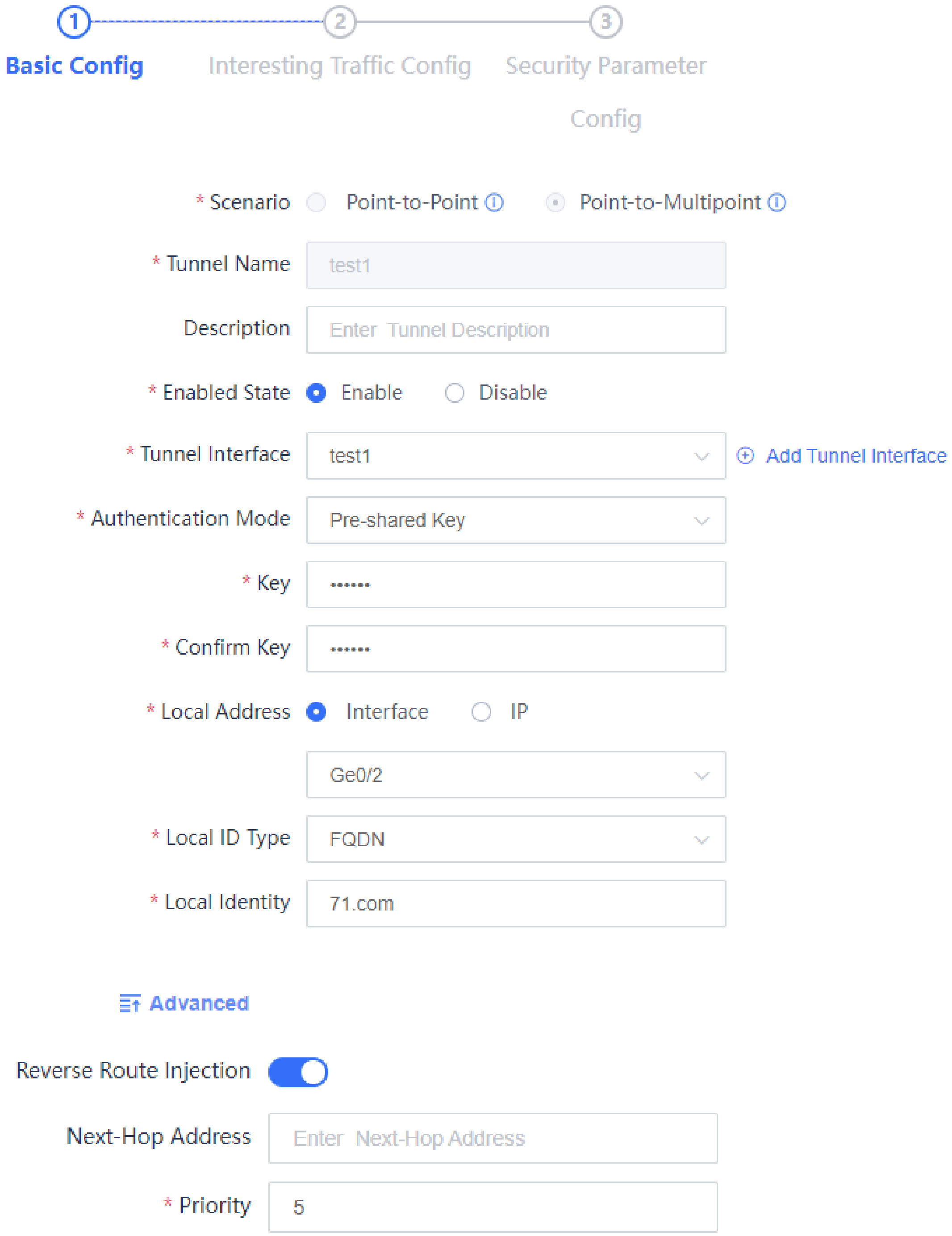
Description: Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **test1**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **test1**.
- Set **Local Address** to **interface Ge0/2**.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.
- Toggle on **Reverse Route Injection** for the hub site. For **Priority**, use the default value 5. Do not configure **Next-Hop Address**.



* Scenario ○ Point-to-Point ● Point-to-Multipoint

* Tunnel Name test1

Description Enter Tunnel Description

* Enabled State ● Enable ○ Disable

* Tunnel Interface test1

* Authentication Mode Pre-shared Key

* Key ••••••

* Confirm Key ••••••

* Local Address ● Interface ○ IP

Ge0/2

* Local ID Type FQDN

* Local Identity 71.com

Reverse Route Injection ●

Next-Hop Address Enter Next-Hop Address

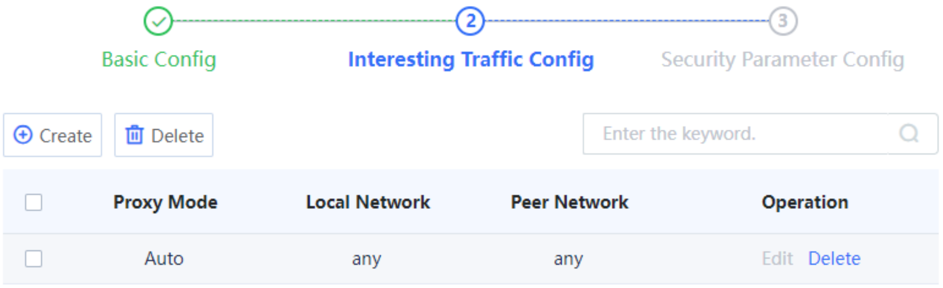
* Priority 5

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Auto**.



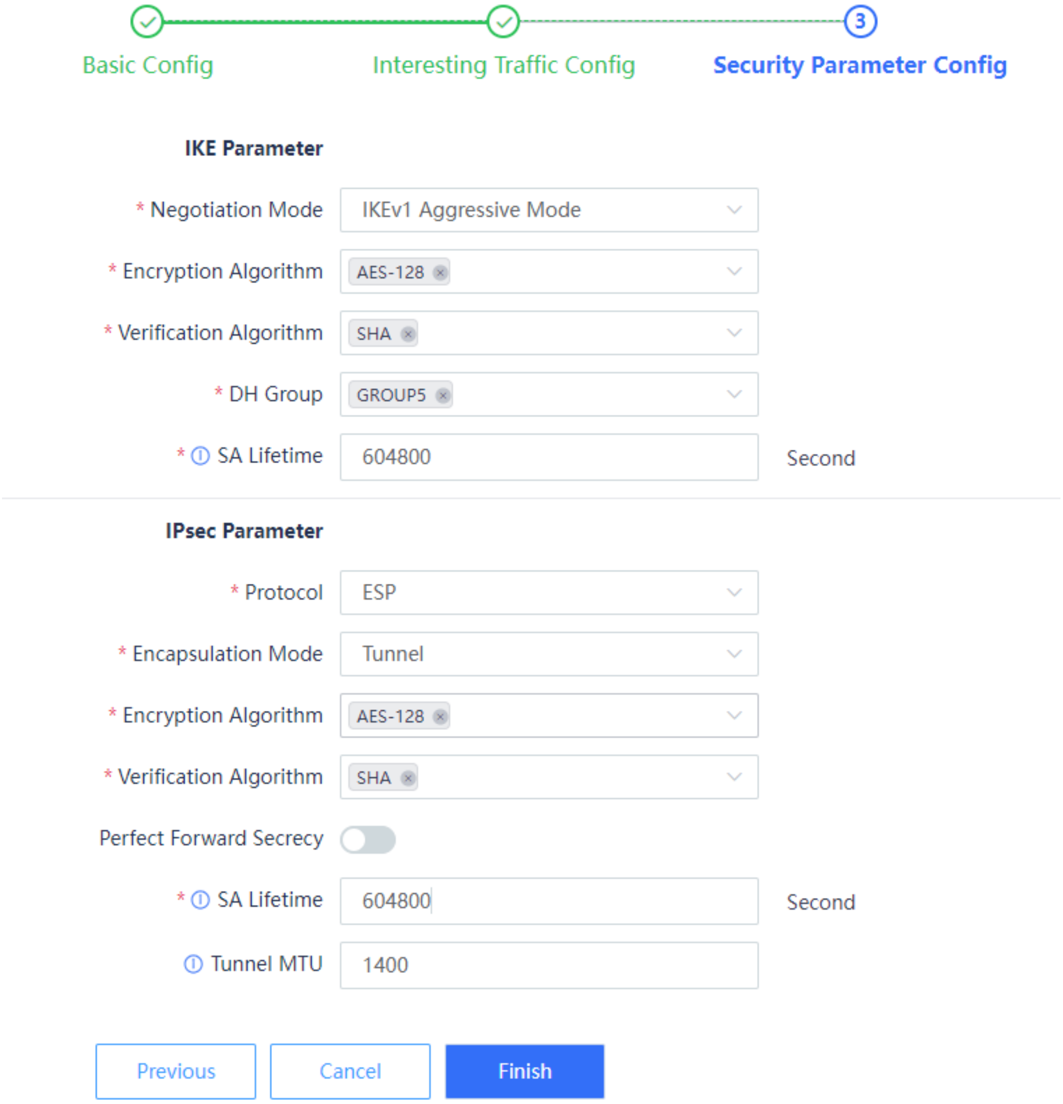
□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Aggressive Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 604800 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 604800 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode	IKEv1 Aggressive Mode	
* Encryption Algorithm	AES-128	
* Verification Algorithm	SHA	
* DH Group	GROUP5	
* SA Lifetime	604800	Second

IPsec Parameter

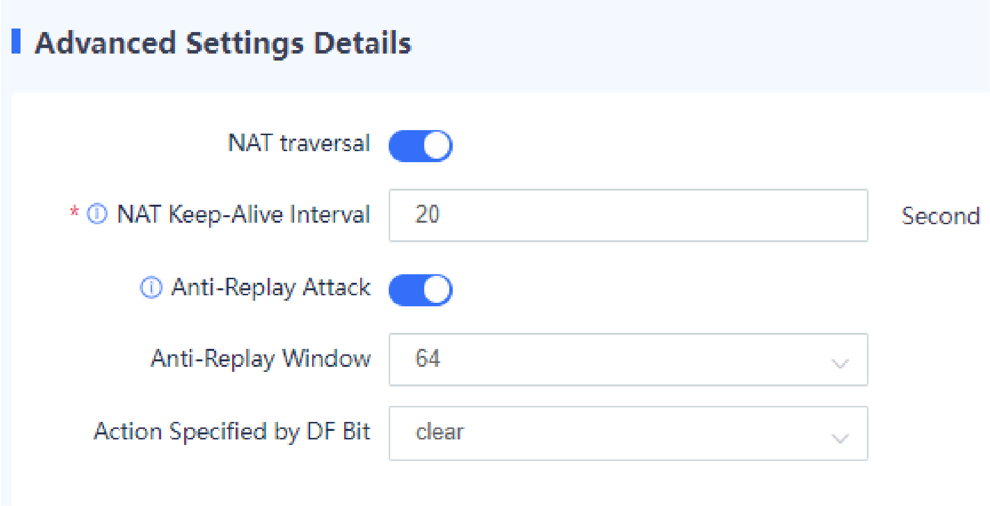
* Protocol	ESP	
* Encapsulation Mode	Tunnel	
* Encryption Algorithm	AES-128	
* Verification Algorithm	SHA	
Perfect Forward Secrecy	○	
* SA Lifetime	604800	Second
Tunnel MTU	1400	

Click **Finish** to complete the IPsec tunnel configuration for the hub site.

(3) Configure advanced IPsec settings.

On a network with NAT, enable NAT traversal for IPsec, and configure the NAT keep-alive interval.

Choose **Network** > **IPsec VPN** > **Advanced Settings Details**. On the advanced IPsec settings page, verify that NAT traversal is enabled, configure a proper NAT keep-alive interval, and click **Save**.



Advanced Settings Details

NAT traversal: ●

* ⓘ NAT Keep-Alive Interval: 20 Second

ⓘ Anti-Replay Attack: ●

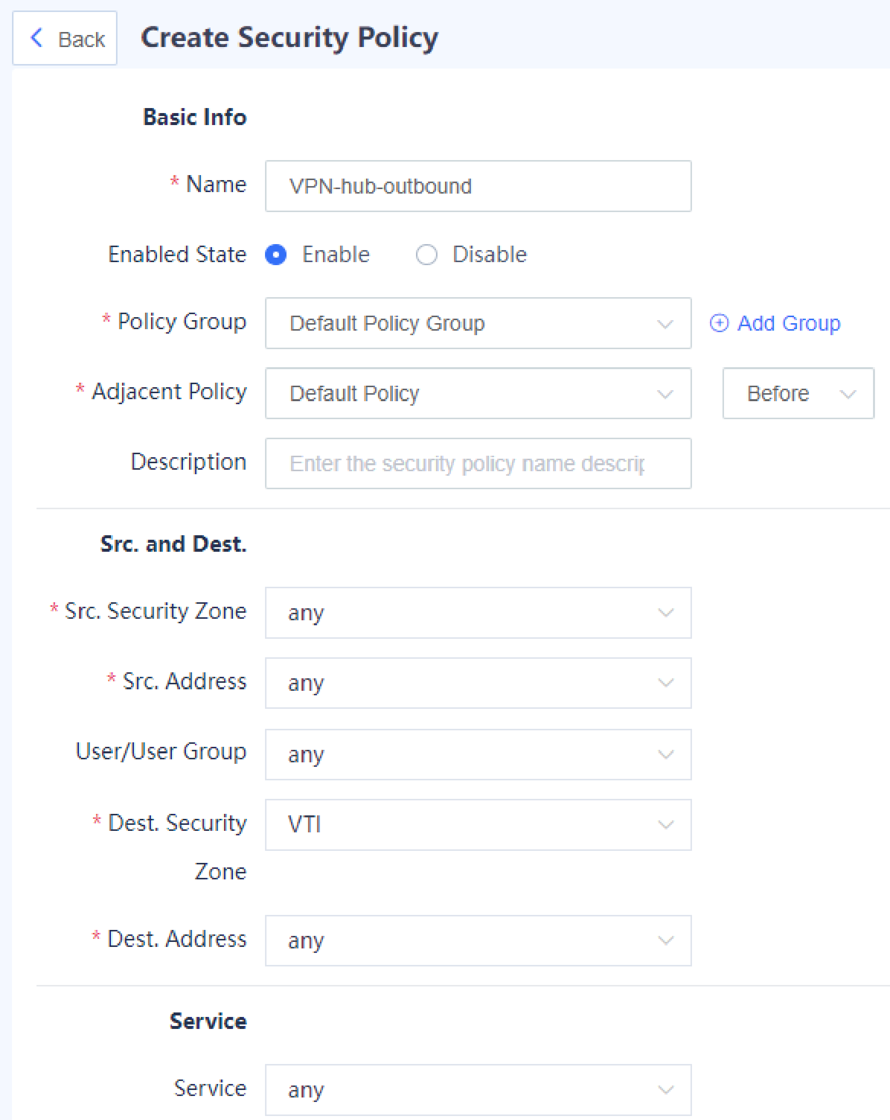
Anti-Replay Window: 64

Action Specified by DF Bit: clear

(4) Create security policies.

a Choose **Policy** > **Security Policy** > **Security Policy**.

b On the page that is displayed, click **Create** and create outbound security policy **VPN-hub-outbound** and inbound security policy **VPN-hub-inbound** separately.



< Back **Create Security Policy**

Basic Info

* Name: VPN-hub-outbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

* Adjacent Policy: Default Policy Before

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: any

* Src. Address: any

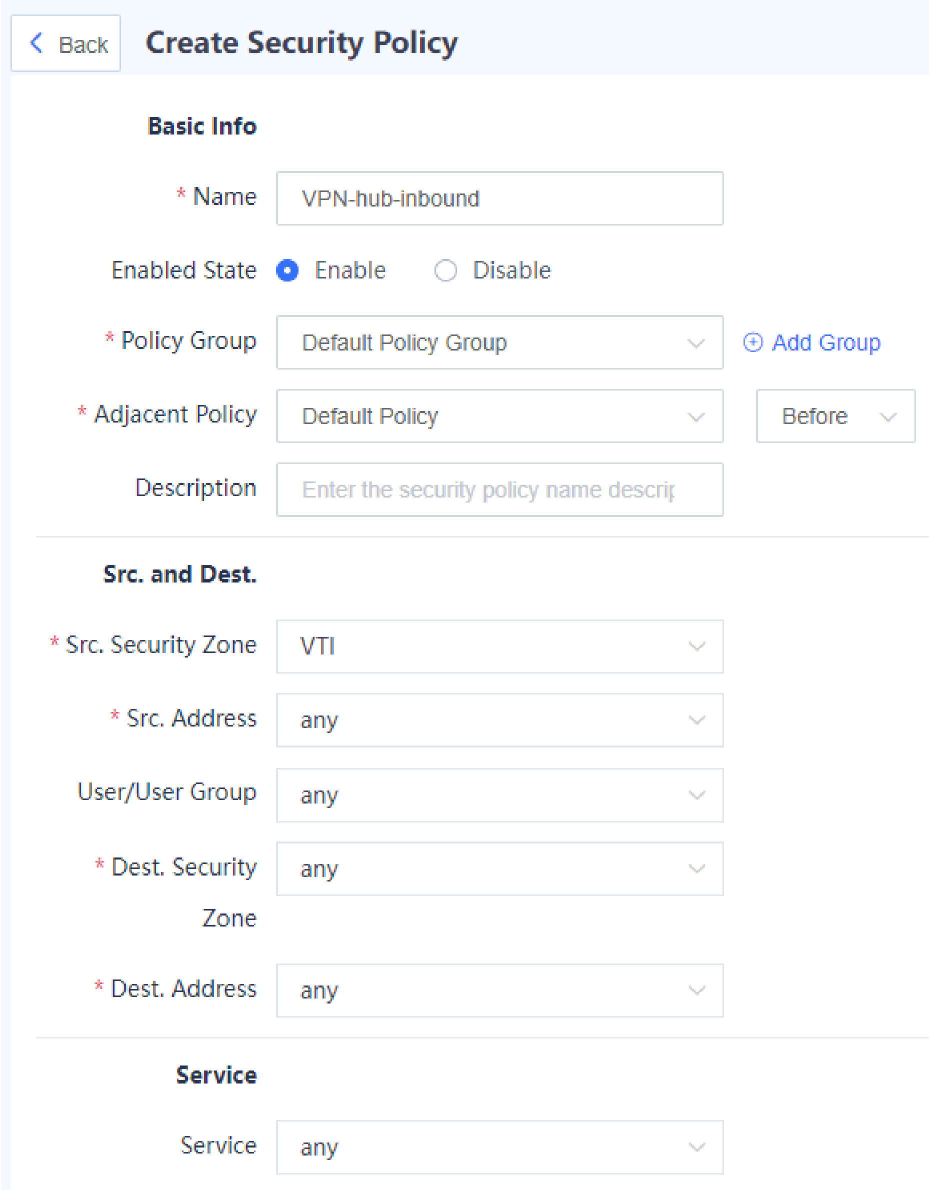
User/User Group: any

* Dest. Security Zone: VTI

* Dest. Address: any

Service

Service: any



Basic Info

* Name: VPN-hub-inbound

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

* Adjacent Policy: Default Policy | Before

Description: Enter the security policy name descrip

Src. and Dest.

* Src. Security Zone: VTI

* Src. Address: any

User/User Group: any

* Dest. Security Zone: any

* Dest. Address: any

Service

Service: any

2. Configuring Spoke A

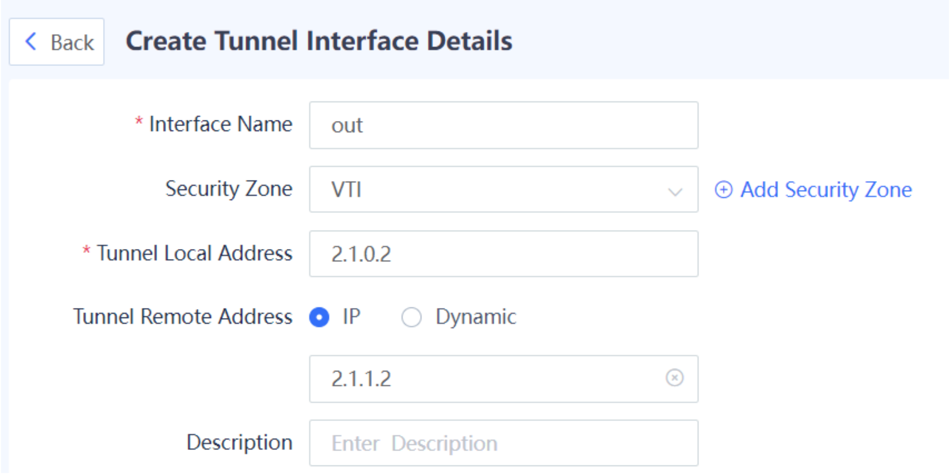
(1) Configure a tunnel interface.

a Choose **Network** > **Interface** > **Tunnel Interface**.

b On the page that is displayed, click **Create**.

c On the tunnel interface configuration page that is displayed, configure parameters as follows:

- Set **Interface Name** to **out**.
- Add security zone VTI and set **Security Zone** to **VTI** for this interface.
- Set **Tunnel Local Address** to the default outbound interface address of Site A: 2.1.0.2.
- Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 2.1.1.2.



Create Tunnel Interface Details

* Interface Name: out

Security Zone: VTI

* Tunnel Local Address: 2.1.0.2

Tunnel Remote Address: ● IP ○ Dynamic

2.1.1.2

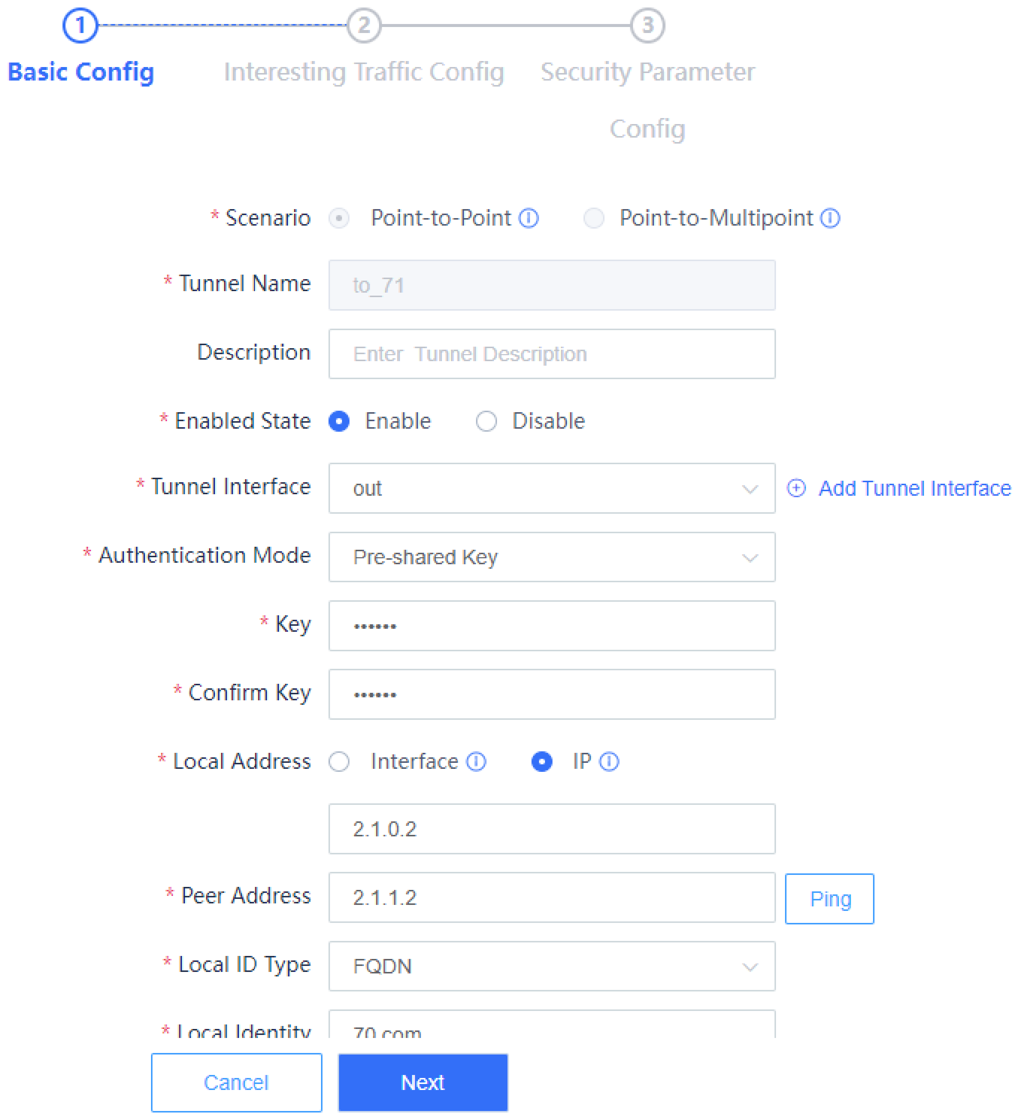
Description: Enter Description

(2) Configure an IPsec tunnel.

a Perform basic configuration.

Choose **Network** > **IPsec VPN** > **Custom Tunnel**. Click **Create**. On the basic configuration page of the custom tunnel, configure parameters as follows:

- Set **Tunnel Name** to **to_71**.
- Set **Enabled State** to **Enable**.
- Set **Tunnel Interface** to **out**.
- Set **Local Address** to 2.1.0.2, and **Peer Address** to 2.1.1.2.
- For **Authentication Mode**, use the default value **Pre-shared Key**. Set both **Key** and **Confirm Key** to **ruijie123**.



* Scenario ○ Point-to-Point ⓘ ○ Point-to-Multipoint ⓘ

* Tunnel Name: to_71

Description: Enter Tunnel Description

* Enabled State ● Enable ○ Disable

* Tunnel Interface: out

* Authentication Mode: Pre-shared Key

* Key: ••••••

* Confirm Key: ••••••

* Local Address ○ Interface ⓘ ● IP ⓘ

2.1.0.2

* Peer Address: 2.1.1.2

* Local ID Type: FQDN

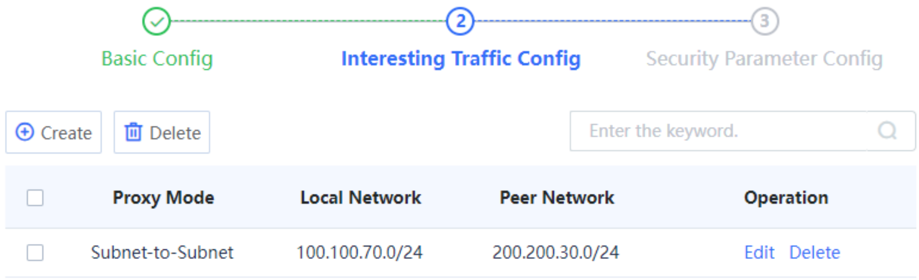
* Local Identity: 70.com

After completing the basic configuration, click **Next**.

b Configure interesting traffic.

On the interesting traffic configuration page, click **Create**. Then configure parameters as follows:

- Set **Proxy Mode** to **Subnet-to-Subnet**.
- Set **Local Network** to 100.100.70.0/24 and **Peer Network** to 200.200.30.0/24.



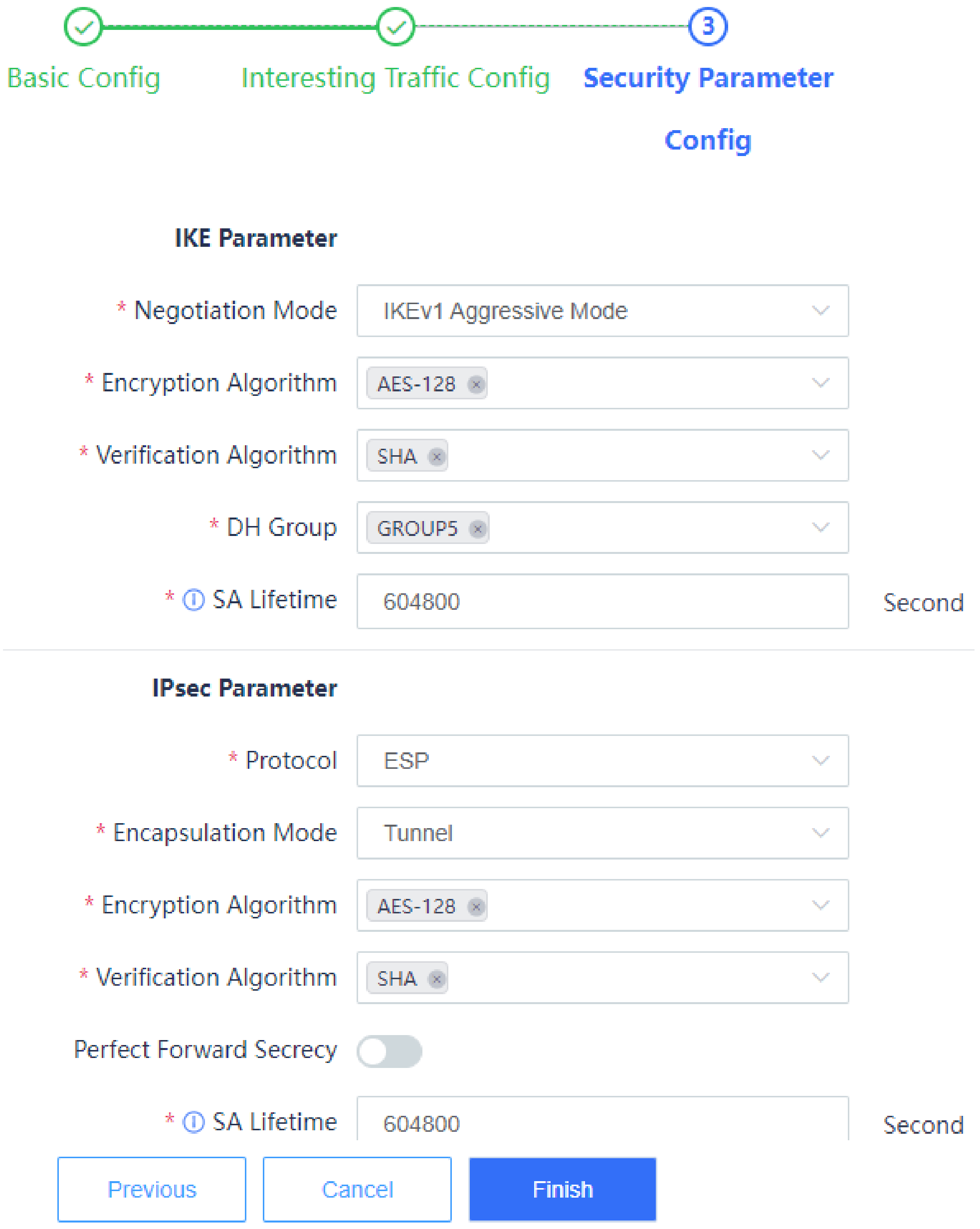
□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	100.100.70.0/24	200.200.30.0/24	Edit Delete

After completing the configuration for interesting traffic, click **Next**.

c Configure security parameters.

On the security parameter configuration page, configure IKE and IPsec parameters and ensure that the configuration matches that on the peer device.

- IKE parameters: Set **Negotiation Mode** to **IKEv1 Aggressive Mode**, **Encryption Algorithm** to **AES-128**, **Verification Algorithm** to **SHA**, **DH Group** to **GROUP5**, and **SA Lifetime** to 604800 (in seconds).
- IPsec parameters: Set **Protocol** to **ESP**, **Encapsulation Mode** to **Tunnel**, **Encryption Algorithm** to **AES-128**, and **Verification Algorithm** to **SHA**. Do not toggle on **Perfect Forward Secrecy**. Set **SA Lifetime** to 604800 (in seconds) and **Tunnel MTU** to 1400.



IKE Parameter

* Negotiation Mode: IKEv1 Aggressive Mode

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* SA Lifetime: 604800 Second

IPsec Parameter

* Protocol: ESP

* Encapsulation Mode: Tunnel

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

Perfect Forward Secrecy: ○

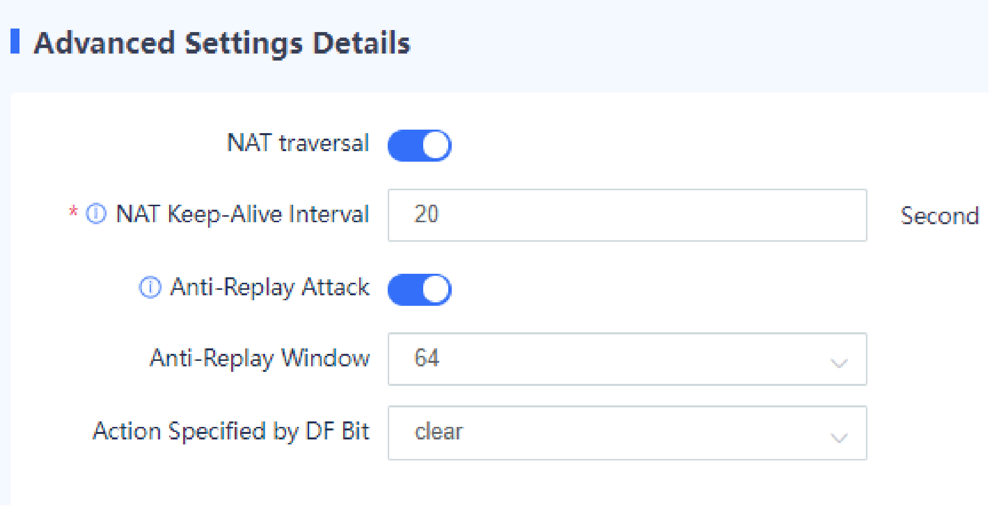
* SA Lifetime: 604800 Second

Click **Finish** to complete the configuration for the IPsec tunnel.

(3) Configure advanced IPsec settings.

On a network with NAT, enable NAT traversal for IPsec, and configure the NAT keep-alive interval.

Choose **Network** > **IPsec VPN** > **Advanced Settings Details**. On the advanced IPsec settings page, verify that NAT traversal is enabled, configure a proper NAT keep-alive interval, and click **Save**.



Advanced Settings Details

NAT traversal: on

* NAT Keep-Alive Interval: 20 Second

Anti-Replay Attack: on

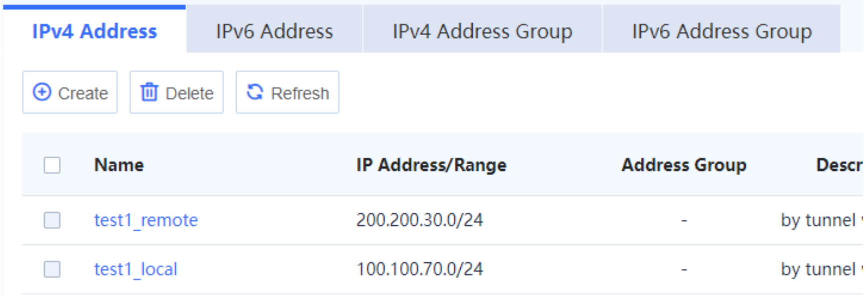
Anti-Replay Window: 64

Action Specified by DF Bit: clear

(4) Create security policies.

a Choose **Object** > **Address** > **IPv4 Address**.

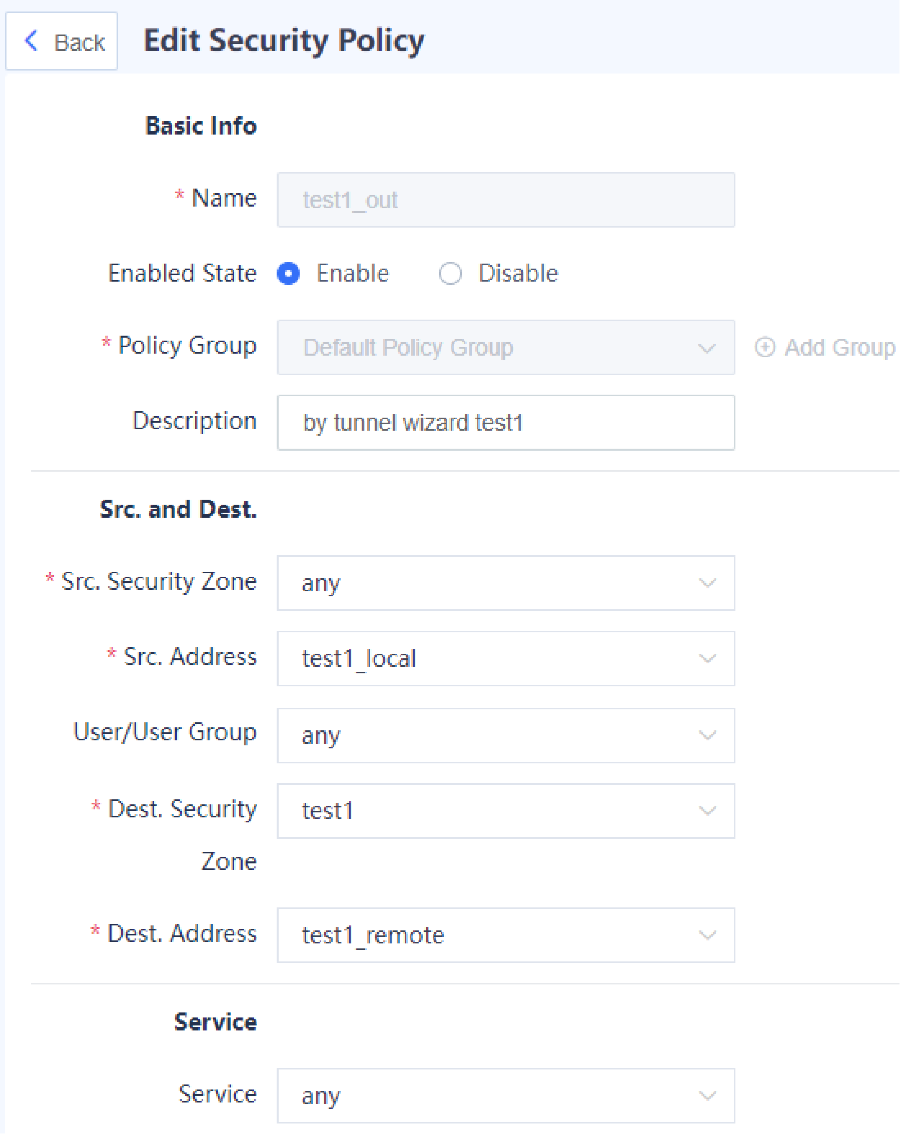
b On the page that is displayed, click **Create** to create two address objects **test1_local** and **test1_remote** separately. Set **IP Address/Range** to local network address 100.100.70.0/24 and peer network address 200.200.30.0/24 in the interesting traffic for the two address objects, respectively.



□	Name	IP Address/Range	Address Group	Descr
□	test1_remote	200.200.30.0/24	-	by tunnel
□	test1_local	100.100.70.0/24	-	by tunnel

c Choose **Policy** > **Security Policy** > **Security Policy**.

d On the page that is displayed, click **Create** and create outbound security policy **test1_out** and inbound security policy **test1_in** separately.



Edit Security Policy

Basic Info

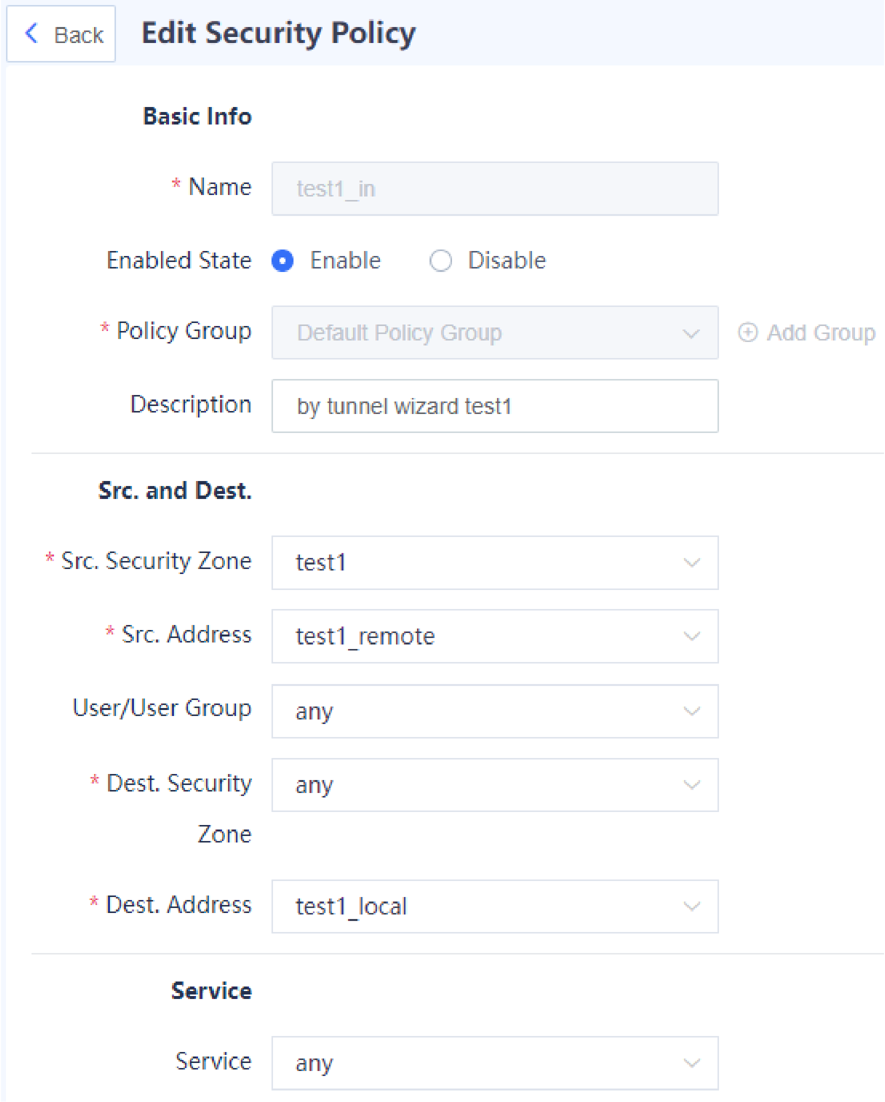
* Name	test1_out
Enabled State	● Enable ○ Disable
* Policy Group	Default Policy Group
Description	by tunnel wizard test1

Src. and Dest.

* Src. Security Zone	any
* Src. Address	test1_local
User/User Group	any
* Dest. Security Zone	test1
* Dest. Address	test1_remote

Service

Service	any



Edit Security Policy

Basic Info

* Name: test1_in

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

Description: by tunnel wizard test1

Src. and Dest.

* Src. Security Zone: test1

* Src. Address: test1_remote

User/User Group: any

* Dest. Security Zone: any

* Dest. Address: test1_local

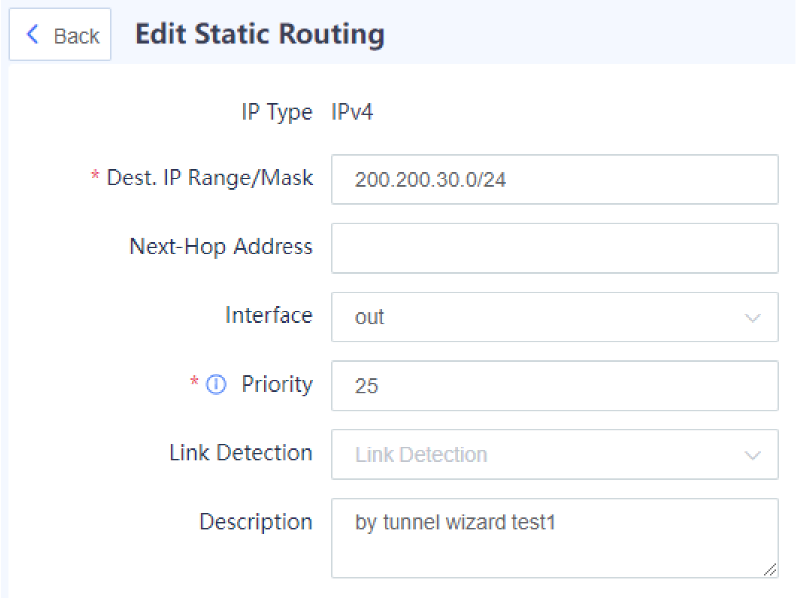
Service

Service: any

(5) Configure a static route.

a Choose **Network** > **Routing** > **Static Routing** > **IPv4**.

b Click **Create** and create a static route to the peer protected subnet of the VPN.

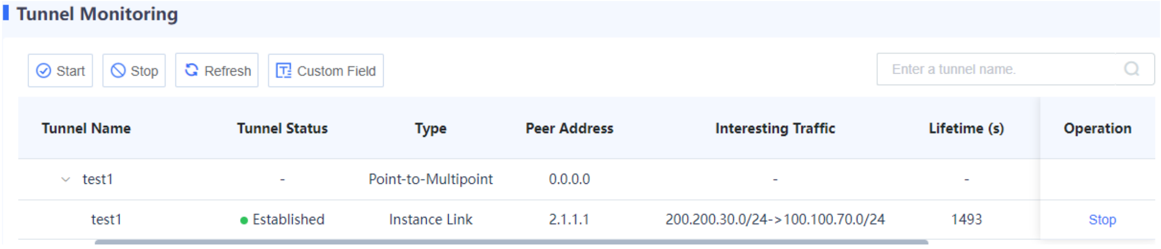


IP Type	IPv4
* Dest. IP Range/Mask	200.200.30.0/24
Next-Hop Address	
Interface	out
* ⓘ Priority	25
Link Detection	Link Detection
Description	by tunnel wizard test1

6.6 Verification

6.6.1 Verifying Configuration of the Hub Site

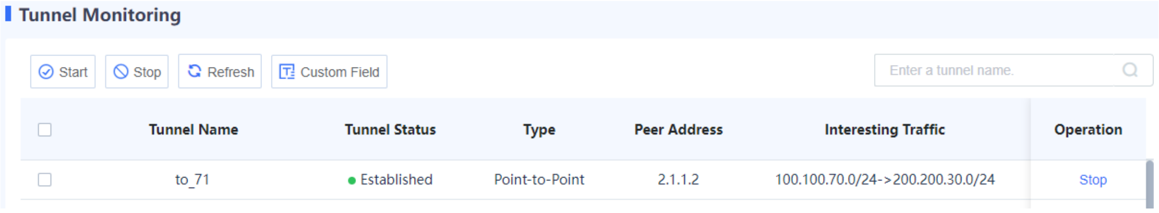
- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.



Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Operation
test1	-	Point-to-Multipoint	0.0.0.0	-	-	
test1	● Established	Instance Link	2.1.1.1	200.200.30.0/24->100.100.70.0/24	1493	Stop

6.6.2 Verifying Configuration of Spoke A

- Choose **Network** > **IPsec VPN** > **Tunnel Monitoring**. On the page that is displayed, check tunnel establishment and status information.



□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Operation
□	to_71	● Established	Point-to-Point	2.1.1.2	100.100.70.0/24->200.200.30.0/24	Stop

7 Configuration Examples of IPsec VPN Networking with Link Redundancy

7.1 Applicable Products and Versions

Table 7-1 Products and Versions

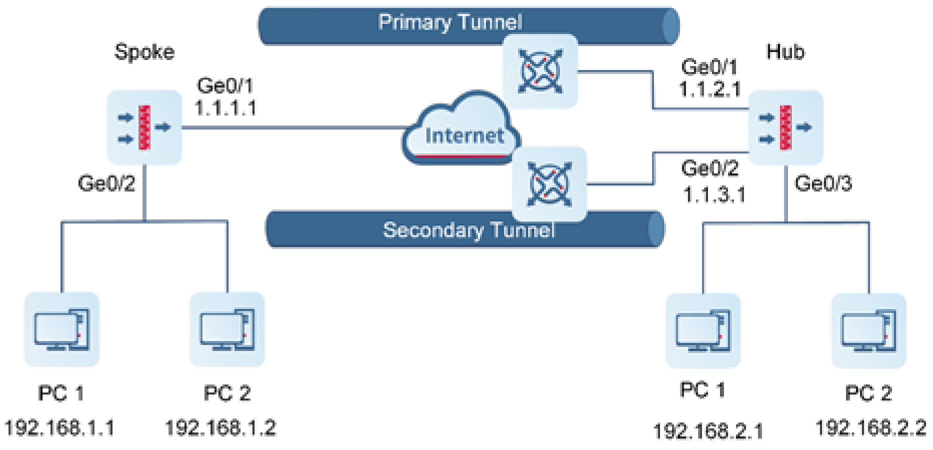
Device Type	Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R6P2 or later

7.2 Service Demands

Typically, multiple physical links need to be deployed to ensure high reliability of IPsec VPN tunnels and prevent service interruption caused by single point of failures (SPOFs) of links. In this case, if a link is disconnected, the IPsec VPN tunnel can automatically switch to another link through Dead Peer Detection (DPD).

As shown in the following figure, the hub site accesses the Internet through two links in active/standby mode, and both the active and standby outbound interfaces are configured with fixed public IP addresses. The spoke site accesses the Internet through one link, and the outbound interface is configured with a fixed public IP address.

Figure 7-1 IPsec VPN Networking with Link Redundancy



7.3 Restrictions and Guidelines

- When RG-WALL 1600 serves as the IPsec VPN hub site, all spoke sites must use the same pre-shared key to negotiate with the hub site.

7.4 Prerequisites

You have completed basic network configurations for the two sites, including interface IP addresses and default routes. Pay attention to the following points during configuration:

- The IP address of the hub site is fixed.
- All spoke sites can obtain the pre-shared key configured on the hub site in OOB mode.

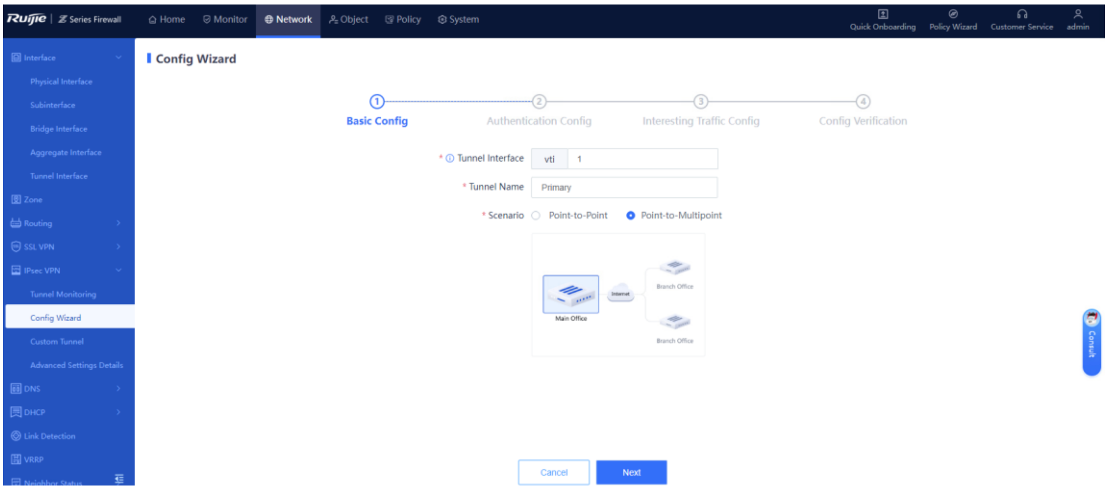
7.5 Procedure (Using a Configuration Wizard)

7.5.1 Configuring the Primary Tunnel for the Hub Site

1. Performing Basic Configuration

(1) Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Site-to-Multisite**, and set the other parameters according to the following figure.



Config Wizard

① Basic Config ② Authentication Config ③ Interesting Traffic Config ④ Config Verification

* Tunnel Interface: vti 1

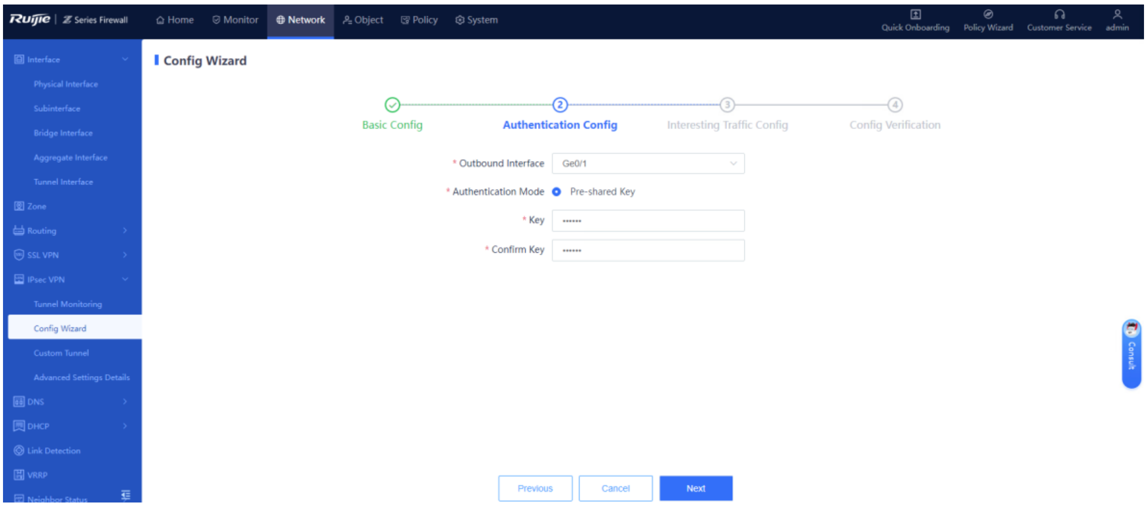
* Tunnel Name: Primary

* Scenario: ○ Point-to-Point ● Point-to-Multipoint

(3) After completing the configuration, click **Next**.

2. Configuring Authentication

(1) Configure parameters according to the following figure.



Config Wizard

* Outbound Interface: Ge0/1

* Authentication Mode: ● Pre-shared Key

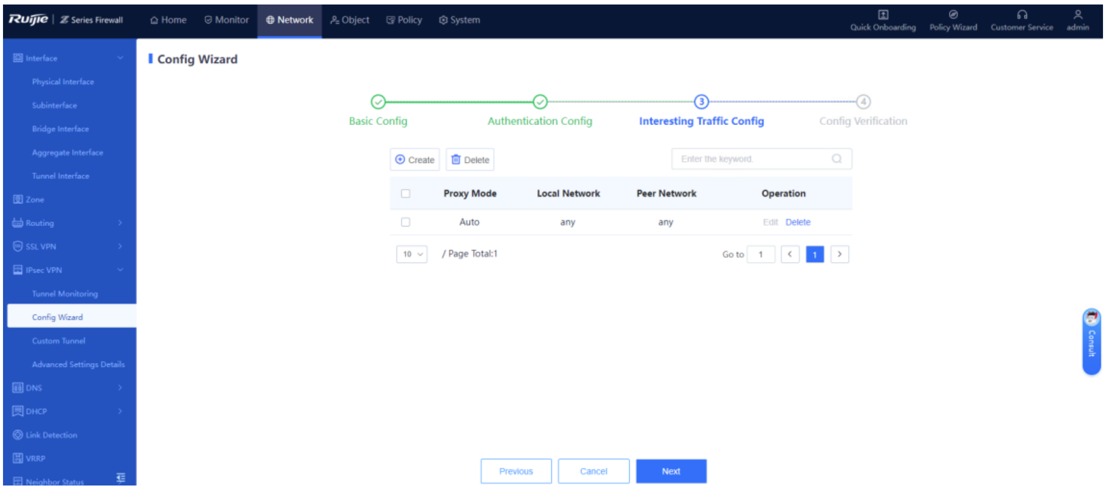
* Key: ••••••

* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Configuring Interesting Traffic

(1) Click **Create**. Configure parameters for interesting traffic according to the following figure.



Config Wizard

□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

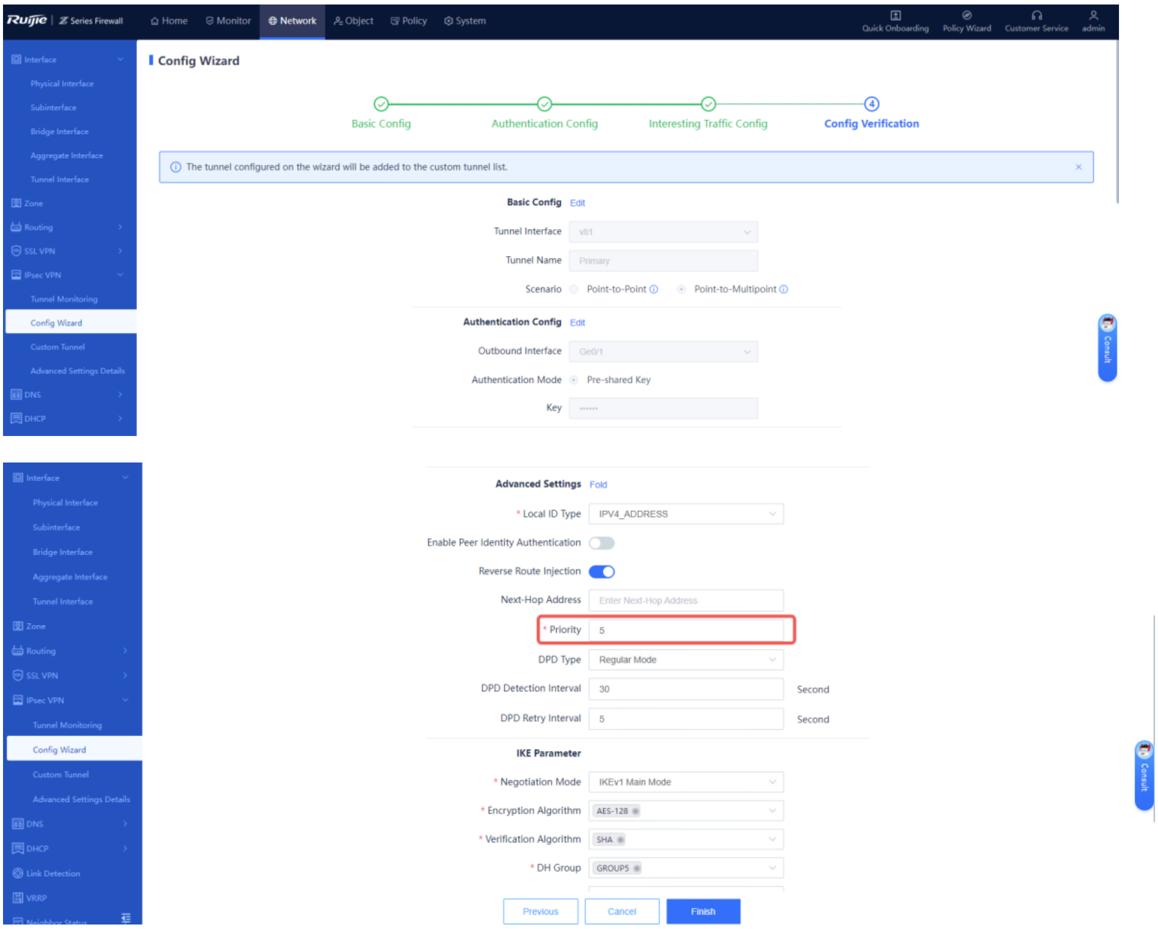
(2) After completing the configuration, click **Next**.

4. Verifying Configuration

(1) Verify that the priority of the reverse route of the primary IPsec VPN tunnel is higher than that of the secondary tunnel. In this example, the reverse route priority value of the primary tunnel is set to 5. (A larger value indicates a lower priority.)

Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the reverse route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



Config Wizard

The tunnel configured on the wizard will be added to the custom tunnel list.

Basic Config

Tunnel Interface: vti1

Tunnel Name: Primary

Scenario: ○ Point-to-Point ● Point-to-Multipoint

Authentication Config

Outbound Interface: Ge0/1

Authentication Mode: ● Pre-shared Key

Key: ······

Advanced Settings

* Local ID Type: IPV4_ADDRESS

Enable Peer Identity Authentication: off

Reverse Route Injection: on

Next-Hop Address: Enter Next-Hop Address

* Priority: 5

DPD Type: Regular Mode

DPD Detection Interval: 30 Second

DPD Retry Interval: 5 Second

IKE Parameter

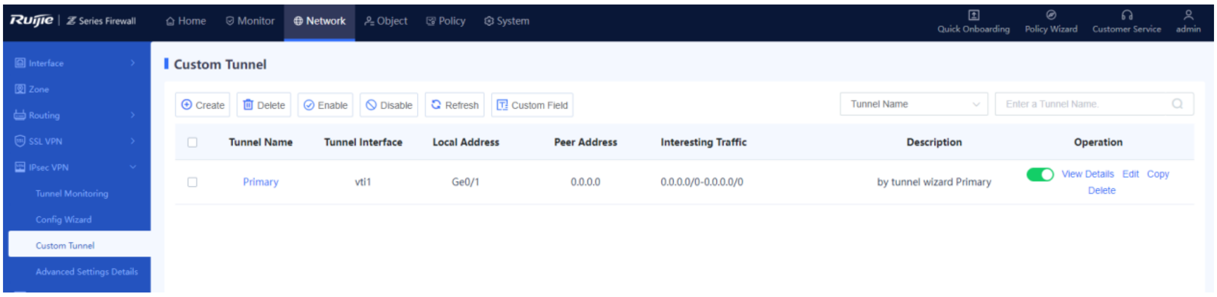
* Negotiation Mode: IKEv1 Main Mode

* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

(2) After verifying the configuration, click **Finish**.



Custom Tunnel

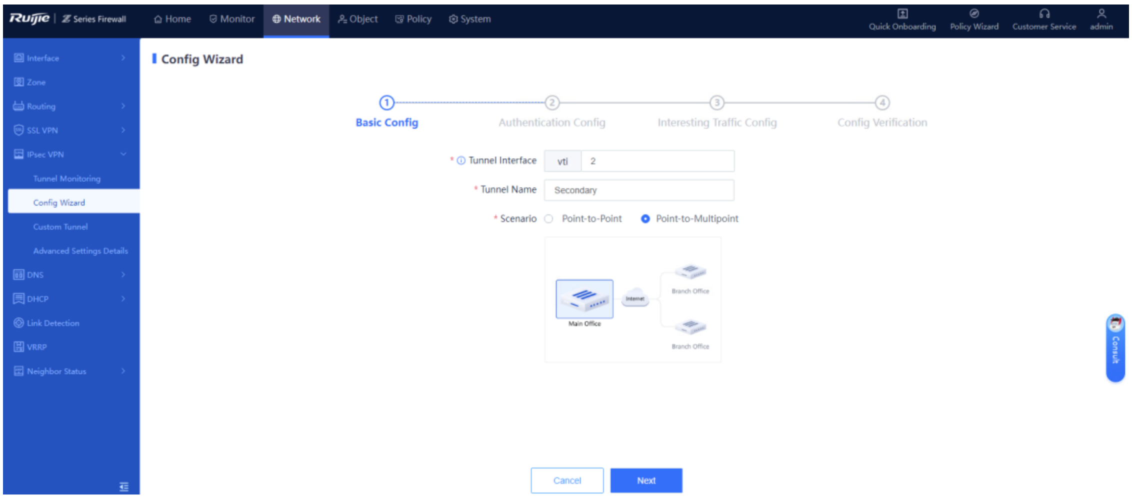
☐	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
☐	Primary	vti1	Ge0/1	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Primary	View Details Edit Copy Delete

7.5.2 Configuring the Secondary Tunnel for the Hub Site

1. Performing Basic Configuration

(1) Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Site-to-Multisite**, and set the other parameters according to the following figure.



* Tunnel Interface: vti 2

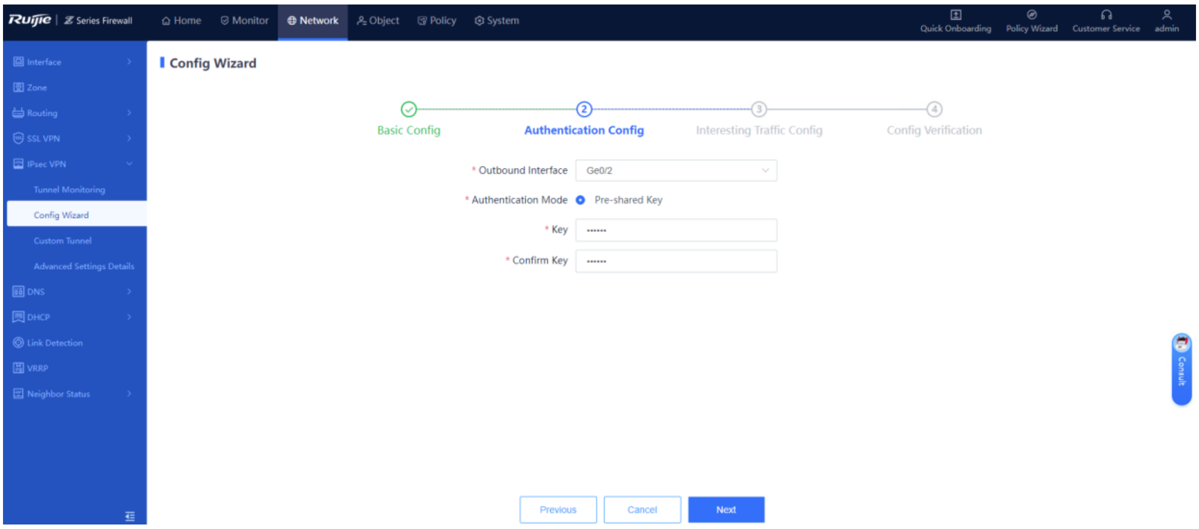
* Tunnel Name: Secondary

* Scenario: ○ Point-to-Point ● Point-to-Multipoint

(3) After completing the configuration, click **Next**.

2. Configuring Authentication

(1) Configure parameters according to the following figure.



* Outbound Interface: Ge0/2

* Authentication Mode: ● Pre-shared Key

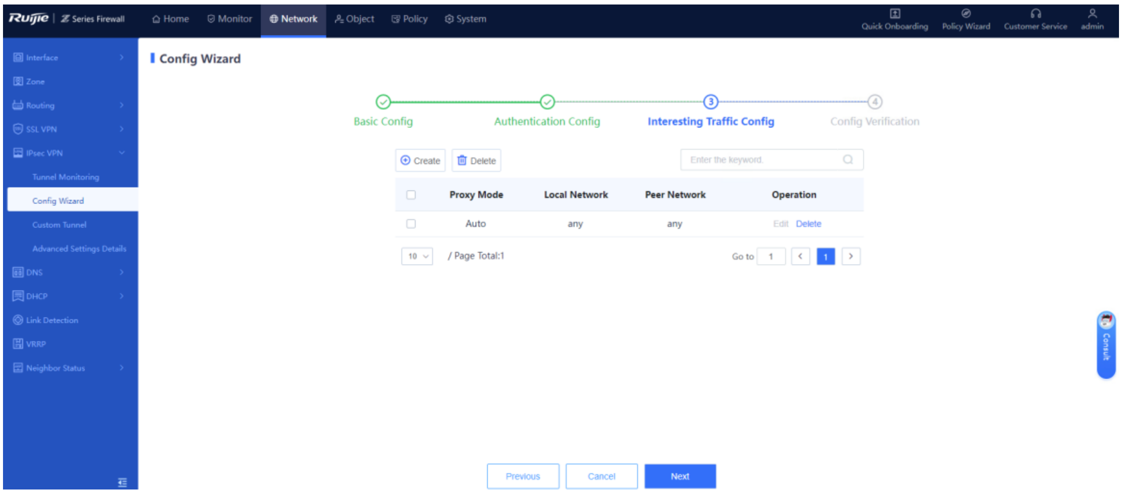
* Key: ••••••

* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Configuring Interesting Traffic

(1) Click **Create**. Configure parameters for interesting traffic according to the following figure.



□	Proxy Mode	Local Network	Peer Network	Operation
□	Auto	any	any	Edit Delete

10 / Page Total:1 Go to 1 < 1 >

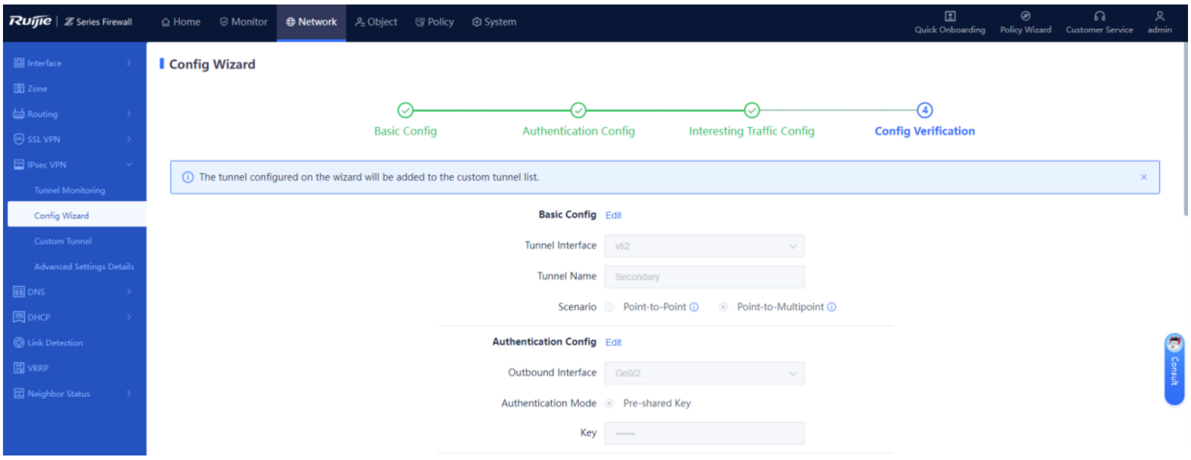
(2) After completing the configuration, click **Next**.

4. Verifying Configuration

(1) Verify that the priority of the reverse route of the secondary IPsec VPN tunnel is lower than that of the primary tunnel. In this example, the reverse route priority value of the secondary tunnel is set to 10. (A larger value indicates a lower priority.)

⚠ Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the reverse route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



The tunnel configured on the wizard will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti2

Tunnel Name: Secondary

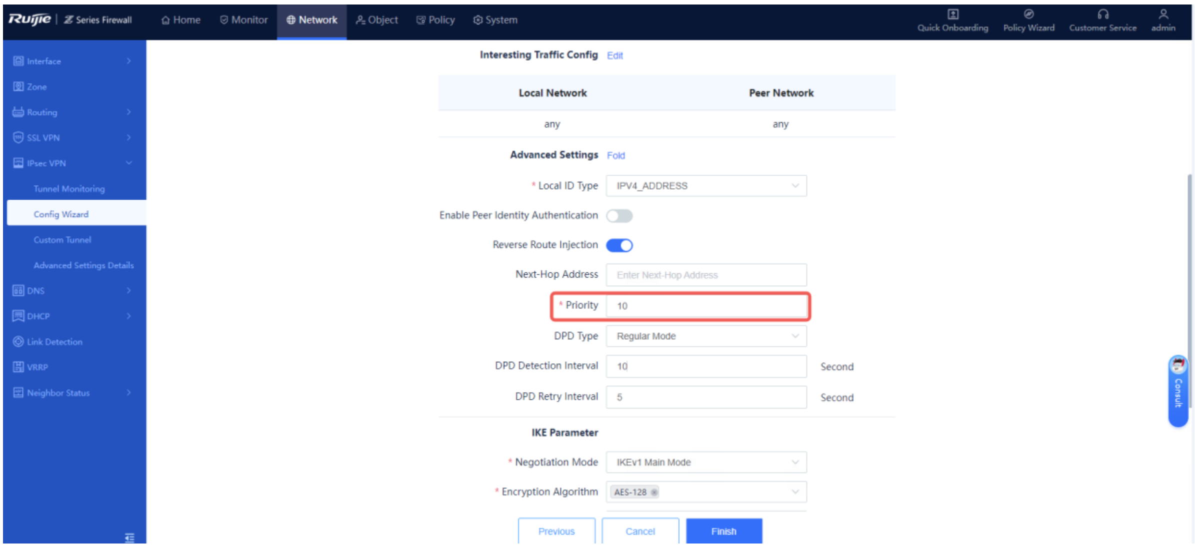
Scenario: ○ Point-to-Point ● Point-to-Multipoint

Authentication Config Edit

Outbound Interface: Ge0/2

Authentication Mode: ● Pre-shared Key

Key: ••••••



Interesting Traffic Config Edit

Local Network	Peer Network
any	any

Advanced Settings Fold

* Local ID Type: IPV4_ADDRESS

Enable Peer Identity Authentication: off

Reverse Route Injection: on

Next-Hop Address: Enter Next-Hop Address

* Priority: 10

DPD Type: Regular Mode

DPD Detection Interval: 10 Second

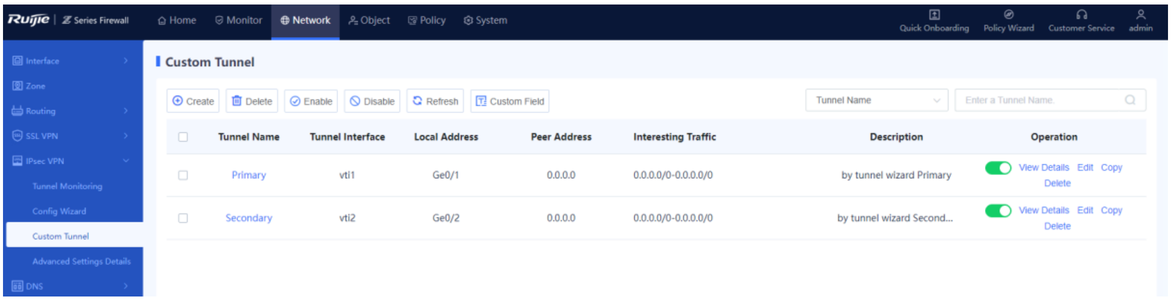
DPD Retry Interval: 5 Second

IKE Parameter

* Negotiation Mode: IKEv1 Main Mode

* Encryption Algorithm: AES-128

(2) After verifying the configuration, click **Finish**.



Custom Tunnel

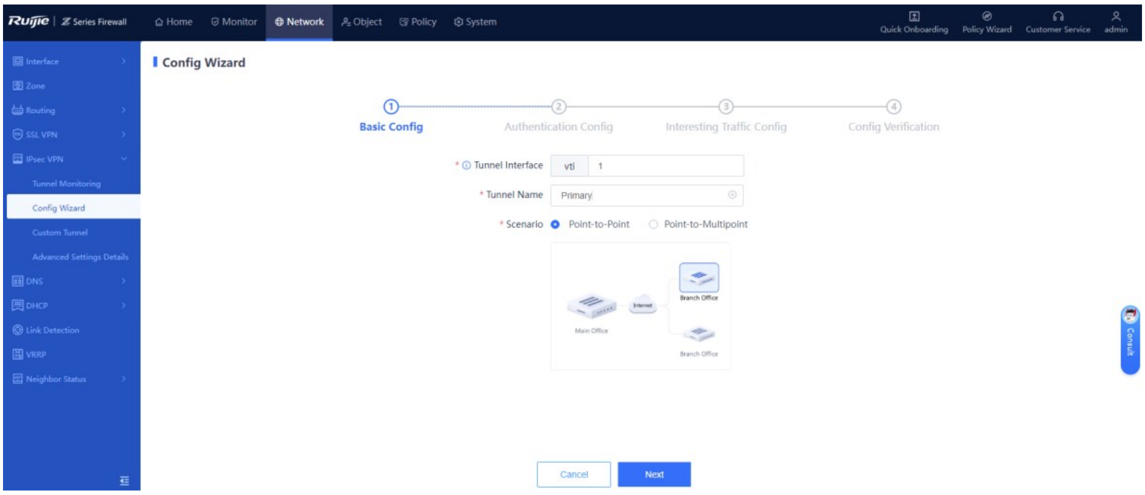
□	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
□	Primary	vti1	Ge0/1	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Primary	View Details Edit Copy Delete
□	Secondary	vti2	Ge0/2	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Second...	View Details Edit Copy Delete

7.5.3 Configuring the Primary Tunnel for the Spoke Site

1. Performing Basic Configuration

(1) Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



Config Wizard

* Tunnel Interface: vti 1

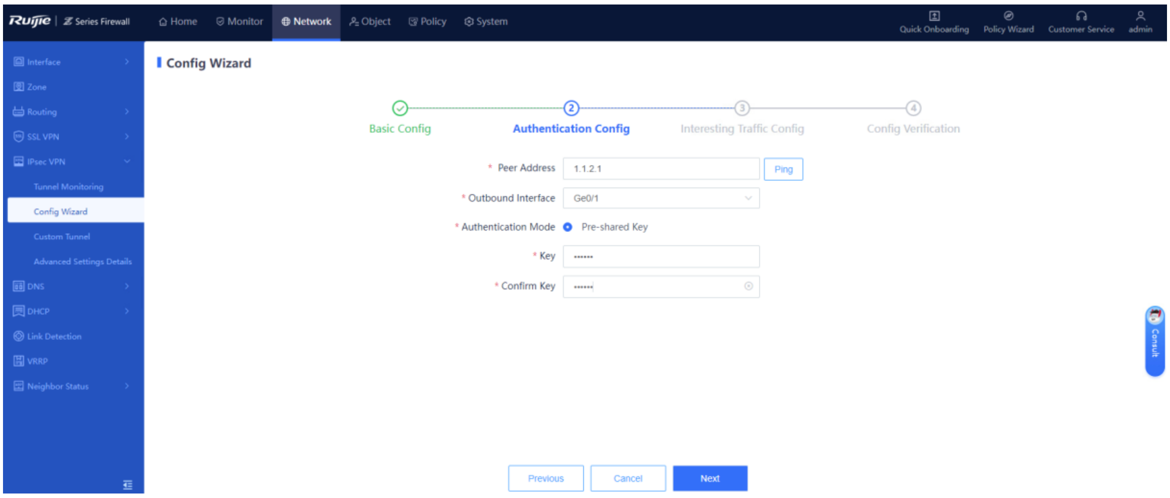
* Tunnel Name: Primary

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

(3) After completing the configuration, click **Next**.

2. Configuring Authentication

(1) Configure parameters according to the following figure.



* Peer Address: 1.1.2.1

* Outbound Interface: Ge0/1

* Authentication Mode: ● Pre-shared Key

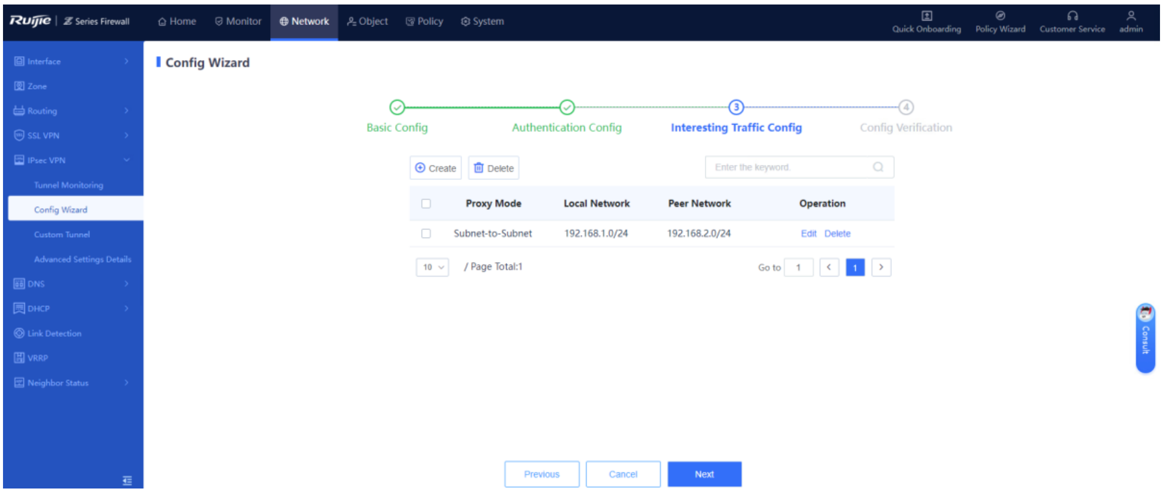
* Key: ••••••

* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Configuring Interesting Traffic

(1) Click **Create**. Configure parameters for interesting traffic according to the following figure.

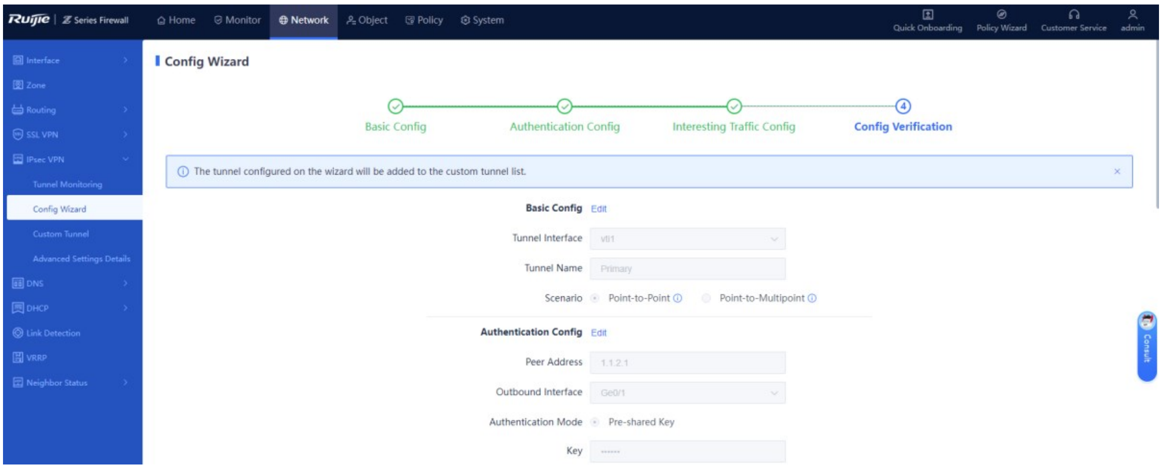


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	192.168.1.0/24	192.168.2.0/24	Edit Delete

(2) After completing the configuration, click **Next**.

4. Verifying Configuration

(1) After verifying the configuration, click **Finish**.



Config Wizard

Basic Config — Authentication Config — Interesting Traffic Config — 4 Config Verification

ⓘ The tunnel configured on the wizard will be added to the custom tunnel list. ×

Basic Config Edit

Tunnel Interface: vti1

Tunnel Name: Primary

Scenario: ● Point-to-Point ⓘ ○ Point-to-Multipoint ⓘ

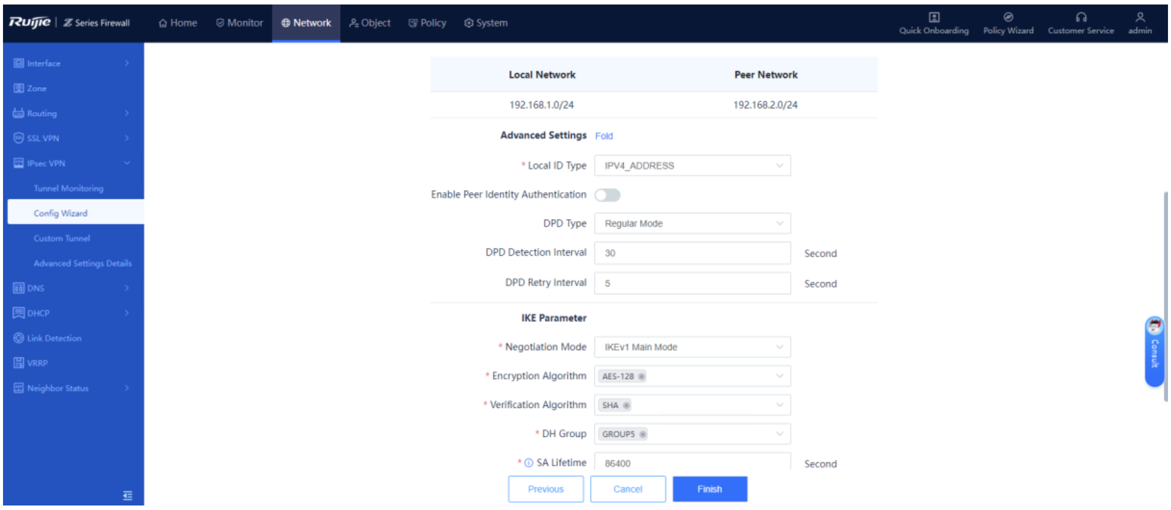
Authentication Config Edit

Peer Address: 1.1.2.1

Outbound Interface: Ge0/1

Authentication Mode: ● Pre-shared Key

Key: ······



Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

Advanced Settings Fold

* Local ID Type: IPV4_ADDRESS

Enable Peer Identity Authentication: ○

DPD Type: Regular Mode

DPD Detection Interval: 30 Second

DPD Retry Interval: 5 Second

IKE Parameter

* Negotiation Mode: IKEv1 Main Mode

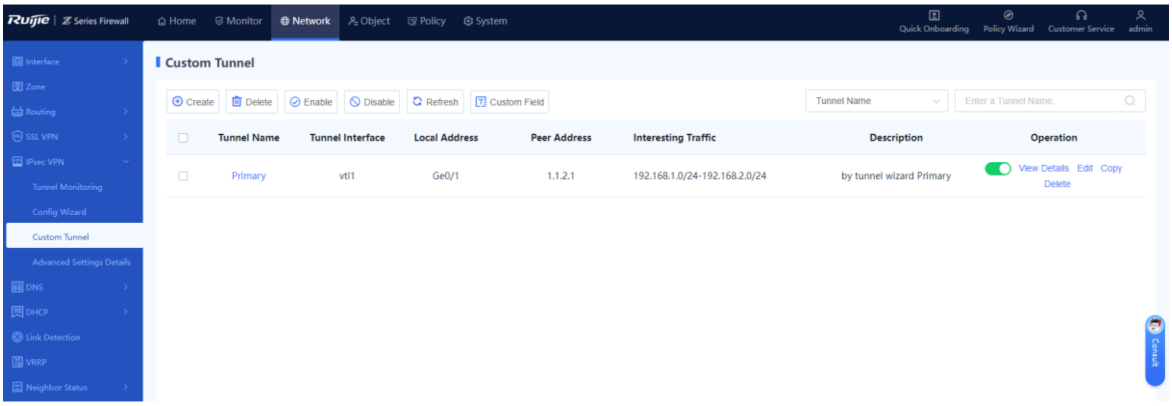
* Encryption Algorithm: AES-128

* Verification Algorithm: SHA

* DH Group: GROUP5

* ⓘ SA Lifetime: 86400 Second

Previous Cancel Finish



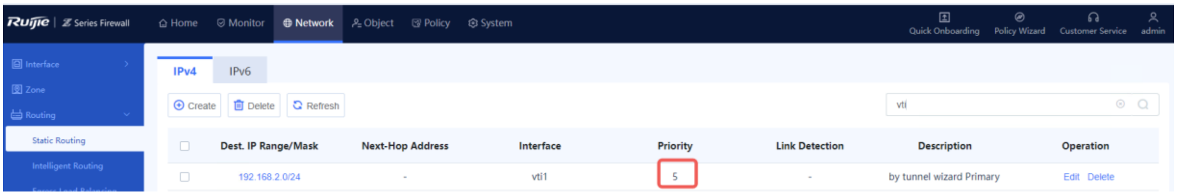
Custom Tunnel

□	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
□	Primary	vti1	Ge0/1	1.1.2.1	192.168.1.0/24-192.168.2.0/24	by tunnel wizard Primary	View Details Edit Copy Delete

(2) When you create a primary tunnel using the wizard, a static route is automatically created based on the destination subnet of the interesting traffic. The outbound interface is **vti1** and the priority value is 5 by default.

Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



vti

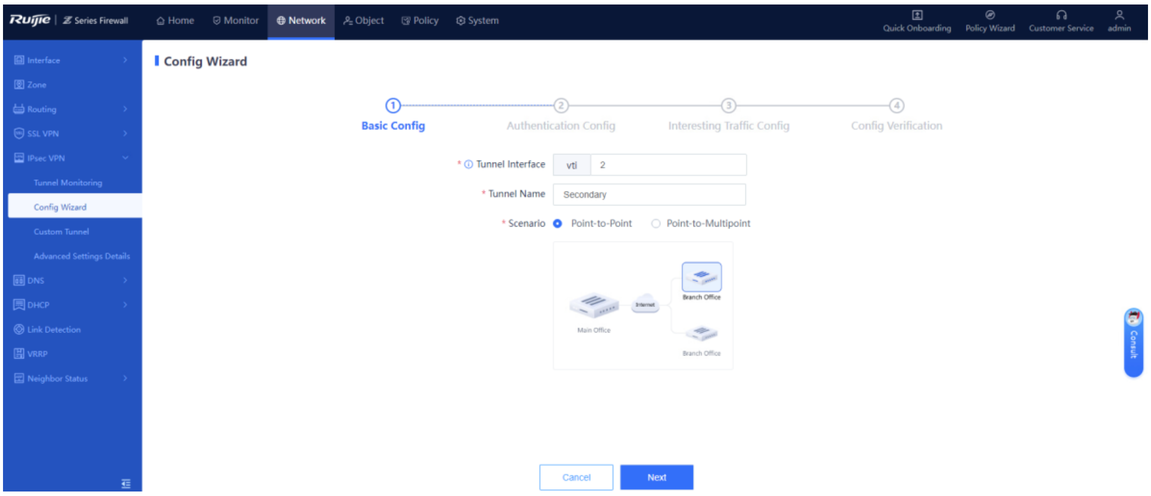
Dest. IP Range/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description	Operation
192.168.2.0/24	-	vti1	5	-	by tunnel wizard Primary	Edit Delete

7.5.4 Configuring the Secondary Tunnel for the Spoke Site

1. Performing Basic Configuration

(1) Choose **Network** > **IPsec VPN** > **Config Wizard**. The basic configuration page of the configuration wizard is displayed.

(2) Set **Scenario** to **Point-to-Point**, and set the other parameters according to the following figure.



Config Wizard

* Tunnel Interface: vti 2

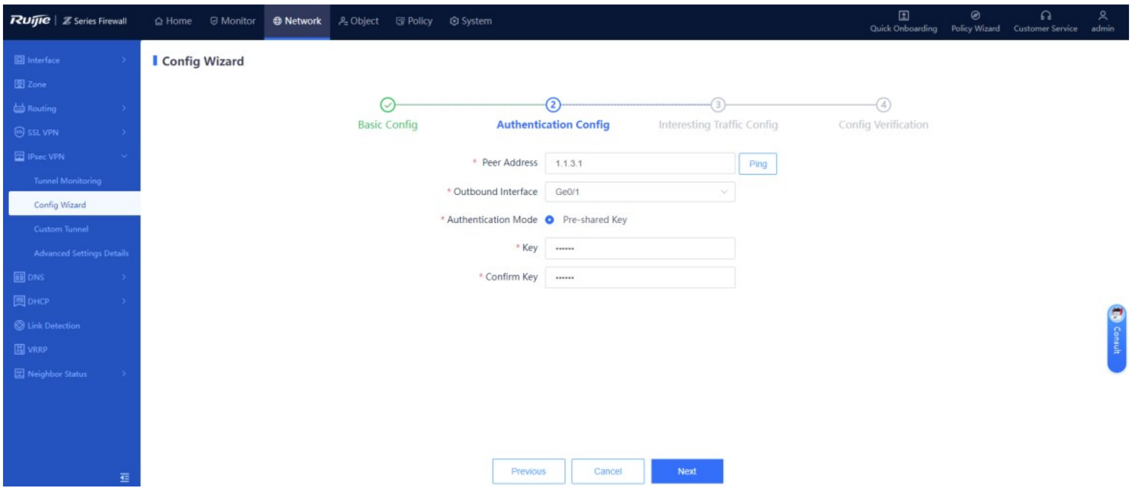
* Tunnel Name: Secondary

* Scenario: ● Point-to-Point ○ Point-to-Multipoint

(3) After completing the configuration, click **Next**.

2. Configuring Authentication

(1) Configure parameters according to the following figure.



Config Wizard

* Peer Address: 1.1.3.1

* Outbound Interface: Ge0/1

* Authentication Mode: ● Pre-shared Key

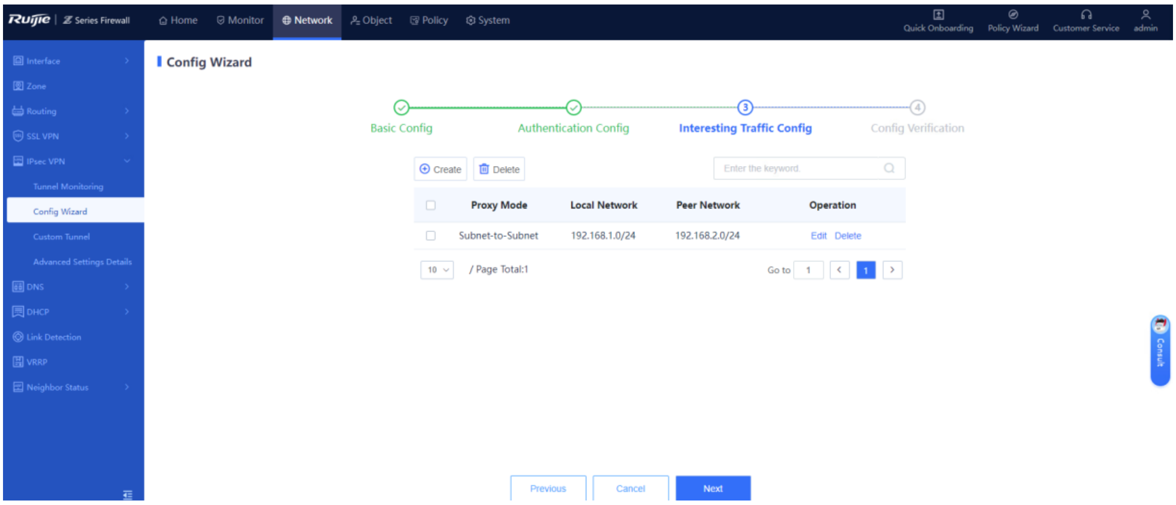
* Key: ••••••

* Confirm Key: ••••••

(2) After completing the configuration, click **Next**.

3. Configuring Interesting Traffic

(1) Click **Create**. Configure parameters for interesting traffic according to the following figure.

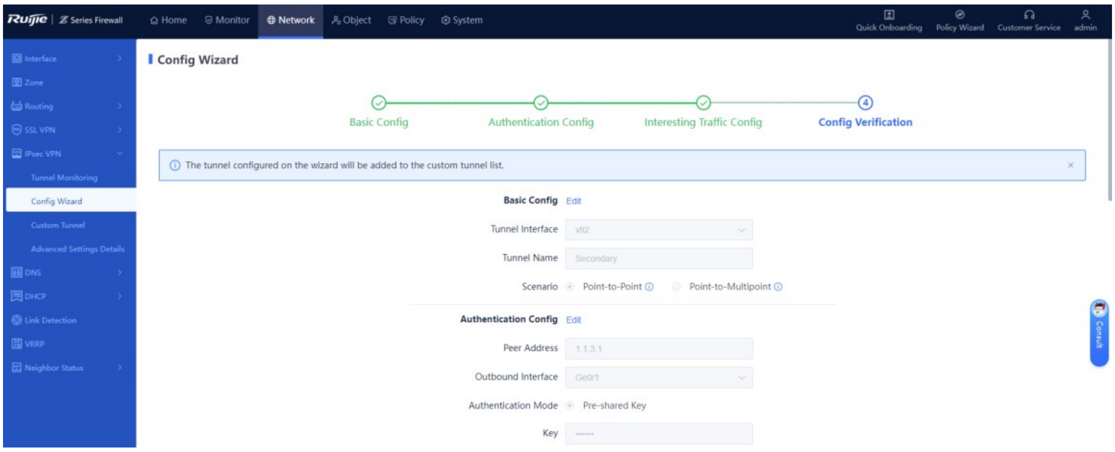


□	Proxy Mode	Local Network	Peer Network	Operation
□	Subnet-to-Subnet	192.168.1.0/24	192.168.2.0/24	Edit Delete

(2) After completing the configuration, click **Next**.

4. Verifying Configuration

(1) After verifying the configuration, click **Finish**.



The tunnel configured on the wizard will be added to the custom tunnel list.

Basic Config Edit

Tunnel Interface: vti2

Tunnel Name: Secondary

Scenario: ● Point-to-Point ○ Point-to-Multipoint

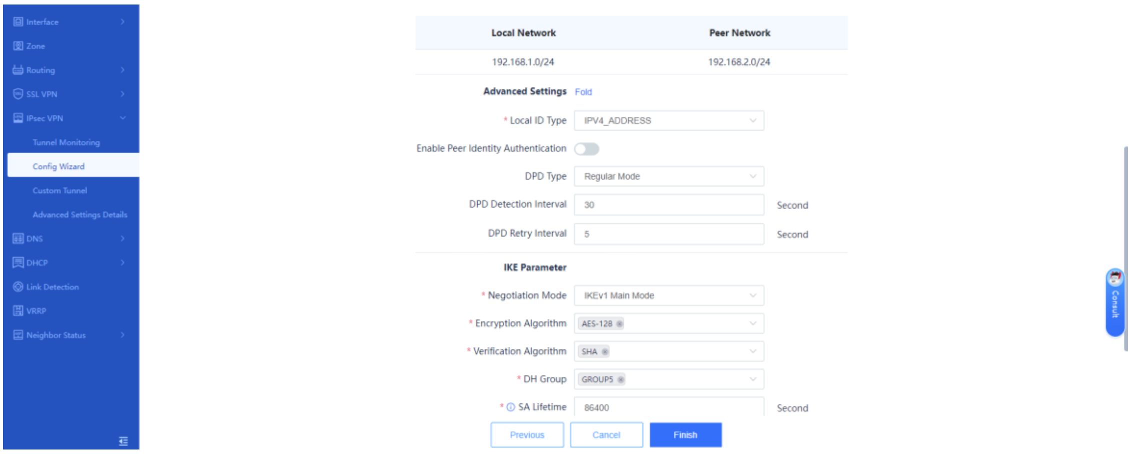
Authentication Config Edit

Peer Address: 1.1.3.1

Outbound Interface: Ge0/1

Authentication Mode: ● Pre-shared Key

Key: ······



Local Network	Peer Network
192.168.1.0/24	192.168.2.0/24

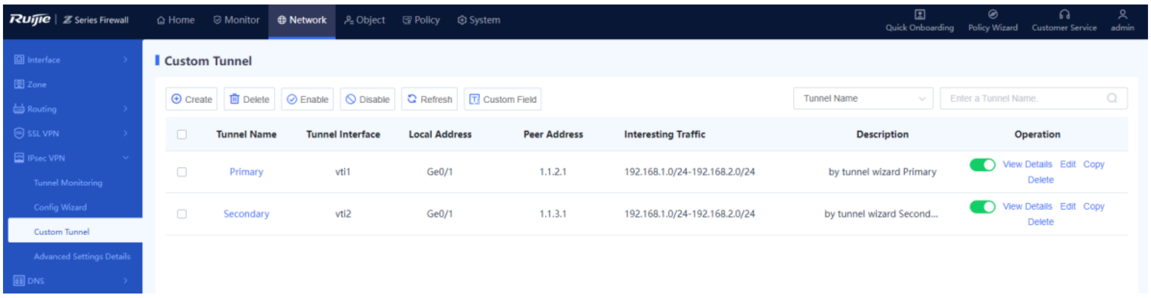
Advanced Settings Fold

- * Local ID Type: IPV4_ADDRESS
- Enable Peer Identity Authentication: off
- DPD Type: Regular Mode
- DPD Detection Interval: 30 Second
- DPD Retry Interval: 5 Second

IKE Parameter

- * Negotiation Mode: IKEv1 Main Mode
- * Encryption Algorithm: AES-128
- * Verification Algorithm: SHA
- * DH Group: GROUP5
- * SA Lifetime: 86400 Second

Previous | Cancel | Finish



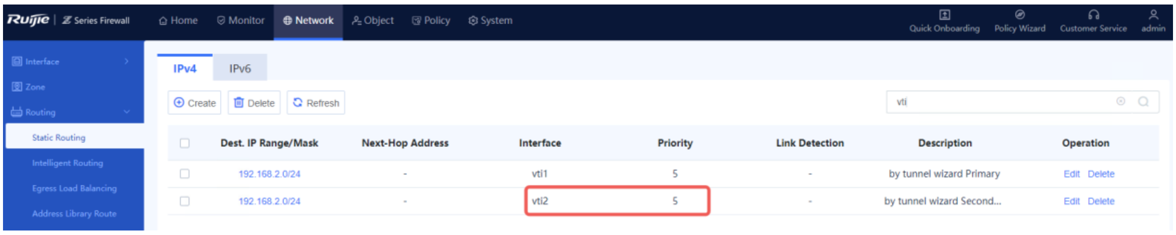
Custom Tunnel

□	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
□	Primary	vti1	Ge0/1	1.1.2.1	192.168.1.0/24-192.168.2.0/24	by tunnel wizard Primary	View Details Edit Copy Delete
□	Secondary	vti2	Ge0/1	1.1.3.1	192.168.1.0/24-192.168.2.0/24	by tunnel wizard Second...	View Details Edit Copy Delete

(2) When you create a secondary tunnel using the wizard, a static route is automatically created based on the destination subnet of the interesting traffic. The outbound interface is **vti2** and the priority value is 5 by default. Therefore, you need to lower the priority of this route by changing the value to 10. (A larger value indicates a lower priority.)

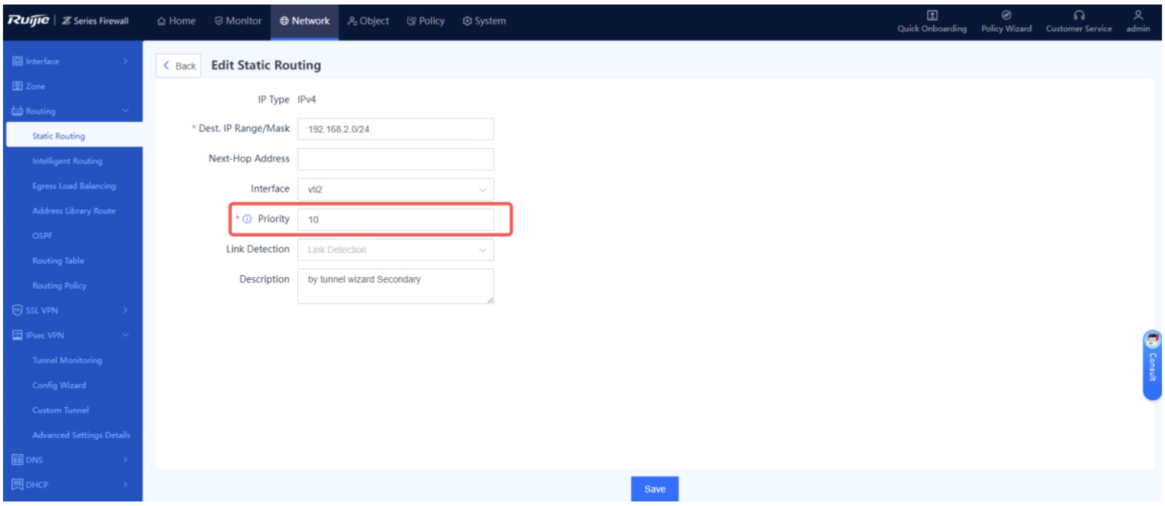
Caution

NTOS IPsec VPN is implemented based on routing. The primary and secondary tunnels are determined by the route priority of the interesting traffic. Therefore, you need to modify the priority of the route of the secondary tunnel to ensure that it is lower than that of the primary tunnel.



vti

□	Dest. IP Range/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description	Operation
□	192.168.2.0/24	-	vti1	5	-	by tunnel wizard Primary	Edit Delete
□	192.168.2.0/24	-	vti2	5	-	by tunnel wizard Second...	Edit Delete



Edit Static Routing

IP Type: IPv4

* Dest. IP Range/Mask: 192.168.2.0/24

Next-Hop Address:

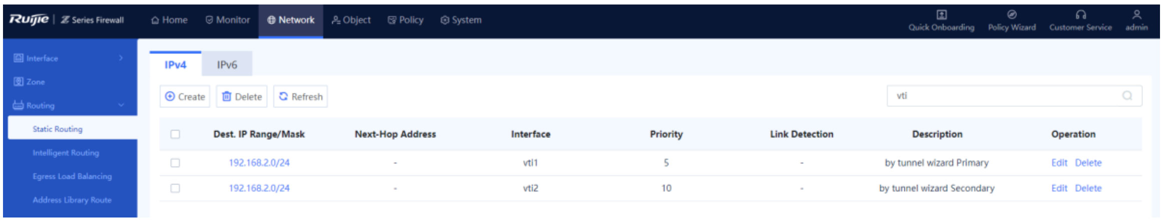
Interface: vti2

* Priority: 10

Link Detection: Link Detection

Description: by tunnel wizard Secondary

After the modification, the following static route configuration is displayed.



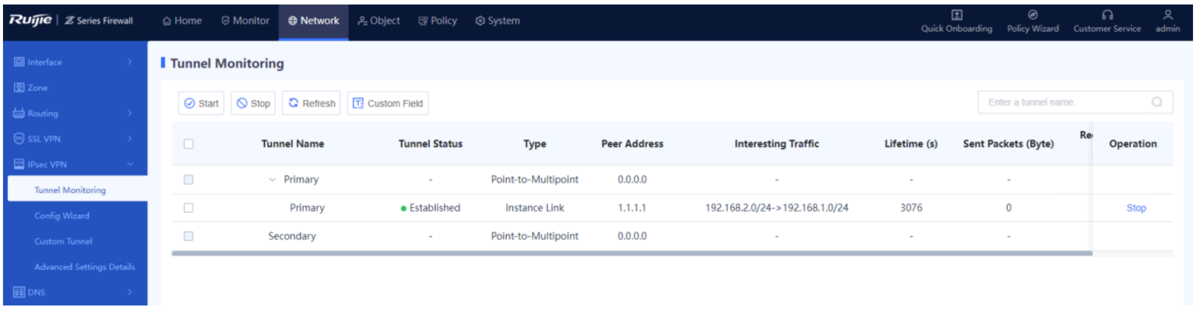
□	Dest. IP Range/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description	Operation
□	192.168.2.0/24	-	vti1	5	-	by tunnel wizard Primary	Edit Delete
□	192.168.2.0/24	-	vti2	10	-	by tunnel wizard Secondary	Edit Delete

7.6 Verification

7.6.1 Verifying Tunnel Establishment When the Primary Link Is Normal

After the configuration is successful, the spoke site first establishes a tunnel with the primary link address of the hub site. Check the following tunnel status.

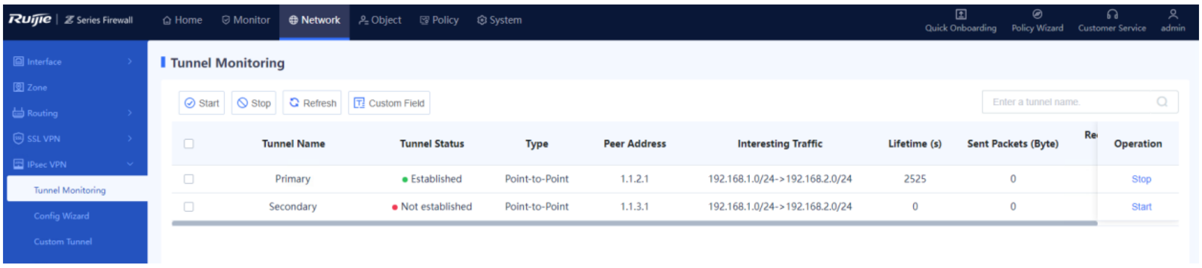
1. Checking the Tunnel Status of the Hub Site



Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
□	Primary	● Established	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3076	0		Stop
□	Secondary	-	Point-to-Multipoint	0.0.0.0	-	-	-		

2. Checking the Tunnel Status of the Spoke Site



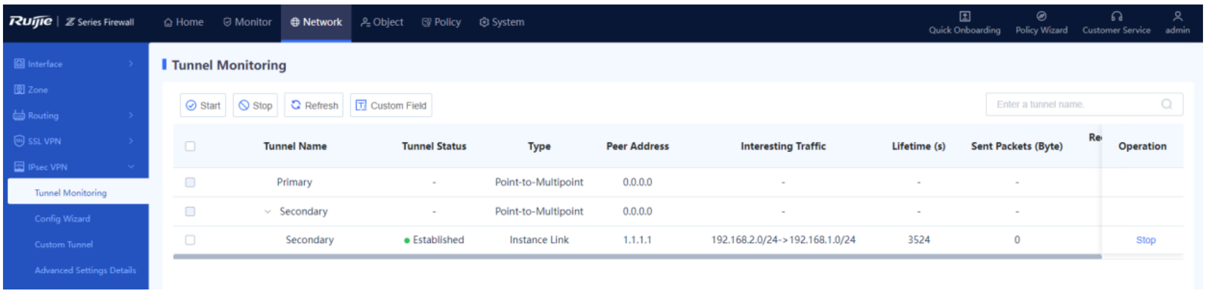
Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	● Established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0		Stop
□	Secondary	● Not established	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0		Start

7.6.2 Verifying Tunnel Switching When the Primary Link Is Faulty

Shut down the interface of the primary link on the hub site, and check the tunnel switching result. The primary tunnel is disconnected and the secondary tunnel is established successfully.

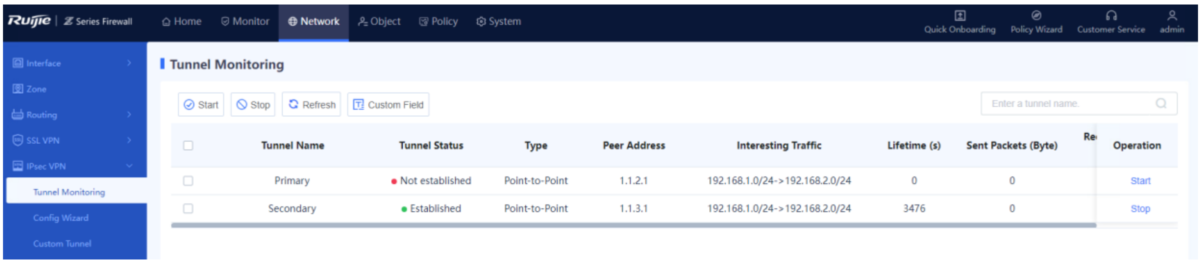
1. Checking the Tunnel Status of the Hub Site



Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
□	Secondary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
□	Secondary	● Established	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3524	0		Stop

2. Checking the Tunnel Status of the Spoke Site

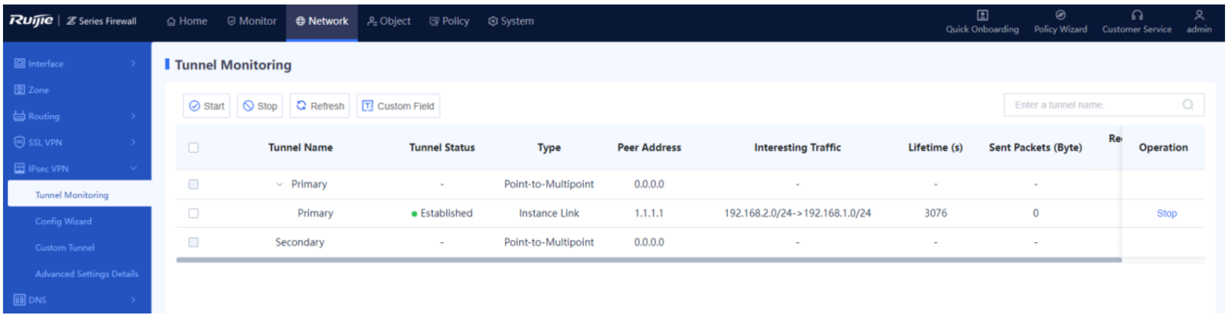


Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	● Not established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	0	0		Start
□	Secondary	● Established	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	3476	0		Stop

7.6.3 Verifying Tunnel Switchback After the Primary Link Recovers

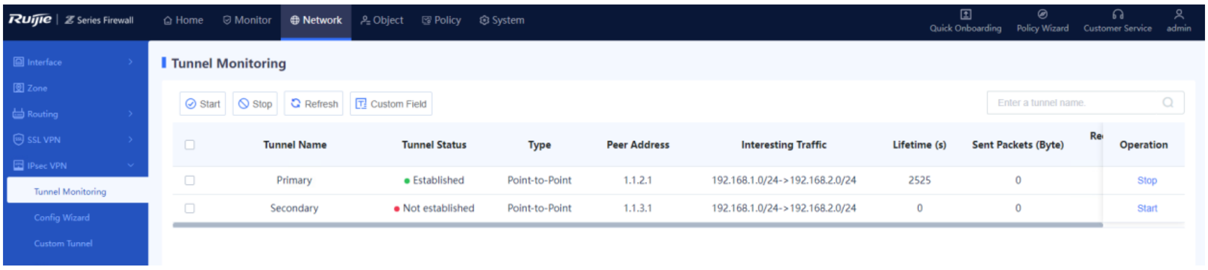
1. Checking the Tunnel Status of the Hub Site



Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	-	Point-to-Multipoint	0.0.0.0	-	-	-		
□	Primary	● Established	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3076	0		Stop
□	Secondary	-	Point-to-Multipoint	0.0.0.0	-	-	-		

2. Checking the Tunnel Status of the Spoke Site



Tunnel Monitoring

□	Tunnel Name	Tunnel Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	Operation
□	Primary	● Established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0		Stop
□	Secondary	● Not established	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0		Start

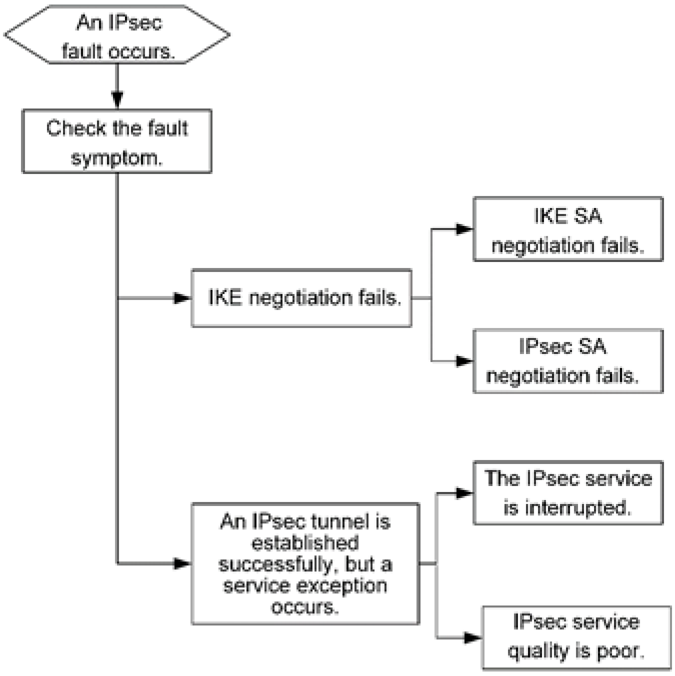
8 Common Faults and Troubleshooting Roadmaps

Common IPsec faults are as follows:

- An IPsec tunnel cannot be established. That is, IKE negotiation failed.
- An IPsec tunnel is established successfully, but a service exception occurs.

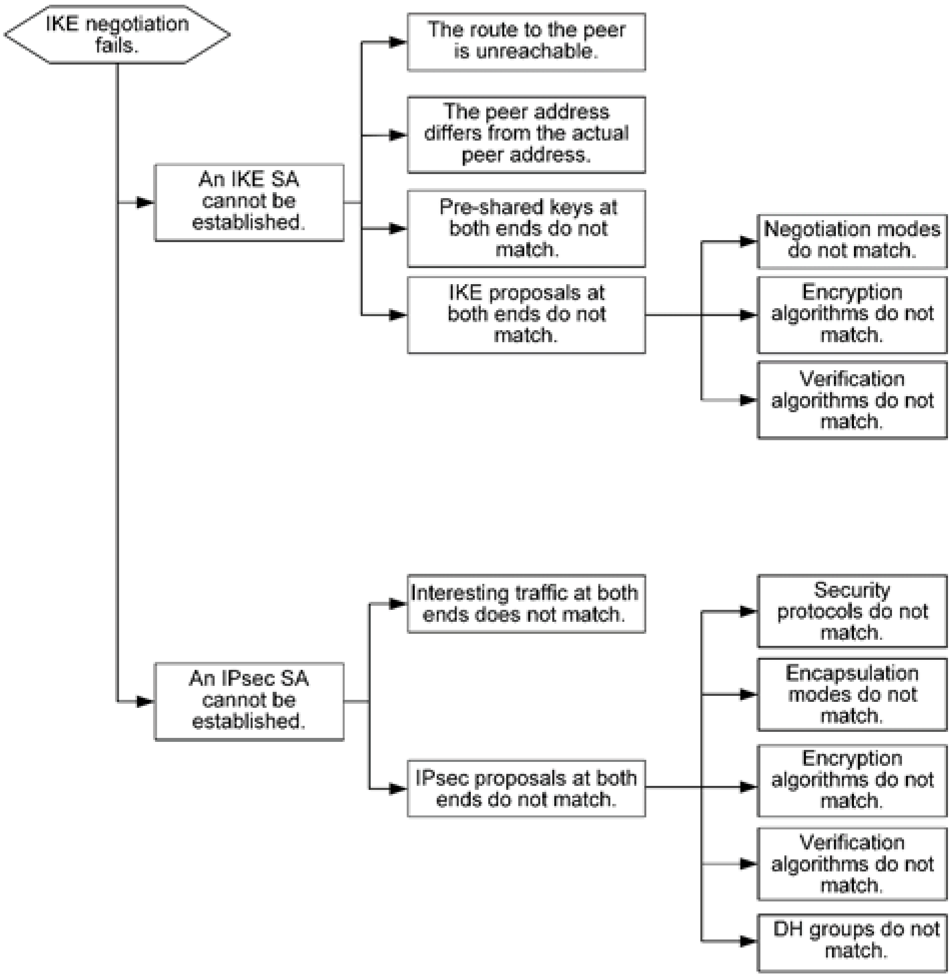
Figure 8-1 shows the typical troubleshooting roadmap for IPsec faults.

Figure 8-1 Troubleshooting Roadmap for IPsec Faults


An IPsec fault occurs.
Check the fault symptom.
IKE negotiation fails.
IKE SA negotiation fails.
IPsec SA negotiation fails.
An IPsec tunnel is established successfully, but a service exception occurs.
The IPsec service is interrupted.
IPsec service quality is poor.

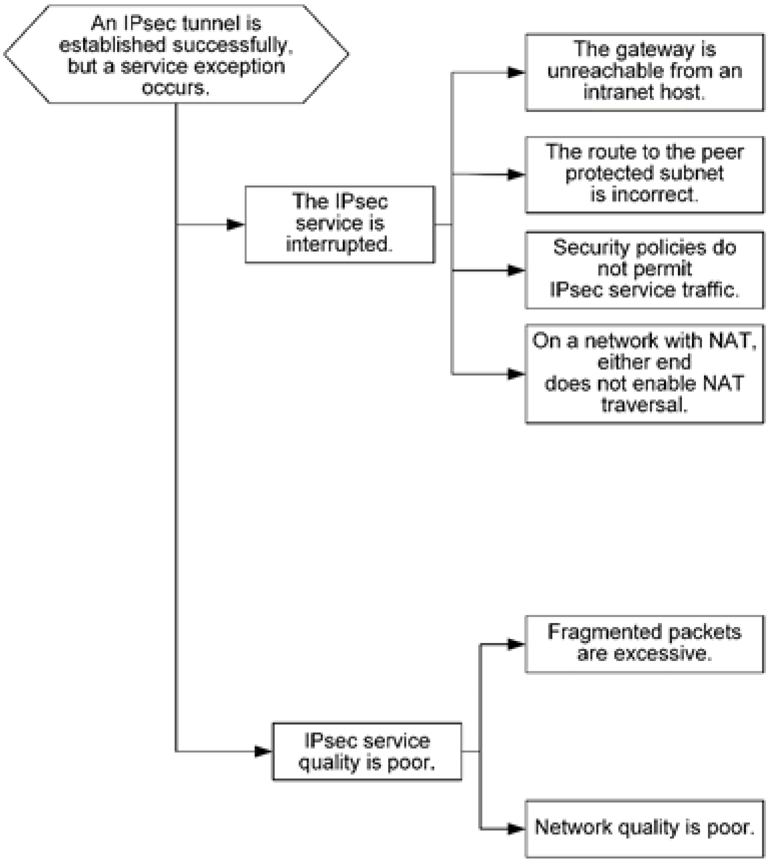
8.1 IKE Negotiation Failure

Figure 8-2 Troubleshooting Roadmap for IKE Negotiation Failures


IKE negotiation fails.
An IKE SA cannot be established.
The route to the peer is unreachable.
The peer address differs from the actual peer address.
Pre-shared keys at both ends do not match.
IKE proposals at both ends do not match.
Negotiation modes do not match.
Encryption algorithms do not match.
Verification algorithms do not match.
An IPsec SA cannot be established.
Interesting traffic at both ends does not match.
IPsec proposals at both ends do not match.
Security protocols do not match.
Encapsulation modes do not match.
Encryption algorithms do not match.
Verification algorithms do not match.
DH groups do not match.

8.2 IPsec Service Exception

Figure 8-3 Troubleshooting Roadmap for IPsec Service Exceptions


An IPsec tunnel is established successfully, but a service exception occurs.
The IPsec service is interrupted.
The gateway is unreachable from an intranet host.
The route to the peer protected subnet is incorrect.
Security policies do not permit IPsec service traffic.
On a network with NAT, either end does not enable NAT traversal.
IPsec service quality is poor.
Fragmented packets are excessive.
Network quality is poor.