

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

IPsec VPN Typical Configuration Examples



Document version: V1.2 Date: August 28, 2024 Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, no organization or individual is permitted to reproduce, extract, back up, modify, or distribute the content of this document in any manner or form. It is also prohibited to translate the document into other languages or use any or all parts of it for commercial purposes.



Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

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: <u>https://reyee.ruijie.com/</u>
- Online support center: https://reyee.ruijie.com/en-global/support
- Case portal: <u>https://www.ruijie.com/support/caseportal</u>
- 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	 Button names Window names, tab name, field name and menu items Link 	 Click OK. Select Config Wizard. 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.

1 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.

PrefaceI
1 Overview
2 Configuration Examples of Site-to-Site IPsec VPN
2.1 Applicable Products and Versions
2.2 Service Demands
2.3 Restrictions and Guidelines
2.4 Prerequisites
2.5 Procedure4
2.5.1 Using a Configuration Wizard4
2.5.2 Manually Configuring a Tunnel10
2.6 Verification22
2.6.1 Verifying Configuration of Site A22
2.6.2 Verifying Configuration of Site B22
3 Configuration Examples of Site-to-Site IPsec VPN (Interconnection with Fortinet Firewall)
3.1 Applicable Products and Versions23
3.2 Service Demands23
3.3 Restrictions and Guidelines23
3.4 Prerequisites
3.5 Procedure
3.5.1 Configuring Site A (RG-WALL Z3200-S)24
3.5.2 Configuring Site B (Fortinet Firewall)28
3.6 Verification
3.6.1 Verifying Configuration of Site A (RG-WALL Z3200-S)

3.6.2 Verifying Configuration of Site B (Fortinet Firewall)
4 Configuration Examples of Site-to-Multisite IPsec VPN
4.1 Applicable Products and Versions
4.2 Service Demands
4.3 Restrictions and Guidelines
4.4 Prerequisites
4.5 Procedure
4.5.1 Using a Configuration Wizard35
4.5.2 Manually Configuring a Tunnel40
4.6 Verification
4.6.1 Verifying Configuration of the Hub Site52
4.6.2 Verifying Configuration of Spoke A52
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
 5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
 5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
 5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions
5 Configuration Examples of Site-to-Multisite IPsec VPN (Interconnection with Fortinet Firewall) 53 5.1 Applicable Products and Versions 5.2 Service Demands 5.3 Restrictions and Guidelines 5.4 Prerequisites 5.5 Procedure 5.5.1 Configuring Spoke A (RG-WALL Z3200-S) 5.5.2 Configuring Spoke B (RG-WALL Z3200-S) 5.5.3 Configuring the Hub Site (Fortinet Firewall) 5.6 Verification 60 5.6.1 Verifying Configuration of Spoke Sites (Spoke A as an Example)

6 Configuration Examples of IPsec VPN with NAT Traversal	62
6.1 Applicable Products and Versions	62
6.2 Service Demands	62
6.3 Restrictions and Guidelines	62
6.4 Prerequisites	62
6.5 Procedure	63
6.5.1 Using a Configuration Wizard	63
6.5.2 Manually Configuring a Tunnel	70
6.6 Verification	84
6.6.1 Verifying Configuration of the Hub Site	84
6.6.2 Verifying Configuration of Spoke A	84
7 Configuration Examples of IPsec VPN Networking with Link Redundancy	85
7.1 Applicable Products and Versions	85
7.1 Applicable Products and Versions	85
7.1 Applicable Products and Versions7.2 Service Demands7.3 Restrictions and Guidelines	85 85 85
 7.1 Applicable Products and Versions 7.2 Service Demands 7.3 Restrictions and Guidelines 7.4 Prerequisites 	85 85 85 86
 7.1 Applicable Products and Versions	85 85 85 86 86
 7.1 Applicable Products and Versions	85 85 86 86 86
 7.1 Applicable Products and Versions	85 85 86 86 86 86 88
 7.1 Applicable Products and Versions	
 7.1 Applicable Products and Versions	
 7.1 Applicable Products and Versions	85 85 86 86 86 86
 7.1 Applicable Products and Versions	

rs98	7.6.3 Verifying Tunnel Switchback After the Primary Link Recove
100	8 Common Faults and Troubleshooting Roadmaps
	8.1 IKE Negotiation Failure
	8.2 IPsec Service Exception

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-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. Spoke (Peer End) 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 <u>Figure 2-1</u>, 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.

1	2					4
Basic Config	Authentication	Config	Interest	ting Traffi	c Config	Config Verificatio
	* () Tunnel Interface	vti	1			
	* Tunnel Name	Site-to	o-Site			
	* Scenario	• Poin	t-to-Point	O Poir	nt-to-Multipo	bint
		Main	a Office	internet	Branch Office Branch Office	
	Const	Nort				

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø	2		3	
Basic Config	Authentication	Config	Interesting Traffic Config	Config Verification
	* Peer Address	10.1.5.2	211	Ping
	* Outbound Interface	Ge0/2		~
	* Authentication Mode	• Pre-s	hared Key	
	* Key	•••••	•••	
	* Confirm Key	•••••		

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

Cancel

Previous

- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Next

⊘-				(3	4
Basic Config		Auther	Authentication Config		Interesting Traffic Config	
	🕣 Cre	ate 🔟 Delete		Enter th	e keyword.	Q
		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Sub	192.168.1.0/24	192.168.2.0/24	Edit Delet	e
	10 ~	/ Page Total:1			Go to 1	1

Previous Cancel Next	
----------------------	--

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

Ø—			 Ø		4
Basic Config	Authentication	Config Ir	teresting Traffic Con	fig Co	nfig Verification
will be added to t	he custom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti1	~		
	Tunnel Name	Site-to-Site			
	Scenario	Point-to-Point ()	Point-to-Multipo	bint (1)	
	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 Netwo	rk	
	192.168.1.0/24		192.168.2.0/	24	
	Advanced Settings	Expand			
	Previous	ncel Finish			

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.

1	2	3		
Basic Config	Authentication Co	fig Interesting Tra	affic Config	Config Verification
	* (i) Tunnel Interface	ti 1		
	* Tunnel Name S	te-to-Site	\otimes	
	* Scenario 🧿	Point-to-Point 🔿 F	oint-to-Multipoir	nt
		Main Office	Branch Office Branch Office	
	Cancel Ne	ĸt		

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

<i>—</i>		2			3		(4
Basic Con	fig Au	thentication	Config	Interesti	ng Traffic Co	nfig	Config \	/erification
	*	Peer Address	10.1.5.2	.03			Ping	
	* Outbo	und Interface	Ge0/2			\sim		
	* Authent	ication Mode	• Pre-sl	hared Key				
		* Key	•••••	••				
	*	Confirm Key	•••••	••		(\times)		
	Previous	Cancel		Next				

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

\bigcirc				(3	
Basic Co		Autner	itication Config	Interesting	e kevword.	
		Proxy Mode	Local Network	Peer Network	Operation	
		Subnet-to-Sub	192.168.2.0/24	192.168.1.0/24	Edit Delete	
	10 、	/ Page Total:1			Go to 1	1

Previous	Cancel	Next	

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

(~) 	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~)	(··)		(4)
Basic Config	Authenticati	on Config	Interesting Traf	fic Config	Config Verification
be added to the cu	ustom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti1	~		
	Tunnel Name	Site-to-Site			
	Scenario	Point-to-Point	 Point-to-Multip 	point 🕕	
	Authentication Config	Edit			
	Peer Address	10.1.5.203			
	Outbound Interface	Ge0/2			
	Authentication Mode	 Pre-shared Key 			
	Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Pee	r Network	
	192.168.2.0/24		192.	.168.1.0/24	
	Advanced Settings	Expand			
	Previous	Cancel Finis	sh		

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:
 - o Set Interface Name to vti1.
 - o Add security zone VPN-Zone and set Security Zone to VPN-Zone for this interface.
 - o Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
 - o 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 ~	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.
- o Set Enabled State to Enable.
- o 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.

1	2	3
Basic Config	Interesting Traffic Config Sec	curity Parameter Config
* Scenario	Point-to-Point Point-to-Multip	ooint 🕕
* Tunnel Name	Site-to-Site	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	⊕ Add Tunnel Interface
* Authentication Mode	Pre-shared Key \sim	
* Key	•••••	
* Confirm Key	•••••	
* Local Address	● Interface ① ○ IP ①	
	Ge0/2 v	
* Peer Address	10.1.5.211	Ping
* Local ID Type	IPV4_ADDRESS v	
Verify Peer ID		
≣ ∓ Advanced		
Cancel	Next	

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.
- o Set Local Network to 192.168.1.0/24 and Peer Network to 192.168.2.0/24.

⊘ Basic Config	Interesting	2 Traffic Config	Security Parameter Co	nfig
😌 Create 🔟 Delete		Enter th	e keyword.	Q
Proxy Mode	Local Network	Peer Network	Operation	
Subnet-to-Sub	192.168.1.0/24	192.168.2.0/24	Edit Delete	
10 v / Page Total:1			Go to 1 < 1	>

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.

Basic Config Interes	ting Traffic Config	3 Security Paramet	er
IKE Parameter		Config	
* Negotiation Mode	IKEv1 Main Mode	\sim	
* Encryption Algorithm	AES-128 🛞	\sim	
* Verification Algorithm	SHA 🛞	\sim	
* DH Group	GROUP5 ®	\sim	
* ① SA Lifetime	86400		Second
IPsec Parameter			
* Protocol	ESP	~	
* Encapsulation Mode	Tunnel	\sim	
* Encryption Algorithm	AES-128 🛞	\sim	
* Verification Algorithm	SHA 🛞	\sim	
Perfect Forward Secrecy			
* (1) SA Lifetime	3600		Second

Click Finish to complete the configuration for the IPsec tunnel.

Cancel

(3) Create security policies.

Previous

Finish

.

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.

IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group
⊖ Create 🔟 De	elete C Refresh		
Name	1	P Address/Range	Address Group
Name VPN-remot	esubnet 1	P Address/Range 192.168.2.0/24	Address Group

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.

< Back Edit Secu	rity Policy	
Basic Info		
* Name	VPN-outbound	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	⊕ Add Group
Description	Enter the security policy name descrip	
Src. and Dest.		
* Src. Security Zone	any \lor	
* Src. Address	VPN-localsubnet \vee	
User/User Group	any \vee	
* Dest. Security	VPN-Zone \lor	
Zone		
* Dest. Address	VPN-remotesubnet \sim	
Service		
Service	any \lor	

K Back Edit Secu	rity 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	\sim	
* Dest. Security	any	~	
Zone			
* 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 Rou	ıting
	IP Туре	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:
 - o Set Interface Name to vti1.
 - o Add security zone VPN-Zone and set Security Zone to VPN-Zone for this interface.
 - o Set Tunnel Local Address to the default outbound interface address of Site B: 10.1.5.211.
 - o Set Tunnel Remote Address to the default outbound interface address of Site A: 10.1.5.203.

< Back	Edit Tunnel Int	erface Details	
	* Interface Name	vti1	
	Security Zone	Select Security Zone V	⊕ Add Security Zone
* T	unnel Local Address	10.1.5.211	
Tun	nel 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:

- o Set Tunnel Name to Site-to-Site.
- o Set Enabled State to Enable.
- o 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.

1	2	3
Basic Config	Interesting Traffic Config	Security Parameter Config
* Scenario	Point-to-Point ①	point ()
* Tunnel Name	Site-to-Site	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti1 ~	Add Tunnel Interface
* Authentication Mode	Pre-shared Key V	
* Key	•••••	
* Confirm Key	•••••	
* Local Address	● Interface ①	
	Ge0/2 ~	
* Peer Address	10.1.5.203	Ping
* Local ID Type	IPV4_ADDRESS ~	
Verify Peer ID		
≣ ∓ Advanced		
Cance	Next	

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 Subnet-to-Subnet.
- o Set Local Network to 192.168.2.0/24 and Peer Network to 192.168.1.0/24.

⊘ Basic Config	Interesting 1	2) Traffic Config	Security Parameter Cor	fig
Oreate ☐ Delete		Enter	the keyword.	Q
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.

6	<u>)</u>		⊘			3	
Basic	Config I	ntere	sting Traffic	c Config	Secu	urity Parameter	
						Config	
	IKE Paran	neter					
	* Negotiation N	Node	IKEv1 Ma	in Mode		\sim	
*	Encryption Algo	rithm	AES-128 🛞			\sim	
*	Verification Algo	rithm	SHA 🛞			~	
	* DH G	iroup	GROUP5 ®			\sim	
	* 🕕 SA Life	etime	86400				Second
	IPsec Paran	neter					
	* Pro	tocol	ESP			~	
	* Encapsulation N	Node	Tunnel			\sim	
*	Encryption Algo	rithm	AES-128 🛞			\sim	
*	Verification Algo	rithm	SHA 🛞			\sim	
Pe	erfect Forward Se	crecy					
	* (1) SA Life	etime	3600				Second
	Previous		Cancel	Fin	ish		

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.

IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group				
Name	I	P Address/Range	Address Group				
VPN-remot	esubnet	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.

< Back Edit Secu	rity Policy	
Basic Info		
* Name	VPN-outbound	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group ~	⊕ Add Group
Description	Enter the security policy name descrip	
Src. and Dest.		
* Src. Security Zone	any \lor	
* Src. Address	VPN-localsubnet \sim	
User/User Group	any \vee	
* Dest. Security	VPN-Zone \lor	
Zone		
* Dest. Address	VPN-remotesubnet \sim	
Service		
Service	any \checkmark	

< Back Edit Secu	rity Policy			
Basic Info				
* Name	VPN-inbound			
Enabled State	• Enable 🔿 Disable			
* Policy Group	Default Policy Group	Add Group		
Description	Description Enter the security policy name description			
Src. and Dest.				
* Src. Security Zone	VPN-Zone \lor			
* Src. Address	VPN-remotesubnet ~			
User/User Group	any ~			
* Dest. Security	any ~			
Zone				
* Dest. Address	VPN-localsubnet ~			
Service				
Service	any \lor			

- (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.

K Back Ed	lit Static Rou	ting	
	IP Туре	IPv4	
* Dest.	IP Range/Mask	192.168.1.0/24	
Nex	t-Hop Address		
	Interface	vti1	\sim
	* () Priority	5	
	Link Detection	Link Detection	\sim
	Description	ipsec-route	
			- 11

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.

Ľ	Tunnel Monitoring							
	Start Stop	Refresh Custom Field				Enter a tunnel name		Q
	Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sei	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							
Start Stop	Refresh Custom Fi	eld			Enter a tu	nnel name.	Q
Tunnel Name	Tunnel Status	Туре	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.





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

- 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.

(1)	(2)-					4)
Basic Config	Authenticatio	on Config	Interes	sting Traffic	Config	Config Verification
	* () Tunnel Interface	vti 2				
	* Tunnel Name	tunnel-to-	Fortinet		\otimes	
	* Scenario	• Point-to-	Point) Point-to-M	ultipoint	
					Propeh	
				Internet		once
		Main	Office			
					Branch	Office
	Conc	al	Novt			
	Canc		Next			

(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.

Ø	2			-3		4
Basic Config	Authenticatic	on Config	Interestin	g Traffic Con	fig	Config Verification
	* Peer Address	10.51.212.2	236		Ping	
	* Outbound Interface	Ge0/0			~	
	* Authentication Mode	 Pre-share 	ed Key			
	* 🕕 Key	•••••				
	* 🕕 Confirm Key	•••••		(8	
	[] [
	Previous	Cancel	Nex	ct		

(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.

O Create	T Dalata		Entor the	konword	0
Create	Uelete		Enter the	e keyword.	ų
D PI	oxy Mode	Local Network	Peer Network	Operation	
Sub	onet-to-Su	192.168.1.0/24	192.168.2.0/24	Edit Delete	
10 ~	/ Page Total:1			Go to 1 < 1	>

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

4. Verification

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

Ø	⊘		Ø		4
sic Config	Authenticatic	on Config	Interesting Traffi	c Config	Config Verification
	Basic Config	Edit			
	Tunnel Interface	vti2	~		
	Tunnel Name	tunnel-to-Fortinet			
	Scenario	Point-to-Point	Point-to-Multi	point 🕕	
	Authentication Config	Edit			
	Peer Address	10.51.212.236			
	Outbound Interface	Ge0/0	~		
	Authentication Mode	Pre-shared Key			
	① Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Peer	Network	
	192.168.1.0/24		192.1	68.2.0/24	

- (2) Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.
- IKE parameters:
 - o Set IKE Version to IKEv1.
 - Set Negotiation Mode to IKEv1 Main Mode.
 - Set Encryption Algorithm to AES-128.
 - o Set Verification Algorithm to SHA.
 - o Set DH Group to GROUP5.

Advanced Settings	Fold	
* Local ID Type	IPV4_ADDRESS ~	
① Peer ID Authentication		
DPD Type	Regular Mode \vee	
DPD Detection Interval	30	Second
DPD Retry Interval	5	Second
IKE Parameter		
IKE Parameter * ① IKE Version	☑ IKEv1	
IKE Parameter * ① IKE Version * ① Negotiation Mode	IKEv1 IKEv2 IKEv1 Main Mode	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm	 ✓ IKEv1 □ IKEv2 IKEv1 Main Mode ∨ AES-128 ⊗ ∨ 	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm * ① Verification Algorithm	 ✓ IKEv1 □ IKEv2 IKEv1 Main Mode ~ AES-128 ⊗ ~ SHA ⊗ ~ 	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm * ① Verification Algorithm * ① H Group	 ✓ IKEv1 □ IKEv2 IKEv1 Main Mode ✓ ✓	

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

≣↑ IPsec Parameter

* Protoco	ESP		~	
* Encapsulation Mod	le Tunnel		\sim	
* Encryption Algorithm	M AES-128 ®		\sim	
* Verification Algorithm	m SHA ®		\sim	
Perfect Forward Secred	xy 💽			
* DH Grou	p GROUP5		~	
* 🕕 SA Lifetim	ae 3600			Second
① Tunnel MT	U 1400			
Previous	Cancel	Finish		

(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					
1 VPN Setup	2 Authentication $>$ 3 Policy & Routing $>$ 4 Review Settings				
Name	tunnel-to-z32-s		Site to Site - FortiGate		
Template type	Site to Site Hub-and-Spoke Remote Access Custom				<u>^</u>
NAT configuration	No NAT between sites				
	This site is behind NAT			Internet	
	The remote site is behind NAT				
Remote device type	FortiGate		This FortiGate		Remote FortiGate
	and cisco				
		- De els	ta Carat		
		< Back Nex	t > Cancel		

(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			
VPN Setup 2 A	uthentication > 3 Policy & Routing	3 A Review Settings	
Remote device	IP Address Dynamic DNS	Site to Site - FortiGate	
Remote IP address	172.17.149.218		^
Outgoing Interface	im wan1 (mgmt)		
Authentication method	Pre-shared Key Signature	Internet	
Pre-shared key	•••••		
		inis Fortigate H	emote FortiGate
		< Back Next > Cancel	

(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.
| VPN Creation Wizard | | | |
|---------------------|-----------------------------------|--------------------------|------------------|
| VPN Setup | Authentication 3 Policy & Routing | Review Settings | |
| Local interface | 🖮 wan1 (mgmt) 🗙 | Site to Site - FortiGate | |
| Local subnets | 192.168.2.0/24 | | |
| | 0 | Internet | |
| Remote Subnets | 192.168.1.0/24 | | |
| | • | This FortiGate | Remote FortiGate |
| Internet Access 🚯 | None Share Local Use Remote | | |
| | | | |
| | | < Back Next > Cancel | |
| | | | |

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

VPN Creation Wizard	
The of outlot the dra	
VPN Setup 🔪 🗸	Authentication V Policy & Routing Active Settings
• The following set	ttings 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
	< Back Create Cancel

(3) After verifying the configuration, click Create.

4. VPN Authentication Configuration

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

H	Create New 🔹 🤞	🖊 Edit 🗎 🗊 Delet	e Lul Show Matching Lo	gs Search	(2	
		Tunnel ≑			Interface Binding \$	Status 🗢	Ref. 🗘
۵	📰 Site to Site - For	tiGate ③					
	O 11			internal (port5)		O Inactive	2
	🔮 s2s			m port2		O Inactive	2
	🔮 tunnel-to-z32-s	5		🖮 wan1 (mgmt)		O Inactive	4
Ð	□ Custom 2	IPsec Tunnel	🔮 tunnel-to-z32-s				
		Туре	💶 Site to Site - FortiGate				
		Remote Gateway	172.17.149.218				
		Phase 2 Tunnel	🔮 tunnel-to-z32-s				
	Phase 1 O tunnel-to-z32-s						
	Comments VPN: tunnel-to-z32-s (Created by VPN wizard)		eated by VPN				
		References	4				
		🖋 Edit					

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

+Create New - Edit 🗎 🖻 Delete 🛛 🖽 Show Matching Lo	gs Search	Edit VPN Tunnel		
Tunnel \$	Interfac	Tunnel Template	Site to Site - FortiGate	
🖃 🗱 Site to Site - FortiGate 🚳			Convert To Custom Tunnel	
• 11	internal (port5)			
♥ s2s	im port2	Name	tunnel-to-z32-s	
🔮 tunnel-to-z32-s	🏾 wan1 (mgmt)	Comments	VPN: tunnel-to-z32-s (Created by VPN wizard)	
		Network	🖋 Edit	
		Remote Gateway :	Static IP Address (172.17.149.218), Outgoing Interface : mgmt	
		Authentication	🖋 Edit	
		Authentication Me	hod : Pre-shared Key	
		Phase 2 Selectors	Address Remote Address	
		tunnel- to- tunnel- z32-s	o-z32-s_local tunnel-to-z32-s_remote	
			OK Cancel	

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

Phase 1 Proposal	🖋 Edit				
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.

	Phase 1 Proposal	O Add				3	0	ບ
1	Encryption	AES128	•	Authentication	SHA1	•		
	Diffie-Hellman Group			31 30 20 19 14 ✓	29 28 18 17 2 1) 27) 16		
	Key Lifetime (secor	nds)	86400) 2] '		
	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	5		
Name	Local Address	Remote Address	O Add
tunnel-to-z32-s	tunnel-to-z32-s_local	tunnel-to-z32-s_remote	ø

- 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			4 🕑 ୯			
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	1			
Advanced						
Phase 2 Proposal	Add					
Encryption	AES128	Authentication SHA1	✓ 2			
Enable Replay Det	ection 🔽					
Enable Perfect For	ward Secre	cy (PFS) 🔽				
Diffie-Hellman Gro	oup	32 31 30 29 28 21 20 19 18 17 15 14 5 2 1	27 16			
Local Port		All 🗹 3				
Remote Port		All 🗹				
Protocol		All 🗹				
Auto-negotiate						
Autokey Keep Alive						
Key Lifetime						
Key Lifetime	e	Seconds				

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

+Create New - Zelit 🗍 Delete 🔟 Sho	w Matching Logs Search	Edit VPN Tunnel			
Tunnel ≑	Interf	ace Name	tunnel-to-z32-s		
			VPN: tunnel-to-z32-s (Cre	ated by VPN	
• 11	internal (port5)	Comments	wizard)		
○ s2s	m port2			4	
🙁 tunnel-to-z32-s	🖮 wan1 (mgmt)				
		Network		de Edit	
		Remote Gate	way : Static IP Address (172.17.149.218)	, Interface : mgmt	
		Authentication		🖉 Edit	
		Authenticatio	on Method - Pre-shared Key		
		IKE Version ::	1 Mode : Main (ID protection)		
		ince version			
		Phase 1 Propos	al	🖋 Edit	
		Algorithms : A	AES128-SHA1		
		Diffie-Hellma	in Group : 5		
		XAUTH		🖋 Edit	
		Type : Disable	ed		
		Dhase 2 Selecto	vre		
		Name	Local Address Remote	Address O Add	
		rallie	Local Audress Relificie		
		tunnel-to-z32-s	192.168.2.0/24 192.16	8.1.0/24 <i>F</i>	
		_			
				OK Cancel	

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 N	Ionitoring								
⊘ Start	Stop Refresh	Custom Field						Enter a tunnel name.	Q
	Tunnel Name	Tunnel Status	Туре	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.

IPsec V	PN Logs						
🚺 Expo	rt C Refresh	Custom Field	Date 2024-08-23	to 2024-08-23	Log Level All	 Enter a tunnel name, a peer address or a details. 	
Lo	g Level	Time	Tunnel Name	Peer Address		Details	
• 1	Vedium	2024-08-23 19:22:37	tunnel-to-Fortinet	10.51.212.236	IKE SA建立完成, cookie为: bce7f9412dacc6a4:8ca6232faf5d9cce		
• 1	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.

+Create New - & Edit Delete	ogs Search	Q				
Tunnel 🗢 Interface Binding 🗢		Ref. 🗢	Template 🗢			
🗹 🛇 Inactive 🚱						
♦ tunnel-to-z32-s	im wan1 (mgmt)	4	🖵 Custom			

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

IPsec VPN Typical Configuration Examples

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

[+Create New 🔹 🖋 Edit 🖄 Delete	Le Show Matching Logs	Search	Q				
Tunnel 🗢			Interface Binding 🗢	Ref. 🗢	Template 🗘			
I	E O inactive G							
I								
	O tunnel-to-z32-s	m	wan1 (mgmt)	4	😐 Custom			

Summary O Logs								
C VPN Tunnel == tunnel-to-z3	VPN Tunnel == tunnel-to-z32-s X O Q Search							
Date/Time	Level	Action	Status	Message	VPN Tunnel T			
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 <u>Figure 4-1</u>. In a site-tomultisite 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.





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.

1	2	3	4
Basic Config	Authentication	Config Interesting Traffic Config	Config Verifica
	* 🕕 Tunnel Interface	vti 100	
	* Tunnel Name	Hub-Spoke	
	* Scenario	O Point-to-Point O Point-to-Multipoir	nt
		Main Office Branch Office Branch Office	
	Cancel	Next	

- c After completing the configuration, click Next.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

<i>_</i>		2			3		4
Basic Cor	nfig Au	Ithentication	Config	Interesti	ng Traffic Config		Config Verification
	* Outbo	ound Interface	Ge0/2			~	
	* Authen	tication Mode	• Pre-sł	nared Key			
		* Key	•••••	•			
		* Confirm Key	•••••	•		(\times)	
_							
	Previous	Cancel		Next			

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

Basic Config		Authe	Authentication Config		3 Interesting Traffic Config		
	🕀 Creat	e 🔟 Delete		Enter th	e keyword.	Q	
		Proxy Mode	Local Network	Peer Network	Operation		
		Auto	any	any	Edit Delete	e	
	10 ~	/ Page Total:1			Go to 1 <	1	

Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

⊘ Basic Config	Authentication	Config Interesting Traffic C	onfig Config Verification
① The tunnel configured on the wizard will be added to the	he custom tunnel list.		
	Basic Config	Edit	
	Tunnel Interface	vti100 ~	
	Tunnel Name	Hub-Spoke	
	Scenario	Point-to-Point () Point-to-Mult	ipoint 🕕
	Authentication Config	Edit	
	Outbound Interface	Ge0/2 ~	
	Authentication Mode	Pre-shared Key	
	Key		
	Interesting Traffic Config	Edit	
	Local Network	Peer Net	work
	any	any	
	Advanced Settings	Expand	
	Previous Car	icel Finish	

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	2					
Basic Config	Authentication	Config	Interest	ing Traff	ic Config	Config Verificatio
	* () Tunnel Interface	vti	100			
	* Tunnel Name	Site-to	-Site			\otimes
	* Scenario	 Point 	t-to-Point	🔿 Poi	nt-to-Multip	point
		Main	Office	nternet	Branch Office	
	Cancel	Next				

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

O Basic Config	Q Authentication Config		3 Interesting Traffic Config		Config Verification		
	* Peer Address	10.1.5.211	\otimes	Ping			
	* Outbound Interface	Ge0/2	\sim				
	* Authentication Mode	• Pre-shared	Кеу				
	* Key	•••••					
	* Confirm Key	•••••					

Previous	Cancel	Next	

- b After completing the configuration, click Next.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.

⊘ Basic Config		Authentication Config		3- Interesting Traf	Config Verification		
	Crea	te 🔟 Delete		Enter ti	ne keyword.	Q	
		Proxy Mode	Local Network	Peer Network	Operation		
		Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	Edit Delete	e	
	10 ~	/ Page Total:1			Go to 1	1	

- b After completing the configuration, click Next.
- (4) Verify configuration.

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

Ø	©)			4
Basic Config	Authenticati	on Config	Interesting Traf	fic Config	Config Verification
ill be added to the custom tun	nel list.				
	Basic Config	Edit			
	Tunnel Interface	vti100			
	Tunnel Name	Site-to-Site			
	Scenario	Point-to-Point ①	 Point-to-Multip 	point 🕕	
	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		Pee	r Network	
	192.168.3.0/24		192.1	68.100.0/24	
	Advanced Settings	Expand			
	Previous	Cancel Finis	sh		

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:
 - o Set Interface Name to vti100.
 - o Add security zone VPN-Zone and set Security Zone to VPN-Zone for this interface.
 - o 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 v	⊕ Add Security Zone
* Tunnel Local Address	10.1.5.211	
Tunnel Remote Address	O IP O 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:

- o Set Tunnel Name to Hub-Spoke.
- o 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**.

(1)	2	3
Basic Config	Interesting Traffic Config	Security Parameter Config
* Scenario	 Point-to-Point ① Point-to-Multip 	point ()
* Tunnel Name	Hub-Spoke	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	vti100 \lor	
* Authentication Mode	Pre-shared Key \sim	
* Key	•••••	
* Confirm Key	•••••	
* Local Address	● Interface IP	
	Ge0/2 v	
* Local ID Type	IPV4_ADDRESS ~	
Verify Peer ID		
≣ ↑ Advanced		
Reverse Route Injection		
Next-Hop Address	Enter Next-Hop Address	
* Priority	5	
с	ancel Next	

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.

	Ø	2)	3	
	Basic Config	Interesting Tr	affic Config	Security Parameter Config	I
🕀 Create	e 🔟 Delete		Enter	the keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	Auto	any	any	Edit Delete	
10 ~	/ Page Total:1			Go to 1 < 1	>

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.



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 Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-outbound		
Enabled State	• Enable O Disable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	any	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	VPN-Zone	\sim	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

< Back Create Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-inbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	Add Group
* Adjacent Policy	Default Policy	~	Before v
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	VPN-Zone	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	any	~	
Zone			
* 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:
 - o Set Interface Name to vti1.
 - o Add security zone VPN-Zone and set Security Zone to VPN-Zone for this interface.
 - o Set **Tunnel Local Address** to the default outbound interface address of Site A: 10.1.5.203.
 - o Set **Tunnel Remote Address** to the default outbound interface address of the hub site: 10.1.5.211.

< Back Edit Tunnel Int	erface Details	
* Interface Name	vti1	
Security Zone	VPN-Zone v	⊕ 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:

- o Set Tunnel Name to Site-to-Site.
- o Set Enabled State to Enable.
- o 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**.

1	2	3
Basic Config	Interesting Traffic Config	Security Parameter Config
* Scenar	io 💿 Point-to-Point 🕕 🔿 Point-to-Mult	ipoint 🕕
* Tunnel Nam	Site-to-Site	
Descriptio	Enter Tunnel Description	
* Enabled Sta	te 💿 Enable i Disable	
* Tunnel Interfac	ce vti1	Add Tunnel Interface
* Authentication Mod	de Pre-shared Key	/
* Ke	ey	
* Confirm Ke	еу	
* Local Addres	ss 💿 Interface 🕕 🛛 IP 🕕	
	Ge0/2	·
* Peer Addre	ss 10.1.5.211 0	Ping
* Local ID Typ	De IPV4_ADDRESS	/
Verify Peer I	D	
<u>≣</u> ↓ Advance	d	
	Cancel Next	

After completing the basic configuration, click $\ensuremath{\textit{Next}}.$

b Configure interesting traffic.

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

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

	O Basic Config	Interesting 1	2) Traffic Config	Security Parameter Con	fig
🕀 Crea	ate 🔟 Delete		Ente	er the keyword.	Q
	Proxy Mode	Local Network	Peer Network	Operation	
	Subnet-to-Subnet	192.168.3.0/24	192.168.100.0/24	4 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.

isic coning interes	sting Traffic Config	Security Paramet	er
		Config	
IKE Parameter			
* Negotiation Mode	IKEv1 Main Mode	~	
* Encryption Algorithm	AES-128 🛞	~	
* Verification Algorithm	SHA 🛞	~	
* DH Group	GROUP5 ®	~	
* ① SA Lifetime	86400		Second
IPsec Parameter			
* Protocol	ESP	~	
	Tunnel		
* Encapsulation Mode	Turrier	~	
* Encapsulation Mode * Encryption Algorithm	AES-128 ®	~	
* Encapsulation Mode * Encryption Algorithm * Verification Algorithm	AES-128 ®	`	
* Encapsulation Mode * Encryption Algorithm * Verification Algorithm Perfect Forward Secrecy	AES-128 ®	× ×	

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.

IPv4 Address	IPv6 Address	IPv4 Address Group	IPv6 Address Group		
 Oreate ☑ Delete ☑ Refresh 					
Name		IP Address/Range	Address Group		
		-			
VPN-remot	esubnet	192.168.100.0/24	-		

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.

Back Edit Security Policy					
Basic Info					
* Name	VPN-outbound				
Enabled State	• Enable 🔿 Disable				
* Policy Group	Default Policy Group	⊕ Add Group			
Description	Enter the security policy name descrip				
Src. and Dest.					
* Src. Security Zone	any ~				
* Src. Address	VPN-localsubnet \vee				
User/User Group	any \vee				
* Dest. Security	VPN-Zone ~				
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	any ~			
Zone				
* 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 Rou	iting
	IP Туре	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.

11	unnel Monitoring							
	⊘ Start 🚫 Stop 🕻	Refresh Custom Fie	eld			Enter a tunnel nar	me.	Q
	Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent	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.

1	Tunnel Monitoring							
	Start Stop	C Refresh Custom Field				Enter a tunnel na	me.	Q
	Tunnel Name	Tunnel Status	Туре	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 <u>Figure 5-1</u>, 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.





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

- 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.

1	2_		(3)		-4
Basic Config	Authentication	n Config	Interesting	Traffic Config	Confi	g Verification
	* ① Tunnel Interface	vti 2				
	* Tunnel Name	tunnel-to-Fo	ortinet	\otimes		
	* Scenario	• Point-to-Po	oint 🔿 Poin	t-to-Multipoin	t	
		W.	Inte	rnet	anch Office	
		Main C	Office			
				Br	anch Office	
	Cance	el	Next			

(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.

Ø	2-		3			
Basic Config	Authenticatio	n Config	Interesting Tra	affic Config	С	onfig Verification
	* Peer Address	10.51.212.2	36		Ping	
	* Outbound Interface	Ge0/0		\sim		
	* Authentication Mode	• Pre-share	d Key			
	* () Key	•••••				
	* 🕕 Confirm Key	•••••		\otimes		
	Deview	Canad	Neut			
	Previous	Cancel	Next			

(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.

<mark>⊘</mark> asic Co	onfig	Auther	⊘ ntication Config	Interesting	3 Traffic Config	Config Veri	fication
	🕀 Cre	ate 🔟 Delete		Enter the	e keyword.	Q	
		Proxy Mode	Local Network	Peer Network	Operation		
		Subnet-to-Su	192.168.2.0/24	192.168.1.0/24	Edit Delet	te	
	10 ~	/ Page Total:1			Go to 1	1 >	
		Previou	s Cancel	Next			

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

4. Verification

B

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

Ø					4
Basic Config	Authenticatio	on Config	Interesting Traffic	c Config	Config Verification
	Basic Config	Edit			
	Tunnel Interface	vti2	~		
	Tunnel Name	tunnel-to-Fortinet			
	Scenario	Point-to-Point	Point-to-Multip	point 🕕	
	Authentication Config	Edit			
	Peer Address	10.51.212.236			
	Outbound Interface	Ge0/0	~		
	Authentication Mode	 Pre-shared Key 			
	① Кеу				
	Interesting Traffic Config	Edit			
	Local Network		Peer	Network	
	192.168.2.0/24		192.10	68.1.0/24	

- (2) Click **Advanced Settings** and modify the following IKE and IPsec parameters. Use the default configuration for the other parameters.
- IKE parameters:
 - o 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		
DPD Type	Regular Mode \vee	
DPD Detection Interval	30	Second
DPD Retry Interval	5	Second
IKE Parameter		
IKE Parameter * ① IKE Version	✓ IKEv1 □ IKEv2	
IKE Parameter * ① IKE Version * ① Negotiation Mode	✓ IKEv1 □ IKEv2 IKEv1 Main Mode ✓	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm	 ✓ IKEv1 □ IKEv2 IKEv1 Main Mode ∨ AES-128 ⊗ ∨ 	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm * ① Verification Algorithm	 ✓ IKEv1 □ IKEv2 IKEv1 Main Mode ∨ AES-128 ⊗ ∨ SHA ⊗ ∨ 	
IKE Parameter * ① IKE Version * ① Negotiation Mode * Encryption Algorithm * ① Verification Algorithm * DH Group	IKEv1 IKEv2 IKEv1 Main Mode AES-128 SHA GROUP5	

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

≣↑ IPsec Parameter

* Protocol	ESP	
* Encapsulation Mode	Tunnel	
* Encryption Algorithm	AES-128 🛞	
* Verification Algorithm	SHA 🛞 🗸	
Perfect Forward Secrecy		
* DH Group	GROUP5 ~	
* 🕕 SA Lifetime	3600	Second
① Tunnel MTU	1400	
Previous	Cancel Finish	

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 Wi	zard	
VPN Setup Name Template type	Authentication O Tunnel Interface Policy & Routing S R tunnel-to-RJ Site to Site Hub-and-Spoke Remote Access Custom The Hub-and-Spoke VPN will be set up using auto-discovery with BGP as the routing protocol.	eview Settings Hub-and-Spoke - FortiGate (Hub)
Role 0	Hub Spoke	This FortiGate Bemote FortiGate Remote FortiGate
		< Back Next > Cancel

(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				
VPN Setup	Authentication $>$ 3 Tunnel Interfa	ce $>$ 4 Policy & Routing $>$ 5 Review Settings	3	
Incoming Interface	🔳 wan1 (mgmt)	-	Hub-and-Spoke - FortiGate (Hub)	
Authentication method	Pre-shared Key Signature		Spoke1	
Pre-shared key		۲	Hub This FortiGate Hub Internet This FortiGate Remote FortiG	iate
		< Back	Next > Cancel	

(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 🔪 🗸 A	uthentication 3 Tunnel Interface	4 Policy & Routing > 5 Review Settings	
Tunnel IP 🚯	10.10.3.1		Hub-and-Spoke - FortiGate (Hub)
Remote IP/netmask	10.10.3.2/24		Spoke1
			Hub This FortiGate Remote FortiGat Remote FortiGat
		< Back	Next > Cancel

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.



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

VPN Creation Wizard	
✓ VPN Setup > ✓	Authentication 🔰 🗸 Tunnel Interface 🔪 🗸 Policy & Routing 🔰 🗿 Review Settings
The following set	ttings 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
	< Back Create Cancel

(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.

Ľ	Tunnel Monitoring										
	⊘ Start	Stop Refresh	Custom Field						Enter a tunnel name.	Q	
		Tunnel Name	Tunnel Status	Туре	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.

Psec VPN Logs								
🚺 Export 🖸 Refree	h 🖪 Custom Field	Date 2024-08-23	to 2024-08-23	Log Level All ~ Enter a tunnel name, a peer address or a details. Q				
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.

+	Create New 👻 🖌 Kit 🖄 Delete 🖬 Show Matching Logs	Search	Q				
	Tunnel 🗢	٣	Interface Binding 🜩	Ref. ≑			
	🖃 😫 Hub-and-Spoke-FortiGate (Hub) 🕢						
	• tunnel-to-RJ		🖮 wan1 (mgmt)	4			

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

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

+Create New - A Edit Delete	L Show Matching Logs Search	٩				
Tunnel 🗢	т	▼ Interface Binding \$				
🖃 🗱 Hub-and-Spoke - FortiGate (Hub) 🥑						
📀 tunnel-to-RJ		🔳 wan1 (mgmt)	4			

Summary O Logs								
C VPN Tunnel == tunnel-to-RJ X C Q Search C Details								
Date/Time	Level	Action	Status	Message	VPN Tunnel T			
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. <u>Figure 6-1</u> shows the typical networking diagram.





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.

1	2		3_		
Basic Config	Authentication	Config	Interesting Traf	fic Config	Config Verification
	* 🕕 Tunnel Interface	vti	100		
	* Tunnel Name	test1			
	* Scenario	O Poin	t-to-Point 💿 Po	oint-to-Multipc	pint
		Mair	Internet	Branch Office	
	Cancel	Next			

- c After completing the configuration, click **Next**.
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø		2		3		(4)
Basic Con	fig <mark>A</mark> ı	Ithentication	Config	Interesting Traffic (Config	Config Verification
	* Outbo	ound Interface	Ge0/2		\sim	
	* Authen	tication Mode	• Pre-sł	nared Key		
		* Key	•••••	0		
		* Confirm Key	•••••	•	\otimes	
_						
	Previous	Cancel		Next		

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.
| onfig | Author | | (| 3 | Config | (4)
Verification |
|---------|----------------|---------------|--------------|-------------|--------|---------------------|
| • Creat | e 🔟 Delete | | Enter th | le keyword. | Q | venneauon |
| | Proxy Mode | Local Network | Peer Network | Operation | | |
| | Auto | any | any | Edit Delete | е | |
| 10 🗸 | / Page Total:1 | | | Go to 1 < | 1 | |

Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

(~) 	(~)	(~)		(4)
Basic Config	Authenticati	on Config	Interesting Traf	fic Config Co	onfig Verification
pe added to the cu	istom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti100	\sim		
	Tunnel Name	test1			
	Scenario	O Point-to-Point (1)	Point-to-Multip	point ()	
	Authentication Config	Edit			
	Outbound Interface	Ge0/2	~		
	Authentication Mode	 Pre-shared Key 			
	Key	0000000			
	Interesting Traffic Config	Edit			
	Local Network		Pee	r Network	
	any			any	
	Advanced Settings	Expand			
			_		
	Previous	Cancel Finisl	h		

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	2		3		4
Basic Config	Authenticatio	n Config	Interesting Traffic	Config	Config Verification
	* ① Tunnel Interface	vti 1			
	* Tunnel Name	test1		\otimes	
	* Scenario 🧧	Point-to-Po	pint 🔿 Point-to-Mu	Itipoint	
			_		
			Branch Office		
			Internet		
		Main Office	Branch Office	611	
			_		
	Cancel	Next			

- c After completing the configuration, click $\ensuremath{\textbf{Next}}.$
- (2) Configure authentication.
 - a Configure parameters according to the following figure.

Ø	2		3		4
Basic Config	Authenticati	on Config	Interesting Traffic Conf	ig	Config Verification
	* Peer Address	2.1.1.2	\otimes	Ping	
	* Outbound Interface	Ge0/2	~		
	* Authentication Mode	 Pre-shared 	Кеу		
	* Key	•••••			
	* Confirm Key	•••••			

Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (3) Configure interesting traffic.
 - a Click Create. Configure parameters for interesting traffic according to the following figure.



Previous	Cancel	Next

- b After completing the configuration, click **Next**.
- (4) Verify configuration.
 - a After verifying the configuration, click **Finish**.

Ø	⊘		⊘		4
Basic Config	Authentication	Config	Interesting Traffic Co	onfig Co	nfig Verification
I will be added to the cu	istom tunnel list.				
	Basic Config	Edit			
	Tunnel Interface	vti1	\sim		
	Tunnel Name	test1			
	Scenario	Point-to-Point	O Point-to-Multi	point ()	
	Authentication Config	Edit			
	Peer Address	2.1.1.2			
	Outbound Interface	Ge0/2	~		
	Authentication Mode	Pre-shared Key	/		
	Key				
	Interesting Traffic Config	Edit			
	Local Network		Peer Net	work	
	100.100.70.0/24		200.200.30	.0/24	
	Advanced Settings	Expand			
	Previous Can	icel Finis	sh		

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:
 - o Set Interface Name to test1.
 - o 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.

< Back Create Tunnel	Interface Details	
* Interface Name	test1	
Security Zone	VTI ~	⊕ Add Security Zone
* Tunnel Local Address	2.1.0.1	
Tunnel Remote Address	O IP O 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:

- o Set Tunnel Name to test1.
- Set Enabled State to Enable.
- o Set Tunnel Interface to test1.
- o 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**.

1	3	
Basic Config Interesti	ng Traffic Config Security Parameter	
	Config	
* Scenario	Point-to-Point () Point-to-Multip	point ()
* Tunnel Name	test1	
Description	Enter Tunnel Description	
* Enabled State	• Enable 🔿 Disable	
* Tunnel Interface	test1 ~	Add Tunnel Interface
* Authentication Mode	Pre-shared Key \sim	
* Key		
* Confirm Key		
* Local Address	• Interface 🔿 IP	
	Ge0/2 ~	
* Local ID Type	FQDN V	
* Local Identity	71.com	
≣↑ Advanced		
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:

o Set Proxy Mode to Auto.

	⊘ Basic Config	Interesting T	2) Traffic Config	3 Security Parameter Cont	fig
🕒 Creat	e <u> </u> Delete		Ente	r the keyword.	Q
	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.

Ø	⊘		3
Basic Config	Interesting Traffic Config	Secu	rity Parameter Config
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 🛞	\sim	
* Verification Algorithm	SHA 🛞	~	
Perfect Forward Secrecy			
* 🕕 SA Lifetime	604800		Second
① Tunnel MTU	1400		
Previous C	ancel Finish		

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
① Anti-Replay Attack		
Anti-Replay Window	64 ~	
Action Specified by DF Bit	clear v	

- (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 Se	curity Policy		
Basic Info			
* Name	VPN-hub-outbound		
Enabled State	• Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	any	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	VTI	~	
Zone			
* Dest. Address	any	~	
Service			
Service	any	~	

< Back Create Se	ecurity Policy		
Basic Info			
* Name	VPN-hub-inbound		
Enabled State	● Enable 🔿 Disable		
* Policy Group	Default Policy Group	~	⊕ Add Group
* Adjacent Policy	Default Policy	~	Before \lor
Description	Enter the security policy name descrip		
Src. and Dest.			
* Src. Security Zone	VTI	~	
* Src. Address	any	~	
User/User Group	any	~	
* Dest. Security	any	~	
Zone			
* 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:
 - o Set Interface Name to out.
 - o Add security zone VTI and set Security Zone to VTI for this interface.
 - o Set **Tunnel Local Address** to the default outbound interface address of Site A: 2.1.0.2.
 - o Set Tunnel Remote Address to the default outbound interface address of the hub site: 2.1.1.2.

< Back Create Tunnel	Interface Details	
* Interface Name	out	
Security Zone	VTI ~	⊕ Add Security Zone
* Tunnel Local Address	2.1.0.2	
Tunnel Remote Address	• IP O 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:

- o Set Tunnel Name to to_71.
- o Set Enabled State to Enable.
- o Set Tunnel Interface to out.
- o 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**.

1		-2	3			
Basic Config	Interestir	ng Traffic Config	Security Paramete	er		
			Config			
	* Scenario	Point-to-Point	🕕 💿 Point-to-Mu	ultipo	oint 🕕	
	* Tunnel Name	to_71				
	Description	Enter Tunnel Des	scription			
	* Enabled State	💿 Enable 🔿 I	Disable			
*	Tunnel Interface	out		~	🕀 Add T	unnel Interface
* Authe	entication Mode	Pre-shared Key		~		
	* Key	*****				
	* Confirm Key	*****				
	* Local Address	O Interface (1)	• IP 1)			
		2.1.0.2				
	* Peer Address	2.1.1.2			Ping	
	* Local ID Type	FQDN		~		
	* Local Identity	70.com				
	Cancel	Next				

After completing the basic configuration, click $\ensuremath{\textit{Next}}.$

b Configure interesting traffic.

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

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

	O Basic Config	Interesting 1	2) Traffic Config	Security Parameter Con	fig
🕀 Crea	ate 🔟 Delete		Ente	er the keyword.	Q
	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

* Pr	rotocol ESP		~	
* Encapsulation	Mode Tunn	el	~	
* Encryption Alg	orithm AES-1	28 🛞	~	
* Verification Alg	orithm SHA (0	~	
Perfect Forward S	ecrecy			
* 🕕 SA Li	fetime 6048	00		Second
Previous	Cancel	Finish		

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		
* ① 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 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.

IPv4	Address	IPv6 Address	IPv4 Address Group	IPv6 Address G	roup
🕀 Cre	eate 🔟 De	elete			
	Name		IP Address/Range	Address Group	Descr
	test1_remo	te	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.

K Back Edit Secu	rity Policy	
Basic Info		
* Name	test1_out	
Enabled State	• Enable 🔾 Disable	
* Policy Group	Default Policy Group ~	Add Group
Description	by tunnel wizard test1	
Src. and Dest.		
* Src. Security Zone	any \lor	
* Src. Address	test1_local ~	
User/User Group	any ~	
* Dest. Security	test1 ~	
Zone		
* Dest. Address	test1_remote ~	
Service		
Service	any ~	

< Back Edit Secu	ırity Policy	
Basic Info		
* Name	test1_in	
Enabled State	• Enable 🔿 Disable	
* Policy Group	Default Policy Group	⊕ Add Group
Description	by tunnel wizard test1	
Src. and Dest.		
* Src. Security Zone	test1 ~	
* Src. Address	test1_remote ~	
User/User Group	any \vee	
* Dest. Security	any \checkmark	
Zone		
* Dest. Address	test1_local ~	
Service		
Service	any \lor	

- (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.

< Back	Edit Static Rou	iting
	IP Туре	IPv4
* [Dest. IP Range/Mask	200.200.30.0/24
	Next-Hop Address	
	Interface	out \checkmark
	* () 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.

T	unnel Monitoring	1					
	Start Stop	C Refresh Custom F	ield			Enter a tunnel name.	Q
	Tunnel Name Tunnel Status		Туре	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 N	Vonitoring					
⊘ Start	Stop C Refresh	Enter a tunnel name.	Q			
	Tunnel Name	Tunnel Status	Туре	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

192.168.2.2

192.168.2.1

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.





7.3 Restrictions and Guidelines

192.168.1.2

192.168.1.1

• 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

- 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.

Ruijie Z Series Firewall	ය Home ම Monitor	Network	우 Object 🛛 영 Policy	© System	(L) Quick Onboarding	Ø Policy Wizard	G Customer Service	Q admin
Interface Physical Interface	Config Wizard							
Subinterface			1 Basic Config	O Authentication Config Interesting Traffic Config	(4) Config Verification			
Bridge Interface Aggregate Interface				* ① Tunnel Interface vti 1				
Tunnel Interface				Tunnel Name Primary				
lig Zone →				* Scenario O Point-to-Point O Point-to-Multipoint				
SSL VPN >								
Tunnel Monitoring				there have been block				
Config Wizard Custom Tunnel				Main Office Branch Office				Con
Advanced Settings Details								Ę
IEI DNS 〉 同 DHCP 〉								
© Link Detection								
Neiobhor Status				Cancel Next				

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

2. Configuring Authentication

(1) Configure parameters according to the following figure.

Configuration Examples of IPsec VPN Networking with Link Redundancy

Ruffie Z Series Firewall	û Home	Network	A Object 🖾 Policy	😒 System				L Quick Onboarding	Ø Policy Wizard	Customer Service	ې admin
Interface ~	Config Wizard										
Subinterface			⊘	(2	3		(4)			
Bridge Interface			Basic Config	Authentica	tion Config	Interesting Traffi	c Config	Config Verification			
Aggregate Interface				* Outbound Interface	Ge0/1						
Tunnel Interface				* Authentication Mode	Pre-shared Key						
[편] Zone				* Key	•••••						
SSL VPN				* Confirm Key							
IPsec VPN Y											
Tunnel Monitoring											
Config Wizard											
Custom Tunnel											onsult
DNS											
DHCP >											
O Link Detection											
				Previous	Cancel	Next					

(2) After completing the configuration, click Next.

3. Configuring Interesting Traffic

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

Ruífie Z Series Firewall	☆ Home G Monitor	Network	,₽_ Object	Policy	System				1 Quick Onboarding	Ø Policy Wizard	G Customer Service	오 admin
Interface Physical Interface Subinterface	Config Wizard		Ø)		⊘	3		(4)			
Bridge Interface Aggregate Interface			Basic C	Config © Create	Auth	nentication Config	Interesting Tra	ffic Config Confi	g Verification			
Iunnel Interface					Proxy Mode	Local Network	Peer Network	Operation				
⇔ Routing >					Auto	any	any	Edit Delete				
🗐 SSL VPN 💦 🔶				10 ~	/ Page Total:1			Go to 1 < 1 >				
🔄 IPsec VPN 🛛 🗸												
Tunnel Monitoring												
Config Wizard												۲
Custom Tunnel												onsult
Advanced Settings Details												
₩ DNS >												
問 DHCP >												
© Link Detection												
					Pri	evious Cancel	Next					
리 Neighbor Status 🛛 😤												

(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.

Configuration Examples of IPsec VPN Networking with Link Redundancy

Ruíjie Z Series Firewall	Chome Omonitor Ononitor P₂ Object System	로 🥝 🎧 옷 Quick Onboarding Policy Wizard Customer Service admin
🖨 Interface 🗸 🗸	Config Wizard	
Physical Interface		
Subinterface	Basic Config Authentication Config Interesting Traffic Config	(4)
Bridge Interface	овле сонну зациенскиот сонну шистехну пине сонну со	
Aggregate Interface	() The tunnel configured on the wizard will be added to the custom tunnel list.	×
iunnel Interface 이 Zone	Basic Config Free	
a Routing >	Tunnel Interface util	
— → → — SSL VPN →		
IPsec VPN 🗸	lunnel Name Primary	
Tunnel Monitoring	Scenario 🔘 Point-to-Point 🛈 💿 Point-to-Multipoint 🛈	
Config Wizard	Authentication Config Edit	8
Custom Tunnel	Outbound Interface Ge0/1 ~	Consult
Advanced Settings Details	Authentication Mode 💿 Pre-shared Key	•
DNS >	Key	
튀DHCP >		
	Advanced Settings Fold	
	* Local ID Type IPV4_ADDRESS V	
	Enable Peer Identity Authentication	
	Reverse Route Injection	
	Next-Hop Address Enter Next-Jion &ddress	
⊒ ⊐ Routing >	- Puonty 5	
	DPD Type Regular Mode V	
	DPD Detection Interval 30 Second	
	DPD Retry Interval 5 Second	
Config Wizard	IKE Parameter	
Custom Tunnel	* Negotiation Mode KEvit Main Mode	
	* Encryption Algorithm	
	* Verification Algorithm SHA #	
	* DH Group GROUPS *	
	Previous Cancel California	
🗉 Neighbor Status 🛛 📮	Previous Cancer Pittish	

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

Ruijie Z Series Firewall	ර Home ම	I Monitor		☞ Policy 💿 Sy	rstem		Quick Onboarding	Policy Wizard Customer Service admin
☐ Interface >	Custom T	Funnel						
👰 Zone	Create	Delete		D Defrech	Custom Field		Tunnel Name	
🖶 Routing >	O Create	Delete	Citable Usable	C Reliesi	Custom Field			
SSL VPN >	. 1	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
🖾 IPsec VPN 🛛 🗸		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
Tunnel Monitoring		,			0101010		-, (2.1.0. 1.2.)	Delete
Config Wizard								
Custom Tunnel								
Advanced Settings Details								

7.5.2 Configuring the Secondary Tunnel for the Hub Site

- 1. Performing Basic Configuration
- 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.

Ruijie Z Series Firewall	ය Home ා ම Monitor	Network	은 Object 🖾 Policy	(ð) System	L Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
Interface >	Config Wizard							
図 Zone								
🖶 Routing 🔷 🗧			(1)	(3)	(4)			
SSL VPN			Basic Config	Authentication Config Interesting Traffic Config				
IPsec VPN 🗸				O Tunnel Interface vtj 2				
Tunnel Monitoring				* Tunnel Name Secondary				
Config Wizard				* Companie O Balat to Balat to Multicolat				
Custom Tunnel				- scenario O Pointeto-Point O Pointeto-Multipoint				
Advanced Settings Details								
66 DNS >								
■ DHCP >				Brandt Office				
O Link Detection				Main Office				e
H VRRP				Branch Office				Contu
🖾 Neighbor Status 💦 🗧								
				Cancel Next				
Ē				Cancer Next				

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

2. Configuring Authentication

(1) Configure parameters according to the following figure.

Rujje Z Series Firewall	û Home	Network	우 Object 🛛 Polic	y 😥 System				Quick Onboarding	Policy Wizard	Customer Service	오 admin
Interface >	Config Wizard										
⑨ Zone											
⇔ Routing			Ø		2	3-					
⊜ SSL VPN →			Basic Config	Authenti	cation Config	Interesting Traf	fic Config	Config Verification			
IPsec VPN 🗸 🗸				* Outbound Interface	Ge0/2						
Tunnel Monitoring				* Authentication Mode	 Pre-shared Key 						
Config Wizard				* Key	- · ·						
Custom Tunnel											
Advanced Settings Details				* Confirm Key							
₩ DNS →											
■ DHCP →											
O Link Detection											2
🖽 VRRP											Consul
🖾 Neighbor Status 💦 🗧											Ű
				Previou	s Cancel	Next					
Ē											

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

3. Configuring Interesting Traffic

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

Ruijie Z Series Firewall	☆ Home	Network	, <mark>≗</mark> Object	🖫 Policy	System				Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
☐ Interface >	Config Wizard											
图 Zone												
🖶 Routing >			\odot)		O	3					
SSL VPN			Basic Co	onfig	Auth	hentication Config	Interesting Traf	fic Config	Config Verification			
📰 IPsec VPN 🛛 🗸				• Create	e 🔟 Delete		Enter the	keyword.				
Tunnel Monitoring												
Config Wizard					Proxy Mode	Local Network	Peer Network	Operation				
Custom Tunnel					Auto	any	any	Edit Delete				
Advanced Settings Details				10 ~	/ Page Total:1			Go to 1 < 1	>			
DNS >												
DHCP >												
O Link Detection												
H VRRP												Consu
📰 Neighbor Status 💦 🗧												Ŭ
					P	revious Cancel	Next					
E					Pr	Cancel	Next					

(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.

Ruijie Z Series Firewall	û Home © Monitor	Quick Onboarding	Ø Policy Wizard	Customer Service	्र admin
Interface >	Config Wizard				
😰 Zone					
⇔ Routing	Ø <u></u> Ø	4			
[™] SSL VPN >	Basic Config Authentication Config Interesting Traffic Config Confi	ig Verification			
IPsec VPN 🗸 🗸	The tunnel coefficient on the informational will be added to the suctors tunnel list				
Tunnel Monitoring	The tunner comigured on the wizard will be added to the custom tunner list.				
Config Wizard	Basic Config Edit				
Custom Tunnel	Tunnel Interface VII2				
Advanced Settings Details	Tunnel Name Secondary				
ee dns >					
DHCP >	Scenario 🥚 Point-to-Point 🛈 🛞 Point-to-Multipoint 🛈				
S Link Detection	Authentication Config Edit				2
🗒 VRRP	Outbound Interface Geti/2 V				Consu
☑ Neighbor Status >	Authentication Mode 🛞 Pre-shared Key				Ű
	Key				

Configuration Examples of IPsec VPN Networking with Link Redundancy

Rujje Z Series Firewall	Network					Quick Onboarding	Policy Wizard	Customer Service	오 admin
☐ Interface >			Interesting Traffic Config	Edit					
図 Zone			Local Network	Peer N	etwork				
Here Routing			any	a	ny				
SSLVPN >			Advanced Settings	Fold					
Tunnel Monitoring			* Local ID Type	IPV4_ADDRESS					1
Config Wizard		Enab	le Peer Identity Authentication						
Custom Tunnel			Reverse Route Injection						
Advanced Settings Details			Next-Hop Address	Enter Next-Hop Address					
Binter >			* Priority	10					
S Link Detection			DPD Type	Regular Mode	~				
URRP VRRP			DPD Detection Interval	10	Second				2
🖾 Neighbor Status 💦 🗧 🗎			DPD Retry Interval	5	Second				Consult
			IKE Parameter						
			* Negotiation Mode	IKEv1 Main Mode					
			* Encryption Algorithm	AES-128 ®					
Ē			Previous	Cancel Finish					

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

Ruijie Z Series Firewall	습 Home 🛛 Monitor	⊕ Network	양 Policy ⓒ System	m		Quick Onboarding	Policy Wizard Customer Service admin
Interface	Custom Tunnel						
ি Zone	Create		D Refresh	istom Field		Tunnel Name V	nter a Tunnel Name
Here Routing	o oreate	Chable Chable		301111010			
SSL VPN >	Tunnel Name	Tunnel Interface	Local Address	Peer Address	Interesting Traffic	Description	Operation
IPsec VPN V	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
Tunnel Monitoring							View Details Edit Copy
Custom Tunnel	Secondary	vti2	Ge0/2	0.0.0.0	0.0.0.0/0-0.0.0.0/0	by tunnel wizard Second	Delete
Advanced Settings Details							
€ DNS →							

7.5.3 Configuring the Primary Tunnel for the Spoke Site

- 1. Performing Basic Configuration
- 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.

Ruffie Z Series Firewall	ය Home 🛛 Monitor	Network	은 Object 🛛 Policy	(ð) System	L Quick Onboarding	Policy Wizard	Customer Service	오 admin
☐ Interface →	Config Wizard							
2 Zone			0					
₩ Routing >			()	(2) (3)	(4)			
SSL VPN			Basic Config	Autoentication Comig Interesting franc Comig				
IPsec VPN Y				* ① Tunnel Interface vti 1				
Tunnel Monitoring				* Tunnel Name Primary 💿				
Config Wizard								
Custom Tunnel				- Scenario O Point-to-Point O Point-to-Multipoint				
Advanced Settings Details								
DNS >								
貝 рнср >				Andrea Andreas				(7)
O Link Detection				Main Office				Con
III VRRP				Branch Office				5
🖾 Neighbor Status 🔷 🗧								-
亜				Cancel Next				

(3) After completing the configuration, click Next.

2. Configuring Authentication

(1) Configure parameters according to the following figure.

	Home 😔 Monitor 🌐 Ne	etwork & Object 😨 Policy					Quick Onboarding	Policy Wizard	Customer Service	오 admin
☐ Interface → Compared and	Config Wizard									
圆 Zone										
🖶 Routing >		⊘		-@	3					
Image: SSL VPN → SSL V		Basic Config	Authentio	cation Config	Interesting Traf	fic Config	Config Verification			
🖼 IPsec VPN 🛛 🝸			* Peer Address	1.1.2.1		Ping				
Tunnel Monitoring			* Outbound Interface	Ge0/1						
Config Wizard				0001						
Custom Tunnel			* Authentication Mode	 Pre-shared Key 						
Advanced Settings Details			* Key							
			* Confirm Key							
DHCP >										7
S Link Detection										Cons
II VRRP										F
🖾 Neighbor Status 💦 🗧										-
歪			Previous	s Cancel	Néxt					

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

3. Configuring Interesting Traffic

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

Ruffie Z Series Firewall	🖨 Home 🛛 🛛 Monitor	Network	Pe Object ☐ Policy	System				L Quick Onboarding	Policy Wizard	G Customer Service	오 admin
Interface	Config Wizard										
図 Zone											
➡ Routing >			O	4th		(3)	la Canfla	(4)			
SSL VPN >			Basic Config	Autre	nucation Config	Interesting Iran	ic comig Col				
🖾 IPsec VPN 🛛 🗸			⊕ Cre	ate 📋 Delete		Enter the	keyword. (
Tunnel Monitoring											
Config Wizard				Proxy Mode	Local Network	Peer Network	Operation				
Custom Tunnel				Subnet-to-Subnet	192.168.1.0/24	192.168.2.0/24	Edit Delete				
Advanced Settings Details			10 \	/ Page Total:1			Go to 1 < 1	>			
₩ DNS >											
DHCP >											
O Link Detection											Const
H VRRP											Ĩ
🖾 Neighbor Status 💦 🗧											
				Dres	ious Cancel	Next					
臣				Pier	Cancer	HEXT					

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

4. Verifying Configuration

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

Configuration Examples of IPsec VPN Networking with Link Redundancy

Ruijie Z Series Firewall		Network						(L) Quick Onboarding	Policy Wizard	Customer Service	adm
Interface	Config Wizard										
			0		F	<u> </u>					
			Basic Config	Authentication	Config	Interesting Traffic Config) Con	tig Verification			
	① The tunnel configu	ured on the wiz	ard will be added to the	custom tunnel list.							×
Config Wizard				Basic Config	Edit						
				Tunnel Interface	V81						
				Tunnel Name							
				Scanario	Point-to-Point	Point-to-Multing	int ()				
				scenario	- Point-to-Point	· ····································					
				Authentication Config	Edit						
				Peer Address	1.1.2.1						
				Outbound Interface	Ge0/1						
				Authentication Mode	Pre-shared Ker	v					
				Kau							
				(AL)							
								F	Ø	0	
Rujje Z Series Firewall	ය Home ා Monitor	Network	& Object ເ⊒ Policy	9 (ð) System				1 Quick Onboarding	Ø Policy Wizard	ဂ Customer Service	
Ruffic Z Series Firewall	ධ Home ම Monitor	Network	, ዶੂ Object 🛛 😨 Policy	© System		Peer Networ	k	Quick Onboarding	Ø Policy Wizard	Ω Customer Service	
Ruffic Z Series Firewall	ය Home ම Monitor	Network	A₂ Object 🛛 😨 Policy	© System		Peer Networ	k	Quick Onboarding	Policy Wizard	Customer Service	
Ruffie Z Series Firewall Interface > (2) Zone Couling >	බ Home ම Monitor	Network	A≞ Object 🛛 ເชื Policy	© System Local Network 192.168.1.0/24		Peer Networ 192.168.2.0/2	k 4	L Quick Onboarding	Ø Policy Wizard	G Customer Service	
Ruffe Z Series Firewall Interface > Zome > Stanling > Stating >	ධ Home ම Monitor	Network	옷_Object 양 Policy	C System Local Network 192,168.1.0/24 Advanced Settings	Fold	Peer Networ 192.168.2.0/2	k 4	E Quick Onboarding	⊘ Policy Wizard	Customer Service	
Ruffie Z Series Firewall Immunication > State > Immunication > State > State > Immunication > State > Immunication > Immunication >	ූ Home ම Monitor	Network	ළී Object ි පු Policy	C System	Fold IPV4_ADDRESS	Peer Networ 192.168.2.0/2 3 V	k	E Quick Onboarding	⊘ Policy Wizard	ရှ Customer Service	
Ruffe Z Series Firenall	Q Home @ Monitor	Network	A₂ Object ତ Policy	C System	Fold	Peer Networ 192.168.2.0/2 3 v	k 4	E Quick Orboarding	Ø Policy Wizard	្អា Customer Service	2
Ruffie Z Series Firenall Souther Sout	Q Home © Monitor	Network	A, Object SP Policy	C System	Fold IPV4_ADDRESS Regular Mode	Peer Networ 192.168.2.0/2 8	k 4	Curick Onboarding	🧭 Policy Wizard	Customer Service	
Ruffie Z Series Firewall Series Firewall Series 2 Series Firewall Series 2 Series	Q Home ⊘ Monitor	Network	A, Object SP Policy	C System	Fold IPV4_ADDRESS Regular Mode	Peer Networ 192.168.2.0/2 5 ~	k 4	Curick Onboarding	⊘ Policy Wizard	Customer Service	
Ruffie Z Series Firewall Immediate > Config Waard Custom Turnel Advanced Settings Details	Q Home ⊘ Monitor	Network	As Object SP Policy	C System	Fold IPV4_ADDRESS Regular Mode S0	Peer Networ 192.168.2.0/2 5 ~ ~	k 4	(E) Quick Orboarding	⊘ Policy Wizard	A Customer Service	
Ruffie Z Series Firewall Immediate > Immediate Config Waard Costom Turnel Advanced Settings Details Immediate >	Q Home	Network	, A₂ Object SP Policy Ena	C System Local Network 192.168.10/24 Advanced Settings Local ID Type Local ID Type DPD Detection Interval DPD Retry Interval	Fold IPV4_ADDRESS Regular Mode 30 5	Peer Networ 192.168.2.0/2 3 ~ ~	k 4 Second	E Quick Orboarding	⊘ Policy Wizard	A Guatomer Service	
Ruffie Z Series Firewall Imitarface >	Q Home	Network	, A₂ Object SP Policy Ena	C System	Fold IPV4_ADDRESS Regular Mode 30 5	Peer Networ 192.168.2.0/2 3	k 4 Second Second	E Quick Orboarding	© Policy Wizard	A Customer Service	
Ruffe 2 Series Firewall Image: Series Seri	û Home	Network	, As Object SP Policy Ena	C System C Syst	Fold IPV4_ADDRESS Regular Mode 50 5 5	Peer Networ 192.168.2.0/2 3 ✓	k 4 Second Second	E Quick Orboarding	© Policy Wizard	A Customer Service	
Ruffie 2 Series Firewall Image: Series Ser	û Home	Network	, As Object SP Policy Ena	C System	Fold PV4_ADDRESC P	Peer Networ 192.168.2.0/2 3 ~	k 4 Second Second	Cuick Orboarding	e Pelicy Wizard	A Customer Service	
Ruffe Z Series Freewall S Corre S Corre S SUL VN S SUL VN Config Waard Custom Turnel Manitation Custom Turnel Manitation Custom Turnel Manitation D USS Custom Turnel D USS Custom Turnel Custom	û Home	Network	A Object S Policy	C System	Fold PV4_ADDRESS PV4_ADDRESS PV4_ADDRESS Regular Mode 30 5 KEv1 Main Mod	Peer Networ 192.168.2.0/2 3 ~	k 4 Second Second	Curick Oreboarding	e Policy Wizard	A Customer Service	
Ruffle 2 Series Firewall Source 2 Source 2 Source 2 Source 2 Source 2 Cutors Monitoring Cutors Monito	û Home	Network	, A: Object	C System	Fold IPV4_ADDRESS Regular Mode 30 5 5 IREV1 Main Mode [AES-128 [SHA]	Peer Networ 192.168.2.0/2 3 ✓ 4 ✓ 5 ✓	k 4 Second Second	Curick Orboarding	Policy Wizard	A Customer Service	
Ruffe 2 Series Freenal	û Home	® Network	A: Object	C System	Fold IPV4_ADDRESS Regular Mode 30 5 5 IRCEV1 Main Mode IRCEV1 Main Mode IRCEV1 Main Mode IRCEV1 Main Mode IRCEV1 Main Mode IRCEV1 Main Mode IRCEV1 Main Mode	Peer Networ 192.168.2.0/2 8 ~ ~ 192.168.2.0/2 8 ~ ~ 192.168.2.0/2 192.1000 192.100 192.10000 192.10000 192.10000 192.100000000000000000000000000000000000	k 4 Second Second	(2) Quick Orboarding	Policy Wizard	A Customer Service	
Ruffe 2 Series Firewall	û Home	® Network	A Object	Local Network 192.168.1.0/24 Advanced Settings 4 Local ID Type 4 Local ID Type ble Peer Identity Authentication DPD Type DPD Detection Interval DPD Retry Interval REParameter 4 Negotiation Mode 6 Encryption Algorithm 4 Verification Algorithm 6 Uber Group 6 D DH Coup 6 D	Fold IPV4_ADDRESS Regular Mode 30 5 KEV1 Main Mod AES-128 SHA EGROUPS BS40	Peer Networ 192.168.2.0/2 8	k 4 Second Second	(2) Quick Orboarding	Policy Wizzed	A Custorer Service	



(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.

Ruffe Z Series Firewall	습 Home 🛛 Monitor 🕀 Network	,은 Object 🐨 Policy 🗧	🕽 System			E Quick Onboarding	Policy Wizard	Customer Service	्र admin
Interface	IPv4 IPv6								
	 Ocreate O	h				vti			
Static Routing	Dest. IP Range/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description		Operation	
Intelligent Routing	192.168.2.0/24	-	vti1	5		by tunnel wizard Prim	ary	Edit Delete	

7.5.4 Configuring the Secondary Tunnel for the Spoke Site

1. Performing Basic Configuration

- 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.

Ruffie Z Series Firewall	🛆 Home 🛛 🗇 Monit	or	, A≞ Object 🖾 Po	licy 🕲 System			Quick Onboarding	Policy Wizard	G Customer Service	ې admin
Interface >	Config Wizard									
🔞 Zone										
₩ Routing >			0		-2	3				
SSL VPN			Basic Config	Authenti	ication Config	Interesting Traffic Config	Config Verification			
IPsec VPN Y				* () Tunnel Interface	vti 2					
Tunnel Monitoring				* Tunnel Name	Secondary					
Config Wizard				t Cronodo	Delet to Delet	Delet to Multicelet				
Custom Tunnel				* Scenario	• Point-to-Point	Point-to-multipoint				
Advanced Settings Details										
DNS >										
DHCP >					arente atterne	Branch Unice				(7)
O Link Detection					Main Office					Se on
I VRRP						Branch Office				EUR .
📰 Neighbor Status 💦 🗧										
				_						
Œ					Cancel	lext				

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

2. Configuring Authentication

(1) Configure parameters according to the following figure.

Ruijie Z Series Firewall		A Object ເຜ Policy I System		🔝 Quick Onboarding	Policy Wizard	Customer Service	오 admin
Interface >	Config Wizard						
2 Zone							
🖶 Routing 🔷 🗧		Ø	3				
⊜ SSL VPN →		Basic Config Authe	ntication Config Interesting Traffic Config	Config Verification			
IPsec VPN 🗸 🗸		* Peer Addre	ss 1.1.3.1 Ping				
Tunnel Monitoring		* Outbound Interfa	ce Ge0/1				
Config Wizard		* Authentication Mo	a Dra charad Kau				
Custom Tunnel		Addientication Mo	Je Pre-shared key				
Advanced Settings Details		* 1	ey				
III DNS >		* Confirm #	еу				
🔲 рнср >							
S Link Detection							0
III VRRP							sult
🔄 Neighbor Status 🔷 🗧							
亞		Pre	ious Cancel Next				
	•						

(2) After completing the configuration, click Next.

3. Configuring Interesting Traffic

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

Ruijie Z Series Firewall		Network						L Quick Onboarding	Policy Wizard	Customer Service	오 admin
Interface >	Config Wizard										
図 Zone											
⇔ Routing			Ø			3-		4			
Image: SSL VPN →			Basic Config	Authe	entication Config	Interesting Trat	ffic Config Co	nfig Verification			
🖾 IPsec VPN 👋			⊕ Crea	ite 🔟 Delete		Enter the	e keyword.				
Tunnel Monitoring											
Config Wizard				Proxy Mode	Local Network	Peer Network	Operation				
Custom Tunnel				Subnet-to-Subnet	192.168.1.0/24	192.168.2.0/24	Edit Delete				
Advanced Settings Details			10 ~	/ Page Total:1			Go to 1 < 1	>			
III DNS >											
📃 DHCP >											(7)
S Link Detection											0
III VRRP											n an
☑ Neighbor Status >											
Œ				Prev	vious Cancel	Next					

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

4. Verifying Configuration

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

Ruífie Z Series Firewall	ය Home	Network	은 Object 🐨 Pol	icy 🕲 System					Quick Onboarding	Policy Wizard	Customer Service	오 admin
Interface >	Config Wizard											
😰 Zone												
🖶 Routing 💦 🗧			Ø		-0		O					
SSL VPN →			Basic Config	Auth	ientication Conf	ıg	Interesting Traffic 0	ontig	Config Verification			
🔄 IPsec VPN 🛛 🗸	The tunnel configur	red on the wiz	ard will be added to t	he custom tunnel list.								×
Tunnel Monitoring												
Config Wizard				B	asic Config Edit							
Custom Tunnel				Tunn	el Interface							
Advanced Settings Details				Tu	innel Name Se	condary						
					Scenario 💿 🖡	Point-to-Poi	int 🕕 📄 Point-to-N	ultipoint ()				
□ DHCP >												(7
O Link Detection				Authenticat	tion Config Edit							Con
II VRRP				Pe	eer Address 1.1							IUR I
🖬 Neighbor Status 💦 👌				Outbour	nd Interface Ge							
				Authentica	ation Mode 💿 🖡	Pre-shared	Key					
					Key							

IPsec VPN Typical Configuration Examples

Configuration Examples of IPsec VPN Networking with Link Redundancy

by tunnel wizard Primary

by tunnel wizard Second...

Interface >							
		Local Network	Peer Network	k			
] Zone		192 158 1 0/24	192 168 2 0/2				
Routing >		15ETOS TOPET	1361100400/6-				
) SSL VPN >		Advanced Settings	Fold				
IPsec VPN V		* Local ID Type	IPV4_ADDRESS V				
Tunnel Monitoring	F	Enable Peer Identity Authentication					
Config Wizard		DPD Type	Regular Mode \vee				
Custorn Tunnel		DPD Detection Interval	30	Second			
Advanced Settings Details		DPD Retry Interval	E	Casand			
DNS >		GPD Netry Interval	U	Second			
Прись >		IKE Parameter					1
) Link Detection		* Negotiation Mode	IKEv1 Main Mode $\qquad \lor$				
U VRRP		* Encryption Algorithm	AES-128 ®				
Neighbor Status >		* Verification Algorithm	SHA 🛞 🗸 🗸				
		* DH Group	GROUPS *				
		* O SA Lifetime	86400	Casand			
			00100	Second			
Œ		Previous	Cancel Finish				
ا ترتو ا 🗷 Series Firewall	ය Home	olicy 💿 System			L Quick Onboardir	@ Ω ng Policy Wizard Customer Se	ervice
Ruffice Z Series Firewall	G Home Ø Monitor	Policy 💿 System			ی Quick Onboardir	Ø ெ ng Policy Wizard Customer Se	arvice
ا المتحدة (المحدة المحدة ال	© Home © Monitor ♥ Network & Object © F	folicy © System			E Quick Onboardir	Ø ♀ ng Policy Wizard Customer Se	ervice
Interface Zone	G Home ⓒ Monitor ♥ Network & Object (© F I Custom Tunnel ⓒ Create 意 Delete ⓒ Enable ் Disable C	Kolicy © System		Tunnel Nam	Quick Onboardin	O Policy Wizard Customer Se Enter a Tunnel Name.	ervice
Ruffie Z Series Firewall] Interface >] Zone] Routing >] Secure	© Home ⓒ Monitor ♥ Network & Object (© F I Custom Tunnel ⓒ Create ⓒ Deate ⓒ Disable ℃	Tollcy © System		Tunnel Nam	Quick Onboardin	O Policy Wizard Customer Se Enter a Tunnel Name.	ervice

1.1.2.1

1.1.3.1

192.168.1.0/24-192.168.2.0/24

192.168.1.0/24-192.168.2.0/24

Ge0/1

Ge0/1

vti1

vti2

Primar

(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.)

A 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.

Ruffe Z Series Firewall	☆ Home	⊘ Monitor	Network	우= Object 🛛 🐨 Policy	System			1 Quick Onboarding	Ø Policy Wizard	G Customer Service	ې admin
☐ Interface >	IPv4	IPv6									
☑ Zone ➡ Routing ~	Oreate	e 间 Delete	C Refresh					vti			
Static Routing		Dest. IP Ran	ge/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description		Operation	
Intelligent Routing		192.168.2	2.0/24	-	vti1	5		by tunnel wizard Prim	ary	Edit Delete	
Egress Load Balancing Address Library Route		192.168.3	2.0/24		vti2	5	-	by tunnel wizard Secon	d	Edit Delete	

Ruijie Z Series Firewall	🗅 Home 🛛 Monitor 🔀 🖡	Network & Object 🕃 Policy 💿 System	1 Quick Onboarding	Ø Policy Wizard	Customer Service	Q admin
Interface Zone	Back Edit Static Rou	iting				
	IP Type	IPv4				
Static Routing	* Dest. IP Range/Mask	192.168.2.0/24				
Intelligent Routing	Next-Hop Address					
Egress Load Balancing	Interface	v12 ~				
Address Library Route	* ① Priority	10				
OSPF	Link Detection	Link Detection V				
Routing Table	Description	by tunnel wizard Secondary				
Routing Policy						
E IPsec VPN						-
Tunnel Monitoring						0
Config Wizard						and a
Custom Tunnel						
Advanced Settings Details						
🔲 DHCP >		Save				

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

Ruíjie Z Series Firewall	🛆 Home	G Monitor	Network	,A≞ Object 6	Policy	☺ System					L Quick Onboarding	Ø Policy Wizard	က Customer Service	Q admin
Interface	IPv4	IPv6												
図 Zone Routing ~	 Oreate 	e 🔟 Delet	e 🔉 Refresh								vti			
Static Routing		Dest. IP Ra	ange/Mask	Next-Ho	p Address		Interface	Priority	L	ink Detection	Description		Operation	
Intelligent Routing		192.16	8.2.0/24		-		vti1	5			by tunnel wizard Primar	ry	Edit Delete	
Egress Load Balancing Address Library Route		192.16	8.2.0/24		-		vti2	10		-	by tunnel wizard Second	ary	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

Ruffe Z Series Firewall	습 Home	G Monitor	Network	은 Object 🛛 Policy	System			Quick C	1) Inboarding	Ø Policy Wizard	Custome) r Service a	오 dmin
Interface >	Tunne	Monitorin	9										
🕲 Zone	🕢 st	art 🚫 Stop	Refresh	Custom Field							e.		
🖶 Routing >													
SSL VPN >		Tun	nel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Pac	(ets (Byte)	Re	Operation	
🖙 IPsec VPN 🛛 🗸			Delesson		Delete the Middle elete	0000							
Tunnel Monitoring		Ň	Primary	-	Point-to-Multipoint	0.0.0.0		-					
Config Wizard			Primary	 Established 	Instance Link	1.1.1.1	192.168.2.0/24->192.168.1.0/24	3076		0		Stop	
Custom Tunnel		Se	condary	-	Point-to-Multipoint	0.0.0.0	-	-		-			
Advanced Settings Details													
iii DNS >													

2. Checking the Tunnel Status of the Spoke Site

Ruijie Z Series Firewall	습 Home 🛛 😡	Monitor	ද≞ Object ි ව Policy ද	🕄 System			Quick C	t	G Customer Service	्र admin
Interface	Tunnel Mo	onitoring								
囹 Zone	Start	Ston Refresh	Custom Field							
Here Routing >	Clart									
SSL VPN >		Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operat	ion
📰 IPsec VPN 🛛 🗸		Primary	 Established 	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	2525	0	Sto	0
Tunnel Monitoring		Secondary	Not established	Point-to-Point	1131	192 168 1 0/24-> 192 168 2 0/24	0	0	Sta	
Config Wizard		secondary	• Not established	Fourt to Fourt		132.100.10/24 7 132.100.20/24	v	Ŭ		
Custom Tunnel										

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.

- Ruíjie | Z Series Fi ⊕ N Tunnel Monitoring ⊘ Start Stop Custom Field Peer Addres Tunnel Name Tunnel Status Туре ting Traffic Sent Packets (E Primary Point-to-Multipoint 0.0.0.0 Secondary Point-to-Multipoint 0.0.0.0 1.1.1.1 192.168.2.0/24->192.168.1.0/24 3524 Secondary Established Instance Link
- 1. Checking the Tunnel Status of the Hub Site

2. Checking the Tunnel Status of the Spoke Site

Ruijie Z Series Firewall	🛆 Home 🛛 Ø Monitor 🗲	● Network 온 Object	t 😨 Policy	System			Quick C	1 🕑 nboarding Policy Wizard	ဂ Customer Service	ې admin
☐ Interface >	Tunnel Monitoring									
图 Zone	⊘ Start Stop 3	Custor	n Field					Enter a tunnel nam	e.	
SSL VPN >	Tunnel	el Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re- Operat	ion
Tunnel Monitoring	Prim	mary •	Not established	Point-to-Point	1.1.2.1	192.168.1.0/24->192.168.2.0/24	0	0	Star	rt
Config Wizard	Secor	ondary	 Established 	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	3476	0	Sto	p
Custom Tunnel										

7.6.3 Verifying Tunnel Switchback After the Primary Link Recovers

1. Checking the Tunnel Status of the Hub Site

Ruijie Z Series Firewall	≙ Home	G Monitor	Network	A_Object ☑ F	Policy	System			Quick C	Dnboarding Policy Wizard	റെ Customer Ser	ې rvice admin
Interface	I Tunne	l Monitorin	g									
図 Zone	⊘ si	art 🚫 Stop	C Refresh	Custom Field						Enter a tunnel nam	10.	
SSL VPN		Tur	nnel Name	Tunnel	Status	Type	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re	eration
IPsec VPN V			Delmany			Point to Multinoint	0000					
Tunnel Monitoring			Primary	• Estab	blished	Instance Link	1.1.1.1	- 192.168.2.0/24->192.168.1.0/24	3076	0		Stop
Config Wizard Custom Tunnel		Si	econdary	-		Point-to-Multipoint	0.0.0.0	-	-	-		
Advanced Settings Details	_										_	
to DNS >												

2. Checking the Tunnel Status of the Spoke Site

Ruffe Z Series Firewall	습 Home ි ල	Monitor 	A≘ Object 🖾 Policy 📀	System			Quick C	Onboarding Policy Wizard	Customer Service	्र admin
☐ Interface >	Tunnel M	onitoring								
图 Zone iii Routing >	Start	Stop C Refresh	Custom Field					Enter a tunnel nam	e.	
⊕ SSL VPN →		Tunnel Name	Tunnel Status	Туре	Peer Address	Interesting Traffic	Lifetime (s)	Sent Packets (Byte)	Re Operatio	on
🖬 IPsec VPN 🛛 🗸		Primary	Established	Point-to-Point	1121	192 168 1 0/24-> 192 168 2 0/24	2525	0	Stop	
Tunnel Monitoring		T Initiary	• Established	Found to Found	1.1.6.1	132100.10/24 2132.100.20/24	LJLJ	ů.	City	
Config Wizard		Secondary	 Not established 	Point-to-Point	1.1.3.1	192.168.1.0/24->192.168.2.0/24	0	0	Start	1
Custom Tunnel										

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
8.1 IKE Negotiation Failure



Figure 8-2 Troubleshooting Roadmap for IKE Negotiation Failures

8.2 IPsec Service Exception



Figure 8-3 Troubleshooting Roadmap for IPsec Service Exceptions