Virtual Private Network

Administrator Guide

 Issue
 01

 Date
 2025-01-24





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

- Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China Website: https://www.huawei.com
- Email: <u>support@huawei.com</u>

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page: <u>https://securitybulletin.huawei.com/enterprise/en/security-advisory</u>

S2C Enterprise Edition VPN

1.1 Interconnection with an AR Router of Huawei (Active-Active Connections)

1.1.1 Static Routing Mode

1.1.1.1 Operation Guide

Scenario

Figure 1-1 shows the typical networking where a VPN gateway connects to an access router (AR) of Huawei in static routing mode.



Figure 1-1 Typical networking diagram

In this scenario, the AR router has only one IP address, and the VPN gateway uses the active-active mode. A VPN connection is created between each of the two active EIPs of the VPN gateway and the IP address of the AR router.

Limitations and Constraints

VPN and AR routers support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

Data Plan

Categor y	ltem	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/16	192.168.0.0/24192.168.1.0/24
VPN gateway	Gateway IP address	1.1.1.1 (IP address of the uplink public network interface GE0/0/8 on the AR router)	Active EIP: 1.1.1.2Active EIP 2: 2.2.2.2
	Interconn ection subnet	-	192.168.2.0/24
VPN connecti on	Tunnel interface address IKE policy	 Tunnel 1: 169.254.70.1/30 Tunnel 2: 169.254.71.1/30 IKE version: IKEv2 Authentication algorithm: Encryption algorithm: AES- DH algorithm: group 14 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address 	 Tunnel 1: 169.254.70.2/30 Tunnel 2: 169.254.71.2/30 SHA2-256 -128
	IPsec policy	 Authentication algorithm: Encryption algorithm: AES PFS: DH group 14 Transfer protocol: ESP Lifetime (s): 3600 	SHA2-256 -128

Operation Process

Figure 1-2 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-2 Operation process



Table 1-2 Operation process description

N o.	Configurat ion Interface	Step	Description
1	Manageme nt console	Create a VPN gateway.	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2		Create a customer gateway.	Configure the AR router as the customer gateway.
3		Create VPN connection 1.	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4		Create VPN connection 2.	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	Command- line interface (CLI) of the AR router	Configure the AR router.	 The local and remote tunnel interface addresses configured on the AR router must be the same as the customer and local tunnel interface addresses configured on the VPN console, respectively. The connection mode, PSK, IKE policy, and IPsec policy settings on the AR router must be same as those of VPN connections.
6	-	Verify network connectivity.	Run the ping command to verify network connectivity.

1.1.1.2 Configuration on the Cloud Console

Prerequisites

A VPC and its subnets have been created on the management console.

Procedure

- **Step 1** Log in to Huawei Cloud management console.
- **Step 2** Choose **Networking > Virtual Private Network**.
- **Step 3** Configure a VPN gateway.
 - Choose Virtual Private Network > Enterprise VPN Gateways. On the S2C VPN Gateways tab page, click Buy S2C VPN Gateway.
 - Set parameters as prompted.
 Table 1-3 describes the parameters for creating a VPN gateway.

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select VPC .	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0. 0/16)
Interconn ection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on- premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

	Table 1-3	Parameters	for	creating	а	VPN	datewa	/
--	-----------	------------	-----	----------	---	-----	--------	---

Step 4	Configure	a customer	gateway.
--------	-----------	------------	----------

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

Table 1-4 describes the parameters for creating a customer gateway.

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar
Identifier	Select IP Address , and enter the public IP address of the AR router.	IP Address 1.1.1.1
BGP ASN	ASN of your on-premises data center or private network.	65000
	The value must be different from the BGP ASN of the VPN gateway.	

Table 1-4 Parameters	for	creating	а	customer	gateway
------------------------------	-----	----------	---	----------	---------

Step 5 Configure VPN connections.

In this scenario, a VPN connection is created between the AR router and each of the active EIP and active EIP 2 of the VPN gateway.

- 1. Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- 1. Create VPN connection 1.

 Table 1-5 describes the parameters for creating a VPN connection.

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-ar
VPN Type	Select Static routing.	Static routing

Table 1-5 Parame	ter settings	for VPN	connection	1
------------------	--------------	---------	------------	---

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. - A customer subnet cannot be	172.16.0.0/16
	included in any local subnet or any subnet of the VPC to which the VPN gateway is attached.	
	as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	
Interface IP Address Assignment	 Manually specify In this example, Manually specify is selected. Automatically assign 	Manually specify
Local Tunnel Interface	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. The VPN gateway can	NQA enabled
	automatically perform NQA detection on the peer interface address that has been configured on the customer gateway.	
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway device.	<i>Set this parameter based on the site requirements.</i>

Parameter	Description	Value	
Policy Settings	The policy settings must be the same as those on the firewall.	IKE PolicyVersion: v2	
		 Authentication Algorithm: SHA2-256 	
		 Encryption Algorithm: AES-128 	
		 DH Algorithm: Group 14 	
		 Lifetime (s): 86400 	
			 Local ID: IP Address
		 Customer ID: IP Address IPsec Policy 	
		 Authentication Algorithm: SHA2-256 	
		 Encryption Algorithm: AES-128 	
		 PFS: DH group 14 	
		 Transfer Protocol: ESP 	
		 Lifetime (s): 3600 	

2. Create VPN connection 2.

NOTE

For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

	-	
Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

Table 1-6 Parameter settings for VPN connection 2

----End

1.1.1.3 Configuration on the AR Router

Procedure

- **Step 1** Log in to the AR router.
- **Step 2** Enter the system view.

<AR651>system-view

Step 3 Configure an IP address for the WAN interface.

[AR651]interface GigabitEthernet 0/0/8

[AR651-GigabitEthernet0/0/8]ip address 1.1.1.1 255.255.255.0

[AR651-GigabitEthernet0/0/8]quit

Step 4 Configure a default route.

[AR651]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254

In this command, 1.1.1.254 is the gateway address for the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Configure routes to the active EIP and active EIP 2 of the VPN gateway.

[AR651]ip route-static 1.1.1.2 255.255.255.255 1.1.1.254

[AR651]ip route-static 2.2.2.2 255.255.255.255 1.1.1.254

- 1.1.1.2 and 2.2.2.2 are the active EIP and active EIP 2 of the VPN gateway, respectively.
- 1.1.1.254 is the gateway address for the AR router's public IP address.
- **Step 6** Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

[AR651]IPsec authentication sha2 compatible enable

- **Step 7** Configure an IPsec proposal.
 - [AR651]IPsec proposal hwproposal1
 - [AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
 - [AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
 - [AR651-IPsec-proposal-hwproposal1]quit
- Step 8 Configure an IKE proposal.
 - [AR651]ike proposal 2
 - [AR651-ike-proposal-2]encryption-algorithm aes-128
 - [AR651-ike-proposal-2]dh Group14
 - [AR651-ike-proposal-2]authentication-algorithm sha2-256
 - [AR651-ike-proposal-2]authentication-method pre-share
 - [AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
 - [AR651-ike-proposal-2]prf hmac-sha2-256
 - [AR651-ike-proposal-2]quit
- **Step 9** Configure IKE peers.
 - [AR651]ike peer hwpeer1
 - [AR651-ike-peer-hwpeer1]undo version 1
 - [AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
 - [AR651-ike-peer-hwpeer1]ike-proposal 2
 - [AR651-ike-peer-hwpeer1]local-address 1.1.1.1
 - [AR651-ike-peer-hwpeer1]remote-address 1.1.1.2
 - [AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
 - [AR651-ike-peer-hwpeer1]rsa signature-padding pss
 - [AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
 - [AR651-ike-peer-hwpeer1]quit
 - #
 - [AR651]ike peer hwpeer2
 - [AR651-ike-peer-hwpeer2]undo version 1
 - [AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
 - [AR651-ike-peer-hwpeer2]ike-proposal 2
 - [AR651-ike-peer-hwpeer2]local-address 1.1.1.1
 - [AR651-ike-peer-hwpeer2]remote-address 2.2.2.2
 - [AR651-ike-peer-hwpeer2]rsa encryption-padding oaep

[AR651-ike-peer-hwpeer2]rsa signature-padding pss

[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256

[AR651-ike-peer-hwpeer2]quit

The commands are described as follows:

- **ike peer hwpeer1** and **ike peer hwpeer2**: correspond to two VPN connections.
- pre-shared-key cipher: specifies a pre-shared key.
- local-address: specifies the public IP address of the AR router.
- remote-address: specifies the active EIP or active EIP 2 of the VPN gateway.
- **Step 10** Configure an IPsec profile.

[AR651]IPsec profile hwpro1

[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1

[AR651-IPsec-profile-hwpro1]proposal hwproposal1

[AR651-IPsec-profile-hwpro1]pfs dh-Group14

[AR651-IPsec-profile-hwpro1]quit

#

[AR651]IPsec profile hwpro2

[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2

[AR651-IPsec-profile-hwpro2]proposal hwproposal1

[AR651-IPsec-profile-hwpro2]pfs dh-Group14

[AR651-IPsec-profile-hwpro2]quit

Step 11 Configure virtual tunnel interfaces.

[AR651]interface Tunnel0/0/1

[AR651-Tunnel0/0/1]mtu 1400

[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252

[AR651-Tunnel0/0/1]tunnel-protocol IPsec

[AR651-Tunnel0/0/1]source 1.1.1.1

[AR651-Tunnel0/0/1]destination 1.1.1.2

[AR651-Tunnel0/0/1]IPsec profile hwpro1

[AR651-Tunnel0/0/1]quit

#

[AR651]interface Tunnel0/0/2

[AR651-Tunnel0/0/2]mtu 1400

[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252

[AR651-Tunnel0/0/2]tunnel-protocol IPsec

[AR651-Tunnel0/0/2]source 1.1.1.1

[AR651-Tunnel0/0/2]destination 2.2.2.2

[AR651-Tunnel0/0/2]IPsec profile hwpro2

[AR651-Tunnel0/0/2]quit

The commands are described as follows:

• **interface Tunnel0/0/1** and **interface Tunnel0/0/2**: indicate the tunnel interfaces corresponding to the two VPN connections.

In this example, Tunnel0/0/1 establishes a VPN connection with the active EIP of the VPN gateway, and Tunnel0/0/2 establishes a VPN connection with active EIP 2 of the VPN gateway.

- **ip address**: configures an IP address for a tunnel interface on the AR router.
- **source**: specifies the public IP address of the AR router.
- **destination**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 12 Configure NQA.

[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now

[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit

#

[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1

[AR651-nqa-IPsec_nqa2-IPsec_nqa2] frequency 15

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now

[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit

The commands are described as follows:

• nqa test-instance IPsec_nqa1 IPsec_nqa1 and nqa test-instance IPsec_nqa2 IPsec_nqa2: configure two NQA test instances named IPsec_nqa1 and IPsec_nqa2. In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.

- destination-address: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.
- **Step 13** Configure association between the static route and NQA.

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

The parameters are described as follows:

- 192.168.0.0 and 192.168.1.0: indicate VPC subnets.
 - Association between the static route and NQA needs to be configured for each subnet.
 - Tunnel x and IPsec_nqa x in the same command correspond to the same VPN connection.
- **preference 100** indicates the route preference. If this parameter is not specified, the default value 60 is used.

In this example, the two VPN connections work in active-active mode, and traffic is preferentially transmitted through the VPN connection to which the active EIP of the VPN gateway belongs.

To load balance traffic between the two VPN connections, delete **preference 100** from the preceding configuration.

----End

1.1.1.4 Verification

- About 5 minutes later, check states of the VPN connections.
 - Cloud console

Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Normal**.

AR router

Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**. The states of the two VPN connections are both **READY**|**STAYLIVE**.

• Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

1.1.2 BGP Routing Mode

1.1.2.1 Operation Guide

Scenario

Figure 1-3 shows the typical networking where a VPN gateway connects to the Huawei AR router in an on-premises data center in BGP routing mode.

Figure 1-3 Typical networking diagram



In this scenario, the AR router has only one IP address, and the VPN gateway uses the active-active mode. A VPN connection is created between each of the two active EIPs of the VPN gateway and the IP address of the AR router.

Limitations and Constraints

VPN and AR routers support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

Data Plan

Categor y	ltem	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/16	192.168.0.0/24 192.168.1.0/24
VPN gateway	Gateway IP address	1.1.1.1 (IP address of the uplink public network interface GE0/0/8 on the AR router)	Active EIP: 1.1.1.2 Active EIP 2: 2.2.2.2
	Interconn ection subnet	-	192.168.2.0/24
	BGP ASN	64515	64512

Table 1-7 Data plan

Categor	ltem	Example Value for the AR	Example Value for the	
y		Router	Huawei Cloud Side	
VPN	Tunnel	 Tunnel 1:	 Tunnel 1:	
connecti	interface	169.254.70.1/30 Tunnel 2:	169.254.70.2/30 Tunnel 2:	
on	address	169.254.71.1/30	169.254.71.2/30	
	IKE policy	 IKE version: IKEv2 Authentication algorithm: Encryption algorithm: AES DH algorithm: group 14 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address 	IKE version: IKEv2 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 DH algorithm: group 14 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address	
	 IPsec policy Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 PFS: DH group 14 Transfer protocol: ESP Lifetime (s): 3600 		SHA2-256 -128	

Operation Process

Figure 1-4 shows the process of using the VPN service to enable communication between the data center and VPC.



Figure 1-4 Operation process

N o.	Configurat ion Interface	Step	Description
1	Manageme nt console	Create a VPN gateway.	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2		Create a customer gateway.	Configure the AR router as the customer gateway.
З		Create VPN connection 1.	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4		Create VPN connection 2.	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	CLI of the AR router	Configure the AR router.	 The local and remote tunnel interface addresses configured on the AR router must be the same as the customer and local tunnel interface addresses configured on the VPN console, respectively. The connection mode, PSK, IKE policy, and IPsec policy settings on the AR router must be same as those of VPN connections.
6	-	Verify network connectivity.	Run the ping command to verify network connectivity.

Table 1-8 Operation process desc	cription
----------------------------------	----------

1.1.2.2 Configuration on the Cloud Console

Prerequisites

A VPC and its subnets have been created on the management console.

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking > Virtual Private Network**.

Step 3 Configure a VPN gateway.

- Choose Virtual Private Network > Enterprise VPN Gateways. On the S2C VPN Gateways tab page, click Buy S2C VPN Gateway.
- 2. Set parameters as prompted and click **Buy Now**.

Table 1-9 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select VPC .	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0. 0/16)
Interconn ection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on- premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Table 1-9 Key parameters for	^r creating a	VPN gatewa	ay
------------------------------	-------------------------	------------	----

Step 4 Configure a customer gateway.

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

 Table 1-10 describes the parameters for creating a customer gateway.

Table 1-10 Parameters for	creating a	customer gateway
---------------------------	------------	------------------

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar

Parameter	Description	Value
Identifier	Select IP Address , and enter the public IP address of the AR router.	IP Address 1.1.1.1
BGP ASN	BGP AS number of the AR router.	65000

Step 5 Configure VPN connections.

In this scenario, a VPN connection is created between the AR router and each of the active EIP and active EIP 2 of the VPN gateway.

- 1. Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- 1. Create VPN connection 1.

 Table 1-11 describes the parameters for creating a VPN connection.

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-ar
VPN Type	Select BGP routing .	BGP routing
Customer Subnet	 Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. 	172.16.0.0/16
Interface IP Address Assignment	 Manually specify In this example, Manually specify is selected. Automatically assign 	Manually specify

Table 1-11 Parameter settings for VPN connection 1

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the firewall.	<i>Set this parameter based on the site requirements.</i>
Policy Settings	The policy settings must be the same as those on the firewall.	 IKE Policy Version: v2 Authentication Algorithm: SHA2-256 Encryption Algorithm: AES-128 DH Algorithm: Group 14 Lifetime (s): 86400 Local ID: IP Address Customer ID: IP Address Customer ID: IP Address IPsec Policy Authentication Algorithm: SHA2-256 Encryption Algorithm: AES-128 PFS: DH group 14 Transfer Protocol: ESP
		 Lifetime (s): 3600

2. Create VPN connection 2.

D NOTE

For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

Table 1-12 Parameter settings	for VPN connection 2
-------------------------------	----------------------

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.1.2.3 Configuration on the AR Router

Prerequisites

- The uplink public network interface GE0/0/8 of the AR router has been configured. Assume that the public IP address of the interface is 1.1.1.1.
- The downlink private network interface GE0/0/1 of the AR router has been configured. Assume that the private IP address of the interface is 172.16.0.1.

Procedure

Step 1 Log in to the web system of the AR router.

An AR651 running V300R019C13SPC200 is used as an example. The web system may vary according to the device model and software version.

Step 2 Complete basic settings.

Choose Advanced > IP > Routing > Static Route Configuration. In the IPv4 Static Route area, configure static routes to the active EIP and active EIP 2 of the VPN gateway, and click Add, as shown in Figure 1-5.

Routing Table Sta	atic Route Configuration	Dynamic Route Configuration			
IPv4 Static Route	Configure a static route to the active FIP of the VPN gateway.				
Static Route Setting	s				
* Destination IP :	1 . 1 . 1 . 2		* Subnet mask :	255 . 255 . 255 . 252	
VPN instance :	- none - 🔍	Public potwork gotowow			
Next hop address :	1 . 1 . 1 . 254	 address of the AR router, which is subject to the actual value. 	Outbound interface :	GigabitEthernet0/0/8	×
Priority : 60		is subject to the actual value.	Description :		
i nong i	00				
Advanced > IP > Routing	Add				
Advanced > IP > Routing Routing Table	Add atic Route Configuration	Dynamic Route Configuration			
Advanced > IP > Routing Routing Table State	Add atic Route Configuration Configure a static route to acth	Dynamic Route Configuration /e			
Advanced > IP > Routing Routing Table Static Route Static Route Setting	Add atic Route Configuration Configure a static route to activ EIP 2 of the VPN gateway. S	Dynamic Route Configuration <i>r</i> e			
Advanced > IP > Routing Routing Table Sta IPv4 Static Route Static Route Setting * Destination IP :	Add atic Route Configuration Configure a static route to acth EIP 2 of the VPN gateway. Is 2 . 2 . 2 . 2	Dynamic Route Configuration re	* Subnet mask :	255 . 255 . 255 . 252	
Advanced > IP > Routing Routing Table Static Route Static Route Setting • Destination IP : VPN instance : • PP	Add atic Route Configuration Configure a static route to activ EIP 2 of the VPN gateway. IS 2 . 2 . 2 . 2 . 2 - none - V	Dynamic Route Configuration	* Subnet mask :	255 . 255 . 255 . 252	
Advanced > IP > Routing Routing Table Sta IPv4 Static Route Static Route Setting • Destination IP : VPN instance : Next hop address :	Add atic Route Configuration Configure a static route to acthe EIP 2 of the VPN gateway. is 2 . 2 . 2 . 2 - none - 1 . 1 . 1 . 254	Dynamic Route Configuration re Public network gateway dadress of the AR router, which to review to the action under	 Subnet mask : Outbound interface : 	255 . 255 . 255 . 252 GigabitEthernet0/0/8	

Figure 1-5 Configuring static routes

Step 3 Configure tunnel interfaces.

- 1. Choose **Advanced** > **Interface** > **Logical Interface**.
- Configure two tunnel interfaces and click Add.
 Figure 1-6 shows the key parameter settings.

Figure 1-6 Configuring tunnel interfaces

Advanced > Interface >	Logical Interface	2) Advanced > Interface >	Logical Interface	
Logical Interface Settings		Logical Interface Settings		
* Interface type :	* Interface type : O LoopBack		C LoopBack	
* Interface number :	1	* Interface number :	2	
* IP address/mask :	169 . 254 . 70 . 1 / 255 . 255 . 255 . 252	* IP address/mask :	169 . 254 . 71 . 1 / 255 . 255 . 255 . 252	
Interface description :		Interface description :		
Tunnel mode :	IPSec *	Tunnel mode :	IPSec 🔻	
* Source IP :	GigabitEthernet0/0/8	* Source IP :	GigabitEthernet0/0/8	
Destination IP :	1 . 1 . 1 . 2	Destination IP :	2 . 2 . 2 . 2	
VPN instance :	- none -	VPN instance :	- none - 🔻	
	Add		Add	

Step 4 Configure VPN connections.

- 1. Choose Advanced > VPN > IPSec > IPSec Policy Management.
- 2. Configure the IKE and IPsec policies for the two tunnels, as shown in Figure 1-7 and Figure 1-8.

NOTE

- When IKEv1 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function.
- When IKEv2 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on a device, this device disables the traffic timeout function.

Figure 1-7 Configuring VPN connection 1

IPSe	c policy settings						
• 1	PSec connection name :	ar-to-hwvpn-01			* Interface name :	Tunnel0/0/1	
◙	IKE Parameter setting						
	IKE version :	○ v1&v2 ○ v1	• v2	(V2 is recommended, other II	KE version has potential security ri	sks.)	
	Authentication mode :	Pre-shared key	🔿 RSA si	gnature	Pre-shared key :		
	Authentication algorithm :	SHA2-256	T		Encryption algorithm :	AES-128	
	DH group ID :	Group14			Integrity algorithm :	HMAC-SHA2-256	
୕	IPSec Parameter setting						
Ĩ	Security protocol :	ESP	v				
	ESP authentication algorithm :	SHA2-256			ESP encryption algorithm :	AFS-128	
	Encapsulation mode :	Tunnel mode	Transpo	rt mode			
	SHA2 algorithm compatible :						
	onne algoriann compatible i						
◙	Advanced						
	Local identity type :	• IP address) Name				
	Remote identity type :	• IP address) Name				
	Reauthentication interval (s) :	86400					
	DPD :	ON					
	DPD type :	Periodic sending	Ŧ		DPD packet payload sequence :	notify-hash 🔻	
	DPD idle time (s) :	30			DPD packet retransmission interval (s) :	15	
	DPD packet retransmission count :	3					
	PRF:	PRF-HMAC-SHA	2-256 🔻				
	PFS:	Group14	T				
	IKE SA duration (s) :	86400					
	IPSec SA aging mode :	Time-based (s) :	3600				
		Traffic-based (KB) :	1843200	0			
	Pre-extraction of original IP packets :	OFF					

IPSec policy settings						
* IPSec connection name :	ar-to-hwvpn-02			* Interface name :	Tunnel0/0/2	
♥ IKE Parameter setting						
IKE version :	⊖ v1&v2 ⊖ v	1 💿 1	2 (V2 is reco	ommended, other IKE version has potential security ri	sks.)	
Authentication mode :	• Pre-shared ke	/ () R	SA signature	Pre-shared key :		
Authentication algorithm :	SHA2-256		Ŧ	Encryption algorithm :	AES-128	•
DH group ID :	Group14		T	Integrity algorithm :	HMAC-SHA2-256	-
Security protocol :	ESP		-			
ESP authentication algorithm :	SHA2-256		-	ESP encryption algorithm :	AES-128	T
Encapsulation mode :	• Tunnel mode	🔿 Tra	nsport mode			
SHA2 algorithm compatible :	ON					
Advanced	IP address	Name				
Bounda identity type :	IP address	Name				
Remote identity type :) i vaine				
Reauthentication interval (s) :	86400					
DPD :						
DPD type :	Periodic sendin	9	~	DPD packet payload sequence :	notify-hash	*
DPD idle time (s) :	30			DPD packet retransmission interval (s) :	15	
DPD packet retransmission count :	3					
PRF:	PRF-HMAC-SH	2-256	•			
PFS :	Group14		T			
IKE SA duration (s) :	86400					
IPSec SA aging mode :	Time-based (s) :	3600				
	Traffic-based (KB) :	184320	0 🕜			
Pre-extraction of original IP packets :	OFF					

Figure 1-8 Configuring VPN connection 2

Step 5 Configure BGP.

- 1. Choose **Advanced** > **IP** > **Routing** > **Dynamic Route Configuration** > **BGP**.
- 2. Toggle on **Enable BGP**, set **AS Number** to the BGP ASN of the AR router, set **Router ID** to the gateway address of the downlink private network interface on the AR router, and click **Apply**.
- 3. Configure BGP peers, as shown in Figure 1-9.

Figure 1-9 Configuring BGP peers

Peer Configuration				
Peer Settings				
* Peer IP :	169 . 254 . 70 . 2	* Peer AS number :	64512	
Description :		Source interface :	Tunnel0/0/1	×
Maximum EBGP connection hop count :	255	Authentication :	OFF	
	Add			
Peer Configuration				
Peer Settings				
* Peer IP :	169 . 254 . 71 . 2	* Peer AS number :	64512	
Description :		Source interface :	Tunnel0/0/2	×
Maximum EBGP count :	255	Authentication :	OFF	
	Add			

4. In the **Route Import Configuration** area, set **Protocol type** to **Direct**.

1.1.2.4 Verification

- About 5 minutes later, check states of the VPN connections.
 - Huawei Cloud

Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Normal**.

AR router

Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**. The states of the two VPN connections are both **READY**|**STAYLIVE**.

• Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

1.1.3 Policy-based Mode

1.1.3.1 Operation Guide

Scenario

Figure 1-10 shows the typical networking where a VPN gateway connects to the Huawei AR router in an on-premises data center in policy-based mode.

Figure 1-10 Typical networking diagram



In this scenario, the AR router has only one IP address, and the VPN gateway uses the active-active mode. A VPN connection is created between each of the two active EIPs of the VPN gateway and the IP address of the AR router.

Limitations and Constraints

VPN and AR routers support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

Data Plan

Table	1-13 Data	plan
-------	-----------	------

Category	ltem	Example Value for the AR Router	Example Value for the Huawei Cloud Side	
VPC	Subnet	172.16.0.0/16	192.168.0.0/24192.168.1.0/24	
VPN gateway	Gatewa y IP address	1.1.1.1 (IP address of the uplink public network interface GE0/0/8 on the AR router)	Active EIP: 1.1.1.2Active EIP 2: 2.2.2.2	
Intercon nection subnet		-	192.168.2.0/24	
VPN connectio n	IKE policy	 IKE version: IKEv2 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 DH algorithm: group 14 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address 		
	IPsec policy	 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 PFS: DH group 14 Transfer protocol: ESP Lifetime (s): 3600 		

Operation Process

Figure 1-11 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-11 Operation process



N o.	Configurat ion Interface	Step	Description
1	Manageme nt console	Create a VPN gateway.	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2		Create a customer gateway.	Configure the AR router as the customer gateway.
3		Create VPN connection 1.	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4		Create VPN connection 2.	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	CLI of the AR router	Configure the AR router.	 The local and remote tunnel interface addresses configured on the AR router must be the same as the customer and local tunnel interface addresses configured on the VPN console, respectively. The connection mode, PSK, IKE policy, and IPsec policy settings on the AR router must be same as those of VPN connections.
6	-	Verify network connectivity.	Run the ping command to verify network connectivity.

1.1.3.2 Configuration on the Cloud Console

Prerequisites

A VPC and its subnets have been created on the management console.

Procedure

- **Step 1** Log in to Huawei Cloud management console.
- **Step 2** Choose **Networking > Virtual Private Network**.
- **Step 3** Configure a VPN gateway.
 - Choose Virtual Private Network > Enterprise VPN Gateways. On the S2C VPN Gateways tab page, click Buy S2C VPN Gateway.
 - 2. Set parameters as prompted and click **Buy Now**.

Table 1-15 only describes the key parameters for configuring a VPN gateway. For other parameters, use their default settings.

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select VPC .	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0. 0/16)
Interconn ection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on- premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2

 Table 1-15 Key parameters for creating a VPN gateway

Paramete r	Description	Value
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

Table 1-16 describes the parameters for creating a customer gateway.

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar
Identifier	Select IP Address , and enter the public IP address of the AR router.	IP Address 1.1.1.1
BGP ASN	BGP AS number of the AR router.	65000

Table 1-16 Parameters for creating a customer gateway

Step 5 Configure VPN connections.

In this scenario, a VPN connection is created between the AR router and each of the active EIP and active EIP 2 of the VPN gateway.

- 1. Choose Virtual Private Network > Enterprise VPN Connections, and click Buy VPN Connection.
- 2. Create VPN connection 1.

 Table 1-17 describes the parameters for creating a VPN connection.

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-ar
VPN Type	Select Policy-based.	Policy-based

Table 1-17	' Parameter	settings	for VPN	connection	1
------------	-------------	----------	---------	------------	---

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud.	172.16.0.0/16
	 A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. 	
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway device.	<i>Set this parameter based on the site requirements.</i>
Policy	 A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. Destination CIDR Block The destination CIDR Block must contain all customer subnets. 	 Source CIDR block 1: 192.168.0.0/24 Destination CIDR block 1: 172.16.0.0/16 Source CIDR block 2: 192.168.1.0/24 Destination CIDR block 2: 172.16.0.0/16

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	IKE PolicyVersion: v2
		 Authentication Algorithm: SHA2-256
		 Encryption Algorithm: AES-128
		 DH Algorithm: Group 14
		 Lifetime (s): 86400
		 Local ID: IP Address
		 Customer ID: IP Address IPsec Policy
		 Authentication Algorithm: SHA2-256
		 Encryption Algorithm: AES-128
		 PFS: DH group 14
		 Transfer Protocol: ESP
		 Lifetime (s): 3600

3. Create VPN connection 2.

NOTE

For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2

 Table 1-18 Parameter settings for VPN connection 2

----End

1.1.3.3 Configuration on the AR Router

Prerequisites

- The WAN interface GE0/0/8 on the AR router has been configured. Assume that the public IP address of the WAN interface is 1.1.1.1.
- The LAN interface GE0/0/1 on the AR router has been configured. Assume that the public IP address of the LAN interface is 172.16.0.1.

Procedure

Step 1 Log in to the web system of the AR router.

An AR651 running V300R019C13SPC200 is used as an example. The web system may vary according to the device model and software version.

Step 2 Configure VPN connections.

- 1. Choose Advanced > VPN > IPSec > IPSec Policy Management.
- 2. Configure the IKE and IPsec policies, as shown in Figure 1-12.

- When IKEv1 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function.
- When IKEv2 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on a device, this device disables the traffic timeout function.
- If the AR router uses a non-fixed IP address to connect to the VPN gateway, click Advanced, set Local identity type to Name, and enter the customer gateway identifier configured on the cloud in the Local name text box.

IPSec Policy Management	IPSec Global	Settings				
as policy sottings		5				
inconstanting settings				* 1-*f		
IPSec connection name :	ar-to-vpn			- Interface name :	GigabitEthernet0/0/8	
Networking mode :	Branch He	eadquarters		* Connection ID :	1	
ACL Number :	3999					
IKE Parameter setting						
IKE version :	○ v1&v2 ○ v	v1 • v2	(V2 is recommended, other	IKE version has potential security ri	sks.)	
* Remote address :	IP address	Ŧ	1.1.1.2	0		
	IP address	Ŧ	2.2.2.2	×		
Authentication mode :	 Pre-shared key 	y ORSA s	gnature	Pre-shared key :		
Authentication algorithm :	SHA2-256	Ŧ		Encryption algorithm :	AES-128	T
DH group ID :	Group14	T		Integrity algorithm :	HMAC-SHA2-256	•
PSec Parameter setting						
Security protocol :	ESP	Ŧ				
ESP authentication algorithm :	SHA2-256	~		ESP encryption algorithm :	AES-128	-
Encapsulation mode :	Tunnel mode	Transpo	rt mode			
		110110000	i c moue			
CHA2 algorithm compatible :			i induc			
SHA2 algorithm compatible :			i node			
SHA2 algorithm compatible :						
SHA2 algorithm compatible : Advanced IKE negotiation :	Auto Tra	affic-based	i indec			
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type :	Auto Tra IP address	affic-based OName				
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type :	Auto Tra IP address IP address	affic-based Name				
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) :	Auto Tra IP address IP address 86400	affic-based Name Name				
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD :	Auto Tr. IP address IP address 86400 ON	affic-based Name Name				
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type :	Auto Tri IP address IP address IP address IP address IP address	affic-based Name Name)	DPD packet payload sequence :	notify-hash	v
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD job :	Auto Trr IP address IP address B6400 ON Periodic sendin 30	affic-based Name Name)	DPD packet payload sequence : DPD packet etransmission interval (c)	notify-hash 15	Ŧ
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD dile time (s) : DPD packet retransmission	Auto Tri IP address IP address B6400 ON Periodic sendin 30 3	affic-based Name Name		DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	¥
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD dale time (s) : DPD packet retransmission count : PRF :	Auto Trr IP address IP Addres IP Address IP Address IP Address IP A	affic-based Name Name		DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	¥
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD dide time (s) : DPD packet retransmission count : PRF : PFS :	Auto IP address IP address IP address B6400 ON Periodic sendin 30 3 PRF-HMAC-SH. Group14	affic-based Name Name		DPD packet payload sequence : DPD packet retransmission interval (6) :	notify-hash 15	¥
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD tidle time (s) : DPD packet retransmission count : PRF : PFS : IKE SA duration (s) :	Auto Tri IP address IP addres IP addres IP address IP address IP address I	affic-based Name Name		DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	v
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD dide time (s) : DPD packet retransmission count : PRF : PFS : IKE SA duration (s) : IVC = Charine under	Auto Trr IP address IP	affic-based Name Name		DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	v
 SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD jacket retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode : 	Auto Tri IP address If address	affic-based Name Name A2-256 ¥ 3600		DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	•
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD dile time (s) : DPD packet retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode :	Auto Tri IP address IP address IP address If address If address IP address If address	affic-based Name Name ag A2-256 ¥ 3600 1843200	2 2	DPD packet payload sequence : DPD packet retransmission interval (s) :	notify-hash 15	•
SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD jacket retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode : Local address :	Auto Tri IP address IP address IP address If address IP address IP address If address IP address IF address	affic-based Name Name A2-256 ¥ 3600 1843200		DPD packet payload sequence : DPD packet retransmission interval (5) : Address type :	notify-hash 15 • Interface address	• Specified addre
 SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD jacket retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode : Local address : IP address : 	Auto Tri IP address IP address B6400 Periodic sendin 30 3 PRF-HMAC-SHI Group14 86400 Time-based (s) : Traffic-based (KB): . .	affic-based Name Name A2-256 ¥ 3600 1843200		DPD packet payload sequence : DPD packet retransmission interval (s) : Address type :	notify-hash 15 • Interface address	Specified addres
 SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD jacket retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode : Local address : IP address : Route import : 	Auto Tri IP address IF address	affic-based Name Name A2-256 ¥ A2-256 ¥		DPD packet payload sequence : DPD packet retransmission interval (s) : Address type :	notify-hash 15 • Interface address	• Specified addres
 SHA2 algorithm compatible : SHA2 algorithm compatible : Advanced IKE negotiation : Local identity type : Remote identity type : Reauthentication interval (s) : DPD : DPD type : DPD type : DPD jacket retransmission count : PRF : PFS : IKE SA duration (s) : IPSec SA aging mode : Local address : IP address : Route import : Route import type : 	Auto Tri IP address IF addres If address If address If address If address	affic-based Name Name A2-256 ¥ A2-256 ¥ 3600 1843200		DPD packet payload sequence : DPD packet retransmission interval (5) : Address type : Route priority :	notify-hash 15 • Interface address 60	Specified addre

Figure 1-12 Configuring VPN connections

Step 3 Configure a VPN security policy.

Choose **Configuration** > **Attack Defense** > **ACL** > **Advanced ACL**, configure an advanced ACL, and click **Add**. **Figure 1-13** shows the key parameter settings.

 Configuration > Attack Defense 	e > ACL			
Basic ACL Advance	d ACL	Layer 2 AC	L	Time Range
Rule Settings				
* Rule number :	1			
Action :	• Permit	O Deny		
ACL Type :	● IPv4 ○) IPv6		
* Protocol type :	IP			
* Effective ACL :	GE0/0/8			Create
Advanced 💿				
Matched priority :	- none -			
ToS priority :				
Matched IP address				
Source IP/Wildcard :	172 . 16	j. O.	0	/ 0 . 0 . 255 . 255
Destination IP/Wildcard :	192 . 168	Β.Ο.	0	/ 0 . 0 . 255 . 255
Time range name :	- none -			
	Add			

Figure 1-13 Configuring an advance ACL

Step 4 Configure service routes.

Choose Advanced > IP > Routing > Static Route Configuration. In the IPv4 Static Route area, configure static routes to the active EIP and active EIP 2 of the VPN gateway and a static route to the VPC, and click Add. Figure 1-14 shows the key parameter settings.

Routing Table Sta	tic Route Configuration	Dynamic Route Configuration		
IPv4 Static Route	Configure a static route to the			
Static Route Setting	s			
* Destination IP :	1 . 1 . 1 . 2		* Subnet mask :	255 . 255 . 255 . 252
VPN instance (Public network gateway		
vi i i istance i				
Next hop address :	1 . 1 . 1 . 254	address of the AR router, which is subject to the actual value.	Outbound interface :	GigabitEthernet0/0/8 X
Priority :	60		Description :	
	Add			
Advanced > IP > Routing				
Routing Table Sta	atic Route Configuration	Dynamic Route Configuration		
Dud Statis Boute	Configure a static route to acti	ve		
Static Route Catting	EIP 2 of the VPN gateway.			
static Route setting	5			
* Destination IP :	2.2.2.2		* Subnet mask :	255 . 255 . 255 . 252
VPN instance :	- none - 🔍 🔻			
VPN instance : Next hop address :	- none - 🔻	Public network gateway ddress of the AR router, which	Outbound interface :	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority :	- none - v	 Public network gateway address of the AR router, which is subject to the actual value. 	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority :	- none	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description :	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority :	- none - v 1 . 1 . 1 . 254 60 Add	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority :	- none - v 1 . 1 . 1 . 254 60 Add	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority :	- none	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority : Advanced > IP > Routing	- none	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table	- none	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table St. P IPv4 Static Route	- none - ▼ 1 . 1 . 1 . 254 60 Add atic Route Configuration Configure a static	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration	Outbound interface : Description :	GigabitEthernet0/0/8 X
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table St. IPV4 Static Route Static Route Setting	none - T 1 . 1 . 1 . 254 60 Add atic Route Configuration Configure a static route to the VPC. S	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration	Outbound interface : Description :	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table Static Route Setting	- none - ▼ 1 . 1 . 1 . 254 60 Add Add atic Route Configuration Configure a static route to the VPC. s 122 . 150 . 0 . 0 . 0	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration	Outbound interface : Description :	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table Static Route Static Route Static Route Setting > Destination IP :	- none - ▼ 1 . 1 . 254 60 Add atic Route Configuration .	Public network gateway address of the AR router, which is subject to the actual value.	Outbound interface : Description : 	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table Static Route Static Route Static Route Setting * Destination IP : VPN instance :	- none - ▼ 1 . 1 . 254 60 Add atic Route Configuration .	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration Public network gateway	Outbound interface : Description : Subnet mask :	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table St i IPv4 Static Route Setting * Destination IP : VPN instance : Next hop address :	- none - ▼ 1 1 254 60 - - Add - - atic Route Configuration - - Configure a static - - route to the VPC. s - 12 .168 0 .0 - none - ▼ 1 .1 .254	Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration Public network gateway datress of the AR router, which is rouble to the actual value.	Outbound interface : Description : 	GigabitEthernet0/0/8 ×
VPN instance : Next hop address : Priority : Advanced > IP > Routing Routing Table St > IPv4 Static Route — Static Route Setting • Destination IP : VPN instance : Next hop address : Priority :	- none - ▼ 1 1 254 60 - Add - atic Route Configuration - Configure a static - route to the VPC. S 192 .168 0 - none - ▼ 1 .1 .254 60 - -	 Public network gateway address of the AR router, which is subject to the actual value. Dynamic Route Configuration Public network gateway address of the AR router, which is subject to the actual value. 	Outbound interface : Description : 	GigabitEthernet0/0/8 ×

Figure 1-14 Configuring service routes

----End

1.1.3.4 Verification

NOTE

In policy-based mode, an AR router uses one interface to establish two VPN connections. Due to the specification limit of the AR router, only one VPN connection can be established at a time.

- About 5 minutes later, check states of the VPN connections.
 - Management console of the cloud

Choose **Virtual Private Network** > **Enterprise – VPN Connections**. Only one VPN connection is in **Normal** state.

AR router

Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**. Only one VPN connection is in **READY|STAYLIVE** state.

• Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

2 P2C VPN

2.1 Using the CCM to Manage a Server Certificate

Procedure

- **Step 1** Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select the desired region and project.
- **Step 3** Click in the upper left corner of the page, and choose **Networking** > **Virtual Private Network**.
- **Step 4** In the navigation pane on the left, choose **Virtual Private Network > Enterprise VPN Gateways**.
- **Step 5** Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** in the **Operation** column.
- **Step 6** On the **Server** tab page, click **Upload** in the **Server Certificate** drop-down list box. The **Cloud Certificate Manager** page is displayed.
- **Step 7** On the **SSL Certificate Manager** page, click the **Hosted Certificates** tab, click **Upload Certificate**, and enter related information as prompted.

 Table 2-1 describes the parameters for uploading a certificate.

Parameter	Description
Certificate standard	Select International.
Certificate Name	User-defined name of a certificate.
Enterprise Project	Select the enterprise project to which the SSL certificate is to be added.

 Table 2-1 Parameters for uploading an international standard certificate

Parameter	Description
Certificate File	Use a text editor (such as Notepad++) to open the certificate file in CER or CRT format to be uploaded, and copy the certificate content to this text box.
	You need to upload a combined certificate file that contains both the server certificate content and CA certificate content. The CA certificate content must be pasted below the server certificate content.
	NOTE If you do not have a certificate, you can generate a self-issued certificate and upload it. For details, see Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate).
	For the format of the certificate file content to be uploaded, see Figure 2-1 .
Private Key	Use a text editor (such as Notepad++) to open the certificate file in KEY format to be uploaded, and copy the private key content to this text box.
	You only need to upload the private key of the server certificate.
	For the format of the private key content to be uploaded, see Figure 2-1 .

Figure 2-1	Format of the	certificate	content to	be uploaded
------------	---------------	-------------	------------	-------------

* Certificate File	Upload	
	BEGIN CERTIFICATE +OlfG82xmmjOZkE6bQ== END CERTIFICATE BEGIN CERTIFICATE 9z3BpmtjJ5fgf7ufUg/Npv6Tpu51 END CERTIFICATE	
* Private Key	Upload BEGIN PRIVATE KEY MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDWkvw9dofJLcEA END PRIVATE KEY	
		4

NOTE

The common name (CN) of a server certificate must be in the domain name format.

- **Step 8** Click **Submit**. The certificate is uploaded.
- **Step 9** In the certificate list, verify that the certificate status is **Hosted**.

----End

2.2 Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate)

Scenario

Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

This example describes how to use Easy-RSA to issue certificates on the Windows operating system in the scenario where the server and client share a CA certificate. In this example, Easy-RSA 3.1.7 is used. For other software versions, visit the official website for the corresponding operation guide.

Procedure

- 1. Download an Easy-RSA installation package to the **D**:\ directory based on your Windows operating system.
 - 32-bit Windows operating system: Download EasyRSA-3.1.7-win32.zip.
 - 64-bit Windows operating system: Download EasyRSA-3.1.7-win64.zip.

In this example, EasyRSA-3.1.7-win64 is downloaded.

▼Assets 8		
HeasyRSA-3.1.7-win32.zip	3.31 MB	Oct 14, 2023
⊗EasyRSA-3.1.7-win32.zip.sig	310 Bytes	Oct 14, 2023
⊗EasyRSA-3.1.7-win64.zip	3.63 MB	Oct 14, 2023
⊗EasyRSA-3.1.7-win64.zip.sig	310 Bytes	Oct 14, 2023
⊗EasyRSA-3.1.7.tgz	79.5 KB	Oct 14, 2023
⊗EasyRSA-3.1.7.tgz.sig	310 Bytes	Oct 14, 2023
Bource code (zip)		Oct 11, 2023
Source code (tar.gz)		Oct 11, 2023

- Decompress EasyRSA-3.1.7-win64.zip to a specified directory, for example, D:\EasyRSA-3.1.7.
- 3. Go to the D:\EasyRSA-3.1.7 directory.
- 4. Enter cmd in the address bar and press Enter to open the CLI.
- 5. Run the .\EasyRSA-Start.bat command to start Easy-RSA.

Information similar to the following is displayed:

Welcome to the EasyRSA 3 Shell for Windows. Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell

6. Run the **./easyrsa init-pki** command to initialize the PKI environment.

Information similar to the following is displayed:

Notice

'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is: * D:/EasyRSA-3.1.7/pki

Using Easy-RSA configuration:

* undefined

EasyRSA Shell

After the command is executed, the **pki** folder is automatically generated in the **D:\EasyRSA-3.1.7** directory.

- 7. Set parameters.
 - a. Copy the vars.example file in D:\EasyRSA-3.1.7 to the D:\EasyRSA-3.1.7\pki directory.
 - b. Rename vars.example in the D:\EasyRSA-3.1.7\pki directory to vars.

NOTE

By default, the **vars** file uses the same parameter settings as the **vars.example** file. You can also set parameters in the **vars** file as required.

8. Run the **./easyrsa build-ca nopass** command to generate a CA certificate.

Information similar to the following is displayed:

Using Easy-RSA 'vars' configuration: * D:/EasyRSA-3.1.7/pki/vars

Using SSL:

If you enter '.', the field will be left blank.

Common Name (eg: your user, host, or server name) [Easy-RSA CA]:**p2cvpn.com** //Set a name for the CA certificate.

Notice

CA creation complete. Your new CA certificate is at: * D:/EasyRSA-3.1.7/pki/ca.crt

EasyRSA Shell

- 9. View the CA certificate and private key.
 - By default, the generated CA certificate is stored in the D:\EasyRSA-3.1.7\pki directory.

In this example, the certificate **ca.crt** is generated.

 By default, the generated CA private key is stored in the D:\EasyRSA-3.1.7\pki\private directory.

In this example, the private key **ca.key** is generated.

10. Run the **./easyrsa build-server-full** *p2cserver.com* **nopass** command to generate a server certificate and private key.

In this command, *p2cserver.com* is the common name (CN) of the server certificate. Replace it with the actual CN. The CN must be in the domain

name format; otherwise, the certificate cannot be managed by the Cloud Certificate Manager (CCM).

Information similar to the following is displayed:

Using Easy-RSA 'vars' configuration: * D:/EasyRSA-3.1.7/pki/vars

Using SSL:

* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)

Notice

Private-Key and Public-Certificate-Request files created. Your files are:

* req: D:/EasyRSA-3.1.7/pki/reqs/p2cserver.com.req

* key: D:/EasyRSA-3.1.7/pki/private/p2cserver.com.key

You are about to sign the following certificate: Request subject, to be signed as a server certificate for '825' days:

subject= commonName

= p2cserver.com

Type the word 'yes' to continue, or any other input to abort. Confirm request details: **yes** //Enter **yes** to continue.

Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf Check that the request matches the signature Signature ok The Subject's Distinguished Name is as follows commonName :ASN.1 12:'p2cserver.com' Certificate is to be certified until Sep 22 09:56:54 2026 GMT (825 days)

Write out database with 1 new entries Database updated

Notice

------Certificate created at: * D:/EasyRSA-3.1.7/pki/issued/p2cserver.com.crt

Notice

------Inline file created: * D:/EasyRSA-3.1.7/pki/inline/p2cserver.com.inline

EasyRSA Shell #

11. View the server certificate and private key.

 By default, the generated server certificate is stored in the D:\EasyRSA-3.1.7\pki\issued directory.

In this example, the server certificate p2cserver.com.crt is generated.

 By default, the generated server private key is stored in the D:\EasyRSA-3.1.7\pki\private directory.

In this example, the server private key p2cserver.com.key is generated.

12. Run the **./easyrsa build-client-full** *p2cclient.com* **nopass** command to generate a client certificate and private key.

In this command, the client certificate name (for example, *p2cclient.com*) must be different from the server certificate name (for example, *p2cserver.com*).

Information similar to the following is displayed:

Using Easy-RSA 'vars' configuration: * D:/EasyRSA-3.1.7/pki/vars

Using SSL:

* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)

Notice

Private-Key and Public-Certificate-Request files created. Your files are:

* req: D:/EasyRSA-3.1.7/pki/reqs/p2cclient.com.req * key: D:/EasyRSA-3.1.7/pki/private/p2cclient.com.key

You are about to sign the following certificate:

Request subject, to be signed as a client certificate for '825' days:

subject=

commonName = p2cclient.com

Type the word 'yes' to continue, or any other input to abort. Confirm request details: **yes** //Enter **yes** to continue.

Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf Check that the request matches the signature Signature ok The Subject's Distinguished Name is as follows commonName :ASN.1 12:'p2cclient.com' Certificate is to be certified until Sep 22 09:58:26 2026 GMT (825 days)

Write out database with 1 new entries Database updated

Notice -----Certificate created at: * D:/EasyRSA-3.1.7/pki/issued/p2cclient.com.crt

Notice

```
Inline file created:
* D:/EasyRSA-3.1.7/pki/inline/p2cclient.com.inline
```

EasyRSA Shell #

- 13. View the client certificate and private key.
 - By default, the generated client certificate is stored in the D:\EasyRSA-3.1.7\pki\issued directory.
 - In this example, the client certificate **p2cclient.com.crt** is generated.
 - By default, the generated client private key is stored in the D:\EasyRSA-3.1.7\pki\private directory.

In this example, the client private key **p2cclient.com.key** is generated.

2.3 Using Easy-RSA to Issue Certificates (Server and Client Using Different CA Certificates)

Scenario

Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

This example describes how to use Easy-RSA to issue certificates on the Windows operating system in the scenario where the server and client use different CA certificates. In this example, Easy-RSA 3.1.7 is used. For other software versions, visit the official website for the corresponding operation guide.

Procedure

- 1. Download an Easy-RSA installation package to the **D:** directory based on your Windows operating system.
 - 32-bit Windows operating system: Download EasyRSA-3.1.7-win32.zip.
 - 64-bit Windows operating system: Download EasyRSA-3.1.7-win64.zip.

In this example, **EasyRSA-3.1.7-win64** is downloaded.

▼ Assets 8		
𝔅EasyRSA-3.1.7-win32.zip	3.31 MB	Oct 14, 2023
𝔅EasyRSA-3.1.7-win32.zip.sig	310 Bytes	Oct 14, 2023
⊗EasyRSA-3.1.7-win64.zip	3.63 MB	Oct 14, 2023
⊗EasyRSA-3.1.7-win64.zip.sig	310 Bytes	Oct 14, 2023
𝔅EasyRSA-3.1.7.tgz	79.5 KB	Oct 14, 2023
𝔅EasyRSA-3.1.7.tgz.sig	310 Bytes	Oct 14, 2023
Source code (zip)		Oct 11, 2023
Source code (tar.gz)		Oct 11, 2023

- 2. Decompress **EasyRSA-3.1.7-win64.zip** to a specified directory, for example, **D:\EasyRSA-3.1.7**.
- 3. Go to the D:\EasyRSA-3.1.7 directory.
- 4. Enter cmd in the address bar and press Enter to open the CLI.
- Run the .\EasyRSA-Start.bat command to start Easy-RSA. Information similar to the following is displayed:

Welcome to the EasyRSA 3 Shell for Windows. Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell #

6. Run the ./easyrsa init-pki command to initialize the PKI environment.

Information similar to the following is displayed: Notice

'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is: * D:/EasyRSA-3.1.7/pki

Using Easy-RSA configuration: * undefined

EasyRSA Shell #

After the command is executed, the **pki** folder is automatically generated in the **D:\EasyRSA-3.1.7** directory.

- 7. Set parameters.
 - a. Copy the vars.example file in D:\EasyRSA-3.1.7 to the D:\EasyRSA-3.1.7\pki directory.
 - b. Rename vars.example in the D:\EasyRSA-3.1.7\pki directory to vars.

NOTE

By default, the **vars** file uses the same parameter settings as the **vars.example** file. You can also set parameters in the **vars** file as required.

- 8. Generate a server CA certificate and private key.
 - a. Copy the decompressed **EasyRSA-3.1.7** folder to the **D**:\ directory, and rename the folder, for example, **EasyRSA-3.1.7 server**.
 - b. Go to the D:\EasyRSA-3.1.7 server directory.
 - c. In the address bar of the **D:\EasyRSA-3.1.7 server** folder, enter **cmd** and press **Enter** to open the CLI.
 - d. Run the .\EasyRSA-Start.bat command to start Easy-RSA.

Information similar to the following is displayed:

Welcome to the EasyRSA 3 Shell for Windows. Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell

e. Run the **./easyrsa build-ca nopass** command to generate a server CA certificate.

When this command is run, set **[Easy-RSA CA]** to the name of the server CA certificate as prompted, for example, **p2cvpn_server.com**.

Information similar to the following is displayed:

Using Easy-RSA 'vars' configuration:

* D:/EasyRSA-3.1.7 - server/pki/vars

Using SSL:

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

i you enter ., the held will be left

Common Name (eg: your user, host, or server name) [Easy-RSA CA]:**p2cvpn_server.com** //Set a name for the server CA certificate.

Notice ------CA creation complete. Your new CA certificate is at: * D:/EasyRSA-3.1.7 - server/pki/ca.crt

EasyRSA Shell

- 9. View the server CA certificate and private key.
 - By default, the generated server CA certificate is stored in the D:\EasyRSA-3.1.7 - server\pki directory.

In this example, the server certificate **ca.crt** is generated.

 By default, the generated server CA private key is stored in the D:\EasyRSA-3.1.7 - server\pki\private directory.

In this example, the server private key **ca.key** is generated.

10. Run the **./easyrsa build-server-full** *p2cserver.com* **nopass** command to generate a server certificate and private key.

In this command, *p2cserver.com* is the common name (CN) of the server certificate. Replace it with the actual CN. The CN must be in the domain name format; otherwise, the certificate cannot be managed by the Cloud Certificate Manager (CCM).

Information similar to the following is displayed:

```
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7 - server/pki/reqs/p2cserver.com.req
* key: D:/EasyRSA-3.1.7 - server/pki/private/p2cserver.com.key
You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:
subject=
  commonName
                              = p2cserver.com
Type the word 'yes' to continue, or any other input to abort.
 Confirm request details: yes //Enter yes to continue.
Using configuration from D:/EasyRSA-3.1.7 - server/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName
                       :ASN.1 12:'p2cserver.com'
Certificate is to be certified until Oct 6 03:28:14 2026 GMT (825 days)
Write out database with 1 new entries
Database updated
Notice
Certificate created at:
* D:/EasyRSA-3.1.7 - server/pki/issued/p2cserver.com.crt
Notice
Inline file created:
* D:/EasyRSA-3.1.7 - server/pki/inline/p2cserver.com.inline
EasyRSA Shell
```

- 11. View the server certificate and private key.
 - By default, the generated server certificate is stored in the
 D:\EasyRSA-3.1.7 server\pki\issued directory.
 In this example, the server certificate p2cserver.com.crt is generated.
 - By default, the generated server private key is stored in the D:\EasyRSA-3.1.7 - server\pki\private directory.

In this example, the server private key **p2cserver.com.key** is generated.

- 12. Generate a client CA certificate and private key.
 - a. Copy the decompressed **EasyRSA-3.1.7** folder to the **D:** directory, and rename the folder, for example, **EasyRSA-3.1.7 client**.
 - b. Go to the **EasyRSA-3.1.7 client** directory.
 - c. In the address bar of the **EasyRSA-3.1.7 client** folder, enter **cmd** and press **Enter** to open the CLI.
 - d. Run the **.\EasyRSA-Start.bat** command to start Easy-RSA. Information similar to the following is displayed: Welcome to the EasyRSA 3 Shell for Windows. Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell

e. Run the **./easyrsa build-ca nopass** command to generate a client CA certificate.

Information similar to the following is displayed:

Using Easy-RSA 'vars' configuration: * D:/EasyRSA-3.1.7 - client/pki/vars Using SSL: * openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023) +++++++*....+...+....+....+++++++ **** You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn_client.com //Set a name for the client CA certificate.

Notice

CA creation complete. Your new CA certificate is at: * D:/EasyRSA-3.1.7 - client/pki/ca.crt

EasyRSA Shell

- 13. View the client CA certificate and private key.
 - By default, the generated client CA certificate is stored in the D:\EasyRSA-3.1.7 - client\pki directory.

In this example, the client certificate **ca.crt** is generated.

 By default, the generated client CA private key is stored in the D:\EasyRSA-3.1.7 - client\pki\private directory.

In this example, the client private key **ca.key** is generated.

14. Run the **./easyrsa build-client-full** *p2cclient.com* **nopass** command to generate a client certificate and private key.

In this command, the client certificate name (for example, *p2cclient.com*) must be different from the server certificate name (for example, *p2cserver.com*).

Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - client/pki/vars
```

Using SSL:

Notice
Private-Key and Public-Certificate-Request files created. Your files are: * req: D:/EasyRSA-3.1.7 - client/pki/reqs/p2cclient.com.req * key: D:/EasyRSA-3.1.7 - client/pki/private/p2cclient.com.key
You are about to sign the following certificate: Request subject, to be signed as a client certificate for '825' days:
subject= commonName = p2cclient.com
Type the word 'yes' to continue, or any other input to abort. Confirm request details: yes
Using configuration from D:/EasyRSA-3.1.7 - client/pki/openssl-easyrsa.cn Check that the request matches the signature Signature ok The Subject's Distinguished Name is as follows commonName :ASN.1 12:'p2cclient.com' Certificate is to be certified until Oct 7 11:19:52 2026 GMT (825 days)
Write out database with 1 new entries Database updated
Notice
Certificate created at: * D:/EasyRSA-3.1.7 - client/pki/issued/p2cclient.com.crt
Notice
Inline file created: * D:/EasyRSA-3.1.7 - client/pki/inline/p2cclient.com.inline
EasyRSA Shell #

- 15. View the client certificate and private key.
 - By default, the generated client certificate is stored in the D:\EasyRSA-3.1.7 - client\pki\issued directory.

In this example, the client certificate **p2cclient.com.crt** is generated.

By default, the generated client private key is stored in the D:\EasyRSA-3.1.7 - client\pki\private directory.

In this example, the client private key **p2cclient.com.key** is generated.

2.4 Using the CCM to Purchase Certificates

Context

In addition to purchasing certificates from CAs and issuing certificates by yourselves, you can use the CCM to purchase certificates, including the server and client certificates.

Constraints

If you purchase a server certificate using the CCM, you need to add the server root certificate content to the client configuration file.

Procedure

- Purchasing a server certificate
 - a. Log in to the CCM console.
 - b. Purchase an SSL certificate.
 - c. Apply for an SSL certificate.

Certificates purchased from the CCM are automatically hosted.

- d.
- e. Install the root certificate.

Open the root certificate using a text editor (for example, Notepad++), and copy the certificate content to the end of the existing CA certificate in the client configuration file. For details, see **How Do I Fix an Incomplete SSL Certificate Chain?**.

The format is as follows:

```
...

<ca>

-----BEGIN CERTIFICATE-----

Default level-2 CA certificate content of the server

-----END CERTIFICATE-----

Server root certificate content

-----END CERTIFICATE-----

</ca>

...
```

- Purchasing a client certificate
 - a. Log in to the CCM console.
 - b. Purchase an SSL certificate.
 - c. Apply for an SSL certificate.
 - d. .