

Virtual Private Network

Administrator Guide

Issue 01
Date 2025-02-05



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



HUAWEI 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: support@huawei.com

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:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

1 S2C Enterprise Edition VPN

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

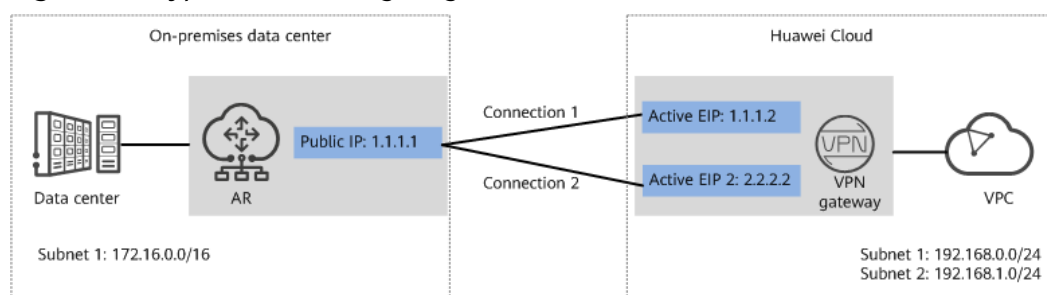
1.1.1 Static Routing Mode

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

Table 1-1 Data plan

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/16	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Active EIP: 1.1.1.2• Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	Tunnel interface address	<ul style="list-style-type: none">• Tunnel 1: 169.254.70.1/30• Tunnel 2: 169.254.71.1/30	<ul style="list-style-type: none">• Tunnel 1: 169.254.70.2/30• Tunnel 2: 169.254.71.2/30
	IKE policy	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Authentication algorithm: SHA2-256• Encryption algorithm: AES-128• PFS: DH group 14• Transfer protocol: ESP• Lifetime (s): 3600	

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

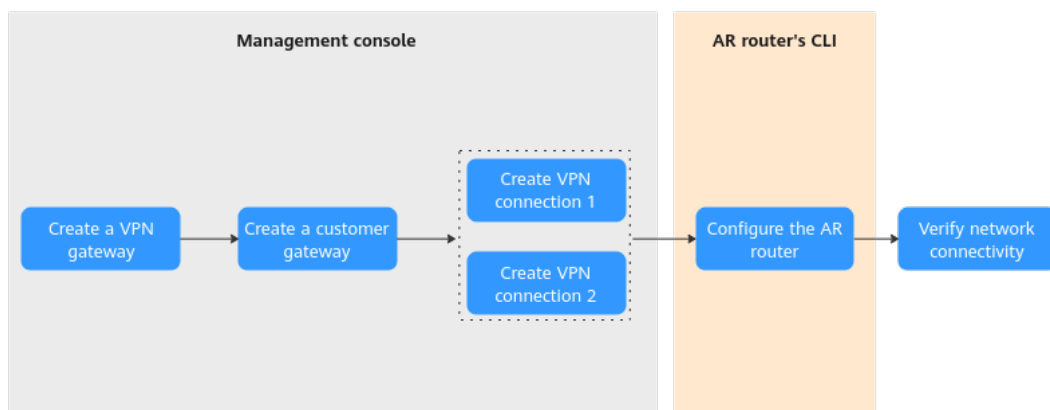


Table 1-2 Operation process description

N o.	Configurat ion Interface	Step	Description
1	Managem ent 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.	<ul style="list-style-type: none"> 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.

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

Table 1-3 describes the parameters for creating a VPN gateway.

Table 1-3 Parameters for creating a VPN gateway

Parameter	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)
Interconnection 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 1	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

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.

Table 1-4 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. The value must be different from the BGP ASN of the VPN gateway.	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 1-5 describes the parameters for creating a VPN connection.

Table 1-5 Parameter settings for VPN connection 1

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

Parameter	Description	Value
Customer Subnet	<p>Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud.</p> <ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Manually specify In this example, Manually specify is selected.- Automatically assign	Manually specify
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
Link Detection	<p>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.</p> <p>The VPN gateway can automatically perform NQA detection on the peer interface address that has been configured on the customer gateway.</p>	NQA enabled
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.	<ul style="list-style-type: none">- IKE Policy<ul style="list-style-type: none">▪ 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- IPsec Policy<ul style="list-style-type: none">▪ 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.

Table 1-6 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

1.1.1.3 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.
 - **Tunnelx** and **IPsec_nqax** 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.

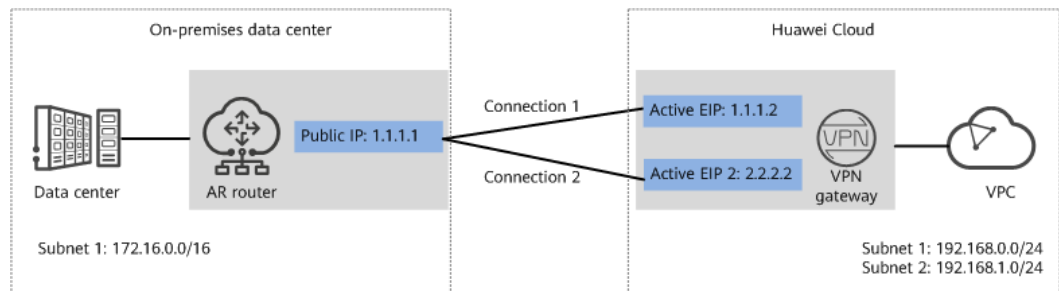
1.1.2 BGP Routing Mode

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

Table 1-7 Data plan

Category	Item	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
	Interconnection subnet	-	192.168.2.0/24
	BGP ASN	64515	64512

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface address	<ul style="list-style-type: none"> Tunnel 1: 169.254.70.1/30 Tunnel 2: 169.254.71.1/30 	<ul style="list-style-type: none"> Tunnel 1: 169.254.70.2/30 Tunnel 2: 169.254.71.2/30
	IKE policy	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 PFS: DH group 14 Transfer protocol: ESP Lifetime (s): 3600 	

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

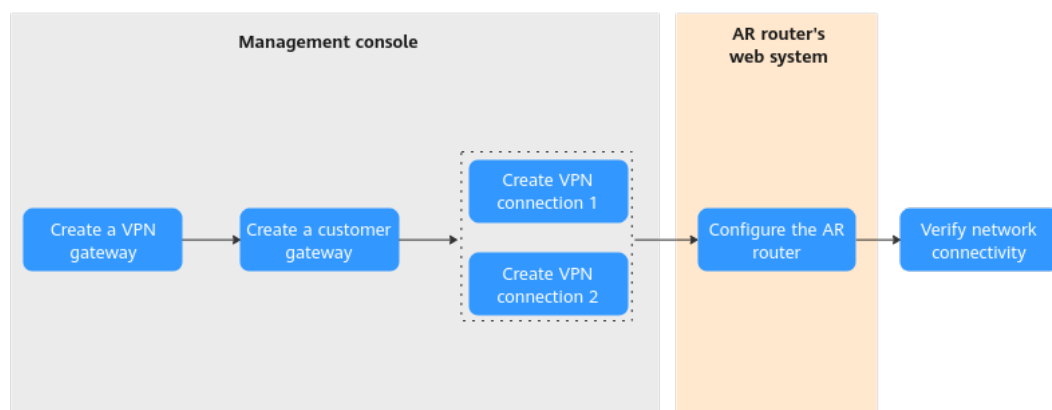


Table 1-8 Operation process description

N o.	Configurat ion Interface	Step	Description
1	Management 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.	<ul style="list-style-type: none">• 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.

1.1.2.2 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.

1. 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.

Table 1-9 Key parameters for creating a VPN gateway

Parameter	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)
Interconnection 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

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.

Table 1-11 Parameter settings for VPN connection 1

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. <ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– Manually specify In this example, Manually specify is selected.– Automatically assign	Manually specify

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.	<ul style="list-style-type: none">- IKE Policy<ul style="list-style-type: none">▪ 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- IPsec Policy<ul style="list-style-type: none">▪ 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.

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](#).

Figure 1-5 Configuring static routes

Advanced > IP > Routing

Routing Table **Static Route Configuration** Dynamic Route Configuration

IPv4 Static Route Configure a static route to the active EIP of the VPN gateway.

Static Route Settings

* Destination IP: 1 . 1 . 1 . 2

* Subnet mask: 255 . 255 . 255 . 252

VPN instance: - none -

Next hop address: 1 . 1 . 1 . 254 Public network gateway 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 **Static Route Configuration** Dynamic Route Configuration

IPv4 Static Route Configure a static route to active EIP 2 of the VPN gateway.

Static Route Settings

* Destination IP: 2 . 2 . 2 . 2

* Subnet mask: 255 . 255 . 255 . 252

VPN instance: - none -

Next hop address: 1 . 1 . 1 . 254 Public network gateway address of the AR router, which is subject to the actual value.

Outbound interface: GigabitEthernet0/0/8 ... X

Priority: 60

Description:

Add

Step 3 Configure tunnel interfaces.

1. Choose **Advanced > Interface > Logical Interface**.
2. 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

Logical Interface Settings

* Interface type: LoopBack Tunnel

* Interface number: 1

* IP address/mask: 169 . 254 . 70 . 1 / 255 . 255 . 255 . 252

Interface description:

Tunnel mode: IPSec

* Source IP: GigabitEthernet0/0/8 ...

Destination IP: 1 . 1 . 1 . 2

VPN instance: - none -

Add

Advanced > Interface > Logical Interface

Logical Interface Settings

* Interface type: LoopBack Tunnel

* Interface number: 2

* IP address/mask: 169 . 254 . 71 . 1 / 255 . 255 . 255 . 252

Interface description:

Tunnel mode: IPSec

* Source IP: GigabitEthernet0/0/8 ...

Destination IP: 2 . 2 . 2 . 2

VPN instance: - none -

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

IPSec policy settings

* IPSec connection name : ar-to-hwvpn-01 * Interface name : Tunnel0/0/1 ...

IKE Parameter setting

IKE version : v1&v2 v1 v2 (V2 is recommended, other IKE version has potential security risks.)

Authentication mode : Pre-shared key RSA signature Pre-shared key :

Authentication algorithm : SHA2-256 Encryption algorithm : AES-128

DH group ID : Group14 Integrity algorithm : HMAC-SHA2-256

IPSec Parameter setting

Security protocol : ESP

ESP authentication algorithm : SHA2-256 ESP encryption algorithm : AES-128

Encapsulation mode : Tunnel mode Transport mode

SHA2 algorithm compatible : ON

Advanced

Local identity type : IP address Name

Remote identity type : IP address Name

Reauthentication interval (s) : 86400

DPD : ON

DPD type : Periodic sending

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-SHA2-256

PFS : Group14

IKE SA duration (s) : 86400

IPSec SA aging mode : Time-based (s) : 3600

Traffic-based (KB) : 1843200 ?

Pre-extraction of original IP packets : OFF

Figure 1-8 Configuring VPN connection 2

IPsec policy settings

* IPsec connection name : ar-to-hwvpn-02 * Interface name : Tunnel0/0/2

IKE Parameter setting

IKE version : v1&v2 v1 v2 (V2 is recommended, other IKE version has potential security risks.)

Authentication mode : Pre-shared key RSA signature Pre-shared key :

Authentication algorithm : SHA2-256 Encryption algorithm : AES-128

DH group ID : Group14 Integrity algorithm : HMAC-SHA2-256

IPsec Parameter setting

Security protocol : ESP

ESP authentication algorithm : SHA2-256 ESP encryption algorithm : AES-128

Encapsulation mode : Tunnel mode Transport mode

SHA2 algorithm compatible : ON

Advanced

Local identity type : IP address Name

Remote identity type : IP address Name

Reauthentication interval (s) : 86400

DPD : ON

DPD type : Periodic sending 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-SHA2-256

PFS : Group14

IKE SA duration (s) : 86400

IPsec SA aging mode : Time-based (s) : 3600

Traffic-based (KB) : 1843200

Pre-extraction of original IP packets : OFF

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 1

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 2

Peer Settings

* Peer IP : 169 . 254 . 71 . 2 * Peer AS number : 64512

Description : Source interface : Tunnel0/0/2

Maximum EBGP connection hop count : 255 Authentication : OFF

Add

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

----End

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.

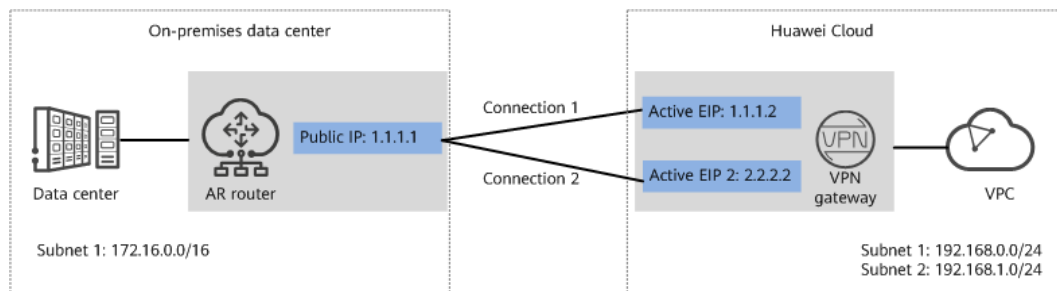
1.1.3 Policy-based Mode

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	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/16	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Active EIP: 1.1.1.2• Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	IKE policy	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

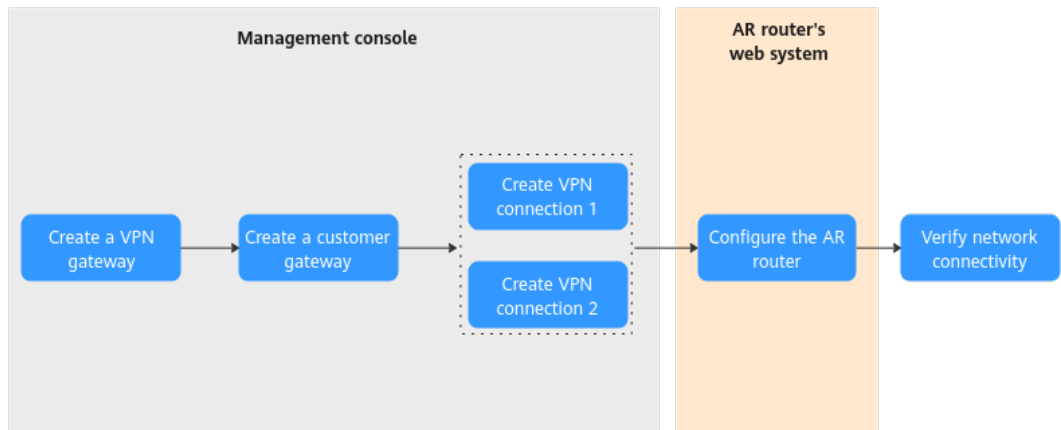


Table 1-14 Operation process description

N o.	Configurat ion Interface	Step	Description
1	Managemen t 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.	<ul style="list-style-type: none"> 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.

1. 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.

Table 1-15 Key parameters for creating a VPN gateway

Parameter	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)
Interconnection 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

Parameter	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.

Table 1-16 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

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.

Table 1-17 Parameter settings for VPN connection 1

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

Parameter	Description	Value
Customer Subnet	<p>Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud.</p> <ul style="list-style-type: none">- 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
PSK, Confirm PSK	<p>The value must be the same as the PSK of the connection configured on the customer gateway device.</p>	<i>Set this parameter based on the site requirements.</i>
Policy	<p>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.</p> <ul style="list-style-type: none">- 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.	<ul style="list-style-type: none">- 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.	<ul style="list-style-type: none">- IKE Policy<ul style="list-style-type: none">▪ 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- IPsec Policy<ul style="list-style-type: none">▪ 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.

Table 1-18 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

----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](#).

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.
- 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.

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.

Figure 1-13 Configuring an advance ACL

The screenshot displays the configuration page for an Advanced ACL. The breadcrumb path is Configuration > Attack Defense > ACL. The 'Advanced ACL' tab is selected, with other tabs being 'Basic ACL', 'Layer 2 ACL', and 'Time Range'. Under 'Rule Settings', the 'Rule number' is 1, 'Action' is 'Permit', and 'ACL Type' is 'IPv4'. The 'Protocol type' is 'IP' and the 'Effective ACL' is 'GE0/0/8'. The 'Matched IP address' section shows 'Source IP/Wildcard' as 172.16.0.0/0.0.255.255 and 'Destination IP/Wildcard' as 192.168.0.0/0.0.255.255. The 'Time range name' is '- none -'. An 'Add' button is at the bottom.

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.

Figure 1-14 Configuring service routes

The figure consists of three screenshots of the 'Static Route Configuration' interface, each showing a different configuration for a static route. The interface is titled 'Advanced > IP > Routing' and has three tabs: 'Routing Table', 'Static Route Configuration', and 'Dynamic Route Configuration'. The 'Static Route Configuration' tab is active, and the 'IPv4 Static Route' option is selected. A red note above the configuration fields reads: 'Configure a static route to the active EIP of the VPN gateway.' The configuration fields are as follows:

- Destination IP:** 1 . 1 . 1 . 2
- Subnet mask:** 255 . 255 . 255 . 252
- VPN instance:** - none -
- Next hop address:** 1 . 1 . 1 . 254
- Priority:** 60
- Outbound interface:** GigabitEthernet0/0/8
- Description:** (empty)

A red note next to the 'Next hop address' field reads: 'Public network gateway address of the AR router, which is subject to the actual value.' An 'Add' button is located at the bottom of the configuration area.

The second screenshot shows the same configuration but with the 'Destination IP' set to 2 . 2 . 2 . 2 and the 'Subnet mask' set to 255 . 255 . 255 . 252.

The third screenshot shows the same configuration but with the 'Destination IP' set to 192 . 168 . 0 . 0 and the 'Subnet mask' set to 255 . 255 . 0 . 0.

----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 S2C Classic VPN

2.1 Overview

This guide helps you configure your local VPN device to implement interconnection between your network and a VPC subnet.

A VPN connection connects your data center or network to your VPC. A customer gateway can be a physical or software device.

- [Huawei USG6600 Series](#)
- [Configuring VPN When Fortinet FortiGate Firewall Is Used](#)
- [Configuring VPN When Sangfor Firewall Is Used](#)
- [Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication](#)
- [Using Openswan to Configure On- and Off-Cloud Communication](#)
- [Using strongSwan to Configure On- and Off-Cloud Communication](#)

2.2 Huawei USG6600 Series

This section uses a Huawei USG6600 series firewall running V100R001C30SPC300 as an example to describe how to configure VPN.

Assume that the subnets of the data center are 192.168.3.0/24 and 192.168.4.0/24, the subnets of the VPC are 192.168.1.0/24 and 192.168.2.0/24, and the public IP address of the IPsec tunnel egress in the VPC is 1.1.1.1, which can be obtained from the local gateway parameters of the IPsec VPN in the VPC.

Procedure

1. Log in to the CLI of the firewall.
2. Check firewall version information.

```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300(VRP (R) Software, Version 5.30)
```

3. Create an access control list (ACL) and bind it to the target VPN instance.

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```

4. Create an IKE proposal.

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. Create an IKE peer and bind it to the created IKE proposal. The peer IP address is 1.1.1.1.

```
ike peer vpnikepeer_64
pre-shared-key ***** (***** specifies the pre-shared key.)
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```

6. Create an IPsec proposal.

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. Create an IPsec policy, and bind the IKE policy and IPsec proposal to it.

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address xx.xx.xx.xx
q
```

8. Apply the IPsec policy to the corresponding sub-interface.

```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. Test the connectivity.

After you perform the preceding operations, you can test the connectivity between your ECSs in the cloud and the hosts in your data center. For details, see the following figure.

```
root@i-psiwbqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiwbqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

2.3 Configuring VPN When Fortinet FortiGate Firewall Is Used

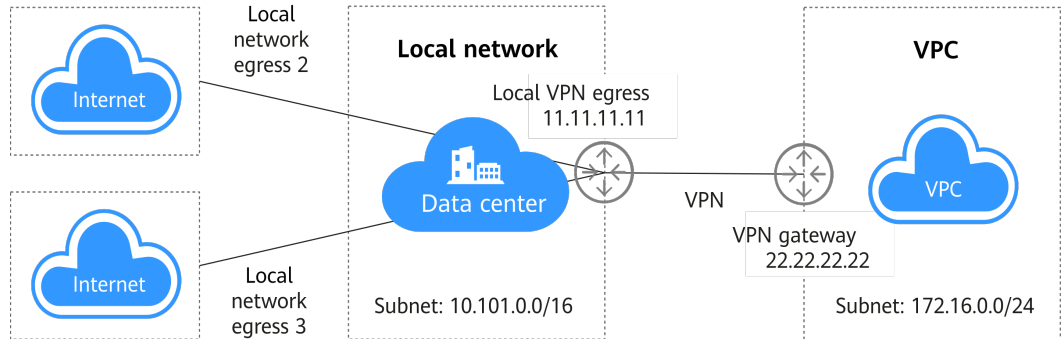
Scenarios

This section describes how to purchase a VPN gateway and create VPN connections on HUAWEI CLOUD to connect your on-premises network to a VPC subnet if your local data center uses FortiGate firewalls as Internet egresses.

Topology Connection

As shown in [Figure 2-1](#), the local data center has multiple Internet egresses. The egress 11.11.11.11 is specified to establish a VPN connection with a HUAWEI CLOUD VPC. The subnet of the local data center is 10.10.0.0/16, and the VPC subnet on HUAWEI CLOUD is 172.16.0.0/24. The IP address of the VPN gateway you purchased on HUAWEI CLOUD is 22.22.22.22. Create a VPN connection to connect your on-premises network to the VPC subnet.

Figure 2-1 Multi-egress on-premises network connecting to a VPC through a VPN



Configure the VPN connection policies on HUAWEI CLOUD based on [Figure 2-2](#).

Figure 2-2 Policy details

Policy Details

IKE Policy			
Authentication Algorithm	SHA1	Version	v1
Encryption Algorithm	AES-128	Lifecycle (s)	86400
DH Algorithm	Group 5	Negotiation Mode	Main

IPsec Policy			
Authentication Algorithm	SHA1	Transfer Protocol	ESP
Encryption Algorithm	AES-128	Lifecycle (s)	3600
PFS	DH group 5		

Close

Configuration Procedure

This example describes how to configure a VPN when a FortiGate firewall is used in your local data center.

Step 1 Configure IPsec VPN.

1. Create a tunnel.
2. Configure the basic information for the tunnel.
3. Configure IKE phase 1 parameters.
4. Configure IPsec phase 2 parameters.
5. Configure the IPsec tunnel.

Step 2 Configure routes.

1. Add a static route.
Add a route to the cloud VPC subnet 172.16.0.0/24, with the outbound interface being the VPN tunnel interface.
2. Configure policy-based routes for multiple egresses.
Set the source address to the subnet of the local data center and the destination address to the subnet of the VPC. Adjust the configuration sequence of the policy-based routes to ensure that the policy-based routes will be preferentially used.

Step 3 Configure policies and NAT.

1. Configure a policy for access to the cloud from the local data center.
2. Configure a policy for access to the local data center from the cloud.

----End

Configuration Verification

1. Check whether the on-premises VPN status is normal.
2. Check whether the cloud-based VPN status is normal.

Configuration Using the CLI

1. Configure the physical interface.

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 11.11.11.11 255.255.255.0
    set type physical
  next
  edit "IPsec" //Tunnel interface configuration
    set vdom "root"
    set type tunnel
    set interface "port1" //Physical interface bound to the tunnel
    next
  end
```

2. Configure interface zones.

```
config system zone
  edit "trust"
    set intrazone allow
    set interface "A1"
  next
  edit "untrust"
    set intrazone allow
    set interface "port1 "
  next
end
```

3. Configure subnets.

```
config firewall address
  edit "hw-172.16.0.0/24"
    set uuid f612b4bc-5487-51e9-e755-08456712a7a0
    set subnet 172.16.0.0 255.255.255.0 //Subnet on the cloud
  next
  edit "local-10.10.0.0/16"
    set uuid 9f268868-5489-45e9-d409-5abc9a946c0c
    set subnet 10.10.0.0 255.255.0.0 //Subnet of the local data center
  next
```

4. Configure IPsec.

```
config vpn IPsec phase1-interface //Phase 1 configuration
  edit "IPsec"
```

```
set interface "port1"
set natTraversal disable
set proposal aes128-sha1
set comments "IPsec"
set dhgrp 5
set remote-gw 22.22.22.22
set psksecret ENC dmFyLzF4tRrIjV3T
+ISzhQeU2nGEoYKC31NaYRWFJl8krlwNmZX5SfwUi5W5RLJqFu82VYKYsXp5+HZJ13VYY8O2Sn/
vruzdLxqu84zbHEIQkTlf5n/
63KEru1rRoNiHDTWfh3A3ep3fKJmxf43pQ7OD64t151ol06FMjUBLHgj1ep9d32Q0F3foUxfDQs21Bi9RA
==
next
end
config vpn IPsec phase2-interface //Phase 2 configuration
edit "IP-TEST"
set phase1name "IPsec "
set proposal aes128-sha1
set dhgrp 5
set keylifeseconds 3600
set src-subnet 10.10.0.0 255.255.0.0
set dst-subnet 172.16.0.0 255.255.255.0
next
end
```

5. Configure access policies.

```
config firewall policy
edit 15 //Policy 15 is used to access the on-premises data center
from the cloud. NAT is disabled.
set uuid 4f452870-ddb2-51e5-35c9-38a987ebdb6c
set srcintf "IPsec"
set dstintf "trust"
set srcaddr "hw-172.16.0.0/24"
set dstaddr "local-10.10.0.0/16"
set action accept
set schedule "always"
set service "ALL"
set logtraffic all
next
edit 29 //Policy 29 is used to access the cloud from the on-premises
data center. NAT is disabled.
set uuid c2d0ec77-5254-51e9-80dc-2813ccf51463
set srcintf "trust"
set dstintf "IPsec"
set srcaddr "local-10.10.0.0/16"
set dstaddr "hw-172.16.0.0/24"
set action accept
set schedule "always"
set service "ALL"
set logtraffic all
next
```

6. Configure routes.

```
config router static
edit 24 //Route 24 is a static route that is used to access on the cloud.
set dst 172.16.0.0 255.255.255.0
set gateway 11.11.11.1
set distance 10
set device "port1"
config router policy
edit 2 //Policy-based route 2 is used to access the cloud from the on-premises data
center.
set input-device "A1"
set src "10.10.0.0/255.255.0.0"
set dst "172.16.0.0/255.255.255.0"
set gateway 11.11.11.1
set output-device "port1"
```

2.4 Configuring VPN When Sangfor Firewall Is Used

Scenarios

Your local data center uses Sangfor firewalls as Internet egresses. An IPsec VPN device is connected to the DMZ zone and needs to access the HUAWEI CLOUD network through a VPN connection.

Topology Connection

Topology connection mode:

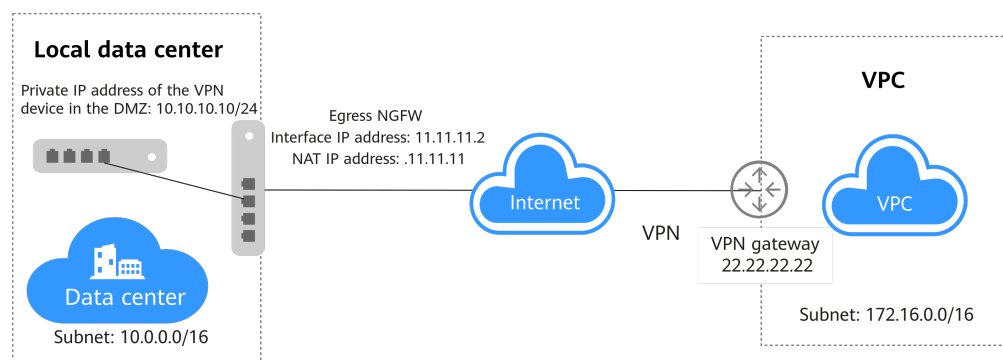
- Use the firewall to establish a VPN connection with the cloud.
- Use the VPN device in the DMZ zone and the NAT traversal technique to establish a VPN connection with the cloud.

The configuration details are as follows.

- Private IP address of the VPN device in the local data center: 10.10.10.10/24
- On-premises subnet: 10.0.0.0/16
- IP address of the next-generation firewall: 11.11.11.2/24; Public network gateway: 11.11.11.1; NAT IP address of the VPN device: 11.11.11.11
- IP address of the VPN gateway on the cloud: 22.22.22.22; Subnet on the cloud: 172.16.0.0/16

Create a VPN connection to connect an on-premises network to the VPC subnet.

Figure 2-3 Using a VPN to Connect a VPC with a local data center that uses Sangfor firewall and the NAT traversal technique



Configure the VPN connection on HUAWEI CLOUD based on [Figure 2-4](#). If the VPN device in the DMZ zone uses NAT traversal, the aggressive negotiation mode should be used. If a firewall is used, the main negotiation mode should be used.

Figure 2-4 Policy details on HUAWEI CLOUD

Policy Details			
IKE Policy			
Authentication Algorithm	SHA1	Version	v1
Encryption Algorithm	AES-128	Lifecycle (s)	86400
DH Algorithm	Group 5	Negotiation Mode	Aggressive
IPsec Policy			
Authentication Algorithm	SHA1	Transfer Protocol	ESP
Encryption Algorithm	AES-128	Lifecycle (s)	3600
PFS	DH group 5		

[Close](#)

Configuration Procedure

This example describes how to configure a VPN when a Sangfor firewall is used in your local data center.

Step 1 Configure IPsec VPN.

1. **Configure IKE phase 1 parameters.**
2. **Configure IPsec phase 2 parameters.**
3. **Configure security parameters.**

Step 2 Configure routes.

Step 3 Configure policies and NAT.

----End

Configuration Verification

Check whether the on-premises subnet can communicate with the subnet on the cloud.

2.5 Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication

Scenarios

This section describes how to use TheGreenBow IPsec VPN Client to establish a VPN connection between a VPC and a cloud desktop or between two VPCs.

The following describes the configuration details if TheGreenBow IPsec VPN Client is used.

- **Scenario 1: Install the client on the cloud desktop that connects to the VPN gateway of the VPC.**
 - a. The cloud desktop must run the Windows OS.
 - b. The cloud desktop can ping the VPN gateway IP address of the VPC. (If the ping fails, the VPN connection cannot be established.)
- **Scenario 2: Install the client on the ECS in VPC1 that connects to the VPN gateway of VPC2.**
 - a. Windows ECS in VPC1 has EIP.
 - b. The ECS in VPC1 can ping the VPN gateway IP address of VPC2. (If the ping fails, the VPN connection cannot be established.)

Prerequisites

- **Scenario 1: Cloud desktop + VPC**
 - The VPC, subnet, and ECS have been configured on the cloud.
 - The VPN gateway and VPN connection on the cloud have been configured.

Figure 2-5 Policy details

Policy Details

IKE Policy			
Authentication Algorithm	SHA1	Version	v1
Encryption Algorithm	AES-128	Lifecycle (s)	86400
DH Algorithm	Group 5	Negotiation Mode	Main

IPsec Policy			
Authentication Algorithm	SHA1	Transfer Protocol	ESP
Encryption Algorithm	AES-128	Lifecycle (s)	3600
PFS	DH group 5		

Close

- TheGreenBow IPsec VPN Client has been installed on the cloud desktop.
- The cloud desktop can ping the IP address of the VPN gateway.
- **Scenario 2: VPC + VPC**
 - The VPCs, subnets, and ECSs in two regions have been configured. The ECS in VPC2 runs the Windows OS.
 - The VPN gateway and VPN connection in VPC1 have been configured.

Figure 2-6 Policy details

Policy Details			
IKE Policy			
Authentication Algorithm	SHA1	Version	v1
Encryption Algorithm	AES-128	Lifecycle (s)	86400
DH Algorithm	Group 5	Negotiation Mode	Main
IPsec Policy			
Authentication Algorithm	SHA1	Transfer Protocol	ESP
Encryption Algorithm	AES-128	Lifecycle (s)	3600
PFS	DH group 5		

Close

- TheGreenBow IPsec VPN Client has been installed on the Windows ECS in VPC2.
- The ECS in VPC2 can ping the VPN gateway IP address of VPC1.

NOTE

Use the default VPN configurations on HUAWEI CLOUD.

Configuration Procedure

Scenario 1: Client configuration in the "cloud desktop + VPC" scenario

1. Configure global parameters.
2. Configure IKE phase 1 parameters.
3. Configure IPsec phase 2 parameters.

Scenario 2: Client configuration in the "VPC + VPC" scenario

1. Configure global parameters.
2. Configure IKE phase 1 parameters.
3. Configure IPsec phase 2 parameters.

Configuration Verification

- **Scenario 1: Cloud desktop + VPC**

Check whether the cloud desktop and the ECS in the VPC can communicate with each other.

- a. Check whether the VPN connection is successfully established.
- b. Check the VPN connection status of the VPC.
- c. Check the network configurations of the cloud desktop.
- d. Ping the ECS in the VPC from the cloud desktop.
- e. Ping the cloud desktop from the ECS in the VPC.

The cloud desktop and the ECS in the VPC can communicate with each other successfully.

- **Scenario 2: VPC + VPC**

Check whether the ECS in VPC1 and the ECS installed with the client in VPC2 can communicate with each other.

The ECS in VPC1 and the ECS installed with the client in VPC2 can communicate with each other successfully.

2.6 Using Openswan to Configure On- and Off-Cloud Communication

Scenarios

The VPC on the cloud has VPN gateways and VPN connections. Servers in customer data center are installed with the IPsec software to interconnect with the cloud. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.

Topology Connection

Figure 2-7 shows the topology connection and policy negotiation configurations.

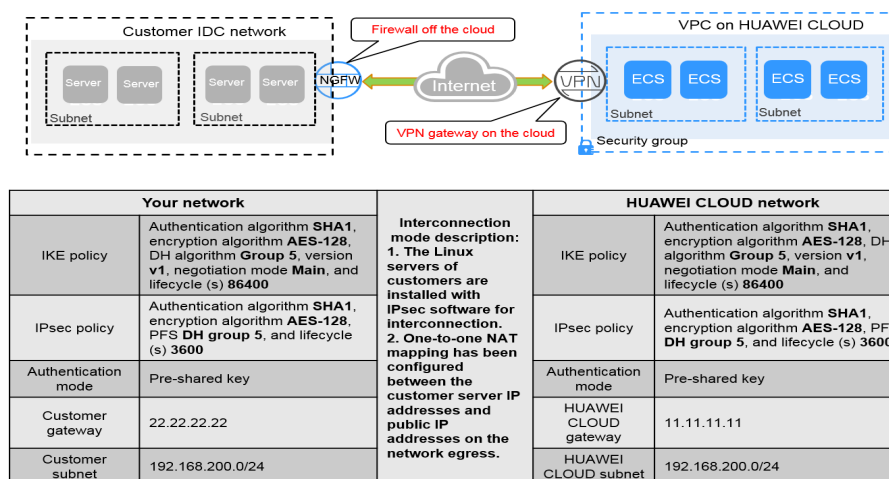
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

The NAT mapping IP address of the customer server is 22.22.22.22 and the local subnet is 192.168.222.0/24.

The ECS IP address and the customer server IP address are 192.168.200.200 and 192.168.222.222, respectively.

The negotiation parameters of the VPN connection use the default configurations defined on Huawei Cloud.

Figure 2-7 Topology connection and policy negotiation configuration information



Configuration Procedure

In this example, the Openswan IPsec client is installed on CentOS 6.8.

Step 1 Install the Openswan client.

```
yum install -y openswan
```

Step 2 Enable IPv4 forwarding.

```
vim /etc/sysctl.conf
```

1. Add the following content to this file:
net.ipv4.ip_forward = 1
2. Run the `/sbin/sysctl -p` command for the forwarding configuration to take effect.

Step 3 Configure iptables.

Run the `iptables -L` command to check whether the firewall is disabled or the data flow forwarding is allowed.

```
iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Step 4 Configure the pre-shared key.

```
vim /etc/ipsec.d/open_IPsec.secrets
```

Add the following content to this file:

```
22.22.22.22 11.11.11.11 : psk "IPsec-key"
```

Format: IP address for connection+Space+Customer gateway IP address+Space+English colon (:)+Space+PSK (case insensitive)+Pre-shared key. There are spaces on both sides of the colon. The key is enclosed in double quotation marks.

Step 5 Configure the IPsec connection.

```
vim /etc/ipsec.d/open_IPsec.conf
```

Add the following content to this file:

```
conn openswan_IPsec          # Set the connection name to openswan_IPsec.
type=tunnel                  # Enable the tunnel mode.
auto=start                   # The value can be add, route, or start.

left=192.168.222.222          # Set the local IP address. The value must be the actual host IP address in
the NAT scenario.
leftid=22.22.22.22           # Set the local ID.
leftsourceip=22.22.22.22     # In the NAT scenario, enter the post-NAT public IP address.
leftsubnet=192.168.222.0/24  # Set the local subnet.
leftnexthop=22.22.22.1       # In the NAT scenario, enter the post-NAT gateway IP address.
right=11.11.11.11            # Set the VPN gateway IP address.
rightid=11.11.11.11         # Set the ID of the VPN gateway.
rightsourceip=11.11.11.11   # Set the VPN gateway IP address.
rightsubnet=192.168.200.0/24 # Set the subnet of the VPN gateway.
rightnexthop=%defaultroute   # Set the default route.

authby=secret                # Set the authentication mode to PSK.
keyexchange=ike              # Set the IKE key exchange mode.
ike=aes128-sha1;modp1536     # Define the IKE algorithm and group based on the configuration of
the VPN gateway.
ikev2=never                  # Disable the IKEv2 version.
ikelifetime=86400s          # Set the lifetime of IKE SAs.

phase2=esp                   # Set the data transmission format in phase 2.
phase2alg=aes128-sha1;modp1536 # Set the algorithm and group in the IPsec policy based on the
```



```
configuration of the VPN gateway.
pfs=yes                # Enable PFS.
compress=no           # Disable compression.
salifetime=3600s      # Set the lifetime of SAs in phase 2.
```

NOTE

- In NAT traversal scenarios, you can set **forceencaps** to yes as required.
- For details about the bits of DH groups used by Huawei Cloud VPN, see [What Are the Bits of the DH Groups Used by Huawei Cloud VPN?](#)

After the configuration is complete, run the **ipsec verify** command to verify the configuration items. If **OK** is displayed for all items in the command output, the configuration is successful.

```
ipsec verify
Verifying installed system and configuration files
Version check and IPsec on-path [OK]
Libreswan 3.25 (netkey) on 3.10.0-957.5.1.el7.x86_64
Checking for IPsec support in kernel [OK]
NETKEY: Testing XFRM related proc values
  ICMP default/send_redirects [OK]
  ICMP default/accept_redirects [OK]
  XFRM larval drop [OK]
Pluto IPsec.conf syntax [OK]
Two or more interfaces found, checking IP forwarding[OK]
Checking rp_filter [OK]
Checking that pluto is running [OK]
Pluto listening for IKE on udp 500 [OK]
Pluto listening for IKE/NAT-T on udp 4500 [OK]
Pluto IPsec.secret syntax [OK]
Checking 'ip' command [OK]
Checking 'iptables' command [OK]
Checking 'prelink' command does not interfere with FIPS[OK]
Checking for obsolete IPsec.conf options [OK]
```

If the following information is displayed, the configuration fails:

```
Checking rp_filter [ENABLED]
/proc/sys/net/ipv4/conf/default/rp_filter [ENABLED]
/proc/sys/net/ipv4/conf/lo/rp_filter [ENABLED]
/proc/sys/net/ipv4/conf/eth0/rp_filter [ENABLED]
/proc/sys/net/ipv4/conf/eth1/rp_filter [ENABLED]
/proc/sys/net/ipv4/conf/ip_vti01/rp_filter [ENABLED]
```

To rectify the fault, run the following commands:

```
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/lo/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/ip_vti01/rp_filter
```

Step 6 Start the service.

service ipsec stop # Stop the service.

service ipsec start # Start the service.

service ipsec restart # Restart the service.

ipsec auto --down openswan_IPsec # Disable the connection.

ipsec auto --up openswan_IPsec # Enable the connection.

 NOTE

Restart the service and enable the connection after each modification.

----End

Configuration Verification

Run the `ipsec --status` command to query the IPsec status. Information (extract) similar to the following is displayed.

```
Connection list:
000
000 "openswan_IPsec":
192.168.222.0/24===192.168.222.222<192.168.222.222>[22.22.22.22]---22.22.22.1...11.11.11.11<11.11.11.11>
===192.168.200.0/24; erouted; eroute owner: #30
000 "openswan_IPsec":   oriented; my_ip=22.22.22.22; their_ip=11.11.11.11; my_updown=IPsec_updown;
000 "openswan_IPsec":   xauth us:none, xauth them:none, my_username=[any]; their_username=[any]
000 "openswan_IPsec":   our_auth:secret, their_auth:secret
000 "openswan_IPsec":   modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset,
banner:unset, cat:unset;
000 "openswan_IPsec":   labeled_IPsec:no;
000 "openswan_IPsec":   policy_label:unset;
000 "openswan_IPsec":   ike_life: 86400s; IPsec_life: 3600s; replay_window: 32; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 0;
000 "openswan_IPsec":   retransmit-interval: 500ms; retransmit-timeout: 60s;
000 "openswan_IPsec":   initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-
esp-tfc:no;
000 "openswan_IPsec":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1_ALLOW+SAREF_TRACK
+IKE_FRAG_ALLOW+ESN_NO;
000 "openswan_IPsec":   conn_prio: 24,24; interface: eth0; metric: 0; mtu: unset; sa_prio:auto; sa_tfc:none;
000 "openswan_IPsec":   nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-
offload:auto;
000 "openswan_IPsec":   our_idtype: ID_IPV4_ADDR; our_id=1.1.1.1; their_idtype: ID_IPV4_ADDR; their
id=2.2.2.2
000 "openswan_IPsec":   dpd: action:hold; delay:0; timeout:0; nat-t: encaps:auto; nat_keepalive:yes;
ikev1_natt:both
000 "openswan_IPsec":   newest ISAKMP SA: #3; newest IPsec SA: #30;
000 "openswan_IPsec":   IKE algorithms: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   IKE algorithm newest: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   ESP algorithms: AES_CBC_128-HMAC_SHA1_96-MODP1536
000 "openswan_IPsec":   ESP algorithm newest: AES_CBC_128-HMAC_SHA1_96; pfsgroup=MODP1536
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #3: "openswan_IPsec":4500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE
in 15087s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #30: "openswan_IPsec":4500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in
1744s; newest IPsec; eroute owner; isakmp#3; idle; import:admin initiate
000 #30: "openswan_IPsec" esp.b810a24@11.11.11.11 esp.aab7b496@192.168.222.222 tun.0@11.11.11.11
tun.0@192.168.222.222 ref=0 rehim=0 Traffic: ESPin=106KB ESPout=106KB! ESPmax
=4194303B
```

2.7 Using strongSwan to Configure On- and Off-Cloud Communication

Scenarios

The VPC on the cloud has VPN gateways and VPN connections. Servers in customer data center are installed with the IPsec software to interconnect with

the cloud. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.

Topology Connection

Figure 2-8 shows the topology connection and policy negotiation configurations.

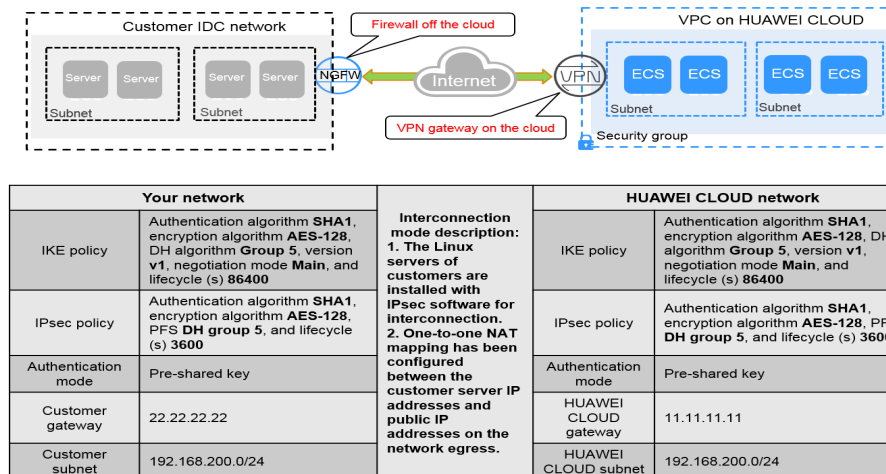
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

The NAT mapping IP address of the customer server is 22.22.22.22 and the local subnet is 192.168.222.0/24.

The ECS IP address and the customer server IP address are 192.168.200.200 and 192.168.222.222, respectively.

The negotiation parameters of the VPN connection use the default configurations defined on Huawei Cloud.

Figure 2-8 Topology connection and policy negotiation configuration information



Configuration Procedure

The configurations may vary according to the strongSwan version. The following uses strongSwan 5.7.2 as an example to describe the VPN configurations of strongSwan in the Linux system.

Step 1 Install the IPsec VPN client.

yum install strongswan

During the installation, select **Y**. The installation is complete when the message "Complete!" is displayed. The configuration files of strongSwan are stored in the `/etc/strongswan` directory. During the configuration, you only need to edit the `ipsec.conf` and `ipsec.secrets` files.

Step 2 Enable IPv4 forwarding.

vim /etc/sysctl.conf

1. Add the following content to this file:

```
net.ipv4.ip_forward = 1
```

2. Run the `/sbin/sysctl -p` command for the forwarding configuration to take effect.

Step 3 Configure iptables.

Run the `iptables -L` command to check whether the firewall is disabled or the data flow forwarding is allowed.

```
iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Step 4 Configure the pre-shared key.

```
vim /etc/strongswan/ipsec.secrets # Edit the ipsec.secrets file.
22.22.22.22 11.11.11.11 : PSK "ipsec-key"
```

Format: IP address for connection+Space+Customer gateway IP address+Space+English colon (:)+Space+PSK (uppercase)+Pre-shared key. There are spaces on both sides of the colon. The key is enclosed in double quotation marks.

Step 5 Configure the IPsec connection.

`vim /etc/strongswan/ipsec.conf`

Add the following content to this file:

```
config setup
conn strong_ipsec # Set the connection name to strong_ipsec.
auto=route # The value can be add, route, or start.
type=tunnel # Enable the tunnel mode.
compress=no # Disable compression.
leftauth=psk # Set the local authentication mode to PSK.
rightauth=psk # Set the remote authentication mode to PSK.
ikelifetime=86400s # Set the lifetime of IKE SAs.
lifetime=3600s # Set the lifetime of IPsec SAs.
keyexchange=ikev1 # Set the IKE version to version 1.
ike=aes128-sha1-modp1536! # Set the algorithm and DH group in the IKE policy based on
the configuration of the VPN gateway.
esp=aes128-sha1-modp1536! # Set the algorithm and DH group in the IPsec policy based on
the configuration of the VPN gateway.
leftid=22.22.22.22 # Set the local ID.
left=192.168.222.222 # Set the local IP address. The value must be the actual host IP
address in the NAT scenario.
leftsubnet=192.168.222.0/24 # Set the local subnet.
rightid=11.11.11.11 # Set the ID of the VPN gateway.
right=11.11.11.11 # Set the VPN gateway IP address.
rightsubnet=192.168.200.0/24 # Set the subnet of the VPN gateway.
```

NOTE

For details about the bits of DH groups used by Huawei Cloud VPN, see [What Are the Bits of the DH Groups Used by Huawei Cloud VPN?](#).

Step 6 Start the service.

`service strongswan stop` # Stop the service.

`service strongswan start` # Start the service.

`service strongswan restart` # Restart the service.

`strongswan stop` # Disable the connection.

strongswan start # Enable the connection.

 **NOTE**

Restart the service and enable the connection after each modification.

----End

Configuration Verification

Run the **strongswan statusall** command to query the connection start time.

```
Status of IKE charon daemon (strongSwan 5.7.2, Linux 3.10.0-957.5.1.el7.x86_64, x86_64):
  uptime: 5 minutes, since Apr 24 19:25:29 2019
  malloc: sbrk 1720320, mmap 0, used 593088, free 1127232
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 1
  loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha2 sha1 md4 md5 mgf1 random nonce x509
  revocation constra
  ints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519
  chapoly x
  cbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-
  identity ea
  p-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-
  tls eap-ttls eap
  -peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp led duplicheck unity counters
  Listening IP addresses:192.168.222.222
  Connections:
  strong_ipsec: 192.168.222.222...11.11.11.11 IKEv1
  strong_ipsec: local: [22.22.22.22] uses pre-shared key authentication
  strong_ipsec: remote: [11.11.11.11] uses pre-shared key authentication
  strong_ipsec: child: 192.168.222.0/24 === 192.168.200.0/24 TUNNEL
  Routed Connections:
  strong_ipsec{1}: ROUTED, TUNNEL, reqid 1
  strong_ipsec{1}: 192.168.222.0/24 === 192.168.200.0/24
  Security Associations (0 up, 1 connecting):
  strong_ipsec[1]: CONNECTING, 192.168.222.222[%any]...11.11.11.11[%any]
  strong_ipsec[1]: IKEv1 SPIs: c3090f6512ec6b7d_i* 0000000000000000_r
  strong_ipsec[1]: Tasks queued: QUICK_MODE QUICK_MODE
  strong_ipsec[1]: Tasks active: ISAKMP_VENDOR ISAKMP_CERT_PRE MAIN_MODE ISAKMP_CERT_POST
  ISAKMP_NATD
```

Ping the server with the IPsec client installed in VPC 2 from VPC 1.

```
ping 192.168.222.222
PING 192.168.222.222 (192.168.222.222) 56(84) bytes of data.
 64 bytes from 192.168.222.222: icmp_seq=1 ttl=62 time=3.07 ms
 64 bytes from 192.168.222.222: icmp_seq=2 ttl=62 time=3.06 ms
 64 bytes from 192.168.222.222: icmp_seq=3 ttl=62 time=3.98 ms
 64 bytes from 192.168.222.222: icmp_seq=4 ttl=62 time=3.04 ms
 64 bytes from 192.168.222.222: icmp_seq=5 ttl=62 time=3.11 ms
 64 bytes from 192.168.222.222: icmp_seq=6 ttl=62 time=3.71 ms
```

3 P2C VPN

3.1 Using the CCM to Manage a Server Certificate

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  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 3-1 describes the parameters for uploading a certificate.

Table 3-1 Parameters for uploading an international standard 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.

Parameter	Description
Certificate File	<p>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.</p> <p>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.</p> <p>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).</p> <p>For the format of the certificate file content to be uploaded, see Figure 3-1.</p>
Private Key	<p>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.</p> <p>You only need to upload the private key of the server certificate.</p> <p>For the format of the private key content to be uploaded, see Figure 3-1.</p>

Figure 3-1 Format of the certificate content to be uploaded

```
* Certificate File
Upload
-----BEGIN CERTIFICATE-----
+01fG82xmnj0ZkE6bQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
9z3BpmtjJ5fgf7ufUg/Npv6Tpu5l
-----END CERTIFICATE-----

* Private Key
Upload
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQDWkrvw9dofJLcEA
-----END PRIVATE KEY-----
```

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

3.2 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		
EasyRSA-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
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.
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 './easysrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell
#
```

6. Run the **./easysrsa 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:
```


- 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.

3.3 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.



File Name	Size	Date
EasyRSA-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
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.
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. 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:
* 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_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:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - server/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 - 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
#
```



```
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.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 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.

3.4 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. [Download a root certificate.](#)
 - 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-----
-----BEGIN 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. [Download the SSL certificate.](#)