Virtual Private Network

Administrator Guide

Issue	01
Date	2023-10-20

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.

Contents

1 Interconnection with a Huawei AR Router (Active-Active Connections)

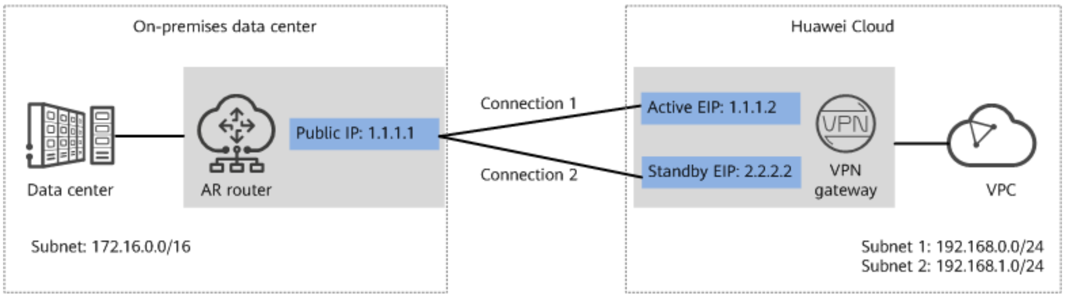
1.1 Static Routing Mode

1.1.1 Operation Guide

Scenario

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

Figure 1-1 Typical networking diagram



In this scenario, the AR router has only one public IP address. VPN connections need to be created between the public IP address of the firewall and the active and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	● 192.168.0.0/24 ● 192.168.1.0/24
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Standby EIP: 2.2.2.2
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
AR router	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 1.1.1.1
	Tunnel interface address	● VPN connection 1: 169.254.70.1/30 ● VPN connection 2: 169.254.71.1/30
IKE and IPsec policies	PSK	Test@123

Category	Item	Data
	IKE policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: DH Group 14 ● IKE version: IKEv2 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● PFS: DH Group 14 ● Transfer protocol: ESP ● Lifetime (s): 3600

Operation Process

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

Figure 1-2 Operation process

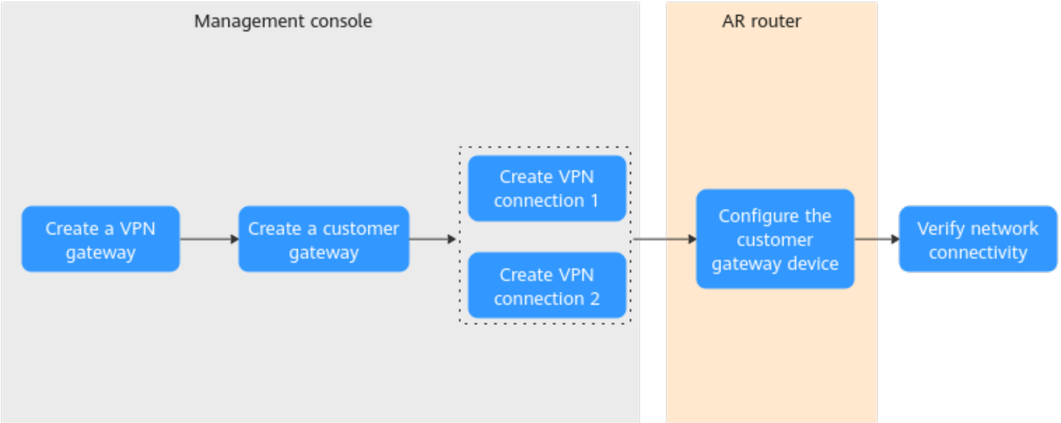


Table 1-2 Operation process description

No.	Configuration 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.

No.	Configuration Interface	Step	Description
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 the standby EIP of the VPN gateway and the customer gateway. It is recommended that the routing mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	CLI of the AR router	**Configuration on the AR Router**	● The local and remote interface addresses configured on the AR router must be the same as the customer and local interface addresses configured on the VPN console. ● The routing mode, PSK, IKE policy, and IPsec policy settings on the AR router must be same as those of VPN connections.
6	-	**Verification**	Run the **ping** command to verify network connectivity.

1.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Create a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.
2. Set parameters as prompted.

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

Table 1-3 VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
Network Type	– **Public network**: A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet. – **Private network**: A VPN gateway communicates with a customer gateway in an on-premises data center through a private network.	Public network
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0.0/16)
Local Subnet	VPC subnets that the on-premises data center needs to access.	192.168.0.0/24,192.168.1.0/24
Interconnection Subnet	Subnet used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Create a customer gateway, that is, an AR router.

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

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

Table 1-4 Customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar
Routing Mode	Select **Static**.	Static
Gateway IP Address	Public IP address of the AR router.	1.1.1.1

Step 5 Create VPN connections.

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

   Table 1-5 only describes the key 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
VPN Type	Select **Static routing**.	Static routing
Customer Gateway	Name of a customer gateway.	cgw-ar
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Interface IP Address	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Interface IP Address	Tunnel IP address of the AR router.	169.254.70.1/30
Routing Mode	Select **Static**.	Static

Parameter	Description	Value
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the AR router.	Test@123
Policy Settings	The policy settings must be the same as those on the AR router.	Default

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 1-6 Parameter settings for VPN connection 2

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

----End

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 and standby EIPs 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 and standby EIPs 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 or standby EIP 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 the standby EIP 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 or standby EIP 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 the standby EIP of the VPN gateway belongs.
- **destination-address**: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 13 Configure association between the static route and NQA.

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

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

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

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

The parameters are described as follows:

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

  In this example, the two VPN connections work in active/standby 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 commands.

----End

1.1.4 Verification

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

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Available**.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.