Virtual Private Network

Best Practices

Issue	01
Date	2023-10-11

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active-Active Mode)

1.1 Overview

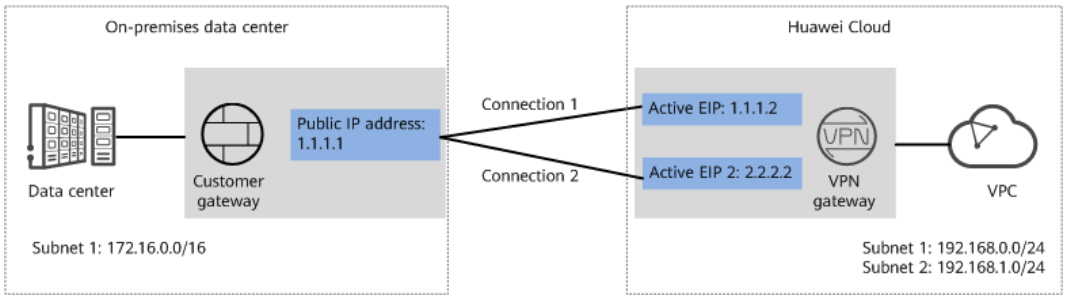
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 1-1 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
- Active-active VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.2 Planning Networks and Resources

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
	HA mode	Active-active
	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 • Active EIP 2: 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: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30

Category	Item	Data
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	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: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Version: v2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

1.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

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

Step 3 Configure a VPN gateway.

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

   Table 1-2 only describes the key parameters for creating a VPN gateway.

Table 1-2 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0.0/16)
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
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2

Parameter	Description	Value
Active EIP 2	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

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

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

Table 1-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 1-4 only describes the key parameters for creating a VPN connection.

Table 1-4 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-fw
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface IP Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface IP Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
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.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	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 1-5 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 IP Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface IP Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

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 subnet can ping each other.

2 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active/Standby Mode)

2.1 Overview

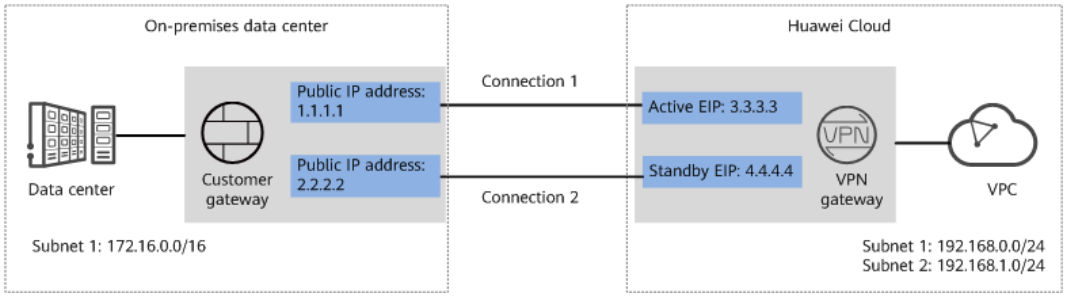
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections working in active/standby mode are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 2-1 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.

- Active and standby VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

2.2 Planning Networks and Resources

Data Plan

Table 2-1 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
	HA mode	Active-standby
	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: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30

Category	Item	Data
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	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: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Version: v2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

2.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

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

Step 3 Configure a VPN gateway.

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

   Table 2-2 only describes the key parameters for creating a VPN gateway.

Table 2-2 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0.0/16)
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
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-standby**.	Active-standby
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2

Parameter	Description	Value
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

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

   Table 2-3 only describes the key parameters for creating a customer gateway.

Table 2-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 2-4 only describes the key parameters for creating a VPN connection.

Table 2-4 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-fw
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface IP Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface IP Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
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.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	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 2-5 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 Tunnel Interface IP Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface IP Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

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 subnet can ping each other.

3 Connecting Multiple On-premises Branch Networks Through a VPN Hub

3.1 Overview

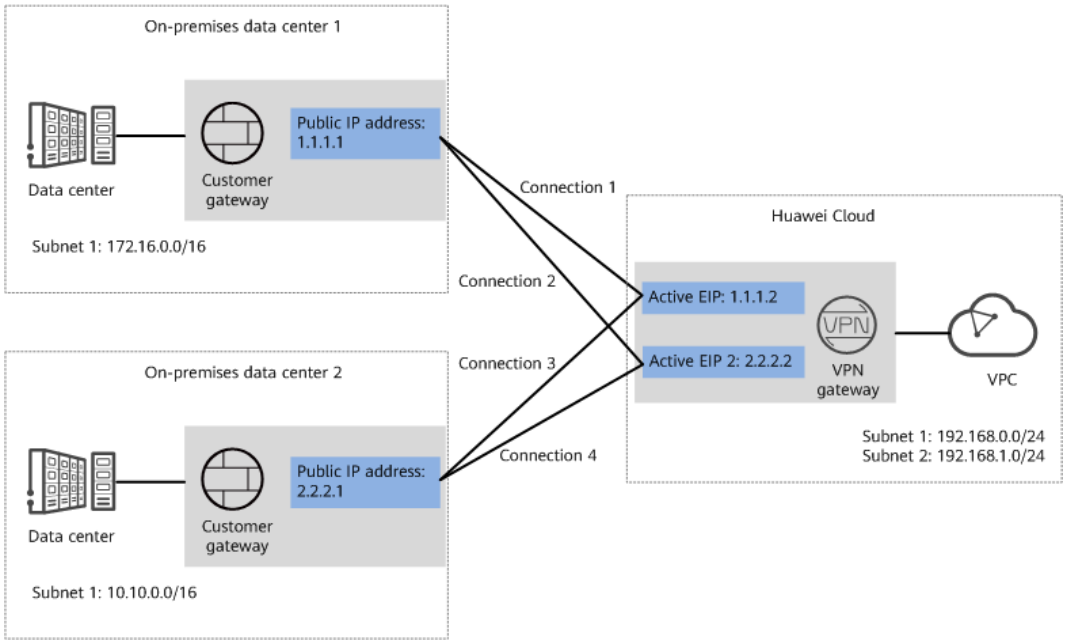
Scenario

To meet service requirements, enterprise A needs to implement communication between its two on-premises data centers.

Networking

Figure 3-1 shows the networking where the VPN service is used to connect the two on-premises data centers.

Figure 3-1 Networking diagram



Solution Advantages

- A VPN gateway on the cloud can function as a VPN hub to enable communication between on-premises branch sites. This eliminates the need to configure VPN connections between every two sites.
- A VPN gateway provides two IP addresses to establish dual independent VPN connections with each customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection, ensuring reliability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

3.2 Planning Networks and Resources

Data Plan

Table 3-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data centers	• 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
	HA Mode	Active-active
	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 • Active EIP 2: 2.2.2.2

Category	Item	Data
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 connections set up with on-premises data center 1 – VPN connection 1: 169.254.70.1/30 – VPN connection 2: 169.254.71.1/30 • VPN connections set up with on-premises data center 2 – VPN connection 3: 169.254.72.1/30 – VPN connection 4: 169.254.73.1/30
On-premises data center 1	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway in on-premises data center 1	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: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
On-premises data center 2	Subnet that needs to access the VPC	10.10.0.0/16
Customer gateway in on-premises data center 2	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 2.2.2.1
	Tunnel interface address	• VPN connection 3: 169.254.72.2/30 • VPN connection 4: 169.254.73.2/30
IKE and IPsec policies	PSK	Test@123

Category	Item	Data
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Version: v2 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

3.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.
- Data center side
  - IPsec has been configured on the VPN devices in the two on-premises data centers. For details, see **Administrator Guide**.
  - The remote subnets of the VPN device in on-premises data center 1 must contain the local subnet of the Huawei Cloud VPC and the subnet to be interconnected in on-premises data center 2. The remote subnets of the VPN device in on-premises data center 2 must contain the local subnet of the Huawei Cloud VPC and the subnet to be interconnected in on-premises data center 1.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Configure a VPN gateway.

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

Table 3-2 only describes the key parameters for creating a VPN gateway.

Table 3-2 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud VPC that the on-premises data centers need to access.	vpc-001(192.168.0.0/16)
Local Subnet	VPC subnets that the on-premises data centers need to access.	192.168.0.0/24,192.168.1.0/24
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
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	Active EIP used by the VPN gateway to access the on-premises data centers.	1.1.1.2
Active EIP 2	Standby EIP used by the VPN gateway to access the on-premises data centers.	2.2.2.2

Step 2 Configure customer gateways.

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

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

Table 3-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw1
Routing Mode	Select **Static**.	Static

Parameter	Description	Value
Gateway IP Address	IP address used by the customer gateway in on-premises data center 1 to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

3. Repeat the preceding operations to configure the customer gateway (2.2.2.1) in on-premises data center 2.

Step 3 Configure VPN connections between the cloud side and on-premises data center 1.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 3-4 only describes the key parameters for creating a VPN connection.

Table 3-4 Description of VPN connection parameters

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-fw1
Customer Subnet	Subnet in on-premises data center 1 that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify

Parameter	Description	Value
Local Tunnel Interface IP Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface IP Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
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.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	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 3-5 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 IP Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface IP Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 4 Configure VPN connections between the cloud side and on-premises data center 2.

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

2. Set parameters for VPN connection 1 as prompted and click **Submit**.
   Table 3-6 only describes the key parameters for creating a VPN connection.

   Table 3-6 Description of VPN connection parameters

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-003
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-fw2
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in on-premises data center 2 that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	10.10.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface IP Address	Tunnel interface IP address configured on the VPN gateway.	169.254.72.1
Customer Tunnel Interface IP Address	Tunnel interface IP address configured on the customer gateway device.	169.254.72.2
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.	**NQA** enabled

Parameter	Description	Value
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device in on-premises data center 2.	Test@123
Policy Settings	The policy settings must be the same as those configured on the customer gateway device in on-premises data center 2.	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 3-7 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-004
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface IP Address	Tunnel IP address of the VPN gateway.	169.254.73.1
Customer Tunnel Interface IP Address	Tunnel IP address of the customer gateway in on-premises data center 2.	169.254.73.2

Step 5 Configure customer gateway devices in on-premises data centers 1 and 2.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the four VPN connections are all **Available**.
- Verify that servers in on-premises data center 1 and servers in on-premises data center 2 can ping each other.