Virtual Private Network

Getting Started

Issue	01
Date	2023-03-07

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. 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


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

 Copyright © Huawei Technologies Co., Ltd.

1 Preparations

Before you use VPN, make the following preparations:

Registering with Huawei Cloud and Completing Real-Name Authentication

Skip this part if you already have a Huawei Cloud account. If you do not have a Huawei Cloud account, perform the following steps to register one:

1. Visit the **Huawei Cloud official website** and click **Register**.
2. Complete the registration as prompted. For details, see **Registering with Huawei Cloud**.

   If the registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For VPN pricing details, see **Pricing Details**.

 Copyright © Huawei Technologies Co., Ltd.

2 Configuring Enterprise Edition VPN to Connect an On-premises Data Center and a VPC

This section describes how to implement communication between a VPC and an on-premises data center by creating VPN connections between them.

2.1 Overview

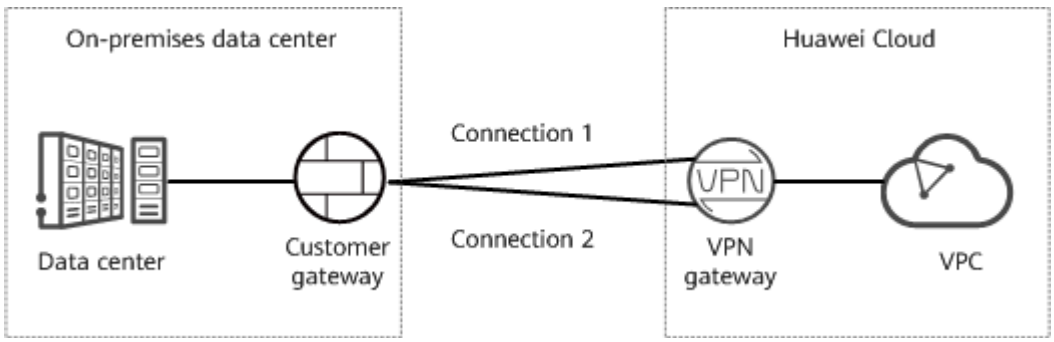
Supported Regions

AP-Bangkok, CN-Hong Kong, AP-Singapore, AP-Jakarta, TR-Istanbul, and LA-Mexico City2

Scenario

To meet business development requirements, enterprise A needs to implement communication between its on-premises data center and its VPC. In this case, enterprise A can use the VPN service to create connections between the on-premises data center and the VPC, as shown in **Figure 2-1**.

Figure 2-1 VPN networking



This solution has the following requirements on the on-premises data center and customer gateway device:

 Copyright © Huawei Technologies Co., Ltd.

- The customer gateway device must support standard IKE and IPsec protocols.
- The customer gateway has a static public IP address.
- The on-premises data center subnets that need to access the VPC do not contain 100.64.0.0/10 or overlap with the VPC subnets.

  If the VPC uses Direct Cloud or Cloud Connect connections to communicate with other VPCs, the on-premises data center subnets cannot overlap with those of these VPCs.

Data Plan

Table 2-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/16
VPN gateway	Interconnection subnet	This subnet is used by the VPN gateway for interconnection with the VPC, which cannot overlap with the VPC subnets in use. 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: 11.xx.xx.11 • Standby EIP: 11.xx.xx.12
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
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: 22.xx.xx.22
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30

Copyright © Huawei Technologies Co., Ltd.

Operation Process

Figure 2-2 shows the process of using the VPN service to enable communication between an on-premises data center and a VPC.

Figure 2-2 Operation process

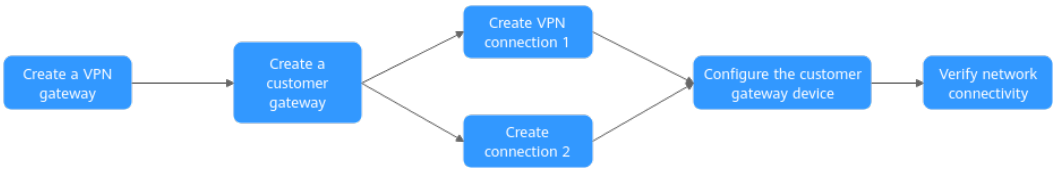


Table 2-2 Operation process description

No.	Step	Description
1	**Step 1: Creating 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	**Step 2: Creating a Customer Gateway**	Configure the VPN device in the on-premises data center as the customer gateway.
3	**Step 3: Creating VPN Connection 1**	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4	**Step 4: Creating 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	**Step 5: Configuring the Customer Gateway Device**	• The local and remote interface addresses configured on the customer gateway device must be the same as the customer and local interface addresses of the Huawei Cloud VPN connection, respectively. • The routing mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the Huawei Cloud VPN connection.
6	**Step 6: Verifying Network Connectivity**	Log in to an ECS and run the **ping** command to verify the network connectivity.

Copyright © Huawei Technologies Co., Ltd.

2.2 Step 1: Creating a VPN Gateway

Prerequisites

- 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 ECSs in the VPC, and allow the customer gateway in the on-premises data center to access VPC resources. For details about how to configure security group rules, see **Security Group Rules**.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.

Step 4 Set parameters as prompted and click **Next**.

The following table only lists the key parameters for creating a VPN gateway. For more information, see Creating a VPN Gateway.

Table 2-3 Key VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	The options include **Yearly/Monthly** and **Pay-per-use**.	Yearly/Monthly
Region	Select the region nearest to you.	AP-Singapore
Name	Name a VPN gateway.	vpngw-001
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
Associate With	The options include **VPC** and **Enterprise Router**	VPC
VPC	Select the VPC that needs to access the on-premises data center.	vpc-001(192.168.0.0/16)

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Interconnection Subnet	Specify an independent subnet for the VPN gateway, which cannot overlap with the VPC subnets in use.	192.168.2.0/24
Local Subnet	Specify the VPC subnet that needs to access the on-premises data center. You can manually enter a CIDR block or select a subnet from the drop-down list box.	192.168.0.0/24
Active EIP	You can buy a new EIP or use an existing EIP.	11.xx.xx.11
Standby EIP		11.xx.xx.12

----End

Verification

Check the created VPN gateway on the **VPN Gateways** page. The initial state of the VPN gateway is **Creating**. After about 2 minutes, the state changes to **Normal**, indicating that the VPN gateway is successfully created.

2.3 Step 2: Creating a Customer Gateway

Procedure

Step 1 Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.

Step 2 Set parameters as prompted and click **OK**.

The following table only lists the key parameters for creating a VPN gateway. For more information, see Creating a Customer Gateway.

Table 2-4 Customer gateway parameters

Parameter	Description	Example Value
Name	Name a customer gateway.	cgw-001
Routing Mode	Select **Static**.	Static
Gateway IP Address	Enter the IP address of the customer gateway in the on-premises data center.	22.xx.xx.22

----End

Copyright © Huawei Technologies Co., Ltd.

Verification

Check the created customer gateway on the **Customer Gateways** page.

2.4 Step 3: Creating VPN Connection 1

Procedure

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**.

   The following table only lists the key parameters for creating a VPN gateway. For more information, see Creating a VPN Connection.

Table 2-5 Parameter settings for VPN connection 1

Parameter	Description	Example Value
Name	Enter the name of VPN connection 1.	vpn-001
VPN Gateway	Select the VPN gateway created in **Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway	Select the customer gateway created in **Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Interface IP Address	Specify the tunnel IP address of the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Interface IP Address** and **Local Interface IP Address**, respectively.	169.254.70.2/30
Customer Interface IP Address	Specify the tunnel IP address of the customer gateway.	169.254.70.1/30

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Link Detection	This function is used for route reliability detection in multi-link scenarios. **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	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.5 Step 4: Creating VPN Connection 2

Procedure

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

   For VPN connection 2, you are advised to use the same settings as VPN connection 1, except the connection name, gateway IP address, local interface IP address, and customer interface IP address.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-6 Parameter settings for VPN connection 2

Parameter	Description	Example Value
Name	Enter the name of VPN connection 2.	vpn-002
VPN Gateway	Select the VPN gateway created in **Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select the standby EIP of the VPN gateway.	11.xx.xx.12
Customer Gateway	Select the customer gateway created in **Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Interface IP Address	Specify the tunnel IP address of the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Interface IP Address** and **Local Interface IP Address**, respectively.	169.254.71.2/30
Customer Interface IP Address	Specify the tunnel IP address of the customer gateway.	169.254.71.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. **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	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.6 Step 5: Configuring the Customer Gateway Device

Procedure

NOTE

In this example, the customer gateway device is a Huawei AR router. For more examples of configuring customer gateway devices, see **Administrator Guide**.

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. In this example, the WAN interface of the AR router is GigabitEthernet 0/0/8.

[AR651]interface GigabitEthernet 0/0/8

[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0

[AR651-GigabitEthernet0/0/8]quit

Step 4 Configure a default route.

[AR651]ip route-static 0.0.0.0 0.0.0.0 *22.xx.xx.1*

In this command, *22.xx.xx.1* is the gateway address of the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

[AR651]IPsec authentication sha2 compatible enable

Step 6 Configure an IPsec proposal.

[AR651]IPsec proposal hwproposal1

 Copyright © Huawei Technologies Co., Ltd.

```
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

Step 7 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 8 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 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[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 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[AR651-ike-peer-hwpeer2]quit
```

The commands are described as follows:

- **pre-shared-key cipher**: configures a PSK, which must be the same as that configured on the VPN console.
- **local-address**: specifies the public IP address of the AR router.
- **remote-address**: specifies the active or standby EIP of the VPN gateway.

Step 9 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 10 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 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[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 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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 11 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.

 Copyright © Huawei Technologies Co., Ltd.

- **destination-address**: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 12 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 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2

The parameters are described as follows:

- **192.168.0.0** indicates the local subnet of the VPC.
- **Tunnel***x* and **IPsec_nqa***x* in the same command correspond to the same VPN connection.

----End

Verification

Step 1 Log in to the management console.

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

Step 3 Choose **Virtual Private Network** > **Enterprise – VPN Connections**. Verify that the states of the two VPN connections are both **Available**.

----End

2.7 Step 6: Verifying Network Connectivity

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 **Service List** and choose **Compute** > **Elastic Cloud Server**.

Step 4 Log in to an ECS.

Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

In this example, use VNC provided on the management console to log in to an ECS.

Step 5 Run the following command on the ECS:

ping 172.16.0.100

172.16.0.100 is the IP address of a server in the on-premises data center. Replace it with an actual server IP address.

 Copyright © Huawei Technologies Co., Ltd.

If information similar to the following is displayed, the VPC on the cloud and the on-premises data center can communicate with each other.

```
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```

----End

Copyright © Huawei Technologies Co., Ltd.

3 Classic VPN Purchase Process

3.1 Overview

The process of configuring Classic VPNs varies in different regions, as described in **Table 3-1**.

Table 3-1 Overview

Supported Regions	CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, and LA-Santiago	LA-Mexico City1 and LA-Sao Paulo1
VPN Creation	Perform the following steps in sequence: 1. **Buying a VPN Gateway** 2. **Buying a VPN Connection** 3. **Configuring the Remote Device**	Perform the following steps in sequence: 1. **Creating a VPN (LA-Mexico City1/LA-Sao Paulo1)** 2. **Configuring the Remote Device**

3.2 Buying a VPN (LA-Mexico City1/LA-Sao Paulo1)

Overview

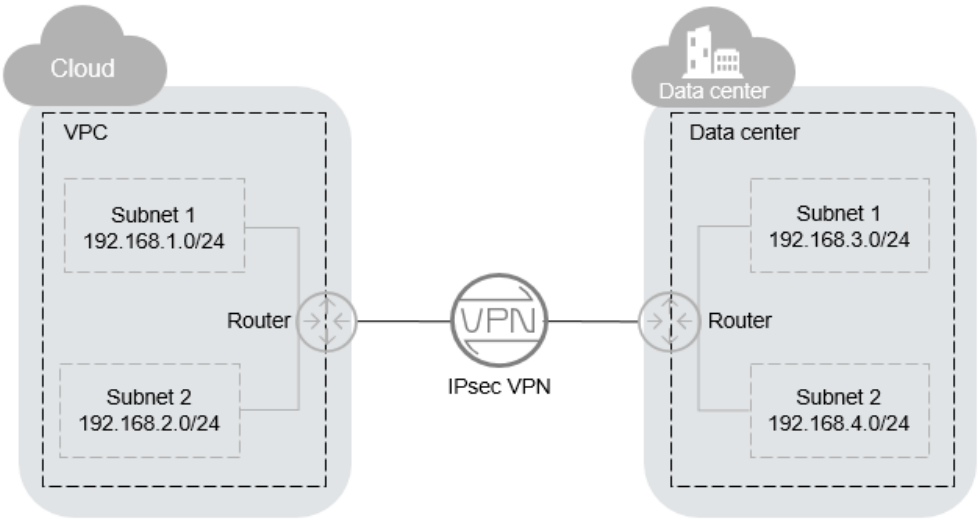
By default, ECSs in a VPC cannot communicate with devices in your on-premises data center or private network. To enable communication between them, you can use a VPN by creating it in your VPC and updating security group rules.

 Copyright © Huawei Technologies Co., Ltd.

IPsec VPN Topology

In **Figure 3-1**, the VPC has subnets 192.168.1.0/24 and 192.168.2.0/24. Your on-premises data center has subnets 192.168.3.0/24 and 192.168.4.0/24. You can use VPN to enable subnets in the VPC to communicate with those in your data center.

Figure 3-1 IPsec VPN



Huawei Cloud supports site-to-site VPN to enable communication between VPC subnets and on-premises data center subnets. Before establishing an IPsec VPN, ensure that the on-premises data center where the VPN is to be established meets the following conditions:

- On-premises devices that support the standard IPsec protocol are available.
- The on-premises devices have fixed public IP addresses, which can be statically configured or translated by NAT.
- The on-premises subnets do not conflict with VPC subnets, and devices in the on-premises subnets can communicate with the on-premises devices.

If the preceding conditions are met, ensure that the IKE policies and IPsec policies at both ends are consistent and the subnets at both ends are matched pairs when configuring IPsec VPN.

After the configuration is complete, VPN negotiation needs to be triggered by private network data flows.

Scenarios

You need a VPN that sets up a secure, isolated communications tunnel between your on-premises data center and cloud services.

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.

 Copyright © Huawei Technologies Co., Ltd.

- 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**.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. On the **Virtual Private Network** page, click **Buy VPN**.
5. Configure required parameters and click **Next**.

   Table 3-2, **Table 3-3**, and **Table 3-4** lists the parameters and their descriptions.

Table 3-2 Basic parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	AP-Singapore
Billing Mode	VPNs are billed on a pay-per-use basis.	Pay-per-use
Name	The VPN name	VPN-001
VPC	The VPC name	VPC-001
Local Subnet	VPC subnets that will access your on-premises network through a VPN.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnets cannot overlap with CIDR blocks involved in existing VPC peering connections created for the VPC.	192.168.3.0/24, 192.168.4.0/24
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK can contain 6 to 128 characters.	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details, see **Table 3-3** and **Table 3-4**.	Custom

Table 3-3 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 The default value is **Group 14**.	Group 14
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400
Negotiation Mode	This parameter is only available when **Version** is set to **v1**. You can set **Negotiation Mode** to **Main** or **Aggressive**. The default mode is **Main**.	Main

Copyright © Huawei Technologies Co., Ltd.

Table 3-4 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 The default algorithm is **DH group 14**.	DH group 14

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithm: 3DES
- DH algorithms: Group 1, Group 2, and Group 5

6. Submit your application.

   After the IPsec VPN is created, a public IP address is assigned to the VPN. The IP address is the local gateway address of the created VPN. When configuring the remote tunnel in your data center, you must set the remote gateway address to this IP address.

7. You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

3.3 Buying a VPN Gateway

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, buy a VPN gateway first. If you choose to buy a pay-per-use VPN gateway, a VPN connection will be created together with the VPN gateway.

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.

 Copyright © Huawei Technologies Co., Ltd.

- 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**.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. On the **VPN Gateways** page, click **Buy VPN Gateway**.
6. Configure the parameters based on **Table 3-5** and click **Buy Now**.

Table 3-5 Description of VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	Billing mode of a VPN gateway, which can be pay-per-use **Pay-per-use**: When you buy a pay-per-use VPN gateway, you must buy a VPN connection together with the VPN gateway.	Pay-per-use
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	AP-Singapore
Name	Name of a VPN gateway.	vpngw-001
VPC	Name of the VPC to which the VPN gateway connects.	vpc-001
Type	VPN type. **IPsec** is selected by default.	IPsec

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Billed By	A pay-per-use VPN gateway can be billed by bandwidth or by traffic. • **Bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. • **Traffic**: You need to specify a bandwidth limit and pay for the traffic you generate.	Traffic
Bandwidth (Mbit/s)	The bandwidth of the VPN gateway. The bandwidth is shared by all VPN connections created for the VPN gateway. The total bandwidth size used by all VPN connections created for a VPN gateway cannot exceed the VPN gateway bandwidth size. During the use of VPN, if the network traffic exceeds the VPN gateway bandwidth, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. You can configure alarm rules on Cloud Eye to monitor the bandwidth.	100

NOTE

When you buy a pay-per-use VPN gateway, you also need to configure a VPN connection that will be created together with the gateway (excepting the **CN South-Shenzhen** region). For details, see **Table 3-6**.

Table 3-6 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Local Subnet	VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: • **Select subnet**: Select the subnets that need to access your on-premises data center or private network. • **Specify CIDR block**: Enter the CIDR blocks that need to access your on-premises data center or private network. **NOTE** CIDR blocks of local subnets cannot overlap.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC. **NOTE** CIDR blocks of remote subnets cannot overlap.	192.168.3.0/24, 192.168.4.0/24
PSK	PSKs configured at both ends of a VPN connection must be the same. The PSK: • Contains 6 to 128 characters. • Can contain only: – Digits – Letters – Special characters: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 3-7** and **Table 3-8**.	Custom

Table 3-7 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is **Group 14**. DH algorithms configured at both ends of a VPN connection must be the same. Otherwise, the negotiation will fail.	Group 14
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

 Copyright © Huawei Technologies Co., Ltd.

Table 3-8 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default algorithm is **DH group 14**.	DH group 14

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • ESP • AH • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

CAUTION

The following algorithms are not recommended because they are not secure enough:

Authentication algorithms: SHA1 and MD5

Encryption algorithm: 3DES

DH algorithms: Group 1, Group 2, and Group 5

7. Confirm the VPN gateway information and click **Buy Now**.

   After a VPN gateway is created, the system automatically assigns a public IP address, that is, the IP address displayed in the **Gateway IP Address** column in the VPN gateway list. The gateway IP address is also the remote gateway IP address configured on the on-premises VPN network. **Figure 3-2** shows the gateway IP address.

Figure 3-2 VPN gateway list

3.4 Buying a VPN Connection

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN connection after a VPN gateway is obtained.

Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. On the **VPN Connections** page, click **Buy VPN Connection**.
6. Configure the parameters as prompted and click **Next**. **Table 3-9** lists the VPN connection parameters.

Table 3-9 Description of VPN connection parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	CN North-Beijing4
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001
Local Subnet	VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: • **Select subnet**: Select the subnets that need to access your on-premises data center or private network. • **Specify CIDR block**: Enter the CIDR blocks that need to access your on-premises data center or private network. **NOTE** CIDR blocks of local subnets cannot overlap.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC. **NOTE** CIDR blocks of remote subnets cannot overlap.	192.168.3.0/24, 192.168.4.0/24
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK: • Contains 6 to 128 characters. • Can contain only: – Digits – Letters – Special characters: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Existing**: Use existing IKE and IPsec policies. • **Custom**: including **IKE Policy** and **IPsec Policy**, which specifies the encryption and authentication algorithms of a VPN tunnel. For details about the policies, see **Table 3-10** and **Table 3-11**.	Custom

Copyright © Huawei Technologies Co., Ltd.

Table 3-10 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default algorithm is **Group 14**.	Group 14
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

Copyright © Huawei Technologies Co., Ltd.

Table 3-11 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default algorithm is **DH group 14**.	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • ESP • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

Copyright © Huawei Technologies Co., Ltd.

NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithm: 3DES
- DH algorithms: Group 1, Group 2, and Group 5

7. Click **Submit**.
8. You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

3.5 Configuring the Remote Device

For details about how to configure the remote device, see **Virtual Private Network Administrator Guide**. This guide helps you configure the local VPN device to implement the interconnection between your local network and the VPC subnet.

For details about the configuration examples, see the following:

- **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**

 Copyright © Huawei Technologies Co., Ltd.