Virtual Private Network

User Guide

Issue	01
Date	2020-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Overview

1.1 Virtual Private Network

Overview

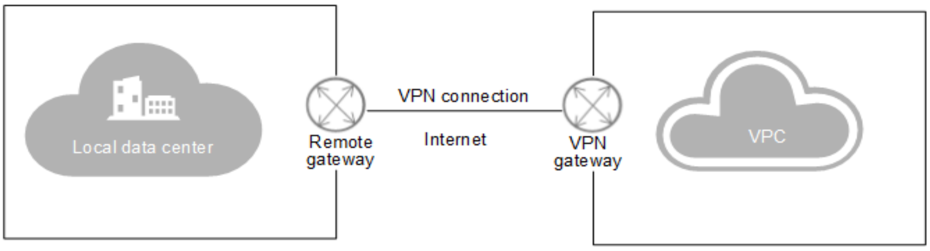
A Virtual Private Network (VPN) establishes an encrypted, Internet-based communications tunnel between your on-premises data center and a Virtual Private Cloud (VPC). With VPN, you can connect to a VPC and access the resources deployed there from your data center.

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN.

A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an Internet egress for a VPC and works together with the remote gateway in an on-premises data center. A VPN connection uses the Internet-based encryption technology to connect a VPN gateway and a remote gateway to establish cross-premises connectivity between your data center and your VPC. The VPN connection allows you to quickly build secure hybrid cloud environment.

Figure 1-1 shows the VPN networking.

Figure 1-1 VPN networking



Components

- **VPN Gateway**

A VPN gateway is an egress gateway of a VPC. With a VPN gateway, you can establish secure, reliable, and encrypted connectivity between a VPC and an on-premises data center or between two VPCs in different regions.

A VPN gateway works together with the gateway in an on-premises data center, that is the remote gateway. Each data center must have a remote gateway, and each VPC must have a VPN gateway. The VPN service allows you to set up point-to-point VPN connections or VPN connections from one point to multiple points. A VPN gateway can connect to one or more remote gateways.

- **VPN Connection**

  A VPN connection uses the Internet-based IPsec encryption technology to establish a secure and reliable communications tunnel between a VPN gateway and the remote gateway in your data center. Currently, only IPsec VPN connections are supported.

  VPN connections use IKE and IPsec protocols to encrypt and safely transmit data over the Internet, which are cost-effective.

1.2 Application Scenarios

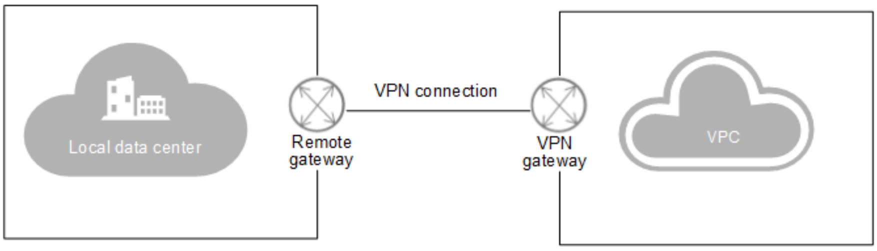
With the VPN between the VPC and your data center, you can easily use the ECSs and block storage resources on the cloud. Applications can be migrated to the cloud and additional web servers can be deployed to increase the computing capacity on a network. In this way, a hybrid cloud is built, which reduces IT O&M costs and protects enterprise core data from being leaked.

The VPN service allows you to set up site-to-site VPN connections or VPN connections from one site to multiple sites.

Site-to-site VPN connection

You can set up a VPN to connect a local data center to a VPC, thus building a hybrid cloud. **Figure 1-2** shows a site-to-site VPN connection.

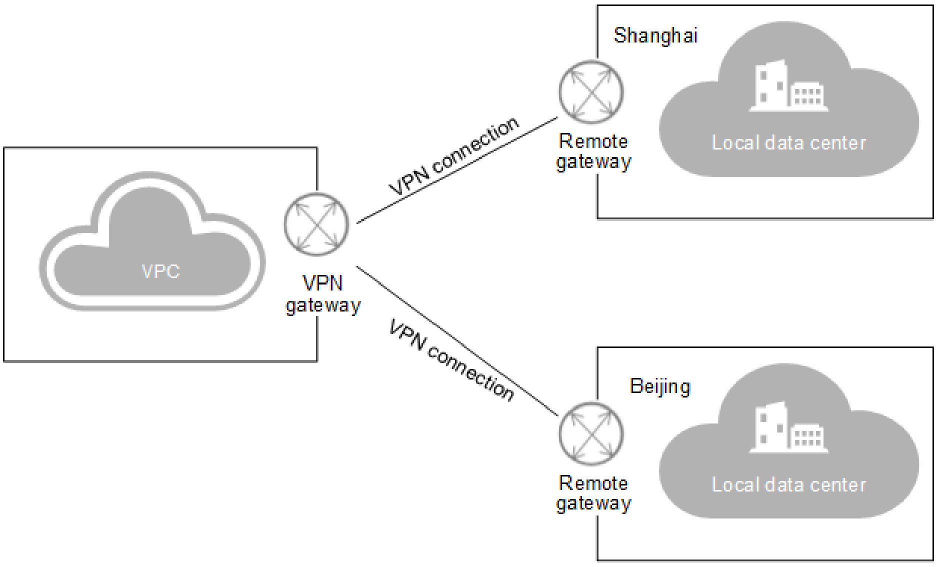
Figure 1-2 Site-to-site VPN connection



VPN connection from one site to multiple sites

You can also set up a VPN to connect multiple data centers to a VPC, thus building a hybrid cloud. **Figure 1-3** shows a VPN connection from one site to multiple sites.

Figure 1-3 VPN connection from one site to multiple sites



NOTE

The subnet CIDR blocks of each site involved in the VPN connection cannot overlap.

1.3 Reference Standards and Protocols

The following standards and protocols are associated with the IPsec VPN:

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2) Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

- RFC 4322: Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359: The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)

1.4 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your cloud resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your cloud service resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific cloud service resources. For example, some software developers in your enterprise need to use VPN resources but should not be allowed to delete them or perform any high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using VPN resources.

If your account does not need individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account.

For more information, see **IAM Service Overview**.

VPN Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

VPN is a project-level service deployed in specific physical regions. To assign VPN permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing VPN, the users need to switch to a region where they have been authorized to use this service.

Table 1-1 lists all system-defined roles supported by VPN.

Table 1-1 System-defined roles supported by VPN

Role	Description	Dependencies
VPN Administrator	All operations on VPN resources. To be granted this permission, users must also have the **Tenant Guest** and **VPC Administrator** permissions.	**Tenant Guest** and **VPC Administrator** ● **VPC Administrator**: project-level policy, which must be assigned in the same project as the **VPN Administrator** ● **Tenant Guest**: project-level policy, which must be assigned in the same project as the **VPN Administrator**

Table 1-2 lists the common operations supported by each system-defined policy of VPN. Select the permissions as needed.

Table 1-2 Common operations supported by **VPN Administrator**

Operation	VPN Administrator
Creating a VPN gateway	√
Viewing a VPN gateway	√
Modifying a VPN gateway	√
Deleting a VPN gateway	√
Creating a VPN connection	√
Viewing a VPN connection	√
Modifying a VPN connection	√
Deleting a VPN connection	√

Helpful Links

- **What Is IAM?**
- **Creating a User and Granting VPN Permissions**

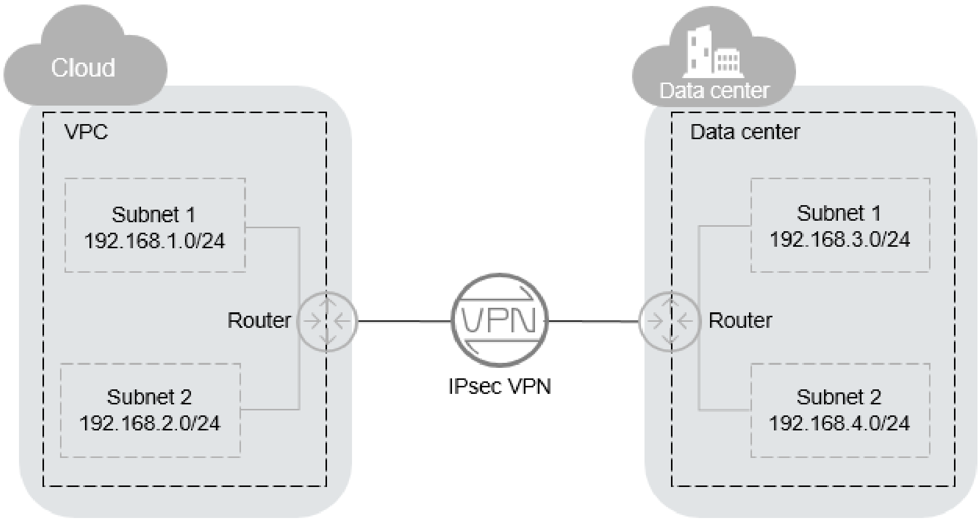
1.5 Basic Concepts

1.5.1 IPsec VPN

The Internet Protocol Security (IPsec) VPN is an encrypted tunneling technology that can establish confidential and secure communication tunnels between different networks.

In **Figure 1-4**, 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 create a VPN to enable subnets in your VPC to communicate with those in your data center.

Figure 1-4 IPsec VPN



Currently, both site-to-site and hub-and-spoke VPNs are supported. You need to set up VPNs in both your data center and the VPC to establish the VPN connection.

Ensure that the Internet Key Exchange (IKE) and IPsec policies at both ends of the VPN are the same. Your device should comply with IPsec standards and protocols.

1.5.2 Region and AZ

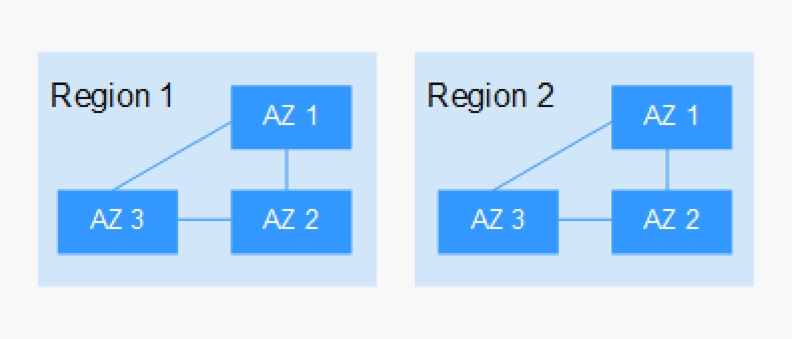
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-5 shows the relationship between regions and AZs.

Figure 1-5 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2 Getting Started

2.1 Creating a Security Group

Scenarios

You can create security groups, define security group rules, and add ECSs in the VPC to the security groups, improving ECS access security. It is recommended that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Create Security Group**.
6. In the **Create Security Group** area, set the parameters as prompted. **Table 2-1** lists the parameters to be configured.

Table 2-1 Parameter descriptions

Parameter	Description	Example Value
Template	A template comes with default security group rules, helping you quickly create security groups. The following templates are provided: ● **Custom**: This template allows you to create security groups with custom security group rules. ● **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389. ● **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks. Exercise caution when using this template.	General-purpose web server
Name	Specifies the security group name. This parameter is mandatory. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces. **NOTE** You can change the security group name after a security group is created. It is recommended that you give each security group a different name.	sg-318b
Description	Provides supplementary information about the security group. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. Click **OK**.

2.2 Adding a Security Group Rule

Scenarios

After you create a security group, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After you add ECSs to the security group, they are protected by the rules of the group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.

   You can click **+** to add more inbound rules.

Table 2-2 Inbound rule parameter descriptions

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Example values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	Custom TCP
	Port: specifies the port or port range over which the traffic can reach your ECS. Ports 1 to 65535 are all allowed.	22, or 22-30
Source	Specifies the source of the security group rule. The value can be another security group or a single IP address. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (subnet CIDR block) ● 0.0.0.0/0 (any IP address) ● sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.

   You can click **+** to add more outbound rules.

Table 2-3 Outbound rule parameter descriptions

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Example values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	Custom TCP
	Port: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Source	Specifies the source of the security group rule. The value can be another security group or a single IP address. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (subnet CIDR block) ● 0.0.0.0/0 (any IP address) ● sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

8. Click **OK**.

3 Management

3.1 Managing VPN Connections

3.1.1 Viewing a VPN Connection

Scenarios

After creating a VPN connection, you can view details about your VPN connection.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connections**.
5. View all of your VPN connections on the **VPN Connections** page.
6. Locate the row that contains the target VPN connection, click **View Policy** in the **Operation** column to view IKE and IPsec policy details about the VPN connection.

3.1.2 Modifying a VPN Connection

Scenarios

A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an external data center. You can modify a VPN connection when required.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connections**.
5. On the **VPN Connections** page, locate the row that contains the target VPN connection and click **Modify** in the **Operation** column.
6. In the displayed dialog box, set parameters as prompted.
7. Click **OK**.

3.1.3 Deleting a VPN Connection

Scenarios

You can delete a VPN connection to release network resources if it is no longer required.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connections**.
5. On the **VPN Connections** page, locate the row that contains the target VPN connection and click **Delete** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.

3.2 Managing VPN Gateways

3.2.1 Viewing a VPN Gateway

Scenarios

After creating a VPN gateway, you can view information about your VPN gateway.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateways**.

5. View information about your VPN gateway on the **VPN Gateways** page.

3.2.2 Modifying a VPN Gateway

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateways**.
5. On the **VPN Gateways** page, locate the row that contains the target VPN gateway, and choose **More** > **Modify Bandwidth**.

   You can also choose **More** > **Modify Basic Information**.
6. Modify the VPN gateway bandwidth, name, or description as required.
7. Click **OK**.

3.2.3 Deleting a VPN Gateway

Scenarios

You can delete a VPN gateway to release network resources if it is no longer required.

A VPN gateway cannot be deleted if it is being used by a VPN connection. You must delete the VPN connection before deleting the VPN gateway.

Procedure

1. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateways**.
2. On the **VPN Gateways** page, locate the row that contains the target VPN gateway and click **Delete** in the **Operation** column.
3. Click **Yes** in the displayed dialog box.

3.3 Monitoring

3.3.1 Monitoring VPN

Monitoring is the key for ensuring VPN performance, reliability, and availability. Using monitored data, you can determine VPN resource usage. The cloud platform provides the Cloud Eye service to help you to obtain the running status of your VPNs. You can use Cloud Eye to automatically monitor VPNs in real time and manage alarms and notifications, so that you can keep track of VPN performance metrics.

This section covers the following content:

- **Monitoring Metrics**
- **Setting Alarm Rules**

- Viewing Monitoring Metrics

3.3.2 Metrics

Description

This section describes monitored metrics reported by VPN to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console to query the metrics of the monitored objects and alarms generated for VPN.

Namespace

SYS.VPN

Metrics

Table 3-1 Monitoring on VPN connection status

Parameter	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
connection_status	VPN Connection Status	VPN connection tunnel status **0**: indicates the not connected status. **1**: indicates the connected status.	0 or 1	VPN connection	5 minutes

Table 3-2 EIP and Bandwidth metrics

Parameter	Metric	Description	Value Range	Measurement Object & Dimension	Monitoring Period (Raw Data)
upstream_bandwidth	Outbound Bandwidth (originally named "Upstream Bandwidth")	Network rate of outbound traffic Unit: bit/s	≥ 0 bits/s	Monitored object: bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
downstream_bandwidth	Inbound Bandwidth (originally named "Downstream Bandwidth")	Network rate of inbound traffic Unit: bit/s	≥ 0 bits/s	Monitored object: bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage rate of outbound bandwidth in the unit of percent.	0-100%	Monitored object: bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
up_stream	Outbound Traffic (originally named "Upstream Traffic")	Network traffic going out of the cloud platform Unit: byte	≥ 0 bytes	Monitored object: bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute

Parameter	Metric	Description	Value Range	Measurement Object & Dimension	Monitoring Period (Raw Data)
down_stream	Inbound Traffic (originally named "Downstream Traffic")	Network traffic going into the cloud platform Unit: byte	≥ 0 bytes	Monitored object: bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute

Dimensions

key	Value
connection_id	VPN connection

3.3.3 Creating Alarm Rules

Scenarios

You can configure alarm rules to customize the monitored objects and notification policies and to learn VPN status at any time.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
4. In the left navigation pane, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.
6. After the parameters are set, click **Create**.

   After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

NOTE

For more information about alarm rules of VPN, see the *Cloud Eye User Guide*.

3.3.4 Viewing Metrics

Scenarios

View the VPN connection status and the usage of bandwidth and EIP.

Procedure

Viewing VPN connection status

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
4. Click **Cloud Service Monitoring** on the left navigation pane and then **Virtual Private Network**.
5. Click **View Metric** in the **Operation** column to view the VPN connection status.

   You can view data during the last one, three, or twelve hours.

   NOTE

   You can also log in to the management console, under **Network**, click **Virtual Private Network**, and then click **VPN Connections**. Locate the row that contains the target VPN connection and click **View Metric** in the **Operation** column to view the VPN connection status.

Viewing bandwidth or EIP usage

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. On the left navigation pane, click **VPN Gateways**.
5. Locate the row that contains the target VPN gateway and click **View Metric** in the **Operation** column to check the bandwidth or EIP monitoring information.

   You can view data during the last one, three, or twelve hours.

3.4 Permissions Management

3.4.1 Creating a User and Granting VPN Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your VPN resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to VPN resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust account or cloud service to perform professional and efficient O&M on your VPN resources.

If your account does not require individual IAM users, skip over this section.

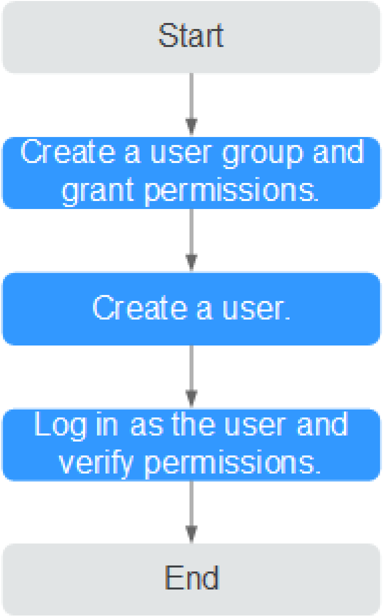
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by VPN. For system permissions of other cloud services, see **Permissions**.

Process Flow

Figure 3-1 Process for granting VPN permissions


Start
Create a user group and grant permissions.
Create a user.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions to it**.

   Create a user group on the IAM console and attach the **VPN Administrator** policy to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console as the created user. Switch to the authorized region and verify the permissions.

   – Choose **Service List** > **Network** > **Virtual Private Network**. Then click **Buy VPN Gateway** in the upper right corner. If the VPN gateway is successfully created, the **VPN Administrator** policy has already taken effect.

- Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPN Administrator** policy has already taken effect.

3.5 Quotas

What Is Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click 📊 .

   The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. Click **Increase Quota**.
3. On the **Create Service Ticket** page, configure parameters as required.

   In **Problem Description** area, fill in the content and reason for adjustment.
4. After all necessary parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

4 Best Practice

4.1 Connecting to a VPC Through a VPN

Scenarios

By default, ECSs in a VPC cannot communicate with your on-premises network. To enable communication between them, use a VPN. After a VPN is created, configure the security group and check the connectivity between the local and remote networks to ensure that the VPN is available. VPNs can be classified into the following two types:

- Site-to-site VPN: The local side is a VPC on the cloud service platform, and the remote side is a user data center. A site-to-site VPN is a communication tunnel between a user data center and a single VPC.
- Hub-and-spoke VPN: The local side is a VPC on the cloud service platform, and the remote side is user data centers. A hub-and-spoke VPN is a communication tunnel between user data centers and a VPC.

Ensure that the following requirements are met when configuring a VPN:

- The local and remote subnets cannot overlap.
- Different local subnets cannot overlap.
- IKE policies, IPsec policies, and PSK at both ends of the VPN must be the same.
- The local and remote subnet and gateway parameters must be matched pairs.
- The security group used by ECSs in the VPC allows traffic from and to the remote side.
- After a VPN is created, its status changes to **Normal** only after the VMs or physical servers on the two sides of the VPN communicate with each other.

Prerequisites

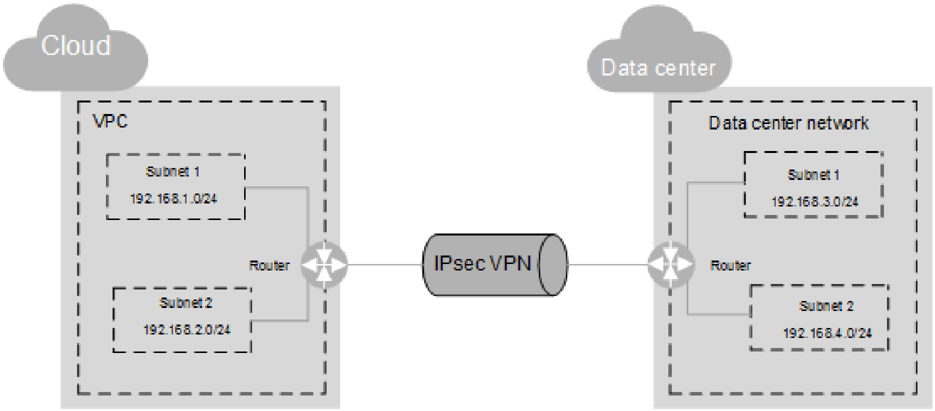
You have created the VPC and subnet required by the VPN.

Procedure

1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.
2. Check the IP address pools for the local and remote subnets.

   In **Figure 4-1**, 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 create a VPN to enable subnets in your VPC to communicate with those in your data center.

   Figure 4-1 IPsec VPN

   The IP address pools for the local and remote subnets cannot overlap with each other. For example, if the local VPC has two subnets, 192.168.1.0/24 and 192.168.2.0/24, the IP address pool for the remote subnets cannot contain these two subnets.
3. Configure security group rules for the VPC.
4. Check the security group of the VPC.

   The security group must allow packets from the VPN to pass. You can run the **ping** command to check whether the security group of the VPC allows packets from the VPN to pass.
5. Check the remote LAN configuration (network configuration of the remote data center).

   A route must be configured for the remote LAN to enable VPN traffic to be forwarded to network devices on the LAN. If the VPN traffic cannot be forwarded to the network devices, check whether the remote LAN has policies configured to refuse the traffic.

5 FAQs

5.1 Do IPsec VPNs Support Automatic Negotiation?

The IPsec VPN tunnel works in passive mode, which triggers automatic negotiation only when traffic sent by the local end passes through the tunnel.

5.2 What Do I Do If VPN Connection Setup Fails?

1. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms between the local and remote sides of the VPN are the same.
   a. If the IKE policy has been set up during phase one and the IPsec policy has not been enabled in phase two, the IPsec policies between the local and remote sides of the VPN may be inconsistent.
   b. If a Cisco physical device is used at the customer side, it is recommended that you use MD5. Then, you need to set **Authentication Mode** to **MD5** in the IPsec policy for the VPN created on the cloud.
2. Check whether the ACL configurations are correct.

   If the subnets of your data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24, configure the ACL rules for each data center subnet to allow the communication with the VPC subnets. The following provides an example of ACL configurations:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   ```
3. After the configuration is complete, ping the local and the remote side from each other to check whether the VPN connection is normal.

5.3 What Should I Do If I Cannot Access the ECSs on the Cloud from My Data Center or LAN Even If the VPN Has Been Set Up?

The security group denies the access from all sources by default. If you want to access your ECSs, modify the security group configuration and allow the access from the remote subnets.

5.4 What Should I Do If I Cannot Access My Data Center or LAN from the ECSs After a VPN Connection Has Been Set Up?

Check whether you have properly configured the firewall policies for the access from the public IP address of the cloud VPN to the public IP address of your data center or LAN. No policies are configured to limit the access by default.

5.5 Does a VPN Allow for Communication Between Two VPCs?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.

5.6 What Is the Limitation on the Number of Local and Remote Subnets of a VPN?

The maximum number obtained by multiplying the number of local subnets and that of remote subnets cannot exceed 225.

5.7 Why Is Not Connected Displayed as the Status for a Successfully Created VPN?

After a VPN is created, its status changes to **Normal** only after the VMs or physical servers on the two sides of the VPN communicate with each other.

- IKE v1:

  If no traffic goes through the VPN for a period of time, the VPN needs to be renegotiated. The negotiation time depends on the value of **Lifecycle (s)** in the IPsec policy. Generally, the value of **Lifecycle (s)** is **3600** (1 hour), indicating that the negotiation will be initiated in the fifty-fourth minute. If the negotiation succeeds, the connection remains to the next round of negotiation. If the negotiation fails, the status is set to be disconnected within one hour. The connection can be restored after the two sides of the VPN communicates with each other. The disconnection can be avoided by using a network monitoring tool, such as IP SLA, to generate packets.

- IKE v2: If no traffic goes through the VPN for a period of time, the VPN remains in the connected status.

5.8 How Long Is Required for Issued VPN Configurations to Take Effect?

The time required for VPN configurations to take effect increases linearly with the number obtained by multiplying the number of local subnets and that of remote subnets.

5.9 How Do I Configure a Remote Device for a VPN?

Due to the symmetry of the tunnel, the VPN parameters configured on the cloud must be the same as those configured in your own data center. If they are different, a VPN cannot be established.

To set up a VPN, you also need to configure the IPsec VPN on the router or firewall in your own data center. The configuration method may vary depending on your network device in use. For details, see the configuration guide of your network device.

This section describes how to configure the IPsec VPN on a Huawei USG6600 series V100R001C30SPC300 firewall for your reference.

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

Procedure

1. Log in to the CLI of the firewall.
2. Check firewall version information.
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
   ```
3. Create an access control list (ACL) and bind it to the target VPN instance.
   ```
   acl number 3065 vpn-instance vpn64
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   q
   ```
4. Create an IKE proposal.
   ```
   ike proposal 64
   dh group5
   authentication-algorithm sha1
   integrity-algorithm hmac-sha2-256
   ```

```
sa duration 3600
q
```

5. Create an IKE peer and reference the created IKE proposal. The peer IP address is *x.x.x.x*.

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

6. Create an IPsec protocol.

```
ipsec proposal ipsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. Create an IPsec policy and reference the IKE policy and IPsec proposal.

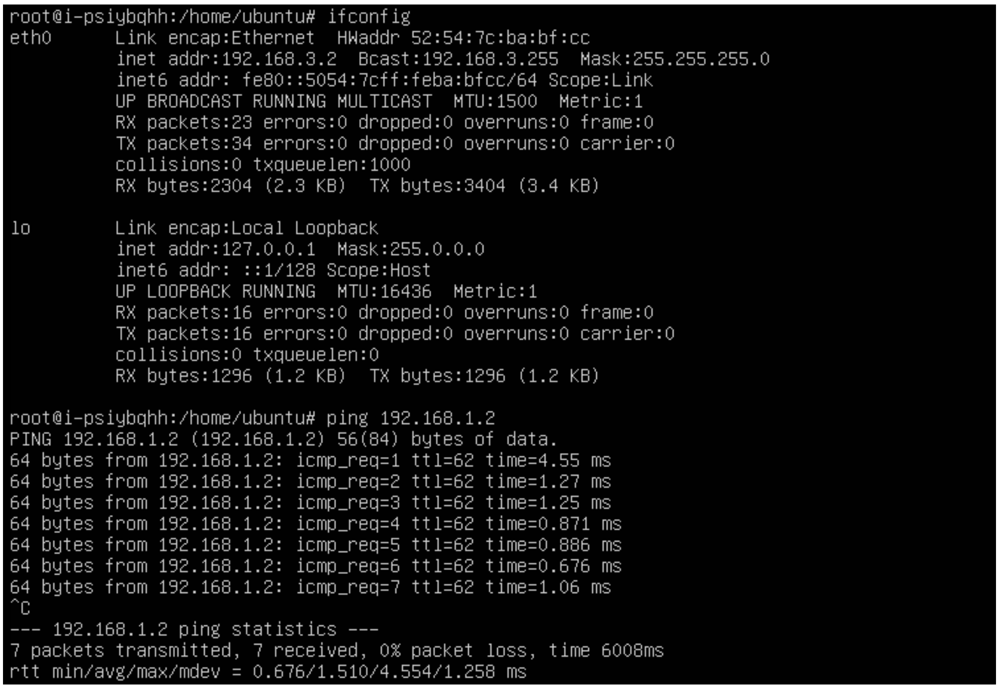
```
ipsec policy vpnipsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal ipsecpro64
local-address xx.xx.xx.xx
q
```

8. Apply the IPsec policy to the subinterface.

```
interface GigabitEthernet0/0/2.64
ipsec policy vpnipsec64
q
```

9. Test the connectivity.

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



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

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

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

5.10 Which Remote VPN Devices Are Supported?

Most devices that meet IPsec VPN standard and reference protocol requirements can be used as the remote VPN devices, for example, Cisco ASA firewalls, Huawei USG6*xxxx* series firewalls, USG9*xxxx* series firewalls, Hillstone firewalls, and Cisco ISR routers. **Table 5-1** lists the supported Huawei USG6*xxxx* and USG9*xxxx* firewalls.

Table 5-1 Huawei VPN devices

Supported Remote VPN Device	Description
Huawei USG6000 series	USG6320/6310/6510-SJJ USG6306/6308/6330/6350/6360/6370/6380/6390/6507/6530/6550/6570:2048 USG6620/6630/6650/6660/6670/6680
Huawei USG9000 series	USG9520/USG9560/USG9580

Other devices that meet the requirements in the reference protocols described in section **Reference Standards and Protocols** can also be deployed. However, some devices may fail to add because of inconsistent protocol implementation methods of these devices. If the connection setup fails, rectify the fault by following the instructions provided in section **What Do I Do If VPN Connection Setup Fails?** or contact customer service.

5.11 What Should I Do If the VPN Connection Fails or the Network Speed of the VPN Connection Is Slow?

You can perform the following steps to handle the issues:

1. Check the ECS specifications. Rate limiting is not performed for the VPN ingress on the cloud, so the issue may be caused by the ECS specifications.
2. Rate limiting has been configured for the VPN egress on the cloud. Check whether your bandwidth has reached or exceeded the maximum limit allowed.
3. Check your local network to see whether the network speed is slow.
4. Check whether packets sent between the cloud and the customer data center have been lost.

5.12 Are SSL VPNs Supported?

Currently, the VPN service does not support the SSL VPNs.

A Change History

Release Date	Description
2020-08-30	This issue is the first official release.