Virtual Private Network

Administrator Guide

Issue	01
Date	2020-09-30

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 Overview

Welcome to the *Virtual Private Network Administrator Guide*. This guide helps you configure the VPN device to implement the interconnection between your network and the VPC subnet.

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

- **Huawei USG6600 Series**
- **Configuring VPN When Fortinet FortiGate Firewall Is Used**
- **Configuring VPN When Sangfor Firewall Is Used**
- **Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication**
- **Using Openswan to Configure On- and Off-Cloud Communication**
- **Using strongSwan to Configure On- and Off-Cloud Communication**
- **Interconnecting HUAWEI CLOUD with Alibaba Cloud**

2 Huawei USG6600 Series

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 93.188.242.110, 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 93.188.242.110.
   ```
   ike peer vpnikepeer_64
   pre-shared-key ******** (******** specifies the pre-shared key.)
   ike-proposal 64
   undo version 2
   remote-address vpn-instance vpn64 93.188.242.110
   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.

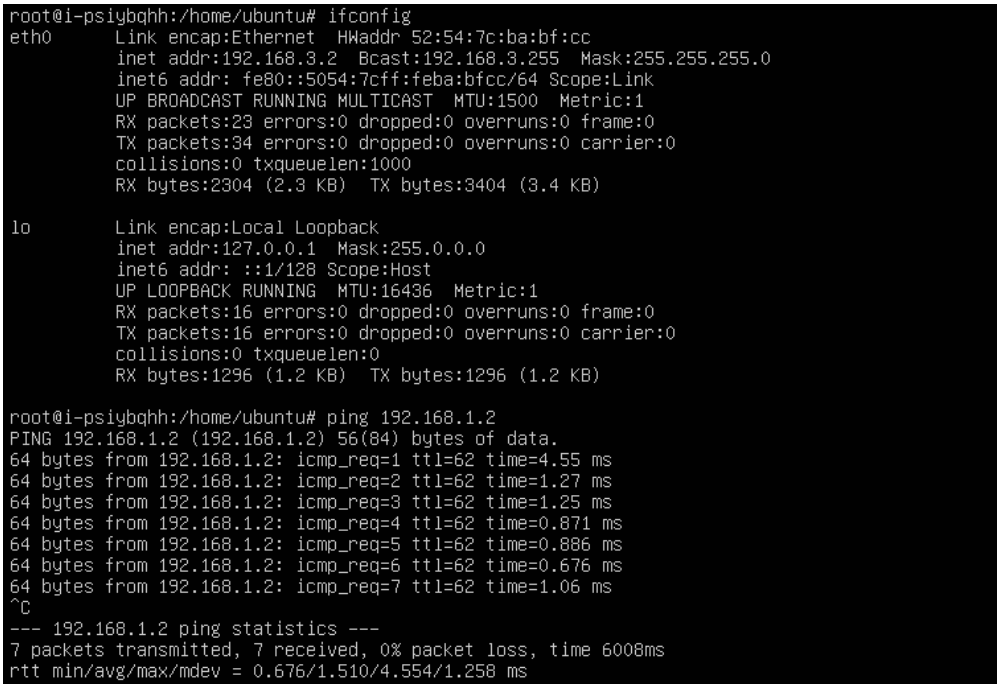
```
ipsec policy vpnipsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal ipsecpro64
local-address xx.xx.xx.xx
q
```

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.



3 Configuring VPN When Fortinet FortiGate Firewall Is Used

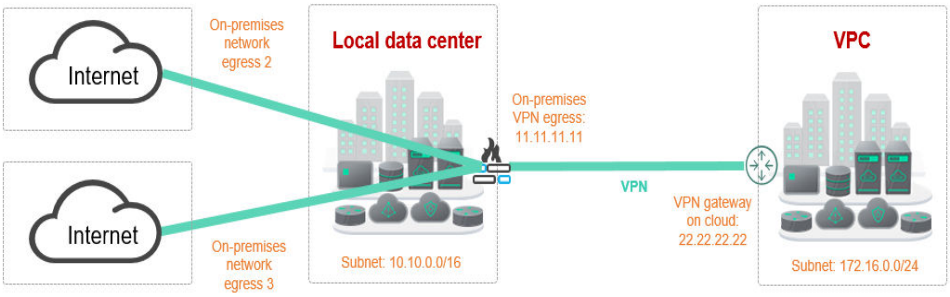
Scenarios

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

Topology Connection

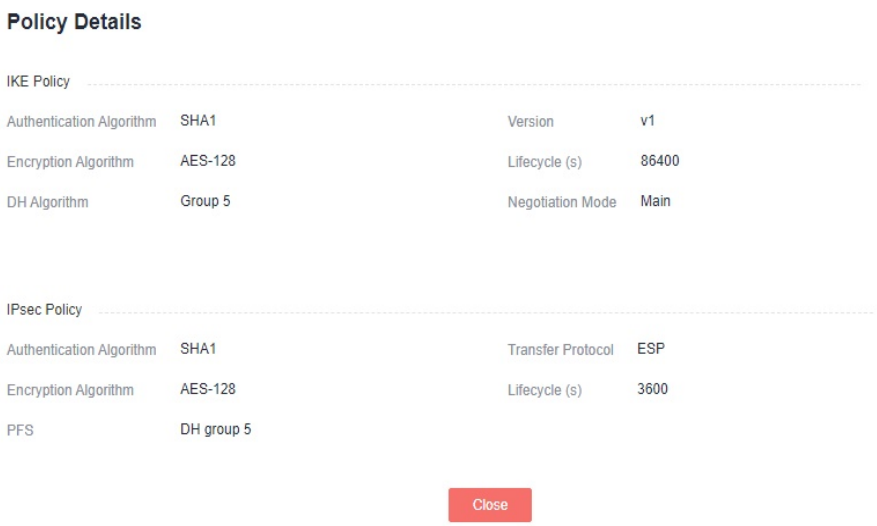
As shown in **Figure 3-1**, the local data center has multiple Internet egresses. The egress 11.11.11.11 is specified to establish a VPN connection with the HUAWEI CLOUD VPC. The subnet of the local data center is 10.10.0.0/16, and the VPC subnet on HUAWEI CLOUD is 172.16.0.0/24. The IP address of the VPN gateway you purchased on HUAWEI CLOUD is 22.22.22.22. Create a VPN connection to connect your on-premises network to the VPC subnet.

Figure 3-1 Multi-egress on-premises network connecting to a VPC through a VPN



Configure the VPN connection policies on HUAWEI CLOUD based on **Figure 3-2**.

Figure 3-2 Policy details on HUAWEI CLOUD



Configuration Procedure

This example describes how to configure a VPN if the FortiGate firewall is used on your local data center.

Step 1 Configure IPsec VPN.

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

Step 2 Configure routes.

1. Add a static route.

   Add an egress route to the VPC subnet. The outbound interface is the VPN interface, and the next-hop gateway is the gateway of the outbound interface.

2. Configure policy-based routes for multiple egresses.

   Set the source address to the subnet of the local data center and the destination address to the subnet of the VPC. Adjust the configuration sequence of the policy-based routes to ensure that the policy-based routes will be preferentially used.

Step 3 Configure policies and NAT.

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

----End

Configuration Verification

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

Configuration Using the CLI

1. Configure the physical interface.

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

2. Configure interface zones.

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

3. Configure subnets.

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

4. Configure IPsec.

```
config vpn ipsec phase1-interface                              //Phase 1 configuration
   edit "ipsec"
      set interface "port1"
      set nattraversal disable
      set proposal aes128-sha1
      set comments "IPsec"
      set dhgrp 5
      set remote-gw 22.22.22.22
      set psksecret ENC dmFyLzF4tRrIjV3T
+lSzhQeU2nGEoYKC31NaYRWFJl8krlwNmZX5SfwUi5W5RLJqFu82VYKYsXp5+HZJ13VYY8O2Sn/
vruzdLxqu84zbHEIQkTlf5n/
63KEru1rRoNiHDTWfh3A3ep3fKJmxf43pQ7OD64t151ol06FMjUBLHgJ1ep9d32Q0F3f3oUxfDQs21Bi9RA
==
   next
end
config vpn ipsec phase2-interface                              //Phase 2 configuration
   edit "IP-TEST"
      set phase1name "ipsec "
      set proposal aes128-sha1
      set dhgrp 5
      set keylifeseconds 3600
      set src-subnet 10.10.0.0 255.255.0.0
      set dst-subnet 172.16.0.0 255.255.255.0
```

```
    next
end
```

5. Configure access policies.

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

6. Configure routes.

```
config router static
    edit 24                          //Route 24 is a static route that is used to access on the cloud.
        set dst 172.16.0.0 255.255.255.0
        set gateway 11.11.11.1
        set distance 10
        set device "port1"
config router policy
edit 2                      //Policy-based route 2 is used to access the cloud from the on-premises data
center.
        set input-device "A1"
        set src "10.10.00/255.255.0.0"
        set dst "172.16.0.0/255.255.255.0"
        set gateway 11.11.11.1
        set output-device "port1"
```

4 Configuring VPN When Sangfor Firewall Is Used

Scenarios

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

Topology Connection

Topology connection mode:

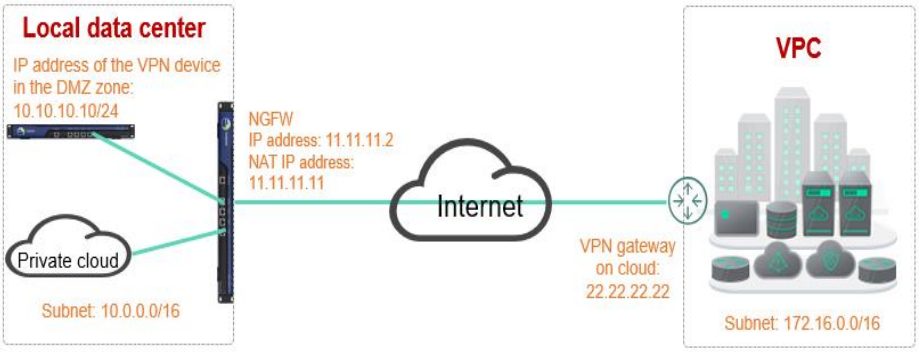
- Use the firewall to establish a VPN connection with the cloud.
- Use the VPN device in the DMZ zone and the NAT traversal technique to establish a VPN connection with the cloud.

The configuration details are as follows.

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

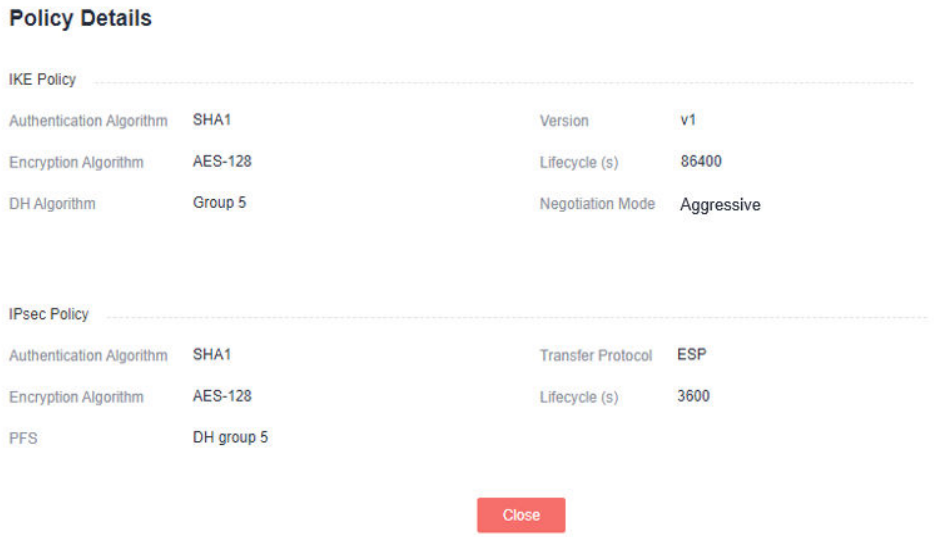
Create a VPN connection to connect an on-premises network to the VPC subnet.

Figure 4-1 Using a VPN to Connect a VPC with a local data center that uses Sangfor firewall and the NAT traversal technique



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

Figure 4-2 Policy details on HUAWEI CLOUD



Configuration Procedure

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

Step 1 Configure IPsec VPN.

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

Step 2 Configure routes.

Step 3 Configure policies and NAT.

----End

Configuration Verification

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

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

Scenarios

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

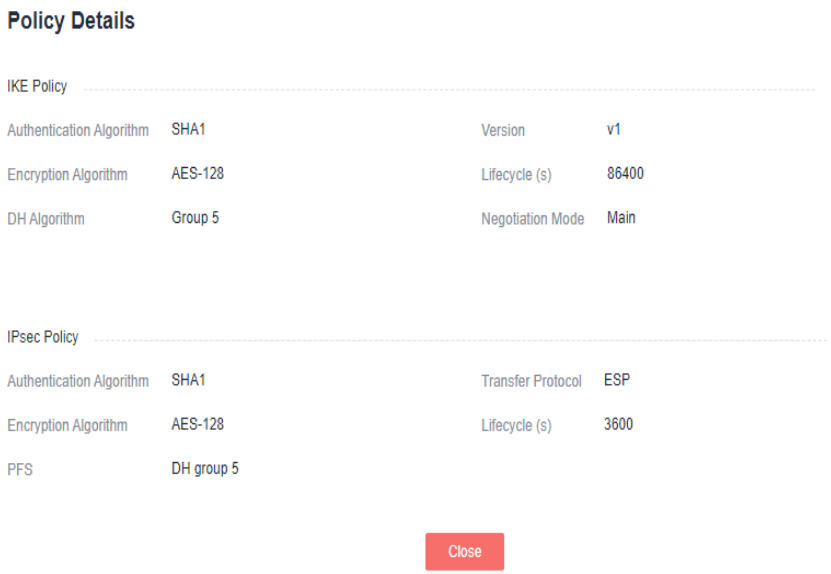
This following describes the configuration details if TheGreenBow IPsec VPN Client is used.

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

Prerequisites

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

Figure 5-1 Policy details



c. TheGreenBow IPsec VPN Client has been installed on the cloud desktop.

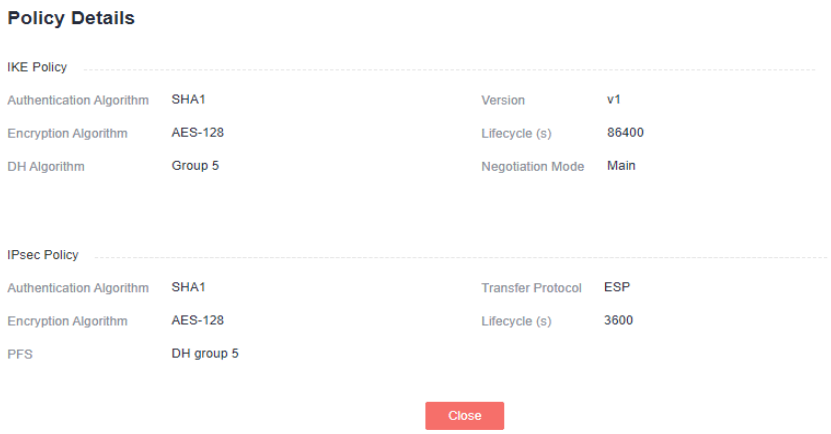
d. The cloud desktop can ping the IP address of the VPN gateway.

2. Scenario 2: VPC + VPC

a. The VPCs, subnets, and ECSs in two regions have been configured. The ECS in VPC2 runs the Windows OS.

b. The VPN gateway and VPN connection in VPC1 have been configured.

Figure 5-2 Policy details



c. TheGreenBow IPsec VPN Client has been installed on the Windows ECS in VPC2.

d. The ECS in VPC2 can ping the VPN gateway IP address of VPC1.

NOTE

Use the default VPN configurations on HUAWEI CLOUD.

Configuration Procedure

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

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

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

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

Configuration Verification

1. Scenario 1: Cloud desktop + VPC

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

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

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

2. Scenario 2: VPC + VPC

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

   a. Check whether the VPN connection is successfully established.
   b. Check the VPN connection status of the VPC.
   c. Check the VPC network configurations.
   d. Ping the ECS in VPC2 from the ECS in VPC1.
   e. Ping the ECS in VPC1 from the ECS in VPC2.

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

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

Scenarios

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

Topology Connection

Figure 6-1 shows the topology connection and policy negotiation configurations.

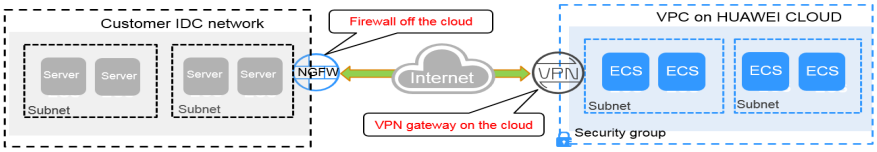
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

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

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

The negotiation parameters of the VPN connection use the default configurations defined on HUAWEI CLOUD.

Figure 6-1 Topology connection and policy negotiation configuration information



Your network		Interconnection mode description: 1. The Linux servers of customers are installed with IPsec software for interconnection. 2. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.	HUAWEI CLOUD network	
IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**		IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**
IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**		IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**
Authentication mode	Pre-shared key		Authentication mode	Pre-shared key
Customer gateway	22.22.22.22		HUAWEI CLOUD gateway	11.11.11.11
Customer subnet	192.168.200.0/24		HUAWEI CLOUD subnet	192.168.200.0/24

Configuration Procedure

This example describes the VPN configurations of two types of Openswan IPsec clients in Linux systems.

Step 1 Enable IPv4 forwarding.

```
vim /etc/sysctl.conf
net.ipv4.ip_forward = 1        //Add the content.
/sbin/sysctl -p                //Run the command to make the forwarding configuration take effect.
```

Step 2 Configure iptables.

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

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

Step 3 Configure the pre-shared key.

openswan

```
vim /etc/ipsec.d/open_ipsec.secrets          //Create and edit the open_ipsec.secrets file.
22.22.22.22 11.11.11.11 : psk "ipsec-key"
```

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

Step 4 Configure the IPsec connection.

```
vim /etc/ipsec.d/open_ipsec.conf      //Create and edit the open_ipsec.secrets file.
conn openswan_ipsec                        //Set the connection name to openswan_ipsec.
authby=secret                         //Set the authentication mode to PSK.
auto=start                            //The value can be add, route, or start.
ikev2=never                           //Disable the IKEv2 version.
ike=aes128-sha1;modp1536              //Define the IKE algorithm and group based on the configuration on
the customer side.
keyexchange=ike                       //IKE key exchange mode
ikelifetime=86400s                    //IKE phase lifecycle
phase2=esp                            //Phase two transmission format
```



```
phase2alg=aes128-sha1;modp1536 //Define the IPsec algorithm and group based on the configuration on the customer side.
compress=no                    //Disable compression.
pfs=yes                        //Enable PFS.
salifetime=3600s               //Lifecycle in phase two
type=tunnel                    //Enable the tunnel mode.
left=192.168.222.222           //Local IP address. Set it to the actual server IP address in the NAT scenario.
leftid=22.22.22.22             //Local ID
leftsourceip=22.22.22.22       //If the source is a private IP address, set this value to the IP address after NAT translation.
leftsubnet=192.168.222.0/24    //Local subnet
leftnexthop=22.22.22.1         //In the NAT scenario, set the value to the gateway IP address after NAT translation.
right=11.11.11.11              //VPN gateway IP address on the customer side
rightid=11.11.11.11            //Customer side ID
rightsourceip=11.11.11.11      //Set the source address on the customer side to the VPN gateway IP address.
rightsubnet=192.168.200.0/24   //Subnet on the customer side
rightnexthop=%defaultroute     //Configure the route on the customer side according to the default configurations.
```

Step 5 Start the service.

```
service ipsec stop                  //Stop the service.
service ipsec start                 //Start the service.
service ipsec restart               //Restart the service.
openswan auto -down openswan_ipsec  //Disable the connection.
openswan auto -up openswan_ipsec    //Enable the connection.
```

NOTE

- CentOS6.8 is required.
- Restart the service and then enable the connection after each modification.

----End

Configuration Verification

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

```
Connection list:
000
000 "openswan_ipsec":
192.168.222.0/24===192.168.222.222<192.168.222.222>[22.22.22.22]---22.22.22.1...11.11.11.11<11.11.11.11>
===192.168.200.0/24; erouted; eroute owner: #30
000 "openswan_ipsec":     oriented; my_ip=22.22.22.22; their_ip=11.11.11.11; my_updown=ipsec _updown;
000 "openswan_ipsec":   xauth us:none, xauth them:none,  my_username=[any]; their_username=[any]
000 "openswan_ipsec":   our auth:secret, their auth:secret
000 "openswan_ipsec":   modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset,
banner:unset, cat:unset;
000 "openswan_ipsec":   labeled_ipsec:no;
000 "openswan_ipsec":   policy_label:unset;
000 "openswan_ipsec":   ike_life: 86400s; ipsec_life: 3600s; replay_window: 32; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 0;
000 "openswan_ipsec":   retransmit-interval: 500ms; retransmit-timeout: 60s;
000 "openswan_ipsec":   initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-
esp-tfc:no;
000 "openswan_ipsec":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1_ALLOW+SAREF_TRACK
+IKE_FRAG_ALLOW+ESN_NO;
000 "openswan_ipsec":   conn_prio: 24,24; interface: eth0; metric: 0; mtu: unset; sa_prio:auto; sa_tfc:none;
000 "openswan_ipsec":   nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-
offload:auto;
000 "openswan_ipsec":   our idtype: ID_IPV4_ADDR; our id=119.3.88.8; their idtype: ID_IPV4_ADDR; their
id=122.112.222.188
000 "openswan_ipsec":   dpd: action:hold; delay:0; timeout:0; nat-t: encaps:auto; nat_keepalive:yes;
ikev1_natt:both
000 "openswan_ipsec":   newest ISAKMP SA: #3; newest IPsec SA: #30;
```



```
000 "openswan_ipsec":   IKE algorithms: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_ipsec":   IKE algorithm newest: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_ipsec":   ESP algorithms: AES_CBC_128-HMAC_SHA1_96-MODP1536
000 "openswan_ipsec":   ESP algorithm newest: AES_CBC_128-HMAC_SHA1_96; pfsgroup=MODP1536
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #3: "openswan_ipsec":4500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE
in 15087s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #30: "openswan_ipsec":4500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in
1744s; newest IPSEC; eroute owner; isakmp#3; idle; import:admin initiate
000 #30: "openswan_ipsec" esp.b810a24@11.11.11.11 esp.aab7b496@192.168.222.222 tun.0@11.11.11.11
tun.0@192.168.222.222 ref=0 refhim=0 Traffic: ESPin=106KB ESPout=106KB! ESPmax
=4194303B
```

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

Scenarios

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

Topology Connection

Figure 7-1 shows the topology connection and policy negotiation configurations.

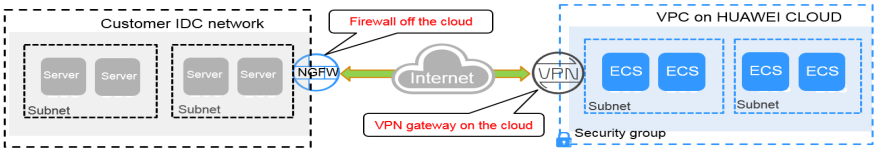
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

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

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

The negotiation parameters of the VPN connection use the default configurations defined on HUAWEI CLOUD.

Figure 7-1 Topology connection and policy negotiation configuration information



Your network		Interconnection mode description: 1. The Linux servers of customers are installed with IPsec software for interconnection. 2. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.	HUAWEI CLOUD network	
IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**		IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**
IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**		IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**
Authentication mode	Pre-shared key		Authentication mode	Pre-shared key
Customer gateway	22.22.22.22		HUAWEI CLOUD gateway	11.11.11.11
Customer subnet	192.168.200.0/24		HUAWEI CLOUD subnet	192.168.200.0/24

Configuration Procedure

This example describes the VPN configurations of two types of strongSwan IPsec clients in Linux systems.

Step 1 Install the IPsec VPN client.

```
yum install strongswan
```

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

Step 2 Enable IPv4 forwarding.

```
vim /etc/sysctl.conf
net.ipv4.ip_forward = 1        //Add the content.
 /sbin/sysctl –p               //Run the command to make the forwarding configuration take effect.
```

Step 3 Configure iptables.

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

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

Step 4 Configure the pre-shared key.

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

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

Step 5 Configure the IPsec connection.

```
vim /etc/strongswan / ipsec.conf           //Edit the ipsec.conf file.
config setup
conn strong_ipsec                          //Set the connection name to strong_ipsec.
```



```
auto=route                              //The value can be add, route, or start.
type=tunnel                             //Enable the tunnel mode.
compress=no                             //Disable compression.
leftauth=psk                            //Set the local authentication mode to PSK.
rightauth=psk                           //Set the authentication mode on the customer side to PSK.
ikelifetime=86400s                      //Lifecycle in IKE phase
lifetime=3600s                          //Lifecycle in phase two
keyexchange=ikev1                       //The IKE key exchange mode is version 1.
ike=aes128-sha1-modp1536!               //Define the IKE algorithm and group based on the configuration on the customer side.
esp=aes128-sha1-modp1536!               //Define the IPsec algorithm and group based on the configuration on the customer side.
leftid=22.22.22.22                      //Local ID
left=192.168.222.222                    //Local IP address. Set it to the actual server IP address in the NAT scenario.
leftsubnet=192.168.222.0/24             //Local subnet
rightid=11.11.11.11                     //Customer side ID
right=11.11.11.11                       //VPN gateway IP address on the customer side
rightsubnet=192.168.200.0/24            //Subnet on the customer side
```

After the configuration is complete, run the **ipsec verify** command to verify the configuration items in the Openswan scenario. But in the strongSwan scenario, verify the configuration items when the service is enabled. If all the command output is **OK**, the configuration is successful.

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

If the following error information is displayed:

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

Run the following commands:

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

Step 6 Start the service.

```
service strongswan stop             //Stop the service.
service strongswan start            //Start the service.
service strongswan restart          //Restart the service.
strongswan down strong_ipsec                //Disable the connection.
strongswan up strong_ipsec                  //Enable the connection.
```


NOTE

Restart the service and then enable the connection after each modification.

----End

Configuration Verification

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

```
Status of IKE charon daemon (strongSwan 5.7.2, Linux 3.10.0-957.5.1.el7.x86_64, x86_64):
  uptime: 5 minutes, since Apr 24 19:25:29 2019
  malloc: sbrk 1720320, mmap 0, used 593088, free 1127232
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 1
  loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha2 sha1 md4 md5 mgf1 random nonce x509
revocation constra
ints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519
chapoly x
cbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-
identity ea
p-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-
tls eap-ttls eap
-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp led duplicheck unity counters
Listening IP addresses:192.168.222.222
Connections:
strong_ipsec:  192.168.222.222...11.11.11.11  IKEv1
strong_ipsec:   local:  [22.22.22.22] uses pre-shared key authentication
strong_ipsec:   remote: [11.11.11.11] uses pre-shared key authentication
strong_ipsec:   child:  192.168.222.0/24 === 192.168.200.0/24 TUNNEL
Routed Connections:
strong_ipsec{1}:  ROUTED, TUNNEL, reqid 1
strong_ipsec{1}:   192.168.222.0/24 === 192.168.200.0/24
Security Associations (0 up, 1 connecting):
strong_ipsec[1]: CONNECTING, 192.168.222.222[%any]...11.11.11.11[%any]
strong_ipsec[1]: IKEv1 SPIs: c3090f6512ec6b7d_i* 0000000000000000_r
strong_ipsec[1]: Tasks queued: QUICK_MODE QUICK_MODE
strong_ipsec[1]: Tasks active: ISAKMP_VENDOR ISAKMP_CERT_PRE MAIN_MODE ISAKMP_CERT_POST
ISAKMP_NATD
Ping the server with IPsec client installed in VPC 2 from the VPC 1.
ping 192.168.222.222
PING 192.168.222.222 (192.168.222.222) 56(84) bytes of data.
64 bytes from 192.168.222.222: icmp_seq=1 ttl=62 time=3.07 ms
64 bytes from 192.168.222.222: icmp_seq=2 ttl=62 time=3.06 ms
64 bytes from 192.168.222.222: icmp_seq=3 ttl=62 time=3.98 ms
64 bytes from 192.168.222.222: icmp_seq=4 ttl=62 time=3.04 ms
64 bytes from 192.168.222.222: icmp_seq=5 ttl=62 time=3.11 ms
64 bytes from 192.168.222.222: icmp_seq=6 ttl=62 time=3.71 ms
```

8 Interconnecting HUAWEI CLOUD with Alibaba Cloud

Scenarios

Set up a VPN connection between HUAWEI CLOUD and Alibaba Cloud to transmit data between the two clouds.

Topology Connection

Figure 8-1 shows the topology connection in this scenario.

HUAWEI CLOUD VPC information

- VPN gateway: 139.139.139.2
- Subnets: 192.168.10.0/24 and 192.168.20.0/24

Alibaba Cloud VPC information

- VPN gateway: 39.39.39.2
- Subnets: 172.16.10.0/24 and 172.16.20.0/24

Figure 8-1 Topology connection

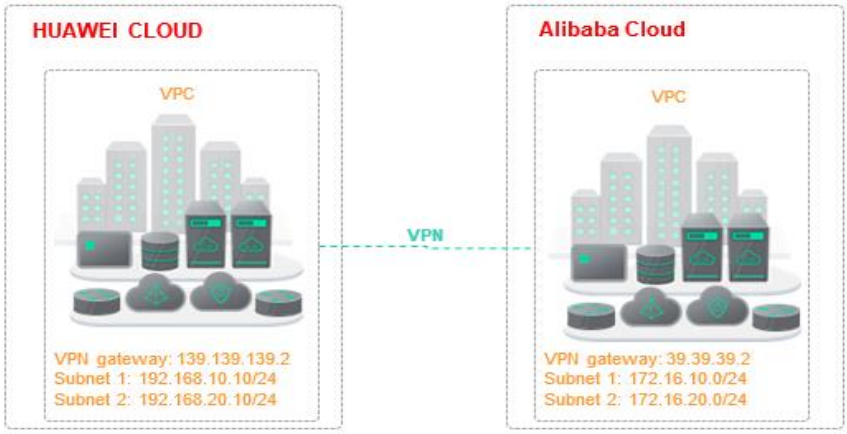
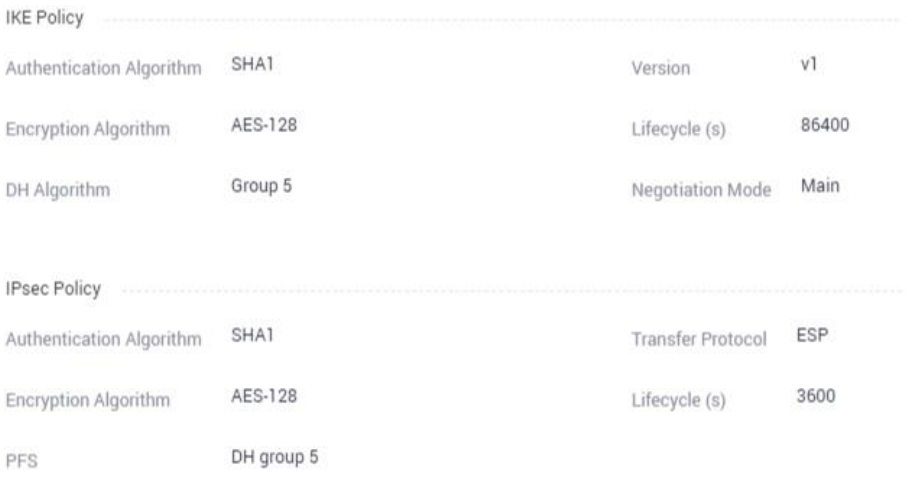


Figure 8-2 Interconnection policy



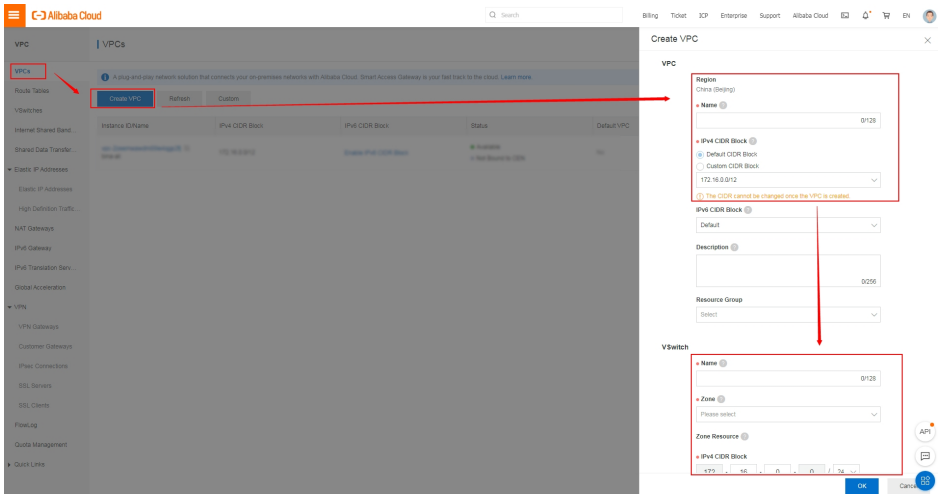
Configuration Procedure

Log in to the Alibaba Cloud console, and click **Products** and then **Virtual Private Cloud** under **Networking**. On the displayed page, create required VPC, VSwitch, VPN resources, and ECS to verify the connectivity between HUAWEI CLOUD and Alibaba Cloud.

Step 1 Create a VPC.

Choose **VPCs**, click **Create VPC**, enter the VPC name, set the CIDR block, and configure VSwitches. Two VSwitches with CIDR blocks 172.16.10.0/24 and 172.16.20.0/24 must be created. **Figure 8-3** shows the creation process.

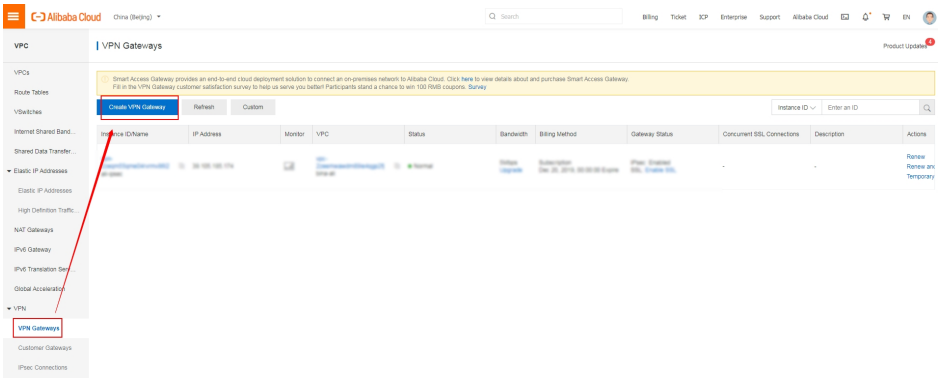
Figure 8-3 Create VPC



Step 2 Create VPN resources.

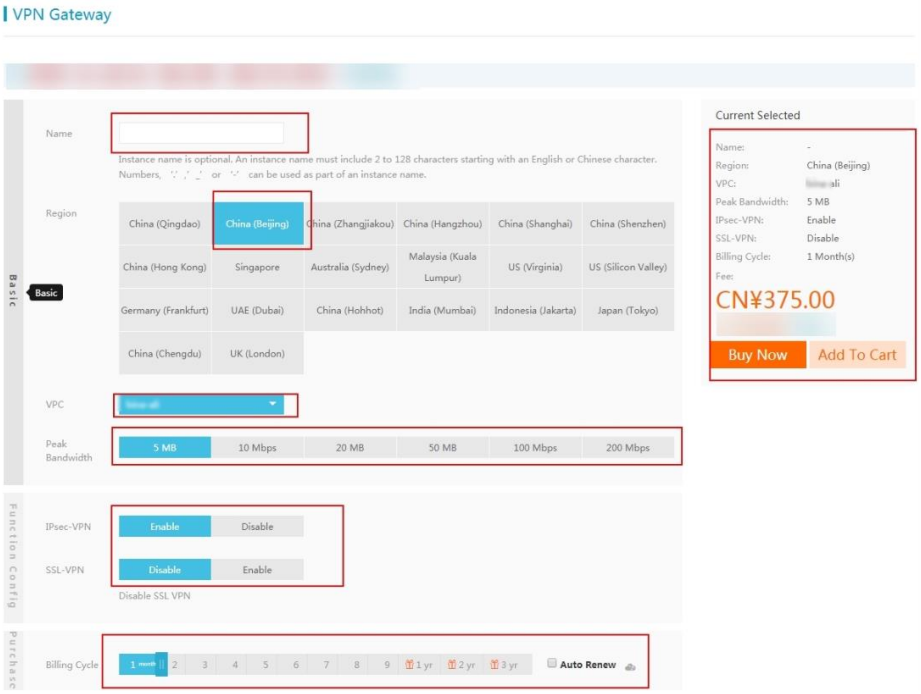
1. Create a VPN gateway. Choose **VPN Gateways** and click **Create VPN Gateway**.

Figure 8-4 Create VPN Gateway



On the displayed page, enter the name, select a region, VPC, and bandwidth, and specify the function configuration and billing cycle. The configuration information and price is displayed on the right in real time. In this example, the VPN gateway name is **ali-ipsec**, the region is **China (Beijing)**, and the bandwidth is **5 MB**. Only IPsec VPN is enabled and the billing cycle is one month. Then click **Buy Now**.

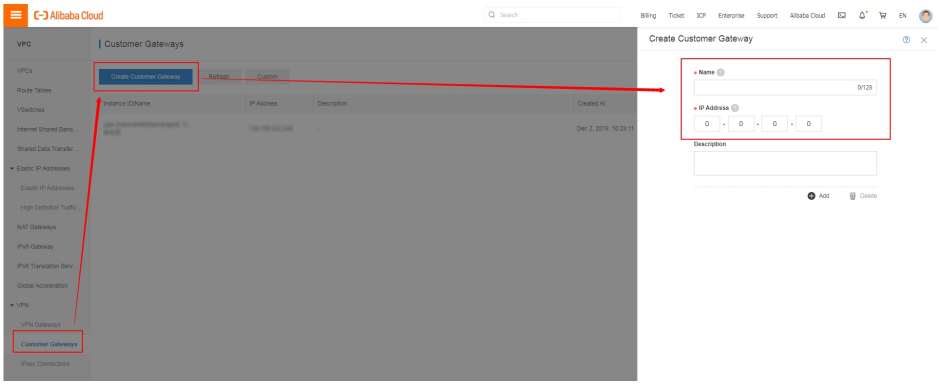
Figure 8-5 Create VPN Gateway



2. Create a customer gateway.

   Choose **Customer Gateways** and click **Create Customer Gateway**. On the displayed page, enter the customer gateway name and the IP address (139.139.139.2) of the VPN gateway on the HUAWEI CLOUD side, and click **OK**.

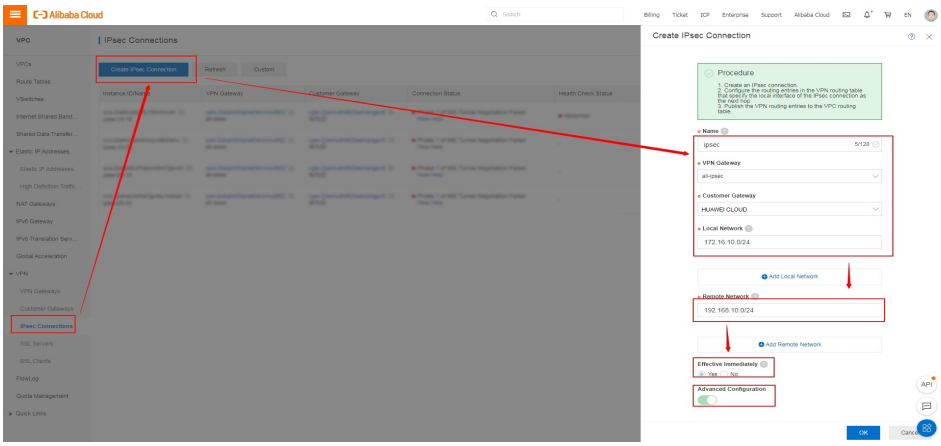
Figure 8-6 Create Customer Gateway



3. Create an IPsec connection.

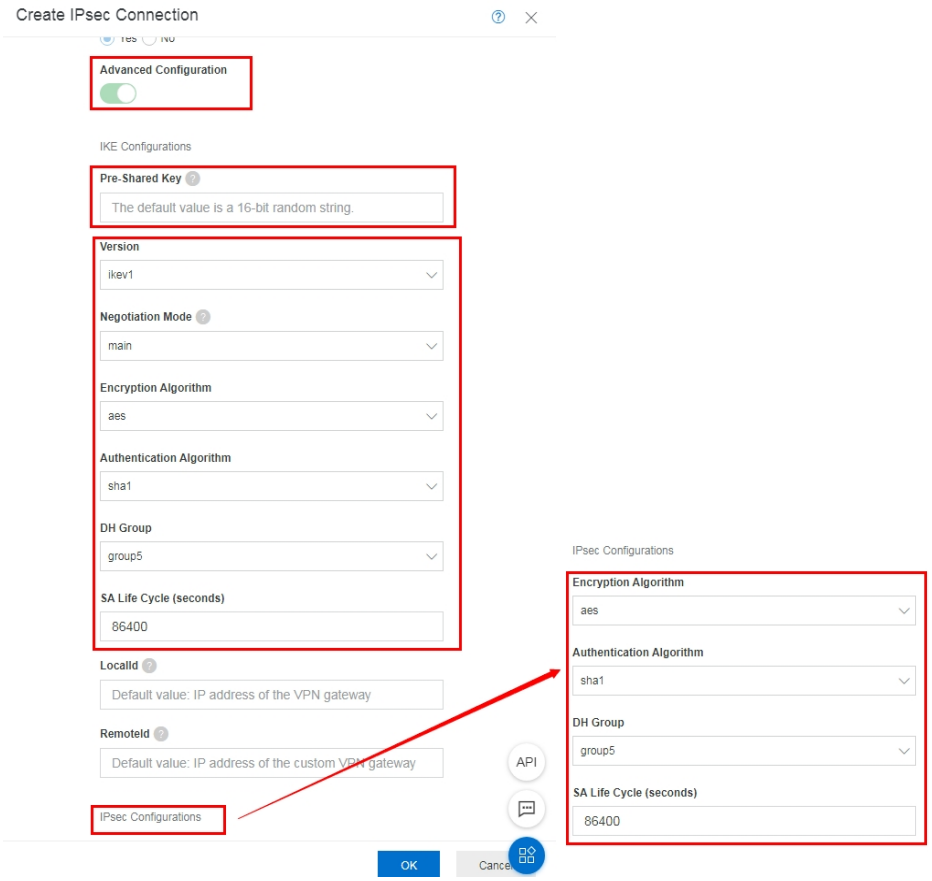
   Choose **IPsec Connection** under **VPN** and click **Create IPsec Connection**. On the displayed page, enter the name of the connection, for example, **TO-HW**. Set **VPN Gateway** to **ali-ipsec** created in step 1, **Customer Gateway** to the gateway of the HUAWEI CLOUD side created in step 2, and **Local Network** to the first VSwitch subnet. Select the first remote subnet for **Remote Network** and set **Effective Immediately** to **Yes**. Figure 8-7 shows the configuration process.

Figure 8-7 Create IPsec Connection



   Enable **Advanced Configuration** and modify the advanced configuration (that is, the negotiation policy of the VPN connection) to be the same as the preset configuration.

Figure 8-8 Advanced Configuration



NOTE

To connect Alibaba Cloud to HUAWEI CLOUD, if each side has one subnet, the IPsec VPN connection configuration is complete after performing the preceding steps. If each side has more than one subnet, creating one IPsec connection on HUAWEI CLOUD is enough. Configure the local and remote subnets based on site requirements. In this example, the subnets on HUAWEI CLOUD are 192.168.10.0/24 and 192.168.20.0/24, and the subnets on Alibaba Cloud are 172.16.10.0/24 and 172.16.20.0/24. Alibaba Cloud requires four connections. Configure the subnets to 172.16.10.0/24 (Alibaba Cloud) and 192.168.10.0/24 (HUAWEI CLOUD), 172.16.10.0/24 (Alibaba Cloud) and 192.168.20.0/24 (HUAWEI CLOUD), 172.16.20.0/24 (Alibaba Cloud) and 192.168.10.0/24 (HUAWEI CLOUD), and 172.16.20.0/24 (Alibaba Cloud) and 192.168.20.0/24 (HUAWEI CLOUD), correspondingly.

Figure 8-9 shows the HUAWEI CLOUD VPN connection configuration.

Figure 8-9 HUAWEI CLOUD VPN connection

Figure 8-10 shows the Alibaba Cloud IPsec connection configuration.

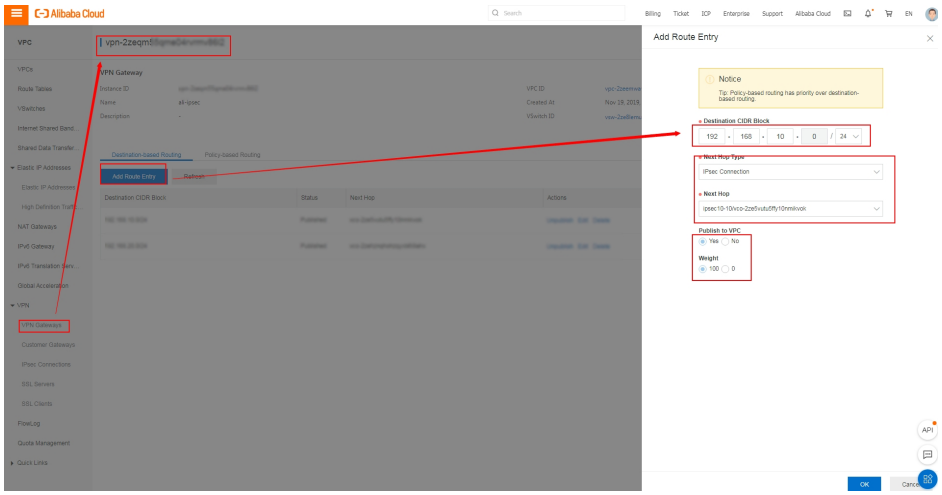
Figure 8-10 Alibaba Cloud IPsec connection

Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status
vco-2ze5vu... ipsec10-10	vpn-2zeq... ali-ipsec	cgw-2z... HUAWEI CLOUD	Phase 1 of IKE Tunnel Negotiation Failed View Help
vco-2zehzn... ipsec10-20	vpn-2zeq... ali-ipsec	cgw-2z... HUAWEI CLOUD	Phase 1 of IKE Tunnel Negotiation Failed View Help
vco-2zeah9... ipsec20-10	vpn-2zeq... ali-ipsec	cgw-2z... HUAWEI CLOUD	Phase 1 of IKE Tunnel Negotiation Failed View Help
vco-2zeheu... ipsec20-20	vpn-2zeq... ali-ipsec	cgw-2z... HUAWEI CLOUD	Phase 1 of IKE Tunnel Negotiation Failed View Help

Step 3 Add routes.

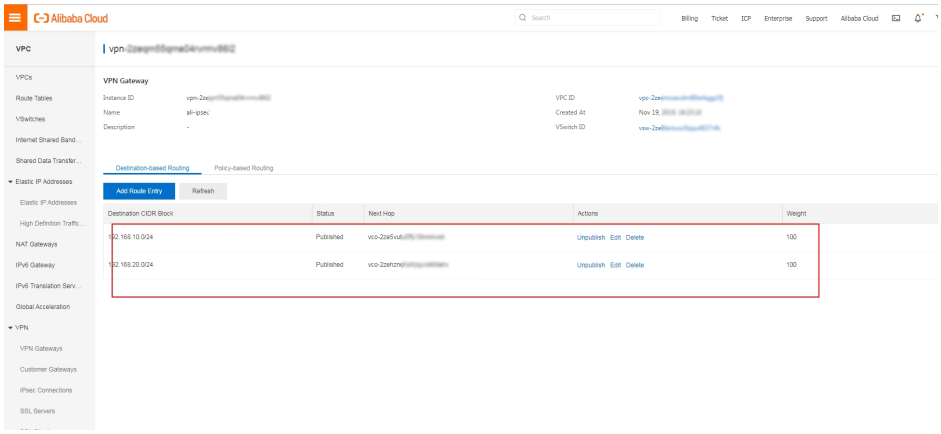
After the VPN connection is created, the system automatically displays the message indicating that the IPsec connection is created successfully and you can choose whether to add routes to the VPN gateway now. If you add a route later, choose **VPN Gateways**. In the VPN gateway list, click the ID of the gateway that you want to add a route to and click **Add Route Entry** on the displayed page. Set **Destination CIDR Block** to **192.168.10.0/24**, **Next Hop Type** to **IPsec Connection**, and **Next Hop** to the gateway ID of the TO-HW connection. Remain the default values for **Publish to VPC** and **Weight**. You can repeat the preceding steps to add routes as required.

Figure 8-11 Adding a route



After the routes have been added, the list information as shown in **Figure 8-12** is displayed.

Figure 8-12 Added routes



----End

After the IPsec VPN configuration on Alibaba Cloud is complete, Alibaba Cloud automatically initiates connection negotiation with HUAWEI CLOUD. To verify data connectivity, you need to create an ECS on the VPC.

Configuration Verification

If VPCs of Alibaba Cloud and HUAWEI CLOUD each has one subnet, the two VPC subnets can communicate with each other through the IPsec VPN connection after the preceding configuration is complete.

If one VPC has M subnets but the other has N subnets, one VPN connection is enough on HUAWEI CLOUD and you can configure multiple CIDR blocks for the **Local Subnet** and **Remote Subnet** parameters. You need to create M x N VPN connections on Alibaba Cloud and each connection has one local subnet and one remote subnet.

In this example, subnets in the HUAWEI CLOUD VPC are 192.168.10.0/24 and 192.168.20.0/24, and subnets in the Alibaba Cloud VPC are 172.16.10.0/24 and 172.16.20.0/24. One connection created on HUAWEI CLOUD is configured with local subnets 192.168.10.0/24 and 192.168.20.0/24, and remote subnets 172.16.10.0/24 and 172.16.20.0/24. Four connections created on Alibaba Cloud are configured with local and remote subnets 172.16.10.0/24 and 192.168.10.0/24, 172.16.10.0/24 and 192.168.20.0/24, 172.16.20.0/24 and 192.168.10.0/24, and 172.16.20.0/24 and 192.168.20.0/24, respectively.