Virtual Private Network

Pasos iniciales

Edición	01
Fecha	2025-01-21

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: https://www.huawei.com

Email: support@huawei.com

1 Preparaciones

Antes de usar VPN, realice los siguientes preparativos:

Registro en Huawei Cloud y finalización de la autenticación con nombre real

Omita esta parte si ya tiene la cuenta de Huawei Cloud. Si no tiene una cuenta de Huawei Cloud, realice los siguientes pasos para crearla:

1. Visite el **sitio web oficial de Huawei Cloud** y haga clic en **Regístrese**.
2. Complete la creación como se le solicite. Para obtener más información, consulte **Registro con Huawei Cloud**.

   Si la creación se realiza correctamente, el sistema le redirige automáticamente a su página de información personal.
3. Complete la autenticación de nombre real siguiendo las instrucciones de **Autenticación individual de nombre real**.

Recarga de su cuenta

Asegúrese de que el saldo de la cuenta sea suficiente.

- Para obtener información sobre los precios de VPN, consulta **Detalles de Precios**.

2 Configuración de Enterprise Edition VPN para conectar un centro de datos local y una VPC

2.1 Descripción general

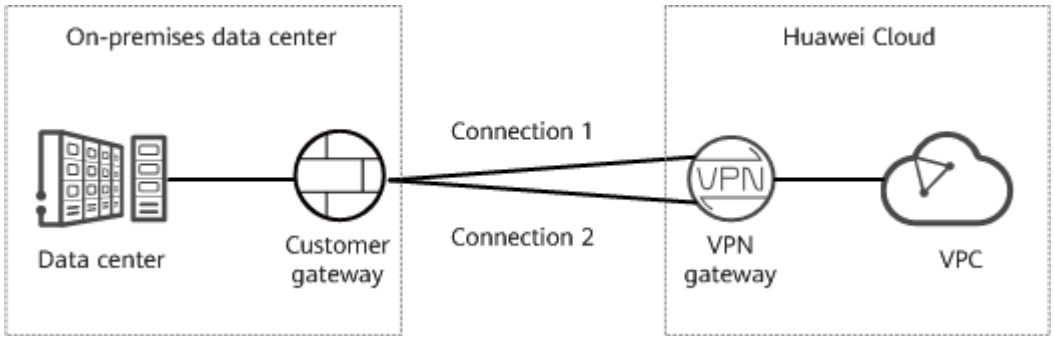
Regiones admitidas

AP-Bangkok, CN-Hong Kong, AP-Singapore, AP-Jakarta, TR-Istanbul, LA-Mexico City1, and LA-Mexico City2

Escenario

Para cumplir con los requisitos de desarrollo empresarial, la empresa A necesita implementar la comunicación entre su centro de datos local y su VPC. En este caso, la empresa A puede utilizar el servicio VPN para crear conexiones entre el centro de datos local y la VPC, como se muestra en **Figura 2-1**.

Figura 2-1 Red de VPN



Esta solución tiene los siguientes requisitos para el centro de datos local y el dispositivo de gateway del cliente:

- El dispositivo de gateway del cliente debe admitir los protocolos IKE e IPsec estándar.

- El gateway del cliente tiene una dirección IP pública estática.
- Las subredes del centro de datos local que necesitan acceder a la VPC no se superponen con las subredes de VPC ni contienen 100.64.0.0/10 o 214.0.0.0/8.

  Si la VPC utiliza conexiones de Direct Cloud o de Cloud Connect para comunicarse con otras VPC, las subredes del centro de datos local no pueden solaparse con las de estas VPC.

Plan de datos

Tabla 2-1 Plan de datos

Categoría	Concepto	Datos
VPC	Subred que necesita acceder al centro de datos local	192.168.0.0/16
Gateway de VPN	Subred de interconexión	Esta subred se utiliza para la comunicación entre el gateway de VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables. 192.168.2.0/24
	EIP	Las EIP se generan automáticamente al comprarlas. De forma predeterminada, un gateway de VPN utiliza dos EIP. En este ejemplo, las EIP son las siguientes: ● EIP activa: 11.xx.xx.11 ● EIP en espera: 11.xxx.xx.12
Conexión de VPN	Dirección de la interfaz del túnel	Esta dirección es utilizada por un gateway de VPN para establecer un túnel IPsec con un gateway de cliente. En los dos extremos del túnel IPsec, se deben invertir las direcciones de interfaz de túnel local y remoto configuradas. ● Conexión 1 de VPN: 169.254.70.1/30 ● Conexión 2 de VPN: 169.254.71.1/30
Centro de datos local	Subred que necesita acceder a la VPC	172.16.0.0/16
Gateway del cliente	dirección IP de la gateway	La dirección IP del gateway es asignada por un operador. En este ejemplo, la dirección IP del gateway es: 22.xx.xx.22
	Dirección de la interfaz del túnel	● Conexión 1 de VPN: 169.254.70.2/30 ● Conexión 2 de VPN: 169.254.71.2/30

Procedimiento operativo

Figura 2-2 muestra el proceso de uso del servicio VPN para permitir la comunicación entre un centro de datos local y una VPC.

Figura 2-2 Procedimiento operativo

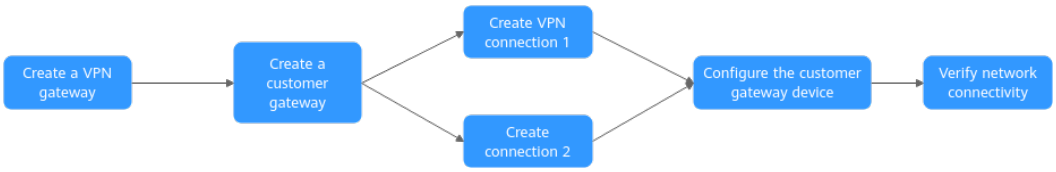


Tabla 2-2 Descripción del proceso de operación

N.º	Paso	Descripción
1	**2.2 Paso 1: Creación de un gateway de VPN**	Vincule dos EIPs al gateway de VPN. Si ha comprado las EIP, puede vincularlas directamente al gateway de VPN.
2	**2.3 Paso 2: Creación de un gateway de cliente**	Configure el dispositivo VPN en el centro de datos local como el gateway del cliente.
3	**2.4 Paso 3: Creación de la conexión 1 de VPN**	Cree una conexión de VPN entre la EIP activa del gateway de VPN y el gateway del cliente.
4	**2.5 Paso 4: Creación de una conexión 2 de VPN**	Cree una conexión de VPN entre la EIP en espera del gateway de VPN y el gateway del cliente. Se recomienda que el modo de enrutamiento, la política PSK, IKE y la configuración de la política IPsec de las dos conexiones VPN sean iguales.
5	**2.6 Paso 5: Configuración del dispositivo de gateway del cliente**	● Las direcciones de interfaz local y remota configuradas en el dispositivo de gateway del cliente deben ser las mismas que las direcciones de interfaz del cliente y local de la conexión de VPN de Huawei Cloud, respectivamente. ● El modo de enrutamiento, la política PSK, IKE y la configuración de la política IPsec en el dispositivo de gateway del cliente deben ser los mismos que los de la conexión de VPN de Huawei Cloud.
6	**2.7 Paso 6: Verificación de la conectividad de red**	Inicie sesión en un ECS y ejecute el comando **ping** para verificar la conectividad de red.

2.2 Paso 1: Creación de un gateway de VPN

Requisitos previos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte **Creación de una VPC y subred**.
- Las reglas de grupo de seguridad se han configurado para los ECS en la VPC y permiten que el gateway del cliente en el centro de datos local acceda a los recursos de la VPC. Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Reglas de grupo de seguridad**.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.

Paso 3 Elija **Virtual Private Network** > **Enterprise – VPN Gateways** y haga clic en **Buy VPN Gateway**.

Paso 4 Defina los parámetros según se le solicite y haga clic en **Next**.

A continuación se describen solo los parámetros clave. Para obtener más información sobre más parámetros, consulte **Crear un gateway de VPN**.

Tabla 2-3 Parámetros clave del gateway de VPN

Parámetro	Descripción	Valor de ejemplo
Billing Mode	Las opciones incluyen **Yearly/Monthly** y **Pay-per-use**.	Yearly/Monthly
Region	Seleccione la región más cercana a usted.	AP-Singapore
Name	Asigne un nombre a un gateway de VPN.	vpngw-001
Network Type	• **Public network**: Un gateway de VPN se comunica con un gateway del cliente en un centro de datos local con Internet. • **Private network**: Un gateway de VPN se comunica con un gateway del cliente en un centro de datos local con una red privada.	Public network
Associate With	Las opciones incluyen **VPC** y **Enterprise Router**	VPC
VPC	Seleccione la VPC que necesita para acceder al centro de datos local.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Esta subred se utiliza para la comunicación entre el gateway de VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables.	192.168.2.0/24

Parámetro	Descripción	Valor de ejemplo
Local Subnet	Especifique la subred de VPC que necesita acceder al centro de datos local. Puede introducir manualmente un bloque CIDR o seleccionar una subred en el cuadro de lista desplegable.	192.168.0.0/24
Active EIP	Puede comprar una nueva EIP o utilizar una EIP existente.	11.xx.xx.11
Standby EIP		11.xx.xx.12

----Fin

Verificación

Compruebe el gateway de VPN creado en la página **VPN Gateways**. El estado inicial del gateway de VPN es **Creating**. Después de unos 2 minutos, el estado cambia a **Normal**, lo que indica que el gateway de VPN se ha creado correctamente.

2.3 Paso 2: Creación de un gateway de cliente

Procedimiento

Paso 1 Elija **Virtual Private Network** > **Enterprise – Customer Gateways** y haga clic en **Create Customer Gateway**.

Paso 2 Defina los parámetros según se le solicite y haga clic en **OK**.

A continuación se describen solo los parámetros clave. Para obtener más información acerca de más parámetros, consulte **Creación de un gateway de cliente**.

Tabla 2-4 Parámetros del gateway del cliente

Parámetro	Descripción	Valor de ejemplo
Name	Asigne un nombre a un gateway de cliente.	cgw-001
Routing Mode	Seleccione **Static**.	Static
Gateway IP Address	Introduzca la dirección IP del gateway del cliente en el centro de datos local.	22.xx.xx.22

----Fin

Verificación

Compruebe el gateway de cliente creado en la página **Customer Gateways**.

2.4 Paso 3: Creación de la conexión 1 de VPN

Procedimiento

1. Elija **Virtual Private Network** > **Enterprise – VPN Connections** y haga clic en **Buy VPN Connection**.
2. Establezca los parámetros para la conexión de VPN 1 como se le solicite y haga clic en **Submit**.

   A continuación se describen solo los parámetros clave. Para obtener más información sobre más parámetros, consulte **Crear una conexión VPN**.

Tabla 2-5 Configuración de parámetros para la conexión 1 de VPN

Parámetro	Descripción	Valor de ejemplo
Name	Introduzca el nombre de la conexión 1 de VPN.	vpn-001
VPN Gateway	Seleccione el gateway de VPN creada en **2.2 Paso 1: Creación de un gateway de VPN**.	vpngw-001
Gateway IP Address	Seleccione la EIP activa del gateway de VPN.	11.xx.xx.11
Customer Gateway	Seleccione el gateway de cliente creado en **2.3 Paso 2: Creación de un gateway de cliente**.	cgw-001
VPN Type	Seleccione **Static routing**.	Static routing
Customer Subnet	Introduzca la subred del centro de datos local que necesita acceder a la VPC.	172.16.0.0/16
Interface IP Address Assignment	Las opciones incluyen **Manually specify** y **Automatically assign**.	Manually specify
Local Interface IP Address	Especifique la dirección IP del túnel del gateway de VPN. **NOTA** Las direcciones de interfaz local y remota configuradas en el dispositivo de gateway del cliente deben ser las mismas que los valores de **Customer Interface IP Address** y **Local Interface IP Address** respectivamente.	169.254.70.2/30
Customer Interface IP Address	Especifique la dirección IP del túnel del gateway del cliente.	169.254.70.1/30

Parámetro	Descripción	Valor de ejemplo
Link Detection	Esta función se utiliza para la detección de confiabilidad de ruta en escenarios de enlaces múltiples. **NOTA** Al habilitar esta función, asegúrese de que el gateway del cliente sea compatible con ICMP y esté correctamente configurada con la dirección IP de la interfaz del cliente de la conexión de VPN. De lo contrario, el tráfico de VPN no se reenviará.	**NQA** enabled
PSK, Confirm PSK	Especifique la clave de negociación de la conexión de VPN. Las PSK configuradas en la consola de VPN y el dispositivo de gateway del cliente deben ser las mismas.	Test@123
Policy Settings	Configure las políticas IKE e IPsec, que definen los algoritmos de encriptación utilizados por el túnel de VPN. La configuración de política en la consola de VPN y el dispositivo de gateway del cliente debe ser la misma.	Predeterminado

Verificación

Compruebe la conexión de VPN creada en la página **VPN Connections**. El estado inicial de la conexión de VPN es **Creating**. Como el dispositivo de gateway del cliente no se ha configurado, no se puede establecer ninguna conexión de VPN. Después de unos 2 minutos, el estado de la conexión de VPN cambia a **Not connected**.

2.5 Paso 4: Creación de una conexión 2 de VPN

Procedimiento

1. Elija **Virtual Private Network** > **Enterprise – VPN Connections** y haga clic en **Buy VPN Connection**.
2. Establezca los parámetros para la conexión de VPN 2 como se le solicite y haga clic en **Submit**.

   Para la conexión 2 de VPN, se recomienda utilizar la misma configuración que para la conexión 1 de VPN, excepto el nombre de la conexión, la dirección IP del gateway, la dirección IP de la interfaz local y la dirección IP de la interfaz de cliente.

Tabla 2-6 Configuración de parámetros para la conexión 2 de VPN

Parámetro	Descripción	Valor de ejemplo
Name	Introduzca el nombre de la conexión 2 de VPN.	vpn-002
VPN Gateway	Seleccione el gateway de VPN creada en **2.2 Paso 1: Creación de un gateway de VPN**.	vpngw-001
Gateway IP Address	Seleccione la EIP en espera del gateway de VPN.	11.xx.xx.12
Customer Gateway	Seleccione el gateway de cliente creado en **2.3 Paso 2: Creación de un gateway de cliente**.	cgw-001
VPN Type	Seleccione **Static routing**.	Static routing
Customer Subnet	Introduzca la subred del centro de datos local que necesita acceder a la VPC.	172.16.0.0/16
Interface IP Address Assignment	Las opciones incluyen **Manually specify** y **Automatically assign**.	Manually specify
Local Interface IP Address	Especifique la dirección IP del túnel del gateway de VPN. **NOTA** Las direcciones de interfaz local y remota configuradas en el dispositivo de gateway del cliente deben ser las mismas que los valores de **Customer Interface IP Address** y **Local Interface IP Address** respectivamente.	169.254.71.2/30
Customer Interface IP Address	Especifique la dirección IP del túnel del gateway del cliente.	169.254.71.1/30
Link Detection	Esta función se utiliza para la detección de confiabilidad de ruta en escenarios de enlaces múltiples. **NOTA** Al habilitar esta función, asegúrese de que el gateway del cliente sea compatible con ICMP y esté correctamente configurada con la dirección IP de la interfaz del cliente de la conexión de VPN. De lo contrario, el tráfico de VPN no se reenviará.	**NQA** enabled

Parámetro	Descripción	Valor de ejemplo
PSK, Confirm PSK	Especifique la clave de negociación de la conexión de VPN. Las PSK configuradas en la consola de VPN y el dispositivo de gateway del cliente deben ser las mismas.	Test@123
Policy Settings	Configure las políticas IKE e IPsec, que definen los algoritmos de encriptación utilizados por el túnel de VPN. La configuración de política en la consola de VPN y el dispositivo de gateway del cliente debe ser la misma.	Default

Verificación

Compruebe la conexión de VPN creada en la página **VPN Connections**. El estado inicial de la conexión de VPN es **Creating**. Como el dispositivo de gateway del cliente no se ha configurado, no se puede establecer ninguna conexión de VPN. Después de unos 2 minutos, el estado de la conexión de VPN cambia a **Not connected**.

2.6 Paso 5: Configuración del dispositivo de gateway del cliente

Procedimiento

NOTA

En este ejemplo, el dispositivo de gateway del cliente es un router AR de Huawei. Para obtener más ejemplos de configuración de dispositivos de gateway del cliente, consulte la **Guía del Administrator**.

Paso 1 Inicie sesión en el router AR.

Paso 2 Ingrese a la vista del sistema.

<AR651>system-view

Paso 3 Configure una dirección IP para la interfaz WAN. En este ejemplo, la interfaz WAN del router AR es 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

Paso 4 Configure una ruta predeterminada.

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

En este comando, *22.xx.xx.1* es la dirección de gateway de la dirección IP pública del router AR. Reemplácelo con la dirección de gateway real.

Paso 5 Habilite el algoritmo SHA-2 para que sea compatible con los algoritmos RFC estándar.

```
[AR651]IPsec authentication sha2 compatible enable
```

Paso 6 Configure una propuesta de IPsec.

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

Paso 7 Configure una propuesta IKE.

```
[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
```

Paso 8 Configure una propuesta IKE de pares.

```
[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

[AR651-ike-peer-hwpeer2]quit

Los comandos se describen de la siguiente manera:

- **pre-shared-key cipher**: configura una PSK, que debe ser la misma que la configurada en la consola de VPN.
- **local-address**: especifica la dirección IP pública del router AR.
- **remote-address**: especifica la EIP activa o en espera del gateway de VPN.

Paso 9 Configure un perfil IPsec.

[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

Paso 10 Configurar interfaces de túnel virtual.

[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
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

Los comandos se describen de la siguiente manera:

- **interface Tunnel0/0/1** e **interface Tunnel0/0/2** indican las interfaces de túnel correspondientes a las dos conexiones de VPN.

  En este ejemplo, Tunnel0/0/1 establece una conexión de VPN con la EIP activa del gateway de VPN, y Tunnel0/0/2 establece una conexión de VPN con la EIP en espera del gateway de VPN.
- **ip address**: configura una dirección IP para una interfaz de túnel en el router AR.
- **source**: especifica la dirección IP pública del router AR.
- **destination**: especifica la EIP activa o en espera del gateway de VPN.

Paso 11 Configurar 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
```

Los comandos se describen de la siguiente manera:

- **nqa test-instance IPsec_nqa1 IPsec_nqa1** y **nqa test-instance IPsec_nqa2 IPsec_nqa2**: configuran dos instancias de prueba de NQA denominadas **IPsec_nqa1** y **IPsec_nqa2**.

  En este ejemplo, se crea la instancia de prueba **IPsec_nqa1** para la conexión de VPN a la que pertenece la EIP activa del gateway de VPN; se crea la instancia de prueba **IPsec_nqa2** para la conexión de VPN a la que pertenece la EIP en espera del gateway de VPN.
- **destination-address**: especifica la dirección de la interfaz de túnel del gateway de VPN.
- **source-address**: especifica la dirección de la interfaz de túnel del router AR.

Paso 12 Configure la asociación entre la ruta estática y 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

Los parámetros se describen de la siguiente manera:

- **192.168.0.0** indica la subred local de la VPC.
- **Tunnel***x* y **IPsec_nqa***x* en el mismo comando corresponden a la misma conexión de VPN.

----Fin

Verificación

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.

Paso 3 Elija **Virtual Private Network** > **Enterprise – VPN Connections**. Verifique que los estados de las dos conexiones de VPN sean **Available** ambos.

----Fin

2.7 Paso 6: Verificación de la conectividad de red

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.

Paso 3 Haga clic en **Service List** y elija **Compute** > **Elastic Cloud Server**.

Paso 4 Inicie sesión en un ECS.

Hay varios métodos disponibles para iniciar sesión en un ECS. Para obtener más información, consulte **Iniciar sesión en un ECS**.

En este ejemplo, utilice VNC proporcionado en la consola de gestión para iniciar sesión en un ECS.

Paso 5 Ejecute el siguiente comando en el ECS:

ping 172.16.0.100

172.16.0.100 es la dirección IP de un servidor en el centro de datos local. Reemplácelo con una dirección IP del servidor real.

Si se muestra información similar a la siguiente, la VPC en la nube y el centro de datos local pueden comunicarse entre sí.

```
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
```

----Fin

3 Proceso de compra de VPN clásica

3.1 Descripción general

El proceso de configuración de las VPN clásicas varía en diferentes regiones, como se describe en **Tabla 3-1**.

Tabla 3-1 Descripción general

Regiones admitidas	CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg y LA-Santiago	LA-Mexico City1 y LA-Sao Paulo1
Creación de VPN	Realice los siguientes pasos en secuencia: 1. **3.3 Adquisición de un gateway de VPN** 2. **3.4 Adquisición de una conexión de VPN** 3. **3.5 Configuración del dispositivo remoto**	Realice los siguientes pasos en secuencia: 1. **Creación de una VPN (LA-Mexico City1/LA-Sao Paulo1)** 2. **3.5 Configuración del dispositivo remoto**

3.2 Compra de una VPN (LA-Mexico City1/LA-Sao Paulo1)

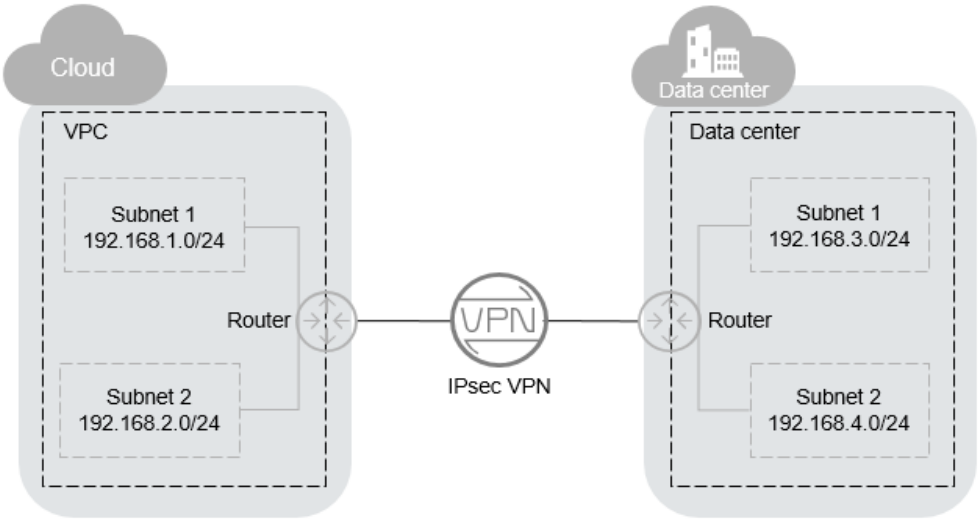
Descripción general

De forma predeterminada, los ECS de una VPC no pueden comunicarse con los dispositivos de su centro de datos local o red privada. Para habilitar la comunicación entre ellos, puede usar una VPN creándola en su VPC y actualizando las reglas del grupo de seguridad.

Topología de IPsec VPN

En **Figura 3-1**, la VPC tiene subredes 192.168.1.0/24 y 192.168.2.0/24. Su centro de datos local tiene subredes 192.168.3.0/24 y 192.168.4.0/24. Puede usar VPN para permitir que las subredes de la VPC se comuniquen con las de su centro de datos.

Figura 3-1 VPN sobre IPsec



Huawei Cloud admite la VPN de sitio a sitio para permitir la comunicación entre subredes de VPC y subredes de centros de datos locales. Antes de establecer una VPN IPsec, asegúrese de que el centro de datos local donde se va a establecer la VPN cumple las siguientes condiciones:

- Los dispositivos locales que admiten el protocolo IPsec estándar están disponibles.
- Los dispositivos locales tienen direcciones IP públicas fijas, que pueden ser configuradas estáticamente o traducidas por NAT.
- Las subredes locales no entran en conflicto con las subredes de VPC, y los dispositivos de las subredes locales pueden comunicarse con los dispositivos locales.

Si se cumplen las condiciones anteriores, asegúrese de que las políticas de IKE y de IPsec en ambos extremos sean consistentes y que las subredes en ambos extremos sean pares coincidentes al configurar IPsec VPN.

Una vez completada la configuración, la negociación de VPN debe ser activada por flujos de datos de red privada.

Escenarios

Necesita una VPN que configure un túnel de comunicaciones seguro y aislado entre su centro de datos local y los servicios en la nube.

Requisitos previos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte **Creación de una VPC y subred**.

- Se han configurado reglas de grupo de seguridad para la VPC, y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Reglas de grupo de seguridad**.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.
4. En la página **Virtual Private Network**, haga clic en **Buy VPN**.
5. Configure los parámetros requeridos y haga clic en **Next**.

   Tabla 3-2, **Tabla 3-3** y **Tabla 3-4** enumera los parámetros y sus descripciones.

Tabla 3-2 Parámetros básicos

Parámetro	Descripción	Valor de ejemplo
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre regiones. Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a los usuarios de destino.	AP-Singapore
Billing Mode	Las VPN se facturan sobre una base de pago por uso.	Pay-per-use
Name	El nombre de la VPN	VPN-001
VPC	El nombre de la VPC	VPC-001
Local Subnet	Subredes de VPC que accederán a su red local con una VPN.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	La dirección IP pública del gateway en su centro de datos o en la red privada. Esta dirección IP se utiliza para comunicarse con su VPC.	N/A
Remote Subnet	Las subredes de su red local que accederán a una VPC con una VPN. Las subredes remota y local no pueden solaparse entre sí. Las subredes remotas no pueden superponerse con bloques CIDR implicados en las interconexiones de VPC existentes creadas para la VPC.	192.168.3.0/24, 192.168.4.0/24

Parámetro	Descripción	Valor de ejemplo
PSK	Clave privada compartida por dos extremos de una conexión de VPN para negociación. Las PSK configuradas en ambos extremos de la conexión de VPN deben ser las mismas. La PSK puede contener de 6 a 128 caracteres.	Test@123
Confirm PSK	Ingrese la PSK de nuevo.	Test@123
Advanced Settings	● **Default**: Utilice las políticas de IKE y de IPsec predeterminadas. ● **Custom**: Utilice políticas IKE e IPsec personalizadas. Para más detalles, véase **Tabla 3-3** y **Tabla 3-4**.	Custom

Tabla 3-3 Política de IKE

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256

Parámetro	Descripción	Valor de ejemplo
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128
DH Algorithm	Algoritmo de intercambio de claves Diffie-Hellman. Se admiten los siguientes algoritmos: ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Group 14 El valor predeterminado es **Group 14**.	Group 14
Version	Versión del protocolo de IKE. El valor puede ser uno de los siguientes: ● v1 (no recomendado debido a riesgos de seguridad) ● v2 El valor predeterminado es **v2**.	v2
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **86400**.	86400
Negotiation Mode	Este parámetro solo está disponible cuando **Version** está establecido en **v1**. Puede establecer **Negotiation Mode** en **Main** o **Aggressive**. El modo predeterminado es **Main**.	Main

Tabla 3-4 Política de IPsec

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128
PFS	Algoritmo utilizado por la función Perfect forward secrecy (PFS). PFS admite los siguientes algoritmos: ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH group 14 El algoritmo predeterminado es **DH group 14**.	DH group 14

Parámetro	Descripción	Valor de ejemplo
Transfer Protocol	Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos de usuario. Se admiten los siguientes protocolos: ● AH ● AH-ESP El protocolo predeterminado es **ESP**.	ESP
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **3600**.	3600

NOTA

Una política de IKE especifica los algoritmos de encriptación y autenticación que se utilizarán en la fase de negociación de un túnel IPsec. Una política de IPsec especifica el protocolo, el algoritmo de encriptación y el algoritmo de autenticación que se utilizarán en la fase de transmisión de datos de un túnel de IPsec. Las políticas de IKE y de IPsec deben ser las mismas en ambos extremos de una conexión de VPN. Si son diferentes, la conexión de VPN no se puede configurar.

No se recomiendan los siguientes algoritmos porque no son lo suficientemente seguros:

- Algoritmos de autenticación: SHA1 y MD5
- Algoritmo de cifrado: 3DES
- Algoritmos de DH: Grupo 1, Grupo 2 y Grupo 5

6. Envíe su solicitud.

   Después de crear la VPN IPsec, se asigna una dirección IP pública a la VPN. La dirección IP es la dirección de gateway local de la VPN creada. Al configurar el túnel remoto en su centro de datos, debe establecer la dirección de gateway remota en esta dirección IP.

7. Necesita configurar un túnel VPN IPsec en el router o firewall en su centro de datos local.

3.3 Adquisición de un gateway de VPN

Escenarios

Para conectar su centro de datos local o red privada a sus ECS en una VPC, compre primero un gateway de VPN. Si elige comprar un gateway de VPN de pago por uso, se creará una conexión de VPN junto con el gateway de VPN.

Requisitos previos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte **Creación de una VPC y subred**.

- Se han configurado reglas de grupo de seguridad para la VPC, y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Reglas de grupo de seguridad**.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network** > **Classic – VPN Gateways**.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija **Virtual Private Network** > **Classic**.
5. En la página **VPN Gateways**, haga clic en **Buy VPN Gateway**.
6. Configure los parámetros basados en **Tabla 3-5** y haga clic en **Buy Now**.

Tabla 3-5 Descripción de los parámetros del gateway de VPN

Parámetro	Descripción	Valor de ejemplo
Billing Mode	Modo de facturación de un gateway de VPN, que puede ser pago por uso **Pay-per-use**: Cuando compra un gateway de VPN de pago por uso, debe comprar una conexión de VPN junto con este gateway de VPN.	Pay-per-use
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre regiones. Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a los usuarios de destino.	AP-Singapore
Name	Nombre de un gateway de VPN.	vpngw-001
VPC	Nombre de la VPC a la que se conecta el gateway de VPN.	vpc-001
Type	Tipo de VPN. **IPsec** está seleccionado de forma predeterminada.	IPsec

Parámetro	Descripción	Valor de ejemplo
Billed By	Un gateway de VPN de pago por uso se puede facturar por ancho de banda o por tráfico. ● **Bandwidth**: Debe especificar un límite de ancho de banda y pagar por la cantidad de tiempo que usa el ancho de banda. ● **Traffic**: Debe especificar un límite de ancho de banda y pagar por el tráfico que genera.	Traffic
Bandwidth (Mbit/s)	El ancho de banda del gateway de VPN. El ancho de banda es compartido por todas las conexiones de VPN creadas para el gateway de VPN. El tamaño total del ancho de banda utilizado por todas las conexiones de VPN creadas para un gateway de VPN no puede exceder el tamaño del ancho de banda del gateway de VPN. Durante el uso de VPN, si el tráfico de red excede el ancho de banda del gateway de VPN, puede producirse congestión de red y pueden interrumpirse las conexiones de VPN. Por lo tanto, asegúrese de configurar suficiente ancho de banda. Puede configurar reglas de alarma en Cloud Eye para hacer un seguimiento del ancho de banda.	100

NOTA

Cuando compra un gateway de VPN de pago por uso, también necesita configurar una conexión de VPN que se creará junto con el gateway (excepto la región **CN South-Shenzhen**). Para obtener más información, véase **Tabla 3-6**.

Tabla 3-6 Descripción de los parámetros de conexión de VPN

Parámetro	Descripción	Example Value
Name	Nombre de una conexión de VPN.	vpn-001
VPN Gateway	Nombre del gateway de VPN para el que se crea la conexión de VPN.	vpcgw-001

Parámetro	Descripción	Example Value
Local Subnet	Subredes de VPC que accederán a su red local con una VPN. Puede establecer la subred local a través de cualquiera de los siguientes métodos: ● **Select subnet**: seleccione las subredes que necesitan acceder a su centro de datos local o red privada. ● **Specify CIDR block**: Ingrese los bloques CIDR que necesitan acceder a su centro de datos local o red privada. **NOTA** Los bloques CIDR de subredes locales no se pueden superponer.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	La dirección IP pública del gateway en su centro de datos o en la red privada. Esta dirección IP se utiliza para comunicarse con su VPC.	N/A
Remote Subnet	Las subredes de su red local que accederán a una VPC con una VPN. Las subredes remota y local no pueden solaparse entre sí. La subred remota no puede superponerse con bloques CIDR involucrados en las existentes interconexiones de VPC, conexiones de Direct Connect o de Cloud Connect creadas para la VPC local. **NOTA** Los bloques CIDR de subredes remotas no se pueden superponer.	192.168.3.0/24, 192.168.4.0/24
PSK	Las PSK configuradas en ambos extremos de una conexión de VPN deben ser las mismas. La PSK: ● Contiene de 6 a 128 caracteres. ● Solo puede contener: – Dígitos – Letras – Caracteres especiales: ~ ` !@ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Ingrese la PSK de nuevo.	Test@123

Parámetro	Descripción	Example Value
Advanced Settings	● **Default**: Utilice las políticas de IKE y de IPsec predeterminadas. ● **Custom**: Utilice políticas IKE e IPsec personalizadas. Para obtener más información sobre las políticas, consulte **Tabla 3-7** y **Tabla 3-8**.	Custom

Tabla 3-7 Política de IKE

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128

Parámetro	Descripción	Valor de ejemplo
DH Algorithm	Algoritmo de intercambio de claves Diffie-Hellman. Se admiten los siguientes algoritmos: ● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 El valor predeterminado es **Group 14**. Los algoritmos de DH configurados en ambos extremos de una conexión de VPN deben ser los mismos. De lo contrario, la negociación no funcionará.	Group 14
Version	Versión del protocolo de IKE. El valor puede ser uno de los siguientes: ● v1 (no recomendado debido a riesgos de seguridad) ● v2 El valor predeterminado es **v2**.	v2
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **86400**.	86400

Tabla 3-8 Política de IPsec

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128
PFS	Algoritmo utilizado por la función Perfect forward secrecy (PFS). PFS admite los siguientes algoritmos: ● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 El algoritmo predeterminado es **DH group 14**.	DH group 14

Parámetro	Descripción	Valor de ejemplo
Transfer Protocol	Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos de usuario. Se admiten los siguientes protocolos: ● ESP ● AH ● AH-ESP El protocolo predeterminado es **ESP**.	ESP
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **3600**.	3600

ATENCIÓN

No se recomiendan los siguientes algoritmos porque no son lo suficientemente seguros:

Algoritmos de autenticación: SHA1 y MD5

Algoritmo de cifrado: 3DES

Algoritmos de DH: Grupo 1, Grupo 2 y Grupo 5

7. Confirme la información del gateway de VPN y haga clic en **Buy Now**.

   Después de crear un gateway de VPN, el sistema asigna automáticamente una dirección IP pública, es decir, la dirección IP mostrada en la columna **Gateway IP Address** de la lista de gateway de VPN. La dirección IP del gateway también es la dirección IP del gateway remoto configurado en la red VPN local. **Figura 3-2** muestra la dirección IP del gateway.

Figura 3-2 Lista de gateway de VPN

3.4 Adquisición de una conexión de VPN

Escenarios

Para conectar su centro de datos local o red privada a sus ECS en una VPC, debe crear una conexión de VPN después de obtener un gateway de VPN.

Procedimiento

1. Inicie sesión en la consola de gestión.

2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network** > **Classic – VPN Connections**.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija **Virtual Private Network** > **Classic**.
5. En la página **VPN Connections**, haga clic en **Buy VPN Connection**.
6. Configure los parámetros como se le solicite y haga clic en **Next**. **Tabla 3-9** enumera los parámetros de conexión de VPN.

Tabla 3-9 Descripción de los parámetros de conexión de VPN

Parámetro	Descripción	Valor de ejemplo
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre regiones. Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a los usuarios de destino.	CN North-Beijing4
Name	Nombre de una conexión de VPN.	vpn-001
VPN Gateway	Nombre del gateway de VPN para el que se crea la conexión de VPN.	vpcgw-001
Local Subnet	Subredes de VPC que accederán a su red local con una VPN. Puede establecer la subred local a través de cualquiera de los siguientes métodos: ● **Select subnet**: seleccione las subredes que necesitan acceder a su centro de datos local o red privada. ● **Specify CIDR block**: Ingrese los bloques CIDR que necesitan acceder a su centro de datos local o red privada. **NOTA** Los bloques CIDR de subredes locales no se pueden superponer.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	La dirección IP pública del gateway en su centro de datos o en la red privada. Esta dirección IP se utiliza para comunicarse con su VPC.	N/A

Parámetro	Descripción	Valor de ejemplo
Remote Subnet	Las subredes de su red local que accederán a una VPC con una VPN. Las subredes remota y local no pueden solaparse entre sí. La subred remota no puede superponerse con bloques CIDR involucrados en las existentes interconexiones de VPC, conexiones de Direct Connect o de Cloud Connect creadas para la VPC local. **NOTA** Los bloques CIDR de subredes remotas no se pueden superponer.	192.168.3.0/24, 192.168.4.0/24
PSK	Clave privada compartida por dos extremos de una conexión de VPN para negociación. Las PSK configuradas en ambos extremos de la conexión de VPN deben ser las mismas. La PSK: ● Contiene de 6 a 128 caracteres. ● Solo puede contener: – Dígitos – Letras – Caracteres especiales: ~ ` !@ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Ingrese la PSK de nuevo.	Test@123
Advanced Settings	● **Default**: Utilice las políticas de IKE y de IPsec predeterminadas. ● **Existing**: Utilice las políticas de IKE y de IPsec existentes. ● **Custom**: incluye **IKE Policy** y **IPsec Policy** que especifica los algoritmos de encriptación y autenticación de un túnel de VPN. Para obtener más información sobre las políticas, consulte **Tabla 3-10** y **Tabla 3-11**.	Custom

Tabla 3-10 Política de IKE

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128

Parámetro	Descripción	Valor de ejemplo
DH Algorithm	Algoritmo de intercambio de claves Diffie-Hellman. Se admiten los siguientes algoritmos: ● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 El algoritmo predeterminado es **Group 14**.	Group 14
Version	Versión del protocolo de IKE. El valor puede ser uno de los siguientes: ● v1 (no recomendado debido a riesgos de seguridad) ● v2 El valor predeterminado es **v2**.	v2
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **86400**.	86400

Tabla 3-11 Política de IPsec

Parámetro	Descripción	Valor de ejemplo
Authentication Algorithm	Algoritmo de hash utilizado para la autenticación. Se admiten los siguientes algoritmos: ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 El algoritmo predeterminado es **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encriptación. Se admiten los siguientes algoritmos: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) El algoritmo predeterminado es **AES-128**.	AES-128

Parámetro	Descripción	Valor de ejemplo
PFS	Algoritmo utilizado por la función Perfect forward secrecy (PFS). PFS admite los siguientes algoritmos: ● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 El algoritmo predeterminado es **DH group 14**.	DH group 14
Transfer Protocol	Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos de usuario. Se admiten los siguientes protocolos: ● AH ● ESP ● AH-ESP El protocolo predeterminado es **ESP**.	ESP
Lifetime (s)	Duración de una SA, en segundos Una SA se renegociará cuando expire su vida útil. El valor predeterminado es **3600**.	3600

NOTA

Una política de IKE especifica los algoritmos de encriptación y autenticación que se utilizarán en la fase de negociación de un túnel IPsec. Una política de IPsec especifica el protocolo, el algoritmo de encriptación y el algoritmo de autenticación que se utilizarán en la fase de transmisión de datos de un túnel de IPsec. Las políticas de IKE y de IPsec deben ser las mismas en ambos extremos de una conexión de VPN. Si son diferentes, la conexión de VPN no se puede configurar.

No se recomiendan los siguientes algoritmos porque no son lo suficientemente seguros:

- Algoritmos de autenticación: SHA1 y MD5
- Algoritmo de cifrado: 3DES
- Algoritmos de DH: Grupo 1, Grupo 2 y Grupo 5

7. Haga clic en **Submit**.
8. Necesita configurar un túnel VPN IPsec en el router o firewall en su centro de datos local.

3.5 Configuración del dispositivo remoto

Para obtener más información acerca de cómo configurar el dispositivo remoto, consulte la **Guía del administrador de Virtual Private Network**. Esta guía le ayuda a configurar el dispositivo de VPN local para implementar la interconexión entre su red local y la subred de VPC.

Para obtener más información sobre los ejemplos de configuración, consulte lo siguiente:

- **Serie de Huawei USG6600**
- **Configuración de VPN cuando se utiliza Fortinet FortiGate Firewall**
- **Configuración de VPN cuando se utiliza Sangfor Firewall**
- **Uso del cliente de TheGreenBow IPsec VPN para configurar la comunicación en y fuera de la nube**
- **Uso de Openswan para configurar la comunicación en y fuera de la nube**
- **Uso de strongSwan para configurar la comunicación en y fuera de la nube**

