Virtual Private Network

Primeiros passos

Edição 01

Data 21-09-2023

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Índice

1 Preparações

Antes de usar a VPN, faça as seguintes preparações:

Registrar-se com a Huawei Cloud e conclusão da autenticação de nome real

Pule esta parte se você já tiver uma conta da Huawei Cloud. Se você não tiver uma conta da Huawei Cloud, execute as seguintes etapas para criar uma:

1. Visite o **site oficial da Huawei Cloud** e clique em **Register**.
2. Conclua o registro conforme solicitado. Para obter detalhes, consulte **Registro da Huawei Cloud**.

   Se seu registro for bem-sucedido, o sistema redireciona-o automaticamente para sua página de informações pessoais.
3. Conclua a autenticação de nome real seguindo as instruções em **Autenticação de nome real**.

Recarregar sua conta

Certifique-se de que o saldo da sua conta é suficiente.

- Para obter detalhes sobre os preços da VPN, consulte **Detalhes de preços**.

2 Configuração de VPN da edição Enterprise para conectar um data center local e uma VPC

2.1 Visão geral

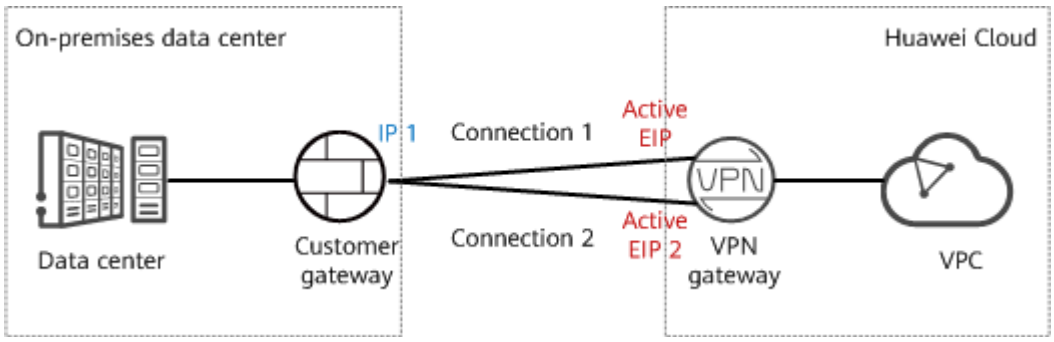
Regiões suportadas

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

Cenário

Para atender aos requisitos de desenvolvimento de negócios, a empresa A precisa implementar a comunicação entre seu data center local e sua VPC. Nesse caso, a empresa A pode usar o serviço de VPN para criar conexões entre o data center local e a VPC, conforme mostrado em **Figura 2-1**.

Figura 2-1 Rede VPN



Esta solução tem os seguintes requisitos no data center local e no dispositivo de gateway do cliente:

- O dispositivo de gateway do cliente deve oferecer suporte aos protocolos IKE e IPsec padrão.
- O gateway do cliente tem um endereço IP público estático.

- As sub-redes do data center local que precisam acessar a VPC não se sobrepõem às sub-redes da VPC nem contêm 100.64.0.0/10 ou 214.0.0.0/8.

  Se a VPC usar conexões Direct Cloud ou Cloud Connect para se comunicar com outras VPCs, as sub-redes do data center local não poderão se sobrepor às dessas VPCs.

Plano de dados

Tabela 2-1 Plano de dados

Categoria	Item	Dados
VPC	Sub-rede que precisa acessar o data center local	192.168.0.0/16
Gateway de VPN	Sub-rede de interconexão	Essa sub-rede é usada para comunicação entre o gateway de VPN e a VPC. Certifique-se de que a sub-rede de interconexão selecionada tenha quatro ou mais endereços IP atribuíveis. 192.168.2.0/24
	EIP	Os EIPs são gerados automaticamente quando você os compra. Por padrão, um gateway de VPN usa dois EIPs. Neste exemplo, os EIPs são os seguintes: ● EIP ativo: 11.xx.xx.11 ● EIP em espera: 11.xx.xx.12
Conexão de VPN	Endereço da interface do túnel	Esse endereço é usado por um gateway de VPN para estabelecer um túnel IPsec com um gateway de cliente. Nas duas extremidades do túnel IPsec, os endereços de interface de túnel local e remoto configurados devem ser invertidos. ● Conexão de VPN 1: 169.254.70.1/30 ● Conexão de VPN 2: 169.254.71.1/30
Data center local	Sub-rede que precisa acessar a VPC	172.16.0.0/16
Gateway de cliente	Endereço IP do gateway	O endereço IP do gateway é atribuído por uma operadora. Neste exemplo, o endereço IP do gateway é: 22.xx.xx.22
	Endereço da interface do túnel	● Conexão de VPN 1: 169.254.70.2/30 ● Conexão de VPN 2: 169.254.71.2/30

Processo de operação

Figura 2-2 mostra o processo de uso do serviço de VPN para habilitar a comunicação entre um data center local e uma VPC.

Figura 2-2 Processo de operação

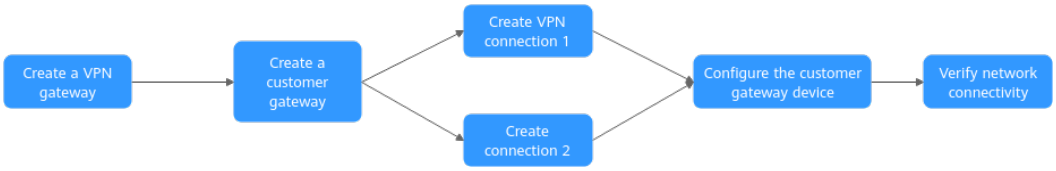


Tabela 2-2 Descrição do processo de operação

Nº	Etapa	Descrição
1	**Passo 1: criar um gateway de VPN**	Vincule dois EIPs ao gateway de VPN. Se você comprou EIPs, pode vinculá-los diretamente ao gateway de VPN.
2	**Passo 2: criar um gateway de cliente**	Configure o dispositivo VPN no data center local como gateway do cliente.
3	**Passo 3: criar conexão de VPN 1**	Crie uma conexão de VPN entre o EIP ativo do gateway de VPN e o gateway do cliente.
4	**Passo 4: criar conexão de VPN 2**	Crie uma conexão de VPN entre o EIP em espera do gateway de VPN e o gateway do cliente. Recomenda-se que as configurações de modo de roteamento, PSK, política de IKE e IPsec das duas conexões de VPN sejam as mesmas.
5	**Passo 5: configurar o dispositivo de gateway do cliente**	● Os endereços de interface local e remota configurados no dispositivo de gateway do cliente devem ser iguais aos endereços de interface local e de cliente da conexão de VPN da Huawei Cloud, respectivamente. ● As configurações de modo de roteamento, PSK, política de IKE e política IPsec no dispositivo de gateway do cliente devem ser as mesmas da conexão VPN da Huawei Cloud.
6	**Passo 6: verificar a conectividade da rede**	Faça logon em um ECS e execute o comando **ping** para verificar a conectividade de rede.

2.2 Passo 1: criar um gateway de VPN

Pré-requisitos

- Uma VPC foi criada. Para obter detalhes sobre como criar uma VPC, consulte **Criação de uma VPC e sub-rede**.

- As regras do grupo de segurança foram configuradas para ECSs na VPC e permitem que o gateway do cliente no data center local acesse os recursos da VPC. Para obter detalhes sobre como configurar regras de grupo de segurança, consulte **Regras de grupo de segurança**.

Procedimento

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.

Passo 3 Escolha **Virtual Private Network** > **Enterprise － VPN Gateways** e clique em **Buy VPN Gateway**.

Passo 4 Defina os parâmetros conforme solicitado e clique em **Next**.

O seguinte descreve apenas os parâmetros principais. Para obter detalhes sobre mais parâmetros, consulte **Criação de um gateway de VPN**.

Tabela 2-3 Principais parâmetros do gateway de VPN

Parâmetro	Descrição	Exemplo de valor
Billing Mode	As opções incluem **Yearly/Monthly** e **Pay-per-use**.	Yearly/Monthly
Region	Selecione a região mais próxima de você.	AP-Singapore
Name	Nomeie um gateway de VPN.	vpngw-001
Network Type	● **Public network**: um gateway de VPN se comunica com um gateway de cliente em um data center local por meio da Internet. ● **Private network**: um gateway de VPN se comunica com um gateway de cliente em um data center local por meio de uma rede privada.	Public network
Associate With	As opções incluem **VPC** e **Enterprise Router**	VPC
VPC	Selecione a VPC que precisa acessar o data center local.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Essa sub-rede é usada para comunicação entre o gateway de VPN e a VPC. Certifique-se de que a sub-rede de interconexão selecionada tenha quatro ou mais endereços IP atribuíveis.	192.168.2.0/24
Local Subnet	Especifique a sub-rede da VPC que precisa acessar o data center local. Você pode inserir manualmente um bloco CIDR ou selecionar uma sub-rede na caixa de listagem suspensa.	192.168.0.0/24

Parâmetro	Descrição	Exemplo de valor
Active EIP	Você pode comprar um novo EIP ou usar um EIP existente.	11.xx.xx.11
Standby EIP		11.xx.xx.12

----Fim

Verificação

Verifique o gateway de VPN criado na página **VPN Gateways**. O estado inicial do gateway de VPN é **Creating**. Após cerca de 2 minutos, o estado muda para **Normal**, indicando que o gateway de VPN foi criado com êxito.

2.3 Passo 2: criar um gateway de cliente

Procedimento

Passo 1 Escolha **Virtual Private Network** > **Enterprise** - **Customer Gateways** e clique em **Create Customer Gateway**.

Passo 2 Defina os parâmetros conforme solicitado e clique em **OK**.

O seguinte descreve apenas os parâmetros principais. Para obter detalhes sobre mais parâmetros, consulte **Criação de um gateway de cliente**.

Tabela 2-4 Parâmetros de gateway do cliente

Parâmetro	Descrição	Exemplo de valor
Name	Nomeie um gateway de cliente.	cgw-001
Routing Mode	Selecione **Static**.	Static
Gateway IP Address	Insira o endereço IP do gateway do cliente no data center local.	22.xx.xx.22

----Fim

Verificação

Verifique o gateway do cliente criado na página **Customer Gateways**.

2.4 Passo 3: criar conexão de VPN 1

Procedimento

1. Escolha **Virtual Private Network** > **Enterprise** - **VPN Connections** e clique em **Buy VPN Connection**.

2. Defina os parâmetros para a conexão de VPN 1 conforme solicitado e clique em **Submit**.

   O seguinte descreve apenas os parâmetros principais. Para obter detalhes sobre mais parâmetros, consulte **Criacao de um a conexão de VPN**.

Tabela 2-5 Configurações de parâmetro para conexão de VPN 1

Parâmetro	Descrição	Exemplo de valor
Name	Digite o nome da conexão de VPN 1.	vpn-001
VPN Gateway	Selecione o gateway de VPN criado em **Passo 1: criar um gateway de VPN**.	vpngw-001
Gateway IP Address	Selecione o EIP ativo do gateway de VPN.	11.xx.xx.11
Customer Gateway	Selecione o gateway do cliente criado em **Passo 2: criar um gateway de cliente**.	cgw-001
VPN Type	Selecione **Static routing**.	Static routing
Customer Subnet	Digite a sub-rede do data center local que precisa acessar a VPC.	172.16.0.0/16
Interface IP Address Assignment	As opções incluem **Manually specify** e **Automatically assign**.	Manually specify
Local Interface IP Address	Especifique o endereço IP do túnel do gateway de VPN. **NOTA** Os endereços de interface local e remoto configurados no dispositivo de gateway do cliente devem ser os mesmos que os valores de **Customer Interface IP Address** e **Local Interface IP Address**, respectivamente.	169.254.70.2/30
Customer Interface IP Address	Especifique o endereço IP do túnel do gateway do cliente.	169.254.70.1/30
Link Detection	Esta função é usada para a detecção da confiança da rota em cenários de vários links. **NOTA** Ao ativar essa função, certifique-se de que o gateway de cliente ofereça suporte a ICMP e esteja configurado corretamente com o endereço IP da interface do cliente da conexão de VPN. Caso contrário, o tráfego de VPN não será encaminhado.	**NQA** ativado

Parâmetro	Descrição	Exemplo de valor
PSK, Confirm PSK	Especifique a chave de negociação da conexão de VPN. As PSKs configuradas no console de VPN e no dispositivo de gateway do cliente devem ser as mesmas.	Test@123
Policy Settings	Configure as políticas de IKE e IPsec, que definem os algoritmos de criptografia usados pelo túnel de VPN. As configurações de política no console de VPN e no dispositivo de gateway do cliente devem ser as mesmas.	Padrão

Verificação

Verifique a conexão de VPN criada na página **VPN Connections**. O estado inicial da conexão de VPN é **Creating**. Como o dispositivo de gateway do cliente não foi configurado, nenhuma conexão de VPN pode ser estabelecida. Após cerca de 2 minutos, o estado da conexão de VPN muda para **Not connected**.

2.5 Passo 4: criar conexão de VPN 2

Procedimento

1. Escolha **Virtual Private Network** > **Enterprise** – **VPN Connections** e clique em **Buy VPN Connection**.
2. Defina os parâmetros para a conexão de VPN 2 conforme solicitado e clique em **Submit**.

   Para a conexão de VPN 2, é aconselhável usar as mesmas configurações da conexão de VPN 1, exceto o nome da conexão, o endereço IP do gateway, o endereço IP da interface local e o endereço IP da interface do cliente.

Tabela 2-6 Configurações de parâmetro para conexão de VPN 2

Parâmetro	Descrição	Exemplo de valor
Name	Digite o nome da conexão de VPN 2.	vpn-002
VPN Gateway	Selecione o gateway de VPN criado em **Passo 1: criar um gateway de VPN**.	vpngw-001
Gateway IP Address	Selecione o EIP em espera do gateway de VPN.	11.xx.xx.12
Customer Gateway	Selecione o gateway do cliente criado em **Passo 2: criar um gateway de cliente**.	cgw-001

Parâmetro	Descrição	Exemplo de valor
VPN Type	Selecione **Static routing**.	Static routing
Customer Subnet	Digite a sub-rede do data center local que precisa acessar a VPC.	172.16.0.0/16
Interface IP Address Assignment	As opções incluem **Manually specify** e **Automatically assign**.	Manually specify
Local Interface IP Address	Especifique o endereço IP do túnel do gateway de VPN. **NOTA** Os endereços de interface local e remoto configurados no dispositivo de gateway do cliente devem ser os mesmos que os valores de **Customer Interface IP Address** e **Local Interface IP Address**, respectivamente.	169.254.71.2/30
Customer Interface IP Address	Especifique o endereço IP do túnel do gateway do cliente.	169.254.71.1/30
Link Detection	Esta função é usada para a detecção da confiança da rota em cenários de vários links. **NOTA** Ao ativar essa função, certifique-se de que o gateway de cliente ofereça suporte a ICMP e esteja configurado corretamente com o endereço IP da interface do cliente da conexão de VPN. Caso contrário, o tráfego de VPN não será encaminhado.	**NQA** ativado
PSK, Confirm PSK	Especifique a chave de negociação da conexão de VPN. As PSKs configuradas no console de VPN e no dispositivo de gateway do cliente devem ser as mesmas.	Test@123
Policy Settings	Configure as políticas IKE e IPsec, que definem os algoritmos de criptografia usados pelo túnel de VPN. As configurações de política no console de VPN e no dispositivo de gateway do cliente devem ser as mesmas.	Padrão

Verificação

Verifique a conexão de VPN criada na página **VPN Connections**. O estado inicial da conexão de VPN é **Creating**. Como o dispositivo de gateway do cliente não foi configurado, nenhuma

conexão de VPN pode ser estabelecida. Após cerca de 2 minutos, o estado da conexão de VPN muda para **Not connected**.

2.6 Passo 5: configurar o dispositivo de gateway do cliente

Procedimento

NOTA

Neste exemplo, o dispositivo de gateway do cliente é um roteador AR da Huawei. Para obter mais exemplos de configuração de dispositivos de gateway do cliente, consulte **Guia de administrador**.

Passo 1 Efetue logon no roteador AR.

Passo 2 Entre na visão do sistema.

<AR651>system-view

Passo 3 Configure um endereço IP para a interface WAN. Neste exemplo, a interface WAN do roteador AR é 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

Passo 4 Configure uma rota padrão.

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

Neste comando, *22.xx.xx.1* é o endereço de gateway do endereço IP público do roteador AR. Substitua-o pelo endereço de gateway atual.

Passo 5 Permita que o algoritmo SHA-2 seja compatível com os algoritmos RFC padrão.

[AR651]IPsec authentication sha2 compatible enable

Passo 6 Configure uma proposta 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

Passo 7 Configure uma proposta de 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
```

Passo 8 Configure pares de IKE.

```
[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
```

Os comandos são descritos da seguinte forma:

- **pre-shared-key cipher**: configura uma PSK, que deve ser a mesma configurada no console da VPN.
- **local-address**: especifica o endereço IP público do roteador AR.
- **remote-address**: especifica o EIP ativo ou em espera do gateway de VPN.

Passo 9 Configure um perfil de 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
```

Passo 10 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
#
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

Os comandos são descritos da seguinte forma:

- **interface Tunnel0/0/1** e **interface Tunnel0/0/2**: indicam as interfaces de túnel correspondentes às duas conexões de VPN.

  Neste exemplo, Tunnel0/0/1 estabelece uma conexão de VPN com o EIP ativo do gateway de VPN, e Tunnel0/0/2 estabelece uma conexão de VPN com o EIP em espera do gateway de VPN.
- **ip address**: configura um endereço IP para uma interface de túnel no roteador AR.
- **source**: especifica o endereço IP público do roteador AR.
- **destination**: especifica o EIP ativo ou em espera do gateway de VPN.

Passo 11 Configure NQA.

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
#
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

Os comandos são descritos da seguinte forma:

- **nqa test-instance IPsec_nqa1 IPsec_nqa1** e **nqa test-instance IPsec_nqa2 IPsec_nqa2**: configure duas instâncias de teste de NQA chamadas **IPsec_nqa1** e **IPsec_nqa2**.

  Neste exemplo, a instância de teste **IPsec_nqa1** é criada para a conexão de VPN à qual o EIP ativo do gateway de VPN pertence; a instância de teste **IPsec_nqa2** é criada para a conexão de VPN à qual pertence o EIP em espera do gateway de VPN.
- **destination-address**: especifica o endereço da interface do túnel do gateway de VPN.
- **source-address**: especifica o endereço da interface de túnel do roteador AR.

Passo 12 Configure a associação entre a rota estática e 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
```

Os parâmetros são descritos como segue:

- **192.168.0.0** indica a sub-rede local da VPC.
- **Tunnel***x* e **IPsec_nqa***x* no mesmo comando correspondem à mesma conexão de VPN.

----Fim

Verificação

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.

Passo 3 Escolha **Virtual Private Network** > **Enterprise - VPN Connections**. Verifique se os estados das duas conexões VPN estão **Available**.

----Fim

2.7 Passo 6: verificar a conectividade da rede

Procedimento

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.

Passo 3 Clique em **Service List** e escolha **Compute** > **Elastic Cloud Server**.

Passo 4 Efetue logon em um ECS.

Vários métodos estão disponíveis para efetuar logon em um ECS. Para obter detalhes, consulte **Logon em um ECS**.

Neste exemplo, use o VNC fornecido no console de gerenciamento para fazer logon em um ECS.

Passo 5 Execute o seguinte comando no ECS:

ping 172.16.0.100

172.16.0.100 é o endereço IP de um servidor no data center local. Substitua-o por um endereço IP de servidor real.

Se informações semelhantes às seguintes forem exibidas, a VPC na nuvem e o data center local poderão se comunicar entre si.

```
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
```

----Fim

3 Processo de compra de VPN Clássica

3.1 Visão geral

O processo de configuração de VPNs clássicas varia em diferentes regiões, conforme descrito em **Tabela 3-1**.

Tabela 3-1 Visão geral

Regiões suportadas	CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg e LA-Santiago	LA-Mexico City1 e LA-Sao Paulo1
Criação de VPN	Execute as seguintes etapas em sequência: 1. **Compra de um gateway de VPN** 2. **Compra de uma conexão de VPN** 3. **Configuração do dispositivo remoto**	Execute as seguintes etapas em sequência: 1. **Criação de uma VPN (LA-Mexico City1/LA-Sao Paulo1)** 2. **Configuração do dispositivo remoto**

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

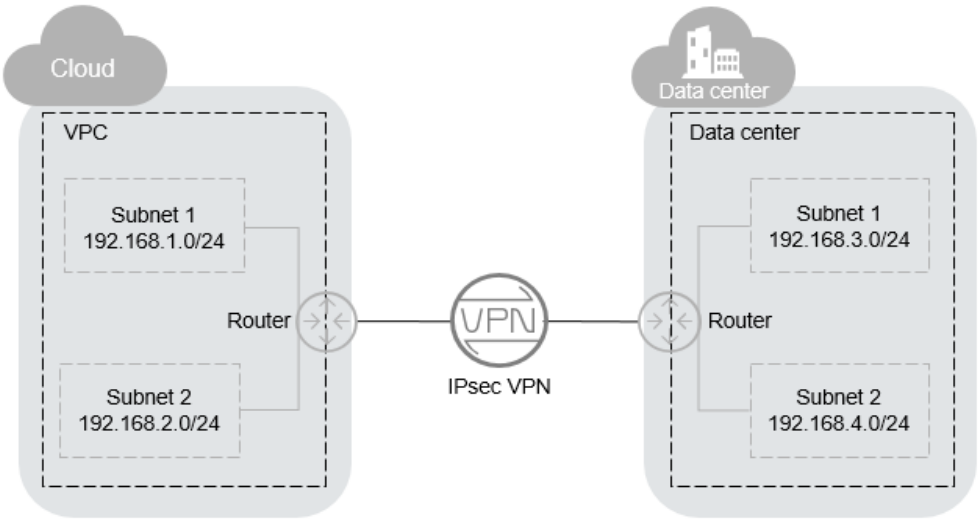
Visão geral

Por padrão, os ECSs em uma VPC não podem se comunicar com dispositivos no data center local ou na rede privada. Para permitir a comunicação entre eles, você pode usar uma VPN criando-a na VPC e atualizando as regras do grupo de segurança.

Topologia de VPN IPsec

Em **Figura 3-1**, a VPC tem sub-redes 192.168.1.0/24 e 192.168.2.0/24. Seu data center local tem sub-redes 192.168.3.0/24 e 192.168.4.0/24. Você pode usar a VPN para ativar as sub-redes na VPC para se comunicar com as do seu data center.

Figura 3-1 VPN IPsec



A Huawei Cloud suporta VPN site a site para permitir a comunicação entre sub-redes da VPC e sub-redes locais de data center. Antes de estabelecer uma VPN IPsec, verifique se o data center local em que a VPN será estabelecida atende às seguintes condições:

- Estão disponíveis dispositivos no local que suportam o protocolo IPsec padrão.
- Os dispositivos locais têm endereços IP públicos fixos, que podem ser configurados estaticamente ou convertidos por NAT.
- As sub-redes locais não entram em conflito com as sub-redes da VPC, e os dispositivos nas sub-redes locais podem se comunicar com os dispositivos locais.

Se as condições anteriores forem atendidas, certifique-se de que as políticas de IKE e as políticas de IPsec em ambas as extremidades sejam consistentes e as sub-redes em ambas as extremidades sejam pares correspondentes ao configurar a VPN IPsec.

Após a conclusão da configuração, a negociação de VPN precisa ser acionada por fluxos de dados da rede privada.

Cenários

Você precisa de uma VPN que configure um túnel de comunicações seguro e isolado entre seu data center local e os serviços em nuvem.

Pré-requisitos

- Uma VPC foi criada. Para obter detalhes sobre como criar uma VPC, consulte **Criação de uma VPC e sub-rede**.

- As regras de grupo de segurança foram configuradas para a VPC, e os ECSs podem se comunicar com outros dispositivos na nuvem. Para obter detalhes sobre como configurar regras de grupo de segurança, consulte **Regras de grupo de segurança**.

Procedimento

1. Faça logon no console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
4. Na página **Virtual Private Network**, clique em **Buy VPN**.
5. Configure os parâmetros necessários e clique em **Next**.

   Tabela 3-2, **Tabela 3-3** e **Tabela 3-4** lista os parâmetros e suas descrições.

Tabela 3-2 Parâmetros básicos

Parâmetro	Descrição	Exemplo de valor
Region	As regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas umas às outras, portanto, os recursos não podem ser compartilhados entre regiões. Para baixa latência de rede e rápido acesso a recursos, selecione a região mais próxima de seus usuários-alvo.	AP-Singapore
Billing Mode	As VPNs são cobradas em uma base de pagamento por uso.	Pay-per-use
Name	O nome da VPN	VPN-001
VPC	O nome da VPC	VPC-001
Local Subnet	Sub-redes da VPC que acessarão sua rede local por meio de uma VPN.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	O endereço IP público do gateway em seu data center ou na rede privada. Esse endereço IP é usado para se comunicar com sua VPC.	N/A
Remote Subnet	As sub-redes da sua rede local que acessarão uma VPC por meio de uma VPN. As sub-redes locais e remotas não podem se sobrepor. As sub-redes remotas não podem se sobrepor aos blocos CIDR envolvidos nas conexões de emparelhamento de VPC existentes criadas para a VPC.	192.168.3.0/24, 192.168.4.0/24

Parâmetro	Descrição	Exemplo de valor
PSK	Chave privada compartilhada por duas extremidades de uma conexão de VPN para negociação. As PSKs configuradas em ambas as extremidades da conexão de VPN devem ser as mesmas. A PSK pode conter de 1 a 128 caracteres.	Test@123
Confirm PSK	Digite a PSK novamente.	Test@123
Advanced Settings	● **Default**: utilizar políticas de IKE e IPsec predefinidas. ● **Custom**: utilizar políticas de IKE e IPsec personalizadas. Para mais detalhes, veja **Tabela 3-3** e **Tabela 3-4**.	Custom

Tabela 3-3 IKE policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128

Parâmetro	Descrição	Exemplo de valor
DH Algorithm	Algoritmo de troca de chaves Diffie-Hellman. Os seguintes algoritmos são suportados: ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 14 O valor padrão é **Group 14**.	Group 14
Version	Versão do protocolo IKE. O valor pode ser um dos seguintes: ● v1 (não recomendado devido a riscos de segurança) ● v2 O valor padrão é **v2**.	v2
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma AS será renegociada quando sua vida útil expirar. O valor padrão é **86400**.	86400
Negotiation Mode	Este parâmetro só está disponível quando **Version** é definida como **v1**. Você pode definir **Negotiation Mode** como **Main** ou **Aggressive**. O modo padrão é **Main**.	Main

Tabela 3-4 IPsec policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128
PFS	Algoritmo usado pela função Perfect forward secret (PFS). PFS suporta os seguintes algoritmos: ● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 14 O algoritmo padrão é **DH group 14**.	DH group 14
Transfer Protocol	Protocolo de segurança usado no IPsec para transmitir e encapsular dados do usuário. Os seguintes protocolos são suportados: ● AH ● AH-ESP O protocolo padrão é **ESP**.	ESP

Parâmetro	Descrição	Exemplo de valor
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma AS será renegociada quando sua vida útil expirar. O valor padrão é **3600**.	3600

NOTA

Uma política de IKE especifica os algoritmos de encritação e autenticação a utilizar na fase de negociação de um túnel de IPsec. Uma política de IPsec especifica o protocolo, o algoritmo de encritação e o algoritmo de autenticação a utilizar na fase de transmissão de dados de um túnel de IPsec. As políticas de IKE e IPsec devem ser as mesmas em ambas as extremidades de uma conexão de VPN. Se forem diferentes, a conexão de VPN não pode ser configurada.

Os seguintes algoritmos não são recomendados porque não são seguros o suficiente:

- Algoritmos de autenticação: SHA1 e MD5
- Algoritmo de encritação: 3DES
- Algoritmos DH: Group 1, Group 2 e Group 5

6. Submeta a sua solicitação.

   Depois que a VPN IPsec é criada, um endereço IP público é atribuído à VPN. O endereço IP é o endereço de gateway local da VPN criada. Ao configurar o túnel remoto em seu data center, você deve definir o endereço do gateway remoto para esse endereço IP.

7. Você precisa configurar um túnel de VPN IPsec no roteador ou firewall em seu data center local.

3.3 Compra de um gateway de VPN

Cenários

Para conectar seu data center local ou sua rede privada aos ECSs em uma VPC, primeiro compre um gateway de VPN. Se você optar por criar um gateway de VPN de pagamento por uso, uma conexão de VPN será criada junto com o gateway de VPN.

Pré-requisitos

- Uma VPC foi criada. Para obter detalhes sobre como criar uma VPC, consulte **Criação de uma VPC e sub-rede**.
- As regras de grupo de segurança foram configuradas para a VPC, e os ECSs podem se comunicar com outros dispositivos na nuvem. Para obter detalhes sobre como configurar regras de grupo de segurança, consulte **Regras de grupo de segurança**.

Procedimento

1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.

3. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
4. No painel de navegação à esquerda, escolha **Virtual Private Network** > **Classic – VPN Gateways**.

   Se a VPN de edição Enterprise estiver disponível para a região selecionada, escolha **Virtual Private Network** > **Classic**.
5. Na página **VPN Gateways**, clique em **Buy VPN Gateway**.
6. Configure parâmetros com base em **Tabela 3-5** e clique em **Buy Now**.

Tabela 3-5 Descrição dos parâmetros do gateway de VPN

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Modo de cobrança de um gateway de VPN, que pode ser pagamento por uso **Pay-per-use**: quando você compra um gateway de VPN pagamento por uso, você deve comprar uma conexão de VPN juntamente com o gateway de VPN.	Pay-per-use
Region	As regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas umas às outras, portanto, os recursos não podem ser compartilhados entre regiões. Para baixa latência de rede e rápido acesso a recursos, selecione a região mais próxima de seus usuários-alvo.	AP-Singapore
Name	Nome de um gateway de VPN.	vpngw-001
VPC	Nome da VPC à qual o gateway de VPN se conecta.	vpc-001
Type	Tipo de VPN. **IPsec** é selecionado por padrão.	IPsec
Billed By	Um gateway de VPN pagamento por uso pode ser cobrado por largura de banda ou por tráfego. ● **Bandwidth**: você precisa especificar um limite de largura de banda e pagar pela quantidade de tempo que você usa a largura de banda. ● **Traffic**: você precisa especificar um limite de largura de banda e pagar pelo tráfego que gera.	Traffic

Parâmetro	Descrição	Exemplo de valor
Bandwidth (Mbit/s)	A largura de banda do gateway de VPN. A largura de banda é compartilhada por todas as conexões de VPN criadas para o gateway de VPN. O tamanho total da largura de banda usada por todas as conexões de VPN criadas para um gateway de VPN não pode exceder o tamanho da largura de banda do gateway de VPN. Durante o uso da VPN, se o tráfego de rede exceder a largura de banda do gateway de VPN, poderá ocorrer congestionamento da rede e as conexões de VPN poderão ser interrompidas. Como tal, certifique-se de configurar largura de banda suficiente. Você pode configurar regras de alarme no Cloud Eye para monitorar a largura de banda.	100

NOTA

Quando você compra um gateway de VPN de pagamento por uso, também precisa configurar uma conexão de VPN que será criada junto com o gateway (exceto a região **CN South-Shenzhen**). Para mais detalhes, consulte **Tabela 3-6**.

Tabela 3-6 Descrição dos parâmetros de conexão de VPN

Parâmetro	Descrição	Exemplo de valor
Name	Nome de uma conexão de VPN.	vpn-001
VPN Gateway	Nome do gateway de VPN para o qual a conexão VPN é criada.	vpcgw-001
Local Subnet	Sub-redes da VPC que acessarão sua rede local por meio de uma VPN. Você pode definir a sub-rede local usando um dos seguintes métodos: ● **Select subnet**: selecione as sub-redes que precisam acessar seu data center local ou rede privada. ● **Specify CIDR block**: insira os blocos CIDR que precisam acessar seu data center local ou rede privada. **NOTA** Blocos CIDR de sub-redes locais não podem se sobrepor.	192.168.1.0/24, 192.168.2.0/24

Parâmetro	Descrição	Exemplo de valor
Remote Gateway	O endereço IP público do gateway em seu data center ou na rede privada. Esse endereço IP é usado para se comunicar com sua VPC.	N/A
Remote Subnet	As sub-redes da sua rede local que acessarão uma VPC por meio de uma VPN. As sub-redes locais e remotas não podem se sobrepor. A sub-rede remota não pode se sobrepor a blocos CIDR envolvidos em conexões de emparelhamento de VPC, Direct Connect ou Cloud Connect existentes criadas para a VPC local. **NOTA** Blocos CIDR de sub-redes remotas não podem se sobrepor.	192.168.3.0/24, 192.168.4.0/24
PSK	As PSKs configuradas em ambas as extremidades de uma conexão de VPN devem ser as mesmas. A PSK: ● Contém 6 a 128 caracteres. ● Pode conter apenas: – Dígitos – Letras – Caracteres especiais: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Digite a PSK novamente.	Test@123
Advanced Settings	● **Default**: utilizar políticas de IKE e IPsec predefinidas. ● **Custom**: utilizar políticas de IKE e IPsec personalizadas. Para obter detalhes sobre as políticas, consulte **Tabela 3-7** e **Tabela 3-8**.	Custom

Tabela 3-7 IKE policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128
DH Algorithm	Algoritmo de troca de chaves Diffie-Hellman. Os seguintes algoritmos são suportados: ● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 O valor padrão é **Group 14**. Os algoritmos DH configurados em ambas as extremidades de uma conexão de VPN devem ser os mesmos. Caso contrário, a negociação falhará.	Group 14

Parâmetro	Descrição	Exemplo de valor
Version	Versão do protocolo IKE. O valor pode ser um dos seguintes: ● v1 (não recomendado devido a riscos de segurança) ● v2 O valor padrão é **v2**.	v2
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma AS será renegociada quando sua vida útil expirar. O valor padrão é **86400**.	86400

Tabela 3-8 IPsec policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128

Parâmetro	Descrição	Exemplo de valor
PFS	Algoritmo usado pela função Perfect forward secret (PFS). PFS suporta os seguintes algoritmos: ● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 O algoritmo padrão é **DH group 14**.	DH group 14
Transfer Protocol	Protocolo de segurança usado no IPsec para transmitir e encapsular dados do usuário. Os seguintes protocolos são suportados: ● ESP ● AH ● AH-ESP O protocolo padrão é **ESP**.	ESP
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma SA será renegociada quando sua vida útil expirar. O valor padrão é **3600**.	3600

⚠ CUIDADO

Os seguintes algoritmos não são recomendados porque não são seguros o suficiente:

Algoritmos de autenticação: SHA1 e MD5

Algoritmo de encritação: 3DES

Algoritmos DH: Group 1, Group 2 e Group 5

7. Confirme as informações do gateway de VPN e clique em **Buy Now**.

   Depois que um gateway de VPN é criado, o sistema atribui automaticamente um endereço IP público, ou seja, o endereço IP exibido na coluna **Gateway IP Address** na

lista de gateways de VPN. O endereço IP do gateway também é o endereço IP do gateway remoto configurado na rede da VPN local. **Figura 3-2** mostra o endereço IP do gateway.

Figura 3-2 Lista de gateways de VPN

3.4 Compra de uma conexão de VPN

Cenários

Para conectar seu data center local ou rede privada aos ECSs em uma VPC, você precisa criar uma conexão de VPN depois que um gateway de VPN for obtido.

Procedimento

1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
4. No painel de navegação à esquerda, escolha **Virtual Private Network** > **Classic – VPN Connections**.

   Se a VPN de Edição Empresarial estiver disponível para a região selecionada, escolha **Virtual Private Network** > **Classic**.
5. Na página **VPN Connections**, clique em **Buy VPN Connection**.
6. Configure os parâmetros conforme solicitado e clique em **Next**. **Tabela 3-9** lista os parâmetros de conexão de VPN.

Tabela 3-9 Descrição dos parâmetros de conexão de VPN

Parâmetro	Descrição	Exemplo de valor
Region	As regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas umas às outras, portanto, os recursos não podem ser compartilhados entre regiões. Para baixa latência de rede e rápido acesso a recursos, selecione a região mais próxima de seus usuários-alvo.	CN North-Beijing4
Name	Nome de uma conexão de VPN.	vpn-001
VPN Gateway	Nome do gateway de VPN para o qual a conexão de VPN é criada.	vpcgw-001

Parâmetro	Descrição	Exemplo de valor
Local Subnet	Sub-redes da VPC que acessarão sua rede local por meio de uma VPN. Você pode definir a sub-rede local usando um dos seguintes métodos: ● **Select subnet**: selecione as sub-redes que precisam acessar seu data center local ou rede privada. ● **Specify CIDR block**: insira os blocos CIDR que precisam acessar seu data center local ou rede privada. **NOTA** Blocos CIDR de sub-redes locais não podem se sobrepor.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	O endereço IP público do gateway em seu data center ou na rede privada. Esse endereço IP é usado para se comunicar com sua VPC.	N/D
Remote Subnet	As sub-redes da sua rede local que acessarão uma VPC por meio de uma VPN. As sub-redes locais e remotas não podem se sobrepor. A sub-rede remota não pode se sobrepor a blocos CIDR envolvidos em conexões de emparelhamento de VPC, Direct Connect ou Cloud Connect existentes criadas para a VPC local. **NOTA** Blocos CIDR de sub-redes remotas não podem se sobrepor.	192.168.3.0/24, 192.168.4.0/24
PSK	Chave privada compartilhada por duas extremidades de uma conexão de VPN para negociação. As PSKs configuradas em ambas as extremidades da conexão da VPN devem ser as mesmas. A PSK: ● Contém 6 a 128 caracteres. ● Pode conter apenas: – Dígitos – Letras – Caracteres especiais: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Digite a PSK novamente.	Test@123

Parâmetro	Descrição	Exemplo de valor
Advanced Settings	● **Default**: utilizar políticas de IKE e IPsec predefinidas. ● **Existing**: usar as políticas de IKE e IPsec existentes. ● **Custom**: incluindo a **IKE Policy** e a **IPsec Policy**, que especificam os algoritmos de encriptação e autenticação de um túnel de VPN. Para obter detalhes sobre as políticas, consulte **Tabela 3-10** e **Tabela 3-11**.	Custom

Tabela 3-10 IKE policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128

Parâmetro	Descrição	Exemplo de valor
DH Algorithm	Algoritmo de troca de chaves Diffie-Hellman. Os seguintes algoritmos são suportados: ● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 O algoritmo padrão é **Group 14**.	Group 14
Version	Versão do protocolo IKE. O valor pode ser um dos seguintes: ● v1 (não recomendado devido a riscos de segurança) ● v2 O valor padrão é **v2**.	v2
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma AS será renegociada quando sua vida útil expirar. O valor padrão é **86400**.	86400

Tabela 3-11 IPsec policy

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● SHA2-256 ● SHA2-384 ● SHA2-512 O algoritmo padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-192 ● AES-256 ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) O algoritmo padrão é **AES-128**.	AES-128
PFS	Algoritmo usado pela função Perfect forward secret (PFS). PFS suporta os seguintes algoritmos: ● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 O algoritmo padrão é **DH group 14**.	DH group 14

Parâmetro	Descrição	Exemplo de valor
Transfer Protocol	Protocolo de segurança usado no IPsec para transmitir e encapsular dados do usuário. Os seguintes protocolos são suportados: ● AH ● ESP ● AH-ESP O protocolo padrão é **ESP**.	ESP
Lifetime (s)	Tempo de vida de uma Associação de segurança, em segundos Uma AS será renegociada quando sua vida útil expirar. O valor padrão é **3600**.	3600

NOTA

Uma política de IKE especifica os algoritmos de encritação e autenticação a utilizar na fase de negociação de um túnel de IPsec. Uma política de IPsec especifica o protocolo, o algoritmo de encritação e o algoritmo de autenticação a utilizar na fase de transmissão de dados de um túnel de IPsec. As políticas de IKE e IPsec devem ser as mesmas em ambas as extremidades de uma conexão de VPN. Se forem diferentes, a conexão de VPN não pode ser configurada.

Os seguintes algoritmos não são recomendados porque não são seguros o suficiente:

- Algoritmos de autenticação: SHA1 e MD5
- Algoritmo de encritação: 3DES
- Algoritmos DH: Group 1, Group 2 e Group 5

7. Clique em **Submit**.
8. Você precisa configurar um túnel de VPN de IPsec no roteador ou firewall em seu data center local.

3.5 Configuração do dispositivo remoto

Para obter detalhes sobre como configurar o dispositivo remoto, consulte **Virtual Private Network Administrator Guide**. Este guia ajuda você a configurar o dispositivo de VPN local para implementar a interconexão entre sua rede local e a sub-rede da VPC.

Para obter detalhes sobre os exemplos de configuração, consulte o seguinte:

- **Série Huawei USG6600**
- **Configuração de VPN quando o firewall Fortinet FortiGate é usado**
- **Configuração de VPN quando o firewall Sangfor é usado**
- **Uso do cliente de VPN IPSec TheGreenBow para configurar a comunicação dentro e fora da nuvem**
- **Uso de Openswan para configurar a comunicação dentro e fora da nuvem**

- **Uso de strongSwan para configurar a comunicação dentro e fora da nuvem**

