Virtual Private Network

Guia de usuário

Edição 01

Data 14-04-2023

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 Gerenciamento de gateway de VPN

1.1 Criação de um gateway de VPN

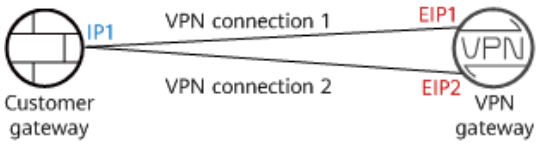
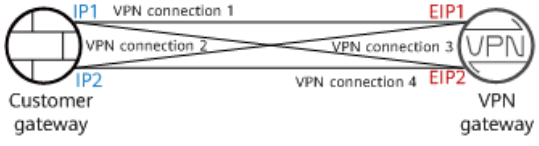
Cenários

Para conectar seu data center local ou sua rede privada aos ECSs em uma VPC, primeiro crie um gateway VPN.

Contexto

A rede recomendada varia de acordo com o número de endereços IP do gateway de cliente, conforme descrito em **Tabela 1-1**.

Tabela 1-1 Redes

Número de endereços IP do gateway de cliente	Redes recomendadas	Descrição
1		Um grupo de conexão de VPN é usado.
2		Dois grupos de conexão de VPN são usados.

- Se o data center local tiver apenas um gateway de cliente configurado com apenas um endereço IP, recomendamos que você crie uma conexão de VPN entre cada um dos EIPs

ativos e em espera do gateway de VPN e o endereço IP do gateway de cliente. Neste cenário, apenas um grupo de conexão de VPN é utilizado.

- Se o data center local tiver dois gateways de cliente ou um gateway de cliente configurado com dois endereços IP, Recomendamos que você crie uma conexão VPN entre cada um dos EIPs ativos e em espera do gateway de VPN e os dois gateways de cliente ou endereços IP diferentes do mesmo gateway de cliente. Nesse cenário, dois grupos de conexão de VPN são usados.

Pré-requisitos

- Uma VPC foi criada. Para obter detalhes sobre como criar uma VPC, consulte **Criação de uma VPC e uma 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** .
- Um roteador empresarial foi criado se você quiser usá-lo para se conectar a um gateway de VPN. Para obter detalhes, consulte a documentação do roteador corporativo.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, clique em **Buy VPN Gateway**.
6. Defina os parâmetros conforme solicitado e clique em **Next**.

   Tabela 1-2 lista os parâmetros do gateway de VPN.

Tabela 1-2 Descrição dos parâmetros do gateway de VPN

Parâmetro	Descrição	Exemplo de valor
Billing Mode	● **Yearly/Monthly**: você é cobrado por mês ou ano ao criar um gateway de VPN Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. ● **Pay-per-use**: os gateways de VPN e os grupos de conexão de VPN são cobrados por duração de uso e o ciclo de cobrança é de 1 hora.	Yearly/Monthly
Region	Para baixa latência de rede e rápido acesso a recursos, selecione a região mais próxima de seus usuários-alvo. Os recursos não podem ser compartilhados entre regiões.	AP-Singapore

Parâmetro	Descrição	Exemplo de valor
Name	Nome de um gateway de VPN.	vpngw-001
Tipo de rede	● **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	● VPC Por meio de uma VPC, o gateway de VPN envia mensagens para o gateway de cliente ou para os servidores na sub-rede local. ● Enterprise Router Por meio de um roteador empresarial, o gateway de VPN envia mensagens para o gateway do cliente ou para os servidores nas sub-redes de todas as VPCs conectadas ao roteador empresarial. **NOTA** Nesta encenação, preste atenção ao limite superior das entradas na tabela de roteamento do roteador empresarial. Se o número de rotas anunciadas pelo gateway de cliente e pelo gateway de VPN exceder esse limite superior, o roteador empresarial não poderá aprender as rotas em excesso. Como resultado, o tráfego não será encaminhado entre o gateway de VPN e o gateway de cliente.	VPC
Enterprise Router	Este parâmetro está disponível somente quando **Associate With** está definido como **Enterprise Router**. Selecione um roteador empresarial.	er-001
VPC	Selecione uma VPC.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Sub-rede usada pelo gateway de VPN para se comunicar com uma VPC. Planeje uma sub-rede independente com uma máscara de menos de 29 bits na VPC para o gateway de VPN. A sub-rede não pode se sobrepor às sub-redes da VPC em uso.	192.168.66.0/24

Parâmetro	Descrição	Exemplo de valor
Local Subnet	Esse parâmetro está disponível somente quando **Associate With** está definido como **VPC**. Sub-redes da VPC com as quais seu data center local precisa se comunicar por meio do gateway de cliente. ● Selecionar sub-rede Selecione as sub-redes da VPC local. ● Inserir bloco CIDR Insira sub-redes da VPC local ou sub-redes da VPC que estabelecem uma conexão de emparelhamento com a VPC local.	192.168.1.0/24,192.168.2.0/24
BGP ASN	BGP ASN do gateway de VPN, que não pode ser 100. O BGP ASN do gateway de VPN deve ser diferente daquele do gateway de cliente.	64512
Specification	Largura de banda de encaminhamento e número máximo de conexões de VPN suportadas pelo gateway de VPN. ● Edição profissional – Largura de banda máxima: 1 Gbit/s – Número máximo de grupos de conexão de VPN: 100	Edição profissional
AZ	Uma AZ é uma localização geográfica com fonte de alimentação independente e instalações de rede em uma região. As AZs na mesma VPC são interconectadas por meio de redes privadas e são fisicamente isoladas. ● Se duas ou mais AZs estiverem disponíveis, selecione duas AZs. O gateway de VPN implantado em duas AZs tem maior disponibilidade. Recomendamos que você selecione as AZs nas quais os recursos da VPC estão localizados. ● Se apenas uma AZ estiver disponível, selecione essa AZ.	AZ1, AZ2

Parâmetro	Descrição	Exemplo de valor
VPN Connection Groups	Esse parâmetro está disponível somente quando o **Billing Mode** está definido como **Yearly/Monthly**. Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. ● Se uma conexão de VPN for criada entre cada um dos EIPs ativos e em espera de um gateway de VPN e o mesmo endereço IP de um gateway de cliente, somente um grupo de conexão será usado. ● Se uma conexão de VPN for criada entre cada um dos EIPs ativos e em espera de um gateway de VPN e endereços IP diferentes de um gateway de cliente ou endereços IP de gateways de cliente diferentes, dois grupos de conexão serão usados.	10
Active EIP	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. EIP usado pelo gateway de VPN para se comunicar com um gateway de cliente. ● **Buy Now**: comprar um novo EIP. O modo de cobrança do novo EIP é o mesmo do gateway de VPN. ● **Use existing**: usar um EIP existente.	Buy Now
Billed By	Esse parâmetro está disponível somente quando o **Billing Mode** está definido como **Pay-per-use** e o **Network Type** está definido como **Public network**. 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 de saída enviado pela VPC.	Traffic

Parâmetro	Descrição	Exemplo de valor
Bandwidth (Mbit/s)	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. Largura de banda do EIP, em Mbit/s. ● Todas as conexões de VPN criadas usando o EIP compartilham a largura de banda do EIP. A largura de banda total consumida por todas as conexões de VPN não pode exceder a largura de banda do EIP. Se o tráfego de rede exceder a largura de banda do EIP, poderá ocorrer congestionamento da rede e as conexões 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. ● Algumas regiões suportam apenas 300 Mbit/s de largura de banda por padrão. Se for necessária uma largura de banda maior, solicite uma largura de banda de 300 Mbit/s e, em seguida, **envie um tíquete de serviço** para a expansão da capacidade.	10 Mbit/s
Bandwidth Name	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. Nome da largura de banda do EIP.	Vpngw-bandwtidh1
Standby EIP	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. Um gateway de VPN precisa estar vinculado a um par de EIPs: EIPs ativos e em espera. Você pode planejar a largura de banda e o modo de cobrança para cada EIP.	-

Parâmetro	Descrição	Exemplo de valor
Billed By	Esse parâmetro está disponível somente quando o **Billing Mode** está definido como **Pay-per-use** e o **Network Type** está definido como **Public network**. 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 de saída enviado pela VPC.	Traffic
Bandwidth (Mbit/s)	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. Largura de banda do EIP, em Mbit/s. ● Todas as conexões de VPN criadas usando o EIP compartilham a largura de banda do EIP. A largura de banda total consumida por todas as conexões de VPN não pode exceder a largura de banda do EIP. Se o tráfego de rede exceder a largura de banda do EIP, 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. ● Algumas regiões suportam apenas 300 Mbit/s de largura de banda por padrão. Se for necessária uma largura de banda maior, solicite uma largura de banda de 300 Mbit/s e, em seguida, **envie um tíquete de serviço** para a expansão da capacidade.	10 Mbit/s
Bandwidth Name	Este parâmetro só está disponível quando o **Network Type** está definido como **Public network**. Nome da largura de banda do EIP.	Vpngw-bandwtidh2

Parâmetro	Descrição	Exemplo de valor
Enterprise Project	O projeto empresarial ao qual a VPN pertence. Um projeto empresarial facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O projeto padrão é **default**. Para obter detalhes sobre como criar e gerenciar projetos da empresa, consulte o *Guia de usuário do Enterprise Management*.	default
Access VPC	Este parâmetro só está disponível quando o **Network Type** está definido como **Private network**. Se um gateway de VPN precisar se conectar a VPCs diferentes nas direções sul e norte, defina a VPC na direção norte como a VPC de acesso. A VPC na direção sul é a VPC associada ao gateway de VPN.	O mesmo que a VPC associado
Access Subnet	Este parâmetro só está disponível quando o **Network Type** está definido como **Private network**. Por padrão, um gateway de VPN usa a sub-rede de interconexão para se conectar à VPC associada. Defina este parâmetro quando outra sub-rede precisar ser usada.	Igual à sub-rede de interconexão
Required Duration	Esse parâmetro está disponível somente quando o **Billing Mode** está definido como **Yearly/Monthly**. Se o saldo da sua conta for suficiente e você selecionar **Auto-renew**, o sistema renovará automaticamente o serviço quando a duração necessária terminar. ● Assinatura mensal: seu serviço é renovado automaticamente mensalmente. ● Assinatura anual: seu serviço é renovado automaticamente por ano.	6

7. Confirme os detalhes do pedido e clique em **Pay Now**.

1.2 Visualização de um gateway de VPN

Cenários

Depois de criar um gateway de VPN, você pode ver seus detalhes.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, veja a lista de gateways de VPN.
6. Clique no nome de um gateway de VPN para visualizar suas informações básicas e endereços IP públicos.

NOTA

Na lista de gateways de VPN, você pode localizar a conexão de VPN de destino e clicar em para exibir a largura de banda e o tráfego do gateway de VPN.

1.3 Modificação de um gateway de VPN

Cenários

- Você pode modificar informações básicas sobre um gateway de VPN, incluindo o nome e as sub-redes locais.

Modificar informações básicas

Cenário

Você pode modificar o nome e a sub-rede local de um gateway de VPN.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e clique em **Modify Basic Information** na coluna **Operation**.

   Para modificar apenas o nome de um gateway de VPN, você também pode clicar em ao lado do nome do gateway de VPN.

6. Modifique o nome e a sub-rede local do gateway de VPN conforme solicitado.
7. Clique em **OK**.

1.4 Vinculação de um EIP a um gateway de VPN

Cenários

Você pode vincular um EIP a um gateway de VPN que tenha sido criado.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e clique em **Bind EIP** na coluna **Operation**.

   Um gateway de VPN pode ter um EIP ativo e um EIP em espera vinculado.
6. Selecione o EIP desejado e clique em **OK**.

1.5 Desvinculação de um EIP de um gateway de VPN

Cenários

Depois de criar um gateway de VPN, você pode desvincular um EIP dele.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e clique em **Unbind EIP** na coluna **Operation**.

   Você pode desvincular o EIP ativo ou em espera, ou ambos, do gateway de VPN.
6. Na caixa de diálogo exibida, clique em **Yes**.

   NOTA

   - Um EIP que está em uso por uma conexão de VPN não pode ser desvinculado de um gateway de VPN.
   - Um EIP continuará a ser cobrado depois de ser desvinculado de um gateway de VPN. Se você não precisar mais de um EIP, é aconselhável liberá-lo.

1.6 Cancelamento de assinatura de um gateway de VPN anual/mensal

Cenários

Se um gateway de VPN anual/mensal não for mais necessário, você pode cancelar a assinatura dele.

NOTA

Cancelar a assinatura de um gateway anual/mensal também excluirá as conexões VPN criadas para o gateway. Portanto, tenha cuidado ao realizar esta operação.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e escolha **More** > **Unsubscribe** na coluna **Operation**.
6. Cancele a assinatura do gateway de VPN conforme solicitado.

1.7 Renovação de um gateway de VPN anual/mensal

Cenários

Você pode renovar um gateway de VPN anual/mensal que está prestes a expirar.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino. Na coluna **Operation**, escolha **More** > **Renew**.
6. Conclua a renovação conforme solicitado.

1.8 Exclusão de um gateway de VPN de pagamento por uso

Cenários

Você pode excluir um gateway de VPN de pagamento por uso não é mais necessário.

Restrições e limitações

- Um gateway de VPN que está sendo criado, atualizado ou excluído não pode ser excluído.
- Se um gateway de VPN tiver conexões de VPN configuradas, você precisará excluir todas as conexões de VPN antes de excluir o gateway de VPN.

  Para obter detalhes sobre como excluir uma conexão de VPN, consulte **Exclusão de uma conexão de VPN**.
- Se um gateway de VPN estiver vinculado a um EIP cobrado no modo anual/mensal, você precisará desvincular o EIP antes de excluir o gateway de VPN.

  Para obter detalhes sobre como desvincular um EIP, consulte **Desvinculação de um EIP de um gateway de VPN**.
- Se um gateway de VPN estiver vinculado a um EIP faturado no modo de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP.

  Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway de VPN. Para obter detalhes sobre como desvincular um EIP, consulte **Desvinculação de um EIP de um gateway de VPN**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. No painel de navegação à esquerda, escolha **Virtual Private Network** > **VPN Gateways**.
4. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e escolha **More** > **Delete** na coluna **Operation**.
5. Na caixa de diálogo exibida, clique em **Yes**.

2 Gerenciamento do gateway de cliente

2.1 Criação de um gateway de cliente

Cenários

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

Procedimento

1. Acesse o 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** > **Customer Gateways**.
5. Na página **Customer Gateways**, clique em **Create Customer Gateway**.
6. Defina os parâmetros conforme solicitado e clique em **OK**.

   Tabela 2-1 lista os parâmetros do gateway do cliente.

   Tabela 2-1 Descrição dos parâmetros do gateway do cliente

Parâmetro	Descrição	Exemplo de valor
Name	Nome de um gateway do cliente.	cgw-001

Parâmetro	Descrição	Exemplo de valor
Routing Mode	Modo de roteamento do gateway do cliente. ● Selecione **Static** quando **VPN Type** estiver definido como **Route-based** e **Routing Mode** estiver definido como **Static** para a conexão de VPN. ● Selecione **Dynamic (BGP)** quando o **VPN Type** estiver definido como **Route-based** e o **Routing Mode** estiver definido como **Dynamic (BGP)** para a conexão de VPN. – Ao selecionar esta opção, certifique-se de que o gateway de cliente ofereça suporte ao BGP dinâmico. – O gateway de cliente pode anunciar um máximo de 100 rotas BGP ao gateway de VPN. Se mais de 100 rotas BGP forem anunciadas, o relacionamento de par de BGP será desconectado, causando a interrupção do tráfego entre o gateway de VPN e o gateway de cliente. ● Recomendamos que selecione **Static** quando o **VPN Type** estiver definido como **Policy-based** para a conexão de VPN.	Static
BGP ASN	Este parâmetro só está disponível quando o **Routing Mode** está definido como **Dynamic (BGP)**. Insira o ASN do seu data center local ou rede privada. O BGP ASN do gateway de cliente deve ser diferente daquele do gateway de VPN.	65000
Endereço IP do gateway	Endereço IP público usado pelo gateway de cliente para se comunicar com o gateway de VPN. O valor deve ser um endereço estático. Assegure-se que a porta UDP 4500 é permitida em uma regra de firewall no gateway de cliente em seu data center local ou rede privada.	1.2.3.4

7. (Opcional) Se houver dois endereços IP de gateway do cliente, repita as operações anteriores para configurar o gateway de cliente com outro endereço IP.

Operações relacionadas

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

2.2 Visualização de um gateway de cliente

Cenários

Depois de criar um gateway de cliente, você pode visualizar seus detalhes.

Procedimento

1. Acesse o 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** > **Customer Gateways**.
5. Na página **Customer Gateway**, visualize a lista de gateways de cliente.

2.3 Modificação de um gateway de cliente

Cenários

Depois de criar um gateway de cliente, você pode alterar seu nome.

Procedimento

1. Acesse o 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** > **Customer Gateways**.
5. Na página **Customer Gateway**, clique em ao lado do nome de um gateway de cliente.
6. Digite um novo nome para o gateway de cliente e clique em **OK**.

2.4 Exclusão de um gateway de cliente

Cenários

Você pode excluir um gateway de cliente que você criou.

Procedimento

1. Acesse o 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** > **Customer Gateways**.
5. Na página **Customer Gateway**, localize o gateway de cliente a ser deletado e clique em **Delete** na coluna **Operation**.

   Antes de excluir um gateway de cliente associado a uma conexão de VPN, remova o gateway de cliente da conexão de VPN.
6. Clique em **Yes**.

3 Gerenciamento de conexão de VPN

3.1 Criação de uma conexão de VPN

Cenários

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

Procedimento

1. Acesse o 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** > **VPN Connections**.
5. Na página **VPN Connections**, clique em **Buy VPN Connection**.

   NOTA

   Para maior confiabilidade, é recomendável criar uma conexão de VPN entre cada um dos EIPs ativos e em espera de um gateway de VPN da Huawei Cloud e o endereço IP de um gateway de cliente.
6. Defina os parâmetros conforme solicitado e clique em **Next**.

   Tabela 3-1 lista os parâmetros de conexão de VPN.

   Tabela 3-1 Descrição dos parâmetros de conexão de VPN

Parâmetro	Descrição	Exemplo de valor
Name	Nome de uma conexão de VPN.	vpn-001

Parâmetro	Descrição	Exemplo de valor
VPN Gateway	Nome do gateway VPN para o qual a conexão VPN é criada. Você também pode clicar em **Create VPN Gateway** para criar um gateway de VPN. Para obter detalhes sobre os parâmetros relacionados, consulte **Tabela 1-2**.	vpngw-001
Gateway IP Address	EIP ativo ou em espera vinculado ao gateway de VPN. O mesmo EIP de um gateway de VPN não pode ser selecionado repetidamente quando você cria conexões VPN entre o gateway de VPN e o mesmo gateway de cliente.	EIP ativo/em espera no grupo de EIP
Customer Gateway	Nome de um gateway de cliente. Você também pode clicar em **Create Customer Gateway** para criar um gateway de cliente. Para obter detalhes sobre os parâmetros relacionados, consulte **Tabela 2-1**. **NOTA** Se um gateway de cliente se conectar a vários gateways de VPN, os ASNs BGP e os tipos de VPN dos gateways de VPN deverão ser os mesmos.	cgw-001

Parâmetro	Descrição	Exemplo de valor
VPN Type	Modo de conexão de IPsec, que pode ser baseado em rotas ou políticas. ● Static routing Determina os dados que entram no túnel de VPN IPsec com base na configuração da rota (sub-rede local e sub-rede do cliente). O protocolo BGP é suportado. Cenário de aplicação: acesso multi-site e acesso de rota em larga escala ● BGP routing O gateway de cliente pode anunciar um máximo de 100 rotas BGP ao gateway de VPN. Se mais de 100 rotas BGP forem anunciadas, o relacionamento de par de BGP será desconectado, causando a interrupção do tráfego entre o gateway de VPN e o gateway do cliente. ● Policy-based Determina os dados que entram no túnel VPN IPsec com base na política (entre a rede do cliente e a VPC). Os fluxos de dados a serem criptografados podem ser personalizados. Cenário de aplicação: acesso a um único local	Static routing

Parâmetro	Descrição	Exemplo de valor
Sub-rede do cliente	Sub-redes em seu data center local que precisam se comunicar com uma VPC por meio do gateway do cliente. Se houver várias sub-redes de clientes, separe-as com vírgulas (,). **NOTA** ● Uma sub-rede de cliente não pode ser incluída em nenhuma sub-rede local ou em nenhuma sub-rede da VPC à qual o gateway da VPN está conectado. ● Não use 100.64.0.0/10 como a sub-rede do cliente. Caso contrário, serviços como Object Storage Service (OBS), DNS e gateway de API ficarão indisponíveis. ● Quando **Associate With** estiver definido como **VPC** para o gateway de VPN e **VPN Type** estiver definido como **Static routing** para a conexão de VPN, não defina **Customer Subnet** como **0.0.0.0**. Caso contrário, o tráfego pode não ser encaminhado.	172.16.1.0/24,172.16.2.0/24

Parâmetro	Descrição	Exemplo de valor
Interface IP Address Assignment	Esse parâmetro está disponível somente quando o **VPN Type** é definido como **Route-based**. **NOTA** • Defina os endereços IP da interface para os endereços IP da interface do túnel usados pelo gateway de VPN e pelo gateway de cliente para se comunicarem entre si. • Se o endereço da interface do túnel do gateway de cliente for fixo, selecione **Manually specify** e defina o endereço da interface do túnel do gateway deVPN com base no endereço da interface do túnel do gateway do cliente. • Manually specify Defina o **Local Interface IP Address** como o endereço da interface do túnel do gateway de VPN, que pode residir apenas no bloco CIDR 169.254.x.x/30 (exceto 169.254.195.x/30). Em seguida, o sistema define automaticamente **Customer Interface IP Address** para um valor aleatório com base na configuração do **Local Interface IP Address**. Por exemplo, quando você define o **Local Interface IP Address** como **169.254.1.6/30**, o sistema define automaticamente o **Customer Interface IP Address** como **169.254.1.5/30**. • Automatically assign Por padrão, um endereço IP no bloco CIDR 169.254.x.x/30 é atribuído à interface de túnel do gateway de VPN. Para exibir os endereços IP da interface local e do cliente atribuídos automaticamente, clique em **Modify VPN Connection** na página **VPN Connections**.	Automatically assign

Parâmetro	Descrição	Exemplo de valor
Endereço IP da interface local	Esse parâmetro está disponível somente quando a **Interface IP Address Assignment** está definida como **Manually specify**. Endereço IP da interface do túnel configurado no gateway de VPN.	N/D
Customer Interface IP Address	Esse parâmetro está disponível somente quando a **Interface IP Address Assignment** está definida como **Manually specify**. Endereço IP da interface do túnel configurado no dispositivo de gateway de cliente.	N/D
Link Detection	Este parâmetro só está disponível quando o **Routing Mode** está definido como **Static**. **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 não será encaminhado. Depois que essa função é ativada, o gateway de VPN executa automaticamente a Análise de Qualidade da Rede (NQA) no endereço IP da interface do cliente do gateway de cliente.	Selecionado
PSK	As PSKs configuradas para o gateway de VPN e o gateway do cliente devem ser os mesmos. A PSK: ● contém de 8 a 128 caracteres. ● Pode conter apenas três ou mais tipos dos seguintes caracteres: – Dígitos – Letras maiúsculas – Letras minúsculas – Caracteres especiais: ~ ! @ # $ % ^ ( ) - _ + = { } , . / : ;	Test@123
Confirm PSK	Digite o PSK novamente.	Test@123

Parâmetro	Descrição	Exemplo de valor
Policy	Este parâmetro só está disponível quando o **VPN Type** está definido como **Policy-based**. Define o fluxo de dados que entra na conexão de VPN criptografada entre as sub-redes local e cliente. Você precisa configurar os blocos CIDR de origem e destino em cada regra de política. Por padrão, um máximo de cinco regras de política podem ser configuradas. ● Source CIDR Block O bloco CIDR de origem deve conter alguns blocos CIDR do local sub-redes. **0.0.0.0/0** indica qualquer endereço IP. ● Destination CIDR block O bloco CIDR de destino deve conter todos os blocos CIDR das sub-redes do cliente. Uma regra de política suporta um máximo de cinco blocos CIDR de destino, que são separados por vírgulas (,). **NOTA** Quando **Associate With** estiver definido como **VPC** para o gateway de VPN e **VPN Type** estiver definido como **Static routing** para a conexão DE VPN, não defina **Destination CIDR Block** como **0.0.0.0**. Caso contrário, o tráfego pode não ser encaminhado.	● Source CIDR block 1: 192.168.1.0/24 ● Destination CIDR block 1: 172.16.1.0/24,172.16.2.0/24 ● Source CIDR block 2: 192.168.2.0/24 ● Destination CIDR block 2: 172.16.1.0/24,172.16.2.0/24
Policy Settings	● **Default**: utilizar políticas IKE e IPsec predefinidas. ● **Custom**: utilizar políticas IKE e IPsec personalizadas. Para obter detalhes sobre as políticas, consulte **Tabela 3-2** e **Tabela 3-3**.	Custom

Tabela 3-2 Política IKE

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● SHA1 (não recomendado devido a riscos de segurança) ● MD5 (não recomendado devido a riscos de segurança) ● SHA2-256 ● SHA2-384 ● SHA2-512 O valor padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-256 ● AES-192 ● 3DES (não recomendado devido a riscos de segurança) ● AES-256-GCM-16 Quando este algoritmo de encritação é utilizado, a versão IKE só pode ser **v2**. O valor padrão é **AES-128**.	AES-128
DH Algorithm	Os seguintes algoritmos são suportados: ● Group 1 (não recomendado devido a riscos de segurança) ● Group 2 (não recomendado devido a riscos de segurança) ● Group 5 (não recomendado devido a riscos de segurança) ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 O valor padrão é **Group 14**.	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 (SA). Uma SA será renegociada quando sua vida útil expirar. ● Unidade: segundo ● O valor padrão é **86400**.	86400
Negotiation Mode	Esse parâmetro está disponível somente quando a **Version** é **v1**. ● Main ● Aggressive	Main
Local ID	Identificador de autenticação do gateway de VPN usado na negociação de IPsec. O ID do gateway de VPN configurado no gateway de cliente deve ser o mesmo que o ID local configurado aqui. Caso contrário, a negociação IPsec falha. ● IP Address (valor padrão) O sistema define automaticamente esse parâmetro para o EIP selecionado do gateway de VPN. ● FQDN Defina o nome de domínio qualificado completo (FQDN) para uma cadeia de 6 a 16 caracteres que pode conter letras maiúsculas, minúsculas, dígitos e pontos (.).	IP Address

Parâmetro	Descrição	Exemplo de valor
Customer ID	Identificador de autenticação do gateway do cliente usado na negociação de IPsec. O ID do gateway do cliente configurado no gateway do cliente deve ser o mesmo que o ID do cliente configurado aqui. Caso contrário, a negociação IPsec falha. ● Endereço IP (valor padrão) O sistema define automaticamente esse parâmetro para o endereço IP do gateway do cliente. ● FQDN Defina o FQDN para uma cadeia de 6 a 16 caracteres que pode conter letras maiúsculas, minúsculas, dígitos e pontos (.).	IP Address

Tabela 3-3 Política IPSec

Parâmetro	Descrição	Exemplo de valor
Authentication Algorithm	Algoritmo de hash usado para autenticação. Os seguintes algoritmos são suportados: ● SHA1 (não recomendado devido a riscos de segurança) ● MD5 (não recomendado devido a riscos de segurança) ● SHA2-256 ● SHA2-384 ● SHA2-512 O valor padrão é **SHA2-256**.	SHA2-256
Encryption Algorithm	Algoritmo de encritação. Os seguintes algoritmos são suportados: ● AES-128 ● AES-256 ● AES-192 ● 3DES (não recomendado devido a riscos de segurança) ● AES-256-GCM-16 O valor padrão é **AES-128**.	AES-128

Parâmetro	Descrição	Exemplo de valor
PFS	Algoritmo usado pela função Perfect forward secret (PFS). O PFS suporta os seguintes algoritmos: ● DH group 1 (não recomendado devido a riscos de segurança) ● DH group 2 (não recomendado devido a riscos de segurança) ● DH group 5 (não recomendado devido a riscos de segurança) ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 ● Disable O valor 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 O valor padrão é **ESP**.	ESP
Lifetime (s)	Tempo de vida de uma SA. Uma SA será renegociada quando sua vida útil expirar. ● Unidade: segundo ● O valor padrão é **3600**.	3600
Modo de encapsulamento de pacotes	O valor padrão é **TUNNEL**.	TUNNEL

NOTA

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

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

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

7. Confirme a nova configuração de conexão de VPN e clique em **Submit**.
8. Repita as operações anteriores para criar a outra conexão de VPN.

   Para obter detalhes sobre a configuração do endereço IP, consulte **Contexto**.

3.2 Visualização de uma conexão de VPN

Cenários

Depois de criar uma conexão de VPN, você pode ver seus detalhes.

Procedimento

1. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
2. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
3. No painel de navegação à esquerda, escolha **Virtual Private Network** > **VPN Connections**.
4. Na página **VPN Connections**, veja a lista de conexões de VPN.
5. Clique no nome de uma conexão de VPN para exibir suas informações básicas.

NOTA

- Na página de detalhes da conexão de VPN, pode clicar em **Modify Policy Settings** para ver detalhes sobre as políticas IKE e IPsec da conexão de VPN.
- Na lista de conexões de VPN, você pode localizar a conexão de VPN de destino e clicar em **View Metric** para exibir informações de monitoramento sobre a conexão de VPN.

3.3 Modificação de uma conexão de VPN

Cenários

Uma conexão de VPN é um canal de comunicação criptografado estabelecido entre um gateway de VPN em uma VPC e um gateway de cliente em seu data center local. Você pode modificar uma conexão de VPN quando necessário.

Procedimento

1. Acesse o 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** > **VPN Connections**.
5. Na página **VPN Connections**, localize a conexão de VPN a ser modificada e clique em **Modify VPN Connection**.
6. Modifique os parâmetros de conexão de VPN conforme solicitado.
7. Clique em **OK**.

⚠ CUIDADO

Se você alterar o PSK ou modificar a política IKE ou IPsec de uma conexão de VPN, certifique-se de que as novas configurações sejam consistentes com as do gateway do cliente. Caso contrário, a conexão de VPN será interrompida.

Apenas alguns dos parâmetros entram em vigor imediatamente após serem modificados, conforme descrito em **Tabela 3-4**.

Tabela 3-4 Hora em que as novas configurações de parâmetros entram em vigor

Item	Parâmetro	Quando as novas configurações entram em vigor	Como modificar
-	PSK	● Quando IKEv1 é usado, as novas configurações tomam o efeito no período de negociação seguinte. ● Quando o IKEv2 é usado, o PSK não pode ser alterado no console de gerenciamento.	● Quando IKEv1 é usado: localize a conexão de VPN a ser modificada, escolha **More** > **Reset PSK** à direita e altere a PSK conforme solicitado. ● Quando IKEv2 é usado: 1. Exclua a conexão de VPN atual. 2. Crie uma nova conexão de VPN.
Política IKE (IKEv1)	Encryption Algorithm	As novas configurações entram em vigor no próximo período de negociação.	Localize a conexão de VPN a ser modificada e clique em **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		

Item	Parâmetro	Quando as novas configurações entram em vigor	Como modificar
	Negotiation Mode		
	Local ID		
	Customer ID		
	Version	As novas configurações entram em vigor imediatamente.	
	Lifetime (s)		
Política IKE (IKEv2)	Encryption Algorithm	As novas configurações entram em vigor no próximo período de negociação.	Localize a conexão de VPN a ser modificada e clique em **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		
	Version	As novas configurações entram em vigor imediatamente.	
	Lifetime (s)		
	Local ID	Atualmente, os parâmetros não podem ser modificados no console de gerenciamento.	1. Exclua a conexão de VPN atual. 2. Crie uma nova conexão de VPN.
	Customer ID		
Política IPSec	Encryption Algorithm	As novas configurações entram em vigor no próximo período de negociação.	Localize a conexão de VPN a ser modificada e clique em **Modify VPN Configuration**.
	Authentication Algorithm		
	PFS		
	Transfer Protocol	As novas configurações entram em vigor imediatamente.	

Item	Parâmetro	Quando as novas configurações entram em vigor	Como modificar
	Lifetime (s)		

3.4 Exclusão de uma conexão de VPN

Cenários

Se uma conexão de VPN não for mais necessária, você poderá excluí-la para liberar recursos de rede.

Procedimento

1. Acesse o 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** > **VPN Connections**.
5. Na página **VPN Connections**, escolha **More** > **Delete** na coluna **Operation** de uma conexão de VPN.
6. Na caixa de diálogo exibida, clique em **Yes**.

4 VPN Fee Management

4.1 Changing the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateways**.
5. Locate a pay-per-use VPN gateway, and choose **More** > **Change Billing Mode** in the **Operation** column.
   - You can change the billing mode of the VPN gateway and bound EIPs to yearly/monthly simultaneously. Alternatively, you can only change the billing mode of the VPN gateway to yearly/monthly, and retain the billing mode of the bound EIPs as pay-per-use.

     Only when the EIPs bound to a VPN gateway are billed by bandwidth in pay-per-use mode, you can change the billing modes of the VPN gateway and EIPs to yearly/monthly simultaneously.
   - Billing formula change

     Assume that *X* VPN connection groups are in use before the billing mode is changed to yearly/monthly. Then, after the billing mode is changed, the billing formula changes to: Fee of the VPN gateway + Fee of (*X* – 10) VPN connection groups.
6. In the **Change Billing Mode** dialog box, click **OK**.
7. Confirm the VPN gateway information and set a renewal duration.
8. Click **Pay**.
9. On the payment page, confirm the order information, select a coupon or discount, and select the payment method.
10. Click **Pay**.

NOTA

Changing the billing mode of a VPN gateway from pay-per-use to yearly/monthly will not affect your services.

4.2 Increasing or Decreasing the Bandwidth of an EIP Billed on a Yearly/Monthly Basis

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateways**.
5. Click the name of a pay-per-use VPN gateway.
6. In the **EIP** area, click **Change** next to **Bandwidth (Mbit/s)**.
7. On the **Modify Bandwidth** page, select your required bandwidth and click **Next**.
8. Click **Submit**.
   - If the bandwidth is increased, the new bandwidth takes effect immediately after you pay the extra fees.
   - If the bandwidth is decreased, the new bandwidth takes effect only within the renewal period.

5 Gerenciamento de gateway de VPN clássica

5.1 Visualização de um gateway de VPN

Cenários

Depois de criar um gateway de VPN, você pode visualizar seus detalhes.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Veja informações sobre o seu gateway de VPN.

5.2 Modificação de um gateway de VPN

Modificar informações básicas sobre um gateway de VPN

Cenário

Você pode modificar o nome e a descrição de um gateway de VPN.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway VPN que você deseja modificar e escolha **More** > **Modify Basic Information** na coluna **Operation**.

6. Modifique o nome ou a descrição do gateway de VPN conforme necessário.
7. Clique em **OK**.

Modificar a largura de banda do gateway de VPN

Cenário

Quando a largura de banda de um gateway de VPN não pode atender aos seus requisitos de serviço, você pode modificar a largura de banda do gateway de VPN.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e escolha **More** > **Modify Bandwidth** na coluna **Operation**.
6. Modifique a largura de banda conforme necessário.
7. Clique em **Submit**.

5.3 Cancelamento da assinatura de um gateway de VPN anual/mensal

Cenários

Se um gateway de VPN anual/mensal não for mais necessário, você pode cancelar a assinatura dele.

NOTA

- Você não precisa criar uma conexão de VPN juntamente com um gateway de VPN anual/mensal.
- Cancelar a assinatura de um gateway anual/mensal também excluirá as conexões de VPN criadas para o gateway. Portanto, tenha cuidado ao realizar esta operação.

Procedimento

1. Acesse o 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** > **VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e escolha **More** > **Unsubscribe** na coluna **Operation**.
6. Cancele a assinatura do gateway de VPN conforme solicitado.

5.4 Exclusão de um gateway de VPN de pagamento por uso

Cenários

Se um gateway de VPN não for mais necessário, você poderá excluí-lo para liberar recursos de rede, desde que ele não tenha conexões de VPN configuradas.

Se tiver alguma conexão configurada, exclua as conexões primeiro.

NOTA

Se você criar um gateway de VPN de pagamento por uso, uma conexão de VPN será criada junto com o gateway. Se você excluir todas as conexões de VPN criadas para um gateway de VPN pago por uso, o gateway de VPN será excluído automaticamente. Para mais detalhes, consulte **Exclusão de uma conexão de VPN**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. No painel de navegação à esquerda, escolha **Virtual Private Network** > **VPN Gateways**.
4. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino. Na coluna **Operation**, escolha **More** > **Delete**.
5. Na caixa de diálogo exibida, clique em **Yes**.

6 Gerenciamento de conexões de VPN clássica

6.1 Visualização de uma conexão de VPN

Cenários

Depois de criar uma conexão de VPN, você pode ver seus detalhes.

Procedimento

1. Acesse o 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** > **VPN Connections**.

   Se a VPN estiver disponível para a região selecionada, escolha **Virtual Private Network** > **Classic VPNs** e clique na guia **VPN Connections**.
5. Na página **VPN Connections**, visualize as informações de conexão de VPN. Também pode localizar a linha que contém a conexão de VPN de destino e, na coluna **Operation**, clique em **View Policy** para ver os detalhes da política IKE e IPsec sobre a conexão de VPN.

6.2 Modificação de uma conexão de VPN

Cenários

Uma conexão de VPN é um canal de comunicação criptografado estabelecido entre o gateway de VPN em sua VPC e aquele em um data center local. A conexão de VPN pode ser modificada após a criação.

⚠ CUIDADO

Se você modificar as configurações avançadas, as comunicações de rede podem ser interrompidas. Tenha cuidado ao realizar esta operação.

Modificar o PSK somente não excluirá a conexão de VPN atual. O novo PSK entra em vigor durante a renegociação do IKE após a expiração da vida útil do IKE.

Procedimento

1. Acesse o 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** > **VPN Connections**.

   Se a VPN estiver disponível para a região selecionada, escolha **Virtual Private Network** > **Classic VPNs** e clique na guia **VPN Connections**.
5. Na página **VPN Connections**, localize a linha que contém a conexão de VPN de destino e clique em **Modify** na coluna **Operation**.
6. Na caixa de diálogo **Modify VPN Connection** exibida, modifique os parâmetros conforme necessário.
7. Clique em **OK**.

6.3 Exclusão de uma conexão de VPN

Cenários

Se uma conexão de VPN não for mais necessária, você poderá excluí-la para liberar recursos de rede.

Quando você excluir a última conexão de VPN de um gateway de VPN pago por uso, o gateway de VPN associado também será excluído.

Procedimento

1. Acesse o 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** > **VPN Connections**.

   Se a VPN estiver disponível para a região selecionada, escolha **Virtual Private Network** > **Classic VPNs** e clique na guia **VPN Connections**.
5. Na página **VPN Connections**, localize a linha que contém a conexão de VPN. Na coluna **Operation**, escolha **More** > **Delete**.
6. Na caixa de diálogo exibida, clique em **Yes**.

7 Gerenciamento de VPN clássica (LA-Mexico City1/LA-Sao Paulo1)

7.1 Visualização de VPNs compradas

Cenários

Você pode ver detalhes sobre uma VPN existente.

Procedimento

1. Acesse o 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** exibida, visualize a VPN de destino. **Tabela 7-1** descreve o status da VPN.

Tabela 7-1 Status da VPN

Status	Descrição
Normal	A VPN é criada com êxito e o data center local pode acessar a VPC corretamente.
Not connected	A VPN foi criada com sucesso, mas não foi usada para comunicação com o data center local.
Creating	A VPN está sendo criada.
Updating	As informações da VPN estão sendo atualizadas.
Deleting	A VPN está sendo excluída.
Abnormal	A VPN é anormal.
Frozen	A VPN está congelada.

7.2 Modificação de uma VPN comprada

Cenários

Se as informações de rede VPN entrarem em conflito com as informações de rede da VPC ou precisarem ser ajustadas com base no ambiente de rede mais recente, você poderá modificar a VPN.

Procedimento

1. Acesse o 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**, localize a VPN de destino e clique em **Modify**.
5. Na caixa de diálogo exibida, modifique os parâmetros como solicitado.
6. Clique em **OK**.

7.3 Exclusão de uma VPN

Cenários

Você pode excluir uma VPN se ela não for mais necessária.

Procedimento

1. Acesse o 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**, localize a VPN de destino e clique em **Delete**.
5. Na caixa de diálogo exibida, clique em **Yes**.

8 Classic VPN Fee Management

8.1 Changing a Pay-Per-Use VPN Gateway from Being Billed by Bandwidth to Being Billed by Traffic or the Other Way Around

Procedure

1. On the **VPN Gateways** page, locate the row that contains the target VPN gateway.
2. Choose **More** > **Modify Bandwidth** in the **Operation** column.
3. On the **Modify Bandwidth** page, set **Billed By** to **Bandwidth** in the **Modify Specifications** area.
4. Click **Submit**.

9 Monitoramento

9.1 Monitoramento de VPN

O Cloud Eye permite que você fique atento ao desempenho e à utilização de recursos das VPNs, garantindo a confiabilidade e disponibilidade de VPN. Você pode usar o Cloud Eye para monitorar as VPN automaticamente em tempo real e gerenciar alarmes e notificações para acompanhar as métricas de desempenho de VPN.

NOTA

O Cloud Eye não é suportado na região LA-Sao Paulo1.

9.2 Métricas

Descrição

Esta seção descreve as métricas monitoradas e relatadas pela VPN ao Cloud Eye, bem como seus namespaces e dimensões. Você pode usar o console de gerenciamento do Cloud Eye para consultar as métricas dos objetos monitorados e dos alarmes gerados para a VPN.

Namespace

SYS.VPN

Métricas

Tabela 9-1 Métricas suportadas para gateways de VPN e gateways de VPN clássica

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
upstream_bandwidth	Largura de banda de saída	Taxa de rede de tráfego de saída (anteriormente chamada de "Largura de banda upstream") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto
downstream_bandwidth	Largura de banda de entrada	Taxa de rede de tráfego de entrada (anteriormente chamada de "Largura de banda downstream") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto
upstream_bandwidth_usage	Uso de largura de banda de saída	Uso da largura de banda de saída, em porcentagem.	0-100%	Largura de banda ou EIP	1 minuto
downstream_bandwidth_usage	Uso da largura de banda de entrada	Uso da largura de banda de entrada, em porcentagem.	0-100%	Largura de banda ou EIP	1 minuto
up_stream	Tráfego de saída	Tráfego de rede de saída (anteriormente chamado de "Tráfego upstream") Unidade: byte	≥ 0 bytes	Largura de banda ou EIP	1 minuto
down_stream	Tráfego de entrada	Tráfego de rede de entrada (anteriormente chamado de "Tráfego downstream") Unidade: byte	erro 0 bytes	Largura de banda ou EIP	1 minuto

Tabela 9-2 Métricas de conexão de VPN

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
private_average_latency	Tempo médio de ida e volta da rede privada	Tempo médio de ida e volta (RTT) entre o endereço da interface de túnel do gateway de VPN e o do gateway de cliente	0 - 5000 ms	Conexão de VPN	1 minuto
private_max_latency	Tempo máximo de ida e volta da rede privada	RTT máximo entre o endereço da interface de túnel do gateway de VPN e o do gateway de cliente	0 - 5000 ms	Conexão de VPN	1 minuto
private_packet_loss_rate	taxa de perda de pacotes da rede privada	Taxa de perda de pacotes entre o endereço da interface de túnel do gateway de VPN e o do gateway de cliente	0-100 %	Conexão de VPN	1 minuto
public_average_latency	Tempo médio de ida e volta da rede pública	RTT médio entre o endereço IP público do gateway de VPN e o do gateway de cliente	0 - 5000 ms	Conexão de VPN	1 minuto
public_max_latency	Tempo máximo de ida e volta da rede pública	RTT máximo entre o endereço IP público do gateway de VPN e o do gateway de cliente	0 - 5000 ms	Conexão de VPN	1 minuto
public_packet_loss_rate	Taxa de perda de pacotes da rede pública	Taxa de perda de pacotes entre o endereço IP público do gateway de VPN e o do gateway de cliente	0 - 100 %	Conexão de VPN	1 minuto

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
connection_status	Status da conexão de VPN	Status da conexão de VPN: **0**: uma conexão de VPN está no status **Not connected**. **1**: uma conexão de VPN está no status **Connected**.	0 ou 1	Conexão de VPN	1 minuto

Tabela 9-3 Métricas de conexão de VPN clássica

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
connection_status	Status da conexão de VPN	Status da conexão de VPN: **0**: uma conexão de VPN está no status **Not connected**. **1**: uma conexão de VPN está no status **Connected**.	0 ou 1	Conexão de VPN	5 minutos

Dimensões

chave	Valor
connection_id	Conexões VPN
vpn_connection_id	Conexões dedicadas
publicip_id	ID do EIP
bandwidth_id	ID da largura de banda

9.3 Exibição de métricas

Cenários

Exibir o status da conexão de VPN e os usos da largura de banda e do EIP.

Suporte para Métricas

Tabela 9-4 Suporte para métricas

Nome da métrica	Suporte	Habilitado por padrão?
Status da conexão de VPN	Suportado por VPN e VPN clássico	Sim
● Tempo médio de ida e volta da rede pública ● tempo máximo de ida e volta da rede pública ● taxa de perda de pacotes da rede pública	Suportados apenas por VPN	Não Você pode clicar no nome de uma conexão de VPN e adicionar um item de verificação de integridade na página da guia **Summary**.
● Tempo médio de ida e volta da rede privada ● rede privada tempo máximo de ida e volta ● taxa de perda de pacotes da rede privada	Suportados apenas por VPN	Sim As métricas de monitoramento de rede privada são suportadas somente quando uma conexão de VPN usa o modo de roteamento estático e tem NQA ativado.

Exibir métricas de conexão de VPN

- Visualizar métricas no console da VPN
  a. Acesse o console de gerenciamento.
  b. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
  c. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
  d. Escolha **Virtual Private Network** > **VPN Connections**.
     Para VPN clássica, escolha **Virtual Private Network** > **Classic VPNs**, e clique na guia **VPN Connections**.
  e. Localize a conexão de VPN de destino e clique no ícone de **View Metric**.

Para VPN clássica, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

Você pode exibir dados das últimas 1, 3, 12 ou 24 horas ou dos últimos 7 dias.

- Visualização de métricas no console do Cloud Eye
  a. Acesse o console de gerenciamento.
  b. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
  c. Clique em **Service List** e escolha **Management & Governance** > **Cloud Eye**.
  d. Escolha **Cloud Service Monitoring** > **Virtual Private Network**.
  e. Clique na guia **Dedicated Connections**, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

     Para a VPN clássica, clique na guia **VPN Connections**, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

     Você pode exibir dados das últimas 1, 3, 12 ou 24 horas ou dos últimos 7 dias.

Exibir as métricas do gateway de VPN

- Visualizar de métricas no console da VPN (recomendado)
  a. Acesse o console de gerenciamento.
  b. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
  c. Clique em **Service List** e escolha **Networking** > **Virtual Private Network**.
  d. Escolha **Virtual Private Network** > **VPN Gateways**.

     Para VPN Clássica, escolha **Virtual Private Network** > **Classic VPNs**, e clique na guia **VPN Gateways**.

  e. Localize o gateway de VPN de destino e clique em na coluna **Public IP Address** para exibir os dados de monitoramento de EIP do gateway de VPN.

     Para a VPN Clássica, localize o gateway de VPN de destino e clique em **View Metric** na coluna **Operation** para exibir os dados de monitoramento de EIP do gateway de VPN.

     Você pode exibir dados das últimas 1, 3, 12 ou 24 horas ou dos últimos 7 dias.
- Visualizar métricas no console do Cloud Eye
  a. Acesse o console de gerenciamento.
  b. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
  c. Clique em **Service List** e escolha **Management & Governance** > **Cloud Eye**.
  d. Escolha **Cloud Service Monitoring** > **Elastic IP and Bandwidth**.
  e. Localize o EIP de um gateway de VPN e clique em **View Metric** na coluna **Operation** para exibir os dados de monitoramento do EIP.

     Você pode exibir dados das últimas 1, 3, 12 ou 24 horas ou dos últimos 7 dias.

9.4 Criação de regras de alarme

Cenários

Você pode configurar regras de alarme no console do Cloud Eye para acompanhar o status da VPN a qualquer momento.

Procedimento

1. Acesse o 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 **Management & Governance** > **Cloud Eye**.
4. Escolha a **Cloud Service Monitoring** > **Virtual Private Network**, localize a conexão de VPN do alvo, e o clique **Create Alarm Rule** na coluna **Operation**.

   Para VPN, configure regras de alarme na página de guia **Dedicated Connections**. Para a VPN clássica, configure as regras de alarme na página de guia **VPN Connections**.

   - Por padrão, a VPN não fornece nenhum modelo de alarme. Você precisa clicar em **Create Custom Template** para criar um modelo primeiro. Em seguida, escolha **Cloud Service Monitoring** > **Virtual Private Network** e clique em **Create Alarm Rule** para configurar uma regra de alarme.
   - Por padrão, a VPN clássica fornece um modelo de alarme chamado **Virtual Private Network Alarm Template**. Você pode usar esse modelo padrão sem criar um novo.

     Se a política de alarme no modelo de alarme padrão não atender aos seus requisitos, você poderá criar um modelo de alarme personalizado clicando em **Create Custom Template**. Em seguida, escolha **Cloud Service Monitoring** > **Virtual Private Network** e clique em **Create Alarm Rule** para configurar uma regra de alarme.
5. Clique em **Create**.

   Depois que a regra de alarme for criada, se você tiver ativado a **Alarm Notification** e configurado os parâmetros necessários, você receberá notificações assim que um alarme for acionado.

   NOTA

   Para obter mais informações sobre regras de alarme de VPN, consulte **Guia de usuário do Cloud Eye**.

10 Auditoria

10.1 Operações de VPN que podem ser gravadas pelo CTS

NOTA

O Cloud Trace Service (CTS) não é suportado nas regiões LA-Mexico City1 e LA-Sao Paulo1.

Tabela 10-1 Operações de VPN que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criar um gateway do cliente	customer-gateway	createCgw
Atualizar um gateway do cliente	customer-gateway	updateCgw
Excluir um gateway do cliente	customer-gateway	deleteCgw
Criar um gateway de VPN	vpn-gateway	createVgw
Atualizar um gateway de VPN	vpn-gateway	updateVgw
Excluir um gateway de VPN	vpn-gateway	deleteVgw
Criar um gateway de VPN anual/mensal	vpn-gateway	CreatePrePaidVgw
Atualizar o status do gateway de VPN	vpn-gateway	UpdateResourceState
Criar uma conexão de VPN	vpn-connection	createVpnConnection

Operação	Tipo de recurso	Nome do rastreamento
Atualizar uma conexão de VPN	vpn-connection	updateVpnConnection
Excluir uma conexão de VPN	vpn-connection	deleteVpnConnection

Tabela 10-2 Operações de VPN clássica que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criar uma conexão de VPN	VpnConnection	createVpnConnection
Atualizar uma conexão de VPN	VpnConnection	updateVpnConnection
Excluir uma conexão de VPN	VpnConnection	deleteVpnConnection
Criar um gateway de VPN	VpnGw	createVpnGw
Atualizar um gateway de VPN	VpnGw	updateVpnGw
Excluir um gateway de VPN	VpnGw	deleteVpnGw

10.2 Consulta de rastreamentos do CTS

Quando o CTS está habilitado, o sistema começa a gravar as operações executadas em recursos de VPN. Você pode exibir os registros de operação dos últimos sete dias no console de gerenciamento do CTS.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 No painel de navegação à esquerda, clique em  e escolha **Management & Governance** > **Cloud Trace Service**.

Passo 3 No painel de navegação, escolha **Trace List**.

Passo 4 Especifique os critérios de pesquisa conforme necessário.

- Intervalo de tempo de pesquisa: no canto superior direito, escolha **Last 1 hour**, **Last 1 day** ou **Last 1 week**, ou especifique um intervalo de tempo personalizado.
- **Trace Type**, **Trace Source**, **Resource Type** e **Search By**: selecione um filtro na lista suspensa.

Se você selecionar **Resource ID** para **Search By**, especifique um ID do recurso.

Se você selecionar **Data** para **Trace Type**, só poderá filtrar os rastreamentos por rastreador.

- **Operator**: selecione um ou mais operadores na lista suspensa.
- **Trace Status**: selecione um dos **All trace statuses**, **Normal**, **Warning** e **Incident**.

Passo 5 Clique em **Query**.

Passo 6 Clique em à esquerda de um traço para expandir seus detalhes.

Passo 7 Clique em **View Trace** na coluna **Operation** para exibir o conteúdo detalhado de um rastreamento.

----Fim

11 Gerenciamento de permissões

11.1 Criação de um usuário e concessão de permissões de VPN

Este tópico descreve como usar **IAM** para implementar o controle de permissões refinado para seus recursos de VPN. Com o IAM, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos de VPN.
- Conceder somente as permissões necessárias para que os usuários executem uma tarefa específica.
- Confiar uma conta da Huawei Cloud ou serviço de nuvem para realizar O&M profissional e eficiente em seus recursos de VPN.

Se sua conta da Huawei Cloud não exigir usuários individuais do IAM, pule este capítulo.

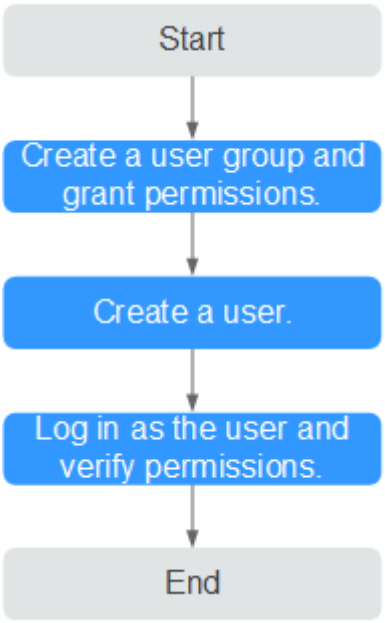
Esta seção descreve o procedimento para conceder permissões (consulte **Figura 11-1**).

Pré-requisitos

Saiba mais sobre as permissões (consulte **Gerenciamento de permissões**) suportadas pela VPN e escolha políticas ou funções com base em seus requisitos. Para obter permissões de sistema de outros serviços de nuvem, consulte **Permissões do sistema**.

Fluxo do processo

Figura 11-1 Processo para conceder permissões da VPN



1. **Crie um grupo de usuários e atribua permissões** para ele.

   Crie um grupo de usuários no console do IAM e anexe a política **VPN Administrator** ao grupo.

2. **Crie um usuário do IAM** e adicione-o a um grupo de usuários.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.

3. **Faça logon** e verifique as permissões.

   Faça logon no console de gerenciamento como o usuário criado. Alterne para a região autorizada e verifique as permissões.

   - Clique em **Service List** e escolha **Networking** > **Virtual Private Network**. Clique em **Buy VPN Gateway** no canto superior direito. Se o gateway de VPN for criado com êxito, a política **VPN Administrator** já entrou em vigor.
   - Escolha qualquer outro serviço na **Service List**. Se for exibida uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política **VPN Administrator** já entrou em vigor.

11.2 Políticas personalizadas de VPN

As políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema da VPN.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: selecione serviços em nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe de política.
- JSON: edite políticas de JSON do zero ou com base em uma política existente.

Para obter detalhes, consulte **Criação de uma política personalizada**. A seção seguinte contém exemplos de políticas personalizadas comuns de VPN.

Exemplo de política personalizada de VPN

- Exemplo 1: permitir que os usuários excluam gateways de VPN

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        }
    ]
}
```

- Exemplo 2: negar aos utilizadores a exclusão de uma conexão de VPN

  Uma política com apenas permissões de Deny deve ser usada em conjunto com outras políticas para entrar em vigor. Se as políticas atribuídas a um usuário contiverem ações Allow e Deny, as ações Deny terão precedência sobre as ações Allow.

  O método a seguir pode ser usado se você precisar atribuir permissões da política de **VPN FullAccess** a um usuário, mas também proibir o usuário de excluir conexões de VPN. Crie uma política personalizada para negar a exclusão de conexão e atribua ambas as políticas ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações na VPN, exceto excluir conexões de VPN. O seguinte é um exemplo de uma política de negação:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        }
    ]
}
```

- Exemplo 3: definir várias ações em uma política

  Uma política personalizada pode conter ações de vários serviços do tipo global ou de nível de projeto. Veja a seguir um exemplo de política que contém ações de vários serviços:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:create",
                "vpn:vpnConnections:create",
                "vpn:customerGateways:create"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "vpn:vpnGateways:delete",
                "vpn:vpnConnections:delete",
                "vpn:customerGateways:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:vpcs:list",
```



```
                "vpc:subnets:get"
            ]
        }
    ]
}
```


12 Cotas

O que é cota?

As cotas podem limitar o número ou a quantidade de recursos disponíveis para os usuários, como o número máximo dos ECSs ou discos EVS que podem ser criados.

Se a cota de recursos existente não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.

Tipos de recurso

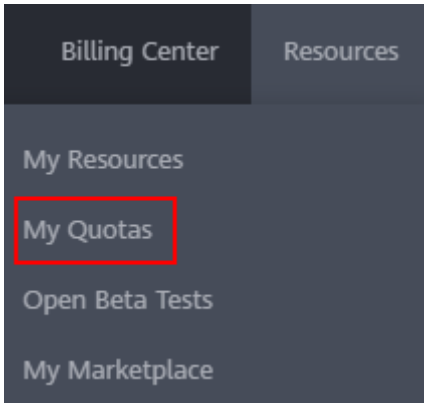
- Os recursos de VPN clássica incluem gateways de VPN clássica e conexões de VPN clássica.
- Os recursos de VPN incluem gateways de VPN, grupos de conexão de VPN e gateways de clientes.

A cota total de cada tipo de recurso varia de acordo com as regiões.

Como fazer para ver minhas cotas?

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Service Quota** é exibida.

   Figura 12-1 Minhas cotas

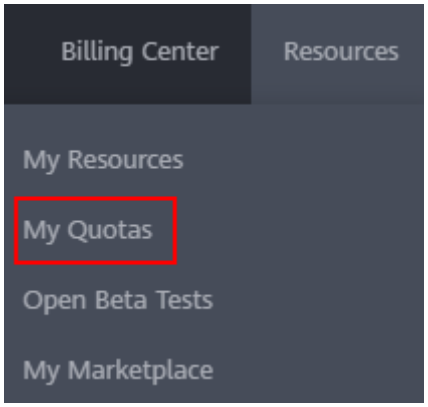


4. Visualize a cota usada e total de cada tipo de recursos na página exibida.
   Se uma cota não puder atender aos requisitos de serviço, solicite uma cota mais alta.

Como fazer para solicitar uma cota mais alta?

1. Acesse o console de gerenciamento.
2. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Service Quota** é exibida.

   Figura 12-2 Minhas cotas



3. Clique em **Increase Quota**.
4. Na página **Create Service Ticket**, configure os parâmetros conforme necessário.
   Na área **Problem Description**, preencha o conteúdo e o motivo do ajuste.
5. Depois que todos os parâmetros necessários estiverem configurados, selecione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** e clique em **Submit**.

