Virtual Private Network

# Perguntas frequentes

**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 Perguntas populares

## 1.1 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud é compatível com o protocolo IPsec (Internet Protocol Security) padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implementado atrás de um gateway NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores domésticos comuns de banda larga, hosts de Windows que fornecem serviços VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os seguintes produtos podem se conectar à Huawei Cloud por meio de VPNs:
  - Dispositivos: firewalls e roteadores de acesso (ARs) da Huawei, firewalls de Hillstone e firewalls de Check Point
  - Serviços em nuvem: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) e Microsoft Azure
  - Software: StrongSwan
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud através de uma VPN.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- Alguns dispositivos suportam VPN IPsec somente após a compra das licenças de software necessárias.

  O administrador do centro de dados no local pode verificar com o fornecedor do dispositivo se é necessária uma licença com base no modelo do dispositivo.

# 1.2 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 1-1** Parâmetros de negociação de VPN

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● AES-256-GCM-16 |
| | DH Algorithm | ● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21 |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Lifetime (s) | **86400** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Local ID | ● Endereço IP<br>O endereço IP local é exibido automaticamente como o EIP do gateway de VPN, eliminando a necessidade de configurá-lo manualmente.<br>● FQDN<br>Por padrão, o tipo de ID local é o endereço IP e o valor de ID local é o EIP do gateway de VPN. |
| | Customer ID | ● Endereço IP<br>● FQDN<br>Por padrão, o tipo de ID do cliente é o endereço IP e o valor de ID do cliente é o endereço IP público do gateway do cliente. |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256-GCM-16 |
| | PFS | ● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor padrão)<br>● DH group 15<br>● DH group 16<br>● DH group 19<br>● DH group 20<br>● DH group 21<br>● Disable |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Transfer Protocol | ● ESP (valor padrão) |
| | Lifetime (s) | **3600** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **30** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Quando o PFS estiver habilitado, uma troca de DH adicional será executada durante a negociação da AS do IPsec para gerar uma nova chave da AS do IPsec, melhorando a segurança da AS do IPsec.
- Por motivos de segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no dispositivo de gateway no data center local e que as configurações do PFS em ambas as extremidades sejam as mesmas. Caso contrário, a negociação falhará.
- O tempo de vida padrão baseado em tráfego de uma AS de IPsec é de 1.843.200 KB e não pode ser alterado para a VPN da Huawei Cloud. Este parâmetro não está envolvido na negociação e não tem impacto no estabelecimento de uma AS de IPsec.

# 1.3 Quais são os tipos de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

1. Acesse ao console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

   **Figura 1-1** Criar tíquete de serviço

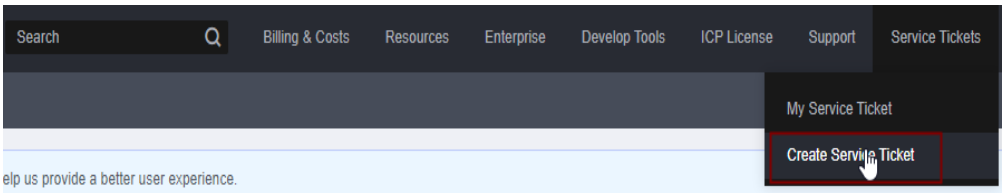
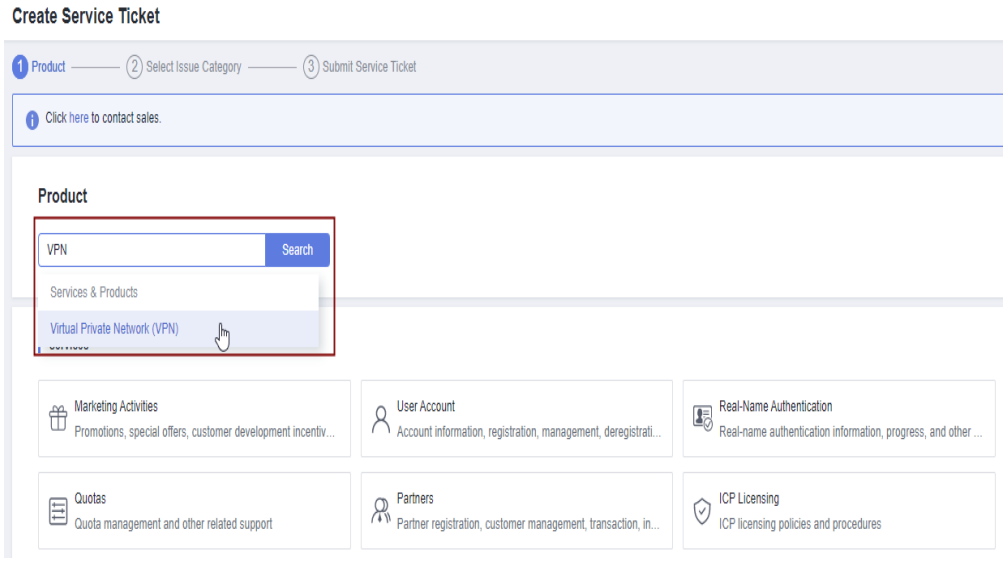
   
   
3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 1-2** Selecionar **Virtual Private Network (VPN)**



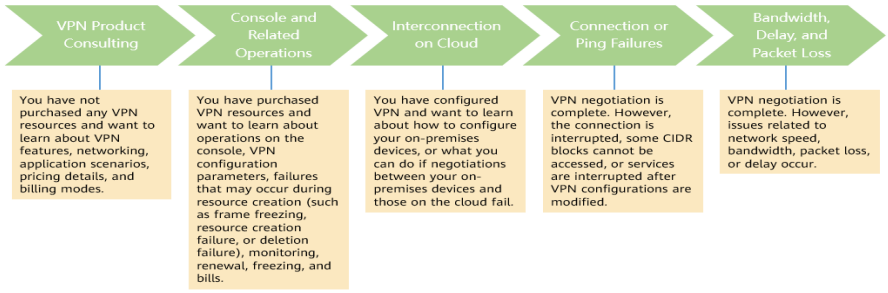

4. Selecione uma categoria de problema.

**Figura 1-3** Selecionar categoria de problema


NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 1-4** Categoria de emissão e base de classificação



# 1.4 Posso implementar uma aplicação na nuvem, bancos de dados em um data center local e depois conectá-la por meio de uma VPN?

Sim.

Uma VPN conecta uma VPC e um data center local.

Depois que uma VPN é configurada, o tráfego de serviço pode ser transmitido entre a VPC e o data center local. Para um servidor de aplicações na nuvem, o acesso a um banco de dados local é logicamente o mesmo que o acesso a outros hosts na mesma LAN. Diante disso, é possível usar uma VPN para conectar uma aplicação na nuvem a um banco de dados em um data center local.

Este é um cenário típico de VPN IPsec.

Além disso, não há limitações no iniciador do serviço. Ou seja, as solicitações de serviço podem ser iniciadas a partir da nuvem ou do data center local.

**AVISO**

- Depois que uma VPN estiver configurada, verifique a latência da rede e a taxa de perda de pacotes para garantir o bom funcionamento do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

# 1.5 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

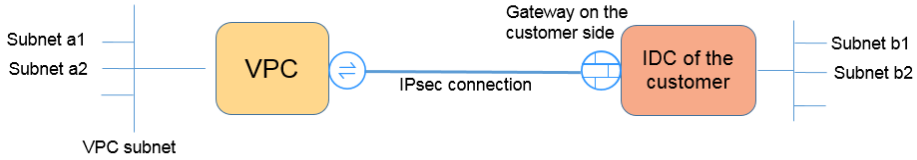
A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

# 1.6 O que é uma conexão de VPN? Como definir o número de conexões de VPN ao comprar um gateway de VPN?

Uma conexão de VPN da Huawei Cloud é uma conexão IPsec estabelecida entre um gateway de VPN na nuvem e um endereço IP público independente de um data center local. Você pode configurar várias sub-redes locais (sub-redes da VPC) e sub-redes de clientes (sub-redes locais) para uma conexão de VPN.

O número de conexões de VPN a serem criadas é determinado pelo número de data centers locais. Cada conexão de VPN pode conectar uma VPC a apenas um data center local.




NOTA

Na figura anterior, se as sub-redes a1 e a2 na Huawei Cloud precisarem se comunicar com as sub-redes b1 e b2 na rede local, você precisará criar apenas uma conexão de VPN, com os blocos CIDR de origem definidos como a1 e a2 e os blocos CIDR de destino definidos como b1 e b2.

# 1.7 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Para exibir o status de uma conexão de VPN, clique em na coluna **Monitoring** da conexão de VPN.

# 1.8 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A PSK é configurada em um gateway de VPN e uma conexão será estabelecida após a conclusão da negociação de VPN. Portanto, nenhum nome de usuário ou senha é necessário para criar uma conexão de VPN IPsec. Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

O IPsec XAUTH fornece autenticação estendida para VPN IPsec. Ele requer que os usuários insiram seus nomes de usuário e senhas durante a negociação da VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

# 1.9 Quais são as diferenças entre VPN IPsec e VPN SSL em cenários de aplicações e modos de conexão?

## Cenários de aplicação

VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

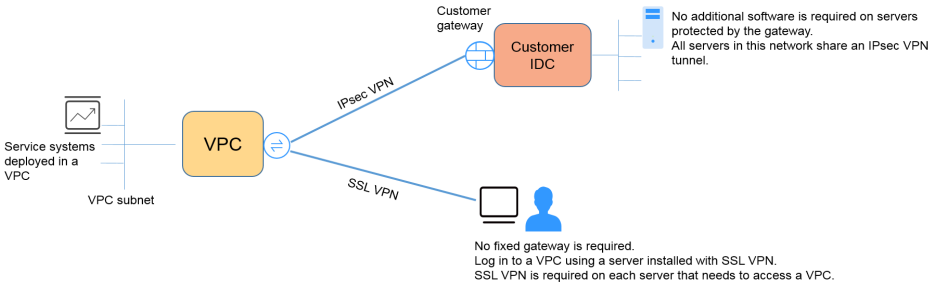
VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

### Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para permitir que eles concluam a negociação de VPN IPsec.

VPN SSL requer um programa cliente específico instalado em hosts. Os usuários precisam inserir nomes de usuário e senha para conectar os hosts aos servidores SSL.




**NOTA**

A Huawei Cloud suporta apenas VPN IPsec.

# 1.10 Uma conexão de VPN IPsec é estabelecida automaticamente?

Sim. Uma conexão de VPN IPsec é estabelecida automaticamente.

# 1.11 Como será cobrado pelo uso de uma VPN? Será cobrado pelos EIPs do gateway de VPN?

As VPNs são cobradas pelos seguintes itens em uma base anual/mensal ou pagamento por uso.

- Gateway de VPN
- Conexão de VPN

  Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Caso necessário você pode comprar conexões de VPN adicionais.
- Largura de banda EIP de um gateway de VPN

  A largura de banda do gateway de VPN pode ser faturada por tráfego ou largura de banda.

  a. Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.

  b. O ciclo de faturamento do modo de cobrança pagamento por uso é de 1 hora. Quando você cria um gateway de VPN pago por uso, o sistema solicita que você crie conexões de VPN. Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Se mais grupos de conexão forem necessários, você precisará comprá-los.

NOTA

Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

# 1.12 O EIP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Se um EIP de pagamento por uso estiver vinculado a um gateway de VPN de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP vinculado.

Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway da VPN.

# 1.13 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As seguintes informações de largura de banda de um endereço IP de gateway de VPN podem ser monitoradas: tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as informações de monitoramento, clique em  na coluna **Gateway IP Address** na lista de gateways de VPN.

**Conexão de VPN**

As seguintes informações sobre uma conexão de VPN podem ser monitoradas: status da conexão de VPN, tempo médio de ida e volta (RTT) do link, RTT máximo do link, taxa de perda de pacotes do link, RTT médio do túnel, RTT máximo do túnel e taxa de perda de pacotes do túnel.

Para monitorar o RTT médio do link, o RTT máximo do link, a taxa de perda de pacotes do link, o RTT médio do túnel, o RTT máximo do túnel e a taxa de perda de pacotes do túnel, clique no nome da conexão de VPN e em **Add** na área **Health Check** da página da guia **Summary** para adicionar itens de verificação de integridade.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 1.14 Em que direção a largura de banda da VPN é limitada? Qual é a unidade de largura de banda?

A largura de banda do gateway de VPN adquirida aplica-se à direção de saída da Huawei Cloud. Para obter um equilíbrio entre as larguras de banda nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada da seguinte forma:

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

# 1.15 Como a velocidade da rede de uma conexão de VPN é testada?

Ambiente de teste: uma conexão de VPN foi criada. Os ECSs foram criados nas sub-redes locais das VPCs nas duas extremidades da conexão de VPN. Os ECSs podem fazer ping um ao outro.

**Quando a largura de banda de um gateway de VPN adquirido é de 200 Mbit/s:**

1. Quando os ECSs nas duas extremidades da conexão de VPN executam o Windows, o iPerf3 e o FileZilla são usados para testar a velocidade da rede. O resultado do teste é de 180 Mbit/s, atendendo aos requisitos.

   NOTA

   O protocolo FTP baseado em TCP tem um mecanismo de controle de congestionamento e o protocolo IPsec adiciona novos cabeçalhos aos pacotes originais. Como tal, é normal na indústria, ter um desvio de velocidade de rede de cerca de 10%.

   **Figura 1-5** mostra o resultado do teste da largura de banda de 200 Mbit/s no cliente iPerf3.

   **Figura 1-5** Resultado do teste para largura de banda de 200 Mbit/s (cliente de iPerf3)

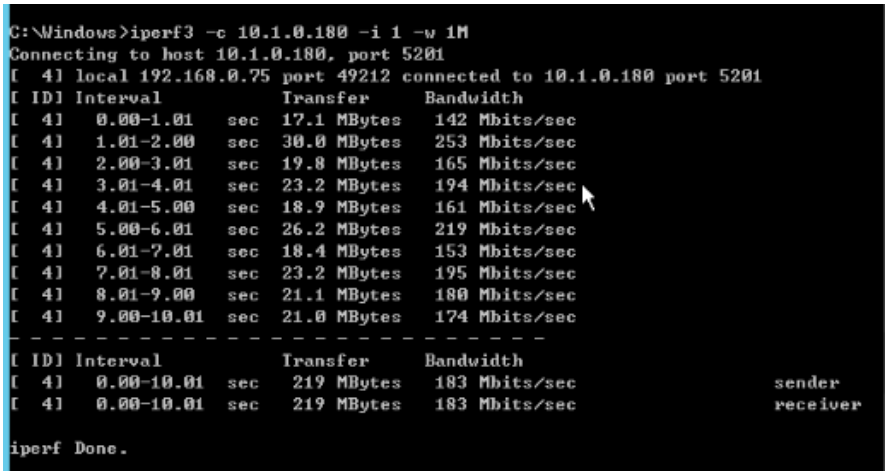
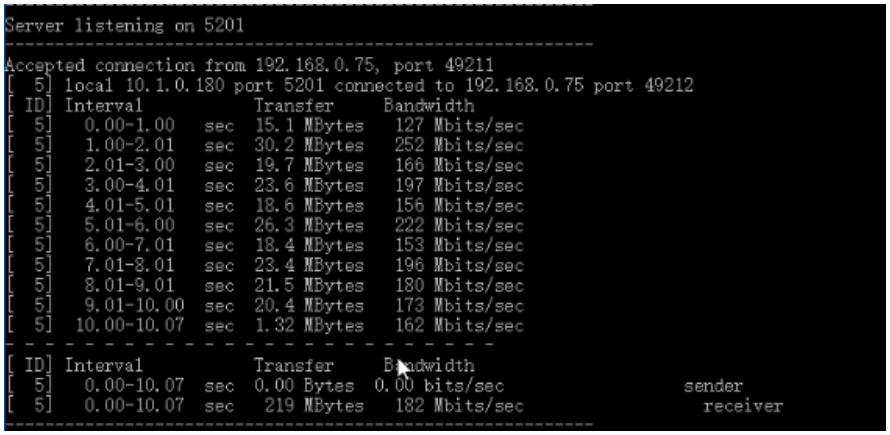



   **Figura 1-6** mostra o resultado do teste da largura de banda de 200 Mbit/s no servidor iPerf3.

**Figura 1-6** Resultado do teste para largura de banda de 200 Mbit/s (servidor de iPerf3)

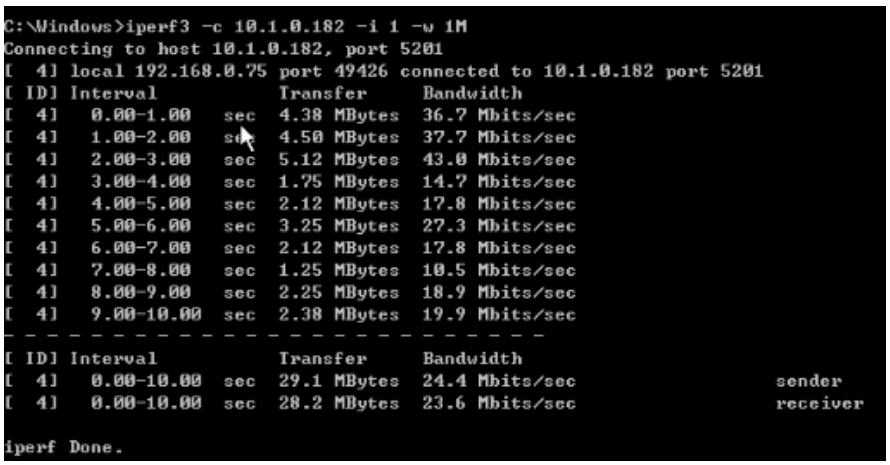



2. Quando os ECSs nas duas extremidades da conexão de VPN executam o CentOS 7, o iPerf3 é usado para testar a velocidade da rede. O resultado do teste é de 180 Mbit/s, atendendo aos requisitos.
3. Quando o ECS funciona como um servidor executa o CentOS 7 e o ECS funciona como um cliente que executa Windows, iPerf3 e FileZilla são usados para testar a velocidade da rede. O resultado do teste é de 20 Mbit/s, não atendendo aos requisitos.

   Isso ocorre porque as implementações de TCP no Windows e no Linux são diferentes.

   **Figura 1-7** mostra o resultado do uso do iPerf3 para testar a velocidade da rede entre dois ECSs que executam sistemas operacionais diferentes.

**Figura 1-7** Resultado do teste no iPerf3




**Quando a largura de banda de um gateway de VPN adquirido é de 1000 Mbit/s:**

NOTA

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.

A largura de banda do gateway de VPN é compartilhada por todas as suas conexões de VPN. Para usar totalmente a grande largura de banda de 1.000 Mbit/s, implemente vários ECSs com altas especificações, pois o desempenho de encaminhamento de um único ECS é limitado. Os ECSs com suas NICs que suportam a largura de banda de 2 Gbit/s ou superior são recomendados.

**Conclusões: com base nos resultados dos testes anteriores, as larguras de banda dos gateways de VPN da Huawei Cloud atendem aos requisitos. Para usar totalmente a largura de banda adquirida, recomenda-se que você use servidores executando o mesmo sistema operacional e usando NICs que atendam a determinados requisitos nas duas extremidades de uma conexão de VPN.**

# 1.16 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

# 1.17 Como alterar o modo de cobrança de um gateway da VPN de pagamento por uso para anual/mensal?

## Pré-requisitos

- O gateway de VPN de pagamento por uso é cobrado por largura de banda.
- Para alterar o modo de cobrança de um gateway de VPN cobrado por tráfego de pagamento por uso para anual/mensal, primeiro mude o gateway de VPN de ser cobrado por tráfego para ser cobrado por largura de banda e, em seguida, de pagamento por uso para anual/mensal.

## Procedimento

Realize as operações a seguir:

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** > **Enterprise – VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino, escolha **More** > **Change Billing Mode** na coluna **Operation**.
6. Na caixa de diálogo **Change Billing Mode**, clique em **OK**.

   NOTA

   O modo de cobrança de um gateway de VPN não pode ser alterado de anual/mensal para pago por uso e a largura de banda do gateway de VPN incluída na assinatura anual/mensal não pode ser diminuída.
7. Confirme as informações do gateway de VPN, configure a duração da renovação e clique em **Pay**.
8. Na página de pagamento, confirme as informações do pedido, selecione cupom ou desconto, selecione o método de pagamento e clique em **Pay**.

NOTA

Alterar o modo de cobrança de um gateway VPN de pagamento por uso para anual/mensal não afetará seus serviços.

# 1.18 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter vários gateways de VPN e um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

  NOTA

  O número de conexões de VPN é irrelevante para o número de sub-redes locais ou para o número de sub-redes de clientes. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

# 1.19 O que são um gateway de cliente e uma sub-rede de cliente em uma conexão de VPN?

Uma conexão de VPN é criada na Huawei Cloud. Como tal, uma sub-rede de uma VPC da Huawei Cloud é uma sub-rede local e um gateway de VPN criado na Huawei Cloud é um gateway local. A sub-rede e o gateway em um data center local conectado à VPC são uma sub-rede do cliente e um gateway do cliente, respectivamente.

Um endereço IP de gateway de cliente é um endereço IP público.

# 1.20 Quantas conexões de VPN são necessárias para conectar vários servidores locais à nuvem?

A VPN da Huawei Cloud usa a tecnologia VPN IPsec. Ela conecta uma VPC na nuvem e seu data center local. Portanto, o número de conexões de VPN é irrelevante para o número de servidores a serem conectados à nuvem, mas para o número de data centers onde os servidores estão localizados.

Dois EIPs podem ser vinculados a um gateway de VPN para comunicação com um gateway de cliente.

- Se um data center local tiver apenas um gateway de saída, todos os servidores ou hosts no data center se conectarão à Internet por meio desse gateway. Neste caso, você precisa configurar um grupo de conexão de VPN que consiste em duas conexões de VPN. Ou seja, configure uma conexão de VPN para cada um dos dois EIPs do gateway de VPN para se comunicar com o gateway de saída no data center local.

- Se um data center local tiver dois gateways de saída, os servidores ou hosts de usuário no data center se conectarão à Internet por meio dos gateways de saída de reboque. Nesse caso, você precisa configurar dois grupos de conexão de VPN, cada um consistindo de duas conexões de VPN. Ou seja, configure uma conexão de VPN para cada um dos dois EIPs de cada gateway de VPN para se comunicar com os dois gateways de saída no data center local.

# 1.21 Uma VPN permite comunicações entre as duas VPC?

- Se as duas VPCs estiverem na mesma região, use uma conexão de emparelhamento de VPC para conectá-las.
- Se as duas VPCs estiverem em regiões diferentes, use uma VPN para conectá-las. As operações são as seguintes:
  a. Crie um gateway de VPN para cada VPC e crie uma conexão de VPN para os dois gateways de VPN.
  b. Para a conexão de VPN, defina o gateway do cliente para o EIP do gateway de VPN de par.
  c. Para a conexão de VPN, defina a sub-rede do cliente como a sub-rede da VPC de mesmo nível.
  d. Defina as mesmas chaves pré-compartilhadas (PSKs) e algoritmos para as duas VPCs.

# 1.22 Quais são os impactos de uma VPN em uma rede local? Quais são as mudanças na rota para acessar um ECS?

Ao configurar uma VPN, você precisa executar as seguintes operações no gateway em seu data center local:

- Configure políticas de IKE e IPsec.
- Defina o modo de conexão para baseado em rota ou baseado em política.
- Verifique a configuração da rota no gateway para garantir que o tráfego destinado a uma VPC da Huawei Cloud possa ser roteado para a interface de saída correta (interface que tem uma política de IPsec vinculada).

# 1.23 Posso conectar uma rede com duas saídas a uma VPC por meio de duas conexões de VPN?

Sim.

# 1.24 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- As ACLs em ambas as extremidades da conexão de VPN não correspondem.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são diferentes.
- A Detecção de par inativo (DPD) não está configurada no dispositivo em seu data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- Nas duas extremidades da conexão de VPN, as configurações de sub-rede local e remota são invertidas.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- A DPD está ativada no dispositivo de gateway local e o número de vezes de detecção é 3 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do dispositivo de gateway local é grande o suficiente para a conexão de VPN.
- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.

# 1.25 O que fazer se uma conexão de VPN falha ao ser estabelecida?

1. Faça logon no console de gerenciamento e escolha **Virtual Private Network** > **Enterprise - VPN Connections**.
2. Na lista de conexões de VPN, localize a conexão VPN de destino e escolha **More** > **Modify Policy Settings** à direita para exibir as políticas de IKE e IPsec da conexão de VPN.
3. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.

   Se a AS de IKE tiver sido configurada na fase 1, mas nenhuma AS de IPsec tiver sido estabelecida na fase 2, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.
4. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
```

5. Faça ping nas duas extremidades da conexão de VPN uma da outra para verificar se a conexão de VPN está normal.

# 1.26 EIPs podem ser usados como endereços IP de gateway de VPN?

Não.

Quando você cria um gateway de VPN, seu endereço IP é atribuído automaticamente. Esse endereço IP tem configurações predefinidas e pode ser usado para interconexão com uma VPC. No entanto, um EIP não pode ser usado para interconexão com uma VPC.

# 1.27 Por que uma conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

A configuração pode estar incorreta.

1. Nas duas extremidades (nuvem e centro de dados no local) da conexão de VPN, certifique-se de que as chaves pré-compartilhadas (PSKs) e as informações de negociação sejam consistentes, as sub-redes locais e remotas sejam revertidas, e os gateways locais e remotos também são invertidos.
2. Certifique-se de que as rotas, a NAT e as políticas de segurança estejam configurados corretamente no dispositivo do data center local.

# 1.28 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa configurar regras de política (regras de ACL) para uma conexão de VPN no console de gerenciamento da Huawei Cloud somente quando **VPN Type** estiver definido como **Policy-based**.

# 2 Consultoria geral

## 2.1 Quais são os cenários típicos da VPN IPsec?

Uma VPN é uma conexão ponto a ponto que implementa o acesso à rede privada entre dois pontos.

- Cenários aplicáveis:
  - Uma VPN é criada entre diferentes regiões da Huawei Cloud para permitir comunicações de VPC entre regiões.
  - Uma VPN é criada entre VPCs da Huawei Cloud e outra nuvem pública, por exemplo, a Alibaba Cloud.
  - Uma VPN é criada entre uma VPC da Huawei Cloud e seu data center local.
  - Um hub de VPN é usado em conjunto com conexões de emparelhamento VPC e conexões Cloud Connect para permitir a comunicação entre um data center local e várias VPCs na nuvem.
  - Uma VPN é usada em conjunto com a NAT de origem para permitir o acesso a endereços IP específicos em nuvens.
- Cenários não aplicáveis:
  - Uma VPN não pode ser usada para conectar VPCs na mesma região da Huawei Cloud. É recomendável usar conexões de emparelhamento de VPC para permitir comunicações entre VPCs na mesma região.
  - Uma VPN não pode ser usada entre a Huawei Cloud e sua rede doméstica que usa discagem PPPoE.
  - Uma VPN não pode ser usada entre a Huawei Cloud e roteadores 4G/5G.
  - Uma VPN não pode ser usada entre a Huawei Cloud e seus terminais pessoais.

## 2.2 O que é uma VPC, um gateway de VPN e uma conexão de VPN?

As VPCs permitem você criar redes virtuais isoladas e privadas. Você pode usar a VPN para acessar ECSs com segurança em VPCs.

Um gateway de VPN é um gateway de saída para uma VPC. Com um gateway de VPN, você pode criar uma conexão segura, confiável e criptografada entre uma VPC e um data center local ou entre duas VPCs em diferentes regiões.

Uma conexão de VPN é um túnel de comunicação criptografado IPsec seguro e confiável estabelecido entre um gateway de VPN e o gateway do cliente em um data center local.

Para criar uma VPN na nuvem, execute as seguintes operações:

1. Crie um gateway de VPN Você precisa especificar a VPC a ser conectada, bem como a largura de banda e os EIPs do gateway de VPN.
2. Crie uma conexão de VPN Você precisa especificar o EIP do gateway usado para se conectar ao gateway do cliente, às sub-redes e às políticas de negociação.

# 2.3 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter vários gateways de VPN e um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

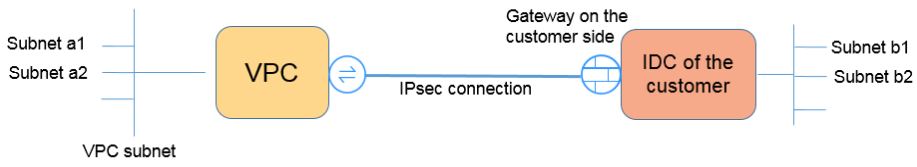
  NOTA

  O número de conexões de VPN é irrelevante para o número de sub-redes locais ou para o número de sub-redes de clientes. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

# 2.4 O que é uma conexão de VPN? Como definir o número de conexões de VPN ao comprar um gateway de VPN?

Uma conexão de VPN da Huawei Cloud é uma conexão IPsec estabelecida entre um gateway de VPN na nuvem e um endereço IP público independente de um data center local. Você pode configurar várias sub-redes locais (sub-redes da VPC) e sub-redes de clientes (sub-redes locais) para uma conexão de VPN.

O número de conexões de VPN a serem criadas é determinado pelo número de data centers locais. Cada conexão de VPN pode conectar uma VPC a apenas um data center local.



NOTA

Na figura anterior, se as sub-redes a1 e a2 na Huawei Cloud precisarem se comunicar com as sub-redes b1 e b2 na rede local, você precisará criar apenas uma conexão de VPN, com os blocos CIDR de origem definidos como a1 e a2 e os blocos CIDR de destino definidos como b1 e b2.

# 2.5 O que são um gateway de cliente e uma sub-rede de cliente em uma conexão de VPN?

Uma conexão de VPN é criada na Huawei Cloud. Como tal, uma sub-rede de uma VPC da Huawei Cloud é uma sub-rede local e um gateway de VPN criado na Huawei Cloud é um gateway local. A sub-rede e o gateway em um data center local conectado à VPC são uma sub-rede do cliente e um gateway do cliente, respectivamente.

Um endereço IP de gateway de cliente é um endereço IP público.

# 2.6 Como planejar blocos CIDR para acesso a uma VPC por meio de uma conexão de VPN?

- Os blocos CIDR de uma VPC não podem entrar em conflito com os blocos CIDR locais.
- Para evitar conflitos com endereços de serviço de nuvem, não use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3 ou 100.64.0.0/10 para sua rede local.

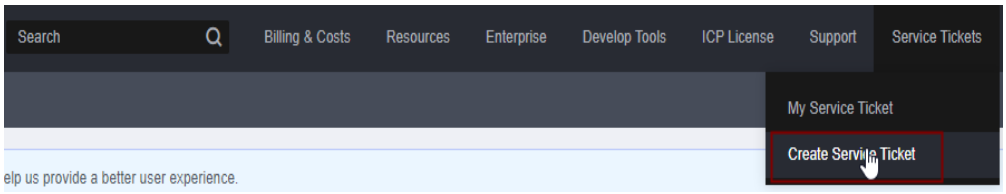
# 2.7 Uma conexão de VPN IPsec é estabelecida automaticamente?

Sim. Uma conexão de VPN IPsec é estabelecida automaticamente.

# 2.8 Quais são os tipos de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

1. Faça logon no console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

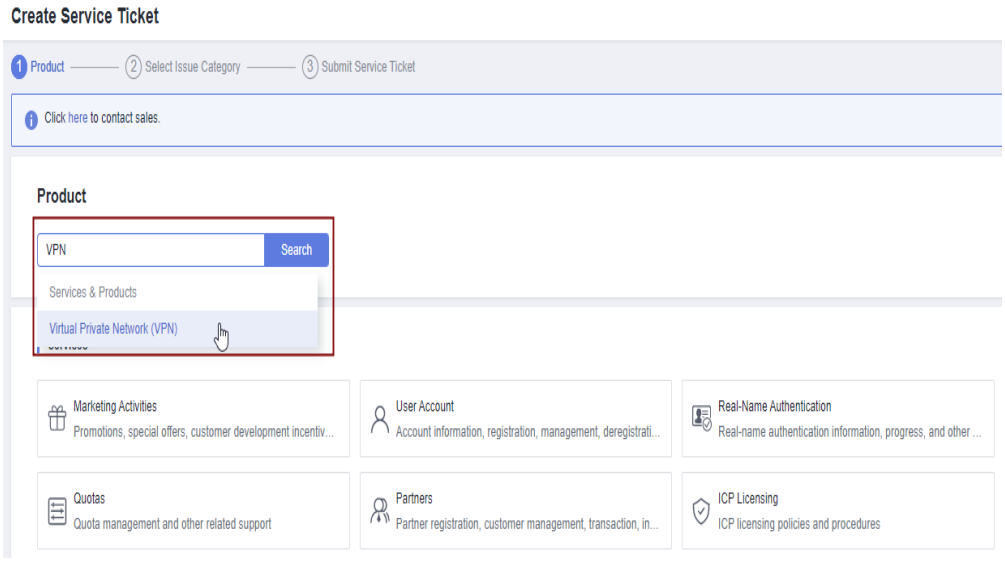
   **Figura 2-1** Criar tíquete de serviço

3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 2-2** Selecionar **Virtual Private Network (VPN)**



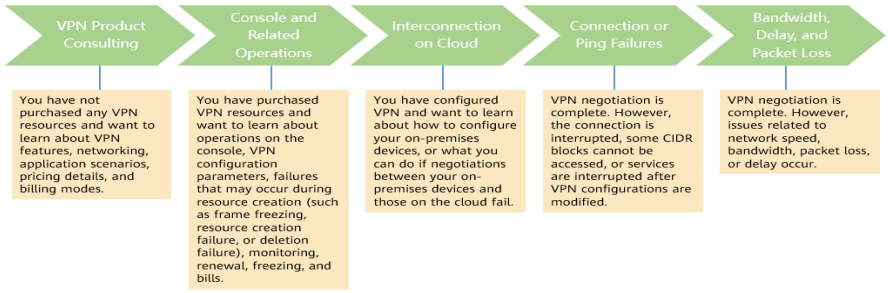

4. Selecione uma categoria de problema.

**Figura 2-3** Selecionar categoria de problema


NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 2-4** Categoria de emissão e base de classificação



# 2.9 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud é compatível com o protocolo IPsec (Internet Protocol Security) padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implementado atrás de um gateway de NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores de banda larga domésticos comuns, hosts de Windows que fornecem serviços de VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os seguintes produtos podem se conectar à Huawei Cloud por meio de VPNs:
  - Dispositivos: firewalls e roteadores de acesso (ARs) da Huawei, firewalls de Hillstone e firewalls de Check Point
  - Serviços em nuvem: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) e Microsoft Azure
  - Software: StrongSwan
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud através de uma VPN.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- Alguns dispositivos suportam VPN IPsec somente após a compra das licenças de software necessárias.

  O administrador do centro de dados no local pode verificar com o fornecedor do dispositivo se é necessária uma licença com base no modelo do dispositivo.

# 2.10 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 2-1** Parâmetros de negociação de VPN

| Protocolo | Parâmetro | Valor |
|---|---|---|
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● AES-256-GCM-16 |
| | DH Algorithm | ● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21 |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Tempo de vida (s) | **86400** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Local ID | ● Endereço IP<br>O endereço IP local é exibido automaticamente como o EIP do gateway de VPN, eliminando a necessidade de configurá-lo manualmente.<br>● FQDN<br>Por padrão, o tipo de ID local é o endereço IP e o valor de ID local é o EIP do gateway de VPN. |
| | Customer ID | ● Endereço IP<br>● FQDN<br>Por padrão, o tipo de ID do cliente é o endereço IP e o valor de ID do cliente é o endereço IP público do gateway do cliente. |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256-GCM-16 |
| | PFS | ● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor predefinido)<br>● DH grupo 15<br>● DH grupo 16<br>● DH grupo 19<br>● DH grupo 20<br>● DH grupo 21<br>● Disable |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Transfer Protocol | ● ESP (valor padrão) |
| | Lifetime (s) | **3600** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **30** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Quando o PFS estiver habilitado, uma troca de DH adicional será executada durante a negociação da AS do IPsec para gerar uma nova chave da AS do IPsec, melhorando a segurança da AS do IPsec.
- Por motivos de segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no dispositivo de gateway no data center local e que as configurações do PFS em ambas as extremidades sejam as mesmas. Caso contrário, a negociação falhará.
- O tempo de vida padrão baseado em tráfego de uma AS de IPsec é de 1.843.200 KB e não pode ser alterado para a VPN da Huawei Cloud. Este parâmetro não está envolvido na negociação e não tem impacto no estabelecimento de uma AS de IPsec.

# 2.11 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A PSK é configurada em um gateway de VPN e uma conexão será estabelecida após a conclusão da negociação de VPN. Portanto, nenhum nome de usuário ou senha é necessário para criar uma conexão de VPN IPsec. Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

O IPsec XAUTH fornece autenticação estendida para VPN IPsec. Ele requer que os usuários insiram seus nomes de usuário e senhas durante a negociação da VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

# 2.12 Como permitir que hosts específicos acessem uma sub-rede da VPC por meio de uma conexão de VPN criada?

Restrições no data center local:

- Políticas de controle de acesso no dispositivo de VPN
- Regras de ACL no roteador ou comutador

Restrições no lado da nuvem:

- Regras de grupo de segurança que permitem o acesso apenas a partir de endereços IP especificados
- Regras de ACL

NOTA

Recomenda-se que você não altere a sub-rede local ou do cliente para controlar o acesso.

# 2.13 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As seguintes informações de largura de banda de um endereço IP de gateway de VPN podem ser monitoradas: tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as informações de monitoramento, clique em na coluna **Gateway IP Address** na lista de gateways de VPN.

**Conexão de VPN**

As seguintes informações sobre uma conexão de VPN podem ser monitoradas: status da conexão de VPN, tempo médio de ida e volta (RTT) do link, RTT máximo do link, taxa de perda de pacotes do link, RTT médio do túnel, RTT máximo do túnel e taxa de perda de pacotes do túnel.

Para monitorar o RTT médio do link, o RTT máximo do link, a taxa de perda de pacotes do link, o RTT médio do túnel, o RTT máximo do túnel e a taxa de perda de pacotes do túnel, clique no nome da conexão VPN e em **Add** na área **Health Check** da página da guia **Summary** para adicionar itens de verificação de integridade.

Para exibir o status de uma conexão de VPN, clique em na coluna **Monitoring** da conexão de VPN.

# 2.14 EIPs podem ser usados como endereços IP de gateway de VPN?

Não.

Quando você cria um gateway de VPN, seu endereço IP é atribuído automaticamente. Esse endereço IP tem configurações predefinidas e pode ser usado para interconexão com uma VPC. No entanto, um EIP não pode ser usado para interconexão com uma VPC.

# 2.15 Preciso comprar EIPs para que os hosts se comuniquem entre si por meio de uma VPN?

Se os hosts locais precisarem acessar um ECS na nuvem por meio de uma VPN, você não precisará comprar EIPs para o ECS.

Se um ECS precisar fornecer serviços acessíveis pela Internet, será necessário adquirir um EIP para o ECS.

# 2.16 As VPNs SSL são suportadas?

VPNs SSL não são suportadas.

# 2.17 Quanto tempo demora para que as configurações de VPN entregues entrem em vigor?

Demora de 1 a 5 minutos para que as configurações de VPN entrem em vigor.

NOTA

Depois que as configurações de VPN entrarem em vigor, configure seu dispositivo de gateway na rede local para concluir a negociação do túnel com o gateway de VPN na Huawei Cloud.

# 2.18 A VPN da Huawei Cloud oferece suporte a endereços IPv6?

Não.

A VPN da Huawei Cloud oferece suporte apenas a endereços IPv4.

# 2.19 Como determinar minha largura de banda da VPN?

Considere o seguinte ao determinar a largura de banda:

- Quantidade de dados transmitidos por um túnel de VPN em um período de tempo (Reserve largura de banda suficiente para evitar o congestionamento do link.)
- Larguras de banda de saída nas duas extremidades de uma conexão de VPN: a largura de banda de saída no lado da nuvem deve ser menor do que no lado local.

# 2.20 Uma conexão de VPN suporta algoritmos criptográficos da série SM?

Não.

Use os algoritmos fornecidos no console de gerenciamento da Huawei Cloud para negociação de VPN. Além disso, certifique-se de que as duas extremidades de uma conexão de VPN usem os mesmos algoritmos.

# 2.21 Qual versão do IKE devo selecionar ao criar uma conexão de VPN?

A Huawei Cloud recomenda o IKEv2 porque o IKEv1 não é seguro. Além disso, o IKEv2 supera o IKEv1 na negociação e estabelecimento de conexão, métodos de autenticação, processamento de tempo limite de detecção de par inativo (DPD) e processamento de tempo limite de associação de segurança (AS).

A Huawei Cloud não suportará o IKEv1 em breve.

## Introdução ao IKEv1 e IKEv2

- Como um protocolo híbrido, o IKEv1 traz alguns defeitos de segurança e desempenho devido à sua complexidade. Como tal, tornou-se um gargalo no sistema de IPsec.
- IKEv2 aborda os problemas de IKEv1 mantendo funções básicas de IKEv1. O IKEv2 é mais simplificado, eficiente, seguro e robusto que o IKEv1. Além disso, o IKEv2 é definido pelo RFC 4306 em um único documento, enquanto o IKEv1 é definido em vários documentos. Ao minimizar as funções principais e os algoritmos de senha padrão, o IKEv2 melhora significativamente a interoperabilidade entre diferentes VPNs IPsec.

## Riscos de segurança do IKEv1

- Os algoritmos criptográficos suportados pelo IKEv1 não foram atualizados por mais de 10 anos. Além disso, o IKEv1 não oferece suporte a algoritmos criptográficos fortes, como AES-GCM e ChaCha20-Poly1305. Para IKEv1, o bit E (criptografia) no cabeçalho ISALMP especifica que as cargas úteis seguintes ao cabeçalho ISALMP são criptografadas, mas qualquer verificação de integridade de dados dessas cargas úteis é tratada por uma carga útil hash separada. Essa separação entre criptografia e proteção de integridade de dados impede o uso de criptografia autenticada (AES-GCM) com o IKEv1.
- O IKEv1 é vulnerável a ataques de amplificação de DoS e ataques de conexão semiaberta. Depois de responder a pacotes falsificados, o respondedor mantém relações iniciador-responder, consumindo um grande número de recursos do sistema.

  Este defeito é inerente ao IKEv1 e é abordado no IKEv2.
- O modo agressivo do IKEv1 não é seguro. Nesse modo, os pacotes de informações não são criptografados, apresentando riscos de vazamento de informações. Há também ataques de força bruta visando o modo agressivo, como ataques man-in-the-middle.

## Diferenças entre IKEv1 e IKEv2

- **Processo de negociação**
  - O IKEv1 é complexo e consome uma grande quantidade de largura de banda. Negociação de AS de IKEv1 consiste em duas fases. No IKEv1 fase 1, uma AS de IKE é estabelecida em modo principal ou modo agressivo. O modo principal requer três trocas entre pares, totalizando seis mensagens ISAKMP, enquanto o modo agressivo requer duas trocas, totalizando três mensagens ISAKMP. O modo agressivo é mais rápido, mas não fornece proteção de identidade para pares, pois a troca de chaves e a autenticação de identidade são realizadas simultaneamente. Na fase 2 do IKEv1, as ASs de IPsec são estabelecidas por meio de três mensagens ISAKMP no modo rápido.
  - Comparado com o IKEv1, o IKEv2 simplifica o processo de negociação de AS. O IKEv2 requer apenas duas trocas, totalizando quatro mensagens, para estabelecer uma AS de IKE e um par de ASs de IPsec. Para criar vários pares de ASs de IPsec, apenas uma troca adicional é necessária para cada par adicional de ASs.

    NOTA

    Para negociação de IKEv1, o seu modo principal envolve nove (6+3) mensagens, e seu modo agressivo envolve seis (3+3) mensagens. Em contraste, a negociação de IKEv2 requer apenas quatro (2+2) mensagens.

- **Métodos de autenticação**
  - Somente o IKEv1 (que exige um cartão de criptografia) suporta autenticação de envelope digital (HSS-DE).
  - O IKEv2 oferece suporte à autenticação EAP (Extensible Authentication Protocol). O IKEv2 pode usar um servidor AAA para autenticar remotamente usuários de dispositivos móveis e de PC e atribuir endereços IP privados a esses usuários. O IKEv1 não fornece essa função e deve usar o L2TP para atribuir endereços IP privados.
  - Apenas o IKEv2 suporta algoritmos de integridade de AS de IKE.
- **Processamento de tempo limite da DPD**
  - Somente o IKEv1 suporta o parâmetro **retry-interval**. Se um dispositivo envia um pacote de DPD, mas não recebe nenhuma resposta dentro do intervalo de repetição especificado, o dispositivo grava um evento de falha de DPD. Quando o número de eventos de falha de DPD atinge 5, ambas ASs de IKE e IPsec são excluídas. A negociação da AS de IKE será iniciada novamente somente quando houver tráfego a ser transmitido pelo túnel de IPsec.
  - No IKEv2, o intervalo de retransmissão aumenta de 1, 2, 4, 8, 16, 32 para 64, em segundos. Se nenhuma resposta for recebida dentro de oito transmissões consecutivas, a extremidade do par será considerada inativa e as ASs de IKE e IPsec serão excluídas.
- **Processamento de tempo limite da AS de IKE e processamento de tempo limite da AS de IPsec**

  No IKEv2, a vida útil suave da AS de IKE é 9/10 da vida útil dura da AS de IKE mais ou menos um número aleatório. Isso reduz a probabilidade de que duas extremidades iniciem a renegociação simultaneamente. Portanto, você não definir manualmente a vida útil suave em IKEv2.

### Vantagens do IKEv2 em relação ao IKEv1

- Simplifica o processo de negociação de AS, melhorando a eficiência.
- Corrige muitas vulnerabilidades de segurança criptográfica, melhorando a segurança.
- Suporta autenticação EAP, melhorando a flexibilidade e escalabilidade da autenticação.

  O EAP é um protocolo de autenticação que suporta vários métodos de autenticação. A maior vantagem do EAP é a sua escalabilidade. Ou seja, novos métodos de autenticação podem ser adicionados sem alterar o sistema de autenticação original. A autenticação EAP tem sido amplamente utilizada em redes de acesso de discagem.
- Emprega uma carga útil criptografada com base no ESP. Essa carga útil contém um algoritmo de criptografia e um algoritmo de integridade de dados. O AES-GCM garante confidencialidade, integridade e autenticação e funciona bem com o IKEv2.

## 2.22 Quantos bits têm os grupos DH usados pela VPN da Huawei Cloud?

Os grupos Diffie-Hellman (DH) determinam a força da chave usada no processo de troca de chaves. Números de grupo DH mais altos são geralmente mais seguros, mas é necessário mais tempo para calcular a chave.

**Tabela 2-2** lista o número de bits correspondentes aos grupos DH usados pela VPN.

**Tabela 2-2** Número de bits correspondentes a cada grupo DH

| Grupo DH | Módulo |
| --- | --- |
| 1 | 768 bits |
| 2 | 1024 bits |
| 5 | 1536 bits |
| 14 | 2048 bits |
| 15 | 3072 bits |
| 16 | 4096 bits |
| 19 | 256 bits (ECP) |
| 20 | 384 bits (ECP) |
| 21 | 521 bits (ECP) |

NOTA

Os seguintes algoritmos de DH têm riscos de segurança e não são recomendados: DH group 1, DH group 2 e DH group 5.

# 2.23 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

# 2.24 Posso implementar uma aplicação na nuvem, bancos de dados em um data center local e depois conectá-la por meio de uma VPN?

Sim.

Uma VPN conecta uma VPC e um data center local.

Depois que uma VPN é configurada, o tráfego de serviço pode ser transmitido entre a VPC e o data center local. Para um servidor de aplicações na nuvem, o acesso a um banco de dados local é logicamente o mesmo que o acesso a outros hosts na mesma LAN. Diante disso, é possível usar uma VPN para conectar uma aplicação na nuvem a um banco de dados em um data center local.

Este é um cenário típico de VPN IPsec.

Além disso, não há limitações no iniciador do serviço. Ou seja, as solicitações de serviço podem ser iniciadas a partir da nuvem ou do data center local.

**AVISO**

- Depois que uma VPN estiver configurada, verifique a latência da rede e a taxa de perda de pacotes para garantir o bom funcionamento do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

# 2.25 Quais são as diferenças entre VPN IPsec e VPN SSL em cenários de aplicações e modos de conexão?

## Cenários de aplicação

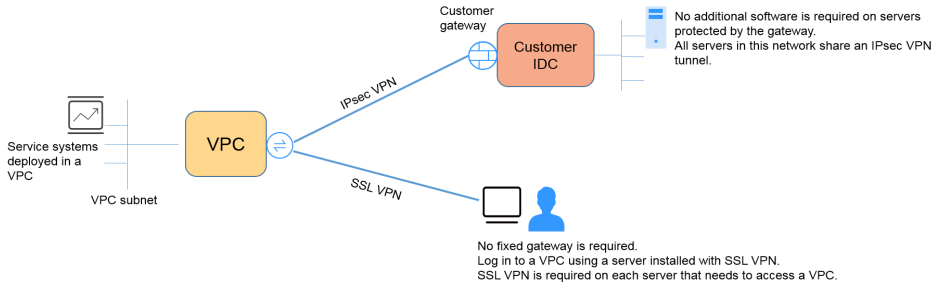
VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

## Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para permitir que eles concluam a negociação de VPN IPsec.

VPN SSL requer um programa cliente específico instalado em hosts. Os usuários precisam inserir nomes de usuário e senha para conectar os hosts aos servidores SSL.




**NOTA**

A Huawei Cloud suporta apenas VPN IPsec.

# 2.26 Como será cobrado pelo uso de uma VPN? Será cobrado pelos EIPs do gateway de VPN?

As VPNs são cobradas pelos seguintes itens em uma base anual/mensal ou pagamento por uso.

- Gateway de VPN

- Conexão de VPN

  Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Caso necessário você pode comprar conexões de VPN adicionais.

- Largura de banda EIP de um gateway de VPN

  A largura de banda do gateway de VPN pode ser faturada por tráfego ou largura de banda.

  a. Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.

  b. O ciclo de faturamento do modo de cobrança pagamento por uso é de 1 hora. Quando você cria um gateway de VPN pago por uso, o sistema solicita que você crie conexões de VPN. Por padrão, 10 grupos de conexões de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Se mais grupos de conexão forem necessários, você precisará comprá-los.

  NOTA

  Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

# 2.27 Quais são as diferenças entre a cobrança da largura de banda de EIP do gateway de VPN por largura de banda e por tráfego?

A largura de banda de EIP do gateway de VPN pode ser cobrada por largura de banda ou por tráfego.

As diferenças são as seguintes:

- Cobrança por largura de banda: o ciclo de cobrança é de 1 hora. A taxa gerada depende da largura de banda.
- Cobrança por tráfego: a taxa é calculada com base no tráfego de saída de uma VPC gerado a cada hora, o que não é afetado pela largura de banda.

# 2.28 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

# 2.29 O EIP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Se um EIP de pagamento por uso estiver vinculado a um gateway de VPN de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP vinculado.

Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway da VPN.

# 2.30 Onde adicionar rotas para sub-redes do cliente no console da VPN?

Quando uma conexão de VPN é criada, as rotas para as sub-redes do cliente são entregues automaticamente.

# 2.31 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 2.32 O que fazer se uma conexão de VPN falha ao ser estabelecida?

1. Faça logon no console de gerenciamento e escolha **Virtual Private Network** > **Enterprise - VPN Connections**.
2. Na lista de conexões de VPN, localize a conexão VPN de destino e escolha **More** > **Modify Policy Settings** à direita para exibir as políticas de IKE e IPsec da conexão de VPN.
3. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.

   Se a AS de IKE tiver sido configurada na fase 1, mas nenhuma AS de IPsec tiver sido estabelecida na fase 2, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.
4. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   ```
5. Faça ping nas duas extremidades da conexão de VPN uma da outra para verificar se a conexão de VPN está normal.

# 2.33 Em que direção a largura de banda da VPN é limitada? Qual é a unidade de largura de banda?

A largura de banda do gateway de VPN adquirida aplica-se à direção de saída da Huawei Cloud. Para obter um equilíbrio entre as larguras de banda nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada da seguinte forma:

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

# 2.34 Posso restaurar um gateway de VPN ou uma conexão de VPN que foi excluída incorretamente?

- Um gateway de VPN anual/mensal ou uma conexão de VPN não pode ser restaurada.
- Um gateway de VPN pago por uso pode ser restaurado somente quando as seguintes condições forem atendidas:
  - O gateway de VPN foi excluído em 24 horas.
  - Ambos os EIPs vinculados ao gateway de VPN não foram ilimitados.
  - O roteador de VPC ou empresarial interconectado com o gateway de VPN está disponível. Se a VPC ou roteador corporativo não existir, restaure a VPC ou o roteador empresarial primeiro.
  - Sua conta está normal e não está em atraso ou congelada.
- Uma conexão de VPN de um gateway de VPN pago por uso pode ser restaurada somente quando as seguintes condições forem atendidas:
  - O gateway de VPN e o gateway do cliente estão disponíveis. Se um deles não existir, restaure-o primeiro.
  - Sua conta está normal e não está em atraso ou congelada.

  A configuração de verificação de integridade de uma conexão de VPN paga por uso não pode ser restaurada mesmo após a conexão de VPN ser restaurada. Portanto, você precisa reconfigurar a função de verificação de integridade.

# 3 Rede e cenários de aplicação

## 3.1 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

## 3.2 Posso implementar uma aplicação na nuvem, bancos de dados em um data center local e depois conectá-la por meio de uma VPN?

Sim.

Uma VPN conecta uma VPC e um data center local.

Depois que uma VPN é configurada, o tráfego de serviço pode ser transmitido entre a VPC e o data center local. Para um servidor de aplicações na nuvem, o acesso a um banco de dados local é logicamente o mesmo que o acesso a outros hosts na mesma LAN. Diante disso, é possível usar uma VPN para conectar uma aplicação na nuvem a um banco de dados em um data center local.

Este é um cenário típico de VPN IPsec.

Além disso, não há limitações no iniciador do serviço. Ou seja, as solicitações de serviço podem ser iniciadas a partir da nuvem ou do data center local.

**AVISO**

- Depois que uma VPN estiver configurada, verifique a latência da rede e a taxa de perda de pacotes para garantir o bom funcionamento do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

# 3.3 Quantas conexões de VPN são necessárias para conectar vários servidores locais à nuvem?

A VPN da Huawei Cloud usa a tecnologia VPN IPsec. Ela conecta uma VPC na nuvem e seu data center local. Portanto, o número de conexões de VPN é irrelevante para o número de servidores a serem conectados à nuvem, mas para o número de data centers onde os servidores estão localizados.

Dois EIPs podem ser vinculados a um gateway de VPN para comunicação com um gateway de cliente.

- Se um data center local tiver apenas um gateway de saída, todos os servidores ou hosts no data center se conectarão à Internet por meio desse gateway. Neste caso, você precisa configurar um grupo de conexão de VPN que consiste em duas conexões de VPN. Ou seja, configure uma conexão de VPN para cada um dos dois EIPs do gateway de VPN para se comunicar com o gateway de saída no data center local.
- Se um data center local tiver dois gateways de saída, os servidores ou hosts de usuário no data center se conectarão à Internet por meio dos gateways de saída de reboque. Nesse caso, você precisa configurar dois grupos de conexão de VPN, cada um consistindo de duas conexões de VPN. Ou seja, configure uma conexão de VPN para cada um dos dois EIPs de cada gateway de VPN para se comunicar com os dois gateways de saída no data center local.

# 3.4 Quais são as diferenças entre VPN IPsec e VPN SSL em cenários de aplicações e modos de conexão?

## Cenários de aplicação

VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

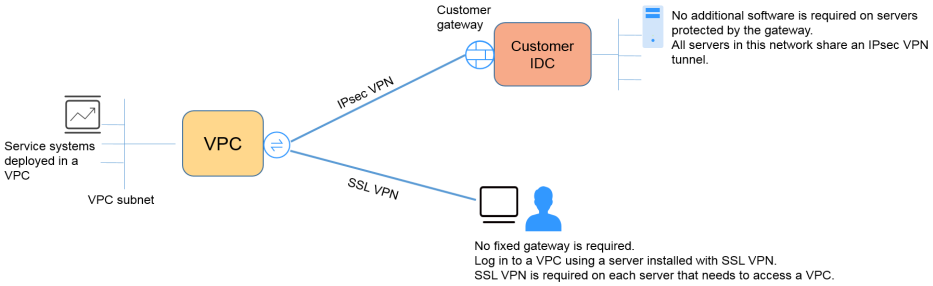
VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

## Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para permitir que eles concluam a negociação de VPN IPsec.

VPN SSL requer um programa cliente específico instalado em hosts. Os usuários precisam inserir nomes de usuário e senha para conectar os hosts aos servidores SSL.




**NOTA**

A Huawei Cloud suporta apenas VPN IPsec.

# 3.5 Uma VPN permite comunicações entre as duas VPC?

- Se as duas VPCs estiverem na mesma região, use uma conexão de emparelhamento de VPC para conectá-las.
- Se as duas VPCs estiverem em regiões diferentes, use uma VPN para conectá-las. As operações são as seguintes:
  a. Crie um gateway de VPN para cada VPC e crie uma conexão de VPN para os dois gateways de VPN.
  b. Para a conexão de VPN, defina o gateway do cliente para o EIP do gateway de VPN de par.
  c. Para a conexão de VPN, defina a sub-rede do cliente como a sub-rede da VPC de mesmo nível.
  d. Defina as mesmas chaves pré-compartilhadas (PSKs) e algoritmos para as duas VPCs.

# 3.6 Quais são os impactos de uma VPN em uma rede local? Quais são as mudanças na rota para acessar um ECS?

Ao configurar uma VPN, você precisa executar as seguintes operações no gateway em seu data center local:

- Configure políticas de IKE e IPsec.
- Defina o modo de conexão para baseado em rota ou baseado em política.
- Verifique a configuração da rota no gateway para garantir que o tráfego destinado a uma VPC da Huawei Cloud possa ser roteado para a interface de saída correta (interface que tem uma política de IPsec vinculada).

# 3.7 Quais configurações são necessárias em ambas as extremidades de uma VPN que conecta um data center local a uma VPC?

Para implementar a interconexão de VPN, crie uma VPN na nuvem e configure o dispositivo de VPN no data center local.

- Criar uma VPN na nuvem.
  - Compre um gateway de VPN e configure o modo de cobrança, a largura de banda e a VPC interconectada.
  - Crie um gateway de cliente e configure o modo de roteamento.
  - Compre uma conexão de VPN e configure os endereços IP de gateway e as sub-redes em ambas as extremidades, bem como as políticas de negociação.
- Configurar o dispositivo de VPN no data center local.
  a. Configure o endereço IP público usado pelo data center local para se conectar à nuvem e conclua as configurações da fase 1 e fase 2 de negociação de IPsec no dispositivo de VPN.
  b. Configure rotas, NAT e políticas de segurança no dispositivo de VPN.

# 3.8 Posso conectar uma rede com duas saídas a uma VPC por meio de duas conexões de VPN?

Sim.

# 3.9 Posso conectar duas VPCs na mesma região por meio de uma VPN?

Não.

Você pode usar uma conexão de emparelhamento de VPC ou uma conexão Cloud Connect para conectar duas VPCs na mesma região.

# 3.10 Como conectar duas VPCs na mesma região?

Você pode usar uma conexão de emparelhamento de VPC ou uma conexão Cloud Connect para conectar duas VPCs na mesma região. O emparelhamento de VPC só pode conectar VPCs na mesma região, e a Cloud Connect também pode conectar VPCs em diferentes regiões.

# 3.11 Como habilitar comunicações entre duas VPCs e uma rede local?

## Topologia de rede

IDC–VPC 1–VPC 2


IDC indica um centro de dados no local. Uma conexão de VPN é estabelecida entre a VPC 1 e o IDC.

## Procedimento

1. Verifique se as duas VPCs estão na mesma região.
   - Em caso afirmativo, use uma conexão de emparelhamento da VPC ou uma conexão Cloud Connect para conectar as duas VPCs. Tal conexão é gratuita.
   - Caso contrário, use uma conexão Cloud Connect para conectar as duas VPCs. Você precisa pagar pela largura de banda da Cloud Connect.
2. Estabeleça uma conexão de VPN entre o IDC e uma VPC (VPC 1 neste exemplo).

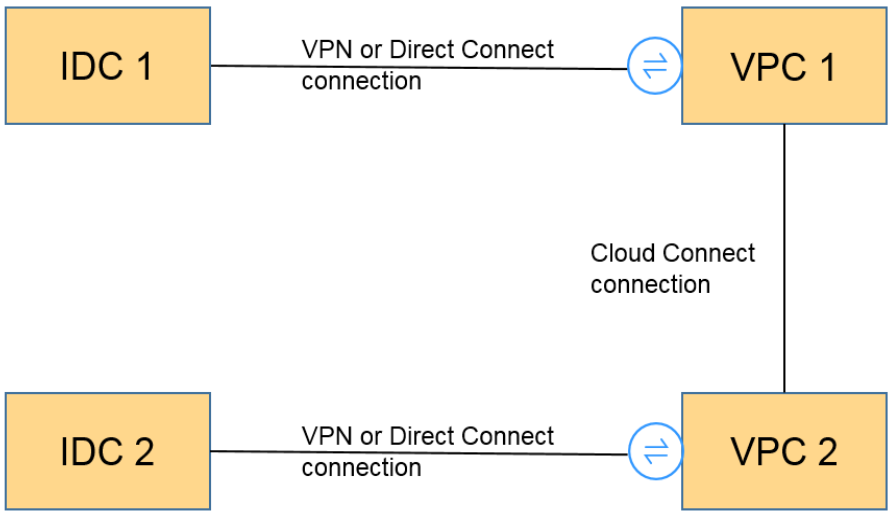
   No data center local, defina as sub-redes da VPC 1 e da VPC 2 como sub-redes remotas. A sub-rede local da VPC 1 deve conter a sub-rede conectada por meio de uma conexão de emparelhamento da VPC ou Cloud Connect. A rota de sub-rede da conexão de emparelhamento da VPC ou da conexão Cloud Connect precisa se destinar à sub-rede local.

# 3.12 Como conectar quatro sub-redes?

**Figura 3-1** mostra a topologia da rede.

**Figura 3-1** Topologia de rede




1. Use uma conexão de VPN ou conexão Direct Connect para conectar o IDC 1 à VPC 1.
2. Use uma conexão Cloud Connect para conectar a VPC 1 à VPC 2. (Também é possível usar uma conexão de emparelhamento da VPC para conectar a VPC 1 à VPC 2, se elas estiverem na mesma região.)
3. Use uma conexão de VPN ou conexão Direct Connect para conectar a VPC 2 à IDC 2.
4. Atualize as sub-redes de VPN, as rotas de sub-rede da Cloud Connect e as rotas de sub-rede da Direct Connect. Em seguida, as quatro sub-redes são alcançáveis para alcançar outras.

# 3.13 Preciso de duas conexões de VPN para conectar quatro sub-redes de duas regiões se cada região tiver duas sub-redes?

Não.

Apenas uma conexão de VPN é necessária entre duas regiões. Todas as sub-redes podem ser adicionadas à conexão de VPN.

Neste cenário, se tentar criar uma segunda conexão de VPN, o console de gerenciamento apresenta uma mensagem a indicar que ocorre um conflito porque as duas conexões têm o mesmo endereço de gateway de cliente.

# 3.14 Posso acessar o OBS através de uma VPN?

Sim.

1. Com a ajuda do serviço VPC Endpoint, você pode acessar o OBS por meio de uma VPN. Você precisa criar dois pontos de extremidade de VPC para o servidor DNS privado e o OBS da Huawei Cloud, respectivamente.
2. Configure o servidor DNS privado e as rotas no seu data center local.

# 3.15 Como conectar meu computador pessoal à nuvem por meio de uma VPN?

Roteadores de banda larga domésticos comuns, hosts de Windows que fornecem serviços de VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.

Para usar a VPN da Huawei Cloud, os dispositivos locais devem suportar o protocolo IPsec padrão.

# 3.16 Como acessar os ECSs da Huawei Cloud em casa quando minha rede corporativa foi conectada à Huawei Cloud por meio de uma VPN?

Uma VPN da Cloud Huawei é uma VPN IPsec que conecta uma LAN local a uma VPC na nuvem. Sua rede doméstica não faz parte da LAN corporativa, portanto, você não pode se conectar diretamente à VPC na nuvem em casa.

Se o host em casa precisar acessar recursos da VPC na nuvem, ele poderá acessar diretamente o EIP do serviço correspondente. Como alternativa, seu host pode se conectar à LAN de sua empresa por meio de VPN SSL (se houver suporte) e, em seguida, acessar os recursos da VPC na nuvem por meio da LAN.

# 3.17 Como estabelecer uma conexão de VPN temporariamente se nenhum dispositivo local compatível com IPsec estiver disponível após a compra de um gateway de VPN da Huawei Cloud e de uma conexão de VPN?

Para estabelecer uma conexão de VPN com a Huawei Cloud, você deve ter um dispositivo local que ofereça suporte ao protocolo IPsec padrão e tenha um endereço IP público fixo.

Se os requisitos anteriores não forem atendidos, você pode instalar software IPsec de terceiros em um host para se conectar temporariamente à Huawei Cloud.

Os softwares IPsec de terceiros recomendados incluem GreenBow, StrongSwan e Openswan. Para obter detalhes sobre a interconexão, consulte **Guia de administrador da Virtual Private Network**.

# 3.18 Como selecionar uma região adequada na nuvem quando comprar um gateway de VPN?

Você pode selecionar uma VPC em qualquer região ao comprar um gateway de VPN.

É recomendável selecionar a região mais próxima do data center local para minimizar o impacto da Internet na VPN.

- Para se conectar a várias VPCs na mesma região, você pode usar a VPN e a Direct Connect.
- Para se conectar a várias VPCs em diferentes regiões, você pode usar a VPN e a Cloud Connect.

# 4 Cobrança e pagamentos

## 4.1 Como será cobrado pelo uso de uma VPN? Será cobrado pelos EIPs do gateway de VPN?

As VPNs são cobradas pelos seguintes itens em uma base anual/mensal ou pagamento por uso.

- Gateway de VPN
- Conexão de VPN

  Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Caso necessário você pode comprar conexões de VPN adicionais.
- Largura de banda de EIP de um gateway de VPN

  A largura de banda do gateway de VPN pode ser faturada por tráfego ou largura de banda.

  a. Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.

  b. O ciclo de faturamento do modo de cobrança pagamento por uso é de 1 hora. Quando você cria um gateway de VPN pago por uso, o sistema solicita que você crie conexões de VPN. Por padrão, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN. Se mais grupos de conexão forem necessários, você precisará comprá-los.

  NOTA

  Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

## 4.2 Quais são as diferenças entre a cobrança da largura de banda de EIP do gateway de VPN por largura de banda e por tráfego?

A largura de banda de EIP do gateway de VPN pode ser cobrada por largura de banda ou por tráfego.

As diferenças são as seguintes:

- Cobrança por largura de banda: o ciclo de cobrança é de 1 hora. A taxa gerada depende da largura de banda.
- Cobrança por tráfego: a taxa é calculada com base no tráfego de saída de uma VPC gerado a cada hora, o que não é afetado pela largura de banda.

# 4.3 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

# 4.4 Por quantas conexões de VPN serão cobradas para conectar VPCs em diferentes regiões?

As VPNs podem ser usadas para conectar VPCs em diferentes regiões. A largura de banda e as conexões de VPN de cada região serão cobradas de forma independente. Portanto, ao calcular as taxas estimadas, você precisa verificar o número total de regiões e suas relações de conexão.

Por exemplo, suponha que a Região A precise estabelecer uma conexão de VPN com a Região B e a Região C, respectivamente. O gateway de VPN da Região A tem duas conexões; o gateway de VPN da Região B tem uma conexão; e o gateway de VPN da Região C tem uma conexão.

Nesse caso, você será cobrado por quatro conexões de VPN.

# 4.5 Como alterar o modo de cobrança de um gateway da VPN de pagamento por uso para anual/mensal?

## Pré-requisitos

- O gateway de VPN de pagamento por uso é cobrado por largura de banda.
- Para alterar o modo de cobrança de um gateway de VPN cobrado por tráfego de pagamento por uso para anual/mensal, primeiro mude o gateway de VPN de ser cobrado por tráfego para ser cobrado por largura de banda e, em seguida, de pagamento por uso para anual/mensal.

## Procedimento

Realize as operações a seguir:

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** > **Enterprise - VPN Gateways**.
5. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino, escolha **More** > **Change Billing Mode** na coluna **Operation**.
6. Na caixa de diálogo **Change Billing Mode**, clique em **OK**.

   NOTA

   O modo de cobrança de um gateway de VPN não pode ser alterado de anual/mensal para pago por uso e a largura de banda do gateway de VPN incluída na assinatura anual/mensal não pode ser diminuída.
7. Confirme as informações do gateway de VPN, configure a duração da renovação e clique em **Pay**.
8. Na página de pagamento, confirme as informações do pedido, selecione cupom ou desconto, selecione o método de pagamento e clique em **Pay**.

   NOTA

   Alterar o modo de cobrança de um gateway de VPN de pagamento por uso para anual/mensal não afetará seus serviços.

# 4.6 Um gateway de VPN anual/mensal será renovado automaticamente?

Sim.

A Huawei Cloud cobrará automaticamente as taxas de renovação do seu saldo.

Um gateway de VPN anual/mensal precisa ser pré-pago. Para garantir que sua conexão seja normal, recarregue sua conta se seu saldo não for suficiente.

# 4.7 Posso cancelar a assinatura de um gateway de VPN anual/mensal?

Sim.

Na página **VPN Gateways**, localize a linha que contém o gateway de VPN que deseja cancelar a assinatura e escolha **More** > **Delete** na coluna **Operation**. Depois de cancelar a assinatura de um gateway de VPN anual/mensal, todas as conexões de VPN criadas para o gateway também serão excluídas e não poderão ser recuperadas.

Após o cancelamento da assinatura, as taxas pré-pagas restantes serão reembolsadas.

# 4.8 Quando meus recursos de VPN serão congelados? Como descongelar os recursos da VPN?

- Se os recursos de VPN de pagamento por uso estiverem em atraso, os recursos entrarão no período de carência, durante o qual você ainda poderá acessar e usar os recursos. Se o período de carência terminar e você não tiver quitado os atrasos, os recursos entrarão no período de retenção, durante o qual os recursos serão congelados. Os recursos

congelados estão indisponíveis e não podem ser modificados ou liberados. Se o período de retenção terminar e você ainda não tiver recarregado sua conta e quitado os pagamentos em atraso, os recursos serão liberados e não poderão ser restaurados. Para garantir que os recursos estejam disponíveis, recarregue sua conta e pague os atrasos antes que os recursos expirem.

- Os recursos congelados da VPN ficarão disponíveis depois que você renová-los ou recarregar sua conta.

# 4.9 Como os recursos da VPN são cobrados e como uso cupons?

Um gateway de VPN pode ser cobrado em uma base de pagamento por uso ou anual/mensal.

- Pagamento por uso: as taxas são deduzidas do saldo da conta com base no uso de recursos.
- Anual/mensal: a assinatura deve ser paga antecipadamente.

Se você tiver um cupom da Huawei Cloud, poderá usá-lo para recarregar sua conta, desde que o cupom ainda seja válido. Em seguida, você pode usar o novo saldo em sua conta para pagar seus recursos.

Os recursos anuais/mensais são rentáveis.

Os usuários do contrato da Huawei Cloud precisam selecionar **Download Contract and Pay** e pagar no console.

# 5 Operações no console

## 5.1 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter vários gateways de VPN e um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

  NOTA

  O número de conexões de VPN é irrelevante para o número de sub-redes locais ou para o número de sub-redes de clientes. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

## 5.2 Quanto tempo demora para que as configurações de VPN entregues entrem em vigor?

Demora de 1 a 5 minutos para que as configurações de VPN entrem em vigor.

NOTA

Depois que as configurações de VPN entrarem em vigor, configure seu dispositivo de gateway na rede local para concluir a negociação do túnel com o gateway de VPN na Huawei Cloud.

# 5.3 Por que uma conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

A configuração pode estar incorreta.

1. Nas duas extremidades (nuvem e centro de dados no local) da conexão de VPN, certifique-se de que as chaves pré-compartilhadas (PSKs) e as informações de negociação sejam consistentes, as sub-redes locais e remotas sejam revertidas, e os gateways locais e remotos também são invertidos.
2. Certifique-se de que as rotas, a NAT e as políticas de segurança estejam configurados corretamente no dispositivo do data center local.

# 5.4 O EIP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Se um EIP de pagamento por uso estiver vinculado a um gateway de VPN de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP vinculado.

Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway da VPN.

# 5.5 Quais informações sobre uma VPN criada podem ser modificadas e quais informações não podem ser modificadas?

- Gateway de VPN
  - Você pode modificar as seguintes informações:
    - Nome
    - Sub-rede local
    - EIPs ativo e em espera
      - Para modificar o EIP ativo ou em espera, desvincule o EIP original e vincule um novo.

        Se uma conexão de VPN tiver sido criada para um EIP, o EIP não poderá ser desvinculado.
      - Para obter detalhes sobre como modificar atributos EIP, como nome, tipo e largura de banda, consulte a **documentação de serviço EIP**.
  - Não é possível modificar as seguintes informações:
    - Região
    - Modo de associação (VPC ou roteador empresarial)
    - Roteador empresarial

      O roteador empresarial associado precisa ser especificado somente quando **Associate With** estiver definido como **Enterprise Router**.
    - VPC

        - Sub-rede de interconexão
        - ASN de BGP
        - Modo de cobrança (anual/mensal ou pagamento por uso)
        - Especificação
        - AZ
        - Número de grupos de conexão de VPN

          O número de grupos de conexão de VPN precisa ser especificado somente quando o **Billing Mode** estiver definido como **Yearly/Monthly**.
- Gateway de cliente
  - Você pode modificar as seguintes informações:
    - Nome
  - Não é possível modificar as seguintes informações:
    - Modo de roteamento
    - ASN de BGP

      O ASN de BGP precisa de ser especificado somente quando **Routing Mode** é definido como **Dynamic (BGP)**.
    - Endereço IP público
- Conexão de VPN
  - Você pode modificar as seguintes informações:
    - Nome
    - Endereço da interface local
    - Gateway de cliente
    - Sub-rede de cliente
    - Configuração de políticas, incluindo políticas de IKE e IPsec
    - PSK
  - Não é possível modificar as seguintes informações:
    - Gateway de VPN
    - EIP
    - Tipo de VPN (baseado em rota ou baseado em política)
    - Modo de roteamento (estático ou BGP)

      O modo de roteamento precisa ser especificado somente quando **VPN Type** é definido como **Route-based**.
    - Configuração de detecção de link

      A configuração de detecção de link está disponível somente quando **VPN Type** é definido como **Route-based**.
    - Configuração da política, incluindo os blocos CIDR de origem e destino

      A configuração da política está disponível somente quando **VPN Type** é definido como **Route-based**.

# 5.6 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa configurar regras de política (regras de ACL) para uma conexão de VPN no console de gerenciamento da Huawei Cloud somente quando **VPN Type** estiver definido como **Policy-based**.

# 5.7 O que fazer se ocorrer uma exceção quando adicionar uma sub-rede do cliente durante a criação da conexão de VPN?

Verifique se essa sub-rede do cliente está envolvida em uma rota de uma conexão de emparelhamento de VPC, Cloud Connect ou Direct Connect. Em caso afirmativo, ocorre um conflito de rota e você precisa excluir a rota e criar uma nova para evitar o conflito.

# 5.8 Onde configurar rotas para sub-redes do cliente no console da VPN?

Quando uma conexão de VPN é criada, as rotas para as sub-redes do cliente são entregues automaticamente.

# 5.9 Posso chamar APIs para gerenciar os recursos da VPN da Huawei Cloud?

Sim.

# 5.10 O que são um gateway de cliente e uma sub-rede de cliente em uma conexão de VPN?

Uma conexão de VPN é criada no Huawei Cloud. Como tal, uma sub-rede de uma VPC da Huawei Cloud é uma sub-rede local e um gateway de VPN criado na Huawei Cloud é um gateway local. A sub-rede e o gateway em um data center local conectado à VPC são uma sub-rede do cliente e um gateway do cliente, respectivamente.

Um endereço IP de gateway de cliente é um endereço IP público.

# 5.11 Como desativar o PFS ao criar uma conexão de VPN?

- Huawei Cloud

  Na configuração da conexão de VPN, defina **PFS** na política de IPsec para **Disable**. Por padrão, o PFS está ativado na Huawei Cloud.

- Gateway do cliente em seu data center local

  Por padrão, o PFS é desativado em dispositivos de alguns fornecedores. Para obter detalhes sobre como desativar o PFS, consulte a documentação do produto correspondente.

NOTA

Certifique-se de que as configurações do PFS na Huawei Cloud e no gateway do cliente sejam consistentes. Caso contrário, a negociação falhará.

Para fins de segurança, recomendamos que você ative o PFS na Huawei Cloud e no gateway do cliente.

# 5.12 Quantas sub-redes locais e de clientes posso adicionar a uma VPN?

- Você pode configurar um máximo de 50 sub-redes locais para cada gateway de VPN.
- Você pode configurar um máximo de 50 sub-redes de clientes para cada conexão de VPN.

# 5.13 Quais são as precauções para configurar as sub-redes locais e de cliente para uma conexão de VPN?

- O número de sub-redes locais e o número de sub-redes de clientes são limitados. Se o número de sub-redes locais ou de clientes exceder o limite superior, agregue as sub-redes.
  - Número máximo de sub-redes locais para cada gateway de VPN: 50
  - Número máximo de sub-redes de clientes para cada conexão de VPN: 50
- A sub-rede local não pode incluir o bloco CIDR da sub-rede remota. A sub-rede remota pode incluir o bloco CIDR da sub-rede local.
- Há rotas que apontam para as sub-redes locais na VPC onde o gateway de VPN reside.
- Se houver duas conexões (conexão A e conexão B) criadas para um gateway de VPN, e a sub-rede remota da conexão A estiver dentro da conexão B, quando a rede de destino a ser acessada pertencer ao bloco CIDR sobreposto, a conexão criada primeiro será correspondida primeiro, independentemente do status da conexão. (A correspondência de comprimento da máscara não é usada para a VPN baseada em políticas.)

# 5.14 Por que uma conexão de VPN está no estado Not Connected no console de gerenciamento quando já está disponível?

Há um certo atraso na atualização do estado da conexão de VPN no console de gerenciamento.

Se o acesso ao serviço for normal, a conexão de VPN foi estabelecida. O estado da conexão de VPN será atualizado para **Connected** após alguns minutos.

# 5.15 O que fazer se uma mensagem for exibida indicando que a conexão de VPN não existe depois que as políticas de negociação forem modificadas?

Esse problema é causado pelo intervalo de atualização de página.

Quando modifica as definições de política avançadas, o sistema elimina a conexão de VPN e, em seguida, cria uma. Se a página exibir temporariamente uma mensagem indicando que a conexão está sendo excluída ou criada, não crie a mesma conexão com a mesma sub-rede local, sub-rede do cliente e gateway do cliente novamente.

Se a página permanecer no estado de exclusão ou criação de conexão por muito tempo, **envie um tíquete de serviço**.

# 5.16 Qual é a largura de banda máxima suportada por um gateway de VPN?

A largura de banda máxima suportada por um gateway de VPN é de 1 Gbit/s.

# 5.17 Qual versão do IKE devo selecionar ao criar uma conexão de VPN?

A Huawei Cloud recomenda o IKEv2 porque o IKEv1 não é seguro. Além disso, o IKEv2 supera o IKEv1 na negociação e estabelecimento de conexão, métodos de autenticação, processamento de tempo limite de detecção de par inativo (DPD) e processamento de tempo limite de associação de segurança (AS).

A Huawei Cloud não suportará o IKEv1 em breve.

## Introdução ao IKEv1 e IKEv2

- Como um protocolo híbrido, o IKEv1 traz alguns defeitos de segurança e desempenho devido à sua complexidade. Como tal, tornou-se um gargalo no sistema de IPsec.
- IKEv2 aborda os problemas de IKEv1 mantendo funções básicas de IKEv1. O IKEv2 é mais simplificado, eficiente, seguro e robusto que o IKEv1. Além disso, o IKEv2 é definido pelo RFC 4306 em um único documento, enquanto o IKEv1 é definido em vários documentos. Ao minimizar as funções principais e os algoritmos de senha padrão, o IKEv2 melhora significativamente a interoperabilidade entre diferentes VPNs IPsec.

## Riscos de segurança do IKEv1

- Os algoritmos criptográficos suportados pelo IKEv1 não foram atualizados por mais de 10 anos. Além disso, o IKEv1 não oferece suporte a algoritmos criptográficos fortes, como AES-GCM e ChaCha20-Poly1305. Para IKEv1, o bit E (criptografia) no cabeçalho ISALMP especifica que as cargas úteis seguintes ao cabeçalho ISALMP são criptografadas, mas qualquer verificação de integridade de dados dessas cargas úteis é tratada por uma carga útil hash separada. Essa separação entre criptografia e proteção de

integridade de dados impede o uso de criptografia autenticada (AES-GCM) com o IKEv1.

- O IKEv1 é vulnerável a ataques de amplificação de DoS e ataques de conexão semiaberta. Depois de responder a pacotes falsificados, o respondedor mantém relações iniciador-responder, consumindo um grande número de recursos do sistema.

  Este defeito é inerente ao IKEv1 e é abordado no IKEv2.

- O modo agressivo do IKEv1 não é seguro. Nesse modo, os pacotes de informações não são criptografados, apresentando riscos de vazamento de informações. Há também ataques de força bruta visando o modo agressivo, como ataques man-in-the-middle.

## Diferenças entre IKEv1 e IKEv2

- **Processo de negociação**
  - O IKEv1 é complexo e consome uma grande quantidade de largura de banda. Negociação de AS de IKEv1 consiste em duas fases. No IKEv1 fase 1, uma AS de IKE é estabelecida em modo principal ou modo agressivo. O modo principal requer três trocas entre pares, totalizando seis mensagens ISAKMP, enquanto o modo agressivo requer duas trocas, totalizando três mensagens ISAKMP. O modo agressivo é mais rápido, mas não fornece proteção de identidade para pares, pois a troca de chaves e a autenticação de identidade são realizadas simultaneamente. Na fase 2 do IKEv1, as ASs de IPsec são estabelecidas por meio de três mensagens ISAKMP no modo rápido.
  - Comparado com o IKEv1, o IKEv2 simplifica o processo de negociação de AS. O IKEv2 requer apenas duas trocas, totalizando quatro mensagens, para estabelecer uma AS de IKE e um par de ASs de IPsec. Para criar vários pares de ASs de IPsec, apenas uma troca adicional é necessária para cada par adicional de ASs.

    NOTA

    Para negociação de IKEv1, o seu modo principal envolve nove (6+3) mensagens, e seu modo agressivo envolve seis (3+3) mensagens. Em contraste, a negociação de IKEv2 requer apenas quatro (2+2) mensagens.

- **Métodos de autenticação**
  - Somente o IKEv1 (que exige um cartão de criptografia) suporta autenticação de envelope digital (HSS-DE).
  - O IKEv2 oferece suporte à autenticação EAP (Extensible Authentication Protocol). O IKEv2 pode usar um servidor AAA para autenticar remotamente usuários de dispositivos móveis e de PC e atribuir endereços IP privados a esses usuários. O IKEv1 não fornece essa função e deve usar o L2TP para atribuir endereços IP privados.
  - Apenas o IKEv2 suporta algoritmos de integridade de AS de IKE.

- **Processamento de tempo limite da DPD**
  - Somente o IKEv1 suporta o parâmetro **retry-interval**. Se um dispositivo envia um pacote de DPD, mas não recebe nenhuma resposta dentro do intervalo de repetição especificado, o dispositivo grava um evento de falha de DPD. Quando o número de eventos de falha de DPD atinge 5, ambas ASs de IKE e IPsec são excluídas. A negociação da AS de IKE será iniciada novamente somente quando houver tráfego a ser transmitido pelo túnel de IPsec.
  - No IKEv2, o intervalo de retransmissão aumenta de 1, 2, 4, 8, 16, 32 para 64, em segundos. Se nenhuma resposta for recebida dentro de oito transmissões

consecutivas, a extremidade do par será considerada inativa e as ASs de IKE e IPsec serão excluídas.

- **Processamento de tempo limite da AS de IKE e processamento de tempo limite da AS de IPsec**

  No IKEv2, a vida útil suave da AS de IKE é 9/10 da vida útil dura da AS de IKE mais ou menos um número aleatório. Isso reduz a probabilidade de que duas extremidades iniciem a renegociação simultaneamente. Portanto, você não definir manualmente a vida útil suave em IKEv2.

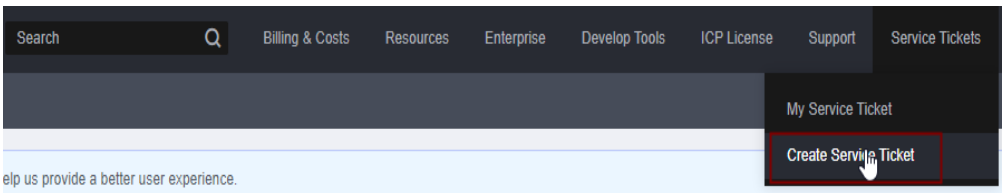
### Vantagens do IKEv2 em relação ao IKEv1

- Simplifica o processo de negociação de AS, melhorando a eficiência.
- Corrige muitas vulnerabilidades de segurança criptográfica, melhorando a segurança.
- Suporta autenticação EAP, melhorando a flexibilidade e escalabilidade da autenticação.
- O EAP é um protocolo de autenticação que suporta vários métodos de autenticação. A maior vantagem do EAP é a sua escalabilidade. Ou seja, novos métodos de autenticação podem ser adicionados sem alterar o sistema de autenticação original. A autenticação EAP tem sido amplamente utilizada em redes de acesso de discagem.
- Emprega uma carga útil criptografada com base no ESP. Essa carga útil contém um algoritmo de criptografia e um algoritmo de integridade de dados. O AES-GCM garante confidencialidade, integridade e autenticação e funciona bem com o IKEv2.

## 5.18 Quais são os tipos de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

1. Faça logon no console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

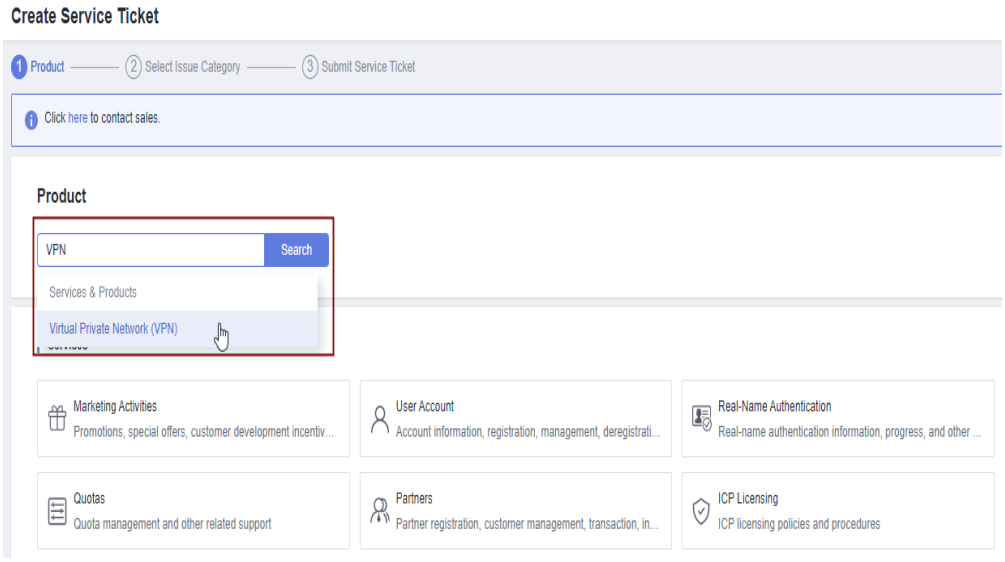
   **Figura 5-1** Criar tíquete de serviço

3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 5-2** Selecionar **Virtual Private Network (VPN)**



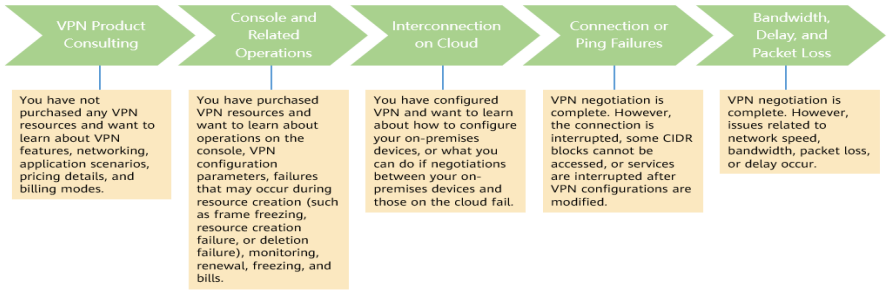

4. Selecione uma categoria de problema.

**Figura 5-3** Selecionar categoria de problema


NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 5-4** Categoria de emissão e base de classificação



# 5.19 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A PSK é configurada em um gateway de VPN e uma conexão será estabelecida após a conclusão da negociação de VPN. Portanto, nenhum nome de usuário ou senha é necessário para criar uma conexão de VPN IPsec. Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

O IPsec XAUTH fornece autenticação estendida para VPN IPsec. Ele requer que os usuários insiram seus nomes de usuário e senhas durante a negociação da VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

# 5.20 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As seguintes informações de largura de banda de um endereço IP de gateway de VPN podem ser monitoradas: tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as informações de monitoramento, clique em  na coluna **Gateway IP Address** na lista de gateways de VPN.

**Conexão de VPN**

As seguintes informações sobre uma conexão de VPN podem ser monitoradas: status da conexão de VPN, tempo médio de ida e volta (RTT) do link, RTT máximo do link, taxa de perda de pacotes do link, RTT médio do túnel, RTT máximo do túnel e taxa de perda de pacotes do túnel.

Para monitorar o RTT médio do link, o RTT máximo do link, a taxa de perda de pacotes do link, o RTT médio do túnel, o RTT máximo do túnel e a taxa de perda de pacotes do túnel, clique no nome da conexão de VPN e em **Add** na área **Health Check** da página da guia **Summary** para adicionar itens de verificação de integridade.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 5.21 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 6 Negociação e interconexão de VPN

## 6.1 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud é compatível com o protocolo IPsec (Internet Protocol Security) padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implantado atrás de um gateway de NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores domésticos comuns de banda larga, hosts de Windows que fornecem serviços VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os seguintes produtos podem se conectar à Huawei Cloud por meio de VPNs:
  - Dispositivos: firewalls e roteadores de acesso (ARs) da Huawei, firewalls de Hillstone e firewalls de Check Point
  - Serviços em nuvem: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) e Microsoft Azure
  - Software: StrongSwan
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud através de uma VPN.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- Alguns dispositivos suportam VPN IPsec somente após a compra das licenças de software necessárias.

  O administrador do centro de dados no local pode verificar com o fornecedor do dispositivo se é necessária uma licença com base no modelo do dispositivo.

# 6.2 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 6-1** Parâmetros de negociação de VPN

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● AES-256-GCM-16 |
| | DH Algorithm | ● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21 |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Lifetime (s) | **86400** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Local ID | ● Endereço IP<br>O endereço IP local é exibido automaticamente como o EIP do gateway de VPN, eliminando a necessidade de configurá-lo manualmente.<br>● FQDN<br>Por padrão, o tipo de ID local é o endereço IP e o valor de ID local é o EIP do gateway de VPN. |
| | Customer ID | ● Endereço IP<br>● FQDN<br>Por padrão, o tipo de ID do cliente é o endereço IP e o valor de ID do cliente é o endereço IP público do gateway do cliente. |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256-GCM-16 |
| | PFS | ● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor predefinido)<br>● DH group 15<br>● DH group 16<br>● DH group 19<br>● DH group 20<br>● DH group 21<br>● Disable |

| Protocolo | Parâmetro | Valor |
| --- | --- | --- |
| | Transfer Protocol | ● ESP (valor padrão) |
| | Lifetime (s) | **3600** (valor padrão)<br>Unidade: segundo<br>Intervalo de valores: **30** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Quando o PFS estiver habilitado, uma troca de DH adicional será executada durante a negociação da AS do IPsec para gerar uma nova chave da AS do IPsec, melhorando a segurança da AS do IPsec.
- Por motivos de segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no dispositivo de gateway no data center local e que as configurações do PFS em ambas as extremidades sejam as mesmas. Caso contrário, a negociação fracassará.
- O tempo de vida padrão baseado em tráfego de uma AS de IPsec é de 1.843.200 KB e não pode ser alterado para a VPN da Huawei Cloud. Este parâmetro não está envolvido na negociação e não tem impacto no estabelecimento de uma AS de IPsec.

# 6.3 Uma conexão de VPN IPsec é estabelecida automaticamente?

Sim. Uma conexão de VPN IPsec é estabelecida automaticamente.

# 6.4 Como configurar uma VPN em um dispositivo local? (Exemplo de configuração de VPN em um firewall da série USG6600 da Huawei)

As configurações de VPN no dispositivo em seu data center local devem ser consistentes com as da nuvem. Caso contrário, a VPN não pode ser estabelecida.

Para configurar uma VPN, você também precisa configurar um túnel de VPN IPsec no roteador ou firewall em seu data center local. O método de configuração varia de acordo com o dispositivo de rede em uso. Para obter detalhes, consulte o guia de configuração do dispositivo de rede.

A seguir, é usado um firewall da série USG6600 da Huawei executando V100R001C30SPC300 como um exemplo para descrever como configurar uma VPN em um dispositivo local.

Suponha que as sub-redes de um centro de dados no local são 192.168.3.0/24 e 192.168.4.0/24 e o endereço IP público da saída de túnel de IPsec no centro de dados no local é 1.1.1.2. As sub-redes de uma VPC são 192.168.1.0/24 e 192.168.2.0/24, e o endereço IP público da saída do túnel de IPsec na VPC é 1.1.1.1.

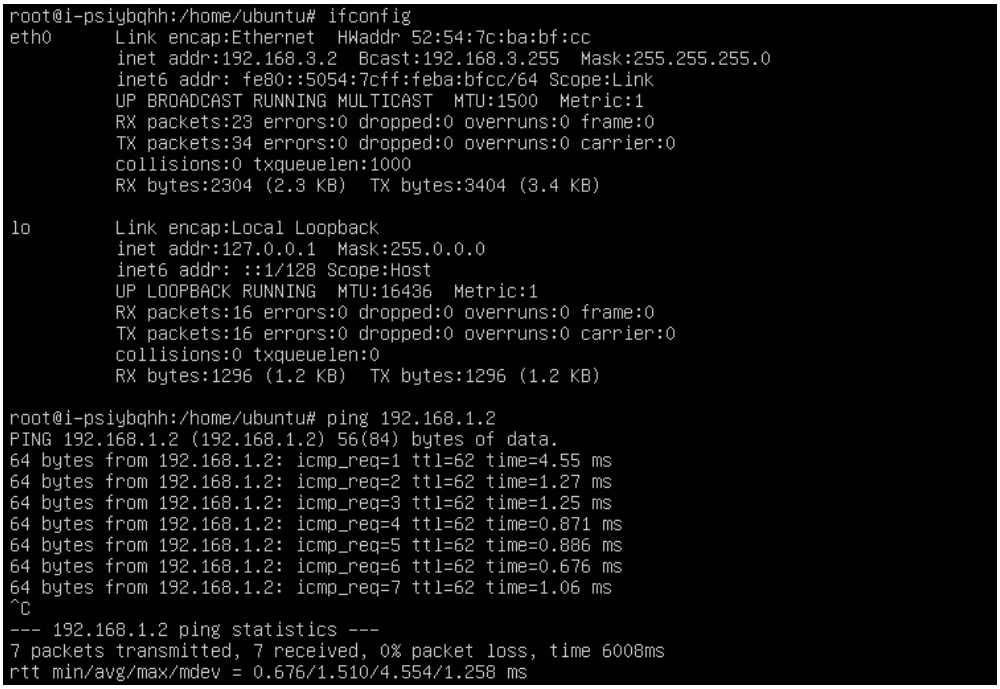
## Procedimento

1. Efetue logon na interface de linha de comando (CLI) do firewall.
2. Verifique as informações de versão do firewall.
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
   ```
3. Crie uma ACL.
   ```
   acl number 3065 vpn-instance vpn64
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   q
   ```
4. Crie uma proposta de IKE.
   ```
   ike proposal 64
   dh group5
   authentication-algorithm sha1
   integrity-algorithm hmac-sha2-256
   sa duration 3600
   q
   ```
5. Crie um par IKE e vincule-o à proposta de IKE criada. O endereço IP do par é 1.1.1.1.
   ```
   ike peer vpnikepeer_64
   pre-shared-key ******** (******** indicates a pre-shared key.)
   ike-proposal 64
   undo version 2
   remote-address vpn-instance vpn64 1.1.1.1
   sa binding vpn-instance vpn64
   q
   ```
6. Configure uma proposta de IPsec.
   ```
   IPsec proposal IPsecpro64
   encapsulation-mode tunnel
   esp authentication-algorithm sha1
   q
   ```
7. Configure uma política de IPsec e vincule a proposta de IPsec a ela.
   ```
   IPsec policy vpnIPsec64 1 isakmp
   security acl 3065
   pfs dh-group5
   ike-peer vpnikepeer_64
   proposal IPsecpro64
   local-address 1.1.1.2
   q
   ```
8. Aplique a política de IPsec à subinterface correspondente.
   ```
   interface GigabitEthernet0/0/2.64
   IPsec policy vpnIPsec64
   q
   ```
9. Teste a conectividade.

   Teste a conectividade entre o ECS na nuvem e um host no data center local, conforme mostrado em **Figura 6-1**.

**Figura 6-1** Teste de conectividade




# 6.5 A VPN da Huawei Cloud oferece suporte à interconexão com um gateway de cliente por meio de um nome de domínio?

Não. A VPN da Huawei Cloud oferece suporte à interconexão com um gateway do cliente apenas por meio do endereço IP público do gateway do cliente.

# 6.6 Quantos túneis minha conexão de VPN tem?

Número de túneis em uma conexão de VPN = número de sub-redes locais x número de sub-redes de clientes

- Um túnel de IPsec está no estado Active quando o tráfego de dados é transmitido entre duas sub-redes nas duas extremidades do túnel de IPsec.
- Uma conexão de VPN está no estado Connected, desde que um de seus túneis esteja no estado Active

# 6.7 Como permitir que hosts específicos acessem uma sub-rede da VPC por meio de uma conexão VPN criada?

Restrições no data center local:

- Políticas de controle de acesso no dispositivo de VPN
- Regras de ACL no roteador ou comutador

Restrições no lado da nuvem:

- Regras de grupo de segurança que permitem o acesso apenas a partir de endereços IP especificados
- Regras de ACL

NOTA

Recomenda-se que você não altere a sub-rede local ou do cliente para controlar o acesso.

# 6.8 As VPNs da Huawei Cloud têm a função DPD ativada?

Sim.

Por padrão, a função de detecção de par inativo (DPD) está ativada para que as VPNs da Huawei Cloud detectem o estado do processo IKE em um data center local.

Após três falhas de detecção consecutivas, o processo IKE no data center local é considerado anormal e o túnel na nuvem é excluído automaticamente.

O protocolo de DPD não exige que a extremidade do par esteja configurada igualmente com DPD, mas exige que a extremidade do par possa responder às detecções de DPD. Para garantir estados de túnel consistentes nas duas extremidades, é recomendável que você ative a DPD no gateway local para detectar o estado do processo IKE do serviço VPN na Huawei Cloud.

NOTA

A exclusão do túnel no caso de falhas de detecção DPD não afetará a estabilidade do serviço.

# 6.9 Como usar grupos de segurança para impedir o acesso da VPN a alguns ECSs em uma VPC para implementar o isolamento de segurança?

Você pode configurar grupos de segurança para permitir acesso apenas a blocos CIDR ou ECSs específicos em uma VPC por meio de uma VPN.

**Exemplo de configuração**: impedir que a sub-rede do cliente 192.168.1.0/24 acesse ECSs na sub-rede da VPC 10.1.0.0/24.

**Procedimento:**

1. Crie os grupos de segurança 1 e 2.
2. Configure o grupo de segurança 1 para negar acesso da sub-rede 192.168.1.0/24.
3. Configure o grupo de segurança 2 para permitir o acesso da sub-rede 192.168.1.0/24.
4. Associe ECSs na sub-rede 10.1.0.0/24 ao grupo de segurança 1 e associe outros ECSs na VPC ao grupo de segurança 2.

# 6.10 Uma conexão de VPN será restabelecida após sua configuração ser modificada?

Uma conexão de VPN consiste em sub-redes locais, sub-redes do cliente, gateway do cliente, chaves pré-compartilhadas (PSKs), política de negociação de IKE e política de negociação de IPsec. Uma conexão de VPN será modificada se ocorrer uma das seguintes situações:

- Se as sub-redes locais e do cliente forem modificadas, o ID de conexão permanecerá inalterada. Se nem todas as sub-redes forem atualizadas, o túnel estabelecido entre as sub-redes não será restabelecido.
- Se o endereço IP do gateway do cliente for alterado, o ID de conexão permanecerá inalterado, mas a conexão de VPN será restabelecida.
- Se apenas as PSKs forem alteradas, o ID e o status da conexão permanecerão inalterados. A PSK será verificada novamente durante a renegociação. Se as PSKs não combinam, a renegociação falha.
- Se uma política de negociação for modificada (é necessária a verificação da PSK), o ID da conexão será alterado e a conexão precisará ser restabelecida.

# 6.11 Por que não consigo iniciar uma negociação da Amazon Web Services para a Huawei Cloud depois que elas estão interconectadas?

Depois que uma conexão de VPN é estabelecida entre a Amazon Web Services (AWS) e a Huawei Cloud, a AWS trabalha no modo Response e não inicia a negociação. Como tal, o estabelecimento de AS não será acionado quando um EC2 de AWS acessar um ECS da Huawei Cloud.

De acordo com o documento da AWS, a negociação pode ser iniciada apenas do lado do cliente (neste caso, a Huawei Cloud).

# 6.12 Como configurar DPD para interconexão com a Huawei Cloud?

Por padrão, a DPD está ativada na Huawei Cloud e não pode ser desativada.

Você pode configurar a DPD da seguinte maneira:

- DPD-type: sob demanda
- DPD idle-time: 30 s
- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

O formato de **DPD msg** em ambas as extremidades da conexão de VPN deve ser o mesmo, mas o tipo de DPD, o tempo ocioso, o intervalo de retransmissão e o limite de repetição podem ser diferentes.

# 6.13 O que fazer se meu firewall não puder receber pacotes de resposta de gateway da VPN da Huawei Cloud na fase 1 do IKE?

1. Verifique se os endereços IP públicos das duas extremidades podem se comunicar executando o comando ping. Por padrão, os EIPs do gateway de VPN na Huawei Cloud podem ser pingados.
2. Verifique se o gateway local (firewall) e o gateway de VPN da Huawei Cloud podem trocar pacotes com as portas UDP 500 e 4500.
3. Verifique se o número da porta de origem não está traduzido quando o gateway local acessar o gateway de VPN na Huawei Cloud. Em uma encenação da travessia de NAT, assegure-se de que o número da porta de origem não esteja mudado após a travessia de NAT.
4. Verifique se as configurações do parâmetro de negociação de IKE são consistentes nas duas extremidades da VPN.

   Em um cenário de travessia de NAT, defina o tipo de ID do cliente como endereço IP e o valor como endereço IP público pós-NAT do gateway local.

# 6.14 O que fazer se meu firewall não conseguir receber pacotes de resposta de uma sub-rede da VPN da Huawei Cloud?

1. Verifique as rotas, as políticas de segurança, a configuração de NAT, o tráfego interessante e as políticas de negociação para a negociação da fase 2 no dispositivo de gateway local.
   - Configurações da rota: encaminhe os dados para acessar sub-redes de nuvem para túneis.
   - Políticas de segurança: permita tráfego de sub-redes locais para sub-redes na nuvem.
   - Políticas de NAT: não execute NAT de origem no tráfego originado de sub-redes locais para sub-redes de nuvem.
   - Trânsito interessante: as configurações de tráfego interessantes em ambas as extremidades são revertidas nas duas extremidades de uma conexão de VPN. O nome do objeto de endereço não pode ser usado para o tráfego interessante configurado usando IKEv2.
   - Políticas de negociação: certifique-se de que as políticas de negociação, especialmente o PFS, em ambas as extremidades sejam as mesmas.
2. Após ter confirmado que as negociações da fase 1 e da fase 2 são normais, assegure-se de que os grupos de segurança na nuvem permitam pacotes ICMP originados das sub-redes locais às sub-redes da nuvem.

# 6.15 Quantos bits têm os grupos DH usados pela VPN da Huawei Cloud?

Os grupos Diffie-Hellman (DH) determinam a força da chave usada no processo de troca de chaves. Números de grupo DH mais altos são geralmente mais seguros, mas é necessário mais tempo para calcular a chave.

Tabela 6-2 lista o número de bits correspondentes aos grupos DH usados pela VPN.

**Tabela 6-2** Número de bits correspondentes a cada grupo DH

| Grupo DH | Módulo |
| --- | --- |
| 1 | 768 bits |
| 2 | 1024 bits |
| 5 | 1536 bits |
| 14 | 2048 bits |
| 15 | 3072 bits |
| 16 | 4096 bits |
| 19 | 256 bits (ECP) |
| 20 | 384 bits (ECP) |
| 21 | 521 bits (ECP) |

NOTA

Os seguintes algoritmos de DH têm riscos de segurança e não são recomendados: DH group 1, DH group 2 e DH group 5.

# 7 Falha de conexão ou ping

## 7.1 Por que uma conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

A configuração pode estar incorreta.

1. Nas duas extremidades (nuvem e centro de dados no local) da conexão de VPN, certifique-se de que as chaves pré-compartilhadas (PSKs) e as informações de negociação sejam consistentes, as sub-redes locais e remotas sejam revertidas, e os gateways locais e remotos também são invertidos.
2. Certifique-se de que as rotas, a NAT e as políticas de segurança estejam configurados corretamente no dispositivo do data center local.

## 7.2 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- As ACLs em ambas as extremidades da conexão de VPN não correspondem.
- As configurações de vida útil da AS em ambas as extremidades da conexão VPN são diferentes.
- A Detecção de par inativo (DPD) não está configurada no dispositivo em seu data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- Nas duas extremidades da conexão de VPN, as configurações de sub-rede local e remota são invertidas.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- DPD está habilitada no dispositivo de gateway local e o número de vezes de detecção é 3 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do dispositivo de gateway local é grande o suficiente para a conexão de VPN.
- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.

# 7.3 Como restaurar rapidamente uma conexão de VPN IPsec interrompida?

1. Se a negociação não puder ser disparada, verifique a conectividade entre os endereços IP públicos dos gateways em ambas as extremidades da conexão de VPN IPsec. Por exemplo, você pode executar o comando ping para verificar a conectividade. Por padrão, o gateway de VPN da Huawei Cloud responde a pacotes ICMP.
2. Se a conectividade for normal, verifique se troca de link ocorre entre interfaces de saída. Ou seja, verifique se o tráfego para acesso ao gateway de VPN da Huawei Cloud é encaminhado para fora de uma interface não negociada.
3. Se o tráfego for encaminhado através do link correto, altere as PSKs em ambas as extremidades da conexão de VPN IPsec para disparar a renegociação.
4. Se a renegociação falhar, verifique se as políticas de negociação configuradas em ambas as extremidades são consistentes e se as configurações de tráfego interessantes em ambas as extremidades são invertidas (mesmo número de configurações e mesmas sub-redes).
5. Se as políticas de negociação e as configurações de tráfego interessantes estiverem corretas, desative a conexão de VPN no dispositivo local. Depois que o estado da conexão de VPN na Huawei Cloud mudar para **Not connected**, ative a conexão de VPN no dispositivo local e acione um fluxo de dados.
6. Se a negociação ainda falhar, execute as seguintes operações:
   a. Registre as políticas de negociação, PSK, sub-redes locais, gateway do cliente e sub-redes do cliente da conexão de VPN configurada na Huawei Cloud.
   b. Use o gateway de VPN existente para criar outra conexão de VPN. As políticas de negociação, PSK e sub-redes locais são as mesmas da conexão de VPN original. O gateway do cliente e as sub-redes do cliente podem ser configurados aleatoriamente.
   c. Depois que a nova conexão de VPN for criada, exclua a conexão de VPN original e altere o gateway do cliente e as sub-redes do cliente da nova conexão de VPN para que sejam as mesmas da conexão de VPN original.
   d. Acione a negociação novamente.

Se a falha persistir, **envie um tíquete de serviço** para o atendimento ao cliente da Huawei Cloud.

# 7.4 O que acontecerá se o tráfego exceder a largura de banda de um gateway de VPN?

A largura de banda do gateway de VPN aplica-se ao tráfego na direção de saída de uma VPC. Se o tráfego de saída na VPC exceder a largura de banda, ocorrerá congestionamento da rede, algumas sub-redes não poderão ser acessadas ou até mesmo a conexão de VPN será interrompida devido ao tempo limite de detecção da VPN.

Neste caso, é aconselhável aumentar a largura de banda do gateway de VPN.

NOTA

A largura de banda máxima de uma VPN é de 1 Gbit/s.

# 7.5 Uma conexão de VPN IPsec é estabelecida automaticamente?

Sim. Uma conexão de VPN IPsec é estabelecida automaticamente.

# 7.6 Por que os ECSs não podem fazer ping entre si nas duas extremidades de uma conexão de VPN normal entre regiões?

Por padrão, um grupo de segurança permite o tráfego de saída com qualquer número de porta. Para permitir tráfego de entrada, adicione regras de entrada ao grupo de segurança. Certifique-se de que o grupo de segurança associado ao ECS que precisa receber pacotes de ping permita solicitações ICMP de entrada.

# 7.7 Por que as sub-redes nas duas extremidades de uma conexão de VPN normal não podem acessar uma à outra?

A conexão de VPN está normal, indicando que os parâmetros de negociação em ambas as extremidades da conexão de VPN estão corretos. Você precisa executar as seguintes operações:

- Verifique se as rotas para o dispositivo de VPN em seu data center local estão configuradas corretamente.
- Verifique se a troca de dados entre sub-redes é permitida no dispositivo de VPN.
- Verifique se a NAT não é executada nas sub-redes locais que precisam acessar a nuvem.
- Verifique se o acesso mútuo entre os endereços IP públicos do gateway de VPN e do gateway do cliente é permitido.

# 7.8 O que fazer se uma conexão de VPN for interrompida e uma mensagem indicando a incompatibilidade de fluxo de dados for exibida?

Isso geralmente é causado por uma incompatibilidade de ACL entre o gateway de VPN na nuvem e o gateway do cliente em seu data center local.

1. Verifique se nas duas extremidades da conexão de VPN, as sub-redes locais e remotas estão invertidas e as configurações ACL também estão invertidas.
2. Use o formato de sub-rede/máscara ao configurar tráfego interessante em seu data center local. Não use o modo de objeto de endereço, pois ele pode causar problemas de incompatibilidade.

# 7.9 O que fazer se uma conexão de VPN for interrompida e uma mensagem indicando o tempo limite de DPD for exibida?

Isso acontece porque não há troca de dados pela conexão de VPN. Quando a vida útil da AS termina, a conexão de VPN é excluída, pois a extremidade do par não responde à detecção de par inativo (DPD).

**Solução**

1. Habilite a DPD no dispositivo de gateway local e verifique se os fluxos de dados de ambas as extremidades podem acionar o estabelecimento de conexão.
2. Implemente um script de shell de ping nos servidores em ambas as extremidades. Como alternativa, configure uma função de manutenção de atividade (por exemplo, NQA em dispositivos da Huawei) no dispositivo de gateway local para manter a conexão ativa.

# 7.10 Por que uma conexão de VPN está no estado Not Connected no console de gerenciamento quando já está disponível?

Há um certo atraso na atualização do estado da conexão de VPN no console de gerenciamento.

Se o acesso ao serviço for normal, a conexão de VPN foi estabelecida.

# 7.11 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 7.12 O que fazer se uma conexão de VPN falha ao ser estabelecida?

1. Faça logon no console de gerenciamento e escolha **Virtual Private Network** > **Enterprise - VPN Connections**.
2. Na lista de conexões de VPN, localize a conexão VPN de destino e escolha **More** > **Modify Policy Settings** à direita para exibir as políticas de IKE e IPsec da conexão de VPN.
3. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.

   Se a AS de IKE tiver sido configurada na fase 1, mas nenhuma AS de IPsec tiver sido estabelecida na fase 2, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.
4. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   ```
5. Faça ping nas duas extremidades da conexão de VPN uma da outra para verificar se a conexão de VPN está normal.

# 7.13 O que devo fazer se não conseguir acessar os ECSs na nuvem a partir do meu data center ou LAN local após a conexão de VPN ter sido configurada?

Por predefinição, o grupo de segurança nega o acesso a todas as origens. Se você quiser acessar seus ECSs, configure regras de grupo de segurança para permitir o acesso de suas sub-redes locais.

# 7.14 Por que o estado de uma conexão de VPN criada com sucesso é exibido como Not Connected?

Há um atraso na atualização do estado de uma conexão de VPN no console de gerenciamento. Por favor, atualize a página em cerca de 2 minutos.

# 7.15 As VPNs da Huawei Cloud têm a função DPD ativada?

Sim.

Por padrão, a função de detecção de par inativo (DPD) está ativada para que as VPNs da Huawei Cloud detectem o estado do processo IKE em um data center local.

Após três falhas de detecção consecutivas, o processo IKE no data center local é considerado anormal e o túnel na nuvem é excluído automaticamente.

O protocolo de DPD não exige que a extremidade do par esteja configurada igualmente com DPD, mas exige que a extremidade do par possa responder às detecções de DPD. Para garantir estados de túnel consistentes nas duas extremidades, é recomendável que você ative a DPD no gateway local para detectar o estado do processo IKE do serviço VPN na Huawei Cloud.

**NOTA**

A exclusão do túnel no caso de falhas de detecção DPD não afetará a estabilidade do serviço.

DPD pode detectar exceções no processo IKE na extremidade do par no tempo e redefinir o túnel para garantir a sincronização do túnel entre as duas extremidades. Depois que um túnel é excluído, se houver tráfego transmitido pelo túnel, o túnel poderá ser restabelecido por meio da negociação.

# 8 Endereços públicos

## 8.1 O EIP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Se um EIP de pagamento por uso estiver vinculado a um gateway de VPN de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP vinculado.

Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway da VPN.

## 8.2 EIPs podem ser usados como endereços IP de gateway de VPN?

Não.

Quando você cria um gateway de VPN, seu endereço IP é atribuído automaticamente. Esse endereço IP tem configurações predefinidas e pode ser usado para interconexão com uma VPC. No entanto, um EIP não pode ser usado para interconexão com uma VPC.

## 8.3 Preciso comprar EIPs para que os hosts se comuniquem entre si por meio de uma VPN?

Se os seus hosts locais precisarem acessar um ECS na nuvem por meio de uma VPN, você não precisará comprar EIPs para o ECS.

Se um ECS precisar fornecer serviços acessíveis pela Internet, será necessário adquirir um EIP para o ECS.

## 8.4 Por que um ECS tem informações de acesso de EIP depois que habilitar uma VPN?

Uma causa possível é que o ECS tem um EIP vinculado antes que a VPN seja usada. Nesse cenário, você pode acessar o ECS por meio da VPN e do EIP.

Para permitir que apenas hosts na VPN acessem o ECS, desvincule o EIP do ECS depois que a conexão de VPN for estabelecida.

# 8.5 Meu gateway local pode ter um endereço IP público não fixo?

Não.

Para conectar seu data center local à Huawei Cloud por meio de uma VPN, seu gateway local deve ter um endereço IP público fixo. Esse endereço IP público fixo que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implementado atrás de um gateway NAT).

NOTA

Roteadores domésticos comuns de banda larga, hosts de Windows que fornecem serviços VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.

# 9 Configurações da rota

## 9.1 O que são um gateway de cliente e uma sub-rede de cliente em uma conexão de VPN?

Uma conexão de VPN é criada na Huawei Cloud. Como tal, uma sub-rede de uma VPC da Huawei Cloud é uma sub-rede local e um gateway de VPN criado na Huawei Cloud é um gateway local. A sub-rede e o gateway em um data center local conectado à VPC são uma sub-rede do cliente e um gateway do cliente, respectivamente.

Um endereço IP de gateway de cliente é um endereço IP público.

## 9.2 Onde adicionar rotas para sub-redes do cliente no console da VPN?

Quando uma conexão de VPN é criada, as rotas para as sub-redes do cliente são entregues automaticamente.

## 9.3 Preciso adicionar uma rota para um ECS com várias NICs para alcançar a rede local?

- Se a placa de interface de rede (NIC) primária for usada para estabelecer uma conexão de VPN com a rede local, nenhuma rota precisará ser adicionada.
- Se uma NIC não primária for usada para estabelecer uma conexão de VPN com a rede local, adicione uma rota para a rede local com o endereço de gateway da NIC não primária como o próximo salto.

# 10 Configurações de sub-rede

## 10.1 Quais são as precauções para configurar as sub-redes locais e de cliente para uma conexão de VPN?

- O número de sub-redes locais e o número de sub-redes de clientes são limitados. Se o número de sub-redes locais ou de clientes exceder o limite superior, agregue as sub-redes.
  - Número máximo de sub-redes locais para cada gateway de VPN: 50
  - Número máximo de sub-redes de clientes para cada conexão de VPN: 50
- A sub-rede local não pode incluir o bloco CIDR da sub-rede remota. A sub-rede remota pode incluir o bloco CIDR da sub-rede local.
- Há rotas que apontam para as sub-redes locais na VPC onde o gateway de VPN reside.
- Se houver duas conexões (conexão A e conexão B) criadas para um gateway de VPN, e a sub-rede remota da conexão A estiver dentro da conexão B, quando a rede de destino a ser acessada pertencer ao bloco CIDR sobreposto, a conexão criada primeiro será correspondida primeiro, independentemente do status da conexão. (A correspondência de comprimento da máscara não é usada para a VPN baseada em políticas.)

## 10.2 Quantas sub-redes locais e de clientes posso adicionar a uma VPN?

- Você pode configurar um máximo de 50 sub-redes locais para cada gateway de VPN.
- Você pode configurar um máximo de 50 sub-redes de clientes para cada conexão de VPN.

# 10.3 O que fazer se ocorrer uma exceção quando adicionar uma sub-rede do cliente durante a criação da conexão de VPN?

Verifique se essa sub-rede do cliente está envolvida em uma rota de uma conexão de emparelhamento de VPC, Cloud Connect ou Direct Connect. Em caso afirmativo, ocorre um conflito de rota e você precisa excluir a rota e criar uma nova para evitar o conflito.

# 10.4 O EIP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Se um EIP de pagamento por uso estiver vinculado a um gateway de VPN de pagamento por uso, a exclusão do gateway de VPN também excluirá o EIP vinculado.

Para manter esse EIP de pagamento por uso, desvincule-o antes de excluir o gateway da VPN.

# 10.5 Como planejar blocos CIDR para acesso a uma VPC por meio de uma conexão de VPN?

- Os blocos CIDR de uma VPC não podem entrar em conflito com os blocos CIDR locais.
- Para evitar conflitos com endereços de serviço de nuvem, não use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3 ou 100.64.0.0/10 para sua rede local.

# 10.6 Como um endereço IP de gateway de VPN é alocado?

Os endereços IP do gateway de VPN da Huawei Cloud são um grupo de endereços IP planejados antes da aquisição dos gateways de VPN. Esses endereços IP são predefinidos com configurações de VPN.

Quando você compra um gateway de VPN, o sistema atribui aleatoriamente um endereço IP e o vincula à VPC selecionada. Esse endereço IP pode ser vinculado a apenas uma VPC.

Você não pode alterar o endereço IP de um gateway de VPN, pois esse endereço IP tem configurações predefinidas. Quando um gateway de VPN é excluído, a relação de vinculação entre o endereço IP do gateway e a VPC do gateway é liberada. Quando um novo gateway de VPN é comprado, o sistema aloca aleatoriamente um novo endereço IP de gateway.

# 11 Tráfego interessante da VPN

## 11.1 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa configurar regras de política (regras de ACL) para uma conexão de VPN no console de gerenciamento da Huawei Cloud somente quando **VPN Type** estiver definido como **Policy-based**.

## 11.2 Como configurar e modificar o tráfego interessante de uma VPN na nuvem?

O número de regras que especificam o tráfego interessante é o produto do número de sub-redes locais e do número de sub-redes de clientes. Por exemplo, quando há sub-redes locais A e B e sub-redes de clientes C, D e E, as seis regras a seguir precisam ser configuradas para especificar o tráfego interessante:

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

Se você modificar as sub-redes locais ou do cliente no console de gerenciamento, a configuração de tráfego interessante será atualizada automaticamente. Ou seja, as regras de ACL na nuvem são modificadas.

# 12 Manutenção das conexões de VPN ativas

## 12.1 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- As ACLs em ambas as extremidades da conexão de VPN não correspondem.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são diferentes.
- A Detecção de par inativo (DPD) não está configurada no dispositivo em seu data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- Nas duas extremidades da conexão de VPN, as configurações de sub-rede local e remota são invertidas.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- A DPD está ativada no dispositivo de gateway local e o número de vezes de detecção é 3 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do dispositivo de gateway local é grande o suficiente para a conexão de VPN.

- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.

# 13 Monitoramento

## 13.1 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As seguintes informações de largura de banda de um endereço IP de gateway de VPN podem ser monitoradas: tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as informações de monitoramento, clique em  na coluna **Gateway IP Address** na lista de gateways de VPN.

**Conexão de VPN**

As seguintes informações sobre uma conexão de VPN podem ser monitoradas: status da conexão de VPN, tempo médio de ida e volta (RTT) do link, RTT máximo do link, taxa de perda de pacotes do link, RTT médio do túnel, RTT máximo do túnel e taxa de perda de pacotes do túnel.

Para monitorar o RTT médio do link, o RTT máximo do link, a taxa de perda de pacotes do link, o RTT médio do túnel, o RTT máximo do túnel e a taxa de perda de pacotes do túnel, clique no nome da conexão de VPN e em **Add** na área **Health Check** da página da guia **Summary** para adicionar itens de verificação de integridade.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

## 13.2 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Para exibir o status de uma conexão de VPN, clique em  na coluna **Monitoring** da conexão de VPN.

# 13.3 Posso ver o tráfego de cada conexão de VPN?

Não. O tráfego de VPN é monitorado por um gateway de VPN. Você pode visualizar o tráfego de entrada e saída, bem como as larguras de banda de entrada e saída de um gateway de VPN, mas não pode visualizar as estatísticas de tráfego de uma conexão de VPN específica.

# 13.4 Será notificado de resultados anormais de monitoramento de VPN?

Sim.

Você pode configurar, nos consoles de Simple Message Notification (SMN) e Cloud Eye, para receber notificações se ocorrerem resultados anormais de monitoramento de VPN.

# 14 Largura de banda e velocidade da rede

## 14.1 Como a velocidade da rede de uma conexão de VPN é testada?

Ambiente de teste: uma conexão de VPN foi criada. Os ECSs foram criados nas sub-redes locais das VPCs nas duas extremidades da conexão de VPN. Os ECSs podem fazer ping um ao outro.

**Quando a largura de banda de um gateway de VPN adquirido é de 200 Mbit/s:**

1. Quando os ECSs nas duas extremidades da conexão de VPN executam o Windows, o iPerf3 e o FileZilla são usados para testar a velocidade da rede. O resultado do teste é de 180 Mbit/s, atendendo aos requisitos.

   NOTA

   O protocolo FTP baseado em TCP tem um mecanismo de controle de congestionamento e o protocolo IPsec adiciona novos cabeçalhos aos pacotes originais. Como tal, é normal na indústria, ter um desvio de velocidade de rede de cerca de 10%.

   **Figura 14-1** mostra o resultado do teste da largura de banda de 200 Mbit/s no cliente iPerf3.

   **Figura 14-1** Resultado do teste para largura de banda de 200 Mbit/s (cliente de iPerf3)

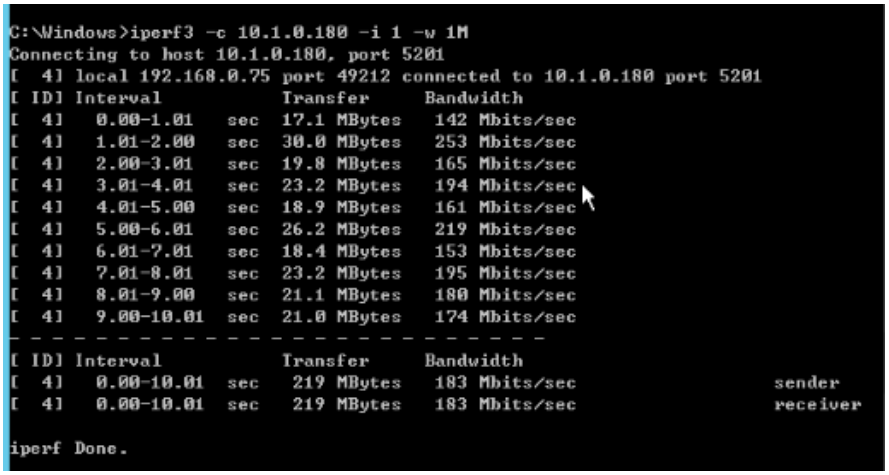
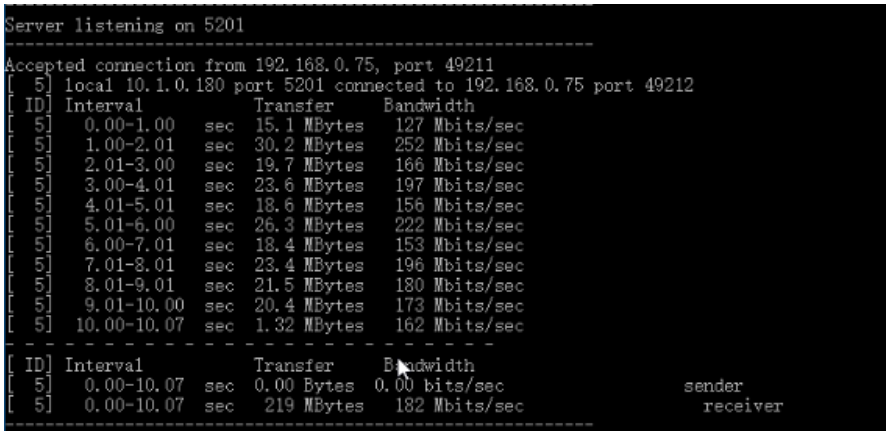


**Figura 14-2** mostra o resultado do teste da largura de banda de 200 Mbit/s no servidor iPerf3.

**Figura 14-2** Resultado do teste para largura de banda de 200 Mbit/s (servidor de iPerf3)

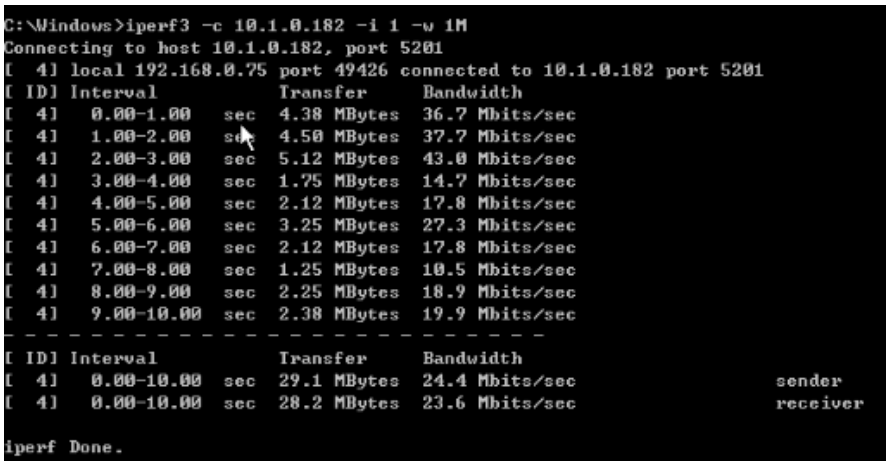



2. Quando os ECSs nas duas extremidades da conexão de VPN executam o CentOS 7, o iPerf3 é usado para testar a velocidade da rede. O resultado do teste é de 180 Mbit/s, atendendo aos requisitos.
3. Quando o ECS funciona como um servidor executa o CentOS 7 e o ECS funciona como um cliente que executa Windows, iPerf3 e FileZilla são usados para testar a velocidade da rede. O resultado do teste é de 20 Mbit/s, não atendendo aos requisitos.

   Isso ocorre porque as implementações de TCP no Windows e no Linux são diferentes.

   **Figura 14-3** mostra o resultado do uso do iPerf3 para testar a velocidade da rede entre dois ECSs que executam sistemas operacionais diferentes.

**Figura 14-3** Resultado do teste no iPerf3




**Quando a largura de banda de um gateway de VPN adquirido é de 1000 Mbit/s:**

NOTA

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.

A largura de banda do gateway de VPN é compartilhada por todas as suas conexões de VPN. Para usar totalmente a grande largura de banda de 1.000 Mbit/s, implemente vários ECSs com

altas especificações, pois o desempenho de encaminhamento de um único ECS é limitado. Os ECSs com suas NICs que suportam a largura de banda de 2 Gbit/s ou superior são recomendados.

**Conclusões: com base nos resultados dos testes anteriores, as larguras de banda dos gateways de VPN da Huawei Cloud atendem aos requisitos. Para usar totalmente a largura de banda adquirida, recomenda-se que você use servidores executando o mesmo sistema operacional e usando NICs que atendam a determinados requisitos nas duas extremidades de uma conexão de VPN.**

# 14.2 Em que direção a largura de banda da VPN é limitada? Qual é a unidade de largura de banda?

A largura de banda do gateway de VPN adquirida aplica-se à direção de saída da Huawei Cloud. Para obter um equilíbrio entre as larguras de banda nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada da seguinte forma:

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

# 14.3 Como alterar a largura de banda da VPN?

1. Na lista de gateways de VPN, clique no nome de um gateway de VPN. A página de detalhes do gateway é exibida.
2. Na área **EIP**, clique em **Change** ao lado de **Bandwidth**.
3. Altere a largura de banda do EIP.

# 14.4 O que acontecerá se o tráfego exceder a largura de banda de um gateway de VPN?

A largura de banda do gateway de VPN aplica-se ao tráfego na direção de saída de uma VPC. Se o tráfego de saída na VPC exceder a largura de banda, ocorrerá congestionamento da rede, algumas sub-redes não poderão ser acessadas ou até mesmo a conexão de VPN será interrompida devido ao tempo limite de detecção da VPN.

Neste caso, é aconselhável aumentar a largura de banda do gateway de VPN.

NOTA

A largura de banda máxima de uma VPN é de 1000 Mbit/s.

# 14.5 Por que a mudança de largura de banda da VPN não faz efeito?

Há uma latência para que a alteração da largura de banda da VPN entre em vigor.

Teste a largura de banda 5 minutos depois de alterar a largura de banda.

NOTA

Alterar a largura de banda da VPN não interromperá os serviços nas redes.

# 14.6 Quais são as diferenças entre a largura de banda de uma conexão de VPN e a de uma conexão direta?

## Conceitos

- A largura de banda de uma conexão Direct Connect é a largura de banda da conexão física criada por um usuário.
- A largura de banda de uma conexão de VPN aplica-se à direção de saída da Huawei Cloud.

## Largura de banda máxima

- Por padrão, a largura de banda máxima de uma conexão Direct Connect é de 1000 Mbit/s. Quando você cria uma conexão no console de gerenciamento e define **Port Type** para **10GE single-mode optical port**, a largura de banda máxima é de 10 Gbit/s.
- A largura de banda máxima de uma VPN é de 1000 Mbit/s.

## Qualidade da rede

- Um usuário da Direct Connect tem uma conexão dedicada com alta qualidade de rede.
- As conexões de VPN compartilham a largura de banda de seu gateway de VPN. Ou seja, a largura de banda total das conexões de VPN não pode exceder a largura de banda do gateway de VPN correspondente. A qualidade da rede será afetada pela qualidade da Internet.

# 14.7 Como determinar minha largura de banda da VPN?

Considere o seguinte ao determinar a largura de banda:

- Quantidade de dados transmitidos por um túnel de VPN em um período de tempo (Reserve largura de banda suficiente para evitar o congestionamento do link.)
- Larguras de banda de saída nas duas extremidades de uma conexão de VPN: a largura de banda de saída no lado da nuvem deve ser menor do que no lado local.

# 15 Cotas

## 15.1 Quais cotas uma VPN tem?

### O que é uma 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.

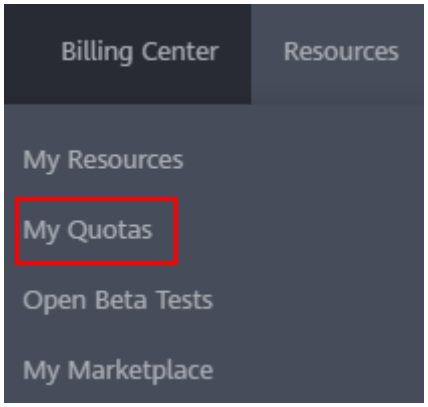
### Tipos de recurso

Os recursos de VPN incluem gateways de VPN, conexões 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. Escolha **Resources** > **My Quotas** no canto superior direito da página.
   A página **Service Quota** é exibida.

   **Figura 15-1** Minhas cotas



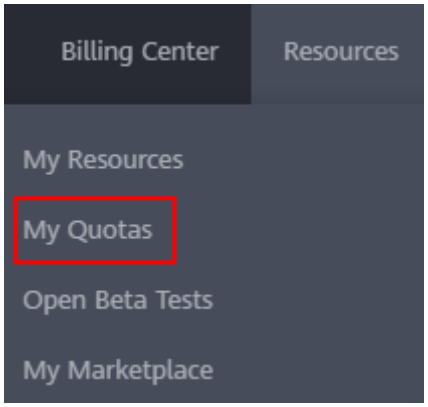

  

4. Visualize a cota usada e total de cada tipo de recursos na página exibida.
   Se uma cota não puder atender aos requisitos de serviço, solicite uma cota mais alta.

## Como solicitar uma cota mais alta?

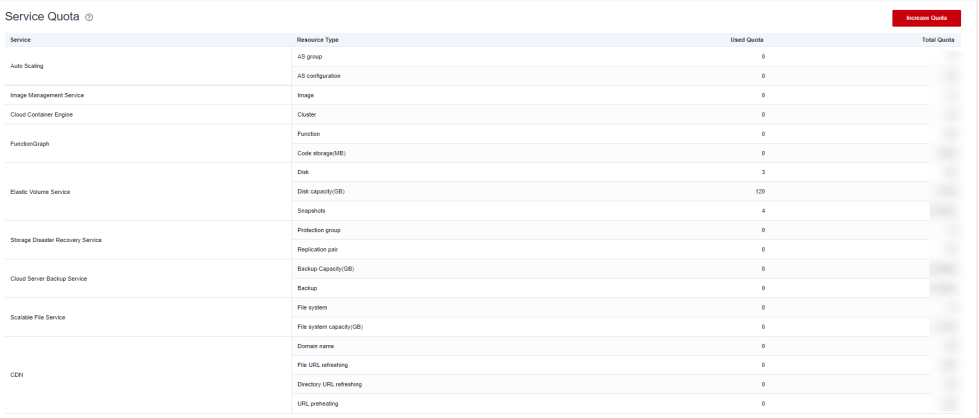
1. Acesse o console de gerenciamento.
2. Escolha **Resources** > **My Quotas** no canto superior direito da página.
   A página **Service Quota** é exibida.

   **Figura 15-2** Minhas cotas




3. Clique em **Increase Quota** no canto superior direito da página.

   **Figura 15-3** Solicitar uma cota maior.




4. Na página **Create Service Ticket**, configure os parâmetros conforme necessário.
   Na área **Problem Description**, insira a cota necessária e o motivo do ajuste da cota.
5. Selecione o acordo e clique em **Submit**.

# 15.2 Quantos gateways de VPN e conexões de VPN posso criar por padrão?

Por padrão, cada usuário pode criar um máximo de 50 gateways de VPN e 100 gateways de clientes. Cada gateway de VPN pode ter um máximo de 100 grupos de conexão. Quando dois EIPs de um gateway de VPN estão conectados ao mesmo endereço IP público de um gateway de cliente, um grupo de conexão de VPN é usado. Quando dois EIPs de um gateway de VPN

estão conectados a dois gateways de cliente ou dois endereços IP públicos do mesmo gateway de cliente, dois grupos de conexão de VPN são usados.

Antes de comprar gateways de VPN, verifique sua cota disponível. Se a cota for insuficiente, **envie um tíquete de serviço** para aumentar a cota.

# 15.3 Como alterar meu gateway de VPN e cotas de conexão?

1. Faça login no console de gerenciamento e escolha **Service Tickets** > **Create Service Ticket** na barra de menus.
2. Na página **Create Service Ticket**, clique em **Quotas** na área **Services**.
3. Clique em **Quota Application** em **Issue Categories**.
4. Clique em **Create Now**.

   Insira as informações necessárias e clique em **Submit**.

# 15.4 Quantas VPNs IPsec posso ter?

Por padrão, cada usuário pode criar um máximo de 50 gateways de VPN e 100 gateways de clientes. Cada gateway de VPN pode ter um máximo de 100 grupos de conexão. Quando dois EIPs de um gateway de VPN estão conectados ao mesmo endereço IP público de um gateway de cliente, um grupo de conexão de VPN é usado. Quando dois EIPs de um gateway de VPN estão conectados a dois gateways de cliente ou dois endereços IP públicos do mesmo gateway de cliente, dois grupos de conexão de VPN são usados.

Antes de comprar gateways de VPN, verifique sua cota disponível. Se a cota for insuficiente, **envie um tíquete de serviço** para aumentar a cota.

# 16 Permissões da conta

## 16.1 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A PSK é configurada em um gateway de VPN e uma conexão será estabelecida após a conclusão da negociação de VPN. Portanto, nenhum nome de usuário ou senha é necessário para criar uma conexão de VPN IPsec. Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

O IPsec XAUTH fornece autenticação estendida para VPN IPsec. Ele requer que os usuários insiram seus nomes de usuário e senhas durante a negociação da VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

## 16.2 O que fazer se o sistema exibir uma mensagem indicando que não tenho as permissões para criar uma VPN?

- Verifique se sua conta é uma conta do IAM.
- Certifique-se de que sua conta do IAM tenha as permissões **VPC Administrator**, **Tenant Guest** e **VPN Administrator**.

  Se sua conta do IAM não tiver operações de operação de VPC, faça logon no console do IAM usando uma conta da Huawei Cloud e conceda as permissões para sua conta do IAM. Para obter detalhes, consulte **Criação de um grupo de usuários e atribuição de permissões** e **Adição de usuários ou remoção de usuários de um grupo de usuários**.

# 16.3 Como determinar que minha conta não pode criar uma VPN devido a permissões insuficientes?

- Os gateways de VPN e as conexões criadas por uma conta da Huawei Cloud são invisíveis para as contas de usuário do IAM.
- Uma mensagem será exibida indicando que o sistema está ocupado se você criar um gateway de VPN ou conexão usando uma conta de usuário do IAM.

Para obter detalhes sobre as permissões necessárias para criar uma conexão de VPN, consulte **O que fazer se o sistema exibir uma mensagem indicando que não tenho as permissões para criar uma VPN?**.

# 17 Classic VPN

## 17.1 Questões gerais

### 17.1.1 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud suporta o protocolo IPsec padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implementado atrás de um gateway NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores domésticos comuns de banda larga, hosts de Windows que fornecem serviços VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os dispositivos que podem se interconectar com o serviço VPN da Huawei Cloud geralmente são dos seguintes:
  - Fornecedores como Huawei (roteadores e firewalls), H3C (roteadores e firewalls), Cisco (roteadores e firewalls), Ruijie (roteadores e firewalls), ZTE, Sangfor, Fortinet, 360, Topsec, NetentSec, Hillstone, NSFOCUS, DELL, ZyXEL e Juniper
  - Provedores de serviços em nuvem, como Alibaba Cloud, Tencent Cloud e Amazon Web Services
  - Fornecedores de software como Openswan, strongSwan e TheGreenBow
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- No entanto, alguns dispositivos suportam VPN IPsec somente após de comprar as licenças de software necessárias.

  Entre em contato com o administrador do data center local para confirmar o modelo do dispositivo com o fornecedor.

## 17.1.2 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 17-1** Parâmetros de negociação de VPN

| Política | Parâmetro | Valor |
| --- | --- | --- |
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256<br>● AES-192<br>● AES-128 (valor padrão) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | DH Algorithm | ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 15<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21<br>**NOTA**<br>Em algumas regiões, apenas **Group 14**, **Group 2** e **Group 5** estão disponíveis. |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Lifecycle (s) | **86400** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | PFS | ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor padrão)<br>● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 15<br>● DH group 16<br>● DH group 19<br>● DH group 20<br>● DH group 21<br>● Disable<br>**NOTA**<br>Em algumas regiões, apenas **DH group 14**, **DH group 2** e **DH group 5** estão disponíveis. |
| | Transfer Protocol | ● ESP (valor padrão)<br>● AH<br>● AH-ESP |
| | Lifecycle (s) | **3600** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **480** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

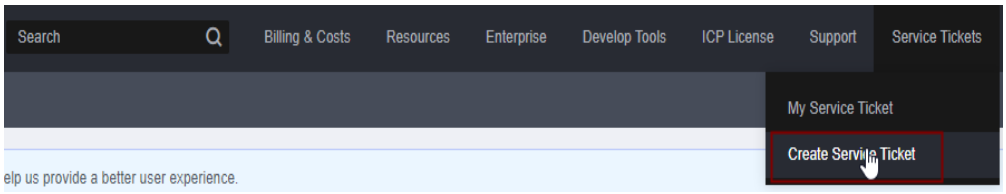
  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Depois que o PFS for configurado, uma troca de DH adicional será executada durante a negociação da AS do IPsec e uma nova chave da AS do IPsec será gerada, melhorando a segurança da AS do IPsec.
- Para garantir a segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no gateway local. Caso contrário, a negociação falhará.
- Para habilitar o PFS, certifique-se de que as configurações em ambas as extremidades de uma VPN sejam as mesmas.
- O tempo de vida baseado em tráfego da AS do IPsec na VPN da Huawei Cloud é padrão para 1.843.200 KB e não pode ser alterado. Esse tempo de vida não afeta o estabelecimento de uma AS de IPsec.

# 17.1.3 Quais são as categorias de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

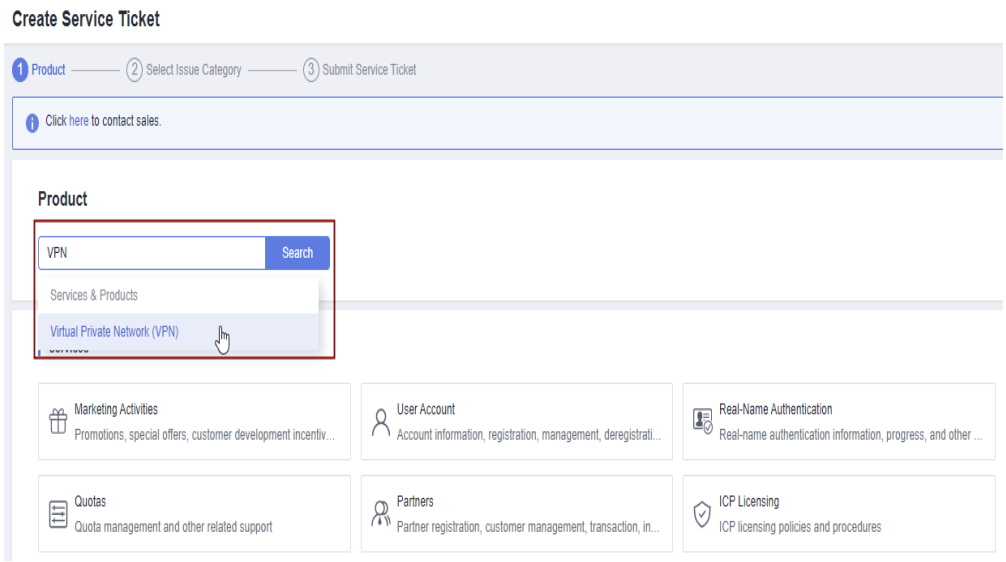
1. Faça logon no console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

**Figura 17-1** Criar tíquete de serviço



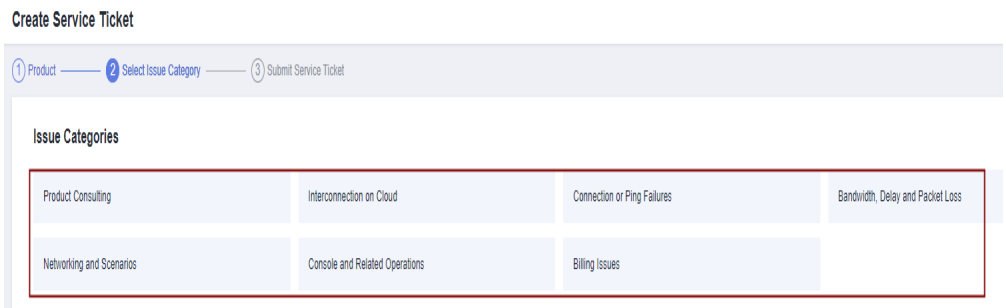

3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 17-2** Selecionar **Virtual Private Network (VPN)**




4. Selecione uma categoria de problema.

**Figura 17-3** Selecionar categoria de problema

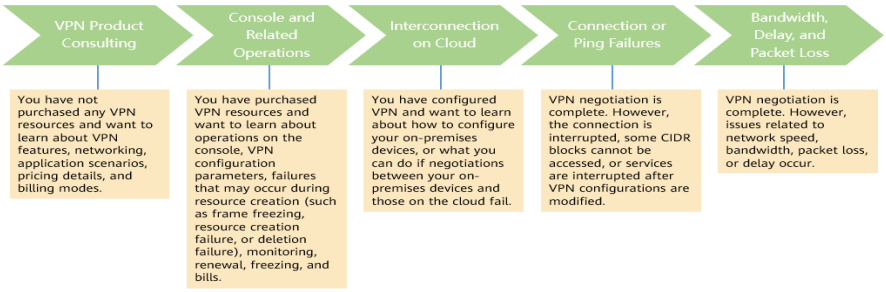


NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 17-4** Categoria de emissão e base de classificação




## 17.1.4 Posso implementar aplicações na nuvem, bancos de dados em um data center local e depois conectá-las por meio de uma VPN?

VPN conecta uma VPC e uma rede local.

Depois que a VPN é configurada com sucesso, a VPC e a rede local podem se comunicar entre si. Nesse caso, o servidor de aplicações que acessa o banco de dados é o mesmo que acessar outros servidores na mesma LAN.

Servidores de nuvem e servidores locais podem se comunicar uns com os outros.

AVISO

- Depois que uma VPN é configurada, verifique se a latência da rede e a perda de pacotes afetam negativamente a execução do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

## 17.1.5 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

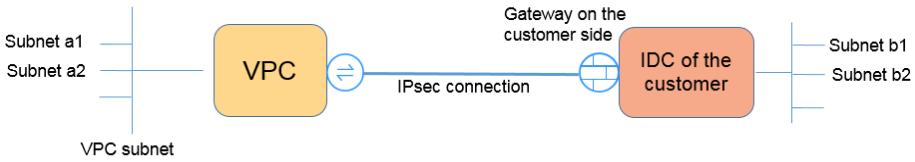
## 17.1.6 O que é uma conexão de VPN? Como definir o número de conexões de VPN ao comprar um gateway de VPN?

Uma conexão de VPN da Huawei Cloud é uma conexão IPsec estabelecida entre um gateway de VPN na nuvem e um endereço IP público independente de um data center local. Você pode configurar várias sub-redes locais (sub-redes da VPC) e sub-redes remotas (sub-redes locais) para uma conexão de VPN.

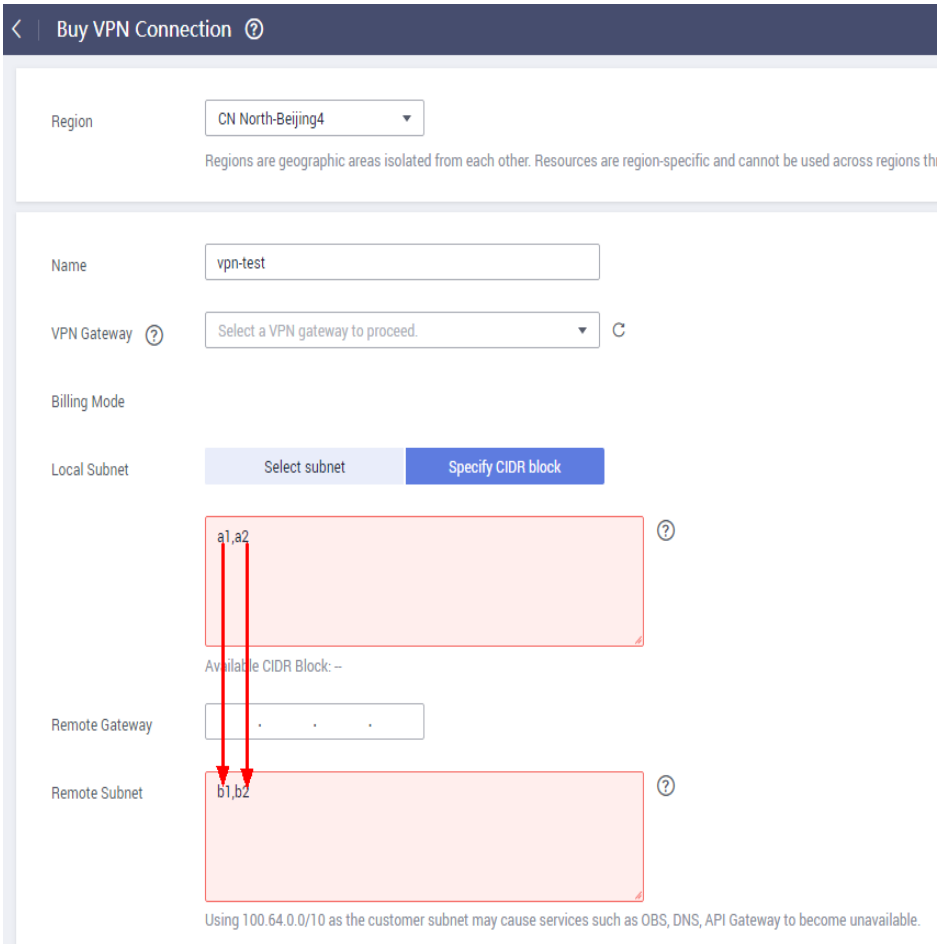
O número de conexões de VPN a serem criadas é determinado pelo número de data centers locais. Cada conexão de VPN pode conectar uma VPC a apenas um data center local.

Se você optar por comprar um gateway de VPN anual/mensal, defina o número de conexões de VPN com base no número de data centers locais a serem conectados.




**NOTA**

Na figura anterior, se as sub-redes a1 e a2 na Huawei Cloud precisarem se comunicar com as sub-redes b1 e b2 na rede local, você precisará criar apenas uma conexão de VPN, com os blocos CIDR de origem definidos como a1 e a2 e os blocos CIDR de destino definidos como b1 e b2. A figura a seguir apresenta um exemplo.



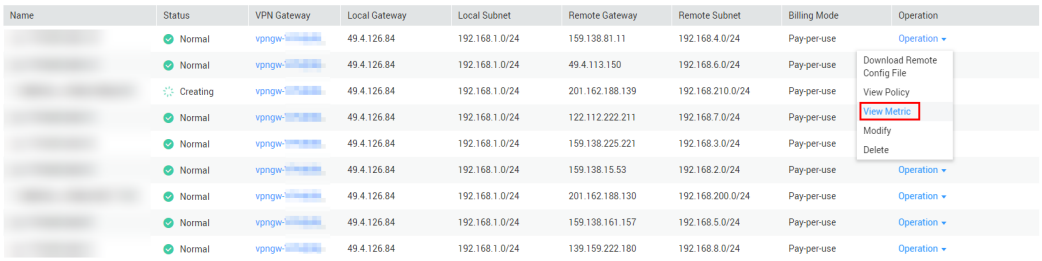

## 17.1.7 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme automaticamente para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Depois que uma conexão de VPN for criada, você poderá localizar a linha que contém a conexão de VPN e escolher **Operation** > **View Metric** para exibir o status da conexão de VPN.

**Figura 17-5** Ver métrica




## 17.1.8 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A chave é configurada em um gateway de VPN. Um túnel será estabelecido após a conclusão da negociação de VPN. Portanto, nomes de usuário e senhas não são necessários.

Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

**NOTA**

IPsec XAUTH é uma tecnologia estendida da VPN IPsec. Ele solicita que os usuários insiram seus nomes de usuário e senhas durante a negociação de VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

## 17.1.9 Quais são as diferenças entre os cenários de aplicação e os modos de conexão de VPNs IPsec e SSL?

### Cenários

VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

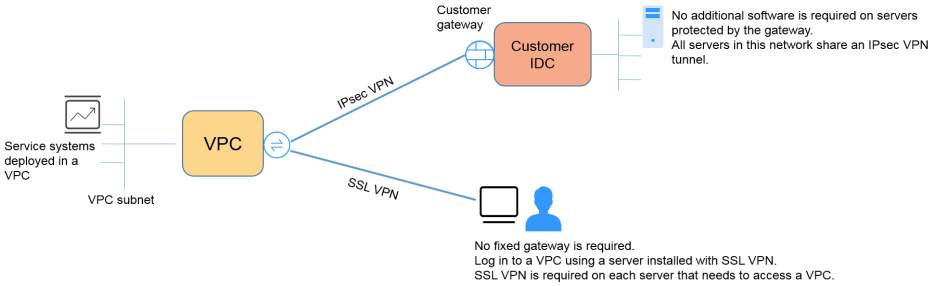
VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

### Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para concluir a negociação de VPN IPsec.

A VPN SSL precisa instalar um software cliente especificado no servidor e, em seguida, o servidor se conecta ao dispositivo SSL através do nome de usuário e senha.




NOTA

A Huawei Cloud suporta apenas VPNs IPsec.

## 17.1.10 Uma conexão de VPN IPsec será estabelecida automaticamente?

Depois de concluir as configurações em ambas as extremidades de uma conexão de VPN IPsec, a conexão de VPN não será estabelecida automaticamente somente após os fluxos de dados entre as duas extremidades da conexão. Se nenhum fluxo de dados entre a nuvem e o data center local, a conexão de VPN estará sempre no estado inativo. Quaisquer dados gerados pelo acesso a servidores ou pelo ping entre servidores podem acionar o estabelecimento de uma conexão de VPN.

O estabelecimento de uma conexão de VPN pode ser acionado em uma das duas condições a seguir: o gateway de VPN e o gateway remoto disparam automaticamente a negociação. Os servidores em nuvem e locais acedem uns aos outros através da conexão de VPN a estabelecer.

No entanto, o estabelecimento automático de uma conexão de VPN não pode ser acionado por um gateway de VPN na Huawei Cloud. Verifique se o estabelecimento de sua conexão de VPN pode ser acionado pelos fluxos de dados entre as duas extremidades da conexão de VPN. Ou seja, verifique se é possível estabelecer uma conexão de VPN depois de efetuar um ping a um servidor na nuvem a partir de um servidor no local e se é possível estabelecer uma conexão de VPN depois de desligar a conexão e efetuar um ping a um servidor no local a partir de um servidor na nuvem.

NOTA

Os endereços de origem e destino dos pacotes de ping devem ser protegidos pela VPN.

Antes que uma conexão de VPN seja estabelecida, os endereços IP do gateway em ambas as extremidades podem ser pingados. No entanto, o ping dos endereços IP do gateway não aciona o estabelecimento da conexão de VPN.

## 17.1.11 Quanto será cobrado pela criação de uma VPN? Será cobrado pelos endereços IP do gateway de VPN?

VPNs podem ser cobradas em uma base anual/mensal ou de pagamento por uso. Você precisa pagar pela largura de banda ou pelo preço do tráfego do gateway de VPN e pelo preço da conexão de VPN.

Os gateways de VPN podem ser cobrados por tráfego ou largura de banda.

- Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.
- O ciclo de faturamento do modo de cobrança de pagamento por uso é de 1 hora. Se você escolher um gateway de VPN de pagamento por uso, uma conexão de VPN deve ser adquirida juntamente com o gateway de VPN. O preço inclui a largura de banda do gateway de VPN ou o preço do tráfego e o preço da conexão de VPN criada junto com o gateway. Se você criar outra conexão para o gateway, será cobrado pela conexão adicional.

  NOTA

  - O endereço IP do gateway de VPN não será cobrado.
  - Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

## 17.1.12 Um endereço IP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Não. O endereço IP do gateway de VPN será liberado depois que o gateway de VPN for excluído.

A exclusão de um gateway de VPN também excluirá os recursos associados ao gateway.

AVISO

A exclusão da última conexão de um gateway de VPN pagamento por uso também excluirá o gateway. Se você quiser manter o endereço IP, não exclua a última conexão de VPN.

## 17.1.13 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As informações de largura de banda que podem ser monitoradas incluem tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as métricas do gateway de VPN, localize o gateway de VPN de destino e clique em **View Metric** na coluna **Operation**.

**Conexão de VPN**

O status da conexão de VPN pode ser monitorado.

O valor **1** indica que a conexão é normal.

O valor **0** indica que a conexão não está conectada.

Para exibir o status da conexão de VPN, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

# 17.1.14 Qual direção da largura de banda é limitada e qual é a unidade da largura de banda?

Sua largura de banda de gateway de VPN adquirida é usada na direção de saída. Para equilibrar o tráfego nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada.

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

# 17.1.15 Qual é a velocidade de rede real de uma conexão de VPN?

Uma conexão de VPN foi criada. Dois ECSs foram criados com um na extremidade local e outro na extremidade remota. Os dois ECSs podem fazer ping um ao outro.

**Execute as etapas a seguir para testar a velocidade da rede do gateway de VPN se a largura de banda do gateway de VPN for de 200 Mbit/s:**

1. Se os ECSs nas duas extremidades da VPN executarem o Windows, use iPerf3 e FileZilla (uma aplicação FTP gratuito para upload e download de arquivos) para testar a velocidade da rede.

   NOTA

   O teste mostra que a velocidade média da rede da VPN é de 180 Mbit/s, e há cerca de 10% de desvio de velocidade da rede. Os protocolos TCP e FTP têm o mecanismo de controle de congestionamento e o protocolo IPsec adiciona um novo cabeçalho de IP. Portanto, cerca de 10% de desvio de velocidade da rede é normal para a rede VPN.

   Figura 17-6 mostra o resultado do teste.

**Figura 17-6** Resultado do teste para largura de banda de 200 Mbit/s (cliente de iPerf3)

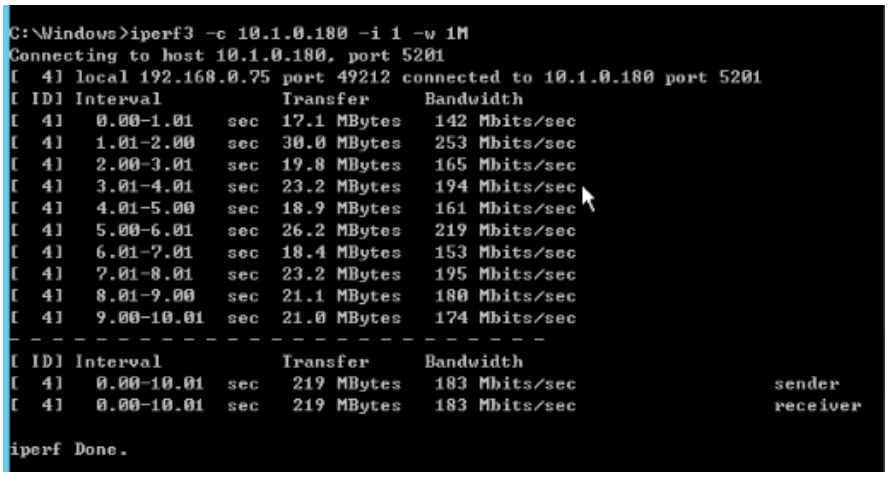
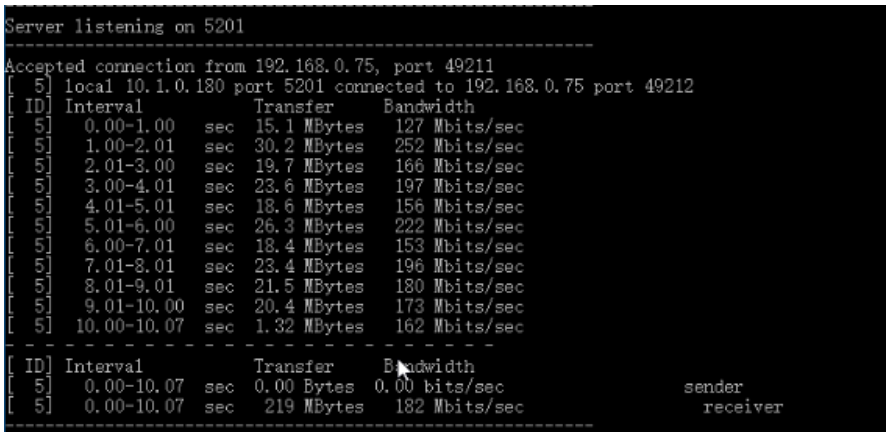



   Figura 17-7 mostra o resultado do teste.

**Figura 17-7** Resultado do teste para largura de banda de 200 Mbit/s (servidor de iPerf3)

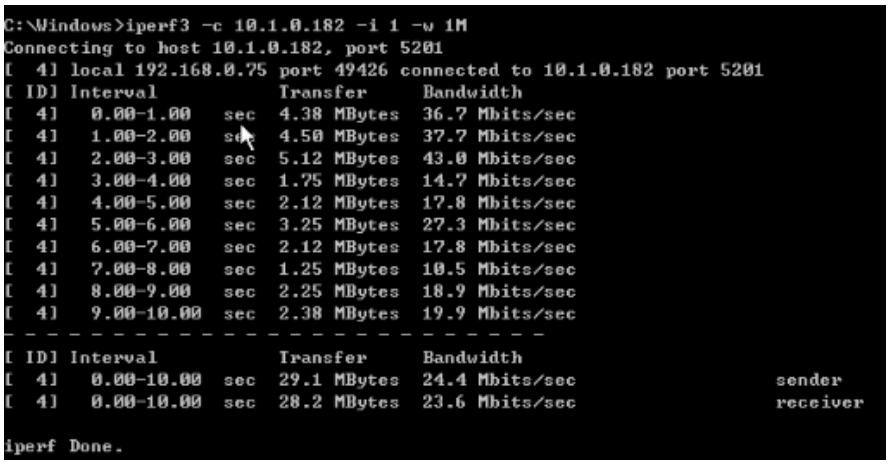



2. Se os ECSs nas duas extremidades da VPN executarem o CentOS 7, use o iPerf3 para testar a velocidade da rede. A velocidade da rede pode chegar a 180 Mbit/s.
3. Se o ECS estiver funcionando como o servidor executar o CentOS 7 e o cliente executar o Windows, use iPerf3 e FileZilla para testar a velocidade da rede.

   A velocidade da rede é de cerca de 20 Mbit/s, uma velocidade de rede lenta. Isso porque as implementações de TCP no Windows e no Linux são diferentes. Portanto, se os ECSs nas duas extremidades da VPN executarem sistemas operacionais diferentes, a velocidade da rede de VPN não atenderá aos requisitos de largura de banda.

   **Figura 17-8** mostra o resultado do teste.

**Figura 17-8** Resultado do teste quando os ECSs nas duas extremidades executam sistemas operacionais diferentes (iPerf3)




**Execute as etapas a seguir para testar a velocidade da rede do gateway de VPN se a largura de banda do gateway de VPN for de 1.000 Mbit/s:**

A largura de banda do gateway de VPN é compartilhada por todas as suas conexões de VPN. Se o tamanho da largura de banda for grande, vários ECSs serão necessários para testar a largura de banda do gateway de VPN porque o desempenho de encaminhamento de um ECS é limitado. Esse cenário tem altos requisitos nas especificações do ECS. Os ECSs devem ter NICs que suportem a largura de banda de 2 Gbit/s ou mais.

**Os testes mostram que a velocidade de rede real de um gateway de VPN na Huawei Cloud está dentro da faixa normal. No entanto, os servidores usados em ambas as**

**extremidades da conexão de VPN devem executar os sistemas operacionais do mesmo tipo e as NICs do servidor devem atender aos requisitos de configuração.**

## 17.1.16 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

## 17.1.17 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter apenas um gateway de VPN, enquanto um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

  NOTA

  O número de conexões de VPN é irrelevante para o número de sub-redes locais ou o número de sub-redes remotas. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

## 17.1.18 O que é um gateway remoto e uma sub-rede remota em uma conexão de VPN?

Ao criar uma conexão de VPN, uma sub-rede na VPC da Huawei Cloud é a sub-rede local e o gateway de VPN criado é o gateway local. A sub-rede e o gateway conectados no data center local são a sub-rede remota e o gateway remoto.

Um endereço IP de gateway remoto é um endereço IP público.

## 17.1.19 Quantas conexões de VPN são necessárias para me conectar a vários servidores locais?

A VPN IPsec da Huawei Cloud conecta uma VPC na nuvem e seu data center local. Portanto, o número de conexões de VPN é irrelevante para o número de servidores, mas para o número de data centers onde os servidores estão localizados.

Na maioria dos casos, um data center local tem um gateway público. Todos os servidores se conectam à Internet através deste gateway. Portanto, você só precisa configurar uma conexão de VPN para permitir comunicações entre a VPC da Huawei Cloud e seu data center local.

## 17.1.20 Uma VPN permite comunicações entre as duas VPC?

- Se as duas VPCs estiverem implementadas na mesma região, use uma conexão de emparelhamento de VPC para conectá-las.
- Se as duas VPCs forem implementadas em regiões diferentes, use uma conexão de VPN para conectá-las. As operações detalhadas são as seguintes:
  a. Crie um gateway de VPN para cada VPC e crie conexões de VPN para os dois gateways de VPN.
  b. Defina o endereço do gateway remoto de cada conexão de VPN para o endereço IP do gateway do lado do par.
  c. Defina as sub-redes remotas de cada conexão de VPN para as sub-redes da VPC de mesmo nível.
  d. As chaves pré-compartilhadas e os parâmetros do algoritmo das duas conexões de VPN devem ser os mesmos.

## 17.1.21 Quais são os impactos de uma VPN em uma rede local? Quais são as mudanças na rota para acessar um ECS?

Quando configurar uma VPN, execute as seguintes operações no gateway no local:

1. Configure políticas de IKE e IPsec.
2. Especifique o tráfego interessante (regras de ACL).
3. Verifique a rota do gateway local para garantir que o tráfego destinado à VPC da Huawei Cloud seja roteado para a interface de saída correta (a interface com a política de IPsec vinculada).

Após a conclusão da configuração de VPN, somente o tráfego correspondente às regras de ACL entra no túnel de VPN.

Por exemplo, antes de uma VPN ser criada, os usuários locais acessam o ECS por meio do EIP vinculado ao ECS. Depois que a VPN é criada, os fluxos de dados correspondentes às regras de ACL acessam o endereço IP privado do ECS por meio do túnel de VPN.

## 17.1.22 Posso usar uma rede com duas saídas para estabelecer duas conexões de VPN com a mesma VPC?

Não.

Ao criar uma VPN na nuvem, uma sub-rede local é uma sub-rede de VPC e uma sub-rede remota é uma sub-rede local. Se as duas conexões usarem a mesma sub-rede local e sub-rede remota, as conexões de VPN falharão.

## 17.1.23 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- ACLs dos dispositivos em ambas as extremidades da conexão de VPN não coincidem.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são diferentes.
- A DPD não está configurada no data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Os pacotes são fragmentados porque o tamanho dos dados excede a MTU.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- As sub-redes locais e remotas são pares correspondentes.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- A DPD está ativada no dispositivo de gateway local e o número de vezes de detecção é 5 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do gateway local é grande o suficiente para ser usada pela conexão de VPN.
- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.
- Faça ping nas sub-redes em ambas as extremidades continuamente. O script é o seguinte:

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Use o editor vi para copiar o script anterior para o arquivo **ping.sh**.
2. Execute o comando **chmod 777 ping.sh** para conceder permissões ao arquivo.
3. Execute o comando ping:

   **./ping.sh** *x.x.x.x* **>>/dev/null &**

   *x.x.x.x* indica o endereço IP a ser pingado.
4. Execute o seguinte comando:

   **tail -f** *x.x.x.x***.log**

   Você pode ver o resultado do ping em tempo real.

## 17.1.24 Por que Not Connected exibido como o status de uma conexão de VPN criada com êxito?

Depois que uma conexão de VPN é criada, seu status muda para **Normal** somente depois que os servidores em ambas as extremidades da conexão de VPN se comunicam uns com os outros.

- IKE v1:

  Se nenhum tráfego passar pela conexão de VPN por um período de tempo, a conexão de VPN precisa ser renegociada. O tempo de negociação depende do valor do **Lifecycle (s)** na política de IPsec. Geralmente, **Lifecycle (s)** é definido como **3600** (1 hora), indicando que a negociação será iniciada no quinquagésimo quarto minuto. Se a negociação for bem-sucedida, a conexão permanece para a próxima rodada de negociação. Se a negociação falhar, o status da conexão de VPN será alterado para **Not Connected** dentro de uma hora. A conexão pode ser restaurada somente após as duas extremidades da conexão de VPN se comunicarem uma com a outra. A desconexão pode ser evitada usando uma ferramenta de monitoramento de rede, como IP SLA, para gerar pacotes.
- IKE v2: se nenhum tráfego passar pela conexão de VPN por um período de tempo, a conexão de VPN permanecerá no status conectado.

## 17.1.25 O que fazer se a configuração da conexão de VPN falhar?

1. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.

   a. Se a política de IKE tiver sido configurada durante a primeira fase e a política de IPsec não tiver sido ativada na segunda fase, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.

   b. Se você usa um dispositivo físico de Cisco em seu data center local, recomenda-se que você use MD5 e defina **Authentication Mode** como **MD5** ao configurar a política de IPsec para a conexão de VPN na nuvem.

2. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   ```

3. Verifique se a conexão de VPN está normal pingando a extremidade local a partir da extremidade remota e pingando a extremidade remota a partir da extremidade local.

## 17.1.26 Um EIP pode ser usado como um endereço IP de gateway de VPN?

Sim para VPN, mas não para a Classic VPN.

## 17.1.27 Por que a conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

Certifique-se de que as chaves pré-compartilhadas e as informações de negociação em ambas as extremidades sejam consistentes. As sub-redes locais e o gateway de VPN na nuvem são as sub-redes remotas e o gateway remoto no data center local. O gateway remoto e as sub-redes remotas na nuvem são o gateway local e as sub-redes locais no data center local.

Certifique-se de que as regras de rotas, NAT e política de segurança estão corretamente configuradas no dispositivo de gateway local. Em seguida, faça ping nos servidores em sub-redes em ambas as extremidades.

NOTA

A VPN é acionada com base em fluxos de dados. Depois que você configura a VPN, sibile um dispositivo na sub-rede do par. Antes de executar o comando ping, desabilite a função de firewall no dispositivo e permita pacotes ICMP de entrada no grupo de segurança na nuvem.

O ping do endereço IP do gateway não pode acionar a negociação de VPN. Efetue o ping do servidor na sub-rede protegida pelo gateway.

## 17.1.28 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa criar regras de ACL dedicadas para seu dispositivo de gateway local. As regras da ACL serão referenciadas pelas políticas de IPsec.

Quando você configura a VPN na nuvem, as regras da ACL serão geradas automaticamente com base nas sub-redes locais e remotas inseridas no console de gerenciamento e, em seguida, entregues ao gateway de VPN.

(Huawei Cloud) O número de regras da ACL = o número de sub-redes locais x o número de sub-redes remotas

# 17.2 Consulta de produto

## 17.2.1 Quais são os cenários típicos da VPN IPsec?

Uma VPN é uma conexão ponto a ponto que implementa o acesso à rede privada entre dois pontos.

- Cenários aplicáveis:
  - Crie uma VPN é criada entre diferentes regiões da Huawei Cloud para permitir comunicações de VPC entre regiões.
  - Crie uma VPN entre a Huawei Cloud e outra nuvem, por exemplo, a Alibaba Cloud.
  - Crie uma VPN entre a Huawei Cloud e seu data center local para permitir a comunicação entre uma VPC da Huawei Cloud e uma rede local.
  - VPN HUB é usado em conjunto com conexões de emparelhamento VPC e conexões Cloud Connect para permitir a comunicação entre um data center local e várias VPCs na nuvem.

  - A VPN funciona com a SNAT para acessar endereços IP específicos em nuvens.
- Cenários não aplicáveis:
  - Não use VPN para conectar VPCs na mesma região da Huawei Cloud. É recomendável usar conexões de emparelhamento de VPC para permitir comunicações entre VPCs na mesma região.
  - Não estabeleça conexões de VPN entre a Huawei Cloud e a sua rede doméstica que utilize a discagem PPPoE.
  - Não estabeleça conexões de VPN entre a Huawei Cloud e roteadores (4G ou 5G).
  - Não estabeleça conexões de VPN entre a Huawei Cloud e terminais pessoais.

## 17.2.2 O que é uma VPC, um gateway de VPN e uma conexão de VPN?

As VPCs permitem você criar redes virtuais isoladas e privadas. Você pode usar a VPN para acessar ECSs com segurança em VPCs.

Um gateway de VPN é um gateway de saída para uma VPC. Com um gateway de VPN, você pode criar uma conexão segura, confiável e criptografada entre uma VPC e um data center local ou entre duas VPCs em diferentes regiões.

Uma conexão de VPN é um túnel de comunicação IPsec criptografado seguro e confiável estabelecido entre um gateway de VPN e o gateway remoto num data center local.

Para criar uma VPN na nuvem, execute as seguintes operações:

1. Criar um gateway de VPN Você precisa especificar a VPC a ser conectada, bem como a largura de banda e os EIPs do gateway de VPN.
2. Criar uma conexão de VPN Você precisa especificar o EIP do gateway usado para se conectar ao gateway remoto, às sub-redes e às políticas de negociação.

## 17.2.3 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter apenas um gateway de VPN, enquanto um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

  NOTA

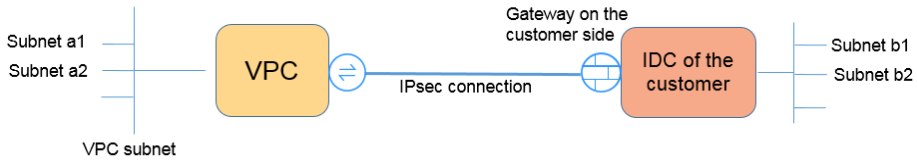
  O número de conexões de VPN é irrelevante para o número de sub-redes locais ou o número de sub-redes remotas. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

# 17.2.4 O que é uma conexão de VPN? Como definir o número de conexões de VPN ao comprar um gateway de VPN?

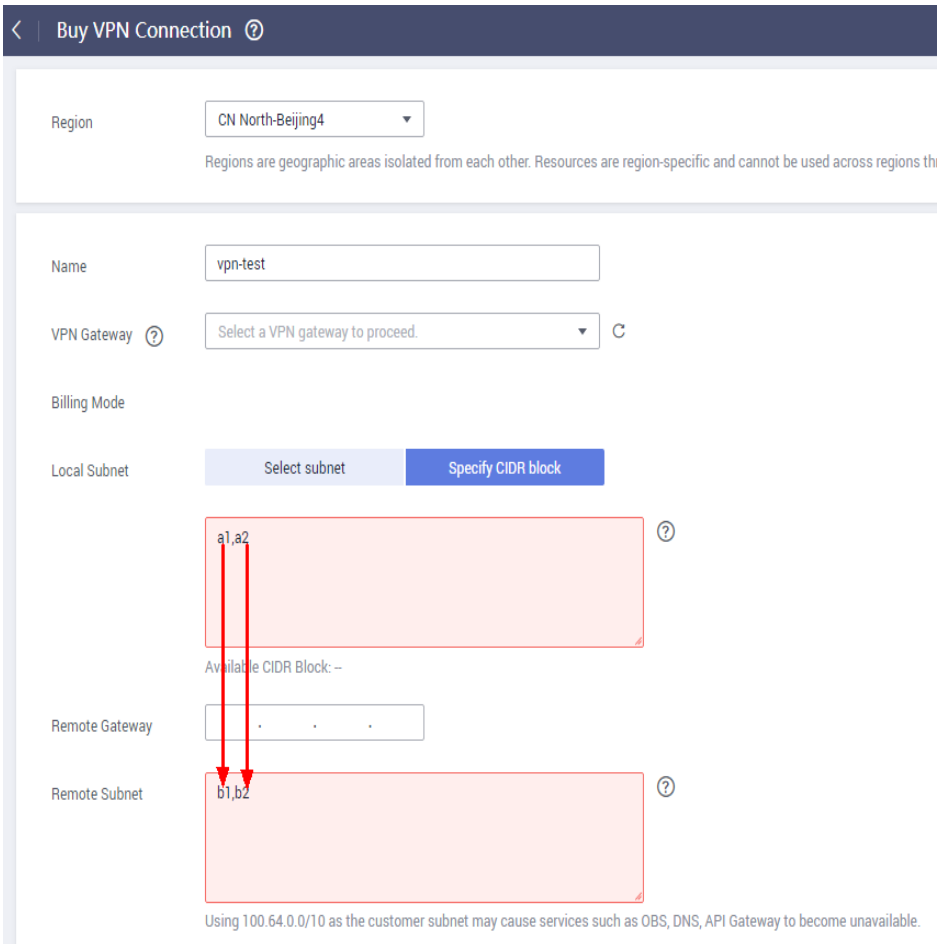
Uma conexão de VPN da Huawei Cloud é uma conexão IPsec estabelecida entre um gateway de VPN na nuvem e um endereço IP público independente de um data center local. Você pode configurar várias sub-redes locais (sub-redes da VPC) e sub-redes remotas (sub-redes locais) para uma conexão de VPN.

O número de conexões de VPN a serem criadas é determinado pelo número de data centers locais. Cada conexão de VPN pode conectar uma VPC a apenas um data center local.




**NOTA**

Na figura anterior, se as sub-redes a1 e a2 na Huawei Cloud precisarem se comunicar com as sub-redes b1 e b2 na rede local, você precisará criar apenas uma conexão de VPN, com os blocos CIDR de origem definidos como a1 e a2 e os blocos CIDR de destino definidos como b1 e b2. A figura a seguir apresenta um exemplo.



## 17.2.5 O que é um gateway remoto e uma sub-rede remota em uma conexão de VPN?

Ao criar uma conexão de VPN, uma sub-rede na VPC da Huawei Cloud é a sub-rede local e o gateway de VPN criado é o gateway local. A sub-rede e o gateway conectados no data center local são a sub-rede remota e o gateway remoto.

Um endereço IP de gateway remoto é um endereço IP público.

## 17.2.6 Como planejar o bloco CIDR de uma VPC acessada por uma conexão de VPN?

- O bloco CIDR da VPC não pode entrar em conflito com o bloco CIDR local.
- Para evitar conflitos com endereços de serviço de nuvem, não use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3 ou 100.64.0.0/10 para sua rede local.

## 17.2.7 Uma conexão de VPN IPsec será estabelecida automaticamente?

Depois de concluir as configurações em ambas as extremidades de uma conexão de VPN IPsec, a conexão de VPN não será estabelecida automaticamente somente após os fluxos de dados entre as duas extremidades da conexão. Se nenhum fluxo de dados entre a nuvem e o data center local, a conexão de VPN estará sempre no estado inativo. Quaisquer dados gerados pelo acesso a servidores ou pelo ping entre servidores podem acionar o estabelecimento de uma conexão de VPN.

O estabelecimento de uma conexão de VPN pode ser acionado em uma das duas condições a seguir: o gateway de VPN e o gateway remoto disparam automaticamente a negociação. Os servidores em nuvem e locais acedem uns aos outros através da conexão de VPN a estabelecer.

No entanto, o estabelecimento automático de uma conexão de VPN não pode ser acionado por um gateway de VPN na Huawei Cloud. Verifique se o estabelecimento de sua conexão de VPN pode ser acionado pelos fluxos de dados entre as duas extremidades da conexão de VPN. Ou seja, verifique se é possível estabelecer uma conexão de VPN depois de efetuar um ping a um servidor na nuvem a partir de um servidor no local e se é possível estabelecer uma conexão de VPN depois de desligar a conexão e efetuar um ping a um servidor no local a partir de um servidor na nuvem.

NOTA

Os endereços de origem e destino dos pacotes de ping devem ser protegidos pela VPN.

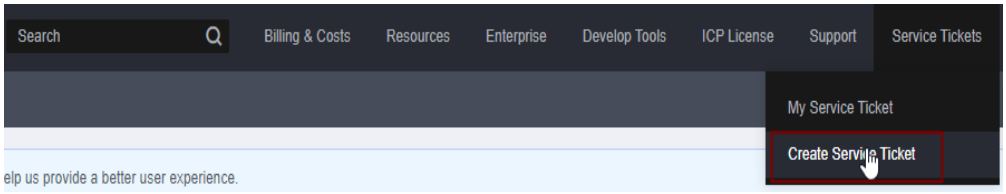
Antes que uma conexão de VPN seja estabelecida, os endereços IP do gateway em ambas as extremidades podem ser pingados. No entanto, o ping dos endereços IP do gateway não aciona o estabelecimento da conexão de VPN.

## 17.2.8 Quais são as categorias de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

1. Faça logon no console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

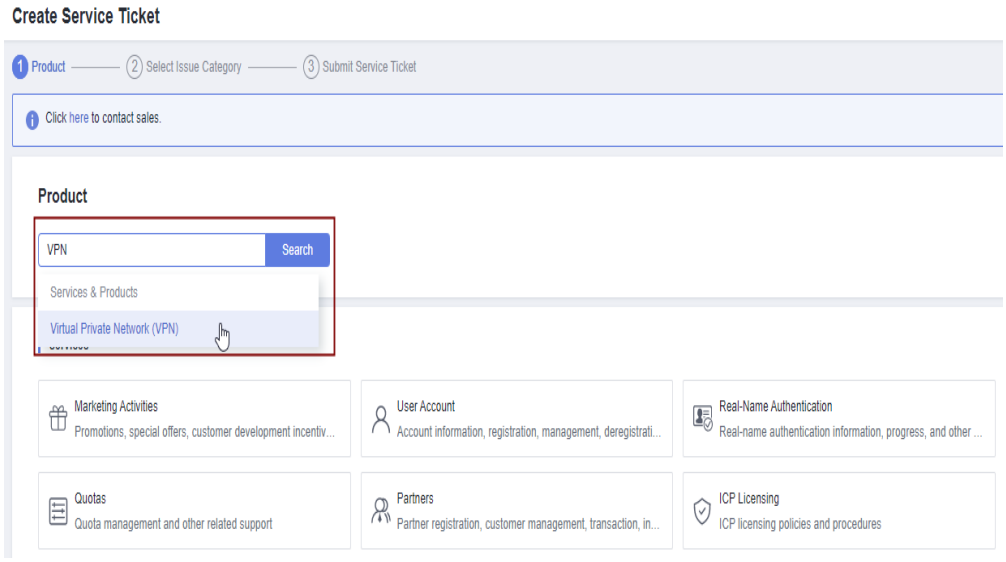
  

**Figura 17-9** Criar tíquete de serviço




3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 17-10** Selecionar **Virtual Private Network (VPN)**




4. Selecione uma categoria de problema.

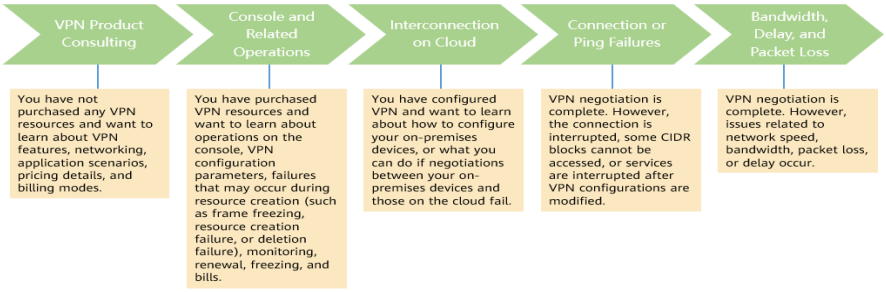
**Figura 17-11** Selecionar categoria de problema

NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 17-12** Categoria de emissão e base de classificação




## 17.2.9 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 17-2** Parâmetros de negociação de VPN

| Política | Parâmetro | Valor |
| --- | --- | --- |
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256<br>● AES-192<br>● AES-128 (valor padrão) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | Algoritmo DH | ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 15<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21<br>**NOTA**<br>Em algumas regiões, apenas **Group 14**, **Group 2** e **Group 5** estão disponíveis. |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Lifecycle (s) | **86400** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | PFS | ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor predefinido)<br>● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 15<br>● DH group 16<br>● DH group 19<br>● DH group 20<br>● DH group 21<br>● Disable<br>**NOTA**<br>Em algumas regiões, apenas **DH group 14**, **DH group 2** e **DH group 5** estão disponíveis. |
| | Transfer Protocol | ● ESP (valor predefinido)<br>● AH<br>● AH-ESP |
| | Lifecycle (s) | **3600** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **480** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Depois que o PFS for configurado, uma troca de DH adicional será executada durante a negociação da AS do IPsec e uma nova chave da AS do IPsec será gerada, melhorando a segurança da AS do IPsec.
- Para garantir a segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no gateway local. Caso contrário, a negociação falhará.
- Para habilitar o PFS, certifique-se de que as configurações em ambas as extremidades de uma VPN sejam as mesmas.
- O tempo de vida baseado em tráfego da AS do IPsec na VPN da Huawei Cloud é padrão para 1.843.200 KB e não pode ser alterado. Esse tempo de vida não afeta o estabelecimento de uma AS de IPsec.

# 17.2.10 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud suporta o protocolo IPsec padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implementado atrás de um gateway NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores domésticos comuns de banda larga, hosts de Windows que fornecem serviços VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os seguintes produtos podem se conectar à Huawei Cloud por meio de VPNs:
  - Dispositivos: firewalls e roteadores de acesso (ARs) da Huawei, firewalls de Hillstone e firewalls de Check Point
  - Serviços em nuvem: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) e Microsoft Azure
  - Software: StrongSwan
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- No entanto, alguns dispositivos suportam VPN IPsec somente após de comprar as licenças de software necessárias.

  Entre em contato com o administrador do data center local para confirmar o modelo do dispositivo com o fornecedor.

# 17.2.11 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A chave é configurada em um gateway de VPN. Um túnel será estabelecido após a conclusão da negociação de VPN. Portanto, nomes de usuário e senhas não são necessários.

Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

IPsec XAUTH é uma tecnologia estendida da VPN IPsec. Ele solicita que os usuários insiram seus nomes de usuário e senhas durante a negociação de VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

## 17.2.12 Como permitir que servidores específicos acessem uma sub-rede da VPC por meio de uma conexão de VPN criada?

Configurações no data center local

- Configure regras de negação em dispositivos de VPN.
- Configure regras de ACL no roteador ou no comutador.

Configurações na nuvem

- Configure regras de grupo de segurança para negar acesso a endereços IP específicos.
- Configure regras de ACL.

NOTA

Todas as regras devem ser adicionadas ao dispositivo antes que o túnel de VPN seja estabelecido. Não altere a sub-rede local e a sub-rede remota para restringir o acesso.

## 17.2.13 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As informações de largura de banda que podem ser monitoradas incluem tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as métricas do gateway de VPN, localize o gateway de VPN de destino e clique em **View Metric** na coluna **Operation**.

**Conexão de VPN**

O status da conexão de VPN pode ser monitorado.

O valor **1** indica que a conexão é normal.

O valor **0** indica que a conexão não está conectada.

Para exibir o status da conexão de VPN, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

## 17.2.14 Um EIP pode ser usado como um endereço IP de gateway de VPN?

Não.

O endereço IP de um gateway de VPN é de configurações predefinidas e é atribuído automaticamente quando o gateway de VPN é criado. Um EIP não pode ser usado por um gateway de VPN.

## 17.2.15 Preciso comprar EIPs para servidores que se comunicam uns com os outros por meio de uma VPN?

Se o servidor local precisar acessar um ECS na nuvem por meio de uma VPN, você não precisará adquirir um EIP.

Se o ECS precisar fornecer serviços acessíveis pela Internet, será necessário um EIP.

## 17.2.16 As VPNs SSL são suportadas?

VPNs SSL não são suportadas.

## 17.2.17 Quanto tempo demora para que as configurações de VPN entregues entrem em vigor?

Leva de 1 a 5 minutos para que as configurações de VPN entrem em vigor.

NOTA

Depois que as configurações de VPN entrarem em vigor, configure seu gateway local para concluir a negociação do túnel com o gateway de VPN na Huawei Cloud.

## 17.2.18 O que fazer se não conseguir criar conexões para um gateway de VPN que não tenha informações de largura de banda?

Se um gateway de VPN não tiver informações de largura de banda, a VPN é da edição anterior. Esse tipo de VPN não pode mais ser criado na Huawei Cloud.

- Apenas uma conexão de VPN pode ser criada para cada gateway de VPN da edição anterior e sua largura de banda não é garantida. Você pode excluir o gateway e criar um da nova edição. Mas os serviços serão afetados.
- Você também pode **enviar um tíquete de serviço** para alterar o gateway para uma das novas edições e seus serviços não serão afetados.

  Por padrão, a largura de banda de um gateway de VPN alterado para a nova edição é de 10 Mbit/s. Você pode ajustar a largura de banda conforme necessário. A largura de banda de um gateway de VPN que é cobrado anualmente/mensalmente não pode ser reduzida.

## 17.2.19 A VPN da Huawei Cloud oferece suporte a endereços IPv6?

Não.

A VPN da Huawei Cloud suporta apenas endereços IPv4.

## 17.2.20 Como determinar o tamanho da largura de banda da minha VPN?

Considere o seguinte ao determinar a largura de banda:

- Quantidade de dados transmitidos por um túnel de VPN em um período de tempo (Reserve largura de banda suficiente para evitar o congestionamento do link.)
- A largura de banda de saída no final da conexão de VPN na nuvem deve ser menor do que no final da conexão de VPN no data center local.

## 17.2.21 Uma conexão de VPN suporta algoritmos de criptografia chineses?

Não.

Use os algoritmos fornecidos no console de gerenciamento da Huawei Cloud para negociação. Certifique-se de que os algoritmos usados em ambas as extremidades sejam os mesmos.

# 17.2.22 Qual versão do IKE devo selecionar ao criar uma conexão de VPN?

A Huawei Cloud recomenda o IKEv2 para negociação porque o IKEv1 não é seguro. Além, IKEv2 executa melhor do que IKEv1 em termos da negociação da conexão e do estabelecimento, métodos de autenticação, tempo limite de DPD e tempo limite de AS.

A Huawei Cloud não suportará o IKEv1 em breve.

## Introdução ao IKEv1 e IKEv2

- A complexidade do IKEV1, um protocolo híbrido, inevitavelmente traz alguns defeitos de segurança e desempenho. Isso se tornou o gargalo para o atual sistema de IPsec.
- O protocolo IKEv2 reserva funções básicas do IKEv1 e supera alguns problemas trazidos pelo IKEv1. Além disso, para a simplicidade, eficiência, segurança e robustez, RFC 4306, um documento descreve a versão 2 do IKE, combina o conteúdo do que eram anteriormente separados documentos de IKEv1. Ao minimizar as funções principais e os algoritmos de senha padrão, o IKEv2 melhora muito a interoperabilidade entre diferentes VPNs IPsec.

## Vulnerabilidades de segurança de IKEv1

- Os algoritmos criptográficos suportados pelo IKEv1 não foram atualizados por mais de 10 anos. Além disso, o IKEv1 não oferece suporte a algoritmos criptográficos fortes, como AES-GCM e ChaCha20-Poly1305. Para IKEv1, o bit E (criptografia) no cabeçalho ISALMP especifica que as cargas úteis seguintes ao cabeçalho ISALMP são criptografadas, mas qualquer verificação de integridade de dados dessas cargas úteis é tratada por uma carga útil hash separada. Essa separação entre criptografia e proteção de integridade de dados impede o uso de criptografia autenticada (AES-GCM) com o IKEv1.
- O protocolo IKEv1 é vulnerável a ataques de amplificação de DoS. O IKEv1 é vulnerável a conexões semi-abertas.

  O IKEv2 pode se defender contra ataques DoS.
- O modo agressivo de IKEv1 não é suficientemente seguro. No modo agressivo, os pacotes de informações não são criptografados. Há também ataques de força bruta visando o modo agressivo, como ataques man-in-the-middle.

## Diferenças entre IKEv1 e IKEv2

- **Processo de negociação**
  - Negociação de AS de IKEv1 consiste em duas fases. O IKEv1 é complexo e consome uma grande quantidade de largura de banda. A negociação da fase 1 do IKEv1 visa estabelecer a AS de IKE. Este processo suporta o modo principal e o modo agressivo. O modo principal usa seis mensagens ISAKMP para estabelecer a AS de IKE, mas o modo agressivo usa apenas três. Portanto, o modo agressivo é mais rápido no estabelecimento da AS de IKE. No entanto, o modo agressivo não fornece proteção de identidade de par porque a troca de chaves e a autenticação de identidade são realizadas ao mesmo tempo. A negociação da fase 2 do IKEv1 visa configurar a AS do IPsec para transmissão de dados. Esse processo usa o modo de troca rápida (3 mensagens de ISAKMP) para concluir a negociação.

- Comparado com o IKEv1, o IKEv2 simplifica o processo de negociação de AS. O IKEv2 usa duas trocas (um total de 4 mensagens) para criar uma AS de IKE e um par de ASs de IPsec. Para criar vários pares de ASs de IPsec, apenas uma troca adicional é necessária para cada par adicional de ASs.

  NOTA

  Para a negociação de IKEv1, seu modo principal requer nove (6+3) pacotes no total e seu modo agressivo requer 6 (3+3) pacotes. A negociação de IKEv2 exige somente 4 (2+2) pacotes.

- **Métodos de autenticação**
  - Somente o IKEv1 (que exige um cartão de criptografia) suporta autenticação de envelope digital (HSS-DE).
  - O IKEv2 oferece suporte à autenticação EAP (Extensible Authentication Protocol). O IKEv2 pode usar um servidor AAA para autenticar remotamente usuários de dispositivos móveis e de PC e atribuir endereços IP privados a esses usuários. O IKEv1 não fornece essa função e deve usar o L2TP para atribuir endereços IP privados.
  - Apenas o IKEv2 suporta algoritmos de integridade de AS de IKE.
- **Tempo limite de DPD**
  - Somente o IKEv1 suporta o parâmetro **retry-interval**. Se um dispositivo envia um pacote de DPD, mas não recebe nenhuma resposta dentro do intervalo de repetição especificado, o dispositivo grava um evento de falha de DPD. Quando o número de eventos de falha de DPD atinge 5, ambas ASs de IKE e de IPsec são excluídas. A negociação de AS de IKE será iniciada novamente quando o dispositivo tiver tráfego IPsec para lidar.
  - No modo de IKEv2, o intervalo de retransmissão aumenta de 1, 2, 4, 8, 16, 32 para 64, em segundos. Se nenhuma resposta for recebida dentro de oito transmissões consecutivas, a extremidade do par será considerada inativa e as ASs de IKE e de IPsec serão excluídas.
- **Processamento de tempo limite da AS de IKE e processamento de tempo limite da AS de IPsec**

  No IKEv2, a vida útil da AS de IKE é 9/10 da vida útil da AS de IKE mais ou menos um valor aleatório para reduzir a probabilidade de que duas extremidades iniciem a renegociação ao mesmo tempo. Portanto, a vida útil do soft não requer configurações manuais no IKEv2.

## Vantagens do IKEv2 em relação ao IKEv1

- Processo de negociação de AS simplificado e eficiência de negociação aprimorada.
- Fechou muitas brechas criptográficas, melhorando a segurança.
- Suporta autenticação EAP, melhorando a flexibilidade e escalabilidade da autenticação.
- O EAP é um protocolo de autenticação que suporta vários métodos de autenticação. A maior vantagem de EAP é a escalabilidade. Ou seja, novos modos de autenticação podem ser adicionados sem alterar o sistema de autenticação original. A autenticação EAP tem sido amplamente utilizada em redes de acesso de discagem.
- O IKEv2 emprega uma carga útil criptografada baseada no projeto do ESP. A carga útil criptografada de IKEv2 associa criptografia e proteção de integridade de dados de uma forma que torna possível o uso de algoritmos de criptografia autenticados. O AES-GCM garante confidencialidade, integridade e autenticação.

## 17.2.23 Quais são os bits dos grupos DH usados pela VPN da Huawei Cloud?

Os grupos Diffie-Hellman (DH) determinam a força da chave usada no processo de troca de chaves. Números de grupo DH mais altos são geralmente mais seguros, mas é necessário tempo extra para calcular a chave.

**Tabela 17-3** lista os bits correspondentes aos grupos de DH usados pela VPN.

**Tabela 17-3** Bit correspondente a cada grupo DH

| Grupo DH | Módulo |
| --- | --- |
| 1 | 768 bits |
| 2 | 1024 bits |
| 5 | 1536 bits |
| 14 | 2048 bits |
| 15 | 3072 bits |
| 16 | 4096 bits |
| 19 | ecp256 bits |
| 20 | ecp384 bits |
| 21 | ecp521 bits |

NOTA

Os seguintes algoritmos de DH têm riscos de segurança e não são recomendados: DH group 1, DH group 2 e DH group 5.

## 17.2.24 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

## 17.2.25 Posso implementar aplicações na nuvem, bancos de dados em um data center local e depois conectá-las por meio de uma VPN?

VPN conecta uma VPC e uma rede local.

Depois que a VPN é configurada com sucesso, a VPC e a rede local podem se comunicar entre si. Nesse caso, o servidor de aplicações que acessa o banco de dados é o mesmo que acessar outros servidores na mesma LAN.

Servidores de nuvem e servidores locais podem se comunicar uns com os outros.

**AVISO**

- Depois que uma VPN é configurada, verifique se a latência da rede e a perda de pacotes afetam negativamente a execução do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

# 17.2.26 Quais são as diferenças entre os cenários de aplicação e os modos de conexão de VPNs IPsec e SSL?

## Cenários

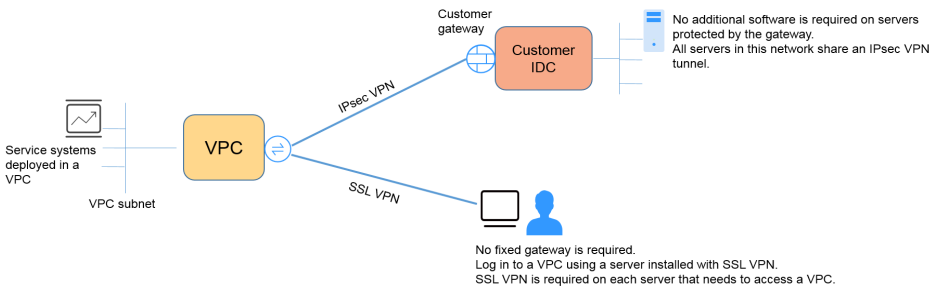
VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

## Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para concluir a negociação de VPN IPsec.

VPN SSL precisa instalar um software cliente especificado no servidor e, em seguida, o servidor se conecta ao dispositivo SSL através do nome de usuário e senha.




**NOTA**

A Huawei Cloud suporta apenas VPNs IPsec.

# 17.2.27 Quanto será cobrado pela criação de uma VPN? Será cobrado pelos endereços IP do gateway de VPN?

VPNs podem ser cobradas em uma base anual/mensal ou de pagamento por uso. Você precisa pagar pela largura de banda ou pelo preço do tráfego do gateway de VPN e pelo preço da conexão de VPN.

Os gateways de VPN podem ser cobrados por tráfego ou largura de banda.

1. Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.
2. O ciclo de faturamento do modo de cobrança de pagamento por uso é de 1 hora. Se você escolher um gateway de VPN de pagamento por uso, uma conexão de VPN deve ser adquirida juntamente com o gateway de VPN. O preço inclui a largura de banda do gateway de VPN ou o preço do tráfego e o preço da conexão de VPN criada junto com o gateway. Se você criar outra conexão para o gateway, será cobrado pela conexão adicional.

   NOTA

   - O endereço IP do gateway de VPN não será cobrado.
   - Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

## 17.2.28 Qual é a diferença entre a cobrança de um gateway de VPN por largura de banda e por tráfego?

Um gateway de VPN pagamento por uso pode ser cobrado por largura de banda ou por tráfego.

As suas diferenças são as seguintes:

- Cobrança por largura de banda: o ciclo de faturamento é de uma hora. A taxa gerada depende do tamanho da largura de banda.
- Cobrança por tráfego: as taxas de trânsito geradas a cada hora serão cobradas. A cobrança é baseada no tráfego gerado saindo de uma VPC. O tamanho da largura de banda não afeta o preço do tráfego público por GB.

## 17.2.29 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

## 17.2.30 Um endereço IP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Não. O endereço IP do gateway de VPN será liberado depois que o gateway de VPN for excluído.

A exclusão de um gateway de VPN também excluirá os recursos vinculados ao gateway.

AVISO

A exclusão da última conexão de um gateway de VPN pagamento por uso também excluirá o gateway. Se você quiser manter o endereço IP, não exclua a última conexão de VPN.

## 17.2.31 Preciso comprar EIPs para servidores que se comunicam uns com os outros por meio de uma VPN?

Se o servidor local precisar acessar um ECS na nuvem por meio de uma VPN, você não precisará adquirir um EIP.

Se o ECS precisar fornecer serviços acessíveis pela Internet, será necessário um EIP.

## 17.2.32 Onde posso adicionar rotas no console da VPN para alcançar as sub-redes remotas?

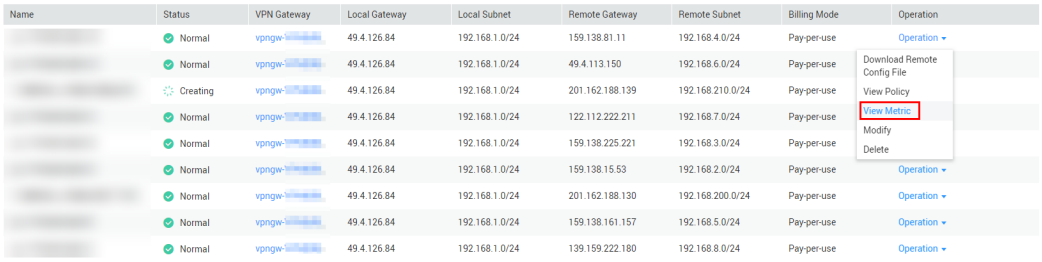
Quando uma conexão de VPN é criada, as rotas são entregues automaticamente para alcançar as sub-redes remotas.

## 17.2.33 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme automaticamente para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Depois que uma conexão de VPN for criada, você poderá localizar a linha que contém a conexão de VPN e escolher **Operation** > **View Metric** para exibir o status da conexão de VPN.

**Figura 17-13** Ver métrica




## 17.2.34 O que fazer se a configuração da conexão de VPN falhar?

1. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.
   a. Se a política de IKE tiver sido configurada durante a primeira fase e a política de IPsec não tiver sido ativada na segunda fase, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.
   b. Se você usa um dispositivo físico de Cisco em seu data center local, recomenda-se que você use MD5 e defina **Authentication Mode** como **MD5** ao configurar a política de IPsec para a conexão de VPN na nuvem.
2. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
```

3. Verifique se a conexão de VPN está normal pingando a extremidade local a partir da extremidade remota e pingando a extremidade remota a partir da extremidade local.

## 17.2.35 Qual direção da largura de banda é limitada e qual é a unidade da largura de banda?

Sua largura de banda de gateway de VPN adquirida é usada na direção de saída. Para equilibrar o tráfego nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada.

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

# 17.3 Rede e cenários de aplicação

## 17.3.1 Posso visitar sites além das fronteiras internacionais usando uma VPN?

Não.

A VPN conecta uma VPC e a rede de um data center local, ou seja, conexão site a site.

## 17.3.2 Posso implementar aplicações na nuvem, bancos de dados em um data center local e depois conectá-las por meio de uma VPN?

VPN conecta uma VPC e uma rede local.

Depois que a VPN é configurada com sucesso, a VPC e a rede local podem se comunicar entre si. Nesse caso, o servidor de aplicações que acessa o banco de dados é o mesmo que acessar outros servidores na mesma LAN.

Servidores de nuvem e servidores locais podem se comunicar uns com os outros.

**AVISO**

- Depois que uma VPN é configurada, verifique se a latência da rede e a perda de pacotes afetam negativamente a execução do serviço.
- Recomenda-se executar o comando ping para verificar a perda de pacotes e os detalhes da latência da rede.

## 17.3.3 Quantas conexões de VPN são necessárias para me conectar a vários servidores locais?

A VPN IPsec da Huawei Cloud conecta uma VPC na nuvem e seu data center local. Portanto, o número de conexões de VPN é irrelevante para o número de servidores, mas para o número de data centers onde os servidores estão localizados.

Na maioria dos casos, um data center local tem um gateway público. Todos os servidores se conectam à Internet através deste gateway. Portanto, você só precisa configurar uma conexão de VPN para permitir comunicações entre a VPC da Huawei Cloud e seu data center local.

## 17.3.4 Preciso instalar o software de IPsec em cada servidor que precisa acessar um ECS para estabelecer uma conexão de VPN?

Não.

A VPN da Huawei Cloud conecta duas LANs. Vários servidores no data center local usam o mesmo endereço IP público para acessar a nuvem. Se você instalar o software de IPsec nos servidores locais, o gateway de VPN na nuvem receberá pacotes de negociação de servidores diferentes e, em seguida, o sistema receberá uma grande quantidade de informações de negociação repetidas, o que causa exceções de conexão ou até mesmo indisponibilidade de conexão.

Recomenda-se que você use o firewall de saída para configurar uma VPN para se conectar à nuvem. Ao criar uma VPN, você pode especificar vários blocos CIDR. Você só deve permitir que servidores de desenvolvedores acessem o ECS na nuvem com base nas regras de grupo de segurança na nuvem ou nas regras de segurança do data center local.

## 17.3.5 Quais são as diferenças entre os cenários de aplicação e os modos de conexão de VPNs IPsec e SSL?

### Cenários

VPN IPsec conecta duas LANs, como uma filial e sua sede, ou um data center local e uma VPC.

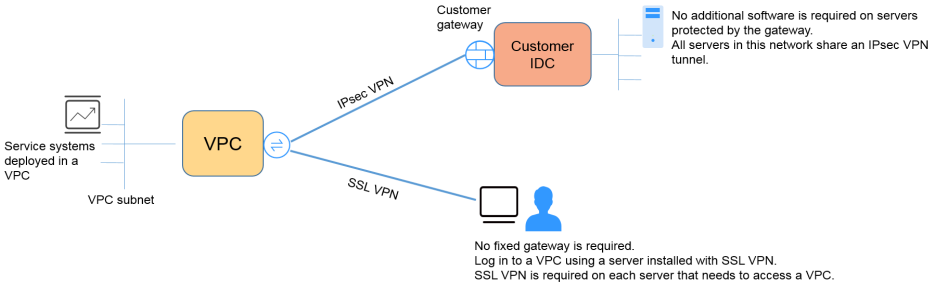
VPN SSL conecta um cliente a uma LAN. Por exemplo, o computador portátil de um funcionário em uma viagem de negócios acessa a rede interna da empresa.

### Modos de conexão

VPN IPsec requer gateways fixos, como firewalls ou roteadores, em ambas as extremidades. O administrador precisa configurar gateways em ambas as extremidades para concluir a negociação de VPN IPsec.

VPN SSL precisa instalar um software cliente especificado no servidor e, em seguida, o servidor se conecta ao dispositivo SSL através do nome de usuário e senha.




NOTA

A Huawei Cloud suporta apenas VPNs IPsec.

## 17.3.6 Uma VPN permite comunicações entre as duas VPC?

- Se as duas VPCs estiverem implementadas na mesma região, use uma conexão de emparelhamento de VPC para conectá-las.
- Se as duas VPCs forem implementadas em regiões diferentes, use uma conexão de VPN para conectá-las. As operações detalhadas são as seguintes:
  a. Crie um gateway de VPN para cada VPC e crie conexões de VPN para os dois gateways de VPN.
  b. Defina o endereço do gateway remoto de cada conexão de VPN para o endereço IP do gateway do lado do par.
  c. Defina as sub-redes remotas de cada conexão de VPN para as sub-redes da VPC de mesmo nível.
  d. As chaves pré-compartilhadas e os parâmetros do algoritmo das duas conexões de VPN devem ser os mesmos.

## 17.3.7 Quais são os impactos de uma VPN em uma rede local? Quais são as mudanças na rota para acessar um ECS?

Quando configurar uma VPN, execute as seguintes operações no gateway no local:

1. Configure políticas de IKE e IPsec.
2. Especifique o tráfego interessante (regras ACL).
3. Verifique a rota do gateway local para garantir que o tráfego destinado à VPC da Huawei Cloud seja roteado para a interface de saída correta (a interface com a política IPsec vinculada).

Após a conclusão da configuração de VPN, somente o tráfego correspondente às regras de ACL entra no túnel de VPN.

Por exemplo, antes de uma VPN ser criada, os usuários locais acessam o ECS por meio do EIP vinculado ao ECS. Depois que a VPN é criada, os fluxos de dados correspondentes às regras de ACL acessam o endereço IP privado do ECS por meio do túnel de VPN.

## 17.3.8 Quais configurações são necessárias em ambas as extremidades de uma VPN que conecta um data center local a uma VPC?

Para implementar a interconexão de VPN, crie uma VPN na nuvem e configure o dispositivo de VPN no data center local.

- Criar uma VPN na nuvem: compre um gateway de VPN selecionando o modo de cobrança, a VPC e a largura de banda. Compre uma conexão de VPN especificando os endereços IP do gateway, as sub-redes e as políticas de negociação em ambas as extremidades.
- Configurar o dispositivo de VPN local: selecione o endereço IP público no lado do centro de dados no local, conclua as configurações das fases 1 e 2 de negociação de IPsec no dispositivo que suporta VPN IPsec e, em seguida, configure rotas de rede, NAT e regras de segurança.

## 17.3.9 Posso usar uma rede com duas saídas para estabelecer duas conexões de VPN com a mesma VPC?

Não.

Ao criar uma VPN na nuvem, uma sub-rede local é uma sub-rede de VPC e uma sub-rede remota é uma sub-rede local. Se as duas conexões usarem a mesma sub-rede local e sub-rede remota, as conexões de VPN falharão.

## 17.3.10 Posso conectar duas VPCs na mesma região por meio de uma VPN?

Não.

Para duas VPCs na mesma região, você pode usar uma conexão de emparelhamento de VPC ou da Cloud Connect para conectá-las.

## 17.3.11 Como conectar duas VPCs na mesma região?

Duas VPCs na mesma região podem ser conectadas usando uma conexão de emparelhamento de VPC ou Cloud Connect. O emparelhamento de VPC só pode conectar VPCs na mesma região, e a Cloud Connect também pode conectar VPCs em diferentes regiões.

## 17.3.12 Como substituir uma Direct Connect por uma VPN?

1. Certifique-se de que o gateway local oferece suporte a VPN IPsec.
2. Crie um gateway de VPN e uma conexão de VPN na Huawei Cloud. Selecione a VPC para a qual a conexão Direct Connect é usada para o gateway de VPN.

**AVISO**

Ao criar uma conexão de VPN, configure sua sub-rede remota da seguinte maneira para evitar conflitos de roteamento.

- Exclua a interface virtual da conexão Direct Connect primeiro e, em seguida, configure a conexão de VPN.
- Divida a sub-rede remota em duas sub-redes e configure a conexão de VPN. Depois que a conexão Direct Connect for excluída, configure a conexão de VPN novamente.

# 17.3.13 Como habilitar comunicações entre duas VPCs e uma rede local?

## Topologia de rede

IDC-VPC 1-VPC 2


**NOTA**

IDC indica o centro de dados no local. Uma conexão de VPN é estabelecida entre a VPC 1 e o IDC.

## Procedimento

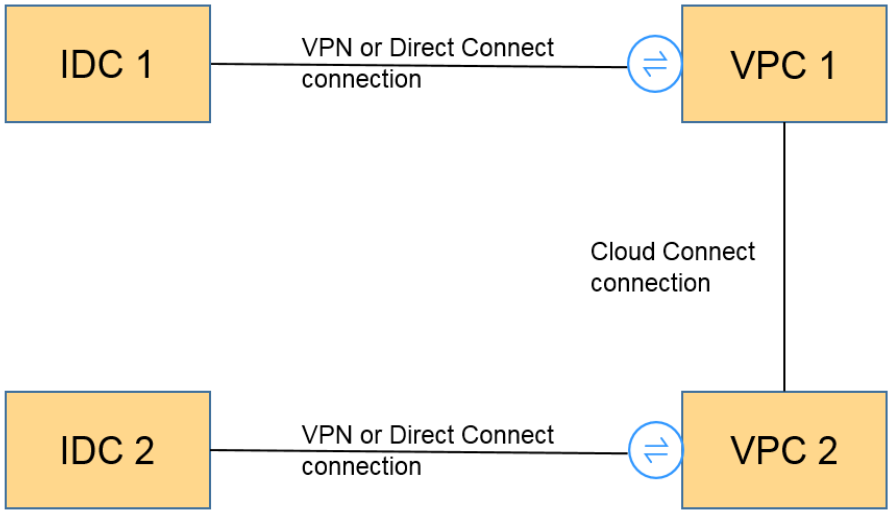
1. Verifique se as duas VPCs estão na mesma região.
   - Se as duas VPCs estiverem na mesma região, use uma conexão de emparelhamento de VPC ou Cloud Connect (gratuitamente) para conectá-las.
   - Se as duas VPCs estiverem em regiões diferentes, use uma conexão Cloud Connect. (Você precisa pagar pela taxa de largura de banda.)
2. Estabeleça uma conexão de VPN entre o local e uma VPC. No data center local, defina a sub-rede remota como as sub-redes da VPC 1 e da VPC 2. A sub-rede local da VPC 1 deve conter a sub-rede conectada por meio de uma conexão de emparelhamento da VPC ou Cloud Connect. A rota de sub-rede da conexão de emparelhamento da VPC ou Cloud Connect deve destinar-se à sub-rede local.

# 17.3.14 Como conectar quatro sub-redes?

**Figura 17-14** mostra a topologia da rede.

**Figura 17-14** Topologia de rede




1. Use uma conexão de VPN ou Direct Connect para conectar o IDC 1 à VPC 1.
2. Use uma conexão Cloud Connect para conectar a VPC 1 à VPC 2. (Você também pode usar uma conexão de emparelhamento da VPC para habilitar as comunicações entre a VPC 1 e a VPC 2, se elas estiverem na mesma região.)
3. Use uma conexão de VPN ou Direct Connect para conectar o IDC 2 à VPC 2.
4. Configure rotas para permitir que o tráfego entre e saia das quatro sub-redes envolvidas nas conexões de VPN, Cloud Connect e Direct Connect.

## 17.3.15 Preciso de duas conexões de VPN para conectar quatro sub-redes de duas regiões se cada região tiver duas sub-redes?

Não.

Apenas uma conexão de VPN é necessária entre duas regiões. Todas as sub-redes podem ser adicionadas à conexão de VPN.

Neste cenário, se tentar criar uma segunda conexão de VPN, o console de gerenciamento apresenta uma mensagem a indicar que ocorre um conflito porque as duas conexões têm o mesmo endereço de gateway de cliente.

## 17.3.16 Posso acessar o OBS através de uma VPN?

Sim.

Com a ajuda do serviço VPC Endpoint, você acessa o OBS por meio de uma VPN. Crie dois pontos de extremidade de VPC para o servidor DNS privado e o OBS, respectivamente.

Configure o servidor DNS privado e a rota da Huawei Cloud em seu data center local.

## 17.3.17 Como conectar meu computador pessoal à nuvem por meio de uma VPN?

Roteadores domésticos de banda larga comuns, terminais móveis pessoais e serviços de VPN (como L2TP) fornecidos por hosts de Windows não podem se interconectar com a VPN da Huawei Cloud.

Para usar a VPN da Huawei Cloud, os dispositivos locais devem suportar o protocolo IPsec padrão.

## 17.3.18 Como acessar os ECSs da Huawei Cloud em casa quando minha rede corporativa foi conectada à Huawei Cloud por meio de uma VPN?

Uma VPN da Huawei Cloud conecta uma VPC na nuvem e uma rede local (LAN) local.

A rede doméstica não faz parte da LAN da sua empresa e não pode ser conectada diretamente à VPC na nuvem.

Se seu host em casa precisar acessar recursos da VPC na nuvem, ele poderá acessar diretamente o EIP do serviço em nuvem ou se conectar à LAN da sua empresa por meio de VPN SSL (se sua empresa suportar acesso SSL) e depois acessar recursos da VPC na nuvem por meio da LAN.

## 17.3.19 Como criar uma conexão de VPN temporariamente se nenhum dispositivo local que ofereça suporte a IPsec estiver disponível após a compra de um gateway de VPN da Huawei Cloud e uma conexão de VPN?

Para estabelecer uma conexão de VPN com a Huawei Cloud, um dispositivo que suporte IPsec padrão e um endereço IP público fixo deve estar disponível na rede local.

Para se conectar temporariamente à Huawei Cloud, instale software de terceiros no host.

Os softwares IPsec de terceiros recomendados incluem GreenBow, StrongSwan e Openswan. Para obter detalhes, consulte **Guia de administrador de rede privada**.

## 17.3.20 Como selecionar uma região adequada na nuvem quando estou comprando um gateway de VPN?

Você pode selecionar uma VPC em qualquer região ao comprar um gateway de VPN.

Mas é recomendável que você selecione a região onde seu data center local se localiza para menor latência de rede.

- Para várias VPCs na mesma região, você só precisa criar um gateway de VPN, pois as VPCs podem ser conectadas usando conexões de emparelhamento de VPC (gratuitamente).
- Para se conectar a várias VPCs em diferentes regiões, você pode usar a VPN e a Cloud Connect.

# 17.4 Cobrança e pagamentos

## 17.4.1 Quanto será cobrado pela criação de uma VPN? Será cobrado pelos endereços IP do gateway de VPN?

VPNs podem ser cobradas em uma base anual/mensal ou de pagamento por uso. Você precisa pagar pela largura de banda ou pelo preço do tráfego do gateway de VPN e pelo preço da conexão de VPN.

Os gateways de VPN podem ser cobrados por tráfego ou largura de banda.

- Um gateway de VPN anual/mensal só pode ser cobrado por largura de banda. O preço de um gateway de VPN anual/mensal inclui o preço das conexões de VPN que podem ser criadas para o gateway e o preço da largura de banda.
- O ciclo de faturamento do modo de cobrança de pagamento por uso é de 1 hora. Se você escolher um gateway de VPN de pagamento por uso, uma conexão de VPN deve ser adquirida juntamente com o gateway de VPN. O preço inclui a largura de banda do gateway de VPN ou o preço do tráfego e o preço da conexão de VPN criada junto com o gateway. Se você criar outra conexão para o gateway, será cobrado pela conexão adicional.

  NOTA

  - O endereço IP do gateway de VPN não será cobrado.
  - Um gateway de VPN não pode compartilhar uma largura de banda com um EIP vinculado a um ECS.

## 17.4.2 Qual é a diferença entre a cobrança de um gateway de VPN por largura de banda e por tráfego?

Um gateway de VPN pagamento por uso pode ser cobrado por largura de banda ou por tráfego. As suas diferenças são as seguintes:

- Cobrança por largura de banda: o ciclo de faturamento é de uma hora. A taxa gerada depende do tamanho da largura de banda.
- Cobrança por tráfego: as taxas de trânsito geradas a cada hora serão cobradas. A cobrança é baseada no tráfego gerado saindo de uma VPC. O tamanho da largura de banda não afeta o preço do tráfego público por GB.

## 17.4.3 Uma VPN cobrada por tráfego pode usar um pacote de dados compartilhados?

Não.

O serviço VPN é cobrado de forma independente e não pode usar pacotes de dados compartilhados.

### 17.4.4 Quantas conexões de VPN serão cobradas para conectar VPCs em regiões diferentes?

As VPNs podem ser usadas para conectar VPCs em diferentes regiões. A largura de banda e as conexões de VPN de cada região serão cobradas de forma independente. Exemplo:

Na Região A, você estabelece uma conexão de VPN com a Região B e outra conexão de VPN com a Região C, então

- O gateway de VPN da Região A tem duas conexões.
- O gateway de VPN da Região B tem uma conexão.
- O gateway de VPN da Região C tem uma conexão.

Nesse caso, você será cobrado por quatro conexões de VPN.

### 17.4.5 Quando meus recursos de VPN serão congelados? Como descongelar os recursos da VPN?

- Se os recursos de VPN de pagamento por uso estiverem em atraso, os recursos entrarão no período de carência, durante o qual você ainda poderá acessar e usar os recursos. Se o período de carência terminar e você não tiver quitado os atrasos, os recursos entrarão no período de retenção, durante o qual os recursos serão congelados. Os recursos congelados estão indisponíveis e não podem ser modificados ou liberados. Se o período de retenção terminar e você ainda não tiver recarregado sua conta e quitado os pagamentos em atraso, os recursos serão liberados e não poderão ser restaurados. Para garantir que os recursos estejam disponíveis, recarregue sua conta e pague os atrasos antes que os recursos expirem.
- Os recursos congelados da VPN ficarão disponíveis depois que você renová-los ou recarregar sua conta. Se uma conexão de VPN estiver no estado não conectado, inicie os fluxos de dados para acionar a conexão de VPN e deixe-a no estado normal. Por exemplo, você pode fazer ping em hosts em diferentes sub-redes para acionar fluxos de dados.

## 17.5 Operações relacionadas no console

### 17.5.1 Quais são as relações entre uma VPC, um gateway de VPN e uma conexão de VPN?

- Uma VPC é uma rede privada na nuvem. Várias VPCs podem ser criadas na mesma região enquanto estão isoladas umas das outras. Uma VPC pode ser dividida em várias sub-redes.
- Um gateway de VPN é criado em uma VPC e é o ponto de acesso de uma conexão de VPN. Uma VPC da Huawei Cloud pode ter apenas um gateway de VPN, enquanto um gateway de VPN pode ter várias conexões de VPN.
- Uma conexão de VPN é criada para um gateway de VPN e conecta uma VPC a um data center local (ou uma VPC em outra região).

NOTA

O número de conexões de VPN é irrelevante para o número de sub-redes locais ou o número de sub-redes remotas. Ele está relacionado apenas ao número de data centers locais (ou VPCs em outras regiões) a serem conectados à sua VPC. As conexões de VPN criadas são exibidas na lista de conexões de VPN. Você também pode visualizar o número de conexões de VPN criadas para cada gateway de VPN.

## 17.5.2 Quanto tempo demora para que as configurações de VPN entregues entrem em vigor?

Leva de 1 a 5 minutos para que as configurações de VPN entrem em vigor.

NOTA

Depois que as configurações de VPN entrarem em vigor, configure seu gateway local para concluir a negociação do túnel com o gateway de VPN na Huawei Cloud.

## 17.5.3 Por que a conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

Certifique-se de que as chaves pré-compartilhadas e as informações de negociação em ambas as extremidades sejam consistentes. As sub-redes locais e o gateway de VPN na nuvem são as sub-redes remotas e o gateway remoto no data center local. O gateway remoto e as sub-redes remotas na nuvem são o gateway local e as sub-redes locais no data center local.

Certifique-se de que as regras de rotas, NAT e política de segurança estão corretamente configuradas no dispositivo de gateway local. Em seguida, faça ping nos servidores em sub-redes em ambas as extremidades.

NOTA

A VPN é acionada com base em fluxos de dados. Depois que você configura a VPN, sibile um dispositivo na sub-rede do par. Antes de executar o comando ping, desabilite a função de firewall no dispositivo e permita pacotes ICMP de entrada no grupo de segurança na nuvem.

O ping do endereço IP do gateway não pode acionar a negociação de VPN. Efetue o ping do servidor na sub-rede protegida pelo gateway.

## 17.5.4 Um endereço IP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Não. O endereço IP do gateway de VPN será liberado depois que o gateway de VPN for excluído.

A exclusão de um gateway de VPN também excluirá os recursos associados ao gateway.

AVISO

A exclusão da última conexão de um gateway de VPN pagamento por uso também excluirá o gateway. Se você quiser manter o endereço IP, não exclua a última conexão de VPN.

## 17.5.5 Preciso criar um gateway de VPN ou uma conexão de VPN para criar uma VPN? Quais informações sobre uma VPN criada podem ser modificadas?

Pré-requisitos para criar uma VPN

Crie uma VPC e sub-redes da VPC. As sub-redes da VPC não podem entrar em conflito com as sub-redes locais.

Para criar uma VPN, você precisa:

- Criar um gateway de VPN Defina **Billing Mode**, **Region**, **Name**, **VPC**, **Billed By** e **Bandwidth (Mbit/s)**. Um endereço IP será atribuído ao gateway de VPN depois que o gateway for criado. Apenas as configurações de **Name** e **Bandwidth** podem ser modificadas após a criação do gateway de VPN.
- Criar uma conexão de VPN Especifique o nome da conexão, o gateway de VPN vinculado, as sub-redes locais, o gateway remoto, as sub-redes remotas, a PSK e as políticas de negociação. O nome da conexão, sub-redes locais, PSK, gateway remoto, sub-redes remotas e políticas de negociação podem ser modificados após a criação da conexão de VPN.

## 17.5.6 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa criar regras de ACL dedicadas para seu dispositivo de gateway local. As regras da ACL serão referenciadas pelas políticas de IPsec.

Quando você configura a VPN na nuvem, as regras da ACL serão geradas automaticamente com base nas sub-redes locais e remotas inseridas no console de gerenciamento e, em seguida, entregues ao gateway de VPN.

(Huawei Cloud) O número de regras da ACL = o número de sub-redes locais x o número de sub-redes remotas

## 17.5.7 O que fazer se ocorrer uma exceção quando adicionar uma sub-rede remota durante a criação da conexão de VPN?

Verifique se essa sub-rede remota foi usada como destino de uma rota de conexão de emparelhamento de VPC, Cloud Connect ou Direct Connect, o que causa conflitos de rota. Se sim, exclua a rota e crie uma nova.

## 17.5.8 Onde posso adicionar rotas no console da VPN para alcançar as sub-redes remotas?

Quando uma conexão de VPN é criada, as rotas são entregues automaticamente para alcançar as sub-redes remotas.

## 17.5.9 Posso chamar APIs para gerenciar os recursos da VPN da Huawei Cloud?

A VPN requer configurações complexas. Atualmente, os recursos de VPN não podem ser criados, consultados ou modificados por meio de APIs. Você só pode gerenciar recursos de VPN no console de VPN.

## 17.5.10 O que é um gateway remoto e uma sub-rede remota em uma conexão de VPN?

Ao criar uma conexão de VPN, uma sub-rede na VPC da Huawei Cloud é a sub-rede local e o gateway de VPN criado é o gateway local. A sub-rede e o gateway conectados no data center local são a sub-rede remota e o gateway remoto.

Um endereço IP de gateway remoto é um endereço IP público.

## 17.5.11 Como desativar o PFS ao criar uma conexão de VPN?

Você pode desativar o Perfect Forward Secrecy (PFS) em algumas regiões da Huawei Cloud. É aconselhável ativar o PFS em seu data center local, pois ele melhora a segurança da negociação IKE na fase 2.

Por padrão, o PFS é desativado em dispositivos de alguns fornecedores. Verifique o manual de configuração do dispositivo para garantir que o PFS esteja ativado.

NOTA

- O PFS é um recurso de segurança.

  A negociação IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Depois que o PFS for configurado, uma troca de DH adicional será executada durante a negociação da AS do IPsec e uma nova chave da AS do IPsec será gerada, melhorando a segurança da AS do IPsec.
- Para garantir a segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no gateway local. Caso contrário, a negociação falhará.

## 17.5.12 Quantas sub-redes locais e remotas posso adicionar a uma VPN? Por que uma mensagem de erro é exibida quando atualizar a sub-rede local especificando um bloco CIDR?

- Você pode configurar até 5 sub-redes locais. O produto do número de sub-redes locais e do número de sub-redes remotas não pode exceder 225.
- Uma VPC fornece rotas de sub-rede da VPC com base nas sub-redes remotas da conexão de VPN, nas sub-redes remotas da conexão Direct Connect e nas sub-redes da conexão de emparelhamento da VPC. Cada sub-rede tem uma rota de sub-rede.
- O número de rotas de sub-rede da VPC não pode exceder 200. Ou seja, o número total de sub-redes remotas da conexão de VPN, sub-redes remotas da conexão Direct Connect, sub-redes da conexão de emparelhamento da VPC e rotas personalizadas em uma VPC não pode exceder 200.

## 17.5.13 Quais são as precauções para configurar as sub-redes locais e remotas de uma conexão de VPN?

- Você pode configurar até 5 sub-redes locais. O produto do número de sub-redes locais e do número de sub-redes remotas não pode exceder 225. Se 225 é excedido, considere supernetting as sub-redes locais ou remotas.
- A sub-rede local não pode incluir o bloco CIDR da sub-rede remota. A sub-rede remota pode incluir o bloco CIDR da sub-rede local.
- Há rotas que apontam para as sub-redes locais na VPC onde o gateway de VPN reside.
- Se houver duas conexões (conexão A e conexão B) criadas para um gateway de VPN, e a sub-rede remota da conexão A estiver dentro da conexão B, quando a rede de destino a ser acessada pertencer ao bloco CIDR sobreposto, a conexão criada primeiro será correspondida primeiro, independentemente do status da conexão. (A correspondência de comprimento da máscara não é usada para a VPN baseada em políticas.)

## 17.5.14 Por que o status de uma conexão de VPN é Not Connected no console de gerenciamento quando ele já está disponível?

Há uma latência para exibir o status de conexão de VPN mais recente no console de gerenciamento.

Se o acesso ao serviço for normal, a conexão de VPN é estabelecida. Após alguns minutos, o status da conexão de VPN será **Connected**.

## 17.5.15 O que fazer se uma mensagem for exibida indicando que a conexão de VPN não existe depois que as políticas de negociação forem modificadas?

Esse problema é causado pelo intervalo de atualização de página.

Quando você modifica as configurações avançadas, o sistema primeiro exclui a conexão de VPN e, em seguida, cria uma. Se a página contiver a mensagem indicando que a conexão está sendo excluída ou criada é exibida por um curto período de tempo, não crie a mesma conexão (com a mesma sub-rede local, sub-rede remota e gateway remoto) novamente.

Se a página permanecer na conexão, excluindo ou criando o estado por um longo tempo, **envie um tíquete de serviço**.

## 17.5.16 O que fazer se não conseguir criar conexões para um gateway de VPN que não tenha informações de largura de banda?

Se um gateway de VPN não tiver informações de largura de banda, a VPN é da edição anterior. Esse tipo de VPN não pode mais ser criado na Huawei Cloud.

- Apenas uma conexão de VPN pode ser criada para cada gateway de VPN da edição anterior e sua largura de banda não é garantida. Você pode excluir o gateway e criar um da nova edição. Mas os serviços serão afetados.
- Você também pode **enviar um tíquete de serviço** para alterar o gateway para uma das novas edições e seus serviços não serão afetados.

Por padrão, a largura de banda de um gateway de VPN alterado para a nova edição é de 10 Mbit/s. Você pode ajustar a largura de banda conforme necessário. A largura de banda de um gateway de VPN que é cobrado anualmente/mensalmente não pode ser reduzida.

# 17.5.17 Como redefinir uma conexão de VPN?

- Desative a conexão de VPN no dispositivo local. Depois que o status da conexão de VPN na nuvem for alterado para **Not connected**, ative a conexão de VPN no dispositivo local.
- Altere o endereço IP do gateway remoto da conexão de VPN na nuvem para qualquer outro endereço IP. Depois que o status da conexão no data center local for alterado para inativo, altere o endereço IP do gateway remoto na nuvem para o endereço IP anterior.

# 17.5.18 Qual é a largura de banda máxima suportada por um gateway de VPN?

A largura de banda máxima suportada por um gateway de VPN é de 300 Mbit/s.

# 17.5.19 Qual versão do IKE devo selecionar ao criar uma conexão de VPN?

A Huawei Cloud recomenda o IKEv2 para negociação porque o IKEv1 não é seguro. Além, IKEv2 executa melhor do que IKEv1 em termos da negociação da conexão e do estabelecimento, métodos de autenticação, tempo limite de DPD e tempo limite de AS.

A Huawei Cloud não suportará o IKEv1 em breve.

## Introdução ao IKEv1 e IKEv2

- A complexidade do IKEV1, um protocolo híbrido, inevitavelmente traz alguns defeitos de segurança e desempenho. Isso se tornou o gargalo para o atual sistema de IPsec.
- O protocolo IKEv2 reserva funções básicas do IKEv1 e supera alguns problemas trazidos pelo IKEv1. Além disso, para a simplicidade, eficiência, segurança e robustez, RFC 4306, um documento descreve a versão 2 do IKE, combina o conteúdo do que eram anteriormente separados documentos de IKEv1. Ao minimizar as funções principais e os algoritmos de senha padrão, o IKEv2 melhora muito a interoperabilidade entre diferentes VPNs IPsec.

## Vulnerabilidades de segurança de IKEv1

- Os algoritmos criptográficos suportados pelo IKEv1 não foram atualizados por mais de 10 anos. Além disso, o IKEv1 não oferece suporte a algoritmos criptográficos fortes, como AES-GCM e ChaCha20-Poly1305. Para IKEv1, o bit E (criptografia) no cabeçalho ISALMP especifica que as cargas úteis seguintes ao cabeçalho ISALMP são criptografadas, mas qualquer verificação de integridade de dados dessas cargas úteis é tratada por uma carga útil hash separada. Essa separação entre criptografia e proteção de integridade de dados impede o uso de criptografia autenticada (AES-GCM) com o IKEv1.
- O protocolo IKEv1 é vulnerável a ataques de amplificação de DoS. O IKEv1 é vulnerável a conexões semi-abertas.

  O IKEv2 pode se defender contra ataques DoS.

- O modo agressivo de IKEv1 não é suficientemente seguro. No modo agressivo, os pacotes de informações não são criptografados. Há também ataques de força bruta visando o modo agressivo, como ataques man-in-the-middle.

## Diferenças entre IKEv1 e IKEv2

- **Processo de negociação**
  - Negociação de AS de IKEv1 consiste em duas fases. O IKEv1 é complexo e consome uma grande quantidade de largura de banda. A negociação da fase 1 do IKEv1 visa estabelecer a AS de IKE. Este processo suporta o modo principal e o modo agressivo. O modo principal usa seis mensagens ISAKMP para estabelecer a AS de IKE, mas o modo agressivo usa apenas três. Portanto, o modo agressivo é mais rápido no estabelecimento da AS de IKE. No entanto, o modo agressivo não fornece proteção de identidade de par porque a troca de chaves e a autenticação de identidade são realizadas ao mesmo tempo. A negociação da fase 2 do IKEv1 visa configurar a AS do IPsec para transmissão de dados. Esse processo usa o modo de troca rápida (3 mensagens de ISAKMP) para concluir a negociação.
  - Comparado com o IKEv1, o IKEv2 simplifica o processo de negociação de AS. O IKEv2 usa duas trocas (um total de 4 mensagens) para criar uma AS de IKE e um par de ASs de IPsec. Para criar vários pares de ASs de IPsec, apenas uma troca adicional é necessária para cada par adicional de ASs.

    NOTA

    Para a negociação de IKEv1, seu modo principal requer nove (6+3) pacotes no total e seu modo agressivo requer 6 (3+3) pacotes. A negociação de IKEv2 exige somente 4 (2+2) pacotes.

- **Métodos de autenticação**
  - Somente o IKEv1 (que exige um cartão de criptografia) suporta autenticação de envelope digital (HSS-DE).
  - O IKEv2 oferece suporte à autenticação EAP (Extensible Authentication Protocol). O IKEv2 pode usar um servidor AAA para autenticar remotamente usuários de dispositivos móveis e de PC e atribuir endereços IP privados a esses usuários. O IKEv1 não fornece essa função e deve usar o L2TP para atribuir endereços IP privados.
  - Apenas o IKEv2 suporta algoritmos de integridade de AS de IKE.
- **Tempo limite de DPD**
  - Somente o IKEv1 suporta o parâmetro **retry-interval**. Se um dispositivo envia um pacote de DPD, mas não recebe nenhuma resposta dentro do intervalo de repetição especificado, o dispositivo grava um evento de falha de DPD. Quando o número de eventos de falha de DPD atinge 5, ambas ASs de IKE e de IPsec são excluídas. A negociação de AS de IKE será iniciada novamente quando o dispositivo tiver tráfego IPsec para lidar.
  - No modo de IKEv2, o intervalo de retransmissão aumenta de 1, 2, 4, 8, 16, 32 para 64, em segundos. Se nenhuma resposta for recebida dentro de oito transmissões consecutivas, a extremidade do par será considerada inativa e as ASs de IKE e de IPsec serão excluídas.
- **Processamento de tempo limite da AS de IKE e processamento de tempo limite da AS de IPsec**

  No IKEv2, a vida útil da AS de IKE é 9/10 da vida útil da AS de IKE mais ou menos um valor aleatório para reduzir a probabilidade de que duas extremidades iniciem a

renegociação ao mesmo tempo. Portanto, a vida útil do soft não requer configurações manuais no IKEv2.

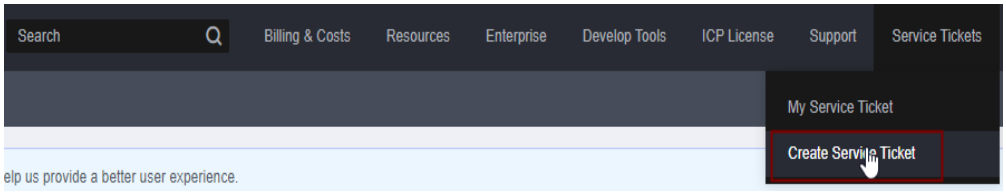
### Vantagens do IKEv2 em relação ao IKEv1

- Processo de negociação de AS simplificado e eficiência de negociação aprimorada.
- Fechou muitas brechas criptográficas, melhorando a segurança.
- Suporta autenticação EAP, melhorando a flexibilidade e escalabilidade da autenticação.
- O EAP é um protocolo de autenticação que suporta vários métodos de autenticação. A maior vantagem de EAP é a escalabilidade. Ou seja, novos modos de autenticação podem ser adicionados sem alterar o sistema de autenticação original. A autenticação EAP tem sido amplamente utilizada em redes de acesso de discagem.
- O IKEv2 emprega uma carga útil criptografada baseada no projeto do ESP. A carga útil criptografada de IKEv2 associa criptografia e proteção de integridade de dados de uma forma que torna possível o uso de algoritmos de criptografia autenticados. O AES-GCM garante confidencialidade, integridade e autenticação.

## 17.5.20 Quais são as categorias de tíquetes de serviço de VPN? Como criar um tíquete de serviço de VPN?

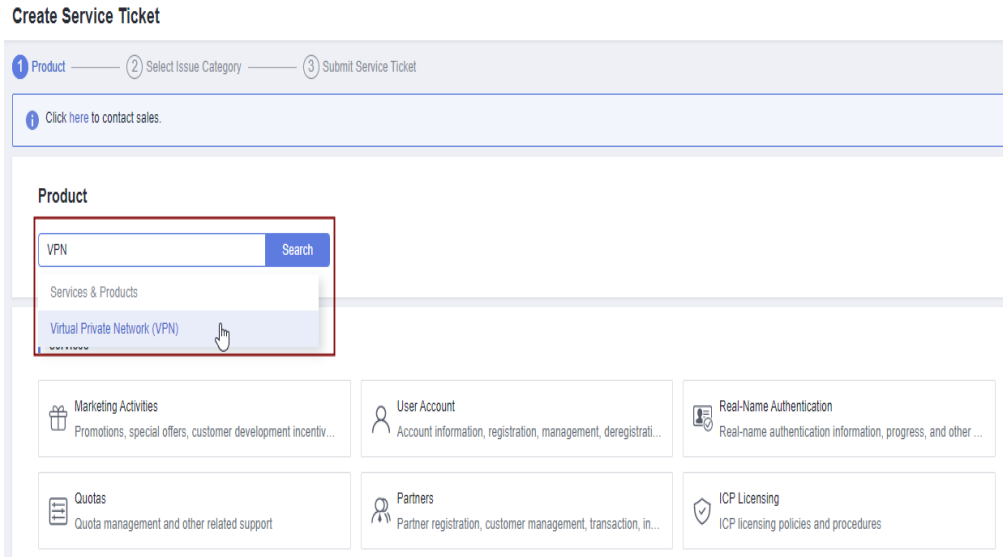
1. Faça logon no console de gerenciamento.
2. No canto superior direito do console de gerenciamento, escolha **Service Tickets** > **Create Service Ticket**.

**Figura 17-15** Criar tíquete de serviço




3. Procure **VPN** e selecione **Virtual Private Network (VPN)**.

**Figura 17-16** Selecionar **Virtual Private Network (VPN)**



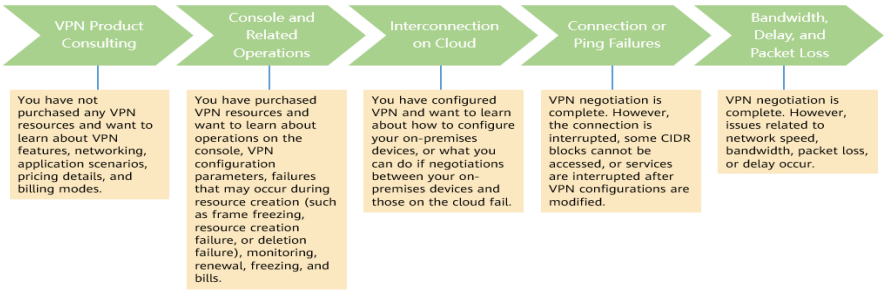
4. Selecione uma categoria de problema.

**Figura 17-17** Selecionar categoria de problema


NOTA

Ao **enviar um tíquete de serviço**, selecione uma categoria de problema para facilitar o tratamento do problema.

**Figura 17-18** Categoria de emissão e base de classificação




## 17.5.21 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A chave é configurada em um gateway de VPN. Um túnel será estabelecido após a conclusão da negociação de VPN. Portanto, nomes de usuário e senhas não são necessários.

Geralmente, as VPNs SSL, PPTP e L2TP usam nomes de usuário e senhas para autenticação.

NOTA

IPsec XAUTH é uma tecnologia estendida da VPN IPsec. Ele solicita que os usuários insiram seus nomes de usuário e senhas durante a negociação de VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

## 17.5.22 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As informações de largura de banda que podem ser monitoradas incluem tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as métricas do gateway de VPN, localize o gateway de VPN de destino e clique em **View Metric** na coluna **Operation**.

**Conexão de VPN**

O status da conexão de VPN pode ser monitorado.

O valor **1** indica que a conexão é normal.

O valor **0** indica que a conexão não está conectada.

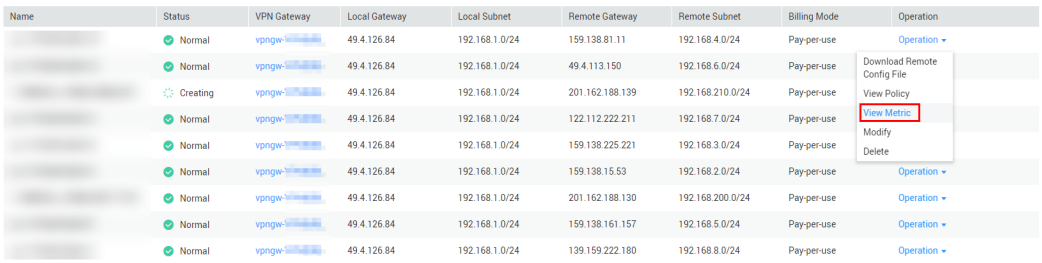
Para exibir o status da conexão de VPN, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

## 17.5.23 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme automaticamente para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Depois que uma conexão de VPN for criada, você poderá localizar a linha que contém a conexão de VPN e escolher **Operation** > **View Metric** para exibir o status da conexão de VPN.

**Figura 17-19** Ver métrica




# 17.6 Negociação e interconexão de VPN

## 17.6.1 Quais dispositivos podem ser conectados à Huawei Cloud por meio de uma VPN?

A VPN da Huawei Cloud suporta o protocolo IPsec padrão. Um dispositivo em seu data center local pode se conectar à Huawei Cloud se o dispositivo atender aos seguintes requisitos:

1. Suporta VPN IPsec.
2. Tem um endereço IP público fixo, que pode ser configurado estaticamente ou traduzido por meio de NAT em cenários de travessia de NAT (seu dispositivo é implantado atrás de um gateway de NAT).

A maioria dos dispositivos são roteadores e firewalls. Para obter detalhes sobre a configuração de interconexão, consulte **Guia de administrador**.

NOTA

- Roteadores de banda larga domésticos comuns, hosts de Windows que fornecem serviços de VPN (como L2TP) e terminais móveis pessoais não podem se conectar à Huawei Cloud por meio de uma VPN.
- Os seguintes produtos podem se conectar à Huawei Cloud por meio de VPNs:
  - Dispositivos: firewalls e roteadores de acesso (ARs) da Huawei, firewalls de Hillstone e firewalls de Check Point
  - Serviços em nuvem: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) e Microsoft Azure
  - Software: StrongSwan
- O protocolo IPsec é um protocolo IETF padrão. Os dispositivos que suportam IPsec podem interconectar-se com a Huawei Cloud.

  A maioria dos roteadores e firewalls de classe empresarial suportam o protocolo IPsec.
- No entanto, alguns dispositivos suportam VPN IPsec somente após de comprar as licenças de software necessárias.

  Entre em contato com o administrador do data center local para confirmar o modelo do dispositivo com o fornecedor.

## 17.6.2 Quais são os parâmetros de negociação de VPN? Quais são seus valores padrão?

**Tabela 17-4** Parâmetros de negociação de VPN

| Política | Parâmetro | Valor |
| --- | --- | --- |
| IKE | Authentication Algorithm | ● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● AES-256<br>● AES-192<br>● AES-128 (valor padrão) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | DH Algorithm | ● Group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 14 (valor padrão)<br>● Group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● Group 15<br>● Group 16<br>● Group 19<br>● Group 20<br>● Group 21<br>**NOTA**<br>Em algumas regiões, apenas **Group 14**, **Group 2** e **Group 5** estão disponíveis. |
| | Version | ● v1 (não recomendada devido a riscos de segurança)<br>● v2 (valor padrão) |
| | Lifecycle (s) | **86400** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **60** a **604800** |
| IPsec | Authentication Algorithm | ● SHA1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● MD5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● SHA2-256 (valor padrão)<br>● SHA2-384<br>● SHA2-512 |
| | Encryption Algorithm | ● AES-128 (valor padrão)<br>● AES-192<br>● AES-256<br>● 3DES (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.) |

| Política | Parâmetro | Valor |
| --- | --- | --- |
| | PFS | ● DH group 5 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 2 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 14 (valor predefinido)<br>● DH group 1 (Este algoritmo é inseguro. Tenha cuidado ao usar este algoritmo.)<br>● DH group 15<br>● DH group 16<br>● DH group 19<br>● DH group 20<br>● DH group 21<br>● Disable<br>**NOTA**<br>Em algumas regiões, apenas **DH group 14**, **DH group 2** e **DH group 5** estão disponíveis. |
| | Transfer Protocol | ● ESP (valor padrão)<br>● AH<br>● AH-ESP |
| | Lifecycle (s) | **3600** (padrão)<br>Unidade: segundo<br>Intervalo de valores: **480** a **604800** |

NOTA

- Perfect Forward Secrecy (PFS) é um recurso de segurança.

  A negociação de IKE tem duas fases, fase um e fase dois. A chave da fase dois (AS de IPsec) é derivada da chave gerada na fase um. Uma vez que a chave na primeira fase é divulgada, a segurança da VPN IPsec pode ser afetada negativamente. Para melhorar a segurança da chave, o IKE fornece o PFS. Depois que o PFS for configurado, uma troca de DH adicional será executada durante a negociação da AS do IPsec e uma nova chave da AS do IPsec será gerada, melhorando a segurança da AS do IPsec.
- Para garantir a segurança, o PFS é ativado na Huawei Cloud por padrão. Certifique-se de que o PFS também esteja ativado no gateway local. Caso contrário, a negociação falhará.
- Para habilitar o PFS, certifique-se de que as configurações em ambas as extremidades de uma VPN sejam as mesmas.
- O tempo de vida baseado em tráfego da AS do IPsec na VPN da Huawei Cloud é padrão para 1.843.200 KB e não pode ser alterado. Esse tempo de vida não afeta o estabelecimento de uma AS de IPsec.

## 17.6.3 Uma conexão de VPN IPsec será estabelecida automaticamente?

Depois de concluir as configurações em ambas as extremidades de uma conexão de VPN IPsec, a conexão de VPN não será estabelecida automaticamente somente após os fluxos de

dados entre as duas extremidades da conexão. Se nenhum fluxo de dados entre a nuvem e o data center local, a conexão de VPN estará sempre no estado inativo. Quaisquer dados gerados pelo acesso a servidores ou pelo ping entre servidores podem acionar o estabelecimento de uma conexão de VPN.

O estabelecimento de uma conexão de VPN pode ser acionado em uma das duas condições a seguir: O gateway de VPN e o gateway remoto disparam automaticamente a negociação. Os servidores em nuvem e locais acedem uns aos outros através da conexão de VPN a estabelecer.

No entanto, o estabelecimento automático de uma conexão de VPN não pode ser acionado por um gateway de VPN na Huawei Cloud. Verifique se o estabelecimento de sua conexão de VPN pode ser acionado pelos fluxos de dados entre as duas extremidades da conexão de VPN. Ou seja, verifique se é possível estabelecer uma conexão de VPN depois de efetuar um ping a um servidor na nuvem a partir de um servidor no local e se é possível estabelecer uma conexão de VPN depois de desligar a conexão e efetuar um ping a um servidor no local a partir de um servidor na nuvem.

**NOTA**

Os endereços de origem e destino dos pacotes de ping devem ser protegidos pela VPN.

Antes que uma conexão de VPN seja estabelecida, os endereços IP do gateway em ambas as extremidades podem ser pingados. No entanto, o ping dos endereços IP do gateway não aciona o estabelecimento da conexão de VPN.

# 17.6.4 Como configurar uma VPN em um dispositivo local? (Configuração da VPN em um firewall da série USG6600 da Huawei)

Devido à simetria do túnel, os parâmetros de VPN configurados na nuvem devem ser os mesmos configurados no data center local. Se eles forem diferentes, uma VPN não pode ser estabelecida.

Para configurar uma VPN, você também precisa configurar a VPN IPsec em seu roteador ou firewall local. O método de configuração pode variar dependendo do dispositivo de rede em uso. Para obter detalhes, consulte o guia de configuração do dispositivo de rede.

A seguir, é usado um firewall da série USG6600 da Huawei executando V100R001C30SPC300 como um exemplo para descrever como configurar uma VPN em um dispositivo local.

Suponha que as sub-redes locais sejam 192.168.3.0/24 e 192.168.4.0/24, as sub-redes da VPC sejam 192.168.1.0/24 e 192.168.2.0/24, e o endereço IP público da saída do túnel IPsec na VPC é *XXX.XXX.XX.XX*, que pode ser obtido a partir dos parâmetros de gateway local da VPN IPsec na VPC.

## Procedimento

1. Faça logon na CLI do firewall.
2. Verifique as informações de versão do firewall.
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
   ```
3. Crie uma lista de controle de acesso (ACL) e vincule-a à instância de VPN de destino.

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
0.0.0.255
q
```

4. Crie uma proposta de IKE.

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. Crie um IKE de par e refira à proposta de IKE criada. O endereço IP do par é 93.188.242.110.

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

6. Crie um protocolo IPsec.

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. Crie uma política de IPsec e vincule a política de IKE e a proposta de IPsec a ela.

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address xx.xx.xx.xx
q
```

8. Aplique a política de IPsec à subinterface.

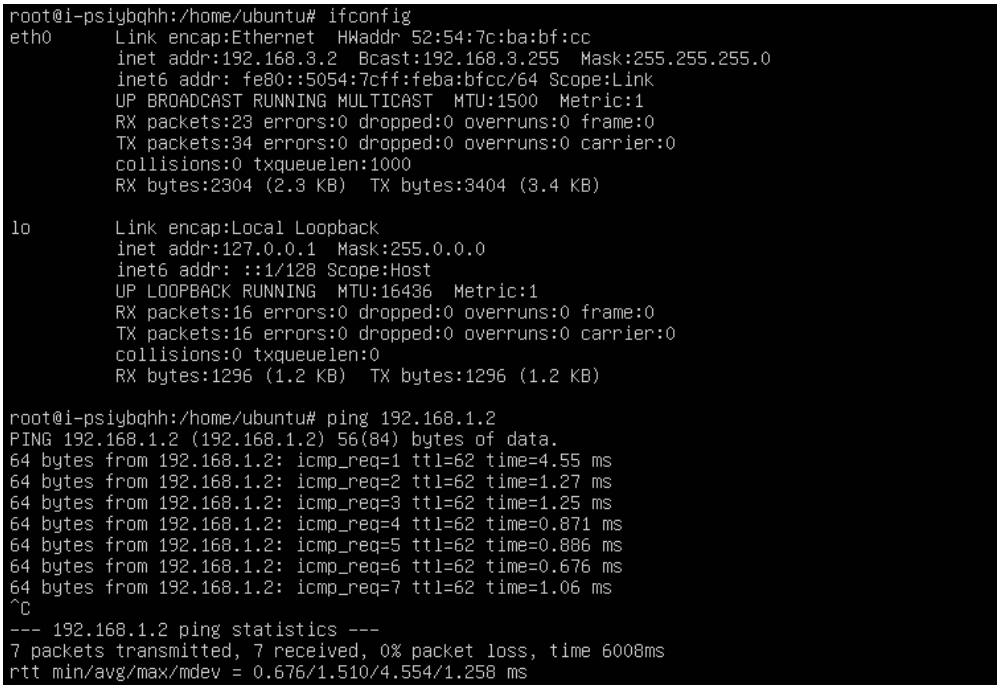
```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. Teste a conectividade.

   Teste a conectividade entre seu ECS na nuvem e os servidores no data center local, conforme mostrado em **Figura 17-20**.

**Figura 17-20** Teste de conectividade




## 17.6.5 Como configurar um gateway local quando usar uma VPN para me conectar à nuvem?

Determine sub-redes locais, sub-redes da VPC e endereços IP de gateway em ambas as extremidades.

Configurar políticas de IPsec no gateway local de acordo com as políticas de IPsec configuradas na nuvem. Adicione regras ao grupo de segurança associado à VPC para permitir pacotes ICMP nas direções de entrada e saída.

- Configuração de rota: adicione rotas começando do gateway local e destinando-se ao gateway de VPN. O próximo salto da rota no gateway de VPN é o endereço IP do gateway público na direção de saída.
- Configuração de NAT: no gateway local, desative a NAT para as sub-redes locais que acessarão as sub-redes da VPC. Adicione regras de grupo de segurança para permitir o acesso mútuo entre as sub-redes locais e as sub-redes VPC e permita o UDP 500, UDP 4500, ESP (protocolo IP 50) e o AH (protocolo IP 51) empacotam de e para endereços IP do gateway de VPN na nuvem e no gateway local.

## 17.6.6 A VPN da Huawei Cloud pode se conectar a um gateway remoto por meio de um nome de domínio?

Não. Uma conexão de VPN só pode se conectar a um gateway remoto através do endereço IP público do gateway.

## 17.6.7 Quantos túneis minha conexão de VPN tem?

O número de túneis em uma conexão de VPN = o número de sub-redes locais x o número de sub-redes remotas da conexão de VPN

O status de uma conexão de VPN é normal, desde que um dos túneis esteja no estado ativo. Se você precisa que cada túnel esteja no estado ativo, os fluxos de dados precisam de ser provocados entre cada duas sub-redes.

## 17.6.8 Como permitir que servidores específicos acessem uma sub-rede da VPC por meio de uma conexão de VPN criada?

Configurações no data center local

- Configure regras de negação em dispositivos de VPN.
- Configure regras de ACL no roteador ou no comutador.

Configurações na nuvem

- Configure regras de grupo de segurança para negar acesso a endereços IP específicos.
- Configure regras de ACL.

NOTA

Todas as regras devem ser adicionadas ao dispositivo antes que o túnel de VPN seja estabelecido. Não altere a sub-rede local e a sub-rede remota para restringir o acesso.

## 17.6.9 As VPNs da Huawei Cloud têm o mecanismo de DPD ativado?

Sim.

As VPNs da Huawei Cloud têm o mecanismo de DPD ativado por padrão para detectar o status do processo de IKE no data center local.

Após três falhas de detecção consecutivas, a Huawei Cloud considera que o processo de IKE no data center local é anormal. Nesse caso, a Huawei Cloud exclui o túnel local para garantir a sincronização do túnel entre as duas extremidades.

O protocolo de DPD não exige que a extremidade do par esteja configurada de forma síncrona, mas exige que a extremidade do par possa responder às detecções de DPD. Para garantir que o status do túnel das duas extremidades seja consistente e evitar que uma extremidade tenha um túnel e a outra não, é recomendável ativar o mecanismo de DPD no gateway local para detectar o status do processo de IKE do serviço VPN na Huawei Cloud.

NOTA

Depois que DPD falhar, o túnel será excluído sem afetar a estabilidade do serviço.

DPD pode detectar exceções no processo IKE na extremidade do par no tempo e redefinir o túnel para garantir a sincronização do túnel entre as duas extremidades. Depois que um túnel é excluído, se houver tráfego transmitido pelo túnel, o túnel poderá ser restabelecido por meio da negociação.

## 17.6.10 Como usar grupos de segurança para evitar que ECSs em uma VPC sejam acessados por meio de uma VPN para implementar o isolamento de segurança?

Você pode configurar grupos de segurança para permitir acesso apenas a blocos CIDR ou ECSs específicos em uma VPC por meio de uma VPN.

**Exemplo de configuração**: impedir que ECSs na sub-rede VPC 10.1.0.0/24 acessem a sub-rede local 192.168.1.0/24.

**Procedimento:**

1. Crie os grupos de segurança 1 e 2.
2. O grupo de segurança 1 nega o acesso da sub-rede 192.168.1.0/24.
3. O grupo de segurança 2 permite o acesso da sub-rede 192.168.1.0/24.
4. Associe ECSs na sub-rede 10.1.0.0/24 ao grupo de segurança 1 e associe outros ECSs na VPC ao grupo de segurança 2.

## 17.6.11 Uma conexão de VPN será restabelecida após sua configuração ser modificada?

Uma conexão de VPN consiste em sub-redes locais, sub-redes remotas, gateway remoto, chave pré-compartilhada, políticas de negociação de IKE e políticas de negociação de IPsec. Uma conexão de VPN será modificada se ocorrer uma das seguintes situações:

- Se as sub-redes locais e remotas forem modificadas, o ID de conexão permanecerá inalterado. Se nem todas as sub-redes forem atualizadas, o túnel estabelecido entre as sub-redes não será restabelecido.
- Se o endereço IP do gateway remoto for alterado, até mesmo o ID de conexão permanecerá inalterado, a extremidade remota foi alterada. Portanto, a conexão de VPN precisa ser restabelecida.
- Se apenas as chaves pré-compartilhadas da conexão forem alteradas, o ID e o status da conexão permanecerão inalterados. As chaves serão verificadas novamente durante a renegociação. Se as chaves não combinam, a renegociação falha.
- Se a política de negociação for modificada (é necessária a verificação da chave pré-compartilhada), o ID da conexão será alterado e a conexão precisará ser restabelecida.

## 17.6.12 Por que não consigo iniciar uma negociação da Amazon Web Services para a Huawei Cloud depois que elas estão interconectadas?

Depois que uma conexão de VPN é estabelecida, a Amazon Web Services (AWS) trabalha no modo de resposta e não inicia a negociação. Quando um EC2 da AWS acessa um ECS da Huawei Cloud, a conexão de VPN não será acionada para estabelecer uma AS.

De acordo com o documento da AWS, a negociação pode ser iniciada apenas do lado do cliente (neste caso, a Huawei Cloud).

## 17.6.13 Como configurar DPD para interconexão com a Huawei Cloud?

Por padrão, a DPD está ativada na Huawei Cloud e não pode ser desativada.

Configure a DPD da seguinte forma:

- DPD-type: sob demanda
- DPD idle-time: 30s

- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

O formato de **DPD msg** em ambas as extremidades da conexão de VPN deve ser o mesmo, mas o tipo de DPD, o tempo ocioso, o intervalo de retransmissão e o limite de repetição podem ser diferentes.

## 17.6.14 O que fazer se meu firewall não puder receber pacotes de resposta do gateway da VPN da Huawei Cloud na fase IKE?

1. Verifique se os endereços IP públicos das duas extremidades podem se comunicar entre si. Você pode executar o comando ping. Por padrão, o endereço IP do gateway de VPN na Huawei Cloud pode ser pingado.
2. O gateway local e o gateway de VPN da Huawei Cloud podem trocar pacotes nas portas UDP 500 e 4500.
3. Certifique-se de que o número da porta de origem não seja traduzido quando o endereço IP público local acessar o endereço IP do gateway na Huawei Cloud. Se a travessia de NAT existir, certifique-se de que o número da porta não será alterado após a travessia de NAT.
4. As configurações de parâmetro de negociação de IKE em ambas as extremidades devem ser as mesmas. No cenário de travessia de NAT, defina o tipo de ID no data center local como IP e o ID local na Huawei Cloud como o endereço IP público após a NAT.

## 17.6.15 O que fazer se meu firewall não conseguir receber pacotes de resposta da sub-rede da VPN da Huawei Cloud?

1. Verifique as rotas, as políticas de segurança, a configuração de NAT, o tráfego interessante e as políticas de negociação para a negociação da fase 2 no dispositivo de gateway local.
   - Configurações da rota: encaminhe os dados para acessar sub-redes de nuvem para túneis.
   - Políticas de segurança: permita tráfego de sub-redes locais para sub-redes na nuvem.
   - Políticas de NAT: não execute a NAT quando as sub-redes locais acessarem sub-redes da nuvem.
   - Trânsito interessante: o tráfego interessante em ambas as extremidades é configurado na maneira espelhada. O nome do objeto de endereço não pode ser usado para o tráfego interessante configurado usando IKEv2.
   - Políticas de negociação: certifique-se de que as políticas de negociação, especialmente o PFS, em ambas as extremidades sejam as mesmas.
2. Após ter confirmado que as negociações da fase 1 e da fase 2 são normais, assegure-se de que as regras do grupo de segurança na nuvem permitam que as sub-redes locais acessem as sub-redes da nuvem usando ICMP.

## 17.6.16 Quais são os bits dos grupos DH usados pela VPN da Huawei Cloud?

Os grupos Diffie-Hellman (DH) determinam a força da chave usada no processo de troca de chaves. Números de grupo DH mais altos são geralmente mais seguros, mas é necessário tempo extra para calcular a chave.

**Tabela 17-5** lista os bits correspondentes aos grupos de DH usados pela VPN.

**Tabela 17-5** Bit correspondente a cada grupo DH

| Grupo DH | Módulo |
| --- | --- |
| 1 | 768 bits |
| 2 | 1024 bits |
| 5 | 1536 bits |
| 14 | 2048 bits |
| 15 | 3072 bits |
| 16 | 4096 bits |
| 19 | ecp256 bits |
| 20 | ecp384 bits |
| 21 | ecp521 bits |

NOTA

Os seguintes algoritmos de DH têm riscos de segurança e não são recomendados: DH group 1, DH group 2 e DH group 5.

# 17.7 Falha de conexão ou ping

## 17.7.1 Por que a conexão de VPN está sempre no estado Not Connected depois que sua configuração é concluída?

Certifique-se de que as chaves pré-compartilhadas e as informações de negociação em ambas as extremidades sejam consistentes. As sub-redes locais e o gateway de VPN na nuvem são as sub-redes remotas e o gateway remoto no data center local. O gateway remoto e as sub-redes remotas na nuvem são o gateway local e as sub-redes locais no data center local.

Certifique-se de que as regras de rotas, NAT e política de segurança estão corretamente configuradas no dispositivo de gateway local. Em seguida, faça ping nos servidores em sub-redes em ambas as extremidades.

NOTA

A VPN é acionada com base em fluxos de dados. Depois que você configura a VPN, sibile um dispositivo na sub-rede do par. Antes de executar o comando ping, desabilite a função de firewall no dispositivo e permita pacotes ICMP de entrada no grupo de segurança na nuvem.

O ping do endereço IP do gateway não pode acionar a negociação de VPN. Efetue o ping do servidor na sub-rede protegida pelo gateway.

## 17.7.2 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- ACLs dos dispositivos em ambas as extremidades da conexão de VPN não coincidem.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são diferentes.
- A DPD não está configurada no data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Os pacotes são fragmentados porque o tamanho dos dados excede a MTU.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- As sub-redes locais e remotas são pares correspondentes.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- A DPD está ativada no dispositivo de gateway local e o número de vezes de detecção é 5 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do gateway local é grande o suficiente para ser usada pela conexão de VPN.
- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.
- Faça ping nas sub-redes em ambas as extremidades continuamente. O script é o seguinte:

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
```

```
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Use o editor vi para copiar o script anterior para o arquivo **ping.sh**.
2. Execute o comando **chmod 777 ping.sh** para conceder permissões ao arquivo.
3. Execute o comando ping:

   **./ping.sh** *x.x.x.x* **>>/dev/null &**

   *x.x.x.x* indica o endereço IP a ser pingado.
4. Execute o seguinte comando:

   **tail -f** *x.x.x.x***.log**

   Você pode ver o resultado do ping em tempo real.

# 17.7.3 Como restaurar rapidamente uma conexão de VPN IPsec interrompida?

1. Acione negociação de IPsec por fluxos de dados de rede privada. Por exemplo, duas redes privadas em ambas as extremidades da conexão de VPN fazem ping entre si. Se o tráfego puder ser acionado corretamente, implemente um script de ping contínuo. Para mais detalhes, consulte **Como evitar desconexões de VPN?**.
2. Se a negociação não puder ser acionada, verifique a conectividade com a Internet pingando o endereço IP do gateway de VPN e o endereço IP do gateway remoto. Por padrão, o gateway de VPN da Huawei Cloud responde a pacotes ICMP.
3. Se a Internet for normal, verifique se ocorre uma troca de link entre vários gateways. Ou seja, o tráfego para acessar o endereço IP do gateway da Huawei Cloud não flui para fora das portas negociadas.
4. Se não houver várias portas ou se o caminho da porta for normal, altere as PSKs nas duas extremidades do túnel para acionar a negociação novamente.
5. Se a negociação falhar, verifique se as políticas de negociação configuradas em ambas as extremidades são consistentes e se o tráfego interessante em ambas as extremidades é espelhado mutuamente.
6. Se as políticas de negociação e a configuração de tráfego interessantes estiverem corretas, desative a conexão de VPN no dispositivo local. Depois que o estado da conexão na Huawei Cloud mudar para **Not connected**, redefina a conexão de VPN no dispositivo local e acione um fluxo de dados.
7. Se a negociação ainda não puder ser acionada, execute as seguintes operações:
   a. Registre a política de negociação, PSK, sub-redes locais, gateway remoto e sub-redes remotas da conexão de VPN da Huawei Cloud.
   b. Use o gateway de VPN existente para criar outra conexão de VPN. A política de negociação, PSK e sub-redes locais são as mesmas da conexão de VPN original. Configure aleatoriamente o gateway remoto e as sub-redes remotas.
   c. Depois que a nova conexão de VPN for criada, exclua a conexão de VPN original e altere o gateway remoto e as sub-redes remotas da nova conexão de VPN para as informações gravadas.

d. Acione a negociação novamente.

Se o status do túnel IPsec ainda for anormal após você executar as operações anteriores, **envie um tíquete de serviço** para o atendimento ao cliente da Huawei Cloud para obter ajuda.

## 17.7.4 O que acontece se a largura de banda de um gateway de VPN exceder o tamanho especificado ao criar o gateway?

A largura de banda do gateway de VPN é usada na direção de saída de uma VPC. Se a largura de banda exceder o tamanho especificado, ocorrerá congestionamento da rede, algumas sub-redes não poderão ser acessadas ou até mesmo a conexão de VPN será interrompida, porque os pacotes de detecção de VPN podem não ser recebidos.

Neste caso, é aconselhável aumentar a largura de banda do gateway de VPN.

NOTA

A largura de banda máxima de uma conexão de VPN é de 300 Mbit/s.

## 17.7.5 Uma conexão de VPN IPsec será estabelecida automaticamente?

Depois de concluir as configurações em ambas as extremidades de uma conexão de VPN IPsec, a conexão de VPN não será estabelecida automaticamente somente após os fluxos de dados entre as duas extremidades da conexão. Se nenhum fluxo de dados entre a nuvem e o data center local, a conexão de VPN estará sempre no estado inativo. Quaisquer dados gerados pelo acesso a servidores ou pelo ping entre servidores podem acionar o estabelecimento de uma conexão de VPN.

O estabelecimento de uma conexão de VPN pode ser acionado em uma das duas condições a seguir: o gateway de VPN e o gateway remoto disparam automaticamente a negociação. Os servidores em nuvem e locais acedem uns aos outros através da conexão de VPN a estabelecer.

No entanto, o estabelecimento automático de uma conexão de VPN não pode ser acionado por um gateway de VPN na Huawei Cloud. Verifique se o estabelecimento de sua conexão de VPN pode ser acionado pelos fluxos de dados entre as duas extremidades da conexão de VPN. Ou seja, verifique se é possível estabelecer uma conexão de VPN depois de efetuar um ping a um servidor na nuvem a partir de um servidor no local e se é possível estabelecer uma conexão de VPN depois de desligar a conexão e efetuar um ping a um servidor no local a partir de um servidor na nuvem.

NOTA

Os endereços de origem e destino dos pacotes de ping devem ser protegidos pela VPN.

Antes que uma conexão de VPN seja estabelecida, os endereços IP do gateway em ambas as extremidades podem ser pingados. No entanto, o ping dos endereços IP do gateway não aciona o estabelecimento da conexão de VPN.

## 17.7.6 Por que os ECSs em ambas as extremidades de uma conexão de VPN normal entre regiões não podem acessar um ao outro?

Por padrão, um grupo de segurança permite todo o tráfego de saída. Para permitir tráfego de entrada, adicione regras de entrada ao grupo de segurança. Certifique-se de que o grupo de

segurança associado ao ECS que precisa receber pacotes de ping permita solicitações ICMP de entrada.

## 17.7.7 Por que as sub-redes em ambas as extremidades de uma conexão de VPN normal não podem acessar umas às outras?

A conexão de VPN está normal, indicando que os parâmetros de negociação em ambas as extremidades da conexão de VPN estão corretos. Você precisa executar as seguintes operações:

- Verifique se as rotas para o dispositivo de VPN em seu data center local estão configuradas corretamente.
- Verifique se a troca de dados entre sub-redes é permitida no dispositivo de VPN.
- Verifique se a NAT não é executada nas sub-redes locais que precisam acessar a nuvem.
- Verifique se o acesso mútuo entre os endereços IP públicos do gateway de VPN e do gateway do cliente é permitido.

## 17.7.8 O que fazer se uma conexão de VPN em uso for interrompida e uma mensagem for exibida indicando que o tráfego de endereços IP não incluídos na lista branca é gerado?

Isso geralmente é causado pela incompatibilidade de ACL entre os gateways local e remoto.

1. Verifique se as sub-redes locais e remotas da conexão de VPN são pares correspondentes. Certifique-se de que as regras da ACL em ambas as extremidades da conexão de VPN não entrem em conflito.
2. Use o formato de sub-rede/máscara ao configurar tráfego interessante em seu data center local. Não use o modo de objeto de endereço, pois ele pode causar problemas de incompatibilidade.

## 17.7.9 O que fazer se uma conexão de VPN for interrompida e uma mensagem for exibida indicando que o tempo limite de DPD?

Isso acontece porque não há troca de dados por meio da conexão de VPN. Após o término do ciclo de vida da AS, a conexão de VPN será excluída se a extremidade do par não responder à DPD.

**Solução**

1. Ative a DPD no dispositivo de gateway local e verifique se os fluxos de dados de ambas as extremidades podem acionar o estabelecimento de conexão.
2. Implemente o script de shell de ping nos servidores em ambas as extremidades. Você também pode configurar o dispositivo de gateway local para manter a conexão ativa, por exemplo, configurar NQA em dispositivos da Huawei ou IP SLA em dispositivos de Cisco. A Análise de qualidade de rede (NQA) é um recurso da Huawei que monitora o desempenho da rede em tempo real e ajuda a diagnosticar falhas que ocorrem na rede.

# 17.7.10 Por que o status de uma conexão de VPN é Not Connected no console de gerenciamento quando ele já está disponível?

Há uma latência para exibir o status de conexão de VPN mais recente no console de gerenciamento.

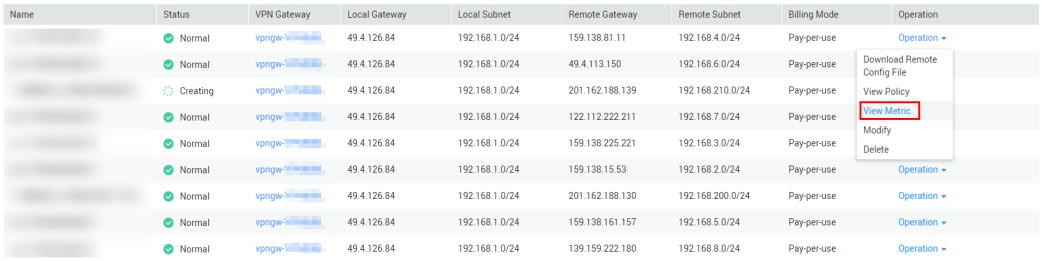
Se o acesso ao serviço for normal, a conexão de VPN é estabelecida.

# 17.7.11 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme automaticamente para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Depois que uma conexão de VPN for criada, você poderá localizar a linha que contém a conexão VPN e escolher **Operation** > **View Metric** para exibir o status da conexão de VPN.

**Figura 17-21** Ver métricas




# 17.7.12 O que fazer se a configuração da conexão de VPN falhar?

1. Verifique as políticas de IKE e IPsec para ver se os modos de negociação e os algoritmos de criptografia em ambas as extremidades da conexão de VPN são os mesmos.
   a. Se a política de IKE tiver sido configurada durante a primeira fase e a política de IPsec não tiver sido ativada na segunda fase, as políticas de IPsec em ambas as extremidades da conexão de VPN poderão ser inconsistentes.
   b. Se você usa um dispositivo físico de Cisco em seu data center local, recomenda-se que você use MD5 e defina **Authentication Mode** como **MD5** ao configurar a política de IPsec para a conexão de VPN na nuvem.
2. Verifique se as regras de ACL estão corretas.

   Se as sub-redes do data center local forem 192.168.3.0/24 e 192.168.4.0/24, e as sub-redes da VPC forem 192.168.1.0/24 e 192.168.2.0/24, configurar as regras de ACL para cada sub-rede local para permitir a comunicação com as sub-redes da VPC. O seguinte fornece um exemplo de configurações de ACL:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0
   0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0
   0.0.0.255
   ```
3. Verifique se a conexão de VPN está normal pingando a extremidade local a partir da extremidade remota e pingando a extremidade remota a partir da extremidade local.

## 17.7.13 O que fazer se não conseguir acessar os ECSs na nuvem a partir do meu data center ou LAN local após a conexão de VPN ter sido configurada?

Por predefinição, o grupo de segurança nega o acesso a todas as origens. Se você quiser acessar seus ECSs, modifique as regras do grupo de segurança e permita o acesso das sub-redes locais.

## 17.7.14 Por que Not Connected exibido como o status de uma conexão de VPN criada com êxito?

Depois que uma conexão de VPN é criada, seu status muda para **Normal** somente depois que os servidores em ambas as extremidades da conexão de VPN se comunicam uns com os outros.

- IKE v1:

  Se nenhum tráfego passar pela conexão de VPN por um período de tempo, a conexão de VPN precisa ser renegociada. O tempo de negociação depende do valor do **Lifecycle (s)** na política de IPsec. Geralmente, **Lifecycle (s)** é definido como **3600** (1 hora), indicando que a negociação será iniciada no quinquagésimo quarto minuto. Se a negociação for bem-sucedida, a conexão permanece para a próxima rodada de negociação. Se a negociação falhar, o status da conexão de VPN será alterado para **Not Connected** dentro de uma hora. A conexão pode ser restaurada somente após as duas extremidades da conexão de VPN se comunicarem uma com a outra. A desconexão pode ser evitada usando uma ferramenta de monitoramento de rede, como IP SLA, para gerar pacotes.
- IKE v2: se nenhum tráfego passar pela conexão de VPN por um período de tempo, a conexão de VPN permanecerá no status conectado.

## 17.7.15 As VPNs da Huawei Cloud têm o mecanismo de DPD ativado?

Sim.

As VPNs da Huawei Cloud têm o mecanismo de DPD ativado por padrão para detectar o status do processo de IKE no data center local.

Após três falhas de detecção consecutivas, a Huawei Cloud considera que o processo de IKE no data center local é anormal. Nesse caso, a Huawei Cloud exclui o túnel local para garantir a sincronização do túnel entre as duas extremidades.

O protocolo de DPD não exige que a extremidade do par esteja configurada de forma síncrona, mas exige que a extremidade do par possa responder às detecções de DPD. Para garantir que o status do túnel das duas extremidades seja consistente e evitar que uma extremidade tenha um túnel e a outra não, é recomendável ativar o mecanismo de DPD no gateway local para detectar o status do processo de IKE do serviço VPN na Huawei Cloud.

**NOTA**

Depois que DPD falhar, o túnel será excluído sem afetar a estabilidade do serviço.

DPD pode detectar exceções no processo IKE na extremidade do par no tempo e redefinir o túnel para garantir a sincronização do túnel entre as duas extremidades. Depois que um túnel é excluído, se houver tráfego transmitido pelo túnel, o túnel poderá ser restabelecido por meio da negociação.

# 17.8 EIPs

## 17.8.1 Um endereço IP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Não. O endereço IP do gateway de VPN será liberado depois que o gateway de VPN for excluído.

A exclusão de um gateway de VPN também excluirá os recursos associados ao gateway.

AVISO

A exclusão da última conexão de um gateway de VPN pagamento por uso também excluirá o gateway. Se você quiser manter o endereço IP, não exclua a última conexão de VPN.

## 17.8.2 Um EIP pode ser usado como um endereço IP de gateway de VPN?

Não.

O endereço IP de um gateway de VPN é de configurações predefinidas e é atribuído automaticamente quando o gateway de VPN é criado. Um EIP não pode ser usado por um gateway de VPN.

## 17.8.3 Preciso comprar EIPs para servidores que se comunicam uns com os outros por meio de uma VPN?

Se o servidor local precisar acessar um ECS na nuvem por meio de uma VPN, você não precisará adquirir um EIP.

Se o ECS precisar fornecer serviços acessíveis pela Internet, será necessário um EIP.

## 17.8.4 Por que um ECS tem informações de acesso de EIP depois que habilitar uma VPN?

Isso ocorre porque o ECS tem um EIP vinculado antes que a VPN seja usada. Ou seja, você pode acessar o ECS por meio da VPN ou do EIP.

Depois que a VPN é estabelecida, o tráfego de servidores que atendem às regras da ACL pode entrar no túnel para acessar ECSs.

- Se um EIP estiver vinculado a um ECS, os dispositivos em uma rede não VPN poderão acessar o ECS usando o EIP.
- Se o ECS puder ser acessado somente por meio de uma VPN, desvincule o EIP do ECS depois que a conexão de VPN estiver ativa. Quando um ECS precisa de um EIP, você pode usar regras de ACL para especificar o tráfego que pode acessar o ECS por meio do EIP.

NOTA

Manter um EIP ou não depende dos seus serviços. Se um ECS for usado para acessar um data center local por meio de uma VPN e também for usado para fornecer serviços acessíveis pela Internet, seu EIP precisará ser mantido.

### 17.8.5 Meu gateway local pode não ter endereço IP público fixo?

Não.

Para conectar seu data center local à Huawei Cloud por meio de uma VPN, seu data center local deve ter um endereço IP público fixo ou um endereço IP público fixo após o NAT.

NOTA

Roteadores de banda larga domésticos comuns, terminais móveis pessoais e serviços VPN (como L2TP) fornecidos por hosts de Windows não podem se interconectar com a VPN da Huawei Cloud.

## 17.9 Configurações da rota

### 17.9.1 O que é um gateway remoto e uma sub-rede remota em uma conexão de VPN?

Ao criar uma conexão de VPN, uma sub-rede na VPC da Huawei Cloud é a sub-rede local e o gateway de VPN criado é o gateway local. A sub-rede e o gateway conectados no data center local são a sub-rede remota e o gateway remoto.

Um endereço IP de gateway remoto é um endereço IP público.

### 17.9.2 Onde posso adicionar rotas no console da VPN para alcançar as sub-redes remotas?

Quando uma conexão de VPN é criada, as rotas são entregues automaticamente para alcançar as sub-redes remotas.

### 17.9.3 Preciso adicionar uma rota para um ECS com várias NICs para alcançar a rede local?

- Se uma NIC primária for usada para estabelecer uma VPN com a rede local, nenhuma rota precisará ser adicionada.
- Se uma NIC não primária for usada para estabelecer uma VPN com a rede local, adicione uma rota para alcançar o gateway da NIC não primária.

## 17.10 Configuração de sub-rede

## 17.10.1 Quais são as precauções para configurar as sub-redes locais e remotas de uma conexão de VPN?

- Você pode configurar até 5 sub-redes locais. O produto do número de sub-redes locais e do número de sub-redes remotas não pode exceder 225. Se 225 é excedido, considere supernetting as sub-redes locais ou remotas.
- A sub-rede local não pode incluir o bloco CIDR da sub-rede remota. A sub-rede remota pode incluir o bloco CIDR da sub-rede local.
- Há rotas que apontam para as sub-redes locais na VPC onde o gateway de VPN reside.
- Se houver duas conexões (conexão A e conexão B) criadas para um gateway de VPN, e a sub-rede remota da conexão A estiver dentro da conexão B, quando a rede de destino a ser acessada pertencer ao bloco CIDR sobreposto, a conexão criada primeiro será correspondida primeiro, independentemente do status da conexão. (A correspondência de comprimento da máscara não é usada para a VPN baseada em políticas.)

## 17.10.2 Quantas sub-redes locais e remotas posso adicionar a uma VPN? Por que uma mensagem de erro é exibida quando atualizo a sub-rede local especificando um bloco CIDR?

- Você pode configurar até 5 sub-redes locais. O produto do número de sub-redes locais e do número de sub-redes remotas não pode exceder 225.
- Uma VPC fornece rotas de sub-rede VPC com base em sub-redes remotas de uma conexão VPN, sub-redes remotas de uma conexão Direct Connect, sub-redes de uma conexão de emparelhamento de VPC e sub-redes de uma conexão Cloud Connect. Cada sub-rede tem uma rota.
- O número de rotas de sub-rede da VPC não pode exceder 200. Ou seja, em uma VPC, o número total de sub-redes remotas de uma conexão VPN, sub-redes remotas de uma conexão Direct Connect, sub-redes de uma conexão de emparelhamento de VPC e sub-redes de uma conexão Cloud Connect e rotas personalizadas não podem exceder 200.

## 17.10.3 O que fazer se ocorrer uma exceção quando adicionar uma sub-rede remota durante a criação da conexão de VPN?

Verifique se essa sub-rede remota foi usada como destino de uma rota de conexão de emparelhamento de VPC, Cloud Connect ou Direct Connect, o que causa conflitos de rota. Se sim, exclua a rota e crie uma nova.

## 17.10.4 Um endereço IP de um gateway de VPN pode ser retido após o gateway de VPN ser excluído?

Não. O endereço IP do gateway de VPN será liberado depois que o gateway de VPN for excluído.

A exclusão de um gateway de VPN também excluirá os recursos associados ao gateway.

**AVISO**

A exclusão da última conexão de um gateway de VPN pagamento por uso também excluirá o gateway. Se você quiser manter o endereço IP, não exclua a última conexão de VPN.

## 17.10.5 Como planejar o bloco CIDR de uma VPC acessada por uma conexão de VPN?

- O bloco CIDR da VPC não pode entrar em conflito com o bloco CIDR local.
- Para evitar conflitos com endereços de serviço de nuvem, não use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3 ou 100.64.0.0/10 para sua rede local.

## 17.10.6 Como um endereço IP de gateway de VPN é alocado?

O endereço IP do gateway de VPN da Huawei Cloud é um grupo de endereços IP planejados antes da aquisição dos gateways de VPN. Esses endereços IP são predefinidos com configurações de VPN.

Quando você compra um gateway de VPN, o sistema atribui aleatoriamente um endereço IP e o vincula à VPC selecionada. Esse endereço IP pode ser vinculado a apenas uma VPC.

O endereço IP do gateway de VPN tem dados predefinidos. Portanto, não é intercambiável com um EIP e você não pode especificar um EIP como o endereço IP do gateway de VPN quando estiver comprando o gateway de VPN. O endereço IP do gateway de VPN só pode ser atribuído aleatoriamente a partir do pool de endereços IP de VPN predefinido. Quando um gateway de VPN é excluído, a relação de vinculação entre o endereço IP do gateway e a VPC do gateway é liberada. Quando um novo gateway de VPN é comprado, o sistema aloca aleatoriamente um novo endereço IP de gateway.

# 17.11 Tráfego interessante da VPN

## 17.11.1 Preciso configurar regras de ACL no console de gerenciamento da Huawei Cloud após configurar regras de ACL no dispositivo de gateway local?

Você precisa criar regras de ACL dedicadas para seu dispositivo de gateway local. As regras da ACL serão referenciadas pelas políticas de IPsec.

Quando você configura a VPN na nuvem, as regras de ACL serão geradas automaticamente com base nas sub-redes locais e remotas inseridas no console de gerenciamento e, em seguida, entregues ao gateway de VPN.

(Huawei Cloud) O número de regras da ACL = o número de sub-redes locais x o número de sub-redes remotas

## 17.11.2 Como configurar e modificar o tráfego interessante de uma VPN na nuvem?

O tráfego interessante é gerado quando a sub-rede local e a sub-rede remota se comunicam usando a topologia de malha completa. Por exemplo, existem duas sub-redes locais A e B e três sub-redes remotas C, D e E. As regras de ACL para o tráfego interessante são as seguintes:

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
```

```
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

Se você modificar a sub-rede local e a sub-rede remota no console de gerenciamento, o tráfego interessante do dispositivo de VPN será atualizado automaticamente. Ou seja, as regras de ACL na nuvem são modificadas.

# 17.12 Manutenção da conexão de VPN ativa

## 17.12.1 Como evitar desconexões de VPN?

As conexões de VPN são renegociadas quando a vida útil da AS do IPsec está prestes a expirar ou quando os dados transmitidos por meio de uma conexão de VPN excedem 20 GB. Normalmente, a renegociação não interrompe as conexões de VPN.

A maioria das desconexões são causadas por configurações incorretas nas duas extremidades da conexão de VPN ou falhas de renegociação devido a exceções da Internet.

As causas comuns de desconexões são as seguintes:

- ACLs dos dispositivos em ambas as extremidades da conexão de VPN não coincidem.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são diferentes.
- A DPD não está configurada no data center local.
- A configuração é modificada quando a conexão de VPN está em uso.
- Os pacotes são fragmentados porque o tamanho dos dados excede a MTU.
- Tremulação ocorre na rede da operadora.

Como tal, certifique-se de que as seguintes configurações de VPN estejam corretas para manter as conexões de VPN ativas:

- As sub-redes locais e remotas são pares correspondentes.
- As configurações de vida útil da AS em ambas as extremidades da conexão de VPN são as mesmas.
- A DPD está ativada no dispositivo de gateway local e o número de vezes de detecção é 5 ou mais.
- Os parâmetros são modificados em ambas as extremidades da conexão de VPN durante o uso da conexão de VPN.
- Defina TCP MAX-MSS como 1300 para o dispositivo de gateway local.
- A largura de banda do gateway local é grande o suficiente para ser usada pela conexão de VPN.
- A negociação da conexão de VPN pode ser acionada por ambas as extremidades e a negociação ativa foi habilitada no dispositivo de gateway local.
- Faça ping nas sub-redes em ambas as extremidades continuamente. O script é o seguinte:

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"
```

```
while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Use o editor vi para copiar o script anterior para o arquivo **ping.sh**.
2. Execute o comando **chmod 777 ping.sh** para conceder permissões ao arquivo.
3. Execute o comando ping:

   **./ping.sh** *x.x.x.x* **>>/dev/null &**

   *x.x.x.x* indica o endereço IP a ser pingado.
4. Depois que o comando ping é executado, o arquivo *x.x.x.x***.log** é gerado. Execute o seguinte comando:

   **tail -f** *x.x.x.x***.log**

   Você pode ver o resultado do ping em tempo real.

# 17.13 Monitoramento

## 17.13.1 Quais recursos de VPN podem ser monitorados?

**Gateway de VPN**

As informações de largura de banda que podem ser monitoradas incluem tráfego de entrada, largura de banda de entrada, tráfego de saída, largura de banda de saída e uso de largura de banda de saída.

Para exibir as métricas do gateway de VPN, localize o gateway de VPN de destino e clique em **View Metric** na coluna **Operation**.

**Conexão de VPN**

O status da conexão de VPN pode ser monitorado.

O valor **1** indica que a conexão é normal.

O valor **0** indica que a conexão não está conectada.

Para exibir o status da conexão de VPN, localize a conexão de VPN de destino e clique em **View Metric** na coluna **Operation**.

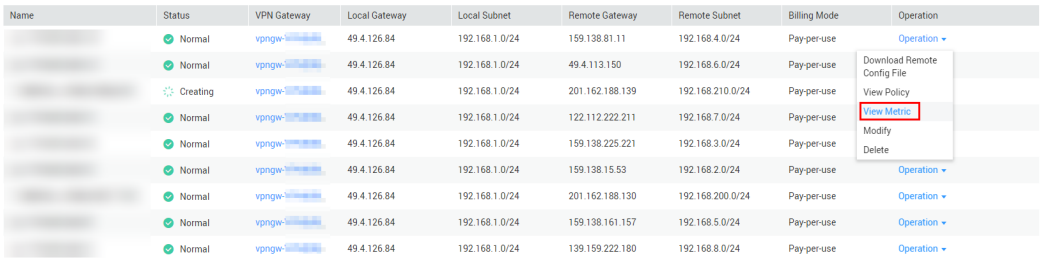
## 17.13.2 Será notificado se uma conexão de VPN for interrompida?

O status da conexão de VPN pode ser monitorado. Depois que uma conexão de VPN é criada, o serviço VPN relata as informações de status da conexão para o Cloud Eye, mas não envia notificações de alarme automaticamente para você. Para receber notificações, crie regras de alarme e ative **Alarm Notification** no console do Cloud Eye.

Depois que uma conexão de VPN for criada, você poderá localizar a linha que contém a conexão de VPN e escolher **Operation** > **View Metric** para exibir o status da conexão de VPN.

**Figura 17-22** Ver métrica




## 17.13.3 Posso ver o tráfego de cada conexão de VPN?

Não. O monitoramento de tráfego de VPN é sobre o gateway de VPN. Você pode visualizar o tráfego de entrada e saída, bem como as larguras de banda de entrada e saída de um gateway de VPN, mas não pode visualizar o uso de tráfego de uma conexão de VPN específica.

## 17.13.4 Será notificado quando o resultado do monitoramento de VPN for anormal?

Sim.

Você pode configurar, nos consoles de Simple Message Notification (SMN) e Cloud Eye, para receber notificações se ocorrerem resultados anormais de monitoramento de VPN.

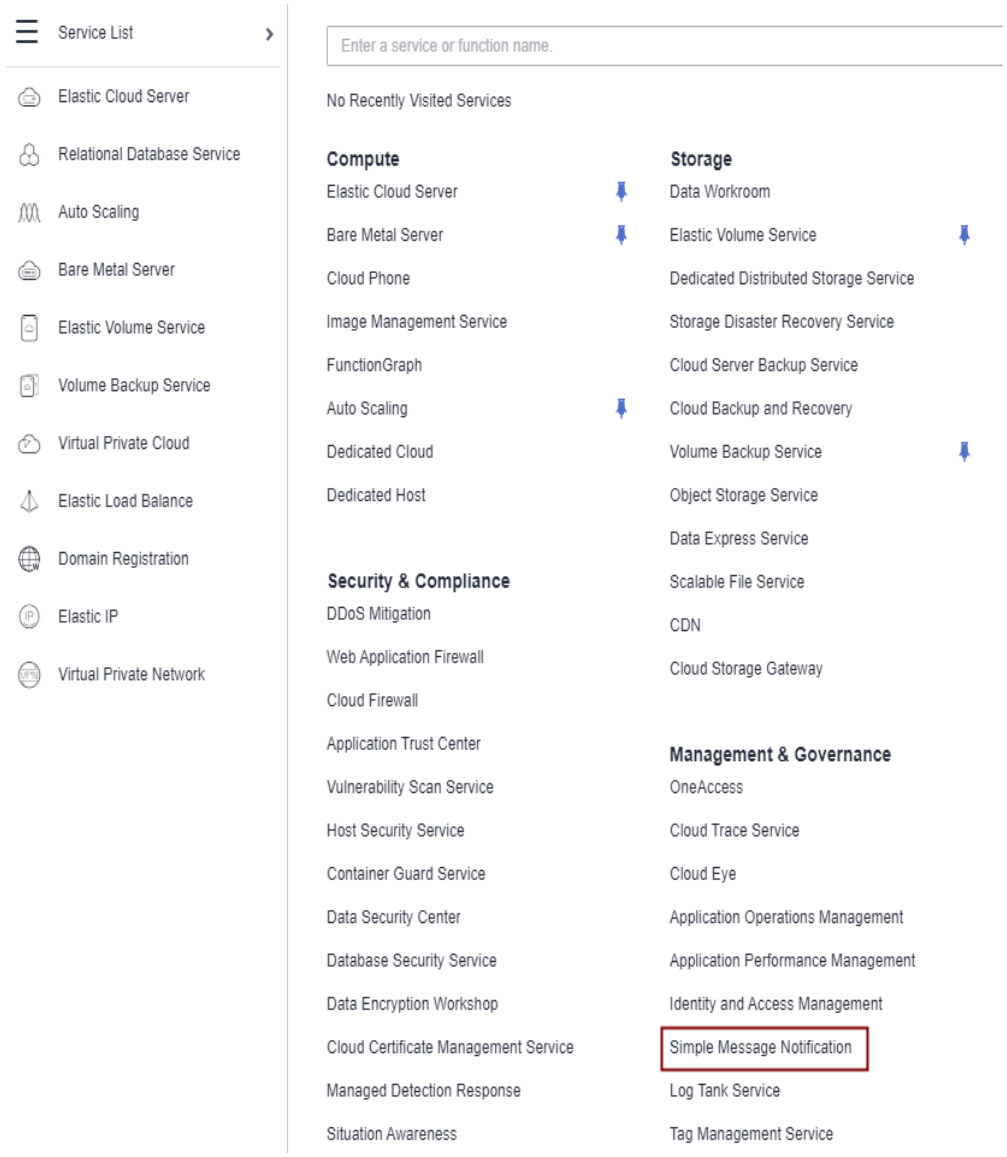
### Criar tópicos e adicionar assinaturas no console de SMN

1. Faça logon no console de gerenciamento.

   Em **Management & Governance**, selecione **Simple Message Notification**.

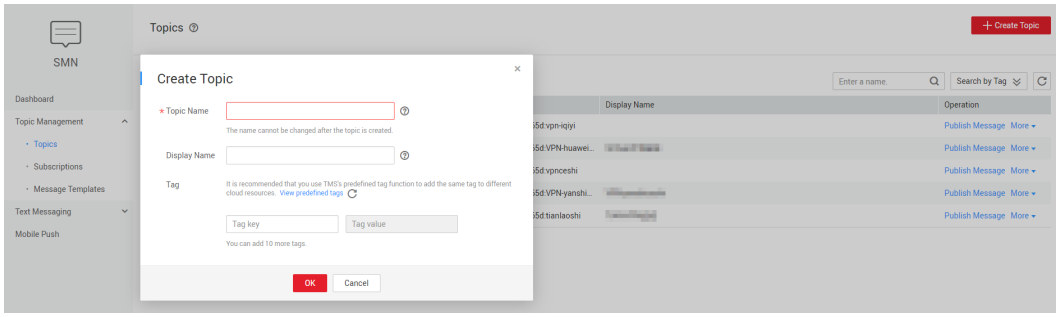
  

**Figura 17-23** Simple Message Notification




2. Escolha **Topic Management** > **Topics** e clique em **Create Topic** para criar um tópico, por exemplo, **VPN-huaweicloud**.

**Figura 17-24** Criar tópico

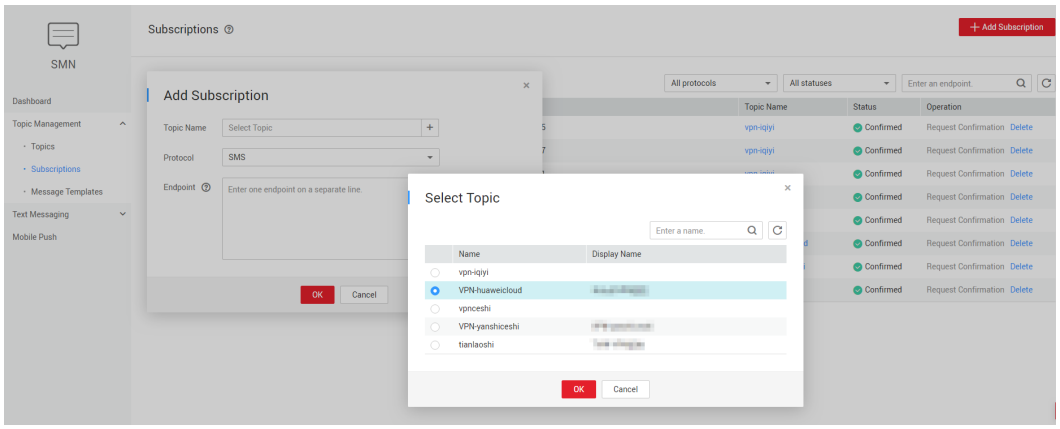



3. Escolha **Topic Management** > **Subscriptions** e clique em **Add Subscription**.

   Selecione um tópico, defina **Protocol** como **Email** e insira um endereço de e-mail para receber notificações de alarme na caixa **Endpoint**.

**Figura 17-25** Adicionar assinatura




**NOTA**

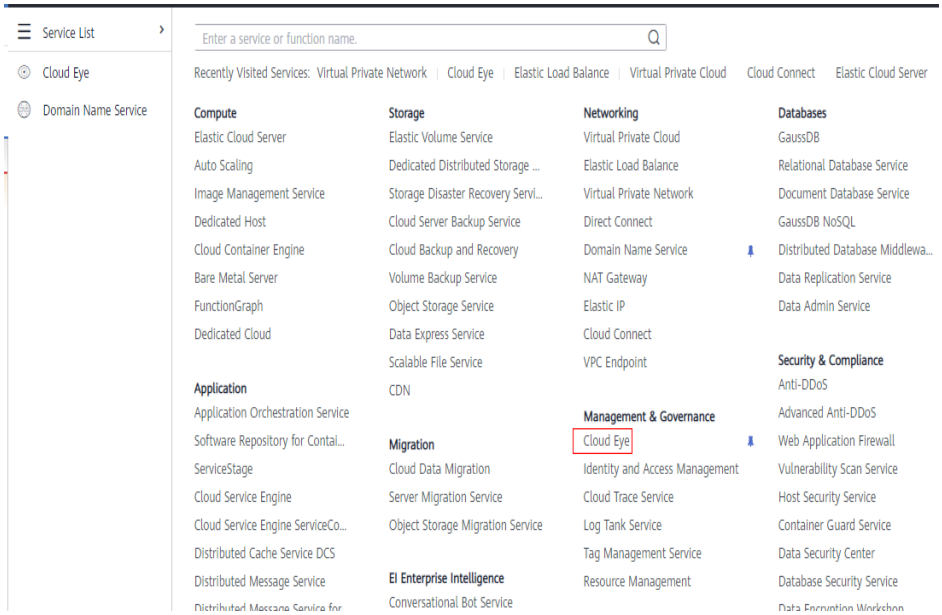
Depois que a assinatura for adicionada, o sistema enviará um e-mail de confirmação para o seu endereço de e-mail. Confirme a assinatura no seu e-mail.

## Criar regras de alarme de VPN no console do Cloud Eye

1. Faça logon no console de gerenciamento.

   Em **Management & Governance**, selecione **Cloud Eye**.

**Figura 17-26** Cloud Eye




2. Crie uma regra de alarme para monitorar o uso de largura de banda de um gateway de VPN.

   Digite um nome de regra de alarme, selecione **Elastic IP and Bandwidth** para **Resource Type**, defina **Dimension** para **Bandwidths**, **Monitoring Scope** para **Specific resources** e selecione o gateway de VPN de destino, defina **Method** para **Create manually** e **Alarm Policy** para **Outbound Bandwidth Usage**, **5 consecutive periods**, **>** e **90**. Defina **Notification Object** como um tópico de SMN e use as configurações padrão para outros parâmetros.

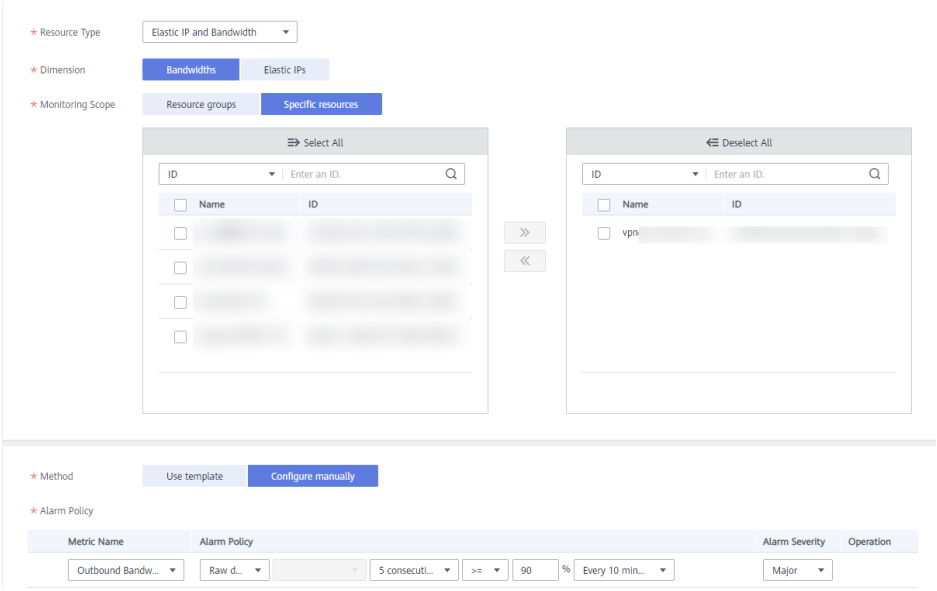
3. Crie uma regra de alarme para monitorar o status da conexão de VPN.

   O processo de criação é semelhante ao da largura de banda. Selecione **Virtual Private Network** para **Resource Type**, defina **Dimension** para **VPN connections**, **Monitoring Scope** para **Specific resources** e selecione a conexão de VPN de destino, defina **Method** para **Create manually** e **Alarm Policy** para **VPN Connection Status**, **<** e **1**. Defina **Notification Object** como um tópico de SMN e use as configurações padrão para outros parâmetros.

4. Crie uma regra de alarme para monitorar seus links locais.

   Crie uma tarefa de monitoramento de sites, defina **Type** para **PING**, **URL** para o endereço IP do gateway do data center local e mantenha as configurações padrão para outros parâmetros. Crie uma regra de alarme, selecione **Website Monitoring** para **Resource Type**, defina **Monitoring Scope** para **Specific resources** e selecione a tarefa de monitoramento de site de destino, defina **Method** para **Create manually** e **Alarm Policy** para **Available Monitoring Location Count** e configure outros parâmetros conforme necessário. Defina **Notification Object** como um tópico de SMN e use as configurações padrão para outros parâmetros.

**Figura 17-27** Criar uma regra de alarme




# 17.14 Largura de banda e velocidade da rede

## 17.14.1 Qual é a velocidade de rede real de uma conexão de VPN?

Uma conexão de VPN foi criada. Dois ECSs foram criados com um na extremidade local e outro na extremidade remota. Os dois ECSs podem fazer ping um ao outro.

**Execute as etapas a seguir para testar a velocidade da rede do gateway de VPN se a largura de banda do gateway de VPN for de 200 Mbit/s:**

1. Se os ECSs nas duas extremidades da VPN executarem o Windows, use iPerf3 e FileZilla (uma aplicação FTP gratuito para upload e download de arquivos) para testar a velocidade da rede.

> **NOTA**
>
> O teste mostra que a velocidade média da rede da VPN é de 180 Mbit/s, e há cerca de 10% de desvio de velocidade da rede. Os protocolos TCP e FTP têm o mecanismo de controle de congestionamento e o protocolo IPsec adiciona um novo cabeçalho de IP. Portanto, cerca de 10% de desvio de velocidade da rede é normal para a rede VPN.

**Figura 17-28** mostra o resultado do teste.

**Figura 17-28** Resultado do teste para largura de banda de 200 Mbit/s (cliente de iPerf3)

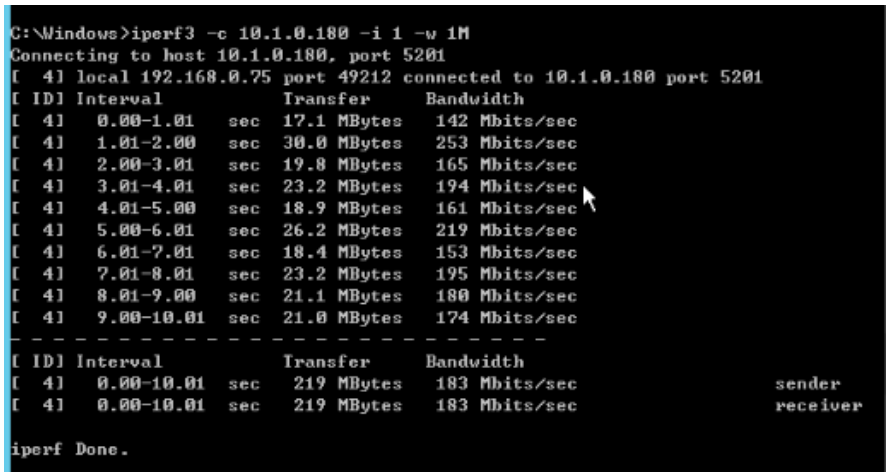
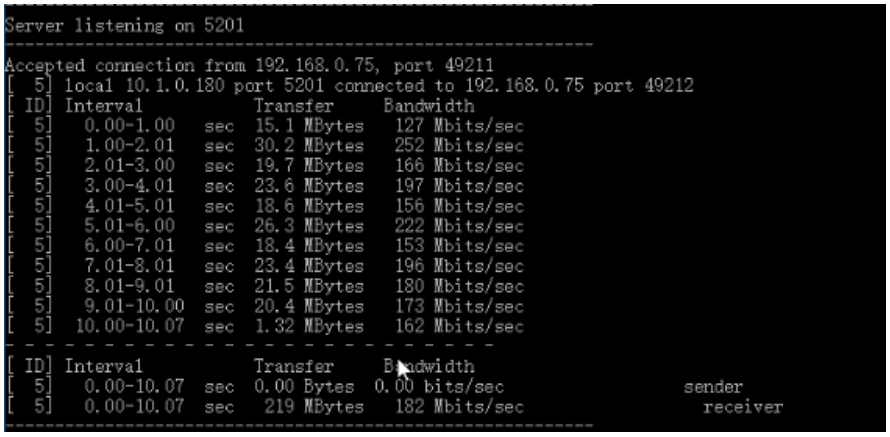



**Figura 17-29** mostra o resultado do teste.

**Figura 17-29** Resultado do teste para largura de banda de 200 Mbit/s (servidor de iPerf3)



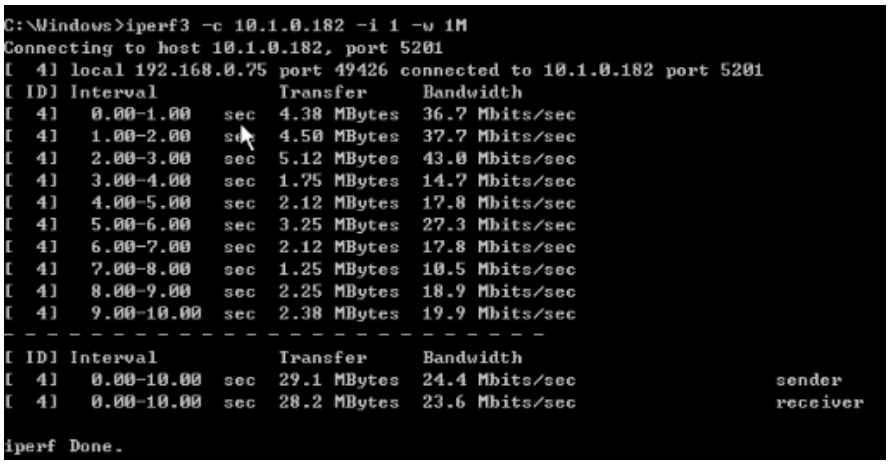

2. Se os ECSs nas duas extremidades da VPN executarem o CentOS 7, use o iPerf3 para testar a velocidade da rede. A velocidade da rede pode chegar a 180 Mbit/s.
3. Se o ECS estiver funcionando como o servidor executar o CentOS 7 e o cliente executar o Windows, use iPerf3 e FileZilla para testar a velocidade da rede.

   A velocidade da rede é de cerca de 20 Mbit/s, uma velocidade de rede lenta. Isso porque as implementações de TCP no Windows e no Linux são diferentes. Portanto, se os ECSs nas duas extremidades da VPN executarem sistemas operacionais diferentes, a velocidade da rede de VPN não atenderá aos requisitos de largura de banda.

   **Figura 17-30** mostra o resultado do teste.

**Figura 17-30** Resultado do teste quando os ECSs nas duas extremidades executam sistemas operacionais diferentes (iPerf3)




**Execute as etapas a seguir para testar a velocidade da rede do gateway de VPN se a largura de banda do gateway de VPN for de 1.000 Mbit/s:**

A largura de banda do gateway de VPN é compartilhada por todas as suas conexões de VPN. Se o tamanho da largura de banda for grande, vários ECSs serão necessários para testar a largura de banda do gateway de VPN porque o desempenho de encaminhamento de um ECS é limitado. Esse cenário tem altos requisitos nas especificações do ECS. Os ECSs devem ter NICs que suportem a largura de banda de 2 Gbit/s ou mais.

**Os testes mostram que a velocidade de rede real de um gateway de VPN na Huawei Cloud está dentro da faixa normal. No entanto, os servidores usados em ambas as extremidades da conexão de VPN devem executar os sistemas operacionais do mesmo tipo e as NICs do servidor devem atender aos requisitos de configuração.**

## 17.14.2 Qual direção da largura de banda é limitada e qual é a unidade da largura de banda?

Sua largura de banda de gateway de VPN adquirida é usada na direção de saída. Para equilibrar o tráfego nas direções de entrada e de saída, a largura de banda na direção de entrada é limitada.

- Se a largura de banda comprada for de 10 Mbit/s ou menos, a largura de banda na direção de entrada é limitada a 10 Mbit/s.
- Se a largura de banda comprada for maior que 10 Mbit/s, a largura de banda na direção de entrada será a mesma que a largura de banda comprada.

A unidade de largura de banda é Mbit/s e a unidade de tráfego é GB.

## 17.14.3 Como alterar o tamanho da largura de banda da VPN?

1. Na página **VPN Gateways**, localize a linha que contém o gateway de VPN de destino e escolha **More** > **Modify Bandwidth** na coluna **Operation**.
2. Na página **Modify Bandwidth**, selecione o tamanho de largura de banda necessário.
3. Clique em **Submit**.

## 17.14.4 O que acontece se a largura de banda de um gateway de VPN exceder o tamanho que especifiquei?

A largura de banda do gateway de VPN é usada na direção de saída de uma VPC. Se a largura de banda exceder o tamanho especificado, ocorrerá congestionamento da rede, algumas sub-redes não poderão ser acessadas ou até mesmo a conexão de VPN será interrompida, porque os pacotes de detecção de VPN podem não ser recebidos.

Neste caso, é aconselhável aumentar a largura de banda do gateway de VPN.

NOTA

A largura de banda máxima de uma conexão de VPN é de 300 Mbit/s.

## 17.14.5 Por que a mudança de largura de banda da VPN não faz efeito?

Há uma latência para que a alteração da largura de banda da VPN tenha efeito.

Teste a largura de banda 5 minutos depois de alterar a largura de banda.

NOTA

Alterar a largura de banda da VPN não interromperá a execução da carga de trabalho e as redes.

## 17.14.6 Uma VPN pode compartilhar largura de banda com um EIP?

Não.

Atualmente, um endereço IP público é gerado automaticamente e sua largura de banda é definida quando você cria um gateway de VPN. A VPN não pode compartilhar largura de banda com um EIP.

## 17.14.7 Quais são as diferenças entre a largura de banda de uma conexão de VPN e a de uma conexão direta?

### Conceitos

- A largura de banda de uma conexão Direct Connect é a largura de banda da conexão criada por um usuário.
- A largura de banda da conexão de VPN refere-se à largura de banda na direção de saída.

### Tamanho da largura de banda

- A largura de banda máxima padrão de uma conexão direta é de 1.000 Mbit/s. Quando você cria uma conexão no console de gerenciamento e define **Port Type** para **10GE single-mode optical port**, a largura de banda máxima é de 10 Gbit/s.
- A largura de banda máxima de uma conexão de VPN é de 300 Mbit/s.

### Qualidade da rede

- Um usuário da Direct Connect tem uma conexão dedicada com alta qualidade de rede.
- As conexões de VPN compartilham a largura de banda de seu gateway de VPN. A largura de banda total das conexões de VPN não pode exceder a largura de banda de seu gateway. A qualidade da rede será afetada pela qualidade da Internet.

## 17.14.8 Como determinar o tamanho da largura de banda da minha VPN?

Considere o seguinte ao determinar a largura de banda:

- Quantidade de dados transmitidos por um túnel de VPN em um período de tempo (Reserve largura de banda suficiente para evitar o congestionamento do link.)
- A largura de banda de saída no final da conexão de VPN na nuvem deve ser menor do que no final da conexão de VPN no data center local.

# 17.15 Cotas

## 17.15.1 O que é a cota de VPN?

### O que é uma cota?

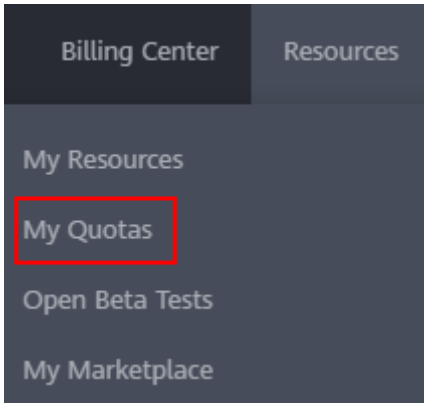
As cotas podem limitar o número ou a quantidade de recursos disponíveis para os usuários, como o número máximo dos ECSs ou discos EVS que podem ser criados.

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

### Como visualizar minha cota?

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

**Figura 17-31** Minhas cotas



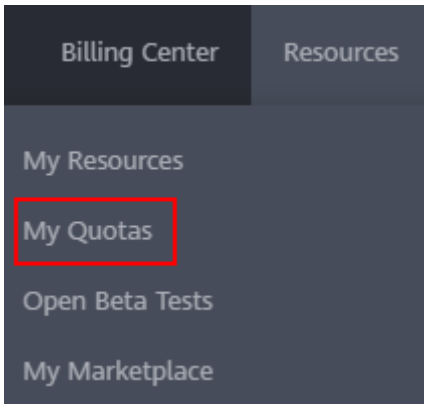

  

4. Visualize a cota usada e total de cada tipo de recursos na página exibida.
   Se uma cota não puder atender aos requisitos de serviço, solicite uma cota mais alta.

## Como solicitar uma cota mais alta?

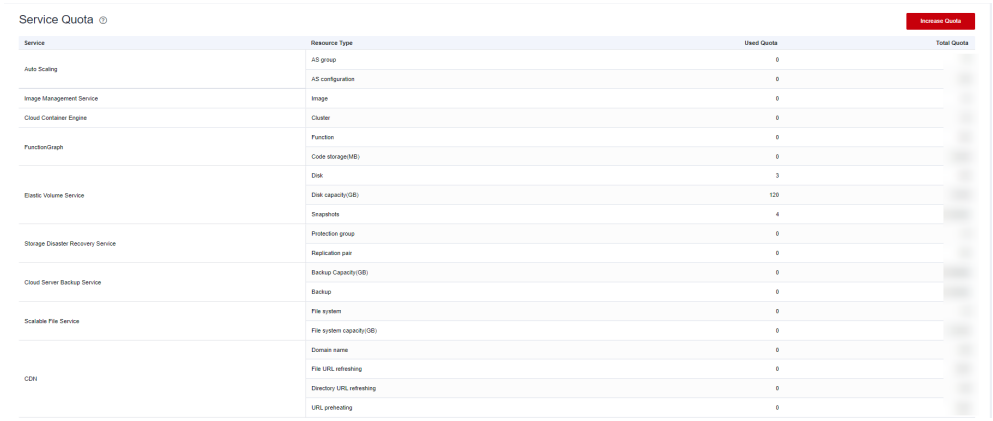
1. Faça logon no console de gerenciamento.
2. Escolha **Resources** > **My Quotas** no canto superior direito da página.
   A página **Service Quota** é exibida.

   **Figura 17-32** Minhas cotas




3. Clique em **Increase Quota** no canto superior direito da página.

   **Figura 17-33** Solicitar uma cota maior.




4. Na página **Create Service Ticket**, configure os parâmetros conforme necessário.
   Na área **Problem Description**, insira a cota necessária e o motivo do ajuste da cota.
5. Selecione o acordo e clique em **Submit**.

# 17.15.2 Quantos gateways de VPN e conexões de VPN posso criar por padrão?

- VPN: por padrão, cada usuário pode criar até 50 gateways de VPN e 100 gateways remotos. Antes de comprar gateways de VPN, verifique sua cota restante. Se a cota tiver sido atingida, **envie um tíquete de serviço** para solicitar o aumento da cota.

- Classic VPN: por padrão, cada usuário pode criar dois gateways de VPN e 12 conexões de VPN. Antes de comprar gateways de VPN, verifique sua cota restante. Se a cota tiver sido atingida, **envie um tíquete de serviço** para solicitar o aumento da cota.

## 17.15.3 Como alterar meu gateway de VPN e cotas de conexão?

1. Acesse o console de gerenciamento. No canto superior direito da página, escolha **Service Tickets** > **Create Service Ticket**.
2. Na página **Create Service Ticket**, clique em **Quotas** na área **Services**.
3. Clique em **Quota Application** em **Issue Categories**.
4. Clique em **Create Now**.

   Insira as informações necessárias e clique em **Submit**.

## 17.15.4 Quantas VPNs IPsec posso ter?

Por padrão, um usuário pode ter no máximo cinco VPNs IPsec. Se a cota não puder atender aos seus requisitos de serviço, solicite o aumento da cota.

# 17.16 Permissões da conta

## 17.16.1 Um nome de usuário e senha são necessários para criar uma conexão de VPN IPsec?

Não. A VPN IPsec da Huawei Cloud usa uma chave pré-compartilhada (PSK) para autenticação. A chave é configurada em um gateway de VPN. Um túnel será estabelecido após a conclusão da negociação de VPN. Portanto, nomes de usuário e senhas não são necessários.

Geralmente, as VPNs de Secure Sockets Layer (SSL), Point to Point Tunneling Protocol (PPTP) e Layer 2 Tunneling Protocol (L2TP) usam nomes de usuário e senhas para autenticação.

NOTA

IPsec XAUTH é uma tecnologia estendida da VPN IPsec. Ele solicita que os usuários insiram seus nomes de usuário e senhas durante a negociação de VPN.

A VPN da Huawei Cloud não suporta IPsec XAUTH.

## 17.16.2 O que fazer se o sistema exibir uma mensagem indicando que não tenho as permissões para criar uma VPN?

Verifique se sua conta é uma conta de usuário do IAM. Em caso afirmativo, execute operações no console do IAM como usuário da conta da Huawei Cloud para autorizar as permissões de operação da VPC. Certifique-se de que sua conta tenha as permissões **VPC Administrator**, **Tenant Guest** e **VPN Administrator**.

# 17.16.3 Como determinar se é por causa de permissões insuficientes que minha conta não pode criar uma VPN?

- Os gateways de VPN e as conexões criadas por uma conta da Huawei Cloud são invisíveis para as contas de usuário do IAM.
- Uma mensagem será exibida indicando que o sistema está ocupado se você criar um gateway de VPN ou conexão usando uma conta de usuário do IAM.

Para obter detalhes sobre as permissões necessárias para criar uma conexão de VPN, consulte **O que fazer se o sistema exibir uma mensagem indicando que não tenho as permissões para criar uma VPN?**.