Virtual Private Network

Visão geral de serviço

Edição 01

Data 14-04-2023

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


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

Aviso

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

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

Índice

1 O que é Virtual Private Network?

Visão geral

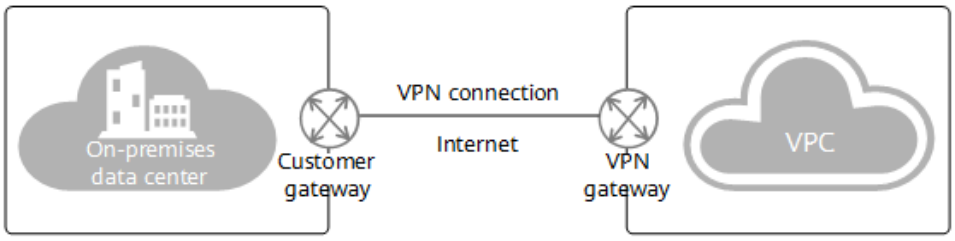
A Virtual Private Network (VPN) estabelece conexões criptografadas seguras, confiáveis e econômicas entre sua rede ou data center local e uma rede virtual na Huawei Cloud.

Uma VPN consiste em um gateway de VPN, um gateway de cliente e uma ou mais conexões de VPN.

- Um gateway de VPN fornece uma saída de Internet para uma VPC se conectar a um gateway de cliente em seu data center local.
- Uma conexão de VPN conecta um gateway de VPN a um gateway de cliente por meio de túneis criptografados, permitindo a comunicação entre uma VPC e seu data center local. Isso ajuda a estabelecer rapidamente um ambiente de nuvem híbrida seguro.

Figura 1-1 mostra a rede VPN.

Figura 1-1 Rede VPN



Componentes

- **VPN gateway**: é um gateway virtual de uma VPN na Huawei Cloud. Ele estabelece conexões privadas seguras com um gateway de cliente em sua rede local ou data center.
- **Customer gateway**: é um recurso que fornece informações à Huawei Cloud sobre seu dispositivo de gateway de cliente, que pode ser um dispositivo físico ou uma aplicação de software em seu data center local.
- **VPN connection**: é um canal seguro entre um gateway de VPN e um gateway de cliente. As conexões de VPN usam os protocolos Internet Key Exchange (IKE) e Internet Protocol Security (IPsec) para criptografar os dados transmitidos.

Acessar o serviço VPN

Você pode acessar o serviço VPN por meio do console de gerenciamento baseado na Web.

- Se você registrou uma conta, faça logon no console de gerenciamento e escolha **Networking** > **Virtual Private Network** para fazer logon no console de VPN.

2 Vantagens do produto

VPN possui as seguintes vantagens:

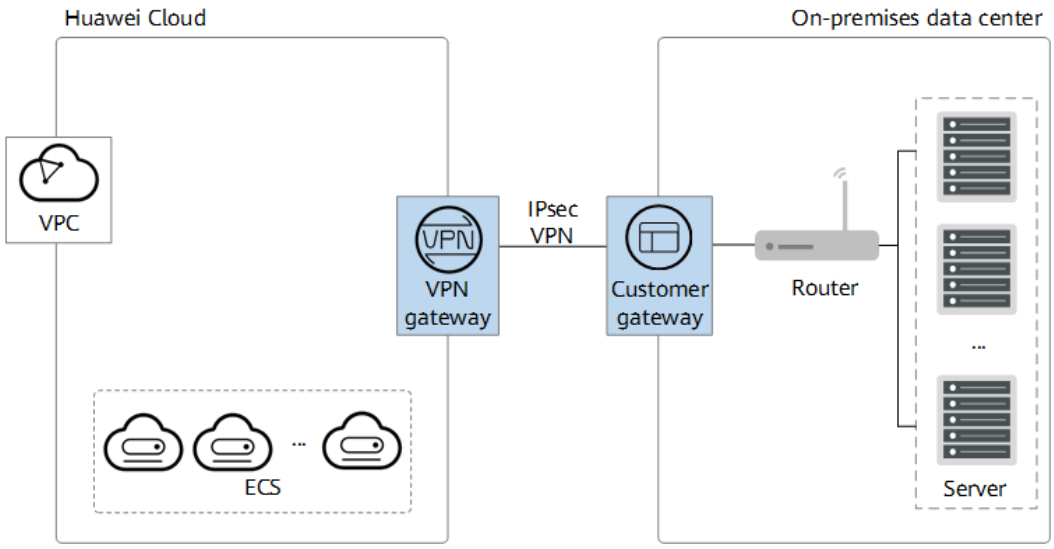
- **Alta segurança**
  - Os dados são criptografados usando IKE e IPsec, garantindo alta segurança de dados.
  - Um gateway de VPN é exclusivo de um locatário, isolando os locatários uns dos outros.
- **Alta disponibilidade**
  - Um gateway de VPN fornece dois endereços IP elásticos (EIPs) para estabelecer conexões de VPN independentes duplas com um gateway de cliente. Se uma conexão de VPN falhar, o tráfego pode ser rapidamente comutado para a outra conexão de VPN.
  - Os gateways ativo-ativos são implementados em diferentes zonas de disponibilidade (AZs) para garantir alta disponibilidade em nível de AZ.
- **Custo-benefício**
  - As conexões de IPsec pela Internet fornecem uma alternativa econômica a Direct Connect.
- **Facilidade de uso**
  - Um gateway de VPN suporta vários modos de conexão, incluindo roteamento estático baseado em políticas e roteamento BGP, para atender aos diferentes requisitos de acesso dos gateways do cliente.
  - Um gateway de VPN na nuvem pode funcionar como um hub de VPN, permitindo que os sites de filiais locais acessem uns aos outros.
  - Uma conexão de VPN pode ser criada em algumas etapas simples no dispositivo VPN em um data center local e no console de VPN, e está pronta para uso imediatamente após a criação.
  - A VPN pode ser usada em conjunto com o serviço de roteador empresarial, permitindo que as empresas criem redes baseadas em nuvem mais flexíveis.
  - O backup entre VPN e Direct Connect é suportado e o failover automático é suportado.

3 Cenários de aplicação

Implementação de nuvem híbrida

Você pode usar uma VPN para conectar seu data center local a uma VPC na nuvem e usar os recursos elásticos e de escalonamento rápido da nuvem para expandir os recursos de computação de aplicações. **Figura 3-1** mostra a implantação da nuvem híbrida.

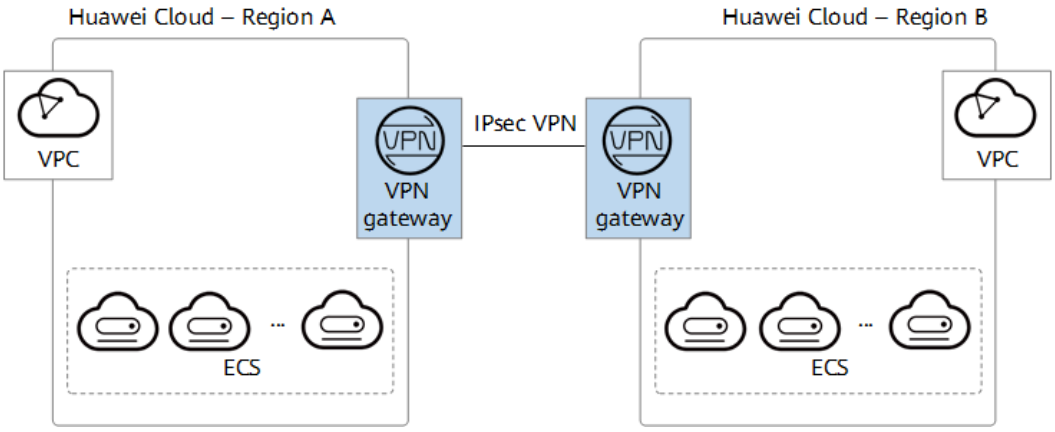
Figura 3-1 Implementação de nuvem híbrida



Interconexão entre regiões entre VPCs

Com as VPNs, você pode conectar VPCs em diferentes regiões para habilitar a conectividade entre os serviços do usuário nessas regiões, conforme mostrado na **Figura 3-2**.

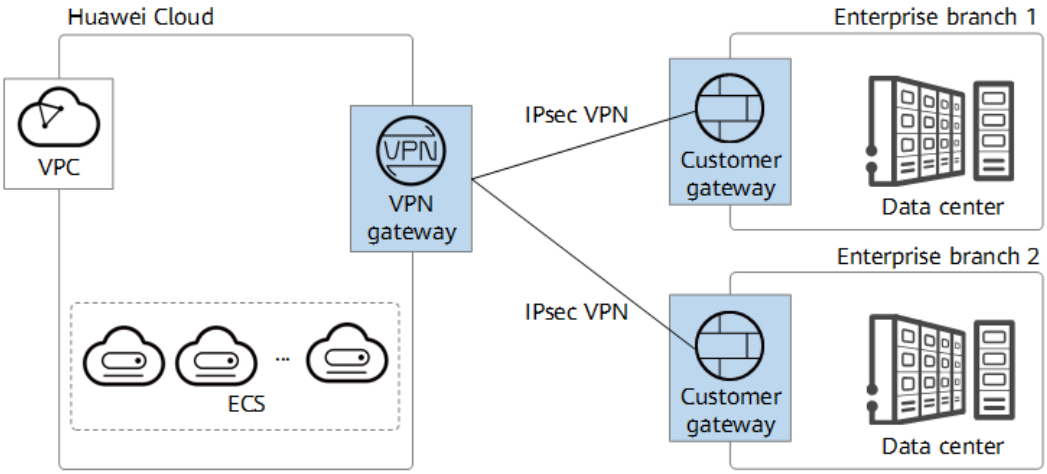
Figura 3-2 Interconexão entre regiões entre VPCs



Interconexão de filiais da empresa

Um gateway de VPN funciona como um hub da VPN para conectar as filiais da empresa, conforme mostrado na **Figura 3-3**. Isso elimina a necessidade de configurar conexões de VPN entre cada duas filiais.

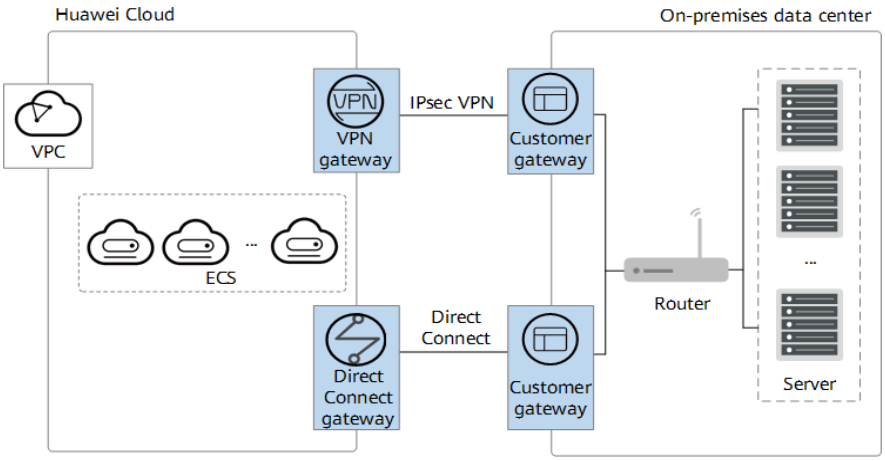
Figura 3-3 Interconexão de filiais da empresa



Backup entre VPN e Direct Connect

Para fins de alta confiabilidade, você pode conectar seu data center local a uma VPC na nuvem por meio da Direct Connect e da VPN que fazem backup um do outro, conforme mostrado na **Figura 3-4**.

Figura 3-4 Backup entre VPN e Direct Connect



4 Diferenças entre VPN e VPN clássica

NOTA

A menos que especificado de outra forma, a VPN mencionada neste documento refere-se à VPN da edição profissional (VPN, para abreviar).

Tabela 4-1 Diferenças entre VPN e VPN clássica

Categoria	Item	VPN	VPN clássica
Isolamento de locatário	Gateway exclusivo de locatário	Compatível	Incompatível
Funcionalidades	Modo baseado em políticas	Compatível	Compatível
	Modo baseado em rota: roteamento estático	Compatível	Incompatível
	Modo baseado em rota: roteamento BGP	Compatível	Incompatível
	Hub de VPN	Compatível	Incompatível
Capacidade	Número de sub-redes	• Modo baseado em rota: 50 • Modo baseado em políticas: 5	Modo baseado em políticas: 5
	Largura de banda máxima	1 Gbit/s	300 Mbit/s
Confiabilidade	Modo de proteção do gateway	Ativo-ativo	Ativo/em espera
	Implementação de gateway entre AZs	Compatível	Incompatível
	Conexões de VPN ativas-ativas	Compatível	Incompatível

5 Observações e restrições

Tabela 5-1 Observações e restrições

Tipo de VPN	Recurso	Cota padrão	Como aumentar a cota
VPN	Gateways de VPN por locatário em cada região	50 ● Se você tiver apenas uma VPC, poderá criar no máximo 50 gateways de VPN para a VPC. ● Se você tiver várias VPCs, poderá criar no máximo 50 gateways de VPN para todas essas VPCs.	**Envie um tíquete de serviço**.
	Gateways de cliente por locatário em cada região	100	**Envie um tíquete de serviço**.
	Grupos de conexão de VPN por gateway de VPN	100	Esta cota não pode ser aumentada.
	Sub-redes locais por gateway de VPN	50	Esta cota não pode ser aumentada.
	Regras de política por conexão de VPN	5	Esta cota não pode ser aumentada.
	Sub-redes de cliente por conexão de VPN	50	Esta cota não pode ser aumentada.

Tipo de VPN	Recurso	Cota padrão	Como aumentar a cota
	Número de rotas BGP que um gateway de VPN pode receber de um gateway de cliente por meio de uma conexão	100	Esta cota não pode ser aumentada.
VPN clássica	Gateways de VPN por locatário em cada região	2 Apenas um gateway VPN pode ser criado para uma VPC.	**Envie um tíquete de serviço**.
	Conexões de VPN por locatário em cada região	12	**Envie um tíquete de serviço**.

6 Padrões e protocolos de referência

Os seguintes padrões e protocolos estão associados à VPN:

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- RFC 6989: Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321: Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)

7 Cobrança (VPN)

Itens cobrados

Tabela 7-1 Itens de cobrança da VPN

Modo de cobrança	Item cobrado 1	Item cobrado 2	Item cobrado 3	Item cobrado 4	Fórmula de cobrança
Anual/mensal	Gateway de VPN	Conexão de VPN	Largura de banda de EIP Este item de cobrança está envolvido somente quando o tipo de rede é rede pública. A largura de banda EIP pode ser faturada em uma base anual/mensal ou pagamento por uso.	As taxas do roteador empresarial incluem taxas de conexão do roteador empresarial e taxas de tráfego do roteador empresarial. Este item de faturamento é envolvido somente quando **Associate With** está definido	Preço total = taxa de gateway de VPN + taxa de conexão de VPN + taxa de largura de banda de EIP + taxa de roteador empresarial

Modo de cobrança	Item cobrado 1	Item cobrado 2	Item cobrado 3	Item cobrado 4	Fórmula de cobrança
Pagamento por uso	Gateway de VPN (cobrado por hora)	Conexão de VPN (cobrada por hora)		como **Enterprise Router**.	Preço total = taxa de gateway de VPN (por hora) + taxa de conexão de VPN (por hora) + taxa de largura de banda de EIP + taxa de roteador empresarial

O preço total da VPN consiste nas seguintes partes:

- **Taxa de gateway de VPN**: indica a taxa cobrada pelo uso de um único gateway de VPN. Um gateway de VPN é dedicado a um locatário, garantindo seu desempenho de encaminhamento.
- **Taxa de conexão de VPN**: indica a taxa cobrada pelas conexões entre um gateway de VPN e um gateway do cliente.
  - No modo de cobrança anual/mensal, 10 grupos de conexão de VPN são incluídos gratuitamente com a compra de um gateway de VPN por padrão. Um grupo de conexões de VPN consiste em duas conexões de VPN entre um gateway de VPN e um gateway de cliente. Você pode comprar grupos de conexão VPN adicionais conforme necessário. Os grupos de conexão de VPN são vendidos em unidades de 10.
  - No modo de cobrança pagamento por uso, os grupos de conexão de VPN são vendidos em unidades de 1. A taxa de um único grupo de conexão de VPN é calculada da seguinte forma:

    taxa de um grupo de conexão de VPN = preço unitário de um grupo de conexão (USD/hora) x duração do uso (hora)
- **Taxa de largura de banda de EIP**: indica a taxa cobrada pela largura de banda consumida pelos EIPs vinculados a um gateway de VPN.
  - Por padrão, um gateway de VPN ativo-ativo tem dois EIPs. Você precisa comprar largura de banda para cada EIP.
  - Se você usar EIPs existentes como os EIPs de um gateway de VPN, não será cobrado novamente por esses EIPs.

  Para obter detalhes, consulte **Detalhes de preços do Elastic IP**.
- **Taxa do roteador empresarial**: indica a taxa de conexão do roteador empresarial e a taxa de tráfego do roteador empresarial gerada quando um gateway de VPN é associado a um roteador empresarial.

  Para obter detalhes, consulte a calculadora de preço do roteador empresarial.

Para obter detalhes sobre preços da VPN, consulte **Detalhes de preços do produto**.

Modos de cobrança

O serviço VPN é cobrado em uma base anual/mensal ou pagamento por uso.

Anual/mensal

Você é cobrado por mês ou ano ao criar um gateway de VPN

- **Fórmula de cobrança**: preço total = taxa de gateway de VPN (USD/mês por gateway) + taxa de grupo de conexão de VPN (USD/mês por 10 grupos de conexão) + taxa de banda de EIP (USD/mês por Mbit/s) + taxa de conexão do roteador empresarial (USD/hora) + taxa de tráfego do roteador empresarial (USD/GB)

  A largura de banda de um gateway de VPN é compartilhada por todas as conexões de VPN criadas para o gateway de VPN. Como tal, você precisa estimar a largura de banda necessária com base na quantidade de dados transmitidos em todas as conexões de VPN.

- **Modo de cobrança**:

  dez grupos de conexão VPN estão incluídos gratuitamente com a compra de um gateway de VPN. Se mais grupos de conexão de VPN forem necessários, você precisará comprá-los. O modo de cobrança anual/mensal oferece mais descontos do que o modo de pagamento por uso.

Pagamento por uso

Os gateways de VPN e os grupos de conexão de VPN são cobrados por duração de uso e o ciclo de cobrança é de 1 hora. A largura de banda de EIP pode ser cobrada por largura de banda ou tráfego.

- **Cobrado por largura de banda**
  - **Fórmula de cobrança**: preço total = taxa de gateway de VPN (USD/hora por gateway) + taxa de grupo de conexão de VPN (USD/hora por grupo de conexão) + taxa de largura de banda de EIP (USD/hora por Mbit/s) + taxa de conexão de roteador empresarial (USD/hora) + taxa de tráfego de roteador empresarial (USD/GB)

    A largura de banda de EIP refere-se à largura de banda de saída, ou seja, largura de banda para o tráfego enviado de uma VPC na nuvem para um gateway de cliente em um data center local.

    i. Se a largura de banda de EIP adquirida for de 10 Mbit/s ou menos, a largura de banda de entrada é limitada a 10 Mbit/s.

    ii. Se a largura de banda de EIP adquirida for maior que 10 Mbit/s, a largura de banda de entrada será a mesma que a largura de banda de EIP.

    Por exemplo, assumindo que a largura de banda que você comprou é de 50 Mbit/s e você usa o gateway de VPN por 5 horas e depois o exclui, você será cobrado pelo uso de 50 Mbit/s de largura de banda por 5 horas, mesmo que você não transmita nenhum dado durante as 5 horas.

- **Cobrado por tráfego**

  Se você selecionar a cobrança por tráfego, será cobrado pelo tráfego gerado na direção de saída da nuvem a cada hora, com a unidade de cobrança sendo 1 GB. Se for gerado menos de 1 GB, a taxa é calculada com base no volume de tráfego realmente gerado. Modificar a largura de banda não tem impacto nas taxas incorridas.
  - **Fórmula de cobrança**: preço total = taxa de gateway de VPN (USD/hora por gateway) + taxa de grupo de conexão de VPN (USD/hora por grupo de conexão) +

taxa de tráfego de EIP (USD/GB) + taxa de conexão de roteador empresarial (USD/hora) + taxa de tráfego de roteador empresarial (USD/GB)

Alteração do modo de cobrança

Você pode alterar os modos de cobrança de um gateway de VPN da seguinte forma:

- Altere o modo de cobrança de um gateway de VPN de pagamento por uso para anual/mensal. Para obter detalhes, consulte **Alteração do modo de cobrança de um gateway de VPN de pagamento por uso para anual/mensal**.
- Aumente ou diminua a largura de banda de um EIP cobrado anualmente/mensalmente. Para obter detalhes, consulte **Aumento ou diminuição da largura de banda de um EIP cobrado em um em uma base anual/mensal** .

NOTA

Você pode alterar o modo de faturamento do EIP (por exemplo, do pagamento por uso do tráfego ao pagamento por uso da largura de banda) no console do EIP. Para obter detalhes, consulte **Detalhes de preços do Elastic IP**.

Renovação

Para obter detalhes, consulte **Gerenciamento de renovação**.

Se os EIPs vinculados forem adquiridos quando um gateway de VPN for criado, o gateway de VPN e os EIPs poderão ser renovados simultaneamente. Caso contrário, você precisará renovar o gateway de VPN e os EIPs separadamente.

Expiração e pagamento em atraso

Para obter detalhes, consulte **Suspensão de serviço e liberação de recursos** e **Pagamento e repagamento**.

8 Cobrança (VPN clássica)

As VPNs clássicas da Huawei Cloud podem ser cobradas com base em pagamento por uso (por hora). Você paga apenas pelo que usar e pelo tempo que usar. Não são necessárias previsões e orçamentos complexos. Você pode comprar uma ou mais conexões VPN e será cobrado com base no número de conexões VPN e na duração do uso.

Itens cobrados

Tabela 8-1 Itens de cobrança de VPNs clássicas

Modo de cobrança	Item cobrado 1	Item cobrado 2	Item cobrado 3	Fórmula de cobrança
Pagamento por uso	Gateway de VPN clássica (cobrado por hora)	Conexão de VPN (cobrada por hora)	• Largura de banda Taxa de largura de banda (por hora) • Tráfego Taxa de tráfego (por GB)	• Cobrado por largura de banda Preço total = taxa de gateway de VPN clássica + taxa de conexão de VPN + taxa de largura de banda • Cobrado por tráfego Preço total = taxa de gateway VPN clássica + taxa de conexão VPN + taxa de tráfego

O preço total da VPN clássica consiste em três partes:

- **Taxa de gateway de VPN clássica**: indica a taxa cobrada pelo uso de um único gateway de VPN clássica.
- **Taxa de conexão de VPN clássica**: indica a taxa cobrada pelas conexões entre um gateway de VPN clássica e um gateway de cliente.
  - No modo de cobrança anual/mensal, 10 conexões de VPN estão incluídas gratuitamente com a compra de um gateway de VPN clássica por padrão. Você

pode comprar conexões de VPN adicionais conforme necessário. As conexões de VPN são vendidas em unidades de 10.

- No modo de cobrança de pagamento por uso, as conexões de VPN são vendidas em unidades de 1. A fórmula de cobrança é a seguinte: taxa de conexão de VPN = preço unitário da conexão (USD/hora) x duração do uso (hora).

- **Taxa de largura de banda**: indica a taxa cobrada pela largura de banda consumida por um gateway de VPN clássica.

Para obter detalhes sobre os preços da VPN clássica, consulte **Detalhes de preços do produto**.

Billing Modes

Pay-per-use

- **Billed by bandwidth**

  If you select billing by bandwidth, the billing cycle is one hour. The generated fee also varies depending on the bandwidth size. The price includes the VPN gateway bandwidth or traffic price and the price of the VPN connection created together with the gateway. If you create another connection for the gateway, you will be charged for the additional connection.

  Total price = VPN gateway bandwidth fee + VPN connection fee

  The bandwidth you purchased for a VPN gateway refers to outbound bandwidth, that is, bandwidth for traffic sent from a VPC on the cloud to a customer gateway in an on-premises data center.

  a. If the purchased EIP bandwidth is 10 Mbit/s or less, the inbound bandwidth is limited to 10 Mbit/s.

  b. If the purchased EIP bandwidth is greater than 10 Mbit/s, the inbound bandwidth is the same as the EIP bandwidth.

  For example, assuming that the bandwidth you purchased is 50 Mbit/s and you use the VPN gateway for 5 hours and then delete it, you will be charged for the use of 50 Mbit/s bandwidth for 5 hours even if you do not transmit any data during the 5 hours.

- **Billed by traffic**

  If you select billing by traffic, you will be charged for the traffic generated in every hour, with the billing unit being 1 GB. If less than 1 GB is generated, the fee is calculated based on the actually generated traffic volume. In this case, modifying the bandwidth size does not change the public network traffic price per GB. Only traffic in the outbound direction is billed.

  Total price = Public network traffic fee + VPN connection fee

Alteração do modo de cobrança

Os gateways de VPN de pagamento por uso faturados por largura de banda podem ser alterados para serem faturados por tráfego ou vice-versa. Para obter detalhes, consulte **Alteração de um gateway de VPN de pagamento por uso de ser cobrado por largura de banda para ser cobrado por tráfego ou o contrário**.

Renovação

Para obter detalhes, consulte **Gerenciamento de renovação**.

Expiração e pagamento em atraso

Para obter detalhes, consulte **Suspensão de serviço e liberação de recursos** e **Pagamento e repagamento**.

9 Segurança

9.1 Responsabilidade compartilhada

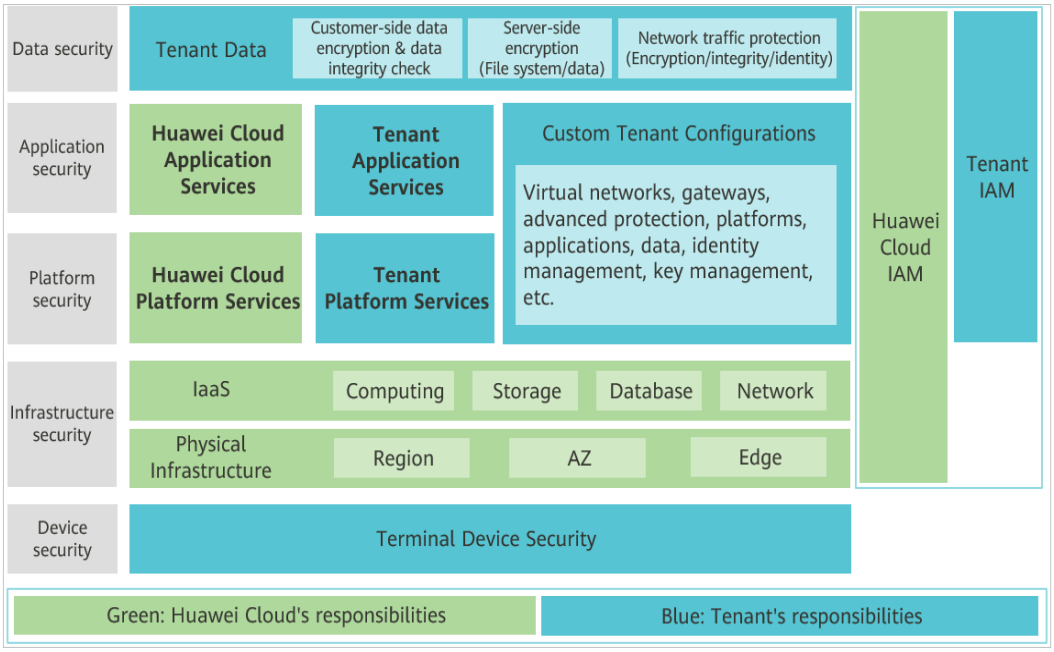
A Huawei Cloud garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para enfrentar os desafios emergentes à segurança na nuvem e ameaças e ataques à segurança na nuvem generalizada, a Huawei Cloud constrói um sistema de segurança abrangente que está em conformidade com leis, regulamentos e padrões do setor para serviços em nuvem em diferentes regiões e setores, aproveitando o ecossistema de segurança da Huawei e as vantagens exclusivas em software e hardware.

Figura 9-1 mostra as responsabilidades compartilhadas por si (locatários) e pela Huawei Cloud.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem. A Huawei Cloud é responsável pela segurança de seus serviços de nuvem IaaS, PaaS e SaaS, bem como pelos ambientes físicos dos data centers da Huawei Cloud onde esses serviços são implantados. A Huawei Cloud está comprometida não apenas com a segurança e o desempenho de sua infraestrutura, serviços em nuvem e tecnologias, mas também com a segurança geral de O&M na nuvem e, mais amplamente, com a conformidade de segurança.
- **Locatários**: garanta o uso seguro dos serviços em nuvem. Sua responsabilidade é usar os serviços em nuvem IaaS, PaaS e SaaS com segurança e gerenciar efetivamente as configurações de segurança personalizadas para firewalls virtuais, gateways de API, serviços avançados de segurança, serviços em nuvem, dados de usuário, gerenciamento de identidade e chaves, e os sistemas operacionais para redes virtuais, hosts virtuais e máquinas virtuais (VMs) convidadas.

O Livro branco de segurança da Huawei Cloud elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

Figura 9-1 Modelo de responsabilidade compartilhada da Huawei Cloud



9.2 Autenticação de identidade e controle de acesso

Uma conexão de VPN suporta a autenticação de um gateway de cliente usando uma chave pré-compartilhada (PSK).

A autenticação de identidade é bem-sucedida e a conexão VPN pode ser configurada somente quando a PSK configurada no gateway do cliente for a mesma configurada para a conexão de VPN.

Figura 9-2 Gerenciamento de identidade e acesso

9.3 Tecnologias de proteção de dados

- O IPsec de VPN é uma tecnologia de tunelamento que fornece segurança de camada IP usando o conjunto de protocolos IKE/IPsec. Ele garante a confidencialidade e integridade dos pacotes de dados IP e impede que eles sejam interceptados, divulgados ou adulterados em redes inseguras (como a Internet).
- Ao criar uma conexão de IPsec de VPN, você pode configurar algoritmos de criptografia e autenticação de dados em uma política de IPsec.

  Algoritmos criptográficos comerciais comuns são suportados. Os algoritmos recomendados são listados da seguinte forma em ordem decrescente de segurança:

- Algoritmos de encritação:
  - AES-256-GCM-16 (suportado apenas por VPN)
  - AES-256
  - AES-192
  - AES-128
- Algoritmos de autenticação:
  - SHA2-512
  - SHA2-384
  - SHA2-256

PFS

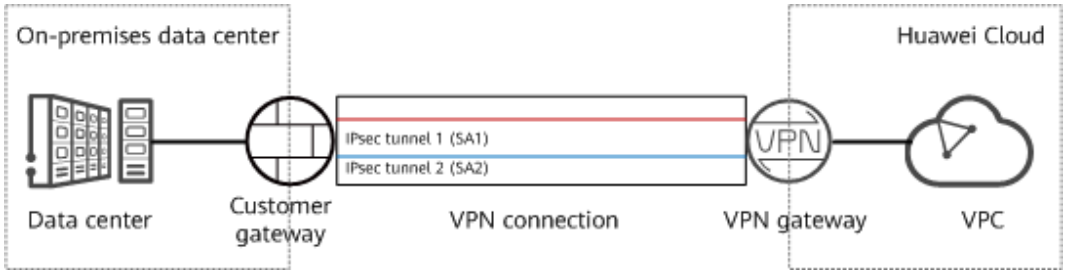
O Perfect Forward Secrecy (PFS) garante que o comprometimento das chaves de um túnel IPsec não afete a segurança de outros túneis, aproveitando que as chaves desses túneis sejam irrelevantes entre si. Por predefinição, o PFS está ativado para o serviço VPN.

Cada conexão de IPsec de VPN consiste em pelo menos um túnel IPsec, cada um dos quais usa um conjunto independente de chaves para proteger o tráfego do usuário.

Algoritmos comuns de PFS são suportados. Os algoritmos recomendados são os seguintes:

- DH grupo 14
- DH grupo 15
- DH grupo 16
- DH grupo 19
- DH grupo 20
- DH grupo 21

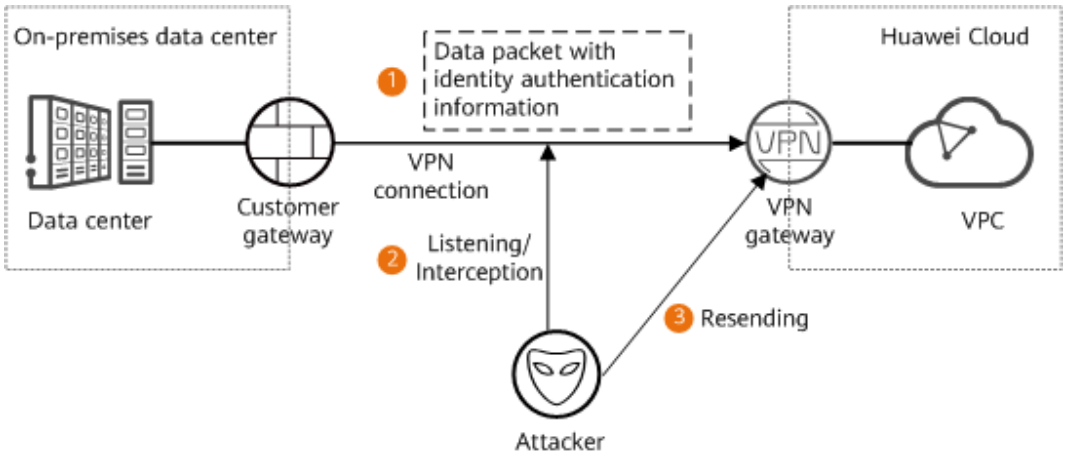
Figura 9-3 PFS



Anti-repetição

Anti-repetição usa números de sequência para proteger pacotes criptografados de IPsec contra ataques de repetição, que são iniciados enviando repetidamente pacotes de dados interceptados. Por predefinição, a função anti-repetição está ativada para o serviço VPN.

Figura 9-4 Ataque de repetição

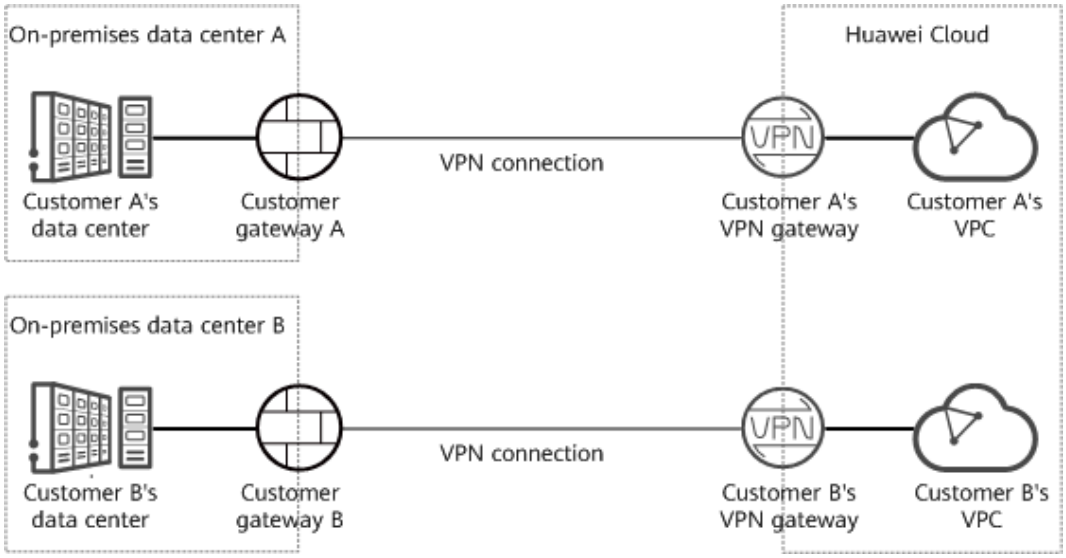


Isolamento de recursos

Um gateway de VPN é exclusivo de um locatário. Como tal, os locatários são isolados de cada um, garantindo a segurança dos dados dos locatários.

O isolamento de dados é suportado apenas pela VPN, mas não pela VPN clássica.

Figura 9-5 Isolamento de dados

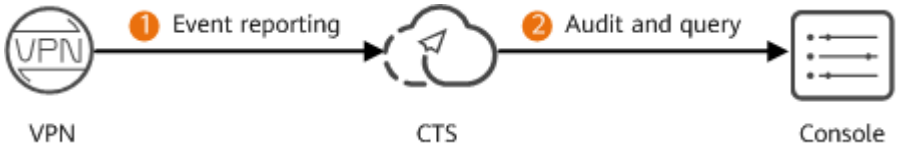


Conforme mostrado na figura, uma falha do gateway de VPN do cliente A não tem impacto no gateway de VPN do cliente B.

9.4 Auditoria e logs

A VPN registra as operações de criação, exclusão e modificação realizadas em todos os recursos iniciados pela sua conta e envia os registros para o Cloud Trace Service (CTS) em arquivos de log para consulta, auditoria e rastreamento de origem.

Figura 9-6 Auditoria e logs

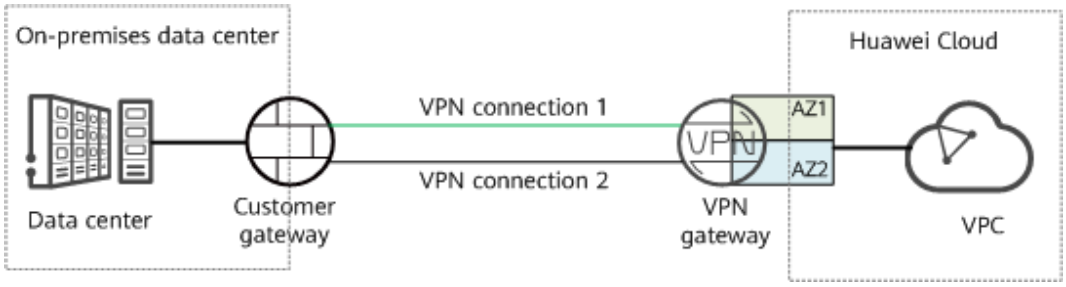


9.5 Resiliência de serviço

A VPN oferece a função de recuperação de desastres de AZ dupla. Você pode criar um gateway de VPN em duas AZs na mesma região e criar uma conexão VPN entre o gateway do cliente e cada AZ.

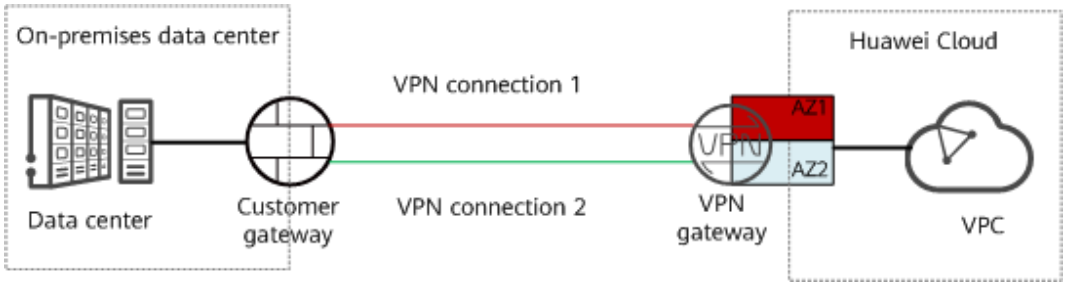
A recuperação de desastres de AZ dupla é suportada apenas pela VPN, mas não pela VPN clássica.

Figura 9-7 Cenário em que os serviços estão sendo executados corretamente



Se o gateway de VPN ou a conexão de VPN em uma AZ estiver defeituosa, o tráfego é automaticamente comutado para a outra conexão de VPN, garantindo a execução normal do serviço.

Figura 9-8 Cenário de failover



10 Gerenciamento de permissões

Se você precisar atribuir permissões diferentes a funcionários em sua empresa para acessar seus recursos da VPN na Huawei Cloud, o Identity and Access Management (IAM) é uma boa escolha para o gerenciamento de permissões refinado. IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos.

Com o IAM, você pode usar sua conta da Huawei Cloud para criar usuários do IAM e atribuir permissões aos usuários para controlar seu acesso a recursos específicos. Por exemplo, alguns desenvolvedores de software em sua empresa precisam usar recursos da VPN, mas não devem ter permissão para excluir os recursos ou executar qualquer outra operação de alto risco. Nesse cenário, você pode criar usuários do IAM para os desenvolvedores de software e conceder a eles apenas as permissões necessárias para usar os recursos da VPN.

Se sua conta da HUAWEI CLOUD não precisar de usuários individuais do IAM para gerenciamento de permissões, pule esta seção.

O IAM é gratuito. Você paga apenas pelos recursos na sua conta. Para obter mais informações sobre o IAM, consulte **Visão geral de serviço do IAM**.

Permissões de VPN

Por padrão, os novos usuários do IAM não têm permissões atribuídas. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos. Os usuários herdam permissões dos grupos aos quais são adicionados e podem executar operações especificadas em serviços em nuvem com base nas permissões.

VPN é um serviço de nível de projeto implantado em regiões físicas específicas. Para atribuir permissões da VPN a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione os projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Ao acessar a VPN, os usuários precisam mudar para uma região onde foram autorizados a usar este serviço.

Você pode conceder permissões usando funções ou políticas.

- Funções: um tipo de mecanismo de autorização de granulação grosseira que define permissões relacionadas às responsabilidades do usuário. Há apenas um número limitado de funções para conceder permissões aos usuários. Alguns papéis dependem de outros papéis para ter efeito. Ao atribuir tais funções aos usuários, lembre-se de atribuir as

funções das quais eles dependem. No entanto, as funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.

- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos em nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível, atendendo aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários da VPN somente as permissões necessárias para gerenciar um determinado tipo de recursos de ECSs.

Tabela 10-1 lista todas as funções e permissões definidas pelo sistema suportadas pela VPN.

Tabela 10-1 Funções e permissões definidas pelo sistema de VPN

Nome da função/ política do sistema	Descrição	Dependência
VPN Administrator	Todas as operações em recursos VPN. Os usuários com essa permissão têm as permissões **VPC Administrator** e **Tenant Guest** por padrão. ● **VPC Administrator**: política no nível do projeto, que é selecionada no mesmo projeto que o **VPN Administrator**. ● **Tenant Guest**: política de nível de projeto, que é selecionada no mesmo projeto que o **VPN Administrator**.	-
VPN FullAccess	Permissões completas para a VPN.	Para executar as seguintes operações, você precisa configurar as permissões **VPC Administrator** e **Tenant Guest**, além da permissão **VPN FullAccess**: ● Criar gateways de VPN clássica ● Criar conexões de VPN
VPN ReadOnlyAccess	Permissões somente leitura em recursos de VPN. Os usuários que têm essas permissões só podem exibir informações sobre os recursos da VPN.	N/D

Tabela 10-2 lista as operações comuns suportadas por cada política de VPN definida pelo sistema. Selecione as permissões conforme necessário.

Tabela 10-2 Operações comuns suportadas pelo **VPN Administrator**

Operação	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
Criar um gateway de VPN	Compatível	● VPN: √ ● VPN clássica: ×	×
Visualizar um gateway de VPN	Compatível	√	√
Modificar um gateway de VPN	Compatível	● VPN: √ ● VPN clássica: ×	×
Excluir um gateway de VPN	Compatível	● VPN: √ ● VPN clássica: ×	×
Criar uma conexão de VPN	Compatível	● VPN: × ● VPN clássica: √	×
Visualizar uma conexão de VPN	Compatível	√	√
Modificar uma conexão de VPN	Compatível	● VPN: × ● VPN clássica: √	×
Excluir uma conexão de VPN	Compatível	● VPN: × ● VPN clássica: √	×
Criar um gateway de cliente	√	● VPN: √ ● VPN clássica: N/D	×
Visualizar um gateway de cliente	√	● VPN: √ ● VPN clássica: N/D	√
Modificar um gateway de cliente	√	● VPN: √ ● VPN clássica: N/D	×
Excluir um gateway de cliente	√	● VPN: √ ● VPN clássica: N/D	×

Links úteis

- **O que é IAM?**
- **Criação de um usuário e concessão de permissões**

11 VPN e outros serviços

Figura 11-1 mostra serviços relacionados à VPN.

Figura 11-1 VPN e serviços relacionados

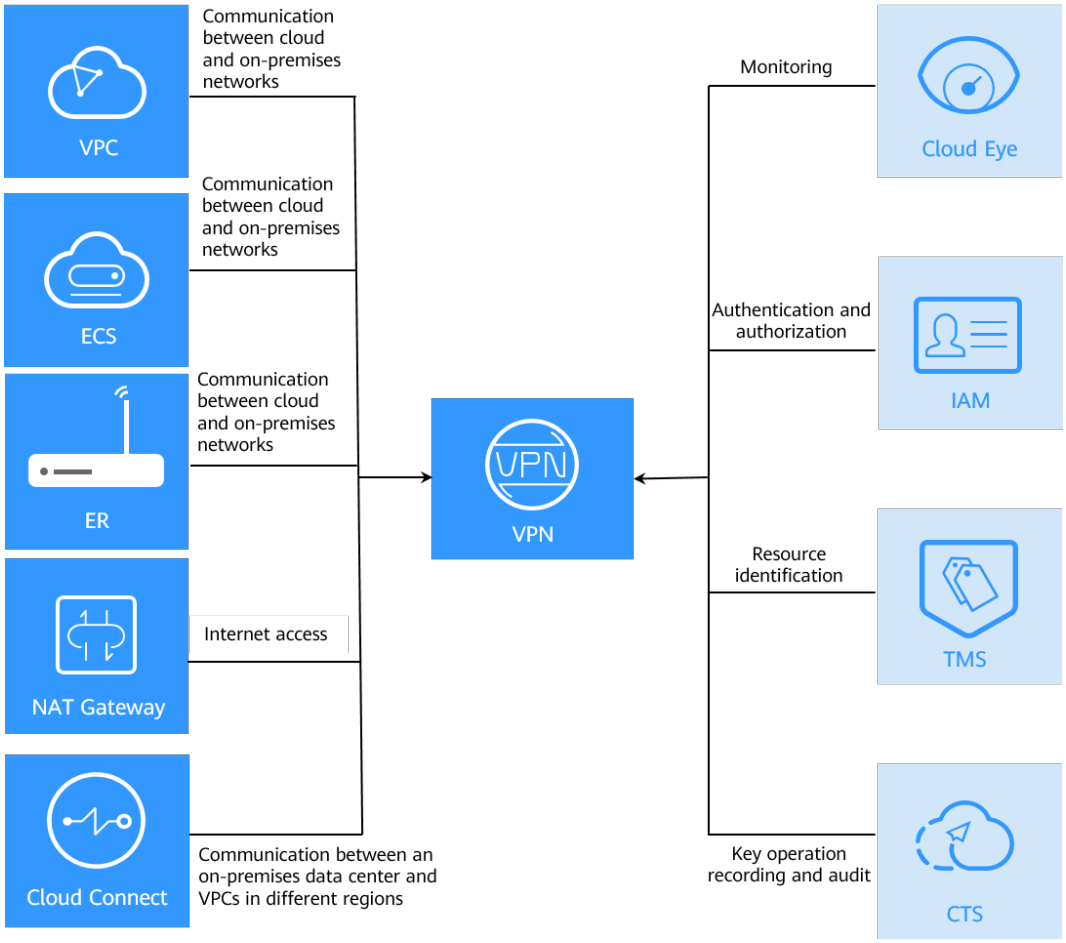


Tabela 11-1 Serviços relacionados

Serviço relacionado	Função	Referência
Virtual Private Cloud (VPC)	Permite criar uma nuvem privada virtual à qual seu data center local deve ser conectado.	**VPC**
Elastic Cloud Server (ECS)	Permite criar grupos de segurança, adicionar regras de grupo de segurança e adicionar ECSs aos grupos de segurança, melhorando a segurança de acesso ao ECS.	**ECS**
Enterprise Router (ER)	Conecta um data center local à nuvem por meio de uma VPN e da Direct Connect que fazem backup um do outro. Este serviço é suportado apenas por gateways de VPN, mas não por gateways de VPN clássica.	**Enterprise Router**
Network address translation (NAT) gateway	Permite que servidores em um data center local acessem a Internet ou forneçam serviços acessíveis a partir da Internet.	**NAT Gateway**
Elastic IP address (EIP)	Permite que um gateway de VPN se comunique com um gateway de cliente através de uma rede pública. Este serviço é suportado apenas por VPN.	**Elastic IP**
Cloud Connect	Funciona em conjunto com a VPN para permitir comunicações de rede estáveis entre seu data center local e VPCs em diferentes regiões.	**Cloud Connect**
Cloud Eye	Monitora os recursos da VPN e permite que você visualize as métricas.	**Cloud Eye**
Identity and Access Management (IAM)	Permite atribuir permissões diferentes a usuários diferentes. Ele permite um controle refinado sobre seus recursos de VPN.	**Identity and Access Management**

Serviço relacionado	Função	Referência
Tag Management Service (TMS)	Identifica as VPNs para facilitar a classificação e a pesquisa. Este serviço é suportado apenas pela VPN clássica.	**Tag Management Service**
Cloud Trace Service (CTS)	Registra as operações realizadas na VPN.	**Cloud Trace Service**

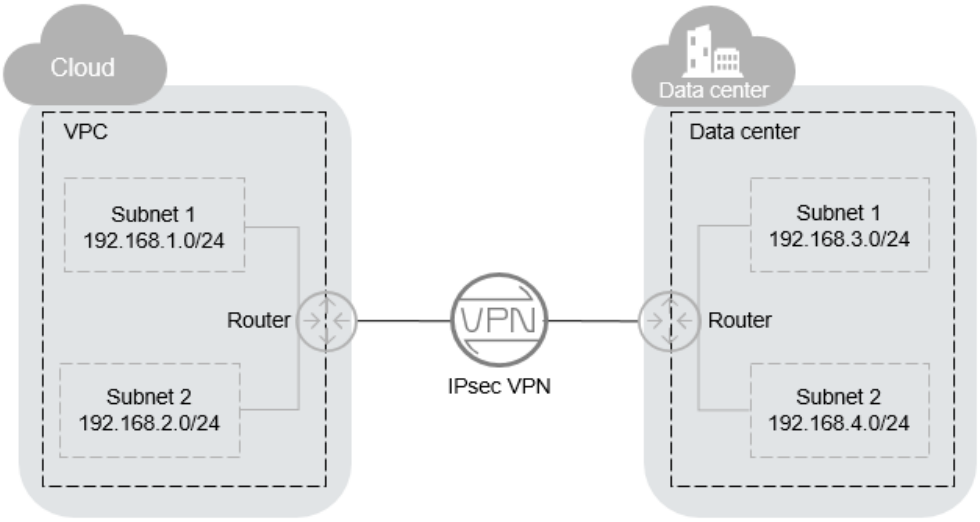
12 Conceitos básicos

12.1 VPN IPsec

Internet Protocol Security (IPsec) de VPN usa um conjunto de protocolos de rede segura que autentica e criptografa os pacotes de dados para fornecer comunicação criptografada segura entre diferentes redes.

No exemplo mostrado em **Figura 12-1**, suponha que você tenha criado uma VPC com duas sub-redes (192.168.1.0/24 e 192.168.2.0/24) na nuvem, e o roteador em seu data center local também tem duas sub-redes (192.168.3.0/24 e 192.168.4.0/24). Nesse caso, você pode criar uma VPN para conectar as sub-redes da VPC e as sub-redes do data center.

Figura 12-1 VPN IPsec



A VPN site-to-site é suportada para permitir a comunicação entre sub-redes da VPC e sub-redes de data center locais.

12.2 Gateway de VPN

Um gateway de VPN é um gateway virtual de uma VPN na Huawei Cloud. Ele estabelece conexões privadas seguras com um gateway de cliente em sua rede local ou data center.

Um gateway de VPN precisa funcionar com um gateway de cliente em seu data center local.

12.3 Conexão de VPN

Uma conexão de VPN é um canal seguro entre um gateway de VPN e um gateway de cliente. As conexões de VPN utilizam os protocolos IKE e IPsec para encriptar os dados transmitidos.

Uma conexão de VPN usa os protocolos IKE e IPsec para criptografar os dados transmitidos, garantindo a segurança e a confiabilidade dos dados.

12.4 Largura de banda do gateway de VPN

A largura de banda adquirida para um gateway de VPN refere-se à largura de banda de saída, ou seja, largura de banda para o tráfego enviado de uma VPC na nuvem para um gateway de cliente em um data center local.

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

Se o seu gateway de VPN for cobrado por tráfego em uma base de pagamento por uso, o tamanho da largura de banda do gateway de VPN não afetará o preço total. Mas é recomendável que você defina o tamanho da largura de banda com base nos requisitos reais para evitar uma grande quantidade de tráfego causada por erros de programa ou acesso malicioso.

12.5 Sub-rede local

Sub-redes locais são sub-redes da VPC que precisam se comunicar com uma rede local por meio de VPN. Ao comprar um gateway de VPN, você pode definir a **Local Subnet** como uma das seguintes opções:

- **Select subnet**: selecione sub-redes na lista suspensa. Isso é recomendado se todas as sub-redes que exigem comunicação de VPN estiverem na VPC.
- **Enter CIDR block**: insira uma sub-rede usando a notação CIDR (exemplo: 192.168.0.0/16). Se várias sub-redes forem especificadas, separe-as por uma vírgula (,). Isso é recomendado se os blocos CIDR que exigem comunicação de VPN não estiverem na VPC à qual o gateway de VPN pertence. Por exemplo, os blocos CIDR (como 0.0.0.0/0) que estão conectados usando um emparelhamento de VPC não estão na VPC à qual o gateway de VPN pertence.

12.6 Gateway de cliente

Um gateway de cliente é um recurso que fornece informações no console sobre seu dispositivo de gateway de cliente, que pode ser um dispositivo físico ou uma aplicação de software em seu data center local.

12.7 Sub-rede de cliente

As sub-redes de cliente são sub-redes em um data center local que acessam uma VPC na nuvem por meio de uma VPN. Você precisa inserir sub-redes usando a notação CIDR (exemplo: 192.168.0.0/16), e com cada entrada separada por uma vírgula.

Depois de configurar uma sub-rede de cliente, você não precisa adicionar uma rota para ela. O serviço VPN entregará automaticamente rotas apontando para a sub-rede de cliente.

NOTA

Uma sub-rede do cliente não pode ser definida como um endereço IP de Classe D ou Classe E ou um endereço IP que comece com 127.

12.8 PSK

Uma chave pré-compartilhada (PSK) é uma chave configurada para uma conexão de VPN em nuvem. Ela é usada para negociação IKE entre dispositivos de VPN em ambas as extremidades de uma conexão de VPN. Assegure-se de que as configurações de PSK em ambas as extremidades da conexão de VPN sejam as mesmas. Caso contrário, a negociação IKE falhará.

Link de referência:

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

