NAT Gateway

Visão geral de serviço

Edição	01
Data	2025-02-26

HUAWEI CLOUD COMPUTING 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, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem 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 ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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 Infográficos do NAT Gateway....1
2 O que é o NAT Gateway?....3
3 Vantagens do produto....8
4 Cenários....10
5 Especificações do gateway NAT....17
6 Observações e restrições....19
7 Usar o NAT Gateway com outros serviços....21
8 Cobrança (NAT Gateway público)....24
9 Cobrança (NAT Gateway privado)....25
10 Gerenciamento de permissões....27
11 Região e AZ....31
12 Conceitos básicos....33

1 Infográficos do NAT Gateway

What Is NAT Gateway?

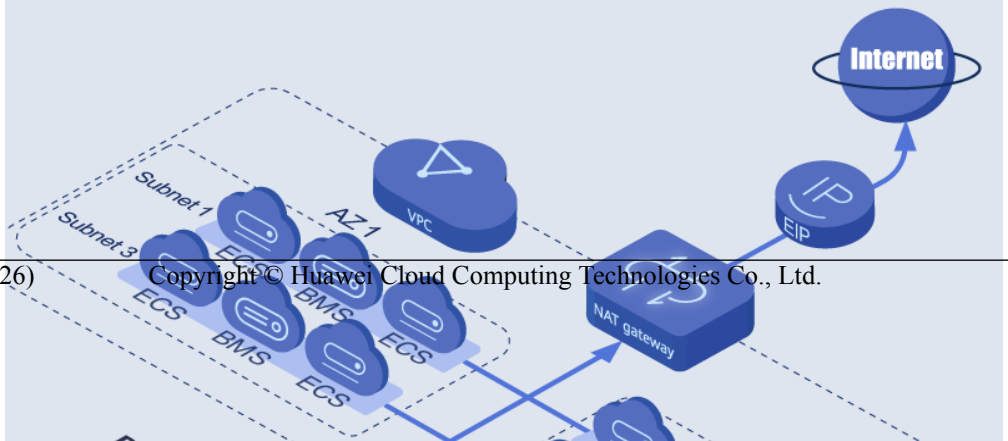
NAT Gateway provides network address translation (NAT). Public NAT gateways help you save EIPs. Private NAT gateways enable your servers in a Virtual Private Cloud (VPC) to communicate with servers in remote private networks (other VPCs or on-premises servers).

Public NAT Gateway

Public NAT gateways provide NAT for servers in a VPC or on-premises servers that connect to the cloud through Direct Connect or Virtual Private Network (VPN), allowing multiple servers to share EIPs for Internet connectivity.

Public NAT gateways support **source NAT (SNAT)** and **destination NAT (DNAT)**.

SNAT translates private IP addresses into EIPs, allowing servers within an AZ or across multiple AZs in a VPC to share EIPs to access the Internet.



2 O que é o NAT Gateway?

NAT Gateway é um serviço de conversão de endereços de rede (NAT). Pode ser um gateway NAT público ou um gateway NAT privado.

Gateways NAT público

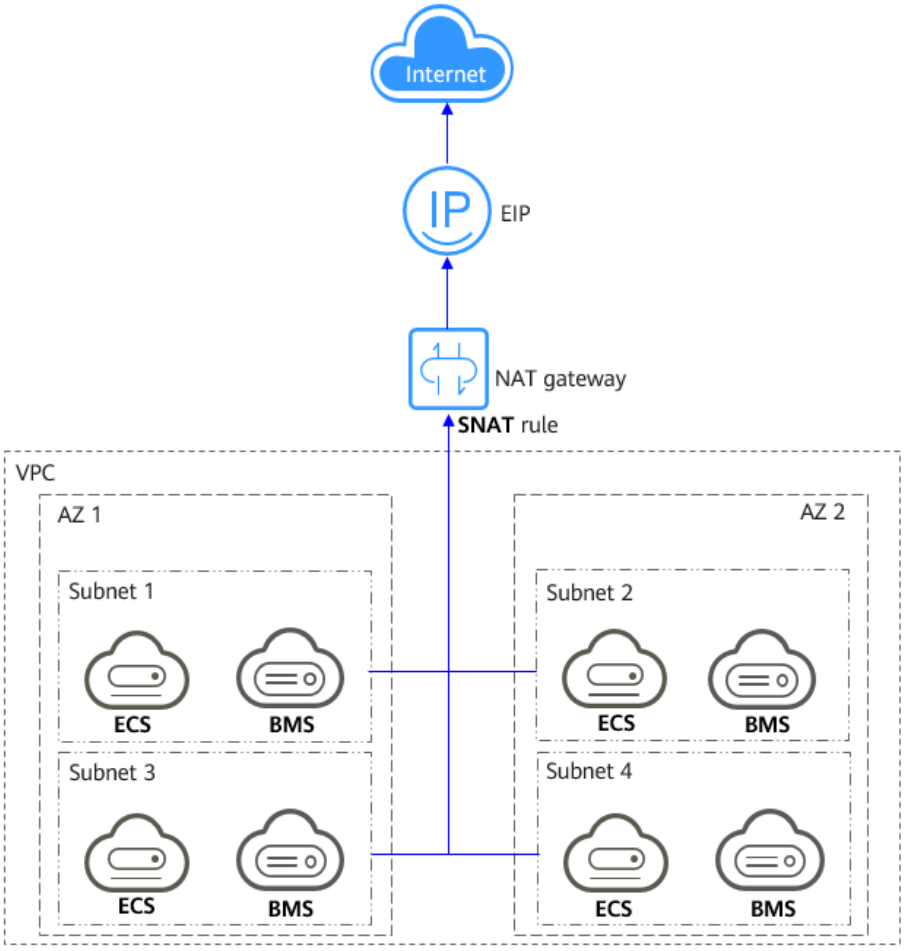
Um gateway NAT público permite que servidores na nuvem e locais em uma sub-rede privada acessem a Internet ou forneçam serviços acessíveis a partir da Internet. Os servidores em nuvem são ECSs e BMSs em uma VPC. Servidores locais são servidores em data centers locais que se conectam a uma VPC por meio do Direct Connect ou da Virtual Private Network (VPN). Um gateway NAT público suporta até 20 Gbit/s de largura de banda.

Os gateways NAT públicos oferecem NAT de origem (SNAT) e NAT de destino (DNAT).

- O SNAT traduz endereços IP privados em endereços IP elásticos (EIPs), permitindo que o tráfego de uma rede privada saia para a Internet.

  Figura 2-1 mostra como funciona uma regra SNAT.

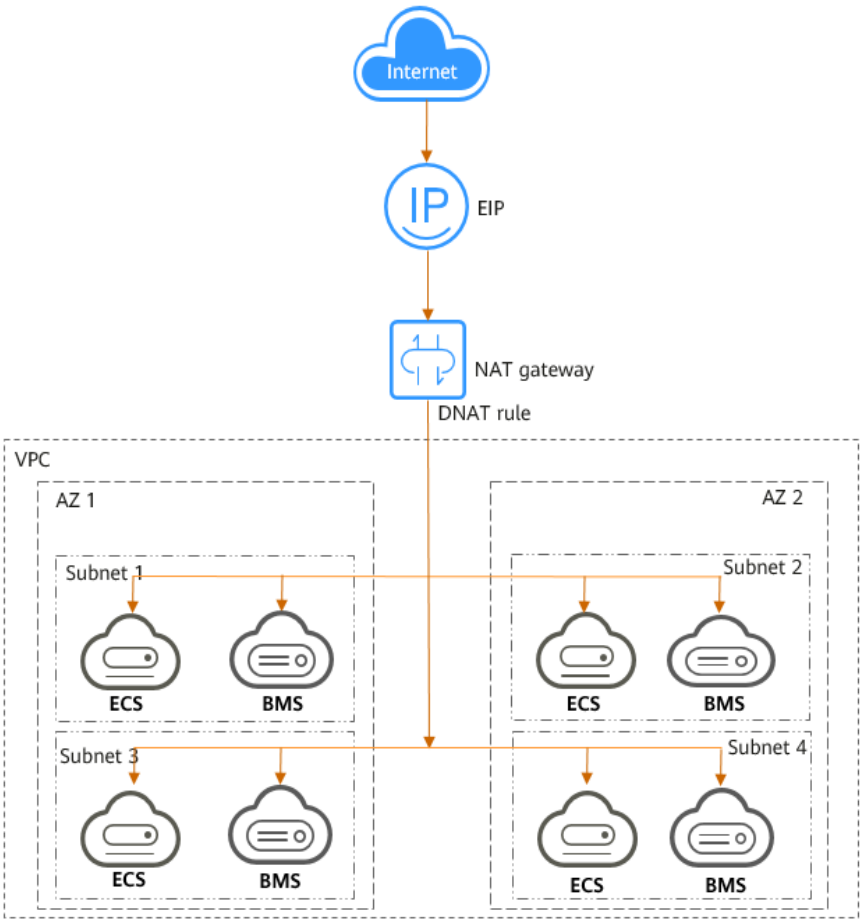
Figura 2-1 Gateway NAT com uma regra de SNAT



- O DNAT permite que vários servidores em uma AZ ou em várias AZs em uma VPC compartilhem EIPs para fornecer serviços acessíveis pela Internet. Com um EIP, um gateway NAT encaminha as solicitações da Internet de apenas uma porta específica e através de um protocolo específico para uma porta específica de um servidor, ou pode encaminhar todas as solicitações para o servidor, independentemente de qual porta elas se originaram.

  Figura 2-2 mostra como funciona uma regra de DNAT.

Figura 2-2 Gateway NAT com uma regra DNAT



Gateway NAT privado

Os gateways de NAT privado fornecem tradução de endereços de rede, permitindo que ECSs e BMSs em uma VPC se comuniquem com servidores em outras VPCs ou data centers locais. Você pode configurar regras de SNAT e de DNAT para que o NAT Gateway converta os endereços IP de origem e destino dos pacotes de origem em um endereço IP de trânsito.

Especificamente,

- O SNAT permite que vários servidores em uma AZ ou em várias AZs em uma VPC compartilhem um endereço IP de trânsito para acessar data centers locais ou outras VPCs.
- O DNAT permite que servidores que compartilham o mesmo endereço IP de trânsito em uma VPC forneçam serviços acessíveis a partir de data centers locais ou outras VPCs.

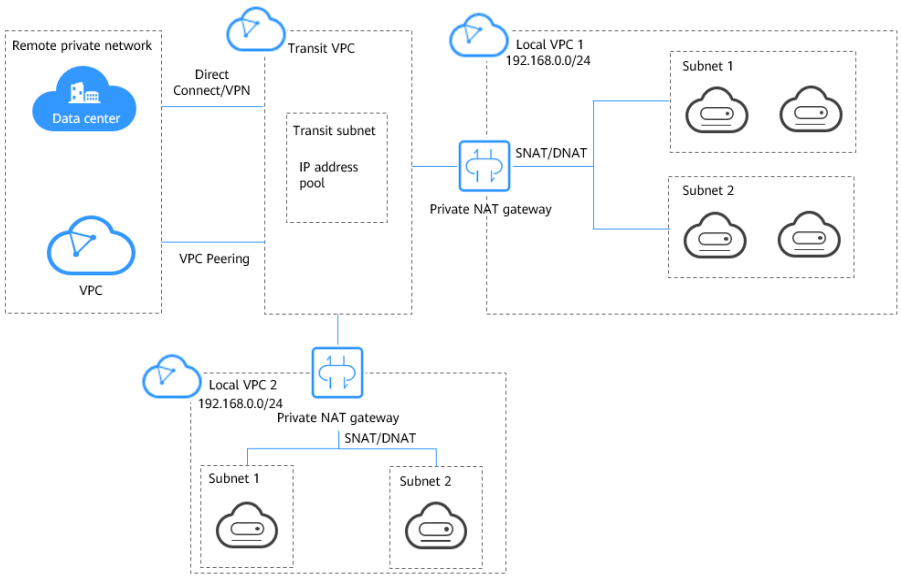
Sub-rede de trânsito

Uma sub-rede de trânsito é onde reside um endereço IP de trânsito.

VPC de trânsito

Uma VPC de trânsito é onde uma sub-rede de trânsito reside.

Figura 2-3 Gateway NAT privado



Um gateway NAT privado pode ser implantado em:

- **Conecte VPCs com blocos CIDR sobrepostos**

  Você pode implantar um gateway NAT privado e configurar regras de SNAT e de DNAT para permitir que duas VPCs com blocos CIDR sobrepostos se comuniquem entre si.

- **Acesse uma rede privada a partir de um endereço IP específico**

  Um gateway NAT privado permite que você use um endereço IP específico para acessar um data center local ou uma VPC em uma rede privada remota. O data center local se conecta à VPC de trânsito por meio do Direct Connect ou VPN. A VPC remota se conecta à VPC de trânsito por meio de uma conexão de emparelhamento de VPC. Conforme mostrado na figura, um gateway NAT privado é implantado e uma regra de SNAT é configurada para que o gateway NAT privado substitua os endereços IP privados na VPC 1 por um endereço IP específico para que a VPC 1 possa se comunicar com a rede privada à esquerda por meio desse endereço IP específico.

NOTA

- Os gateways NAT privados são gratuitos por tempo limitado nas seguintes regiões: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg e LA-Mexico City2.
- Os gateways NAT privados são faturados nas seguintes regiões: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok e AP-Singapore.

Como faço para acessar o serviço de NAT Gateway?

Você pode acessar o serviço NAT Gateway por meio do console de gerenciamento ou usando APIs baseadas em HTTPS.

- Console de gerenciamento

  Faça login no console de gerenciamento e escolha o **NAT Gateway** na lista de serviços para executar operações no gateway NAT.

- APIs

Use APIs se precisar integrar o NAT Gateway em sua própria solução de sistema. Para obter detalhes, consulte a ***Referência de API do NAT Gateway***.

3 Vantagens do produto

Vantagens dos gateways NAT públicos

- **Implementação flexível**

  Um gateway NAT pode ser compartilhado entre sub-redes e AZs, de modo que, mesmo que um AZ falhe, o gateway NAT público ainda possa ser executado normalmente em outro AZ. O tipo e o EIP de um gateway NAT público podem ser alterados a qualquer momento.

- **Facilidade de uso**

  Diversos tipos de gateways NAT estão disponíveis. A configuração do gateway NAT público é simples, a operação e a manutenção são fáceis e podem ser provisionadas rapidamente. Uma vez provisionados, eles podem ser executados de forma estável.

- **Custo-benefício**

  Vários servidores podem compartilhar um EIP. Você pode associar um ou mais EIPs a um gateway NAT público para permitir que vários servidores em uma rede privada se conectem à Internet por meio desse EIP. Você não precisa mais configurar um EIP para cada servidor, o que economiza dinheiro em EIPs e largura de banda.

Vantagens dos gateways NAT privados

- **Planejamento de rede mais fácil**

  Diferentes departamentos em uma grande empresa podem ter blocos CIDR sobrepostos, portanto, a empresa precisa replanejar sua rede antes de migrar suas cargas de trabalho para a nuvem. O replanejamento é demorado e estressante. O gateway NAT privado elimina a necessidade de replanejar a rede para que os clientes possam reter sua rede original enquanto migram para a nuvem.

- **Fácil operação & manutenção**

  Os departamentos de uma grande empresa geralmente têm redes hierárquicas para organizações hierárquicas, gerenciamento baseado em direitos e domínio e isolamento de segurança. Tais redes hierárquicas precisam ser mapeadas para uma rede de grande escala para permitir a comunicação entre elas. Um gateway NAT privado pode mapear o bloco CIDR de cada departamento para o mesmo bloco CIDR da VPC, o que simplifica o gerenciamento de redes complexas.

- **Segurança forte**

  Os departamentos de uma empresa podem precisar de diferentes níveis de segurança. Os gateways NAT privados podem expor os endereços IP e as portas de apenas blocos CIDR

especificados para atender aos requisitos de alta segurança. Uma agência de regulamentação do setor pode exigir que outras organizações usem um endereço IP especificado para acessar seu sistema de regulamentação. Os gateways NAT privado podem ajudar a atender a esse requisito mapeando endereços IP privados para esse endereço IP especificado.

- **Zero conflitos de IP**

  Serviços isolados de vários departamentos geralmente usam endereços IP do mesmo bloco CIDR privado. Depois que a empresa migra as cargas de trabalho para a nuvem, ocorrem conflitos de endereço IP. Graças ao mapeamento de endereços IP, os gateways NAT privados permitem a comunicação entre blocos CIDR sobrepostos.

4 Cenários

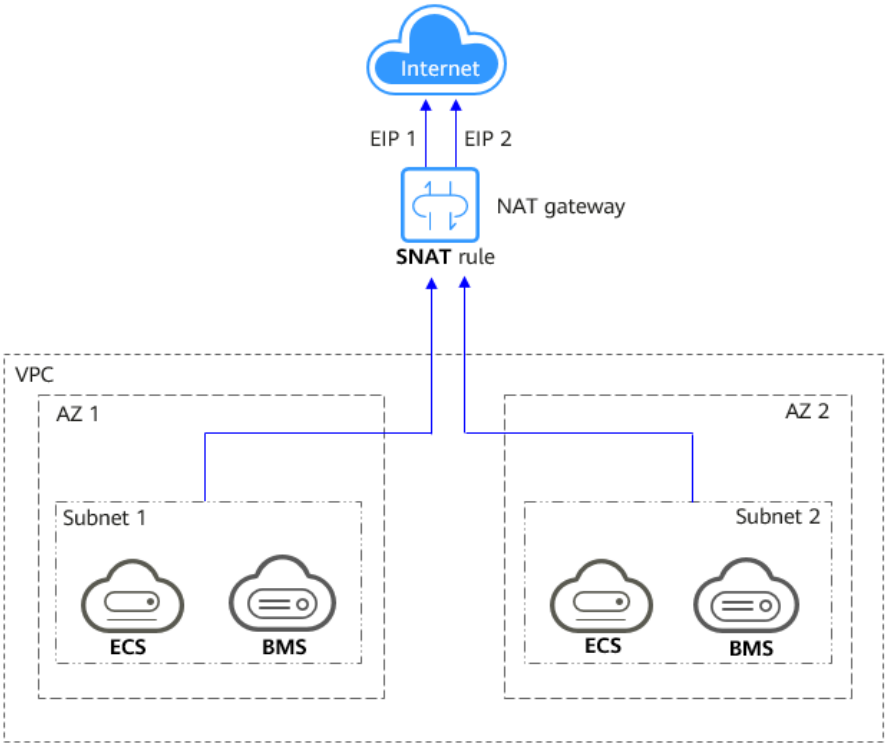
Gateway NAT público

- **Permitir que uma rede privada acesse a Internet usando SNAT**

  Se os servidores de uma VPC precisarem acessar a Internet, você poderá configurar regras de SNAT para permitir que esses servidores usem um ou mais EIPs para acessar a Internet sem expor seus endereços IP privados. Você pode configurar apenas uma regra de SNAT para cada sub-rede em uma VPC e selecionar um ou mais EIPs para cada regra de SNAT. O NAT Gateway público fornece diferentes números de conexões e você pode criar várias regras de SNAT para atender aos requisitos de serviço.

  Figura 4-1 mostra como os servidores em uma VPC acessam a Internet usando o SNAT.

Figura 4-1 Usar o SNAT para permitir que os servidores em uma VPC acessem a Internet



- **Permitir que os usuários da Internet acessem um serviço em uma rede privada usando o DNAT**

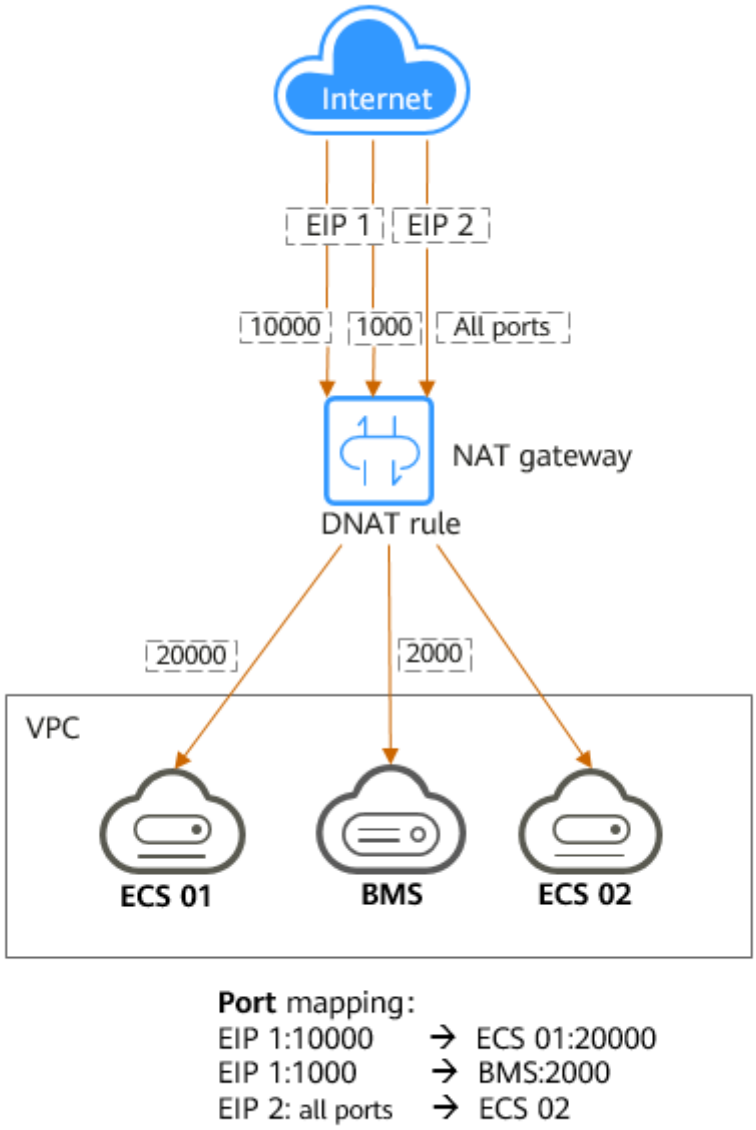
  As regras do DNAT permitem que os servidores em uma VPC forneçam serviços acessíveis pela Internet.

  Depois de receber solicitações de uma porta específica sobre um protocolo específico, o gateway NAT público pode encaminhar as solicitações para uma porta específica de um servidor através do mapeamento de portas. O gateway NAT público também pode encaminhar todas as solicitações destinadas a um EIP para um servidor específico por meio do mapeamento de endereços IP.

  Uma regra de DNAT pode ser configurada para cada servidor. Se houver vários servidores, você poderá criar várias regras de DNAT para mapear um ou mais EIPs para os endereços IP privados desses servidores.

  Figura 4-2 mostra como os servidores (ECSs ou BMSs) em uma VPC fornecem serviços acessíveis da Internet usando o DNAT.

Figura 4-2 Usar o DNAT para permitir que os servidores em uma VPC forneçam serviços acessíveis pela Internet

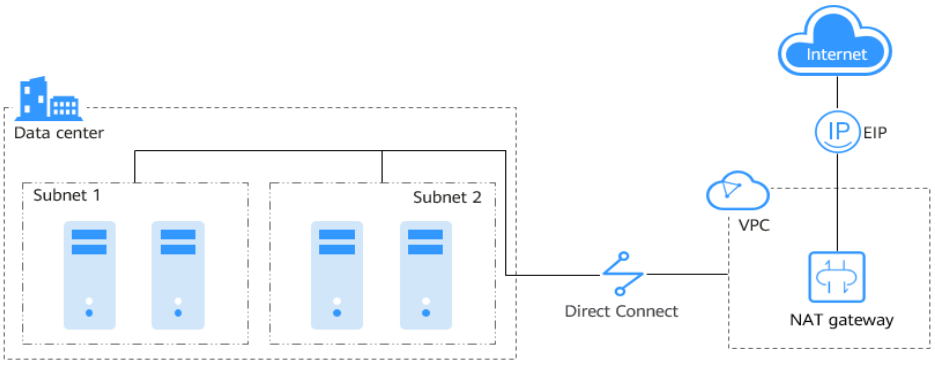


- **Permitir que servidores em um data center local acessem a Internet ou sejam acessíveis a partir da Internet**

  Em certos cenários de Internet, jogos, comércio eletrônico e financeiros, um grande número de servidores em uma nuvem privada está conectado a uma VPC por meio do Direct Connect ou VPN. Se esses servidores precisarem de acesso seguro e de alta velocidade à Internet ou precisarem fornecer serviços acessíveis pela Internet, você poderá implantar um gateway NAT e configurar regras de SNAT e de DNAT para atender aos requisitos deles.

  Figura 4-3 mostra como usar SNAT e DNAT para fornecer acesso à Internet de alta velocidade ou fornecer serviços acessíveis a partir da Internet.

Figura 4-3 Usar SNAT e DNAT para permitir a comunicação de alta velocidade com a Internet



- **Configurar um sistema altamente disponível adicionando vários EIPs a uma regra de SNAT**

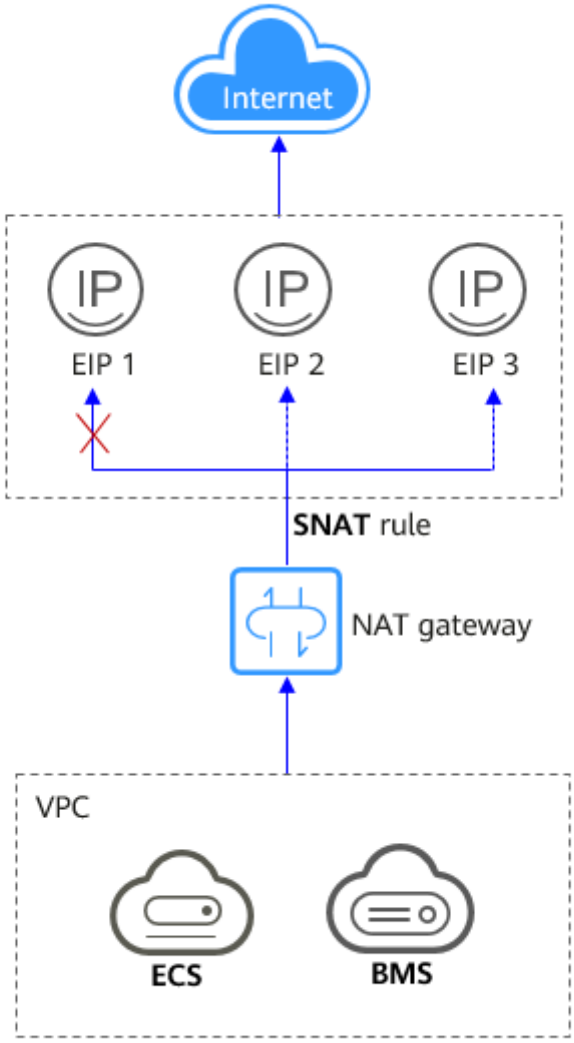
  EIPs podem ser atacados. Para melhorar a confiabilidade do sistema, você pode vincular vários EIPs a uma regra de SNAT para que, se um EIP for atacado, outro EIP possa ser usado para garantir a continuidade do serviço.

  Cada regra de SNAT pode ter até 20 EIPs. Se uma regra de SNAT tiver vários EIPs, o sistema selecionará aleatoriamente um EIP para os servidores usarem para acessar a Internet.

  Se algum EIP for bloqueado ou atacado, remova-o manualmente do pool de EIP.

  Figura 4-4 mostra um sistema altamente disponível usando uma regra de SNAT de um gateway NAT público.

Figura 4-4 Usar a regra de SNAT de um gateway NAT público para criar um sistema altamente disponível



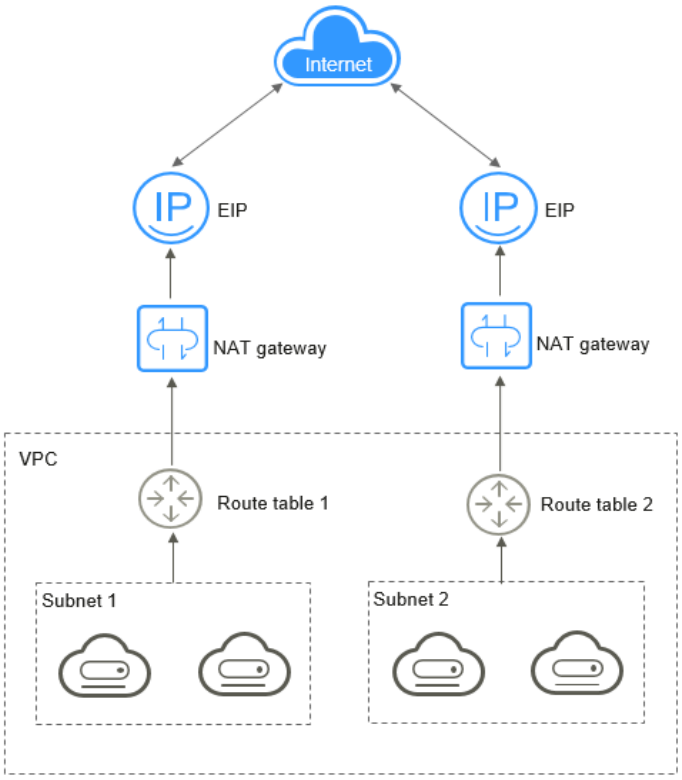
- **Usar vários gateways NAT juntos**

  Se um único gateway NAT não puder atender aos requisitos de desempenho, por exemplo, se houver mais de um milhão de conexões de SNAT ou se a largura de banda máxima de 20 Gbit/s não puder atender aos requisitos de serviço, você poderá usar vários gateways NAT juntos.

  Para usar vários gateways NAT juntos, é necessário associar as tabelas de rotas das sub-redes VPC a esses gateways NAT públicos.

  Figura 4-5 mostra como vários gateways NAT públicos são usados para superar o gargalo de desempenho.

Figura 4-5 Usar vários gateways NAT públicos juntos



NOTA

- O sistema não adiciona uma rota padrão para um gateway NAT público. Você precisa adicionar uma rota apontando para o gateway NAT público à tabela de rotas correspondente.
- Cada gateway NAT público tem uma tabela de rotas associada. O número de gateways NAT públicos que podem ser criados em uma VPC é determinado pelo número de tabelas de rotas para a VPC.

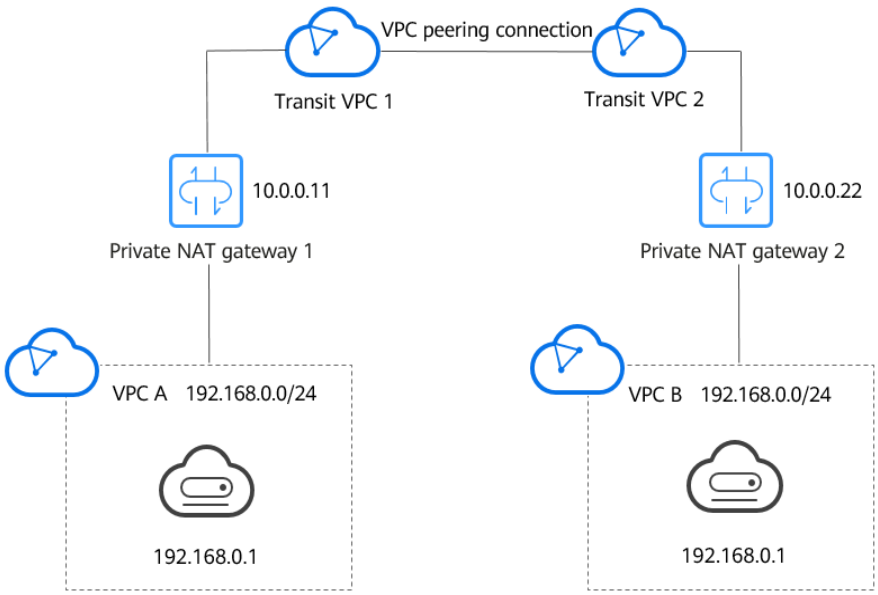
Gateway NAT privado

- **Conectar VPCs com blocos CIDR sobrepostos**

  Você pode configurar dois gateways NAT privados para duas VPCs com blocos CIDR sobrepostos, e, em seguida, adicione regras de SNAT e de DNAT nos dois gateways NAT privados para permitir que os servidores nas duas VPCs usem os endereços IP de trânsito para se comunicarem entre si.

  Na figura a seguir, há duas VPCs de trânsito e dois gateways NAT privados. O endereço 192.168.0.1 na VPC A é convertido para 10.0.0.11 e o endereço IP 192.168.0.1 na VPC B é convertido para 10.0.0.22. Uma conexão de emparelhamento de VPC pode ser estabelecida entre as duas VPCs de trânsito para permitir a comunicação entre elas.

Figura 4-6 Conectar VPCs com blocos CIDR sobrepostos

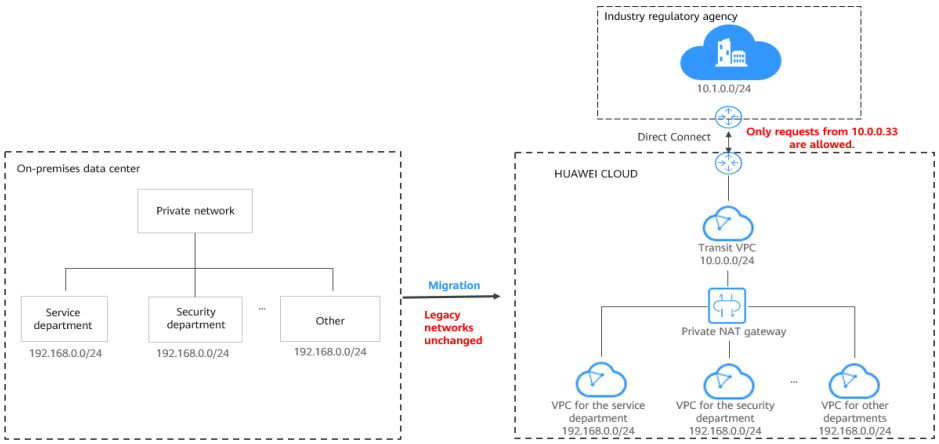


- **Migração de cargas de trabalho para a nuvem sem alterar a topologia da rede ou acessar agências reguladoras a partir de endereços IP específicos**

  As organizações podem querer migrar suas cargas de trabalho para a nuvem sem fazer alterações na topologia de rede existente. Eles também podem ter que acessar agências reguladoras a partir de endereços IP específicos, conforme exigido por essas agências. Um gateway NAT privado é uma boa escolha.

  A figura a seguir representa uma rede corporativa onde as sub-redes de diferentes departamentos se sobrepõem. Um gateway NAT privado permite que a empresa mantenha a topologia de rede existente inalterada enquanto migra suas cargas de trabalho para a nuvem. Neste exemplo, o gateway NAT privado mapeia o endereço IP de cada departamento para 10.0.0.33 para que cada departamento possa usar 10.0.0.33 para acessar com segurança a agência reguladora.

  Figura 4-7 Migrar cargas de trabalho para a nuvem sem alterar a topologia da rede ou acessar agências reguladoras de endereços IP específicos



5 Especificações do gateway NAT

O desempenho do gateway NAT é determinado pelo número máximo de conexões de SNAT suportadas.

Gateway NAT público

Uma conexão de SNAT consiste em um endereço IP de origem, porta de origem, endereço IP de destino, porta de destino e um protocolo de camada de transmissão. O endereço IP de origem é o EIP e a porta de origem é a porta EIP. Uma conexão de SNAT identifica exclusivamente uma sessão.

A taxa de transferência é a largura de banda total de todos os EIPs nas regras do DNAT. Por exemplo, um gateway NAT público tem duas regras de DNAT. A largura de banda do EIP na primeira regra de DNAT é de 10 Mbit/s, e que na segunda regra de DNAT é de 5 Mbit/s. A taxa de transferência do gateway NAT público será de 15 Mbit/s.

Um gateway NAT público suporta até 20 Gbit/s de largura de banda.

O período de tempo limite padrão de uma conexão de SNAT sobre TCP é de 900 segundos.

O período de tempo limite padrão de uma conexão de SNAT em UDP é de 300 segundos.

Selecione um gateway NAT público com base em seus requisitos de serviço. **Tabela 5-1** lista as especificações públicas do gateway NAT.

Tabela 5-1 Especificações de gateway NAT público

Tipo	Número máximo de conexões de SNAT	Largura de banda	Pacotes por segundo (PPS)
Pequeno	10.000	20 Gbit/s	2.000.000
Médio	50.000	20 Gbit/s	2.000.000
Grande	200.000	20 Gbit/s	2.000.000
Extra-grande	1.000.000	20 Gbit/s	2.000.000

NOTA

- O PPS de cada tipo de gateway NAT é 2.000.000 nas direções de entrada e saída.
- Se o número de solicitações exceder o máximo permitido de conexões de um gateway NAT público, os serviços serão afetados negativamente. Para evitar essa situação, crie regras de alarme no console do Cloud Eye para monitorar o número de conexões de SNAT.
- As regras de DNAT de um gateway NAT público são irrelevantes para o tipo de gateway NAT. Até 200 regras de DNAT podem ser adicionadas a um gateway NAT público. Para aumentar o número de regras do DNAT, **envie um tíquete de serviço**

Gateway NAT privado

Uma conexão de SNAT consiste em um endereço IP de origem, porta de origem, endereço IP de destino, porta de destino e um protocolo de camada de transmissão. O endereço IP de origem é o endereço IP de trânsito e a porta de origem é a porta do endereço IP de trânsito.

Selecione um gateway NAT privado com base em seus requisitos de serviço. **Tabela 5-2** lista as especificações do gateway NAT privado.

Tabela 5-2 Especificações do gateway NAT privado

Tipo	Número máximo de conexões de SNAT	Largura de banda	PPS	Número de regras de NAT (Regras de SNAT +regras de DNAT)
Pequeno	2000	200 Mbit/s	20.000	20
Médio	5000	500 Mbit/s	50.000	50
Grande	20.000	2 Gbit/s	200.000	200
Extra-grande	50.000	5 Gbit/s	500.000	500

NOTA

Se o número de solicitações exceder o máximo de conexões permitidas de um gateway NAT privado, os serviços serão afetados negativamente. Para evitar essa situação, crie regras de alarme no console do Cloud Eye para monitorar o número de conexões de SNAT.

6 Observações e restrições

Gateway NAT público

Ao usar um gateway NAT público:

- Várias regras para um gateway NAT público podem usar o mesmo EIP, mas as regras para diferentes gateways NAT devem usar diferentes EIPs.
- Cada VPC pode ser associada a vários gateways NAT públicos.
- Apenas uma regra de SNAT pode ser adicionada para cada sub-rede da VPC.
- O SNAT e o DNAT podem compartilhar um EIP para economizar recursos do EIP. No entanto, uma regra SNAT não pode compartilhar um EIP com uma regra DNAT cujo **Port Type** é definido como **All ports**.
- Se um EIP e um gateway NAT público estiverem configurados para um servidor, os dados serão encaminhados por meio do EIP.
- Se a regra for usada no cenário Direct Connect, o bloco CIDR personalizado deverá ser um bloco CIDR de uma conexão de Direct Connect e não poderá se sobrepor às sub-redes de VPC do gateway NAT.
- Depois de executar operações em recursos subjacentes de um ECS, por exemplo, alterando suas especificações, as regras de gateway NAT configuradas se tornarão inválidas. Exclua as regras e as recrie para as novas especificações.
- Apenas uma regra DNAT pode ser configurada para cada porta em um servidor. Uma porta pode ser mapeada para apenas um EIP.
- Os endereços IP privados usados pelos balanceadores de carga não podem ser configurados quando você adiciona regras de DNAT em gateways NAT públicos para comunicações pela Internet.
- Até 200 regras de DNAT podem ser adicionadas a um gateway NAT público. O número de regras de SNAT que podem ser adicionadas a um gateway NAT público não é limitado.
- Algumas operadoras bloquearão as seguintes portas por razões de segurança. Recomenda-se que você não use as seguintes portas.

Protocolo	Porta
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996

Protocolo	Porta
UDP	135 a 139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

Gateway NAT privado

Ao usar um gateway NAT privado:

- Adicione manualmente rotas na VPC para conectá-la à rede privada remota por meio de uma conexão de emparelhamento de VPC, Direct Connect ou conexão de VPN.
- Apenas uma regra de SNAT pode ser adicionada para cada sub-rede da VPC.
- As regras de SNAT e de DNAT não podem compartilhar um endereço IP de trânsito.
- Uma regra de DNAT com **Port Type** definido como **All ports** não pode compartilhar o mesmo endereço IP de trânsito com uma regra de DNAT com **Port Type** definido como **Specific port**.
- O número total de regras de DNAT e de SNAT que podem ser adicionadas a um gateway NAT privado varia de acordo com o tipo de gateway NAT privado.
  - Pequeno: 20 ou menos
  - Médio: 50 ou menos
  - Grande: 200 ou menos
  - Extra-grande: 500 ou menos

NOTA

- Os gateways NAT privados são gratuitos por tempo limitado nas seguintes regiões: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg e LA-Mexico City2.
- Os gateways NAT privados são faturados nas seguintes regiões: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok e AP-Singapore.

7 Usar o NAT Gateway com outros serviços

Figura 7-1 mostra a relação entre o NAT Gateway e outros serviços.

Figura 7-1 Relação entre o NAT Gateway e outros serviços

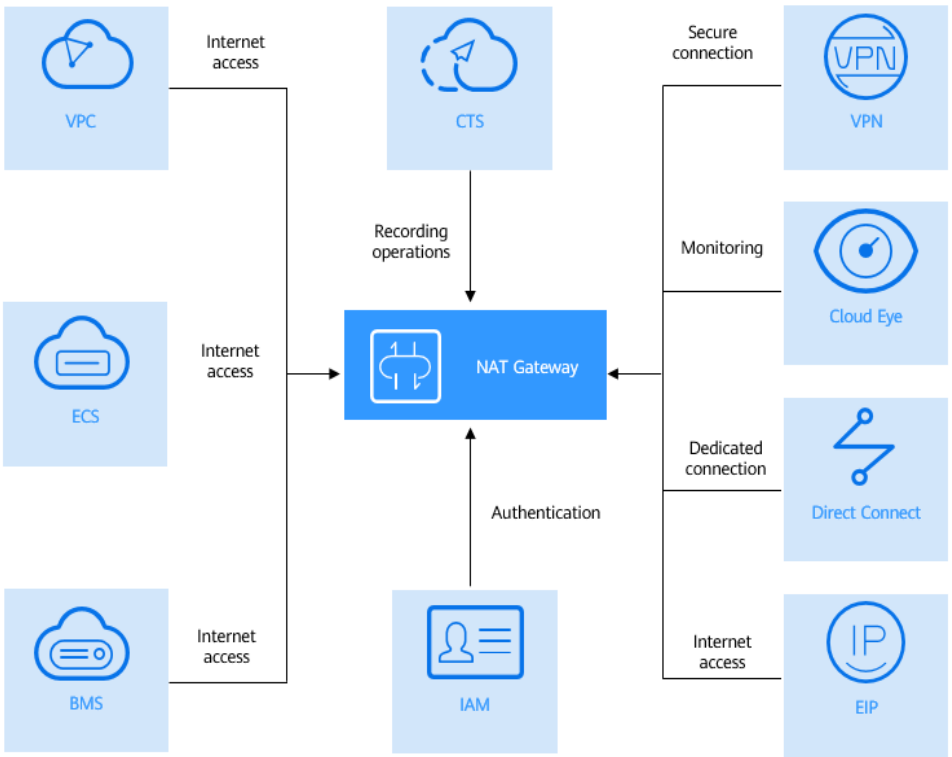


Tabela 7-1 Serviços relacionados

Serviço de nuvem	Interação	Referência
Direct Connect	Os servidores locais conectados a uma VPC por meio do Direct Connect podem usar um gateway NAT público para acessar a Internet ou fornecer serviços acessíveis pela Internet.	**Configuração de regras de SNAT e de DNAT para permitir que servidores locais se comuniquem com a Internet em alta velocidade**
Virtual Private Network (VPN)	Uma VPN estabelece um túnel de comunicação criptografado baseado na Internet entre sua rede local e uma VPC. Isso garante acesso seguro à Internet por meio de um gateway NAT público.	**Configuração de regras de SNAT e de DNAT para permitir que servidores locais se comuniquem com a Internet em alta velocidade**
ECS e BMS	Os ECSs e os BMSs podem usar um gateway NAT público para acessar a Internet ou fornecer serviços acessíveis a partir da Internet.	**Configuração de regras de SNAT para permitir que servidores acessem a Internet** **Configuração de regras do DNAT para permitir que os servidores forneçam serviços acessíveis a partir da Internet**
VPC	Os ECSs em uma VPC podem se conectar à Internet.	**Configuração de regras de SNAT para permitir que servidores acessem a Internet**
Elastic IP (EIP)	Com um gateway NAT público, os servidores em uma VPC podem compartilhar um EIP para acessar a Internet ou fornecer serviços acessíveis pela Internet.	**Usar o SNAT para permitir que os servidores acessem a Internet** **Configuração de regras do DNAT para permitir que os servidores forneçam serviços acessíveis a partir da Internet**
Cloud Eye	Você pode visualizar os dados de monitoramento do gateway NAT no console do Cloud Eye.	**Visualização de métricas**

Serviço de nuvem	Interação	Referência
Identity and Access Management (IAM)	Se você precisar atribuir permissões diferentes aos funcionários da sua empresa para controlar o acesso deles aos recursos do NAT Gateway, o IAM é uma boa opção para o gerenciamento de permissões refinado.	**Identity and Access Management**
Cloud Trace Service (CTS)	Com o CTS, você pode gravar operações no NAT Gateway para consulta, auditoria e retrocesso posteriores.	**Cloud Trace Service**

8 Cobrança (NAT Gateway público)

Itens cobrados

Os gateways NAT público são faturados com base no tipo de gateway NAT público e na duração do uso.

Quatro tipos de gateways NAT públicos estão disponíveis: pequeno, médio, grande e extra-grande.

Para obter detalhes sobre preços, consulte **Calculadora de preços do NAT Gateway**.

Modos de cobrança

Os gateways NAT públicos são faturados por dia.

Configuração alterada

Se o tipo de gateway NAT for alterado, o gateway NAT com especificações mais altas será cobrado nesse dia.

Cancelamento da assinatura

Para cancelar a assinatura de um gateway NAT público de pagamento por uso, você só precisa excluí-lo.

9 Cobrança (NAT Gateway privado)

Os gateways NAT privados começaram a cobrar a partir de 1º de junho de 2022.

Esta seção descreve os detalhes de faturamento sobre gateways NAT privados.

Itens cobrados

Os gateways de NAT privado são faturados com base no tipo de gateway NAT privado e na duração do uso.

Quatro tipos de gateways NAT privados estão disponíveis: pequeno, médio, grande e extra-grande.

Modos de cobrança

Os gateways NAT privados são cobrados por hora.

NOTA

- Os gateways NAT privados são gratuitos por tempo limitado nas seguintes regiões: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg e LA-Mexico City2.
- Os gateways NAT privados são faturados nas seguintes regiões: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok e AP-Singapore.

Tabela 9-1 Preços unitários do gateway NAT privado de especificações diferentes

Região	Pequeno	Médio	Grande	Extra-grande
CN South-Guangzhou	$0,076/gateway/hora	$0,146/gateway/hora	$0,286/gateway/hora	$0,508/gateway/hora
CN East-Shanghai1				
CN North-Beijing4				

Configuração alterada

As novas especificações entram em vigor imediatamente após a mudança. Você é então cobrado com base nas novas especificações.

cancelamento da assinatura

Para cancelar a inscrição de um gateway NAT privado de pagamento por uso, você só precisa excluí-lo.

10 Gerenciamento de permissões

Você pode usar o Identity and Access Management (IAM) para gerenciar as permissões do NAT Gateway e controlar o acesso aos seus recursos. IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso.

Você pode criar usuários de IAM para seus funcionários e atribuir permissões a esses usuários com base em princípio de privilégio mínimo (PoLP) para controlar o acesso a tipos de recursos específicos. Por exemplo, você pode criar usuários do IAM para desenvolvedores de software e atribuir permissões específicas para permitir que eles usem recursos do NAT Gateway, mas impedi-los de excluir recursos ou executar operações de alto risco.

Se sua conta da Huawei Cloudconta não exigir usuários individuais do IAM para gerenciamento de permissões, pule esta seção.

O IAM pode ser usado gratuitamente. Você paga apenas pelos recursos em sua conta. Para obter mais informações sobre o IAM, consulte **O que é o IAM?**

Permissões do NAT Gateway

Por padrão, os novos usuários do IAM não têm nenhuma permissão atribuída. Para atribuir permissões a esses novos usuários, o administrador da conta precisa adicioná-los a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos.

O NAT Gateway é um serviço de nível de projeto implantado e acessado em regiões físicas específicas. Ao atribuir permissões de NAT Gateway a um grupo de usuários, especifique os projetos específicos da região em que as permissões entrarão em vigor. Se você selecionar **All projects**, as permissões serão concedidas para todos os projetos específicos da região. Ao acessar o NAT Gateway, os usuários precisam mudar para uma região onde foram autorizados a usar esse serviço.

Você pode conceder permissões aos usuários usando funções e políticas.

- Funções: um tipo de mecanismo de autorização grosseira que fornece apenas um número limitado de funções de nível de serviço. Ao usar funções para conceder permissões, você também precisa atribuir funções de dependência. 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 de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível para um controle de acesso mais seguro. Por exemplo, o administrador da conta pode

conceder aos usuários do NAT Gateway apenas as permissões para gerenciar um determinado tipo de gateways NAT e regras de SNAT. A maioria das políticas define permissões com base em APIs. Para as ações de API suportadas pelo NAT Gateway, consulte **Políticas de permissões e ações suportadas**.

Tabela 10-1 lista todas as funções e políticas definidas pelo sistema suportadas pelo NAT Gateway.

Tabela 10-1 Funções e políticas definidas pelo sistema suportadas pelo NAT Gateway

Nome da política	Descrição	Tipo	Dependência
NATFullAccess	Todas as operações em recursos do NAT Gateway.	Política definida pelo sistema	N/A
NATReadOnlyAccess	Permissões somente leitura para todos os recursos do NAT Gateway.	Política definida pelo sistema	N/A
NAT Administrator	Todas as operações em recursos do NAT Gateway.	Função definida pelo sistema	Para receber essa permissão, os usuários também devem ter a permissão **Tenant Guest**.

Tabela 10-2 lista as operações comuns suportadas por cada política ou função do sistema NAT Gateway. Selecione as políticas ou funções conforme necessário.

Tabela 10-2 Operações comuns suportadas por cada política definida pelo sistema ou função do NAT Gateway

Operação	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Criar um gateway NAT	√	x	√
Consultar gateways NAT	√	√	√
Consultar detalhes do gateway NAT	√	√	√
Atualizar um gateway NAT	√	x	√
Excluir um gateway NAT	√	x	√

Operação	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Adicionar uma regra de SNAT	√	x	√
Exibir uma regra de SNAT	√	√	√
Modificar uma regra de SNAT	√	x	√
Deletar uma regra de SNAT	√	x	√
Adicionar uma regra de DNAT	√	x	√
Visualizar uma regra de DNAT	√	√	√
Modificar uma regra de DNAT	√	x	√
Excluir uma regra de DNAT	√	x	√
Excluir regras do DNAT em um lote	√	x	√
Importar regras do DNAT usando modelos	√	x	√
Exportar regras do DNAT usando modelos	√	√	√
Criar uma sub-rede de trânsito	√	x	√
Consultar sub-redes de trânsito	√	√	√
Consultar detalhes sobre uma sub-rede de trânsito	√	√	√
Modificar uma sub-rede de trânsito	√	x	√
Excluir uma sub-rede de trânsito	√	x	√

Operação	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Atribuir um endereço IP de trânsito	√	x	√
Consultar um endereço IP de trânsito	√	√	√
Liberar um endereço IP de trânsito	√	x	√

NOTA

Para adicionar ou modificar uma regra do DNAT, sua conta deve ter a permissão **NAT FullAccess** ou a permissão refinada **nat:dnatRules:create/nat:dnatRules:update**. Após a configuração de uma regra DNAT, adicione uma regra de grupo de segurança para permitir que a Internet acesse os servidores para os quais a regra DNAT está configurada. Caso contrário, a regra de DNAT não pode entrar em vigor. Portanto, a permissão **VPC FullAccess** ou a permissão refinada **vpc:securityGroups:create** é necessária.

Links úteis

- **O que é o IAM?**
- **Criação de um usuário e concessão de permissões de NAT Gateway**
- **Políticas de permissões e ações suportadas**

11 Região e AZ

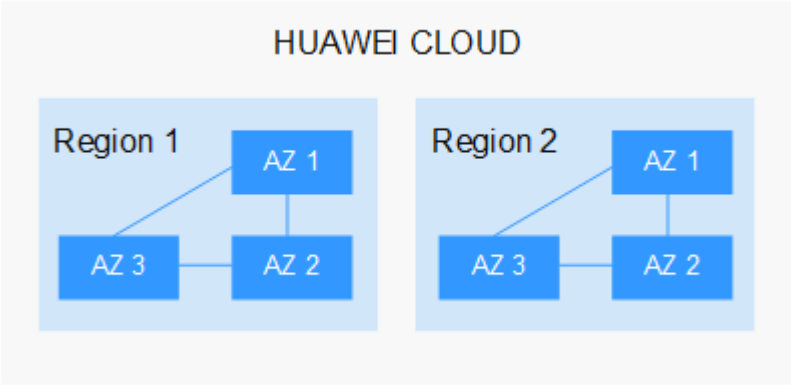
Conceito

Uma região e uma zona de disponibilidade (AZ) identificam a localização de um centro de dados. Você pode criar recursos em uma região e AZ específicas.

- As regiões são divididas com base na localização geográfica e na latência da rede. Serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas em regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços específicos para locatários específicos.
- Uma AZ contém um ou mais centros de data físicos. Cada AZ possui resfriamento, sistema de extinção de incêndio, proteção contra umidade e instalações elétricas independentes. Dentro de uma AZ, computação, rede, armazenamento e outros recursos são logicamente divididos em vários clusters. As AZs dentro de uma região são interconectadas usando fibras ópticas de alta velocidade, para suportar sistemas de alta disponibilidade entre AZs.

Figura 11-1 mostra a relação entre regiões e AZs.

Figura 11-1 Regiões e as AZs



HUAWEI CLOUD fornece serviços em muitas regiões do mundo. Selecione uma região e uma AZ com base nos requisitos. Para obter mais informações, consulte **Regiões globais do Huawei Cloud**.

Selecionar uma região

Ao selecionar uma região, considere os seguintes fatores:

- Localização

  É recomendável selecionar a região mais próxima para menor latência de rede e acesso rápido. As regiões dentro do continente chinês fornecem a mesma infraestrutura, qualidade de rede BGP, bem como operações e configurações de recursos. Portanto, se seus usuários-alvo estiverem no continente chinês, você não precisará considerar as diferenças de latência da rede ao selecionar uma região.

  – Se seus usuários-alvo estiverem na Ásia-Pacífico (excluindo o continente chinês), selecione a região **CN-Hong Kong**, **AP-Bangkok**, ou **AP-Singapore**.

  – Se seus usuários-alvo estão na África, selecione a região **AF-Johannesburg**.

  – Se seus usuários de destino estiverem na América Latina, selecione a região **LA-Santiago**.

  NOTA

  A região **LA-Santiago** está localizada no Chile.

- Preço do recurso

  Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes.

Selecionar uma AZ

Ao implantar recursos, considere os requisitos de recuperação de desastres (DR) e latência de rede de seus aplicativos.

- Para alta capacidade de DR, implante recursos nas diferentes AZs dentro da mesma região.
- Para menor latência de rede, implante recursos na mesma AZ.

Regiões e endpoints

Antes de usar uma API para chamar recursos, especifique sua região e endpoint. Para obter mais detalhes, consulte Regions and Endpoints.

12 Conceitos básicos

EIP

O EIP é um endereço IP estático e público.

Um EIP pode ser acessado diretamente pela Internet. Um endereço IP privado é um endereço IP em uma rede local (LAN) e não pode ser roteado pela Internet.

Você pode vincular um EIP a um ECS em sua sub-rede para permitir que o ECS se comunique com a Internet.

Cada um EIP só pode ser usado por um EIP de cada vez. Se você quiser que vários ECSs na mesma VPC compartilhem um EIP, use um gateway NAT. Para obter mais informações, consulte o **Guia de usuário do NAT Gateway**.

Conexões de SNAT

Uma conexão de SNAT consiste em um endereço IP de origem, porta de origem, endereço IP de destino, porta de destino e um protocolo de camada de transmissão. O endereço IP de origem é o EIP e a porta de origem é a porta EIP. Uma conexão de SNAT identifica exclusivamente uma sessão.

Conexões de DNAT

As conexões de DNAT permitem que os servidores em uma VPC compartilhem um EIP para fornecer serviços acessíveis pela Internet.

