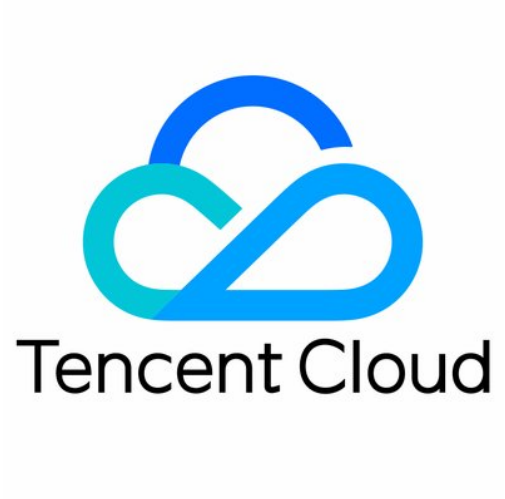
Virtual Private Cloud

Perguntas frequentes

Product Documentation



Contents

Perguntas frequentes
Geral
Conceitos e funcionalidades

Last updated：2024-01-24 17:44:04

Como estabelecer a comunicação entre sub-redes diferentes de um VPC?

Cada VPC tem interconexões de rede privada por padrão, e você pode observar uma rota padrão na tabela de rotas correspondente. Essa rota indica que todos os recursos nesse VPC podem se conectar entre si pela rede privada. As sub-redes em VPCs diferentes não podem se interconectar pela rede privada e podem se comunicar entre si apenas usando Peering Connections ou o CCN.

É possível implantar CVMs diferentes em zonas de disponibilidade diferentes no mesmo VPC?

Sim. Um VPC tem um atributo de região (como Guangzhou, Pequim ou Seul), e as sub-redes no VPC têm um atributo de zona de disponibilidade (como Zona 1 de Guangzhou ou Zona 2 de Guangzhou); portanto, as sub-redes no mesmo VPC podem ser implantadas em zonas de disponibilidade diferentes na mesma região. O atributo de zona de disponibilidade de uma CVM herda o atributo da sub-rede à qual pertence, e as CVMs são adquiridas em sub-redes em zonas de disponibilidade. Portanto, é possível que CVMs diferentes sejam implantados em zonas de disponibilidade diferentes.

Como estabelecer a comunicação entre CVMs e bancos de dados em zonas de disponibilidade diferentes?

Mesmo VPC: há interconexão por padrão. Se eles não se conectarem, você pode dar prioridade à solução de problemas das políticas de firewall do grupo de segurança e da ACL de rede.
VPCs diferentes: você pode usar Peering Connections ou o CCN para implementar a interconexão pela rede privada entre dois VPCs.

Quantos endereços IP privados cada VPC pode fornecer para instâncias de serviço da Tencent Cloud?

Cada VPC pode fornecer até 65.533 endereços IP privados para instâncias de serviço da Tencent Cloud.

O que é o CIDR?

O roteamento entre domínios sem classe (CIDR, na sigla em inglês) implementa a divisão geral da rede usando o bloco de endereços de espaço de rede independente designado por você junto com o IP e a máscara. Ele elimina os conceitos tradicionais de intervalos de endereços e sub-redes de classe A, classe B e classe C, e aloca o espaço de

endereço IP com mais eficiência. Ao criar um VPC e uma sub-rede, você precisa criar o intervalo de IP correspondente na forma de bloco CIDR. Por exemplo, para criar um intervalo de IP de `10.0.16.0 – 10.0.17.255`:
converta `10.0.16.0 – 10.0.17.255` para o formato binário `00001010.00000000.00010000.00000000 – 00001010.00000000.00010001.11111111`, com os primeiros 23 bits sendo os mesmos. O formato do bloco CIDR após a conversão é `10.0.16.0/23`.

Por que não consigo excluir o VPC e a sub-rede depois de encerrar manualmente uma instância do TencentDB for Redis?

Se houver apenas uma instância do TencentDB for Redis no VPC, depois que a instância for encerrada manualmente, ela será movida para a lixeira do TencentDB. No momento, os recursos do Redis ainda não foram liberados, portanto, o VPC não pode ser excluído imediatamente. Você pode resolver esse problema das seguintes maneiras:
Na lixeira do TencentDB, **eliminate (elimine)** a instância do TencentDB for Redis e, depois, exclua o VPC e a sub-rede.
Aguarde a instância do TencentDB for Redis expirar automaticamente na lixeira do TencentDB e, depois, exclua o VPC e a sub-rede.
Para mais informações, consulte Encerramento de instâncias.

Por que uma solicitação de EIP falha?

Quando a cota de EIP for excedida, a solicitação de EIP falhará. Para mais informações sobre como exibir os detalhes da cota, consulte Limites de cota de EIP.

IP e intervalos de IP

Last updated：2024-01-24 17:44:04

Quais são os limites nos intervalos de IP de VPCs e sub-redes?

O bloco CIDR do VPC da Tencent Cloud aceita o uso de qualquer um dos seguintes intervalos de IP privado:
`10.0.0.0` - `10.255.255.255` (intervalo de máscara entre 12 e 28)
`172.16.0.0` - `172.31.255.255` (intervalo de máscara entre 12 e 28)
`192.168.0.0` - `192.168.255.255` (intervalo de máscara entre 16 e 28)
O bloco CIDR da sub-rede deve estar dentro ou ser igual ao bloco CIDR do VPC.

É possível modificar os intervalos de IP de VPCs e sub-redes?

Ao criar o VPC e a sub-rede, é necessário designar blocos CIDR a eles, e não é possível alterá-los depois de criados. Se não for possível estabelecer um Peering Connection devido à sobreposição de intervalos de IP do VPC, você pode tentar o Cloud Connect Network, que tem granularidade de limite menor (somente os intervalos de IP da sub-rede não podem se sobrepor) ou migrar as instâncias para outro VPC. Para mais detalhes, consulte Alteração para VPC.

O que deve ser feito quando um Peering Connection não é estabelecido devido a um conflito de intervalo de IP do VPC?

Ao estabelecer um Peering Connection, os blocos CIDR dos dois VPCs não podem se sobrepor, caso contrário, o Peering Connection não será estabelecido.
Se os intervalos de IP das sub-redes de dois VPCs que precisam se comunicar não se sobrepuserem, você poderá usar o CCN para estabelecer a comunicação. O CCN reduz os limites de intervalo de IP para o nível da sub-rede quando os VPCs se comunicam.
Por exemplo, se os intervalos de IP dos dois VPCs que precisam se comunicar entre si forem `10.0.0.0/16`, mas os das sub-redes forem respectivamente `10.0.1.0/24` e `10.0.2.0/24`, você pode estabelecer a comunicação usando o CCN. Consulte a Documentação do produto CCN.
Se suas necessidades não forem atendidas usando o CCN, você precisará migrar os recursos dentro das sub-redes sobrepostas.
Para mais detalhes sobre como alterar a sub-rede da CVM, consulte Alterar sub-rede da instância.
Migre as instâncias no VPC conforme instruído em Alteração para VPC.

Posso modificar os IPs privados de recursos em VPCs (CVMs e bancos de dados)?

É possível modificar o IP privado principal de um ENI principal de uma CVM, mas não o IP privado principal de um ENI secundário. Para mais detalhes, consulte Modificação de endereços IP privados.
Você pode modificar o IP privado de instâncias do TencentDB (como instâncias do MySQL). Consulte Personalização de IP e porta.
Não é possível modificar o IP privado do CLB.

Posso migrar CVMs ou bancos de dados de um VPC para outro?

Por enquanto, você pode migrar instâncias da CVM e do TencentDB for MySQL para outro VPC na mesma conta. Outras instâncias do TencentDB não são aceitas.

Para migrar instâncias da CVM, consulte Alteração para VPC.

Para migrar instâncias do TencentDB for MySQL, consulte Opção de rede.

O que os EIPs fazem?

Os EIPs são aplicáveis aos seguintes cenários:

1. **Recuperação de desastres**

É altamente recomendável que você use EIPs para recuperação de desastres. Quando um dos CVMs falhar em fornecer serviços normalmente, você poderá desvincular o EIP dessa CVM e vinculá-lo a uma CVM íntegra para retomar o serviço rapidamente.

2. **Retenção de um IP público específico**

Se você precisar reter um IP público específico em sua conta, poderá convertê-lo em um EIP, que poderá ser usado para acessar redes públicas depois de ser vinculado ao dispositivo. Esse EIP será retido em sua conta até que seja “liberado” por você.

3. **Outros cenários especiais**

Quando você precisar alterar um IP em outros casos especiais, poderá converter o IP público comum em um EIP e, em seguida, vincular/desvincular o EIP. No entanto, com a disponibilidade limitada de recursos EIP, uma cota é imposta à quantidade de EIPs para cada região em uma única conta. Portanto, o planejamento e o uso razoáveis de EIPs são muito importantes.

Como mantenho um IP público inalterado?

Se você precisar reter um IP público específico em sua conta, poderá convertê-lo em um EIP, que poderá ser usado para acessar redes públicas depois de ser vinculado ao dispositivo. Esse EIP será retido em sua conta até que seja “liberado” por você.

Para maiores instruções, consulte Conversão de IPs públicos comuns em EIPs.

É possível converter um EIP novamente em um IP público?

Não é possível converter um EIP novamente em um IP público.

Relacionado à rede clássica

Last updated：2024-01-24 17:44:05

Qual é a diferença entre uma rede clássica e um VPC?

Um Virtual Private Cloud (VPC) é um espaço de rede logicamente isolado na Tencent Cloud.
Os VPCs fornecem mais funcionalidades do que a rede clássica. Para mais informações sobre suas diferenças e como escolher entre eles, consulte Gerenciamento de redes clássicas.

Posso mudar uma CVM de uma rede clássica para um VPC?

Sim. A Tencent Cloud permite migrar uma CVM ou um lote de CVMs de uma rede clássica para um VPC. Para mais etapas e instruções detalhadas, consulte Alteração para VPC.

Atenção:

Essa operação não pode ser desfeita. Leia atentamente o documento antes de realizá-la.

Posso mudar uma CVM de um VPC para uma rede clássica?

Não. Um VPC fornece mais funcionalidades com maior flexibilidade e, portanto, recomendamos que você migre os CVMs da rede clássica para o VPC.

Como posso estabelecer comunicação entre uma CVM da rede clássica e uma CVM baseado no VPC?

Você pode usar o Classiclink para estabelecer a comunicação entre a rede clássica e o VPC.
O uso do Classiclink está sujeito às seguintes limitações:
1. A rede clássica e o VPC que precisam se comunicar estão localizados na mesma região (podem estar em zonas de disponibilidade diferentes, como Zona 1 de Guangzhou e Zona 2 de Guangzhou).
2. O bloco CIDR do VPC (intervalo de IP) deve estar dentro de `10.[0-47].0.0/16` (incluindo subconjuntos). Caso contrário, haverá conflitos.

Se a rede clássica e o VPC atenderem a essas condições, você poderá configurar o Classiclink na página de detalhes do VPC no console, a fim de associar o VPC aos CVMs da rede clássica para interconexão.

Os recursos como Cloud Load Balancers e bancos de dados na rede clássica podem se comunicar com o VPC?

Uma conexão de terminal ajuda a estabelecer a comunicação entre as instâncias em um VPC e outras instâncias em uma rede clássica por meio da rede privada. Ela mapeia os endereços IP de instâncias da rede clássica para endereços IP do VPC, permitindo que você acesse as instâncias da rede clássica por meio de um endereço IP do VPC. Os produtos da rede clássica, incluindo o CLB clássico, o TencentDB, o CMEM, o REDIS e o MongoDB, podem se comunicar com o VPC dessa maneira. A comunicação entre regiões e entre contas diferentes não é aceita.

Direção: unidirecional (o VPC acessa a rede clássica).
Se necessário, envie um tíquete para solicitar.

As instâncias da rede clássica e do VPC em contas diferentes podem se comunicar?

Não. Um VPC fornece mais funcionalidades com maior flexibilidade e, portanto, recomendamos que você migre os recursos da rede clássica para o VPC.

Como posso desassociar uma CVM de um VPC ou de uma rede clássica?

Realize as etapas a seguir para desassociar uma CVM.
1. Faça login no Console do VPC.
2. Clique no ID do VPC que está interconectado com a rede clássica para acessar a página de detalhes do VPC.
3. Clique em **Classiclink**. Na lista de CVMs da rede clássica, selecione a CVM a ser desassociada e clique em **Disassociate (Desassociar)**.
4. Clique em **OK**.
5.
Para mais instruções detalhadas, consulte a seção “Desassociação de uma CVM do VPC e da rede clássica” em Gerenciamento de redes clássicas.

Sobre a cota de produtos

Last updated：2024-01-24 17:44:05

Existe um limite de cota para as instâncias do VPC? Quantos VPCs podem ser criados para cada conta?

Alguns recursos do VPC estão sujeitos a limites de cota de uso. Por padrão, uma conta pode criar até 20 VPCs em cada região.

Quantos EIPs uma conta pode solicitar?

Cada conta da Tencent Cloud pode solicitar até 20 EIPs em cada região.
Para cada conta da Tencent Cloud, o limite máximo diário de chances de aquisição é padronizado para 40 (cota * 2).
Depois que um EIP é desvinculado, cada conta pode ser reatribuída com endereços IP públicos 10 vezes por dia gratuitamente.
Cada conta de faturamento por CVM tem uma cota diária gratuita de 10 chances de obter endereços IP públicos depois de desvincular um EIP. Para mais informações, consulte a seção **Limites de cota** em IP elástico (EIP).

Conexão

Conexão com a rede pública

Last updated：2024-01-24 17:44:05

Como solicito um IP público se não tiver sido atribuído na aquisição da CVM?

Se um IP público não foi atribuído quando você adquiriu a CVM, não há como solicitar novamente um IP público comum para essa CVM. No entanto, a mesma função pode ser realizada usando EIPs. Para mais informações sobre como usá-los, consulte Solicitação de EIPs.

Um EIP é um tipo de IP público que é fixado em um endereço IP público específico em uma determinada região. Ao contrário de um IP público comum, ele é vinculado à sua conta. Em outras palavras, você pode vincular e desvincular um EIP a CVMs diferentes conforme necessário (apenas um pode ser vinculado por vez).

Devido à natureza especial de um EIP, se você solicitar um EIP, mas não o vincular a uma instância, serão cobradas taxas de recursos de IP. Para mais detalhes, consulte Faturamento de EIP.

Como uma instância (da CVM ou banco de dados) pode acessar a rede pública sem um endereço IP público?

Uma instância sem um IP público pode solicitar um EIP (confira a pergunta anterior) ou pode acessar a rede pública por meio do NAT Gateway.

O NAT Gateway pode fornecer funcionalidades SNAT e DNAT para instâncias da CVM em VPCs. Se você tiver várias instâncias e quiser que elas acessem a rede pública por meio do mesmo IP público, poderá usar um NAT Gateway.

É possível alterar o IP público de uma CVM?

Sim.

Se a instância da CVM usa o IP público atribuído no momento da aquisição, consulte Alteração de endereços IP públicos.

Se a instância da CVM estiver vinculada a um EIP, primeiro você precisará desvincular o EIP e depois solicitar outro EIP ou vincular um EIP existente.

Atenção:

Recomendamos que você libere o EIP imediatamente após ele ser convertido de um IP público. Caso contrário, o EIP que não estiver vinculado a uma instância incorrerá em taxas de recursos de IP.

É possível recuperar um IP público usado anteriormente? Posso solicitar um EIP específico?

Você pode recuperar os IPs públicos que usou anteriormente e que não estão atribuídos a outros usuários. Os IPs públicos recuperados são todos EIPs. Para mais informações, consulte Recuperar o endereço IP da rede pública.

Uma cota maior pode ser solicitada depois que a quantidade de EIPs atingir o limite máximo?

Devido aos recursos limitados de EIP, você pode solicitar apenas 20 por conta por região, e não pode solicitar um aumento de cota. As instâncias da CVM sem IPs públicos podem usar NAT Gateways e outros métodos para acessar a rede pública.

Como uma CVM acessa a rede pública se possui um IP público ou EIP e sua sub-rede também está associada a um NAT Gateway?

Se uma CVM tiver um IP público ou EIP e sua sub-rede também estiver associada a um NAT Gateway (ou seja, a tabela de rotas especifica que o próximo salto do tráfego dessa sub-rede para acessar a rede pública é um NAT Gateway), então a configuração padrão é para que todo o tráfego dessa CVM acesse a rede pública por meio do NAT Gateway.
Se você precisar modificar a prioridade para que o tráfego da instância da CVM para a rede pública passe pelo IP público, consulte Ajuste das prioridades dos NAT Gateways e EIPs.

Quando uma instância da CVM acessa a rede pública por meio de um gateway público ou NAT Gateway, a taxa de rede será cobrada duas vezes?

Não, a taxa de rede será cobrada apenas uma vez. Ao acessar a rede pública por meio de um gateway público ou NAT Gateway, será cobrada apenas a taxa de rede do gateway público correspondente ou a taxa de rede do NAT Gateway.

Comunicação entre VPCs

Last updated：2024-01-24 17:44:04

Como os CVMs ou os bancos de dados se interconectam pela rede privada?

A comunicação de rede privada de CVMs ou bancos de dados em um VPC é, na verdade, a comunicação de endereços IP privados no nível da rede e, portanto, não há diferença entre eles. Os métodos de comunicação em diferentes cenários de endereço IP privado são os seguintes:

Cenário de comunicação	Método de comunicação
Regiões diferentes	Os CVMs ou bancos de dados em regiões diferentes pertencem a instâncias do VPC diferentes e se comunicam por meio de Peering Connections ou do CCN. (Tanto a comunicação da mesma conta quanto a comunicação entre contas diferentes são aceitas.)
Zonas de disponibilidade diferentes	Mesmo VPC: permite a interconexão por padrão. Instâncias do VPC diferentes: comunicam-se por meio de Peering Connections ou do CCN. (Tanto a comunicação da mesma conta quanto a comunicação entre contas diferentes são aceitas.)
Instâncias do VPC diferentes	Comunicam-se por meio de Peering Connections ou do CCN. (Tanto a comunicação da mesma conta quanto a comunicação entre contas diferentes são aceitas.)
Sub-redes diferentes	Mesmo VPC: permite a interconexão por padrão. VPCs diferentes: comunicam-se por meio de Peering Connections ou do CCN. (Tanto a comunicação da mesma conta quanto a comunicação entre contas diferentes são aceitas.)
Entre contas diferentes	A comunicação entre contas diferentes é feita por meio de Peering Connections ou do CCN. (Tanto a comunicação da mesma região quanto a comunicação entre regiões diferentes são aceitas.)

Atenção:

Para a interconexão de VPC entre contas diferentes por meio de Peering Connection ou do CCN, atenção ao seguinte:

A conta raiz possui os recursos. Se você quiser se comunicar com outra conta por meio de Peering Connection ou do CCN, insira a conta raiz.

A subconta só tem permissão de operação por padrão. Solicite a permissão da conta raiz para estabelecer o Peering Connection ou CCN, se necessário.

A **interconexão padrão de rede privada** está presente entre sub-redes diferentes do mesmo VPC (estejam ou não na mesma zona de disponibilidade). Se elas não puderem se conectar umas com as outras, primeiro você pode solucionar os problemas das políticas de firewall do grupo de segurança e da ACL de rede.

O que devo fazer quando um Peering Connection não é estabelecido devido a um conflito de intervalo de IP do VPC?

Quando você tenta estabelecer um Peering Connection, os blocos CIDR das duas instâncias do VPC não podem se sobrepor, caso contrário, o Peering Connection não pode ser estabelecido.

Se os intervalos de IP de ambas as instâncias do VPC que precisam se intercomunicar se sobrepuserem, mas os intervalos de IP da sub-rede não se sobrepuserem, você poderá tentar estabelecer a comunicação por meio do CCN. O CCN pode reduzir os limites do intervalo de endereços IP para o nível da sub-rede quando as instâncias do VPC se comunicam.

Por exemplo, os intervalos de IP das duas instâncias do VPC que precisam se comunicar entre si são `10.0.0.0/16`, mas os das sub-redes são `10.0.1.0/24` e `10.0.2.0/24`, respectivamente. Nesse caso, você pode estabelecer a comunicação por meio do CCN. Para mais informações, consulte CCN.

Se suas necessidades não forem atendidas usando o CCN, você precisará migrar os recursos dentro das sub-redes sobrepostas.

Para mais detalhes sobre como alterar as sub-redes de CVMs, consulte Alterar sub-rede da instância.

Para mais detalhes sobre a migração entre VPCs, consulte Alteração para VPC.

Se o VPC1 estabelece Peering Connections separadamente com o VPC2 e o VPC3, o VPC2 e o VPC3 podem se comunicar entre si?

Não. Duas instâncias do VPC podem estabelecer interconexão por meio de um Peering Connection, mas essa relação de interconexão não é transitiva. Isso significa que quando um Peering Connection é estabelecido entre o VPC1 e o VPC2 enquanto outro Peering Connection é estabelecido entre o VPC1 e o VPC3, a interconexão de tráfego fica indisponível entre o VPC2 e o VPC3 porque o Peering Connection não é transitivo.

Relacionado ao Classiclink

Last updated：2024-01-24 17:44:04

O que é o Classiclink?

O Classiclink é usado para associar os CVMs na rede clássica ao VPC específico, permitindo que os CVMs se comuniquem com serviços da Tencent Cloud, incluindo os CVMs e os bancos de dados no VPC. Para mais informações, consulte Gerenciamento de redes clássicas.

Como posso estabelecer a comunicação entre uma CVM em uma rede clássica e uma CVM em um VPC?

Você pode usar o Classiclink para estabelecer a comunicação entre as redes clássicas e os VPCs.
Ao usar o Classiclink, atenção os seguintes limites:
1. A rede clássica e o VPC que precisam se comunicar devem estar na mesma região (mas podem estar em zonas de disponibilidade diferentes, como Zona 1 de Guangzhou e Zona 2 de Guangzhou).
2. O CIDR (intervalo de IP) do VPC deve ser `10.0.0.0/16 – 10.47.0.0/16` (incluindo subconjuntos), caso contrário ocorrerá um conflito.

Se a rede clássica e o VPC atenderem a essas condições, você poderá configurar a guia **Classiclink** na página de detalhes do VPC no console, a fim de associar o VPC aos CVMs na rede clássica para interconexão.

Os recursos como Cloud Load Balancers e bancos de dados na rede clássica podem se comunicar com o VPC?

Uma conexão de terminal ajuda a estabelecer a comunicação entre as instâncias em um VPC e outras instâncias em uma rede clássica por meio da rede privada. O princípio é mapear os endereços IP de instâncias na rede clássica para endereços IP do VPC, a fim de que você possa acessar uma instância da rede clássica acessando o endereço IP do VPC correspondente. Os serviços que aceitam a rede clássica incluem o CLB clássico, o TencentDB, o CMEM, o REDIS e o MongoDB. A comunicação entre regiões e entre contas diferentes não é aceita.
Direção: unidirecional (o VPC acessa a rede clássica).
Se precisar de mais direções, envie um tíquete para solicitar.

As instâncias da rede clássica e do VPC em contas diferentes podem se comunicar?

Não. Atualmente, os recursos (CVMs e bancos de dados) em instâncias da rede clássica e do VPC em contas diferentes não podem se comunicar entre si. Um VPC fornece mais funcionalidades com maior flexibilidade, por isso recomendamos a migração da rede clássica para o VPC.

Segurança

Relacionado à segurança da VPC

Last updated：2024-01-24 17:44:04

Como posso garantir a segurança de instâncias da CVM no VPC?

O próprio VPC é um ambiente de rede logicamente isolado, e o tráfego pode ser controlado configurando grupos de segurança e ACLs de rede:
Grupo de segurança: fornece controle de tráfego de rede para CVMs no nível da instância. O tráfego que não tem permissão para entrar ou sair da instância é automaticamente rejeitado.
ACL de rede: fornece controle de tráfego de rede no nível da sub-rede.

Porta e grupo de segurança

Last updated：2024-01-24 17:44:05

Perguntas frequentes sobre portas

Quais portas devo abrir antes de fazer login em uma instância?

Normalmente, você precisa abrir a porta 22 para uma instância do Linux ou a porta 3389 para uma instância do Windows. Para mais informações, consulte Casos de aplicação de grupos de segurança.

Por que devo abrir uma porta, e como?

Você deve abrir a porta no grupo de segurança para usar os serviços relacionados.
Por exemplo, se você deseja acessar páginas da Web usando a porta 8080, abra essa porta no grupo de segurança.
Etapas para abrir uma porta:
1. Faça login no console do grupo de segurança e clique no ID/nome do grupo de segurança vinculado a essa instância para acessar sua página de detalhes.
2. Selecione **Inbound/Outbound rule (Regra de entrada/saída)** e clique em **Add a Rule (Adicionar uma regra)**.
3. Digite seu (intervalo de) endereço IP e a porta a ser aberta e selecione **Allow (Permitir)** para abrir a porta.
Para mais informações, consulte Adição de regras de grupos de segurança.

Meus negócios ficaram inacessíveis depois que modifiquei a porta.

Depois de modificar a porta de serviço, você também precisa abrir a porta correspondente no grupo de segurança.

Quais portas não são permitidas pela Tencent Cloud?

As portas a seguir não são permitidas, pois apresentam riscos de segurança e provavelmente serão bloqueadas por ISPs.

Protocolo	Portas não permitidas
TCP	42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900 e 9996
UDP	1026, 1027, 1434, 1068, 5554, 9996, 1028, 1433 e 135 - 139

Não consigo me conectar a um endereço externo pela porta 25 do TCP.

Para melhorar a qualidade do envio de e-mails por meio de endereços IP da Tencent Cloud, os CVMs são impedidos de usar a porta 25 do TCP para se conectarem a endereços externos por padrão. Para desbloquear essa porta, você pode fazer login no console, passar o mouse sobre a área de navegação da conta na parte superior e clicar em **Security Control (Controle de segurança)** que exibirá o link para desbloquear a porta 25.
É possível desbloquear os CVMs cinco vezes em cada conta. Atenção: os CVMs com pagamento conforme o uso não são aceitos.
Para mais informações, consulte Portas comuns do servidor.

Perguntas frequentes sobre grupos de segurança

Por que há uma regra de rejeição definida por padrão em um grupo de segurança?

As regras de grupos de segurança são selecionadas para entrar em vigor com base em sua ordem de cima para baixo; portanto, depois que a regra de permissão definida pela primeira vez for validada, as outras regras serão rejeitadas por padrão. Se a regra abrir todas as portas para a Internet, a regra de rejeição final será inválida. Fornecemos essa configuração padrão por questões de segurança.

Se eu vincular um grupo de segurança incorreto a uma instância, qual será o efeito na instância? Como isso pode ser corrigido?

Possíveis problemas
Você pode não conseguir se conectar remotamente a uma instância do Linux (SSH) ou fazer login remotamente na Área de Trabalho de uma instância do Windows.
Pode falhar ao executar ping remotamente nos endereços IP público e privado da instância da CVM nesse grupo de segurança.
Pode falhar ao acessar por HTTP os serviços da Web expostos pela instância da CVM nesse grupo de segurança.
Pode falhar ao acessar a Internet com a instância nesse grupo de segurança.
Soluções
Caso aconteça algum dos problemas acima, você pode acessar “Security Group Management (Gerenciamento de grupos de segurança)” no console e redefinir a regra do grupo de segurança para, por exemplo, “only bind all-pass security groups by default (apenas vincular grupos de segurança passa-tudo por padrão)”.
Para mais detalhes sobre como definir as regras de grupos de segurança, consulte Grupo de segurança - Regras de grupos de segurança.

O que significam a direção e a política de grupos de segurança?

A política de grupo de segurança funciona nas direções de saída e entrada. A primeira é para filtrar o tráfego de saída da CVM, e a segunda é para filtrar o tráfego de entrada da CVM.
As políticas do grupo de segurança são divididas entre aquelas que **allow (permitem)** e **refuse (recusam)** o tráfego.

Qual é a ordem em que as políticas de grupos de segurança entram em vigor?

A ordem em que as políticas de grupos de segurança entram em vigor é de cima para baixo. O tráfego passa pela sequência de correspondência do grupo de segurança de cima para baixo, e a política entra em vigor assim que houver uma correspondência bem-sucedida.

Por que uma porta aberta para a Internet por um grupo de segurança não pode acessar a instância da CVM?

A CVM está vinculada a vários grupos de segurança, e essa porta é rejeitada por outro grupo de segurança com prioridade mais alta.
A ACL de rede ou o firewall foi configurado.

Como um IP que não é permitido pelo grupo de segurança ainda pode acessar a CVM?

Motivos possíveis:
A CVM está vinculada a vários grupos de segurança, e o IP é permitido por outro grupo de segurança.
Esse endereço IP pertence a um serviço público aprovado da Tencent Cloud.

O iptables pode ser usado junto com grupos de segurança?

Sim, o iptables e os grupos de segurança podem ser usados ao mesmo tempo. O tráfego será filtrado duas vezes da seguinte forma:
Saída: processos na instância > iptables > grupos de segurança.
Entrada: grupos de segurança > iptables > processos na instância.

Todos os CVMs associados ao grupo de segurança foram retornados. Mas ainda não consigo excluir o grupo de segurança.

Além de CVMs, um grupo de segurança também pode ser vinculado a instâncias do CLB, do ENI e de banco de dados na nuvem. Verifique se todas as instâncias vinculadas ao grupo de segurança a ser excluído foram desassociadas.

O nome de um grupo de segurança clonado pode ser o mesmo de um grupo de segurança na região de destino?

Sim.

Posso clonar um grupo de segurança para outro projeto ou região usando uma API?

Sim. Para mais detalhes, consulte CloneSecurityGroup.

Quando eu clono um grupo de segurança para outro projeto ou região, os CVMs associados aos grupos de segurança também serão clonados?

Não. Apenas as regras de entrada e saída do grupo de segurança serão clonadas. Será necessário associar os CVMs novamente após a clonagem.