VPN do cliente da AWS

Guia do administrador

VPN do cliente da AWS: Guia do administrador

Table of Contents

O que é VPN do cliente da AWS?

A VPN do cliente da AWS é um serviço de VPN gerenciado baseado no cliente que protege o acesso aos recursos da AWS e aos recursos na sua rede on-premises. Com o VPN do Cliente, você pode acessar seus recursos de qualquer local usando um cliente de VPN com base no OpenVPN.

Tópicos

Recursos do VPN do Cliente

O VPN do Cliente oferece os seguintes recursos e funcionalidades:

- Conexões seguras: — fornece uma conexão TLS segura de qualquer local usando o cliente OpenVPN.
- Serviço gerenciado: é um serviço gerenciado da AWS e, como tal, remove o peso operacional da implantação e do gerenciamento de uma solução de VPN com acesso remoto de terceiros.
- Altamente disponível e elástico: escala automaticamente para o número de usuários que se conectam aos seus recursos da AWS e aos recursos on-premises.
- Autenticação: oferece suporte para autenticação de cliente usando o Active Directory, a autenticação federada e a autenticação baseada em certificado.
- Controle granular: permite implementar controles de segurança personalizados definindo regras de acesso baseadas na rede. Essas regras podem ser configuradas na granularidade dos grupos do Active Directory. Você também pode implementar o controle de acesso usando grupos de segurança.
- Facilidade de uso: permite que você acesse seus recursos da AWS e recursos on-premises usando um único túnel de VPN.
- Capacidade de gerenciamento: permite que você visualize logs de conexão, que fornecem detalhes sobre tentativas de conexão de clientes. Você também pode gerenciar conexões de clientes ativas, com a capacidade de encerrá-las.
- Integração profunda: integra-se aos serviços da AWS existentes, incluindo o AWS Directory Service e a Amazon VPC.

Componentes do VPN do Cliente

Veja a seguir os principais conceitos de VPN do Cliente:

Endpoint do cliente VPN

O endpoint do cliente VPN é o recurso que você cria e configura para habilitar e gerenciar sessões do cliente VPN. É o ponto de término de todas as sessões da VPN do cliente.

Rede de destino

Uma rede de destino é a rede que você associa a um endpoint do cliente VPN. Uma sub-rede de uma VPC é uma rede de destino. Associar uma sub-rede a um endpoint do cliente VPN permite

estabelecer sessões de VPN. Você pode associar várias sub-redes a um endpoint do cliente VPN para alta disponibilidade. Todas as sub-redes devem ser provenientes da mesma VPC. Cada sub-rede deve pertencer a uma Zona de disponibilidade diferente.

Rota

Cada endpoint do cliente VPN tem uma tabela de rotas que descreve as rotas de redes de destino disponíveis. Cada rota na tabela de rotas especifica o caminho do tráfego para recursos ou redes específicos.

Regras de autorização

Uma regra de autorização restringe os usuários que podem acessar uma rede. Para uma rede especificada, configure o grupo do provedor de identidade (IdP) ou do Active Directory que tem permissão de acesso. Somente os usuários pertencentes a esse grupo podem acessar a rede especificada. Por padrão, não há regras de autorização, e você deve configurá-las para permitir que os usuários acessem recursos e redes.

Cliente

O usuário final que se conecta ao endpoint do cliente VPN para estabelecer uma sessão de VPN. Para estabelecerem uma sessão de VPN, os usuários finais precisam fazer download de um cliente OpenVPN e usar o arquivo de configuração do VPN do Cliente que você criou.

Intervalo CIDR do cliente

Um intervalo de endereços IP do qual devem ser atribuídos endereços IP do cliente. Cada conexão com o endpoint do cliente VPN recebe um endereço IP exclusivo do intervalo CIDR do cliente. Você escolhe o intervalo CIDR do cliente, por exemplo, `10.2.0.0/16`.

Portas VPN do cliente

A VPN do cliente da AWS é compatível com as portas 443 e 1194 para TCP e UDP. O padrão é a porta 443.

Interfaces de rede do VPN do Cliente

Quando você associa uma sub-rede ao endpoint do cliente VPN, criamos interfaces de rede do VPN do Cliente nessa sub-rede. O tráfego enviado para a VPC do endpoint do cliente VPN é enviado por meio de uma interface de rede do VPN do Cliente. A conversão de endereço de rede de origem (SNAT) é aplicada e o endereço IP de origem do intervalo CIDR do cliente é convertido no endereço IP da interface de rede do VPN do Cliente.

Registro em log de conexão

Você pode habilitar o registro em log de conexão para o endpoint do cliente VPN a fim de registrar eventos de conexão. Você pode usar essas informações para executar perícia, analisar como seu endpoint da cliente VPN está sendo usado ou depurar problemas de conexão.

Portal de autoatendimento

Um Cliente VPN fornece um portal de autoatendimento como uma página da Web para que os usuários finais baixem a versão mais recente do AWS VPN Desktop Client e a versão mais recente do arquivo de configuração do endpoint do Cliente VPN, que contém as configurações necessárias para se conectar ao endpoint. O administrador do endpoint do Cliente VPN pode habilitar ou desabilitar o portal de autoatendimento para o endpoint do Cliente VPN. O portal de autoatendimento é um serviço global com suporte de pilhas de serviços nas regiões Ásia-Pacífico (Tóquio), Leste dos EUA (Norte da Virgínia) e Europa (Irlanda) e no AWS GovCloud (EUA-Oeste).

Trabalhar com o Cliente VPN

Você pode trabalhar com o VPN do Cliente de qualquer uma das seguintes formas:

Console da Amazon VPC

O console da Amazon VPC fornece uma interface de usuário baseada na Web para o VPN do Cliente. Se você tiver se registrado para uma conta da AWS, poderá fazer login no console da Amazon VPC e selecionar a cliente VPN no painel de navegação.

AWS Command Line Interface (CLI)

A AWS CLI fornece acesso direto às APIs públicas da cliente VPN. É compatível com Windows, macOS e Linux. Para obter mais informações sobre os conceitos básicos da AWS CLI, consulte o Guia do usuário do AWS Command Line Interface. Para obter mais informações sobre os comandos para a cliente VPN, consulte Referência de comando da AWS CLI.

AWS Tools for Windows PowerShell

A AWS fornece comandos para um amplo conjunto de ofertas da AWS voltadas a usuários que desenvolvem scripts no ambiente do PowerShell. Para obter mais informações sobre os conceitos básicos do AWS Tools for Windows PowerShell, consulte o Guia do usuário do AWS Tools for Windows PowerShell. Para obter mais informações sobre cmdlets para a cliente VPN, consulte Referência de cmdlets do AWS Tools for Windows PowerShell.

API de consulta

A API de consulta HTTPS da cliente VPN proporciona acesso programático à cliente VPN e à AWS. A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço. Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte Ações do AWS Client VPN.

Limitações e regras do VPN do Cliente

O VPN do Cliente tem as seguintes regras e limitações:

- Os intervalos CIDR de cliente não podem se sobrepor ao CIDR local da VPC na qual a sub-rede associada está localizada ou a quaisquer rotas adicionadas manualmente à tabela de rotas do endpoint do cliente VPN.
- Os intervalos de CIDRs do cliente devem ter um tamanho de bloco de pelo menos /22 e não deve ser maior que /12.
- Uma parte dos endereços no intervalo de CIDR do cliente é usada para oferecer suporte ao modelo de disponibilidade do endpoint do cliente VPN e não pode ser atribuída aos clientes. Portanto, é recomendável atribuir um bloco CIDR que contenha o dobro do número de endereços IP necessários para habilitar o número máximo de conexões simultâneas às quais você planeja oferecer suporte no endpoint do cliente VPN.
- O intervalo CIDR do cliente não pode ser alterado depois de criar o endpoint do cliente VPN.
- As sub-redes associadas a um endpoint do cliente VPN deve estar na mesma VPC.
- Você não pode associar várias sub-redes da mesma Zona de disponibilidade a um endpoint do cliente VPN.
- Um endpoint do cliente VPN não é compatível com associações de sub-rede em uma VPC de locação dedicada.
- O VPN do Cliente é compatível somente com tráfego IPv4. Consulte Considerações sobre IPv6 (p. 72) para obter detalhes sobre o IPv6.
- O VPN do Cliente não está em conformidade com o FIPS (Federal Information Processing Standards).
- Se a autenticação multifator (MFA) estiver desabilitada para o Active Directory, uma senha de usuário não poderá estar no seguinte formato.

```
SCRV1:<base64_encoded_string>:<base64_encoded_string>
```

- O portal de autoatendimento não está disponível para clientes autenticados usando a autenticação mútua.
- Não é recomendável se conectar ao endpoint da cliente VPN usando endereços IP. Como a cliente VPN é um serviço gerenciado, você ocasionalmente verá os endereços IP que o nome DNS resolve alterar. Além disso, você verá interfaces de rede da cliente VPN excluídas e recriadas nos seus logs do Cloud Trail, bem como esse comportamento é esperado. É recomendável se conectar ao endpoint da cliente VPN usando o nome DNS fornecido.
- O encaminhamento de IP está desativado atualmente ao usar a aplicação de desktop AWS Client VPN. Ele está desativado desde o lançamento do serviço em 18 de dezembro de 2018, a fim de resolver um problema relatado pelo NIST. Entretanto, entendemos que alguns clientes podem precisar dessa funcionalidade para seus serviços. Embora não tenhamos uma data específica no momento, planejamos habilitar, com segurança, o encaminhamento de IP em uma próxima versão.

Definição de preço para VPN do Cliente

Você é cobrado por cada associação de endpoint e cada conexão VPN por hora. Para obter mais informações, consulte Preço do AWS Client VPN.

Você é cobrado pela transferência de dados do Amazon EC2 para a Internet. Para obter mais informações, consulte a seção Data Transfer (Transferência de dados) na página de definição de preços sob demanda do Amazon EC2.

Se você habilitar o registro em log de conexão para seu endpoint do cliente VPN, será necessário criar um grupo de CloudWatch Logs em sua conta. Aplicam-se cobranças ao uso de grupos de log. Para obter mais informações, consulte Definição de preço do Amazon CloudWatch (em Paid tier [Camada paga], selecione Logs [Registros]).

Se você habilitar o manipulador de conexão do cliente para o endpoint do cliente VPN, será necessário criar e invocar uma função do Lambda. Cobranças são aplicadas ao invocar funções do Lambda. Para obter mais informações, consulte Preço do AWS Lambda.

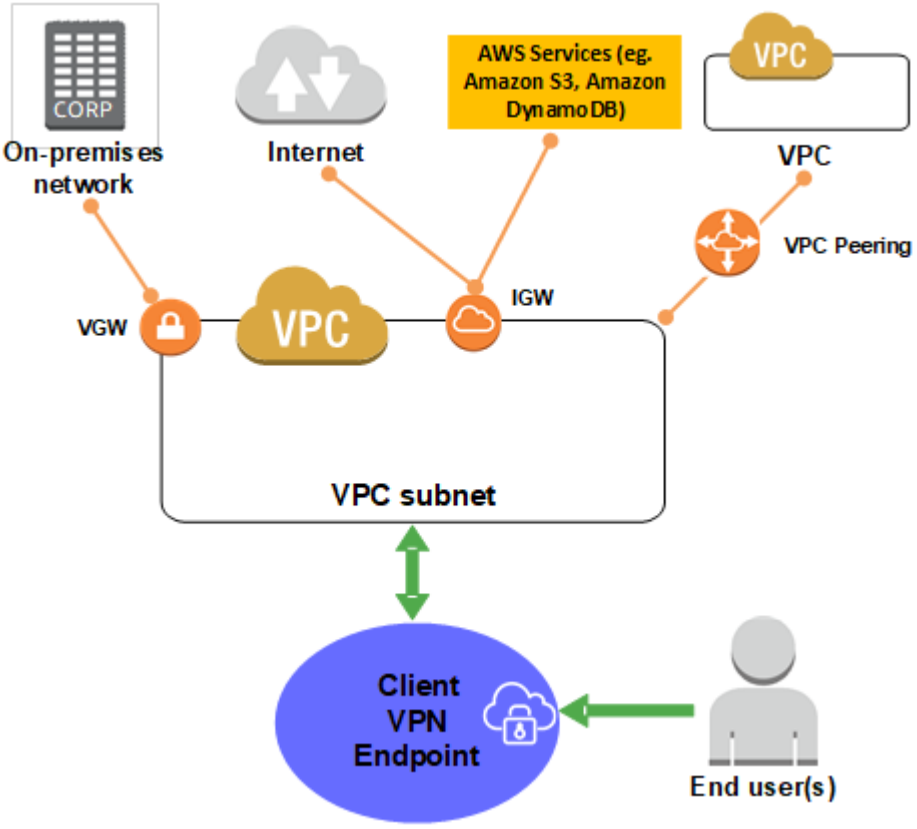
Como a VPN do cliente da AWS funciona

Com a VPN do cliente da AWS, há dois tipos de usuários que interagem com o endpoint da cliente VPN: administradores e clientes.

O administrador é responsável por criar e configurar o serviço. Isso envolve criar o endpoint da cliente VPN, associar a rede de destino, configurar as regras de autorização e configurar rotas adicionais (se necessário). Depois que o endpoint da cliente VPN é criado e configurado, o administrador faz download do arquivo de configuração do endpoint da cliente VPN e o distribui aos clientes que precisam de acesso. O arquivo de configuração do endpoint da cliente VPN inclui o nome DNS do endpoint da cliente VPN e as informações de autenticação necessárias para estabelecer uma sessão de VPN. Para obter mais informações sobre a configuração do serviço, consulte Conceitos básicos da cliente VPN (p. 36).

O cliente é o usuário final. É a pessoa que se conecta ao endpoint da cliente VPN para estabelecer uma sessão de VPN. O cliente estabelece a sessão de VPN em seu computador local ou dispositivo móvel usando um aplicativo cliente de VPN baseado no OpenVPN. Depois de estabelecer a sessão de VPN, ele pode acessar com segurança os recursos na VPC em que a sub-rede associada está localizada. Ele também poderá acessar outros recursos na AWS, em uma rede on-premises ou em outros clientes se a rota necessária e as devidas regras de autorização tiverem sido configuradas. Para obter mais informações sobre como se conectar a um endpoint da cliente VPN para estabelecer uma sessão de VPN, consulte Conceitos básicos no Guia do usuário da VPN do cliente da AWS.

O gráfico a seguir ilustra a arquitetura básica do VPN do Cliente.



Autenticação de cliente

A autenticação do cliente é implementada no primeiro ponto de entrada na Nuvem AWS. Ela é usada para determinar se os clientes têm permissão para se conectar ao endpoint da cliente VPN. Se a autenticação for bem-sucedida, os clientes se conectarão ao endpoint da cliente VPN e estabelecerão uma sessão de VPN. Se a autenticação falhar, a conexão será negada, e o cliente será impedido de estabelecer uma sessão de VPN.

O VPN do Cliente oferece os seguintes tipos de autenticação de cliente:

- Autenticação do Active Directory (p. 6) (baseada no usuário)
- Autenticação mútua (p. 6) (baseada em certificado)
- Single Sign-On (autenticação federada baseada em SAML) (p. 9) (baseado no usuário)

Você pode usar um dos métodos listados acima sozinho ou uma combinação de autenticação mútua com um método baseado em usuário, como o seguinte:

- Autenticação mútua e autenticação federada
- Autenticação mútua e autenticação do Active Directory

> **Important**
>
> Para criar um endpoint da cliente VPN, você deve provisionar um certificado de servidor no AWS Certificate Manager, independentemente do tipo de autenticação usado. Para obter mais informações sobre como criar e provisionar um certificado de servidor, consulte as etapas em Autenticação mútua (p. 6).

Autenticação do Active Directory

O VPN do Cliente é compatível com o Active Directory por meio da integração com o AWS Directory Service. Com a autenticação via Active Directory, os clientes são autenticados com grupos existentes do Active Directory. Usando o AWS Directory Service, a cliente VPN pode se conectar a Active Directories existentes provisionados na AWS ou na sua rede on-premises. Isso permite que você use sua infraestrutura de autenticação de cliente existente. Se você estiver usando um Active Directory on-premises e não tiver um Managed Microsoft AD da AWS, será necessário configurar um Active Directory Connector (AD Connector). Você pode usar um servidor do Active Directory para autenticar os usuários. Para obter mais informações sobre a integração do Active Directory, consulte o Guia de administração do AWS Directory Service.

A cliente VPN é compatível com a autenticação multifator (MFA) quando ela está habilitada para o Managed Microsoft AD da AWS ou o AD Connector. Se a MFA estiver habilitada, os clientes devem inserir um nome de usuário, senha e código MFA ao se conectarem a um endpoint do cliente VPN. Para obter mais informações sobre como habilitar a MFA, consulte Habilitar a autenticação multifator para o Managed Microsoft AD da AWS e Habilitar a autenticação multifator para o AD Connector no Guia de administração do AWS Directory Service.

Para obter cotas e regras para configurar usuários e grupos no Active Directory, consulte Cotas de usuários e grupos (p. 79).

Autenticação mútua

Com a autenticação mútua, a cliente VPN usa certificados para realizar a autenticação entre o cliente e o servidor. Os certificados são uma forma digital de identificação emitida por uma autoridade certificadora (CA). O servidor usa certificados de cliente para autenticar clientes quando eles tentam se conectar ao

endpoint do cliente VPN. É necessário criar um certificado e uma chave de servidor e pelo menos um certificado e uma chave de cliente.

É necessário fazer upload do certificado do servidor para o AWS Certificate Manager (ACM) e especificá-lo ao criar um endpoint da cliente VPN. Ao fazer upload do certificado do servidor no ACM, você também especifica a autoridade de certificação (CA). Você só precisa fazer upload do certificado de cliente no ACM quando a CA do certificado de cliente for diferente da CA do certificado de servidor. Para obter mais informações sobre o ACM, consulte o Guia do usuário do AWS Certificate Manager.

Você pode criar um certificado de cliente separado e uma chave para cada cliente que se conectará ao endpoint do cliente VPN. Isso permite revogar um certificado de cliente específico se um usuário sair de sua organização. Nesse caso, ao criar o endpoint do cliente VPN, é possível especificar o ARN de certificado de servidor para o certificado de cliente, desde que o certificado de cliente seja emitido pela mesma CA que o certificado de servidor.

Note

Um endpoint do cliente VPN é compatível apenas com tamanhos de chave RSA de 1024 bits e 2048 bits. Além disso, o certificado do cliente deve ter o atributo CN no campo Subject (Assunto).

Linux/macOS

O procedimento a seguir usa o OpenVPN easy-rsa para gerar os certificados e as chaves de servidor e cliente e faz upload do certificado e da chave de servidor no ACM. Para obter mais informações, consulte a seção LER de início rápido do Easy-RSA 3.

Para gerar os certificados e as chaves de servidor e cliente e transferi-los por upload ao ACM

1. Clone o repositório easy-rsa do OpenVPN para o computador local e navegue até a pasta `easy-rsa/easyrsa3`.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. Inicialize um novo ambiente PKI.

```
$ ./easyrsa init-pki
```

3. Para criar uma nova autoridade de certificação (CA), execute este comando e siga as instruções.

```
$ ./easyrsa build-ca nopass
```

4. Gere o certificado e a chave de servidor.

```
$ ./easyrsa build-server-full server nopass
```

5. Gere o certificado e a chave de cliente.

   Certifique-se de salvar o certificado de cliente e a chave privada de cliente, pois você precisará deles ao configurar o cliente.

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

   Opcionalmente, você pode repetir essa etapa para cada cliente (usuário final) que exija um certificado e uma chave de cliente.

6. Copie os certificados e as chaves de servidor e de cliente para uma pasta personalizada e depois navegue até ela.

Antes de copiar os certificados e as chaves, crie a pasta personalizada usando o comando `mkdir`. O exemplo a seguir cria uma pasta personalizada em seu diretório base.

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. Faça upload do certificado e da chave do servidor e do certificado e da chave do cliente no ACM. Certifique-se de fazer upload deles na mesma região em que pretende criar o endpoint do cliente VPN. Os comandos a seguir usam a AWS CLI para fazer upload dos certificados. Para fazer upload dos certificados usando o console do ACM, consulte Importar certificados no Guia do usuário do AWS Certificate Manager.

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Você não precisa necessariamente carregar o certificado do cliente no ACM. Se os certificados de servidor e de cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor tanto para o servidor quanto para o cliente ao criar o endpoint do cliente VPN. Nas etapas acima, a mesma CA foi usada para criar ambos os certificados. Entretanto, as etapas para carregar o certificado do cliente estão incluídas para que as instruções fiquem completas.

Windows

O procedimento a seguir instala o software Easy-RSA 3.x e o usa para gerar os certificados e chaves do servidor e do cliente.

Para gerar os certificados e as chaves de servidor e cliente e carregá-los no ACM

1. Acesse a página de lançamentos do EasyRSA, baixe o arquivo ZIP para sua versão do Windows e extraia-o.
2. Abra um prompt de comando e navegue até o local para o qual a pasta `EasyRSA-3.x` foi extraída.
3. Execute o comando a seguir para abrir o shell do EasyRSA 3.

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. Inicialize um novo ambiente PKI.

```
# ./easyrsa init-pki
```

5. Para criar uma nova autoridade de certificação (CA), execute este comando e siga as instruções.

```
# ./easyrsa build-ca nopass
```

6. Gere o certificado e a chave de servidor.

```
# ./easyrsa build-server-full server nopass
```

7. Gere o certificado e a chave de cliente.

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

Opcionalmente, você pode repetir essa etapa para cada cliente (usuário final) que exija um certificado e uma chave de cliente.

8. Saia do shell do EasyRSA 3.

```
# exit
```

9. Copie os certificados e as chaves de servidor e de cliente para uma pasta personalizada e depois navegue até ela.

Antes de copiar os certificados e as chaves, crie a pasta personalizada usando o comando `mkdir`. O exemplo a seguir cria uma pasta personalizada na unidade C:\.

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. Faça upload do certificado e da chave do servidor e do certificado e da chave do cliente no ACM. Certifique-se de fazer upload deles na mesma região em que pretende criar o endpoint do cliente VPN. Os comandos a seguir usam a AWS CLI para fazer upload dos certificados. Para fazer upload dos certificados usando o console do ACM, consulte Importar certificados no Guia do usuário do AWS Certificate Manager.

```
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://
server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-
key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Você não precisa necessariamente carregar o certificado do cliente no ACM. Se os certificados de servidor e de cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor tanto para o servidor quanto para o cliente ao criar o endpoint do cliente VPN. Nas etapas acima, a mesma CA foi usada para criar ambos os certificados. Entretanto, as etapas para carregar o certificado do cliente estão incluídas para que as instruções fiquem completas.

Single Sign-On (autenticação federada baseada em SAML 2.0)

AWS Client VPN suporta federação de identidades com Security Assertion Markup Language 2.0 (SAML 2.0) para terminais do VPN do Cliente. Você pode usar provedores de identidade (IdPs) que sejam compatíveis com SAML 2.0 para criar identidades de usuário centralizadas. Depois, você pode configurar

um endpoint do cliente VPN para usar a autenticação federada baseada em SAML e associá-lo ao IdP. Os usuários se conectam ao endpoint do cliente VPN usando as respectivas credenciais centralizadas.

Para permitir que o IdP baseado em SAML funcione com um endpoint do cliente VPN, você deve fazer o seguinte.

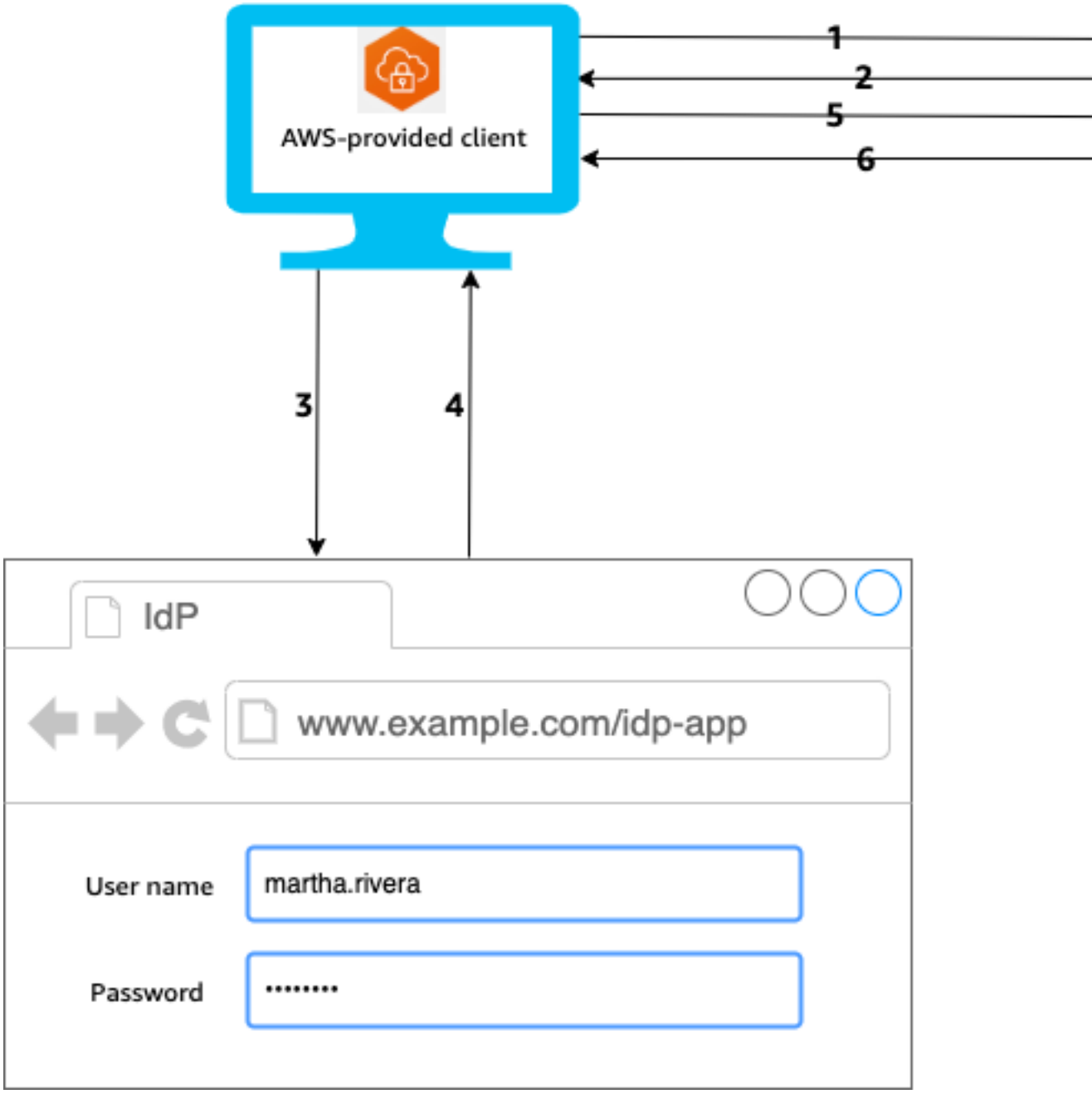
1. Crie um aplicativo baseado em SAML no IdP escolhido para usar com o AWS Client VPN ou use um aplicativo existente.
2. Configure seu IdP para estabelecer uma relação de confiança com a AWS. Para obter recursos, consulte Recursos de configuração de IdPs baseados em SAML (p. 12).
3. No IdP, gere e faça download de um documento de metadados de federação que descreve sua organização como um IdP. Esse documento XML assinado é usado para estabelecer a relação de confiança entre a AWS e o IdP.
4. Crie um provedor de identidade SAML do IAM na mesma conta da AWS que o endpoint da cliente VPN. O provedor de identidade SAML do IAM define a relação de confiança entre o IdP e a AWS da sua organização usando o documento de metadados gerado pelo IdP. Para obter mais informações, consulte Criar provedores de identidade SAML do IAM no Guia do usuário do IAM. Se você atualizar posteriormente a configuração do aplicativo no IdP, gere um novo documento de metadados e atualize seu provedor de identidade SAML do IAM.

   Note

   Não é necessário criar uma função do IAM para usar o provedor de identidade SAML do IAM.
5. Crie um endpoint do cliente VPN. Especifique a autenticação federada como o tipo de autenticação e especifique o provedor de identidade SAML do IAM que você criou. Para obter mais informações, consulte Criar um endpoint do Client VPN (p. 51).
6. Exporte o arquivo de configuração do cliente (p. 58) e distribua-o aos usuários. Instrua os usuários a fazerem download da versão mais recente do cliente fornecido pela AWS e usá-la para carregar o arquivo de configuração e se conectar ao endpoint da cliente VPN. Como alternativa, se você tiver habilitado o portal de autoatendimento para o endpoint da cliente VPN, instrua os usuários a acessá-lo para obter o arquivo de configuração e o cliente fornecido pela AWS. Para obter mais informações, consulte Acessar o portal de autoatendimento (p. 42).

Fluxo de trabalho de autenticação

O diagrama a seguir fornece uma visão geral do fluxo de trabalho de autenticação para um endpoint do cliente VPN que usa autenticação federada baseada em SAML. Ao criar e configurar o endpoint do cliente VPN, você especifica o provedor de identidade SAML do IAM.



1. O usuário abre o cliente fornecido pela AWS no dispositivo e inicia uma conexão com o endpoint da cliente VPN.
2. O endpoint do cliente VPN envia um URL de IdP e uma solicitação de autenticação de volta ao cliente, com base nas informações fornecidas no provedor de identidade SAML do IAM.
3. O cliente fornecido pela AWS abre uma nova janela do navegador no dispositivo do usuário. O navegador faz uma solicitação para o IdP e exibe uma página de login.
4. O usuário insere as credenciais na página de login e o IdP envia uma declaração SAML assinada de volta ao cliente.
5. O cliente fornecido pela AWS envia uma declaração do SAML ao endpoint da cliente VPN.
6. O endpoint do cliente VPN valida a declaração e permite ou nega o acesso ao usuário.

Requisitos e considerações para autenticação federada baseada em SAML

Veja a seguir requisitos e considerações para autenticação federada baseada em SAML.

- Para obter cotas e regras para configurar usuários e grupos em um IdP baseado em SAML, consulte Cotas de usuários e grupos (p. 79).
- A resposta SAML deve ser assinada e sem criptografia.
- O tamanho máximo compatível com respostas SAML é 128 KB.
- AWS Client VPN não fornece solicitações de autenticação assinadas.
- Não há suporte para logout único SAML. Os usuários podem fazer logoff desconectando-se do cliente fornecido pela AWS, ou você pode encerrar as conexões (p. 48).
- Um endpoint do cliente VPN oferece suporte apenas para um único IdP.
- A autenticação multifator (MFA) é permitida quando está habilitada no IdP.
- Os usuários devem usar o cliente fornecido pela AWS para se conectar ao endpoint da cliente VPN. Eles devem usar a versão 1.2.0 ou posterior. Para obter mais informações, consulte Conectar-se usando um cliente fornecido pela AWS.
- Os seguintes navegadores são compatíveis com a autenticação IdP: Apple Safari, Google Chrome, Microsoft Edge e Mozilla Firefox.
- O cliente fornecido pela AWS reserva a porta TCP 35001 nos dispositivos dos usuários para a resposta SAML.
- Se o documento de metadados do provedor de identidade SAML do IAM for atualizado com um URL incorreto ou mal-intencionado, isso poderá causar problemas de autenticação para os usuários ou resultar em ataques de phishing. Portanto, recomendamos que você use o AWS CloudTrail para monitorar atualizações feitas no provedor de identidade SAML do IAM. Para obter mais informações, consulte Como registrar o IAM e chamadas do AWS STS com o AWS CloudTrail no Guia do usuário do IAM.
- AWS Client VPN envia uma solicitação AuthN para o IdP por meio de uma vinculação de redirecionamento HTTP. Portanto, o IdP deve oferecer suporte à vinculação de redirecionamento HTTP e deve estar presente no documento de metadados do IdP.
- Para a declaração SAML, é preciso usar um formato de endereço de e-mail para o atributo `NameID`.

Recursos de configuração de IdPs baseados em SAML

A tabela a seguir lista os IdPs baseados em SAML que foram testados para uso com o AWS Client VPN e os recursos que podem ajudar você a configurar o IdP.

IdP	Recurso
Okta	Autenticar usuários do AWS Client VPN com SAML
Microsoft Azure Active Directory	Para obter mais informações, consulte Tutorial: Integração da autenticação única (SSO) do Azure Active Directory com a VPN do cliente da AWS no site de documentação da Microsoft.

Informações do provedor de serviços para criar um aplicativo

Para criar um aplicativo baseado em SAML usando um IdP que não esteja listado na tabela anterior, use as informações a seguir para configurar as informações do provedor de serviços do AWS Client VPN.

- URL do Assertion Consumer Service (ACS): `http://127.0.0.1:35001`
- URI do público: `urn:amazon:webservices:clientvpn`

O atributo a seguir é obrigatório.

Atributo	Descrição
`memberOf`	Os grupos aos quais o usuário pertence.

Os atributos diferenciam letras maiúsculas de minúsculas e devem ser configurados exatamente como especificado.

Suporte para o portal de autoatendimento

Se você habilitar o portal de autoatendimento do endpoint do cliente VPN, os usuários fazem login no portal usando as credenciais IdP baseadas em SAML.

Se o IdP for compatível com URLs de Assertion Consumer Service (ACS), adicione o seguinte URL do ACS ao aplicativo.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Se você estiver usando o endpoint da cliente VPN em uma região GovCloud, use a seguinte URL ACS. Se você usar a mesma aplicação IDP para autenticar para as regiões padrão e GovCloud, poderá adicionar ambos os URLs.

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Se o IdP não oferecer suporte a vários URLs do ACS, faça o seguinte:

1. Crie um aplicativo adicional baseado em SAML no IdP e especifique o seguinte URL do ACS.

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. Gere e faça download de um documento de metadados de federação.
3. Crie um provedor de identidade SAML do IAM na mesma conta da AWS que o endpoint da cliente VPN. Para obter mais informações, consulte Criar provedores de identidade SAML do IAM no Guia do usuário do IAM.

   Note

   Crie este provedor de identidade SAML além daquele criado para o aplicativo principal (p. 9).
4. Crie o endpoint do cliente VPN (p. 51) e especifique os provedores de identidade SAML do IAM.

Autorização do cliente

A VPN do cliente é compatível com dois tipos de autorização do cliente: grupos de segurança e autorização com base na rede (usando regras de autorização).

Grupos de segurança

Ao criar um terminal do VPN do Cliente, você pode especificar os grupos de segurança de uma VPC específica a serem aplicados ao terminal do VPN do Cliente. Quando você associa uma sub-rede a um terminal do VPN do Cliente, aplicamos automaticamente o grupo de segurança padrão da VPC. Você pode alterar os grupos de segurança depois de criar o terminal do VPN do Cliente. Para obter mais informações, consulte Aplicar um grupo de segurança a uma rede de destino (p. 63). Os grupos de segurança estão associados às interfaces de rede do VPN do Cliente.

Você pode permitir que os usuários do VPN do Cliente acessem suas aplicações em uma VPC adicionando uma regra aos grupos de segurança para permitir o tráfego do grupo de segurança que foi aplicado à associação.

Como adicionar uma regra que permita o tráfego do grupo de segurança do terminal do VPN do Cliente

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security Groups.(Grupos de segurança).
3. Escolha o grupo de segurança associado ao seu recurso ou aplicativo e escolha Ações, Editar regras de entrada.
4. Escolha Adicionar regra.
5. Para Tipo, escolha Todo o tráfego. Como alternativa, é possível restringir o acesso a um tipo específico de tráfego, por exemplo, SSH.

   Em Origem, especifique o ID do grupo de segurança associado à rede de destino (sub-rede) do terminal do VPN do Cliente.
6. Escolha Salvar regras.

Por outro lado, é possível restringir o acesso para usuários do VPN do Cliente não especificando o grupo de segurança que foi aplicado à associação ou removendo a regra que faz referência ao grupo de segurança de terminal do VPN do Cliente. As regras de grupo de segurança necessárias podem depender do tipo de acesso VPN a ser configurado. Para obter mais informações, consulte Cenários e exemplos (p. 23).

Para obter mais informações sobre grupos de segurança de VPC, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Autorização com base em rede

A autorização com base em rede é implementada com o uso de regras de autorização. Para cada rede à qual você deseja habilitar o acesso, é necessário configurar regras de autorização que limitam os usuários que têm acesso. Para uma rede especificada, configure o grupo do Active Directory ou o grupo do IdP baseado em SAML que tem permissão de acesso. Somente os usuários que pertencerem ao grupo especificado poderão acessar a rede especificada. Se não estiver usando a autenticação federada baseada em Active Directory ou SAML, ou se quiser abrir o acesso a todos os usuários, você poderá especificar uma regra que conceda acesso a todos os clientes. Para obter mais informações, consulte Regras de autorização (p. 43).

Autorização de conexão

É possível configurar um manipulador de conexão de cliente para o endpoint da cliente VPN. O manipulador permite executar a lógica que autoriza uma nova conexão, baseada em atributos de

dispositivo, usuário e conexão. O manipulador de conexão do cliente é executado depois que o serviço do VPN do cliente autenticou o dispositivo e o usuário.

Para configurar um manipulador de conexão do cliente para o endpoint da cliente VPN, crie uma função do AWS Lambda que utilize os atributos do dispositivo, usuário e conexão como entradas e retorne uma decisão para o serviço da cliente VPN para permitir ou negar uma nova conexão. Especifique a função Lambda no endpoint da cliente VPN. Quando os dispositivos forem conectados ao endpoint da cliente VPN, o serviço da cliente VPN invocará a função Lambda . Somente as conexões autorizadas pela função Lambda podem se conectar ao endpoint da cliente VPN.

Note

Atualmente, o único tipo de manipulador de conexão do cliente compatível é uma função Lambda.

Requisitos e considerações

Veja a seguir requisitos e considerações para o manipulador de conexão do cliente:

- O nome da função Lambda deve começar com o prefixo `AWSClientVPN-`.
- As funções Lambda qualificadas são compatíveis.
- A função Lambda deve estar na mesma região da AWS e na mesma conta da AWS que o endpoint da cliente VPN.
- A função Lambda atinge o tempo limite após 30 segundos. Esse valor não pode ser alterado.
- A função Lambda é de forma sincronizada. Ela é invocada depois da autenticação de dispositivo e usuário e antes de as regras de autorização serem avaliadas.
- Se a função Lambda for invocada para uma nova conexão e o serviço da cliente VPN não obtiver uma resposta esperada da função, o serviço da cliente VPN negará a solicitação de conexão. Por exemplo, isso pode ocorrer se a função Lambda for limitada, atingir o tempo limite ou encontrar outros erros inesperados, ou se a resposta da função não estiver em um formato válido.
- Recomendamos configurar a simultaneidade provisionada da função Lambda para permitir que ela seja dimensionada sem flutuações na latência.
- Se você atualizar a função Lambda, as conexões existentes com o endpoint da cliente VPN não serão afetadas. É possível encerrar as conexões existentes e orientar seus clientes a estabelecer novas conexões. Para obter mais informações, consulte Encerrar uma conexão de cliente (p. 48).
- Se os clientes usarem o cliente fornecido pela AWS para se conectar ao endpoint da cliente VPN, eles deverão usar a versão 1.2.6 ou posterior para Windows e a versão 1.2.4 ou posterior para macOS. Para obter mais informações, consulte Conecte-se usando o cliente fornecido pela AWS.

Interface do Lambda

A função Lambda usa atributos de dispositivo, usuário e conexão como entradas do serviço da cliente VPN. Depois, retoma a decisão de permitir ou negar a conexão para o serviço da cliente VPN.

Esquema de solicitação

A função Lambda usa o blob JSON que contém os campos a seguir como entrada.

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
```

```
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "groups": <group identifier>,
    "schema-version": "v2"
}
```

- `connection-id`: o ID da conexão do cliente ao endpoint da cliente VPN.
- `endpoint-id`: o ID do endpoint da cliente VPN.
- `common-name`: o identificador do dispositivo. No certificado do cliente criado para o dispositivo, o nome comum identifica o dispositivo de forma exclusiva.
- `username`: o identificador do usuário, se aplicável. Para autenticação do Active Directory, este é o nome de usuário. Para autenticação federada baseada em SAML, é `NameID`. Para autenticação mútua, este campo fica vazio.
- `platform`: a plataforma do sistema operacional do cliente.
- `platform-version`: a versão do sistema operacional. O serviço da cliente VPN fornece um valor quando a diretiva `--push-peer-info` está presente na configuração do cliente OpenVPN quando ele se conecta a um endpoint da cliente VPN e está executando a plataforma Windows.
- `public-ip`: o endereço IP público do dispositivo de conexão.
- `client-openvpn-version`: a versão do OpenVPN que o cliente está usando.
- `groups`: o identificador do grupo, se aplicável. Para autenticação do Active Directory, esta será uma lista de grupos do Active Directory. Para autenticação federada baseada em SAML, esta será uma lista de grupos de provedores de identidade (IdP). Para autenticação mútua, este campo fica vazio.
- `schema-version`: a versão do esquema. O padrão é `v2`.

Esquema de resposta

A função Lambda deve retornar os campos a seguir.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v2"
}
```

- `allow`: obrigatório. Um booleano (`true` | `false`) que indica se deseja permitir ou negar a nova conexão.
- `error-msg-on-denied-connection`: obrigatório. Uma série de até 255 caracteres que pode ser usada para fornecer etapas e diretrizes para os clientes se a conexão for negada pela função Lambda. No caso de falhas durante a execução da função Lambda (por exemplo, durante a limitação), a seguinte mensagem padrão será apresentada para os clientes.

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses`: obrigatório. Se você usa a função Lambda para avaliação da postura (p. 17), esta é uma lista de status para o dispositivo de conexão. Você define os nomes de status de acordo com as categorias de avaliação da postura dos dispositivos, por exemplo, `compliant`, `quarantined` `unknown` e assim por diante. Os nomes podem ter até 255 caracteres. É possível especificar até 10 status.
- `schema-version`: obrigatório. A versão do esquema. O padrão é `v2`.

Você pode usar a mesma função Lambda para vários endpoints da cliente VPN na mesma região.

Para obter mais informações sobre como criar uma função Lambda, consulte a seção Conceitos básicos do AWS Lambda no Guia do desenvolvedor do AWS Lambda.

Usar o manipulador de conexão do cliente para avaliação da postura

É possível usar o manipulador de conexão do cliente para integrar o endpoint da cliente VPN à solução de gerenciamento de dispositivos existente para avaliar a conformidade da postura dos dispositivos de conexão. Para que a função Lambda funcione como um manipulador de autorização de dispositivo, use a autenticação mútua (p. 6) para o endpoint da cliente VPN. Crie um certificado de cliente exclusivo e uma chave para cada cliente (dispositivo) que se conectará ao endpoint da cliente VPN. A função Lambda pode usar o nome comum exclusivo para o certificado de cliente (que é passado do serviço da cliente VPN) para identificar o dispositivo e buscar o status de conformidade da postura da solução de gerenciamento de dispositivo. É possível usar a autenticação mútua combinada com a autenticação baseada em usuário.

Como alternativa, você pode realizar uma avaliação de postura básica na própria função Lambda. Por exemplo, é possível avaliar os campos `platform` e `platform-version` que são passados para a função Lambda pelo serviço da cliente VPN.

Habilitar o manipulador de conexão do cliente

Para habilitar o manipulador de conexão do cliente, crie ou modifique um endpoint da cliente VPN e especifique o nome de recurso da Amazon (ARN) da função Lambda. Para obter mais informações, consulte Criar um endpoint do Client VPN (p. 51) e Modificar um endpoint do Client VPN (p. 53).

Função vinculada ao serviço

A AWS Client VPN cria automaticamente uma função vinculada a serviços na conta chamada AWSServiceRoleForClientVPNConnections. A função tem permissões para invocar a função Lambda quando uma conexão é estabelecida com o endpoint da cliente VPN. Para obter mais informações, consulte Uso de funções vinculadas a serviços para o Client VPN (p. 69).

Monitorar falhas de autorização de conexão

Você pode ver o status de autorização de conexões com o endpoint da cliente VPN. Para obter mais informações, consulte Visualizar conexões de clientes (p. 47).

Quando o manipulador de conexão do cliente é usado para avaliação da postura, também é possível visualizar os status de conformidade da postura de dispositivos que se conectam ao endpoint da cliente VPN nos logs de conexão. Para obter mais informações, consulte Registro em log de conexão (p. 20).

Caso um dispositivo falhe na autorização da conexão, o campo `connection-attempt-failure-reason` nos logs de conexão apresentará um dos seguintes motivos de falha:

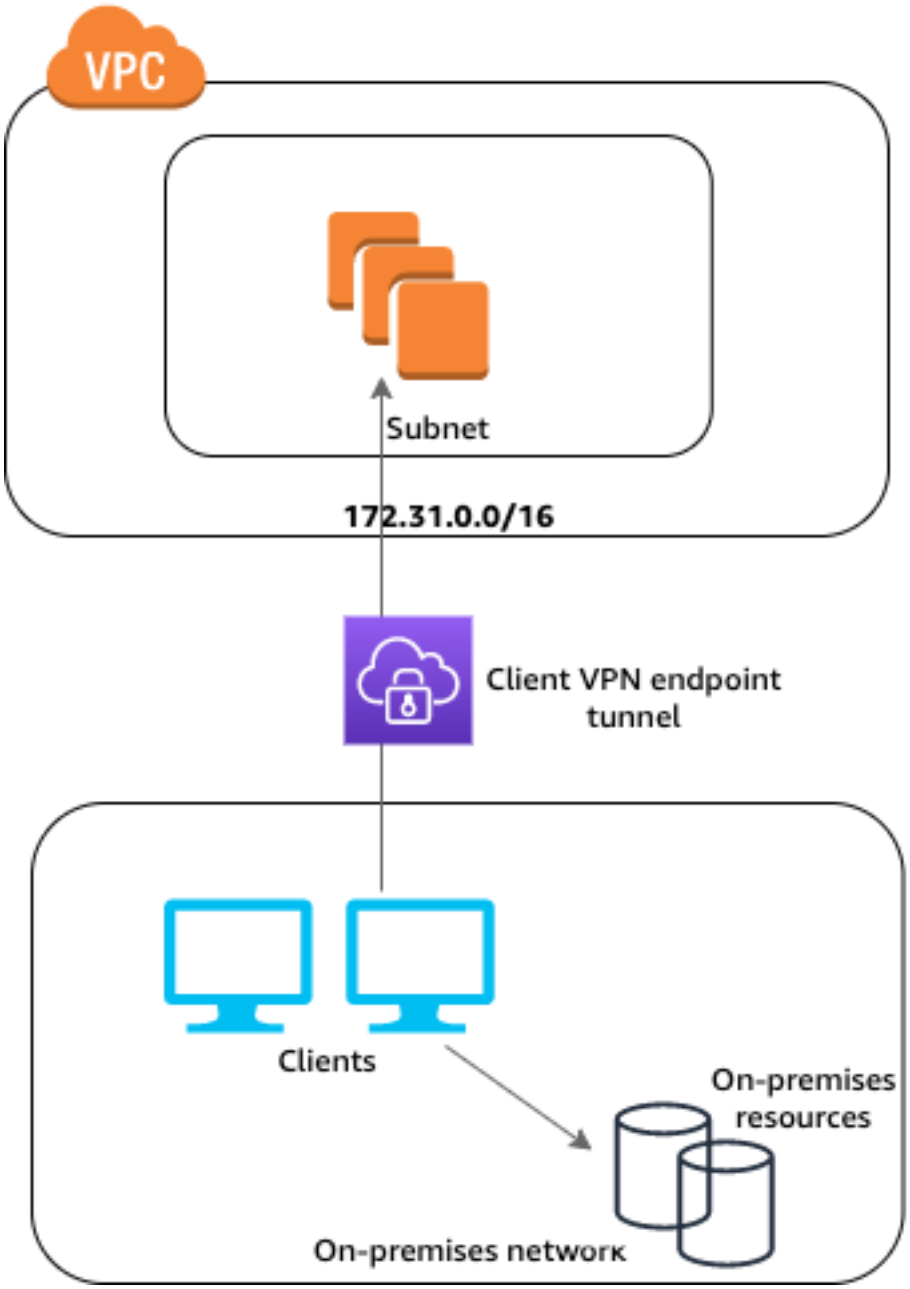
- `client-connect-failed`: a função Lambda impediu que a conexão fosse estabelecida.
- `client-connect-handler-timed-out`: a função Lambda atingiu o tempo limite.
- `client-connect-handler-other-execution-error`: a função Lambda encontrou um erro inesperado.
- `client-connect-handler-throttled`: a função Lambda foi limitada.
- `client-connect-handler-invalid-response`: a função Lambda retornou uma resposta inválida.
- `client-connect-handler-service-error`: houve um erro no serviço durante a tentativa de conexão.

Túnel dividido em endpoints do AWS Client VPN

Por padrão, quando você tem um endpoint do Client VPN, todo o tráfego dos clientes é roteado pelo túnel do Client VPN. Quando você habilita o túnel dividido no endpoint do Client VPN, as rotas são enviadas por push na tabela de rotas do endpoint do Client VPN (p. 60) para o dispositivo que está conectado ao endpoint do Client VPN. Isso garante que somente o tráfego com um destino para a rede correspondente a uma rota da tabela de rotas do endpoint do Client VPN seja roteado pelo do túnel do Client VPN.

Você poderá usar um endpoint de túnel dividido do Client VPN quando não quiser que todo o tráfego de usuário seja roteado pelo endpoint do Client VPN.

No exemplo a seguir, o túnel dividido está habilitado no endpoint do Client VPN. Somente o tráfego destinado à VPC (`172.31.0.0/16`) é roteado pelo túnel do Client VPN. O tráfego destinado a recursos locais não é roteado pelo túnel do Client VPN.



Benefícios do túnel dividido

O túnel dividido em endpoints do Client VPN oferece os seguintes benefícios:

- Você pode otimizar o roteamento do tráfego de clientes fazendo com que apenas o tráfego destinado da AWS atravesse o túnel da VPN.
- É possível reduzir o volume do tráfego de saída da AWS, reduzindo, portanto, o custo de transferência de dados.

Considerações sobre roteamento

Quando você habilita o túnel dividido em um endpoint do Client VPN, todas as rotas que estão nas tabelas de rotas do Client VPN são adicionadas à tabela de rotas do cliente quando a VPN é estabelecida. Essa operação é diferente da operação do endpoint do Client VPN padrão, que substitui a tabela de rotas do cliente pela entrada 0.0.0.0/0 para rotear todo o tráfego pela VPN.

Habilitar o túnel dividido

Você pode habilitar o túnel dividido em um endpoint novo ou existente do Client VPN. Para obter mais informações, consulte os tópicos a seguir:

- Criar um endpoint do Client VPN (p. 51)
- Modificar um endpoint do Client VPN (p. 53)

Registro em log de conexão

O registro em log de conexão é um recurso da AWS Client VPN que habilita capturar logs de conexão para o endpoint da cliente VPN.

Um log de conexão contém entradas de log de conexão. Cada entrada de log de conexão contém informações sobre um evento de conexão, que é quando um cliente (usuário final) se conecta, tenta se conectar ou se desconecta do terminal do VPN do Cliente. Você pode usar essas informações para executar perícia, analisar como seu endpoint da cliente VPN está sendo usado ou depurar problemas de conexão.

O registro em log de conexão está disponível em todas as regiões em que a VPN do cliente da AWS está disponível. Os logs de conexão são publicados em um grupo de logs do CloudWatch Logs na sua conta.

Entradas de log de conexão

Uma entrada de log de conexão é um blob em formato JSON de pares de chave/valor. Este é um exemplo de entrada de log de conexão.

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA"
}
```

Uma entrada de log de conexão contém as seguintes chaves:

- `connection-log-type`: o tipo de entrada de log de conexão (`connection-attempt` ou `connection-reset`).
- `connection-attempt-status`: o status da solicitação de conexão (`successful`, `failed`, `waiting-for-assertion` ou `NA`).
- `connection-reset-status`: o status de um evento de redefinição de conexão (`NA` ou `assertion-received`).
- `connection-attempt-failure-reason`: o motivo da falha de conexão, se aplicável.
- `connection-id`: o ID da conexão.
- `client-vpn-endpoint-id`: o ID do terminal do VPN do Cliente com o qual a conexão foi feita.
- `transport-protocol`: o protocolo de transporte que foi usado para a conexão.
- `connection-start-time`: a hora de início da conexão.
- `connection-last-update-time`: o horário da última atualização da conexão. Esse valor é atualizado periodicamente nos logs.
- `client-ip`: o endereço IP do cliente, que é alocado a partir do intervalo CIDR IPv4 do cliente para o terminal do VPN do Cliente.
- `common-name`: o nome comum do certificado usado para autenticação baseada em certificado.
- `device-type`: o tipo de dispositivo usado para a conexão pelo usuário final.
- `device-ip`: o endereço IP público do dispositivo.
- `port`: o número da porta para a conexão.
- `ingress-bytes`: o número de bytes de entrada para a conexão. Esse valor é atualizado periodicamente nos logs.
- `egress-bytes`: o número de bytes de saída para a conexão. Esse valor é atualizado periodicamente nos logs.
- `ingress-packets`: o número de pacotes de entrada para a conexão. Esse valor é atualizado periodicamente nos logs.
- `egress-packets`: o número de pacotes de saída para a conexão. Esse valor é atualizado periodicamente nos logs.
- `connection-end-time`: a hora de término da conexão. O valor será `NA` se a conexão ainda estiver em andamento ou se a tentativa de conexão falhar.
- `posture-compliance-statuses`: os status da conformidade da postura retornados pelo cliente conectam o manipulador (p. 14), se aplicável.

Para obter mais informações sobre como habilitar o registro em log de conexão, consulte Trabalhando com logs de conexão (p. 55).

Considerações sobre dimensionamento do Client VPN

Ao criar um endpoint do Client VPN, considere o número máximo de conexões VPN simultâneas que você planeja suportar. Você deve levar em conta o número de clientes que você suporta atualmente e se seu endpoint do Client VPN pode atender à demanda adicional, se necessário.

Os fatores a seguir afetam o número máximo de conexões VPN simultâneas que podem ser suportadas em um endpoint do Client VPN.

Tamanho do intervalo CIDR do cliente

Ao criar um endpoint do Client VPN (p. 51), você deve especificar um intervalo CIDR do cliente, que é um bloco CIDR IPv4 entre uma máscara de rede /12 e /22. Cada conexão da VPN com o

endpoint do Client VPN recebe um endereço IP exclusivo do intervalo CIDR do cliente. Uma parte dos endereços no intervalo de CIDR do cliente também é usada para suportar o modelo de disponibilidade do endpoint do Client VPN e não pode ser atribuída aos clientes. Não é possível alterar o intervalo CIDR do cliente depois de criar o endpoint do Client VPN.

Em geral, recomendamos que você especifique um intervalo CIDR do cliente que contenha o dobro do número de endereços IP (e, portanto, conexões simultâneas) que você planeja suportar no endpoint do Client VPN.

Número de sub-redes associadas

Quando associa uma sub-rede (p. 62) a um endpoint do Client VPN, você permite que os usuários estabeleçam sessões de VPN com o endpoint do Client VPN. Você pode associar várias sub-redes a um endpoint do Client VPN para alta disponibilidade e para habilitar a capacidade de conexão adicional.

Veja a seguir o número de conexões VPN simultâneas suportadas com base no número de associações de sub-rede para o endpoint do Client VPN.

Associações de sub-rede	Número suportado de conexões
1	7.000
2	36.500
3	66.500
4	96.500
5	126.000

Você não pode associar várias sub-redes da mesma Zona de disponibilidade a um endpoint do Client VPN. Portanto, o número de associações de sub-rede também depende do número de zonas de disponibilidade disponíveis em uma região da AWS.

Por exemplo, se você espera suportar 8.000 conexões VPN ao endpoint do Cliente VPN, especifique um tamanho mínimo de intervalo CIDR do cliente de `/18` (16.384 endereços IP) e associe pelo menos 2 sub-redes ao endpoint do Client VPN.

Se você não tiver certeza de qual é o número de conexões VPN esperadas para o endpoint do Client VPN, recomendamos que você especifique um bloco CIDR com um tamanho de `/16` ou maior.

Para obter mais informações sobre as regras e limitações para trabalhar com intervalos CIDR do cliente e redes de destino, consulte Limitações e regras do VPN do Cliente (p. 3).

Para obter mais informações sobre cotas para o endpoint do Client VPN, consulte Cotas do cliente VPN da AWS (p. 79).

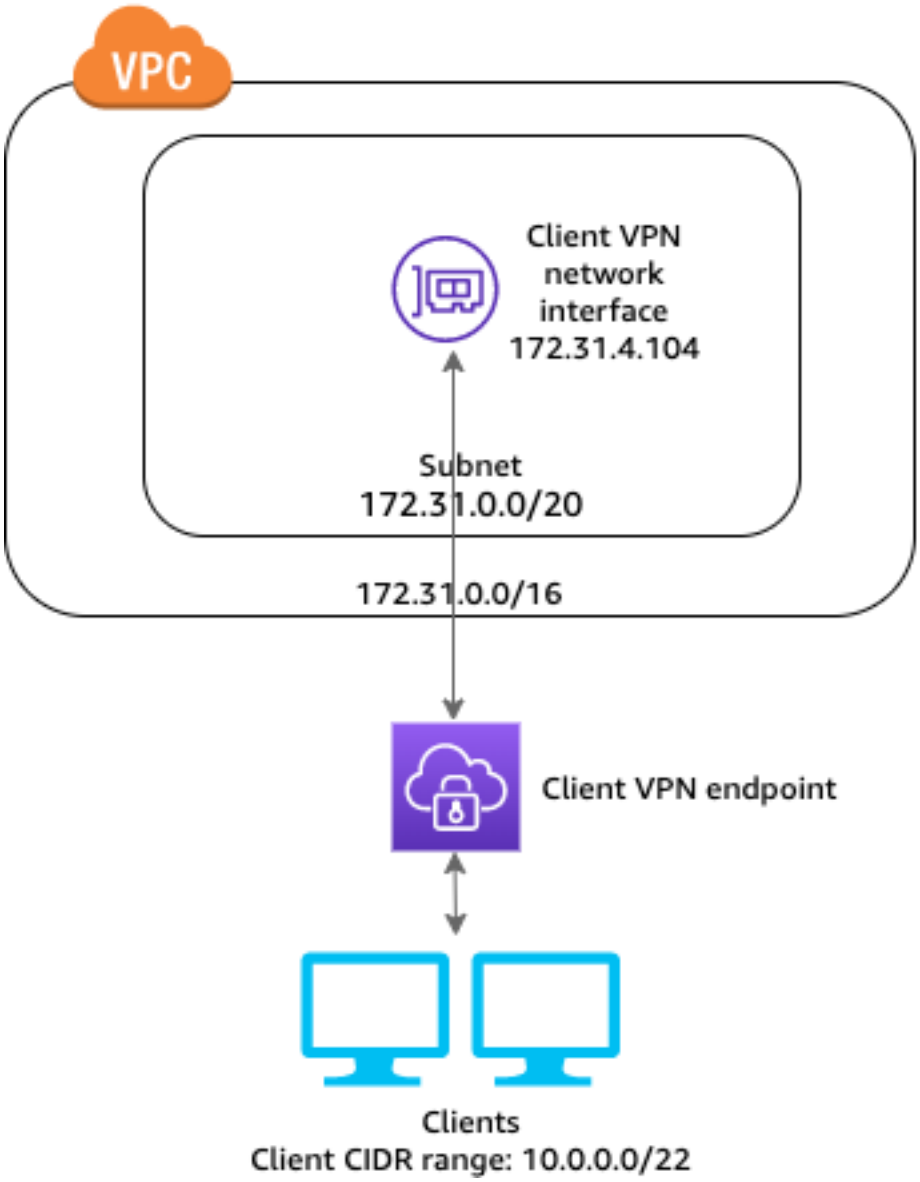
Cenários e exemplos

Esta seção fornece exemplos de como criar e configurar o acesso ao Client VPN para seus clientes.

Tópicos

Acesso a uma VPC

A configuração deste cenário inclui uma única VPC de destino. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN em Limitações e regras do VPN do Cliente (p. 3).

Para implementar essa configuração

1. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Criar um endpoint do Client VPN (p. 51).

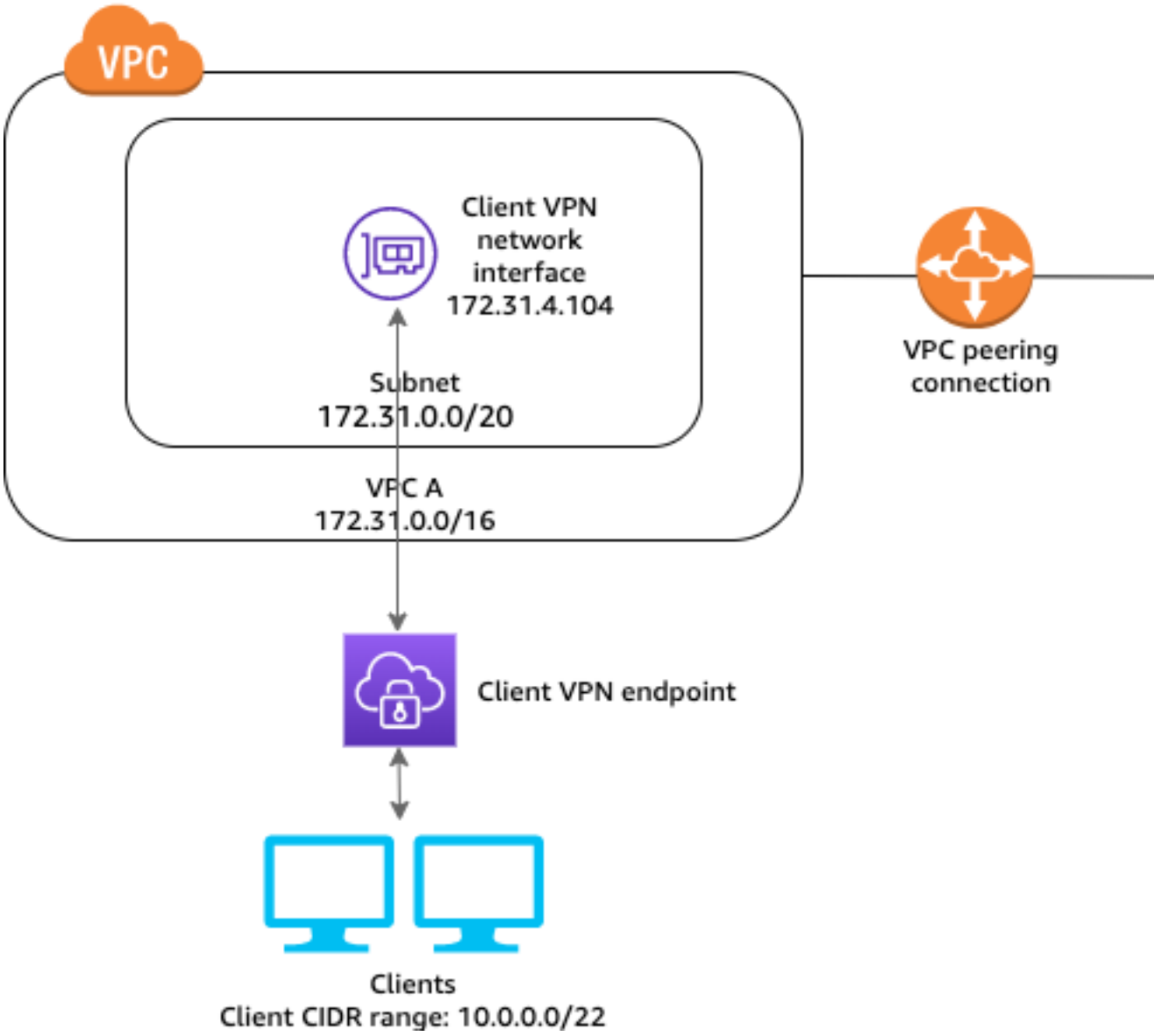
2. Associe a sub-rede ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em Associa uma rede de destino a um endpoint do Client VPN. (p. 62) e selecione a sub-rede e a VPC que você identificou anteriormente.
3. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43) e, em Destination network (Rede de destino), insira o intervalo CIDR IPv4 da VPC.
4. Adicione uma regra aos grupos de segurança dos recursos para permitir o tráfego do grupo de segurança que foi aplicado à associação de sub-rede na etapa 2. Para obter mais informações, consulte Grupos de segurança (p. 14).

Acesso a uma VPC emparelhada

A configuração desse cenário inclui uma VPC de destino (VPC A) que é emparelhada com uma VPC adicional (VPC B). Ela é recomendada quando você precisa dar acesso para os clientes aos recursos dentro de uma VPC de destino e a outras VPCs que estejam emparelhadas com ela (como a VPC B).

Note

O procedimento descrito abaixo para permitir acesso a uma VPC com peering só é necessário se o endpoint do cliente VPN tiver sido configurado para o modo de túnel dividido. No modo de túnel inteiro, o acesso à VPC com peering seria permitido por padrão.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN em Limitações e regras do VPN do Cliente (p. 3).

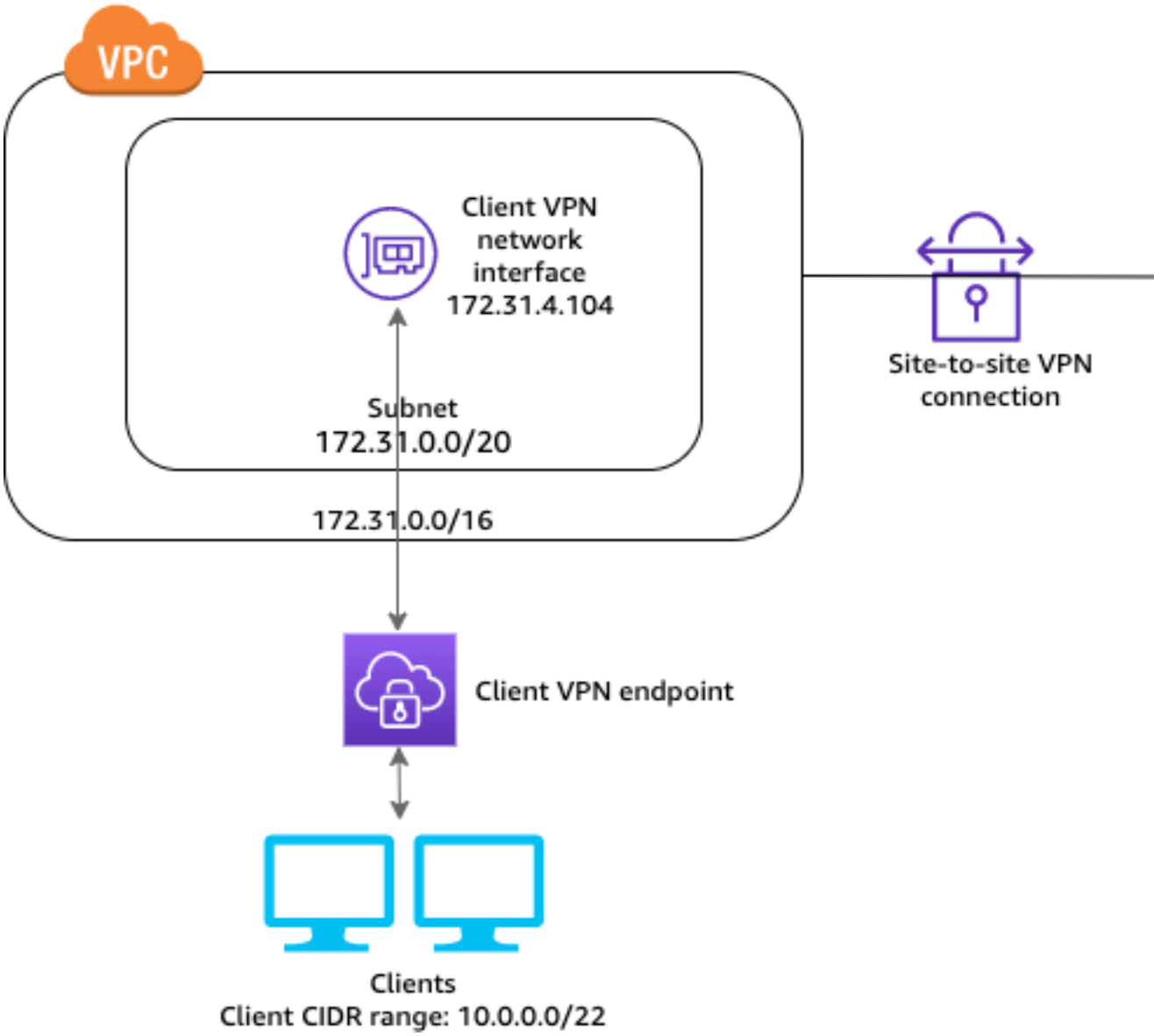
Para implementar essa configuração

1. Estabeleça a conexão de emparelhamento de VPCs entre as VPCs. Siga as etapas em Criar e aceitar uma conexão de emparelhamento de VPC no Guia de emparelhamento da Amazon VPC.

2. Teste a conexão de emparelhamento de VPCs. Confirme se as instâncias em qualquer uma das VPCs podem se comunicar umas com as outras como se estivessem na mesma rede. Se a conexão de emparelhamento funcionar conforme esperado, siga para a próxima etapa.
3. Crie um endpoint do Client VPN na mesma região que a VPC de destino. No exemplo anterior, esta é a VPC A. Execute as etapas descritas em Criar um endpoint do Client VPN (p. 51).
4. Associe a sub-rede anteriormente identificada ao endpoint do Client VPN que você criou. Para fazer isso, execute as etapas descritas em Associa uma rede de destino a um endpoint do Client VPN. (p. 62) e selecione a sub-rede e a VPC.
5. Adicione uma regra de autorização para fornecer acesso à VPC de destino para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43) e, em Destination network to enable (Rede de destino para habilitar), insira o intervalo CIDR IPv4 da VPC.
6. Adicione uma rota para direcionar o tráfego à VPC emparelhada. No exemplo anterior, esta é a VPC B. Para fazer isso, execute as etapas descritas em Criar uma rota de endpoint (p. 60). Em Route destination (Destino da rota), insira o intervalo CIDR IPv4 da VPC emparelhada e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede associada ao endpoint do Client VPN.
7. Adicione uma regra de autorização para fornecer os acesso à VPC emparelhada para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43). Em Destination network (Rede de destino), insira o intervalo CIDR IPv4 da VPC emparelhada.
8. Adicione uma regra aos grupos de segurança dos recursos na VPC A e na VPC B para permitir o tráfego do grupo de segurança que foi aplicado à associação de sub-rede na etapa 2. Para obter mais informações, consulte Grupos de segurança (p. 14).

Acesso a uma rede no local

A configuração deste cenário inclui acesso a uma rede local apenas. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma rede no local apenas.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN em Limitações e regras do VPN do Cliente (p. 3).

Para implementar essa configuração

1. Habilite a comunicação entre a VPC e sua própria rede on-premises por meio de uma conexão VPN de local a local da AWS. Para fazer isso, execute as etapas descritas em Conceitos básicos no Guia do usuário do AWS Site-to-Site VPN.

Note

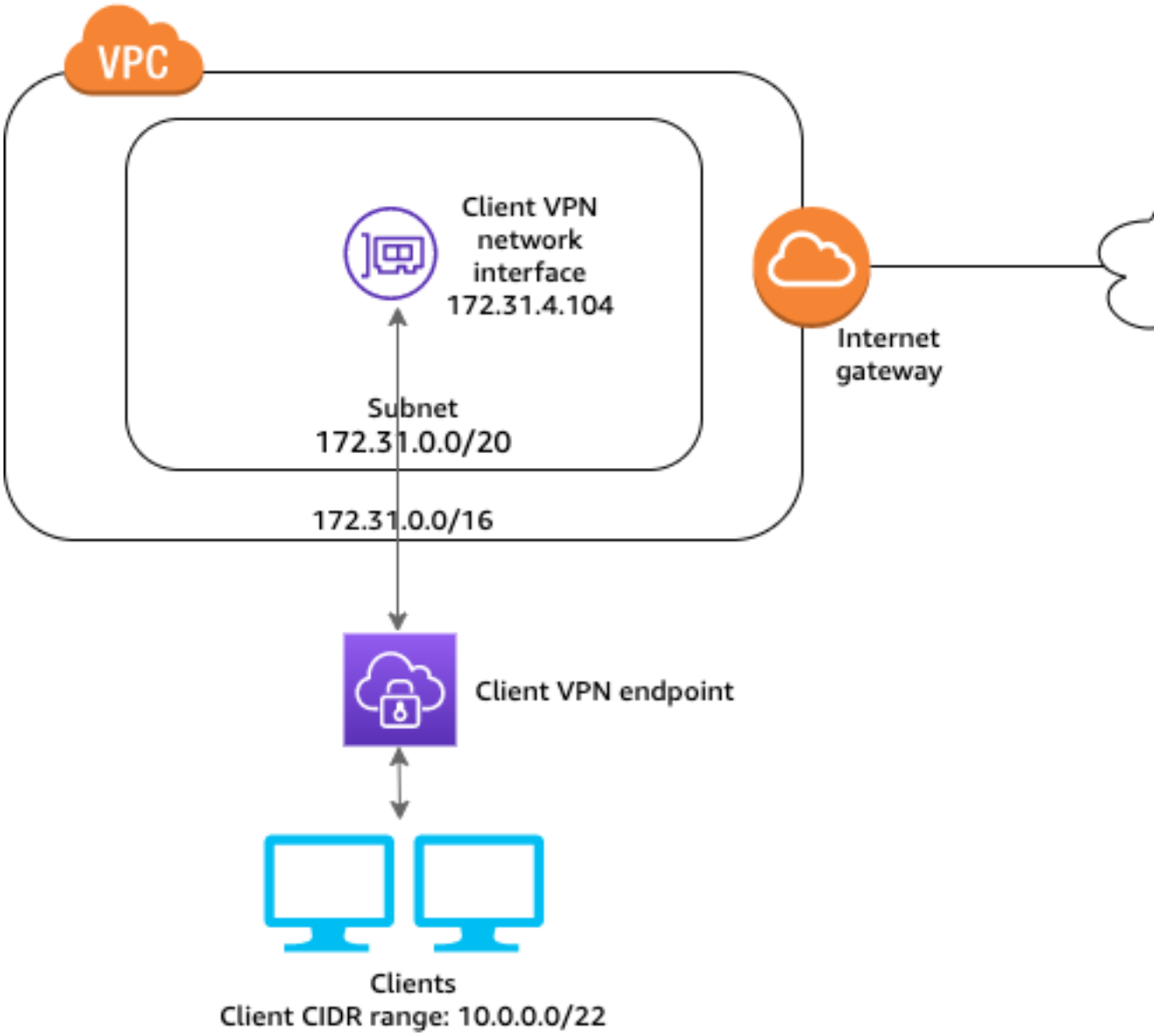
Como alternativa, você pode implementar esse cenário usando uma conexão do AWS Direct Connect entre a VPC e a rede local. Para obter mais informações, consulte o Guia do usuário do AWS Direct Connect.

2. Teste a conexão da VPN de local a local da AWS criada na etapa anterior. Para fazer isso, execute as etapas descritas em Testar a conexão da VPN de local a local no Guia do Usuário do AWS Site-to-Site VPN. Se a conexão VPN estiver funcionando conforme o esperado, continue para a próxima etapa.
3. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Criar um endpoint do Client VPN (p. 51).
4. Associe a sub-rede que você identificou anteriormente ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em Associa uma rede de destino a um endpoint do Client VPN. (p. 62) e selecione a VPC e a sub-rede.
5. Adicione uma rota que permita acesso à conexão da VPN de local a local da AWS. Para fazer isso, execute as etapas descritas em Criar uma rota de endpoint (p. 60). Em Route destination (Destino da rota), insira o intervalo CIDR IPv4 da conexão VPN de local a local da AWS, e, em Target VPC Subnet ID (ID da sub-rede da VPC destino), selecione a sub-rede que você associou ao endpoint do cliente VPN.
6. Adicione uma regra de autorização para fornecer acesso à conexão da VPN de local a local da AWS aos clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43). Em Destination network (Rede de destino), insira o intervalo CIDR IPv4 de conexão da VPN de local a local da AWS.

Acesso à Internet

A configuração deste cenário inclui uma única VPC de destino e acesso à Internet. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC de destino e permitir o acesso à Internet.

Se você já concluiu o tutorial Conceitos básicos da cliente VPN (p. 36), então já implementou esse cenário.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN em Limitações e regras do VPN do Cliente (p. 3).

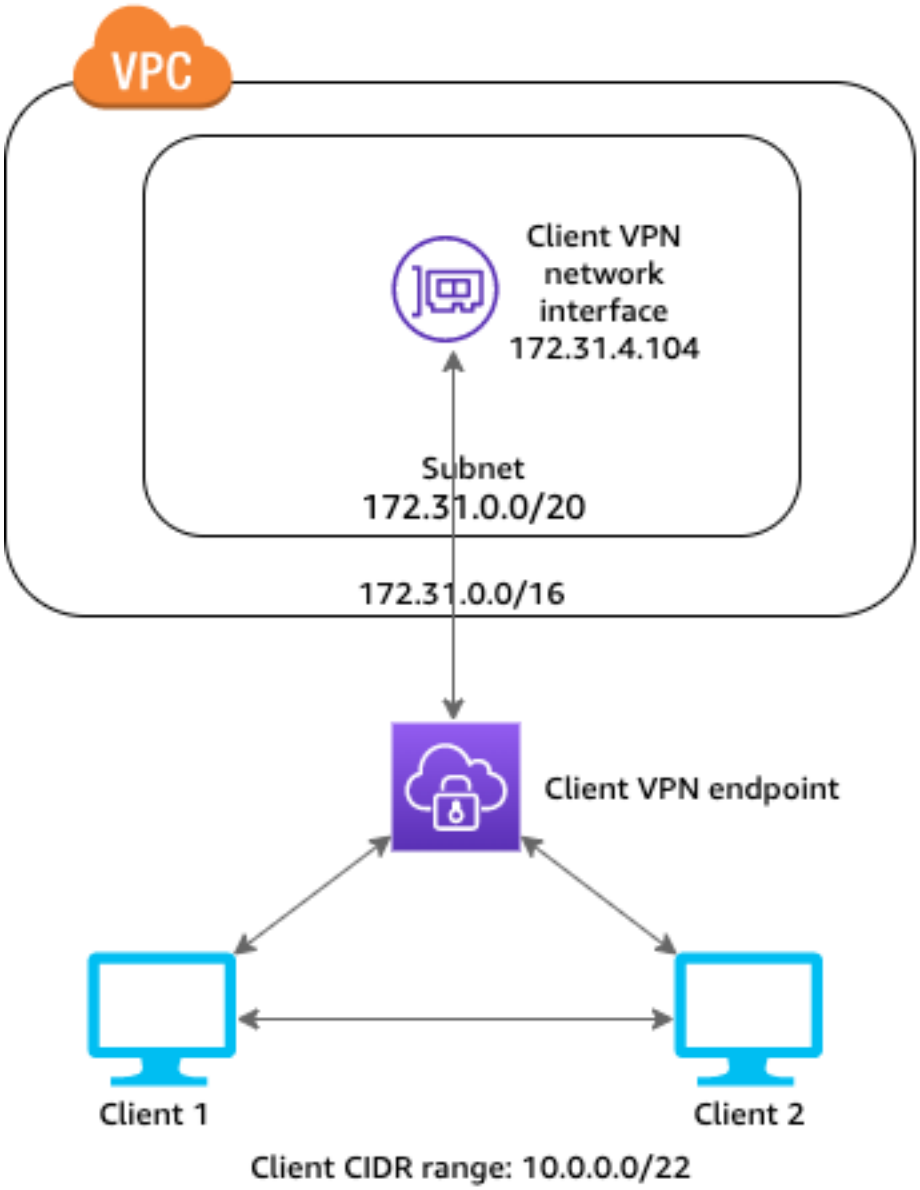
Para implementar essa configuração

1. Verifique se o grupo de segurança que você usará para o endpoint da VPN do cliente permite tráfego de saída para a Internet. Para fazer isso, adicione regras de saída que permitam tráfego HTTP e HTTPS para 0.0.0.0/0.

2. Crie um gateway de internet e anexe-o à sua VPC. Para obter mais informações, consulte Criar e anexar um gateway da Internet no Guia do usuário do Amazon VPC.
3. Torne a sub-rede pública, adicionando uma rota para o gateway de internet à sua tabela de rotas. No console da VPC, escolha Subnets (Sub-redes), selecione a sub-rede que você pretende associar ao endpoint do Client VPN, escolha Route Table (Tabela de rotas) e escolha o ID da tabela de rotas. Escolha Actions (Ações), Edit routes (Editar rotas) e depois Add route (Adicionar rota). Em Destination (Destino), insira `0.0.0.0/0` e, em Target (Destino), escolha o gateway de internet da etapa anterior.
4. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Criar um endpoint do Client VPN (p. 51).
5. Associe a sub-rede que você identificou anteriormente ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em Associa uma rede de destino a um endpoint do Client VPN. (p. 62) e selecione a VPC e a sub-rede.
6. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43) e, em Destination network to enable (Rede de destino para habilitar), insira o intervalo CIDR IPv4 da VPC.
7. Adicione uma rota que permita tráfego para a Internet. Para fazer isso, execute as etapas descritas em Criar uma rota de endpoint (p. 60). Em Route destination (Destino da rota), insira `0.0.0.0/0` e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede que você associou ao endpoint do Client VPN.
8. Adicione uma regra de autorização para fornecer acesso à Internet para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43). Em Destination network (Rede de destino), insira `0.0.0.0/0`.
9. Verifique se os grupos de segurança para os recursos em sua VPC têm uma regra que permita o acesso do grupo de segurança com o endpoint da VPN do cliente. Isso permite que os clientes acessem os recursos na VPC.

Acesso cliente a cliente

A configuração desse cenário permite que os clientes acessem uma única VPC e que eles roteiem o tráfego entre si. Recomendamos essa configuração se os clientes que se conectam ao mesmo endpoint do Client VPN também precisam se comunicar uns com os outros. Os clientes podem se comunicar entre si usando o endereço IP exclusivo atribuído a eles do intervalo CIDR do cliente quando se conectam ao endpoint do Client VPN.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN em Limitações e regras do VPN do Cliente (p. 3).

> **Note**
>
> Não há suporte neste cenário a regras de autorização baseadas em rede que utilizam grupos do Active Directory ou grupos IdP baseados em SAML.

Para implementar essa configuração

1. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Criar um endpoint do Client VPN (p. 51).
2. Associe a sub-rede que você identificou anteriormente ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em Associa uma rede de destino a um endpoint do Client VPN. (p. 62) e selecione a VPC e a sub-rede.
3. Adicione uma rota à rede local na tabela de rotas. Para fazer isso, execute as etapas descritas em Criar uma rota de endpoint (p. 60). Em Route destination (Destino da rota), insira o intervalo CIDR do cliente e, em Target VPC Subnet ID (ID de sub-rede da VPC de destino), especifique `local`.
4. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43). Em Destination network to enable (Rede de destino para permitir acesso), insira o intervalo CIDR IPv4 da VPC.
5. Adicione uma regra de autorização para conceder aos clientes acesso ao intervalo CIDR do cliente. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43). Em Destination network to enable (Rede de destino para permitir acesso), insira o intervalo CIDR do cliente.

Restringir o acesso à sua rede

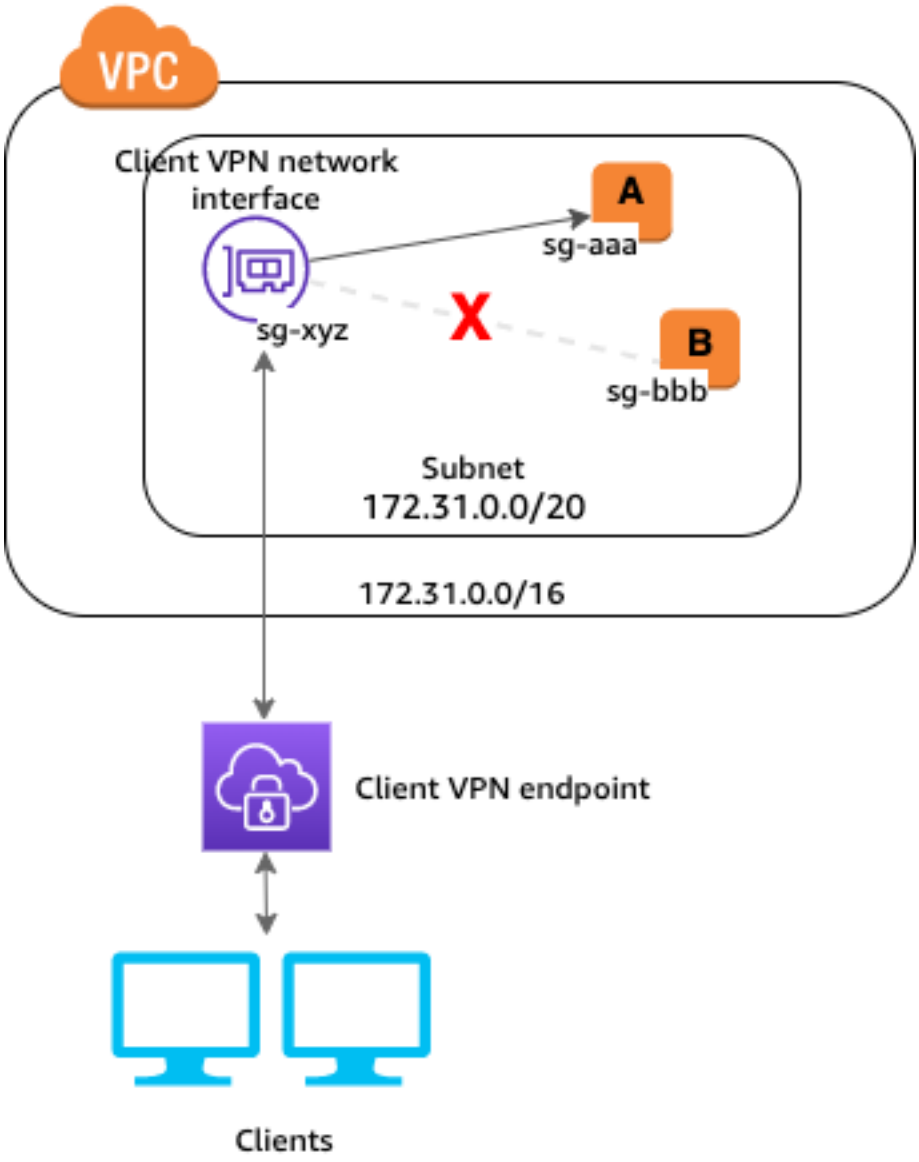
Você pode configurar seu endpoint do cliente VPN para restringir o acesso a recursos específicos em sua VPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa o endpoint do cliente VPN.

Restringir o acesso usando grupos de segurança

Você pode conceder ou negar acesso a recursos específicos em sua VPC adicionando ou removendo regras de grupo de segurança que fazem referência ao grupo de segurança que foi aplicado à associação da rede de destino (o grupo de segurança do Client VPN). Essa configuração é comentada no cenário descrito em Acesso a uma VPC (p. 23). Ela é aplicada além da regra de autorização configurada naquele cenário.

Para conceder acesso a um recurso específico, identifique o grupo de segurança associado à instância em que o recurso está sendo executado. Crie uma regra que permita o tráfego do grupo de segurança do Client VPN.

No exemplo a seguir, `sg-xyz` é o grupo de segurança do Client VPN, o grupo de segurança `sg-aaa` está associado à instância A e o grupo de segurança `sg-bbb` está associado à instância B. Você adiciona uma regra a `sg-aaa` que permite o acesso a partir de `sg-xyz`, portanto, os clientes podem acessar seus recursos na instância A. O grupo de segurança `sg-bbb` não tem uma regra que permita o acesso a partir de `sg-xyz` ou da interface de rede do Client VPN. Os clientes não podem acessar os recursos na instância B.



Antes de começar, verifique se o grupo de segurança do Client VPN está associado a outros recursos em sua VPC. Se você adicionar ou remover regras que fazem referência ao grupo de segurança do Client VPN, poderá conceder ou negar acesso aos outros recursos associados também. Para evitar isso, use um grupo de segurança criado especificamente para uso com seu endpoint do Client VPN.

Como criar uma regra de grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security Groups.(Grupos de segurança).
3. Escolha o grupo de segurança associado à instância em que o recurso está sendo executado.
4. Escolha Actions (Ações), Edit inbound rules (Editar regras de entrada).
5. Selecione Add Rule (Adicionar regra) e faça o seguinte:

   - Em Type (Tipo), escolha All traffic (Todo o tráfego), ou um tipo específico de tráfego que você deseja permitir.

- Para Source (Origem), escolha Custom (Personalizar) e insira ou escolha o ID do grupo de segurança do Client VPN.

6. Selecione Save rules (Salvar regras).

Para remover o acesso a um recurso específico, verifique o grupo de segurança associado à instância em que o recurso está sendo executado. Se houver uma regra que permita o tráfego do grupo de segurança do Client VPN, exclua-a.

Como verificar as regras do grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security Groups.(Grupos de segurança).
3. Escolha Inbound Rules (Regras de entrada).
4. Revise a lista de regras. Se houver uma regra em que Source (Origem) seja o grupo de segurança do Client VPN, escolha Edit rules (Editar Regras) e selecione Delete (Excluir) (o ícone x) para a regra. Escolha Save rules (Salvar regras).

Restringir o acesso com base em grupos de usuários

Se o endpoint do Client VPN estiver configurado para autenticação baseada no usuário, você poderá conceder a grupos específicos de usuários acesso a partes específicas da rede. Para fazer isso, conclua as seguintes etapas:

1. Configure usuários e grupos no AWS Directory Service ou no seu IdP. Para obter mais informações, consulte os tópicos a seguir:
   - Autenticação do Active Directory (p. 6)
   - Requisitos e considerações para autenticação federada baseada em SAML (p. 12)
2. Crie uma regra de autorização para seu endpoint do Client VPN que permita a um grupo especificado acesso a toda a rede ou parte dela. Para obter mais informações, consulte Regras de autorização (p. 43).

Se o endpoint do Client VPN estiver configurado para autenticação mútua, você não poderá configurar grupos de usuários. Ao criar uma regra de autorização, você deve conceder acesso a todos os usuários. Para permitir que grupos específicos de usuários acessem partes específicas da rede, é possível criar vários endpoints do Client VPN. Por exemplo, para cada grupo de usuários que acessa sua rede, faça o seguinte:

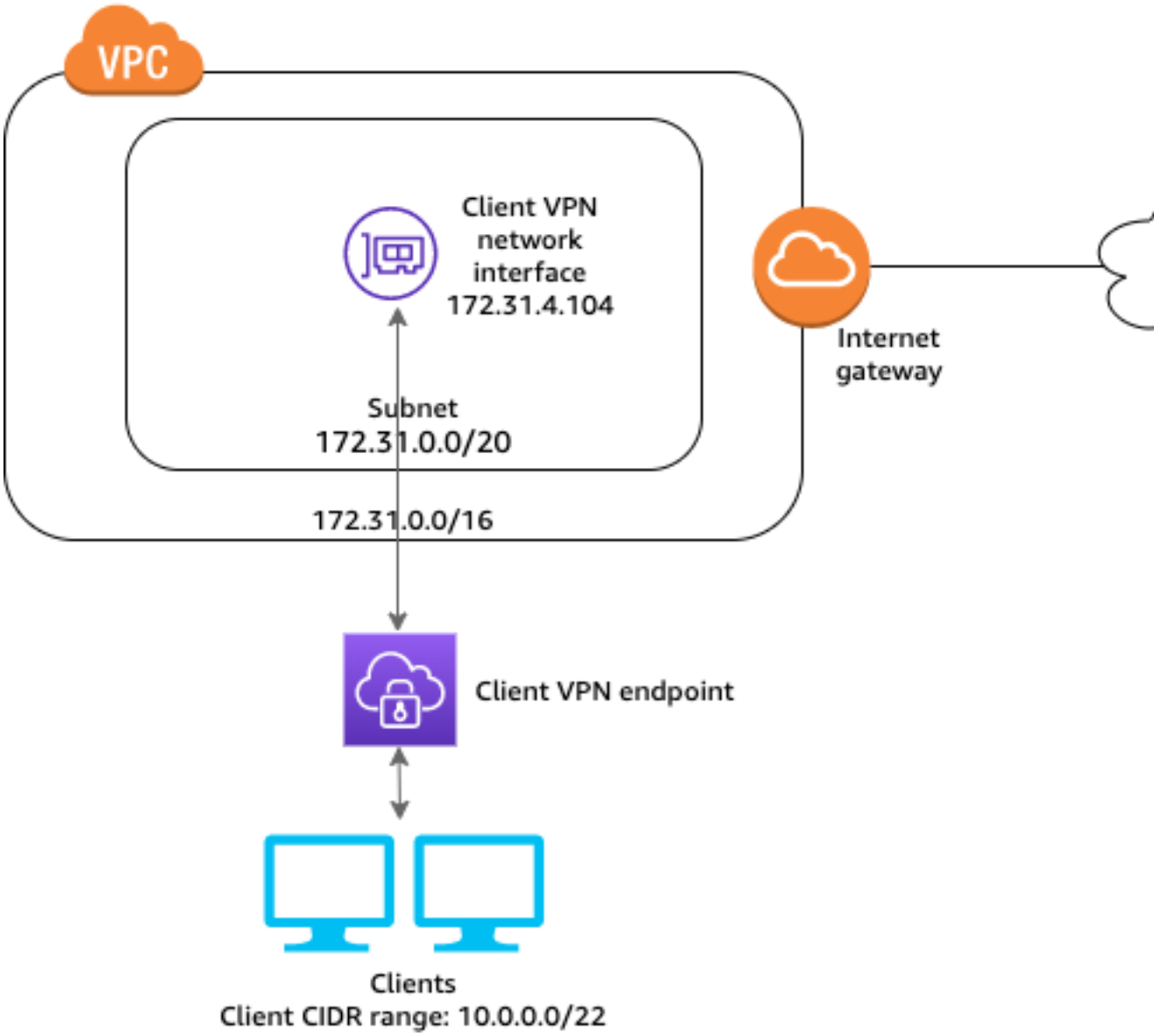
1. Crie um conjunto de certificados e chaves de servidor e cliente para esse grupo de usuários. Para obter mais informações, consulte Autenticação mútua (p. 6).
2. Crie um endpoint do cliente VPN. Para obter mais informações, consulte Criar um endpoint do Client VPN (p. 51).
3. Crie uma regra de autorização que conceda acesso a toda a rede ou parte dela. Por exemplo, para um endpoint do Client VPN usado por administradores, você pode criar uma regra de autorização que conceda acesso a toda a rede. Para obter mais informações, consulte Adicionar uma regra de autorização a um endpoint do Client VPN (p. 43).

Conceitos básicos da cliente VPN

Neste tutorial, você criará um endpoint de VPN do cliente que faz o seguinte:

- Fornece a todos os clientes acesso a uma única VPC.
- Fornece a todos os clientes acesso à Internet.
- Usa autenticação mútua (p. 6).

O diagrama a seguir representa a configuração da VPC e do endpoint da cliente VPN depois da conclusão deste tutorial.



Etapas

Pré-requisitos

Antes de começar este tutorial de conceitos básicos, verifique se você tem o seguinte:

- As permissões necessárias para trabalhar com endpoints da cliente VPN.
- As permissões necessárias para importar certificados no AWS Certificate Manager.
- Uma VPC com pelo menos uma sub-rede e um gateway da Internet. A tabela de rota associada à sua sub-rede deve ter uma rota para o gateway da Internet.

Etapa 1: gerar chaves e certificados de servidor e cliente

Este tutorial usa a autenticação mútua. Com a autenticação mútua, a VPN do cliente usa certificados para realizar a autenticação entre os clientes e o endpoint da VPN do cliente. Você precisará ter um certificado e uma chave de servidor e pelo menos um certificado e uma chave de cliente. No mínimo, o certificado do servidor precisará ser importado para o AWS Certificate Manager (ACM) e especificado quando você criar o endpoint da VPN do cliente. A importação do certificado do cliente para o ACM é opcional.

Se você ainda não tiver certificados para usar para esse fim, eles poderão ser criados usando o utilitário easy-rsa do OpenVPN. Para obter as etapas detalhadas de geração dos certificados e das chaves de servidor e cliente usando o utilitário easy-rsa do OpenVPN e obter instruções sobre como importá-los para o ACM, consulte Autenticação mútua (p. 6).

Etapa 2: Criar um endpoint da cliente VPN.

O endpoint do cliente VPN é o recurso que você cria e configura para habilitar e gerenciar sessões do cliente VPN. É o ponto de término de todas as sessões da VPN do cliente.

Como criar um endpoint da cliente VPN.

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints da VPN do cliente) e escolha Create Client VPN endpoint (Criar endpoint da VPN do cliente).
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o endpoint da VPN do cliente.
4. Em CIDR IPv4 do cliente, especifique um intervalo de endereços IP, em notação CIDR, para atribuir endereços IP do cliente. Por exemplo, `10.0.0.0/22`.

Note

O intervalo de endereços não pode se sobrepor ao intervalo de endereços da rede de destino, ao intervalo de endereços da VPC nem a nenhuma das rotas que serão associadas ao endpoint da VPN do cliente. O intervalo de endereços do cliente deve ser de, no mínimo, /22 e não maior que o tamanho do bloco CIDR /12. Não é possível alterar o intervalo de endereços do cliente depois de criar o endpoint da VPN do cliente.

5. Em Server certificate ARN (ARN do certificado do servidor), selecione o ARN do certificado do servidor gerado na Etapa 1 (p. 37).

   Note

   O certificado do servidor deve ser provisionado ou importado para o AWS Certificate Manager (ACM) na mesma região da AWS.

6. Em Authentication options (Opções de autenticação), escolha Use mutual authentication (Usar autenticação mútua) e, em Client certificate ARN (ARN do certificado do cliente), escolha o ARN do certificado que você deseja usar como o certificado do cliente.

   Note

   Se os certificados do servidor e do cliente forem assinados pela mesma autoridade de certificação (CA), você terá a opção de especificar o ARN do certificado do servidor tanto para os certificados do cliente como para os do servidor. Nesse cenário, qualquer certificado do cliente que corresponda ao certificado do servidor pode ser usado para autenticar.

7. Mantenha o restante das configurações padrão e selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Depois que você cria o endpoint da cliente VPN, seu estado é `pending-associate`. Os clientes só poderão estabelecer uma conexão VPN depois que você associar pelo menos uma rede de destino.

Para obter mais informações sobre as outras opções que você pode especificar ao criar um endpoint da cliente VPN., consulte Criar um endpoint do Client VPN (p. 51).

Etapa 3: associar uma rede de destino

Para permitir que os clientes estabeleçam uma sessão de VPN, associe uma rede de destino ao endpoint da VPN do cliente. Uma rede de destino é uma sub-rede em uma VPC.

Como associar uma rede de destino a um endpoint da VPN do cliente

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente que você criou no procedimento anterior e escolha Target network associations (Associações de rede de destino), Associate target network (Associar rede de destino).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada.
5. Em Choose a subnet to associate (Escolher uma sub-rede para associar), escolha a sub-rede a ser associada ao endpoint da VPN do cliente.
6. SelecioneAssociate target network (Associar rede de destino).

   Note

   Se as regras de autorização permitirem, uma associação de sub-rede é suficiente para que os clientes acessem toda a rede de uma VPC. É possível associar sub-redes adicionais para fornecer alta disponibilidade caso uma das zonas de disponibilidade seja desativada.

Quando você associa a primeira sub-rede ao endpoint da cliente VPN, acontece o seguinte:

- O estado do endpoint da cliente VPN muda para `available`. Agora, os clientes podem estabelecer uma conexão VPN, mas não poderão acessar recursos na VPC até que você adicione as regras de autorização.
- A rota local da VPC é adicionada automaticamente à tabela de rotas do endpoint da cliente VPN.
- O grupo de segurança padrão da VPC é aplicado automaticamente ao endpoint da VPN do cliente.

Etapa 4: adicionar uma regra de autorização para a VPC

Para que os clientes acessem a VPC, é preciso haver uma rota para a VPC na tabela de rotas do endpoint da VPN do cliente e uma regra de autorização. A rota já foi adicionada automaticamente na etapa anterior. Neste tutorial, queremos conceder acesso à VPC para todos os usuários.

Como adicionar uma regra de autorização para a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Escolha o endpoint da VPN do cliente ao qual deseja adicionar a regra de autorização. Escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
4. Em Destination network to enable access (Rede de destino para permitir acesso), insira o CIDR da rede à qual você deseja permitir acesso. Por exemplo, para permitir acesso a toda a VPC, especifique o bloco CIDR IPv4 da VPC.
5. Para Conceder acesso a, escolha Permitir acesso a todos os usuários.
6. (Opcional) Em Description (Descrição), insira uma breve descrição da regra de autorização.
7. Escolha Adicionar regra de autorização.

Etapa 5: conceder acesso à Internet

Você pode conceder acesso a redes adicionais conectadas à VPC, como serviços da AWS, VPCs emparelhadas, redes on-premises e a Internet. Para cada rede adicional, adicione uma rota à rede na tabela de rotas do endpoint da VPN do cliente e configure uma regra de autorização para conceder acesso aos clientes.

Neste tutorial, queremos conceder acesso à Internet e também à VPC para todos os usuários. Você já configurou o acesso à VPC, portanto, essa etapa é para acesso à Internet.

Como conceder acesso à Internet

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Escolha o endpoint da VPN do cliente que você criou para este tutorial. Escolha Route Table (Tabela de rotas) e Create Route (Criar rota).
4. Em Destino da rota, insira `0.0.0.0/0`. Em Subnet ID for target network association (ID da sub-rede para a associação da rede de destino), especifique o ID da sub-rede pela qual deseja encaminhar o tráfego.
5. Escolha Criar rota.
6. Escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).

7. Em Destination network to enable access (Rede de destino para permitir acesso), insira `0.0.0.0/0` e escolha Allow access to all users (Permitir acesso a todos os usuários).
8. Escolha Adicionar regra de autorização.

Etapa 6: verificar os requisitos do grupo de segurança

Neste tutorial, nenhum grupo de segurança foi especificado durante a criação do endpoint da VPN do cliente na Etapa 2. Isso significa que o grupo de segurança padrão da VPC é aplicado automaticamente ao endpoint da VPN do cliente quando uma rede de destino é associada. Como resultado, o grupo de segurança padrão da VPC agora deve estar associado ao endpoint da VPN do cliente.

Verificar os requisitos de grupo de segurança a seguir

- O grupo de segurança associado à sub-rede pela qual você está roteando tráfego (nesse caso, o grupo de segurança da VPC padrão) deve permitir tráfego de saída para a Internet. Para fazer isso, adicione uma regra de saída que permita todo o tráfego para o destino `0.0.0.0/0`.
- Os grupos de segurança para os recursos na VPC devem ter uma regra que permita o acesso do grupo de segurança aplicado ao endpoint da VPN do cliente (nesse caso, o grupo de segurança da VPC padrão). Isso permite que os clientes acessem os recursos na VPC.

Para mais informações, consulte Grupos de segurança (p. 14).

Etapa 7: baixar o arquivo de configuração do endpoint da VPN do cliente

A próxima etapa é baixar o arquivo de configuração do endpoint da VPN do cliente e prepará-lo. O arquivo de configuração inclui os detalhes do endpoint da VPN do cliente e as informações de certificado necessárias para estabelecer uma conexão VPN. Forneça esse arquivo aos usuários finais que precisam se conectar ao endpoint da VPN do cliente. O usuário final usa o arquivo para configurar a aplicação da VPN do cliente.

Como fazer download do arquivo de configuração do endpoint da cliente VPN e prepará-lo

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN que você criou para este tutorial e escolha Download client configuration (Baixar a configuração do cliente).
4. Localize o certificado de cliente e a chave que foram gerados na etapa 1 (p. 37). A chave e o certificado de cliente estão disponíveis nos seguintes locais no repositório clonado OpenVPN easy-rsa:

   - Certificado do cliente — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Chave do cliente — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Abra o arquivo de configuração do endpoint do Client VPN usando seu editor de texto preferido. Adicione as etiquetas `<cert></cert>` e `<key></key>` ao arquivo. Coloque o conteúdo do certificado do cliente e o conteúdo da chave privada entre as etiquetas correspondentes, como:

```
<cert>
```

```
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. Localize a linha que especifica o nome DNS do endpoint da cliente VPN e adicione uma string aleatória ao início dela para que o formato seja *string_aleatória.nome_DNS_exibido*. Por exemplo:

   - Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
   - Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`

   Note

   Recomenda-se sempre usar o nome DNS fornecido para o endpoint da VPN do cliente no arquivo de configuração, conforme descrito. Os endereços IP para os quais o nome DNS vai resolver estão sujeitos a alterações.
7. Salve e feche o arquivo de configuração do endpoint da cliente VPN.
8. Distribua o arquivo de configuração do endpoint da VPN do cliente para os usuários finais.

Para obter mais informações sobre o arquivo de configuração do endpoint da cliente VPN, consulte Exportar e configurar o arquivo de configuração do cliente (p. 58).

Etapa 8: conectar-se ao endpoint da VPN do cliente

Você pode se conectar ao endpoint da VPN do cliente usando o cliente fornecido pela AWS ou outra aplicação do cliente baseada no OpenVPN e o arquivo de configuração que acabou de criar. Para obter mais informações, consulte o Guia do usuário da AWS Client VPN.

Trabalhar com o Cliente VPN

Você pode trabalhar com o cliente VPN usando o console da Amazon VPC ou a AWS CLI.

Tópicos

Acessar o portal de autoatendimento

Se você ativou o portal de autoatendimento para o endpoint do Client VPN, é possível fornecer um URL do portal de autoatendimento para seus clientes. Os clientes podem acessar o portal no navegador da Web e usar as credenciais baseadas em usuário para fazer login. No portal, os clientes podem baixar o arquivo de configuração de endpoint do cliente VPN e a versão mais recente do cliente fornecido pela AWS.

As seguintes regras se aplicam:

- O portal de autoatendimento não está disponível para clientes autenticados usando a autenticação mútua.
- O arquivo de configuração disponível no portal de autoatendimento é o mesmo que você exportou usando o console da Amazon VPC ou a AWS CLI CLI. Caso seja necessário personalizar o arquivo de configuração antes de distribuí-lo aos clientes, essa distribuição deverá ser feita por você.
- É necessário habilitar a opção do portal de autoatendimento para o endpoint do Client VPN ou os clientes não conseguirão acessar o portal. Se esta opção não estiver ativada, você poderá modificar o endpoint do Client VPN para ativá-lo.

Depois de habilitar a opção do portal de autoatendimento, forneça um dos seguintes URLs aos clientes:

- `https://self-service.clientvpn.amazonaws.com/`

  Se os clientes acessarem o portal usando esse URL, será necessário inserir o ID do endpoint do Client VPN antes que eles possam fazer login.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Substitua `<endpoint-id>` no URL anterior pelo ID do endpoint do Client VPN, por exemplo, `cvpn-endpoint-0123456abcd123456`.

Também é possível visualizar o URL do portal de autoatendimento na saída do comando describe-client-vpn-endpoints da AWS CLI. Como alternativa, o URL está disponível na guia Details (Detalhes) na página Client VPN Endpoints (Endpoints da VPN do cliente) no console da Amazon VPC.

Para obter mais informações sobre como configurar o portal de autoatendimento para uso com a autenticação federada, consulte Suporte para o portal de autoatendimento (p. 13).

Regras de autorização

Regras de autorização atuam como regras de firewall que concedem acesso a redes. Adicionando regras de autorização, você concede acesso à rede especificada a clientes específicos. Você deve ter uma regra de autorização para cada rede à qual deseja conceder acesso. É possível adicionar regras de autorização a um endpoint do Client VPN usando o console e a AWS CLI.

> Note
>
> O cliente VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização. Consulte o tópico sobre solução de problemas Regras de autorização para grupos do Active Directory não funcionando conforme esperado (p. 82) e Prioridade de rota no Guia do usuário do Amazon VPC para obter mais detalhes.

Índice

Adicionar uma regra de autorização a um endpoint do Client VPN

Para adicionar uma regra de autorização a um endpoint do cliente VPN usando AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente ao qual a regra de autorização deve ser adicionada, escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
4. Em Destination network to enable access (Rede de destino para habilitar o acesso), insira o endereço IP, em notação CIDR, da rede que você deseja que os usuários acessem (por exemplo, o bloco CIDR da VPC).
5. Especifique quais clientes têm permissão para acessar a rede especificada. Em For grant access to (Para conceder acesso a), siga um destes procedimentos:
   - Para conceder acesso a todos os clientes, escolha Allow access to all users (Permitir acesso a todos os usuários).
   - Para restringir o acesso a clientes específicos, escolha Permitir acesso a usuários em um grupo de acesso específico e, em ID do grupo de acesso, insira o ID do grupo ao qual conceder acesso. Por exemplo, o identificador de segurança (SID) de um grupo do Active Directory ou o ID/nome de um grupo definido em um provedor de identidade baseado em SAML (IdP).
     - (Active Directory) Para conseguir o SID, você pode usar o cmdlet Get-ADGroup do Microsoft PowerShell, por exemplo:

```
Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
```

Como alternativa, abra a ferramenta Usuários e Computadores do Active Directory, visualize as propriedades do grupo, acesse a guia Editor de atributos e obtenha o valor de `objectSID`. Se necessário, primeiro selecione View (Visualizar), Advanced Features (Recursos avançados) para habilitar a guia Editor de atributos.

- (Autenticação federada baseada em SAML) O ID/nome do grupo deve corresponder às informações de atributo de grupo retornadas na declaração SAML.

6. Em Descrição, insira uma breve descrição da regra de autorização.
7. Escolha Adicionar regra de autorização.

Adicionar uma regra de autorização a um endpoint do Client VPN (AWS CLI)

Use o comando authorize-client-vpn-ingress.

Remover uma regra de autorização de um endpoint do Client VPN

Ao excluir uma regra de autorização, você remove o acesso à rede especificada.

É possível remover regras de autorização de um endpoint do Client VPN usando o console e a AWS CLI.

Para remover uma regra de autorização de um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente ao qual a regra de autorização foi adicionada e escolha Authorization rules (Regras de autorização).
4. Selecione a regra de autorização a ser excluída, escolha Remove authorization rule (Remover regra de autorização) e Remove authorization rule (Remover regra de autorização).

Para remover uma regra de autorização de um endpoint do Client VPN (AWS CLI)

Use o comando revoke-client-vpn-ingress.

Visualizar regras de autorização

É possível visualizar regras de autorização de um endpoint específico do Client VPN usando o console e a AWS CLI.

Para visualizar regras de autorização (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente para o qual deseja visualizar regras de autorização e escolha Authorization rules (Regras de autorização).

Para visualizar regras de autorização (AWS CLI)

Use o comando describe-client-vpn-authorization-rules.

Listas de revogação de certificados de cliente

É possível usar listas de revogação de certificados de cliente para revogar o acesso a um endpoint do Client VPN para certificados de cliente específicos.

> **Note**
>
> Para obter mais informações sobre como gerar os certificados e as chaves de servidor e cliente, consulte Autenticação mútua (p. 6)

Para obter mais informações sobre o número de entradas que você pode adicionar a uma lista de revogação de certificados de cliente, consulte Cotas do Client VPN (p. 79).

Índice

Gerar uma lista de revogação de certificados de cliente

Linux/macOS

No procedimento a seguir, gere uma lista de revogação de certificados de cliente usando o utilitário de linha de comando OpenVPN easy-rsa.

Para gerar uma lista de revogação de certificados de cliente usando o OpenVPN easy-rsa

1. Clone o repositório OpenVPN easy-rsa no seu computador local.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

2. Navegue até a pasta `easy-rsa/easyrsa3` no seu repositório local.

```
$ cd easy-rsa/easyrsa3
```

3. Revogar o certificado de cliente e gerar a lista de revogação de cliente.

```
$ ./easyrsa revoke client_certificate_name
$ ./easyrsa gen-crl
```

Digite `yes` quando solicitado.

Windows

O procedimento a seguir usa o software OpenVPN para gerar uma lista de revogação de cliente. Ele pressupõe que você seguiu as etapas para usar o software OpenVPN (p. 6) para gerar os certificados e as chaves de cliente e servidor.

Para gerar uma lista de revogação de certificados de cliente usando o EasyRSA versão 3.x.x

1. Abra um prompt de comando e navegue até o diretório EasyRSA-3.x.x, o que dependerá de onde ele estiver instalado no sistema.

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. Execute o arquivo “EasyRSA-Start.bat” para iniciar o shell EasyRSA.

```
C:\> .\EasyRSA-Start.bat
```

3. No shell EasyRSA, revogue o certificado do cliente.

```
# ./easyrsa revoke client_certificate_name
```

4. Digite “yes” (sim) quando solicitado.
5. Gere a lista de revogação de clientes.

```
# ./easyrsa gen-crl
```

6. A lista de revogação de cliente será criada neste local:

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

Para gerar uma lista de revogação de certificados de cliente usando versões anteriores do EasyRSA

1. Abra um prompt de comando e navegue até o diretório OpenVPN.

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. Execute o arquivo `vars.bat`.

```
C:\> vars
```

3. Revogar o certificado de cliente e gerar a lista de revogação de cliente.

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

Importar uma lista de revogação de certificados de cliente

Você deve ter um arquivo de lista de revogação de certificados de cliente para importar. Para obter mais informações sobre como gerar uma lista de revogação de certificados de cliente, consulte Gerar uma lista de revogação de certificados de cliente (p. 45).

Você pode importar uma lista de revogação de certificados de cliente usando o console e a AWS CLI.

Para importar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do Client VPN para o qual você deseja importar a lista de revogação de certificados de cliente.

4. Escolha Actions (Ações) e Import Client Certificate CRL (Importar CRL de certificados de cliente).
5. Em Certificate Revocation List (Lista de revogação de certificado), insira o conteúdo do arquivo de lista de revogação de certificados de cliente e escolha Import client certificate CRL (Importar CRL de certificados de cliente).

Para importar uma lista de revogação de certificados de cliente (AWS CLI)

Use o comando import-client-vpn-client-certificate-revocation-list.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-revocation-
list file:path_to_CRL_file --client-vpn-endpoint-id endpoint_id --region region
```

Exportar uma lista de revogação de certificados de cliente

Você pode exportar listas de revogação de certificados de cliente usando o console e a AWS CLI.

Para exportar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do Client VPN para o qual você deseja exportar a lista de revogação de certificados de cliente.
4. Escolha Actions (Ações), Export Client Certificate CRL (Exportar CRL de certificados de cliente) e Export Client Certificate CRL (Exportar CRL de certificados de cliente).

Para exportar uma revogação de certificado de cliente (AWS CLI)

Use o comando export-client-vpn-client-certificate-revocation-list.

Conexões de cliente

Conexões são sessões de VPN que foram estabelecidas pelos clientes. Uma conexão é estabelecida quando um cliente se conecta com êxito a um endpoint do Client VPN.

Tópicos

Visualizar conexões de clientes

Você pode visualizar conexões de clientes usando o console e a AWS CLI. As informações de conexão incluem o endereço IP atribuído do intervalo CIDR do cliente.

Para visualizar conexões de clientes (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN para o qual você deseja visualizar conexões de clientes.
4. Escolha a guia Connections (Conexões). A guia Connections (Conexões) lista todas as conexões de clientes ativas e encerradas.

Para visualizar conexões de clientes (AWS CLI)

Use o comando describe-client-vpn-connections.

Encerrar uma conexão de cliente

Quando você encerra uma conexão de cliente, a sessão de VPN também é encerrada.

É possível terminar conexões de cliente usando o console e a AWS CLI.

Para encerrar uma conexão de cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual o cliente está conectado e escolha Connections (Conexões).
4. Selecione a conexão a ser encerrada, escolha Terminate Connection (Encerrar conexão) e depois Terminate Connection (Encerrar conexão) novamente.

Para terminar uma conexão de cliente (AWS CLI)

Use o comando terminate-client-vpn-connections.

Banner de login do cliente

O AWS Client VPN fornece a opção de exibir um banner de texto em aplicações de desktop do cliente VPN fornecidas pela AWS quando uma sessão VPN é estabelecida. Você pode definir o conteúdo do banner de texto de modo a atender às suas necessidades regulamentares e de conformidade. É possível usar no máximo 1400 caracteres codificados em UTF-8.

> Note
>
> Quando um banner de login do cliente for habilitado, ele será exibido somente em sessões VPN recém-criadas. As sessões VPN existentes não serão interrompidas, mas o banner será exibido quando uma sessão existente for restabelecida.

Consulte Notas de release do cliente fornecido pela AWS no Guia do usuário do AWS Client VPN para obter detalhes sobre aplicações de desktop do cliente.

Índice

Configurar um banner de login do cliente durante a criação de um endpoint do cliente VPN

Para obter etapas detalhadas para habilitar um banner de login do cliente durante a criação de um endpoint do cliente VPN, consulte Criar um endpoint do Client VPN (p. 51).

Configurar um banner de login do cliente para um endpoint do cliente VPN existente

Realize as etapas a seguir para configurar um banner de login do cliente para um endpoint do cliente VPN existente.

Habilitar banner de login do cliente em um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do cliente VPN que deseja modificar, escolha Actions (Ações) e escolha Modify Client VPN Endpoint (Modificar endpoint do cliente VPN).
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Ative Enable client login banner (Habilitar o banner de login do cliente).
6. Em Client login banner text (Texto do banner de login do cliente), insira o texto que será exibido em um banner nos clientes fornecidos pela AWS quando uma sessão VPN for estabelecida. Use apenas caracteres codificados UTF-8, com um máximo de 1400 caracteres permitidos.
7. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Habilitar banner de login do cliente em um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Desativar um banner de login do cliente para um endpoint da VPN do cliente existente

Use as etapas a seguir para desativar um banner de login do cliente para um endpoint da VPN do cliente existente.

Desativar o banner de login do cliente em um endpoint da VPN do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente que você deseja modificar, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Desative Enable client login banner? (Habilitar o banner de login do cliente?).
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Desativar o banner de login do cliente em um endpoint da VPN do cliente (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Modificar o texto do banner existente em um endpoint do cliente VPN

Realize as etapas a seguir para modificar o texto existente em um banner de login do cliente.

Modificar o texto do banner existente em um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente que você deseja modificar, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Enable client login banner? (Habilitar banner de login do cliente?), verifique se essa opção está ativada.
5. Em Client login banner text (Texto do banner de login do cliente), substitua o texto existente pelo novo texto que você deseja exibir em um banner de clientes fornecidos pela AWS quando uma sessão VPN for estabelecida. Use apenas caracteres codificados UTF-8, com um máximo de 1400 caracteres.
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar banner de login do cliente em um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Visualizar banner de login configurado atualmente

Realize as etapas a seguir para visualizar um banner de login configurado atualmente.

Visualizar banner de login atual para um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do cliente VPN que deseja visualizar.
4. Verifique se a guia Details (Detalhes) está selecionada.
5. Visualize o texto do banner de login configurado atualmente ao lado de Client login banner text (Texto do banner de login do cliente).

Visualizar banner de login configurado atualmente para um endpoint do cliente VPN (AWS CLI)

Use o comando describe-client-vpn-endpoints.

Endpoints do Client VPN

Todas as sessões de Client VPN são encerradas no endpoint do Client VPN. Você configura o endpoint do Client VPN para gerenciar e controlar todas as sessões de Client VPN.

Índice

- Excluir um endpoint do Client VPN (p. 55)

Criar um endpoint do Client VPN

Crie um endpoint do Client VPN para permitir que seus clientes estabeleçam uma sessão de VPN.

O cliente VPN deve ser criado na mesma conta da AWS na qual a rede de destino pretendida é provisionada.

Pré-requisitos

Antes de começar, faça o seguinte:

- Revise as regras e as limitações em Limitações e regras do VPN do Cliente (p. 3).
- Gere o certificado do servidor e, se necessário, o certificado do cliente. Para mais informações, consulte Autenticação de cliente (p. 6).

Para criar um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN. e escolha Criar endpoint da cliente VPN.
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o endpoint da VPN do cliente.
4. Em CIDR IPv4 do cliente, especifique um intervalo de endereços IP, em notação CIDR, para atribuir endereços IP do cliente. Por exemplo, `10.0.0.0/22`.

   Note

   O intervalo de endereços não pode se sobrepor ao intervalo de endereços da rede de destino, ao intervalo de endereços da VPC nem a nenhuma das rotas que serão associadas ao endpoint da VPN do cliente. O intervalo de endereços do cliente deve ser de, no mínimo, /22 e não maior que o tamanho do bloco CIDR /12. Não é possível alterar o intervalo de endereços do cliente depois de criar o endpoint da VPN do cliente.
5. Para ARN do certificado de servidor, especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint da cliente VPN. ao qual estão se conectando.

   Note

   O certificado de servidor deve estar presente no AWS Certificate Manager (ACM) na região em que o endpoint do cliente VPN está sendo criado. O certificado pode ser provisionado com o ACM ou importado para o ACM.
6. Especifique o método de autenticação a ser usado para autenticar os clientes quando eles estabelecer uma conexão VPN. Você deve selecionar um método de autenticação.

   - Para utilizar a autenticação baseada no usuário, selecione Utilizar autenticação baseada no usuário e, depois, escolha uma das seguintes opções:
     - Autenticação do Active Directory: escolha esta opção para autenticação do Active Directory. Em ID do diretório, especifique o ID do Active Directory a ser usado.
     - Autenticação federada: escolha esta opção para autenticação federada baseada em SAML.

       Em ARN do provedor SAML, especifique o ARN do provedor de identidade SAML do IAM.

       (Opcional) Em Self-service SAML provider ARN (ARN do provedor SAML de autoatendimento), especifique o ARN do provedor de identidade SAML do IAM que você criou para oferecer suporte ao portal de autoatendimento (p. 13), se aplicável.

- Para usar a autenticação de certificado mútua, selecione Use mutual authentication (Usar autenticação mútua) e, em Client certificate ARN (ARN do certificado de cliente), especifique o ARN do certificado de cliente provisionado no AWS Certificate Manager (ACM).

  Note

  Se os certificados de servidor e cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor para ambos, servidor e cliente. Se o certificado do cliente tiver sido emitido por uma autoridade de certificação diferente, o ARN do certificado do cliente deverá ser especificado.

7. (Opcional) Em Connection logging (Log de conexão), especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente). Em Nome do grupo de logs do CloudWatch Logs, insira o nome do grupo de logs a ser usado. Em Nome do stream de logs do CloudWatch Logs, insira o nome do stream de logs a ser usado ou deixe essa opção em branco para que possamos criar um stream de logs para você.
8. (Opcional) Em Client Connect Handler (Manipulador de conexão do cliente), ative Enable client connect handler (Habilitar o manipulador de conexão do cliente) para executar o código personalizado que permite ou nega uma nova conexão com o endpoint da VPN do cliente. Em Client Connect Handler ARN (ARN do manipulador de conexão do cliente), especifique o nome de recurso da Amazon (ARN) da função do Lambda que contém a lógica que permite ou nega conexões.
9. (Opcional) Especifique quais servidores DNS devem ser usados para a resolução de DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

   Note

   Verifique se os servidores DNS possam ser acessados pelos clientes.

10. (Opcional) Por padrão, o servidor da VPN do cliente usa o protocolo de transporte `UDP`. Para usar o protocolo de transporte `TCP`, em Transport Protocol (Protocolo de transporte), selecione TCP.

    Note

    Em geral, o UDP oferece melhor performance que o TCP. Não é possível alterar o protocolo de transporte depois de criar o endpoint do Client VPN.

11. (Opcional) Para que o endpoint seja um endpoint de VPN do cliente de túnel dividido, ative Enable split-tunnel (Habilitar túnel dividido). Por padrão, o túnel dividido em um endpoint do cliente VPN está desabilitado.
12. (Opcional) Em VPC ID (ID da VPC), selecione a VPC a ser associada ao endpoint do Client VPN. Em Security Group IDs (IDs de grupo de segurança), selecione um ou mais grupos de segurança da VPC a serem aplicados ao endpoint do Client VPN.
13. (Opcional) Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.
14. (Opcional) Para gerar um URL do portal de autoatendimento (p. 42) para clientes, ative Enable self-service portal (Habilitar portal de autoatendimento).
15. (Opcional) Em Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração da sessão VPN em horas, conforme as opções disponíveis, ou deixe definido como padrão de 24 horas.
16. (Opcional) Especifique se deseja habilitar o texto do banner de login do cliente. Ative Enable client login banner (Habilitar o banner de login do cliente). Em Client login banner text (Texto do banner de login do cliente), insira o texto que será exibido em um banner nos clientes fornecidos pela AWS quando uma sessão VPN for estabelecida. Somente caracteres com codificação UTF-8. Máximo de 1400 caracteres.
17. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Depois de criar o endpoint do Client VPN, faça o seguinte para concluir a configuração e permitir que os clientes se conectem:

- O estado inicial do endpoint do Client VPN é `pending-associate`. Os clientes só poderão se conectar ao endpoint do Client VPN depois que você associar a primeira rede de destino (p. 62).
- Crie uma regra de autorização (p. 43) para especificar quais clientes têm acesso à rede.
- Baixe e prepare o arquivo de configuração (p. 58) do endpoint do Client VPN para distribuir aos seus clientes.
- Instrua seus clientes a usar o cliente fornecido pela AWS ou outra aplicação de cliente baseada em OpenVPN para conectar-se ao endpoint do cliente VPN. Para obter mais informações, consulte o Guia do usuário do AWS Client VPN.

Como criar um endpoint do Client VPN (AWS CLI)

Use o comando create-client-vpn-endpoint.

Modificar um endpoint do Client VPN

Após a criação de um Client VPN, é possível modificar qualquer uma das seguintes configurações:

- A descrição
- O certificado de servidor
- As opções de registro em log da conexão do cliente
- A opção do manipulador de conexão do cliente
- Os servidores DNS
- A opção de túnel dividido
- A VPC e as associações do grupo de segurança
- O número da porta VPN
- A opção do portal de autoatendimento
- Duração máxima da sessão VPN
- Habilitar ou desabilitar o texto do banner de login do cliente
- Texto do banner de login do cliente

Não é possível modificar o intervalo CIDR IPv4 do cliente, as opções de autenticação nem o protocolo de transporte após a criação do endpoint do Client VPN.

Quando você modifica qualquer um dos seguintes parâmetros em um endpoint do Client VPN, a conexão é redefinida:

- O certificado de servidor
- Os servidores DNS
- A opção de túnel dividido (ligar ou desligar o suporte)
- Rotas (quando você usa a opção de túnel dividido)
- Lista de revogação de certificados (CRL)
- Regras de autorização
- O número da porta VPN

É possível modificar um endpoint do Client VPN usando o console ou a AWS CLI.

Para modificar um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente a ser modificado, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Description (Descrição), digite uma breve descrição do endpoint do Client VPN.
5. Para ARN do certificado de servidor, especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint da cliente VPN. ao qual estão se conectando.

   Note

   O certificado de servidor deve estar presente no AWS Certificate Manager (ACM) na região em que o endpoint do cliente VPN está sendo criado. O certificado pode ser provisionado com o ACM ou importado para o ACM.
6. Especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Em Enable log details on client connections (Habilitar detalhes de log em conexões de cliente), siga um destes procedimentos:

   - Para ativar o log de conexão de cliente, ative Enable log details on client connections (Habilitar detalhes de log em conexões de cliente). Em CloudWatch Logs log group name (Nome do grupo de logs do CloudWatch Logs), selecione o nome do grupo de logs a ser usado. Em CloudWatch Logs log stream name (Nome do stream de logs do CloudWatch Logs), selecione o nome do fluxo de logs a ser usado ou deixe essa opção em branco para que possamos criar um fluxo de logs para você.
   - Para desativar o log de conexão de cliente, desative Enable log details on client connections (Habilitar detalhes de log em conexões de cliente).
7. Em Client connect handler (Manipulador de conexão de cliente), ative Enable client connect handler (Habilitar manipulador de conexão de cliente) para ativar o manipulador de conexão de cliente (p. 14). Em Client Connect Handler ARN (ARN do manipulador de conexão do cliente), especifique o nome de recurso da Amazon (ARN) da função do Lambda que contém a lógica que permite ou nega conexões.
8. Ative ou desative Enable DNS servers (Habilitar servidores DNS). Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

   Note

   Verifique se os servidores DNS possam ser acessados pelos clientes.
9. Ative ou desative Enable split-tunnel (Habilitar túnel dividido). Por padrão, o túnel dividido em um endpoint da VPN está desativado.
10. Em VPC ID (ID da VPC), escolha a VPC a ser associada ao endpoint da VPN do cliente. Em Security Group IDs (IDs de grupo de segurança), selecione um ou mais grupos de segurança da VPC a serem aplicados ao endpoint do Client VPN.
11. Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.
12. Para gerar um URL do portal de autoatendimento (p. 42) para clientes, ative Enable self-service portal (Habilitar portal de autoatendimento).
13. Em Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração da sessão VPN em horas, conforme as opções disponíveis, ou deixe definido como padrão de 24 horas.
14. Ative ou desative Enable client login banner (Habilitar o banner de login do cliente). Se quiser usar o banner de login do cliente, insira o texto que será exibido em um banner nos clientes fornecidos pela

AWS quando uma sessão VPN for estabelecida. Somente caracteres com codificação UTF-8. Máximo de 1400 caracteres.

15. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar um endpoint do Client VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Visualizar endpoints do Client VPN

É possível visualizar informações sobre endpoints do Client VPN ao usar o console ou a AWS CLI.

Como visualizar endpoints da VPN do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do Client VPN a ser visualizado.
4. Use as guias Details (Detalhes), Target network associations (Associações de rede de destino), Security groups (Grupos de segurança), Authorization rules (Regras de autorização), Route table (Tabela de rotas), Connections (Conexões) e Tags (Etiquetas) para visualizar informações sobre os endpoints da VPN do cliente existentes.

   Você também pode usar filtros para ajudar a refinar a pesquisa.

Como visualizar endpoints da VPN do cliente (AWS CLI)

Use o comando describe-client-vpn-endpoints.

Excluir um endpoint do Client VPN

Você deverá desassociar todas as redes de destino para excluir um endpoint da VPN do cliente. Ao excluir um endpoint do Client VPN, seu estado é alterado para `deleting` e os clientes não podem mais se conectar a ele.

É possível excluir um endpoint do Client VPN usando o console ou a AWS CLI.

Para excluir um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Escolha o endpoint da VPN do cliente a ser excluído. Escolha Actions (Ações), Delete Client VPN endpoint (Excluir endpoint da VPN do cliente).
4. Insira delete (excluir) na janela de confirmação e escolha Delete (Excluir).

Para excluir um endpoint do Client VPN (AWS CLI)

Use o comando delete-client-vpn-endpoint.

Trabalhando com logs de conexão

Você pode habilitar o registro em log de conexão para um endpoint do Client VPN, novo ou existente, e começar a capturar logs de conexão.

Antes de começar, é preciso ter um grupo de logs do CloudWatch Logs na sua conta. Para obter mais informações, consulte Como trabalhar com grupos de logs e transmissões de log no Manual do usuário do Amazon CloudWatch Logs. Aplicam-se cobranças ao uso do CloudWatch Logs. Para obter mais informações, consulte Preço do Amazon CloudWatch.

Ao habilitar o registro em log de conexão, você pode especificar o nome de um stream de logs no grupo de logs. Se você não especificar um stream de logs, o serviço do Client VPN criará um para você.

Habilitar o registro em log de conexão para um novo endpoint do Client VPN

Você pode habilitar o registro em log de conexão ao criar um endpoint do Client VPN usando o console ou a linha de comando.

Como habilitar o registro em log de conexão para um novo endpoint do Client VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Client VPN Endpoints (Endpoints da VPN do cliente) e Create Client VPN Endpoint (Criar endpoint da VPN do cliente).
3. Conclua as opções até chegar à seção Geração de logs de conexão . Para obter mais informações sobre essas opções, consulte Criar um endpoint do Client VPN (p. 51).
4. Em Connection logging (Log de conexão), ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente).
5. Em Nome do grupo de logs do CloudWatch Logs, escolha o nome do grupo de logs do CloudWatch Logs.
6. (Opcional) Em Nome do stream de logs do CloudWatch Logs, escolha o nome do stream de logs do CloudWatch Logs.
7. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Para habilitar o registro em log de conexão para um novo endpoint do Client VPN usando a AWS CLI

Use o comando create-client-vpn-endpoint e especifique o parâmetro `--connection-log-options`. Você pode especificar as informações de logs de conexão no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Habilitar o registro em log de conexão para um endpoint existente do Client VPN

É possível habilitar o registro em log de conexão para um endpoint do Client VPN existente usando o console ou a linha de comando.

Como habilitar o registro em log de conexão para um endpoint do Client VPN existente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Connection logging (Log de conexão), ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente).
5. Em Nome do grupo de logs do CloudWatch Logs, escolha o nome do grupo de logs do CloudWatch Logs.
6. (Opcional) Em Nome do stream de logs do CloudWatch Logs, escolha o nome do stream de logs do CloudWatch Logs.
7. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Para habilitar o registro em log de conexão para um endpoint do Client VPN existente usando a AWS CLI

Use o comando modify-client-vpn-endpoint e especifique o parâmetro `--connection-log-options`. Você pode especificar as informações de logs de conexão no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Visualizar logs de conexão

É possível visualizar os logs de conexão por meio do console do CloudWatch Logs.

Como visualizar os logs de conexão usando o console

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Grupos de logs e o grupo de log que contém seus logs de conexão.
3. Selecione o stream de logs para o endpoint do Client VPN.

   Note

   A coluna Timestamp exibe a hora em que o registro em log de conexão foi publicado no CloudWatch Logs, não a hora da conexão.

Para obter mais informações sobre como pesquisar dados de log, consulte Pesquisar dados de log usando padrões de filtro no Guia do usuário do Amazon CloudWatch Logs.

Desativar o log de conexão

É possível desativar o log de conexão de um endpoint da VPN do cliente usando o console ou a linha de comando. Quando você desativa o log de conexão, os logs de conexão existentes no CloudWatch Logs não são excluídos.

Como desativar o log de conexão usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.

3. Selecione o endpoint da VPN do cliente, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Connection logging (Log de conexão), desative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente).
5. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Como desativar o log de conexão usando a AWS CLI

Use o comando modify-client-vpn-endpoint e especifique o parâmetro `--connection-log-options`. Verifique se `Enabled` está definido como `false`.

Exportar e configurar o arquivo de configuração do cliente

O arquivo de configuração do endpoint do Client VPN é o arquivo que os clientes (usuários) usam para estabelecer uma conexão VPN com o endpoint do Client VPN. Você deve fazer download (exportar) desse arquivo e distribuí-lo a todos os clientes que precisam de acesso à VPN. Como alternativa, se você habilitou o portal de autoatendimento para o endpoint do Client VPN, os clientes podem fazer login no portal e baixar o arquivo de configuração. Para obter mais informações, consulte . Acessar o portal de autoatendimento (p. 42).

Se o endpoint do Client VPN usar a autenticação mútua, será necessário adicionar o certificado de cliente e a chave privada do cliente ao arquivo de configuração .ovpn do (p. 59) qual foi feito download. Depois de adicionar as informações, os clientes poderão importar o arquivo .ovpn para o software cliente OpenVPN.

> **Important**
>
> Se você não adicionar o certificado de cliente e as informações da chave privada do cliente ao arquivo, os clientes que se autenticam usando a autenticação mútua não poderão se conectar ao endpoint do Client VPN.

Por padrão, a opção "--remote-random-hostname" na configuração do cliente OpenVPN habilita o DNS curinga. Como o DNS curinga está habilitado, o cliente não armazena em cache o endereço IP do endpoint, e você não poderá executar ping no nome DNS do endpoint.

Se o endpoint do Client VPN usar a autenticação do Active Directory e se você habilitar o Multi-Factor Authentication (MFA) no diretório após distribuir o arquivo de configuração do cliente, será necessário fazer download de um novo arquivo e redistribuí-lo aos clientes. Os clientes não podem usar o arquivo de configuração anterior para se conectar ao endpoint do Client VPN.

Exportar o arquivo de configuração do cliente

É possível exportar a configuração do cliente usando o console ou a AWS CLI.

Para exportar configuração do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do Client VPN cuja configuração do cliente deve ser transferida por download e escolha Download Client Configuration (Fazer download da configuração do cliente).

Para exportar configuração do cliente (AWS CLI)

Use o comando export-client-vpn-client-configuration e especifique o nome do arquivo de saída.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id --
output text>config_filename.ovpn
```

Adicionar o certificado de cliente e as informações de chave (autenticação mútua)

Se o endpoint do Client VPN usar a autenticação mútua, será necessário adicionar o certificado de cliente e a chave privada do cliente ao arquivo de configuração .ovpn do qual foi feito download.

Você não pode modificar o certificado de cliente ao usar a autenticação mútua.

Como adicionar o certificado de cliente e as informações de chave (autenticação mútua)

Você pode usar uma das opções a seguir:

(Opção 1) Distribuir o certificado e a chave do cliente aos clientes junto com o arquivo de configuração do endpoint do Client VPN. Nesse caso, especifique o caminho para o certificado e a chave no arquivo de configuração. Abra o arquivo de configuração usando o editor de texto de sua preferência e adicione o seguinte ao final desse arquivo. Substitua */path/* pelo local do certificado e da chave do cliente (o local é relativo ao cliente que está se conectando ao endpoint).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(Opção 2) Adicionar o conteúdo do certificado do cliente entre as tags <cert></cert> e o conteúdo da chave privada entre as tags <key></key> ao arquivo de configuração. Se você escolher essa opção, somente o arquivo de configuração será distribuído aos clientes.

Se você gerou certificados de clientes separados e chaves para cada usuário que se conectará ao endpoint do Client VPN, repita essa etapa para cada usuário.

Veja a seguir um exemplo do formato de um arquivo configuração do Client VPN que inclui o certificado e a chave do cliente.

```
client
dev tun
proto udp
remote asdf.cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

```
reneg-sec 0
```

Rotas

Cada endpoint do cliente VPN tem uma tabela de rotas que descreve as rotas de redes de destino disponíveis. Cada rota na tabela de rotas determina para onde o tráfego de rede é direcionado. Você deve configurar regras de autorização para cada rota do endpoint do Client VPN para especificar quais clientes têm acesso à rede de destino.

Quando você associa uma sub-rede de uma VPC a um endpoint do Client VPN, uma rota para essa VPC é automaticamente adicionada à tabela de rotas do endpoint do Client VPN. Para habilitar o acesso a redes adicionais, como VPCs emparelhadas, redes locais, a rede local (para permitir que os clientes se comuniquem entre si) ou a Internet, você deve adicionar manualmente uma rota à tabela de rotas do endpoint do Client VPN.

> **Note**
>
> Se você estiver associando várias sub-redes ao endpoint do cliente VPN, certifique-se de criar uma rota para cada sub-rede, conforme descrito aqui O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente (p. 85). Cada sub-rede associada deve ter um conjunto idêntico de rotas.

Índice

Considerações sobre túnel dividido no endpoint do Client VPN

Quando você usa túnel dividido em um endpoint do Client VPN, todas as rotas que estão nas tabelas de rotas do Client VPN são adicionadas à tabela de rotas do cliente quando a VPN é estabelecida. Se você adicionar uma rota após a VPN ser estabelecida, deverá redefinir a conexão para que a nova rota seja enviada ao cliente.

É recomendável contabilizar o número de rotas que o dispositivo cliente pode manipular antes de modificar a tabela de rotas do endpoint do Client VPN.

Criar uma rota de endpoint

Ao criar uma rota, você especifica como o tráfego para a rede de destino deve ser direcionado.

Para permitir que os clientes acessem a Internet, adicione uma rota de destino `0.0.0.0/0`.

É possível adicionar rotas a um endpoint do Client VPN usando o console e a AWS CLI

Como criar uma rota de endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente ao qual você deseja adicionar a rota, escolha Route table (Tabela de rotas) e Create route (Criar rota).

4. Em Route destination (Destino da rota), especifique o intervalo CIDR IPv4 da rede de destino. Por exemplo:
   - Para adicionar uma rota à VPC do endpoint da VPN do cliente, insira o intervalo CIDR IPv4 da VPC.
   - Para adicionar uma rota para acesso à Internet, insira `0.0.0.0/0`.
   - Para adicionar uma rota a uma VPC emparelhada, insira o intervalo CIDR IPv4 da VPC emparelhada.
   - Para adicionar uma rota para uma rede on-premises, insira o intervalo CIDR IPv4 da conexão de VPN de local a local AWS.
5. Em Subnet ID for target network association (ID de sub-rede da associação de rede de destino), selecione a sub-rede associada ao endpoint da VPN do cliente.

   Como alternativa, se você estiver adicionando uma rota à rede local do endpoint da VPN do cliente, selecione `local`.
6. (Opcional) Em Description (Descrição), insira uma breve descrição da rota.
7. Escolha Create route (Criar rota).

Para criar uma rota de endpoint do Client VPN (AWS CLI)

Use o comando create-client-vpn-route.

Visualizar rotas de endpoint

Você pode visualizar as rotas de um endpoint específico do Client VPN usando o console ou a AWS CLI.

Para visualizar rotas do endpoint do Client VPN (console)

1. No painel de navegação, escolha Endpoints da cliente VPN.
2. Selecione o endpoint da VPN do cliente cujas rotas você deseja visualizar e escolha Route table (Tabela de rotas).

Para visualizar rotas do endpoint do Client VPN (AWS CLI)

Use o comando describe-client-vpn-routes .

Excluir uma rota de endpoint

Você só pode excluir rotas que foram adicionadas manualmente. Não é possível excluir rotas que foram adicionadas automaticamente quando você associou uma sub-rede ao endpoint do Client VPN. Para excluir rotas que foram adicionadas automaticamente, você deve desassociar a sub-rede que iniciou sua criação do endpoint do Client VPN.

É possível excluir uma rota de um endpoint do Client VPN usando o console ou a AWS CLI.

Como excluir uma rota de endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente do qual deseja excluir a rota e escolha Route table (Tabela de rotas).
4. Selecione a rota a ser excluída, escolha Delete route (Excluir rota) e Delete route (Excluir rota).

Para excluir uma rota de endpoint do Client VPN (AWS CLI)

Use o comando delete-client-vpn-route.

Redes de destino

Uma rede de destino é uma sub-rede em uma VPC. Um endpoint do Client VPN deve ter pelo menos uma rede de destino para permitir que os clientes se conectar a ele e estabeleçam uma conexão VPN.

Para obter mais informações sobre os tipos de acesso que você pode configurar (como permitir que os clientes acessem a Internet), consulte Cenários e exemplos (p. 23).

Índice

Associa uma rede de destino a um endpoint do Client VPN.

Você pode associar uma ou mais redes de destino (sub-redes) a um endpoint do Client VPN.

As seguintes regras se aplicam:

- A sub-rede deve ter um bloco CIDR com pelo menos uma máscara de bits /27, por exemplo 10.0.0.0/27. A sub-rede deve ter pelo menos 8 endereços IP disponíveis.
- O bloco CIDR da sub-rede não pode se sobrepor ao intervalo CIDR cliente do endpoint do Client VPN.
- Se você associar mais de uma sub-rede a um endpoint do Client VPN, cada sub-rede deverá estar em uma zona de disponibilidade diferente. Recomendamos que você associe pelo menos duas sub-redes para fornecer redundância de zona de disponibilidade.
- Se você especificou uma VPC ao criar o endpoint do Client VPN, a sub-rede deverá estar na mesma VPC. Se você ainda não associou uma VPC ao endpoint do Client VPN, poderá escolher qualquer sub-rede em qualquer VPC.

  Todas as associações de sub-rede adicionais devem ser na mesma VPC. Para associar uma sub-rede de uma VPC diferente, primeiro você deve modificar o endpoint do Client VPN e alterar a VPC associada a ele. Para mais informações, consulte Modificar um endpoint do Client VPN (p. 53).

Quando você associa uma sub-rede a um endpoint do Client VPN, nós adicionamos automaticamente a rota local da VPC na qual a sub-rede associada está provisionada à tabela de rotas do endpoint do Client VPN.

> **Note**
>
> Depois que as redes de destino forem associadas, quando você adicionar ou remover CIDRs adicionais à VPC anexada, você deverá executar uma das seguintes operações para atualizar a rota local da tabela de rotas de endpoint do Client VPN:
>
> - Desassocie o endpoint do Client VPN da rede de destino e, em seguida, associe-o novamente.
> - Adicione manualmente a rota ou remova-a da tabela de rotas do endpoint do Client VPN.

Depois de associar a primeira sub-rede ao endpoint do Client VPN, o status do endpoint do Client VPN muda de `pending-associate` para `available`, e os clientes podem estabelecer uma conexão VPN.

Como associar uma rede de destino a um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint de VPN do cliente ao qual deseja associar a rede de destino, escolha Target network associations (Associações da rede de destino) e Associate target network (Associar rede de destino).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada. Se você especificou uma VPC ao criar o endpoint do Client VPN ou se tiver associações de sub-rede anteriores, ela deverá ser a mesma VPC.
5. Em Choose a subnet to associate (Escolher uma sub-rede para associar), escolha a sub-rede a ser associada ao endpoint da VPN do cliente.
6. SelecioneAssociate target network (Associar rede de destino).

Para associar uma rede de destino a um endpoint do Client VPN (AWS CLI)

Use o comando associate-client-vpn-target-network.

Aplicar um grupo de segurança a uma rede de destino

Ao criar um endpoint do Client VPN, você pode especificar os grupos de segurança a serem aplicados à rede de destino. Quando você associa a primeira rede de destino a um endpoint do Client VPN, aplicamos automaticamente o grupo de segurança padrão da VPC na qual a sub-rede associada está localizada. Para mais informações, consulte Grupos de segurança (p. 14).

Você pode alterar os grupos de segurança para o endpoint do Client VPN. As regras de grupo de segurança de que você precisa dependem do tipo de acesso VPN que você deseja configurar. Para mais informações, consulte Cenários e exemplos (p. 23).

Para aplicar um grupo de segurança a uma rede de destino (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do Client VPN ao qual aplicar os grupos de segurança.
4. Escolha Security Groups (Grupos de segurança) e Apply Security Groups (Aplicar grupos de segurança).
5. Selecione os grupos de segurança apropriados em Security group IDs (IDs dos grupos de segurança).
6. Escolha Apply Security Groups (Aplicar grupos de segurança).

Para aplicar um grupo de segurança a uma rede de destino (AWS CLI)

Use o comando apply-security-groups-to-client-vpn-target-network.

Desassociar uma rede de destino de um endpoint do Client VPN

Se você desassociar todas as redes de destino de um endpoint do Client VPN, os clientes não poderão mais estabelecer uma conexão VPN. Quando você desassocia uma sub-rede, removemos a rota que foi criada automaticamente quando a associação foi feita.

Como desassociar uma rede de destino de um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint de VPN do cliente ao qual a rede de destino está associada e escolha Target network associations (Associações da rede de destino).
4. Selecione a rede de destino a ser desassociada, escolha Disassociate (Desassociar) e Disassociate target network (Desassociar rede de destino).

Para desassociar uma rede de destino de um endpoint do Client VPN (AWS CLI)

Use o comando disassociate-client-vpn-target-network.

Visualizar redes de destino

Você pode visualizar os destinos associados a um endpoint do Client VPN usando o console ou a AWS CLI.

Para visualizar redes de destino (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint de VPN do cliente apropriado e escolha Target network associations (Associações da rede de destino).

Para visualizar redes de destino usando a AWS CLI

Use o comando describe-client-vpn-target-networks.

Duração máxima da sessão VPN

O AWS Client VPN fornece várias opções para a duração máxima da sessão VPN. É possível configurar uma duração máxima de sessão VPN menor para atender aos requisitos de segurança e conformidade. Por padrão, a duração máxima da sessão VPN é 24 horas.

> Note
>
> Quando o valor máximo da duração da sessão VPN for diminuído, as sessões VPN ativas mais antigas do que o novo valor de tempo limite serão desconectadas.

Consulte Notas de release do cliente fornecido pela AWS no Guia do usuário do AWS Client VPN para obter detalhes sobre aplicações de desktop do cliente.

Índice

Configurar a sessão VPN máxima durante a criação de um endpoint do cliente VPN

Para obter as etapas detalhadas para configurar a sessão VPN máxima durante a criação de um endpoint do cliente VPN, consulte Criar um endpoint do Client VPN (p. 51).

Visualizar a duração máxima da sessão VPN atual

Realize as etapas a seguir para visualizar a duração máxima da sessão VPN atual.

Visualizar a duração máxima da sessão do cliente VPN para um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint do cliente VPN que deseja visualizar.
4. Verifique se a guia Details (Detalhes) está selecionada.
5. Veja a duração máxima da sessão VPN atual ao lado de Session timeout hours (Horas do tempo limite da sessão).

Veja a duração máxima da sessão do cliente VPN atual para um endpoint do cliente VPN (AWS CLI)

Use o comando describe-client-vpn-endpoints.

Modificar a duração máxima da sessão VPN

Realize as etapas a seguir para modificar uma duração máxima de sessão VPN existente.

Modificar uma duração máxima de sessão do cliente VPN existente para um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints (Endpoints da VPN do cliente).
3. Selecione o endpoint do cliente VPN que deseja modificar, escolha Actions (Ações) e escolha Modify Client VPN Endpoint (Modificar endpoint do cliente VPN).
4. Na sessão Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração de sessão VPN em horas.
5. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar uma duração máxima de sessão VPN existente para um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Segurança em AWS Client VPN

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Client VPN, consulte Serviços da AWS em escopo por programa de conformidade.
- Segurança da nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Client VPN. Os tópicos a seguir mostram como configurar o Client VPN para atender aos seus objetivos de segurança e de conformidade. Você também aprende a usar outros serviços da AWS que ajudam a monitorar e proteger os recursos do cliente VPN.

Tópicos

Proteção de dados no AWS Client VPN

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no AWS Client VPN. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da Conta da AWS e configure as contas de usuário individuais com o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.

- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com cliente VPN ou outros serviços da AWS usando o console, a APIAWS CLI ou SDKs da AWS. Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em trânsito

O AWS Client VPN fornece conexões seguras de qualquer local usando Transport Layer Security (TLS) 1.2 ou posterior.

Privacidade do tráfego entre redes

Habilitar o acesso entre redes

Você pode permitir que os clientes se conectem à sua VPC e outras redes por meio de um endpoint da VPN do Cliente Para obter mais informações e exemplos, consulte Cenários e exemplos (p. 23).

Restringir o acesso a redes

Você pode configurar seu endpoint da VPN do Cliente para restringir o acesso a recursos específicos em sua VPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa o endpoint do VPN do Cliente Para obter mais informações, consulte Restringir o acesso à sua rede (p. 33).

Autenticar clientes

A autenticação é implementada no primeiro ponto de entrada na Nuvem AWS. Ela é usada para determinar se os clientes têm permissão para se conectar ao endpoint da cliente VPN. Se a autenticação for bem-sucedida, os clientes se conectarão ao endpoint da cliente VPN e estabelecerão uma sessão de VPN. Se a autenticação falhar, a conexão será negada, e o cliente será impedido de estabelecer uma sessão de VPN.

O VPN do Cliente oferece os seguintes tipos de autenticação de cliente:

- Autenticação do Active Directory (p. 6) (baseada no usuário)
- Autenticação mútua (p. 6) (baseada em certificado)
- Single Sign-On (autenticação federada baseada em SAML) (p. 9) (baseado no usuário)

Gerenciamento de identidade e acesso para o Client VPN

A AWS usa credenciais de segurança para identificar você e conceder acesso aos seus recursos da AWS. Você pode usar recursos do AWS Identity and Access Management (IAM) para permitir que outros

usuários, serviços e aplicações usem seus recursos da AWS, totalmente ou de maneira limitada, sem compartilhar suas credenciais de segurança.

Por padrão, os usuários do IAM não têm permissão para criar, visualizar ou modificar os recursos da AWS. Para permitir que um usuário do IAM acesse recursos, como um endpoint do Client VPN, e realizar tarefas, você deve criar uma política do IAM. Essa política deve conceder permissão ao usuário do IAM para usar os recursos específicos e as ações de API de que ele precisa. Em seguida, anexe a política ao usuário do IAM ou ao grupo ao qual o usuário do IAM pertence. Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos recursos especificados.

Por exemplo, a política a seguir permite acesso somente leitura. Os usuários podem visualizar endpoints do Client VPN e seus componentes, mas não podem criá-los, modificá-los ou excluí-los.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeClientVpnEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Você também pode usar permissões em nível de recurso para restringir quais recursos os usuários podem usar quando invocam ações do Client VPN. Por exemplo, a política a seguir permite que os usuários trabalhem com endpoints do Client VPN, mas somente se o endpoint do Client VPN tiver a tag `purpose=test`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteClientVpnEndpoint",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:CreateClientVpnRoute",
                "ec2:DeleteClientVpnRoute",
                "ec2:RevokeClientVpnIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre o IAM, consulte o Manual do usuário do IAM. Para ver uma lista de ações do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no Guia do usuário do IAM.

Uso de funções vinculadas a serviços para o Client VPN

O cliente VPN da AWS usa funções vinculadas ao serviço para as permissões necessárias para chamar os outros produtos da AWS em seu nome. Para obter mais informações, consulte Usar funções vinculadas ao serviço no Guia do usuário do IAM.

Permissões de função vinculada ao serviço para o Client VPN

O cliente VPN da AWS usa a função vinculada ao serviço chamada AWSServiceRoleForClientVPN para chamar as seguintes ações em seu nome quando você trabalha com endpoints do cliente VPN:

- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeInternetGateways`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ds:AuthorizeApplication`
- `ds:DescribeDirectories`
- `ds:GetDirectoryLimits`
- `ds:ListAuthorizedApplications`
- `ds:UnauthorizeApplication`
- `lambda:GetFunctionConfiguration`
- `logs:DescribeLogStreams`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogGroups`
- `acm:GetCertificate`
- `acm:DescribeCertificate`

A função vinculada ao serviço AWSServiceRoleForClientVPN confia no principal clientvpn.amazonaws.com para assumir a função.

Se você usar o manipulador de conexão do cliente para seu endpoint do cliente VPN, o cliente VPN usará uma função vinculada ao serviço chamada AWSServiceRoleForClientVPNConnections. Essa função obtém permissões da política ClientVPNServiceConnectionsRolePolicy que permite que o cliente VPN invoque funções Lambda para você. A política permite a ação `lambda:InvokeFunction` somente nas funções Lambda com o prefixo `AWSClientVPN-`. Para obter mais informações, consulte . Autorização de conexão (p. 14).

Criação de funções vinculadas a serviços para o Client VPN

Você não precisa criar manualmente as funções AWSServiceRoleForClientVPN ou AWSServiceRoleForClientVPNConnections. O Client VPN cria as funções para você ao criar o primeiro endpoint do Client VPN em sua conta.

Para o Client VPN criar funções vinculadas ao serviço em seu nome, é necessário ter as permissões necessárias. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Editar uma função vinculada ao serviço para o Client VPN

Você não pode editar as funções vinculadas ao serviço AWSServiceRoleForClientVPN ou AWSServiceRoleForClientVPNConnections.

Exclusão de uma função vinculada ao serviço para o Client VPN

Se você não precisar mais usar o Client VPN, recomendamos que você exclua as funções vinculadas ao serviço AWSServiceRoleForClientVPN e AWSServiceRoleForClientVPNConnections.

Você deve primeiro excluir os recursos do Client VPN relacionados. Isso garante que você não remova por engano a permissão para acessar os recursos.

Use o console, a CLI ou a API do IAM para excluir funções vinculadas ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Registro em log e monitoramento

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do endpoint do Client VPN. Você deve coletar dados de monitoramento de todas as partes de sua solução para que possa depurar uma falha de vários pontos com mais facilidade caso ela ocorra. O AWS fornece várias ferramentas para monitorar seus recursos e responder a incidentes em potencial:

Amazon CloudWatch

O Amazon CloudWatch monitora os recursos da AWS e as aplicações que você executa na AWS em tempo real. Você pode coletar e rastrear métricas para seu endpoint do Client VPN. Para obter mais informações, consulte Monitorar o com o Amazon CloudWatch (p. 74).

AWS CloudTrail

O AWS CloudTrail captura chamadas de API do Amazon EC2 e eventos relacionados realizados por sua conta da AWS ou em nome dela. Desse modo, ele fornece os arquivos de log para um bucket do Amazon S3 especificado por você. Para obter mais informações, consulte Monitorar com o AWS CloudTrail (p. 76).

Amazon CloudWatch Logs

Você pode ver os logs de conexão para obter informações sobre os eventos de conexão, que ocorrem quando os clientes se conectam, tentam se conectar ou se desconectam do seu endpoint do Client VPN. Para obter mais informações, consulte Registro em log de conexão (p. 20).

Resiliência no AWS Client VPN

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são

conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões da AWS e zonas de disponibilidade, consulte AWS Infraestrutura global.

Além da infraestrutura global da AWS, a AWS Client VPN oferece recursos para ajudar a oferecer suporte às suas necessidades de resiliência e backup de dados.

Várias redes de destino para alta disponibilidade

Associe uma rede de destino a um endpoint do Client VPN para permitir que os clientes estabeleçam sessões VPN. As redes de destino são sub-redes em sua VPC. Cada sub-rede que você associa ao endpoint do Client VPN deve pertencer a uma zona de disponibilidade diferente. Você pode associar várias sub-redes a um endpoint Client VPN para alta disponibilidade.

Segurança da infraestrutura no AWS Client VPN

Como serviço gerenciado, o AWS Client VPN é protegido pelos procedimentos de segurança da rede global da AWS que estão descritos no whitepaper Amazon Web Services: visão geral dos processos de segurança.

Use as chamadas de API publicadas pela AWS para acessar o cliente VPN por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas Recomendadas de segurança para AWS Client VPN

O AWS Client VPN oferece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

Regras de autorização

Use regras de autorização para restringir quais usuários podem acessar sua rede. Para obter mais informações, consulte Regras de autorização (p. 43).

Grupos de segurança

Use grupos de segurança para controlar quais recursos os usuários podem acessar em sua VPC. Para obter mais informações, consulte Grupos de segurança (p. 14).

Listas de revogação de certificados de cliente

Use listas de revogação de certificados de cliente para revogar o acesso a um endpoint do Client VPN para certificados de cliente específicos. Por exemplo, quando um usuário sai da sua organização. Para obter mais informações, consulte Listas de revogação de certificados de cliente (p. 45).

Ferramentas de monitoramento

Use ferramentas de monitoramento para controlar a disponibilidade e o desempenho de seus endpoints do Client VPN. Para obter mais informações, consulte Monitorar o Client VPN (p. 74).

Identity and Access Management

Gerencie o acesso aos recursos e APIs do Client VPN usando políticas do IAM para seus usuários e funções do IAM. Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Client VPN (p. 67).

Considerações sobre IPv6

Atualmente, o serviço cliente VPN não é compatível com o roteamento de tráfego IPv6 pelo túnel VPN. No entanto, há casos em que o tráfego IPv6 deve ser roteado para o túnel VPN a fim de evitar vazamento de IPv6. O vazamento de IPv6 pode ocorrer quando o IPv4 e o IPv6 estão habilitados e conectados à VPN, mas a VPN não roteia o tráfego IPv6 para o túnel respectivo. Nesse caso, ao se conectar a um destino habilitado para IPv6, você ainda está se conectando com seu endereço IPv6 fornecido pelo ISP. Isso causará o vazamento do seu endereço IPv6 real. As instruções abaixo explicam como rotear o tráfego IPv6 para o túnel VPN.

As seguintes diretivas relacionadas ao IPv6 devem ser adicionadas ao arquivo de configuração do cliente VPN a fim de evitar vazamento de IPv6:

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

Um exemplo pode ser:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

Nesse exemplo,`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` definirá o endereço IPv6 do dispositivo de túnel local como `fd15:53b6:dead::2` e o endereço IPv6 do endpoint da VPN remota como `fd15:53b6:dead::1`.

O próximo comando, `route-ipv6 2000::/4`, roteará os endereços IPv6 de `2000:0000:0000:0000:0000:0000:0000:0000`para `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` na conexão VPN.

> **Note**
>
> Para o roteamento do dispositivo “TAP” no Windows, por exemplo, o segundo parâmetro de `ifconfig-ipv6` será usado como destino de rota para `--route-ipv6`.

As próprias organizações devem configurar os dois parâmetros de `ifconfig-ipv6` e podem usar endereços em `100::/64` (de`0100:0000:0000:0000:0000:0000:0000:0000` a `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) ou `fc00::/7` (de `fc00:0000:0000:0000:0000:0000:0000:0000` a `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` é um bloco de endereços somente para descarte e `fc00::/7` é exclusivo no local.

Outro exemplo:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

Neste exemplo, a configuração roteará todo o tráfego IPv6 alocado atualmente para a conexão VPN.

Verification

Provavelmente, sua organização terá os próprios testes. Uma verificação básica é configurar uma conexão VPN de túnel completo e, em seguida, executar ping6 para um servidor IPv6 usando o endereço IPv6. O endereço IPv6 do servidor deve estar no intervalo especificado pelo comando `route-ipv6`. Esse teste de ping deve falhar. No entanto, isso pode mudar se o suporte para IPv6 for adicionado ao serviço cliente VPN no futuro. Se o ping for bem-sucedido e você conseguir acessar sites públicos quando conectado no modo de túnel completo, talvez seja necessário fazer mais uma solução de problemas. Você também pode testar usando algumas ferramentas disponíveis publicamente, como ipleak.org.

Monitorar o Client VPN

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e da performance da VPN do Cliente AWS e de outras soluções da AWS. Você pode usar os recursos a seguir para monitorar seus endpoints de Client VPN, analisar padrões de tráfego e solucionar problemas com os endpoints de Client VPN.

Amazon CloudWatch

Monitora seus recursos da AWS e os aplicativos que você executa na AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode fazer o CloudWatch acompanhar o uso da CPU ou outras métricas das instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

AWS CloudTrail

Captura chamadas de API e eventos relacionados feitos por/em nome da sua conta AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Amazon CloudWatch Logs

Permite monitorar as tentativas de conexão feitas a seu endpoint AWS Client VPN. Você pode exibir as tentativas de conexão e as redefinições de conexão para as conexões do Client VPN. Você pode ver as tentativas de conexão bem-sucedidas e com falha. Você pode especificar o fluxo de log do CloudWatch Logs para registrar os detalhes da conexão em log. Para obter mais informações, consulte Registro em log de conexão (p. 20) e o Guia do usuário do Amazon CloudWatch Logs.

Monitorar o com o Amazon CloudWatch

A VPN do Cliente AWS publica as seguintes métricas do Amazon CloudWatch para os endpoints de VPN do Cliente. As métricas são publicadas no Amazon CloudWatch a cada cinco minutos.

Métrica	Descrição
ActiveConnectionsCount	O número de conexões ativas ao endpoint do Client VPN. Unidade: contagem
AuthenticationFailures	O número de falhas de autenticação para o endpoint do Client VPN. Unidade: contagem
CrlDaysToExpiry	O número de dias até a Lista de revogação de certificados (CRL) configurada no endpoint do Client VPN expirar. Unidades: dias
EgressBytes	Número de bytes enviados do endpoint do Client VPN.

Métrica	Descrição
	Unidade: bytes
EgressPackets	Número de pacotes enviados do endpoint do Client VPN. Unidade: contagem
IngressBytes	O número de bytes recebidos pelo endpoint do Client VPN. Unidade: bytes
IngressPackets	O número de pacotes recebidos pelo endpoint do Client VPN. Unidade: contagem
SelfServicePortalClientConfigurationDownloads	O número de downloads do arquivo de configuração do endpoint do Client VPN do portal de autoatendimento. Unidade: contagem

A VPN do Cliente AWS publica as seguintes métricas de avaliação da postura (p. 17) para os endpoints da sua VPN de Cliente.

Métrica	Descrição
ClientConnectHandlerTimeouts	O número de tempos limite ao chamar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidade: contagem
ClientConnectHandlerInvalidResponses	O número de respostas inválidas devolvidas pelo gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidade: contagem
ClientConnectHandlerOtherExecutionErrors	O número de erros inesperados ao executar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidade: contagem
ClientConnectHandlerThrottlingErrors	O número de erros de controle de utilização ao chamar o gerenciador de conexão do cliente para conexões com o endpoint do Client VPN. Unidade: contagem
ClientConnectHandlerDeniedConnections	O número de conexões negadas pelo gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidade: contagem

Métrica	Descrição
ClientConnectHandlerFailedServiceErrors	O número de erros colaterais no serviço ao executar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidade: contagem

Você pode filtrar as métricas de seu endpoint do Client VPN por endpoint.

O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um alarme do CloudWatch para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair do que você considera um intervalo aceitável.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Visualizar métricas do CloudWatch do

Você pode ver as métricas do endpoint da sua VPN de Cliente da maneira a seguir.

Para exibir métricas usando o console do CloudWatch

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace.

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Em All metrics (Todas as métricas), escolha o namespace da métrica ClientVPN (VPN do Cliente).
4. Para visualizar as métricas, selecione a dimensão da métrica by endpoint (por endpoint).

Para visualizar métricas usando o AWS CLI

Em um prompt de comando, use o comando a seguir para listar as métricas que estão disponíveis para a VPN do Cliente.

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

Monitorar com o AWS CloudTrail

A VPN do Cliente AWS é integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço AWS na VPN do Cliente. O CloudTrail captura todas as chamadas de API para o Client VPN como eventos. As chamadas capturadas incluem as chamadas do console do Client VPN e as chamadas de código para as operações de API do Client VPN. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Client VPN. Se você não configurar uma trilha, ainda poderá visualizar os eventos

mais recentes no console do CloudTrail em Event history (Histórico de eventos). Use as informações coletadas pelo CloudTrail para determinar a solicitação feita para o Client VPN, o endereço IP dessa solicitação, o solicitante, quando ela foi feita e outros detalhes adicionais.

Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações de Client VPN no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre atividade na VPN do Cliente, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar os eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro de eventos em andamento na sua conta AWS, incluindo eventos da VPN do Cliente, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configuração de notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações de Client VPN são registradas pelo CloudTrail e estão documentadas na Referência da API do Amazon EC2. Por exemplo, as chamadas para as APIs `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` e `AuthorizeClientVpnIngress` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do Client VPN

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Para obter mais informações, consulte Registrar chamadas de API do Amazon EC2, Amazon EBS e Amazon VPC com AWS CloudTrail na referência de API do Amazon EC2.

Cotas do cliente VPN da AWS

Sua conta da AWS tem as seguintes cotas padrão, anteriormente chamadas de limites, relacionadas a endpoints do cliente VPN. A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para solicitar o aumento da cota para uma cota ajustável, selecione Yes (Sim) na coluna Adjustable (Ajustável). Para obter mais informações, consulte Solicitar um aumento da cota no Guia do usuário do Service Quotas.

Cotas do Client VPN

Nome	Padrão	Ajustável
Regras de autorização por endpoint do cliente VPN	50	Sim
Endpoints do cliente VPN por região	5	Sim
Conexões de cliente simultâneas por endpoint de cliente VPN	Esse valor depende do número de associações de sub-rede por endpoint. • 1 a 7.000 • 2 a 36.500 • 3 a 66.500 • 4 a 96.500 • 5 a 126.000	Sim
Operações simultâneas por endpoint do cliente VPN †	10	Não
Entradas em uma lista de revogação de certificados de cliente para endpoints do cliente VPN	20.000	Não
Rotas por endpoint do cliente VPN	10	Sim

† As operações incluem:

- Associar ou desassociar sub-redes
- Criar ou excluir rotas
- Criar ou excluir regras de entrada e de saída
- Criar ou excluir grupos de segurança

Cotas de usuários e grupos

Ao configurar usuários e grupos para o Active Directory ou para um IdP baseado em SAML, as seguintes cotas se aplicam:

- Os usuários podem pertencer a, no máximo, 200 grupos. Todos os grupos após o 200º grupo são ignorados.
- O tamanho máximo do ID do grupo é 255 caracteres.
- O tamanho máximo do ID do nome é 255 caracteres. Os caracteres após o 255º caractere são truncados.

Considerações gerais

Leve o seguinte em consideração ao usar endpoints do Client VPN:

- Se você usar o Active Directory para autenticar o usuário, o endpoint do cliente VPN deverá pertencer à mesma conta que o recurso do AWS Directory Service usado para autenticação do Active Directory.
- Se você usar a autenticação federada baseada em SAML para autenticar um usuário, o endpoint do cliente VPN deverá pertencer à mesma conta que o provedor de identidade SAML do IAM criado para definir a relação de confiança entre o IdP e a AWS. O provedor de identidade SAML do IAM pode ser compartilhado entre vários endpoints do cliente VPN na mesma conta da AWS.

Solução de problemas do Client VPN

O tópico a seguir pode ajudar a solucionar problemas que possam surgir com um endpoint do Client VPN.

Para obter mais informações sobre a solução de problemas de software baseado em OpenVPN que os clientes usam para se conectar a um cliente VPN, consulte Solução de problemas de conexão do cliente VPN no Guia do usuário do AWS Client VPN.

Problemas comuns

Não é possível resolver o nome DNS do endpoint do Client VPN.

Problem

Não consigo resolver o nome DNS do endpoint do Client VPN.

Cause

O arquivo de configuração do endpoint do Client VPN inclui um parâmetro chamado `remote-random-hostname`. Esse parâmetro força o cliente a preceder o nome DNS com uma string aleatória para impedir o armazenamento em cache de DNS. Alguns clientes não reconhecem esse parâmetro e, portanto, não precedem o nome DNS com a string aleatória necessária.

Solution

Abra o arquivo de configuração do endpoint do Client VPN usando seu editor de texto preferido. Localize a linha que especifica o nome DNS do endpoint da cliente VPN e adicione uma string aleatória ao início dela para que o formato seja *`string_aleatória.nome_DNS_exibido`*. Por exemplo:

- Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

O tráfego não está sendo dividido entre as sub-redes

Problem

Estou tentando dividir o tráfego de rede entre duas sub-redes. O tráfego privado deve ser roteado por uma sub-rede privada, enquanto o tráfego da Internet deve ser roteado por uma sub-rede pública. No entanto, somente uma rota está sendo usada, embora eu tenha adicionado ambas as rotas à tabela de rotas do endpoint do Client VPN.

Cause

É possível associar várias sub-redes a um endpoint do Client VPN, mas somente uma sub-rede por zona de disponibilidade. O objetivo da associação de várias sub-redes é fornecer alta disponibilidade e redundância de zona de disponibilidade para os clientes. No entanto, o Client VPN não permite dividir o tráfego seletivamente entre as sub-redes associadas ao endpoint do Client VPN.

Os clientes se conectam a um endpoint do Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

Por exemplo, digamos que você configure as seguintes associações de sub-rede e rotas:

- Associações de sub-rede
  - Associação 1: sub-rede A (us-east-1a)
  - Associação 2: sub-rede B (us-east-1b)
- Rotas
  - Rota 1:10.0.0.0/16 roteada para a sub-rede A
  - Rota 2:172.31.0.0/16 roteada para a sub-rede B

Neste exemplo, os clientes que entrarem na sub-rede A quando se conectarem não poderão acessar a Rota 2, enquanto os clientes que aterrissarem na sub-rede B quando se conectarem não poderão acessar a Rota 1.

Solution

Verifique se o endpoint do Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede pela qual seu tráfego seja roteado.

Regras de autorização para grupos do Active Directory não funcionando conforme esperado

Problem

Configurei regras de autorização para meus grupos do Active Directory, mas elas não estão funcionando como eu esperava. Adicionei uma regra de autorização para `0.0.0.0/0` para autorizar o tráfego para todas as redes, mas ainda há falha no tráfego para CIDRs de destino específicos.

Cause

As regras de autorização são indexadas em CIDRs de rede. As regras de autorização devem conceder aos grupos do Active Directory acesso a CIDRs de rede específicos. As regras de autorização para `0.0.0.0/0` são tratadas como um caso especial e, portanto, são avaliadas por último, independentemente da ordem na qual as regras de autorização são criadas.

Por exemplo, digamos que você crie cinco regras de autorização na seguinte ordem:

- Regra 1: acesso do grupo 1 a `10.1.0.0/16`
- Regra 2: acesso do grupo 1 a `0.0.0.0/0`
- Regra 3: acesso do grupo 2 a `0.0.0.0/0`
- Regra 4: acesso do grupo 3 a `0.0.0.0/0`
- Regra 5: acesso do grupo 2 a `172.131.0.0/16`

Neste exemplo, a regra 2, a regra 3 e a regra 4 são avaliadas por último. O grupo 1 tem acesso somente a `10.1.0.0/16`, e o grupo 2 tem acesso somente a `172.131.0.0/16`. O grupo 3 não tem acesso a `10.1.0.0/16` ou a `172.131.0.0/16`, mas tem acesso a todas as outras redes. Se você remover as regras 1 e 5, todos os três grupos terão acesso a todas as redes.

O cliente VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização. Consulte Prioridade de rota no Guia do usuário do Amazon VPC para obter mais detalhes.

Solution

Verifique se as regras de autorização criadas concedem explicitamente aos grupos do Active Directory acesso a CIDRs de rede específicos. Se você adicionar uma regra de autorização para `0.0.0.0/0`, tenha em mente que ela será avaliada por último e que as regras de autorização anteriores podem limitar as redes às quais ela concede acesso.

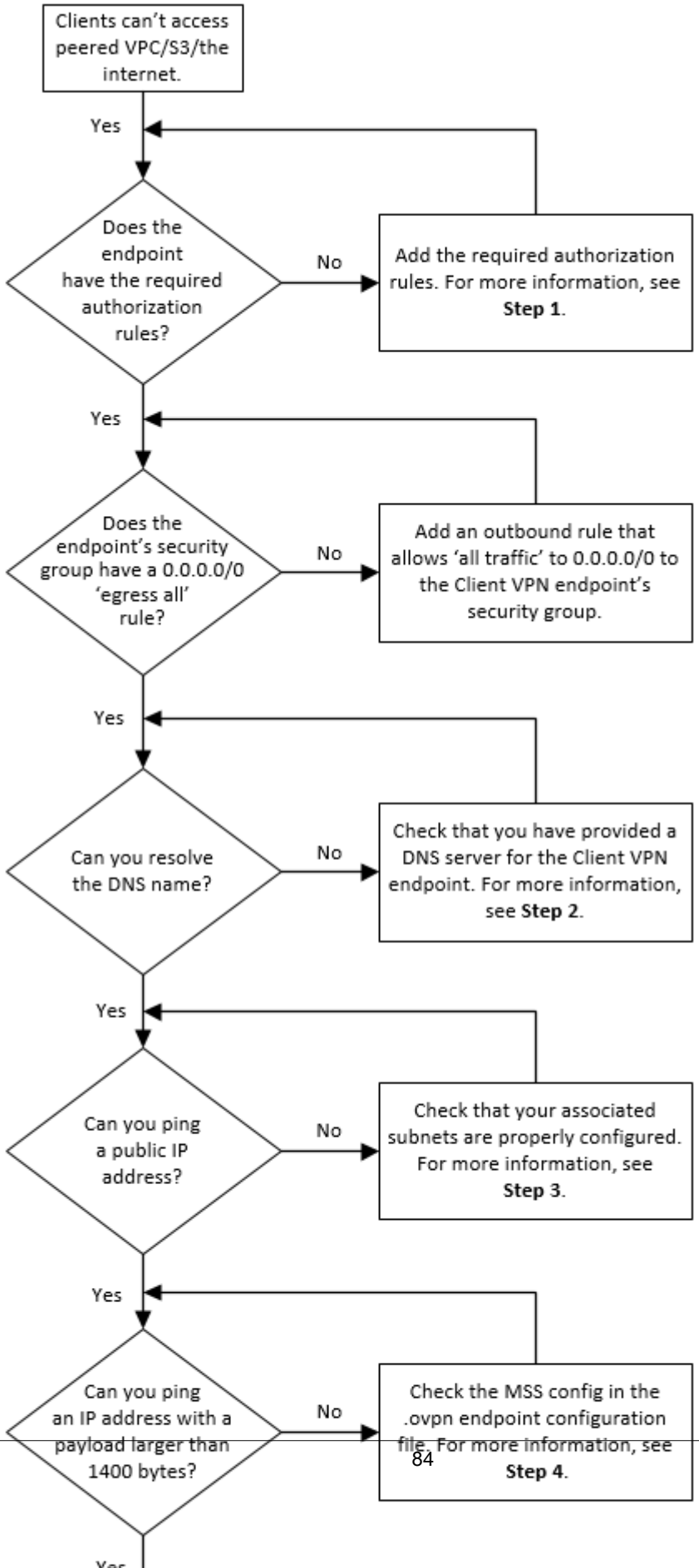
Os clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet

Problem

Configurei corretamente minhas rotas do endpoint do Client VPN, mas meus clientes não conseguem acessar uma VPC emparelhada, o Amazon S3 ou a Internet.

Solution

O fluxograma a seguir contém as etapas para diagnosticar problemas de conectividade da Internet, da VPC emparelhada e do Amazon S3.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Para acesso à Internet, adicione uma regra de autorização para `0.0.0.0/0`.

   Para acesso a uma VPC emparelhada, adicione uma regra de autorização para o intervalo CIDR IPv4 da VPC.

   Para acesso ao S3, especifique o endereço IP do endpoint do Amazon S3.
2. Verifique se é possível resolver o nome DNS.

   Se não for possível resolver o nome DNS, verifique se você especificou os servidores DNS para o endpoint do Client VPN. Se você gerenciar seu próprio servidor DNS, especifique seu endereço IP. Verifique se o servidor DNS é acessível pela VPC.

   Se você não tiver certeza sobre qual endereço IP especificar para os servidores DNS, especifique o resolvedor DNS da VPC no endereço IP .2 na VPC.
3. Para ter acesso à Internet, verifique se você consegue executar ping em um endereço IP público ou em um site público, por exemplo, `amazon.com`. Se não receber uma resposta, certifique-se de que a tabela de rotas para as sub-redes associadas tenha uma rota padrão que tenha como destino um gateway da Internet ou um gateway NAT. Se a rota estiver em vigor, certifique-se de que a sub-rede associada não tenha regras de lista de controle de acesso à rede que bloqueiem o tráfego de entrada e saída.

   Se você não conseguir acessar uma VPC emparelhada, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para a VPC emparelhada.

   Se não conseguir acessar o Amazon S3, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para o VPC endpoint do gateway.
4. Verifique se é possível executar ping em um endereço IP público com uma carga maior que 1400 bytes. Use um dos seguintes comandos:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

   Se não for possível executar ping em um endereço IP com uma carga útil maior que 1400 bytes, abra o arquivo de configuração `.ovpn` do endpoint do Client VPN usando seu editor de texto preferido e adicione o seguinte.

   ```
   mssfix 1328
   ```

O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente

Problem

Tenho problemas de conectividade intermitentes ao me conectar a uma VPC emparelhada, ao Amazon S3 ou à Internet, mas o acesso a sub-redes associadas não foi afetado. Preciso me desconectar e reconectar para resolver os problemas de conectividade.

Cause

Os clientes se conectam a um endpoint do Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

Solution

Verifique se o endpoint do Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede associada pela qual o tráfego é roteado.

Por exemplo, digamos que o endpoint do Client VPN tenha três sub-redes associadas (sub-rede A, B e C) e que você queira habilitar o acesso à Internet para seus clientes. Para fazer isso, adicione três rotas `0.0.0.0/0` – uma que tenha como destino cada sub-rede associada:

- Rota 1: `0.0.0.0/0` para a sub-rede A
- Rota 2: `0.0.0.0/0` para a sub-rede B
- Rota 3: `0.0.0.0/0` para a sub-rede C

O software cliente retorna erro TLS

Problem

Antes eu podia conectar meus clientes ao Client VPN com êxito, mas agora o cliente baseado em OpenVPN-retorna o seguinte erro quando ele tenta se conectar:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

Possíveis causas

Se você usa autenticação mútua e importou uma lista de revogação de certificados de cliente, a lista de revogação de certificados de cliente pode ter expirado. Durante a fase de autenticação, o endpoint do Client VPN verifica o certificado de cliente em relação à lista de revogação de certificados de cliente importada. Se a lista de revogação de certificados de cliente tiver expirado, não será possível conectar-se ao endpoint do Client VPN.

Como alternativa, pode haver um problema com o software baseado em OpenVPN que o cliente está usando para se conectar ao Client VPN.

Solution

Verifique a data de expiração da lista de revogação de certificados do cliente usando a ferramenta OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

A saída exibe a data e a hora de expiração. Se a lista de revogação de certificados do cliente tiver expirado, você deverá criar uma nova e importá-la para o endpoint do Client VPN. Para obter mais informações, consulte . Listas de revogação de certificados de cliente (p. 45).

Para obter mais informações sobre a solução de problemas de software baseado em OpenVPN, consulte Solução de problemas de conexão do cliente VPN no Guia do usuário do AWS Client VPN.

O software cliente retorna erros de nome de usuário e senha (autenticação do Active Directory)

Problem

Uso a autenticação do Active Directory para meu endpoint do Client VPN e antes podia conectar meus clientes ao Client VPN com êxito. Mas agora, os clientes estão recebendo erros de nome de usuário e senha inválidos.

Possíveis causas

Se usar a autenticação do Active Directory e se tiver habilitado a autenticação multifator (MFA) depois de distribuir o arquivo de configuração do cliente, o arquivo não conterá as informações necessárias para pedir aos usuários que insiram o código da MFA. Os usuários são solicitados a inserir o nome de usuário e a senha, mas há falha na autenticação.

Solution

Baixe um novo arquivo de configuração do cliente e distribua-o para seus clientes. Verifique se o novo arquivo contém a seguinte linha:

```
static-challenge "Enter MFA code " 1
```

Para obter mais informações, consulte . Exportar e configurar o arquivo de configuração do cliente (p. 58). Teste a configuração de MFA para o Active Directory sem usar o endpoint do Client VPN para verificar se a MFA está funcionando conforme o esperado.

Clientes não conseguem se conectar (autenticação mútua)

Problem

Uso autenticação mútua para o meu endpoint do Client VPN. Os clientes estão recebendo erros de falha na negociação de chave TLS e erros de tempo limite.

Possíveis causas

O arquivo de configuração que foi fornecido aos clientes não contém o certificado do cliente e a chave privada do cliente ou o certificado e a chave estão incorretos.

Solution

Certifique-se de que o arquivo de configuração contenha o certificado e a chave do cliente corretos. Se necessário, corrija o arquivo de configuração e redistribua-o para seus clientes. Para obter mais informações, consulte . Exportar e configurar o arquivo de configuração do cliente (p. 58).

O cliente retorna um erro de tamanho máximo de credenciais excedido (autenticação federada)

Problem

Uso autenticação federada para meu endpoint do Client VPN. Quando os clientes inserem o nome de usuário e a senha na janela do navegador do provedor de identidade (IdP) baseado em SAML, eles recebem um erro informando que as credenciais excedem o tamanho máximo permitido.

Cause

A resposta SAML retornada pelo IdP excede o tamanho máximo permitido. Para obter mais informações, consulte . Requisitos e considerações para autenticação federada baseada em SAML (p. 12).

Solution

Tente reduzir o número de grupos aos quais o usuário pertence no IdP e tente se conectar novamente.

O cliente não abre o navegador (autenticação federada)

Problem

Uso autenticação federada para meu endpoint do Client VPN. Quando os clientes tentam se conectar ao endpoint, o software cliente não abre uma janela do navegador e, em vez disso, exibe uma janela pop-up de nome de usuário e senha.

Cause

O arquivo de configuração fornecido aos clientes não contém o sinalizador `auth-federate`.

Solution

Exporte o arquivo de configuração mais recente (p. 58), importe-o para o cliente fornecido pela AWS e tente se conectar novamente.

O cliente não retorna nenhum erro de portas disponíveis (autenticação federada)

Problem

Uso autenticação federada para meu endpoint do Client VPN. Quando os clientes tentam se conectar ao endpoint, o software cliente retorna o seguinte erro:

```
The authentication flow could not be initiated. There are no available ports.
```

Cause

O cliente fornecido pela AWS requer o uso da porta TCP 35001 para concluir a autenticação. Para obter mais informações, consulte . Requisitos e considerações para autenticação federada baseada em SAML (p. 12).

Solution

Verifique se o dispositivo do cliente não está bloqueando a porta TCP 35001 ou a está usando para um processo diferente.

Verificar o limite de largura de banda para um endpoint do Client VPN

Problem

Preciso verificar o limite de largura de banda para um endpoint do Client VPN.

Cause

A taxa de transferência depende de vários fatores, como a capacidade da conexão do local e a latência da rede entre o aplicativo para desktop de Client VPN no computador e o VPC endpoint.

Solution

Execute os comandos a seguir para verificar a largura de banda.

```
sudo iperf3 -s -V
```

No cliente:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Histórico do documento

A tabela a seguir descreve as atualizações do Guia do administrador do cliente VPN da AWS.

update-history-change	update-history-description	update-history-date
Duração máxima da sessão VPN	É possível configurar uma duração máxima de sessão VPN menor para atender aos requisitos de segurança e conformidade.	20 de janeiro de 2022
Banner de login do cliente	É possível habilitar um banner de texto em aplicações de desktop do cliente VPN fornecidas pela AWS quando uma sessão VPN é estabelecida para atender às necessidades regulamentares e de conformidade.	20 de janeiro de 2022
Manipulador de conexão do cliente	Você pode habilitar o manipulador de conexão do cliente para seu endpoint do Client VPN para executar uma lógica personalizada que autoriza novas conexões.	4 de novembro de 2020
Portal de autoatendimento	Você pode habilitar um portal de autoatendimento em seu endpoint do Client VPN para seus clientes.	29 de outubro de 2020
Acesso cliente a cliente	Você pode permitir que clientes que se conectam a um endpoint do Client VPN se conectem entre si.	29 de setembro de 2020
Autenticação federada baseada em SAML	Você pode autenticar usuários do Client VPN usando a autenticação federada baseada em SAML 2.0.	19 de maio de 2020
Especificar grupos de segurança durante a criação	É possível especificar uma VPC e grupos de segurança ao criar seu endpoint do cliente VPN da AWS.	5 de março de 2020
Portas VPN configuráveis	Você pode especificar um número de porta VPN com suporte para seu endpoint do cliente VPN da AWS.	16 de janeiro de 2020
Suporte à autenticação multifator (MFA)	Seu endpoint do cliente VPN da AWS será compatível com MFA se estiver habilitado para o Active Directory.	30 de setembro de 2019

Suporte a túnel dividido	Você pode habilitar o túnel dividido no endpoint do cliente VPN da AWS.	24 de julho de 2019
Versão inicial (p. 90)	Esta versão apresenta a VPM do cliente da AWS.	18 de dezembro de 2018