Guia do administrador

AWS Client VPN

AWS Client VPN: Guia do administrador

Table of Contents

O que AWS Client VPNé

AWS Client VPN é um VPN serviço gerenciado baseado em cliente que permite acessar com segurança seus AWS recursos e recursos em sua rede local. Com o ClientVPN, você pode acessar seus recursos de qualquer local usando um VPN cliente VPN baseado em Open.

Tópicos

Características do cliente VPN

O cliente VPN oferece os seguintes recursos e funcionalidades:

- Conexões seguras — Ele fornece uma TLS conexão segura de qualquer local usando o VPN cliente Open.
- Serviço gerenciado — É um serviço AWS gerenciado, portanto, elimina a carga operacional de implantar e gerenciar uma VPN solução de acesso remoto de terceiros.
- Alta disponibilidade e elasticidade — Ele é escalado automaticamente de acordo com o número de usuários conectados aos seus AWS recursos e aos recursos locais.
- 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 — Ele permite que você acesse seus AWS recursos e recursos locais usando um único VPN túnel.

- 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 — Ele se integra aos AWS serviços existentes, incluindo AWS Directory Service a AmazonVPC.

Componentes do cliente VPN

A seguir estão os principais conceitos para o ClienteVPN:

VPNEndpoint do cliente

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

Rede de destino

Uma rede de destino é a rede que você associa a um VPN endpoint do cliente. Uma sub-rede de a VPC é uma rede de destino. Associar uma sub-rede a um VPN endpoint do cliente permite que você estabeleça sessões. VPN Você pode associar várias sub-redes a um VPN endpoint do cliente para obter alta disponibilidade. Todas as sub-redes devem ser da mesma. VPC Cada sub-rede deve pertencer a uma Zona de disponibilidade diferente.

Rota

Cada VPN endpoint do cliente tem uma tabela de rotas que descreve as rotas de rede 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 se conectando ao VPN endpoint do cliente para estabelecer uma VPN sessão. Os usuários finais precisam baixar um VPN cliente aberto e usar o arquivo de VPN configuração do cliente que você criou para estabelecer uma VPN sessão.

CIDRGama de clientes

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

VPNPortas do cliente

AWS Client VPN suporta as portas 443 e 1194 para ambos e. TCP UDP O padrão é a porta 443.

Interfaces VPN de rede do cliente

Quando você associa uma sub-rede ao seu VPN endpoint do cliente, criamos interfaces de VPN rede do cliente nessa sub-rede. O tráfego enviado para o do VPN endpoint VPC do cliente é enviado por meio de uma interface de VPN rede do cliente. A tradução do endereço de rede de origem (SNAT) é então aplicada, em que o endereço IP de origem do CIDR intervalo de clientes é traduzido para o endereço IP da interface de VPN rede do cliente.

Registro em log de conexão

Você pode ativar o registro de conexão para o VPN endpoint do seu cliente para registrar eventos de conexão. Você pode usar essas informações para executar análises forenses, analisar como o VPN endpoint do seu cliente está sendo usado ou depurar problemas de conexão.

Portal de autoatendimento

VPNO cliente 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 VPN endpoint do cliente, que contém as configurações necessárias para se conectar ao endpoint. O administrador do VPN endpoint do cliente pode ativar ou desativar o portal de autoatendimento do endpoint do clienteVPN. O portal de autoatendimento é um serviço global apoiado por pilhas de serviços nas seguintes regiões: Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Tóquio), Europa (Irlanda) e AWS GovCloud (Oeste dos EUA).

Trabalhando com o cliente VPN

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

AWS Management Console

O console fornece uma interface de usuário baseada na web para o ClienteVPN. Se você se inscreveu em um Conta da AWS, você pode entrar no VPC console da Amazon e selecionar Cliente VPN no painel de navegação.

AWS Command Line Interface (AWS CLI)

AWS CLI Fornece acesso direto ao VPN público do ClienteAPIs. É compatível com Windows, macOS e Linux. Para obter mais informações sobre como começar a usar o AWS CLI, consulte o Guia AWS Command Line Interface do usuário. Para obter mais informações sobre os comandos do ClientVPN, consulte a Referência de AWS CLI Comandos.

AWS Tools for Windows PowerShell

AWS fornece comandos para um amplo conjunto de AWS ofertas para quem cria scripts no PowerShell ambiente. Para obter mais informações sobre os conceitos básicos da AWS Tools for Windows PowerShell, consulte o Guia do usuário do AWS Tools for Windows PowerShell. Para obter mais informações sobre os cmdlets para ClientVPN, consulte a Referência do AWS Tools for Windows PowerShell Cmdlet.

Consulta API

A VPN HTTPS Consulta do Cliente API fornece acesso programático ao Cliente VPN e. AWS A HTTPS consulta API permite que você HTTPS emita solicitações diretamente para o serviço. Ao usar o HTTPSAPI, você deve incluir um código para assinar digitalmente as solicitações usando suas credenciais. Para obter mais informações, consulte Ações do AWS Client VPN.

Preços para o cliente VPN

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

Você é cobrado pela transferência de dados da Amazon EC2 para a Internet. Para obter mais informações, consulte Transferência de dados na página de preços EC2 sob demanda da Amazon.

Se você ativar o registro de conexão para seu VPN endpoint do cliente, deverá criar um grupo de CloudWatch registros de registros em sua conta. Aplicam-se cobranças ao uso de grupos de log. Para obter mais informações, consulte os CloudWatch preços da Amazon (em Nível pago, escolha Logs).

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

Os VPN endpoints do cliente estão associados a uma rede de destino, que é uma sub-rede em um. VPC Se VPC ele tiver um Internet Gateway, associamos endereços IP elásticos às interfaces de rede VPN elástica do cliente (ENIs). Esses endereços IP elásticos são cobrados como IPv4 endereços públicos em uso. Para obter mais informações, consulte a guia IPv4 Endereço público na página VPC de preços.

Regras e melhores práticas de uso AWS Client VPN

A seguir estão as regras e as melhores práticas de uso AWS Client VPN

- Uma largura de banda mínima de 10 Mbps é suportada por conexão de usuário. A largura de banda máxima por conexão de usuário depende do número de conexões feitas com o VPN endpoint do cliente.
- Os CIDR intervalos CIDR de clientes não podem se sobrepor ao local VPC em que a sub-rede associada está localizada ou a nenhuma rota adicionada manualmente à tabela de rotas do VPN endpoint do cliente.
- Os CIDR intervalos de clientes devem ter um tamanho de bloco de pelo menos /22 e não devem ser maiores que /12.
- Uma parte dos endereços na CIDR faixa de clientes é usada para dar suporte ao modelo de disponibilidade do VPN endpoint do cliente e não pode ser atribuída aos clientes. Portanto, recomendamos que você atribua um CIDR bloco que contenha o dobro do número de endereços IP necessários para habilitar o número máximo de conexões simultâneas que você planeja oferecer suporte no VPN endpoint do Cliente.
- O CIDR intervalo de clientes não pode ser alterado após a criação do VPN endpoint do cliente.
- As sub-redes associadas a um VPN endpoint do cliente devem estar nas mesmas. VPC
- Você não pode associar várias sub-redes da mesma zona de disponibilidade a um endpoint do clienteVPN.
- Um VPN endpoint de cliente não oferece suporte a associações de sub-rede em uma locação dedicada. VPC
- O cliente VPN oferece suporte somente ao IPv4 tráfego. Consulte IPv6considerações para AWS Client VPN para obter detalhes sobreIPv6.

- VPNO cliente não está em conformidade com os Padrões Federais de Processamento de Informações (FIPS).
- O portal de autoatendimento não está disponível para clientes autenticados usando a autenticação mútua.
- Não recomendamos conectar-se a um VPN endpoint do cliente usando endereços IP. Como o Client VPN é um serviço gerenciado, você ocasionalmente verá alterações nos endereços IP para os quais o DNS nome é resolvido. Além disso, você verá as interfaces de VPN rede do cliente excluídas e recriadas em seus CloudTrail registros. Recomendamos conectar-se ao VPN endpoint do cliente usando o DNS nome fornecido.
- Atualmente, o encaminhamento de IP não é suportado ao usar o aplicativo AWS Client VPN de desktop. O encaminhamento de IP é compatível com outros clientes.
- VPNO cliente não oferece suporte à replicação multirregional em. AWS Managed Microsoft AD O VPN endpoint do cliente deve estar na mesma região do AWS Managed Microsoft AD recurso.
- Se a autenticação multifator (MFA) estiver desativada para o Active Directory, as senhas de usuário não poderão usar o formato a seguir.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Você não pode estabelecer uma VPN conexão a partir de um computador se houver vários usuários conectados ao sistema operacional.
- O VPN serviço do cliente exige que o endereço IP ao qual o cliente está conectado corresponda ao IP para o qual o DNS nome do VPN endpoint do cliente é resolvido. Em outras palavras, se você definir um DNS registro personalizado para o VPN endpoint do cliente e encaminhar o tráfego para o endereço IP real para o qual o DNS nome do endpoint é resolvido, essa configuração não funcionará usando clientes fornecidos recentemente AWS . Esta regra foi adicionada para mitigar um ataque de IP do servidor, conforme descrito aqui: TunnelCrack.
- O VPN serviço de cliente exige que os intervalos de endereços IP da rede local (LAN) dos dispositivos do cliente estejam dentro dos seguintes intervalos de endereços IP privados padrão:`10.0.0.0/8`,`172.16.0.0/12`,`192.168.0.0/16`, ou`169.254.0.0/16`. Se for detectado que o intervalo de LAN endereços do cliente está fora dos intervalos acima, o VPN endpoint do cliente enviará automaticamente a VPN diretiva Open “redirect-gateway block-local” para o cliente, forçando todo o tráfego para o. LAN VPN Portanto, se você precisar de LAN acesso durante VPN as conexões, é recomendável usar os intervalos de endereços convencionais listados acima para o seuLAN. Esta regra é aplicada para mitigar as chances de um ataque local na rede, conforme descrito aqui:. TunnelCrack

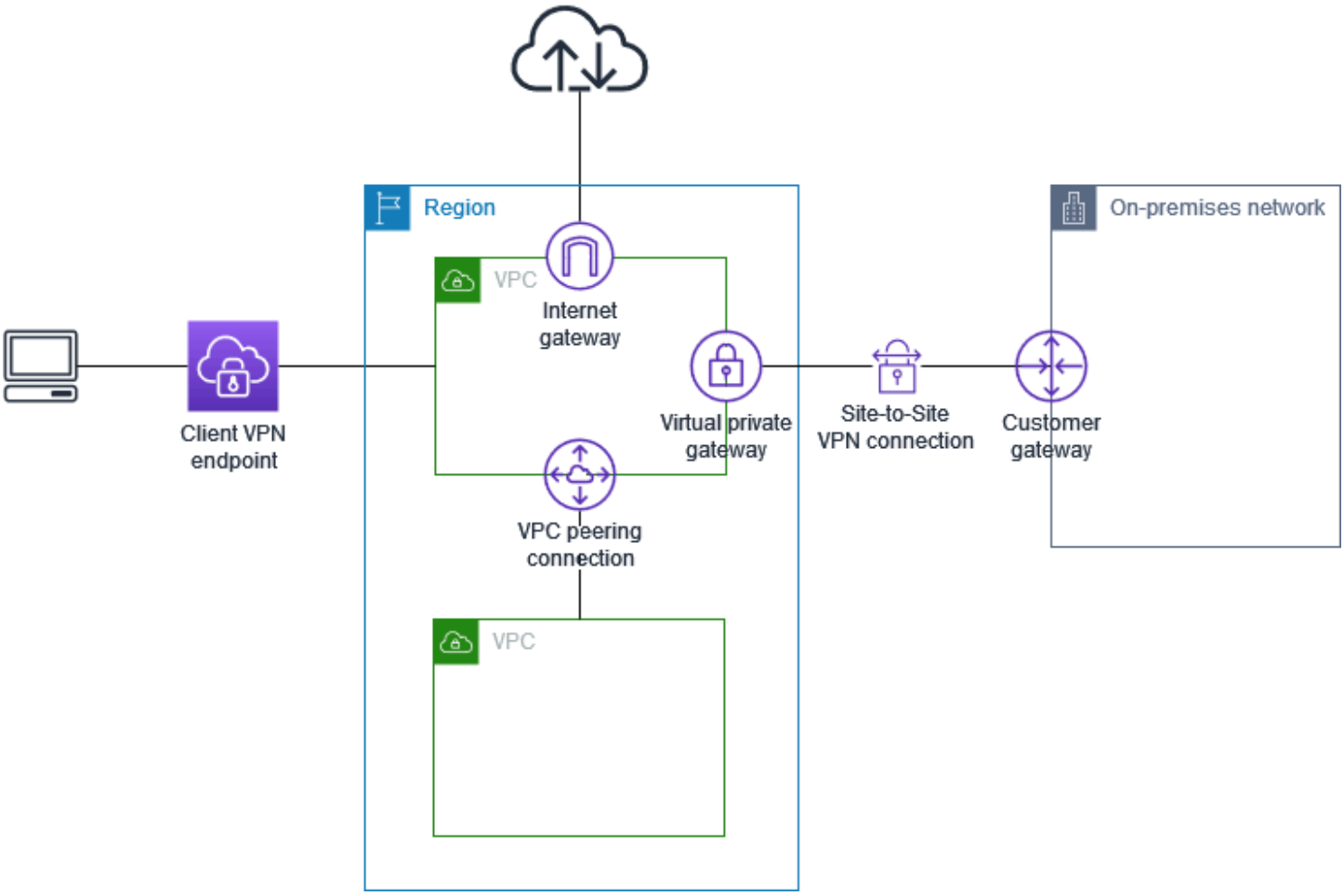
Como AWS Client VPN funciona

Com AWS Client VPN, existem dois tipos de personas de usuário que interagem com o VPN endpoint do cliente: administradores e clientes.

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

O cliente é o usuário final. Essa é a pessoa que se conecta ao VPN endpoint do cliente para estabelecer uma VPN sessão. O cliente estabelece a VPN sessão a partir de seu computador local ou dispositivo móvel usando um aplicativo VPN cliente VPN baseado em Open. Depois de estabelecerem a VPN sessão, eles podem acessar com segurança os recursos VPC nos quais a sub-rede associada está localizada. Eles também podem acessar outros recursos em AWS uma rede local ou em outros clientes se as regras de rota e autorização necessárias tiverem sido configuradas. Para obter mais informações sobre como se conectar a um VPN endpoint do cliente para estabelecer uma VPN sessão, consulte Introdução no Guia do AWS Client VPN usuário.

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



Cenários e exemplos para o cliente VPN

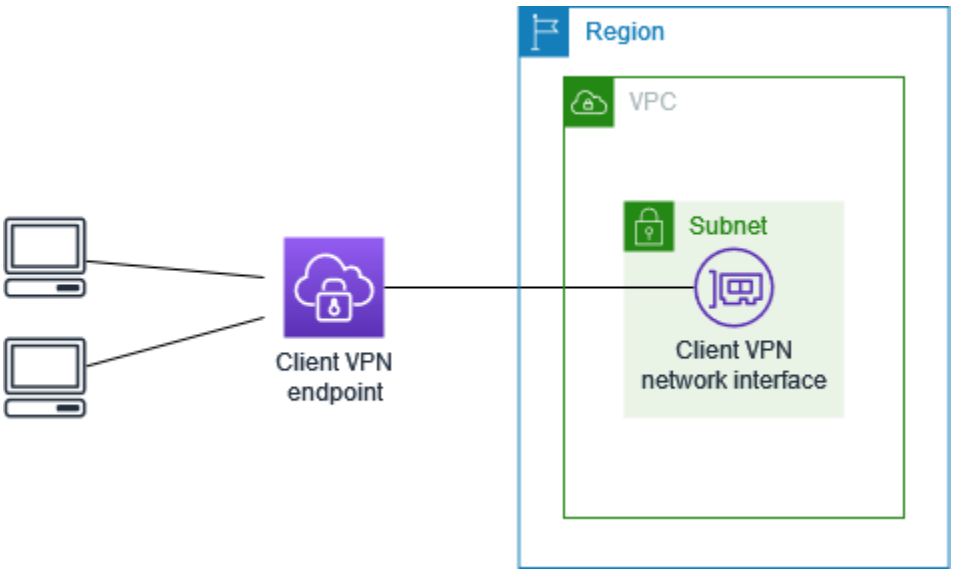
AWS Client VPN é uma VPN solução de acesso remoto totalmente gerenciada que você usa para permitir que os clientes tenham acesso seguro aos recursos tanto na rede local AWS quanto na sua. Há várias opções de como você configura o acesso. Esta seção fornece exemplos para criar e configurar o VPN acesso do cliente para seus clientes.

Cenários

- the section called “Acesse um VPC”
- the section called “Acesse um peering VPC”
- the section called “Acesso a uma rede on-premises”
- the section called “Acesso à Internet”
- the section called “lient-to-clientAcesso C”
- the section called “Restringir o acesso à sua rede”

Acesse um VPC cliente usuário VPN

A AWS Client VPN configuração desse cenário inclui um único alvoVPC. Recomendamos essa configuração se você precisar dar aos clientes acesso aos recursos em apenas um VPC único.



Antes de começar, faça o seguinte:

- Crie ou identifique um VPC com pelo menos uma sub-rede. Identifique a sub-rede na a VPC ser associada ao VPN endpoint do cliente e anote seus IPv4 CIDR intervalos.
- Identifique um CIDR intervalo adequado para os endereços IP do cliente que não se sobreponha ao VPCCIDR.
- Analise as regras e limitações dos VPN endpoints do cliente emRegras e melhores práticas de uso AWS Client VPN.

Para implementar essa configuração

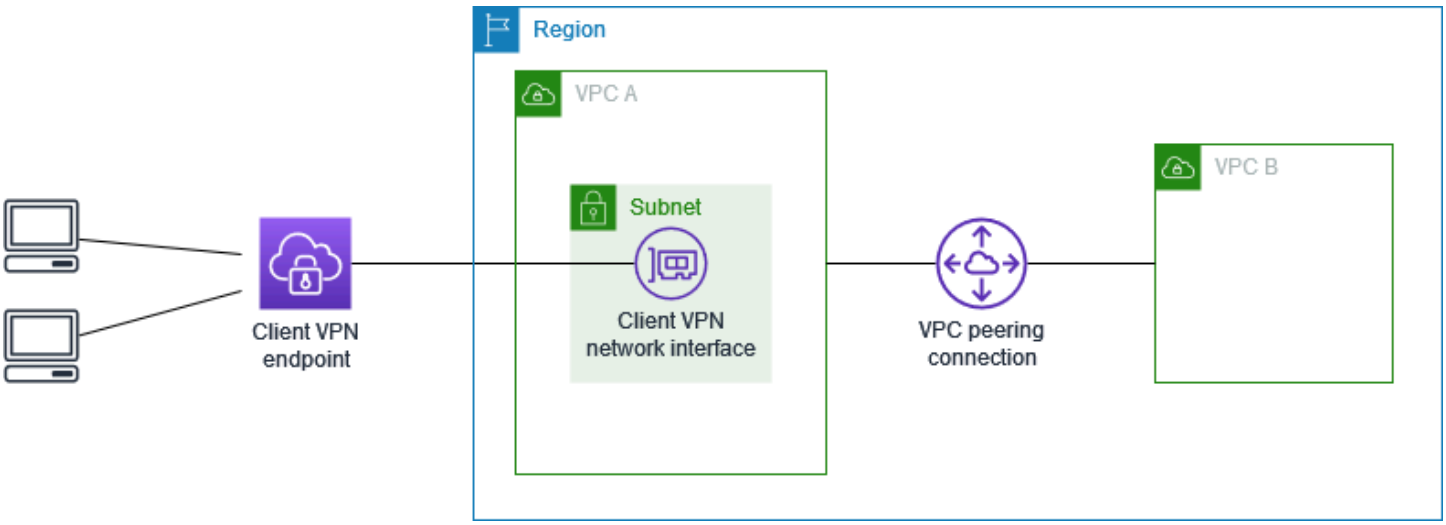
1. Crie um VPN endpoint de cliente na mesma região doVPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
2. Associe a sub-rede ao VPN endpoint do cliente. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um AWS Client VPN endpoint e selecione a sub-rede e a VPC que você identificou anteriormente.
3. Adicione uma regra de autorização para dar aos clientes acesso aoVPC. Para fazer isso, execute as etapas descritas em eAdicionar uma regra de autorização, em Rede de destino, insira o IPv4 CIDR intervalo doVPC.

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.

Acesse um peering VPC usando o Client VPN

A AWS Client VPN configuração desse cenário inclui um alvo VPC (VPCA) que é emparelhado com um adicional VPC (VPCB). Recomendamos essa configuração se você precisar dar aos clientes acesso aos recursos dentro de um destino VPC e a outros VPCs que estão emparelhados com ele (como VPC B).

> **Note**
>
> O procedimento para permitir o acesso a um peering VPC (descrito a seguir o diagrama de rede) é necessário somente se o VPN endpoint do cliente tiver sido configurado para o modo de túnel dividido. No modo de túnel completo, o acesso ao peering VPC é permitido por padrão.



Antes de começar, faça o seguinte:

- Crie ou identifique um VPC com pelo menos uma sub-rede. Identifique a sub-rede na a VPC ser associada ao VPN endpoint do cliente e anote seus IPv4 CIDR intervalos.
- Identifique um CIDR intervalo adequado para os endereços IP do cliente que não se sobreponha ao VPCCIDR.

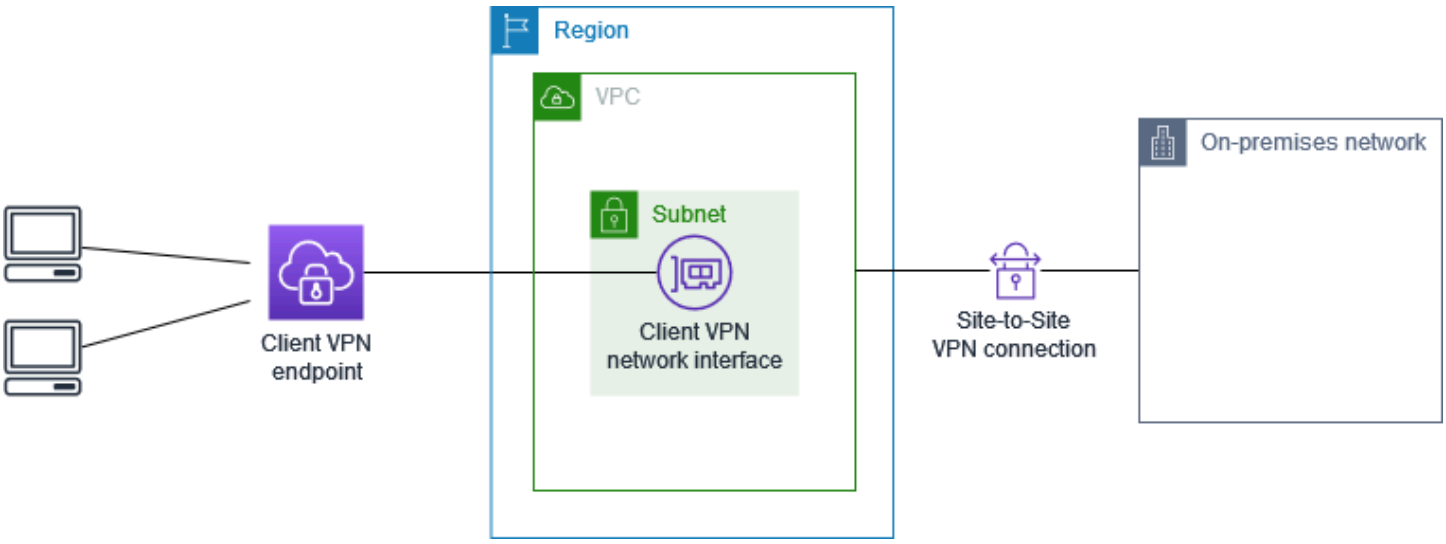
- Analise as regras e limitações dos VPN endpoints do cliente emRegras e melhores práticas de uso AWS Client VPN.

Para implementar essa configuração

1. Estabeleça a conexão VPC de emparelhamento entre o. VPCs Siga as etapas em Criar e aceitar uma conexão de VPC peering no Amazon VPC Peering Guide. Confirme se as instâncias em VPC A podem se comunicar com instâncias em VPC B usando a conexão de peering.
2. Crie um VPN endpoint de cliente na mesma região do destinoVPC. No diagrama, isso é VPC A. Execute as etapas descritas emCrie um AWS Client VPN endpoint.
3. Associe a sub-rede que você identificou ao VPN endpoint do cliente que você criou. Para fazer isso, execute as etapas descritas emAssociar uma rede de destino a um AWS Client VPN endpoint, selecionando a VPC e a sub-rede. Por padrão, associamos o grupo de segurança padrão do VPC ao VPN endpoint do Cliente. Você pode associar um grupo de segurança diferente utilizando as etapas descritas em the section called “Aplicar um grupo de segurança a uma rede de destino”.
4. Adicione uma regra de autorização para dar aos clientes acesso ao destinoVPC. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Para ativar a Rede de destino, insira o IPv4 CIDR intervalo doVPC.
5. Adicione uma rota para direcionar o tráfego para o peeringVPC. No diagrama, isso é VPC B. Para fazer isso, execute as etapas descritas emCrie uma rota AWS Client VPN de endpoint. Em Destino da rota, insira o IPv4 CIDR intervalo do peeringVPC. Em Target VPC Subnet ID, selecione a sub-rede que você associou ao endpoint do ClienteVPN.
6. Adicione uma regra de autorização para dar aos clientes acesso ao peeringVPC. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Em Rede de destino, insira o IPv4 CIDR intervalo do peeringVPC.
7. Adicione uma regra aos grupos de segurança de suas instâncias em VPC A e VPC B para permitir o tráfego do grupo de segurança que foi aplicado ao VPN endpoint do cliente na etapa 3. Para obter mais informações, consulte Grupos de segurança.

Acesse uma rede local usando o Client VPN

A AWS Client VPN configuração desse cenário inclui acesso somente a uma rede local. 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 um VPC com pelo menos uma sub-rede. Identifique a sub-rede na a VPC ser associada ao VPN endpoint do cliente e anote seus IPv4 CIDR intervalos.
- Identifique um CIDR intervalo adequado para os endereços IP do cliente que não se sobreponha ao VPCCIDR.
- Analise as regras e limitações dos VPN endpoints do cliente emRegras e melhores práticas de uso AWS Client VPN.

Para implementar essa configuração

1. Habilite a comunicação entre a VPC e sua própria rede local por meio de uma conexão site a AWS siteVPN. 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 AWS Direct Connect conexão entre sua rede VPC e sua rede local. Para obter mais informações, consulte o Guia do usuário do AWS Direct Connect.

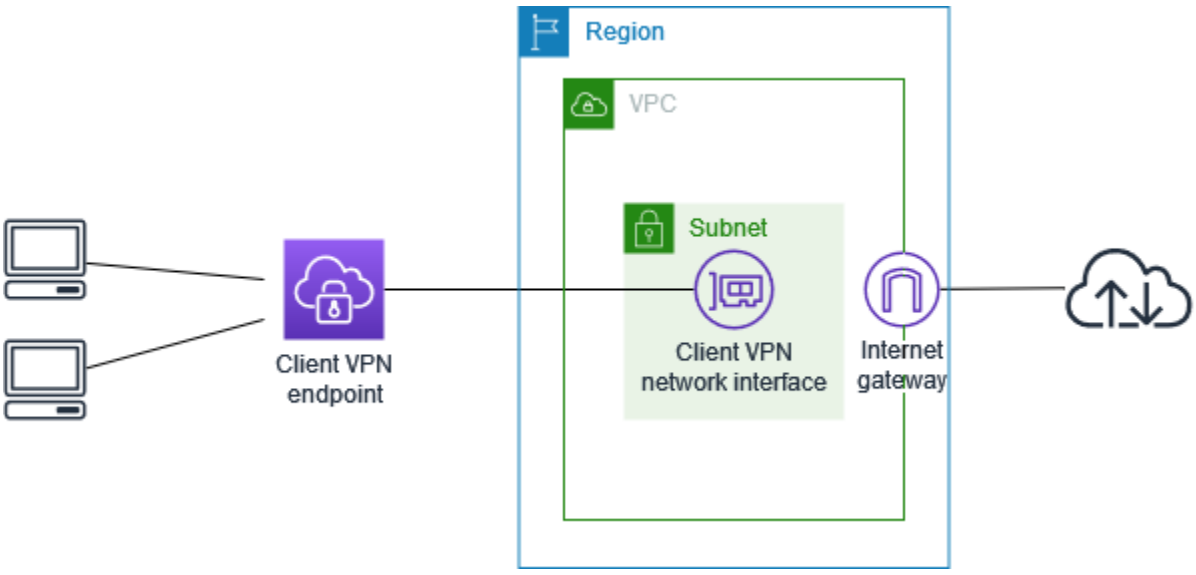
2. Teste a VPN conexão AWS site a site que você criou na etapa anterior. Para fazer isso, execute as etapas descritas em Teste da VPN conexão site a site no Guia do AWS Site-to-Site VPN usuário. Se a VPN conexão estiver funcionando conforme o esperado, vá para a próxima etapa.

3. Crie um VPN endpoint de cliente na mesma região doVPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
4. Associe a sub-rede que você identificou anteriormente ao VPN endpoint do cliente. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um AWS Client VPN endpoint e selecione a VPC e a sub-rede.
5. Adicione uma rota que permita o acesso à conexão AWS site a siteVPN. Para fazer isso, execute as etapas descritas emCrie uma rota AWS Client VPN de endpoint; em Destino da rota, insira o IPv4 CIDR intervalo da VPN conexão AWS site a site e, em ID da sub-rede de destino, selecione a VPC sub-rede que você associou ao endpoint do cliente. VPN
6. Adicione uma regra AWS de autorização para dar aos clientes acesso à conexão site a siteVPN. Para fazer isso, execute as etapas descritas emAdicionar uma regra de autorização a um AWS Client VPN endpoint; para Rede de destino, insira o intervalo AWS de conexão site a siteVPN. IPv4 CIDR

Acesse a internet usando o Cliente VPN

A AWS Client VPN configuração desse cenário inclui um único destino VPC e acesso à Internet. Recomendamos essa configuração se você precisar dar aos clientes acesso aos recursos dentro de um único destino VPC e também permitir o acesso à Internet.

Se você já concluiu o tutorial Comece com AWS Client VPN, então já implementou esse cenário.



Antes de começar, faça o seguinte:

- Crie ou identifique um VPC com pelo menos uma sub-rede. Identifique a sub-rede na a VPC ser associada ao VPN endpoint do cliente e anote seus IPv4 CIDR intervalos.
- Identifique um CIDR intervalo adequado para os endereços IP do cliente que não se sobreponha ao VPCCIDR.
- Analise as regras e limitações dos VPN endpoints do cliente emRegras e melhores práticas de uso AWS Client VPN.

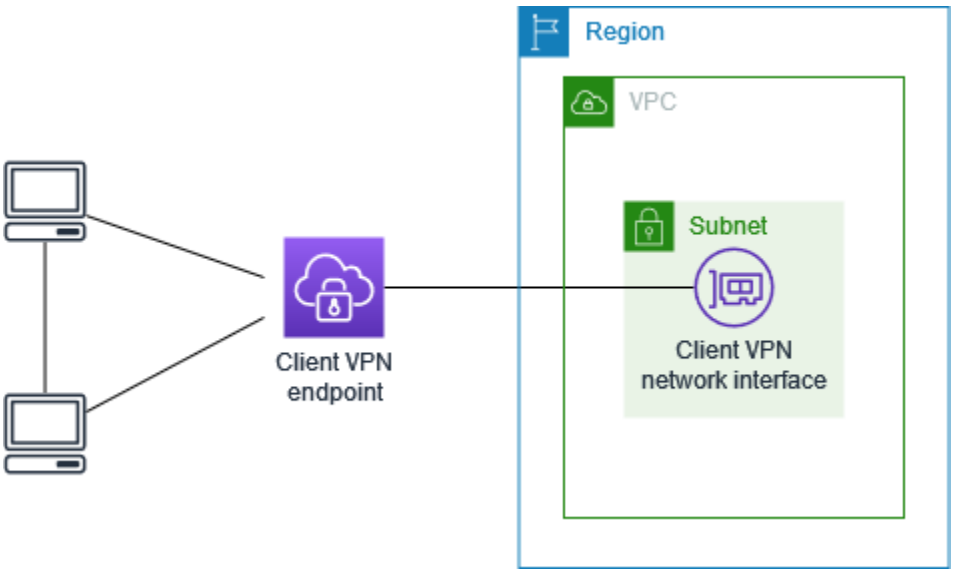
Para implementar essa configuração

1. Certifique-se de que o grupo de segurança que você usará para o VPN endpoint do cliente permita tráfego de saída para a Internet. Para fazer isso, adicione regras de saída que permitam tráfego para 0.0.0.0/0 para tráfego e. HTTP HTTPS
2. Crie um gateway de internet e conecte-o ao seuVPC. Para obter mais informações, consulte Criando e anexando um Internet Gateway no Guia do VPC usuário da Amazon.
3. Torne a sub-rede pública, adicionando uma rota para o gateway de internet à sua tabela de rotas. No VPC console, escolha Sub-redes, selecione a sub-rede que você pretende associar ao VPN endpoint do cliente, escolha Tabela de rotas e, em seguida, escolha a 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 VPN endpoint de cliente na mesma região doVPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
5. Associe a sub-rede que você identificou anteriormente ao VPN endpoint do cliente. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um AWS Client VPN endpoint e selecione a VPC e a sub-rede.
6. Adicione uma regra de autorização para dar aos clientes acesso aoVPC. Para fazer isso, execute as etapas descritas emAdicionar uma regra de autorização; e para ativar a rede de destino, insira o IPv4 CIDR intervalo doVPC.
7. Adicione uma rota que permita tráfego para a Internet. Para fazer isso, execute as etapas descritas emCrie uma rota AWS Client VPN de endpoint; em Destino da rota, insira e`0.0.0.0/0`, em ID da VPC sub-rede de destino, selecione a sub-rede que você associou ao endpoint do clienteVPN.
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. Em Destination network (Rede de destino), insira `0.0.0.0/0`.

9. Certifique-se de que os grupos de segurança dos recursos em seu VPC tenham uma regra que permita o acesso do grupo de segurança associado ao VPN endpoint do cliente. Isso permite que seus clientes acessem os recursos em seuVPC.

lient-to-client Acesso C usando o cliente VPN

A AWS Client VPN configuração desse cenário permite que os clientes acessem um único VPC e permite que os clientes roteiem o tráfego entre si. Recomendamos essa configuração se os clientes que se conectam ao mesmo VPN endpoint do cliente também precisarem se comunicar entre si. Os clientes podem se comunicar entre si usando o endereço IP exclusivo atribuído a eles pela CIDR faixa de clientes quando se conectam ao VPN endpoint do cliente.



Antes de começar, faça o seguinte:

- Crie ou identifique um VPC com pelo menos uma sub-rede. Identifique a sub-rede na a VPC ser associada ao VPN endpoint do cliente e anote seus IPv4 CIDR intervalos.
- Identifique um CIDR intervalo adequado para os endereços IP do cliente que não se sobreponha ao VPCCIDR.
- Analise as regras e limitações dos VPN endpoints do cliente emRegras e melhores práticas de uso AWS Client VPN.

> **Note**
>
> As regras de autorização baseadas em rede usando grupos do Active Directory ou grupos de SAML IdP baseados não são suportadas nesse cenário.

Para implementar essa configuração

1. Crie um VPN endpoint de cliente na mesma região doVPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
2. Associe a sub-rede que você identificou anteriormente ao VPN endpoint do cliente. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um AWS Client VPN endpoint 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 Crie uma rota AWS Client VPN de endpoint. Em Destino da rota, insira o CIDR intervalo de clientes e, em Target VPC Subnet ID, especifique`local`.
4. Adicione uma regra de autorização para dar aos clientes acesso aoVPC. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Para ativar a Rede de destino, insira o IPv4 CIDR intervalo doVPC.
5. Adicione uma regra de autorização para dar aos clientes acesso ao CIDR intervalo de clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Para ativar a rede de destino, insira o CIDR intervalo de clientes.

Restrinja o acesso à sua rede usando o Cliente VPN

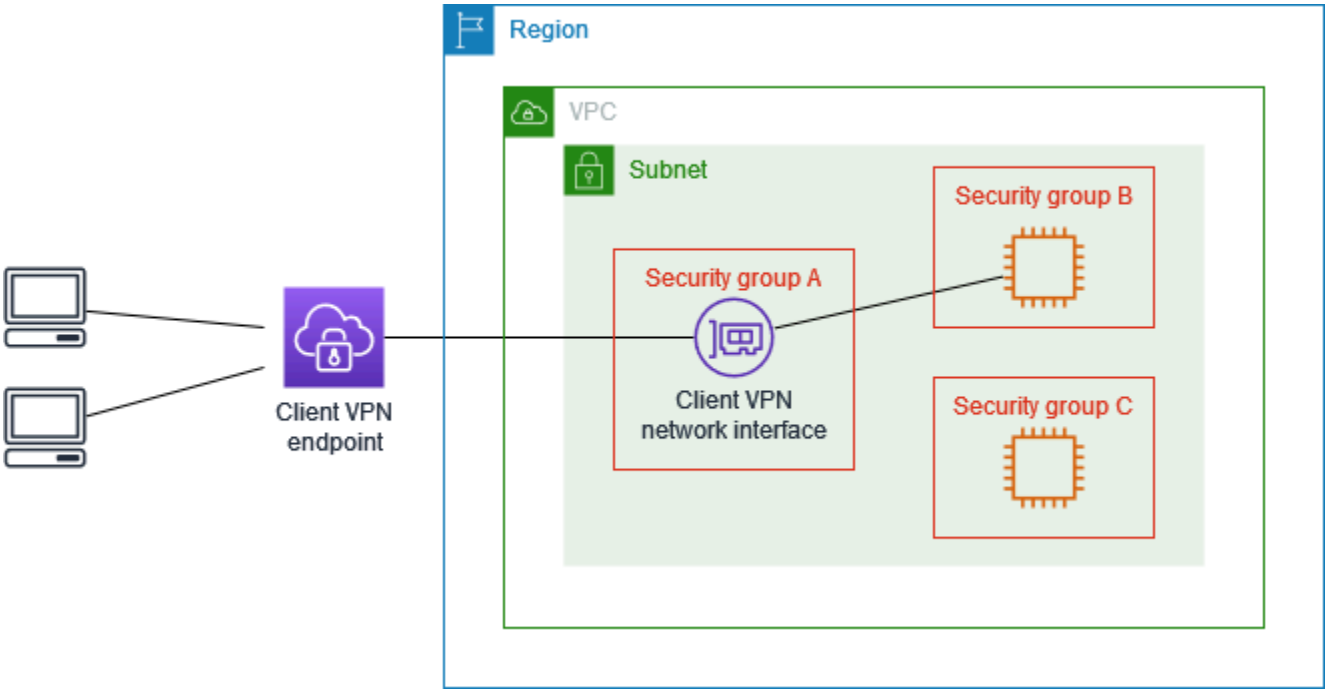
Você pode configurar seu AWS Client VPN endpoint para restringir o acesso a recursos específicos em seuVPC. Para a autenticação baseada no usuário, você também pode restringir o acesso a partes da sua rede, com base no grupo de usuários que acessa o endpoint do clienteVPN.

Restringir o acesso usando grupos de segurança

Você pode conceder ou negar acesso a recursos específicos no seu VPC adicionando ou removendo regras de grupo de segurança que fazem referência ao grupo de segurança que foi aplicado à associação de rede de destino (o grupo de VPN segurança do Cliente). Essa configuração é comentada no cenário descrito em Acesse um VPC cliente usuário VPN. 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. Em seguida, crie uma regra que permita o tráfego do grupo de VPN segurança do Cliente.

No diagrama a seguir, o grupo de segurança A é o grupo de VPN segurança do cliente, o grupo de segurança B está associado a uma EC2 instância e o grupo de segurança C está associado a uma EC2 instância. Se você adicionar uma regra ao grupo de segurança B que permita o acesso do grupo de segurança A, os clientes poderão acessar a instância associada ao grupo de segurança B. Se o grupo de segurança C não tiver uma regra que permita o acesso do grupo de segurança A, os clientes não poderão acessar a instância associada ao grupo de segurança C.



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

Como criar uma regra de grupo de segurança

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha 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.
   - Em Origem, escolha Personalizado e, em seguida, insira ou escolha a ID do grupo de VPN segurança do Cliente.
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 VPN segurança do Cliente, exclua-a.

Como verificar as regras do grupo de segurança

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha 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 seja o grupo VPN de segurança do Cliente, escolha Editar regras e escolha Excluir (o ícone x) para a regra. Escolha Salvar regras.

Restringir o acesso com base em grupos de usuários

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

1. Configure usuários e grupos em AWS Directory Service ou em seu IdP. Para obter mais informações, consulte os tópicos a seguir.
   - Autenticação do Active Directory no cliente VPN
   - Requisitos e considerações para autenticação SAML federada baseada
2. Crie uma regra de autorização para o VPN endpoint do seu cliente que permita que um grupo específico acesse toda ou parte da sua rede. Para obter mais informações, consulte AWS Client VPN regras de autorização.

Se o VPN endpoint do seu cliente 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 sua rede, você pode criar vários VPN endpoints de cliente. 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 em AWS Client VPN.
2. Crie um VPN endpoint de cliente. Para obter mais informações, consulte Crie um AWS Client VPN endpoint.
3. Crie uma regra de autorização que conceda acesso a toda a rede ou parte dela. Por exemplo, para um VPN endpoint de cliente 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.

Autenticação do cliente em AWS Client VPN

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

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

- Autenticação do Active Directory (baseada no usuário)
- Autenticação mútua (baseada em certificado)
- Login único (autenticação federada SAML baseada) (baseada no usuário)

Você pode usar apenas um dos métodos anteriores ou pode usar uma combinação de autenticação mútua com um método baseado no usuário, como o seguinte:

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

> **Important**
>
> Para criar um VPN endpoint de cliente, você deve provisionar um certificado de servidor AWS Certificate Manager, independentemente do tipo de autenticação que você usa. Para obter mais informações sobre como criar e provisionar um certificado de servidor, consulte as etapas em Autenticação mútua em AWS Client VPN.

Autenticação do Active Directory no cliente VPN

VPNO cliente fornece suporte ao 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 AWS Directory Service, o Cliente VPN pode se conectar aos Active Directories existentes provisionados em AWS ou em sua rede local. Isso permite que você use sua infraestrutura de autenticação de cliente existente. Se você estiver usando um Active Directory local e não tiver um Microsoft AD AWS gerenciado existente, deverá configurar um conector do Active Directory (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.

O cliente VPN oferece suporte à autenticação multifator (MFA) quando está habilitada para AWS Managed Microsoft AD ou AD Connector. Se MFA estiver ativado, os clientes devem inserir um nome de usuário, senha e MFA código ao se conectarem a um VPN endpoint do cliente. Para obter mais informações sobre a habilitaçãoMFA, consulte Habilitar a autenticação multifator para o Microsoft AD AWS gerenciado e Ativar a autenticação multifator para o AD Connector no Guia de AWS Directory Service Administração.

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

Autenticação mútua em AWS Client VPN

Com a autenticação mútua, o 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 VPN endpoint do cliente. É necessário criar um certificado e uma chave de servidor e pelo menos um certificado e uma chave de cliente.

Você deve carregar o certificado do servidor para AWS Certificate Manager (ACM) e especificá-lo ao criar um VPN endpoint de cliente. Ao carregar o certificado do servidor paraACM, você também especifica a autoridade de certificação (CA). Você só precisa carregar o certificado do cliente para ACM quando a CA do certificado do cliente for diferente da CA do certificado do servidor. Para obter mais informações sobreACM, consulte o Guia AWS Certificate Manager do usuário.

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

> **Note**
>
> Um VPN endpoint de cliente suporta somente tamanhos de chave de 1024 bits e 2048 RSA bits. Além disso, o certificado do cliente deve ter o atributo CN no campo Subject (Assunto). Quando os certificados usados com o VPN serviço do Cliente são atualizados, seja por meio de ACM rotação automática, importação manual de um novo certificado ou atualizações de metadados para o IAM Identity Center, o VPN serviço do Cliente atualizará automaticamente o VPN endpoint do Cliente com o certificado mais recente. Esse processo é automatizado e pode levar até 24 horas.

Tarefas

- Habilite a autenticação mútua para AWS Client VPN
- Renove seu certificado de servidor para AWS Client VPN

Habilite a autenticação mútua para AWS Client VPN

Você pode habilitar a autenticação mútua no Client VPN no Linux/macOS ou no Windows.

Linux/macOS

O procedimento a seguir usa o Open VPN easy-rsa para gerar os certificados e chaves do servidor e do cliente e, em seguida, carrega o certificado e a chave do servidor para. ACM Para obter mais informações, consulte o RSAEasy-3 Quickstart README.

Para gerar os certificados e chaves do servidor e do cliente e enviá-los para ACM

1. Clone o repositório Open VPN easy-rsa em seu 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 PKI ambiente.

   ```
   $ ./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 --san=DNS:server 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. Carregue o certificado e a chave do servidor e o certificado e a chave do cliente paraACM. Certifique-se de carregá-los na mesma região em que você pretende criar o VPN endpoint do cliente. Os comandos a seguir usam a AWS CLI para fazer upload dos certificados. Para carregar os certificados usando o ACM console em vez disso, consulte Importar um certificado no Guia AWS Certificate Manager do usuário.

```
$ 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 fazer o upload do certificado do cliente para ACM o. Se os certificados do servidor e do cliente tiverem sido emitidos pela mesma Autoridade de Certificação (CA), você poderá usar o certificado do servidor ARN para o servidor e o cliente ao criar o VPN endpoint do cliente. 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 RSA Easy-3.x e o usa para gerar certificados e chaves de servidor e cliente.

Para gerar certificados e chaves de servidor e cliente e enviá-los para ACM

1. Abra a página de RSAlançamentos do Easy, baixe o ZIP arquivo 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 Easy RSA 3.

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

4. Inicialize um novo PKI ambiente.

```
# ./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 --san=DNS:server 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 Easy RSA 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. Carregue o certificado e a chave do servidor e o certificado e a chave do cliente paraACM. Certifique-se de carregá-los na mesma região em que você pretende criar o VPN endpoint do cliente. Os comandos a seguir usam o AWS CLI para carregar os certificados. Para carregar os certificados usando o ACM console em vez disso, consulte Importar um certificado no Guia AWS Certificate Manager do usuário.

```
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 fazer o upload do certificado do cliente para ACM o. Se os certificados do servidor e do cliente tiverem sido emitidos pela mesma Autoridade de Certificação (CA), você poderá usar o certificado do servidor ARN para o servidor e o cliente ao criar o VPN endpoint do cliente. 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.

Renove seu certificado de servidor para AWS Client VPN

Você pode renovar e reimportar um certificado de VPN servidor cliente que tenha expirado. Dependendo da versão do Open VPN easy-rsa que você está usando, o procedimento pode variar. Consulte a documentação de renovação e revogação de certificados RSA Easy-3 para obter mais detalhes.

Para renovar seu certificado de servidor

1. Faça um dos seguintes:
   - Easy - RSA versão 3.1.x
     - Execute o comando de renovação do certificado.

```
$ ./easyrsa renew server nopass
```

- Easy - RSA versão 3.2.x

  a. Execute o comando expire.

  ```
  $ ./easyrsa expire server
  ```

  b. Assine um novo certificado.

  ```
  $ ./easyrsa sign-req server server
  ```

2. Crie uma pasta personalizada, copie os novos arquivos para ela e navegue até a pasta.

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. Importe os novos arquivos para ACM o. Certifique-se de importá-los na mesma região do VPN endpoint do cliente.

```
$ aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Login único — autenticação federada SAML baseada em 2.0 — no Cliente VPN

AWS Client VPN oferece suporte à federação de identidades com a Security Assertion Markup Language 2.0 (SAML2.0) para endpoints de clientesVPN. Você pode usar provedores de identidade (IdPs) que suportam SAML 2.0 para criar identidades de usuário centralizadas. Em seguida, você pode configurar um VPN endpoint do cliente para usar a autenticação federada SAML baseada e

associá-la ao IdP. Em seguida, os usuários se conectam ao VPN endpoint do Cliente usando suas credenciais centralizadas.

Tópicos

Habilitar SAML para AWS Client VPN

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

1. Crie um aplicativo SAML baseado no IdP escolhido para usar com 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 SAMLrecursos de configuração de IdP baseados em.
3. No IdP, gere e faça download de um documento de metadados de federação que descreve sua organização como um IdP.

   Esse XML documento assinado é usado para estabelecer a relação de confiança entre AWS e o IdP.
4. Crie um provedor de IAM SAML identidade na mesma AWS conta do VPN endpoint do cliente.

   O provedor de IAM SAML identidade define a relação de AWS confiança do IdP da sua organização usando o documento de metadados gerado pelo IdP. Para obter mais informações, consulte Criação de provedores de IAM SAML identidade no Guia IAM do usuário. Se você atualizar posteriormente a configuração do aplicativo no IdP, gere um novo documento de metadados e atualize seu IAM SAML provedor de identidade.

   > **Note**
   >
   > Você não precisa criar uma IAM função para usar o provedor de IAM SAML identidade.
5. Crie um VPN endpoint de cliente.

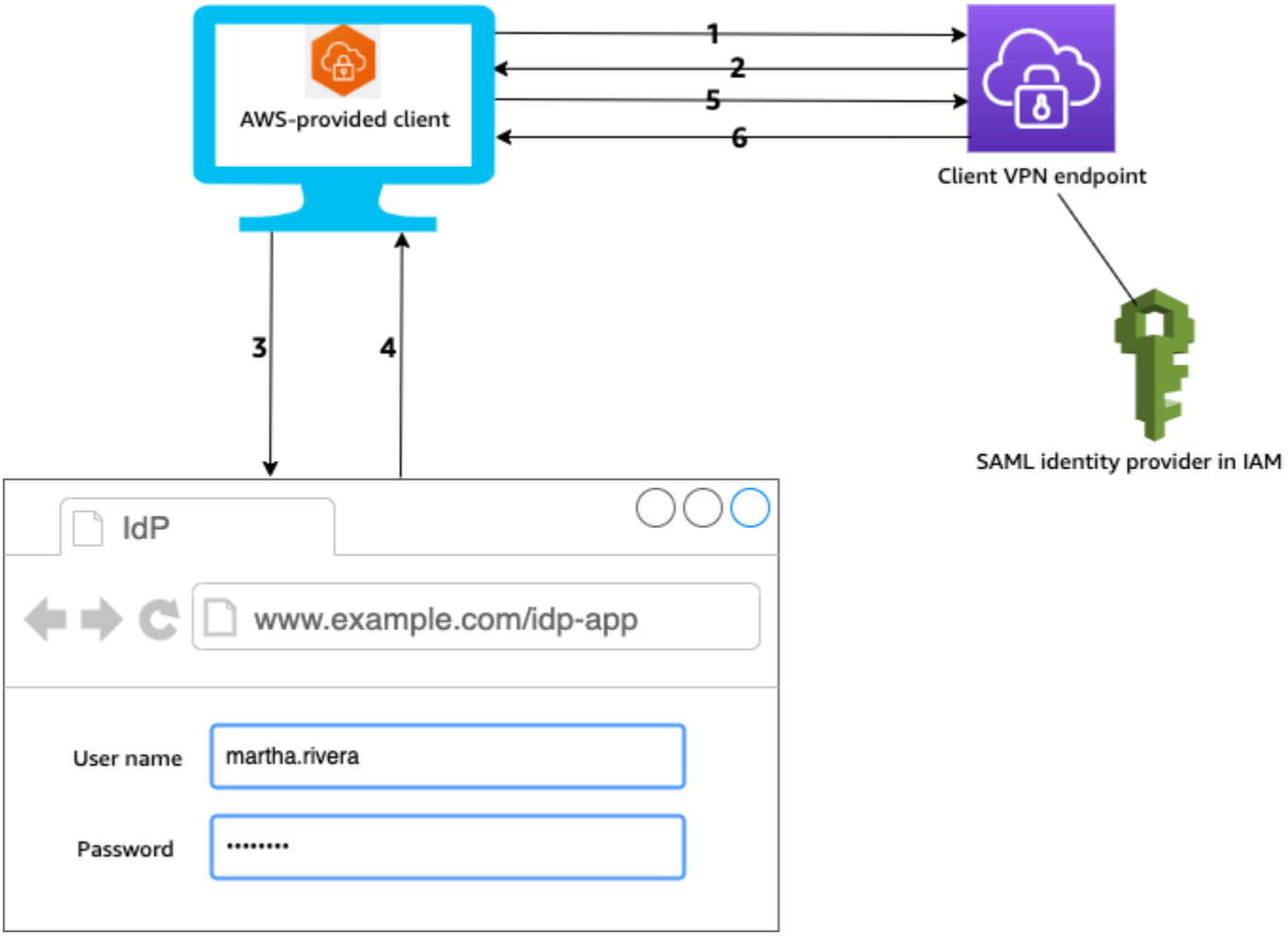
Especifique a autenticação federada como o tipo de autenticação e especifique o provedor de IAM SAML identidade que você criou. Para obter mais informações, consulte Crie um AWS Client VPN endpoint.

6. Exporte o arquivo de configuração do cliente e distribua-o aos usuários. Instrua seus usuários a baixar a versão mais recente do cliente AWS fornecido e usá-la para carregar o arquivo de configuração e se conectar ao VPN endpoint do cliente.

   Como alternativa, se você habilitou o portal de autoatendimento para seu VPN endpoint de cliente, instrua seus usuários a acessarem o portal de autoatendimento para obter o arquivo de configuração e o cliente fornecido. AWS Para obter mais informações, consulte AWS Client VPN acesso ao portal de autoatendimento.

Fluxo de trabalho de autenticação

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



1. O usuário abre o cliente AWS fornecido em seu dispositivo e inicia uma conexão com o VPN endpoint do cliente.
2. O VPN endpoint do cliente envia um URL IdP e uma solicitação de autenticação de volta ao cliente, com base nas informações fornecidas IAM SAML no provedor de identidade.
3. O cliente AWS fornecido 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 suas credenciais na página de login e o IdP envia uma declaração SAML assinada de volta ao cliente.
5. O cliente AWS fornecido envia a SAML afirmação para o VPN endpoint do cliente.
6. O VPN endpoint do cliente valida a afirmação e permite ou nega o acesso ao usuário.

Requisitos e considerações para autenticação SAML federada baseada

A seguir estão os requisitos e considerações para a autenticação federada SAML baseada.

- Para obter cotas e regras para configurar usuários e grupos em um SAML IdP baseado, consulte. Cotas de usuários e grupos
- A SAML declaração e SAML os documentos devem ser assinados.
- AWS Client VPN só suporta as condições AudienceRestriction "" e "NotBefore e NotOnOrAfter" nas SAML afirmações.
- O tamanho máximo suportado para SAML respostas é 128 KB.
- AWS Client VPN não fornece solicitações de autenticação assinadas.
- SAMLo logout único não é suportado. Os usuários podem sair desconectando-se do cliente AWS fornecido ou você pode encerrar as conexões.
- Um VPN endpoint de cliente oferece suporte somente a um único IdP.
- A autenticação multifator (MFA) é suportada quando ativada em seu IdP.
- Os usuários devem usar o cliente AWS fornecido para se conectar ao VPN endpoint do cliente. Eles devem usar a versão 1.2.0 ou posterior. Para obter mais informações, consulte Conectar usando o cliente AWS fornecido.
- Os seguintes navegadores são compatíveis com a autenticação IdP: Apple Safari, Google Chrome, Microsoft Edge e Mozilla Firefox.
- O cliente AWS fornecido reserva a TCP porta 35001 nos dispositivos dos usuários para a SAML resposta.
- Se o documento de metadados do provedor de IAM SAML identidade for atualizado com uma mensagem incorreta ou maliciosaURL, isso poderá causar problemas de autenticação para os usuários ou resultar em ataques de phishing. Portanto, recomendamos que você use AWS CloudTrail para monitorar as atualizações feitas no provedor de IAM SAML identidade. Para obter mais informações, consulte Registro IAM e AWS STS chamadas com AWS CloudTrail no Guia IAM do usuário.
- AWS Client VPN envia uma solicitação AuthN para o IdP por meio de uma associação de redirecionamento. HTTP Portanto, o IdP deve suportar a vinculação de HTTP redirecionamento e deve estar presente no documento de metadados do IdP.
- Para a SAML afirmação, você deve usar um formato de endereço de e-mail para o `NameID` atributo.

SAMLrecursos de configuração de IdP baseados em

A tabela a seguir lista as SAML bases IdPs com as quais testamos para uso e AWS Client VPN os recursos que podem ajudá-lo a configurar o IdP.

IdP	Recurso
Okta	Autentique AWS Client VPN usuários com SAML
Microsoft Azure Active Directory	Para obter mais informações, consulte Tutorial: integração de login único (SSO) do Azure Active Directory com o AWS Cliente VPN no site de documentação da Microsoft.
JumpCloud	Login único (SSO) com AWS Client VPN
AWS IAM Identity Center	Usando o IAM Identity Center com AWS Client VPN para autenticação e autorização

Informações do provedor de serviços para criar um aplicativo

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

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

Pelo menos um atributo deve ser incluído na SAML resposta do IdP. Veja os exemplos de atributo a seguir.

Atributo	Descrição
`FirstName`	O nome do usuário.
`LastName`	O sobrenome do usuário.
`memberOf`	Os grupos aos quais o usuário pertence.

> **Note**
>
> O `memberOf` atributo é necessário para usar as regras de autorização baseadas em grupos do Active Directory ou do SAML IdP. Também diferencia letras maiúsculas de minúsculas e deve ser configurado exatamente como especificado. Consulte Autorização com base em rede e AWS Client VPN regras de autorização para obter mais informações.

Suporte para o portal de autoatendimento

Se você habilitar o portal de autoatendimento para seu VPN endpoint do Cliente, os usuários se conectarão ao portal usando suas credenciais de SAML IdP baseadas.

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

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

Se você estiver usando o VPN endpoint do Cliente em uma GovCloud região, use o seguinte ACS URL em vez disso. Se você usar o mesmo IDP aplicativo para se autenticar tanto para o padrão quanto para GovCloud as regiões, poderá adicionar os doisURLs.

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

Se o seu IdP não suportar vários ACSURLs, faça o seguinte:

1. Crie um aplicativo adicional SAML baseado em seu IdP e especifique o seguinte. ACS URL

   ```
   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 IAM SAML identidade na mesma AWS conta do VPN endpoint do cliente. Para obter mais informações, consulte Criação de provedores de IAM SAML identidade no Guia IAM do usuário.

> **Note**
>
> Você cria esse provedor de IAM SAML identidade além daquele criado para o aplicativo principal.

4. Crie o VPN endpoint do cliente e especifique os dois provedores de IAM SAML identidade que você criou.

Autorização do cliente em AWS Client VPN

O cliente VPN oferece suporte a dois tipos de autorização de cliente: grupos de segurança e autorização baseada em rede (usando regras de autorização).

Grupos de segurança

Ao criar um VPN endpoint do cliente, você pode especificar os grupos de segurança de um específico VPC para aplicar ao VPN endpoint do cliente. Quando você associa uma sub-rede a um VPN endpoint do cliente, aplicamos automaticamente o grupo de segurança padrão VPC do cliente. Você pode alterar os grupos de segurança depois de criar o VPN endpoint do cliente. Para obter mais informações, consulte Aplique um grupo de segurança a uma rede de destino no AWS Client VPN. Os grupos de segurança estão associados às interfaces de VPN rede do cliente.

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

Por outro lado, você pode restringir o acesso dos VPN usuários do Cliente não especificando o grupo de segurança que foi aplicado à associação ou removendo a regra que faz referência ao grupo de segurança do VPN endpoint do Cliente. As regras de grupo de segurança necessárias também podem depender do tipo de VPN acesso que você deseja configurar. Para obter mais informações, consulte Cenários e exemplos para o cliente VPN.

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

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, você configura o grupo do Active Directory ou o grupo de IdP SAML baseado que tem acesso permitido. Somente os usuários que pertencerem ao grupo especificado poderão acessar a rede especificada. Se você não estiver usando o Active Directory ou a autenticação federada SAML baseada, ou se quiser abrir o acesso a todos os usuários, poderá especificar uma regra que conceda acesso a todos os clientes. Para obter mais informações, consulte AWS Client VPN regras de autorização.

Tarefas

- Crie uma regra de grupo AWS Client VPN de segurança de endpoint

Crie uma regra de grupo AWS Client VPN de segurança de endpoint

Crie uma VPN regra de cliente que permita o tráfego do grupo de segurança de VPN endpoint do cliente.

Para adicionar uma regra que permita o tráfego do grupo de segurança de VPN endpoint do cliente

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha 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, você pode restringir o acesso a um tipo específico de tráfego, por exemplo, SSH.

   Em Origem, especifique a ID do grupo de segurança associado à rede de destino (sub-rede) do VPN endpoint do cliente.
6. Escolha Salvar regras.

Autorização de conexão em AWS Client VPN

Você pode configurar um manipulador de conexão de cliente para seu VPN endpoint de cliente. 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 VPN serviço do cliente autenticou o dispositivo e o usuário.

Para configurar um manipulador de conexão do cliente para seu VPN endpoint do cliente, crie uma AWS Lambda função que use os atributos do dispositivo, do usuário e da conexão como entradas e retorne uma decisão ao VPN serviço do cliente para permitir ou negar uma nova conexão. Você especifica a função Lambda no endpoint do seu clienteVPN. Quando os dispositivos se conectam ao seu VPN endpoint do cliente, o VPN serviço do cliente invoca a função Lambda em seu nome. Somente conexões autorizadas pela função Lambda podem se conectar ao endpoint do clienteVPN.

> **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 AWS região e na mesma AWS conta do endpoint do clienteVPN.
- 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 VPN serviço Client não obtiver uma resposta esperada da função, o VPN serviço Client 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 sua função Lambda, as conexões existentes com o VPN endpoint do cliente 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 AWS Client VPN cliente.
- Se os clientes usarem o cliente AWS fornecido para se conectar ao VPN endpoint do cliente, 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 do dispositivo, atributos do usuário e atributos de conexão como entradas do serviço do cliente. VPN Em seguida, ele deve retornar ao VPN serviço do Cliente a decisão de permitir ou negar a conexão.

Esquema de solicitação

A função Lambda usa um JSON blob contendo os seguintes campos 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>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id`— O ID da conexão do cliente com o VPN endpoint do cliente.
- `endpoint-id`— O ID do VPN endpoint do cliente.
- `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 SAML baseada, isso 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 VPN serviço Client fornece um valor quando a `--push-peer-info` diretiva está presente na configuração do Open VPN Client, quando os clientes se conectam a um VPN endpoint do Client e quando o cliente está executando a plataforma Windows.
- `public-ip`: o endereço IP público do dispositivo de conexão.
- `client-openvpn-version`— A VPN versão aberta que o cliente está usando.
- `aws-client-version`— A versão AWS do cliente.
- `groups`: o identificador do grupo, se aplicável. Para autenticação do Active Directory, esta será uma lista de grupos do Active Directory. Para autenticação federada SAML baseada, essa 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 `v3`.

Esquema de resposta

A função Lambda deve retornar os campos a seguir.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `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, 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 `v3`.

Você pode usar a mesma função Lambda para vários VPN endpoints do cliente 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 .

Use o manipulador de conexão do cliente para avaliação da postura

Você pode usar o manipulador de conexão do cliente para integrar seu VPN endpoint do cliente à sua 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 dispositivos, use a autenticação mútua para o endpoint do seu cliente. VPN Crie um certificado de cliente e uma chave exclusivos para cada cliente (dispositivo) que se conectará ao VPN endpoint do cliente. A função Lambda pode usar o nome comum exclusivo para o certificado do cliente (que é passado pelo VPN serviço do cliente) para identificar o dispositivo e obter seu status de conformidade de postura na sua solução de gerenciamento de dispositivos. 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, você pode avaliar os `platform-version` campos `platform` e que são passados para a função Lambda pelo serviço de clienteVPN.

> **Note**
>
> Embora o manipulador de conexão possa ser usado para impor uma versão mínima do AWS Client VPN aplicativo, o campo `aws-client-version` no manipulador de conexão só é aplicável ao AWS Client VPN aplicativo e está sendo preenchido a partir de variáveis de ambiente no dispositivo do usuário.

Ativar o manipulador de conexão do cliente

Para habilitar o manipulador de conexão do cliente, crie ou modifique um VPN endpoint do cliente e especifique o Amazon Resource Name (ARN) da função Lambda. Para ter mais informações, consulte Crie um AWS Client VPN endpoint e Modificar um AWS Client VPN endpoint.

Função vinculada ao serviço

AWS Client VPN cria automaticamente uma função vinculada ao serviço em sua conta chamada. AWSServiceRoleForClientVPNConnections A função tem permissões para invocar a função Lambda quando uma conexão é feita com o endpoint do VPN cliente. Para obter mais informações, consulte Usando funções vinculadas a serviços para AWS Client VPN.

Monitore falhas na autorização de conexão

Você pode visualizar o status de autorização de conexão das conexões com o VPN endpoint do cliente. Para obter mais informações, consulte Exibir conexões de AWS Client VPN clientes.

Quando o manipulador de conexão do cliente é usado para avaliação da postura, você também pode visualizar os status de conformidade da postura dos dispositivos que se conectam ao seu VPN endpoint do cliente nos registros de conexão. Para obter mais informações, consulte Registro de conexão para um AWS Client VPN endpoint.

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:

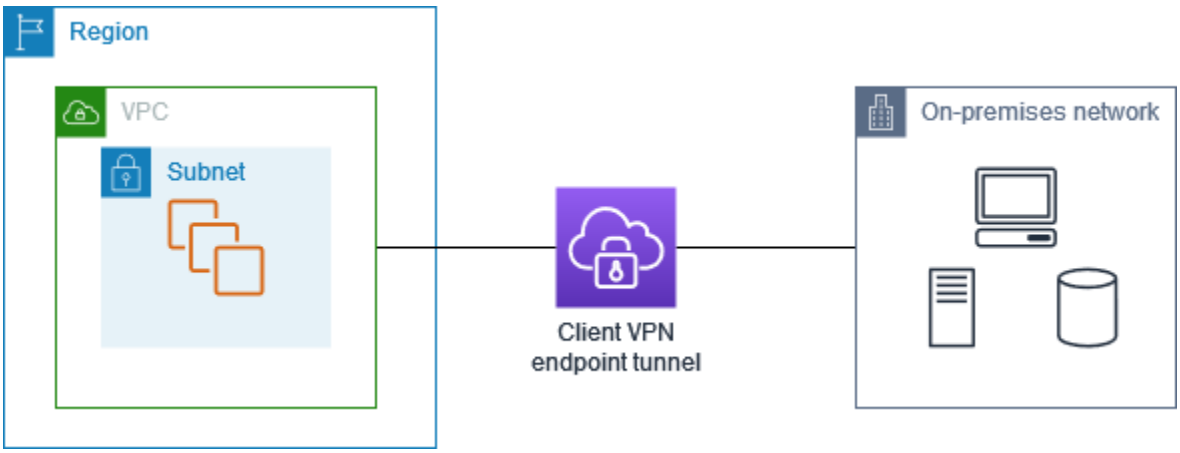
- `client-connect-failed`: a função Lambda impediu que a conexão fosse estabelecida.
- `client-connect-handler-timed-out`: a função Lambda atingiu o tempo limite.
- `client-connect-handler-other-execution-error`: a função Lambda encontrou um erro inesperado.
- `client-connect-handler-throttled`: a função 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 nos endpoints do cliente VPN

Por padrão, quando você tem um VPN endpoint do cliente, todo o tráfego dos clientes é roteado pelo túnel do clienteVPN. Quando você ativa o túnel dividido no VPN endpoint do cliente, enviamos as rotas na tabela de rotas do VPN endpoint do cliente para o dispositivo que está conectado ao endpoint do cliente. VPN Isso garante que somente o tráfego com um destino para a rede correspondente a uma rota da tabela de rotas do VPN endpoint do cliente seja roteado pelo túnel do clienteVPN.

Você pode usar um VPN endpoint do cliente de túnel dividido quando não quiser que todo o tráfego do usuário passe pelo endpoint do cliente. VPN

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



Benefícios do túnel dividido

O túnel dividido nos VPN endpoints do cliente oferece os seguintes benefícios:

- Você pode otimizar o roteamento do tráfego dos clientes fazendo com que somente o tráfego AWS destinado atravesse o túnel. VPN
- Você pode reduzir o volume de tráfego de saída e AWS, portanto, reduzir o custo de transferência de dados.

Considerações sobre roteamento

- Quando você ativa o modo de túnel dividido, todas as rotas na tabela de rotas do VPN endpoint do cliente são adicionadas à tabela de rotas do cliente quando a VPN conexão é estabelecida. Essa operação é diferente do comportamento padrão, que substitui a tabela de rotas do cliente pela entrada `0.0.0.0/0` para rotear todo o VPN tráfego pelo.

  > **Note**
  >
  > Não é recomendável adicionar uma `0.0.0.0/0` rota à tabela de rotas do VPN endpoint do cliente ao usar o modo de túnel dividido.

- Quando o modo de túnel dividido está ativado, qualquer modificação na tabela de rotas do VPN endpoint do cliente resultará na redefinição de todas as conexões do cliente.

Habilitando o túnel dividido

Você pode ativar o túnel dividido em um endpoint de cliente novo ou existente. VPN Para obter mais informações, consulte os tópicos a seguir.

- Crie um AWS Client VPN endpoint
- Modificar um AWS Client VPN endpoint

Registro de conexão para um AWS Client VPN endpoint

O registro de conexão é um recurso AWS Client VPN que permite capturar registros de conexão para o VPN endpoint do seu cliente.

Um registro de conexão contém entradas de registro de conexão que capturam informações sobre eventos de conexão, como quando um cliente (usuário final) se conecta, tenta se conectar ou se desconecta do VPN endpoint do cliente. Você pode usar essas informações para executar análises forenses, analisar como o VPN endpoint do seu cliente está sendo usado ou depurar problemas de conexão.

O registro de conexão está disponível em todas as regiões em AWS Client VPN que está disponível. Os registros de conexão são publicados em um grupo de CloudWatch registros de registros em sua conta.

> **Note**
>
> As tentativas fracassadas de autenticação mútua não são registradas.

Entradas de log de conexão

Uma entrada de registro de conexão é um blob JSON formatado de pares de valores-chave. 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",
    "username": "joe"
    }
```

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 VPN endpoint do cliente ao 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 da IPv4 CIDR faixa de clientes para o VPN endpoint 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, se aplicável.
- `username`— O nome de usuário é registrado quando a autenticação baseada no usuário (AD ouSAML) é usada para o endpoint.
- `connection-duration-seconds`: a duração de uma conexão em segundos. Igual à diferença entre "connection-start-time" e "connection-end-time”.

Para obter mais informações sobre como habilitar o registro em log de conexão, consulte AWS Client VPN registros de conexão.

Considerações sobre a VPN escalabilidade do cliente

Ao criar um VPN endpoint de cliente, considere o número máximo de VPN conexões simultâneas que você planeja oferecer suporte. Você deve levar em consideração o número de clientes aos quais você oferece suporte atualmente e se o VPN endpoint do seu cliente pode ser escalado para atender à demanda adicional, se necessário.

Os seguintes fatores afetam o número máximo de VPN conexões simultâneas que podem ser suportadas em um VPN endpoint do cliente:

Tamanho da CIDR gama de clientes

Ao criar um VPN endpoint de cliente, você deve especificar um CIDR intervalo de clientes, que é um IPv4 CIDR bloco entre uma máscara de rede /12 e /22. Cada VPN conexão com o VPN endpoint do cliente recebe um endereço IP exclusivo do CIDR intervalo de clientes. Uma parte dos endereços na CIDR faixa de clientes também é usada para dar suporte ao modelo de disponibilidade do VPN endpoint do cliente e não pode ser atribuída aos clientes. Você não pode alterar o CIDR intervalo de clientes depois de criar o VPN endpoint do cliente.

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

Número de sub-redes associadas

Ao associar uma sub-rede a um VPN endpoint do cliente, você permite que os usuários estabeleçam VPN sessões no endpoint do clienteVPN. Você pode associar várias sub-redes a um VPN endpoint do cliente para obter alta disponibilidade e permitir capacidade de conexão adicional.

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

Associações de sub-rede	Número suportado de conexões
1	7.000

Associações de sub-rede	Número suportado de conexões
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 clienteVPN. Portanto, o número de associações de sub-rede também depende do número de zonas de disponibilidade disponíveis em uma AWS região.

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

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

Para obter mais informações sobre as regras e limitações para trabalhar com CIDR intervalos de clientes e redes de destino, consulteRegras e melhores práticas de uso AWS Client VPN.

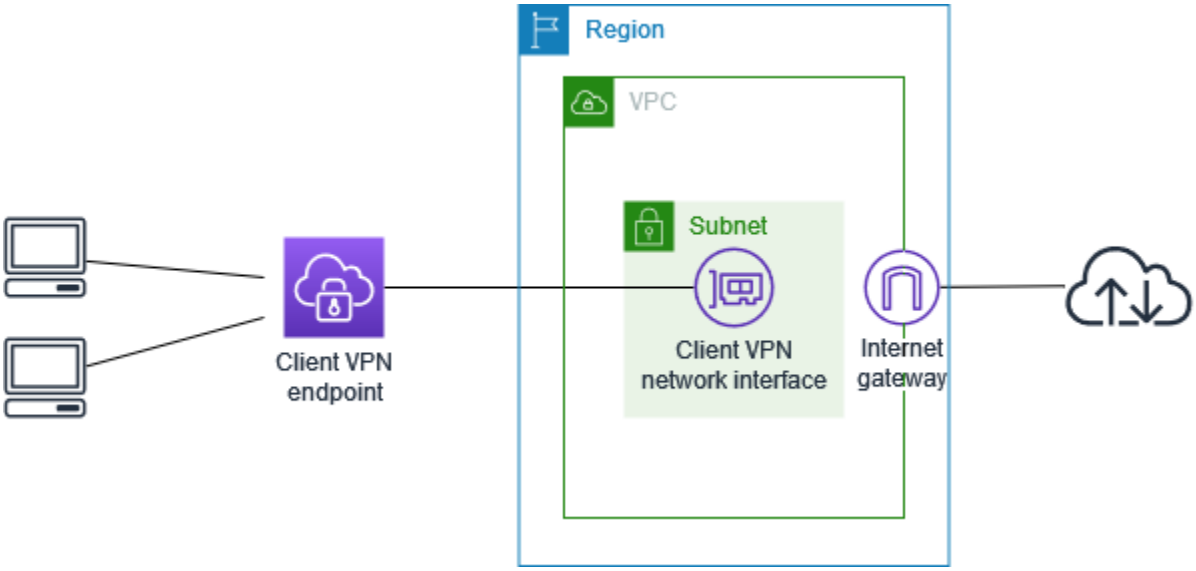
Para obter mais informações sobre cotas para seu VPN endpoint de cliente, consulte. AWS Client VPN cotas

Comece com AWS Client VPN

Neste tutorial, você criará um AWS Client VPN endpoint que faz o seguinte:

- Fornece a todos os clientes acesso a um únicoVPC.
- Fornece a todos os clientes acesso à Internet.
- Usa autenticação mútua.

O diagrama a seguir representa a configuração do seu VPN endpoint VPC e do Client depois de concluir este tutorial.



Etapas

- Pré-requisitos
- Etapa 1: gerar chaves e certificados de servidor e cliente
- Etapa 2: criar um VPN endpoint de cliente
- Etapa 3: associar uma rede de destino
- Etapa 4: Adicionar uma regra de autorização para o VPC
- Etapa 5: conceder acesso à Internet
- Etapa 6: verificar os requisitos do grupo de segurança
- Etapa 7: Baixar o arquivo de configuração do VPN endpoint do cliente
- Etapa 8: Conectar-se ao VPN endpoint do cliente

Pré-requisitos

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

- As permissões necessárias para trabalhar com VPN endpoints do cliente.
- As permissões necessárias para importar certificados no AWS Certificate Manager.
- A VPC com pelo menos uma sub-rede e um gateway de 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, o Cliente VPN usa certificados para realizar a autenticação entre os clientes e o VPN endpoint 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 AWS Certificate Manager (ACM) e especificado quando você criar o VPN endpoint do cliente. Importar o certificado do cliente para ACM é opcional.

Se você ainda não tiver certificados para usar para essa finalidade, eles podem ser criados usando o utilitário Open VPN easy-rsa. Para obter etapas detalhadas para gerar os certificados e chaves do servidor e do cliente usando o utilitário Open VPN easy-rsa e importá-los para o see. ACM Autenticação mútua em AWS Client VPN

> **Note**
>
> O certificado do servidor deve ser provisionado ou importado para AWS Certificate Manager (ACM) na mesma AWS região em que você criará o endpoint do clienteVPN.

Etapa 2: criar um VPN endpoint de cliente

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

Para criar um VPN endpoint de cliente

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

2. No painel de navegação, escolha Client VPN Endpoints e, em seguida, escolha Create Client VPN endpoint.
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o VPN endpoint do cliente.
4. Para Cliente IPv4 CIDR, especifique um intervalo de endereços IP, em CIDR notação, a partir do qual atribuir endereços IP do cliente.

   > **Note**
   >
   > O intervalo de endereços não pode se sobrepor ao intervalo de endereços da rede de destino, ao intervalo de VPC endereços ou a qualquer uma das rotas que serão associadas ao VPN endpoint do Cliente. O intervalo de endereços do cliente deve ter no mínimo /22 e não maior que o tamanho do CIDR bloco /12. Você não pode alterar o intervalo de endereços do cliente depois de criar o VPN endpoint do cliente.

5. ARNEm Certificado ARN de servidor, selecione o certificado do servidor que você gerou na Etapa 1.
6. Em Opções de autenticação, escolha Usar autenticação mútua e, em Certificado ARN do cliente ARN, selecione o certificado que você deseja usar como certificado do cliente.

   Se os certificados do servidor e do cliente forem assinados pela mesma autoridade de certificação (CA), você terá a opção de especificar o certificado do servidor ARN para os certificados do cliente e do servidor. Nesse cenário, qualquer certificado do cliente que corresponda ao certificado do servidor pode ser usado para autenticar.
7. (Opcional) Especifique quais DNS servidores usar para DNS resolução. Para usar DNS servidores personalizados, para endereço IP DNS do Servidor 1 e Endereço IP DNS do Servidor 2, especifique os endereços IP dos DNS servidores a serem usados. Para usar o VPC DNS servidor, para o endereço IP DNS do Servidor 1 ou o endereço IP DNS do Servidor 2, especifique os endereços IP e adicione o endereço IP VPC DNS do servidor.

   > **Note**
   >
   > Verifique se os DNS servidores podem ser acessados pelos clientes.

8. Mantenha o restante das configurações padrão e escolha Criar VPN endpoint do cliente.

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

Para obter mais informações sobre as opções que você pode especificar para um VPN endpoint do cliente, consulteCrie um AWS Client VPN endpoint.

Etapa 3: associar uma rede de destino

Para permitir que os clientes estabeleçam uma VPN sessão, você associa uma rede de destino ao VPN endpoint do cliente. Uma rede de destino é uma sub-rede em umVPC.

Para associar uma rede de destino ao VPN endpoint do cliente

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente que você criou no procedimento anterior e escolha Associações de rede de destino, Associar rede de destino.
4. Para VPC, escolha o local VPC em que a sub-rede está localizada.
5. Em Escolha uma sub-rede para associar, escolha a sub-rede a ser associada ao endpoint do clienteVPN.
6. SelecioneAssociate target network (Associar rede de destino).
7. Se as regras de autorização permitirem, uma associação de sub-rede será suficiente para que os clientes acessem toda VPC a rede. É possível associar outras sub-redes para fornecer alta disponibilidade caso uma zona de disponibilidade tenha algum problema.

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

- O estado do VPN endpoint do cliente muda para`available`. Agora, os clientes podem estabelecer uma VPN conexão, mas não podem acessar nenhum recurso no VPC até que você adicione as regras de autorização.
- A rota local do VPC é adicionada automaticamente à tabela de rotas do VPN endpoint do cliente.
- O grupo VPC de segurança padrão do é aplicado automaticamente ao VPN endpoint do cliente.

Etapa 4: Adicionar uma regra de autorização para o VPC

Para que os clientes acessem oVPC, é necessário que haja uma rota para o VPC na tabela de rotas do VPN endpoint do cliente e uma regra de autorização. A rota já foi adicionada automaticamente na etapa anterior. Para este tutorial, queremos conceder a todos os usuários acesso aoVPC.

Para adicionar uma regra de autorização para o VPC

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual adicionar a regra de autorização. Escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
4. Para que a Rede de destino habilite o CIDR acesso, insira a rede para a qual você deseja permitir o acesso. Por exemplo, para permitir o acesso ao todoVPC, especifique o IPv4 CIDR bloco doVPC.
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 fornecer acesso a redes adicionais conectadas aoVPC, como AWS serviços, redes com peeringVPCs, redes locais e Internet. Para cada rede adicional, você adiciona uma rota à rede na tabela de rotas do VPN endpoint do cliente e configura uma regra de autorização para dar acesso aos clientes.

Para este tutorial, queremos conceder a todos os usuários acesso à Internet e também aoVPC. Você já configurou o acesso aoVPC, então esta etapa é para acesso à Internet.

Como conceder acesso à Internet

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint 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 VPN endpoint do cliente na Etapa 2. Isso significa que o grupo de segurança padrão do VPC é aplicado automaticamente ao VPN endpoint do Cliente quando uma rede de destino é associada. Como resultado, o grupo de segurança padrão do agora VPC deve estar associado ao VPN endpoint do Cliente.

Verificar os requisitos de grupo de segurança a seguir

- O fato de o grupo de segurança associado à sub-rede pela qual você está roteando o tráfego (nesse caso, o grupo de VPC segurança padrão) permite 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`.
- Que os grupos de segurança dos recursos em seu VPC tenham uma regra que permita o acesso do grupo de segurança aplicado ao VPN endpoint do Cliente (nesse caso, o grupo de VPC segurança padrão). Isso permite que seus clientes acessem os recursos em seuVPC.

Para obter mais informações, consulte Grupos de segurança.

Etapa 7: Baixar o arquivo de configuração do VPN endpoint do cliente

A próxima etapa é baixar e preparar o arquivo de configuração do VPN endpoint do cliente. O arquivo de configuração inclui os detalhes do VPN endpoint do cliente e as informações do certificado necessárias para estabelecer uma VPN conexão. Você fornece esse arquivo aos usuários finais que precisam se conectar ao VPN endpoint do Cliente. O usuário final usa o arquivo para configurar seu aplicativo VPN cliente.

Para baixar e preparar o arquivo de configuração do VPN endpoint do cliente

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente que você criou para este tutorial e escolha Baixar a configuração do cliente.
4. Localize o certificado de cliente e a chave que foram gerados na etapa 1. O certificado e a chave do cliente podem ser encontrados nos seguintes locais no repositório clonado do Open VPN 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 VPN endpoint do cliente 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. Salve e feche o arquivo de configuração do VPN endpoint do cliente.
7. Distribua o arquivo de configuração do VPN endpoint do cliente para seus usuários finais.

Para obter mais informações sobre o arquivo de configuração do VPN endpoint do cliente, consulteAWS Client VPN exportação do arquivo de configuração do endpoint.

Etapa 8: Conectar-se ao VPN endpoint do cliente

Você pode se conectar ao VPN endpoint do cliente usando o cliente AWS fornecido ou outro aplicativo cliente VPN baseado em Open e o arquivo de configuração que você acabou de criar. Para obter mais informações, consulte o Guia do usuário do AWS Client VPN.

Trabalhe com AWS Client VPN

Os tópicos a seguir explicam as principais tarefas administrativas necessárias para trabalhar com o ClienteVPN:

- Acesse o portal de autoatendimento — configure o acesso ao portal de VPN autoatendimento do cliente para que os próprios clientes possam baixar o arquivo de configuração do VPN endpoint do cliente. Para obter informações sobre como acessar o portal de autoatendimento, consultethe section called “Acesso ao portal de autoatendimento”.
- Regras de autorização — adicione regras de autorização para controlar o acesso do cliente às redes especificadas. Para obter informações sobre como adicionar regras de autorização, consultethe section called “Regras de autorização”.
- Listas de revogação de certificados de clientes — Use listas de revogação de certificados de clientes para revogar o acesso a um endpoint de cliente. VPN Para obter informações sobre listas de revogação de certificados de clientes, consulte. the section called “Listas de revogação de certificados de cliente”
- Conexões do cliente — Visualize ou encerre uma conexão do cliente com um VPN endpoint do cliente. Para obter informações sobre como visualizar ou encerrar uma conexão de cliente, consultethe section called “Conexões de cliente”.
- Banner de login do cliente — Adicione um banner de texto em um aplicativo de VPN desktop do cliente quando uma VPN sessão for estabelecida. Você pode usar o banner de texto para atender às suas necessidades regulatórias e de conformidade. Para obter informações sobre banners de login, consultethe section called “Banners de login de clientes”.
- VPNEndpoints do cliente — configure os VPN endpoints do cliente para gerenciar e controlar todas as VPN sessões. Para obter informações sobre a configuração de endpoints, consulte. the section called “Endpoints”
- Registros de conexão — Ative o registro de conexão para VPN endpoints de cliente novos ou existentes para começar a capturar registros de conexão. Para obter informações sobre o registro de conexão, consultethe section called “Logs de conexão”.
- Exportação do arquivo de configuração do cliente — Configure o arquivo de configuração do cliente que VPN os clientes do cliente precisam para estabelecer VPN conexões. Depois de configurar o arquivo, baixe-o (exporte-o) para distribuição aos clientes. Para obter mais informações sobre a exportação de um arquivo de configuração do cliente, consultethe section called “Exportação do arquivo de configuração do cliente”.

- Rotas — Configure as regras de autorização para cada VPN rota do cliente para especificar quais clientes têm acesso à rede de destino. Para obter informações sobre como configurar regras de autorização, consulte the section called “Regras de autorização”
- Redes de destino — associe as redes de destino a um VPN endpoint do cliente para permitir que os clientes se conectem a ele e estabeleçam uma VPN conexão. Para obter informações sobre redes de destino, consultethe section called “Redes de destino”.
- Duração máxima da VPN sessão — defina opções para a duração máxima da VPN sessão para atender aos seus requisitos de segurança e conformidade. Para obter informações sobre a duração máxima da VPN sessão, consultethe section called “Duração máxima VPN da sessão”.

AWS Client VPN acesso ao portal de autoatendimento

Se você habilitou o portal de autoatendimento para seu VPN endpoint de cliente, poderá fornecer a seus clientes um portal de autoatendimento. URL 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 do VPN endpoint do cliente e podem baixar a versão mais recente do cliente AWS fornecido.

As seguintes regras se aplicam:

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

Depois de habilitar a opção de portal de autoatendimento, forneça aos seus clientes uma das seguintes opções: URLs

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

Se os clientes acessarem o portal usando issoURL, eles deverão inserir a ID do VPN endpoint do Cliente antes de poderem fazer login.

- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Substituir *<endpoint-id>* no anterior URL com o ID do seu VPN endpoint do cliente, por exemplo,. `cvpn-endpoint-0123456abcd123456`

Você também pode visualizar o URL para o portal de autoatendimento na saída do describe-client-vpn-endpoints AWS CLI comando. Como alternativa, o URL está disponível na guia Detalhes na página Client VPN Endpoints no VPC console da Amazon.

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

AWS Client VPN 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. Você pode adicionar regras de autorização a um VPN endpoint do cliente usando o console e o. AWS CLI

> **Note**
>
> O cliente VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização. Consulte o tópico de solução de problemas Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado e a prioridade da rota no Guia VPC do usuário da Amazon para obter mais detalhes.

Pontos-chave para entender as regras de autorização

Os seguintes pontos explicam alguns dos comportamentos das regras de autorização:

- Para permitir o acesso a uma rede de destino, é necessário adicionar explicitamente uma regra de autorização. O comportamento padrão é negar acesso.
- Você não pode adicionar uma regra de autorização para restringir acesso a uma rede de destino.

- `0.0.0.0/0`CIDRÉ tratado como um estojo especial. Ele é processado por último, independentemente da ordem na qual as regras de autorização foram criadas.
- Isso `0.0.0.0/0` CIDR pode ser considerado como “qualquer destino” ou “qualquer destino não definido por outras regras de autorização”.
- A correspondência de prefixo mais longo é a regra que tem precedência.

Tópicos

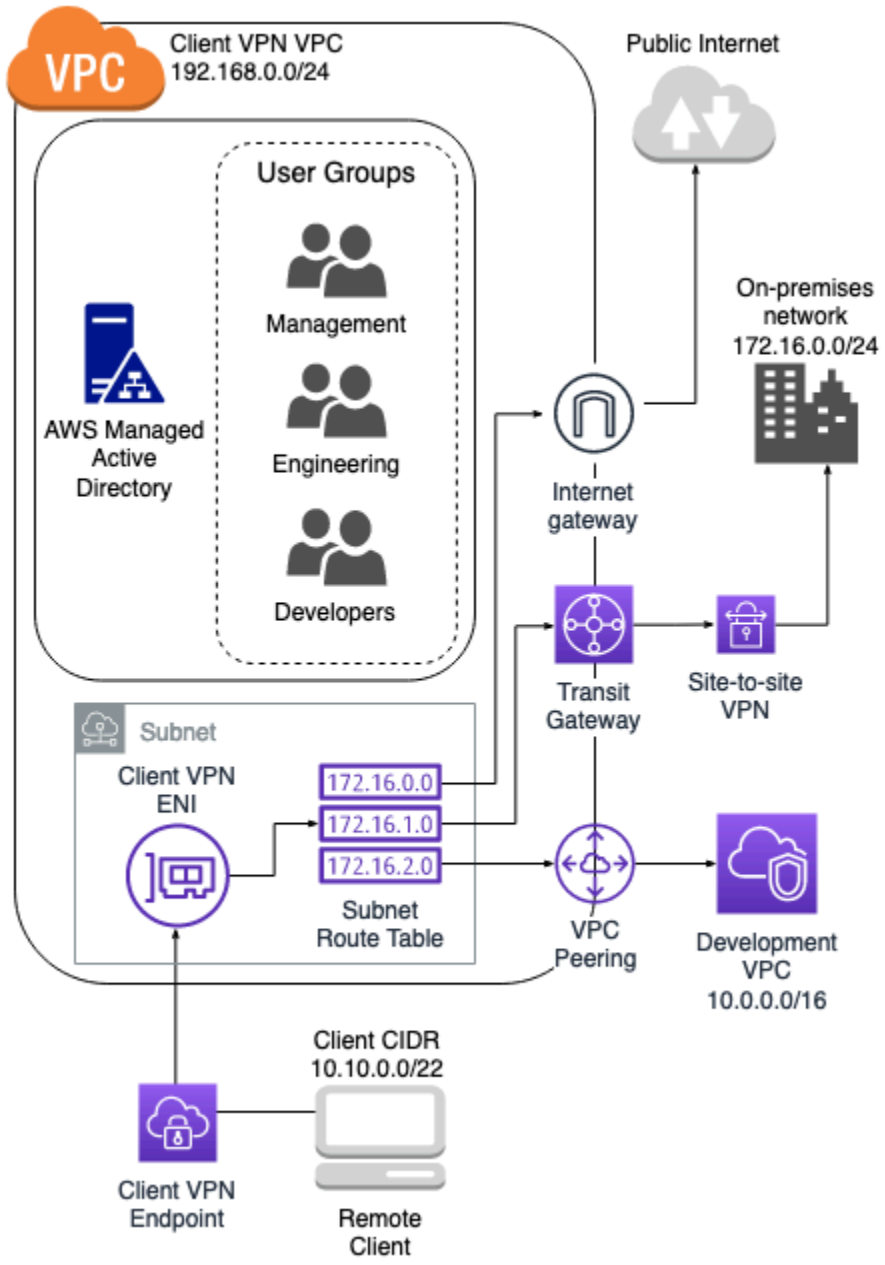
Cenários de exemplo para regras de VPN autorização do cliente

Esta seção descreve como as regras de autorização funcionam para AWS Client VPN. Ela inclui pontos-chave para entender as regras de autorização, um exemplo de arquitetura e uma discussão sobre cenários que correspondem à arquitetura de exemplo.

Cenários

Exemplo de arquitetura para cenários de regras de autorização

O diagrama a seguir mostra a arquitetura de exemplo usada para os cenários encontrados nesta seção.



Acesso a um único destino

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Forneça acesso ao desenvolvimento para grupos de desenvolv imento VPC	S-xxxxx15	Falso	10.0.0.0/16
Forneça acesso ao grupo de gerentes ao Cliente VPN VPC	S-xxxxx16	Falso	192.168.0.0/24

Comportamento resultante

- O grupo de engenharia só pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento só pode acessar `10.0.0.0/16`.
- O grupo de gerentes só pode acessar `192.168.0.0/24`.
- Todos os outros tráfegos são descartados pelo VPN endpoint do cliente.

> **Note**
>
> Nesse cenário, nenhum grupo de usuários tem acesso à Internet pública.

Use qualquer destino (0.0.0.0/0) CIDR

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Forneça acesso ao desenvolvimento para grupos de desenvolvimento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0

Comportamento resultante

- O grupo de engenharia só pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento só pode acessar `10.0.0.0/16`.
- O grupo de gerentes pode acessar a Internet pública e `192.168.0.0/24`, mas não pode acessar `172.16.0.0/24` nem `10.0.0.0/16`.

> **Note**
>
> Nesse cenário, como nenhuma regra está se referindo a `192.168.0.0/24`, o acesso a essa rede também é fornecido pela regra `0.0.0.0/0`.
> Uma regra com `0.0.0.0/0` é sempre avaliada por último, independentemente da ordem em que as regras foram criadas. Por esse motivo, lembre-se de que as regras avaliadas antes de `0.0.0.0/0` desempenham um papel na determinação das redes às quais `0.0.0.0/0` concede acesso.

Correspondência de prefixo IP mais longa

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Forneça acesso ao desenvolvimento para grupos de desenvolvimento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes a um único host em desenvolvimento VPC	S-xxxxx16	Falso	10.0.2.119/32

Comportamento resultante

- O grupo de engenharia só pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública e um único host (`10.0.2.119/32`) dentro do desenvolvimentoVPC, mas não tem acesso `172.16.0.0/24` nem a nenhum dos hosts restantes no desenvolvimentoVPC. `192.168.0.0/24`

> **Note**
>
> Aqui, você vê como uma regra com um prefixo de IP mais longo tem precedência sobre uma regra com um prefixo de IP mais curto. Se você quiser que o grupo de desenvolvimento

tenha acesso a `10.0.2.119/32`, é necessário adicionar mais uma regra que conceda à equipe de desenvolvimento acesso a `10.0.2.119/32`.

Sobreposição CIDR (mesmo grupo)

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Forneça acesso ao desenvolvimento para grupos de desenvolv imento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes a um único host em desenvolvimento VPC	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a uma sub-rede menor na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia tem acesso a `172.16.0.0/24`, inclusive à sub-rede mais específica `172.16.0.128/25`.

Regra 0.0.0.0/0 adicional

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Forneça acesso ao desenvolvimento para grupos de desenvolvimento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes a um único host em desenvolvimento VPC	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a	S-xxxxx14	Falso	172.16.0.128/25

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
uma sub-rede menor na rede on-premises			
Fornecer ao grupo de engenharia acesso a qualquer destino	S-xxxxx14	Falso	0.0.0.0/0

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `192.168.0.0/24` e `172.16.0.0/24`, inclusive a sub-rede mais específica `172.16.0.128/25`.

> **Note**
>
> Observe que os grupos de engenharia e de gerentes agora podem acessar `192.168.0.0/24`. Isso ocorre porque os dois grupos têm acesso a `0.0.0.0/0` (qualquer destino) e nenhuma outra regra está fazendo referência a `192.168.0.0/24`.

Adicione uma regra para 192.168.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Forneça acesso ao desenvolvimento para grupos de desenvolvimento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes a um único host em desenvolvimento VPC	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a uma sub-rede na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25
Fornecer ao grupo de engenharia acesso a qualquer destino	S-xxxxx14	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes ao Cliente VPN VPC	S-xxxxx16	Falso	192.168.0.0/24

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.

- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `172.16.0.0/24` e `172.16.0.128/25`.

> **Note**
>
> Observe que a adição da regra para o grupo de gerentes acessar`192.168.0.0/24` faz com que o grupo de desenvolvimento não tenha mais acesso a essa rede de destino.

Acesso para todos os grupos de usuários

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Forneça acesso ao desenvolvimento para grupos de desenvolv imento VPC	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes a um único host em desenvolvimento VPC	S-xxxxx16	Falso	10.0.2.119/32

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	Destino CIDR
Fornecer ao grupo de engenharia acesso a uma sub-rede na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25
Fornecer ao grupo de engenharia acesso a todas as redes	S-xxxxx14	Falso	0.0.0.0/0
Forneça acesso ao grupo de gerentes ao Cliente VPN VPC	S-xxxxx16	Falso	192.168.0.0/24
Fornecer acesso a todos os grupos	N/D	Verdadeiro	0.0.0.0/0

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `172.16.0.0/24` e `172.16.0.128/25`.
- Qualquer outro grupo de usuários, por exemplo, “grupo de administradores”, pode acessar a Internet pública, mas nenhuma outra rede de destino definida nas outras regras.

Adicionar uma regra de autorização a um AWS Client VPN endpoint

Você pode adicionar uma regra de autorização a um VPN endpoint do cliente usando o. AWS Management Console

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

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual adicionar a regra de autorização, escolha Regras de autorização e escolha Adicionar regra de autorização.
4. Para que a rede de destino habilite o acesso, insira o endereço IP, em CIDR nota, da rede que você deseja que os usuários acessem (por exemplo, o CIDR bloco da suaVPC).
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 SAML baseado (IdP).
     - (Active Directory) Para obter oSID, você pode usar o ADGroup cmdlet Get- 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 SAML baseada) O ID/nome do grupo deve corresponder às informações do atributo do grupo retornadas na declaração. SAML
6. Em Descrição, insira uma breve descrição da regra de autorização.
7. Escolha Adicionar regra de autorização.

Para adicionar uma regra de autorização a um VPN endpoint do cliente ()AWS CLI

Use o authorize-client-vpn-ingresscomando.

Remover uma regra de autorização de um AWS Client VPN endpoint

Você pode remover as regras de autorização de um VPN endpoint de cliente específico usando o console e o. AWS CLI

Para remover as regras de autorização (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual a regra de autorização foi adicionada e, em seguida, escolha Regras de autorização.
4. Selecione a regra de autorização a ser excluída, escolha Remover regra de autorização e, em seguida, escolha Remover regra de autorização novamente para confirmar a exclusão.

Para remover as regras de autorização (AWS CLI)

Use o revoke-client-vpn-ingresscomando.

Exibir regras AWS Client VPN de autorização

Você pode visualizar as regras de autorização para um VPN endpoint de cliente específico usando o console e o. AWS CLI

Para visualizar regras de autorização (console)

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

Para visualizar regras de autorização (AWS CLI)

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

AWS Client VPN listas de revogação de certificados de clientes

As listas de revogação de certificados de VPN cliente cliente são usadas para revogar o acesso a um VPN endpoint de cliente para certificados de cliente específicos. Você pode gerar a lista de revogação, bem como importar uma lista existente ou exportar sua lista atual como um arquivo de lista de revogação. A geração de uma lista é realizada usando o VPN software Open no Linxu/macOS ou no Windows. A importação e exportação podem ser feitas usando o Amazon VPC Console ou usando o. AWS CLI

> **Note**
>
> Para obter mais informações sobre como gerar os certificados e as chaves de servidor e cliente, consulte Autenticação mútua em AWS Client VPN

Você pode adicionar somente um número limitado de entradas à lista de revogação de certificados de clientes. Para obter mais informações sobre o número de entradas que você pode adicionar a uma lista de revogação, consulte. VPNCotas de clientes

Tarefas

- Gere uma lista de revogação de certificados de AWS Client VPN clientes
- Importar uma lista de revogação de certificados de AWS Client VPN cliente
- Exportar uma AWS Client VPN lista de revogação de certificados de cliente

Gere uma lista de revogação de certificados de AWS Client VPN clientes

Linux/macOS

No procedimento a seguir, você gera uma lista de revogação de certificados de cliente usando o utilitário de linha de comando Open VPN easy-rsa.

Para gerar uma lista de revogação de certificados de clientes usando o Open easy-rsa VPN

1. Faça login no servidor que hospeda a instalação do easyrsa usada para gerar o certificado.
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 client1.domain.tld
$ ./easyrsa gen-crl
```

Digite `yes` quando solicitado.

Windows

O procedimento a seguir usa o VPN software Open para gerar uma lista de revogação de clientes. Ele pressupõe que você seguiu as etapas de uso do VPN software Open para gerar os certificados e chaves do cliente e do servidor.

Para gerar uma lista de revogação de certificados de clientes usando a versão 3.x.x do Easy RSA

1. Abra um prompt de comando e navegue até o diretório Easy RSA -3.x.x, que dependerá de onde ele está instalado em seu sistema.

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

2. Execute o `EasyRSA-Start.bat` arquivo para iniciar o RSA shell Easy.

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

3. No RSA shell Easy, revogue o certificado do cliente.

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

4. Digite `yes` 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 clientes usando versões anteriores do Easy RSA

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

```
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 AWS Client VPN cliente

Você deve ter um arquivo de lista de revogação de certificados de VPN cliente cliente para importar. Para obter mais informações sobre como gerar uma lista de revogação de certificados de cliente, consulte Gere uma lista de revogação de certificados de AWS Client VPN clientes.

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 VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente para o qual importar a lista de revogação de certificados do cliente.
4. Escolha Ações e escolha Importar certificado do cliente CRL.
5. Em Lista de revogação de certificados, insira o conteúdo do arquivo da lista de revogação de certificados do cliente e escolha Importar certificado do cliente. CRL

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

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

```
$ 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 AWS Client VPN lista de revogação de certificados de cliente

Você pode exportar listas de revogação de certificados de VPN clientes clientes usando o console e o. AWS CLI

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

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

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

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

AWS Client VPN conexões de clientes

AWS Client VPN conexões são VPN sessões ativas que foram estabelecidas pelos clientes em um VPN endpoint específico do cliente, bem como conexões que foram encerradas nos últimos 60 minutos para esse endpoint. Uma conexão é estabelecida quando um cliente se conecta com sucesso a um VPN endpoint do cliente. O encerramento de uma sessão encerra a conexão do cliente com o VPN endpoint do cliente.

Você pode visualizar e encerrar as VPN conexões do cliente. A visualização das informações de conexão retorna informações como o endereço IP atribuído pelo intervalo de CIDR blocos do cliente, o ID do endpoint e o carimbo de data/hora. O encerramento de uma sessão encerra a VPN conexão especificada com o endpoint. A visualização e o encerramento das sessões podem ser feitos usando o Amazon VPC Console ou o. AWS CLI Se você não conseguir se conectar ao endpoint, e dependendo do erro, consulte Solução de problemas as etapas a serem seguidas para resolver o problema.

Tarefas

- Exibir conexões de AWS Client VPN clientes
- Encerrar uma conexão de AWS Client VPN cliente

Exibir conexões de AWS Client VPN clientes

Você pode visualizar as VPN conexões ativas do cliente usando o Amazon VPC Console ou AWS CLI o.

Para visualizar as conexões VPN cliente-cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente para o qual visualizar as conexões do cliente.
4. Escolha a guia Connections (Conexões). A guia Connections (Conexões) lista todas as conexões de clientes ativas e encerradas.

Para ver as conexões VPN cliente-cliente (AWS CLI)

Use o describe-client-vpn-connectionscomando.

Encerrar uma conexão de AWS Client VPN cliente

Você pode encerrar uma conexão de VPN cliente cliente usando o Amazon VPC Console ou o. AWS CLI

Para encerrar uma conexão VPN cliente-cliente (console)

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

Para encerrar uma conexão VPN cliente-cliente ()AWS CLI

Use o terminate-client-vpn-connectionscomando.

AWS Client VPN banners de login de clientes

AWS Client VPN fornece a opção de exibir um banner de texto nos aplicativos de VPN desktop do Cliente AWS fornecidos quando uma VPN sessão é estabelecida. Você pode definir o conteúdo do banner de texto de modo a atender às suas necessidades regulamentares e de conformidade. Um máximo de 1400 a UTF 8 caracteres codificados podem ser usados.

> **Note**
>
> Quando um banner de login do cliente for ativado, ele será exibido somente nas VPN sessões recém-criadas. VPNAs sessões existentes não são interrompidas, embora o banner seja exibido quando uma sessão existente for restabelecida.

Consulte as notas de versão do cliente AWS fornecido no Guia do AWS Client VPN usuário para obter detalhes sobre os aplicativos de desktop do cliente.

Criação de banners

Os banners de login são inicialmente criados e ativados durante a criação do VPN endpoint do cliente. Para obter as etapas para ativar um banner de login do cliente durante a criação de um VPN endpoint do cliente, consulteCrie um AWS Client VPN endpoint.

Tarefas

- Configurar um banner de login do cliente para um AWS Client VPN endpoint existente
- Desativar um banner de login do cliente para um endpoint existente AWS Client VPN
- Modificar o texto do banner existente em um AWS Client VPN endpoint
- Exibir um banner de AWS Client VPN login atualmente configurado

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

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

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

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente que você deseja modificar, escolha Ações e, em seguida, escolha Modificar VPN endpoint do cliente.
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. Para o texto do banner de login do cliente, insira o texto que será exibido em um banner nos clientes AWS fornecidos quando uma VPN sessão for estabelecida. Use somente UTF -8 caracteres codificados, com um máximo de 1400 caracteres permitidos.
7. Escolha Modificar VPN endpoint do cliente.

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

Use o modify-client-vpn-endpointcomando.

Desativar um banner de login do cliente para um endpoint existente AWS Client VPN

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

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

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente que você deseja modificar, escolha Ações e, em seguida, escolha Modificar VPN endpoint 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 Modificar VPN endpoint do cliente.

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

Use o modify-client-vpn-endpointcomando.

Modificar o texto do banner existente em um AWS Client VPN endpoint

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

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

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

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

Use o modify-client-vpn-endpointcomando.

Exibir um banner de AWS Client VPN login atualmente configurado

Use as etapas a seguir para visualizar um banner de login de cliente VPN cliente atualmente configurado.

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

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente que você 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).

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

Use o describe-client-vpn-endpointscomando.

AWS Client VPN endpoints

Todas as AWS Client VPN sessões estabelecem comunicação com um VPN endpoint do cliente. Você pode gerenciar o VPN endpoint do cliente para criar, modificar, visualizar e excluir VPN sessões do cliente com esse endpoint. Os endpoints podem ser criados e modificados usando o Amazon VPC Console ou usando o. AWS CLI

Requisitos para criar VPN endpoints de clientes

> **Important**
>
> Um VPN endpoint de cliente deve ser criado na mesma AWS conta na qual a rede de destino pretendida é provisionada. Você também precisará gerar um certificado de servidor e, se necessário, um certificado de cliente. Para obter mais informações, consulte Autenticação do cliente em AWS Client VPN.

Antes de começar, faça o seguinte:

- Revise as regras e as limitações em Regras e melhores práticas de uso AWS Client VPN.
- Gere o certificado do servidor e, se necessário, o certificado do cliente. Para obter mais informações, consulte Autenticação do cliente em AWS Client VPN.

Modificação do endpoint

Depois que um cliente VPN for criado, você poderá 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 DNS servidores
- A opção de túnel dividido

- Rotas (ao usar a opção de túnel dividido)
- Lista de revogação de certificados () CRL
- Regras de autorização
- As VPC e associações de grupos de segurança
- O número VPN da porta
- A opção do portal de autoatendimento
- A duração máxima VPN da sessão
- Habilitar ou desabilitar o texto do banner de login do cliente
- Texto do banner de login do cliente

> **Note**
>
> As modificações nos VPN endpoints do Cliente, incluindo alterações na Lista de Revogação de Certificados (CRL), entrarão em vigor até 4 horas após a solicitação ser aceita pelo serviço ao Cliente. VPN
> Você não pode modificar o IPv4 CIDR intervalo de clientes, as opções de autenticação, o certificado do cliente ou o protocolo de transporte após a criação do VPN endpoint do cliente.

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

- O certificado de servidor
- Os DNS servidores
- 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 VPN da porta

Tarefas

- Crie um AWS Client VPN endpoint
- Exibir AWS Client VPN endpoints

- Modificar um AWS Client VPN endpoint
- Excluir um AWS Client VPN endpoint

Crie um AWS Client VPN endpoint

Crie um VPN endpoint de cliente para permitir que seus clientes estabeleçam uma VPN sessão usando o Amazon VPC Console ou o. AWS CLI

Antes de criar um endpoint, familiarize-se com os requisitos. Para obter mais informações sobre os requisitos de endpoints, consultethe section called “Requisitos para criar VPN endpoints de clientes”.

Para criar um VPN endpoint de cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints e, em seguida, escolha Create Client VPN Endpoint.
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o VPN endpoint do cliente.
4. Para Cliente IPv4 CIDR, especifique um intervalo de endereços IP, em CIDR notação, a partir do qual 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 VPC endereços ou a qualquer uma das rotas que serão associadas ao VPN endpoint do Cliente. O intervalo de endereços do cliente deve ter no mínimo /22 e não maior que o tamanho do CIDR bloco /12. Você não pode alterar o intervalo de endereços do cliente depois de criar o VPN endpoint do cliente.

5. Em Certificado de servidor ARN, especifique o ARN TLS certificado a ser usado pelo servidor. Os clientes usam o certificado do servidor para autenticar o VPN endpoint do cliente ao qual estão se conectando.

   > **Note**
   >
   > O certificado do servidor deve estar presente em AWS Certificate Manager (ACM) na região em que você está criando o VPN endpoint do cliente. O certificado pode ser provisionado ACM ou importado para o. ACM

6. Especifique o método de autenticação a ser usado para autenticar clientes quando eles estabelecem uma VPN conexão. 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 essa opção para autenticação federada SAML baseada.

       Para SAMLprovedor ARN, especifique o ARN do provedor de IAM SAML identidade.

       (Opcional) Para SAMLprovedor de autoatendimento ARN, especifique o provedor ARN de IAM SAML identidade que você criou para oferecer suporte ao portal de autoatendimento, se aplicável.
   - Para usar a autenticação de certificado mútuo, selecione Usar autenticação mútua e, em Certificado do cliente ARN, especifique o certificado ARN do cliente que está provisionado em 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 certificado de servidor tanto ARN para servidor quanto para cliente. Se o certificado do cliente tiver sido emitido por uma CA diferente, o certificado do cliente ARN deverá ser especificado.

7. (Opcional) Para registro 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 CloudWatch registros de registros, insira o nome do grupo de registros a ser usado. Em Nome do fluxo de CloudWatch registros, insira o nome do fluxo de registros a ser usado ou deixe essa opção em branco para que possamos criar um fluxo de registros para você.
8. (Opcional) Para o Client Connect Handler, ative Habilitar o gerenciador de conexão do cliente para executar um código personalizado que permite ou nega uma nova conexão com o endpoint do cliente. VPN Para o Client Connect Handler ARN, especifique o Amazon Resource Name (ARN) da função Lambda que contém a lógica que permite ou nega conexões.
9. (Opcional) Especifique quais DNS servidores usar para DNS resolução. Para usar DNS servidores personalizados, para endereço IP DNS do Servidor 1 e Endereço IP DNS do

Servidor 2, especifique os endereços IP dos DNS servidores a serem usados. Para usar o VPC DNS servidor, para o endereço IP DNS do Servidor 1 ou o endereço IP DNS do Servidor 2, especifique os endereços IP e adicione o endereço IP VPC DNS do servidor.

> **Note**
>
> Verifique se os DNS servidores podem ser acessados pelos clientes.

10. (Opcional) Por padrão, o VPN endpoint do cliente usa o protocolo de UDP transporte. Para usar o protocolo de TCP transporte em vez disso, em Protocolo de Transporte, selecione TCP.

> **Note**
>
> UDPnormalmente oferece melhor desempenho do queTCP. Você não pode alterar o protocolo de transporte depois de criar o VPN endpoint do cliente.

11. (Opcional) Para que o endpoint seja um endpoint de cliente VPN de túnel dividido, ative Habilitar túnel dividido. Por padrão, o túnel dividido em um VPN endpoint do cliente está desativado.
12. (Opcional) Em VPCID, escolha a VPC para associar ao VPN endpoint do cliente. Para Grupo de segurança IDs, escolha um ou mais dos grupos de segurança VPC do para aplicar ao VPN endpoint do cliente.
13. (Opcional) Em VPNporta, escolha o número da VPN porta. O padrão é 443.
14. (Opcional) Para gerar um portal de autoatendimento URL para clientes, ative Habilitar portal de autoatendimento.
15. (Opcional) Em Horas de tempo limite da sessão, escolha o tempo máximo desejado de duração da VPN sessão em horas entre 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). Para o texto do banner de login do cliente, insira o texto que será exibido em um banner nos clientes AWS fornecidos quando uma VPN sessão for estabelecida. UTF-8 caracteres codificados somente. Máximo de 1400 caracteres.
17. Escolha Criar VPN endpoint do cliente.

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

- O estado inicial do VPN endpoint do cliente é`pending-associate`. Os clientes só podem se conectar ao VPN endpoint do cliente depois que você associar a primeira rede de destino.
- Crie uma regra de autorização para especificar quais clientes têm acesso à rede.
- Baixe e prepare o arquivo de configuração do VPN endpoint do cliente para distribuir aos seus clientes.
- Instrua seus clientes a usar o cliente AWS fornecido ou outro aplicativo cliente VPN baseado em Open para se conectar ao VPN endpoint do cliente. Para obter mais informações, consulte o Guia do usuário do AWS Client VPN.

Para criar um VPN endpoint de cliente ()AWS CLI

Use o create-client-vpn-endpointcomando.

Exibir AWS Client VPN endpoints

Você pode visualizar informações sobre VPN endpoints do cliente usando o Amazon VPC Console ou o. AWS CLI

Para visualizar os VPN endpoints do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente a ser visualizado.
4. Use as guias Detalhes, Associações de rede de destino, Grupos de segurança, Regras de autorização, tabela de rotas, Conexões e Tags para visualizar informações sobre VPN endpoints de clientes existentes.

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

Para visualizar os VPN endpoints do cliente ()AWS CLI

Use o describe-client-vpn-endpointscomando.

Modificar um AWS Client VPN endpoint

Você pode modificar um VPN endpoint do cliente usando o Amazon VPC Console ou o. AWS CLI Para obter mais informações sobre os campos que você pode usar. VPN Campos do cliente que você pode modificar, consultethe section called “Modificação do endpoint”.

> **Note**
>
> As modificações nos VPN endpoints do Cliente, incluindo alterações na Lista de Revogação de Certificados (CRL), entrarão em vigor até 4 horas após a solicitação ser aceita pelo serviço ao Cliente. VPN
> Você não pode modificar o IPv4 CIDR intervalo de clientes, as opções de autenticação, o certificado do cliente ou o protocolo de transporte após a criação do VPN endpoint do cliente.

Para modificar um VPN endpoint do cliente (console)

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

   > **Note**
   >
   > O certificado do servidor deve estar presente em AWS Certificate Manager (ACM) na região em que você está criando o VPN endpoint do cliente. O certificado pode ser provisionado 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 Nome do grupo de CloudWatch registros de registros, selecione o nome do grupo de registros a ser usado. Em Nome do fluxo de CloudWatch registros, selecione o nome do fluxo de registros a ser usado ou deixe essa opção em branco para que possamos criar um fluxo de registros 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. Para o Client Connect Handler ARN, especifique o Amazon Resource Name (ARN) da função Lambda que contém a lógica que permite ou nega conexões.
8. Ative ou desative a opção Ativar DNS servidores. Para usar DNS servidores personalizados, para endereço IP DNS do Servidor 1 e Endereço IP DNS do Servidor 2, especifique os endereços IP dos DNS servidores a serem usados. Para usar o VPC DNS servidor, para o endereço IP DNS do Servidor 1 ou o endereço IP DNS do Servidor 2, especifique os endereços IP e adicione o endereço IP VPC DNS do servidor.

   > **Note**
   >
   > Verifique se os DNS servidores podem ser acessados pelos clientes.

9. Ative ou desative Enable split-tunnel (Habilitar túnel dividido). Por padrão, o túnel dividido em um VPN endpoint está desativado.
10. Em VPCID, escolha a VPC para associar ao VPN endpoint do cliente. Para Grupo de segurança IDs, escolha um ou mais dos grupos de segurança VPC do para aplicar ao VPN endpoint do cliente.
11. Em VPNporta, escolha o número da VPN porta. O padrão é 443.
12. Para gerar um portal de autoatendimento URL para clientes, ative Habilitar portal de autoatendimento.
13. Em Horas de tempo limite da sessão, escolha o tempo máximo desejado de duração da VPN sessão em horas a partir das 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 você quiser usar o banner de login do cliente, insira o texto que será exibido em um banner nos clientes AWS fornecidos quando uma VPN sessão for estabelecida. UTF-8 caracteres codificados somente. Máximo de 1400 caracteres.
15. Escolha Modificar VPN endpoint do cliente.

Para modificar um VPN endpoint do cliente ()AWS CLI

Use o modify-client-vpn-endpointcomando.

Excluir um AWS Client VPN endpoint

Você precisará desassociar todas as redes de destino antes de excluir um VPN endpoint do Cliente. Quando você exclui um VPN endpoint do cliente, seu estado é alterado `deleting` e os clientes não podem mais se conectar a ele.

Você pode excluir um VPN endpoint do cliente usando o console ou o. AWS CLI

Para excluir um VPN endpoint do cliente (console)

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

Para excluir um VPN endpoint do cliente ()AWS CLI

Use o delete-client-vpn-endpointcomando.

AWS Client VPN registros de conexão

Você pode ativar o registro de conexão para um VPN endpoint de cliente novo ou existente e começar a capturar registros de conexão. Os registros de conexão mostram a sequência de eventos de log para o VPN endpoint do cliente. Ao habilitar o registro em log de conexão, é possível especificar o nome de um stream de logs no grupo de logs. Se você não especificar um fluxo de log, o VPN serviço Client criará um para você. Em seguida, o registro de conexão registra as seguintes informações: solicitações de conexão do cliente, resultados da conexão do cliente (bem-sucedidos ou malsucedidos), motivos dos resultados malsucedidos da conexão e o horário de encerramento do cliente no endpoint.

Antes de começar, você precisa ter um grupo de CloudWatch registros de registros em sua conta. Para obter mais informações, consulte Como trabalhar com grupos de registros e fluxos de registros no Guia do usuário do Amazon CloudWatch Logs. Aplicam-se cobranças pelo uso do CloudWatch Logs. Para obter mais informações, consulte os CloudWatch preços da Amazon.

Os registros de VPN conexão do cliente podem ser criados usando o Amazon VPC Console ou AWS CLI o.

Tarefas

- Habilitar o registro em log de conexão para um novo endpoint do AWS Client VPN
- Habilitar o registro em log de conexão para um endpoint do AWS Client VPN existente
- Exibir registros de AWS Client VPN conexão
- Desativar o registro de AWS Client VPN conexão

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

Você pode ativar o registro de conexão ao criar um novo VPN endpoint de cliente usando o console ou a linha de comando.

Para habilitar o registro de conexão para um novo VPN endpoint do cliente usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints e, em seguida, escolha Create Client VPN endpoint.
3. Conclua as opções até chegar à seção Geração de logs de conexão . Para obter mais informações sobre essas opções, consulte Crie um AWS Client VPN endpoint.
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 CloudWatch registros de registros, escolha o nome do grupo de CloudWatch registros de registros.
6. (Opcional) Em Nome do fluxo de CloudWatch registros, escolha o nome do fluxo de CloudWatch registros.
7. Escolha Criar VPN endpoint do cliente.

Para habilitar o registro de conexão para um novo VPN endpoint do Cliente usando o AWS CLI

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

```
{
```

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

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

Você pode ativar o registro de conexão para um VPN endpoint de cliente existente usando o console ou a linha de comando.

Para habilitar o registro de conexão para um VPN endpoint de cliente existente usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente, escolha Ações e, em seguida, escolha Modificar VPN endpoint 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 CloudWatch registros de registros, escolha o nome do grupo de CloudWatch registros de registros.
6. (Opcional) Em Nome do fluxo de CloudWatch registros, escolha o nome do fluxo de CloudWatch registros.
7. Escolha Modificar VPN endpoint do cliente.

Para habilitar o registro de conexão para um VPN endpoint de cliente existente usando o AWS CLI

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

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

Exibir registros de AWS Client VPN conexão

Você pode ver seus registros de VPN conexão do cliente usando o console de CloudWatch registros.

Como visualizar os logs de conexão usando o console

1. Abra o CloudWatch console 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 fluxo de log para seu VPN endpoint do cliente.

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

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

Desativar o registro de AWS Client VPN conexão

Você pode desativar o registro de conexão para um VPN endpoint do cliente usando o console ou a linha de comando. Quando você desativa o registro de conexão, os registros de conexão existentes nos CloudWatch Registros não são excluídos.

Como desativar o log de conexão usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente, escolha Ações e, em seguida, escolha Modificar VPN endpoint 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 Modificar VPN endpoint do cliente.

Para desativar o registro de conexão usando o AWS CLI

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

AWS Client VPN exportação do arquivo de configuração do endpoint

O arquivo de configuração do AWS Client VPN endpoint é o arquivo que os clientes (usuários) usam para estabelecer uma VPN conexão com o VPN endpoint do cliente. Você deve baixar (exportar) esse arquivo e distribuí-lo a todos os clientes que precisam acessar VPN o. Como alternativa, se você habilitou o portal de autoatendimento para seu VPN endpoint de cliente, os clientes podem fazer login no portal e baixar o arquivo de configuração eles mesmos. Para obter mais informações, consulte AWS Client VPN acesso ao portal de autoatendimento.

Se o VPN endpoint do cliente usa autenticação mútua, você deve adicionar o certificado do cliente e a chave privada do cliente ao arquivo de configuração.ovpn que você baixou. Depois de adicionar as informações, os clientes podem importar o arquivo.ovpn para o software VPN cliente Open.

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

Por padrão, a opção “remote-random-hostname” na configuração do Open VPN Client ativa o caractere curingaDNS. Como o caractere curinga DNS está ativado, o cliente não armazena em cache o endereço IP do endpoint e você não poderá fazer ping no DNS nome do endpoint.

Se o VPN endpoint do cliente usar a autenticação do Active Directory e se você habilitar a autenticação multifator (MFA) no seu diretório depois de distribuir o arquivo de configuração do cliente, você deverá baixar um novo arquivo e redistribuí-lo aos seus clientes. Os clientes não podem usar o arquivo de configuração anterior para se conectar ao VPN endpoint do cliente.

Tarefas

- Exportar o arquivo de configuração do AWS Client VPN cliente
- Adicione o certificado AWS Client VPN do cliente e as principais informações para autenticação mútua

Exportar o arquivo de configuração do AWS Client VPN cliente

Você pode exportar a configuração do VPN cliente cliente usando o console ou AWS CLI o.

Para exportar configuração do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente para o qual baixar a configuração do cliente e escolha Baixar 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
```

Adicione o certificado AWS Client VPN do cliente e as principais informações para autenticação mútua

Se o VPN endpoint do cliente usa autenticação mútua, você deve adicionar o certificado do cliente e a chave privada do cliente ao arquivo de configuração.ovpn que você baixou.

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) Distribua o certificado e a chave do cliente aos clientes junto com o arquivo de configuração do VPN endpoint do cliente. 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. Substituir */path/* com a localização do certificado e da chave do cliente (a localização é relativa 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 e chaves de cliente separados para cada usuário que se conectará ao VPN endpoint do cliente, repita essa etapa para cada usuário.

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

```
client
dev tun
proto udp
remote 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
```

AWS Client VPN rotas

Cada AWS Client VPN endpoint tem uma tabela de rotas que descreve as rotas de rede de destino disponíveis. Cada rota na tabela de rotas determina para onde o tráfego de rede é direcionado. Você

deve configurar as regras de autorização para cada rota de VPN endpoint do cliente para especificar quais clientes têm acesso à rede de destino.

Quando você associa uma sub-rede de a a um VPC VPN endpoint do Client, uma rota para o VPC é automaticamente adicionada à tabela de rotas do VPN endpoint do Client. Para permitir o acesso a redes adicionais, como redes locais com peeringVPCs, 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 VPN endpoint do cliente.

> **Note**
>
> Se você estiver associando várias sub-redes ao VPN endpoint do cliente, certifique-se de criar uma rota para cada sub-rede, conforme descrito aqui. Solução de problemas AWS Client VPN: o acesso a um Amazon S3 VPC emparelhado ou à Internet é intermitente Cada sub-rede associada deve ter um conjunto idêntico de rotas.

Considerações sobre o uso de túnel dividido em endpoints do cliente VPN

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

Recomendamos que você contabilize o número de rotas que o dispositivo cliente pode manipular antes de modificar a tabela de rotas do VPN endpoint do cliente.

Tarefas

- Crie uma rota AWS Client VPN de endpoint
- Exibir AWS Client VPN rotas de endpoints
- Excluir uma rota AWS Client VPN de endpoint

Crie uma rota AWS Client VPN de endpoint

Ao criar uma rota de VPN endpoint do cliente, você especifica como o tráfego da rede de destino deve ser direcionado.

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

Você pode adicionar rotas a um VPN endpoint do cliente usando o console e o. AWS CLI

Para criar uma rota de VPN endpoint do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual adicionar a rota, escolha Tabela de rotas e, em seguida, escolha Criar rota.
4. Em Destino da rota, especifique o IPv4 CIDR intervalo da rede de destino. Por exemplo:
   - Para adicionar uma rota para o VPN endpoint VPC do cliente, insira VPC o IPv4 CIDR intervalo.
   - Para adicionar uma rota para acesso à Internet, insira `0.0.0.0/0`.
   - Para adicionar uma rota para um peeringVPC, insira o alcance do peeringVPC. IPv4 CIDR
   - Para adicionar uma rota para uma rede local, insira o intervalo da AWS conexão site a siteVPN. IPv4 CIDR
5. Em ID de sub-rede para associação de rede de destino, selecione a sub-rede associada ao endpoint do clienteVPN.

   Como alternativa, se você estiver adicionando uma rota para a rede local de VPN endpoints 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 VPN endpoint do cliente ()AWS CLI

Use o create-client-vpn-routecomando.

Exibir AWS Client VPN rotas de endpoints

Você pode visualizar as rotas para um VPN endpoint de cliente específico usando o console ou o. AWS CLI

Para visualizar as rotas dos VPN endpoints do cliente (console)

1. No painel de navegação, escolha Client VPN Endpoints.
2. Selecione o VPN endpoint do cliente para o qual visualizar as rotas e escolha Tabela de rotas.

Para visualizar as rotas do VPN endpoint do cliente ()AWS CLI

Use o describe-client-vpn-routescomando.

Excluir uma rota AWS Client VPN de endpoint

Você só pode excluir as VPN rotas do cliente que você adicionou manualmente. Você não pode excluir rotas que foram adicionadas automaticamente quando você associou uma sub-rede ao VPN endpoint do cliente. Para excluir rotas que foram adicionadas automaticamente, você deve desassociar a sub-rede que iniciou sua criação do endpoint do ClienteVPN.

Você pode excluir uma rota de um VPN endpoint do cliente usando o console ou o. AWS CLI

Para excluir uma rota de VPN endpoint do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente do qual excluir a rota e escolha 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 VPN endpoint do cliente ()AWS CLI

Use o delete-client-vpn-routecomando.

AWS Client VPN redes alvo

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

Para obter mais informações sobre os tipos de acesso que você pode configurar (como permitir que seus clientes acessem a Internet), consulteCenários e exemplos para o cliente VPN.

Requisitos de rede VPN alvo do cliente

Ao criar uma rede de destino, as seguintes regras se aplicam:

- A sub-rede deve ter um CIDR bloco com pelo menos uma máscara de bits /27, por exemplo, 10.0.0.0/27. A sub-rede também deve ter sempre 20 endereços IP disponíveis, pelo menos.

- O CIDR bloco da sub-rede não pode se sobrepor ao CIDR intervalo de clientes do endpoint do clienteVPN.
- Se você associar mais de uma sub-rede a um VPN endpoint do cliente, 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 um VPC quando criou o VPN endpoint do cliente, a sub-rede deve estar na mesma. VPC Se você ainda não associou a VPC ao VPN endpoint do cliente, você pode escolher qualquer sub-rede em qualquer. VPC

  Todas as outras associações de sub-rede devem ser da mesmaVPC. Para associar uma sub-rede de outraVPC, você deve primeiro modificar o VPN endpoint do cliente e alterar o VPC que está associado a ele. Para obter mais informações, consulte Modificar um AWS Client VPN endpoint.

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

> **Note**
>
> Depois que suas redes de destino forem associadas, ao adicionar ou remover outras CIDRs à sua conexãoVPC, você deverá executar uma das seguintes operações para atualizar a rota local da tabela de rotas do VPN endpoint do cliente:
>
> - Desassocie o VPN endpoint do cliente da rede de destino e, em seguida, associe o VPN endpoint do cliente à rede de destino.
> - Adicione manualmente a rota ou remova-a da tabela de rotas do VPN endpoint do cliente.

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

Tarefas

- Associar uma rede de destino a um AWS Client VPN endpoint
- Aplique um grupo de segurança a uma rede de destino no AWS Client VPN
- Exibir redes de AWS Client VPN destino

- Desassociar uma rede de destino de um endpoint AWS Client VPN

Associar uma rede de destino a um AWS Client VPN endpoint

Você pode associar uma ou mais redes de destino (sub-redes) a um VPN endpoint do cliente usando o Amazon VPC Console ou o. AWS CLI Antes de associar uma rede de destino a um VPN endpoint do cliente, familiarize-se com os requisitos. Consulte Requisitos para criar uma rede de destino.

Para associar uma rede de destino a um VPN endpoint do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual associar a rede de destino, escolha Associações de rede de destino e, em seguida, escolha Associar rede de destino.
4. Para VPC, escolha o local VPC em que a sub-rede está localizada. Se você especificou um VPC ao criar o VPN endpoint do cliente ou se tiver associações de sub-rede anteriores, ele deverá ser o mesmo. VPC
5. Em Escolha uma sub-rede para associar, escolha a sub-rede a ser associada ao endpoint do clienteVPN.
6. SelecioneAssociate target network (Associar rede de destino).

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

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

Aplique um grupo de segurança a uma rede de destino no AWS Client VPN

Ao criar um VPN endpoint de cliente, você pode especificar os grupos de segurança a serem aplicados à rede de destino. Quando você associa a primeira rede de destino a um VPN endpoint do Cliente, aplicamos automaticamente o grupo de segurança padrão do VPC em que a sub-rede associada está localizada. Para obter mais informações, consulte Grupos de segurança.

Você pode alterar os grupos de segurança do VPN endpoint do cliente. As regras do grupo de segurança necessárias dependem do tipo de VPN acesso que você deseja configurar. Para obter mais informações, consulte Cenários e exemplos para o cliente VPN.

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

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

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

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

Exibir redes de AWS Client VPN destino

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

Para visualizar redes de destino (console)

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

Para visualizar as redes de destino usando o AWS CLI

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

Desassociar uma rede de destino de um endpoint AWS Client VPN

Quando você desassocia uma rede de destino, todas as rotas que foram adicionadas manualmente à tabela de rotas do VPN endpoint do cliente são excluídas, bem como a rota que foi criada automaticamente quando a associação da rede de destino foi feita (a rota local daVPC). Se você dissociar todas as redes de destino de um VPN endpoint do cliente, os clientes não poderão mais estabelecer uma VPN conexão.

Para desassociar uma rede de destino de um VPN endpoint do cliente (console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN Endpoints.
3. Selecione o VPN endpoint do cliente ao qual a rede de destino está associada e escolha Associações de 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 VPN endpoint do cliente ()AWS CLI

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

AWS Client VPN duração máxima VPN da sessão

AWS Client VPN fornece várias opções para a duração máxima da VPN sessão, que é o tempo máximo permitido para uma conexão do cliente com o VPN endpoint do cliente. Você pode configurar uma duração máxima de VPN sessão mais curta para atender aos requisitos de segurança e conformidade. Por padrão, a duração máxima VPN da sessão é de 24 horas.

> **Note**
>
> Quando o valor máximo da duração da VPN sessão é reduzido em relação ao valor atual, todas VPN as sessões ativas conectadas ao endpoint por um período maior do que a duração recém-definida são desconectadas. Novas sessões precisarão ser iniciadas.

Consulte as notas de versão do cliente AWS fornecido no Guia do AWS Client VPN usuário para obter detalhes sobre a duração da sessão para aplicativos de desktop do cliente.

Configurar a VPN sessão máxima durante a criação de um AWS Client VPN endpoint

A duração de uma VPN sessão é configurada durante a criação de um VPN endpoint do cliente. Veja as etapas Crie um AWS Client VPN endpoint para criar um VPN endpoint de cliente e definir a duração máxima da sessão.

Tarefas

Exibir a duração máxima AWS Client VPN atual da VPN sessão

Use as etapas a seguir para ver a duração VPN máxima da VPN sessão atual do Cliente.

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

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

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

Use o describe-client-vpn-endpointscomando.

Modificar a duração máxima da AWS Client VPN sessão

Use as etapas a seguir para modificar a duração VPN máxima da VPN sessão de um cliente existente.

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

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints.
3. Selecione o VPN endpoint do cliente que você deseja modificar, escolha Ações e, em seguida, escolha Modificar VPN endpoint do cliente.
4. Em Horas de tempo limite da sessão, escolha o tempo máximo desejado de duração da VPN sessão em horas.
5. Escolha Modificar VPN endpoint do cliente.

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

Use o modify-client-vpn-endpointcomando.

Segurança em AWS Client VPN

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS Client VPN, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

AWS Client VPN faz parte do VPC serviço da Amazon. Para obter mais informações sobre segurança na AmazonVPC, consulte Segurança no Guia do VPC usuário da Amazon.

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

Tópicos

Proteção de dados em AWS Client VPN

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no AWS ClienteVPN. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou 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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Client VPN ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia em trânsito

AWS Client VPN fornece conexões seguras de qualquer local usando o 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 a outras redes por meio de um VPN endpoint de cliente. Para obter mais informações e exemplos, consulte Cenários e exemplos para o cliente VPN.

Restringir o acesso a redes

Você pode configurar seu VPN endpoint de cliente para restringir o acesso a recursos específicos em seuVPC. Para a autenticação baseada no usuário, você também pode restringir o acesso a partes da sua rede, com base no grupo de usuários que acessa o endpoint do clienteVPN. Para obter mais informações, consulte Restrinja o acesso à sua rede usando o Cliente VPN.

Autenticar clientes

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

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

- Autenticação do Active Directory (baseada no usuário)
- Autenticação mútua (baseada em certificado)
- Login único (autenticação federada SAML baseada) (baseada no usuário)

Gerenciamento de identidade e acesso para AWS Client VPN

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do ClienteVPN. IAMé um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no ClientVPN.

Usuário do serviço — Se você usar o VPN serviço de cliente para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais VPN recursos do Cliente para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no ClienteVPN, consulteSolução de problemas AWS Client VPN de identidade e acesso.

Administrador de serviços — Se você é responsável pelos VPN recursos do cliente em sua empresa, provavelmente tem acesso total ao clienteVPN. É seu trabalho determinar quais VPN recursos e recursos do Cliente seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar IAM com o ClienteVPN, consulteComo AWS Client VPN funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao ClienteVPN. Para ver exemplos de políticas VPN baseadas

na identidade do cliente que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade para o AWS Client VPN

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista

completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.

- Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
- Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida

ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado

pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como AWS Client VPN funciona com IAM

Antes de usar IAM para gerenciar o acesso ao ClienteVPN, saiba quais IAM recursos estão disponíveis para uso com o ClienteVPN.

IAMrecursos que você pode usar com o AWS Cliente VPN

IAMrecurso	VPNSuporte ao cliente
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC(tags nas políticas)	Não

IAMrecurso	VPNSuporte ao cliente
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para obter uma visão de alto nível de como o Cliente VPN e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAM Usuário.

Políticas baseadas em identidade para clientes VPN

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para clientes VPN

Para ver exemplos de políticas VPN baseadas na identidade do cliente, consulte. Exemplos de políticas baseadas em identidade para o AWS Client VPN

Políticas baseadas em recursos no Cliente VPN

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para o cliente VPN

Compatível com ações de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de VPN ações do cliente, consulte Ações definidas pelo AWS cliente VPN na Referência de autorização de serviço.

As ações de política no Cliente VPN usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Para ver exemplos de políticas VPN baseadas na identidade do cliente, consulte. Exemplos de políticas baseadas em identidade para o AWS Client VPN

Recursos de política para o cliente VPN

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de VPN recursos do cliente e seusARNs, consulte Recursos definidos pelo AWS cliente VPN na Referência de autorização de serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo AWS cliente VPN. ARN

Para ver exemplos de políticas VPN baseadas na identidade do cliente, consulte. Exemplos de políticas baseadas em identidade para o AWS Client VPN

Chaves de condição de política para o cliente VPN

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

Para ver uma lista das chaves de VPN condição do cliente, consulte Chaves de condição para o AWS cliente VPN na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo AWS cliente VPN.

Para ver exemplos de políticas VPN baseadas na identidade do cliente, consulte. Exemplos de políticas baseadas em identidade para o AWS Client VPN

ACLsno cliente VPN

SuportesACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

ABACcom o cliente VPN

Suportes ABAC (tags nas políticas): Não

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o Cliente VPN

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS esse trabalho IAM no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões principais entre serviços para o cliente VPN

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço para o cliente VPN

Compatível com perfis de serviço: Sim

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a VPN funcionalidade do cliente. Edite as funções de serviço somente quando o Cliente VPN fornecer orientação para fazer isso.

Funções vinculadas ao serviço para o cliente VPN

Suporte a perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao

serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte AWS serviços que funcionam com. IAM Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço .

Exemplos de políticas baseadas em identidade para o AWS Client VPN

Por padrão, usuários e funções não têm permissão para criar ou modificar VPN recursos do cliente. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ClienteVPN, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o AWS Cliente VPN na Referência de Autorização de Serviço.

Tópicos

- Melhores práticas de política
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir VPN recursos do Cliente em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso.

Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.

- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas AWS Client VPN de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Client VPN e. IAM

Tópicos

- Não estou autorizado a realizar uma ação no Cliente VPN
- Não estou autorizado a realizar iam: PassRole

- Quero permitir que pessoas fora da minha acessem Conta da AWS os VPN recursos do meu cliente

Não estou autorizado a realizar uma ação no Cliente VPN

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`ec2:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `ec2:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o ClienteVPN.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no ClientVPN. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem Conta da AWS os VPN recursos do meu cliente

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Client VPN oferece suporte a esses recursos, consulteComo AWS Client VPN funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Usando funções vinculadas a serviços para AWS Client VPN

AWS Client VPN usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao Cliente. VPN As funções vinculadas ao serviço são predefinidas pelo Cliente VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Tópicos

- Usando funções para AWS Client VPN
- Usando funções para autorização de conexão no ClienteVPN;

Usando funções para AWS Client VPN

AWS Client VPN usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao Cliente. VPN As funções vinculadas ao serviço são predefinidas pelo Cliente VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Cliente VPN porque você não precisa adicionar manualmente as permissões necessárias. O cliente VPN define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o cliente VPN pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege os VPN recursos do seu cliente porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para o cliente VPN

O cliente VPN usa a função vinculada ao serviço chamada AWSServiceRoleForClientVPN— Permitir que VPN o cliente crie e gerencie recursos relacionados às suas VPN conexões.

A função AWSServiceRoleForClientVPNvinculada ao serviço confia no seguinte serviço para assumir a função:

- `clientvpn.amazonaws.com`

A política de permissões de função chamada C lientVPNService RolePolicy permite que VPN o Cliente conclua as seguintes ações nos recursos especificados:

- Ação: `ec2:CreateNetworkInterface` em `Resource: "*"`
- Ação: `ec2:CreateNetworkInterfacePermission` em `Resource: "*"`
- Ação: `ec2:DescribeSecurityGroups` em `Resource: "*"`

- Ação: `ec2:DescribeVpcs` em `Resource: "*"`
- Ação: `ec2:DescribeSubnets` em `Resource: "*"`
- Ação: `ec2:DescribeInternetGateways` em `Resource: "*"`
- Ação: `ec2:ModifyNetworkInterfaceAttribute` em `Resource: "*"`
- Ação: `ec2:DeleteNetworkInterface` em `Resource: "*"`
- Ação: `ec2:DescribeAccountAttributes` em `Resource: "*"`
- Ação: `ds:AuthorizeApplication` em `Resource: "*"`
- Ação: `ds:DescribeDirectories` em `Resource: "*"`
- Ação: `ds:GetDirectoryLimits` em `Resource: "*"`
- Ação: `ds:UnauthorizeApplication` em `Resource: "*"`
- Ação: `logs:DescribeLogStreams` em `Resource: "*"`
- Ação: `logs:CreateLogStream` em `Resource: "*"`
- Ação: `logs:PutLogEvents` em `Resource: "*"`
- Ação: `logs:DescribeLogGroups` em `Resource: "*"`
- Ação: `acm:GetCertificate` em `Resource: "*"`
- Ação: `acm:DescribeCertificate` em `Resource: "*"`
- Ação: `iam:GetSAMLProvider` em `Resource: "*"`
- Ação: `lambda:GetFunctionConfiguration` em `Resource: "*"`

Você deve configurar permissões para permitir que uma IAM entidade (como usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

Criação de uma função vinculada ao serviço para o Cliente VPN

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria o primeiro VPN endpoint do Cliente em sua conta com o AWS Management Console, o ou o AWS CLI AWS API, o Cliente VPN cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria o primeiro VPN endpoint do Cliente em sua conta, o Cliente VPN cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para o Cliente VPN

VPNO cliente não permite que você edite a função AWSServiceRoleForClientVPN vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluindo uma função vinculada ao serviço para o Cliente VPN

Se você não precisar mais usar o ClientVPN, recomendamos que você exclua a função AWSServiceRoleForClientVPNvinculada ao serviço.

Primeiro, você deve excluir os VPN recursos relacionados ao Cliente. Isso garante que você não remova por engano a permissão para acessar os recursos.

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

Regiões suportadas para funções vinculadas ao VPN serviço de cliente

O cliente VPN suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Usando funções para autorização de conexão no ClienteVPN;

AWS Client VPN usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao Cliente. VPN As funções vinculadas ao serviço são predefinidas pelo Cliente VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Cliente VPN porque você não precisa adicionar manualmente as permissões necessárias. O cliente VPN define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o cliente VPN pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege os VPN recursos do seu cliente porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para o cliente VPN

O cliente VPN usa a função vinculada ao serviço chamada AWSServiceRoleForClientVPNConnections— Função vinculada ao serviço para conexões do clienteVPN.

A função AWSServiceRoleForClientVPNConnections vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `clientvpn-connections.amazonaws.com`

A política de permissões de função chamada C lientVPNService ConnectionsRolePolicy permite que VPN o Cliente conclua as seguintes ações nos recursos especificados:

- Ação: `lambda:InvokeFunction` em `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Você deve configurar permissões para permitir que uma IAM entidade (como usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

Criação de uma função vinculada ao serviço para o Cliente VPN

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria o primeiro VPN endpoint do Cliente em sua conta com o AWS Management Console, o ou o AWS CLI AWS API, o Cliente VPN cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria o primeiro VPN endpoint do Cliente em sua conta, o Cliente VPN cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para o Cliente VPN

VPNO cliente não permite que você edite a função AWSServiceRoleForClientVPNConnections vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar

a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluindo uma função vinculada ao serviço para o Cliente VPN

Se você não precisar mais usar o ClientVPN, recomendamos que você exclua a função AWSServiceRoleForClientVPNConnectionsvinculada ao serviço.

Primeiro, você deve excluir os VPN recursos relacionados ao Cliente. Isso garante que você não remova por engano a permissão para acessar os recursos.

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

Regiões suportadas para funções vinculadas ao VPN serviço de cliente

O cliente VPN suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Resiliência em AWS Client VPN

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos 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 AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

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

Várias redes de destino para alta disponibilidade

Você associa uma rede de destino a um VPN endpoint do cliente para permitir que os clientes estabeleçam VPN sessões. As redes de destino são sub-redes em sua. VPC Cada sub-rede que

você associa ao VPN endpoint do cliente deve pertencer a uma zona de disponibilidade diferente. Você pode associar várias sub-redes a um VPN endpoint do cliente para obter alta disponibilidade.

Segurança da infraestrutura em AWS Client VPN

Como um serviço gerenciado, AWS o Cliente VPN é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar o Cliente VPN pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

Melhores práticas de segurança para AWS Client VPN

AWS Client VPN fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Regras de autorização

Use regras de autorização para restringir quais usuários podem acessar sua rede. Para obter mais informações, consulte AWS Client VPN regras de autorização.

Grupos de segurança

Use grupos de segurança para controlar quais recursos os usuários podem acessar no seuVPC. Para obter mais informações, consulte Grupos de segurança.

Listas de revogação de certificados de cliente

Use listas de revogação de certificados de cliente para revogar o acesso a um VPN endpoint de cliente para certificados de cliente específicos. Por exemplo, quando um usuário sai da sua organização. Para obter mais informações, consulte AWS Client VPN listas de revogação de certificados de clientes.

Ferramentas de monitoramento

Use ferramentas de monitoramento para acompanhar a disponibilidade e o desempenho dos VPN endpoints do seu cliente. Para obter mais informações, consulte Monitoramento AWS Client VPN.

Gerenciamento de identidade e acesso

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

IPv6considerações para AWS Client VPN

Atualmente, o VPN serviço Client não oferece suporte ao roteamento de IPv6 tráfego pelo VPN túnel. No entanto, há casos em que o IPv6 tráfego deve ser direcionado para o VPN túnel para evitar IPv6 vazamentos. IPv6o vazamento pode ocorrer quando ambos IPv4 IPv6 estão habilitados e conectados aoVPN, mas VPN não direcionam o IPv6 tráfego para o túnel. Nesse caso, ao se conectar a um destino IPv6 habilitado, você ainda está se conectando com o IPv6 endereço fornecido pelo seuISP. Isso vazará seu IPv6 endereço real. As instruções abaixo explicam como direcionar o IPv6 tráfego para o VPN túnel.

As seguintes diretivas IPv6 relacionadas devem ser adicionadas ao arquivo de VPN configuração do seu cliente para evitar IPv6 vazamentos:

```
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
```

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

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

> **Note**
>
> Para roteamento de dispositivos “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 IPv6 tráfego atualmente alocado para a VPN conexão.

Verificação

Provavelmente, sua organização terá os próprios testes. Uma verificação básica é configurar uma VPN conexão de túnel completa e, em seguida, executar o ping6 em um IPv6 servidor usando o IPv6 endereço. O IPv6 endereço do servidor deve estar no intervalo especificado pelo `route-ipv6` comando. Esse teste de ping deve falhar. No entanto, isso pode mudar se o IPv6 suporte for adicionado ao VPN serviço do Cliente 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. Também existem algumas ferramentas disponíveis publicamente.

Monitoramento AWS Client VPN

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Client VPN suas outras AWS soluções. Você pode usar os seguintes recursos para monitorar seus VPN endpoints Client, analisar padrões de tráfego e solucionar problemas com seus endpoints ClientVPN.

Amazon CloudWatch

Monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível 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 CloudWatch rastrear o CPU uso ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

AWS CloudTrail

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

CloudWatch Registros da Amazon

Permite monitorar as tentativas de conexão feitas a seu endpoint AWS Client VPN . Você pode ver as tentativas de conexão e as redefinições de conexão para as VPN conexões do Cliente. Você pode ver as tentativas de conexão bem-sucedidas e com falha. Você pode especificar o stream de CloudWatch registros de registros para registrar os detalhes da conexão. Para obter mais informações, consulte Registro de conexão para um AWS Client VPN endpoint o Guia do usuário do Amazon CloudWatch Logs.

Tópicos

CloudWatch Métricas da Amazon para AWS Client VPN

AWS Client VPN publica as seguintes métricas na Amazon CloudWatch para seus VPN endpoints de clientes. As métricas são publicadas na Amazon CloudWatch a cada cinco minutos.

Métrica	Descrição
ActiveConnectionsCount	O número de conexões ativas com o VPN endpoint do cliente. Unidades: contagem
AuthenticationFailures	O número de falhas de autenticação para o VPN endpoint do cliente. Unidades: contagem
CrlDaysToExpiry	O número de dias até que a Lista de Revogação de Certificados (CRL), que está configurada no VPN endpoint do Cliente, expire. Unidades: dias
EgressBytes	O número de bytes enviados do VPN endpoint do cliente. Unidade: bytes
EgressPackets	O número de pacotes enviados do VPN endpoint do cliente. Unidades: contagem
IngressBytes	O número de bytes recebidos pelo VPN endpoint do cliente. Unidade: bytes

Métrica	Descrição
IngressPackets	O número de pacotes recebidos pelo VPN endpoint do cliente. Unidades: contagem
SelfServicePortalClientConfigurationDownloads	O número de downloads do arquivo de configuração do VPN endpoint do cliente a partir do portal de autoatendimento. Unidade: contagem

AWS Client VPN publica as seguintes métricas de avaliação de postura para seus endpoints de clienteVPN.

Métrica	Descrição
ClientConnectHandlerTimeouts	O número de tempos limite ao invocar o manipulador de conexão do cliente para conexões com o endpoint do cliente. VPN Unidades: contagem
ClientConnectHandlerInvalidResponses	O número de respostas inválidas retornadas pelo manipulador de conexão do cliente para conexões com o endpoint do clienteVPN. Unidades: contagem
ClientConnectHandlerOtherExecutionErrors	O número de erros inesperados ao executar o manipulador de conexão do cliente para conexões com o VPN endpoint do cliente. Unidades: contagem
ClientConnectHandlerThrottlingErrors	O número de erros de limitação ao invocar o manipulador de conexão do cliente para conexões com o endpoint do cliente. VPN

Métrica	Descrição
	Unidades: contagem
ClientConnectHandlerDeniedConnections	O número de conexões negadas pelo manipulador de conexão do cliente para conexões com o VPN endpoint do cliente. Unidades: contagem
ClientConnectHandlerFailedServiceErrors	O número de erros do lado do serviço ao executar o manipulador de conexão do cliente para conexões com o VPN endpoint do cliente. Unidades: contagem

Você pode filtrar as métricas do seu cliente VPN endpoint por endpoint.

CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido 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 CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

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

Tarefas

- Veja as métricas de VPN endpoint do cliente na Amazon CloudWatch

Veja as métricas de VPN endpoint do cliente na Amazon CloudWatch

Você pode visualizar as métricas do VPN endpoint do seu cliente da seguinte forma.

Para visualizar métricas usando o CloudWatch console

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

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Em Todas as métricas, escolha o namespace da VPN métrica Client.
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 o Cliente VPN

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

AWS CloudTrail registros para AWS Client VPN

AWS Client VPN é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ClienteVPN. CloudTrail captura todas as API chamadas para o Cliente VPN como eventos. As chamadas capturadas incluem chamadas do VPN console do cliente e chamadas de código para as VPN API operações do cliente. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o cliente. VPN Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Use as informações coletadas por CloudTrail para determinar a solicitação que foi feita ao ClienteVPN, o endereço IP solicitante, o solicitante, quando foi feita e detalhes adicionais.

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

VPNInformações do cliente em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no ClienteVPN, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para o ClienteVPN, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão Geral para Criar uma Trilha
- Serviços compatíveis e integrações do CloudTrail
- Configurando as SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas as VPN ações do cliente são registradas CloudTrail e documentadas na Amazon EC2 API Reference. Por exemplo, chamadas para as `AuthorizeClientVpnIngress` ações `CreateClientVpnEndpointAssociateClientVpnTargetNetwork`, e geram entradas nos arquivos de CloudTrail log.

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 root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o CloudTrail userIdentity Elemento.

Entendendo as entradas do arquivo de VPN log do cliente

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por

diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

Para obter mais informações, consulte Registro de VPC API chamadas da AmazonEBS, Amazon e Amazon AWS CloudTrail no Amazon EC2 API Reference. EC2

AWS Client VPN cotas

Sua AWS conta tem as seguintes cotas, anteriormente chamadas de limites, relacionadas aos endpoints do clienteVPN. A menos que especificado de outra forma, cada cota é específica da região . É possível 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 Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

VPNCotas de clientes

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

Nome	Padrão	Ajustável
Rotas por VPN endpoint do cliente	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

Quando você configura usuários e grupos para o Active Directory ou um IdP SAML baseado, 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 VPN endpoints do cliente:

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

Solução de problemas AWS Client VPN

As seções a seguir podem ajudá-lo a solucionar problemas que você possa ter com um VPN endpoint do cliente.

Para obter mais informações sobre a solução de problemas VPN de software aberto que os clientes usam para se conectar a um clienteVPN, consulte Solucionando problemas de VPN conexão com o cliente no Guia AWS Client VPN do usuário.

Problemas comuns

- Solução de problemas AWS Client VPN: Não foi possível resolver o nome do VPN endpoint DNS do cliente
- Solução de problemas AWS Client VPN: o tráfego não está sendo dividido entre sub-redes
- Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado
- Solução de problemas AWS Client VPN: os clientes não conseguem acessar um Amazon S3 VPC emparelhado ou a Internet
- Solução de problemas AWS Client VPN: o acesso a um Amazon S3 VPC emparelhado ou à Internet é intermitente
- Solução de problemas AWS Client VPN: o software cliente retorna um TLS erro ao tentar se conectar ao cliente VPN
- Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação do Active Directory
- Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação federada
- Solução de problemas AWS Client VPN: os clientes não conseguem se conectar — autenticação mútua
- Solução de problemas AWS Client VPN: o cliente retorna um erro de credenciais que excedem o tamanho máximo em Cliente VPN — autenticação federada
- Solução de problemas AWS Client VPN: o cliente não abre o navegador para um endpoint — autenticação federada
- Solução de problemas AWS Client VPN: o cliente retorna erro sem portas disponíveis — autenticação federada

- Solução de problemas AWS Client VPN: uma conexão é encerrada devido a uma incompatibilidade de IP
- Solução de problemas AWS Client VPN: rotear o tráfego para LAN não funcionar conforme o esperado
- Solução de problemas AWS Client VPN: verifique o limite de largura de banda para um endpoint do cliente VPN

Solução de problemas AWS Client VPN: Não foi possível resolver o nome do VPN endpoint DNS do cliente

Problema

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

Causa

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

Solução

Abra o arquivo de configuração do VPN endpoint do cliente usando seu editor de texto preferido. Localize a linha que especifica o DNS nome do VPN endpoint do cliente e acrescente uma string aleatória a ela para que o formato seja *`random_string.displayed_DNS_name`*. Por exemplo:

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

Solução de problemas AWS Client VPN: o tráfego não está sendo dividido entre sub-redes

Problema

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, apenas uma rota está sendo usada, embora eu tenha adicionado as duas rotas à tabela de rotas do VPN endpoint do cliente.

Causa

Você pode associar várias sub-redes a um VPN endpoint do cliente, mas só pode associar 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, VPN o Client não permite que você divida seletivamente o tráfego entre as sub-redes associadas ao endpoint do Client. VPN

Os clientes se conectam a um VPN endpoint do cliente com base no algoritmo DNS round-robin. 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.

Solução

Verifique se o VPN endpoint do cliente 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.

Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado

Problema

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

Causa

As regras de autorização são indexadas na redeCIDRs. As regras de autorização devem conceder aos grupos do Active Directory acesso a uma rede específicaCIDRs. 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 VPC do usuário da Amazon para obter mais detalhes.

Solução

Verifique se você criou regras de autorização que concedam explicitamente aos grupos do Active Directory acesso a uma rede CIDRs específica. 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.

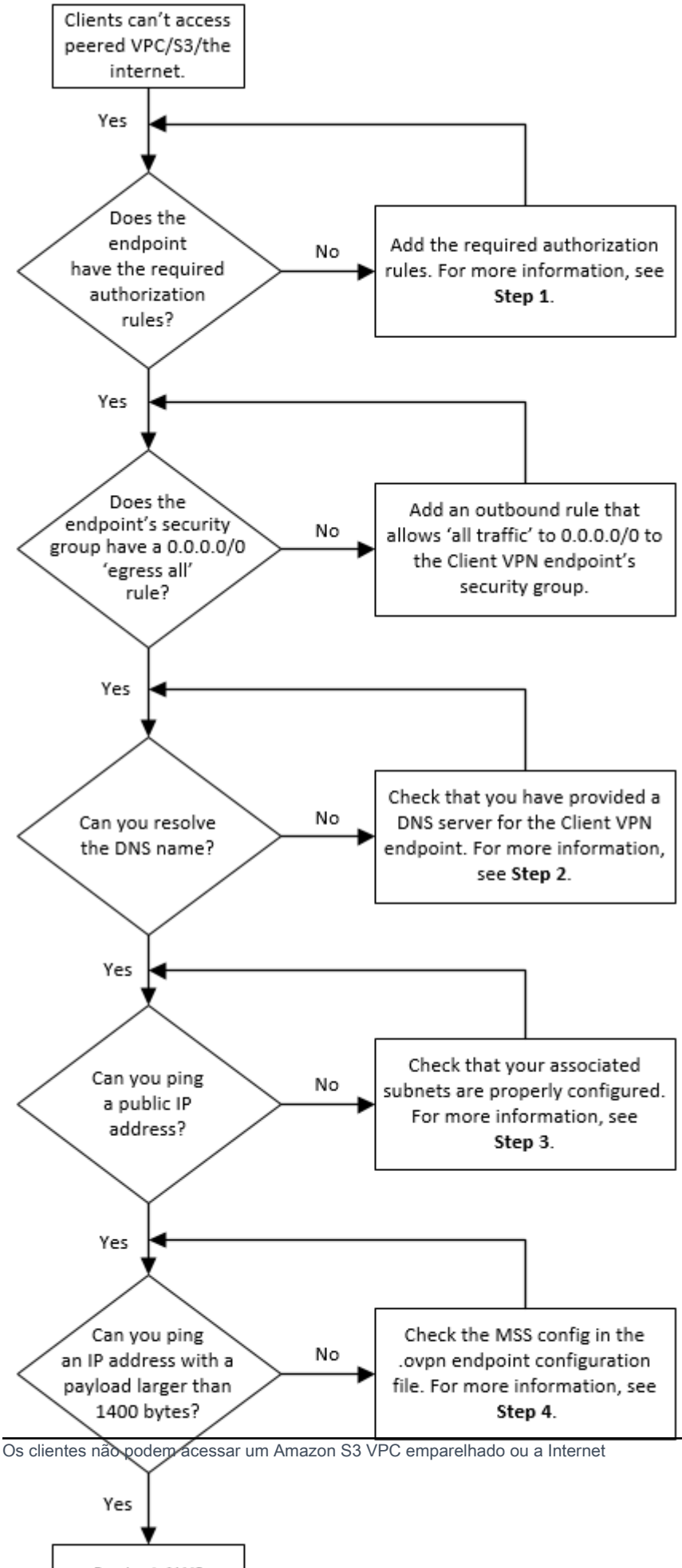
Solução de problemas AWS Client VPN: os clientes não conseguem acessar um Amazon S3 VPC emparelhado ou a Internet

Problema

Eu configurei corretamente minhas rotas de VPN endpoint de cliente, mas meus clientes não conseguem acessar um Amazon S3 VPC emparelhado ou a Internet.

Solução

O fluxograma a seguir contém as etapas para diagnosticar problemas de conectividade com a InternetVPC, com peering e com o 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 acessar um peeringVPC, adicione uma regra de autorização para o IPv4 CIDR intervalo doVPC.

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

   Se você não conseguir resolver o DNS nome, verifique se você especificou os DNS servidores para o VPN endpoint do cliente. Se você gerencia seu próprio DNS servidor, especifique seu endereço IP. Verifique se o DNS servidor está acessível a partir doVPC.

   Se você não tiver certeza sobre qual endereço IP especificar para os DNS servidores, especifique o VPC DNS resolvedor no endereço IP .2 em seu. 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 você não receber uma resposta, certifique-se de que a tabela de rotas das sub-redes associadas tenha uma rota padrão direcionada a um gateway da Internet ou a um NAT gateway. 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 um peeringVPC, verifique se a tabela de rotas da sub-rede associada tem uma entrada de rota para o peering. VPC

   Se você não conseguir acessar o Amazon S3, verifique se a tabela de rotas da sub-rede associada tem uma entrada de rota para o endpoint do gateway. VPC
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 você não conseguir fazer ping em um endereço IP com uma carga útil maior que 1400 bytes, abra o arquivo de `.ovpn` configuração do VPN endpoint do cliente usando seu editor de texto preferido e adicione o seguinte.

```
mssfix 1328
```

Solução de problemas AWS Client VPN: o acesso a um Amazon S3 VPC emparelhado ou à Internet é intermitente

Problema

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

Causa

Os clientes se conectam a um VPN endpoint do cliente com base no algoritmo DNS round-robin. 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.

Solução

Verifique se o VPN endpoint do cliente 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 seu VPN endpoint de cliente tenha três sub-redes associadas (sub-rede A, B e C) e 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

Solução de problemas AWS Client VPN: o software cliente retorna um TLS erro ao tentar se conectar ao cliente VPN

Problema

Eu costumava conectar meus clientes ao cliente VPN com sucesso, mas agora o cliente VPN baseado em Open retorna um dos seguintes erros quando tenta se conectar:

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

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

Possível causa nº. 1

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 VPN endpoint do cliente verifica o certificado do cliente em relação à lista de revogação de certificados do cliente que você importou. Se a lista de revogação de certificados do cliente tiver expirado, você não poderá se conectar ao endpoint do cliente. VPN

Solução nº. 1

Verifique a data de expiração da sua lista de revogação de certificados de cliente usando a ferramenta Open. SSL

```
$ 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 cliente. VPN Para obter mais informações, consulte AWS Client VPN listas de revogação de certificados de clientes.

Possível causa nº. 2

O certificado do servidor que está sendo usado para o VPN endpoint do cliente expirou.

Solução nº. 2

Verifique o status do seu certificado de servidor no AWS Certificate Manager console ou usando AWS CLI o. Se o certificado do servidor estiver expirado, crie um novo certificado e faça o upload paraACM. Para obter etapas detalhadas para gerar os certificados e chaves do servidor e do cliente usando o utilitário Open VPN easy-rsa e importá-los para o see. ACM Autenticação mútua em AWS Client VPN

Como alternativa, pode haver um problema com o software VPN aberto que o cliente está usando para se conectar ao clienteVPN. Para obter mais informações sobre a solução de problemas de software VPN baseado em aberto, consulte Solucionando problemas de VPN conexão com o cliente no Guia AWS Client VPN do usuário.

Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação do Active Directory

Problema

Eu uso a autenticação do Active Directory para meu VPN endpoint de cliente e costumava conectar meus clientes ao cliente VPN com sucesso. Mas agora, os clientes estão recebendo erros de nome de usuário e senha inválidos.

Possíveis causas

Se você usa a autenticação do Active Directory e habilitou a autenticação multifator (MFA) depois de distribuir o arquivo de configuração do cliente, o arquivo não contém as informações necessárias para solicitar que os usuários insiram o MFA código. Os usuários são solicitados a inserir o nome de usuário e a senha, mas há falha na autenticação.

Solução

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 AWS Client VPN exportação do arquivo de configuração do endpoint. Teste a MFA configuração do Active Directory sem usar o VPN endpoint do cliente para verificar se MFA está funcionando conforme o esperado.

Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação federada

Problema

Tentando fazer login com um nome de usuário e senha com autenticação federada e recebendo o erro “As credenciais recebidas estavam incorretas. Entre em contato com seu administrador de TI.”

Causa

Esse erro pode ser causado por não ter pelo menos um atributo incluído na SAML resposta do IdP.

Solução

Certifique-se de que pelo menos um atributo esteja incluído na SAML resposta do IdP. Consulte SAMLrecursos de configuração de IdP baseados em Para mais informações.

Solução de problemas AWS Client VPN: os clientes não conseguem se conectar — autenticação mútua

Problema

Eu uso autenticação mútua para o VPN endpoint do meu cliente. Os clientes estão recebendo erros TLS importantes de falha na negociação 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.

Solução

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 AWS Client VPN exportação do arquivo de configuração do endpoint.

Solução de problemas AWS Client VPN: o cliente retorna um erro de credenciais que excedem o tamanho máximo em Cliente VPN — autenticação federada

Problema

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

Causa

A SAML resposta retornada pelo IdP excede o tamanho máximo suportado. Para obter mais informações, consulte Requisitos e considerações para autenticação SAML federada baseada.

Solução

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

Solução de problemas AWS Client VPN: o cliente não abre o navegador para um endpoint — autenticação federada

Problema

Eu uso a autenticação federada para o VPN endpoint do meu cliente. 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.

Causa

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

Solução

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

Solução de problemas AWS Client VPN: o cliente retorna erro sem portas disponíveis — autenticação federada

Problema

Eu uso a autenticação federada para o VPN endpoint do meu cliente. 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.
```

Causa

O cliente AWS fornecido exige o uso da TCP porta 35001 para concluir a autenticação. Para obter mais informações, consulte Requisitos e considerações para autenticação SAML federada baseada.

Solução

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

Solução de problemas AWS Client VPN: uma conexão é encerrada devido a uma incompatibilidade de IP

Problema

VPNa conexão foi encerrada e o software cliente retornará o seguinte erro: `"The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."`

Causa

O cliente AWS fornecido exige que o endereço IP ao qual ele está conectado corresponda ao IP do VPN servidor que dá suporte ao VPN endpoint do cliente. Para obter mais informações, consulte Regras e melhores práticas de uso AWS Client VPN.

Solução

Verifique se não há DNS proxy entre o cliente AWS fornecido e o VPN endpoint do cliente.

Solução de problemas AWS Client VPN: rotear o tráfego para LAN não funcionar conforme o esperado

Problema

A tentativa de rotear o tráfego para a rede local (LAN) não funciona conforme o esperado quando os intervalos de endereços LAN IP não estão dentro dos seguintes intervalos de endereços IP privados padrão: `10.0.0.0/8`172.16.0.0/12,,`192.168.0.0/16`, ou`169.254.0.0/16`.

Causa

Se for detectado que o intervalo de LAN endereços do cliente está fora dos intervalos padrão acima, o VPN endpoint do cliente enviará automaticamente a VPN diretiva Open “redirect-gateway block-local” para o cliente, forçando todo o tráfego para o. LAN VPN Para obter mais informações, consulte Regras e melhores práticas de uso AWS Client VPN.

Solução

Se você precisar de LAN acesso durante VPN as conexões, é recomendável usar os intervalos de endereços convencionais listados acima para o seuLAN.

Solução de problemas AWS Client VPN: verifique o limite de largura de banda para um endpoint do cliente VPN

Problema

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

Causa

A taxa de transferência depende de vários fatores, como a capacidade da conexão a partir da sua localização e a latência da rede entre o aplicativo de VPN desktop do cliente no computador e o VPC endpoint. Também há um limite de largura de banda de 10 Mbps por conexão de usuário.

Solução

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 de documentos do Guia do VPN usuário do cliente

A tabela a seguir descreve as atualizações do Guia AWS Client VPN do Administrador.

Alteração	Descrição	Data
Exemplo de regras de autorização	Adição de cenários de exemplo para regras de autorização.	15 de setembro de 2022
VPNduração máxima da sessão	Você pode configurar uma duração máxima de VPN sessão mais curta para atender aos requisitos de segurança e conformidade.	20 de janeiro de 2022
Banner de login do cliente	Você pode ativar um banner de texto nos aplicativos de VPN desktop do Cliente AWS fornecidos quando uma VPN sessão for estabelecida para atender às necessidades regulatórias e de conformid ade.	20 de janeiro de 2022
Manipulador de conexão do cliente	Você pode habilitar o manipulador de conexão do cliente para que seu VPN endpoint do cliente execute uma lógica personalizada que autorize novas conexões.	4 de novembro de 2020
Portal de autoatendimento	Você pode habilitar um portal de autoatendimento em seu VPN endpoint de cliente para seus clientes.	29 de outubro de 2020

lient-to-client Acesso C	Você pode permitir que os clientes que se conectam a um VPN endpoint do cliente se conectem entre si.	29 de setembro de 2020
SAMLAutenticação federada baseada em 2.0	Você pode autenticar VPN usuários do Client usando a autenticação federada SAML baseada em 2.0.	19 de maio de 2020
Especificar grupos de segurança durante a criação	Você pode especificar um VPC e grupos de segurança ao criar seu AWS Client VPN endpoint.	5 de março de 2020
Portas configuráveis VPN	Você pode especificar um número de VPN porta compatível para seu AWS Client VPN endpoint.	16 de janeiro de 2020
Support para autenticação multifatorial () MFA	Seu AWS Client VPN endpoint oferece suporte MFA se estiver habilitado para o Active Directory.	30 de setembro de 2019
Suporte a túnel dividido	Você pode ativar o túnel dividido em seu endpoint. AWS Client VPN	24 de julho de 2019
Lançamento inicial	Essa versão apresenta o AWS Client VPN.	18 de dezembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.