Manual do usuário

AWS Site-to-Site VPN

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Site-to-Site VPN: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que AWS Site-to-Site VPNé

Por padrão, uma instância que você executa na Amazon VPC não pode se comunicar com uma rede local (Nuvem AWS) e um dispositivo remoto, que pode ser, por exemplo, um dispositivo local ou on-premises. Você pode habilitar o acesso aos seus dispositivos remotos a partir da sua VPC criando uma conexão AWS Site-to-Site VPN(Site-to-Site VPN) e configurando o roteamento para transmitir o tráfego pela conexão.

Embora o termo conexão VPN seja um termo geral, nesta documentação, uma conexão VPN se refere à conexão entre sua VPC e sua própria rede local. Site-to-Site A VPN oferece suporte a conexões VPN de segurança do Protocolo de Internet (IPsec).

Conteúdo

Conceitos

A seguir estão os principais conceitos da Site-to-Site VPN:

- Conexão VPN: uma conexão segura entre seu equipamento local e seu VPCs.
- Túnel VPN: um link criptografado em que os dados podem transmitir da rede do cliente para a AWS ou vice-versa.

  Cada conexão VPN inclui dois túneis VPN que podem ser usados simultaneamente para alta disponibilidade.
- Gateway do cliente: um AWS recurso que fornece informações AWS sobre seu dispositivo de gateway do cliente.
- Dispositivo de gateway do cliente: um dispositivo físico ou aplicativo de software no seu lado da conexão Site-to-Site VPN.
- Gateway de destino: um termo genérico para o endpoint VPN no lado Amazon da conexão Site-to-Site VPN.

- Gateway privado virtual: um gateway privado virtual é o endpoint VPN no lado Amazon da sua conexão Site-to-Site VPN que pode ser conectado a uma única VPC.
- Transit Gateway: um hub de trânsito que pode ser usado para interconectar várias redes locais VPCs e como um endpoint de VPN para o lado Amazon da Site-to-Site conexão VPN.
- Túnel de grande largura de banda: uma configuração de túnel que suporta largura de banda de até 5 Gbps por túnel, em comparação com o padrão de 1,25 Gbps. Disponível para conexões VPN conectadas ao Transit Gateway ou Cloud WAN.

Site-to-Site Recursos de VPN

Os seguintes recursos são compatíveis com AWS Site-to-Site VPN conexões:

- Internet Key Exchange versão 2 (IKEv2)
- NAT Traversal
- ASN de 4 bytes no intervalo de 1 a 2147483647 para configuração do Gateway Privado Virtual (VGW). Consulte Opções de gateway do cliente para sua conexão AWS Site-to-Site VPN para obter mais informações.
- ASN de 2 bytes para CGW (Gateway do Cliente) na faixa de 1 a 65535. Consulte Opções de gateway do cliente para sua conexão AWS Site-to-Site VPN para obter mais informações.
- CloudWatch métricas
- Endereços IP reutilizáveis para os gateways do cliente
- Opções de criptografia adicionais; incluindo criptografia AES de 256 bits, hashing SHA-2 e grupos Diffie-Hellman adicionais
- Opções de túnel configuráveis
- ASN privado do cliente para o lado da Amazon de uma sessão BGP
- Certificado privado de uma CA subordinada de Autoridade de Certificação Privada da AWS
- Support for IPv6 support for AWS Site-to-Site VPN
  - IPv6 para endereços IP de túneis internos (IP de pacote)
  - IPv6 para endereços IP de túnel externo (IP de túnel) no Transit Gateway e no Cloud WAN
- Suporte total à IPv6 migração com as seguintes combinações:
  - IPv6 IP do túnel externo com IP de pacote IPv6 interno (IPv6-in-) IPv6
  - IPv6 IP do túnel externo com IP de pacote IPv4 interno (IPv4-in-) IPv6

Site-to-Site Limitações da VPN

Uma conexão Site-to-Site VPN tem as seguintes limitações.

- IPv6 o tráfego não é suportado para conexões VPN em um gateway privado virtual. IPv6 para túnel externo só IPs é compatível com Transit Gateway e Cloud WAN.
- Uma Site-to-Site VPN conexão não oferece suporte ao Path MTU Discovery.
- Uma única conexão Site-to-Site VPN não suporta ambos IPv4 e IPv6 tráfego simultaneamente. Você precisa de conexões VPN separadas para transporte IPv4 e IPv6 pacotes.
- As conexões VPN IP privadas não oferecem suporte a IPv6 endereços para túneis externos IPs.
- Você não pode modificar uma conexão IPv4 VPN existente para usar IPv6. Nesse caso, você deverá excluir a conexão existente e criar outra.

Além disso, leve em consideração o seguinte ao usar Site-to-Site uma VPN.

- Ao conectar você VPCs a uma rede local comum, recomendamos que você use blocos CIDR não sobrepostos para suas redes.

Site-to-Site Recursos de VPN

Você pode criar, acessar e gerenciar seus recursos de Site-to-Site VPN usando qualquer uma das seguintes interfaces:

- Console de gerenciamento da AWS— Fornece uma interface web que você pode usar para acessar seus recursos de Site-to-Site VPN.
- AWS Command Line Interface(AWS CLI) — Fornece comandos para um amplo conjunto de AWS serviços, incluindo Amazon VPC, e é compatível com Windows, macOS e Linux. As linhas de comando estão incluídas na referência maior da linha de AWS Site-to-Site VPN comando EC2
  - Para ter mais informações sobre a interfaces de linha de comandos, consulte AWS Command Line Interface.
  - Para ver a lista de EC2 comandos disponíveis, incluindo os comandos Site-to-Site VPN, consulte Referência da linha de EC2 comando.

> **Note**
>
> A referência da linha de comando não diferencia entre os comandos da Site-to-Site VPN e o conjunto maior de EC2 comandos

- AWS SDKs— forneça informações específicas para o idioma APIs e cuide de muitos detalhes da conexão, como calcular assinaturas, lidar com novas tentativas de solicitação e tratamento de erros. Para obter mais informações, consulte AWS SDKs.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta para acessar a Amazon VPC, mas exige que a aplicação lide com detalhes de baixo nível, como geração de hash para assinar a solicitação e tratamento de erros. Para obter mais informações, consulte a Amazon EC2 API Reference.

Preços

Você é cobrado por cada hora de conexão VPN em que a sua conexão VPN é provisionada e disponível. Para obter mais informações, consulte AWS Site-to-Site VPN os preços da conexão Site-to-Site VPN acelerada.

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.

Quando você cria uma conexão VPN acelerada, criamos e gerenciamos dois aceleradores em seu nome. Você é cobrado por uma taxa horária e custos de transferência de dados para cada acelerador. Para obter mais informações, consulte Preços do AWS Global Accelerator.

Não há cobranças adicionais pelo uso de IPv6 endereços com suas conexões Site-to-Site VPN VPN.

Como AWS Site-to-Site VPN funciona

Uma conexão Site-to-Site VPN consiste nos seguintes componentes:

- Um gateway privado virtual ou um gateway de trânsito
- Um dispositivo de gateway do cliente
- Um gateway do cliente

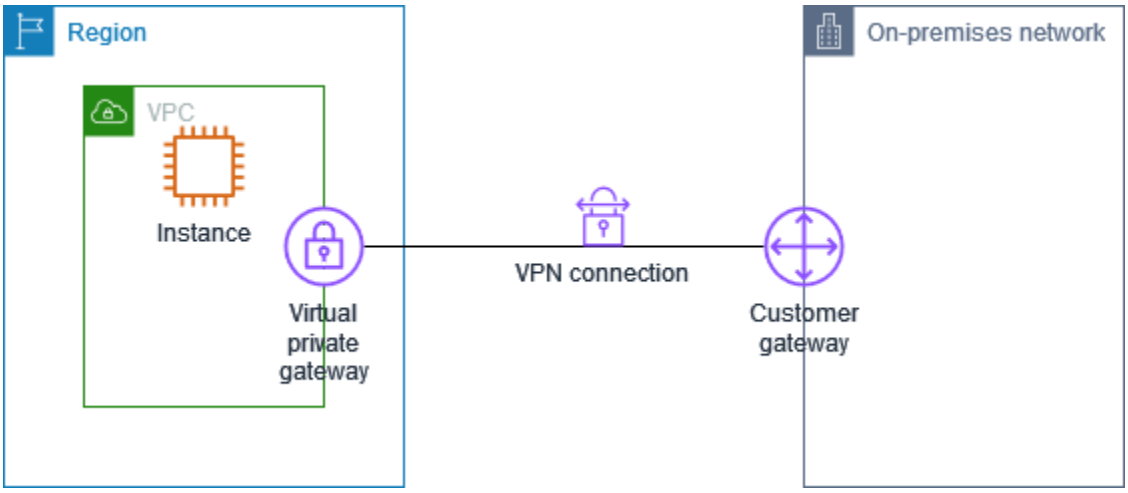
A conexão VPN oferece dois túneis VPN entre um gateway privado virtual ou gateway de trânsito no AWS lado e um gateway de cliente no lado local.

Para obter mais informações sobre cotas de Site-to-Site VPN, consulteAWS Site-to-Site VPN cotas.

Gateway privado virtual

Um gateway privado virtual é o Site-to-Site VPN Concentrator no lado Amazon da conexão Site-to-Site VPN. Você cria um gateway privado virtual e o anexa a uma nuvem privada virtual (VPC) com recursos que devem acessar a Site-to-Site conexão VPN.

O diagrama a seguir mostra uma conexão VPN entre uma VPC e a rede on-premises usando um gateway privado virtual.



Quando você cria um gateway privado virtual, é possível especificar o Número de sistema autônomo privado (ASN) para o lado da Amazon do gateway. Se você não especificar um ASN, o gateway privado virtual é criado com o ASN (64512) padrão. Você não poderá alterar o ASN depois de ter

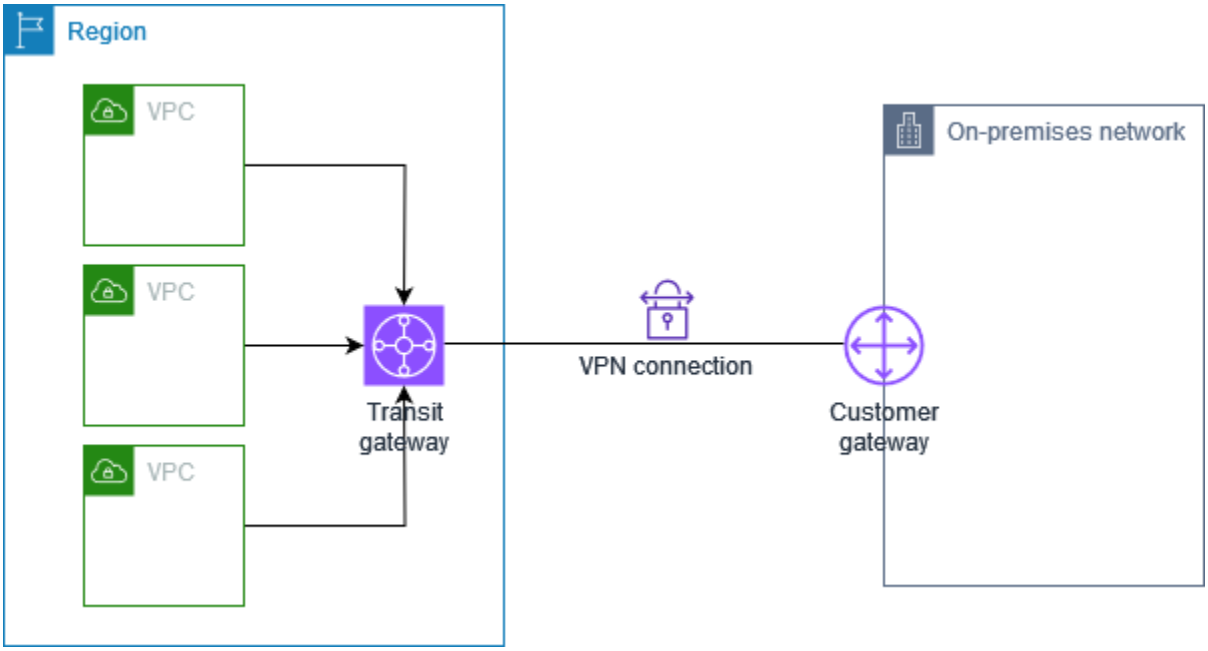
criado o gateway privado virtual. Para verificar o ASN do seu gateway privado virtual, veja seus detalhes na página Gateways privados virtuais no console da Amazon VPC ou use o comando. describe-vpn-gateways AWS CLI

> **Note**
>
> Os gateways privados virtuais não oferecem suporte IPv6 para conexões Site-to-Site VPN. Se precisar de IPv6 suporte, use um gateway de trânsito ou Cloud WAN para sua conexão VPN.

Transit gateway

Um gateway de trânsito é um hub de trânsito que você pode usar para interconectar sua rede VPCs e sua rede local. Para obter mais informações, consulte Gateways de trânsito da Amazon VPC. Você pode criar uma conexão Site-to-Site VPN como anexo em um gateway de trânsito.

O diagrama a seguir mostra uma conexão VPN entre várias VPCs e sua rede local usando um gateway de trânsito. O gateway de trânsito tem três anexos de VPC e um anexo de VPN.



Sua conexão Site-to-Site VPN em um gateway de trânsito pode suportar IPv4 ou IPv6 trafegar dentro dos túneis VPN (endereços IP internos). Além disso, os gateways de trânsito oferecem suporte a IPv6 endereços IP do túnel externo. Para obter mais informações, consulte Tráfego IPv4 e IPv6 no AWS Site-to-Site VPN.

Você pode modificar o gateway de destino de uma conexão Site-to-Site VPN de um gateway privado virtual para um gateway de trânsito. Para obter mais informações, consulte the section called "Modificar o gateway de destino de uma conexão VPN".

Dispositivo de gateway do cliente

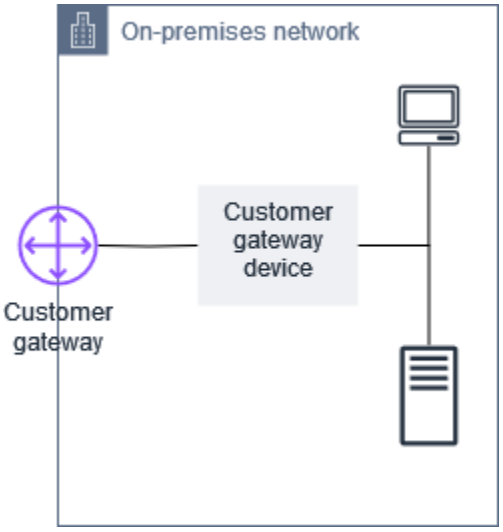
Um dispositivo de gateway do cliente é um dispositivo físico ou aplicativo de software no seu lado da conexão Site-to-Site VPN. Você configura o dispositivo para funcionar com a conexão Site-to-Site VPN. Para obter mais informações, consulte AWS Site-to-Site VPN dispositivos de gateway do cliente.

Por padrão, o dispositivo de gateway do cliente deve abrir os túneis da sua conexão Site-to-Site VPN gerando tráfego e iniciando o processo de negociação do Internet Key Exchange (IKE). Você pode configurar sua conexão Site-to-Site VPN para especificar que, em vez disso, AWS deve iniciar o processo de negociação do IKE. Para obter mais informações, consulte AWS Site-to-Site VPN opções de iniciação de túnel.

Se você estiver usando endereços IP IPv6 para túneis externos, seu dispositivo de gateway do cliente deve suportar IPv6 endereçamento e ser capaz de estabelecer IPsec túneis com IPv6 endpoints.

Gateway do cliente

Um gateway do cliente é um recurso que você cria na AWS e representa o dispositivo de gateway do cliente na rede local. Ao criar um gateway do cliente, você fornece informações sobre seu dispositivo para AWS. Para obter mais informações, consulte the section called "Opções de gateway do cliente".



Para usar o Amazon VPC com uma conexão Site-to-Site VPN, você ou seu administrador de rede também devem configurar o dispositivo ou aplicativo de gateway do cliente em sua rede remota. Quando você cria a conexão Site-to-Site VPN, fornecemos as informações de configuração necessárias e seu administrador de rede normalmente executa essa configuração. Para obter informações sobre os requisitos e a configuração do gateway do cliente, consulte AWS Site-to-Site VPN dispositivos de gateway do cliente.

IPv6 gateway do cliente

Ao criar um gateway de cliente para uso com túnel IPv6 externo IPs, você especifica um IPv6 endereço em vez de um IPv4 endereço. Você pode criar um gateway IPv6 do cliente usando o AWS Management Console ou a AWS CLI.

Para criar um gateway IPv6 do cliente usando a AWS CLI, use o seguinte comando:

```
aws ec2 create-customer-gateway --Ipv6-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

O IPv6 endereço deve ser um endereço válido e roteável pela Internet para seu dispositivo de IPv6 gateway do cliente.

IPv6 Conexões VPN

Site-to-Site As conexões VPN VPN suportam as seguintes IPv6 configurações:

- IPv4 túnel externo com pacotes IPv4 internos - O recurso básico de IPv4 VPN suportado no Virtual Private Gateway (VGW), Transit Gateway (TGW) e Cloud WAN.
- IPv4 túnel externo com pacotes IPv6 internos - Permite IPv6 aplicativos/transporte dentro do túnel VPN. Compatível com TGW e Cloud WAN (não compatível com VGW).
- IPv6 túnel externo com pacotes IPv6 internos - Permite a IPv6 migração completa com IPv6 endereços tanto para o túnel IPs externo quanto para o pacote IPs interno. Compatível com TGW e Cloud WAN.
- IPv6 túnel externo com pacotes IPv4 internos - Permite o endereçamento de túneis IPv6 externos e, ao mesmo tempo, oferece suporte a IPv4 aplicativos legados dentro do túnel. Compatível com TGW e Cloud WAN.

Para criar uma conexão VPN com o túnel IPv6 externo IPs, você especifica `0utsideIPAddressType=Ipv6` ao criar a conexão VPN. A AWS configura automaticamente os IPv6 endereços de túneis externos para o lado AWS dos túneis VPN.

Exemplo de comando CLI para criar uma conexão VPN com túnel IPv6 externo IPs e túnel IPv6 interno: IPs

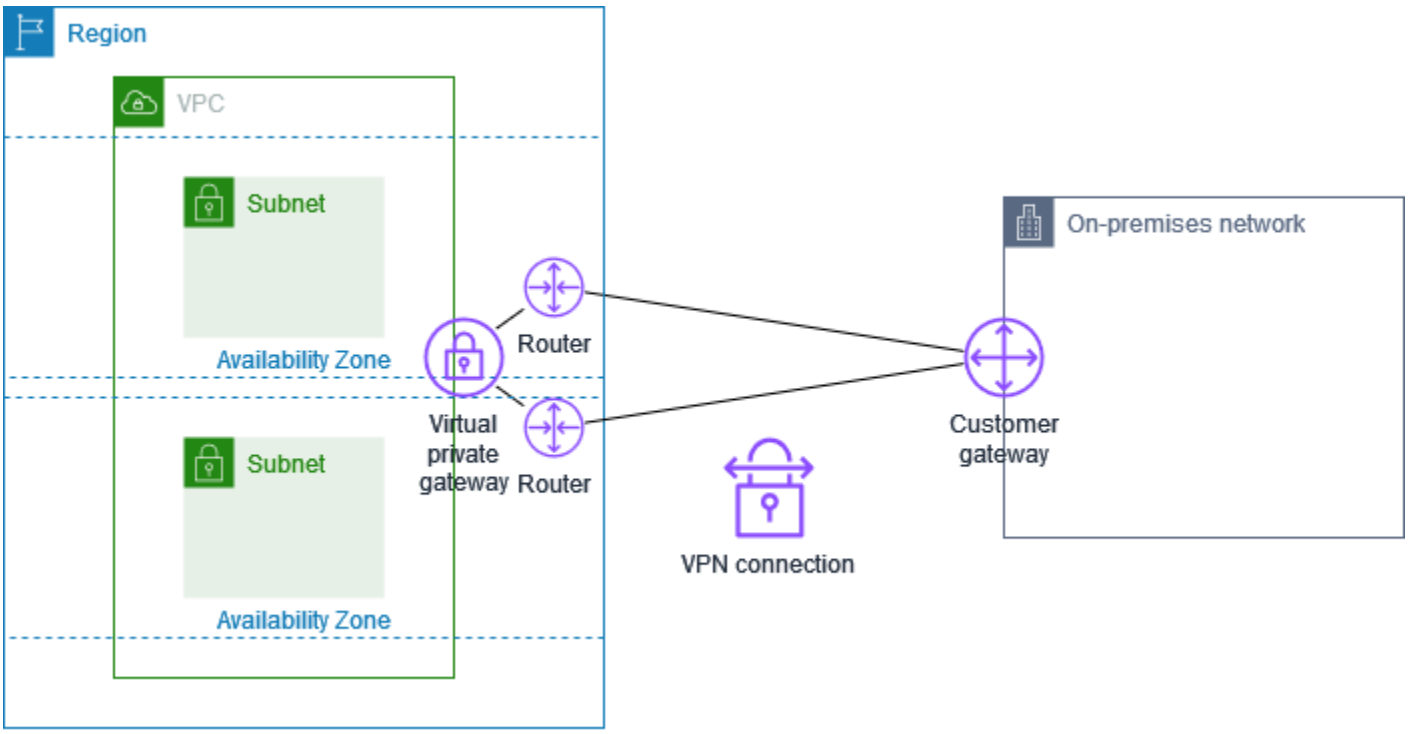
```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Você pode ver os IPv6 endereços atribuídos à sua conexão VPN usando o comando `describe-vpn-connection` CLI.

Opções de túnel para sua AWS Site-to-Site VPN conexão

Você usa uma conexão Site-to-Site VPN para conectar sua rede remota a uma VPC. Cada conexão Site-to-Site VPN tem dois túneis, com cada túnel usando um endereço IP público exclusivo. Para a redundância, é importante configurar ambos os túneis. Quando um túnel fica indisponível (por exemplo, inativo para manutenção), o tráfego da rede é roteado automaticamente para o túnel disponível para essa Site-to-Site conexão VPN específica.

O diagrama a seguir mostra os dois túneis de uma conexão VPN. Cada túnel termina em uma zona de disponibilidade diferente para fornecer maior disponibilidade. Tráfego da rede local para AWS usar os dois túneis. O tráfego AWS para a rede local prefere um dos túneis, mas pode passar automaticamente para o outro túnel se houver uma falha lateral. AWS



Ao criar uma conexão Site-to-Site VPN, você baixa um arquivo de configuração específico para o dispositivo de gateway do cliente que contém informações para configurar o dispositivo, incluindo informações para configurar cada túnel. Opcionalmente, você mesmo pode especificar algumas das opções de túnel ao criar a conexão Site-to-Site VPN. Caso contrário, a AWS fornece os valores padrão.

Opções de largura de banda do túnel

Você pode configurar a capacidade de largura de banda para seus túneis VPN:

- Largura de banda padrão: até 1,25 Gbps por túnel (padrão)
- Túnel de grande largura de banda (LBT): até 5 Gbps por túnel

Túneis de grande largura de banda estão disponíveis somente para conexões VPN conectadas ao Transit Gateway ou ao Cloud WAN. Para obter mais informações, consulte Túneis de grande largura de banda.

> **Note**
>
> Site-to-Site Os endpoints de túnel VPN avaliam as propostas do gateway do cliente, começando com o menor valor configurado na lista abaixo, independentemente do pedido

de proposta do gateway do cliente. Você pode usar o `modify-vpn-connection-options` comando para restringir a lista de opções que os AWS endpoints aceitarão. Para obter mais informações, consulte a modify-vpn-connection-optionsReferência de linha de comando do Amazon EC2.

Túneis de grande largura de banda

Os túneis de grande largura de banda permitem que você configure túneis Site-to-Site VPN que suportam largura de banda de até 5 Gbps por túnel, em comparação com o padrão de 1,25 Gbps. Túneis de grande largura de banda estão disponíveis para conexões VPN conectadas ao Transit Gateway ou ao Cloud WAN. Isso elimina ou reduz a necessidade de implantar protocolos complexos, como ECMP (Equal Cost Multi Path), para obter maior largura de banda e garantir uma largura de banda de túnel consistente de 5 Gbps por túnel. Os túneis de grande largura de banda foram projetados para serem usados nos seguintes casos de uso:

- Conectividade de data center: Support aplicativos híbridos que consomem muita largura de banda, migrações de big data ou arquiteturas de recuperação de desastres que exigem conectividade de alta capacidade entre cargas de trabalho da AWS e datacenters locais.
- Backup Direct Connect: forneça conectividade de backup ou sobreposição para circuitos Direct Connect de alta capacidade (mais de 10 Gbps) para data centers locais ou instalações de colocation.

Disponibilidade de regiões

Túneis de grande largura de banda estão disponíveis em todas as regiões, exceto nas seguintes:

Indisponível Regiões da AWS

AWS Região	Description
ap-southeast-4	Ásia-Pacífico (Melbourne)
ca-west-1	Oeste do Canadá (Calgary)
eu-central-2	Europa (Zurique)
il-central-1	Israel (Tel Aviv)

AWS Região	Description
me-central-1	Oriente Médio (Emirados Árabes Unidos)

Requisitos e limitações

- Disponível somente para conexões VPN conectadas a um gateway de trânsito ou à Cloud WAN. Não há suporte para anexos do Virtual Private Gateway.
- Ambos os túneis de uma conexão VPN devem usar a mesma configuração de largura de banda (1,25 Gbps ou ambos 5 Gbps).
- A VPN acelerada não é suportada.
- Todos os outros recursos principais da VPN, como VPN IP privada, roteamento e manutenção de túneis, funcionam da mesma forma com o túnel de grande largura de banda.
- O limite de MTU permanece em 1500 bytes. Saiba mais sobre como ajustar os tamanhos de MTU e MSS de acordo com os algoritmos em uso.
- Você não pode modificar um túnel existente para usar túneis de grande largura de banda. Você precisará primeiro excluir o túnel e, em seguida, criar um novo túnel e definir a largura de banda do túnel como Grande.
- Os gateways de cliente (CGWs) somente com um IP fixo podem ser usados com túneis de grande largura de banda.
- Os gateways do cliente (CGWs) sem um endereço IP não podem ser usados com túneis de grande largura de banda.
- Túneis de grande largura de banda não suportam alterações na porta NAT-T enquanto o túnel está estabelecido.
- Pacotes que exigem fragmentação podem apresentar desempenho inferior. Saiba mais

Preços para túneis de grande largura de banda

Informações sobre preços de conexões VPN de grande largura de banda podem ser encontradas na página de preços de AWS VPN.

Escalabilidade além de 5 Gbps

Para requisitos de largura de banda superiores a 5 Gbps por túnel, você pode usar o ECMP em várias conexões VPN. Por exemplo, você pode obter uma largura de banda de 20 Gbps implantando

duas conexões VPN com túneis de grande largura de banda e usando ECMP em todos os quatro túneis.

Configurar opções de túnel para AWS Site-to-Site VPN

Esta seção fornece orientação abrangente sobre a configuração de opções de túnel para AWS Site-to-Site VPN conexões, abrangendo parâmetros essenciais, como detecção de pares mortos, versões IKE e configurações de criptografia. Você pode personalizar essas opções de túnel para otimizar a segurança, o desempenho e a compatibilidade da sua conexão VPN com sua infraestrutura de rede local.

Veja a seguir as opções de túnel que você pode configurar.

> **Note**
>
> Algumas opções de túnel têm vários valores padrão. Por exemplo, as versões IKE têm dois valores de opção de túnel padrão: `ikev1` e `ikev2`. Todos os valores padrão serão associados a essa opção de túnel se você não escolher valores específicos. Clique para remover qualquer valor padrão que você não queira associar à opção de túnel. Por exemplo, se você quiser usar `ikev1` apenas para a versão IKE, clique em `ikev2` para removê-lo.

Tempo limite do Dead Peer Detection (DPD)

A duração, em segundos, após a qual ocorre o tempo limite do DPD. Um tempo limite de DPD de 30 segundos significa que o endpoint da VPN considerará o par morto 30 segundos após a primeira falha no keep-alive. É possível especificar 30 ou superior.

Padrão: 60

Ação de tempo limite do DPD

A ação a ser executada após atingir o tempo limite do Dead Peer Detection (DPD). É possível especificar o seguinte:

- `Clear`: finalizar a sessão do protocolo IKE quando o tempo limite do DPD for atingido (interromper o túnel e limpar as rotas)
- `None`: nenhuma ação quando o tempo limite do DPD for atingido
- `Restart`: reiniciar a sessão do protocolo IKE quando o tempo limite do DPD for atingido

Para obter mais informações, consulte AWS Site-to-Site VPN opções de iniciação de túnel.

Padrão: `Clear`

Opções de registro em log da VPN

Com os registros de Site-to-Site VPN, você pode obter acesso a detalhes sobre o estabelecimento do túnel IP Security (IPsec), negociações do Internet Key Exchange (IKE) e mensagens do protocolo Dead Peer Detection (DPD).

Para obter mais informações, consulte AWS Site-to-Site VPN troncos.

Formatos de log disponíveis: `json`, `text`

Versões do IKE

As versões do IKE que são permitidas para o túnel VPN. É possível especificar um ou mais dos valores padrão.

Padrões: `ikev1`, `ikev2`

Dentro do túnel IPv4 CIDR

O intervalo de IPv4 endereços internos (internos) do túnel VPN. É possível especificar um bloco CIDR de tamanho /30 a partir do intervalo `169.254.0.0/16`. O bloco CIDR deve ser exclusivo em todas as conexões Site-to-Site VPN que usam o mesmo gateway privado virtual.

> **Note**
>
> O bloco CIDR não precisa ser exclusivo em todas as conexões em um gateway de trânsito. No entanto, se eles não forem exclusivos, isso pode criar um conflito no gateway do cliente. Prossiga com cuidado ao reutilizar o mesmo bloco CIDR em várias conexões Site-to-Site VPN em um gateway de trânsito.

Os blocos CIDR a seguir são reservados e não podem ser usados:

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`

- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

Padrão: um bloco IPv4 CIDR de tamanho /30 do `169.254.0.0/16` intervalo.

Armazenamento de chaves pré-compartilhadas

O tipo do armazenamento para a chave pré-compartilhada:

- Padrão — A chave pré-compartilhada é armazenada diretamente no serviço Site-to-Site VPN.
- Secrets Manager — A chave pré-compartilhada é armazenada usando AWS Secrets Manager. Para ter mais informações sobre o Secrets Manager, consulte Recursos de segurança aprimorados usando o Secrets Manager.

Largura de banda do túnel

A largura de banda suportada pelo túnel.

- Padrão — A largura de banda do túnel é definida para um máximo de até 1,25 Gbps por túnel (padrão).
- Grande — A largura de banda do túnel até um máximo de até 5 Gbps por túnel.

> **Note**
>
> A opção Large só está disponível para conexões VPN conectadas a um gateway de trânsito ou à Cloud WAN. Ele não é compatível com conexões de gateway privado virtual.

Dentro do túnel IPv6 CIDR

(Somente conexões IPv6 VPN) O intervalo de IPv6 endereços internos (internos) do túnel VPN. É possível especificar um bloco CIDR de tamanho /126 a partir do intervalo `fd00::/8` local. O bloco CIDR deve ser exclusivo em todas as conexões Site-to-Site VPN que usam o mesmo gateway de trânsito. Se você não especificar uma IPv6 sub-rede, a Amazon selecionará automaticamente uma sub-rede /128 desse intervalo. Independentemente de você especificar a sub-rede ou se a Amazon a selecionar, a Amazon usa o primeiro IPv6 endereço utilizável na sub-rede para seu lado da conexão, e seu lado usa o segundo endereço utilizável. IPv6

Padrão: um bloco IPv6 CIDR de tamanho /126 do intervalo local`fd00::/8`.

Tipo de endereço IP do túnel externo

O tipo de endereço IP para os endereços IP do túnel externo. É possível especificar um dos seguintes:

- `PrivateIpv4`: use o IPv4 endereço privado para implantar conexões Site-to-Site VPN pelo Direct Connect.
- `PublicIpv4`: (Padrão) Use IPv4 endereços para o túnel externo IPs.
- `Ipv6`: Use IPv6 endereços para o túnel externo IPs. Essa opção só está disponível para conexões VPN em um gateway de trânsito ou Cloud WAN.

Quando você seleciona`Ipv6`, a AWS configura automaticamente os IPv6 endereços de túneis externos para o lado AWS dos túneis VPN. Seu dispositivo de gateway do cliente deve suportar IPv6 endereçamento e ser capaz de estabelecer IPsec túneis com IPv6 endpoints.

Padrão: `PublicIpv4`

CIDR IPv4 de rede local

(Somente conexão IPv4 VPN) O intervalo CIDR usado durante a negociação da fase 2 do IKE para o lado do cliente (local) do túnel VPN. Esse intervalo é usado para propor rotas, mas não impõe restrições de tráfego, pois AWS usa exclusivamente rotas baseadas em rotas VPNs . VPNs Os baseados em políticas não são suportados, pois AWS limitariam a capacidade de oferecer suporte a protocolos de roteamento dinâmico e arquiteturas multirregionais. Isso deve incluir os intervalos de IP da sua rede on-premises que precisam se comunicar pelo túnel VPN. Configurações adequadas da tabela de rotas e grupos de segurança devem ser usados para controlar o fluxo real do tráfego. NACLs

Padrão: 0.0.0.0/0

CIDR IPv4 de rede remota

(Somente conexão IPv4 VPN) O intervalo CIDR usado durante a negociação da fase 2 do IKE para o AWS lado do túnel VPN. Esse intervalo é usado para propor rotas, mas não impõe restrições de tráfego, pois a AWS usa exclusivamente rotas baseadas em rotas VPNs. A AWS não oferece suporte a políticas baseadas em políticas VPNs porque elas não têm a flexibilidade necessária para cenários complexos de roteamento e são incompatíveis com recursos como gateways de trânsito e VPN Equal Cost Multi-Path (ECMP). Pois VPCs, esse é normalmente o intervalo CIDR da sua VPC. Para gateways de trânsito, isso pode incluir vários intervalos de CIDR da rede conectada VPCs ou de outra rede.

Padrão: 0.0.0.0/0

CIDR IPv6 de rede local

(Somente conexão IPv6 VPN) O intervalo IPv6 CIDR no lado do gateway do cliente (local) que tem permissão para se comunicar pelos túneis VPN.

Padrão: ::/0

CIDR IPv6 de rede remota

(Somente conexão IPv6 VPN) O intervalo IPv6 CIDR no AWS lado que pode se comunicar pelos túneis VPN.

Padrão: ::/0

Fase 1 Números de grupos Diffie-Hellman (DH)

Os números de grupos DH que são permitidos para o túnel VPN para a fase 1 das negociações de IKE. É possível especificar um ou mais dos valores padrão.

Padrões: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Fase 2 Números de grupos Diffie-Hellman (DH)

Os números de grupos DH que são permitidos para o túnel VPN para a fase 2 das negociações de IKE. É possível especificar um ou mais dos valores padrão.

Padrões: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Fase 1 Algoritmos de criptografia

Os algoritmos de criptografia permitidos para o túnel VPN para a fase 1 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrões:,, -GCM-16 AES128 AES256, AES128 -GCM-16 AES256

Fase 2 Algoritmos de criptografia

Os algoritmos de criptografia permitidos para o túnel VPN para a fase 2 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrões:,, -GCM-16 AES128 AES256, AES128 -GCM-16 AES256

Fase 1 Algoritmos de integridade

Os algoritmos de integridade permitidos para o túnel VPN para a fase 1 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrões: SHA1, SHA2 -256, -384, -512 SHA2 SHA2

Fase 2 Algoritmos de integridade

Os algoritmos de integridade permitidos para o túnel VPN para a fase 2 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrões: SHA1, SHA2 -256, -384, -512 SHA2 SHA2

Tempo de vida da fase 1

> **Note**
>
> AWS inicie as rechaves com os valores de tempo definidos nos campos Vida útil da Fase 1 e Vida útil da Fase 2. Se as vidas úteis forem diferentes dos valores negociados no handshake, isso poderá interromper a conectividade do túnel.

O tempo de vida em segundos da fase 1 da negociação de IKE. É possível especificar um número entre 900 e 28.800.

Padrão: 28.800 (8 horas)

Tempo de vida da fase 2

> **Note**
>
> AWS inicie as rechaves com os valores de tempo definidos nos campos Vida útil da Fase 1 e Vida útil da Fase 2. Se as vidas úteis forem diferentes dos valores negociados no handshake, isso poderá interromper a conectividade do túnel.

O tempo de vida em segundos da fase 2 da negociação de IKE. É possível especificar um número entre 900 e 3.600. O número especificado deve ser menor que o número de segundos para a vida útil da fase 1.

Padrão: 3.600 (1 hora)

Chaves pré-compartilhadas (PSK)

Chave pré-compartilhada (PSK) para estabelecer a associação de IKE (Internet key exchange – Troca de chaves da Internet) inicial entre o gateway de destino e o gateway do cliente.

O PSK deve estar entre 8 e 64 caracteres de extensão e não pode começar com zero (0). Os caracteres permitidos são alfanuméricos, pontos (.) e sublinhados (_).

Padrão: uma string de 32 caracteres alfanuméricos.

Fuzz de rechaveamento

A porcentagem da janela de rechaveamento (determinada pelo tempo de margem de rechaveamento) dentro da qual o tempo de rechaveamento é selecionado aleatoriamente.

É possível especificar um valor percentual entre 0 e 100.

Padrão: 100

Tempo de margem de rechaveamento

O tempo de margem em segundos antes da expiração da vida útil das fases 1 e 2, durante o qual o AWS lado da conexão VPN executa uma rechave IKE.

É possível especificar um número entre 60 e metade do valor de vida útil da fase 2.

A hora exata do rechaveamento é selecionada aleatoriamente com base no valor de fuzz de rechaveamento.

Padrão: 270 (4,5 minutos)

Reproduzir pacotes de tamanho da janela

O número de pacotes em uma janela de reprodução de IKE.

É possível especificar um valor entre 64 e 2048.

Padrão: 1024

Ação de inicialização

A ação a ser realizada ao estabelecer o túnel para uma conexão VPN. É possível especificar o seguinte:

- `Start`: AWS inicia a negociação do IKE para abrir o túnel. Somente compatível se o gateway do cliente estiver configurado com um endereço IP.
- `Add`: o dispositivo de gateway do cliente deve iniciar a negociação do protocolo IKE para ativar o túnel.

Para obter mais informações, consulte AWS Site-to-Site VPN opções de iniciação de túnel.

Padrão: `Add`

Controle de ciclo de vida do endpoint de túnel

O controle de ciclo de vida do endpoint de túnel oferece controle sobre o cronograma de substituições de endpoints.

Para obter mais informações, consulte AWS Site-to-Site VPN controle do ciclo de vida do endpoint do túnel.

Padrão: `Off`

Você pode especificar as opções de túnel ao criar uma conexão Site-to-Site VPN ou pode modificar as opções de túnel para uma conexão VPN existente. Para saber mais, consulte os seguintes tópicos:

- Etapa 5: criar uma conexão VPN
- Modificar opções de túnel de AWS Site-to-Site VPN

AWS Site-to-Site VPNOpções de autenticação de túnel

É possível usar chaves pré-compartilhadas ou certificados para autenticar seus endpoints de túnel da Site-to-Site VPN.

Chaves pré-compartilhadas

Uma chave pré-compartilhada (PSK) é a opção de autenticação padrão para túneis do Site-to-Site VPN. Ao criar um túnel, você pode especificar sua própria PSK ou permitir que a AWS gere uma para você automaticamente. A PSK é armazenada usando um dos seguintes métodos:

- Diretamente no serviço Site-to-Site VPN. Para obter mais informações, consulte Site-to-Site Dispositivos VPN de gateway de clientes.
- No AWS Secrets Manager para aumentar a segurança. Para ter mais informações sobre como usar o Secrets Manager, consulte Recursos de segurança aprimorados usando o Secrets Manager.

A string da PSK é então usada ao configurar o dispositivo do gateway do cliente.

Certificado privado do Autoridade de Certificação Privada da AWS

Se você não quiser usar chaves pré-compartilhadas, poderá usar um certificado privado do Autoridade de Certificação Privada da AWS para autenticar sua VPN.

Crie um certificado privado de uma CA subordinada usando o Autoridade de Certificação Privada da AWS (CA privada da AWS). Para assinar a CA subordinada do ACM, você pode usar uma CA raiz do ACM ou uma CA externa. Para obter mais informações sobre como criar um certificado privado, consulte Criar e gerenciar uma CA privada no Guia do usuário do Autoridade de Certificação Privada da AWS.

É necessário criar um perfil vinculado ao serviço para gerar e usar o certificado no lado da AWS do endpoint do túnel da Site-to-Site VPN. Para obter mais informações, consulte the section called "Perfis vinculados ao serviço".

> **Note**
>
> Para facilitar a alternância contínua de certificados, qualquer certificado com a mesma cadeia de autoridade de certificação que a originalmente especificada na chamada de API `CreateCustomerGateway` é suficiente para estabelecer uma conexão VPN.

Se você não especificar o endereço IP do dispositivo de gateway do cliente, não verificaremos o endereço IP. Essa operação permite que você mova o dispositivo de gateway do cliente para um endereço IP diferente sem precisar reconfigurar a conexão VPN.

A Site-to-Site VPN realiza a verificação da cadeia de certificados no certificado do gateway do cliente quando você cria um certificado da Site-to-Site VPN. Além das verificações básicas de CA e validade, a Site-to-Site VPN verifica se as extensões X.509 estão presentes, incluindo Identificador de Chave de Autoridade, Identificador de Chave de Assunto e Restrições Básicas.

AWS Site-to-Site VPN opções de iniciação de túnel

Por padrão, o dispositivo de gateway do cliente deve abrir os túneis da sua conexão Site-to-Site VPN gerando tráfego e iniciando o processo de negociação do Internet Key Exchange (IKE). Você pode configurar seus túneis VPN para especificar que, em vez disso, AWS devem iniciar ou reiniciar o processo de negociação do IKE.

Opções de iniciação do protocolo IKE de túnel da VPN

As seguintes opções de iniciação do protocolo IKE estão disponíveis. Você pode implementar uma ou ambas as opções para um ou ambos os túneis em sua Site-to-Site conexão VPN. Consulte Opções de túnel VPN para obter mais detalhes sobre essas e outras configurações de opções de túnel.

- Ação de inicialização: a ação a ser executada ao estabelecer o túnel da VPN para uma conexão VPN nova ou modificada. Por padrão, o dispositivo de gateway do cliente inicia o processo de negociação do protocolo IKE para ativar o túnel Você pode especificar que, em vez disso, AWS deve iniciar o processo de negociação do IKE.
- Ação de tempo limite do DPD: a ação a ser executada após atingir o tempo limite do Dead Peer Detection (DPD). Por padrão, a sessão do protocolo IKE é interrompida, o túnel fica inativo e as rotas são removidas. Você pode especificar que AWS deve reiniciar a sessão IKE quando ocorrer o tempo limite do DPD ou pode especificar que não AWS deve realizar nenhuma ação quando o tempo limite do DPD ocorrer.

Regras e limitações

As seguintes regras e limitações são aplicáveis:

- Para iniciar a negociação do IKE, é AWS necessário o endereço IP público do seu dispositivo de gateway do cliente. Se você configurou a autenticação baseada em certificado para sua conexão VPN e não especificou um endereço IP ao criar o recurso de gateway do cliente AWS, deverá criar um novo gateway do cliente e especificar o endereço IP. Depois, modifique a conexão VPN e especifique o novo gateway do cliente. Para obter mais informações, consulte Alterar o gateway do cliente para uma conexão do AWS Site-to-Site VPN.
- A iniciação IKE (ação de inicialização) do AWS lado da conexão VPN é suportada apenas por IKEv2 .
- Se estiver usando a iniciação IKE do AWS lado da conexão VPN, ela não inclui uma configuração de tempo limite. Ela tentará continuamente estabelecer uma conexão até conseguir. Além disso, o AWS lado da conexão VPN reiniciará a negociação do IKE ao receber uma mensagem SA de exclusão do gateway do cliente.
- Se o dispositivo de gateway do cliente estiver protegido por um firewall ou outro dispositivo usando Network Address Translation (NAT), ele deverá ter uma identidade (IDr) configurada. Para obter mais informações sobre IDr, consulte RFC 7296.

Se você não configurar a iniciação do IKE pela AWS lateral do túnel VPN e a conexão VPN passar por um período de inatividade (geralmente 10 segundos, dependendo da configuração), o túnel poderá cair. Para evitar isso, você pode usar uma ferramenta de monitoramento de rede que envie pings keepalive.

Trabalhar com opções de iniciação de túnel da VPN

Para obter mais informações sobre como trabalhar com opções de iniciação de túnel da VPN, consulte os seguintes tópicos:

- Para criar uma conexão VPN e especificar as opções de iniciação de túnel da VPN: Etapa 5: criar uma conexão VPN
- Para modificar as opções de iniciação de túnel da VPN em uma conexão VPN existente: Modificar opções de túnel de AWS Site-to-Site VPN

AWS Site-to-Site VPN substituições de terminais de túneis

Sua conexão Site-to-Site VPN consiste em dois túneis VPN para redundância. Às vezes, um ou ambos os endpoints do túnel VPN são substituídos ao AWS realizar atualizações do túnel ou quando você modifica sua conexão VPN. Durante a substituição de um endpoint de túnel, a conectividade através do túnel pode ser interrompida enquanto o novo endpoint de túnel é provisionado.

Tópicos

- Substituições de endpoint iniciadas pelo cliente
- Substituições de endpoints gerenciados pela AWS
- AWS Site-to-Site VPN controle do ciclo de vida do endpoint do túnel

Substituições de endpoint iniciadas pelo cliente

Quando você modifica os seguintes componentes de sua conexão VPN, um ou ambos os endpoints do túnel são substituídos.

Modificação	Ação da API	Impacto do túnel
Modificar o gateway de destino para a conexão VPN	ModifyVpnConnection	Ambos os túneis estão indisponíveis enquanto

Modificação	Ação da API	Impacto do túnel
		novos endpoints do túnel são provisionados.
Alterar o gateway do cliente para a conexão VPN	ModifyVpnConnection	Ambos os túneis estão indisponíveis enquanto novos endpoints do túnel são provisionados.
Modificar as opções da conexão VPN	ModifyVpnConnectionOptions	Ambos os túneis estão indisponíveis enquanto novos endpoints do túnel são provisionados.
Modificar as opções do túnel da VPN	ModifyVpnTunnelOptions	O túnel modificado não está disponível durante a atualizaç ão.

Substituições de endpoints gerenciados pela AWS

AWS Site-to-Site VPN é um serviço gerenciado e aplica periodicamente atualizações aos endpoints do túnel VPN. Essas atualizações acontecem por vários motivos, incluindo os seguintes:

- Como aplicar atualizações gerais, como patches, aprimoramentos de resiliência e outras melhorias
- Para retirar o hardware subjacente
- Quando o monitoramento automatizado determina que um endpoint de túnel da VPN não está íntegro

AWS aplica atualizações de endpoint de túnel a um túnel de sua conexão VPN por vez. Durante uma atualização de endpoint de túnel, sua conexão de VPN pode sofrer uma breve perda de redundância. Portanto, é importante configurar ambos os túneis em sua conexão VPN para alta disponibilidade.

AWS Site-to-Site VPN controle do ciclo de vida do endpoint do túnel

O controle do ciclo de vida do endpoint do túnel fornece controle sobre o cronograma de substituições do endpoint e pode ajudar a minimizar as interrupções de conectividade durante

as substituições gerenciadas do endpoint do túnel. AWS Com esse recurso, você pode optar por aceitar atualizações AWS gerenciadas para endpoints de túnel no momento que for melhor para sua empresa. Utilize esse recurso se você tiver necessidades comerciais de curto prazo ou puder comportar somente um túnel por conexão de VPN.

> **Note**
>
> Em raras circunstâncias, AWS pode aplicar atualizações críticas aos endpoints do túnel imediatamente, mesmo se o recurso de controle do ciclo de vida do endpoint do túnel estiver ativado.

Tópicos

Como o controle de ciclo de vida do endpoint de túnel funciona

Ative o recurso de controle de ciclo de vida do endpoint de túnel para túneis individuais em uma conexão de VPN. Ele pode ser habilitado no momento da criação da VPN ou modificando as opções de túnel para uma conexão de VPN existente.

Depois que o controle de ciclo de vida do endpoint de túnel for habilitado, você obterá visibilidade adicional sobre os próximos eventos de manutenção do túnel de duas maneiras:

- Você receberá AWS Health notificações sobre futuras substituições de terminais de túneis.
- O status da manutenção pendente, junto com os carimbos de data/hora da Manutenção aplicada automaticamente após e da Última manutenção aplicada, pode ser visto no Console de gerenciamento da AWS ou usando o get-vpn-tunnel-replacement comando -status. AWS CLI

Quando a manutenção de um endpoint de túnel estiver disponível, você terá a oportunidade de aceitar a atualização em um horário que seja conveniente para você, antes do determinado carimbo de data e hora Manutenção aplicada automaticamente após.

Se você não aplicar as atualizações antes da data de aplicação automática da Manutenção, AWS executará automaticamente a substituição do endpoint do túnel logo depois, como parte do ciclo regular de atualização de manutenção.

Habilite o AWS Site-to-Site VPN controle do ciclo de vida do endpoint do túnel

O controle do ciclo de vida do endpoint pode ser ativado em uma conexão VPN nova ou existente. Isso pode ser feito usando o Console de gerenciamento da AWS ou AWS CLI.

> **Note**
>
> Por padrão, quando o recurso para uma conexão de VPN existente é ativado, uma substituição de endpoints de túnel é iniciada ao mesmo tempo. Se quiser ativar o recurso, mas não iniciar a substituição imediata do endpoint de túnel, você pode utilizar a opção Ignorar substituição do túnel.

Existing VPN connection

As etapas a seguir demonstram como habilitar o controle de ciclo de vida do endpoint de túnel em uma conexão de VPN existente.

Para habilitar o controle do ciclo de vida do endpoint do túnel usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do lado esquerdo, escolha Site-to-Site Conexões VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações, Modificar opções de túnel de VPN.
5. Selecione o túnel específico que você deseja modificar escolhendo o Endereço IP externo do túnel VPN apropriado.
6. Em Controle de ciclo de vida do endpoint de túnel, marque a caixa de seleção Habilitar.
7. (Opcional) Selecione Ignorar substituição de túnel.

8. Escolha Salvar alterações.

Para habilitar o controle do ciclo de vida do endpoint do túnel usando o AWS CLI

Use o modify-vpn-tunnel-optionscomando para ativar o controle do ciclo de vida do endpoint do túnel.

New VPN connection

As etapas a seguir demonstram como habilitar o controle de ciclo de vida do endpoint de túnel durante a criação de uma conexão de VPN.

Para habilitar o controle do ciclo de vida do endpoint do túnel durante a criação de uma nova conexão VPN usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Connections (Conexões VPN).
3. Escolha Create VPN Connection (Criar conexão VPN).
4. Nas seções de Opões de túnel 1 e Opções de túnel 2, em Controle de ciclo de vida do endpoint de túnel, selecione Habilitar.
5. Escolha Create VPN Connection (Criar conexão VPN).

Para habilitar o controle do ciclo de vida do endpoint do túnel durante a criação de uma nova conexão VPN usando o AWS CLI

Use o create-vpn-connectioncomando para ativar o controle do ciclo de vida do endpoint do túnel.

Verifique se o controle AWS Site-to-Site VPN do ciclo de vida do endpoint do túnel está ativado

Você pode verificar se o controle do ciclo de vida do endpoint do túnel está habilitado em um túnel VPN existente usando a CLI ou Console de gerenciamento da AWS .

- Se o controle do ciclo de vida do endpoint do túnel estiver desabilitado e você quiser habilitá-lo, consulte Habilitar o controle de ciclo de vida do endpoint de túnel do .
- Se o controle do ciclo de vida do endpoint do túnel estiver ativado e você quiser desativá-lo, consulte Desativar o controle de ciclo de vida do endpoint de túnel do .

Para verificar se o controle do ciclo de vida do endpoint do túnel está ativado usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do lado esquerdo, escolha Site-to-Site Conexões VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione a guia Detalhes do túnel.
5. Nos detalhes do túnel, procure Controle de ciclo de vida do endpoint de túnel, que informará se o recurso está habilitado ou desabilitado.

Para verificar se o controle do ciclo de vida do endpoint do túnel está ativado usando o AWS CLI

Use o describe-vpn-connectionscomando para verificar se o controle do ciclo de vida do endpoint do túnel está ativado.

Verifique as atualizações de AWS Site-to-Site VPN túneis disponíveis

Depois de habilitar o recurso de controle de ciclo de vida do endpoint de túnel, você pode visualizar se uma atualização de manutenção está disponível para sua conexão de VPN utilizando o Console de gerenciamento da AWS ou a CLI. A verificação de uma atualização de túnel Site-to-Site VPN disponível não baixa e implementa automaticamente a atualização. É possível escolher quando deseja implantá-lo. Para obter as etapas para baixar e implantar uma atualização, consulte Aceitar uma atualização de manutenção.

Para verificar as atualizações disponíveis usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do lado esquerdo, escolha Site-to-Site Conexões VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione a guia Detalhes do túnel.
5. Confira a coluna Manutenção pendente. O status será Disponível ou Nenhum.

Para verificar as atualizações disponíveis usando o AWS CLI

Use o comando get-vpn-tunnel-replacement-status para verificar as atualizações disponíveis.

Aceitar uma atualização de manutenção AWS Site-to-Site VPN do túnel

Quando uma atualização de manutenção está disponível, você pode aceitá-la usando a CLI Console de gerenciamento da AWS ou. Você pode optar por aceitar a atualização de manutenção do túnel Site-to-Site VPN em um momento conveniente para você. Depois de aceitar a atualização de manutenção, ela será implantada.

> **Note**
>
> Se você não aceitar a atualização de manutenção, a AWS implantará automaticamente durante um ciclo regular de atualização de manutenção.

Para aceitar uma atualização de manutenção disponível usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do lado esquerdo, escolha Site-to-Site Conexões VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações e, depois, Substituir túnel VPN.
5. Selecione o túnel específico que você deseja substituir escolhendo o Endereço IP externo do túnel VPN.
6. Selecione Replace (Substituir).

Para aceitar uma atualização de manutenção disponível usando o AWS CLI

Use o replace-vpn-tunnelcomando para aceitar uma atualização de manutenção disponível.

Desative o AWS Site-to-Site VPN controle do ciclo de vida do endpoint do túnel

Se você não quiser mais usar o recurso de controle do ciclo de vida do endpoint de túnel, poderá desativá-lo usando o Console de gerenciamento da AWS ou o. AWS CLI Quando você desativar esse recurso, a AWS implantará as atualizações de manutenção automaticamente e periodicamente, e elas poderão ocorrer durante o horário comercial. Para evitar qualquer impacto, é altamente recomendável configurar os dois túneis em sua conexão de VPN para alta disponibilidade.

> **Note**
>
> Embora haja uma manutenção pendente disponível, você não pode especificar a opção Ignorar substituição de túnel ao desativar o recurso. Você sempre pode desativar o recurso sem usar a opção ignorar a substituição do túnel, mas AWS implantará automaticamente as atualizações de manutenção pendentes disponíveis iniciando imediatamente a substituição do endpoint do túnel.

Para desativar o controle do ciclo de vida do endpoint do túnel usando o Console de gerenciamento da AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do lado esquerdo, escolha Site-to-Site Conexões VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações, Modificar opções de túnel de VPN.
5. Selecione o túnel específico que você deseja modificar escolhendo o Endereço IP externo do túnel VPN apropriado.
6. Para desativar o controle de ciclo de vida do endpoint de túnel, em Controle de ciclo de vida do endpoint de túnel, desmarque a caixa de seleção Habilitar.
7. (Opcional) Selecione Ignorar substituição de túnel.
8. Escolha Salvar alterações.

Para desativar o controle do ciclo de vida do endpoint do túnel usando o AWS CLI

Use o modify-vpn-tunnel-optionscomando para desativar o controle do ciclo de vida do endpoint do túnel.

Opções de gateway do cliente para sua conexão AWS Site-to-Site VPN

A tabela a seguir descreve as informações necessárias para criar um recurso de gateway do cliente na AWS.

Item	Descrição
(Opcional) Etiqueta de nome.	Cria uma etiqueta com a chave de “Nome” e um valor especificado por você.
(Apenas roteamento dinâmico) Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.	ASN na faixa de 1–4.294.967.295 é compatível. É possível usar um ASN público já existente e atribuído para a rede, com exceção do seguinte: • 7224: reservado em todas as Regiões • 9059: reservado na região `eu-west-1` • 10124: reservado na região `ap-northeast-1` • 17943: reservado na região `ap-southeast-1` Caso não possua um ASN público, você poderá usar um ASN privado no intervalo de 64.512 a 65.534 a 65.534 ou 4.200.000.000 a 4.294.967.294. O ASN padrão é 64512. Para obter mais informações sobre roteamento, consulte AWS Site-to-Site VPN opções de roteamento.
O endereço IP da interface externa do dispositivo de gateway do cliente.	O endereço IP deve ser estático e pode ser IPv4 ou IPv6. Para endereços IPv4: se o dispositivo de gateway do cliente estiver atrás de um dispositivo de conversão de endereços de rede (NAT), use o endereço IP do dispositivo NAT. Além disso, verifique se os pacotes UDP na porta 500 (e na porta 4500, se o NAT Traversal estiver sendo usado) têm permissão para passar entre sua rede e os endpoints do AWS

Item	Descrição
	Site-to-Site VPN. Consulte Regras de firewall para obter mais informações. Para endereços IPv6: o endereço deve ser um endereço IPv6 válido e roteável pela internet. Endereços IPv6 só são compatíveis com conexões VPN em um gateway de trânsito ou Cloud WAN. Um endereço IP não é necessário quando você usa um certificado privado do Autoridad e de Certificação Privada da AWS e uma VPN pública.

Item	Descrição
(Opcional) Certificado privado de uma CA subordinada usando o AWS Certificate Manager (ACM).	Se você quiser usar a autenticação baseada em certificado, forneça o ARN de um certifica do privado do ACM que será usado no dispositi vo de gateway do cliente. Ao criar um gateway do cliente, você pode configurá-lo para usar certificados privados do Autoridade de Certificação Privada da AWS para autenticar a VPN de local a local. Quando escolher usar essa opção, você criará uma Private Certificate Authority (CA) totalment e hospedada na AWS para uso interno por sua organização. O certificado CA raiz e os certificados CA subordinados são armazenad os e gerenciados pelo CA privada da AWS. Antes de criar o gateway do cliente, crie um certificado privado de uma CA subordina do usando o Autoridade de Certificação Privada da AWS e especifique o certificado ao configurar o gateway do cliente. Para obter informações sobre como criar um certificado privado, consulte Criar e gerenciar uma CA privada no Guia do usuário do Autoridade de Certificação Privada da AWS.
(Opcional) Dispositivo.	Um nome para o dispositivo de gateway do cliente associado a esse gateway do cliente.

Opções de gateway de cliente IPv6

Ao criar um gateway de cliente com um endereço IPv6, considere o seguinte:

- Os gateways de cliente IPv6 só são compatíveis com conexões VPN em um gateway de trânsito ou Cloud WAN.

- O endereço IPv6 deve ser válido e roteável pela internet.
- O dispositivo de gateway do cliente deve permitir endereçamento IPv6 e ser capaz de estabelecer túneis IPsec com endpoints IPv6.
- Para criar um gateway de cliente IPv6 usando a AWS CLI, use um endereço IPv6 para o parâmetro `--ip-address`:

```
aws ec2 create-customer-gateway --ip-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

Conexões aceleradas AWS Site-to-Site VPN

Opcionalmente, você pode ativar a aceleração para sua conexão Site-to-Site VPN. Uma conexão Site-to-Site VPN acelerada (conexão VPN acelerada) é usada AWS Global Accelerator para rotear o tráfego da sua rede local para um ponto de AWS presença mais próximo do seu dispositivo de gateway do cliente.AWS Global Accelerator otimiza o caminho da rede, usando a rede AWS global livre de congestionamento para rotear o tráfego para o endpoint que fornece o melhor desempenho do aplicativo (para obter mais informações, consulte). AWS Global Accelerator É possível usar uma conexão VPN acelerada para evitar interrupções de rede que possam ocorrer quando o tráfego é roteado pela Internet pública.

Quando você cria uma conexão VPN acelerada, criamos e gerenciamos dois aceleradores em seu nome, um para cada túnel VPN. Você não pode visualizar ou gerenciar esses aceleradores sozinho usando o AWS Global Accelerator console ou APIs.

Para obter informações sobre as AWS regiões que oferecem suporte a conexões VPN aceleradas, consulte a VPN AWS acelerada Site-to-Site. FAQs

Habilitar a aceleração

Por padrão, quando você cria uma conexão Site-to-Site VPN, a aceleração é desativada. Opcionalmente, você pode ativar a aceleração ao criar um novo anexo de Site-to-Site VPN em um gateway de trânsito. Para obter mais informações e etapas, consulte Crie uma AWS Site-to-Site VPN conexão.

As conexões VPN aceleradas usam um grupo separado de endereços IP para os endereços IP do endpoint do túnel. Os endereços IP dos dois túneis VPN são selecionados em duas zonas de rede separadas.

Regras e restrições

Para usar uma conexão VPN acelerada, aplicam-se as seguintes regras:

- A aceleração só é suportada para conexões Site-to-Site VPN conectadas a um gateway de trânsito. Os gateways privados virtuais não são compatíveis com conexões VPN aceleradas.
- Uma conexão Site-to-Site VPN acelerada não pode ser usada com uma interface virtual AWS Direct Connect pública.
- Você não pode ativar ou desativar a aceleração de uma conexão Site-to-Site VPN existente. Em vez disso, você pode criar uma nova conexão Site-to-Site VPN com aceleração ativada ou desativada conforme necessário. Em seguida, configure seu dispositivo de gateway do cliente para usar a nova conexão Site-to-Site VPN e excluir a conexão Site-to-Site VPN antiga.
- O NAT-traversal (NAT-T) é necessário para uma conexão VPN acelerada e é habilitado por padrão. Se você fez download de um arquivo de configuração do console da Amazon VPC, verifique a configuração NAT-T e ajuste-a, se necessário.
- A negociação IKE para túneis VPN acelerados deve ser iniciada no dispositivo de gateway do cliente. As duas opções de túnel que afetam esse comportamento são `Startup Action` e `DPD Timeout Action`. Consulte Opções de túnel VPN e Opções de iniciação do túnel da VPN para obter mais informações.
- Site-to-Site As conexões VPN que usam autenticação baseada em certificado podem não ser compatíveis com AWS Global Accelerator, devido ao suporte limitado à fragmentação de pacotes no Global Accelerator. Para ter mais informações, consulte Como o AWS Global Accelerator funciona. Se for necessária uma conexão VPN acelerada que use a autenticação baseada em certificado, o dispositivo de gateway do cliente deverá ser compatível com a fragmentação IKE. Caso contrário, não habilite sua VPN para aceleração.

AWS Site-to-Site VPN opções de roteamento

AWS recomenda anunciar rotas BGP específicas para influenciar as decisões de roteamento no gateway privado virtual. Verifique as informações sobre comandos específicos do dispositivo na documentação do fornecedor.

Ao criar várias conexões VPN, o gateway privado virtual envia tráfego de rede para a conexão VPN apropriada, usando rotas atribuídas estaticamente ou anúncios de rotas de BGP. Qual rota será usada dependerá de como a conexão VPN foi configurada. Quando há rotas idênticas no gateway privado virtual, deve-se preferir as rotas atribuídas estaticamente, em detrimento das rotas

anunciadas pela BGP. Se você optar por usar o anúncio do BGP, não poderá especificar rotas estáticas.

Para obter mais informações sobre prioridade de rotas, consulte Tabelas de rotas e prioridade de rota.

Ao criar uma conexão Site-to-Site VPN, você deve fazer o seguinte:

- Especifique o tipo de roteamento que você planeja usar (estático ou dinâmico)
- Atualize a tabela de rotas da sub-rede

Existem cotas para o número de rotas que podem ser adicionadas a uma tabela de rotas. Para obter mais informações, consulte a seção Tabelas de rotas em Cotas da Amazon VPC no Guia do usuário da Amazon VPC.

Tópicos

Roteamento estático e dinâmico em AWS Site-to-Site VPN

O tipo de roteamento selecionado pode depender da marca e do modelo do dispositivo de gateway do cliente. Se o dispositivo de gateway do cliente suportar o Border Gateway Protocol (BGP), especifique o roteamento dinâmico ao configurar sua Site-to-Site conexão VPN. Se o dispositivo de gateway do cliente não for compatível com BGP, especifique o roteamento estático.

> **Note**
>
> Site-to-Site Os concentradores VPN suportam somente o roteamento BGP. O roteamento estático não é suportado para conexões VPN que usam um Site-to-Site VPN Concentrator.

Se você usa um dispositivo compatível com publicidade BGP, não especifica rotas estáticas para a conexão Site-to-Site VPN porque o dispositivo usa o BGP para anunciar suas rotas para o gateway

privado virtual. Caso use um dispositivo que não seja compatível com publicidade BGP, selecione o roteamento estático e insira as rotas (prefixos IP) para a rede que fazem a comunicação com o gateway privado virtual.

Recomendamos, quando disponíveis, o uso de dispositivos compatíveis com o protocolo BGP que verificam se a detecção é de boa qualidade, o quê pode ajudar o failover para o segundo túnel VPN, caso haja uma redução do primeiro túnel. Os dispositivos que não são compatíveis com o BGP também podem fazer a verificação de integridade, auxiliando o failover para o segundo túnel, quando necessário.

Você deve configurar seu dispositivo de gateway do cliente para rotear o tráfego da sua rede local para a conexão Site-to-Site VPN. A configuração depende da marca e do modelo do seu dispositivo. Para obter mais informações, consulte AWS Site-to-Site VPN dispositivos de gateway do cliente.

Tabelas de rotas e prioridade de AWS Site-to-Site VPN rotas

Tabelas de rotas determinam para onde o tráfego da VPC é direcionado. Na tabela de rotas da VPC, adicione uma rota à rede remota e especifique o gateway privado virtual como destino. Isso permite que o tráfego da VPC destinado para a rede remota seja roteado por meio do gateway privado virtual e sobre um dos túneis VPN. É possível habilitar a propagação automática de rotas da rede para a tabela de rotas.

Para determinar como o tráfego deve ser roteado, usamos a rota mais específica em sua tabela de rotas que corresponde ao tráfego (correspondência de prefixo mais longa). Se a tabela de rotas tiver rotas sobrepostas ou correspondentes, as seguintes regras serão aplicadas:

- Se as rotas propagadas de uma conexão Site-to-Site VPN ou Direct Connect conexão se sobrepuserem à rota local da sua VPC, a rota local será a preferida, mesmo que as rotas propagadas sejam mais específicas.
- Se as rotas propagadas de uma conexão ou Direct Connect conexão Site-to-Site VPN tiverem o mesmo bloco CIDR de destino de outras rotas estáticas existentes (a correspondência de prefixo mais longa não pode ser aplicada), priorizamos as rotas estáticas cujos destinos são um gateway de internet, um gateway privado virtual, uma interface de rede, um ID de instância, uma conexão de emparelhamento de VPC, um gateway NAT, um gateway de trânsito ou um gateway VPC endpoint.

Por exemplo, a tabela de rotas a seguir tem uma rota estática para um gateway da Internet e uma rota propagada para um gateway privado virtual. O destino de ambas as rotas é `172.31.0.0/24`.

Nesse caso, todo tráfego destinado para `172.31.0.0/24` é roteado para o gateway da Internet – é uma rota estática e, portanto, tem prioridade sobre a rota propagada.

Destino	Destino
10.0.0.0/16	Local
172.31.0.0/24	vgw-11223344556677889 (propagado)
172.31.0.0/24	igw-12345678901234567 (estático)

Somente os prefixos IP que sejam conhecidos do gateway privado virtual, seja por meio de anúncios BGP ou de uma entrada da rota estática, podem receber o tráfego da VPC. O gateway privado virtual não roteia nenhum outro tráfego cujo destino seja fora dos anúncios BGP recebidos, das entradas de rota estática ou do CIDR da VPC anexada. Os gateways privados virtuais não oferecem suporte ao IPv6 tráfego.

Quando um gateway privado virtual recebe informações de roteamento, ele usa a seleção de caminho para determinar como rotear o tráfego. A correspondência de prefixo mais longa se aplicará se todos os endpoints estiverem íntegros. A integridade de um endpoint de túnel tem precedência sobre outros atributos de roteamento. Essa precedência se aplica a VPNs gateways privados virtuais e gateways de trânsito. Se os prefixos forem os mesmos, o gateway privado virtual prioriza as rotas da seguinte forma, da mais preferida para a menos preferida:

- Rotas propagadas pelo BGP a partir de uma conexão Direct Connect

  As rotas do Blackhole não são propagadas para um gateway de cliente Site-to-Site VPN via BGP.
- Rotas estáticas adicionadas manualmente para uma conexão Site-to-Site VPN
- Rotas propagadas pelo BGP a partir de uma conexão VPN Site-to-Site
- Para combinar prefixos em que cada conexão Site-to-Site VPN usa BGP, o AS PATH é comparado e o prefixo com o AS PATH mais curto é preferido.

> **Note**
>
> AWS recomenda fortemente o uso de dispositivos de gateway do cliente que suportem roteamento assimétrico.

Para dispositivos de gateway do cliente compatíveis com roteamento assimétrico, nós não recomendamos usar o prefixo AS PATH, para garantir que os dois túneis tenham um AS PATH igual. Isso ajuda a garantir que o valor multi-exit discriminator (MED) que definimos em um túnel durante as atualizações de endpoint do túnel VPN seja usado para determinar a prioridade do túnel.
Para dispositivos de gateway do cliente incompatíveis com o roteamento assimétrico, use no início AS PATH e a preferência local para escolher um túnel em vez do outro. No entanto, quando o caminho de saída muda, o tráfego pode cair.

- Quando o PATHs AS tem o mesmo comprimento e se o primeiro AS no AS_SEQUENCE é o mesmo em vários caminhos, multi-exit discriminators (MEDs) são comparados. O caminho com o menor valor MED será o preferido.

A prioridade de rota é afetada durante as atualizações de endpoint do túnel de VPN.

Em uma conexão Site-to-Site VPN, AWS seleciona um dos dois túneis redundantes como o caminho de saída principal. Essa seleção pode mudar às vezes, e é altamente recomendável que você configure ambos os túneis para alta disponibilidade e permita o roteamento assimétrico. A integridade de um endpoint de túnel tem precedência sobre outros atributos de roteamento. Essa precedência se aplica a VPNs gateways privados virtuais e gateways de trânsito.

Para um gateway privado virtual, um túnel em todas as conexões Site-to-Site VPN no gateway será selecionado. Para usar mais de um túnel, recomendamos explorar o Equal Cost Multipath (ECMP), que é compatível com conexões Site-to-Site VPN em um gateway de trânsito. Para obter mais informações, consulte Gateways de trânsito em Gateways de trânsito da Amazon VPC. O ECMP não é compatível com conexões Site-to-Site VPN em um gateway privado virtual.

Para conexões Site-to-Site VPN que usam BGP, o túnel primário pode ser identificado pelo valor multi-exit discriminator (MED). Recomendamos anunciar rotas BGP mais específicas para influenciar as decisões de roteamento.

Para conexões Site-to-Site VPN que usam roteamento estático, o túnel primário pode ser identificado por estatísticas ou métricas de tráfego.

Roteamento durante atualizações de endpoint do túnel de VPN

Uma conexão Site-to-Site VPN consiste em dois túneis VPN entre um dispositivo de gateway do cliente e um gateway privado virtual ou um gateway de trânsito. Recomendamos que você configure ambos os túneis para redundância. De tempos em tempos, AWS também realiza manutenção de

rotina em sua conexão VPN, o que pode desativar brevemente um dos dois túneis da sua conexão VPN. Para obter mais informações, consulte Notificações de substituição de endpoint do túnel.

Quando realizamos atualizações em um túnel de VPN, definimos um valor menor de multi-exit discriminator (MED) no outro túnel. Se você configurou o dispositivo de gateway do cliente para usar os dois túneis, a conexão VPN usará o outro túnel (ativo) durante o processo de atualização do endpoint do túnel.

> **Note**
>
> - Para garantir que o túnel ativo com o valor MED inferior seja o preferencial, certifique-se de que o dispositivo de gateway do cliente use os mesmos valores de Peso e Preferência Local para ambos os túneis (Peso e Preferência Local têm prioridade mais alta do que MED).

Tráfego IPv4 e IPv6 no AWS Site-to-Site VPN

A conexão do Site-to-Site VPN em um gateway de trânsito pode ser compatível com tráfego IPv4 ou IPv6 dentro dos túneis VPN. Por padrão, uma conexão da Site-to-Site VPN é compatível com o tráfego IPv4 dentro dos túneis VPN. É possível configurar uma nova conexão da Site-to-Site VPN para ser compatível com o tráfego IPv6 dentro dos túneis VPN. Depois, se a VPC e a rede local estiverem configuradas para endereçamento IPv6, você poderá enviar tráfego IPv6 pela conexão VPN.

Se você habilitar o IPv6 para os túneis VPN da conexão da Site-to-Site VPN, cada túnel terá dois blocos CIDR. Um é um bloco CIDR do IPv4 de tamanho /30 e o outro é um bloco CIDR do IPv6 de tamanho /126.

Suporte a IPv4 e IPv6

As conexões do Site-to-Site VPN são compatíveis com as seguintes configurações de IP:

- Túnel externo IPv4 com pacotes internos IPv4: o recurso básico de VPN IPv4 permitido em gateways privados virtuais, gateways de trânsito e Cloud WAN.
- Túnel externo IPv4 com pacotes internos IPv6: permite aplicações/transporte IPv6 dentro do túnel VPN. Compatível com gateways de trânsito e Cloud WAN. Não há compatibilidade para gateways privados virtuais.

- Túnel externo IPv6 com pacotes internos IPv6: permite a migração completa de IPv6 com endereços IPv6 para IPs de túnel externo e IPs de pacotes internos. Compatível tanto com gateways de trânsito quanto com Cloud WAN.
- Túnel externo IPv6 com pacotes internos IPv4: permite endereçamento de túnel externo IPv6 ao mesmo tempo em que oferece suporte a aplicações IPv4 legadas dentro do túnel. Compatível tanto com gateways de trânsito quanto com Cloud WAN.

As seguintes regras se aplicam:

- É possível usar endereços IPv6 para IPs de túnel externo somente em conexões do Site-to-Site VPN que são encerradas em um gateway de trânsito ou Cloud WAN. As conexões do Site-to-Site VPN em um gateway privado virtual não são compatíveis com IPv6 para IPs de túnel externo.
- Ao usar IPv6 para IPs de túnel externo, você deve atribuir endereços IPv6 do lado da AWS da conexão VPN e no gateway do cliente para ambos os túneis VPN.
- Não é possível habilitar o suporte a IPv6 para uma conexão existente do Site-to-Site VPN. Nesse caso, você deverá excluir a conexão existente e criar outra.
- Uma conexão do Site-to-Site VPN não consegue processar tráfego IPv4 e IPv6 simultaneamente. Os pacotes encapsulados internos podem ser IPv6 ou IPv4, mas não ambos. Você precisa de conexões do Site-to-Site VPN para transportar pacotes IPv4 e IPv6.
- As VPNs de IP privado não aceitam endereços IPv6 para IPs de túnel externo. Elas usam endereços RFC 1918 ou CGNAT. Para ter mais informações sobre o RFC 1918, consulte Address Allocation for Private Internets, no “RFC 1918”.
- As VPNs IPv6 comportam os mesmos limites de throughput (Gbps e PPS), MTU e rota das VPNs IPv4.
- A criptografia IPSec e a troca de chaves funcionam da mesma forma para VPNs IPv4 e IPv6.

Para ter mais informações sobre como criar uma conexão VPN com suporte a IPv6, consulte Criar uma conexão VPN em “Comece com o Site-to-Site VPN”.

AWS Site-to-Site VPN Concentradores

O AWS Site-to-Site VPN Concentrator é um novo recurso que simplifica a conectividade de vários sites para empresas distribuídas. O VPN Concentrator é adequado para clientes que precisam conectar mais de 25 locais remotos à AWS, com cada site precisando de baixa largura de banda (menos de 100 Mbps).

Serviços e recursos de gateway compatíveis

Os concentradores de VPN são compatíveis somente com o Transit Gateway. Esse recurso não é compatível com o Cloud WAN ou o Virtual Private Gateway.

A tabela a seguir descreve os recursos suportados pelo Site-to-Site VPN Concentrator:

Recurso	Compatível?
IPv6	Sim
Conexões VPN privadas do Direct Connect	Não
VPN acelerada	Sim
Vários dispositivos de gateway de clientes do mesmo site	Sim. No entanto, cada dispositivo de gateway do cliente deve ter um endereço IP exclusivo.
Restrições geográficas	Não. Você pode anexar um site localizado em qualquer região a um concentrador em qualquer AWS região.
Site-to-Site Registros de VPN	Sim. Você pode gerar registros de VPN para todos os sites conectados ao Concentrator ou individua lmente.
Suporte à criptografia do Transit Gateway	Não

Largura de banda

Atualmente, os concentradores Site-to-Site VPN suportam largura de banda agregada de 5 Gbps. Cada site pode suportar uma largura de banda máxima de 100 Mbps. No entanto, se você precisar de maior largura de banda, entre em contato com AWS Support.

Roteamento

Site-to-Site Os concentradores VPN suportam somente o roteamento BGP (Border Gateway Protocol). O roteamento estático não é suportado.

Todos os gateways do cliente conectados ao Site-to-Site VPNConcentrator usam o mesmo anexo do Site-to-Site VPN Concentrator ao gateway de trânsito para roteamento. Cada site conectado ao Site-to-Site VPN Concentrator pode enviar no máximo 5.000 rotas do gateway de trânsito para um gateway do cliente e 1.000 rotas do gateway do cliente para o gateway de trânsito.

Alocação de endereço IP

Cada conexão VPN por meio do Site-to-Site VPN Concentrator ainda terá um endereço IP exclusivo da AWS (um por túnel).

Monitoramento

As conexões VPN via Site-to-Site VPN Concentrators suportam as mesmas métricas das conexões VPN regulares.

Ao ativar os registros de fluxo do Transit Gateway no anexo do VPN Concentrator, você verá os registros de fluxo de todo o tráfego que entra e sai de todos os sites remotos conectados ao concentrador.

Manutenção do túnel

A manutenção do túnel funciona da mesma forma que os túneis Site-to-Site VPN padrão existentes para ambos os endpoints ao usar um Site-to-Site VPN Concentrator. Consulte Substituições de endpoint para obter mais informações.

Preços

Informações sobre preços do Site-to-Site VPN Concentrator podem ser encontradas na página de preços de VPN da AWS.

Comece com AWS Site-to-Site VPN

Use o procedimento a seguir para configurar uma AWS Site-to-Site VPN conexão. Durante a criação, você especificará um gateway privado virtual, um gateway de trânsito, um concentrador de Site-to-Site VPN ou “Não associado” como o tipo de gateway de destino. Se você especificar “Não associado”, poderá escolher o tipo de gateway de destino posteriormente ou usá-lo como um anexo VPN para o AWS Cloud WAN. Este tutorial ajuda você a criar uma conexão VPN usando um gateway privado virtual. Ele presume que você já tenha uma VPC com uma ou mais sub-redes.

Para configurar uma conexão VPN usando um gateway privado virtual, conclua as seguintes etapas:

Tarefas

- Pré-requisitos
- Etapa 1: criar um gateway do cliente
- Etapa 2: criar um gateway de destino
- Etapa 3: configurar o roteamento
- Etapa 4: atualizar o grupo de segurança
- Etapa 5: criar uma conexão VPN
- Etapa 6: baixar o arquivo de configuração
- Etapa 7: configurar o dispositivo de gateway do cliente

Tarefas relacionadas

- Para criar uma conexão VPN para o AWS Cloud WAN, consulteCrie uma conexão VPN Cloud WAN usando a CLI ou a API.
- Para criar uma conexão VPN em um gateway de trânsito, consulte Criar uma conexão VPN.

Pré-requisitos

Você precisa das informações a seguir para definir e configurar os componentes de uma conexão VPN.

Item	Informações
Dispositivo de gateway do cliente	O dispositivo físico ou de software no seu lado da conexão VPN. Você precisa do fornecedor (por exemplo, Cisco), da plataforma (por exemplo, roteadores da série ISR) e da versão do software (por exemplo, IOS 12.4).
Gateway do cliente	Para criar o recurso de gateway do cliente em AWS, você precisa das seguintes informações: • O endereço IP roteável na Internet para a interface externa do dispositivo. • O tipo de roteamento: estático ou dinâmico • Para roteamento dinâmico, o número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) • (Opcional) Certificado privado de Autoridade de Certificação Privada da AWS para autenticar sua VPN Para obter mais informações, consulte Opções de gateway do cliente.
(Opcional) O ASN para o AWS lado da sessão do BGP	Isso é especificado ao criar um gateway privado virtual ou um gateway de trânsito. Se você não especificar um valor, o ASN padrão será aplicado. Para obter mais informações, consulte Gateway privado virtual.
Conexão VPN	Para criar uma conexão VPN, você precisa das seguintes informações: • Para roteamento estático, os prefixos IP para a rede privada. • (Opcional) Opções de túnel para cada túnel de VPN. Para obter mais informações,

Item	Informações
	consulte Opções de túnel para sua AWS Site-to-Site VPN conexão.

Etapa 1: criar um gateway do cliente

Um gateway do cliente fornece informações AWS sobre seu dispositivo de gateway do cliente ou aplicativo de software. Para obter mais informações, consulte Gateway do cliente.

Se você planeja usar um certificado privado para autenticar sua VPN, crie um certificado privado de uma CA subordinada usando. Autoridade de Certificação Privada da AWS Para obter informações sobre como criar um certificado privado, consulte Criar e gerenciar uma CA privada no Guia do usuário do Autoridade de Certificação Privada da AWS .

> **Note**
>
> É necessário especificar um endereço IP ou o nome de recurso da Amazon do certificado privado.

Para criar um gateway do cliente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways do cliente.
3. Escolha Criar gateway do cliente.
4. (Opcional) Em Name (Nome), insira um nome para o gateway do cliente. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
5. Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.
6. Em Tipo de endereço IP, escolha uma das seguintes opções:
   - IPv4- (Padrão) Especifique um IPv4 endereço para seu dispositivo de gateway do cliente.
   - IPv6- Especifique um IPv6 endereço para seu dispositivo de gateway do cliente. Essa opção é necessária ao criar uma conexão VPN com o túnel IPv6 externo IPs.

7. Em Endereço IP, insira o endereço IP estático roteável pela internet do dispositivo de gateway do cliente. Se o dispositivo de gateway do cliente estiver atrás de um dispositivo NAT que seja habilitado para NAT-T, use o endereço IP público do dispositivo NAT.
8. (Opcional) Se você quiser usar um certificado privado, em Certificate ARN (Certificado ARN), selecione o nome de recurso da Amazon do certificado privado.
9. (Opcional) Em Dispositivo, insira um nome para o gateway do cliente associado a esse gateway do cliente.
10. Escolha Criar gateway do cliente.

Para criar um gateway do cliente usando a linha de comando ou a API

- CreateCustomerGateway(API de consulta do Amazon EC2)
- create-customer-gateway (AWS CLI)

  Exemplo de criação de um gateway de IPv6 cliente:

```
aws ec2 create-customer-gateway --ipv6-address
 2001:0db8:85a3:0000:0000:8a2e:0370:7334 --bgp-asn 65051 --type ipsec.1 --region us-
west-1
```

- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Etapa 2: criar um gateway de destino

Para estabelecer uma conexão VPN entre sua VPC e sua rede local, você deve criar um gateway de destino no AWS lado da conexão. O gateway de destino pode ser um gateway privado virtual ou um gateway de trânsito.

Criar um gateway privado virtual

Quando você cria um gateway privado virtual, é possível especificar um Número de sistema autônomo (ASN) privado e personalizado para o lado da Amazon do gateway ou usar o ASN padrão da Amazon. Esse ASN deve ser diferente do BGP ASN especificado para o gateway do cliente.

Depois que você criar um gateway privado virtual, você deve anexá-lo à sua VPC.

Para criar um gateway privado virtual e anexá-lo à sua VPC

1. No painel de navegação, escolha Gateways privados virtuais.
2. Escolha Create virtual private gateway (Criar gateway privado virtual).
3. (Opcional) Em Etiqueta de nome, insira um nome para o gateway privado virtual. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
4. Em Número de sistema autônomo (ASN), mantenha a seleção padrão, ASN padrão da Amazon, para usar o ASN padrão da Amazon. Caso contrário, selecione Custom ASN (Personalizar ASN) e insira um valor. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar no intervalo de 4200000000 a 4294967294.
5. Escolha Create virtual private gateway (Criar gateway privado virtual).
6. Selecione o gateway privado virtual e, depois, escolha Actions (Ações), Attach to VPC (Anexar à VPC).
7. VPCsEm Disponível, escolha sua VPC e, em seguida, escolha Anexar à VPC.

Para criar um gateway privado virtual usando a linha de comando ou a API

- CreateVpnGateway(API de consulta do Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para anexar um gateway privado virtual a uma VPC usando a linha de comando ou a API

- AttachVpnGateway(API de consulta do Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Criar um gateway de trânsito

Para obter mais informações sobre como criar um gateway de trânsito, consulte Gateways de trânsito em Gateways de trânsito da Amazon VPC.

Etapa 3: configurar o roteamento

Para permitir que as instâncias na VPC acessem o gateway do cliente, é necessário configurar a tabela de rotas para incluir as rotas usadas pela conexão VPN e apontá-las para o gateway privado virtual ou o gateway de trânsito.

(Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas

Você pode ativar a propagação de rotas para sua tabela de rotas para propagar automaticamente as rotas de Site-to-Site VPN.

Para o roteamento estático, os prefixos IP estáticos especificados para a configuração VPN serão propagados para a tabela de rotas sempre que o status da conexão VPN for UP. Da mesma forma, para o roteamento dinâmico, as rotas anunciadas no BGP a partir do gateway do cliente também serão propagadas para a tabela de rotas sempre que o status da conexão VPN for UP.

> **Note**
>
> Se a conexão for interrompida, mas a conexão VPN permanecer no estado UP, todas as rotas propagadas que estão na tabela de rotas não serão removidas automaticamente. Tenha isso em mente se, por exemplo, você quiser que o tráfego faça failover para uma rota estática. Nesse caso, talvez seja necessário desabilitar a propagação de rotas para remover as rotas propagadas.

Para ativar a propagação de rotas usando o console

1. No painel de navegação, escolha Route tables.
2. Selecione a tabela de rotas associada à sub-rede.
3. Na guia Propagação de rotas, selecione Editar propagação de rotas. Selecione o gateway privado virtual que você criou no procedimento anterior e escolha Salvar.

> **Note**
>
> Se você não habilitar a propagação de rotas, será necessário inserir manualmente as rotas estáticas usadas pela conexão VPN. Para fazer isso, selecione a tabela de rotas, escolha Routes (Rotas), Edit (Editar). Em Destino, adicione a rota estática usada pela sua conexão

Site-to-Site VPN. Em Destination (Destino), selecione o ID do gateway privado virtual, e escolha Save (Salvar).

Para desativar a propagação de rotas usando o console

1. No painel de navegação, escolha Route tables.
2. Selecione a tabela de rotas associada à sub-rede.
3. Na guia Propagação de rotas, selecione Editar propagação de rotas. Limpe a caixa de seleção Propagar do gateway privado virtual.
4. Escolha Salvar.

Para ativar a propagação de rotas usando a linha de comando ou a API

- EnableVgwRoutePropagation(API de consulta do Amazon EC2)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Para desativar a propagação de rotas usando a linha de comando ou a API

- DisableVgwRoutePropagation(API de consulta do Amazon EC2)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

(Gateway de trânsito) Adicionar uma rota à tabela de rotas

Se você habilitou a propagação da tabela de rotas para o gateway de trânsito, as rotas para o anexo da VPN são propagadas para a tabela de rotas do gateway de trânsito. Para obter mais informações, consulte Roteamento em Gateways de trânsito da Amazon VPC.

Se você anexar uma VPC ao gateway de trânsito e quiser habilitar recursos na VPC para acessar o gateway do cliente, será necessário adicionar uma rota à tabela de rotas da sub-rede para apontar para o gateway de trânsito.

Para adicionar uma rota a uma tabela de roteamento da VPC

1. No painel de navegação, escolha Tabelas de rotas.
2. Selecione uma tabela de rotas associada à VPC.
3. Na guia Rotas, escolha Editar rotas.
4. Escolha Adicionar rota.
5. Na coluna Destino, insira o intervalo de endereços IP de destino. Em Target (Destino), escolha o gateway de trânsito.
6. Escolha Salvar alterações.

Etapa 4: atualizar o grupo de segurança

Para permitir acesso às instâncias na VPC de sua rede, você deve atualizar as regras de grupo de segurança para permitir o acesso SSH, RDP e ICMP de entrada.

Como adicionar regras ao grupo de segurança para permitir o acesso

1. No painel de navegação, selecione Grupos de segurança.
2. Selecione o grupo de segurança ao qual você deseja conceder acesso para as instâncias em sua VPC.
3. Na guia Regras de entrada, selecione Editar regras de entrada.
4. Adicione as regras que permitem acesso SSH, RDP e ICMP de entrada da rede e selecione Salvar regras. Para obter mais informações, consulte Regras de grupos de segurança no Guia do usuário da Amazon VPC.

Etapa 5: criar uma conexão VPN

Para criar a conexão VPN, use o gateway do cliente com o gateway privado virtual ou o gateway de trânsito criado anteriormente.

Para criar uma conexão VPN

1. No painel de navegação, escolha Conexões Site-to-Site VPN.
2. Escolha Create VPN Connection (Criar conexão VPN).

3. (Opcional) Em Etiqueta de nome, insira um nome para a conexão VPN. Ao fazer isso, é criada uma marcação com a chave de `Name` e o valor que você especificar.
4. Em Target gateway type (Tipo de gateway de destino), selecione Virtual private gateway (Gateway privado virtual) ou Transit gateway (Gateway de trânsito). Depois, selecione o gateway privado virtual ou o gateway de trânsito criado anteriormente.
5. Em Gateway do cliente, selecione Existente e, depois, escolha o gateway do cliente criado anteriormente em ID do gateway do cliente.
6. Escolha uma das opções de roteamento dependendo se o seu dispositivo de gateway do cliente é compatível com o Protocolo de Gateway da Borda (BGP):

   - Se o dispositivo de gateway do cliente for compatível com o BGP, selecione Dynamic (requires BGP) (Dinâmico [requer BGP]).
   - Se o dispositivo de gateway do cliente não for compatível com o BGP, selecione Static (Estático). Em Static IP Prefixes (Prefixos do IP estático), especifique cada prefixo IP para a rede privada da conexão VPN.
7. Escolha o tipo de armazenamento de chaves pré-compartilhadas:

   - Padrão — A chave pré-compartilhada é armazenada diretamente no serviço Site-to-Site VPN.
   - Secrets Manager — A chave pré-compartilhada é armazenada usando AWS Secrets Manager. Para ter mais informações sobre o Secrets Manager, consulte Recursos de segurança aprimorados usando o Secrets Manager.
8. Se o tipo de gateway de destino for gateway de trânsito, para a versão Tunnel inside IP, especifique se os túneis VPN oferecem suporte IPv4 ou IPv6 tráfego. IPv6 o tráfego só é suportado para conexões VPN em um gateway de trânsito.
9. Se você especificou IPv4a versão Túnel dentro do IP, você pode, opcionalmente, especificar os intervalos de IPv4 CIDR para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão é `0.0.0.0/0`.

   Se você especificou IPv6a versão Túnel dentro do IP, você pode, opcionalmente, especificar os intervalos de IPv6 CIDR para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão para ambos os intervalos é `::/0`.
10. Em Tipo de endereço IP externo, escolha uma das seguintes opções:

    - PublicIpv4 - (Padrão) Use IPv4 endereços para o túnel externo IPs.
    - IPv6- Use IPv6 endereços para o túnel externo IPs. Essa opção só está disponível para conexões VPN em um gateway de trânsito ou Cloud WAN.

11. (Opcional) Em Opções de túnel, é possível especificar as seguintes informações para cada túnel:

    - Um bloco IPv4 CIDR de tamanho /30 do `169.254.0.0/16` intervalo dos endereços internos do túnel IPv4 .
    - Se você especificou IPv6a versão IP do túnel interno, um bloco IPv6 CIDR /126 do `fd00::/8` intervalo dos endereços do túnel IPv6 interno.
    - A chave pré-compartilhada do IKE (PSK). As seguintes versões são suportadas: IKEv1 ou IKEv2.
    - Para editar as opções avançadas do túnel, escolha Editar opções de túnel. Para obter mais informações, consulte Opções de túnel VPN.

12. Escolha Create VPN Connection (Criar conexão VPN). Pode levar alguns minutos para criar a conexão VPN.

Para criar uma conexão VPN usando a linha de comando ou a API

- CreateVpnConnection(API de consulta do Amazon EC2)
- create-vpn-connection (AWS CLI)

  Exemplo de criação de uma conexão VPN com túnel IPv6 externo IPs e túnel IPv6 interno IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

  Exemplo de criação de uma conexão VPN com túnel IPv6 externo IPs e túnel IPv4 interno IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Etapa 6: baixar o arquivo de configuração

Depois de criar a conexão VPN, você poderá baixar um arquivo de configuração de exemplo para usar na configuração do dispositivo de gateway do cliente.

> **Important**
>
> O arquivo de configuração é apenas um exemplo e pode não corresponder totalmente às configurações da conexão VPN pretendidas. Ele especifica os requisitos mínimos para uma conexão VPN do grupo 2 do AES128 Diffie-Hellman na maioria das AWS regiões e do grupo 14 do Diffie-Hellman nas regiões. SHA1 AES128 SHA2 AWS GovCloud Ele também especifica chaves pré-compartilhadas para autenticação. Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6
> Introduzimos IKEv2 suporte nos arquivos de configuração para muitos dispositivos populares de gateway de clientes e continuaremos adicionando arquivos adicionais ao longo do tempo. Para obter uma lista de arquivos de configuração com IKEv2 suporte, consulteAWS Site-to-Site VPN dispositivos de gateway do cliente.

Permissões

Para carregar adequadamente a tela de configuração de download a partir do Console de gerenciamento da AWS, você deve garantir que sua função ou usuário do IAM tenha permissão para o seguinte Amazon EC2 APIs: e. `GetVpnConnectionDeviceTypes` `GetVpnConnectionDeviceSampleConfiguration`

Como baixar o arquivo de configuração usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão VPN e escolha Baixar a configuração.
4. Escolha o fornecedor, a plataforma, o software e a versão do IKE que correspondem ao dispositivo do gateway do cliente. Se o dispositivo não estiver listado, selecione Generic (Genérico).
5. Escolha Download.

Para baixar um arquivo de configuração de exemplo usando a linha de comando ou API da

- GetVpnConnectionDeviceTypes(API do Amazon EC2)
- GetVpnConnectionDeviceSampleConfiguration(API de consulta do Amazon EC2)
- get-vpn-connection-device-tipos ()AWS CLI
- get-vpn-connection-device-configuração de amostra ()AWS CLI

Etapa 7: configurar o dispositivo de gateway do cliente

Use o arquivo de configuração de exemplo para configurar os dispositivos de gateway do cliente. O dispositivo de gateway do cliente é o dispositivo físico ou software situado no seu lado da conexão VPN. Para obter mais informações, consulte AWS Site-to-Site VPN dispositivos de gateway do cliente.

AWS Site-to-Site VPN cenários arquitetônicos

Veja a seguir os cenários em que você pode criar várias conexões VPN com um ou mais dispositivos de gateway do cliente.

Várias conexões VPN usando o mesmo dispositivo de gateway do cliente

Você pode criar conexões VPN adicionais de sua localização local para outra VPCs usando o mesmo dispositivo de gateway do cliente. É possível reutilizar o mesmo endereço IP de gateway do cliente para cada uma das conexões VPN.

Vários dispositivos de gateway do cliente em um único gateway privado virtual (Site-to-Site VPN CloudHub)

É possível estabelecer várias conexões VPN com um único gateway privado virtual a partir de vários gateways do cliente. Isso permite que você tenha vários locais conectados à AWS VPN CloudHub. Para obter mais informações, consulte Comunicação segura entre AWS Site-to-Site VPN conexões usando VPN CloudHub. Quando há dispositivos de gateway do cliente em várias localizações geográficas, cada dispositivo deve anunciar um conjunto exclusivo de intervalos de IP específicos da localização.

Conexão VPN redundante usando um segundo dispositivo de gateway do cliente

Para se proteger contra uma perda de conectividade, caso o dispositivo de gateway do cliente fique indisponível, é possível configurar uma segunda conexão VPN usando um segundo dispositivo de gateway do cliente. Para obter mais informações, consulte Conexões do AWS Site-to-Site VPN redundantes para failover. Ao estabelecer dispositivos de gateway do cliente redundantes em uma única localização, os dois dispositivos devem anunciar os mesmos intervalos de IP.

A seguir estão as arquiteturas comuns de Site-to-Site VPN:

- Conexões VPN única e múltipla
- the section called “Conexões VPN redundantes”
- Comunicações seguras entre conexões VPN usando VPN CloudHub

Exemplos de conexão única e de várias conexões VPN do AWS Site-to-Site VPN

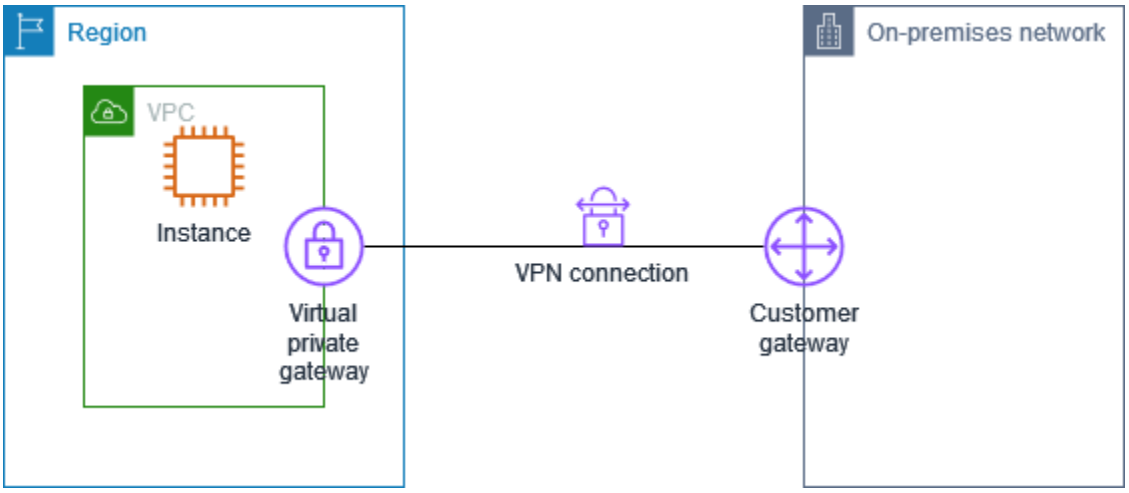
Os diagramas a seguir exibem tanto uma única como várias conexões da Site-to-Site VPN.

Exemplos

- Conexão única da Site-to-Site VPN
- Conexão única da Site-to-Site VPN com um gateway de trânsito
- Várias conexões da Site-to-Site VPN
- Várias conexões da Site-to-Site VPN com um gateway de trânsito
- Conexão Site-to-Site VPN com Direct Connect
- Conexão Site-to-Site VPN de IP privado com o Direct Connect

Conexão única da Site-to-Site VPN

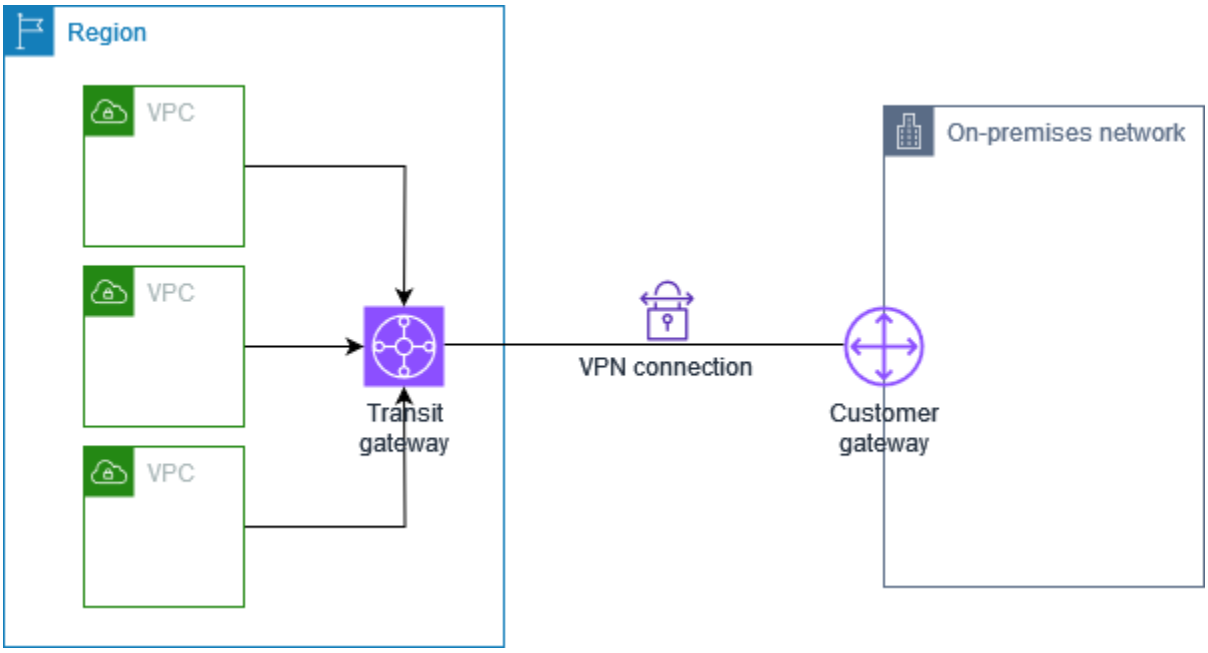
A VPC tem um gateway privado virtual anexado, e a rede on-premises (remota) inclui um dispositivo de gateway do cliente que precisa ser configurado para habilitar a conexão VPN. É necessário atualizar as tabelas de rotas da VPC para que qualquer tráfego da VPC vinculado à rede vá para o gateway privado virtual.



Para conhecer as etapas para configurar esse cenário, consulte Comece com AWS Site-to-Site VPN.

Conexão única da Site-to-Site VPN com um gateway de trânsito

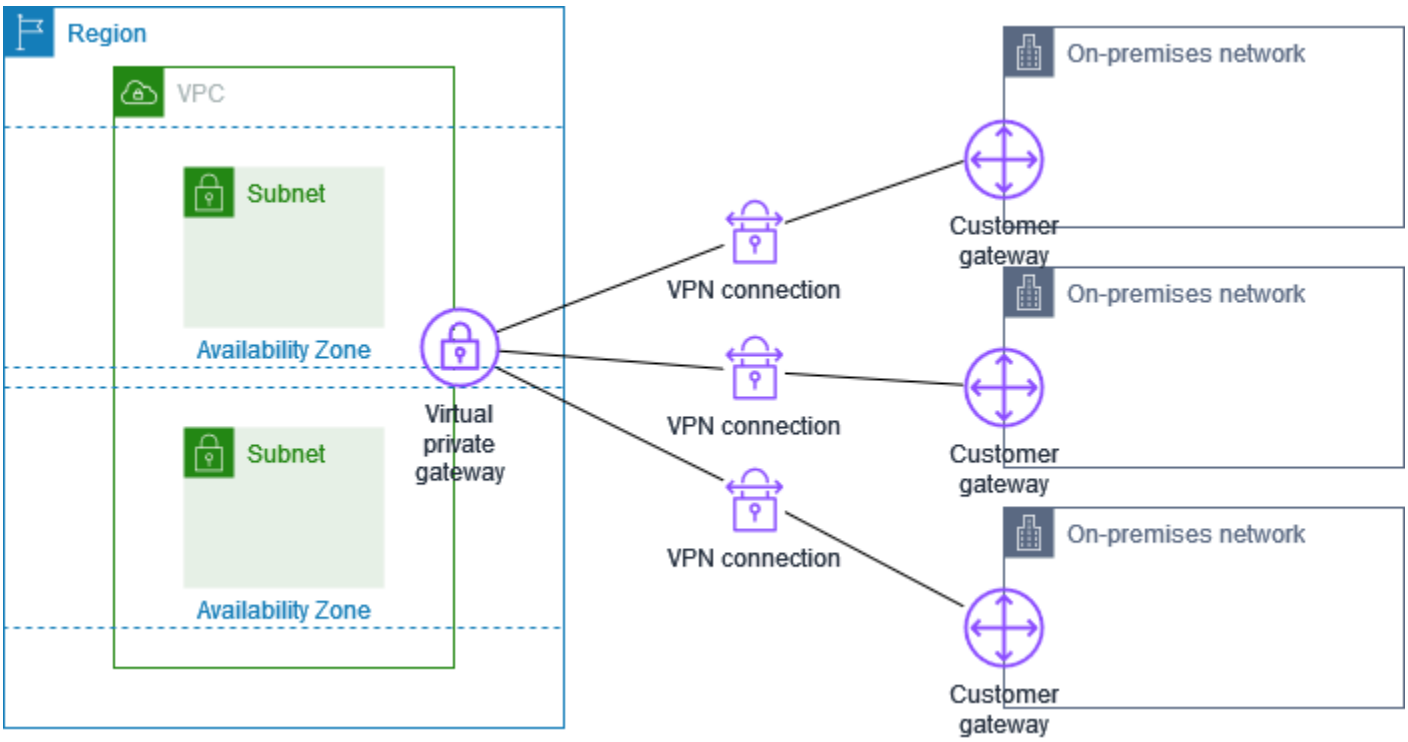
A VPC tem um gateway de trânsito anexado, e a rede on-premises (remota) inclui um dispositivo de gateway do cliente que precisa ser configurado para habilitar a conexão VPN. É necessário atualizar as tabelas de rota da VPC para que qualquer tráfego da VPC vinculado à rede vá para o gateway de trânsito.



Para conhecer as etapas para configurar esse cenário, consulte Comece com AWS Site-to-Site VPN.

Várias conexões da Site-to-Site VPN

A VPC tem um gateway privado virtual anexado e você tem várias conexões da Site-to-Site VPN a várias localidades no local. Configure o roteamento para que qualquer tráfego da VPC vinculado às redes seja roteado para o gateway privado virtual.

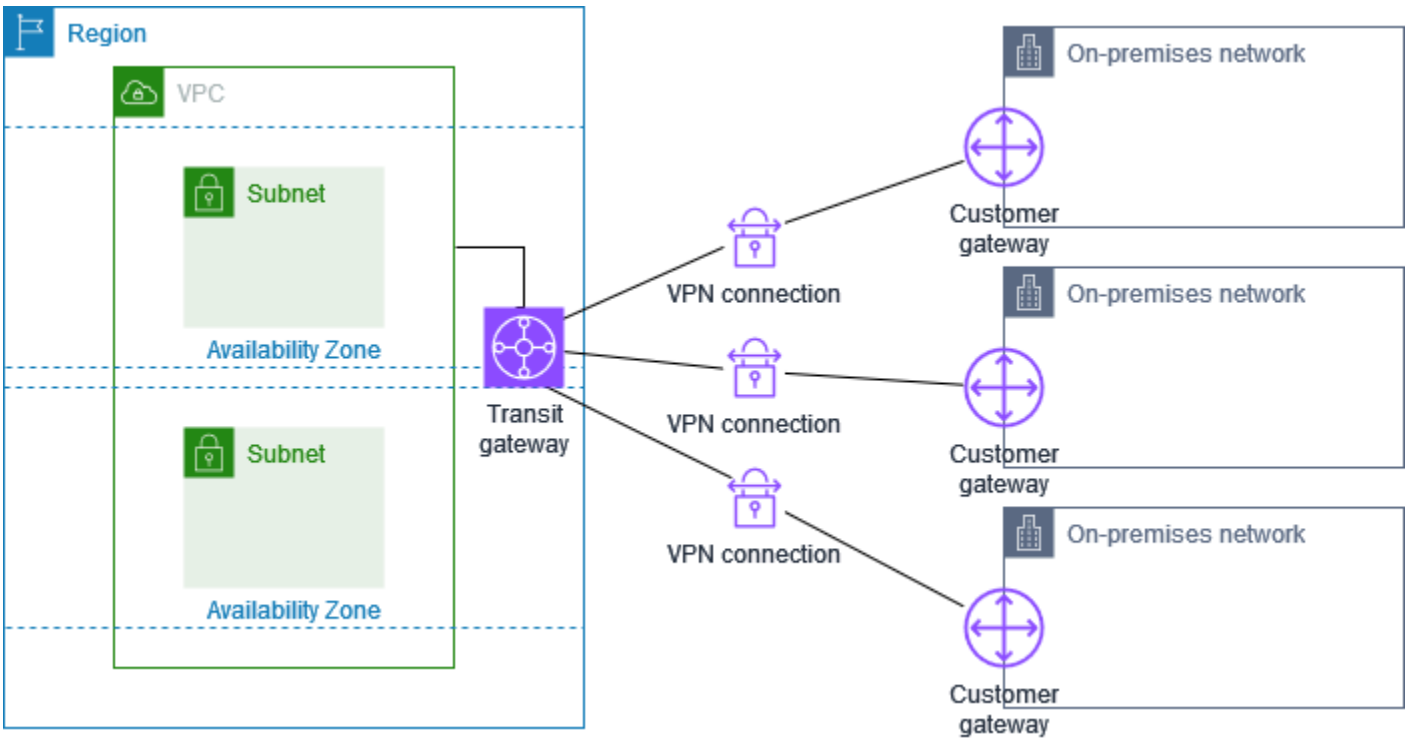


Ao estabelecer várias conexões da Site-to-Site VPN para uma única VPC, é possível configurar um segundo gateway do cliente e, assim, criar uma conexão redundante para o mesmo local externo. Para obter mais informações, consulte Conexões do AWS Site-to-Site VPN redundantes para failover.

Você também pode usar esse cenário para criar conexões da Site-to-Site VPN com várias localizações geográficas e fornecer comunicação segura entre sites. Para obter mais informações, consulte Comunicação segura entre AWS Site-to-Site VPN conexões usando VPN CloudHub.

Várias conexões da Site-to-Site VPN com um gateway de trânsito

A VPC tem um gateway de trânsito anexado e você tem várias conexões da Site-to-Site VPN para vários locais. Configure o roteamento para que qualquer tráfego da VPC vinculado às suas redes seja roteado para o gateway de trânsito.

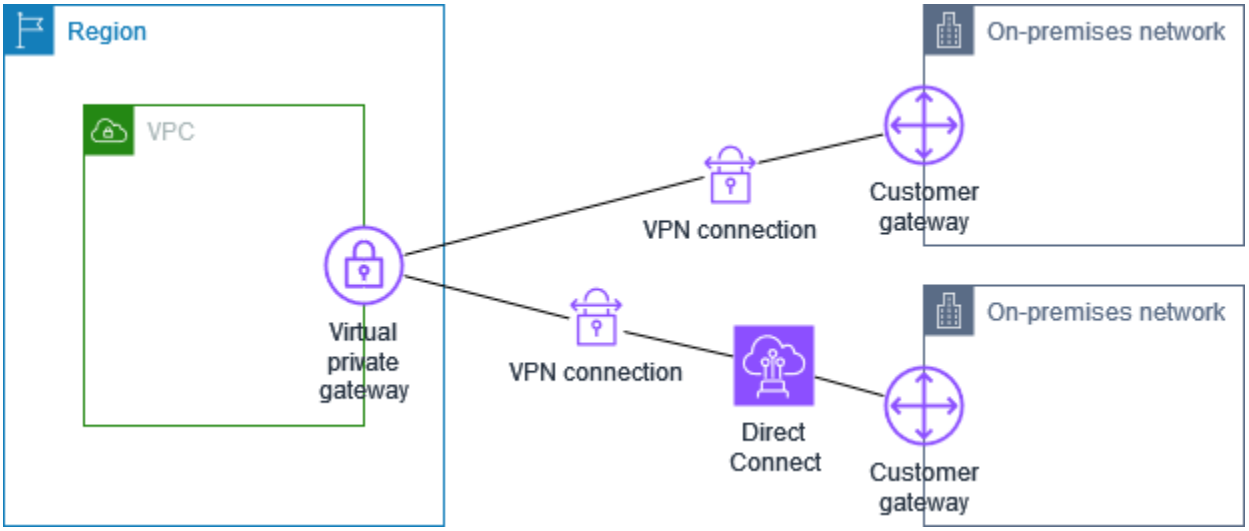


Ao estabelecer várias conexões da Site-to-Site VPN para um único gateway de trânsito, é possível configurar um segundo gateway do cliente e, assim, criar uma conexão redundante para o mesmo local externo.

Você também pode usar esse cenário para criar conexões da Site-to-Site VPN com várias localizações geográficas e fornecer comunicação segura entre sites.

Conexão Site-to-Site VPN com Direct Connect

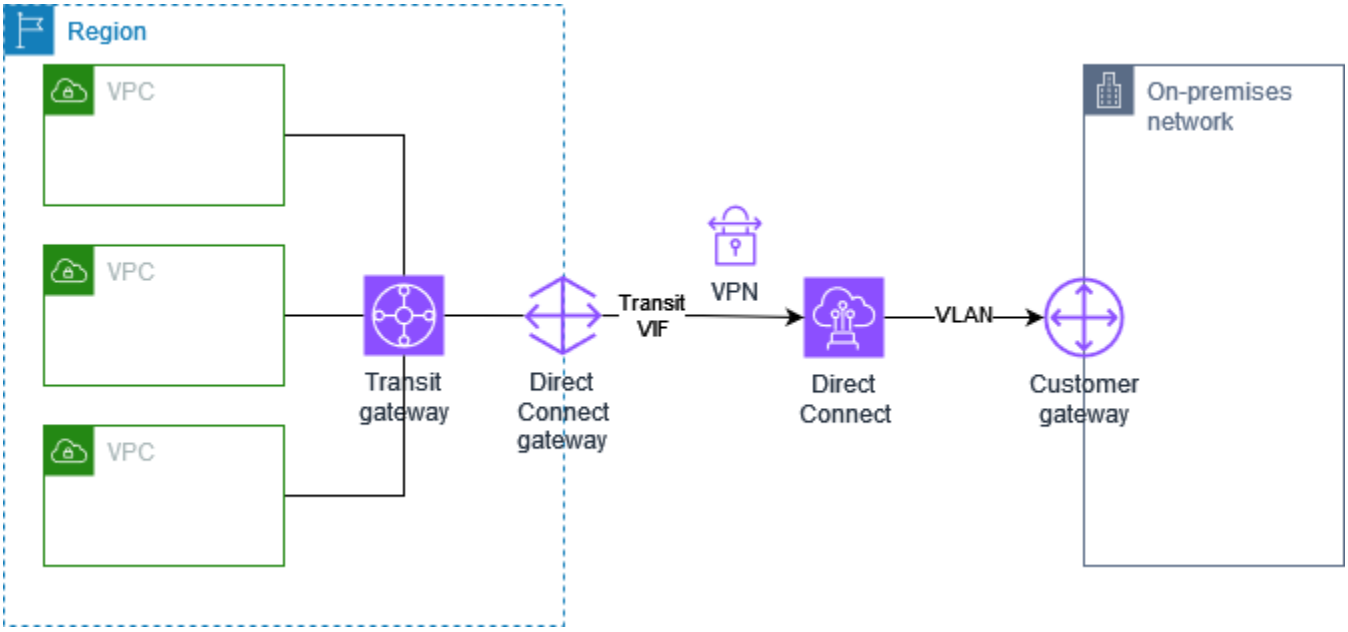
A VPC tem um gateway privado virtual conectado e se conecta à sua rede local (remota) por meio do Direct Connect AWS Direct Connect. É possível configurar uma interface virtual pública do Direct Connect Direct Connect para estabelecer uma conexão de rede dedicada entre sua rede e os recursos públicos da AWS por meio de um gateway privado virtual. Você deve configurar o roteamento para que qualquer tráfego da VPC salte das rotas de rede para o gateway privado virtual e a conexão do Direct Connect.



Quando o Direct Connect e a conexão VPN são configurados no mesmo gateway privado virtual, adicionar ou remover objetos pode fazer com que o gateway privado virtual entre no estado de “anexação”. Isso indica que uma alteração está sendo feita no roteamento interno que alternará entre o Direct Connect e a conexão VPN para minimizar interrupções e perda de pacotes. Quando isso estiver concluído, o gateway privado virtual retorna ao estado “anexado”.

Conexão Site-to-Site VPN de IP privado com o Direct Connect

Com uma Site-to-Site VPN de IP privado, você pode criptografar o tráfego do Direct Connect entre a rede on-premises e a AWS sem o uso de endereços IP públicos. A VPN de IP privado sobre o Direct Connect garante que o tráfego entre a AWS e as redes on-premises seja seguro e privado, permitindo que os clientes cumpram ordens regulamentares e de segurança.



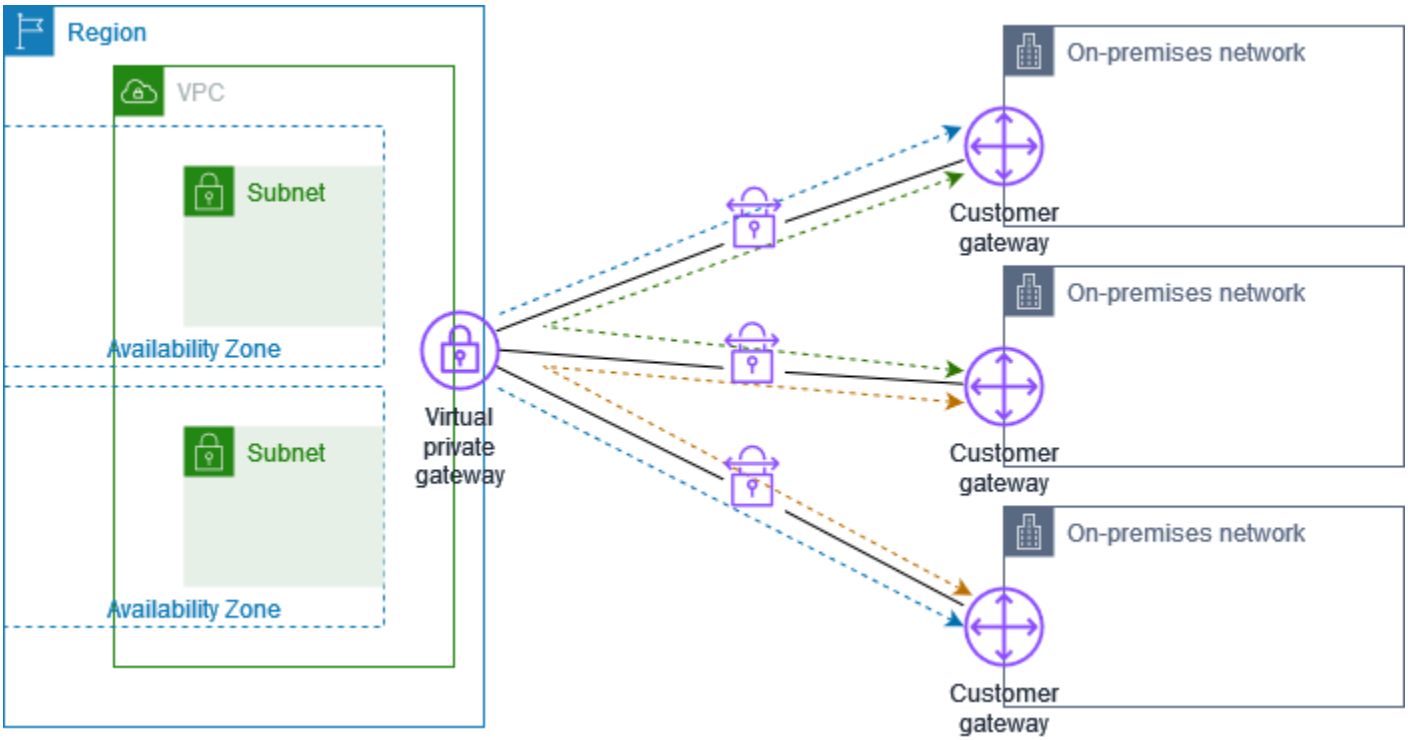
Para obter mais informações, consulte a seguinte publicação do blog: Apresentação das VPNs de IP privadas do AWS Site-to-Site VPN.

Comunicação segura entre AWS Site-to-Site VPN conexões usando VPN CloudHub

Se você tiver várias AWS Site-to-Site VPN conexões, poderá fornecer comunicação segura entre sites usando a AWS VPN CloudHub. Isso permite que os sites comuniquem-se entre si e não somente com os recursos na VPC. A VPN CloudHub opera em um hub-and-spoke modelo simples que você pode usar com ou sem uma VPC. Esse design é adequado se você tiver várias filiais e conexões de Internet existentes e quiser implementar um hub-and-spoke modelo conveniente e potencialmente de baixo custo para conectividade primária ou de backup entre esses locais.

Visão geral do

O diagrama a seguir mostra a CloudHub arquitetura da VPN. As linhas tracejadas mostram o tráfego de rede entre sites remotos roteado pelas conexões VPN. Os sites não devem ter intervalos de IP sobrepostos.



Para este cenário, faça o seguinte:

1. Crie um único gateway privado virtual.

2. Crie vários gateways do cliente, cada um com o endereço IP público do gateway. Você deve usar um número de sistema autônomo (ASN) do Protocolo de Gateway da Borda (BGP) exclusivo para cada gateway do cliente.
3. Crie uma conexão Site-to-Site VPN roteada dinamicamente de cada gateway do cliente para o gateway privado virtual comum.
4. Configure cada dispositivo de gateway do cliente para anunciar um prefixo específico do site (como 10.0.0.0/24, 10.0.1.0/24) para o gateway privado virtual. Esses anúncios de roteamento são recebidos e novamente anunciados para cada ponto BGP, permitindo o envio e o recebimento de dados entre os sites. Isso é feito usando as instruções de rede nos arquivos de configuração da VPN para a conexão Site-to-Site VPN. As instruções da rede diferem ligeiramente, dependendo do tipo de roteador usado.
5. Configure as rotas em suas tabelas de rotas de sub-rede para permitir que as instâncias em sua VPC se comuniquem com seus sites. Para obter mais informações, consulte (Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas. É possível configurar uma rota agregada na tabela de rotas (por exemplo, 10.0.0.0/16). Use prefixos mais específicos entre os dispositivos de gateway do cliente e o gateway privado virtual.

Sites que usam Direct Connect conexões com o gateway privado virtual também podem fazer parte da AWS VPN CloudHub. Por exemplo, sua sede corporativa em Nova York pode ter uma Direct Connect conexão com a VPC e suas filiais podem usar conexões Site-to-Site VPN com a VPC. As filiais em Los Angeles e Miami podem enviar e receber dados umas com as outras e com a sede da sua empresa, todas usando a AWS VPN CloudHub.

Preços

Para usar AWS VPN CloudHub, você paga taxas de conexão Site-to-Site VPN típicas da Amazon VPC. A quantia devida pela taxa de conexão é calculada pelo total de horas em que cada VPN esteve conectada ao gateway privado virtual. Quando você envia dados de um site para outro usando a AWS VPN CloudHub, não há custo para enviar dados do seu site para o gateway privado virtual. Você só paga as taxas de transferência de dados padrão da AWS referentes aos dados que são retransmitidos do gateway privado virtual para o endpoint.

Por exemplo, se você tem um site em Los Angeles e um segundo site em Nova York e os dois sites têm uma conexão Site-to-Site VPN com o gateway privado virtual, você paga a taxa por hora para cada conexão Site-to-Site VPN (portanto, se a taxa fosse de $0,05 por hora, seria um total de $0,10 por hora). Você também paga as taxas de transferência de AWS dados padrão para todos os dados enviados de Los Angeles para Nova York (e vice-versa) que atravessam cada Site-to-Site conexão

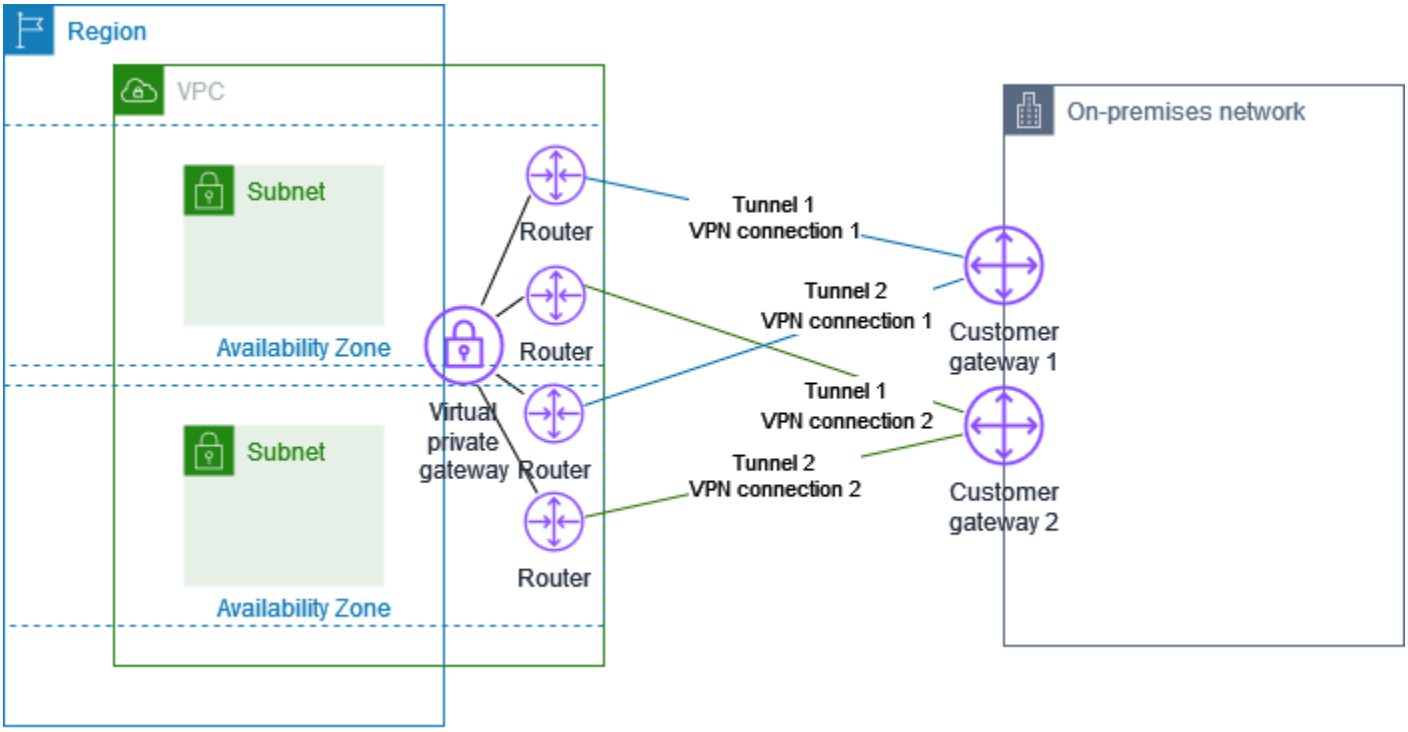
VPN. O tráfego de rede enviado pela conexão Site-to-Site VPN para o gateway privado virtual é gratuito, mas o tráfego de rede enviado pela conexão Site-to-Site VPN do gateway privado virtual para o endpoint é cobrado de acordo com a taxa de transferência de AWS dados padrão.

Para obter mais informações, consulte Site-to-Site Definição de preço da conexão VPN.

Conexões do AWS Site-to-Site VPN redundantes para failover

A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, adicione um segundo gateway do cliente e configure uma segunda conexão da Site-to-Site VPN à sua VPC e para o gateway privado virtual. O uso de conexões VPN e dispositivos de gateway do cliente redundantes permite executar a manutenção de um dos gateways enquanto o tráfego flui por meio da conexão VPN do segundo gateway do cliente.

O diagrama a seguir mostra as duas conexões VPN. Cada conexão VPN tem seus próprios túneis e seu próprio gateway do cliente.



Para este cenário, faça o seguinte:

- Configure uma segunda conexão da Site-to-Site VPN usando o mesmo gateway privado virtual e criando um gateway do cliente. O endereço IP do gateway do cliente para a segunda conexão da Site-to-Site VPN deve ser acessível ao público.

- Configure um segundo dispositivo de gateway do cliente. Os dois dispositivos devem anunciar os mesmos intervalos de IP para o gateway privado virtual. Usamos o roteamento BGP a fim de determinar o caminho para o tráfego. Se ocorrer uma falha no dispositivo de gateway do cliente, o gateway privado virtual direcionará todo o tráfego para o dispositivo de gateway do cliente em funcionamento.

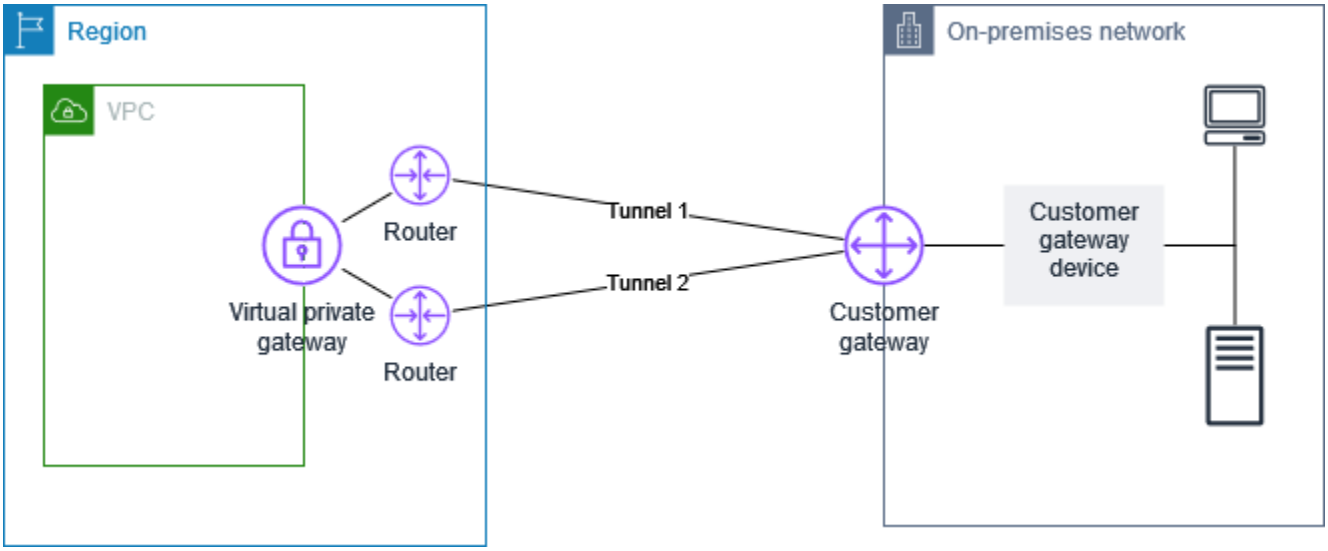
As conexões da Site-to-Site VPN roteadas dinamicamente usam o Border Gateway Protocol (BGP) para trocar informações de roteamento entre os gateways do cliente e os gateways privados virtuais. As conexões da Site-to-Site VPN roteadas estaticamente requerem que as rotas estáticas sejam inseridas na rede remota situada no seu lado do gateway do cliente. As informações de rotas anunciadas em BGP e estaticamente inseridas permitem os gateways em ambos os lados, indicando a disponibilidade dos túneis e redirecionando o tráfego, caso ocorra uma falha. Recomendamos que configure a rede para usar as informações de roteamento fornecidas pelo BGP (se disponível) e, assim, selecionar um caminho disponível. A configuração exata depende da arquitetura da rede.

Para obter mais informações sobre como criar e configurar um gateway do cliente e uma conexão da Site-to-Site VPN, consulte Comece com AWS Site-to-Site VPN.

AWS Site-to-Site VPN dispositivos de gateway do cliente

Um dispositivo de gateway do cliente é um dispositivo físico ou de software que você possui ou gerencia em sua rede local (do seu lado de uma conexão Site-to-Site VPN). Você ou seu administrador de rede devem configurar o dispositivo para funcionar com a conexão Site-to-Site VPN.

O diagrama a seguir mostra a rede, o dispositivo de gateway do cliente e a conexão VPN que vai para o gateway privado virtual anexado à VPC. As duas linhas entre o gateway do cliente e o gateway privado virtual representam os túneis para a conexão VPN. Se houver uma falha no dispositivo AWS, sua conexão VPN automaticamente passará para o segundo túnel para que seu acesso não seja interrompido. De tempos em tempos, AWS também realiza manutenção de rotina na conexão VPN, o que pode desativar brevemente um dos dois túneis da sua conexão VPN. Para obter mais informações, consulte AWS Site-to-Site VPN substituições de terminais de túneis. É importante configurar o dispositivo de gateway do cliente para usar os dois túneis.



Para obter as etapas para configurar uma conexão VPN, consulte Comece com AWS Site-to-Site VPN. Durante esse processo, você cria um recurso de gateway do cliente no AWS, que fornece informações AWS sobre seu dispositivo, por exemplo, seu endereço IP público. Para obter mais informações, consulte Opções de gateway do cliente para sua conexão AWS Site-to-Site VPN. O recurso de gateway do cliente em AWS não configura nem cria o dispositivo de gateway do cliente. Você precisará configurar o dispositivo por conta própria.

Também é possível encontrar dispositivos de programa de VPN no AWS Marketplace.

Requisitos para um dispositivo de gateway do AWS Site-to-Site VPN cliente

AWS suporta vários dispositivos Site-to-Site VPN de gateway de clientes, para os quais fornecemos arquivos de configuração para download. Para ver uma lista dos dispositivos compatíveis e as etapas para baixar os arquivos de configuração, consulte Arquivos de configuração de roteamento estático e dinâmico.

Se você tiver um dispositivo que não esteja na lista de dispositivos compatíveis, a seção a seguir descreve os requisitos que o dispositivo deve atender para estabelecer uma conexão Site-to-Site VPN.

Há quatro etapas principais para a configuração do seu dispositivo de gateway do cliente. Os símbolos a seguir representam cada parte da configuração.

IKE	Associação de segurança do Internet Key Exchange (IKE). Isso é necessário para trocar as chaves usadas para estabelecer a associação IPsec de segurança.
IPsec	IPsec associação de segurança. Isso lida com a criptografia do túnel, com a autenticação e assim por diante.
Tunnel	Interface do túnel. Isso recebe tráfego de e para o túnel.
BGP	(Opcional) Emparelhamento de Protocolo de Gateway da Borda (BGP) Para dispositivos que usam BGP, isso troca as rotas entre o dispositivo de gateway do cliente e o gateway privado virtual.

A tabela a seguir lista os requisitos para o dispositivo de gateway do cliente, o RFC relacionado (para referência) e comentários sobre os requisitos.

Cada conexão VPN consiste em dois túneis separados. Cada túnel contém uma associação de segurança IKE, uma associação IPsec de segurança e um peering BGP. Você está limitado a um par exclusivo de associação de segurança (SA) por túnel (um de entrada e um de saída) e, portanto, a dois pares de SA exclusivos no total para dois túneis (quatro). SAs Alguns dispositivos usam uma VPN baseada em políticas e criam tantas entradas de SAs ACL. Assim, talvez seja necessário consolidar as regras e, depois, filtrar para não permitir o tráfego indesejado.

Por padrão, o túnel da VPN é ativado quando o tráfego é gerado e a negociação do protocolo IKE é iniciada do seu lado da conexão VPN. Em vez disso, você pode configurar a conexão VPN para iniciar a negociação IKE do AWS lado da conexão. Para obter mais informações, consulte AWS Site-to-Site VPN opções de iniciação de túnel.

Os endpoints de VPN são compatíveis com o rechaveamento e poderão iniciar renegociações quando a fase 1 estiver prestes a expirar, se o dispositivo de gateway do cliente não tiver enviado nenhum tráfego de renegociação.

Requisito	RFC	Comentários
Estabelecer associação de segurança IKE IKE	RFC 2409 RFC 7296	A associação de segurança IKE é estabelecida primeiro entre o gateway privado virtual e o dispositivo de gateway do cliente usando uma chave pré-compartilhada ou um certificado privado usado Autoridade de Certificação Privada da AWS como autenticador. Quando estabelecido, o IKE negocia uma chave efêmera para proteger futuras mensagens de IKE. Deve haver um acordo completo entre os parâmetros, incluindo parâmetros de criptografia e de autenticação. Ao criar uma conexão VPN no AWS, você pode especificar sua própria chave pré-compartilhada para cada túnel ou deixar AWS gerar uma para você. Como alternativa, você pode especificar o certificado privado usado Autoridade de Certificação Privada da AWS para usar em seu dispositivo de gateway do cliente. Para obter mais informações, sobre como configurar túneis da VPN, consulte Opções de túnel para sua AWS Site-to-Site VPN conexão. As seguintes versões são suportadas: IKEv1 IKEv2 e. Suportamos o modo principal somente com IKEv1. O serviço Site-to-Site VPN é uma solução baseada em rotas. Se você estiver usando uma configuração com

Requisito	RFC	Comentários
		base em políticas, limite a configuração a uma única associação de segurança (SA).
Estabeleça associações de IPsec segurança no modo Túnel IPsec	RFC 4301	Usando a chave efêmera IKE, as chaves são estabelecidas entre o gateway privado virtual e o dispositivo de gateway do cliente para formar uma associação de IPsec segurança (SA). O tráfego entre os gateways é criptografado e descriptografado. usando essa SA. As chaves efêmeras usadas para criptografar o tráfego dentro do IPsec SA são alternadas automaticamente pelo IKE regularmente para garantir a confidencialidade das comunicações.
Usar a função de criptografia AES de 128 bits ou AES de 256 bits	RFC 3602	A função de criptografia é usada para garantir a privacidade do IKE e das associações IPsec de segurança.
Usar a função de hashing SHA-1 ou SHA-2 (256)	RFC 2404	Essa função de hashing é usada para autenticar tanto o IKE quanto as associações de segurança. IPsec
Use o Diffie-Hellman Perfect Forward Secrecy.	RFC 2409	O IKE usa Diffie-Hellman para estabelecer chaves efêmeras para proteger toda a comunicação entre os dispositivos de gateway do cliente e os gateways privados virtuais. Os seguintes grupos são compatíveis: • Grupos da fase 1: 2, 14-24 • Grupos da fase 2: 2, 5, 14-24

Requisito	RFC	Comentários
(Conexões VPN roteadas dinamicamente) Use o Dead Peer Detection IPsec	RFC 3706	O Dead Peer Detection permite que os dispositivos de VPN identifiquem rapidamente quando uma condição de rede impede a entrega de pacotes pela Internet. Quando isso ocorre, os gateways excluem as associações de segurança e tentam criar outras associações. Durante esse processo, o IPsec túnel alternativo é usado, se possível.
(Conexões VPN roteadas dinamicamente) Vincular o túnel à interface lógica (VPN baseada em rota) 	Nenhum	Seu dispositivo deve ser capaz de vincular o IPsec túnel a uma interface lógica. A interface lógica contém um endereço IP que é usado para estabelecer o emparelhamento de BGP com o gateway privado virtual. Essa interface lógica não deve executar encapsulamento adicional (por exemplo, GRE ou IP em IP). A interface deve ser configurada para uma Maximum Transmission Unit (MTU) de 1.399 bytes.
(Conexões VPN roteadas dinamicamente) Estabelecer emparelhamentos de BGP 	RFC 4271	O BGP é usado para trocar as rotas entre o dispositivo de gateway do cliente e o gateway privado virtual para dispositivos que usam o BGP. Todo o tráfego BGP é criptografado e transmitido pela IPsec Security Association. O BGP é necessário para que ambos os gateways troquem os prefixos IP que podem ser acessados por meio do SA. IPsec

Uma conexão AWS VPN não oferece suporte ao Path MTU Discovery (RFC 1191).

Se houver um firewall entre o dispositivo de gateway do cliente e a Internet, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Melhores práticas para um dispositivo de gateway AWS Site-to-Site VPN do cliente

Use IKEv2

É altamente recomendável usar IKEv2 para sua conexão Site-to-Site VPN. IKEv2 é um protocolo mais simples, robusto e seguro do que o. IKEv1 Você só deve usar IKEv1 se o dispositivo de gateway do cliente não for compatível IKEv2. Para obter mais detalhes sobre as diferenças entre IKEv1 e IKEv2, consulte o Apêndice A do. RFC7296

Redefinir o sinalizador “Não fragmentar (DF)” nos pacotes

Alguns pacotes carregam um sinalizador chamado de Não fragmentar (DF), que indica que o pacote não deve ser fragmentado. Quando os pacotes usam o sinalizador, os gateways geram uma mensagem de MTU de caminho ICMP excedido. Em alguns casos, as aplicações não possuem mecanismos adequados para processar essas mensagens ICMP e para reduzir a quantidade de dados transmitidos em cada pacote. Alguns dispositivos VPN podem substituir o sinalizador DF e fragmentar os pacotes incondicionalmente, se necessário. Se o dispositivo de gateway do cliente tiver essa capacidade, recomendamos o uso, conforme apropriado. Consulte RFC 791 para obter mais detalhes.

Fragmentar pacotes IP antes da criptografia

Se os pacotes enviados pela sua conexão Site-to-Site VPN excederem o tamanho da MTU, eles deverão ser fragmentados. Para evitar a diminuição do desempenho, recomendamos que você configure seu dispositivo de gateway do cliente para fragmentar os pacotes antes de serem criptografados. Site-to-Site A VPN então remontará todos os pacotes fragmentados antes de encaminhá-los para o próximo destino, a fim de obter packet-per-second fluxos mais altos pela rede. AWS Consulte RFC 4459 para obter mais detalhes.

Certifique-se de que o tamanho do pacote não exceda a MTU para redes de destino

Como a Site-to-Site VPN reagrupará todos os pacotes fragmentados recebidos do dispositivo de gateway do cliente antes de encaminhá-los para o próximo destino, lembre-se de que pode haver size/MTU considerações sobre pacotes para redes de destino para as quais esses pacotes serão encaminhados em seguida, como over Direct Connect ou com determinados protocolos, como o Radius.

Ajuste os tamanhos MTU e MSS de acordo com os algoritmos em uso

Os pacotes TCP geralmente são o tipo mais comum de pacote em túneis. IPsec Site-to-Site A VPN suporta uma unidade de transmissão máxima (MTU) de 1446 bytes e um tamanho máximo de segmento (MSS) correspondente de 1406 bytes. No entanto, os algoritmos de criptografia têm tamanhos de cabeçalho variados e podem impedir a capacidade de atingir esses valores máximos.

Para obter a performance ideal evitando a fragmentação, recomendamos que você defina o MTU e o MSS com base especificamente nos algoritmos que estão sendo usados.

Use a tabela a seguir para definir o seu MTU/MSS para evitar a fragmentação e obter o desempenho ideal:

Algoritmo de criptografia	Algoritmo de hash	NAT Traversal	MTU	MANUSCRITO (1) IPv4	SMS (IPv6-em-) IPv4
AES-GCM-16	N/D	desabilitado	1446	1406	1386
AES-GCM-16	N/D	habilitado	1438	1398	1378
AES-CBC	SHA1/SHA2-256	desabilitado	1438	1398	1378
AES-CBC	SHA1/SHA2-256	habilitado	1422	1382	1362
AES-CBC	SHA2-384	desabilitado	1422	1382	1362
AES-CBC	SHA2-384	habilitado	1422	1382	1362
AES-CBC	SHA2-512	desabilitado	1422	1382	1362
AES-CBC	SHA2-512	habilitado	1406	1366	1346

> **Note**
>
> Os algoritmos AES-GCM cobrem criptografia e autenticação, portanto, não há escolha de algoritmo de autenticação distinta que afetaria a MTU.

Desativar IKE exclusivo IDs

Alguns dispositivos de gateway do cliente são compatíveis com configuração que garante que, no máximo, exista uma associação de segurança de fase 1 por configuração de túnel. Essa configuração pode resultar em estados inconsistentes da Fase 2 entre os pares de VPN. Se o dispositivo de gateway do cliente for compatível com configuração, recomendamos desabilitá-la.

Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente

Você deve ter um endereço IP estático para usar como ponto final dos IPsec túneis que conectam seu dispositivo de gateway do cliente aos endpoints. AWS Site-to-Site VPN Se houver um firewall entre AWS e seu dispositivo de gateway do cliente, as regras nas tabelas a seguir devem estar em vigor para estabelecer os IPsec túneis. Os endereços IP do AWS lado -estarão no arquivo de configuração.

Entrada (pela Internet)

Regra de entrada I1	
IP de origem	IP externo do túnel 1
Dest IP	Gateway do cliente
Protocolo	UDP
Porta de origem	500
Destino	500
Regra de entrada I2	
IP de origem	IP externo do túnel 2
Dest IP	Gateway do cliente
Protocolo	UDP
Porta de origem	500
Porta de destino	500
Regra de entrada I3	
IP de origem	IP externo do túnel 1
Dest IP	Gateway do cliente

Protocolo	IP 50 (ESP)
Regra de entrada I4	
IP de origem	IP externo do túnel 2
Dest IP	Gateway do cliente
Protocolo	IP 50 (ESP)

Saída (para a Internet)

Regra de saída O1	
IP de origem	Gateway do cliente
Dest IP	IP externo do túnel 1
Protocolo	UDP
Porta de origem	500
Porta de destino	500
Regra de saída O2	
IP de origem	Gateway do cliente
Dest IP	IP externo do túnel 2
Protocolo	UDP
Porta de origem	500
Porta de destino	500
Regra de saída O3	
IP de origem	Gateway do cliente
Dest IP	IP externo do túnel 1

Protocolo	IP 50 (ESP)
Regra de saída O4	
IP de origem	Gateway do cliente
Dest IP	IP externo do túnel 2
Protocolo	IP 50 (ESP)

As regras I1, I2, O1 e O2 permitem a transmissão de pacotes IKE. As regras I3, I4, O3 e O4 permitem a transmissão de IPsec pacotes que contêm o tráfego de rede criptografado.

> **Note**
>
> Se você estiver usando a passagem NAT (NAT-T) em seu dispositivo, certifique-se de que o tráfego UDP na porta 4500 também possa passar entre sua rede e os endpoints. AWS Site-to-Site VPN Verifique se o seu dispositivo está anunciando NAT-T.

Arquivos de configuração estáticos e dinâmicos para um dispositivo de gateway AWS Site-to-Site VPN do cliente

Depois de criar a conexão VPN, você também tem a opção de baixar um arquivo de configuração de exemplo fornecido pela AWS do console da Amazon VPC ou usando a API do EC2. Consulte Etapa 6: baixar o arquivo de configuração para obter mais informações. Você também pode baixar arquivos .zip de configurações de exemplo especificamente para roteamento estático vs. dinâmico nessas respectivas páginas.

O arquivo AWS de configuração de amostra fornecido contém informações específicas da sua conexão VPN que você pode usar para configurar seu dispositivo de gateway do cliente. Esses arquivos de configuração específicos do dispositivo estão disponíveis para dispositivos testados pela AWS. Se o dispositivo de gateway do cliente específico não estiver listado, você poderá baixar um arquivo de configuração genérica para começar.

Important

O arquivo de configuração é apenas um exemplo e pode não corresponder totalmente às configurações de conexão Site-to-Site VPN pretendidas. Ele especifica os requisitos mínimos para uma conexão Site-to-Site VPN do grupo 2 do AES128 Diffie-Hellman na maioria das AWS regiões e do grupo 14 do Diffie-Hellman nas regiões. SHA1 AES128 SHA2 AWS GovCloud Ele também especifica chaves pré-compartilhadas para autenticação. Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

Note

Esses arquivos de configuração específicos do dispositivo são fornecidos com AWS base no melhor esforço. Embora tenham sido testados por AWS, esse teste é limitado. Em caso de problemas com os arquivos de configuração, talvez seja necessário entrar em contato com o fornecedor específico para obter suporte adicional.

A tabela a seguir contém uma lista de dispositivos que têm um exemplo de arquivo de configuração disponível para download que foi atualizado para oferecer suporte IKEv2. Introduzimos IKEv2 suporte nos arquivos de configuração para muitos dispositivos populares de gateway de clientes e continuaremos adicionando arquivos adicionais ao longo do tempo. Esta lista será atualizada à medida que mais arquivos de configuração de exemplo forem adicionados.

Fornecedor	Plataforma	Software
AXGATE	NF	AOS 3.2+
AXGATE	UTM	AOS 2.1+
Ponto de verificação	Gaia	R80.10+
Cisco Meraki	MX Series	15.12+ (WebUI)
Cisco Systems, Inc.	ASA 5500 Series	ASA 9.7+ VTI
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+

Fornecedor	Plataforma	Software
Fortinet	Fortigate 40+ Series	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc.	J-Series Routers	JunOS 9.5+
Juniper Networks, Inc.	SRX Routers	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	PA Series	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	RTX Routers	Rev.10.01.16+

Arquivos de configuração de roteamento estático que podem ser baixados para um dispositivo de gateway AWS Site-to-Site VPN do cliente

Para baixar um arquivo de configuração de amostra com valores específicos para sua configuração de conexão Site-to-Site VPN, use o console da Amazon VPC, a linha de AWS comando ou a API do Amazon EC2. Para obter mais informações, consulte Etapa 6: baixar o arquivo de configuração.

Você também pode baixar arquivos de configuração de exemplo genéricos para roteamento estático que não incluem valores específicos para sua configuração de conexão Site-to-Site VPN: .zip static-routing-examples

Os arquivos usam valores de espaço reservado para alguns componentes. Por exemplo, eles usam:

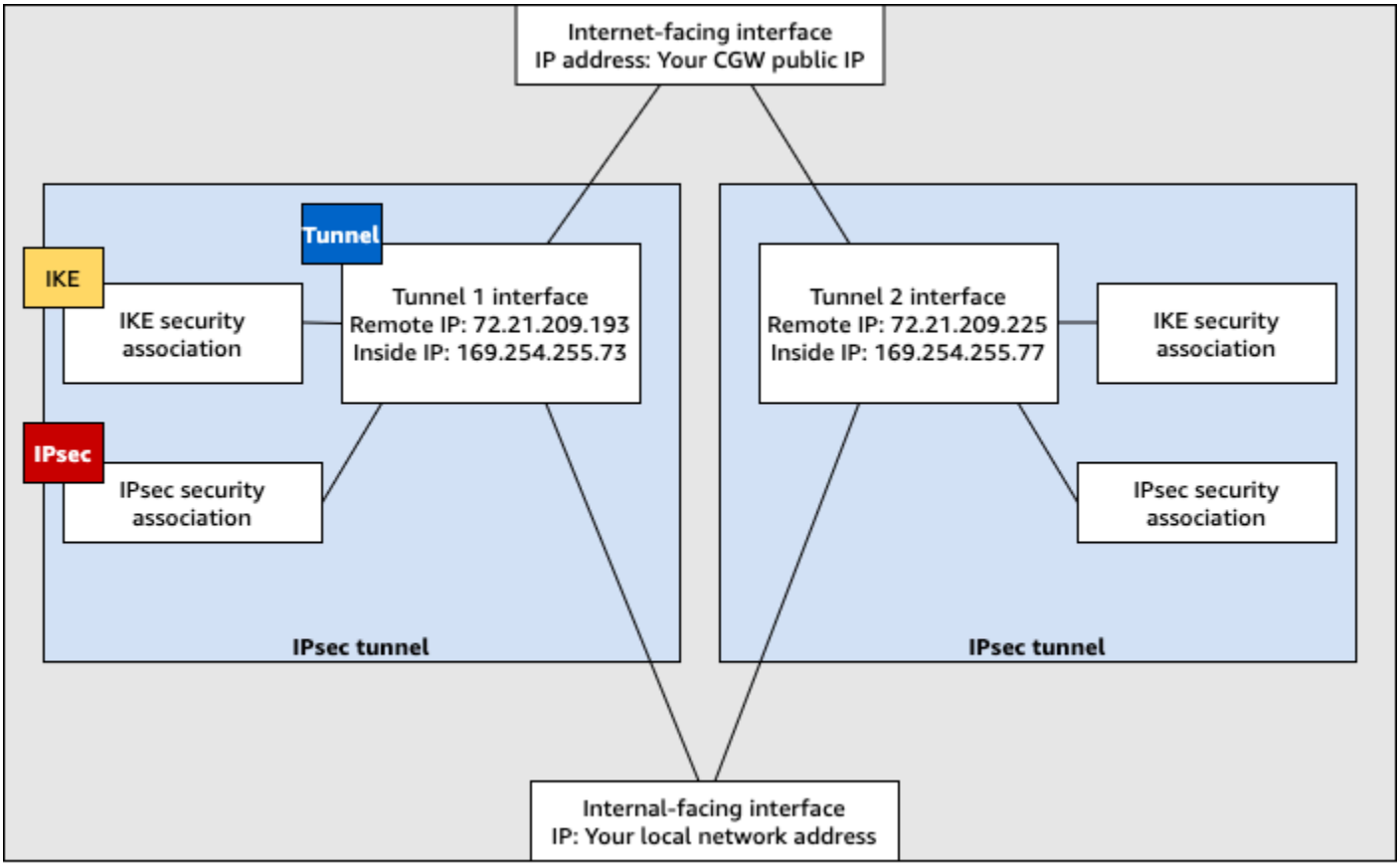
- Valores de exemplo para o ID da conexão VPN, ID do gateway do cliente e ID do gateway privado virtual
- Espaços reservados para os AWS endpoints de endereço IP remoto (externo) (*AWS_ENDPOINT_1*e) *AWS_ENDPOINT_2*
- Um espaço reservado para o endereço IP da interface externa roteável pela Internet no dispositivo de gateway do cliente () *your-cgw-ip-address*

- Um espaço reservado para o valor da chave pré-compartilhada () pre-shared-key
- Valores de exemplo para o túnel dentro de endereços IP.
- Valores de exemplo para a configuração de MTU.

> **Note**
>
> As configurações de MTU fornecidas nos arquivos de configuração de amostra são apenas exemplos. Consulte Melhores práticas para um dispositivo de gateway AWS Site-to-Site VPN do cliente para obter informações sobre como definir o valor MTU ideal para a sua situação.

Além de fornecer valores de espaço reservado, os arquivos especificam os requisitos mínimos para uma conexão Site-to-Site VPN de AES128, SHA1, e Diffie-Hellman grupo 2 na maioria das AWS regiões e, AES128 SHA2, e Diffie-Hellman grupo 14 nas regiões. AWS GovCloud Eles também especificam chaves pré-compartilhadas para autenticação. Você deve modificar o arquivo de configuração de exemplo para aproveitar algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

O diagrama a seguir fornece uma visão geral dos diferentes componentes configurados no dispositivo de gateway do cliente. Ele inclui valores de exemplo para os endereços IP da interface do túnel.



Customer gateway device

Configurar o roteamento estático para um dispositivo de gateway AWS Site-to-Site VPN do cliente

Veja a seguir alguns procedimentos de exemplo para configurar um dispositivo de gateway do cliente usando sua interface de usuário (se disponível).

Check Point

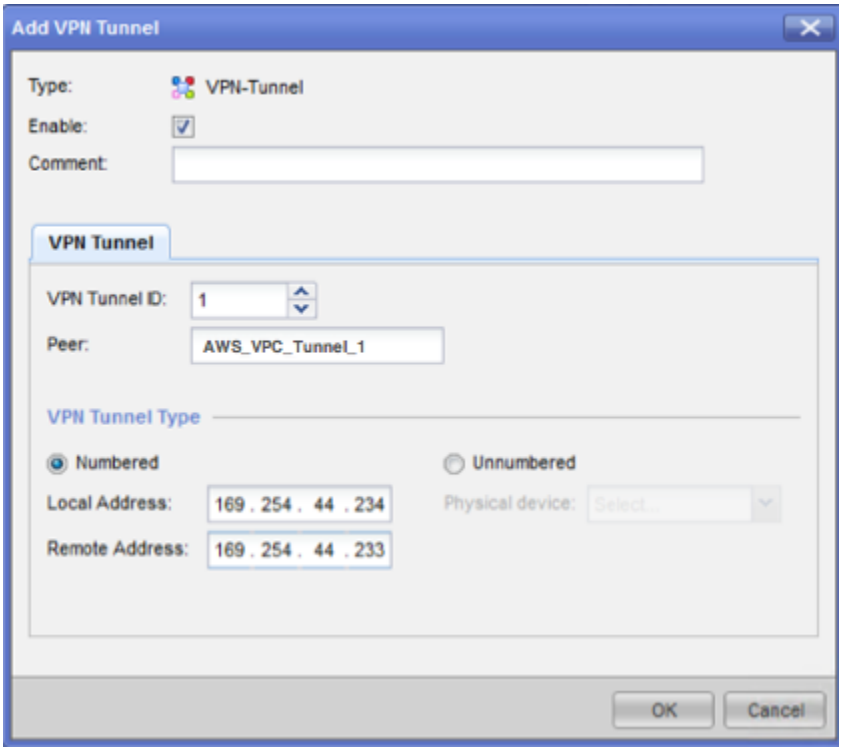
A seguir estão as etapas para configurar seu dispositivo de gateway de cliente se seu dispositivo for um dispositivo Check Point Security Gateway executando R77.10 ou superior, usando o sistema operacional Gaia e o Check Point. SmartDashboard Você também pode consultar o artigo Check Point Security Gateway IPsec VPN to Amazon Web Services VPC no Check Point Support Center.

Para configurar a interface do túnel

O primeiro passo é criar túneis de VPN e fornecer os endereços IP privados (internos) do gateway do cliente e do gateway privado virtual de cada túnel. Para criar o primeiro túnel, use

as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração. Para criar o segundo túnel, use os valores fornecidos na seção `IPSec Tunnel #2` do arquivo de configuração.

1. Abra o portal Gaia do dispositivo Check Point Security Gateway.
2. Escolha Network Interfaces, Add, VPN tunnel.
3. Na caixa de diálogo, defina as configurações como a seguir e escolha OK ao concluir:
   - Em VPN Tunnel ID, insira qualquer valor único exclusivo, como 1.
   - Em Peer, insira um nome exclusivo para seu túnel, como `AWS_VPC_Tunnel_1` or `AWS_VPC_Tunnel_2`.
   - Confirme se Numbered (Numerado) está selecionado e, em Local Address (Endereço local), insira o endereço IP especificado para `CGW Tunnel IP` no arquivo de configuração; por exemplo, `169.254.44.234`.
   - Em Remote Address, insira o endereço IP especificado para `VGW Tunnel IP` no arquivo de configuração; por exemplo, `169.254.44.233`.



4. Conecte seu gateway de segurança por SSH. Se estiver usando um shell não padrão, mude para clish executando o comando a seguir: `clish`

5. Para o túnel 1, execute o comando a seguir:

```
set interface vpnt1 mtu 1436
```

   Para o túnel 2, execute o comando a seguir:

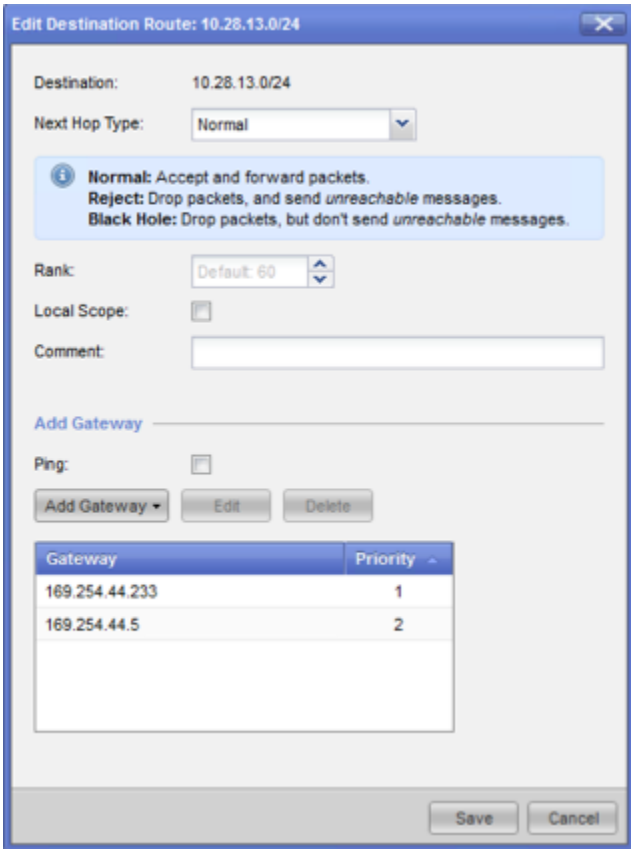
```
set interface vpnt2 mtu 1436
```

6. Repita essas etapas para criar um segundo túnel, usando as informações na seção `IPSec Tunnel #2` do arquivo de configuração.

Para configurar rotas estáticas

Nesta etapa, especifique a rota estática para a sub-rede na VPC de cada túnel para poder enviar tráfego pelas interfaces de túnel. O segundo túnel permite failover, caso haja um problema com o primeiro túnel. Se um problema é detectado, a rota estática baseada na política é removida da tabela de roteamento e a segunda rota é ativada. Você deve também ativar o gateway do Check Point para executar ping na outra extremidade do túnel e verificar se o túnel está ativo.

1. No portal Gaia, escolha Rotas IPv4 estáticas, Adicionar.
2. Especifique o CIDR de sua sub-rede; por exemplo, `10.28.13.0/24`.
3. Escolha Add Gateway (Adicionar Gateway), IP Address (Endereço de IP).
4. Insira o endereço IP especificado para `VGW Tunnel IP` no arquivo de configuração (por exemplo, `169.254.44.233`) e especifique 1 como prioridade.
5. Selecione Ping.
6. Repita as etapas 3 e 4 para o segundo túnel, usando o valor `VGW Tunnel IP` na seção `IPSec Tunnel #2` do arquivo de configuração. Especifique 2 como prioridade.



7. Escolha Salvar.

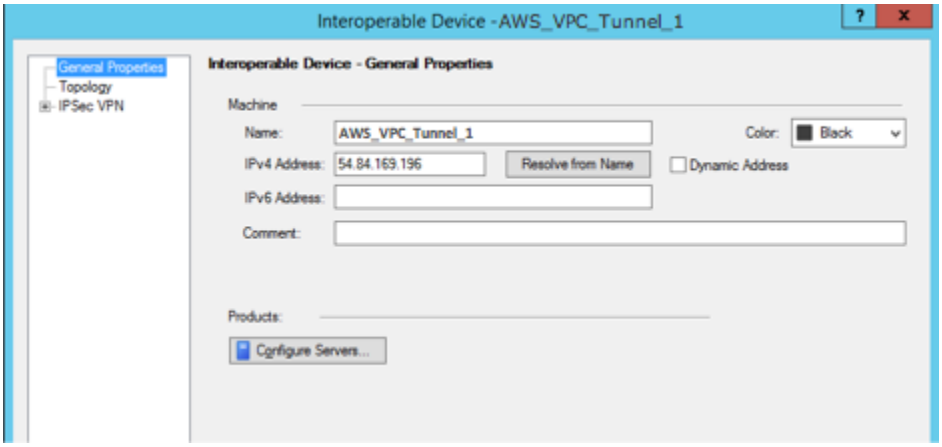
Se estiver usando um cluster, repita as etapas anteriores para os outros membros do cluster.

Para definir um novo objeto de rede

Nesta etapa, você criará um objeto de rede para cada túnel de VPN, especificando os endereços IP públicos (externos) para o gateway privado virtual. Posteriormente, você adicionará esses objetos de rede como gateways secundários para sua comunidade VPN. Você precisa também criar um grupo vazio para funcionar como espaço reservado para o domínio de VPN.

1. Abra o Check Point SmartDashboard.
2. Em Groups (Grupos), abra o menu de contexto e escolha Groups (Grupos), Simple Group (Grupo Simples). É possível usar o mesmo grupo para cada objeto de rede.
3. Em Network Objects (Objetos de rede), abra o menu de contexto (clique com o botão direito) e escolha New (Novo), Interoperable Device (Dispositivo interoperável).
4. Em Name (Nome), insira o nome que você forneceu para o túnel; por exemplo, `AWS_VPC_Tunnel_1` ou `AWS_VPC_Tunnel_2`.

5. Em IPv4 Endereço, insira o endereço IP externo do gateway privado virtual fornecido no arquivo de configuração, por exemplo,`54.84.169.196`. Salve as configurações e feche a caixa de diálogo.



6. Em SmartDashboard, abra as propriedades do gateway e, no painel de categorias, escolha Topologia.
7. Para recuperar a configuração da interface, escolha Get Topology.
8. Na seção VPN Domain (Domínio da VPN), escolha Manually defined (Definido manualmente) e procure e selecione o grupo vazio simples criado na etapa 2. Escolha OK.

> **Note**
>
> É possível manter qualquer domínio de VPN existente que configurou. Entretanto, verifique se os hosts e as redes que são usadas ou fornecidas pela nova conexão VPN não estão declarados nesse domínio de VPN, especialmente se esse domínio de VPN for originado automaticamente.

9. Repita essas etapas para criar um segundo objeto de rede, usando as informações na seção `IPSec Tunnel #2` do arquivo de configuração.

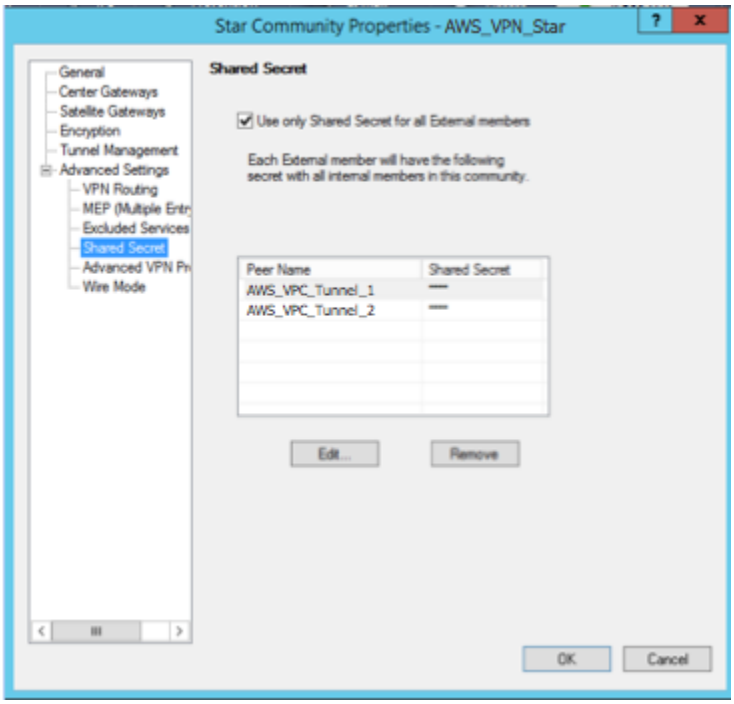
> **Note**
>
> Se estiver usando clusters, edite a topologia e defina as interfaces como interfaces de cluster. Use os endereços IP especificados no arquivo de configuração.

Para criar e configurar a comunidade VPN, o IKE e IPsec as configurações

Nesta etapa, você criará uma comunidade VPN no gateway do Check Point à qual adicionará objetos de rede (dispositivos interoperáveis) para cada túnel. Você também define o Internet Key Exchange (IKE) e IPsec as configurações.

1. Nas propriedades do gateway, escolha IPSecVPN no painel de categorias.
2. Escolha Communities, New, Star Community.
3. Forneça um nome para a comunidade (por exemplo, `AWS_VPN_Star`) e escolha Center Gateways no painel de categoria.
4. Escolha Adicionar e adicione o gateway ou cluster à lista de gateways participantes.
5. No painel de categoria, escolha Satellite Gateways (Gateways secundários), Add (Adicionar) e adicione os dispositivos interoperáveis que você criou anteriormente (`AWS_VPC_Tunnel_1` e `AWS_VPC_Tunnel_2`) à lista de gateways participantes.
6. No painel de categoria, escolha Encryption. Na seção Método de criptografia, escolha IKEv1 somente. Na seção Encryption Suite, escolha Custom, Custom Encryption.
7. Na caixa de diálogo, configure as propriedades de criptografia como a seguir e escolha OK ao concluir:
   - Propriedades da associação de segurança IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Propriedades da Associação de Segurança (Fase 2):
     - Execute a criptografia IPsec de dados com: AES-128
     - Perform data integrity with: SHA-1
8. No painel de categoria, escolha Tunnel Management. Escolha Set Permanent Tunnels, On all tunnels in the community. Na seção VPN Tunnel Sharing (Compartilhamento de túnel VPN), escolha One VPN tunnel per Gateway pair (Um túnel VPN por par de gateway).
9. No painel de categoria, expanda Advanced Settings (Configurações Avançadas) e escolha Shared Secret.
10. Selecione o nome do par do primeiro túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção `IPSec Tunnel #1`.

11. Selecione o nome do par do segundo túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção `IPSec Tunnel #2`.



12. Ainda na categoria Advanced Settings (Configurações avançadas), selecione Advanced VPN Properties (Propriedades avançadas da VPN), configure as propriedades da forma a seguir e escolha OK ao concluir:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): `Group 2`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Fase 2):
        - Escolha Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): `Group 2`
        - Renegocie associações de IPsec segurança a cada segundo **`3600`**

Para criar regras de firewall

Nesta etapa, você configurará uma politica com regras de firewall e regras de correspondência direcional que permitem a comunicação entre a VPC e a rede local. Em seguida, você instalará a política em seu gateway.

1. No SmartDashboard, escolha Propriedades globais para seu gateway. No painel de categoria, expanda VPN e escolha Advanced.
2. Escolha Enable VPN Directional Match in VPN Column e salve suas alterações.
3. No SmartDashboard, escolha Firewall e crie uma política com as seguintes regras:
   - Permitir que a sub-rede da VPC comunique-se com a rede local nos protocolos exigidos.
   - Permitir que a rede local comunique-se com a sub-rede da VPC nos protocolos exigidos.
4. Abra o menu de contexto da célula na coluna VPN e escolha Editar Célula.
5. Na caixa de diálogo Condições de correspondência VPN, escolha Corresponder o tráfego apenas nesta direção. Crie as regras de correspondência direcional a seguir escolhendo Add para cada uma e escolha OK ao concluir:
   - `internal_clear` > comunidade VPN (a comunidade estrela da VPN que você criou anteriormente, por exemplo, `AWS_VPN_Star`)
   - Comunidade VPN > Comunidade VPN
   - Comunidade VPN > `internal_clear`
6. Em SmartDashboard, escolha Política, Instalar.
7. Na caixa de diálogo, escolha seu gateway e clique em OK para instalar a política.

Para modificar a propriedade tunnel_keepalive_method

O gateway do Check Point pode usar o Dead Peer Detection (DPD) para identificar quando uma associação IKE está inativa. Para configurar o DPD para um túnel permanente, o túnel permanente deve ser configurado na comunidade AWS VPN (consulte a Etapa 8).

Por padrão, a propriedade `tunnel_keepalive_method` para um gateway VPN é configurada como `tunnel_test`. Você precisa alterar o valor para dpd. Cada gateway de VPN na comunidade VPN que requer monitoramento de DPD deve ser configurado com a propriedade `tunnel_keepalive_method`, incluindo qualquer gateway de VPN de terceiros. Você não pode configurar diferentes mecanismos de monitoramento para o mesmo gateway.

Você pode atualizar a `tunnel_keepalive_method` propriedade usando a DBedit ferramenta Gui.

1. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.

2. Escolha File (Arquivo), Database Revision Control...(Controle de revisão de banco de dados…) e crie um snapshot de revisão.
3. Feche todas as SmartConsole janelas, como a SmartDashboard, SmartView Rastreador e SmartView Monitor.
4. Inicie a BDedit ferramenta Gui. Para obter mais informações, consulte o artigo Check Point Database Tool (Ferramenta de banco de dados de pontos de verificação) no Check Point Support Center.
5. Escolha Security Management Server(Servidor de gerenciamento de segurança), Domain Management Server (Servidor de gerenciamento de domínio).
6. No painel superior esquerdo, escolha Table (tabela), Network Objects (Objetos de rede), network_objects.
7. No painel superior direito, selecione o objeto Security Gateway (Gateway de Segurança), Cluster pertinente.
8. Pressione CTRL+F ou use o menu Search (Buscar) para procurar o seguinte: `tunnel_keepalive_method`.
9. No painel inferior, abra o menu de contexto para `tunnel_keepalive_method` e escolha Edit... (Editar). Escolha dpd e OK.
10. Repita as etapas de 7 a 9 para cada gateway que fizer parte da comunidade da AWS VPN.
11. Escolha File (Arquivo), Save All (Salvar Tudo).
12. Feche a DBedit ferramenta Gui.
13. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
14. Instale a política no objeto Security Gateway (Gateway de Segurança), Cluster pertinente.

Para obter mais informações, consulte o artigo New VPN features in R77.10 (Novos recursos de VPN no R77.10) no Check Point Support Center.

Para ativar o ajuste de MSS TCP

O ajuste MSS TCP reduz o tamanho máximo de segmento dos pacotes TCP para impedir a fragmentação de pacotes.

1. Navegue até o seguinte diretório `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Abra o Check Point Database Tool executando o arquivo `GuiDBEdit.exe`.

3. Escolha Table (Tabela), Global Properties (Propriedades Globais), properties (propriedades).
4. Em `fw_clamp_tcp_mss`, escolha Edit (Editar). Altere o valor para `true` e escolha OK.

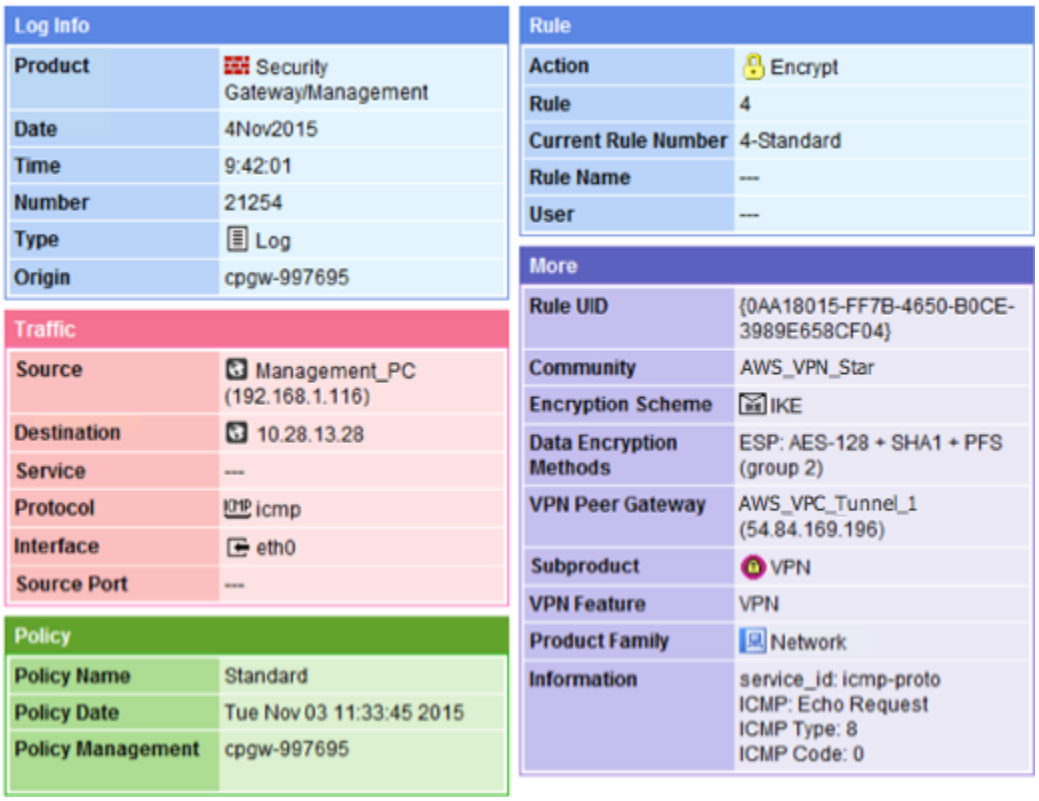
Como verificar o status do túnel

É possível verificar o status do túnel executando o comando a seguir na ferramenta da linha de comando, no modo especialista.

```
vpn tunnelutil
```

Nas opções exibidas, escolha 1 para verificar as associações IKE e 2 para verificar as IPsec associações.

É possível usar também Check Point Smart Tracker Log para verificar se os pacotes na conexão estão sendo criptografados. Por exemplo, o log a seguir indica que a VPC foi enviada pelo túnel 1 e foi criptografada.



SonicWALL

O procedimento a seguir demonstra como configurar os túneis VPN no dispositivo SonicWALL usando a interface de gerenciamento SonicOS.

Para configurar os túneis

1. Abra a interface de gerenciamento SonicWALL SonicOS.
2. No painel esquerdo, escolha VPN, Configurações. Em VPN Policies, escolha Adicionar....
3. Na janela de política VPN na guia Geral , conclua com as seguintes informações:
   - Policy Type (Tipo de política): escolha Tunnel Interface (Interface do túnel).
   - Em Método de autenticação: Escolha IKE using Preshared Secret.
   - Nome: Insira um nome para a política VPN. Recomendamos que você use o nome do ID VPN, conforme fornecido no arquivo de configuração.
   - IPsec Nome ou endereço do gateway primário: insira o endereço IP do gateway privado virtual conforme fornecido no arquivo de configuração (por exemplo,`72.21.209.193`).
   - IPsec Nome ou endereço do gateway secundário: deixe o valor padrão.
   - Shared Secret: Insira a chave pré-compartilhada conforme fornecida no arquivo de configuração, e insira-a novamente em Confirm Shared Secret.
   - ID IKE local: insira o IPv4 endereço do gateway do cliente (o dispositivo SonicWall).
   - ID IKE de mesmo nível: insira o IPv4 endereço do gateway privado virtual.
4. Na guia Network, conclua com as seguintes informações:
   - Em Local Networks, escolha Any address (Qualquer endereço). Recomendamos esta opção para evitar problemas de conectividade na rede local.
   - Em Remote Networks (Redes remotas), escolha Choose a destination network from list (Escolha uma rede de destino na lista). Crie um objeto de endereço com o CIDR da VPC na AWS.
5. Na guia Proposals (Propostas) conclua com as seguintes informações.
   - Em IKE (Phase 1) Proposal, faça o seguinte:
     - Exchange: Escolha Main Mode (Modo Principal).
     - DH Group (Grupo DH): insira um valor para o grupo Diffie-Hellman (por exemplo, `2`).
     - Encriptação: Escolha AES-128 ou AES-256.
     - Autenticação: escolha SHA1ou SHA256.
     - Life Time: Insira `28800`.
   - Em IKE (Phase 2) Proposal, faça o seguinte:
     - Protocolo: Escolha ESP.

- Encriptação: Escolha AES-128 ou AES-256.
- Autenticação: escolha SHA1ou SHA256.
- Selecione a caixa de seleção Enable Perfect Forward Secrecy (Habilite o sigilo de encaminhamento perfeito) e escolha o grupo Diffie-Hellman.
- Life Time: Insira `3600`.

> **Important**
>
> Se você criou seu gateway privado virtual antes de outubro de 2015, deverá especificar o grupo 2 do Diffie-Hellman, AES-128 e para ambas as fases. SHA1

6. Na guia Advanced (Avançado) conclua com as seguintes informações:
   - Selecione Enable Keep Alive.
   - Selecione Enable Phase2 Dead Peer Detection e insira o seguinte:
     - Em Dead Peer Detection Interval, insira `60` (este é o mínimo que o dispositivo SonicWALL aceita).
     - Em Failure Trigger Level, insira `3`.
   - Em VPN Policy bound to, selecione Interface X1. Essa é a interface designada normalmente para endereços IP públicos.
7. Escolha OK. Na página Configurações a caixa de seleção Habilitar para o túnel deve ser selecionada por padrão. Um ponto verde indica que o túnel está ativo.

Dispositivos Cisco: informações adicionais

Alguns Cisco suportam ASAs apenas o Active/Standby modo. Quando você usa esses Cisco ASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo se o primeiro túnel ficar indisponível. Com essa redundância, você sempre deverá ter conectividade com sua VPC por meio de um dos túneis.

Cisco ASAs a partir da versão 9.7.1 e posterior do modo de suporte Active/Active . Ao usar esses Cisco ASAs, você pode ter os dois túneis ativos ao mesmo tempo. Com essa redundância, você sempre deverá ter conectividade com sua VPC por meio de um dos túneis.

Para dispositivos Cisco, é necessário fazer o seguinte:

- Configurar a interface externa.
- Garantir que o número Crypto ISAKMP Policy Sequence seja exclusivo.
- Garanta que o número Crypto List Policy Sequence seja exclusivo.
- Certifique-se de que o conjunto de IPsec transformações criptográficas e a sequência de políticas do Crypto ISAKMP estejam em harmonia com quaisquer outros IPsec túneis configurados no dispositivo.
- Garantir que o número de monitoramento de SLA seja exclusivo.
- Configurar todo o roteamento interno que move o tráfego entre o gateway do cliente e a rede local.

Arquivos de configuração de roteamento dinâmico que podem ser baixados para o dispositivo de gateway AWS Site-to-Site VPN do cliente

Para baixar um arquivo de configuração de amostra com valores específicos para sua configuração de conexão Site-to-Site VPN, use o console da Amazon VPC, a linha de AWS comando ou a API do Amazon EC2. Para obter mais informações, consulte Etapa 6: baixar o arquivo de configuração.

Você também pode baixar arquivos de configuração de exemplo genéricos para roteamento dinâmico que não incluem valores específicos para sua configuração de conexão Site-to-Site VPN: .zip dynamic-routing-examples

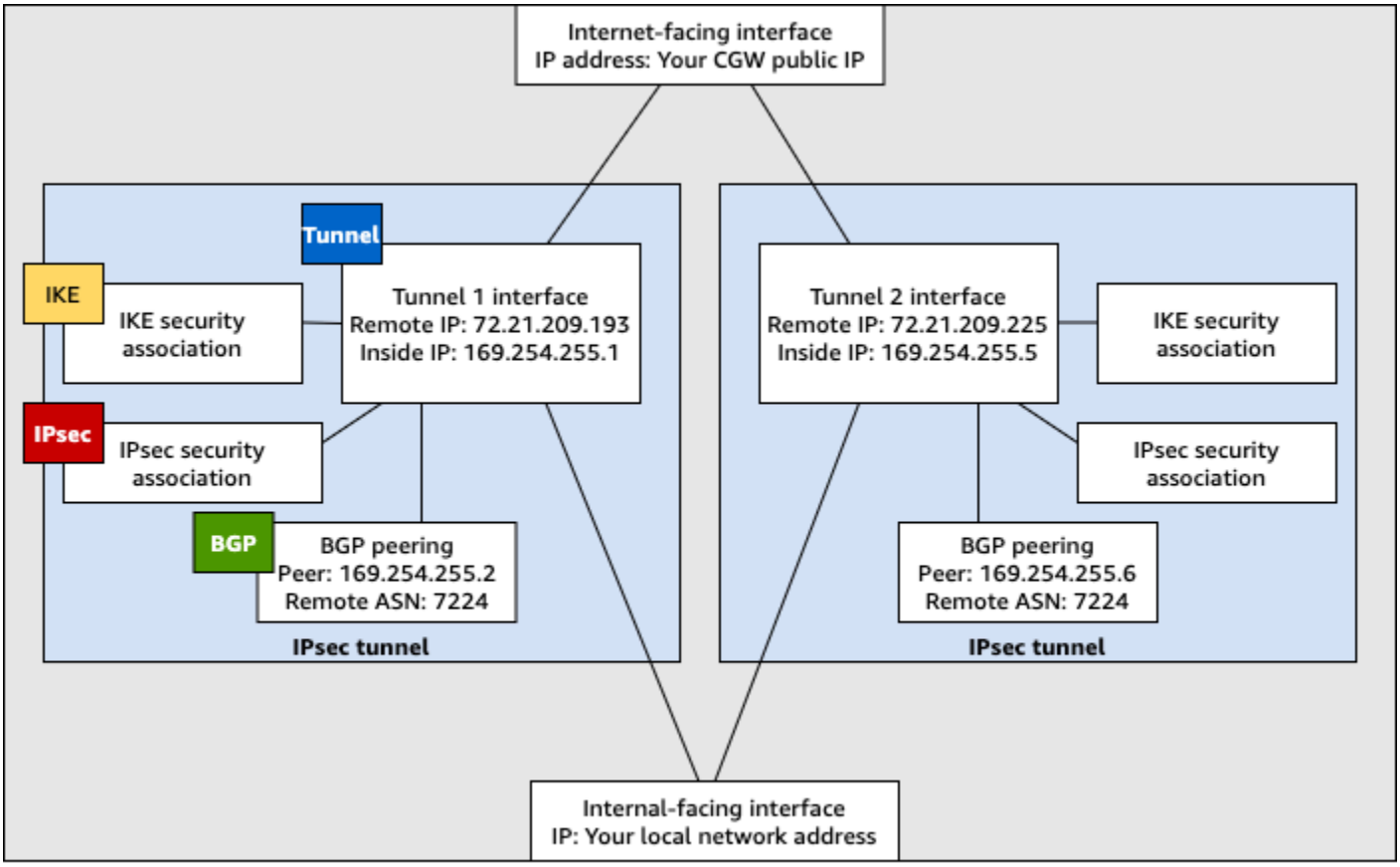
Os arquivos usam valores de espaço reservado para alguns componentes. Por exemplo, eles usam:

- Valores de exemplo para o ID da conexão VPN, ID do gateway do cliente e ID do gateway privado virtual
- Espaços reservados para os AWS endpoints de endereço IP remoto (externo) (*AWS_ENDPOINT_1*e) *AWS_ENDPOINT_2*
- Um espaço reservado para o endereço IP da interface externa roteável pela Internet no dispositivo de gateway do cliente () *your-cgw-ip-address*
- Um espaço reservado para o valor da chave pré-compartilhada () pre-shared-key
- Valores de exemplo para o túnel dentro de endereços IP.
- Valores de exemplo para a configuração de MTU.

> **Note**
>
> As configurações de MTU fornecidas nos arquivos de configuração de amostra são apenas exemplos. Consulte Melhores práticas para um dispositivo de gateway AWS Site-to-Site VPN do cliente para obter informações sobre como definir o valor MTU ideal para a sua situação.

Além de fornecer valores de espaço reservado, os arquivos especificam os requisitos mínimos para uma conexão Site-to-Site VPN de AES128, SHA1, e Diffie-Hellman grupo 2 na maioria das AWS regiões e, AES128 SHA2, e Diffie-Hellman grupo 14 nas regiões. AWS GovCloud Eles também especificam chaves pré-compartilhadas para autenticação. Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

O diagrama a seguir fornece uma visão geral dos diferentes componentes configurados no dispositivo de gateway do cliente. Ele inclui valores de exemplo para os endereços IP da interface do túnel.



Configurar o roteamento dinâmico para um dispositivo de gateway AWS Virtual Private Network do cliente

Veja a seguir alguns procedimentos de exemplo para configurar um dispositivo de gateway do cliente usando sua interface de usuário (se disponível).

Check Point

A seguir estão as etapas para configurar um dispositivo Check Point Security Gateway executando o R77.10 ou superior, usando o portal web Gaia e o Check Point. SmartDashboard Você também pode consultar o artigo Amazon Web Services (AWS) VPN BGP no Check Point Support Center.

Para configurar a interface do túnel

O primeiro passo é criar túneis de VPN e fornecer os endereços IP privados (internos) do gateway do cliente e do gateway privado virtual de cada túnel. Para criar o primeiro túnel, use as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração. Para criar o segundo túnel, use os valores fornecidos na seção `IPSec Tunnel #2` do arquivo de configuração.

1. Conecte seu gateway de segurança por SSH. Se estiver usando um shell não padrão, mude para clish executando o comando a seguir: `clish`
2. Defina o ASN do gateway do cliente (o ASN fornecido quando o gateway do cliente foi criado em AWS) executando o comando a seguir.

   ```
   set as 65000
   ```

3. Crie a interface para o primeiro túnel, usando as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração. Forneça um nome exclusivo para seu túnel, como `AWS_VPC_Tunnel_1`.

   ```
   add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
    peer AWS_VPC_Tunnel_1
   set interface vpnt1 state on
   set interface vpnt1 mtu 1436
   ```

4. Repita esses comandos para criar o segundo túnel, usando as informações fornecidas na seção `IPSec Tunnel #2` do arquivo de configuração. Forneça um nome exclusivo para seu túnel, como `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Defina o ASN do gateway privado virtual:

```
set bgp external remote-as 7224 on
```

6. Configure o BGP para o primeiro túnel, usando as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração:

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Configure o BGP para o segundo túnel, usando as informações fornecidas na seção `IPSec Tunnel #2` do arquivo de configuração:

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Salve a configuração.

```
save config
```

Para criar uma política de BGP

Depois, crie uma política de BGP que permita a importação das rotas anunciadas pela AWS. Em seguida, configure seu gateway do cliente para anunciar suas rotas locais para a AWS.

1. Na Gaia WebUI, escolha Advanced Routing (Roteamento avançado), Inbound Route Filters (Filtros de rota de entrada). Escolha Add (Adicionar) e selecione Add BGP Policy (Based on AS) (Adicionar política de BGP (com base em AS)).
2. Em Add BGP Policy (Adicionar política de BGP), selecione um valor entre 512 e 1024 no primeiro campo e insira o ASN do gateway privado virtual no segundo campo (por exemplo, 7224).

3. Escolha Salvar.

Para anunciar rotas locais

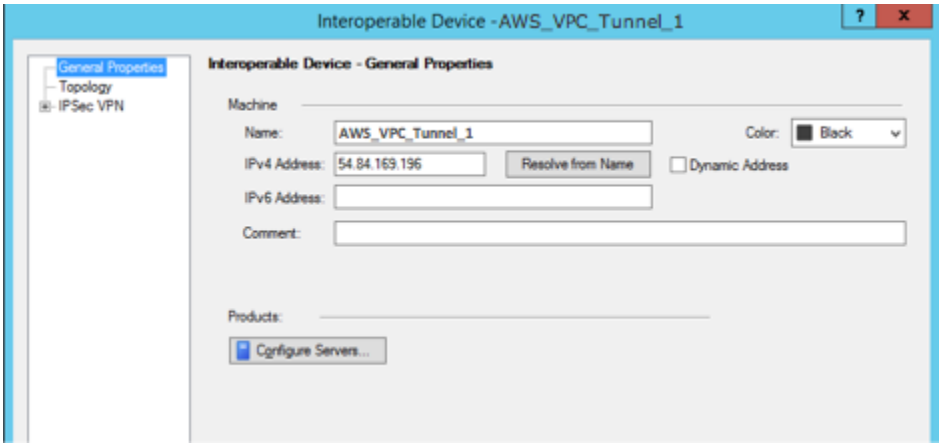
As etapas a seguir destinam-se à distribuição de rotas de interface locais. Além disso, você pode redistribuir as rotas de diferentes origens (por exemplo, rotas estáticas ou rotas obtidas por meio de protocolos de roteamento dinâmico). Para obter mais informações, consulte Gaia Advanced Routing R77 Versions Administration Guide.

1. Na Gaia WebUI, escolha Advanced Routing (Roteamento Avançado), Routing Redistribution (Redistribuição de Roteamento). Selecione Add Redistribution From (Adicionar redistribuição de) e escolha Interface.
2. Em To Protocol (Para o protocolo), selecione o ASN do gateway privado virtual (por exemplo, `7224`).
3. Em Interface, selecione uma interface interna. Escolha Salvar.

Para definir um novo objeto de rede

Depois, crie um objeto de rede para cada túnel de VPN, especificando os endereços IP públicos (externos) para o gateway privado virtual. Posteriormente, você adicionará esses objetos de rede como gateways secundários para sua comunidade VPN. Você precisa também criar um grupo vazio para funcionar como espaço reservado para o domínio de VPN.

1. Abra o Check Point SmartDashboard.
2. Em Groups (Grupos), abra o menu de contexto e escolha Groups (Grupos), Simple Group (Grupo Simples). É possível usar o mesmo grupo para cada objeto de rede.
3. Em Network Objects, abra o menu de contexto (clique com o botão direito) e escolha New, Interoperable Device.
4. Em Name (Nome), insira o nome que você forneceu para o túnel na etapa 1, por exemplo, `AWS_VPC_Tunnel_1` ou `AWS_VPC_Tunnel_2`.
5. Em IPv4 Endereço, insira o endereço IP externo do gateway privado virtual fornecido no arquivo de configuração, por exemplo,`54.84.169.196`. Salve as configurações e feche a caixa de diálogo.



6. No painel de categoria, escolha Topology (Topologia).
7. Na seção VPN Domain (Domínio da VPN), escolha Manually defined (Definido manualmente) e procure e selecione o grupo vazio simples criado na etapa 2. Escolha OK.
8. Repita essas etapas para criar um segundo objeto de rede, usando as informações na seção `IPSec Tunnel #2` do arquivo de configuração.
9. Acesse o objeto de rede do gateway, abra o gateway ou objeto do cluster e escolha Topology (Topologia).
10. Na seção VPN Domain (Domínio da VPN), escolha Manually defined (Definido manualmente) e procure e selecione o grupo vazio simples criado na etapa 2. Escolha OK.

> **Note**
>
> É possível manter qualquer domínio de VPN existente que configurou. Entretanto, verifique se os hosts e as redes que são usadas ou fornecidas pela nova conexão VPN não estão declarados nesse domínio de VPN, especialmente se esse domínio de VPN for originado automaticamente.

> **Note**
>
> Se estiver usando clusters, edite a topologia e defina as interfaces como interfaces de cluster. Use os endereços IP especificados no arquivo de configuração.

Para criar e configurar a comunidade VPN, o IKE e IPsec as configurações

Depois, crie uma comunidade VPN no gateway do Check Point, à qual você adicionará objetos de rede (dispositivos interoperáveis) para cada túnel. Você também define o Internet Key Exchange (IKE) e IPsec as configurações.

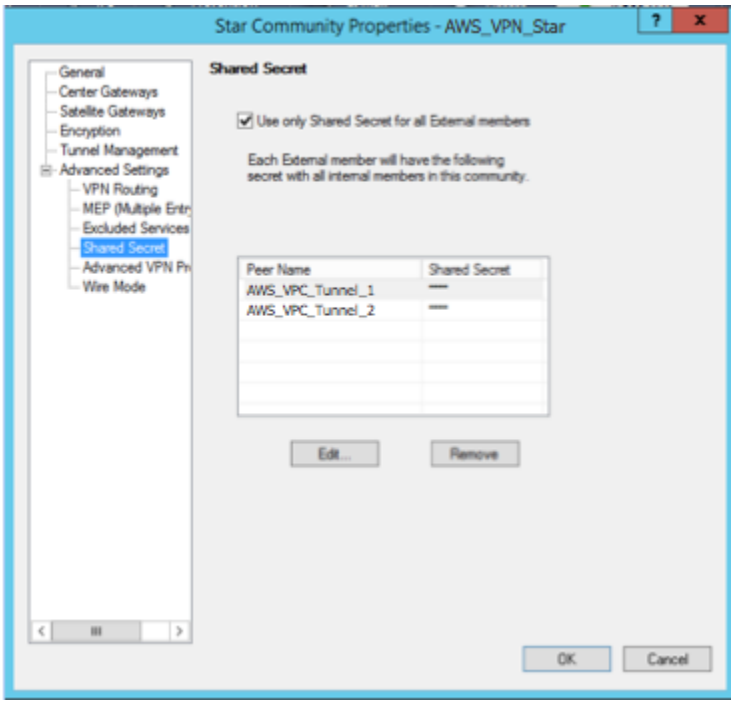
1. Nas propriedades do gateway, escolha IPSecVPN no painel de categorias.
2. Escolha Communities, New, Star Community.
3. Forneça um nome para a comunidade (por exemplo, `AWS_VPN_Star`) e escolha Center Gateways no painel de categoria.
4. Escolha Adicionar e adicione o gateway ou cluster à lista de gateways participantes.
5. No painel de categoria, selecione Satellite Gateways (Gateways secundários), Add (Adicionar) e adicione os dispositivos interoperáveis criados anteriormente (`AWS_VPC_Tunnel_1` e `AWS_VPC_Tunnel_2`) à lista de gateways participantes.
6. No painel de categoria, escolha Encryption. Na seção Método de criptografia, escolha IKEv1 para IPv4 e IKEv2 para IPv6. Na seção Encryption Suite, escolha Custom, Custom Encryption.

   > **Note**
   >
   > Você deve selecionar a IPv6 opção IKEv1 para IPv4 e IKEv2 para para a IKEv1 funcionalidade.

7. Na caixa de diálogo, configure as propriedades de criptografia como indicado a seguir e selecione OK ao concluir:

   - Propriedades da associação de segurança IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Propriedades da Associação de Segurança (Fase 2):
     - Execute a criptografia IPsec de dados com: AES-128
     - Perform data integrity with: SHA-1
8. No painel de categoria, escolha Tunnel Management. Escolha Set Permanent Tunnels, On all tunnels in the community. Na seção VPN Tunnel Sharing (Compartilhamento de túnel VPN), escolha One VPN tunnel per Gateway pair (Um túnel VPN por par de gateway).

9. No painel de categoria, expanda Advanced Settings (Configurações Avançadas) e escolha Shared Secret.
10. Selecione o nome do par do primeiro túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção `IPSec Tunnel #1`.
11. Selecione o nome do par do segundo túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção `IPSec Tunnel #2`.



12. Ainda na categoria Advanced Settings (Configurações avançadas), selecione Advanced VPN Properties (Propriedades avançadas da VPN), configure as propriedades da forma a seguir e escolha OK ao concluir:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Fase 2):
        - Escolha Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegocie associações de IPsec segurança a cada segundo **`3600`**

Para criar regras de firewall

Depois, configure uma politica com regras de firewall e regras de correspondência direcional que permitam a comunicação entre a VPC e a rede local. Em seguida, você instalará a política em seu gateway.

1. No SmartDashboard, escolha Propriedades globais para seu gateway. No painel de categoria, expanda VPN e escolha Advanced (Avançado).
2. Escolha Enable VPN Directional Match in VPN Column (Habilitar correspondência direcional VPN na coluna VPN) e clique em OK.
3. No SmartDashboard, escolha Firewall e crie uma política com as seguintes regras:
   - Permitir que a sub-rede da VPC comunique-se com a rede local nos protocolos exigidos.
   - Permitir que a rede local comunique-se com a sub-rede da VPC nos protocolos exigidos.
4. Abra o menu de contexto da célula na coluna VPN e escolha Editar Célula.
5. Na caixa de diálogo VPN Match Conditions (Condições de correspondência VPN), escolha Match traffic in this direction only (Corresponder tráfego apenas nesta direção). Crie as regras de correspondência direcional a seguir selecionando Add (Adicionar) para cada uma e selecione OK ao concluir:
   - `internal_clear` **>** comunidade VPN (a comunidade estrela da VPN que você criou anteriormente, por exemplo, `AWS_VPN_Star`)
   - Comunidade VPN **>** Comunidade VPN
   - Comunidade VPN **>** `internal_clear`
6. Em SmartDashboard, escolha Política, Instalar.
7. Na caixa de diálogo, escolha seu gateway e clique em OK para instalar a política.

Para modificar a propriedade tunnel_keepalive_method

O gateway do Check Point pode usar o Dead Peer Detection (DPD) para identificar quando uma associação IKE está inativa. Para configurar o DPD para um túnel permanente, o túnel permanente deve ser configurado na comunidade AWS VPN.

Por padrão, a propriedade `tunnel_keepalive_method` para um gateway VPN é configurada como `tunnel_test`. Você precisa alterar o valor para `dpd`. Cada gateway de VPN na comunidade VPN que requer monitoramento de DPD deve ser configurado com a propriedade

`tunnel_keepalive_method`, incluindo qualquer gateway de VPN de terceiros. Você não pode configurar diferentes mecanismos de monitoramento para o mesmo gateway.

Você pode atualizar a `tunnel_keepalive_method` propriedade usando a DBedit ferramenta Gui.

1. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
2. Escolha File (Arquivo), Database Revision Control...(Controle de revisão de banco de dados…) e crie um snapshot de revisão.
3. Feche todas as SmartConsole janelas, como, por exemplo SmartDashboard, o SmartView Rastreador e o SmartView Monitor.
4. Inicie a BDedit ferramenta Gui. Para obter mais informações, consulte o artigo Check Point Database Tool (Ferramenta de banco de dados de pontos de verificação) no Check Point Support Center.
5. Escolha Security Management Server(Servidor de gerenciamento de segurança), Domain Management Server (Servidor de gerenciamento de domínio).
6. No painel superior esquerdo, escolha Table (tabela), Network Objects (Objetos de rede), network_objects.
7. No painel superior direito, selecione o objeto Security Gateway (Gateway de Segurança), Cluster pertinente.
8. Pressione CTRL+F ou use o menu Search (Buscar) para procurar o seguinte: `tunnel_keepalive_method`.
9. No painel inferior, abra o menu de contexto para `tunnel_keepalive_method` e selecione Edit... (Editar…). Escolha dpd, OK.
10. Repita as etapas de 7 a 9 para cada gateway que fizer parte da comunidade da AWS VPN.
11. Escolha File (Arquivo), Save All (Salvar Tudo).
12. Feche a DBedit ferramenta Gui.
13. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
14. Instale a política no objeto Security Gateway (Gateway de Segurança), Cluster pertinente.

Para obter mais informações, consulte o artigo New VPN features in R77.10 (Novos recursos de VPN no R77.10) no Check Point Support Center.

Para ativar o ajuste de MSS TCP

O ajuste MSS TCP reduz o tamanho máximo de segmento dos pacotes TCP para impedir a fragmentação de pacotes.

1. Navegue até o seguinte diretório `C:\Program Files (x86)\CheckPoint \SmartConsole\R77.10\PROGRAM\`.
2. Abra o Check Point Database Tool executando o arquivo `GuiDBEdit.exe`.
3. Escolha Table (Tabela), Global Properties (Propriedades Globais), properties (propriedades).
4. Em `fw_clamp_tcp_mss`, escolha Edit (Editar). Altere o valor para `true` e selecione OK.

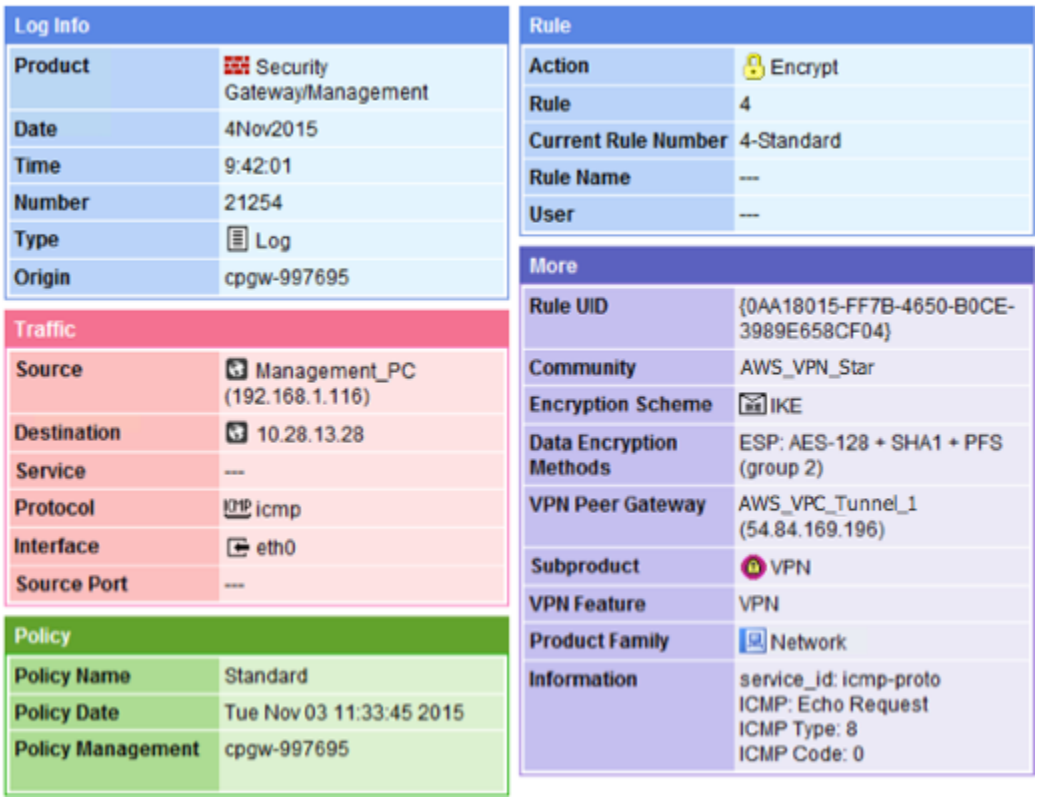
Como verificar o status do túnel

É possível verificar o status do túnel executando o comando a seguir na ferramenta da linha de comando, no modo especialista.

```
vpn tunnelutil
```

Nas opções exibidas, escolha 1 para verificar as associações IKE e 2 para verificar as IPsec associações.

É possível usar também Check Point Smart Tracker Log para verificar se os pacotes na conexão estão sendo criptografados. Por exemplo, o log a seguir indica que a VPC foi enviada pelo túnel 1 e foi criptografada.



SonicWALL

É possível configurar um dispositivo SonicWALL usando a interface de gerenciamento SonicOS. Para obter mais informações sobre a configuração de túneis, consulte Configurar o roteamento estático para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Não é possível configurar o BGP para o dispositivo, usando a interface de gerenciamento. Em vez disso, use as instruções da linha de comando fornecidas no arquivo de configuração de exemplo, na seção chamada BGP.

Dispositivos Cisco: informações adicionais

Alguns Cisco suportam ASAs apenas o Active/Standby modo. Quando você usa esses Cisco ASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo se o primeiro túnel ficar indisponível. Com essa redundância, você sempre deverá ter conectividade com sua VPC por meio de um dos túneis.

Cisco ASAs a partir da versão 9.7.1 e posterior do modo de suporte Active/Active . Ao usar esses Cisco ASAs, você pode ter os dois túneis ativos ao mesmo tempo. Com essa redundância, você sempre deverá ter conectividade com sua VPC por meio de um dos túneis.

Para dispositivos Cisco, é necessário fazer o seguinte:

- Configurar a interface externa.
- Garantir que o número Crypto ISAKMP Policy Sequence seja exclusivo.
- Garanta que o número Crypto List Policy Sequence seja exclusivo.
- Certifique-se de que o conjunto de IPsec transformações criptográficas e a sequência de políticas do Crypto ISAKMP estejam em harmonia com quaisquer outros IPsec túneis configurados no dispositivo.
- Garantir que o número de monitoramento de SLA seja exclusivo.
- Configurar todo o roteamento interno que move o tráfego entre o gateway do cliente e a rede local.

Dispositivos Juniper: informações adicionais

As informações a seguir se aplicam aos arquivos de configuração de exemplo para dispositivos de gateway do cliente Juniper J-Series e SRX.

- A interface externa é chamada de *ge-0/0/0.0*.
- A interface do IDs túnel é chamada de *st0.1* *st0.2* e.
- Certifique-se de identificar a zona de segurança da interface de uplink (as informações de configuração usam a zona padrão "untrust").
- Certifique-se de identificar a zona de segurança da interface interna (as informações de configuração usam a zona padrão "trust").

Configurar o Windows Server como um dispositivo de gateway AWS Site-to-Site VPN do cliente

É possível configurar o servidor que executa o Windows Server como um dispositivo de gateway do cliente para sua VPC. Use o processo a seguir se estiver executando o Windows Server em uma instância do EC2, em uma VPC ou em seu próprio servidor. Os procedimentos a seguir se aplicam ao Windows Server 2012 R2 e versões posteriores.

Conteúdo

- Etapa 2: Baixar o arquivo de configuração para a conexão VPN
- Etapa 3: configurar o Windows Server
- Etapa 4: Configurar o túnel VPN
- Etapa 5: Habilitar a detecção de gateway inativo
- Etapa 6: Testar a conexão VPN

Configurar a instância do Windows

Se você estiver configurando o Windows Server em uma instância do EC2 executada em uma AMI do Windows, faça o seguinte:

- Desative a source/destination verificação da instância:
  1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
  2. Selecione a sua instância do Windows e escolha Actions (Ações), Networking (Rede), Change source/destination check (Alterar verificação de origem/destino). Escolha Stop (Interromper) e, em seguida, escolha Save (Salvar).
- Atualize as configurações do adaptador de modo que você possa rotear tráfego de outras instâncias:
  1. Conecte-se à sua instância do Windows. Para obter mais informações, consulte Conectar-se à sua instância do Windows.
  2. Abra o Painel de controle e inicie o Gerenciador de dispositivos.
  3. Expanda o nó Adaptadores de rede.
  4. Selecione o adaptador de rede (dependendo do tipo de instância, pode ser Amazon Elastic Network Adapter ou Intel 82599 Virtual Function) e escolha Action (Ação), Properties (Propriedades).
  5. Na guia Avançado, desative as propriedades IPv4Checksum Offload, TCP Checksum Offload (IPv4) e UDP Checksum Offload () e escolha OK. IPv4
- Aloque um endereço IP elástico à sua conta e associe-o à instância. Para obter mais informações, consulte Endereços IP elásticos no Guia do usuário do Amazon EC2. Anote esse endereço, pois ele será necessário quando você criar o gateway do cliente.
- Certifique-se de que as regras do grupo de segurança da instância permitam IPsec tráfego de saída. Por padrão, um grupo de segurança permite todo o tráfego de saída. No entanto, se as regras de saída do grupo de segurança tiverem sido modificadas de seu estado original,

você deverá criar as seguintes regras de protocolo de saída personalizadas para IPsec tráfego: protocolo IP 50, protocolo IP 51 e UDP 500.

Tome nota do intervalo CIDR da rede na qual sua instância do Windows está localizada, por exemplo, `172.31.0.0/16`.

Etapa 1: Criar uma conexão VPN e configurar a VPC

Para criar uma conexão VPN partindo de sua VPC, faça o seguinte:

1. Crie um gateway privado virtual e anexe-o à sua VPC. Para obter mais informações, consulte Criar um gateway privado virtual.
2. Crie uma conexão VPN e um novo gateway do cliente. Para o gateway do cliente, especifique o endereço IP público do Windows Server. Para a conexão VPN, escolha roteamento estático e insira o intervalo CIDR para a rede na qual o Windows Server está localizado, por exemplo, `172.31.0.0/16`. Para obter mais informações, consulte Etapa 5: criar uma conexão VPN.

Depois de criar a conexão VPN, configure a VPC para habilitar a comunicação pela conexão VPN.

Para configurar a VPC

- Crie uma sub-rede privada na sua VPC (se ainda não tiver uma) para executar instâncias que se comunicarão com o Windows Server. Para obter mais informações, consulte Criar uma sub-rede na sua VPC.

  > **Note**
  >
  > Uma sub-rede privada é uma sub-rede que não tem uma rota para um gateway da Internet. O roteamento para esta sub-rede é descrito no próximo item.

- Atualize as tabelas de rotas para a conexão VPN:
  - Adicione uma rota à tabela de rotas de sua sub-rede privada com o gateway privado virtual como destino e a rede (intervalo CIDR) do Windows Server como destino. Para obter mais informações, consulte Adicionar e remover rotas de uma tabelas no Amazon Virtual Private Cloud - Guia do usuário.
  - Ative a propagação de rotas para o gateway privado virtual. Para obter mais informações, consulte (Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas.

- Crie um grupo de segurança para suas instâncias que permita a comunicação entre a rede e sua VPC:
  - Adicione regras que permitam acesso de entrada RDP ou SSH de sua rede. Isso possibilita que você se conecte de sua rede a instâncias em sua VPC. Por exemplo, para permitir que computadores em sua rede acessem instâncias do Linux em sua VPC, crie uma regra de entrada com um tipo de SSH e o conjunto de fontes para o intervalo CIDR de sua rede (por exemplo, `172.31.0.0/16`). Para mais informações, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.
  - Adicione uma regra que permita acesso ICMP de entrada de sua rede. Isso possibilita que você teste sua conexão VPN executando ping em uma instância em sua VPC em seu Windows Server.

Etapa 2: Baixar o arquivo de configuração para a conexão VPN

É possível usar o console da Amazon VPC para baixar um arquivo de configuração do Windows Server para sua conexão VPN.

Para baixar o arquivo de configuração

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Connections (Conexões VPN).
3. Selecione sua conexão VPN e escolha Download Configuration (Baixar configuração).
4. Selecione Microsoft como fornecedor, Windows Server como plataforma e 2012 R2 como software. Escolha Baixar. É possível abrir ou salvar o arquivo.

O arquivo de configuração contém uma seção de informações semelhante ao exemplo a seguir. Essas informações serão apresentadas duas vezes, uma vez para cada túnel.

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

O endereço IP especificado para o gateway do cliente quando criou a conexão VPN.

`Remote Tunnel Endpoint`

Um dos dois endereços IP do gateway privado virtual que encerra a conexão VPN no AWS lado da conexão.

`Endpoint 1`

O prefixo de IP especificado como rota estática ao criar a conexão VPN. Esses são os endereços IP em sua rede que têm permissão para usar a conexão VPN para acessar sua VPC.

`Endpoint 2`

O intervalo de endereços IP (bloco CIDR) da VPC anexado ao gateway privado virtual (por exemplo, 10.0.0.0/16).

`Preshared key`

A chave pré-compartilhada usada para estabelecer a conexão IPsec VPN entre `Local Tunnel Endpoint` e. `Remote Tunnel Endpoint`

Sugerimos que você configure os dois túneis como parte da conexão VPN. Cada túnel se conecta a um concentrador Site-to-Site VPN separado no lado Amazon da conexão VPN. Embora somente um túnel por vez fique ativo, o segundo túnel se estabelece quando o primeiro é desativado. Ter túneis redundantes garante disponibilidade contínua no caso de falha de um dispositivo. Pelo fato de somente um túnel por vez estar disponível, o console da Amazon VPC indica que um túnel está desativado. Como esse comportamento é esperado, nenhuma ação é necessária de sua parte.

Com dois túneis configurados, se ocorrer uma falha no dispositivo AWS, sua conexão VPN automaticamente passará para o segundo túnel do gateway privado virtual em questão de minutos. Ao configurar o dispositivo de gateway do cliente, é importante configurar ambos os túneis.

> **Note**
>
> De tempos em tempos, AWS realiza manutenção de rotina no gateway privado virtual. Essa manutenção pode desabilitar um dos dois túneis da conexão VPN durante um breve espaço de tempo. Sua conexão VPN executa failover automaticamente no segundo túnel enquanto realizamos essa manutenção.

Informações adicionais sobre o Internet Key Exchange (IKE) e as IPsec Security Associations (SA) são apresentadas no arquivo de configuração baixado.

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

Os algoritmos de criptografia e autenticação da SA IKE. Essas são as configurações sugeridas para a conexão VPN e as configurações padrão para conexões IPsec VPN do Windows Server.

`MainModeKeyLifetime`

Vida útil da chave SA IKE. Essa é a configuração sugerida para a conexão VPN e é a configuração padrão para conexões IPsec VPN do Windows Server.

`QuickModeSecMethods`

Os algoritmos de criptografia e autenticação para o IPsec SA. Essas são as configurações sugeridas para a conexão VPN e as configurações padrão para conexões IPsec VPN do Windows Server.

`QuickModePFS`

Sugerimos que você use a chave mestra perfect forward secrecy (PFS) para suas sessões. IPsec

Etapa 3: configurar o Windows Server

Antes de configurar o túnel VPN, você precisa instalar e configurar os Serviços de Roteamento e Acesso Remoto no Windows Server. Isso permite que os usuários remotos acessem os recursos na rede.

Para instalar os Serviços de Roteamento e Acesso Remoto

1. Faça logon no seu Windows Server.
2. Vá para o menu Start e escolha Server Manager.
3. Instale Serviços de Roteamento e Acesso Remoto:

    a. No menu Manage (Gerenciar), escolha Add Roles and Features (Adicionar funções e recursos).

b. Na página Before You Begin (Antes de iniciar), verifique se seu servidor atende aos pré-requisitos e escolha Next (Próximo).

c. Escolha Role-based or feature-based installation (Instalação baseada em funções ou recursos) e Next (Próximo).

d. Escolha Select a server from the server pool (Selecionar um servidor no pool de servidor), selecione o Windows Server e escolha Next (Avançar).

e. Selecione Network Policy and Access Services (Política de rede e serviços de acesso) na lista. Na caixa de diálogo exibida, escolha Add Features (Adicionar recursos) para confirmar os recursos necessários para esta função.

f. Na mesma lista, escolha Acesso Remoto, Próximo.

g. Na página Select features (Selecionar recursos), escolha Next (Próximo).

h. Na página Network Policy and Access Services (Política de rede e serviços de acesso), escolha Next (Próximo).

i. Na página Remote Access (Acesso remoto), escolha Next (Próximo). Na próxima página, selecione DirectAccess VPN (RAS). Na caixa de diálogo exibida, escolha Add Features (Adicionar Recursos) para confirmar os recursos necessários para este serviço de função. Na mesma lista, selecione Routing (Roteamento) e escolha Next (Próximo).

j. Na página Web Server Role (IIS), escolha Next. Deixe a seleção padrão e escolha Next (Próximo).

k. Escolha Instalar. Quando a instalação terminar, escolha Fechar.

Para configurar e ativar o Servidor de Roteamento e Acesso Remoto

1. No painel, selecione Notifications (Notificações). Deve haver uma tarefa a ser concluída na configuração depois da implantação. Escolha o link Open the Getting Started Wizard (Abra o assistente de primeiros passos).
2. Escolha Deploy VPN only (Implantar apenas VPN).
3. Na caixa de diálogo Routing and Remote Access (Roteamento e acesso remoto), escolha o nome do servidor, escolha Action (Ação) e Configure and Enable Routing and Remote Access (Configurar e habilitar o roteamento e o acesso remoto).
4. Em Routing and Remote Access Server Setup Wizard, na primeira página, escolha Next.
5. Na página Configuração, escolha Configuração Personalizada, Próximo.
6. Escolha Roteamento de LAN, Próximo, Concluir.

7. Quando solicitado pela caixa de diálogo Routing and Remote Access (Roteamento e acesso remoto), escolha Start service (Iniciar serviço).

Etapa 4: Configurar o túnel VPN

É possível configurar o túnel de VPN executando os scripts netsh incluídos no arquivo de configuração baixado ou usando a interface do usuário do Windows Server.

> **Important**
>
> Sugerimos que você use a chave mestra perfect forward secrecy (PFS) para suas sessões. IPsec Se você optar por executar o script netsh, ele incluirá um parâmetro para ativar o PFS ()`qmpfs=dhgroup2`. Você não pode habilitar o PFS usando a interface do usuário do Windows — é preciso habilitá-lo usando a linha de comando.

Opções

- Opção 1: Executar o script netsh
- Opção 2: Usar a interface de usuário do Windows Server

Opção 1: Executar o script netsh

Copie o script netsh do arquivo de configuração baixado e substitua as variáveis. A seguir encontra-se um exemplo de script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: É possível substituir o nome sugerido (`vgw-1a2b3c4d Tunnel 1`) por um nome de sua escolha.

LocalTunnelEndpoint: insira o endereço IP privado do Windows Server na sua rede.

Endpoint1: o bloco CIDR da sua rede em que o Windows Server reside, por exemplo, `172.31.0.0/16`. Cerque esse valor com aspas duplas (“).

Endpoint2: o bloco CIDR da sua VPC ou uma sub-rede na sua VPC, por exemplo, `10.0.0.0/16`. Cerque esse valor com aspas duplas (“).

Execute o script atualizado em uma janela do prompt de comando no Windows Server. (O sinal ^ permite que você corte e cole o texto contornado na linha de comando.) Para configurar o segundo túnel VPN para essa conexão VPN, repita o processo usando o segundo script netsh no arquivo de configuração.

Quando terminar, vá para Configurar o firewall do Windows.

Para obter mais informações sobre os parâmetros netsh, consulte Comandos Netsh AdvFirewall Consec na Microsoft Library. TechNet

Opção 2: Usar a interface de usuário do Windows Server

É possível também usar a interface do usuário do Windows Server para configurar o túnel de VPN.

> **Important**
>
> Você não pode habilitar o Perfect Forward Secrecy (PFS - "sigilo encaminhado") da chave mestra usando a interface do usuário do Windows Server. Você precisa habilitar o PFS usando a linha de comando, conforme descrito em Habilitar segredo de encaminhamento perfeito da chave mestra.

Tarefas

- Configurar uma regra de segurança para um túnel de VPN
- Confirmar a configuração do túnel
- Habilitar segredo de encaminhamento perfeito da chave mestra
- Configurar o firewall do Windows

Configurar uma regra de segurança para um túnel de VPN

Nesta seção, você configurará uma regra de segurança no Windows Server para criar um túnel de VPN.

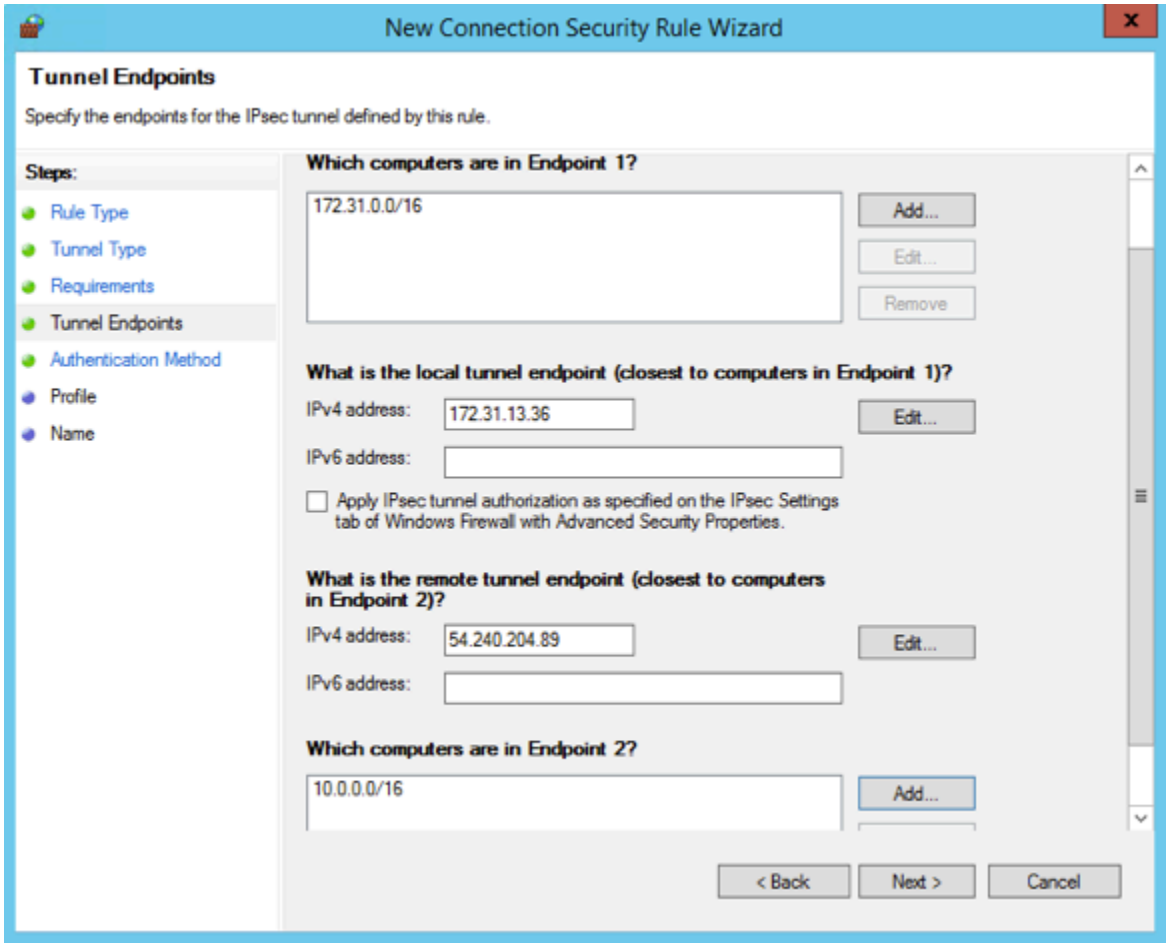
Para configurar uma regra de segurança para um túnel VPN

1. Abra o Gerenciador do Servidor, escolha Tools (Ferramentas) e selecione Windows Firewall with Advanced Security (Firewall do Windows com Segurança Avançada).
2. Selecione Connection Security Rules, escolha Action e New Rule.
3. No assistente New Connection Security Rule (Nova Regra de Segurança de Conexão) da página Rule Type (Tipo de regra), selecione Tunnel (Túnel) e Next (Próximo).
4. Na página Tunnel Type (Tipo de túnel), em What type of tunnel would you like to create (Qual tipo de túnel gostaria de criar), selecione Custom configuration (Configuração personalizada). Em Você gostaria de isentar conexões IPsec protegidas desse túnel, deixe o valor padrão marcado (Não. Envie todo o tráfego de rede que corresponda a essa regra de segurança de conexão (através do túnel) e escolha Avançar.
5. Na página Requisitos, escolha Exigir autenticação para conexões de entrada. Não estabeleça túneis para conexões de saída e escolha Próximo.
6. Na página Tunnel Endpoints (Endpoints de túnel), em Which computers are in Endpoint 1 (Quais computadores estão no endpoint 1), escolha Add (Adicionar). Insira o intervalo CIDR da sua rede (atrás do dispositivo de gateway do cliente do Windows Server; por exemplo, `172.31.0.0/16`) e escolha OK. O intervalo pode incluir o endereço IP do dispositivo de gateway do cliente.
7. Em What is the local tunnel endpoint (closest to computer in Endpoint 1), escolha Edit. No campo de IPv4 endereço, insira o endereço IP privado do Windows Server e escolha OK.
8. Em What is the remote tunnel endpoint (closest to computers in Endpoint 2), escolha Edit. No campo de IPv4 endereço, insira o endereço IP do gateway privado virtual para o túnel 1 do arquivo de configuração (consulte`Remote Tunnel Endpoint`) e escolha OK.

   > **Important**
   >
   > Se você estiver repetindo este procedimento para o túnel 2, certifique-se de selecionar o endpoint para o túnel 2.

9. Em Which computers are in Endpoint 2(Quais computadores estão no Endpoint 2), escolha Add (Adicionar). Em This IP address or subnet field (Este endereço IP ou campo de sub-rede), digite o bloco CIDR da VPC e escolha OK.

> **Important**
>
> Você precisa rolar para baixo na caixa de diálogo até localizar Which computers are in Endpoint 2 (Quais computadores estão no Endpoint 2). Não escolha Next (Próximo) até ter concluído esta etapa, caso contrário, não poderá se conectar ao servidor.



10. Confirme se todas as configurações especificadas estão corretas e escolha Next (Próximo).
11. Na página Método de Autenticação, selecione Avançado e escolha Personalizar.
12. Em First authentication methods (Primeiros métodos de autenticação), escolha Add (Adicionar).
13. Selecione Preshared key (Chave pré-compartilhada), insira o valor da chave pré-compartilhada do arquivo de configuração e escolha OK.

> **Important**
>
> Se você estiver repetindo este procedimento para o túnel 2, certifique-se de selecionar a chave pré-compartilhada para o túnel 2.

14. Certifique-se de que First authentication is optional não esteja selecionada e escolha OK.
15. Escolha Próximo.
16. Na página Perfil, marque todas as três caixas de seleção: Domínio, Privado e Público. Escolha Próximo.
17. Na página Name (Nome), digite um nome para a regra de conexão, por exemplo, `VPN to Tunnel 1` e escolha Finish (Concluir).

Repita o procedimento anterior especificando os dados para o túnel 2 de seu arquivo de configuração.

Assim que concluir, terá dois túneis configurados para sua conexão VPN.

Confirmar a configuração do túnel

Para confirmar a configuração do túnel

1. Abra o Server Manager, escolha Tools (Ferramentas), selecione Windows Firewall with Advanced Security (Firewall do Windows com segurança avançada) e Connection Security Rules (Regras de segurança de conexão).
2. Verifique o seguinte para os dois túneis:
   - Enabled (Habilitado) está como `Yes`
   - Endpoint 1 é o bloco CIDR para a rede
   - Endpoint 2 é o bloco CIDR da VPC
   - Authentication mode (Modo de autenticação) é `Require inbound and clear outbound`.
   - Authentication method (Método de autenticação) é `Custom`
   - Endpoint 1 port (Porta do endpoint 1) é `Any`
   - Endpoint 2 port (Porta do endpoint 2) é `Any`
   - Protocol (Protocolo) é `Any`
3. Selecione a primeira regra e escolha Properties (Propriedades).

4. Na guia Authentication (Autenticação) em Method (Método), escolha Customize (Personalizar). Verifique se a opção First authentication methods (Primeiros métodos de autenticação) contém a chave pré-compartilhada correta do arquivo de configuração para o túnel e escolha OK.
5. Na guia Avançado, verifique se Domínio, Privado e Público estão todos selecionados.
6. Em IPsec Tunelamento, escolha Personalizar. Verifique as configurações de IPsec tunelamento a seguir e escolha OK e OK novamente para fechar a caixa de diálogo.

   - Usar IPsec tunelamento está selecionado.
   - Local tunnel endpoint (closest to Endpoint 1) (Ponto de extremidade de túnel local (mais próximo ao Ponto de Extremidade 1)) contém o endereço IP do Windows Server. Se o dispositivo de gateway do cliente for uma instância do EC2, esse será o endereço IP privado da instância.
   - Remote tunnel endpoint (closest to Endpoint 2) (Ponto de extremidade de túnel remoto [mais próximo ao Ponto de Extremidade 2]) contém o endereço IP do gateway privado virtual para esse túnel.
7. Abra as propriedades para o segundo túnel. Repita as etapas 4 a 7 para esse túnel.

Habilitar segredo de encaminhamento perfeito da chave mestra

É possível habilitar o Perfect Forward Secrecy (PFS - Sigilo de encaminhamento perfeito) da chave mestra usando a linha de comando. Você não pode habilitar esse recurso usando a interface do usuário.

Para habilitar o Perfect Forward Secrecy (PFS - Sigilo de encaminhamento perfeito) da chave mestra

1. No Windows Server, abra uma nova janela do prompt de comando.
2. Insira o comando a seguir, substituindo `rule_name` pelo nome que você deu à primeira regra de conexão.

   ```
   netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
    QMSecMethods=ESP:SHA1-AES128+60min+100000kb
   ```
3. Repita a etapa 2 para o segundo túnel, desta vez substituindo `rule_name` pelo nome que você deu à segunda regra de conexão.

Configurar o firewall do Windows

Depois de configurar suas regras de segurança no servidor, defina algumas IPsec configurações básicas para trabalhar com o gateway privado virtual.

Para configurar o Firewall do Windows

1. Abra o Gerenciador do Servidor, escolha Tools (Ferramentas), selecione Windows Defender Firewall with Advanced Security (Firewall do Windows Defender com Segurança Avançada) e escolha Properties (Propriedades).
2. Na guia IPsec Configurações, em IPsecisenções, verifique se Isentar ICMP de IPsec é Não (padrão). Verifique se a autorização IPsec do túnel é Nenhuma.
3. Em IPsec padrões, escolha Personalizar.
4. Em Key exchange (Main Mode), selecione Advanced e Customize.
5. Em Customize Advanced Key Exchange Settings (Personalizar configurações de troca de chaves avançada), sob Security methods (Métodos de segurança), verifique se os seguintes valores padrão são usados para a primeira entrada:

   - Integridade: SHA-1
   - Criptografia: AES-CBC 128
   - Algoritmo de troca de chaves: Grupo Diffie-Hellman 2
   - Em Key lifetimes, verifique se Minutes está `480` e se Sessions está `0`.

   Essas configurações correspondem às seguintes entradas no arquivo de configuração:

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. Em Key exchange options, selecione Use Diffie-Hellman for enhanced security e escolha OK.
7. Em Data protection (Quick Mode), selecione Advanced e Customize.
8. Selecione Require encryption for all connection security rules that use these settings (Exigir criptografia para todas as regras de segurança de conexão que usam essas configurações).
9. Em Data integrity and encryption (Integridade e criptografia de dados), deixe os valores padrão:

   - Protocolo: ESP
   - Integridade: SHA-1

- Criptografia: AES-CBC 128
- Tempo de vida: 60 minutos

Esses valores correspondem à seguinte entrada no arquivo de configuração.

```
QuickModeSecMethods:
ESP:SHA1-AES128+60min+100000kb
```

10. Escolha OK para retornar à caixa de diálogo Personalizar IPsec configurações e escolha OK novamente para salvar a configuração.

Etapa 5: Habilitar a detecção de gateway inativo

Em seguida, configure o TCP para detectar quando um gateway fica indisponível. É possível fazer isso, modificando esta chave de registro: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. Não execute esta etapa enquanto não concluir as seções precedentes. Assim que alterar a chave de registro, deverá reinicializar o servidor.

Para habilitar a detecção de gateway inativo

1. No Windows Server, inicie o prompt de comando ou uma PowerShell sessão e digite regedit para iniciar o Editor do Registro.
2. Expanda HKEY_LOCAL_MACHINE, expanda SYSTEM, expanda, expanda Serviços, expanda Tcpip e CurrentControlSet, em seguida, expanda Parâmetros.
3. No menu Editar, selecione Novo e DWORD (32-bit) Value.
4. Insira o nome EnableDeadGWDetect.
5. Selecione EnableDeadGWDetecte escolha Editar, Modificar.
6. Em Value data (Dados de valor), digite 1 e escolha OK.
7. Feche o Registry Editor e reinicie o servidor.

Para obter mais informações, consulte EnableDeadGWDetectna Microsoft TechNet Library.

Etapa 6: Testar a conexão VPN

Para testar se a conexão VPN está funcionando corretamente, execute uma instância em sua VPC e garanta que ela não tenha uma conexão com a Internet. Assim que executar a instância, execute

ping no respectivo endereço IP privado no Windows Server. O túnel VPN é ativado quando tráfego é gerado no dispositivo de gateway do cliente. Portanto, o comando ping também inicia a conexão VPN.

Para obter as etapas para testar a conexão VPN, consulte Testar uma conexão com o AWS Site-to-Site VPN.

Se o comando `ping` falhar, verifique as seguintes informações:

- Confira se você configurou as regras de security group para permitir ICMP na instância de sua VPC. Se o seu Windows Server for uma instância do EC2, certifique-se de que as regras de saída do grupo de segurança permitam IPsec tráfego. Para obter mais informações, consulte Configurar a instância do Windows.
- Confirme se o sistema operacional da instância em que você está executando ping está configurada para responder a ICMP. Recomendamos que você use um dos Amazon Linux AMIs.
- Se a instância que você está fazendo ping for uma instância do Windows, conecte-se à instância e ative a entrada ICMPv4 no firewall do Windows.
- Verifique se configurou as tabelas de rota corretamente para a sua VPC ou sub-rede. Para obter mais informações, consulte Etapa 1: Criar uma conexão VPN e configurar a VPC.
- Se o dispositivo de gateway do cliente for uma instância do EC2, certifique-se de ter desativado a source/destination verificação da instância. Para obter mais informações, consulte Configurar a instância do Windows.

No console da Amazon VPC, na página VPN Connections, selecione sua conexão VPN. O primeiro túnel encontra-se no estado ATIVO. O segundo túnel deve ser configurado, mas ele somente será usado se o primeiro ficar inativo. Pode demorar alguns instantes para estabelecer os túneis criptografados.

Solução de problemas AWS Site-to-Site VPN do dispositivo de gateway do cliente

Ao solucionar problemas com o dispositivo de gateway do cliente, é importante ter uma abordagem estruturada. Os dois primeiros tópicos desta seção fornecem fluxogramas generalizados para solucionar problemas ao usar um dispositivo configurado para roteamento dinâmico (habilitado para BGP) e um dispositivo configurado para roteamento estático (sem BGP ativado), respectivamente.

A seguir esses tópicos, estão os guias de solução de problemas específicos do dispositivo para dispositivos de gateway do cliente Cisco, Juniper e Yamaha.

Além dos tópicos desta seção, habilitar o AWS Site-to-Site VPN troncos pode ser muito útil para solucionar problemas de conectividade VPN. Para obter instruções gerais de teste, consulte também Testar uma conexão com o AWS Site-to-Site VPN.

Tópicos

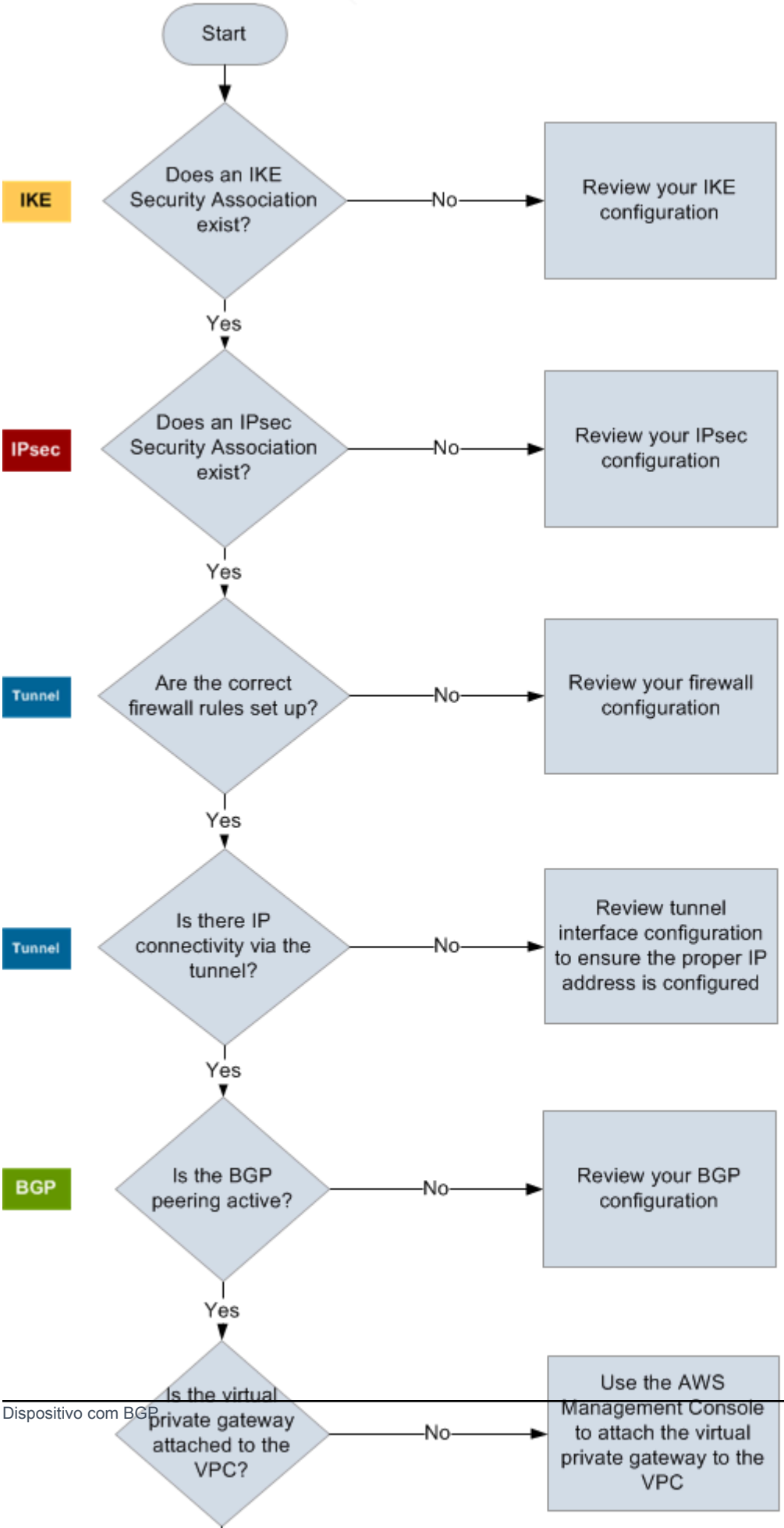
- Solucione problemas de AWS Site-to-Site VPN conectividade ao usar o Border Gateway Protocol
- Solucione problemas de AWS Site-to-Site VPN conectividade sem o Border Gateway Protocol
- Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco ASA Customer Gateway
- Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco IOS Customer Gateway
- Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco IOS Customer Gateway sem o Border Gateway Protocol
- Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Juniper JunOS Customer Gateway
- Solucione problemas de AWS Site-to-Site VPN conectividade com um dispositivo de gateway de cliente ScreenOS da Juniper
- Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Yamaha Customer Gateway

Recursos adicionais do

- Fórum da Amazon VPC

Solucione problemas de AWS Site-to-Site VPN conectividade ao usar o Border Gateway Protocol

O diagrama e a tabela a seguir fornecem instruções gerais para a solução de problemas de um dispositivo de gateway do cliente que usa o Protocolo de Gateway da Borda (BGP). Também recomendamos que você habilite os recursos de depuração do dispositivo. Consulte o fornecedor do dispositivo do gateway para obter informações detalhadas.

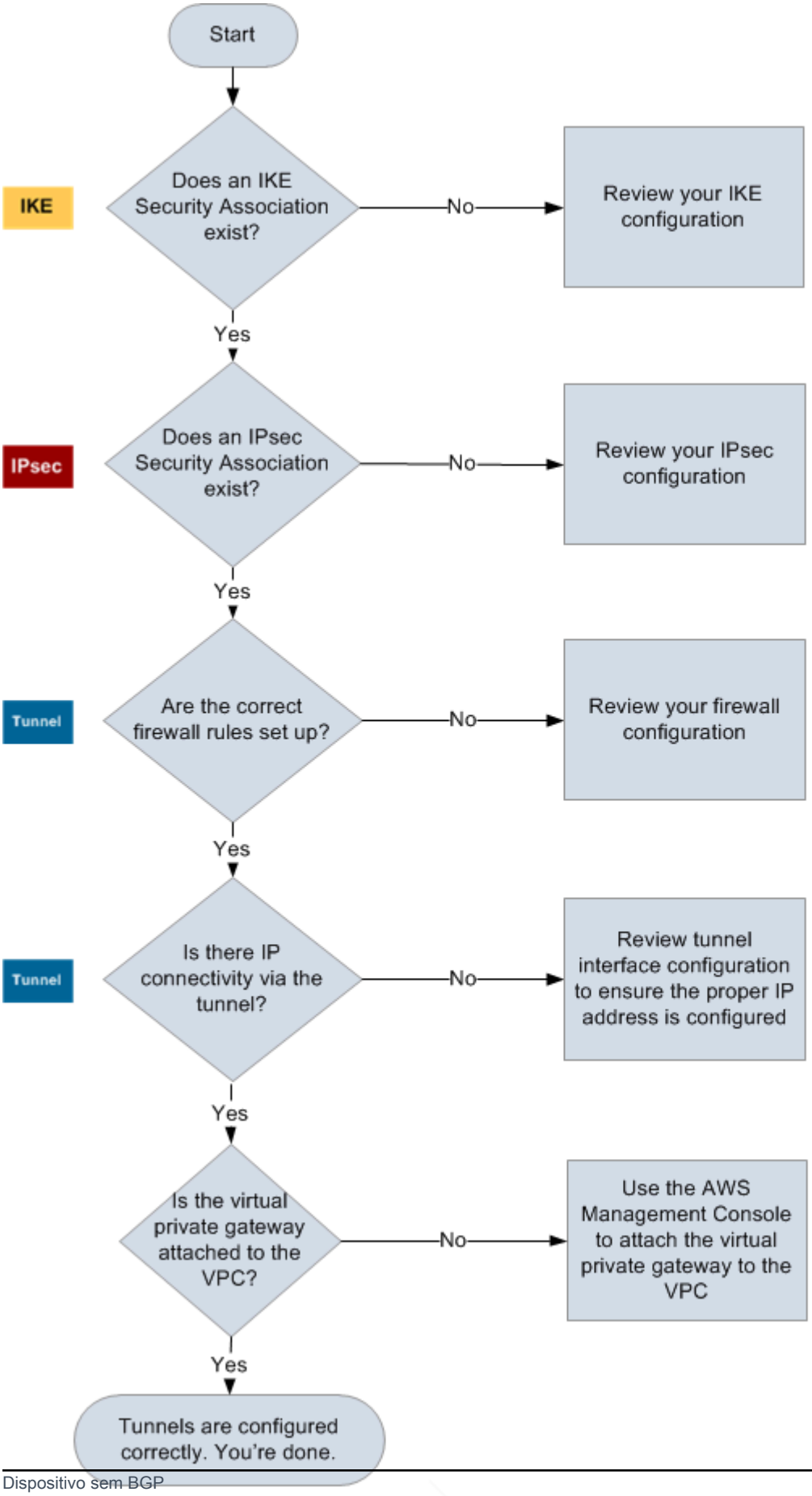

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	Determine se existe uma associação de segurança IKE. É necessária uma associação de segurança IKE para trocar as chaves usadas para estabelecer a associação IPsec de segurança. Se não houver nenhuma associação de segurança IKE, revise as definições de configuração de IKE. É necessário configurar os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração. Se existir uma associação de segurança IKE, vá para 'IPsec'.
IPsec	Determine se existe uma associação de IPsec segurança (SA). Um IPsec SA é o próprio túnel. Consulte seu dispositivo de gateway do cliente para determinar se um IPsec SA está ativo. Configure os parâmetros de criptogra fia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração. Se nenhum IPsec SA existir, revise sua IPsec configuração. Se existir um IPsec SA, vá para “Túnel”.
Túnel	Confirme se as regras necessárias de firewall estão configuradas (para obter uma lista de regras, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente). Se não, prossiga. Determine se existe conectividade IP por meio do túnel. Cada lado do túnel tem um endereço IP conforme especificado no arquivo de configuração. O endereço do gateway privado virtual é endereço usado como endereço de vizinho BGP. No dispositivo de gateway do cliente, execute ping nesse endereço para determinar se o tráfego de IP está sendo criptografado e descripto grafado adequadamente. Se o ping não tiver êxito, revise a configuração da interface do túnel para verificar se o endereço IP apropriado está configurado. Se o ping for bem-sucedido, prossiga para "BGP".

BGP	Determine se a sessão de emparelhamento de BGP está ativa. Para cada túnel, faça o seguinte: • No dispositivo de gateway do cliente, determine se o status do BGP é `Active` ou `Established` . Pode levar aproximadamente 30 segundos para uma sessão de BGP entre pares ficar ativa. • Confirme se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o gateway privado virtual. Se os túneis não estiverem nesse estado, revise a configuração do BGP. Se a sessão de BGP entre pares for estabelecida e você estiver recebendo um prefixo e anunciando um prefixo, isso quer dizer que o túnel está configurado corretamente. Certifique-se de que os dois túneis estão nesse estado.

Solucione problemas de AWS Site-to-Site VPN conectividade sem o Border Gateway Protocol

O diagrama e a tabela a seguir fornecem instruções gerais para a solução de problemas para um dispositivo de gateway do cliente que não usa o Protocolo de Gateway da Borda (BGP). Também recomendamos que você habilite os recursos de depuração do dispositivo. Consulte o fornecedor do dispositivo do gateway para obter informações detalhadas.


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	Determine se existe uma associação de segurança IKE. É necessária uma associação de segurança IKE para trocar as chaves usadas para estabelecer a associação IPsec de segurança. Se não houver nenhuma associação de segurança IKE, revise as definições de configuração de IKE. É necessário configurar os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração. Se existir uma associação de segurança IKE, vá para 'IPsec'.
IPsec	Determine se existe uma associação de IPsec segurança (SA). Um IPsec SA é o próprio túnel. Consulte seu dispositivo de gateway do cliente para determinar se um IPsec SA está ativo. Configure os parâmetros de criptogra fia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração. Se nenhum IPsec SA existir, revise sua IPsec configuração. Se existir um IPsec SA, vá para “Túnel”.
Túnel	Confirme se as regras necessárias de firewall estão configuradas (para obter uma lista de regras, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente). Se não, prossiga. Determine se existe conectividade IP por meio do túnel. Cada lado do túnel tem um endereço IP conforme especificado no arquivo de configuração. O endereço do gateway privado virtual é endereço usado como endereço de vizinho BGP. No dispositivo de gateway do cliente, execute ping nesse endereço para determinar se o tráfego de IP está sendo criptografado e descripto grafado adequadamente. Se o ping não tiver êxito, revise a configuração da interface do túnel para verificar se o endereço IP apropriado está configurado. Se o ping for bem-sucedido, avance para "Rotas estáticas".

Rotas estáticas	Para cada túnel, faça o seguinte: • Verifique se você adicionou uma rota estática ao CIDR da VPC com os túneis como o salto seguinte. • Verifique se você adicionou uma rota estática ao console da Amazon VPC a fim de informar o gateway privado virtual para rotear o tráfego de volta para as redes internas. Se os túneis não estiverem nesse estado, revise a configuração de seu dispositivo. Verifique se ambos os túneis estão nesse estado. Se sim, você terá terminado.

Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco ASA Customer Gateway

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway, considere o IKE e o roteamento. IPsec É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

> **Important**
>
> Alguns Cisco suportam ASAs apenas o Active/Standby modo. Quando você usa esses Cisco ASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo somente se o primeiro túnel ficar indisponível. O túnel em espera pode gerar o seguinte erro nos arquivos de log, o qual pode ser ignorado: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O valor de `state` deve ser `MM_ACTIVE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que o IKE não está configurado apropriadamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto isakmp
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

Para a interface de cada túnel, você deve ver `inbound esp sas` e `outbound esp sas`. Isso pressupõe que uma SA esteja listada (por exemplo,`spi: 0x48B456A6`) e que IPsec esteja configurada corretamente.

No Cisco ASA, o IPsec só aparece após o envio de tráfego interessante (tráfego que deve ser criptografado). Para manter sempre o IPsec ativo, recomendamos configurar um monitor de SLA. O monitor de SLA continua enviando tráfego interessante, mantendo o IPsec ativo.

Você também pode usar o seguinte comando ping para forçá-lo IPsec a iniciar a negociação e subir.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto ipsec
```

Roteamento

Execute ping na outra extremidade do túnel. Se isso estiver funcionando, você IPsec deve estar estabelecido. Se isso não estiver funcionando, verifique suas listas de acesso e consulte a IPsec seção anterior.

Se não conseguir acessar as instâncias, verifique as seguintes informações:

1. Verifique se a lista de acesso está configurada para permitir tráfego associado ao mapa de criptografia.

   É possível fazer isso usando o comando a seguir.

   ```
   ciscoasa# show run crypto
   ```

   ```
   crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
   crypto map VPN_crypto_map_name 1 match address access-list-name
   crypto map VPN_crypto_map_name 1 set pfs
   ```

```
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Verifique a lista de acesso usando o comando a seguir.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Verifique se a lista de acesso está correta. A lista de acesso de exemplo a seguir permite todo o tráfego interno para a sub-rede 10.0.0.0/16 da VPC.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Execute um traceroute a partir do dispositivo Cisco ASA para ver se ele alcança os roteadores Amazon (por exemplo,/). *AWS_ENDPOINT_1 AWS_ENDPOINT_2*

   Se conseguir acessar o roteador da Amazon, verifique as rotas estáticas adicionadas no console da Amazon VPC e os grupos de segurança para instâncias específicas.

5. Para solucionar outros problemas, revise a configuração.

Desabilitar e reabilitar a interface do túnel

Se o túnel parecer ativo, mas o tráfego não estiver fluindo adequadamente, desabilitar e reabilitar a interface do túnel geralmente pode resolver problemas de conectividade. Para desabilitar e reabilitar a interface do túnel em um Cisco ASA:

1. Execute o seguinte:

```
ciscoasa# conf t
ciscoasa(config)# interface tunnel X  (where X is your tunnel ID)
ciscoasa(config-if)# shutdown
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# end
```

   Como alternativa, você pode usar um comando de linha única:

```
ciscoasa# conf t ; interface tunnel X ; shutdown ; no shutdown ; end
```

2. Depois de desabilitar e reabilitar a interface, verifique se a conexão VPN foi restabelecida e se o tráfego agora está fluindo corretamente.

Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco IOS Customer Gateway

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway, considere quatro coisas: IKE IPsec, túnel e BGP. É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O `state` deve ser `QM_IDLE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que o IKE não está configurado apropriadamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto isakmp
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
```

```
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xF59A3FF6(4120526838)

     inbound esp sas:
      spi: 0xB6720137(3060924727)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

```
    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

Para a interface de cada túnel, você deve ver `inbound esp sas` e `outbound esp sas`. Supondo que um SA esteja `spi: 0xF95D2F3C` listado (por exemplo) e `Status` IPsec esteja `ACTIVE` configurado corretamente.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Use o comando a seguir para desativar a depuração.

```
router# no debug crypto ipsec
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter mais informações, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
```

```
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Verifique se o `line protocol` está em execução. Verifique se o endereço IP de origem, a interface de origem e o destino correspondem respectivamente à configuração do túnel para o endereço IP externo do dispositivo de gateway do cliente, à interface e ao endereço IP externo do gateway privado virtual. Verifique se o `Tunnel protection via IPSec` está presente. Execute o comando em ambas as interfaces do túnel. Para resolver qualquer problema, revise a configuração e verifique as conexões físicas com o dispositivo de gateway do cliente.

Além disso, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Você deve ver cinco pontos de exclamação.

Para solucionar outros problemas, revise a configuração.

BGP

Use o seguinte comando.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

Ambos os vizinhos deve ser listados. Para cada um, você deve ver um valor `State/PfxRcd` de `1`.

Se o emparelhamento de BGP estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para a VPC.

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

Além disso, confirme se você está recebendo o prefixo correspondente à sua VPC do gateway privado virtual.

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Para solucionar outros problemas, revise a configuração.

Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Cisco IOS Customer Gateway sem o Border Gateway Protocol

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway, considere três coisas: IKE e IPsec túnel. É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O `state` deve ser `QM_IDLE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que o IKE não está configurado apropriadamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto isakmp
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:
```

```
     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xF59A3FF6(4120526838)

     inbound esp sas:
      spi: 0xB6720137(3060924727)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE
```

```
    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

Para a interface de cada túnel, você deve ver `esp sas` de entrada e `esp sas` de saída. Isso pressupõe que um SA esteja listado (por exemplo,`spi: 0x48B456A6`), que o status seja `ACTIVE` e que IPsec esteja configurado corretamente.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto ipsec
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter mais informações, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Verifique se o protocolo de linha está em execução. Verifique se o endereço IP de origem, a interface de origem e o destino correspondem respectivamente à configuração do túnel para o endereço IP externo do dispositivo de gateway do cliente, à interface e ao endereço IP externo do gateway privado virtual. Verifique se o `Tunnel protection through IPSec` está presente. Execute o comando em ambas as interfaces do túnel. Para resolver qualquer problema, revise a configuração e verifique as conexões físicas com o dispositivo de gateway do cliente.

É possível também usar o comando a seguir e substituir `169.254.249.18` pelo endereço IP interno de seu gateway privado virtual.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Você deve ver cinco pontos de exclamação.

Roteamento

Para ver sua tabela de rotas estáticas, use o comando a seguir.

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Você verá que existe uma rota estática para o CIDR da VPC por meio de ambos os túneis. Se não houver, adicione as rotas estáticas conforme indicado a seguir.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Verificação do monitor de SLA

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
```

```
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

O valor para `Number of successes` indica se o monitor de SLA foi configurado com êxito.

Para solucionar outros problemas, revise a configuração.

Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Juniper JunOS Customer Gateway

Ao solucionar problemas de conectividade de um dispositivo de gateway de cliente da Juniper, considere quatro coisas: IKE IPsec, túnel e BGP. É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

Você deve ver uma ou mais linhas contendo um endereço remoto do gateway remoto especificado nos túneis. O `State` deve ser `UP`. A ausência de uma entrada, ou de qualquer entrada em outro estado (como `DOWN`), indica que o IKE não está configurado apropriadamente.

Para solucionar outros problemas, habilite as opções de rastreamento de IKE, conforme recomendado no arquivo de configuração de exemplo. Em seguida, execute o comando a seguir para imprimir na tela uma variedade de mensagens de depuração.

```
user@router> monitor start kmd
```

Em um host externo, é possível recuperar o arquivo de log completo com o comando a seguir.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway         Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

Mais especificamente, você deve ver pelo menos duas linhas por endereço de gateway (correspondentes ao gateway remoto). Os operadores maior e menor no início de cada linha (**< >**) indicam a direção do tráfego para a entrada específica. A saída tem linhas distintas para tráfego de entrada ("**<**", tráfego do gateway privado virtual para esse dispositivo de gateway do cliente) e tráfego de saída ("**>**").

Para solucionar outros problemas, habilite as opções de rastreamento de IKE (para obter mais informações, consulte a seção precedente sobre IKE).

Túnel

Primeiro, verifique novamente se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
user@router> show interfaces st0.1
```

```
 Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
    Input packets : 8719
```

```
    Output packets: 41841
    Security: Zone: Trust
    Allowed host-inbound traffic : bgp ping ssh traceroute
    Protocol inet, MTU: 9192
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
      Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Verifique se `Security: Zone` está correto e se o endereço `Local` corresponde ao túnel do dispositivo de gateway do cliente dentro do endereço.

Em seguida, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual. Os resultados devem ser semelhantes à resposta mostrada aqui.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Para solucionar outros problemas, revise a configuração.

BGP

Execute o seguinte comando.

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

Para solucionar outros problemas, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

Aqui você deve visualizar `Received prefixes` e `Advertised prefixes` listados com 1. Isso dever estar dentro da seção `Table inet.0`.

Se o `State` não for `Established`, verifique o `Last State` e o `Last Error` para obter detalhes sobre o que é necessário para corrigir o problema.

Se o emparelhamento de BGP estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para a VPC.

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

Além disso, verifique se você está recebendo o prefixo que corresponde à VPC do gateway privado virtual.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

Solucione problemas de AWS Site-to-Site VPN conectividade com um dispositivo de gateway de cliente ScreenOS da Juniper

Ao solucionar problemas de conectividade de um dispositivo de gateway de cliente baseado em ScreenOS da Juniper, considere quatro coisas: IKE IPsec, túnel e BGP. É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

IKE e IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
```

```
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

Você deve ver uma ou mais linhas contendo um endereço remoto do gateway remoto especificado nos túneis. O valor `Sta` deve ser `A/-` e o `SPI` deve ser um número hexadecimal diferente de `00000000`. As entradas em outros estados indicam que o IKE não está configurado apropriadamente.

Para solucionar outros problemas, habilite as opções de rastreamento de IKE (conforme recomendado no arquivo de configuração de exemplo).

Túnel

Primeiro, verifique novamente se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
```

```
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Verifique se `link:ready` está presente e se o endereço `IP` corresponde ao endereço interno do túnel do dispositivo de gateway do cliente.

Em seguida, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual. Os resultados devem ser semelhantes à resposta mostrada aqui.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Para solucionar outros problemas, revise a configuração.

BGP

Execute o comando a seguir.

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

O estado de ambos os peers de BGP deve ser `ESTABLISH`, o que significa que a conexão de BGP com o gateway privado virtual está ativa.

Para solucionar outros problemas, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Se o emparelhamento de BGP estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para a VPC. Esse comando aplica-se ao ScreenOS versão 6.2.0 e superior.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

Além disso, verifique se você está recebendo o prefixo correspondente à VPC do gateway privado virtual. Esse comando aplica-se ao ScreenOS versão 6.2.0 e superior.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

Solucionar problemas de AWS Site-to-Site VPN conectividade com um dispositivo Yamaha Customer Gateway

Ao solucionar problemas de conectividade de um dispositivo Yamaha Customer Gateway, considere quatro coisas: IKE IPsec, túnel e BGP. É possível solucionar problemas nessas áreas em qualquer sequência, mas é recomendável começar pelo IKE (na parte inferior da pilha de rede) e seguir em frente.

> **Note**
>
> A configuração `proxy ID` usada na fase 2 do IKE está desabilitada por padrão no roteador Yamaha. Isso pode causar problemas na conexão com a Site-to-Site VPN. Se o não `proxy ID` estiver configurado em seu roteador, consulte o exemplo de arquivo AWS de configuração fornecido para que a Yamaha defina corretamente.

IKE

Execute o comando a seguir. A resposta mostra um dispositivo de gateway do cliente com o IKE configurado corretamente.

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                    remote-id       # of sa
-------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

Você deve ver uma linha contendo um valor `remote-id` do gateway remoto especificado nos túneis. Você pode listar todas as associações de segurança (SAs) omitindo o número do túnel.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log de nível de DEPURAÇÃO que fornecem informações de diagnóstico.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Para cancelar os itens registrados, execute o comando a seguir.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Execute o comando a seguir. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
```

```
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
```

Para a interface de cada túnel, você deve ver `receive sas` e `send sas`.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Execute o comando a seguir para desabilitar a depuração.

```
# no ipsec ike log
# no syslog debug on
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte Regras de firewall para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Certifique-se de que o `current status` valor esteja on-line e `Interface type` pronto IPsec. Lembre-se de executar o comando em ambas as interfaces do túnel. Para solucionar qualquer problema aqui, revise a configuração.

BGP

Execute o comando a seguir.

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
```

```
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

Ambos os vizinhos deve ser listados. Para cada um, você deve ver um valor `BGP state` de `Active`.

Se o emparelhamento de BGP estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para a VPC.

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

Além disso, verifique se você está recebendo o prefixo correspondente à VPC do gateway privado virtual.

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

Integração entre AWS Site-to-Site VPN e eero

A AWS Site-to-Site VPN colaborou com a eero para tornar simples e conveniente que as organizações estabeleçam conectividade segura entre seus sites remotos e a AWS em apenas alguns cliques.

Essa solução aproveita os pontos de WiFi acesso e gateways de rede da eero para fornecer conectividade local. Usando os dispositivos de gateway e a Site-to-Site VPN da eero, os clientes podem estabelecer automaticamente a conectividade VPN para acessar seus aplicativos hospedados na AWS, como gateways de pagamento para sistemas de ponto de venda, com apenas alguns cliques. Isso torna mais simples e rápido para os clientes escalar a conectividade do site remoto em centenas de sites e elimina a necessidade de um técnico local com experiência em rede

para configurar a conectividade. Essa solução é adequada para empresas distribuídas com até 500 escritórios remotos, com cada escritório tendo até 100 usuários.

Para saber mais sobre essa integração, incluindo um guia de configuração detalhado, consulte a documentação do eero.

> **Note**
>
> Não há alterações na funcionalidade do AWS Site-to-Site VPN como parte dessa integração.

Considerações:

- Disponível somente para conexões VPN conectadas a um Transit Gateway ou à Cloud WAN. Não há suporte para anexos do Virtual Private Gateway.
- Túneis de 5 Gbps não são suportados.
- Site-to-Site O VPN Concentrator não é suportado.
- Site-to-Site As cotas de VPN não mudam com essa integração.

Trabalhe com AWS Site-to-Site VPN

Você pode trabalhar com recursos de Site-to-Site VPN usando o console Amazon VPC ou o.AWS CLI

Tópicos

Crie e gerencie AWS Site-to-Site VPN concentradores

Site-to-SiteOs concentradores VPN permitem que você agregue e gerencie várias conexões VPN de sites remotos, fornecendo gerenciamento centralizado.

Depois de criar seus concentradores de Site-to-Site VPN, você pode visualizá-los e gerenciá-los na página principal dos concentradores de Site-to-Site VPN no console da Amazon VPC. Esse painel exibe todos os concentradores de VPN ativos que gerenciam conexões seguras entre a AWS e seus sites remotos.

Tópicos

- Excluir um AWS Site-to-Site VPN concentrador

Crie um AWS Site-to-Site VPN concentrador

Crie um concentrador usando o console da Amazon VPC, APIs o ou o. AWS CLI Antes de criar um concentrador, você deve primeiro ter criado um gateway de trânsito para associar ao concentrador. Para obter mais informações sobre a criação de gateways de trânsito, consulte Criar um gateway de trânsito no Guia do Amazon AWS VPC Transit Gateway.

Crie um concentrador de Site-to-Site VPN usando o console

Para criar um Site-to-Site VPN Concentrator usando o AWS Management Console, siga estas etapas:

Para criar um Site-to-Site VPN Concentrator usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Concentrators.
3. Escolha Criar Site-to-Site VPN Concentrator.
4. (Opcional) Em Etiqueta de nome, insira um nome para seu Site-to-Site VPN Concentrator.
5. Para Transit Gateway, selecione um gateway de trânsito existente.
6. (Opcional) Adicione tags para ajudar a identificar e organizar seu Site-to-Site VPN Concentrator.
    a. Selecione Adicionar nova tag.
    b. Em Chave, insira uma chave de tag (por exemplo,**`Name`**).
    c. Em Valor, insira um valor de tag (por exemplo,**`Production-VPN-Concentrator`**).
    d. Repita as etapas anteriores para adicionar outras tags conforme necessário.
7. Escolha Criar Site-to-Site VPN Concentrator.

Após a criação, o Site-to-Site VPN Concentrator estará em um `pending` estado enquanto estiver sendo provisionado. Quando estiver pronto, o estado mudará para `available` e você poderá começar a criar conexões VPN que usam o Site-to-Site VPN Concentrator.

Crie um concentrador de Site-to-Site VPN usando a CLI

Antes de criar um Site-to-Site VPN Concentrator usando a CLI, verifique se você tem o seguinte:

- Um Transit Gateway existente em sua AWS conta
- Permissões apropriadas do IAM para criar Site-to-Site concentradores de VPN
- O ID do Transit Gateway ao qual você deseja conectar o concentrador

O exemplo a seguir cria um concentrador de Site-to-Site VPN para o gateway de trânsito especificado:

```
aws ec2 create-vpn-concentrator --transit-gateway-id tgw-123456789
```

O seguinte mostra uma resposta bem-sucedida:

```
{
    "VpnConcentrator": {
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "State": "pending",
        "TransitGatewayId": "tgw-123456789",
        "CreationTime": "2025-09-29T17:26:31.000Z",
        "Tags": []
    }
}
```

Crie um concentrador de Site-to-Site VPN usando a API

Você pode criar um concentrador de Site-to-Site VPN usando a CreateVpnConcentrators API.

A API aceita os seguintes parâmetros principais:

`TransitGatewayId`

O ID do Transit Gateway ao qual conectar o Site-to-Site VPN Concentrator.

`TagSpecification`

Tags a serem atribuídas ao Site-to-Site VPN Concentrator para organização e cobrança de recursos.

O exemplo a seguir mostra como criar um Site-to-Site VPN Concentrator conectado a um Transit Gateway:

```
POST / HTTP/1.1
```

```
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=...

Action=CreateVpnConcentrator
&Version=2016-11-15
&TransitGatewayId=tgw-0123456789abcdef0
&TagSpecification.1.ResourceType=vpn-concentrator
&TagSpecification.1.Tag.1.Key=Name
&TagSpecification.1.Tag.1.Value=MyVpnConcentrator
```

Após a criação bem-sucedida, a API retorna detalhes sobre o Site-to-Site VPN Concentrator recém-criado:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>12345678-1234-1234-1234-123456789012</requestId>
    <vpnConcentrator>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <state>pending</state>
        <transitGatewayId>tgw-0123456789abcdef0</transitGatewayId>
        <creationTime>2024-01-15T10:30:00.000Z</creationTime>
        <tagSet>
            <item>
                <key>Name</key>
                <value>MyVpnConcentrator</value>
            </item>
        </tagSet>
    </vpnConcentrator>
</CreateVpnConcentratorResponse>
```

Gerenciar AWS Site-to-Site VPN tags do concentrador

As tags são pares de valores-chave que ajudam você a organizar e gerenciar seus concentradores de Site-to-Site VPN. Você pode usar tags para categorizar os concentradores de Site-to-Site VPN por finalidade, ambiente, centro de custo ou qualquer outro critério que faça sentido para sua organização.

Gerenciar tags usando o console

Você pode adicionar ou excluir tags para um Site-to-Site VPN Concentrator usando o AWS Management Console.

Para adicionar tags a um concentrador de Site-to-Site VPN

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Concentrators.
3. Selecione o Site-to-Site VPN Concentrator que você deseja marcar.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Selecione Adicionar nova tag.
7. Em Chave, insira uma chave de tag (por exemplo,**`Environment`**).
8. Em Valor, insira um valor de tag (por exemplo,**`Production`**).
9. Escolha Salvar alterações.

Para excluir tags de um concentrador de Site-to-Site VPN

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Concentrators.
3. Selecione o Site-to-Site VPN Concentrator do qual você deseja remover as tags.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Para cada tag que você deseja remover, escolha Remover.
7. Escolha Salvar alterações.

Gerencie tags usando a CLI

Você pode adicionar, modificar ou remover tags usando AWS CLI o.

Adicionar tags.

O exemplo a seguir adiciona tags a um Site-to-Site VPN Concentrator:

```
aws ec2 create-tags --resources vcn-0123456789abcdef0 --tags
 Key=Environment,Value=Production Key=Team,Value=NetworkOps
```

Esse comando não retorna nenhuma saída em caso de sucesso.

Visualizar tags

O exemplo a seguir descreve as tags de um Site-to-Site VPN Concentrator:

```
aws ec2 describe-tags --filters "Name=resource-id,Values=vcn-0123456789abcdef0"
```

A resposta a seguir será retornada:

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "vcn-0123456789abcdef0",
            "ResourceType": "vpn-concentrator",
            "Value": "Production"
        },
        {
            "Key": "Team",
            "ResourceId": "vcn-0123456789abcdef0",
            "ResourceType": "vpn-concentrator",
            "Value": "NetworkOps"
        }
    ]
}
```

Remover marcações

O exemplo a seguir remove as tags de um Site-to-Site VPN Concentrator:

```
aws ec2 delete-tags --resources vcn-0123456789abcdef0 --tags Key=Environment Key=Team
```

Esse comando não retorna nenhuma saída em caso de sucesso.

Gerencie tags usando a API

Você pode gerenciar programaticamente as tags do Site-to-Site VPN Concentrator usando as operações de API da Amazon EC2 .

CreateTags

Use a `CreateTags` operação para adicionar ou atualizar tags:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
```

```
Content-Type: application/x-www-form-urlencoded

Action=CreateTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.1.Value=Production
&Tag.2.Key=Team
&Tag.2.Value=NetworkOps
&Version=2016-11-15
```

A resposta a seguir será retornada:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <return>true</return>
</CreateTagsResponse>
```

DescribeTags

Use a `DescribeTags` operação para recuperar as tags:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DescribeTags
&Filter.1.Name=resource-id
&Filter.1.Value.1=vcn-0123456789abcdef0
&Version=2016-11-15
```

A resposta a seguir será retornada:

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <tagSet>
        <item>
            <resourceId>vcn-0123456789abcdef0</resourceId>
            <resourceType>vpn-concentrator</resourceType>
            <key>Environment</key>
            <value>Production</value>
        </item>
```

```
        <item>
            <resourceId>vcn-0123456789abcdef0</resourceId>
            <resourceType>vpn-concentrator</resourceType>
            <key>Team</key>
            <value>NetworkOps</value>
        </item>
    </tagSet>
</DescribeTagsResponse>
```

DeleteTags

Use a `DeleteTags` operação para remover as tags:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.2.Key=Team
&Version=2016-11-15
```

A resposta a seguir será retornada:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <return>true</return>
</DeleteTagsResponse>
```

Excluir um AWS Site-to-Site VPN concentrador

Quando você não precisar mais de um Site-to-Site VPN Concentrator, poderá excluí-lo para parar de incorrer em cobranças. A exclusão de um Site-to-Site VPN Concentrator o remove permanentemente e todas as configurações associadas.

Pré-requisitos

Antes de excluir um Site-to-Site VPN Concentrator, verifique o seguinte:

- Todas as conexões VPN associadas ao Site-to-Site VPN Concentrator são excluídas.

- Você tem as permissões necessárias para excluir Site-to-Site VPN Concentrators (`ec2:DeleteVpnConcentrator`).

Exclua um Site-to-Site VPN Concentrator usando o console

Para excluir um Site-to-Site VPN Concentrator

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Concentradores site a site.
3. Selecione o Site-to-Site VPN Concentrator que você deseja excluir.
4. Escolha Ações e, em seguida, escolha Excluir Site-to-Site VPN Concentrator.
5. Na caixa de diálogo de confirmação, digite **`delete`** para confirmar a exclusão.
6. Escolha Excluir.

Exclua um Site-to-Site VPN Concentrator usando a CLI

Use o `delete-vpn-concentrator` comando para excluir um Site-to-Site VPN Concentrator. Você precisará do `vpn-concentrator-id` para excluí-lo.

O exemplo a seguir exclui um Site-to-Site VPN Concentrator:

```
aws ec2 delete-vpn-concentrator --vpn-concentrator-id vcn-0123456789abcdef0
```

A resposta a seguir será retornada:

```
{
    "VpnConcentrator": {
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "State": "deleting",
        "Message": "The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
 deleted and will be removed from your account."
    }
}
```

Exclua um concentrador de Site-to-Site VPN usando a API

Use a `DeleteVpnConcentrator` operação para excluir um Site-to-Site VPN Concentrator. Você precisará do `VpnConcentratorId` para excluí-lo.

O exemplo a seguir exclui um Site-to-Site VPN Concentrator:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteVpnConcentrator
&VpnConcentratorId=vcn-0123456789abcdef0
&Version=2016-11-15
```

A resposta a seguir será retornada:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <vpnConcentrator>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <state>deleting</state>
        <message>The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
 deleted and will be removed from your account.</message>
    </vpnConcentrator>
</DeleteVpnConcentratorResponse>
```

Crie uma AWS Site-to-Site VPN conexão

Você pode criar conexões Site-to-Site VPN que se conectam a gateways de trânsito ou redes globais Cloud WAN. Ambos os tipos de anexo oferecem suporte a IPv6 protocolos IPv4 e, opcionalmente, podem usar concentradores Site-to-Site VPN para conectar vários locais remotos de forma econômica.

Crie uma conexão VPN usando o console

Para criar uma conexão VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. (Opcional) Em Etiqueta de nome, insira um nome para a conexão. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.

5. Para o tipo de gateway de destino, escolha uma das seguintes opções:

   - Gateway privado virtual - Crie uma nova conexão VPN de gateway privado virtual escolhendo um gateway privado virtual existente.
   - Transit Gateway - Crie uma nova conexão VPN do Transit Gateway escolhendo um Transit Gateway existente. Para obter mais informações sobre como criar um gateway de trânsito, consulte Gateways de trânsito em Gateways de trânsito da Amazon VPC.
   - Site-to-Site VPN Concentrator - Crie uma nova conexão Site-to-Site VPN Concentrator usando um Site-to-Site VPN Concentrator existente ou criando um novo. Escolha uma das seguintes opções:
     - Existente - Crie uma nova conexão Site-to-Site VPN Concentrator usando um Concentrador existente.
     - Novo - Insira um nome opcional para o Site-to-Site VPN Concentrator e escolha o gateway de trânsito a ser associado a ele.
   - Não associada: crie uma conexão VPN independente que possa ser associada posteriormente à Cloud WAN por meio do console ou da API do Network Manager. Para obter mais informações sobre anexos VPN e Cloud WAN, consulte Anexos Site-to-site VPN na Cloud WAN no Guia do usuário da AWSAWS Cloud WAN.

6. Em Customer Gateway (Gateway do cliente), execute um dos procedimentos a seguir:

   - Para usar um gateway do cliente existente, escolha Existente, e selecione ID do gateway do cliente.
   - Para criar um novo gateway do cliente, escolha Novo e faça o seguinte:
     - Para o endereço IP, insira um endereço estático IPv4ou um IPv6endereço.
     - (Opcional) Em ARN do certificado, escolha o ARN do certificado privado (se estiver usando autenticação baseada em certificado).
     - Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente. Para obter mais informações, consulte Opções de gateway do cliente.

7. Em Opções de roteamento, escolha Dinâmico (requer BGP) ou Estático.

> **Note**
>
> As conexões VPN Cloud WAN e as conexões VPN usando concentradores oferecem suporte somente ao roteamento BGP. O roteamento estático não é suportado para esses tipos de conexão.

8. Em Armazenamento de chaves pré-compartilhadas, escolha Padrão ou Secrets Manager. A seleção predefinida é Padrão. Para obter mais informações sobre o uso de AWS Secrets Manager, consulte Segurança.
9. Para túnel dentro da versão IP, escolha IPv4ou IPv6.
10. (Opcional) Em Habilitar aceleração, marque a caixa de seleção para habilitar a aceleração. Para obter mais informações, consulte Conexões VPN aceleradas.

    Se você habilitar a aceleração, criaremos dois aceleradores que são usados pela sua conexão VPN. Aplicam-se cobranças adicionais do .
11. (Opcional) Dependendo da versão de IP interna do túnel escolhida, siga um destes procedimentos:

    - IPv4 — Para CIDR de IPv4 rede local, especifique o intervalo de IPv4 CIDR no lado do gateway do cliente (local) que tem permissão para se comunicar pelos túneis VPN. Para CIDR IPv4 de rede remota, escolha o intervalo CIDR no AWS lado que tem permissão para se comunicar por túneis VPN. O valor padrão para ambos os campo é `0.0.0.0/0`.
    - IPv6 — Para CIDR de IPv6 rede local, especifique o intervalo de IPv6 CIDR no lado do gateway do cliente (local) que tem permissão para se comunicar pelos túneis VPN. Para CIDR IPv6 de rede remota, escolha o intervalo CIDR no AWS lado que tem permissão para se comunicar por túneis VPN. O valor padrão para ambos os campo é `::/0`.
12. Em Tipo de endereço IP, escolha uma das seguintes opções:

    - Público IPv4 - (Padrão) Use IPv4 endereços para o túnel externo IPs.
    - Privado IPv4 - Use um IPv4 endereço privado para uso em redes privadas.
    - IPv6- Use IPv6 endereços para o túnel externo IPs. Essa opção exige que seu dispositivo de gateway do cliente ofereça suporte IPv6 ao endereçamento.

> **Note**
>
> Se você selecionar IPv6o tipo de endereço IP externo, deverá criar um gateway do cliente com um IPv6 endereço

13. (Opcional) Em Opções do túnel 1, é possível especificar as seguintes informações para cada túnel:
    - Um bloco IPv4 CIDR de tamanho /30 do `169.254.0.0/16` intervalo dos endereços internos do túnel IPv4 .
    - Se você especificou IPv6a versão IP do túnel interno, um bloco IPv6 CIDR /126 do `fd00::/8` intervalo dos endereços do túnel IPv6 interno.
    - A chave pré-compartilhada do IKE (PSK). As seguintes versões são suportadas: IKEv1 ou IKEv2.
    - Para editar as opções avançadas do túnel, escolha Editar opções de túnel. Para obter mais informações, consulte Opções de túnel VPN.
    - (Opcional) Escolha Habilitar para o registro de atividades do túnel para capturar mensagens de registro de IPsec atividades e mensagens do protocolo DPD.
    - (Opcional) Escolha Ativar em Ciclo de vida do endpoint de túnel para controlar o cronograma de substituições do endpoint. Para ter mais informações sobre o ciclo de vida de um endpoint de túnel, consulte Ciclo de vida do endpoint de túnel.
14. (Opcional) Escolha Opções do túnel 2 e siga as etapas anteriores para configurar um segundo túnel.
15. Escolha Create VPN Connection (Criar conexão VPN).

Crie uma conexão AWS Site-to-Site VPN de gateway de trânsito usando a CLI ou a API

Crie uma conexão VPN com o Transit Gateway usando a CLI

Use o create-vpn-connectioncomando e especifique o ID do gateway de trânsito para a `--transit-gateway-id` opção.

O exemplo a seguir demonstra a criação de uma conexão VPN com túnel IPv6 externo IPs e túnel IPv6 IPs interno:

```
aws ec2 create-vpn-connection \
--type ipsec.1 \
--transit-gateway-id tgw-12312312312312312 \
--customer-gateway-id cgw-001122334455aabbc \
--options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Exemplo de resposta:

```
{
    "VpnConnection": {
        "VpnConnectionId": "vpn-0abcdef1234567890",
        "State": "pending",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Type": "ipsec.1",
        "TransitGatewayId": "tgw-12312312312312312",
        "Category": "VPN",
        "Routes": [],
        "Options": {
            "StaticRoutesOnly": false,
            "OutsideIPAddressType": "Ipv6",
            "TunnelInsideIpVersion": "ipv6"
        }
    }
}
```

Crie uma conexão VPN com o Transit Gateway usando a API

Você pode criar uma conexão VPN usando a API do Amazon EC2. Esta seção fornece exemplos de mensagens de solicitação e resposta para criar uma conexão VPN de gateway de trânsito usando a API.

Pré-requisitos

Antes de criar uma conexão VPN usando a API, verifique se você tem:

- Um gateway de trânsito criado e disponível

- Um gateway de cliente configurado com os detalhes do seu dispositivo local

O exemplo a seguir mostra como criar uma conexão VPN usando a ação `CreateVpnConnection` da API:

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&TransitGatewayId=tgw-12345678901234567
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

Este exemplo cria uma conexão VPN com roteamento dinâmico (BGP) entre o gateway de trânsito especificado e o gateway do cliente.

Uma resposta bem-sucedida da API retorna os detalhes da conexão VPN:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <vpnConnection>
        <vpnConnectionId>vpn-1a2b3c4d5e6f78901</vpnConnectionId>
        <state>pending</state>
        <customerGatewayId>cgw-12345678901234567</customerGatewayId>
        <type>ipsec.1</type>
        <transitGatewayId>tgw-12345678901234567</transitGatewayId>
        <category>VPN</category>
        <options>
            <staticRoutesOnly>false</staticRoutesOnly>
        </options>
    </vpnConnection>
</CreateVpnConnectionResponse>
```

A resposta inclui o ID da conexão VPN, o estado atual e os detalhes da configuração. Inicialmente, a conexão estará em um estado “pendente” enquanto a AWS provisiona os túneis VPN.

Crie uma conexão AWS Site-to-Site VPN Cloud WAN usando a CLI ou a API

Você pode criar uma conexão Site-to-Site VPN entre sua WAN local e a AWS Cloud WAN seguindo o procedimento abaixo. Para obter mais informações, consulte Anexos de Site-to-site VPN na AWS Cloud WAN no Guia do usuário da AWS Cloud WAN.

Crie uma conexão VPN com o Cloud WAN usando a CLI

Use o create-vpn-connectioncomando para criar uma conexão VPN que será posteriormente conectada a uma rede global Cloud WAN. Isso cria uma conexão VPN não conectada que pode ser posteriormente associada ao Cloud WAN por meio do console ou da API do Network Manager.

Pré-requisitos

Antes de criar uma conexão VPN Cloud WAN, verifique se você tem o seguinte:

- `customer-gateway-id`- Um recurso de gateway do cliente existente (`cgw-xxxxxxxxx`) que representa seu dispositivo VPN local.
- Rede global de WAN em nuvem - Uma rede global de WAN em nuvem deve ser criada e configurada com segmentos de rede apropriados.
- Configuração BGP - As conexões VPN Cloud WAN exigem roteamento BGP; o roteamento estático não é suportado. Você deve definir `StaticRoutesOnly=false` no parâmetro options

Esse comando cria uma conexão VPN sem especificar um gateway de destino. A conexão estará em um estado independente e poderá ser associada posteriormente à sua rede global Cloud WAN por meio do console ou da API do Network Manager. A `StaticRoutesOnly=false` opção ativa o roteamento BGP, que é obrigatório para anexos do Cloud WAN VPN, pois o roteamento estático não é suportado.

O exemplo a seguir cria uma conexão VPN não conectada para o Cloud WAN:

```
aws ec2 create-vpn-connection \
            --type ipsec.1 \
            --customer-gateway-id cgw-0123456789abcdef0 \
            --options StaticRoutesOnly=false
```

A resposta retorna o seguinte:

```
{
            "VpnConnection": {
            "VpnConnectionId": "vpn-0abcdef1234567890",
            "State": "pending",
            "CustomerGatewayId": "cgw-0123456789abcdef0",
            "Type": "ipsec.1",
            "Category": "VPN",
            "Routes": [],
            "Options": {
            "StaticRoutesOnly": false
            }
            }
            }
```

Depois de criar a conexão VPN, você pode conectá-la à sua rede global Cloud WAN usando o console do Network Manager ou a chamada de `create-site-to-site-vpn-attachment` API.

Crie uma conexão VPN Cloud WAN usando a API

Você pode usar a API EC2 para criar uma conexão VPN para integração com o Cloud WAN. Isso envolve fazer uma chamada de `CreateVpnConnection` API que cria uma conexão VPN não conectada, que pode então ser associada à sua rede global Cloud WAN.

A solicitação da API cria uma conexão VPN sem especificar um gateway de destino, deixando-a em um estado independente, pronto para a integração com a Cloud WAN. A conexão usa o roteamento BGP, que é necessário para anexos do Cloud WAN VPN.

O exemplo a seguir mostra a solicitação HTTP para criar uma conexão Cloud WAN VPN:

```
POST / HTTP/1.1
            Host: ec2.us-east-1.amazonaws.com
            Content-Type: application/x-www-form-urlencoded
            Authorization: AWS4-HMAC-SHA256 Credential=...

            Action=CreateVpnConnection
            &Type=ipsec.1
            &CustomerGatewayId=cgw-0123456789abcdef0
            &Options.StaticRoutesOnly=false
            &Version=2016-11-15
```

A API retorna uma resposta bem-sucedida contendo os detalhes da conexão VPN. Inicialmente, a conexão estará em um `pending` estado enquanto AWS provisiona os túneis VPN, momento em que o status mudará para. `available`

```
<?xml version="1.0" encoding="UTF-8"?>
            <CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/
doc/2016-11-15/">
            <requestId>12345678-1234-1234-1234-123456789012</requestId>
            <vpnConnection>
            <vpnConnectionId>vpn-0abcdef1234567890</vpnConnectionId>
            <state>pending</state>
            <customerGatewayId>cgw-0123456789abcdef0</customerGatewayId>
            <type>ipsec.1</type>
            <category>VPN</category>
            <options>
            <staticRoutesOnly>false</staticRoutesOnly>
            </options>
            <vgwTelemetry/>
            <routes/>
            </vpnConnection>
            </CreateVpnConnectionResponse>
```

Detalhes da resposta

A resposta da API fornece as seguintes informações principais:

- vpnConnectionId- O identificador exclusivo da sua conexão VPN (por exemplo,`vpn-0abcdef1234567890`) que você usará para anexá-la à Cloud WAN
- estado — Inicialmente “pendente”, enquanto a AWS provisiona os túneis VPN e, em seguida, muda para “disponível” quando estiver pronta para ser anexada
- categoria - Mostra “VPN” indicando que esta é uma conexão VPN não conectada adequada para integração de Cloud WAN
- staticRoutesOnly- Defina como “false” para ativar o roteamento BGP, que é necessário para anexos do Cloud WAN VPN

Quando a conexão VPN atingir o estado “disponível”, você poderá conectá-la à sua rede global Cloud WAN usando a `CreateSiteToSiteVpnAttachment` API do Network Manager ou por meio do console da AWS.

Crie uma conexão AWS Site-to-Site VPN Concentrator usando a CLI ou a API

Crie uma conexão Site-to-Site VPN Concentrator usando a CLI

Depois de criar um Site-to-Site VPN Concentrator, você precisa estabelecer conexões VPN individuais de seus sites remotos com o Site-to-Site VPN Concentrator. Cada local remoto exige sua própria conexão VPN que faça referência ao ID do Site-to-Site VPN Concentrator. Isso permite que vários sites remotos compartilhem a mesma infraestrutura do Site-to-Site VPN Concentrator, mantendo túneis separados e seguros para cada local.

Para estabelecer uma conexão VPN usando um Site-to-Site VPN Concentrator, especifique o Site-to-Site VPN Concentrator em vez do gateway de trânsito ao criar a conexão VPN. O exemplo a seguir cria uma conexão VPN usando um Site-to-Site VPN Concentrator:

```
aws ec2 create-vpn-connection \
--type ipsec.1 \
--customer-gateway-id cgw-123456789 \
--vpn-concentrator-id vcn-0123456789abcdef0
```

Uma resposta bem-sucedida retorna o seguinte:

```
{
    "VpnConnection": {
        "VpnConnectionId": "vpn-0abcdef1234567890",
        "State": "pending",
        "CustomerGatewayId": "cgw-123456789",
        "Type": "ipsec.1",
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "Category": "VPN",
        "Routes": [],
        "Options": {
            "StaticRoutesOnly": false
        }
    }
}
```

Crie uma conexão Site-to-Site VPN Concentrator usando a API

Você pode criar uma conexão VPN que usa um concentrador de Site-to-Site VPN usando a API do Amazon EC2. Esta seção fornece exemplos de mensagens de solicitação e resposta para criar uma conexão VPN com um Site-to-Site VPN Concentrator.

Antes de criar uma conexão VPN com um Site-to-Site VPN Concentrator usando a API, certifique-se de ter:

- Um concentrador de Site-to-Site VPN criado e disponível
- Um gateway de cliente configurado para seu local remoto
- Configuração de rede que permite IPsec tráfego entre seu site e a AWS

O exemplo a seguir mostra como criar uma conexão VPN usando um Site-to-Site VPN Concentrator com a ação da `CreateVpnConnection` API:

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&VpnConcentratorId=vcn-0123456789abcdef0
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

Este exemplo cria uma conexão VPN entre o Site-to-Site VPN Concentrator especificado e o gateway do cliente. O Site-to-Site VPN Concentrator atua como um terminal AWS lateral, permitindo que vários sites remotos se conectem por meio de um hub centralizado.

Uma resposta de API bem-sucedida retorna os detalhes da conexão VPN com as informações do Site-to-Site VPN Concentrator:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>8b73d60f-458f-5gc5-a442-7f9fEXAMPLE</requestId>
    <vpnConnection>
```

```
        <vpnConnectionId>vpn-9z8y7x6w5v4u32109</vpnConnectionId>
        <state>pending</state>
        <customerGatewayId>cgw-12345678901234567</customerGatewayId>
        <type>ipsec.1</type>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <category>VPN</category>
        <options>
            <staticRoutesOnly>false</staticRoutesOnly>
        </options>
    </vpnConnection>
</CreateVpnConnectionResponse>
```

A resposta inclui a ID da conexão VPN e faz referência à Site-to-Site VPN Concentrator ID em vez de uma ID de gateway de trânsito. Essa conexão permite que seu site remoto se comunique com outros sites conectados ao mesmo Site-to-Site VPN Concentrator, habilitando topologias de hub-and-spoke rede.

Exibir AWS Site-to-Site VPN conexões

Exibir conexões VPN usando o console

Você pode visualizar suas conexões VPN e seus detalhes usando o AWS Management Console. Isso fornece uma interface visual para monitorar o status da conexão, a integridade do túnel e os detalhes da configuração.

Para visualizar conexões VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Connections (Conexões VPN).
3. Selecione sua conexão VPN para ver informações detalhadas, incluindo:
    - Estado e status da conexão
    - Detalhes do túnel e estado de saúde
    - Informações sobre a rota
    - Parâmetros de configuração

O console exibe informações de status em tempo real e permite monitorar a conectividade do túnel, visualizar tabelas de roteamento e acessar detalhes de configuração para solucionar problemas.

Visualize conexões VPN usando a CLI

Use a AWS CLI para consultar e recuperar informações detalhadas sobre suas conexões VPN de forma programática. Esse método permite automação, criação de scripts e integração com ferramentas de monitoramento.

Para consultar todas as conexões VPN em sua conta e região atuais da AWS, execute o `describe-vpn-connections` comando sem parâmetros. No entanto, se você quiser ver os detalhes sobre uma conexão VPN específica, precisará saber o ID da conexão VPN.

Para recuperar informações detalhadas de uma conexão VPN específica, especifique o ID da conexão como parâmetro. O exemplo a seguir mostra uma solicitação para ver detalhes sobre uma conexão VPN específica.

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1234567890abcdef0
```

A resposta inclui informações abrangentes sobre a conexão VPN, incluindo opções de túnel, detalhes de roteamento e status atual.

- `State`- O estado atual da conexão VPN
- `TunnelOptions`- Configuração e status de cada túnel
- `OutsideIpAddress`- Os endereços IP públicos dos túneis VPN
- `Routes`- Informações de roteamento para a conexão

Exemplo de trecho de resposta mostrando os principais detalhes da conexão:

```
{
    "VpnConnections": [
        {
            "VpnConnectionId": "vpn-1234567890abcdef0",
            "State": "available",
            "CustomerGatewayId": "cgw-1234567890abcdef0",
            "Type": "ipsec.1",
            "Options": {
                "StaticRoutesOnly": false,
                "TunnelOptions": [
                    {
                        "OutsideIpAddress": "203.0.113.12",
                        "TunnelInsideCidr": "169.254.10.0/30",
```

```
                        "PreSharedKey": "example_key_1234567890abcdef0",
                        "Phase1LifetimeSeconds": 28800,
                        "Phase2LifetimeSeconds": 3600
                    },
                    {
                        "OutsideIpAddress": "203.0.113.34",
                        "TunnelInsideCidr": "169.254.11.0/30",
                        "PreSharedKey": "example_key_0987654321fedcba0",
                        "Phase1LifetimeSeconds": 28800,
                        "Phase2LifetimeSeconds": 3600
                    }
                ]
            }
        }
    ]
}
```

Visualize conexões VPN usando a API

Faça chamadas diretas de API para o EC2 serviço da Amazon para recuperar informações de conexão VPN. Essa abordagem fornece flexibilidade máxima para aplicativos personalizados e integrações programáticas.

A ação `DescribeVpnConnections` da API consulta e retorna informações detalhadas sobre uma ou mais conexões VPN. Você pode aplicar filtros por ID de conexão, estado ou outros atributos para restringir seus resultados.

Veja a seguir um exemplo de solicitação para fornecer detalhes sobre uma única conexão VPN.

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20230101/us-east-1/ec2/
aws4_request, SignedHeaders=host;x-amz-date, Signature=example_signature

Action=DescribeVpnConnections
&VpnConnectionId.1=vpn-1234567890abcdef0
&Version=2016-11-15
```

A resposta retorna detalhes sobre essa conexão VPN.

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeVpnConnectionsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>12345678-1234-1234-1234-123456789012</requestId>
    <vpnConnectionSet>
        <item>
            <vpnConnectionId>vpn-1234567890abcdef0</vpnConnectionId>
            <state>available</state>
            <customerGatewayId>cgw-1234567890abcdef0</customerGatewayId>
            <type>ipsec.1</type>
            <options>
                <staticRoutesOnly>false</staticRoutesOnly>
                <tunnelOptionSet>
                    <item>
                        <outsideIpAddress>203.0.113.12</outsideIpAddress>
                        <tunnelInsideCidr>169.254.10.0/30</tunnelInsideCidr>
                        <preSharedKey>example_key_1234567890abcdef0</preSharedKey>
                    </item>
                    <item>
                        <outsideIpAddress>203.0.113.34</outsideIpAddress>
                        <tunnelInsideCidr>169.254.11.0/30</tunnelInsideCidr>
                        <preSharedKey>example_key_0987654321fedcba0</preSharedKey>
                    </item>
                </tunnelOptionSet>
            </options>
        </item>
    </vpnConnectionSet>
</DescribeVpnConnectionsResponse>
```

Testar uma conexão com o AWS Site-to-Site VPN

Após criar a conexão AWS Site-to-Site VPN e configurar o gateway do cliente, você pode executar uma instância e testar a conexão executando um ping na instância.

Antes de começar, certifique-se do seguinte:

- Use uma AMI que responda a solicitações de ping. Recomendamos que você use uma das Amazon Linux AMIs.

- Configure qualquer grupo de segurança ou network ACL na VPC que filtre o tráfego para a instância para permitir o tráfego ICMP de entrada e de saída. Isso permite que a instância receba solicitações `ping`.
- Caso as instâncias executem o Windows Server, conecte-se à instância e permita o ICMPv4 de entrada no firewall do Windows para que o ping seja executado na instância.
- (Roteamento estático) Certifique-se de que o dispositivo de gateway do cliente tenha uma rota estática para a VPC e que a conexão VPN tenha uma rota estática para que o tráfego possa retornar ao dispositivo de gateway do cliente.
- (Roteamento dinâmico) Certifique-se de que o status BGP no dispositivo de gateway do cliente esteja estabelecido. Leva cerca de 30 segundos para que a sessão de emparelhamento de BGP seja estabelecida. Verifique se as rotas estão anunciadas com BGP corretamente e à mostra na tabela de rotas da sub-rede de modo que o tráfego possa voltar ao gateway do cliente. Verifique se os dois túneis estão configurados com roteamento BGP.
- Verifique se você configurou o roteamento nas tabelas de rotas da sub-rede para a conexão VPN.

Como testar a conectividade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. (Opcional) Em Nome, insira um nome descritivo para a instância.
4. Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Início rápido e, depois, escolha o sistema operacional da instância.
5. Em Nome do par de chaves, escolha um par de chaves existente ou crie outro.
6. Em Configurações de rede, escolha Selecionar grupo de segurança existente e, depois, escolha o grupo de segurança que você configurou.
7. No painel Resumo painel, escolha Iniciar instância.
8. Depois que a instância estiver em execução, obtenha o endereço IP privado (por exemplo, 10.0.0.4). O console do Amazon EC2 exibe o endereço como parte dos detalhes da instância.
9. Em um computador na rede que esteja por trás do gateway do cliente, use o comando ping com o endereço IP privado da instância.

   ```
   ping 10.0.0.4
   ```

   Uma resposta bem-sucedida assemelha-se ao seguinte.

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Para testar o failover de túnel, é possível desabilitar temporariamente um dos túneis no dispositivo de gateway do cliente e repetir esta etapa. Não é possível desabilitar um túnel no lado da AWS da conexão VPN.

10. Para testar a conexão da AWS com sua rede on-premises, você pode usar SSH ou RDP para se conectar à instância pela rede. Depois, é possível executar o comando `ping` com o endereço IP privado de outro computador na rede, para verificar se ambos os lados da conexão podem iniciar e receber solicitações.

    Para obter mais informações sobre como se conectar a uma instância do Linux, consulte Conectar-se à instância do Linux no Guia do usuário do Amazon EC2. Para obter mais informações sobre como se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows no Guia do usuário do Amazon EC2.

Excluir uma conexão do AWS Site-to-Site VPN e um gateway

É possível excluir uma conexão AWS Site-to-Site VPN caso não precise mais dela. Quando você exclui uma conexão da Site-to-Site VPN, não excluímos o gateway do cliente ou o gateway privado virtual associado à conexão da Site-to-Site VPN. Se você não precisar mais do gateway do cliente e do gateway privado virtual, poderá excluí-los.

> **Warning**
>
> Se você excluir a conexão da Site-to-Site VPN e criar outra, será necessário baixar um novo arquivo de configuração e reconfigurar o dispositivo de gateway do cliente.

Tarefas

- Exclusão de uma conexão do AWS Site-to-Site VPN
- Excluir um gateway do cliente do AWS Site-to-Site VPN
- Desanexar e excluir um gateway privado virtual no AWS Site-to-Site VPN

Exclusão de uma conexão do AWS Site-to-Site VPN

Depois de excluir a conexão da Site-to-Site VPN, ela permanece visível por um curto período com um estado de `deleted` e, depois, a entrada é removida automaticamente.

Para excluir uma conexão VPN usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Ações, Excluir conexão VPN.
4. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para excluir uma conexão VPN usando a linha de comando ou a API

- DeleteVpnConnection (API de consulta do Amazon EC2)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Excluir um gateway do cliente do AWS Site-to-Site VPN

Caso não precise mais de um gateway do cliente, é possível excluí-lo. Não é possível excluir um gateway do cliente que está sendo usado em uma conexão da Site-to-Site VPN.

Para excluir um gateway do cliente usando o console

1. No painel de navegação, escolha Gateways do cliente.
2. Selecione o gateway do cliente e escolha Ações, Excluir gateway do cliente.
3. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para excluir um gateway do cliente usando a linha de comando ou a API

- DeleteCustomerGateway (API de consulta do Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Desanexar e excluir um gateway privado virtual no AWS Site-to-Site VPN

Caso não precise mais de um gateway privado virtual para a VPC, desanexe-o dela.

Para desanexar um gateway privado virtual usando o console

1. No painel de navegação, escolha Gateways privados virtuais.
2. Selecione o gateway privado virtual e escolha Actions, Detach from VPC.
3. Escolha Desanexar gateway privado virtual.

Caso não precise mais de um gateway privado virtual desanexado, exclua-o. Não é possível excluir um gateway privado virtual que ainda esteja anexado à VPC. Depois de excluir o gateway privado virtual, ele permanecerá visível por um breve período com um estado de `deleted` e, em seguida, a entrada é removida automaticamente.

Para excluir um gateway privado virtual usando o console

1. No painel de navegação, escolha Gateways privados virtuais.
2. Selecione o gateway privado virtual e escolha Ações, Excluir gateway privado virtual.
3. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para desanexar um gateway privado virtual usando a linha de comando ou a API

- DetachVpnGateway (API de consulta do Amazon EC2)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para excluir um gateway privado virtual usando a linha de comando ou a API

- DeleteVpnGateway (API de consulta do Amazon EC2)

- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modificar o gateway de destino de uma AWS Site-to-Site VPN conexão

Você pode modificar o gateway de destino de uma AWS Site-to-Site VPN conexão. As seguintes opções de migração estão disponíveis:

- Um gateway privado virtual existente para um gateway de trânsito
- Um gateway privado virtual existente para outro gateway privado virtual
- Um gateway de trânsito existente para outro gateway de trânsito
- Um gateway de trânsito existente para um gateway privado virtual

Depois de modificar o gateway de destino, sua conexão Site-to-Site VPN ficará temporariamente indisponível por um breve período enquanto provisionamos os novos endpoints.

As tarefas a seguir ajudam você a concluir a migração para um novo gateway.

Tarefas

- Etapa 1: Criar o gateway de destino
- Etapa 2: excluir as rotas estáticas (condicional)
- Etapa 3: Migrar para um novo gateway
- Etapa 4: Atualizar tabelas de rotas da VPC
- Etapa 5: Atualizar o roteamento do gateway de destino (condicional)
- Etapa 6: atualizar o ASN do gateway do cliente (condicional)

Etapa 1: Criar o gateway de destino

Antes de realizar a migração para o novo gateway, é necessário configurá-lo. Para obter informações sobre como adicionar um gateway privado virtual, consulte the section called “Criar um gateway privado virtual”. Para obter mais informações sobre como adicionar um gateway de trânsito, consulte Criar um gateway de trânsito em Gateways de trânsito da Amazon VPC.

Se o novo gateway de destino for um gateway de trânsito, conecte-o VPCs ao gateway de trânsito. Para obter informações sobre anexos de VPC, consulte Anexos do gateway de trânsito de uma VPC em Gateways de trânsito da Amazon VPC.

Ao modificar o destino de um gateway privado virtual para um gateway de trânsito, você pode, opcionalmente, definir o ASN do gateway de trânsito para ter o mesmo valor que o ASN do gateway privado virtual. Se você optar por ter um ASN diferente, deverá definir o ASN no dispositivo gateway do cliente como o ASN do gateway de trânsito. Para obter mais informações, consulte the section called “Etapa 6: atualizar o ASN do gateway do cliente (condicional)”.

Etapa 2: excluir as rotas estáticas (condicional)

Esta etapa é necessária quando você migra de um gateway privado virtual com rotas estáticas para um gateway de trânsito.

É necessário excluir as rotas estáticas antes de migrar para o novo gateway.

> **Tip**
>
> Mantenha uma cópia da rota estática antes de excluí-la. Você precisará adicionar novamente essas rotas ao gateway de trânsito depois que a migração da conexão VPN for concluída.

Para excluir uma rota da tabela

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Rotas, escolha Editar rotas.
4. Escolha Remover para a rota estática do gateway privado virtual.
5. Escolha Salvar alterações.

Etapa 3: Migrar para um novo gateway

Como alterar o gateway de destino

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão VPN e escolha Ações, Modificar conexão VPN.

4. Em Tipo de destino, escolha o tipo de gateway.
    a. Se o novo gateway de destino for um gateway privado virtual, escolha Gateway VPN.
    b. Se o novo gateway de destino for um gateway de trânsito, escolha Gateway de trânsito.
5. Escolha Salvar alterações.

Para modificar uma conexão Site-to-Site VPN usando a linha de comando ou a API

- ModifyVpnConnection(API de consulta do Amazon EC2)
- modify-vpn-connection (AWS CLI)

Etapa 4: Atualizar tabelas de rotas da VPC

Depois de migrar para o novo gateway, talvez seja necessário modificar a tabela de rotas da VPC. Para obter mais informações, consulte Tabelas de rotas no Guia do usuário da Amazon VPC.

A tabela a seguir fornece informações sobre as atualizações da tabela de rotas da VPC a serem feitas após modificar o destino do gateway VPN.

Gateway existente	Novo gateway	Alteração de tabela de rotas da VPC
Gateway privado virtual com rotas propagadas	Transit gateway	Adicione uma rota que contenha o ID do gateway de trânsito.
Gateway privado virtual com rotas propagadas	Gateway privado virtual com rotas propagadas	Nenhuma ação é necessária.
Gateway privado virtual com rotas propagadas	Gateway privado virtual com rota estática	Adicione uma rota que contenha o ID do novo gateway privado virtual.
Gateway privado virtual com rotas estáticas	Transit gateway	Atualize a rota que contém o ID do gateway privado virtual para o ID do gateway de trânsito.

Gateway existente	Novo gateway	Alteração de tabela de rotas da VPC
Gateway privado virtual com rotas estáticas	Gateway privado virtual com rotas estáticas	Atualize a rota que contém o ID do gateway privado virtual para o ID do novo gateway privado virtual.
Gateway privado virtual com rotas estáticas	Gateway privado virtual com rotas propagadas	Exclua a rota que contém o ID do gateway privado virtual.
Transit gateway	Gateway privado virtual com rotas estáticas	Atualize a rota que contém o ID do gateway de trânsito para o ID do gateway privado virtual.
Transit gateway	Gateway privado virtual com rotas propagadas	Exclua a rota que contém o ID de gateway de trânsito.
Transit gateway	Transit gateway	Atualize a rota que contém o ID do gateway de trânsito para o ID do novo gateway de trânsito.

Etapa 5: Atualizar o roteamento do gateway de destino (condicional)

Quando o novo gateway for um gateway de trânsito, modifique a tabela de rotas do gateway de trânsito para permitir o tráfego entre a VPC e a Site-to-Site VPN. Para obter mais informações, consulte Tabelas de rota de Transit gateway em Amazon VPC Transit Gateway.

Se você tiver excluído rotas estáticas de VPN, deverá adicionar essas rotas estáticas à tabela de rotas do gateway de trânsito.

Ao contrário de um gateway privado virtual, um gateway de trânsito define o mesmo valor para o discriminador de várias saídas (MED) em todos os túneis em um anexo da VPN. Se você está migrando de um gateway privado virtual para um gateway de trânsito e baseou-se no valor MED para seleção de túnel, recomendamos que faça alterações de roteamento para evitar problemas de

conexão. Por exemplo, você pode anunciar rotas mais específicas em seu gateway de trânsito. Para obter mais informações, consulte Tabelas de rotas e prioridade de AWS Site-to-Site VPN rotas.

Etapa 6: atualizar o ASN do gateway do cliente (condicional)

Quando o novo gateway tiver um ASN diferente do gateway antigo, atualize o ASN no dispositivo de gateway do cliente para apontar para o novo ASN. Consulte Opções de gateway do cliente para sua conexão AWS Site-to-Site VPN para obter mais informações.

Modificar opções da conexão do AWS Site-to-Site VPN

É possível modificar as opções de conexão para sua conexão da Site-to-Site VPN. É possível modificar as opções a seguir:

- Os intervalos CIDR IPv4 no lado local (gateway do cliente) e no lado remoto (AWS) da conexão VPN que pode se comunicar pelos túneis da VPN. O padrão é `0.0.0.0/0` para ambos os intervalos.
- Os intervalos CIDR IPv6 no lado local (gateway do cliente) e no lado remoto (AWS) da conexão VPN que pode se comunicar pelos túneis da VPN. O padrão é `::/0` para ambos os intervalos.

Quando você modifica as opções de conexão VPN, os endereços IP do endpoint da VPN no lado da AWS não são alterados e as opções de túnel não são alteradas. A conexão VPN ficará temporariamente indisponível enquanto a conexão VPN for atualizada.

Como modificar as opções de conexão VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Ações, Modificar opções de conexão VPN.
4. Insira novos intervalos de CIDR, conforme necessário.
5. Escolha Salvar alterações.

Como modificar as opções de conexão VPN usando a linha de comando ou a API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions (API de consulta do Amazon EC2)

Modificar opções de túnel de AWS Site-to-Site VPN

É possível modificar as opções dos túneis VPN em sua conexão da Site-to-Site VPN. É possível modificar um túnel VPN de cada vez.

> **Important**
>
> Quando você modifica um túnel VPN, a conectividade pelo túnel é interrompida por até vários minutos. Planeje o tempo de inatividade esperado.

Como modificar as opções de túnel VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão da Site-to-Site VPN e escolha Ações, Modificar opções de túnel VPN.
4. Em Endereço IP externo do túnel VPN, escolha o IP do endpoint do túnel VPN.
5. Escolha ou insira novos valores para as opções de túnel, conforme necessário. Para obter mais informações sobre as opções de túnel, consulte Opções de túnel VPN.

   > **Note**
   >
   > Algumas opções de túnel têm vários valores padrão. Clique para remover qualquer valor padrão. Esse valor padrão é então removido da opção de túnel.

6. Escolha Salvar alterações.

Como modificar as opções de túnel VPN usando a linha de comando ou a API

- (AWS CLI) Use describe-vpn-connections para visualizar as opções de túnel atuais e modify-vpn-tunnel-options para modificar as opções de túnel.
- (API de consulta do Amazon EC2) Use DescribeVpnConnections para visualizar as opções de túnel atuais e ModifyVpnTunnelOptions para modificar as opções de túnel.

Editar rotas estáticas para uma conexão do AWS Site-to-Site VPN

Para uma conexão da Site-to-Site VPN em um gateway privado virtual configurado para roteamento estático, você pode adicionar ou remover as rotas estáticas da configuração de VPN.

Como adicionar ou remover uma rota estática usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN.
4. Escolha Editar rotas estáticas.
5. Adicione ou remova rotas, conforme necessário.
6. Escolha Salvar alterações.
7. Se a propagação da rota não estiver habilitada para a tabela de rotas, será preciso atualizar as rotas manualmente na tabela de rotas para, assim, refletir os prefixos IP estáticos atualizados na conexão VPN. Para obter mais informações, consulte (Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas.
8. Para uma conexão VPN em um gateway de trânsito, você adiciona, modifica ou remove as rotas estáticas na tabela de rotas do gateway de trânsito. Para obter mais informações, consulte Tabelas de rota de Transit gateway em Amazon VPC Transit Gateway.

Para adicionar uma rota estática usando a linha de comando ou a API

- CreateVpnConnectionRoute (API de consulta do Amazon EC2)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Para excluir uma rota estática usando a linha de comando ou a API

- DeleteVpnConnectionRoute (API de consulta do Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Alterar o gateway do cliente para uma conexão do AWS Site-to-Site VPN

É possível alterar o gateway do cliente da sua conexão da Site-to-Site VPN usando o console da Amazon VPC ou uma ferramenta de linha de comando.

Depois de alterar o gateway do cliente, a conexão VPN ficará indisponível durante um breve período enquanto provisionamos os novos endpoints.

Como alterar o gateway do cliente usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN.
4. Escolha Ações, Modificar conexão VPN.
5. Em Tipo de destino, escolha Gateway do cliente.
6. Em Gateway do cliente de destino, escolha o novo gateway do cliente.
7. Escolha Salvar alterações.

Como excluir um gateway do cliente usando a linha de comando ou a API

- ModifyVpnConnection (API de consulta do Amazon EC2)
- modify-vpn-connection (AWS CLI)

Substitua credenciais comprometidas para uma conexão do AWS Site-to-Site VPN

Caso suspeite que as credenciais do túnel para sua conexão da Site-to-Site VPN tenham sido comprometidas, altere a chave pré-compartilhada IKE ou altere o certificado do ACM. O método usado depende da opção de autenticação usada para seus túneis de VPN. Para obter mais informações, consulte AWS Site-to-Site VPNOpções de autenticação de túnel.

Alterar a chave pré-compartilhada IKE

É possível modificar as opções de túnel para a conexão VPN e especificar uma nova chave IKE pré-compartilhada para cada túnel. Para obter mais informações, consulte Modificar opções de túnel de AWS Site-to-Site VPN.

Como alternativa, é possível excluir a conexão VPN. Para obter mais informações, consulte Excluir uma conexão VPN e um gateway. Não é preciso excluir a VPC nem o gateway privado virtual. Depois, crie uma conexão VPN usando o mesmo gateway privado virtual e configure as novas chaves no dispositivo do gateway do cliente. É possível especificar suas próprias chaves pré-compartilhadas para os túneis ou deixar que a AWS gere novas chaves para você. Para obter mais informações, consulte Criar uma conexão VPN. Os endereços internos e externos do túnel podem mudar quando se cria novamente a conexão VPN.

Como alterar o certificado para o lado da AWS do endpoint do túnel

Alterne o certificado. Para obter mais informações, consulte Alternar os certificados de endpoint do túnel da VPN.

Como alterar o certificado no dispositivo de gateway do cliente

1. Crie um novo certificado. Para obter informações, consulte Emissão e gerenciamento de certificados no Guia do usuário do AWS Certificate Manager.
2. Adicione o certificado ao dispositivo de gateway do cliente.

Alternar certificados de endpoint do túnel do AWS Site-to-Site VPN

É possível alternar os certificados nos endpoints do túnel no lado da AWS usando o console da Amazon VPC. Quando o certificado de um endpoint de túnel está próximo da expiração, a AWS alterna automaticamente o certificado usando a função vinculada ao serviço. Para obter mais informações, consulte the section called “Perfis vinculados ao serviço”.

Como alternar o certificado de endpoint do túnel da Site-to-Site VPN usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão da Site-to-Site VPN e escolha Ações, Modificar certificado de túnel VPN.
4. Selecione o endpoint do túnel.
5. Escolha Salvar.

Para alternar o certificado de endpoint do túnel da Site-to-Site VPN usando a AWS CLI

Use o comando modify-vpn-tunnel-certificate.

IP privado AWS Site-to-Site VPN com Direct Connect

Com a VPN IP privada, você pode implantar a IPsec VPN Direct Connect, criptografando o tráfego entre sua rede local e AWS sem o uso de endereços IP públicos ou equipamentos VPN adicionais de terceiros.

Um dos principais casos de uso da VPN IP privada Direct Connecté ajudar clientes dos setores financeiro, de saúde e federal a cumprir as metas regulatórias e de conformidade. A VPN IP privada Direct Connect garante que o tráfego entre redes locais AWS e redes locais seja seguro e privado, permitindo que os clientes cumpram suas exigências regulatórias e de segurança.

Benefícios da VPN de IP privado

- Gerenciamento e operações de rede simplificados: sem VPN IP privada, os clientes precisam implantar VPN e roteadores de terceiros para implementar Direct Connect redes privadas VPNs . Com o recurso da VPN de IP privado, os clientes não precisam implantar nem gerenciar sua própria infraestrutura de VPN. Isso resulta em operações de rede simplificadas e custos reduzidos.
- Postura de segurança aprimorada: anteriormente, os clientes precisavam usar uma interface Direct Connect virtual pública (VIF) para criptografar o tráfego Direct Connect, o que exigia endereços IP públicos para endpoints de VPN. O uso público IPs aumenta a probabilidade de ataques externos (DOS), o que, por sua vez, obriga os clientes a implantar equipamentos de segurança adicionais para proteção da rede. Além disso, uma VIF pública abre o acesso entre todos os serviços AWS públicos e as redes locais do cliente, aumentando a gravidade do risco. O recurso VPN IP privado permite a criptografia em Direct Connect trânsito VIFs (em vez de pública VIFs), juntamente com a capacidade de configuração privada IPs. Isso fornece conectividade end-to-end privada, além da criptografia, melhorando a postura geral de segurança.
- Maior escala de rota: as conexões VPN IP privadas oferecem limites de rota mais altos (5.000 rotas de saída e 1.000 rotas de entrada) em comparação com as Direct Connectúnicas, que atualmente têm um limite de 200 rotas de saída e 100 rotas de entrada.

Como funciona a VPN de IP privado

A Site-to-Site VPN IP privada funciona em uma interface virtual de Direct Connect trânsito (VIF). Ele usa um Direct Connect gateway e um gateway de trânsito para interconectar suas redes locais com.AWS VPCs Uma conexão VPN IP privada tem pontos de terminação no gateway de trânsito na AWS lateral e no dispositivo de gateway do cliente no lado local. Você deve atribuir endereços IP privados às extremidades dos IPsec túneis do gateway de trânsito e do dispositivo de gateway do cliente. Você pode usar endereços IP privados de qualquer um RFC1918 ou de intervalos IPv4 de endereços RFC6598 privados.

Anexe uma conexão VPN de IP privado a um gateway de trânsito. Em seguida, você roteia o tráfego entre o anexo VPN e qualquer rede VPCs (ou outras) que também esteja conectada ao gateway de trânsito. Isso é feito associando uma tabela de rotas ao anexo da VPN. Na direção inversa, você pode VPCs rotear o tráfego do seu anexo IP VPN privado usando tabelas de rotas associadas ao VPCs.

A tabela de rotas associada ao anexo VPN pode ser a mesma ou diferente daquela associada ao Direct Connect anexo subjacente. Isso permite rotear tráfego criptografado e não criptografado simultaneamente entre sua rede VPCs e sua rede local.

Para obter mais detalhes sobre o caminho do tráfego que sai da VPN, consulte Políticas de roteamento da interface virtual privada e da interface virtual de trânsito no Guia do usuário do Direct Connect.

Pré-requisitos

A tabela a seguir descreve os pré-requisitos antes de criar uma VPN IP privada pelo Direct Connect.

Item	Steps	Informações
Prepare o gateway de trânsito para Site-to-Site VPN.	Crie o gateway de trânsito usando o console Amazon Virtual Private Cloud(VPC) ou usando a linha de comando ou a API. Consulte Gateways de trânsito no Guia de gateways de trânsito da Amazon VPC.	Um gateway de trânsito é um hub de trânsito de rede que você pode usar para intercone ctar sua rede com VPCs a rede local. É possível criar um gateway de trânsito ou usar um existente para a conexão da VPN de IP privado. Ao

Item	Steps	Informações
		criar o gateway de trânsito ou modificar um existente, especifique um bloco CIDR de IP privado para a conexão. **Note** Ao especificar o bloco CIDR do gateway de trânsito a ser associado à VPN de IP privado, garanta que o bloco CIDR não se sobreponha a nenhum endereço IP referente a qualquer outro anexo de rede no gateway de trânsito. Se algum bloco CIDR IP se sobrepuser, isso poderá causar problemas de configuração com o dispositivo gateway do cliente.
Crie o Direct Connect gateway para Site-to-Site VPN.	Crie o gateway Direct Connect usando o console do Direct Connect ou usando a linha de comando ou a API. Consulte Criar um gateway AWS Direct Connect no Guia Direct Connect do usuário.	Um gateway Direct Connect permite que você conecte interfaces virtuais (VIFs) em várias AWS regiões. Esse gateway é usado para se conectar à sua VIF.

Item	Steps	Informações
Crie a associação de gateway de trânsito para Site-to-Site VPN.	Crie a associação entre o gateway Direct Connect e o gateway de trânsito usando o console Direct Connect ou a linha de comando ou API. Consulte Associar ou desassociar Direct Connect com um gateway de trânsito no Guia do Direct Connect usuário.	Depois de criar o Direct Connect gateway, crie uma associação de gateway de trânsito para o Direct Connect gateway. Especifique o CIDR de IP privado para o gateway de trânsito identific ado anteriormente na lista de prefixos permitidos.

Tarefas

- Crie um IP privado AWS Site-to-Site VPN sobre Direct Connect

Crie um IP privado AWS Site-to-Site VPN sobre Direct Connect

Para criar uma VPN IP privada, Direct Connect siga estas etapas. Antes de criar a VPN IP privada pelo Direct Connect, é preciso criar um gateway de trânsito e um gateway Direct Connect primeiro. Depois de criar os dois gateways, será preciso criar uma associação entre os dois. Esses pré-requisitos estão descritos na tabela a seguir. Depois de criar e associar os dois gateways, crie um gateway de cliente VPN e uma conexão usando essa associação.

Pré-requisitos

A tabela a seguir descreve os pré-requisitos antes de criar uma VPN IP privada pelo Direct Connect.

Item	Etapas	Informações
Prepare o gateway de trânsito para Site-to-Site VPN.	Crie o gateway de trânsito usando o console Amazon Virtual Private Cloud (VPC) ou usando a linha de comando ou a API.	Um gateway de trânsito é um hub de trânsito de rede que você pode usar para intercone ctar sua rede com VPCs a rede local. É possível criar um gateway de trânsito ou usar

Item	Etapas	Informações
	Consulte Gateways de trânsito no Guia de gateways de trânsito da Amazon VPC.	um existente para a conexão da VPN de IP privado. Ao criar o gateway de trânsito ou modificar um existente, especifique um bloco CIDR de IP privado para a conexão. **Note** Ao especificar o bloco CIDR do gateway de trânsito a ser associado à VPN de IP privado, garanta que o bloco CIDR não se sobreponha a nenhum endereço IP referente a qualquer outro anexo de rede no gateway de trânsito. Se algum bloco CIDR IP se sobrepuser, isso poderá causar problemas de configuração com o dispositivo gateway do cliente.

Item	Etapas	Informações
Crie o Direct Connect gateway para Site-to-Site VPN.	Crie o gateway Direct Connect usando o console do Direct Connect ou usando a linha de comando ou a API. Consulte Criar um gateway AWS Direct Connect no Guia Direct Connect do usuário.	Um gateway Direct Connect permite que você conecte interfaces virtuais (VIFs) em várias AWS regiões. Esse gateway é usado para se conectar à sua VIF.
Crie a associação de gateway de trânsito para Site-to-Site VPN.	Crie a associação entre o gateway Direct Connect e o gateway de trânsito usando o console Direct Connect ou a linha de comando ou API. Consulte Associar ou desassociar Direct Connect com um gateway de trânsito no Guia do Direct Connect usuário.	Depois de criar o Direct Connect gateway, crie uma associação de gateway de trânsito para o Direct Connect gateway. Especifique o CIDR de IP privado para o gateway de trânsito identific ado anteriormente na lista de prefixos permitidos.

Crie o gateway do cliente e a conexão para Site-to-Site VPN

Um gateway do cliente é um recurso que você cria em AWS. Ele representa o dispositivo de gateway do cliente na rede on-premises. Ao criar um gateway do cliente, você fornece informações sobre seu dispositivo para AWS. Consulte mais detalhes em Gateway do cliente.

Para criar um gateway do cliente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways do cliente.
3. Escolha Criar gateway do cliente.
4. (Opcional) Em Name (Nome), insira um nome para o gateway do cliente. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.

5. Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.
6. Em IP address (Endereço IP), insira o endereço IP privado do dispositivo de gateway do cliente.

> **Important**
>
> Ao configurar o IP AWS privado AWS Site-to-Site VPN, você deve especificar seus próprios endereços IP de endpoint de túnel usando endereços RFC 1918. Não use os endereços point-to-point IP para o emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint. Direct Connect AWS recomenda usar uma interface de loopback ou LAN no roteador de gateway do cliente como endereço de origem ou destino em vez de point-to-point conexões.
> Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.

7. (Opcional) Em Dispositivo, insira um nome para o dispositivo que hospeda esse gateway do cliente.
8. Escolha Criar gateway do cliente.
9. No painel de navegação, escolha Conexões Site-to-Site VPN.
10. Escolha Create VPN Connection (Criar conexão VPN).
11. (Opcional) Em Etiqueta de nome, insira um nome para sua conexão Site-to-Site VPN. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
12. Em Target gateway type (Tipo de gateway de destino), escolha Transit gateway (Gateway de trânsito). Depois, selecione o gateway de trânsito identificado anteriormente.
13. Em Customer gateway (Gateway do cliente), selecione Existing (Existente). Depois, selecione o gateway do cliente criado anteriormente.
14. Escolha uma das opções de roteamento dependendo se o seu dispositivo de gateway do cliente é compatível com o Protocolo de Gateway da Borda (BGP):
    - Se o dispositivo de gateway do cliente for compatível com o BGP, selecione Dynamic (requires BGP) (Dinâmico [requer BGP]).
    - Se o dispositivo de gateway do cliente não oferecer suporte ao BGP, selecione Static (Estático).
15. Para túnel dentro da versão IP, especifique se os túneis VPN suportam IPv4 ou IPv6 tráfego.

16. (Opcional) Se você especificou IPv4o túnel dentro da versão IP, você pode, opcionalmente, especificar os intervalos de IPv4 CIDR para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão é `0.0.0.0/0`.

    Se você especificou IPv6a versão Túnel dentro do IP, você pode, opcionalmente, especificar os intervalos de IPv6 CIDR para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão para ambos os intervalos é `::/0`.
17. Em Tipo de endereço IP externo, escolha PrivateIpv4.
18. Em ID do anexo de transporte, escolha o anexo do gateway de trânsito para o Direct Connect gateway apropriado.
19. Escolha Create VPN Connection (Criar conexão VPN).

> **Note**
>
> A opção Enable acceleration (Habilitar a aceleração) não é aplicável para conexões VPN sobre o Direct Connect.

Para criar um gateway do cliente usando a linha de comando ou a API

- CreateCustomerGateway(API de consulta do Amazon EC2)
- create-customer-gateway (AWS CLI)

Segurança na AWS Site-to-Site 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 no Nuvem AWS. 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 que se aplicam à AWS Site-to-Site 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.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Site-to-Site VPN. Os tópicos a seguir mostram como configurar a Site-to-Site VPN para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de Site-to-Site VPN.

Conteúdo

Recursos AWS Site-to-Site VPN de segurança aprimorados usando o Secrets Manager

O recurso Security Rebase do AWS Site-to-Site VPN fornece recursos de segurança aprimorados que oferecem maior controle e visibilidade sobre suas conexões VPN. Uma melhoria importante é a capacidade de armazenar chaves pré-compartilhadas (PSKs) em AWS Secrets Manager vez de diretamente no serviço Site-to-Site VPN, permitindo um melhor gerenciamento de segredos e conformidade com as melhores práticas de segurança. O recurso também inclui a API `GetActiveVpnTunnelStatus`, que oferece visibilidade em tempo real dos parâmetros de segurança usados em túneis VPN ativos, como algoritmos de criptografia, algoritmos de integridade e grupos Diffie-Hellman para ambas as fases do Internet Key Exchange (IKE). Além disso, agora você pode gerar configurações de segurança recomendadas que impõem o uso de protocolos modernos excluindo opções legadas, como. IKEv1 Esses aprimoramentos são particularmente valiosos se sua organização precisar manter padrões de segurança rígidos, precisar de trilhas de auditoria detalhadas das configurações de VPN ou quiser garantir que as conexões VPN usem os protocolos mais seguros disponíveis.

Conteúdo

Altere a chave pré-compartilhada do Secrets Manager em AWS Site-to-Site VPN

Se o túnel estiver inacessível no Secrets Manager, você poderá alterar a chave pré-compartilhada desse túnel.

> **Note**
>
> - Ao alterar a chave pré-compartilhada, verifique se você tem as permissões do IAM necessárias para o serviço Secrets Manager.
> - Após a alteração da chave pré-compartilhada de um túnel VPN, a conectividade fica suspensa por vários minutos. Você deve ter um plano para o tempo de inatividade esperado.

Como alterar a chave pré-compartilhada do Secrets Manager para um túnel VPN

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão Site-to-Site VPN e escolha Ações, Modificar as opções de túnel VPN.
4. Em Endereço IP externo do túnel VPN, escolha o IP do endpoint do túnel VPN.
5. Em Nova chave pré-compartilhada, escolha uma nova chave pré-compartilhada.

> **Note**
>
> Essa opção só está disponível para chaves armazenadas no Secrets Manager.

6. Escolha Salvar alterações.
7. Repita essas etapas para qualquer outro túnel.

Altere o modo de armazenamento de chaves pré-compartilhadas em AWS Site-to-Site VPN

Altere o modo de armazenamento de chaves pré-compartilhadas para um túnel VPN existente.

> **Note**
>
> - Ao alterar os modos de armazenamento, verifique se você tem as permissões necessárias do IAM para os serviços Site-to-Site VPN e Secrets Manager.
> - Após a alteração do modo de armazenamento para um túnel VPN, a conectividade fica suspensa por vários minutos. Você deve ter um plano para o tempo de inatividade esperado.

Como alterar o modo de armazenamento de chaves pré-compartilhadas

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão Site-to-Site VPN e escolha Ações, Modificar as opções de túnel VPN.
4. Em Endereço IP externo do túnel VPN, escolha o IP do endpoint do túnel VPN.

5. Em Armazenamento de chaves pré-compartilhadas, escolha um dos tipos de armazenamento de chaves pré-compartilhadas a seguir.
   - Padrão — A chave pré-compartilhada é armazenada diretamente no serviço Site-to-Site VPN.
   - Secrets Manager: a chave pré-compartilhada é armazenada usando o AWS Secrets Manager. Para ter mais informações sobre o Secrets Manager, consulte Recursos de segurança aprimorados usando o Secrets Manager.
6. Escolha Salvar alterações.

Ao alterar o modo de armazenamento do Secrets Manager para o Padrão:

- A chave pré-compartilhada é removida do Secrets Manager e movida para o serviço Site-to-Site VPN.
- A entrada do túnel é removida do segredo do Secrets Manager.

Ao alterar o modo de armazenamento do padrão para o Secrets Manager:

- A chave pré-compartilhada é removida do Site-to-Site serviço VPN
- Um segredo do Secrets Manager é criado, caso ainda não exista.
- A nova chave pré-compartilhada é armazenada no Secrets Manager.

Proteção de dados em AWS Site-to-Site VPN

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados na AWS Site-to-Site VPN. 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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as Data Privacy FAQ. Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM 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 uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- 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 sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Site-to-Site VPN ou outro Serviços da AWS usando o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em 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 fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Privacidade do tráfego entre redes

Uma conexão Site-to-Site VPN conecta de forma privada sua VPC à sua rede local. Os dados que são transferidos entre a VPC e suas rotas de rede por meio de uma conexão VPN criptografada para ajudar a manter a confidencialidade e a integridade dos dados em trânsito. A Amazon oferece suporte a conexões VPN de segurança do Internet Protocol (IPsec). IPsec é um conjunto de protocolos para proteger as comunicações IP autenticando e criptografando cada pacote IP em um fluxo de dados.

Cada conexão Site-to-Site VPN consiste em dois túneis IPsec VPN criptografados que se AWS conectam à sua rede. O tráfego em cada túnel pode ser criptografado com AES128 ou AES256 e usar grupos Diffie-Hellman para troca de chaves, fornecendo Perfect Forward Secrecy. AWS autentica com funções de hashing SHA1 ou de SHA2 hashing.

As instâncias na sua VPC não exigem um endereço IP público para se conectar aos recursos do outro lado da sua conexão Site-to-Site VPN. As instâncias podem rotear o tráfego da Internet por meio da conexão Site-to-Site VPN para sua rede local. Elas podem acessar a Internet por meio de seus pontos de tráfego de saída existentes e seus dispositivos de segurança e monitoramento de rede.

Consulte os tópicos a seguir para obter mais informações:

- Opções de túnel para sua AWS Site-to-Site VPN conexão: fornece informações sobre as opções IPsec e o Internet Key Exchange (IKE) que estão disponíveis para cada túnel.
- AWS Site-to-Site VPNOpções de autenticação de túnel: fornece informações sobre as opções de autenticação para os terminais de túneis VPN.
- Requisitos para um dispositivo de gateway do AWS Site-to-Site VPN cliente: fornece informações sobre os requisitos para o dispositivo de gateway do cliente no seu lado da conexão VPN.
- Comunicação segura entre AWS Site-to-Site VPN conexões usando VPN CloudHub: se você tiver várias conexões Site-to-Site VPN, poderá fornecer comunicação segura entre seus sites locais usando a AWS VPN CloudHub.

Gerenciamento de identidade e acesso para AWS Site-to-Site VPN

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

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas

- Como a AWS Site-to-Site VPN funciona com o IAM
- Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site
- Solução de problemas de identidade e acesso à AWS Site-to-Site VPN
- AWS políticas gerenciadas para Site-to-Site VPN
- Usando funções vinculadas a serviços para VPN Site-to-Site

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso à AWS Site-to-Site VPN).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como a AWS Site-to-Site VPN funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site)

Autenticação com identidades

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

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente

recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos 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 corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

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

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

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 políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como a AWS Site-to-Site VPN funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à Site-to-Site VPN, saiba quais recursos do IAM estão disponíveis para uso com a Site-to-Site VPN.

Recursos do IAM que você pode usar com AWS Site-to-Site VPN

Recurso do IAM	Site-to-Site Suporte de VPN
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não

Recurso do IAM	Site-to-Site Suporte de VPN
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Sim

Para ter uma visão de alto nível de como a Site-to-Site VPN e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para VPN Site-to-Site

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para VPN Site-to-Site

Para ver exemplos de políticas baseadas em identidade de Site-to-Site VPN, consulte. Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site

Políticas baseadas em recursos dentro da VPN Site-to-Site

Compatibilidade com políticas baseadas em recursos: não

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

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para Site-to-Site VPN

Compatível com ações de políticas: sim

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

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações de Site-to-Site VPN, consulte Ações definidas pela AWS Site-to-Site VPN na Referência de autorização de serviço.

As ações de política na Site-to-Site VPN usam o seguinte prefixo antes da ação:

```
ec2
```

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

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

Para ver exemplos de políticas baseadas em identidade de Site-to-Site VPN, consulte. Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site

Recursos de política para Site-to-Site VPN

Compatível com recursos de políticas: sim

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

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos de Site-to-Site VPN e seus ARNs, consulte Recursos definidos pela AWS Site-to-Site VPN na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pela AWS Site-to-Site VPN.

Para ver exemplos de políticas baseadas em identidade de Site-to-Site VPN, consulte. Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site

Chaves de condição de política para Site-to-Site VPN

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

Os administradores podem usar políticas AWS JSON 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` especifica quando as instruções são executadas com base em critérios definidos. 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. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de condição de Site-to-Site VPN, consulte Chaves de condição para AWS Site-to-Site VPN na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela AWS Site-to-Site VPN.

Para ver exemplos de políticas baseadas em identidade de Site-to-Site VPN, consulte. Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site

ACLs em Site-to-Site VPN

Suportes ACLs: Não

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

ABAC com VPN Site-to-Site

Oferece compatibilidade com ABAC (tags em políticas): não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

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 for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com VPN Site-to-Site

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões principais entre serviços para VPN Site-to-Site

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para Site-to-Site VPN

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade da Site-to-Site VPN. Edite as funções de serviço somente quando a Site-to-Site VPN fornecer orientação para fazer isso.

Funções vinculadas a serviços para VPN Site-to-Site

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil 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 administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para VPN AWS Site-to-Site

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos de Site-to-Site VPN. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pela Site-to-Site VPN, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para AWS Site-to-Site VPN na Referência de Autorização de Serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Usando o console Site-to-Site VPN
- Descreva conexões Site-to-Site VPN específicas
- Crie e descreva os recursos necessários para uma AWS Site-to-Site VPN conexão

Práticas recomendadas de política

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

- Comece com políticas AWS gerenciadas e avance para permissões de privilégios mínimos — Para começar a conceder permissões para 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 saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o console Site-to-Site VPN

Para acessar o console da AWS Site-to-Site VPN, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos de Site-to-Site VPN em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console da Site-to-Site VPN, anexe também a Site-to-Site VPN `AmazonVPCFullAccess` ou a política `AmazonVPCReadOnlyAccess` AWS gerenciada às entidades. Para saber mais, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Descreva conexões Site-to-Site VPN específicas

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
      }
   ]
}
```

Crie e descreva os recursos necessários para uma AWS Site-to-Site VPN conexão

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
         }
      }
   ]
}
```

Solução de problemas de identidade e acesso à AWS Site-to-Site VPN

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

Tópicos

- Não estou autorizado a realizar uma ação na Site-to-Site VPN
- Não estou autorizado a realizar iam: PassRole

- Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos de Site-to-Site VPN

Não estou autorizado a realizar uma ação na Site-to-Site VPN

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

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

```
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 a Site-to-Site VPN.

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 usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação na Site-to-Site VPN. 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 de fora da minha Conta da AWS acessem meus recursos de Site-to-Site VPN

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 a Site-to-Site VPN oferece suporte a esses recursos, consulteComo a AWS Site-to-Site VPN funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

AWS políticas gerenciadas para Site-to-Site VPN

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais

informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AWSVPCS2 SVpn ServiceRolePolicy

É possível anexar a política `AWSVPCS2SVpnServiceRolePolicy` às suas identidades do IAM. Essa política permite que a Site-to-Site VPN gerencie um AWS Secrets Manager segredo dentro da Site-to-Site VPN. Para obter mais informações, consulte the section called “Uso de perfis vinculados ao serviço”.

Para visualizar as permissões para esta política, consulte AWSVPCS2SVpnServiceRolePolicy na Referência de políticas gerenciadas pela AWS .

Site-to-Site Atualizações de VPN para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas de Site-to-Site VPN desde que esse serviço começou a monitorar essas mudanças em maio de 2025.

Alteração	Descrição	Data
AWSVPCS2SVpnServiceRolePolicy: atualizar política.	Novas permissões adicionadas à política, permitindo que a Site-to-Site VPN gerencie	14 de maio de 2025

Alteração	Descrição	Data
	o segredo AWS Secrets Manager `s2svpn` gerenciado da conexão VPN.	

Usando funções vinculadas a serviços para VPN Site-to-Site

AWS Site-to-Site A VPN usa AWS Identity and Access Management funções vinculadas ao serviço (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente à Site-to-Site VPN. As funções vinculadas ao serviço são predefinidas pela Site-to-Site VPN e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

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

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos de Site-to-Site VPN porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Permissões de função vinculadas ao serviço para VPN Site-to-Site

Site-to-Site A VPN usa a função vinculada ao serviço chamada AWSServiceRoleForVPCS2SVPN — Permita que a Site-to-Site VPN crie e gerencie recursos relacionados às suas conexões VPN.

A função vinculada ao serviço AWSService RoleFor VPCS2 SVPN confia no seguinte serviço para assumir a função:

- `s2svpn.amazonaws.com`

Essa função vinculada ao serviço usa a política gerenciada AWSVPCS2 SVpn ServiceRolePolicy para concluir as seguintes ações nos recursos especificados:

- Ao usar a autenticação de certificado para sua conexão VPN, AWS Site-to-Site VPN exporta os AWS Certificate Manager certificados do túnel VPN para uso nos endpoints do túnel VPN.

- Ao usar a autenticação de certificado para sua conexão VPN, AWS Site-to-Site VPN gerencia a renovação dos AWS Certificate Manager certificados do túnel VPN.
- Ao usar o armazenamento de chaves SecretsManager pré-compartilhadas para sua conexão VPN, AWS Site-to-Site VPN gerencia o segredo gerenciado AWS Secrets Manager s2svpn da conexão VPN.

Para visualizar as permissões para esta política, consulte AWSVPCS2SVpnServiceRolePolicy na Referência de políticas gerenciadas pela AWS .

Crie uma função vinculada ao serviço para VPN Site-to-Site

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um gateway de cliente com um certificado privado do ACM associado na Console de gerenciamento da AWS, na ou na AWS API AWS CLI, a Site-to-Site VPN cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria um gateway de cliente com um certificado privado do ACM associado, a Site-to-Site VPN cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para VPN Site-to-Site

Site-to-Site A VPN não permite que você edite a função vinculada ao serviço AWSService RoleFor VPCS2 SVPN. 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, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma descrição de perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para VPN Site-to-Site

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

> **Note**
>
> Se o serviço de Site-to-Site VPN estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos de Site-to-Site VPN usados pelo AWSService RoleFor VPCS2 SVPN

Você pode excluir essa função vinculada ao serviço somente depois de excluir todos os gateways do cliente que tenham um certificado privado do ACM associado. Isso garante que você não possa remover inadvertidamente a permissão para acessar seus certificados ACM em uso por conexões VPN. Site-to-Site

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função vinculada ao serviço AWSService RoleFor VPCS2 SVPN. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Resiliência em AWS Site-to-Site 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 aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são 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, a Site-to-Site VPN oferece recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Dois túneis por conexão VPN

Uma conexão Site-to-Site VPN consiste em dois túneis, cada um terminando em uma zona de disponibilidade diferente, para fornecer maior disponibilidade à sua VPC. Se houver uma falha no

dispositivo AWS, sua conexão VPN automaticamente passará para o segundo túnel para que seu acesso não seja interrompido. De tempos em tempos, AWS também realiza manutenção de rotina em sua conexão VPN, o que pode desativar brevemente um dos dois túneis da sua conexão VPN. Para obter mais informações, consulte AWS Site-to-Site VPN substituições de terminais de túneis. Ao configurar o gateway do cliente, é importante configurar ambos os túneis.

Redundância

Para se proteger contra a perda de conectividade caso o gateway do cliente fique indisponível, você pode configurar uma segunda conexão Site-to-Site VPN. Para saber mais, consulte a documentação a seguir:

- Conexões do AWS Site-to-Site VPN redundantes para failover
- Opções de conectividade da Amazon Virtual Private Cloud
- Construindo uma infraestrutura de rede AWS multi-VPC escalável e segura

Segurança de infraestrutura em AWS Site-to-Site VPN

Como um serviço gerenciado, a AWS Site-to-Site VPN é protegida 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 chamadas de API AWS publicadas para acessar a Site-to-Site VPN pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Monitore uma AWS Site-to-Site VPN conexão

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho da sua AWS Site-to-Site VPN conexão. Você deve coletar dados de monitoramento de todas as partes de sua solução para facilitar a depuração de uma falha multipontos, caso ocorra. Antes de começar a monitorar sua conexão Site-to-Site VPN, no entanto, você deve criar um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

A próxima etapa é estabelecer um parâmetro de performance normal da VPN no ambiente medindo a performance em vários momentos e em diferentes condições de carga. À medida que você monitorar a VPN, armazene dados históricos de monitoramento para que possa compará-los com os dados de performance atuais, identificar padrões de performance normais e anomalias de performance e idealizar métodos para solucionar problemas.

Para estabelecer um parâmetro, é preciso monitorar os seguintes itens:

- O estado dos túneis da VPN
- Os dados no túnel
- Os dados fora do túnel

Tópicos

Ferramentas de monitoramento

AWS fornece várias ferramentas que você pode usar para monitorar uma conexão Site-to-Site VPN. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Você pode usar as seguintes ferramentas de monitoramento automatizado para observar uma conexão Site-to-Site VPN e relatar quando algo está errado:

- Amazon CloudWatch Alarms — Observe uma única métrica durante um período de tempo especificado por você e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para obter mais informações, consulte Monitore AWS Site-to-Site VPN túneis usando a Amazon CloudWatch.
- AWS CloudTrail Monitoramento de registros — compartilhe arquivos de log entre contas, monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs, grave aplicativos de processamento de log em Java e valide se seus arquivos de log não foram alterados após a entrega. CloudTrail Para obter mais informações, consulte Registrar chamadas de API usando AWS CloudTrail na Referência de API do Amazon EC2 e Trabalho com arquivos de CloudTrail log no Guia do AWS CloudTrail usuário.
- AWS Health eventos — Receba alertas e notificações relacionados a mudanças na integridade de seus túneis Site-to-Site VPN, recomendações de configuração de melhores práticas ou ao se aproximar dos limites de escalabilidade. Use eventos no Personal Health Dashboard para acionar failovers automatizados, reduzir o tempo de solução de problemas ou otimizar conexões para alta disponibilidade. Para obter mais informações, consulte AWS Health e AWS Site-to-Site VPN eventos.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento de uma conexão Site-to-Site VPN envolve o monitoramento manual dos itens que os CloudWatch alarmes não cobrem. Os painéis do Amazon VPC e CloudWatch do console fornecem uma at-a-glance visão do estado do seu ambiente. AWS

> **Note**
>
> No console da Amazon VPC, os parâmetros de estado do túnel Site-to-Site VPN, como “Status” e “Última alteração de status”, podem não refletir mudanças de estado transitórias ou oscilações momentâneas do túnel. É recomendável usar CloudWatch métricas e registros para atualizações granulares de alterações de estado do túnel.

- O painel da Amazon VPC mostra:
  - Integridade do serviço por região
  - Site-to-Site Conexões VPN
  - Status do túnel VPN (no painel de navegação, escolha Conexões Site-to-Site VPN, selecione uma conexão Site-to-Site VPN e escolha Detalhes do túnel)
- A página CloudWatch inicial mostra:
  - Alertas e status atual
  - Gráficos de alertas e recursos
  - Estado de integridade do serviço

  Além disso, você pode usar CloudWatch para fazer o seguinte:
  - Crie painéis personalizados para monitorar os serviços com os quais você se preocupa.
  - Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências
  - Pesquise e navegue em todas as suas métricas AWS de recursos
  - Criar e editar alertas para ser notificado sobre problemas

AWS Site-to-Site VPN troncos

AWS Site-to-Site VPN os registros fornecem uma visibilidade mais profunda de suas implantações de Site-to-Site VPN. Com esse recurso, você tem acesso aos registros de conexão Site-to-Site VPN que fornecem detalhes sobre o estabelecimento do túnel IP Security (IPsec), negociações do Internet Key Exchange (IKE), mensagens do protocolo Dead Peer Detection (DPD), status do protocolo Border Gateway (BGP) e atualizações de roteamento.

Site-to-Site Os registros de VPN podem ser publicados no Amazon CloudWatch Logs. Esse recurso fornece aos clientes uma maneira única e consistente de acessar e analisar registros detalhados de todas as suas conexões Site-to-Site VPN.

Tópicos

Benefícios dos registros de Site-to-Site VPN

- Solução de problemas simplificada de Site-to-Site VPN: os registros de VPN ajudam você a identificar incompatibilidades de configuração entre AWS o dispositivo de gateway do cliente e a resolver os problemas iniciais de conectividade da VPN. As conexões VPN podem oscilar intermitentemente ao longo do tempo devido a configurações incorretas (como tempos limite mal ajustados). Pode haver problemas nas redes de transporte subjacentes (como clima da Internet) ou alterações de roteamento ou falhas de caminho podem provocar interrupção da conectividade pela VPN. Esse recurso permite diagnosticar com precisão a causa de falhas de conexão intermitentes e ajustar a configuração do túnel de baixo nível para uma operação confiável.
- AWS Site-to-Site VPN Visibilidade centralizada: os registros de Site-to-Site VPN podem fornecer atividades de túneis e registros de roteamento BGP em todos os Site-to-Site tipos de conexão VPN. Esse recurso fornece aos clientes uma maneira única e consistente de acessar e analisar registros detalhados de todas as suas conexões Site-to-Site VPN.
- Segurança e conformidade: os registros de Site-to-Site VPN podem ser enviados ao Amazon CloudWatch Logs para análise retrospectiva do status e da atividade da conexão VPN ao longo do tempo. Isso pode ajudar você a atender a requisitos de conformidade e regulamentares.

Restrições de tamanho da política de recursos do Amazon CloudWatch Logs

CloudWatch As políticas de recursos de registros estão limitadas a 5120 caracteres. Quando o CloudWatch Logs detecta que uma política se aproxima desse limite de tamanho, ele ativa

automaticamente grupos de registros que começam com `/aws/vendedlogs/`. Quando você ativa o registro, a Site-to-Site VPN deve atualizar sua política de recursos de CloudWatch registros com o grupo de registros especificado. Para evitar atingir o limite de tamanho da política de recursos de CloudWatch registros, prefixe os nomes dos seus grupos de registros com `/aws/vendedlogs/`.

Site-to-Site Conteúdo do registro de VPN

As informações a seguir estão incluídas no registro de atividades do túnel Site-to-Site VPN. O nome do arquivo do fluxo de log usa VpnConnection ID TunnelOutside IPAddress e.

Campo	Description
VpnLogCreationTimestamp (`event_timestamp`)	Carimbo de data/hora de criação de log no formato de época.
VpnLogCreationTimestampReadable (`timestamp`)	Carimbo de data/hora de criação de log em formato de hora legível por humanos.
Túnel DPDEnabled (`dpd_enabled`)	Status habilitado do protocolo Dead Peer Detection (True/False).
CGWNATTDetectionStatus do túnel (`nat_t_detected`)	NAT-T detectado no dispositivo de gateway do cliente (True/False).
IKEPhase1Estado do túnel (`ike_phase1_state`)	Estado do protocolo IKE Fase 1 (Established | Rekeying | Negotiating | Down).
IKEPhase2Estado do túnel (`ike_phase2_state`)	Estado do protocolo IKE Fase 2 (Established | Rekeying | Negotiating | Down).
VpnLogDetail (`details`)	Mensagens detalhadas para os protocolos IPsec IKE e DPD.

As informações a seguir estão incluídas no registro BGP do túnel Site-to-Site VPN. O nome do arquivo do fluxo de log usa VpnConnection ID TunnelOutside IPAddress e.

Campo	Description
id_do_recurso	Um ID exclusivo para identificar o túnel e a conexão VPN à qual o registro está associado.
event_timestamp	Carimbo de data/hora de criação de log no formato de época.
timestamp	Carimbo de data/hora de criação de log em formato de hora legível por humanos.
type	Tipo de evento de registro do BGP (BGPStatus | RouteStatus).
status	atualização de status para um tipo específico de evento de registro (BGPStatus: UP | DOWN) (RouteStatus: ANUNCIADO {a rota foi anunciada pelo par} | ATUALIZADO: {a rota existente foi atualizada pelo par} | RETIRADA: {a rota foi retirada pelo par}).
message	Fornece detalhes adicionais sobre o evento e o status do registro. Esse campo ajudará você a entender por BGPStatus que os atributos de rota foram trocados na RouteStatus mensagem.

Conteúdo

IKEv1 Mensagens de erro

Mensagem	Explicação
O par não responde: declaração de par desativado	O par não respondeu às mensagens de DPD, aplicando a ação de tempo limite de DPD.
AWS A decodificação da carga útil do túnel não teve êxito devido à chave pré-compartilhada inválida	A mesma chave pré-compartilhada precisa ser configurada em ambos os pares do IKE.
Nenhuma proposta correspondente encontrada por AWS	Os atributos propostos para a fase 1 (criptogr afia, hashing e grupo DH) não são compatíve is com o AWS VPN Endpoint. Por exemplo, `3DES`.
Nenhuma proposta correspondente encontrad a. Notificação com “Nenhuma proposta escolhida”	Nenhuma mensagem de erro de proposta escolhida é trocada entre pares para informar que a configuração correta Proposals/Policies deve ser configurada para a fase 2 nos pares IKE.
AWS o túnel recebeu DELETE para a fase 2 SA com SPI: xxxx	O CGW enviou a mensagem Delete_SA para a Fase 2.
AWS túnel recebeu DELETE para IKE_SA da CGW	O CGW enviou a mensagem Delete_SA para a Fase 1.

IKEv2 Mensagens de erro

Mensagem	Explicação
AWS O tempo limite do DPD do túnel foi atingido após a retransmissão de {retry_count}	O par não respondeu às mensagens de DPD, aplicando a ação de tempo limite de DPD.
AWS túnel recebeu DELETE para IKE_SA da CGW	O par enviou a mensagem Delete_SA para Parent/IKE_SA.

Mensagem	Explicação
AWS o túnel recebeu DELETE para a fase 2 SA com SPI: xxxx	O par enviou a mensagem Delete_SA para CHILD_SA.
AWS o túnel detectou uma colisão (CHILD_RE KEY) como CHILD_DELETE	O CGW enviou a mensagem Delete_SA para o SA ativo, que está sendo recodificado.
AWS A SA redundante do túnel (CHILD_SA) está sendo excluída devido à colisão detectada	Devido à colisão, se SAs forem gerados redundantes, os pares fecharão o SA redundante após combinar os valores de nonce de acordo com o RFC.
AWS A fase 2 do túnel não foi capaz de se estabelecer enquanto mantinha a fase 1	O par não conseguiu estabelecer CHILD_SA devido a um erro de negociação; por exemplo, proposta incorreta.
AWS: seletor de tráfego: TS_UNACCE PTABLE: recebido do respondente	Peer propôs um Selectors/Encryption domínio de tráfego incorreto. Os pares devem ser configurados de forma idêntica e correta CIDRs.
AWS o túnel está enviando AUTHENTIC ATION_FAILED como resposta	O par não consegue autenticar o par verifican do o conteúdo da mensagem IKE_AUTH
AWS o túnel detectou uma incompatibilidade de chave pré-compartilhada com cgw: xxxx	A mesma chave pré-compartilhada precisa ser configurada em ambos os pares do IKE.
AWS Tempo limite do túnel: excluindo IKE_SA da Fase 1 não estabelecida com cgw: xxxx	A exclusão do IKE_SA semiaberto como par não prosseguiu com as negociações
Nenhuma proposta correspondente encontrad a. Notificação com “Nenhuma proposta escolhida”	Nenhuma mensagem de erro da proposta escolhida é trocada entre os pares para informar que as propostas corretas devem ser configuradas em pares do IKE.

Mensagem	Explicação
Nenhuma proposta correspondente encontrada por AWS	Os atributos propostos para a fase 1 ou fase 2 (criptografia, hashing e grupo DH) não são suportados pelo AWS VPN Endpoint — por exemplo,. `3DES`

IKEv2 Mensagens de negociação

Mensagem	Explicação
AWS solicitação processada por túnel (id=xxx) para CREATE_CHILD_SA	AWS recebeu a solicitação CREATE_CHILD_SA da CGW.
AWS o túnel está enviando resposta (id=xxx) para CREATE_CHILD_SA	AWS está enviando a resposta CREATE_CHILD_SA para o CGW.
AWS o túnel está enviando a solicitação (id=xxx) para CREATE_CHILD_SA	AWS está enviando a solicitação CREATE_CHILD_SA para a CGW.
AWS resposta processada em túnel (id = xxx) para CREATE_CHILD_SA	AWS recebeu a resposta CREATE_CHILD_SA do CGW.

Mensagens de status do BGP

As mensagens de status do BGP contêm informações relacionadas às transições de estado da sessão do BGP, avisos de limite de prefixo, violações de limite, notificações da sessão do BGP, mensagens do BGP OPEN e atualizações de atributos de um vizinho do BGP para uma determinada sessão do BGP.

Mensagem	Status do BGP	Explicação
O estado da sessão BGP peer do lado da AWS mudou de Idle para Connect with neighbor {ip: xxx}	PARA BAIXO	O estado da conexão BGP no lado da AWS foi atualizado para Connect.

Mensagem	Status do BGP	Explicação
O estado da sessão BGP peer do lado da AWS foi alterado de Connect para OpenSent with neighbor {ip: xxx}	PARA BAIXO	O estado da conexão BGP no lado da AWS foi atualizado para. OpenSent
O estado da sessão BGP peer do lado da AWS foi alterado de OpenSent para OpenConfi rm com o vizinho {ip: xxx}	PARA BAIXO	O estado da conexão BGP no lado da AWS foi atualizado para. OpenConfirm
O estado da sessão BGP peer do lado da AWS foi alterado de OpenConfirm para Estabelecido com o vizinho {ip: xxx}	PARA CIMA	O estado da conexão BGP no lado da AWS foi atualizado para Estabelecido.
O estado da sessão BGP peer do lado da AWS foi alterado de Estabelecido para Ocioso com vizinho {ip: xxx}	PARA BAIXO	O estado da conexão BGP no lado da AWS foi atualizado para Idle.
O estado da sessão BGP peer do lado da AWS foi alterado de Connect para Active with neighbor {ip: xxx}	PARA BAIXO	O estado da conexão BGP no lado da AWS passou de Connect para Active. Verifique a disponibilidade da porta TCP 179 no CGW se a sessão BGP estiver travada no estado Connect.
Um colega do lado da AWS está relatando um aviso de limite máximo de prefixo - recebido {prefixes (count): xxx} prefixos do vizinho {ip: xxx}, o limite é {limit (numeric) : xxx}	PARA CIMA	O lado da AWS gera periodica mente uma mensagem de log quando o número de prefixos recebidos do CGW se aproxima do limite permitido.

Mensagem	Status do BGP	Explicação
Um par do lado da AWS detectou que o limite máximo de prefixo foi excedido - recebeu {prefixes (count): xxx} prefixos do vizinho {ip: xxx}, o limite é {limit (numeric): xxx}	PARA BAIXO	O lado da AWS gera uma mensagem de log quando o número de prefixos recebidos do CGW excede o limite permitido.
Um colega do lado da AWS enviou uma notificação 6/1 (cessação/número máximo de prefixos atingidos) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao colega BGP da CGW para indicar que a sessão do BGP foi encerrada devido a uma violação do limite de prefixo.
O colega do lado da AWS recebeu uma notificação 6/1 (número máximo de prefixos atingidos) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do colega da CGW indicando que a sessão do BGP foi encerrada devido a uma violação do limite de prefixo.
Um colega do lado da AWS enviou uma notificação 6/2 (cessação/desligamento administrativo) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao peer do CGW BGP para indicar que a sessão do BGP foi encerrada.
O colega do lado da AWS recebeu a notificação 6/2 (cessação/desligamento administrativo) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do colega da CGW indicando que a sessão do BGP foi encerrada.

Mensagem	Status do BGP	Explicação
O peer do lado da AWS enviou uma notificação 6/3 (Cease/Peer não configurado) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao peer da CGW para indicar que o peer não está configurado ou foi removido da configuração.
O peer do lado da AWS recebeu uma notificação 6/3 (cessação/peer não configurado) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do peer CGW para indicar que o peer não está configurado ou foi removido da configuração.
Um colega do lado da AWS enviou uma notificação 6/4 (cessação/redefinição administrativa) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao peer BGP da CGW para indicar que a sessão do BGP foi redefinida.
O colega do lado da AWS recebeu uma notificação 6/4 (cessação/redefinição administrativa) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do colega da CGW para indicar que a sessão do BGP foi redefinida.
Um colega do lado da AWS enviou uma notificação 6/5 (cessação/conexão rejeitada) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao colega BGP da CGW para indicar que a sessão do BGP foi rejeitada.
O colega do lado da AWS recebeu uma notificação 6/5 (cessação/conexão rejeitada) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do colega da CGW indicando que a sessão do BGP foi rejeitada.

Mensagem	Status do BGP	Explicação
O colega do lado da AWS enviou uma notificação 6/6 (cessação/outra alteração de configuração) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao peer BGP da CGW para indicar que ocorreu uma alteração na configura ção da sessão do BGP.
O par do lado da AWS recebeu uma notificação 6/6 (cessação/outra alteração de configuração) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do par da CGW que indica que ocorreu uma alteração na configuração da sessão do BGP.
Um colega do lado da AWS enviou uma notificação 6/7 (resolução de colisão de cessação/conexão) ao vizinho {ip: xxx}	PARA BAIXO	O lado da AWS enviou uma notificação ao colega da CGW para resolver uma colisão de conexão quando os dois pares tentarem estabelecer uma conexão simultaneamente.
O colega do lado da AWS recebeu uma notificação 6/7 (resolução de colisão de cessação/conexão) do vizinho {ip: xxx}	PARA BAIXO	O lado da AWS recebeu uma notificação do colega da CGW indicando a resolução de uma colisão de conexão quando os dois pares tentam estabelec er uma conexão simultane amente.
Um colega do lado da AWS enviou uma notificação expirada do Hold Timer para o vizinho {ip: xxx}	PARA BAIXO	O cronômetro de espera do BGP expirou e uma notificaç ão foi enviada pelo lado da AWS ao CGW.

Mensagem	Status do BGP	Explicação
O peer do lado da AWS detectou uma mensagem OPEN inválida do vizinho {ip: xxx} - o AS remoto é {asn: xxx}, esperado {asn: xxx}	PARA BAIXO	O lado da AWS detectou que uma mensagem OPEN incorreta foi recebida do par CGW, o que indica uma incompatibilidade de configuração.
O colega do lado da AWS recebeu uma mensagem OPEN do vizinho {ip: xxx} - versão 4, AS {asn: xxx}, holdtime {holdtime (seconds): xxx}, router-id {id: xxx}}	PARA BAIXO	O lado da AWS recebeu uma mensagem aberta do BGP para iniciar uma sessão do BGP com o par do CGW.
Um colega do lado da AWS enviou uma mensagem OPEN para o vizinho {ip: xxx} - versão 4, AS {asn: xxx}, holdtime {holdtime (seconds): xxx}, router-id {id: xxx}	PARA BAIXO	O par do CGW enviou uma mensagem aberta do BGP para iniciar uma sessão do BGP com o par do BGP do lado da AWS.
O peer do lado da AWS está iniciando uma conexão (via Connect) com o vizinho {ip: xxx}	PARA BAIXO	O lado da AWS está tentando se conectar com o vizinho CGW BGP.
Um colega do lado da AWS enviou uma End-of-RIB mensagem para o vizinho {ip: xxx}	PARA CIMA	O lado da AWS terminou de transmitir rotas para o CGW após o estabelecimento da sessão do BGP.
O par do lado da AWS recebeu atualização com atributos do vizinho {ip: xxx} - caminho do AS: {aspath (list): xxx xxx xxx}	PARA CIMA	O lado da AWS recebeu uma atualização do atributo de sessão do BGP do vizinho.

Mensagens de status da rota

Diferentemente das mensagens de status do BGP, as mensagens de status da rota contêm dados sobre os atributos do BGP de um determinado prefixo, como caminho AS, preferência local, discriminador de múltiplas saídas (MED), endereço IP do próximo salto e peso. Uma mensagem de status da rota conterá apenas um campo de detalhes quando houver um erro com uma rota que foi ANUNCIADA, ATUALIZADA ou RETIRADA. Exemplos dos quais são os seguintes

Mensagem	Explicação
NEGADO devido a: as-path contém nosso próprio AS	As mensagens de atualização do BGP para um novo prefixo do CGW foram negadas pela AWS devido à rota contendo o próprio AS dos pares do lado da AWS.
NEGADO devido a: próximo salto não conectado	A AWS rejeitou um anúncio de rota BGP para o prefixo do CGW devido a uma falha de validação de próximo salto não conectada. Certifique-se de que a rota seja acessível no lado do CGW.

Exemplo de formato de log para registros do Tunnel BGP


```
{
    "resource_id": "vpn-1234abcd_1.2.3.4",
    "event_timestamp": 1762580429641,
    "timestamp": "2025-11-08 05:40:29.641Z",
    "type": "BGPStatus",
    "status": "UP",
    "message": {
        "details": "AWS-side peer BGP session state has changed from OpenConfirm to
 Established with neighbor 169.254.50.85"
    }
}

{
    "resource_id": "vpn-1234abcd_1.2.3.4",
    "event_timestamp": 1762579573243,
```

```
    "timestamp": "2025-11-08 05:26:13.243Z",
    "type": "RouteStatus",
    "status": "UPDATED",
    "message": {
        "prefix": "172.31.0.0/16",
        "asPath": "64512",
        "localPref": 100,
        "med": 100,
        "nextHopIp": "169.254.50.85",
        "weight": 32768,
        "details": "DENIED due to: as-path contains our own AS"
    }
}
```

Requisitos do IAM para publicar no CloudWatch Logs

Para que o recurso de log funcione corretamente, a política do IAM anexada à entidade principal do IAM que está sendo usada para configurar o recurso deve incluir, no mínimo, as permissões a seguir. Mais detalhes também podem ser encontrados na seção Habilitando o registro em determinados AWS serviços do Guia do usuário do Amazon CloudWatch Logs.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
```

```
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Exibir configuração de AWS Site-to-Site VPN registros

Veja o registro de atividades de uma conexão Site-to-Site VPN. Aqui você pode ver detalhes sobre a configuração desses algoritmos de criptografia ou se os registros de VPN de túnel estão habilitados. Você também pode visualizar o estado do túnel. Isso ajuda a monitorar melhor quaisquer problemas ou conflitos que você possa ter com uma conexão VPN.

Como visualizar configurações atuais do registro em log do túnel

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão VPN que você deseja visualizar por meio da lista VPN connections (Conexões de VPN).
4. Selecione a guia Tunnel details (Detalhes do túnel).
5. Expanda as seções Tunnel 1 options (Opções de túnel 1) e Tunnel 2 options (Opções de túnel 2) para visualizar todos os detalhes de configuração do túnel.
6. Você pode ver o status atual do recurso de log de VPN de túnel e o grupo de CloudWatch log configurado atualmente (se houver) em grupo de log para CloudWatch log de VPN de túnel e o formato de saída de log em Formato de saída para log de VPN de túnel.
7. Você pode visualizar o status atual do recurso de log BGP do túnel e o grupo de log configurado atualmente (se houver) em grupo de CloudWatch log para CloudWatch log de VPN de túnel e o formato de saída de log em Formato de saída para log de BGP de túnel.

Para ver as configurações atuais de registro de túneis em uma conexão Site-to-Site VPN usando a linha de AWS comando ou a API

- DescribeVpnConnections(API de consulta do Amazon EC2)
- describe-vpn-connections (AWS CLI)

Ativar AWS Site-to-Site VPN registros

Ative Site-to-Site os registros da VPN para registrar a atividade da VPN, como o estado do túnel e outros detalhes. É possível ativar o registro em log em uma nova conexão ou modificar uma conexão existente para iniciar a atividade de registro em log. Se você quiser desabilitar o registro em log para uma conexão, consulte Desativar registros de Site-to-Site VPN.

> **Note**
>
> Quando você ativa os registros de Site-to-Site VPN para um túnel de conexão VPN existente, sua conectividade nesse túnel pode ser interrompida por vários minutos. No entanto, cada conexão VPN oferece dois túneis para alta disponibilidade, a fim de que você possa ativar o registro em log em um túnel por vez e manter a conectividade pelo túnel inalterada. Para obter mais informações, consulte AWS Site-to-Site VPN substituições de terminais de túneis.

Para habilitar o registro de VPN durante a criação de uma nova conexão Site-to-Site VPN

Siga o procedimento do Etapa 5: criar uma conexão VPN. Durante a Etapa 9 Tunnel Options (Opções de túnel), você pode especificar todas as opções que deseja usar para ambos os túneis, incluindo as opções de VPN logging (Registro em log de VPN). Para saber mais sobre essas opções, consulte Opções de túnel para sua AWS Site-to-Site VPN conexão.

Para habilitar o registro de túneis em uma nova conexão Site-to-Site VPN usando a linha de AWS comando ou a API

- CreateVpnConnection(API de consulta do Amazon EC2)
- create-vpn-connection (AWS CLI)

Para habilitar o registro de atividades de túneis em uma conexão Site-to-Site VPN existente

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

2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Tunnel activity log (Log de atividades do túnel), selecione Enable (Habilitar).
7. Em Grupo de CloudWatch registros da Amazon, selecione o grupo de CloudWatch registros da Amazon para o qual você deseja que os registros sejam enviados.
8. (Opcional) Em Output format (Formato de saída), escolha o formato desejado para a saída do log, json ou texto.
9. Selecione Save Changes (Salvar alterações).
10. (Opcional) Repita as etapas de 4 a 9 para o outro túnel, se desejar.

Para habilitar o registro de BGP em túnel em uma conexão VPN existente Site-to-Site

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Registro BGP do túnel, selecione Ativar.
7. Em Grupo de CloudWatch registros da Amazon, selecione o grupo de CloudWatch registros da Amazon para o qual você deseja que os registros sejam enviados.
8. (Opcional) Em Output format (Formato de saída), escolha o formato desejado para a saída do log, json ou texto.
9. Selecione Save Changes (Salvar alterações).
10. (Opcional) Repita as etapas de 4 a 9 para o outro túnel, se desejar.

Para habilitar o registro de túneis em uma conexão Site-to-Site VPN existente usando a linha de AWS comando ou a API

- ModifyVpnTunnelOptions(API de consulta do Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Desativar AWS Site-to-Site VPN registros

Desabilite o log VPN em uma conexão se não quiser mais rastrear nenhuma atividade nessa conexão. Esta ação apenas desativa o registro em log e não afeta mais nada nessa conexão. Para ativar ou reativar o registro em log em uma conexão, consulte Ativar registros de Site-to-Site VPN.

Para desativar o registro de atividades de túneis em uma conexão Site-to-Site VPN

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Connections (Conexões VPN).
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Tunnel activity log (Log de atividades do túnel), desmarque Enable (Habilitar).
7. Selecione Save Changes (Salvar alterações).
8. (Opcional) Repita as etapas de 4 a 7 para o outro túnel, se desejar.

Para desativar o registro do túnel BGP em uma conexão VPN Site-to-Site

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Connections (Conexões VPN).
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Registro BGP do túnel, desmarque Habilitar.

7. Selecione Save Changes (Salvar alterações).
8. (Opcional) Repita as etapas de 4 a 7 para o outro túnel, se desejar.

Para desativar o registro de túneis em uma conexão Site-to-Site VPN usando a linha de AWS comando ou a API

- ModifyVpnTunnelOptions(API de consulta do Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Monitore AWS Site-to-Site VPN túneis usando a Amazon CloudWatch

Você pode monitorar túneis VPN usando CloudWatch, que coleta e processa dados brutos do serviço VPN em métricas legíveis e quase em tempo real. Essas estatísticas são registradas para um período de 15 meses, de forma que você possa acessar informações históricas e ganhar uma perspectiva melhor sobre como seu serviço ou aplicação Web está se saindo. Os dados métricos da VPN são enviados automaticamente CloudWatch assim que ficam disponíveis.

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

Conteúdo

- Métricas e dimensões da VPN
- Veja as métricas do Amazon CloudWatch Logs para AWS Site-to-Site VPN
- Crie CloudWatch alarmes da Amazon para monitorar túneis AWS Site-to-Site VPN

Métricas e dimensões da VPN

As CloudWatch métricas a seguir estão disponíveis para suas conexões Site-to-Site VPN.

Métrica	Descrição
`TunnelState`	O estado dos túneis. Para estática VPNs, 0 indica PARA BAIXO e 1 indica PARA CIMA. Para o BGP VPNs, 1 indica ESTABELECIDO e 0 é usado para todos os outros estados. Para

Métrica	Descrição
	ambos os tipos de VPNs, valores entre 0 e 1 indicam que pelo menos um túnel não está ativo. Unidades: valor fracionário entre 0 e 1
`TunnelDataIn` †	Os bytes recebidos no AWS lado da conexão por meio do túnel VPN de um gateway do cliente. Cada ponto de dados da métrica representa o número de bytes recebidos após o ponto de dados anterior. Use a estatística de soma para mostrar o número total de bytes recebidos durante o período. Essa métrica conta os dados após a descripto grafia. Unidades: bytes
`TunnelDataOut` †	Os bytes enviados do AWS lado da conexão pelo túnel VPN até o gateway do cliente. Cada ponto de dados da métrica represent a o número de bytes enviados após o ponto de dados anterior. Use a estatística de soma para mostrar o número total de bytes enviados durante o período. Essa métrica conta os dados antes da criptogra fia. Unidades: bytes

Métrica	Descrição
`ConcentratorBandwidthUsage`	O uso da largura de banda para uma Site-to-Site conexão VPN Concentrator. Essa métrica está disponível para conexões VPN que usam um Site-to-Site VPN Concentrator. Use a estatística Média para mostrar o uso médio da largura de banda durante o período. Unidades: bits por segundo

† Essas métricas podem relatar o uso da rede mesmo quando o túnel está inativo. Isso se deve a verificações periódicas de status realizadas no túnel e solicitações ARP e BGP em segundo plano.

Para filtrar os dados das métricas, use as dimensões a seguir.

Dimensão	Description
`VpnId`	Filtra os dados métricos pelo ID da conexão Site-to-Site VPN.
`TunnelIpAddress`	Filtra os dados da métrica pelo endereço IP do túnel para o gateway privado virtual.

Veja as métricas do Amazon CloudWatch Logs para AWS Site-to-Site VPN

Quando você cria uma conexão Site-to-Site VPN, o serviço VPN envia métricas sobre sua conexão VPN à CloudWatch medida que elas se tornam disponíveis. É possível ver as métricas da conexão VPN da maneira a seguir.

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 All metrics, escolha o namespace de métrica VPN.

4. Selecione a dimensão métrica para visualizar as métricas. Por exemplo, Métricas do túnel VPN.

> **Note**
>
> O namespace VPN não aparecerá no CloudWatch console até que uma conexão Site-to-Site VPN tenha sido criada na AWS região que você está visualizando.

Para visualizar métricas usando o AWS CLI

Em um prompt de comando, use o seguinte comando:

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

Crie CloudWatch alarmes da Amazon para monitorar túneis AWS Site-to-Site VPN

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica por um período especificado por você e envia uma notificação para um tópico do Amazon SNS com base no valor da métrica em relação a determinado limite ao longo de vários períodos.

Por exemplo, é possível criar um alarme que monitora o estado de um único túnel VPN e envia uma notificação quando o estado do túnel fica INATIVO para 3 pontos de dados em 15 minutos.

Como criar um alarme para o estado de um único túnel

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e Métricas do túnel VPN.
5. Selecione o endereço IP do túnel desejado, na mesma linha da TunnelStatemétrica. Escolha Selecionar métrica.
6. For Whenever TunnelState is... , selecione Inferior e, em seguida, digite “1" no campo de entrada abaixo de... .
7. Em Configuração adicional, defina as entradas como “3 de 3” em Pontos de dados a acionar.
8. Escolha Próximo.

9. Em Enviar uma notificação ao seguinte tópico do SNS, selecione uma lista de notificações existente ou crie uma.
10. Escolha Próximo.
11. Insira um nome para o alarme. Escolha Próximo.
12. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Você pode criar um alarme que monitore o estado da conexão Site-to-Site VPN. Por exemplo, é possível criar um alarme que envie uma notificação quando o status de um ou de ambos os túneis estiver INATIVO por um período de 5 minutos.

Para criar um alarme para o estado da conexão Site-to-Site VPN

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Connection Metrics (Métricas de conexão VPN).
5. Selecione sua conexão Site-to-Site VPN e a TunnelStatemétrica. Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Maximum (Máximo).

   Como alternativa, se você configurou sua conexão Site-to-Site VPN para que os dois túneis estejam ativos, você pode especificar uma estatística de Mínimo para enviar uma notificação quando pelo menos um túnel estiver inativo.
7. Em Sempre que, escolha Inferior ou igual a (<=) e insira 0 (ou 0,5 para quando pelo menos um túnel estiver inativo). Escolha Próximo.
8. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
9. Insira um nome e uma descrição para o alarme. Escolha Próximo.
10. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Além disso, você pode criar alarmes que monitoram a quantidade de tráfego que está entrando ou saindo de um túnel VPN. Por exemplo, o alarme a seguir monitora a quantidade de tráfego de sua rede que está entrando no túnel VPN e envia uma notificação quando o número de bytes atingir o limite de 5.000.000 durante o período de 15 minutos.

Para criar um alarme para tráfego de rede de entrada

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Tunnel Metrics (Métricas de túnel VPN).
5. Selecione o endereço IP do túnel VPN e a TunnelDataInmétrica. Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Sum (Soma).
7. Em Period (Período), selecione 15 minutes (15 minutos).
8. Em Whenever (Sempre que), escolha Greater/Equal (Maior que/igual a) (>=) e insira 5000000. Escolha Próximo.
9. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
10. Insira um nome e uma descrição para o alarme. Escolha Próximo.
11. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

O alarme a seguir monitora a quantidade de tráfego de sua rede que está saindo do túnel VPN e envia uma notificação quando o número de bytes for inferior a 1.000.000 durante o período de 15 minutos.

Para criar um alarme para tráfego de rede de saída

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Tunnel Metrics (Métricas de túnel VPN).
5. Selecione o endereço IP do túnel VPN e a TunnelDataOutmétrica. Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Sum (Soma).
7. Em Period (Período), selecione 15 minutes (15 minutos).
8. Em Whenever (Sempre que), escolha Lower/Equal (Inferior/igual) (<=) e insira `1000000`. Escolha Próximo.

9. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
10. Insira um nome e uma descrição para o alarme. Escolha Próximo.
11. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Para obter mais exemplos de criação de alarmes, consulte Criação de CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

AWS Health e AWS Site-to-Site VPN eventos

AWS Site-to-Site VPN envia notificações automaticamente para Health Dashboardo. Esse painel não requer configuração e está pronto para ser usado por AWS usuários autenticados. É possível configurar várias ações em resposta às notificações de eventos por meio do Health Dashboard.

O Health Dashboard fornece os seguintes tipos de notificações para suas conexões VPN:

- Notificações de substituição de endpoint do túnel
- Notificações de VPN de túnel único

Notificações de substituição de endpoint do túnel

Você recebe uma notificação de substituição de endpoint de túnel Health Dashboard quando um ou ambos os endpoints de túnel VPN em sua conexão VPN são substituídos. Um endpoint de túnel é substituído quando a AWS executa atualizações de túnel ou quando você modifica a conexão VPN. Para obter mais informações, consulte AWS Site-to-Site VPN substituições de terminais de túneis.

Quando uma substituição do endpoint do túnel é concluída, AWS envia a notificação de substituição do endpoint do túnel por meio de um Health Dashboard evento.

Notificações de VPN de túnel único

Uma conexão Site-to-Site VPN consiste em dois túneis para redundância. É altamente recomendável configurar ambos os túneis para alta disponibilidade. Se sua conexão VPN tiver um túnel ativado e o outro desativado por mais de uma hora em um dia, você receberá uma notificação de túnel único de VPN mensal por meio de um evento Health Dashboard . Esse evento será atualizado diariamente com todas as novas conexões VPN detectadas como um único túnel, com notificações enviadas

semanalmente. A cada mês será criado um evento, o que apagará todas as conexões VPN que não forem mais detectadas como um único túnel.

AWS Site-to-Site VPN cotas

Sua AWS conta tem as seguintes cotas, anteriormente chamadas de limites, relacionadas à Site-to-Site VPN. A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas 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.

Site-to-Site Recursos de VPN

Nome	Padrão	Ajustável
Gateways do cliente por região	50	Sim
Gateways privados virtuais por região	5	Sim
Site-to-Site Conexões VPN por região	50	Sim
Site-to-Site Conexões VPN por gateway privado virtual	10	Sim
Conexões Site-to-Site VPN aceleradas por região	10	Sim
Conexões Site-to-Site VPN não associadas por região	10	Sim
Conexões de túnel de grande largura de banda por região	50	Sim
Site-to-Site Concentradores de VPN por região	50	Sim
Site-to-Site Concentradores VPN por Transit Gateway ou Cloud WAN	5	Sim
Sites remotos por Site-to-Site VPN Concentra tor	100	Sim

> **Note**
>
> As conexões aceleradas e não associadas contam para a cota total de conexões Site-to-Site VPN por região.

Um gateway privado virtual pode ser associado a uma VPC de cada vez. Para conectar a mesma conexão Site-to-Site VPN a várias VPCs, recomendamos que você explore o uso de um gateway de trânsito. Para obter mais informações, consulte Gateways de trânsito em Gateways de trânsito da Amazon VPC.

Site-to-Site As conexões VPN em um gateway de trânsito estão sujeitas ao limite total de anexos do gateway de trânsito. Para obter mais informações, consulte Cotas para os gateways de trânsito.

Rotas

As fontes de rota publicadas incluem rotas da VPC, outras rotas da VPN e rotas de interfaces virtuais do Direct Connect. As rotas publicadas vêm da tabela de rotas associada ao anexo da VPN.

> **Note**
>
> Se você estiver usando um gateway privado virtual e a propagação de rotas estiver ativada na tabela de rotas da VPC, as rotas dinâmicas e estáticas serão adicionadas automaticamente à sua conexão VPN, até o limite da tabela de rotas da VPC. Consulte Cotas da Amazon VPC no Guia do usuário da Amazon VPC para obter mais detalhes.

Nome	Padrão	Ajustável
Rotas dinâmicas anunciadas de um dispositivo de gateway do cliente para uma conexão Site-to-Site VPN em um gateway privado virtual	100	Não
Rotas anunciadas de uma conexão Site-to-Site VPN em um gateway privado virtual para um dispositivo de gateway do cliente	1.000	Não

Nome	Padrão	Ajustável
Rotas dinâmicas anunciadas de um dispositivo de gateway do cliente para uma conexão Site-to-Site VPN em um gateway de trânsito	1.000	Não
Rotas anunciadas de uma conexão Site-to-Site VPN em um gateway de trânsito para um dispositivo de gateway do cliente	5.000	Não
Rotas estáticas de um dispositivo de gateway do cliente para uma conexão Site-to-Site VPN em um gateway privado virtual	100	Não

Largura de banda e taxa de transferência

Há muitos fatores que podem afetar a largura de banda obtida por meio de uma conexão Site-to-Site VPN, incluindo, mas não se limitando a: tamanho do pacote, combinação de tráfego (TCP/UDP), definição ou limitação de políticas em redes intermediárias, clima da Internet e requisitos específicos de aplicativos.

Nome	Padrão	Ajustável
Largura de banda máxima por túnel VPN Concentrator VPN	Até 100 Mbps	Não
Máximo de pacotes por segundo (PPS) por túnel VPN Concentrator VPN	Até 10 mil	Não
Largura de banda máxima por túnel VPN padrão	Até 1,25 Gbps	Não
Máximo de pacotes por segundo (PPS) por túnel VPN padrão	Até 140.000	Não
Largura de banda máxima por túnel VPN de grande largura de banda	Até 5 Gbps	Não

Nome	Padrão	Ajustável
Máximo de pacotes por segundo (PPS) por túnel VPN de grande largura de banda	Até 400.000	Não

Para conexões Site-to-Site VPN em um gateway de trânsito, você pode usar o ECMP para obter maior largura de banda VPN agregando vários túneis VPN. Para usar o ECMP, a conexão VPN deve ser configurada para roteamento dinâmico. O ECMP não é compatível com conexões VPN que usam roteamento estático. Para obter mais informações, consulte Gateways de trânsito.

> **Note**
>
> IPv6 VPNs suportam os mesmos limites de taxa de transferência (Gbps e PPS), MTU e rota que. IPv4 VPNs Não há diferenças de desempenho IPv4 entre conexões IPv6 VPN.

Unidade de transmissão máxima (MTU)

Site-to-Site A VPN suporta uma unidade de transmissão máxima (MTU) de 1446 bytes e um tamanho máximo de segmento (MSS) correspondente de 1406 bytes. No entanto, certos algoritmos que usam cabeçalhos TCP maiores podem efetivamente reduzir esse valor máximo. Para evitar fragmentação, recomendamos que você configure a MTU e o MSS com base nos algoritmos selecionados. Para obter mais detalhes sobre MTU, MSS e os valores ótimos, consulte Melhores práticas para um dispositivo de gateway AWS Site-to-Site VPN do cliente.

Não há compatibilidade com frames jumbo. Para obter mais informações, consulte Jumbo frames no Guia do EC2 usuário da Amazon.

Uma conexão Site-to-Site VPN não é compatível com o Path MTU Discovery.

As limitações da MTU se aplicam tanto às conexões VPN IPv4 quanto às conexões IPv6 VPN.

Recursos de cota adicionais

Para cotas relacionadas a gateways de trânsito, incluindo o número de anexos em um gateway de trânsito, consulte Cotas para seus gateways de trânsito no Guia dos gateways de trânsito da Amazon VPC.

Para obter as cotas adicionais da VPC, consulte Cotas da Amazon VPC no Guia do usuário da Amazon VPC.

Histórico de documentos do Guia do usuário da Site-to-Site VPN

A tabela a seguir descreve as atualizações AWS Site-to-Site VPN do Guia do usuário.

Alteração	Descrição	Data
Site-to-Site Concentradores VPN	Site-to-Site Os concentradores VPN fornecem um hub centralizado para gerenciar várias conexões VPN com escalabilidade aprimorada e arquitetura de rede simplificada.	15 de novembro de 2025
Site-to-Site Suporte de VPN para túneis de grande largura de banda	Site-to-Site A VPN agora suporta largura de banda de túnel grande, permitindo gateway de trânsito e anexos VPN Cloud WAN com taxa de transferência de até 5 Gbps.	25 de setembro de 2025
IPv6 suporte para AWS Site-to-Site VPN para túnel externo IPs	Site-to-Site A VPN agora suporta IPv6 endereços para o túnel externo IPs nas conexões VPN Transit Gateway e Cloud WAN. Isso permite a IPv6 migração completa com IPv6 endereços para o túnel externo IPs e o pacote interno IPs (IPv6-in-IPv6), bem como o túnel IPv6 externo IPs com o pacote IPv4 interno IPs (IPv4-in-). IPv6	1.º de julho de 2025

Atualizou a política AWSVPCS2 SVpn ServiceRolePolicy AWS gerenciada	Foram adicionadas novas permissões à política AWS gerenciada, permitindo que a Site-to-Site VPN gerencie o segredo AWS Secrets Manager gerenciado da conexão VPN.	27 de maio de 2025
Opções atualizadas de armazenamento de chaves pré-compartilhadas	Site-to-Site A VPN agora suporta AWS Secrets Manager o armazenamento de uma chave pré-compartilhada.	27 de maio de 2025
Informações sobre a VPN clássica removidas	As informações sobre a VPN clássica foram removidas do guia.	19 de janeiro de 2023
Exemplo de mensagens de log da VPN	Registros de amostra adicionados para conexões Site-to-Site VPN.	9 de dezembro de 2022

Utilitário de configuração de download atualizado	Site-to-Site Os clientes de VPN podem gerar modelos de configuração para dispositivos Customer Gateway (CGW) compatíveis, facilitando a criação de conexões VPN com o.AWS Esta atualizaç ão adiciona suporte aos parâmetros do Internet Key Exchange versão 2 (IKEv2) para muitos dispositi vos CGW populares e inclui dois novos APIs — e. GetVpnConnectionDe viceTypes GetVpnCon nectionDeviceSampleConfigur ation	21 de setembro de 2021
Notificações de conexão VPN	Site-to-Site A VPN envia automaticamente notificações sobre sua conexão VPN para Health Dashboard o.	29 de outubro de 2020
Iniciação do túnel da VPN	Você pode configurar seus túneis VPN para que os AWS túneis apareçam.	27 de agosto de 2020
Modificar opções da conexão VPN	Você pode modificar as opções de conexão da sua conexão Site-to-Site VPN.	27 de agosto de 2020
Algoritmos de segurança adicionais	É possível aplicar algoritmos de segurança adicionais aos túneis VPN.	14 de agosto de 2020

IPv6 apoio	Seus túneis VPN podem suportar o IPv6 tráfego dentro dos túneis.	12 de agosto de 2020
Guias de mesclagem AWS Site-to-Site VPN	Esta versão mescla o conteúdo do Guia do Administrador de AWS Site-to-Site VPN Rede com este guia.	31 de março de 2020
Conexões aceleradas AWS Site-to-Site VPN	Você pode ativar a aceleração para sua AWS Site-to-Site VPN conexão.	3 de dezembro de 2019
Modificar opções de AWS Site-to-Site VPN túnel	Você pode modificar as opções de um túnel VPN em uma AWS Site-to-Site VPN conexão. Também é possível configurar opções de túnel adicionais.	29 de agosto de 2019
Autoridade de Certificação Privada da AWS suporte a certificados privados	Você pode usar um certificado privado de Autoridade de Certificação Privada da AWS para autenticar sua VPN.	15 de agosto de 2019
Novo guia do usuário de Site-to-Site VPN	Esta versão separa o conteúdo AWS Site-to-Site VPN(anteriormente conhecido como VPN AWS gerenciada) do Guia do usuário da Amazon VPC.	18 de dezembro de 2018
Modificar o gateway de destino	Você pode modificar o gateway de destino da AWS Site-to-Site VPN conexão.	18 de dezembro de 2018

ASN personalizado	Quando você cria um gateway privado virtual, é possível especificar o Número de sistema autônomo (ASN) privado para o lado da Amazon do gateway.	10 de outubro de 2017
Opções de túnel VPN	É possível especificar blocos CIDR de túnel e personalizar as chaves pré-compartilhadas para seus túneis VPN.	3 de outubro de 2017
Métricas da VPN	Você pode ver CloudWatch as métricas de suas conexões VPN.	15 de maio de 2017
Melhorias do VPN	Uma conexão VPN agora é compatível com a função de criptografia AES de 256 bits, função hashing SHA-256, NAT transversal e outros grupos Diffie-Hellman durante a Fase 1 e a Fase 2 de uma conexão. Além disso, agora você pode usar o mesmo endereço IP do gateway do cliente para cada conexão VPN que usa o mesmo dispositivo de gateway do cliente.	28 de outubro de 2015

Conexões VPN usando configuração de roteamento estático	Você pode criar conexões IPsec VPN com a Amazon VPC usando configurações de roteamento estático. Anteriormente, as conexões VPN exigiam o uso do Protocolo de Gateway da Borda (BGP). Agora oferecemos compatibilidade com ambos os tipos de conexões e você pode estabelecer conectividade de dispositivos que não oferece suporte ao BGP, incluindo Cisco ASA e Microsoft Windows Server 2008 R2.	13 de setembro de 2012
Propagação automática de rotas	Agora você pode configurar a propagação automática de rotas de sua VPN e AWS Direct Connect links para suas tabelas de roteamento de VPC.	13 de setembro de 2012
Site-to-Site VPN CloudHub e conexões VPN redundantes	É possível se comunicar seguramente de um local para outro com ou sem uma VPC. É possível usar conexões VPN redundantes para oferecer à sua VPC uma conexão tolerante a falhas.	29 de setembro de 2011

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.