Whitepaper da AWS

Opções de conectividade da Amazon Virtual Private Cloud

Opções de conectividade da Amazon Virtual Private Cloud: Whitepaper da AWS

Table of Contents

Opções de conectividade da Amazon Virtual Private Cloud

Data de publicação: 5 de abril de 2023 (Revisões do documento)

Resumo

A Amazon Virtual Private Cloud (Amazon VPC) permite que os clientes provisionem uma seção privada e isolada da nuvem da Amazon Web Services (AWS), na qual eles podem lançar recursos da AWS em uma rede virtual usando intervalos de endereços IP definidos pelo cliente. A Amazon VPC oferece aos clientes várias opções para conectar suas redes virtuais da AWS com outras redes remotas. Este documento descreve várias opções comuns de conectividade de rede disponíveis para nossos clientes. Isso inclui opções de conectividade para integrar redes remotas de clientes com o Amazon VPC e conectar vários Amazon VPCs em uma rede virtual contígua.

Este whitepaper é destinado a arquitetos e engenheiros de redes corporativas ou administradores da Amazon VPC que gostariam de analisar as opções de conectividade disponíveis. Ele fornece uma visão geral das várias opções para facilitar as discussões sobre conectividade de rede, bem como dicas para documentação e recursos adicionais com informações ou exemplos mais detalhados.

Introdução

A Amazon VPC fornece várias opções de conectividade de rede para você usar, dependendo dos seus projetos e requisitos de rede atuais. Essas opções de conectividade incluem o uso da Internet ou de uma AWS Direct Connect conexão como backbone da rede e o encerramento da conexão na AWS ou em endpoints de rede gerenciados pelo usuário. Além disso, com a AWS, você pode escolher como o roteamento de rede é fornecido entre a Amazon VPC e suas redes, aproveitando os serviços da AWS ou equipamentos e rotas de rede gerenciados pelo usuário. Este whitepaper considera as seguintes opções com uma visão geral e uma comparação de alto nível de cada uma:

- Opções de conectividade entre a rede e a Amazon VPC
  - VPN site a site da AWS — descreve o estabelecimento de uma conexão VPN IPsec gerenciada do seu equipamento de rede em uma rede remota com a Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN — Descreve o estabelecimento de uma conexão VPN IPsec gerenciada do seu equipamento de rede em uma rede remota até um hub de rede regional para Amazon VPCs, usando. AWS Transit Gateway
  - AWS Direct Connect- Descreve o estabelecimento de uma conexão lógica e privada de sua rede remota com a Amazon VPC, usando. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway— Descreve o estabelecimento de uma conexão lógica e privada de sua rede remota com um hub de rede regional para Amazon VPCs, usando AWS Direct Connect e. AWS Transit Gateway
  - AWS Direct Connect+ VPN site a site da AWS — descreve o estabelecimento de uma conexão privada e criptografada da sua rede remota com a Amazon VPC, usando uma VPN site a site da AWS. AWS Direct Connect
  - AWS Direct ConnectAWS Transit Gateway + VPN site a site da AWS— Descreve o estabelecimento de uma conexão privada e criptografada da sua rede remota com um hub de rede regional para Amazon VPCs, usando AWS Direct Connect e. AWS Transit Gateway
  - AWS VPN CloudHub— Descreve o estabelecimento de um hub-and-spoke modelo para conectar filiais remotas.
  - Software VPN— Descreve o estabelecimento de uma conexão VPN do seu equipamento em uma rede remota com um dispositivo VPN de software gerenciado pelo usuário executado dentro de uma Amazon VPC.
  - AWS Transit Gateway + Soluções SD-WAN- Descreve a integração de soluções de rede de área ampla definidas por software (SD-WAN) para interconectar vários locais remotos a um hub de

rede regional para Amazon VPCs, usando o AWS backbone ou a Internet como uma rede de trânsito.

- Opções de conectividade entre Amazon VPC e Amazon VPC
  - emparelhamento da VPC— Descreve a conexão das Amazon VPCs dentro e entre regiões usando o recurso de emparelhamento da Amazon VPC.
  - AWS Transit Gateway— Descreve a conexão de Amazon VPCs dentro e entre AWS Transit Gateway regiões usando um hub-and-spoke modelo.
  - AWS PrivateLink— Descreve a conexão de Amazon VPCs com endpoints de interface VPC e serviços de endpoint VPC.
  - Software VPN— Descreve a conexão de Amazon VPCs usando conexões VPN estabelecidas entre dispositivos VPN de software gerenciados pelo usuário executados dentro de cada Amazon VPC.
  - Software VPN para AWS VPN site-to-site— Descreve a conexão das Amazon VPCs com uma conexão VPN estabelecida entre um dispositivo VPN de software gerenciado pelo usuário em uma Amazon VPC e uma VPN AWS Site-to-Site conectada à outra Amazon VPC.
- Opções de acesso remoto de software à Amazon VPC
  - AWS Client VPN— Descreve a conexão do acesso remoto do software à Amazon VPC, utilizando o AWS Client VPN.
  - Cliente de software VPN— Descreve a conexão do acesso remoto ao software à Amazon VPC, aproveitando dispositivos VPN de software gerenciados pelo usuário.
- VPC de trânsito- Descreve o estabelecimento de uma rede de trânsito global na AWS usando uma VPN de software em conjunto com uma VPN gerenciada pela AWS.
- WAN na nuvem da AWS- Descreve o estabelecimento de uma rede de área ampla (WAN) gerenciada para criar, gerenciar e monitorar facilmente interconexões globais entre recursos em Amazon VPCs, datacenters e filiais remotas.

Opções de conectividade entre a rede e a Amazon VPC

Esta seção fornece padrões de design para conectar redes remotas ao seu ambiente Amazon VPC. Essas opções são úteis para integrar recursos da AWS com seus serviços locais existentes (por exemplo, monitoramento, autenticação, segurança, dados ou outros sistemas) estendendo suas redes internas para a nuvem da AWS. Essa extensão de rede também permite que seus usuários internos se conectem perfeitamente aos recursos hospedados na AWS, assim como qualquer outro recurso interno.

A conectividade VPC com redes remotas de clientes é melhor alcançada ao usar intervalos de IP não sobrepostos para cada rede conectada. Por exemplo, se você quiser conectar uma ou mais VPCs à sua rede corporativa, verifique se elas estão configuradas com intervalos exclusivos de roteamento entre domínios sem classe (CIDR). Recomendamos alocar um único bloco CIDR contíguo e não sobreposto para ser usado por cada VPC. Para obter informações adicionais sobre o roteamento e as restrições da Amazon VPC, consulte as Perguntas frequentes da Amazon VPC.

Opção	Caso de uso	Vantagens	Limitações
AWS Site-to-Site VPN	A AWS gerenciou a conexão VPN IPsec pela Internet para uma VPC individual	Reutilize equipamentos e processos de VPN existentes Reutilize as conexões de internet existentes Serviço de VPN de alta disponibilidade gerenciado pela AWS Suporta rotas estáticas ou políticas dinâmicas de emparelhamento e roteamento do Border Gateway Protocol (BGP)	A latência, a variabilidade e a disponibilidade da rede dependem das condições da Internet Você é responsável por implementar redundância e failover (se necessário) O dispositivo remoto deve suportar BGP de salto único (ao aproveitar o BGP para roteamento dinâmico)

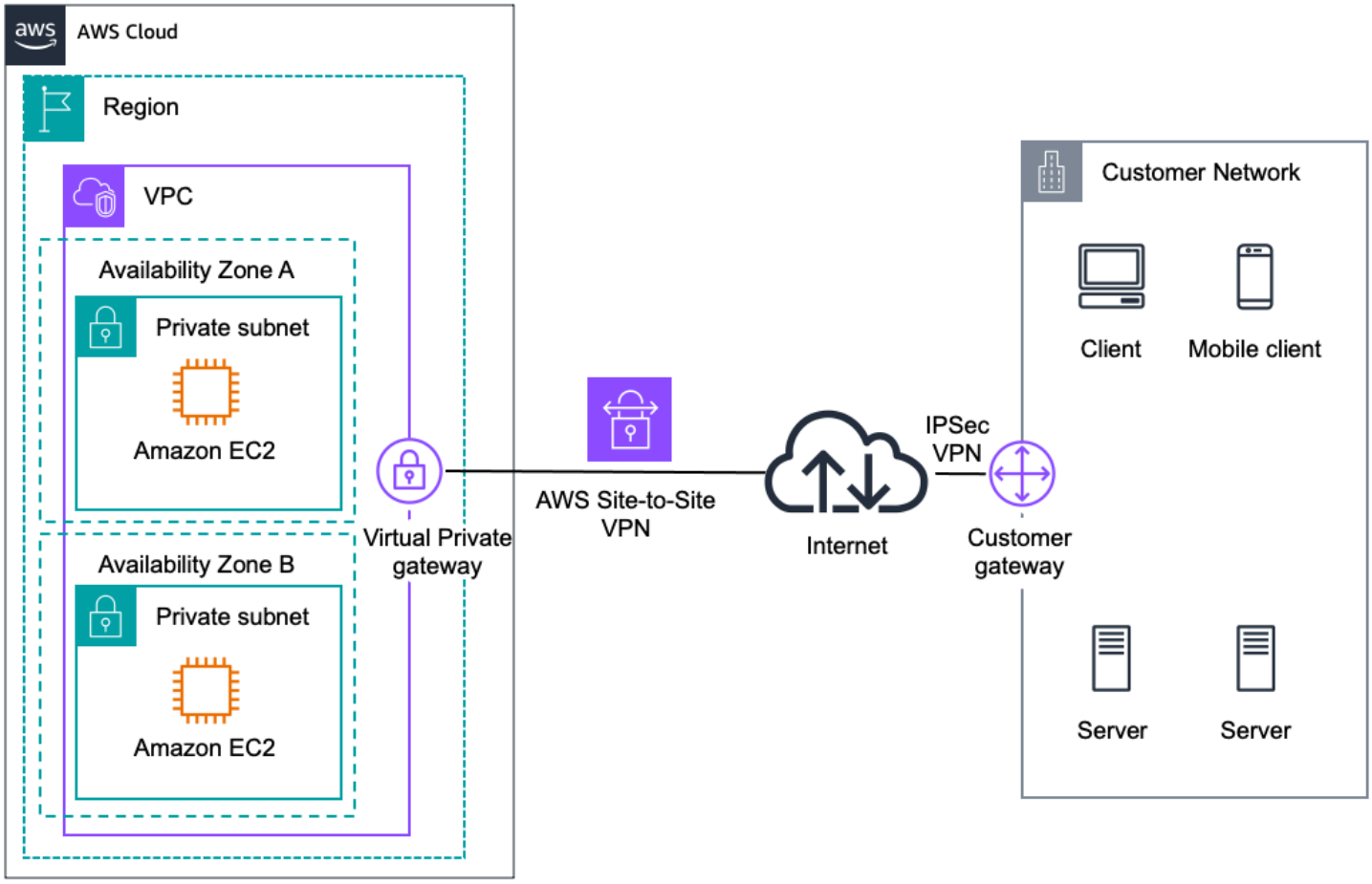
Opção	Caso de uso	Vantagens	Limitações
AWS Transit Gateway + VPN site a site da AWS	A AWS gerenciou a conexão VPN IPsec pela Internet com um roteador regional para várias VPCs	Igual à opção anterior Hub de rede regional gerenciado pela AWS de alta disponibilidade e escalabilidade para até 5.000 anexos	Igual à opção anterior
AWS Direct Connect	Conexão de rede dedicada em linhas privadas	Desempenho de rede mais previsível Custos reduzidos de largura de banda Suporta políticas de emparelhamento e roteamento do BGP	Pode exigir que relacionamentos adicionais com provedores de telecomunicações e hospedagem ou que novos circuitos de rede sejam provision ados
AWS Direct Connect + AWS Transit Gateway	Conexão de rede dedicada por linhas privadas ao roteador regional para várias VPCs	Igual à opção anterior Hub de rede regional gerenciado pela AWS de alta disponibilidade e escalabilidade para até 5.000 anexos	Igual à opção anterior

Opção	Caso de uso	Vantagens	Limitações
AWS Direct Connect + VPN site a site da AWS	Conexão VPN IPsec em linhas privadas	Desempenho de rede mais previsível Custos reduzidos de largura de banda Suporta políticas de emparelhamento e roteamento do BGP em AWS Direct Connect Reutilize equipamentos e processos de VPN existentes Serviço de VPN de alta disponibilidade gerenciado pela AWS Suporta rotas estáticas ou políticas dinâmicas de emparelhamento e roteamento do Border Gateway Protocol (BGP) na conexão VPN	Pode exigir que relacionamentos adicionais com provedores de telecomunicações e hospedagem ou que novos circuitos de rede sejam provisionados Você é responsável por implementar redundância e failover (se necessário) O dispositivo remoto deve suportar BGP de salto único (ao aproveitar o BGP para roteamento dinâmico)
AWS Direct ConnectAWS Transit Gateway + VPN site a site da AWS	Conexão VPN IPsec por linhas privadas ao roteador regional para várias VPCs	Igual à opção anterior Hub de rede regional gerenciado pela AWS de alta disponibilidade e escalabilidade para até 5.000 anexos	Igual à opção anterior

Opção	Caso de uso	Vantagens	Limitações
AWS VPN CloudHub	Conecte filiais remotas em um hub-and-spoke modelo para conectividade primária ou de backup	Reutilize conexões e AWS VPN conexões de internet existentes Serviço de VPN de alta disponibilidade gerenciado pela AWS Suporta BGP para troca de rotas e prioridades de roteamento	A latência, a variabilidade e a disponibilidade da rede dependem da Internet Os endpoints de filiais gerenciados pelo usuário são responsáveis pela implementação de redundância e failover (se necessário)
AWS Transit Gateway + Soluções SD-WAN	Conecte filiais e escritórios remotos com uma rede de área ampla definida por software usando o AWS backbone ou a Internet como uma rede de trânsito.	Oferece suporte a uma variedade maior de fornecedores, produtos e protocolos de SD-WAN Algumas soluções de fornecedores têm integração com os serviços nativos da AWS.	Você é responsável pela implementação de HA (alta disponibilidade) dos dispositivos SD-WAN se eles forem colocados em uma Amazon VPC.
Software VPN	Conexão VPN baseada em dispositivo de software pela Internet	Oferece suporte a uma variedade maior de fornecedores, produtos e protocolos de VPN Solução totalmente gerenciada pelo cliente	Você é responsável pela implementação de soluções HA (alta disponibilidade) para todos os endpoints de VPN (se necessário)

AWS Site-to-Site VPN

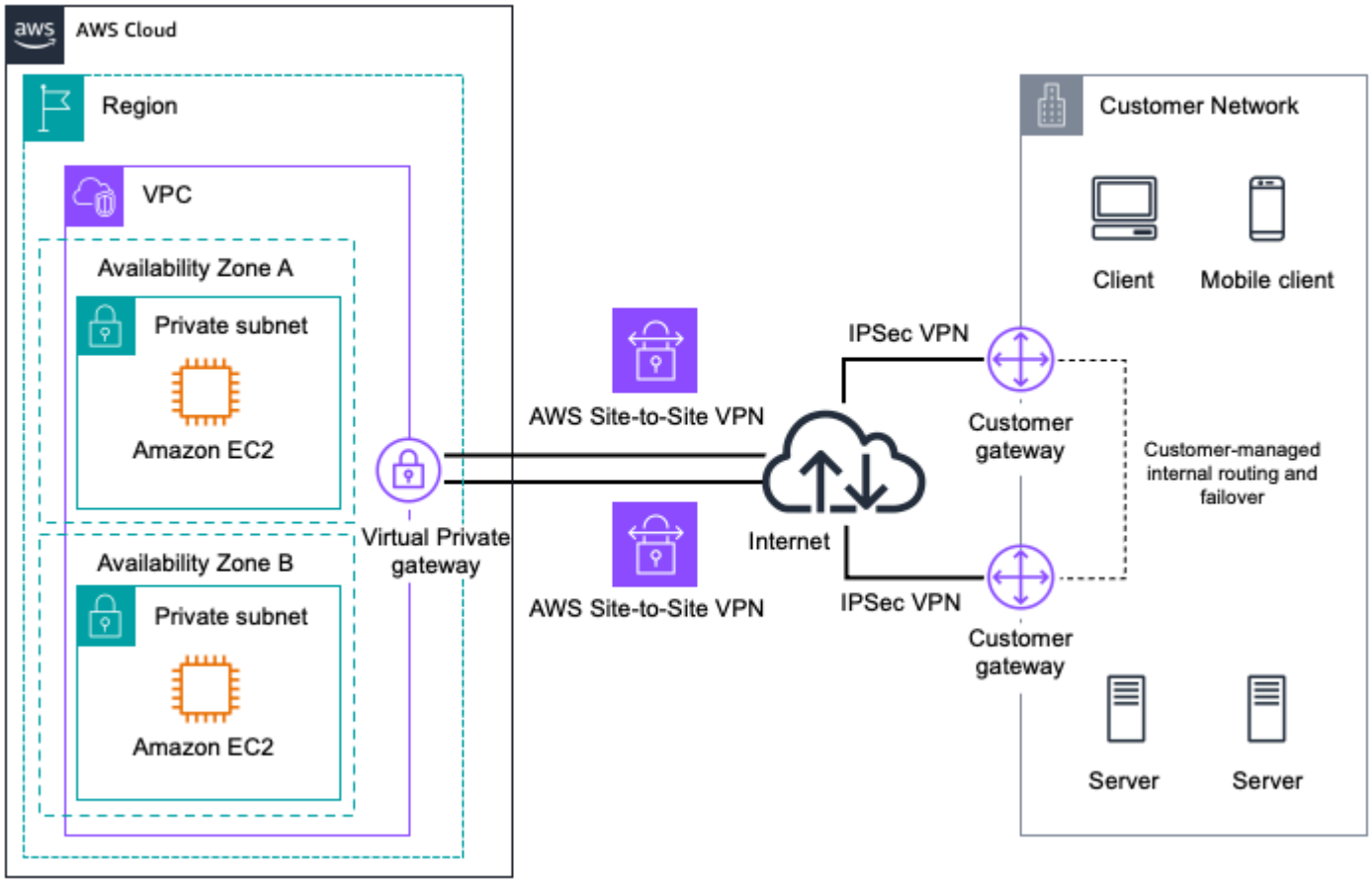
A Amazon VPC oferece a opção de criar uma conexão VPN IPsec entre suas redes remotas e a Amazon VPC pela Internet, conforme mostrado na figura a seguir.



AWS Managed VPN

Considere adotar essa abordagem quando quiser tirar proveito de um endpoint de VPN gerenciado pela AWS que inclui redundância automatizada e failover incorporados ao lado da AWS da conexão VPN.

O gateway privado virtual também suporta e incentiva várias conexões de gateway de usuário para que você possa implementar redundância e failover no seu lado da conexão VPN, conforme mostrado na figura a seguir.



Redundant AWS Site-to-Site VPN Connections

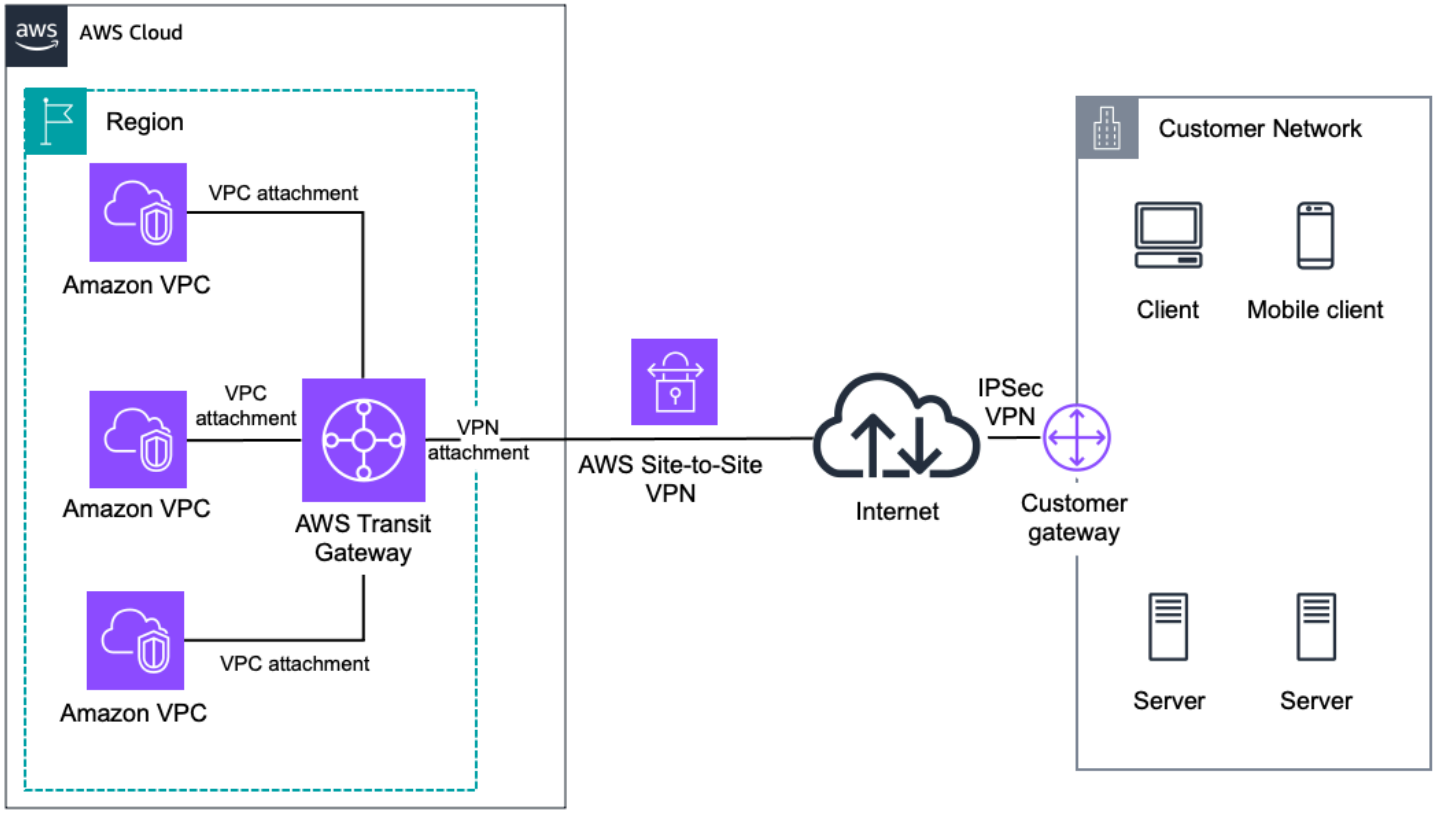
As opções de roteamento dinâmico e estático são fornecidas para oferecer flexibilidade em sua configuração de roteamento. O roteamento dinâmico usa o emparelhamento BGP para trocar informações de roteamento entre a AWS e esses endpoints remotos. Com o roteamento dinâmico, você também pode especificar prioridades, políticas e pesos (métricas) de roteamento em seus anúncios do BGP e influenciar o caminho da rede entre suas redes e a AWS. É importante observar que, quando você usa o BGP, as sessões IPsec e BGP devem ser encerradas no mesmo dispositivo de gateway de usuário, portanto, ele deve ser capaz de encerrar as sessões IPsec e BGP.

Recursos adicionais do

- Guia do usuário da AWS Site-to-Site VPN
- Requisitos para dispositivos de gateway do cliente
- Dispositivos de gateway do cliente testados com o Amazon VPC

AWS Transit Gateway + VPN site a site da AWS

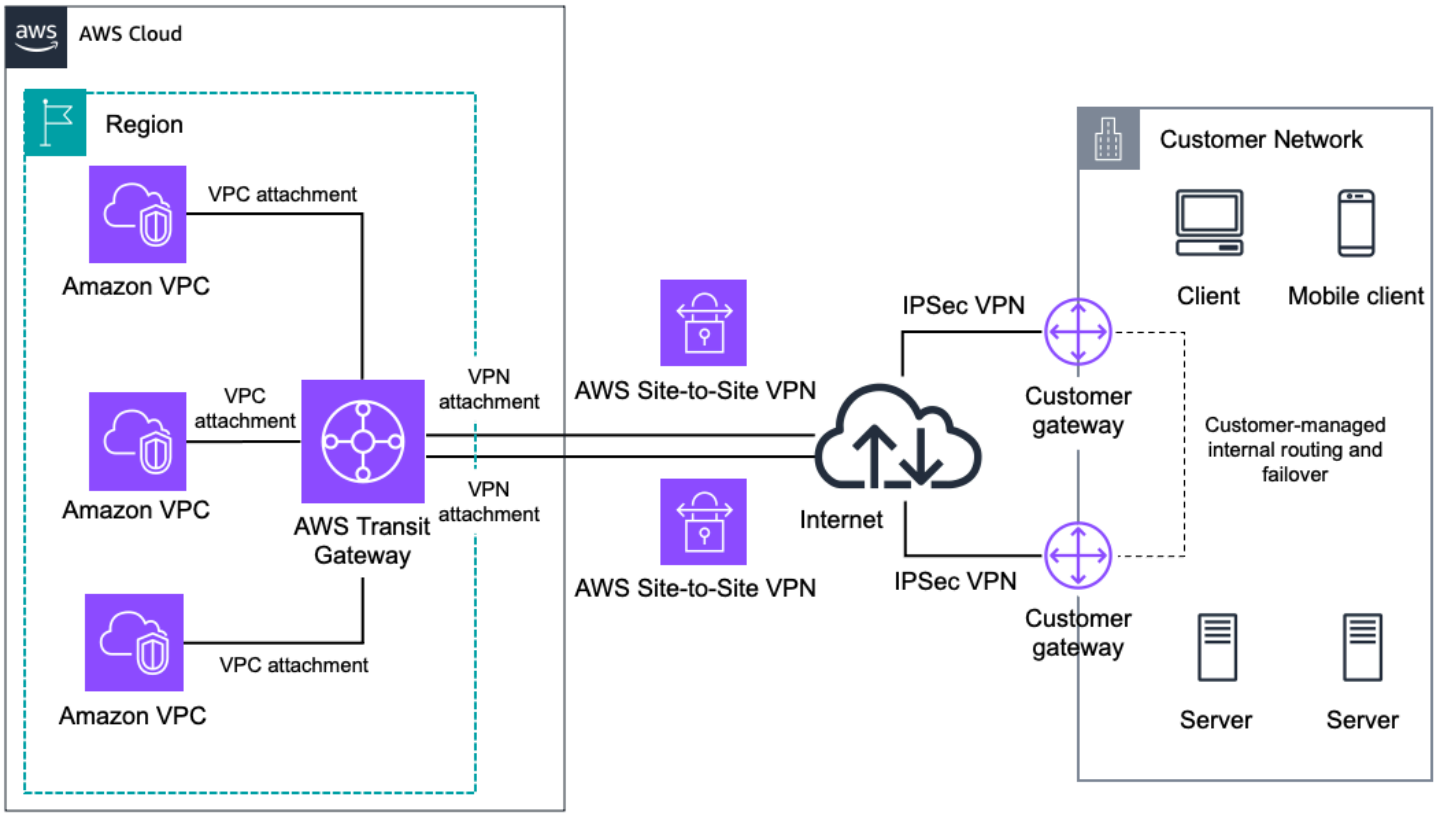
O AWS Transit Gateway é um hub de trânsito de rede regional gerenciado pela AWS, de alta disponibilidade e escalabilidade, usado para interconectar VPCs e redes de clientes. O AWS Transit Gateway + VPN, usando o anexo VPN Transit Gateway, oferece a opção de criar uma conexão VPN IPsec entre sua rede remota e o Transit Gateway pela Internet, conforme mostrado na figura a seguir.



AWS Transit Gateway and AWS Site-to-Site VPN

Considere usar essa abordagem quando quiser tirar proveito de um endpoint de VPN gerenciado pela AWS para se conectar a várias VPCs na mesma região sem o custo adicional e o gerenciamento de várias conexões VPN IPsec com várias VPCs da Amazon.

O AWS Transit Gateway também oferece suporte e incentiva várias conexões de gateway de usuário para que você possa implementar redundância e failover no seu lado da conexão VPN, conforme mostrado na figura a seguir.



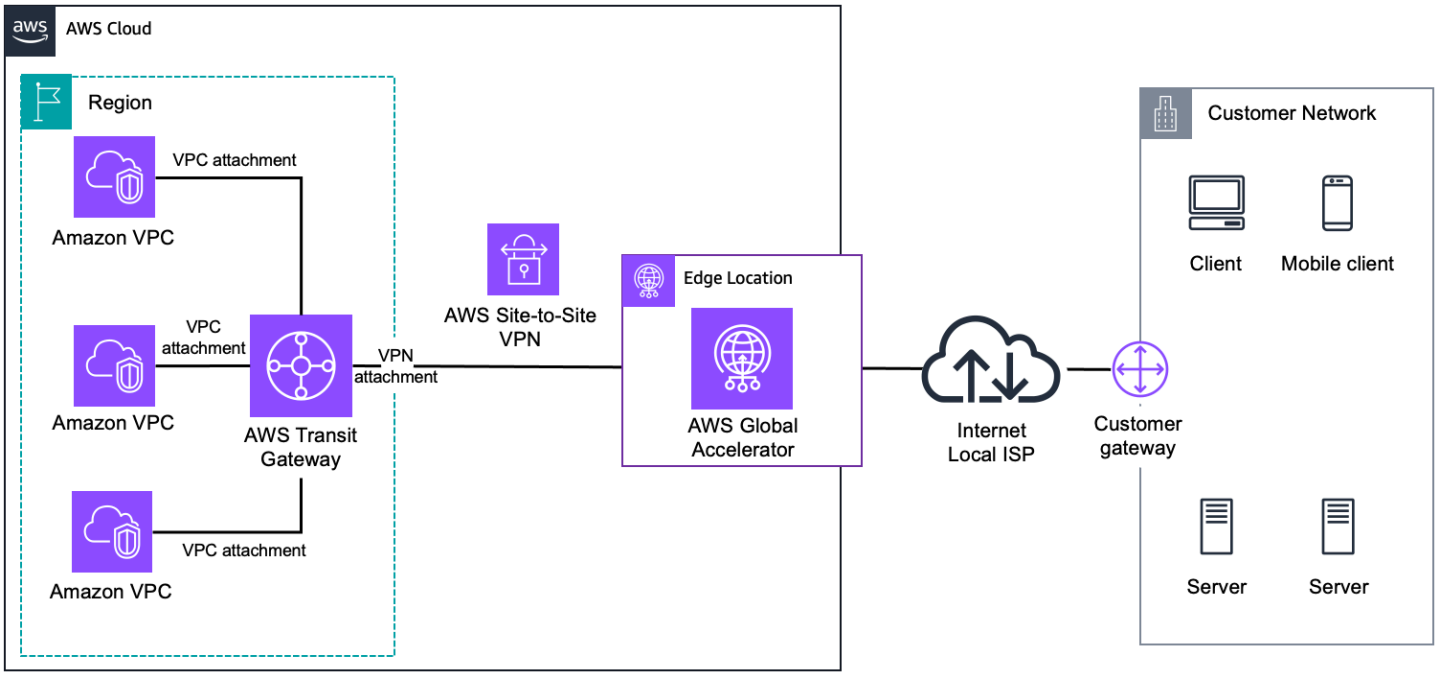
AWS Transit Gateway and Redundant VPN

As opções de roteamento dinâmico e estático são fornecidas para oferecer flexibilidade em sua configuração de roteamento no anexo IPsec do Transit Gateway VPN. O roteamento dinâmico usa o emparelhamento BGP para trocar informações de roteamento entre a AWS e esses endpoints remotos. Com o roteamento dinâmico, você também pode especificar prioridades, políticas e pesos (métricas) de roteamento em seus anúncios do BGP e influenciar o caminho da rede entre suas redes e a AWS. É importante observar que, quando você usa o BGP, as sessões IPsec e BGP devem ser encerradas no mesmo dispositivo de gateway de usuário, portanto, ele deve ser capaz de encerrar as sessões IPsec e BGP.

Por conexão VPN, você pode atingir 1,25 Gbps de taxa de transferência e 140.000 pacotes por segundo. Ao encerrar as conexões VPN no Transit Gateway, você pode usar o roteamento Equal Cost Multi-Path (ECMP) para obter uma maior largura de banda VPN agregando vários túneis VPN. Para usar o ECMP, você precisa configurar o roteamento dinâmico nas conexões VPN — o ECMP não é suportado usando roteamento estático.

Além disso, você pode ativar a aceleração em suas conexões VPN Site-to-Site da AWS. Uma conexão VPN acelerada usa o AWS Global Accelerator para rotear o tráfego da sua rede para um ponto de presença da AWS que esteja mais próximo do seu dispositivo de gateway do cliente.

Você pode usar essa opção para evitar interrupções na rede que podem ocorrer quando o tráfego é roteado pela Internet pública. A aceleração só é compatível com conexões VPN conectadas a um Transit Gateway, conforme mostrado na figura a seguir:



Accelerated AWS Site-to-Site VPN

Por último, em relação ao endereçamento IP, as conexões VPN Site-to-Site em AWS Transit Gateway an suportam tráfego IPv4 e IPv6. As seguintes regras se aplicam:

- O IPv6 só é suportado para os endereços IP internos do túnel VPN. O endereço IP externo dos AWS endpoints são endereços IPv4 públicos. O endereço IP do gateway do cliente deve ser um endereço IPv4 público.
- Uma conexão do Site-to-Site VPN não é compatível com tráfego IPv4 e IPv6. Se sua conectividade híbrida exigir comunicação de pilha dupla, você deverá criar túneis VPN diferentes para o tráfego IPv4 e IPv6.

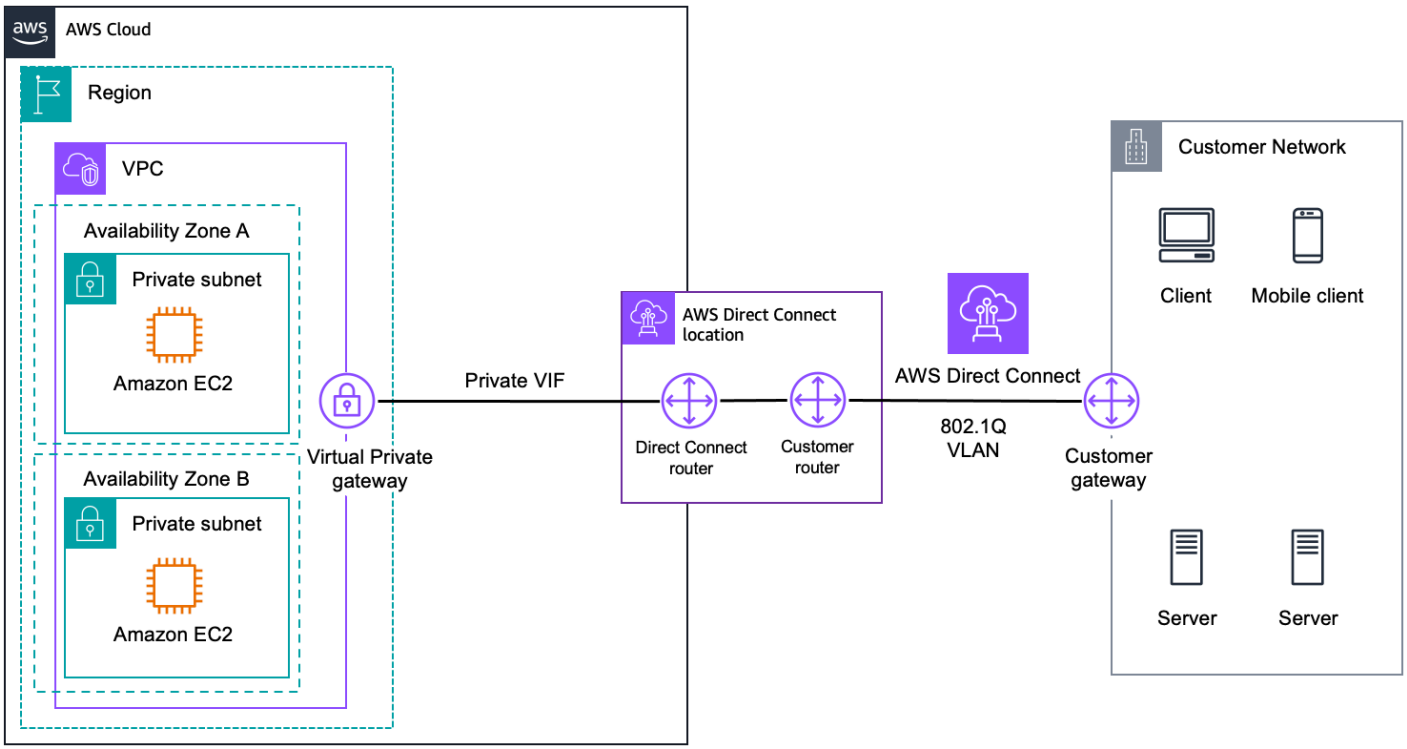
Recursos adicionais do

- Anexos VPN do Transit Gateway
- Gateway do cliente
- Trabalhando com VPN Site-to-Site
- Conexões VPN aceleradas de site a site

AWS Direct Connect

AWS Direct Connectfacilita o estabelecimento de uma conexão dedicada de uma rede local com uma ou mais VPCs. AWS Direct Connect pode reduzir os custos da rede, aumentar a taxa de transferência da largura de banda e fornecer uma experiência de rede mais consistente do que as conexões baseadas na Internet. Ele usa VLANs 802.1Q padrão do setor para se conectar à Amazon VPC usando endereços IP privados. As VLANs são configuradas usando interfaces virtuais (VIFs), e você pode configurar três tipos diferentes de VIFs:

- Interface virtual pública - Estabeleça conectividade entre endpoints AWS públicos e seu data center, escritório ou ambiente de colocation.
- Interface virtual de trânsito - Estabeleça conectividade privada entre AWS Transit Gateway seu data center, escritório ou ambiente de colocation. Essa opção de conectividade é abordada na seção???.
- Interface virtual privada - Estabeleça conectividade privada entre os recursos da Amazon VPC e seu data center, escritório ou ambiente de colocation. O uso de VIFs privados é mostrado na figura a seguir.



AWS Direct Connect

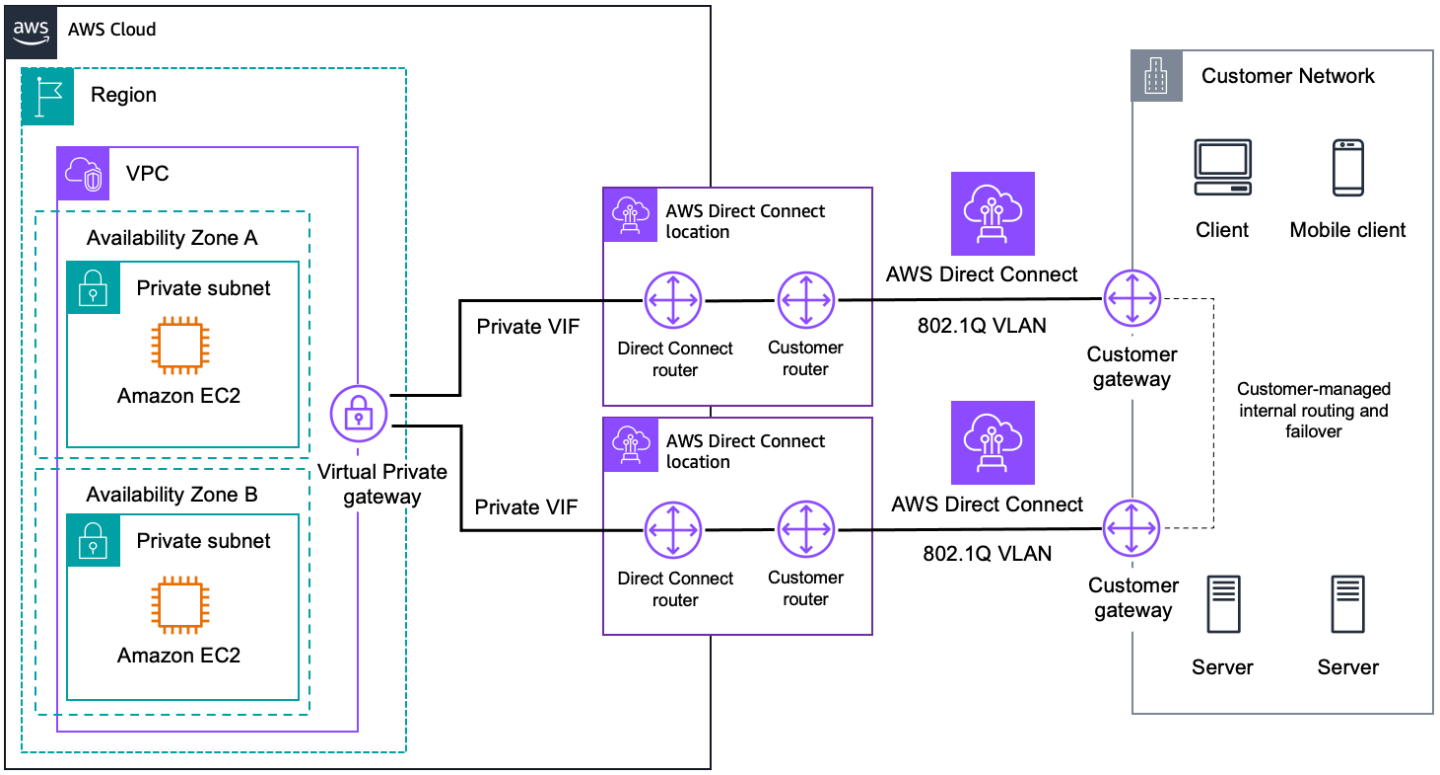
Você pode estabelecer conectividade com o AWS backbone usando AWS Direct Connect o estabelecimento de uma conexão cruzada com AWS dispositivos em um local do Direct Connect. Você pode acessar qualquer AWS região de qualquer um dos nossos locais do Direct Connect (exceto a China). Se você não tiver equipamentos em um local, poderá escolher entre um ecossistema de provedores de serviços de WAN para integrar seu AWS Direct Connect endpoint em um AWS Direct Connect local com suas redes remotas.

Com AWS Direct Connect, você tem dois tipos de conexão:

- Conexões dedicadas, nas quais uma conexão Ethernet física é associada a um único cliente. Você pode solicitar velocidades de porta de 1, 10 ou 100 Gbps. Talvez você precise trabalhar com um AWS Direct Connect parceiro no Programa de Parcerias para ajudá-lo a estabelecer circuitos de rede entre uma AWS Direct Connect conexão e seu data center, escritório ou ambiente de colocation.
- Conexões hospedadas, nas quais uma conexão Ethernet física é provisionada por um AWS Direct Connect parceiro e compartilhada com você. Você pode solicitar velocidades de porta entre 50 Mbps e 10 Gbps. Seu trabalho com o parceiro na AWS Direct Connect conexão que eles estabeleceram e nos circuitos de rede entre uma AWS Direct Connect conexão e seu data center, escritório ou ambiente de colocation.

Para conexões dedicadas, você também pode usar um grupo de agregação de links (LAG) para agregar várias conexões em um único endpoint. AWS Direct Connect Você os trata como uma conexão única e gerenciada. Você pode agregar até quatro conexões de 1 ou 10 Gbps e até duas conexões de 100 Gbps.

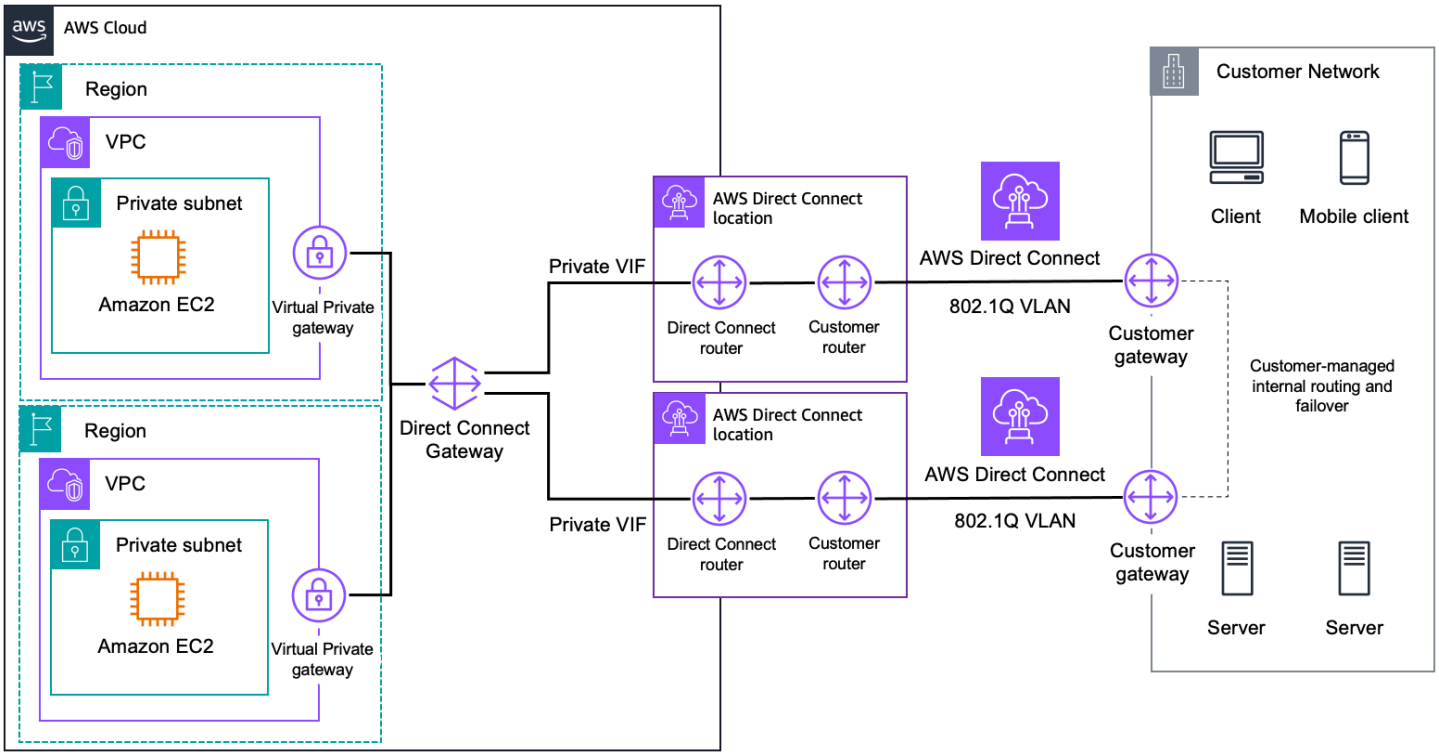
Ao discutir a alta disponibilidade em AWS Direct Connect, recomendamos o uso de AWS Direct Connect conexões adicionais. O AWS Direct Connect Resiliency Toolkit oferece orientação na criação de conexões de rede altamente resilientes entre AWS seu data center, escritório ou ambiente de colocation. A figura a seguir mostra um exemplo de uma opção de conectividade de alta resiliência, com duas AWS Direct Connect conexões terminadas em dois locais diferentes. AWS Direct Connect



Redundante AWS Direct Connect

AWS Direct Connect não é criptografado por padrão. Para conexões dedicadas de 10 ou 100 Gbps, você pode usar a segurança MAC (MACsec) como uma opção de criptografia. Para conexões de 1 Gbps ou menos, você pode criar túneis VPN em cima da conexão — essa opção é abordada nas AWS Direct Connect + VPN site a site da AWS seções 1 e 2. AWS Direct ConnectAWS Transit Gateway + VPN site a site da AWS

Um recurso importante AWS Direct Connect é o gateway Direct Connect, que é um recurso disponível globalmente para permitir conexões com várias Amazon VPCs ou Transit Gateways em diferentes regiões ou AWS contas. Esse recurso também permite que você se conecte a qualquer VPC ou Transit Gateway participante a partir de uma VIF privada ou VIF de trânsito, reduzindo o AWS Direct Connect gerenciamento, conforme mostrado na figura a seguir.



AWS Direct Connect Gateway

Com relação ao endereçamento IP, as interfaces AWS Direct Connect virtuais oferecem suporte a sessões BGP IPv4 e IPv6 para operação de pilha dupla.

- A configuração IPv4 de VIFs privadas e de trânsito usa endereços IPv4 gerados pela AWS ou endereços configurados por você. Para o peering IPv4 BGP de VIFs públicas, você deve especificar um CIDR IPv4 público /31 exclusivo de sua propriedade (ou enviar uma solicitação para atribuir um bloco CIDR).
- Para todos os tipos de emparelhamento BGP IPv6 de VIFs, a AWS atribui um CIDR /125, que não é configurável.

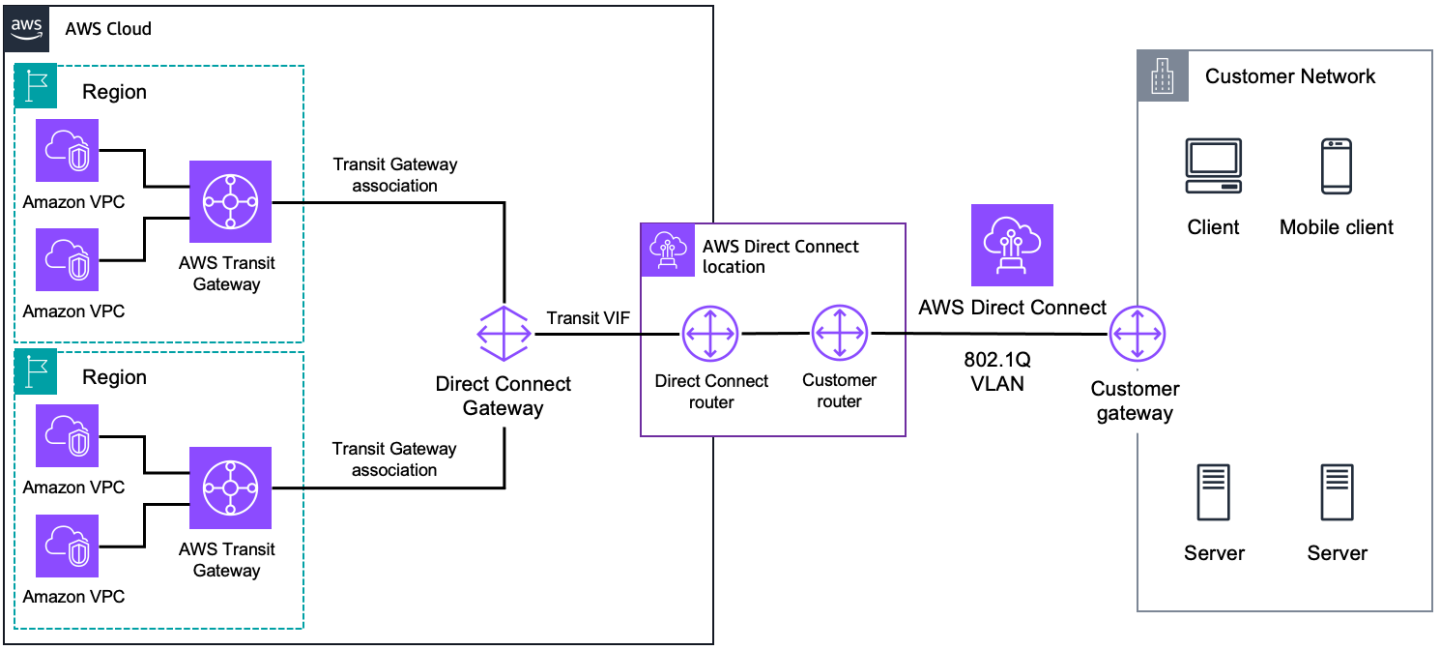
Recursos adicionais do

- AWS Direct Connect Guia do usuário
- AWS Direct Connect interfaces virtuais
- AWS Direct Connect gateways
- AWS Direct Connect Kit de ferramentas de resiliência
- AWS Direct Connect Segurança MAC
- AWS Direct Connect localizações

- AWS Direct Connect Parceiros de entrega

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, usando o anexo VIF de trânsito ao gateway Direct Connect, permite que sua rede conecte vários roteadores regionais centralizados por meio de uma conexão privada dedicada. O diagrama a seguir mostra a conexão com dois roteadores.



AWS Direct Connect and AWS Transit Gateway

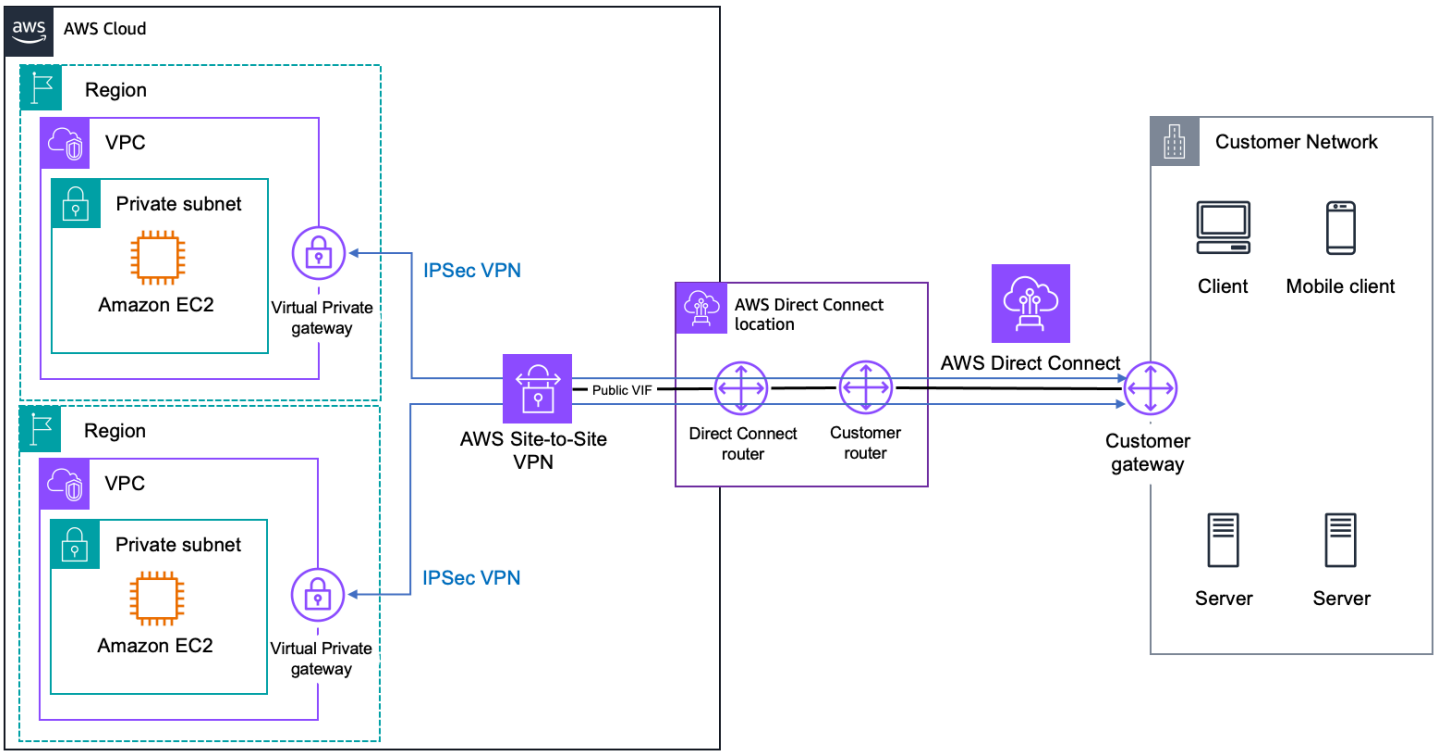
Cada um AWS Transit Gateway é um hub de trânsito de rede para interconectar VPCs na mesma região, consolidando a configuração de roteamento da Amazon VPC em um só lugar. Essa solução simplifica o gerenciamento de conexões entre uma Amazon VPC e suas redes por meio de uma conexão privada que pode reduzir os custos da rede, aumentar a taxa de transferência da largura de banda e fornecer uma experiência de rede mais consistente do que as conexões baseadas na Internet.

Recursos adicionais do

- Guia do usuário do AWS Direct Connect
- Grupos de agregação de links em AWS Direct Connect
- Publicação no blog: Integração de conexões hospedadas abaixo de 1 Gbps com o AWS Transit Gateway

AWS Direct Connect + VPN site a site da AWS

Com AWS Direct Connect+ AWS Site-to-Site VPN, você pode AWS Direct Connect combinar conexões com uma solução de VPN gerenciada pela AWS. AWS Direct Connect As VIFs públicas estabelecem uma conexão de rede dedicada entre sua rede e os recursos públicos da AWS, como um endpoint VPN Site-to-Site da AWS. Depois de estabelecer a conexão com o serviço, você pode criar conexões IPsec com os gateways privados virtuais correspondentes da Amazon VPC. A figura a seguir ilustra essa opção.



AWS Direct Connect and AWS Site-to-Site VPN

Essa solução combina os benefícios da conexão IPsec end-to-end segura com baixa latência e maior largura de banda do AWS Direct Connect para fornecer uma experiência de rede mais consistente do que as conexões VPN baseadas na Internet. Uma sessão de conexão BGP é estabelecida entre AWS Direct Connect e seu roteador na VIF pública. Outra sessão BGP ou uma rota estática será estabelecida entre o gateway privado virtual e seu roteador nos túneis VPN IPsec.

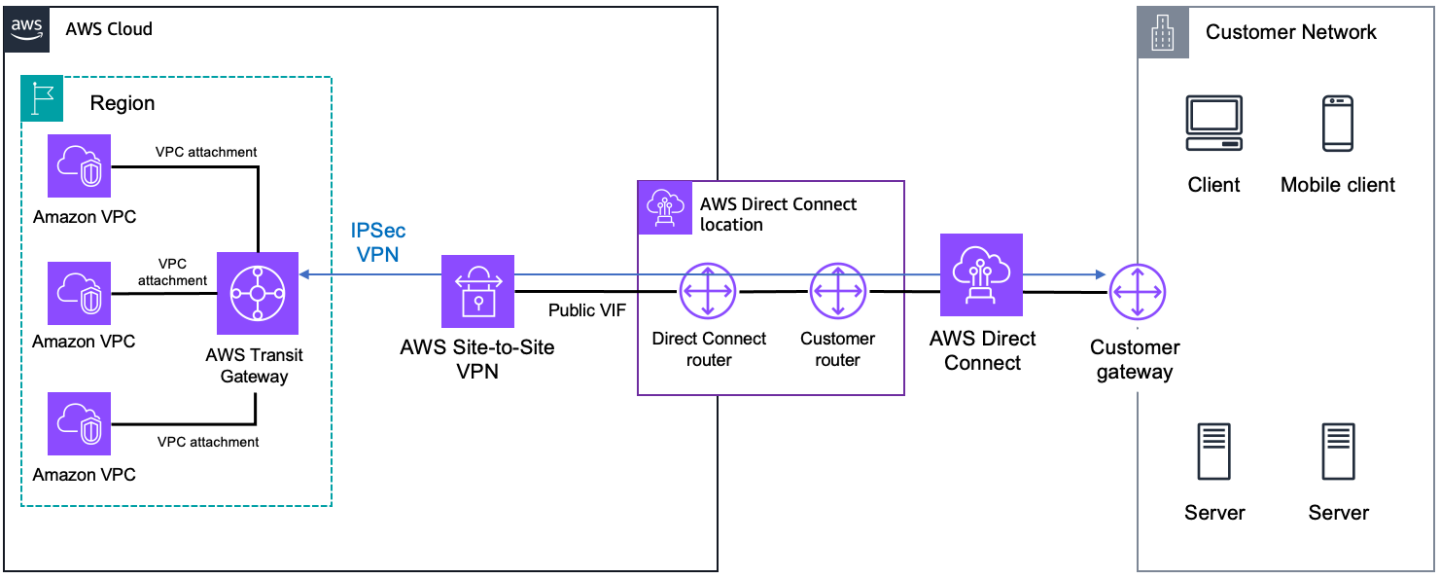
Recursos adicionais do

- AWS Direct Connect
- AWS Direct Connect interfaces virtuais
- Guia do usuário da AWS Site-to-Site VPN

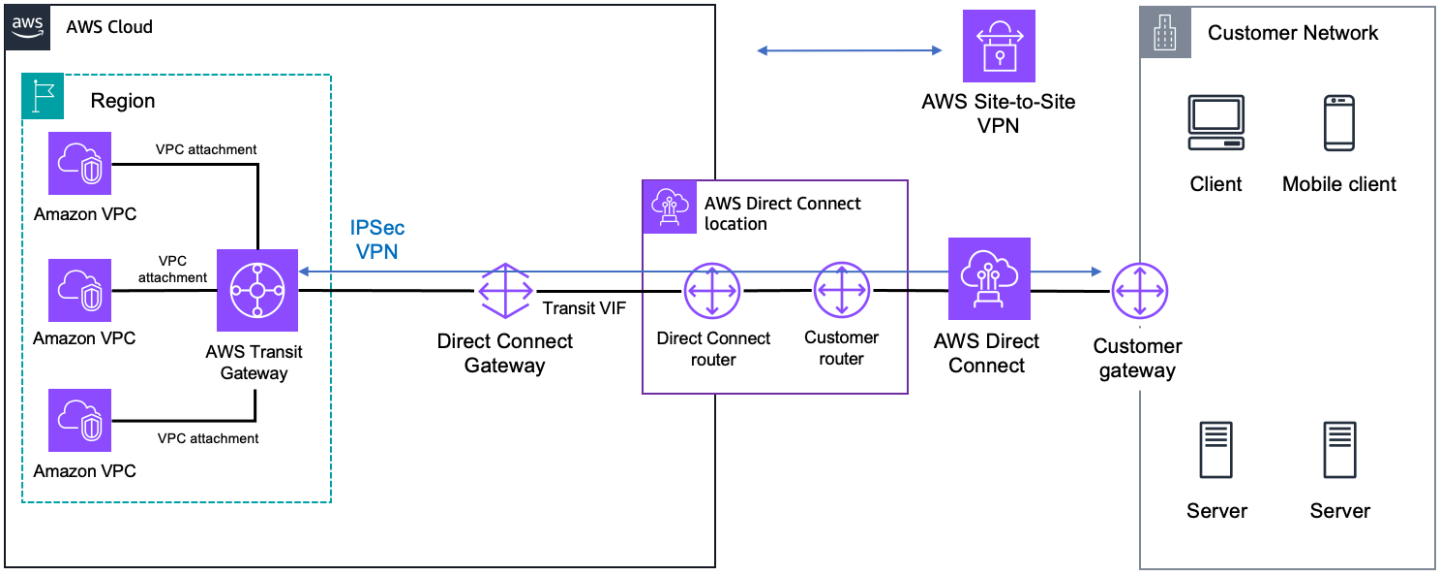
AWS Direct ConnectAWS Transit Gateway + VPN site a site da AWS

Com o AWS Direct ConnectAWS Transit Gateway+ AWS Site-to-Site VPN, você pode end-to-end habilitar conexões criptografadas por IPsec entre suas redes e um roteador regional centralizado para Amazon VPCs por meio de uma conexão privada dedicada.

Você pode usar VIFs AWS Direct Connect públicas para primeiro estabelecer uma conexão de rede dedicada entre sua rede e recursos públicos da AWS, como endpoints de VPN Site-to-Site da AWS. Depois que essa conexão for estabelecida, você poderá criar uma conexão IPsec com o. AWS Transit Gateway A figura a seguir ilustra essa opção.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Considere adotar essa abordagem quando quiser simplificar o gerenciamento e minimizar o custo das conexões VPN IPsec com várias Amazon VPCs na mesma região, com os benefícios de baixa latência e experiência de rede consistente de uma conexão privada dedicada em uma VPN baseada na Internet. Uma sessão BGP é estabelecida entre AWS Direct Connect e seu roteador usando a VIF pública ou de trânsito. Outra sessão BGP ou uma rota estática será estabelecida entre AWS Transit Gateway e seu roteador no túnel VPN IPsec.

Recursos adicionais do

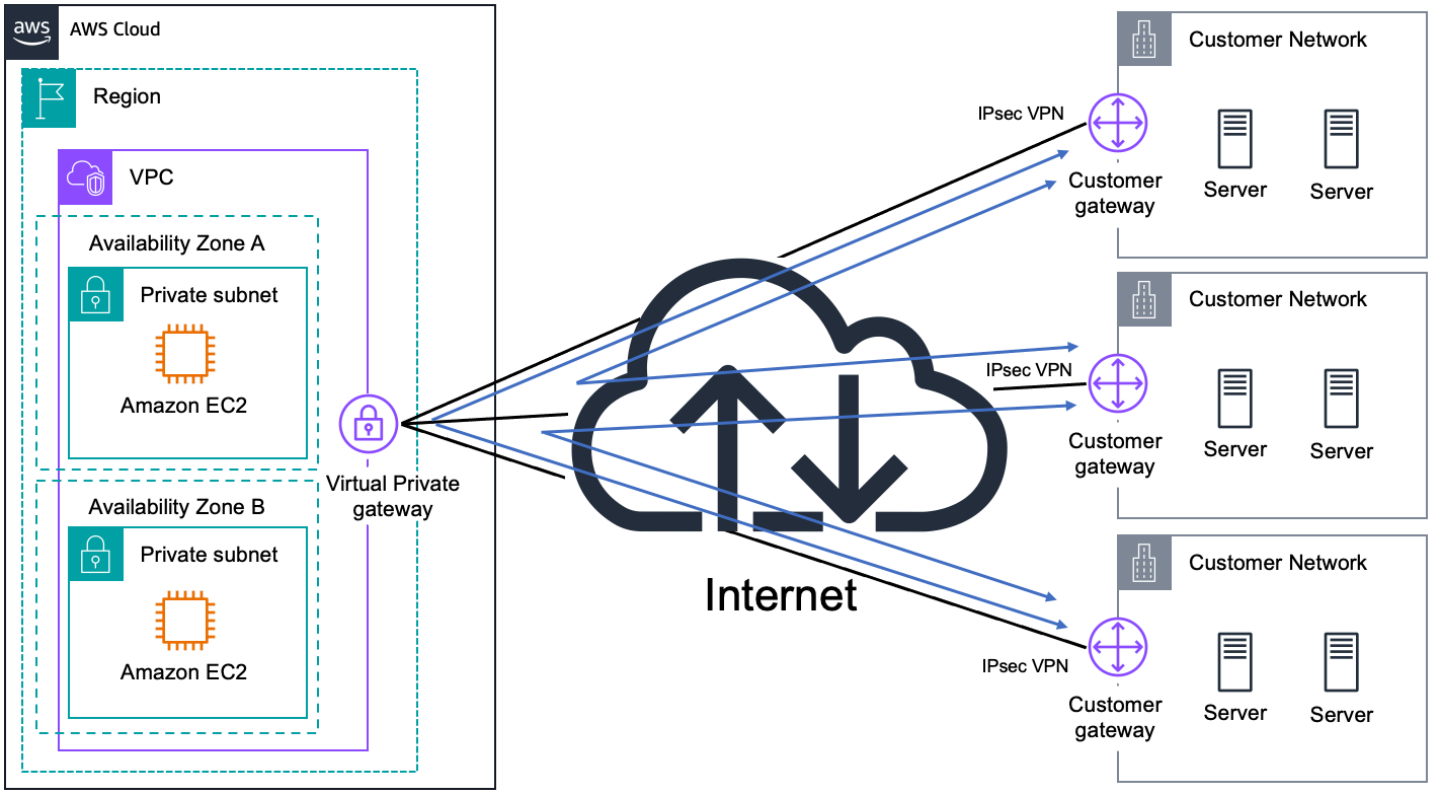
- Interfaces virtuais do AWS Direct Connect
- Anexos VPN do Transit Gateway
- Requisitos para dispositivos de gateway do cliente
- Dispositivos de gateway do cliente testados com o Amazon VPC
- VPN Site-to-Site da AWS — VPN IP privada com AWS Direct Connect

AWS VPN CloudHub

Com base nas opções de VPN gerenciada pela AWS descritas anteriormente, você pode se comunicar com segurança de um site para outro usando o. AWS VPN CloudHub O AWS VPN CloudHub opera em um hub-and-spoke modelo simples que você pode usar com ou sem uma VPC. Use essa abordagem 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 escritórios remotos.

A figura a seguir mostra a AWS VPN CloudHub arquitetura, com linhas indicando o tráfego de rede entre sites remotos sendo roteado por suas AWS VPN conexões.



AWS VPN CloudHub

AWS VPN CloudHub usa um gateway privado virtual Amazon VPC com vários gateways de clientes, cada um usando números de sistema autônomo (ASNs) exclusivos do BGP. Os sites remotos não devem ter intervalos de IP sobrepostos. Seus gateways anunciam as rotas apropriadas (prefixos BGP) em suas conexões VPN. Esses anúncios de roteamento são recebidos e anunciados novamente para cada par do BGP para que cada site possa enviar e receber dados de outros sites.

Recursos adicionais do

- Fornecendo comunicação segura entre sites usando VPN CloudHub
- Guia do usuário da AWS Site-to-Site VPN
- Requisitos para dispositivos de gateway do cliente
- Dispositivos de gateway do cliente testados com o Amazon VPC

AWS Transit Gateway + Soluções SD-WAN

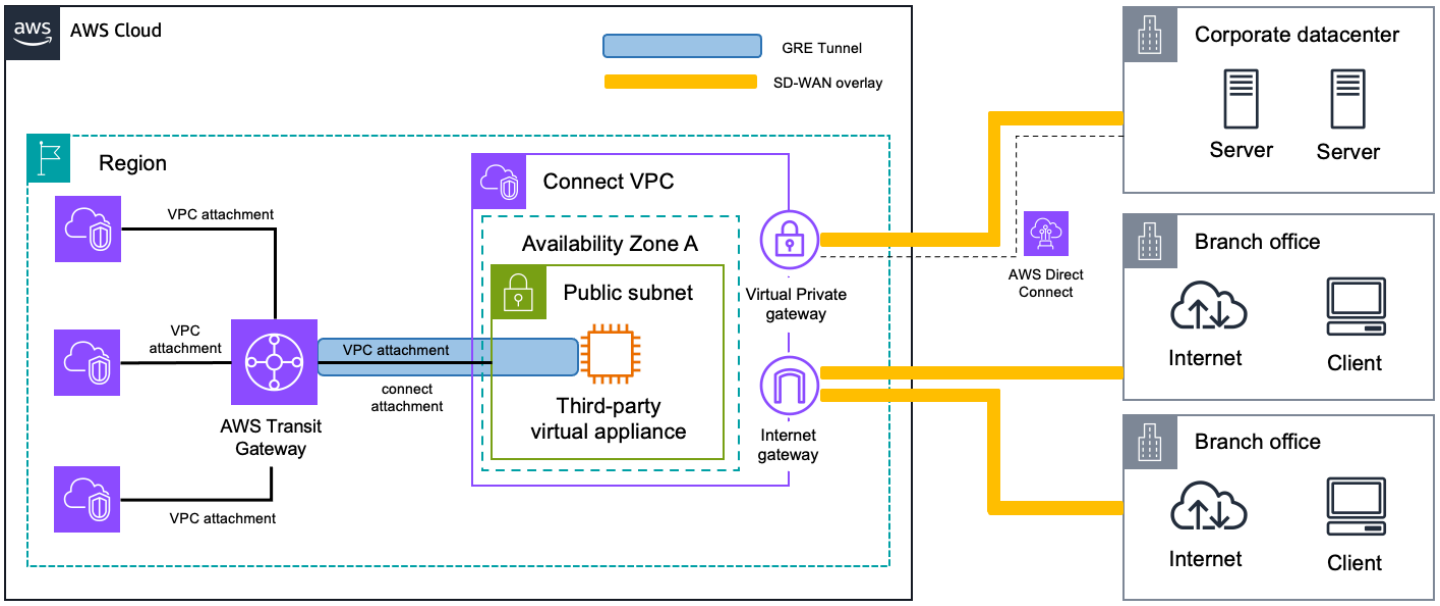
As redes de área ampla definidas por software (SD-WANs) são usadas para conectar seus datacenters, escritórios ou ambientes de colocation em diferentes redes de trânsito (como a Internet pública, redes MPLS ou o backbone da AWS AWS Direct Connect), gerenciando o tráfego de forma automática e dinâmica no caminho mais adequado e eficiente com base nas condições da rede, no tipo de aplicativo ou nos requisitos de qualidade de serviço (QoS).

Use essa abordagem se você tiver uma topologia de rede complexa, com vários datacenters, escritórios ou ambientes de colocation que precisam se comunicar entre si e com a AWS. As soluções SD-WAN podem ajudá-lo a gerenciar com eficiência esse tipo de rede.

Ao falar sobre a conexão de uma rede SD-WAN com a AWS, AWS Transit Gateway fornece um hub de trânsito de rede regional gerenciado, altamente disponível e escalável para interconectar VPCs e sua rede SD-WAN. Os anexos de conexão do Transit Gateway fornecem uma forma nativa de conectar sua infraestrutura e dispositivos de SD-WAN com a AWS. Isso facilita a extensão da sua SD-WAN para a AWS sem precisar configurar VPNs IPsec.

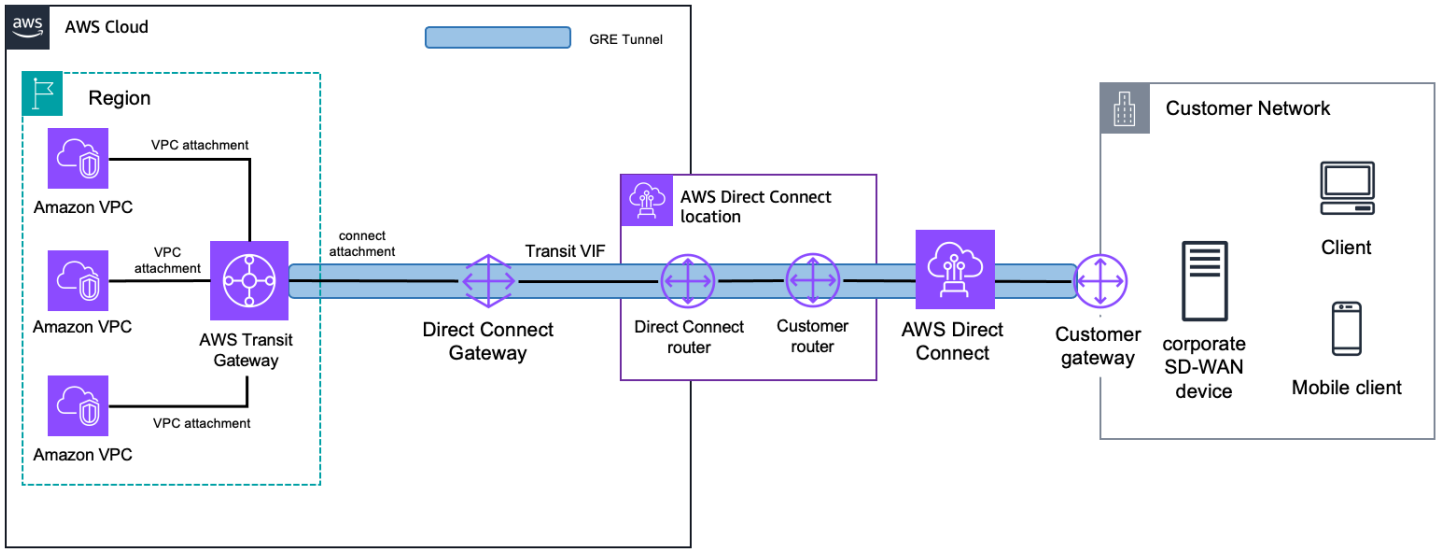
Os anexos de conexão do Transit Gateway oferecem suporte ao Encapsulamento de Roteamento Genérico (GRE) para maior desempenho de largura de banda em comparação com uma conexão VPN. Ele suporta o Border Gateway Protocol (BGP) para roteamento dinâmico e elimina a necessidade de configurar rotas estáticas. Isso simplifica o design da rede e reduz os custos operacionais associados. Além disso, sua integração com o Transit Gateway Network Manager fornece visibilidade avançada por meio de topologia de rede global, métricas de desempenho em nível de conexão e dados de telemetria.

Ao integrar sua rede SD-WAN ao Transit Gateway usando anexos de conexão, você tem dois padrões comuns. A primeira é colocar dispositivos virtuais da rede SD-WAN em uma VPC dentro da AWS. Em seguida, você usa um anexo VPC como transporte subjacente para o anexo de conexão do Transit Gateway entre os dispositivos virtuais e o Transit Gateway, conforme mostrado na figura a seguir.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

Como alternativa, você pode estender e segmentar seu tráfego de SD-WAN para a AWS sem adicionar infraestrutura extra. Você pode criar anexos de conexão do Transit Gateway usando uma AWS Direct Connect conexão como transporte subjacente, conforme mostrado na figura a seguir.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Há algumas considerações a serem observadas ao usar os anexos de conexão do Transit Gateway:

- Você pode criar anexos de conexão nos Transit Gateways existentes.

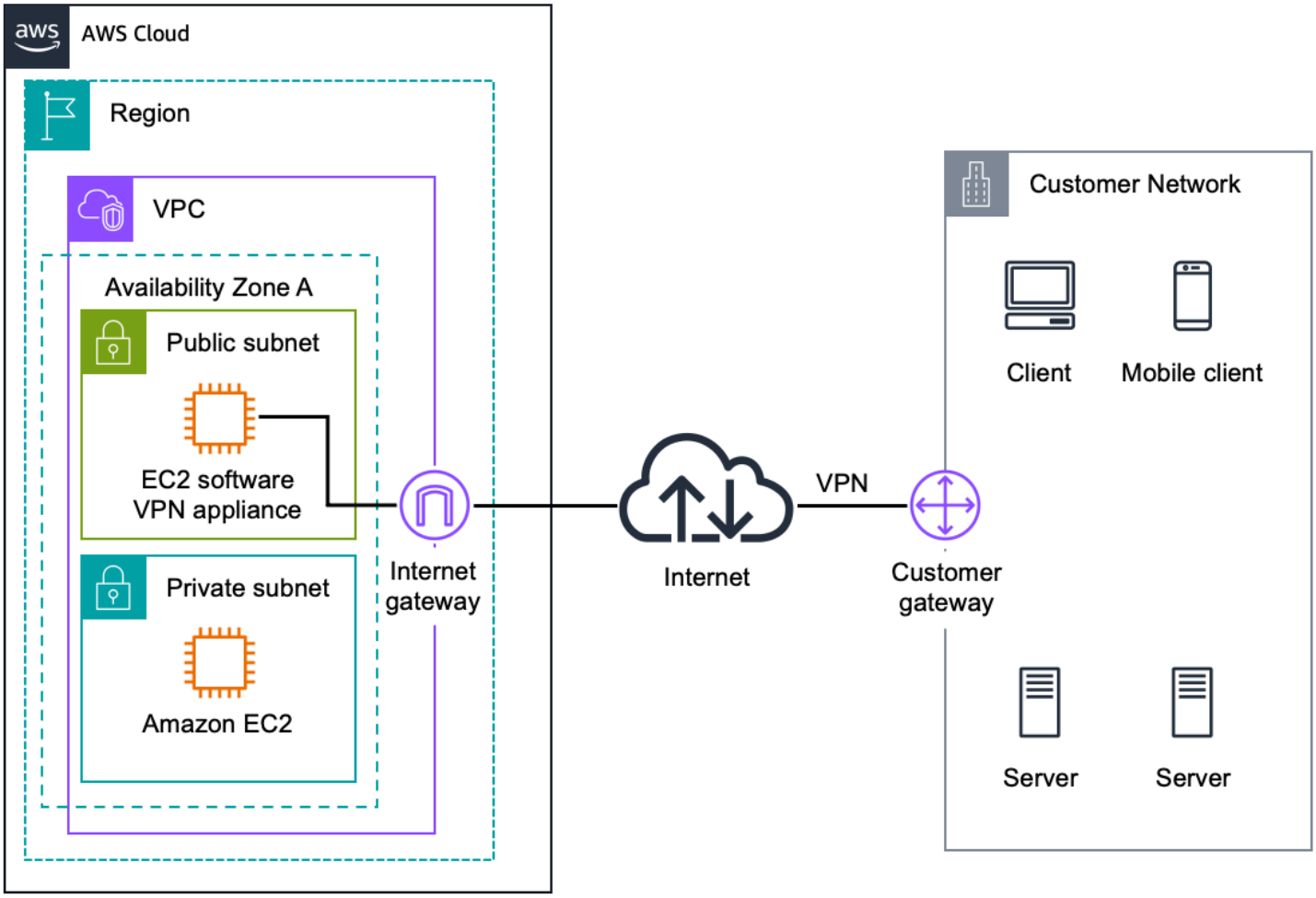
- Os dispositivos de terceiros devem ser configurados com um túnel GRE para enviar e receber tráfego do Transit Gateway usando anexos de conexão. O equipamento deve ser configurado com o BGP para atualizações de rotas dinâmicas e verificações de integridade.
- Os anexos do Connect não oferecem suporte a rotas estáticas.
- Os anexos de conexão do Transit Gateway suportam uma largura de banda máxima de cinco Gbps por túnel GRE. A largura de banda acima de cinco Gbps pode ser obtida anunciando os mesmos prefixos em vários Connect peer (túneis GRE) para o mesmo anexo Connect.
- Há suporte para um máximo de quatro Connect peers para cada conexão.
- Os anexos de conexão do Transit Gateway oferecem suporte a anúncios de rotas dinâmicas e IPv6 por meio de extensões multiprotocolo para BGP (MBGP ou MP-BGP).

Recursos adicionais do

- Anexos de emparelhamento do gateway de trânsito
- Requisitos e considerações
- Publicação no blog: Simplifique a conectividade SD-WAN com o AWS Transit Gateway Connect

Software VPN

A Amazon VPC oferece a flexibilidade de gerenciar totalmente os dois lados da sua conectividade com a Amazon VPC criando uma conexão VPN entre sua rede remota e um dispositivo VPN de software executado na sua rede Amazon VPC. Essa opção é recomendada se você precisar gerenciar as duas extremidades da conexão VPN, seja para fins de conformidade ou para aproveitar dispositivos de gateway que atualmente não são suportados pela solução VPN da Amazon VPC. A figura a seguir mostra essa opção.



Software VPN site a site

Você pode escolher entre um ecossistema de vários parceiros e comunidades de código aberto que produziram dispositivos VPN de software que funcionam no Amazon EC2. Junto com essa escolha, vem a responsabilidade de gerenciar o dispositivo de software, incluindo configuração, patches e atualizações.

Observe que esse design introduz um possível ponto único de falha no design da rede porque o dispositivo VPN de software é executado em uma única instância do Amazon EC2. Para obter mais informações, consulte Apêndice A: Arquitetura HA de alto nível para instâncias de VPN de software Arquitetura para instâncias de VPN de software.

Recursos adicionais do

- Dispositivos VPN disponíveis no AWS Marketplace
- Resumo técnico - Conectando o Cisco ASA à instância VPC EC2 (IPsec)

- Resumo técnico - Conectando várias VPCs com instâncias EC2 (IPsec)
- Resumo técnico — Conectando várias VPCs com instâncias EC2 (SSL)

Opções de conectividade entre Amazon VPC e Amazon VPC

Use esses padrões de design quando quiser integrar várias Amazon VPCs em uma rede virtual maior. Isso é útil se você precisar de várias VPCs devido à segurança, cobrança, presença em várias regiões ou requisitos internos de estorno, para integrar mais facilmente os recursos da AWS entre as Amazon VPCs. Você também pode combinar esses padrões com as opções de conectividade de rede com a Amazon VPC para criar uma rede corporativa que abrange redes remotas e várias VPCs.

A conectividade de VPC entre VPCs é melhor alcançada ao usar intervalos de IP não sobrepostos para cada VPC que está sendo conectada. Por exemplo, se você quiser conectar várias VPCs, certifique-se de que cada VPC esteja configurada com intervalos exclusivos de roteamento entre domínios sem classe (CIDR). Portanto, recomendamos que você aloque um único bloco CIDR contíguo e não sobreposto para ser usado por cada VPC. Para obter informações adicionais sobre o roteamento e as restrições da Amazon VPC, consulte as Perguntas frequentes da Amazon VPC.

Opção	Caso de uso	Vantagens	Limitações
emparelhamento da VPC	Conectividade de rede fornecida pela AWS entre duas VPCs.	Aproveita a infraestrutura de rede escalável gerenciada pela AWS	O emparelhamento de VPC não oferece suporte a relacionamentos de emparelhamento transitivos Difícil de gerenciar em grande escala
AWS Transit Gateway	Conectividade de roteador regional fornecida pela AWS para VPCs	Serviço gerenciado de alta disponibilidade e escalabilidade da AWS Hub de rede regional para até 5.000 anexos	O emparelhamento do Transit Gateway suporta apenas rotas estáticas
AWS PrivateLink	Conectividade de rede fornecida	Aproveita a infraestrutura de rede	Serviços de VPC Endpoint disponíveis

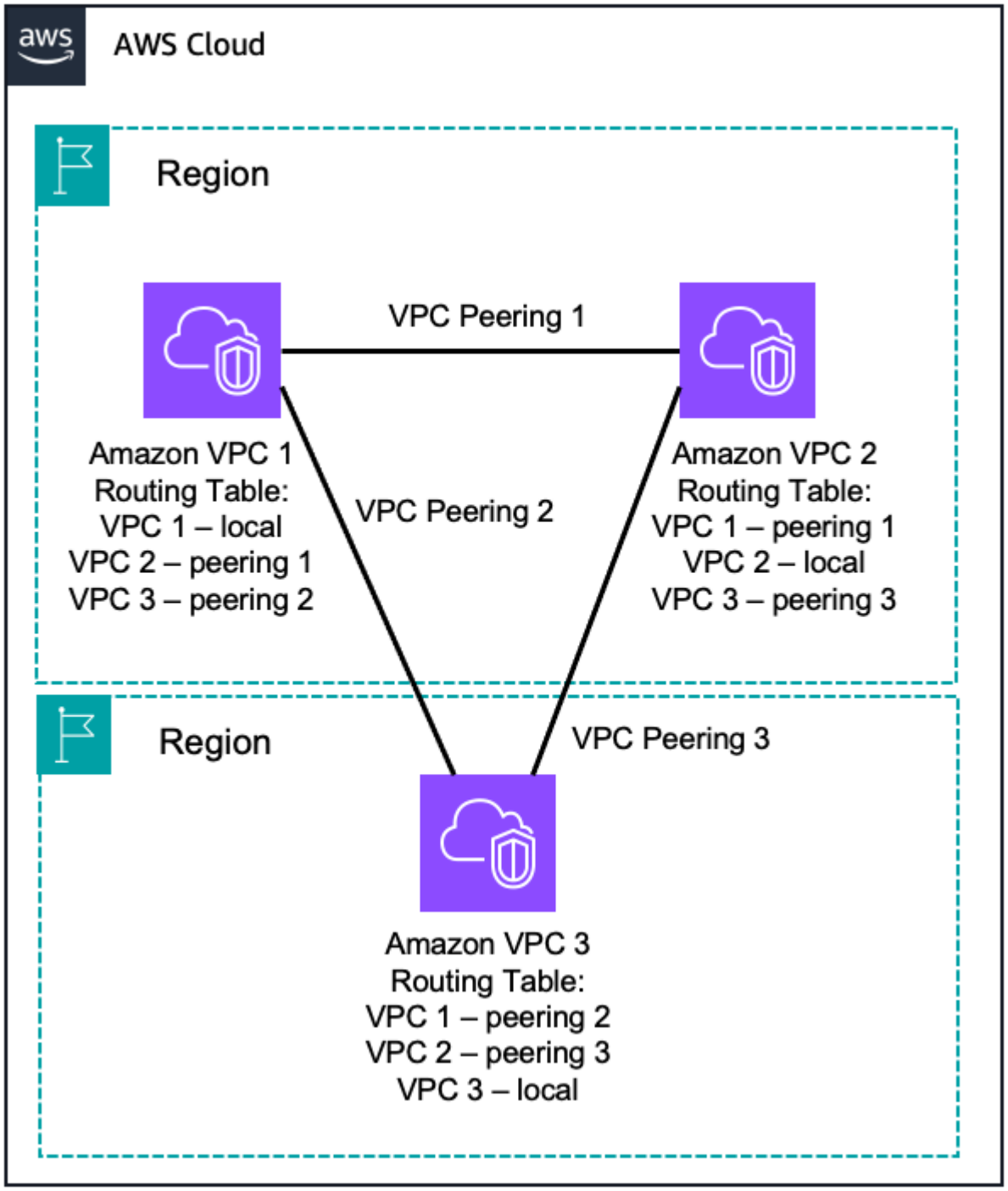
Opção	Caso de uso	Vantagens	Limitações
	pela AWS entre duas VPCs usando endpoints de interface	escalável gerenciada pela AWS	somente na região da AWS em que foram criados
Software VPN	Conexões VPN baseadas em dispositivos de software entre VPCs	Oferece suporte a uma ampla variedade de fornecedores, produtos e protocolos de VPN Gerenciado inteiramente por você	Você é responsável pela implementação de soluções de HA para todos os endpoints de VPN (se necessário) Instâncias de VPN podem se tornar um gargalo de rede
Software VPN para AWS VPN site-to-site	Dispositivo de software para conexão VPN entre VPCs	Conexão VPN VPC gerenciada pela AWS de alta disponibilidade Oferece suporte a uma ampla variedade de fornecedores e produtos de VPN gerenciados por você Suporta rotas estáticas e políticas dinâmicas de emparelhamento e roteamento de BGP	Você é responsável pela implementação de soluções de HA para os endpoints VPN do dispositivo de software (se necessário) Instâncias de VPN podem se tornar um gargalo de rede Protocolo VPN IPsec somente para o AWS Managed VPN

emparelhamento da VPC

Uma conexão de emparelhamento de VPC é uma conexão de redes entre dois VPCs, que permite roteamento usando endereços IP privados de cada VPC como se estivessem na mesma rede. As

conexões de emparelhamento de VPC podem ser criadas entre suas próprias VPCs ou com uma VPC em outra conta da AWS. O peering de VPC também oferece suporte ao peering entre regiões.

O tráfego que usa o VPC Peering entre regiões sempre permanece no backbone global da AWS e nunca atravessa a Internet pública, reduzindo assim os vetores de ameaças, como exploits comuns e ataques de DDoS.



VPC-to-VPC Peering

A AWS usa a infraestrutura existente de uma VPC para criar conexões de emparelhamento de VPC e não depende de uma peça separada de hardware físico. Portanto, eles não introduzem um possível ponto único de falha ou gargalo de largura de banda de rede entre as VPCs. Além disso, tabelas de roteamento da VPC, grupos de segurança e listas de controle de acesso à rede podem ser aproveitadas para controlar quais sub-redes ou instâncias podem utilizar a conexão de emparelhamento da VPC.

As Amazon VPCs não oferecem suporte ao peering transitivo, o que significa que você não pode comunicar duas VPCs que não estejam diretamente emparelhadas usando uma terceira VPC como trânsito. Se você quiser que todas as suas VPCs se comuniquem entre si usando o emparelhamento de VPC, você precisará criar conexões de emparelhamento de VPC 1:1 entre cada uma delas. Como alternativa, você pode usar AWS Transit Gateway nossa AWS Cloud WAN para atuar como um hub de trânsito de rede.

Tanto o tráfego IPv4 quanto o IPv6 são compatíveis com conexões de emparelhamento de VPC. No entanto, duas VPCs não podem ser emparelhadas se o bloco CIDR IPv4 primário se sobrepuser, independentemente dos blocos CIDR IPv4 ou IPv6 secundários usados. Leve isso em consideração ao atribuir o bloco CIDR primário às suas VPCs se você planeja usar o emparelhamento de VPC entre elas.

Recursos adicionais do

- Emparelhamento de Amazon VPC
- O que é peering de VPC?

AWS Transit Gateway

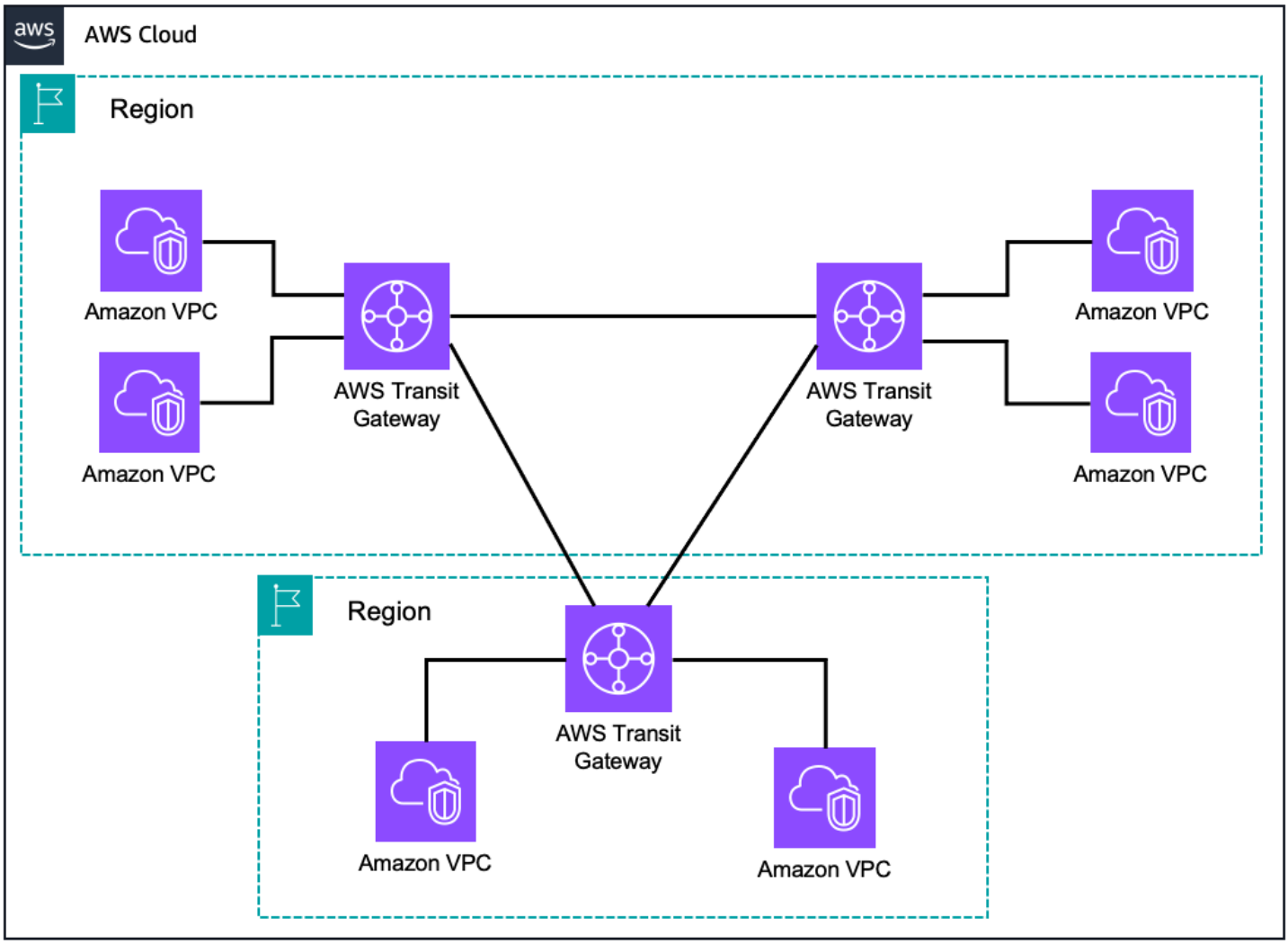
AWS Transit Gatewayé um serviço altamente disponível e escalável para consolidar a configuração de roteamento de VPC da AWS para uma região com uma arquitetura. hub-and-spoke Cada VPC spoke só precisa se conectar ao Transit Gateway para ter acesso a outras VPCs conectadas. Tanto o tráfego IPv4 quanto o IPv6 são suportados no. AWS Transit Gateway

Você pode aproveitar várias tabelas de rotas, associações e propagações do Transit Gateway para segmentar seu tráfego dentro do mesmo Transit Gateway. Você poderá gerenciar diferentes domínios de roteamento (por exemplo, tráfego de produção e não produção) a partir de um único ponto de gerenciamento, garantindo que esses domínios de roteamento não consigam se comunicar entre si.

Você também pode aproveitar a hub-and-spoke arquitetura criada pelo Transit Gateway para centralizar o acesso a serviços compartilhados, como inspeção de tráfego, acesso a endpoints VPC de interface ou tráfego de saída por meio de um gateway NAT ou instâncias NAT. Essa centralização simplifica a complexidade do gerenciamento desses recursos em várias VPCs e permite um melhor controle à medida que você amplia sua presença na AWS.

Os gateways de trânsito podem ser emparelhados entre si dentro da mesma região da AWS ou entre diferentes regiões da AWS. AWS Transit Gatewayo tráfego sempre permanece no backbone global da AWS e nunca atravessa a Internet pública, reduzindo assim os vetores de ameaças, como explorações comuns e ataques de DDoS.

Com um grande número de VPCs, o Transit Gateway fornece um gerenciamento mais simples da comunicação de VPC para VPC por meio do emparelhamento de VPC, conforme mostrado na figura a seguir.



AWS Transit Gateway

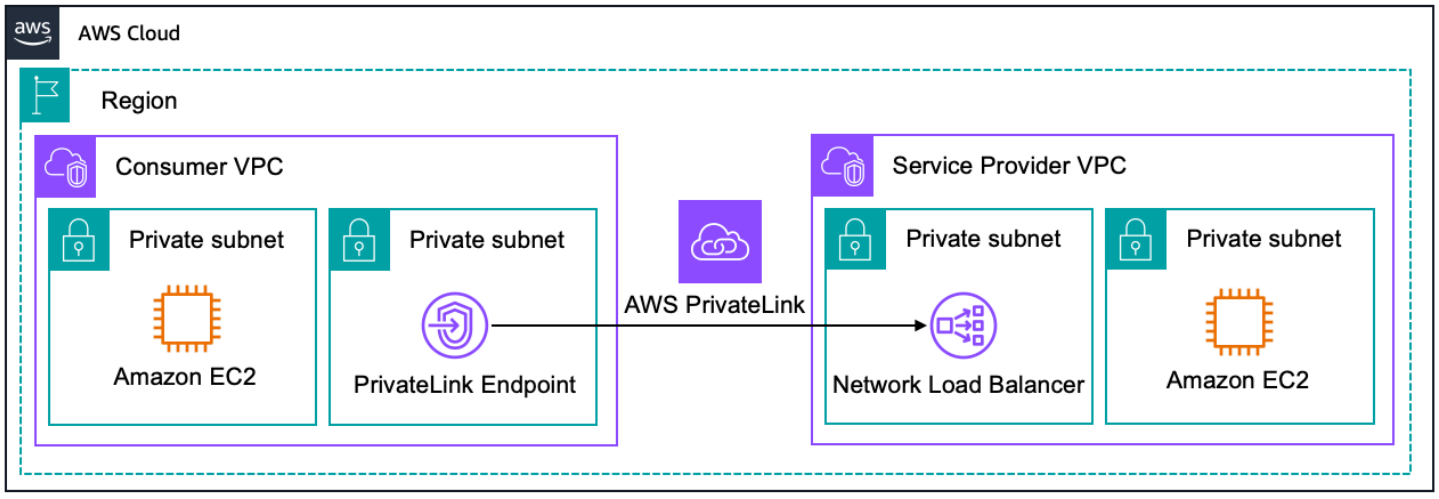
Para uma visibilidade central do tráfego IP que entra e sai dos seus Transit Gateways, você pode publicar os registros de fluxo do Transit Gateway no Amazon CloudWatch Logs e no Amazon S3. Os dados do log de fluxo são coletados fora do caminho do tráfego de rede e, portanto, não afetam a throughput nem a latência da rede.

Recursos adicionais do

- Gateway de trânsito Amazon VPC
- Anexos de emparelhamento do gateway de trânsito
- Trabalhe com Transit Gateways
- Registrando o tráfego de rede usando os registros de fluxo do Transit Gateway

AWS PrivateLink

AWS PrivateLinkpermite que você se conecte a alguns serviços da AWS, serviços hospedados por outras contas da AWS (chamados de serviços de endpoint) e serviços de AWS Marketplace parceiros compatíveis, por meio de endereços IP privados em sua VPC. Os endpoints da interface são criados diretamente dentro da sua VPC, usando interfaces de rede elástica e endereços IP nas sub-redes da sua VPC. Isso significa que os grupos de segurança da VPC podem ser usados para gerenciar o acesso aos endpoints.



AWS PrivateLink

Recomendamos essa abordagem se você quiser usar os serviços oferecidos por outra VPC com segurança em uma rede da AWS, usando endereços IP privados. Como alternativa, AWS PrivateLink é uma boa solução quando as VPCs têm endereços IP sobrepostos.

AWS PrivateLinké totalmente compatível com IPv6, mas tanto as VPCs de destino quanto as sub-redes VPC, o Network Load Balancer e os nomes DNS precisam ser habilitados ou modificados para usar o dual-stack. Depois que esses pré-requisitos forem atendidos, o IPv6 poderá ser habilitado na configuração do serviço para o endpoint.

Controles de acesso ao AWS PrivateLink

Os endpoints da interface são criados diretamente dentro da sua VPC usando interfaces de rede elástica e endereços IP nas sub-redes da VPC. Isso significa que os grupos de segurança da VPC podem ser usados para gerenciar o acesso à rede aos endpoints.

Ao criar um endpoint de interface ou um endpoint de gateway, você também pode anexar uma política de endpoint. A política de endpoint controla quais diretores da AWS (contas da AWS, usuários do IAM e funções) podem usar o VPC endpoint para acessar o serviço de endpoint.

Não é possível anexar mais de uma política a um endpoint. No entanto, o endpoint pode ser modificado a qualquer momento.

Uma política de endpoint não substitui nem substitui as políticas de usuário do IAM ou políticas específicas de serviços (como as políticas de bucket do Amazon S3). Se você estiver usando um endpoint da interface para se conectar ao Amazon S3, também poderá usar políticas de bucket do Amazon S3 para controlar o acesso a buckets de endpoints específicos ou de VPCs específicas.

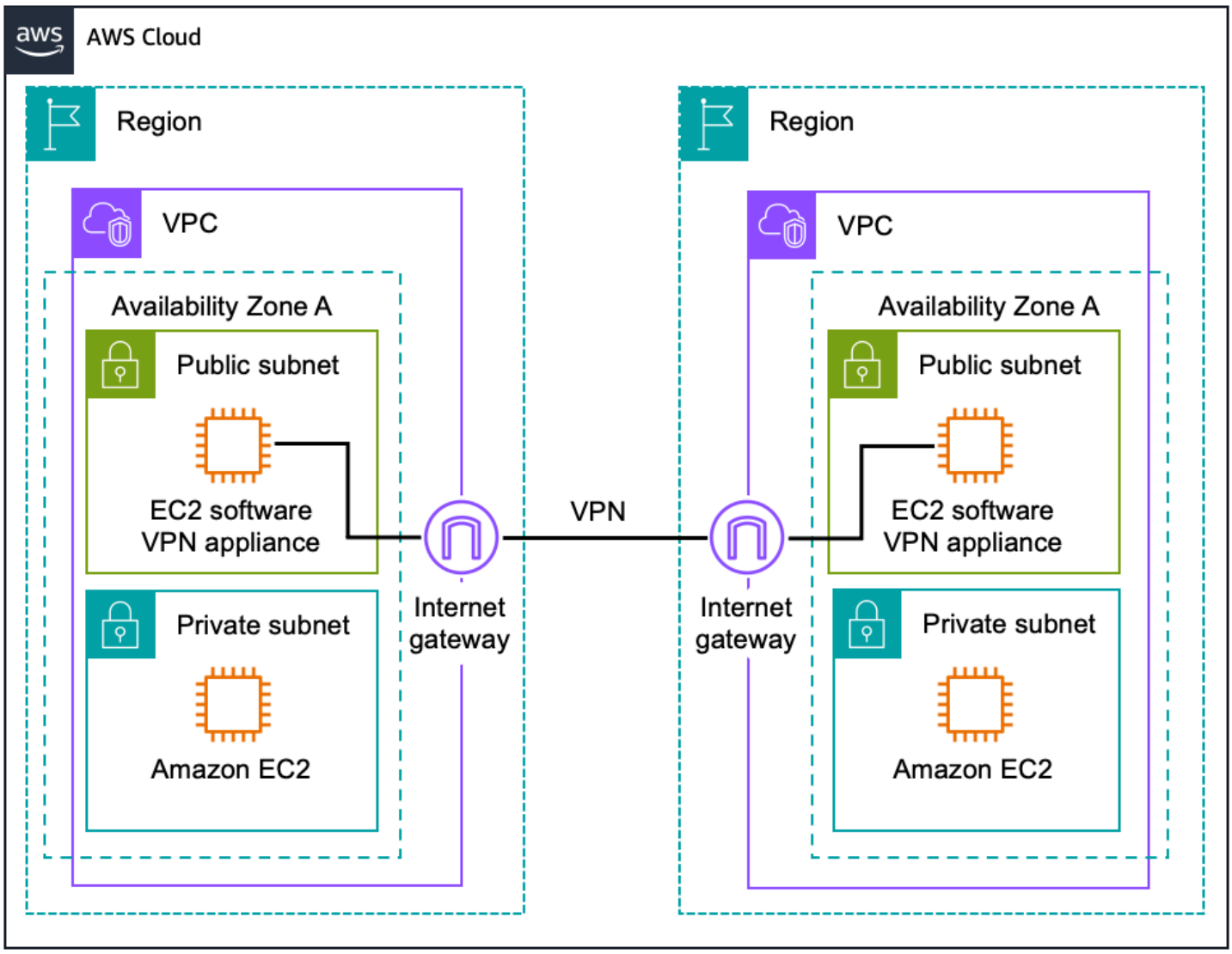
Recursos adicionais do

- Endpoints de interface VPC () AWS PrivateLink
- Serviços de endpoint VPC () AWS PrivateLink
- Publicação no blog: Acelere sua adoção do IPv6 com serviços e endpoints PrivateLink
- Publicação do blog: Conectando redes com intervalos de IP sobrepostos
- AWS PrivateLinkParceiros

Software VPN

A Amazon VPC oferece flexibilidade de roteamento de rede. Isso inclui a capacidade de criar túneis VPN seguros entre dois ou mais dispositivos VPN de software para conectar várias VPCs

a uma rede privada virtual maior, de modo que as instâncias em cada VPC possam se conectar perfeitamente umas às outras usando endereços IP privados. Essa opção é recomendada quando você deseja gerenciar as duas extremidades da conexão VPN usando seu provedor de software VPN preferido. Essa opção usa um gateway de internet conectado a cada VPC para facilitar a comunicação entre os dispositivos VPN do software.



Software Site-to-Site VPN VPC-to-VPC Routing

Você pode escolher entre um ecossistema de vários parceiros e comunidades de código aberto que produziram dispositivos VPN de software que são executados no Amazon EC2. Junto com essa escolha, vem a responsabilidade de gerenciar o dispositivo de software, incluindo configuração, patches e atualizações.

Observe que esse design introduz um possível ponto único de falha no design da rede, pois o dispositivo VPN de software é executado em uma única instância do Amazon EC2. Para obter

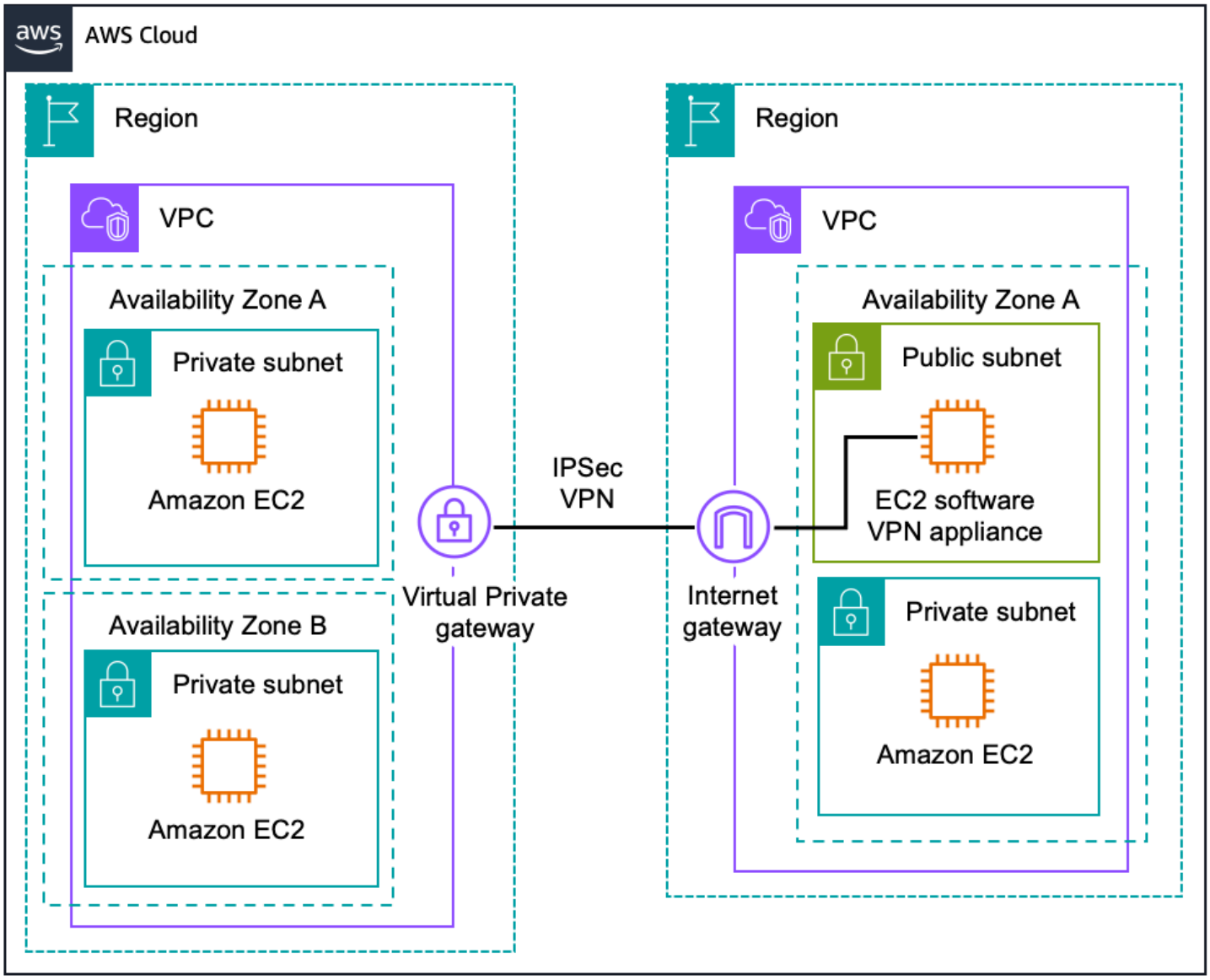
informações adicionais, consulte Apêndice A: Arquitetura HA de alto nível para instâncias de VPN de software.

Recursos adicionais do

- Dispositivos VPN disponíveis no AWS Marketplace
- Resumo técnico - Conectando várias VPCs com instâncias EC2 (IPsec)
- Resumo técnico — Conectando várias VPCs com instâncias EC2 (SSL)

Software VPN para AWS VPN site-to-site

A Amazon VPC oferece a flexibilidade de combinar as opções de VPN gerenciada pela AWS e VPN de software para conectar várias VPCs. Com esse design, você pode criar túneis VPN seguros entre um dispositivo VPN de software e um gateway privado virtual, permitindo que as instâncias em cada VPC se conectem perfeitamente umas às outras usando endereços IP privados. Essa opção usa um gateway privado virtual em uma Amazon VPC e uma combinação de um gateway de internet e um dispositivo VPN de software em outra Amazon VPC, conforme mostrado na figura a seguir.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Observe que esse design introduz um possível ponto único de falha no design da rede. Para obter informações adicionais, consulte Apêndice A: Arquitetura HA de alto nível para instâncias de VPN de software.

Recursos adicionais do

- Dispositivos VPN disponíveis no AWS Marketplace
- Guia do usuário da AWS Site-to-Site VPN
- Requisitos para dispositivos de gateway do cliente

Opções de acesso remoto de software à Amazon VPC

Com o software VPN de acesso remoto, você pode aproveitar serviços de baixo custo, elásticos e seguros para implementar soluções de acesso remoto e, ao mesmo tempo, fornecer uma experiência perfeita de conexão com recursos hospedados na AWS. Essa opção geralmente é preferida por empresas menores com redes remotas menos extensas ou que ainda não criaram e implantaram soluções de acesso remoto para seus funcionários.

Você pode combinar esses padrões com as opções de Opções de conectividade entre a rede e a Amazon VPC conectividade e Opções de conectividade entre Amazon VPC e Amazon VPC criar uma rede que abranja redes remotas e várias VPCs.

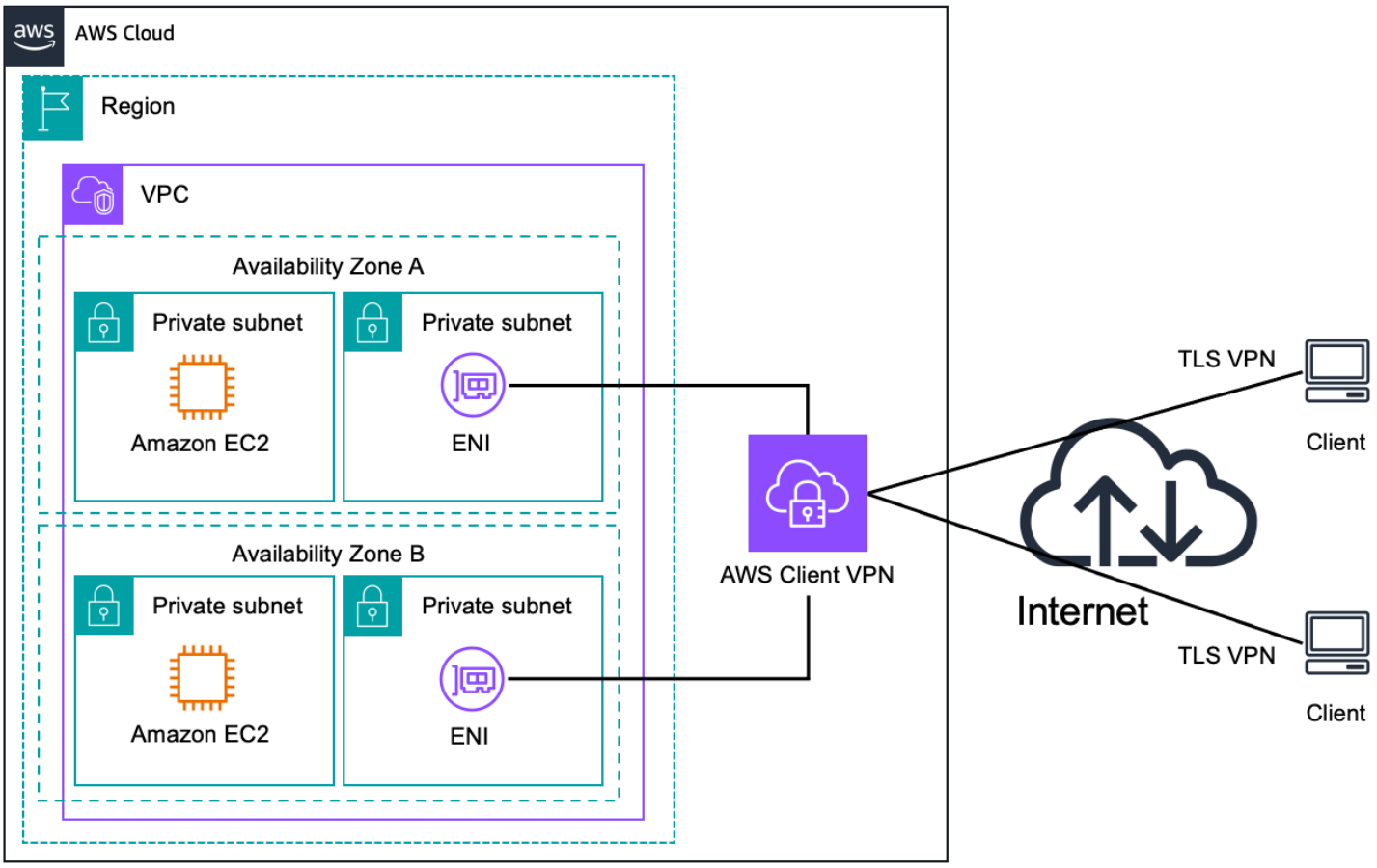
A tabela a seguir descreve as vantagens e limitações dessas opções.

Opção	Caso de uso	Vantagens	Limitações
AWS Client VPN	Solução de acesso remoto gerenciad o pela AWS para Amazon VPC e/ou redes internas	Serviço gerenciado de alta disponibilidade e escalabilidade da AWS	Somente clientes OpenVPN
Cliente de software VPN	Solução de acesso remoto de dispositi vo VPN de software para Amazon VPC e/ ou redes internas	Oferece suporte a uma variedade maior de fornecedores, produtos e protocolos de VPN Solução totalment e gerenciada pelo cliente	Você é responsável pela implementação de soluções de HA

AWS Client VPN

O AWS Client VPN é um serviço gerenciado pela AWS de alta disponibilidade e escalabilidade que permite o acesso remoto seguro ao software. Ele oferece a opção de criar uma conexão TLS segura

entre clientes remotos e suas Amazon VPCs, para acessar com segurança os recursos da AWS e locais pela Internet, conforme mostrado na figura a seguir.



AWS Client VPN Remote Access

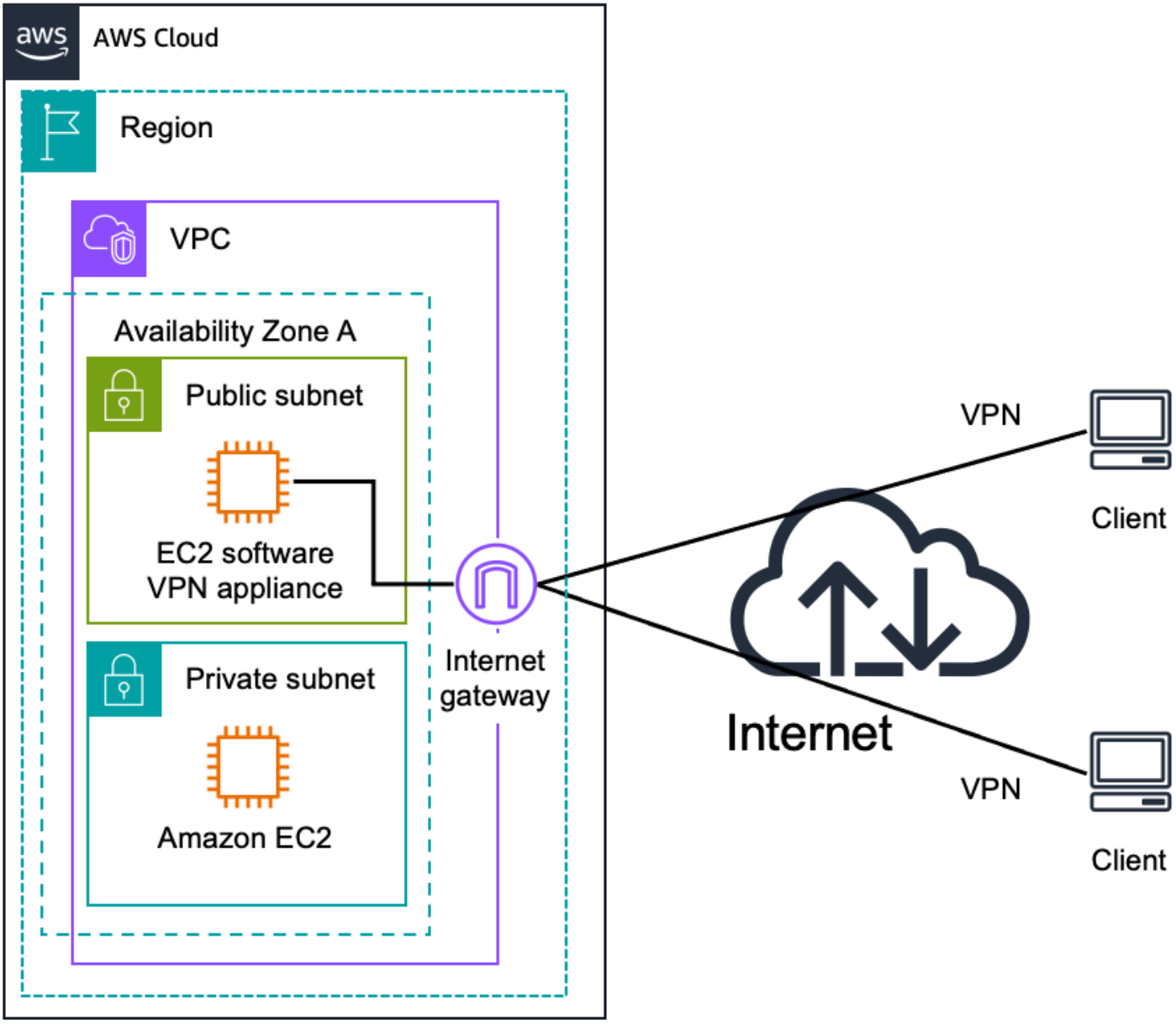
Os clientes remotos podem ser o AWS Client VPN for Desktop ou clientes OpenVPN VPN de terceiros, com autenticação pelo Active Directory ou autenticação de certificado mútuo.

Recursos adicionais do

- Guia do administrador da AWS Client VPN

Cliente de software VPN

Você pode escolher entre um ecossistema de vários parceiros e comunidades de código aberto que produziram soluções de acesso remoto que são executadas no Amazon EC2. Essas soluções oferecem grande flexibilidade no uso do protocolo de segurança para acesso remoto às suas Amazon VPCs, para acessar com segurança os recursos da AWS e no local pela Internet, conforme mostrado na figura a seguir.



Software Client VPN Remote Access

As soluções de acesso remoto variam em complexidade, oferecem suporte a várias opções de autenticação de clientes (incluindo autenticação multifatorial) e podem ser integradas ao Amazon VPC ou a soluções de gerenciamento de identidade e acesso hospedadas remotamente (aproveitando uma das opções de rede para Amazon VPC), como o Microsoft Active Directory ou outras soluções de autenticação multifatorial e LDAP.

Você é responsável por gerenciar o software de acesso remoto, incluindo gerenciamento de usuários, configuração, patches e atualizações. Esse design introduz um possível ponto único de falha no design da rede, pois o servidor de acesso remoto é executado em uma única instância do

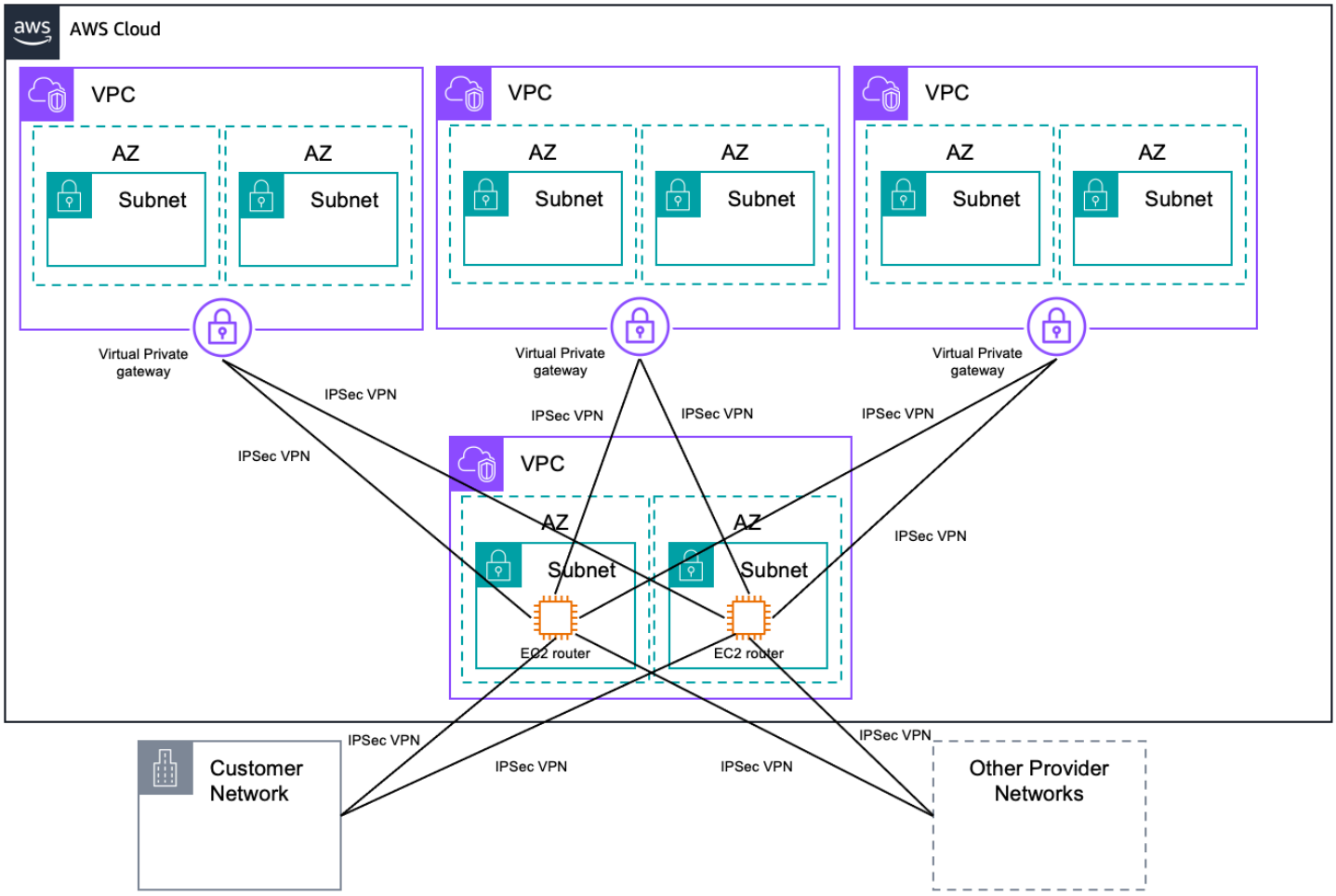
Amazon EC2. Para obter informações adicionais, consulte Apêndice A: Arquitetura HA de alto nível para instâncias de VPN de software.

Recursos adicionais do

- Dispositivos VPN disponíveis no AWS Marketplace
- Guia de início rápido do OpenVPN Access Server

VPC de trânsito

Com base nos designs de VPN de software mencionados acima, você pode criar uma rede de trânsito global na AWS. Uma VPC de trânsito é uma estratégia comum para conectar várias VPCs e redes remotas geograficamente dispersas a fim de criar um centro de trânsito de rede global. Uma VPC de trânsito simplifica o gerenciamento da rede e minimiza o número de conexões necessárias para conectar várias VPCs e redes remotas. A figura a seguir ilustra esse design.



Transit VPC

Além de fornecer roteamento de rede direto entre VPCs e redes locais, esse design também permite que a VPC de trânsito implemente regras de roteamento mais complexas, como conversão de endereços de rede entre intervalos de rede sobrepostos, ou adicione mais filtragem ou inspeção de pacotes no nível da rede. O design da VPC de trânsito pode ser usado para dar suporte a casos de uso importantes, como redes privadas, conectividade compartilhada e uso entre contas da AWS.

Recursos adicionais do

- AWS Transit Gateway
- Cisco Catalyst 8000V para SD-WAN e roteamento em AWS Marketplace

WAN na nuvem da AWS

A AWS Cloud WAN é uma rede de área ampla (WAN) gerenciada e orientada por intenção, descrita por uma política que você define e que unifica seu datacenter, filiais e redes da AWS. Embora você possa criar sua própria rede global interconectando vários Transit Gateways entre regiões, o Cloud WAN fornece recursos integrados de automação, segmentação e gerenciamento de configuração projetados especificamente para criar e operar redes globais, com base em sua política de rede principal. O Cloud WAN adicionou recursos como anexos automatizados de VPC, monitoramento de desempenho integrado e configuração centralizada.

A política de rede principal é escrita em uma linguagem declarativa que define os segmentos, o roteamento da região da AWS e como os anexos devem ser mapeados para os segmentos. Com uma política de rede básica, você pode descrever sua intenção de controle de acesso e roteamento de tráfego, enquanto o AWS Cloud WAN lida com os detalhes da configuração da rede.

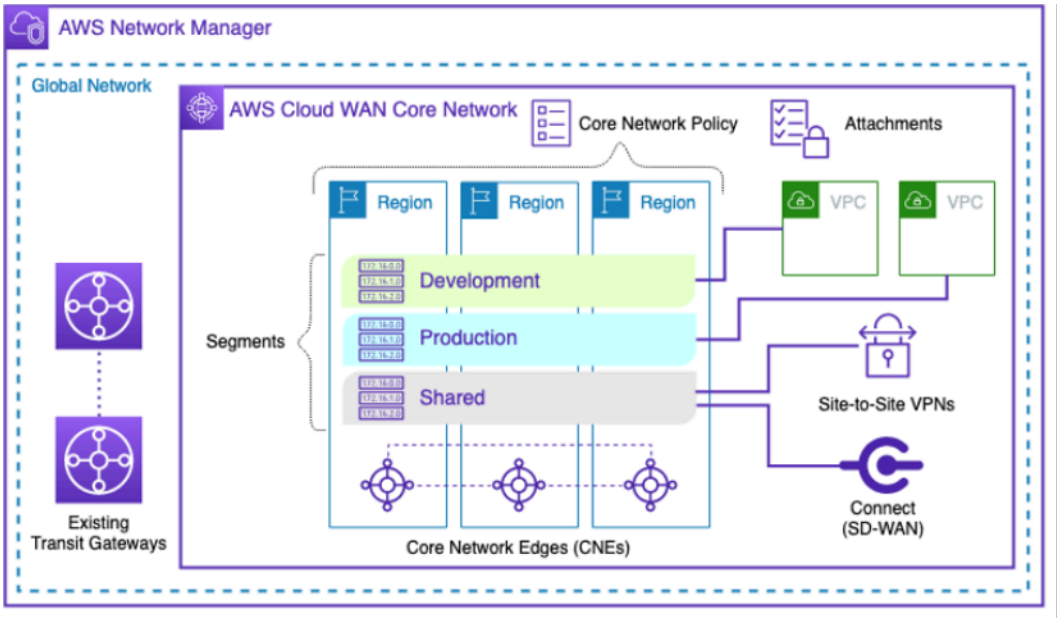
A WAN na nuvem é gerenciada no AWS Network Manager, o que permite que você gerencie e visualize centralmente sua rede principal de WAN em nuvem e redes do Transit Gateway em todas as contas, regiões e locais locais da AWS. O Network Manager fornece várias visualizações de painel para ajudá-lo a visualizar e monitorar todos os aspectos da sua rede global. Alguns dos painéis incluem:

- Mapas mundiais que indicam onde seus recursos de rede, como pontos de presença, dispositivos e anexos, estão localizados.
- Monitoramento que usa CloudWatch eventos para rastrear estatísticas de 15 meses, oferecendo uma perspectiva melhor sobre o desempenho de suas redes.
- Rastreamento de eventos que transmite eventos em tempo real para um painel de eventos.
- Diagramas topológicos e lógicos de suas redes de gateway de trânsito e gateways de trânsito.

Tanto o Transit Gateway quanto o Cloud WAN permitem conectividade centralizada entre VPCs e locais locais. O Transit Gateway é um hub regional de conectividade de rede e é ideal para clientes que operam em algumas regiões da AWS, desejam gerenciar sua própria configuração de peering e roteamento ou preferem usar sua própria automação. O Cloud WAN é ideal para clientes que desejam definir sua rede global por meio de políticas e fazer com que o serviço implemente os componentes subjacentes automaticamente.

Coisas a saber

- O CNE (Core Network Edge) herda muitas características do Transit Gateway, como a taxa de transferência por anexo de VPC.
- O Cloud WAN é compatível com IPv4 e IPv6.
- Atualmente, o Cloud WAN não oferece suporte nativo a AWS Direct Connect anexos. Para usar AWS Direct Connect com o Cloud WAN, você precisa de um Transit Gateway conectado a um AWS Direct Connect gateway e, em seguida, do Transit Gateway emparelhado para o Cloud WAN.
- Para redes grandes com muitas mudanças, considere criar uma rede global separada de desenvolvimento e teste na qual você possa validar as alterações.



AWS Cloud WAN

Recursos adicionais do

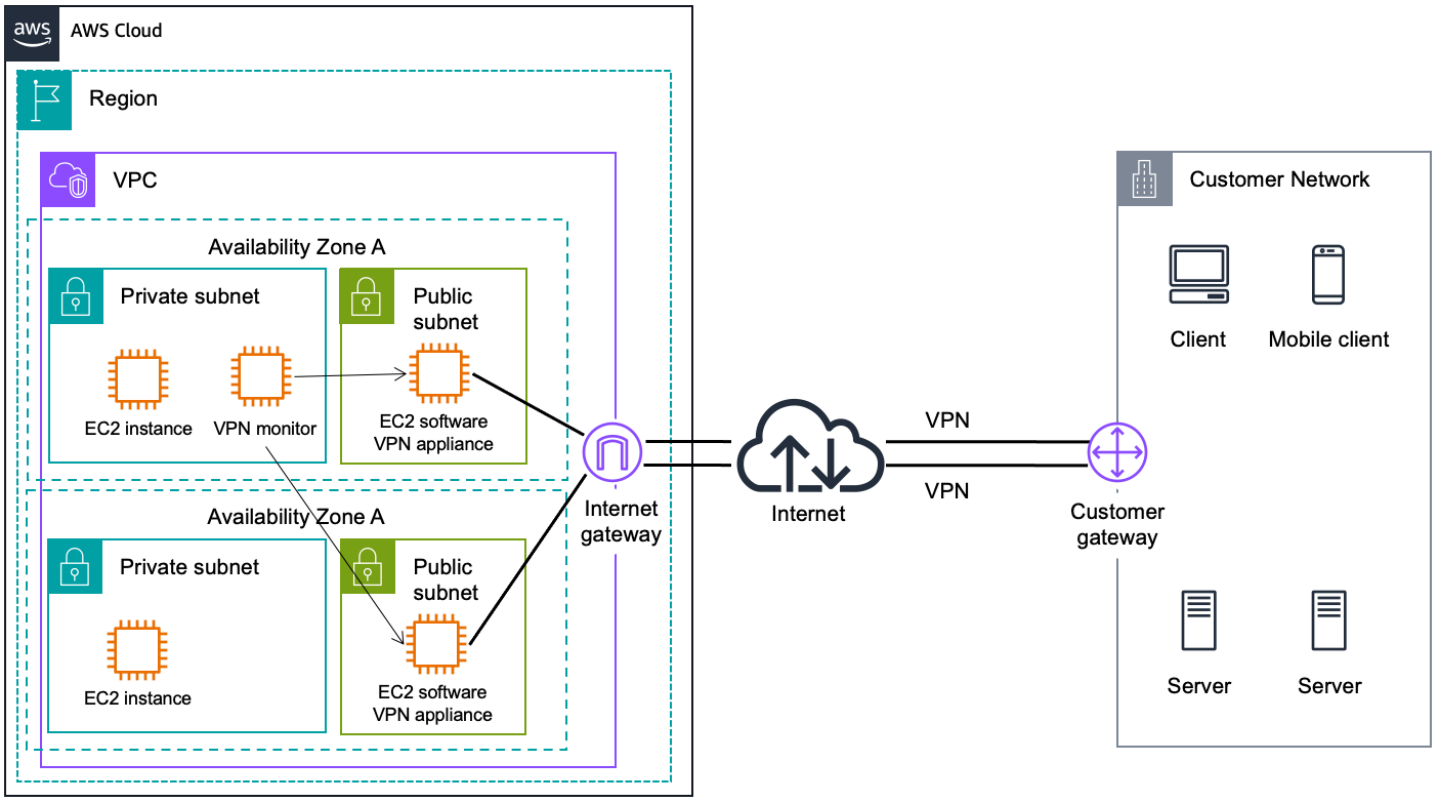
- Documentação da AWS Cloud WAN
- Publicação no blog: Padrões de migração e interoperabilidade do AWS Cloud WAN e do AWS Transit Gateway

Conclusão

A AWS oferece várias opções de conectividade eficientes e seguras para ajudar você a aproveitar ao máximo a AWS ao integrar suas redes remotas com a Amazon VPC. As opções fornecidas neste whitepaper destacam várias opções e padrões de conectividade que os clientes usaram para integrar com sucesso suas redes remotas ou várias redes da Amazon VPC. Você pode usar as informações fornecidas aqui para determinar o mecanismo mais apropriado para conectar a infraestrutura necessária para administrar sua empresa, independentemente de onde ela esteja fisicamente localizada ou hospedada.

Apêndice A: Arquitetura HA de alto nível para instâncias de VPN de software

A criação de uma conexão VPC totalmente resiliente para instâncias de VPN de software requer a instalação e a configuração de várias instâncias de VPN e uma instância de monitoramento para monitorar a integridade das conexões VPN.



Software de alto nível VPN HA

Recomendamos configurar suas tabelas de rotas de VPC para aproveitar todas as instâncias de VPN simultaneamente, direcionando o tráfego de todas as sub-redes em uma zona de disponibilidade por meio de suas respectivas instâncias de VPN na mesma zona de disponibilidade. Em seguida, cada instância de VPN fornece conectividade VPN para instâncias que compartilham a mesma zona de disponibilidade.

Monitoramento de VPN

Para monitorar um dispositivo VPN baseado em software, você pode criar um monitor VPN. O monitor VPN é uma instância personalizada que você precisará para executar os scripts de

monitoramento da VPN. Essa instância tem como objetivo executar e monitorar o estado da conexão VPN e das instâncias de VPN. Se uma instância ou conexão de VPN cair, o monitor precisará parar, encerrar ou reiniciar a instância de VPN e, ao mesmo tempo, redirecionar o tráfego das sub-redes afetadas para a instância de VPN ativa até que ambas as conexões funcionem novamente. Como os requisitos do cliente variam, a AWS atualmente não fornece orientação prescritiva para configurar essa instância de monitoramento. No entanto, um exemplo de script para habilitar o HA entre instâncias NAT pode ser usado como ponto de partida para criar uma solução de HA para instâncias de VPN de software. Recomendamos que você pense na lógica comercial necessária para fornecer uma notificação ou tentar reparar automaticamente a conectividade de rede no caso de uma falha na conexão VPN.

Além disso, você pode monitorar os túneis VPN gerenciados pela AWS usando CloudWatch métricas da Amazon, que coleta pontos de dados do serviço de VPN em métricas legíveis e quase em tempo real. Cada conexão VPN coleta e publica uma variedade de métricas de túnel na Amazon. CloudWatch Essas métricas permitem monitorar a integridade e a atividade do túnel e criar ações automatizadas.

Colaboradores

Os colaboradores deste documento incluem:

- Daniel Yu, gerente técnico sênior de contas, AWS Enterprise Support
- Garvit Singh, criador de soluções, arquitetura de soluções da AWS
- Steve Morad, gerente sênior de criadores de soluções, arquitetura de soluções da AWS
- Sohaib Tahir, arquiteto de soluções, arquitetura de soluções da AWS
- Fiona Armada, arquiteta de soluções principal, arquitetura de soluções da AWS
- Pablo Sánchez Carmona, arquiteto de soluções especialista em redes, arquitetura de soluções da AWS
- Tony Hawke, especialista sênior em redes, gerente técnico de contas, AWS Enterprise Support

Revisões do documento

Para ser notificado sobre atualizações nesse whitepaper, inscreva-se no feed RSS.

Alteração	Descrição	Data
Whitepaper atualizado	O AWS Cloud WAN e o Transit Gateway adicionaram opções de anexos, diagramas atualizados e informações por toda parte.	5 de abril de 2023
Whitepaper atualizado	Foram adicionadas opções de AWS Transit Gateway e AWS Client VPN, diagramas e informações atualizados por toda parte.	6 de junho de 2020
Atualização secundária	Pequena alteração para corrigir a referência ao dispositivo VPN de software.	20 de maio de 2020
Whitepaper atualizado	Informações atualizadas por toda parte. Concentre-se nos seguintes projetos/recursos: VPC de trânsito, gateway Direct Connect e. AWS PrivateLink	1º de janeiro de 2018
Publicação inicial	As opções de conectividade da Amazon Virtual Private Cloud foram publicadas.	1 de julho de 2014

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento é: (a) fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.

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.