Whitepaper da AWS

Construção de uma infraestrutura de rede da AWS escalável e segura com várias VPCs

Construção de uma infraestrutura de rede da AWS escalável e segura com várias VPCs: Whitepaper da AWS

Table of Contents

Construção de uma infraestrutura de rede da AWS escalável e segura com várias VPCs

Data de publicação: 10 de junho de 2020 (Histórico do documento)

Resumo

Os clientes da AWS geralmente dependem de centenas de contas e VPCs para segmentar suas workloads e expandir a presença deles. Normalmente, esse nível de escala cria dificuldades com relação ao compartilhamento de recursos, à conectividade entre VPCs e à conectividade on-premises com a VPC.

Este whitepaper descreve as práticas recomendadas para criar arquiteturas de rede escaláveis e seguras em uma grande rede usando serviços da AWS como Amazon VPC, AWS Transit Gateway, AWS PrivateLink e AWS Direct Connect Gateway. Ele demonstra soluções para gerenciar uma infraestrutura crescente e garantir escalabilidade, alta disponibilidade e segurança, bem como manter os custos indiretos baixos.

Introdução

Para começar, os clientes da AWS criam recursos em uma única conta da AWS que representa um limite de gerenciamento que segmenta permissões, custos e serviços. No entanto, à medida que a organização do cliente se expande, é necessária uma maior segmentação dos serviços para monitorar custos, controlar o acesso e facilitar o gerenciamento do ambiente. A solução de várias contas resolve esses problemas por fornecer contas específicas para serviços de TI e usuários dentro de uma organização. A AWS fornece várias ferramentas para gerenciar e configurar essa infraestrutura, como o AWS Landing Zone e o AWS Control Tower.

Figura 1: estrutura da conta Landing Zone

O AWS Landing Zone e o AWS Control Tower automatizam a configuração e a integração de vários serviços da AWS para fornecer um ambiente de referência, altamente controlado e de várias contas com Identity and Access Management (IAM), governança, segurança de dados, design de rede e registro em log.

Na Figura 1, a solução AWS Landing Zone inclui quatro contas: a conta do AWS Organizations (usada para gerenciar a configuração e o acesso às contas gerenciadas do AWS Landing Zone), a conta de serviços compartilhados (usada para criar serviços compartilhados de infraestrutura, como serviços de diretório), a conta de arquivo de logs (registro em log centralizado em buckets do S3) e a conta de segurança (a ser usada pela equipe de segurança e conformidade de uma empresa para auditar ou executar operações de segurança de emergência no caso de um incidente nas contas spoke).

Este whitepaper apresenta uma conta de serviços de rede de propriedade da equipe de redes que gerencia sua infraestrutura da AWS. Os serviços de rede e a infraestrutura de rede da conta são compartilhados por todas as contas e VPCs de forma centralizada (semelhante a um design hub e spoke). Esse design oferece uma melhor capacidade de gerenciamento para sua zona de aterrissagem e ajuda a reduzir os custos ao eliminar a necessidade de duplicar serviços de rede em cada conta e VPC spoke.

> **Note**
>
> Neste whitepaper, “zona de aterrissagem” é um termo abrangente que se refere à configuração escalável, segura e funcional de várias contas/várias VPCs em que você implanta suas workloads. Essa configuração pode ser criada usando qualquer ferramenta.

A maioria dos clientes começa com algumas VPCs para implantar a infraestrutura. O número de VPCs que um cliente possui geralmente está relacionado ao número de contas, usuários e ambientes preparados (produção, desenvolvimento, teste etc.). À medida que o uso da nuvem aumenta, o número de usuários, unidades de negócios, aplicações e regiões com os quais um cliente interage multiplica-se, levando à criação de novas VPCs.

À medida que o número de VPCs aumenta, o gerenciamento entre VPCs se torna essencial para a operação da rede em nuvem do cliente. Este whitepaper aborda as práticas recomendadas para três áreas específicas em conectividade híbrida e entre VPCs:

- Conectividade de rede: interconexão de VPCs e redes on-premises em escala.
- Segurança de rede: criação de pontos de saída centralizados para acessar a Internet e endpoints de gateway NAT, de VPC e do AWS PrivateLink.
- Gerenciamento de DNS: resolução de DNS dentro da zona de aterrissagem e do DNS híbrido.

Conectividade de VPC para VPC

Os clientes podem usar dois padrões de fluxo de VPC diferentes para configurar ambientes de várias VPCs: muitos para muitos ou hub e spoke. Na abordagem de muitos para muitos, o tráfego entre cada VPC é gerenciado individualmente entre cada VPC. No modelo hub e spoke, todo tráfego entre VPCs flui por meio de um recurso central, que encaminha o tráfego com base em regras estabelecidas.

Tópicos

Emparelhamento de VPC

A maneira mais simples de conectar duas VPCs é usar o emparelhamento de VPC. Nessa configuração, uma conexão permite conectividade bidirecional completa entre as VPCs. Essa conexão de emparelhamento é usada para encaminhar o tráfego entre as VPCs. As VPCs nas contas e regiões da AWS também podem ser emparelhadas. O emparelhamento de VPC gera apenas custos para o tráfego que ocorre na conexão (não há taxa de infraestrutura por hora).

O emparelhamento de VPC é uma conectividade ponto a ponto e não comporta roteamento transitivo. Por exemplo, se você tiver uma conexão de emparelhamento de VPC entre a VPC A e a VPC B e entre a VPC A e a VPC C, uma instância na VPC B não poderá transitar pela VPC A para alcançar a VPC C. Para encaminhar pacotes entre a VPC B e a VPC C, será necessário criar uma conexão direta de emparelhamento de VPC.

Em escala, quando você tem de 10 a 100 VPCs, a interconexão com o emparelhamento gera uma malha de 100 a 1.000 conexões de emparelhamento, as quais são difíceis de gerenciar e escalar. Há um limite máximo de 125 conexões de emparelhamento por VPC.

Figura 2: configuração de rede usando emparelhamento de VPC

Se você estiver usando o emparelhamento de VPC, será necessário estabelecer conectividade on-premises (VPN e/ou Direct Connect) para cada VPC. Os recursos em uma VPC não podem ser acessados on-premises usando a conectividade híbrida de uma VPC emparelhada (Figura 2).

O emparelhamento de VPC é mais adequado quando os recursos em uma VPC precisam se comunicar com recursos em outra VPC, o ambiente de ambas as VPCs é controlado e protegido e o número de VPCs a serem conectadas é inferior a dez (para permitir o gerenciamento individual de cada conexão). O emparelhamento de VPC oferece o menor custo geral quando comparado a outras opções de conectividade entre VPCs.

Solução Transit VPC

As VPCs de trânsito podem resolver algumas das deficiências do emparelhamento de VPC por meio da introdução de um design hub e spoke para conectividade entre VPCs. Em uma rede de VPC de trânsito, uma VPC central (a VPC de hub) se conecta a todas as outras VPCs (VPC spoke) por meio de uma conexão VPN que normalmente utiliza BGP sobre IPsec. A VPC central contém instâncias do EC2 que executam dispositivos de software que encaminham o tráfego de entrada aos respectivos destinos usando a sobreposição de VPN (Figura 3). O emparelhamento de VPC de trânsito oferece as seguintes vantagens:

- O roteamento transitivo é ativado usando a VPN de sobreposição, o que permite um design hub e spoke mais simples.
- Ao usar software de fornecedor terceirizado na instância do EC2 na VPC de trânsito hub, é possível utilizar a funcionalidade de segurança avançada do fornecedor (firewall/IPS/IDs de camada 7). Se os clientes estiverem usando o mesmo software on-premises, eles se beneficiam de uma experiência operacional/de monitoramento unificada.

Figura 3: VPC de trânsito com CSRs da Cisco

A VPC de trânsito tem seus próprios desafios, como custos mais altos para a execução de dispositivos virtuais, taxa de transferência limitada por VPC (até 1,25 Gbps por túnel VPN) e sobrecarga adicional de configuração e gerenciamento (os clientes precisam gerenciar a disponibilidade e a redundância de instâncias do EC2).

Gateway de trânsito

O AWS Transit Gateway oferece um design hub e spoke para conectar VPCs e redes on-premises como um serviço totalmente gerenciado sem exigir o provisionamento de dispositivos virtuais como os CSRs da Cisco. Nenhuma sobreposição de VPN é necessária, e a AWS gerencia a alta disponibilidade e escalabilidade.

O Transit Gateway permite que os clientes conectem milhares de VPCs. Você pode anexar toda conectividade híbrida (conexões VPN e Direct Connect) a um único Transit Gateway, consolidando e controlando toda a configuração de roteamento da AWS de sua organização em um só lugar (Figura 4). O Transit Gateway controla como o tráfego é encaminhado entre todas as redes spoke conectadas usando tabelas de rotas. Esse modelo de hub e spoke simplifica o gerenciamento e reduz os custos operacionais porque as VPCs só se conectam ao Transit Gateway para obter acesso às redes conectadas.

Figura 4: design hub e spoke com o AWS Transit Gateway

O Transit Gateway é um recurso regional e pode conectar milhares de VPCs na mesma região da AWS. Você pode criar vários Transit Gateways por região, mas os Transit Gateways em uma região da AWS não podem ser emparelhados. Além disso, você pode se conectar a no máximo três Transit Gateways em uma única conexão do Direct Connect para conectividade híbrida. Por esses motivos, você deve restringir sua arquitetura a apenas um Transit Gateway para conectar todas as VPCs em determinada região e usar tabelas de roteamento do Transit Gateway para isolá-las sempre que necessário. Há um caso válido para a criação de vários Transit Gateways puramente para limitar o raio de expansão dos erros de configuração.

Coloque o Transit Gateway de sua organização em sua conta de serviços de rede. Isso permite o gerenciamento centralizado por engenheiros de rede que gerenciam a conta de serviços de rede. Use o AWS Resource Access Manager (RAM) para compartilhar um Transit Gateway e conectar VPCs em várias contas em sua organização da AWS na mesma região. O AWS RAM permite que você compartilhe recursos da AWS com facilidade e segurança com qualquer conta da AWS ou dentro de sua organização da AWS. Para obter mais informações, consulte a publicação de blog Automating AWS Transit Gateway attachments to a transit gateway in a central account (Automação de anexos do AWS Transit Gateway para um transit gateway em uma conta central).

Tópicos

- Transit Gateway versus Transit VPC

Transit Gateway versus Transit VPC

O Transit Gateway oferece várias vantagens em relação ao Transit VPC:

- O Transit Gateway abstrai a complexidade de manter conexões VPN com centenas de VPCs.
- Ele elimina a necessidade de gerenciar e escalar dispositivos de software baseados no EC2. A AWS é responsável por gerenciar todos os recursos necessários para encaminhar o tráfego.
- O Transit Gateway elimina a necessidade de gerenciar a alta disponibilidade, fornecendo uma infraestrutura multi-AZ altamente disponível e redundante.
- O Transit Gateway melhora a largura de banda para comunicação entre VPCs para velocidades de intermitência de 50 Gbps por AZ.
- Ele otimiza os custos do usuário com um modelo simples por hora por GB transferido.
- O Transit Gateway diminui a latência ao remover proxies do EC2 e a necessidade de encapsulamento de VPN.

Transit Gateway versus emparelhamento de VPC

O Transit Gateway resolve a complexidade relacionada à criação e ao gerenciamento de várias conexões de emparelhamento de VPC em escala. Embora isso torne o Transit Gateway (TGW) um bom padrão para a maioria das arquiteturas de rede, o emparelhamento de VPC ainda é uma opção válida devido às seguintes vantagens que ele tem sobre o TGW:

- Custo mais baixo: com o emparelhamento de VPC, você paga apenas as cobranças de transferência de dados. Além das taxas de transferência de dados, o Transit Gateway tem uma cobrança por hora por anexo.
- Ausência de limites de largura de banda: com o Transit Gateway, a largura de banda máxima (de pico) por conexão VPC é 50 Gbps. O emparelhamento de VPC não oferece largura de banda agregada. Os limites de performance de rede de instâncias individuais e os limites de fluxo (10 Gbps dentro de um grupo de posicionamento e 5 Gbps de outra forma) se aplicam a ambas as opções. Somente o emparelhamento de VPC comporta grupos de posicionamento.
- Latência: diferentemente do emparelhamento de VPC, o Transit Gateway é um salto adicional entre as VPCs.

- Compatibilidade com grupos de segurança: a referência a grupos de segurança funciona com o emparelhamento de VPC dentro da região. No momento, isso não funciona com o Transit Gateway.

Na configuração da zona de aterrissagem, o emparelhamento de VPC pode ser usado com o modelo hub e spoke habilitado pelo Transit Gateway.

AWS PrivateLink

Os clientes podem querer expor de forma privada um serviço/aplicação que reside em uma VPC (provedor de serviços) a outras VPCs de consumidor em uma região da AWS de uma maneira que somente as VPCs de consumidor iniciem conexões com a VPC do provedor de serviços. Um exemplo é a possibilidade de suas aplicações privadas acessarem APIs do provedor de serviços.

Para usar o AWS PrivateLink, crie um Network Load Balancer para sua aplicação em sua VPC, bem como uma configuração de serviço de endpoint da VPC apontando para esse balanceador de carga. Em seguida, um consumidor de serviços cria um endpoint de interface para o seu serviço. Isso cria uma interface de rede elástica na sua sub-rede com um endereço IP privado que serve de ponto de entrada para o tráfego destinado ao serviço. O consumidor e o serviço não precisam estar na mesma VPC. Se a VPC for diferente, as VPCs de consumidor e de provedor de serviços poderão ter intervalos de endereços IP sobrepostos. Além de criar o endpoint de interface da VPC para acessar serviços em outras VPCs, você pode criar endpoints de interface de VPC para acessar de forma privada os serviços da AWS compatíveis por meio do AWS PrivateLink (Figura 5).

Figura 5: AWS PrivateLink

A escolha entre o Transit Gateway, o emparelhamento de VPC e o AWS PrivateLink depende da conectividade.

AWS PrivateLink: use o AWS PrivateLink quando você tiver um cliente/servidor configurado e quiser conceder acesso unidirecional a uma ou mais VPCs de consumidor a um serviço específico ou a um conjunto de instâncias na VPC do provedor de serviços. Somente os clientes na VPC de consumidor podem iniciar uma conexão com o serviço na VPC do provedor de serviços. Essa opção também é adequada quando o cliente e os servidores nas duas VPCs têm endereços IP sobrepostos, pois o AWS PrivateLink utiliza ENIs dentro da VPC cliente para que não haja conflitos de IP com o provedor de serviços. Você pode acessar endpoints do AWS PrivateLink por meio do emparelhamento da VPC, da VPN e do AWS Direct Connect.

Emparelhamento de VPC e Transit Gateway: use o emparelhamento de VPC e o Transit Gateway quando quiser habilitar a conectividade IP de camada 3 entre VPCs.

Sua arquitetura conterá uma combinação dessas tecnologias para atender a diferentes casos de uso. Todos esses serviços podem ser combinados e operados entre si. Por exemplo, o AWS PrivateLink, para lidar com a conectividade cliente-servidor do estilo API, o emparelhamento de VPC, para lidar com requisitos de conectividade direta em que os grupos de posicionamento ainda possam ser desejados na conectividade de região ou entre regiões, e o Transit Gateway, para simplificar a conectividade de VPCs em escala, bem como a consolidação da borda para conectividade híbrida.

Compartilhamento da Amazon VPC

O compartilhamento de VPCs é útil quando o isolamento de rede entre equipes não precisa ser gerenciado estritamente pelo proprietário da VPC, mas os usuários e as permissões em nível de conta precisam. Com a VPC compartilhada, várias contas da AWS criam os respectivos recursos da aplicação (como instâncias do Amazon EC2) em Amazon VPCs compartilhadas e gerenciadas centralmente. Nesse modelo, a conta que possui a VPC (proprietária) compartilha uma ou mais sub-redes com outras contas (participantes). Quando uma sub-rede é compartilhada, os participantes podem visualizar, criar, modificar e excluir os recursos de seus aplicativos nas sub-redes compartilhadas com eles. Os participantes não poderão visualizar, modificar ou excluir recursos que pertencerem a outros participantes ou proprietários da VPC. A segurança entre recursos em VPCs compartilhadas é gerenciada por meio de grupos de segurança e ACLs de rede da sub-rede.

Benefícios do compartilhamento de VPC:

- Design simplificado: ausência de complexidade com relação à conectividade entre VPCs.
- Menos VPCs gerenciadas.
- Segregação de tarefas entre equipes de rede e proprietários de aplicações.
- Melhor utilização do endereço IPv4.
- Custos mais baixos: ausência de cobranças de transferência de dados entre instâncias pertencentes a contas diferentes dentro da mesma zona de disponibilidade.

Observação: quando você compartilha uma sub-rede com várias contas, seus participantes devem ter algum nível de cooperação, pois estão compartilhando espaço IP e recursos de rede. Se necessário, você pode optar por compartilhar uma sub-rede diferente para cada conta participante.

Uma sub-rede por participante permite que a ACL da rede forneça isolamento de rede, além de grupos de segurança.

A maioria das arquiteturas de cliente conterá várias VPCs, e muitas delas serão compartilhadas com duas ou mais contas. O Transit Gateway e o emparelhamento de VPC podem ser usados para conectar as VPCs compartilhadas. Por exemplo, digamos que você tenha dez aplicações. Cada uma requer uma conta da AWS exclusiva. As aplicações podem ser categorizadas em dois portfólios (aquelas dentro do mesmo portfólio têm requisitos de rede semelhantes, como aplicações 1-5 em “Marketing'” e aplicações 6-10 em “Vendas”).

Você pode ter uma VPC para cada portfólio de aplicações (um total de duas VPCs), e a VPC é compartilhada com as diferentes contas de proprietário de aplicações dentro desse portfólio. Os proprietários implantam as aplicações na respectiva VPC compartilhada (nesse caso, nas diferentes sub-redes para segmentação e isolamento de rotas de rede usando NACLs). As duas VPCs compartilhadas são conectadas por meio do Transit Gateway. Com essa configuração, em vez de precisar conectar dez VPCs, você conecta apenas duas (Figura 6).

Figura 6: exemplo de configuração de VPC compartilhada

> **Note**
>
> Os participantes do compartilhamento de VPC não podem criar todos os recursos da AWS em uma sub-rede compartilhada. Para obter mais informações, consulte Limites da Amazon VPC.

Conectividade híbrida

Esta seção aborda principalmente a conexão segura de seus recursos de nuvem com seus datacenters on-premises. Existem duas abordagens para permitir a conectividade híbrida:

1. Conectividade individualizada: nessa configuração, uma conexão VPN e/ou VIF privada do Direct Connect é criada para cada VPC. Para isso, utiliza-se o gateway privado virtual (VGW). Essa opção é ótima para um pequeno número de VPCs, mas, à medida que o cliente escala as VPCs dele, o gerenciamento da conectividade híbrida por VPC pode se tornar difícil.
2. Consolidação de borda: nessa configuração, os clientes consolidam a conectividade de TI híbrida para várias VPCs em um único endpoint. Todas as VPCs compartilham essas conexões híbridas. Isso é feito usando o AWS Transit Gateway e o Direct Connect Gateway.

Tópicos

VPN

Figura 7:AWS VPN opções de terminação

Existem três maneiras de configurar a VPN para a AWS:

1. Consolidar a conectividade da VPN no Transit Gateway: essa opção utiliza o anexo da VPN do gateway de trânsito no Transit Gateway. O Transit Gateway comporta a terminação de IPsec para VPN de local a local. Os clientes podem criar túneis VPN para o Transit Gateway e acessar as VPCs anexadas a ele. O Transit Gateway comporta conexões VPN tanto estáticas quanto dinâmicas baseadas em BGP. O Transit Gateway também comporta vários caminhos de custo igual) (ECMP) em anexos da VPN. Cada conexão VPN tem uma taxa de transferência máxima de 1,25 Gbps, e habilitar o ECMP permite agregar a taxa de transferência entre conexões VPN. Nessa opção, você paga o preço do Transit Gateway, bem como o do AWS VPN. Recomendamos usar essa opção para conectividade de VPN. Para obter mais informações, consulte Visão geral sobre AWS VPN.

2. Terminar a VPN na instância do EC2: essa opção é utilizada pelos clientes em casos extremos quando eles querem um conjunto de recursos de software de fornecedor específico (como Cisco DMVPN ou GRE) ou desejam consistência operacional em várias implantações de VPN. Você pode utilizar o design da VPC de trânsito para consolidação de borda, mas é importante lembrar que todas as principais considerações da seção de conectividade de VPC para VPC de trânsito são aplicáveis à conectividade de VPN híbrida. Você é responsável pelo gerenciamento da alta disponibilidade e paga pelos custos da instância do EC2, bem como pelo licenciamento de software de qualquer fornecedor.
3. Terminar a VPN em um gateway privado virtual (VGW): essa opção permite um design de conectividade individualizada em que você cria uma conexão VPN (que consiste em um par de túneis VPN redundantes) por VPC. Essa é uma ótima maneira de começar a usar a conectividade de VPN na AWS. Entretanto, à medida que você escalar o número de VPCs, o projeto de consolidação de borda que utiliza o Transit Gateway vai acabar se evidenciando uma opção melhor. A taxa de transferência de VPN para uma VPC é limitada a 1,25 Gbps e o balanceamento de carga ECMP não é comportado. Do ponto de vista de preço, você paga apenas o preço da AWS VPN. Não há cobrança pela execução de um VGW. Para obter mais informações, consulte Preços do AWS VPN e AWS VPN no gateway privado virtual.

Direct Connect

Embora a VPN pela Internet seja uma ótima opção para começar, a conectividade com a Internet pode não ser confiável para o tráfego de produção. Devido a essa falta de confiabilidade, muitos clientes optam pelo AWS Direct Connect, que permite uma conectividade de fibra dedicada, consistente, de baixa latência e de alta largura de banda entre os datacenters dos clientes e a AWS. Há quatro maneiras de utilizar o AWS Direct Connect para se conectar a VPCs:

Figura 8: quatro maneiras de conectar seus datacenters on-premises à zona de aterrissagem

- Criar uma VIF (interface virtual) privada para um VGW anexado a uma VPC: é possível criar 50 VIFs por conexão do Direct Connect, o que permite que você se conecte 50 VPCs no máximo (uma VIF fornece conectividade para uma VPC). Há um emparelhamento BGP por VPC. A conectividade nessa configuração é restrita à região da AWS em que o Direct Connect está localizado. O mapeamento individualizado da VIF para VPC (e a falta de acesso global) torna esse meio o menos preferido para acessar VPCs na zona de aterrissagem.
- Criar uma VIF privada para um gateway do Direct Connect associado a vários VGWs (cada VGW é anexado a uma VPC): Um gateway do Direct Connect pode se conectar a até 10 VGWs

globalmente (exceto a China) em qualquer conta da AWS. Essa é uma excelente opção quando uma zona de aterrissagem consiste em um pequeno número de VPCs (dez ou menos VPCs) e/ou você precisa de acesso global. Há um emparelhamento BGP por Direct Connect Gateway e por conexão do Direct Connect. O gateway do Direct Connect destina-se apenas ao fluxo de tráfego norte/sul e não permite conectividade de VPC para VPC.

- Criar uma VIF de trânsito para um gateway do Direct Connect associado ao Transit Gateway: você pode associar um Transit Gateway a um gateway do Direct Connect por meio de uma conexão do Direct Connect dedicada ou hospedada em execução a 1 Gbps ou mais. Essa opção permite conectar seu datacenter on-premises a até três Transit Gateways (que podem se conectar a milhares de VPCs) em diferentes regiões da AWS e contas da AWS em um emparelhamento de VIF e BGP. Essa é a configuração mais simples entre as quatro opções para conectar várias VPCs em escala, mas você deve estar atento às limitações do Transit Gateway. Uma limitação importante é que você pode anunciar apenas 20 intervalos CIDR de um Transit Gateway para um roteador on-premises na VIF de trânsito. Com as opções 1 e 2, você paga o preço do Direct Connect. Para a opção 3, você também paga pelo anexo do Transit Gateway e cobranças de transferência de dados. Acesse a documentação Transit Gateway Associations on Direct Connect para obter mais informações.
- Criar uma conexão VPN com o Transit Gateway via VIF pública do Direct Connect: uma interface virtual pública permite acessar todos os serviços públicos e endpoints da AWS usando os endereços IP públicos. Ao criar um anexo de VPN em um Transit Gateway, você obtém dois endereços IP públicos para terminação da VPN no lado da AWS. Esses IPs públicos podem ser acessados pela VIF pública. Você pode criar quantas conexões VPN para quantos Transit Gateways quiser por meio da VIF pública. Quando você cria um emparelhamento BGP na VIF pública, a AWS anuncia todo o intervalo de IP público da AWS para seu roteador. Para que você permita apenas determinado tráfego (por exemplo, tráfego apenas para os endpoints de terminação da VPN), é aconselhável usar um firewall on-premises. Essa opção pode ser usada para criptografar o Direct Connect na camada de rede.

Embora a terceira opção (VIF de trânsito para o gateway do Direct Connect) possa parecer a melhor, pois permite consolidar toda conectividade on-premises para determinada região da AWS em um único ponto (Transit Gateway) usando uma única sessão BGP por conexão do Direct Connect, tendo em vista alguns dos limites e considerações sobre a opção 3, esperamos que os clientes utilizem as opções 2 e 3 para os requisitos de conectividade de zona de aterrissagem deles. A Figura 9 mostra um exemplo de configuração em que a VIF de trânsito é usada como método padrão para conexão com VPCs e uma VIF privada é usada para um caso de uso de borda em que é necessário transferir uma grande quantidade de dados de um datacenter on-premises para a VPC de mídia.

A VIF privada é usada para evitar cobranças de transferência de dados do Transit Gateway. Como prática recomendada, você deve ter pelo menos duas conexões em dois locais diferentes do Direct Connect para obter redundância máxima; isto é, um total de quatro conexões. Você cria uma VIF por conexão para um total de quatro VIFs privadas e quatro VIFs de trânsito. Você também cria uma VPN como uma conectividade de backup para conexões do AWS Direct Connect.

Figura 9: exemplo de arquitetura de referência para conectividade híbrida

Use a conta de serviços de rede para criar recursos do Direct Connect que permitem a demarcação dos limites administrativos da rede. A conexão do Direct Connect, o gateway do Direct Connect e o Transit Gateway podem residir em uma conta de serviços de rede. Para compartilhar a conectividade do AWS Direct Connect com sua zona de aterrissagem, basta compartilhar o Transit Gateway com outras contas por meio do RAM.

Saída centralizada para a Internet

Ao implantar aplicações em sua zona de aterrissagem, muitas delas exigirão apenas acesso de saída à Internet (por exemplo, baixar atualizações de bibliotecas/patches/sistema operacional). Você pode conseguir isso de preferência usando um gateway de conversão de endereço de rede (NAT) ou, alternativamente, uma instância do EC2 (configurada com NAT de origem (SNAT)) como o próximo salto para todo o acesso de saída à Internet. As aplicações internas residem em sub-redes privadas, enquanto as instâncias de gateway NAT/EC2 NAT residem em uma sub-rede pública.

Utilização de um gateway NAT

A implantação de um gateway NAT em cada VPC spoke pode se tornar cara porque você paga uma taxa por hora para cada gateway NAT implantado (consulte Preço da Amazon VPC). Por isso, centralizá-lo pode ser uma opção viável. Para centralizá-lo, criamos uma VPC de saída na conta de serviços de rede e, utilizando o Transit Gateway, que é mostrado na Figura 10, encaminhamos todo o tráfego de saída das VPCs spoke por meio de um gateway NAT localizado nessa VPC.

Observação: ao centralizar o gateway NAT usando o Transit Gateway, você paga uma taxa extra de processamento de dados do Transit Gateway, comparativamente à abordagem descentralizada de execução de um gateway NAT em cada VPC. Em alguns casos extremos, quando você envia grandes quantidades de dados de uma VPC por meio do gateway NAT, manter o NAT local na VPC para evitar a cobrança de processamento de dados do Transit Gateway pode ser uma opção mais econômica.

Figura 10: gateway NAT centralizado usando o Transit Gateway (visão geral)

Figura 11: gateway NAT centralizado usando o Transit Gateway (design de tabela de rotas)

Nesta configuração, os anexos da VPC spoke são associados à tabela de rotas 1 (RT1) e propagados para a tabela de rotas 2 (RT2). Adicionamos explicitamente uma rota blackhole para impedir que as duas VPCs se comuniquem entre si. Se quiser permitir a comunicação entre VPCs, você pode remover a entrada de rota “10.0.0.0/8 -> Blackhole” da RT1. Isso permite que elas se comuniquem por meio do gateway NAT. Você também pode propagar os anexos da VPC spoke para a RT1 (ou, alternativamente, usar uma tabela de rotas e associar/propagar tudo para ela), o que permite um fluxo de tráfego direto entre as VPCs por meio do Transit Gateway.

Adicionamos uma rota estática na RT1 apontando todo o tráfego para a VPC de saída. Devido a essa rota estática, o Transit Gateway envia todo o tráfego da Internet por meio de ENIs na VPC de saída. Uma vez na VPC de saída, o tráfego segue as regras definidas na tabela de rotas de sub-rede em que essas ENIs do Transit Gateway estão presentes. Adicionamos uma rota nesta tabela de rotas de sub-rede apontando todo o tráfego para o gateway NAT. A tabela de rotas de sub-rede do gateway NAT tem o gateway da Internet (IGW) como próximo salto. Para que o tráfego de retorno retorne, você deve adicionar uma entrada de tabela de rotas estática na tabela de rotas de sub-rede do gateway NAT apontando todo o tráfego direcionado à VPC spoke para o Transit Gateway como próximo salto.

Alta disponibilidade

Para alta disponibilidade, você deve usar dois gateways NAT (um em cada zona de disponibilidade). Em uma zona de disponibilidade (AZ), o gateway NAT tem um Acordo de Nível de Serviço de disponibilidade de 99,9%. A redundância contra falha de componentes em uma AZ é tratada pela AWS de acordo com o Acordo de Nível de Serviço. O tráfego é descartado durante 0,1% do tempo em que o gateway NAT pode estar indisponível em uma AZ. Se uma AZ falhar completamente, o endpoint do Transit Gateway e o gateway NAT nessa AZ apresentarão falha e todo o tráfego fluirá através dos endpoints do Transit Gateway e do gateway NAT na outra AZ.

Segurança

Você conta com grupos de segurança nas instâncias de origem, rotas blackhole nas tabelas de rotas do Transit Gateway e a ACL de rede da sub-rede na qual o gateway NAT está localizado.

Escalabilidade

Um gateway NAT comporta no máximo 55.000 conexões simultâneas para cada destino exclusivo. Do ponto de vista de taxa de transferência, você está restrito aos limites de performance do gateway NAT. O Transit Gateway não é um balanceador de carga e não distribuirá o tráfego uniformemente no gateway NAT nas várias AZs. O tráfego no Transit Gateway permanecerá dentro de uma AZ, se possível. Se a instância do EC2 que está iniciando o tráfego estiver na AZ 1, o tráfego fluirá para fora da interface de rede elástica do Transit Gateway na mesma AZ 1 na VPC de saída e fluirá para o próximo salto com base na tabela de rotas da sub-rede em que a interface de rede elástica reside. Para obter uma lista completa de regras, consulte Regras e limites do gateway NAT.

Para obter mais informações, consulte a publicação de blog Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway (Como criar um único ponto de saída da Internet de várias VPCs usando o AWS Transit Gateway).

Utilização de uma instância do EC2 para saída centralizada

A utilização de um dispositivo de firewall baseado em software (no EC2) do AWS Marketplace como ponto de saída é semelhante à configuração do gateway NAT. Essa opção pode ser usada se você quiser utilizar os recursos de firewall/sistema de prevenção/detecção de intrusões (IPS/IDS) da camada 7 oferecidos por vários fornecedores.

Na Figura 12, substituímos o gateway NAT por uma instância do EC2 (com SNAT habilitada na instância do EC2). Existem alguns fatores importantes a serem levados em conta com essa opção:

Alta disponibilidade

Nessa configuração, você é responsável por monitorar e detectar falhas na instância do EC2 e substituí-la por uma instância de backup/em espera. A maioria dos fornecedores da AWS tem automação pré-integrada para os respectivos softwares implantados nessa configuração. Essa automação pode controlar o seguinte:

- Detecção de falha da instância primária EC2-1.
- Alteração da tabela de rotas “Route Table Egx 1” para apontar todo o tráfego para a instância EC2-2 de backup na falha da instância primária. Isso também deve ser feito para as sub-redes na AZ 2.

Figura 12: NAT centralizada usando instâncias do EC2 e do Transit Gateway

Escalabilidade

O Transit Gateway não é um balanceador de carga e não distribuirá o tráfego uniformemente entre as instâncias nas duas AZs. O tráfego no Transit Gateway permanecerá dentro de uma AZ, se possível. Você está restrito aos recursos de largura de banda de uma única instância do EC2. É possível escalar verticalmente essa instância do EC2 à medida que o uso aumentar.

Se o fornecedor escolhido para inspeção de tráfego de saída não comportar automação para detecção de falhas ou se você precisar de escalabilidade horizontal, poderá usar um design alternativo. Nesse design (Figura 13), não criamos um anexo de VPC no gateway de trânsito para a VPC de saída. Em vez disso, criamos um anexo da VPN IPsec e uma VPN IPsec do Transit Gateway para as instâncias do EC2 utilizando BGP para trocar rotas.

Vantagens

- Detecção de falhas e redirecionamento do tráfego processado pelo BGP. Não é necessária nenhuma automação da tabela de rotas da sub-rede da VPC.
- O ECMP do BGP pode ser usado para balancear a carga do tráfego em várias instâncias do EC2. A escalabilidade horizontal é possível.

Figura 13: NAT centralizada usando instâncias do EC2 e VPN do Transit Gateway

Principais considerações

- Sobrecarga de gerenciamento de VPN em instâncias do EC2.
- A largura de banda no Transit Gateway é limitada a 1,25 Gbps por túnel VPN. Com o ECMP, o Transit Gateway pode comportar um total de até 50 Gbps de largura de banda de VPN. Os recursos de VPN e processamento de pacotes do dispositivo do fornecedor podem ser um fator limitante.
- Esse design pressupõe que a instância de firewall do EC2 está operando com a mesma interface de rede elástica para tráfego de entrada e saída.
- Se você habilitar o balanceamento de carga ECMP do tráfego em várias instâncias do EC2, deverá aplicar SNAT no tráfego da instância do EC2 para garantir a simetria do fluxo de retorno, o que significa que o destino não conhecerá a verdadeira origem.

Segurança de rede centralizada para tráfego de VPC para VPC e on-premises para VPC

A AWS fornece grupos de segurança e NACLS de sub-rede para implementar a segurança de rede em sua zona de aterrissagem. Esses firewalls são de camada 4. Pode haver situações em que um cliente queira implementar um firewall/IPS/IDs de camada 7 na zona de aterrissagem dele para inspecionar o tráfego entre VPCs ou entre um datacenter on-premises e uma VPC. Isso pode ser obtido usando o Transit Gateway e dispositivos de software de terceiros em execução em instâncias do EC2. Usando a arquitetura exibida na Figura 14, podemos permitir que o tráfego de VPC para VPC e on-premises para VPC flua por meio das instâncias do EC2. A configuração é semelhante à que já discutimos na Figura 12, mas além disso removemos a rota blackhole da Tabela de Rotas 1 para permitir o fluxo de tráfego da VPC interna e atribuímos o anexo da VPN e/ou o anexo do Direct Connect GW à Tabela de Rotas 1 para permitir o fluxo de tráfego híbrido. Isso permite que todo o tráfego proveniente das spokes flua para a VPC de saída antes de ser enviado ao destino. Você precisa de rotas estáticas na tabela de rotas de sub-rede da VPC de saída (onde residem os dispositivos EC2 do firewall) para enviar tráfego destinado a VPCs spoke e ao CIDR on-premises por meio do Transit Gateway após a inspeção de tráfego.

> **Note**
>
> As informações de rota não são propagadas dinamicamente do Transit Gateway para a tabela de rotas de sub-rede e devem ser inseridas estaticamente. Há um limite flexível de 50 rotas estáticas em uma tabela de rotas de sub-rede.

Figura 14: controle de tráfego de VPC para VPC e VPC para on-premises

Principais considerações ao enviar tráfego a instâncias do EC2 para inspeção em linha:

- Taxas adicionais de processamento de dados do Transit Gateway.
- O tráfego deve passar por dois outros saltos (instância do EC2 e Transit Gateway).
- Possibilidade de gargalos de largura de banda e performance.
- Maior complexidade para manutenção, gerenciamento e escalabilidade de instâncias do EC2:
  - Detecção de falhas e failover para o modo de espera.

- Rastreamento de uso e escalabilidade horizontal/vertical.
- Configuração de firewall, gerenciamento de patches.
- Conversão de endereço de rede de origem (SNAT) do tráfego durante o balanceamento de carga para garantir um fluxo simétrico.

Você deve ser seletivo quanto ao tráfego que passa por essas instâncias do EC2. Uma maneira de proceder é definir zonas de segurança e inspecionar o tráfego entre zonas não confiáveis. Uma zona não confiável pode ser um local remoto gerenciado por terceiros, uma VPC de fornecedor que você não controla/confia ou uma VPC de sandbox/desenvolvimento, que tem uma framework de segurança mais flexível em comparação com o restante de seu ambiente. A Figura 15 mostra a permissão do fluxo de tráfego direto entre redes confiáveis enquanto o fluxo de tráfego de/para redes não confiáveis é inspecionado por meio de instâncias do EC2 em linha. Criamos três zonas neste exemplo:

- Zona não confiável: destina-se a qualquer tráfego proveniente da “VPN para o local remoto não confiável” ou da VPC de um fornecedor terceirizado.
- Zona de produção: contém o tráfego da VPC de produção e do datacenter on-premises do cliente.
- Zona de desenvolvimento: contém o tráfego das duas VPCs de desenvolvimento.

A seguir são apresentados exemplos das regras que definimos para comunicação entre zonas:

1. Zona não confiável/zona de produção: comunicação não permitida
2. Zona de produção/zona de desenvolvimento: comunicação permitida por meio de dispositivos de firewall do EC2 na VPC de saída
3. Zona não confiável/zona de desenvolvimento: comunicação permitida por meio de dispositivos de firewall do EC2 na VPC de saída
4. Zona de produção/zona de produção e zona de desenvolvimento/zona de desenvolvimento: comunicação direta por meio do Transit Gateway

Essa configuração tem três zonas de segurança, mas você pode ter mais. Você pode usar várias tabelas de rotas e rotas blackhole para obter isolamento de segurança e um fluxo de tráfego ideal. A escolha das zonas certas depende da estratégia geral de design da zona de aterrissagem (estrutura da conta, design da VPC). Você pode ter zonas para permitir o isolamento entre unidades de negócios, aplicações, ambientes etc.

Neste exemplo, terminamos a VPN remota não confiável no Transit Gateway e enviamos todo o tráfego a dispositivos de firewall de software no EC2 para inspeção. Você pode também terminar essas VPNs diretamente nas instâncias do EC2 em vez de no Transit Gateway. Com essa abordagem, o tráfego não confiável da VPN nunca interage diretamente com o Transit Gateway. O número de saltos no fluxo de tráfego é reduzido em 1 e você diminui os custos da AWS VPN. Para habilitar a troca de rotas dinâmicas (para que o Transit Gateway conheça o CIDR da VPN remota via BGP), as instâncias de firewall devem ser conectadas ao Transit Gateway por meio da VPN. No modelo de anexo TGW nativo, você deve adicionar rotas estáticas na tabela de rotas TGW para VPN CIDE e o próximo salto como a VPC de saída/segurança. Em nossa configuração (Figura 15), temos uma rota padrão para todo tráfego para a VPC de saída. Por isso, não precisamos adicionar explicitamente nenhuma rota estática específica. Com essa abordagem, você passa de um endpoint de terminação da VPN do Transit Gateway totalmente gerenciado para uma instância do EC2 autogerenciada, adicionando sobrecarga de gerenciamento da VPN, bem como carga adicional na instância do EC2 em termos de computação e memória.

Figura 15: isolamento de tráfego por meio do Transit Gateway e da definição de zonas de segurança

DNS

Quando você inicia uma instância em uma VPC não padrão, a AWS fornece a ela um nome de host de DNS privado (e possivelmente um nome de host de DNS público), dependendo dos atributos de DNS que você especifica para a VPC e de sua instância ter ou não um endereço IPv4 público. Quando o atributo “enableDnsSupport” é definido como true (verdadeiro), você obtém uma resolução de DNS na VPC do Route 53 Resolver (deslocamento de IP +2 para o CIDR da VPC). Por padrão, o Route 53 Resolver responde a consultas de DNS para nomes de domínio da VPC, como nomes de domínio de instâncias do EC2 ou de balanceadores de carga do Elastic Load Balancing. Com o emparelhamento da VPC, os hosts em uma VPC podem resolver nomes de host de DNS público para endereços IP privados para instâncias em VPCs emparelhadas, desde que a opção para fazê-los esteja habilitada. O mesmo se aplica a VPCs conectadas por meio do AWS Transit Gateway. Para obter mais informações, consulte Habilitação da compatibilidade com resolução de DNS para uma conexão de emparelhamento de VPC.

Se você quiser mapear suas instâncias para um nome de domínio personalizado, poderá usar o Amazon Route 53 para criar um registro de mapeamento de DNS para IP personalizado. Uma zona hospedada do Amazon Route 53 é um contêiner com informações sobre como você deseja que o Amazon Route 53 responda a consultas de DNS para um domínio e os respectivos subdomínios. As zonas hospedadas públicas contêm informações de DNS que podem ser resolvidas pela Internet pública, enquanto as zonas hospedadas privadas são uma implementação específica que apresenta apenas informações para VPCs que foram anexadas à zona hospedada privada específica. Em uma configuração de zona de aterrissagem em que há várias VPCs/contas, você pode associar uma única zona hospedada privada a várias VPCs nas contas da AWS e nas regiões. Os hosts finais nas VPCs usam o respectivo IP do Resolvedor Route 53 (deslocamento +2 para o CIDR da VPC) como o servidor de nomes para consultas de DNS. O Route 53 Resolver na VPC aceita consultas de DNS somente de recursos dentro de uma VPC.

DNS híbrido

Coordenar a resolução de DNS entre a configuração do AWS Landing Zone e os recursos on-premises é um dos fatores mais importantes em uma rede híbrida. Os clientes que implementam ambientes híbridos geralmente têm um sistema de resolução de DNS já instalado e desejam uma solução de DNS que funcione em conjunto com o sistema atual. Quando você deseja integrar o DNS das VPCs em uma região da AWS ao DNS de sua rede, normalmente é necessário um endpoint de entrada do Route 53 Resolver (para consultas de DNS que esteja encaminhando às suas VPCs)

e um endpoint de saída do Route 53 Resolver (para consultas que esteja encaminhando de suas VPCs à rede). Conforme mostrado na Figura 16, você pode configurar endpoints do Resolver de saída para encaminhar consultas recebidas de instâncias do EC2 em suas VPCs para servidores de DNS de em sua rede. Para encaminhar consultas selecionadas, de uma VPC para on-premises, crie regras do Route 53 Resolver que especificam os nomes de domínio para as consultas de DNS que você deseja encaminhar (como example.com) e os endereços IP dos resolvedores de DNS na rede para os quais você deseja encaminhar as consultas. Para consultas de entrada on-premises para zonas hospedadas do Route 53, os servidores de DNS em sua rede podem encaminhar consultas para endpoints do Resolver de entrada em uma VPC especificada.

Figura 16: resolução de DNS híbrido usando o Route 53 Resolver

Isso permite que os resolvedores de DNS on-premises resolvam facilmente os nomes de domínio para recursos da AWS, como instâncias do EC2 ou registros em uma zona hospedada privada do Route 53 associada a essa VPC.

Não é recomendado criar endpoints do Route 53 Resolver em cada VPC da zona de aterrissagem. Centralize-os em uma VPC de saída central (na conta de serviços de rede). Essa abordagem melhora capacidade de gerenciamento e, ao mesmo tempo, mantém os custos baixos (é cobrada uma taxa por hora para cada endpoint de entrada/saída criado). Você compartilha o endpoint de entrada e saída centralizado com o resto da zona de aterrissagem.

Resolução de saída: use a conta de serviços de rede para redigir regras de resolução (com base em quais consultas de DNS serão encaminhadas a servidores de DNS on-premises). Usando o Resource Access Manager (RAM), compartilhe essas regras do Route 53 Resolver com várias contas (e as associe a VPCs nas contas). As instâncias do EC2 em VPCs spoke podem enviar consultas de DNS ao Route 53 Resolver. O Route 53 Resolver Service encaminhará essas consultas ao servidor de DNS on-premises por meio dos endpoints do Route 53 Resolver de saída na VPC de saída. Você não precisa emparelhar VPCs spoke com a VPC de saída nem as conectar por meio do Transit Gateway. Não use o IP do endpoint do resolvedor de saída como o DNS primário nas VPCs spoke. As VPCs spoke devem usar o Route 53 Resolver (para compensar o CIDR da VPC) na respectiva VPC.

Figura 17: centralização dos endpoints do Route 53 Resolver na VPC de saída

Resolução de DNS de entrada: crie endpoints de entrada do Route 53 Resolver em uma VPC centralizada e associe todas as zonas hospedadas privadas em sua zona de aterrissagem a

essa VPC centralizada. Para obter mais informações, consulte Associação de mais VPCs a uma zona hospedada privada. As várias zonas hospedadas privadas (PHZ) associadas a uma VPC não podem se sobrepor. Conforme mostrado na Figura 17, essa associação de PHZ à VPC centralizada permitirá que os servidores on-premises resolvam o DNS para qualquer entrada em qualquer zona hospedada privada (associada à VPC central) usando o endpoint de entrada na VPC centralizada. Para obter mais informações sobre configurações de DNS híbrido, consulte Gerenciamento centralizado de DNS da nuvem híbrida com o Amazon Route 53 e o AWS Transit Gateway e Opções de DNS de nuvem híbrida para a Amazon VPC.

Acesso centralizado a endpoints privados da VPC

Um endpoint da VPC permite que você conecte sua VPC de forma privada a serviços da AWS compatíveis sem a necessidade de um gateway da Internet ou de um dispositivo NAT. Com esse endpoint de interface, as instâncias em sua VPC não requerem endereços IP públicos para se comunicarem com endpoints de serviço da AWS. O tráfego entre a VPC e outros serviços não sai da estrutura da rede da AWS. Atualmente, dois tipos de endpoint podem ser provisionados: endpoints de interface (desenvolvidos com o AWS PrivateLink) e endpoints de gateway. Os endpoints de gateway podem ser provisionados livremente e não há um caso de uso de peso para centralização.

Endpoints de interface da VPC

Endpoint de interface é uma interface de rede elástica com endereço IP privado que serve de ponto de entrada para o tráfego destinado ao serviço da AWS compatível. Quando você provisiona um endpoint de interface, os usuários arcam com um custo para cada hora em que o endpoint estiver em execução. Por padrão, você cria um endpoint de interface em cada VPC da qual deseja acessar o serviço da AWS. Esse processo pode ser caro e difícil de gerenciar na configuração da zona de aterrissagem em que o cliente deseja interagir com um serviço específico da AWS em várias VPCs. Para evitar isso, você pode hospedar os endpoints de interface em uma VPC centralizada. Todas as VPCs spoke usarão esses endpoints centralizados.

Ao criar um endpoint de VPC para um serviço da AWS, você pode habilitar o DNS privado. Quando habilitada, a configuração cria uma zona hospedada privada (PHZ) do Route 53 que é gerenciada pela AWS e permite a resolução do endpoint de serviço público da AWS para o IP privado do endpoint da interface. A PHZ gerenciada só funciona dentro da VPC com o endpoint da interface. Em nossa configuração, quando queremos que as VPCs spoke resolvam o DNS do endpoint da VPC hospedado em uma VPC centralizada, a PHZ gerenciada não funciona. Para resolver isso, desabilite a opção que cria automaticamente o DNS privado quando um endpoint de interface é criado. Você também pode criar uma PHZ do Route 53 manualmente e adicionar um registro de alias com o nome completo do endpoint de serviço da AWS apontando para o endpoint de interface, conforme mostrado na Figura 18.

Figura 18: PHZ criada manualmente

Nós associamos essa zona hospedada privada a outras VPCs dentro da zona de aterrissagem. Essa configuração permite que as VPCs spoke resolvam os nomes de endpoint de serviço completo para endpoints de interface na VPC centralizada.

> **Note**
>
> Para acessar a zona hospedada privada compartilhada, os hosts nas VPCs spoke devem usar o IP do Route 53 Resolver da respectiva VPC. Os endpoints de interface também podem ser acessados de redes on-premises por VPN e pelo Direct Connect. Use regras de encaminhamento condicional para enviar todo o tráfego DNS dos nomes de endpoint de serviço completo aos endpoints de entrada do Route 53 Resolver, os quais resolverão as solicitações de DNS de acordo com a zona hospedada privada.

Na Figura 19, o Transit Gateway habilita o fluxo de tráfego das VPCs spoke para os endpoints de interface centralizados. Crie endpoints da VPC e a respectiva zona hospedada privada na conta de serviços de rede e compartilhe-os com as VPCs spoke nas contas spoke. Para obter mais detalhes sobre o compartilhamento de informações de endpoint com outras VPCs, consulte a publicação de blog Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver (Integração do AWS Transit Gateway ao AWS PrivateLink e ao Amazon Route 53 Resolver).

Observação: a abordagem distribuída de endpoint de VPC, isto é, um endpoint por VPC, permite que você aplique políticas de privilégio mínimo em endpoints da VPC. Em uma abordagem centralizada, você aplicará e gerenciará políticas para todos os acessos à VPC spoke em um único endpoint. Tendo em vista o número crescente de VPCs, a complexidade de manter o privilégio mínimo com um único documento de política pode aumentar. Quando há um único documento de política, o raio de expansão também é maior. Além disso, há restrição quanto ao tamanho do documento de política (20.480 caracteres).

Figura 19: centralização dos endpoints de interface da VPC

Conclusão

À medida que você escala o uso da AWS e implanta aplicações no AWS Landing Zone, o número de VPCs e componentes de rede aumenta. Este whitepaper explicou como podemos gerenciar essa infraestrutura crescente, garantindo escalabilidade, alta disponibilidade e segurança e, ao mesmo tempo, mantendo os custos baixos. Tomar as decisões corretas de design ao utilizar serviços como o Transit Gateway, VPC compartilhada, AWS Direct Connect, endpoints da VPC e dispositivos de software de terceiros passa a ser fundamental. É importante entender as principais considerações de cada abordagem e trabalhar retroativamente com base em seus requisitos e analisar qual opção ou combinação de opções é mais adequada para você.

Colaboradores

As seguintes pessoas contribuíram para este documento:

- Sidhartha Chauhan, arquiteto de soluções, Amazon Web Services
- Amir Abu-Akeel, arquiteto de infraestrutura de nuvem, Amazon Web Services
- Sohaib Tahir, arquiteto de soluções, Amazon Web Services

Histórico do documento

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

update-history-change	update-history-description	update-history-date
Atualização secundária	Seção Transit Gateway versus emparelhamento da VPC atualizada.	2 de abril de 2021
Whitepaper atualizado	Texto corrigido para corresponder às opções mostradas na Figura 7.	10 de junho de 2020
Atualização secundária	Texto corrigido para corresponder às opções mostradas na Figura 7.	10 de junho de 2020
Publicação inicial	Whitepaper publicado.	15 de novembro de 2019

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 de produto e práticas atuais da AWS, que estão sujeitas a alterações sem aviso prévio, e (c) não pressupõe nenhum compromisso ou garantia da AWS e de 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.