AWS Informe técnico

Construindo uma infraestrutura de rede AWS multi-VPC escalável e segura

Construindo uma infraestrutura de rede AWS multi-VPC escalável e segura: AWS Informe técnico

Table of Contents

Construindo uma infraestrutura de rede AWS multi-VPC escalável e segura

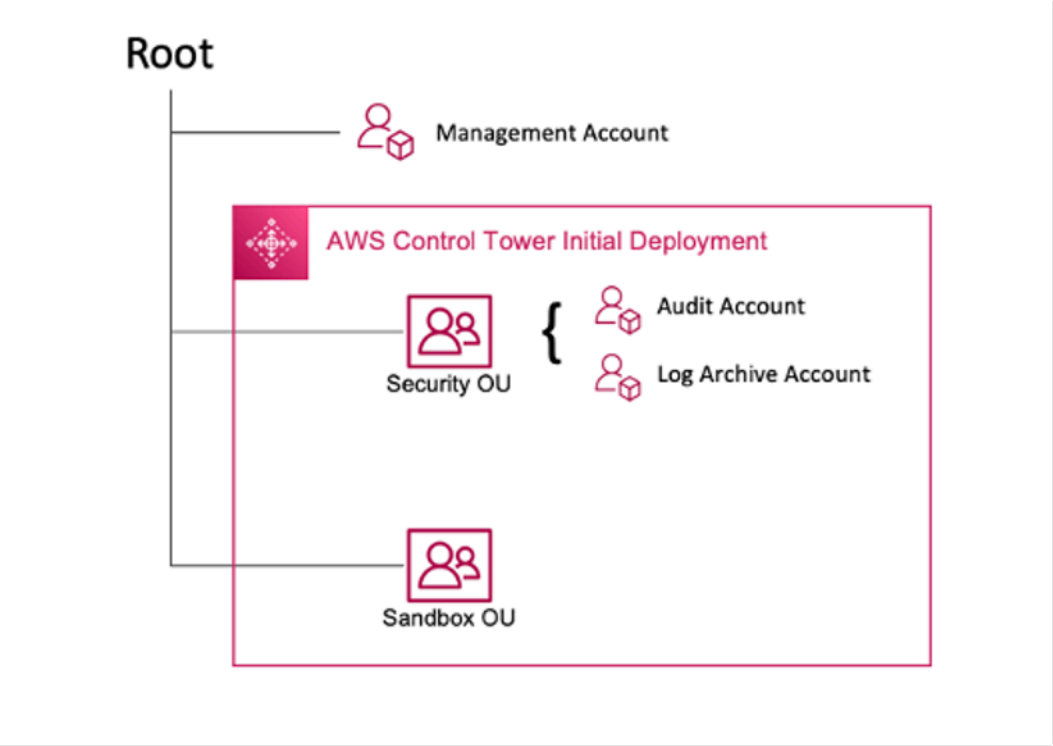
Data de publicação: 17 de abril de 2024 () Histórico do documento

Os clientes da Amazon Web Services (AWS) geralmente confiam em centenas de contas e nuvens privadas virtuais (VPCs) para segmentar suas cargas de trabalho e expandir sua presença. Esse nível de escala geralmente cria desafios em relação ao compartilhamento de recursos, conectividade entre VPCs e instalações locais à conectividade VPC.

Este whitepaper descreve as melhores práticas para criar arquiteturas de rede escaláveis e seguras em uma grande rede usando AWS serviços como Amazon Virtual Private Cloud (Amazon VPC),,, AWS Transit Gateway, AWS PrivateLinkGateway AWS Direct ConnectLoad Balancer e Amazon Route 53. AWS Network Firewall Ele demonstra soluções para gerenciar uma infraestrutura em crescimento, garantindo escalabilidade, alta disponibilidade e segurança, mantendo os custos indiretos baixos.

Introdução

AWS os clientes começam criando recursos em uma única AWS conta que representa um limite de gerenciamento que segmenta permissões, custos e serviços. No entanto, à medida que a organização do cliente cresce, torna-se necessária uma maior segmentação dos serviços para monitorar custos, controlar o acesso e facilitar o gerenciamento ambiental. Uma solução com várias contas resolve esses problemas fornecendo contas específicas para serviços de TI e usuários dentro de uma organização. AWS fornece várias ferramentas para gerenciar e configurar essa infraestrutura, inclusive AWS Control Tower.



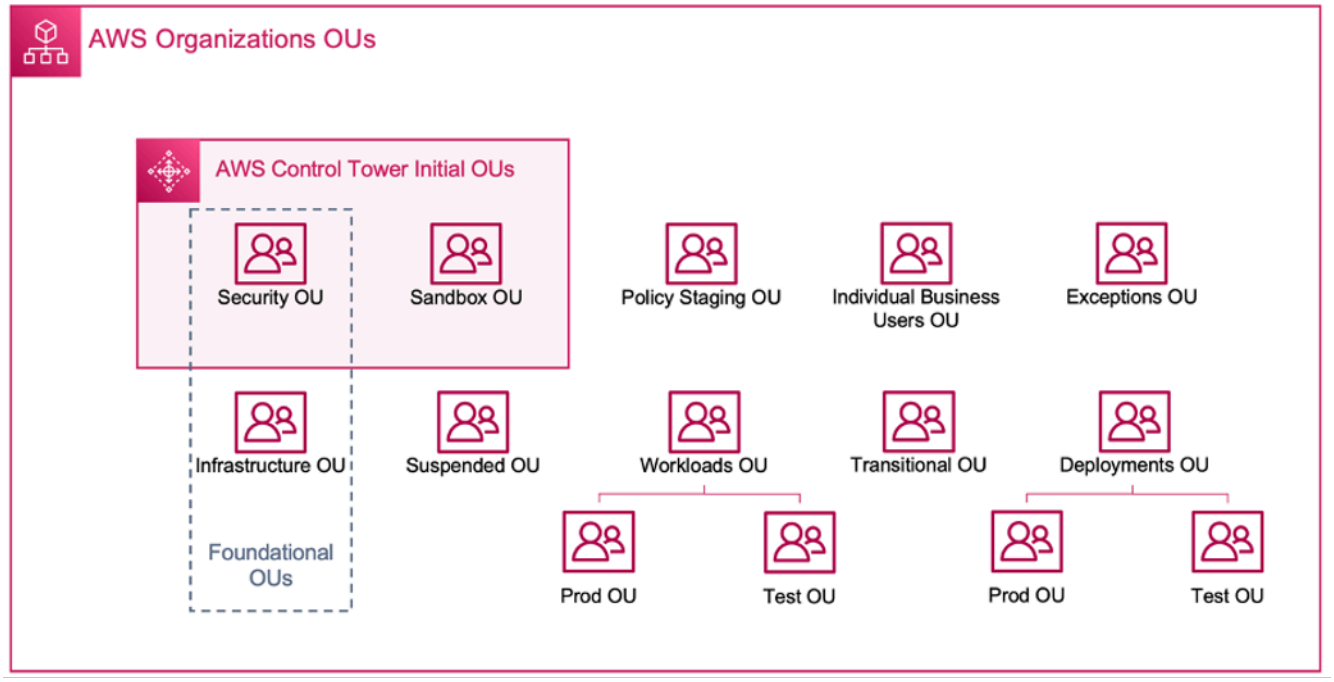
AWS Implantação inicial da Control Tower

Quando você configura seu ambiente de várias contas usando AWS Control Tower, ele cria duas unidades organizacionais (OUs):

- OU de segurança — Dentro dessa OU, AWS Control Tower cria duas contas:
- Arquivo de registros
- Auditoria (essa conta corresponde à conta do Security Tooling discutida anteriormente na orientação.)
- Sandbox OU — Essa OU é o destino padrão para contas criadas dentro AWS Control Tower dela. Ele contém contas nas quais seus criadores podem explorar e experimentar AWS serviços e outras ferramentas e serviços, de acordo com as políticas de uso aceitável da sua equipe.

AWS Control Tower permite criar, registrar e gerenciar OUs adicionais para expandir o ambiente inicial e implementar a orientação.

O diagrama a seguir mostra as OUs inicialmente implantadas pelo AWS Control Tower. Você pode expandir seu AWS ambiente para implementar qualquer uma das OUs recomendadas incluídas no diagrama, para atender às suas necessidades.



AWS OUs organizacionais

Para obter mais detalhes sobre o uso de ambientes com várias contas AWS Control Tower, consulte o Apêndice E no whitepaper Organizando seu AWS ambiente usando várias contas.

> **Note**
>
> Neste whitepaper, “Control Tower” é um termo amplo para a configuração escalável, segura e de alto desempenho de várias contas/VPC na qual você implanta suas cargas de trabalho. Essa configuração pode ser criada usando ferramentas diferentes. Você pode encontrar mais informações sobre as melhores práticas, os princípios de design e os benefícios da base de nuvem para várias contas no whitepaper Organizando seu AWS ambiente usando várias contas.

A maioria dos clientes começa com algumas VPCs para implantar sua infraestrutura. O número de VPCs que um cliente cria geralmente está relacionado ao número de contas, usuários e ambientes em estágios (produção, desenvolvimento, teste etc.). À medida que o uso da nuvem cresce, o número de usuários, unidades de negócios, aplicativos e regiões com os quais um cliente interage também cresce, 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 melhores práticas para três áreas específicas em conectividade híbrida e entre VPCs:

- Conectividade de rede — interconectando VPCs e redes locais em grande escala.
- Segurança de rede — Criação de pontos de saída centralizados para acessar a Internet e endpoints, como gateway de tradução de endereços de rede (NAT), VPC endpoints e balanceadores de carga de gateway. AWS PrivateLinkAWS Network Firewall
- Gerenciamento de DNS — Resolvendo o DNS dentro da Control Tower e do DNS híbrido.

Planejamento e gerenciamento de endereços IP

Para criar um design escalável de rede multi-VPC com várias contas, o planejamento e o gerenciamento de endereços IP são essenciais. Um bom esquema de endereçamento IP precisa considerar suas necessidades de rede atuais e futuras. Seu esquema de endereços IP O IP precisa cobrir suas cargas de trabalho locais, suas cargas de trabalho na nuvem e também deve permitir uma expansão futura (por exemplo, adição de novas Regiões da AWS unidades de negócios e fusões ou aquisições). Isso também deve evitar que suas equipes criem inadvertidamente CIDRs IP sobrepostos. Se a sobreposição de CIDR IP for desejada, como para cargas de trabalho isoladas ou desconectadas, essa decisão precisa ser consciente e deve levar em conta as implicações no roteamento, na segurança e nos custos. Talvez você também precise considerar a criação dos processos de aprovação necessários para essas exceções. Um bom esquema de endereçamento IP também ajuda a simplificar o design da rede e a configuração de roteamento.

Considerações importantes:

- Planeje seu esquema de endereçamento IP (IPs públicos e privados) com antecedência e selecione uma ferramenta de gerenciamento de endereços IP para alocar, gerenciar e rastrear o uso de endereços IP em todas as suas cargas de trabalho.
- Use esquemas de endereçamento IP hierárquicos e resumidos.
- Planeje uma atribuição consistente de IP com base no ambiente Região da AWS, na organização ou na unidade de negócios.
- Designe CIDRs IP distintos (IPv4 e IPv6) para redes locais e na nuvem.
- Previna e rastreie proativamente a sobreposição de CIDRs IP.
- Dimensione seus CIDRs IP adequadamente para permitir o escalonamento e o crescimento futuro.

- Habilite suas cargas de trabalho para compatibilidade com IPv6 ou pilha dupla para reduzir conflitos de IP e lidar com o esgotamento do espaço IPv4.

Você pode usar o Amazon VPC IP Address Manager (IPAM) para simplificar o planejamento, o rastreamento e o monitoramento de endereços IP públicos e privados para suas cargas de trabalho. AWS O IPAM permite que você organize, aloque, monitore e compartilhe espaço de endereço IP entre vários e. Regiões da AWS Contas da AWS Também ajuda na alocação automática de CIDRs para VPCs usando regras comerciais específicas.

Consulte as melhores práticas do Amazon VPC IP Address Manager, o gerenciamento de grupos de IP entre VPCs e regiões usando o Amazon VPC IP Address Manager e o gerenciamento de endereços IP para ver postagens de AWS Control Tower blog para aprender as melhores práticas de endereçamento IP e como usar o IPAM para gerenciar pools de IP em VPCs, e. Regiões da AWS AWS Control Tower

Você é Well-Architected?

O Well-Architected Framework da AWS ajuda você a entender os prós e os contras das decisões que você toma ao criar sistemas na nuvem. Os seis pilares do framework permitem a você conhecer as melhores práticas de arquitetura para criar e operar sistemas confiáveis, seguros, econômicos e sustentáveis na nuvem. Usando o AWS Well-Architected Tool, disponível gratuitamente no AWS Management Console, você pode analisar suas workloads em relação a essas práticas recomendadas respondendo a um conjunto de perguntas para cada pilar.

Para obter orientações especializadas e melhores práticas adicionais para a arquitetura de sua nuvem (implantações de arquitetura de referência, diagramas e whitepapers), consulte o AWS Architecture Center.

Conectividade de VPC para VPC

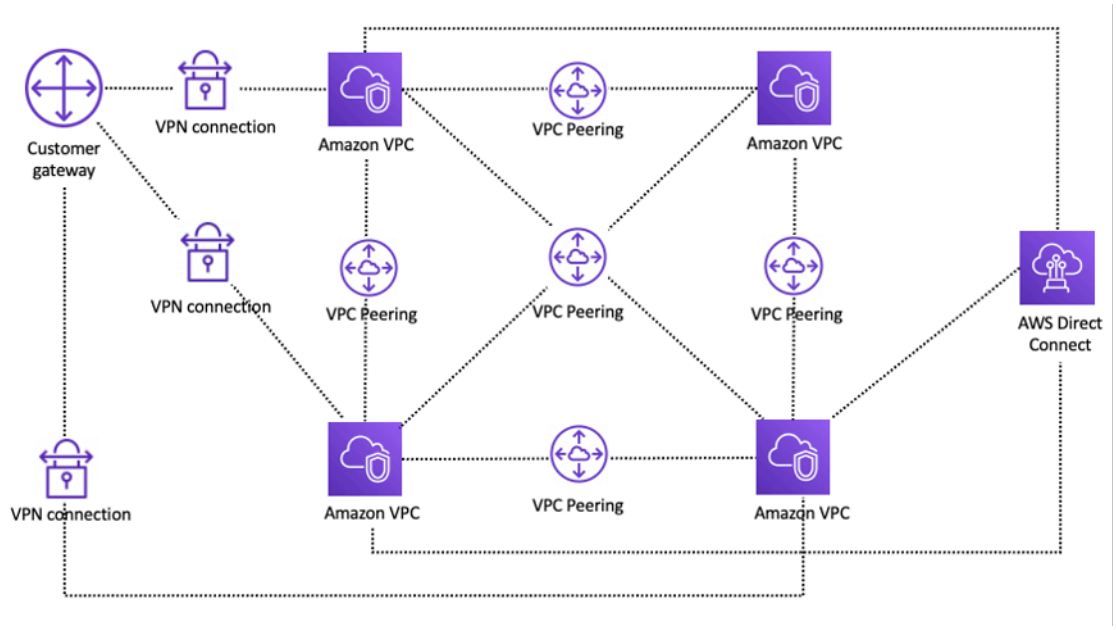
Os clientes podem usar dois padrões diferentes de conectividade de VPC para configurar ambientes de várias VPC: muitas para muitas, ou hub and spoke. Na many-to-many abordagem, o tráfego entre cada VPC é gerenciado individualmente entre cada VPC. No hub-and-spoke modelo, todo o tráfego entre VPC flui por meio de um recurso central, que roteia o tráfego com base nas regras estabelecidas.

emparelhamento da VPC

A primeira maneira de conectar duas VPCs é usar o peering de VPC. Nessa configuração, uma conexão permite a conectividade bidirecional total entre as VPCs. Essa conexão de emparelhamento é usada para rotear o tráfego entre as VPCs. VPCs em diferentes contas e regiões da AWS também podem ser emparelhadas. Toda transferência de dados por uma conexão de emparelhamento VPC que permanece dentro de uma zona de disponibilidade é gratuita. Toda transferência de dados por meio de uma conexão emparelhada de VPC que cruza as zonas de disponibilidade é cobrada de acordo com as taxas de transferência de dados padrão da região. Se as VPCs estiverem emparelhadas entre regiões, serão aplicadas taxas padrão de transferência de dados entre regiões.

O emparelhamento de VPC é point-to-point conectividade e não oferece suporte ao 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 pode transitar pela VPC A para chegar à VPC C. Para rotear pacotes entre a VPC B e a VPC C, é necessário criar uma conexão de emparelhamento de VPC direta.

Em grande escala, quando você tem dezenas ou centenas de VPCs, interconectá-las com o peering pode resultar em uma malha de centenas ou milhares de conexões de peering. Um grande número de conexões pode ser difícil de gerenciar e escalar. Por exemplo, se você tiver 100 VPCs e quiser configurar um peering de malha completa entre elas, serão necessárias 4.950 conexões de emparelhamento [`n(n-1)/2`], onde `n` é o número total de VPCs. Há um limite máximo de 125 conexões de peering ativas por VPC.



Configuração de rede usando emparelhamento de VPC

Se você estiver usando o emparelhamento de VPC, a conectividade local (VPN e/ou Direct Connect) deve ser estabelecida para cada VPC. Os recursos em uma VPC não podem ser acessados localmente usando a conectividade híbrida de uma VPC emparelhada, conforme mostrado na figura anterior.

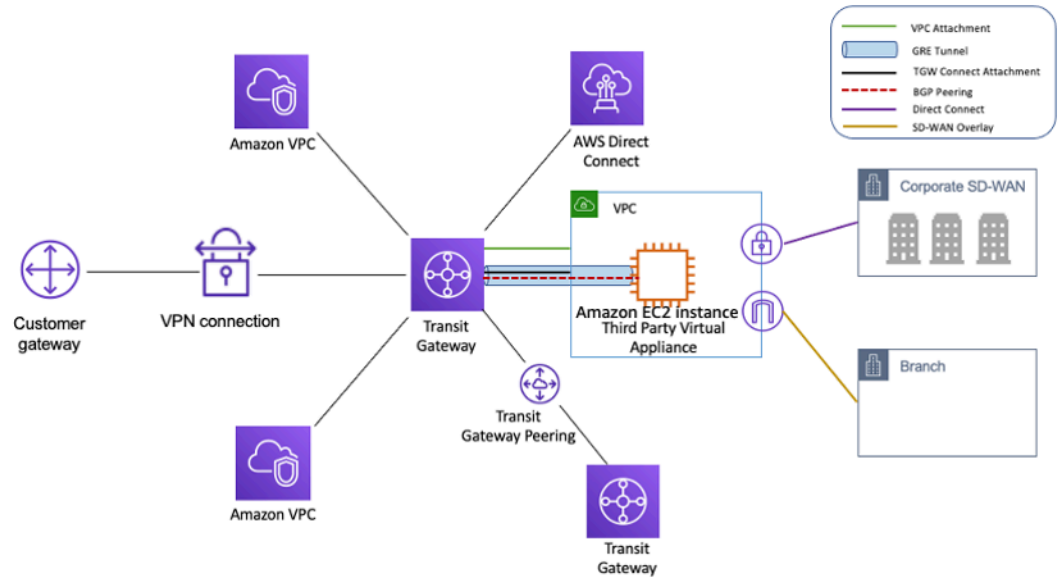
O emparelhamento de VPC é melhor usado quando os recursos em uma VPC devem se comunicar com os recursos em outra VPC, o ambiente de ambas as VPCs é controlado e protegido e o número de VPCs a serem conectadas é menor que 10 (para permitir o gerenciamento individual de cada conexão). O peering de VPC oferece o menor custo geral e o maior desempenho agregado quando comparado a outras opções de conectividade entre VPCs.

AWS Transit Gateway

AWS Transit Gatewayfornece um design de hub and spoke para conectar VPCs e redes locais como um serviço totalmente gerenciado, sem exigir que você provisione dispositivos virtuais de terceiros. Nenhuma sobreposição de VPN é necessária e AWS gerencia alta disponibilidade e escalabilidade.

O Transit Gateway permite que os clientes conectem milhares de VPCs. Você pode conectar toda a sua conectividade híbrida (conexões VPN e Direct Connect) a um único gateway, consolidando e controlando toda a configuração de AWS roteamento da sua organização em um só lugar (consulte a figura a seguir). O Transit Gateway controla como o tráfego é roteado entre todas as redes spoke conectadas usando tabelas de rotas. Esse hub-and-spoke modelo simplifica o gerenciamento e

reduz os custos operacionais porque as VPCs só se conectam à instância do Transit Gateway para obter acesso às redes conectadas.



Design de hub e raio com AWS Transit Gateway

O Transit Gateway é um recurso regional e pode conectar milhares de VPCs dentro do mesmo Região da AWS. Você pode conectar vários gateways em uma única conexão Direct Connect para conectividade híbrida. Normalmente, você pode usar apenas uma instância do Transit Gateway conectando todas as suas instâncias de VPC em uma determinada região e usar tabelas de roteamento do Transit Gateway para isolá-las sempre que necessário. Observe que você não precisa de gateways de trânsito adicionais para alta disponibilidade, porque os gateways de trânsito são altamente disponíveis por design; para redundância, use um único gateway em cada região. No entanto, há um caso válido para criar vários gateways para limitar o raio de explosão de configuração incorreta, segregar as operações do plano de controle e as administrativas. ease-of-use

Com o peering do Transit Gateway, os clientes podem emparelhar suas instâncias do Transit Gateway na mesma ou em várias regiões e rotear o tráfego entre elas. Ele usa a mesma infraestrutura subjacente do peering de VPC e, portanto, é criptografado. Para obter mais informações, consulte Criação de uma rede global usando o emparelhamento entre regiões do AWS Transit Gateway. O AWS Transit Gateway agora oferece suporte ao peering entre regiões.

Coloque a instância do Transit Gateway da 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 uma instância do Transit Gateway para conectar VPCs em várias contas em sua organização da AWS na mesma região.AWS RAM permite que você compartilhe AWS recursos de forma fácil e segura com qualquer Conta

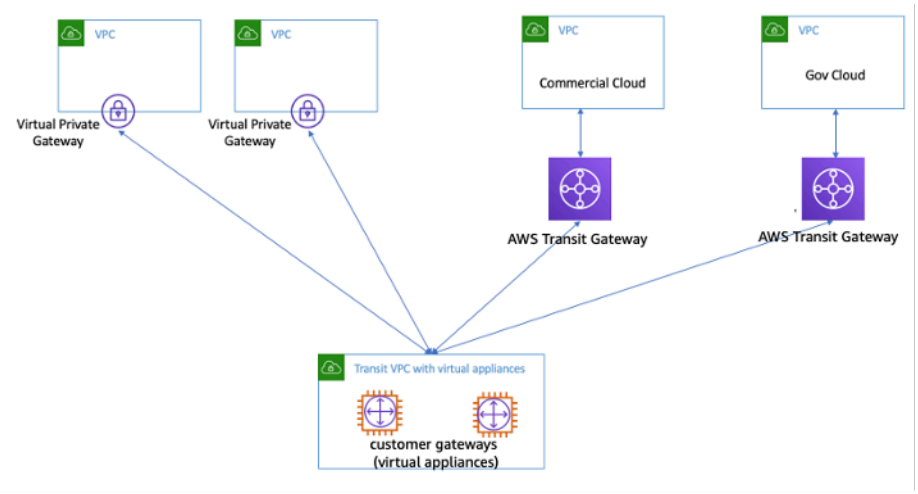
da AWS pessoa ou dentro da sua organização da AWS. Para obter mais informações, consulte Automatizar anexos do AWS Transit Gateway a um gateway de trânsito em uma postagem no blog da conta central.

O Transit Gateway também permite estabelecer conectividade entre a infraestrutura SD-WAN e o AWS uso do Transit Gateway Connect. Use um anexo Transit Gateway Connect com o Border Gateway Protocol (BGP) para roteamento dinâmico e o protocolo de túnel Generic Routing Encapsulation (GRE) para alto desempenho, oferecendo até 20 Gbps de largura de banda total por anexo Connect (até quatro pares do Transit Gateway Connect por anexo Connect). Ao usar o Transit Gateway Connect, você pode integrar a infraestrutura SD-WAN local ou os dispositivos SD-WAN executados na nuvem por meio de um anexo de VPC ou AWS Direct Connect anexo como camada de transporte subjacente. Consulte Simplifique a conectividade SD-WAN com o AWS Transit Gateway Connect para obter arquiteturas de referência e configuração detalhada.

Solução Transit VPC

As VPCs de trânsito podem criar conectividade entre VPCs por um meio diferente do peering de VPC, introduzindo um design de hub and spoke para conectividade entre VPCs. Em uma rede VPC de trânsito, uma VPC central (o hub VPC) se conecta a todas as outras VPC (falei VPC) por meio de uma conexão VPN, normalmente aproveitando o BGP sobre IPsec. A VPC central contém instâncias do Amazon Elastic Compute Cloud (Amazon EC2) executando dispositivos de software que roteiam o tráfego de entrada para seus destinos usando a sobreposição de VPN. O peering de VPC Transit tem as seguintes vantagens:

- O roteamento transitivo é habilitado usando a rede VPN de sobreposição, permitindo um design de hub and spoke.
- Ao usar software de um fornecedor terceirizado na instância do EC2 na VPC de trânsito do hub, a funcionalidade do fornecedor em relação à segurança avançada (firewall de camada 7/Sistema de Prevenção de Intrusões (IPS) /Sistema de Detecção de Intrusões (IDS)) pode ser usada. Se os clientes estiverem usando o mesmo software no local, eles se beneficiarão de uma experiência operacional/de monitoramento unificada.
- A arquitetura Transit VPC permite a conectividade que pode ser desejada em alguns casos de uso. Por exemplo, você pode conectar uma GovCloud instância da AWS e uma VPC de região comercial ou uma instância do Transit Gateway a uma VPC de trânsito e habilitar a conectividade entre VPCs entre as duas regiões. Avalie seus requisitos de segurança e conformidade ao considerar essa opção. Para segurança adicional, você pode implantar um modelo de inspeção centralizado usando os padrões de projeto descritos posteriormente neste whitepaper.



Transit VPC com dispositivos virtuais

O Transit VPC apresenta seus próprios desafios, como custos mais altos para executar dispositivos virtuais de fornecedores terceirizados no EC2 com base no tamanho/família da instância, taxa de transferência limitada por conexão VPN (até 1,25 Gbps por túnel VPN) e sobrecarga adicional de configuração, gerenciamento e resiliência (os clientes são responsáveis por gerenciar o HA e a redundância das instâncias do EC2 que executam os dispositivos virtuais de fornecedores terceirizados).

Emparelhamento de VPC versus Transit VPC versus Transit Gateway

Tabela 1 — Comparação de conectividade

Critérios	emparelhamento da VPC	VPC de trânsito	Gateway de trânsito	PrivateLink	Cloud WAN	VPC Lattice
Escopo	Regional/ Global	Regional	Regional	Regional	Global	Regional
Arquitetura	Malha completa	Baseado em VPN hub-and-spoke	Baseado em anexos hub-and-spoke	Modelo de fornecedor ou consumidor	Baseado em anexos, multirregional	Conectividade de aplicativo para aplicativo

Critérios	emparelhamento da VPC	VPC de trânsito	Gateway de trânsito	PrivateLink	Cloud WAN	VPC Lattice
Escala	125 pares ativos/VPC	Depende do roteador virtual/EC2	5000 anexos por região	Sem limites	5000 anexos por rede principal	500 associações de VPC por serviço
Segmentação	Grupos de segurança	Gerenciado pelo cliente	Tabelas de rotas do Transit Gateway	Sem segmentação	Segmentos	Políticas de serviço e rede de serviços
Latência	Menor	Extra, devido à sobrecarga de criptografia da VPN	Shop adicional do Transit Gateway	O tráfego permanece no backbone da AWS, os clientes devem testar	Usa o mesmo plano de dados do Transit Gateway	O tráfego permanece no backbone da AWS, os clientes devem testar
Limite de largura de banda	Limites por instância, sem limite agregado	Sujeito aos limites de largura de banda da instância EC2 com base no tamanho/família	Até 100 Gbps (rajada) / conexão	10 Gbps por zona de disponibilidade, escalável automaticamente até 100 Gbps	Até 100 Gbps (rajada) / conexão	10 Gbps por zona de disponibilidade

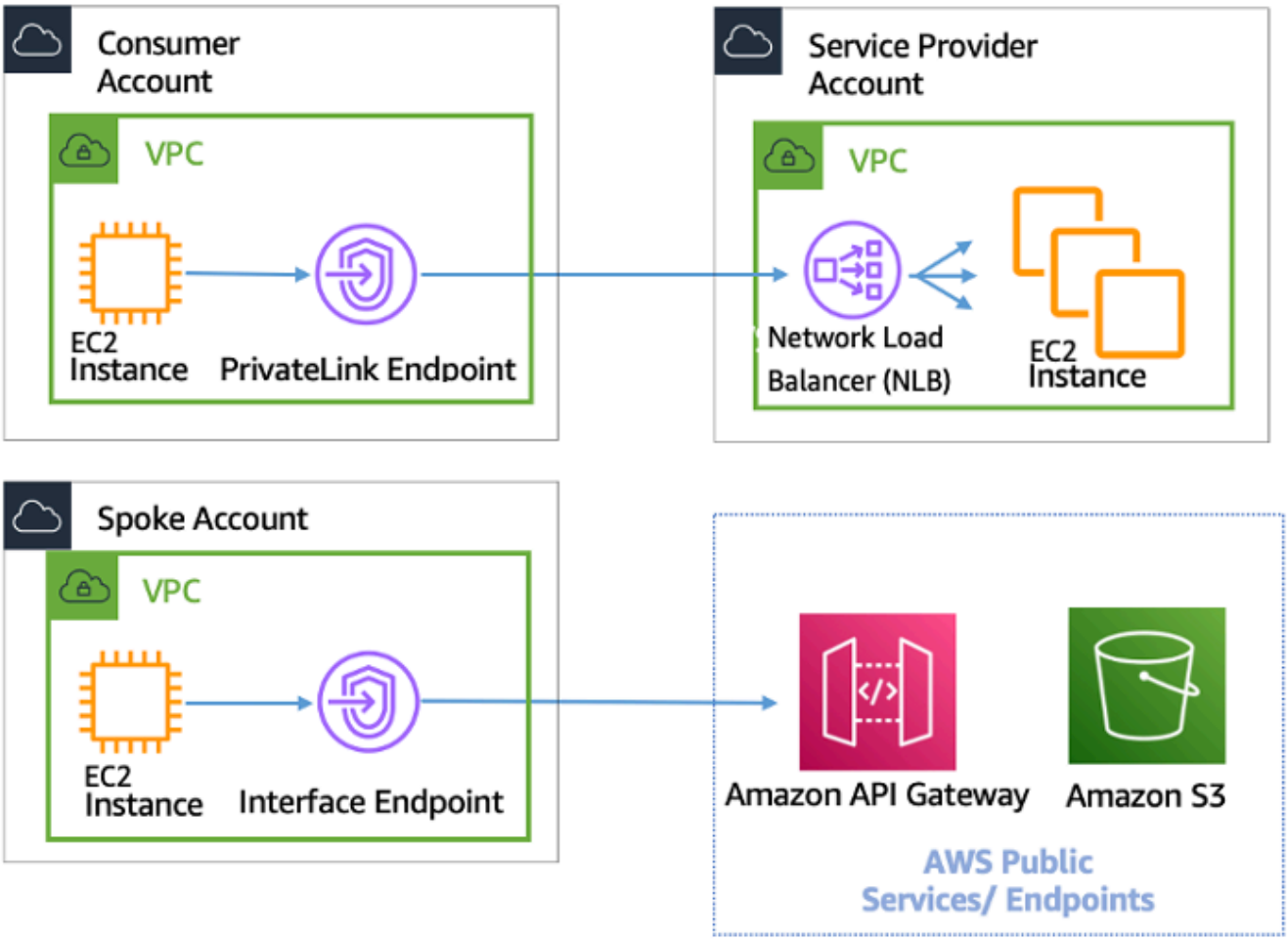
Critérios	emparelhamento da VPC	VPC de trânsito	Gateway de trânsito	PrivateLink	Cloud WAN	VPC Lattice
Visibility	Logs de fluxo da VPC	Registros e métricas de fluxo de VPC CloudWatch	Gerenciador de rede do Transit Gateway, registros de fluxo de VPC, métricas CloudWatch	CloudWatch Métricas	Gerenciador de rede, registros de fluxo de VPC, métricas CloudWatch	CloudWatch Registros de acesso
Grupo de segurança referência cruzada	Compatível	Sem compatibilidade	Sem compatibilidade	Sem compatibilidade	Sem compatibilidade	Não aplicável
Suporte a IPv6	Compatível	Depende do dispositivo virtual	Compatível	Compatível	Compatível	Compatível

AWS PrivateLink

AWS PrivateLinkfornece conectividade privada entre VPCs, serviços da AWS e suas redes locais sem expor seu tráfego à Internet pública. Os endpoints de VPC de interface, alimentados por AWS PrivateLink, facilitam a conexão com outros serviços em diferentes contas AWS e VPCs para simplificar significativamente sua arquitetura de rede. Isso permite que os clientes queiram expor de forma privada um serviço/aplicativo residente em uma VPC (provedor de serviços) a outras VPCs (consumidor) de Região da AWS uma forma que somente as VPCs consumidoras iniciem conexões com a VPC do provedor de serviços. Um exemplo disso é a capacidade de seus aplicativos privados acessarem as APIs do provedor de serviços.

Para usar AWS PrivateLink, crie um Network Load Balancer para seu aplicativo em sua VPC e crie uma configuração de serviço de VPC endpoint apontando para esse balanceador de carga. Em seguida, um consumidor de serviços cria um endpoint de interface para seu serviço. Isso cria uma interface de rede elástica (ENI) na sub-rede do consumidor com um endereço IP privado que serve como 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 do consumidor e do provedor de serviços podem ter intervalos de endereços IP sobrepostos. Além de criar a interface VPC endpoint para acessar serviços em outras VPCs, você pode criar endpoints de VPC de interface para acessar de forma privada os serviços compatíveis da AWS, conforme mostrado na figura a AWS PrivateLink seguir.

Com o Application Load Balancer (ALB) como alvo do NLB, agora você pode combinar os recursos avançados de roteamento do ALB com o. AWS PrivateLink Consulte o Grupo de destino do tipo Application Load Balancer para Network Load Balancer para obter arquiteturas de referência e configuração detalhada.



AWS PrivateLink para conectividade com outras VPCs e serviços da AWS

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

- AWS PrivateLink— Use AWS PrivateLink quando você tiver um cliente/servidor configurado para permitir que uma ou mais VPCs consumidoras tenham acesso unidirecional a um serviço específico ou conjunto de instâncias na VPC do provedor de serviços ou em determinados serviços. AWS Somente os clientes com acesso na VPC do consumidor podem iniciar uma conexão com o serviço na VPC ou no serviço do provedor de serviços. AWS Essa também é uma boa opção quando clientes e servidores nas duas VPCs têm endereços IP sobrepostos porque AWS PrivateLink usa ENIs na VPC cliente de uma maneira que garante que não haja conflitos de IP com o provedor de serviços. Você pode acessar AWS PrivateLink endpoints por meio de emparelhamento de VPC, VPN, Transit Gateway, Cloud WAN e. 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, AWS PrivateLink lidar com conectividade cliente-servidor no estilo API, emparelhamento de VPC para lidar com requisitos de conectividade direta em que grupos de posicionamento ainda podem ser desejados na região ou entre regiões, e o Transit Gateway para simplificar a conectividade de VPCs em grande escala, bem como consolidação de borda para conectividade híbrida.

Compartilhamento da VPC

O compartilhamento de VPCs é útil quando o isolamento da rede entre equipes não precisa ser gerenciado estritamente pelo proprietário da VPC, mas os usuários e as permissões no nível da conta devem ser. Com a VPC compartilhada, várias contas da AWS criam seus recursos de aplicativos (como instâncias do Amazon EC2) em Amazon VPCs compartilhadas e gerenciadas centralmente. Nesse modelo, a conta proprietária da VPC (proprietário) 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 usando grupos de segurança, listas de controle de acesso à rede (NACLs) ou por meio de um firewall entre as sub-redes.

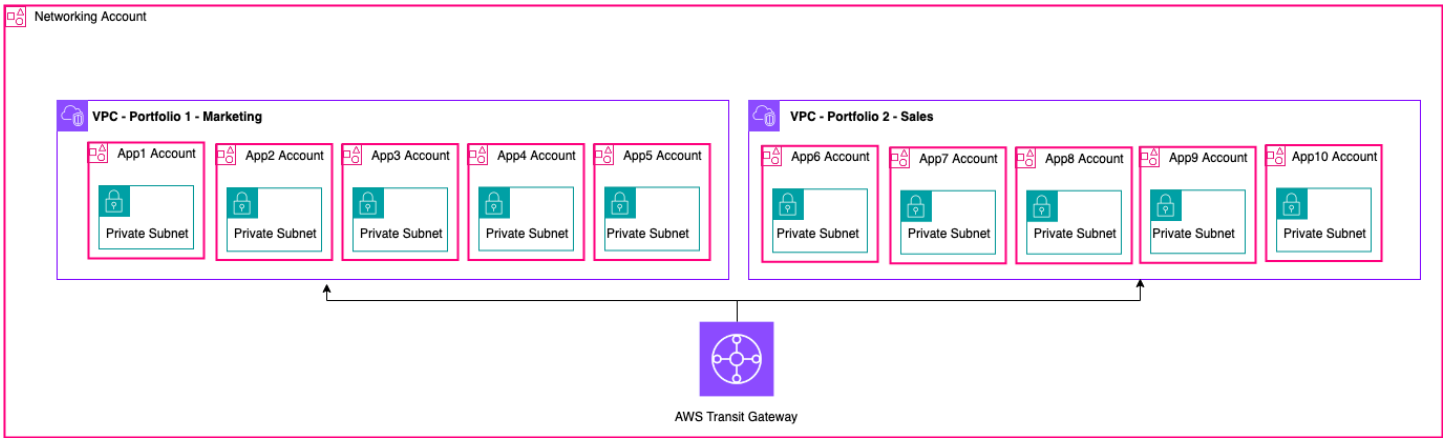
Benefícios do compartilhamento de VPC:

- Design simplificado — sem complexidade em relação à conectividade entre VPCs
- Menos VPCs gerenciadas
- Segregação de tarefas entre equipes de rede e proprietários de aplicativos
- Melhor utilização do endereço IPv4
- Custos mais baixos — sem cobranças de transferência de dados entre instâncias pertencentes a contas diferentes na mesma zona de disponibilidade

> **Note**
>
> 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 de participante. Uma sub-rede por participante permite que a ACL de rede forneça isolamento de rede, além dos grupos de segurança.

A maioria das arquiteturas de clientes conterá várias VPCs, muitas das quais 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, suponha que você tenha 10 aplicativos. Cada aplicativo exige sua própria conta da AWS. Os aplicativos podem ser categorizados em dois portfólios de aplicativos (aplicativos dentro do mesmo portfólio têm requisitos de rede semelhantes, aplicativo 1—5 em 'Marketing' e aplicativo 6—10 em 'Vendas').

Você pode ter uma VPC por portfólio de aplicativos (duas VPCs no total), e a VPC é compartilhada com as diferentes contas do proprietário do aplicativo dentro desse portfólio. Os proprietários de aplicativos implantam aplicativos em sua 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, você poderia deixar de conectar 10 VPCs para apenas duas, conforme mostrado na figura a seguir.

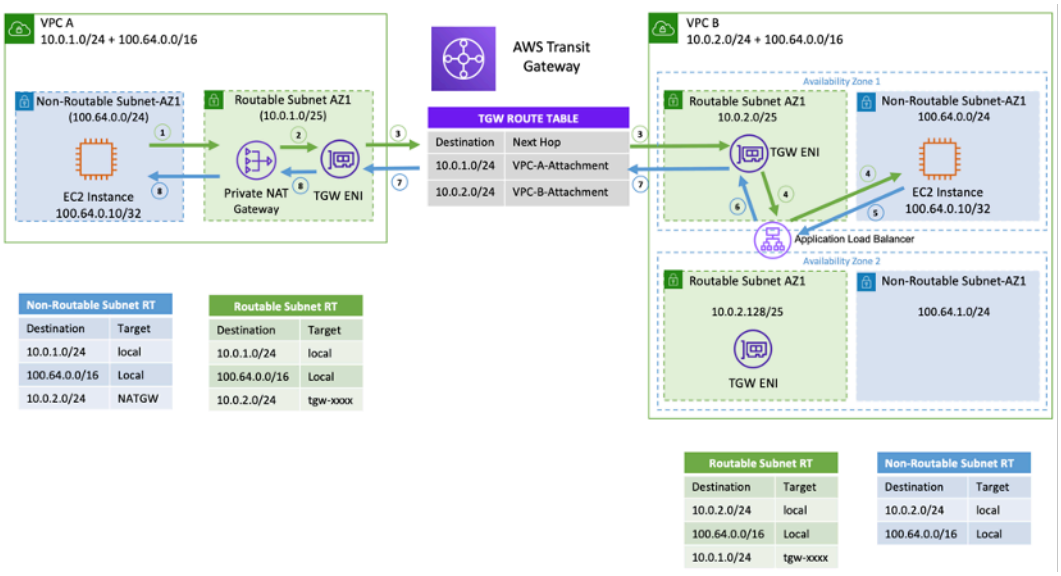


Exemplo de configuração — VPC compartilhada

> **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 a seção Limitações na documentação de compartilhamento de VPC.
> Para obter mais informações sobre as principais considerações e as melhores práticas para o compartilhamento de VPC, consulte a postagem do blog Compartilhamento de VPC: considerações principais e melhores práticas.

Gateway NAT privado

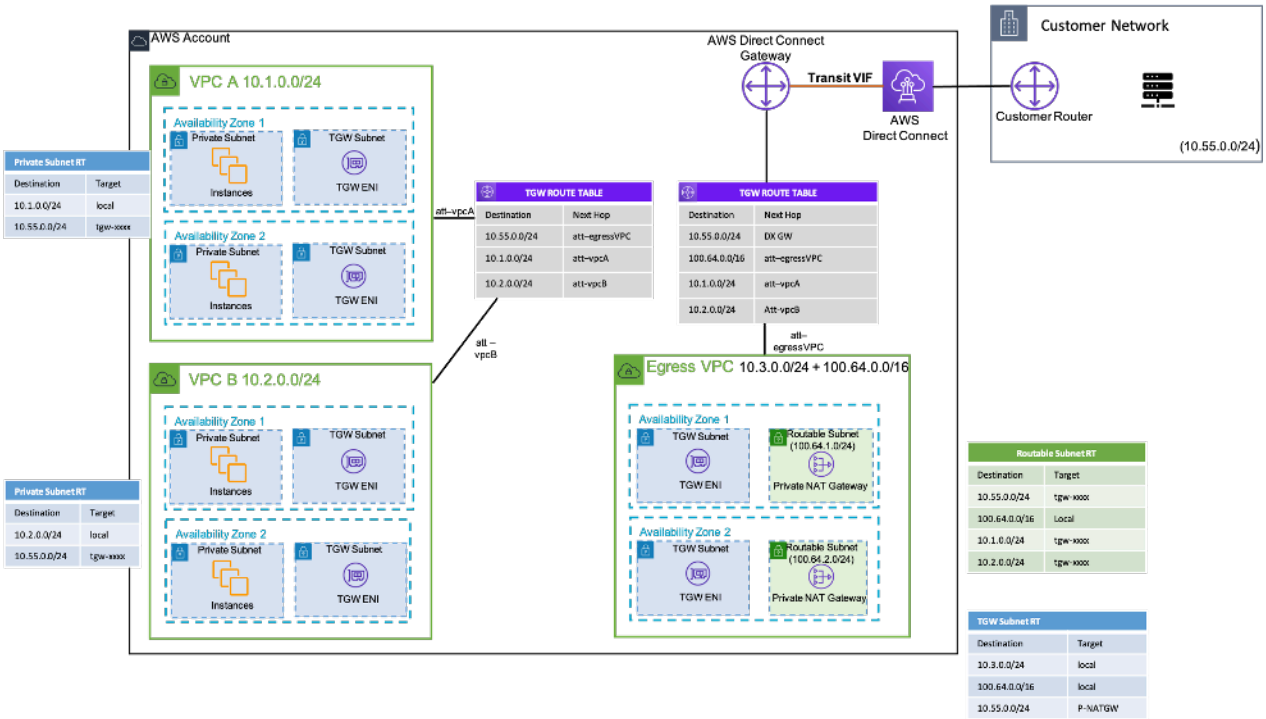
As equipes geralmente trabalham de forma independente e podem criar uma nova VPC para um projeto, que pode ter blocos de roteamento entre domínios (CIDR) sobrepostos sem classes. Para integração, talvez eles queiram permitir a comunicação entre redes com CIDRs sobrepostos, o que não é possível por meio de recursos como emparelhamento de VPC e Transit Gateway. Um gateway NAT privado pode ajudar nesse caso de uso. O gateway NAT privado usa um endereço IP privado exclusivo para realizar o NAT de origem para o endereço IP de origem sobreposto, e o ELB faz o NAT de destino para o endereço IP de destino sobreposto. Você pode rotear o tráfego do seu gateway NAT privado para outras VPCs ou redes locais usando o Transit Gateway ou um gateway privado virtual.



Exemplo de configuração — gateway NAT privado

A figura anterior mostra duas sub-redes não roteáveis (CIDRs sobrepostas) nas VPC A e B. Para estabelecer uma conexão entre elas, você pode adicionar CIDRs secundárias não sobrepostas/roteáveis (`100.64.0.0/16`sub-redes roteáveis e) às VPC A e B, respectivamente. `10.0.1.0/24` `10.0.2.0/24` Os CIDRs roteáveis devem ser alocados pela equipe de gerenciamento de rede responsável pela alocação de IP. Um gateway NAT privado é adicionado à sub-rede roteável na VPC A com um endereço IP de. `10.0.1.125` O gateway NAT privado realiza a conversão do endereço de rede de origem em solicitações de instâncias na sub-rede não roteável da VPC A `100.64.0.10` () `10.0.1.125` como a ENI do gateway NAT privado. Agora, o tráfego pode ser direcionado para um endereço IP roteável atribuído ao Application Load Balancer (ALB) na VPC B `10.0.2.10` (), que tem como destino. `100.64.0.10` O tráfego é roteado pelo Transit Gateway. O tráfego de retorno é processado pelo gateway NAT privado de volta para a instância original do Amazon EC2 solicitando a conexão.

O gateway NAT privado também pode ser usado quando sua rede local restringe o acesso a IPs aprovados. A conformidade exige que as redes locais de poucos clientes se comuniquem somente com redes privadas (sem IGW) somente por meio de um bloco contíguo limitado de IPs aprovados de propriedade do cliente. Em vez de alocar para cada instância um IP separado do bloco, você pode executar grandes cargas de trabalho em AWS VPCs por trás de cada IP da lista de permissões usando um gateway NAT privado. Para obter detalhes, consulte a postagem do blog Como resolver a exaustão de IP privado com a solução NAT privada.



Exemplo de configuração — Como usar o gateway NAT privado para fornecer IPs aprovados para a rede local

AWS WAN em nuvem

O AWS Cloud WAN é uma nova forma de conectar redes que antes podíamos fazer com Transit Gateways, VPC Peering e túneis IPSEC VPN. Anteriormente, você configurava uma ou mais VPCs, as conectava com um dos métodos anteriores e usava a VPN IPSEC ou se conectava AWS Direct Connect a redes locais. Você teria suas construções de postura de rede e segurança definidas em um lugar e suas redes em outro. O Cloud WAN permite que você centralize todas essas construções em um único local. Por política, você pode segmentar suas redes para determinar quem pode falar com quem e isolar o tráfego de produção por meio desses segmentos das cargas de trabalho de desenvolvimento ou teste ou de suas redes locais.

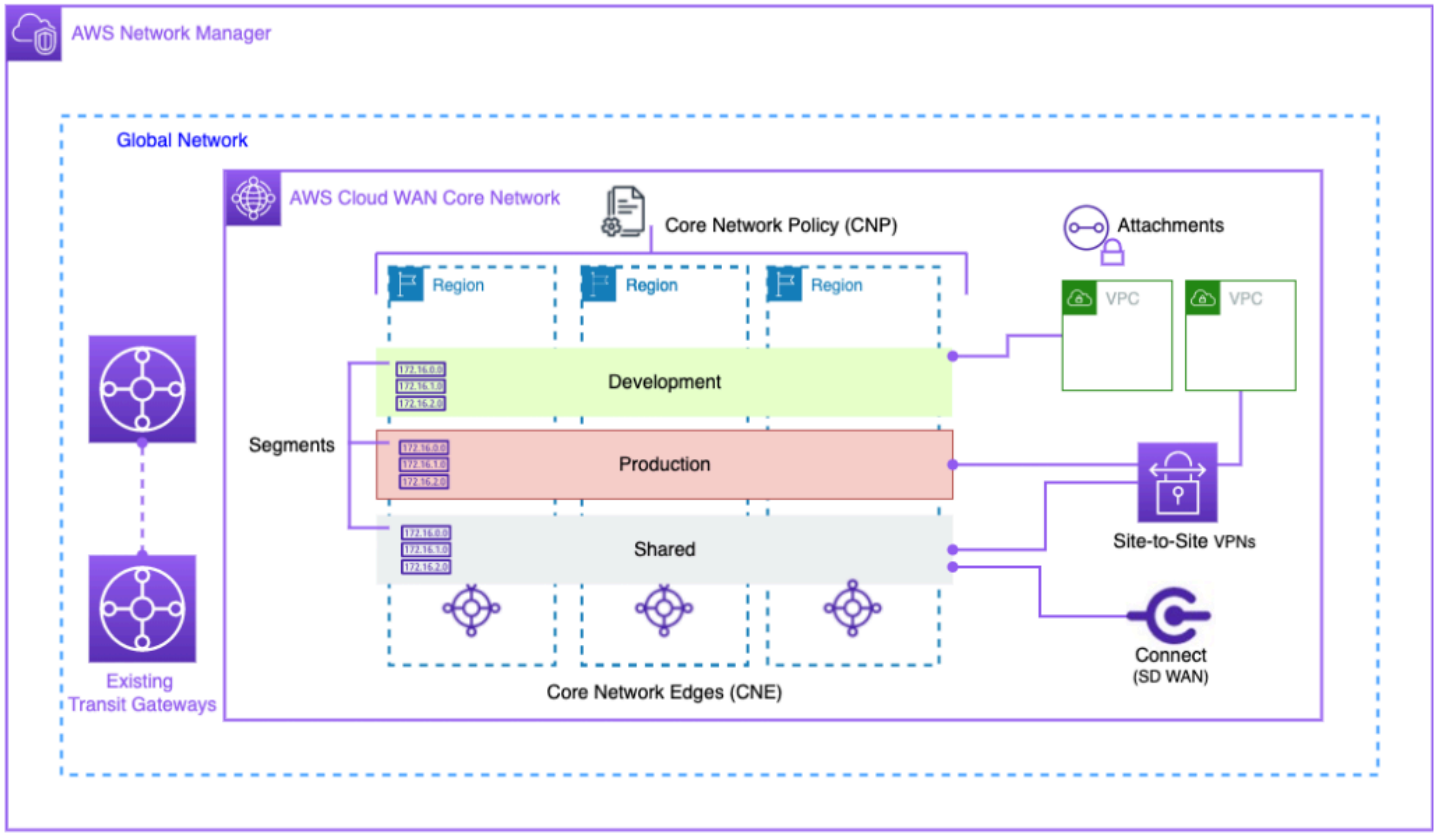


Diagrama de blocos da Cloud WAN

Gerencie sua rede global por meio da interface de usuário e das APIs do AWS Network Manager. A rede global é o contêiner de nível raiz para todos os seus objetos de rede; a rede principal é a parte da sua rede global gerenciada pela AWS. Uma política de rede central (CNP) é um documento de política com versão única que define todos os aspectos da sua rede principal. Anexos são todas as conexões ou recursos que você deseja adicionar à sua rede principal. Uma borda de rede central (CNE) é um ponto de conexão local para anexos que estão em conformidade com a política. Os segmentos de rede são domínios de roteamento que, por padrão, permitem a comunicação somente dentro de um segmento.

Para usar o CloudWAN:

1. No AWS Network Manager, crie uma rede global e uma rede principal associada.
2. Crie um CNP que defina segmentos, intervalo de ASN Regiões da AWS e etiquetas a serem usadas para anexar aos segmentos.
3. Aplique a política de rede.
4. Compartilhe a rede principal com seus usuários, contas ou organizações usando o gerenciador de acesso a recursos.

5. Crie e marque anexos.
6. Atualize as rotas em suas VPCs conectadas para incluir a rede principal.

A Cloud WAN foi projetada para simplificar o processo de conectar sua infraestrutura da AWS globalmente. Ele permite que você segmente o tráfego com uma política de permissões centralizada e use sua infraestrutura existente nas instalações da sua empresa. A Cloud WAN também conecta suas VPCs, SD-WANs, VPNs de cliente, firewalls, VPNs e recursos de data center para se conectar à Cloud WAN. Para obter mais informações, consulte as postagens do blog AWS Cloud WAN.

O AWS Cloud WAN permite uma rede unificada conectando ambientes locais e na nuvem. As organizações usam firewalls de próxima geração (NGFWs) e sistemas de prevenção de intrusões (IPSs) para segurança. A postagem do blog sobre padrões de migração e interoperabilidade da AWS Cloud WAN e do Transit Gateway descreve padrões arquitetônicos para gerenciar e inspecionar centralmente o tráfego de rede de saída em uma rede WAN na nuvem, incluindo redes de região única e multirregional, e configura tabelas de rotas. Essas arquiteturas garantem que os dados e os aplicativos permaneçam seguros e, ao mesmo tempo, mantenham um ambiente de nuvem seguro.

Para obter mais informações sobre a WAN na nuvem, consulte a postagem do blog sobre a arquitetura de inspeção de saída centralizada na AWS Cloud WAN.

Amazon VPC Lattice

O Amazon VPC Lattice é um serviço de rede de aplicativos totalmente gerenciado que é usado para conectar, monitorar e proteger serviços em várias contas e nuvens privadas virtuais. O VPC Lattice ajuda a interconectar serviços dentro de um limite lógico, para que você possa gerenciá-los e descobri-los com eficiência.

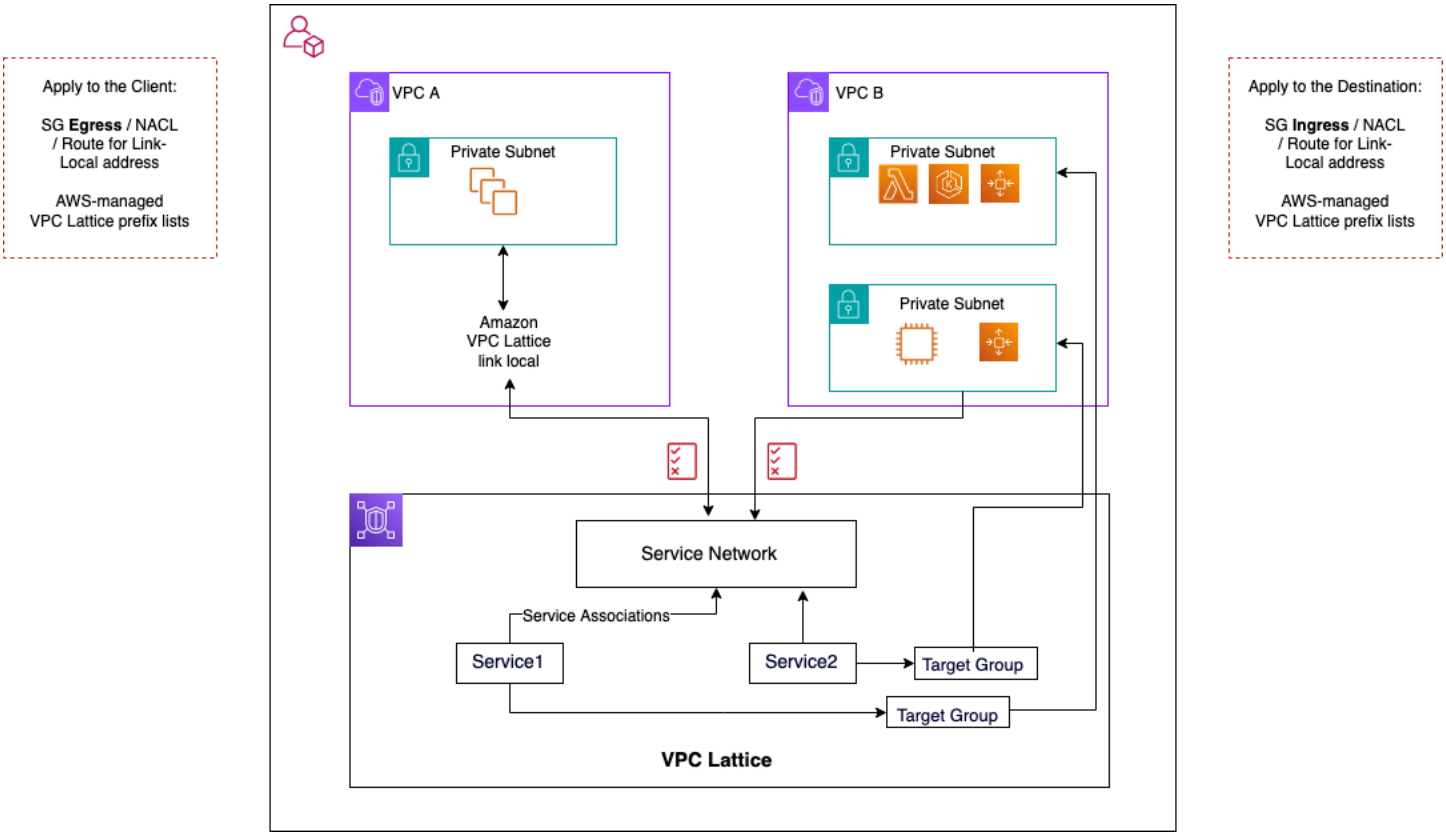
Os componentes do VPC Lattice consistem em:

- Serviço - Essa é uma unidade de aplicativo executada em uma instância, um contêiner ou uma função Lambda e consiste em ouvintes, regras e grupos-alvo.
- Rede de serviços - Esse é o limite lógico usado para implementar automaticamente a descoberta e a conectividade de serviços e aplicar políticas comuns de acesso e observabilidade a uma coleção de serviços.
- Políticas de autenticação — políticas de recursos do IAM que podem ser associadas a uma rede de serviços ou serviços individuais para oferecer suporte à autenticação em nível de solicitação e à autorização específica do contexto.

- Diretório de serviços — Uma visão centralizada dos serviços que você possui ou que foram compartilhados com você por meio do AWS Resource Access Manager.

Etapas de uso do VPC Lattice:

1. Crie a rede de serviços. A rede de serviços geralmente reside em uma conta de rede na qual o administrador da rede tem acesso total. A rede de serviços pode ser compartilhada entre várias contas dentro de uma organização. O compartilhamento pode ser realizado em serviços individuais ou em toda a conta de serviço.
2. Conecte VPCs à rede de serviços para habilitar a rede de aplicativos para cada VPC, para que diferentes serviços possam começar a consumir outros serviços registrados na rede. Os grupos de segurança são aplicados para controlar o tráfego.
3. Os desenvolvedores definem os serviços, que são preenchidos no diretório de serviços e registrados na rede de serviços. O VPC Lattice contém o catálogo de endereços de todos os serviços configurados. Os desenvolvedores também podem definir políticas de roteamento para usar implantações azul/verde. A segurança é gerenciada no nível da rede de serviço em que as políticas de autenticação e autorização são definidas e no nível do serviço em que as políticas de acesso com o IAM são implementadas.



Fluxos de comunicação VPC Lattice

Mais detalhes podem ser encontrados no guia do usuário do VPC Lattice.

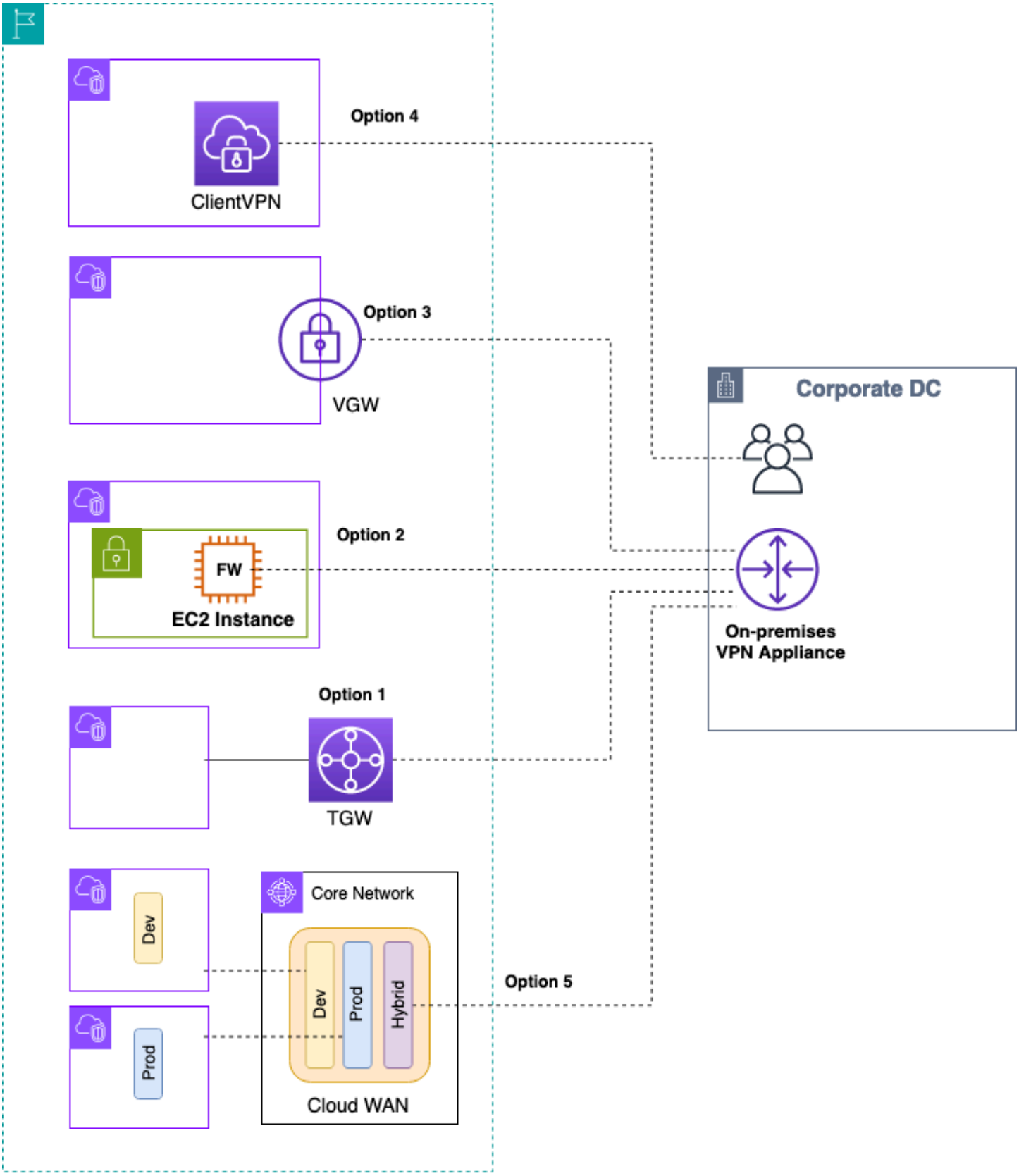
Conectividade híbrida

Esta seção se concentra em conectar com segurança seus recursos de nuvem com seus data centers locais. Há três abordagens para permitir a conectividade híbrida:

- O ne-to-one conectividade — Nessa configuração, uma conexão VPN e/ou VIF privada do Direct Connect é criada para cada VPC. Isso é feito usando o gateway privado virtual (VGW). Essa opção é ótima para um pequeno número de VPCs, mas à medida que um cliente expande suas VPCs, gerenciar a conectividade híbrida por VPC pode se tornar difícil.
- 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 AWS Transit Gateway o AWS Direct Connect gateway.
- Consolidação híbrida de malha completa — Nessa configuração, os clientes consolidam a conectividade de várias VPCs em um único endpoint usando o CloudWAN, incorporado. AWS Transit Gateway Essa é uma abordagem totalmente baseada em políticas para redes em uma ou mais contas da AWS, representadas em código. No momento, o uso AWS Direct Connect da conectividade de ponta requer o emparelhamento do Transit Gateway com o CloudWAN.

VPN

Há várias maneiras de configurar a VPN na AWS:



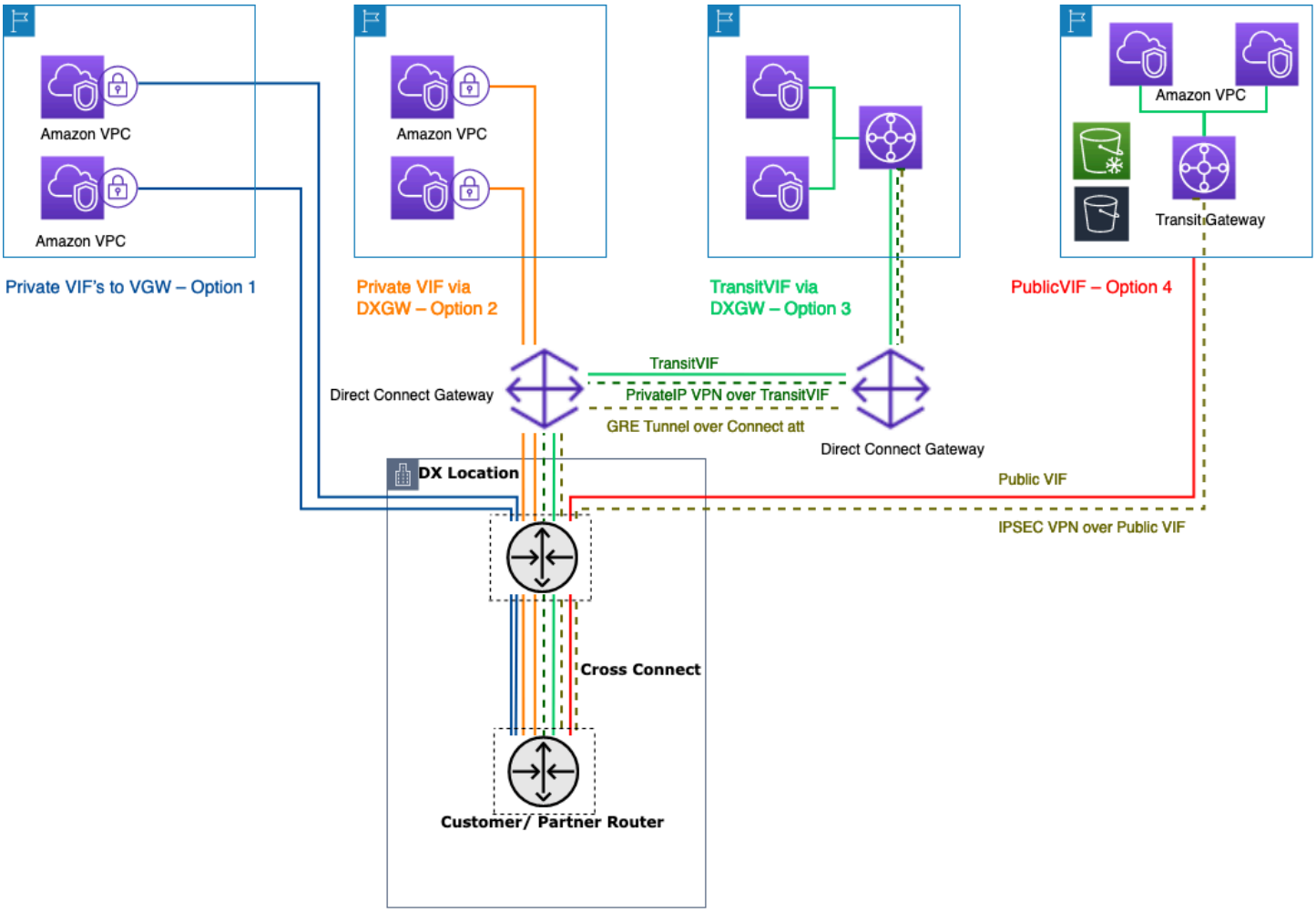
AWS VPN opções

- Opção 1: Consolidar a conectividade VPN no Transit Gateway — Essa opção aproveita o anexo VPN do Transit Gateway no Transit Gateway. O Transit Gateway oferece suporte à terminação IPsec para site-to-site VPN. Os clientes podem criar túneis VPN para o Transit Gateway e acessar as VPCs conectadas a ele. O Transit Gateway oferece suporte a conexões VPN estáticas e dinâmicas baseadas em BGP. O Transit Gateway também oferece suporte a vários caminhos de custo igual (ECMP) em anexos VPN. Cada conexão VPN tem uma taxa de transferência máxima de 1,25 Gbps por túnel. A ativação do ECMP permite agregar a taxa de transferência em conexões VPN, permitindo escalar além do limite máximo padrão de 1,25 Gbps. Nessa opção, você paga pelos preços e pelos preços do Transit Gateway.AWS VPN A AWS recomenda usar essa opção para conectividade VPN. Para obter mais informações, consulte a postagem do blog Scaling VPN usando o AWS Transit Gateway.
- Opção 2: encerrar a VPN na instância do Amazon EC2 — Essa opção é usada por clientes em casos extremos quando eles desejam um conjunto de recursos de software de um fornecedor específico (como Cisco DMVPN ou Generic Routing Encapsulation (GRE)) ou querem consistência operacional em várias implantações de VPN. Você pode usar o design da VPC de trânsito para consolidação de borda, mas é importante lembrar que todas as principais considerações da seção sobre VPC de trânsito são Conectividade de VPC para VPC aplicáveis à conectividade de VPN híbrida. Você é responsável por gerenciar a alta disponibilidade e paga pela instância EC2, bem como pelos custos de licenciamento e suporte de software do fornecedor.
- Opção 3: encerrar a VPN em um gateway privado virtual (VGW) — Essa opção de serviço VPN Site-to-Site da AWS permite one-to-one um design de conectividade em que você cria uma conexão VPN (consistindo em um par de túneis VPN redundantes) por VPC. Essa é uma ótima maneira de começar a usar a conectividade VPN na AWS, mas à medida que você aumenta o número de VPCs, gerenciar um número crescente de conexões VPN pode se tornar um desafio. Portanto, o design de consolidação de borda utilizando o Transit Gateway acabará sendo uma opção melhor. A taxa de transferência de VPN para um VGW é limitada a 1,25 Gbps por túnel e o balanceamento de carga ECMP não é suportado. Do ponto de vista dos preços, você paga apenas pelos preços do AWS VPN, não há cobrança pela execução de um VGW. Para obter mais informações, consulte AWS VPN Preços e AWS VPN sobre o gateway privado virtual.
- Opção 4: Encerrar a conexão VPN no endpoint VPN do cliente — O AWS Client VPN é um serviço VPN gerenciado baseado no cliente que permite que você acesse com segurança seus recursos e recursos da AWS em sua rede local. Com o Client VPN, você pode acessar seus recursos de qualquer local usando um cliente VPN fornecido pelo OpenVPN ou pela AWS. Ao configurar um endpoint Client VPN, clientes e usuários podem se conectar para estabelecer uma conexão VPN TLS (Transport Layer Security). Para obter mais informações, consulte a documentação do AWS Client VPN.

- Opção 5: consolidar a conexão VPN na AWS Cloud WAN — Essa opção é semelhante à primeira opção nesta lista, mas usa a estrutura do CloudWAN para configurar programaticamente as conexões VPN por meio do documento de política de rede.

AWS 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. Por causa dessa falta de confiabilidade, muitos clientes escolhem AWS Direct Connect. AWS Direct Connect é um serviço de rede que fornece uma alternativa ao uso da Internet para se conectar à AWS. Usando AWS Direct Connect, dados que antes seriam transportados pela Internet são entregues por meio de uma conexão de rede privada entre suas instalações e a AWS. Em muitas circunstâncias, as conexões de rede privada podem reduzir custos, aumentar a largura de banda e fornecer uma experiência de rede mais consistente do que as conexões baseadas na Internet. Há várias maneiras de se conectar AWS Direct Connect a VPCs:



Maneiras de conectar seus data centers locais usando AWS Direct Connect

- Opção 1: criar uma interface virtual privada (VIF) para um VGW conectado a uma VPC — Você pode criar 50 VIFs por conexão Direct Connect, permitindo que você se conecte a no máximo 50 VPCs (uma VIF fornece conectividade a uma VPC). Há um peering de BGP por VPC. A conectividade nessa configuração é restrita à região da AWS na qual o local do Direct Connect está hospedado. O one-to-one mapeamento de VIF para VPC (e a falta de acesso global) torna essa a forma menos preferida de acessar VPCs na Landing Zone.
- Opção 2: criar uma VIF privada em um gateway Direct Connect associado a vários VGWs (cada VGW é anexado a uma VPC) — um gateway Direct Connect é um recurso disponível globalmente. Você pode criar o gateway Direct Connect em qualquer região e acessá-lo de todas as outras regiões, inclusive GovCloud (exceto a China). Um Direct Connect Gateway pode se conectar a até 20 VPCs (via VGWs) globalmente em qualquer conta da AWS por meio de uma única VIF privada. Essa é uma ótima opção se uma Landing Zone consistir em um pequeno número de VPCs (dez ou menos VPCs) e/ou você precisar de acesso global. Há uma sessão de emparelhamento BGP por Direct Connect Gateway por conexão Direct Connect. O gateway Direct Connect é somente para fluxo de tráfego norte/sul e não permite conectividade de VPC para VPC. Consulte Associações de gateway privado virtual na AWS Direct Connect documentação para obter mais detalhes. Com essa opção, a conectividade não está restrita à região da AWS onde a localização do Direct Connect está localizada. AWS Direct Connect O gateway é somente para o fluxo de tráfego norte/sul e não permite a conectividade de VPC a VPC. Uma exceção a essa regra é quando uma superrede é anunciada em duas ou mais VPCs que têm seus VGWs conectados associados ao mesmo AWS Direct Connect gateway e na mesma interface virtual. Nesse caso, as VPCs podem se comunicar umas com as outras por meio do AWS Direct Connect endpoint. Consulte a documentação dos AWS Direct Connect gateways para obter mais detalhes.
- Opção 3: criar uma VIF de trânsito para um gateway Direct Connect associado ao Transit Gateway — Você pode associar uma instância do Transit Gateway a um gateway Direct Connect usando uma VIF de trânsito. AWS Direct Connect agora suporta conexões com o Transit Gateway para todas as velocidades de porta, oferecendo uma opção mais econômica para os usuários do Transit Gateway quando conexões de alta velocidade (maiores que 1 Gbps) não são necessárias. Isso permite que você use o Direct Connect em velocidades de 50, 100, 200, 300, 400 e 500 Mbps conectando-se ao Transit Gateway. O Transit VIF permite que você conecte seu datacenter local a até seis instâncias do Transit Gateway por AWS Direct Connect gateway (que podem se conectar a milhares de VPCs) em diferentes regiões e contas da AWS por meio de um único emparelhamento de VIF e BGP de trânsito. Essa é a configuração mais simples entre as opções para conectar várias VPCs em grande escala, mas você deve estar atento às cotas do Transit

Gateway. Um limite importante a ser observado é que você pode anunciar somente 200 prefixos de um Transit Gateway para um roteador local pela VIF de trânsito. Com as opções anteriores, você paga pelos preços do Direct Connect. Para essa opção, você também paga pelo anexo do Transit Gateway e pelas taxas de processamento de dados. Para obter mais informações, consulte a documentação do Transit Gateway Associations on Direct Connect.

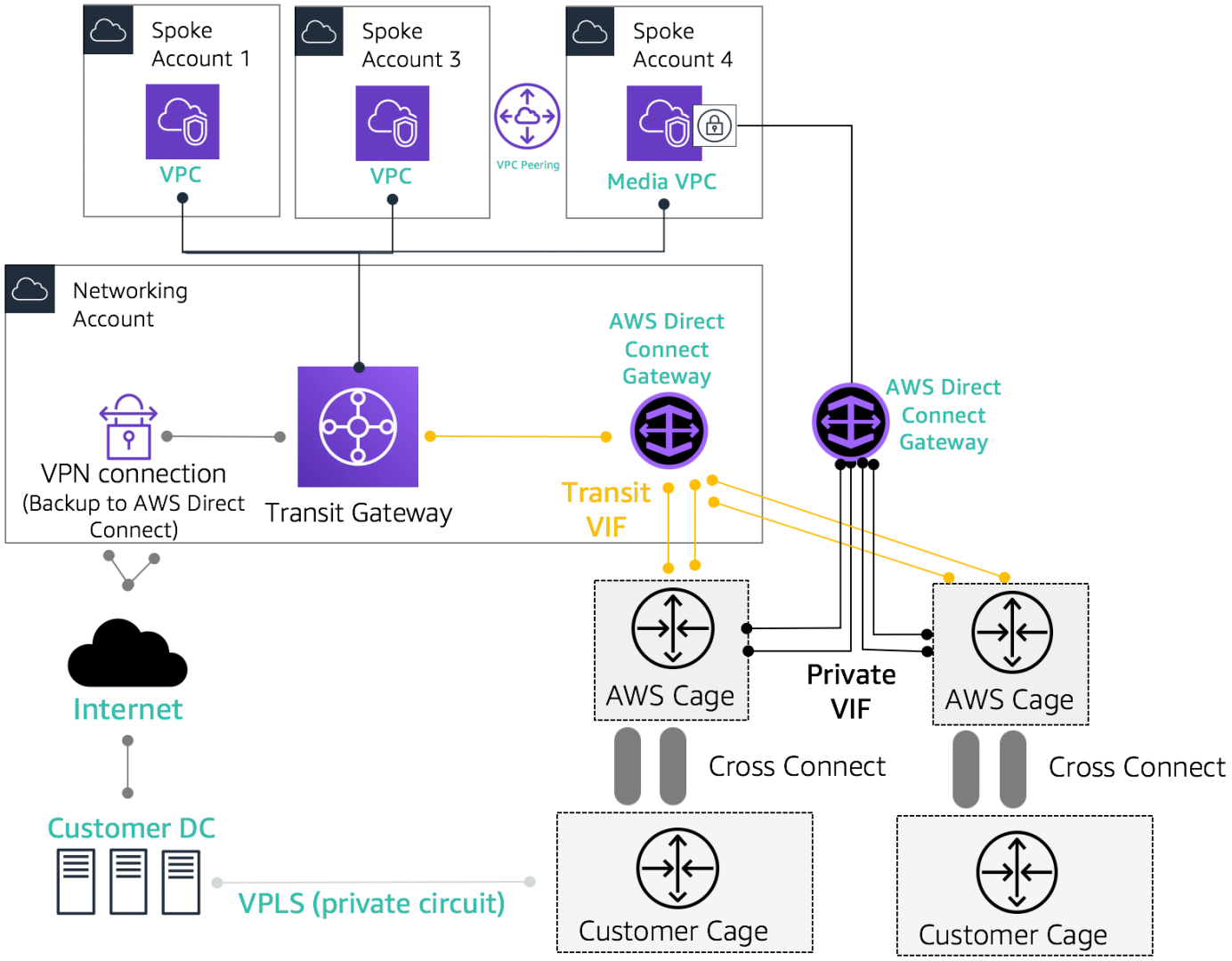
- Opção 4: criar uma conexão VPN com o Transit Gateway por meio da VIF pública do Direct Connect — Uma VIF pública permite que você acesse todos os serviços e endpoints públicos da AWS usando os endereços IP públicos. Ao criar um anexo de VPN em um Transit Gateway, você obtém dois endereços IP públicos para endpoints de VPN no lado da AWS. Esses IPs públicos podem ser acessados pelo VIF público. Você pode criar quantas conexões VPN quiser com quantas instâncias do Transit Gateway quiser por meio do Public VIF. Quando você cria um emparelhamento de BGP pela VIF pública, a AWS anuncia toda a faixa de IP público da AWS para o seu roteador. Para garantir que você permita apenas determinado tráfego (por exemplo, permitindo tráfego somente para os terminais de terminação de VPN), é recomendável usar um firewall em instalações locais. Essa opção pode ser usada para criptografar seu Direct Connect na camada de rede.
- Opção 5: criar uma conexão VPN com o Transit Gateway AWS Direct Connect usando VPN IP privada — A VPN IP privada é um recurso que oferece aos clientes a capacidade de implantar conexões VPN Site-to-Site da AWS pelo Direct Connect usando endereços IP privados. Com esse recurso, você pode criptografar o tráfego entre suas redes locais e a AWS por meio de conexões Direct Connect sem a necessidade de endereços IP públicos, aumentando assim a segurança e a privacidade da rede ao mesmo tempo. A VPN IP privada é implantada sobre os Transit VIFs, portanto, permite que você use o Transit Gateway para o gerenciamento centralizado das VPCs dos clientes e das conexões com as redes locais de uma maneira mais segura, privada e escalável.
- Opção 6: Criar túneis GRE para o Transit Gateway por meio de uma VIF de trânsito — O tipo de anexo Transit Gateway Connect é compatível com GRE. Com o Transit Gateway Connect, a infraestrutura SD-WAN pode ser conectada nativamente à AWS sem precisar configurar VPNs IPsec entre os dispositivos virtuais de rede SD-WAN e o Transit Gateway. Os túneis GRE podem ser estabelecidos em uma VIF de trânsito, tendo o Transit Gateway Connect como o tipo de conexão, fornecendo maior desempenho de largura de banda em comparação com uma conexão VPN. Para obter mais informações, consulte a postagem do blog Simplifique a conectividade SD-WAN com o AWS Transit Gateway Connect.

A opção “VIF de trânsito para gateway Direct Connect” pode parecer a melhor opção, pois permite consolidar toda a conectividade local de um determinado ponto Região da AWS em um único ponto

(Transit Gateway) usando uma única sessão BGP por conexão do Direct Connect; no entanto, alguns dos limites e considerações sobre essa opção podem levar você a usar VIFs privadas e de trânsito em conjunto para atender aos requisitos de conectividade da Landing Zone.

A figura a seguir ilustra um exemplo de configuração em que o Transit VIF é usado como um método padrão para conexão com VPCs e um VIF privado é usado para um caso de uso periférico em que quantidades excepcionalmente grandes de dados devem ser transferidas de um data center local para a VPC de mídia. O VIF privado é usado para evitar cobranças de processamento 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 — 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 pode criar uma VPN como conectividade de backup às AWS Direct Connect conexões.

Com a opção “Create GRE tunnels to Transit Gateway over a transit VIF”, você tem a capacidade de conectar de forma nativa sua infraestrutura de SD-WAN à AWS. Ele elimina a necessidade de configurar VPNs IPsec entre os dispositivos virtuais de rede SD-WAN e o Transit Gateway.



Exemplo de arquitetura de referência para conectividade híbrida

Use a conta de Serviços de Rede para criar recursos do Direct Connect, permitindo a demarcação dos limites administrativos da rede. As conexões Direct Connect, os gateways Direct Connect e os Transit Gateways podem residir em uma conta de Serviços de Rede. Para compartilhar a AWS Direct Connect conectividade com sua Landing Zone, basta compartilhar o Transit Gateway AWS RAM com outras contas.

Segurança MACsec em conexões Direct Connect

Os clientes podem usar a criptografia MAC Security Standard (MACsec) (IEEE 802.1AE) com suas conexões Direct Connect para conexões dedicadas de 10 Gbps e 100 Gbps em locais selecionados. Com esse recurso, os clientes podem proteger seus dados no nível da camada 2, e o Direct Connect

fornece point-to-point criptografia. Para ativar o recurso Direct Connect MACsec, certifique-se de que os pré-requisitos do MACsec sejam atendidos. Como o MACsec protege os links em uma hop-by-hop base, seu dispositivo deve ter uma adjacência direta de camada 2 com nosso dispositivo Direct Connect. Seu provedor de última milha pode ajudá-lo a verificar se sua conexão funcionará com o MACsec. Para obter mais informações, consulte Adicionar segurança MACsec às conexões do AWS Direct Connect.

AWS Direct Connect recomendações de resiliência

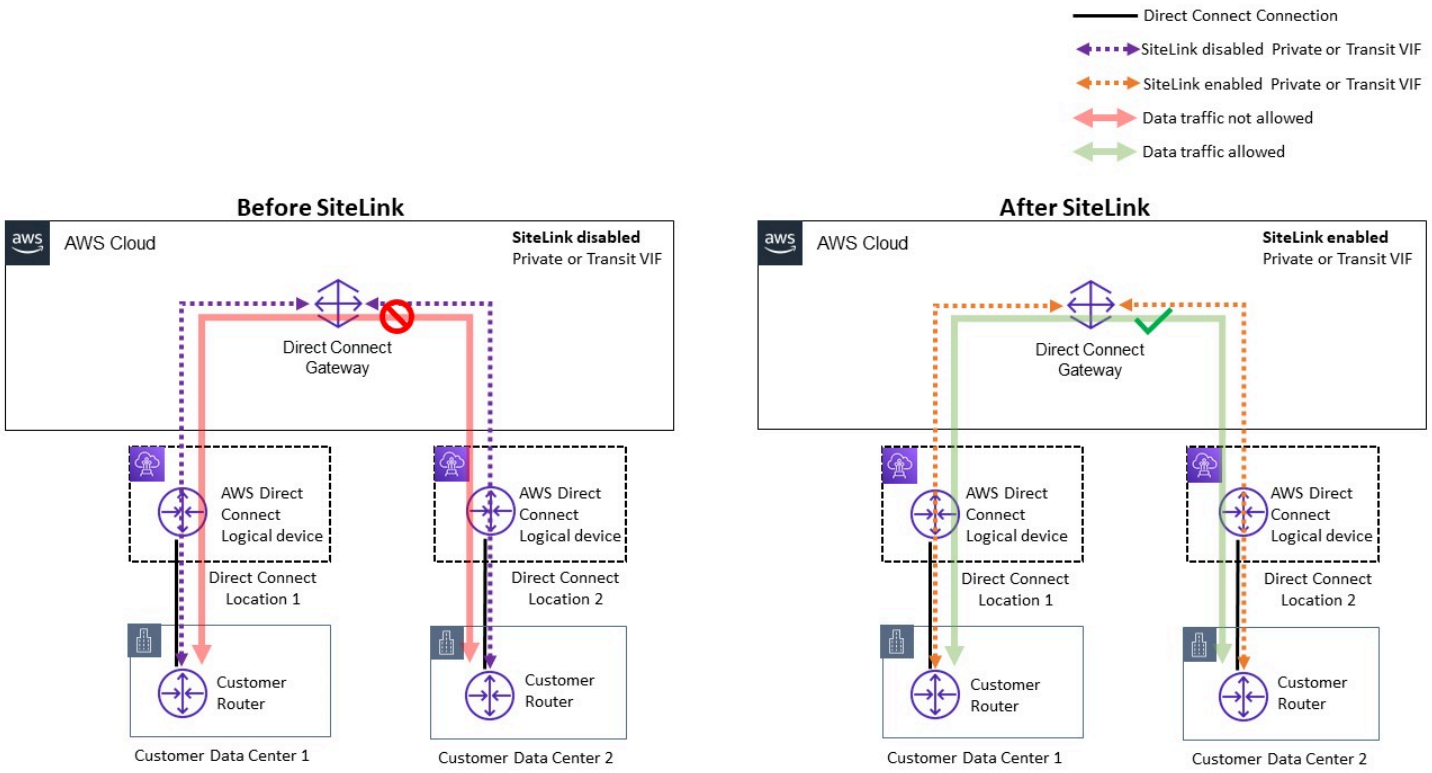
Com isso AWS Direct Connect, os clientes podem obter conectividade altamente resiliente em suas Amazon VPCs e recursos da AWS a partir de suas redes locais. É uma prática recomendada que os clientes se conectem a partir de vários data centers para eliminar qualquer falha de localização física em um único ponto. Também é recomendável que, dependendo do tipo de carga de trabalho, os clientes utilizem mais de uma conexão Direct Connect para redundância.

A AWS também oferece o AWS Direct Connect Resiliency Toolkit, que fornece aos clientes um assistente de conexão com vários modelos de redundância; para ajudá-los a determinar qual modelo funciona melhor para seus requisitos de acordo de nível de serviço (SLA) e projetar sua conectividade híbrida usando conexões Direct Connect adequadamente. Para obter mais informações, consulte Recomendações de AWS Direct Connect resiliência.

AWS Direct Connect SiteLink

Anteriormente, a configuração de site-to-site links para suas redes locais só era possível usando a criação direta de circuitos por meio de fibra escura ou outras tecnologias, VPNs IPSEC, ou usando provedores de circuitos terceirizados com tecnologias como MPLS ou circuitos T1 antigos. MetroEthernet Com o advento do SiteLink, os clientes agora podem habilitar a site-to-site conectividade direta para seus locais, que terminam em um local. AWS Direct Connect Use seu circuito Direct Connect para fornecer site-to-site conectividade sem precisar rotear o tráfego pelas suas VPCs, ignorando completamente a região da AWS.

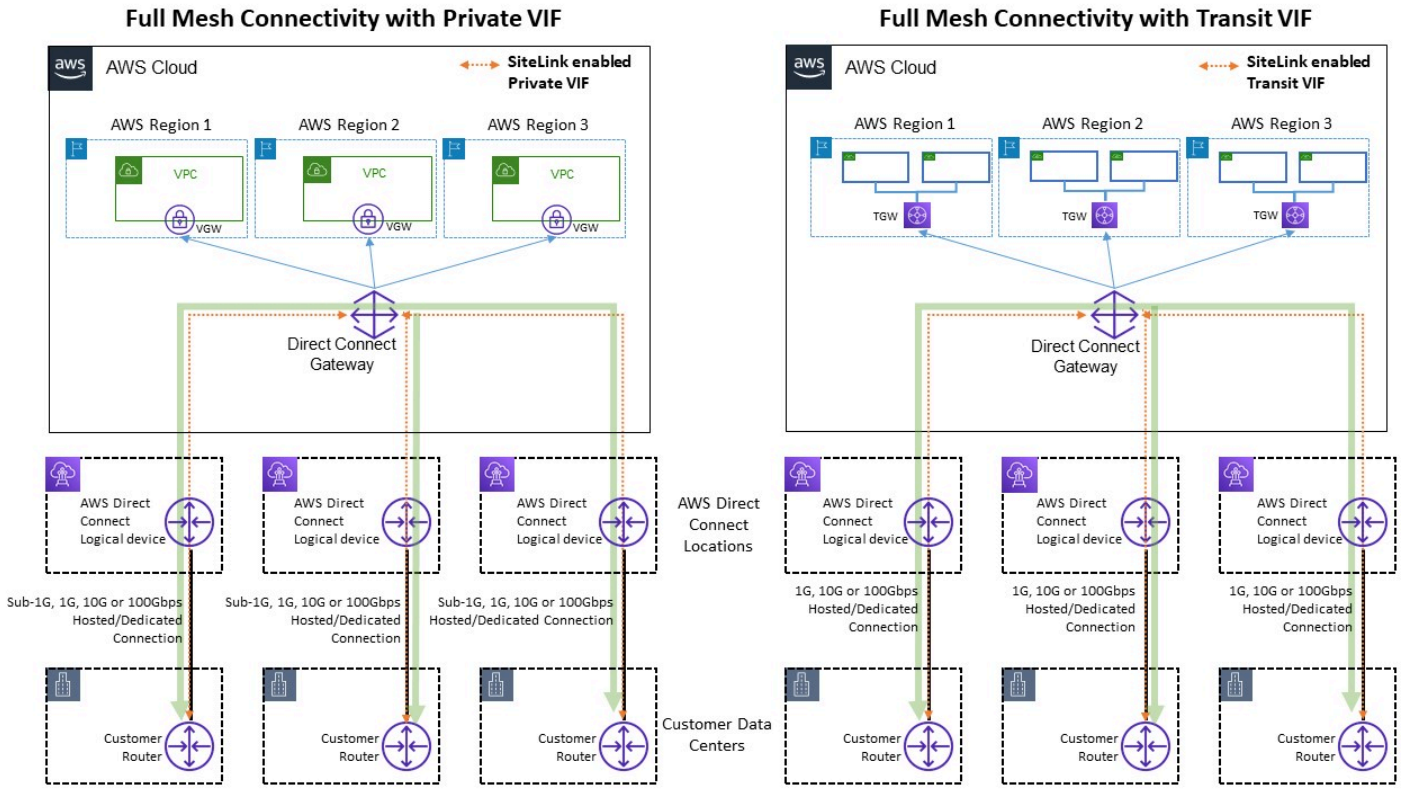
Agora, você pode criar pay-as-you-go conexões globais e confiáveis entre os escritórios e data centers em sua rede global enviando dados pelo caminho mais rápido entre os AWS Direct Connect locais.



Exemplo de arquitetura de referência para AWS Direct Connect SiteLink

Ao usar SiteLink, você primeiro conecta suas redes locais à AWS em qualquer um dos mais de 100 AWS Direct Connect locais em todo o mundo. Em seguida, você cria interfaces virtuais (VIFs) nessas conexões e as ativa SiteLink. Depois que todas as VIFs estiverem conectadas ao mesmo AWS Direct Connect gateway (DXGW), você poderá começar a enviar dados entre elas. Seus dados seguem o caminho mais curto entre os AWS Direct Connect locais até o destino, usando a rede global rápida, segura e confiável da AWS. Você não precisa ter nenhum recurso Região da AWS para usar SiteLink.

Com SiteLink, o DXGW aprende prefixos IPv4/IPv6 de seus roteadores em VIFs SiteLink habilitados, executa o algoritmo de melhor caminho do BGP, atualiza atributos como NextHop e as_Path e anuncia novamente esses prefixos BGP para o restante dos VIFs habilitados associados a esse DXGW. SiteLink Se você desabilitar SiteLink em uma VIF, o DXGW não anunciará os prefixos locais aprendidos sobre essa VIF para outras VIFs habilitadas. SiteLink Os prefixos locais de uma VIF SiteLink desativada são anunciados somente para as associações do DXGW Gateway, como instâncias do AWS Virtual Private Gateways (VGWS) ou Transit Gateway (TGW) associadas ao DXGW.



Exemplo de link de site que permite fluxos de tráfego

SiteLink permite que os clientes usem a rede global da AWS para funcionar como uma conexão primária ou secundária/de backup entre seus locais remotos, com alta largura de banda e baixa latência, com roteamento dinâmico para controlar quais locais podem se comunicar entre si e com seus recursos regionais da AWS.

Para obter mais informações, consulte Apresentando AWS Direct Connect SiteLink.

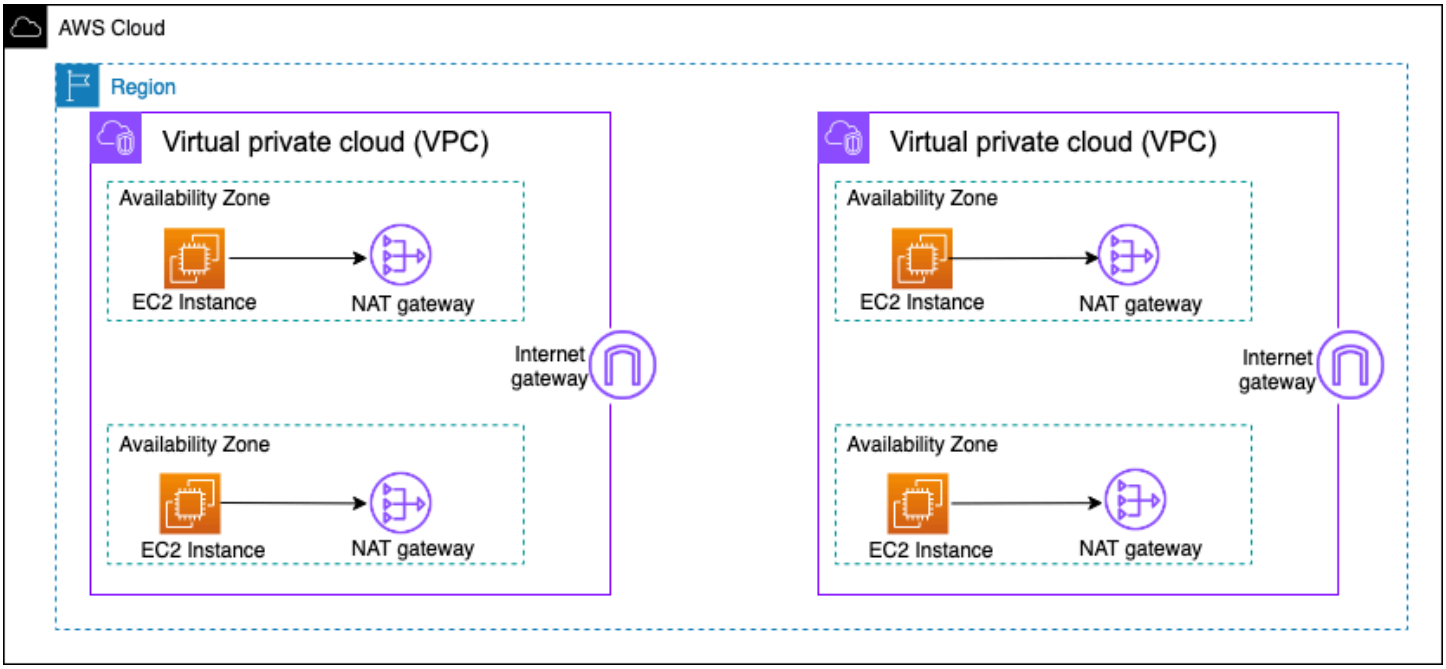
Saída centralizada para a Internet

À medida que você implanta aplicativos em seu ambiente de várias contas, muitos aplicativos exigirão acesso somente de saída à Internet (por exemplo, download de bibliotecas, patches ou atualizações do sistema operacional). Isso pode ser feito para tráfego IPv4 e IPv6. Para IPv4, isso pode ser obtido por meio da conversão de endereços de rede (NAT) na forma de um gateway NAT (recomendado) ou, alternativamente, de uma instância NAT autogerenciada em execução em uma instância do Amazon EC2, como meio de acesso à Internet de saída. Os aplicativos internos residem em sub-redes privadas, enquanto as instâncias NAT Gateways/Amazon EC2 NAT residem em uma sub-rede pública. A AWS recomenda que você use gateways NAT porque eles oferecem melhor disponibilidade e largura de banda e exigem menos esforço de sua parte para administrar. Para obter mais informações, consulte Compare gateways NAT e instâncias NAT. Para tráfego IPv6, o tráfego de saída pode ser configurado para sair de cada VPC por meio de um gateway de Internet somente de saída de forma descentralizada ou pode ser configurado para ser enviado para uma VPC centralizada usando instâncias NAT ou instâncias de proxy. Os padrões IPv6 são discutidos abaixo na seção Saída centralizada para IPv6 deste documento.

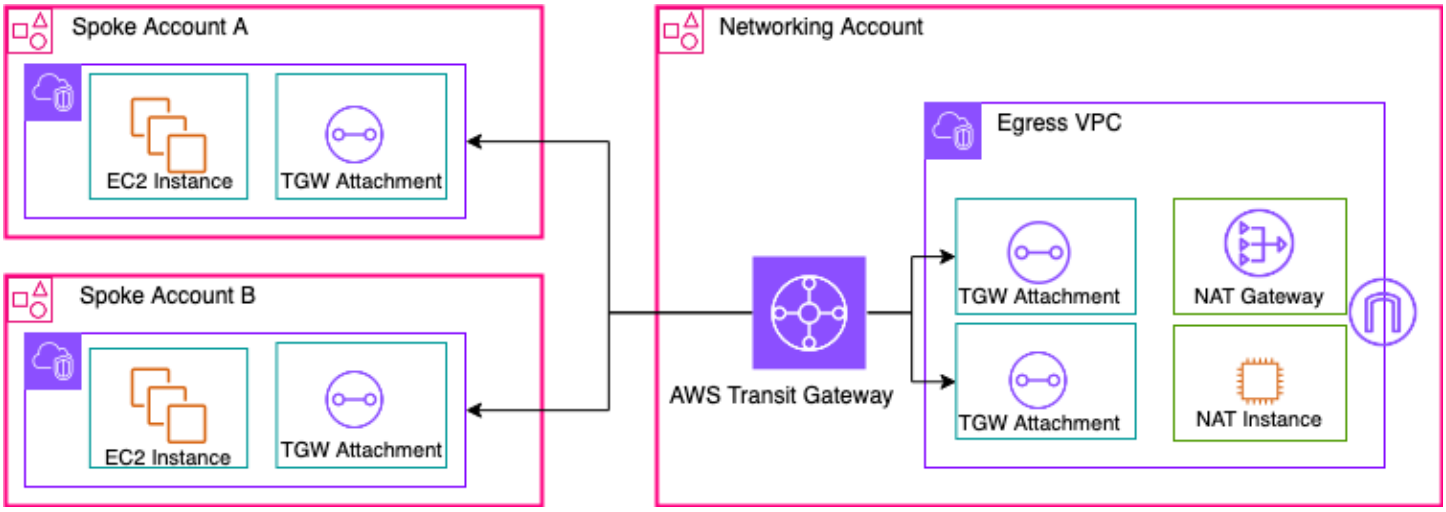
Usando o gateway NAT para saída IPv4 centralizada

O gateway NAT é um serviço gerenciado de tradução de endereços de rede. A implantação de um gateway NAT em cada VPC spoke pode se tornar um custo proibitivo, pois você paga uma taxa por hora por cada gateway NAT que você implanta (consulte os preços da Amazon VPC). Centralizar os gateways NAT pode ser uma opção viável para reduzir custos. Para centralizar, você cria uma VPC de saída separada na conta de serviços de rede, implanta gateways NAT na VPC de saída e roteia todo o tráfego de saída das VPCs spoke para os gateways NAT que residem na VPC de saída usando Transit Gateway ou CloudWAN, conforme mostrado na figura a seguir.

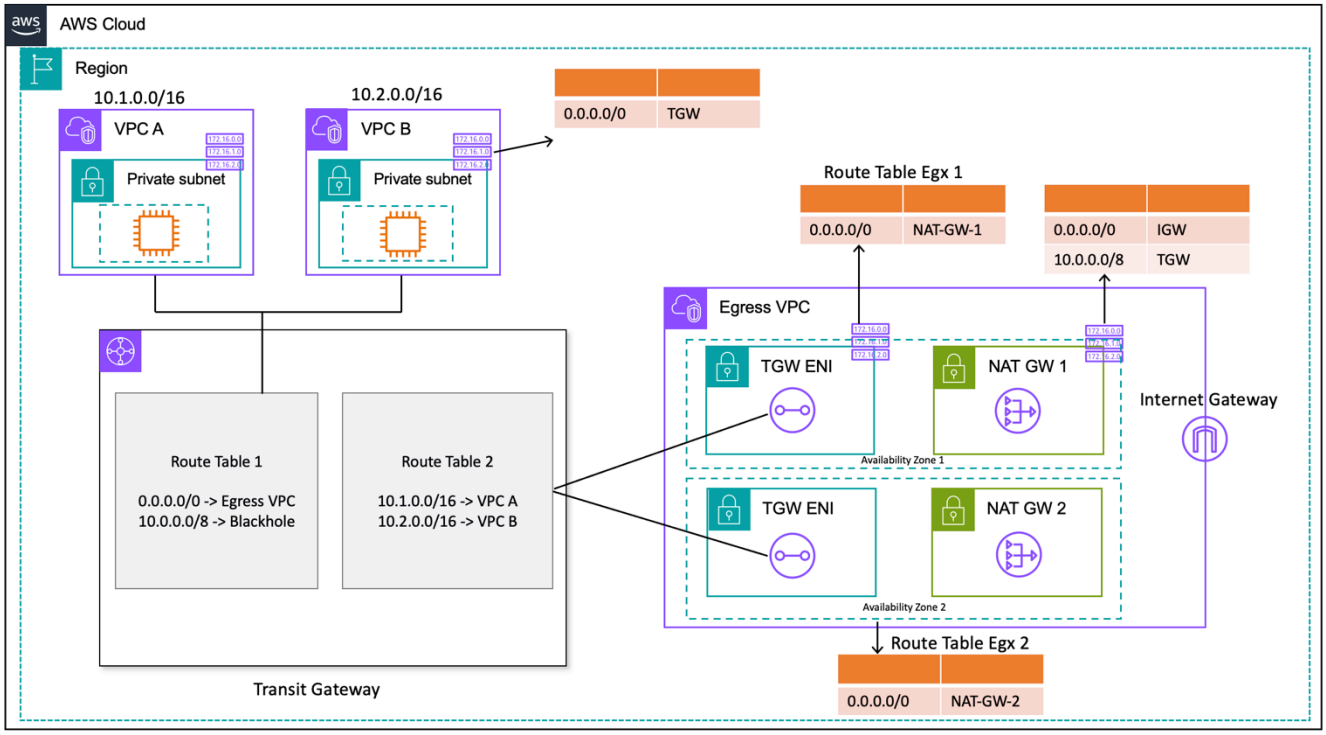
> **Note**
>
> Ao centralizar o gateway NAT usando o Transit Gateway, você paga uma taxa extra de processamento de dados do Transit Gateway, em comparação com a abordagem descentralizada de executar um gateway NAT em cada VPC. Em alguns casos extremos, quando você envia grandes quantidades de dados por meio do gateway NAT de uma VPC, manter a NAT local na VPC para evitar a cobrança de processamento de dados do Transit Gateway pode ser uma opção mais econômica.



Arquitetura de gateway NAT descentralizada de alta disponibilidade



Gateway NAT centralizado usando o Transit Gateway (visão geral)



Gateway NAT centralizado usando Transit Gateway (design de tabela de rotas)

Nessa configuração, os anexos VPC do spoke são associados à Tabela de Rota 1 (RT1) e são propagados para a Tabela de Rota 2 (RT2). Existe uma rota Blackhole para impedir que as duas VPCs se comuniquem umas com as outras. Se quiser permitir a comunicação entre VPC, você pode remover a entrada da `10.0.0.0/8 -> Blackhole` rota do RT1. Isso permite que eles se comuniquem por meio do gateway de trânsito. Você também pode propagar os anexos do VPC spoke para o RT1 (ou, alternativamente, você pode usar uma tabela de rotas e associar/propagar tudo a ela), permitindo o fluxo direto de tráfego entre as VPCs usando o Transit Gateway.

Você adiciona uma rota estática no RT1 apontando todo o tráfego para a VPC de saída. Por causa dessa rota estática, o Transit Gateway envia todo o tráfego da Internet por meio de seus ENIs na VPC de saída. Uma vez na VPC de saída, o tráfego segue as rotas definidas na tabela de rotas da sub-rede em que esses ENIs do Transit Gateway estão presentes. Você adiciona uma rota nas tabelas de rotas de sub-rede apontando todo o tráfego para o respectivo gateway NAT na mesma zona de disponibilidade para minimizar o tráfego da zona de disponibilidade cruzada (AZ). A tabela de rotas de sub-rede do gateway NAT tem o Internet Gateway (IGW) como o 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 vinculado ao VPC do Spoke para o Transit Gateway como o próximo salto.

Alta disponibilidade

Para alta disponibilidade, você deve usar mais de um gateway NAT (um em cada zona de disponibilidade). Se um gateway NAT não estiver disponível, o tráfego poderá ser descartado na zona de disponibilidade que está atravessando o gateway NAT afetado. Se uma zona de disponibilidade não estiver disponível, o endpoint do Transit Gateway junto com o gateway NAT nessa zona de disponibilidade falharão e todo o tráfego fluirá pelos endpoints do Transit Gateway e do gateway NAT na outra zona de disponibilidade.

Segurança

Você pode confiar em grupos de segurança nas instâncias de origem, nas rotas blackhole nas tabelas de rotas do Transit Gateway e na ACL de rede da sub-rede na qual o gateway NAT está localizado. Por exemplo, os clientes podem usar ACLs nas sub-redes públicas do NAT Gateway para permitir ou bloquear endereços IP de origem ou destino. Como alternativa, você pode usar o NAT Gateway com AWS Network Firewall a saída centralizada descrita na próxima seção para atender a esse requisito.

Escalabilidade

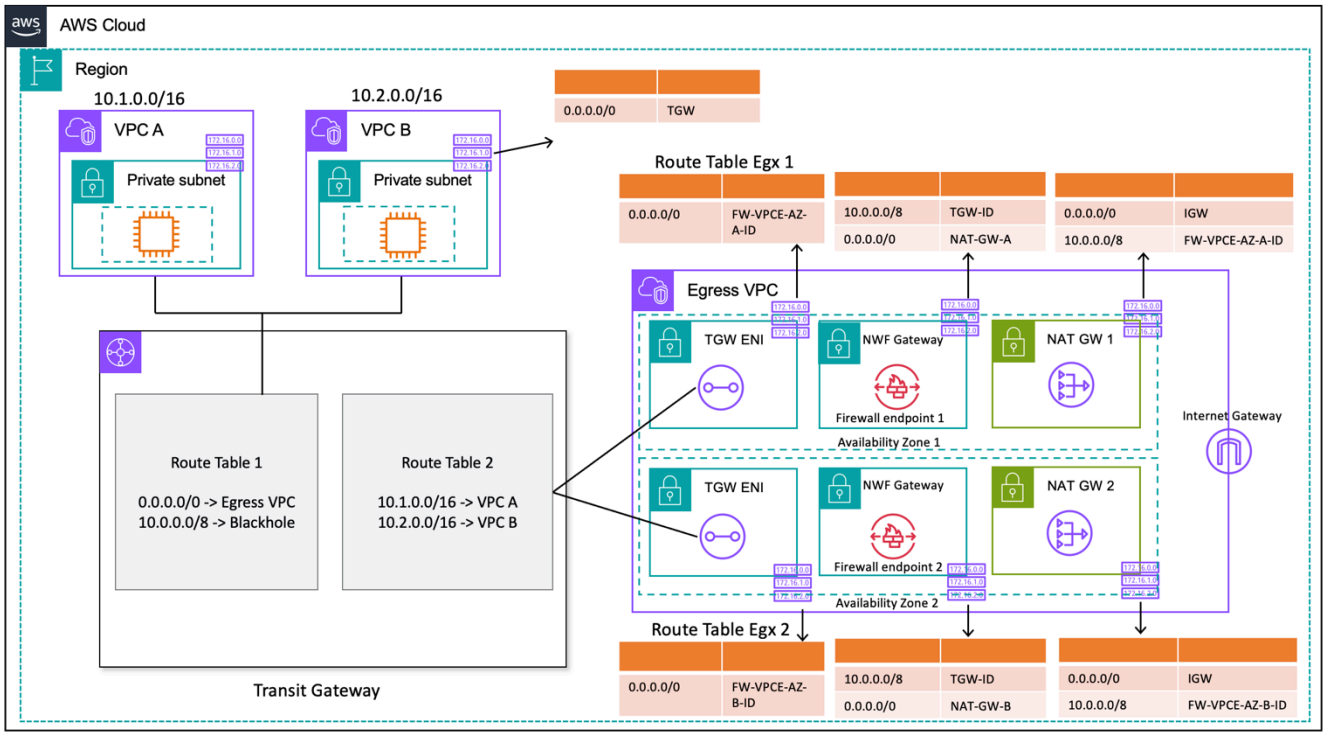
Um único gateway NAT pode suportar até 55.000 conexões simultâneas por endereço IP atribuído a cada destino exclusivo. Você pode solicitar um ajuste de cota para permitir até oito endereços IP atribuídos, permitindo 440.000 conexões simultâneas com um único IP e porta de destino. O gateway NAT fornece 5 Gbps de largura de banda e escala automaticamente para 100 Gbps. O Transit Gateway geralmente não atua como um balanceador de carga e não distribuiria seu tráfego uniformemente entre gateways NAT nas várias zonas de disponibilidade. O tráfego no Transit Gateway permanecerá dentro de uma zona de disponibilidade, se possível. Se o tráfego inicial da instância do Amazon EC2 estiver na Zona de Disponibilidade 1, o tráfego fluirá da interface de rede elástica do Transit Gateway na mesma Zona de Disponibilidade 1 na VPC de saída e fluirá para o próximo salto com base na tabela de rotas de sub-rede na qual a interface de rede elástica reside. Para obter uma lista completa de regras, consulte os gateways NAT na documentação da Amazon Virtual Private Cloud.

Para obter mais informações, consulte a postagem do blog Como criar um único ponto de saída de internet a partir de várias VPCs usando o AWS Transit Gateway.

Usando o gateway NAT com AWS Network Firewall para saída IPv4 centralizada

Se quiser inspecionar e filtrar seu tráfego de saída, você pode incorporar o AWS Network Firewall com o gateway NAT em sua arquitetura de saída centralizada. AWS Network Firewall é um serviço gerenciado que facilita a implantação de proteções de rede essenciais para todas as suas VPCs. Ele fornece controle e visibilidade do tráfego de rede de camada 3-7 para toda a sua VPC. Você pode fazer a filtragem de URL/nome de domínio, endereço IP e tráfego de saída com base em conteúdo para impedir possíveis perdas de dados, ajudar a atender aos requisitos de conformidade e bloquear comunicações de malware conhecidas. AWS Network Firewall suporta milhares de regras que podem filtrar o tráfego de rede destinado a endereços IP inválidos conhecidos ou nomes de domínio inválidos. Você também pode usar as regras IPS do Suricata como parte do AWS Network Firewall serviço importando conjuntos de regras de código aberto ou criando suas próprias regras do Sistema de Prevenção de Intrusões (IPS) usando a sintaxe de regras do Suricata. AWS Network Firewall também permite que você importe regras compatíveis provenientes de parceiros da AWS.

Na arquitetura de saída centralizada com inspeção, o AWS Network Firewall endpoint é um destino padrão da tabela de rotas na tabela de rotas de sub-rede de anexos do gateway de trânsito para a VPC de saída. O tráfego entre VPCs spoke e a Internet é inspecionado usando AWS Network Firewall conforme mostrado no diagrama a seguir.



Saída centralizada com AWS Network Firewall gateway NAT (design de tabela de rotas)

Para um modelo de implantação centralizada com o Transit Gateway, a AWS recomenda a implantação de AWS Network Firewall endpoints em várias zonas de disponibilidade. Deve haver um endpoint de firewall em cada zona de disponibilidade em que o cliente está executando cargas de trabalho, conforme mostrado no diagrama anterior. Como prática recomendada, a sub-rede do firewall não deve conter nenhum outro tráfego porque não AWS Network Firewall é capaz de inspecionar o tráfego de origens ou destinos dentro de uma sub-rede do firewall.

Semelhante à configuração anterior, os anexos de VPC do spoke são associados à Tabela de Rota 1 (RT1) e são propagados para a Tabela de Rota 2 (RT2). Uma rota Blackhole é adicionada explicitamente para impedir que as duas VPCs se comuniquem uma com a outra.

Continue usando uma rota padrão no RT1 apontando todo o tráfego para a VPC de saída. O Transit Gateway encaminhará todos os fluxos de tráfego para uma das duas zonas de disponibilidade na VPC de saída. Quando o tráfego atinge uma das ENIs do Transit Gateway na VPC de saída, você atinge uma rota padrão que encaminhará o tráfego para um dos AWS Network Firewall endpoints em sua respectiva zona de disponibilidade. AWS Network Firewall em seguida, inspecionará o tráfego com base nas regras definidas antes de encaminhá-lo para o gateway NAT usando uma rota padrão.

Esse caso não exige o modo de dispositivo Transit Gateway, porque você não está enviando tráfego entre anexos.

> **Note**
>
> AWS Network Firewall não realiza a tradução de endereços de rede para você, essa função seria tratada pelo gateway NAT após a inspeção de tráfego através do. AWS Network Firewall O roteamento de entrada não é necessário nesse caso, pois o tráfego de retorno será encaminhado para os IPs NATGW por padrão.

Como você está usando um Transit Gateway, aqui podemos colocar o firewall antes do gateway NAT. Nesse modelo, o firewall pode ver o IP de origem por trás do Transit Gateway.

Se você estiver fazendo isso em uma única VPC, podemos usar os aprimoramentos de roteamento da VPC que permitem inspecionar o tráfego entre sub-redes na mesma VPC. Para obter detalhes, consulte a postagem do blog sobre modelos de implantação AWS Network Firewall com aprimoramentos de roteamento de VPC.

Escalabilidade

AWS Network Firewall pode aumentar ou diminuir automaticamente a capacidade do firewall com base na carga de tráfego para manter um desempenho estável e previsível e minimizar os custos. AWS Network Firewall foi projetado para suportar dezenas de milhares de regras de firewall e pode escalar até 100 Gbps de taxa de transferência por zona de disponibilidade.

Considerações importantes

- Cada endpoint de firewall pode lidar com cerca de 100 Gbps de tráfego. Se você precisar de maior intermitência ou taxa de transferência sustentada, entre em contato com o suporte da AWS.
- Se você optar por criar um gateway NAT em sua conta da AWS junto com o Network Firewall, o processamento padrão do gateway NAT e as cobranças de uso por hora serão dispensadas com one-to-one base no processamento por GB e nas horas de uso cobradas pelo seu firewall.
- Você também pode considerar endpoints de firewall distribuídos AWS Firewall Manager sem um Transit Gateway.
- Teste as regras de firewall antes de movê-las para a produção, semelhante a uma lista de controle de acesso à rede, conforme a ordem for importante.
- Regras avançadas de Suricata são necessárias para uma inspeção mais profunda. O firewall de rede oferece suporte à inspeção criptografada de tráfego para entrada e saída.
- A variável do grupo de `HOME_NET` regras definiu o intervalo de IP de origem elegível para processamento no mecanismo Stateful. Usando uma abordagem centralizada, você deve adicionar todos os CIDRs de VPC adicionais anexados ao Transit Gateway para torná-los elegíveis para processamento. Consulte a documentação do Network Firewall para obter mais detalhes sobre a variável do grupo de `HOME_NET` regras.
- Considere implantar o Transit Gateway e a VPC de saída em uma conta separada dos Serviços de Rede para segregar o acesso com base na delegação de tarefas; por exemplo, somente administradores de rede podem acessar a conta dos Serviços de Rede.
- Para simplificar a implantação e o gerenciamento deste AWS Network Firewall modelo, AWS Firewall Manager pode ser usado. O Firewall Manager permite que você administre centralmente seus diferentes firewalls aplicando automaticamente a proteção criada no local centralizado a várias contas. O Firewall Manager oferece suporte a modelos de implantação distribuídos e centralizados para o Firewall de Rede. Para saber mais, consulte a postagem do blog Como implantar AWS Network Firewall usando AWS Firewall Manager.

Usando o gateway NAT e o Gateway Load Balancer com instâncias do Amazon EC2 para saída IPv4 centralizada

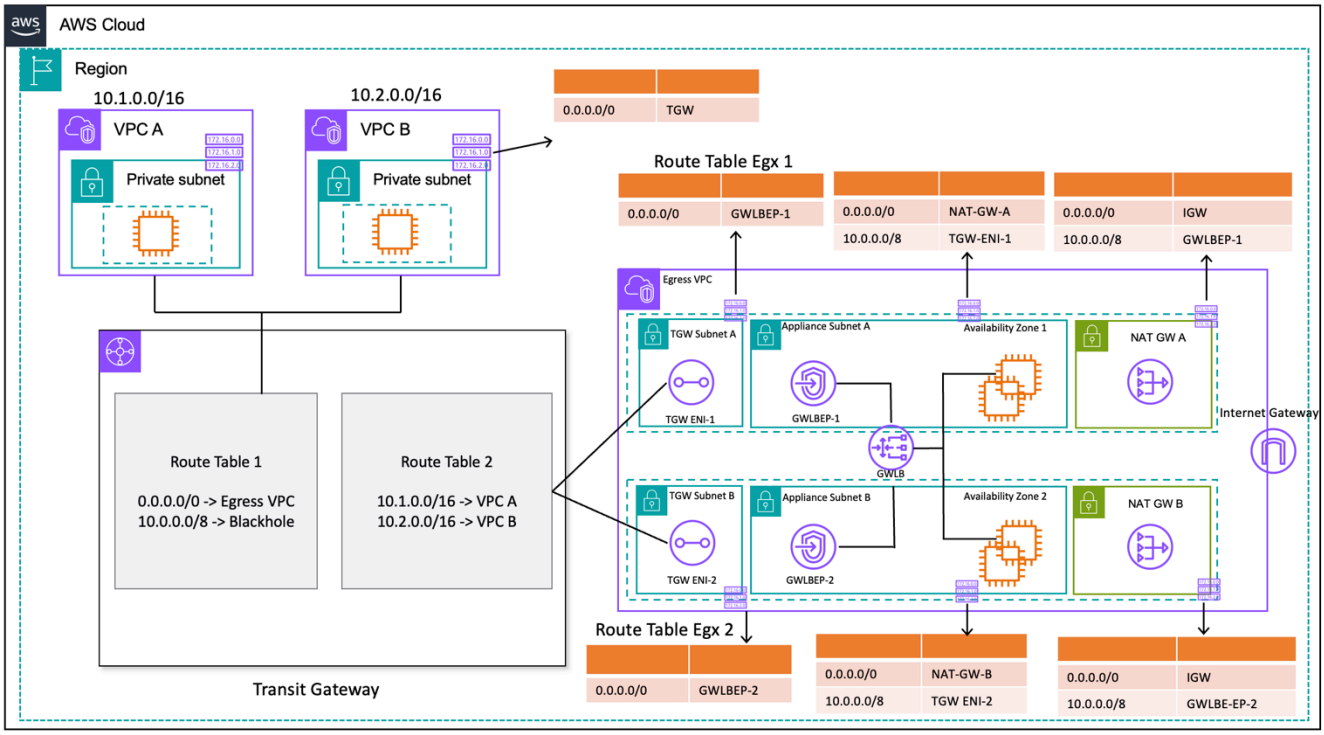
Usar um dispositivo virtual baseado em software (no Amazon EC2) de AWS Marketplace e AWS Partner Network como um ponto de saída é semelhante à configuração do gateway NAT. Essa opção pode ser usada se você quiser usar o avançado Firewall/Sistema de Prevenção/Detecção de Intrusões (IPS/IDS) de camada 7 e os recursos de inspeção profunda de pacotes das ofertas de vários fornecedores.

Na figura a seguir, além do gateway NAT, você implanta dispositivos virtuais usando instâncias EC2 por trás de um Gateway Load Balancer (GWLB). Nessa configuração, o GWLB, o Gateway Load Balancer Endpoint (GWLBE), os dispositivos virtuais e os gateways NAT são implantados em uma VPC centralizada conectada ao Transit Gateway usando o anexo VPC. As VPCs spoke também são conectadas ao Transit Gateway usando um anexo VPC. Como os GWLBEs são um destino roteável, você pode rotear o tráfego que se move de e para o Transit Gateway para a frota de dispositivos virtuais configurados como destinos por trás de um GWLB. O GWLB atua como um bump-in-the-wire e transmite de forma transparente todo o tráfego de camada 3 por meio de dispositivos virtuais de terceiros e, portanto, é invisível para a origem e o destino do tráfego. Portanto, essa arquitetura permite que você inspecione centralmente todo o tráfego de saída que passa pelo Transit Gateway.

Para obter mais informações sobre como o tráfego flui dos aplicativos nas VPCs para a Internet e de volta por meio dessa configuração, consulte Arquitetura de inspeção centralizada com o AWS Gateway Load Balancer e. AWS Transit Gateway

Você pode ativar o modo de dispositivo no Transit Gateway para manter a simetria do fluxo por meio de dispositivos virtuais. Isso significa que o tráfego bidirecional é roteado pelo mesmo dispositivo e pela zona de disponibilidade durante toda a vida útil do fluxo. Essa configuração é particularmente importante para firewalls com estado que realizam inspeção profunda de pacotes. A ativação do modo de dispositivo elimina a necessidade de soluções alternativas complexas, como tradução de endereço de rede de origem (SNAT), para forçar o tráfego a retornar ao dispositivo correto para manter a simetria. Consulte Melhores práticas para implantar o Gateway Load Balancer para obter detalhes.

Também é possível implantar endpoints GWLB de forma distribuída sem o Transit Gateway para permitir a inspeção de saída. Saiba mais sobre esse padrão de arquitetura na publicação do blog Introducing AWS Gateway Load Balancer: Supported architecture patterns.



Saída centralizada com Gateway Load Balancer e instância EC2 (design de tabela de rotas)

Alta disponibilidade

A AWS recomenda a implantação de balanceadores de carga de gateway e dispositivos virtuais em várias zonas de disponibilidade para maior disponibilidade.

O Gateway Load Balancer pode realizar verificações de integridade para detectar falhas no dispositivo virtual. No caso de um dispositivo não íntegro, o GWLB redireciona os novos fluxos para dispositivos saudáveis. Os fluxos existentes sempre vão para o mesmo alvo, independentemente do estado de saúde do alvo. Isso permite a drenagem da conexão e acomoda falhas na verificação de integridade devido a picos de CPU nos dispositivos. Para obter mais detalhes, consulte a seção 4: Entenda os cenários de falha do dispositivo e da zona de disponibilidade na postagem do blog Melhores práticas para a implantação do Gateway Load Balancer. O Gateway Load Balancer pode usar grupos de escalonamento automático como alvos. Esse benefício elimina o trabalho pesado de gerenciar a disponibilidade e a escalabilidade das frotas de dispositivos.

Vantagens

Os endpoints do Gateway Load Balancer e do Gateway Load Balancer são alimentados AWS PrivateLink por, o que permite a troca de tráfego entre os limites da VPC com segurança, sem a necessidade de atravessar a Internet pública.

O Gateway Load Balancer é um serviço gerenciado que elimina o trabalho pesado indiferenciado de gerenciar, implantar e escalar dispositivos de segurança virtual para que você possa se concentrar nas coisas que importam. O Gateway Load Balancer pode expor a pilha de firewalls como um serviço de endpoint para os clientes assinarem usando o. AWS Marketplace Isso é chamado de Firewall as a Service (FWaaS); ele introduz uma implantação simplificada e elimina a necessidade de confiar no BGP e no ECMP para distribuir o tráfego em várias instâncias do Amazon EC2.

Considerações importantes

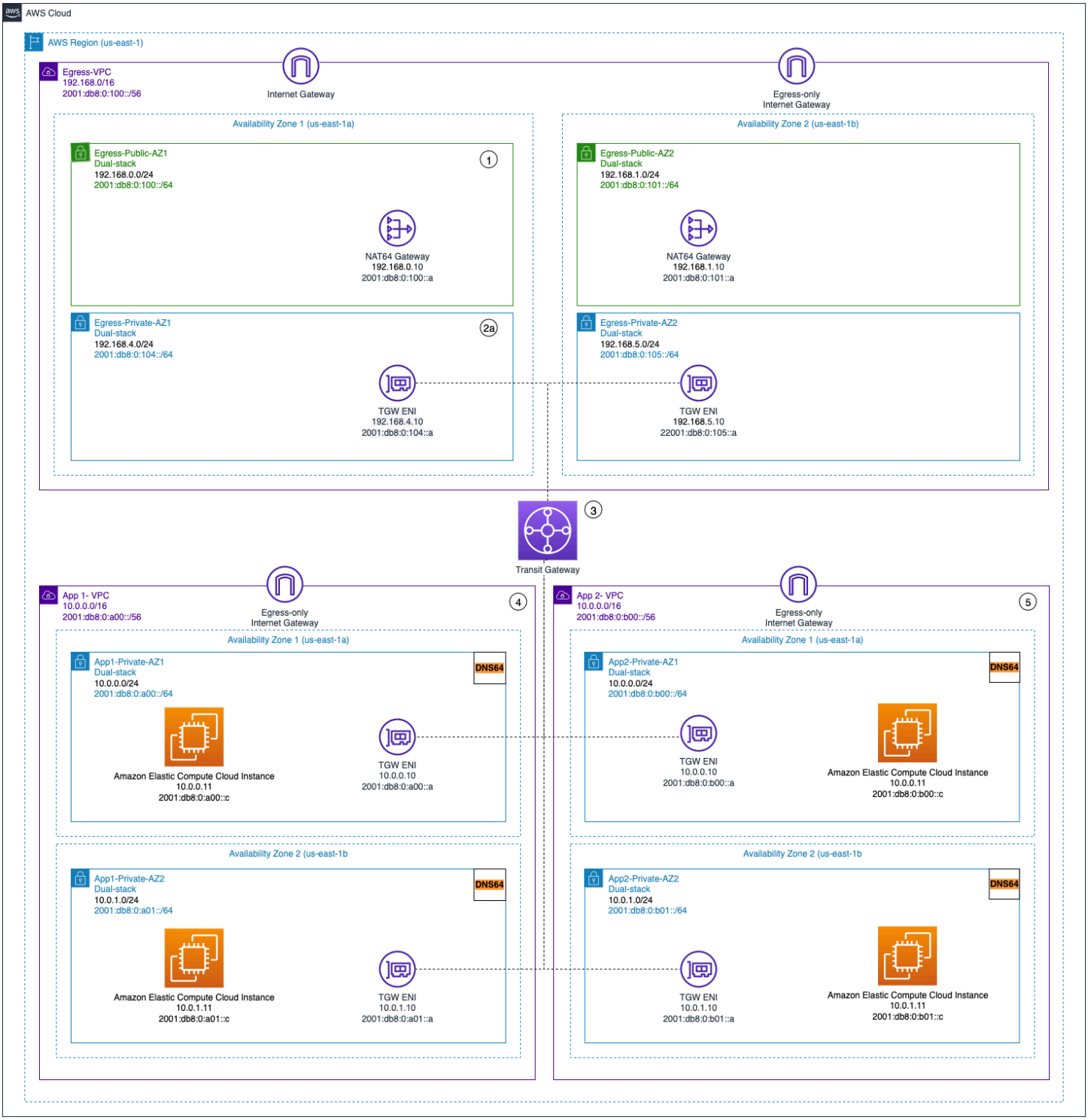
- Os dispositivos precisam suportar o protocolo de encapsulamento Geneve para se integrarem ao GWLB.
- Alguns dispositivos de terceiros podem suportar roteamento SNAT e sobreposição (modo de dois braços), eliminando assim a necessidade de criar gateways NAT para economizar custos. No entanto, consulte um parceiro da AWS de sua escolha antes de usar esse modo, pois isso depende do suporte e da implementação do fornecedor.
- Anote o tempo limite de inatividade do GWLB. Isso pode resultar em tempos limite de conexão nos clientes. Você pode ajustar seus tempos limite no nível do cliente, servidor, firewall e sistema operacional para evitar isso. Consulte a Seção 1: Ajuste os valores de manutenção de atividade ou tempo limite de TCP para oferecer suporte a fluxos de TCP de longa duração na postagem do blog Melhores práticas para implantar o Gateway Load Balancer para obter mais informações.
- Os GWLBE são alimentados por AWS PrivateLink, portanto, AWS PrivateLink as taxas serão aplicáveis. Você pode saber mais na página AWS PrivateLink de preços. Se você estiver usando o modelo centralizado com o Transit Gateway, as taxas de processamento de dados do TGW serão aplicáveis.
- Considere implantar o Transit Gateway e a VPC de saída em uma conta separada de serviços de rede para segregar o acesso com base na delegação de tarefas, como por exemplo, somente administradores de rede podem acessar a conta de serviços de rede.

Saída centralizada para IPv6

Para oferecer suporte à saída IPv6 em implantações de pilha dupla que tenham saída IPv4 centralizada, um dos dois padrões deve ser escolhido:

- Saída IPv4 centralizada com saída IPv6 descentralizada
- Saída IPv4 centralizada e saída IPv6 centralizada

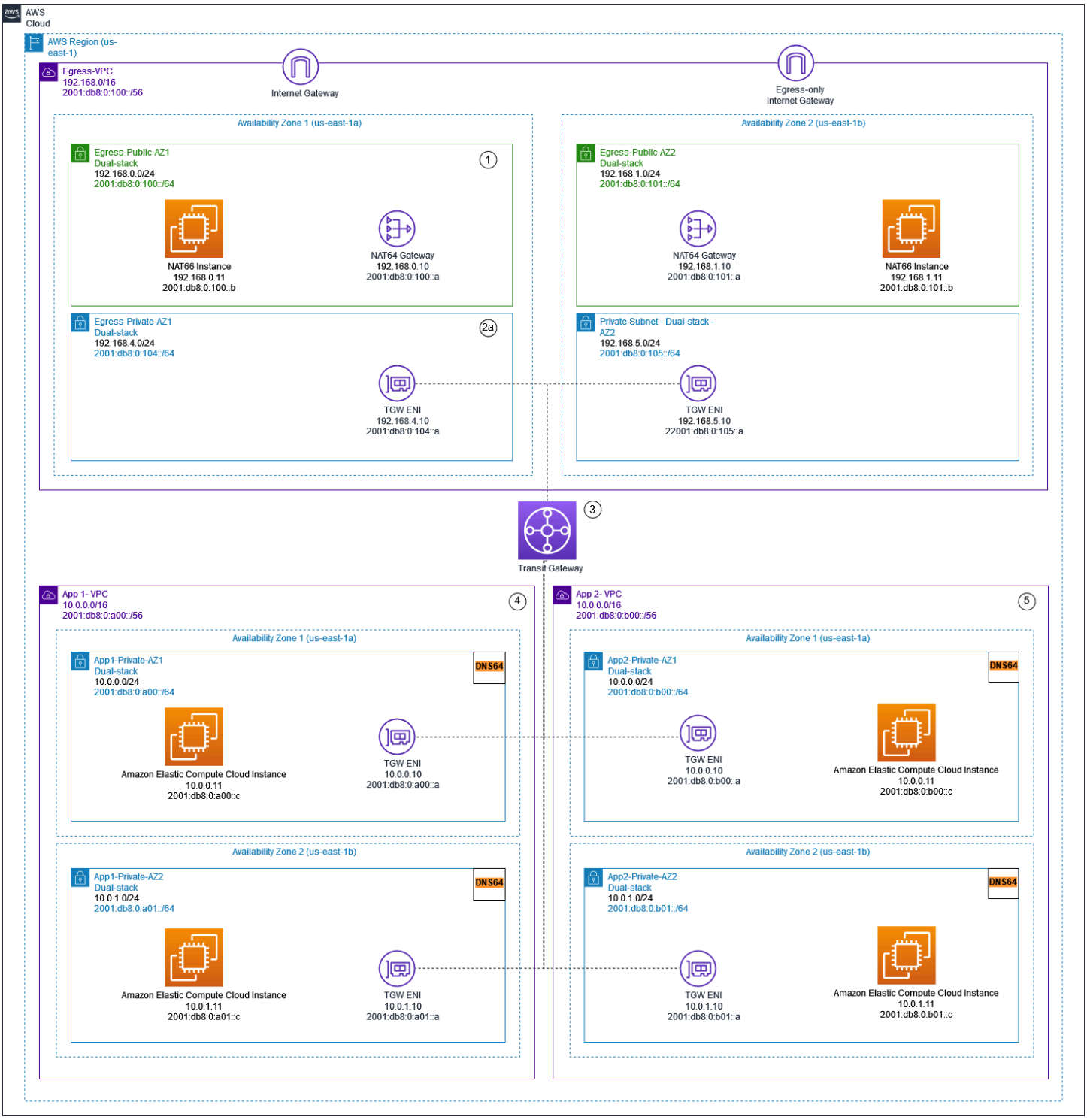
No primeiro padrão, mostrado no diagrama a seguir, gateways de internet somente de saída são implantados em cada VPC spoke. Os gateways de internet somente de saída são gateways escalonados horizontalmente, redundantemente e altamente disponíveis que permitem a comunicação de saída via IPv6 a partir de instâncias dentro da sua VPC. Eles impedem que a Internet inicie conexões IPv6 com suas instâncias. Os gateways de internet somente para saída são gratuitos. Nesse modelo de implantação, o tráfego IPv6 flui dos gateways de Internet somente de saída em cada VPC e o tráfego IPv4 flui pelos gateways NAT centralizados implantados.



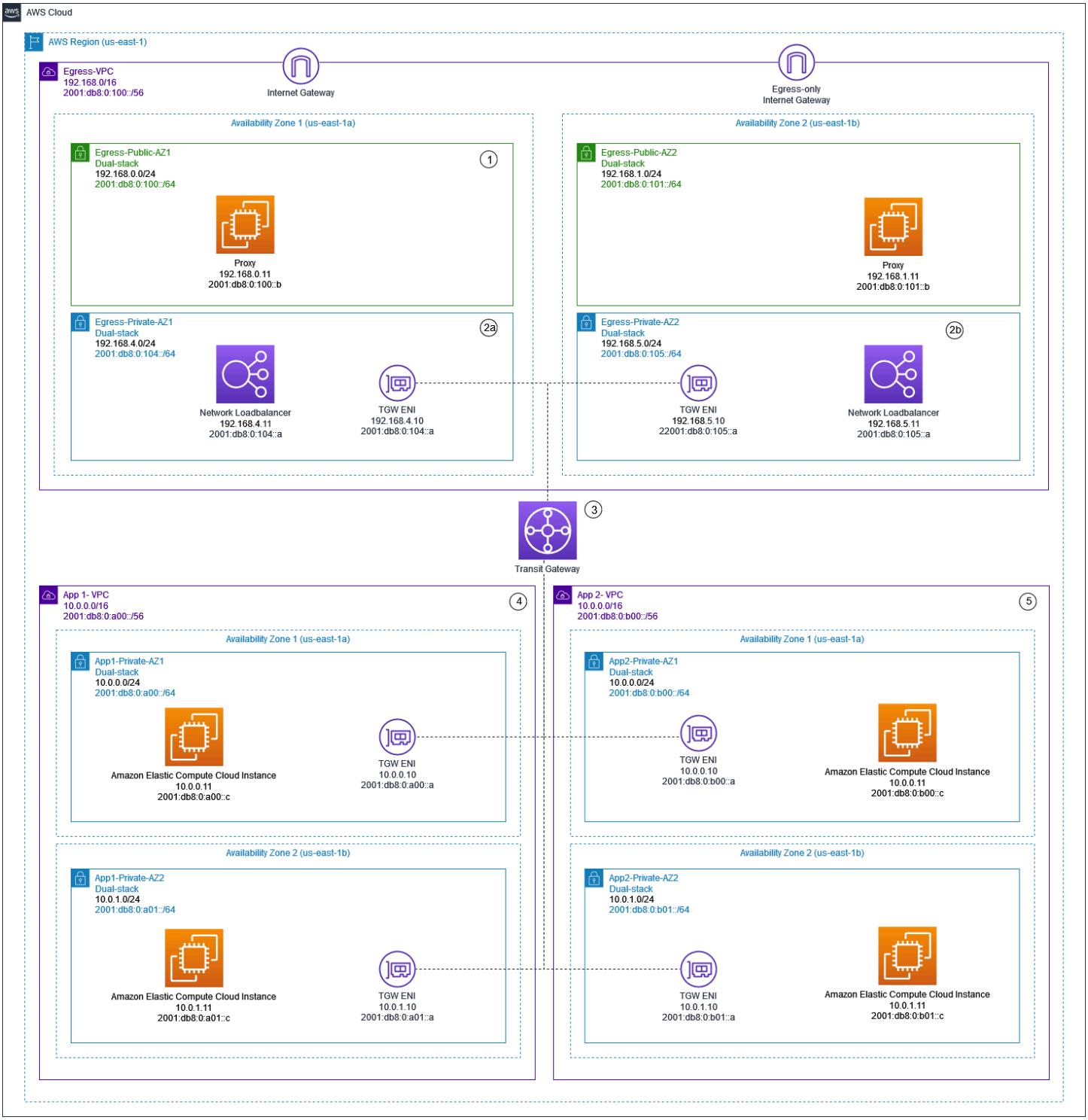
Saída IPV4 centralizada e saída IPv6 de saída descentralizada (somente saída IPv6)

No segundo padrão, mostrado nos diagramas a seguir, o tráfego IPv6 de saída das suas instâncias é enviado para uma VPC centralizada. Isso pode ser feito usando a tradução de prefixo de rede IPv6 para IPv6 (NPTv6) com instâncias NAT66 e gateways NAT ou usando instâncias de proxy e

Network Load Balancer. Esse padrão é aplicável se a inspeção centralizada do tráfego de saída for necessária e não puder ser executada em cada VPC de fala.



Saída IPv6 centralizada usando gateways NAT e instâncias NAT66



Saída centralizada de IPv4 e IPv6 usando instâncias de proxy e Network Load Balancer

O whitepaper IPv6 na AWS descreve os padrões centralizados de saída do IPv6. Os padrões de saída IPv6 são discutidos com mais detalhes no blog Tráfego centralizado de saída da Internet

para VPCs IPv4 e IPv6 de pilha dupla, junto com considerações especiais, exemplos de soluções e diagramas.

Segurança de rede centralizada para tráfego de VPC para VPC e local para VPC

Pode haver cenários em que um cliente queira implementar um firewall/IPS/IDs de camada 3 a 7 em seu ambiente de várias contas para inspecionar os fluxos de tráfego entre VPCs (tráfego leste-oeste) ou entre um data center local e uma VPC (tráfego norte-sul). Isso pode ser feito de maneiras diferentes, dependendo do caso de uso e dos requisitos. Por exemplo, você pode incorporar o Gateway Load Balancer, o Network Firewall, o Transit VPC ou usar arquiteturas centralizadas com Transit Gateways. Esses cenários são discutidos na seção a seguir.

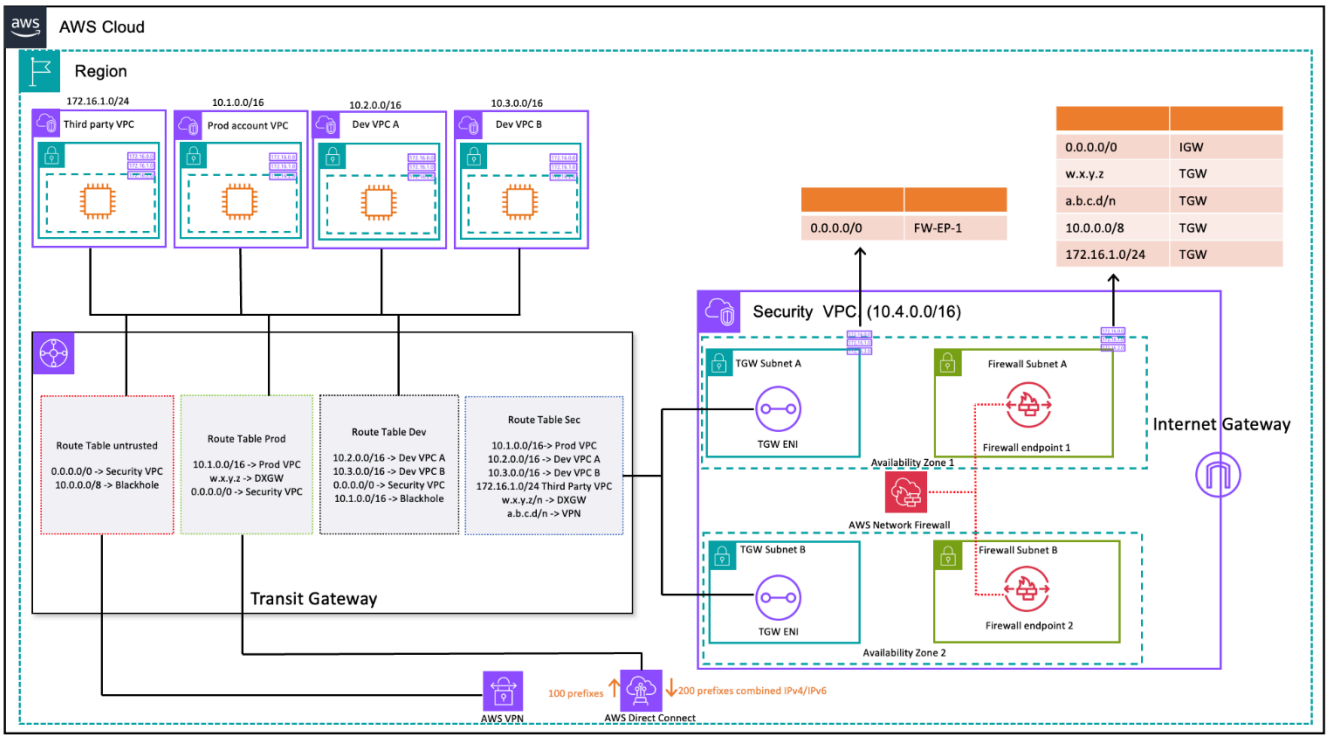
Considerações sobre o uso de um modelo centralizado de inspeção de segurança de rede

Para reduzir custos, você deve ser seletivo quanto ao tráfego que passa pelo seu Load Balancer AWS Network Firewall ou pelo Gateway Load Balancer. Uma forma de proceder é definir zonas de segurança e inspecionar o tráfego entre zonas não confiáveis. Uma zona não confiável pode ser um site remoto gerenciado por terceiros, uma VPC de fornecedor que você não controla/confia ou uma VPC de sandbox/desenvolvimento, que tem regras de segurança mais flexíveis em comparação com o resto do seu ambiente. Há quatro zonas neste exemplo:

- Zona não confiável — Isso é para qualquer tráfego proveniente da “VPN para um site remoto não confiável” ou do fornecedor terceirizado VPC.
- Zona de produção (produção) — contém tráfego da VPC de produção e do DC do cliente local.
- Zona de desenvolvimento (Dev) — contém o tráfego das duas VPCs de desenvolvimento.
- Zona de Segurança (Sec) — Contém nossos componentes de firewall Network Firewall ou Gateway Load Balancer.

Essa configuração tem quatro zonas de segurança, mas você pode ter mais. Você pode usar várias tabelas de rotas e rotas de buraco negro para obter isolamento de segurança e fluxo de tráfego ideal. A escolha do conjunto certo de zonas depende da sua estratégia geral de design da Zona de Aterrissagem (estrutura da conta, design de VPC). Você pode ter zonas para permitir o isolamento entre unidades de negócios (BUs), aplicativos, ambientes e assim por diante.

Se você quiser inspecionar e filtrar seu tráfego de VPC para VPC, tráfego entre zonas e tráfego de VPC no local, você pode incorporar o Transit Gateway em sua arquitetura centralizada. AWS Network Firewall Ao ter o hub-and-spoke modelo do AWS Transit Gateway, um modelo de implantação centralizado pode ser alcançado. O AWS Network Firewall é implantado em uma VPC de segurança separada. Uma VPC de segurança separada fornece uma abordagem simplificada e central para gerenciar a inspeção. Essa arquitetura VPC oferece visibilidade do IP AWS Network Firewall de origem e destino. Os IPs de origem e destino são preservados. Essa VPC de segurança consiste em duas sub-redes em cada zona de disponibilidade; em que uma sub-rede é dedicada à AWS Transit Gateway conexão e a outra é dedicada ao endpoint do firewall. As sub-redes nessa VPC devem conter apenas endpoints AWS Network Firewall porque o Network Firewall não pode inspecionar o tráfego nas mesmas sub-redes dos endpoints. Quando você usa o Network Firewall para inspecionar centralmente o tráfego, ele pode realizar uma inspeção profunda de pacotes (DPI) no tráfego de entrada. O padrão de DPI é expandido na seção Inspeção de entrada centralizada deste paper.



Inspeção de tráfego de VPC para VPC e local para VPC usando Transit Gateway e (design de tabela de rotas) AWS Network Firewall

Na arquitetura centralizada com inspeção, as sub-redes do Transit Gateway exigem uma tabela de rotas de VPC separada para garantir que o tráfego seja encaminhado para o endpoint do firewall dentro da mesma zona de disponibilidade. Para o tráfego de retorno, uma única tabela de rotas de VPC contendo uma rota padrão para o Transit Gateway é configurada. O tráfego é retornado para

AWS Transit Gateway a mesma zona de disponibilidade depois de ser inspecionado pelo AWS Network Firewall. Isso é possível devido ao recurso de modo de equipamento do Transit Gateway. O recurso de modo de dispositivo do Transit Gateway também ajuda a AWS Network Firewall ter uma capacidade de inspeção de tráfego monitorada dentro da VPC de segurança.

Com o modo de dispositivo ativado em um gateway de trânsito, ele seleciona uma única interface de rede usando o algoritmo de hash de fluxo durante toda a vida útil da conexão. O gateway de trânsito usa a mesma interface de rede para o tráfego de retorno. Isso garante que o tráfego bidirecional seja roteado simetricamente. Ele é roteado pela mesma zona de disponibilidade no anexo da VPC durante a vida útil do fluxo. Para obter mais informações sobre o modo de dispositivo, consulte Dispositivos com estado e modo de dispositivo na documentação da Amazon VPC.

Para diferentes opções de implantação de segurança VPC com AWS Network Firewall e Transit Gateway, consulte a postagem no blog Modelos de implantação para o AWS Network Firewall.

Usando o Gateway Load Balancer com o Transit Gateway para segurança de rede centralizada

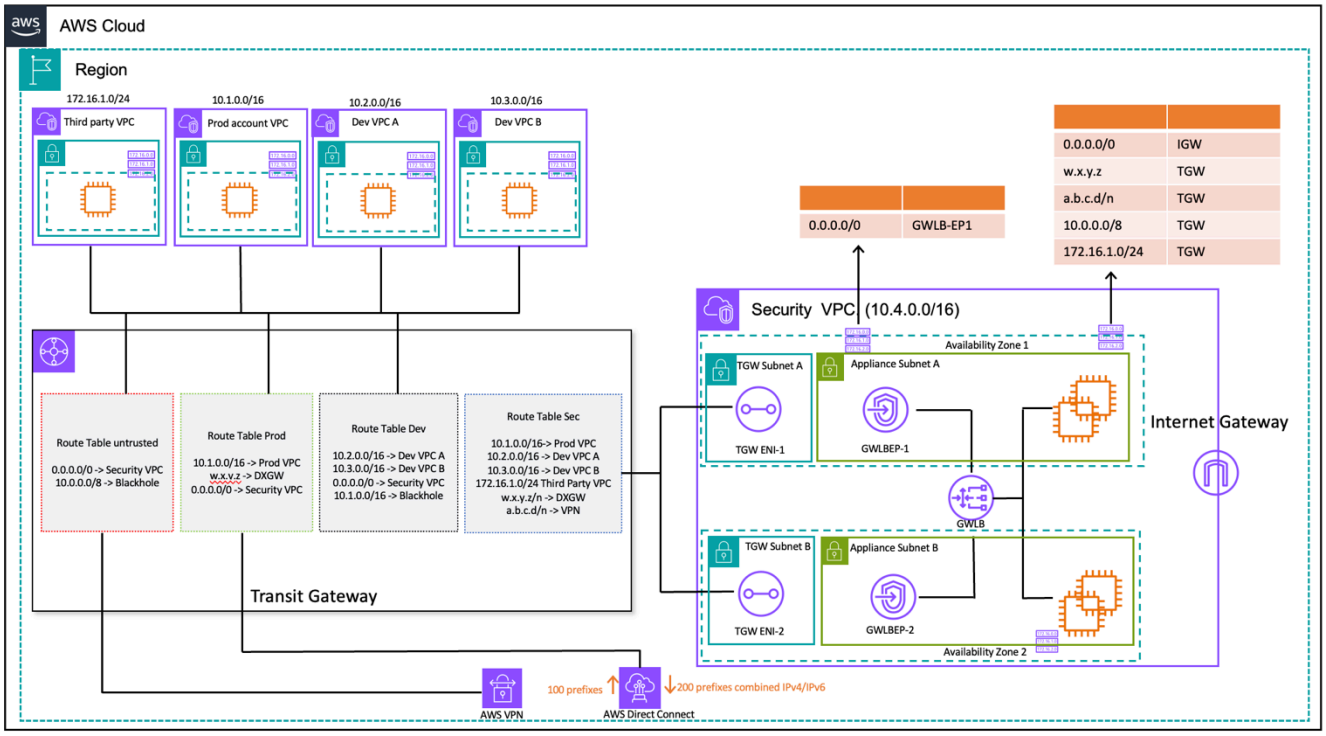
Muitas vezes, os clientes desejam incorporar dispositivos virtuais para lidar com a filtragem de tráfego e fornecer recursos de inspeção de segurança. Nesses casos de uso, eles podem integrar o Gateway Load Balancer, dispositivos virtuais e o Transit Gateway para implantar uma arquitetura centralizada para inspecionar o tráfego de VPC para VPC e VPC. to-on-premises

O Gateway Load Balancer é implantado em uma VPC de segurança separada junto com os dispositivos virtuais. Os dispositivos virtuais que inspecionarão o tráfego são configurados como destinos por trás do Gateway Load Balancer. Como os endpoints do Gateway Load Balancer são um destino roteável, os clientes podem rotear o tráfego que se move de e para o Transit Gateway para a frota de dispositivos virtuais. Para garantir a simetria do fluxo, o modo de dispositivo está ativado no Transit Gateway.

Cada VPC spoke tem uma tabela de rotas associada ao Transit Gateway, que tem a rota padrão para o anexo do Security VPC como próximo salto.

A VPC de segurança centralizada consiste em sub-redes de dispositivos em cada zona de disponibilidade; que têm os endpoints do Gateway Load Balancer e os dispositivos virtuais. Ele também tem sub-redes para anexos do Transit Gateway em cada zona de disponibilidade, conforme mostrado na figura a seguir.

Para obter mais informações sobre a inspeção de segurança centralizada com o Gateway Load Balancer e o Transit Gateway, consulte a Arquitetura de inspeção centralizada com o AWS Gateway Load Balancer e a postagem do blog. AWS Transit Gateway



on-premises-toInspeção de tráfego de VPC para VPC e -VPC usando Transit Gateway e AWS Gateway Load Balancer (design de tabela de rotas)

Principais considerações sobre o AWS Gateway Load Balancer AWS Network Firewall

- O modo de dispositivo deve ser ativado no Transit Gateway ao fazer a inspeção leste-oeste.
- Você pode implantar o mesmo modelo para inspeção de tráfego para outras pessoas Regiões da AWS usando o peering entre regiões do AWS Transit Gateway.
- Por padrão, cada Gateway Load Balancer implantado em uma zona de disponibilidade distribui o tráfego entre os destinos registrados somente na mesma zona de disponibilidade. Isso é chamado de afinidade da zona de disponibilidade. Se você habilitar o balanceamento de carga entre zonas, o Gateway Load Balancer distribuirá o tráfego entre todos os destinos registrados e íntegros em todas as zonas de disponibilidade habilitadas. Se todos os destinos em todas as zonas de disponibilidade não estiverem íntegros, o Gateway Load Balancer falhará ao abrir. Consulte a seção 4: Entenda os cenários de falha do equipamento e da zona de disponibilidade na postagem do blog Melhores práticas para implantar o Gateway Load Balancer para obter mais detalhes.

- Para implantação em várias regiões, AWS recomenda que você configure VPCs de inspeção separadas nas respectivas regiões locais para evitar dependências entre regiões e reduzir os custos associados à transferência de dados. Você deve inspecionar o tráfego na região local em vez de centralizar a inspeção em outra região.
- O custo de executar um par adicional de alta disponibilidade (HA) baseado em EC2 em implantações multirregionais pode aumentar. Para obter mais informações, consulte a postagem do blog sobre as melhores práticas para implantar o Gateway Load Balancer.

AWS Network Firewall versus Gateway Load Balancer

Tabela 2 — AWS Network Firewall versus Gateway Load Balancer

Critérios	AWS Network Firewall	Balanceador de carga de gateway
Caso de uso	Firewall de rede gerenciado e estável com capacidade de serviço de detecção e prevenção de intrusões compatível com o Suricata.	Serviço gerenciado que facilita a implantação, a escalabilidade e o gerenciamento de dispositivos virtuais de terceiros
Complexidade	AWS serviço gerenciado. AWS lida com a escalabilidade e a disponibilidade do serviço.	Serviço gerenciado da AWS. AWS cuidará da escalabilidade e disponibilidade do serviço Gateway Load Balancer. O cliente é responsável por gerenciar o dimensionamento e a disponibilidade dos dispositivos virtuais por trás do Gateway Load Balancer.
Escala	AWS Network Firewall os endpoints são alimentados por AWS PrivateLink. O Firewall de Rede suporta até 100	Os endpoints do Gateway Load Balancer suportam largura de banda máxima de até 100 Gbps por endpoint

Critérios	AWS Network Firewall	Balanceador de carga de gateway
	Gbps de tráfego de rede por endpoint de firewall.	
Custos	AWS Network Firewall custo do endpoint + Cobranças de processamento de dados	Gateway Load Balancer + endpoints do Gateway Load Balancer + dispositivos virtuais + taxas de processamento de dados

Inspeção de entrada centralizada

Os aplicativos voltados para a Internet, por sua natureza, têm uma superfície de ataque maior e estão expostos a categorias de ameaças que a maioria dos outros tipos de aplicativos não precisa enfrentar. Ter a proteção necessária contra ataques a esses tipos de aplicativos e minimizar a área de superfície de impacto são uma parte essencial de qualquer estratégia de segurança.

À medida que você implanta aplicativos em sua Landing Zone, muitos aplicativos serão acessados pelos usuários pela Internet pública (por exemplo, por meio de uma Rede de Distribuição de Conteúdo (CDN) ou por meio de um aplicativo web voltado para o público) por meio de um balanceador de carga voltado para o público, gateway de API ou diretamente por meio de um gateway de Internet. Nesse caso, você pode proteger suas cargas de trabalho e aplicativos usando o AWS Web Application Firewall (AWS WAF) para inspeção de aplicativos de entrada ou, alternativamente, inspeção de entrada de IDS/IPS usando o Gateway Load Balancer ou. AWS Network Firewall

À medida que você continua implantando aplicativos em sua Landing Zone, talvez seja necessário inspecionar o tráfego de entrada da Internet. Você pode conseguir isso de várias maneiras, usando arquiteturas de inspeção distribuídas, centralizadas ou combinadas usando o Gateway Load Balancer executando seus dispositivos de firewall de terceiros AWS Network Firewall ou com recursos avançados de DPI e IDS/IPS por meio do uso de regras Suricata de código aberto. Esta seção aborda o Gateway Load Balancer e AWS Network Firewall uma implantação centralizada, usando a AWS Transit Gateway atuação como um hub central para rotear o tráfego.

AWS WAF e AWS Firewall Manager para inspecionar o tráfego de entrada da Internet

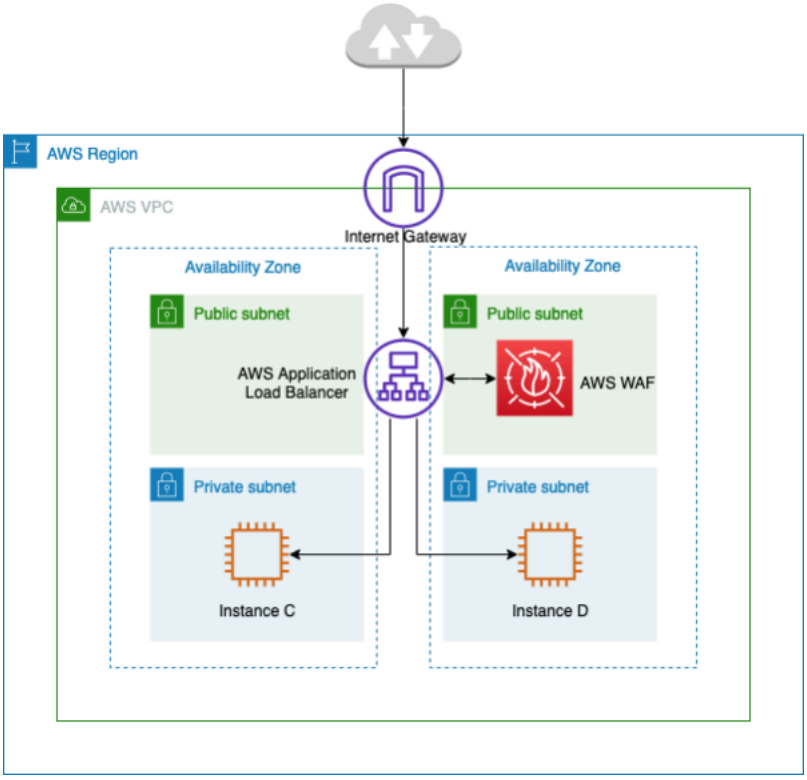
AWS WAF é um firewall de aplicativos da Web que ajuda a proteger seus aplicativos da Web ou APIs contra explorações e bots comuns da Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. AWS WAF oferece controle sobre como o tráfego chega aos seus aplicativos, permitindo que você crie regras de segurança que controlam o tráfego de bots e bloqueiam padrões de ataque comuns, como injeção de SQL ou cross-site scripting (XSS). Você também pode personalizar regras que filtram padrões de tráfego específicos.

Você pode implantar AWS WAF na Amazon CloudFront como parte de sua solução de CDN, o Application Load Balancer que está na frente de seus servidores web, o Amazon API Gateway para suas APIs REST ou AWS AppSync para suas APIs GraphQL.

Depois de implantar AWS WAF, você pode criar suas próprias regras de filtro de tráfego usando o criador visual de regras, código em JSON, regras gerenciadas mantidas por AWS, ou você pode assinar regras de terceiros a partir do AWS Marketplace. Essas regras podem filtrar o tráfego indesejado avaliando o tráfego em relação aos padrões especificados. Você também pode usar a Amazon CloudWatch para monitorar métricas de tráfego de entrada e registrar.

Para gerenciamento centralizado em todas as suas contas e aplicativos em AWS Organizations, você pode usar AWS Firewall Manager. AWS Firewall Manager é um serviço de gerenciamento de segurança que permite configurar e gerenciar centralmente as regras de firewall. À medida que seus novos aplicativos são criados, AWS Firewall Manager fica mais fácil colocar novos aplicativos e recursos em conformidade, aplicando um conjunto comum de regras de segurança.

Usando AWS Firewall Manager, você pode implantar facilmente AWS WAF regras para seus Application Load Balancers, instâncias do API Gateway e CloudFront distribuições da Amazon. AWS Firewall Manager se integra ao AWS Managed Rules for AWS WAF, o que oferece uma maneira fácil de implantar AWS WAF regras pré-configuradas e selecionadas em seus aplicativos. Para obter mais informações sobre o gerenciamento centralizado AWS WAF com AWS Firewall Manager, consulte Gerenciar centralmente AWS WAF (API v2) e AWS Managed Rules em escala com. AWS Firewall Manager



Inspeção centralizada de tráfego de entrada usando AWS WAF

Na arquitetura anterior, os aplicativos são executados em instâncias do Amazon EC2 em várias zonas de disponibilidade nas sub-redes privadas. Há um Application Load Balancer (ALB) voltado para o público implantado na frente das instâncias do Amazon EC2, balanceando a carga das solicitações entre destinos diferentes. O AWS WAF está associado ao ALB.

Vantagens

- Com o AWS WAF Bot Control, você obtém visibilidade e controle sobre o tráfego comum e generalizado de bots em seus aplicativos.
- Com o Managed Rules for AWS WAF, você pode começar rapidamente e proteger seu aplicativo web ou APIs contra ameaças comuns. Você pode escolher entre vários tipos de regras, como aquelas que abordam questões como os 10 principais riscos de segurança do Open Web Application Security Project (OWASP), ameaças específicas a sistemas de gerenciamento de conteúdo (CMS), como o Joomla, WordPress ou até mesmo vulnerabilidades e exposições comuns emergentes (CVE). As regras gerenciadas são atualizadas automaticamente à medida que surgem novos problemas, para que você possa passar mais tempo criando aplicativos.
- AWS WAF é um serviço gerenciado e nenhum dispositivo é necessário para inspeção nessa arquitetura. Além disso, ele fornece registros quase em tempo real por meio do Amazon Data Firehose. AWS WAF oferece visibilidade quase em tempo real do seu tráfego na web, que você pode usar para criar novas regras ou alertas na Amazon. CloudWatch

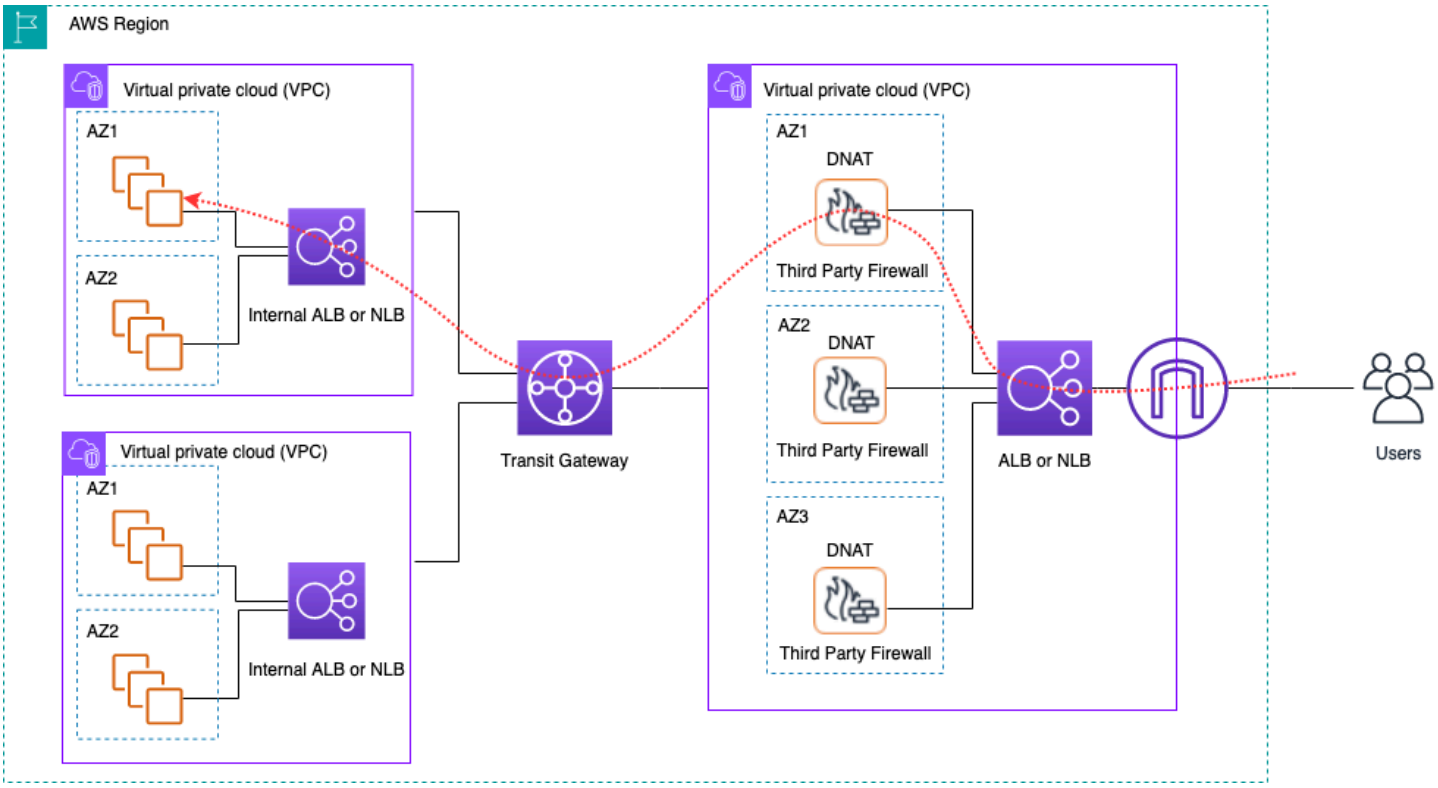
Considerações importantes

- Essa arquitetura é mais adequada para inspeção de cabeçalhos HTTP e inspeções distribuídas, pois AWS WAF está integrada em um gateway por ALB, CloudFront distribuição e API. AWS WAF não registra o corpo da solicitação.
- O tráfego que vai para um segundo conjunto de ALB (se presente) pode não ser inspecionado pela mesma AWS WAF instância; porque uma nova solicitação seria feita para o segundo conjunto de ALB.

Inspeção de entrada centralizada com dispositivos de terceiros

Nesse padrão de projeto arquitetônico, você implanta dispositivos de firewall de terceiros no Amazon EC2 em várias zonas de disponibilidade por trás de um Elastic Load Balancer (ELB), como um Application/Network Load Balancer em uma VPC de inspeção separada.

A VPC de inspeção e outras VPCs Spoke são conectadas por meio de um Transit Gateway como anexos de VPC. Os aplicativos nas VPCs Spoke são front-end por um ELB interno, que pode ser ALB ou NLB, dependendo do tipo de aplicativo. Os clientes pela Internet se conectam ao DNS do ELB externo na VPC de inspeção, que roteia o tráfego para um dos dispositivos de firewall. O Firewall inspeciona o tráfego e, em seguida, roteia o tráfego para o Spoke VPC por meio do Transit Gateway usando o DNS do ELB interno, conforme mostrado na figura a seguir. Para obter mais informações sobre a inspeção de segurança de entrada com dispositivos de terceiros, consulte a postagem do blog Como integrar dispositivos de firewall de terceiros em um ambiente da AWS.



Inspeção centralizada de tráfego de entrada usando dispositivos de terceiros e ELB

Vantagens

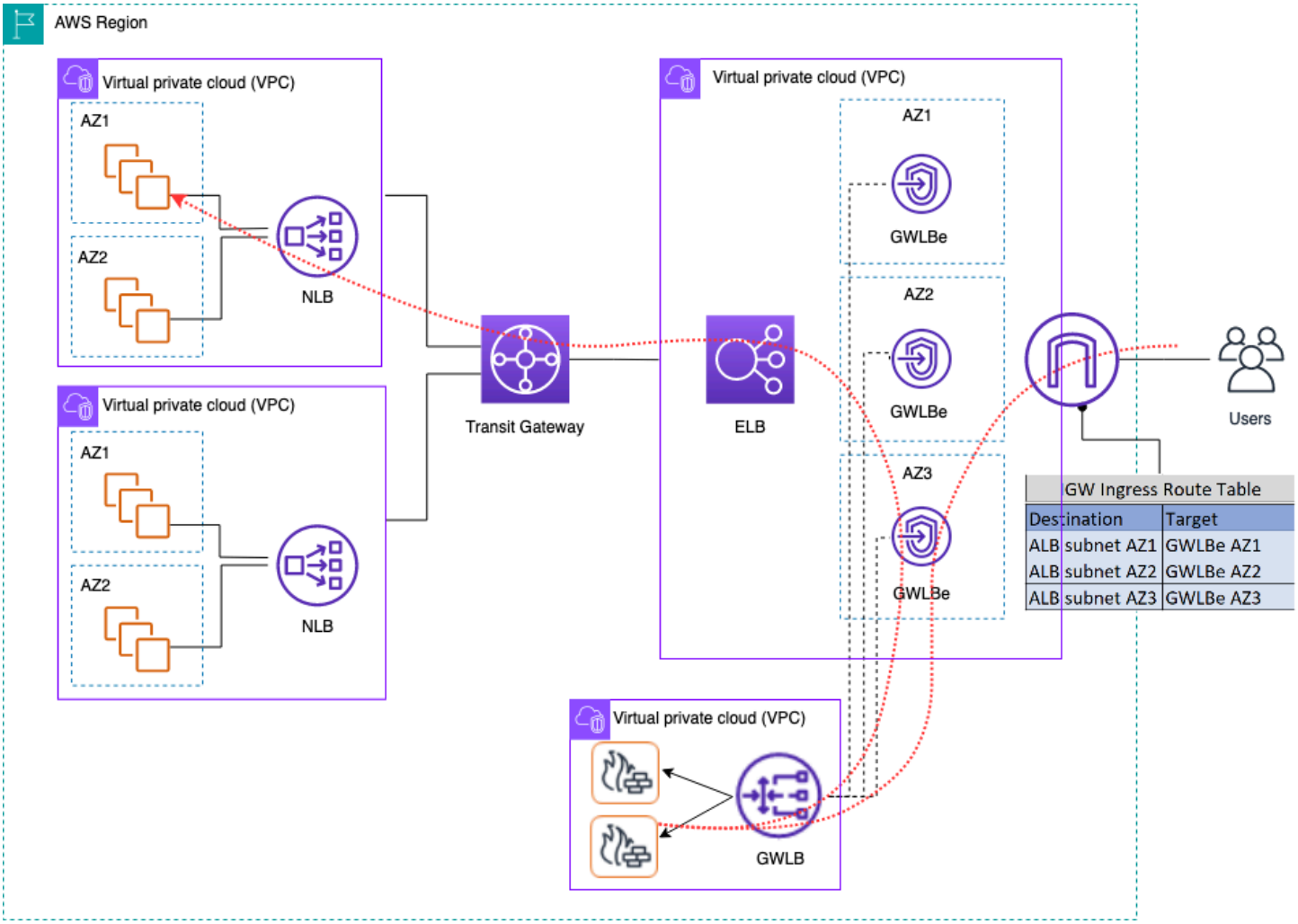
- Essa arquitetura pode suportar qualquer tipo de aplicativo para inspeção e recursos avançados de inspeção oferecidos por meio de dispositivos de firewall de terceiros.
- Esse padrão oferece suporte ao roteamento baseado em DNS de dispositivos de firewall para VPCs spoke, o que permite que os aplicativos em Spoke VPCs sejam escalados independentemente de um ELB.
- Você pode usar o Auto Scaling com o ELB para escalar os dispositivos de firewall na VPC de inspeção.

Considerações importantes

- Você precisa implantar vários dispositivos de firewall nas zonas de disponibilidade para obter alta disponibilidade.
- O firewall precisa ser configurado e executar o NAT de origem para manter a simetria do fluxo, o que significa que o endereço IP do cliente não estará visível para o aplicativo.
- Considere implantar o Transit Gateway e o Inspection VPC na conta de Serviços de Rede.
- Custo adicional de licenciamento/suporte de firewall de um fornecedor terceirizado. As cobranças do Amazon EC2 dependem do tipo de instância.

Inspecionando o tráfego de entrada da Internet usando dispositivos de firewall com o Gateway Load Balancer

Os clientes usam firewalls de próxima geração (NGFW) e sistemas de prevenção de intrusões (IPS) de terceiros como parte de sua estratégia de defesa em profundidade. Tradicionalmente, eles geralmente são hardware ou software/dispositivos virtuais dedicados. Você pode usar o Gateway Load Balancer para escalar esses dispositivos virtuais horizontalmente para inspecionar o tráfego de e para sua VPC, conforme mostrado na figura a seguir.



Inspeção centralizada de tráfego de entrada usando dispositivos de firewall com Gateway Load Balancer

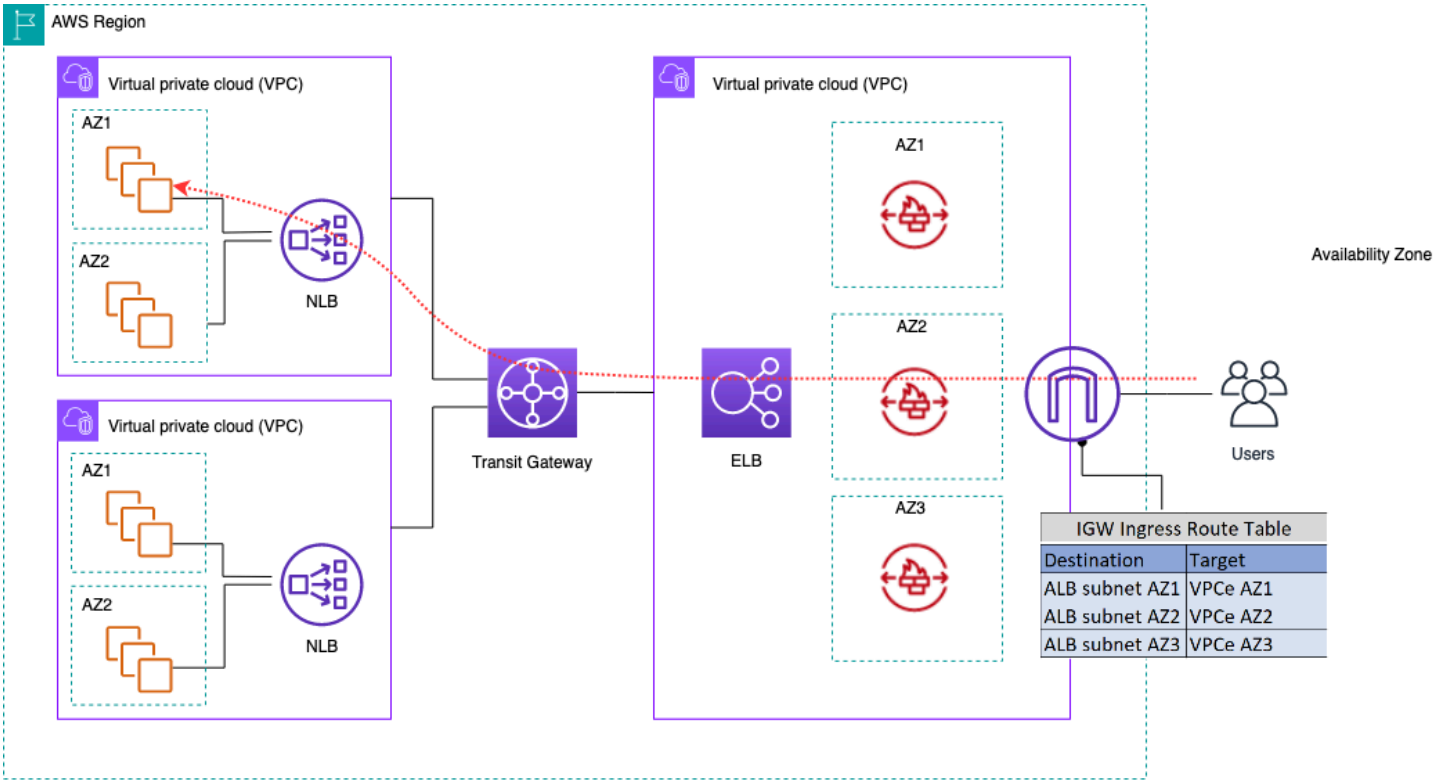
Na arquitetura anterior, os endpoints do Gateway Load Balancer são implantados em cada zona de disponibilidade em uma VPC de borda separada. Os firewalls de próxima geração, os sistemas de prevenção de intrusões etc. são implantados por trás do Gateway Load Balancer na VPC do dispositivo centralizado. Essa VPC do dispositivo pode estar na mesma conta da AWS que as VPCs spoke ou em uma conta diferente da AWS. Os dispositivos virtuais podem ser configurados para usar grupos de Auto Scaling e são registrados automaticamente no Gateway Load Balancer, permitindo o escalonamento automático da camada de segurança.

Esses dispositivos virtuais podem ser gerenciados acessando suas interfaces de gerenciamento por meio de um Internet Gateway (IGW) ou usando uma configuração de bastion host na VPC do appliance.

Usando o recurso de roteamento de entrada da VPC, a tabela de rotas de borda é atualizada para rotear o tráfego de entrada da Internet para os dispositivos de firewall por trás do Gateway Load Balancer. O tráfego inspecionado é roteado por meio de endpoints do Gateway Load Balancer para a instância VPC de destino. Consulte a postagem do blog Introducing AWS Gateway Load Balancer: Supported architecture patterns para obter detalhes sobre várias maneiras de usar o Gateway Load Balancer.

Usando o AWS Network Firewall para entrada centralizada

Nessa arquitetura, o tráfego de entrada é inspecionado AWS Network Firewall antes de chegar ao resto das VPCs. Nessa configuração, o tráfego é dividido entre todos os endpoints de firewall implantados no Edge VPC. Você implanta uma sub-rede pública entre o endpoint do firewall e a sub-rede do Transit Gateway. Você pode usar um ALB ou NLB, que contém destinos IP em suas VPCs spoke e, ao mesmo tempo, manipula o Auto Scaling para alvos por trás delas.



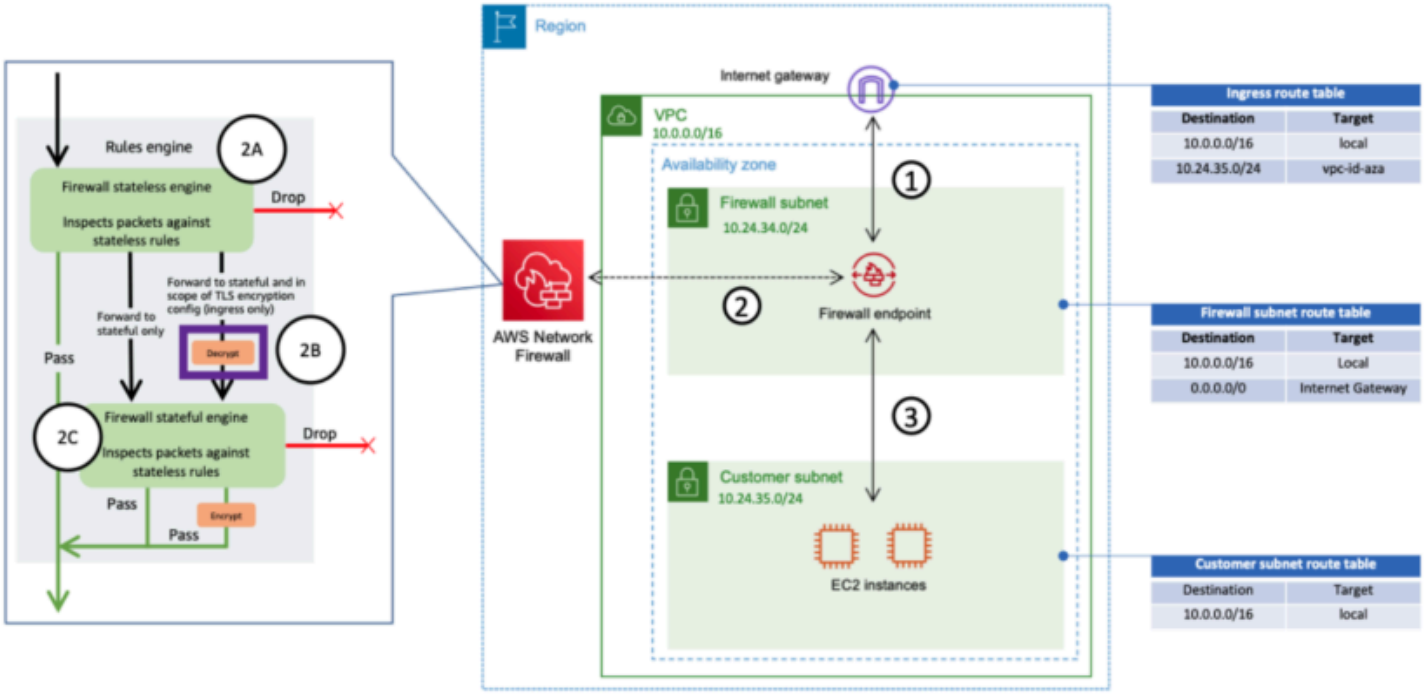
Inspeção de tráfego de entrada usando o AWS Network Firewall

Para simplificar a implantação e o gerenciamento deste AWS Network Firewall modelo, AWS Firewall Manager pode ser usado. O Firewall Manager permite que você administre centralmente seus diferentes firewalls aplicando automaticamente a proteção criada no local centralizado a várias contas. O Firewall Manager oferece suporte a modelos de implantação distribuídos e centralizados

para o Firewall de Rede. A postagem do blog Como implantar AWS Network Firewall usando AWS Firewall Manager fornece mais detalhes sobre o modelo.

Inspeção profunda de pacotes (DPI) com AWS Network Firewall

O Network Firewall pode realizar uma inspeção profunda de pacotes (DPI) no tráfego de entrada. Usando um certificado TLS (Transport Layer Security) armazenado no AWS Certificate Manager (ACM), o Network Firewall pode descriptografar pacotes, executar DPI e recriptografar pacotes. Há algumas considerações para configurar o DPI com um firewall de rede. Primeiro, um certificado TLS confiável deve ser armazenado no ACM. Em segundo lugar, as regras do Firewall de Rede devem ser configuradas para enviar pacotes corretamente para decodificação e recriptografia. Consulte a postagem do blog Configuração de inspeção TLS para tráfego criptografado e AWS Network Firewall para obter mais detalhes.



Inspeção de tráfego de entrada usando o Network Firewall com DPI

Principais considerações AWS Network Firewall em uma arquitetura de entrada centralizada

- O Elastic Load Balancing no Edge VPC só pode ter endereços IP como tipos de destino, não um nome de host. Na figura anterior, os alvos são os IPs privados do Network Load Balancer em VPCs de fala. Usar alvos IP por trás do ELB na VPC de borda resulta na perda do Auto Scaling.

- Considere o uso AWS Firewall Manager como um único painel de vidro para seus endpoints de firewall.
- Esse modelo de implantação usa a inspeção de tráfego logo que entra na VPC de borda, portanto, tem o potencial de reduzir o custo geral de sua arquitetura de inspeção.

DNS

Quando você executa uma instância em uma VPC, excluindo a VPC padrão, AWS fornece à instância um nome de host DNS privado (e potencialmente um nome de host DNS público), dependendo dos atributos de DNS que você especifica para a VPC e se sua instância tem um endereço IPv4 público. Quando o `enableDnsSupport` atributo é definido como`true`, você obtém uma resolução de DNS dentro da VPC do Route 53 Resolver (+2 de deslocamento de IP para o CIDR da VPC). Por padrão, o Route 53 Resolver responde a consultas de DNS para nomes de domínio VPC, como nomes de domínio para instâncias do EC2 ou balanceadores de carga do Elastic Load Balancing. Com o emparelhamento de VPC, os hosts em uma VPC podem transformar nomes de host DNS públicos em endereços IP privados para instâncias em VPCs emparelhadas, desde que a opção de fazer isso esteja habilitada. O mesmo se aplica às VPCs conectadas via AWS Transit Gateway. Para obter mais informações, consulte Habilitando o DNS Resolution Support para uma conexão de emparelhamento de VPC.

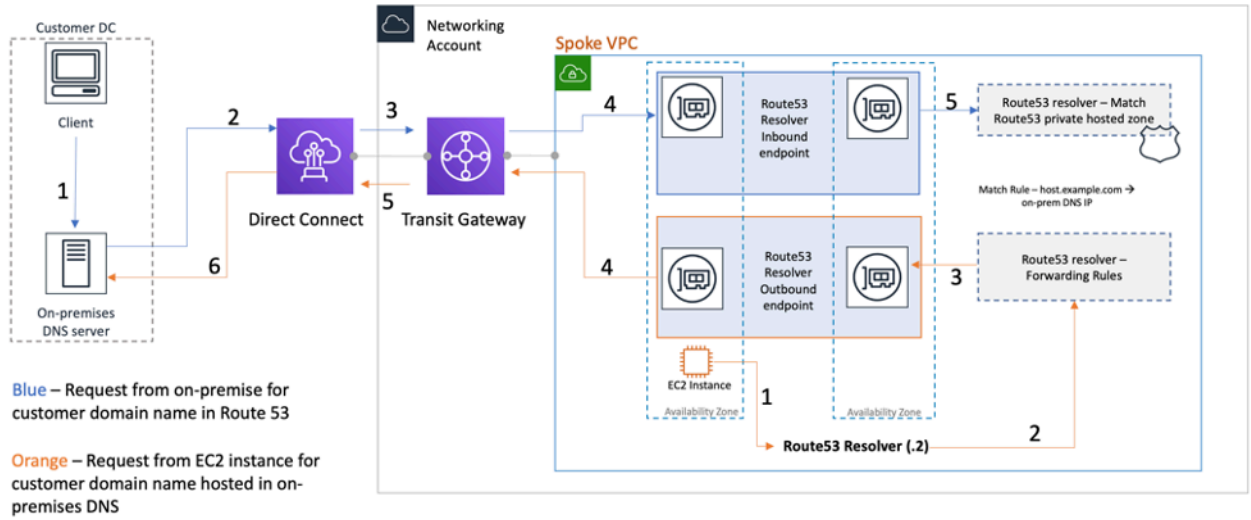
Se você quiser mapear suas instâncias para um nome de domínio personalizado, você pode usar o Amazon Route 53 para criar um registro personalizado de mapeamento de DNS para IP. Uma zona hospedada do Amazon Route 53 é um contêiner que contém informações sobre como você deseja que o Amazon Route 53 responda às consultas de DNS para um domínio e seus 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 informações apenas às VPCs que foram anexadas à zona hospedada privada específica. Em uma configuração de Landing Zone em que você tem várias VPCs ou contas, você pode associar uma única zona hospedada privada a várias VPCs nas contas da AWS e em todas as regiões (possível somente com SDK/CLI/API). Os hosts finais nas VPCs usam seu respectivo IP do Resolvedor Route 53 (+2 compensam o CIDR da VPC) como servidor de nomes para consultas de DNS. O resolvedor do Route 53 na VPC aceita consultas de DNS somente de recursos dentro de uma VPC.

DNS híbrido

O DNS é um componente essencial de qualquer infraestrutura, híbrida ou não, pois fornece a resolução do nome do host para o endereço IP da qual os aplicativos dependem. 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. O resolvedor nativo do Route 53 (+2% do VPC CIDR básico) não pode ser acessado por redes locais usando VPN ou. AWS Direct Connect Portanto, ao integrar o DNS para as VPCs em uma região da AWS com o DNS para

sua rede, você precisa de um endpoint de entrada do Route 53 Resolver (para consultas de DNS que você está encaminhando para suas VPCs) e um endpoint de saída do Route 53 Resolver (para consultas que você está encaminhando de suas VPCs para sua rede).

Conforme mostrado na figura a seguir, você pode configurar endpoints de saída do Resolver para encaminhar as consultas que ele recebe das instâncias do Amazon EC2 em suas VPCs para servidores DNS em sua rede. Para encaminhar consultas selecionadas, de uma VPC para uma rede local, crie regras do Route 53 Resolver que especifiquem os nomes de domínio das consultas DNS que você deseja encaminhar (como exemplo.com) e os endereços IP dos resolvedores de DNS na sua rede para a qual você deseja encaminhar as consultas. Para consultas de entrada de redes locais para zonas hospedadas do Route 53, os servidores DNS em sua rede podem encaminhar consultas para endpoints de Resolver de entrada em uma VPC especificada.

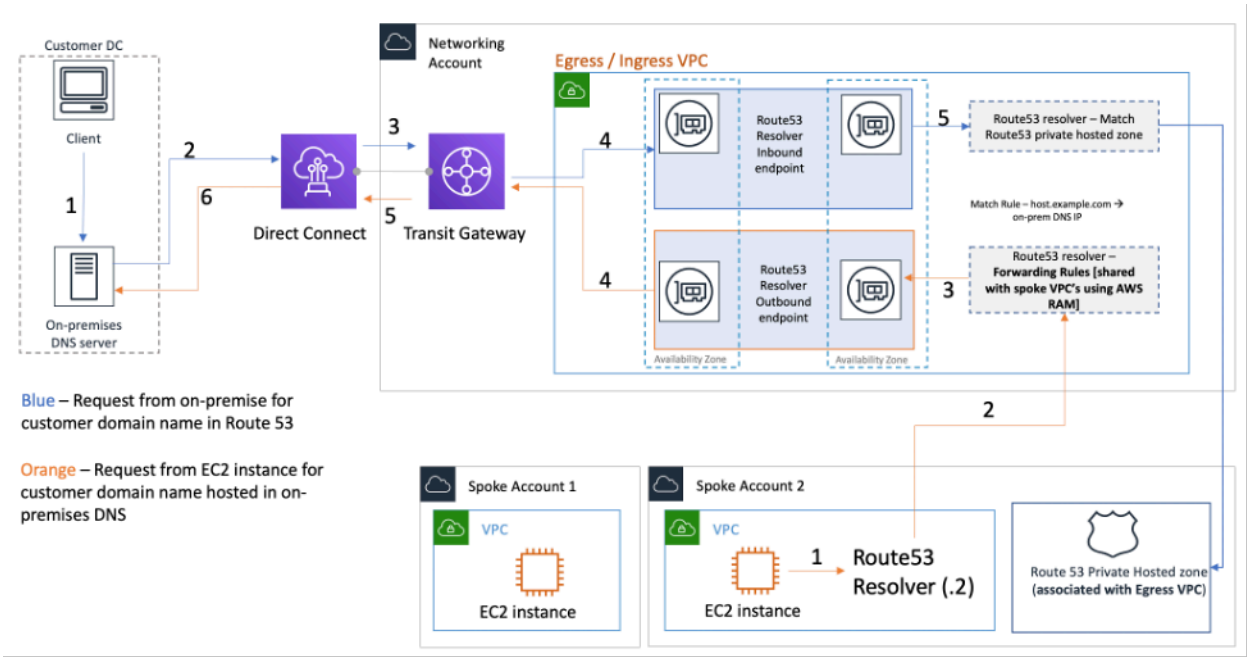


Resolução de DNS híbrida usando o Route 53 Resolver

Isso permite que seus resolvedores de DNS locais resolvam facilmente nomes de domínio para recursos da AWS, como instâncias do Amazon EC2 ou registros em uma zona hospedada privada do Route 53 associada a essa VPC. Além disso, os endpoints do Route 53 Resolver podem lidar com até aproximadamente 10.000 consultas por segundo por ENI, portanto, podem ser escalados facilmente para um volume de consultas de DNS muito maior. Consulte as melhores práticas para o Resolver na documentação do Amazon Route 53 para obter mais detalhes.

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

- Resolução de saída — Use a conta de Serviços de Rede para escrever regras de resolução (com base nas consultas de DNS que serão encaminhadas para servidores DNS locais). Usando o Resource Access Manager (RAM), compartilhe essas regras do Route 53 Resolver com várias contas (e associe às VPCs nas contas). As instâncias EC2 em VPCs spoke podem enviar consultas DNS para o Route 53 Resolver e o Route 53 Resolver Service encaminhará essas consultas para o servidor DNS local por meio dos endpoints de saída do Route 53 Resolver na VPC de saída. Você não precisa conectar VPCs via peer spoke à VPC de saída nem conectá-las via 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) em sua VPC.



Centralizando os endpoints do Route 53 Resolver na VPC de entrada/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 Landing Zone a essa VPC centralizada. Para obter mais informações, consulte Associando mais VPCs a uma zona hospedada privada. Várias zonas hospedadas privadas (PHZ) associadas a uma VPC não podem se sobrepor. Conforme mostrado na figura anterior, essa associação do PHZ com a VPC centralizada permitirá que os servidores locais 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 as opções de DNS da nuvem híbrida para Amazon VPC.

Firewall DNS do Route 53

Amazon Route 53 Resolver O DNS Firewall ajuda a filtrar e regular o tráfego DNS de saída para suas VPCs. O principal uso do Firewall DNS é ajudar a evitar a exfiltração de dados de seus dados, definindo listas de permissão de nomes de domínio que permitem que os recursos em sua VPC façam solicitações de DNS de saída somente para os sites em que sua organização confia. Também oferece aos clientes a capacidade de criar listas de bloqueio para domínios com os quais eles não querem que os recursos dentro de uma VPC se comuniquem via DNS. Amazon Route 53 Resolver O firewall DNS tem os seguintes recursos:

Os clientes podem criar regras para definir como as consultas de DNS são respondidas. As ações que podem ser definidas para os nomes de domínio incluem `NODATA` `OVERRIDE` `NXDOMAIN` e.

Os clientes podem criar alertas tanto para listas de permissão quanto para listas de negação para monitorar a atividade da regra. Isso pode ser útil quando os clientes querem testar a regra antes de colocá-la em produção.

Para obter mais informações, consulte a postagem do blog Como começar a usar o firewall Amazon Route 53 Resolver DNS para Amazon VPC.

Acesso centralizado aos endpoints privados da VPC

Um VPC endpoint permite que você conecte sua VPC de forma privada aos serviços compatíveis da AWS sem exigir um gateway de internet ou um dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect Portanto, sua VPC não é exposta à internet pública. As instâncias em sua VPC não exigem endereços IP públicos para se comunicar com os endpoints de serviço da AWS com esse endpoint de interface. O tráfego entre sua VPC e outros serviços não sai do backbone da rede AWS. Os VPC endpoints são dispositivos virtuais. Eles são componentes de VPC escalados horizontalmente, redundantes e altamente disponíveis. Atualmente, dois tipos de endpoints podem ser provisionados: endpoints de interface (alimentados por AWS PrivateLink) e endpoints de gateway. Os endpoints do gateway podem ser utilizados para acessar os serviços Amazon S3 e Amazon DynamoDB de forma privada. Não há cobrança adicional pelo uso de endpoints do gateway. Aplicam-se as cobranças padrão pela transferência de dados e pela utilização de recursos.

Endpoints da VPC de interface

Um endpoint de interface consiste em uma ou mais interfaces de rede elásticas com um endereço IP privado que serve como ponto de entrada para o tráfego destinado a um serviço compatível AWS . Quando você provisiona um endpoint de interface, um custo é incorrido por cada hora em que o endpoint está funcionando junto com as cobranças de processamento de dados. Por padrão, você cria um endpoint de interface em cada VPC a partir da qual deseja acessar AWS o serviço. Isso pode ter um custo proibitivo e desafiador de gerenciar na configuração da Landing Zone, em que um cliente deseja interagir com um serviço específico da AWS em várias VPCs. Para evitar isso, você pode hospedar os endpoints da interface em uma VPC centralizada. Todas as VPCs spoke usarão esses endpoints centralizados via Transit Gateway.

Ao criar um VPC endpoint para um AWS serviço, você pode ativar o DNS privado. Quando ativada, a configuração cria uma zona hospedada privada (PHZ) do Route 53 gerenciada pela AWS que permite a resolução do endpoint de AWS serviço público para o IP privado do endpoint da interface. O PHZ gerenciado só funciona dentro da VPC com o endpoint de interface. Em nossa configuração, quando queremos que as VPCs spoke sejam capazes de resolver o DNS do VPC endpoint hospedado em uma VPC centralizada, o PHZ gerenciado não funcionará. Para superar isso, desative a opção que cria automaticamente o DNS privado quando um endpoint de interface é criado. Em seguida, crie manualmente um PHZ do Route 53 e adicione um registro Alias com o nome completo do endpoint do serviço AWS apontando para o endpoint da interface.

1. Faça login no console e navegue até o serviço Route 53.

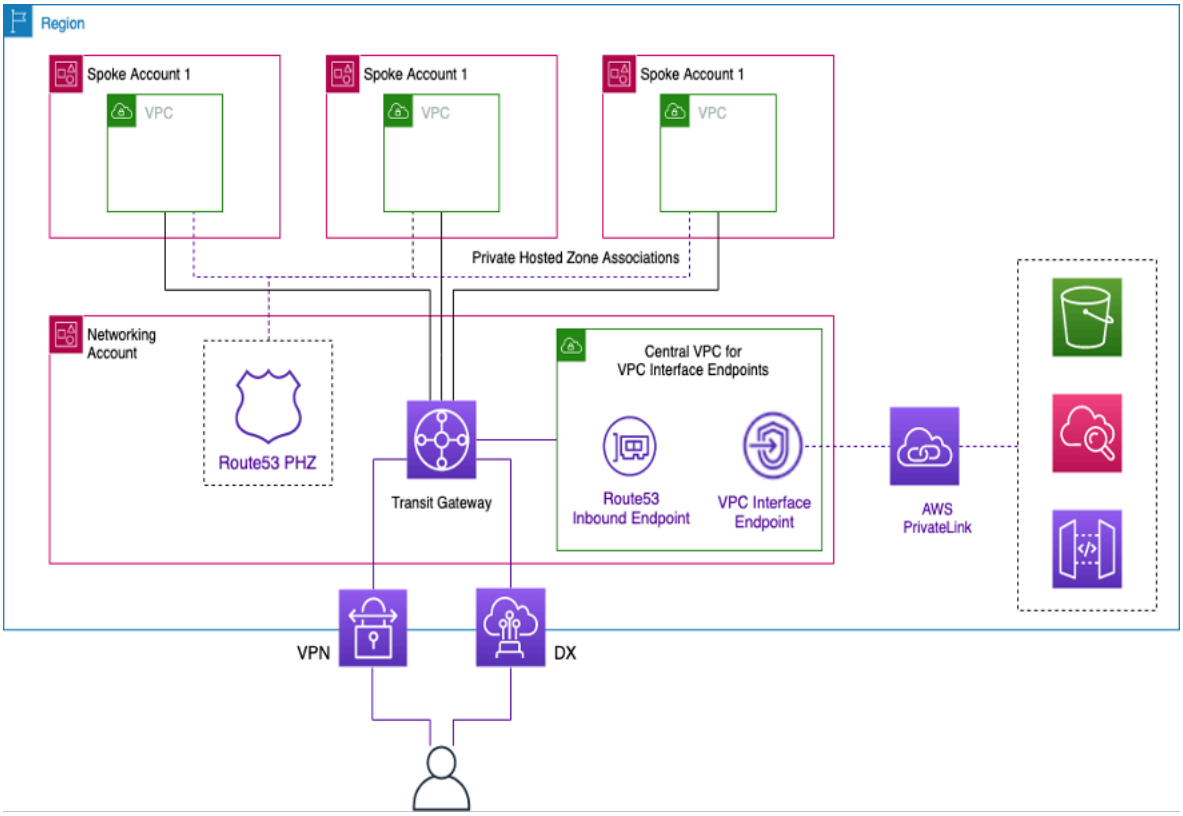
2. Selecione a Zona Hospedada Privada e navegue até Criar registro.
3. Preencha o campo Nome do registro, selecione Tipo de registro como A e ative o Alias.
4. Na seção Rotear tráfego para, selecione o serviço para o qual o tráfego deve ser enviado e selecione a região na lista suspensa.
5. Selecione a política de roteamento apropriada e assegure-se de habilitar a opção Avaliar a integridade do alvo.

Você associa essa zona hospedada privada a outras VPCs dentro da Landing Zone. Essa configuração permite que as VPCs spoke resolvam os nomes dos endpoints de serviço completo para fazer interface com os endpoints na VPC centralizada.

> **Note**
>
> Para acessar a zona hospedada privada compartilhada, os hosts nas VPCs spoke devem usar o IP do Resolvedor Route 53 de sua VPC. Os endpoints de interface também podem ser acessados a partir de redes locais via VPN e Direct Connect. Use regras de encaminhamento condicional para enviar todo o tráfego DNS dos nomes de endpoints de serviço completo para os endpoints de entrada do Route 53 Resolver, que resolverão as solicitações de DNS de acordo com a zona hospedada privada.

Na figura a seguir, o Transit Gateway permite o fluxo de tráfego das VPCs spoke para os endpoints da interface centralizada. Crie VPC Endpoints e a zona hospedada privada para eles na Conta de Serviços de Rede e compartilhe-os com VPCs spoke nas contas spoke. Para obter mais detalhes sobre o compartilhamento de informações de endpoints com outras VPCs, consulte a postagem do blog Integrating AWS Transit Gateway with and AWS PrivateLink Amazon Route 53 Resolver.

> **Note**
>
> Uma abordagem de endpoint de VPC distribuído, ou seja, um endpoint por VPC, permite que você aplique políticas de privilégios mínimos em endpoints de VPC. Em uma abordagem centralizada, você aplicará e gerenciará políticas para todos os acessos VPC do Spoke em um único endpoint. Com o aumento do número de VPCs, a complexidade de manter o mínimo de privilégios com um único documento de política pode aumentar. Um único documento de política também resulta em um raio de explosão maior. Você também está restrito quanto ao tamanho do documento de política (20.480 caracteres).



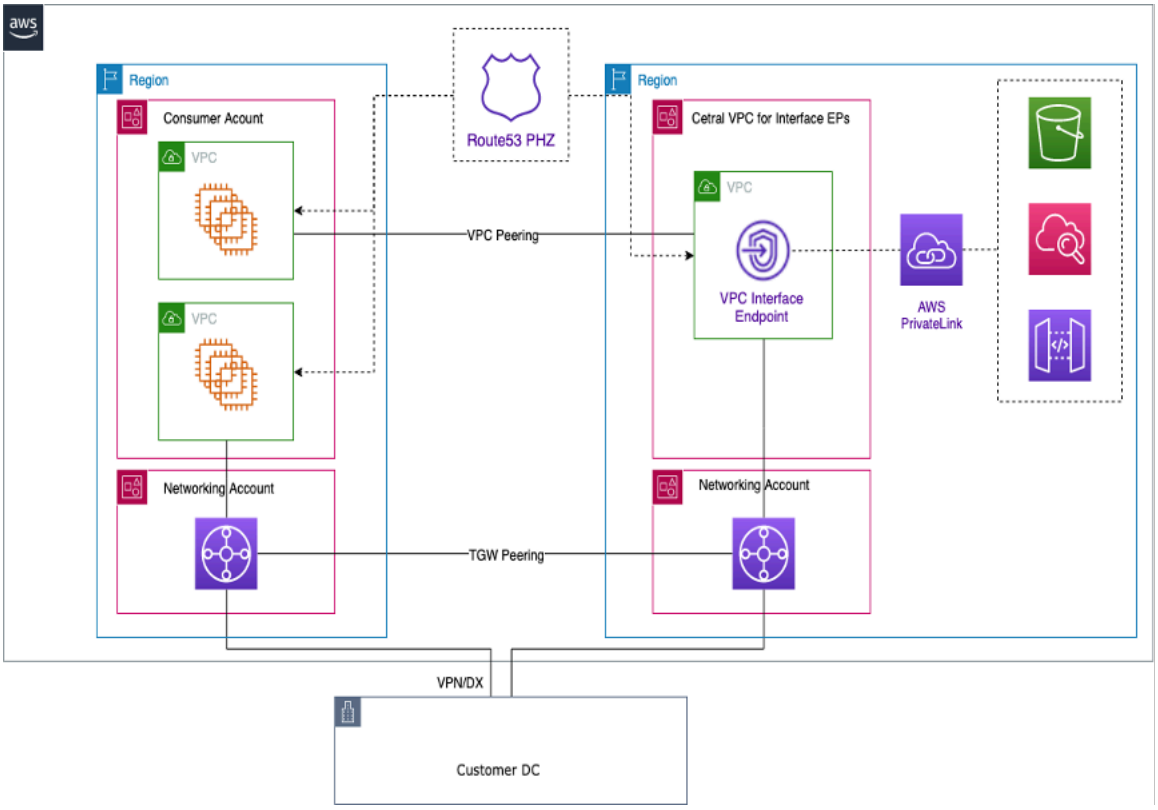
Interface centralizadora de VPC endpoints

Acesso a endpoints entre regiões

Quando você quiser configurar várias VPCs em diferentes regiões que compartilhem um VPC endpoint comum, use um PHZ, conforme descrito anteriormente. As duas VPCs em cada região serão associadas ao PHZ com o alias do endpoint. Para rotear o tráfego entre VPCs em uma arquitetura multirregional, os gateways de trânsito em cada região precisam ser interligados. Para obter mais informações, consulte este blog: Usando zonas hospedadas privadas do Route 53 para arquiteturas multirregionais entre contas.

VPCs de diferentes regiões podem ser roteadas entre si usando Transit Gateways ou VPC Peering. Use a seguinte documentação para emparelhar os Transit Gateways: Transit Gateway peering attachments.

Neste exemplo, a instância do Amazon EC2 na região VPC usará o PHZ para obter o endereço IP privado do endpoint na `us-west-1` região e rotear o tráfego para a `us-west-2` região VPC por meio do peering do Transit Gateway ou do `us-west-2` VPC peering. Usando essa arquitetura, o tráfego permanece na rede da AWS, permitindo com segurança que a instância do EC2 `us-west-1` acesse o serviço VPC `us-west-2` sem passar pela Internet.



Endpoints VPC multirregionais

> **Note**
>
> As taxas de transferência de dados entre regiões se aplicam ao acessar endpoints em todas as regiões.

Com referência à figura anterior, um serviço de endpoint é criado em uma VPC na `us-west-2` região. Esse serviço de endpoint fornece acesso a um serviço da AWS nessa região. Para que suas instâncias em outra região (como`us-east-1`) acessem o endpoint na `us-west-2` região, você precisa criar um registro de endereço no PHZ com um alias para o VPC endpoint desejado.

Primeiro, certifique-se de que as VPCs em cada região estejam associadas à PHZ que você criou.

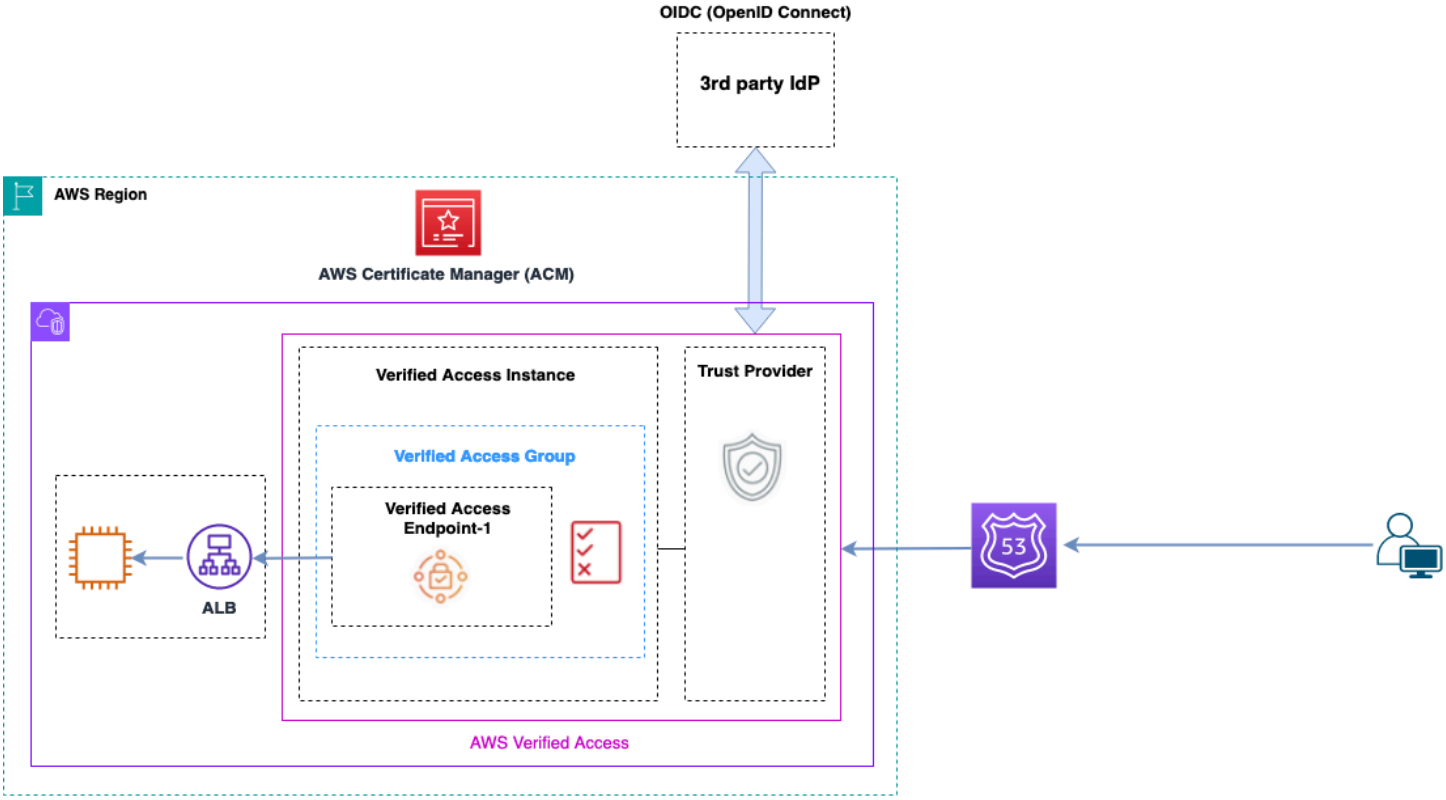
Ao implantar um endpoint em várias zonas de disponibilidade, o endereço IP do endpoint retornado do DNS será de qualquer uma das sub-redes alocadas na zona de disponibilidade.

Ao invocar o endpoint, use o nome de domínio totalmente qualificado (FQDN) que está no PHZ.

Acesso Verificado pela AWS

Acesso Verificado pela AWS fornece acesso seguro a aplicativos em rede privada sem uma VPN. Ele avalia as solicitações em tempo real, como identidade, dispositivo e localização. Esse serviço concede acesso com base na política para aplicativos e conecta os usuários, melhorando a segurança da organização. O Acesso Verificado fornece acesso a aplicativos privados atuando como um proxy reverso com reconhecimento de identidade. A identidade do usuário e a integridade do dispositivo, se aplicável, são executadas antes de rotear o tráfego para o aplicativo.

O seguinte diagrama fornece uma visão geral de alto nível sobre como o Acesso Verificado funciona. Os usuários enviam solicitações para acessar um aplicativo. O Acesso Verificado avalia a solicitação em relação à política de acesso do grupo e a qualquer política de endpoint específica do aplicativo. Se o acesso for permitido, a solicitação será enviada para o aplicativo por meio do endpoint.



Visão geral do acesso verificado

Os principais componentes de uma Acesso Verificado pela AWS arquitetura são:

- Instâncias de Acesso Verificado: uma instância avalia as solicitações de aplicativos e concede acesso somente quando seus requisitos de segurança são atendidos.

- Endpoints de Acesso Verificado: cada endpoint representa um aplicativo. Um endpoint pode ser NLB, ALB ou interface de rede.
- Grupo de Acesso Verificado: uma coleção de endpoints de Acesso Verificado. Recomendamos que você agrupe os endpoints para aplicativos com requisitos de segurança semelhantes para simplificar a administração de políticas.
- Políticas de acesso: um conjunto de regras definidas pelo usuário que determinam se o acesso a um aplicativo deve ser permitido ou negado.
- Provedores de confiança — O Acesso Verificado é um serviço que facilita o gerenciamento das identidades dos usuários e dos estados de segurança do dispositivo. É compatível com provedores confiáveis AWS e terceirizados, exigindo que pelo menos um provedor de confiança seja anexado a cada instância de acesso verificado. Cada uma dessas instâncias pode incluir um único provedor de confiança de identidade, bem como vários provedores de confiança de dispositivos.
- Dados confiáveis — Os dados de segurança que seu provedor de confiança envia ao Verified Access, como o endereço de e-mail do usuário ou o grupo ao qual ele pertence, são avaliados de acordo com suas políticas de acesso sempre que uma solicitação de aplicativo é recebida.

Mais detalhes podem ser encontrados nas postagens do blog do Verified Access.

Conclusão

À medida que você escala seu uso AWS e implanta aplicativos na AWS Landing Zone, o número de VPCs e componentes de rede aumenta. Este whitepaper explicou como você pode gerenciar essa infraestrutura em crescimento, garantindo escalabilidade, alta disponibilidade e segurança, mantendo os custos baixos. Tomar as decisões corretas de design ao usar serviços como Transit Gateway, Shared VPC, AWS Direct Connect VPC endpoints, Gateway Load Balancer, AWS Network Firewall Amazon Route 53 e dispositivos de software de terceiros se torna essencial. É importante entender as principais considerações de cada abordagem, analisar seus requisitos e analisar qual opção ou combinação de opções é mais adequada para você.

Colaboradores

As pessoas a seguir contribuíram na elaboração deste documento:

- Sohaib Tahir, arquiteto de soluções, Amazon Web Services
- Shirin Bhambhani, arquiteta de soluções, Amazon Web Services
- Kunal Pansari, arquiteto de soluções, Amazon Web Services
- Eric Vasquez, arquiteto de soluções, Amazon Web Services
- Tushar Jagdale, arquiteto de soluções, Amazon Web Services
- Ameer Shariff, arquiteto de soluções, Amazon Web Services
- Glenn Davis, arquiteto de soluções, Amazon Web Services
- Nick Kniveton, arquiteto de soluções, Amazon Web Services
- Sidhartha Chauhan, arquiteta de soluções principal, Amazon Web Services

Histórico do documento

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

Alteração	Descrição	Data
Atualização principal	Atualizações em todo o whitepaper sobre alteraçõe s no CloudWAN, Amazon VPC Lattice, ENA Express, conectividade híbrida, Sitelink, Deep Packet AWS Direct Connect Inspection e. Acesso Verificado pela AWS	17 de abril de 2024
Atualização secundária	Diagramas atualizados para serem mais consistentes, opções de conectividade DX atualizadas para incluir VPN IP privada e várias pequenas alterações por toda parte.	6 de julho de 2023
Atualização secundária	AWS Control Tower Informaçõ es atualizadas, novos limites de taxa de transferê ncia refletidos para vários serviços, diagrama de gateway NAT atualizado, seção de segurança atualizad a para centralizar a saída.	4 de abril de 2023
Atualização secundária	Seção adicionada: Acesso ao endpoint entre regiões.	19 de julho de 2022
Atualização principal	Seção Transit Gateway atualizada com Transit Gateway Connect, seção	22 de fevereiro de 2022

	Transit VPC atualizada; AWS Direct Connect seção atualizada com recomenda ções de MACsec e resiliênc ia; seção atualizada. AWS PrivateLink Foi adicionada a tabela de comparação entre VPC e Transit VPC versus Transit Gateway; seção de inspeção de entrada centraliz ada; segurança de rede centralizada atualizada para VPC para VPC e VPC local para VPC e saída centraliz ada para a Internet AWS Network Firewall com padrões de design do Gateway Load Balancer; adição de seções de gateway NAT privado e firewall DNS do Amazon Route 53.	
Atualização secundária	Seção atualizada de emparelhamento Transit Gateway versus VPC	2 de abril de 2021
Whitepaper atualizado	Texto corrigido para correspon der às opções ilustradas na Figura 7	10 de junho de 2020
Publicação inicial	Publicação do whitepaper.	15 de novembro de 2019

Avisos

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.