AWS Whitepaper

Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS

Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS: AWS Whitepaper

Table of Contents

Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS

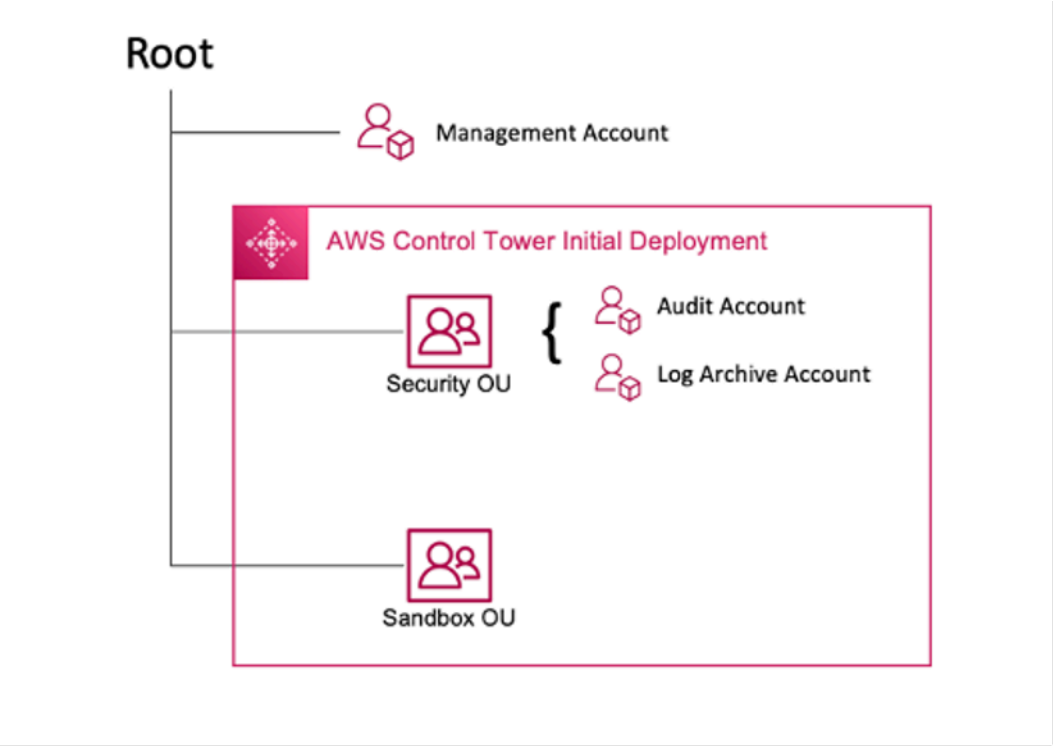
Veröffentlichungsdatum: 17. April 2024 () Dokumentverlauf

Kunden von Amazon Web Services (AWS) verlassen sich häufig auf Hunderte von Konten und virtuellen privaten Clouds (VPCs), um ihre Workloads zu segmentieren und ihren Footprint zu erweitern. Diese Größenordnung führt häufig zu Problemen in Bezug auf die gemeinsame Nutzung von Ressourcen, die Konnektivität zwischen VPCs und die Konnektivität zwischen lokalen Einrichtungen und VPC-Konnektivität.

In diesem Whitepaper werden bewährte Methoden für die Erstellung skalierbarer und sicherer Netzwerkarchitekturen in einem großen Netzwerk mithilfe von AWS Services wie Amazon Virtual Private Cloud (Amazon VPC),, AWS Transit GatewayAWS PrivateLinkDirect Connect, Gateway Load Balancer und Amazon Route AWS Network Firewall53 beschrieben. Es zeigt Lösungen für die Verwaltung einer wachsenden Infrastruktur, die Skalierbarkeit, hohe Verfügbarkeit und Sicherheit gewährleisten und gleichzeitig die Gemeinkosten niedrig halten.

Einführung

AWS Kunden beginnen mit dem Aufbau von Ressourcen in einem einzigen AWS Konto, das eine Verwaltungsgrenze darstellt, die Berechtigungen, Kosten und Dienste segmentiert. Mit dem Wachstum der Kundenorganisation wird jedoch eine stärkere Segmentierung der Services erforderlich, um die Kosten zu überwachen, den Zugang zu kontrollieren und das Umweltmanagement zu vereinfachen. Eine Lösung mit mehreren Konten löst diese Probleme, indem sie spezifische Konten für IT-Dienste und Benutzer innerhalb eines Unternehmens bereitstellt. AWS bietet mehrere Tools zur Verwaltung und Konfiguration dieser Infrastruktur, darunter. AWS Control Tower



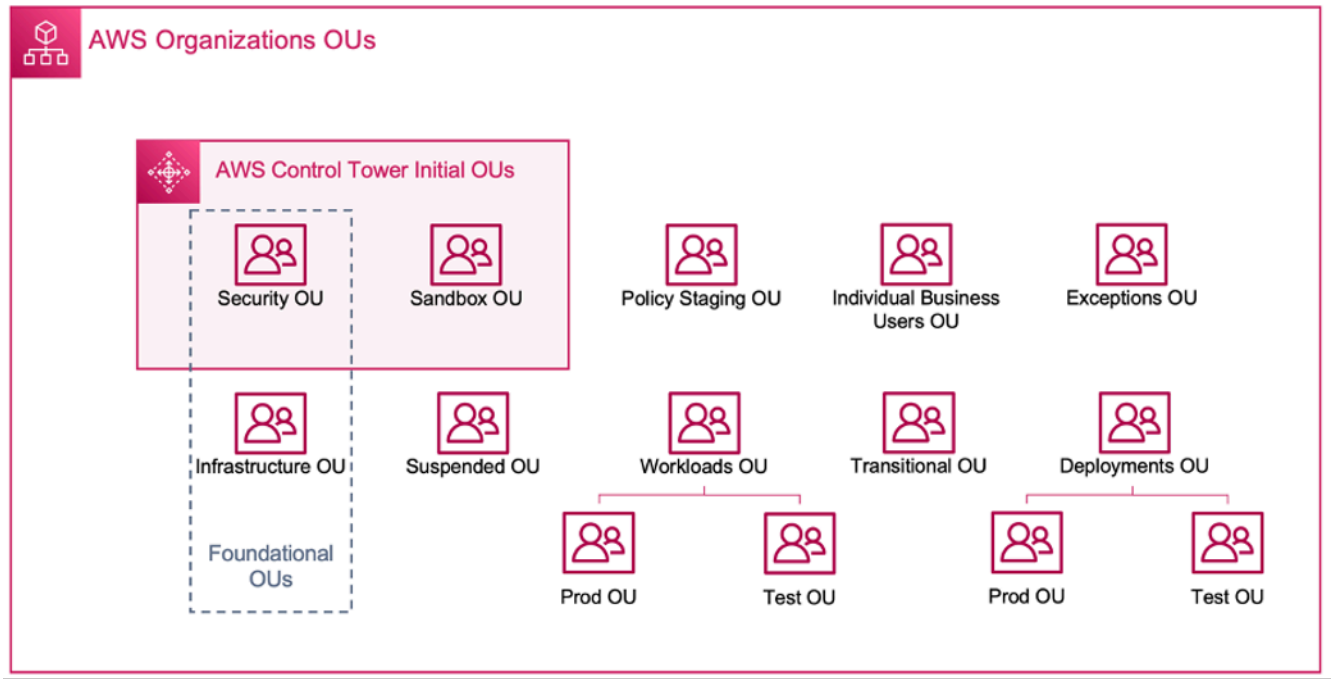
AWS Erstmaliger Einsatz des Control Tower

Wenn Sie Ihre Umgebung mit mehreren Konten einrichten AWS Control Tower, werden zwei Organisationseinheiten (OUs) erstellt:

- Sicherheits-OU — Innerhalb dieser Organisationseinheit werden zwei Konten AWS Control Tower erstellt:
- Log-Archiv
- Audit (Dieses Konto entspricht dem Security-Tooling-Konto, das bereits in der Anleitung beschrieben wurde.)
- Sandbox-Organisationseinheit — Diese Organisationseinheit ist das Standardziel für Konten, die in dieser Organisationseinheit erstellt wurden. AWS Control Tower Sie enthält Konten, in denen Ihre Builder Dienste und andere Tools und AWS Dienste ausprobieren und damit experimentieren können, sofern die Nutzungsbedingungen Ihres Teams eingehalten werden.

AWS Control Tower ermöglicht es Ihnen, zusätzliche Funktionen zu erstellen, zu registrieren und zu verwalten, OUs um die anfängliche Umgebung für die Implementierung der Leitlinien zu erweitern.

Das folgende Diagramm zeigt die OUs ursprünglich von bereitgestellte AWS Control Tower. Sie können Ihre AWS Umgebung erweitern, um alle der im Diagramm OUs enthaltenen Empfehlungen zu implementieren, um Ihren Anforderungen gerecht zu werden.



AWS organisatorisch OUs

Weitere Informationen zur Verwendung von Umgebungen mit AWS Control Tower mehreren Konten finden Sie in Anhang E des Whitepapers Organizing Your AWS Environment Using Multi-Accounts.

Die meisten Kunden beginnen mit einigen wenigen VPCs , um ihre Infrastruktur bereitzustellen. Die Anzahl, die VPCs ein Kunde erstellt, hängt in der Regel von der Anzahl seiner Konten, Benutzer und bereitgestellten Umgebungen (Produktion, Entwicklung, Test usw.) ab. Mit zunehmender Cloud-Nutzung nimmt auch die Anzahl der Benutzer, Geschäftsbereiche, Anwendungen und Regionen zu, mit denen ein Kunde interagiert, was zur Entstehung neuer Anwendungen führt. VPCs

VPCs Mit steigender Anzahl wird das vPCübergreifende Management für den Betrieb des Cloud-Netzwerks des Kunden unverzichtbar. Dieses Whitepaper behandelt bewährte Methoden für drei spezifische Bereiche der Cross-VPC- und Hybrid-Konnektivität:

- Netzwerkkonnektivität — Zusammenschaltung VPCs und lokale Netzwerke in großem Maßstab.
- Netzwerksicherheit — Aufbau zentraler Ausgangspunkte für den Zugriff auf das Internet und Endpunkte wie Network Address Translation (NAT) -Gateway, VPC-Endpunkte und Gateway AWS PrivateLinkLoad AWS Network FirewallBalancers.
- DNS-Management — Auflösen von DNS innerhalb des Control Tower und Hybrid-DNS.

Planung und Verwaltung von IP-Adressen

Um ein skalierbares Multi-Account-Multi-VPC-Netzwerkdesign aufzubauen, ist die Planung und Verwaltung von IP-Adressen unerlässlich. Ein gutes IP-Adressierungsschema muss Ihre aktuellen und future Netzwerkanforderungen berücksichtigen. Ihr IP-Adressschema muss Ihre lokalen Workloads und Ihre Cloud-Workloads abdecken und sollte auch future Erweiterungen ermöglichen (z. B. das Hinzufügen neuer AWS-Regionen Geschäftsbereiche sowie Fusionen oder Übernahmen). Es sollte auch verhindern, dass Ihre Teams versehentlich IP-Überschneidungen erstellen. CIDRs Wenn eine überlappende IP-CIDR gewünscht wird, z. B. für isolierte oder nicht verbundene Workloads, muss diese Entscheidung bewusst getroffen und die Auswirkungen auf Routing, Sicherheit und Kosten berücksichtigt werden. Möglicherweise müssen Sie auch die Einrichtung der erforderlichen Genehmigungsverfahren für solche Ausnahmen in Betracht ziehen. Ein gutes IP-Adressierungsschema hilft auch dabei, Ihr Netzwerkdesign und Ihre Routingkonfiguration zu vereinfachen.

Wesentliche Überlegungen:

- Planen Sie Ihr IP-Adressierungsschema (sowohl öffentlich als auch privat IPs) im Voraus und wählen Sie ein IP-Adressverwaltungstool aus, um die IP-Adressnutzung für all Ihre Workloads zuzuweisen, zu verwalten und zu verfolgen.
- Verwenden Sie hierarchische und zusammengefasste IP-Adressierungsschemata.
- Planen Sie eine konsistente IP-Zuweisung auf der Grundlage von Umgebung AWS-Region, Organisation oder Geschäftseinheit ein.
- Weisen Sie für lokale Netzwerke IPv4 und Cloud-Netzwerke unterschiedliche IP-Adressen CIDRs (sowohl als auch IPv6) zu.
- Vermeiden und verfolgen Sie proaktiv IP-Überschneidungen. CIDRs
- Passen Sie die Größe Ihrer CIDRs IP an, um Skalierung und future Wachstum zu ermöglichen.
- Aktivieren Sie Ihre Workloads für die IPv6 Dual-Stack-Kompatibilität, um IP-Konflikte und die Erschöpfung des IPv4 Adressraums zu reduzieren.

Sie können Amazon VPC IP Address Manager (IPAM) verwenden, um die Planung, Nachverfolgung und Überwachung sowohl öffentlicher als auch privater IP-Adressen für Ihre AWS Workloads zu vereinfachen. IPAM ermöglicht es Ihnen, den IP-Adressraum für mehrere und zu organisieren, zuzuweisen, zu überwachen und gemeinsam zu nutzen. AWS-Regionen AWS-Konten Es hilft auch bei der automatischen Zuweisung von Daten CIDRs VPCs anhand bestimmter Geschäftsregeln.

In den AWS Control Tower Blogbeiträgen Amazon VPC IP Address Manager Best Practices, IP-Pools zwischen VPCs und Regionen mithilfe von Amazon VPC IP Address Manager verwalten und IP Address Management erfahren Sie mehr über bewährte Methoden zur IP-Adressierung und zur Verwendung von IPAM zur Verwaltung von IP-Pools zwischen VPCs, AWS-Regionen und. AWS Control Tower

Sind Sie Well-Architected?

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mithilfe des AWS Well-Architected Tool, das kostenlos im verfügbar ist AWS-Managementkonsole, können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

Weitere Expertentipps und bewährte Methoden für Ihre Cloud-Architektur — Referenzarchitekturbereitstellungen, Diagramme und Whitepapers — finden Sie im Architecture Center.AWS

VPC-zu-VPC-Konnektivität

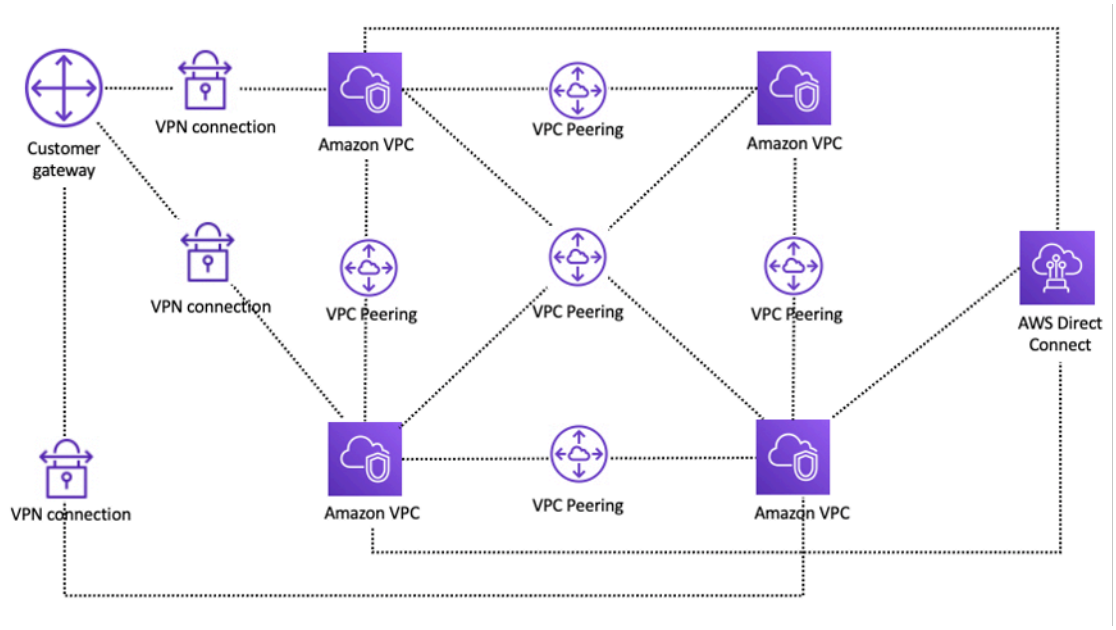
Kunden können zwei verschiedene VPC-Konnektivitätsmuster verwenden, um Multi-VPC-Umgebungen einzurichten: Viele-zu-Many oder Hub-and-Spoke-Umgebungen. Bei diesem many-to-many Ansatz wird der Verkehr zwischen jeder VPC individuell zwischen jeder VPC verwaltet. In dem hub-and-spoke Modell fließt der gesamte Datenverkehr zwischen VPC über eine zentrale Ressource, die den Verkehr auf der Grundlage festgelegter Regeln weiterleitet.

VPC-Peering

Die erste Möglichkeit, zwei zu verbinden, VPCs ist die Verwendung von VPC-Peering. In diesem Setup ermöglicht eine Verbindung die vollständige bidirektionale Konnektivität zwischen den. VPCs Diese Peering-Verbindung wird verwendet, um den Verkehr zwischen den weiterzuleiten. VPCs VPCs in verschiedenen Konten und AWS-Regionen können auch miteinander verbunden werden. Jegliche Datenübertragung über eine VPC-Peering-Verbindung, die innerhalb einer Availability Zone bleibt, ist kostenlos. Alle Datenübertragungen über eine VPC-Peering-Verbindung, die Availability Zones durchquert, werden zu den standardmäßigen regionalen Datenübertragungstarifen berechnet. Bei regionenübergreifendem VPCs Peering fallen die standardmäßigen Gebühren für die Datenübertragung zwischen den Regionen an.

VPC-Peering ist point-to-point Konnektivität und unterstützt kein transitives Routing. Wenn Sie beispielsweise eine VPC-Peering-Verbindung zwischen VPC A und VPC B sowie zwischen VPC A und VPC C haben, kann eine Instance in VPC B nicht über VPC A zu VPC C gelangen. Um Pakete zwischen VPC B und VPC C weiterzuleiten, müssen Sie eine direkte VPC-Peering-Verbindung herstellen.

Im großen Maßstab, wenn Sie Dutzende oder Hunderte von Peering-Verbindungen haben VPCs, kann die Verbindung dieser Verbindungen mit Peering zu einem Netz von Hunderten oder Tausenden von Peering-Verbindungen führen. Eine große Anzahl von Verbindungen kann schwierig zu verwalten und zu skalieren sein. Wenn Sie beispielsweise 100 haben VPCs und ein vollständiges Mesh-Peering zwischen ihnen einrichten möchten, werden 4.950 Peering-Verbindungen [`n(n-1)/2`] benötigt, wobei n die Gesamtzahl von. VPCs Es gibt ein maximales Limit von 125 aktiven Peering-Verbindungen pro VPC.



Netzwerkeinrichtung mit VPC-Peering

Wenn Sie VPC-Peering verwenden, muss zu jeder VPC eine lokale Konnektivität (VPN und/oder Direct Connect) hergestellt werden. Ressourcen in einer VPC können mithilfe der Hybridkonnektivität einer Peer-VPC nicht lokal erreicht werden, wie in der vorherigen Abbildung dargestellt.

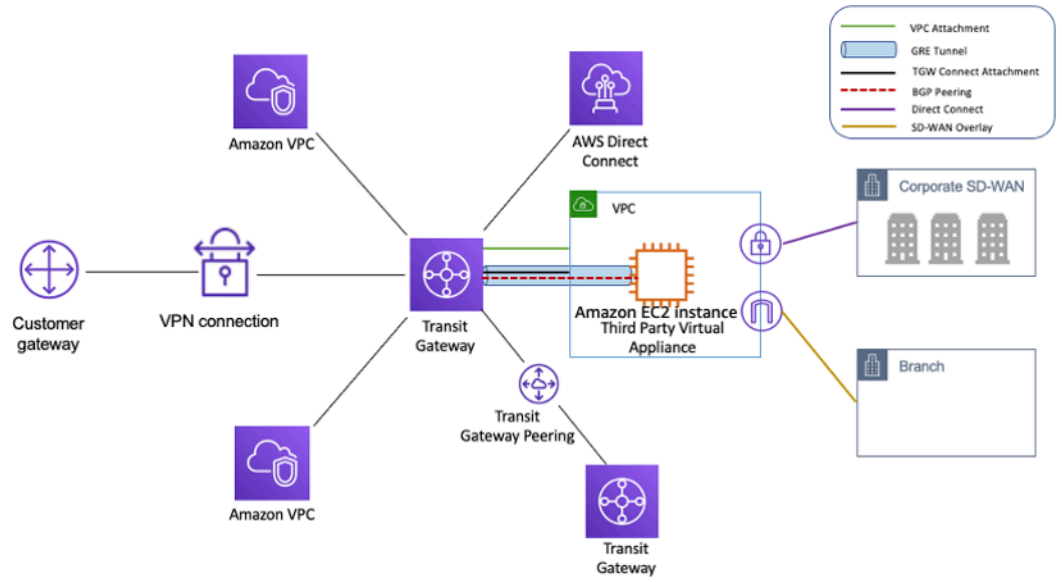
VPC-Peering eignet sich am besten, wenn Ressourcen in einer VPC mit Ressourcen in einer anderen VPC kommunizieren müssen, die Umgebung beider VPC kontrolliert und gesichert VPCs wird und die Anzahl der VPCs zu verbindenden Ressourcen weniger als 10 beträgt (um die individuelle Verwaltung jeder Verbindung zu ermöglichen). VPC-Peering bietet im Vergleich zu anderen Optionen für VPC-Inter-Konnektivität die niedrigsten Gesamtkosten und die höchste Gesamtleistung.

AWS Transit Gateway

AWS Transit Gatewaybietet ein Hub-and-Spoke-Design für Verbindungen VPCs und lokale Netzwerke als vollständig verwalteten Service, ohne dass Sie virtuelle Appliances von Drittanbietern bereitstellen müssen. Es ist kein VPN-Overlay erforderlich und sorgt für hohe AWS Verfügbarkeit und Skalierbarkeit.

Mit Transit Gateway können Kunden Tausende von verbinden VPCs. Sie können Ihre gesamte Hybridkonnektivität (VPN- und Direct Connect-Verbindungen) an ein einziges Gateway anschließen und so die gesamte AWS Routing-Konfiguration Ihres Unternehmens an einem Ort konsolidieren und steuern (siehe folgende Abbildung). Transit Gateway steuert mithilfe von Routentabellen, wie der Verkehr zwischen allen verbundenen Spoke-Netzwerken weitergeleitet wird. Dieses hub-and-spoke

Modell vereinfacht die Verwaltung und senkt die Betriebskosten, da VPCs nur eine Verbindung zur Transit Gateway Gateway-Instanz hergestellt wird, um Zugriff auf die verbundenen Netzwerke zu erhalten.



Design von Nabe und Speiche mit AWS Transit Gateway

Transit Gateway ist eine regionale Ressource und kann Tausende von VPCs innerhalb derselben verbinden AWS-Region. Sie können mehrere Gateways über eine einzige Direct Connect-Verbindung für Hybridkonnektivität verbinden. In der Regel können Sie nur eine Transit Gateway Gateway-Instanz verwenden, die alle Ihre VPC-Instances in einer bestimmten Region verbindet, und Transit Gateway Gateway-Routing-Tabellen verwenden, um sie bei Bedarf zu isolieren. Beachten Sie, dass Sie für eine hohe Verfügbarkeit keine zusätzlichen Transit-Gateways benötigen, da Transit-Gateways von Haus aus hochverfügbar sind. Verwenden Sie aus Redundanzgründen ein einziges Gateway in jeder Region. Es gibt jedoch triftige Argumente für die Einrichtung mehrerer Gateways, um Fehlkonfigurationen, den Explosionsradius zu begrenzen, den Betrieb der Steuerungsebene zu trennen und die Verwaltung zu verwalten. ease-of-use

Mit Transit Gateway Gateway-Peering können Kunden ihre Transit Gateway-Instanzen innerhalb derselben oder mehrerer Regionen miteinander verbinden und den Verkehr zwischen ihnen weiterleiten. Es verwendet dieselbe zugrunde liegende Infrastruktur wie VPC-Peering und ist daher verschlüsselt. Weitere Informationen finden Sie unter Aufbau eines globalen Netzwerks mit AWS Transit Gateway Inter-Region Peering und AWS Transit Gateway unterstützt jetzt Intra-Region Peering.

Platzieren Sie die Transit Gateway Gateway-Instanz Ihrer Organisation in ihrem Network Services-Konto. Dies ermöglicht eine zentrale Verwaltung durch Netzwerktechniker, die das

Netzwerkdienstkonto verwalten. Verwenden Sie AWS Resource Access Manager (RAM), um eine Transit Gateway Gateway-Instance gemeinsam zu nutzen, um Verbindungen VPCs zwischen mehreren Konten in Ihrer AWS-Organisation innerhalb derselben Region herzustellen.AWS RAM ermöglicht Ihnen die einfache und sichere gemeinsame AWS Nutzung von Ressourcen mit beliebigen AWS-Konto oder innerhalb Ihrer AWS-Organisation. Weitere Informationen finden Sie im Blogbeitrag Automating AWS Transit Gateway Attachments to a Transit Gateway in a central account.

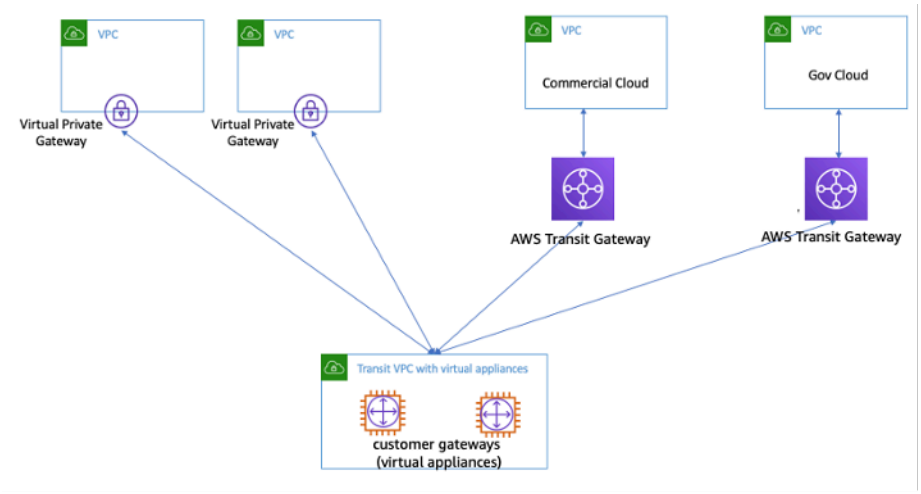
Mit Transit Gateway können Sie auch Konnektivität zwischen der SD-WAN-Infrastruktur und der AWS Verwendung von Transit Gateway Connect herstellen. Verwenden Sie einen Transit Gateway Connect-Anhang mit Border Gateway Protocol (BGP) für dynamisches Routing und das GRE (Generic Routing Encapsulation) -Tunnelprotokoll für hohe Leistung mit einer Gesamtbandbreite von bis zu 20 Gbit/s pro Connect-Anhang (bis zu vier Transit Gateway Connect-Peers pro Connect-Anhang). Mithilfe von Transit Gateway Connect können Sie sowohl die lokale SD-WAN-Infrastruktur als auch SD-WAN-Appliances, die in der Cloud ausgeführt werden, über einen VPC-Anhang oder Direct Connect -Anhang als zugrunde liegende Transportschicht integrieren. Referenzarchitekturen und eine detaillierte Konfiguration finden Sie unter Vereinfachen der SD-WAN-Konnektivität mit AWS Transit Gateway Connect.

Transit VPC-Lösung

Transit VPCs kann Konnektivität zwischen beiden auf andere Weise als VPCs durch VPC-Peering herstellen, indem ein Hub-and-Spoke-Design für Inter-VPC-Konnektivität eingeführt wird. In einem Transit-VPC-Netzwerk verbindet sich eine zentrale VPC (die Hub-VPC) mit jeder anderen VPC (Spoke-VPC) über eine VPN-Verbindung, die in der Regel BGP nutzt. IPsec Die zentrale VPC enthält Amazon Elastic Compute Cloud (Amazon EC2) -Instances, auf denen Software-Appliances ausgeführt werden, die eingehenden Datenverkehr mithilfe des VPN-Overlays an ihre Ziele weiterleiten. Transit-VPC-Peering bietet die folgenden Vorteile:

- Transitives Routing wird mithilfe des Overlay-VPN-Netzwerks aktiviert, was ein Hub-and-Spoke-Design ermöglicht.
- Bei Verwendung von Drittanbietersoftware auf der EC2 Instance in der Hub-Transit-VPC VPC die Funktionen des Anbieters rund um erweiterte Sicherheit (Layer firewall/Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)) can be used. If customers are using the same software on-premises, they benefit from a unified operational/monitoring 7-Erfahrung) zur Verfügung.
- Die Transit VPC-Architektur ermöglicht Konnektivität, die in einigen Anwendungsfällen gewünscht sein kann. Sie können beispielsweise eine GovCloud AWS-Instance und eine Commercial Region-VPC oder eine Transit Gateway Gateway-Instance mit einer Transit-VPC verbinden und die VPC-

Inter-Konnektivität zwischen den beiden Regionen aktivieren. Bewerten Sie Ihre Sicherheits- und Compliance-Anforderungen, wenn Sie diese Option in Betracht ziehen. Für zusätzliche Sicherheit können Sie ein zentralisiertes Inspektionsmodell einsetzen, das auf Entwurfsmustern basiert, die weiter unten in diesem Whitepaper beschrieben werden.



Transit-VPC mit virtuellen Appliances

Transit VPC bringt seine eigenen Herausforderungen mit sich, wie z. B. höhere Kosten für den Betrieb virtueller Appliances von Drittanbietern, je EC2 nach Instanzgröße/Familie, begrenzter Durchsatz pro VPN-Verbindung (bis zu 1,25 Gbit/s pro VPN-Tunnel) und zusätzlicher Aufwand für Konfiguration, Management und Ausfallsicherheit (Kunden sind für die Verwaltung der HA und Redundanz der Instanzen verantwortlich, auf denen virtuelle Appliances von Drittanbietern ausgeführt werden). EC2

VPC-Peering im Vergleich zu Transit VPC im Vergleich zu Transit Gateway

Tabelle 1 — Vergleich der Konnektivität

Kriterien	VPC-Peering	Transit-VPC	Transit-Gateway	PrivateLink	Cloud-WAN	VPC Lattice
Scope	Regional/Global	Regional	Regional	Regional	Global	Regional

Kriterien	VPC-Peering	Transit-VPC	Transit-Gateway	PrivateLink	Cloud-WAN	VPC Lattice
Architektur	Vollmaschiges Netz	VPN-basiert hub-and-spoke	Basiert auf Anhängen hub-and-spoke	Anbieter- oder Verbrauchermodell	Basierend auf Anhängen, regionsübergreifend	Konnektivität von App zu App
Skalieren	125 aktive Peer/VPC	Hängt vom virtuellen Router/ ab EC2	5000 Anlagen pro Region	Keine Grenzen	5000 Anhänge pro Kernnetzwerk	500 VPC-Zuordnungen pro Dienst
Segmentierung	Sicherheitsgruppen	Vom Kunden verwaltet	Transit Gateway Gateway-Routentabellen	Keine Segmentierung	Segmente	Service- und Servicenetzwerkrichtlinien
Latency	Am niedrigsten	Zusätzlich, aufgrund des Overheads bei der VPN-Verschlüsselung	Zusätzlicher Transit Gateway Gateway-Hop	Der Datenverkehr bleibt auf dem AWS-Backbone, Kunden sollten es testen	Verwendet dieselbe Datenebene wie Transit Gateway	Der Datenverkehr bleibt auf dem AWS-Backbone, Kunden sollten es testen

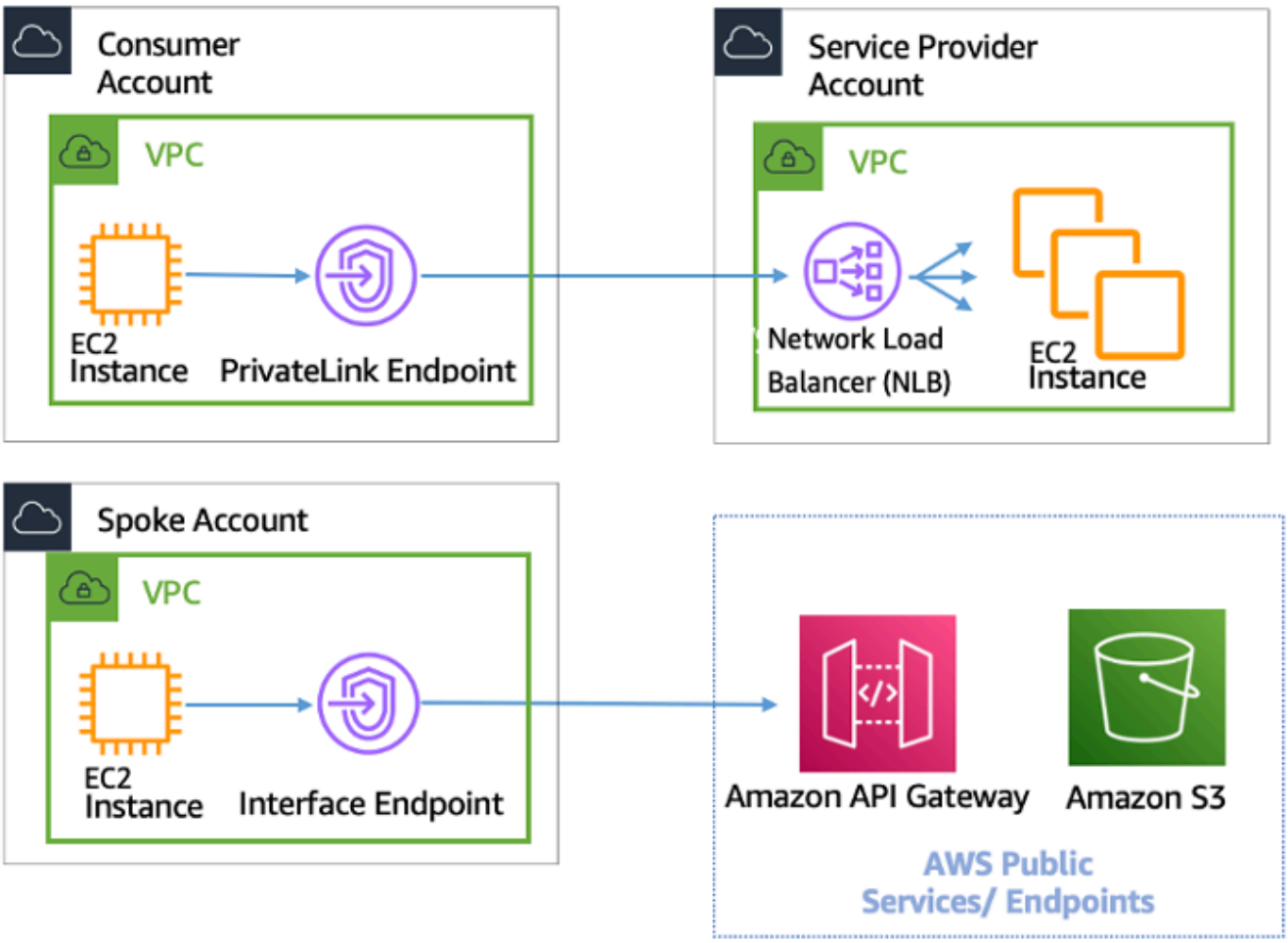
Kriterien	VPC-Peering	Transit-VPC	Transit-Gateway	PrivateLink	Cloud-WAN	VPC Lattice
Bandbreitenbegrenzung	Limits pro Instanz, kein Gesamtlimit	Vorbehaltlich der Bandbreitenbeschränkungen der EC2 Instanz je nach Größe/Familie	Bis zu 100 Gbit/s (Burst) / Verbindung	10 Gbit/s pro Availability Zone, automatische Skalierung auf bis zu 100 Gbit/s	Bis zu 100 Gbit/s (Burst) / Verbindung	10 Gbit/s pro Availability Zone
Sichtbarkeit	VPC Flow Logs	VPC-Flow-Logs und -Metriken CloudWatch	Transit Gateway Network Manager, VPC-Flussprotokolle, Metriken CloudWatch	CloudWatch Metriken	Netzwerkmanager, VPC-Flussprotokolle, Metriken CloudWatch	CloudWatch Zugriffsprotokolle
Sicherheitsgruppe Querverweise	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht zutreffend
IPv6 Unterstützung	Unterstützt	Hängt von der virtuellen Appliance ab	Unterstützt	Unterstützt	Unterstützt	Unterstützt

AWS PrivateLink

AWS PrivateLinkbietet private Konnektivität zwischen VPCs AWS-Services und Ihren lokalen Netzwerken, ohne dass Ihr Datenverkehr dem öffentlichen Internet ausgesetzt wird. Interface-VPC-Endpoints, powered by AWS PrivateLink, machen es einfach, Verbindungen zu AWS und anderen Diensten über verschiedene Konten hinweg herzustellen und Ihre Netzwerkarchitektur erheblich VPCs zu vereinfachen. Auf diese Weise können Kunden, die möglicherweise einen Service oder eine Anwendung, die sich in einer VPC (Service Provider) befindet, privat einer AWS-Region anderen VPCs (Consumer) zugänglich machen möchten, und zwar so, dass nur der Verbraucher Verbindungen zur Service Provider-VPC VPCs initiiert. Ein Beispiel hierfür ist die Möglichkeit, dass Ihre privaten Anwendungen auf den Dienstanbieter zugreifen können. APIs

Erstellen Sie zur Verwendung AWS PrivateLink einen Network Load Balancer für Ihre Anwendung in Ihrer VPC und eine VPC-Endpunktdienstkonfiguration, die auf diesen Load Balancer verweist. Ein Service-Consumer erstellt dann einen Schnittstellen-Endpunkt zu Ihrem Service. Dadurch wird ein elastic network interface (ENI) im Consumer-Subnetz mit einer privaten IP-Adresse erstellt, die als Einstiegspunkt für den Datenverkehr dient, der für den Service bestimmt ist. Der Verbraucher und der Service müssen sich nicht in derselben VPC befinden. Wenn die VPC unterschiedlich ist, VPCs können der Verbraucher und der Dienstanbieter überlappende IP-Adressbereiche haben. Sie können nicht nur den VPC-Schnittstellen-Endpunkt für den Zugriff auf Services in anderen erstellen VPCs, sondern auch Schnittstellen-VPC-Endpunkte erstellen, über die Sie privat auf unterstützte AWS-Services zugreifen können AWS PrivateLink, wie in der folgenden Abbildung dargestellt.

Mit Application Load Balancer (ALB) als Ziel von NLB können Sie jetzt erweiterte ALB-Routing-Funktionen mit kombinieren. AWS PrivateLink Referenzarchitekturen und eine detaillierte Konfiguration finden Sie unter Application Load Balancer Balancer-type Target Group for Network Load Balancer.



AWS PrivateLink für Konnektivität zu anderen VPCs und AWS-Services

Die Wahl zwischen Transit Gateway, VPC-Peering und hängt von AWS PrivateLink der Konnektivität ab.

- AWS PrivateLink— Verwenden Sie diese Option, AWS PrivateLink wenn Sie einen Client/Server eingerichtet haben, auf dem Sie einem oder mehreren Verbrauchern VPCs unidirektionalen Zugriff auf einen bestimmten Dienst oder eine Gruppe von Instanzen in der Service Provider-VPC oder auf bestimmte Dienste gewähren möchten. AWS Nur die Clients mit Zugriff in der Consumer-VPC können eine Verbindung zum Service in der Service Provider-VPC oder AWS im Service initiieren. Dies ist auch eine gute Option, wenn sich die IP-Adressen der Clients und Server der beiden VPCs überschneiden, da die AWS PrivateLink Verwendung ENIs innerhalb der Client-VPC so erfolgt, dass keine IP-Konflikte mit dem Dienstanbieter auftreten. Sie können über VPC-Peering, VPN, Transit Gateway, Cloud WAN und auf AWS PrivateLink Endpunkte zugreifen. AWS Direct Connect

- VPC-Peering und Transit Gateway — Verwenden Sie VPC-Peering und Transit Gateway, wenn Sie Layer-3-IP-Konnektivität zwischen aktivieren möchten. VPCs

  Ihre Architektur wird eine Mischung dieser Technologien enthalten, um unterschiedliche Anwendungsfälle zu erfüllen. All diese Dienste können kombiniert und miteinander betrieben werden. Zum Beispiel die AWS PrivateLink Handhabung von Client-Server-Konnektivität im API-Stil, VPC-Peering zur Erfüllung direkter Konnektivitätsanforderungen, bei denen Platzierungsgruppen innerhalb der Region oder regionsübergreifende Konnektivität erforderlich sind, und Transit Gateway zur Vereinfachung der Konnektivität VPCs im großen Maßstab sowie Edge-Konsolidierung für Hybridkonnektivität.

VPC-Freigabe

VPCs Die gemeinsame Nutzung ist nützlich, wenn die Netzwerkisolierung zwischen Teams nicht strikt vom VPC-Besitzer verwaltet werden muss, sondern die Benutzer und Berechtigungen auf Kontoebene. Mit Shared VPC erstellen mehrere AWS-Konten ihre Anwendungsressourcen (wie EC2 Amazon-Instances) in gemeinsam genutztem, zentral verwaltetem Amazon VPCs. In diesem Modell teilt sich das Konto, dem die VPC gehört (Besitzer), ein oder mehrere Subnetze mit anderen Konten (Teilnehmern). Wenn ein Subnetz freigegeben wurde, können die Teilnehmer ihre Anwendungsressourcen in den für sie freigegebenen Subnetzen anzeigen, erstellen, ändern oder löschen. Teilnehmer können keine Ressourcen anzeigen, ändern oder löschen, die anderen Teilnehmern oder dem VPC-Eigentümer gehören. Die Sicherheit zwischen gemeinsam genutzten Ressourcen VPCs wird mithilfe von Sicherheitsgruppen, Netzwerkzugriffskontrolllisten (NACLs) oder durch eine Firewall zwischen den Subnetzen verwaltet.

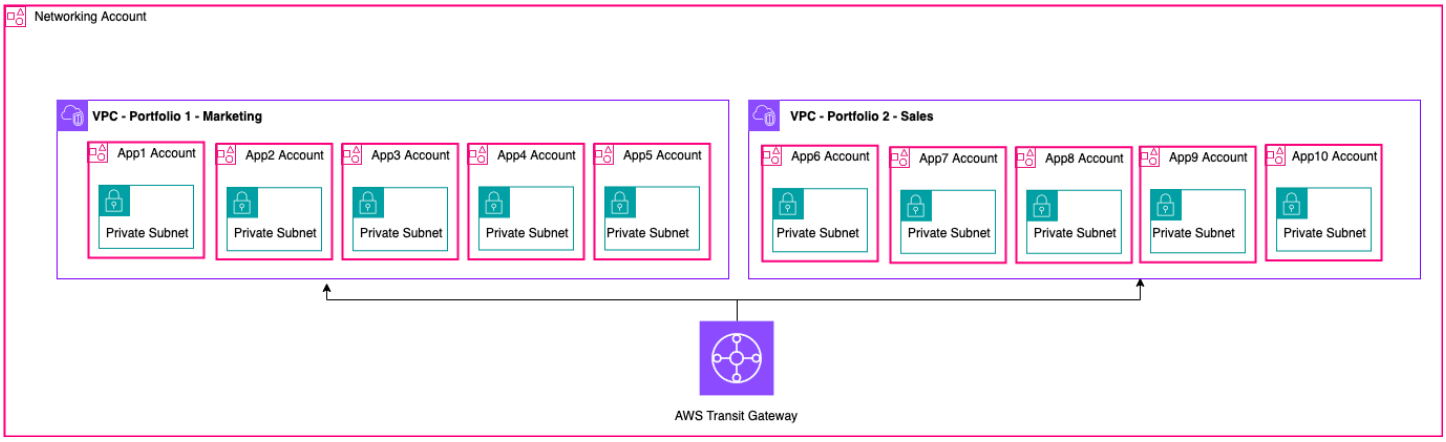
Vorteile VPC VPC-Sharing:

- Vereinfachtes Design — keine Komplexität im Zusammenhang mit Inter-VPC-Konnektivität
- Weniger verwaltet VPCs
- Aufgabentrennung zwischen Netzwerkteams und Anwendungseigentümern
- Bessere IPv4 Adressnutzung
- Niedrigere Kosten — keine Datenübertragungsgebühren zwischen Instances, die zu unterschiedlichen Konten innerhalb derselben Availability Zone gehören

> **Note**
>
> Wenn Sie ein Subnetz mit mehreren Konten gemeinsam nutzen, sollten Ihre Teilnehmer ein gewisses Maß an Kooperation haben, da sie IP-Bereich und Netzwerkressourcen gemeinsam nutzen. Bei Bedarf können Sie für jedes Teilnehmerkonto ein anderes Subnetz gemeinsam nutzen. Ein Subnetz pro Teilnehmer ermöglicht es Netzwerk-ACL, zusätzlich zu Sicherheitsgruppen auch Netzwerkisolierung bereitzustellen.

Die meisten Kundenarchitekturen werden mehrere enthalten VPCs, von denen viele mit zwei oder mehr Konten gemeinsam genutzt werden. Transit Gateway und VPC-Peering können verwendet werden, um die gemeinsam genutzten Geräte zu verbinden. VPCs Nehmen wir zum Beispiel an, Sie haben 10 Anwendungen. Jede Anwendung benötigt ein eigenes AWS-Konto. Die Apps können in zwei Anwendungsportfolios eingeteilt werden (Apps innerhalb desselben Portfolios haben ähnliche Netzwerkanforderungen, App 1—5 unter „Marketing“ und App 6—10 unter „Vertrieb“).

Sie können eine VPC pro Anwendungsportfolio haben (VPCs insgesamt zwei), und die VPC wird mit den verschiedenen Anwendungsbesitzerkonten innerhalb dieses Portfolios gemeinsam genutzt. App-Besitzer stellen Apps in ihrer jeweiligen gemeinsam genutzten VPC bereit (in diesem Fall in den verschiedenen Subnetzen zur Segmentierung und Isolierung von Netzwerkrouten). NACLs Die beiden gemeinsam genutzten VPCs sind über das Transit Gateway verbunden. Mit diesem Setup könnten Sie von 10 auf nur zwei Verbindungen VPCs umsteigen, wie in der folgenden Abbildung dargestellt.

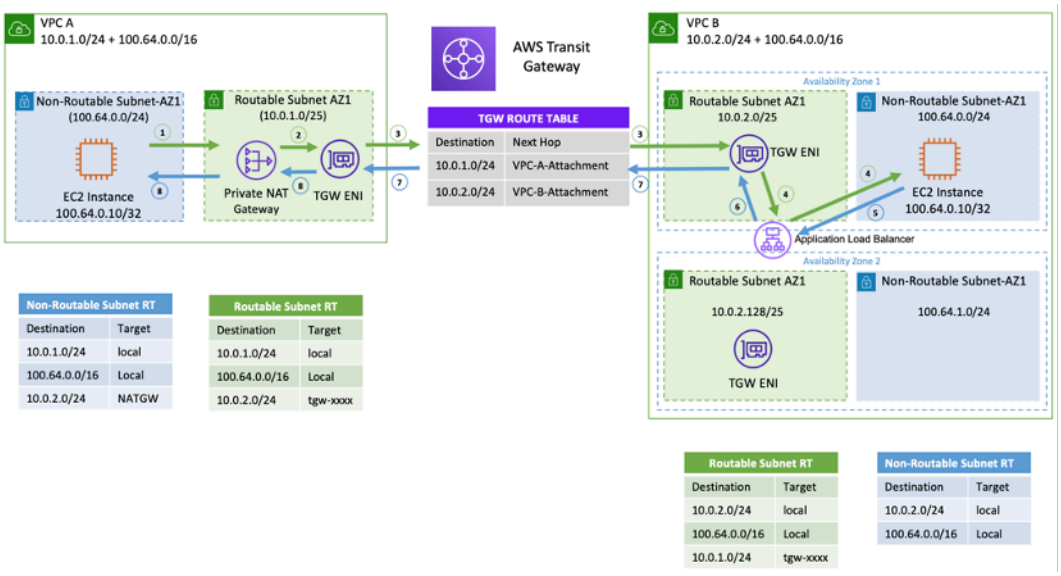


Beispiel-Setup — gemeinsam genutzte VPC

> **Note**
>
> VPC-Sharing-Teilnehmer können nicht alle AWS-Ressourcen in einem gemeinsam genutzten Subnetz erstellen. Weitere Informationen finden Sie im Abschnitt Einschränkungen in der Dokumentation zu VPC Sharing.
> Weitere Informationen zu den wichtigsten Überlegungen und bewährten Methoden für die gemeinsame Nutzung von VPC finden Sie im Blogbeitrag VPC-Sharing: wichtige Überlegungen und bewährte Methoden.

Privates NAT-Gateway

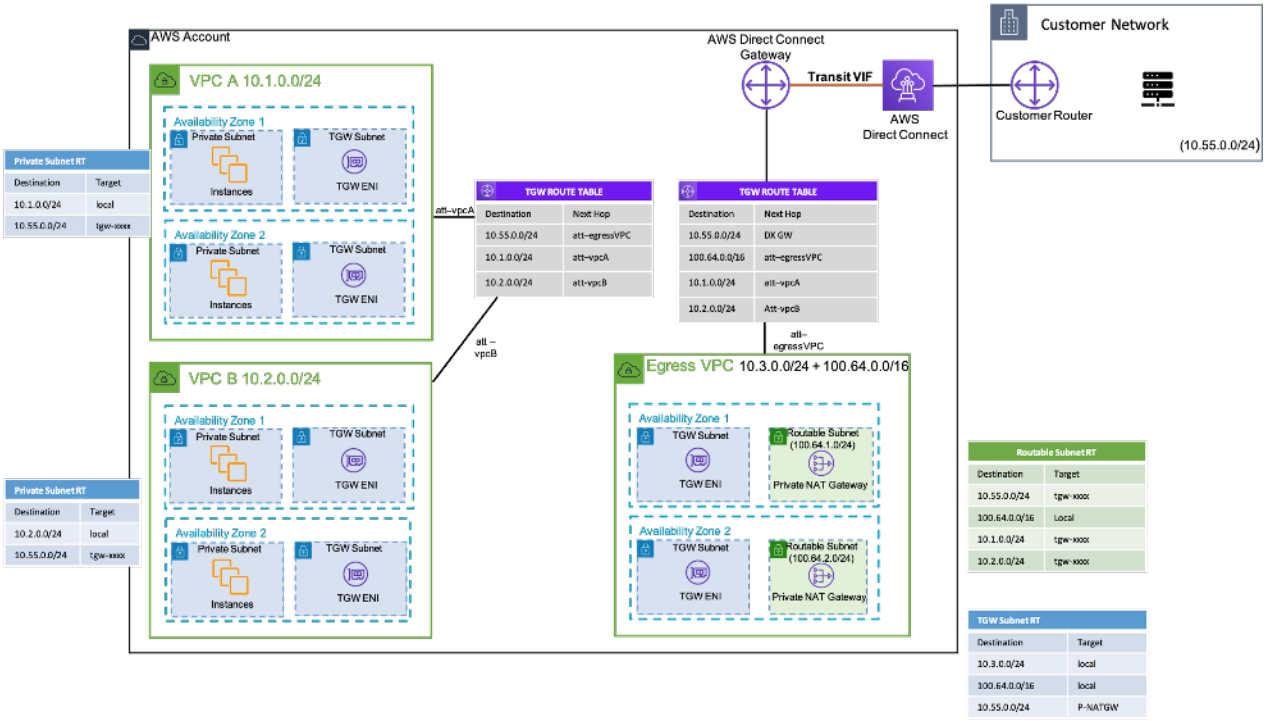
Teams arbeiten oft unabhängig voneinander und erstellen möglicherweise eine neue VPC für ein Projekt, die möglicherweise überlappende CIDR-Blöcke (Classless Interdomain Routing) enthält. Für die Integration möchten sie möglicherweise die Kommunikation zwischen Netzwerken mit Überlappung ermöglichen CIDRs, was mit Funktionen wie VPC-Peering und Transit Gateway nicht erreicht werden kann. Ein privates NAT-Gateway kann bei diesem Anwendungsfall helfen. Ein privates NAT-Gateway verwendet eine eindeutige private IP-Adresse, um die Quell-NAT für die überlappende Quell-IP-Adresse durchzuführen, und ELB führt die Ziel-NAT für die überlappende Ziel-IP-Adresse durch. Mit Transit Gateway oder einem Virtual Private Gateway können Sie den Verkehr von Ihrem privaten NAT-Gateway zu anderen VPCs oder lokalen Netzwerken weiterleiten.



Beispielkonfiguration — Privates NAT-Gateway

Die vorherige Abbildung zeigt zwei nicht routbare (überlappende`100.64.0.0/16`) Subnetze in VPC A und B. Um eine Verbindung zwischen ihnen herzustellen CIDRs, können Sie sekundäre, sich nicht überschneidende/routbare CIDRs (routbare Subnetze und) zu VPC A bzw. B hinzufügen. `10.0.1.0/24` `10.0.2.0/24` Das Routing sollte von dem Netzwerkmanagementteam zugewiesen werden, das für die IP-Zuweisung verantwortlich ist. CIDRs Dem routbaren Subnetz in VPC A wird ein privates NAT-Gateway mit der IP-Adresse von hinzugefügt. `10.0.1.125` Das private NAT-Gateway führt die Übersetzung der Quellnetzwerkadresse für Anfragen von Instances im nicht routbaren Subnetz von VPC A (`100.64.0.10`) als `10.0.1.125` ENI des privaten NAT-Gateways durch. Jetzt kann der Verkehr auf eine routbare IP-Adresse gerichtet werden, die dem Application Load Balancer (ALB) in VPC B (`10.0.2.10`) zugewiesen ist und das Ziel hat. `100.64.0.10` Der Verkehr wird über Transit Gateway geleitet. Der Rückverkehr wird vom privaten NAT-Gateway zurück zur ursprünglichen EC2 Amazon-Instance verarbeitet, die die Verbindung anfordert.

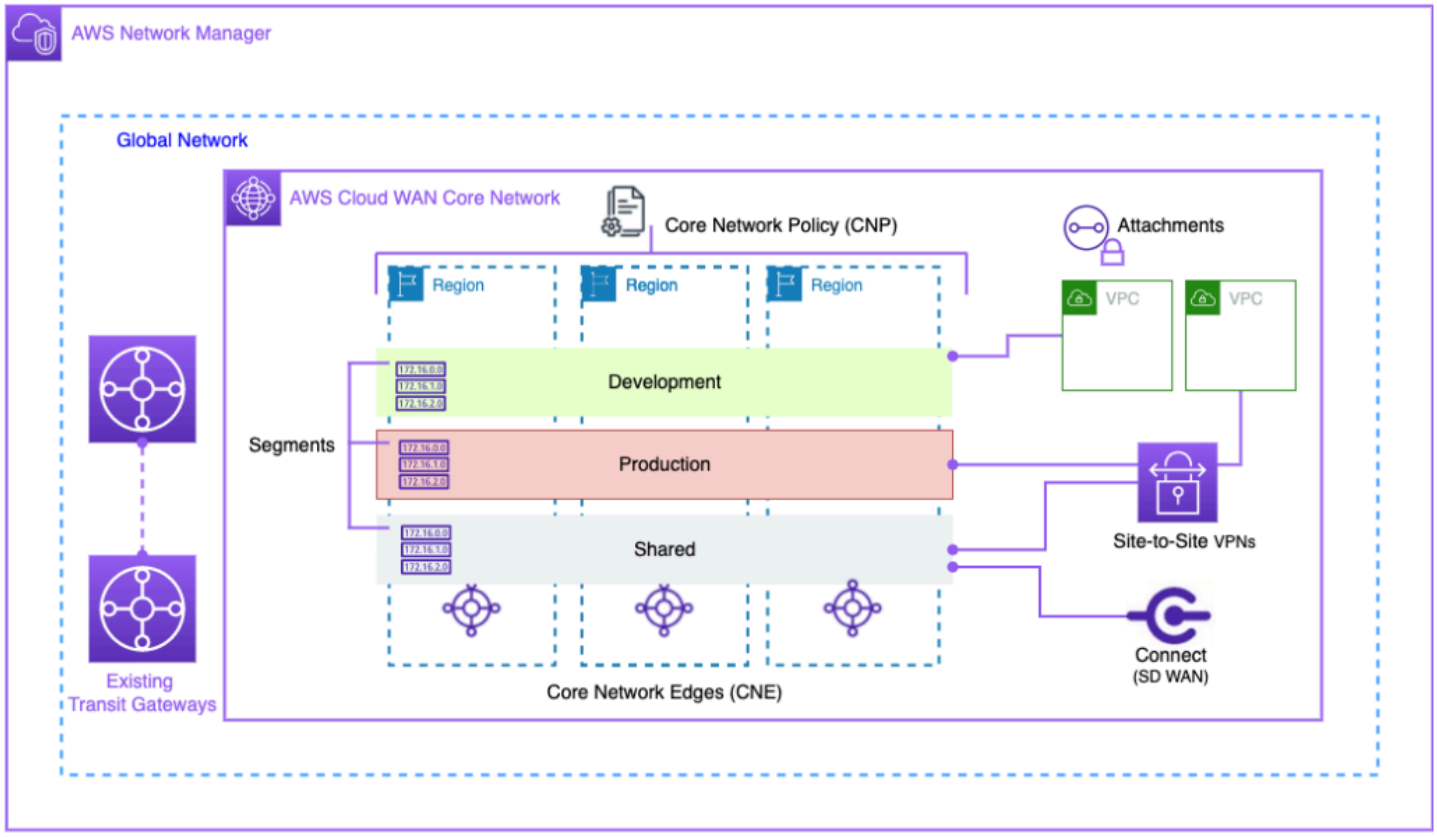
Das private NAT-Gateway kann auch verwendet werden, wenn Ihr lokales Netzwerk den Zugriff auf genehmigt beschränkt. IPs Die lokalen Netzwerke einiger Kunden sind aufgrund gesetzlicher Vorschriften verpflichtet, nur mit privaten Netzwerken (kein IGW) über einen begrenzten zusammenhängenden Block von zugelassenen Netzwerken zu kommunizieren, der dem Kunden gehört. IPs Anstatt jeder Instanz eine separate IP vom Block zuzuweisen, können Sie mithilfe eines privaten NAT-Gateways große Workloads AWS VPCs hinter jeder IP auf der Zulassungsliste ausführen. Einzelheiten finden Sie im Blogbeitrag How to solve Private IP exhaustion with Private NAT Solution.



Beispielkonfiguration — So verwenden Sie ein privates NAT-Gateway, um ein IPs für das lokale Netzwerk freigegebenes Netzwerk bereitzustellen

AWS Cloud-WAN

AWS Cloud WAN ist eine neue Möglichkeit, Netzwerke miteinander zu verbinden, was wir zuvor mit Transit Gateways, VPC Peering und IPSEC-VPN-Tunneln tun konnten. Bisher mussten Sie eine oder mehrere konfigurieren VPCs, sie mit einer der vorherigen Methoden miteinander verbinden und IPSEC-VPN verwenden oder eine Verbindung Direct Connect zu lokalen Netzwerken herstellen. Sie würden Ihre Netzwerk- und Sicherheitsstrukturen an einer Stelle und Ihre Netzwerke an einer anderen Stelle definieren. Cloud WAN ermöglicht es Ihnen, all diese Konstrukte an einem einzigen Ort zu zentralisieren. Gemäß der Richtlinie können Sie Ihre Netzwerke segmentieren, um zu bestimmen, wer mit wem sprechen kann, und den Produktionsdatenverkehr über diese Segmente von Entwicklungs- oder Test-Workloads oder Ihren lokalen Netzwerken isolieren.



Cloud-WAN-Blockdiagramm

Verwalten Sie Ihr globales Netzwerk über die AWS Network Manager-Benutzeroberfläche und APIs. Das globale Netzwerk ist der Container auf Stammebene für all Ihre Netzwerkobjekte.

Das Kernnetzwerk ist der Teil Ihres globalen Netzwerks, der von AWS verwaltet wird. Eine Kernnetzwerkrichtlinie (CNP) ist ein einzelnes, versioniertes Richtliniendokument, das alle Aspekte Ihres Kernnetzwerks definiert. Anlagen sind alle Verbindungen oder Ressourcen, die Sie Ihrem Kernnetzwerk hinzufügen möchten. Ein Core Network Edge (CNE) ist ein lokaler Verbindungspunkt für Anlagen, die der Richtlinie entsprechen. Netzwerksegmente sind Routingdomänen, die standardmäßig nur die Kommunikation innerhalb eines Segments zulassen.

Um CloudWAN zu verwenden:

1. Erstellen Sie in AWS Network Manager ein globales Netzwerk und ein zugehöriges Kernnetzwerk.
2. Erstellen Sie ein CNP, das Segmente, den ASN-Bereich AWS-Regionen und Tags definiert, die zum Anhängen an Segmente verwendet werden sollen.
3. Wenden Sie die Netzwerkrichtlinie an.
4. Teilen Sie das Kernnetzwerk mithilfe des Resource Access Managers mit Ihren Benutzern, Konten oder Organisationen.
5. Anlagen erstellen und taggen.
6. Aktualisieren Sie die Routen in Ihrem Anhang VPCs , sodass sie das Kernnetzwerk einbeziehen.

Cloud WAN wurde entwickelt, um den Prozess der weltweiten Verbindung Ihrer AWS-Infrastruktur zu vereinfachen. Es ermöglicht Ihnen, den Datenverkehr mit einer zentralen Berechtigungsrichtlinie zu segmentieren und Ihre bestehende Infrastruktur an Ihren Unternehmensstandorten zu nutzen. Cloud WAN verbindet auch Ihre SD- VPCs, Client- WANs VPNs, Firewalls- und Rechenzentrumsressourcen VPNs, um eine Verbindung zum Cloud-WAN herzustellen. Weitere Informationen finden Sie in den Blogbeiträgen zu AWS Cloud WAN.

AWS Cloud WAN ermöglicht ein einheitliches Netzwerk, das Cloud- und lokale Umgebungen verbindet. Unternehmen verwenden aus Sicherheitsgründen Firewalls der nächsten Generation (NGFWs) und Intrusion Prevention-Systeme (IPSs). Der Blogbeitrag Migration und Interoperabilitätsmuster für AWS Cloud WAN und Transit Gateway beschreibt Architekturmuster für die zentrale Verwaltung und Inspektion des ausgehenden Netzwerkverkehrs in einem Cloud-WAN-Netzwerk, einschließlich Netzwerken mit einer Region und mehreren Regionen, und konfiguriert Routentabellen. Diese Architekturen stellen sicher, dass Daten und Anwendungen sicher bleiben und gleichzeitig eine sichere Cloud-Umgebung aufrechterhalten wird.

Weitere Informationen zu Cloud WAN finden Sie im Blogbeitrag Centralized Outbound Inspection Architecture in AWS Cloud WAN.

Amazon VPC Lattice

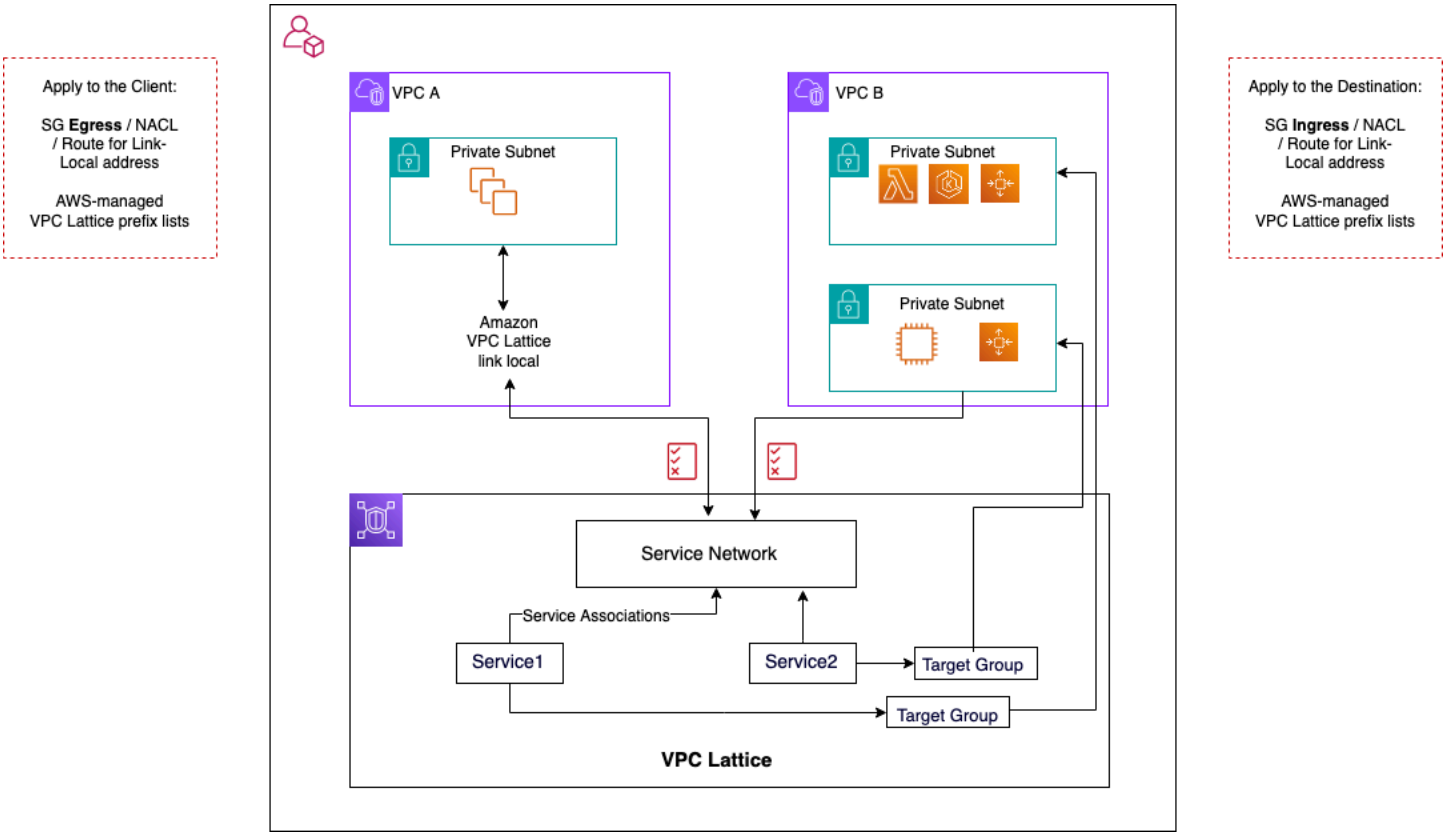
Amazon VPC Lattice ist ein vollständig verwalteter Anwendungsnetzwerkservice, der verwendet wird, um Dienste über verschiedene Konten und virtuelle private Clouds hinweg zu verbinden, zu überwachen und zu sichern. VPC Lattice hilft dabei, Dienste innerhalb einer logischen Grenze miteinander zu verbinden, sodass Sie sie effizient verwalten und ermitteln können.

Die Komponenten von VPC Lattice bestehen aus:

- Service — Dies ist eine Anwendungseinheit, die auf einer Instanz, einem Container oder einer Lambda-Funktion ausgeführt wird und aus Listenern, Regeln und Zielgruppen besteht.
- Servicenetzwerk — Dies ist die logische Grenze, die verwendet wird, um die Serviceerkennung und Konnektivität automatisch zu implementieren und gemeinsame Zugriffs- und Beobachtbarkeitsrichtlinien auf eine Sammlung von Diensten anzuwenden.
- Authentifizierungsrichtlinien — IAM-Ressourcenrichtlinien, die einem Servicenetzwerk oder einzelnen Diensten zugeordnet werden können, um die Authentifizierung auf Anforderungsebene und die kontextspezifische Autorisierung zu unterstützen.
- Serviceverzeichnis — Eine zentrale Ansicht der Services, die Ihnen gehören oder die Ihnen über den AWS Resource Access Manager zur Verfügung gestellt wurden.

Schritte zur Verwendung von VPC Lattice:

1. Erstellen Sie das Servicenetzwerk. Das Dienstnetzwerk befindet sich normalerweise auf einem Netzwerkkonto, auf das ein Netzwerkadministrator vollen Zugriff hat. Das Servicenetzwerk kann von mehreren Konten innerhalb einer Organisation gemeinsam genutzt werden. Die gemeinsame Nutzung kann für einzelne Dienste oder für das gesamte Dienstkonto erfolgen.
2. Stellen Sie eine Verbindung VPCs zum Servicenetzwerk her, um Anwendungsnetzwerke für jede VPC zu aktivieren, sodass verschiedene Dienste andere Dienste nutzen können, die im Netzwerk registriert sind. Sicherheitsgruppen werden zur Steuerung des Datenverkehrs angewendet.
3. Entwickler definieren die Dienste, die in das Dienstverzeichnis aufgenommen und im Dienstnetzwerk registriert werden. VPC Lattice enthält das Adressbuch aller konfigurierten Dienste. Entwickler können auch Routing-Richtlinien definieren, um blaue/grüne Bereitstellungen zu verwenden. Die Sicherheit wird auf der Service-Netzwerkebene verwaltet, auf der Authentifizierungs- und Autorisierungsrichtlinien definiert werden, und auf der Service-Ebene, auf der Zugriffsrichtlinien mit IAM implementiert werden.



VPC-Lattice-Kommunikationsflüsse

Weitere Informationen finden Sie im VPC Lattice-Benutzerhandbuch.

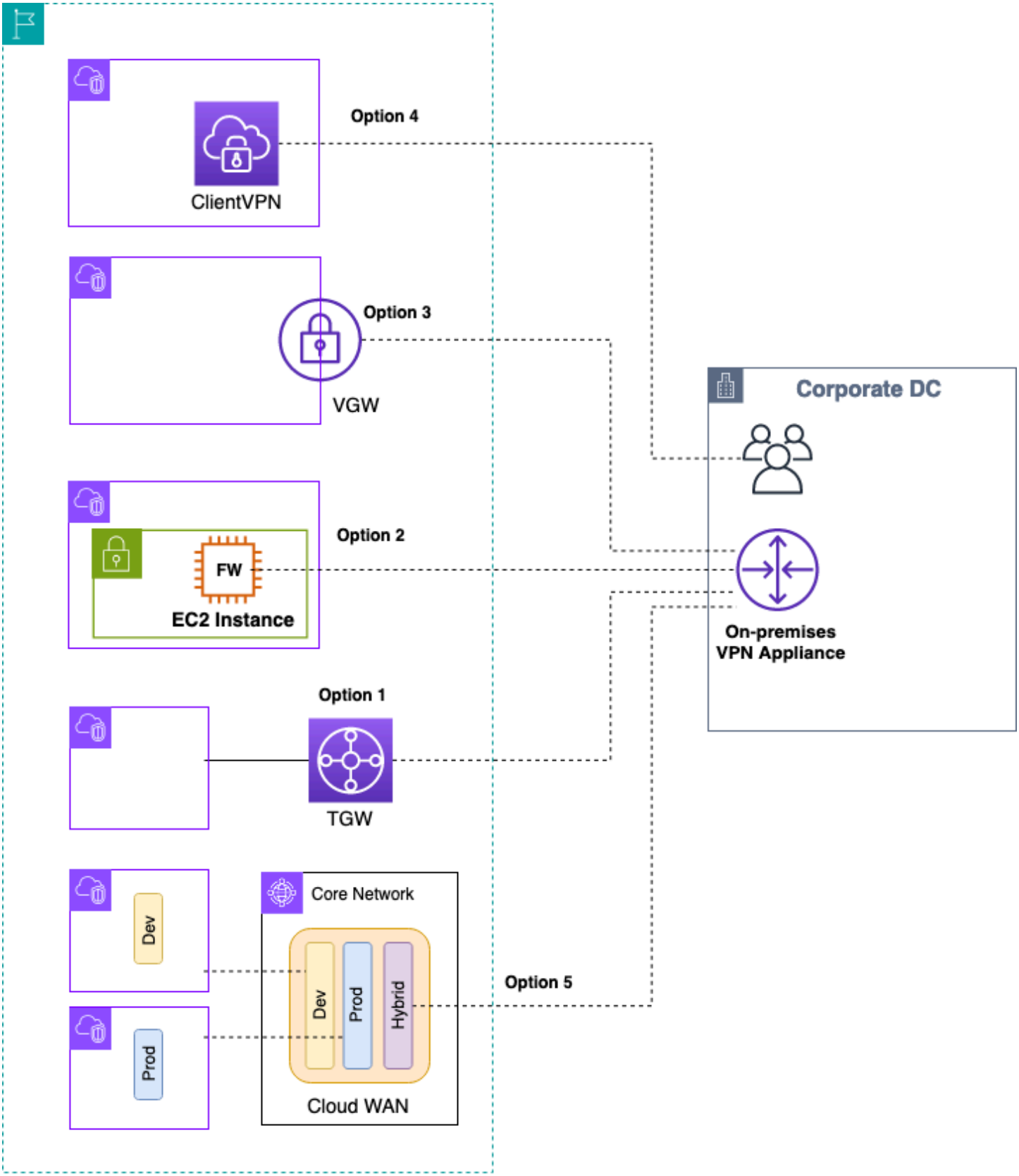
Hybride Konnektivität

Dieser Abschnitt konzentriert sich auf die sichere Verbindung Ihrer Cloud-Ressourcen mit Ihren lokalen Rechenzentren. Es gibt drei Ansätze für die Aktivierung von Hybridkonnektivität:

- One-to-one Konnektivität — In diesem Setup wird für jede VPC eine VPN-Verbindung und/oder eine private Direct Connect-VIF erstellt. Dies wird durch die Verwendung des Virtual Private Gateways (VGW) erreicht. Diese Option eignet sich hervorragend für eine kleine Anzahl von VPCs, aber wenn ein Kunde seine Kapazität skaliert VPCs, kann die Verwaltung der Hybridkonnektivität pro VPC schwierig werden.
- Edge-Konsolidierung — In diesem Setup konsolidieren Kunden Hybrid-IT-Konnektivität für mehrere Geräte VPCs an einem einzigen Endpunkt. Alle VPCs teilen sich diese Hybridverbindungen. Dies wird durch die Verwendung von AWS Transit Gateway und das Direct Connect Gateway erreicht.
- Vollständige Mesh-Hybrid-Konsolidierung — In diesem Setup konsolidieren Kunden mithilfe von CloudWAN die Konnektivität mehrerer Geräte VPCs an einem einzigen Endpunkt. AWS Transit Gateway Dies ist ein vollständig richtlinienbasierter Netzwerkansatz für ein oder mehrere AWS-Konten, dargestellt im Code. Derzeit erfordert die Verwendung von Direct Connect Edge-Konnektivität ein Peering von Transit Gateway zu CloudWAN.

VPN

Es gibt verschiedene Möglichkeiten, VPN für AWS einzurichten:



Site-to-Site VPN Optionen

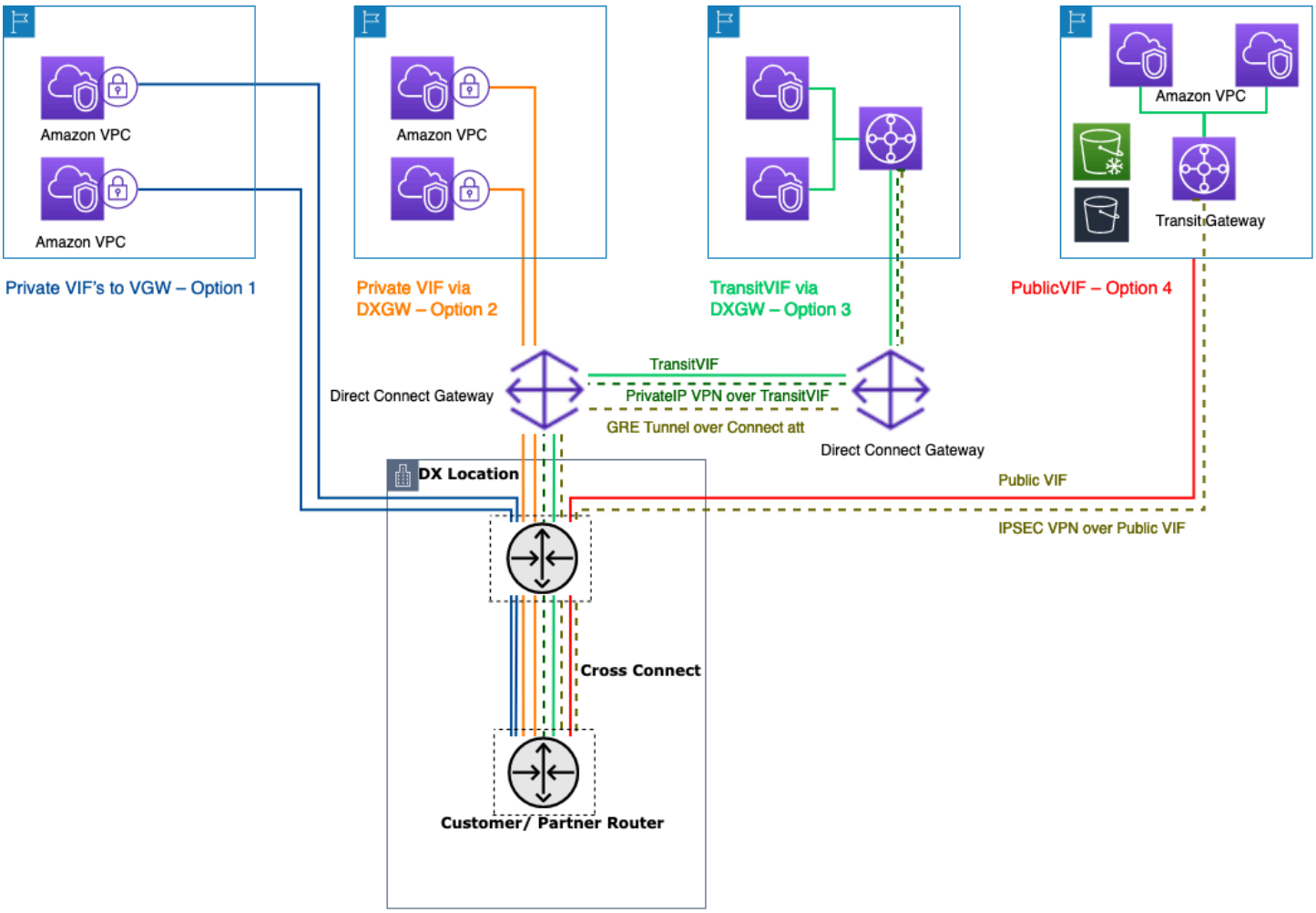
- Option 1: Konsolidierung der VPN-Konnektivität auf dem Transit Gateway — Diese Option nutzt den Transit Gateway-VPN-Anhang auf dem Transit Gateway. Transit Gateway unterstützt die IPsec Terminierung für site-to-site VPN. Kunden können VPN-Tunnel zum Transit Gateway einrichten und auf die damit VPCs verbundenen Verbindungen zugreifen. Transit Gateway unterstützt sowohl statische als auch BGP-basierte dynamische VPN-Verbindungen. Transit Gateway unterstützt auch Equal-Cost Multi-Path (ECMP) für VPN-Anhänge. Jede VPN-Verbindung hat einen maximalen Durchsatz von 1,25 Gbit/s pro Tunnel. Durch die Aktivierung von ECMP können Sie den Durchsatz über VPN-Verbindungen hinweg aggregieren und so über die standardmäßige Höchstgrenze von 1,25 Gbit/s hinaus skalieren. Bei dieser Option zahlen Sie sowohl für die Transit Gateway Gateway-Preise als auch für die Site-to-Site VPN Preise. AWS empfiehlt, diese Option für VPN-Konnektivität zu verwenden. Weitere Informationen finden Sie im Blogbeitrag Skalierung des VPN-Durchsatzes mit AWS Transit Gateway.
- Option 2: VPN auf EC2 Amazon-Instance beenden — Diese Option wird von Kunden in Randfällen genutzt, wenn sie einen bestimmten Softwarefunktionsumfang eines bestimmten Anbieters (wie Cisco DMVPN oder Generic Routing Encapsulation (GRE)) wünschen oder wenn sie Betriebskonsistenz zwischen verschiedenen VPN-Bereitstellungen wünschen. Sie können das Transit-VPC-Design für die Edge-Konsolidierung verwenden. Beachten Sie jedoch, dass alle wichtigen Überlegungen aus dem VPC-zu-VPC-Konnektivität Abschnitt für Transit-VPC auch für Hybrid-VPN-Konnektivität gelten. Sie sind für die Verwaltung der Hochverfügbarkeit verantwortlich und zahlen EC2 beispielsweise die Kosten für Softwarelizenz und Support des Anbieters.
- Option 3: VPN auf einem Virtual Private Gateway (VGW) beenden — Diese Site-to-Site AWS-VPN-Serviceoption ermöglicht ein one-to-one Konnektivitätsdesign, bei dem Sie eine VPN-Verbindung (bestehend aus einem Paar redundanter VPN-Tunnel) pro VPC erstellen. Dies ist eine hervorragende Möglichkeit, mit der VPN-Konnektivität zu AWS zu beginnen. Wenn Sie jedoch die Anzahl der VPN-Verbindungen erhöhen VPCs, kann die Verwaltung einer wachsenden Anzahl von VPN-Verbindungen zu einer Herausforderung werden. Daher wird ein Edge-Konsolidierungsdesign, das Transit Gateway nutzt, irgendwann eine bessere Option sein. Der VPN-Durchsatz zu einem VGW ist auf 1,25 Gbit/s pro Tunnel begrenzt, und der ECMP-Lastenausgleich wird nicht unterstützt. Aus preislicher Sicht zahlen Sie nur für die AWS-VPN-Preise, es fallen keine Gebühren für den Betrieb eines VGW an. Weitere Informationen finden Sie unter Site-to-Site VPN Preise und Site-to-Site VPN auf Virtual Private Gateway.
- Option 4: VPN-Verbindung am Client-VPN-Endpunkt beenden — AWS Client VPN ist ein verwalteter clientbasierter VPN-Service, mit dem Sie sicher auf Ihre AWS-Ressourcen und Ressourcen in Ihrem lokalen Netzwerk zugreifen können. Mit Client VPN können Sie mit einem von OpenVPN oder AWS bereitgestellten VPN-Client von jedem Standort aus auf Ihre Ressourcen zugreifen. Durch die Einrichtung eines Client-VPN-Endpunkts können Clients und Benutzer eine

Verbindung herstellen, um eine Transport Layer Security (TLS) -VPN-Verbindung herzustellen. Weitere Informationen finden Sie in der AWS-Client-VPN-Dokumentation.

- Option 5: VPN-Verbindung auf AWS Cloud WAN konsolidieren — Diese Option ähnelt der ersten Option in dieser Liste, verwendet jedoch die CloudWAN-Fabric, um VPN-Verbindungen mithilfe des Netzwerkrichtliniendokuments programmgesteuert zu konfigurieren.

Direct Connect

VPN über das Internet ist zwar eine hervorragende Option für den Einstieg, aber die Internetverbindung ist für den Produktionsverkehr möglicherweise nicht zuverlässig. Aufgrund dieser Unzuverlässigkeit entscheiden sich viele Kunden dafür Direct Connect. Direct Connect ist ein Netzwerkservice, der eine Alternative zur Nutzung des Internets für die Verbindung zu AWS bietet. Dabei werden Daten Direct Connect, die zuvor über das Internet transportiert worden wären, über eine private Netzwerkverbindung zwischen Ihren Einrichtungen und AWS übertragen. In vielen Fällen können private Netzwerkverbindungen die Kosten senken, die Bandbreite erhöhen und ein einheitlicheres Netzwerkerlebnis bieten als internetbasierte Verbindungen. Es gibt mehrere Möglichkeiten, eine Verbindung Direct Connect herzustellen VPCs mit:



Möglichkeiten zur Verbindung Ihrer lokalen Rechenzentren mit Direct Connect

- Option 1: Erstellen Sie eine private virtuelle Schnittstelle (VIF) zu einem an eine VPC angeschlossenen VGW — Sie können 50 VIFs pro Direct Connect-Verbindung erstellen, sodass Sie eine Verbindung zu maximal 50 herstellen können VPCs (eine VIF bietet Konnektivität zu einer VPC). Es gibt ein BGP-Peering pro VPC. Die Konnektivität in diesem Setup ist auf die AWS-Region beschränkt, in der sich der Direct Connect-Standort befindet. Aufgrund der one-to-one Zuordnung von VIF zu VPC (und des fehlenden globalen Zugriffs) ist dies die am wenigsten bevorzugte Art des Zugriffs VPCs in der Landing Zone.
- Option 2: Erstellen Sie eine private VIF für ein Direct Connect-Gateway, das mehreren zugeordnet ist VGWs (jedes VGW ist mit einer VPC verbunden) — Ein Direct Connect-Gateway ist eine weltweit verfügbare Ressource. Sie können das Direct Connect-Gateway in jeder Region erstellen und von allen anderen Regionen aus darauf zugreifen, einschließlich GovCloud (außer China). Ein Direct Connect Gateway kann über eine einzige private VIF eine Verbindung zu bis zu 20 VPCs

(via VGWs) weltweit in jedem AWS-Konto herstellen. Dies ist eine hervorragende Option, wenn eine Landing Zone aus einer kleinen Anzahl von VPCs (zehn oder weniger VPCs) and/or you need global access. There is one BGP peering session per Direct Connect Gateway per Direct Connect connection. Direct Connect gateway is only for north/south Verkehrsströmen besteht und keine Konnektivität zulässt VPC-to-VPC. Weitere Informationen finden Sie in der Direct Connect Dokumentation unter Virtual Private Gateway Associations. Mit dieser Option ist die Konnektivität nicht auf die AWS-Region beschränkt, in der sich der Direct Connect-Standort befindet. Direct Connect Das Gateway ist nur für den Nord-Süd-Verkehr vorgesehen und ermöglicht keine Konnektivität. VPC-to-VPC Eine Ausnahme von dieser Regel ist, wenn für ein Supernet von zwei oder mehr Teilnehmern geworben wird VPCs , die mit demselben Direct Connect Gateway und derselben virtuellen Schnittstelle VGWs verbunden sind. In diesem Fall VPCs können sie über den Endpunkt miteinander kommunizieren. Direct Connect Weitere Informationen finden Sie in der Dokumentation zu den Direct Connect Gateways.

- Option 3: Erstellen Sie eine Transit-VIF zu einem Direct Connect-Gateway, das mit Transit Gateway verknüpft ist — Sie können eine Transit Gateway Gateway-Instanz einem Direct Connect-Gateway zuordnen, indem Sie eine Transit-VIF verwenden. Direct Connect unterstützt jetzt Verbindungen zu Transit Gateway für alle Portgeschwindigkeiten und bietet so eine kostengünstigere Wahl für Transit Gateway Gateway-Benutzer, wenn Hochgeschwindigkeitsverbindungen (mehr als 1 Gbit/s) nicht erforderlich sind. Auf diese Weise können Sie Direct Connect mit Geschwindigkeiten von 50, 100, 200, 300, 400 und 500 Mbit/s verwenden, um eine Verbindung zum Transit Gateway herzustellen. Transit VIF ermöglicht es Ihnen, Ihr lokales Rechenzentrum mit bis zu sechs Transit Gateway Gateway-Instances pro Direct Connect Gateway (die sich mit Tausenden von Verbindungen verbinden können VPCs) in verschiedenen AWS-Regionen und AWS-Konten über ein einziges Transit-VIF- und BGP-Peering zu verbinden. Dies ist die einfachste Konfiguration unter den Optionen für die Verbindung mehrerer Geräte VPCs in großem Maßstab, aber Sie sollten die Transit Gateway Gateway-Kontingente beachten. Eine wichtige Einschränkung, die es zu beachten gilt, besteht darin, dass Sie nur 200 Präfixe von einem Transit Gateway an einen lokalen Router über die Transit-VIF ankündigen können. Bei den vorherigen Optionen zahlen Sie für die Direct Connect-Preise. Für diese Option zahlen Sie auch die Gebühren für den Transit Gateway Gateway-Anschluss und die Datenverarbeitung. Weitere Informationen finden Sie in der Dokumentation Transit Gateway Associations on Direct Connect.
- Option 4: Stellen Sie eine VPN-Verbindung zu Transit Gateway über die öffentliche Direct Connect-VIF her — Eine öffentliche VIF ermöglicht Ihnen den Zugriff auf alle öffentlichen Dienste und Endpunkte von AWS über die öffentlichen IP-Adressen. Wenn Sie einen VPN-Anhang auf einem Transit Gateway erstellen, erhalten Sie auf AWS-Seite zwei öffentliche IP-Adressen für VPN-

Endpunkte. Diese öffentlichen IPs sind über das öffentliche VIF erreichbar. Sie können über Public VIF beliebig viele VPN-Verbindungen zu beliebig vielen Transit Gateway Gateway-Instanzen herstellen. Wenn Sie ein BGP-Peering über die öffentliche VIF erstellen, gibt AWS Ihrem Router den gesamten öffentlichen AWS-IP-Bereich bekannt. Um sicherzustellen, dass Sie nur bestimmten Datenverkehr zulassen (z. B. nur Datenverkehr zu den VPN-Terminierungsendpunkten zulassen), wird empfohlen, eine Firewall vor Ort zu verwenden. Diese Option kann verwendet werden, um Ihren Direct Connect auf Netzwerkebene zu verschlüsseln.

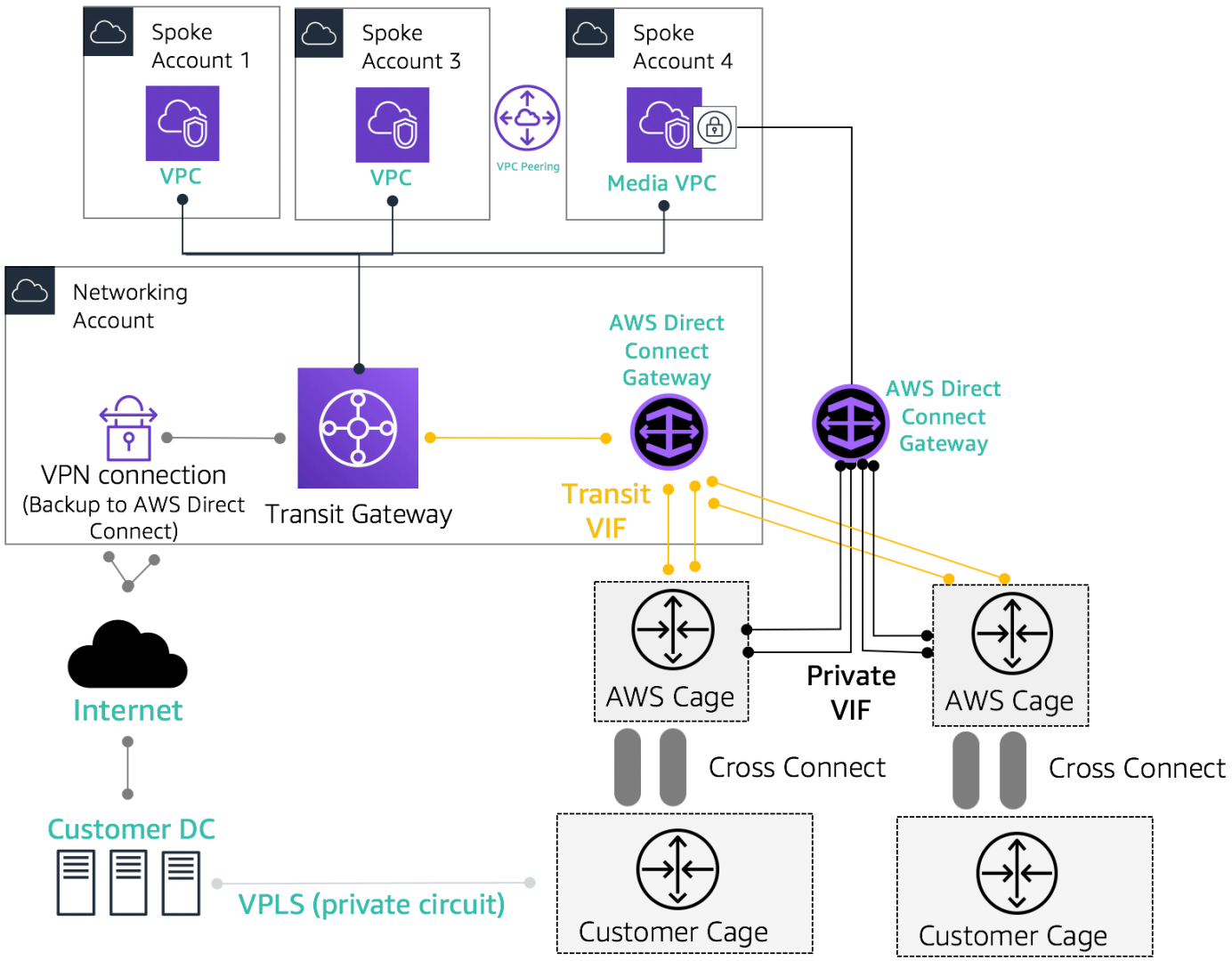
- Option 5: Stellen Sie Direct Connect mithilfe von Private IP VPN eine VPN-Verbindung zu Transit Gateway her — Private IP VPN ist eine Funktion, die Kunden die Möglichkeit bietet, Site-to-Site AWS-VPN-Verbindungen über Direct Connect mithilfe privater IP-Adressen bereitzustellen. Mit dieser Funktion können Sie den Datenverkehr zwischen Ihren lokalen Netzwerken und AWS über Direct Connect-Verbindungen verschlüsseln, ohne dass öffentliche IP-Adressen erforderlich sind, wodurch gleichzeitig die Sicherheit und der Netzwerkdatenschutz verbessert werden. Private IP VPN wird zusätzlich zu Transit bereitgestellt VIFs, sodass Sie Transit Gateway für die zentrale Verwaltung von Kunden VPCs und Verbindungen zu den lokalen Netzwerken auf sicherere, privatere und skalierbarere Weise verwenden können.
- Option 6: GRE-Tunnel zum Transit Gateway über eine Transit-VIF erstellen — Der Transit Gateway Connect-Anhangstyp unterstützt GRE. Mit Transit Gateway Connect kann die SD-WAN-Infrastruktur nativ mit AWS verbunden werden, ohne dass eine Einrichtung IPsec VPNs zwischen virtuellen SD-WAN-Netzwerkgeräten und Transit Gateway erforderlich ist. Die GRE-Tunnel können über eine Transit-VIF eingerichtet werden, wobei Transit Gateway Connect als Verbindungstyp verwendet wird, was im Vergleich zu einer VPN-Verbindung eine höhere Bandbreitenleistung bietet. Weitere Informationen finden Sie im Blogbeitrag Simplify SD-WAN connectivity with AWS Transit Gateway Connect.

Die Option „Transit-VIF zum Direct Connect-Gateway“ scheint die beste Option zu sein, da Sie damit Ihre gesamte lokale Konnektivität für einen bestimmten AWS-Region Punkt (Transit Gateway) mithilfe einer einzigen BGP-Sitzung pro Direct Connect-Verbindung konsolidieren können. Einige Einschränkungen und Überlegungen VIFs im Zusammenhang mit dieser Option können jedoch dazu führen, dass Sie für Ihre Landing Zone-Konnektivitätsanforderungen sowohl private als auch Transitverbindungen zusammen verwenden.

Die folgende Abbildung zeigt eine Beispielkonfiguration, bei der Transit-VIF als Standardmethode für die Verbindung verwendet wird VPCs und eine private VIF für einen Edge-Anwendungsfall verwendet wird, bei dem außergewöhnlich große Datenmengen von einem lokalen Rechenzentrum zur Medien-VPC übertragen werden müssen. Private VIF wird verwendet, um Datenverarbeitungsgebühren

für Transit Gateway zu vermeiden. Als bewährte Methode sollten Sie für maximale Redundanz mindestens zwei Verbindungen an zwei verschiedenen Direct Connect-Standorten haben — insgesamt also vier Verbindungen. Sie erstellen eine VIF pro Verbindung für insgesamt vier private VIFs und vier Transitverbindungen. VIFs Sie können auch ein VPN als Backup-Konnektivität für Direct Connect Verbindungen erstellen.

Mit der Option „GRE-Tunnel zum Transit Gateway über eine Transit-VIF erstellen“ erhalten Sie die Möglichkeit, Ihre SD-WAN-Infrastruktur nativ mit AWS zu verbinden. Dadurch entfällt die Notwendigkeit, IPsec VPNs zwischen virtuellen SD-WAN-Netzwerkgeräten und Transit Gateway einzurichten.



Beispiel für eine Referenzarchitektur für Hybridkonnektivität

Verwenden Sie das Network Services-Konto, um Direct Connect-Ressourcen zu erstellen, die die Abgrenzung der Netzwerkadministrationsgrenzen ermöglichen. Die Direct Connect-Verbindungen, Direct Connect-Gateways und Transit-Gateways können sich alle in einem Network Services-Konto befinden. Um die Direct Connect Konnektivität mit Ihrer Landing Zone zu teilen, teilen Sie das Transit Gateway einfach AWS RAM mit anderen Konten.

MACsec Sicherheit bei Direct Connect-Verbindungen

Kunden können die MAC Security Standard (MACsec) -Verschlüsselung (IEEE 802.1AE) mit ihren Direct Connect-Verbindungen für dedizierte Verbindungen mit 10 Gbit/s und 100 Gbit/s an ausgewählten Standorten verwenden. Mit dieser Funktion können Kunden ihre Daten auf Layer-2-Ebene sichern, und Direct Connect bietet point-to-point Verschlüsselung. Um die Direct MACsec Connect-Funktion zu aktivieren, stellen Sie sicher, dass die MACsec Voraussetzungen erfüllt sind. Da Links auf einer bestimmten hop-by-hop Basis MACsec geschützt werden, muss Ihr Gerät über eine direkte Layer-2-Nachbarschaft zu unserem Direct Connect-Gerät verfügen. Ihr Last-Mile-Anbieter kann Ihnen dabei helfen, zu überprüfen, ob Ihre Verbindung mit funktioniert. MACsec Weitere Informationen finden Sie unter Hinzufügen von MACsec Sicherheit zu AWS Direct Connect Connect-Verbindungen.

Direct Connect Empfehlungen zur Resilienz

Mit Direct Connect können Kunden über ihre lokalen Netzwerke eine äußerst stabile Konnektivität zu ihren Amazon VPCs - und AWS-Ressourcen erreichen. Es hat sich bewährt, dass Kunden von mehreren Rechenzentren aus Verbindungen herstellen, um Ausfälle einzelner physischer Standorte zu vermeiden. Es wird außerdem empfohlen, dass Kunden je nach Art der Workloads aus Redundanzgründen mehr als eine Direct Connect-Verbindung verwenden.

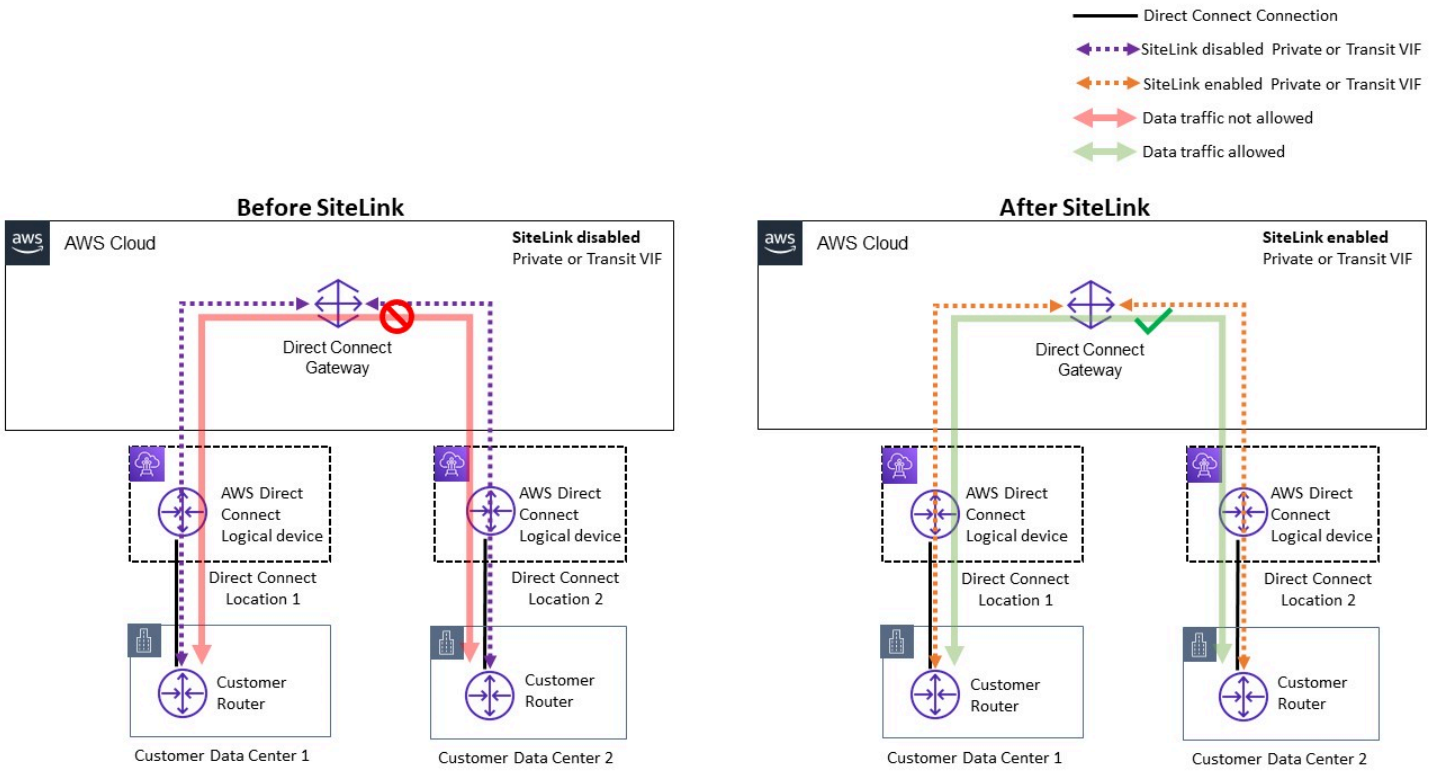
AWS bietet auch das Direct Connect Resiliency Toolkit an, das Kunden einen Verbindungsassistenten mit mehreren Redundanzmodellen zur Verfügung stellt, der ihnen hilft, herauszufinden, welches Modell für ihre Service Level Agreements (SLA) am besten geeignet ist, und ihre Hybridkonnektivität mithilfe von Direct Connect-Verbindungen entsprechend zu gestalten. Weitere Informationen finden Sie unter Resiliency Recommendations.Direct Connect

Direct Connect SiteLink

Bisher war die Konfiguration von site-to-site Links für Ihre lokalen Netzwerke nur durch direkten Verbindungsaufbau über Glasfaser oder andere Technologien, IPSEC VPNs, oder durch den Einsatz von Drittanbietern mit Technologien wie MPLS oder älteren T1-Verbindungen möglich. MetroEthernet

Mit dem Aufkommen von können Kunden nun direkte site-to-site Konnektivität für ihren lokalen Standort aktivieren SiteLink, die an einem Standort endet. Direct Connect Verwenden Sie Ihre Direct Connect, um site-to-site Konnektivität bereitzustellen, ohne den Datenverkehr durch Ihre Leitung leiten zu müssen VPCs, wodurch die AWS-Region vollständig umgangen wird.

Jetzt können Sie globale, zuverlässige pay-as-you-go Verbindungen zwischen den Niederlassungen und Rechenzentren in Ihrem globalen Netzwerk herstellen, indem Sie Daten über den schnellsten Weg zwischen Direct Connect Standorten senden.

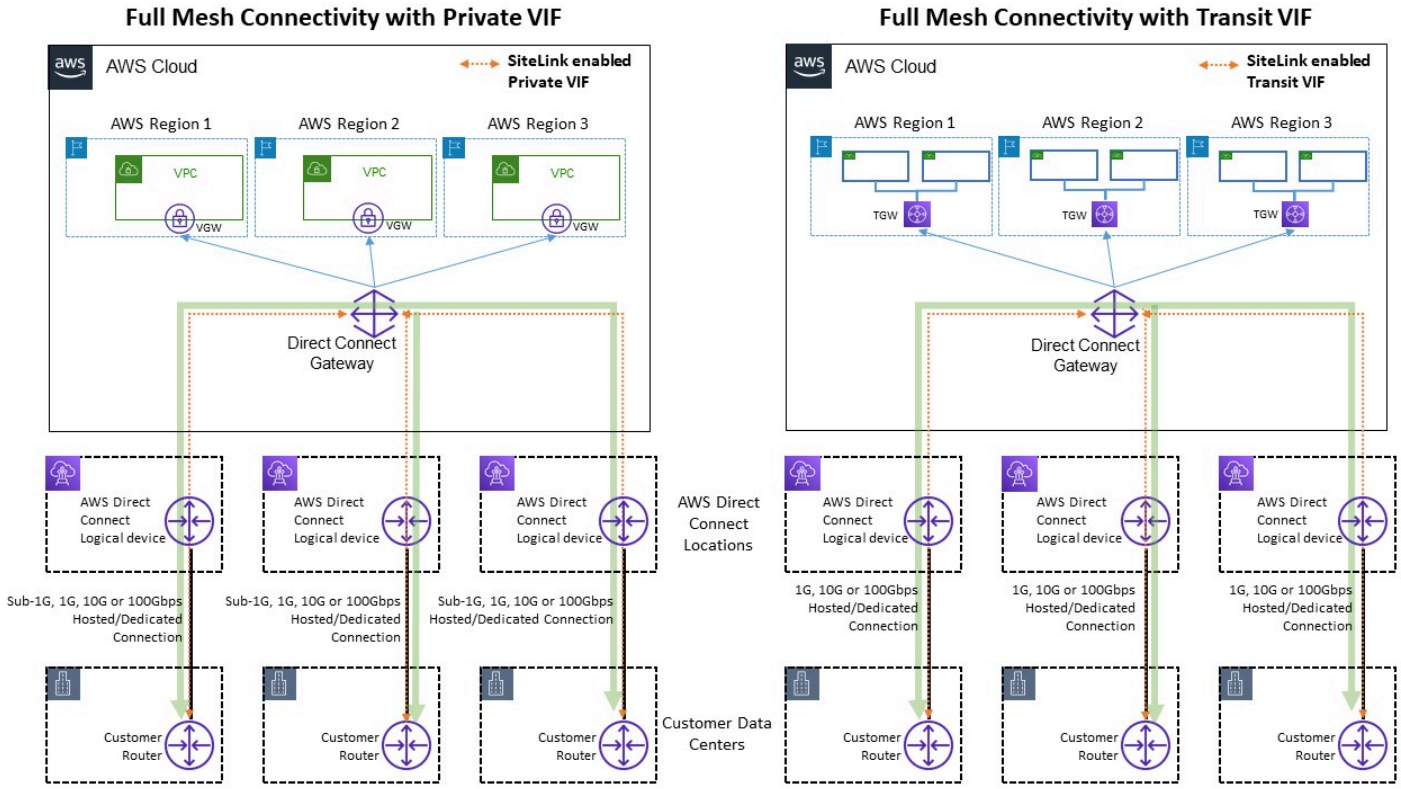


Beispiel für eine Referenzarchitektur für Direct Connect SiteLink

Bei der Nutzung SiteLink verbinden Sie zunächst Ihre lokalen Netzwerke mit AWS an einem der über 100 Direct Connect Standorte weltweit. Anschließend erstellen Sie virtuelle Schnittstellen (VIFs) für diese Verbindungen und aktivieren sie SiteLink. Sobald alle an dasselbe Direct Connect Gateway (DXGW) angeschlossen VIFs sind, können Sie damit beginnen, Daten zwischen ihnen zu senden. Ihre Daten folgen dem kürzesten Weg zwischen den Direct Connect Standorten zum Ziel und nutzen dabei das schnelle, sichere und zuverlässige globale AWS-Netzwerk. Sie benötigen keinerlei Ressourcen, um sie nutzen AWS-Region zu können SiteLink.

Mit SiteLink, das DXGW lernt IPv4 IPv6 /-Präfixe von Ihren Routern über SiteLink aktiviert VIFs, führt den BGP-Best-Path-Algorithmus aus, aktualisiert Attribute wie NextHop und as_Path und gibt diese

BGP-Präfixe erneut an den Rest Ihrer -enabled weiter, die mit diesem DXGW verknüpft sind. SiteLink VIFs Wenn Sie die Option SiteLink auf einem VIF deaktivieren, gibt das DXGW die erlernten lokalen Präfixe nicht an das andere -aktivierte VIF weiter. SiteLink VIFs Die lokalen Präfixe einer SiteLink deaktivierten VIF werden nur den DXGW Gateway-Zuordnungen bekannt gegeben, z. B. AWS Virtual Private Gateways (VGWs) - oder Transit Gateway (TGW) -Instances, die dem DXGW zugeordnet sind.



Beispiel für Sitelink ermöglicht Verkehrsflüsse

SiteLink ermöglicht es Kunden, das globale AWS-Netzwerk als primäre oder sekundäre/Backup-Verbindung zwischen ihren Remote-Standorten zu nutzen, mit hoher Bandbreite und geringer Latenz, mit dynamischem Routing zur Steuerung, welche Standorte miteinander und mit Ihren regionalen AWS-Ressourcen kommunizieren können.

Weitere Informationen finden Sie unter Einführung. Direct Connect SiteLink

Zentralisierter Zugang zum Internet

Wenn Sie Anwendungen in Ihrer Umgebung mit mehreren Konten bereitstellen, benötigen viele Apps nur ausgehenden Internetzugang (z. B. das Herunterladen von Bibliotheken, Patches oder Betriebssystemupdates). Dies kann sowohl für den Datenverkehr als auch für den Datenverkehr erreicht werden. IPv4 IPv6 Denn IPv4 dies kann durch Network Address Translation (NAT) in Form eines NAT-Gateways (empfohlen) oder alternativ durch eine selbstverwaltete NAT-Instance, die auf einer EC2 Amazon-Instance ausgeführt wird, als Mittel für den gesamten ausgehenden Internetzugang erreicht werden. Interne Anwendungen befinden sich in privaten Subnetzen, während sich NAT-Gateways und Amazon EC2 NAT-Instances in einem öffentlichen Subnetz befinden.

AWS empfiehlt die Verwendung von NAT-Gateways, da diese eine bessere Verfügbarkeit und Bandbreite bieten und weniger Verwaltungsaufwand Ihrerseits erfordern. Weitere Informationen finden Sie unter Vergleich von NAT-Gateways und NAT-Instances.

Für den IPv6 Datenverkehr kann der ausgehende Datenverkehr so konfiguriert werden, dass jede VPC dezentral über ein Internet-Gateway nur für ausgehenden Verkehr verlassen wird, oder er kann so konfiguriert werden, dass er mithilfe von NAT-Instances oder Proxy-Instances an eine zentrale VPC gesendet wird. Die IPv6 Muster werden unter erörtert. Zentralisierter Ausgang für IPv6

Themen

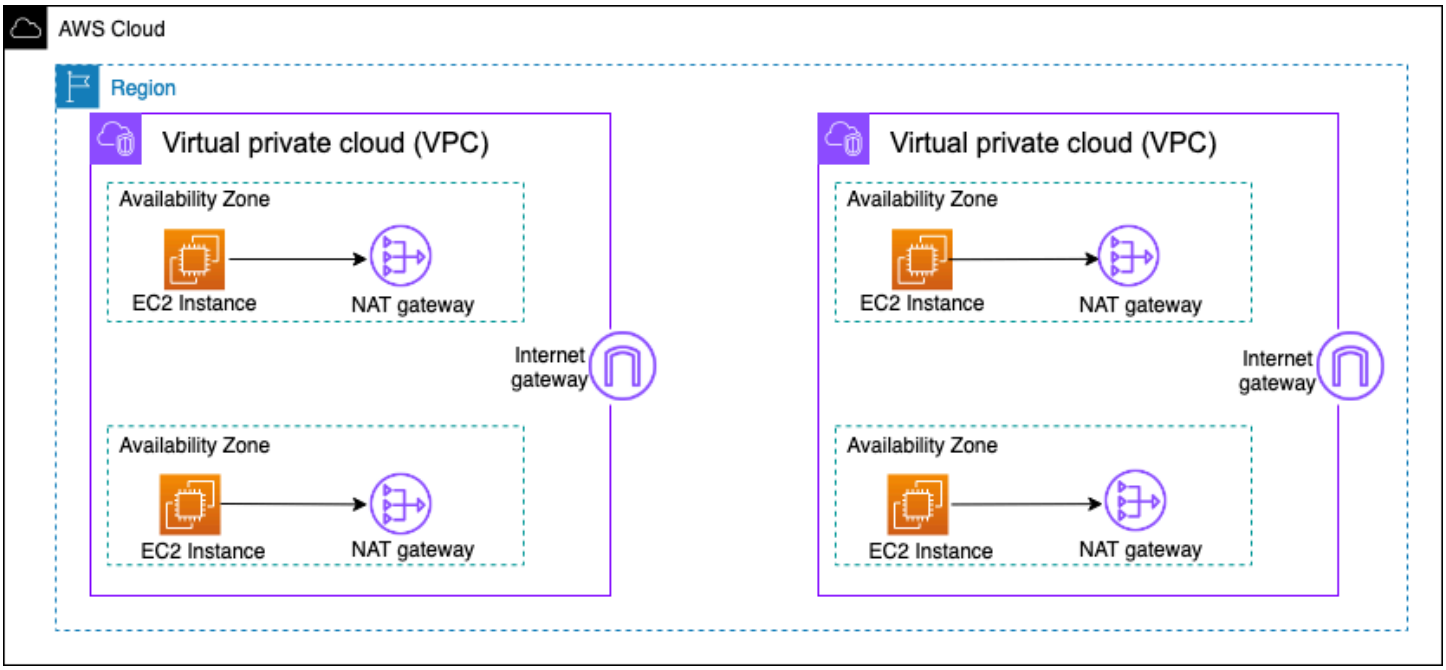
- Verwenden des NAT-Gateways für den zentralisierten IPv4 Ausgang
- Verwenden des NAT-Gateways mit AWS Network Firewall für den zentralisierten IPv4 Ausgang
- Verwenden des NAT-Gateways und des Gateway Load Balancer mit EC2 Amazon-Instances für den zentralisierten Ausgang IPv4
- Zentralisierter Ausgang für IPv6

Verwenden des NAT-Gateways für den zentralisierten IPv4 Ausgang

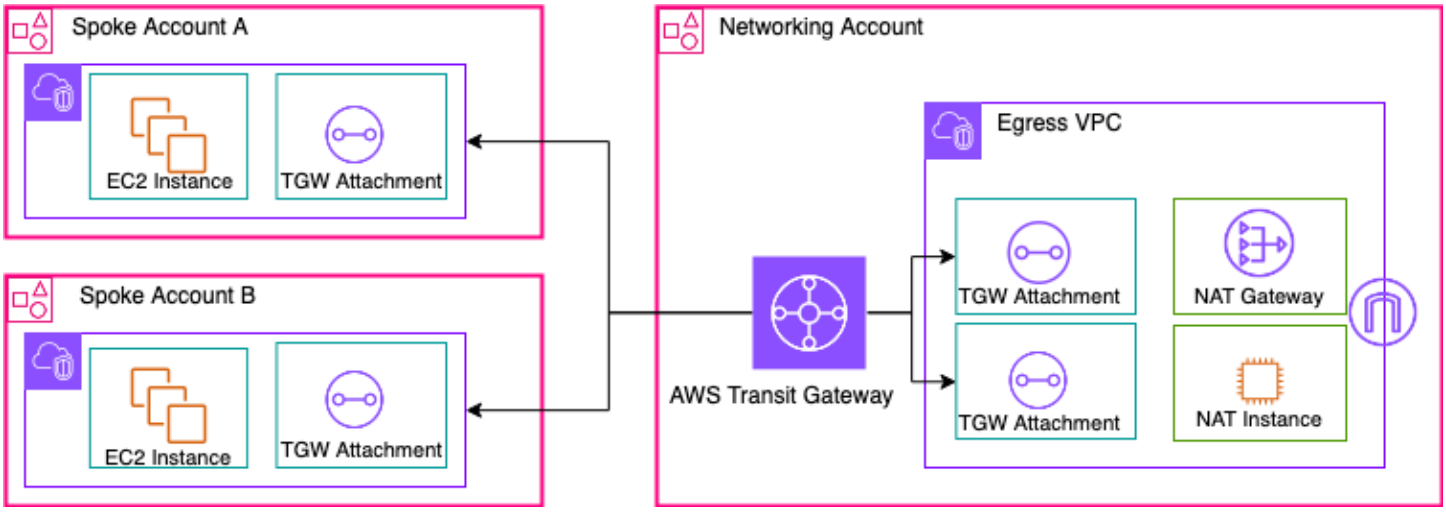
Das NAT-Gateway ist ein verwalteter Übersetzungsdienst für Netzwerkadressen. Die Bereitstellung eines NAT-Gateways in jeder Spoke-VPC kann unerschwinglich werden, da Sie für jedes bereitgestellte NAT-Gateway eine stündliche Gebühr zahlen (siehe Amazon VPC-Preise). Die Zentralisierung von NAT-Gateways kann eine praktikable Option zur Kostensenkung sein. Zur Zentralisierung erstellen Sie eine separate Ausgangs-VPC im Netzwerkdienstkonto, stellen NAT-

Gateways in der Ausgangs-VPC bereit und leiten den gesamten Ausgangsdatenverkehr von der Spoke VPCs zu den NAT-Gateways in der Ausgangs-VPC mithilfe von Transit Gateway oder CloudWAN weiter, wie in der folgenden Abbildung dargestellt.

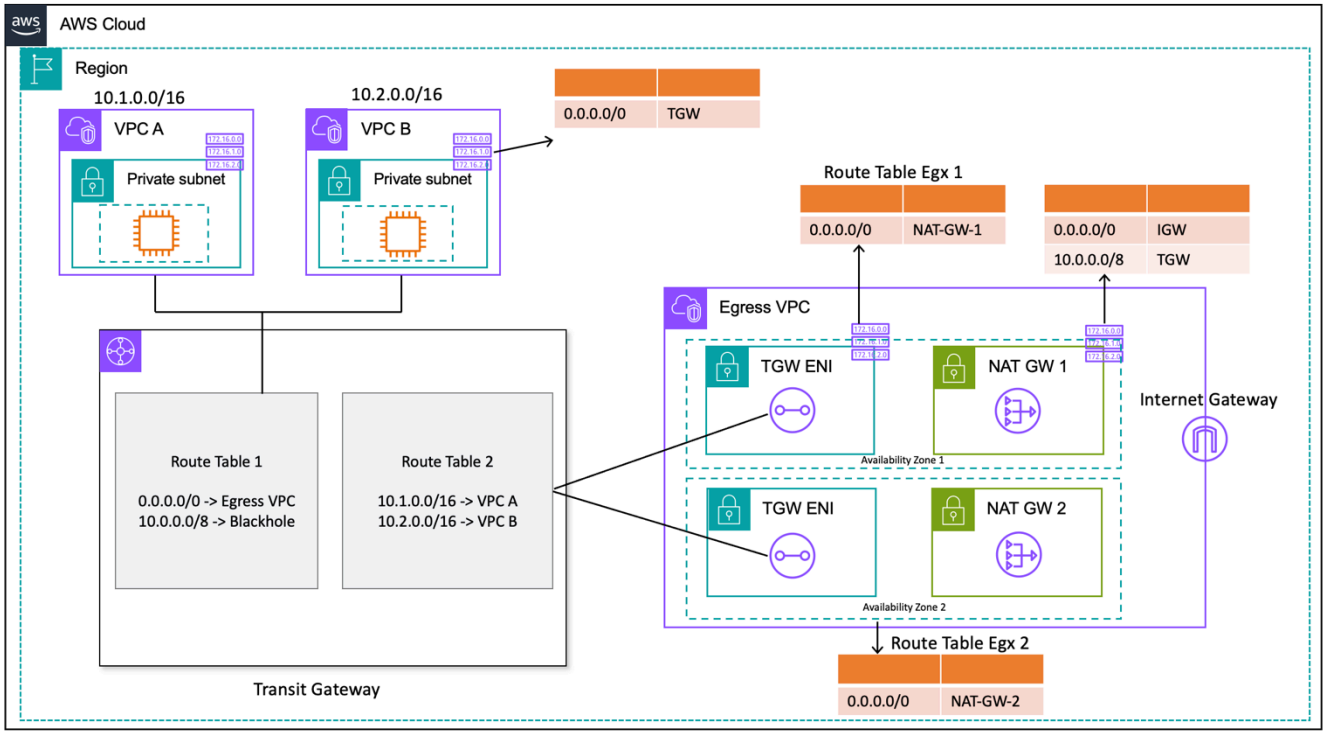
> **Note**
>
> Wenn Sie das NAT-Gateway mithilfe von Transit Gateway zentralisieren, zahlen Sie eine zusätzliche Transit-Gateway-Datenverarbeitungsgebühr — verglichen mit dem dezentralen Ansatz, bei dem in jeder VPC ein NAT-Gateway betrieben wird. In einigen Randfällen, in denen Sie riesige Datenmengen über ein NAT-Gateway von einer VPC aus senden, kann es kostengünstiger sein, das NAT lokal in der VPC beizubehalten, um die Transit Gateway Gateway-Datenverarbeitungsgebühren zu vermeiden.



Dezentrale NAT-Gateway-Architektur mit hoher Verfügbarkeit



Zentralisiertes NAT-Gateway mit Transit Gateway (Überblick)



Zentralisiertes NAT-Gateway mit Transit Gateway (Routentabellendesign)

In diesem Setup werden Spoke-VPC-Anlagen mit Route Table 1 (RT1) verknüpft und an Route Table 2 (RT2) weitergegeben. Es gibt eine Blackhole-Route, die verhindert, dass die beiden VPCs miteinander kommunizieren. Wenn Sie die Kommunikation zwischen VPC zulassen möchten, können Sie den `10.0.0.0/8 -> Blackhole` Routeneintrag von entfernen. RT1 Dadurch können sie über das Transit-Gateway kommunizieren. Sie können die Spoke-VPC-Anlagen auch an weitergeben RT1 (oder alternativ können Sie eine Routing-Tabelle verwenden und alles damit assoziieren/

propagieren), wodurch ein direkter Datenfluss zwischen den verwendeten Transit Gateway ermöglicht wird. VPCs

Sie fügen eine statische Route hinzu, indem Sie den RT1 gesamten Datenverkehr auf die ausgehende VPC weiterleiten. Aufgrund dieser statischen Route sendet Transit Gateway den gesamten Internetverkehr über seine ENIs in der Ausgangs-VPC. Sobald der Verkehr in der Ausgangs-VPC angekommen ist, folgt er den Routen, die in der Subnetz-Routentabelle definiert sind, wo diese Transit Gateway vorhanden sind. ENIs Sie fügen in Subnetz-Routentabellen eine Route hinzu, die den gesamten Datenverkehr auf das jeweilige NAT-Gateway in derselben Availability Zone (AZ) lenkt, um den Verkehr in der Cross-Availability Zone (AZ) zu minimieren. In der Tabelle der NAT-Gateway-Subnetz-Routings ist das Internet-Gateway (IGW) als nächsten Hop angegeben. Damit der Rückverkehr zurückfließen kann, müssen Sie einen Eintrag in der Tabelle mit der statischen Routingtabelle für das Routing des NAT-Gateways hinzufügen, der den gesamten an Spoke VPC gebundenen Verkehr als nächsten Hop auf Transit Gateway verweist.

Hohe Verfügbarkeit

Für eine hohe Verfügbarkeit sollten Sie mehr als ein NAT-Gateway verwenden (eines in jeder Availability Zone). Wenn ein NAT-Gateway nicht verfügbar ist, wird der Verkehr in der Availability Zone, die das betroffene NAT-Gateway durchquert, möglicherweise unterbrochen. Wenn eine Availability Zone nicht verfügbar ist, fallen der Transit Gateway-Endpunkt zusammen mit dem NAT-Gateway in dieser Availability Zone aus, und der gesamte Datenverkehr fließt über die Transit Gateway- und NAT-Gateway-Endpunkte in der anderen Availability Zone.

Sicherheit

Sie können sich auf Sicherheitsgruppen auf den Quell-Instances, Blackhole-Routen in den Transit Gateway Gateway-Routentabellen und die Netzwerk-ACL des Subnetzes verlassen, in dem sich das NAT-Gateway befindet. Beispielsweise können Kunden öffentliche Subnetze ACLs auf dem NAT Gateway verwenden, um Quell- oder Ziel-IP-Adressen zuzulassen oder zu blockieren. Alternativ können Sie NAT Gateway mit AWS Network Firewall für den zentralisierten Ausgang verwenden, wie im nächsten Abschnitt beschrieben, um diese Anforderung zu erfüllen.

Skalierbarkeit

Ein einzelnes NAT-Gateway kann bis zu 55.000 gleichzeitige Verbindungen pro zugewiesener IP-Adresse zu jedem eindeutigen Ziel unterstützen. Sie können eine Kontingentanpassung beantragen, um bis zu acht zugewiesene IP-Adressen zuzulassen, sodass 440.000 gleichzeitige Verbindungen

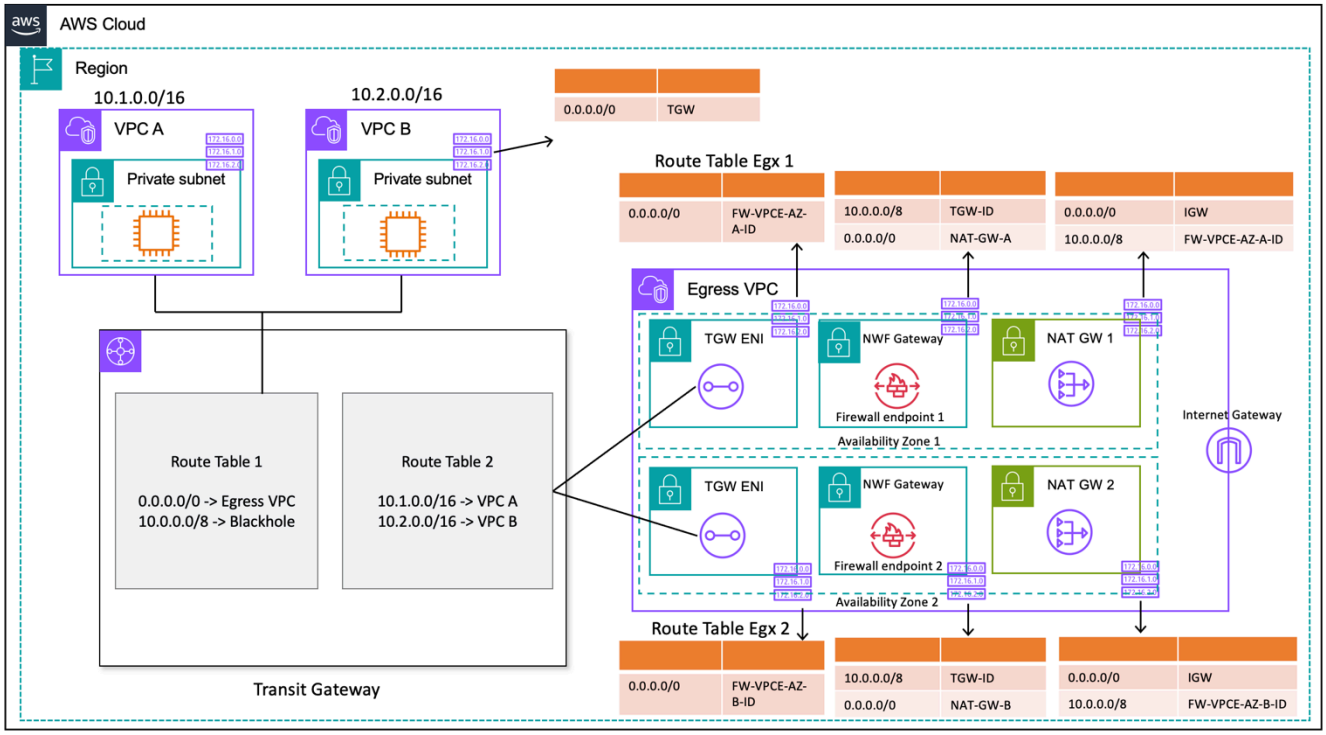
zu einer einzigen Ziel-IP und einem einzigen Zielport möglich sind. Das NAT-Gateway bietet eine Bandbreite von 5 Gbit/s und skaliert automatisch auf 100 Gbit/s. Transit Gateway fungiert im Allgemeinen nicht als Load Balancer und verteilt Ihren Datenverkehr nicht gleichmäßig auf die NAT-Gateways in den verschiedenen Availability Zones. Der Verkehr über das Transit Gateway bleibt, wenn möglich, innerhalb einer Availability Zone. Wenn sich die EC2 Amazon-Instance, die den Verkehr initiiert, in Availability Zone 1 befindet, fließt der Datenverkehr aus der elastic network interface von Transit Gateway in derselben Availability Zone 1 in der Ausgangs-VPC und fließt auf der Grundlage der Subnetz-Routentabelle, in der sich die Elastic Network-Schnittstelle befindet, zum nächsten Hop. Eine vollständige Liste der Regeln finden Sie unter NAT-Gateways in der Amazon Virtual Private Cloud Cloud-Dokumentation.

Weitere Informationen finden Sie im Blogbeitrag Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway.

Verwenden des NAT-Gateways mit AWS Network Firewall für den zentralisierten IPv4 Ausgang

Wenn Sie Ihren ausgehenden Datenverkehr überprüfen und filtern möchten, können Sie die AWS-Netzwerk-Firewall mit NAT-Gateway in Ihre zentralisierte Ausgangsarchitektur integrieren. AWS Network Firewall ist ein verwalteter Service, der es einfach macht, wichtige Netzwerkschutzmaßnahmen für all Ihre Benutzer bereitzustellen. VPCs Es bietet Kontrolle und Transparenz für den Netzwerkverkehr der Schichten 3-7 für Ihre gesamte VPC. Sie können URL-/Domainnamen, IP-Adressen und inhaltsbasierte Filterung des ausgehenden Datenverkehrs durchführen, um möglichen Datenverlust zu verhindern, Compliance-Anforderungen zu erfüllen und bekannte Malware-Kommunikation zu blockieren. AWS Network Firewall unterstützt Tausende von Regeln, mit denen Netzwerkverkehr herausgefiltert werden kann, der für bekanntermaßen schlechte IP-Adressen oder schädliche Domainnamen bestimmt ist. Sie können Suricata-IPS-Regeln auch als Teil des AWS Network Firewall Dienstes verwenden, indem Sie Open-Source-Regelsätze importieren oder Ihre eigenen IPS-Regeln (Intrusion Prevention System) mithilfe der Suricata-Regelsyntax erstellen. AWS Network Firewall ermöglicht es Ihnen auch, kompatible Regeln von AWS-Partnern zu importieren.

In der zentralisierten Ausgangsarchitektur mit Inspektion ist der AWS Network Firewall Endpunkt ein Standard-Routing-Tabellenziel in der Subnetz-Routentabelle für Transit-Gateway-Anlagen für die Ausgangs-VPC. Der Datenverkehr zwischen Spoke VPCs und dem Internet wird AWS Network Firewall wie in der folgenden Abbildung dargestellt überprüft.



Zentralisierter Ausgang mit einem AWS Network Firewall NAT-Gateway (Routing-Tabellen-Design)

Für ein zentralisiertes Bereitstellungsmodell mit Transit Gateway empfiehlt AWS die Bereitstellung von AWS Network Firewall Endpunkten in mehreren Availability Zones. In jeder Availability Zone, in der der Kunde Workloads ausführt, sollte es einen Firewall-Endpunkt geben, wie im vorherigen Diagramm dargestellt. Es hat sich bewährt, dass das Firewall-Subnetz keinen anderen Datenverkehr enthalten sollte, da AWS Network Firewall es nicht in der Lage ist, den Verkehr von Quellen oder Zielen innerhalb eines Firewall-Subnetzes zu untersuchen.

Ähnlich wie bei der vorherigen Konfiguration sind Spoke-VPC-Anlagen mit Route Table 1 (RT1) verknüpft und werden an Route Table 2 (RT2) weitergegeben. Eine Blackhole-Route wird ausdrücklich hinzugefügt, um zu verhindern, dass die beiden VPCs miteinander kommunizieren.

Verwenden Sie weiterhin eine Standardroute, um den gesamten RT1 Datenverkehr auf die ausgehende VPC weiterzuleiten. Transit Gateway leitet alle Verkehrsflüsse an eine der beiden Availability Zones in der Egress-VPC weiter. Sobald der Verkehr eines der Transit Gateway ENIs in der Ausgangs-VPC erreicht, treffen Sie auf eine Standardroute, die den Verkehr an einen der AWS Network Firewall Endpunkte in der jeweiligen Availability Zone weiterleitet. AWS Network Firewall untersucht dann den Datenverkehr anhand der von Ihnen festgelegten Regeln, bevor der Verkehr über eine Standardroute an das NAT-Gateway weitergeleitet wird.

In diesem Fall ist der Transit Gateway Gateway-Appliance-Modus nicht erforderlich, da Sie keinen Datenverkehr zwischen Anhängen senden.

> **Note**
>
> AWS Network Firewall führt keine Netzwerkadressübersetzung für Sie durch. Diese Funktion würde vom NAT-Gateway nach der Überprüfung des Datenverkehrs durch die ausgeführt AWS Network Firewall. Ingress-Routing ist in diesem Fall nicht erforderlich, da der Rückverkehr standardmäßig an das NATGW IPs weitergeleitet wird.

Da Sie ein Transit Gateway verwenden, können wir hier die Firewall vor dem NAT-Gateway platzieren. In diesem Modell kann die Firewall die Quell-IP hinter dem Transit Gateway erkennen.

Wenn Sie dies in einer einzelnen VPC getan haben, können wir die VPC-Routing-Verbesserungen verwenden, mit denen Sie den Verkehr zwischen Subnetzen in derselben VPC überprüfen können. Einzelheiten finden Sie im Blogbeitrag Deployment Models for AWS Network Firewall with VPC Routing Enhancements.

Skalierbarkeit

AWS Network Firewall kann die Firewall-Kapazität je nach Verkehrslast automatisch nach oben oder unten skalieren, um eine konstante, vorhersehbare Leistung aufrechtzuerhalten und so die Kosten zu minimieren. AWS Network Firewall ist so konzipiert, dass es Zehntausende von Firewallregeln unterstützt und einen Durchsatz von bis zu 100 Gbit/s pro Availability Zone ermöglicht.

Die wichtigsten Überlegungen

- Jeder Firewall-Endpunkt kann etwa 100 Gbit/s Datenverkehr verarbeiten. Wenn Sie einen höheren Burst- oder Dauerdurchsatz benötigen, wenden Sie sich an den AWS-Support.
- Wenn Sie sich dafür entscheiden, in Ihrem AWS-Konto zusammen mit der Network Firewall ein NAT-Gateway zu erstellen, werden die standardmäßigen Gebühren für die NAT-Gateway-Verarbeitung und die Nutzung pro Stunde auf der one-to-one Grundlage der Verarbeitung pro GB und der Nutzungsstunden für Ihre Firewall erlassen.
- Sie können auch verteilte Firewall-Endpunkte AWS Firewall Manager ohne Transit Gateway in Betracht ziehen.
- Testen Sie Firewallregeln, bevor Sie sie in die Produktionsumgebung überführen, ähnlich wie bei einer Netzwerkzugriffskontrollliste, da die Reihenfolge wichtig ist.

- Für eine genauere Prüfung sind erweiterte Suricata-Regeln erforderlich. Die Netzwerk-Firewall unterstützt die Überprüfung des verschlüsselten Datenverkehrs sowohl für eingehenden als auch für ausgehenden Datenverkehr.
- Die `HOME_NET` Regelgruppenvariable definierte den Quell-IP-Bereich, der für die Verarbeitung in der Stateful Engine in Frage kommt. Bei einem zentralisierten Ansatz müssen Sie alle zusätzlichen VPC hinzufügen, die an das Transit Gateway CIDRs angeschlossen sind, damit sie verarbeitet werden können. Weitere Informationen zur `HOME_NET` Regelgruppenvariablen finden Sie in der Dokumentation zur Network Firewall.
- Erwägen Sie die Bereitstellung von Transit Gateway und ausgehender VPC in einem separaten Netzwerkdienstkonto, um den Zugriff auf der Grundlage der Delegierung von Aufgaben zu trennen. Beispielsweise können nur Netzwerkadministratoren auf das Network Services-Konto zugreifen.
- Um die Bereitstellung und Verwaltung von AWS Network Firewall zu vereinfachen, AWS Firewall Manager kann dieses Modell verwendet werden. Mit Firewall Manager können Sie Ihre verschiedenen Firewalls zentral verwalten, indem der Schutz, den Sie am zentralen Ort erstellt haben, automatisch auf mehrere Konten angewendet wird. Firewall Manager unterstützt sowohl verteilte als auch zentralisierte Bereitstellungsmodelle für Network Firewall. Weitere Informationen finden Sie im Blogbeitrag How to deploy AWS Network Firewall by using AWS Firewall Manager.

Verwenden des NAT-Gateways und des Gateway Load Balancer mit EC2 Amazon-Instances für den zentralisierten Ausgang IPv4

Die Verwendung einer softwarebasierten virtuellen Appliance (bei Amazon EC2) von AWS Marketplace und AWS Partner Network als Ausgangspunkt ähnelt dem NAT-Gateway-Setup. Diese Option kann verwendet werden, wenn Sie die erweiterten Layer-7- und Deep-Packet-Inspection-Funktionen der verschiedenen Anbieter nutzen möchten. rewall/Intrusion Prevention/Detection System (IPS/IDS

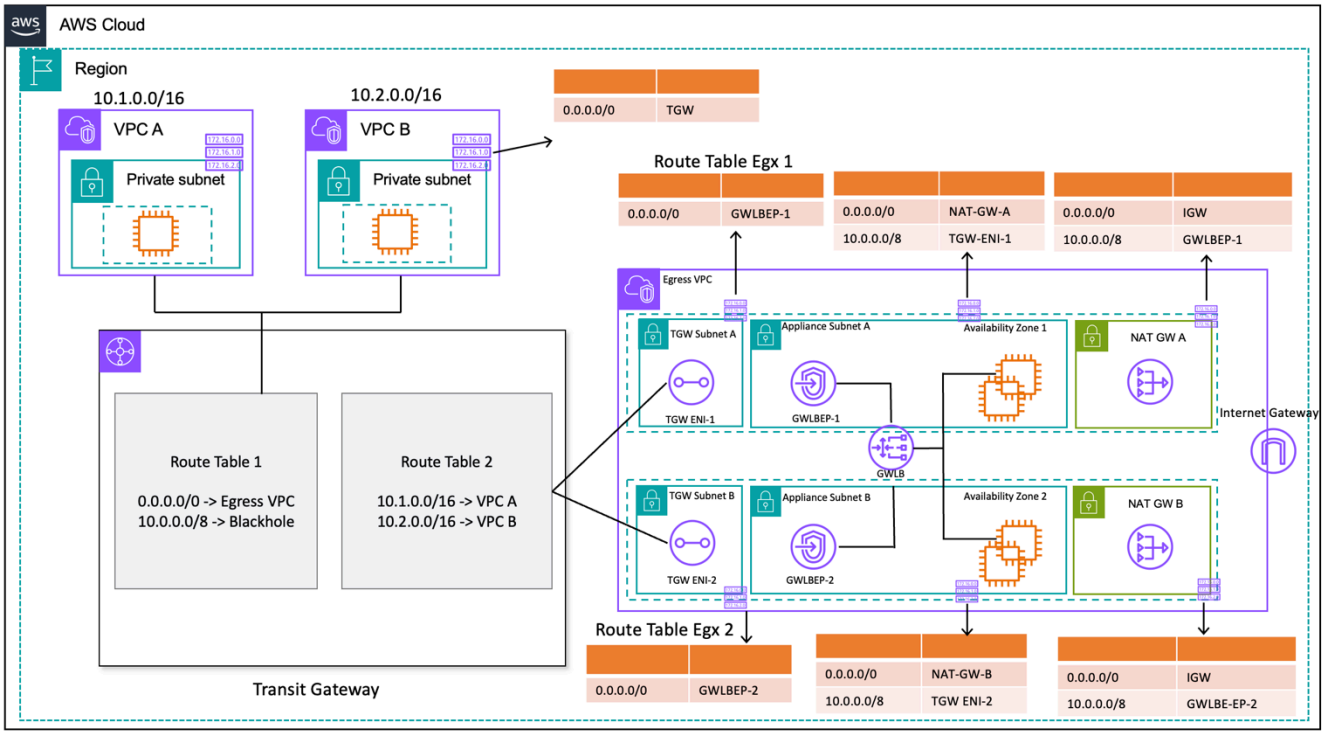
In der folgenden Abbildung stellen Sie zusätzlich zum NAT-Gateway virtuelle Appliances mithilfe von EC2 Instanzen hinter einem Gateway Load Balancer (GWLB) bereit. In diesem Setup werden GWLB, Gateway Load Balancer Endpoint (GWLBE), virtuelle Appliances und NAT-Gateways in einer zentralen VPC bereitgestellt, die über eine VPC-Verbindung mit dem Transit Gateway verbunden ist. Die Spokes VPCs sind auch über einen VPC-Anhang mit dem Transit Gateway verbunden. Da GWLBEs es sich um ein routingfähiges Ziel handelt, können Sie den Datenverkehr, der zu und vom Transit Gateway fließt, zur Flotte virtueller Appliances weiterleiten, die als Ziele hinter einem GWLB konfiguriert sind. GWLB fungiert als bump-in-the-wire und leitet den gesamten Layer-3-Verkehr

transparent über virtuelle Appliances von Drittanbietern weiter und ist somit für Quelle und Ziel des Datenverkehrs unsichtbar. Daher ermöglicht Ihnen diese Architektur, Ihren gesamten ausgehenden Verkehr, der über Transit Gateway fließt, zentral zu überprüfen.

Weitere Informationen darüber, wie der Datenverkehr durch dieses Setup von den Anwendungen in das VPCs Internet und zurück fließt, finden Sie unter Centralized Inspection Architecture with AWS Gateway Load Balancer und AWS Transit Gateway.

Sie können den Appliance-Modus auf dem Transit Gateway aktivieren, um die Flusssymetrie durch virtuelle Appliances aufrechtzuerhalten. Das bedeutet, dass der bidirektionale Verkehr während der gesamten Lebensdauer des Datenflusses über dieselbe Appliance und die Availability Zone geleitet wird. Diese Einstellung ist besonders wichtig für Stateful-Firewalls, die Deep Packet Inspection durchführen. Durch die Aktivierung des Appliance-Modus sind keine komplexen Behelfslösungen mehr erforderlich, wie z. B. die Übersetzung von Quellnetzadressen (Source Network Address Translation, SNAT), um den Datenverkehr zur korrekten Appliance zurückzukehren, um die Symmetrie aufrechtzuerhalten. Einzelheiten finden Sie unter Bewährte Methoden für die Bereitstellung von Gateway Load Balancer.

Es ist auch möglich, GWLB-Endpunkte verteilt ohne Transit Gateway bereitzustellen, um die Ausgangsinspektion zu ermöglichen. Weitere Informationen zu diesem Architekturmuster finden Sie im Blogbeitrag Introducing AWS Gateway Load Balancer: Unterstützte Architekturmuster.



Zentralisierter Ausgang mit Gateway Load Balancer und EC2 Instanz (Routentabellendesign)

Hohe Verfügbarkeit

AWS empfiehlt für eine höhere Verfügbarkeit den Einsatz von Gateway Load Balancers und virtuellen Appliances in mehreren Availability Zones.

Gateway Load Balancer kann Integritätsprüfungen durchführen, um Ausfälle virtueller Appliances zu erkennen. Im Falle einer fehlerhaften Appliance leitet GWLB die neuen Datenflüsse an fehlerfreie Appliances weiter. Bestehende Datenflüsse werden unabhängig vom Status des Ziels immer an dasselbe Ziel weitergeleitet. Auf diese Weise können Verbindungen verloren gehen und Fehler bei der Integritätsprüfung aufgrund von CPU-Spitzen auf Appliances ausgeglichen werden. Weitere Informationen finden Sie in Abschnitt 4: Grundlegendes zu Ausfallszenarien für Appliances und Availability Zones im Blogbeitrag Bewährte Methoden für die Bereitstellung von Gateway Load Balancer. Gateway Load Balancer kann Auto Scaling-Gruppen als Ziele verwenden. Dieser Vorteil macht die Verwaltung der Verfügbarkeit und Skalierbarkeit der Appliance-Flotten überflüssig.

Vorteile

Gateway Load Balancer und Gateway Load Balancer werden mit Strom versorgt AWS PrivateLink, was den sicheren Austausch von Datenverkehr über VPC-Grenzen hinweg ermöglicht, ohne dass das öffentliche Internet durchquert werden muss.

Gateway Load Balancer ist ein verwalteter Service, der die undifferenzierte Schwerstarbeit bei der Verwaltung, Bereitstellung und Skalierung virtueller Sicherheitsanwendungen überflüssig macht, sodass Sie sich auf die wichtigen Dinge konzentrieren können. Gateway Load Balancer kann den Firewall-Stapel als Endpunktdienst bereitstellen, den Kunden über den abonnieren können. AWS Marketplace Dies wird als Firewall as a Service (FWaaS) bezeichnet. Es ermöglicht eine vereinfachte Bereitstellung und macht es überflüssig, sich bei der Verteilung des Datenverkehrs auf mehrere EC2 Amazon-Instances auf BGP und ECMP zu verlassen.

Die wichtigsten Überlegungen

- Die Appliances müssen das Geneve-Kapselungsprotokoll unterstützen, um in GWLB integriert werden zu können.
- Einige Appliances von Drittanbietern können SNAT und Overlay-Routing (Two-Arm-Modus) unterstützen, sodass aus Kostengründen keine NAT-Gateways erstellt werden müssen. Wenden Sie sich jedoch an einen AWS-Partner Ihrer Wahl, bevor Sie diesen Modus verwenden, da dies vom Support und der Implementierung des Anbieters abhängt.

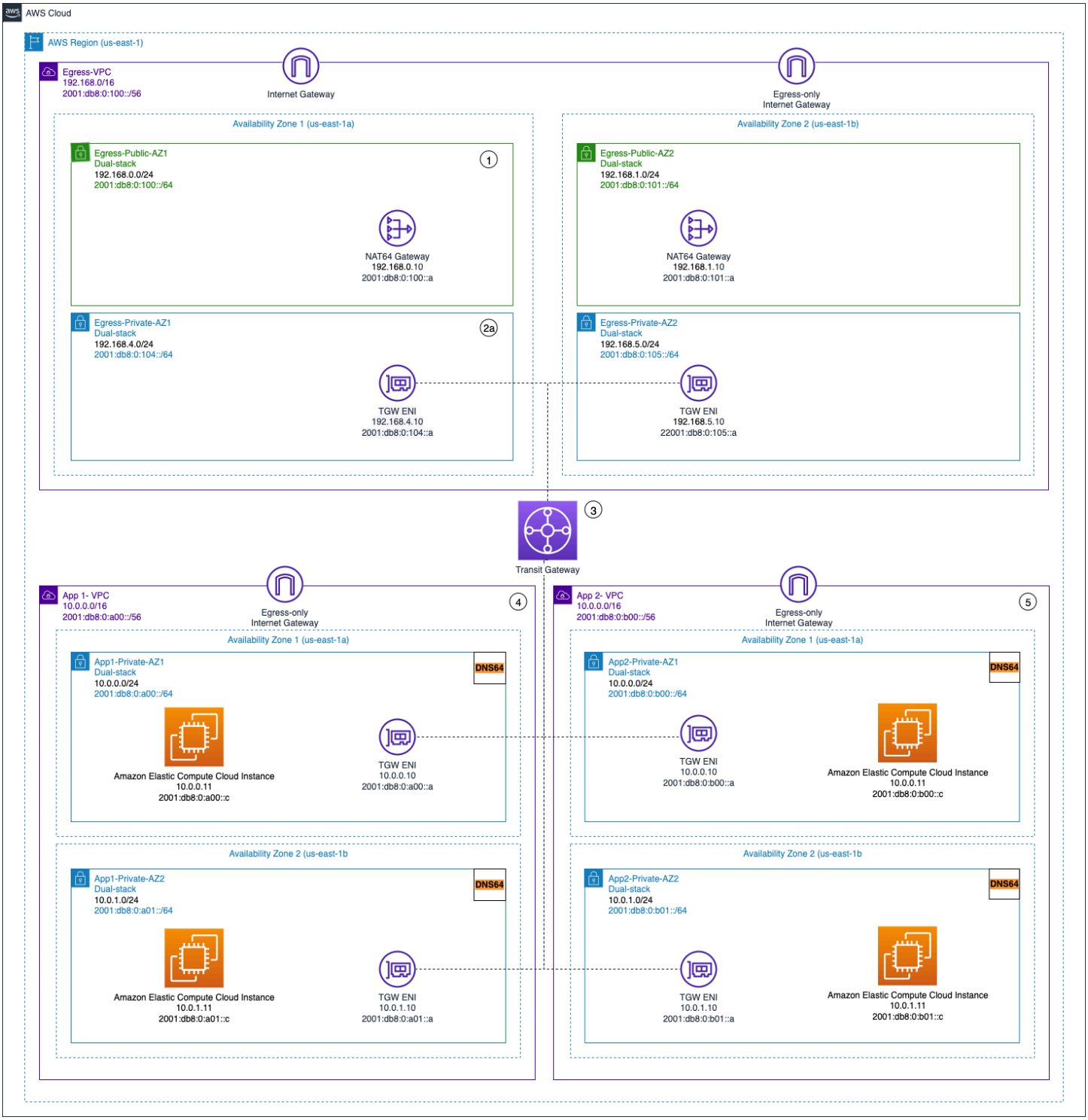
- Notieren Sie sich das GWLB-Leerlauf-Timeout. Dies kann zu Verbindungs-Timeouts auf Clients führen. Sie können Ihre Timeouts auf Client-, Server-, Firewall- und Betriebssystemebene anpassen, um dies zu vermeiden. Weitere Informationen finden Sie in Abschnitt 1: Optimieren von TCP-Keep-Alive- oder Timeout-Werten zur Unterstützung langlebiger TCP-Flüsse im Blogbeitrag Bewährte Methoden für die Bereitstellung von Gateway Load Balancer.
- GWLBE werden von betrieben, daher fallen Gebühren an. AWS PrivateLink AWS PrivateLink Weitere Informationen finden Sie auf der Seite mit den AWS PrivateLink Preisen. Wenn Sie das zentralisierte Modell mit Transit Gateway verwenden, fallen die TGW-Datenverarbeitungsgebühren an.
- Erwägen Sie die Bereitstellung von Transit Gateway und ausgehender VPC in einem separaten Netzwerkdienstkonto, um den Zugriff auf der Grundlage der Delegierung von Aufgaben zu trennen, z. B. können nur Netzwerkadministratoren auf das Netzwerkdienstkonto zugreifen.

Zentralisierter Ausgang für IPv6

Um IPv6 ausgehenden Datenverkehr in Dual-Stack-Bereitstellungen mit zentralisiertem IPv4 Ausgang zu unterstützen, muss eines von zwei Mustern ausgewählt werden:

- Zentralisierter Ausgang mit dezentralisiertem IPv4 Ausgang IPv6
- Zentralisierter Ausgang und IPv4 zentralisierter Ausgang IPv6

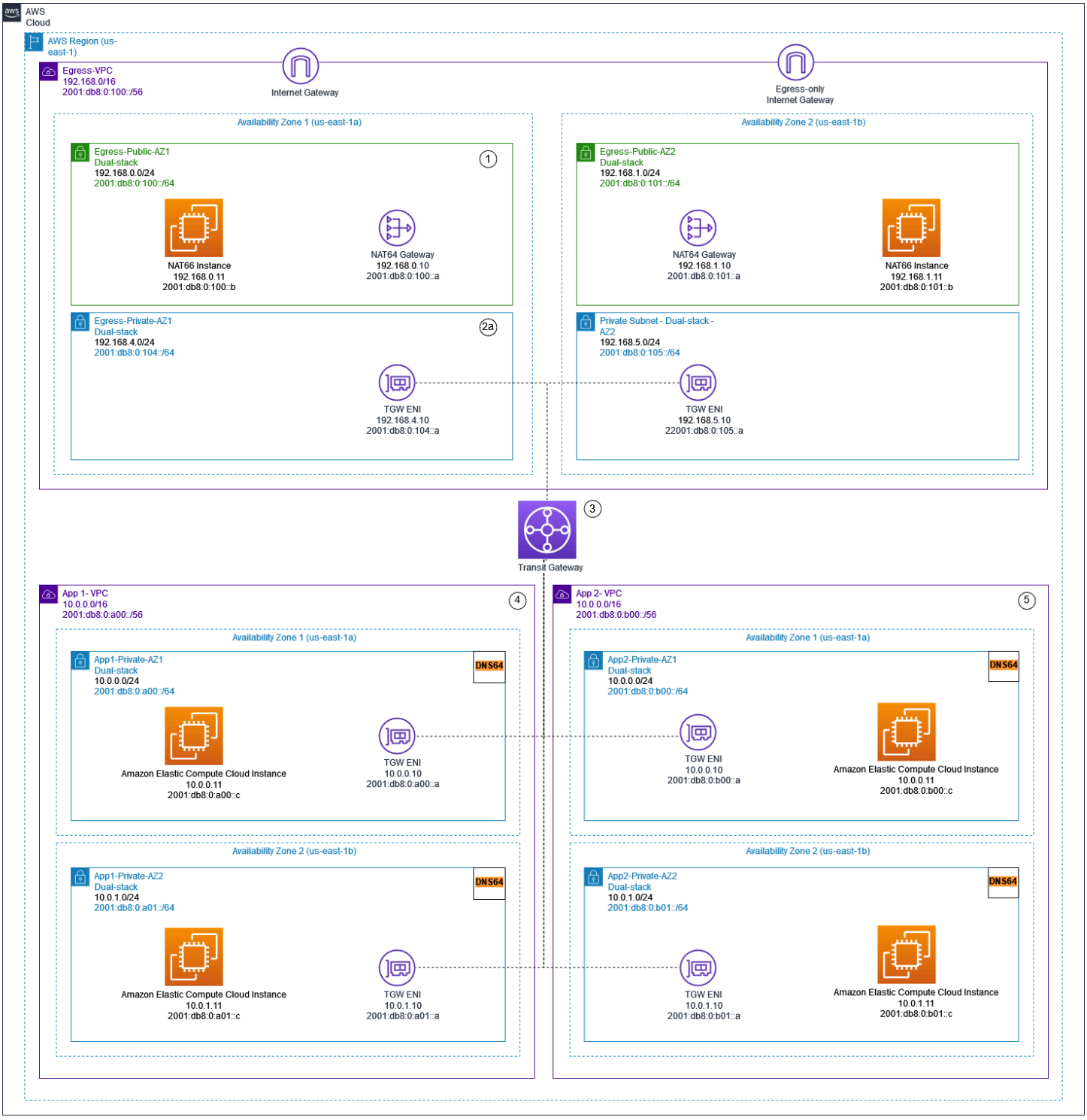
Im ersten Muster, das in der folgenden Abbildung dargestellt ist, werden Internet-Gateways nur für ausgehenden Datenverkehr in jeder Spoke-VPC bereitgestellt. Internet-Gateways nur für ausgehenden Datenverkehr sind horizontal skalierte, redundante und hochverfügbare Gateways, die ausgehende Kommunikation von Instances innerhalb Ihrer VPC aus ermöglichen. IPv6 Sie verhindern, dass das Internet Verbindungen zu Ihren Instances aufbaut. IPv6 Internet-Gateways, die nur für ausgehende Verbindungen genutzt werden, sind kostenlos. In diesem Bereitstellungsmodell fließt der IPv6 Datenverkehr von den Internet-Gateways für ausgehenden Datenverkehr in jeder VPC und der IPv4 Datenverkehr über die bereitgestellten zentralisierten NAT-Gateways.



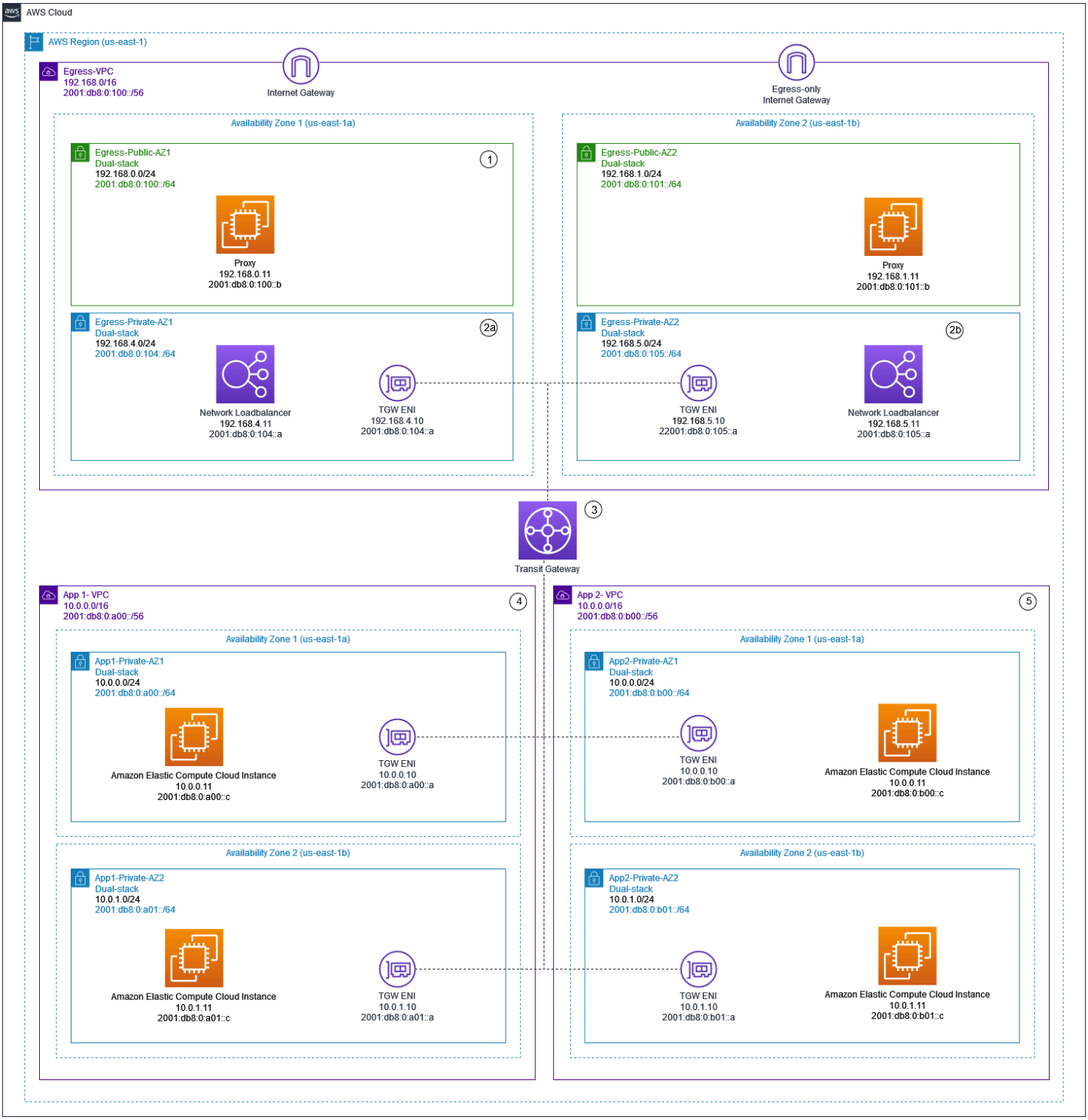
Zentralisierter Ausgang und dezentraler IPV4 reiner Ausgangsausgang IPv6

Im zweiten Muster, das in den folgenden Diagrammen dargestellt ist, wird ausgehender IPv6 Datenverkehr von Ihren Instances an eine zentrale VPC gesendet. Dies kann durch die Verwendung von IPv6 -to- IPv6 Network Prefix Translation (NPTv6) mit NAT66 Instances und NAT-Gateways

oder durch die Verwendung von Proxy-Instances und Network Load Balancer erreicht werden. Dieses Muster ist anwendbar, wenn eine zentrale Verkehrsinspektion für ausgehenden Datenverkehr erforderlich ist und sie nicht in jeder Spoke-VPC durchgeführt werden kann.



Zentralisierter IPv6 Ausgang mithilfe von NAT-Gateways und -Instanzen NAT66



Zentralisiert IPv4 und IPv6 ausgehender Datenverkehr mithilfe von Proxy-Instances und Network Load Balancer

Das IPv6 OnAWS-Whitepaper beschreibt die zentralisierten IPv6 Ausgangsmuster. Die IPv6 Ausgangsmuster werden im Blog Zentralisierter ausgehender Internetverkehr für Dual-Stack-

Verbindungen ausführlicher behandelt IPv4 und zusammen mit speziellen Überlegungen IPv6 VPCs, Musterlösungen und Diagrammen vorgestellt.

Zentralisierte Netzwerksicherheit für VPC-zu-VPC- und On-Premises-zu-VPC-Verkehr

Es kann Szenarien geben, in denen ein Kunde eine Layer-3-7-Firewall/IPs/IDs in seiner Umgebung mit mehreren Konten implementieren möchte, um die Verkehrsflüsse zwischen VPCs (Ost-West-Verkehr) oder zwischen einem lokalen Rechenzentrum und einer VPC (Nord-Süd-Verkehr) zu untersuchen. Dies kann je nach Anwendungsfall und Anforderungen auf unterschiedliche Weise erreicht werden. Sie könnten beispielsweise den Gateway Load Balancer, die Network Firewall, Transit VPC integrieren oder zentralisierte Architekturen mit Transit Gateways verwenden. Diese Szenarien werden im folgenden Abschnitt erörtert.

Überlegungen zur Verwendung eines zentralisierten Modells zur Überprüfung der Netzwerksicherheit

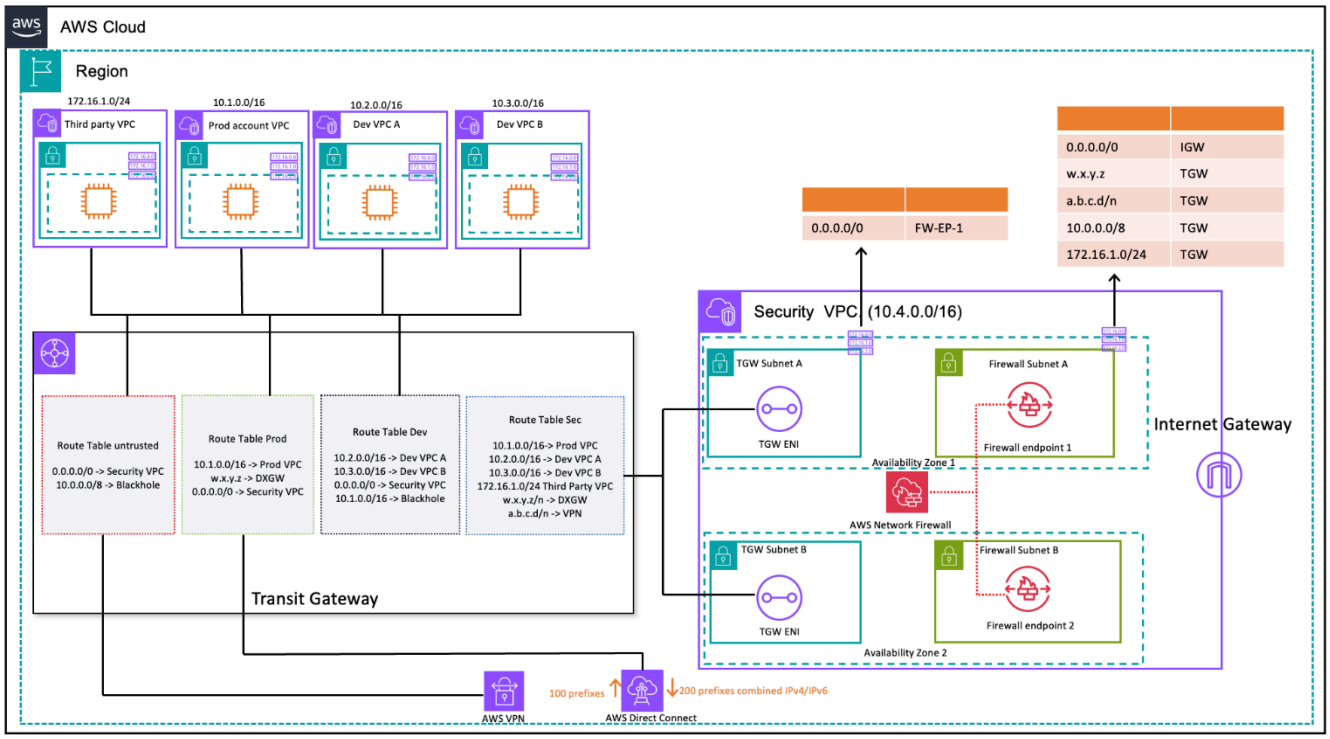
Um die Kosten zu senken, sollten Sie selektiv entscheiden, welcher Datenverkehr über Ihren AWS Network Firewall oder Gateway Load Balancer geleitet wird. Eine Möglichkeit, vorzugehen, besteht darin, Sicherheitszonen zu definieren und den Verkehr zwischen nicht vertrauenswürdigen Zonen zu überprüfen. Eine nicht vertrauenswürdige Zone kann ein Remotestandort sein, der von einem Drittanbieter verwaltet wird, eine VPC eines Anbieters, den Sie nicht kontrollieren/nicht vertrauen, oder eine Sandbox-/Entwicklungs-VPC, für die im Vergleich zum Rest Ihrer Umgebung lockere Sicherheitsregeln gelten. In diesem Beispiel gibt es vier Zonen:

- Nicht vertrauenswürdige Zone — Dies gilt für jeglichen Datenverkehr, der vom „VPN zur nicht vertrauenswürdigen Remote-Site“ oder der VPC eines Drittanbieters stammt.
- Produktionszone (Prod) — Diese Zone enthält den Datenverkehr von der Produktions-VPC und dem lokalen Kunden-DC.
- Entwicklungszone (Dev) — Diese Zone enthält den Datenverkehr von den beiden Entwicklungs-VPCs.
- Sicherheitszone (Sec) — Enthält unsere Firewall-Komponenten Network Firewall oder Gateway Load Balancer.

Dieses Setup hat vier Sicherheitszonen, aber Sie haben möglicherweise mehr. Sie können mehrere Routentabellen und Blackhole-Routen verwenden, um eine Sicherheitsisolierung und einen optimalen

Verkehrsfluss zu erreichen. Die Auswahl der richtigen Zonengruppe hängt von Ihrer allgemeinen Strategie zur Gestaltung der Landing Zone ab (Kontostruktur, VPC-Design). Sie können Zonen einrichten, um die Isolierung zwischen Geschäftseinheiten (BUs), Anwendungen, Umgebungen usw. zu ermöglichen.

Wenn Sie Ihren VPC-zu-VPC-, Zonenverkehr und VPC-On-Premises-Verkehr überprüfen und filtern möchten, können Sie Transit Gateway in Ihre zentralisierte Architektur integrieren AWS Network Firewall . Mit dem Modell von kann ein hub-and-spoke zentralisiertes Bereitstellungsmodell erreicht AWS Transit Gateway werden. Die AWS Network Firewall wird in einer separaten Sicherheits-VPC bereitgestellt. Eine separate Sicherheits-VPC bietet einen vereinfachten und zentralen Ansatz zur Verwaltung der Inspektion. Eine solche VPC-Architektur bietet AWS Network Firewall Quell- und Ziel-IP-Sichtbarkeit. Sowohl Quell- als auch Ziel-IPs werden beibehalten. Diese Sicherheits-VPC besteht aus zwei Subnetzen in jeder Availability Zone, wobei ein Subnetz für eine AWS Transit Gateway Verbindung und das andere Subnetz für den Firewall-Endpunkt reserviert ist. Die Subnetze in dieser VPC sollten nur AWS Network Firewall Endpunkte enthalten, da die Network Firewall den Verkehr in denselben Subnetzen wie die Endpunkte nicht untersuchen kann. Wenn Sie die Network Firewall zur zentralen Überprüfung des Datenverkehrs verwenden, kann sie eine Deep Packet Inspection (DPI) für eingehenden Datenverkehr durchführen. Das DPI-Muster wird im Abschnitt Zentrale Eingangsinspektion dieses Papiers näher erläutert.



Inspektion von VPC-zu-VPC- und On-Premises-zu-VPC-Verkehr mit Transit Gateway und (Routentabellendesign) AWS Network Firewall

In der zentralisierten Architektur mit Inspektion benötigen die Transit Gateway Gateway-Subnetze eine separate VPC-Routentabelle, um sicherzustellen, dass der Datenverkehr an den Firewall-Endpunkt innerhalb derselben Availability Zone weitergeleitet wird. Für den Rückverkehr wird eine einzelne VPC-Routentabelle konfiguriert, die eine Standardroute zum Transit Gateway enthält. Der Verkehr wird AWS Transit Gateway in dieselbe Availability Zone zurückgeleitet, nachdem er von AWS Network Firewallüberprüft wurde. Dies ist aufgrund der Appliance-Modus-Funktion des Transit Gateway möglich. Die Appliance-Modus-Funktion des Transit Gateway unterstützt auch die Funktion AWS Network Firewall zur Überprüfung des zustandsbehafteten Datenverkehrs innerhalb der Sicherheits-VPC.

Wenn der Appliance-Modus auf einem Transit-Gateway aktiviert ist, wählt es eine einzelne Netzwerkschnittstelle mithilfe des Flow-Hash-Algorithmus für die gesamte Lebensdauer der Verbindung aus. Das Transit Gateway verwendet dieselbe Netzwerkschnittstelle für den Rückverkehr. Dadurch wird sichergestellt, dass der bidirektionale Datenverkehr symmetrisch weitergeleitet wird – er wird während der gesamten Lebensdauer des Datenflusses durch dieselbe Availability Zone in den VPC-Anhang weitergeleitet. Weitere Informationen zum Appliance-Modus finden Sie unter Stateful Appliances und Appliance-Modus in der Amazon VPC-Dokumentation.

Informationen zu den verschiedenen Bereitstellungsoptionen von Sicherheits-VPC mit AWS Network Firewall und Transit Gateway finden Sie im Blogbeitrag Bereitstellungsmodelle für AWS Network Firewall.

Verwendung von Gateway Load Balancer mit Transit Gateway für zentralisierte Netzwerksicherheit

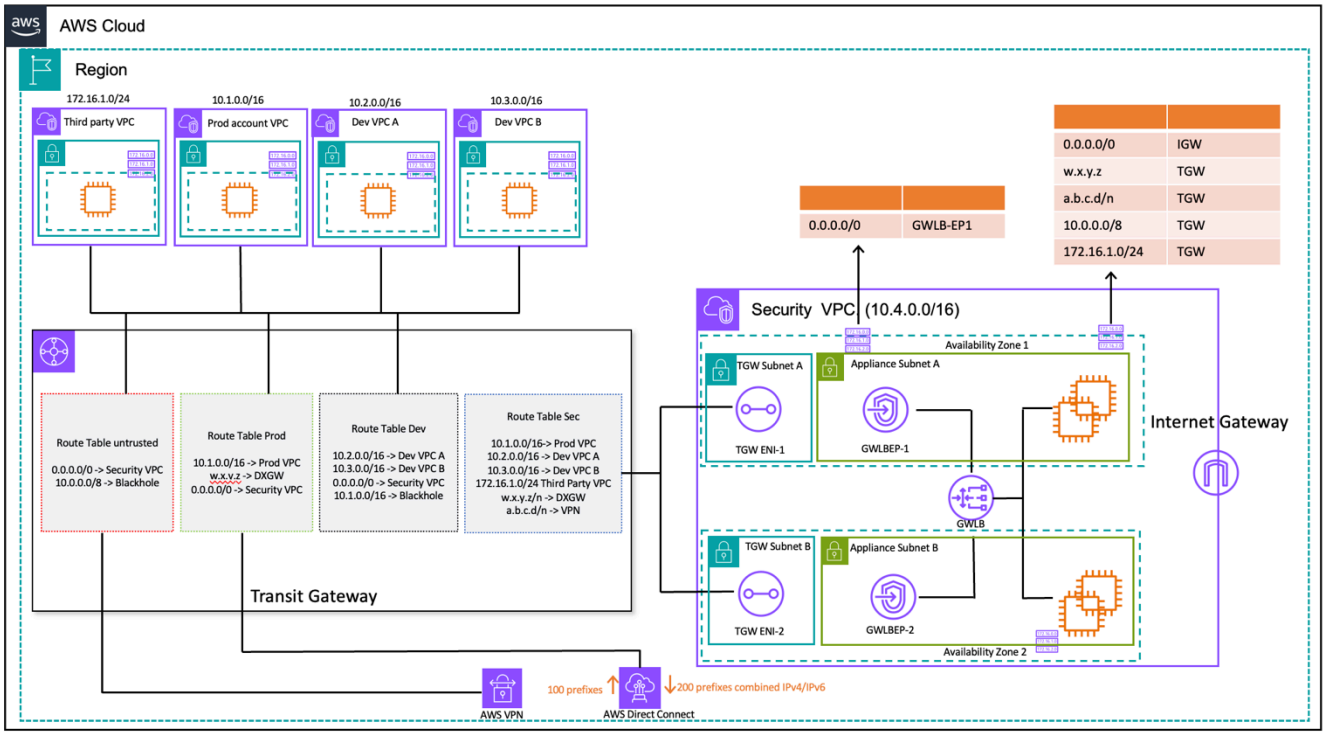
Oft möchten Kunden virtuelle Appliances integrieren, um den Datenverkehr zu filtern und Funktionen zur Sicherheitsprüfung bereitzustellen. In solchen Anwendungsfällen können sie Gateway Load Balancer, virtuelle Appliances und Transit Gateway integrieren, um eine zentrale Architektur für die Inspektion von VPC-zu-VPC- und VPC-Verkehr bereitzustellen. to-on-premises

Gateway Load Balancer wird zusammen mit den virtuellen Appliances in einer separaten Sicherheits-VPC bereitgestellt. Die virtuellen Appliances, die den Datenverkehr untersuchen, sind als Ziele hinter dem Gateway Load Balancer konfiguriert. Da es sich bei Gateway Load Balancer-Endpunkten um routingfähige Ziele handelt, können Kunden den Datenverkehr, der zu und vom Transit Gateway fließt, zur Flotte virtueller Appliances weiterleiten. Um die Strömungssymetrie zu gewährleisten, ist der Appliance-Modus auf dem Transit Gateway aktiviert.

Jede Spoke-VPC hat eine Routing-Tabelle, die dem Transit Gateway zugeordnet ist, das die Standardroute zum Security-VPC-Anhang als Next-Hop hat.

Die zentralisierte Sicherheits-VPC besteht aus Appliance-Subnetzen in jeder Availability Zone, die über die Gateway Load Balancer-Endpunkte und die virtuellen Appliances verfügen. Es hat auch Subnetze für Transit Gateway Gateway-Anlagen in jeder Availability Zone, wie in der folgenden Abbildung dargestellt.

Weitere Informationen zur zentralen Sicherheitsinspektion mit Gateway Load Balancer und Transit Gateway finden Sie in der Centralized Inspection Architecture with AWS Gateway Load Balancer und im AWS Transit Gateway Blogbeitrag.



Inspektion des VPC-zu-VPC- und on-premises-to -VPC-Datenverkehrs mit Transit Gateway und AWS Gateway Load Balancer (Routentabellendesign)

Wichtige Überlegungen zu AWS Network Firewall und AWS Gateway Load Balancer

- Der Gerätemodus sollte auf dem Transit Gateway aktiviert sein, wenn eine Ost-West-Inspektion durchgeführt wird.
- Sie können dasselbe Modell AWS-Regionen mithilfe von AWS Transit Gateway Interregion Peering für die Inspektion des Datenverkehrs zu anderen bereitstellen.

- Standardmäßig verteilt jeder Gateway Load Balancer, der in einer Availability Zone bereitgestellt wird, den Verkehr nur auf die registrierten Ziele innerhalb derselben Availability Zone. Dies wird Availability Zone-Affinität genannt. Wenn Sie zonenübergreifendes Load Balancing aktivieren, verteilt Gateway Load Balancer den Datenverkehr auf alle registrierten und fehlerfreien Ziele in allen aktivierten Availability Zones. Wenn alle Ziele in allen Availability Zones fehlerhaft sind, kann der Gateway Load Balancer nicht geöffnet werden. Weitere Informationen finden Sie im Blogbeitrag Bewährte Methoden für die Bereitstellung von Gateway Load Balancer in Abschnitt 4: Grundlegendes zu Ausfallszenarien für Appliance und Availability Zone.
- Für den Einsatz in mehreren Regionen AWS empfiehlt es sich, separate Inspektions-VPCs in den jeweiligen lokalen Regionen einzurichten, um Abhängigkeiten zwischen Regionen zu vermeiden und die damit verbundenen Datenübertragungskosten zu reduzieren. Sie sollten den Verkehr in der lokalen Region überprüfen, anstatt die Inspektion auf eine andere Region zu konzentrieren.
- Die Kosten für den Betrieb eines zusätzlichen EC2-basierten Hochverfügbarkeitspaars (HA) in Bereitstellungen mit mehreren Regionen können sich summieren. Weitere Informationen finden Sie im Blogbeitrag Bewährte Methoden für die Bereitstellung von Gateway Load Balancer.

AWS Network Firewall im Vergleich zum Gateway Load Balancer

Tabelle 2 — AWS Network Firewall Vergleich zum Gateway Load Balancer

Kriterien	AWS Network Firewall	Gateway Load Balancer
Anwendungsfall	Statefuler, verwalteter Netzwerk-Firewall mit Servicefunktion zur Erkennung und Verhinderung von Eindringlingen, kompatibel mit Suricata.	Verwalteter Service, der die Bereitstellung, Skalierung und Verwaltung virtueller Appliances von Drittanbietern vereinfacht
Komplexität	AWS verwalteter Service. AWS kümmert sich um die Skalierbarkeit und Verfügbar keit des Dienstes.	Von AWS verwalteter Service. AWS kümmert sich um die Skalierbarkeit und Verfügbar keit des Gateway Load Balancer-Dienstes. Der Kunde ist verantwortlich für die Verwaltung der Skalierung

Kriterien	AWS Network Firewall	Gateway Load Balancer
		und Verfügbarkeit der virtuelle n Appliances hinter Gateway Load Balancer.
Skalieren	AWS Network Firewall Endgeräte werden betrieben von AWS PrivateLink. Die Network Firewall unterstützt bis zu 100 Gbit/s Netzwerkv erkehr pro Firewall-Endpunkt.	Gateway Load Balancer-Endpunkte unterstützen eine maximale Bandbreite von bis zu 100 Gbit/s pro Endpunkt
Kosten	AWS Network Firewall Endpunktkosten + Datenvera rbeitungsgebühren	Gateway Load Balancer + Gateway Load Balancer-Endpunkte + virtuelle Appliances + Datenvera rbeitungsgebühren

Zentralisierte Eingangsinspektion

Internetanwendungen haben naturgemäß eine größere Angriffsfläche und sind Bedrohungskategorien ausgesetzt, denen die meisten anderen Arten von Anwendungen nicht ausgesetzt sind. Der notwendige Schutz vor Angriffen auf diese Art von Anwendungen und die Minimierung der Angriffsfläche sind ein zentraler Bestandteil jeder Sicherheitsstrategie.

Wenn Sie Anwendungen in Ihrer Landing Zone bereitstellen, greifen die Benutzer über das öffentliche Internet (z. B. über ein Content Delivery Network (CDN) oder über eine öffentlich zugängliche Webanwendung) über einen öffentlich zugänglichen Load Balancer, ein API-Gateway oder direkt über ein Internet-Gateway auf viele Apps zu. In diesem Fall können Sie Ihre Workloads und Anwendungen sichern, indem Sie die AWS Web Application Firewall (AWS WAF) für die Inspektion eingehender Anwendungen oder alternativ die IDS/IPS eingehende Inspektion mit Gateway Load Balancer oder verwenden. AWS Network Firewall

Wenn Sie weiterhin Anwendungen in Ihrer Landing Zone bereitstellen, müssen Sie möglicherweise den eingehenden Internetverkehr überprüfen. Sie können dies auf verschiedene Arten erreichen, entweder mithilfe verteilter, zentraler oder kombinierter Inspektionsarchitekturen mithilfe von Gateway Load Balancer, auf dem Ihre Firewall-Appliances von Drittanbietern ausgeführt werden, oder AWS Network Firewall mit erweiterten DPI- und IDS/IPS Funktionen durch die Verwendung von Open-Source-Suricata-Regeln. In diesem Abschnitt werden sowohl der Gateway Load Balancer als auch eine zentralisierte Bereitstellung behandelt, AWS Network Firewall bei der die Funktion AWS Transit Gateway als zentraler Hub für das Routing des Datenverkehrs verwendet wird.

AWS WAF und AWS Firewall Manager zur Überprüfung des eingehenden Datenverkehrs aus dem Internet

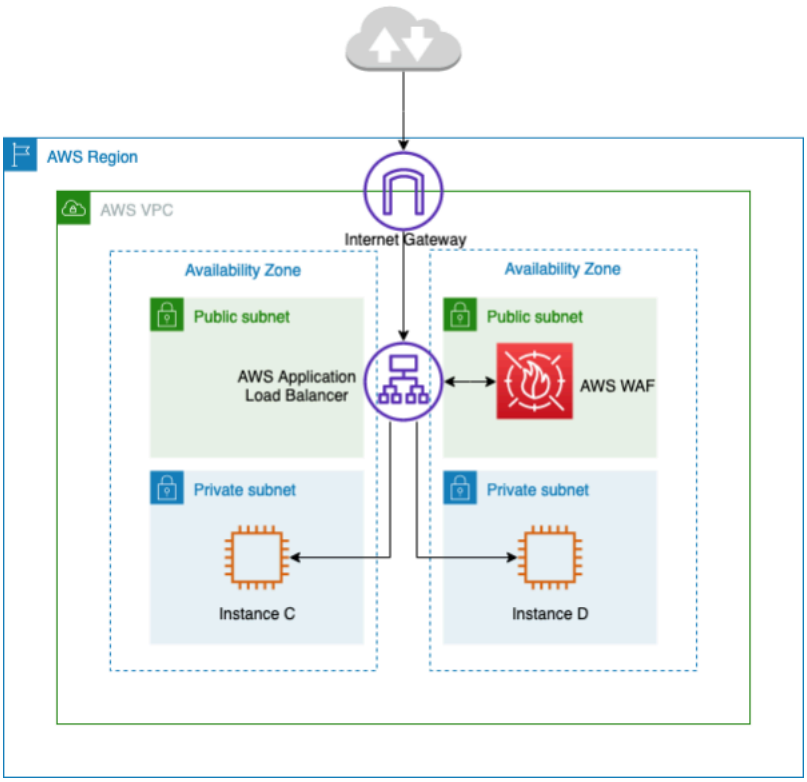
AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits und Bots beiträgt, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. AWS WAF gibt Ihnen die Kontrolle darüber, wie der Datenverkehr Ihre Anwendungen erreicht, indem Sie Sicherheitsregeln erstellen können, die den Bot-Verkehr kontrollieren und gängige Angriffsmuster wie SQL-Injection oder Cross-Site Scripting (XSS) blockieren. Sie können auch Regeln anpassen, die bestimmte Verkehrsmuster herausfiltern.

Sie können AWS WAF auf Amazon CloudFront als Teil Ihrer CDN-Lösung, des Application Load Balancer, der Ihre Webserver unterstützt, Amazon API Gateway für Ihr REST oder AWS AppSync für Ihr APIs GraphQL bereitstellen. APIs

Nach der Bereitstellung können Sie dann mithilfe des Visual Rule Builder AWS WAF, Code in JSON und verwalteten Regeln, die von verwaltet werden, Ihre eigenen Regeln für den Traffic erstellen oder Regeln von AWS Drittanbietern abonnieren. AWS Marketplace Mit diesen Regeln können Sie unerwünschten Datenverkehr herausfiltern, indem sie den Datenverkehr anhand der angegebenen Muster auswerten. Sie können Amazon außerdem CloudWatch für die Überwachung und Protokollierung eingehender Verkehrsdaten verwenden.

Für die zentrale Verwaltung all Ihrer Konten und Anwendungen können Sie Folgendes verwenden AWS Firewall Manager. AWS Organizations AWS Firewall Manager ist ein Sicherheitsverwaltungsdienst, mit dem Sie Firewallregeln zentral konfigurieren und verwalten können. AWS Firewall Manager Durch die Durchsetzung einheitlicher Sicherheitsregeln können Sie bei der Erstellung neuer Anwendungen und Ressourcen ganz einfach die Einhaltung gesetzlicher Vorschriften sicherstellen.

Mithilfe AWS Firewall Manager können Sie ganz einfach AWS WAF Regeln für Ihre Application Load Balancers, API Gateway Gateway-Instances und CloudFront Amazon-Distributionen einführen. AWS Firewall Manager lässt sich in Von AWS verwaltete Regeln for integrieren AWS WAF, sodass Sie auf einfache Weise vorkonfigurierte, kuratierte AWS WAF Regeln für Ihre Anwendungen bereitstellen können. Weitere Informationen zur zentralen Verwaltung AWS WAF mit AWS Firewall Manager finden Sie unter Zentral verwalten AWS WAF (API v2) und Von AWS verwaltete Regeln skalierbar mit. AWS Firewall Manager



Zentralisierte Inspektion des eingehenden Datenverkehrs mit AWS WAF

In der vorherigen Architektur werden Anwendungen auf EC2 Amazon-Instances in mehreren Availability Zones in den privaten Subnetzen ausgeführt. Vor den EC2 Amazon-Instances ist ein öffentlich zugänglicher Application Load Balancer (ALB) installiert, der die Anfragen zwischen verschiedenen Zielen ausgleicht. Der AWS WAF ist dem ALB zugeordnet.

Vorteile

- Mit AWS WAF Bot Control erhalten Sie Transparenz und Kontrolle über den allgemeinen und allgegenwärtigen Bot-Traffic zu Ihren Anwendungen.
- Mit Managed Rules for AWS WAF können Sie schnell loslegen und Ihre Webanwendung oder APIs vor gängigen Bedrohungen schützen. Sie können aus vielen Regeltypen wählen, z. B. solche, die sich mit Problemen wie den 10 größten Sicherheitsrisiken des Open Web Application Security Project (OWASP), spezifischen Bedrohungen für Content Management Systeme (CMS) wie Joomla WordPress oder sogar neu auftretende Common Vulnerabilities and Exposures (CVE) befassen. Verwaltete Regeln werden automatisch aktualisiert, wenn neue Probleme auftreten, sodass Sie mehr Zeit mit der Entwicklung von Anwendungen verbringen können.
- AWS WAF ist ein verwalteter Service, für dessen Inspektion in dieser Architektur keine Appliance erforderlich ist. Darüber hinaus werden über Amazon Data Firehose Protokolle nahezu in

Echtzeit bereitgestellt. AWS WAF bietet nahezu in Echtzeit Einblick in Ihren Web-Traffic, den Sie verwenden können, um neue Regeln oder Benachrichtigungen in Amazon zu erstellen. CloudWatch

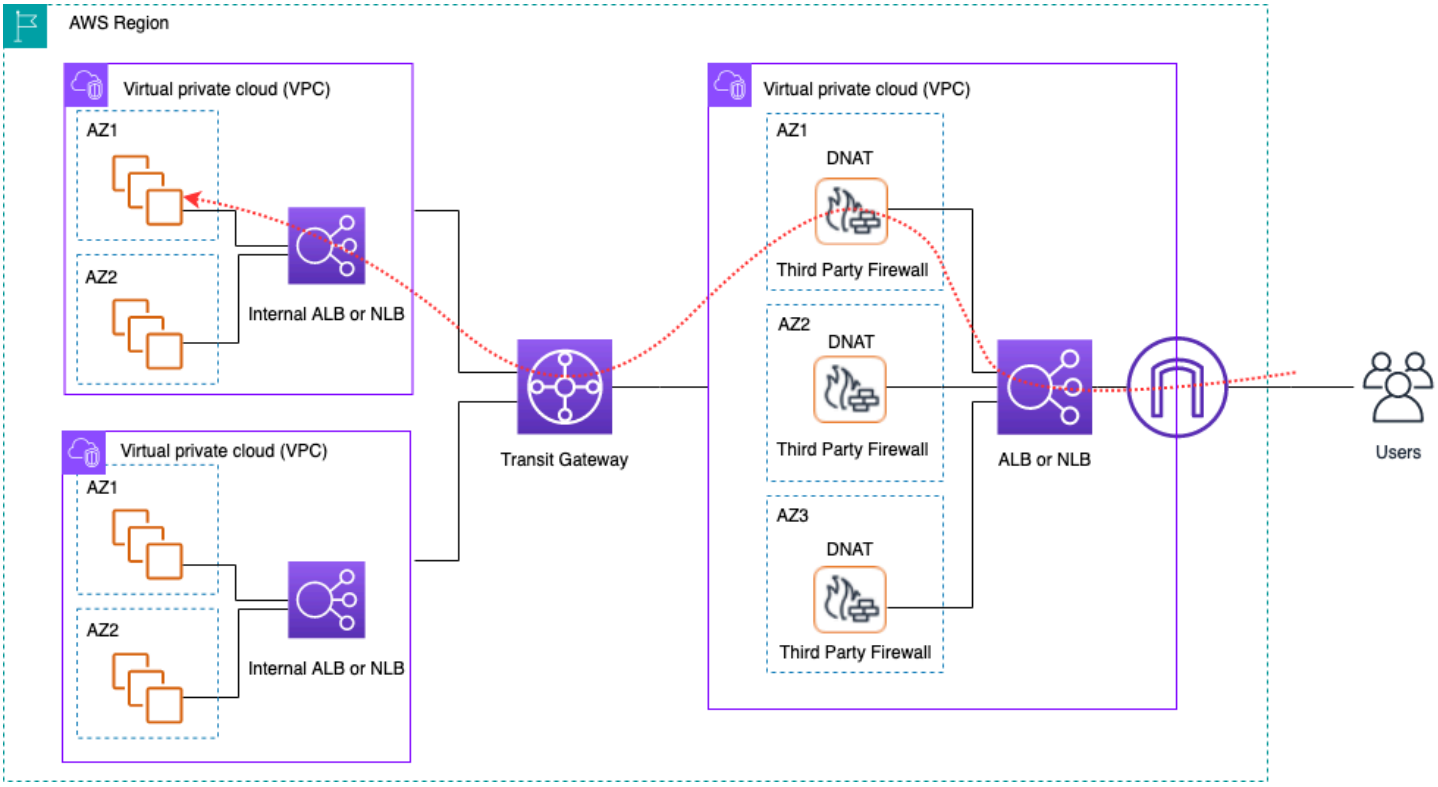
Wesentliche Überlegungen

- Diese Architektur eignet sich am besten für die Inspektion von HTTP-Headern und verteilten Inspektionen, da sie auf einem ALB-, CloudFront Distributions- und API Gateway integriert AWS WAF ist. AWS WAF protokolliert den Hauptteil der Anfrage nicht.
- Datenverkehr, der zu einer zweiten Gruppe von ALB geht (falls vorhanden), wird möglicherweise nicht von derselben AWS WAF Instanz überprüft, da eine neue Anfrage an die zweite Gruppe von ALB gestellt würde.

Zentralisierte eingehende Inspektion mit Appliances von Drittanbietern

In diesem architektonischen Entwurfsmuster stellen Sie Firewall-Appliances von Drittanbietern auf Amazon EC2 in mehreren Availability Zones hinter einem Elastic Load Balancer (ELB) wie einem Load Application/Network Balancer in einer separaten Inspection-VPC bereit.

Die Inspection-VPC und andere Spoke VPCs sind über ein Transit Gateway als VPC-Anhänge miteinander verbunden. Die Anwendungen in Spoke VPCs verfügen über ein internes ELB, das je nach Anwendungstyp entweder ALB oder NLB sein kann. Die Clients stellen über das Internet eine Verbindung zum DNS des externen ELB in der Inspektions-VPC her, der den Datenverkehr an eine der Firewall-Appliances weiterleitet. Die Firewall überprüft den Datenverkehr und leitet ihn dann über das Transit Gateway mithilfe des DNS des internen ELB an die Spoke-VPC weiter, wie in der folgenden Abbildung dargestellt. Weitere Informationen zur Sicherheitsprüfung eingehender Nachrichten mit Appliances von Drittanbietern finden Sie im Blogbeitrag So integrieren Sie Firewall-Appliances von Drittanbietern in eine AWS-Umgebung.



Zentralisierte Inspektion des eingehenden Datenverkehrs mithilfe von Appliances von Drittanbietern und ELB

Vorteile

- Diese Architektur unterstützt alle Arten von Anwendungen für die Inspektion und erweiterte Inspektionsfunktionen, die über Firewall-Appliances von Drittanbietern angeboten werden.
- Dieses Muster unterstützt DNS-basiertes Routing von Firewall-Appliances zu Spoke VPCs, wodurch die Anwendungen in Spoke VPCs unabhängig hinter einem ELB skaliert werden können.
- Sie können Auto Scaling mit dem ELB verwenden, um die Firewall-Appliances in der Inspection-VPC zu skalieren.

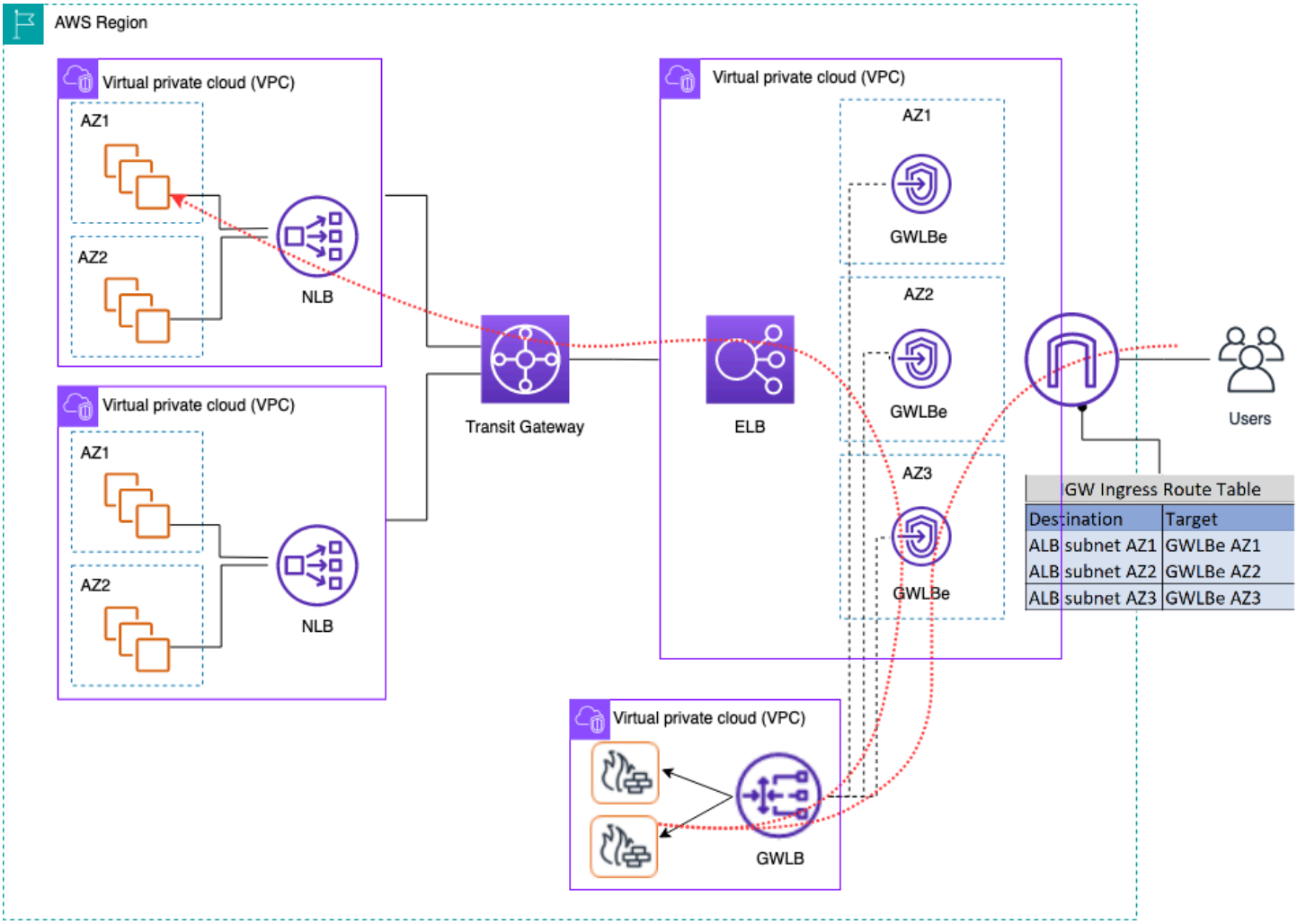
Wesentliche Überlegungen

- Für eine hohe Verfügbarkeit müssen Sie mehrere Firewall-Appliances in allen Availability Zones bereitstellen.
- Die Firewall muss mit Quell-NAT konfiguriert werden und diese ausführen, um die Flusssymetrie aufrechtzuerhalten, was bedeutet, dass die Client-IP-Adresse für die Anwendung nicht sichtbar ist.

- Erwägen Sie die Bereitstellung von Transit Gateway und Inspection VPC im Network Services-Konto.
- Zusätzliche licensing/support Firewall-Kosten von Drittanbietern. Die EC2 Gebühren von Amazon hängen vom Instance-Typ ab.

Untersuchung des eingehenden Datenverkehrs aus dem Internet mithilfe von Firewall-Appliances mit Gateway Load Balancer

Kunden verwenden Firewalls der nächsten Generation (NGFW) und Intrusion Prevention Systems (IPS) von Drittanbietern als Teil ihrer Defense-in-Depth-Strategie. Traditionell handelt es sich dabei häufig um spezielle Hardware oder Appliances. software/virtual Sie können Gateway Load Balancer verwenden, um diese virtuellen Appliances horizontal zu skalieren, um den Verkehr von und zu Ihrer VPC zu untersuchen, wie in der folgenden Abbildung dargestellt.



Zentralisierte Inspektion des eingehenden Datenverkehrs mithilfe von Firewall-Appliances mit Gateway Load Balancer

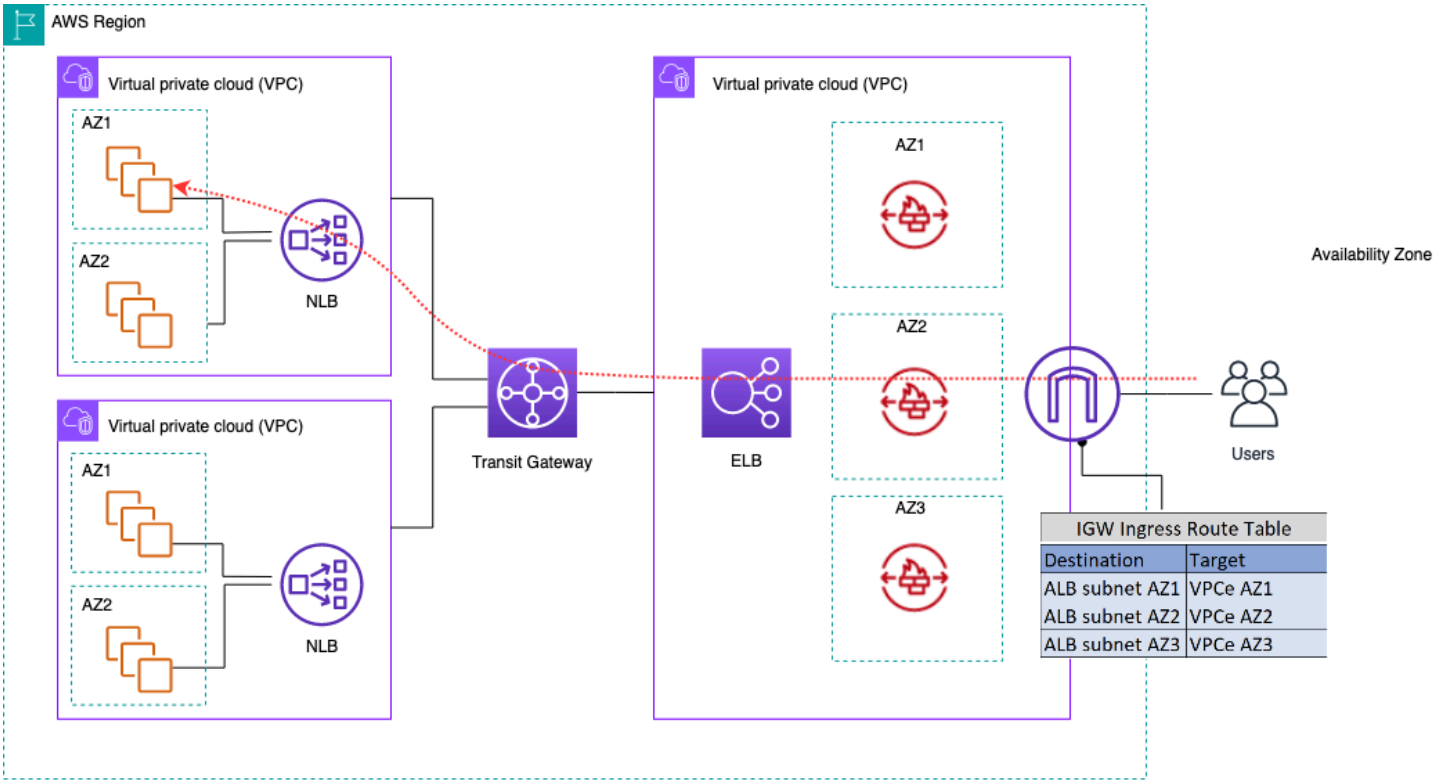
In der vorherigen Architektur werden Gateway Load Balancer-Endpunkte in jeder Availability Zone in einer separaten Edge-VPC bereitgestellt. Die Firewalls, Intrusion Prevention-Systeme usw. der nächsten Generation werden hinter dem Gateway Load Balancer in der zentralen Appliance-VPC bereitgestellt. Diese Appliance-VPC kann sich im selben AWS-Konto wie das Spoke-Konto VPCs oder in einem anderen AWS-Konto befinden. Virtuelle Appliances können für die Verwendung von Auto Scaling-Gruppen konfiguriert werden und werden automatisch beim Gateway Load Balancer registriert, was eine Auto Scaling der Sicherheitsebene ermöglicht.

Diese virtuellen Appliances können verwaltet werden, indem über ein Internet Gateway (IGW) auf ihre Verwaltungsschnittstellen zugegriffen wird oder indem ein Bastion-Host-Setup in der Appliance-VPC verwendet wird.

Mithilfe der VPC-Ingress-Routing-Funktion wird die Edge-Routing-Tabelle aktualisiert, um eingehenden Datenverkehr vom Internet zu Firewall-Appliances hinter dem Gateway Load Balancer weiterzuleiten. Der geprüfte Datenverkehr wird über Gateway Load Balancer-Endpunkte an die VPC-Zielinstanz weitergeleitet. Einzelheiten zu den verschiedenen Verwendungsmöglichkeiten von AWS Gateway Load Balancer finden Sie im Blogbeitrag Einführung in Gateway Load Balancer: Unterstützte Architekturmuster.

Verwendung von AWS Network Firewall für den zentralisierten Dateneingang

In dieser Architektur wird der eingehende Datenverkehr geprüft, AWS Network Firewall bevor er den Rest erreicht. VPCs In diesem Setup wird der Verkehr auf alle Firewall-Endpunkte aufgeteilt, die in der Edge-VPC bereitgestellt werden. Sie stellen ein öffentliches Subnetz zwischen dem Firewall-Endpunkt und dem Transit Gateway Gateway-Subnetz bereit. Sie können eine ALB oder NLB verwenden, die IP-Ziele in Ihrem Spoke enthalten, VPCs während Amazon EC2 Auto Scaling für Ziele dahinter verwaltet wird.



Inspektion des eingehenden Datenverkehrs mithilfe der AWS-Netzwerk-Firewall

Zur Vereinfachung der Bereitstellung und Verwaltung von AWS Network Firewall AWS Firewall Manager kann dieses Modell verwendet werden. Mit Firewall Manager können Sie Ihre verschiedenen Firewalls zentral verwalten, indem der Schutz, den Sie am zentralen Ort erstellt haben, automatisch auf mehrere Konten angewendet wird. Firewall Manager unterstützt sowohl verteilte als auch zentralisierte Bereitstellungsmodelle für Network Firewall. Weitere Informationen zum Modell finden Sie im Blogbeitrag How to Deployment AWS Network Firewall by Using. AWS Firewall Manager

Deep Packet Inspection (DPI) mit AWS Network Firewall

Die Network Firewall kann bei eingehendem Datenverkehr eine Deep Packet Inspection (DPI) durchführen. Mithilfe eines in (ACM) gespeicherten Transport Layer Security AWS Certificate Manager (TLS) -Zertifikats kann die Network Firewall Pakete entschlüsseln, DPI durchführen und Pakete erneut verschlüsseln. Es gibt einige Überlegungen zur Einrichtung von DPI mit der Network Firewall. Zunächst muss ein vertrauenswürdiges TLS-Zertifikat in ACM gespeichert werden. Zweitens müssen die Netzwerk-Firewall-Regeln so konfiguriert werden, dass Pakete korrekt zur Entschlüsselung und erneuten Verschlüsselung gesendet werden. Weitere Informationen finden

Sie im Blogbeitrag Konfiguration der TLS-Inspektion für verschlüsselten AWS Network Firewall Datenverkehr.

Wichtige Überlegungen zu AWS Network Firewall einer zentralisierten Ingress-Architektur

- ELB in Edge VPC kann nur IP-Adressen als Zieltypen haben, keinen Hostnamen. In der vorherigen Abbildung handelt es sich bei den Zielen um die privaten Ziele IPs des Network Load Balancer in Spoke VPCs. Die Verwendung von IP-Zielen hinter dem ELB in der Edge-VPC führt zum Verlust von Auto Scaling.
- Erwägen Sie die Verwendung AWS Firewall Manager als zentrale Anlaufstelle für Ihre Firewall-Endpunkte.
- Dieses Bereitstellungsmodell verwendet die Verkehrsinspektion direkt beim Eintritt in die Edge-VPC, sodass es die Gesamtkosten Ihrer Inspektionsarchitektur senken kann.

DNS

Wenn Sie eine Instance in einer VPC starten, AWS erhält die Instance mit Ausnahme der Standard-VPC einen privaten DNS-Hostnamen (und möglicherweise einen öffentlichen DNS-Hostnamen), abhängig von den DNS-Attributen, die Sie für die VPC angeben, und davon, ob Ihre Instance eine öffentliche Adresse hat. IPv4 Wenn das `enableDnsSupport` Attribut auf gesetzt ist`true`, erhalten Sie eine DNS-Auflösung innerhalb der VPC vom Route 53 Resolver (+2 IP-Offset zum VPC CIDR). Standardmäßig beantwortet Route 53 Resolver DNS-Abfragen für VPC-Domänennamen wie Domänennamen für EC2 Instances oder ELB-Load Balancer. Mit VPC-Peering können Hosts in einer VPC öffentliche DNS-Hostnamen für Peering-Instances in private IP-Adressen auflösen VPCs, sofern die entsprechende Option aktiviert ist. Das Gleiche gilt für Connected Via. VPCs AWS Transit Gateway Weitere Informationen finden Sie unter Support für die DNS-Auflösung für eine VPC-Peering-Verbindung aktivieren.

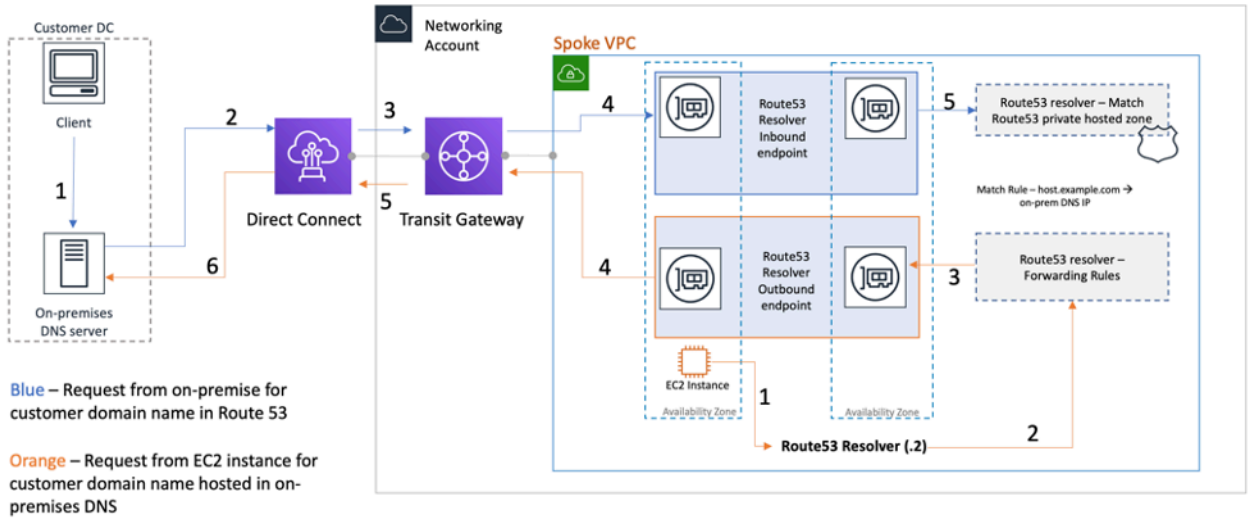
Wenn Sie Ihre Instances einem benutzerdefinierten Domainnamen zuordnen möchten, können Sie Amazon Route 53 verwenden, um einen benutzerdefinierten DNS-to-IP-mapping Datensatz zu erstellen. Eine von Amazon Route 53 gehostete Zone ist ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Anfragen für eine Domain und deren Subdomains antworten soll. Öffentliche gehostete Zonen enthalten DNS-Informationen, die über das öffentliche Internet aufgelöst werden können, während es sich bei privaten gehosteten Zonen um eine spezielle Implementierung handelt, bei der nur Informationen angezeigt werden VPCs , die an die spezifische private gehostete Zone angehängt wurden. In einer Landing Zone-Konfiguration, in der Sie mehrere VPCs OR-Konten haben, können Sie eine einzelne private gehostete Zone VPCs mehreren AWS-Konten und Regionen zuordnen (SDK/CLI/APInur möglich mit). Die Endhosts in der VPCs verwenden ihre jeweilige Route 53-Resolver-IP (+2 Offset gegenüber VPC-CIDR) als Nameserver für DNS-Abfragen. Der Route 53 Resolver in VPC akzeptiert nur DNS-Abfragen von Ressourcen innerhalb einer VPC.

Hybrid-DNS

DNS ist eine wichtige Komponente jeder Infrastruktur, ob hybrid oder nicht, da es die hostname-to-IP-address Auflösung bietet, auf die sich Anwendungen verlassen. Kunden, die Hybridumgebungen implementieren, verfügen in der Regel bereits über ein DNS-Auflösungssystem und wünschen sich eine DNS-Lösung, die mit ihrem aktuellen System zusammenarbeitet. Der native Route 53-Resolver (+2 aus dem Basis-VPC-CIDR) ist von lokalen Netzwerken aus nicht erreichbar, die VPN verwenden oder. Direct Connect Wenn Sie also DNS für die VPCs in einer AWS-Region mit DNS für

Ihr Netzwerk integrieren, benötigen Sie einen eingehenden Route 53 Resolver-Endpunkt (für DNS-Anfragen, die Sie an Ihre weiterleiten VPCs) und einen Route 53 Resolver-Endpunkt für ausgehende Anfragen (für Anfragen, die Sie von Ihrem VPCs zu Ihrem Netzwerk weiterleiten).

Wie in der folgenden Abbildung dargestellt, können Sie ausgehende Resolver-Endpunkte so konfigurieren, dass sie Anfragen, die sie von EC2 Amazon-Instances in Ihren erhalten, an DNS-Server in Ihrem VPCs Netzwerk weiterleiten. Um ausgewählte Abfragen von einer VPC an ein lokales Netzwerk weiterzuleiten, erstellen Sie Route 53-Resolver-Regeln, die die Domänennamen für die DNS-Abfragen angeben, die Sie weiterleiten möchten (z. B. example.com), und die IP-Adressen der DNS-Resolver in Ihrem Netzwerk, an die Sie die Abfragen weiterleiten möchten. Bei eingehenden Anfragen von lokalen Netzwerken zu Route 53-Hosting-Zonen können DNS-Server in Ihrem Netzwerk Anfragen an eingehende Resolver-Endpunkte in einer bestimmten VPC weiterleiten.

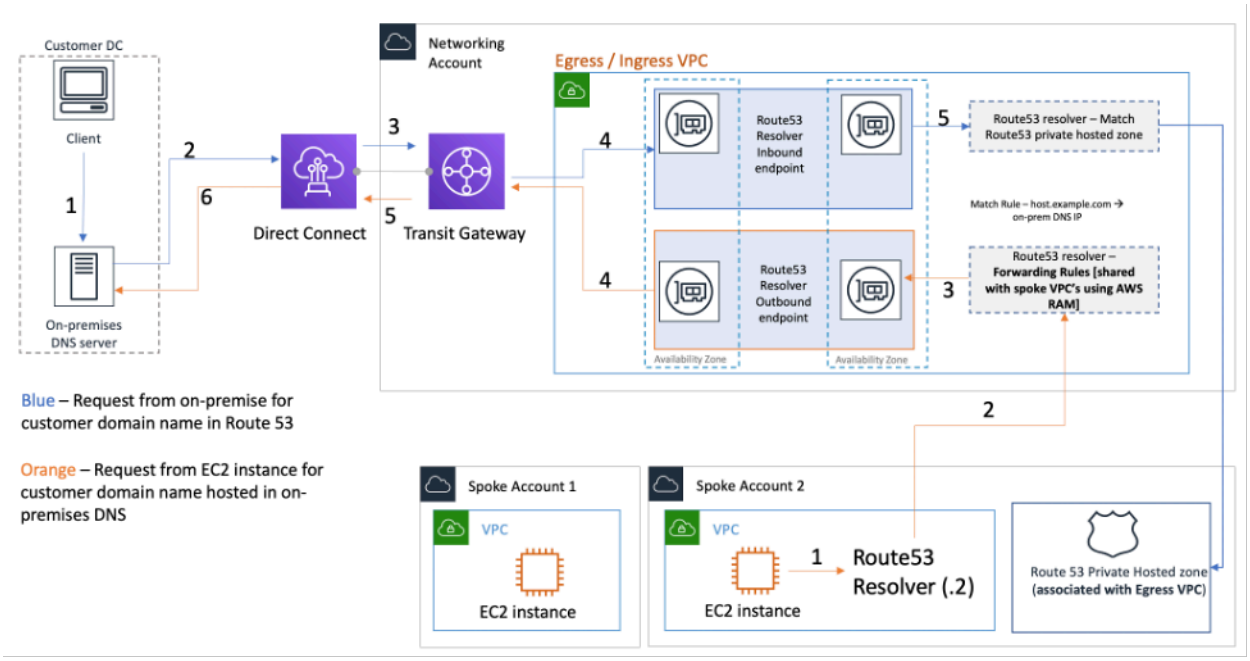


Hybride DNS-Auflösung mit Route 53 Resolver

Auf diese Weise können Ihre lokalen DNS-Resolver problemlos Domainnamen für AWS-Ressourcen wie EC2 Amazon-Instances oder Datensätze in einer privat gehosteten Route 53-Zone auflösen, die dieser VPC zugeordnet ist. Darüber hinaus können Route 53 Resolver-Endpunkte bis zu etwa 10.000 Abfragen pro Sekunde pro ENI verarbeiten, sodass sie problemlos auf ein viel größeres DNS-Abfragevolumen skaliert werden können. Weitere Informationen finden Sie unter Best Practices for Resolver in der Amazon Route 53-Dokumentation.

Es wird nicht empfohlen, Route 53 Resolver-Endpunkte in jeder VPC der Landing Zone zu erstellen. Zentralisieren Sie sie in einer zentralen Ausgangs-VPC (im Netzwerkdienstkonto). Dieser Ansatz ermöglicht eine bessere Verwaltbarkeit und hält gleichzeitig die Kosten niedrig (Ihnen wird für jeden inbound/outbound Resolver-Endpunkt, den Sie erstellen, eine Stundengebühr berechnet). Sie teilen sich den zentralen Eingangs- und Ausgangsendpunkt mit dem Rest der Landing Zone.

- Auflösung ausgehender Nachrichten — Verwenden Sie das Network Services-Konto, um Resolver-Regeln zu schreiben (auf deren Grundlage DNS-Abfragen an lokale DNS-Server weitergeleitet werden). Verwenden Sie Resource Access Manager (RAM), um diese Route 53 Resolver-Regeln mit mehreren Konten zu teilen (und sie VPCs in den Konten zuzuordnen). EC2 Spoke-Instanzen VPCs können DNS-Abfragen an den Route 53 Resolver senden, und der Route 53 Resolver Service leitet diese Abfragen über die ausgehenden Route 53 Resolver-Endpunkte in der Ausgangs-VPC an den lokalen DNS-Server weiter. Sie müssen keine Peer-Spoke mit VPCs der Ausgangs-VPC herstellen oder sie über Transit Gateway verbinden. Verwenden Sie die IP des Outbound-Resolver-Endpunkts nicht als primäres DNS im Spoke. VPCs Spoke VPCs sollte in ihrer VPC den Route 53 Resolver (zum Offset des VPC-CIDR) verwenden.



Zentralisierung von Route 53 Resolver-Endpunkten in VPC ingress/egress

- Eingehende DNS-Auflösung — Erstellen Sie eingehende Route 53 Resolver-Endpunkte in einer zentralen VPC und ordnen Sie alle privaten Hosting-Zonen in Ihrer Landing Zone dieser zentralen VPC zu. Weitere Informationen finden Sie unter Mehr mit einer privaten gehosteten Zone verknüpfen. VPCs Mehrere Private Hosted Zones (PHZ), die einer VPC zugeordnet sind, können sich nicht überschneiden. Wie in der vorherigen Abbildung dargestellt, ermöglicht diese Verknüpfung von PHZ mit der zentralisierten VPC lokale Server, DNS für jeden Eintrag in einer privaten gehosteten Zone (die der zentralen VPC zugeordnet ist) mithilfe des eingehenden Endpunkts in der zentralen VPC aufzulösen. Weitere Informationen zu Hybrid-DNS-Setups finden

Sie unter Zentralisiertes DNS-Management der Hybrid-Cloud mit Amazon Route 53 und AWS Transit Gateway und Hybrid-Cloud-DNS-Optionen für Amazon VPC.

Route 53 DNS-Firewall

Amazon Route 53 Resolver Die DNS-Firewall hilft Ihnen dabei, ausgehenden DNS-Verkehr für Sie zu filtern und zu VPCs regulieren. Die DNS-Firewall wird hauptsächlich verwendet, um die Datenexfiltration Ihrer Daten zu verhindern, indem sie Zulassungslisten für Domainnamen definiert, die es Ressourcen in Ihrer VPC ermöglichen, ausgehende DNS-Anfragen nur für Websites zu stellen, denen Ihr Unternehmen vertraut. Es gibt Kunden auch die Möglichkeit, Blocklisten für Domains zu erstellen, mit denen Ressourcen innerhalb einer VPC nicht über DNS kommunizieren sollen. Amazon Route 53 Resolver Die DNS-Firewall bietet die folgenden Funktionen:

Kunden können Regeln erstellen, um zu definieren, wie DNS-Anfragen beantwortet werden. Zu den Aktionen, die für die Domainnamen definiert werden können`NODATA`, gehören, `OVERRIDE` und`NXDOMAIN`.

Kunden können Warnmeldungen sowohl für Zulassungslisten als auch für Ablehnungslisten erstellen, um die Regelaktivität zu überwachen. Dies kann sich als nützlich erweisen, wenn Kunden die Regel testen möchten, bevor sie sie in die Produktionsumgebung überführen.

Weitere Informationen finden Sie im Blogbeitrag How to Get Started with Amazon Route 53 Resolver DNS Firewall for Amazon VPC.

Zentralisierter Zugriff auf private VPC-Endpunkte

Ein VPC-Endpunkt ermöglicht es Ihnen, Ihre VPC privat mit unterstützten AWS-Services zu verbinden, ohne dass ein Internet-Gateway oder ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung erforderlich ist. Daher ist Ihre VPC nicht im Internet veröffentlicht. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit AWS-Serviceendpunkten mit diesem Schnittstellenendpunkt zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und anderen Services verlässt das AWS-Netzwerk-Backbone nicht. VPC Endpunkte sind virtuelle Geräte. Es handelt sich bei ihnen um horizontal skalierte, redundante und hochverfügbare VPC-Komponenten. Derzeit können zwei Arten von Endpunkten bereitgestellt werden: Schnittstellen-Endpunkte (betrieben von AWS PrivateLink) und Gateway-Endpunkte. Gateway-Endpunkte können für den privaten Zugriff auf Amazon S3- und Amazon DynamoDB-Services verwendet werden. Für die Nutzung von Gateway-Endpunkten fallen keine zusätzlichen Gebühren an. Für die Datenübertragung und Ressourcennutzung fallen die Standardgebühren an.

Schnittstellen-VPC-Endpunkte

Ein Schnittstellenendpunkt besteht aus einer oder mehreren elastischen Netzwerkschnittstellen mit einer privaten IP-Adresse, die als Einstiegspunkt für Datenverkehr dient, der für einen unterstützten Service bestimmt ist. AWS Wenn Sie einen Schnittstellenendpunkt bereitstellen, fallen für jede Stunde, in der der Endpunkt läuft, Kosten sowie Datenverarbeitungsgebühren an. Standardmäßig erstellen Sie in jeder VPC, von der aus Sie auf den AWS Service zugreifen möchten, einen Schnittstellenendpunkt. Dies kann in der Landing Zone-Konfiguration, in der ein Kunde mit einem bestimmten AWS-Service über mehrere hinweg interagieren möchte, unerschwinglich und schwierig zu verwalten sein. VPCs Um dies zu vermeiden, können Sie die Schnittstellenendpunkte in einer zentralen VPC hosten. Alle Spoke VPCs werden diese zentralisierten Endpunkte über Transit Gateway nutzen.

Wenn Sie einen VPC-Endpunkt für einen AWS Dienst erstellen, können Sie privates DNS aktivieren. Wenn diese Einstellung aktiviert ist, erstellt sie eine von AWS verwaltete private Hosted Zone (PHZ) auf Route 53, die die Auflösung des öffentlichen AWS Dienstendpunkts zur privaten IP des Schnittstellenendpunkts ermöglicht. Die verwaltete PHZ funktioniert nur innerhalb der VPC mit dem Schnittstellenendpunkt. Wenn wir in unserem Setup möchten, dass Spoke VPCs VPC-Endpunkt-DNS auflösen kann, das in einer zentralen VPC gehostet wird, funktioniert die verwaltete PHZ nicht. Um dieses Problem zu umgehen, deaktivieren Sie die Option, mit der das private DNS automatisch erstellt wird, wenn ein Schnittstellenendpunkt erstellt wird. Erstellen Sie als Nächstes

manuell eine private gehostete Route 53-Zone, die dem Namen des Dienstendpunkts entspricht, und fügen Sie einen Alias-Datensatz hinzu, dessen vollständiger AWS-Service Endpunktname auf den Schnittstellenendpunkt verweist.

1. Melden Sie sich bei Route 53 an AWS-Managementkonsole und navigieren Sie zu Route 53.
2. Wählen Sie die privat gehostete Zone aus und navigieren Sie zu Create Record.
3. Füllen Sie das Feld Datensatzname aus, wählen Sie für Datensatztyp die Option A aus und aktivieren Sie Alias.

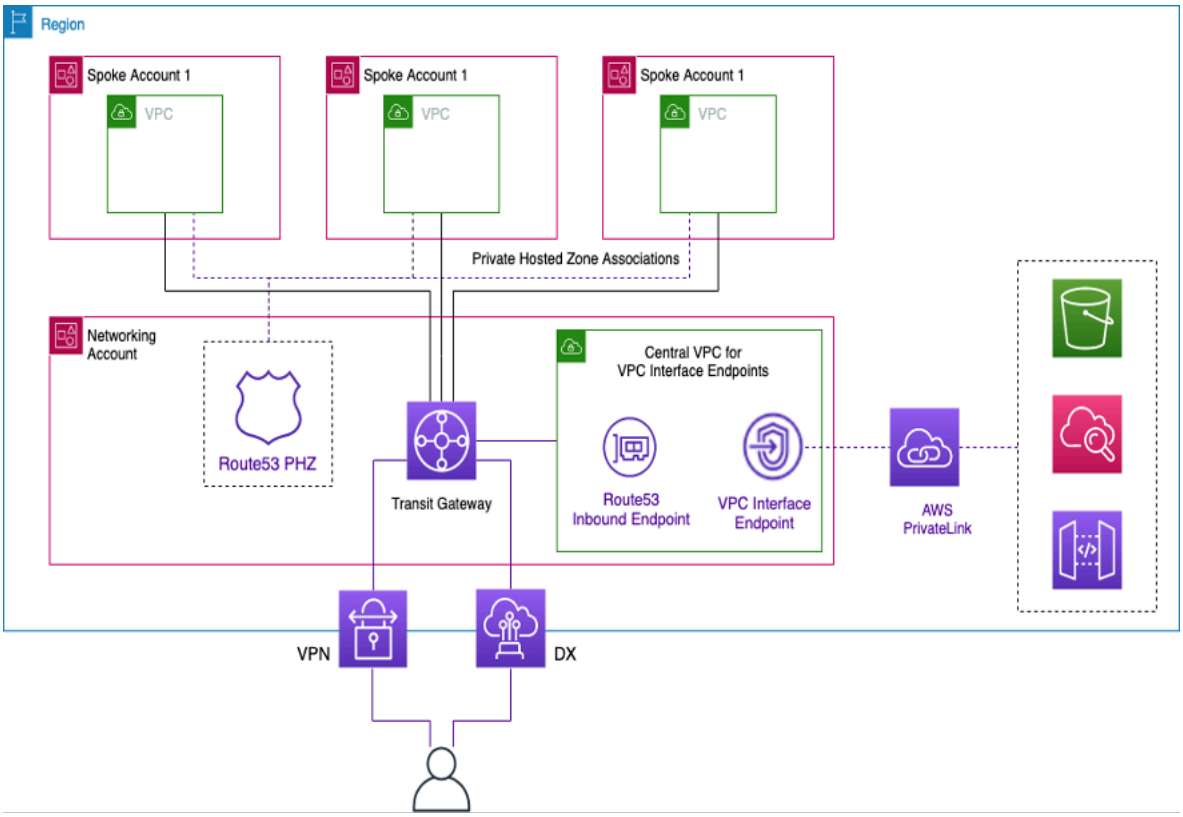
   Beachten Sie, dass für einige Dienste, wie z. B. die Docker- und OCI-Client-Endpunkte (**`dkr.ecr`**), ein Platzhalteralias (**`*`**) für den Datensatznamen verwendet werden muss.
4. Wählen Sie im Abschnitt Traffic weiterleiten an den Service aus, an den der Traffic gesendet werden soll, und wählen Sie die Region aus der Dropdownliste aus.
5. Wählen Sie die entsprechende Routing-Richtlinie aus und aktivieren Sie die Option „Zustand des Ziels bewerten“.

Sie verknüpfen diese private gehostete Zone mit anderen VPCs innerhalb der Landing Zone. Diese Konfiguration ermöglicht es dem Spoke VPCs , die Full-Service-Endpunktnamen für Schnittstellenendpunkte in der zentralen VPC aufzulösen.

> **Note**
>
> Um auf die gemeinsam genutzte private Hosting-Zone zuzugreifen, VPCs sollten die Hosts in der Spoke die Route 53 Resolver-IP ihrer VPC verwenden. Auf Schnittstellenendpunkte kann auch von lokalen Netzwerken aus über VPN und Direct Connect zugegriffen werden. Verwenden Sie Regeln für die bedingte Weiterleitung, um den gesamten DNS-Verkehr für die Full-Service-Endpunktnamen an eingehende Route 53 Resolver-Endpunkte zu senden, die DNS-Anfragen entsprechend der privaten Hosting-Zone auflösen.

In der folgenden Abbildung ermöglicht Transit Gateway den Verkehrsfluss von den Spoke VPCs zu den zentralen Schnittstellenendpunkten. Erstellen Sie VPC-Endpunkte und die private Hosting-Zone dafür im Network Services Account und teilen Sie sie mit VPCs Spoke-in-The-Spoke-Konten. Weitere Informationen zum Teilen von Endpunktinformationen mit anderen VPCs finden Sie im Blogbeitrag Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver.

> **Note**
>
> Ein verteilter VPC-Endpunktansatz, d. h. ein Endpunkt pro VPC, ermöglicht es Ihnen, Richtlinien mit den geringsten Rechten auf VPC-Endpoints anzuwenden. Bei einem zentralisierten Ansatz wenden Sie Richtlinien für den gesamten Spoke-VPC-Zugriff auf einem einzigen Endpunkt an und verwalten diese. Mit der wachsenden Anzahl von Benutzern VPCs kann die Komplexität der Beibehaltung der geringsten Rechte mit einem einzigen Richtliniendokument zunehmen. Ein einziges Strategiedokument führt auch zu einem größeren Explosionsradius. Außerdem sind Sie hinsichtlich der Größe des Richtliniendokuments (20.480 Zeichen) eingeschränkt.



Zentralisierung von VPC-Endpunkten mit Schnittstellen

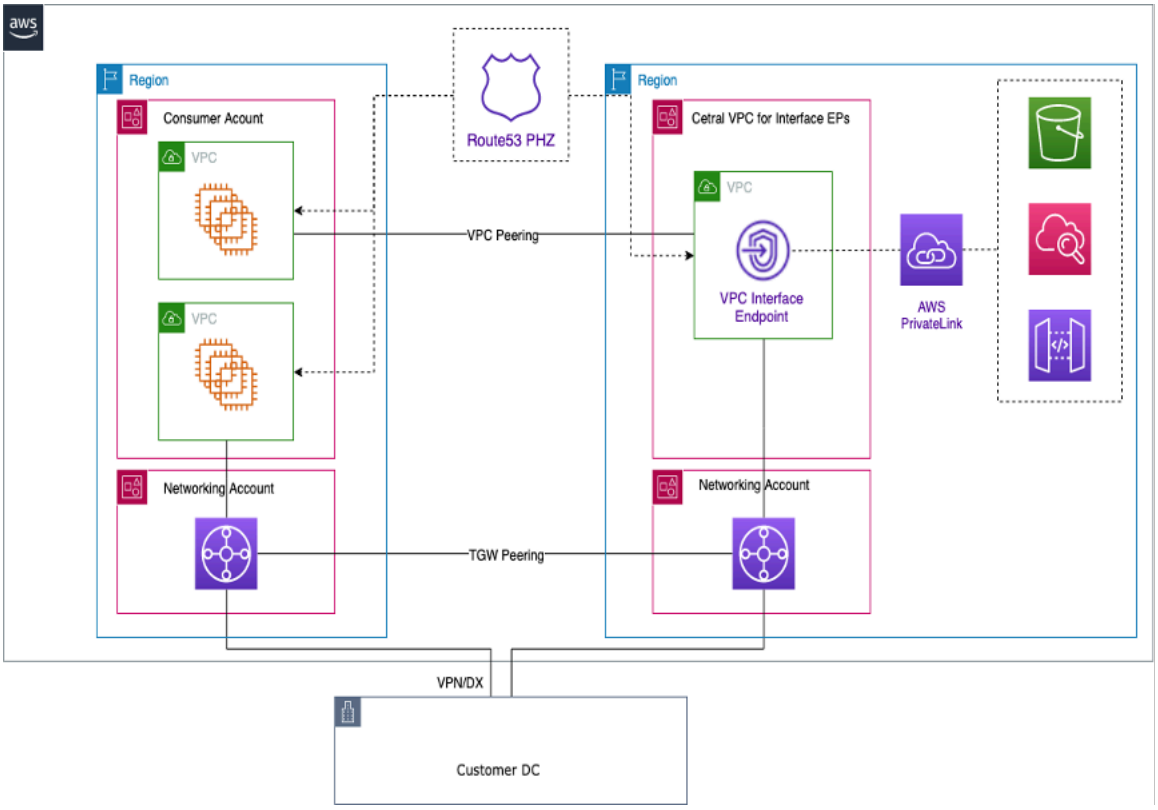
Regionsübergreifender Endpunktzugriff

Wenn Sie mehrere in verschiedenen Regionen VPCs einrichten möchten, die sich einen gemeinsamen VPC-Endpunkt teilen, verwenden Sie eine PHZ, wie bereits beschrieben. Beide VPCs in jeder Region werden der PHZ mit dem Alias für den Endpunkt zugeordnet. Um den Verkehr VPCs

in einer Architektur mit mehreren Regionen weiterzuleiten, müssen die Transit-Gateways in jeder Region miteinander verbunden werden. Weitere Informationen finden Sie in diesem Blog: Using Route 53 Private Hosted Zones for Cross-account Multi-Region-Architectures.

VPCs aus verschiedenen Regionen können entweder mithilfe von Transit Gateways oder VPC Peering zueinander weitergeleitet werden. Verwenden Sie die folgende Dokumentation für das Peering von Transit-Gateways: Transit-Gateway-Peering-Anlagen.

In diesem Beispiel verwendet die EC2 Amazon-Instance in der `us-west-1` VPC-Region die PHZ, um die private IP-Adresse des Endpunkts in der `us-west-2` Region abzurufen und den Datenverkehr über das Transit Gateway Gateway-Peering oder VPC-Peering an die `us-west-2` Regions-VPC weiterzuleiten. Bei Verwendung dieser Architektur verbleibt der Datenverkehr im AWS-Netzwerk, sodass die EC2 Instance auf sichere Weise `us-west-1` auf den VPC-Service zugreifen kann, `us-west-2` ohne über das Internet gehen zu müssen.



VPC-Endpunkte mit mehreren Regionen

> **Note**
>
> Beim Zugriff auf Endpunkte in verschiedenen Regionen fallen Gebühren für die Datenübertragung zwischen Regionen an.

Unter Bezugnahme auf die vorherige Abbildung wird ein Endpunktdienst in einer VPC in der `us-west-2` Region erstellt. Dieser Endpunktservice bietet Zugriff auf einen AWS-Service in dieser Region. Damit Ihre Instances in einer anderen Region (z. B.`us-east-1`) auf den Endpunkt in der `us-west-2` Region zugreifen können, müssen Sie in der PHZ einen Adressdatensatz mit einem Alias für den gewünschten VPC-Endpunkt erstellen.

Stellen Sie zunächst sicher, dass die VPCs in jeder Region mit der von Ihnen erstellten PHZ verknüpft sind.

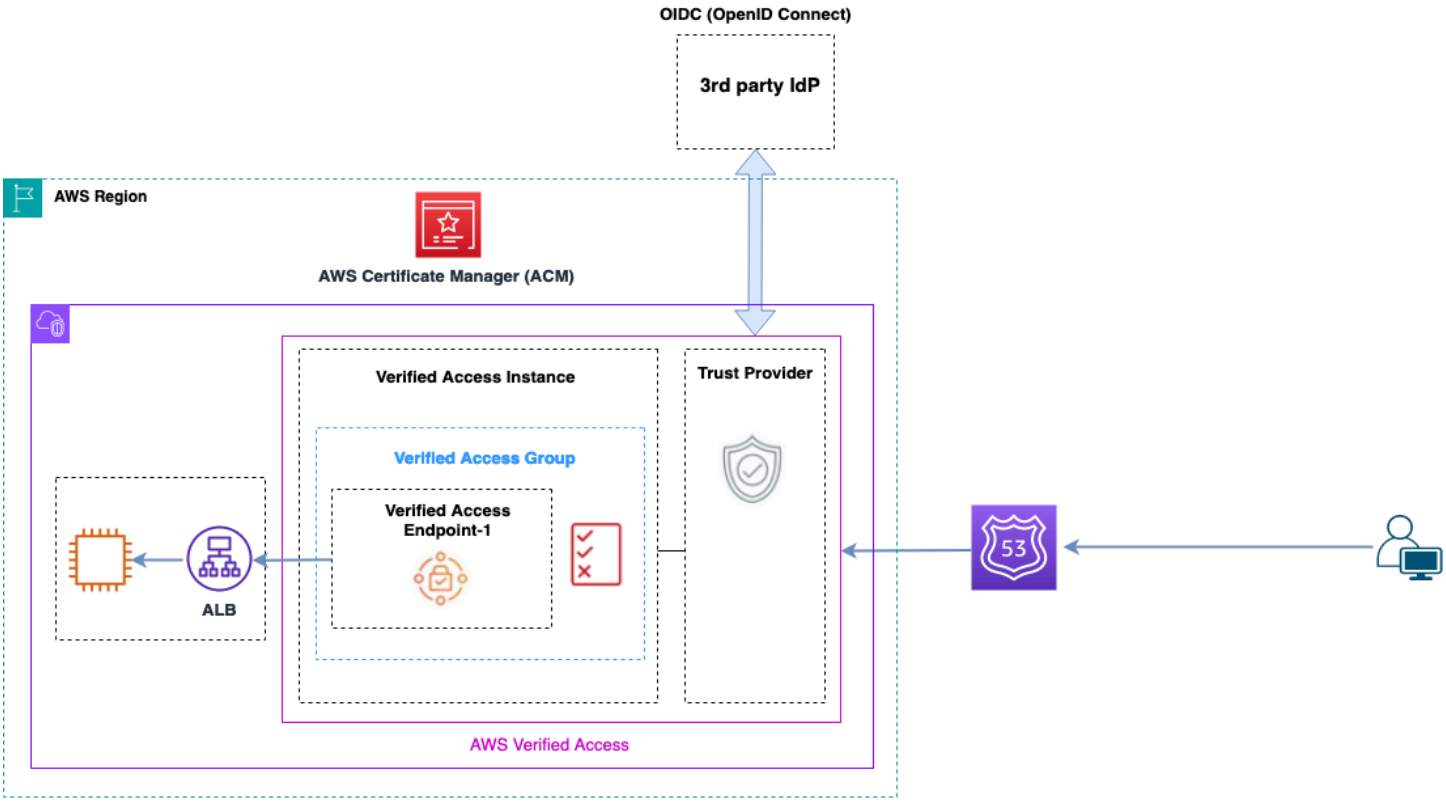
Wenn Sie einen Endpunkt in mehreren Availability Zones bereitstellen, stammt die IP-Adresse des Endpunkts, die von DNS zurückgegeben wird, aus einem der Subnetze in der zugewiesenen Availability Zone.

Verwenden Sie beim Aufrufen des Endpunkts den vollqualifizierten Domänennamen (FQDN), der sich in der PHZ befindet.

AWS Verified Access

AWS Verified Access bietet sicheren Zugriff auf Anwendungen in privaten Netzwerken ohne VPN. Es wertet Anfragen wie Identität, Gerät und Standort in Echtzeit aus. Dieser Dienst gewährt auf der Grundlage von Richtlinien Zugriff auf Anwendungen und verbindet die Benutzer, wodurch die Sicherheit des Unternehmens verbessert wird. Verified Access ermöglicht den Zugriff auf private Anwendungen, indem es als identitätsbewusster Reverse-Proxy fungiert. Benutzeridentität und Geräteintegrität werden, falls zutreffend, vor der Weiterleitung des Datenverkehrs an die Anwendung geprüft.

Das folgende Diagramm bietet einen allgemeinen Überblick über Verified Access. Benutzer senden Anfragen für den Zugriff auf eine Anwendung. Verified Access bewertet die Anfrage anhand der Zugriffsrichtlinie für die Gruppe und aller anwendungsspezifischen Endpunktrichtlinien. Wenn der Zugriff erlaubt ist, wird die Anfrage über den Endpunkt an die Anwendung gesendet.



Überblick über den verifizierten Zugriff

Die Hauptkomponenten einer AWS Verified Access Architektur sind:

- Verifizierte Zugriffsinstanzen — Eine Instanz bewertet Anwendungsanfragen und gewährt Zugriff nur, wenn Ihre Sicherheitsanforderungen erfüllt sind.
- Verifizierte Zugriffsendpunkte — Jeder Endpunkt steht für eine Anwendung. Ein Endpunkt kann eine NLB-, ALB- oder Netzwerkschnittstelle sein.
- Gruppe mit verifiziertem Zugriff — Eine Sammlung von Endpunkten mit verifiziertem Zugriff. Wir empfehlen, die Endpunkte für Anwendungen mit ähnlichen Sicherheitsanforderungen zu gruppieren, um die Richtlinienverwaltung zu vereinfachen.
- Zugriffsrichtlinien — Eine Reihe von benutzerdefinierten Regeln, die festlegen, ob der Zugriff auf eine Anwendung erlaubt oder verweigert wird.
- Trust Providers — Verified Access ist ein Dienst, der die Verwaltung von Benutzeridentitäten und Gerätesicherheitsstatus erleichtert. Er ist sowohl mit Vertrauensanbietern als auch mit Drittanbietern kompatibel AWS und erfordert, dass jeder Verified Access-Instanz mindestens ein Vertrauensanbieter zugeordnet ist. Jede dieser Instanzen kann einen einzelnen Identity Trust Provider sowie mehrere Device Trust Provider umfassen.

- Vertrauensdaten — Die Sicherheitsdaten, die Ihr Vertrauensanbieter an Verified Access sendet, wie z. B. die E-Mail-Adresse eines Benutzers oder die Gruppe, zu der er gehört, werden bei jedem Eingang einer Anwendungsanfrage anhand Ihrer Zugriffsrichtlinien bewertet.

Weitere Informationen finden Sie in den Blogbeiträgen von Verified Access.

Schlussfolgerung

Wenn Sie die Nutzung AWS und Bereitstellung von Anwendungen in der AWS Landing Zone skalieren, nimmt die Anzahl der VPCs Netzwerkkomponenten zu. In diesem Whitepaper wurde erklärt, wie Sie diese wachsende Infrastruktur verwalten können, um Skalierbarkeit, Hochverfügbarkeit und Sicherheit zu gewährleisten und gleichzeitig die Kosten niedrig zu halten. Bei der Verwendung von Services wie Transit Gateway, Shared VPC, VPC-Endpunkten, Gateway Load Balancer Direct Connect, Amazon Route 53 und Software-Appliances von Drittanbietern ist es von AWS Network Firewall entscheidender Bedeutung, die richtigen Designentscheidungen zu treffen. Es ist wichtig, die wichtigsten Überlegungen zu den einzelnen Ansätzen zu verstehen, von Ihren Anforderungen ausgehend zurückzuarbeiten und zu analysieren, welche Option oder Kombination von Optionen am besten zu Ihnen passt.

Mitwirkende

Die folgenden Personen haben zu diesem Dokument beigetragen:

- Sohaib Tahir, Lösungsarchitekt, Amazon Web Services
- Shirin Bhambhani, Lösungsarchitektin, Amazon Web Services
- Kunal Pansari, Lösungsarchitekt, Amazon Web Services
- Eric Vasquez, Lösungsarchitekt, Amazon Web Services
- Tushar Jagdale, Lösungsarchitekt, Amazon Web Services
- Ameer Shariff, Lösungsarchitekt, Amazon Web Services
- Glenn Davis, Lösungsarchitekt, Amazon Web Services
- Nick Kniveton, Lösungsarchitekt, Amazon Web Services
- Sidhartha Chauhan, leitende Lösungsarchitektin, Amazon Web Services

Dokumentverlauf

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Größere Aktualisierung	Updates im gesamten Whitepaper zu Änderungen an CloudWAN, Amazon VPC Lattice, ENA Express, Hybridkonnektivität, Direct Connect Sitelink, Deep Packet Inspection und. AWS Verified Access	17. April 2024
Kleines Update	Die Diagramme wurden aktualisiert, um sie konsistenter zu gestalten, die DX-Konnektivitätsoptionen wurden um private IP-VPNs erweitert und es wurden zahlreiche kleinere Änderungen vorgenommen.	6. Juli 2023
Kleines Update	Aktualisierte AWS Control Tower Informationen, die neue Durchsatzgrenzen für verschiedene Dienste widerspiegeln, aktualisiertes NAT-Gateway-Diagramm, aktualisierter Sicherheitsbereich zur Zentralisierung ausgehender Daten.	4. April 2023

Kleines Update	Abschnitt hinzugefügt: Regionsübergreifender Endpunktzugriff.	19. Juli 2022
Größere Aktualisierung	Aktualisierter Transit Gateway-Bereich mit Transit Gateway Connect, aktualisierter Transit VPC-Bereich; aktualisierter Direct Connect Abschnitt mit Empfehlungen MACsec und Resilienzempfehlungen; aktualisierter AWS PrivateLink Abschnitt. Es wurde eine Vergleichstabelle zwischen VPC-Peering und Transit VPC und Transit Gateway hinzugefügt; ein zentraler Abschnitt zur Eingangsinspektion hinzugefügt; die zentrale Netzwerksicherheit für VPC-to-VPC und VPC-on-premises zu VPC und zentraler Ausgang ins Internet mit AWS Network Firewall und Gateway Load Balancer wurde aktualisiert; die Abschnitte Private NAT-Gateway und Amazon Route 53 DNS-Firewall wurden hinzugefügt.	22. Februar 2022
Kleines Update	Der Abschnitt Transit Gateway im Vergleich zum VPC-Peering wurde aktualisiert	2. April 2021

Whitepaper aktualisiert	Der Text wurde so korrigiert, dass er den in Abbildung 7 dargestellten Optionen entspricht	10. Juni 2020
Erste Veröffentlichung	Whitepaper veröffentlicht.	15. November 2019

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS-Produktangebote und -praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS-Produkte oder -Services werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.