AWS Weißbuch

Hybride Konnektivität

Hybride Konnektivität: AWS Weißbuch

Table of Contents

Hybride Konnektivität

Datum der Veröffentlichung: 6. Juli 2023 (Dokumentversionen)

Viele Unternehmen müssen ihre lokalen Rechenzentren, Remote-Standorte und die Cloud miteinander verbinden. Ein hybrides Netzwerk verbindet diese verschiedenen Umgebungen. In diesem Whitepaper werden die AWS-Bausteine und die wichtigsten Anforderungen beschrieben, die Sie bei der Entscheidung, welches Hybrid-Konnektivitätsmodell für Sie geeignet ist, berücksichtigen sollten. Um Ihnen dabei zu helfen, die beste Lösung für Ihre geschäftlichen und technischen Anforderungen zu finden, stellen wir Entscheidungsbäume zur Verfügung, die Sie durch den logischen Auswahlprozess führen.

Einführung

Ein modernes Unternehmen nutzt eine Vielzahl von IT-Ressourcen. In der Vergangenheit war es üblich, diese Ressourcen in einem lokalen Rechenzentrum oder einer Colocation-Einrichtung zu hosten. Mit der zunehmenden Verbreitung von Cloud Computing stellen Unternehmen IT-Ressourcen von Cloud-Dienstanbietern über eine Netzwerkverbindung bereit und nutzen diese. Organizations können sich dafür entscheiden, einige oder alle ihrer vorhandenen IT-Ressourcen in die Cloud zu migrieren. In beiden Fällen ist ein gemeinsames Netzwerk erforderlich, um lokale Ressourcen und Cloud-Ressourcen miteinander zu verbinden. Die Koexistenz von lokalen und Cloud-Ressourcen wird als Hybrid-Cloud bezeichnet, und das gemeinsame Netzwerk, das sie verbindet, wird als Hybrid-Netzwerk bezeichnet. Selbst wenn Ihr Unternehmen all seine IT-Ressourcen in der Cloud aufbewahrt, ist möglicherweise dennoch eine hybride Konnektivität zu Remote-Standorten erforderlich.

Es stehen mehrere Konnektivitätsmodelle zur Auswahl. Optionen erhöhen zwar die Flexibilität, die Auswahl der optimalen Option erfordert jedoch eine Analyse der geschäftlichen und technischen Anforderungen und die Eliminierung ungeeigneter Optionen. Sie können Anforderungen nach Gesichtspunkten wie Sicherheit, Bereitstellungszeit, Leistung, Zuverlässigkeit, Kommunikationsmodell, Skalierbarkeit und mehr gruppieren. Nachdem sie die Anforderungen sorgfältig gesammelt, analysiert und berücksichtigt haben, können Netzwerk- und Cloud-Architekten die geeigneten Bausteine und Lösungen für AWS hybride Netzwerke identifizieren. Um das oder die optimalen Modelle zu identifizieren und auszuwählen, müssen Architekten die Vor- und Nachteile der einzelnen Modelle verstehen. Es gibt auch technische Einschränkungen, die dazu führen könnten, dass ein ansonsten geeignetes Modell ausgeschlossen wird.

Um den Auswahlprozess zu vereinfachen, führt Sie dieses Whitepaper in logischer Reihenfolge durch alle wichtigen Überlegungen. Zu jeder Überlegung gehören Fragen, anhand derer Anforderungen gesammelt werden. Die Auswirkungen jeder Entwurfsentscheidung werden zusammen mit möglichen Lösungen identifiziert. Das Whitepaper stellt Entscheidungsbäume für einige der Überlegungen als Methode vor, um den Entscheidungsprozess zu unterstützen, Optionen auszuschließen und die Konsequenzen jeder Entscheidung zu verstehen. Es schließt mit einem Szenario, das einen hybriden Anwendungsfall abdeckt, wobei die Auswahl und das Design des end-to-end Konnektivitätsmodells angewendet werden. Anhand dieses Beispiels können Sie anhand eines praktischen Beispiels sehen, wie die in diesem Whitepaper beschriebenen Prozesse ausgeführt werden.

Dieses Whitepaper soll Ihnen helfen, ein optimales Hybrid-Konnektivitätsmodell auszuwählen und zu entwerfen. Dieses Whitepaper ist folgendermaßen strukturiert:

- Bausteine für hybride Konnektivität — Ein Überblick über AWS Dienste, die für hybride Konnektivität verwendet werden.
- Überlegungen zur Auswahl und zum Design der Konnektivität — Definition der einzelnen Konnektivitätsmodelle, deren Auswirkungen auf die Entwurfsentscheidung, Fragen zur Identifizierung von Anforderungen, Lösungen und Entscheidungsbäume.
- Ein Anwendungsfall beim Kunden — Ein Beispiel dafür, wie die Überlegungen und Entscheidungsbäume in der Praxis angewendet werden können.

Sind Sie Well-Architected?

Das AWSWell-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 Management Console, 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

AWSBausteine für hybride Konnektivität

Es gibt drei Bausteine einer hybriden Netzwerkkonnektivitätsarchitektur:

- Hybride Netzwerkverbindungen: Die Verbindungstypen zwischen AWS Konnektivitätsdiensten und lokalen Kunden-Gateway-Geräten.
- AWShybride Konnektivitätsdienste: Die AWS Dienste, die Konnektivität und Routing zwischen der Kundeninfrastruktur und AWS bereitstellen.
- Kunden-Gateway-Gerät vor Ort: Das Gerät im bestehenden Kundennetzwerk, das als lokaler Endpunkt für hybride Netzwerkverbindungen dient. Verschiedene Verbindungstypen haben unterschiedliche technische Anforderungen für diese Geräte, die in den folgenden Abschnitten behandelt werden.

Hybride Netzwerkverbindungen

Es gibt mehrere Möglichkeiten, eine Verbindung zwischen Ihrem Standort und AWS herzustellen. Dieses Whitepaper konzentriert sich darauf, wie diese verschiedenen Möglichkeiten zu Gesamtarchitekturen kombiniert werden können. Es wird jedoch ein kurzer Überblick über die verschiedenen Optionen (AWS Direct ConnectSite-to-Site Virtual Private Network und Transit Gateway Connect) gegeben.

AWS Direct Connect

AWS Direct Connectist ein Service, der eine dedizierte Netzwerkverbindung von Ihrem Standort zu erstelltAWS. Details dazu finden Sie unter AWS Direct Connect.

Es gibt zwei Arten von AWS Direct Connect Verbindungen: dedizierte und gehostete. Eine dedizierte Verbindung ist eine direkte Verbindung zwischen einem AWS Gerät und Ihrem lokalen Gerät, wohingegen eine gehostete Verbindung von einem AWS Partner unterstützt wird, der die Verbindungsdetails für Sie übernehmen kann. Weitere Informationen finden Sie unter AWS Direct ConnectVerbindungen.

Eine Direct Connect-Verbindung verwendet virtuelle Schnittstellen (VIFs), um verschiedene Verkehrsflüsse zu isolieren. Mehrere VIFs können dieselbe Direct Connect verwenden, getrennt durch VLAN-Tags (802.1q). Es gibt drei Arten von VIFs, die Konnektivität zum Netzwerk bereitstellen. AWS Weitere Informationen finden Sie unter AWS Direct Connectvirtuelle Schnittstellen. Die drei Typen sind folgende:

- Private VIF: Eine private VIF ist eine private Verbindung zwischen Ihrem Gerät und Ihren Ressourcen darin. AWS Diese enden entweder direkt AWS auf einem Virtual Private Gateway (VGW) (das eine einzelne VPC unterstützt) oder über ein Direct Connect Gateway, das dann eine Verbindung zu mehreren VGWs herstellt.
- Öffentliche VIF: Eine öffentliche VIF ermöglicht Konnektivität zu beliebigen öffentlichen AWS Ressourcen wie S3, DynamoDB und öffentlichen EC2-IP-Bereichen. Eine öffentliche VIF hat zwar keinen direkten Zugang zum Internet, aber jede öffentliche Ressource von Amazon kann sie erreichen (einschließlich der öffentlichen EC2-Instances anderer Kunden), was Kunden bei der Sicherheitsplanung berücksichtigen sollten.
- Transit-VIF: Eine Transit-VIF ist eine private Verbindung zwischen Ihrem Gerät und einemAWS Transit Gateway, über ein Direct Connect Gateway. Transit-VIFs werden jetzt auf Verbindungen mit Geschwindigkeiten von weniger als 1 Gbit/s unterstützt. Einzelheiten finden Sie in der Ankündigung zur Markteinführung.

> **Note**
>
> Eine gehostete virtuelle Schnittstelle (Hosted VIF) ist eine Art von privater VIF, bei der die VIF einer anderen Person zugewiesen wird AWS-Konto als der, der AWS-Konto die AWS Direct Connect Verbindung besitzt (zu der auch ein Partner gehören kann). AWS Direct Connect AWSerlaubt neuen Partnern nicht mehr, dieses Modell anzubieten. Weitere Informationen finden Sie unter Erstellen einer gehosteten virtuellen Schnittstelle.

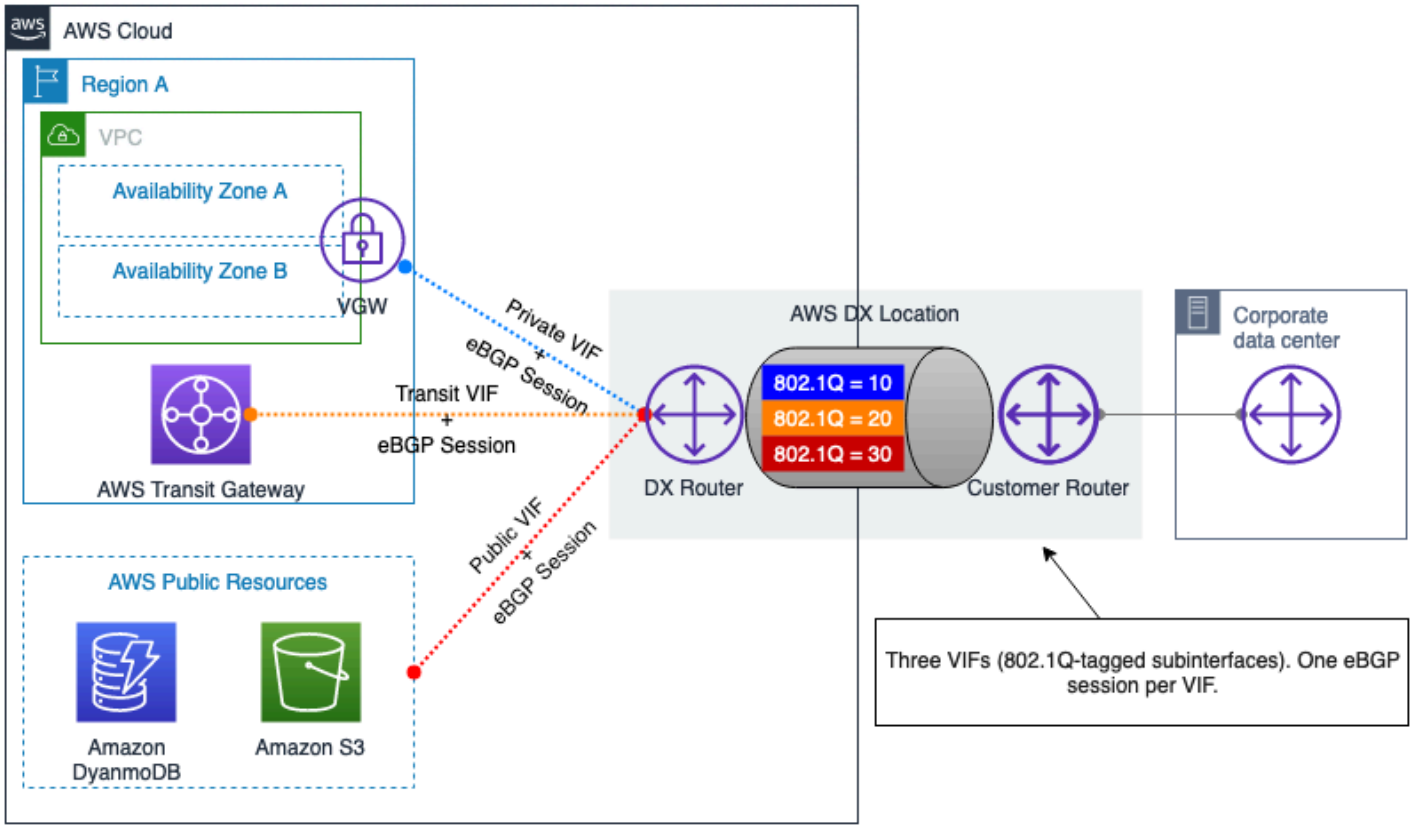

Abbildung 1 — AWS Direct Connect Private und öffentliche VIFs

Virtuelles privates Netzwerk (VPN) von Standort zu Standort

Ein site-to-site VPN ermöglicht die sichere Kommunikation zweier Netzwerke und kann über einen nicht vertrauenswürdigen Transport wie das Internet verwendet werden. Kunden können VPN-Verbindungen zwischen lokalen Standorten und Amazon Virtual Private Clouds (Amazon VPC) über zwei Optionen herstellen:

- AWSManaged Site-to-Site VPN (AWSS2S VPN): Dies ist ein vollständig verwalteter und hochverfügbarer VPN-Dienst, der IPSec verwendet. Weitere Informationen finden Sie unter Was ist. AWS Site-to-Site VPN Sie können optional die Beschleunigung für Ihre Site-to-Site-VPN-Verbindung aktivieren. Weitere Informationen finden Sie unter Beschleunigte Site-to-Site-VPN-Verbindungen. S2S VPN kann auch Direct Connect-Transit-VIFs verwenden, um zu verhindern, dass der Datenverkehr das Internet durchquert, was die Kosten senkt und die Verwendung privater IP-Adressen ermöglicht. Einzelheiten finden Sie unter Privates IP-VPN mit. AWS Direct Connect
- Software Site-to-Site VPN (vom Kunden verwaltetes VPN): Bei dieser VPN-Konnektivitätsoption sind Sie für die Bereitstellung und Verwaltung der gesamten VPN-Lösung verantwortlich, in der

Regel indem Sie VPN-Software auf einer EC2-Instance ausführen. Weitere Informationen finden Sie unter Software Site-to-Site VPN.

Beide Optionen erfordern Unterstützung auf dem Gateway-Gerät des Kunden, um das lokale Ende der VPN-Tunnel zu beenden. Dieses Gerät kann ein physisches Gerät oder eine Software-Appliance sein. Weitere Informationen zu Netzwerkgeräten, die von getestet wurdenAWS, finden Sie in der Liste der getesteten Gateway-Geräte von Kunden.

Transit-Gateway-Verbindung (TGW-Verbindung)

Transit Gateway Connect verwendet GRE-Tunnel zwischen einem AWS Transit Gateway und einem lokalen Gateway-Gerät. BGP wird zusätzlich zu TGW Connect verwendet, um dynamisches Routing zu ermöglichen. Beachten Sie, dass TGW Connect nicht verschlüsselt ist. Weitere Informationen finden Sie unter Transit Gateway Connect.

AWShybride Konnektivitätsdienste

AWSHybride Konnektivitätsdienste bieten hoch skalierbare, hochverfügbare Netzwerkkomponenten. Sie spielen eine wichtige Rolle beim Aufbau hybrider Netzwerklösungen. Zum Zeitpunkt der Erstellung dieses Whitepapers gibt es drei primäre Service-Endpunkte:

- AWSVirtual Private Gateway (VGW) ist ein regionaler, hochredundanter Dienst, der IP-Routing und -Weiterleitung auf VPC-Ebene bereitstellt und als Gateway für die VPC für die Kommunikation mit den Gateway-Geräten Ihrer Kunden fungiert. VGW kann AWS S2S-VPN-Verbindungen und private VIFs beenden. AWS Direct Connect
- AWS Transit Gateway(TGW) ist ein regionaler, hochverfügbarer und skalierbarer Dienst, mit dem Sie mehrere VPCs sowie Ihre lokalen Netzwerke über Site-to-Site VPN und/oder Direct Connect über ein einziges zentrales Gateway miteinander verbinden können. Konzeptionell AWS Transit Gateway fungiert ein als hochverfügbarer und redundanter virtueller Cloud-Router. AWS Transit Gatewayunterstützt ECMP-Routing (Equal Cost Multipath) über mehrere Direct Connect-Verbindungen, VPN-Tunnel oder TGW Connect-Peers. Transit Gateways können sowohl in derselben Region als auch regionsübergreifend miteinander kommunizieren, sodass ihre verbundenen Ressourcen über die Peering-Links kommunizieren können. Weitere Informationen finden Sie unter AWS Transit GatewaySzenarien.
- AWS CloudWAN bietet ein zentrales Dashboard, über das Sie Verbindungen zwischen Ihren Niederlassungen, Rechenzentren und Amazon VPCs herstellen und mit nur wenigen Klicks ein globales Netzwerk aufbauen können. Sie verwenden Netzwerkrichtlinien, um

Netzwerkmanagement- und Sicherheitsaufgaben an einem Standort zu automatisieren. Weitere Informationen finden Sie in der AWS CloudWAN-Dokumentation.

- Direct Connect Gateway (DXGW) ist ein weltweit verfügbarer Dienst, der Routing-Informationen über seine Verbindungen verteilt und sich dabei ähnlich wie BGP-Routenreflektoren in einem herkömmlichen Netzwerk verhält. Daten werden nicht durch ein DXGW geleitet — es verarbeitet nur die Routing-Informationen. Sie können in jedem DXGW ein DXGW erstellen AWS-Region und von allen anderen darauf zugreifen. AWS-Regionen Sie können Direct Connect-VIFs mit einem DXGW verbinden und das DXGW dann entweder VGWs (unter Verwendung von privaten VIFs) oder einem (unter Verwendung von Transit-VIFs) zuordnen. AWS Transit Gateway Weitere Informationen finden Sie unter Direct Connect-Gateways. Aus Redundanzgründen müssen Sie nicht mehrere DXGWs erstellen, da es sich um einen Service mit globaler Verfügbarkeit handelt. Sie können sich jedoch dafür entscheiden, mehrere DXGWs zu verwenden, um Routingdomänen zu trennen, z. B. ein Produktions- und ein Testnetzwerk, das Sie vollständig isoliert halten möchten.

Überlegungen zu Art und Design der Hybridkonnektivität

In diesem Abschnitt des Whitepapers werden die Überlegungen behandelt, die sich auf Ihre Entscheidungen bei der Auswahl eines Hybridnetzwerks auswirken, mit dem Sie Ihre lokalen Umgebungen verbinden möchten. AWS Es folgt einem logischen Denkprozess, der Sie bei der Auswahl einer optimalen Hybrid-Konnektivitätslösung unterstützen soll. Die Überlegungen, die sich auf Ihren Entwurf auswirken, sind in Überlegungen unterteilt, die sich auf Ihren Konnektivitätstyp auswirken, und Überlegungen, die sich auf Ihr Konnektivitätsdesign auswirken. Überlegungen zum Konnektivitätstyp helfen Ihnen bei der Entscheidung, ob Sie ein internetbasiertes VPN oder Direct Connect verwenden möchten. Überlegungen zum Konnektivitätsdesign helfen Ihnen bei der Entscheidung, wie die Verbindungen eingerichtet werden sollen.

Die folgenden Überlegungen, die sich auf Ihren Konnektivitätstyp auswirken, werden behandelt: Zeit bis zur Bereitstellung, Sicherheit, SLA, Leistung und Kosten. Nachdem Sie diese Überlegungen und deren Auswirkungen auf Ihre Entwurfsentscheidungen geprüft haben, können Sie entscheiden, ob die Verwendung einer internetbasierten Verbindung oder Direct Connect zur Erfüllung Ihrer Anforderungen empfohlen wird.

Die folgenden Überlegungen, die sich auf Ihr Konnektivitätsdesign auswirken, werden behandelt: Skalierbarkeit, Kommunikationsmodell, Zuverlässigkeit und SD-WAN-Integration von Drittanbietern. Nachdem Sie diese Überlegungen und deren Auswirkungen auf Ihre Entwurfsentscheidungen geprüft haben, können Sie entscheiden, welches optimale logische Design für Ihre Anforderungen empfohlen wird.

Die folgende Struktur wird verwendet, um die einzelnen Auswahl- und Entwurfsüberlegungen zu erörtern und zu analysieren:

- Definition — Kurze Definition dessen, was die Überlegung ist.
- Wichtige Fragen — Enthält eine Reihe von Fragen, anhand derer Sie die mit der Überlegung verbundenen Anforderungen zusammenfassen können.
- Zu berücksichtigende Fähigkeiten — Lösungen zur Erfüllung der mit der Prüfung verbundenen Anforderungen.
- Entscheidungsbaum — Für einige Überlegungen oder eine Gruppe von Überlegungen steht ein Entscheidungsbaum zur Verfügung, der Sie bei der Auswahl der optimalen hybriden Netzwerklösung unterstützt.

Die Überlegungen, die Ihr hybrides Netzwerkdesign beeinflussen, werden in einer Reihenfolge behandelt, in der das Ergebnis einer Überlegung Teil der Eingabe für die nachfolgende Überlegung ist. Wie in Abbildung 2 dargestellt, besteht der erste Schritt darin, sich für den Konnektivitätstyp zu entscheiden und ihn anschließend anhand der Überlegungen zur Entwurfsauswahl zu verfeinern.

Abbildung 2 zeigt die beiden Kategorien von Überlegungen, die einzelnen Überlegungen und die logische Reihenfolge, in der die Überlegungen in den nachfolgenden Unterabschnitten behandelt werden. Dies sind die wichtigsten Überlegungen, wenn Sie eine Entscheidung über den Entwurf eines hybriden Netzwerks treffen. Wenn das angestrebte Design nicht all diese Überlegungen erfordert, können Sie sich auf die Überlegungen konzentrieren, die für Ihre Anforderungen relevant sind.

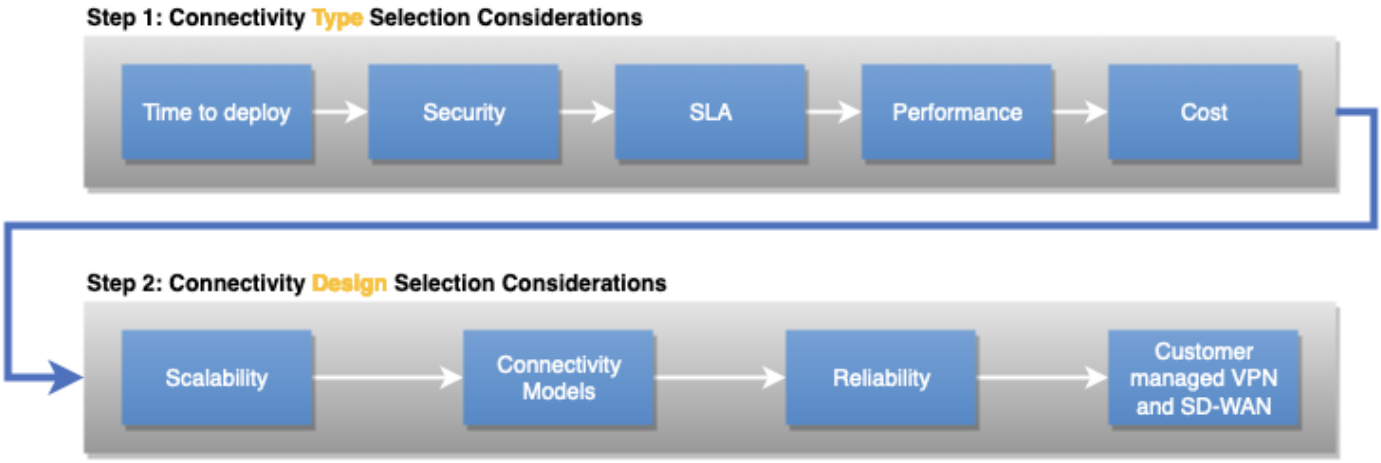

Abbildung 2 — Kategorien von Überlegungen, Einzelaspekte und deren logische Reihenfolge

Auswahl des Konnektivitätstyps

In diesem Abschnitt werden Überlegungen behandelt, die sich auf den Konnektivitätstyp auswirken, den Sie für Ihren Workload auswählen. Dazu gehören Bereitstellungszeit, Sicherheit, SLA, Leistung und Kosten.

Überlegungen

- Zeit für den Einsatz
- Sicherheit
- Service Level Agreement (SLA)
- Leistung
- Kosten

Zeit für den Einsatz

Definition

Die Zeit bis zur Bereitstellung kann ein wichtiger Faktor bei der Auswahl eines geeigneten Konnektivitätstyps für einen Workload sein. Abhängig von der Art der Konnektivität und den Standorten vor Ort kann die Konnektivität innerhalb von Stunden hergestellt werden. Es kann jedoch Wochen oder Monate dauern, wenn zusätzliche Leitungen installiert werden müssen. Dies beeinflusst Ihre Entscheidung, eine internetbasierte Verbindung, eine private dedizierte Verbindung oder eine private gehostete Verbindung zu verwenden, die von einem Partner als verwalteter Service bereitgestellt wird. AWS Direct Connect

Die wichtigsten Fragen

- Was ist der erforderliche Zeitplan für die Bereitstellung — Stunden, Tage, Wochen oder Monate?
- Wie lange wird die Verbindung benötigt — handelt es sich um ein kurzlebiges Projekt oder um eine permanente Infrastruktur?

Zu berücksichtigende Fähigkeiten

Wenn Sie innerhalb von Stunden oder Tagen AWS Konnektivität benötigen, müssen Sie höchstwahrscheinlich eine bestehende Netzwerkverbindung verwenden. Dies bedeutet häufig, dass eine VPN-Verbindung AWS über das öffentliche Internet hergestellt wird. Wenn ein vorhandener AWS DX-Partner Ihnen private AWS Konnektivität zur Verfügung stellt, kann innerhalb weniger Stunden eine neue gehostete Verbindung bereitgestellt werden.

Wenn Sie Tage oder Wochen Zeit haben, können Sie mit einem AWS Direct Connect Partner zusammenarbeiten, um eine private Konnektivität herzustellen. AWS AWS Direct Connect Partner helfen Ihnen dabei, Netzwerkkonnektivität zwischen AWS Direct Connect Standorten und Ihrem Rechenzentrum, Büro oder Ihrer Kollokationsumgebung herzustellen. Bestimmte AWS Direct ConnectPartner sind berechtigt, Direct Connect Hosted Connections anzubieten. Gehostete Verbindungen können oft schneller bereitgestellt werden als dedizierte Verbindungen. AWS Direct Connect Der Partner stellt jede gehostete Verbindung über seine bestehende Infrastruktur bereit, die mit dem AWS Backbone verbunden ist.

Wenn Sie mehrere Wochen bis Monate Zeit haben, können Sie den Aufbau einer dedizierten privaten Verbindung mit prüfenAWS. Dienstanbieter und AWS Direct Connect Partner ermöglichen AWS

Direct Connect dedizierte Verbindungen. Es ist üblich, dass Dienstanbieter Netzwerkgeräte am Standort des Kunden installieren, um eine dedizierte Direct Connect-Verbindung zu ermöglichen. Je nach Dienstanbieter, Standort Ihres Standorts und anderen physikalischen Faktoren kann die Installation einer Direct Connect Dedicated Connection mehrere Wochen bis einige Monate dauern.

Wenn Sie Ihre Netzwerkausrüstung bereits in derselben Colocation-Einrichtung installiert haben, in der sich der AWS Direct Connect Standort befindet, können Sie schnell eine AWS Direct Connect dedizierte Verbindung über eine Querverbindung am Colocation-Standort einrichten. Stellt Ihnen, nachdem Sie die Verbindung angefordert haben, AWS ein LOA-CFA (Letter of Authorization and Connecting Facility Assignment) zum Herunterladen zur Verfügung oder sendet Ihnen eine E-Mail mit der Bitte um weitere Informationen. Der LOA-CFA ist die Autorisierung, mit der Sie eine Verbindung herstellen könnenAWS, und wird von Ihrem Netzwerkanbieter benötigt, um eine Cross-Connect-Verbindung für Sie zu bestellen.

Tabelle 1 — Vergleich der Kostenwirksamkeit

	Internetbasierte Konnektivität	Dedizierte DX-Verbindung (vorhandene Geräte am DX-Standort)	Dedizierte DX-Verbindung (neuwertig)	Gehostete DX-Verbindung (vorhandener Port mit DX-Partner)	DX Hosted Connection (neuwertig)
Bereitstellungszeit	Stunden bis Tage	Tage	Mehrere Wochen bis Monate	Stunden bis Tage	Mehrere Tage bis Wochen bis Monate

> **Note**
>
> Die bereitgestellten Richtlinien für die Bereitstellungszeit basieren auf realen Beobachtungen und dienen nur der Veranschaulichung. Wenn Sie den Standort Ihres Standorts, die Nähe zu Standorten mit Direktverbindungen und die bereits vorhandene Infrastruktur berücksichtigen, wirken sich all diese Faktoren auf die Bereitstellungszeit aus. Ihr AWS Direct Connect Partner wird Sie bezüglich der genauen Bereitstellungszeit beraten.

Sicherheit

Definition

Die Sicherheitsanforderungen wirken sich auf Ihren Hybrid-Konnektivitätstyp aus. Zu diesen Überlegungen gehören:

- Transporttyp — Internet- oder private Netzwerkverbindung
- Anforderungen an die Verschlüsselung

Die wichtigsten Fragen

- Erlauben Ihre Sicherheitsanforderungen und -richtlinien die Verwendung verschlüsselter Verbindungen über das InternetAWS, um eine Verbindung herzustellen, oder schreiben sie die Verwendung von privaten Netzwerkverbindungen vor?
- Muss die Netzwerkschicht bei der Nutzung privater Netzwerkverbindungen für Verschlüsselung bei der Übertragung sorgen?

Technische Lösungen

Ihre Sicherheitsanforderungen und -richtlinien erlauben möglicherweise die Nutzung des Internets oder erfordern die Verwendung einer privaten Netzwerkverbindung zwischen Ihrem Unternehmensnetzwerk AWS und Ihrem Unternehmensnetzwerk. Sie wirken sich auch auf die Entscheidung aus, ob das Netzwerk Verschlüsselung bei der Übertragung bereitstellen muss oder ob eine Verschlüsselung auf Anwendungsebene zulässig ist.

Wenn Sie das Internet nutzen können, AWS Site-to-Site VPN kann es verwendet werden, um verschlüsselte Tunnel zwischen Ihrem Netzwerk und Ihren Amazon VPCs oder AWS Transit Gateway s über das Internet zu erstellen. Die Erweiterung Ihrer SD-WAN-Lösung AWS auf das Internet ist auch eine Option, wenn Sie eine internetbasierte Verbindung nutzen. Im Abschnitt Kundenverwaltetes VPN und SD-WAN weiter unten in diesem Whitepaper werden die spezifischen Überlegungen zu SD-WAN behandelt.

Wenn Sie eine private Netzwerkverbindung zwischen Ihrem Unternehmensnetzwerk AWS und Ihrem Unternehmensnetzwerk benötigen, AWS empfiehlt es sich, Dedicated Connections oder Hosted Connections zu verwendenAWS Direct Connect. Wenn eine Verschlüsselung bei der Übertragung über eine private Netzwerkverbindung erforderlich ist, sollten Sie ein VPN über Direct Connect

einrichten (entweder über öffentliches VIF oder Transit-VIF) oder die Verwendung von MACSec auf einer dedizierten 10-Gbit/s- oder 100-Gbit/s-Verbindung in Betracht ziehen.

Tabelle 2 — Beispiel für Anforderungen an den Konnektivitätstyp von Automotive Corp.

	Site-to-Site-VPN	Direct Connect
Transport	Internet	Private Netzwerkverbindung
Verschlüsselung während der Übertragung	Ja	Erfordert S2S VPN über DX, S2S VPN über eine Transit-VIF oder MACSec auf einer dedizierten Verbindung mit 10 Gbit/s oder 100 Gbit/s

Service Level Agreement (SLA)

Definition

Unternehmensorganisationen verlangen häufig von einem Dienstleister, dass er für jeden Service, den das Unternehmen in Anspruch nimmt, ein SLA einhält. Die Organisation wiederum baut darauf ihre eigenen Dienste auf und kann ihren eigenen Kunden ein SLA anbieten. Das SLA ist wichtig, da es beschreibt, wie der Dienst bereitgestellt und betrieben wird, und es enthält häufig spezifische messbare Merkmale, wie z. B. die Verfügbarkeit. Sollte der Service gegen die definierte SLA verstoßen, bietet ein Dienstanbieter in der Regel eine finanzielle Entschädigung an, die in der Vereinbarung festgelegt ist. Eine SLA definiert die Art der Maßnahme, die Anforderung und den Messzeitraum. Ein Beispiel finden Sie in der Definition des Verfügbarkeitsziels im Rahmen der AWS Direct Connect SLA.

Die wichtigsten Fragen

- Ist ein SLA für Hybrid-Konnektivitätsverbindungen mit Servicegutschriften erforderlich?
- Muss das gesamte Hybridnetzwerk ein Verfügbarkeitsziel einhalten?

Zu berücksichtigende Fähigkeiten

Art der Konnektivität: Die Internetverbindung kann unvorhersehbar sein. Die Verwaltung des Internets AWS erfordert zwar große Sorgfalt, wenn mehrere Links zu einer Vielzahl von ISPs eingerichtet

werden, aber die Verwaltung des Internets erfolgt einfach außerhalb der AWS administrativen Domäne eines einzelnen Anbieters. Ein Cloud-Anbieter kann nur eine begrenzte Menge an Routenplanung und Verkehrsbeeinflussung vornehmen, sobald der Verkehr die Grenze seines Netzwerks verlassen hat. Allerdings gibt es ein AWS Site-to-Site VPNSLA, das Verfügbarkeitsziele für AWS Site-to-Site VPN Endgeräte vorsieht.

AWSDirect Connect bietet ein formelles SLA mit Servicegutschriften, die als Prozentsatz der gesamten AWS Direct Connect Hafenstundengebühren berechnet werden, die Sie für die betreffenden Verbindungen bezahlt haben, die in dem monatlichen Abrechnungszeitraum, in dem die SLA nicht eingehalten wurde, nicht verfügbar waren. Dies ist der empfohlene Transport, wenn eine SLA erforderlich ist. AWS Direct Connectlistet spezifische Mindestkonfigurationsanforderungen für jedes Verfügbarkeitsziel auf, z. B. Anzahl der AWS Direct Connect Standorte, Verbindungen und andere Konfigurationsdetails. Die Nichterfüllung der Anforderungen bedeutet, dass keine Service-Credits angeboten werden können, sollte der Service gegen definierte SLAs verstoßen.

Wichtig ist, dass selbst wenn der für die Hybridkonnektivität ausgewählte Dienst so konfiguriert ist, dass er die SLA-Anforderungen erfüllt, der Rest des Netzwerks möglicherweise nicht das gleiche SLA-Niveau bietet. Die AWS Verantwortung endet am AWS Direct Connect Standort im AWS Direct Connect Hafen. Sobald AWS der Datenverkehr an das Netzwerk Ihres Unternehmens weitergeleitet wurde, liegt er nicht mehr in der Verantwortung vonAWS. Wenn Sie einen Dienstanbieter zwischen AWS und Ihrem lokalen Netzwerk verwenden, unterliegt die Konnektivität gegebenenfalls einer SLA zwischen Ihnen und dem Dienstanbieter. Denken Sie bei der Entwicklung hybrider Konnektivität daran, dass das gesamte Hybridnetzwerk nur so gut ist wie der schwächste Teil davon.

AWS Direct ConnectPartner bieten AWS Direct Connect Konnektivität. Der Partner kann ein SLA mit Servicegutschriften anbieten, die auf seinem Produktangebot bis zum Abgrenzungspunkt mit basieren. AWS Die Option sollte direkt mit den APN-Partnern geprüft und weiter untersucht werden. AWSveröffentlicht eine Liste validierter Lieferpartner.

Logischer Entwurf: Neben dem Konnektivitätstyp müssen Sie bei Ihrem Gesamtentwurf auch andere Bausteine berücksichtigen. AWS Transit GatewayHat beispielsweise ein eigenes SLA, ebenso wie AWSS2S VPN. Möglicherweise verwenden Sie aus Sicherheitsgründen AWS Transit Gateway for Scale und AWS S2S VPN, aber Sie müssen beide so gestalten, dass sie den jeweiligen SLAs entsprechen, um für jeden Dienst Servicegutschriften erhalten zu können.

Lesen Sie die AWS Direct ConnectResilienz-Empfehlungen und das Resiliency Toolkit.

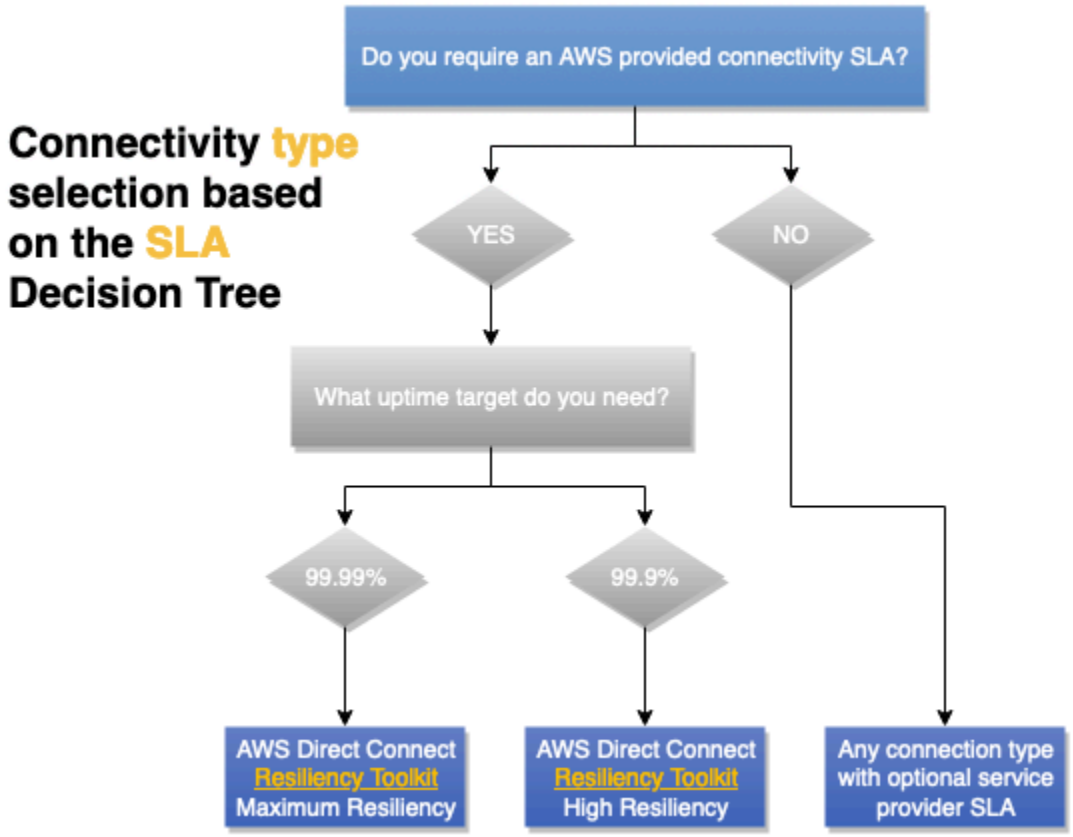

Abbildung 3 — Entscheidungsbaum für SLA-Überlegungen

Leistung

Definition

Es gibt mehrere Faktoren, die die Netzwerkleistung beeinflussen, wie Latenz, Paketverlust, Jitter und Bandbreite. Je nach Anwendungsanforderungen kann die Bedeutung der einzelnen Faktoren variieren.

Die wichtigsten Fragen

Auf der Grundlage Ihrer Anwendungsanforderungen müssen Sie die Netzwerkleistungsfaktoren identifizieren und priorisieren, die sich auf Ihr Anwendungsverhalten und Ihre Benutzererfahrung auswirken.

Bandbreite

Bandbreite bezieht sich auf die Datenübertragungsrate einer Verbindung und wird normalerweise in Bit pro Sekunde (bps) gemessen. Megabit pro Sekunde (Mbit/s) und Gigabit pro Sekunde (Gbit/s)

sind übliche Skalierungen und entsprechen der Basis 10 (1.000.000 Bit pro Sekunde = 1 Mbit/s) im Gegensatz zur Basis 2 (2^10), wie man sie an anderer Stelle findet.

Beachten Sie bei der Bewertung des Bandbreitenbedarfs von Anwendungen, dass sich die Bandbreitenanforderungen im Laufe der Zeit ändern können. Die anfängliche Bereitstellung in der Cloud, der normale Betrieb, neue Workloads und Failover-Szenarien können alle unterschiedliche Bandbreitenanforderungen haben.

Für Anwendungen können eigene Überlegungen zur Bandbreite gelten. Einige Anwendungen erfordern möglicherweise eine deterministische Leistung über eine Verbindung mit hoher Bandbreite, während andere sowohl eine deterministische Leistung als auch eine hohe Bandbreite erfordern können. Eine Anwendung benötigt möglicherweise eine spezielle Konfiguration, um mehrere Verkehrsflüsse (manchmal auch als Streams oder Sockets bezeichnet) parallel zu verwenden, wenn sie die Bandbreitenbeschränkungen pro Verkehrsfluss erreicht, sodass sie einen größeren Teil der Verbindungsbandbreite nutzen kann. VPNs können den Durchsatz aufgrund von Tunnelkosten, niedrigeren MTU-Grenzwerten oder Hardware-Bandbreitenbeschränkungen einschränken.

Latency

Die Latenz ist die Zeit, die ein Paket benötigt, um über eine Netzwerkverbindung von der Quelle zum Ziel zu gelangen. Sie wird normalerweise in Millisekunden (ms) gemessen, wobei niedrige Latenzanforderungen manchmal in Mikrosekunden (µs) ausgedrückt werden. Die Latenz ist eine Funktion der Lichtgeschwindigkeit, daher nimmt die Latenz mit der Entfernung zu.

Die Latenzanforderungen für Anwendungen können unterschiedliche Formen annehmen. Bei einer hochgradig interaktiven Anwendung, wie z. B. einem virtuellen Desktop, kann ein Latenzziel festgelegt werden, das vom Zeitpunkt der Benutzereingabe bis zum Zeitpunkt der Reaktion des virtuellen Desktops auf diese Eingabe gemessen wird. Voice over IP (VoIP) -Anwendungen können ähnliche Anforderungen haben. Eine zweite Art von Workloads, die in Betracht gezogen werden sollten, sind solche, die in hohem Maße transaktionaler Natur sind und eine Antwort vom Server benötigen, bevor sie fortgesetzt werden können. Datenbanken oder andere Arten von Schlüssel-/Wertespeichern können durch eine erhöhte Netzwerklatenz stark beeinträchtigt werden.

Jitter

Jitter misst, wie konsistent die Netzwerklatenz ist, und wird ebenso wie die Latenz normalerweise in Millisekunden (ms) gemessen.

Anwendungs-Jitter-Anforderungen finden sich in der Regel in Echtzeit-Streaming-Anwendungen, einschließlich Video- und Sprachübertragung. Bei diesen Anwendungen ist in der Regel ein

gleichbleibender Datenfluss mit gleichbleibender Geschwindigkeit und Verzögerung sowie kleine Puffer zur Korrektur geringer Jittermengen erforderlich.

Verlust von Paketen

Paketverlust ist das Maß dafür, wie viel Prozent des Netzwerkverkehrs nicht zugestellt werden. In allen Netzwerken kommt es manchmal zu einem gewissen Grad an Paketverlust, was auf hohe Datenverkehrsspitzen, Kapazitätsreduzierungen, Netzwerkausfälle und andere Gründe zurückzuführen ist. Daher müssen Anwendungen eine gewisse Toleranz gegenüber Paketverlusten aufweisen. Wie viel sie tolerieren können, kann jedoch von Anwendung zu Anwendung variieren.

Anwendungen, die TCP zur Übertragung ihres Datenverkehrs verwenden, können Paketverluste durch erneute Übertragung korrigieren. Anwendungen, die zusätzlich zu IP UDP oder ihre eigenen Protokolle verwenden, müssen ihre eigenen Methoden zur Behandlung von Paketverlusten implementieren und reagieren möglicherweise sehr empfindlich darauf. Eine Voice-over-IP-Anwendung kann den Teil des Anrufs, bei dem das Paket verloren gegangen ist, einfach zum Schweigen bringen, anstatt eine erneute Übertragung zu versuchen. Einige VPN-Lösungen verfügen über eigene Mechanismen zur Wiederherstellung nach einem Paketverlust in dem Netzwerk, das sie für die Übertragung des Datenverkehrs verwenden.

Zu berücksichtigende Fähigkeiten

Wenn vorhersehbare Latenz und Durchsatz erforderlich sind, AWS Direct Connect ist dies die empfohlene Wahl, da sie eine deterministische Leistung bietet. Die Bandbreite kann auf der Grundlage der Durchsatzanforderungen ausgewählt werden. AWSempfiehlt die VerwendungAWS Direct Connect, wenn Sie ein konsistenteres Netzwerkerlebnis benötigen, als es internetbasierte Verbindungen bieten können. Private VIFs und Transit-VIFs unterstützen Jumbo-Frames, wodurch die Anzahl der Pakete im Netzwerk reduziert und der Durchsatz aufgrund des geringeren Overheads verbessert werden kann. AWS Direct Connect SiteLinkermöglicht die Nutzung des AWS Backbones zur Bereitstellung von Konnektivität zwischen Ihren Standorten und kann bei Bedarf aktiviert werden. Die verwendete Bandbreite SiteLink sollte bei der Auswahl der Direct Connect-Bandbreite berücksichtigt werden.

Wenn Sie ein VPN-Over verwenden, wird die Verschlüsselung AWS Direct Connect hinzugefügt. Es reduziert jedoch die MTU-Größe, was den Durchsatz verringern könnte. AWSDie verwalteten Site-to-Site (S2S) VPN-Funktionen finden Sie in der Dokumentation. AWS Site-to-Site VPN Viele Standorte mit Direktverbindung unterstützen MACSec, wenn die Verschlüsselung über Ihre Verbindung die primäre Verschlüsselungsanforderung ist. MACSec hat nicht die gleiche MTU oder den potenziellen Durchsatz wie bei Site-to-Site-VPN-Verbindungen. AWS Transit Gatewayermöglicht es Kunden, die

Anzahl der VPN-Verbindungen horizontal zu skalieren und den Durchsatz mit Equal-Cost Multi-Path Routing (ECMP) entsprechend zu erhöhen. AWSDas verwaltete Site-to-Site VPN unterstützt die Verwendung von Direct Connect-Transit-VIFs für private Konnektivität. Weitere Informationen finden Sie unter Private IP VPN mit. AWS Direct Connect

Eine weitere Option ist die Verwendung eines AWS verwalteten Site-to-Site VPN über das Internet. Es kann aufgrund der geringen Kosten eine attraktive Option sein und ist weit verbreitet. Beachten Sie jedoch, dass die Leistung über das Internet am besten ist. Wetterereignisse, Staus und erhöhte Latenzzeiten im Internet können unvorhersehbar sein. AWSbietet eine Lösung mit AWSAccelerated S2S VPN, mit der einige der Nachteile der Nutzung eines Internetpfads gemildert werden können. Accelerated S2S VPN verwendet AWS Global Accelerator, wodurch VPN-Verkehr so früh und so nah wie möglich am Kunden-Gateway-Gerät in das AWS Netzwerk gelangen kann. Dies optimiert den Netzwerkpfad und nutzt das überlastungsfreie AWS globale Netzwerk, um den Datenverkehr an den Endpunkt zu leiten, der die beste Leistung bietet. Sie können beschleunigte VPN-Verbindungen verwenden, um Netzwerkunterbrechungen zu vermeiden, die auftreten können, wenn der Datenverkehr über das öffentliche Internet geleitet wird.

Kosten

Definition

In der Cloud beinhalten die Kosten für Hybridkonnektivität die Kosten für bereitgestellte Ressourcen und deren Nutzung. Die Kosten der bereitgestellten Ressourcen werden in Zeiteinheiten gemessen, normalerweise stündlich. Die Nutzung wird für die Datenübertragung und -verarbeitung in der Regel in Gigabyte (GB) angegeben. Zu den weiteren Kosten gehören die Kosten für die Konnektivität zum AWS Netzwerkpoint of Presence. Wenn sich Ihr Netzwerk in derselben Colocation-Einrichtung befindet, sind die Kosten möglicherweise so gering wie die Kosten für eine Cross-Connect-Verbindung. Wenn sich Ihr Netzwerk an einem anderen Standort befindet, fallen Kosten für einen Dienstanbieter oder einen APN Direct Connect-Partner an.

Die wichtigsten Fragen

- Wie viele Daten werden voraussichtlich AWS pro Monat aus Ihrer Einrichtung und aus dem Internet gesendet?
- Wie viele Daten werden voraussichtlich AWS pro Monat an Ihre Einrichtung und das Internet gesendet?
- Wie oft werden sich diese Beträge ändern?

- Was ändert sich in einem Ausfallszenario?

Zu berücksichtigende Fähigkeiten

Wenn Sie bandbreitenintensive Workloads haben, die Sie ausführen möchtenAWS, AWS Direct Connect können Sie Ihre Netzwerkkosten auf zweierlei Weise senken. AWS Erstens können Sie durch die AWS direkte Übertragung von Daten zu und von dort die Bandbreitenkosten senken, die Sie an Ihren Internetdienstanbieter zahlen. Zweitens werden alle Daten, die über Ihre dedizierte Verbindung übertragen werden, mit der reduzierten AWS Direct Connect Datenübertragungsrate und nicht mit den Internet-Datenübertragungsraten berechnet. Weitere Informationen finden Sie auf der Seite mit den Direct Connect-Preisen.

AWS Direct Connectermöglicht die Nutzung von AWS Direct Connect SiteLink , um Ihre Standorte über den AWS Backbone miteinander zu verbinden. Weitere Informationen finden Sie im SiteLink Launch-Blog. Wenn Sie diese Funktion nutzen, fallen normale Direct Connect-Datenübertragungskosten an, und es SiteLink ist eine Gebühr pro Stunde aktiviert. Sie können sie bei SiteLink Bedarf aktivieren und deaktivieren. Dies ist möglicherweise eine gute Option für Ausfallszenarien, die das Internet oder private Netzwerkkonnektivität betreffen.

Wenn Sie einen Netzwerkdienstanbieter für die Konnektivität zwischen einem lokalen Standort und einem Direct Connect-Standort verwenden, hängen Ihre Fähigkeit und der Zeitaufwand für die Änderung Ihrer Bandbreitenverpflichtungen von Ihrem Vertrag mit dem Dienstanbieter ab.

Der AWS Backbone kann Ihren Datenverkehr von jedem AWS Netzwerkpräsenzpunkt aus in alle Länder AWS-Region außer China weiterleiten. Diese Funktion bietet viele technische Vorteile gegenüber der Nutzung des Internets für den FernzugriffAWS-Regionen, ist jedoch mit Kosten verbunden. Weitere Informationen finden Sie auf der Preisseite für EC2 Data Transfer. Wenn AWS Transit Gatewayim Verkehrspfad eine vorhanden ist, fallen die Datenverarbeitungskosten pro GB an. Wenn Sie jedoch regionsübergreifendes Peering zwischen zwei Transit Gateways verwenden, wird Ihnen die Transit Gateway Gateway-Datenverarbeitung nur einmal in Rechnung gestellt.

Ein optimales Anwendungsdesign sorgt dafür, dass die Datenverarbeitung im Rahmen bleibt AWS und unnötige Gebühren für den Datenausgang minimiert werden. Der Datenzugriff auf ist kostenlos. AWS

> **Note**
>
> Als Teil der gesamten Konnektivitätslösung sollten Sie neben den AWS Verbindungskosten auch die Kosten für die end-to-end Konnektivität berücksichtigen, einschließlich der Kosten

für den Dienstanbieter, Querverbindungen, Racks und Ausrüstung am DX-Standort (falls erforderlich).

Wenn Sie sich nicht sicher sind, ob Sie das Internet oder eine private Verbindung nutzen sollten, berechnen Sie eine Gewinnschwelle, bei der AWS Direct Connect es günstiger ist als die Nutzung des Internets. Wenn das Datenvolumen bedeutet, dass dies günstiger AWS Direct Connect ist und Sie eine permanente Konnektivität benötigen, AWS Direct Connect ist dies die optimale Verbindungsoption.

Wenn die Konnektivität temporär ist und das Internet andere Anforderungen erfüllt, kann es aufgrund der Elastizität des Internets günstiger sein, AWS S2S-VPN über das Internet zu verwenden. Beachten Sie, dass Sie dafür über eine ausreichende Internetverbindung in Ihrem lokalen Netzwerk verfügen.

Wenn Sie sich in einer Einrichtung befinden, in der dies der AWS Direct Connect Fall ist (die Liste ist auf der Direct Connect-Website verfügbar), können Sie eine Cross-Connect-Verbindung zu AWS einrichten. Das bedeutet, dass Sie dedizierte Verbindungen mit 1,10 oder 100 Gbit/s verwenden müssen. AWS Direct ConnectPartner bieten mehr Bandbreitenoptionen und kleinere Kapazitäten, wodurch Ihre Verbindungskosten optimiert werden können. Sie können beispielsweise mit einer gehosteten Verbindung mit 50 Mbit/s beginnen und nicht mit einer dedizierten Verbindung mit 1 Gbit/s.

Mit AWS Transit Gateway können Sie Ihre VPN- und Direct Connect-Verbindungen mit vielen VPCs teilen. Ihnen werden zwar die Anzahl der Verbindungen, die Sie AWS Transit Gateway pro Stunde herstellen, und die Menge des durchfließenden Datenverkehrs in Rechnung gestelltAWS Transit Gateway, dies vereinfacht jedoch die Verwaltung und reduziert die Anzahl der erforderlichen VPN-Verbindungen und VIFs. Die Vorteile und Kosteneinsparungen eines geringeren Betriebsaufwands können die zusätzlichen Kosten der Datenverarbeitung leicht aufwiegen. Optional können Sie ein Design in Betracht ziehen, das AWS Transit Gateway sich im Datenverkehrspfad zu den meisten, aber nicht zu allen VPCs befindet. Dieser Ansatz vermeidet die AWS Transit Gateway Datenverarbeitungsgebühren für Anwendungsfälle, in AWS die Sie große Datenmengen übertragen müssen. Weitere Informationen zu diesem Design finden Sie im Abschnitt Konnektivitätsmodelle. Ein anderer Ansatz besteht darin, AWS Direct Connect als primären Pfad mit AWS S2S-VPN über das Internet als Backup-/Failover-Pfad zu kombinieren. Diese Lösung ist zwar technisch machbar und sehr kosteneffektiv, hat aber auch technische Nachteile (die im Abschnitt Zuverlässigkeit dieses Whitepapers behandelt werden) und kann schwieriger zu verwalten sein. AWSempfiehlt dies nicht für sehr kritische oder kritische Workloads.

Der letzte Ansatz ist ein vom Kunden verwaltetes VPN oder SD-WAN, das in Amazon EC2 EC2-Instances bereitgestellt wird. Dies kann im Vergleich zu S2S-VPN in großem Maßstab günstiger sein, wenn es Dutzende bis Hunderte von Standorten gibt. AWS Für jede virtuelle Appliance müssen jedoch Verwaltungsaufwand, Lizenzkosten und EC2-Ressourcenkosten berücksichtigt werden.

Entscheidungsmatrix

Tabelle 3 — Beispiele für Designeingaben von Corp. Automotive Connectivity

Kategorie	Vom Kunden verwaltetes VPN oder SD-WAN	AWSS2S-VPN	AWSBeschleunigtes S2S-VPN	AWS Direct ConnectGehostete Verbindung	AWS Direct ConnectDedizierte Verbindung
Erfordert eine Internetverbindung	Ja	Ja	Ja	Nein	Nein
Kosten für bereitgestellte Ressourcen	EC2-Instanz- und Softwarelizenzierung	AWSS2S-VPN	AWSS2S VPN und Global Accelerator AWS	Anwendbarer Kapazitätsanteil der Portkosten	Kosten für dedizierten Port
Kosten der Datenübertragung	Internet-Tarif	Internet-Tarif oder Direct Connect-Tarif	Internet mit Premium-Datenübertragung	Rate für direkte Connect	Rate für direkte Connect
Transit Gateway	Optional	Optional	Erforderlich	Optional	Optional
AWSKosten für die Datenverarbeitung	–	Nur mit AWS Transit Gateway	Ja	Nur mit AWS Transit Gateway	Nur mit AWS Transit Gateway
Kann übermäßig	Ja	Ja	Nein	–	–

Kategorie	Vom Kunden verwaltetes VPN oder SD-WAN	AWSS2S-VPN	AWSBeschleunigtes S2S-VPN	AWS Direct ConnectGehostete Verbindung	AWS Direct ConnectDedizierte Verbindung
verwendet werdenAWS Direct Connect?					

Auswahl des Konnektivitätsdesigns

In diesem Abschnitt des Whitepapers werden die Überlegungen behandelt, die sich auf die Auswahl Ihres Konnektivitätsdesigns auswirken. Das Konnektivitätsdesign umfasst die logischen Aspekte sowie die Gestaltung und Optimierung der Zuverlässigkeit Ihrer Hybrid-Konnektivität.

Die folgenden Überlegungen werden behandelt: Skalierbarkeit, Konnektivitätsmodelle, Zuverlässigkeit und vom Kunden verwaltetes VPN und SD-WAN.

Überlegungen

- Skalierbarkeit
- Konnektivitätsmodelle
- Zuverlässigkeit
- Vom Kunden verwaltetes VPN und SD-WAN

Skalierbarkeit

Definition

Skalierbarkeit bezieht sich auf die Fähigkeit Ihrer Konnektivitätslösung, mit der Zeit zu wachsen und sich weiterzuentwickeln, wenn sich Ihre Anforderungen ändern.

Bei der Entwicklung einer Lösung müssen Sie sowohl die aktuelle Größe als auch das erwartete Wachstum berücksichtigen. Dieses Wachstum kann organisches Wachstum sein oder auf eine schnelle Expansion zurückzuführen sein, z. B. bei Zusammenschlüssen und Übernahmen.

Hinweis: Je nach angestrebter Lösungsarchitektur müssen möglicherweise nicht alle oben genannten Elemente berücksichtigt werden. Sie können jedoch als grundlegende Elemente zur Identifizierung der Skalierbarkeitsanforderungen der meisten gängigen hybriden Netzwerklösungen dienen. Dieses Whitepaper konzentriert sich auf die Auswahl und das Design hybrider Konnektivität. Es wird empfohlen, auch den Umfang der Hybridkonnektivität in Bezug auf die VPC-Netzwerkarchitektur zu berücksichtigen. Weitere Informationen finden Sie im Whitepaper Aufbau einer skalierbaren und sicheren AWS Multi-VPC-Netzwerkinfrastruktur.

Die wichtigsten Fragen

- Wie hoch ist die aktuelle und erwartete Anzahl von VPCs, die Konnektivität zu einem oder mehreren lokalen Standorten benötigen?
- Werden VPCs in einer AWS-Region oder mehreren Regionen eingesetzt?
- Mit wie vielen lokalen Standorten muss eine Verbindung hergestellt werden? AWS
- Mit wie vielen Kunden-Gateway-Geräten (in der Regel Router oder Firewalls) müssen Sie pro Standort eine Verbindung herstellen? AWS
- Wie viele Routen werden voraussichtlich auf Amazon VPCs beworben und wie viele Routen werden voraussichtlich von der AWS Seite empfangen?
- Muss die Bandbreite im AWS Laufe der Zeit erhöht werden?

Zu berücksichtigende Fähigkeiten

Die Skalierbarkeit ist ein wichtiger Faktor beim Design hybrider Konnektivität. Bis zu diesem Punkt wird der nachfolgende Abschnitt die Skalierung als Teil des Entwurfs eines gezielten Konnektivitätsmodells berücksichtigen.

Im Folgenden werden bewährte Methoden zur Minimierung der Skalenkomplexität des Designs hybrider Netzwerkkonnektivität empfohlen:

- Die Routenzusammenfassung sollte verwendet werden, um die Anzahl der beworbenen und empfangenen Routen zu reduzieren. AWS Daher muss das IP-Adressierungsschema so konzipiert sein, dass die Routenzusammenfassung optimal genutzt wird. Die Verkehrstechnik ist eine wichtige allgemeine Überlegung. Weitere Informationen zur Verkehrstechnik finden Sie im Unterabschnitt Verkehrstechnik im Abschnitt Zuverlässigkeit.
- Minimiere die Anzahl der BGP-Peering-Sitzungen, indem du DXGW mit VGW oder AWS Transit Gateway, wo eine einzelne BGP-Sitzung Konnektivität zu mehreren VPCs bereitstellen kann, verwendest.

- Ziehen Sie Cloud-WAN in Betracht, wenn mehrere AWS-Regionen und lokale Standorte miteinander verbunden werden müssen.

Konnektivitätsmodelle

Definition

Das Konnektivitätsmodell bezieht sich auf das Kommunikationsmuster zwischen lokalen Netzwerken und den Cloud-Ressourcen in AWS. Sie können Cloud-Ressourcen innerhalb einer Amazon VPC in einer AWS-Region oder mehreren VPCs in mehreren Regionen sowie AWS Dienste mit einem öffentlichen Endpunkt in einer oder mehreren AWS-Regionen, wie Amazon S3 und DynamoDB, bereitstellen.

Die wichtigsten Fragen

- Ist eine VPC-übergreifende Kommunikation innerhalb einer Region und zwischen Regionen erforderlich?
- Besteht die Anforderung, direkt vor Ort auf AWS öffentliche Endgeräte zuzugreifen?
- Ist der Zugriff auf AWS Dienste mithilfe von VPC-Endpunkten vor Ort erforderlich?

Zu berücksichtigende Fähigkeiten

Im Folgenden sind einige der gängigsten Szenarien für Konnektivitätsmodelle aufgeführt. Jedes Konnektivitätsmodell deckt Anforderungen, Eigenschaften und Überlegungen ab.

Hinweis: Wie bereits erwähnt, konzentriert sich dieses Whitepaper auf die hybride Konnektivität zwischen lokalen Netzwerken und. AWS Weitere Informationen zum Design für die Verbindung von VPCs finden Sie im Whitepaper Aufbau einer skalierbaren und sicheren AWS Multi-VPC-Netzwerkinfrastruktur.

Modelle

- AWS Beschleunigtes Site-to-Site VPN —, Single AWS Transit GatewayAWS-Region
- AWS DX — DXGW mit VGW, einzelne Region
- AWS DX — DXGW mit VGW, Multi-Regions und Public Peering AWS
- AWS DX — DXGW mit AWS Transit Gateway, mehreren Regionen und öffentlichem Peering AWS
- AWS DX — DXGW mit AWS Transit Gateway, Multi-Regionen (mehr als 3)

AWS Beschleunigtes Site-to-Site VPN —, Single AWS Transit GatewayAWS-Region

Dieses Modell besteht aus:

- Einzeln AWS-Region.
- AWS Verwaltete Site-to-Site-VPN-Verbindung mit. AWS Transit Gateway
- Beschleunigtes VPN aktiviert.

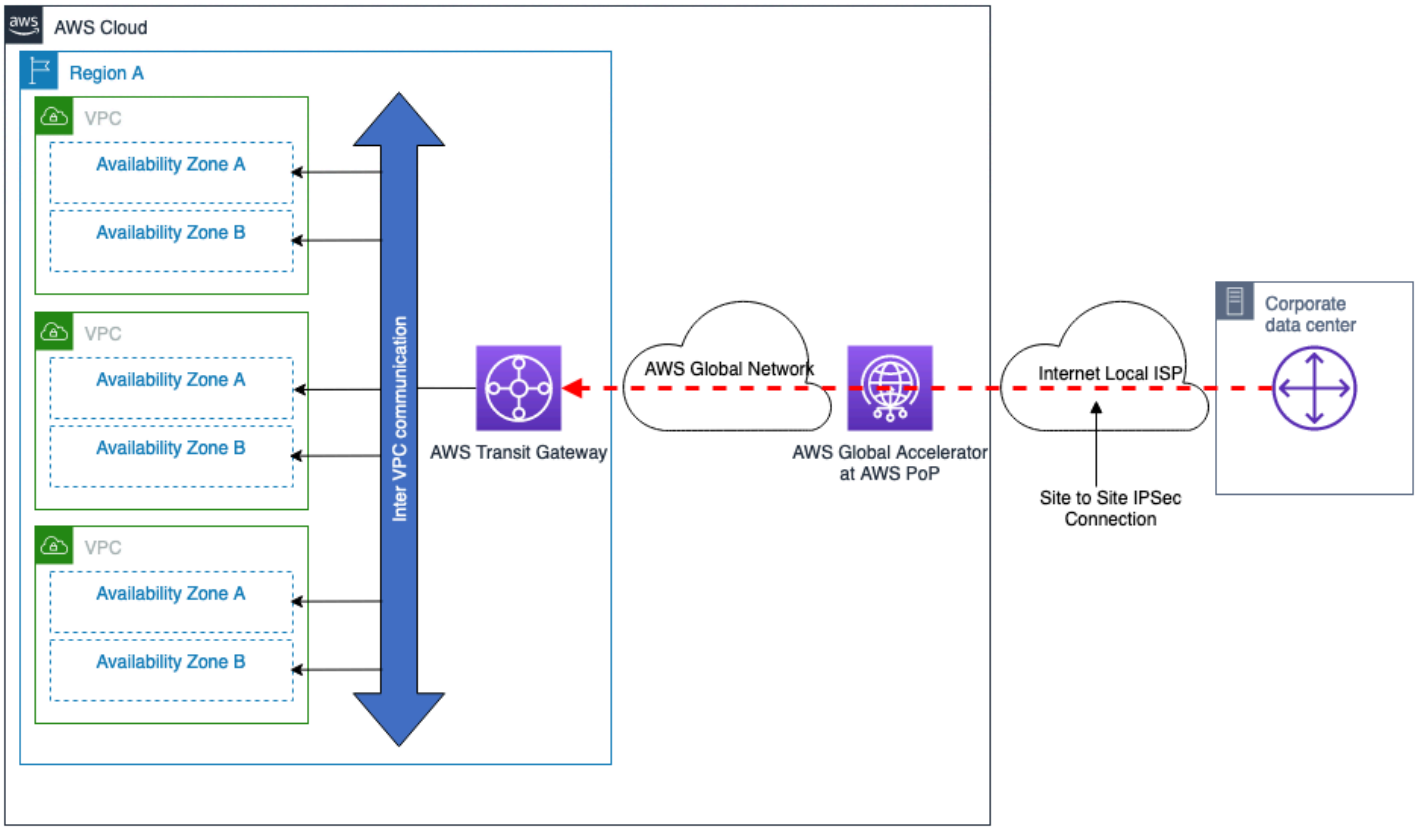

Abbildung 4 — AWS Verwaltetes VPN — AWS Transit Gateway, Single AWS-Region

Eigenschaften des Konnektivitätsmodells:

- Bieten Sie die Möglichkeit, optimierte VPN-Verbindungen über das öffentliche Internet herzustellen, indem Sie AWS beschleunigte Site-to-Site-VPN-Verbindungen verwenden.
- Bieten Sie die Möglichkeit, eine höhere VPN-Verbindungsbandbreite zu erreichen, indem Sie mehrere VPN-Tunnel mit ECMP konfigurieren.
- Kann für Verbindungen von mehreren entfernten Standorten aus verwendet werden.
- Bietet automatisiertes Failover mit dynamischem Routing (BGP).

- Wenn eine AWS Transit Gateway Verbindung zu VPCs besteht, können alle verbundenen VPCs dieselben VPN-Verbindungen verwenden. Sie können auch das gewünschte Kommunikationsmodell zwischen den VPCs steuern. Weitere Informationen finden Sie unter Funktionsweise von Transit-Gateways.
- Bietet flexible Designoptionen zur Integration von Sicherheits- und virtuellen SD-WAN-Appliances von Drittanbietern. AWS Transit Gateway Weitere Informationen finden Sie unter Zentralisierte Netzwerksicherheit für VPC-zu-VPC- und lokalen Datenverkehr zu VPC-Verbindungen.

Überlegungen zur Skalierung:

- Bis zu 50 Gbit/s Bandbreite mit mehreren IPSec-Tunneln und konfiguriertem ECMP (jeder Verkehrsfluss wird auf die maximale Bandbreite pro VPN-Tunnel begrenzt).
- Tausende von VPCs können pro verbunden werden. AWS Transit Gateway
- Weitere Skalierungsbeschränkungen, wie z. B. die Anzahl der Routen, finden Sie in den Site-to-Site-VPN-Kontingenten.

Weitere Überlegungen:

- Die zusätzlichen AWS Transit Gateway Verarbeitungskosten für die Datenübertragung zwischen dem lokalen Rechenzentrum und AWS.
- Auf Sicherheitsgruppen einer Remote-VPC kann nicht verwiesen werden AWS Transit Gateway — dies wird jedoch durch VPC-Peering unterstützt.

AWS DX — DXGW mit VGW, einzelne Region

Dieses Modell besteht aus:

- Einzeln AWS-Region.
- Doppelte AWS Direct Connect Verbindungen zu unabhängigen DX-Standorten.
- AWS DXGW ist über VGW direkt an die VPCs angeschlossen.
- Optionale Verwendung von AWS Transit Gateway für die Kommunikation zwischen VPC.

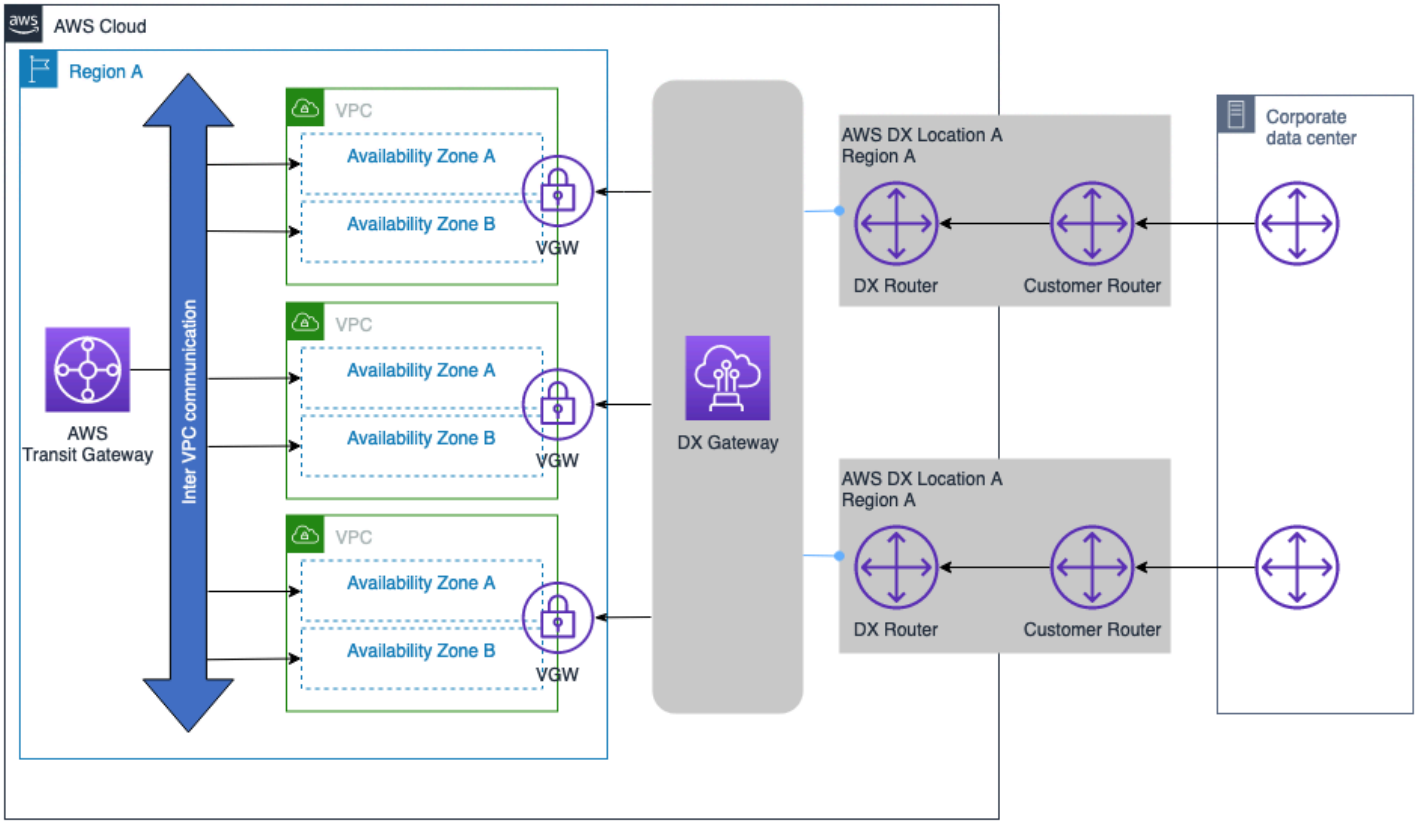

Abbildung 5 — AWS DX — DXGW mit VGW, Single AWS-Region

Eigenschaften des Konnektivitätsmodells:

- Bietet die Möglichkeit, in future eine Verbindung zu VPCs und DX-Verbindungen in anderen Regionen herzustellen.
- Bietet automatisiertes Failover mit dynamischem Routing (BGP).
- Mit können AWS Transit Gateway Sie das gewünschte Kommunikationsmodell zwischen den VPCs steuern. Weitere Informationen finden Sie unter Funktionsweise von Transit-Gateways.

Überlegungen zur Skalierung:

Weitere Informationen zu anderen Skalierungsbeschränkungen, wie z. B. der Anzahl unterstützter Präfixe und der Anzahl der VIFs pro DX-Verbindungstyp (dediziert, gehostet), finden Sie unter AWS Direct Connect Kontingente. Einige wichtige Überlegungen:

- Die BGP-Sitzung für eine private VIF kann jeweils bis zu 100 Routen für IPv4 und IPv6 ankündigen.

- Bis zu 20 VPCs können pro DXGW über eine einzige BGP-Sitzung verbunden werden. Wenn mehr als 20 VPCs benötigt werden, können zusätzliche DXGWs hinzugefügt werden, um die Konnektivität im großen Maßstab zu ermöglichen, oder erwägen Sie die Verwendung der Transit Gateway Gateway-Integration.
- Zusätzliche AWS Direct Connect s können nach Wunsch hinzugefügt werden.

Andere Überlegungen:

- Es fallen keine AWS Transit Gateway entsprechenden Verarbeitungskosten für die Datenübertragung zwischen AWS und lokalen Netzwerken an.
- Auf Sicherheitsgruppen einer Remote-VPC kann nicht verwiesen werden AWS Transit Gateway (VPC-Peering erforderlich).
- VPC-Peering kann verwendet werden, anstatt die Kommunikation zwischen den VPCs AWS Transit Gateway zu erleichtern. Dies erhöht jedoch die betriebliche Komplexität, da eine große Anzahl von point-to-point VPC-Peering in großem Maßstab erstellt und verwaltet werden muss.
- Wenn keine Kommunikation zwischen VPCs erforderlich ist, ist in diesem AWS Transit Gateway Konnektivitätsmodell weder VPC-Peering erforderlich.

AWS DX — DXGW mit VGW, Multi-Regions und Public Peering AWS

Dieses Modell besteht aus:

- Mehrere lokale Rechenzentren mit dualen Verbindungen zu AWS.
- Doppelte AWS Direct Connect Verbindungen zu unabhängigen DX-Standorten.
- AWS DXGW ist mit VGW direkt an mehr als 10 VPCs angeschlossen, mit VGW an bis zu 20 VPCs.
- Optionale Verwendung von AWS Transit Gateway für die Kommunikation zwischen VPC und Region.

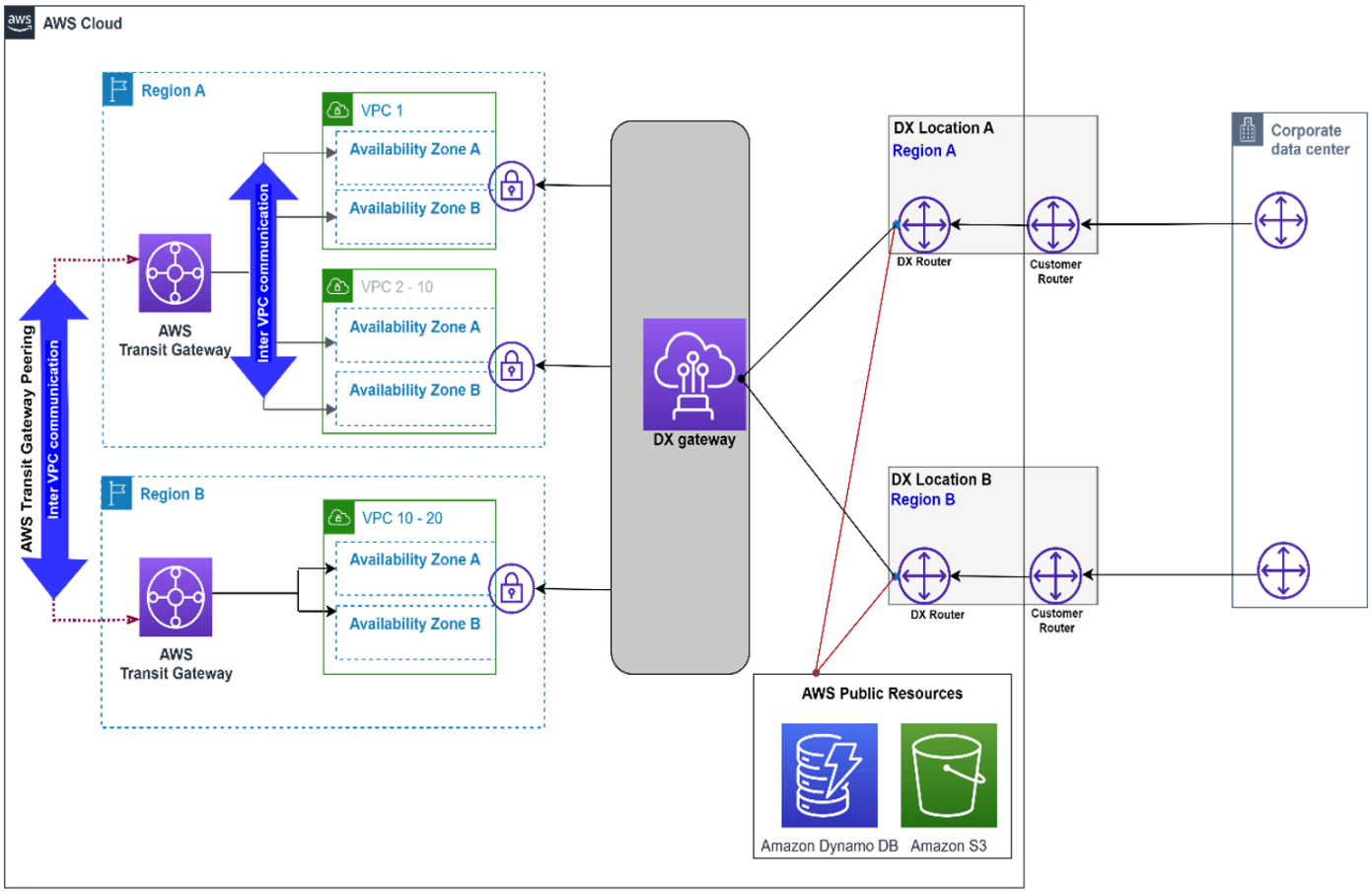

Abbildung 6 — AWS DX — DXGW mit VGW, mehreren Regionen und öffentlicher VIF

Eigenschaften des Konnektivitätsmodells:

- AWS DXGW ist über VGW direkt an mehr als 10 VPCs angeschlossen, bis zu 20 VPCs über VGW.
- AWS DX Public VIF wird verwendet, um direkt über die AWS DX-Verbindungen auf AWS öffentliche Dienste wie Amazon S3 zuzugreifen.
- Bieten Sie in future die Möglichkeit, Verbindungen zu VPCs und DX-Verbindungen in anderen Regionen herzustellen.
- VPC-übergreifende und regionsübergreifende VPC-Kommunikation, die durch AWS Transit Gateway Transit Gateway Gateway-Peering erleichtert wird.

Überlegungen zur Skalierung:

Weitere Informationen zu anderen Skalierungsbeschränkungen, wie z. B. der Anzahl unterstützter Präfixe und der Anzahl der VIFs pro DX-Verbindungstyp (dediziert, gehostet), finden Sie unter AWS Direct Connect Kontingente. Einige wichtige Überlegungen:

- Die BGP-Sitzung für eine private VIF kann jeweils bis zu 100 Routen für IPv4 und IPv6 ankündigen.
- Bis zu 20 VPCs können pro DXGW über eine einzige BGP-Sitzung auf jeder privaten VIF verbunden werden, bis zu 30 private VIFs pro DXGW.
- Zusätzliche s können nach Wunsch hinzugefügt werden. AWS Direct Connect

Andere Überlegungen:

- Es fallen keine AWS Transit Gateway entsprechenden Verarbeitungskosten für die Datenübertragung zwischen AWS und lokalen Netzwerken an.
- Sicherheitsgruppen einer Remote-VPC können nicht referenziert werden AWS Transit Gateway (VPC-Peering erforderlich).
- VPC-Peering kann verwendet werden, anstatt die Kommunikation zwischen den VPCs AWS Transit Gateway zu erleichtern. Dies erhöht jedoch die betriebliche Komplexität, da eine große Anzahl von point-to-point VPC-Peering in großem Maßstab erstellt und verwaltet werden muss.
- Wenn keine Kommunikation zwischen VPCs erforderlich ist, ist in diesem AWS Transit Gateway Konnektivitätsmodell weder VPC-Peering erforderlich.

AWS DX — DXGW mit AWS Transit Gateway, mehreren Regionen und öffentlichem Peering AWS

Dieses Modell besteht aus:

- Mehrfach AWS-Regionen.
- Doppelte AWS Direct Connect Verbindungen zu unabhängigen DX-Standorten.
- Ein einziges lokales Rechenzentrum mit dualen Verbindungen zu AWS.
- AWS DXGW mit. AWS Transit Gateway
- Hohe Anzahl von VPCs pro Region.

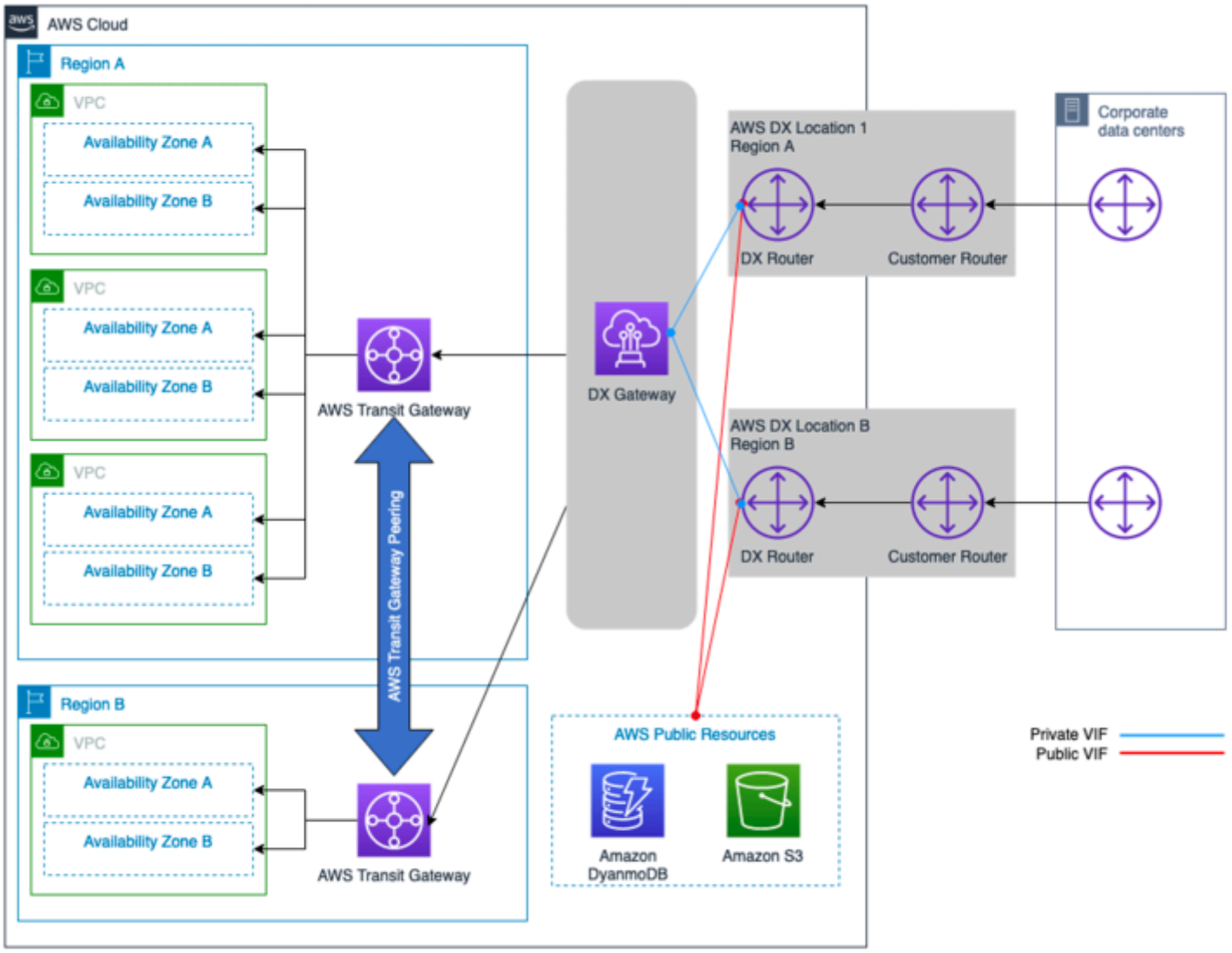

Abbildung 7 — AWS DX — DXGW mit AWS Transit Gateway, Multi-Regionen und öffentlicher VIF AWS

Eigenschaften des Konnektivitätsmodells:

- AWS DX Public VIF wird verwendet, um direkt über die AWS DX-Verbindungen auf AWS öffentliche Ressourcen wie S3 zuzugreifen.
- Bieten Sie in future die Möglichkeit, eine Verbindung zu VPCs und/oder DX-Verbindungen in anderen Regionen herzustellen.
- Bei einer AWS Transit Gateway Verbindung mit VPCs kann eine vollständige oder teilweise Mesh-Konnektivität zwischen den VPCs erreicht werden.

- VPC-übergreifende und regionsübergreifende VPC-Kommunikation, die durch Peering erleichtert wird. AWS Transit Gateway
- Bietet flexible Designoptionen zur Integration von Sicherheits- und virtuellen SD-WAN-Appliances von Drittanbietern. AWS Transit Gateway Siehe: Zentralisierte Netzwerksicherheit für VPC-zu-VPC- und lokalen Verkehr zu VPC-Verkehr.

Überlegungen zur Skalierung:

- Die Anzahl der Routen von und zu den Routen AWS Transit Gateway ist auf die maximal unterstützte Anzahl von Routen über eine Transit-VIF begrenzt (eingehende und ausgehende Nummern variieren). Weitere Informationen zu den Skalenbeschränkungen und der unterstützten Anzahl von Routen und VIFs finden Sie in den AWS Direct Connect Kontingenten.
- Skalieren Sie in einer einzigen BGP-Sitzung AWS Transit Gateway auf bis zu Tausende von VPCs.
- Einzelnes Transit-VIF pro DX. AWS
- Zusätzliche AWS DX-Verbindungen können nach Wunsch hinzugefügt werden.

Weitere Überlegungen:

- Es fallen zusätzliche AWS Transit Gateway Verarbeitungskosten für die Datenübertragung zwischen einem Standort AWS und einem Standort vor Ort an.
- Sicherheitsgruppen einer Remote-VPC können nicht referenziert werden AWS Transit Gateway (VPC-Peering erforderlich).
- VPC-Peering kann verwendet werden, anstatt die Kommunikation zwischen den VPCs AWS Transit Gateway zu erleichtern. Dies erhöht jedoch die betriebliche Komplexität, da eine große Anzahl von point-to-point VPC-Peering in großem Maßstab erstellt und verwaltet werden muss.
- Wenn mehr als drei AWS Transit Gateway s erforderlich sind, können zusätzliche DXGW hinzugefügt werden — siehe den folgenden Konnektivitätsmodus.

AWS DX — DXGW mit AWS Transit Gateway, Multi-Regionen (mehr als 3)

Dieses Modell besteht aus:

- AWS-Regionen Mehrfach (mehr als 3).
- Zwei lokale Rechenzentren.
- Duale AWS Direct Connect Verbindungen zu unabhängigen DX-Standorten pro Region.

- AWS DXGW mit. AWS Transit Gateway
- Hohe Anzahl von VPCs pro Region.
- Vollständiges Peering-Netzwerk zwischen s. AWS Transit Gateway

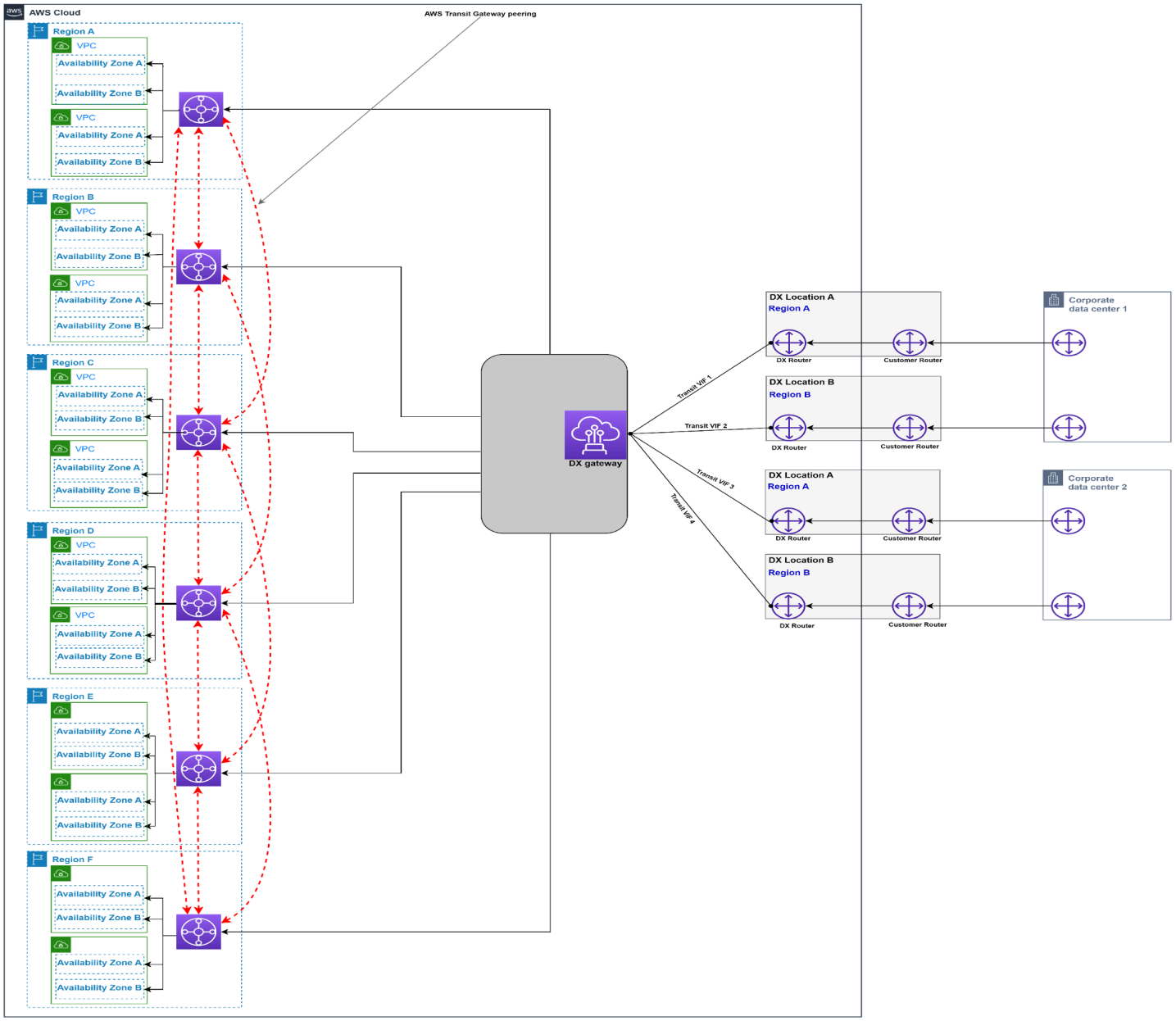

Abbildung 8 — AWS DX — DXGW mit mehreren Regionen (mehr als AWS Transit Gateway drei)

Eigenschaften des Konnektivitätsmodells:

- Niedrigster betrieblicher Overhead.

- AWS DX Public VIF wird verwendet, um direkt über die AWS DX-Verbindungen auf AWS öffentliche Ressourcen wie S3 zuzugreifen.
- Bieten Sie in future die Möglichkeit, Verbindungen zu VPCs und DX-Verbindungen in anderen Regionen herzustellen.
- Bei einer AWS Transit Gateway Verbindung mit VPCs kann eine vollständige oder teilweise Mesh-Konnektivität zwischen den VPCs erreicht werden.
- Die VPC-Kommunikation zwischen Regionen wird durch AWS Transit Gateway Peering erleichtert.
- Bietet flexible Designoptionen zur Integration von Sicherheits- und virtuellen SD-WAN-Appliances von Drittanbietern. AWS Transit Gateway Siehe: Zentralisierte Netzwerksicherheit für VPC-zu-VPC- und lokalen Verkehr zu VPC-Verkehr.

Überlegungen zur Skalierung:

- Die Anzahl der Routen von und zu den Routen AWS Transit Gateway ist auf die maximal unterstützte Anzahl von Routen über eine Transit-VIF begrenzt (eingehende und ausgehende Nummern variieren). Weitere Informationen zu den AWS Direct Connect Staffelbeschränkungen finden Sie in den Kontingenten. Ziehen Sie bei Bedarf eine Routenzusammenfassung in Betracht, um die Anzahl der Routen zu reduzieren.
- Skalieren Sie in einer einzigen BGP-Sitzung pro DXGW AWS Transit Gateway auf bis zu Tausende von VPCs (vorausgesetzt, die von den bereitgestellten DX-Verbindungen AWS bereitgestellte Leistung ist ausreichend).
- Pro DXGW können bis zu sechs AWS Transit Gateway s angeschlossen werden.
- Wenn mehr als drei Regionen miteinander verbunden werden müssen AWS Transit Gateway, sind zusätzliche DXGWs erforderlich.
- Einzelnes Transit-VIF pro DX. AWS
- Zusätzliche AWS DX-Verbindungen können nach Wunsch hinzugefügt werden.

Weitere Überlegungen:

- Es fallen zusätzliche AWS Transit Gateway Verarbeitungskosten für die Datenübertragung zwischen dem Standort vor Ort und an. AWS
- Sicherheitsgruppen einer Remote-VPC können nicht referenziert werden AWS Transit Gateway (VPC-Peering erforderlich).

- VPC-Peering kann verwendet werden, anstatt die Kommunikation zwischen den VPCs AWS Transit Gateway zu erleichtern. Dies erhöht jedoch die betriebliche Komplexität, da eine große Anzahl von point-to-point VPC-Peering in großem Maßstab erstellt und verwaltet werden muss.

Die folgende Entscheidungsstruktur behandelt die Überlegungen zur Skalierbarkeit und zum Kommunikationsmodell:

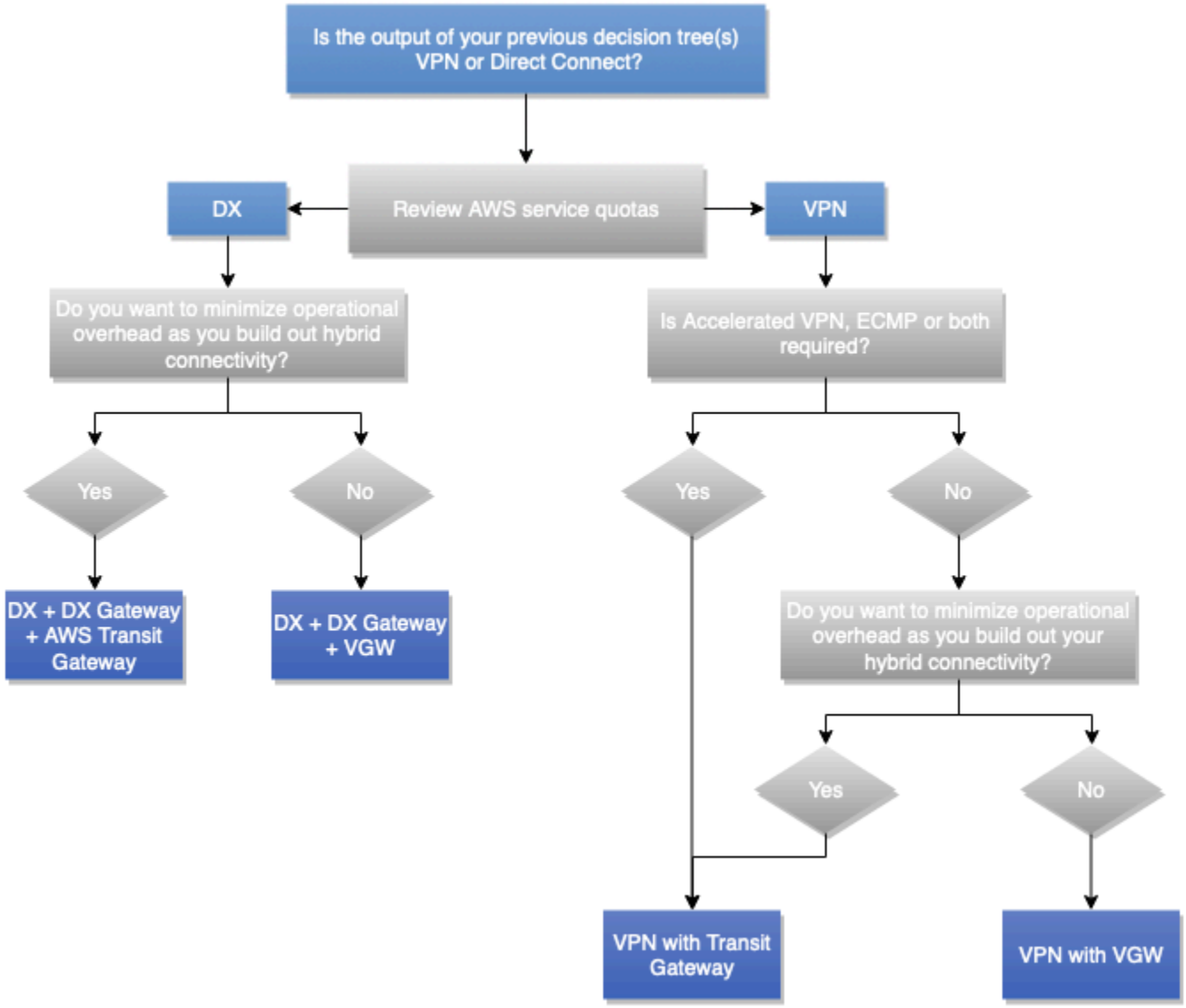

Abbildung 9 — Entscheidungsbaum für Skalierbarkeit und Kommunikationsmodell

> **Note**
>
> Wenn der gewählte Verbindungstyp VPN ist, sollte in der Regel aus Leistungsgründen entschieden werden, ob es sich bei dem VPN-Abschlusspunkt um eine AWS VGW- oder eine AWS Transit Gateway AWS S2S-VPN-Verbindung handelt. Falls noch nicht festgelegt, können Sie das erforderliche Kommunikationsmodell zwischen der VPC zusammen mit der Anzahl der erforderlichen VPC, die mit den VPN-Verbindungen verbunden werden müssen, berücksichtigen, um Ihnen bei der Entscheidung zu helfen.

Zuverlässigkeit

Definition

Zuverlässigkeit bezieht sich auf die Fähigkeit eines Dienstes oder Systems, bei Bedarf die erwartete Funktion zu erfüllen. Die Zuverlässigkeit eines Systems kann anhand seiner Betriebsqualität innerhalb eines bestimmten Zeitraums gemessen werden. Im Gegensatz dazu steht Resilienz, die sich auf die Fähigkeit eines Systems bezieht, sich dynamisch und zuverlässig nach Infrastruktur- oder Serviceunterbrechungen zu erholen.

Weitere Informationen darüber, wie Verfügbarkeit und Resilienz zur Messung der Zuverlässigkeit verwendet werden, finden Sie in der Zuverlässigkeitssäule des AWS Well-Architected Framework.

Die wichtigsten Fragen

Verfügbarkeit

Verfügbarkeit ist der Prozentsatz der Zeit, in der ein Workload zur Nutzung verfügbar ist. Zu den allgemeinen Zielen gehören 99% (3,65 Tage zulässige Ausfallzeit pro Jahr), 99,9% (8,77 Stunden) und 99,99% (52,6 Minuten), wobei die Zahl der neun in der Prozentzahl abgekürzt wird („zwei Neunen“ für 99%, „drei Neunen“ für 99,9% usw.). Die Verfügbarkeit der Netzwerklösung zwischen AWS und dem lokalen Rechenzentrum kann sich von der Verfügbarkeit der Gesamtlösung oder der Anwendung unterscheiden.

Zu den wichtigsten Fragen zur Verfügbarkeit einer Netzwerklösung gehören:

- Können meine AWS Ressourcen weiterarbeiten, wenn sie nicht mit meinen lokalen Ressourcen kommunizieren können? Umgekehrt?

- Sollte ich geplante Ausfallzeiten für geplante Wartungsarbeiten als in der Verfügbarkeitsmetrik eingeschlossen oder ausgeschlossen betrachten?
- Wie messe ich die Verfügbarkeit der Netzwerkschicht unabhängig vom allgemeinen Zustand der Anwendung?

Der Abschnitt Verfügbarkeit des Well-Architected Framework Reliability Pillar enthält Vorschläge und Formeln für die Verfügbarkeit von Berechnungen.

Ausfallsicherheit

Resilienz ist die Fähigkeit eines Workloads, sich nach Infrastruktur- oder Serviceunterbrechungen zu erholen, Rechenressourcen dynamisch zu erwerben, um den Bedarf zu decken, und Störungen wie Fehlkonfigurationen oder vorübergehende Netzwerkprobleme zu minimieren. Wenn eine redundante Netzwerkkomponente (Link, Netzwerkgeräte usw.) nicht ausreichend verfügbar ist, um die erwartete Funktion eigenständig bereitzustellen, ist sie wenig widerstandsfähig gegenüber Ausfällen. Die Folge ist eine schlechte und verschlechterte Benutzererfahrung.

Zu den wichtigsten Fragen zur Ausfallsicherheit einer Netzwerklösung gehören:

- Mit wie vielen gleichzeitigen, diskreten Ausfällen sollte ich rechnen?
- Wie kann ich einzelne Fehlerquellen sowohl bei den Konnektivitätslösungen als auch bei meinem internen Netzwerk reduzieren?
- Was ist meine Sicherheitslücke gegenüber Distributed-Denial-of-Service-Ereignissen (DDoS)?

Technische Lösung

Zunächst ist zu beachten, dass nicht jede hybride Netzwerkverbindungslösung ein hohes Maß an Zuverlässigkeit erfordert und dass ein steigendes Maß an Zuverlässigkeit mit einem entsprechenden Anstieg der Kosten verbunden ist. In einigen Szenarien sind für einen primären Standort möglicherweise zuverlässige (redundante und belastbare) Verbindungen erforderlich, da sich die Ausfallzeit stärker auf das Unternehmen auswirkt, wohingegen regionale Standorte aufgrund der geringeren Auswirkungen auf das Geschäft im Falle eines Ausfalls möglicherweise nicht dasselbe Maß an Zuverlässigkeit erfordern. Es wird empfohlen, sich an die AWS Direct Connect Resilienz-Empfehlungen zu halten, da darin die AWS bewährten Methoden zur Sicherstellung einer AWS Direct Connect hohen Ausfallsicherheit beim Design erläutert werden.

Um eine zuverlässige hybride Netzwerkverbindungslösung im Kontext der Ausfallsicherheit zu erreichen, müssen beim Entwurf die folgenden Aspekte berücksichtigt werden:

- Redundanz: Ziel ist es, jeden einzelnen Fehlerpunkt im hybriden Netzwerkverbindungspfad zu eliminieren, einschließlich, aber nicht beschränkt auf Netzwerkverbindungen, Edge-Netzwerkgeräte, Redundanz zwischen Availability Zones und DX-Standorten sowie Gerätestromquellen, Glasfaserpfade und Betriebssysteme. AWS-Regionen Für Zweck und Umfang dieses Whitepapers konzentriert sich Redundanz auf die Netzwerkverbindungen, Edge-Geräte (z. B. Gateway-Geräte von Kunden), den AWS DX-Standort und AWS-Regionen (für Architekturen mit mehreren Regionen).
- Zuverlässige Failover-Komponenten: In einigen Szenarien ist ein System möglicherweise funktionsfähig, erfüllt seine Funktionen jedoch nicht auf dem erforderlichen Niveau. Eine solche Situation tritt häufig bei einem einzelnen Ausfall auf, bei dem festgestellt wird, dass geplante redundante Komponenten nicht redundant betrieben wurden. Ihre Netzwerklast kann aufgrund der Auslastung nicht an einen anderen Ort geleitet werden, was zu einer unzureichenden Kapazität für die gesamte Lösung führt.
- Failover-Zeit: Die Failover-Zeit ist die Zeit, die eine sekundäre Komponente benötigt, um die Rolle der primären Komponente vollständig zu übernehmen. Die Failover-Zeit hängt von mehreren Faktoren ab: wie lange es dauert, bis der Fehler erkannt wird, wie lange es dauert, die sekundäre Konnektivität zu aktivieren, und wie lange es dauert, bis der Rest des Netzwerks über die Änderung informiert wird. Die Fehlererkennung kann mithilfe von Dead Peer Detection (DPD) für VPN-Verbindungen und Bidirectional Forwarding Detection (BFD) für Verbindungen verbessert werden. AWS Direct Connect Die Aktivierung der sekundären Konnektivität kann sehr kurz sein (wenn diese Verbindungen immer aktiv sind), es kann sich um ein kurzes Zeitfenster handeln (wenn eine vorkonfigurierte VPN-Verbindung aktiviert werden muss) oder länger (wenn physische Ressourcen verschoben oder neue Ressourcen konfiguriert werden müssen). Die Benachrichtigung des restlichen Netzwerks erfolgt in der Regel über Routing-Protokolle innerhalb des Kundennetzwerks, von denen jedes unterschiedliche Konvergenzzeiten und Konfigurationsoptionen hat — deren Konfiguration würde den Rahmen dieses Whitepapers sprengen.
- Verkehrstechnik: Die Verkehrstechnik im Kontext eines robusten hybriden Netzwerkkonnektivitätsdesigns zielt darauf ab, zu regeln, wie der Verkehr in normalen Szenarien und in Ausfallszenarien über mehrere verfügbare Verbindungen fließen sollte. Es wird empfohlen, das Konzept des Entwurfs für Ausfälle zu befolgen, bei dem Sie prüfen müssen, wie die Lösung in verschiedenen Ausfallszenarien funktioniert und ob sie für das Unternehmen akzeptabel ist oder nicht. In diesem Abschnitt werden einige der häufigsten Anwendungsfälle der Verkehrstechnik erörtert, mit denen die allgemeine Ausfallsicherheit der hybriden Netzwerkkonnektivitätslösung verbessert werden soll. Der AWS Direct Connect Abschnitt über Routing und BGP befasst sich mit verschiedenen verkehrstechnischen Optionen zur Beeinflussung des Verkehrsflusses (Gemeinden, BGP-lokale Präferenz, AS-Pfadlänge). Um eine effektive verkehrstechnische Lösung zu entwickeln,

müssen Sie ein gutes Verständnis dafür haben, wie die einzelnen AWS Netzwerkkomponenten das IP-Routing im Hinblick auf die Routenbewertung und -auswahl handhaben, sowie über die möglichen Mechanismen zur Beeinflussung der Routenauswahl verfügen. Die Einzelheiten dazu würden den Rahmen dieses Dokuments sprengen. Weitere Informationen finden Sie je nach Bedarf in der Transit Gateway Route Evaluation Order, Site-to-Site VPN Route Priority und Direct Connect Routing und BGP Dokumentation.

> **Note**
>
> In der VPC-Routentabelle können Sie auf eine Präfixliste verweisen, die zusätzliche Routenauswahlregeln enthält. Weitere Informationen zu diesem Anwendungsfall finden Sie unter Routenpriorität für Präfixlisten. AWS Transit Gateway Routentabellen unterstützen auch Präfixlisten, aber sobald sie angewendet sind, werden sie auf bestimmte Routeneinträge erweitert.

Beispiel für duale Site-to-Site-VPN-Verbindungen mit spezifischeren Routen

Dieses Szenario basiert auf einer kleinen lokalen Site, die AWS-Region über das Internet eine einzige redundante VPN-Verbindung mit herstellt. AWS Transit Gateway Das in Abbildung 10 dargestellte verkehrstechnische Design zeigt, dass Sie mit Hilfe der Verkehrstechnik die Pfadauswahl beeinflussen und so die Zuverlässigkeit der hybriden Konnektivitätslösung erhöhen können, indem Sie:

- Stabile Hybridkonnektivität: Redundante VPN-Verbindungen bieten jeweils dieselbe Leistungskapazität, unterstützen automatisches Failover mithilfe des Dynamic Routing Protocol (BGP) und beschleunigen die Erkennung von Verbindungsausfällen mithilfe der VPN-Dead-Peer-Erkennung.
- Leistungseffizienz: Die Konfiguration von ECMP für beide VPN-Verbindungen AWS Transit Gateway trägt zur Maximierung der gesamten Bandbreite der VPN-Verbindung bei. Alternativ kann die Auslastung unabhängig von den beiden VPN-Verbindungen gesteuert werden, indem verschiedene, spezifischere Routen zusammen mit der Site Summary Route angekündigt werden

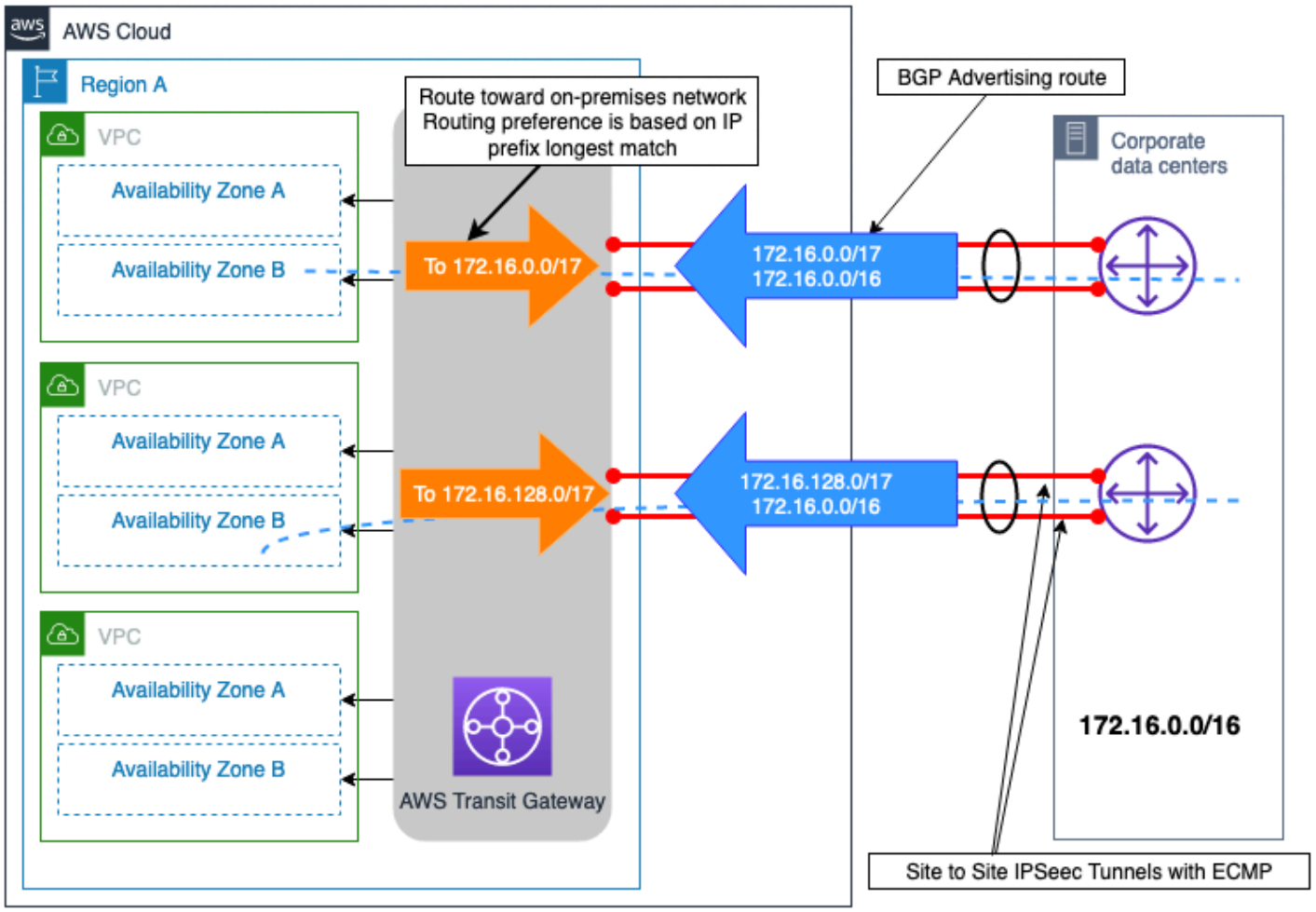

Abbildung 10 — Beispiel für duale Site-to-Site-VPN-Verbindungen mit spezifischeren Routen

Beispiel für zwei lokale Standorte mit mehreren DX-Verbindungen

Das in Abbildung 11 dargestellte Szenario zeigt zwei lokale Rechenzentrumsstandorte, die sich in verschiedenen geografischen Regionen befinden und AWS über das Konnektivitätsmodell mit maximaler Resilienz (beschrieben in den Resilienzempfehlungen) mithilfe AWS Direct Connect von DXGW und AWS Direct Connect VGW miteinander verbunden sind. Diese beiden lokalen Standorte sind über eine DCI-Verbindung (Data Center Interconnect) miteinander verbunden. Die lokalen IP-Präfixe (192.168.0.0/16), die zu Remote-Zweigstellen gehören, werden von beiden lokalen Rechenzentrumsstandorten aus angekündigt. Der primäre Pfad für dieses Präfix sollte Rechenzentrum 1 sein. Bei einem Ausfall von Rechenzentrum 1 oder beiden DX-Standorten erfolgt ein Failover für den Datenverkehr zu und von den Remote-Zweigstellen auf Rechenzentrum 2. Außerdem gibt es für jedes Rechenzentrum ein standortspezifisches IP-Präfix. Diese Präfixe müssen

direkt und über den anderen Rechenzentrumsstandort erreicht werden, falls beide DX-Standorte ausfallen.

Indem Sie BGP Community-Attribute mit den bei AWS DXGW beworbenen Routen verknüpfen, können Sie die Auswahl des Ausgangspfads von DXGW-Seite aus beeinflussen. AWS Diese Community-Attribute steuern das BGP Local Preference-Attribut AWS, das der angekündigten Route zugewiesen ist. Weitere Informationen finden Sie unter AWS DX Routing-Richtlinien und BGP-Communities.

Um die Zuverlässigkeit der Konnektivität auf dieser AWS-Region Ebene zu maximieren, konfiguriert jedes Paar von AWS DX-Verbindungen ECMP so, dass beide gleichzeitig für die Datenübertragung zwischen den einzelnen Standorten vor Ort und verwendet werden können. AWS

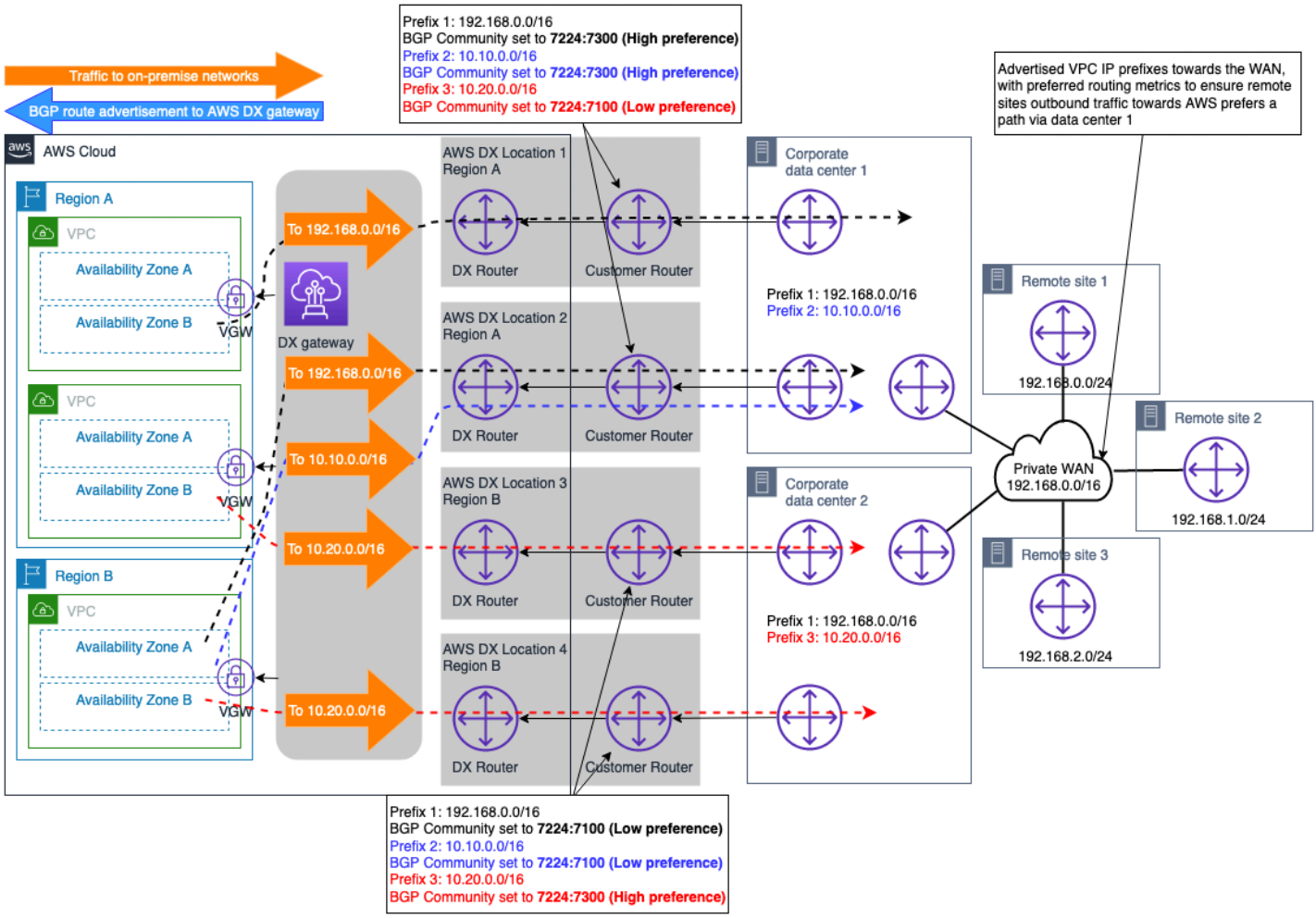

Abbildung 11 — Beispiel für duale lokale Standorte mit mehreren DX-Verbindungen

Bei diesem Design werden die Datenflüsse, die für die lokalen Netzwerke bestimmt sind (mit derselben angegebenen Präfixlänge und BGP-Community), mithilfe von ECMP auf die dualen DX-Verbindungen pro Standort verteilt. Wenn ECMP jedoch nicht für die gesamte DX-Verbindung erforderlich ist, kann dasselbe Konzept, das zuvor besprochen und in der Dokumentation zu Routing-Richtlinien und BGP-Communities beschrieben wurde, verwendet werden, um die Pfadauswahl auf DX-Verbindungsebene weiter zu gestalten.

Hinweis: Wenn sich im Pfad innerhalb der lokalen Rechenzentren Sicherheitsgeräte befinden, müssen diese Geräte so konfiguriert werden, dass Datenströme, die über einen DX-Link gehen und von einem anderen DX-Link (beide Verbindungen werden mit ECMP genutzt) innerhalb desselben Rechenzentrumsstandorts kommen, zulassen.

Beispiel für eine VPN-Verbindung als Backup zur AWS DX-Verbindung

VPN kann ausgewählt werden, um eine Backup-Netzwerkverbindung zu einer AWS Direct Connect Verbindung bereitzustellen. In der Regel wird diese Art von Konnektivitätsmodell von den Kosten bestimmt, da es aufgrund der undeterministischen Leistung über das Internet ein geringeres Maß an Zuverlässigkeit für die gesamte hybride Konnektivitätslösung bietet und es kein SLA gibt, das für eine Verbindung über das öffentliche Internet abgeschlossen werden kann. Es ist ein gültiges und kostengünstiges Konnektivitätsmodell und sollte verwendet werden, wenn die Kosten oberste Priorität haben und ein begrenztes Budget zur Verfügung steht, oder möglicherweise als Zwischenlösung, bis ein sekundärer DX bereitgestellt werden kann. Abbildung 12 zeigt den Entwurf dieses Konnektivitätsmodells. Eine wichtige Überlegung bei diesem Design, bei dem sowohl die VPN- als auch die DX-Verbindungen am enden AWS Transit Gateway, besteht darin, dass die VPN-Verbindung eine höhere Anzahl von Routen ankündigen kann als die, die über eine DX-Verbindung angekündigt werden können, mit der verbunden ist. AWS Transit Gateway Dies kann zu einer suboptimalen Routingsituation führen. Eine Option zur Lösung dieses Problems besteht darin, die Routenfilterung auf dem Kunden-Gateway-Gerät (CGW) für die über die VPN-Verbindung empfangenen Routen zu konfigurieren, sodass nur die Übersichtsrouten akzeptiert werden.

Hinweis: Um die Übersichtsroute auf dem zu erstellen AWS Transit Gateway, müssen Sie in der Routentabelle eine statische Route zu einem beliebigen Anhang angeben, sodass die Zusammenfassung über die spezifischere Route gesendet wird. AWS Transit Gateway

Aus Sicht der AWS Transit Gateway Routingtabelle werden die Routen für das lokale Präfix sowohl von der AWS DX-Verbindung (über DXGW) als auch von VPN mit derselben Präfixlänge empfangen. Gemäß der Route-Prioritätslogik von AWS Transit Gateway haben über Direct Connect empfangene Routen eine höhere Priorität als Routen, die über Site-to-Site VPN empfangen werden. Daher AWS Direct Connect wird der Pfad über den bevorzugt, um die lokalen Netzwerke zu erreichen.

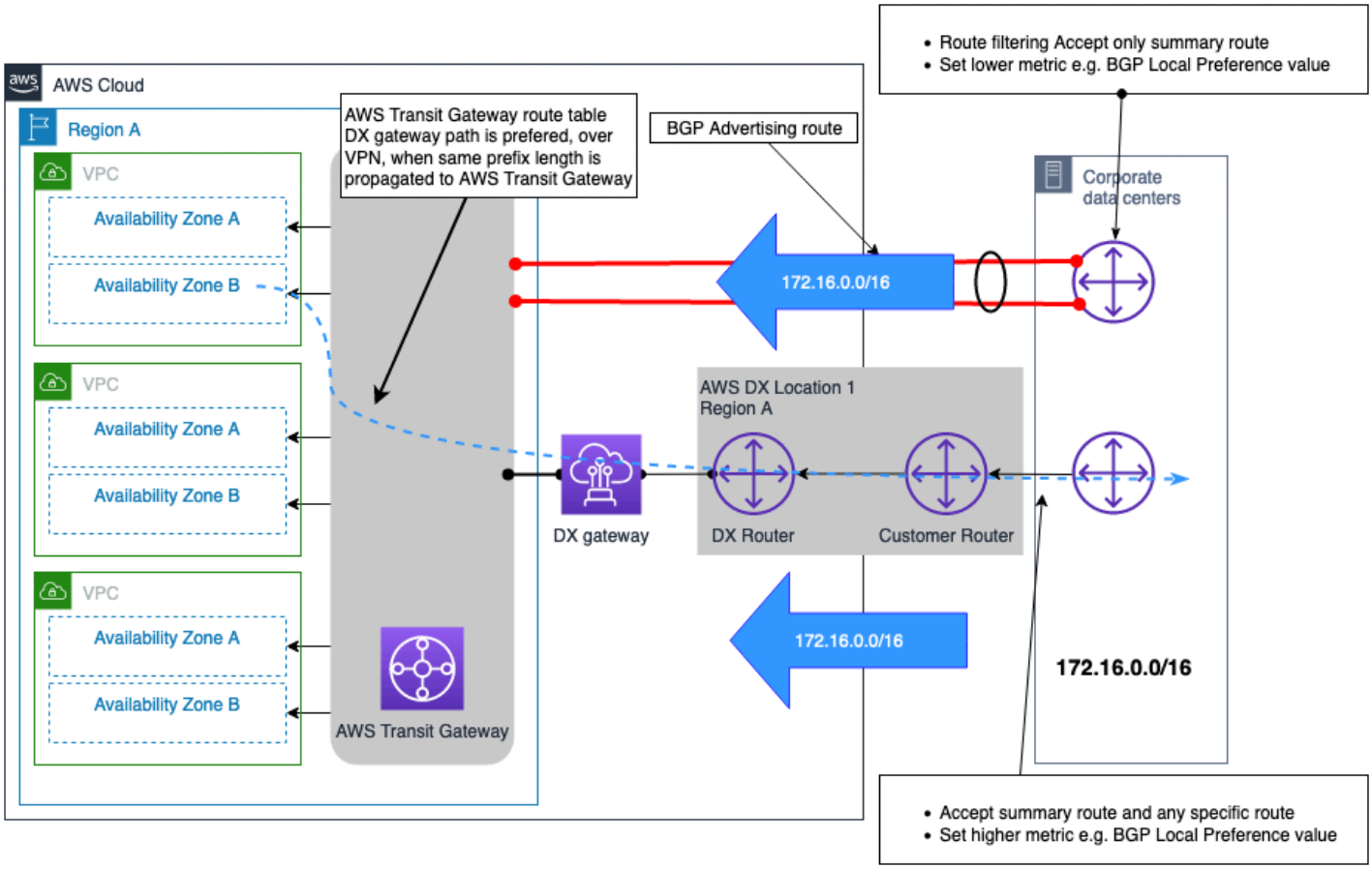

Abbildung 12 — Beispiel für eine VPN-Verbindung als Backup zur AWS DX-Verbindung

Die folgende Entscheidungsstruktur hilft Ihnen dabei, die gewünschte Entscheidung zu treffen, um eine stabile Hybrid-Netzwerkkonnektivität zu erreichen (was zu einer zuverlässigen) Hybrid-Netzwerkkonnektivität führt. Weitere Informationen finden Sie im AWS Direct Connect Resiliency Toolkit.

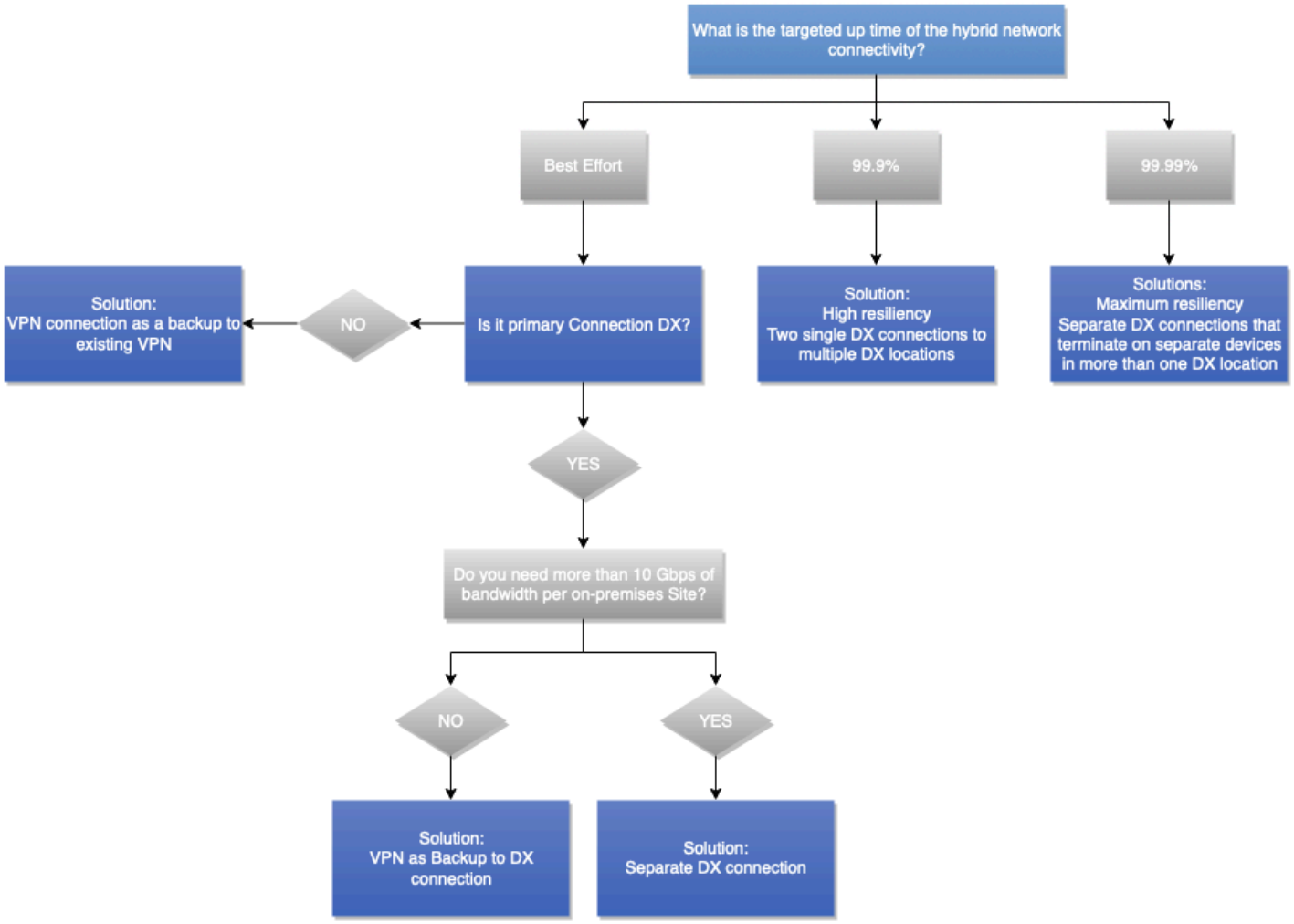

Abbildung 13 — Entscheidungsbaum zur Zuverlässigkeit

Vom Kunden verwaltetes VPN und SD-WAN

Definition

Konnektivität zum Internet ist eine Selbstverständlichkeit, und die verfügbare Bandbreite nimmt von Jahr zu Jahr zu. Einige Kunden entscheiden sich dafür, ein virtuelles WAN auf dem Internet aufzubauen, anstatt ein privates WAN aufzubauen und zu betreiben. Ein softwaredefiniertes Wide Area Network (SD-WAN) ermöglicht es Unternehmen, dieses virtuelle WAN durch geschickten Einsatz von Software schnell bereitzustellen und zentral zu verwalten. Andere Kunden entscheiden sich für herkömmliche, selbst verwaltete Site-to-Site-VPNs.

Auswirkungen auf Designentscheidungen

SD-WAN und vom Kunden verwaltete VPNs können über das Internet oder ausgeführt werden. AWS Direct Connect SD-WAN (oder ein beliebiges Software-VPN-Overlay) ist genauso zuverlässig wie der zugrunde liegende Netzwerktransport. Daher gelten die zuvor in diesem Whitepaper erörterten Überlegungen zu Zuverlässigkeit und SLA auch hier. Beispielsweise bietet der Aufbau eines SD-WAN-Overlays über das Internet nicht die gleiche Zuverlässigkeit wie der Aufbau über einem. AWS Direct Connect

Definition der Anforderung

- Verwenden Sie SD-WAN in Ihrem lokalen Netzwerk?
- Benötigen Sie bestimmte Funktionen, die nur auf bestimmten virtuellen Appliances verfügbar sind, die für die VPN-Terminierung verwendet werden?

Technische Lösungen

AWS empfiehlt die Integration von SD-WAN in und veröffentlicht eine Liste der Anbieter AWS Transit Gateway, die die Integration unterstützen AWS Transit Gateway. AWS kann als Hub für SD-WAN-Sites oder als Spoke-Site fungieren. Der AWS Backbone kann verwendet werden, um verschiedene SD-WAN-Hubs zu verbinden, die in einem äußerst zuverlässigen und leistungsstarken AWS Netzwerk eingesetzt werden. SD-WAN-Lösungen unterstützen automatisiertes Failover über jeden verfügbaren Pfad sowie zusätzliche Überwachungs- und Beobachtungsfunktionen in einem einzigen Verwaltungsbereich. Der umfangreiche Einsatz von auto Konfiguration und Automatisierung ermöglicht eine schnelle Bereitstellung und Transparenz im Vergleich zu herkömmlichen WANs. Der Einsatz von Tunneling- und Verschlüsselungskosten ist jedoch nicht vergleichbar mit dedizierten Hochgeschwindigkeits-Glasfaserverbindungen, die für private Konnektivität verwendet werden.

In einigen Fällen können Sie sich für eine virtuelle Appliance mit VPN-Funktion entscheiden. Zu den Gründen für die Wahl einer selbstverwalteten virtuellen Appliance gehören technische Funktionen und die Kompatibilität mit dem Rest Ihres Netzwerks. Wenn Sie sich für ein selbstverwaltetes VPN oder eine SD-WAN-Lösung entscheiden, die eine virtuelle Appliance verwendet, die in einer EC2-Instanz bereitgestellt wird, sind Sie für die Verwaltung dieser Appliance verantwortlich. Sie sind auch für die Hochverfügbarkeit und den Failover zwischen virtuellen Appliances verantwortlich. Ein solches Design erhöht Ihre betriebliche Verantwortung, könnte Ihnen jedoch mehr Flexibilität bieten. Die Funktionen und Fähigkeiten der Lösung hängen von der ausgewählten virtuellen Appliance ab.

AWS Marketplace enthält viele virtuelle VPN-Appliances, die Kunden auf Amazon EC2 einsetzen können. AWS empfiehlt, mit AWS verwaltetem S2S-VPN zu beginnen und nach anderen Optionen zu suchen, falls es Ihren Anforderungen nicht entspricht. Der Verwaltungsaufwand virtueller Appliances liegt in der Verantwortung des Kunden.

Beispiel für einen Anwendungsfall von Corp. Automotive

In diesem Abschnitt des Whitepapers wird gezeigt, wie die Überlegungen, Fragen zur Anforderungsdefinition und Entscheidungsbäume Ihnen bei der Entscheidung für das optimale Hybridnetzwerkdesign helfen. Das Identifizieren und Erfassen von Anforderungen ist wichtig, da sie als Grundlage für die Entscheidungsbäume verwendet werden. Durch die Erfassung von Anforderungen im Voraus werden weitere Entwurfsiterationen vermieden. Ein Projekt ganz zu unterbrechen, wenn der Entwurf überarbeitet werden muss und wertvolle Ressourcen zurückgehalten werden müssen, kann minimiert und idealerweise vermieden werden, wenn die Anforderungen im Voraus verstanden werden.

Das Beispiel Corp. Automotive wird in diesem Abschnitt zur Veranschaulichung des Kunden verwendet. Sie möchten zunächst ihr erstes Analyseprojekt am durchführen. AWS Das Analyseprojekt konzentriert sich auf die Analyse von Daten von vom Unternehmen hergestellten Autos und anderen Datensätzen, die bereits in den Rechenzentren des Unternehmens vorhanden sind. Zunächst ging die Architekturgruppe des Unternehmens davon ausAWS-Konto, dass sie eine Amazon-VPC und einige Subnetze benötigen, um Produktions- und Entwicklungsumgebungen zu hosten. Das Projektteam möchte unbedingt loslegen und hat so schnell wie möglich um Zugriff auf die Entwicklungsumgebung gebeten. Sie wollen in drei Monaten in Produktion gehen.

Beispiel Corp. Automotive plant außerdem, es in den AWS nächsten 6 Monaten AWS für mehrere zusätzliche Projekte zu nutzen, wie z. B. die Migration seiner ERP-Systeme, der virtuellen Desktop-Infrastruktur (VDI) und weiterer 20 Anwendungen von lokalen auf weitere Anwendungen. Einige Anforderungen für weitere Projekte werden noch definiert, aber es ist klar, dass ihre AWS Cloud Nutzung zunehmen wird.

Das Architekturteam entschied sich dafür, den in diesem Whitepaper beschriebenen Ansatz zu nutzen. Sie nutzten die im Rahmen der einzelnen Überlegungen dargelegten Fragen zur Anforderungsdefinition, um die Inputs für ihre Entwurfsentscheidungen zu erfassen.

Sie beginnen mit den Anforderungen an den Konnektivitätstyp, die in der folgenden Tabelle zusammengefasst sind.

Tabelle 4 — Beispiel für Angaben zur Zuverlässigkeit von Automotive Corp.

Überlegungen zur Auswahl des Konnektivitätstyps	Fragen zur Definition von Anforderungen	Antworten
Zeit für die Bereitstellung	Was ist der erforderliche Zeitplan für die Bereitstellung? Stunden, Tage, Wochen oder Monate?	• Entwicklung/Test: 1 Monat • Produktion: 3 Monate
Sicherheit	Erlauben Ihre Sicherheitsanforderungen und -richtlinien die Verwendung verschlüsselter Verbindungen über das Internet, um eine Verbindung zu privaten Netzwerkverbindungen herzustellen, AWS oder schreiben Sie die Verwendung von privaten Netzwerkverbindungen vor?	• Entwicklung/Test: Site-to-Site VPN akzeptabel • Produktion: Privates Netzwerk erforderlich
	Muss die Netzwerkschicht bei der Nutzung privater Netzwerkverbindungen für Verschlüsselung bei der Übertragung sorgen?	Nein, die Verschlüsselung auf Anwendungsebene wird verwendet.
SLA	Ist ein SLA für Hybridkonnektivität mit Servicegutschriften erforderlich?	• Entwicklung/Test: Nein • Produktion: Ja
	Was ist das Verfügbarkeitsziel?	• Entwicklung/Test: N/A • Produktion: 99,99%
	Hält das gesamte Hybrid-Netzwerk das Verfügbarkeitsziel ein?	• Entwicklung/Test: N/A • Produktion: Ja
Leistung	Was ist der erforderliche Durchsatz?	• Entwicklung/Test: 100 Mbit/s

Überlegungen zur Auswahl des Konnektivitätstyps	Fragen zur Definition von Anforderungen	Antworten
		• Produktion: 500 Mbit/s, die auf 2 Gbit/s anwachsen
	Was ist die maximal akzeptable Latenz zwischen einem lokalen Netzwerk AWS und einem Netzwerk?	• Entwicklung/Test: Keine strengen Anforderungen • Produktion: Weniger als 30 ms
	Was ist der maximal zulässige Netzwerk-Jitter?	• Entwicklung/Test: Keine besonderen Anforderungen • Produktion: Minimaler Jitter erforderlich
Kosten	An wie viele Daten würden Sie AWS pro Monat senden?	• Entwicklung/Test: 2 TB • Produktion: 20 TB, Wachstum auf 50 TB
	Ab wie vielen Daten würden Sie AWS pro Monat versenden?	• Entwicklung/Test: 1 TB • Produktion: 10 TB, Wachstum auf 25 TB
	Ist diese Konnektivität dauerhaft?	Ja

Auf der Grundlage der eingegangenen Anforderungen folgte das Architekturteam dem Entscheidungsbaum für den Konnektivitätstyp aus Abbildung 9. Auf diese Weise konnte das Architekturteam den Konnektivitätstyp für die Entwicklungs-, Test- und Produktionsumgebungen festlegen. Für die Produktionsumgebung berücksichtigten sie sowohl die unmittelbaren als auch die bevorstehenden Anforderungen. Für Entwicklungs- und Testzwecke wird Example Corp. Automotive ein site-to-site VPN über das Internet einrichten. Für die Produktion werden sie mit einem Dienstleister zusammenarbeiten, mit dem sie ihr Unternehmensnetzwerk verbinden können. AWS Direct Connect Example Corp. Automotive erwog zunächst die Verwendung einer gehosteten Direct

Connect-Verbindung, entschied sich jedoch aufgrund der Anforderungen an ein AWSbereitgestelltes SLA für Direct Connect Dedicated Connections.

Nach der Entscheidung für den Konnektivitätstyp besteht der nächste Schritt darin, die Anforderungen zu erfassen, die sich auf die Auswahl des Konnektivitätsdesigns auswirken. Dies hängt mit dem logischen Design zusammen, z. B. mit der Art und Weise, wie die Verbindungen konfiguriert werden und welche AWS Dienste zur Erfüllung der geschäftlichen und technischen Anforderungen verwendet werden sollen.

Um die Anforderungen an Skalierbarkeit und Kommunikationsmodell zu erfassen, verwendete das Architekturteam die Fragen zur Anforderungsdefinition aus den entsprechenden Abschnitten dieses Whitepapers. Die Anforderungen im Zusammenhang mit diesen beiden Überlegungen sind in der folgenden Tabelle zusammengefasst.

Tabelle 5 — Fragen zur Definition von Anforderungen

Überlegungen zur Auswahl des Konnektivitätsdesigns	Fragen zur Anforderungsdefinition	Antworten
Skalierbarkeit	Wie hoch ist die aktuelle oder erwartete Anzahl von VPCs, die Konnektivität zu lokalen Standorten benötigen?	anfänglich 2, innerhalb von 6 Monaten auf 30 angewachsen
	Werden diese VPCs in einer AWS-Region oder mehreren Regionen eingesetzt?	Einzelne Region
	Mit wie vielen lokalen Standorten muss eine Verbindung hergestellt werden? AWS	2 Rechenzentren
	Mit wie vielen Kunden-Gateway-Geräten pro Standort müssen Sie eine Verbindung herstellenAWS?	2 Router pro Rechenzentrum

Überlegungen zur Auswahl des Konnektivitätsdesigns	Fragen zur Anforderungsdefinition	Antworten
	Wie viele Routen werden voraussichtlich an AWS VPCs angekündigt, und wie viele Routen werden voraussichtlich von der Seite empfangen? AWS	• Routen, für die Werbung gemacht werden soll: 20 Routen AWS • Routen, von denen aus empfangen werden soll AWS: 1 /16 Route
	Ist geplant, in naher future eine Erhöhung der Bandbreite der Verbindung AWS in Betracht zu ziehen?	• Entwicklung/Test: 100 Mbit/s • Produktion: 500 Mbit/s, die auf 2 Gbit/s anwachsen.
Modelle für das Konnektivitätsdesign	Muss die Kommunikation zwischen VPC aktiviert sein (innerhalb einer Region und/oder zwischen Regionen)?	Ja, innerhalb eines AWS-Region
	Ist es erforderlich, direkt vor Ort auf AWS öffentliche Endpunktdienste zuzugreifen?	Ja
	Ist der Zugriff auf AWS Dienste mithilfe von VPC-Endpunkten vor Ort erforderlich?	Nein

Auf der Grundlage der Eingaben folgte das Architekturteam der Entscheidungsstruktur aus dem Abschnitt Konnektivitätsdesign. Nachdem das Architekturteam davon ausgegangen war, dass die Anzahl der VPCs in den nächsten 6 Monaten von 2 auf 30 steigen wird, entschied sich das Architekturteam für die Verwendung AWS Transit Gateway als Terminierungs-Gateway für die Verbindung und für das Routing zwischen VPC. Unabhängige AWS Transit Gateway Unternehmen werden die VPN-Verbindung beenden, die für Entwicklung und Tests sowie für die Produktionskonnektivität mit verwendet wurde. AWS Direct Connect Die Verwendung getrennter AWS Transit Gateway s vereinfacht das Änderungsmanagement und sorgt für eine klare Abgrenzung

zwischen Entwicklungs- und Testumgebungen und Produktionsumgebungen. Für die Produktion ist ein AWS Direct Connect Gateway aus folgenden Gründen erforderlich. AWS Transit Gateway Eine öffentliche VIF wird für den Zugriff auf AWS öffentliche Endpunktdienste verwendet. Abbildung 14 zeigt den Pfad, der im Entscheidungsbaum auf der Grundlage der gesammelten Anforderungen eingeschlagen wurde.

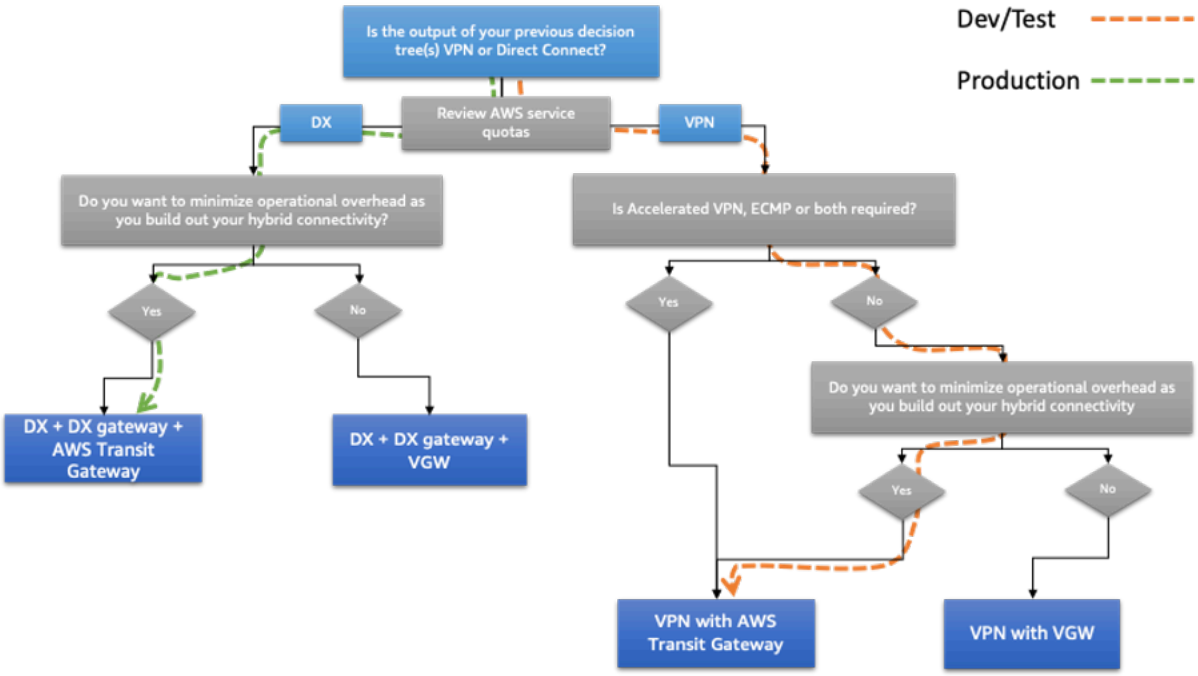

Abbildung 14 — Beispiel für einen Entscheidungsbaum für das Verbindungsdesign von Corp. Automotive

Nachdem Sie sich für die Lösung entschieden haben, die die Anforderungen an Skalierbarkeit und Kommunikationsmodell erfüllt, besteht der nächste Schritt darin, die Anforderungen im Zusammenhang mit der Zuverlässigkeit zu erfassen. Dies hängt mit dem erforderlichen Maß an Verfügbarkeit und Belastbarkeit zusammen.

Um die Zuverlässigkeitsanforderungen zu erfassen, verwendete das Architekturteam die Fragen zur Anforderungsdefinition aus dem entsprechenden Abschnitt dieses Whitepapers. Die Anforderungen sind in der folgenden Tabelle zusammengefasst.

Tabelle 6 — Fragen zu den Zuverlässigkeitsanforderungen

Überlegungen zur Auswahl des Konnektivitätsdesigns	Fragen zur Anforderungsdefinition	Antworten
Zuverlässigkeit	Wie groß sind die Auswirkungen auf das Unternehmen im Falle eines VerbindungsausfallsAWS?	• Entwicklung/Test: Niedrig • Produktion: Hoch
	AWSÜberwiegen aus geschäftlicher Sicht die Kosten für die Folgen eines Verbindungsausfalls die Kosten für die Implementierung eines äußerst zuverlässigen Konnektivitätsmodells fürAWS?	• Entwicklung/Test: Nein • Produktion: Ja

Auf der Grundlage der eingegangenen Beiträge folgte das Architekturteam dem Entscheidungsbaum aus den Abschnitten zu den Zuverlässigkeitsüberlegungen, die zuvor in diesem Whitepaper behandelt wurden. Nach Berücksichtigung des angestrebten Verfügbarkeitsziels von 99,99% für die Produktionskonnektivität und der hohen Auswirkungen auf das Geschäft bei einer Betriebsunterbrechung entschied sich das Architekturteam für die Nutzung von 2 Direct Connect-Standorten und die Einrichtung von 2 Verbindungen von jedem lokalen Rechenzentrum zu jedem Direct Connect-Standort (insgesamt 4 Links). Die für Entwicklung und Tests verwendete VPN-Konnektivität wird außerdem zwei VPN-Verbindungen für zusätzliche Redundanz verwenden. Mithilfe von Techniken zur Routenplanung, die im Abschnitt Zuverlässigkeit erörtert wurden, wird die Konnektivität wie folgt konfiguriert:

- Für Entwicklungs- und Testzwecke wird der Datenverkehr mithilfe von ECMP über die beiden Tunnel zum primären Rechenzentrum verteilt. Dies ermöglicht einen höheren Durchsatz. Die Tunnel, die zum sekundären Rechenzentrum führen, werden im Falle eines Ausfalls der primären Tunnel verwendet.
- In der Produktion ist die Latenz zwischen den lokalen Standorten und AWS über einen der Direct Connect-Standorte sehr ähnlich. In diesem Fall wurde entschieden, für die lokalen Systeme, die im primären Rechenzentrum bereitgestellt werden, einen Lastenausgleich für den Datenverkehr zwischen AWS und vor Ort über die beiden Verbindungen zum primären

Rechenzentrum durchzuführen. In ähnlicher Weise erfolgt bei lokalen Systemen, die im sekundären Rechenzentrum ausgeführt werden, ein Lastenausgleich zwischen den beiden Verbindungen zum sekundären Rechenzentrum. Im Falle eines Ausfalls der Verbindungen ermöglicht BGP einen automatisierten Failover.

Abbildung 15 zeigt den Weg, der in der Entscheidungsstruktur auf der Grundlage der gesammelten Anforderungen eingeschlagen wurde.

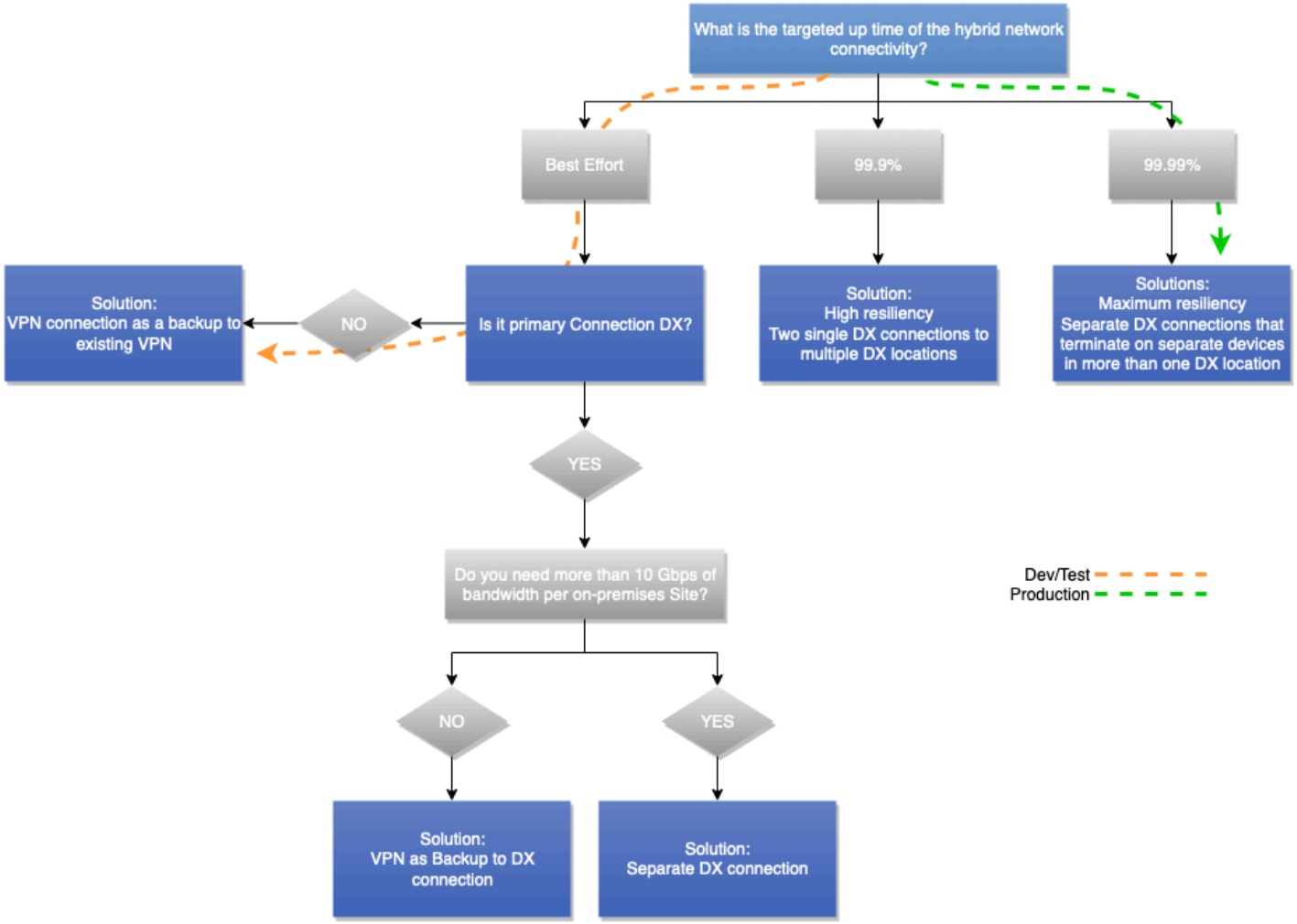

Abbildung 15 — Beispiel für einen Entscheidungsbaum zur Zuverlässigkeit von Corp. Automotive

Von Example Corp. Automotive ausgewählte Architektur

Das folgende Diagramm zeigt die Architektur, die von Example Corp. Automotive nach der Erfassung der Anforderungen und der Navigation durch die in den vorherigen Abschnitten dieses Whitepapers behandelten Entscheidungsbäume ausgewählt wurde.

Es verwendet AWS S2S-VPN über das Internet und endet für Entwicklungs- und Testzwecke. AWS Transit Gateway Es wird dann AWS Direct Connect mit Direct Connect Gateway und einem zweiten AWS Transit Gateway für den Produktionsdatenverkehr verwendet. AWS Transit Gatewaywird für Inter-VPC-Routing verwendet. Aus Sicht der Datenpfade werden die VPN-Tunnel für das primäre Rechenzentrum als primäre Pfade für Entwicklung und Tests verwendet, wobei die Tunnel zum sekundären Rechenzentrum als Failover-Pfade verwendet werden. Für den Produktionsverkehr werden alle Verbindungen gleichzeitig verwendet. Der Datenverkehr von AWS bevorzugt die optionalste Netzwerkverbindung, basierend auf dem Rechenzentrum, in dem sich das lokale System befindet. Beispiel Corp. Automotive verwendet ähnliche Route-Engineering-Techniken, um beim Senden des Datenverkehrs den geeigneten Pfad vorzuziehen, anstatt AWS sicherzustellen, dass symmetrische Verkehrspfade verwendet werden, um die Nutzung des Unternehmensnetzwerks zwischen primären und sekundären Rechenzentren vor Ort zu minimieren.

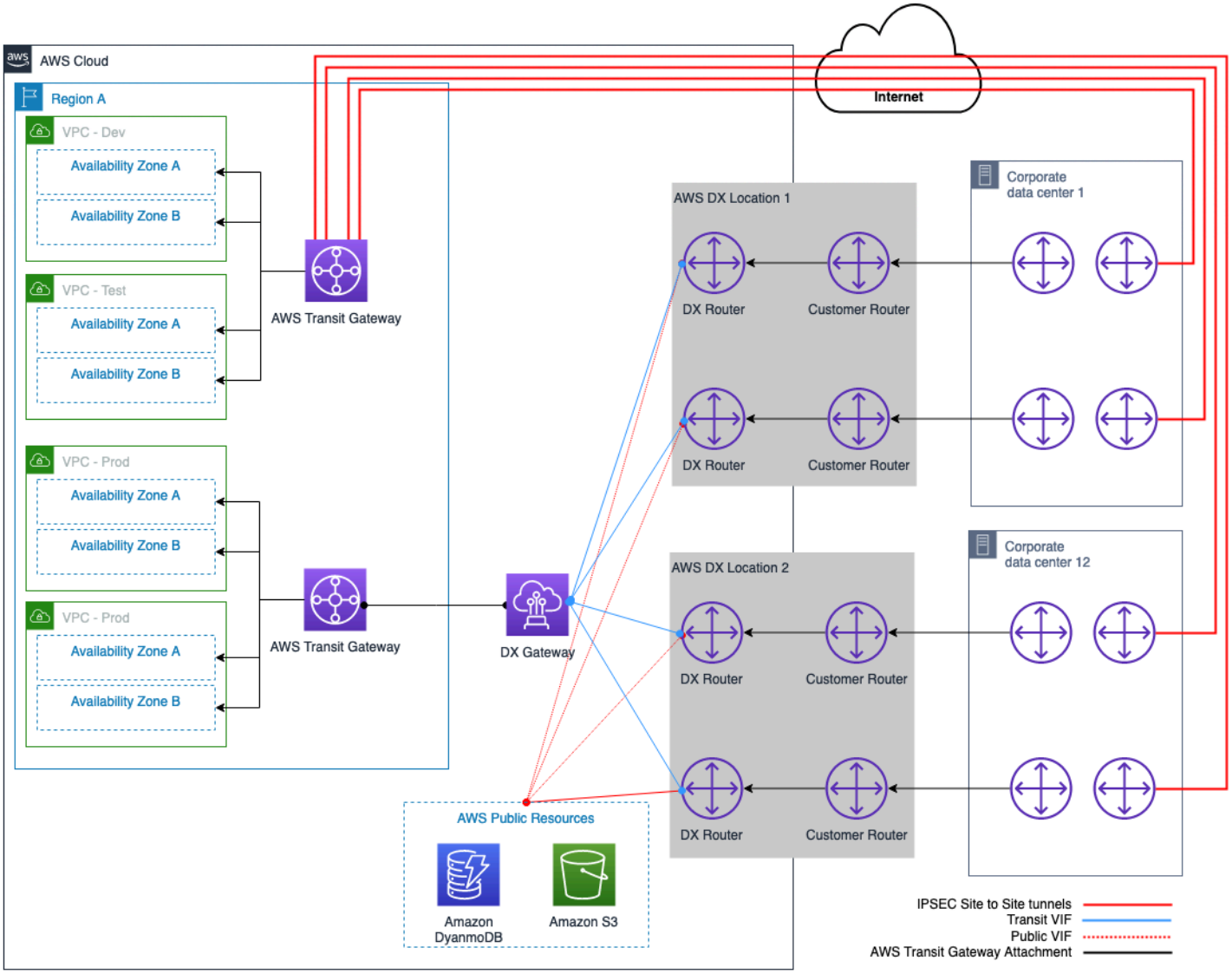

Abbildung 16 — Beispiel für ein von Corp. Automotive ausgewähltes Hybrid-Konnektivitätsmodell

Schlussfolgerung

Ein hybrides Konnektivitätsmodell ist einer der grundlegenden Ausgangspunkte für die Einführung von Cloud Computing. Nach dem in diesem Whitepaper beschriebenen Auswahlprozess für das Konnektivitätsmodell kann ein Hybridnetzwerk mit einer optimalen Architektur aufgebaut werden.

Der Prozess besteht aus Überlegungen, die in einer logischen Reihenfolge angeordnet sind. Die Reihenfolge ähnelt stark einem mentalen Modell, dem erfahrene Netzwerk- und Cloud-Architekten folgen. Innerhalb jeder Gruppe von Überlegungen ermöglichen Entscheidungsbäume eine schnelle Auswahl des Konnektivitätsmodells, selbst bei begrenzten Eingabeanforderungen. Möglicherweise stellen Sie fest, dass einige Überlegungen und die entsprechenden Auswirkungen auf unterschiedliche Lösungen hindeuten. In diesen Fällen müssen Sie als Entscheidungsträger möglicherweise Kompromisse bei einigen Anforderungen eingehen und die optimale Lösung auswählen, die Ihren geschäftlichen und technischen Anforderungen entspricht.

Beitragende Faktoren

Zu den Mitwirkenden an diesem Dokument gehören:

- James Devine, Leitender Lösungsarchitekt, Amazon Web Services
- Andrew Gray, Principal Solutions Architect — Netzwerke, Amazon Web Services
- Maks Khomutskyi, leitender Lösungsarchitekt, Amazon Web Services
- Marwan Al Shawi, Lösungsarchitekt, Amazon Web Services
- Santiago Freitas, Leiter Technologie, Amazon Web Services
- Evgeny Vaganov, spezialisierter Lösungsarchitekt — Netzwerke, Amazon Web Services
- Tom Adamski, spezialisierter Lösungsarchitekt — Netzwerke, Amazon Web Services
- Armstrong Onaiwu, Lösungsarchitekt, Amazon Web Services

Weitere Informationen

- Aufbau einer skalierbaren und sicheren Multi-VPC AWS-Netzwerkinfrastruktur
- Hybrid-Cloud-DNS-Optionen für Amazon VPC
- Amazon Virtual Private Cloud Connectivity Options
- Amazon-Virtual-Private-Cloud-Dokumentation
- AWS Direct Connect-Dokumentation:
- Was ist der Unterschied zwischen einer gehosteten virtuellen Schnittstelle (VIF) und einer gehosteten Verbindung?

Dokumentversionen

Wenn Sie über Aktualisierungen dieses Whitepapers benachrichtigt werden möchten, abonnieren Sie den RSS-Feed.

Änderung	Beschreibung	Datum
Geringfügiges Update	Aktualisiert, um der Erhöhung des DX-Kontingentlimits Rechnung zu tragen.	10. Juli 2023
Wichtiges Update	Aktualisiert, um die neuesten Best Practices, Dienste und Funktionen zu integrieren.	6. Juli 2023
Geringfügiges Update	Die Diagramme der Referenzarchitektur wurden aktualisiert, um Änderungen des DX-Kontingents widerzuspiegeln.	27. Juni 2023
Geringfügiges Update	Fehlerhafte Links behoben.	22. März 2022
Erste Veröffentlichung	Erstveröffentlichtes Whitepaper	22. September 2020

Hinweise

Die Kunden sind dafür verantwortlich, die Informationen in diesem Dokument selbst unabhängig zu beurteilen. 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. AWSProdukte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.