AWS-Whitepaper

Amazon Virtual Private Cloud Connectivity Options

Amazon Virtual Private Cloud Connectivity Options: AWS-Whitepaper

Table of Contents

Amazon Virtual Private Cloud Connectivity Options

Datum der Veröffentlichung: 5. April 2023 () Dokumentversionen

Überblick

Mit Amazon Virtual Private Cloud (Amazon VPC) können Kunden einen privaten, isolierten Bereich der Amazon Web Services (AWS) -Cloud bereitstellen, in dem sie AWS-Ressourcen in einem virtuellen Netzwerk mithilfe von kundendefinierten IP-Adressbereichen starten können. Amazon VPC bietet Kunden mehrere Optionen, um ihre virtuellen AWS-Netzwerke mit anderen Remote-Netzwerken zu verbinden. In diesem Dokument werden verschiedene gängige Netzwerkkonnektivitätsoptionen beschrieben, die unseren Kunden zur Verfügung stehen. Dazu gehören Konnektivitätsoptionen für die Integration von Remote-Kundennetzwerken mit Amazon VPC und die Verbindung mehrerer Amazon VPCs zu einem zusammenhängenden virtuellen Netzwerk.

Dieses Whitepaper richtet sich an Unternehmensnetzwerkarchitekten und -ingenieure oder Amazon VPC-Administratoren, die die verfügbaren Konnektivitätsoptionen überprüfen möchten. Es bietet einen Überblick über die verschiedenen Optionen, um Diskussionen über Netzwerkkonnektivität zu erleichtern, sowie Hinweise auf zusätzliche Dokumentation und Ressourcen mit detaillierteren Informationen oder Beispielen.

Einführung

Amazon VPC bietet mehrere Netzwerkverbindungsoptionen, die Sie je nach Ihren aktuellen Netzwerkdesigns und Anforderungen nutzen können. Zu diesen Konnektivitätsoptionen gehören die Verwendung des Internets oder einer AWS Direct Connect Verbindung als Netzwerk-Backbone und das Beenden der Verbindung zu AWS oder benutzerverwalteten Netzwerkendpunkten. Darüber hinaus können Sie mit AWS wählen, wie das Netzwerk-Routing zwischen Amazon VPC und Ihren Netzwerken bereitgestellt wird, indem Sie entweder AWS-Services oder benutzerverwaltete Netzwerkgeräte und -routen nutzen. In diesem Whitepaper werden die folgenden Optionen mit einem Überblick und einem allgemeinen Vergleich der einzelnen Optionen betrachtet:

- Network-to-Amazon VPC-Konnektivitätsoptionen
  - AWS Site-to-Site VPN — Beschreibt den Aufbau einer verwalteten IPsec VPN-Verbindung von Ihren Netzwerkgeräten in einem Remote-Netzwerk zu Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN — Beschreibt den Aufbau einer verwalteten IPsec VPN-Verbindung von Ihren Netzwerkgeräten in einem Remote-Netzwerk zu einem regionalen Netzwerk-Hub für Amazon VPCs mithilfe von AWS Transit Gateway.
  - AWS Direct Connect- Beschreibt das Herstellen einer privaten, logischen Verbindung von Ihrem Remote-Netzwerk zu Amazon VPC mithilfe von AWS Direct Connect.
  - AWS Direct Connect + AWS Transit Gateway— Beschreibt das Herstellen einer privaten, logischen Verbindung von Ihrem Remote-Netzwerk zu einem regionalen Netzwerk-Hub für Amazon VPCs mithilfe von AWS Direct Connect und AWS Transit Gateway.
  - AWS Direct Connect + Site-to-Site AWS-VPN — Beschreibt den Aufbau einer privaten, verschlüsselten Verbindung von Ihrem Remote-Netzwerk zu Amazon VPC mithilfe eines Direct Connect Site-to-Site AWS-VPN.
  - AWS Direct Connect + AWS Transit Gateway + Site-to-Site AWS-VPN— Beschreibt das Herstellen einer privaten, verschlüsselten Verbindung von Ihrem Remote-Netzwerk zu einem regionalen Netzwerk-Hub für Amazon VPCs mithilfe von Direct Connect und AWS Transit Gateway.
  - Site-to-Site VPN CloudHub— Beschreibt die Einrichtung eines hub-and-spoke Modells für die Verbindung von Zweigstellen an entfernten Standorten.
  - Software-VPN— Beschreibt den Aufbau einer VPN-Verbindung von Ihren Geräten in einem Remote-Netzwerk zu einer benutzerverwalteten Software-VPN-Appliance, die in einer Amazon VPC ausgeführt wird.

  - AWS Transit Gateway + SD-WAN-Lösungen- Beschreibt die Integration von softwaredefinierten Wide Area Network (SD-WAN) -Lösungen zur Verbindung mehrerer entfernter Standorte mit einem regionalen Netzwerkknotenpunkt für Amazon VPCs, wobei der AWS Backbone oder das Internet als Transitnetzwerk genutzt wird.
- Amazon VPC-to-Amazon VPC-Verbindungsoptionen
  - VPC-Peering— Beschreibt die Verbindung VPCs von Amazon innerhalb und zwischen Regionen mithilfe der Amazon VPC-Peering-Funktion.
  - AWS Transit Gateway— Beschreibt die Verbindung VPCs von Amazon innerhalb und zwischen AWS Transit Gateway Regionen mithilfe eines hub-and-spoke Modells.
  - AWS PrivateLink— Beschreibt die Verbindung von Amazon VPCs mit VPC-Schnittstellenendpunkten und VPC-Endpunktdiensten.
  - Software-VPN— Beschreibt die Verbindung VPCs von Amazon über VPN-Verbindungen, die zwischen benutzerverwalteten Software-VPN-Appliances hergestellt werden, die in jeder Amazon VPC ausgeführt werden.
  - VPN-to-AWS Site-to-SiteSoftware-VPN— Beschreibt die Verbindung von Amazon VPCs mit einer VPN-Verbindung, die zwischen einer benutzerverwalteten Software-VPN-Appliance in einer Amazon-VPC und einem an die andere Amazon-VPC angeschlossenen AWS Site-to-Site VPN hergestellt wird.
- Optionen für access-to-Amazon Software-Remote-VPC-Konnektivität
  - AWS Client VPN— Beschreibt die Verbindung des Software-Fernzugriffs mit Amazon VPC unter Nutzung von AWS Client VPN.
  - Software-Client-VPN— Beschreibt die Verbindung von Software-Fernzugriff mit Amazon VPC unter Nutzung von benutzerverwalteten Software-VPN-Appliances.
- Transit-VPC- Beschreibt den Aufbau eines globalen Transitnetzes auf AWS mithilfe eines Software-VPN in Verbindung mit einem von AWS verwalteten VPN.
- AWS-Cloud-WAN- Beschreibt die Einrichtung eines verwalteten Wide Area Network (WAN) zum einfachen Aufbau, zur Verwaltung und Überwachung globaler Verbindungen zwischen Ressourcen in Amazon VPCs, Rechenzentren und Zweigstellen.

Network-to-Amazon VPC-Konnektivitätsoptionen

Dieser Abschnitt enthält Entwurfsmuster für die Verbindung von Remote-Netzwerken mit Ihrer Amazon VPC-Umgebung. Diese Optionen sind nützlich für die Integration von AWS-Ressourcen in Ihre vorhandenen Services vor Ort (z. B. Überwachung, Authentifizierung, Sicherheit, Daten oder andere Systeme), indem Sie Ihre internen Netzwerke in die AWS-Cloud erweitern. Diese Netzwerkerweiterung ermöglicht es Ihren internen Benutzern auch, sich nahtlos mit Ressourcen zu verbinden, die auf AWS gehostet werden, genau wie jede andere intern zugängliche Ressource.

VPC-Konnektivität zu Remote-Kundennetzwerken wird am besten erreicht, wenn für jedes verbundene Netzwerk nicht überlappende IP-Bereiche verwendet werden. Wenn Sie beispielsweise eines oder mehrere VPCs Geräte mit Ihrem Unternehmensnetzwerk verbinden möchten, stellen Sie sicher, dass sie mit eindeutigen CIDR-Bereichen (Classless Inter-Domain Routing) konfiguriert sind. Wir empfehlen, jeder VPC einen einzigen, zusammenhängenden, nicht überlappenden CIDR-Block zuzuweisen. Weitere Informationen zu Amazon VPC-Routing und Einschränkungen finden Sie in den häufig gestellten Fragen zu Amazon VPC.

Option	Anwendungsfall	Vorteile	Einschränkungen
Site-to-SiteAWS-VPN	Von AWS verwaltete IPsec VPN-Verbindung über das Internet zu einer einzelnen VPC	Wiederverwendung vorhandener VPN-Geräte und -Prozesse Verwenden Sie bestehende Internetverbindungen wieder Von AWS verwalteter VPN-Service mit hoher Verfügbarkeit Unterstützt statische Routen oder dynamische Peering- und Routing-Richtlinien für das Border	Netzwerklatenz, Variabilität und Verfügbarkeit hängen von den Internetbedingungen ab Sie sind für die Implementierung von Redundanz und Failover (falls erforderlich) verantwortlich Das Remote-Gerät muss Single-Hop-BGP unterstützen (wenn BGP für dynamisches Routing genutzt wird)

Option	Anwendungsfall	Vorteile	Einschränkungen
		Gateway Protocol (BGP)	
AWS Transit Gateway Gateway+ Site-to-Site AWS-VPN	Von AWS verwaltete IPsec VPN-Verbindung über das Internet zum regionalen Router für mehrere VPCs	Entspricht der vorherigen Option Von AWS verwalteter regionaler Netzwerkhub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5.000 Anlagen	Identisch mit der vorherigen Option
AWS Direct Connect	Dedizierte Netzwerkverbindung über private Leitungen	Vorhersehbarere Netzwerkleistung Geringere Bandbreitenkosten Unterstützt BGP-Peering- und Routing-Richtlinien	Möglicherweise müssen zusätzliche Beziehungen zu Telekommunikations- und Hosting-Anbietern oder die Bereitstellung neuer Netzwerkverbindungen erforderlich sein
AWS Direct Connect + AWS Transit Gateway	Dedizierte Netzwerkverbindung über private Leitungen zum regionalen Router für mehrere VPCs	Entspricht der vorherigen Option Von AWS verwalteter regionaler Netzwerkhub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5.000 Anlagen	Entspricht der vorherigen Option

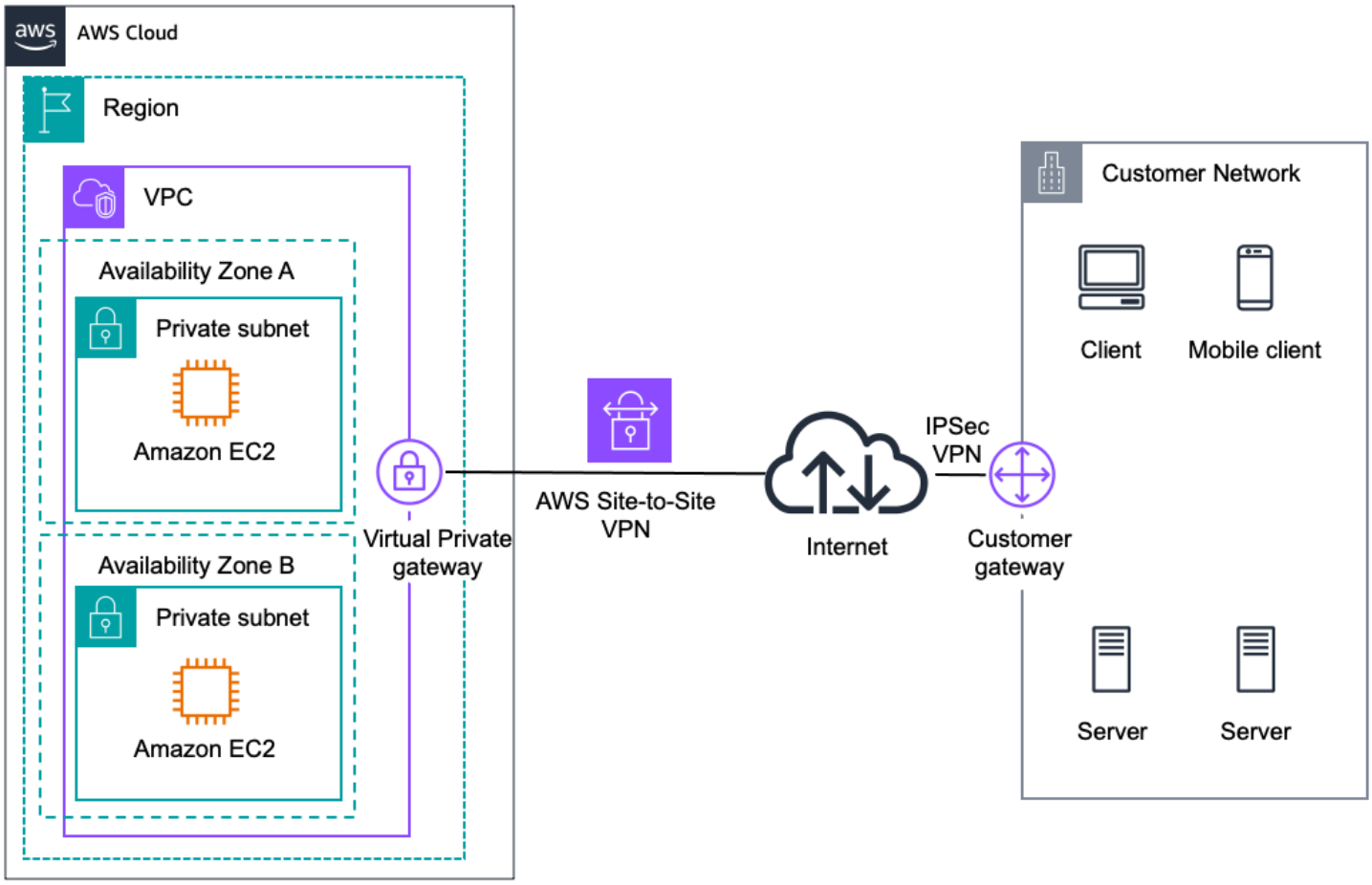
Option	Anwendungsfall	Vorteile	Einschränkungen
AWS Direct Connect + Site-to-Site AWS-VPN	IPsec VPN-Verbindung über private Leitungen	Vorhersehbarere Netzwerkleistung Geringere Bandbreitenkosten Unterstützt BGP-Peering- und Routing-Richtlinien für AWS Direct Connect Verwenden Sie vorhandene VPN-Geräte und -Prozesse wieder Von AWS verwalteter VPN-Service mit hoher Verfügbarkeit Unterstützt statische Routen oder dynamische Peering- und Routing-Richtlinien für das Border Gateway Protocol (BGP) für VPN-Verbindungen	Möglicherweise müssen zusätzliche Beziehungen zu Telekommunikations- und Hosting-Anbietern oder die Bereitstellung neuer Netzwerkverbindungen erforderlich sein Sie sind für die Implementierung von Redundanz und Failover (falls erforderlich) verantwortlich Das Remote-Gerät muss Single-Hop-BGP unterstützen (wenn BGP für dynamisches Routing genutzt wird)

Option	Anwendungsfall	Vorteile	Einschränkungen
AWS Direct Connect + AWS Transit Gateway + Site-to-Site AWS-VPN	IPsec VPN-Verbindung über private Leitungen zum regionalen Router für mehrere VPCs	Wie bei der vorherigen Option Von AWS verwalteter regionaler Netzwerkhub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5.000 Anlagen	Entspricht der vorherigen Option
Site-to-Site VPN CloudHub	Connect entfernte Zweigstellen in einem hub-and-spoke Modell für Primär- oder Backup-Konnektivität	Verwenden Sie bestehende Internetverbindungen und Site-to-Site VPN -verbindungen wieder Von AWS verwalteter VPN-Service mit hoher Verfügbarkeit Unterstützt BGP für den Austausch von Routen und Routing-Prioritäten	Netzwerklatenz, Variabilität und Verfügbarkeit hängen vom Internet ab Benutzerverwaltete Endgeräte in Zweigstellen sind für die Implementierung von Redundanz und Failover (falls erforderlich) verantwortlich
AWS Transit Gateway + SD-WAN-Lösungen	Connect entfernte Niederlassungen und Büros mit einem softwaredefinierten Wide Area Network, indem Sie den AWS Backbone oder das Internet als Transitnetzwerk verwenden.	Unterstützt eine breitere Palette von SD-WAN-Anbietern, -Produkten und -Protokollen Einige Anbieterlösungen sind in native AWS-Services integriert.	Sie sind für die Implementierung von HA (Hochverfügbarkeit) der SD-WAN-Appliances verantwortlich, wenn sie in einer Amazon VPC platziert sind.

Option	Anwendungsfall	Vorteile	Einschränkungen
Software-VPN	VPN-Verbindung auf Software-Appliance -Basis über das Internet	Unterstützt eine breitere Palette von VPN-Anbietern, -Produkten und -Protokollen Vollständig vom Kunden verwaltete Lösung	Sie sind verantwortlich für die Implementierung von HA-Lösungen (Hochverfügbarkeit) für alle VPN-Endpunkte (falls erforderlich)

Site-to-SiteAWS-VPN

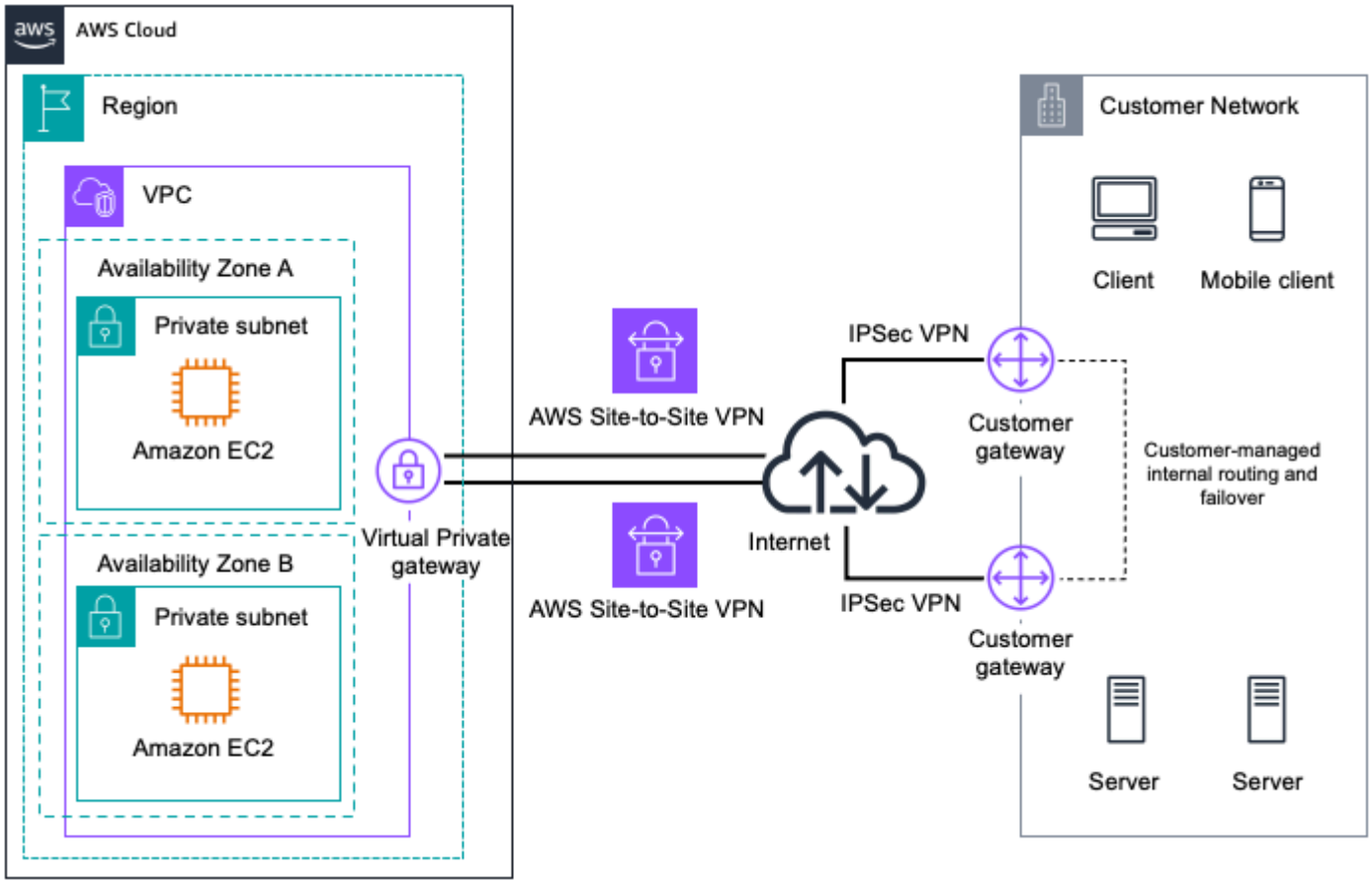
Amazon VPC bietet die Möglichkeit, eine IPsec VPN-Verbindung zwischen Ihren Remote-Netzwerken und Amazon VPC über das Internet herzustellen, wie in der folgenden Abbildung dargestellt.



AWS Managed VPN

Ziehen Sie diesen Ansatz in Betracht, wenn Sie einen von AWS verwalteten VPN-Endpunkt nutzen möchten, der automatische Redundanz und Failover umfasst, die in die AWS-Seite der VPN-Verbindung integriert sind.

Das Virtual Private Gateway unterstützt und unterstützt auch Gateway-Verbindungen für mehrere Benutzer, sodass Sie Redundanz und Failover auf Ihrer Seite der VPN-Verbindung implementieren können, wie in der folgenden Abbildung dargestellt.



Redundant AWS Site-to-Site VPN Connections

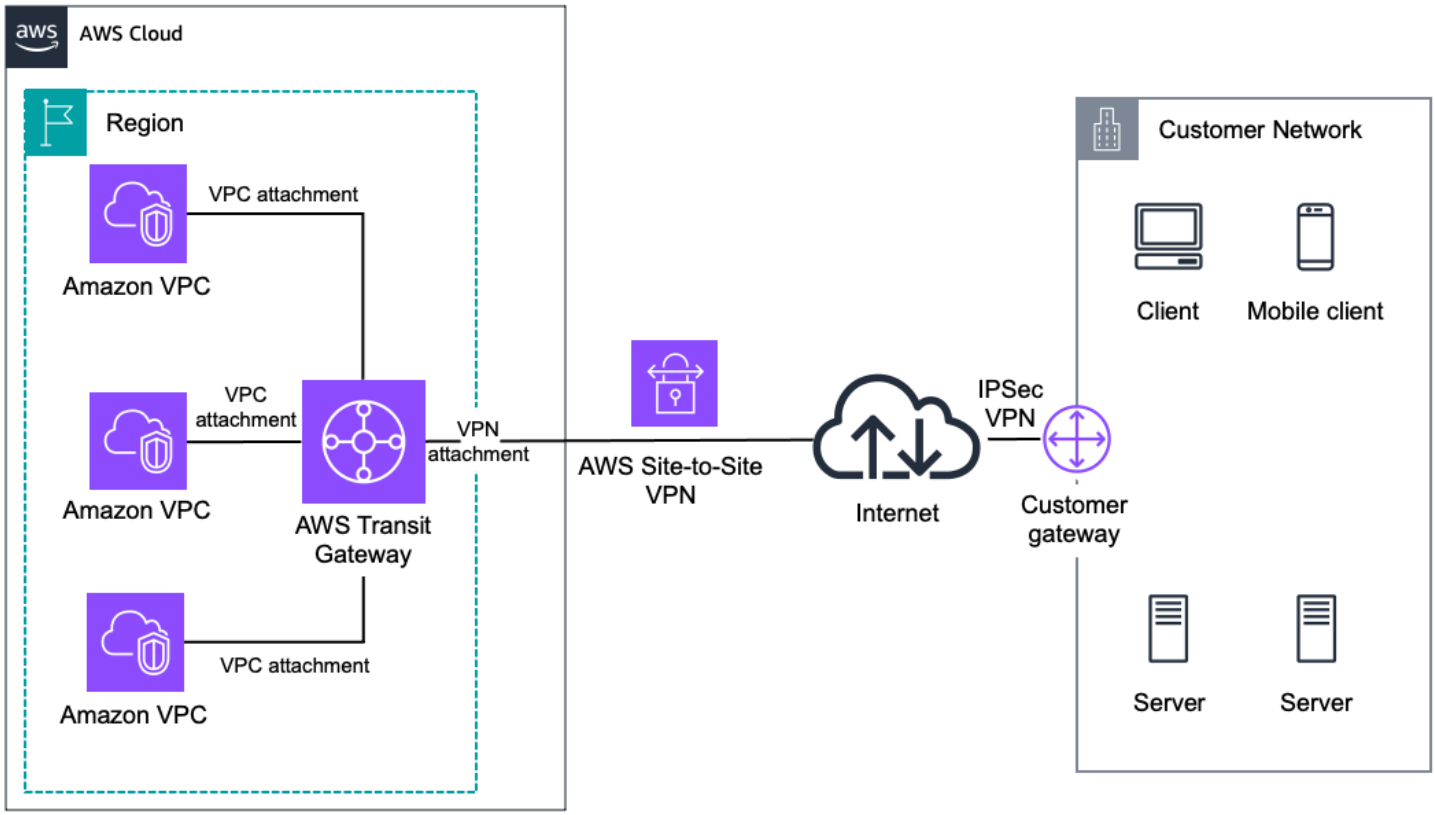
Es stehen sowohl dynamische als auch statische Routing-Optionen zur Verfügung, um Ihnen Flexibilität bei der Routing-Konfiguration zu bieten. Dynamisches Routing verwendet BGP-Peering, um Routing-Informationen zwischen AWS und diesen Remote-Endpunkten auszutauschen. Mit dynamischem Routing können Sie auch Routing-Prioritäten, Richtlinien und Gewichtungen (Metriken) in Ihren BGP-Anzeigen angeben und den Netzwerkpfad zwischen Ihren Netzwerken und AWS beeinflussen. Es ist wichtig zu beachten, dass bei der Verwendung von BGP sowohl die als auch die IPsec BGP-Sitzungen auf demselben Benutzer-Gateway-Gerät beendet werden müssen, sodass es in der Lage sein muss, sowohl IPsec BGP-Sitzungen als auch BGP-Sitzungen zu beenden.

Weitere Ressourcen

- Site-to-SiteAWS-VPN-Benutzerhandbuch
- Anforderungen für Kunden-Gateway-Geräte
- Kunden-Gateway-Geräte, die mit Amazon VPC getestet wurden

AWS Transit Gateway Gateway+ Site-to-Site AWS-VPN

AWS Transit Gateway ist ein von AWS verwalteter regionaler Netzwerk-Transitknotenpunkt mit hoher Verfügbarkeit und Skalierbarkeit, der für Verbindungen VPCs und Kundennetzwerke verwendet wird. AWS Transit Gateway + VPN bietet mithilfe des Transit Gateway-VPN-Anhangs die Möglichkeit, eine IPsec VPN-Verbindung zwischen Ihrem Remote-Netzwerk und dem Transit Gateway über das Internet herzustellen, wie in der folgenden Abbildung dargestellt.

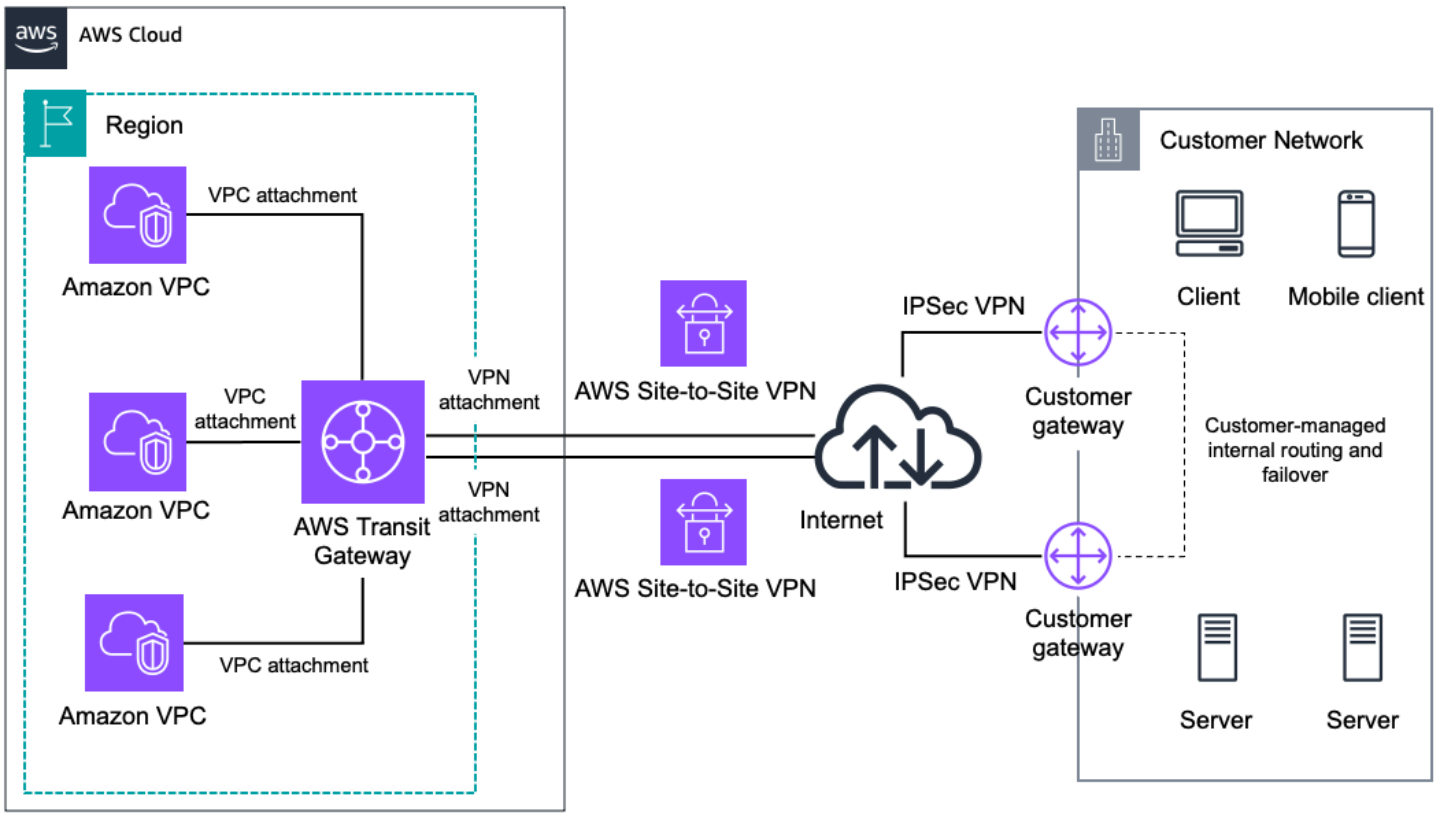


AWS Transit Gateway and AWS Site-to-Site VPN

Ziehen Sie diesen Ansatz in Betracht, wenn Sie einen von AWS verwalteten VPN-Endpunkt nutzen möchten, um eine Verbindung zu mehreren VPCs in derselben Region herzustellen, ohne die

zusätzlichen Kosten und die Verwaltung mehrerer IPsec VPN-Verbindungen zu mehreren Amazon. VPCs

AWS Transit Gateway unterstützt und unterstützt auch Gateway-Verbindungen für mehrere Benutzer, sodass Sie Redundanz und Failover auf Ihrer Seite der VPN-Verbindung implementieren können, wie in der folgenden Abbildung dargestellt.



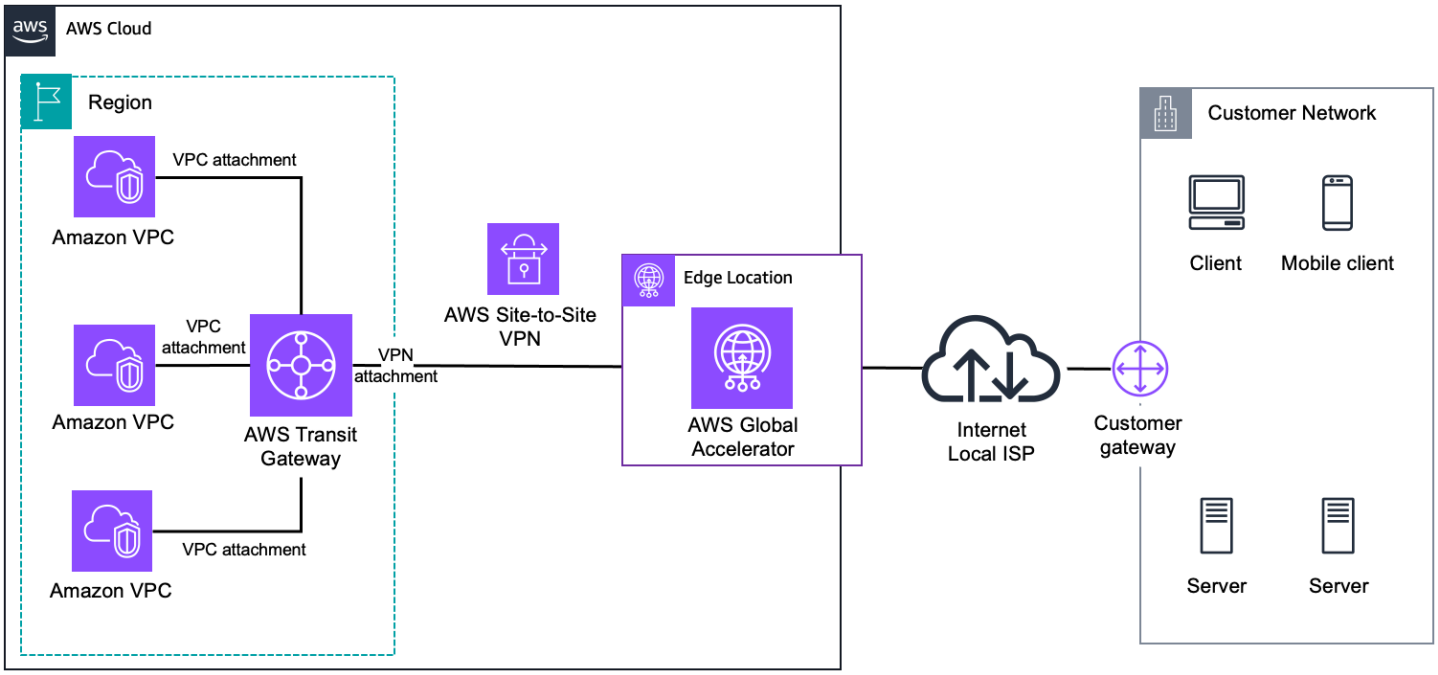
AWS Transit Gateway and Redundant VPN

Sowohl dynamische als auch statische Routing-Optionen stehen zur Verfügung, um Ihnen Flexibilität bei der Routing-Konfiguration des Transit Gateway IPsec Gateway-VPN-Anhangs zu bieten. Dynamisches Routing verwendet BGP-Peering, um Routing-Informationen zwischen AWS und diesen Remote-Endpunkten auszutauschen. Mit dynamischem Routing können Sie auch Routing-Prioritäten, Richtlinien und Gewichtungen (Metriken) in Ihren BGP-Anzeigen angeben und den Netzwerkpfad zwischen Ihren Netzwerken und AWS beeinflussen. Es ist wichtig zu beachten, dass bei der Verwendung von BGP sowohl die als auch die IPsec BGP-Sitzungen auf demselben Benutzer-Gateway-Gerät beendet werden müssen, sodass es in der Lage sein muss, sowohl IPsec BGP-Sitzungen als auch BGP-Sitzungen zu beenden.

Pro VPN-Verbindung können Sie einen Durchsatz von 1,25 Gbit/s und 140.000 Pakete pro Sekunde erreichen. Wenn Sie die VPN-Verbindungen im Transit Gateway beenden, können Sie Equal Cost

Multi-Path (ECMP) -Routing verwenden, um eine höhere VPN-Bandbreite zu erhalten, indem Sie mehrere VPN-Tunnel aggregieren. Um ECMP verwenden zu können, müssen Sie dynamisches Routing in den VPN-Verbindungen konfigurieren. ECMP wird bei Verwendung von statischem Routing nicht unterstützt.

Darüber hinaus können Sie die Beschleunigung Ihrer Site-to-Site AWS-VPN-Verbindungen aktivieren. Eine beschleunigte VPN-Verbindung verwendet AWS Global Accelerator, um den Datenverkehr von Ihrem Netzwerk zu einem AWS-Edge-Standort weiterzuleiten, der Ihrem Kunden-Gateway-Gerät am nächsten ist. Sie können diese Option verwenden, um Netzwerkunterbrechungen zu vermeiden, die auftreten können, wenn der Datenverkehr über das öffentliche Internet geleitet wird. Die Beschleunigung wird nur für VPN-Verbindungen unterstützt, die an ein Transit Gateway angeschlossen sind, wie in der folgenden Abbildung dargestellt:



Accelerated AWS Site-to-Site VPN

Was schließlich die IP-Adressierung anbelangt, so AWS Transit Gateway unterstützen Site-to-Site VPN-Verbindungen auf einem IPv4 sowohl den Datenverkehr als auch IPv6 den Datenverkehr. Die folgenden Regeln gelten:

- IPv6 wird nur für die internen IP-Adressen des VPN-Tunnels unterstützt. Die externen IP-Adressen für die AWS Endpunkte sind öffentliche IPv4 Adressen. Die Gateway-IP-Adresse des Kunden sollte eine öffentliche IPv4 Adresse sein.

- Eine Site-to-Site VPN-Verbindung kann nicht IPv4 sowohl als auch IPv6 Datenverkehr unterstützen. Wenn Ihre Hybrid-Konnektivität eine Dual-Stack-Kommunikation erfordert, sollten Sie verschiedene VPN-Tunnel für den IPv4 IPv6 UND-Verkehr einrichten.

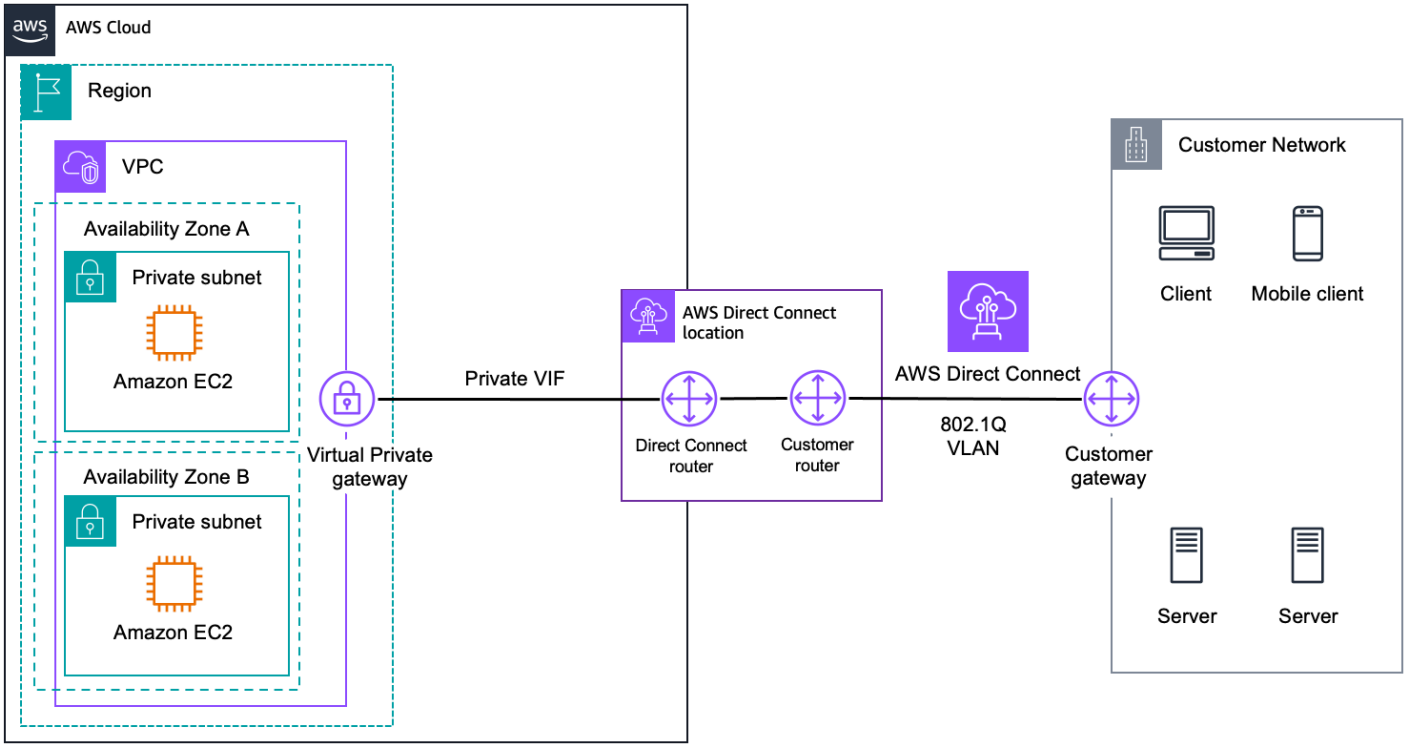
Weitere Ressourcen

- VPN-Anhänge für Transit-Gateways
- Kunden-Gateway
- Arbeitet mit Site-to-Site VPN
- Beschleunigte Site-to-Site VPN-Verbindungen

AWS Direct Connect

AWS Direct Connectmacht es einfach, eine dedizierte Verbindung von einem lokalen Netzwerk zu einem oder mehreren VPCs herzustellen. Direct Connect kann die Netzwerkkosten senken, den Bandbreitendurchsatz erhöhen und ein einheitlicheres Netzwerkerlebnis bieten als internetbasierte Verbindungen. Es verwendet den Industriestandard 802.1Q VLANs , um über private IP-Adressen eine Verbindung zu Amazon VPC herzustellen. Sie VLANs werden mithilfe virtueller Schnittstellen (VIFs) konfiguriert, und Sie können drei verschiedene Typen konfigurieren: VIFs

- Öffentliche virtuelle Schnittstelle — Stellen Sie Konnektivität zwischen AWS öffentlichen Endpunkten und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung her.
- Virtuelle Transitschnittstelle — Stellen Sie eine private Konnektivität zwischen AWS Transit Gateway Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung her. Diese Konnektivitätsoption wird im Abschnitt ??? behandelt.
- Private virtuelle Schnittstelle — Stellen Sie eine private Konnektivität zwischen Amazon VPC-Ressourcen und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung her. Die Verwendung von Private VIFs ist in der folgenden Abbildung dargestellt.



AWS Direct Connect

Sie können die Konnektivität zum AWS Backbone herstellen, AWS Direct Connect indem Sie eine Querverbindung zu AWS Geräten an einem Direct Connect-Standort herstellen. Sie können von jedem unserer Direct Connect-Standorte aus auf jede AWS Region zugreifen (außer China). Wenn Sie an einem Standort keine Geräte haben, können Sie aus einem Ökosystem von WAN-Dienstanbietern wählen, um Ihren AWS Direct Connect Endpunkt an einem AWS Direct Connect Standort in Ihre Remote-Netzwerke zu integrieren.

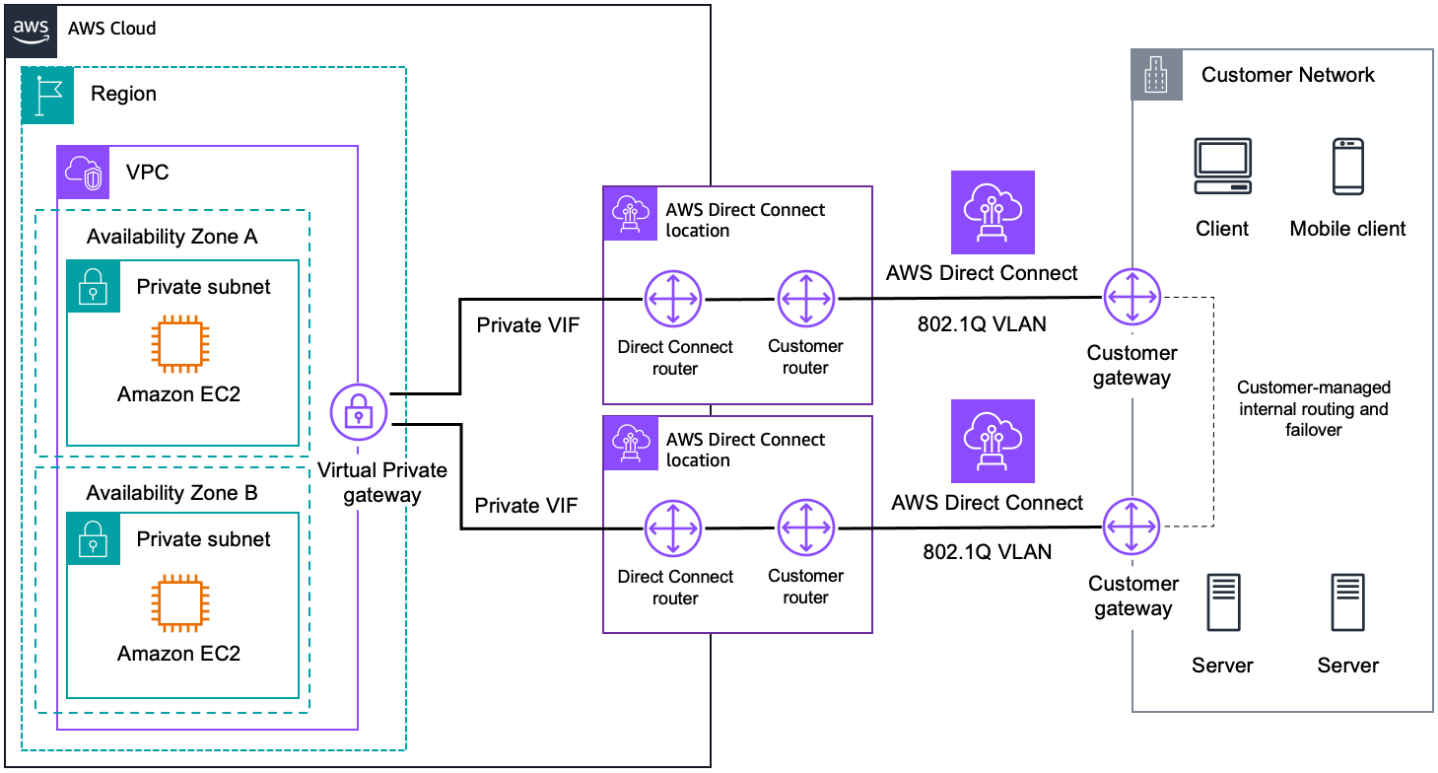
Mit AWS Direct Connect haben Sie zwei Arten von Verbindungen:

- Dedizierte Verbindungen, bei denen eine physische Ethernet-Verbindung einem einzelnen Kunden zugeordnet ist. Sie können Port-Geschwindigkeiten von 1, 10 oder 100 Gbit/s bestellen. Möglicherweise müssen Sie mit einem Partner im AWS Direct Connect Partnerprogramm zusammenarbeiten, der Sie beim Aufbau von Netzwerkverbindungen zwischen einer AWS Direct Connect Verbindung und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung unterstützt.
- Gehostete Verbindungen, bei denen eine physische Ethernet-Verbindung von einem AWS Direct Connect Partner bereitgestellt und mit Ihnen geteilt wird. Sie können Portgeschwindigkeiten zwischen 50 Mbit/s und 10 Gbit/s bestellen. Sie arbeiten mit dem Partner sowohl in Bezug auf die Direct Connect Verbindung, die der Partner hergestellt hat, als auch in Bezug auf

die Netzwerkverbindungen zwischen einer AWS Direct Connect Verbindung und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung zusammen.

Für dedizierte Verbindungen können Sie auch eine Link Aggregation Group (LAG) verwenden, um mehrere Verbindungen an einem einzigen AWS Direct Connect Endpunkt zusammenzufassen. Sie behandeln sie als eine einzige, verwaltete Verbindung. Sie können bis zu vier 1- oder 10-Gbit/s-Verbindungen und bis zu zwei 100-Gbit/s-Verbindungen zusammenfassen.

Wenn es um Hochverfügbarkeit geht AWS Direct Connect, empfehlen wir die Verwendung zusätzlicher Verbindungen. Direct Connect Das Direct Connect Resiliency Toolkit bietet Anleitungen zum Aufbau hochbelastbarer Netzwerkverbindungen zwischen AWS Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung. Die folgende Abbildung zeigt ein Beispiel für eine Verbindungsoption mit hoher Ausfallsicherheit, bei der zwei Direct Connect Verbindungen an zwei verschiedenen Orten beendet werden. Direct Connect

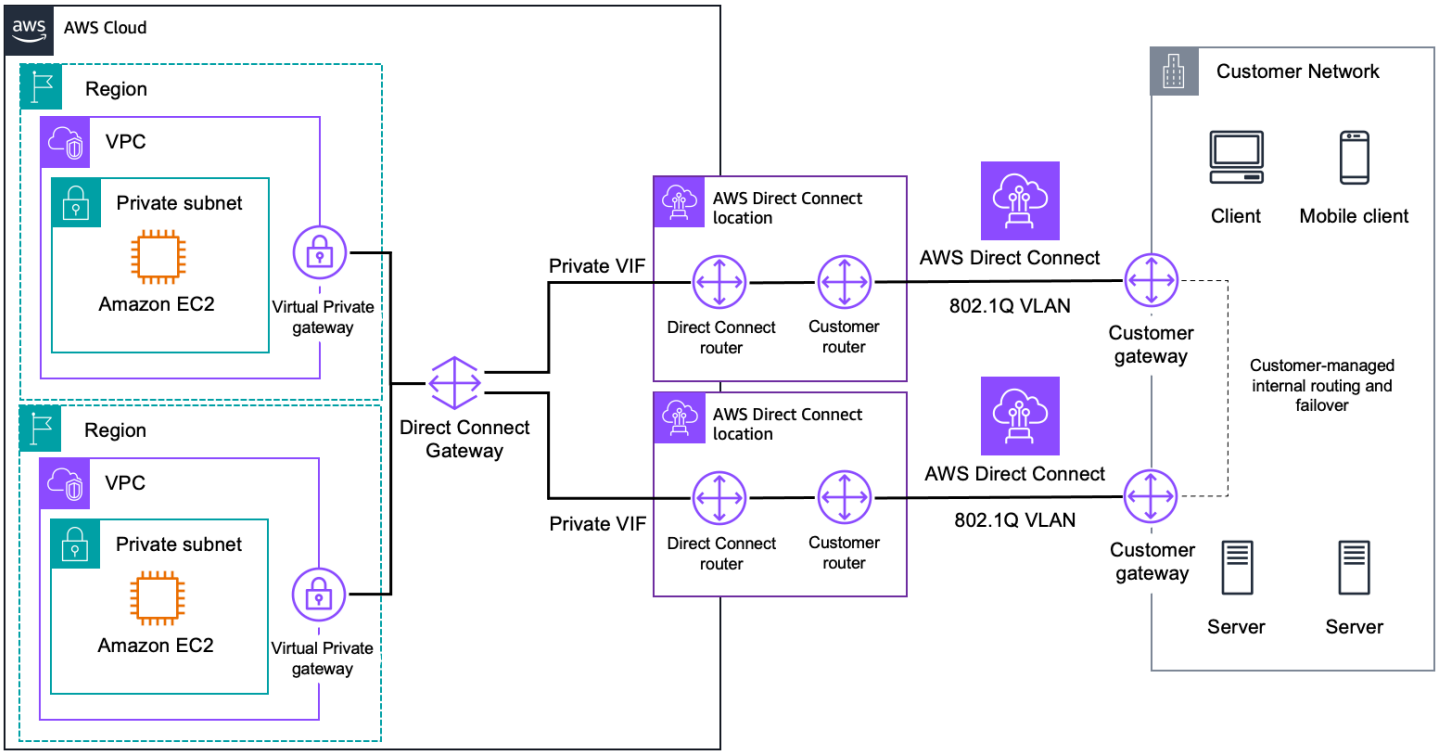


Redundant AWS Direct Connect

AWS Direct Connect ist standardmäßig nicht verschlüsselt. Für dedizierte Verbindungen mit 10 oder 100 Gbit/s können Sie MAC security (MACsec) als Verschlüsselungsoption verwenden. Für Verbindungen mit einer Geschwindigkeit von 1 Gbit/s oder weniger können Sie VPN-Tunnel über

der Verbindung einrichten. Diese Option wird in den Abschnitten AWS Direct Connect + Site-to-Site AWS-VPN und AWS Direct Connect + AWS Transit Gateway + Site-to-Site AWS-VPN 3 beschrieben.

Eine wichtige Ressource AWS Direct Connect ist das Direct Connect-Gateway, eine weltweit verfügbare Ressource, die Verbindungen zu mehreren Amazon VPCs - oder Transit-Gateways in verschiedenen Regionen oder AWS Konten ermöglicht. Mit dieser Ressource können Sie auch von einer privaten VIF oder Transit-VIF aus eine Verbindung zu allen teilnehmenden VPC oder Transit-Gateways herstellen, wodurch der AWS Direct Connect Verwaltungsaufwand reduziert wird, wie in der folgenden Abbildung dargestellt.



AWS Direct Connect Gateway

In Bezug auf die IP-Adressierung unterstützen AWS Direct Connect virtuelle Schnittstellen sowohl IPv4 BGP-Sitzungen als auch IPv6 BGP-Sitzungen für den Dual-Stack-Betrieb.

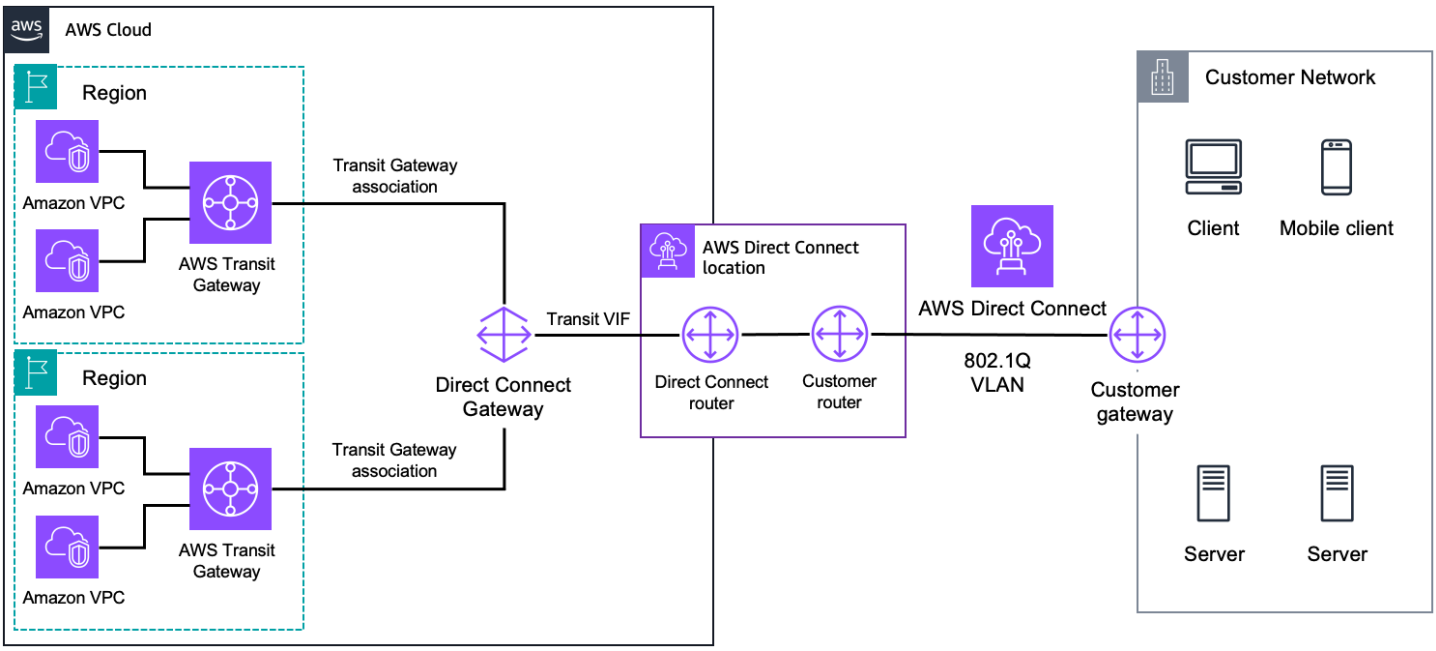
- Privat- und VIFs IPv4 Transitkonfigurationen verwenden entweder AWS-generierte IPv4 Adressen oder von Ihnen konfigurierte Adressen. Für öffentliches VIFs IPv4 BGP-Peering müssen Sie eine eindeutige öffentliche IPv4 /31-CIDR angeben, die Sie besitzen (oder eine Anfrage zur Zuweisung eines CIDR-Blocks einreichen).
- Für alle Arten von VIFs IPv6 BGP-Peering weist AWS einen /125 CIDR zu, der nicht konfigurierbar ist.

Weitere Ressourcen

- AWS Direct Connect Benutzerhandbuch
- AWS Direct Connect virtuelle Schnittstellen
- AWS Direct Connect Gateways
- AWS Direct Connect Toolkit für Resilienz
- AWS Direct Connect MAC-Sicherheit
- AWS Direct Connect Standorte
- AWS Direct Connect Lieferpartner

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gatewayermöglicht es Ihrem Netzwerk mithilfe einer Transit-VIF-Verbindung zum Direct Connect-Gateway, mehrere regionale zentrale Router über eine private, dedizierte Verbindung zu verbinden. Das folgende Diagramm zeigt die Verbindung zu zwei Routern.



AWS Direct Connect and AWS Transit Gateway

Jeder AWS Transit Gateway ist ein Netzwerk-Transit-Hub für Verbindungen VPCs in derselben Region, wodurch die Amazon VPC-Routing-Konfiguration an einem Ort konsolidiert wird. Diese Lösung vereinfacht die Verwaltung von Verbindungen zwischen einer Amazon VPC und Ihren Netzwerken über eine private Verbindung, wodurch die Netzwerkkosten gesenkt,

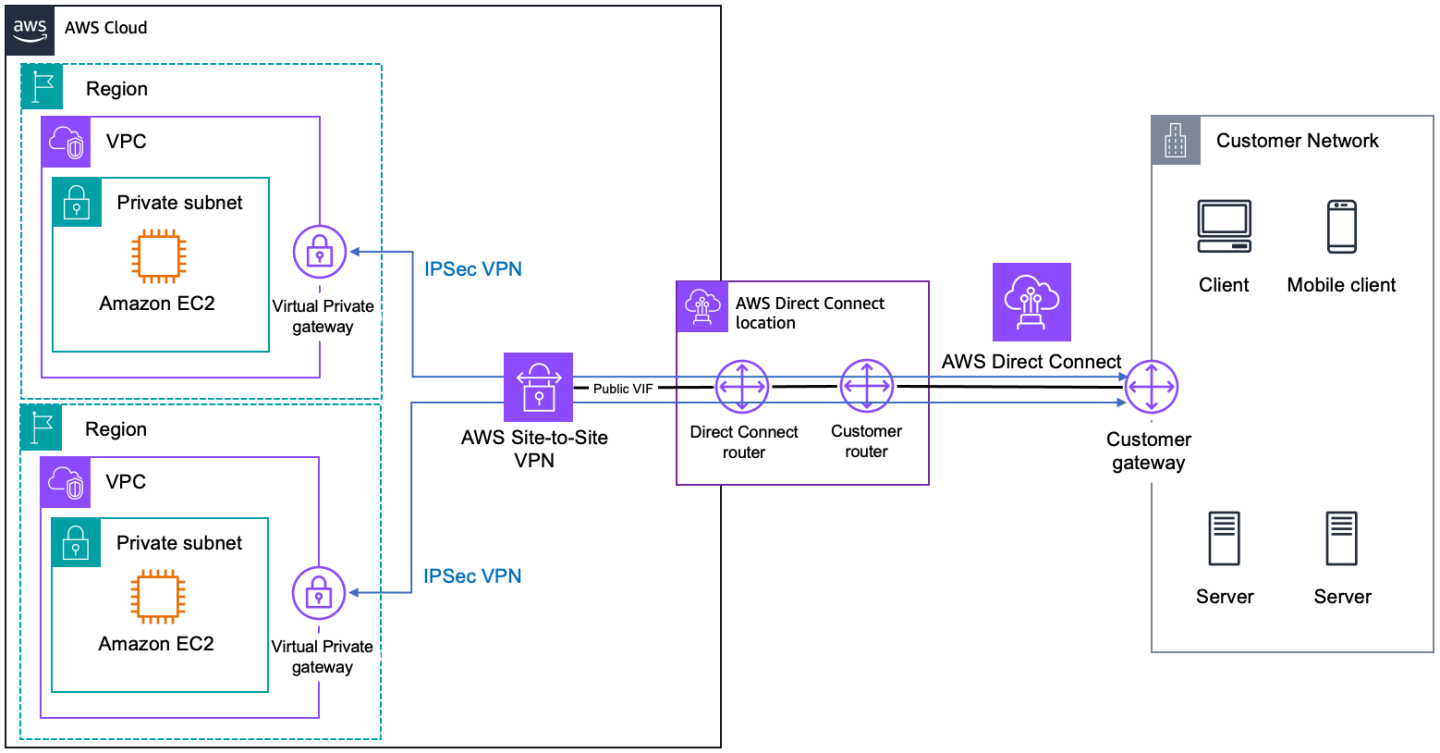
der Bandbreitendurchsatz erhöht und ein einheitlicheres Netzwerkerlebnis als internetbasierte Verbindungen ermöglicht werden können.

Weitere Ressourcen

- AWS Direct Connect-Benutzerhandbuch
- Link-Aggregationsgruppen in AWS Direct Connect
- Blogbeitrag: Integration von gehosteten Verbindungen mit Sub-1 Gbit/s in AWS Transit Gateway

AWS Direct Connect + Site-to-Site AWS-VPN

Mit AWS Direct Connect+ AWS Site-to-Site VPN können Sie AWS Direct Connect Verbindungen mit einer von AWS verwalteten VPN-Lösung kombinieren. AWS Direct Connect public VIFs stellen Sie eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS-Ressourcen wie einem Site-to-Site AWS-VPN-Endpunkt her. Sobald Sie die Verbindung zum Service hergestellt haben, können Sie IPsec Verbindungen zu den entsprechenden virtuellen privaten Gateways von Amazon VPC herstellen. Die folgende Abbildung veranschaulicht diese Option.



AWS Direct Connect and AWS Site-to-Site VPN

Diese Lösung kombiniert die Vorteile einer end-to-end sicheren IPsec Verbindung mit geringer Latenz und erhöhter Bandbreite und bietet so ein einheitlicheres Netzwerkerlebnis als internetbasierte VPN-Verbindungen. AWS Direct Connect Eine BGP-Verbindungssitzung wird zwischen AWS Direct Connect und Ihrem Router auf der öffentlichen VIF eingerichtet. Eine weitere BGP-Sitzung oder eine statische Route wird zwischen dem Virtual Private Gateway und Ihrem Router in den VPN-Tunneln eingerichtet. IPsec

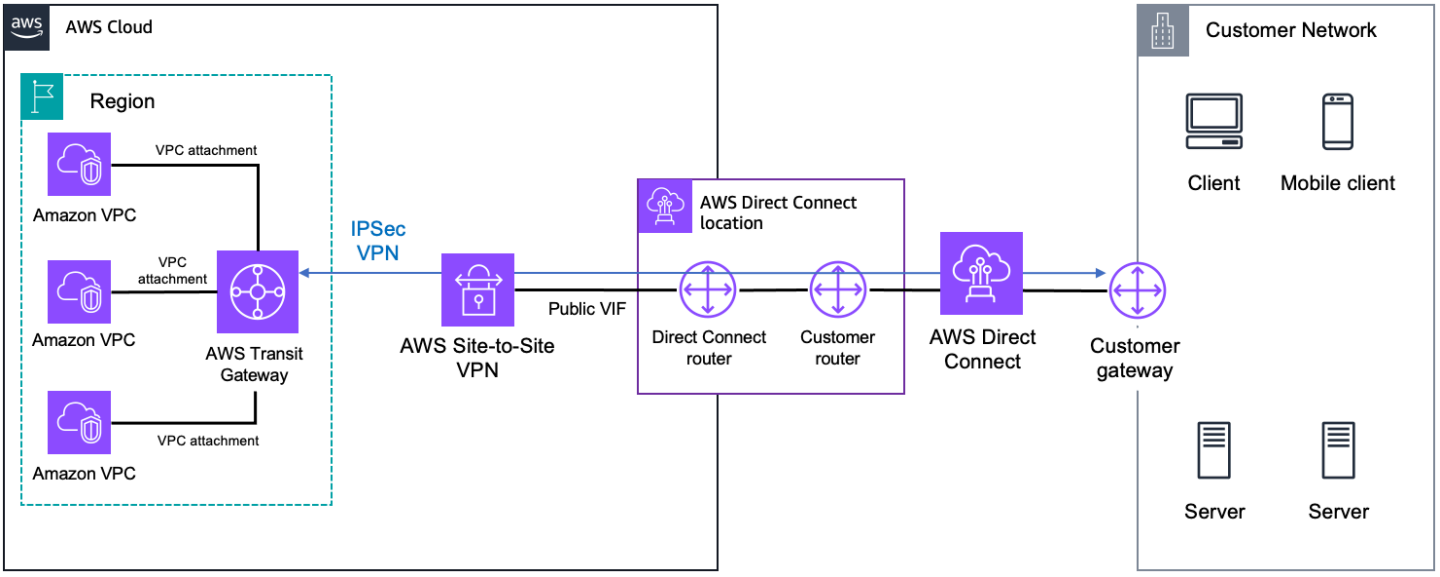
Weitere Ressourcen

- AWS Direct Connect
- AWS Direct Connect virtuelle Schnittstellen
- Site-to-SiteAWS-VPN-Benutzerhandbuch

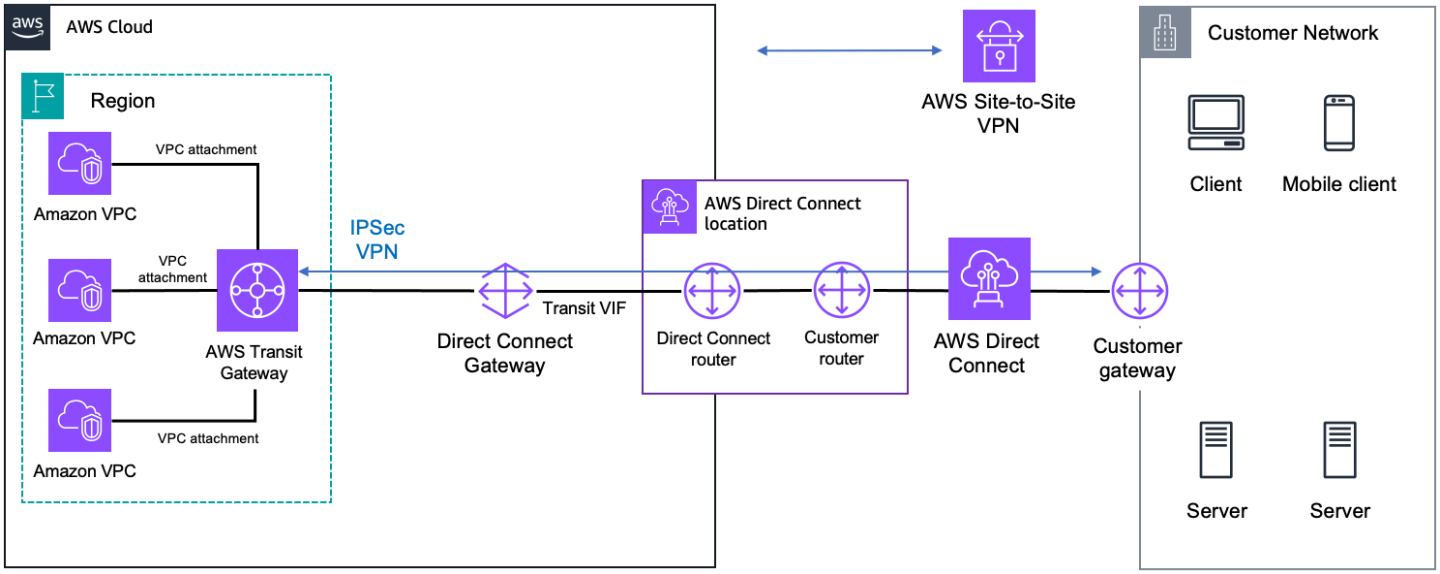
AWS Direct Connect + AWS Transit Gateway + Site-to-Site AWS-VPN

Mit AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN können Sie end-to-end IPsec -verschlüsselte Verbindungen zwischen Ihren Netzwerken und einem regionalen zentralen Router für Amazon VPCs über eine private, dedizierte Verbindung aktivieren.

Sie können AWS Direct Connect public verwenden VIFs , um zunächst eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS-Ressourcen wie Site-to-Site AWS-VPN-Endpunkten herzustellen. Sobald diese Verbindung hergestellt ist, können Sie eine IPsec Verbindung zu AWS Transit Gateway herstellen. Die folgende Abbildung veranschaulicht diese Option.



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



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

Ziehen Sie diesen Ansatz in Betracht, wenn Sie die Verwaltung vereinfachen und die Kosten für IPsec VPN-Verbindungen zu mehreren Amazon-Verbindungen VPCs in derselben Region minimieren möchten. Dabei profitieren Sie von der geringen Latenz und der konsistenten Netzwerkerfahrung, die eine private, dedizierte Verbindung gegenüber einem internetbasierten VPN bietet. Eine BGP-Sitzung zwischen AWS Direct Connect und Ihrem Router wird entweder über die öffentliche oder die Transit-VIF eingerichtet. Eine weitere BGP-Sitzung oder eine statische Route wird zwischen AWS Transit Gateway und Ihrem Router im VPN-Tunnel eingerichtet. IPsec

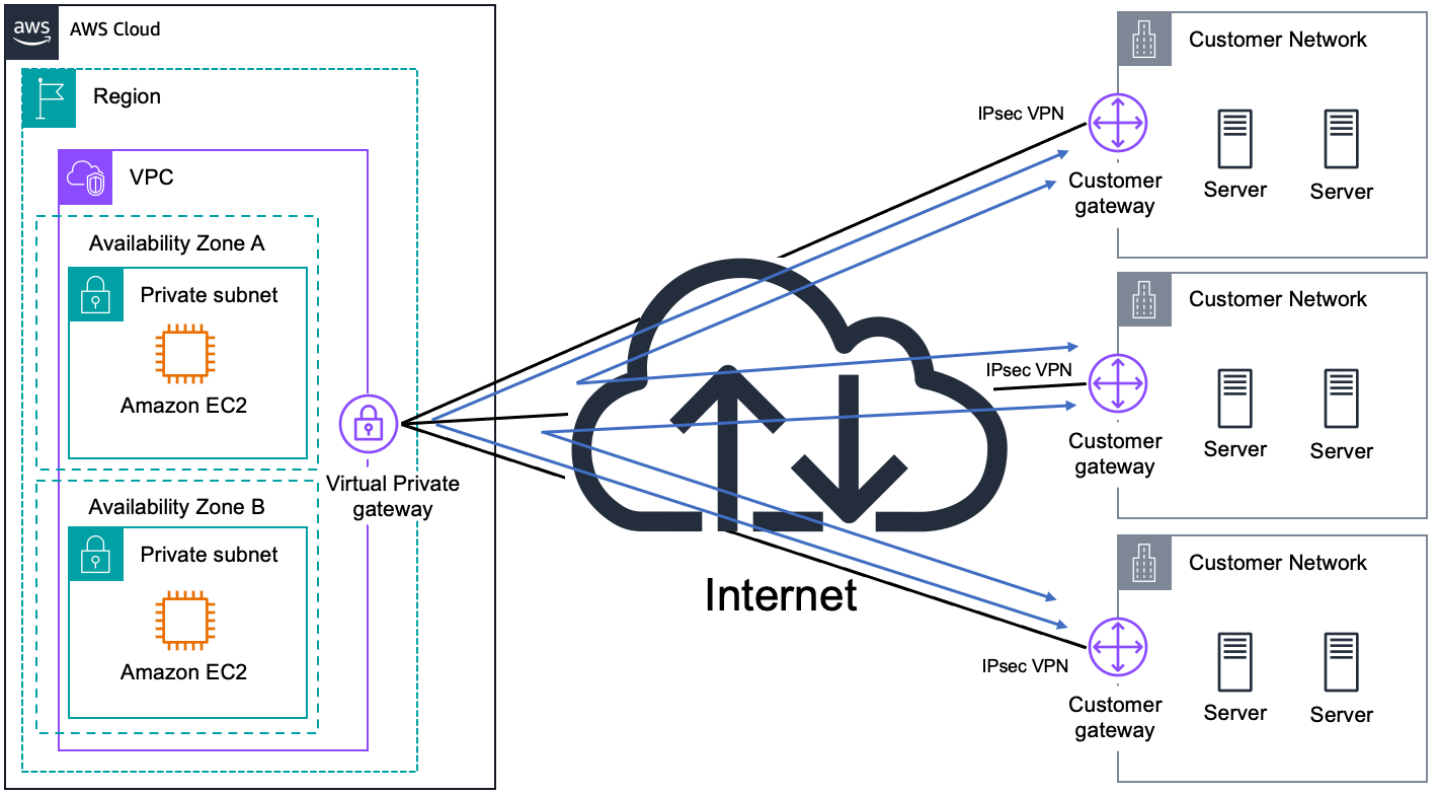
Weitere Ressourcen

- Virtuelle Schnittstellen von AWS Direct Connect
- VPN-Anhänge für das Transit-Gateway
- Anforderungen für Kunden-Gateway-Geräte
- Kunden-Gateway-Geräte, die mit Amazon VPC getestet wurden
- AWS Site-to-Site VPN — Privates IP-VPN mit AWS Direct Connect

Site-to-Site VPN CloudHub

Aufbauend auf den zuvor beschriebenen AWS-verwalteten VPN-Optionen können Sie mit dem sicher von einem Standort zum anderen kommunizieren Site-to-Site VPN CloudHub. Der Site-to-Site VPN CloudHub arbeitet mit einem einfachen hub-and-spoke Modell, das Sie mit oder ohne VPC verwenden können. Verwenden Sie diesen Ansatz, wenn Sie über mehrere Zweigstellen und bestehende Internetverbindungen verfügen und ein praktisches, potenziell kostengünstiges hub-and-spoke Modell für Primär- oder Backup-Konnektivität zwischen diesen Remote-Standorten implementieren möchten.

Die folgende Abbildung zeigt die Site-to-Site VPN CloudHub Architektur mit Linien, die darauf hinweisen, dass der Netzwerkverkehr zwischen Remote-Standorten über deren Site-to-Site VPN Verbindungen geleitet wird.



Site-to-Site VPN CloudHub

Site-to-Site VPN CloudHub verwendet ein virtuelles privates Amazon VPC-Gateway mit mehreren Kunden-Gateways, von denen jedes eindeutige autonome BGP-Systemnummern () verwendet. ASNs Die Remote-Standorte dürfen keine sich überschneidenden IP-Bereiche haben. Ihre Gateways kündigen die entsprechenden Routen (BGP-Präfixe) über ihre VPN-Verbindungen an. Diese Routing-Ankündigungen werden empfangen und für jeden BGP-Peer erneut angekündigt, sodass jede Site Daten an die anderen Standorte senden und Daten von diesen empfangen kann.

Weitere Ressourcen

- Bereitstellung einer sicheren Kommunikation zwischen Standorten mithilfe von VPN CloudHub
- Site-to-SiteAWS-VPN-Benutzerhandbuch
- Anforderungen für Kunden-Gateway-Geräte
- Kunden-Gateway-Geräte, die mit Amazon VPC getestet wurden

AWS Transit Gateway + SD-WAN-Lösungen

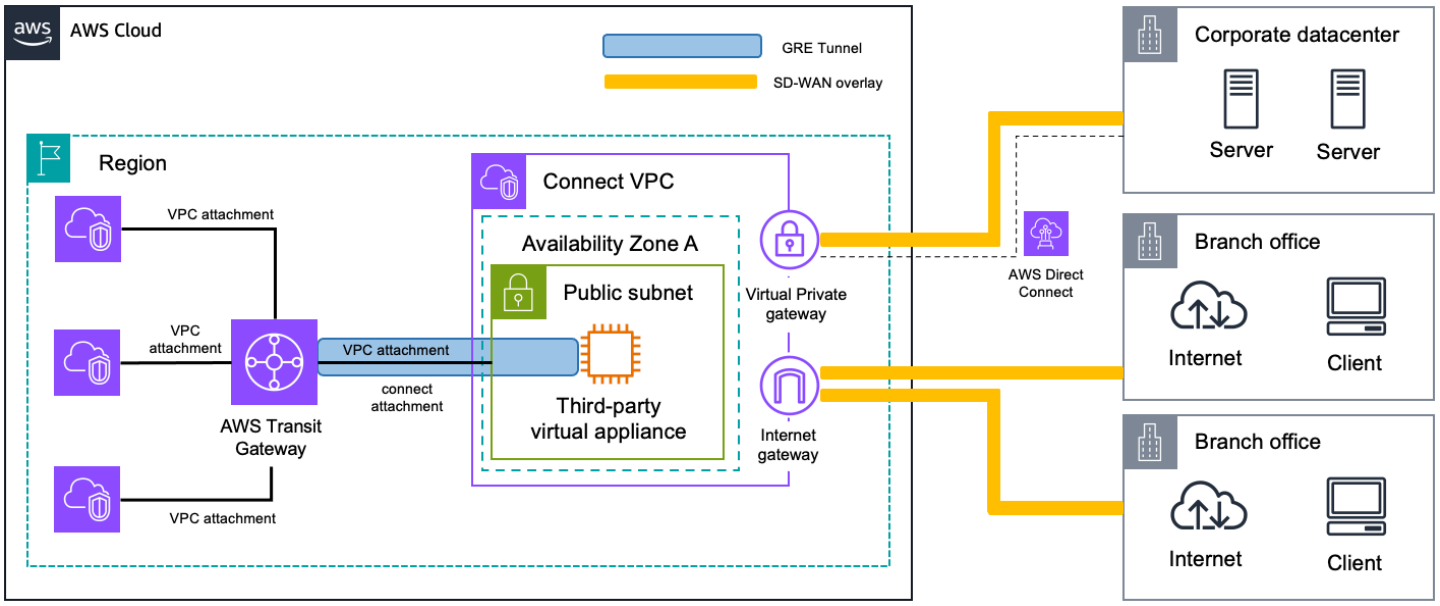
Software Defined Wide Area Networks (SD-WANs) werden verwendet, um Ihre Rechenzentren, Büros oder Colocation-Umgebungen über verschiedene Transitnetzwerke (wie das öffentliche Internet, MPLS-Netzwerke oder den AWS-Backbone mithilfe AWS Direct Connect) zu verbinden und den Datenverkehr automatisch und dynamisch über den geeignetsten und effizientesten Pfad zu verwalten, der auf Netzwerkbedingungen, Anwendungstyp oder QoS-Anforderungen (Quality of Service) basiert.

Verwenden Sie diesen Ansatz, wenn Sie über eine komplexe Netzwerktopologie mit mehreren Rechenzentren, Büros oder Colocation-Umgebungen verfügen, die untereinander und mit AWS kommunizieren müssen. SD-WAN-Lösungen können Ihnen helfen, diese Art von Netzwerk effizient zu verwalten.

Wenn es um die Verbindung eines SD-WAN-Netzwerks mit AWS geht, AWS Transit Gateway bietet es einen verwalteten, hochverfügbaren und skalierbaren regionalen Netzwerk-Transit-Hub für die Verbindung VPCs und Ihr SD-WAN-Netzwerk. Transit Gateway Connect-Anhänge bieten eine native Möglichkeit, Ihre SD-WAN-Infrastruktur und Appliances mit AWS zu verbinden. Dies macht es einfach, Ihr SD-WAN auf AWS zu erweitern, ohne es einrichten zu müssen. IPsec VPNs

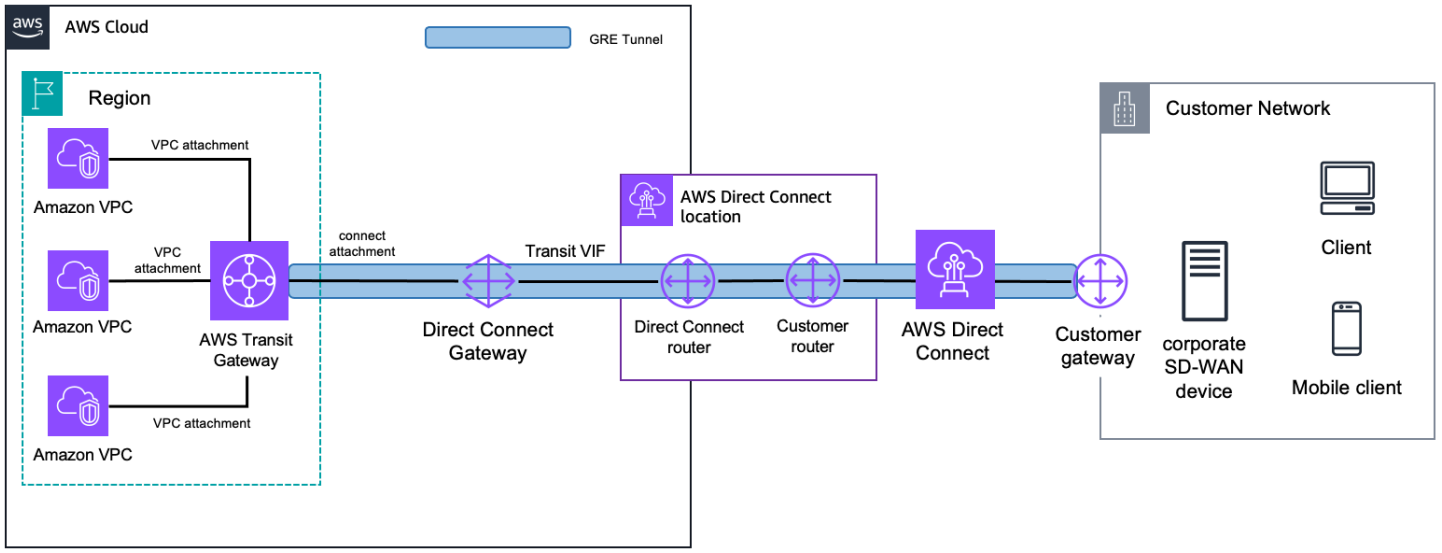
Transit Gateway Connect-Anhänge unterstützen Generic Routing Encapsulation (GRE) für eine höhere Bandbreitenleistung im Vergleich zu einer VPN-Verbindung. Es unterstützt das Border Gateway Protocol (BGP) für dynamisches Routing und macht die Konfiguration statischer Routen überflüssig. Dies vereinfacht das Netzwerkdesign und reduziert die damit verbundenen Betriebskosten. Darüber hinaus bietet die Integration mit Transit Gateway Network Manager erweiterte Transparenz durch globale Netzwerktopologie, Leistungskennzahlen auf Anbindungsebene und Telemetriedaten.

Bei der Integration Ihres SD-WAN-Netzwerks in Transit Gateway mithilfe von Verbindungsanhängen gibt es zwei gängige Muster. Die erste besteht darin, virtuelle Appliances des SD-WAN-Netzwerks in einer VPC innerhalb von AWS zu platzieren. Anschließend verwenden Sie einen VPC-Anhang als zugrunde liegenden Transport für den Transit Gateway Connect-Anhang zwischen den virtuellen Appliances und dem Transit Gateway, wie in der folgenden Abbildung dargestellt.



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

Alternativ können Sie Ihren SD-WAN-Verkehr auf AWS erweitern und segmentieren, ohne zusätzliche Infrastruktur hinzuzufügen. Sie können Transit Gateway Connect-Anlagen erstellen, indem Sie eine AWS Direct Connect Verbindung als zugrunde liegenden Transport verwenden, wie in der folgenden Abbildung dargestellt.



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

Bei der Verwendung von Transit Gateway Connect-Anhängen sind einige Überlegungen zu beachten:

- Sie können Connect-Anhänge auf vorhandenen Transit Gateways erstellen.

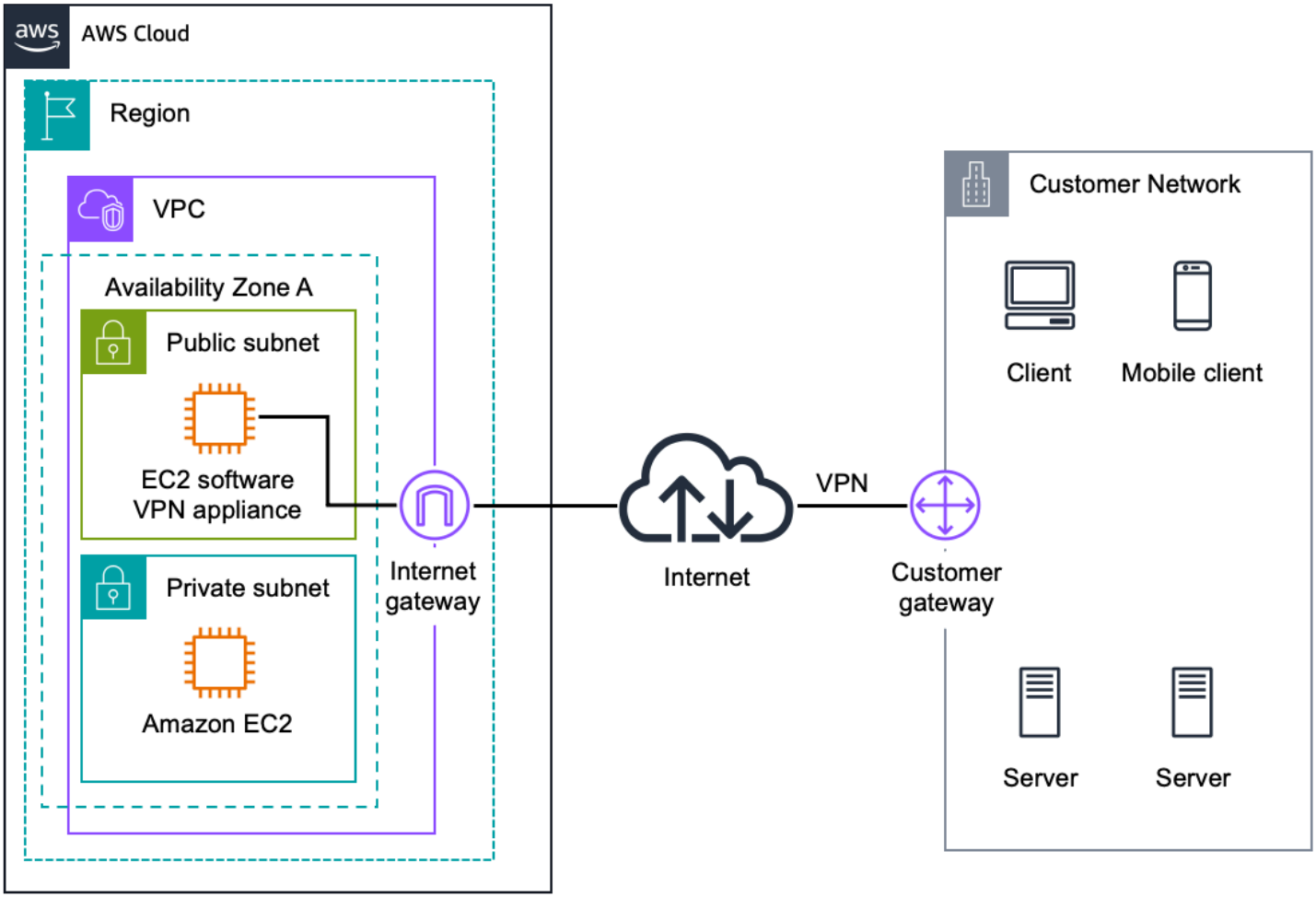
- Appliances von Drittanbietern müssen mit einem GRE-Tunnel konfiguriert sein, um Datenverkehr von Transit Gateway mithilfe von Connect-Anhängen senden und empfangen zu können. Die Appliance muss mit BGP für dynamische Routenaktualisierungen und Integritätsprüfungen konfiguriert sein.
- Connect-Anlagen unterstützen keine statischen Routen.
- Transit Gateway Connect-Anhänge unterstützen eine maximale Bandbreite von fünf Gbit/s pro GRE-Tunnel. Eine Bandbreite von über fünf Gbit/s kann erreicht werden, indem dieselben Präfixe über mehrere Connect-Peer (GRE-Tunnel) für denselben Connect-Anhang verteilt werden.
- Für jeden Connect-Anhang werden maximal vier Connect-Peers unterstützt.
- Unterstützung von Transit Gateway Connect-Anhängen IPv6 und dynamische Routenankündigungen über Multiprotokollerweiterungen für BGP (MBGP oder MP-BGP).

Weitere Ressourcen

- Peering-Anlagen am Transit Gateway
- Anforderungen und Überlegungen
- Blogbeitrag: Vereinfachen Sie die SD-WAN-Konnektivität mit AWS Transit Gateway Connect

Software-VPN

Amazon VPC bietet Ihnen die Flexibilität, beide Seiten Ihrer Amazon VPC-Konnektivität vollständig zu verwalten, indem Sie eine VPN-Verbindung zwischen Ihrem Remote-Netzwerk und einer Software-VPN-Appliance herstellen, die in Ihrem Amazon VPC-Netzwerk läuft. Diese Option wird empfohlen, wenn Sie beide Enden der VPN-Verbindung verwalten müssen, entweder aus Compliance-Gründen oder zur Nutzung von Gateway-Geräten, die derzeit nicht von der VPN-Lösung von Amazon VPC unterstützt werden. Die folgende Abbildung zeigt diese Option.



Site-to-SiteSoftware-VPN

Sie können aus einem Ökosystem mehrerer Partner und Open-Source-Communities wählen, die Software-VPN-Appliances entwickelt haben, die auf Amazon EC2 laufen. Mit dieser Wahl geht die Verantwortung einher, dass Sie die Software-Appliance verwalten müssen, einschließlich Konfiguration, Patches und Upgrades.

Beachten Sie, dass dieses Design einen potenziellen Single Point of Failure in das Netzwerkdesign einführt, da die Software-VPN-Appliance auf einer einzigen EC2 Amazon-Instance ausgeführt wird. Weitere Informationen finden Sie unter Anhang A: Hochrangige HA-Architektur für Software-VPN-Instanzen Architektur für Software-VPN-Instances.

Weitere Ressourcen

- VPN-Appliances sind verfügbar in AWS Marketplace
- Technischer Überblick — Cisco ASA mit EC2 VPC-Instance verbinden () IPsec

- Technischer Überblick — Mehrere EC2 Instanzen VPCs miteinander verbinden () IPsec
- Technischer Überblick — Mehrere VPCs mit EC2 Instanzen verbinden (SSL)

Amazon VPC-to-Amazon VPC-Verbindungsoptionen

Verwenden Sie diese Entwurfsmuster, wenn Sie mehrere Amazon VPCs in ein größeres virtuelles Netzwerk integrieren möchten. Dies ist nützlich, wenn Sie VPCs aufgrund von Sicherheit, Abrechnung, Präsenz in mehreren Regionen oder internen Rückbuchungsanforderungen mehrere benötigen, um AWS-Ressourcen einfacher zwischen Amazon zu integrieren. VPCs Sie können diese Muster auch mit den Netzwerk—zu-Amazon-VPC-Konnektivitätsoptionen kombinieren, um ein Unternehmensnetzwerk zu erstellen, das sich über mehrere Remote-Netzwerke erstreckt. VPCs

VPC-Konnektivität zwischen beiden VPCs wird am besten erreicht, wenn für jede verbundene VPC IP-Bereiche verwendet werden, die sich nicht überschneiden. Wenn Sie beispielsweise mehrere Verbindungen herstellen möchten, stellen Sie sicher VPCs, dass jede VPC mit eindeutigen CIDR-Bereichen (Classless Inter-Domain Routing) konfiguriert ist. Daher empfehlen wir Ihnen, einen einzelnen, zusammenhängenden, sich nicht überlappenden CIDR-Block zuzuweisen, der von jeder VPC verwendet werden soll. Weitere Informationen zu Amazon VPC-Routing und Einschränkungen finden Sie in den häufig gestellten Fragen zu Amazon VPC.

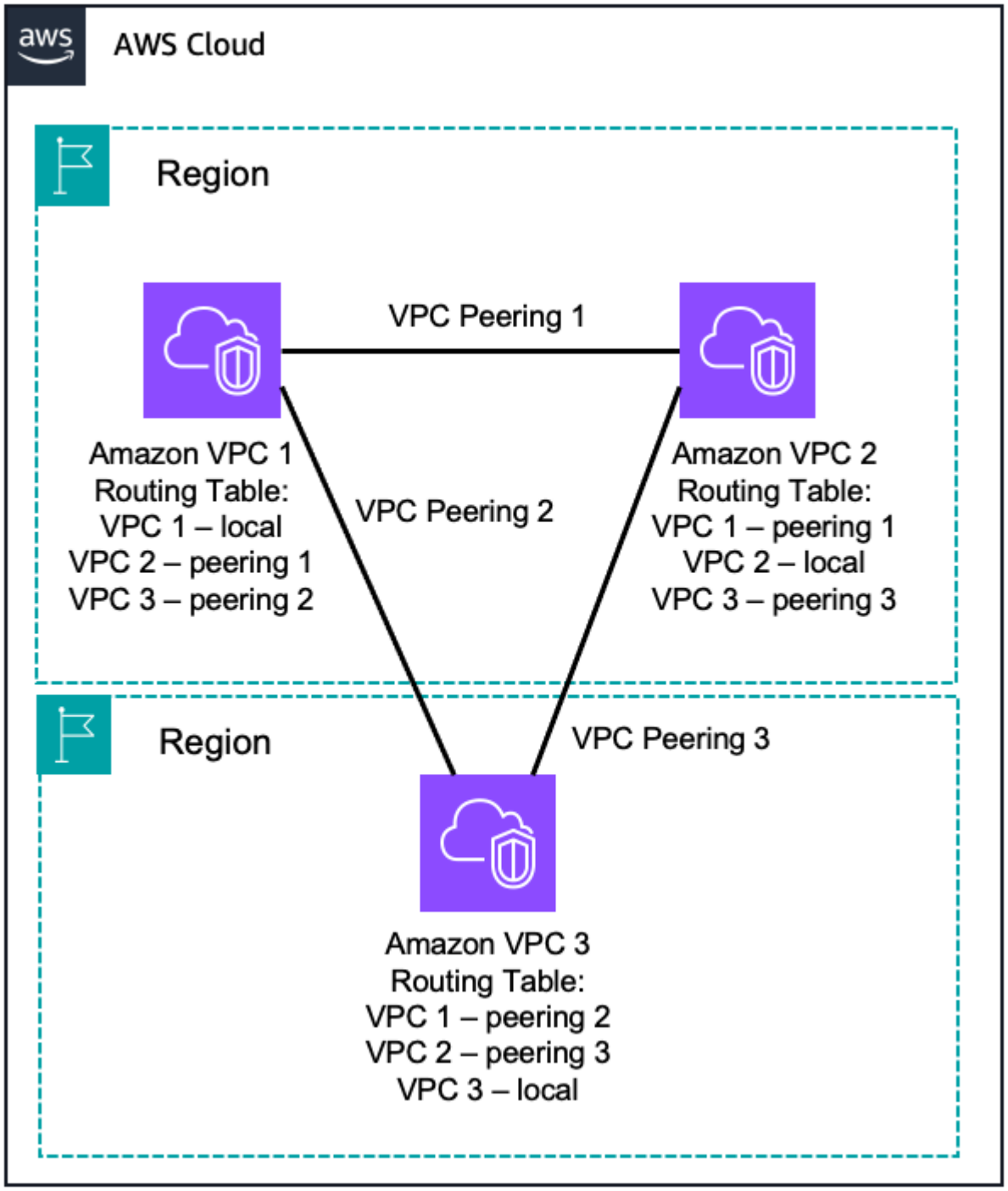
Option	Anwendungsfall	Vorteile	Einschränkungen
VPC-Peering	Von AWS bereitges tellte Netzwerkk onnektivität zwischen zwei. VPCs	Nutzt die von AWS verwaltete skalierbare Netzwerkinfrastruktur	VPC-Peering unterstützt keine transitiven Peering-B eziehungen Es ist schwierig, sie in großem Umfang zu verwalten
AWS Transit Gateway	Von AWS bereitges tellte regionale Router-Konnektivität für VPCs	Von AWS verwalteter Hochverfügbarkeits- und Skalierbarkeitsser vice Regionaler Netzwerk-Hub für bis zu 5.000 Anlagen	Transit Gateway Gateway-Peering unterstützt nur statische Routen

Option	Anwendungsfall	Vorteile	Einschränkungen
AWS PrivateLink	Von AWS bereitgestellte Netzwerkkonnektivität zwischen zwei VPCs mithilfe von Schnittstellenendpunkten	Nutzt die von AWS verwaltete skalierbare Netzwerkinfrastruktur	VPC-Endpunktservices sind nur in der AWS-Region verfügbar, in der sie erstellt wurden
Software-VPN	Auf Software-Appliances basierende VPN-Verbindungen zwischen VPCs	Unterstützt eine Vielzahl von VPN-Anbietern, -Produkten und -Protokollen Wird vollständig von Ihnen verwaltet	Sie sind verantwortlich für die Implementierung von HA-Lösungen für alle VPN-Endpunkte (falls erforderlich) VPN-Instanzen könnten zu einem Netzwerkengpass werden
VPN-to-AWS Site-to-SiteSoftware-VPN	Verbindung zwischen Software-Appliance und VPN VPCs	Von AWS verwaltete VPC-VPN-Verbindung mit hoher Verfügbarkeit Unterstützt eine Vielzahl von VPN-Anbietern und -Produkten, die von Ihnen verwaltet werden Unterstützt statische Routen und dynamische BGP-Peering- und Routing-Richtlinien	Sie sind verantwortlich für die Implementierung von HA-Lösungen für die VPN-Endpunkte der Software-Appliance (falls erforderlich) VPN-Instanzen könnten zu einem Netzwerkengpass werden IPsec VPN-Protokoll nur für AWS Managed VPN

VPC-Peering

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs , die das Routing unter Verwendung der privaten IP-Adressen jeder VPC ermöglicht, als ob sie sich im selben Netzwerk befinden würden. VPC-Peering-Verbindungen können zwischen Ihren eigenen VPCs oder mit einer VPC in einem anderen AWS-Konto hergestellt werden. VPC-Peering unterstützt auch regionsübergreifendes Peering.

Datenverkehr, der regionsübergreifendes VPC-Peering verwendet, verbleibt immer auf dem globalen AWS-Backbone und durchquert niemals das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und S-Angriffe reduziert werden. DDo



VPC-to-VPC Peering

AWS verwendet die bestehende Infrastruktur einer VPC, um VPC-Peering-Verbindungen herzustellen, und ist nicht auf separate physische Hardware angewiesen. Daher führen sie nicht zu einer potenziellen Ausfallstelle oder zu einem Engpass bei der Netzwerkbandbreite dazwischen. VPCs Darüber hinaus können VPC-Routingtabellen, Sicherheitsgruppen und

Netzwerkzugriffskontrolllisten genutzt werden, um zu kontrollieren, welche Subnetze oder Instances die VPC-Peering-Verbindung nutzen können.

Amazon unterstützt VPCs kein transitives Peering, was bedeutet, dass Sie zwei, die nicht direkt miteinander verbunden sind VPCs , nicht über eine dritte VPC als Transit kommunizieren können. Wenn Sie möchten, dass alle über VPC-Peering miteinander kommunizieren, müssen Sie 1:1 -VPC-Peering-Verbindungen zwischen jedem von ihnen herstellen. VPCs Alternativ können Sie unser AWS Transit Gateway AWS Cloud WAN als Netzwerk-Transit-Hub verwenden.

IPv4 Sowohl der Verkehr als auch der IPv6 Verkehr werden in VPC-Peering-Verbindungen unterstützt. Zwei VPCs können jedoch nicht miteinander verbunden werden, wenn sich ihr primärer IPv4 CIDR-Block überschneidet, unabhängig von den verwendeten sekundären IPv4 oder CIDR-Blöcken. IPv6 Berücksichtigen Sie dies bei der Zuweisung des primären CIDR-Blocks zu Ihrem, VPCs wenn Sie VPC-Peering zwischen ihnen verwenden möchten.

Weitere Ressourcen

- Amazon VPC-Peering
- Was ist VPC-Peering?

AWS Transit Gateway

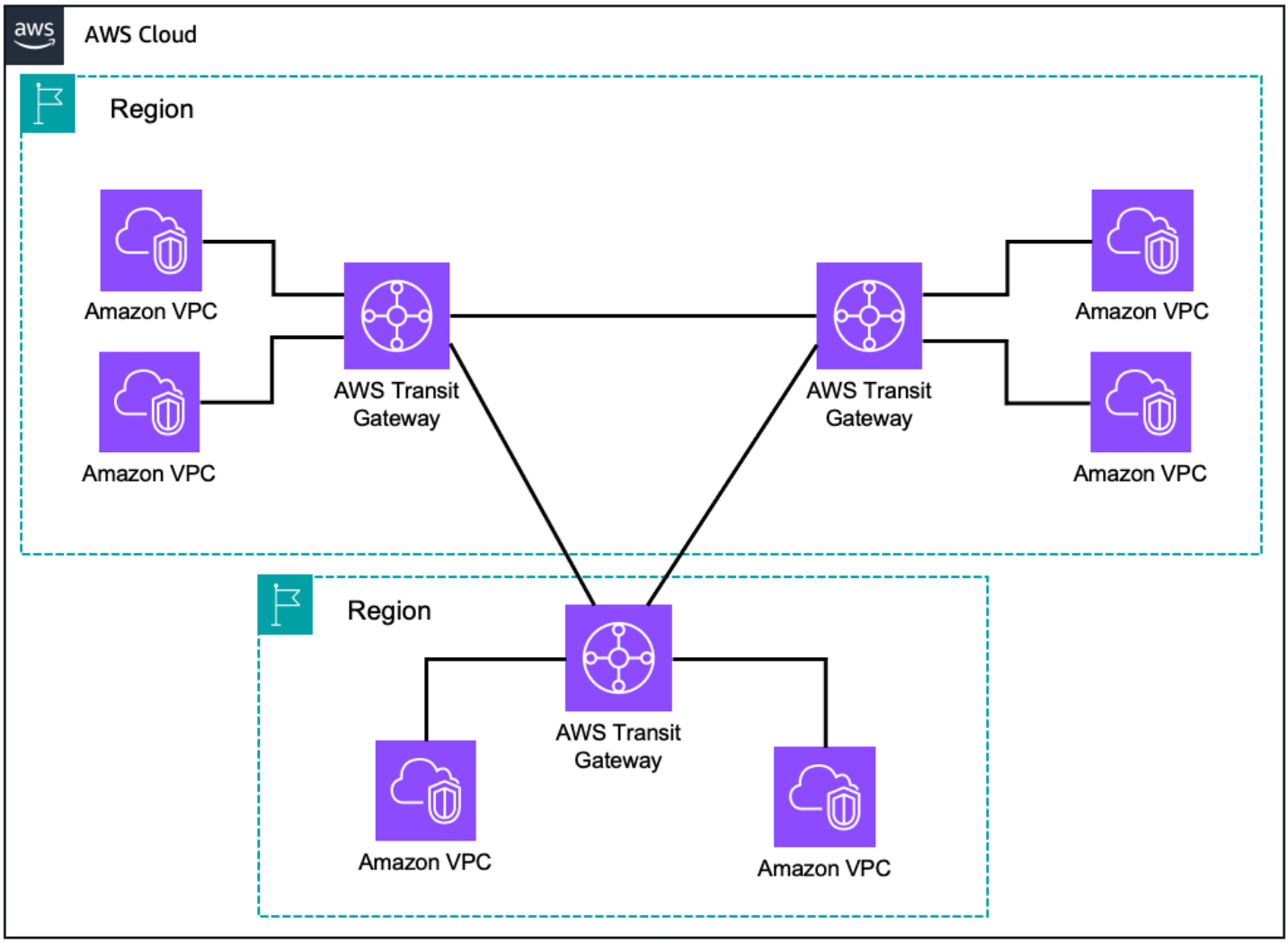
AWS Transit Gateway ist ein hochverfügbarer und skalierbarer Service zur Konsolidierung der AWS-VPC-Routing-Konfiguration für eine Region mit einer hub-and-spoke Architektur. Jede Spoke-VPC muss sich nur mit dem Transit Gateway verbinden, um Zugriff auf andere verbundene VPCs VPCs zu erhalten. Beides IPv4 und der IPv6 Verkehr wird unterstützt in AWS Transit Gateway.

Sie können mehrere Transit Gateway Gateway-Routentabellen, Zuordnungen und Propagationen nutzen, um Ihren Verkehr innerhalb desselben Transit Gateway zu segmentieren. Sie können verschiedene Routingdomänen (z. B. produktiven und nicht produktiven Verkehr) von einem zentralen Verwaltungspunkt aus verwalten und so sicherstellen, dass diese Routingdomänen nicht miteinander kommunizieren können.

Sie können auch die von Transit Gateway geschaffene hub-and-spoke Architektur nutzen, um den Zugriff auf gemeinsam genutzte Dienste wie Verkehrsinspektion, VPC-Schnittstellen-Endpunktzugriff oder ausgehenden Verkehr über ein NAT-Gateway oder NAT-Instances zu zentralisieren. Diese Zentralisierung vereinfacht die Komplexität der Verwaltung dieser Ressourcen in mehreren VPCs Bereichen und ermöglicht eine bessere Kontrolle, wenn Sie Ihre Präsenz in AWS erweitern.

Transit Gateways können innerhalb derselben AWS-Region oder zwischen verschiedenen AWS-Regionen miteinander verbunden werden. AWS Transit Gateway Der Datenverkehr bleibt immer auf dem globalen AWS-Backbone und durchquert niemals das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und DDo S-Angriffe reduziert werden.

Mit einer großen Anzahl von VPCs bietet Transit Gateway ein einfacheres VPC-to-VPC Kommunikationsmanagement über VPC Peering, wie in der folgenden Abbildung dargestellt.



AWS Transit Gateway

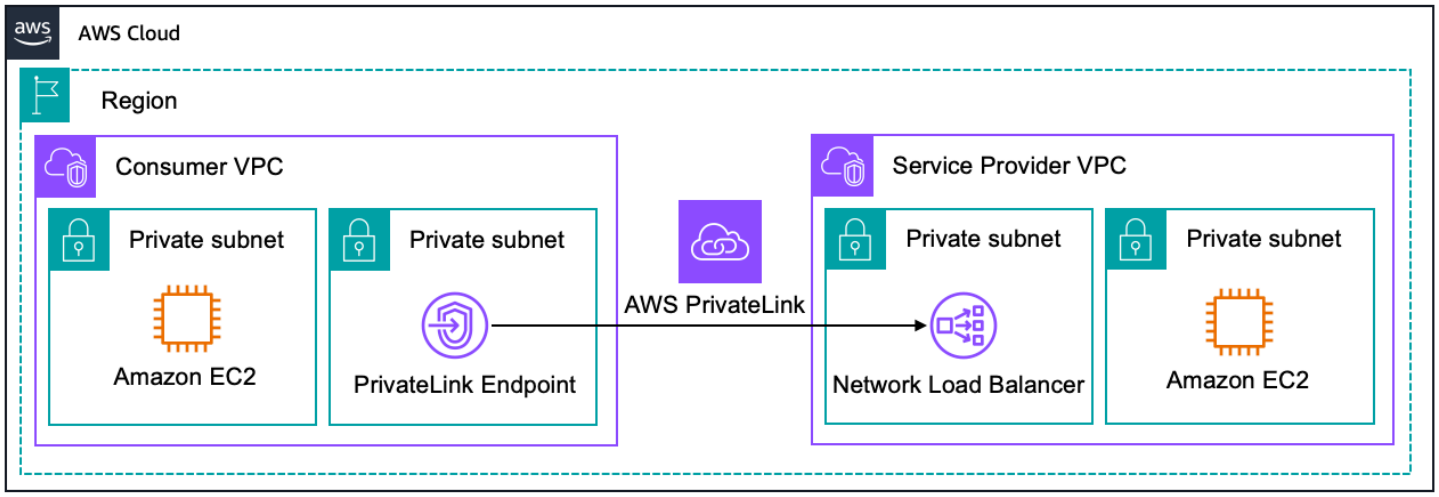
Um einen zentralen Überblick über den IP-Verkehr zu und von Ihren Transit Gateways zu erhalten, können Sie Transit Gateway Flow Logs in Amazon CloudWatch Logs und Amazon S3 veröffentlichen. Flow-Potokolldaten werden außerhalb des Pfades des Netzwerkdatenverkehrs erfasst und wirken sich daher nicht auf den Netzwerkdurchsatz oder die Latenz aus.

Weitere Ressourcen

- Amazon VPC Transit-Gateway
- Peering-Anlagen am Transit-Gateway
- Arbeiten Sie mit Transit Gateways
- Protokollierung des Netzwerkverkehrs mithilfe von Transit Gateway Flow Logs

AWS PrivateLink

AWS PrivateLink ermöglicht es Ihnen, über private IP-Adressen in Ihrer VPC eine Verbindung zu einigen AWS-Services, Services, die von anderen AWS-Konten gehostet werden (als Endpoint Services bezeichnet), und unterstützten AWS Marketplace Partnerservices herzustellen. Die Schnittstellenendpunkte werden direkt in Ihrer VPC mithilfe elastischer Netzwerkschnittstellen und IP-Adressen in den Subnetzen Ihrer VPC erstellt. Das bedeutet, dass VPC-Sicherheitsgruppen verwendet werden können, um den Zugriff auf die Endpoints zu verwalten.



AWS PrivateLink

Wir empfehlen diesen Ansatz, wenn Sie Dienste, die von einer anderen VPC angeboten werden, sicher innerhalb eines AWS-Netzwerks unter Verwendung privater IP-Adressen nutzen möchten. Alternativ AWS PrivateLink ist dies eine gute Lösung, wenn VPCs sich die IP-Adressen überschneiden.

AWS PrivateLink unterstützt vollständig IPv6, aber beide Ziele, VPC-Subnetze VPCs, der Network Load Balancer und die DNS-Namen müssen aktiviert oder geändert werden, um Dual-

Stack verwenden zu können. Sobald diese Voraussetzungen erfüllt sind, IPv6 kann sie in der Dienstkonfiguration für den Endpunkt aktiviert werden.

Zugriffskontrollen für AWS PrivateLink

Die Schnittstellenendpunkte werden direkt in Ihrer VPC mithilfe elastischer Netzwerkschnittstellen und IP-Adressen in den Subnetzen Ihrer VPC erstellt. Das bedeutet, dass VPC-Sicherheitsgruppen verwendet werden können, um den Netzwerkzugriff auf die Endpunkte zu verwalten.

Wenn Sie einen Schnittstellenendpunkt oder einen Gateway-Endpunkt erstellen, können Sie auch eine Endpunktrichtlinie anhängen. Die Endpunktrichtlinie steuert, welche AWS-Prinzipale (AWS-Konten, IAM-Benutzer und Rollen) den VPC-Endpunkt für den Zugriff auf den Endpunktservice verwenden können.

Sie können einem Endpunkt mehr als eine Richtlinie anfügen. Sie können jedoch jederzeit eine Endpunktrichtlinie ändern.

Eine Endpunktrichtlinie überschreibt oder ersetzt weder IAM-Benutzerrichtlinien noch dienstspezifische Richtlinien (wie Amazon S3 S3-Bucket-Richtlinien). Wenn Sie einen Schnittstellenendpunkt verwenden, um eine Verbindung zu Amazon S3 herzustellen, können Sie auch Amazon S3 S3-Bucket-Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten oder bestimmten zu kontrollieren. VPCs

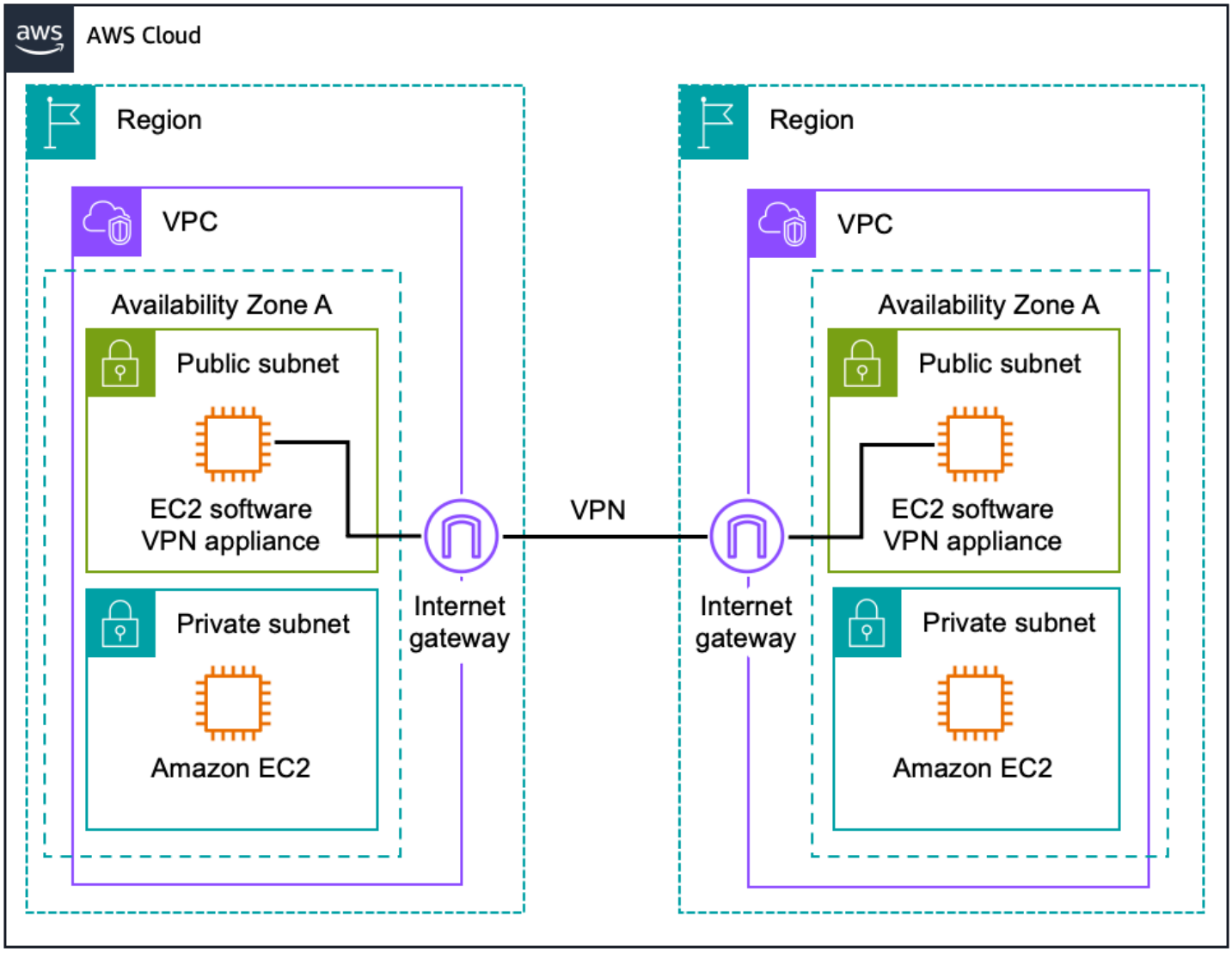
Weitere Ressourcen

- Schnittstelle VPC-Endpunkte ()AWS PrivateLink
- VPC-Endpunktdienste ()AWS PrivateLink
- Blogbeitrag: Beschleunigen Sie Ihre IPv6 Einführung mit PrivateLink Diensten und Endpunkten
- Blogbeitrag: Netzwerke mit überlappenden IP-Bereichen verbinden
- AWS PrivateLink Partner

Software-VPN

Amazon VPC bietet Flexibilität beim Netzwerk-Routing. Dazu gehört die Möglichkeit, sichere VPN-Tunnel zwischen zwei oder mehr Software-VPN-Appliances zu erstellen, um VPCs mehrere Geräte

mit einem größeren virtuellen privaten Netzwerk zu verbinden, sodass Instanzen in jeder VPC über private IP-Adressen nahtlos miteinander verbunden werden können. Diese Option wird empfohlen, wenn Sie beide Enden der VPN-Verbindung mit Ihrem bevorzugten VPN-Softwareanbieter verwalten möchten. Diese Option verwendet ein Internet-Gateway, das an jede VPC angeschlossen ist, um die Kommunikation zwischen den Software-VPN-Appliances zu erleichtern.



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

Sie können aus einem Ökosystem mehrerer Partner und Open-Source-Communities wählen, die Software-VPN-Appliances entwickelt haben, die auf Amazon laufen EC2. Mit dieser Wahl geht die Verantwortung für Sie einher, die Software-Appliance einschließlich Konfiguration, Patches und Upgrades zu verwalten.

Beachten Sie, dass dieses Design einen potenziellen Single Point of Failure in das Netzwerkdesign einführt, da die Software-VPN-Appliance auf einer einzigen EC2 Amazon-Instance ausgeführt wird.

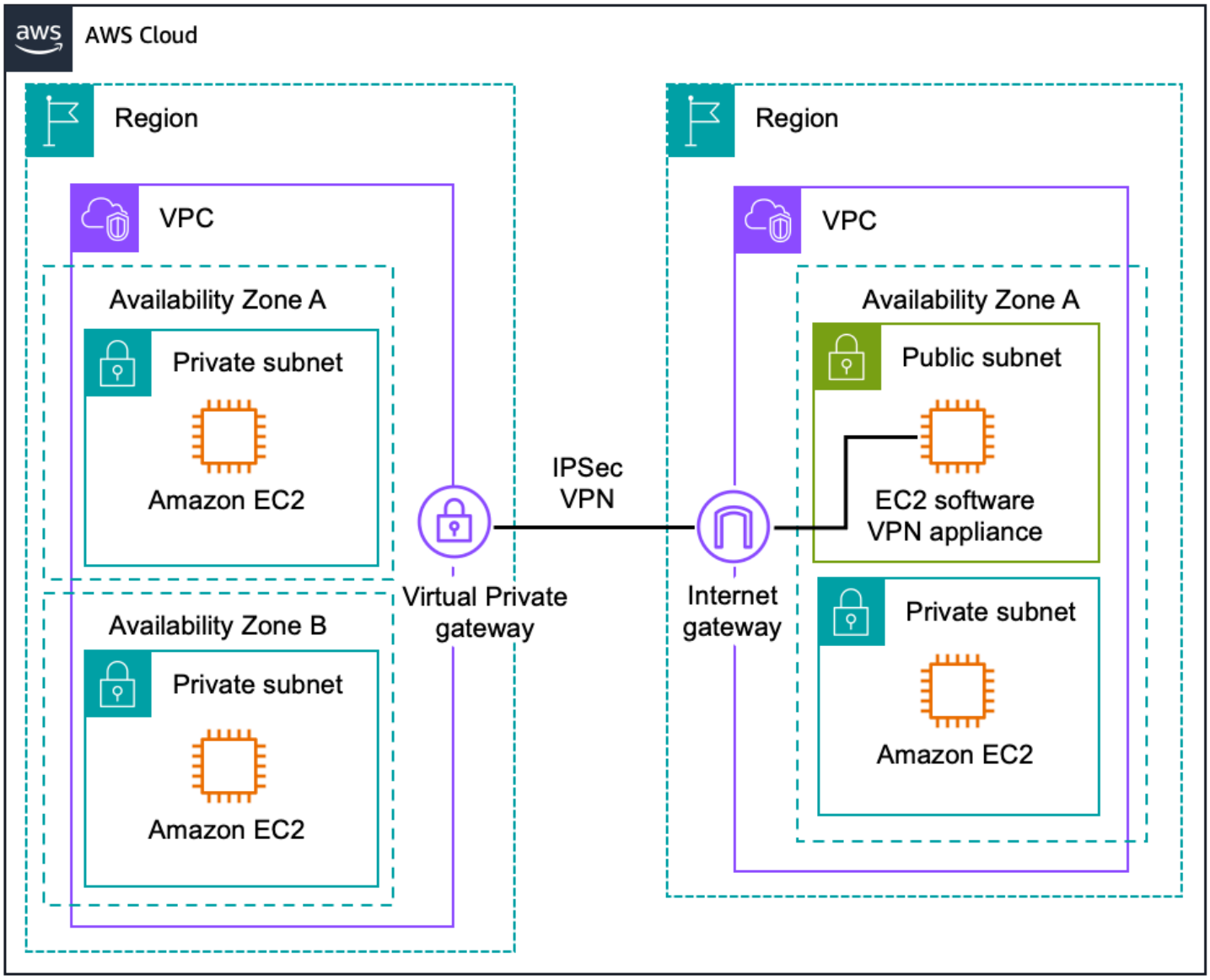
Weitere Informationen finden Sie unter Anhang A: Hochrangige HA-Architektur für Software-VPN-Instanzen.

Weitere Ressourcen

- VPN-Appliances sind erhältlich bei AWS Marketplace
- Technischer Überblick — Mehrere EC2 Instanzen VPCs miteinander verbinden (IPsec)
- Technischer Überblick — Mehrere VPCs mit EC2 Instanzen verbinden (SSL)

VPN-to-AWS Site-to-SiteSoftware-VPN

Amazon VPC bietet die Flexibilität, die von AWS verwalteten VPN- und Software-VPN-Optionen zu kombinieren, um mehrere VPCs zu verbinden. Mit diesem Design können Sie sichere VPN-Tunnel zwischen einer Software-VPN-Appliance und einem virtuellen privaten Gateway einrichten, sodass sich Instanzen in jeder VPC über private IP-Adressen nahtlos miteinander verbinden können. Diese Option verwendet ein virtuelles privates Gateway in einer Amazon VPC und eine Kombination aus einem Internet-Gateway und einer Software-VPN-Appliance in einer anderen Amazon VPC, wie in der folgenden Abbildung dargestellt.



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

Beachten Sie, dass durch dieses Design ein potenzieller einziger Fehlerpunkt in das Netzwerkdesign eingeführt wird. Weitere Informationen finden Sie unter Anhang A: Hochrangige HA-Architektur für Software-VPN-Instanzen.

Weitere Ressourcen

- VPN-Appliances sind erhältlich bei AWS Marketplace
- Site-to-SiteAWS-VPN-Benutzerhandbuch
- Anforderungen für Kunden-Gateway-Geräte

Optionen für access-to-Amazon Software-Remote-VPC-Konnektivität

Mit Software-Fernzugriffs-VPN können Sie kostengünstige, elastische und sichere Services nutzen, um Fernzugriffslösungen zu implementieren und gleichzeitig eine nahtlose Verbindung zu AWS-gehosteten Ressourcen herzustellen. Diese Option wird in der Regel von kleineren Unternehmen mit weniger ausgedehnten Remote-Netzwerken bevorzugt oder die noch keine Fernzugriffslösungen für ihre Mitarbeiter entwickelt und bereitgestellt haben.

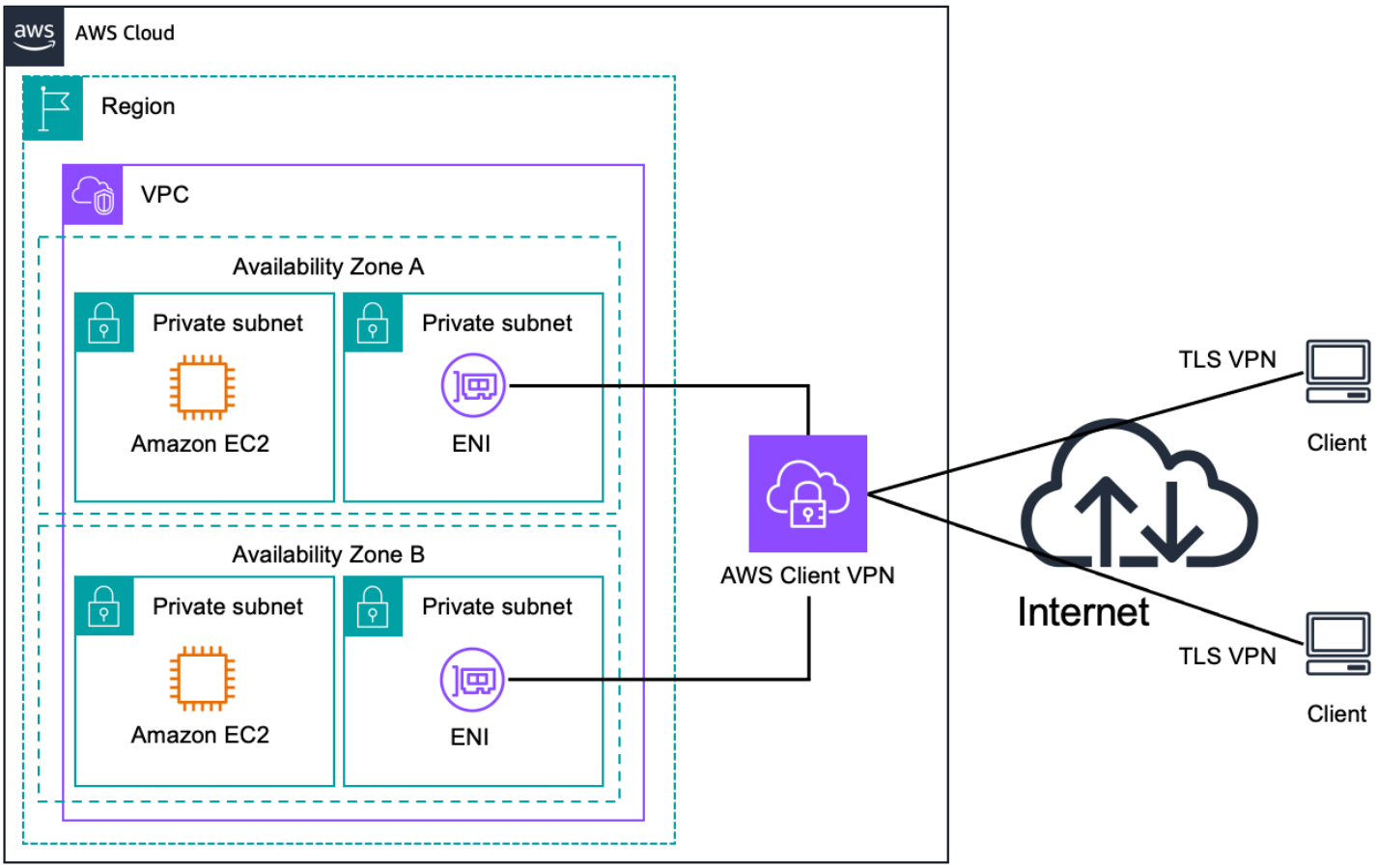
Sie können diese Muster mit den Network-to-Amazon VPC-Konnektivitätsoptionen Konnektivitätsoptionen kombinieren und Amazon VPC-to-Amazon VPC-Verbindungsoptionen so ein Netzwerk erstellen, das sich über mehrere VPCs Remote-Netzwerke erstreckt.

In der folgenden Tabelle werden die Vor- und Nachteile dieser Optionen beschrieben.

Option	Anwendungsfall	Vorteile	Einschränkungen
AWS Client VPN	Von AWS verwaltete Fernzugriffslösung für Amazon VPC und/oder interne Netzwerke	Von AWS verwalteter Hochverfügbarkeits- und Skalierbarkeitsservice	Nur OpenVPN-Clients
Software-Client-VPN	Software-VPN-Appliance-Fernzugriffslösung für and/or interne Amazon VPC-Netzwerke	Unterstützt eine breitere Palette von VPN-Anbietern, -Produkten und -Protokollen Vollständig vom Kunden verwaltete Lösung	Sie sind für die Implementierung von HA-Lösungen verantwortlich

AWS Client VPN

AWS Client VPN ist ein von AWS verwalteter Hochverfügbarkeits- und Skalierbarkeitsservice, der einen sicheren Software-Fernzugriff ermöglicht. Es bietet die Möglichkeit, eine sichere TLS-Verbindung zwischen Remote-Clients und Ihrem Amazon herzustellen VPCs, um sicher über das Internet auf AWS-Ressourcen und lokale Ressourcen zuzugreifen, wie in der folgenden Abbildung dargestellt.



AWS Client VPN Remote Access

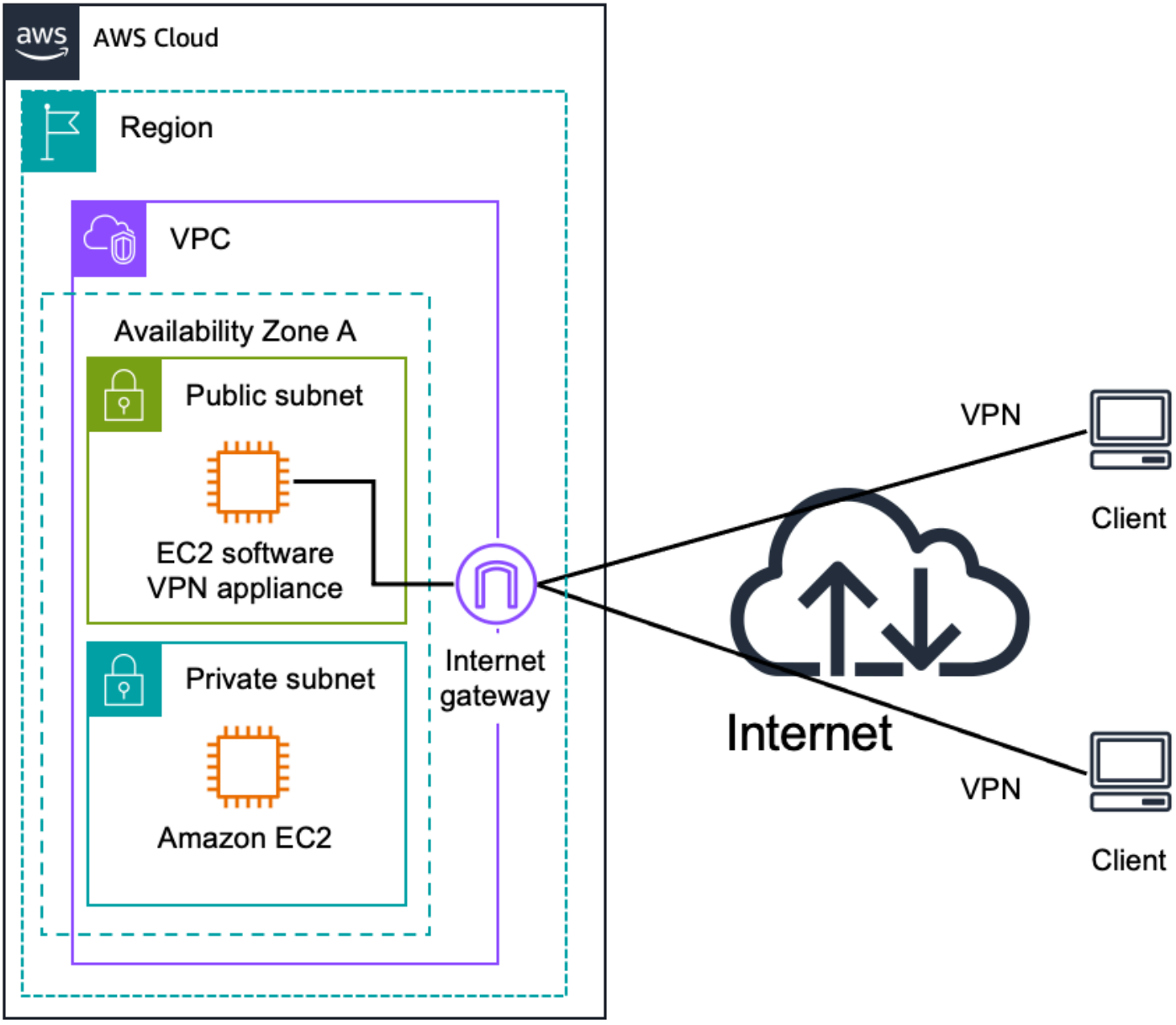
Bei den Remote-Clients kann es sich um den AWS-Client VPN für Desktop oder um OpenVPN-VPN-Clients von Drittanbietern handeln, wobei die Authentifizierung entweder über Active Directory oder durch gegenseitige Zertifikatsauthentifizierung erfolgt.

Weitere Ressourcen

- AWS-Client-VPN-Administratorhandbuch

Software-Client-VPN

Sie können aus einem Ökosystem mehrerer Partner und Open-Source-Communities wählen, die Fernzugriffslösungen entwickelt haben, die auf Amazon EC2 laufen. Diese Lösungen bieten große Flexibilität bei der Verwendung des Sicherheitsprotokolls für den Fernzugriff auf Ihr Amazon VPCs, für den sicheren Zugriff auf AWS-Ressourcen und lokale Ressourcen über das Internet, wie in der folgenden Abbildung dargestellt.



Software Client VPN Remote Access

Fernzugriffslösungen sind unterschiedlich komplex, unterstützen mehrere Client-Authentifizierungsoptionen (einschließlich Multifaktor-Authentifizierung) und können entweder in

Amazon VPC oder in remote gehostete Identitäts- und Zugriffsverwaltungslösungen (unter Nutzung einer der network-to-Amazon VPC-Optionen) wie Microsoft Active Directory oder andere LDAP/Multifaktor-Authentifizierungslösungen integriert werden.

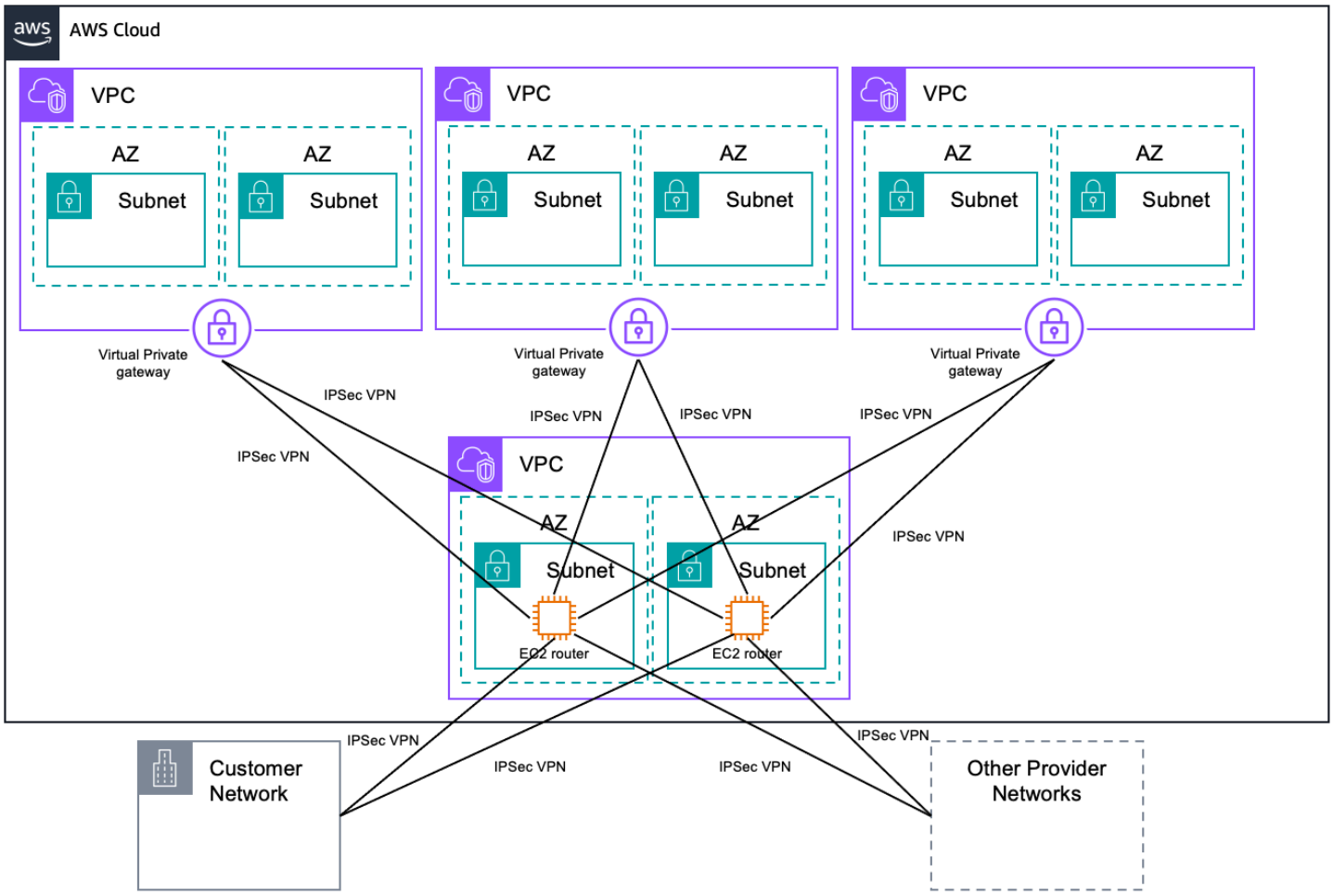
Sie sind verantwortlich für die Verwaltung der Fernzugriffssoftware, einschließlich Benutzerverwaltung, Konfiguration, Patches und Upgrades. Dieses Design führt eine potenzielle Schwachstelle in das Netzwerkdesign ein, da der RAS-Server auf einer einzigen Amazon EC2 EC2-Instance ausgeführt wird. Weitere Informationen finden Sie unter Anhang A: Hochrangige HA-Architektur für Software-VPN-Instanzen.

Weitere Ressourcen

- VPN-Appliances sind erhältlich bei AWS Marketplace
- Schnellstartanleitung für OpenVPN Access Server

Transit-VPC

Aufbauend auf den oben genannten Software-VPN-Designs können Sie ein globales Transitnetzwerk auf AWS einrichten. Eine Transit-VPC ist eine gängige Strategie zur Verbindung mehrerer, geografisch verteilter VPCs und entfernter Netzwerke, um ein globales Netzwerk-Transitzentrum zu schaffen. Eine Transit-VPC vereinfacht die Netzwerkverwaltung und minimiert die Anzahl der Verbindungen, die für die Verbindung mehrerer VPCs und entfernter Netzwerke erforderlich sind. Die folgende Abbildung veranschaulicht diesen Entwurf.



Transit VPC

Dieses Design bietet nicht nur direktes Netzwerk-Routing zwischen VPCs und lokalen Netzwerken, sondern ermöglicht es der Transit-VPC auch, komplexere Routing-Regeln zu implementieren, wie z. B. die Netzwerkadressübersetzung zwischen überlappenden Netzwerkbereichen, oder zusätzliche Paketfilterung oder -inspektion auf Netzwerkebene hinzuzufügen. Das Transit-VPC-Design kann verwendet werden, um wichtige Anwendungsfälle wie private Netzwerke, gemeinsame Konnektivität und kontenübergreifende AWS-Nutzung zu unterstützen.

Weitere Ressourcen

- AWS Transit Gateway
- Cisco Catalyst 8000V für SD-WAN und Routing in AWS Marketplace

AWS-Cloud-WAN

AWS Cloud WAN ist ein zielorientiertes, verwaltetes Wide Area Network (WAN), das durch eine von Ihnen definierte Richtlinie beschrieben wird, die Ihr Rechenzentrum, Ihre Zweigstellen und Ihre AWS-Netzwerke vereinheitlicht. Sie können zwar Ihr eigenes globales Netzwerk aufbauen, indem Sie mehrere Transit-Gateways über Regionen hinweg miteinander verbinden, aber Cloud WAN bietet integrierte Automatisierungs-, Segmentierungs- und Konfigurationsverwaltungsfunktionen, die speziell für den Aufbau und Betrieb globaler Netzwerke auf der Grundlage Ihrer Kernnetzwerkrichtlinie entwickelt wurden. Cloud WAN verfügt über zusätzliche Funktionen wie automatisierte VPC-Anhänge, integrierte Leistungsüberwachung und zentrale Konfiguration.

Die Kernnetzwerkrichtlinie ist in einer deklarativen Sprache verfasst, die Segmente, das Routing in der AWS-Region und die Zuordnung der Anhänge zu Segmenten definiert. Mit einer zentralen Netzwerkrichtlinie können Sie Ihre Absicht für die Zugriffskontrolle und das Routing des Datenverkehrs beschreiben, während AWS Cloud WAN die Netzwerkkonfigurationsdetails verwaltet.

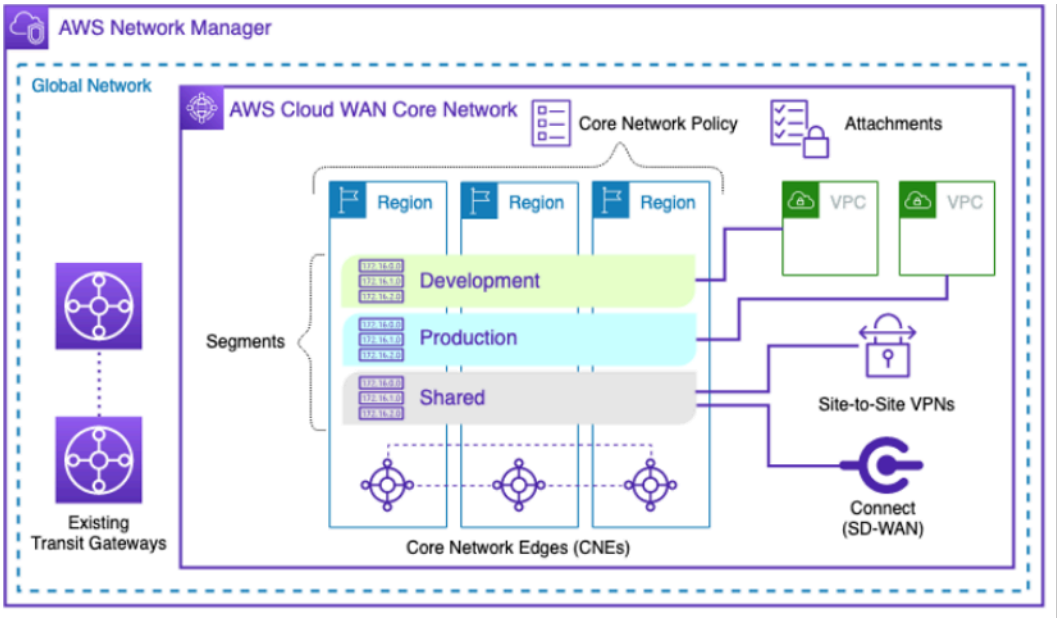
Cloud WAN wird in AWS Network Manager verwaltet, sodass Sie Ihr Cloud WAN-Kernnetzwerk und Ihre Transit Gateway Gateway-Netzwerke über AWS-Konten, Regionen und lokale Standorte hinweg zentral verwalten und visualisieren können. Network Manager bietet Ihnen mehrere Dashboard-Visualisierungen, mit denen Sie alle Aspekte Ihres globalen Netzwerks anzeigen und überwachen können. Einige der Dashboards umfassen:

- Weltkarten, die genau zeigen, wo sich Ihre Netzwerkressourcen wie Edge-Standorte, Geräte und Anlagen befinden.
- Überwachung, bei der mithilfe von CloudWatch Ereignissen Statistiken über einen Zeitraum von 15 Monaten erfasst werden, sodass Sie einen besseren Überblick über die Leistung Ihrer Netzwerke erhalten.
- Event-Tracking, bei dem Ereignisse in Echtzeit in ein Event-Dashboard gestreamt werden.
- Topologische und logische Diagramme Ihrer Transit-Gateway-Netzwerke und Transit-Gateways.

Sowohl Transit Gateway als auch Cloud WAN ermöglichen eine zentrale Konnektivität zwischen VPCs und vor Ort. Transit Gateway ist ein regionaler Knotenpunkt für Netzwerkkonnektivität und eignet sich optimal für Kunden, die in einigen AWS-Regionen tätig sind, ihre eigene Peering- und Routing-Konfiguration verwalten möchten oder ihre eigene Automatisierung bevorzugen. Cloud WAN ist optimal für Kunden, die ihr globales Netzwerk anhand von Richtlinien definieren und den Service die zugrunde liegenden Komponenten automatisch implementieren lassen möchten.

Wissenswertes

- CNE (Core Network Edge) erbt viele Eigenschaften des Transit Gateway, wie z. B. den Durchsatz pro VPC-Verbindung.
- Cloud WAN unterstützt sowohl als auch. IPv4 IPv6
- Bei großen Netzwerken mit vielen Änderungen sollten Sie erwägen, ein separates globales Entwicklungs- und Testnetzwerk einzurichten, in dem Sie Änderungen validieren können.



AWS Cloud WAN

Weitere Ressourcen

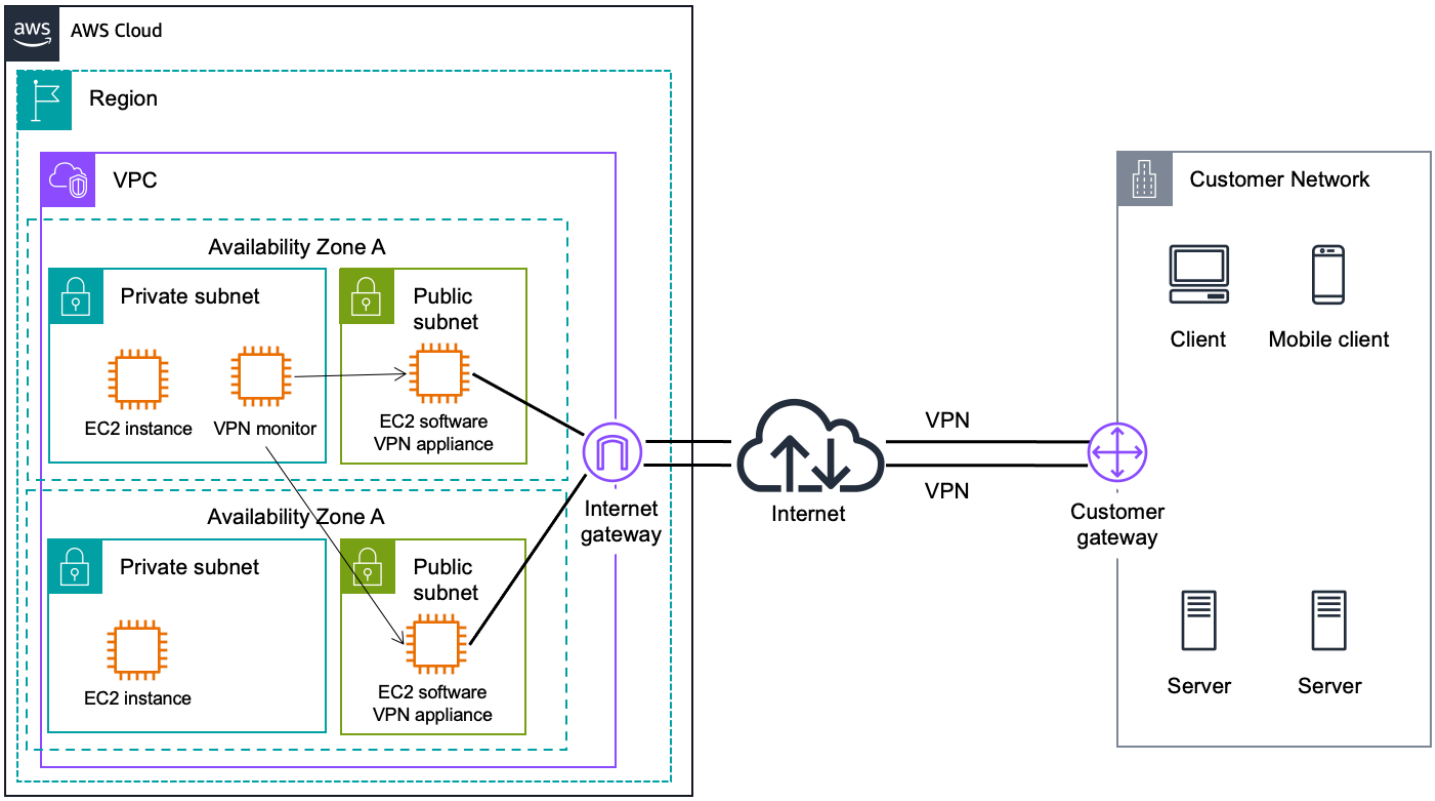
- Dokumentation zu AWS Cloud WAN
- Blogbeitrag: Migrations- und Interoperabilitätsmuster für AWS Cloud WAN und AWS Transit Gateway

Schlussfolgerung

AWS bietet eine Reihe effizienter, sicherer Verbindungsoptionen, mit denen Sie das Beste aus AWS herausholen können, wenn Sie Ihre Remote-Netzwerke mit Amazon VPC integrieren. Die in diesem Whitepaper vorgestellten Optionen heben einige der Konnektivitätsoptionen und -muster hervor, mit denen Kunden ihre Remote-Netzwerke oder mehrere Amazon VPC-Netzwerke erfolgreich integriert haben. Anhand der hier bereitgestellten Informationen können Sie den geeignetsten Mechanismus für die Verbindung der Infrastruktur ermitteln, die für den Betrieb Ihres Unternehmens erforderlich ist, unabhängig davon, wo sie sich physisch befindet oder gehostet wird.

Anhang A: Hochrangige HA-Architektur für Software-VPN-Instanzen

Die Erstellung einer vollständig ausfallsicheren VPC-Verbindung für Software-VPN-Instanzen erfordert die Einrichtung und Konfiguration mehrerer VPN-Instanzen und einer Überwachungsinstanz zur Überwachung des Zustands der VPN-Verbindungen.



Software-VPN HA auf hohem Niveau

Wir empfehlen, Ihre VPC-Routing-Tabellen so zu konfigurieren, dass alle VPN-Instances gleichzeitig genutzt werden, indem der Datenverkehr von allen Subnetzen in einer Availability Zone über die jeweiligen VPN-Instances in derselben Availability Zone geleitet wird. Jede VPN-Instanz bietet dann VPN-Konnektivität für Instances, die sich dieselbe Availability Zone teilen.

VPN-Überwachung

Um die softwarebasierte VPN-Appliance zu überwachen, können Sie einen VPN-Monitor erstellen. Der VPN-Monitor ist eine benutzerdefinierte Instanz, die Sie benötigen, um die VPN-Überwachungsskripte auszuführen. Diese Instanz dient zum Ausführen und Überwachen des

Status von VPN-Verbindungen und VPN-Instanzen. Wenn eine VPN-Instanz oder -Verbindung ausfällt, muss der Monitor die VPN-Instanz stoppen, beenden oder neu starten und gleichzeitig den Datenverkehr von den betroffenen Subnetzen zur funktionierenden VPN-Instanz umleiten, bis beide Verbindungen wieder funktionieren. Da die Kundenanforderungen unterschiedlich sind, bietet AWS derzeit keine verbindlichen Leitlinien für die Einrichtung dieser Monitoring-Instance. Ein Beispielskript zur Aktivierung von HA zwischen NAT-Instances könnte jedoch als Ausgangspunkt für die Erstellung einer HA-Lösung für Software-VPN-Instances verwendet werden. Wir empfehlen Ihnen, die erforderliche Geschäftslogik zu durchdenken, um im Falle eines VPN-Verbindungsfehlers eine Benachrichtigung zu senden oder zu versuchen, die Netzwerkkonnektivität automatisch zu reparieren.

Darüber hinaus können Sie die von AWS verwalteten VPN-Tunnel mithilfe von CloudWatch Amazon-Metriken überwachen. Dabei werden Datenpunkte aus dem VPN-Service in lesbaren, nahezu in Echtzeit verfügbaren Metriken erfasst. Jede VPN-Verbindung sammelt und veröffentlicht eine Vielzahl von Tunnelmetriken für Amazon CloudWatch. Diese Metriken ermöglichen es Ihnen, den Zustand und die Aktivität des Tunnels zu überwachen und automatisierte Aktionen zu erstellen.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Daniel Yu, leitender technischer Kundenbetreuer, AWS Enterprise Support
- Garvit Singh, Solutions Builder, AWS-Lösungsarchitektur
- Steve Morad, Senior Manager, Solution Builders, AWS-Lösungsarchitektur
- Sohaib Tahir, Lösungsarchitekt, AWS-Lösungsarchitektur
- Fiona Armada, Hauptarchitektin für Lösungen, AWS-Lösungsarchitektur
- Pablo Sánchez Carmona, Netzwerkspezialist, Lösungsarchitekt, AWS-Lösungsarchitektur
- Tony Hawke, Senior Networking Specialist, Technischer Kundenbetreuer, AWS Enterprise Support

Dokumentversionen

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

Änderung	Beschreibung	Datum
Whitepaper aktualisiert	Es wurden Verbindungsoptionen für AWS Cloud WAN und Transit Gateway Connect hinzugefügt, Diagramme und Informationen wurden durchgehend aktualisiert.	5. April 2023
Whitepaper aktualisiert	Es wurden die VPN-Optionen für AWS Transit Gateway und AWS Client hinzugefügt, Diagramme und Informationen wurden durchgehend aktualisiert.	6. Juni 2020
Kleines Update	Geringfügige Änderung, um den Verweis auf die Software-VPN-Appliance zu korrigieren.	20. Mai 2020
Whitepaper aktualisiert	Durchgehend aktualisierte Informationen. Konzentrieren Sie sich auf die folgenden Designs/Funktionen: Transit-VPC, Direct Connect-Gateway und. AWS PrivateLink	1. Januar 2018
Erste Veröffentlichung	Die Verbindungsoptionen für Amazon Virtual Private Cloud wurden veröffentlicht.	1. Juli 2014

Hinweise

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

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