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

Veröffentlichungsdatum: 5. April 2023 (Dokumentversionen)

## Überblick

Mit Amazon Virtual Private Cloud (Amazon VPC) können Kunden einen privaten, isolierten Abschnitt der Amazon Web Services (AWS) Cloud bereitstellen, in dem sie AWS-Ressourcen in einem virtuellen Netzwerk mithilfe von vom Kunden definierten IP-Adressbereichen starten können. Amazon VPC bietet Kunden mehrere Möglichkeiten, ihre virtuellen AWS-Netzwerke mit anderen Remote-Netzwerken zu verbinden. In diesem Dokument werden mehrere gängige Netzwerkkonnektivitätsoptionen beschrieben, die unseren Kunden zur Verfügung stehen. Dazu gehören Konnektivitätsoptionen für die Integration von Remote-Kundennetzwerken in 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 Verbindungsoptionen überprüfen möchten. Es bietet einen Überblick über die verschiedenen Optionen, um Diskussionen zur Netzwerkkonnektivität zu erleichtern, sowie Verweise auf zusätzliche Dokumentationen und Ressourcen mit detaillierteren Informationen oder Beispielen.

# Einführung

Amazon VPC bietet je nach Ihren aktuellen Netzwerkdesigns und -anforderungen mehrere Netzwerkkonnektivitätsoptionen, die Sie verwenden können. Zu diesen Verbindungsoptionen gehören die Verwendung des Internets oder einer -AWS Direct ConnectVerbindung als Netzwerk-Backbone und das Beenden der Verbindung mit AWS- oder benutzerverwalteten Netzwerkendpunkten. Darüber hinaus können Sie mit AWS auswählen, wie 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 einer Übersicht und einem allgemeinen Vergleich betrachtet:

- Netzwerk-zu-Amazon-VPC-Konnektivitätsoptionen
  - AWS Site-to-Site VPN – Beschreibt das Herstellen einer verwalteten IPsec-VPN-Verbindung von Ihren Netzwerkgeräten in einem Remote-Netzwerk zu Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN – Beschreibt das Herstellen 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 + AWS Site-to-Site VPN – Beschreibt das Herstellen einer privaten, verschlüsselten Verbindung von Ihrem Remote-Netzwerk zu Amazon VPC mithilfe von AWS Direct Connect und AWS Site-to-Site VPN.
  - AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN – Beschreibt das Herstellen einer privaten, verschlüsselten Verbindung von Ihrem Remote-Netzwerk zu einem regionalen Netzwerk-Hub für Amazon VPCs mithilfe von AWS Direct Connect und AWS Transit Gateway.
  - AWS VPN CloudHub – Beschreibt die Einrichtung eines hub-and-spoke Modells für die Verbindung von Remote-Zweigstellen.
  - Software VPN – Beschreibt das Herstellen 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 Remote-Standorte mit einem regionalen Netzwerk-Hub für Amazon VPCs unter Verwendung des AWS Backbones oder des Internets als Transitnetzwerk.
- Amazon-VPC-zu-Amazon-VPC-Konnektivitätsoptionen
  - VPC-Peering – Beschreibt die Verbindung von Amazon VPCs innerhalb und zwischen Regionen mithilfe der Amazon-VPC-Peering-Funktion.
  - AWS Transit Gateway – Beschreibt die Verbindung von Amazon VPCs innerhalb und zwischen Regionen mithilfe von AWS Transit Gateway in einem hub-and-spoke Modell.
  - AWS PrivateLink – Beschreibt die Verbindung von Amazon VPCs mit VPC-Schnittstellenendpunkten und VPC-Endpunktservices.
  - Software VPN – Beschreibt die Verbindung von Amazon VPCs über VPN-Verbindungen, die zwischen benutzerverwalteten Software-VPN-Appliances hergestellt werden, die in jeder Amazon VPC ausgeführt werden.
  - Software-VPN-zu-AWS-Site-to-Site-VPN – Beschreibt die Verbindung von Amazon VPCs mit einer VPN-Verbindung zwischen einer benutzerverwalteten Software-VPN-Appliance in einer Amazon VPC und einem AWS Site-to-Site VPN, das an die andere Amazon VPC angefügt ist.
- Software-Fernzugriff auf Amazon VPC-Verbindungsoptionen
  - AWS Client VPN – Beschreibt die Verbindung des Remote-Zugriffs von Software mit Amazon VPC unter Verwendung von AWS Client VPN.
  - Software-Client-VPN – Beschreibt die Verbindung des Software-Remote-Zugriffs mit Amazon VPC unter Verwendung von benutzerverwalteten Software-VPN-Appliances.
- Transit-VPC – Beschreibt das Einrichten eines globalen Transitnetzwerks in 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), um globale Verbindungen zwischen Ressourcen in Amazon VPCs , Rechenzentren und Remote-Zweigen einfach aufzubauen, zu verwalten und zu überwachen.

# Netzwerk-zu-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 On-Premises-Services (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.

Die VPC-Konnektivität zu Remote-Kundennetzwerken wird am besten erreicht, wenn für jedes Netzwerk, das verbunden wird, nicht überlappende IP-Bereiche verwendet werden. Wenn Sie beispielsweise eine oder mehrere VPCs mit Ihrem Unternehmensnetzwerk verbinden möchten, stellen Sie sicher, dass sie mit eindeutigen CIDR-Bereichen (Classless Inter-Domain Routing) konfiguriert sind. Wir empfehlen, einen einzelnen, zusammenhängenden, nicht überlappenden CIDR-Block zuzuweisen, der von jeder VPC verwendet werden soll. Weitere Informationen zu Amazon-VPC-Routing und Einschränkungen finden Sie unter Häufig gestellte Fragen zu Amazon VPC.

| Option | Anwendungsfall | Vorteile | Einschränkungen |
|---|---|---|---|
| AWS Site-to-Site-VPN | Von AWS verwaltete IPsec-VPN-Verbindung über das Internet zu einer einzelnen VPC | Wiederverwenden vorhandener VPN-Geräte und -Prozesse<br><br>Wiederverwenden vorhandener Internetverbindungen<br><br>Von AWS verwalteter VPN-Service für hohe Verfügbarkeit<br><br>Unterstützt statische Routen oder dynamische BGP-Peering- und Routing-Richtlinien (Border Gateway Protocol) | Netzwerklatenz, Variabilität und Verfügbarkeit hängen von den Internetbedingungen ab<br><br>Sie sind für die Implementierung von Redundanz und Failover verantwortlich (falls erforderlich)<br><br>Remote-Gerät muss Single-Hop-BGP unterstützen (bei Verwendung von BGP für dynamisches Routing) |

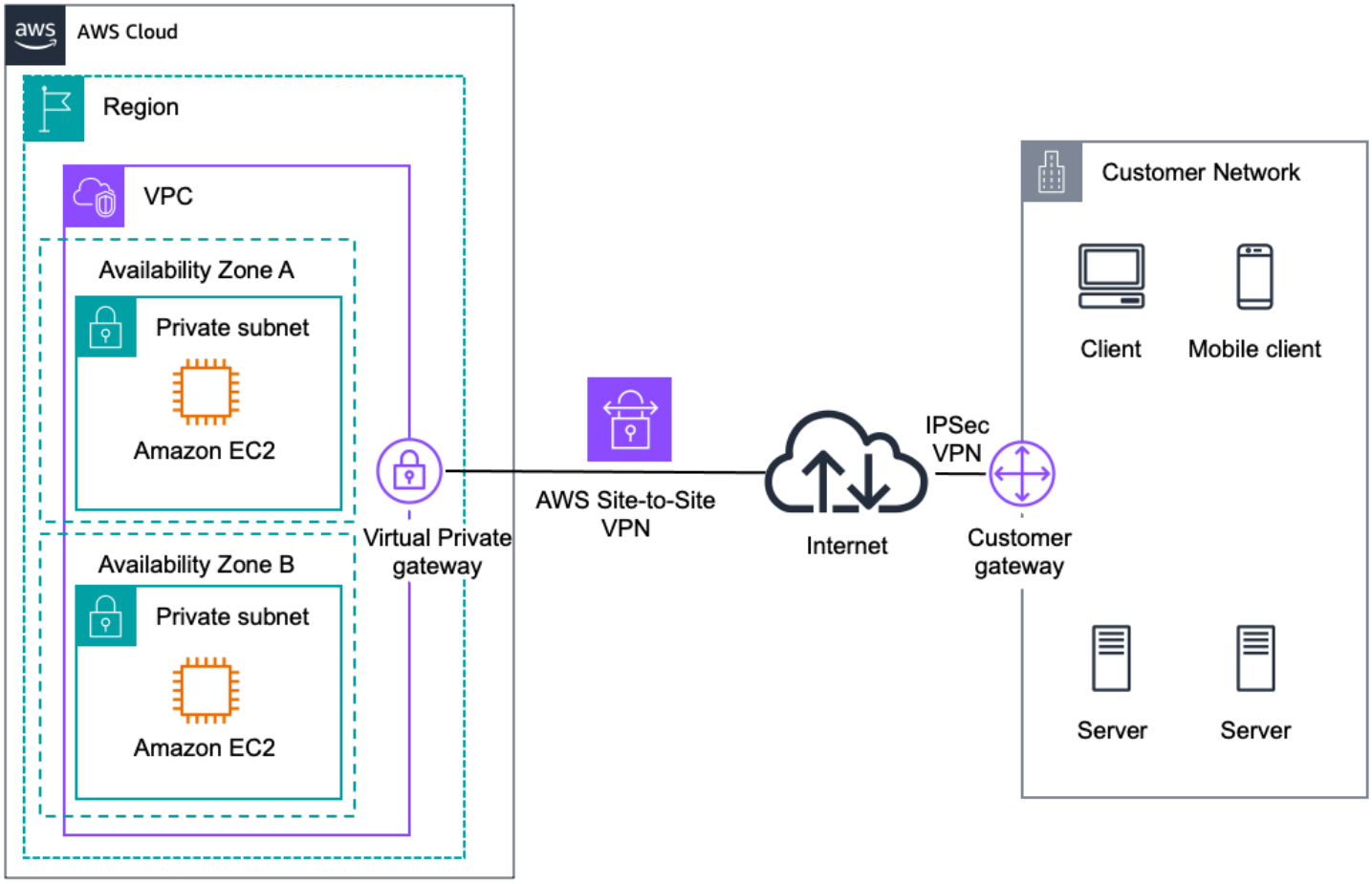
| Option | Anwendungsfall | Vorteile | Einschränkungen |
| --- | --- | --- | --- |
| AWS Transit Gateway + AWS Site-to-Site VPN | Von AWS verwaltete IPsec-VPN-Verbindung über das Internet zum regionalen Router für mehrere VPCs | Wie bei der vorherigen Option<br><br>Von AWS verwalteter regionaler Netzwerk-Hub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5 000 Anlagen | Wie bei der vorherigen Option |
| AWS Direct Connect | Dedizierte Netzwerkverbindung über private Zeilen | Vorhersehbarere Netzwerkleistung<br><br>Geringere Bandbreitenkosten<br><br>Unterstützt BGP-Peering- und Routing-Richtlinien | Möglicherweise erfordern Sie zusätzliche Telekommunikations- und Hosting-Anbieterbeziehungen oder neue Netzwerkschaltungen |
| AWS Direct Connect + AWS Transit Gateway | Dedizierte Netzwerkverbindung über private Zeilen zum regionalen Router für mehrere VPCs | Wie bei der vorherigen Option<br><br>Von AWS verwalteter regionaler Netzwerk-Hub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5 000 Anlagen | Wie bei der vorherigen Option |

| Option | Anwendungsfall | Vorteile | Einschränkungen |
| --- | --- | --- | --- |
| AWS Direct Connect + AWS Site-to-Site VPN | IPsec-VPN-Verbindung über private Zeilen | Vorhersehbarere Netzwerkleistung<br><br>Geringere Bandbreitenkosten<br><br>Unterstützt BGP-Peering- und Routing-Richtlinien auf AWS Direct Connect<br><br>Wiederverwenden vorhandener VPN-Geräte und -Prozesse<br><br>Von AWS verwalteter VPN-Service für hohe Verfügbarkeit<br><br>Unterstützt statische Routen oder dynamische BGP-Peering- und Routing-Richtlinien (Border Gateway Protocol) für VPN-Verbindungen | Möglicherweise müssen zusätzliche Telekommunikations- und Hosting-Anbieterbeziehungen oder neue Netzwerkschaltungen bereitgestellt werden<br><br>Sie sind für die Implementierung von Redundanz und Failover verantwortlich (falls erforderlich)<br><br>Remote-Gerät muss Single-Hop-BGP unterstützen (bei Verwendung von BGP für dynamisches Routing) |
| AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN | IPsec-VPN-Verbindung über private Zeilen zum regionalen Router für mehrere VPCs | Wie bei der vorherigen Option<br><br>Von AWS verwalteter regionaler Netzwerk-Hub mit hoher Verfügbarkeit und Skalierbarkeit für bis zu 5 000 Anlagen | Wie bei der vorherigen Option |

| Option | Anwendungsfall | Vorteile | Einschränkungen |
| --- | --- | --- | --- |
| AWS VPN CloudHub | Verbinden von Remote-Zweigstellen in einem hub-and-spoke Modell für primäre oder Backup-Konnektivität | Wiederverwenden vorhandener Internetverbindungen und AWS VPN Verbindungen<br><br>Von AWS verwalteter VPN-Service für hohe Verfügbarkeit<br><br>Unterstützt BGP für den Austausch von Routen und Routing-Prioritäten | Netzwerklatenz, Variabilität und Verfügbarkeit hängen vom Internet ab<br><br>Benutzerverwaltete Zweigstellenendpunkte sind für die Implementierung von Redundanz und Failover verantwortlich (falls erforderlich) |
| AWS Transit Gateway + SD-WAN-Lösungen | Verbinden Sie Remote-Zweige und -Standorte mit einem softwaredefinierten Wide Area Network, indem Sie das - AWS Backbone oder das Internet als Transitnetzwerk verwenden. | Unterstützt eine breitere Palette von SD-WAN-Anbietern, -Produkten und -Protokollen<br><br>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 werden. |
| Software VPN | Software-Appliance-basierte VPN-Verbindung über das Internet | Unterstützt eine breitere Palette von VPN-Anbietern, -Produkten und -Protokollen<br><br>Vollständige kundenverwaltete Lösung | Sie sind für die Implementierung von HA-Lösungen (Hochverfügbarkeit) für alle VPN-Endpunkte verantwortlich (falls erforderlich) |

# AWS Site-to-Site-VPN

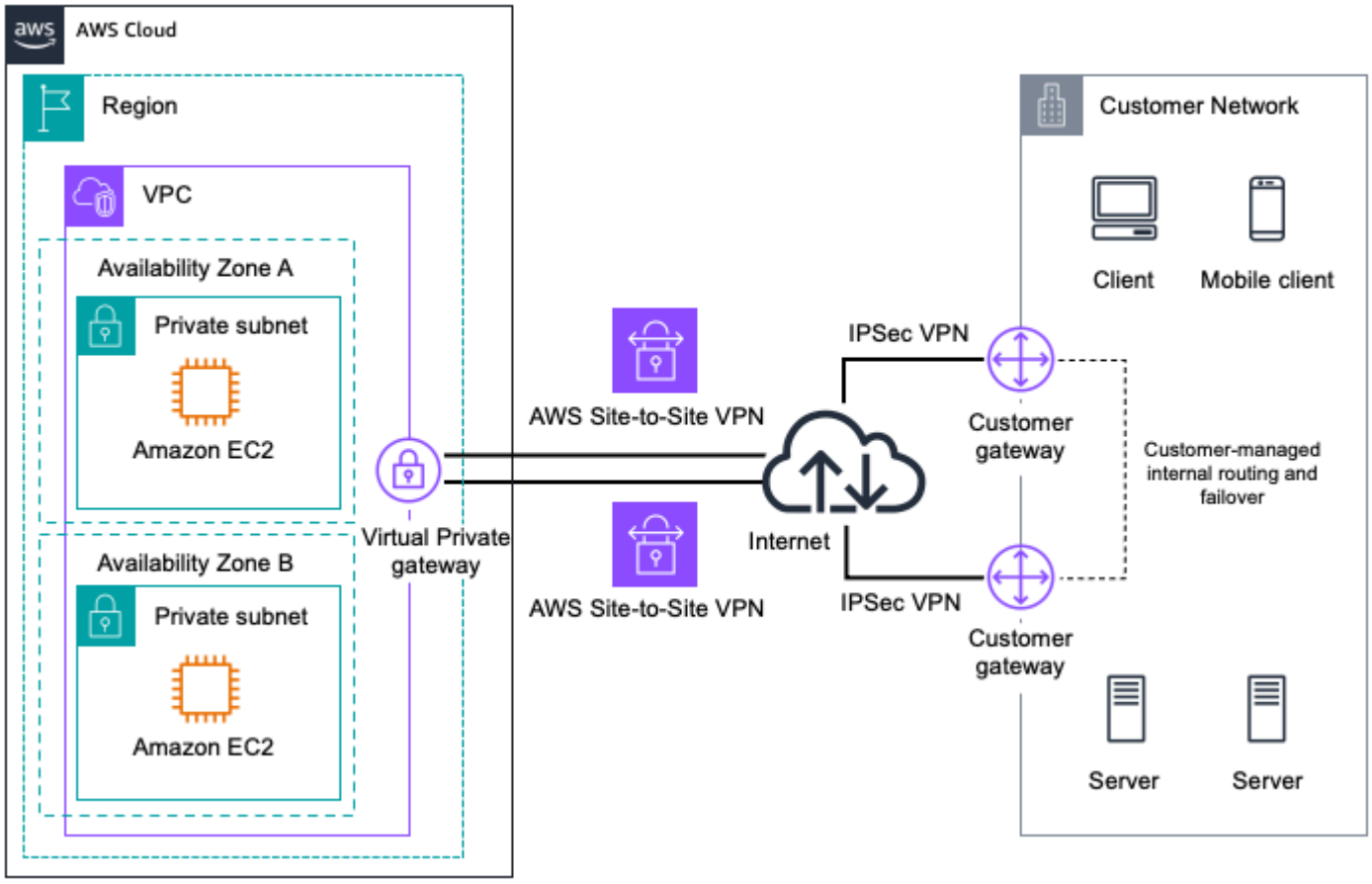
Amazon VPC bietet die Möglichkeit, eine IPsec-VPN-Verbindung zwischen Ihren Remote-Netzwerken und Amazon VPC über das Internet herzustellen, wie in der folgenden Abbildung dargestellt.




AWS Managed VPN

Erwägen Sie, diesen Ansatz zu verwenden, wenn Sie einen von AWS verwalteten VPN-Endpunkt nutzen möchten, der automatisierte Redundanz und Failover umfasst, die in die AWS-Seite der VPN-Verbindung integriert sind.

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




Redundant AWS Site-to-Site VPN Connections

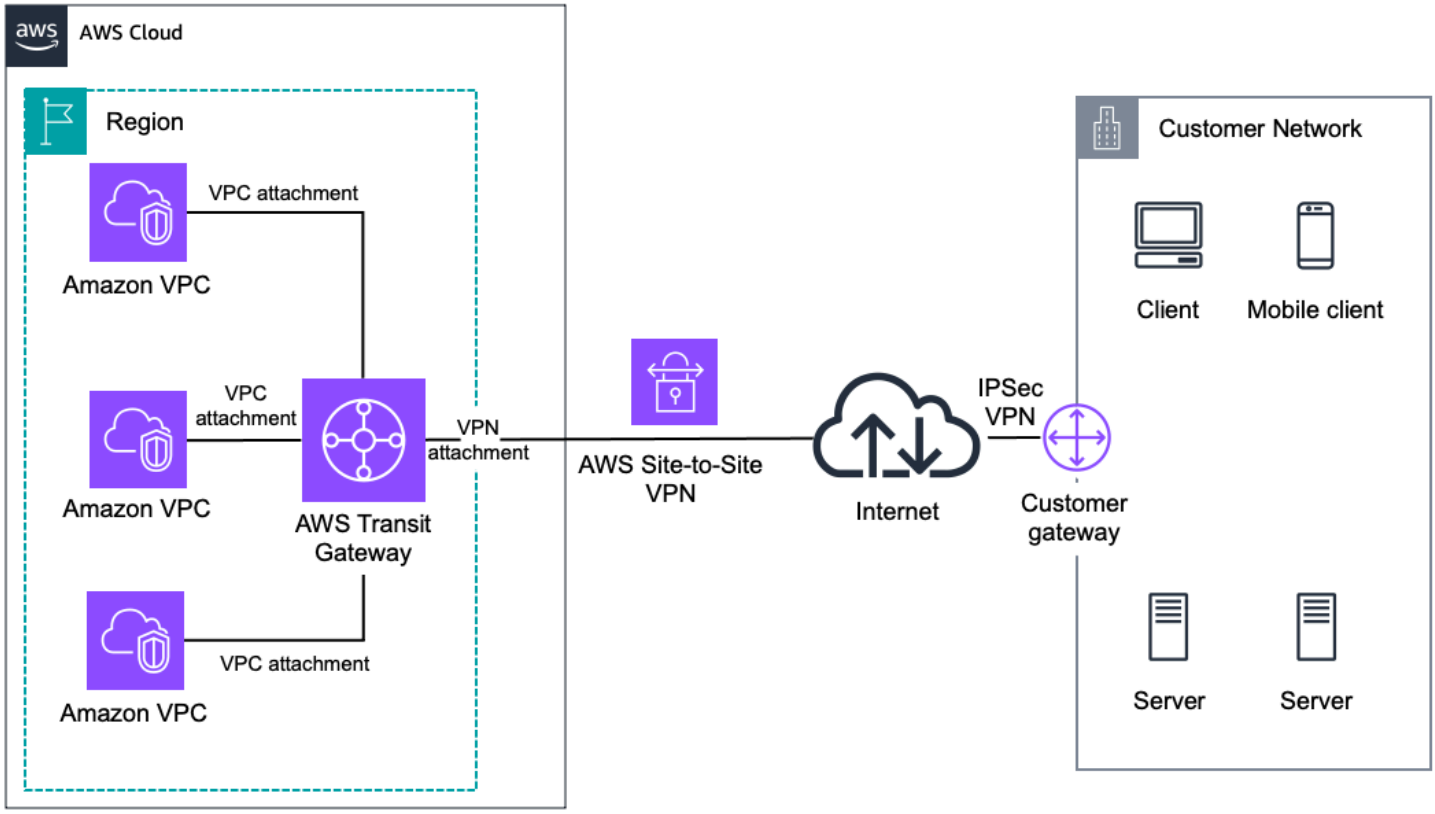
Sowohl dynamische als auch statische Routing-Optionen bieten Ihnen Flexibilität in Ihrer Routing-Konfiguration. Dynamisches Routing verwendet BGP-Peering, um Routing-Informationen zwischen AWS und diesen Remote-Endpunkten auszutauschen. Mit dynamischem Routing können Sie auch Weiterleitungsprioritäten, Richtlinien und Gewichtungen (Metriken) in Ihren BGP-Ankündigungen angeben und den Netzwerkpfad zwischen Ihren Netzwerken und AWS beeinflussen. Beachten Sie, dass bei Verwendung von BGP sowohl die IPsec- als auch die BGP-Sitzungen auf demselben Benutzer-Gateway-Gerät beendet werden müssen, sodass es sowohl IPsec- als auch BGP-Sitzungen beenden kann.

## Weitere Ressourcen

- Benutzerhandbuch zu AWS Site-to-Site-VPN
- Anforderungen für Kunden-Gateway-Geräte
- Mit Amazon VPC getestete Kunden-Gateway-Geräte

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

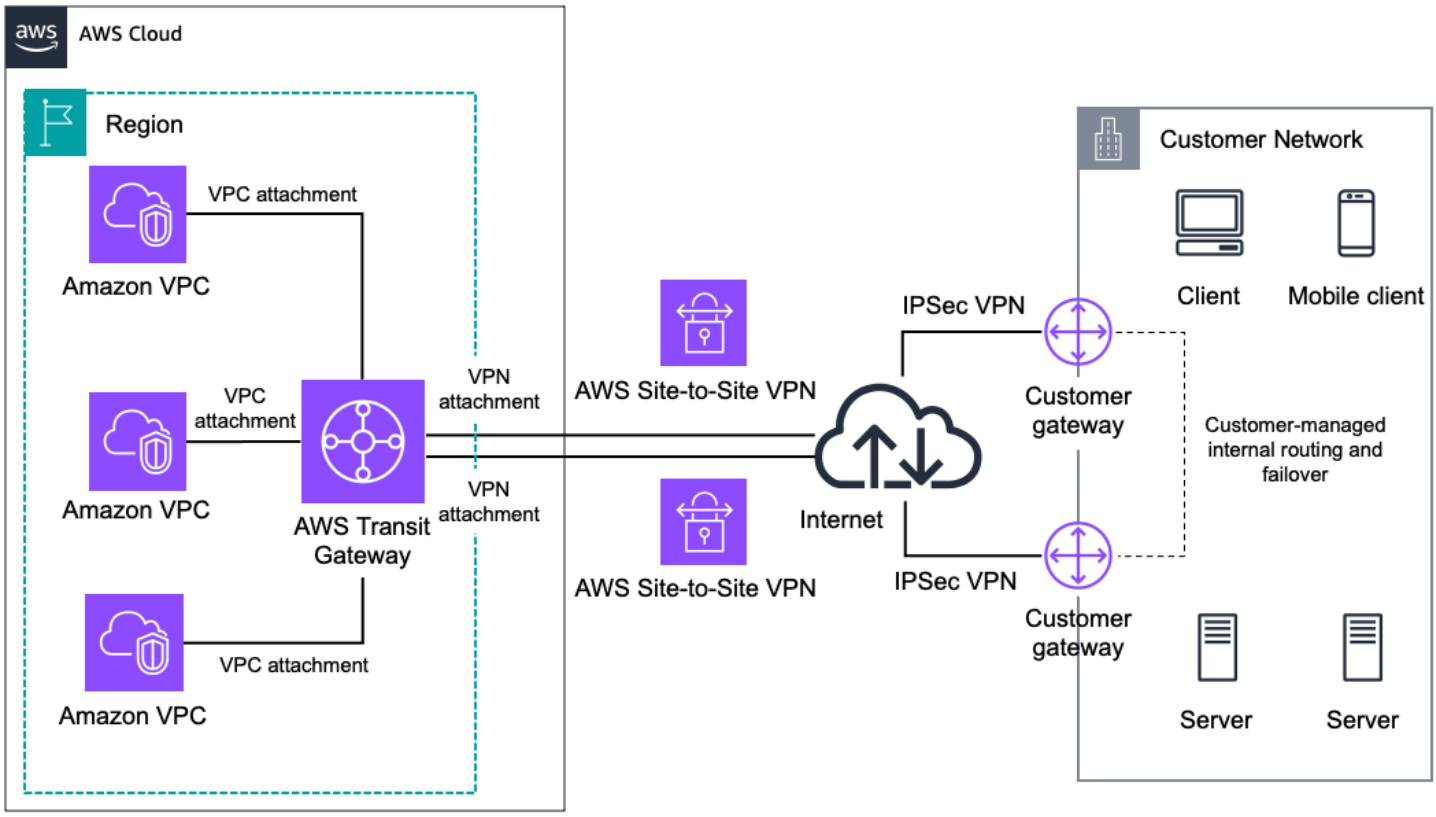
AWS Transit Gateway ist ein von AWS verwalteter regionaler Netzwerk-Transit-Hub mit hoher Verfügbarkeit und Skalierbarkeit, der zur Verbindung von VPCs und Kundennetzwerken verwendet wird. AWS Transit Gateway + VPN bietet mithilfe der Transit Gateway VPN-Anfügung die Möglichkeit, eine IPsec-VPN-Verbindung zwischen Ihrem Remote-Netzwerk und dem Transit Gateway über das Internet herzustellen, wie in der folgenden Abbildung gezeigt.




AWS Transit Gateway and AWS Site-to-Site VPN

Erwägen Sie, diesen Ansatz zu verwenden, wenn Sie die Vorteile eines von AWS verwalteten VPN-Endpunkts für die Verbindung mit mehreren VPCs in derselben Region nutzen möchten, ohne die zusätzlichen Kosten und die Verwaltung mehrerer IPsec-VPN-Verbindungen zu mehreren Amazon VPCs.

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



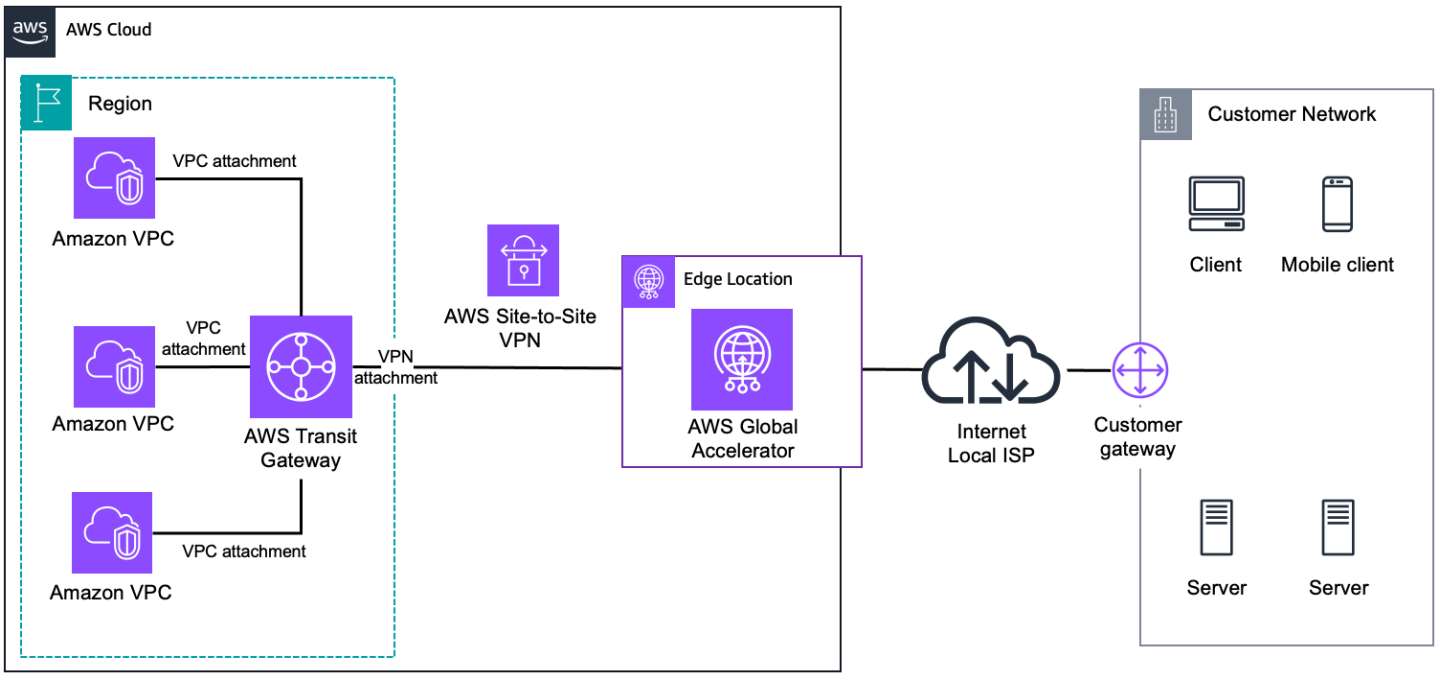

AWS Transit Gateway and Redundant VPN

Es werden sowohl dynamische als auch statische Routing-Optionen bereitgestellt, um Ihnen Flexibilität bei Ihrer Routing-Konfiguration auf dem Transit-Gateway-VPN-IPsec-Anhang zu geben. Dynamisches Routing verwendet BGP-Peering, um Routing-Informationen zwischen AWS und diesen Remote-Endpunkten auszutauschen. Mit dynamischem Routing können Sie auch Weiterleitungsprioritäten, Richtlinien und Gewichtungen (Metriken) in Ihren BGP-Ankündigungen angeben und den Netzwerkpfad zwischen Ihren Netzwerken und AWS beeinflussen. Beachten Sie, dass bei Verwendung von BGP sowohl die IPsec- als auch die BGP-Sitzungen auf demselben Benutzer-Gateway-Gerät beendet werden müssen, sodass es sowohl IPsec- als auch BGP-Sitzungen beenden kann.

Pro VPN-Verbindung können Sie einen Durchsatz von 1,25 Gbit/s und 140 000 Pakete pro Sekunde erreichen. Beim Beenden der VPN-Verbindungen im Transit Gateway 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 nicht mit statischem Routing unterstützt.

Darüber hinaus können Sie die Beschleunigung in Ihren AWS Site-to-Site VPN-Verbindungen aktivieren. Eine beschleunigte VPN-Verbindung verwendet AWS Global Accelerator, um den

Datenverkehr von Ihrem Netzwerk an einen 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 angefügt sind, wie in der folgenden Abbildung dargestellt:




Accelerated AWS Site-to-Site VPN

Schließlich unterstützen Site-to-Site-VPN-Verbindungen auf einem AWS Transit Gateway sowohl IPv4- als auch IPv6-Datenverkehr in Bezug auf die IP-Adressierung. Die folgenden Regeln gelten:

- IPv6 wird nur für die internen IP-Adressen des VPN-Tunnels unterstützt. Die externe IP-Adresse für die AWS Endpunkte sind öffentliche IPv4-Adressen. Die IP-Adresse des Kunden-Gateways sollte eine öffentliche IPv4-Adresse sein.
- Eine Site-to-Site VPN-Verbindung kann nicht gleichzeitig sowohl den IPv4- als auch den IPv6-Datenverkehr unterstützen. Wenn Ihre Hybrid-Konnektivität eine Dual-Stack-Kommunikation erfordert, sollten Sie unterschiedliche VPN-Tunnel für den IPv4- und IPv6-Datenverkehr erstellen.

## Weitere Ressourcen

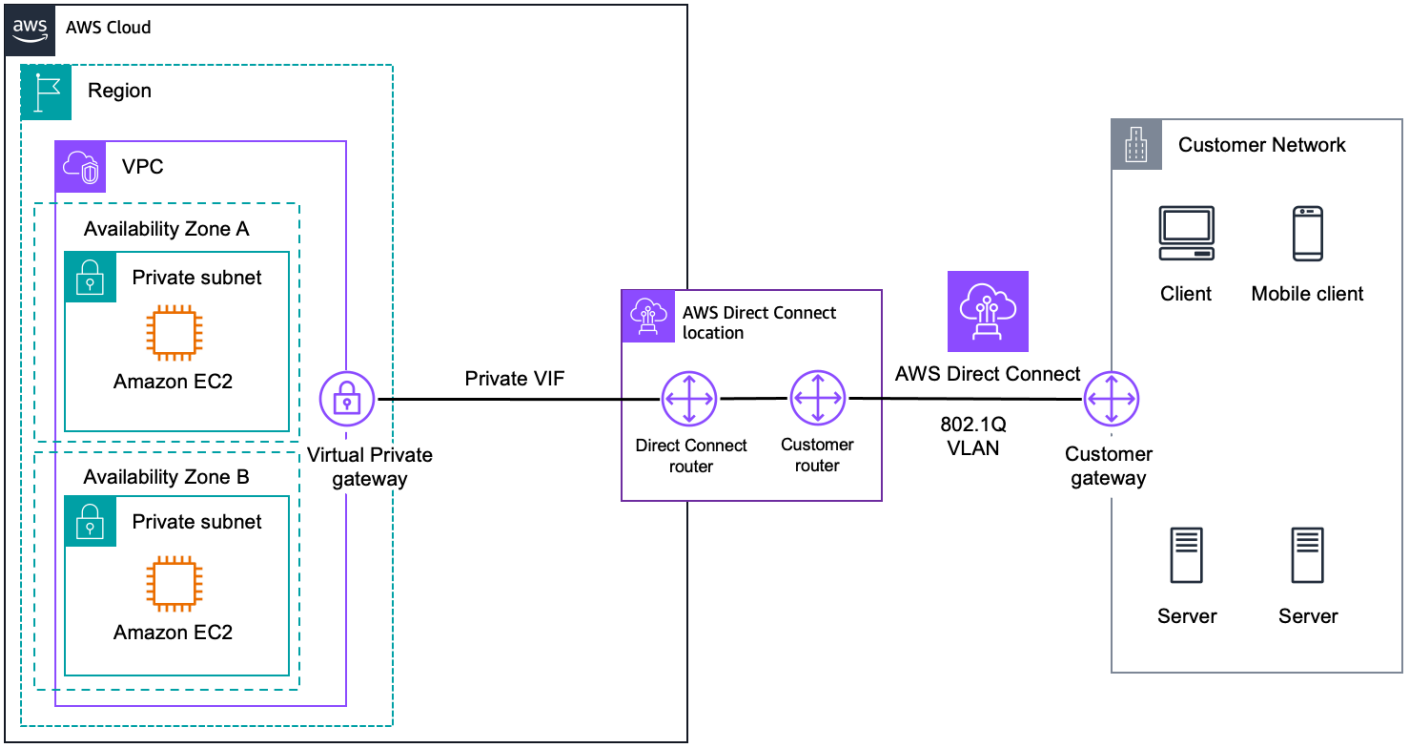
- Transit-Gateway-VPN-Anfügungen
- Kunden-Gateway
- Arbeiten mit Site-to-Site VPN

- Beschleunigte Site-to-Site-VPN-Verbindungen

# AWS Direct Connect

AWS Direct Connect erleichtert das Herstellen einer dedizierten Verbindung von einem On-Premises-Netzwerk zu einer oder mehreren VPCs. AWS Direct Connect kann die Netzwerkkosten senken, den Bandbreitendurchsatz erhöhen und ein konsistenteres Netzwerkerlebnis bieten als internetbasierte Verbindungen. Es verwendet branchenübliche 802.1Q VLANs, um über private IP-Adressen eine Verbindung zu Amazon VPC herzustellen. Die VLANs werden über virtuelle Schnittstellen (VIFs ) konfiguriert und Sie können drei verschiedene Arten von VIFs konfigurieren:

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




AWS Direct Connect

Sie können mithilfe von eine Verbindung 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 keine Ausrüstung an einem Standort haben, können Sie aus einem Ökosystem von WAN-Serviceanbietern wählen, um Ihren AWS Direct Connect Endpunkt an einem AWS Direct Connect Standort in Ihre Remote-Netzwerke zu integrieren.

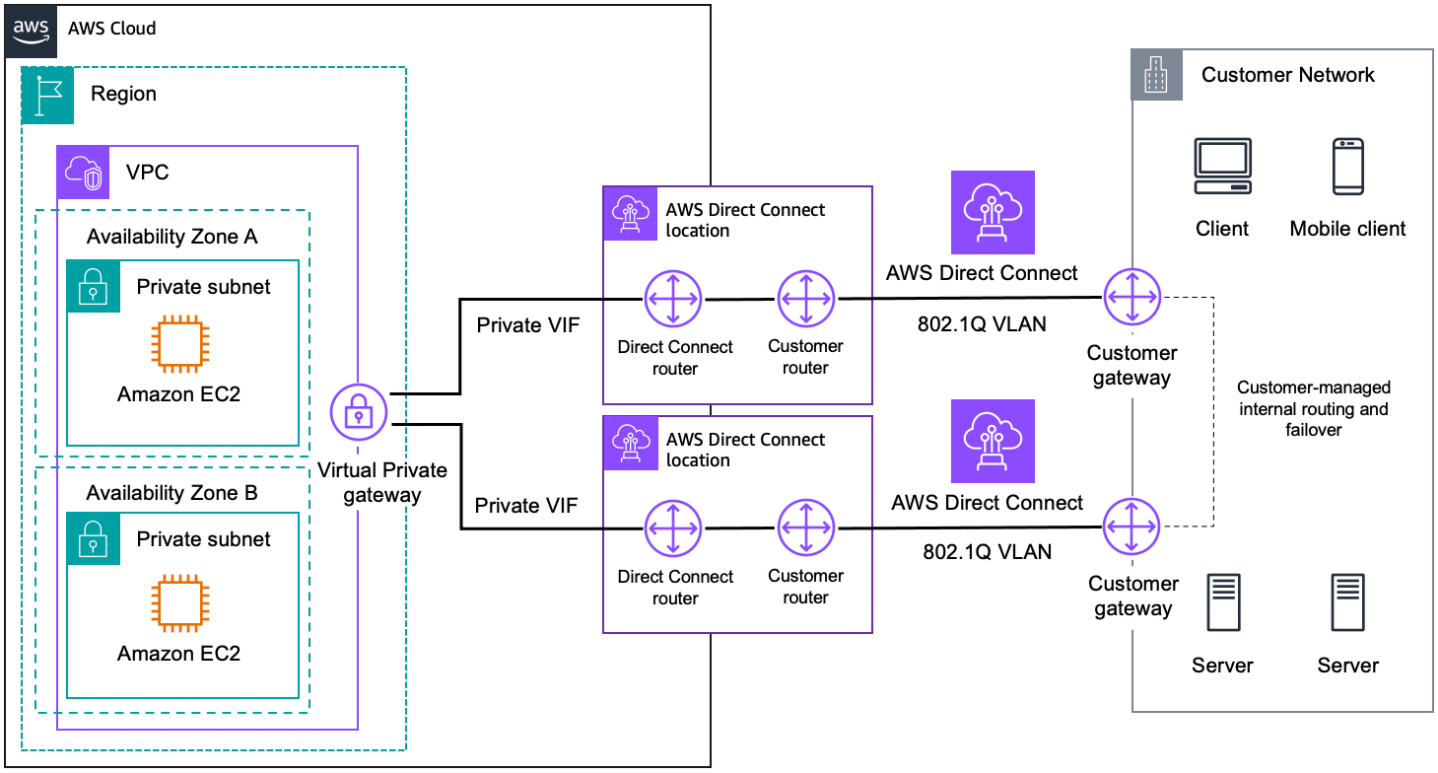
Mit haben AWS Direct Connect Sie zwei Verbindungstypen:

- Dedizierte Verbindungen, bei denen eine physische Ethernet-Verbindung einem einzelnen Kunden zugeordnet ist. Sie können Portgeschwindigkeiten von 1, 10 oder 100 Gbit/s bestellen. Möglicherweise müssen Sie mit einem Partner im - AWS Direct Connect Partnerprogramm zusammenarbeiten, um Netzwerkschaltungen zwischen einer - AWS Direct Connect Verbindung und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung herzustellen.
- Gehostete Verbindungen, bei denen eine physische Ethernet-Verbindung von einem - AWS Direct Connect Partner bereitgestellt und für Sie freigegeben wird. Sie können Portgeschwindigkeiten zwischen 50 Mbit/s und 10 Gbit/s bestellen. Ihre arbeiten sowohl in der von ihnen hergestellten AWS Direct Connect Verbindung als auch in den Netzwerkschaltungen zwischen einer - AWS

Direct Connect Verbindung und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung mit dem -Partner zusammen.

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

Wenn Sie über hohe Verfügbarkeit in sprechen AWS Direct Connect, empfehlen wir die Verwendung zusätzlicher AWS Direct Connect Verbindungen. Das AWS Direct Connect Resiliency Toolkit bietet Anleitungen zum Aufbau äußerst ausfallsicherer Netzwerkverbindungen zwischen AWS und Ihrem Rechenzentrum, Büro oder Ihrer Co-Location-Umgebung. Die folgende Abbildung zeigt ein Beispiel für eine Konnektivitätsoption mit hoher Ausfallsicherheit, wobei zwei AWS Direct Connect Verbindungen an zwei verschiedenen AWS Direct Connect Standorten beendet werden.

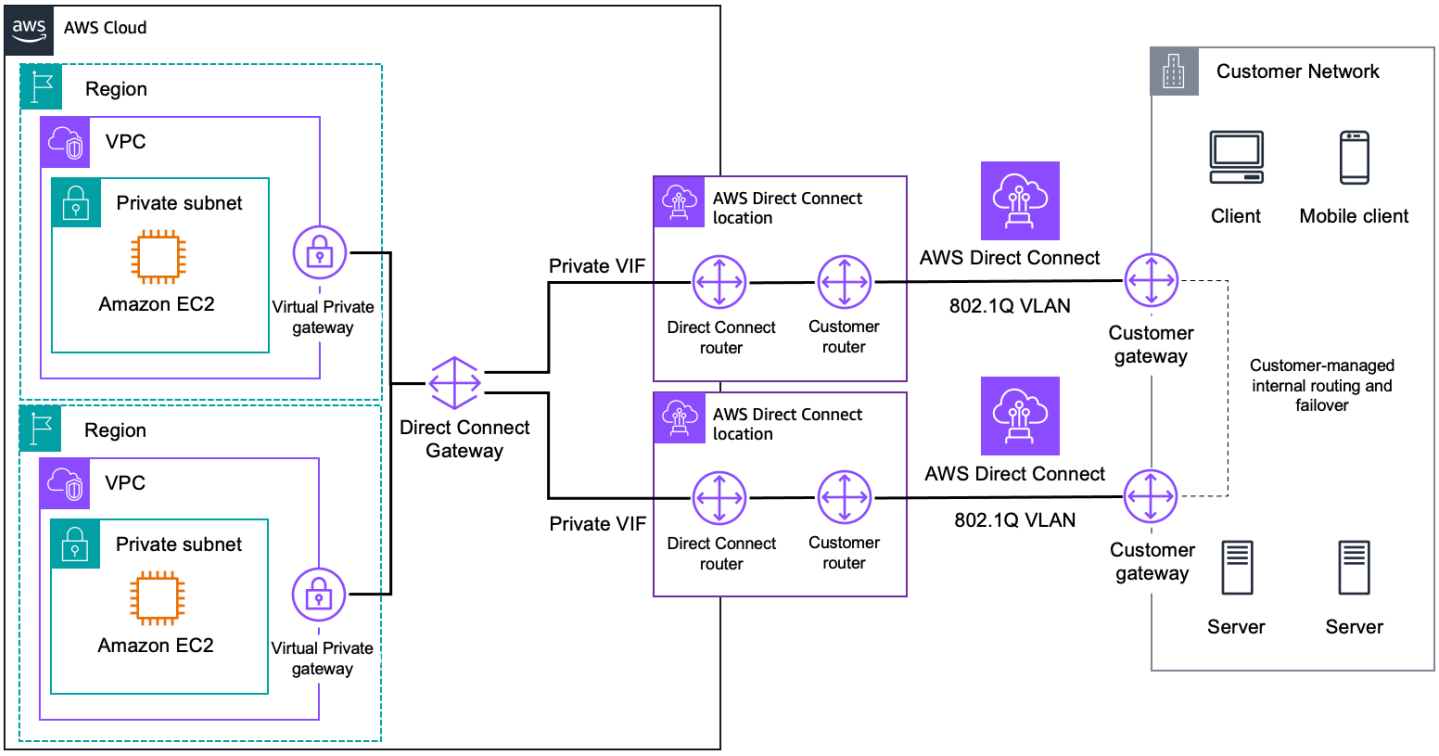



Redundant AWS Direct Connect

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

Verbindung erstellen. Diese Option wird in den AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN Abschnitten AWS Direct Connect + AWS Site-to-Site VPN und behandelt.

Eine wichtige Ressource in AWS Direct Connect ist das Direct Connect Gateway, eine global verfügbare Ressource, um Verbindungen zu mehreren Amazon VPCs oder Transit Gateways über verschiedene Regionen oder AWS Konten hinweg zu ermöglichen. Mit dieser Ressource können Sie sich auch von einer privaten VIF oder Transit-VIF aus mit jeder teilnehmenden VPC oder Transit Gateway verbinden, wodurch die Verwaltung reduziert AWS Direct Connect wird, wie in der folgenden Abbildung dargestellt.




AWS Direct Connect Gateway

Optische IP-Adressierung, AWS Direct Connect virtuelle Schnittstellen unterstützen sowohl IPv4- als auch IPv6-BGP-Sitzungen für Dual-Stack-Operationen.

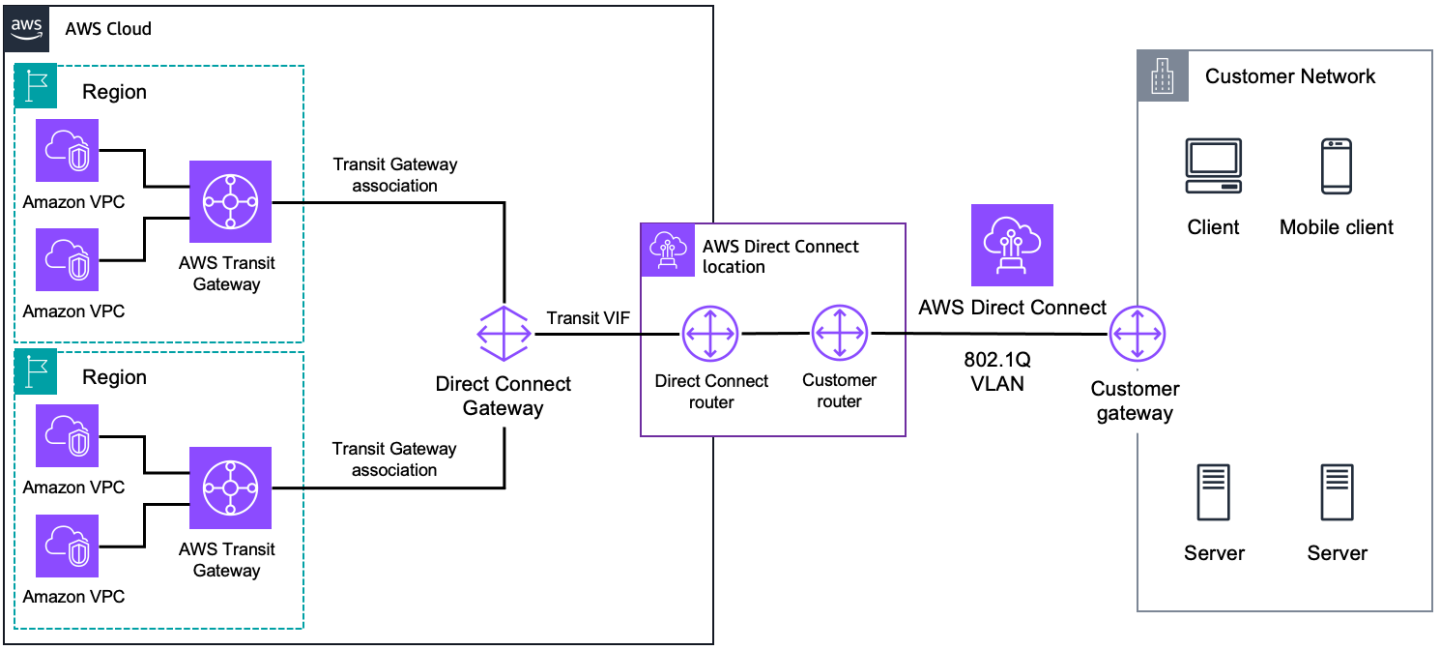
- Die private und Transit-VIFs-IPv4-Konfiguration verwendet entweder von AWS generierte IPv4-Adressen oder von Ihnen konfigurierte Adressen. Für öffentliches VIFs-IPv4-BGP-Peering müssen Sie ein eindeutiges öffentliches /31-IPv4-CIDR angeben, das Sie besitzen (oder eine Anforderung senden, dass ein CIDR-Block zugewiesen wird).
- Für alle Arten von VIFs IPv6 BGP-Peering weist AWS ein /125 CIDR zu, das nicht konfigurierbar ist.

## Weitere Ressourcen

- AWS Direct Connect Benutzerhandbuch
- AWS Direct Connect Virtuelle Schnittstellen
- AWS Direct Connect -Gateways
- AWS Direct Connect Ausfallsicherheit-Toolkit
- AWS Direct Connect MAC-Sicherheit
- AWS Direct Connect Standorte
- AWS Direct Connect Lieferpartner

# AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect + Durch die Verwendung AWS Transit Gatewayder Transit-VIF-Anfügung an das Direct-Connect-Gateway kann Ihr Netzwerk mehrere regionale zentralisierte Router über eine private dedizierte Verbindung verbinden. Das folgende Diagramm zeigt die Verbindung zu zwei Routern.




AWS Direct Connect and AWS Transit Gateway

Jedes AWS Transit Gateway ist ein Netzwerk-Transit-Hub, um VPCs in derselben Region miteinander zu verbinden, wodurch die Amazon-VPC-Routing-Konfiguration an einem Ort konsolidiert wird. Diese Lösung vereinfacht die Verwaltung von Verbindungen zwischen einer

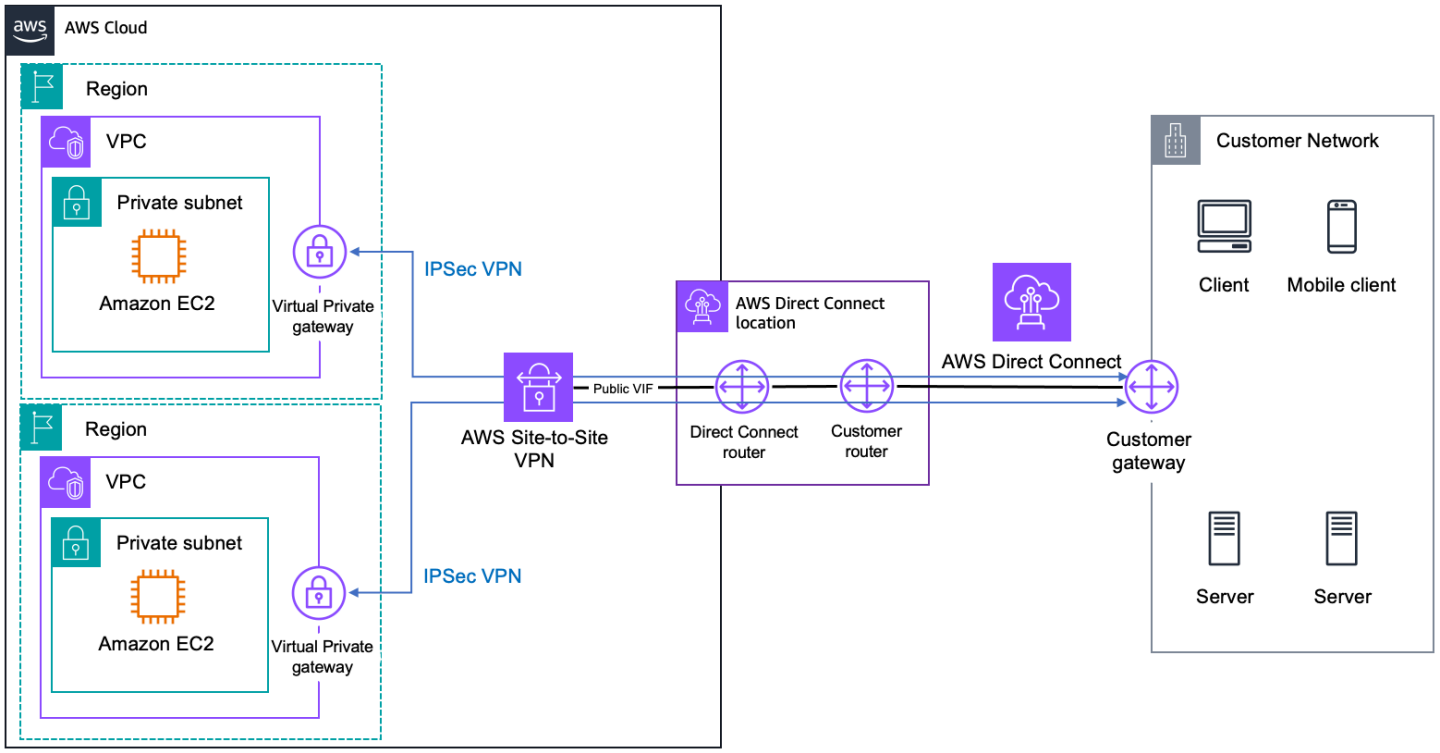
Amazon VPC und Ihren Netzwerken über eine private Verbindung, die die Netzwerkkosten senken, den Bandbreitendurchsatz erhöhen und ein konsistenteres Netzwerkerlebnis bieten kann als internetbasierte Verbindungen.

### Weitere Ressourcen

- AWS Direct Connect-Benutzerhandbuch
- Verknüpfen von Aggregationsgruppen in AWS Direct Connect
- Blog-Beitrag: Integration von Verbindungen mit einer gehosteten Gbit/s in AWS Transit Gateway

## AWS Direct Connect + AWS Site-to-Site 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 Öffentliche VIFs stellen eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS-Ressourcen wie einem AWS Site-to-Site VPN-Endpunkt her. Sobald Sie die Verbindung zum Service hergestellt haben, können Sie IPsec-Verbindungen zu den entsprechenden Virtual Private Gateways von Amazon VPC erstellen. Die folgende Abbildung veranschaulicht diese Option.




AWS Direct Connect and AWS Site-to-Site VPN

Diese Lösung kombiniert die Vorteile der end-to-end sicheren IPsec-Verbindung mit geringer Latenz und erhöhter Bandbreite des , AWS Direct Connect um ein konsistenteres Netzwerkerlebnis als internetbasierte VPN-Verbindungen zu bieten. Zwischen AWS Direct Connect und Ihrem Router auf der öffentlichen VIF wird eine BGP-Verbindungssitzung hergestellt. Zwischen dem Virtual Private Gateway und Ihrem Router in den IPsec-VPN-Tunneln wird eine weitere BGP-Sitzung oder eine statische Route eingerichtet.

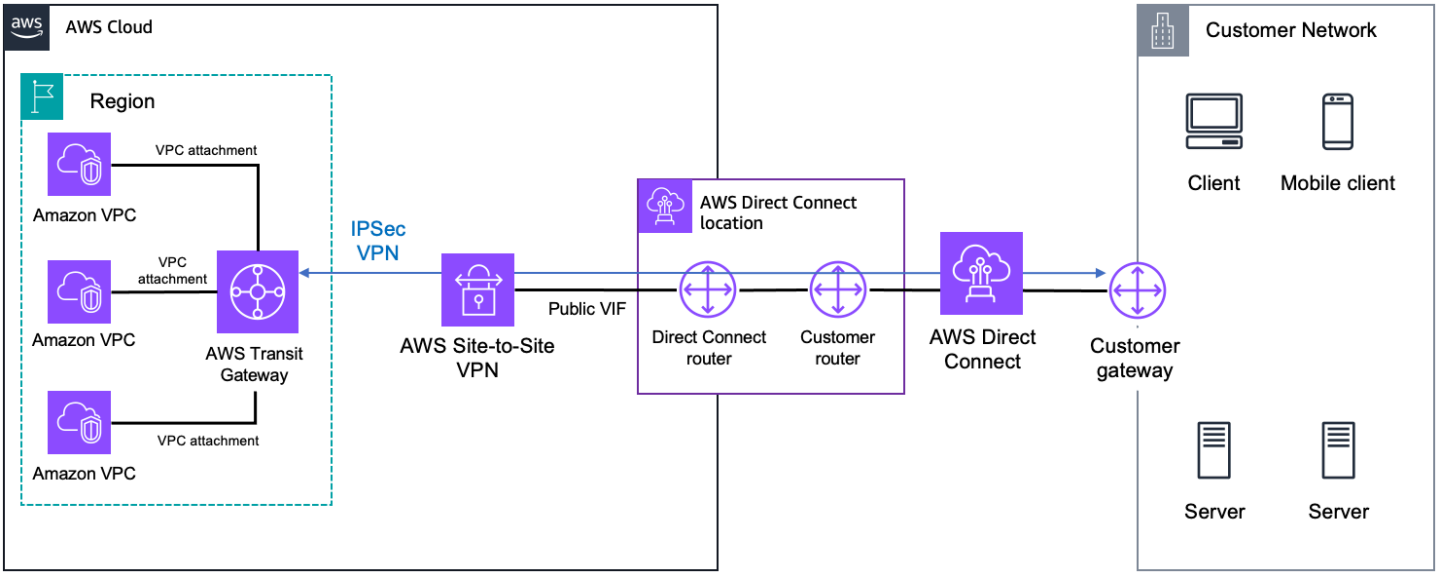
### Weitere Ressourcen

- AWS Direct Connect
- AWS Direct Connect Virtuelle Schnittstellen
- Benutzerhandbuch zu AWS Site-to-Site-VPN

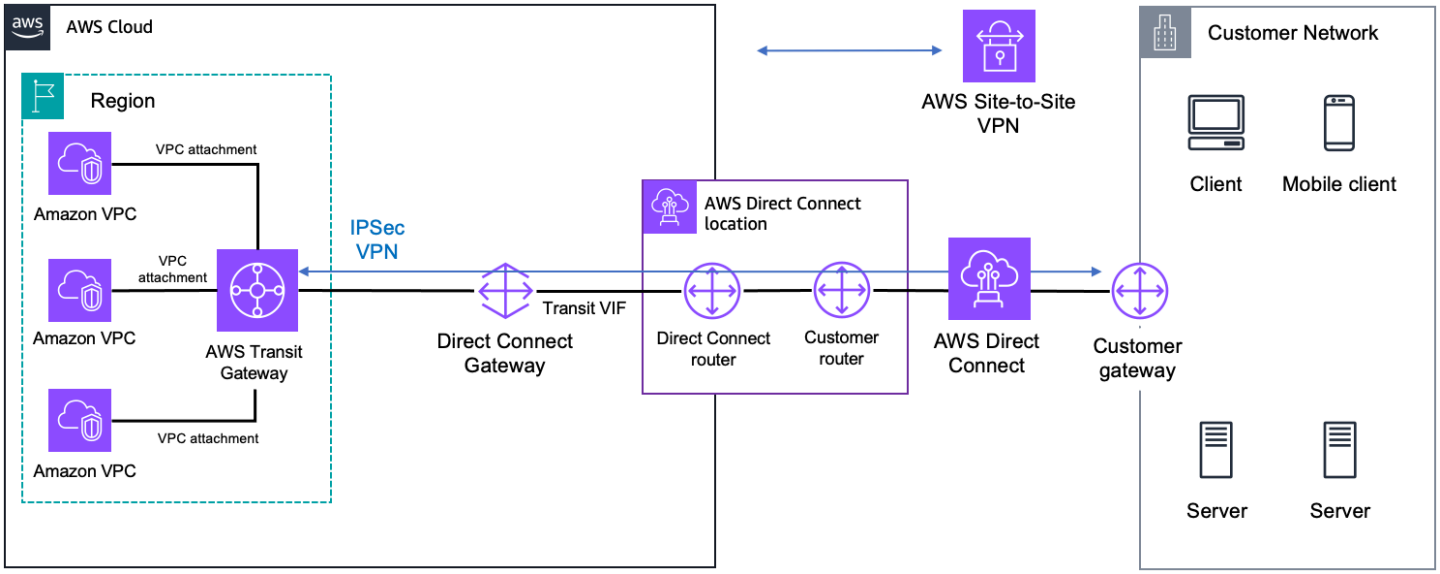
## AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

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 zentralisierten Router für Amazon VPCs über eine private dedizierte Verbindung aktivieren.

Sie können AWS Direct Connect öffentliche VIFs verwenden, um zunächst eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS-Ressourcen wie AWS Site-to-Site VPN-Endpunkten herzustellen. Sobald diese Verbindung hergestellt wurde, können Sie eine IPsec-Verbindung zu erstellen AWS Transit Gateway. 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)

Erwägen Sie diesen Ansatz, wenn Sie die Verwaltung vereinfachen und die Kosten von IPsec-VPN-Verbindungen zu mehreren Amazon VPCs in derselben Region minimieren möchten, wobei die Vorteile einer privaten dedizierten Verbindung gegenüber einem internetbasierten VPN mit geringer Latenz und konsistenter Netzwerkerfahrung bestehen. Eine BGP-Sitzung wird zwischen AWS Direct Connect und Ihrem Router mithilfe der öffentlichen oder der Transit-VIF eingerichtet. Zwischen AWS Transit Gateway und Ihrem Router im IPsec-VPN-Tunnel wird eine weitere BGP-Sitzung oder eine statische Route eingerichtet.

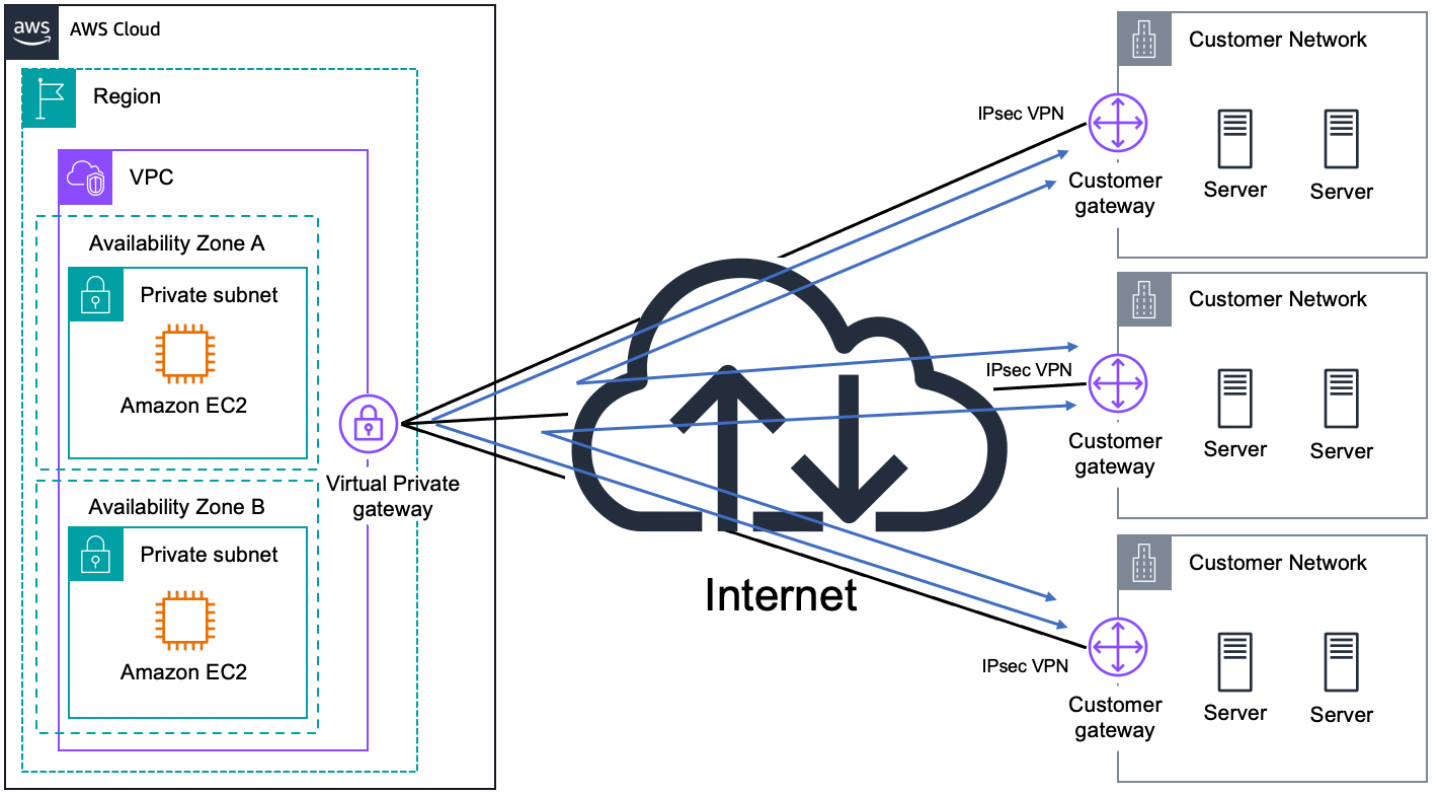
## Weitere Ressourcen

- Virtuelle AWS Direct Connect-Schnittstellen
- Transit-Gateway-VPN-Anfügungen
- Anforderungen für Kunden-Gateway-Geräte
- Mit Amazon VPC getestete Kunden-Gateway-Geräte
- AWS Site-to-Site VPN – Privates IP-VPN mit AWS Direct Connect

# AWS VPN CloudHub

Aufbauend auf den zuvor beschriebenen AWS-verwalteten VPN-Optionen können Sie mithilfe der sicher von einem Standort zum anderen kommunizieren AWS VPN CloudHub. Die AWS VPN CloudHub arbeitet mit einem einfachen hub-and-spoke Modell, das Sie mit oder ohne VPC verwenden können. Verwenden Sie diesen Ansatz, wenn Sie mehrere Niederlassungen und bestehende Internetverbindungen haben und ein praktisches, potenziell kostengünstiges hub-and-spoke Modell für die primäre oder Backup-Konnektivität zwischen diesen Remote-Standorten implementieren möchten.

Die folgende Abbildung zeigt die AWS VPN CloudHub Architektur, wobei Linien den Netzwerkverkehr zwischen Remote-Standorten angeben, der über ihre AWS VPN Verbindungen geleitet wird.




AWS VPN CloudHub

AWS VPN CloudHub verwendet ein Amazon VPC Virtual Private Gateway mit mehreren Kunden-Gateways, die jeweils eindeutige autonome BGP-Systemnummern (ASNs ) verwenden. Die Remote-Standorte dürfen keine überlappenden IP-Bereiche haben. Ihre Gateways geben die entsprechenden Routen (BGP-Präfixe) über ihre VPN-Verbindungen bekannt. Diese Routing-Ankündigungen werden empfangen und jedem BGP-Peer erneut angekündigt, sodass jeder Standort Daten an die anderen Standorte senden und Daten von diesen empfangen kann.

## Weitere Ressourcen

- Sichere Kommunikation zwischen Standorten mithilfe von VPN CloudHub
- Benutzerhandbuch zu AWS Site-to-Site-VPN
- Anforderungen für Kunden-Gateway-Geräte
- Mit Amazon VPC getestete Kunden-Gateway-Geräte

# AWS Transit Gateway + SD-WAN-Lösungen

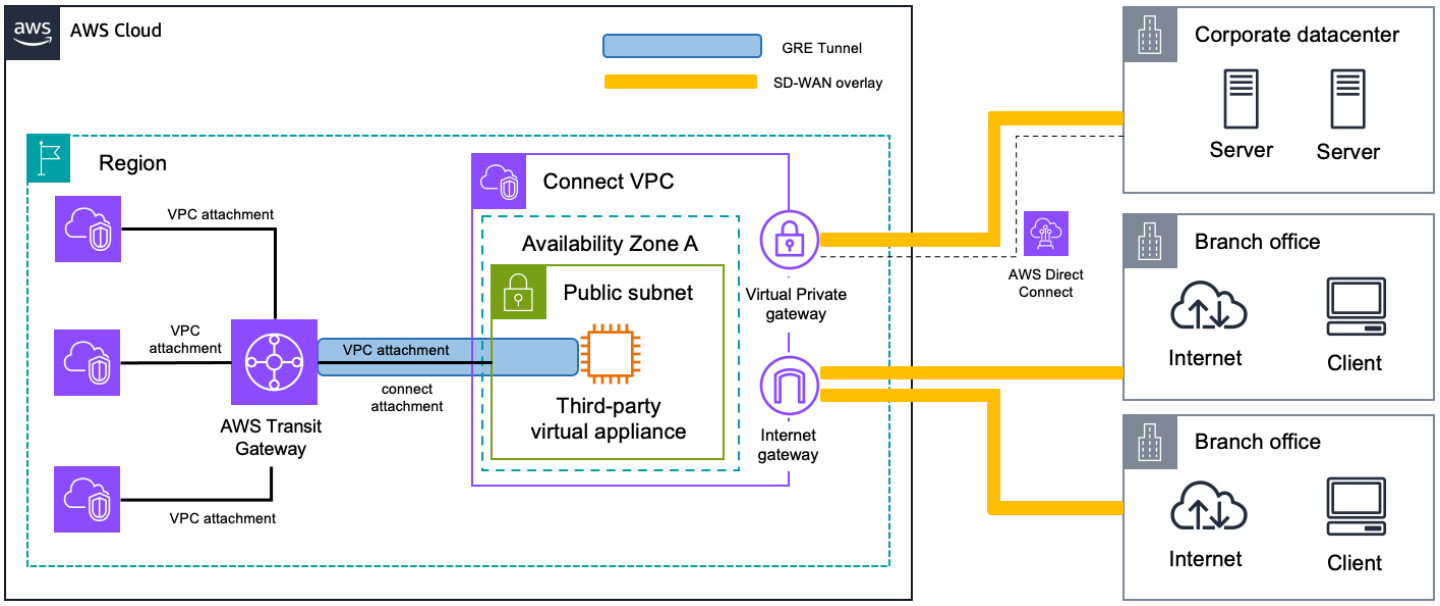
Software Defined Wide Area Networks (SD-WANs) werden verwendet, um Ihre Rechenzentren, Niederlassungen oder Colocation-Umgebungen über verschiedene Transitnetzwerke zu verbinden (z. B. das öffentliche Internet, MPLS-Netzwerke oder das AWS-Backbone mithilfe von AWS Direct Connect). Der Datenverkehr wird automatisch und dynamisch über den geeignetsten und effizientesten Pfad basierend auf Netzwerkbedingungen, Anwendungstyp oder Servicequalität (QoS) verwaltet.

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

Wenn Sie über die Verbindung eines SD-WAN-Netzwerks mit AWS sprechen, AWS Transit Gateway stellt einen verwalteten, hochverfügbaren und skalierbaren regionalen Netzwerk-Transit-Hub bereit, um VPCs und Ihr SD-WAN-Netzwerk miteinander zu verbinden. Transit Gateway Connect-Anfügungen 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 IPsec-VPNs einrichten zu müssen.

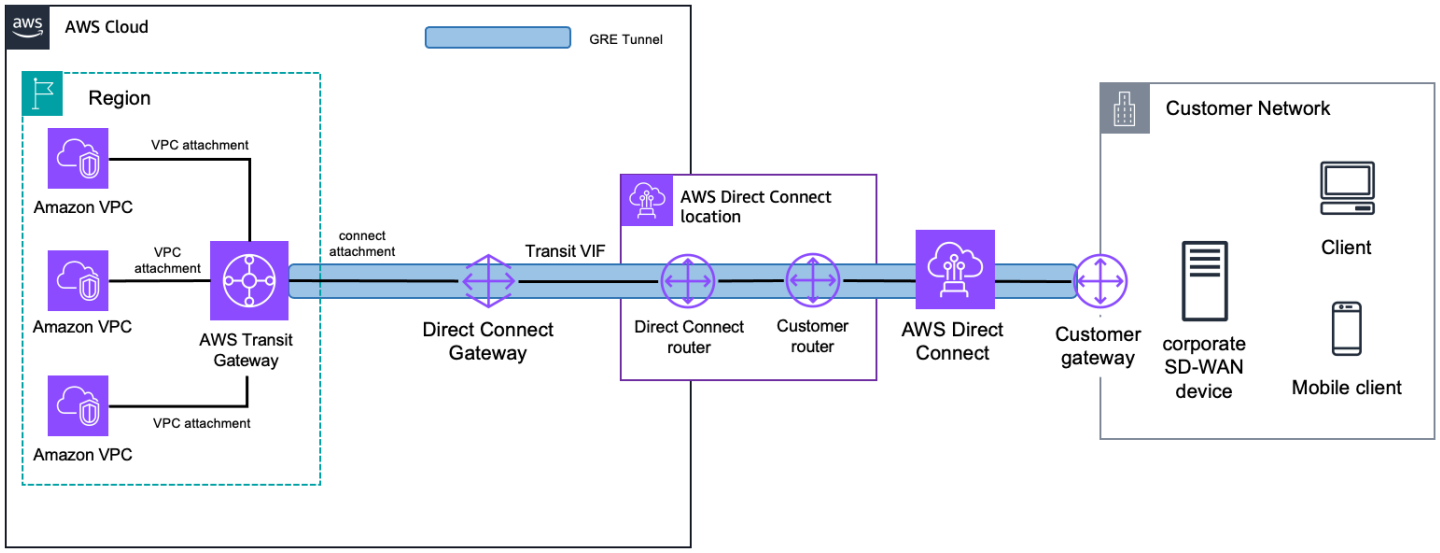
Transit-Gateway-Verbindungsanhänge unterstützen Generic Routing Encapsulation (GRE) für eine höhere Bandbreitenleistung im Vergleich zu einer VPN-Verbindung. Es unterstützt das Border Gateway Protocol (BGP) für dynamisches Routing und macht die Konfiguration statischer Routen überflüssig. Dies vereinfacht das Netzwerkdesign und senkt die damit verbundenen Betriebskosten. Darüber hinaus bietet die Integration mit Transit Gateway Network Manager erweiterte Transparenz über globale Netzwerktopologie, Leistungsmetriken auf Anhangsebene 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 eine VPC-Anfügung als zugrunde liegenden Transport für die Transit-Gateway-Verbindungsanfügung zwischen den virtuellen Appliances und dem Transit Gateway, wie in der folgenden Abbildung gezeigt.




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

Alternativ können Sie Ihren SD-WAN-Datenverkehr zu AWS erweitern und segmentieren, ohne zusätzliche Infrastruktur hinzuzufügen. Sie können Transit-Gateway-Verbindungsanhänge mithilfe einer - AWS Direct Connect Verbindung als zugrunde liegenden Transport erstellen, wie in der folgenden Abbildung gezeigt.




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

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

- Sie können eine Verbindungsanfügung auf vorhandenen Transit Gateways erstellen.

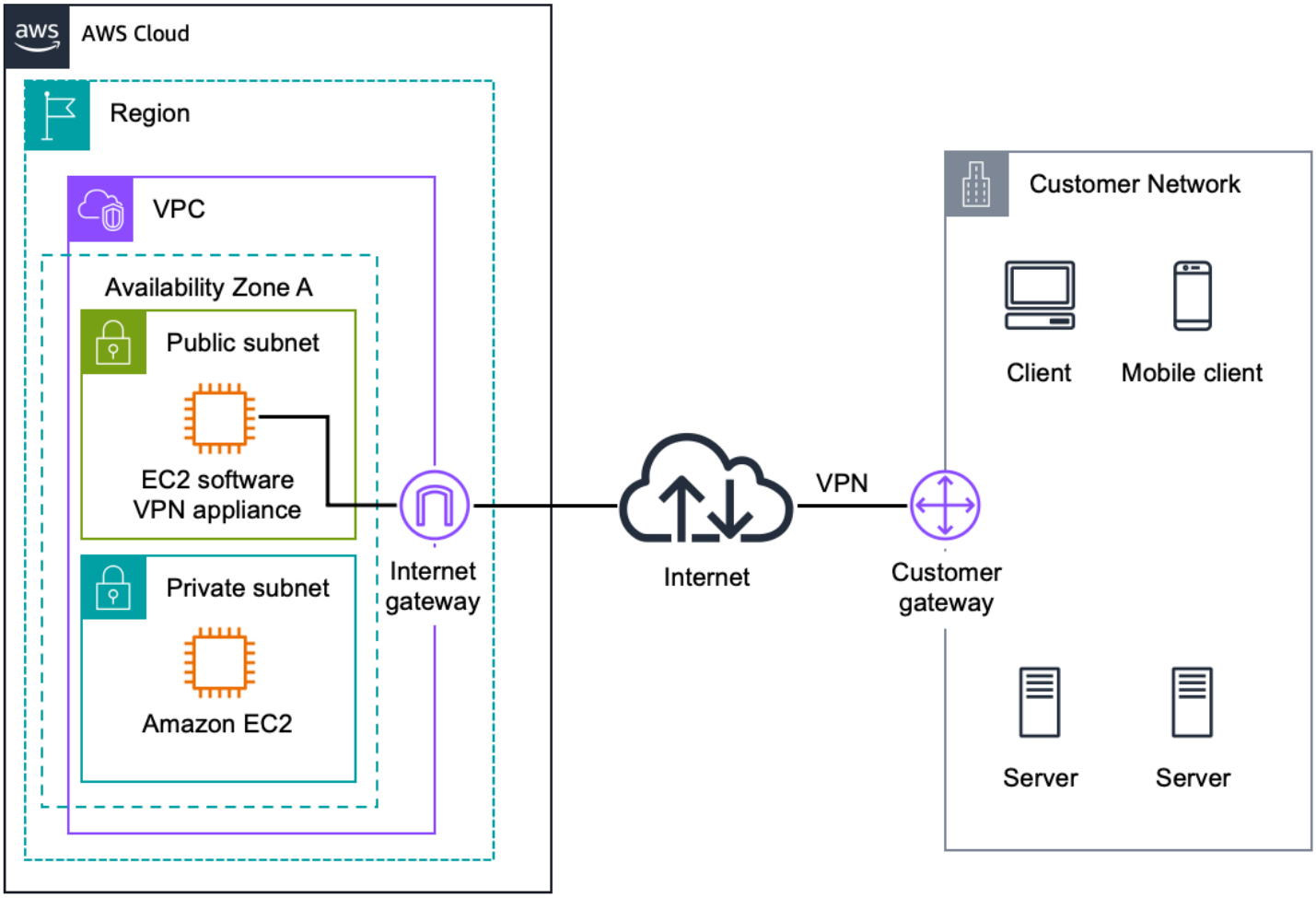
- Drittanbieter-Appliances müssen mit einem GRE-Tunnel konfiguriert sein, um Datenverkehr von Transit Gateway mithilfe von Verbindungsanhängen senden und empfangen zu können. Die Appliance muss mit BGP für dynamische Routenaktualisierungen und Zustandsprüfungen konfiguriert sein.
- Connect-Anfügungen unterstützen keine statischen Routen.
- Transit-Gateway-Connect-Anfügungen unterstützen eine maximale Bandbreite von fünf Gbit/s pro GRE-Tunnel. Bandbreite über fünf Gbit/s kann erreicht werden, indem dieselben Präfixe über mehrere Connect-Peer (GRE-Tunnel) für dieselbe Connect-Anfügung angekündigt werden.
- Für jede Verbindungsanfügung werden maximal vier Connect-Peers unterstützt.
- Transit-Gateway-Verbindungsanhänge unterstützen IPv6- und dynamische Routenankündigungen über Multiprotokollerweiterungen für BGP (MBGP oder MP-BGP).

### Weitere Ressourcen

- Transit-Gateway-Peering-Anfügungen
- Anforderungen und Überlegungen
- Blog-Beitrag: Vereinfachen der 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 ausgeführt wird. Diese Option wird empfohlen, wenn Sie beide Enden der VPN-Verbindung verwalten müssen, entweder zu Compliance-Zwecken oder zur Nutzung von Gateway-Geräten, die derzeit nicht von der VPN-Lösung von Amazon VPC unterstützt werden. Die folgende Abbildung zeigt diese Option.




Software-Site-to-Site-VPN

Sie können aus einem Ökosystem mehrerer Partner und Open-Source-Communitys wählen, die Software-VPN-Appliances erstellt haben, die auf Amazon EC2 ausgeführt werden. Zusammen mit dieser Auswahl liegt die Verantwortung darin, dass Sie die Software-Appliance verwalten müssen, einschließlich Konfiguration, Patches und Upgrades.

Beachten Sie, dass dieses Design einen potenziellen einzelnen Fehlerpunkt in das Netzwerkdesign einführt, da die Software-VPN-Appliance auf einer einzigen Amazon EC2-Instance ausgeführt wird. Weitere Informationen finden Sie unter Anhang A: High-Level-HA-Architektur für Software-VPN-Instances Architektur für Software-VPN-Instances.

## Weitere Ressourcen

- VPN-Appliances sind in der verfügbar AWS Marketplace
- Tech brief – Verbinden von Cisco ASA mit einer VPC-EC2-Instance (IPsec)

- Tech kurze – Verbinden mehrerer VPCs mit EC2-Instances (IPsec)
- Tech brief – Verbinden mehrerer VPCs mit EC2-Instances (SSL)

# Amazon-VPC-zu-Amazon-VPC-Konnektivitätsoptionen

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

Die VPC-Konnektivität zwischen VPCs wird am besten erreicht, wenn für jede VPC, die verbunden wird, nicht überlappende IP-Bereiche verwendet werden. Wenn Sie beispielsweise mehrere VPCs verbinden möchten, stellen Sie sicher, dass jede VPC mit eindeutigen CIDR-Bereichen (Classless Inter-Domain Routing) konfiguriert ist. Daher empfehlen wir Ihnen, einen einzelnen, zusammenhängenden, nicht überlappenden CIDR-Block zuzuweisen, der von jeder VPC verwendet werden soll. Weitere Informationen zu Amazon-VPC-Routing und -Einschränkungen finden Sie unter Häufig gestellte Fragen zu Amazon VPC.

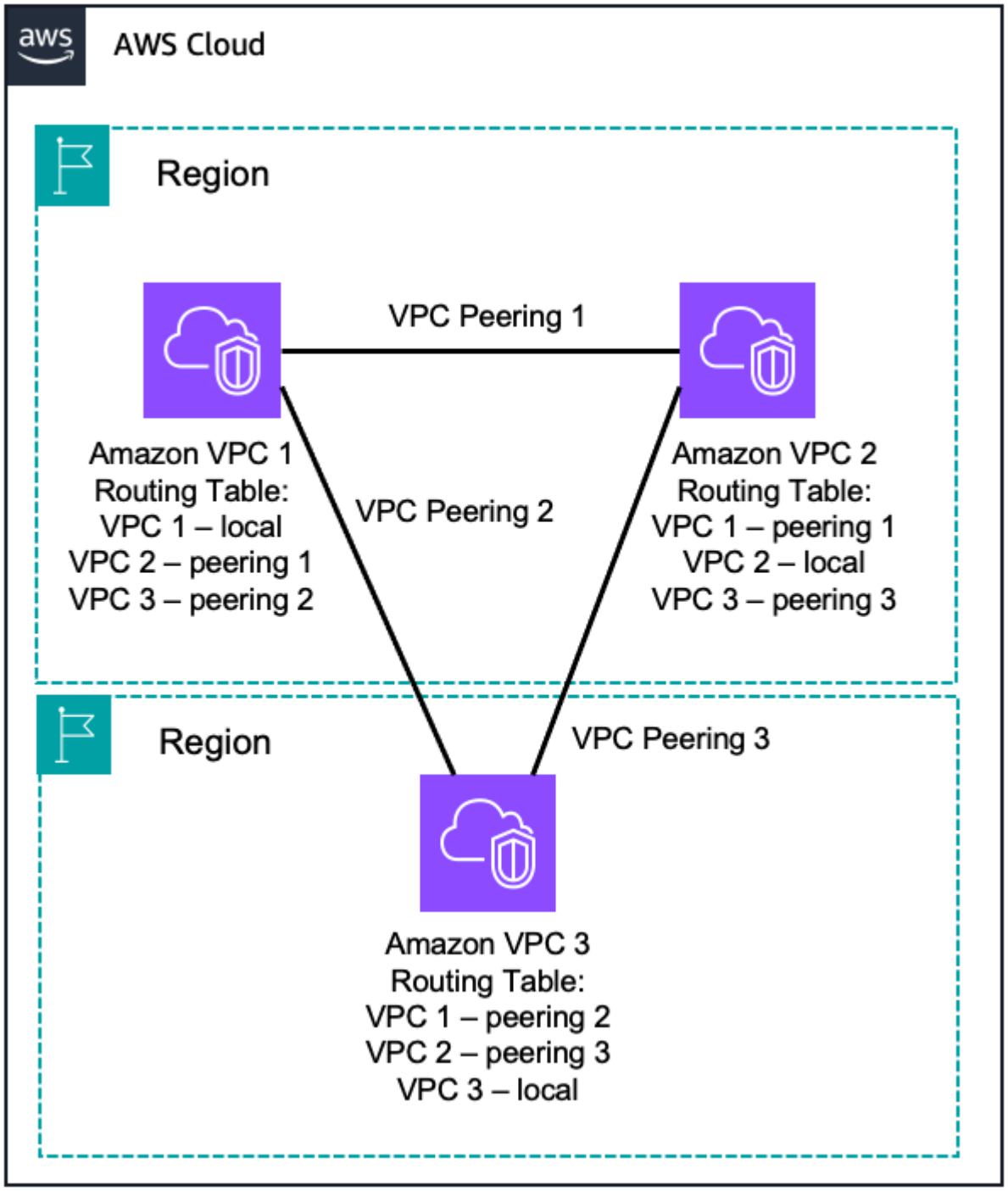
| Option | Anwendungsfall | Vorteile | Einschränkungen |
|---|---|---|---|
| VPC-Peering | Von AWS bereitges tellte Netzwerkk onnektivität zwischen zwei VPCs. | Nutzt die von AWS verwaltete skalierbare Netzwerkinfrastruktur | VPC-Peering unterstützt keine transitiven Peering-B eziehungen<br><br>Schwierigkeiten bei der skalierbaren Verwaltung |
| AWS Transit Gateway | Von AWS bereitges tellte regionale Router-Konnektivität für VPCs | Von AWS verwaltet er Service für hohe Verfügbarkeit und Skalierbarkeit<br><br>Regionaler Netzwerk-Hub für bis zu 5 000 Anlagen | Transit-Gateway-Pe ering unterstützt nur statische Routen |

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

# VPC-Peering

Eine VPC Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Sie ermöglicht die Weiterleitung über die privaten IP-Adressen jeder VPC, als befänden sie sich im selben Netzwerk. VPC-Peering-Verbindungen können zwischen Ihren eigenen VPCs oder mit einer VPC in einem anderen AWS-Konto erstellt werden. VPC-Peering unterstützt auch regionsübergreifendes Peering.

Der Datenverkehr, der regionsübergreifendes VPC-Peering verwendet, verbleibt immer im globalen AWS-Backbone und durchläuft niemals das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und DDoS-Angriffe reduziert werden.




VPC-to-VPC Peering

AWS verwendet die vorhandene Infrastruktur einer VPC zum Erstellen von VPC-Peering-Verbindungen und benötigt keine separate physische Hardware. Daher führen sie nicht zu einem potenziellen einzelnen Fehlerpunkt oder Netzwerkbandbreitenengpass zwischen VPCs. Darüber hinaus können VPC-Routing-Tabellen, Sicherheitsgruppen und Netzwerkzugriffskontrolllisten genutzt

werden, um zu steuern, welche Subnetze oder Instances die VPC-Peering-Verbindung verwenden können.

Amazon VPCs unterstützen kein transitives Peering, was bedeutet, dass Sie nicht zwei VPCs kommunizieren können, die nicht direkt über eine dritte VPC als Transit verbunden sind. Wenn Sie möchten, dass alle Ihre VPCs mithilfe von VPC-Peering miteinander kommunizieren, müssen Sie 1:1-VPC-Peering-Verbindungen zwischen ihnen erstellen. Alternativ können Sie AWS Transit Gateway oder AWS Cloud WAN verwenden, um als Netzwerktransit-Hub zu fungieren.

Sowohl IPv4- als auch IPv6-Datenverkehr wird in VPC-Peering-Verbindungen unterstützt. Zwei VPCs können jedoch nicht per Peering verbunden werden, wenn sich ihr primärer IPv4-CIDR-Block überlappt, unabhängig von den verwendeten sekundären IPv4- oder IPv6-CIDR-Blöcken. Berücksichtigen Sie dies, wenn Sie Ihren VPCs den primären CIDR-Block zuweisen, wenn Sie VPC-Peering zwischen ihnen verwenden möchten.

### Weitere Ressourcen

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

## AWS Transit Gateway

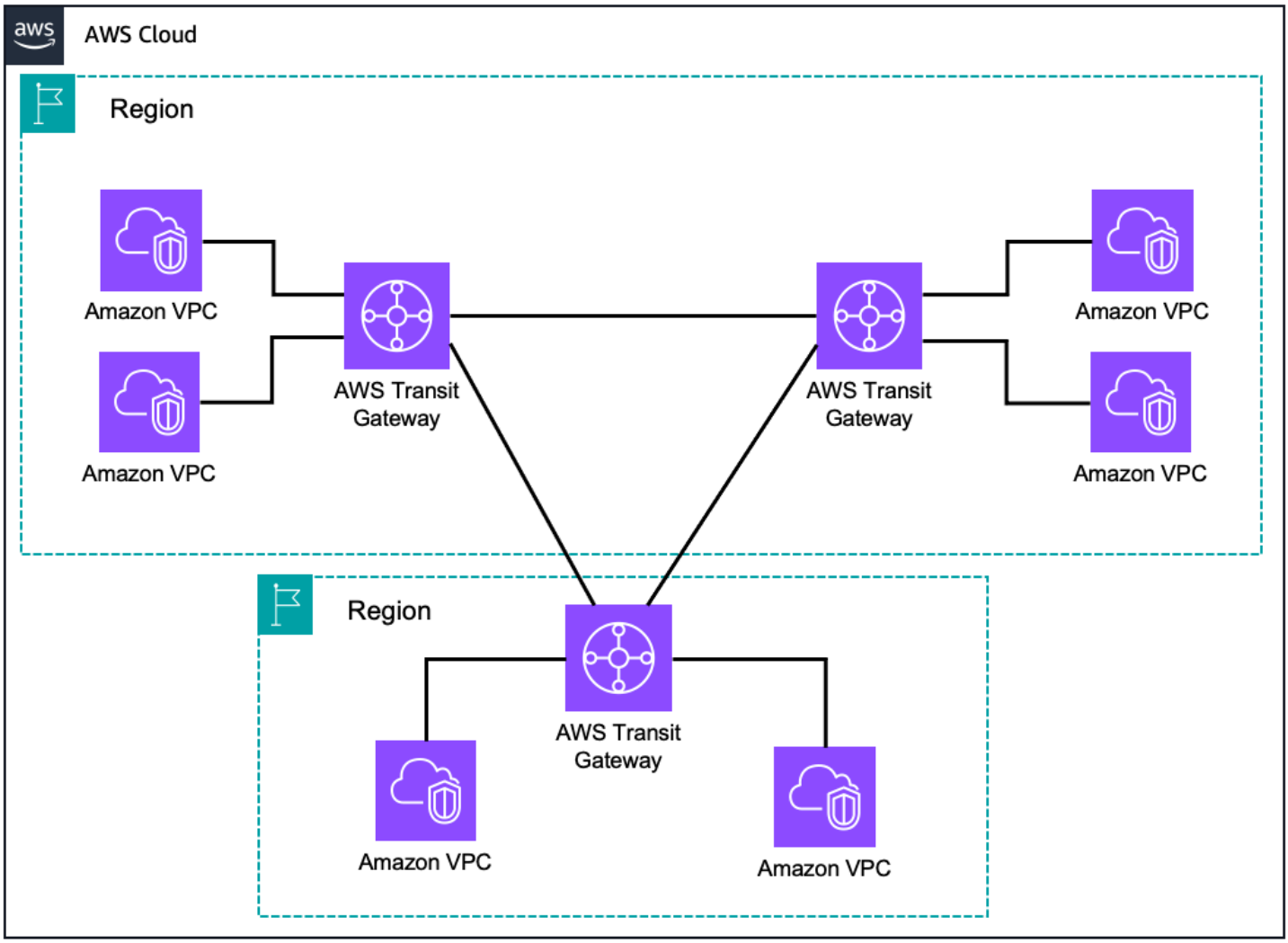
AWS Transit Gateway ist ein hochverfügbarer und skalierbarer Service zur Konsolidierung der AWS VPC-Routing-Konfiguration für eine Region mit einer hub-and-spoke Architektur. Jede Spoke-VPC muss nur eine Verbindung zum Transit Gateway herstellen, um Zugriff auf andere verbundene VPCs zu erhalten. Sowohl IPv4- als auch IPv6-Datenverkehr wird in unterstütztAWS Transit Gateway.

Sie können mehrere Transit-Gateway-Routing-Tabellen, -Zuordnungen und -Verbreitungen nutzen, um Ihren Datenverkehr innerhalb desselben Transit Gateways zu segmentieren. Sie können verschiedene Routing-Domains (z. B. Produktions- und Nicht-Produktionsdatenverkehr) von einem einzigen Verwaltungspunkt aus verwalten, um sicherzustellen, dass diese Routing-Domains nicht miteinander kommunizieren können.

Sie können auch die von Transit Gateway erstellte hub-and-spoke Architektur nutzen, um den Zugriff auf gemeinsam genutzte Services wie Datenverkehrsprüfung, Schnittstellen-VPC-Endpunktzugriff oder ausgehenden Datenverkehr über ein NAT-Gateway oder NAT-Instances zu zentralisieren. Diese Zentralisierung vereinfacht die komplexe Verwaltung dieser Ressourcen in mehreren VPCs und ermöglicht eine bessere Kontrolle, wenn Sie Ihren Platz in AWS erweitern.

Transit Gateways können innerhalb derselben AWS-Region oder zwischen verschiedenen AWS-Regionen miteinander verbunden werden. -AWS Transit GatewayDatenverkehr verbleibt immer im globalen AWS-Backbone und durchläuft niemals das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und DDoS-Angriffe reduziert werden.

Mit einer großen Anzahl von VPCs bietet Transit Gateway eine einfachere VPC-zu-VPC-Kommunikationsverwaltung über VPC Peering, wie in der folgenden Abbildung gezeigt.




AWS Transit Gateway

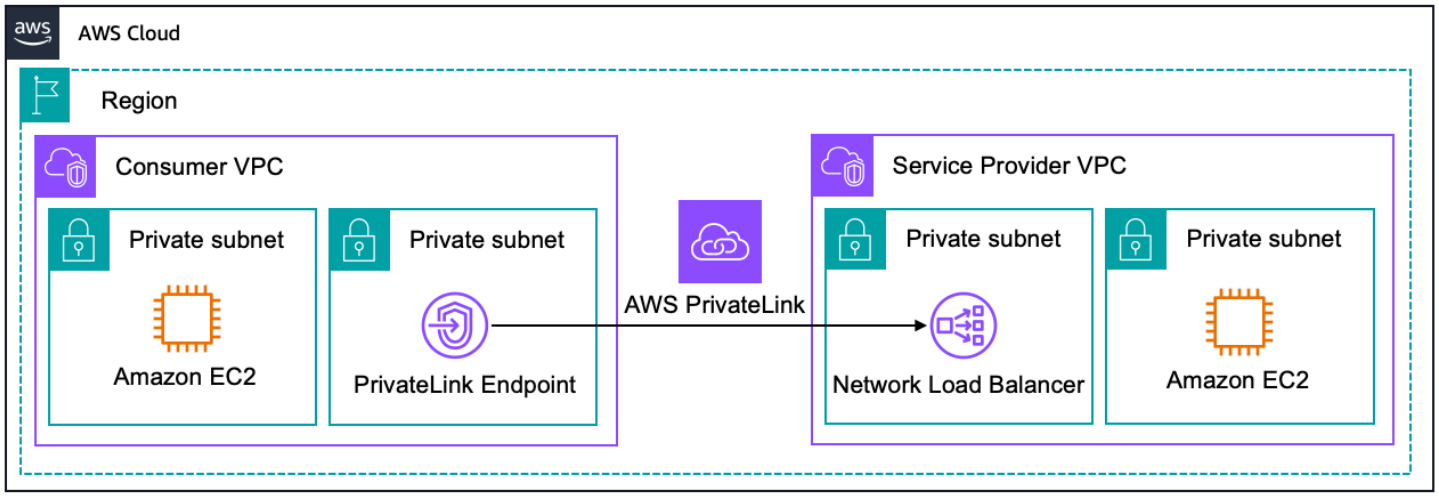
Um einen zentralen Einblick in den IP-Datenverkehr zu und von Ihren Transit Gateways zu erhalten, können Sie Flow-Protokolle für Transit Gateway in Amazon CloudWatch Logs und Amazon S3 veröffentlichen. Flow-Potokolldaten werden außerhalb des Pfades des Netzwerkdatenverkehrs erfasst und wirken sich daher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

## Weitere Ressourcen

- Amazon-VPC-Transit-Gateway
- Transit-Gateway-Peering-Anhänge
- Arbeiten mit Transit Gateways
- Protokollieren des Netzwerkverkehrs mit Flow-Protokollen für Transit Gateway

# AWS PrivateLink

AWS PrivateLink Mit können Sie über private IP-Adressen in Ihrer VPC eine Verbindung zu einigen AWS-Services, Services, die von anderen AWS-Konten gehostet werden (bezeichnet als Endpunktservices), und unterstützten AWS Marketplace Partnerservices herstellen. Die Schnittstellenendpunkte werden direkt in Ihrer VPC mithilfe von Elastic Network-Schnittstellen und IP-Adressen in den Subnetzen Ihrer VPC erstellt. Das bedeutet, dass VPC-Sicherheitsgruppen verwendet werden können, um den Zugriff auf die Endpunkte zu verwalten.




AWS PrivateLink

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

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

verwenden. Nachdem diese Voraussetzungen erfüllt sind, kann IPv6 in der Servicekonfiguration für den Endpunkt aktiviert werden.

## Zugriffskontrollen für AWS PrivateLink

Die Schnittstellenendpunkte werden direkt innerhalb Ihrer VPC mithilfe von Elastic Network-Schnittstellen 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 anfügen. 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 keine IAM-Benutzerrichtlinien oder servicespezifische Richtlinien (z. B. Amazon S3-Bucket-Richtlinien). Wenn Sie einen Schnittstellenendpunkt verwenden, um eine Verbindung zu Amazon S3 herzustellen, können Sie auch Amazon-S3-Bucket-Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten oder VPCs zu steuern.

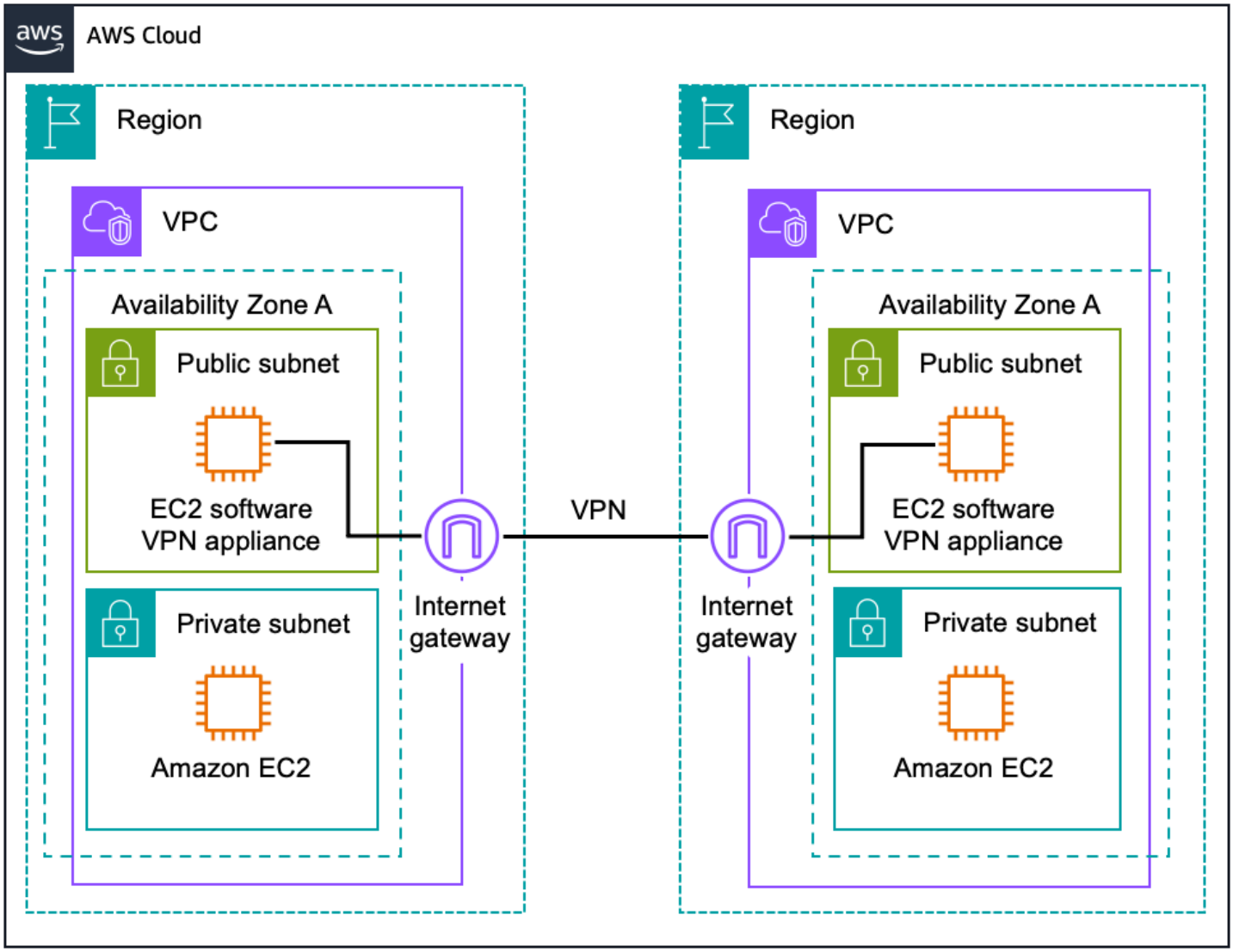
## Weitere Ressourcen

- Schnittstellen-VPC-Endpunkte (AWS PrivateLink)
- VPC-Endpunktservices (AWS PrivateLink)
- Blog-Beitrag: Beschleunigen Sie Ihre IPv6-Einführung mit - PrivateLink Services und -Endpunkten
- Blog-Beitrag: Verbinden von Netzwerken mit überlappenden IP-Bereichen
- 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 mehrere VPCs in einem größeren Virtual Private Network zu verbinden, sodass Instances in jeder VPC mithilfe privater IP-

Adressen nahtlos eine Verbindung miteinander herstellen 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-Communitys wählen, die Software-VPN-Appliances erstellt haben, die auf Amazon EC2 ausgeführt werden. Zusammen mit dieser Auswahl liegt die Verantwortung für Sie bei der Verwaltung der Software-Appliance, einschließlich Konfiguration, Patches und Upgrades.

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

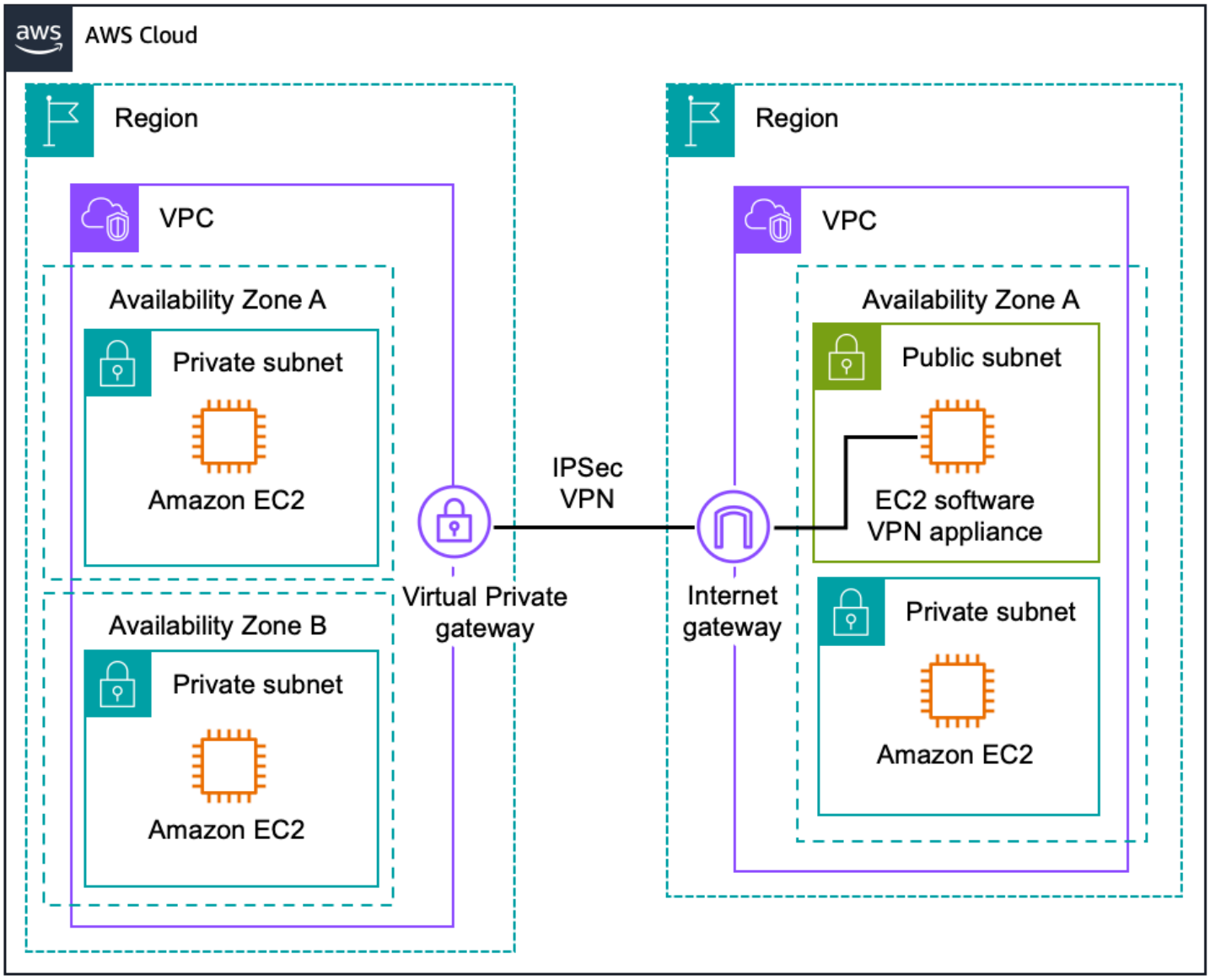
Weitere Informationen finden Sie unter Anhang A: High-Level-HA-Architektur für Software-VPN-Instances.

### Weitere Ressourcen

- VPN-Appliances, die über die verfügbar sind AWS Marketplace
- Tech brief – Verbinden mehrerer VPCs mit EC2-Instances (IPsec)
- Tech brief – Verbinden mehrerer VPCs mit EC2-Instances (SSL)

## Software-VPN-zu-AWS-Site-to-Site-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 Virtual Private Gateway erstellen, sodass Instances in jeder VPC mithilfe privater IP-Adressen nahtlos eine Verbindung miteinander herstellen können. Diese Option verwendet ein Virtual Private Gateway in einer Amazon VPC und eine Kombination aus Internet-Gateway und 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 dieses Design einen potenziellen einzelnen Fehlerpunkt in das Netzwerkdesign einführt. Weitere Informationen finden Sie unter Anhang A: High-Level-HA-Architektur für Software-VPN-Instances.

## Weitere Ressourcen

- VPN-Appliances, die über die verfügbar sind AWS Marketplace
- Benutzerhandbuch zu AWS Site-to-Site-VPN
- Anforderungen für Kunden-Gateway-Geräte

# Software-Fernzugriff auf Amazon VPC-Verbindungsoptionen

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 Netzwerk-zu-Amazon-VPC-Konnektivitätsoptionen Konnektivitätsoptionen kombinieren und Amazon-VPC-zu-Amazon-VPC-Konnektivitätsoptionen so ein Netzwerk erstellen, das sich über Remote-Netzwerke und mehrere VPCs erstreckt.

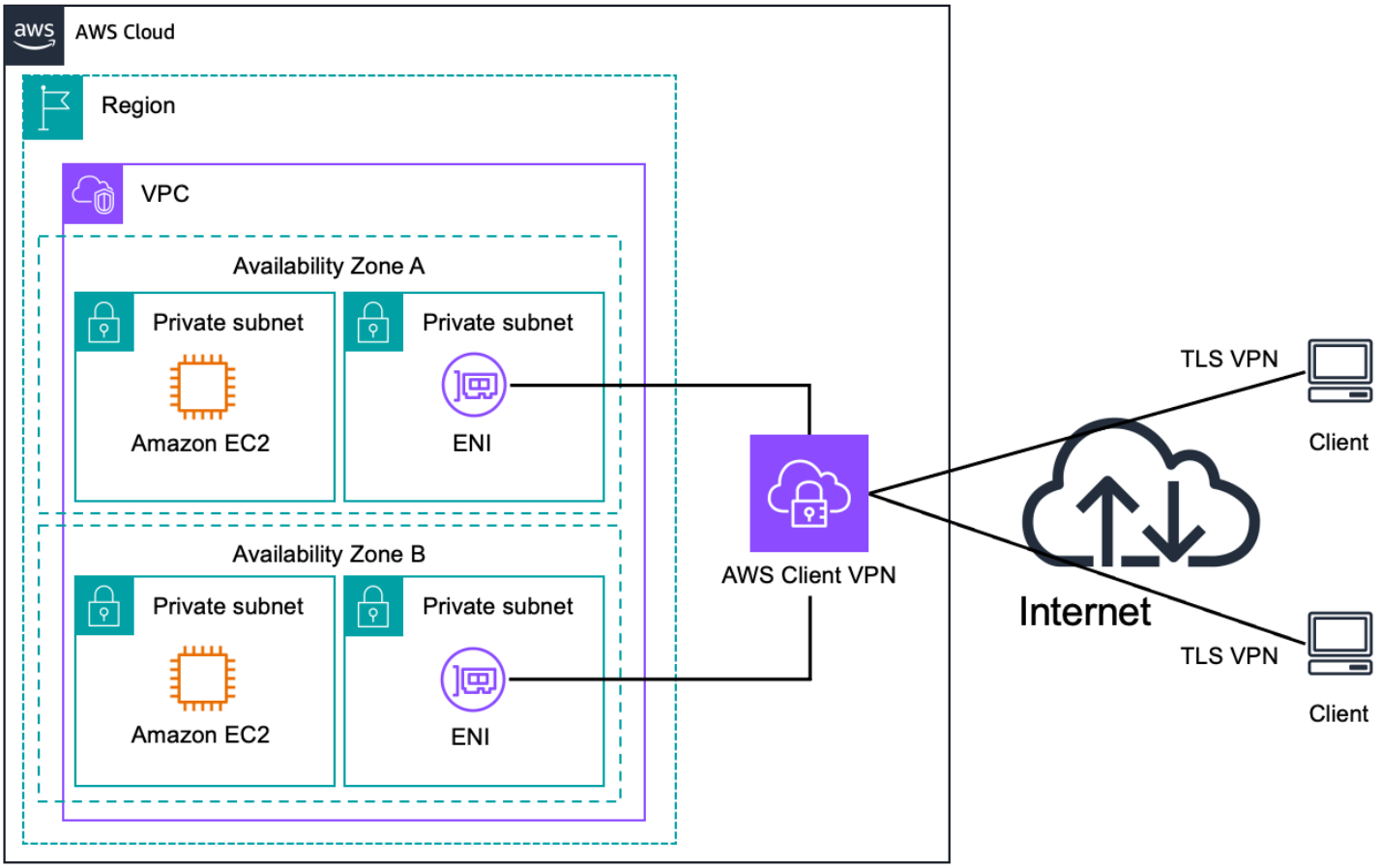
In der folgenden Tabelle werden die Vor- und Nachteile dieser Optionen beschrieben.

| 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 Amazon VPC und/oder interne Netzwerke | Unterstützt eine breitere Palette von VPN-Anbietern, -Produkten und -Protokollen<br><br>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 Ihren Amazon VPCs herzustellen, 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.

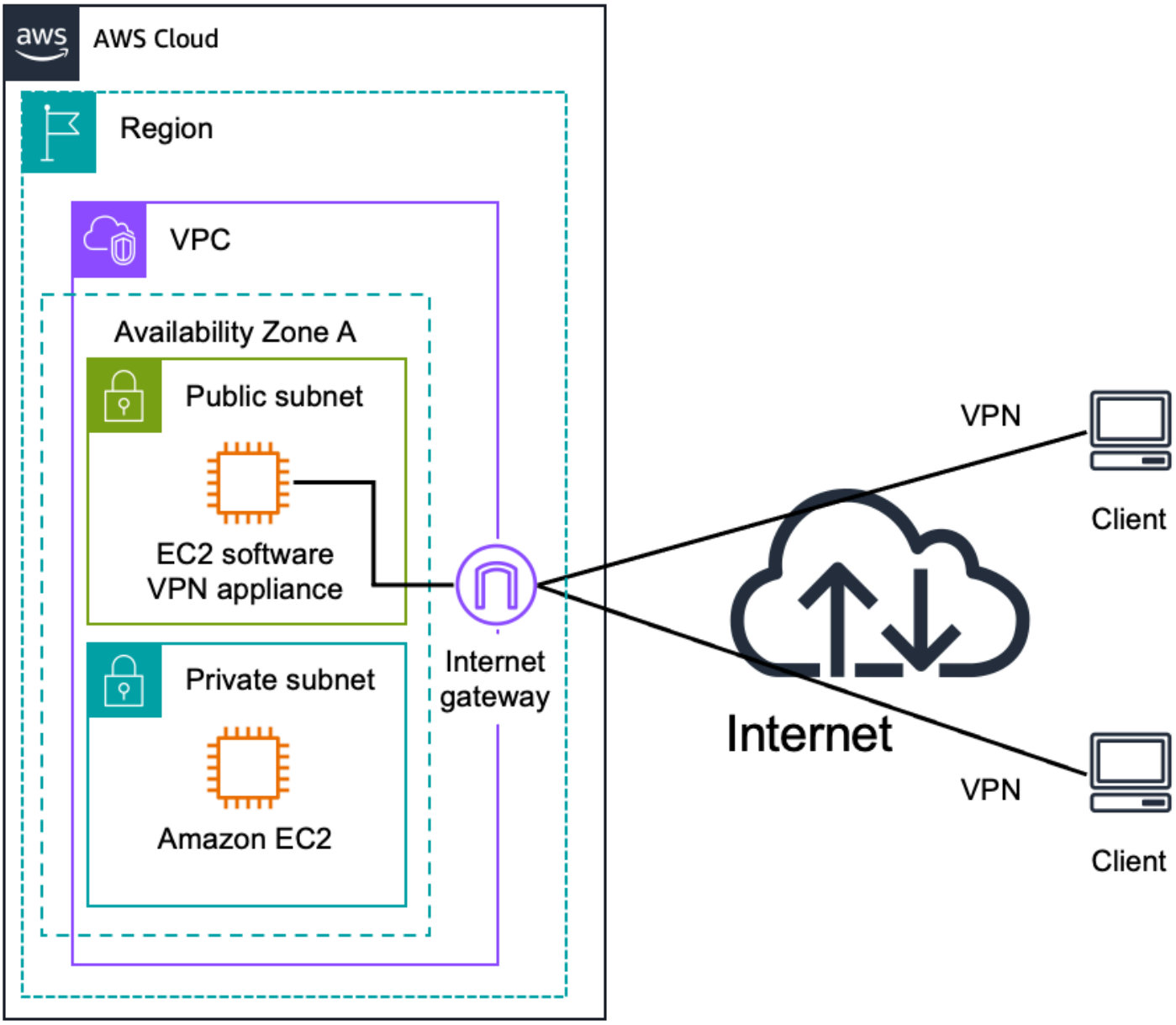
## Weitere Ressourcen

- 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 Ihre 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.

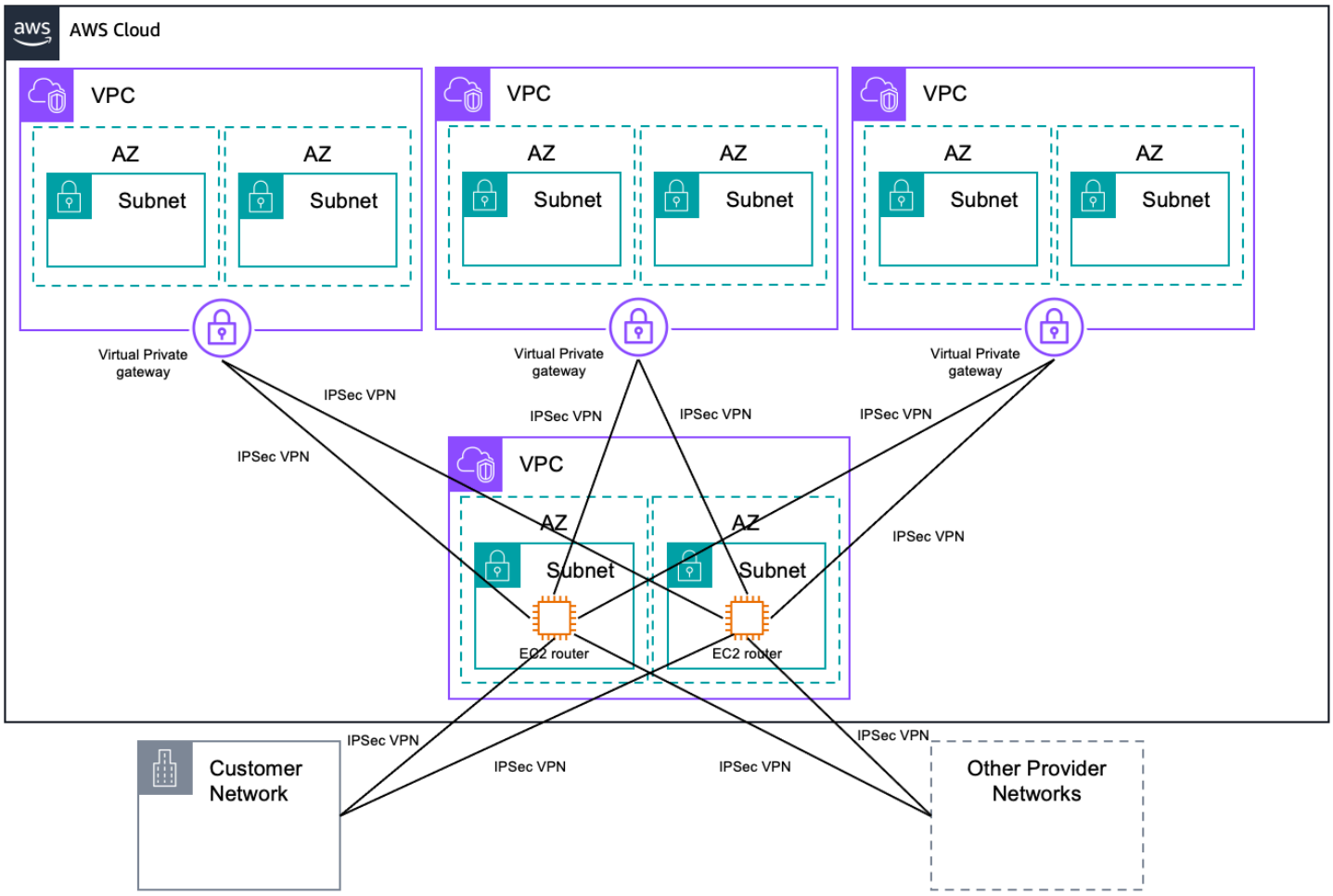
Sie sind verantwortlich für die Verwaltung der Fernzugriffssoftware, einschließlich Benutzerverwaltung, Konfiguration, Patches und Upgrades. Dieses Design führt eine potenzielle Schwachstelle in das Netzwerkdesign ein, da der RAS-Server auf einer einzigen Amazon EC2 EC2-Instance ausgeführt wird. Weitere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

## Weitere Ressourcen

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

# Transit-VPC

Basierend auf den oben genannten Software VPN-Designs können Sie ein globales Transit-Netzwerk in AWS erstellen. Eine Transit-VPC ist eine gängige Strategie für die Verbindung mehrerer geografisch verteilter VPCs und Remote-Netzwerke, um ein globales Netzwerk-Transit-Center zu erstellen. Eine Transit-VPC vereinfacht die Netzwerkverwaltung und minimiert die Anzahl von Verbindungen, die für die Vernetzung mehrerer VPCs mit Remote-Netzwerken erforderlich sind. Die folgende Abbildung veranschaulicht dieses Design.




Transit VPC

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

# Weitere Ressourcen

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

# AWS Cloud WAN

AWS Cloud WAN ist ein absichtsgesteuertes, verwaltetes Wide Area Network (WAN), das durch eine von Ihnen definierte Richtlinie beschrieben wird, die Ihr Rechenzentrum, Ihren Zweig und Ihre AWS-Netzwerke vereinheitlicht. Sie können zwar Ihr eigenes globales Netzwerk erstellen, indem Sie mehrere Transit Gateways über -Regionen hinweg miteinander verbinden, aber Cloud WAN bietet integrierte Funktionen für Automatisierung, Segmentierung und Konfigurationsmanagement, die speziell für den Aufbau und Betrieb globaler Netzwerke entwickelt wurden, basierend auf Ihrer Kernnetzwerkrichtlinie. Cloud WAN hat Funktionen wie automatisierte VPC-Anfügungen, integrierte Leistungsüberwachung und zentrale Konfiguration hinzugefügt.

Die Kernnetzwerkrichtlinie ist in einer deklarativen Sprache geschrieben, die Segmente, AWS-Regions-Routing und die Zuordnung der Anhänge zu Segmenten definiert. Mit einer Kernnetzwerkrichtlinie können Sie Ihre Absicht für die Zugriffskontrolle und das Datenverkehrs-Routing beschreiben, während AWS Cloud WAN die Netzwerkkonfigurationsdetails übernimmt.

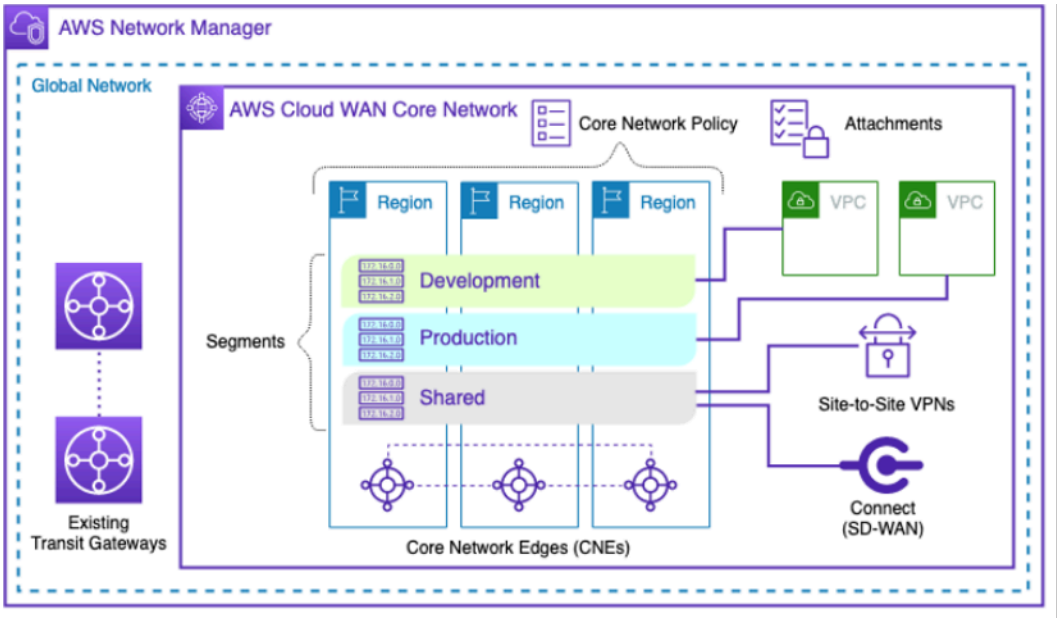
Cloud WAN wird in AWS Network Manager verwaltet, mit dem Sie Ihr Cloud WAN-Kernnetzwerk und Transit Gateway-Netzwerke über AWS-Konten, -Regionen und On-Premises-Standorte hinweg zentral verwalten und visualisieren können. Network Manager bietet Ihnen mehrere Dashboard-Visualisierungen, mit denen Sie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

- Weltkarten, die Aufschluss darüber geben, wo sich Ihre Netzwerkressourcen wie Edge-Standorte, Geräte und Anhänge befinden.
- Überwachung, bei der CloudWatch Ereignisse verwendet werden, um Statistiken von 15 Monaten zu verfolgen, was Ihnen einen besseren Überblick über die Leistung Ihrer Netzwerke gibt.
- Ereignisverfolgung, die Echtzeitereignisse an ein Ereignis-Dashboard streamt.
- 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 On-Premises-Standorten. Transit Gateway ist ein regionaler Netzwerkkonnektivitäts-Hub und optimal für Kunden, die in einigen AWS-Regionen tätig sind, ihre eigene Peering- und Routing-Konfiguration verwalten möchten oder ihre eigene Automatisierung verwenden möchten. Cloud WAN ist optimal für Kunden, die ihr globales Netzwerk durch Richtlinien definieren und den Service die zugrunde liegenden Komponenten automatisch implementieren lassen möchten.

# Wissenswertes

- CNE (Core Network Edge) erbt viele Transit Gateway-Merkmale, z. B. den Durchsatz pro VPC-Anhang.
- Cloud WAN unterstützt sowohl IPv4 als auch IPv6.
- Derzeit unterstützt Cloud WAN keine AnlagenAWS Direct Connect. Um AWS Direct Connect mit Cloud WAN verwenden zu können, benötigen Sie ein Transit Gateway, das an ein -AWS Direct ConnectGateway angehängt ist, und dann das Transit Gateway, das mit Cloud WAN verbunden ist.
- Für große Netzwerke mit vielen Änderungen sollten Sie erwägen, ein separates Entwicklungs- und Testnetzwerk zu erstellen, in dem Sie Änderungen validieren können.




AWS Cloud WAN

# Weitere Ressourcen

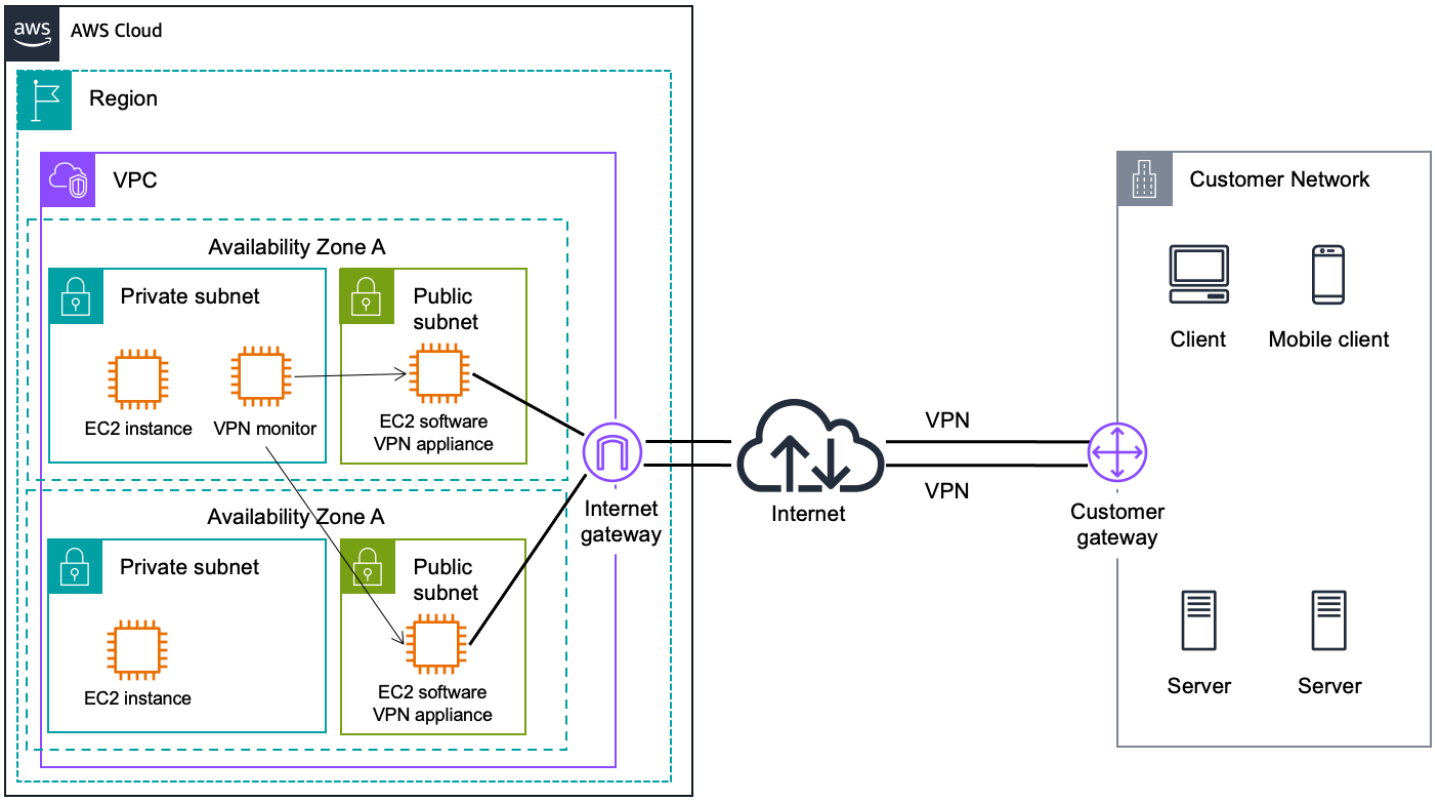
- AWS Cloud WAN-Dokumentation
- Blog-Beitrag: Migrations- und Interoperabilitätsmuster für AWS Cloud WAN und AWS Transit Gateway

# Fazit

AWS bietet eine Reihe effizienter, sicherer Konnektivitätsoptionen, mit denen Sie AWS optimal nutzen können, wenn Sie Ihre Remote-Netzwerke mit Amazon VPC integrieren. Die in diesem Whitepaper bereitgestellten Optionen heben einige der Konnektivitätsoptionen und -muster hervor, mit denen Kunden ihre Remote-Netzwerke oder mehrere Amazon-VPC-Netzwerke erfolgreich integriert haben. Mithilfe der hier bereitgestellten Informationen können Sie den am besten geeigneten Mechanismus für den Anschluss der Infrastruktur ermitteln, die für den Betrieb Ihres Unternehmens erforderlich ist, unabhängig davon, wo sie sich physisch befindet oder gehostet wird.

# Anhang A: High-Level-HA-Architektur für Software-VPN-Instances

Das Erstellen einer voll belastbaren VPC-Verbindung für Software-VPN-Instances erfordert die Einrichtung und Konfiguration mehrerer VPN-Instances und einer Überwachungs-Instance zur Überwachung des Zustands der VPN-Verbindungen.




High-Level-Software-VPN-HA

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 entsprechenden VPN-Instances in derselben Availability Zone geleitet wird. Jede VPN-Instance stellt dann VPN-Konnektivität für Instances bereit, die sich dieselbe Availability Zone teilen.

## VPN-Überwachung

Um eine softwarebasierte VPN-Appliance zu überwachen, können Sie einen VPN Monitor erstellen. Der VPN-Monitor ist eine benutzerdefinierte Instance, die Sie zum Ausführen der VPN-Überwachungsskripts benötigen. Diese Instance soll den Status der VPN-Verbindung und VPN-

Instances ausführen und überwachen. Wenn eine VPN-Instance oder -Verbindung ausfällt, muss der Monitor die VPN-Instance anhalten, beenden oder neu starten und gleichzeitig den Datenverkehr von den betroffenen Subnetzen auf die funktionierende VPN-Instance umleiten, bis beide Verbindungen wieder funktionieren. Da die Kundenanforderungen variieren, bietet AWS derzeit keine vorgeschriebene Anleitung für die Einrichtung dieser Überwachungs-Instance. Ein Beispielskript für die 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 berücksichtigen, um Benachrichtigungen zu senden oder im Falle eines VPN-Verbindungsfehlers automatisch zu versuchen, die Netzwerkkonnektivität zu reparieren.

Darüber hinaus können Sie die von AWS verwalteten VPN-Tunnel mithilfe von Amazon- CloudWatch Metriken überwachen, die Datenpunkte aus dem VPN-Service zu lesbaren, nahezu in Echtzeit bereitgestellten Metriken sammeln. Jede VPN-Verbindung sammelt und veröffentlicht eine Vielzahl von Tunnelmetriken in Amazon CloudWatch. Mit diesen Metriken können Sie Zustand und Aktivität von Tunneln überwachen und automatisierte Aktionen erstellen.

# Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Bol Yu, Technical Account Manager, AWS Enterprise Support
- Garvit Singh, Solutions Builder, AWS-Lösungsarchitektur
- Morad, Executive Manager, Solution Builders, AWS-Lösungsarchitektur
- Sohaib Tahir, Lösungsarchitekt, AWS-Lösungsarchitektur
- Fiona Armada, Architektur für Prinzipallösungen, AWS-Lösungsarchitektur
- Pablo Snchez Carmona, Architektur für Netzwerkarchitekturlösungen, AWS-Lösungsarchitektur
- Tony Hawke, Technical Account Manager für IT-Kundendienstmitarbeiter im Bereich IT-Netzwerk, AWS Enterprise Support

# Dokumentversionen

Um über Aktualisierungen dieses Whitepapers benachrichtigt zu werden, abonnieren Sie den RSS-Feed.

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

# Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und 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.