User Guide

# AWS Site-to-Site VPN

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Site-to-Site VPN: User Guide

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

# Table of Contents

Was ist AWS Site-to-Site VPN? ... 1
Konzepte ... 1
Site-to-Site VPN-Funktionen ... 2
Site-to-Site VPN-Einschränkungen ... 3
Site-to-Site VPN-Ressourcen ... 3
Preisgestaltung ... 4
Wie funktioniert Site-to-Site VPN ... 5
Virtual Private Gateway ... 5
Transit Gateway ... 6
Kunden-Gateway-Gerät ... 7
Kunden-Gateway ... 7
IPv6 Kunden-Gateway ... 8
IPv6 VPN-Verbindungen ... 8
VPN-Tunneloptionen ... 9
Optionen für die VPN-Tunnelauthentifizierung ... 18
Pre-Shared-Key ... 18
Privates Zertifikat von AWS Private Certificate Authority ... 18
Optionen zur Initiierung des VPN-Tunnels ... 19
Optionen zur IKE-Initiierung des VPN-Tunnels ... 19
Regeln und Einschränkungen ... 20
Arbeiten mit Optionen zur VPN-Tunnel-Initiierung ... 20
Ersatz-Endpunkte ... 21
Kunde hat den Austausch von Endpunkten initiiert ... 21
Von AWS verwalteter Endpunktaustausch ... 22
Lebenszyklus eines Tunnelendpunkts ... 22
Kunden-Gateway-Optionen ... 28
IPv6 Kunden-Gateway-Optionen ... 32
Beschleunigte VPN-Verbindungen ... 32
Aktivieren der Beschleunigung ... 33
Regeln und Einschränkungen ... 33
Site-to-Site VPN-Routing-Optionen ... 34
Statisches und dynamisches Routing ... 34
Routentabellen und Routenpriorität ... 35
Routing während VPN-Tunnelendpunkt-Updates ... 38

IPv4 und IPv6 Verkehr ... 38
Fangen Sie mit Site-to-Site VPN an ... 41
Voraussetzungen ... 41
Erstellen eines Kunden-Gateways ... 43
Erstellen Sie ein Ziel-Gateway ... 44
Erstellen eines Virtual Private Gateways ... 44
Erstellen eines Transit-Gateways ... 45
Routing konfigurieren ... 46
(Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle ... 46
(Transit-Gateway) Fügen Sie eine Route zu Ihrer Routing-Tabelle hinzu. ... 47
Aktualisieren Ihrer Sicherheitsgruppe ... 48
Eine VPN-Verbindung erstellen ... 48
Konfigurationsdatei herunterladen ... 51
Konfigurieren Sie das Kunden-Gateway-Gerät. ... 52
Site-to-Site VPN-Architekturszenarien ... 53
Einzel- und Mehrfach-VPN-Verbindungen ... 54
Einzelne Site-to-Site VPN-Verbindung ... 54
Einzelne Site-to-Site VPN-Verbindung mit einem Transit-Gateway ... 55
Mehrere Site-to-Site VPN-Verbindungen ... 55
Mehrere Site-to-Site VPN-Verbindungen mit einem Transit-Gateway ... 56
Site-to-Site VPN-Verbindung mit AWS Direct Connect ... 57
Private Site-to-Site IP-VPN-Verbindung mit AWS Direct Connect ... 58
Sichere Kommunikation zwischen VPN-Verbindungen mithilfe von VPN CloudHub ... 59
Übersicht ... 59
Preisgestaltung ... 61
Redundante VPN-Verbindungen ... 61
Site-to-Site VPN-Kunden-Gateway-Geräte ... 64
Voraussetzungen ... 65
Bewährte Methoden ... 69
Firewall-Regeln ... 71
Statische und dynamische Routing-Konfigurationsdateien ... 74
Herunterladbare Konfigurationsdateien für statisches Routing ... 75
Dynamische Konfigurationsdateien zum Herunterladen ... 90
Konfigurieren Sie Windows Server als Kunden-Gatewaygerät ... 102
Konfigurieren der Windows-Instance ... 102
Schritt 1: Erstellen einer VPN-Verbindung und Konfigurieren Ihrer VPC ... 103

Schritt 2: Herunterladen der Konfigurationsdatei für die VPN-Verbindung ..... 104
Schritt 3: Konfigurieren des Windows-Servers ..... 107
Schritt 4: Einrichten des VPN-Tunnels ..... 108
Schritt 5: Aktivieren von Dead Gateway Detection ..... 116
Schritt 6: Testen der VPN-Verbindung ..... 116
Fehlerbehebung bei Kunden-Gateway-Geräten ..... 117
Gerät mit BGP ..... 118
Gerät ohne BGP ..... 121
Cisco ASA ..... 124
Cisco IOS ..... 129
Cisco IOS ohne BGP ..... 135
Juniper JunOS ..... 141
Juniper ScreenOS ..... 145
Yamaha ..... 149
Arbeite mit Site-to-Site VPN ..... 154
Erstellen Sie einen Cloud WAN VPN-Anhang ..... 154
Einen Transit-Gateway-VPN-Anhang erstellen ..... 157
Erstellen eines VPN-Anhangs mit der CLI ..... 159
IPv6 Adressen für Ihre VPN-Verbindung anzeigen ..... 160
Eine VPN-Verbindung testen ..... 161
Löschen Sie eine VPN-Verbindung und ein Gateway ..... 163
Eine VPN-Verbindung löschen ..... 163
Ein Kunden-Gateway löschen ..... 164
Ein Virtual Private Gateway trennen und löschen ..... 164
Das Ziel-Gateway für die VPN-Verbindung ändern ..... 165
Schritt 1: Das neue Ziel-Gateway erstellen ..... 166
Schritt 2: Die statischen Routen löschen (bedingt) ..... 166
Schritt 3: Migrieren zum neuen Gateway ..... 167
Schritt 4: Aktualisieren der VPC-Routing-Tabellen ..... 168
Schritt 5: Ziel-Gateway-Routing aktualisieren (bedingt) ..... 169
Schritt 6: Kunden-Gateway-ASN aktualisieren (bedingt) ..... 170
VPN-Verbindungsoptionen ändern ..... 170
VPN-Tunnel-Optionen ändern ..... 171
Die statischen Routen für eine VPN-Verbindung bearbeiten ..... 172
Das Kunden-Gateway für die VPN-Verbindung ändern ..... 173
Kompromittierte Anmeldeinformationen ersetzen ..... 173

VPN-Tunnelendpunkt-Zertifikate rotieren ... 174
Privates IP-VPN mit Direct Connect ... 175
Vorteile von privatem IP-VPN ... 175
Funktionsweise von privatem IP-VPN ... 176
Erstellen Sie ein privates IP-VPN über Direct Connect ... 176
Sicherheit ... 182
Verbesserte Sicherheitsfunktionen mit Secrets Manager ... 183
Ändern Sie den Pre-Shared Key von Secrets Manager ... 183
Ändern Sie den Speichermodus für Pre-Shared-Keys ... 184
Datenschutz ... 185
Richtlinie für den Datenverkehr zwischen Netzwerken ... 186
Identity and Access Management ... 187
Zielgruppe ... 188
Authentifizierung mit Identitäten ... 189
Verwalten des Zugriffs mit Richtlinien ... 193
Wie funktioniert AWS Site-to-Site VPN mit IAM ... 196
Beispiele für identitätsbasierte Richtlinien ... 203
Fehlerbehebung ... 206
AWS verwaltete Richtlinien ... 208
Verwenden von serviceverknüpften Rollen ... 210
Ausfallsicherheit ... 212
Zwei Tunnel pro VPN-Verbindung ... 212
Redundanz ... 213
Sicherheit der Infrastruktur ... 213
Überwachen Sie eine Site-to-Site VPN-Verbindung ... 214
Überwachungstools ... 215
Automatisierte Überwachungstools ... 215
Manuelle Überwachungstools ... 215
Site-to-Site VPN-Protokolle ... 216
Vorteile von Site-to-Site VPN-Protokollen ... 217
Größenbeschränkungen der Amazon CloudWatch Logs-Ressourcenrichtlinie ... 218
Site-to-Site Inhalt des VPN-Protokolls ... 218
IAM-Anforderungen für die Veröffentlichung in Logs CloudWatch ... 222
Konfiguration der Site-to-Site VPN-Protokolle anzeigen ... 223
Site-to-SiteVPN-Protokolle aktivieren ... 223
Deaktivieren Sie Site-to-Site VPN-Protokolle ... 225

Überwachen Sie Site-to-Site VPN-Tunnel mit CloudWatch ..... 226
VPN-Metriken und Dimensionen ..... 226
CloudWatch VPN-Metriken anzeigen ..... 228
Erstellen Sie CloudWatch Alarme zur Überwachung von VPN-Tunneln ..... 229
AWS Health und Site-to-Site VPN-Ereignisse ..... 232
Benachrichtigungen über den Austausch von Tunnel-Endpunkten ..... 232
VPN-Benachrichtigungen für einen einzelnen Tunnel ..... 232
Kontingente ..... 234
Site-to-Site VPN-Ressourcen ..... 234
Routen ..... 235
Bandbreite und Durchsatz ..... 236
Maximum Transmission Unit (MTU) ..... 237
Zusätzliche Kontingentressourcen ..... 237
Dokumentverlauf ..... 238
..... ccxliv

# Was ist AWS Site-to-Site VPN?

Standardmäßig kann eine Instance, die Sie in einer Amazon VPC starten, nicht mit einem lokalen (AWS Cloud) Netzwerk und einem Remote-Gerät kommunizieren — dies kann beispielsweise eine Site oder ein lokales Gerät sein. Sie können den Zugriff auf Ihre Remote-Geräte von Ihrer VPC aus ermöglichen, indem Sie eine AWS Site-to-Site VPN (Site-to-Site VPN-) Verbindung herstellen und das Routing so konfigurieren, dass der Datenverkehr über die Verbindung weitergeleitet wird.

Obwohl der Begriff VPN-Verbindung ein allgemeiner Begriff ist, bezieht sich eine VPN-Verbindung in dieser Dokumentation auf die Verbindung zwischen Ihrer VPC und Ihrem eigenen lokalen Netzwerk. Site-to-Site VPN unterstützt Internet Protocol Security (IPsec) VPN-Verbindungen.

Inhalt


- Konzepte
- Site-to-Site VPN-Funktionen
- Site-to-Site VPN-Einschränkungen
- Site-to-Site VPN-Ressourcen
- Preisgestaltung


## Konzepte

Im Folgenden sind die wichtigsten Konzepte für Site-to-Site VPN aufgeführt:

- VPN-Verbindung: Eine sichere Verbindung zwischen Ihren Geräten vor Ort und Ihrem VPCs.
- VPN-Tunnel: Eine verschlüsselte Verbindung, über die Daten vom Kundennetzwerk zu oder von AWS gelangen können.

  Jede VPN-Verbindung umfasst zwei VPN-Tunnel, die Sie für eine hohe Verfügbarkeit gleichzeitig verwenden können.
- Kunden-Gateway: Eine AWS Ressource, die AWS Informationen zu Ihrem Kunden-Gateway-Gerät bereitstellt.
- Kunden-Gateway-Gerät: Ein physisches Gerät oder eine Softwareanwendung auf Ihrer Seite der Site-to-Site VPN-Verbindung.
- Ziel-Gateway: Ein allgemeiner Begriff für den VPN-Endpunkt auf der Amazon-Seite der Site-to-Site VPN-Verbindung.

- Virtuelles privates Gateway: Ein virtuelles privates Gateway ist der VPN-Endpunkt auf der Amazon-Seite Ihrer Site-to-Site VPN-Verbindung, der an eine einzelne VPC angeschlossen werden kann.
- Transit-Gateway: Ein Transit-Hub, der zur Verbindung mehrerer VPCs und lokaler Netzwerke sowie als VPN-Endpunkt für die Amazon-Seite der Site-to-Site VPN-Verbindung verwendet werden kann.

## Site-to-Site VPN-Funktionen

Die folgenden Funktionen werden bei AWS Site-to-Site VPN Verbindungen unterstützt:

- Internet Key Exchange Version 2 (IKEv2)
- NAT-Traversierung
- 4-Byte-ASN im Bereich 1—2147483647 für die Konfiguration eines Virtual Private Gateway (VGW). Weitere Informationen finden Sie unter Kunden-Gateway-Optionen für Ihre AWS Site-to-Site VPN Verbindung.
- 2-Byte-ASN für Customer Gateway (CGW) im Bereich von 1—65535. Weitere Informationen finden Sie unter Kunden-Gateway-Optionen für Ihre AWS Site-to-Site VPN Verbindung.
- CloudWatch Metriken
- Wiederverwendbare IP-Adressen für Ihre Kunden-Gateways
- Zusätzliche Verschlüsselungsoptionen; einschließlich AES 256-Bit-Verschlüsselung, SHA-2-Hash-Funktionen und zusätzliche Diffie-Hellman-Gruppen
- Konfigurierbare Tunnel-Optionen
- Benutzerdefinierte private ASN für die Amazon-Seite einer BGP-Sitzung
- Privates Zertifikat von einer untergeordneten Zertifizierungsstelle von AWS Private Certificate Authority
- IPv6 Support für AWS Site-to-Site VPN-Unterstützung
  - IPv6 für IP-Adressen des inneren Tunnels (Paket-IP)
  - IPv6 für äußere Tunnel-IP-Adressen (Tunnel-IP) auf Transit Gateway und Cloud WAN
- Vollständige IPv6 Migrationsunterstützung mit den folgenden Kombinationen:
  - IPv6 äußere Tunnel-IP mit IPv6 innerer Paket-IP (IPv6-in-IPv6)
  - IPv6 äußere Tunnel-IP mit IPv4 innerer Paket-IP (IPv4-in-IPv6)

# Site-to-Site VPN-Einschränkungen

Eine Site-to-Site VPN-Verbindung hat die folgenden Einschränkungen.

- IPv6 Datenverkehr wird für VPN-Verbindungen auf einem Virtual Private Gateway nicht unterstützt. IPv6 for outer tunnel IPs wird nur auf Transit Gateway und Cloud WAN unterstützt.
- Eine AWS VPN Verbindung unterstützt Path MTU Discovery nicht.
- Eine einzelne Site-to-Site VPN-Verbindung kann nicht beides IPv4 und IPv6 Datenverkehr gleichzeitig unterstützen. Sie benötigen separate VPN-Verbindungen für Transport IPv4 und IPv6 Pakete.
- Private IP-VPN-Verbindungen unterstützen keine IPv6 Adressen für den Außentunnel IPs.
- Sie können eine bestehende IPv4 VPN-Verbindung nicht ändern, um sie zu verwenden IPv6. Sie müssen die bestehende Verbindung löschen und eine neue erstellen.

Beachten Sie außerdem Folgendes, wenn Sie Site-to-Site VPN verwenden.

- Wenn Sie eine Verbindung VPCs zu einem gemeinsamen lokalen Netzwerk herstellen, empfehlen wir, dass Sie für Ihre Netzwerke CIDR-Blöcke verwenden, die sich nicht überschneiden.

# Site-to-Site VPN-Ressourcen

Sie können Ihre Site-to-Site VPN-Ressourcen über eine der folgenden Schnittstellen erstellen, darauf zugreifen und sie verwalten:

- AWS Management Console— Stellt eine Weboberfläche bereit, über die Sie auf Ihre Site-to-Site VPN-Ressourcen zugreifen können.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von AWS Diensten bereit, einschließlich Amazon VPC, und wird unter Windows, macOS und Linux unterstützt. Die AWS Site-to-Site VPN Befehlszeilen sind in der größeren EC2 Befehlszeilenreferenz enthalten
  - Allgemeine Informationen zur Befehlszeilenschnittstelle finden Sie unter. AWS Command Line Interface
  - Eine Liste der verfügbaren EC2 Befehle, einschließlich der Site-to-Site VPN-Befehle, finden Sie unter EC2 Befehlszeilenreferenz.

> **Note**
>
> Die Befehlszeilenreferenz unterscheidet nicht zwischen den Site-to-Site VPN-Befehlen und dem größeren EC2 Befehlssatz

- AWS SDKs— Stellt eine sprachspezifische Sprache bereit APIs und kümmert sich um viele Verbindungsdetails, wie z. B. die Berechnung von Signaturen, die Bearbeitung von Wiederholungsversuchen von Anfragen und die Fehlerbehandlung. Weitere Informationen finden Sie unter AWS SDKs.
- Abfrage-API – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf die Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und die Fehlerbehandlung in der Anwendung durchgeführt werden. Weitere Informationen finden Sie in der Amazon EC2 API-Referenz.

## Preisgestaltung

Sie werden für jede VPN-Verbindungsstunde berechnet, in der Ihre VPN-Verbindung bereitgestellt und verfügbar ist. Weitere Informationen finden Sie unter AWS Site-to-Site VPN und unter Preise für Accelerated Site-to-Site VPN Connection.

Die Datenübertragung von Amazon ins Internet wird Ihnen EC2 in Rechnung gestellt. Weitere Informationen finden Sie unter Datenübertragung auf der Seite mit den Preisen auf Amazon EC2 On-Demand-Preise.

Wenn Sie eine beschleunigte VPN-Verbindung erstellen, erstellen und verwalten wir zwei Beschleuniger in Ihrem Namen. Ihnen werden ein Stundensatz und Datenübertragungskosten für jeden Beschleuniger in Rechnung gestellt. Weitere Informationen finden Sie unter AWS Global Accelerator Preise.

Für die Verwendung von IPv6 Adressen mit Ihren Site-to-Site VPN-Verbindungen fallen keine zusätzlichen Gebühren an.

# Wie AWS Site-to-Site VPN funktioniert

Eine Site-to-Site VPN-Verbindung besteht aus den folgenden Komponenten:

- Ein Virtual Private Gateway oder ein Transit-Gateway
- Ein Kunden-Gateway-Gerät
- Ein Kunden-Gateway

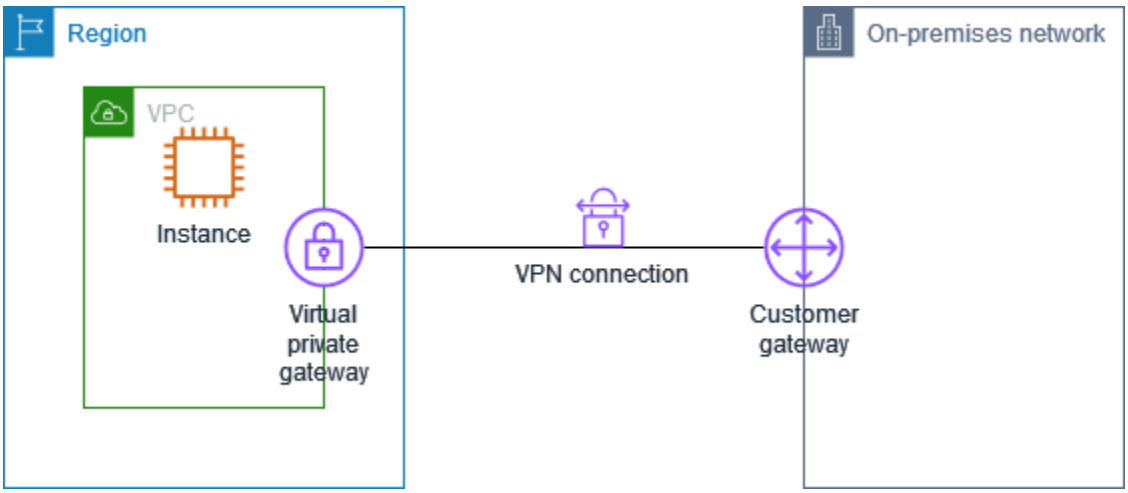
Die VPN-Verbindung bietet zwei VPN-Tunnel zwischen einem virtuellen privaten Gateway oder Transit-Gateway auf der AWS Seite und einem Kunden-Gateway auf der lokalen Seite.

Weitere Informationen zu Site-to-Site VPN-Kontingenten finden Sie unterAWS Site-to-Site VPN Kontingente.

## Virtual Private Gateway

Ein virtuelles privates Gateway ist der VPN-Konzentrator auf der Amazon-Seite der Site-to-Site VPN-Verbindung. Sie erstellen ein virtuelles privates Gateway und fügen es einer Virtual Private Cloud (VPC) mit Ressourcen hinzu, die auf die Site-to-Site VPN-Verbindung zugreifen müssen.

Das folgende Diagramm zeigt eine VPN-Verbindung zwischen einer VPC und Ihrem On-Premises-Netzwerk unter Verwendung eines Virtual Private Gateways.




Während der Erstellung eines Virtual Private Gateway können Sie die private Autonomous System Number (ASN) für die Amazon-Seite des Gateways angeben. Wenn Sie keine ASN angeben, wird der Virtual Private Gateway mit der Standard-ASN (64512) erstellt. Sie können die ASN nicht ändern,

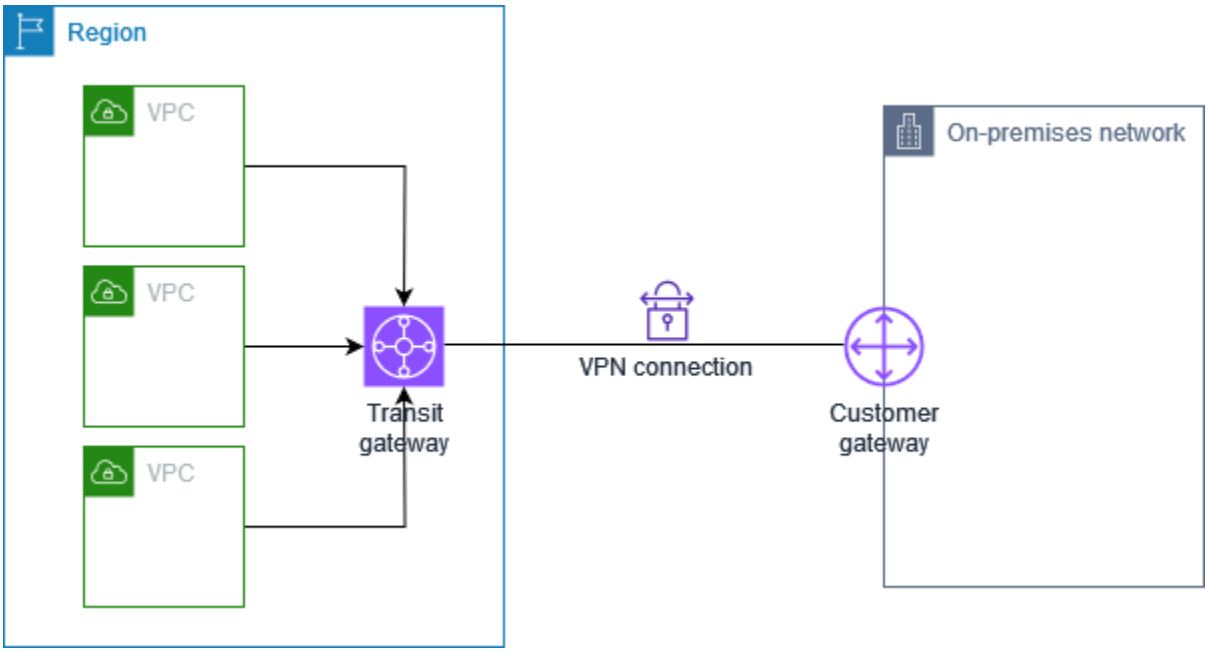
nachdem Sie das Virtual Private Gateway erstellt haben. Um die ASN für Ihr Virtual Private Gateway zu überprüfen, sehen Sie sich dessen Details auf der Seite Virtual Private Gateways in der Amazon VPC-Konsole an oder verwenden Sie den Befehl. describe-vpn-gateways AWS CLI

> **Note**
>
> Virtuelle private Gateways unterstützen IPv6 keine VPN-Verbindungen. Site-to-Site Wenn Sie IPv6 Unterstützung benötigen, verwenden Sie ein Transit-Gateway oder ein Cloud-WAN für Ihre VPN-Verbindung.

## Transit Gateway

Ein Transit-Gateway ist ein Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie unter Amazon VPC Transit Gateways. Sie können eine Site-to-Site VPN-Verbindung als Anlage an einem Transit-Gateway erstellen.

Das folgende Diagramm zeigt eine VPN-Verbindung zwischen mehreren Netzwerken VPCs und Ihrem lokalen Netzwerk mithilfe eines Transit-Gateways. Das Transit Gateway hat drei VPC-Anhänge und einen VPN-Anhang.




Ihre Site-to-Site VPN-Verbindung auf einem Transit-Gateway kann den IPv6 Datenverkehr innerhalb der VPN-Tunnel (innere IP-Adressen) unterstützen IPv4 . Darüber hinaus unterstützen Transit-

Gateways IPv6 Adressen für die IP-Adressen der äußeren Tunnel. Weitere Informationen finden Sie unter IPv4 und IPv6 Verkehr in AWS Site-to-Site VPN.

Sie können das Ziel-Gateway einer Site-to-Site VPN-Verbindung von einem virtuellen privaten Gateway zu einem Transit-Gateway ändern. Weitere Informationen finden Sie unter the section called “Das Ziel-Gateway für die VPN-Verbindung ändern”.

## Kunden-Gateway-Gerät

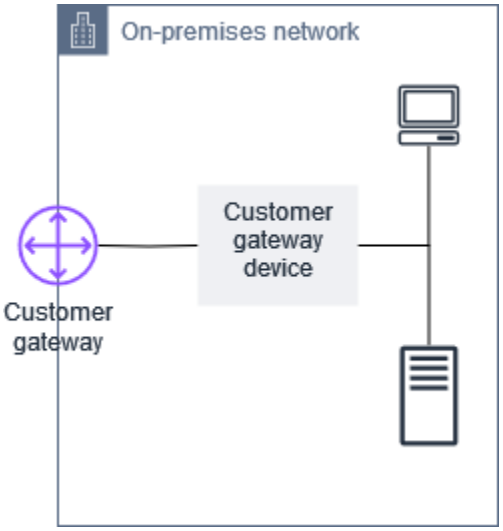
Ein Kunden-Gateway-Gerät ist ein physisches Gerät oder eine Softwareanwendung auf Ihrer Seite der Site-to-Site VPN-Verbindung. Sie konfigurieren das Gerät so, dass es mit der Site-to-Site VPN-Verbindung funktioniert. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Kunden-Gateway-Geräte.

Standardmäßig muss Ihr Kunden-Gateway-Gerät die Tunnel für Ihre Site-to-Site VPN-Verbindung aufrufen, indem es Datenverkehr generiert und den IKE-Verhandlungsprozess (Internet Key Exchange) einleitet. Sie können Ihre Site-to-Site VPN-Verbindung so konfigurieren, dass stattdessen der IKE-Verhandlungsprozess initiiert werden AWS muss. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Optionen zur Tunnelinitiierung.

Wenn Sie IP-Adressen IPv6 für den Außentunnel verwenden, muss Ihr Kunden-Gateway-Gerät die IPv6 Adressierung unterstützen und in der Lage sein, IPsec Tunnel mit IPv6 Endpunkten einzurichten.

## Kunden-Gateway

Ein Kunden-Gateway ist eine Ressource, die Sie in AWS erstellen, die das Kunden-Gateway-Gerät in Ihrem lokalen Netzwerk darstellt. Wenn Sie ein Kunden-Gateway erstellen, geben Sie Informationen über Ihr Gerät an AWS. Weitere Informationen finden Sie unter the section called “Kunden-Gateway-Optionen”.




Um Amazon VPC mit einer Site-to-Site VPN-Verbindung zu verwenden, müssen Sie oder Ihr Netzwerkadministrator auch das Kunden-Gateway-Gerät oder die Anwendung in Ihrem Remote-Netzwerk konfigurieren. Wenn Sie die Site-to-Site VPN-Verbindung herstellen, stellen wir Ihnen die erforderlichen Konfigurationsinformationen zur Verfügung, und Ihr Netzwerkadministrator führt diese Konfiguration in der Regel durch. Weitere Informationen über die Anforderungen und Konfiguration von Kunden-Gateways finden Sie unter AWS Site-to-Site VPN Kunden-Gateway-Geräte.

## IPv6 Kunden-Gateway

Wenn Sie ein Kunden-Gateway für die Verwendung mit einem IPv6 Außentunnel erstellen IPs, geben Sie eine IPv6 Adresse anstelle einer IPv4 Adresse an. Sie können mit der AWS Management Console oder der AWS CLI ein IPv6 Kunden-Gateway erstellen.

Verwenden Sie den folgenden Befehl, um ein IPv6 Kunden-Gateway mit der AWS CLI zu erstellen:

```
aws ec2 create-customer-gateway --Ipv6-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

Die IPv6 Adresse muss eine gültige, über das Internet routingfähige IPv6 Adresse für Ihr Kunden-Gateway-Gerät sein.

# IPv6 VPN-Verbindungen

Site-to-Site VPN-VPN-Verbindungen unterstützen die folgenden IPv6 Konfigurationen:

- IPv4 äußerer Tunnel mit IPv4 inneren Paketen — Die grundlegende IPv4 VPN-Funktion, die auf Virtual Private Gateway (VGW), Transit Gateway (TGW) und Cloud WAN unterstützt wird.

- IPv4 äußerer Tunnel mit IPv6 inneren Paketen — Ermöglicht IPv6 Anwendungen/Transport innerhalb des VPN-Tunnels. Wird auf TGW und Cloud WAN unterstützt (nicht auf VGW unterstützt).
- IPv6 äußerer Tunnel mit IPv6 inneren Paketen — Ermöglicht die vollständige IPv6 Migration mit IPv6 Adressen sowohl für den äußeren Tunnel IPs als auch für das innere Paket. IPs Wird auf TGW und Cloud WAN unterstützt.
- IPv6 äußerer Tunnel mit IPv4 inneren Paketen — Ermöglicht die Adressierung von IPv6 Außentunneln und unterstützt gleichzeitig ältere IPv4 Anwendungen innerhalb des Tunnels. Wird auf TGW und Cloud WAN unterstützt.

Um eine VPN-Verbindung mit IPv6 äußerem Tunnel herzustellen IPs, geben Sie dies `OutsideIPAddressType=Ipv6` beim Erstellen der VPN-Verbindung an. AWS konfiguriert automatisch die externen IPv6 Tunneladressen für die AWS-Seite der VPN-Tunnel.

Beispiel für einen CLI-Befehl zum Erstellen einer VPN-Verbindung mit IPv6 äußerem Tunnel IPs und IPv6 innerem Tunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

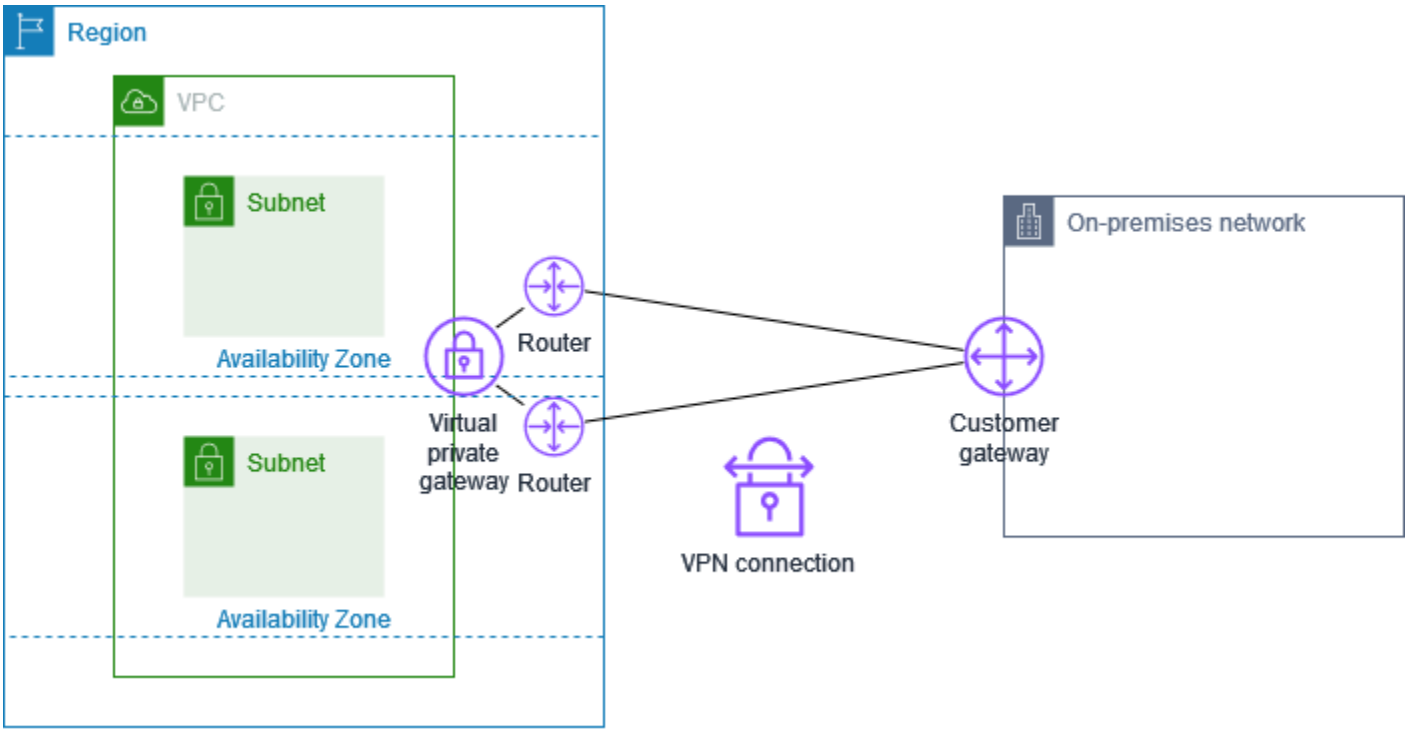
Sie können die Ihrer VPN-Verbindung zugewiesenen IPv6 Adressen mit dem `describe-vpn-connection` CLI-Befehl anzeigen.

## Tunneloptionen für Ihre AWS Site-to-Site VPN Verbindung

Sie verwenden eine Site-to-Site VPN-Verbindung, um Ihr Remote-Netzwerk mit einer VPC zu verbinden. Jede Site-to-Site VPN-Verbindung hat zwei Tunnel, wobei jeder Tunnel eine eindeutige öffentliche IP-Adresse verwendet. Aus Redundanzgründen ist es wichtig, beide Tunnel zu konfigurieren. Wenn ein Tunnel nicht verfügbar ist (z. B. aufgrund von Wartungsarbeiten nicht verfügbar), wird der Netzwerkverkehr automatisch an den verfügbaren Tunnel für diese spezifische Site-to-Site VPN-Verbindung weitergeleitet.

Das folgende Diagramm stellt die beiden Tunnel einer VPN-Verbindung dar. Jeder Tunnel endet in einer anderen Availability Zone, um eine erhöhte Verfügbarkeit zu gewährleisten. Der Datenverkehr vom lokalen Netzwerk zu AWS verwendet beide Tunnel. Der Datenverkehr vom AWS lokalen

Netzwerk bevorzugt einen der Tunnel, kann aber automatisch auf den anderen Tunnel umgeleitet werden, wenn auf der AWS Seite ein Fehler auftritt.




Wenn Sie eine Site-to-Site VPN-Verbindung herstellen, laden Sie eine für Ihr Kunden-Gateway-Gerät spezifische Konfigurationsdatei herunter, die Informationen zur Konfiguration des Geräts enthält, einschließlich Informationen zur Konfiguration der einzelnen Tunnel. Sie können optional einige der Tunneloptionen selbst angeben, wenn Sie die Site-to-Site VPN-Verbindung herstellen. Andernfalls stellt AWS Standardwerte bereit.

> **Note**
>
> Site-to-Site VPN-Tunnel-Endpunkte bewerten Vorschläge von Ihrem Kunden-Gateway, beginnend mit dem niedrigsten konfigurierten Wert aus der folgenden Liste, unabhängig von der Reihenfolge der Angebote vom Kunden-Gateway. Sie können den `modify-vpn-connection-options` Befehl verwenden, um die Liste der Optionen einzuschränken, die AWS Endpunkte akzeptieren. Weitere Informationen finden Sie unter modify-vpn-connection-optionsAmazon EC2 Command Line Reference.

Im Folgenden finden Sie die Tunneloptionen, die Sie konfigurieren können.

> **Note**
>
> Einige Tunneloptionen haben mehrere Standardwerte. Beispielsweise haben IKE-Versionen zwei Standardwerte für Tunneloptionen: `ikev1` und`ikev2`. Alle Standardwerte werden dieser Tunneloption zugeordnet, wenn Sie keine bestimmten Werte auswählen. Klicken Sie hier, um alle Standardwerte zu entfernen, die nicht mit der Tunneloption verknüpft werden sollen. Wenn Sie ihn beispielsweise nur `ikev1` für die IKE-Version verwenden möchten, klicken Sie, `ikev2` um ihn zu entfernen.

Zeitüberschreitung bei DPD-Timeouts (Dead Peer Detection)

Die Zahl der Sekunden, nach denen eine DPD-Zeitüberschreitung auftritt. Ein DPD-Timeout von 30 Sekunden bedeutet, dass der VPN-Endpunkt den Peer 30 Sekunden nach dem ersten fehlgeschlagenen Keep-Alive als tot betrachtet. Sie können 30 oder mehr festlegen.

Standard: 40

DPD-Timeout-Aktion

Die Aktion, die nach dem Timeout der Dead Peer Detection (DPD) ausgeführt wird. Sie können folgende Formen angeben:

- `Clear`: Beenden Sie die IKE-Sitzung bei DPD Timeout (beenden Sie den Tunnel und löschen Sie die Routen)
- `None`: Keine Aktion bei DPD-Timeout
- `Restart`: Starten Sie die IKE-Sitzung bei DPD Timeout neu

Weitere Informationen finden Sie unter AWS Site-to-Site VPN Optionen zur Tunnelinitiierung.

Standard: `Clear`

VPN-Protokollierungsoptionen

Mithilfe von Site-to-Site VPN-Protokollen können Sie auf Details zur Einrichtung eines IP-Security-Tunnels (IPsec), zu IKE-Verhandlungen (Internet Key Exchange) und zu DPD-Protokollnachrichten (Dead Peer Detection) zugreifen.

Weitere Informationen finden Sie unter AWS Site-to-Site VPN Logs.

Verfügbare Protokollformate: `json`, `text`

IKE-Versionen

Die IKE-Versionen, die für den VPN-Tunnel zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardeinstellungen:, `ikev1` `ikev2`

Innerhalb des CIDR-Tunnels IPv4

Der Bereich der internen (internen) IPv4 Adressen für den VPN-Tunnel. Sie können einen CIDR-Block der Größe /30 aus dem Bereich `169.254.0.0/16` angeben. Der CIDR-Block muss für alle Site-to-Site VPN-Verbindungen, die dasselbe Virtual Private Gateway verwenden, eindeutig sein.

> **Note**
>
> Der CIDR-Block muss nicht unter allen Verbindungen eines Transit-Gateways eindeutig sein. Wenn sie jedoch nicht eindeutig sind, kann dies zu einem Konflikt auf Ihrem Kunden-Gateway führen. Gehen Sie vorsichtig vor, wenn Sie denselben CIDR-Block für mehrere Site-to-Site VPN-Verbindungen auf einem Transit-Gateway wiederverwenden.

Die folgenden CIDR-Blöcke sind reserviert und können nicht verwendet werden:

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`
- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

Standard: Ein IPv4 CIDR-Block der Größe /30 aus dem Bereich. `169.254.0.0/16`

Vorab gemeinsam genutzter Schlüsselspeicher

Die Art des Speichers für den Pre-Shared Key:

- Standard — Der Pre-Shared Key wird direkt im Site-to-Site VPN-Dienst gespeichert.
- Secrets Manager — Der Pre-Shared Key wird gespeichert unter AWS Secrets Manager. Weitere Informationen zu Secrets Manager finden Sie unterVerbesserte Sicherheitsfunktionen mit Secrets Manager.

Im IPv6 CIDR-Tunnel

(Nur IPv6 VPN-Verbindungen) Der Bereich der internen (internen) IPv6 Adressen für den VPN-Tunnel. Sie können einen CIDR-Block der Größe /126 aus dem lokalen `fd00::/8`-Bereich angeben. Der CIDR-Block muss für alle Site-to-Site VPN-Verbindungen, die dasselbe Transit-Gateway verwenden, eindeutig sein. Wenn Sie kein IPv6 Subnetz angeben, wählt Amazon automatisch ein /128-Subnetz aus diesem Bereich aus. Unabhängig davon, ob Sie das Subnetz angeben oder Amazon es auswählt, verwendet Amazon die erste verwendbare IPv6 Adresse im Subnetz für seine Seite der Verbindung und Ihre Seite verwendet die zweite verwendbare IPv6 Adresse.

Standard: Ein IPv6 CIDR-Block der Größe /126 aus dem lokalen Bereich. `fd00::/8`

IP-Adresstyp außerhalb des Tunnels

Der IP-Adresstyp für die IP-Adressen des externen (externen) Tunnels. Sie können einen der folgenden Werte angeben:

- `PrivateIpv4`: Verwenden Sie eine private IPv4 Adresse, um Site-to-Site VPN-Verbindungen über Direct Connect bereitzustellen.
- `PublicIpv4`: (Standard) Verwenden Sie IPv4 Adressen für den äußeren Tunnel IPs.
- `Ipv6`: Verwenden Sie IPv6 Adressen für den Außentunnel IPs. Diese Option ist nur für VPN-Verbindungen auf einem Transit-Gateway oder Cloud-WAN verfügbar.

Wenn Sie diese Option auswählen`Ipv6`, konfiguriert AWS automatisch die externen IPv6 Tunneladressen für die AWS-Seite der VPN-Tunnel. Ihr Kunden-Gateway-Gerät muss IPv6 Adressierung unterstützen und in der Lage sein, IPsec Tunnel mit IPv6 Endpunkten einzurichten.

Standard: `PublicIpv4`

Lokales IPv4 Netzwerk (CIDR)

(Nur IPv4 VPN-Verbindung) Der CIDR-Bereich, der während der IKE-Phase-2-Aushandlung für die Kundenseite (vor Ort) des VPN-Tunnels verwendet wurde. Dieser Bereich wird verwendet, um Routen vorzuschlagen, erzwingt jedoch keine Verkehrsbeschränkungen, da er ausschließlich VPNs routenbasiert AWS verwendet wird. Richtlinienbasierte Protokolle VPNs werden nicht unterstützt, da sie die Fähigkeit zur Unterstützung dynamischer Routingprotokolle und Architekturen mit mehreren Regionen einschränken AWS würden. Dies sollte die IP-Bereiche Ihres lokalen Netzwerks beinhalten, die über den VPN-Tunnel kommunizieren müssen. Zur Steuerung des tatsächlichen Datenverkehrs sollten die richtigen Routingtabellenkonfigurationen und Sicherheitsgruppen verwendet werden. NACLs

Standard: 0.0.0.0/0

CIDR IPv4 im Remote-Netzwerk

(Nur IPv4 VPN-Verbindung) Der CIDR-Bereich, der während der IKE-Phase-2-Aushandlung für die AWS Seite des VPN-Tunnels verwendet wurde. Dieser Bereich wird verwendet, um Routen vorzuschlagen, erzwingt jedoch keine Verkehrsbeschränkungen, da AWS ausschließlich routenbasierte Routen VPNs verwendet. AWS unterstützt keine richtlinienbasierten Verfahren, VPNs da ihnen die für komplexe Routing-Szenarien erforderliche Flexibilität fehlt und sie nicht mit Funktionen wie Transit-Gateways und VPN Equal Cost Multi-Path (ECMP) kompatibel sind. Denn VPCs dies ist in der Regel der CIDR-Bereich Ihrer VPC. Bei Transit-Gateways kann dies mehrere CIDR-Bereiche von angeschlossenen VPCs oder anderen Netzwerken umfassen.

Standard: 0.0.0.0/0

Lokales Netzwerk IPv6 (CIDR)

(Nur IPv6 VPN-Verbindung) Der IPv6 CIDR-Bereich auf der Kunden-Gateway-Seite (lokal), der über die VPN-Tunnel kommunizieren darf.

Standard: ::/0

CIDR im Remote-Netzwerk IPv6

(Nur IPv6 VPN-Verbindung) Der IPv6 CIDR-Bereich auf der AWS Seite, die über die VPN-Tunnel kommunizieren darf.

Standard: ::/0

Phase 1 Diffie-Hellman (DH)-Gruppennummern

Die DH-Gruppennummern, die für den VPN-Tunnel für Phase 1 der IKE-Aushandlungen zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardeinstellungen: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Phase 2-Diffie-Hellman (DH)-Gruppennummern

Die DH-Gruppennummern, die für den VPN-Tunnel für Phase 2 der IKE-Aushandlungen zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardeinstellungen: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Phase 1-Verschlüsselungsalgorithmen

Die Verschlüsselungsalgorithmen, die für den VPN-Tunnel für Phase 1 der IKE-Aushandlung zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardeinstellungen: AES128,, -GCM-16 AES256, AES128 -GCM-16 AES256

Verschlüsselungsalgorithmen der Phase 2

Die Verschlüsselungsalgorithmen, die für den VPN-Tunnel für die IKE-Aushandlungen der Phase 2 zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardeinstellungen: AES128, AES256, AES128 -GCM-16, AES256 -GCM-16

Phase 1-Integritätsalgorithmen

Die Integritätsalgorithmen, die für den VPN-Tunnel für Phase 1 der IKE-Aushandlungen zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardwerte: SHA1 SHA2, -256 SHA2, -384, -512 SHA2

Phase 2-Integritätsalgorithmen

Die Integritätsalgorithmen, die für den VPN-Tunnel für Phase 2 der IKE-Aushandlungen zulässig sind. Sie können einen oder mehrere der Standardwerte angeben.

Standardwerte:, -256, -384 SHA1, SHA2 -512 SHA2 SHA2

Lebensdauer für Phase 1

> **Note**
>
> AWS initiiert erneute Schlüssel mit den Timing-Werten, die in den Feldern Phase-1-Lebensdauer und Phase-2-Lebensdauer festgelegt sind. Wenn sich diese Lebensdauer von den ausgehandelten Handshake-Werten unterscheiden, kann dies die Tunnelkonnektivität unterbrechen.

Die Lebensdauer in Sekunden für Phase 1 der IKE-Aushandlungen. Sie können eine Zahl zwischen 900 und 28.800 angeben.

Standard: 28 800 (8 Stunden)

Lebensdauer für Phase 2

> **Note**
>
> AWS initiieren Sie erneute Schlüssel mit den Zeitwerten, die in den Feldern Phase-1-Lebensdauer und Phase-2-Lebensdauer festgelegt sind. Wenn sich diese Lebensdauer von den ausgehandelten Handshake-Werten unterscheiden, kann dies die Tunnelkonnektivität unterbrechen.

Die Lebensdauer in Sekunden für Phase 2 der IKE-Aushandlungen. Sie können eine Zahl zwischen 900 und 3.600 angeben. Die Anzahl, die Sie angeben, muss kleiner als die Anzahl der Sekunden für die Lebensdauer der Phase 1 sein.

Standard: 3 600 (1 Stunde)

Pre-shared key (PSK)

Der Pre-Shared-Key (PSK) zur Herstellung der anfänglichen IKE-Sicherheitszuordnung (Internet Key Exchange) zwischen dem Ziel-Gateway und dem Kunden-Gateway.

Der PSK muss zwischen 8 und 64 Zeichen lang sein und darf nicht mit Null (0) beginnen. Zulässig sind alphanumerische Zeichen, Punkte (.) und Unterstriche (_).

Standard: eine alphanumerische Zeichenfolge mit 32 Zeichen.

Rekey-Fuzz

Der Prozentsatz des Rekey-Fensters (bestimmt durch die Rekey-Zeitspanne), innerhalb dessen die Rekey-Zeit nach dem Zufallsprinzip ausgewählt wird.

Sie können einen Prozentwert zwischen 0 und 100 angeben.

Standard: 100

Rekey-Margin-Time

Die Margenzeit in Sekunden, bevor die Lebensdauer der Phasen 1 und Phase 2 abläuft. Während dieser Zeit führt die AWS Seite der VPN-Verbindung einen IKE-Neuschlüssel durch.

Sie können eine Zahl zwischen 60 und der Hälfte des Wertes der Lebensdauer der Phase 2 angeben.

Der genaue Zeitpunkt der Schlüsselerneuerung wird auf der Grundlage des Wertes für Rekey-Fuzz zufällig ausgewählt.

Standard: 270 (4,5 Minuten)

Replay-Window-Paketgröße

Die Anzahl der Pakete in einem IKE-Wiedergabefenster.

Sie können einen Wert zwischen 64 und 2048 angeben.

Standard: 1024

Start-Aktion

Die Aktion, die beim Aufbau des Tunnels für eine VPN-Verbindung ausgeführt werden soll. Sie können folgende Formen angeben:

- `Start`: AWS leitet die IKE-Verhandlung ein, um den Tunnel hochzufahren. Wird nur unterstützt, wenn Ihr Kunden-Gateway mit einer IP-Adresse konfiguriert ist.
- `Add`: Ihr Kunden-Gateway-Gerät muss die IKE-Aushandlung initiieren, um den Tunnel aufzubauen.

Weitere Informationen finden Sie unter AWS Site-to-Site VPN Optionen zur Tunnelinitiierung.

Standard: `Add`

Steuerung des Lebenszyklus von Tunnelendpunkten

Die Steuerung des Lebenszyklus von Tunnelendpunkten bietet Kontrolle über den Zeitplan für den Austausch von Endpunkten.

Weitere Informationen finden Sie unter AWS Site-to-Site VPN Kontrolle des Lebenszyklus von Tunnelendpunkten.

Standard: `Off`

Sie können die Tunneloptionen angeben, wenn Sie eine Site-to-Site VPN-Verbindung erstellen, oder Sie können die Tunneloptionen für eine bestehende VPN-Verbindung ändern. Weitere Informationen finden Sie unter den folgenden Themen:

- Schritt 5: Eine VPN-Verbindung erstellen
- AWS Site-to-Site VPN Tunneloptionen ändern

# AWS Site-to-Site VPN Optionen für die Tunnelauthentifizierung

Sie können vorinstallierte Schlüssel oder Zertifikate verwenden, um Ihre Site-to-Site VPN-Tunnel-Endpunkte zu authentifizieren.

## Pre-Shared-Key

Ein Pre-Shared Key (PSK) ist die Standardauthentifizierungsoption für VPN-Tunnel. Site-to-Site Wenn Sie einen Tunnel erstellen, können Sie entweder Ihren eigenen PSK angeben oder zulassen AWS , dass einer automatisch für Sie generiert wird. Das PSK wird mit einer der folgenden Methoden gespeichert:

- Direkt im Site-to-Site VPN-Dienst. Weitere Informationen finden Sie unter Site-to-Site VPN-Kunden-Gateway-Geräte.
- Auf der AWS Secrets Manager Suche nach verbesserter Sicherheit. Weitere Informationen zur Verwendung von Secrets Manager zum Speichern eines PSK finden Sie unterVerbesserte Sicherheitsfunktionen mit Secrets Manager.

Die PSK-Zeichenfolge wird dann bei der Konfiguration Ihres Kunden-Gateway-Geräts verwendet.

## Privates Zertifikat von AWS Private Certificate Authority

Wenn Sie keine Pre-Shared-Key verwenden möchten, können Sie ein privates Zertifikat von AWS Private Certificate Authority zur Authentifizierung Ihres VPNs verwenden.

Sie müssen mit AWS Private Certificate Authority (AWS Private CA) ein privates Zertifikat von einer untergeordneten CA erstellen. Um die dem ACM untergeordnete CA zu signieren, können Sie eine ACM Stamm-CA oder eine externe CA verwenden. Für Informationen zum Erstellen eines privaten Zertifikats siehe Erstellen und Verwalten einer privaten CA im AWS Private Certificate Authority - Benutzerhandbuch.

Sie müssen eine dienstbezogene Rolle erstellen, um das Zertifikat für die AWS Seite des Site-to-Site VPN-Tunnelendpunkts zu generieren und zu verwenden. Weitere Informationen finden Sie unter the section called “Service-verknüpfte Rollen”.

> **Note**
>
> Um reibungslose Zertifizierungsrotationen zu ermöglichen, reicht jedes Zertifikat mit derselben Zertifizierungsstellenkette wie das ursprünglich im `CreateCustomerGateway` API-Aufruf angegebene Zertifikat aus, um eine VPN-Verbindung herzustellen.

Wenn Sie die IP-Adresse Ihres Kunden-Gateway-Geräts nicht angeben, überprüfen wir die IP-Adresse nicht. Dieser Vorgang ermöglicht es Ihnen, das Kunden-Gateway-Gerät auf eine andere IP-Adresse zu verlegen, ohne die VPN-Verbindung neu konfigurieren zu müssen.

Site-to-Site VPN führt eine Überprüfung der Zertifikatskette für das Kunden-Gateway-Zertifikat durch, wenn Sie ein VPN-Zertifikat erstellen. Zusätzlich zu den grundlegenden CA- und Gültigkeitsprüfungen prüft Site-to-Site VPN, ob die X.509-Erweiterungen vorhanden sind, einschließlich Authority Key Identifier, Subject Key Identifier und Basic Constraints.

# AWS Site-to-Site VPN Optionen zur Tunnelinitiierung

Standardmäßig muss Ihr Kunden-Gateway-Gerät die Tunnel für Ihre Site-to-Site VPN-Verbindung aufrufen, indem es Datenverkehr generiert und den Internet Key Exchange (IKE) - Verhandlungsprozess einleitet. Sie können Ihre VPN-Tunnel so konfigurieren, dass sie angeben, dass stattdessen der IKE-Verhandlungsprozess initiiert oder neu gestartet werden AWS muss.

## Optionen zur IKE-Initiierung des VPN-Tunnels

Die folgenden Optionen zur IKE-Initiierung sind verfügbar. Sie können eine oder beide Optionen für einen oder beide Tunnel in Ihrer Site-to-Site VPN-Verbindung implementieren. Weitere Informationen zu diesen und anderen Tunneloptionseinstellungen finden Sie unter VPN-Tunneloptionen.

- Startaktion: Die beim Einrichten des VPN-Tunnels für eine neue oder geänderte VPN-Verbindung auszuführende Aktion. Standardmäßig initiiert Ihr Kunden-Gateway-Gerät den IKE-Aushandlungsprozess, um den Tunnel aufzubauen. Sie können angeben, dass stattdessen der IKE-Verhandlungsprozess initiiert werden AWS muss.
- Aktion bei DPD-Timeout  Die nach dem Timeout der Dead Peer Detection (DPD) auszuführende Aktion. Standardmäßig wird die IKE-Sitzung beendet, der Tunnel wird heruntergefahren und die Routen werden entfernt. Sie können angeben, dass die IKE-Sitzung neu gestartet AWS werden muss, wenn ein DPD-Timeout auftritt, oder Sie können angeben, dass bei einem DPD-Timeout keine Aktion ausgeführt AWS werden darf.

## Regeln und Einschränkungen

Die folgenden Regeln und Einschränkungen gelten:

- Um die IKE-Verhandlung einzuleiten, AWS ist die öffentliche IP-Adresse Ihres Kunden-Gateway-Geräts erforderlich. Wenn Sie die zertifikatsbasierte Authentifizierung für Ihre VPN-Verbindung konfiguriert haben und bei der Erstellung der Kunden-Gateway-Ressource keine IP-Adresse angegeben haben AWS, müssen Sie ein neues Kunden-Gateway erstellen und die IP-Adresse angeben. Ändern Sie dann die VPN-Verbindung und geben Sie das neue Kunden-Gateway an. Weitere Informationen finden Sie unter Das Kunden-Gateway für eine AWS Site-to-Site VPN Verbindung ändern.
- Die IKE-Initiierung (Startaktion) von der AWS Seite der VPN-Verbindung aus wird nur für IKEv2 unterstützt.
- Wenn die IKE-Initiierung von der AWS Seite der VPN-Verbindung aus verwendet wird, beinhaltet sie keine Timeout-Einstellung. Sie wird solange versuchen, eine Verbindung herzustellen, bis sie erfolgreich ist. Darüber hinaus initiiert die AWS Seite der VPN-Verbindung erneut die IKE-Verhandlung, wenn sie von Ihrem Kunden-Gateway eine SA-Döschmeldung erhält.
- Wenn sich Ihr Kunden-Gateway-Gerät hinter einer Firewall oder einem anderen Gerät befindet, das Network Address Translation (NAT) verwendet, muss für dieses Gerät eine Identität (IDr) konfiguriert sein. Weitere Informationen dazu finden Sie IDr unter RFC 7296.

Wenn Sie die IKE-Initiierung nicht von der AWS Seite für Ihren VPN-Tunnel konfigurieren und die VPN-Verbindung eine Zeit lang inaktiv ist (normalerweise 10 Sekunden, abhängig von Ihrer Konfiguration), kann der Tunnel ausfallen. Um dies zu verhindern, können Sie ein Tool zur Netzwerküberwachung verwenden, das „Keep-alive“-Pings generiert.

## Arbeiten mit Optionen zur VPN-Tunnel-Initiierung

Weitere Informationen zum Arbeiten mit den Optionen zur VPN-Tunnel-Initiierung finden Sie in den folgenden Themen:

- So erstellen Sie eine neue VPN-Verbindung und geben die Optionen zur VPN-Tunnel-Initiierung an: Schritt 5: Eine VPN-Verbindung erstellen
- So ändern Sie die Optionen zur VPN-Tunnel-Initiierung für eine vorhandene VPN-Verbindung: AWS Site-to-Site VPN Tunneloptionen ändern

# AWS Site-to-Site VPN Ersatz von Tunnelendpunkten

Ihre Site-to-Site VPN-Verbindung besteht aus Redundanzgründen aus zwei VPN-Tunneln. Manchmal werden einer oder beide VPN-Tunnel-Endpunkte ersetzt, wenn AWS Tunnelaktualisierungen durchgeführt werden oder wenn Sie Ihre VPN-Verbindung ändern. Während eines Austauschs des Tunnelendpunkts kann die Konnektivität über den Tunnel unterbrochen werden, während der neue Tunnelendpunkt bereitgestellt wird.

Themen


- Kunde hat den Austausch von Endpunkten initiiert
- Von AWS verwalteter Endpunktaustausch
- AWS Site-to-Site VPN Kontrolle des Lebenszyklus von Tunnelendpunkten


## Kunde hat den Austausch von Endpunkten initiiert

Wenn Sie die folgenden Komponenten Ihrer VPN-Verbindung ändern, werden einer oder beide Ihrer Tunnelendpunkte ersetzt.

| Änderung | API-Aktion | Auswirkungen auf den Tunnel |
| --- | --- | --- |
| Ändern des Ziel-Gateways für die VPN-Verbindung | ModifyVpnConnection | Während neue Tunnelend punkte bereitgestellt werden, sind beide Tunnel nicht verfügbar |
| Ändern des Kunden-Gateways für die VPN-Verbindung | ModifyVpnConnection | Während neue Tunnelend punkte bereitgestellt werden, sind beide Tunnel nicht verfügbar |
| Ändern der VPN-Verbi ndungsoptionen | ModifyVpnConnectionOptions | Während neue Tunnelend punkte bereitgestellt werden, sind beide Tunnel nicht verfügbar |

| Änderung | API-Aktion | Auswirkungen auf den Tunnel |
| --- | --- | --- |
| Ändern der VPN-Tunneloptionen | ModifyVpnTunnelOptions | Während des Updates ist der jeweils geänderte Tunnel nicht verfügbar. |

## Von AWS verwalteter Endpunktaustausch

AWS Site-to-Site VPN ist ein verwalteter Dienst und aktualisiert Ihre VPN-Tunnel-Endpunkte regelmäßig. Diese Updates finden aus verschiedenen Gründen statt, beispielsweise den folgenden:

- Für allgemeine Upgrades, z. B. Patches, Verbesserungen der Ausfallsicherheit und andere Verbesserungen
- Um zugrunde liegende Hardware außer Betrieb zu nehmen
- Wenn die automatische Überwachung feststellt, dass ein VPN-Tunnelendpunkt fehlerhaft ist

AWS wendet Tunnelendpunkt-Updates auf jeweils einen Tunnel Ihrer VPN-Verbindung an. Während der Aktualisierung der Tunnelendpunkte kommt es bei Ihrer VPN-Verbindung möglicherweise zu einem kurzzeitigen Redundanzverlust. Sie müssen aus demselben Grund auch in Ihrer VPN-Verbindung beide Tunnel konfigurieren, um zumindest hohe Verfügbarkeit sicherzustellen.

## AWS Site-to-Site VPN Kontrolle des Lebenszyklus von Tunnelendpunkten

Die Lebenszykluskontrolle von Tunnelendpunkten bietet die Kontrolle über den Zeitplan für den Austausch von Endpunkten und kann dazu beitragen, Verbindungsunterbrechungen beim Austausch AWS verwalteter Tunnelendpunkte zu minimieren. Mit dieser Funktion können Sie festlegen, dass AWS verwaltete Updates für Tunnel-Endpunkte zu einem Zeitpunkt akzeptiert werden, der für Ihr Unternehmen am besten geeignet ist. Verwenden Sie diese Funktion bei kurzfristigen Geschäftsanforderungen, oder wenn Sie nur einen einzigen Tunnel pro VPN-Verbindung unterstützen können.

> **Note**
>
> In seltenen Fällen AWS können wichtige Updates sofort auf Tunnelendpunkte angewendet werden, auch wenn die Funktion zur Lebenszykluskontrolle von Tunnelendpunkten aktiviert ist.

Themen


- So funktioniert die Steuerung des Lebenszyklus von Tunnelendpunkten
- Aktivieren Sie die Lebenszykluskontrolle der AWS Site-to-Site VPN Tunnelend
- Überprüfen Sie, ob die Lebenszykluskontrolle für AWS Site-to-Site VPN Tunnelendpunkte aktiviert ist
- Suchen Sie nach verfügbaren AWS Site-to-Site VPN Tunnel-Updates
- Akzeptieren Sie ein AWS Site-to-Site VPN Tunnel-Wartungsupdate
- Schalten Sie die Lebenszykluskontrolle für AWS Site-to-Site VPN Tunnelendpunkte aus


## So funktioniert die Steuerung des Lebenszyklus von Tunnelendpunkten

Aktivieren Sie die Funktion zur Steuerung des Lebenszyklus von Tunnelendpunkten für einzelne Tunnel innerhalb einer VPN-Verbindung. Sie kann zum Zeitpunkt der VPN-Erstellung oder durch Ändern der Tunneloptionen für eine bestehende VPN-Verbindung aktiviert werden.

Nachdem die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist, erhalten Sie auf zwei Arten zusätzliche Einblicke in bevorstehende Tunnelwartungsereignisse:

- Sie erhalten AWS Health Benachrichtigungen über bevorstehende Austauscharbeiten an Tunnelendpunkten.
- Der Status der ausstehenden Wartung sowie die Zeitstempel Wartung auto angewendet nach und Letzte Wartung angewendet können Sie im AWS Management Console oder mithilfe des Befehls get-vpn-tunnel-replacement-status einsehen AWS CLI .

Wenn eine Wartung für Tunnelendpunkte verfügbar ist, haben Sie die Möglichkeit, das Update zu einem für Sie passenden Zeitpunkt vor dem angegebenen Wartung automatisch angewendet nach-Zeitstempel zu akzeptieren.

Wenn Sie Updates nicht vor dem Datum der auto Wartung anwenden, AWS wird der Tunnelendpunkt bald darauf automatisch als Teil des regulären Wartungsupdatezyklus ausgetauscht.

## Aktivieren Sie die Lebenszykluskontrolle der AWS Site-to-Site VPN Tunnelend

Die Endpoint Lifecycle Control kann für eine bestehende oder neue VPN-Verbindung aktiviert werden. Dies kann entweder mit dem AWS Management Console oder geschehen AWS CLI.

> **Note**
>
> Wenn Sie die Funktion für eine vorhandene VPN-Verbindung aktivieren, wird standardmäßig gleichzeitig ein Austausch von Tunnelendpunkten initiiert. Wenn Sie die Funktion aktivieren, aber nicht sofort einen Austausch von Tunnelendpunkten einleiten möchten, können Sie die Option Tunnelaustausch überspringen verwenden.

Existing VPN connection

Die folgenden Schritte zeigen, wie Sie die Steuerung des Lebenszyklus von Tunnelendpunkten für eine vorhandene VPN-Verbindung aktivieren.

So aktivieren Sie Steuerung des Lebenszyklus von Tunnelendpunkten mithilfe der AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie unter VPN-Verbindungen die entsprechende Verbindung aus.
4. Wählen Sie Aktionen und anschließend Optionen für den VPN-Tunnel ändern aus.
5. Wählen Sie den zu ändernden Tunnel aus, indem Sie die entsprechende IP-Adresse in der Liste Externe IP-Adresse für VPN-Tunnel auswählen.
6. Aktivieren Sie unter Steuerung des Lebenszyklus von Tunnelendpunkten das Kontrollkästchen Aktivieren.
7. (Optional) Wählen Sie Tunnelaustausch überspringen aus.
8. Wählen Sie Änderungen speichern.

So aktivieren Sie Steuerung des Lebenszyklus von Tunnelendpunkten mithilfe der AWS CLI

Verwenden Sie den modify-vpn-tunnel-optionsBefehl, um die Lebenszykluskontrolle für Tunnelendpunkte zu aktivieren.

New VPN connection

Die folgenden Schritte zeigen, wie Sie die Steuerung des Lebenszyklus von Tunnelendpunkten während der Erstellung einer neuen VPN-Verbindung aktivieren.

Um die Lebenszykluskontrolle von Tunnelendpunkten während der Erstellung einer neuen VPN-Verbindung zu aktivieren, verwenden Sie den AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Connections aus.
3. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.
4. Wählen Sie in den Abschnitten für Optionen für Tunnel 1 und Optionen für Tunnel 2 unter Steuerung des Lebenszyklus von Tunnelendpunkten die Option Aktivieren aus.
5. Wählen Sie Create VPN Connection (VPN-Verbindung erstellen) aus.

Um die Lebenszykluskontrolle von Tunnelendpunkten während der Erstellung einer neuen VPN-Verbindung zu aktivieren, verwenden Sie den AWS CLI

Verwenden Sie den create-vpn-connectionBefehl, um die Lebenszykluskontrolle für Tunnelendpunkte zu aktivieren.

## Überprüfen Sie, ob die Lebenszykluskontrolle für AWS Site-to-Site VPN Tunnelendpunkte aktiviert ist

Mithilfe der CLI AWS Management Console oder können Sie überprüfen, ob die Lebenszykluskontrolle für Tunnelendpunkte in einem vorhandenen VPN-Tunnel aktiviert ist.

- Wenn die Lebenszykluskontrolle für Tunnelendpunkte deaktiviert ist und Sie sie aktivieren möchten, finden Sie weitere Informationen unterSteuerung des Lebenszyklus von Tunnelendpunkten.
- Wenn die Lebenszykluskontrolle für Tunnelendpunkte aktiviert ist und Sie sie deaktivieren möchten, finden Sie weitere Informationen unterSteuerung des Lebenszyklus von Tunnelendpunkten deaktivieren.

So überprüfen Sie mithilfe der AWS Management Console, ob die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie unter VPN-Verbindungen die entsprechende Verbindung aus.

4. Wählen Sie die Registerkarte Tunneldetails aus.
5. Suchen Sie in den Tunneldetails nach Steuerung des Lebenszyklus von Tunnelendpunkten. Dies meldet, ob die Funktion Aktiviert der Deaktiviert ist.

So überprüfen Sie mithilfe der AWS CLI, ob die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist

Verwenden Sie den describe-vpn-connectionsBefehl, um zu überprüfen, ob die Lebenszykluskontrolle für Tunnelendpunkte aktiviert ist.

## Suchen Sie nach verfügbaren AWS Site-to-Site VPN Tunnel-Updates

Nachdem Sie die Funktion für die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert haben, können Sie mit der AWS Management Console oder der CLI anzeigen, ob ein Wartungs-Update für Ihre VPN-Verbindung verfügbar ist. Bei der Suche nach einem verfügbaren Site-to-Site VPN-Tunnel-Update wird das Update nicht automatisch heruntergeladen und bereitgestellt. Sie können wählen, wann Sie es bereitstellen möchten. Die Schritte zum Herunterladen und Bereitstellen eines Updates finden Sie unterWartungs-Update annehmen.

Um nach verfügbaren Updates zu suchen, verwenden Sie den AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie unter VPN-Verbindungen die entsprechende Verbindung aus.
4. Wählen Sie die Registerkarte Tunneldetails aus.
5. Überprüfen Sie die Spalte Ausstehende Wartung. Der Status lautet entweder Verfügbar oder Keine.

Um nach verfügbaren Updates zu suchen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl get-vpn-tunnel-replacement-status, um nach verfügbaren Updates zu suchen.

## Akzeptieren Sie ein AWS Site-to-Site VPN Tunnel-Wartungsupdate

Wenn ein Wartungsupdate verfügbar ist, können Sie es mit der AWS Management Console oder CLI akzeptieren. Sie können das Wartungsupdate für den Site-to-Site VPN-Tunnel zu einem für

Sie passenden Zeitpunkt akzeptieren. Sobald Sie das Wartungsupdate akzeptiert haben, wird es bereitgestellt.

> **Note**
>
> Wenn Sie das Wartungsupdate nicht akzeptieren, AWS wird es automatisch während eines regulären Wartungsupdate-Zyklus bereitgestellt.

Um ein verfügbares Wartungsupdate zu akzeptieren, verwenden Sie den AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie unter VPN-Verbindungen die entsprechende Verbindung aus.
4. Wählen Sie Aktionen und dann VPN-Tunnel austauschen aus.
5. Wählen Sie den auszutauschenden Tunnel aus, indem Sie die entsprechende IP-Adresse in der Liste Externe IP-Adresse des VPN-Tunnels auswählen.
6. Wählen Sie Replace (Ersetzen) aus.

Um ein verfügbares Wartungsupdate zu akzeptieren, verwenden Sie den AWS CLI

Verwenden Sie den replace-vpn-tunnelBefehl, um ein verfügbares Wartungsupdate zu akzeptieren.

## Schalten Sie die Lebenszykluskontrolle für AWS Site-to-Site VPN Tunnelendpunkte aus

Wenn Sie die Funktion zur Lebenszykluskontrolle von Tunnelendpunkten nicht mehr verwenden möchten, können Sie sie mit dem AWS Management Console oder dem deaktivieren AWS CLI. Wenn Sie diese Funktion deaktivieren, stellt AWS Wartungs-Updates automatisch in regelmäßigen Abständen bereit. Diese Updates können während Ihrer Geschäftszeiten erfolgen. Um Auswirkungen auf das Geschäft zu vermeiden, empfehlen wir dringend, beide Tunnel in Ihrer VPN-Verbindung für hohe Verfügbarkeit zu konfigurieren.

> **Note**
>
> Bei deaktivierter Funktion ist zwar eine ausstehende Wartung verfügbar, doch können Sie die Option Tunnelaustausch überspringen nicht angeben. Sie können die Funktion jederzeit ausschalten, ohne die Option Tunnelersetzung überspringen zu verwenden. Die verfügbaren

ausstehenden Wartungsupdates AWS werden jedoch automatisch bereitgestellt, indem sofort ein Austausch der Tunnelendpunkte eingeleitet wird.

Um die Lebenszykluskontrolle von Tunnelendpunkten zu deaktivieren, verwenden Sie AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie unter VPN-Verbindungen die entsprechende Verbindung aus.
4. Wählen Sie Aktionen und anschließend Optionen für den VPN-Tunnel ändern aus.
5. Wählen Sie den zu ändernden Tunnel aus, indem Sie die entsprechende IP-Adresse in der Liste Externe IP-Adresse für VPN-Tunnel auswählen.
6. Wenn Sie die Steuerung des Lebenszyklus von Tunnelendpunkten deaktivieren möchten, löschen Sie unter Steuerung des Lebenszyklus von Tunnelendpunkten das Kontrollkästchen Aktivieren.
7. (Optional) Wählen Sie Tunnelaustausch überspringen aus.
8. Wählen Sie Änderungen speichern.

Um die Lebenszykluskontrolle von Tunnelendpunkten zu deaktivieren, verwenden Sie den AWS CLI

Verwenden Sie den modify-vpn-tunnel-optionsBefehl, um die Lebenszykluskontrolle für Tunnelendpunkte zu deaktivieren.

# Kunden-Gateway-Optionen für Ihre AWS Site-to-Site VPN Verbindung

Die folgende Tabelle enthält die Informationen, die Sie zum Erstellen einer Customer-Gateway-Ressource in benötige AWS.

| Item | Beschreibung |
| --- | --- |
| (Optional) Name-Tag. | Dadurch wird eine Markierung mit dem Schlüssel „Name“ und einem von Ihnen angegebenen Wert erstellt. |

| Item | Beschreibung |
| --- | --- |
| (Nur dynamisches Routing) BGP ASN (Border Gateway Protocol Autonomous System Number) Ihres Kunden-Gateways. | ASN im Bereich von 1—4.294.967.295 wird unterstützt. Sie können eine bereits zu Ihrem Netzwerk zugewiesene öffentliche ASN verwenden, mit Ausnahme der folgenden:<br>• 7224 — In allen Regionen reserviert<br>• 9059 — In der Region reserviert `eu-west-1`<br>• 10124 — In der Region reserviert `ap-northeast-1`<br>• 17943 — In der Region reserviert `ap-southeast-1`<br><br>Wenn Sie keine öffentliche ASN haben, können Sie eine private ASN im Bereich von 64.512—65.534 oder 4.200.000.000—4.294.967.294 verwenden. Die Standard-ASN ist 64512. Weitere Informationen zum Routing finden Sie unter. AWS Site-to-Site VPN Routing-Optionen |

| Item | Beschreibung |
| --- | --- |
| Die IP-Adresse der externen Schnittstelle des Kunden-Gateway-Geräts. | Die IP-Adresse muss statisch sein und kann entweder IPv4 oder lauten IPv6.<br><br>Für IPv4 Adressen: Wenn sich Ihr Kunden-Gateway-Gerät hinter einem NAT-Gerät (Network Address Translation) befindet, verwenden Sie die IP-Adresse Ihres NAT-Geräts. Stellen Sie außerdem sicher, dass UDP-Pakete auf Port 500 (und Port 4500, falls NAT-Traversal verwendet wird) zwischen Ihrem Netzwerk und den AWS Site-to-Site VPN Endpunkten übertragen werden dürfen. Weitere Informationen finden Sie unter Firewall-Regeln.<br><br>Für IPv6 Adressen: Die Adresse muss eine gültige, über das Internet routingfähige Adresse sein. IPv6 IPv6 Adressen werden nur für VPN-Verbindungen auf einem Transit-Gateway oder Cloud-WAN unterstützt.<br><br>Eine IP-Adresse ist nicht erforderlich, wenn Sie ein privates Zertifikat von AWS Private Certificate Authority und ein öffentliches VPN verwenden. |

| Item | Beschreibung |
| --- | --- |
| (Optional) Privates Zertifikat von einer untergeordneten Zertifizierungsstelle unter Verwendung von AWS Certificate Manager (ACM). | Wenn Sie zertifikatsbasierte Authentifizierung verwenden möchten, geben Sie den ARN eines privaten ACM-Zertifikats an, das auf Ihrem Kunden-Gateway-Gerät verwendet werden soll.<br><br>Wenn Sie ein Kunden-Gateway erstellen, können Sie das Kunden-Gateway so konfiguri eren, dass AWS Private Certificate Authority private Zertifikate zur Authentifizierung des VPN verwendet werden. Site-to-Site<br><br>Wenn Sie sich für diese Option entscheiden, erstellen Sie eine vollständig AWS gehostete private Zertifizierungsstelle (CA) für den internen Gebrauch in Ihrem Unternehmen. Sowohl das Root-CA-Zertifikat als auch die untergeordneten CA-Zertifikate werden von gespeichert und verwaltet. AWS Private CA<br><br>Bevor Sie das Kunden-Gateway erstellen, erstellen Sie mithilfe AWS Private Certificate Authority von einer untergeordneten Zertifizi erungsstelle ein privates Zertifikat und geben das Zertifikat dann bei der Konfiguration des Kunden-Gateways an. Für Informationen zum Erstellen eines privaten Zertifikats siehe Eine private CA erstellen und verwalten im AWS Private Certificate Authority -Benutzer handbuch. |
| (Optional) Gerät. | Ein Name für das Kunden-Gateway-Gerät ein, das diesem Kunden-Gateway zugeordnet ist. |

## IPv6 Kunden-Gateway-Optionen

Beachten Sie beim Erstellen eines Kunden-Gateways mit einer IPv6 Adresse Folgendes:

- IPv6 Kunden-Gateways werden nur für VPN-Verbindungen auf einem Transit-Gateway oder Cloud-WAN unterstützt.
- Die IPv6 Adresse muss eine gültige, über das Internet IPv6 routbare Adresse sein.
- Ihr Kunden-Gateway-Gerät muss IPv6 Adressierung unterstützen und in der Lage sein, IPsec Tunnel mit Endpunkten einzurichten. IPv6
- Um ein IPv6 Kunden-Gateway mit der AWS-CLI zu erstellen, verwenden Sie eine IPv6 Adresse für den `--ip-address` Parameter:

```
aws ec2 create-customer-gateway --ip-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

# Beschleunigte AWS Site-to-Site VPN Verbindungen

Sie können optional die Beschleunigung für Ihre Site-to-Site VPN-Verbindung aktivieren. Eine beschleunigte Site-to-Site VPN-Verbindung (beschleunigte VPN-Verbindung) leitet AWS Global Accelerator den Datenverkehr von Ihrem lokalen Netzwerk zu einem AWS Edge-Standort weiter, der Ihrem Kunden-Gateway-Gerät am nächsten ist. AWS Global Accelerator optimiert den Netzwerkpfad und verwendet das AWS globale Netzwerk ohne Überlastung, um den Datenverkehr an den Endpunkt weiterzuleiten, der die beste Anwendungsleistung bietet (weitere Informationen finden Sie unter). AWS Global Accelerator Sie können eine beschleunigte VPN-Verbindung verwenden, um Netzwerkunterbrechungen zu vermeiden, die auftreten können, wenn der Datenverkehr über das öffentliche Internet geroutet wird.

Wenn Sie eine beschleunigte VPN-Verbindung erstellen, erstellen und verwalten wir in Ihrem Namen zwei Beschleuniger, einen für jeden VPN-Tunnel. Sie können diese Beschleuniger nicht selbst anzeigen oder verwalten, indem Sie die Konsole oder verwenden. AWS Global Accelerator APIs

Informationen zu den AWS Regionen, die Accelerated VPN-Verbindungen unterstützen, finden Sie unter AWS Accelerated Site-to-Site VPN FAQs.

## Aktivieren der Beschleunigung

Wenn Sie eine Site-to-Site VPN-Verbindung herstellen, ist die Beschleunigung standardmäßig deaktiviert. Sie können optional die Beschleunigung aktivieren, wenn Sie einen neuen Site-to-Site VPN-Anhang auf einem Transit-Gateway erstellen. Weitere Informationen und Schritte finden Sie unter Einen AWS Site-to-Site VPN Transit-Gateway-Anhang erstellen.

Beschleunigte VPN-Verbindungen verwenden einen separaten Pool von IP-Adressen für die IP-Adressen der Tunnelendpunkte. Die IP-Adressen für die beiden VPN-Tunnel werden aus zwei separaten Netzwerkzonen ausgewählt.

## Regeln und Einschränkungen

Für die Verwendung einer beschleunigten VPN-Verbindung gelten die folgenden Regeln:

- Die Beschleunigung wird nur für Site-to-Site VPN-Verbindungen unterstützt, die an ein Transit-Gateway angeschlossen sind. Virtual Private Gateways unterstützen keine beschleunigten VPN-Verbindungen.
- Eine beschleunigte Site-to-Site VPN-Verbindung kann nicht mit einer AWS Direct Connect öffentlichen virtuellen Schnittstelle verwendet werden.
- Sie können die Beschleunigung für eine bestehende Site-to-Site VPN-Verbindung nicht ein- oder ausschalten. Stattdessen können Sie je nach Bedarf eine neue Site-to-Site VPN-Verbindung mit aktivierter oder deaktivierter Beschleunigung erstellen. Konfigurieren Sie dann Ihr Kunden-Gateway-Gerät so, dass es die neue Site-to-Site VPN-Verbindung verwendet, und löschen Sie die alte Site-to-Site VPN-Verbindung.
- NAT-Traversal (NAT-T) ist für eine beschleunigte VPN-Verbindung erforderlich und ist standardmäßig aktiviert. Wenn Sie eine Konfigurationsdatei von der Amazon VPC-Konsole heruntergeladen haben, sollten Sie die NAT-T-Einstellung prüfen und bei Bedarf anpassen.
- Die IKE-Verhandlung für beschleunigte VPN-Tunnel muss vom Gateway-Gerät des Kunden aus initiiert werden. Die beiden Tunneloptionen, die sich auf dieses Verhalten auswirken, sind `Startup Action` und`DPD Timeout Action`. Weitere Informationen finden Sie unter VPN-Tunneloptionen und Optionen zur Initiierung des VPN-Tunnels.
- Site-to-Site VPN-Verbindungen, die zertifikatsbasierte Authentifizierung verwenden, sind möglicherweise nicht kompatibel mit AWS Global Accelerator, da die Paketfragmentierung in Global Accelerator nur eingeschränkt unterstützt wird. Weitere Informationen finden Sie unter Die Funktionsweise von AWS Global Accelerator. Wenn Sie eine beschleunigte VPN-Verbindung

benötigen, die zertifikatbasierte Authentifizierung verwendet, muss Ihr Kunden-Gateway-Gerät die IKE-Fragmentierung unterstützen. Andernfalls aktivieren Sie Ihr VPN nicht für die Beschleunigung.

# AWS Site-to-Site VPN Routing-Optionen

AWS empfiehlt, bestimmte BGP-Routen anzukündigen, um die Routing-Entscheidungen im Virtual Private Gateway zu beeinflussen. Überprüfen Sie in der Herstellerdokumentation die Befehle, die für Ihr Gerät spezifisch sind.

Wenn Sie mehrere VPN-Verbindungen erstellen, sendet das Virtual Private Gateway Datenverkehr mithilfe von statisch zugewiesenen Routen oder BGP-Routenankündigungen an die passende VPN-Verbindung. Die Route hängt davon ab, wie die VPN-Verbindung konfiguriert wurde. Wenn identische Routen im virtuellen privaten Gateway vorhanden sind, werden statisch zugewiesene Routen gegenüber per BGP angekündigten Routen bevorzugt. Wenn Sie BGP-Ankündigungen verwenden, können Sie keine statischen Routen angeben.

Weitere Informationen zur Routenpriorität finden Sie unter Routentabellen und Routenpriorität.

Wenn Sie eine Site-to-Site VPN-Verbindung herstellen, müssen Sie wie folgt vorgehen:

- Geben Sie den Routing-Typ an (statisch oder dynamisch), den Sie verwenden möchten
- Aktualisieren der Routing-Tabelle für Ihr Subnetz

Es gibt Einschränkungen im Hinblick auf die Anzahl der Routen, die Sie einer Routing-Tabelle hinzufügen können. Weitere Informationen finden Sie im Abschnitt „Routing-Tabellen“ in Amazon VPC-Kontingenten im Amazon VPC-Benutzerhandbuch.

Themen


- Statisches und dynamisches Routing in AWS Site-to-Site VPN
- Routentabellen und AWS Site-to-Site VPN Routenpriorität
- Routing während VPN-Tunnelendpunkt-Updates
- IPv4 und IPv6 Verkehr in AWS Site-to-Site VPN


## Statisches und dynamisches Routing in AWS Site-to-Site VPN

Der Routing-Typ, den Sie auswählen, hängt von der Marke und dem Modell Ihres Kunden-Gateway-Geräts ab. Wenn Ihr Kunden-Gateway-Gerät das Border Gateway Protocol (BGP) unterstützt, geben

Sie bei der Konfiguration Ihrer Site-to-Site VPN-Verbindung dynamisches Routing an. Wenn Ihr Kunden-Gateway-Gerät BGP nicht unterstützt, geben Sie das statische Routing an.

Wenn Sie ein Gerät verwenden, das BGP-Werbung unterstützt, geben Sie keine statischen Routen für die Site-to-Site VPN-Verbindung an, da das Gerät BGP verwendet, um seine Routen zum Virtual Private Gateway bekannt zu geben. Wenn Sie ein Gerät verwenden, das BGP-Advertising nicht unterstützt, müssen Sie das statische Routing auswählen und die Routen (IP-Präfixe) für Ihr Netzwerk eingeben, die dem Virtual Private Gateway mitgeteilt werden sollen.

Wir empfehlen, dass Sie, sofern verfügbar, BGP-fähige Geräte verwenden, da das BGP-Protokoll eine zuverlässige Lebenderkennung bietet, die bei einem Ausfall des ersten VPN-Tunnels einen Failover auf den zweiten Tunnel ausführt. Geräte, die BGP nicht unterstützen, können bei Bedarf auch Zustandsprüfungen vornehmen, um einen Failover auf dem zweiten Tunnel auszuführen.

Sie müssen Ihr Kunden-Gateway-Gerät so konfigurieren, dass der Datenverkehr von Ihrem lokalen Netzwerk zur VPN-Verbindung weitergeleitet wird Site-to-Site. Die Konfiguration hängt von der Marke und dem Modell Ihres Geräts ab. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Kunden-Gateway-Geräte.

## Routentabellen und AWS Site-to-Site VPN Routenpriorität

Routing-Tabellen bestimmen, wohin der Netzwerkverkehr von Ihrer VPC geleitet wird. Sie müssen Ihrer VPC-Routing-Tabelle eine Route für Ihr Remote-Netzwerk hinzufügen und das Virtual Private Gateway als Ziel angeben. Dadurch wird der Datenverkehr von Ihrer VPC, der für Ihr Remote-Netzwerk vorgesehen ist, über das virtuelle private Gateway und über einen der VPN-Tunnel geleitet. Sie können die Option Route Propagation für Ihre Routing-Tabelle aktivieren, damit Ihre Netzwerk-Routen automatisch an die Routing-Tabelle weitergeleitet werden.

Wir verwenden die spezifischste mit dem Datenverkehr übereinstimmende Route in der Routing-Tabelle, um Datenverkehr weiterzuleiten (Übereinstimmung mit längstem Präfix). Wenn Ihre Routing-Tabelle sich überschneidende oder übereinstimmende Routen enthält, gelten die folgenden Regeln:

- Wenn sich propagierte Routen von einer Site-to-Site VPN-Verbindung oder AWS Direct Connect Verbindung mit der lokalen Route für Ihre VPC überschneiden, wird die lokale Route am meisten bevorzugt, auch wenn die propagierten Routen spezifischer sind.
- Wenn weitergegebene Routen von einer Site-to-Site VPN-Verbindung oder AWS Direct Connect -Verbindung denselben Ziel-CIDR-Block wie andere bestehende statische Routen haben (die längste Präfixübereinstimmung kann nicht angewendet werden), priorisieren wir die statischen Routen, deren Ziele ein Internet-Gateway, ein virtuelles privates Gateway, eine

Netzwerkschnittstelle, eine Instanz-ID, eine VPC-Peering-Verbindung, ein NAT-Gateway, ein Transit-Gateway oder ein Gateway-VPC-Endpunkt sind.

Die folgende Routing-Tabelle enthält z. B. eine statische Route zu einem Internet-Gateway und eine propagierte Route zu einem Virtual Private Gateway. Beide Routen haben den Zielbereich `172.31.0.0/24`. In diesem Fall wird der gesamte Datenverkehr für `172.31.0.0/24` an das Internet-Gateway geleitet, da die statische Route gegenüber der propagierten Route Priorität hat.

| Zielbereich | Ziel |
| --- | --- |
| 10.0.0.0/16 | Local |
| 172.31.0.0/24 | vgw-11223344556677889 (propagiert) |
| 172.31.0.0/24 | igw-12345678901234567 (statisch) |

Nur IP-Präfixe, die dem Virtual Private Gateway bekannt sind, entweder durch BGP-Ankündigungen oder durch einen statischen Routing-Eintrag, können Datenverkehr von Ihrer VPC empfangen. Das virtuelle private Gateway leitet keinen Datenverkehr weiter, der nicht durch empfangene BGP-Ankündigungen, statische Routing-Einträge oder das zugeordnete VPC CIDR abgedeckt ist. Virtuelle private Gateways unterstützen keinen Datenverkehr. IPv6

Wenn ein virtuelles privates Gateway Routing-Informationen empfängt, bestimmt es anhand der Pfadauswahl, wie der Datenverkehr geleitet wird. Die längste Präfixübereinstimmung gilt, wenn alle Endpunkte fehlerfrei sind. Der Zustand eines Tunnelendpunkts hat Vorrang vor anderen Routing-Attributen. Dieser Vorrang gilt für virtuelle private Gateways und Transit-Gateways. VPNs Wenn die Präfixe gleich sind, dann priorisiert das Virtual Private Gateway die Routen wie folgt (von den am meisten bevorzugten zu den am wenigsten bevorzugten):

- BGP hat Routen von einer Verbindung aus weitergegeben AWS Direct Connect

  Blackhole-Routen werden nicht über BGP an ein Site-to-Site VPN-Kunden-Gateway weitergegeben.
- Manuell hinzugefügte statische Routen für eine VPN-Verbindung Site-to-Site
- BGP hat Routen von einer Site-to-Site VPN-Verbindung aus weitergegeben
- Für übereinstimmende Präfixe, bei denen jede Site-to-Site VPN-Verbindung BGP verwendet, wird der AS-PATH verglichen und das Präfix mit dem kürzesten AS-PATH bevorzugt.

> **Note**
>
> AWS empfiehlt dringend, Kunden-Gateway-Geräte zu verwenden, die asymmetrisches Routing unterstützen.
> Für Kunden-Gateway-Geräte, die asymmetrisches Routing unterstützen, empfehlen wir nicht, AS PATH prepending zu verwenden, um sicherzustellen, dass beide Tunnel gleichermaßen über AS PATH verfügen. Dadurch wird sichergestellt, dass der multi-exit discriminator (MED)-Wert, den wir während der VPN-Tunnelendpunkt-Updates für einen Tunnel festgelegt haben, für die Bestimmung der Tunnelpriorität verwendet wird.
> Bei Kunden-Gateway-Geräten, die kein asymmetrisches Routing unterstützen, können Sie ein vorangestelltes AS PATH sowie Local-Preference verwenden, um einen Tunnel dem anderen gegenüber zu bevorzugen. Wenn sich der Ausgangspfad jedoch ändert, kann dies zu einem Rückgang des Datenverkehrs führen.

- Wenn die AS PATHs dieselbe Länge haben und wenn das erste AS in der AS_SEQUENCE über mehrere Pfade hinweg identisch ist, multi-exit discriminators (MEDs) werden verglichen. Der Pfad mit dem niedrigsten MED-Wert wird bevorzugt.

Die Routenpriorität ist während VPN-Tunnelendpunkt-Updates betroffen.

AWS Wählt bei einer Site-to-Site VPN-Verbindung einen der beiden redundanten Tunnel als primären Ausgangspfad aus. Diese Auswahl kann sich gelegentlich ändern. Es wird nachdrücklich empfohlen, beide Tunnel für hohe Verfügbarkeit zu konfigurieren und asymmetrisches Routing zu gewähren. Der Zustand eines Tunnelendpunkts hat Vorrang vor anderen Routing-Attributen. Diese Priorität gilt für virtuelle private Gateways und Transit-Gateways. VPNs

Für ein virtuelles privates Gateway wird ein Tunnel für alle Site-to-Site VPN-Verbindungen auf dem Gateway ausgewählt. Um mehr als einen Tunnel zu verwenden, empfehlen wir, Equal Cost Multipath (ECMP) zu erkunden, das für Site-to-Site VPN-Verbindungen auf einem Transit-Gateway unterstützt wird. Weitere Informationen finden Sie unter Transit-Gateways in Amazon VPC-Transit-Gateways. ECMP wird für Site-to-Site VPN-Verbindungen auf einem Virtual Private Gateway nicht unterstützt.

Bei Site-to-Site VPN-Verbindungen, die BGP verwenden, kann der primäre Tunnel anhand des multi-exit discriminator (MED)-Wert identifiziert werden. Wir empfehlen, spezifischere BGP-Routen zu bewerben, um Routing-Entscheidungen zu beeinflussen.

Bei Site-to-Site VPN-Verbindungen, die statisches Routing verwenden, kann der primäre Tunnel anhand von Verkehrsstatistiken oder Metriken identifiziert werden.

## Routing während VPN-Tunnelendpunkt-Updates

Eine Site-to-Site VPN-Verbindung besteht aus zwei VPN-Tunneln zwischen einem Kunden-Gateway-Gerät und einem Virtual Private Gateway oder einem Transit-Gateway. Wir empfehlen, dass Sie beide Tunnel für Redundanz konfigurieren. Führt von Zeit zu Zeit AWS auch routinemäßige Wartungsarbeiten an Ihrer VPN-Verbindung durch, wodurch möglicherweise einer der beiden Tunnel Ihrer VPN-Verbindung kurzzeitig deaktiviert wird. Weitere Informationen finden Sie unter Benachrichtigungen über den Austausch von Tunnel-Endpunkten.

Wenn wir Aktualisierungen für einem VPN-Tunnel durchführen, legen wir auf dem anderen Tunnel einen niedrigeren Wert für den ausgehenden multi-exit discriminator (MED) fest. Wenn Sie Ihr Kunden-Gateway-Gerät so konfiguriert haben, dass es beide Tunnel verwendet, verwendet Ihre VPN-Verbindung während des Aktualisierungsvorgangs eines Tunnelendpunkts den anderen (aktiven) Tunnel.

> **Note**
>
> - Um sicherzustellen, dass der aktive Tunnel mit dem niedrigeren MED bevorzugt wird, stellen Sie sicher, dass Ihr Kunden-Gateway-Gerät die gleichen Werte für Gewicht und lokale Präferenz für beide Tunnel verwendet (Gewicht und lokale Präferenz haben eine höhere Priorität als MED).

## IPv4 und IPv6 Verkehr in AWS Site-to-Site VPN

Ihre Site-to-Site VPN-Verbindung auf einem Transit-Gateway kann entweder den IPv4 Verkehr oder den IPv6 Verkehr innerhalb der VPN-Tunnel unterstützen. Standardmäßig unterstützt eine Site-to-Site VPN-Verbindung den IPv4 Verkehr innerhalb der VPN-Tunnel. Sie können eine neue Site-to-Site VPN-Verbindung konfigurieren, um den IPv6 Verkehr innerhalb der VPN-Tunnel zu unterstützen. Wenn Ihre VPC und Ihr lokales Netzwerk dann für die IPv6 Adressierung konfiguriert sind, können Sie IPv6 Datenverkehr über die VPN-Verbindung senden.

Wenn Sie die VPN-Tunnel für Ihre Site-to-Site VPN-Verbindung aktivieren IPv6 , hat jeder Tunnel zwei CIDR-Blöcke. Einer ist ein IPv4 CIDR-Block der Größe /30 und der andere ist ein CIDR-Block der Größe IPv6 /126.

## IPv4 und Unterstützung IPv6

Site-to-Site VPN-VPN-Verbindungen unterstützen die folgenden IP-Konfigurationen:

- IPv4 äußerer Tunnel mit IPv4 inneren Paketen — Die grundlegende IPv4 VPN-Funktion, die auf virtuellen privaten Gateways, Transit-Gateways und Cloud-WAN unterstützt wird.
- IPv4 äußerer Tunnel mit IPv6 inneren Paketen — Ermöglicht IPv6 Anwendungen/Transport innerhalb des VPN-Tunnels. Wird auf Transit-Gateways und Cloud-WAN unterstützt. Dies wird für virtuelle private Gateways nicht unterstützt.
- IPv6 äußerer Tunnel mit IPv6 inneren Paketen — Ermöglicht die vollständige IPv6 Migration mit IPv6 Adressen sowohl für den äußeren Tunnel IPs als auch für das innere Paket IPs. Wird sowohl für Transit-Gateways als auch für Cloud-WAN unterstützt.
- IPv6 äußerer Tunnel mit IPv4 inneren Paketen — Ermöglicht die Adressierung von IPv6 Außentunneln und unterstützt gleichzeitig ältere IPv4 Anwendungen innerhalb des Tunnels. Wird sowohl für Transit-Gateways als auch für Cloud-WAN unterstützt.

Die folgenden Regeln gelten:

- IPv6 Adressen für den Außentunnel IPs werden nur für Site-to-Site VPN-Verbindungen unterstützt, die auf einem Transit-Gateway oder Cloud-WAN beendet sind. Site-to-Site VPN-Verbindungen auf virtuellen privaten Gateways unterstützen IPv6 keinen Außentunnel IPs.
- Bei der Verwendung IPv6 als Außentunnel IPs müssen Sie beiden VPN-Tunneln IPv6 Adressen auf beiden AWS Seiten der VPN-Verbindung und auf Ihrem Kunden-Gateway zuweisen.
- Sie können die IPv6 Unterstützung für eine bestehende Site-to-Site VPN-Verbindung nicht aktivieren. Sie müssen die bestehende Verbindung löschen und eine neue erstellen.
- Eine Site-to-Site VPN-Verbindung kann nicht beides IPv4 und IPv6 Datenverkehr gleichzeitig unterstützen. Bei den inneren gekapselten Paketen kann es sich um eines IPv6 oder IPv4, aber nicht um beides handeln. Sie benötigen separate Site-to-Site VPN-Verbindungen für Transport IPv4 und IPv6 Pakete.
- Private IP-Adressen unterstützen VPNs keine IPv6 Adressen für den Außentunnel IPs. Sie verwenden entweder RFC 1918- oder CGNAT-Adressen. Weitere Informationen zu RFC 1918 finden Sie unter RFC 1918 — Address Allocation for Private Internets.
- IPv6 VPNs unterstützt denselben Durchsatz (Gbit/s und PPS), dieselbe MTU und dieselben Routenlimits wie. IPv4 VPNs

- Die IPSec Verschlüsselung und der Schlüsselaustausch funktionieren für beide IPv4 auf die gleiche Weise. IPv6 VPNs

Weitere Informationen zum Erstellen einer VPN-Verbindung mit IPv6 Support finden Sie unter Erstellen einer VPN-Verbindung in Erste Schritte mit Site-to-Site VPN.

# Fangen Sie an mit AWS Site-to-Site VPN

Gehen Sie wie folgt vor, um eine AWS Site-to-Site VPN Verbindung einzurichten. Bei der Erstellung geben Sie ein Virtual Private Gateway, ein Transit-Gateway oder „Nicht zugeordnet“ als den Typ des Ziel-Gateways an. Wenn Sie „Nicht zugeordnet“ angeben, können Sie den Ziel-Gateway-Typ zu einem späteren Zeitpunkt auswählen oder ihn als VPN-Anhang für AWS Cloud WAN verwenden. Dieses Tutorial hilft Ihnen dabei, eine VPN-Verbindung mithilfe eines Virtual Private Gateway herzustellen. Es wird davon ausgegangen, dass Sie über eine vorhandene VPC mit mindestens einem Subnetz verfügen.

Um eine VPN-Verbindung mit einem Virtual Private Gateway einzurichten, gehen Sie wie folgt vor:

Aufgaben

- Voraussetzungen
- Schritt 1: Kunden-Gateway erstellen
- Schritt 2: Ein Ziel-Gateway erstellen
- Schritt 3: Routing konfigurieren
- Schritt 4: Ihre Sicherheitsgruppe aktualisieren
- Schritt 5: Eine VPN-Verbindung erstellen
- Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen
- Schritt 7: Das Kunden-Gateway-Gerät konfigurieren

Verwandte Aufgaben

- Informationen zum Erstellen einer VPN-Verbindung für AWS Cloud WAN finden Sie unterErstellen Sie einen Cloud WAN VPN-Anhang.
- Schritte zum Erstellen einer VPN-Verbindung auf einem Transit-Gateway finden Sie unter Einen Transit-Gateway-VPN-Anhang erstellen.

## Voraussetzungen

Sie benötigen die folgenden Informationen, um die Komponenten einer VPN-Verbindung einzurichten und zu konfigurieren.

| Item | Informationen |
| --- | --- |
| Kunden-Gateway-Gerät | Das physische Gerät oder das Software-Gerät auf Ihrer Seite der VPN-Verbindung. Sie benötigen den Hersteller (z. B. Cisco), die Plattform (beispielsweise ISR Series Router) und die Softwareversion (z. B. IOS 12.4) |
| Kunden-Gateway | Um die Kunden-Gateway-Ressource in zu erstellen AWS, benötigen Sie die folgenden Informationen:<br>• Die über das Internet routbare IP-Adresse für die externe Schnittstelle des Geräts<br>• Der Routing-Typ: statisch oder dynamisch<br>• Für dynamisches Routing die Border Gateway Protocol (BGP) Autonomous System Number (ASN)<br>• (Optional) Privates Zertifikat von AWS Private Certificate Authority zur Authentif izierung Ihres VPN<br><br>Weitere Informationen finden Sie unter Kunden-Gateway-Optionen. |
| (Optional) Die ASN für die AWS Seite der BGP-Sitzung | Sie geben dies an, wenn Sie ein Virtual Private Gateway oder Transit-Gateway erstellen. Wenn Sie keinen Wert angeben, wird die Standard-ASN übernommen. Weitere Informationen finden Sie unter Virtual Private Gateway. |
| VPN-Verbindung | Um die VPN-Verbindung anzulegen, benötigen Sie die folgenden Informationen:<br>• Für statisches Routing die IP-Präfixe für Ihr privates Netzwerk. |

| Item | Informationen |
| --- | --- |
| | • (Optional) Tunneloptionen für jeden VPN-Tunnel. Weitere Informationen finden Sie unter Tunneloptionen für Ihre AWS Site-to-Site VPN Verbindung. |

## Schritt 1: Kunden-Gateway erstellen

Ein Kunden-Gateway stellt Informationen AWS über Ihr Kunden-Gateway-Gerät oder Ihre Softwareanwendung bereit. Weitere Informationen finden Sie unter Kunden-Gateway.

Wenn Sie beabsichtigen, ein privates Zertifikat zur Authentifizierung Ihres VPN zu verwenden, erstellen Sie mithilfe von. AWS Private Certificate Authority Für Informationen zum Erstellen eines privaten Zertifikats siehe Eine private CA erstellen und verwalten im AWS Private Certificate Authority -Benutzerhandbuch.

> **Note**
>
> Sie müssen entweder eine IP-Adresse oder den Amazon-Ressourcennamen des privaten Zertifikats angeben.

So erstellen Sie ein Kunden-Gateway mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Kunden-Gateways aus.
3. Wählen Sie Kunden-Gateway erstellen aus.
4. (Optional) Geben Sie bei Name tag (Name-Tag) einen Namen für Ihr Kunden-Gateway ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
5. Geben Sie unter BGP ASN eine Border Gateway Protocol (BGP) Autonomous System Number (ASN) für Ihr Kunden-Gateway ein.
6. Wählen Sie für den IP-Adresstyp eine der folgenden Optionen aus:
   - IPv4- (Standard) Geben Sie eine IPv4 Adresse für Ihr Kunden-Gateway-Gerät an.

- IPv6- Geben Sie eine IPv6 Adresse für Ihr Kunden-Gateway-Gerät an. Diese Option ist erforderlich, wenn eine VPN-Verbindung mit einem IPv6 Außentunnel hergestellt wird IPs.

7. Geben Sie als IP-Adresse die statische, über das Internet routbare IP-Adresse für Ihr Kunden-Gateway-Gerät ein. Wenn sich Ihr Kunden-Gateway-Gerät hinter einem NAT-Gerät befindet, das für NAT-T aktiviert ist, verwenden Sie die öffentliche IP-Adresse des NAT-Geräts.
8. (Optional) Wenn Sie ein privates Zertifikat verwenden möchten, wählen Sie für Certificate ARN (Zertifikat ARN) den Amazon-Ressourcennamen des privaten Zertifikats.
9. (Optional) Geben Sie als Gerät einen Namen für das Kunden-Gateway-Gerät ein, das diesem Kunden-Gateway zugeordnet ist.
10. Wählen Sie Kunden-Gateway erstellen aus.

So erstellen Sie ein Kunden-Gateway über die Befehlszeile oder API

- CreateCustomerGateway(Amazon EC2 Query API)
- create-customer-gateway (AWS CLI)

  Beispiel für die Erstellung eines IPv6 Kunden-Gateways:

```
aws ec2 create-customer-gateway --ipv6-address
 2001:0db8:85a3:0000:0000:8a2e:0370:7334 --bgp-asn 65051 --type ipsec.1 --region us-
west-1
```

- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

# Schritt 2: Ein Ziel-Gateway erstellen

Um eine VPN-Verbindung zwischen Ihrer VPC und Ihrem lokalen Netzwerk herzustellen, müssen Sie auf der AWS Seite der Verbindung ein Ziel-Gateway einrichten. Das Ziel-Gateway kann ein Virtual Private Gateway oder ein Transit-Gateway sein.

## Erstellen eines Virtual Private Gateways

Während der Erstellung eines Virtual Private Gateway können Sie die benutzerdefinierte private autonome Systemnummer (ASN) für die Amazon-Seite des Gateways angeben, oder Sie verwenden die Standard-ASN von AWS. Diese ASN muss sich von der ASN unterscheiden, den Sie für den Kunden-Gateway angegeben haben.

Nachdem Sie das Virtual Private Gateway erstellt haben, müssen Sie es Ihrer VPC zuweisen.

So erstellen Sie ein Virtual Private Gateway und weisen Sie es Ihrer VPC zu

1. Wählen Sie im Navigationsbereich Virtual Private Gateways aus.
2. Wählen Sie Create virtual private gateway (Virtual Private Gateway erstellen) aus.
3. (Optional) Geben Sie bei Name-Tag einen Namen für Ihr Virtual Private Gateway ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
4. Übernehmen Sie die Standardauswahl Amazon-Standard-ASN bei Autonome Systemnummer (ASN) , um die standardmäßige Amazon ASN zu verwenden. Andernfalls wählen Sie Custom ASN (Benutzerdefinierte ASN) und geben Sie einen Wert ein. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 4200000000 und 4294967294 liegen.
5. Wählen Sie Create virtual private gateway (Virtual Private Gateway erstellen) aus.
6. Wählen Sie das Virtual Private Gateway aus, das Sie erstellt haben. Wählen Sie anschließend Actions (Aktionen), Attach to VPC (An VPC anfügen) aus.
7. Wählen Sie für Verfügbar VPCs Ihre VPC und dann Attach to VPC aus.

So erstellen Sie ein Virtual Private Gateway über die Befehlszeile oder API

- CreateVpnGateway(Amazon EC2 Query API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

So fügen Sie ein Virtual Private Gateway unter Verwendung der Befehlszeile oder API einer VPC an

- AttachVpnGateway(Amazon EC2 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

## Erstellen eines Transit-Gateways

Weitere Informationen zum Erstellen eines Transit-Gateways finden Sie unter Transit-Gateways in Amazon VPC-Transit-Gateways.

# Schritt 3: Routing konfigurieren

Damit Instances in Ihrer VPC Ihr Kunden-Gateway erreichen, müssen Sie Ihre Routing-Tabelle so konfigurieren, dass sie die Routen, die von Ihrer VPC-Verbindung verwendet werden, enthält und diese Routen zu Ihrem Virtual Private Gateway oder Transit-Gateway leitet.

## (Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle

Sie können die Route-Propagierung für Ihre Routing-Tabelle aktivieren, um Site-to-Site VPN-Routen automatisch weiterzuleiten.

Für das statisches Routing werden die statischen IP-Präfixe, die Sie in der VPN-Konfiguration angegeben haben, an die Routing-Tabelle weitergeleitet, wenn der Status der VPN-Verbindung UP ist. Gleichzeitig werden beim dynamischen Routing die durch BGP angekündigten Routen von Ihrem Kunden-Gateway an die Routing-Tabelle weitergeleitet, wenn der Status der VPN-Verbindung UP ist.

> **Note**
>
> Wenn Ihre Verbindung unterbrochen wird, die VPN-Verbindung jedoch BESTEHEN bleibt, werden die verbreiteten Routen in Ihrer Routing-Tabelle nicht automatisch entfernt. Beachten Sie dies, wenn Sie z. B. Datenverkehr als Failover über eine statische Route routen möchten. In diesem Fall müssen Sie möglicherweise die Routenverbreitung deaktivieren, um die verbreiteten Routen zu entfernen.

So aktivieren Sie die Routing-Verbreitung in der Konsole

1. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
2. Wählen Sie die Routing-Tabelle aus, die dem Subnetz zugewiesen ist.
3. Wählen Sie in der Registerkarte Routing-Verbreitung die Option Routing-Verteilung bearbeiten aus. Wählen Sie das Virual Private Gateway aus, das Sie im vorherigen Verfahren erstellt haben, und klicken Sie auf Speichern.

> **Note**
>
> Wenn Sie die Routing-Verbreitung nicht aktivieren, müssen Sie die statischen Routen, die von der VPN-Verbindung verwendet werden, manuell eingeben. Hierzu wählen Sie Ihre Routing-Tabelle und anschließend Routes, Edit aus. Fügen Sie für Destination die statische Route hinzu, die von Ihrer Site-to-Site VPN-Verbindung verwendet wird. Wählen Sie unter Target die ID des Virtual Private Gateway aus, und wählen Sie dann Save.

Deaktivieren der Routing-Verbreitung mithilfe der Konsole

1. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
2. Wählen Sie die Routing-Tabelle aus, die dem Subnetz zugewiesen ist.
3. Wählen Sie in der Registerkarte Routing-Verbreitung die Option Routing-Verteilung bearbeiten aus. Deaktivieren Sie das Kontrollkästchen Verteilen für das Virtual Private Gateway.
4. Wählen Sie Speichern.

So aktivieren Sie die Routing-Verbreitung unter Verwendung der Befehlszeile oder API

- EnableVgwRoutePropagation(Amazon EC2 Query API)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

So deaktivieren Sie die Routing-Verbreitung über die Befehlszeile oder API

- DisableVgwRoutePropagation(Amazon EC2 Query API)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

## (Transit-Gateway) Fügen Sie eine Route zu Ihrer Routing-Tabelle hinzu.

Wenn Sie die Übermittlung der Routing-Tabelle für Ihr Transit-Gateway aktiviert haben, werden die Routen für den VPN-Anhang an die Routing-Tabelle des Transit-Gateways übermittelt. Weitere Informationen finden Sie unter Routing in Amazon VPC-Transit-Gateways.

Wenn Sie eine VPC mit Ihrem Transit-Gateway verbinden und Ressourcen in der VPC in die Lage versetzen möchten, Ihr Kunden-Gateway zu erreichen, müssen Sie eine Route zu Ihrer Subnetz-Routing-Tabelle hinzufügen, die auf das Transit-Gateway verweist.

Hinzufügen einer Route zu einer VPC-Routing-Tabelle

1. Wählen Sie im Navigationsbereich Routing-Tabellen aus.
2. Wählen Sie die Routing-Tabelle aus, die Ihrer VPC zugeordnet ist.
3. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
4. Wählen Sie Add Route (Route hinzufügen) aus.
5. Geben Sie als Ziel den Ziel-IP-Adressbereich ein. Wählen Sie bei Ziel das Transit-Gateway aus.
6. Wählen Sie Änderungen speichern aus.

## Schritt 4: Ihre Sicherheitsgruppe aktualisieren

Wenn Sie möchten, dass Computer in Ihrem Netzwerk Zugriff auf die Instances in Ihrer VPC haben, müssen Sie die Regeln Ihrer Sicherheitsgruppen aktualisieren, um eingehenden SSH-, RDP- und ICMP-Zugriff zu ermöglichen.

So aktualisieren Sie Ihre Sicherheitsgruppe, um Zugriff zu ermöglichen

1. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
2. Wählen Sie die Sicherheitsgruppe für die Instances in Ihrer VPC aus, für die Sie Zugriff gewähren möchten.
3. Wählen Sie auf der Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) die Option Edt inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.
4. Fügen Sie Regeln hinzu, die den eingehenden SSH-, RDP- und ICMP-Zugriff auf Ihr Netzwerk erlauben und klicken Sie anschließend auf Regeln speichern. Weitere Informationen finden Sie unter Arbeiten mit Sicherheitsgruppenregeln im Amazon-VPC-Benutzerhandbuch.

## Schritt 5: Eine VPN-Verbindung erstellen

Erstellen Sie die VPN-Verbindung unter Verwendung des Kunden-Gateways zusammen mit dem Virtual Private Gateway oder Transit-Gateway, das Sie zuvor erstellt haben.

So erstellen Sie eine VPN-Verbindung

1. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
2. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.
3. (Optional) Geben Sie als Name-Tag einen Namen für Ihr VPN ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
4. Wählen Sie für Target gateway type (Ziel-Gateway-Typ) entweder Virtual private gateway (Virtual Private Gateway) oder Transit gateway (Transit-Gateway) aus. Wählen Sie dann das Virtual Private Gateway oder Transit-Gateway, das Sie zuvor angelegt haben.
5. Wählen Sie bei Kunden-Gateway die Option Vorhanden und das zuvor erstellte Kunden-Gateway unter Kunden-Gateway-ID aus.
6. Wählen Sie je nachdem, ob Ihr Kunden-Gateway-Gerät das Border Gateway Protocol (BGP) unterstützt, eine der Routing-Optionen aus:
   - Wenn Ihr Kunden-Gateway-Gerät BGP unterstützt, wählen Sie Dynamic (requires BGP) (Dynamisch (erfordert BGP)) aus.
   - Wenn Ihr Kunden-Gateway-Gerät BGP nicht unterstützt, wählen Sie Static (Statisch) aus. Geben Sie unter Static IP Prefixes (Statische IP-Präfixe) alle IP-Präfixe für das private Netzwerk Ihrer VPN-Verbindung an.
7. Wählen Sie den Speichertyp „Pre-Shared Key“:
   - Standard — Der Pre-Shared Key wird direkt im Site-to-Site VPN-Dienst gespeichert.
   - Secrets Manager — Der Pre-Shared Key wird gespeichert mit AWS Secrets Manager. Weitere Informationen zu Secrets Manager finden Sie unterVerbesserte Sicherheitsfunktionen mit Secrets Manager.
8. Wenn Ihr Ziel-Gateway-Typ Transit-Gateway ist, geben Sie für Tunnel-interne IP-Version an, ob die VPN-Tunnel IPv6 Datenverkehr IPv4 oder -Verkehr unterstützen. IPv6 Datenverkehr wird nur für VPN-Verbindungen auf einem Transit-Gateway unterstützt.
9. Wenn Sie die IP-Version IPv4für Tunnel angegeben haben, können Sie optional die IPv4 CIDR-Bereiche für das Kunden-Gateway und die AWS Seiten angeben, die über die VPN-Tunnel kommunizieren dürfen. Der Standardwert ist `0.0.0.0/0`.

   Wenn Sie die IP-Version IPv6für Tunnel angegeben haben, können Sie optional die IPv6 CIDR-Bereiche für das Kunden-Gateway und die AWS Seiten angeben, die über die VPN-Tunnel kommunizieren dürfen. Die Standardeinstellung für beide Bereiche lautet `::/0`.
10. Wählen Sie für den Typ der externen IP-Adresse eine der folgenden Optionen aus:

- PublicIpv4 — (Standard) Verwenden Sie IPv4 Adressen für den Außentunnel IPs.
- IPv6- Verwenden Sie IPv6 Adressen für den Außentunnel IPs. Diese Option ist nur für VPN-Verbindungen auf einem Transit-Gateway oder Cloud-WAN verfügbar.

11. (Optional) Für Tunneloptionen können Sie für jeden Tunnel die folgenden Informationen angeben:

    - Ein IPv4 CIDR-Block der Größe /30 aus dem `169.254.0.0/16` Bereich für interne IPv4 Tunneladressen.
    - Wenn Sie IPv6für die Version Tunnel inside IP einen IPv6 CIDR-Block /126 aus dem `fd00::/8` Bereich für interne Tunneladressen angegeben haben. IPv6
    - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 oder. IKEv2
    - Um die erweiterten Optionen für Ihren Tunnel zu bearbeiten, wählen Sie Tunneloptionen bearbeiten aus. Weitere Informationen finden Sie unter VPN-Tunneloptionen.
12. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus. Der Aufbau der VPN-Verbindung kann einige Minuten dauern.

So erstellen Sie eine VPN-Verbindung über die Befehlszeile oder API

- CreateVpnConnection(Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)

  Beispiel für die Erstellung einer VPN-Verbindung mit IPv6 Außentunnel IPs und IPv6 Innentunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

  Beispiel für den Aufbau einer VPN-Verbindung mit IPv6 Außentunnel IPs und IPv4 Innentunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

## Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen

Nachdem Sie die VPN-Verbindung erstellt haben, können Sie eine Beispielkonfigurationsdatei herunterladen, die zur Konfiguration des Kunden-Gateway-Geräts verwendet wird.

> **Important**
>
> Die Konfigurationsdatei ist nur ein Beispiel und entspricht möglicherweise nicht genau den von Ihnen beabsichtigten VPN-Verbindungseinstellungen. Es spezifiziert die Mindestanforderungen für eine VPN-Verbindung von AES128 SHA1, und Diffie-Hellman-Gruppe 2 in den meisten AWS Regionen und, AES128 SHA2, und Diffie-Hellman-Gruppe 14 in den Regionen. AWS GovCloud Es legt außerdem Pre-Shared-Key für die Authentifizierung fest. Sie müssen die Beispielkonfigurationsdatei ändern, um zusätzliche SicherheitsalGORITHmen, Diffie-Hellman-Gruppen, private Zertifikate und Datenverkehr zu nutzen. IPv6
> Wir haben IKEv2 Unterstützung in den Konfigurationsdateien für viele beliebte Kunden-Gateway-Geräte eingeführt und werden im Laufe der Zeit weitere Dateien hinzufügen. Eine Liste der IKEv2 unterstützten Konfigurationsdateien finden Sie unterAWS Site-to-Site VPN Kunden-Gateway-Geräte.

Berechtigungen

Um den Download-Konfigurationsbildschirm von korrekt zu laden, müssen Sie sicherstellen AWS Management Console, dass Ihre IAM-Rolle oder Ihr IAM-Benutzer über Berechtigungen für das folgende Amazon verfügt EC2 APIs: `GetVpnConnectionDeviceTypes` und`GetVpnConnectionDeviceSampleConfiguration`.

So laden Sie die Konfigurationsdatei mit der Konsole herunter

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie erst Ihre VPN-Verbindung und dann Konfiguration herunterladen aus.

4. Wählen Sie den Anbieter, die Plattform, die Software und die IKE-Version aus, die dem Kunden-Gateway-Gerät entsprechen. Wenn Ihr Gerät nicht aufgeführt ist, wählen Sie Generic (Generisch) aus.
5. Wählen Sie Herunterladen aus.

Beispielkonfigurationsdatei mit der -Befehlszeile oder -API herunterladen

- GetVpnConnectionDeviceTypes( EC2 Amazon-API)
- GetVpnConnectionDeviceSampleConfiguration(Amazon EC2 Query API)
- get-vpn-connection-device-Typen ()AWS CLI
- get-vpn-connection-device-Beispielkonfiguration ()AWS CLI

## Schritt 7: Das Kunden-Gateway-Gerät konfigurieren

Verwenden Sie die Beispielkonfigurationsdatei, um Ihr Kunden-Gateway-Gerät zu konfigurieren. Das Kunden-Gateway-Gerät ist das physische Gerät oder die Software-Anwendung auf Ihrer Seite der VPN-Verbindung. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Kunden-Gateway-Geräte.

# AWS Site-to-Site VPN architektonische Szenarien

Im Folgenden sind Szenarien aufgeführt, in denen Sie mehrere VPN-Verbindungen mit einem oder mehreren Kunden-Gateway-Geräten erstellen könnten.

Mehrere VPN-Verbindungen unter Verwendung desselben Kunden-Gateway-Geräts

Sie können mit demselben Kunden-Gateway-Gerät zusätzliche VPN-Verbindungen von Ihrem lokalen Standort zu anderen VPCs herstellen. Sie können auf dem Kunden-Gateway eine einzige IP-Adresse für alle VPN-Verbindungen verwenden.

Mehrere Kunden-Gateway-Geräte zu einem einzigen virtuellen privaten Gateway ()AWS VPN CloudHub

Sie können mehrere VPN-Verbindungen von mehreren Kunden-Gateway-Geräten mit einem einzelnen Virtual Private Gateway einrichten. Auf diese Weise können Sie mehrere Standorte mit dem AWS VPN verbinden CloudHub. Weitere Informationen finden Sie unter Sichere Kommunikation zwischen AWS Site-to-Site VPN Verbindungen mithilfe von VPN CloudHub. Wenn Sie über Kunden-Gateway-Geräte an mehreren geografischen Standorten verfügen, sollte jedes Gerät einen eindeutigen Satz IP-Bereiche für den jeweiligen Standort ankündigen.

Redundante VPN-Verbindung mit einem zweiten Kunden-Gateway-Gerät

Zum Schutz vor einem Verbindungsverlust, wenn Ihr Kunden-Gateway-Gerät nicht mehr verfügbar ist, können Sie eine zweite VPN-Verbindung mit einem zweiten Kunden-Gateway-Gerät einrichten. Weitere Informationen finden Sie unter Redundante AWS Site-to-Site VPN Verbindungen für Failover. Wenn Sie redundante Kunden-Gateway-Geräte an einem Standort einrichten, sollten beide Geräte dieselben IP-Bereiche ankündigen.

Die folgenden Site-to-Site VPN-Architekturen sind gebräuchlich:

- Einzel- und Mehrfach-VPN-Verbindungen
- the section called “Redundante VPN-Verbindungen”
- Sichere Kommunikation zwischen VPN-Verbindungen mithilfe von VPN CloudHub

# AWS Site-to-Site VPN Beispiele für einzelne und mehrere VPN-Verbindungen

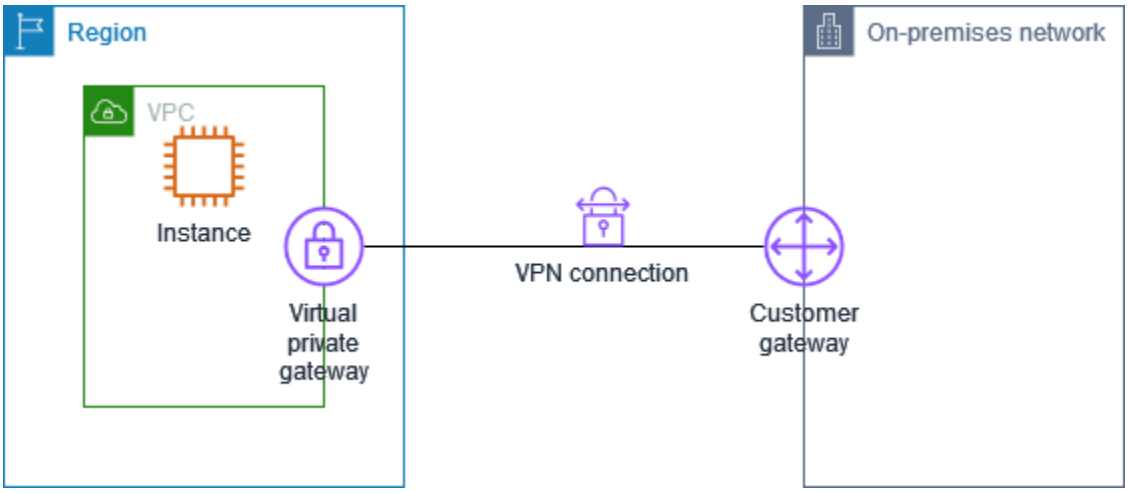
Die folgenden Diagramme veranschaulichen einzelne und mehrere Site-to-Site VPN-Verbindungen.

Beispiele

- Einzelne Site-to-Site VPN-Verbindung
- Einzelne Site-to-Site VPN-Verbindung mit einem Transit-Gateway
- Mehrere Site-to-Site VPN-Verbindungen
- Mehrere Site-to-Site VPN-Verbindungen mit einem Transit-Gateway
- Site-to-Site VPN-Verbindung mit AWS Direct Connect
- Private Site-to-Site IP-VPN-Verbindung mit AWS Direct Connect

## Einzelne Site-to-Site VPN-Verbindung

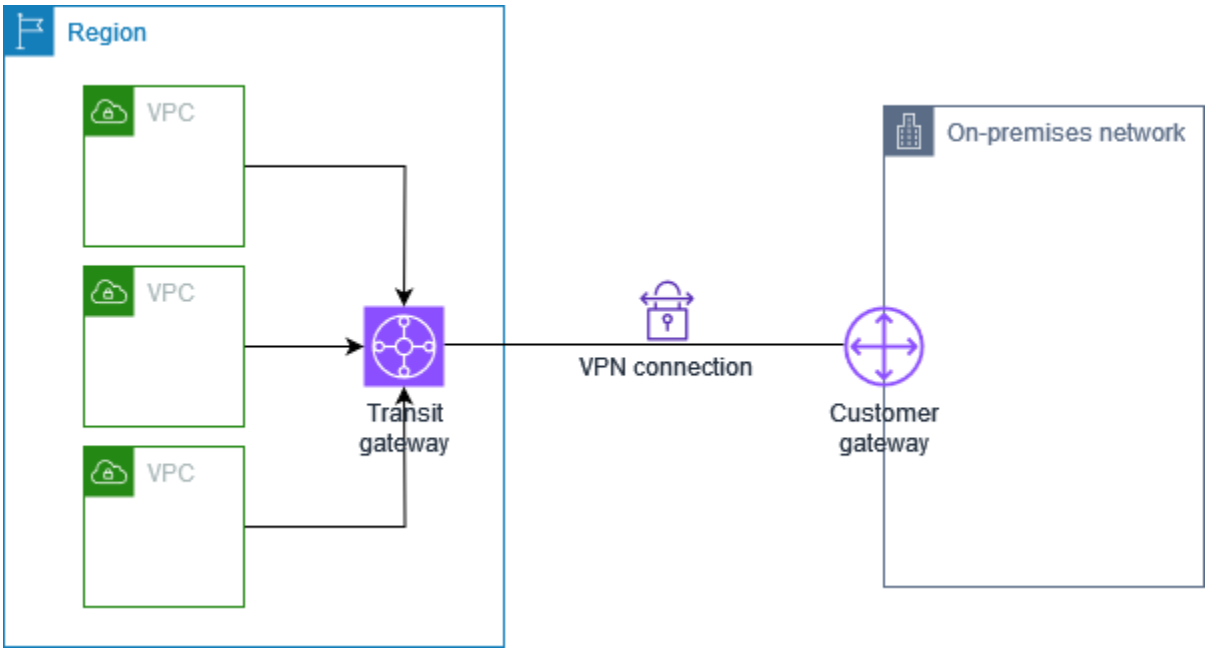
Die VPC verfügt über ein hinzugefügtes Virtual Private Gateway. Ihr On-Premises-Netzwerk (Remote) enthält ein Kunden-Gateway-Gerät, das Sie konfigurieren müssen, um die VPN-Verbindung zu aktivieren. Sie müssen die VPN-Routing-Tabellen so aktualisieren, dass jeglicher Datenverkehr von der VPC zu Ihrem Netzwerk über das Virtual Private Gateway geleitet wird.




Schritte zum Einrichten dieses Szenarios finden Sie unter Fangen Sie an mit AWS Site-to-Site VPN.

## Einzelne Site-to-Site VPN-Verbindung mit einem Transit-Gateway

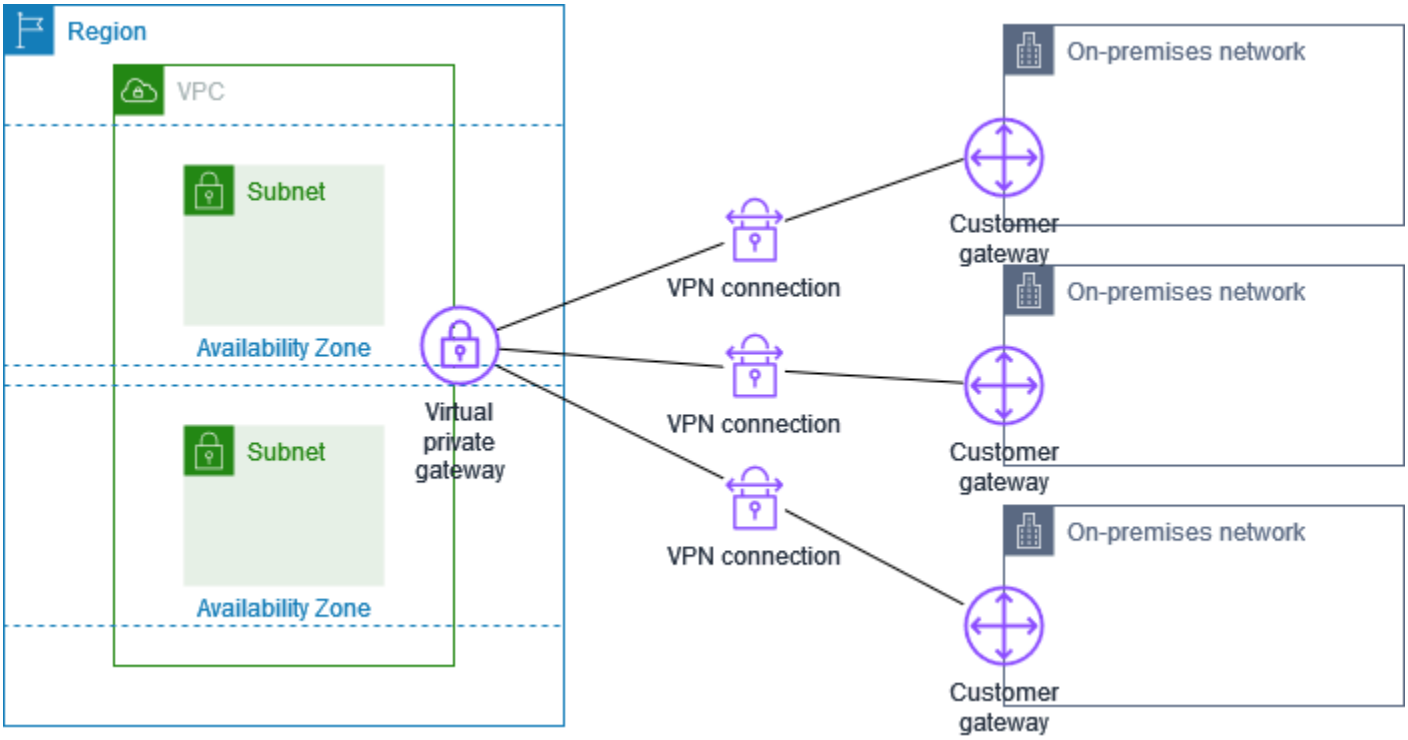
Die VPC verfügt über ein angefügtes Transit-Gateway. Ihr On-Premises-Netzwerk (Remote) enthält ein Kunden-Gateway-Gerät, das Sie konfigurieren müssen, um die VPN-Verbindung zu aktivieren. Sie müssen die VPN-Routing-Tabellen so aktualisieren, dass jeglicher Datenverkehr von der VPC zu Ihrem Netzwerk über das Transit-Gateway geleitet wird.




Schritte zum Einrichten dieses Szenarios finden Sie unter Fangen Sie an mit AWS Site-to-Site VPN.

## Mehrere Site-to-Site VPN-Verbindungen

Die VPC verfügt über ein angeschlossenes virtuelles privates Gateway, und Sie haben mehrere Site-to-Site VPN-Verbindungen zu mehreren lokalen Standorten. Sie richten das Routing so ein, dass der gesamte VPC-Datenverkehr, der für Ihr Netzwerk vorgesehen ist, zum Virtual Private Gateway geleitet wird.

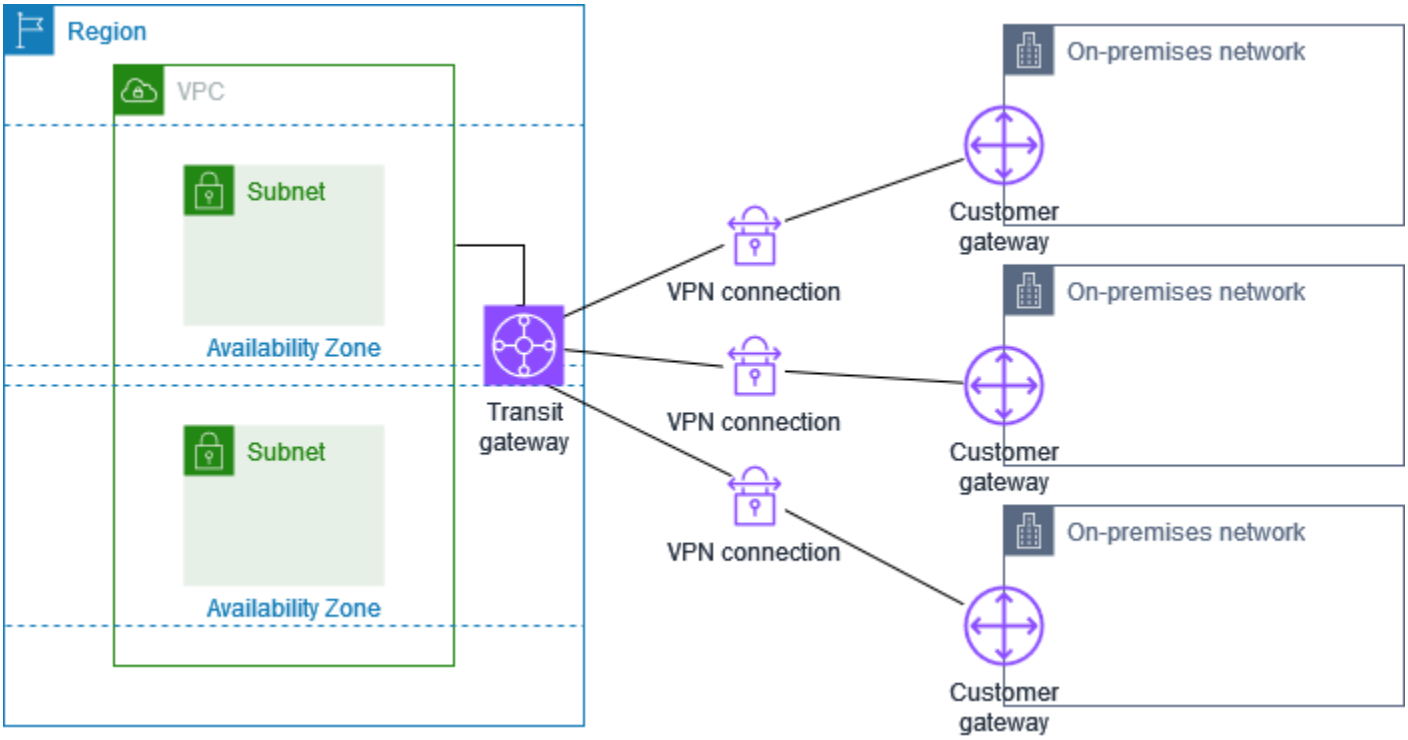



Wenn Sie mehrere Site-to-Site VPN-Verbindungen zu einer einzelnen VPC erstellen, können Sie ein zweites Kunden-Gateway konfigurieren, um eine redundante Verbindung zu demselben externen Standort herzustellen. Weitere Informationen finden Sie unter Redundante AWS Site-to-Site VPN Verbindungen für Failover.

Sie können dieses Szenario auch verwenden, um Site-to-Site VPN-Verbindungen zu mehreren geografischen Standorten herzustellen und eine sichere Kommunikation zwischen Standorten zu gewährleisten. Weitere Informationen finden Sie unter Sichere Kommunikation zwischen AWS Site-to-Site VPN Verbindungen mithilfe von VPN CloudHub.

## Mehrere Site-to-Site VPN-Verbindungen mit einem Transit-Gateway

Die VPC verfügt über ein angeschlossenes Transit-Gateway, und Sie haben mehrere Site-to-Site VPN-Verbindungen zu mehreren lokalen Standorten. Sie richten das Routing so ein, dass der gesamte Datenverkehr von der VPC, der für Ihre Netzwerke bestimmt ist, zum Transit-Gateway geleitet wird.

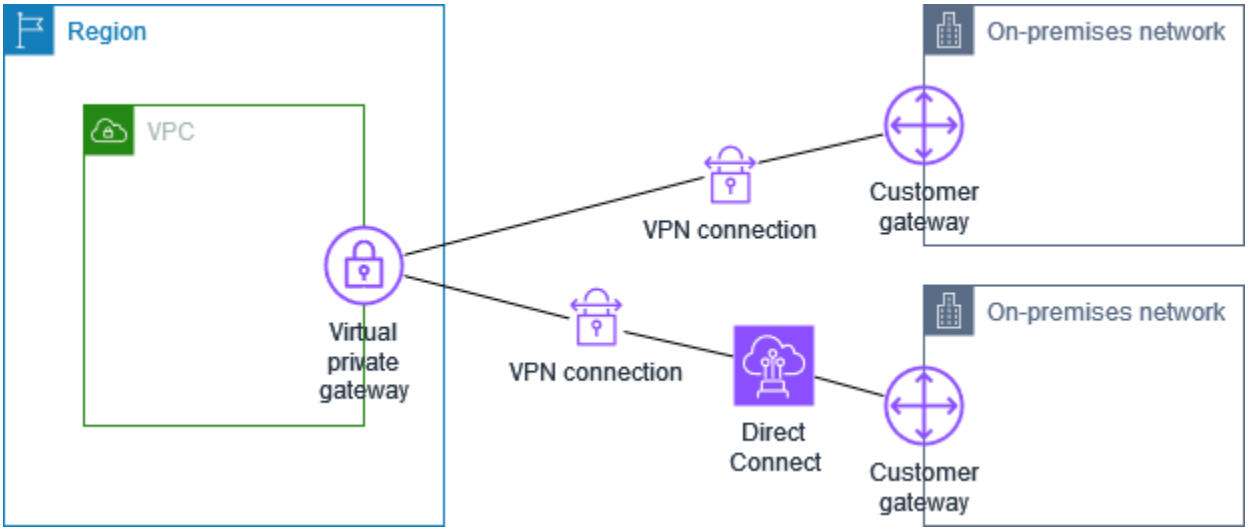



Wenn Sie mehrere Site-to-Site VPN-Verbindungen zu einem einzelnen Transit-Gateway erstellen, können Sie ein zweites Kunden-Gateway konfigurieren, um eine redundante Verbindung zu demselben externen Standort herzustellen.

Sie können dieses Szenario auch verwenden, um Site-to-Site VPN-Verbindungen zu mehreren geografischen Standorten herzustellen und eine sichere Kommunikation zwischen Standorten zu gewährleisten.

## Site-to-Site VPN-Verbindung mit AWS Direct Connect

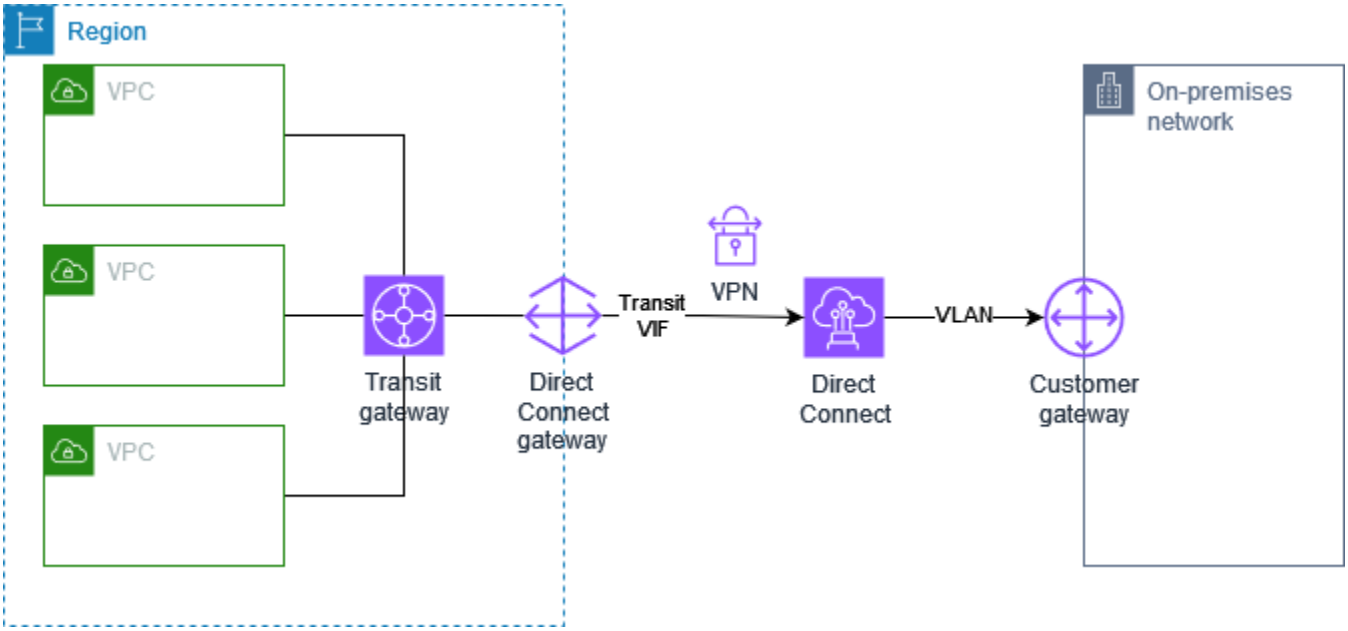
Die VPC verfügt über ein angeschlossenes virtuelles privates Gateway und stellt über eine Verbindung zu Ihrem lokalen (Remote-) Netzwerk eine Verbindung her. AWS Direct Connect Sie können eine AWS Direct Connect öffentliche virtuelle Schnittstelle konfigurieren, um über ein virtuelles privates Gateway eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS Ressourcen herzustellen. Sie richten das Routing so ein, dass der gesamte Datenverkehr von der VPC, der für Ihr Netzwerk bestimmt ist, an das Virtual Private Gateway und die AWS Direct Connect Verbindung weitergeleitet wird.




Wenn AWS Direct Connect sowohl die VPN-Verbindung als auch die VPN-Verbindung auf demselben virtuellen privaten Gateway eingerichtet sind, kann das Hinzufügen oder Entfernen von Objekten dazu führen, dass das virtuelle private Gateway in den Status „Anhängen“ wechselt. Dies deutet darauf hin, dass eine Änderung am internen Routing vorgenommen wird, das zwischen AWS Direct Connect und der VPN-Verbindung wechselt, um Unterbrechungen und Paketverlust zu minimieren. Wenn dies abgeschlossen ist, kehrt das Virtual Private Gateway in den Status „anfügen“ zurück.

## Private Site-to-Site IP-VPN-Verbindung mit AWS Direct Connect

Mit einem privaten Site-to-Site IP-VPN können Sie den AWS Direct Connect Verkehr zwischen Ihrem lokalen Netzwerk und AWS ohne die Verwendung öffentlicher IP-Adressen verschlüsseln. Private IP VPN Over AWS Direct Connect stellt sicher, dass der Datenverkehr zwischen AWS und lokalen Netzwerken sowohl sicher als auch privat ist, sodass Kunden die gesetzlichen Vorschriften und Sicherheitsvorschriften einhalten können.



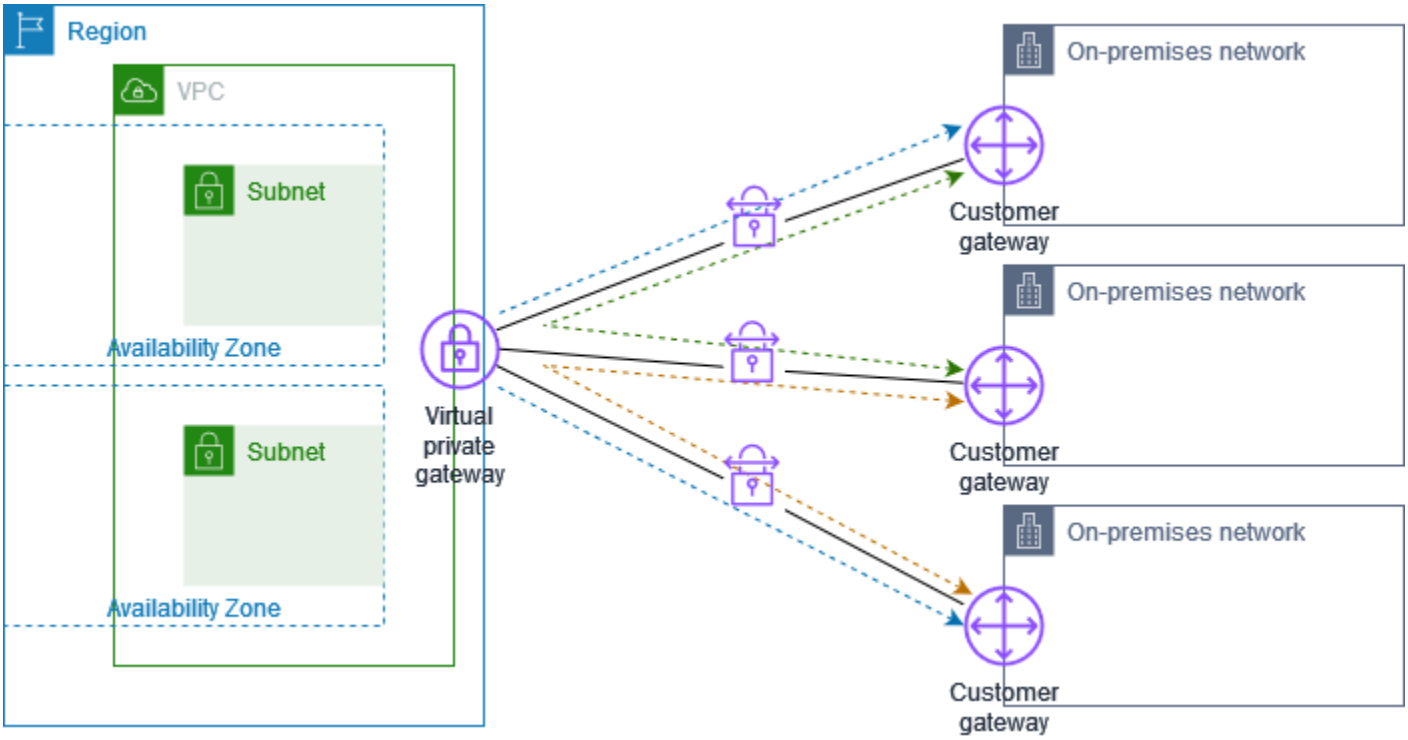

Weitere Informationen finden Sie im folgenden Blogbeitrag: Einführung in AWS Site-to-Site VPN Private IP VPNs.

# Sichere Kommunikation zwischen AWS Site-to-Site VPN Verbindungen mithilfe von VPN CloudHub

Wenn Sie mehrere AWS Site-to-Site VPN Verbindungen haben, können Sie mithilfe des AWS VPN CloudHub eine sichere Kommunikation zwischen Standorten bereitstellen. Dies ermöglicht den Standorten die Kommunikation untereinander und nicht nur mit den Ressourcen in Ihrer VPC. Das VPN CloudHub arbeitet nach einem einfachen hub-and-spoke Modell, das Sie mit oder ohne VPC verwenden können. Dieses Design eignet sich, wenn Sie über mehrere Niederlassungen und bestehende Internetverbindungen verfügen und ein praktisches, potenziell kostengünstiges hub-and-spoke Modell für die Primär- oder Backup-Konnektivität zwischen diesen Standorten implementieren möchten.

## Übersicht

Das folgende Diagramm zeigt die CloudHub VPN-Architektur. Die gestrichelten Linien zeigen den Netzwerkverkehr zwischen entfernten Standorten, der über die VPN-Verbindungen geleitet wird. Die IP-Bereiche der Standorte dürfen sich nicht überschneiden.




Führen Sie für dieses Szenario die folgenden Schritte aus:

1. Erstellen Sie ein einzelnes Virtual Private Gateway.
2. Erstellen Sie mehrere Kunden-Gateways, jedes mit der öffentlichen IP-Adresse des Gateways. Sie müssen eine eindeutige Border Gateway Protocol (BGP) Autonomous System Number (ASN) für jedes Kunden-Gateway verwenden.
3. Erstellen Sie eine dynamisch geroutete Site-to-Site VPN-Verbindung von jedem Kunden-Gateway zum gemeinsamen Virtual Private Gateway.
4. Konfigurieren Sie die Kunden-Gateway-Geräte so, dass dem Virtual Private Gateway ein standortspezifisches Präfix (z. B. 10.0.0.0/24, 10.0.1.0/24) vorangestellt wird. Diese Routing-Ankündigungen werden empfangen und jedem BGP-Peer neu angekündigt, sodass jeder Standort Daten senden und von anderen Standorten Daten empfangen kann. Dies erfolgt mithilfe der Netzwerkanweisungen in den VPN-Konfigurationsdateien für die Site-to-Site VPN-Verbindung. Die Netzwerkanweisungen unterscheiden sich etwas, je nachdem welchen Router-Typ Sie verwenden.
5. Konfigurieren Sie die Routen in Ihren Subnetz-Routing-Tabellen, damit die Instances in Ihrer VPC mit Ihren Standorten kommunizieren können. Weitere Informationen finden Sie unter (Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle. Sie können eine aggregierte Route in Ihrer Routing-Tabelle konfigurieren (z. B. 10.0.0.0/16). Verwenden Sie spezifischere Präfixe zwischen Kunden-Gateway-Geräten und dem Virtual Private Gateway.

Websites, die AWS Direct Connect Verbindungen zum Virtual Private Gateway verwenden, können ebenfalls Teil des AWS VPN sein CloudHub. Beispielsweise kann Ihre Unternehmenszentrale in New York eine AWS Direct Connect Verbindung zur VPC haben und Ihre Niederlassungen können Site-to-Site VPN-Verbindungen zur VPC verwenden. Die Niederlassungen in Los Angeles und Miami können Daten untereinander und mit Ihrer Unternehmenszentrale senden und empfangen, und das alles über das AWS VPN. CloudHub

## Preisgestaltung

Um AWS VPN zu nutzen CloudHub, zahlen Sie die typischen Amazon Site-to-Site VPC-VPN-Verbindungsgebühren. Ihnen werden für jede Stunde, die die einzelnen VPNs mit dem Virtual Private Gateway verbunden sind, Verbindungsgebühren in Rechnung gestellt. Wenn Sie mithilfe des AWS VPN Daten von einem Standort zu einem anderen senden CloudHub, fallen keine Kosten für das Senden von Daten von Ihrer Site an das Virtual Private Gateway an. Sie bezahlen nur den standardmäßigen AWS -Übertragungssatz für Daten, die vom Virtual Private Gateway zu Ihrem Endpunkt übermittelt werden.

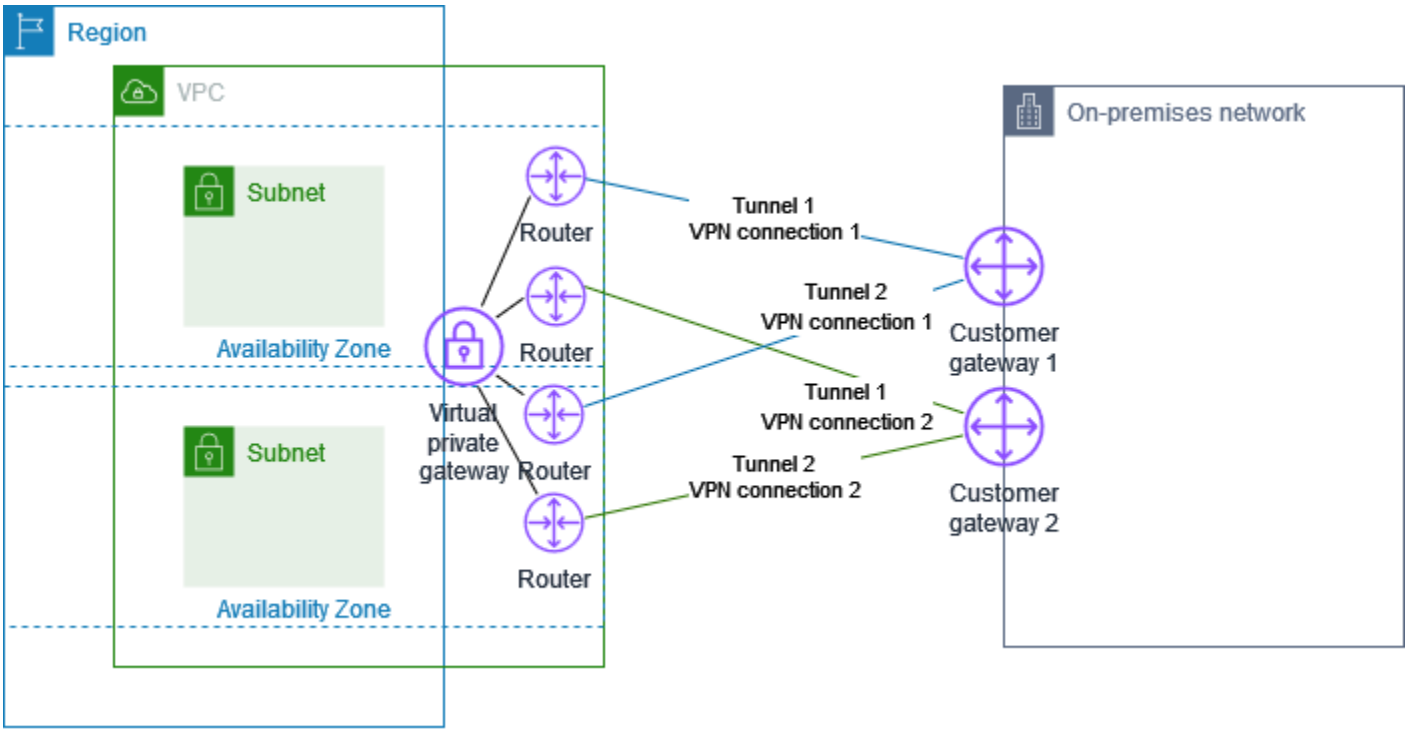
Wenn Sie beispielsweise einen Standort in Los Angeles und einen zweiten Standort in New York haben und beide Standorte über eine Site-to-Site VPN-Verbindung zum Virtual Private Gateway verfügen, zahlen Sie für jede Site-to-Site VPN-Verbindung den Stundensatz (wenn der Tarif also 0,05 USD pro Stunde betragen würde, wären dies insgesamt 0,10 USD pro Stunde). Sie zahlen auch die AWS Standard-Datenübertragungsgebühren für alle Daten, die Sie von Los Angeles nach New York (und umgekehrt) senden und die jede Site-to-Site VPN-Verbindung durchqueren. Netzwerkverkehr, der über die Site-to-Site VPN-Verbindung an das Virtual Private Gateway gesendet wird, ist kostenlos, aber Netzwerkverkehr, der über die Site-to-Site VPN-Verbindung vom Virtual Private Gateway zum Endpunkt gesendet wird, wird zum AWS Standard-Datenübertragungstarif abgerechnet.

Weitere Informationen finden Sie unter Site-to-Site Preise für VPN-Verbindungen.

# Redundante AWS Site-to-Site VPN Verbindungen für Failover

Um sich vor einem Verbindungsverlust zu schützen, falls Ihr Kunden-Gateway-Gerät nicht verfügbar ist, können Sie eine zweite Site-to-Site VPN-Verbindung zu Ihrer VPC und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway-Gerät hinzufügen. Durch die Verwendung redundanter VPN-Verbindungen und Kunden-Gateway-Geräte können Sie die Wartung auf einem Ihrer Kunden-Gateways durchführen, während der Datenverkehr weiter über die zweite VPN-Verbindung geleitet wird.

In der folgenden Abbildung zeigt zwei VPN-Verbindungen. Jede VPN-Verbindung hat ihre eigenen Tunnel und ihr eigenes Kunden-Gateway.




Führen Sie für dieses Szenario die folgenden Schritte aus:

- Richten Sie eine zweite Site-to-Site VPN-Verbindung ein, indem Sie dasselbe Virtual Private Gateway verwenden und ein neues Kunden-Gateway erstellen. Die Kunden-Gateway-IP-Adresse für die zweite Site-to-Site VPN-Verbindung muss öffentlich zugänglich sein.
- Konfigurieren Sie ein zweites Kunden-Gateway-Gerät. Beide Geräte sollten dem Virtual Private Gateway dieselben IP-Bereiche angeben. Wir nutzen BGP-Routing, um den Pfad für den Datenverkehr zu ermitteln. Wenn ein Kunden-Gateway-Gerät ausfällt, leitet das Virtual Private Gateway den gesamten Datenverkehr an das andere Kunden-Gateway-Gerät um.

Dynamisch geroutete Site-to-Site VPN-Verbindungen verwenden das Border Gateway Protocol (BGP), um Routing-Informationen zwischen Ihren Kunden-Gateways und den Virtual Private Gateways auszutauschen. Bei statisch gerouteten Site-to-Site VPN-Verbindungen müssen Sie statische Routen für das Remote-Netzwerk auf Ihrer Seite des Kunden-Gateways eingeben. Über BGP angekündigte Routen und statisch eingegebene Routen-Informationen helfen den Gateways auf beiden Seiten zu erfassen, welche Tunnel verfügbar sind und den Datenverkehr im Falle eines Ausfalls umzuleiten. Wir empfehlen, dass Sie Ihr Netzwerk so konfigurieren, dass es die vom BGP

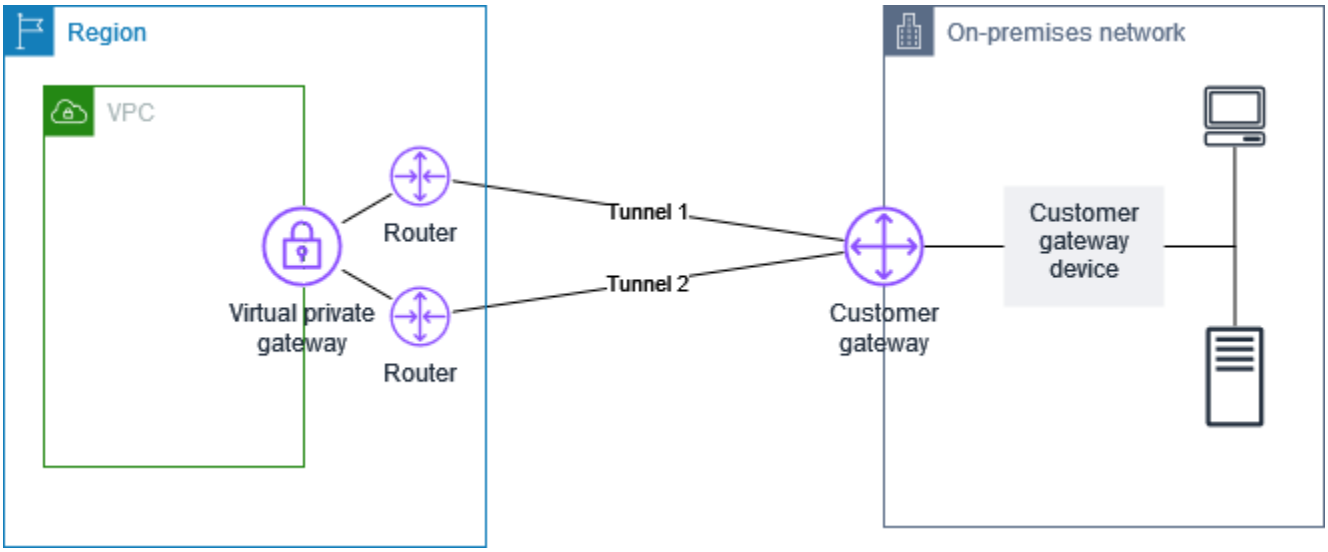
bereitgestellten Routing-Informationen verwendet (sofern verfügbar), um einen verfügbaren Pfad auszuwählen. Die genaue Konfiguration hängt von der Architektur Ihres Netzwerks ab.

Weitere Informationen zum Erstellen und Konfigurieren eines Kunden-Gateways und einer Site-to-Site VPN-Verbindung finden Sie unter. Fangen Sie an mit AWS Site-to-Site VPN

# AWS Site-to-Site VPN Kunden-Gateway-Geräte

Ein Kunden-Gateway-Gerät ist eine physische oder Software-Appliance, die Ihnen gehört oder die Sie in Ihrem lokalen Netzwerk verwalten (auf Ihrer Seite einer Site-to-Site VPN-Verbindung). Sie oder Ihr Netzwerkadministrator müssen das Gerät so konfigurieren, dass es mit der Site-to-Site VPN-Verbindung funktioniert.

Das folgende Diagramm zeigt Ihr Netzwerk, das Kunden-Gateway-Gerät und die VPN-Verbindung, die zu einem Virtual Private Gateway führt, das Ihrer VPC zugewiesen ist. Die beiden Verbindungen zwischen dem Kunden-Gateway und dem Virtual Private Gateway stellen die Tunnel für die VPN-Verbindung dar. Wenn innerhalb des Geräts ein Geräteausfall auftritt AWS, wechselt Ihre VPN-Verbindung automatisch zum zweiten Tunnel, sodass Ihr Zugriff nicht unterbrochen wird. Führt von Zeit zu Zeit AWS auch routinemäßige Wartungsarbeiten an der VPN-Verbindung durch, wodurch einer der beiden Tunnel Ihrer VPN-Verbindung kurzzeitig deaktiviert werden kann. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Ersatz von Tunnelendpunkten. Konfigurieren Sie Ihr Kunden-Gateway-Gerät daher während der Konfiguration unbedingt auf die Verwendung beider Tunnel.




Informationen zu den Schritten zum Einrichten einer VPN-Verbindung finden Sie unter Fangen Sie an mit AWS Site-to-Site VPN. Während dieses Vorgangs erstellen Sie eine Kunden-Gateway-Ressource in AWS, die Informationen AWS über Ihr Gerät bereitstellt, z. B. seine öffentlich zugängliche IP-Adresse. Weitere Informationen finden Sie unter Kunden-Gateway-Optionen für Ihre AWS Site-to-Site VPN Verbindung. Die Kunden-Gateway-Ressource in konfiguriert oder erstellt das Kunden-Gateway-Gerät AWS nicht. Sie müssen das Gerät selbst konfigurieren.

Hier finden Sie softwarebasierte VPN-Anwendungen:AWS Marketplace.

# Anforderungen für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät

AWS unterstützt eine Reihe von Site-to-Site VPN-Kunden-Gateway-Geräten, für die wir Konfigurationsdateien zum Herunterladen bereitstellen. Eine Liste der unterstützten Geräte und die Schritte zum Herunterladen der Konfigurationsdateien finden Sie unterStatische und dynamische Routing-Konfigurationsdateien.

Wenn Sie ein Gerät haben, das nicht in der Liste der unterstützten Geräte aufgeführt ist, werden im folgenden Abschnitt die Anforderungen beschrieben, die das Gerät erfüllen muss, um eine Site-to-Site VPN-Verbindung herzustellen.

Die Konfiguration Ihres Kunden-Gateway-Geräts umfasst vier zentrale Elemente. Die folgenden Symbole stellen die einzelnen Teile der Konfiguration dar.

| | |
|---|---|
| IKE | IKE-Sicherheitszuordnung (Internet Key Exchange). Dies ist für den Austausch von Schlüsseln erforderlich, die zur Einrichtung der IPsec Sicherheitsbeziehung verwendet wurden. |
| IPsec | IPsec Sicherheitsverband. Damit wird die Verschlüsselung, die Authentifizierung usw. des Tunnels abgewickelt. |
| Tunnel | Tunnelschnittstelle. Dadurch wird der zum und vom Tunnel gehende Datenverkehr empfangen. |
| BGP | (Optional) BGP-Peering (Border Gateway Protocol). Bei Geräten, die BGP verwenden, tauscht dies Routen zwischen dem Kunden-Gateway-Gerät und dem Virtual Private Gateway aus. |

In der folgenden Tabelle sind die Anforderungen für das Kunden-Gateway-Gerät, der zugehörige RFC (als Referenz) und Kommentare zu den Anforderungen aufgeführt.

Jede VPN-Verbindung besteht aus zwei separaten Tunneln. Jeder Tunnel enthält eine IKE-Sicherheitsverbindung, eine IPsec Sicherheitsverbindung und ein BGP-Peering. Sie sind auf ein eindeutiges Sicherheitszuordnungspaar (SA) pro Tunnel (ein eingehender und ein ausgehender) und

somit auf insgesamt zwei eindeutige SA-Paare für zwei Tunnel (vier) beschränkt. SAs Einige Geräte verwenden ein richtlinienbasiertes VPN und erstellen bis zu viele SAs ACL-Einträge. Daher müssen Sie möglicherweise Ihre Regeln konsolidieren und dann filtern, damit Sie keinen unerwünschten Datenverkehr zulassen.

Standardmäßig wird der VPN-Tunnel bei der Generierung von Datenverkehr gestartet und die IKE-Aushandlung von Ihrer Seite der VPN-Verbindung initiiert wird. Sie können die VPN-Verbindung so konfigurieren, dass die IKE-Verhandlung stattdessen von der AWS Seite der Verbindung aus initiiert wird. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Optionen zur Tunnelinitiierung.

VPN-Endpunkte unterstützen die Erstellung neuer Schlüssel und können kurz vor Ablauf von Phase 1 Neuverhandlungen starten, wenn das Kunden-Gateway-Gerät keinen Neuverhandlungsdatenverkehr gesendet hat.

| Anforderung | RFC | Kommentare |
| --- | --- | --- |
| IKE-Sicherheitszuordnung herstellen<br><br>IKE | RFC 2409<br><br>RFC 7296 | Die IKE-Sicherheitsverbindung wird zunächst zwischen dem virtuellen privaten Gateway und dem Kunden-Gateway-Gerät mithilfe eines vorab gemeinsam genutzten Schlüssels oder eines privaten Zertifikats, das AWS Private Certificate Authority als Authentifikator verwendet wird, hergestellt. Wenn es eingerichtet ist, handelt IKE einen kurzlebigen Schlüssel aus, um zukünftige IKE-Nachrichten zu sichern. Die Parameter müssen vollständig übereinstimmen, einschließlich der Verschlüsselungs- und Authentifizierungsparameter.<br><br>Wenn Sie in eine VPN-Verbindung herstellen AWS, können Sie für jeden Tunnel Ihren eigenen Pre-Shared Key angeben oder einen für Sie AWS generieren lassen. Alternativ können Sie das private Zertifikat angeben, das für Ihr Kunden-Gateway-Gerät verwendet werden AWS Private Certificate Authority soll. Weitere Informationen zum Konfigurieren von VPN-Tunneln finden Sie unter Tunneloptionen für Ihre AWS Site-to-Site VPN Verbindung. |

| Anforderung | RFC | Kommentare |
| --- | --- | --- |
| | | Die folgenden Versionen werden unterstützt: IKEv1 und IKEv2.<br><br>Wir unterstützen den Hauptmodus nur mit IKEv1.<br><br>Der Site-to-Site VPN-Dienst ist eine routenbasierte Lösung. Wenn Sie eine richtlinienbasierte Konfigura tion verwenden, müssen Sie Ihre Konfiguration auf eine einzelne Sicherheitszuordnung beschränken. |
| Richten Sie IPsec Sicherheitszuordnungen im Tunnelmodus ein<br><br>IPsec | RFC 4301 | Mithilfe des kurzlebigen IKE-Schlüssels werden Schlüssel zwischen dem Virtual Private Gateway und dem Kunden-Gateway-Gerät eingerichtet, um eine IPsec Sicherheitsverbindung (SA) zu bilden. Der Datenverkehr zwischen den Gateways wird über diese SA ver- und entschlüsselt. Die kurzlebigen Schlüssel, die zur Verschlüsselung des Datenverkehrs innerhalb der IPsec SA verwendet werden, werden von IKE regelmäßig automatisch rotiert, um die Vertraulichkeit der Kommunikation zu gewährleisten. |
| Verwenden der AES 128-Bit- oder AES 256-Bit-V erschlüsselungsfunktion | RFC 3602 | Die Verschlüsselungsfunktion wird verwendet, um den Datenschutz sowohl für IKE als auch für Sicherhei tszuordnungen zu gewährleisten. IPsec |
| Verwenden Sie die SHA-1- oder SHA-2 (256)-Hash-Funktion | RFC 2404 | Diese Hashing-Funktion wird verwendet, um sowohl IKE- als auch IPsec Sicherheitszuordnungen zu authentifizieren. |

| Anforderung | RFC | Kommentare |
| --- | --- | --- |
| Verwenden von Diffie-Hellman Perfect Forward Secrecy. | RFC 2409 | IKE nutzt Diffie-Hellman zur Etablierung der temporären Schlüssel zur Absicherung der gesamten Kommunikation zwischen Kunden-Gateway-Geräten und Virtual Private Gateways.<br><br>Folgende Gruppen werden unterstützt:<br><br>• Phase 1-Gruppen: 2, 14-24<br>• Phase 2-Gruppen: 2, 5, 14-24 |
| (Dynamisch geroutete VPN-Verbindungen) Verwenden Sie Dead Peer Detection IPsec | RFC 3706 | Die Nutzung von Dead Peer Detection ermöglicht den VPN-Geräten die schnelle Erkennung von Netzwerkbedingungen, die verhindern, dass Pakete über das Internet zugestellt werden können. Wenn dies auftritt, löschen die Gateways die Sicherheitsaushandlungen und versuchen, neue Aushandlungen zu erstellen. Während dieses Vorgangs wird, wenn möglich, der alternative IPsec Tunnel verwendet. |
| (Dynamisch geroutete VPN-Verbindungen) Binden Sie den Tunnel an die logische Schnittstelle (routenbasiertes VPN)<br><br>Tunnel | Keine | Ihr Gerät muss in der Lage sein, den IPsec Tunnel an eine logische Schnittstelle zu binden. Die logische Schnittstelle umfasst eine IP-Adresse, die zur Etablierung des BGP-Peerings mit dem Virtual Private Gateway verwendet wird. Die logische Schnittstelle sollte keine zusätzliche Kapselung durchführen (z. B. GRE oder IP in IP). Die Schnittstelle sollte mit einer MTU (Maximum Transmission Unit) von 1399 Byte konfiguriert sein. |
| (Dynamisch geroutete VPN-Verbindungen) Richten Sie BGP-Peerings ein<br><br>BGP | RFC 4271 | BGP wird zum Austausch von Routen zwischen dem Kunden-Gateway-Gerät und dem Virtual Private Gateway verwendet. Der gesamte BGP-Verkehr wird verschlüsselt und über die IPsec Security Association übertragen. BGP ist für beide Gateways erforderlich, um die IP-Präfixe auszutauschen, die über die SA erreichbar sind. IPsec |

Eine AWS VPN-Verbindung unterstützt Path MTU Discovery (RFC 1191) nicht.

Wenn sich eine Firewall zwischen Ihrem Kunden-Gateway-Gerät und dem Internet befindet, vgl. Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

## Bewährte Methoden für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät

Verwenden IKEv2

Wir empfehlen dringend, IKEv2 für Ihre Site-to-Site VPN-Verbindung zu verwenden. IKEv2 ist ein einfacheres, robusteres und sichereres Protokoll als IKEv1. Sie sollten es nur verwenden IKEv1 , wenn Ihr Kunden-Gateway-Gerät dies nicht unterstützt IKEv2. Weitere Informationen zu den Unterschieden zwischen IKEv1 und IKEv2 finden Sie in Anhang A von RFC7296.

Zurücksetzen des "Don't Fragment"-Flags (DF) von Paketen

Einige Pakete verfügen über ein Flag namens "Don't Fragment" (DF). Dieses Flag zeigt an, dass das Paket nicht fragmentiert werden soll. Bei Paketen mit dem Flag generieren die Gateways die ICMP-Nachricht "Path MTU Exceeded". In einigen Fällen verfügen Anwendungen nicht über die entsprechenden Mechanismen zur Verarbeitung dieser ICMP-Nachrichten und reduzieren die in jedem Paket übertragene Datenmenge. Einige VPN-Geräte können das DF-Flag übergehen und Pakete bei Bedarf fragmentieren. Wenn Ihr Kunden-Gateway-Gerät über eine solche Möglichkeit verfügt, sollten Sie diese bei Bedarf nutzen. Siehe .RFC 791 für weitere Details.

Fragmentierung von IP-Paketen vor der Verschlüsselung

Wenn Pakete, an die Sie über Ihre Site-to-Site VPN-Verbindung gesendet werden, die MTU-Größe überschreiten, müssen sie fragmentiert werden. Um Leistungseinbußen zu vermeiden, empfehlen wir Ihnen, Ihr Kunden-Gateway-Gerät so zu konfigurieren, dass die Pakete fragmentiert werden, bevor sie verschlüsselt werden. Site-to-Site VPN setzt dann alle fragmentierten Pakete wieder zusammen, bevor es sie an das nächste Ziel weiterleitet, um höhere packet-per-second Datenflüsse durch das AWS Netzwerk zu erreichen. Siehe RFC 4459 für weitere Details.

Stellen Sie sicher, dass die Paketgröße die MTU für Zielnetzwerke nicht überschreitet

Da Site-to-Site VPN alle fragmentierten Pakete, die von Ihrem Kunden-Gateway-Gerät empfangen wurden, wieder zusammensetzt, bevor sie an das nächste Ziel weitergeleitet werden, sollten Sie

bedenken, dass bei Zielnetzwerken, an die diese Pakete als nächstes weitergeleitet werden, möglicherweise Überlegungen zur Paketgröße/MTU anfallen können, z. B. über oder mit bestimmten AWS Direct Connect Protokollen, wie Radius.

Passen Sie die MTU- und MSS-Größen entsprechend den verwendeten Algorithmen an

TCP-Pakete sind häufig die häufigste Art von tunnelübergreifenden Paketen. IPsec Site-to-Site VPN unterstützt eine maximale Übertragungseinheit (MTU) von 1446 Byte und eine entsprechende maximale Segmentgröße (MSS) von 1406 Byte. Verschlüsselungsalgorithmen haben jedoch unterschiedliche Header-Größen und können verhindern, dass diese Maximalwerte erreicht werden können. Um eine optimale Leistung durch Vermeidung von Fragmentierung zu erzielen, empfehlen wir Ihnen, die MTU und MSS speziell auf den verwendeten Algorithmen basierend einzustellen.

Verwenden Sie die folgende Tabelle, um Ihre MTU/MSS festzulegen, sodass eine Fragmentierung vermieden und eine optimale Leistung erzielt wird:

| Verschlüsselungsalgorithmus | Hash-Algorithmus | NAT-Traversierung | MTU | MSS () IPv4 | SMS (IPv6-in-) IPv4 |
|---|---|---|---|---|---|
| AES-GCM-16 | N/A | disabled | 1446 | 1406 | 1386 |
| AES-GCM-16 | N/A | aktiviert | 1438 | 1398 | 1378 |
| AES-CBC | SHA1/-256 SHA2 | disabled | 1438 | 1398 | 1378 |
| AES-CBC | SHA1/-256 SHA2 | aktiviert | 1422 | 1382 | 1362 |
| AES-CBC | SHA2-384 | disabled | 1422 | 1382 | 1362 |
| AES-CBC | SHA2-384 | aktiviert | 1422 | 1382 | 1362 |
| AES-CBC | SHA2-512 | disabled | 1422 | 1382 | 1362 |
| AES-CBC | SHA2-512 | aktiviert | 1406 | 1366 | 1346 |

> **Note**
>
> Die AES-GCM-Algorithmen decken sowohl die Verschlüsselung als auch die Authentifizierung ab, sodass es keine eindeutige Wahl des Authentifizierungsalgorithmus gibt, die sich auf die MTU auswirken würde.

Deaktivieren Sie IKE Unique IDs

Einige Kunden-Gateway-Geräte unterstützen eine Einstellung, die sicherstellt, dass pro Tunnelkonfiguration höchstens eine Phase-1-Sicherheitsverbindung vorhanden ist. Diese Einstellung kann zu inkonsistenten Phase-2-Zuständen zwischen VPN-Peers führen. Wenn Ihr Kunden-Gateway-Gerät diese Einstellung unterstützt, empfehlen wir, sie zu deaktivieren.

## Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät

Sie benötigen eine statische IP-Adresse, die Sie als Endpunkt für die IPsec Tunnel verwenden können, die Ihr Kunden-Gateway-Gerät mit AWS Site-to-Site VPN Endpunkten verbinden. Wenn zwischen AWS und Ihrem Kunden-Gateway-Gerät eine Firewall vorhanden ist, müssen die Regeln in den folgenden Tabellen für die Einrichtung der IPsec Tunnel vorhanden sein. Die IP-Adressen für die AWS-Seite werden in der Konfigurationsdatei enthalten sein.

Eingehend (aus dem Internet)

| | |
|---|---|
| Eingangsregel I1 | |
| Quell-IP | Tunnel1 Externe IP |
| Ziel-IP | Kunden-Gateway |
| Protokoll | UDP |
| Quell-Port | 500 |
| Zielbereich | 500 |
| Eingangsregel I2 | |
| Quell-IP | Tunnel2 Externe IP |

| | |
|---|---|
| Ziel-IP | Kunden-Gateway |
| Protokoll | UDP |
| Quell-Port | 500 |
| Ziel-Port | 500 |
| Eingangsregel I3 | |
| Quell-IP | Tunnel1 Externe IP |
| Ziel-IP | Kunden-Gateway |
| Protokoll | IP 50 (ESP) |
| Eingangsregel I4 | |
| Quell-IP | Tunnel2 Externe IP |
| Ziel-IP | Kunden-Gateway |
| Protokoll | IP 50 (ESP) |

Ausgehend (in das Internet)

| | |
|---|---|
| Ausgangsregel O1 | |
| Quell-IP | Kunden-Gateway |
| Ziel-IP | Tunnel1 Externe IP |
| Protokoll | UDP |
| Quell-Port | 500 |
| Ziel-Port | 500 |
| Ausgangsregel O2 | |
| Quell-IP | Kunden-Gateway |

| | |
|---|---|
| Ziel-IP | Tunnel2 Externe IP |
| Protokoll | UDP |
| Quell-Port | 500 |
| Ziel-Port | 500 |
| Ausgangsregel O3 | |
| Quell-IP | Kunden-Gateway |
| Ziel-IP | Tunnel1 Externe IP |
| Protokoll | IP 50 (ESP) |
| Ausgangsregel O4 | |
| Quell-IP | Kunden-Gateway |
| Ziel-IP | Tunnel2 Externe IP |
| Protokoll | IP 50 (ESP) |

Die Regeln I1, I2, O1 und O2 ermöglichen die Übertragung von IKE-Paketen. Die Regeln I3, I4, O3 und O4 ermöglichen die Übertragung von IPsec Paketen, die den verschlüsselten Netzwerkverkehr enthalten.

> **Note**
>
> Wenn Sie NAT-Traversal (NAT-T) auf Ihrem Gerät verwenden, stellen Sie sicher, dass UDP-Verkehr auf Port 4500 auch zwischen Ihrem Netzwerk und den Endpunkten übertragen werden darf. AWS Site-to-Site VPN Überprüfen Sie, ob Ihr Gerät NAT-T ankündigt.

# Statische und dynamische Konfigurationsdateien für ein Kunden-Gateway-Gerät AWS Site-to-Site VPN

Nachdem Sie die VPN-Verbindung hergestellt haben, haben Sie zusätzlich die Möglichkeit, eine AWS bereitgestellte Beispielkonfigurationsdatei von der Amazon VPC-Konsole oder mithilfe der EC2 API herunterzuladen. Weitere Informationen finden Sie unter Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen. Sie können auch ZIP-Dateien mit Beispielkonfigurationen speziell für statisches und dynamisches Routing von den jeweiligen Seiten herunterladen.

Die AWS mitgelieferte Beispielkonfigurationsdatei enthält spezifische Informationen zu Ihrer VPN-Verbindung, die Sie zur Konfiguration Ihres Kunden-Gateway-Geräts verwenden können. Diese gerätespezifische Konfigurationsdateien sind nur für Geräte verfügbar, die AWS getestet hat. Wenn Ihr spezifisches Kunden-Gateway-Gerät nicht aufgeführt ist, können Sie zunächst eine generische Konfigurationsdatei herunterladen.

> **Important**
>
> Die Konfigurationsdatei dient nur als Beispiel und entspricht möglicherweise nicht vollständig Ihren beabsichtigten Site-to-Site VPN-Verbindungseinstellungen. Sie spezifiziert die Mindestanforderungen für eine Site-to-Site VPN-Verbindung von AES128, SHA1, und Diffie-Hellman-Gruppe 2 in den meisten AWS Regionen und, AES128 SHA2, und Diffie-Hellman-Gruppe 14 in den Regionen. AWS GovCloud Es legt außerdem Pre-Shared-Key für die Authentifizierung fest. Sie müssen die Beispielkonfigurationsdatei ändern, um zusätzliche Sicherheitsalgorithmen, Diffie-Hellman-Gruppen, private Zertifikate und Datenverkehr zu nutzen. IPv6

> **Note**
>
> Diese gerätespezifischen Konfigurationsdateien werden nach bestem Wissen und Gewissen von AWS bereitgestellt. Sie wurden zwar von getestet AWS, diese Tests sind jedoch begrenzt. Wenn Sie ein Problem mit den Konfigurationsdateien haben, müssen Sie sich möglicherweise an den jeweiligen Anbieter wenden, um zusätzlichen Support zu erhalten.

Die folgende Tabelle enthält eine Liste von Geräten, für die eine Beispielkonfigurationsdatei heruntergeladen werden kann, die aktualisiert wurde, um sie zu unterstützen IKEv2. Wir haben IKEv2

Unterstützung in den Konfigurationsdateien für viele beliebte Kunden-Gateway-Geräte eingeführt und werden im Laufe der Zeit weitere Dateien hinzufügen. Diese Liste wird aktualisiert, wenn weitere Beispielkonfigurationsdateien hinzugefügt werden.

| Hersteller | Plattform | Software |
| --- | --- | --- |
| Prüfpunkt | Gaia | R80.10+ |
| Cisco Meraki | MX-Serie | 15.12+ (WebUI) |
| Cisco Systems, Inc. | ASA 5500 Serie | ASA 9.7+ VTI |
| Cisco Systems, Inc. | CSRv AMI | IOS 12.4+ |
| Fortinet | Serie Fortigate 40+ | FortiOS 6.4.4+ (GUI) |
| Juniper Networks, Inc. | Router der J-Serie | JunOS 9.5+ |
| Juniper Networks, Inc. | SRX-Router | JunOS 11.0+ |
| Mikrotik | RouterOS | 6,44,3 |
| Palo Alto Networks | PA-Serie | PANOS 7.0+ |
| SonicWall | NSA, TZ | OS 6.5 |
| Sophos | Sophos Firewall | v19+ |
| Strongswan | Ubuntu 16.04 | Strongswan 5.5.1+ |
| Yamaha | RTX-Router | Rev.10.01.16+ |

## Herunterladbare statische Routing-Konfigurationsdateien für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät

Um eine Beispielkonfigurationsdatei mit Werten herunterzuladen, die für Ihre Site-to-Site VPN-Verbindungskonfiguration spezifisch sind, verwenden Sie die Amazon VPC-Konsole, die AWS Befehlszeile oder die EC2 Amazon-API. Weitere Informationen finden Sie unter Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen.

Sie können auch generische Beispielkonfigurationsdateien für statisches Routing herunterladen, die keine spezifischen Werte für Ihre Site-to-Site VPN-Verbindungskonfiguration enthalten: .zip static-routing-examples

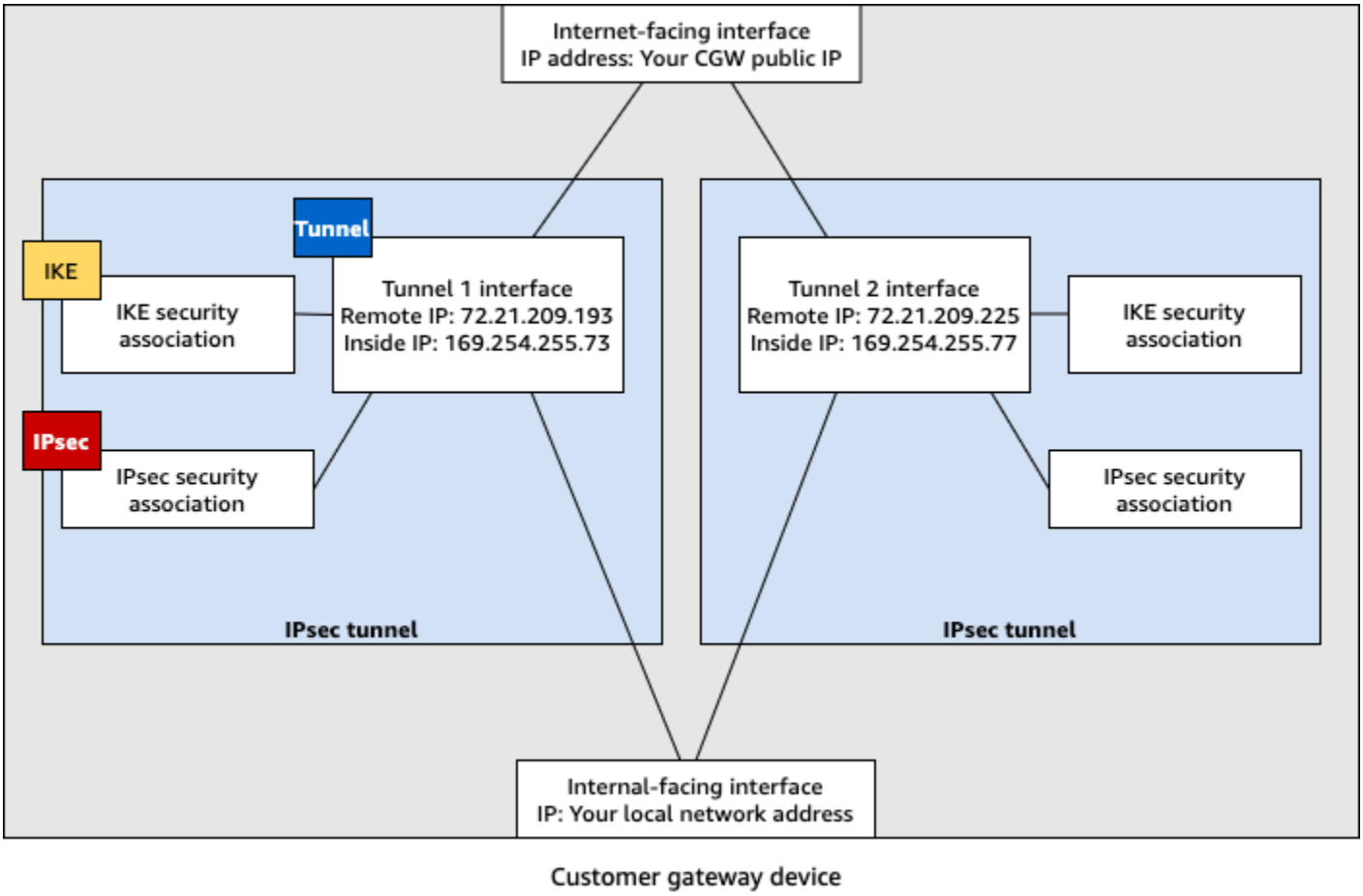
Die Dateien verwenden Platzhalterwerte für einige Komponenten. Sie verwenden zum Beispiel:

- Beispielwerte für die VPN-Verbindungs-ID, die Kunden-Gateway-ID und die ID des Virtual Private Gateways
- Platzhalter für die (externen) AWS Remote-IP-Adressendpunkte (und) *AWS_ENDPOINT_1* *AWS_ENDPOINT_2*
- Ein Platzhalter für die IP-Adresse der externen Schnittstelle, die über das Internet routbar ist, auf dem Kunden-Gateway-Gerät () *your-cgw-ip-address*
- Ein Platzhalter für den Wert des vorab gemeinsam genutzten Schlüssels () pre-shared-key
- Beispielwerte für den Tunnel innerhalb von IP-Adressen.
- Beispielwerte für die MTU-Einstellung.

> **Note**
>
> Die MTU-Einstellungen, die in den Beispielkonfigurationsdateien bereitgestellt werden, sind nur Beispiele. Weitere Informationen zur Einstellung des optimalen MTU-Wertes für Ihre Situation finden Sie unter Bewährte Methoden für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Die Dateien stellen nicht nur Platzhalterwerte bereit, sondern spezifizieren auch die Mindestanforderungen für eine Site-to-Site VPN-Verbindung von AES128 SHA1, und Diffie-Hellman-Gruppe 2 in den meisten AWS Regionen und, AES128 SHA2, und Diffie-Hellman-Gruppe 14 in den Regionen. AWS GovCloud Sie geben auch Pre-Shared-Key für authentication (Authentifizierung) an. Sie müssen die Beispielkonfigurationsdatei ändern, um zusätzliche SicherheitsalGORITHmen, Diffie-Hellman-Gruppen, private Zertifikate und Datenverkehr zu nutzen. IPv6

Das folgende Diagramm gibt einen Überblick über die verschiedenen Komponenten, die auf dem Kunden-Gateway-Gerät konfiguriert werden. Es enthält Beispielwerte für die IP-Adressen der Tunnelschnittstelle.




## Konfigurieren Sie statisches Routing für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät

Im Folgenden finden Sie einige Beispielverfahren zur Konfiguration eines Kunden-Gateway-Geräts unter Verwendung seiner Benutzeroberfläche (falls verfügbar).

### Check Point

Im Folgenden finden Sie Schritte zur Konfiguration Ihres Kunden-Gateway-Geräts, falls es sich bei Ihrem Gerät um ein Check Point Security Gateway-Gerät mit R77.10 oder höher handelt, das das Gaia-Betriebssystem und Check Point verwendet. SmartDashboard Sie können auch den Artikel Check Point Security Gateway IPsec VPN to Amazon Web Services VPC im Check Point Support Center lesen.

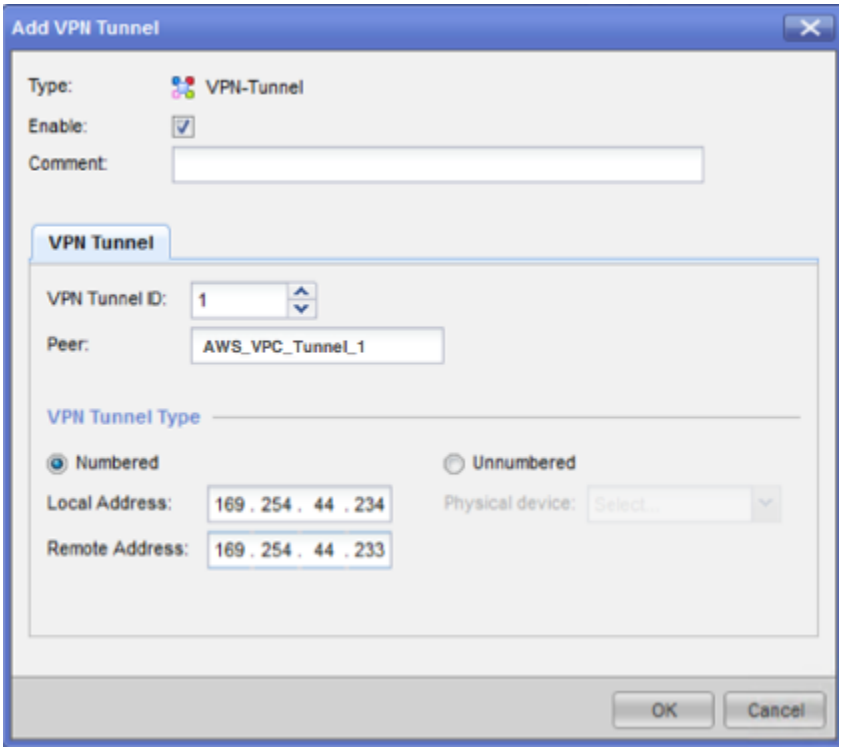
#### So konfigurieren Sie die Tunnelschnittstelle

Als Erstes müssen Sie die VPN-Tunnel erstellen und die privaten (internen) IP-Adressen des Kunden-Gateways und des Virtual Private Gateways für die einzelnen Tunnel angeben. Wie

Sie den ersten Tunnel erstellen, ist im Abschnitt `IPSec Tunnel #1` der Konfigurationsdatei beschrieben. Verwenden Sie zum Erstellen des zweiten Tunnels die Werte im Abschnitt `IPSec Tunnel #2` der Konfigurationsdatei.

1. Öffnen Sie das Gaia-Portal Ihres Check Point-Sicherheits-Gateway-Geräts.
2. Klicken Sie auf Network Interfaces, Add und VPN tunnel.
3. Konfigurieren Sie im Dialogfeld die Einstellungen wie nachfolgend beschrieben und klicken Sie dann auf OK:

   - Geben Sie unter VPN Tunnel ID einen eindeutigen Wert, z. B. 1, ein.
   - Geben Sie unter Peer einen eindeutigen Namen für den Tunnel ein, z. B. `AWS_VPC_Tunnel_1` oder `AWS_VPC_Tunnel_2`.
   - Stellen Sie sicher, dass Numbered (Nummeriert) ausgewählt ist, und geben Sie unter Local Address (Lokale Adresse) die IP-Adresse für `CGW Tunnel IP` aus der Konfigurationsdatei ein, z. B. `169.254.44.234`.
   - Geben Sie unter Remote Address die IP-Adresse für `VGW Tunnel IP` aus der Konfigurationsdatei ein, z. B. `169.254.44.233`.




4. Melden Sie sich über SSH bei Ihrem Sicherheits-Gateway an. Wenn Sie nicht die Standard-Shell verwenden, wechseln Sie mit folgendem Befehl zu Clish: `clish`

5. Führen Sie für Tunnel 1 den folgenden Befehl aus:

```
set interface vpnt1 mtu 1436
```

   Führen Sie für Tunnel 2 den folgenden Befehl aus:

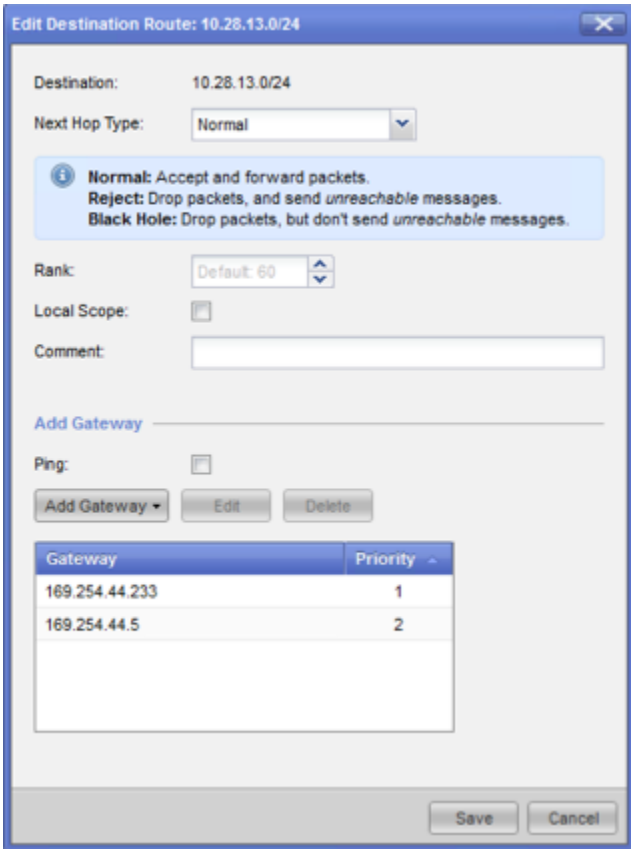
```
set interface vpnt2 mtu 1436
```

6. Wiederholen Sie diese Schritte, um den zweiten Tunnel zu erstellen. Verwenden Sie dafür die Informationen im Bereich `IPSec Tunnel #2` der Konfigurationsdatei.

So konfigurieren Sie die statischen Routen

In diesem Schritt legen Sie für die einzelnen Tunnel die statische Route zum Subnetz in der VPC fest, damit Sie Datenverkehr über die Tunnelschnittstellen senden können. Der zweite Tunnel dient als Failover, falls der erste Tunnel ausfällt. Falls ein Fehler auftritt, wird die richtlinienbasierte statische Route aus der Routing-Tabelle entfernt und es wird eine zweite Route aktiviert. Außerdem müssen Sie das Check Point-Gateway aktivieren, um einen Ping ans andere Ende des Tunnels zu senden und zu prüfen, ob der Tunnel aktiv ist.

1. Wählen Sie im Gaia-Portal IPv4 Static Routes, Add aus.
2. Geben Sie den CIDR-Bereich Ihres Subnetzes an, z. B. `10.28.13.0/24`.
3. Klicken Sie auf Add Gateway und IP Address.
4. Geben Sie die IP-Adresse für `VGW Tunnel IP` aus der Konfigurationsdatei ein (z. B. `169.254.44.233`) und legen Sie als Priorität "1" fest.
5. Wählen Sie Ping aus.
6. Wiederholen Sie die Schritte 3 und 4 für den zweiten Tunnel und verwenden Sie den Wert `VGW Tunnel IP` im Bereich `IPSec Tunnel #2` der Konfigurationsdatei. Legen Sie als Priorität "2" fest.




7. Wählen Sie Save (Speichern) aus.

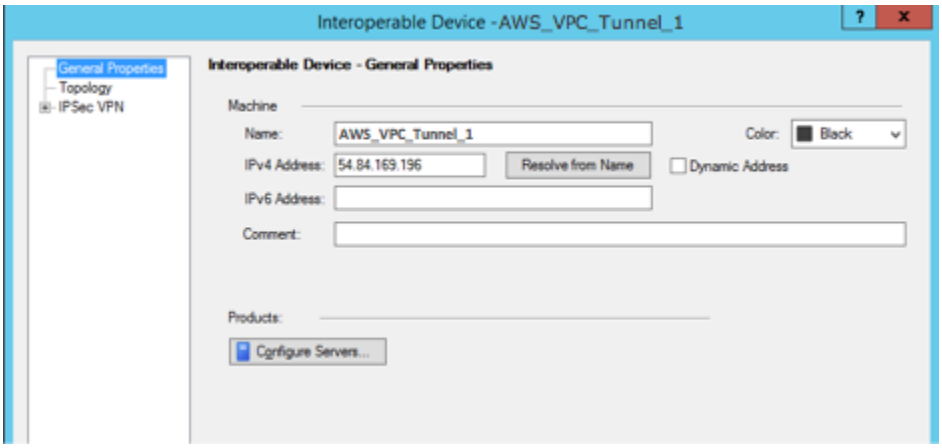
Wenn Sie einen Cluster verwenden, wiederholen Sie die vorhergehenden Schritte für die anderen Mitglieder des Clusters.

So definieren Sie ein neues Netzwerkobjekt

In diesem Schritt erstellen Sie ein Netzwerkobjekt für jeden VPN-Tunnel und legen die öffentlichen (externen) IP-Adressen für das Virtual Private Gateway fest. Später fügen Sie diese Netzwerkobjekte als Satelliten-Gateways für Ihre VPN-Community hinzu. Außerdem müssen Sie eine leere Gruppe erstellen, die als Platzhalter für die VPN-Domäne dient.

1. Öffnen Sie den Check Point SmartDashboard.
2. Öffnen Sie für Groups das Kontextmenü und klicken Sie auf Groups und Simple Group. Sie können für alle Netzwerkobjekte dieselbe Gruppe verwenden.
3. Öffnen Sie mit der rechten Maustaste für Network Objects das Kontextmenü und wählen Sie New und Interoperable Device aus.

4. Geben Sie unter Name den Namen des Tunnels ein, z. B. `AWS_VPC_Tunnel_1` oder `AWS_VPC_Tunnel_2`.
5. Geben Sie unter IPv4 Adresse die externe IP-Adresse des virtuellen privaten Gateways ein, die in der Konfigurationsdatei angegeben ist, `54.84.169.196` z. B. Speichern Sie die Einstellungen und schließen Sie das Dialogfeld.




6. Öffnen Sie Ihre Gateway-Eigenschaften und wählen Sie im Kategorienbereich Topologie aus. SmartDashboard
7. Klicken Sie auf Get Topology, um die Schnittstellenkonfiguration abzurufen.
8. Klicken Sie im Bereich VPN Domain (VPN-Domäne) auf Manually defined (Manuell definiert) und wählen Sie die leere einfache Gruppe aus, die Sie in Schritt 2 erstellt haben. Wählen Sie OK aus.

> **Note**
>
> Sie können eine vorhandene VPN-Domäne, die Sie bereits konfiguriert haben, beibehalten. Stellen Sie jedoch sicher, dass die verwendeten Hosts und Netzwerke von der neuen VPN-Verbindung bedient werden und nicht in dieser VPN-Domäne deklariert werden, insbesondere wenn die VPN-Domäne automatisch abgeleitet wird.

9. Wiederholen Sie diese Schritte, um ein zweites Netzwerkobjekt zu erstellen. Verwenden Sie dafür die Informationen im Bereich `IPSec Tunnel #2` der Konfigurationsdatei.

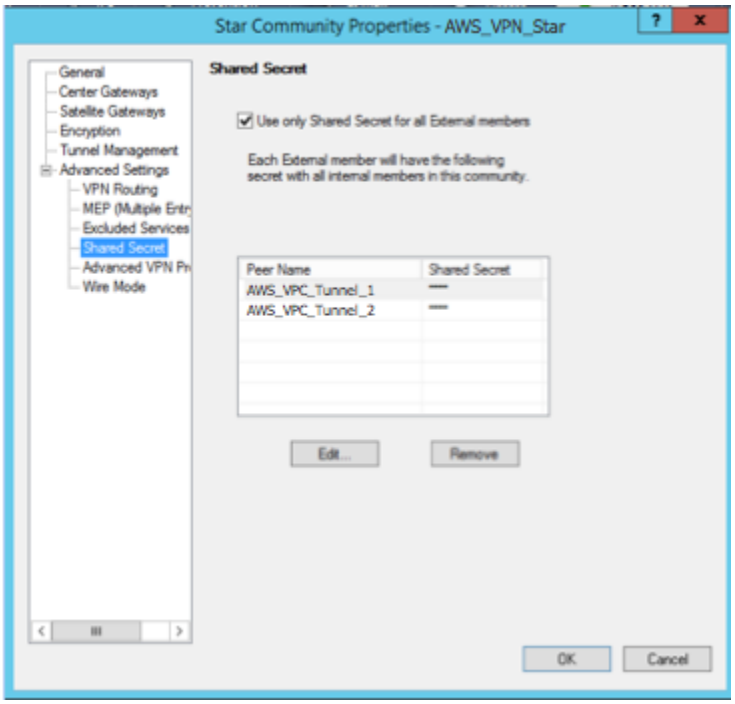
> **Note**
>
> Wenn Sie Cluster verwenden, bearbeiten Sie die Topologie und legen Sie die Schnittstellen als Cluster-Schnittstellen fest. Verwenden Sie die IP-Adressen, die in der Konfigurationsdatei angegeben sind.

So erstellen und konfigurieren Sie die VPN-Community, IKE und IPsec Einstellungen

In diesem Schritt erstellen Sie eine VPN-Community in Ihrem Check Point-Gateway, zu dem Sie die Netzwerkobjekte (interoperablen Geräte) für die einzelnen Tunnel hinzufügen. Sie konfigurieren auch den Internet Key Exchange (IKE) und die IPsec Einstellungen.

1. Wählen Sie in Ihren Gateway-Eigenschaften im Kategorienbereich die Option IPSecVPN aus.
2. Klicken Sie auf Communities, New und Star Community.
3. Geben Sie einen Namen für die Community ein (z. B. `AWS_VPN_Star`) und klicken Sie im Kategoriebereich auf Center Gateways.
4. Klicken Sie auf Add und fügen Sie Ihr Gateway bzw. Ihren Cluster der Liste der teilnehmenden Gateways hinzu.
5. Klicken Sie im Kategoriebereich auf Satellite Gateways (Satelliten-Gateways) und Add (Hinzufügen) und fügen Sie die interoperablen Geräte, die Sie vorher erstellt haben (`AWS_VPC_Tunnel_1` und `AWS_VPC_Tunnel_2`) der Liste der teilnehmenden Gateways hinzu.
6. Klicken Sie im Kategoriebereich auf Encryption. Wählen Sie im Abschnitt Verschlüsselungsmethode die Option IKEv1 Nur aus. Wählen Sie im Bereich Encryption Suite Custom und Custom Encryption aus.
7. Konfigurieren Sie im Dialogfeld die Verschlüsselungseigenschaften wie nachfolgend beschrieben und klicken Sie dann auf OK:
   - Eigenschaften von IKE Security Association (Phase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Eigenschaften von Security Association (Phase 2):
     - Führen Sie eine IPsec Datenverschlüsselung durch mit: AES-128
     - Perform data integrity with: SHA-1

8. Klicken Sie im Kategoriebereich auf Tunnel Management. Klicken Sie auf Set Permanent Tunnels und On all tunnels in the community. Wählen Sie im Bereich VPN Tunnel Sharing One VPN tunnel per Gateway pair aus.
9. Erweitern Sie im Kategoriebereich Advanced Settings und klicken Sie auf Shared Secret.
10. Wählen Sie den Peer-Namen für den ersten Tunnel aus, klicken Sie auf Edit (Bearbeiten) und geben Sie den vorinstallierten Schlüssel aus dem Bereich `IPSec Tunnel #1` der Konfigurationsdatei ein.
11. Wählen Sie den Peer-Namen für den zweiten Tunnel aus, klicken Sie auf Edit (Bearbeiten) und geben Sie den vorinstallierten Schlüssel aus dem Bereich `IPSec Tunnel #2` der Konfigurationsdatei ein.




12. Klicken Sie – noch immer in der Kategorie Advanced Settings (Erweiterte Einstellungen) – auf Advanced VPN Properties (Erweiterte VPN-Eigenschaften), konfigurieren Sie die Eigenschaften wie nachfolgend beschrieben und klicken Sie abschließend auf OK:
    - IKE (Phase 1):
        - Diffie-Hellman-Gruppe verwenden: `Group 2`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Phase 2):
        - Use Perfect Forward Secrecy auswählen
        - Diffie-Hellman-Gruppe verwenden: `Group 2`

- Verhandeln Sie IPsec Sicherheitszuordnungen alle Sekunden neu **`3600`**

So erstellen Sie Firewall-Regeln

In diesem Schritt konfigurieren Sie eine Richtlinie mit Firewall-Regeln und direktionalen Übereinstimmungsregeln, um Kommunikation zwischen der VPC und dem lokalen Netzwerk zu ermöglichen. Dann installieren Sie diese Richtlinie auf Ihrem Gateway.

1. Wählen Sie im SmartDashboard Global Properties für Ihr Gateway aus. Erweitern Sie im Kategoriebereich VPN und klicken Sie auf Advanced.
2. Klicken Sie auf Enable VPN Directional Match in VPN Column und speichern Sie die Änderungen.
3. Wählen Sie im die SmartDashboard Option Firewall aus und erstellen Sie eine Richtlinie mit den folgenden Regeln:
   - Erlauben Sie dem VPC-Subnetz, über die erforderlichen Protokolle mit dem lokalen Netzwerk zu kommunizieren.
   - Erlauben Sie dem lokalen Netzwerk, über die erforderlichen Protokolle mit dem VPC-Subnetz zu kommunizieren.
4. Öffnen Sie das Kontextmenü für die Zelle in der VPN-Spalte und klicken Sie auf Edit Cell.
5. Klicken Sie im Dialogfeld VPN Match Conditions auf Match traffic in this direction only. Klicken Sie jeweils auf Add und abschließend auf OK, um die folgenden direktionalen Übereinstimmungsregeln zu erstellen:
   - `internal_clear` **>** VPN-Community (die VPN-Star-Community, die Sie vorher erstellt haben, z. B. `AWS_VPN_Star`)
   - VPN-Community **>** VPN-Community
   - VPN-Community **>** `internal_clear`
6. Wählen Sie im die SmartDashboard Option Richtlinie, Installieren aus.
7. Wählen Sie im Dialogfeld das Gateway aus und klicken Sie auf OK, um die Richtlinie zu installieren.

So ändern Sie die Eigenschaft "tunnel_keepalive_method"

Sie können für Ihren Check Point-Gateway Dead Peer Detection (DPD) verwenden, um Ausfälle bei der IKE-Zuordnung zu identifizieren. Um DPD für einen permanenten Tunnel zu konfigurieren, muss der permanente Tunnel in der AWS VPN-Community konfiguriert werden (siehe Schritt 8).

Standardmäßig ist für die Eigenschaft `tunnel_keepalive_method` eines VPN-Gateways der Wert `tunnel_test` festgelegt. Sie müssen diesen Wert zu dpd ändern. Für alle VPN-Gateways innerhalb der VPN-Community, einschließlich VPN-Gateways von Drittanbietern, für die Sie DPD-Überwachung aktivieren möchten, muss die Eigenschaft `tunnel_keepalive_method` konfiguriert werden. Es ist nicht möglich, für dasselbe Gateway unterschiedliche Überwachungsmechanismen zu konfigurieren.

Sie können die `tunnel_keepalive_method` Eigenschaft mit dem DBedit GUI-Tool aktualisieren.

1. Öffnen Sie den Check Point SmartDashboard und wählen Sie Security Management Server, Domain Management Server.
2. Klicken Sie auf File und Database Revision Control… und erstellen Sie einen Versions-Snapshot.
3. Schließen Sie alle SmartConsole Fenster, z. B. SmartView Tracker und SmartView Monitor. SmartDashboard
4. Starten Sie das BDedit GUI-Tool. Weitere Informationen finden Sie im Artikel Check Point Database Tool im Check Point-Supportcenter.
5. Klicken Sie auf Security Management Server und Domain Management Server.
6. Klicken Sie oben links auf Table, Network Objects und network_objects.
7. Wählen Sie oben rechts das entsprechende Security Gateway-Cluster-Objekt aus.
8. Drücken Sie STRG + F oder verwenden Sie das Suchmenü, um nach folgender Zeichenfolge zu suchen: `tunnel_keepalive_method`.
9. Öffnen Sie im unteren Bereich das Kontextmenü für `tunnel_keepalive_method` und klicken Sie auf Edit… (Bearbeiten...). Wählen Sie dpd aus. Wählen Sie dann OK aus.
10. Wiederholen Sie die Schritte 7 bis 9 für jedes Gateway, das Teil der AWS VPN-Community ist.
11. Klicken Sie auf File und Save All.
12. Schließen Sie das DBedit GUI-Tool.

13. Öffnen Sie den Check Point SmartDashboard und wählen Sie Security Management Server, Domain Management Server.
14. Installieren Sie die Richtlinie für das entsprechende Security Gateway-Cluster-Objekt.

Weitere Informationen finden Sie im Artikel New VPN features in R77.10 im Check Point-Supportcenter.

So aktivieren Sie TCP MSS Clamping

Mit TCP MSS Clamping können Sie die maximale Segmentgröße von TCP-Paketen reduzieren, um eine Paketfragmentierung zu vermeiden.

1. Öffnen Sie das folgende Verzeichnis: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Führen Sie die Datei `GuiDBEdit.exe` aus, um das Check Point-Datenbank-Tool zu starten.
3. Wählen Sie Table, Global Properties und properties aus.
4. Klicken Sie für `fw_clamp_tcp_mss` auf Edit. Ändern Sie den Wert in `true` und klicken Sie auf OK.

So überprüfen Sie den Tunnelstatus

Sie können den Tunnelstatus überprüfen, indem Sie den folgenden Befehl vom Befehlszeilen-Tool aus im Expertenmodus ausführen.

```
vpn tunnelutil
```

Wählen Sie in den angezeigten Optionen 1 aus, um die IKE-Verknüpfungen zu überprüfen, und 2, um die IPsec Verknüpfungen zu überprüfen.

Im Check Point Smart Tracker-Protokoll können Sie auch überprüfen, ob Pakete über diese Verbindung verschlüsselt werden. Dem folgenden Protokoll können Sie beispielsweise entnehmen, dass ein Paket verschlüsselt über Tunnel 1 an die VPC gesendet wurde.

| Log Info | |
|---|---|
| Product | Security Gateway/Management |
| Date | 4Nov2015 |
| Time | 9:42:01 |
| Number | 21254 |
| Type | Log |
| Origin | cpgw-997695 |

| Traffic | |
|---|---|
| Source | Management_PC (192.168.1.116) |
| Destination | 10.28.13.28 |
| Service | --- |
| Protocol | icmp |
| Interface | eth0 |
| Source Port | --- |

| Policy | |
|---|---|
| Policy Name | Standard |
| Policy Date | Tue Nov 03 11:33:45 2015 |
| Policy Management | cpgw-997695 |

| Rule | |
|---|---|
| Action | Encrypt |
| Rule | 4 |
| Current Rule Number | 4-Standard |
| Rule Name | --- |
| User | --- |

| More | |
|---|---|
| Rule UID | {0AA18015-FF7B-4650-B0CE-3989E658CF04} |
| Community | AWS_VPN_Star |
| Encryption Scheme | IKE |
| Data Encryption Methods | ESP: AES-128 + SHA1 + PFS (group 2) |
| VPN Peer Gateway | AWS_VPC_Tunnel_1 (54.84.169.196) |
| Subproduct | VPN |
| VPN Feature | VPN |
| Product Family | Network |
| Information | service_id: icmp-proto<br>ICMP: Echo Request<br>ICMP Type: 8<br>ICMP Code: 0 |

## SonicWALL

Das folgende Verfahren zeigt die Konfiguration von VPN-Tunneln auf dem SonicWALL-Gerät über die SonicOS-Managementschnittstelle.

So konfigurieren Sie die Tunnel

1. Öffnen Sie die SonicWALL SonicOS-Management-Schnittstelle.
2. Wählen Sie im linken Bereich VPN, Settings aus. Wählen Sie unter VPN Policies Add... aus.
3. Geben Sie die folgenden Informationen im VPN-Richtlinienfenster auf der Registerkarte General ein:
   - Policy Type (Richtlinientyp): Wählel Sie Tunnel Interface.
   - Authentication Method: Wählen Sie IKE using Preshared Secret aus.
   - Name: Geben Sie einen Namen für die VPN-Richtlinie ein. Wir empfehlen, dass Sie den Namen der VPN-ID aus der Konfigurationsdatei verwenden.
   - IPsec Name oder Adresse des primären Gateways: Geben Sie die IP-Adresse des Virtual Private Gateways ein, wie sie in der Konfigurationsdatei angegeben ist (z. B.`72.21.209.193`).
   - IPsec Name oder Adresse des sekundären Gateways: Behalten Sie den Standardwert bei.

- Shared Secret: Geben Sie den vorinstallierten Schlüssel aus der Konfigurationsdatei ein. Geben Sie ihn erneut in Confirm Shared Secret ein.
- Lokale IKE-ID: Geben Sie die IPv4 Adresse des Kunden-Gateways (das SonicWALL-Gerät) ein.
- Peer-IKE-ID: Geben Sie die IPv4 Adresse des virtuellen privaten Gateways ein.

4. Füllen Sie auf der Registerkarte Network die folgenden Informationen aus:

   - Wählen Sie unter Local Networks Any address aus. Wir empfehlen diese Option, um Verbindungsprobleme aus Ihrem lokalen Netzwerk zu vermeiden.
   - Wählen Sie unter Remote Networks Choose a destination network from list aus. Erstellen Sie ein Adressobjekt mit der CIDR Ihrer VPC in AWS.

5. Füllen Sie auf der Registerkarte Proposals (Vorschläge) die folgenden Informationen aus.

   - Führen Sie unter IKE (Phase 1) Proposal die folgenden Schritte aus:
     - Exchange: Wählen Sie Main Mode aus.
     - DH Group: Geben Sie einen Wert für die Diffie-Hellman-Gruppe ein (z. B. 2).
     - Encryption: Wählen Sie AES-128 oder AES-256 aus.
     - Authentifizierung: Wählen Sie SHA1oder SHA256.
     - Life Time: Geben Sie `28800` ein.
   - Führen Sie unter IKE (Phase 2) Proposal die folgenden Schritte aus:
     - Protocol: Wählen Sie ESP aus.
     - Encryption: Wählen Sie AES-128 oder AES-256 aus.
     - Authentifizierung: Wählen Sie SHA1oder SHA256.
     - Wählen Sie das Kontrollkästchen Enable Perfect Forward Secrecy und die Diffie-Hellman-Gruppe aus.
     - Life Time: Geben Sie `3600` ein.

   > **Important**
   >
   > Wenn Sie Ihr Virtual Private Gateway vor Oktober 2015 erstellt haben, müssen Sie Diffie-Hellman-Gruppe 2, AES-128, und für beide Phasen angeben. SHA1

6. Füllen Sie auf der Registerkarte Advanced die folgenden Informationen aus:

- Wählen Sie Enable Keep Alive aus.
- Wählen Sie Enable Phase2 Dead Peer Detection aus und geben Sie Folgendes ein:
  - Geben Sie für Dead Peer Detection Interval `60` ein (der Minimalwert für das SonicWALL-Gerät).
  - Geben Sie in Failure Trigger Level `3` ein.
- Wählen Sie für VPN Policy bound to Interface X1 aus. Dies ist die Schnittstelle, die normalerweise für öffentliche IP-Adressen vorgesehen ist.

7. Wählen Sie OK aus. Auf der Seite Einstellungen sollte das Kontrollkästchen Aktivieren für den Tunnel standardmäßig aktiviert sein. Der grüne Punkt zeigt an, dass der Tunnel aktiv ist.

## Cisco-Geräte: zusätzliche Informationen

Einige Cisco unterstützen ASAs nur den Aktiv-/Standby-Modus. Wenn Sie diese Cisco verwenden ASAs, können Sie jeweils nur einen aktiven Tunnel haben. Der andere Standby-Tunnel wird aktiv, falls der erste Tunnel nicht verfügbar ist. Diese Redundanz sorgt dafür, dass immer ein Tunnel für die Verbindung zu Ihrer VPC verfügbar ist.

Cisco unterstützt ASAs ab Version 9.7.1 und höher den Active/Active-Modus. Wenn Sie diese Cisco verwenden ASAs, können Sie beide Tunnel gleichzeitig aktiv haben. Diese Redundanz sorgt dafür, dass immer ein Tunnel für die Verbindung zu Ihrer VPC verfügbar ist.

Für Cisco-Geräte müssen Sie die folgenden Schritte ausführen:

- Konfigurieren Sie die Außenschnittstelle.
- Stellen Sie sicher, dass die Crypto ISAKMP-Richtliniensequenznummer eindeutig ist.
- Stellen Sie sicher, dass die Crypto List-Richtliniensequenznummer eindeutig ist.
- Stellen Sie sicher, dass das Crypto IPsec Transform Set und die Crypto ISAKMP Policy Sequence mit allen anderen IPsec Tunneln, die auf dem Gerät konfiguriert sind, harmonieren.
- Stellen Sie sicher, dass die SLA-Überwachungsnummer eindeutig ist.
- Konfigurieren Sie sämtliche internen Routen, über die Datenverkehr zwischen dem Kunden-Gateway-Gerät und Ihrem On-Premise-Netzwerk gesendet wird.

## Herunterladbare dynamische Routing-Konfigurationsdateien für AWS Site-to-Site VPN Kunden-Gateway-Geräte

Um eine Beispielkonfigurationsdatei mit Werten herunterzuladen, die für Ihre Site-to-Site VPN-Verbindungskonfiguration spezifisch sind, verwenden Sie die Amazon VPC-Konsole, die AWS Befehlszeile oder die EC2 Amazon-API. Weitere Informationen finden Sie unter Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen.

Sie können auch generische Beispielkonfigurationsdateien für dynamisches Routing herunterladen, die keine spezifischen Werte für Ihre Site-to-Site VPN-Verbindungskonfiguration enthalten: .zip dynamic-routing-examples

Die Dateien verwenden Platzhalterwerte für einige Komponenten. Sie verwenden zum Beispiel:

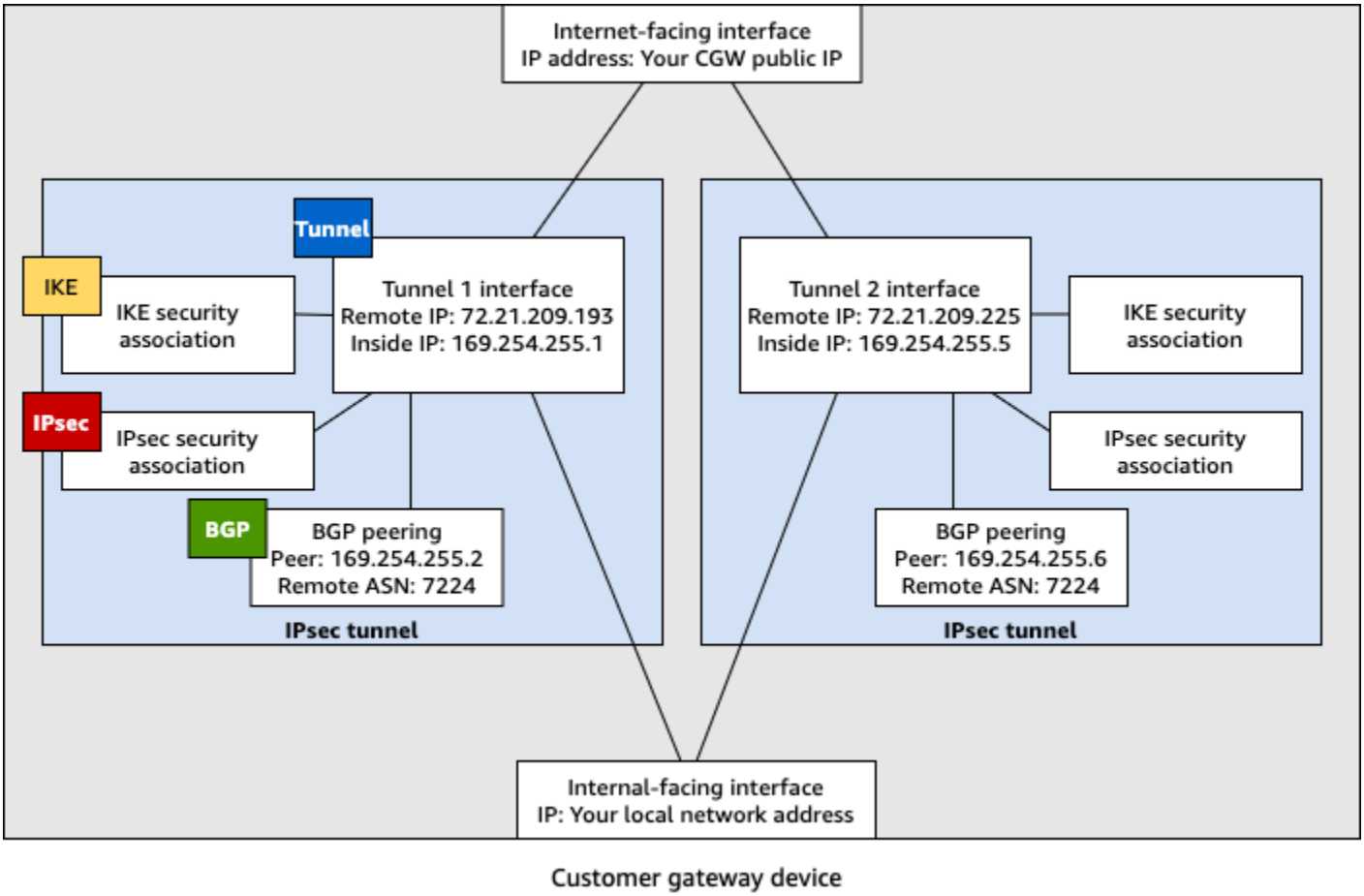
- Beispielwerte für die VPN-Verbindungs-ID, die Kunden-Gateway-ID und die ID des Virtual Private Gateways
- Platzhalter für die (externen) AWS Remote-IP-Adressendpunkte (und) *AWS_ENDPOINT_1* *AWS_ENDPOINT_2*
- Ein Platzhalter für die IP-Adresse der externen Schnittstelle, die über das Internet routbar ist, auf dem Kunden-Gateway-Gerät () *your-cgw-ip-address*
- Ein Platzhalter für den Wert des vorab gemeinsam genutzten Schlüssels () pre-shared-key
- Beispielwerte für den Tunnel innerhalb von IP-Adressen.
- Beispielwerte für die MTU-Einstellung.

> **Note**
>
> Die MTU-Einstellungen, die in den Beispielkonfigurationsdateien bereitgestellt werden, sind nur Beispiele. Weitere Informationen zur Einstellung des optimalen MTU-Wertes für Ihre Situation finden Sie unter Bewährte Methoden für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Die Dateien stellen nicht nur Platzhalterwerte bereit, sondern spezifizieren auch die Mindestanforderungen für eine Site-to-Site VPN-Verbindung von AES128 SHA1, und Diffie-Hellman-Gruppe 2 in den meisten AWS Regionen und, AES128 SHA2, und Diffie-Hellman-Gruppe 14 in den Regionen. AWS GovCloud Sie geben auch Pre-Shared-Key für authentication (Authentifizierung) an.

Sie müssen die Beispielkonfigurationsdatei ändern, um zusätzliche SicherheitsalGORITHmen, Diffie-Hellman-Gruppen, private Zertifikate und Datenverkehr zu nutzen. IPv6

Das folgende Diagramm gibt einen Überblick über die verschiedenen Komponenten, die auf dem Kunden-Gateway-Gerät konfiguriert werden. Es enthält Beispielwerte für die IP-Adressen der Tunnelschnittstelle.




## Konfigurieren Sie dynamisches Routing für ein AWS Virtual Private Network Kunden-Gateway-Gerät

Im Folgenden finden Sie einige Beispielverfahren zur Konfiguration eines Kunden-Gateway-Geräts unter Verwendung seiner Benutzeroberfläche (falls verfügbar).

### Check Point

Im Folgenden finden Sie Schritte zur Konfiguration eines Check Point Security Gateway-Geräts, auf dem R77.10 oder höher ausgeführt wird, mithilfe des Gaia-Webportals und Check Point. SmartDashboard Sie können auch den Amazon Web Services (AWS) VPN BGP-Artikel über das Check Point Support Center lesen.

So konfigurieren Sie die Tunnelschnittstelle

Als Erstes müssen Sie die VPN-Tunnel erstellen und die privaten (internen) IP-Adressen des Kunden-Gateways und des Virtual Private Gateways für die einzelnen Tunnel angeben. Wie Sie den ersten Tunnel erstellen, ist im Abschnitt `IPSec Tunnel #1` der Konfigurationsdatei beschrieben. Verwenden Sie zum Erstellen des zweiten Tunnels die Werte im Abschnitt `IPSec Tunnel #2` der Konfigurationsdatei.

1. Melden Sie sich über SSH bei Ihrem Sicherheits-Gateway an. Wenn Sie nicht die Standard-Shell verwenden, wechseln Sie mit folgendem Befehl zu Clish: `clish`
2. Stellen Sie die Kunden-Gateway-ASN ein (die ASN, die bei der Erstellung des Kunden-Gateways in angegeben wurde AWS), indem Sie den folgenden Befehl ausführen.

```
set as 65000
```

3. Erstellen Sie die Tunnelschnittstelle für den ersten Tunnel anhand der Informationen aus dem Abschnitt `IPSec Tunnel #1` der Konfigurationsdatei. Geben Sie einen eindeutigen Namen für den Tunnel ein, z. B. `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. Wiederholen Sie diese Befehle, um den zweiten Tunnel zu erstellen. Verwenden Sie dafür die Informationen im Bereich `IPSec Tunnel #2` der Konfigurationsdatei. Geben Sie einen eindeutigen Namen für den Tunnel ein, z. B. `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Legen Sie die ASN des Virtual Private Gateways fest.

```
set bgp external remote-as 7224 on
```

6. Konfigurieren Sie das BGP für den ersten Tunnel anhand der Informationen im Abschnitt `IPSec Tunnel #1` der Konfigurationsdatei:

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Konfigurieren Sie das BGP für den zweiten Tunnel anhand der Informationen im Abschnitt `IPSec Tunnel #2` der Konfigurationsdatei:

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Speichern Sie die Konfiguration.

```
save config
```

So erstellen Sie eine BGP-Richtlinie

Erstellen Sie als Nächstes eine BGP-Richtlinie, die den Import von Routen erlaubt, die von AWS verbreitet werden. Anschließend konfigurieren Sie Ihr Kunden-Gateway so, dass dessen lokale Routen an AWS gesendet werden.

1. Klicken Sie im Gaia WebUI auf Advanced Routing und dann auf Inbound Route Filters. Klicken Sie auf Add und wählen Sie Add BGP Policy (Based on AS) aus.
2. Wählen Sie für Add BGP Policy (BGP-Richtlinie hinzufügen) im ersten Feld einen Wert zwischen 512 und 1024 aus und geben Sie im zweiten Feld die ASN des Virtual Private Gateways ein, z. B. `7224`.
3. Wählen Sie Save (Speichern) aus.

So kündigen Sie lokale Routen an

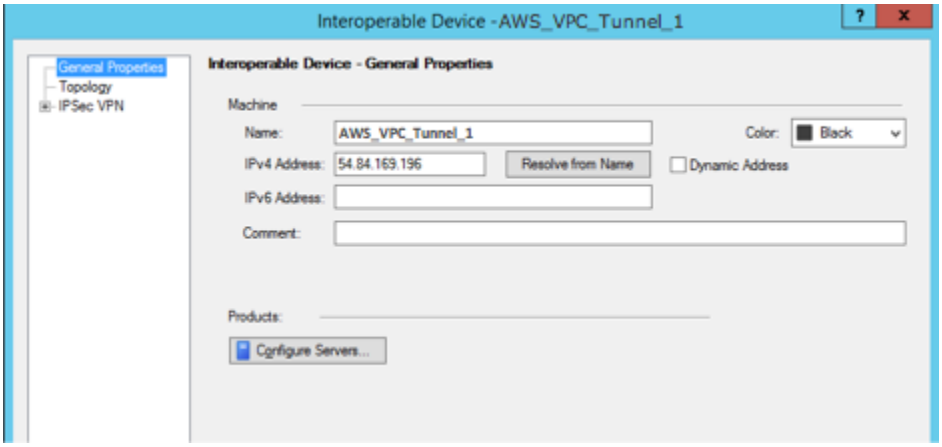
In den folgenden Schritten wird die Verteilung von lokalen Schnittstellenrouten beschrieben. Sie können Routen auch von anderen Quellen neu verteilen, z. B. statische Routen oder Routen, die Sie über dynamische Routing-Protokolle erhalten haben. Weitere Informationen finden Sie unter Gaia Advanced Routing R77 Versions Administration Guide.

1. Klicken Sie im Gaia WebUI auf Advanced Routing und dann auf Routing Redistribution. Wählen Sie Add Redistribution From (Neuverteilung hinzufügen von) aus. Wählen Sie dann Interface (Schnittstelle) aus.
2. Wählen Sie für To Protocol (Zu Protokoll) die ASN des Virtual Private Gateways aus, z. B. `7224`.
3. Wählen Sie für Interface eine interne Schnittstelle aus. Wählen Sie Save (Speichern) aus.

So definieren Sie ein neues Netzwerkobjekt

Dann erstellen Sie ein Netzwerkobjekt für jeden VPN-Tunnel und legen die öffentlichen (externen) IP-Adressen für das Virtual Private Gateway fest. Später fügen Sie diese Netzwerkobjekte als Satelliten-Gateways für Ihre VPN-Community hinzu. Außerdem müssen Sie eine leere Gruppe erstellen, die als Platzhalter für die VPN-Domäne dient.

1. Öffnen Sie den Check Point. SmartDashboard
2. Öffnen Sie für Groups das Kontextmenü und klicken Sie auf Groups und Simple Group. Sie können für alle Netzwerkobjekte dieselbe Gruppe verwenden.
3. Öffnen Sie mit der rechten Maustaste für Network Objects das Kontextmenü und wählen Sie New und Interoperable Device aus.
4. Geben Sie unter Name den Namen des Tunnels aus Schritt 1 ein, z. B. `AWS_VPC_Tunnel_1` oder `AWS_VPC_Tunnel_2`.
5. Geben Sie unter IPv4 Adresse die externe IP-Adresse des virtuellen privaten Gateways ein, die in der Konfigurationsdatei angegeben ist, `54.84.169.196` z. B. Speichern Sie die Einstellungen und schließen Sie das Dialogfeld.




6. Wählen Sie im linken Kategoriebereich Topology aus.

7. Klicken Sie im Bereich VPN Domain (VPN-Domäne) auf Manually defined (Manuell definiert) und wählen Sie die leere einfache Gruppe aus, die Sie in Schritt 2 erstellt haben. Wählen Sie OK aus.
8. Wiederholen Sie diese Schritte, um ein zweites Netzwerkobjekt zu erstellen. Verwenden Sie dafür die Informationen im Bereich `IPSec Tunnel #2` der Konfigurationsdatei.
9. Rufen Sie das Gateway-Netzwerkobjekt auf, öffnen Sie das Gateway oder Cluster-Objekt und klicken Sie auf Topology.
10. Klicken Sie im Bereich VPN Domain (VPN-Domäne) auf Manually defined (Manuell definiert) und wählen Sie die leere einfache Gruppe aus, die Sie in Schritt 2 erstellt haben. Wählen Sie OK aus.

> **Note**
>
> Sie können eine vorhandene VPN-Domäne, die Sie bereits konfiguriert haben, beibehalten. Stellen Sie jedoch sicher, dass die verwendeten Hosts und Netzwerke von der neuen VPN-Verbindung bedient werden und nicht in dieser VPN-Domäne deklariert werden, insbesondere wenn die VPN-Domäne automatisch abgeleitet wird.

> **Note**
>
> Wenn Sie Cluster verwenden, bearbeiten Sie die Topologie und legen Sie die Schnittstellen als Cluster-Schnittstellen fest. Verwenden Sie die IP-Adressen, die in der Konfigurationsdatei angegeben sind.

Um die VPN-Community, IKE und IPsec Einstellungen zu erstellen und zu konfigurieren

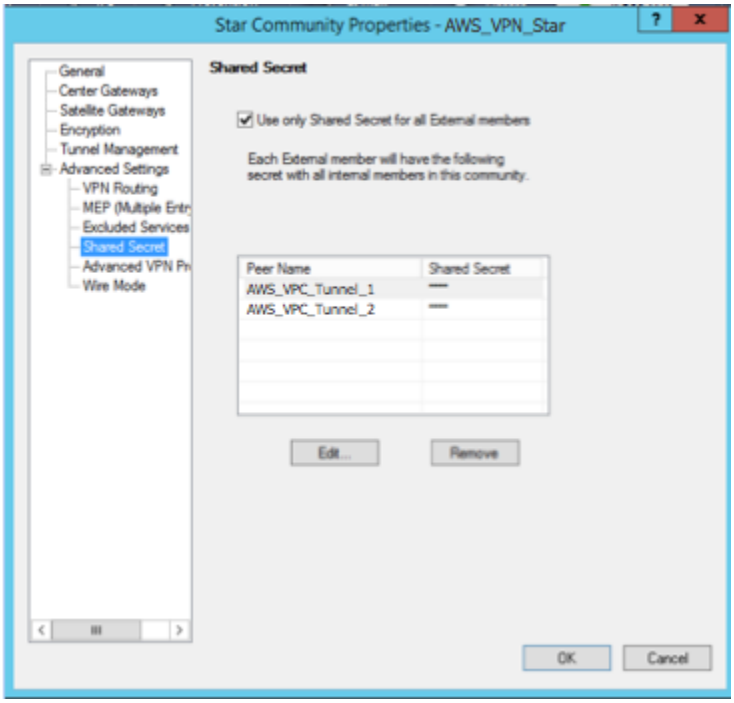
Dann erstellen Sie eine VPN-Community in Ihrem Check Point-Gateway, zu dem Sie die Netzwerkobjekte (interoperablen Geräte) für die einzelnen Tunnel hinzufügen. Sie konfigurieren auch den Internet Key Exchange (IKE) und die IPsec Einstellungen.

1. Wählen Sie in Ihren Gateway-Eigenschaften im Kategorienbereich die Option IPSecVPN aus.
2. Klicken Sie auf Communities, New und Star Community.
3. Geben Sie einen Namen für die Community ein (z. B. `AWS_VPN_Star`) und klicken Sie im Kategoriebereich auf Center Gateways.

4. Klicken Sie auf Add und fügen Sie Ihr Gateway bzw. Ihren Cluster der Liste der teilnehmenden Gateways hinzu.
5. Klicken Sie im Kategoriebereich auf Satellite Gateways (Satelliten-Gateways) und Add (Hinzufügen) und fügen Sie die interoperablen Geräte, die Sie vorher erstellt haben (`AWS_VPC_Tunnel_1` und `AWS_VPC_Tunnel_2`) der Liste der teilnehmenden Gateways hinzu.
6. Klicken Sie im Kategoriebereich auf Encryption. Wählen Sie im Abschnitt Verschlüsselungsmethode die Optionen IKEv1 für IPv4 und IKEv2 für aus IPv6. Wählen Sie im Bereich Encryption Suite Custom und Custom Encryption aus.

   > **Note**
   >
   > Sie müssen IKEv1 für die IKEv1 Funktionalität die IPv6 Optionen IKEv2 für IPv4 und für auswählen.

7. Konfigurieren Sie im Dialogfeld die Verschlüsselungseigenschaften wie nachfolgend beschrieben und klicken Sie dann auf OK:
   - Eigenschaften von IKE Security Association (Phase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Eigenschaften von Security Association (Phase 2):
     - Führen Sie eine IPsec Datenverschlüsselung durch mit: AES-128
     - Perform data integrity with: SHA-1
8. Klicken Sie im Kategoriebereich auf Tunnel Management. Klicken Sie auf Set Permanent Tunnels und On all tunnels in the community. Wählen Sie im Bereich VPN Tunnel Sharing One VPN tunnel per Gateway pair aus.
9. Erweitern Sie im Kategoriebereich Advanced Settings und klicken Sie auf Shared Secret.
10. Wählen Sie den Peer-Namen für den ersten Tunnel aus, klicken Sie auf Edit (Bearbeiten) und geben Sie den vorinstallierten Schlüssel aus dem Bereich `IPSec Tunnel #1` der Konfigurationsdatei ein.
11. Wählen Sie den Peer-Namen für den zweiten Tunnel aus, klicken Sie auf Edit (Bearbeiten) und geben Sie den vorinstallierten Schlüssel aus dem Bereich `IPSec Tunnel #2` der Konfigurationsdatei ein.




12. Klicken Sie – noch immer in der Kategorie Advanced Settings (Erweiterte Einstellungen) – auf Advanced VPN Properties (Erweiterte VPN-Eigenschaften), konfigurieren Sie die Eigenschaften wie nachfolgend beschrieben und klicken Sie abschließend auf OK:

    - IKE (Phase 1):
        - Diffie-Hellman-Gruppe verwenden: `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Phase 2):
        - Use Perfect Forward Secrecy auswählen
        - Diffie-Hellman-Gruppe verwenden: `Group 2 (1024 bit)`
        - Verhandeln Sie IPsec Sicherheitszuordnungen alle Sekunden neu **`3600`**

So erstellen Sie Firewall-Regeln

Dann konfigurieren Sie eine Richtlinie mit Firewall-Regeln und direktionalen Übereinstimmungsregeln, um Kommunikation zwischen der VPC und dem On-Premise-Netzwerk zu ermöglichen. Dann installieren Sie diese Richtlinie auf Ihrem Gateway.

1. Wählen Sie im SmartDashboard Global Properties für Ihr Gateway aus. Erweitern Sie im Kategoriebereich VPN und klicken Sie auf Advanced.
2. Klicken Sie auf Enable VPN Directional Match in VPN Column und anschließend auf OK.

3. Wählen Sie im die SmartDashboard Option Firewall aus und erstellen Sie eine Richtlinie mit den folgenden Regeln:
   - Erlauben Sie dem VPC-Subnetz, über die erforderlichen Protokolle mit dem lokalen Netzwerk zu kommunizieren.
   - Erlauben Sie dem lokalen Netzwerk, über die erforderlichen Protokolle mit dem VPC-Subnetz zu kommunizieren.
4. Öffnen Sie das Kontextmenü für die Zelle in der VPN-Spalte und klicken Sie auf Edit Cell.
5. Klicken Sie im Dialogfeld VPN Match Conditions auf Match traffic in this direction only. Klicken Sie jeweils auf Add (Hinzufügen) und abschließend auf OK:
   - `internal_clear` > VPN-Community (die VPN-Star-Community, die Sie vorher erstellt haben, z. B. `AWS_VPN_Star`)
   - VPN-Community > VPN-Community
   - VPN-Community > `internal_clear`
6. Wählen Sie im die SmartDashboard Option Richtlinie, Installieren aus.
7. Wählen Sie im Dialogfeld das Gateway aus und klicken Sie auf OK, um die Richtlinie zu installieren.

So ändern Sie die Eigenschaft "tunnel_keepalive_method"

Sie können für Ihren Check Point-Gateway Dead Peer Detection (DPD) verwenden, um Ausfälle bei der IKE-Zuordnung zu identifizieren. Um DPD für einen permanenten Tunnel zu konfigurieren, muss der permanente Tunnel in der AWS VPN-Community konfiguriert werden.

Standardmäßig ist für die Eigenschaft `tunnel_keepalive_method` eines VPN-Gateways der Wert `tunnel_test` festgelegt. Sie müssen diesen Wert zu dpd ändern. Für alle VPN-Gateways innerhalb der VPN-Community, einschließlich VPN-Gateways von Drittanbietern, für die Sie DPD-Überwachung aktivieren möchten, muss die Eigenschaft `tunnel_keepalive_method` konfiguriert werden. Es ist nicht möglich, für dasselbe Gateway unterschiedliche Überwachungsmechanismen zu konfigurieren.

Sie können die `tunnel_keepalive_method` Eigenschaft mit dem DBedit GUI-Tool aktualisieren.

1. Öffnen Sie den Check Point SmartDashboard und wählen Sie Security Management Server, Domain Management Server.

2. Klicken Sie auf File und Database Revision Control… und erstellen Sie einen Versions-Snapshot.
3. Schließen Sie alle SmartConsole Fenster, z. B. SmartView Tracker und SmartView Monitor. SmartDashboard
4. Starten Sie das BDedit GUI-Tool. Weitere Informationen finden Sie im Artikel Check Point Database Tool im Check Point-Supportcenter.
5. Klicken Sie auf Security Management Server und Domain Management Server.
6. Klicken Sie oben links auf Table, Network Objects und network_objects.
7. Wählen Sie oben rechts das entsprechende Security Gateway-Cluster-Objekt aus.
8. Drücken Sie STRG + F oder verwenden Sie das Suchmenü, um nach folgender Zeichenfolge zu suchen: `tunnel_keepalive_method`.
9. Öffnen Sie im unteren Bereich das Kontextmenü für `tunnel_keepalive_method` und klicken Sie auf Edit…. Wählen Sie dpd, OK.
10. Wiederholen Sie die Schritte 7 bis 9 für jedes Gateway, das Teil der AWS VPN-Community ist.
11. Klicken Sie auf File und Save All.
12. Schließen Sie das DBedit GUI-Tool.
13. Öffnen Sie den Check Point SmartDashboard und wählen Sie Security Management Server, Domain Management Server.
14. Installieren Sie die Richtlinie für das entsprechende Security Gateway-Cluster-Objekt.

Weitere Informationen finden Sie im Artikel New VPN features in R77.10 im Check Point-Supportcenter.

So aktivieren Sie TCP MSS Clamping

Mit TCP MSS Clamping können Sie die maximale Segmentgröße von TCP-Paketen reduzieren, um eine Paketfragmentierung zu vermeiden.

1. Öffnen Sie das folgende Verzeichnis: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Führen Sie die Datei `GuiDBEdit.exe` aus, um das Check Point-Datenbank-Tool zu starten.
3. Wählen Sie Table, Global Properties und properties aus.

4. Klicken Sie für `fw_clamp_tcp_mss` auf Edit. Ändern Sie den Wert in `true` und wählen Sie dann OK.

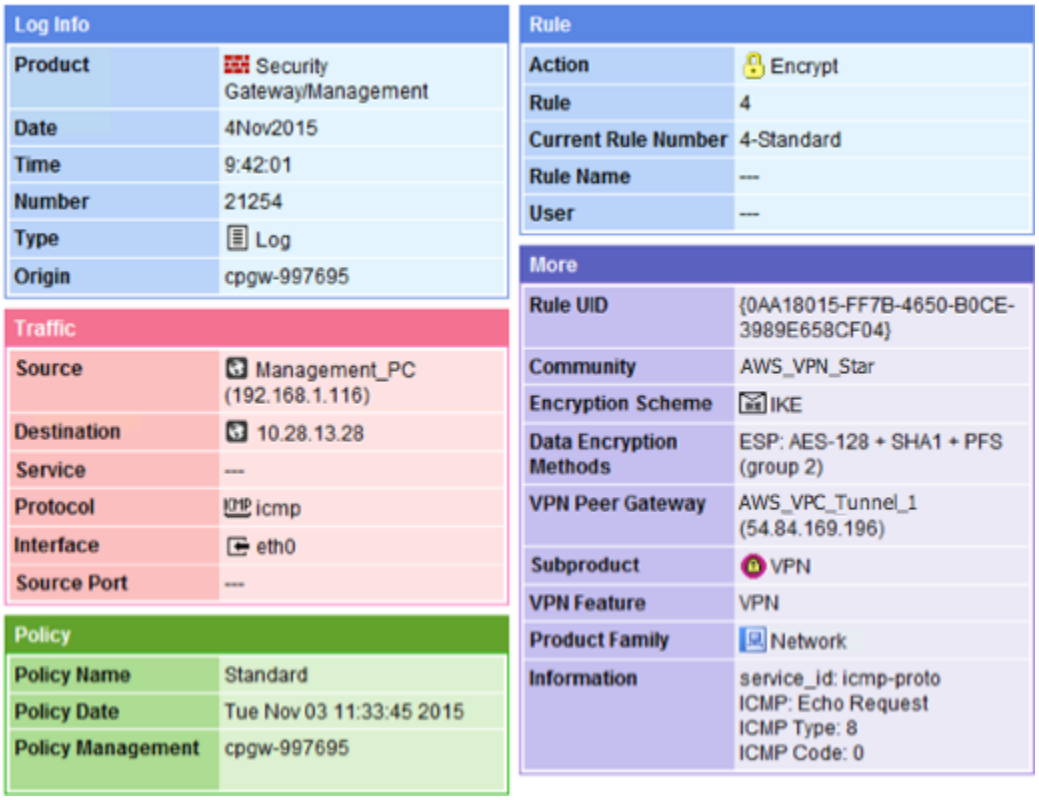
So überprüfen Sie den Tunnelstatus

Sie können den Tunnelstatus überprüfen, indem Sie den folgenden Befehl vom Befehlszeilen-Tool aus im Expertenmodus ausführen.

```
vpn tunnelutil
```

Wählen Sie in den angezeigten Optionen 1 aus, um die IKE-Verknüpfungen zu überprüfen, und 2, um die IPsec Verknüpfungen zu überprüfen.

Im Check Point Smart Tracker-Protokoll können Sie auch überprüfen, ob Pakete über diese Verbindung verschlüsselt werden. Dem folgenden Protokoll können Sie beispielsweise entnehmen, dass ein Paket verschlüsselt über Tunnel 1 an die VPC gesendet wurde.




## SonicWALL

Sie können ein SonicWALL-Gerät über die SonicOS-Verwaltungsoberfläche konfigurieren. Weitere Informationen zur Konfiguration von Tunneln finden Sie unter Konfigurieren Sie statisches Routing für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Sie können das BGP des Geräts nicht mit der Management-Schnittstelle konfigurieren. Verwenden Sie stattdessen die Befehlszeilenanleitungen, die in der oben gezeigten Beispielkonfigurationsdatei unter dem Abschnitt BGP genannt sind.

## Cisco-Geräte: zusätzliche Informationen

Einige Cisco unterstützen ASAs nur den Aktiv-/Standby-Modus. Wenn Sie diese Cisco verwenden ASAs, können Sie jeweils nur einen aktiven Tunnel haben. Der andere Standby-Tunnel wird aktiv, falls der erste Tunnel nicht verfügbar ist. Diese Redundanz sorgt dafür, dass immer ein Tunnel für die Verbindung zu Ihrer VPC verfügbar ist.

Cisco unterstützt ASAs ab Version 9.7.1 und höher den Active/Active-Modus. Wenn Sie diese Cisco verwenden ASAs, können Sie beide Tunnel gleichzeitig aktiv haben. Diese Redundanz sorgt dafür, dass immer ein Tunnel für die Verbindung zu Ihrer VPC verfügbar ist.

Für Cisco-Geräte müssen Sie die folgenden Schritte ausführen:

- Konfigurieren Sie die Außenschnittstelle.
- Stellen Sie sicher, dass die Crypto ISAKMP-Richtliniensequenznummer eindeutig ist.
- Stellen Sie sicher, dass die Crypto List-Richtliniensequenznummer eindeutig ist.
- Stellen Sie sicher, dass das Crypto IPsec Transform Set und die Crypto ISAKMP Policy Sequence mit allen anderen IPsec Tunneln, die auf dem Gerät konfiguriert sind, harmonieren.
- Stellen Sie sicher, dass die SLA-Überwachungsnummer eindeutig ist.
- Konfigurieren Sie sämtliche internen Routen, über die Datenverkehr zwischen dem Kunden-Gateway-Gerät und Ihrem On-Premise-Netzwerk gesendet wird.

## Juniper-Geräte: zusätzliche Informationen

Die folgenden Informationen beziehen sich auf die Beispielkonfigurationsdateien für Kunden-Gateway-Geräte der Juniper J-Serie und SRX.

- Die externe Schnittstelle wird als `ge-0/0/0.0` bezeichnet.
- Die Tunnelschnittstelle IDs wird als `st0.1` und bezeichnet`st0.2`.
- Vergewissern Sie sich, dass Sie die Sicherheitszone für die Uplink-Schnittstelle identifizieren (die Konfigurationsinformationen verwenden die standardmäßige "Nicht vertrauenswürdig"-Zone).

- Stellen Sie sicher, dass Sie die Sicherheitszone für die interne Schnittstelle identifizieren (die Konfigurationsinformationen verwenden die standardmäßige "Vertrauenswürdig"Zone).

# Windows Server als AWS Site-to-Site VPN Kunden-Gatewaygerät konfigurieren

Sie können einen Server mit Windows Server als Kunden-Gateway-Gerät für Ihre VPC konfigurieren. Verwenden Sie den folgenden Prozess, unabhängig davon, ob Sie Windows Server auf einer EC2 Instanz in einer VPC oder auf Ihrem eigenen Server ausführen. Die folgenden Verfahren gelten für Windows Server 2012 R2 und höher.

Inhalt


- Konfigurieren der Windows-Instance
- Schritt 1: Erstellen einer VPN-Verbindung und Konfigurieren Ihrer VPC
- Schritt 2: Herunterladen der Konfigurationsdatei für die VPN-Verbindung
- Schritt 3: Konfigurieren des Windows-Servers
- Schritt 4: Einrichten des VPN-Tunnels
- Schritt 5: Aktivieren von Dead Gateway Detection
- Schritt 6: Testen der VPN-Verbindung


## Konfigurieren der Windows-Instance

Wenn Sie Windows Server auf einer EC2 Instance konfigurieren, die Sie über ein Windows-AMI gestartet haben, gehen Sie wie folgt vor:

- Deaktivieren Sie für die Instance die Quell-/Zielprüfung:
  1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
  2. Wählen Sie Ihre Windows-Instance aus und wählen Sie dann Actions, Networking, Change Source/Dest. check. Wählen Sie Add und dann Save aus.
- Aktualisieren Sie Ihre Adapter-Einstellungen, sodass Sie Datenverkehr von anderen Instances weiterleiten können:
  1. Herstellen einer Verbindung mit Ihrer Windows-Instance. Weitere Informationen finden Sie unter Verbindung zu Ihrer Windows-Instance.

2. Öffnen Sie die Systemsteuerung und starten Sie den Geräte-Manager.
3. Erweitern Sie den Knoten Network adapters.
4. Wählen Sie den Netzwerkadapter (je nach Instance-Typ kann dies Amazon Elastic Network Adapter oder Intel 82599 Virtual Function sein) und wählen Sie Action, Properties.
5. Deaktivieren Sie auf der Registerkarte Erweitert die Eigenschaften IPv4Checksum Offload, TCP Checksum Offload (IPv4) und UDP Checksum Offload (IPv4) und wählen Sie dann OK.

- Weisen Sie Ihrem Konto eine Elastic-IP-Adresse zu und ordnen Sie diese der Instance zu. Weitere Informationen finden Sie unter Elastic IP-Adressen im EC2 Amazon-Benutzerhandbuch. Notieren Sie sich diese Adresse — Sie benötigen sie, wenn Sie das Kunden-Gateway erstellen.
- Stellen Sie sicher, dass die Sicherheitsgruppenregeln der Instanz ausgehenden IPsec Datenverkehr zulassen. Standardmäßig lässt eine Sicherheitsgruppe den gesamten ausgehenden Datenverkehr zu. Wenn die ausgehenden Regeln der Sicherheitsgruppe jedoch gegenüber ihrem ursprünglichen Status geändert wurden, müssen Sie die folgenden benutzerdefinierten Protokollregeln für ausgehenden IPsec Datenverkehr erstellen: IP-Protokoll 50, IP-Protokoll 51 und UDP 500.

Beachten Sie beispielsweise den CIDR-Bereich des Netzwerks, in dem sich Ihre Windows-Instance befindet, z. B. `172.31.0.0/16`.

## Schritt 1: Erstellen einer VPN-Verbindung und Konfigurieren Ihrer VPC

Um eine VPN-Verbindung von Ihrer VPC aus zu erstellen, gehen Sie folgendermaßen vor:

1. Erstellen Sie ein Virtual Private Gateway und weisen Sie es Ihrer VPC zu. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateways.
2. Erstellen Sie eine VPN-Verbindung und ein neues Kunden-Gateway. Geben Sie für das Kunden-Gateway die öffentliche IP-Adresse Ihres Windows-Servers an. Wählen Sie für die VPN-Verbindung statisches Routing aus. Geben Sie dann den CIDR-Bereich für Ihr Netzwerk ein, in dem sich der Windows-Server befindet, z. B. `172.31.0.0/16`. Weitere Informationen finden Sie unter Schritt 5: Eine VPN-Verbindung erstellen.

Nachdem Sie die VPN-Verbindung erstellt haben, konfigurieren Sie die VPC so, dass die Kommunikation über die VPN-Verbindung ermöglicht wird.

Konfigurieren Ihrer VPC

- Erstellen Sie ein privates Subnetz in der VPC (sofern nicht schon vorhanden), mit dem Sie Instances starten können, die mit dem Windows Server kommunizieren sollen. Weitere Informationen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC.

> **Note**
>
> Ein privates Subnetz ist ein Subnetz ohne Weiterleitung an das Internet-Gateway. Das Routing für dieses Subnetz wird unter dem nächsten Punkt beschrieben.

- Aktualisieren der Routing-Tabellen für die VPN-Verbindung:
  - Fügen Sie der Routing-Tabelle Ihres privaten Subnetzes eine Route mit dem Virtual Private Gateway als Ziel und dem Netzwerk des Windows-Servers (CIDR-Bereich) als Zielbereich hinzu. Weitere Informationen finden Sie unter Hinzufügen und Entfernen von Routen aus einer Routing-Tabelle im Amazon VPC-Benutzerhandbuch.
  - Aktivieren Sie die Routing-Verbreitung für das Virtual Private Gateway. Weitere Informationen finden Sie unter (Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle.
- Erstellen Sie eine Sicherheitsgruppe für Ihre Instances, die die Kommunikation zwischen Ihrer VPC und Ihrem Netzwerk ermöglicht:
  - Fügen Sie Regeln hinzu, die eingehenden RDP- bzw. SSH-Zugriff von Ihrem Netzwerk zulassen. So können Sie von Ihrem Netzwerk aus eine Verbindung zu Instances in Ihrer VPC herstellen. Wenn Sie z. B. möchten, dass Computer in Ihrem Netzwerk Zugriff auf die Linux-Instances in Ihrer VPC haben, erstellen Sie eine Eingangsregel mit einem SSH-Typ und stellen Sie die Quelle auf den CIDR-Bereich Ihres Netzwerks ein, z. B. `172.31.0.0/16`. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für Ihre VPC im Amazon VPC-Benutzerhandbuch.
  - Fügen Sie eine Regel hinzu, die eingehenden ICMP-Zugriff von Ihrem Netzwerk zulässt. So können Sie Ihre VPN-Verbindung testen, indem Sie von Ihrem Windows-Server aus einen Ping an eine Instance in der VPC senden.

## Schritt 2: Herunterladen der Konfigurationsdatei für die VPN-Verbindung

Sie können mithilfe der Amazon VPC-Konsole eine Windows-Server-Konfigurationsdatei für die VPN-Verbindung herunterladen.

So laden Sie die Konfigurationsdatei herunter

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Connections aus.
3. Wählen Sie erst Ihre VPN-Verbindung und dann Download Configuration (Konfiguration herunterladen) aus.
4. Wählen Sie als Anbieter Microsoft, als Plattform Windows Server und als Software 2012 R2 aus. Wählen Sie Herunterladen aus. Sie können die Datei öffnen oder speichern.

Die Konfigurationsdatei enthält einen Abschnitt mit Informationen, der dem folgenden Beispiel ähnelt. Diese Informationen werden zweimal angezeigt, einmal für jeden Tunnel.

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

Die IP-Adresse, die Sie für das Kunden-Gateway angegeben haben, als Sie die VPN-Verbindung erstellt haben.

`Remote Tunnel Endpoint`

Eine von zwei IP-Adressen für das Virtual Private Gateway, das die VPN-Verbindung auf der AWS Seite der Verbindung beendet.

`Endpoint 1`

Das IP-Präfix, das Sie beim Erstellen der VPN-Verbindung als statische Route konfiguriert haben. Dabei handelt es sich um die IP-Adressen in Ihrem Netzwerk, die über die VPN-Verbindung auf die VPC zugreifen können.

`Endpoint 2`

Der IP-Adressbereich (CIDR-Block) der VPC, die mit dem Virtual Private Gateway verknüpft ist (z. B. 10.0.0.0/16)

`Preshared key`

Der vorab gemeinsam genutzte Schlüssel, der zum Herstellen der IPsec VPN-Verbindung zwischen und `Local Tunnel Endpoint` verwendet wird. `Remote Tunnel Endpoint`

Wir empfehlen Ihnen, beide Tunnel als Teil der VPN-Verbindung zu konfigurieren. Jeder Tunnel ist mit einem separaten VPN-Konzentrator auf der Amazon-Seite der VPN-Verbindung verbunden. Es ist zwar jeweils nur ein Tunnel aktiv, aber der zweite Tunnel baut sich automatisch auf, wenn der erste Tunnel ausfällt. Redundante Tunnel gewährleisten eine kontinuierliche Verfügbarkeit im Falle eines Geräteausfalls. Da nur ein Tunnel gleichzeitig verfügbar ist, wird auf der Amazon VPC-Konsole angezeigt, dass ein Tunnel inaktiv ist. Dies ist jedoch Absicht und bedarf keiner Handlung Ihrerseits.

Wenn zwei Tunnel konfiguriert sind und innerhalb weniger Minuten ein Geräteausfall auftritt AWS, wird Ihre VPN-Verbindung automatisch auf den zweiten Tunnel des Virtual Private Gateways umgestellt. Konfigurieren Sie beim Konfigurieren Ihres Kunden-Gateway-Geräts unbedingt beide Tunnel.

> **Note**
>
> AWS Führt von Zeit zu Zeit routinemäßige Wartungsarbeiten am Virtual Private Gateway durch. Durch diese Wartungsarbeiten kann es vorkommen, dass ein oder beide Tunnel der VPN-Verbindung kurzzeitig deaktiviert werden. Ihre VPN-Verbindung schaltet automatisch auf den zweiten Tunnel, während diese Wartungen durchgeführt werden.

Zusätzliche Informationen zu Internet Key Exchange (IKE) und IPsec Security Associations (SA) finden Sie in der heruntergeladenen Konfigurationsdatei.

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

Die Verschlüsselungs- und Authentifizierungsalgorithmen für die IKE-SA. Dies sind die empfohlenen Einstellungen für die VPN-Verbindung und die Standardeinstellungen für Windows IPsec Server-VPN-Verbindungen.

`MainModeKeyLifetime`

Die Lebensdauer des IKE-SA-Schlüssels. Dies ist die empfohlene Einstellung für die VPN-Verbindung und die Standardeinstellung für Windows IPsec Server-VPN-Verbindungen.

`QuickModeSecMethods`

Die Verschlüsselungs- und Authentifizierungsalgorithmen für die IPsec SA. Dies sind die empfohlenen Einstellungen für die VPN-Verbindung und die Standardeinstellungen für Windows IPsec Server-VPN-Verbindungen.

`QuickModePFS`

Wir empfehlen Ihnen, Master Key Perfect Forward Secrecy (PFS) für Ihre Sitzungen zu verwenden. IPsec

## Schritt 3: Konfigurieren des Windows-Servers

Bevor Sie den VPN-Tunnel einrichten, müssen Sie Routing- und RAS-Dienste auf Windows Server installieren und konfigurieren. Dadurch können Benutzer auf die Ressourcen in Ihrem Netzwerk zugreifen.

So installieren Sie Routing- und Remotezugriff-Services

1. Melden Sie sich bei Ihrem Windows Server an.
2. Navigieren Sie zum Menü Start und wählen Sie Server-Manager aus.
3. Installation der Routing- und Remotezugriff-Services:
   a. Wählen Sie im Menü Verwalten die Option Rollen und Features hinzufügen aus.
   b. Überprüfen Sie auf der Seite Bevor Sie beginnen, ob Ihr Server alle Voraussetzungen erfüllt, und klicken Sie dann auf Weiter.
   c. Wählen Sie erst Rollenbasierte oder featurebasierte Installation und dann Weiter aus.
   d. Wählen Sie erst die Option Einen Server aus dem Serverpool auswählen, dann den Windows-Server und anschließend Weiter aus.
   e. Wählen Sie Netzwerkrichtlinien- und Zugriffsdienste aus der Liste aus. Wählen Sie im daraufhin angezeigten Dialogfeld Features hinzufügen aus, um die für diese Rolle erforderlichen Funktionen zu bestätigen.
   f. Wählen Sie in derselben Liste Remote Access (Remotezugriff) und dann Next (Weiter) aus.

g. Wählen Sie auf der Seite Features auswählen die Option Weiter aus.

h. Wählen Sie auf der Seite Netzwerkrichtlinien- und Zugriffsdienste Weiter aus.

i. Wählen Sie auf der Seite Remotezugriff die Option Weiter aus. Wählen Sie DirectAccess auf der nächsten Seite VPN (RAS) aus. Wählen Sie im angezeigten Dialogfeld die Option Features hinzufügen aus, um die für diesen Rollenservice erforderlichen Funktionen zu bestätigen. Wählen Sie in derselben Liste Routing und anschließend Weiter aus.

j. Klicken Sie auf der Seite Rolle 'Webserver' (IIS) auf Weiter. Belassen Sie die Standardauswahl und wählen Sie Weiter aus.

k. Wählen Sie Installieren aus. Nach abgeschlossener Installation wählen Sie Schließen aus.

So konfigurieren und aktivieren Sie den Routing- und Remotezugriff-Server

1. Wählen Sie auf dem Dashboard Benachrichtigungen (das Flag-Symbol) aus. Es sollte eine Aufgabe angezeigt werden, mit der Sie die Konfiguration nach der Bereitstellung abschließen können. Wählen Sie den Link Assistent für erste Schritte öffnen aus.
2. Wählen Sie Nur VPN bereitstellen aus.
3. Wählen Sie im Dialogfenster Routing and Remote Access (Routing und Remotezugriff( den Servernamen, dann Action (Aktion) und anschließend Configure and Enable Routing und Remote Access (Routing und RAS konfigurieren und aktivieren) aus.
4. Wählen Sie auf der ersten Seite des Setup-Assistent für den Routing- und RAS-Server die Option Weiter aus.
5. Wählen Sie auf der Seite Configuration (Konfiguration) erst die Option Custom Configuration (Benutzerdefinierte Konfiguration) und anschließend Next (Weiter) aus.
6. Wählen Sie LAN routing (LAN-Routing), Next (Weiter) und Finish (Fertig stellen) aus.
7. Wenn das Dialogfeld Routing und Remotezugriff Sie dazu auffordert, wählen Sie Dienst starten aus.

## Schritt 4: Einrichten des VPN-Tunnels

Sie können den VPN-Tunnel konfigurieren, indem Sie die in der heruntergeladenen Konfigurationsdatei enthaltenen Netsh-Skripte ausführen oder die Windows Server-Benutzeroberfläche verwenden.

> **Important**
>
> Wir empfehlen Ihnen, Master Key Perfect Forward Secrecy (PFS) für Ihre Sitzungen zu verwenden. IPsec Wenn Sie das Netsh-Skript ausführen möchten, enthält es einen Parameter zur Aktivierung von PFS (). `qmpfs=dhgroup2` Sie können PFS nicht über die Windows-Benutzeroberfläche aktivieren, sondern müssen es über die Befehlszeile aktivieren.

Optionen

- Option 1: Ausführen des Netsh-Skripts
- Option 2: Verwenden der Windows-Server-Benutzeroberfläche

## Option 1: Ausführen des Netsh-Skripts

Kopieren Sie das Netsh-Skript aus der heruntergeladenen Konfigurationsdatei und ersetzen Sie die Variablen. Nachfolgend sehen Sie ein Beispielskript.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: Sie können den empfohlenen Namen (`vgw-1a2b3c4d Tunnel 1`) durch einen beliebigen Namen ersetzen.

LocalTunnelEndpoint: Geben Sie die private IP-Adresse des Windows Servers in Ihrem Netzwerk ein.

Endpoint1: Der CIDR-Block Ihres Netzwerks, in dem sich der Windows-Server befindet, beispielsweise `172.31.0.0/16`. Umgeben Sie diesen Wert mit doppelten Anführungszeichen (").

Endpoint2: Der CIDR-Block Ihrer VPC oder eines Subnetzes der VPC, beispielsweise `10.0.0.0/16`. Umgeben Sie diesen Wert mit doppelten Anführungszeichen (").

Führen Sie das aktualisierte Skript in einem Befehlszeilenfenster auf dem Windows-Server aus. (Mit ^ können Sie umgebrochenen Text in der Eingabeaufforderung kopieren und einfügen.) Wiederholen

Sie diese Vorgehensweise mit dem zweiten Netsh-Skript aus der Konfigurationsdatei, um den zweiten VPN-Tunnel einzurichten.

Wenn Sie fertig sind, rufen Sie Konfigurieren der Windows-Firewall auf.

Weitere Informationen zu den Netsh-Parametern finden Sie unter Netsh AdvFirewall Consec-Befehle in der Microsoft-Bibliothek. TechNet

## Option 2: Verwenden der Windows-Server-Benutzeroberfläche

Sie können den VPN-Tunnel auch über die Windows-Server-Benutzeroberfläche einrichten.

> **Important**
>
> Sie können über die Windows-Server-Benutzeroberfläche keinen PFS-fähigen (Perfect Forward Secrecy) Master Key aktivieren. Sie müssen PFS über die Befehlszeile aktivieren, wie in Master Key Perfect Forward Secrecy aktivieren beschrieben.

Aufgaben

- Konfigurieren einer Sicherheitsregel für einen VPN-Tunnel
- Überprüfen der Tunnelkonfiguration
- Master Key Perfect Forward Secrecy aktivieren
- Konfigurieren der Windows-Firewall

### Konfigurieren einer Sicherheitsregel für einen VPN-Tunnel

In diesem Abschnitt konfigurieren Sie eine Sicherheitsregel auf Ihrem Windows-Server, um einen VPN-Tunnel zu erstellen.

So konfigurieren Sie eine Sicherheitsregel für einen VPN-Tunnel

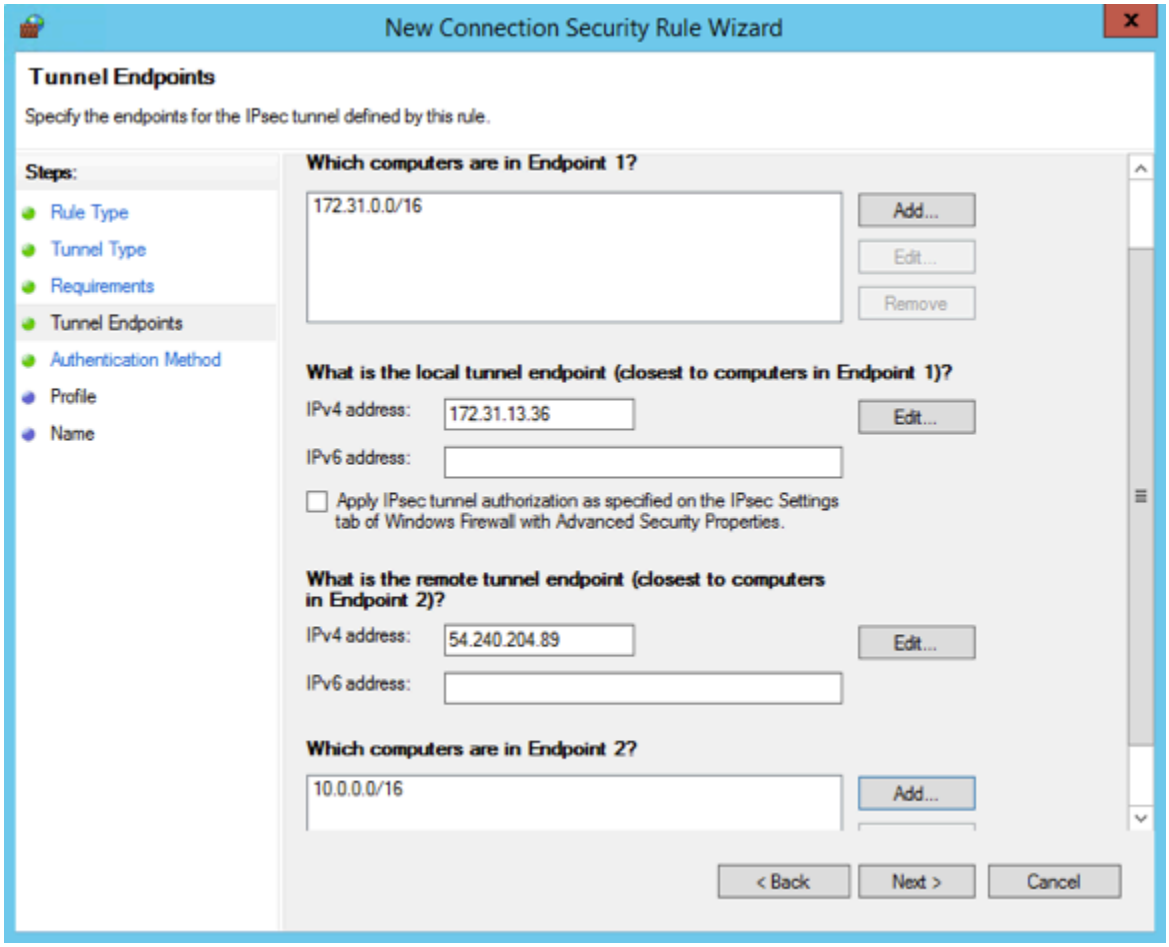
1. Öffnen Sie den Server-Manager, wählen Sie Tools und dann Windows Defender Firewall with Advanced Security (Windows-Firewall mit erweiterter Sicherheit) aus.
2. Wählen Sie erst Verbindungssicherheitsregeln, dann Aktion und anschließend Neue Regel aus.
3. Wählen Sie im Assistent für neue Verbindungssicherheitsregeln auf der Seite Regeltyp erst Tunnel und anschließend Weiter aus.

4. Wählen Sie auf der Seite Tunneltype unter Welche Art von Tunnel möchten Sie erstellen? die Option Benutzerdefinierte Konfiguration aus. Lassen Sie unter Möchten Sie IPsec -geschützte Verbindungen von diesem Tunnel ausnehmen, den Standardwert aktiviert (Nein). Senden Sie den gesamten Netzwerkverkehr, der dieser Verbindungssicherheitsregel entspricht, durch den Tunnel, und klicken Sie dann auf Weiter.
5. Wählen Sie auf der Seite „Anforderungen“ die Option Authentifizierung für eingehende Verbindungen erforderlich aus. Richten Sie keine Tunnel für ausgehende Verbindungen ein und wählen Sie dann Weiter.
6. Wählen Sie auf der Seite Tunnel Endpoints (Tunnelendpunkte) unter Which computers are in Endpoint 1 (Welche Computer befinden sich im Endpunkt 1) die Option Add (Hinzufügen) aus. Geben Sie den CIDR-Bereich Ihres Netzwerks (nach Ihrem Windows Server-Kunden-Gateway) ein, z. B. `172.31.0.0/16`, und wählen Sie dann OK aus. Der Bereich kann die IP-Adresse Ihres Kunden-Gateway-Geräts beinhalten.
7. Wählen Sie unter Was ist der lokale Tunnelendpunkt (am nächsten zu Computer in Endpunkt 1) die Option Bearbeiten aus. Geben Sie in das IPv4 Adressfeld die private IP-Adresse Ihres Windows Servers ein, und wählen Sie dann OK.
8. Wählen Sie unter Was ist der Remotetunnelendpunkt (am nächsten zu Computern in Endpunkt 2)? die Option Bearbeiten aus. Geben Sie in das IPv4 Adressfeld die IP-Adresse des virtuellen privaten Gateways für Tunnel 1 aus der Konfigurationsdatei ein (sieheRemote `Tunnel Endpoint`), und wählen Sie dann OK.

   > **Important**
   >
   > Wenn Sie diesen Vorgang für Tunnel 2 wiederholen, wählen Sie für Tunnel 2 den korrekten Endpunkt aus.

9. Wählen Sie unter Welche Computer befinden sich im Endpunkt 2? die Option Hinzufügen aus. Geben Sie in das Feld Diese IP-Adresse oder Subnetzfeld den CIDR-Block Ihrer VPC ein und wählen Sie dann OK aus.

   > **Important**
   >
   > Blättern Sie im Dialogfeld nach unten bis zu Welche Computer befinden sich im Endpunkt 2?. Wählen Sie erst dann Weiter aus, wenn Sie diesen Schritt abgeschlossen haben, da Sie sonst keine Verbindung zum Server herstellen können.




10. Bestätigen Sie, dass sämtliche Einstellungen korrekt sind und wählen Sie dann Next (Weiter) aus.
11. Wählen Sie auf der Seite Authentication Method (Authentifizierungsmethode) Advanced (Erweitert) und dann die Option Customize (Anpassen).
12. Wählen Sie unter Erste Authentifizierungsmethoden die Option Hinzufügen aus.
13. Wählen Sie Preshared key (Vorinstallierter Schlüssel) aus, geben Sie den Wert des vorinstallierten Schlüssels aus der Konfigurationsdatei ein und wählen Sie OK aus.

> **Important**
>
> Wenn Sie diesen Vorgang für Tunnel 2 wiederholen, achten Sie darauf, dass Sie für Tunnel 2 den korrekten vorinstallierten Schlüssel auswählen.

14. Achten Sie darauf, dass die Option Erste Authentifizierung ist optional nicht ausgewählt ist und wählen Sie OK aus.

15. Wählen Sie Weiter.
16. Aktivieren Sie auf der Seite Profile (Profil) die drei Kontrollkästchen Domain (Domäne), Private (Privat) und Public (Öffentlich). Wählen Sie Weiter.
17. Geben Sie auf der Seite Name einen Namen für Ihre Verbindungsregel ein, z. B. `VPN to Tunnel 1` und wählen Sie dann Fertig stellen aus.

Wiederholen Sie das vorhergehende Verfahren und geben Sie die Daten für Tunnel 2 aus Ihrer Konfigurationsdatei an.

Wenn Sie fertig sind, sind beide Tunnel für Ihre VPN-Verbindung konfiguriert.

Überprüfen der Tunnelkonfiguration

So überprüfen Sie die Tunnelkonfiguration

1. Öffnen Sie den Server-Manager, wählen Sie zuerst Tools, dann Windows-Firewall mit erweiterter Sicherheit und anschließend Verbindungssicherheitsregeln aus.
2. Überprüfen Sie für beide Tunnel Folgendes:
   - Für Aktiviert ist `Yes` ausgewählt.
   - Endpunkt 1 entspricht dem CIDR-Block für Ihr Netzwerk.
   - Endpunkt 2 entspricht dem CIDR-Block Ihrer VPC.
   - Für Authentication mode (Authentifizierungsmodus) ist `Require inbound and clear outbound` ausgewählt.
   - Für Authentifizierungsmethode ist `Custom` ausgewählt.
   - Für Endpunkt 1-Port ist `Any` ausgewählt.
   - Für Endpunkt 2-Port ist `Any` ausgewählt.
   - Für Protokoll ist `Any` ausgewählt.
3. Wählen Sie die erste Regel und dann Eigenschaften aus.
4. Wählen Sie auf der Registerkarte Authentication (Authentifizierung) unter Method (Methode) die Option Customize (Anpassen) aus. Vergewissern Sie sich, dass First authentication methods (Erste Authentifizierungsmethoden) den korrekten Pre-Shared-Key aus Ihrer Konfigurationsdatei für den Tunnel enthält, und wählen Sie dann OK aus.
5. Überprüfen Sie auf der Registerkarte Erweitert, ob die drei Optionen Domäne, Privat und Öffentlich ausgewählt sind.

6. Wählen Sie unter IPsec Tunneling die Option Anpassen aus. Überprüfen Sie die folgenden IPsec Tunneleinstellungen, und klicken Sie dann auf OK und erneut auf OK, um das Dialogfeld zu schließen.

   - IPsec Tunneling verwenden ist ausgewählt.
   - Lokaler Tunnelendpunkt (am nächsten zu Endpunkt 1) enthält die IP-Adresse Ihres Windows-Servers. Wenn es sich bei Ihrem Kunden-Gateway-Gerät um eine EC2 Instanz handelt, ist dies die private IP-Adresse der Instanz.
   - Remotetunnelendpunkt (am nächsten zu Endpunkt 2) enthält die IP-Adresse des Virtual Private Gateways für diesen Tunnel.
7. Öffnen Sie die Eigenschaften für Ihren zweiten Tunnel. Wiederholen Sie für diesen Tunnel die Schritte 4 bis 7.

### Master Key Perfect Forward Secrecy aktivieren

Sie können einen PFS-fähigen (Perfect Forward Secrecy) Master Key über die Befehlszeile aktivieren. Sie können diese Funktion nicht über die Benutzerschnittstelle aktivieren.

#### Aktivieren eines PFS-fähigen (Perfect Forward Secrecy) Master Keys

1. Öffnen Sie auf Ihrem Windows-Server ein neues Befehlszeilenfenster.
2. Geben Sie den folgenden Befehl ein und ersetzen Sie `rule_name` durch den Namen, den Sie der ersten Verbindungsregel gegeben haben.

   ```
   netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
    QMSecMethods=ESP:SHA1-AES128+60min+100000kb
   ```
3. Wiederholen Sie Schritt zwei für den zweiten Tunnel und ersetzen Sie dieses Mal `rule_name` durch den Namen, den Sie der zweiten Verbindungsregel gegeben haben.

### Konfigurieren der Windows-Firewall

Nachdem Sie Ihre Sicherheitsregeln auf Ihrem Server eingerichtet haben, konfigurieren Sie einige IPsec Grundeinstellungen für die Verwendung mit dem Virtual Private Gateway.

So konfigurieren Sie die Windows-Firewall

1. Öffnen Sie den Server-Manager, wählen Sie Tools aus, dann Windows Defender Firewall mit erweiterter Sicherheit und anschließend Eigenschaften.
2. Vergewissern Sie sich, dass auf der Registerkarte IPsec Einstellungen unter IPsecAusnahmen die Option ICMP ausschließen von auf Nein (Standardeinstellung) gesetzt IPsec ist. Stellen Sie sicher, dass die IPsec Tunnelautorisierung auf Keine gesetzt ist.
3. Wählen Sie unter IPsec Standardeinstellungen die Option Anpassen aus.
4. Wählen Sie unter Schlüsselaustausch (Hauptmodus) die Option Erweitert aus und dann Anpassen.
5. Bestätigen Sie unter Customize Advanced Key Exchange Settings (Erweiterte Schlüsselaustauscheinstellungen anpassen) unter Security methods (Sicherheitsmethoden), dass diese Standardwerte für den ersten Eintrag verwendet werden.

   - Integrität: SHA-1
   - Verschlüsselung: AES-CBC 128
   - Schlüsselaustauschalgorithmus: Diffie-Hellman Gruppe 2
   - Überprüfen Sie unter Schlüsselgültigkeitsdauer, ob für Minuten `480` und für Sitzungen `0` ausgewählt ist.

   Diese Einstellungen entsprechen den folgenden Einträgen in der Konfigurationsdatei.

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. Wählen Sie unter Schlüsselaustauschoptionen Diffie-Hellman für verstärkte Sicherheit verwenden aus und anschließend OK.
7. Wählen Sie unter Datenschutz (Schnellmodus) Erweitert aus und dann Anpassen.
8. Wählen Sie Verschlüsselung für alle Verbindungssicherheitsregeln erforderlich, die diese Einstellungen verwenden aus.
9. Übernehmen Sie unter Datenintegritäts- und Verschlüsselungsalgorithmen die Standardwerte:

   - Protokoll: ESP
   - Integrität: SHA-1
   - Verschlüsselung: AES-CBC 128

- Gültigkeitsdauer: 60 Minuten

Diese Werte entsprechen dem folgenden Eintrag in der Konfigurationsdatei.

```
QuickModeSecMethods:
ESP:SHA1-AES128+60min+100000kb
```

10. Wählen Sie OK, um zum Dialogfeld „IPsec Einstellungen anpassen“ zurückzukehren, und klicken Sie erneut auf OK, um die Konfiguration zu speichern.

## Schritt 5: Aktivieren von Dead Gateway Detection

Konfigurieren Sie als Nächstes TCP, sodass erkannt wird, wenn ein Gateway nicht mehr verfügbar ist. Dafür müssen Sie diesen Registrierungsschlüssel ändern: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. Tun Sie dies erst, wenn Sie die vorherigen Schritte abgeschlossen haben. Nach dem Ändern des Registrierungsschlüssels müssen Sie den Server neu starten.

So aktivieren Sie Dead Gateway Detection

1. Starten Sie auf Ihrem Windows Server die Befehlszeile oder eine PowerShell Sitzung und geben Sie regedit ein, um den Registrierungseditor zu starten.
2. Erweitern Sie HKEY_LOCAL_MACHINE, erweitern Sie SYSTEM, erweitern Sie, erweitern Sie Dienste CurrentControlSet, erweitern Sie Tcpip und erweitern Sie dann Parameter.
3. Wählen Sie aus dem Menü Bearbeiten die Option Neu und anschließend DWORD-Wert (32-Bit).
4. Geben Sie den Namen EnableDeadGWDetect ein.
5. Wählen Sie und wählen Sie Bearbeiten, Ändern. EnableDeadGWDetect
6. Geben Sie unter Value data 1 ein und wählen Sie dann OK aus.
7. Schließen Sie den Registrierungseditor und starten Sie den Server neu.

Weitere Informationen finden Sie EnableDeadGWDetectin der TechNetMicrosoft-Bibliothek.

## Schritt 6: Testen der VPN-Verbindung

Um die korrekte Funktionsweise der VPN-Verbindung zu testen, starten Sie eine Instance in Ihrer VPC und stellen Sie sicher, dass diese über keine Internetverbindung verfügt. Senden Sie nach

dem Starten der Instance von Ihrem Windows-Server aus einen Ping an die private IP-Adresse der Instance. Der VPN-Tunnel wird aufgebaut, wenn Datenverkehr vom Kunden-Gateway-Gerät generiert wird. Daher initiiert der Ping-Befehl auch die VPN-Verbindung.

Schritte zum Testen der VPN-Verbindung finden Sie unter Eine AWS Site-to-Site VPN Verbindung testen.

Wenn der Befehl `ping` fehlschlägt, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass die Sicherheitsgruppenregeln so konfiguriert sind, dass ICMP-Datenverkehr zur Instance in Ihrer VPC zulässig ist. Wenn es sich bei Ihrem Windows Server um eine EC2 Instanz handelt, stellen Sie sicher, dass die Regeln der Sicherheitsgruppe für ausgehenden IPsec Datenverkehr zulassen. Weitere Informationen finden Sie unter Konfigurieren der Windows-Instance.
- Stellen Sie sicher, dass das Betriebssystem der Instance, an die Sie den Ping senden, so konfiguriert ist, dass eine Antwort auf ICMP-Datenverkehr gesendet wird. Wir empfehlen Ihnen, eines der Amazon Linux-Betriebssysteme zu verwenden AMIs.
- Wenn es sich bei der Instance, die Sie pingen, um eine Windows-Instance handelt, stellen Sie eine Verbindung zu der Instance her und aktivieren Sie Inbound ICMPv4 auf der Windows-Firewall.
- Stellen Sie sicher, dass die Routing-Tabellen für Ihre VPC oder Ihr Subnetz korrekt konfiguriert sind. Weitere Informationen finden Sie unter Schritt 1: Erstellen einer VPN-Verbindung und Konfigurieren Ihrer VPC.
- Wenn es sich bei Ihrem Kunden-Gateway-Gerät um eine EC2 Instance handelt, stellen Sie sicher, dass Sie die Quell- und Zielüberprüfung für die Instance deaktiviert haben. Weitere Informationen finden Sie unter Konfigurieren der Windows-Instance.

Wählen Sie in der Amazon-VPC-Konsole auf der Seite VPN Connections die VPN-Verbindung aus. Der erste Tunnel hat den Zustand UP. Der zweite Tunnel muss konfiguriert sein, wird jedoch nur dann aktiv, wenn der erste Tunnel ausfällt. Es kann einige Momente dauern, die verschlüsselten Tunnel zu aktivieren.

## Fehlerbehebung AWS Site-to-Site VPN beim Kunden-Gateway-Gerät

Bei der Behebung von Problemen mit Ihrem Kunden-Gateway-Gerät ist ein strukturierter Ansatz wichtig. Die ersten beiden Themen in diesem Abschnitt enthalten allgemeine Flussdiagramme

zur Behebung von Problemen, wenn ein für dynamisches Routing konfiguriertes Gerät (BGP aktiviert) bzw. ein für statisches Routing konfiguriertes Gerät (ohne BGP aktiviert) verwendet wird. Im Anschluss an diese Themen finden Sie gerätespezifische Anleitungen zur Fehlerbehebung für Kunden-Gateway-Geräte von Cisco, Juniper und Yamaha.

Zusätzlich zu den Themen in diesem Abschnitt AWS Site-to-Site VPN Logs kann die Aktivierung bei der Fehlerbehebung und Behebung von VPN-Verbindungsproblemen sehr hilfreich sein. Allgemeine Testanweisungen finden Sie auch unterEine AWS Site-to-Site VPN Verbindung testen.

Themen

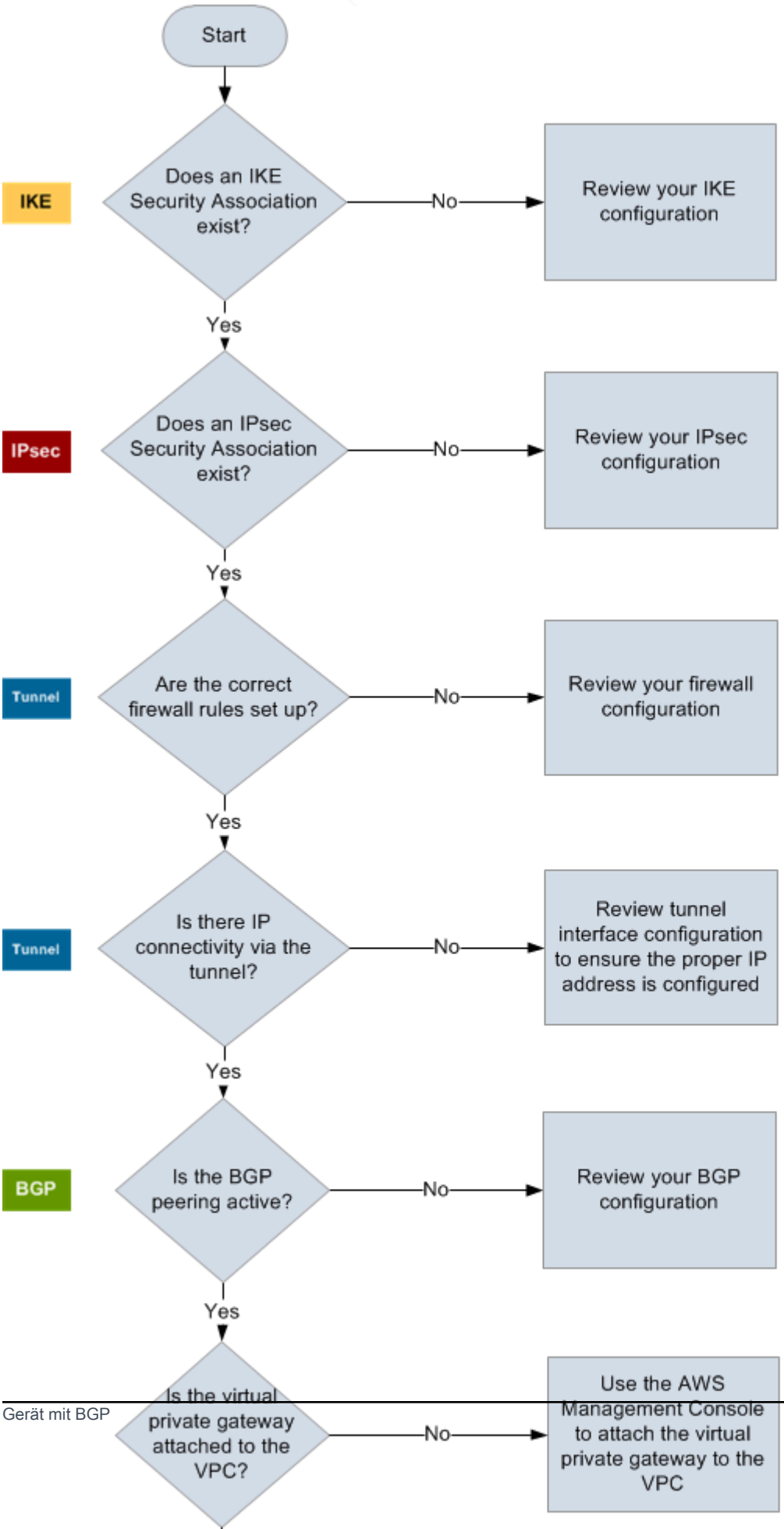

- Beheben Sie AWS Site-to-Site VPN Verbindungsprobleme bei der Verwendung des Border Gateway Protocol
- Beheben Sie AWS Site-to-Site VPN Verbindungsprobleme ohne Border Gateway Protocol
- Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco ASA-Kunden-Gateway-Gerät
- Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco IOS-Kunden-Gateway-Gerät
- Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco IOS-Kunden-Gateway-Gerät ohne Border Gateway Protocol
- Fehlerbehebung bei der AWS Site-to-Site VPN Konnektivität mit einem Juniper JunOS-Kunden-Gateway-Gerät
- Fehlerbehebung bei der AWS Site-to-Site VPN Konnektivität mit einem Juniper ScreenOS-Kunden-Gateway-Gerät
- Beheben Sie Probleme mit der AWS Site-to-Site VPN Konnektivität mit einem Yamaha-Kunden-Gateway-Gerät


Weitere Ressourcen

- Amazon VPC-Forum

## Beheben Sie AWS Site-to-Site VPN Verbindungsprobleme bei der Verwendung des Border Gateway Protocol

Die nachfolgende Abbildung und Tabelle enthalten allgemeine Anweisungen zur Fehlersuche bei Kunden-Gateway-Geräten ohne Border Gateway Protocol (BGP). Wir empfehlen Ihnen auch, die Debug-Funktionen Ihres Geräts zu aktivieren. Weitere Informationen erhalten Sie vom Anbieter Ihres Gateway-Geräts.

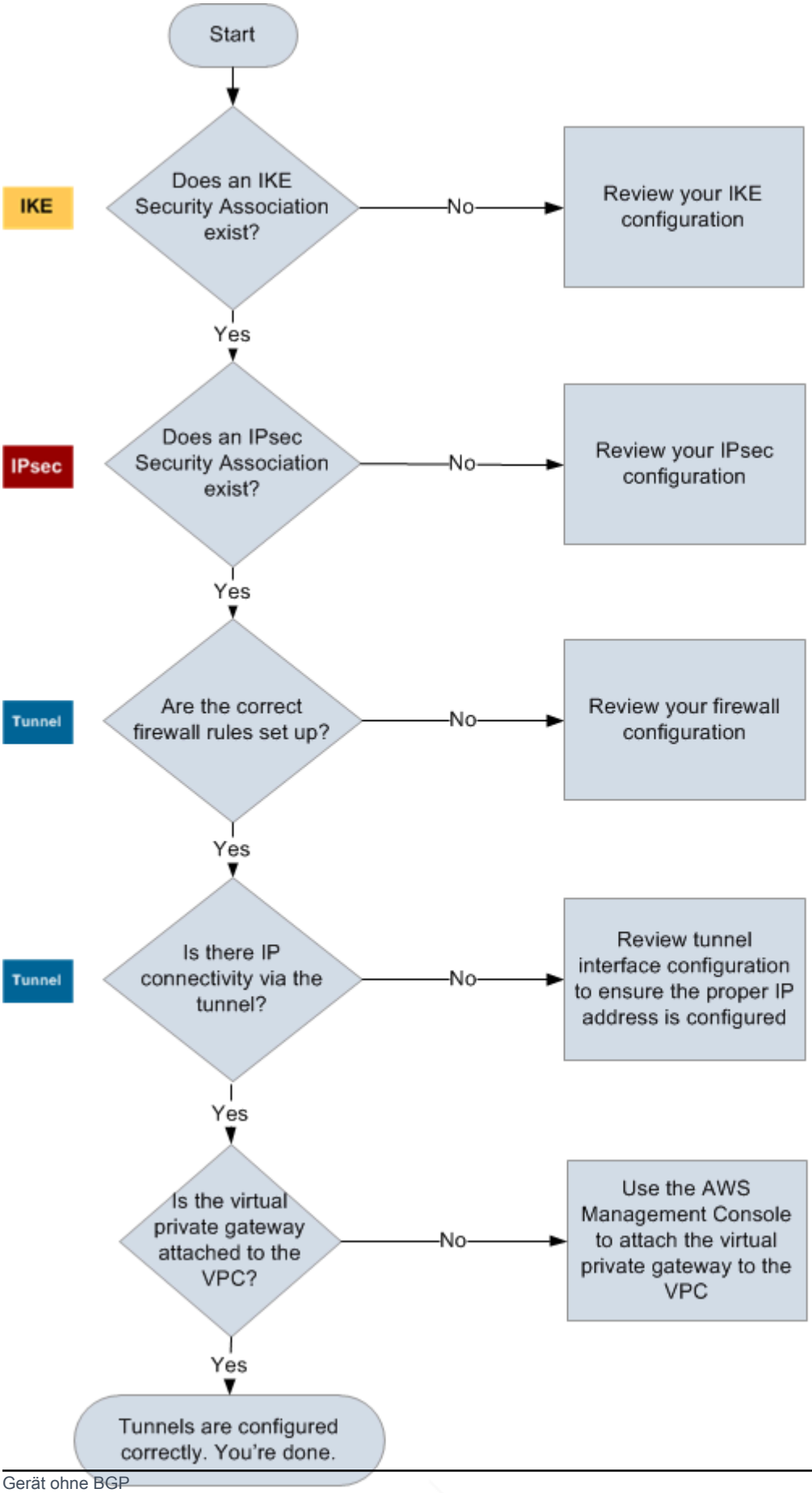

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

| | |
|---|---|
| IKE | Überprüfen Sie, ob eine IKE Sicherheitsaushandlung vorhanden ist.<br><br>Für den Austausch von Schlüsseln, die zur Einrichtung der Sicherheitsverbindung verwendet werden, ist eine IPsec IKE-Sicherheitsverbindung erforderlich.<br><br>Wenn keine IKE Security Association vorhanden ist, überprüfen Sie Ihre IKE-Konfi gurationseinstellungen. Sie müssen die Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modusparameter entsprechend der Konfigurationsdatei konfigurieren.<br><br>Wenn eine IKE-Sicherheitsverbindung vorhanden ist, fahren Sie mit 'IPsec' fort. |
| IPsec | Ermitteln Sie, ob eine IPsec Sicherheitsverbindung (SA) vorhanden ist.<br><br>Eine IPsec SA ist der Tunnel selbst. Fragen Sie Ihr Kunden-Gateway-Gerät ab, um festzustellen, ob eine IPsec SA aktiv ist. Stellen Sie sicher, dass Sie die in der Konfigurationsdatei aufgeführten Parameter für Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modus konfigurieren.<br><br>Wenn keine IPsec SA vorhanden ist, überprüfen Sie Ihre IPsec Konfiguration.<br><br>Wenn eine IPsec SA vorhanden ist, fahren Sie mit „Tunnel“ fort. |
| Tunnel | Stellen Sie sicher, dass die erforderlichen Firewall-Regeln eingerichtet sind. Eine Liste der Regeln finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät. Wenn die Regeln korrekt eingerichtet sind, fahren Sie fort.<br><br>Stellen Sie fest, ob eine IP-Konnektivität durch den Tunnel besteht.<br><br>Jede Seite des Tunnels hat eine IP-Adresse, wie in der Konfigurationsdatei angegeben. Die IP-Adresse des Virtual Private Gateways ist die Adresse des BGP-Nachbarn. Senden Sie von Ihrem Kunden-Gateway-Gerät aus einen Ping an diese Adresse, um zu überprüfen, ob IP-Datenverkehr korrekt verschlüsselt und entschlüs selt wird.<br><br>Sollte dies fehlschlagen, überprüfen Sie die Konfiguration der Tunnelschnittstelle, um sicherzustellen, dass die korrekte IP-Adresse konfiguriert ist.<br><br>Wenn der Ping erfolgreich war, fahren Sie mit "BGP" fort. |

| | |
|---|---|
| BGP | Bestimmen Sie, ob die BGP-Peering-Sitzung aktiv ist.<br><br>Gehen Sie für jeden Tunnel wie folgt vor:<br><br>• Überprüfen Sie auf Ihrem Kunden-Gateway-Gerät, ob der BGP-Status `Active` oder `Established` lautet. Es kann etwa 30 Sekunden dauern, bis BGP Peering aktiviert wird.<br>• Überprüfen Sie, ob das Kunden-Gateway-Gerät die Standardroute (0.0.0.0/0) an das Virtual Private Gateway sendet.<br><br>Wenn die Tunnel einen anderen Zustand aufweisen, überprüfen Sie die BGP-Konfiguration.<br><br>Wenn BGP Peering korrekt eingerichtet wurde, Sie ein Präfix empfangen und auch eines senden, ist der Tunnel korrekt konfiguriert. Stellen Sie sicher, dass beide Tunnel diesen Zustand aufweisen. |

## Beheben Sie AWS Site-to-Site VPN Verbindungsprobleme ohne Border Gateway Protocol

Die nachfolgende Abbildung und Tabelle enthalten allgemeine Anweisungen zur Fehlersuche bei Kunden-Gateway-Geräten ohne Border Gateway Protocol (BGP). Wir empfehlen Ihnen auch, die Debug-Funktionen Ihres Geräts zu aktivieren. Weitere Informationen erhalten Sie vom Anbieter Ihres Gateway-Geräts.


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

| | |
|---|---|
| IKE | Überprüfen Sie, ob eine IKE Sicherheitsaushandlung vorhanden ist.<br><br>Für den Austausch von Schlüsseln, die zur Einrichtung der Sicherheitsverbindung verwendet werden, ist eine IPsec IKE-Sicherheitsverbindung erforderlich.<br><br>Wenn keine IKE Security Association vorhanden ist, überprüfen Sie Ihre IKE-Konfi gurationseinstellungen. Sie müssen die Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modusparameter entsprechend der Konfigurationsdatei konfigurieren.<br><br>Wenn eine IKE-Sicherheitsverbindung vorhanden ist, fahren Sie mit 'IPsec' fort. |
| IPsec | Ermitteln Sie, ob eine IPsec Sicherheitsverbindung (SA) vorhanden ist.<br><br>Eine IPsec SA ist der Tunnel selbst. Fragen Sie Ihr Kunden-Gateway-Gerät ab, um festzustellen, ob eine IPsec SA aktiv ist. Stellen Sie sicher, dass Sie die in der Konfigurationsdatei aufgeführten Parameter für Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modus konfigurieren.<br><br>Wenn keine IPsec SA vorhanden ist, überprüfen Sie Ihre IPsec Konfiguration.<br><br>Wenn eine IPsec SA vorhanden ist, fahren Sie mit „Tunnel“ fort. |
| Tunnel | Stellen Sie sicher, dass die erforderlichen Firewall-Regeln eingerichtet sind. Eine Liste der Regeln finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät. Wenn die Regeln korrekt eingerichtet sind, fahren Sie fort.<br><br>Stellen Sie fest, ob eine IP-Konnektivität durch den Tunnel besteht.<br><br>Jede Seite des Tunnels hat eine IP-Adresse, wie in der Konfigurationsdatei angegeben. Die IP-Adresse des Virtual Private Gateways ist die Adresse des BGP-Nachbarn. Senden Sie von Ihrem Kunden-Gateway-Gerät aus einen Ping an diese Adresse, um zu überprüfen, ob IP-Datenverkehr korrekt verschlüsselt und entschlüs selt wird.<br><br>Sollte dies fehlschlagen, überprüfen Sie die Konfiguration der Tunnelschnittstelle, um sicherzustellen, dass die korrekte IP-Adresse konfiguriert ist.<br><br>Wenn der Ping erfolgreich ist, fahren Sie mit "Statische Routen" fort. |

| | |
|---|---|
| Statische Routen | Gehen Sie für jeden Tunnel wie folgt vor:<br>• Stellen Sie sicher, dass Sie eine statische Route für das CIDR Ihrer VPC mit den Tunneln als nächstem Punkt eingerichtet haben.<br>• Vergewissern Sie sich, dass Sie eine statische Route in der Amazon VPC-Konsole hinzugefügt haben, um den Virtual Private Gateway anzuweisen, den Datenverkehr zurück zu Ihren internen Netzwerken zu routen.<br><br>Wenn die Tunnel einen anderen Zustand aufweisen, überprüfen Sie die Gerätekonfiguration.<br><br>Stellen Sie sicher, dass beide Tunnel diesen Zustand aufweisen. |

## Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco ASA-Kunden-Gateway-Gerät

Wenn Sie Probleme mit der Konnektivität eines Cisco Kunden-Gateway-Geräts beheben, sollten Sie IKE IPsec, und Routing in Betracht ziehen. Sie können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

> **Important**
>
> Einige Cisco unterstützen ASAs nur Active/Standby den Modus. Wenn Sie diese Cisco verwenden ASAs, können Sie jeweils nur einen aktiven Tunnel haben. Der andere Standby-Tunnel wird nur dann aktiv, wenn der erste Tunnel nicht verfügbar ist. Der Standby-Tunnel kann in Protokolldateien folgende Fehlermeldung verursachen: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`. Diese können Sie ignorieren.

### IKE

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
ciscoasa# show crypto isakmp sa
```

```

   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Es sollte mindestens eine Zeile mit einem `src`-Wert für das in den Tunneln angegebene Remote-Gateway angezeigt werden. Der `state`-Wert sollte `MM_ACTIVE` und `status` sollte `ACTIVE` lauten. Wenn kein Eintrag vorhanden ist oder ein anderer Zustand angezeigt wird, ist IKE nicht korrekt konfiguriert.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, führen Sie die folgenden Befehle aus, um Protokollmeldungen mit Diagnoseinformationen zu aktivieren.

```
router# term mon
router# debug crypto isakmp
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto isakmp
```

## IPsec

Verwenden Sie den folgenden -Befehl. In der Antwort wird ein Kunden-Gateway-Gerät angezeigt, das korrekt IPsec konfiguriert ist.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
```

```
      current_peer: integ-ppe1

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

Sie sollten für jede Tunnelschnittstelle sowohl `inbound esp sas` als auch `outbound esp sas` sehen. Dabei wird vorausgesetzt, dass eine SA aufgeführt ist (z. B.`spi: 0x48B456A6`) und dass diese korrekt konfiguriert IPsec ist.

In Cisco ASA wird der IPsec erst angezeigt, nachdem interessanter Datenverkehr (Datenverkehr, der verschlüsselt werden sollte) gesendet wurde. Um stets IPsec aktiv zu bleiben, empfehlen wir die

Konfiguration eines SLA-Monitors. Der SLA-Monitor sendet weiterhin interessanten Datenverkehr, wobei der IPsec Benutzer aktiv bleibt.

Sie können auch den folgenden Ping-Befehl verwenden, um Sie zu zwingen, mit der Verhandlung IPsec zu beginnen und dann nach oben zu gehen.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Aktivieren Sie zur weiteren Problembehebung mit dem folgenden Befehl Debugging.

```
router# debug crypto ipsec
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto ipsec
```

## Routing

Senden Sie einen Ping ans andere Ende des Tunnels. Wenn das funktioniert, IPsec sollten Sie etabliert sein. Wenn das nicht funktioniert, überprüfen Sie Ihre Zugriffslisten und lesen Sie den vorherigen IPsec Abschnitt.

Wenn Sie nicht in der Lage sind, Ihre Instances zu erreichen, überprüfen Sie die folgenden Informationen.

1. Stellen Sie sicher, dass die Zugriffsliste so konfiguriert ist, dass der Crypto-Map zugeordneter Datenverkehr zugelassen wird.

   Führen Sie dazu den folgenden Befehl aus.

```
ciscoasa# show run crypto
```

```
crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
crypto map VPN_crypto_map_name 1 match address access-list-name
crypto map VPN_crypto_map_name 1 set pfs
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Überprüfen Sie die Zugriffsliste mit dem folgenden Befehl.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Vergewissern Sie sich, dass die Zugriffsliste korrekt ist. Die folgende Beispielzugriffsliste erlaubt den gesamten internen Datenverkehr zum VPC-Subnetz 10.0.0.0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Führen Sie eine Traceroute vom Cisco ASA-Gerät aus, um zu sehen, ob sie die Amazon-Router erreicht (z. B.*AWS_ENDPOINT_1*/). *AWS_ENDPOINT_2*

   Ist dies der Fall, überprüfen Sie nun die statischen Routen, die Sie in der Amazon VPC-Konsole hinzugefügt haben, sowie die Sicherheitsgruppen der betroffenen Instances.

5. Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## Lassen Sie die Tunnelschnittstelle abprallen

Wenn der Tunnel in Betrieb zu sein scheint, der Verkehr aber nicht richtig fließt, können Verbindungsprobleme häufig durch Bouncing (Deaktivierung und erneutes Aktivieren) der Tunnelschnittstelle behoben werden. So schalten Sie die Tunnelschnittstelle auf einer Cisco ASA ab:

1. Führen Sie Folgendes aus:

```
ciscoasa# conf t
ciscoasa(config)# interface tunnel X  (where X is your tunnel ID)
ciscoasa(config-if)# shutdown
```

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# end
```

Alternativ können Sie einen einzeiligen Befehl verwenden:

```
ciscoasa# conf t ; interface tunnel X ; shutdown ; no shutdown ; end
```

2. Überprüfen Sie nach dem Abrufen der Schnittstelle, ob die VPN-Verbindung wieder hergestellt wurde und ob der Datenverkehr jetzt korrekt fließt.

## Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco IOS-Kunden-Gateway-Gerät

Wenn Sie Probleme mit der Konnektivität eines Cisco Kunden-Gateway-Geräts beheben, sollten Sie vier Dinge berücksichtigen: IKE IPsec, Tunnel und BGP. Sie können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

### IKE

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

Es sollte mindestens eine Zeile mit einem `src`-Wert für das in den Tunneln angegebene Remote-Gateway angezeigt werden. Der `state` sollte `QM_IDLE` und der `status` sollte `ACTIVE` lauten. Wenn kein Eintrag vorhanden ist oder ein anderer Zustand angezeigt wird, ist IKE nicht korrekt konfiguriert.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, führen Sie die folgenden Befehle aus, um Protokollmeldungen mit Diagnoseinformationen zu aktivieren.

```
router# term mon
```

```
router# debug crypto isakmp
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto isakmp
```

## IPsec

Verwenden Sie den folgenden -Befehl. In der Antwort wird ein Kunden-Gateway-Gerät angezeigt, das korrekt IPsec konfiguriert ist.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE
```

```
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xF59A3FF6(4120526838)

     inbound esp sas:
      spi: 0xB6720137(3060924727)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
```

```
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xF59A3FF6(4120526838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
```

Sie sollten für jede Tunnelschnittstelle sowohl `inbound esp sas` als auch `outbound esp sas` sehen. Angenommen`spi: 0xF95D2F3C`, eine SA ist aufgeführt (zum Beispiel) und `ACTIVE` diese `Status` IPsec ist korrekt konfiguriert.

Aktivieren Sie zur weiteren Problembehebung mit dem folgenden Befehl Debugging.

```
router# debug crypto ipsec
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto ipsec
```

## Tunnel

Überprüfen Sie zunächst, ob die benötigten Firewall-Regeln konfiguriert sind. Weitere Informationen finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Wenn die Firewall-Regeln korrekt eingerichtet sind, können Sie mithilfe des folgenden Befehls mit der Fehlersuche fortfahren.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Stellen Sie sicher, dass das `line protocol` eingerichtet ist. Überprüfen Sie, ob die Quell-IP-Adresse, die Quellschnittstelle und der Zielbereich des Tunnels mit der Tunnelkonfiguration für die externe IP-Adresse des Kunden-Gateway-Geräts, die Schnittstelle und die externe IP-Adresse des Virtual Private Gateways übereinstimmen. Stellen Sie sicher, dass `Tunnel protection via IPSec` aktiviert ist. Führen Sie den Befehl für beiden Tunnelschnittstellen aus. Um etwaige Probleme zu beheben, prüfen Sie die Konfiguration sowie die physischen Verbindungen zum Kunden-Gateway-Gerät.

Führen Sie auch den folgenden Befehl aus und ersetzen Sie dabei `169.254.255.1` durch die interne IP-Adresse des Virtual Private Gateways.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
```

```
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Es sollten fünf Ausrufezeichen angezeigt werden.

Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## BGP

Verwenden Sie den folgenden -Befehl.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

Hier sollten beide Nachbarn aufgeführt sein. Für jeden davon sollte der `State/PfxRcd`-Wert 1 betragen.

Wenn BGP-Peering aktiviert ist, überprüfen Sie, ob Ihr Kunden-Gateway-Gerät die Standardroute (0.0.0.0/0) an die VPC sendet.

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

Stellen Sie außerdem sicher, dass Sie das Präfix Ihrer VPC vom Virtual Private Gateway empfangen.

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## Beheben Sie die AWS Site-to-Site VPN Konnektivität mit einem Cisco IOS-Kunden-Gateway-Gerät ohne Border Gateway Protocol

Wenn Sie Probleme mit der Konnektivität eines Cisco Kunden-Gateway-Geräts beheben, sollten Sie drei Dinge berücksichtigen: IKE und Tunnel. IPsec Sie können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

### IKE

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

Es sollte mindestens eine Zeile mit einem `src`-Wert für das in den Tunneln angegebene Remote-Gateway angezeigt werden. Der `state` sollte `QM_IDLE` und der `status` sollte `ACTIVE` lauten. Wenn kein Eintrag vorhanden ist oder ein anderer Zustand angezeigt wird, ist IKE nicht korrekt konfiguriert.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, führen Sie die folgenden Befehle aus, um Protokollmeldungen mit Diagnoseinformationen zu aktivieren.

```
router# term mon
router# debug crypto isakmp
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto isakmp
```

## IPsec

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt, dass ein Kunden-Gateway-Gerät korrekt IPsec konfiguriert ist.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
```

```
       spi: 0x6ADB173(112046451)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
```

```
    current outbound spi: 0xF59A3FF6(4120526838)

    inbound esp sas:
     spi: 0xB6720137(3060924727)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

Sie sollten für jede Tunnelschnittstelle sowohl eine eingehende `esp sas` als auch eine ausgehende `esp sas` sehen. Dabei wird vorausgesetzt, dass eine SA aufgeführt ist (z. B.`spi: 0x48B456A6`), dass der Status lautet `ACTIVE` und dass diese korrekt konfiguriert IPsec ist.

Aktivieren Sie zur weiteren Problembehebung mit dem folgenden Befehl Debugging.

```
router# debug crypto ipsec
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
router# no debug crypto ipsec
```

## Tunnel

Überprüfen Sie zunächst, ob die benötigten Firewall-Regeln konfiguriert sind. Weitere Informationen finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Wenn die Firewall-Regeln korrekt eingerichtet sind, können Sie mithilfe des folgenden Befehls mit der Fehlersuche fortfahren.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Stellen Sie sicher, dass das Leitungsprotokoll eingerichtet ist. Überprüfen Sie, ob die Quell-IP-Adresse, die Quellschnittstelle und der Zielbereich des Tunnels mit der Tunnelkonfiguration für die externe IP-Adresse des Kunden-Gateway-Geräts, die Schnittstelle und die externe IP-Adresse des Virtual Private Gateways übereinstimmen. Stellen Sie sicher, dass `Tunnel protection through IPSec` aktiviert ist. Führen Sie den Befehl für beiden Tunnelschnittstellen aus. Um etwaige Probleme zu beheben, prüfen Sie die Konfiguration sowie die physischen Verbindungen zum Kunden-Gateway-Gerät.

Sie können auch den folgenden Befehl ausführen; ersetzen Sie dabei `169.254.249.18` durch die interne IP-Adresse des Virtual Private Gateways.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Es sollten fünf Ausrufezeichen angezeigt werden.

Routing

Führen Sie den folgenden Befehl aus, um die statische Routing-Tabelle anzuzeigen.

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Die statische Route sollte für VPC CIDR durch beide Tunnel vorhanden sein. Wenn sie nicht vorhanden ist, fügen Sie die statischen Routen wie folgt hinzu.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Überprüfen der SLA-Überwachung

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
```

```
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

Der Wert für `Number of successes` gibt an, ob der SLA-Monitor erfolgreich eingerichtet wurde.

Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## Fehlerbehebung bei der AWS Site-to-Site VPN Konnektivität mit einem Juniper JunOS-Kunden-Gateway-Gerät

Wenn Sie Probleme mit der Konnektivität eines Kunden-Gateway-Geräts von Juniper beheben, sollten Sie vier Dinge berücksichtigen: IKE IPsec, Tunnel und BGP. Sie können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

### IKE

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

Es sollte mindestens eine Zeile mit einer Remote-Adresse des in den Tunneln angegebenen Remote-Gateways angezeigt werden. Der `State` sollte `UP` sein. Wenn kein Eintrag vorhanden ist oder ein anderer Zustand (z. B. `DOWN`) angezeigt wird, ist IKE nicht korrekt konfiguriert.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, aktivieren Sie die IKE-Trace-Optionen (wie in den Beispielkonfigurationsinformationen empfohlen). Führen Sie dann den folgenden Befehl aus, um verschiedene Debugging-Meldungen auf dem Bildschirm auszugeben.

```
user@router> monitor start kmd
```

Mit dem folgenden Befehl können Sie die gesamte Protokolldatei von einem externen Host abrufen.

```
scp username@router.hostname:/var/log/kmd
```

## IPsec

Verwenden Sie den folgenden -Befehl. In der Antwort wird ein Kunden-Gateway-Gerät angezeigt, das korrekt IPsec konfiguriert ist.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway        Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

Sie sollten mindestens zwei Zeilen pro Gateway-Adresse (entsprechend dem Remote-Gateway) sehen. Beachten Sie die Einfügezeichen am Beginn jeder Zeile (**< >**), die die Richtung des Datenverkehrs für den jeweiligen Eintrag angeben. Für die Ausgabe gibt es eigene Zeilen für eingehenden Datenverkehr ("**<**", Datenverkehr vom Virtual Private Gateway zu diesem Kunden-Gateway) und ausgehenden Datenverkehr ("**>**").

Wenn Sie weitere Informationen zur Fehlersuche benötigen, aktivieren Sie die IKE-Trace-Optionen (weitere Informationen finden Sie im vorherigen Abschnitt zu IKE).

## Tunnel

Überprüfen Sie zunächst noch einmal, ob die benötigten Firewall-Regeln konfiguriert sind. Eine Liste der Regeln finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Wenn die Firewall-Regeln korrekt eingerichtet sind, können Sie mithilfe des folgenden Befehls mit der Fehlersuche fortfahren.

```
user@router> show interfaces st0.1
```

```
 Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
    Input packets : 8719
    Output packets: 41841
    Security: Zone: Trust
    Allowed host-inbound traffic : bgp ping ssh traceroute
    Protocol inet, MTU: 9192
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
      Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Stellen Sie sicher, dass `Security: Zone` korrekt konfiguriert ist und die Adresse `Local` mit der internen Adresse des Kunden-Gateway-Geräte-Tunnels übereinstimmt.

Führen Sie nun den folgenden Befehl aus und ersetzen Sie dabei `169.254.255.1` durch die interne IP-Adresse des Virtual Private Gateways. Ihre Ergebnisse sollten etwa wie folgt aussehen.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## BGP

Führen Sie den folgenden Befehl aus.

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

Führen Sie zur weiteren Fehlersuche den folgenden Befehl aus; ersetzen Sie dabei `169.254.255.1` durch die interne IP-Adresse des Virtual Private Gateways.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
```

```
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

Hier sollten `Received prefixes` und `Advertised prefixes` beide mit "1" aufgelistet sein. Diese Werte befinden sich im Abschnitt `Table inet.0`.

Wenn `State` nicht `Established` ist, finden Sie unter `Last State` und `Last Error` detaillierte Informationen zur Fehlerbehebung.

Wenn BGP-Peering aktiviert ist, überprüfen Sie, ob Ihr Kunden-Gateway-Gerät die Standardroute (0.0.0.0/0) an die VPC sendet.

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

Stellen Sie außerdem sicher, dass Sie das Präfix Ihrer VPC vom Virtual Private Gateway empfangen.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

## Fehlerbehebung bei der AWS Site-to-Site VPN Konnektivität mit einem Juniper ScreenOS-Kunden-Gateway-Gerät

Wenn Sie Probleme mit der Konnektivität eines auf Juniper ScreenOS basierenden Kunden-Gateway-Geräts beheben, sollten Sie vier Dinge berücksichtigen: IKE IPsec, Tunnel und BGP. Sie

können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

## IKE und IPsec

Verwenden Sie den folgenden -Befehl. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

Es sollte mindestens eine Zeile mit einer Remote-Adresse des in den Tunneln angegebenen Remote-Gateways angezeigt werden. Der Wert `Sta` sollte `A/-` sein und unter `SPI` sollte eine andere hexadezimale Zahl als `00000000` angezeigt werden. Wenn die Einträge davon abweichen, ist IKE nicht korrekt konfiguriert.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, aktivieren Sie die IKE-Trace-Optionen (wie in den Beispielkonfigurationsinformationen empfohlen).

## Tunnel

Überprüfen Sie zunächst noch einmal, ob die benötigten Firewall-Regeln konfiguriert sind. Eine Liste der Regeln finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Wenn die Firewall-Regeln korrekt eingerichtet sind, können Sie mithilfe des folgenden Befehls mit der Fehlersuche fortfahren.

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
```

```
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Stellen Sie sicher, dass `link:ready` angezeigt wird und die `IP`-Adresse mit der internen Adresse des Kunden-Gateway-Geräte-Tunnels übereinstimmt.

Führen Sie nun den folgenden Befehl aus und ersetzen Sie dabei `169.254.255.1` durch die interne IP-Adresse des Virtual Private Gateways. Ihre Ergebnisse sollten etwa wie folgt aussehen.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Fahren Sie mit der Fehlersuche in der Konfiguration fort.

## BGP

Führen Sie den folgenden Befehl aus.

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
--------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

Der Status der beiden BGP-Peers sollte `ESTABLISH` sein, was bedeutet, dass die BGP-Verbindung zum Virtual Private Gateway aktiv ist.

Führen Sie zur weiteren Fehlersuche den folgenden Befehl aus; ersetzen Sie dabei `169.254.255.1` durch die interne IP-Adresse des Virtual Private Gateways.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
```

```
Elapsed time since last update: 2 minutes 6 seconds
```

Wenn BGP-Peering aktiviert ist, überprüfen Sie, ob Ihr Kunden-Gateway-Gerät die Standardroute (0.0.0.0/0) an die VPC sendet. Dieser Befehl ist ab ScreenOS 6.2.0 anwendbar.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

Stellen Sie außerdem sicher, dass Sie das Präfix Ihrer VPC vom Virtual Private Gateway empfangen. Dieser Befehl ist ab ScreenOS 6.2.0 anwendbar.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

## Beheben Sie Probleme mit der AWS Site-to-Site VPN Konnektivität mit einem Yamaha-Kunden-Gateway-Gerät

Wenn Sie Probleme mit der Konnektivität eines Yamaha-Kunden-Gateway-Geräts beheben, sollten Sie vier Dinge berücksichtigen: IKE IPsec, Tunnel und BGP. Sie können zwar in beliebiger Reihenfolge nach Fehlern in diesen drei Bereichen suchen, wir empfehlen jedoch, mit IKE (am Ende des Netzwerk-Stacks) zu beginnen und sich hochzuarbeiten.

> **Note**
>
> Die Einstellung für `proxy ID`, die in Phase 2 von IKE verwendet wurde, ist im Yamaha-Router standardmäßig deaktiviert. Dies kann zu Problemen bei der Verbindung mit dem Site-to-Site VPN führen. Wenn der auf Ihrem Router nicht konfiguriert `proxy ID` ist, sehen Sie

sich bitte die AWS mitgelieferte Beispielkonfigurationsdatei an, damit Yamaha sie richtig einstellt.

## IKE

Führen Sie den folgenden Befehl aus. Die Antwort zeigt ein Kunden-Gateway-Gerät mit korrekt konfiguriertem IKE.

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                      remote-id        # of sa
-----------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

Es sollte eine Zeile mit dem Wert `remote-id` für die in den Tunneln angegebene Remote-Gateway angezeigt werden. Sie können alle Sicherheitszuordnungen (SAs) auflisten, indem Sie die Tunnelnummer weglassen.

Wenn Sie weitere Informationen zur Fehlersuche benötigen, führen Sie die folgenden Befehle aus, um Protokollmeldungen auf DEBUG-Ebene mit Diagnoseinformationen zu aktivieren.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Um die protokollierten Elemente zu löschen, führen Sie den folgenden Befehl aus.

```
# no ipsec ike log
# no syslog debug on
```

## IPsec

Führen Sie den folgenden Befehl aus. In der Antwort wird ein Kunden-Gateway-Gerät angezeigt, das korrekt IPsec konfiguriert ist.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
```

```
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
----------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
----------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
----------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
----------------------------------------------------
```

Sie sollten für jede Tunnelschnittstelle sowohl `receive sas` als auch `send sas` sehen.

Aktivieren Sie zur weiteren Problembehebung mit dem folgenden Befehl Debugging.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Wenn Sie Debugging deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
# no ipsec ike log
# no syslog debug on
```

## Tunnel

Überprüfen Sie zunächst, ob die benötigten Firewall-Regeln konfiguriert sind. Eine Liste der Regeln finden Sie unter Firewall-Regeln für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Wenn die Firewall-Regeln korrekt eingerichtet sind, können Sie mithilfe des folgenden Befehls mit der Fehlersuche fortfahren.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Stellen Sie sicher, dass der `current status` Wert online ist und das auch so `Interface type` ist IPsec. Führen Sie den Befehl für beide Tunnelschnittstellen aus. Fehler, die hier auftreten, können Sie in der Konfiguration beheben.

## BGP

Führen Sie den folgenden Befehl aus.

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
```

```
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

Hier sollten beide Nachbarn aufgeführt sein. Für jeden davon sollte der BGP `state`-Wert `Active` betragen.

Wenn BGP-Peering aktiviert ist, überprüfen Sie, ob Ihr Kunden-Gateway-Gerät die Standardroute (0.0.0.0/0) an die VPC sendet.

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

Stellen Sie außerdem sicher, dass Sie das Präfix Ihrer VPC vom Virtual Private Gateway empfangen.

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

# Arbeite mit AWS Site-to-Site VPN

Sie können mit Site-to-Site VPN-Ressourcen über die Amazon VPC-Konsole oder die AWS CLI arbeiten.

Themen


- Einen AWS Site-to-Site VPN Anhang für AWS Cloud WAN erstellen
- Einen AWS Site-to-Site VPN Transit-Gateway-Anhang erstellen
- Eine AWS Site-to-Site VPN Verbindung testen
- Eine AWS Site-to-Site VPN Verbindung und ein Gateway löschen
- Ändern Sie das Ziel-Gateway einer AWS Site-to-Site VPN Verbindung
- AWS Site-to-Site VPN Verbindungsoptionen ändern
- AWS Site-to-Site VPN Tunneloptionen ändern
- Statische Routen für eine AWS Site-to-Site VPN Verbindung bearbeiten
- Das Kunden-Gateway für eine AWS Site-to-Site VPN Verbindung ändern
- Kompromittierte Anmeldeinformationen für eine AWS Site-to-Site VPN Verbindung ersetzen
- AWS Site-to-Site VPN Tunnelendpunkt-Zertifikate rotieren
- Private IP AWS Site-to-Site VPN mit AWS Direct Connect


## Einen AWS Site-to-Site VPN Anhang für AWS Cloud WAN erstellen

Gehen Sie wie folgt vor, um einen Site-to-Site VPN-Anhang für AWS Cloud WAN zu erstellen. Weitere Informationen zu VPN-Anhängen und Cloud WAN finden Sie unter Site-to-site VPN-Anlagen in AWS Cloud WAN im AWS Cloud WAN-Benutzerhandbuch.

Cloud-WAN-VPN-Anhänge unterstützen beide IPv4 IPv6 Protokolle. Weitere Informationen zur Verwendung eines dieser Protokolle für einen Cloud-WAN-VPN-Anhang finden Sie unter IPv4 und IPv6 Traffic in AWS Site-to-Site VPN.

So erstellen Sie mithilfe der Konsole einen VPN-Anhang für AWS Cloud WAN

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.

4. (Optional) Geben Sie als Name-Tag einen Namen für die Verbindung ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
5. Wählen Sie für Target gateway Type (Typ des Ziel-Gateways) die Option Not associated (Nicht zugeordnet) aus.
6. Wählen Sie bei Customer gateway (Kunden-Gateway) eine der folgenden Vorgehensweise:
   - Um ein vorhandenes Kunden-Gateway zu verwenden, wählen Sie Existing und dann die Kunden-Gateway-ID aus.
   - Um ein neues Kunden-Gateway zu erstellen, wählen Sie Neu.
     1. Geben Sie für die IP-Adresse eine statische Adresse IPv4oder eine IPv6Adresse ein.
     2. (Optional) Wählen Sie für Certificate ARN den ARN Ihres privaten Zertifikats aus (falls Sie die zertifikatsbasierte Authentifizierung verwenden).
     3. Geben Sie unter BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) Ihres Kunden-Gateways ein. Weitere Informationen finden Sie unter Kunden-Gateway-Optionen.
7. Wählen Sie für Routing-Optionen Dynamisch (erfordert BGP) oder Statisch.
8. Wählen Sie für Pre-Shared Key Storage entweder Standard oder Secrets Manager. Die Standardauswahl ist Standard. Weitere Informationen zur Verwendung von AWS Secrets Manager finden Sie unter Sicherheit.
9. Wählen Sie für die IP-Version „Tunnel innerhalb von IP“ die Option IPv4oder IPv6.
10. (Optional) Aktivieren Sie für Beschleunigung aktivieren das Kontrollkästchen, um die Beschleunigung zu aktivieren. Weitere Informationen finden Sie unter Beschleunigte VPN-Verbindungen.

    Wenn Sie die Beschleunigung aktivieren, erstellen wir zwei Beschleuniger, die von Ihrer VPN-Verbindung verwendet werden. Es fallen zusätzliche Gebühren an.
11. (Optional) Je nachdem, für welche Version des Tunnels innerhalb der IP Sie sich entschieden haben, führen Sie einen der folgenden Schritte aus:
    - IPv4 — Geben Sie für Local IPv4 Network CIDR den IPv4 CIDR-Bereich auf der Kunden-Gateway-Seite (lokal) an, der über die VPN-Tunnel kommunizieren darf. Wählen Sie für CIDR im IPv4 Remote-Netzwerk den CIDR-Bereich auf der AWS Seite aus, die über VPN-Tunnel kommunizieren darf. Der Standardwert für beide Felder ist. `0.0.0.0/0`
    - IPv6 — Geben Sie für CIDR im lokalen IPv6 Netzwerk den IPv6 CIDR-Bereich auf dem Kunden-Gateway (lokal) an, der über die VPN-Tunnel kommunizieren darf. Wählen Sie für

CIDR im IPv6 Remote-Netzwerk den CIDR-Bereich auf der AWS Seite aus, die über VPN-Tunnel kommunizieren darf. Der Standardwert für beide Felder ist `::/0`

12. Wählen Sie für den Typ der externen IP-Adresse eine der folgenden Optionen aus:

    - Öffentlich IPv4 — (Standard) Verwenden Sie IPv4 Adressen für den Außentunnel IPs.
    - Privat IPv4 — Verwenden Sie eine private IPv4 Adresse für die Verwendung in privaten Netzwerken.
    - IPv6- Verwenden Sie IPv6 Adressen für den Außentunnel IPs. Diese Option setzt voraus, dass Ihr Kunden-Gateway-Gerät die IPv6 Adressierung unterstützt.

    > **Note**
    >
    > Wenn Sie IPv6den externen IP-Adresstyp wählen, müssen Sie ein Kunden-Gateway mit einer IPv6 Adresse erstellen

13. (Optional) Für die Optionen für Tunnel 1 können Sie die folgenden Informationen für jeden Tunnel angeben:

    - Ein IPv4 CIDR-Block der Größe /30 aus dem `169.254.0.0/16` Bereich für die internen IPv4 Tunneladressen.
    - Wenn Sie IPv6für die Version Tunnel inside IP einen IPv6 CIDR-Block /126 aus dem `fd00::/8` Bereich für interne Tunneladressen angegeben haben. IPv6
    - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 oder. IKEv2
    - Um die erweiterten Optionen für Ihren Tunnel zu bearbeiten, wählen Sie Tunneloptionen bearbeiten aus. Weitere Informationen finden Sie unter VPN-Tunneloptionen.
    - (Optional) Wählen Sie „Aktivieren“ für das Tunnel-Aktivitätsprotokoll, um Protokollnachrichten für IPsec Aktivitäten und DPD-Protokollnachrichten zu erfassen.
    - (Optional) Wählen Sie für den Lebenszyklus von Tunnel-Endpunkten die Option Aktivieren aus, um den Zeitplan für den Austausch von Endpunkten zu steuern. Weitere Informationen zum Lebenszyklus von Tunnelendpunkten finden Sie unterLebenszyklus eines Tunnelendpunkts.

14. (Optional) Wählen Sie die Optionen für Tunnel 2 und folgen Sie den vorherigen Schritten, um einen zweiten Tunnel einzurichten.

15. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.

Um eine Site-to-Site VPN-Verbindung über die Befehlszeile oder API herzustellen

- CreateVpnConnection(Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)

  Beispiel für die Erstellung einer VPN-Verbindung mit IPv6 Außentunnel IPs und IPv6 Innentunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --customer-gateway-id
 cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=pv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

# Einen AWS Site-to-Site VPN Transit-Gateway-Anhang erstellen

Um einen VPN-Anhang auf einem Transit-Gateway zu erstellen, müssen Sie das Transit-Gateway und das Kunden-Gateway angeben. Das Transit-Gateway muss erstellt werden, bevor Sie dieses Verfahren ausführen. Weitere Informationen zum Erstellen eines Transit-Gateways finden Sie unter Transit-Gateways in Amazon VPC-Transit-Gateways.

VPN-Anhänge des Transit-Gateways unterstützen beide IPv4 oder IPv6. Weitere Informationen zur Verwendung eines dieser Protokolle für eine Transit-Gateway-VPN-Verbindung finden Sie unter IPv4 und IPv6 Traffic in AWS Site-to-Site VPN.

So erstellen Sie einen VPN-Anhang in einen Transit–Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.
4. (Optional) Geben Sie als Name-Tag einen Namen für die Verbindung ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
5. Wählen Sie unter Ziel die Option Transit Gateway und dann die Transit-Gateway-ID aus.
6. Wählen Sie bei Customer gateway (Kunden-Gateway) eine der folgenden Vorgehensweise:
   - Um ein vorhandenes Kunden-Gateway zu verwenden, wählen Sie Existing und dann die Kunden-Gateway-ID aus.
   - Um ein neues Kunden-Gateway zu erstellen, wählen Sie Neu.

   1. Geben Sie für die IP-Adresse eine statische Adresse IPv4oder eine IPv6Adresse ein.
   2. (Optional) Wählen Sie für Certificate ARN den ARN Ihres privaten Zertifikats aus (falls Sie die zertifikatsbasierte Authentifizierung verwenden).
   3. Geben Sie unter BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) Ihres Kunden-Gateways ein. Weitere Informationen finden Sie unter Kunden-Gateway-Optionen.
7. Wählen Sie für Routing-Optionen Dynamisch (erfordert BGP) oder Statisch.
8. Wählen Sie für Pre-Shared Key Storage entweder Standard oder Secrets Manager. Die Standardauswahl ist Standard. Weitere Informationen zur Verwendung von AWS Secrets Manager finden Sie unter Sicherheit.
9. Wählen Sie für die IP-Version „Tunnel innerhalb von IP“ die Option IPv4oder IPv6.
10. (Optional) Aktivieren Sie für Beschleunigung aktivieren das Kontrollkästchen, um die Beschleunigung zu aktivieren. Weitere Informationen finden Sie unter Beschleunigte VPN-Verbindungen.

    Wenn Sie die Beschleunigung aktivieren, erstellen wir zwei Beschleuniger, die von Ihrer VPN-Verbindung verwendet werden. Es fallen zusätzliche Gebühren an.
11. (Optional) Je nachdem, für welche Version des Tunnels innerhalb der IP Sie sich entschieden haben, führen Sie einen der folgenden Schritte aus:

    - IPv4 — Geben Sie für Local IPv4 Network CIDR den IPv4 CIDR-Bereich auf der Kunden-Gateway-Seite (lokal) an, der über die VPN-Tunnel kommunizieren darf. Wählen Sie für CIDR im IPv4 Remote-Netzwerk den CIDR-Bereich auf der AWS Seite aus, die über VPN-Tunnel kommunizieren darf. Der Standardwert für beide Felder ist `0.0.0.0/0`
    - IPv6 — Geben Sie für CIDR im lokalen IPv6 Netzwerk den IPv6 CIDR-Bereich auf dem Kunden-Gateway (lokal) an, der über die VPN-Tunnel kommunizieren darf. Wählen Sie für CIDR im IPv6 Remote-Netzwerk den CIDR-Bereich auf der AWS Seite aus, die über VPN-Tunnel kommunizieren darf. Der Standardwert für beide Felder ist `::/0`
12. Wählen Sie für den Typ der externen IP-Adresse eine der folgenden Optionen aus:

    - Öffentlich IPv4 — (Standard) Verwenden Sie IPv4 Adressen für den Außentunnel IPs.
    - Privat IPv4 — Verwenden Sie eine private IPv4 Adresse für die Verwendung in privaten Netzwerken.
    - IPv6- Verwenden Sie IPv6 Adressen für den Außentunnel IPs. Diese Option setzt voraus, dass Ihr Kunden-Gateway-Gerät die IPv6 Adressierung unterstützt.

> **Note**
>
> Wenn Sie IPv6den externen IP-Adresstyp wählen, müssen Sie ein Kunden-Gateway mit einer IPv6 Adresse erstellen

13. (Optional) Für die Optionen für Tunnel 1 können Sie die folgenden Informationen für jeden Tunnel angeben:
    - Ein IPv4 CIDR-Block der Größe /30 aus dem `169.254.0.0/16` Bereich für die internen IPv4 Tunneladressen.
    - Wenn Sie IPv6für die Version Tunnel inside IP einen IPv6 CIDR-Block /126 aus dem `fd00::/8` Bereich für interne Tunneladressen angegeben haben. IPv6
    - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 oder. IKEv2
    - Um die erweiterten Optionen für Ihren Tunnel zu bearbeiten, wählen Sie Tunneloptionen bearbeiten aus. Weitere Informationen finden Sie unter VPN-Tunneloptionen.
    - (Optional) Wählen Sie „Aktivieren“ für das Tunnel-Aktivitätsprotokoll, um Protokollnachrichten für IPsec Aktivitäten und DPD-Protokollnachrichten zu erfassen.
    - (Optional) Wählen Sie für den Lebenszyklus von Tunnel-Endpunkten die Option Aktivieren aus, um den Zeitplan für den Austausch von Endpunkten zu steuern. Weitere Informationen zum Lebenszyklus von Tunnelendpunkten finden Sie unterLebenszyklus eines Tunnelendpunkts.
14. (Optional) Wählen Sie die Optionen für Tunnel 2 und folgen Sie den vorherigen Schritten, um einen zweiten Tunnel einzurichten.
15. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.

## Erstellen eines VPN-Anhangs mit der CLI

Verwenden Sie den create-vpn-connectionBefehl und geben Sie die Transit-Gateway-ID für die `--transit-gateway-id` Option an.

Beispiel für die Erstellung einer VPN-Verbindung mit IPv6 Außentunnel IPs und IPv6 Innentunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
```

```
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Beispiel für den Aufbau einer VPN-Verbindung mit IPv6 Außentunnel IPs und IPv4 Innentunnel IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

## IPv6 Adressen für Ihre VPN-Verbindung anzeigen

Nachdem Sie eine VPN-Verbindung mit IPv6 äußerem Tunnel hergestellt haben IPs, können Sie die zugewiesenen IPv6 Adressen mit dem `describe-vpn-connections` CLI-Befehl anzeigen:

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-12345678901234567
```

Suchen Sie in der Antwort nach dem `OutsideIpAddress` Feld im `TunnelOptions` Abschnitt. Bei IPv6 VPN-Verbindungen enthält dieses Feld die IPv6 Adressen, die der AWS Seite der VPN-Tunnel zugewiesen sind.

Beispiel für einen Antwortauszug:

```
"Options": {
    "OutsideIPAddressType": "Ipv6",
    "TunnelInsideIpVersion": "ipv6",
    "TunnelOptions": [
        {
            "OutsideIpAddress": "2600:1f14:2dcf:d556:c3db:e57f:2414:2d9a",
            "TunnelInsideCidr": "2001:db8:1001:b110::/64",
            ...
        },
        {
            "OutsideIpAddress": "2600:1f14:2dcf:d57d:6318:60af:37c5:7ce1",
            "TunnelInsideCidr": "2001:db8:1001:b111::/64",
            ...
        }
    ]
}
```

# Eine AWS Site-to-Site VPN Verbindung testen

Nachdem Sie die AWS Site-to-Site VPN Verbindung hergestellt und das Kunden-Gateway konfiguriert haben, können Sie eine Instanz starten und die Verbindung testen, indem Sie die Instanz anpingen.

Bevor Sie anfangen, prüfen Sie Folgendes:

- Verwenden Sie ein AMI, das auf Ping-Anfragen reagiert. Wir empfehlen Ihnen, eines der Amazon Linux-Betriebssysteme zu verwenden AMIs.
- Konfigurieren Sie in Ihrer VPC alle Sicherheitsgruppen oder Netzwerk-ACLs, die den Datenverkehr zur Instance filtern, damit sowohl eingehender als auch ausgehender ICMP-Datenverkehr zugelassen wird. Dadurch kann die Instance `ping`-Anfragen empfangen.
- Wenn Sie Instances verwenden, auf denen Windows Server ausgeführt wird, stellen Sie eine Verbindung zur Instance her und aktivieren Sie Inbound ICMPv4 auf der Windows-Firewall, um die Instance zu pingen.
- (Statisches Routing) Stellen Sie sicher, dass das Kunden-Gateway-Gerät eine statische Route zu Ihrer VPC besitzt und Ihre VPN-Verbindung über eine statische Route verfügt, damit der Netzwerkdatenverkehr zurück zum Kunden-Gateway-Gerät gelangen kann.
- (Dynamisches Routing) Stellen Sie sicher, dass der BGP-Status auf Ihrem Kunden-Gateway-Gerät eingerichtet ist. Es dauert etwa 30 Sekunden, bis eine BGP-Peering-Sitzung aufgebaut ist. Stellen Sie sicher, dass Routen mit BGP ordnungsgemäß angekündigt und in der Routing-Tabelle gezeigt werden, sodass der Verkehr zu Ihrem Kunden-Gateway zurückgelangen kann. Stellen Sie sicher, dass beide Tunnel mit BGP-Routing konfiguriert sind.
- Stellen Sie sicher, dass Sie das Routing in Ihren Subnetz-Routing-Tabellen für die VPN-Verbindung konfiguriert haben.

So testen Sie die Konnektivität

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
3. (Optional) Geben Sie unter Name einen beschreibenden Namen für Ihre Instance ein.
4. Wählen Sie bei Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Schnellstart und dann das Betriebssystem für Ihre Instance aus.

5. Wählen Sie bei Schlüsselpaarname ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues.
6. Wählen Sie unter Firewall die Option Vorhandene Sicherheitsgruppe auswählen und dann die erstellte Sicherheitsgruppe aus.
7. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.
8. Rufen Sie, sobald die Instance ausgeführt wird, die private IP-Adresse (z. B. 10.0.0.4) ab. Die EC2 Amazon-Konsole zeigt die Adresse als Teil der Instance-Details an.
9. Verwenden Sie auf einem Computer in Ihrem Netzwerk, der sich hinter dem Kunden-Gateway-Gerät befindet, den ping-Befehl mit der privaten IP-Adresse der Instance.

```
ping 10.0.0.4
```

Eine erfolgreiche Antwort ähnelt dem folgenden Beispiel.

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Um ein Tunnel-Failover zu testen, können Sie vorübergehend einen der Tunnel des Kunden-Gateway-Geräts deaktivieren und den Schritt dann wiederholen. Es ist nicht möglich, einen Tunnel auf der AWS -Seite der VPN-Verbindung zu deaktivieren.

10. Um die Verbindung zu Ihrem lokalen Netzwerk AWS zu testen, können Sie SSH oder RDP verwenden, um von Ihrem Netzwerk aus eine Verbindung zu Ihrer Instance herzustellen. Anschließend können Sie den `ping`-Befehl mit der privaten IP-Adresse eines anderen Computers in Ihrem Netzwerk ausführen, um sicherzustellen, dass beide Seiten der Verbindung Anforderungen initiieren und empfangen können.

    Weitere Informationen zum Herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Connect to your Linux Instance im EC2 Amazon-Benutzerhandbuch. Weitere Informationen zum

Herstellen einer Connect einer Windows-Instance finden Sie unter Verbindung zu Ihrer Windows-Instance herstellen im EC2 Amazon-Benutzerhandbuch.

# Eine AWS Site-to-Site VPN Verbindung und ein Gateway löschen

Wenn Sie keine AWS Site-to-Site VPN Verbindung mehr benötigen, können Sie sie löschen. Wenn Sie eine Site-to-Site VPN-Verbindung löschen, löschen wir nicht das Kunden-Gateway oder das virtuelle private Gateway, das mit der Site-to-Site VPN-Verbindung verknüpft war. Wenn Sie das Kunden-Gateway und das Virtual Private Gateway nicht mehr benötigen, können Sie diese löschen.

> **Warning**
>
> Wenn Sie Ihre Site-to-Site VPN-Verbindung löschen und dann eine neue erstellen, müssen Sie eine neue Konfigurationsdatei herunterladen und das Kunden-Gateway-Gerät neu konfigurieren.

Aufgaben

- Löschen Sie eine Verbindung AWS Site-to-Site VPN
- Löschen Sie ein AWS Site-to-Site VPN Kunden-Gateway
- Trennen und löschen Sie ein virtuelles privates Gateway in AWS Site-to-Site VPN

## Löschen Sie eine Verbindung AWS Site-to-Site VPN

Nachdem Sie Ihre Site-to-Site VPN-Verbindung gelöscht haben, bleibt sie für kurze Zeit mit dem Status von `deleted` sichtbar. Danach wird der Eintrag automatisch entfernt.

So löschen Sie eine VPN-Verbindung mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie erst die VPN-Verbindung und dann Aktionen und VPN-Verbindung löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So löschen Sie eine VPN-Verbindung über die Befehlszeile oder API

- DeleteVpnConnection(Amazon EC2 Query API)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

## Löschen Sie ein AWS Site-to-Site VPN Kunden-Gateway

Wenn Sie ein Kunden-Gateway nicht mehr benötigen, können Sie es löschen. Sie können kein Kunden-Gateway löschen, das in einer Site-to-Site VPN-Verbindung verwendet wird.

So löschen Sie ein Kunden-Gateway mithilfe der Konsole

1. Wählen Sie im Navigationsbereich Kunden-Gateways aus.
2. Wählen Sie das Kunden-Gateway und Aktionen, Kunden-Gateway löschen aus.
3. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So löschen Sie ein Kunden-Gateway über die Befehlszeile oder API

- DeleteCustomerGateway(Amazon EC2 Query API)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

## Trennen und löschen Sie ein virtuelles privates Gateway in AWS Site-to-Site VPN

Wenn Sie ein Virtual Private Gateway in Ihrer VPC nicht mehr benötigen, können Sie es von der VPC trennen.

So trennen Sie ein Virtual Private Gateway mithilfe der Konsole

1. Wählen Sie im Navigationsbereich Virtual Private Gateways aus.
2. Wählen Sie den Virtual Private Gateway und dann Actions, Detach from VPC.
3. Wählen Sie Virtuelles privates Gateway trennen aus.

Wenn Sie ein Virtual Private Gateway, das getrennt wurde, nicht mehr benötigen, können Sie es löschen. Sie können ein Virtual Private Gateway, das noch immer einer VPC zugeordnet ist, nicht löschen. Nachdem Sie Ihr virtuelles privates Gateway gelöscht haben, bleibt es kurze Zeit mit dem Status `deleted` sichtbar und dann wird der Eintrag automatisch entfernt.

So löschen Sie ein Virtual Private Gateway mithilfe der Konsole

1. Wählen Sie im Navigationsbereich Virtual Private Gateways aus.
2. Wählen Sie das Virtual Private Gateway und Aktionen, Virtual Private Gateway löschen aus.
3. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So trennen Sie ein Virtual Private Gateway über die Befehlszeile oder API

- DetachVpnGateway(Amazon EC2 Query API)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

So löschen Sie ein Virtual Private Gateway über die Befehlszeile oder API

- DeleteVpnGateway(Amazon EC2 Query API)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

# Ändern Sie das Ziel-Gateway einer AWS Site-to-Site VPN Verbindung

Sie können das Ziel-Gateway einer AWS Site-to-Site VPN Verbindung ändern. Die folgenden Migrationsoptionen sind verfügbar:

- Ein vorhandenes Virtual Private Gateway zu einem Transit-Gateway
- Ein vorhandenes Virtual Private Gateway zu einem anderen Virtual Private Gateway
- Ein vorhandenes Transit-Gateway zu einem anderen Transit-Gateway
- Ein vorhandenes Transit-Gateway zu einem Virtual Private Gateway

Nachdem Sie das Ziel-Gateway geändert haben, ist Ihre Site-to-Site VPN-Verbindung vorübergehend für einen kurzen Zeitraum nicht verfügbar, solange wir die neuen Endpunkte bereitstellen.

Die folgenden Aufgaben helfen Ihnen, die Migration zu einem neuen Gateway durchzuführen.

Aufgaben

- Schritt 1: Das neue Ziel-Gateway erstellen
- Schritt 2: Die statischen Routen löschen (bedingt)
- Schritt 3: Migrieren zum neuen Gateway
- Schritt 4: Aktualisieren der VPC-Routing-Tabellen
- Schritt 5: Ziel-Gateway-Routing aktualisieren (bedingt)
- Schritt 6: Kunden-Gateway-ASN aktualisieren (bedingt)

## Schritt 1: Das neue Ziel-Gateway erstellen

Bevor Sie die Migration zu einem neuen Ziel-Gateway durchführen, müssen Sie das neue Gateway zunächst konfigurieren. Weitere Informationen zum Hinzufügen eines Virtual Private Gateway finden Sie unter the section called “Erstellen eines Virtual Private Gateways”. Weitere Informationen zum Hinzufügen eines Transit-Gateways finden Sie unter Erstellen eines Transit-Gateways in Amazon VPC Transit-Gateways.

Wenn es sich bei dem neuen Ziel-Gateway um ein Transit-Gateway handelt, schließen Sie VPCs es an das Transit-Gateway an. Weitere Informationen zu VPC-Anhängen finden Sie auf der Seite über Transit-Gateway-Verbindungen mit einer VPC in Amazon VPC Transit-Gateways.

Wenn Sie das Ziel von einem Virtual Private Gateway zu einem Transit-Gateway ändern, können Sie optional die Transit Gateway-ASN auf denselben Wert wie die ASN des Virtual Private Gateways setzen. Wenn Sie sich für eine andere ASN entscheiden, müssen Sie die ASN auf Ihrem Kunden-Gateway-Gerät auf die Transit-Gateway-ASN festlegen. Weitere Informationen finden Sie unter the section called “Schritt 6: Kunden-Gateway-ASN aktualisieren (bedingt)”.

## Schritt 2: Die statischen Routen löschen (bedingt)

Dieser Schritt ist erforderlich, wenn Sie eine Migration von einem Virtual Private Gateway mit statischen Routen zu einem Transit-Gateway durchführen.

Sie müssen die statischen Routen löschen, bevor Sie die Migration zum neuen Gateway durchführen können.

> **Tip**
>
> Erstellen Sie eine Kopie der statischen Route, ehe Sie diese löschen. Sie müssen diese Routen wieder zum Transit-Gateway hinzufügen, wenn die Migration der VPN-Verbindung abgeschlossen ist.

So löschen Sie Routen aus einer Routing-Tabelle

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
4. Wählen Sie bei der statischen Route zum Virtual Private Gateway Entfernen aus.
5. Wählen Sie Änderungen speichern.

## Schritt 3: Migrieren zum neuen Gateway

So ändern Sie das Ziel-Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die VPN-Verbindung und Aktionen, VPN-Verbindung ändern aus.
4. Wählen Sie als Zieltyp den Gateway-Typ aus.
   a. Wenn das neue Ziel-Gateway ein virtuelles privates Gateway ist, wählen Sie VPN-Gateway aus.
   b. Wenn das neue Ziel-Gateway ein Transit-Gateway ist, wählen Sie Transit-Gateway aus.
5. Wählen Sie Änderungen speichern.

Um eine Site-to-Site VPN-Verbindung über die Befehlszeile oder API zu ändern

- ModifyVpnConnection(Amazon EC2 Query API)
- modify-vpn-connection (AWS CLI)

## Schritt 4: Aktualisieren der VPC-Routing-Tabellen

Nach der Migration zum neuen Gateway müssen Sie möglicherweise Ihre VPC-Routing-Tabelle ändern. Weitere Informationen finden Sie unter Routing-Tabellen im Amazon VPC-Benutzerhandbuch.

Die folgende Tabelle enthält Informationen zu den Aktualisierungen der VPC-Routentabelle, die nach dem Ändern des VPN-Gateway-Ziels vorgenommen werden sollen.

| Vorhandenes Gateway | Neues Gateway | Änderung der VPC-Routing-Tabelle |
| --- | --- | --- |
| Virtual Private Gateway mit verbreiteten Routen | Transit Gateway | Fügen Sie eine Route hinzu, in der die ID des Transit-Gateway enthalten ist. |
| Virtual Private Gateway mit verbreiteten Routen | Virtual Private Gateway mit verbreiteten Routen | Es ist keine Aktion erforderlich. |
| Virtual Private Gateway mit verbreiteten Routen | Virtual Private Gateway mit statischer Route | Fügen Sie eine Route hinzu, in der die ID des neuen Virtual Private Gateway enthalten ist. |
| Virtual Private Gateway mit statischen Routen | Transit Gateway | Aktualisieren Sie die Route, in der die ID des Virtual Private Gateway enthalten ist, auf die ID des Transit-Gateway. |
| Virtual Private Gateway mit statischen Routen | Virtual Private Gateway mit statischen Routen | Aktualisieren Sie die Route, in der die ID des Virtual Private Gateway enthalten ist, auf die ID des neuen Virtual Private Gateway. |
| Virtual Private Gateway mit statischen Routen | Virtual Private Gateway mit verbreiteten Routen | Löschen Sie die Route, in der die ID des Virtual Private Gateway enthalten ist. |

| Vorhandenes Gateway | Neues Gateway | Änderung der VPC-Routing-Tabelle |
| --- | --- | --- |
| Transit Gateway | Virtual Private Gateway mit statischen Routen | Aktualisieren Sie die Route, in der die ID des Transit Gateway enthalten ist, auf die ID des Virtual Private Gateway. |
| Transit Gateway | Virtual Private Gateway mit verbreiteten Routen | Löschen Sie die Route, in der die ID des Transit-Gateway enthalten ist. |
| Transit Gateway | Transit Gateway | Aktualisieren Sie die Route, in der die ID des Transit Gateway enthalten ist, auf die ID des neuen Transit-G ateway. |

## Schritt 5: Ziel-Gateway-Routing aktualisieren (bedingt)

Wenn es sich bei dem neuen Gateway um ein Transit-Gateway handelt, ändern Sie die Routentabelle des Transit-Gateways, um den Verkehr zwischen der VPC und dem Site-to-Site VPN zuzulassen. Weitere Informationen finden Sie unter Transit-Gateway-Routing-Tabellen in Amazon-VPC-Transit-Gateways.

Wenn Sie statische VPN-Routen gelöscht haben, müssen Sie die statischen Routen zur Transit-Gateway-Routing-Tabelle hinzufügen.

Im Gegensatz zu einem virtuellen privaten Gateway legt ein Transit-Gateway den gleichen Wert für den Multi-Exit-Diskriminator (MED) in allen Tunneln eines VPN-Anhangs fest. Wenn Sie von einem virtuellen privaten Gateway zu einem Transit-Gateway migrieren und sich bei der Tunnelauswahl auf den MED-Wert verlassen, empfehlen wir Ihnen, Routing-Änderungen vorzunehmen, um Verbindungsprobleme zu vermeiden. Sie können beispielsweise spezifischere Routen auf Ihrem Transit-Gateway bewerben. Weitere Informationen finden Sie unter Routentabellen und AWS Site-to-Site VPN Routenpriorität.

## Schritt 6: Kunden-Gateway-ASN aktualisieren (bedingt)

Wenn das neue Gateway eine andere ASN als das alte Gateway hat, müssen Sie die ASN auf Ihrem Kunden-Gateway-Gerät aktualisieren, um auf die neue ASN zu verweisen. Weitere Informationen finden Sie unter Kunden-Gateway-Optionen für Ihre AWS Site-to-Site VPN Verbindung.

# AWS Site-to-Site VPN Verbindungsoptionen ändern

Sie können die Verbindungsoptionen für Ihre Site-to-Site VPN-Verbindung ändern. Sie können die folgenden Optionen ändern:

- Der IPv4 CIDR erstreckt sich auf der lokalen Seite (Kunden-Gateway) und der Remote-Seite (AWS) der VPN-Verbindung, die über die VPN-Tunnel kommunizieren kann. Der Standardwert für beide Bereiche lautet „`0.0.0.0/0`“.
- Der IPv6 CIDR erstreckt sich auf der lokalen (Kunden-Gateway) und der Remote-Seite (AWS) der VPN-Verbindung, die über die VPN-Tunnel kommunizieren kann. Der Standardwert für beide Bereiche lautet „`::/0`“.

Wenn Sie die VPN-Verbindungsoptionen ändern, ändern sich die IP-Adressen der VPN-Endpunkte auf der AWS Seite nicht, und die Tunneloptionen ändern sich nicht. Ihre VPN-Verbindung ist für einen kurzen Zeitraum nicht verfügbar, während die VPN-Verbindung aktualisiert wird.

So ändern Sie die VPN-Verbindungsoptionen über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie Ihre VPN-Verbindung und Aktionen, VPN-Verbindungsoptionen ändern aus.
4. Geben Sie nach Bedarf neue CIDR-Bereiche ein.
5. Wählen Sie Änderungen speichern.

So ändern Sie die VPN-Verbindungsoptionen über die Befehlszeile oder API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions(Amazon EC2 Query API)

# AWS Site-to-Site VPN Tunneloptionen ändern

Sie können die Tunneloptionen für die VPN-Tunnel in Ihrer Site-to-Site VPN-Verbindung ändern. Sie können nur jeweils einen VPN-Tunnel ändern.

> **Important**
>
> Wenn Sie einen VPN-Tunnel ändern, wird die Konnektivität über den Tunnel unter Umständen für mehrere Minuten unterbrochen. Planen Sie die erwartete Ausfallzeit unbedingt ein.

So ändern Sie die VPN-Tunneloptionen über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die Site-to-Site VPN-Verbindung und dann Aktionen, VPN-Tunneloptionen ändern aus.
4. Wählen Sie bei Externe IP-Adresse des VPN-Tunnels die Tunnelendpunkt-IP des VPN-Tunnels aus.
5. Wählen Sie bei Bedarf neue Werte für die Tunnel-Optionen aus oder geben Sie sie ein. Weitere Informationen zu den Tunneloptionen finden Sie unterVPN-Tunneloptionen.

   > **Note**
   >
   > Einige Tunneloptionen haben mehrere Standardwerte. Klicken Sie hier, um einen beliebigen Standardwert zu entfernen. Dieser Standardwert wird dann aus der Tunneloption entfernt.

6. Wählen Sie Änderungen speichern.

So ändern Sie die VPN-Tunneloptionen über die Befehlszeile oder API

- (AWS CLI) Wird verwendet describe-vpn-connections, um die aktuellen Tunneloptionen anzuzeigen und die Tunneloptionen modify-vpn-tunnel-optionszu ändern.
- (Amazon EC2 Query API) Wird verwendet DescribeVpnConnections, um die aktuellen Tunneloptionen anzuzeigen und die Tunneloptionen ModifyVpnTunnelOptionszu ändern.

# Statische Routen für eine AWS Site-to-Site VPN Verbindung bearbeiten

Für eine Site-to-Site VPN-Verbindung auf einem virtuellen privaten Gateway, das für statisches Routing konfiguriert ist, können Sie statische Routen zu Ihrer VPN-Konfiguration hinzufügen oder daraus entfernen.

So können Sie eine statische Route mithilfe der Konsole hinzufügen oder entfernen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die VPN-Verbindung aus.
4. Wählen Sie Statische Routen bearbeiten aus.
5. Fügen Sie Routen nach Bedarf hinzu oder entfernen Sie sie.
6. Wählen Sie Änderungen speichern.
7. Wenn Sie die Routing-Verbreitung für Ihre Routing-Tabelle nicht aktiviert haben, müssen Sie die Routen in der Routing-Tabelle manuell aktualisieren, um die aktualisierten statischen IP-Präfixe in Ihrer VPN-Verbindung widerzuspiegeln. Weitere Informationen finden Sie unter (Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle.
8. Verwenden Sie bei einer VPN-Verbindung auf einem Transit-Gateway die Transit-Gateway-Routing-Tabelle zum Hinzufügen, Ändern oder Entfernen der statischen Routen. Weitere Informationen finden Sie unter Transit-Gateway-Routing-Tabellen in Amazon-VPC-Transit-Gateways.

So fügen Sie eine statische Route über die Befehlszeile oder API hinzu

- CreateVpnConnectionRoute(Amazon EC2 Query API)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

So löschen Sie eine statische Route über die Befehlszeile oder API

- DeleteVpnConnectionRoute(Amazon EC2 Query API)
- delete-vpn-connection-route (AWS CLI)

- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

## Das Kunden-Gateway für eine AWS Site-to-Site VPN Verbindung ändern

Sie können das Kunden-Gateway Ihrer Site-to-Site VPN-Verbindung mithilfe der Amazon VPC-Konsole oder eines Befehlszeilentools ändern.

Nachdem Sie das Kunden-Gateway geändert haben, ist Ihre VPN-Verbindung für einen kurzen Zeitraum vorübergehend nicht verfügbar, während wir die neuen Endpunkte bereitstellen.

So ändern Sie das Kunden-Gateway mithilfe der Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die VPN-Verbindung aus.
4. Wählen Sie Aktionen, VPN-Verbindung ändern aus.
5. Wählen Sie unter Zieltyp die Option Kunden-Gateway aus.
6. Wählen Sie unter Ziel-Kunden-Gateway das neue Kunden-Gateway aus.
7. Wählen Sie Änderungen speichern.

So ändern Sie das Kunden-Gateway über die Befehlszeile oder API

- ModifyVpnConnection(Amazon EC2 Query API)
- modify-vpn-connection (AWS CLI)

## Kompromittierte Anmeldeinformationen für eine AWS Site-to-Site VPN Verbindung ersetzen

Wenn Sie glauben, dass die Tunnelanmeldedaten für Ihre Site-to-Site VPN-Verbindung kompromittiert wurden, können Sie den IKE-Pre-Shared-Schlüssel oder das ACM-Zertifikat ändern. Welche Methode Sie verwenden, hängt von der Authentifizierungsoption ab, die Sie für Ihre VPN-Tunnel verwendet haben. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Optionen für die Tunnelauthentifizierung.

So ändern Sie den vorinstallierten IKE-Schlüssel

Sie können die Tunneloptionen für die VPN-Verbindung ändern und einen neuen vorinstallierten IKE-Schlüssel für jeden Tunnel angeben. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Tunneloptionen ändern.

Alternativ können Sie die VPN-Verbindung löschen. Weitere Informationen finden Sie unter Löschen Sie eine VPN-Verbindung und ein Gateway. Sie müssen die VPC oder das Virtual Private Gateway nicht löschen. Erstellen Sie mit demselben Virtual Private Gateway eine neue VPN-Verbindung und konfiguriere Sie die neuen Schlüssel auf Ihrem Kunden-Gateway. Sie können Ihre eigenen Pre-Shared Keys für die Tunnel angeben oder sich neue Pre-Shared Keys AWS generieren lassen. Weitere Informationen finden Sie unter Eine VPN-Verbindung erstellen. Die internen und externen Adressen des Tunnels ändern sich möglicherweise, wenn Sie die VPN-Verbindung neu erstellen.

Um das Zertifikat für die AWS Seite des Tunnelendpunkts zu ändern

Rotieren des Zertifikats. Weitere Informationen finden Sie unter VPN-Tunnelendpunkt-Zertifikate rotieren.

So ändern Sie das Zertifikat auf dem Kunden-Gateway-Gerät

1. Erstellen Sie ein neues Zertifikat. Informationen finden Sie unter Ausstellen und Verwalten von Zertifikaten im AWS Certificate Manager -Benutzerhandbuch.
2. Fügen Sie das Zertifikat zum Kunden-Gateway-Gerät hinzu.

# AWS Site-to-Site VPN Tunnelendpunkt-Zertifikate rotieren

Mithilfe der Amazon VPC-Konsole können Sie die Zertifikate auf den Tunnelendpunkten auf der AWS Seite rotieren. Wenn das Zertifikat eines Tunnelendpunkts kurz vor dem Ablauf steht, wird das Zertifikat mithilfe der serviceverknüpften Rolle AWS automatisch rotiert. Weitere Informationen finden Sie unter the section called “Service-verknüpfte Rollen”.

Um das Zertifikat für den Site-to-Site VPN-Tunnelendpunkt mithilfe der Konsole zu rotieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die Site-to-Site VPN-Verbindung und dann Aktionen, VPN-Tunnelzertifikat ändern aus.

4. Wählen Sie den Tunnelendpunkt aus.
5. Wählen Sie Save (Speichern) aus.

Um das Site-to-Site VPN-Tunnel-Endpunktzertifikat zu rotieren, verwenden Sie AWS CLI

Verwenden Sie den modify-vpn-tunnel-certificate-Befehl.

# Private IP AWS Site-to-Site VPN mit AWS Direct Connect

Mit Private IP VPN können Sie IPsec VPN über AWS Direct Connect bereitstellen und dabei den Datenverkehr zwischen Ihrem lokalen Netzwerk verschlüsseln AWS, ohne öffentliche IP-Adressen oder zusätzliche VPN-Geräte von Drittanbietern verwenden zu müssen.

Einer der Hauptanwendungsfälle für privates IP-VPN AWS Direct Connect ist die Unterstützung von Kunden in der Finanz-, Gesundheits- und Bundesbranche bei der Einhaltung gesetzlicher Vorschriften und Compliance-Ziele. Private IP VPN Over AWS Direct Connect stellt sicher, dass der Datenverkehr zwischen AWS und lokalen Netzwerken sowohl sicher als auch privat ist, sodass Kunden ihre regulatorischen und sicherheitstechnischen Anforderungen einhalten können.

## Vorteile von privatem IP-VPN

- Vereinfachtes Netzwerkmanagement und -betrieb: Ohne privates IP-VPN müssen Kunden VPNs und Router von Drittanbietern einsetzen, um private VPNs Netzwerke zu implementieren. AWS Direct Connect Mit der Funktion für privates IP-VPN müssen Kunden keine eigene VPN-Infrastruktur bereitstellen und verwalten. Das Ergebnis ist ein vereinfachter Netzwerkbetrieb zu geringeren Kosten.
- Verbesserter Sicherheitsstatus: Bisher mussten Kunden eine öffentliche AWS Direct Connect virtuelle Schnittstelle (VIF) für die Verschlüsselung des Datenverkehrs verwenden AWS Direct Connect, wofür öffentliche IP-Adressen für VPN-Endpunkte erforderlich waren. Die Nutzung öffentlicher IPs Netzwerke erhöht die Wahrscheinlichkeit von externen Angriffen (DOS), was wiederum Kunden dazu zwingt, zusätzliche Sicherheitsausrüstung für den Netzwerkschutz einzusetzen. Darüber hinaus ermöglicht eine öffentliche VIF den Zugang zwischen allen AWS öffentlichen Diensten und den lokalen Netzwerken der Kunden, was die Schwere des Risikos erhöht. Die private IP-VPN-Funktion ermöglicht die Verschlüsselung über die AWS Direct Connect Übertragung VIFs (statt über die öffentliche Verbindung VIFs) und bietet zudem die Möglichkeit, private Verbindungen zu konfigurieren. IPs Dies bietet zusätzlich zur Verschlüsselung end-to-end private Konnektivität und verbessert so die allgemeine Sicherheitslage.

- Höherer Routenumfang: Private IP-VPN-Verbindungen bieten höhere Routenlimits (5000 ausgehende Routen und 1000 eingehende Routen) im Vergleich zu AWS Direct Connect reinen Verbindungen, bei denen derzeit ein Limit von 200 ausgehenden und 100 eingehenden Routen gilt.

## Funktionsweise von privatem IP-VPN

Privates Site-to-Site IP-VPN funktioniert über eine virtuelle AWS Direct Connect Transitschnittstelle (VIF). Es verwendet ein AWS Direct Connect Gateway und ein Transit-Gateway, um Ihre lokalen Netzwerke miteinander zu verbinden. AWS VPCs Eine private IP-VPN-Verbindung hat Endpunkte am Transit-Gateway auf der AWS Seite und an Ihrem Kunden-Gateway-Gerät auf der lokalen Seite. Sie müssen sowohl dem Transit-Gateway als auch dem Kunden-Gateway-Geräteende der IPsec Tunnel private IP-Adressen zuweisen. Sie können private IP-Adressen aus einem RFC1918 oder RFC6598 privaten IPv4 Adressbereichen verwenden.

Sie hängen eine private IP-VPN-Verbindung an ein Transit Gateway an. Anschließend leiten Sie den Verkehr zwischen der VPN-Verbindung und allen VPCs (oder anderen Netzwerken) weiter, die ebenfalls an das Transit-Gateway angeschlossen sind. Dazu ordnen Sie dem VPN-Anhang eine Routing-Tabelle zu. In umgekehrter Richtung können Sie den Verkehr von Ihrem VPCs zum privaten IP-VPN-Anhang weiterleiten, indem Sie Routentabellen verwenden, die dem zugeordnet sind VPCs.

Die Routing-Tabelle, die der VPN-Anlage zugeordnet ist, kann dieselbe oder eine andere sein als die Routing-Tabelle, die der zugrunde liegenden AWS Direct Connect Anlage zugeordnet ist. Auf diese Weise können Sie sowohl verschlüsselten als auch unverschlüsselten Datenverkehr gleichzeitig zwischen Ihren VPCs und Ihren lokalen Netzwerken weiterleiten.

Weitere Informationen zum Datenverkehrspfad, der das VPN verlässt, finden Sie unter Routing-Richtlinien für private virtuelle Schnittstellen und virtuelle Transitschnittstellen im AWS Direct Connect Benutzerhandbuch.

Aufgaben

- Erstellen Sie eine private IP AWS Site-to-Site VPN über AWS Direct Connect

## Erstellen Sie eine private IP AWS Site-to-Site VPN über AWS Direct Connect

Gehen Sie AWS Direct Connect folgendermaßen vor, um ein privates IP-VPN mit zu erstellen. Bevor Sie das private IP-VPN über Direct Connect erstellen, müssen Sie sicherstellen, dass zuerst

ein Transit-Gateway und ein Direct Connect-Gateway erstellt werden. Nachdem Sie die beiden Gateways erstellt haben, müssen Sie dann eine Zuordnung zwischen den beiden erstellen. Diese Voraussetzungen werden in der folgenden Tabelle beschrieben. Nachdem Sie die beiden Gateways erstellt und verknüpft haben, erstellen Sie mithilfe dieser Zuordnung ein VPN-Kundenportal und eine VPN-Verbindung.

## Voraussetzungen

In der folgenden Tabelle werden die Voraussetzungen beschrieben, bevor Sie ein privates IP-VPN über Direct Connect einrichten.

| Item | Schritte | Informationen |
| --- | --- | --- |
| Bereiten Sie das Transit-Gateway für Site-to-Site VPN vor. | Erstellen Sie das Transit-Gateway mithilfe der Amazon Virtual Private Cloud (VPC-) Konsole oder mithilfe der Befehlszeile oder API.<br><br>Weitere Informationen finden Sie unter Transit-Gateways im Amazon VPC Transit Gateways-Handbuch. | Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke und Ihre VPCs lokalen Netzwerke miteinander verbinden können. Sie können ein neues Transit Gateway erstellen oder ein vorhandenes für die private IP-VPN-Verbindung verwenden. Wenn Sie das Transit Gateway erstellen oder ein vorhandenes Transit Gateway ändern, geben Sie einen privaten IP-CIDR-Block für die Verbindung an.<br><br>**Note**<br>Wenn Sie den CIDR-Block des Transit Gateways angeben, der mit Ihrem privaten IP-VPN verknüpft werden soll, stellen Sie sicher, dass sich |

| Item | Schritte | Informationen |
| --- | --- | --- |
| | | der CIDR-Block nicht mit IP-Adressen für andere Netzwerka nhänge auf dem Transit Gateway überschneidet. Wenn sich IP-CIDR-Blöcke überschneiden, kann dies zu Problemen bei der Konfiguration Ihres Kunden-Gateway-Ger äts führen. |
| Erstellen Sie das AWS Direct Connect Gateway für Site-to-S ite VPN. | Erstellen Sie das Direct Connect-Gateway mithilfe der Direct Connect-Konsole oder mithilfe der Befehlszeile oder API.<br><br>Weitere Informationen finden Sie unter Erstellen eines AWS Direct Connect-Gateways im AWS Direct Connect Benutzerhandbuch. | Ein Direct Connect-Gateway ermöglicht es Ihnen, virtuelle Schnittstellen (VIFs) über mehrere AWS Regionen hinweg zu verbinden. Dieses Gateway wird verwendet, um eine Verbindung zu Ihrer VIF herzustellen. |

| Item | Schritte | Informationen |
| --- | --- | --- |
| Erstellen Sie die Transit-Gateway-Zuordnung für Site-to-Site VPN. | Erstellen Sie die Zuordnung zwischen dem Direct Connect-Gateway und dem Transit-Gateway mithilfe der Direct Connect-Konsole oder mithilfe der Befehlszeile oder API.<br><br>Weitere Informationen finden Sie im Benutzerhandbuch unter Zuordnen oder AWS Direct Connect Aufheben der Verbindung zu einem Transit-Gateway.AWS Direct Connect | Nachdem Sie das AWS Direct Connect Gateway erstellt haben, erstellen Sie eine Transit-Gateway-Zuordnung für das AWS Direct Connect Gateway. Geben Sie das private IP-CIDR für das Transit Gateway an, das zuvor in der Liste zulässiger Präfixe identifiziert wurde. |

## Erstellen Sie das Kunden-Gateway und die Verbindung für Site-to-Site VPN

Ein Kunden-Gateway ist eine Ressource, die Sie in erstellen AWS. Es stellt das Kunden-Gateway-Gerät in Ihrem On-Premises-Netzwerk dar. Wenn Sie ein Kunden-Gateway erstellen, geben Sie Informationen über Ihr Gerät an AWS. Weitere Details finden Sie unter Kunden-Gateway.

So erstellen Sie ein Kunden-Gateway mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Kunden-Gateways aus.
3. Wählen Sie Kunden-Gateway erstellen aus.
4. (Optional) Geben Sie bei Name tag (Name-Tag) einen Namen für Ihr Kunden-Gateway ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
5. Geben Sie unter BGP ASN eine Border Gateway Protocol (BGP) Autonomous System Number (ASN) für Ihr Kunden-Gateway ein.
6. Geben Sie unter IP address (IP-Adresse) die private IP-Adresse für Ihr Kunden-Gateway-Gerät ein.

> **Important**
>
> Bei der Konfiguration von AWS Private IP AWS Site-to-Site VPN müssen Sie Ihre eigenen IP-Adressen für Tunnelendpunkte mithilfe von RFC 1918-Adressen angeben. Verwenden Sie die point-to-point IP-Adressen nicht für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Endpunkt. AWS Direct Connect AWS empfiehlt, anstelle von Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
> Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

7. (Optional) Geben Sie bei Device (Gerät) einen Namen für das Gerät ein, das dieses Kunden-Gateway hostet.
8. Wählen Sie Kunden-Gateway erstellen aus.
9. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
10. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.
11. (Optional) Geben Sie unter Namensschild einen Namen für Ihre Site-to-Site VPN-Verbindung ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
12. Wählen Sie für Target gateway type (Typ des Ziel-Gateways) die Option Transit gateway (Transit Gateway) aus. Wählen Sie dann das zuvor identifizierte Transit-Gateway aus.
13. Wählen Sie für Customer gateway (Kunden-Gateway) die Option Existing (Vorhanden) aus. Wählen Sie dann das zuvor identifizierte Kunden-Gateway aus.
14. Wählen Sie eine der Routing-Optionen aus, je nachdem, ob Ihr Kunden-Gateway-Gerät das Border Gateway Protocol (BGP) unterstützt:
    - Wenn Ihr Kunden-Gateway-Gerät BGP unterstützt, wählen Sie Dynamic (requires BGP) (Dynamisch (erfordert BGP)) aus.
    - Wenn Ihr Kunden-Gateway-Gerät BGP nicht unterstützt, wählen Sie Static (Statisch) aus.
15. Geben Sie für die IP-Version für Tunnel an, ob die VPN-Tunnel IPv6 Datenverkehr unterstützen IPv4 .
16. (Optional) Wenn Sie die Option Tunnel inside IP Version angegeben IPv4haben, können Sie optional die IPv4 CIDR-Bereiche für das Kunden-Gateway und die AWS Seiten angeben, die über die VPN-Tunnel kommunizieren dürfen. Der Standardwert ist `0.0.0.0/0`.

Wenn Sie die IP-Version IPv6für Tunnel angegeben haben, können Sie optional die IPv6 CIDR-Bereiche für das Kunden-Gateway und die AWS Seiten angeben, die über die VPN-Tunnel kommunizieren dürfen. Die Standardeinstellung für beide Bereiche lautet `::/0`.

17. Wählen Sie für den Typ der externen IP-Adresse die Option PrivateIpv4.
18. Wählen Sie unter Transport Attachment ID den Transit-Gateway-Anhang für das entsprechende AWS Direct Connect Gateway aus.
19. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.

> **Note**
>
> Die Option Enable acceleration (Beschleunigung aktivieren) ist für VPN-Verbindungen über AWS Direct Connect nicht anwendbar.

So erstellen Sie ein Kunden-Gateway über die Befehlszeile oder API

- CreateCustomerGateway(Amazon EC2 Query API)
- create-customer-gateway (AWS CLI)

# Sicherheit in AWS Site-to-Site VPN

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS Site-to-Site VPN gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Site-to-Site VPN anwenden können. In den folgenden Themen erfahren Sie, wie Sie Site-to-Site VPN konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Site-to-Site VPN-Ressourcen helfen.

Inhalt


- Verbesserte AWS Site-to-Site VPN Sicherheitsfunktionen mit Secrets Manager
- Datenschutz im VPN AWS Site-to-Site
- Identitäts- und Zugriffsmanagement für VPN AWS Site-to-Site
- Resilienz in AWS Site-to-Site VPN
- Sicherheit der Infrastruktur in VPN AWS Site-to-Site

# Verbesserte AWS Site-to-Site VPN Sicherheitsfunktionen mit Secrets Manager

Die Security Rebase-Funktion von AWS Site-to-Site VPN bietet erweiterte Sicherheitsfunktionen, die Ihnen mehr Kontrolle und Transparenz über Ihre VPN-Verbindungen bieten. Eine wichtige Verbesserung ist die Möglichkeit, vorab gemeinsam genutzte Schlüssel (PSKs) nicht direkt im AWS Secrets Manager Site-to-Site VPN-Dienst zu speichern, was eine bessere Verwaltung von Geheimnissen und die Einhaltung bewährter Sicherheitsverfahren ermöglicht. Die Funktion umfasst auch eine `GetActiveVpnTunnelStatus` API, die in Echtzeit Einblick in die Sicherheitsparameter bietet, die in aktiven VPN-Tunneln verwendet werden, einschließlich Verschlüsselungsalgorithmen, Integritätsalgorithmen und Diffie-Hellman-Gruppen für beide IKE-Phasen. Darüber hinaus können Sie jetzt empfohlene Sicherheitskonfigurationen generieren, die die Verwendung moderner Protokolle erzwingen, indem Sie ältere Optionen ausschließen, wie z. IKEv1 Diese Verbesserungen sind besonders nützlich, wenn Ihr Unternehmen strenge Sicherheitsstandards einhalten muss, detaillierte Prüfprotokolle Ihrer VPN-Konfigurationen benötigt oder sicherstellen möchte, dass Ihre VPN-Verbindungen die sichersten verfügbaren Protokolle verwenden.

Inhalt


- Ändern Sie den Pre-Shared Key von Secrets Manager in AWS Site-to-Site VPN
- Ändern Sie den Speichermodus für Pre-Shared Keys in AWS Site-to-Site VPN


## Ändern Sie den Pre-Shared Key von Secrets Manager in AWS Site-to-Site VPN

Wenn Ihr Tunnel in Secrets Manager nicht zugänglich ist, können Sie den Pre-Shared Key für diesen Tunnel ändern.

> **Note**
>
> - Stellen Sie beim Ändern des Pre-Shared Keys sicher, dass Sie über die erforderlichen IAM-Berechtigungen für beide Secrets Manager Manager-Dienste verfügen.
> - Nach dem Ändern des Pre-Shared-Schlüssels für einen VPN-Tunnel wird die Konnektivität für bis zu mehrere Minuten unterbrochen. Stellen Sie sicher, dass Sie die zu erwartenden Ausfallzeiten einplanen.

So ändern Sie den Pre-Shared Key von Secrets Manager für einen VPN-Tunnel

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie die Site-to-Site VPN-Verbindung aus und klicken Sie dann auf Aktionen, VPN-Tunneloptionen ändern.
4. Wählen Sie bei Externe IP-Adresse des VPN-Tunnels die Tunnelendpunkt-IP des VPN-Tunnels aus.
5. Wählen Sie im Feld Neuer vorinstallierter Schlüssel einen neuen vorinstallierten Schlüssel aus.

   > **Note**
   >
   > Diese Option ist nur für Schlüssel verfügbar, die in Secrets Manager gespeichert sind.

6. Wählen Sie Änderungen speichern aus.
7. Wiederholen Sie diese Schritte für jeden anderen Tunnel.

## Ändern Sie den Speichermodus für Pre-Shared Keys in AWS Site-to-Site VPN

Ändern Sie den Speichermodus für vorinstallierte Schlüssel für einen vorhandenen VPN-Tunnel.

> **Note**
>
> - Stellen Sie beim Ändern des Speichermodus sicher, dass Sie über die erforderlichen IAM-Berechtigungen für die Site-to-Site VPN- und Secrets Manager Manager-Dienste verfügen.
> - Nach dem Ändern des Speichermodus für einen VPN-Tunnel wird die Konnektivität für bis zu mehrere Minuten unterbrochen. Stellen Sie sicher, dass Sie die zu erwartenden Ausfallzeiten einplanen.

Um den Speichermodus für Pre-Shared Keys zu ändern

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.

3. Wählen Sie die Site-to-Site VPN-Verbindung aus und klicken Sie dann auf Aktionen, VPN-Tunneloptionen ändern.
4. Wählen Sie bei Externe IP-Adresse des VPN-Tunnels die Tunnelendpunkt-IP des VPN-Tunnels aus.
5. Wählen Sie unter Pre-Shared Key Storage einen der folgenden Pre-Shared Key-Speichertypen aus.
   - Standard — Der Pre-Shared Key wird direkt im VPN-Dienst gespeichert. Site-to-Site
   - Secrets Manager — Der Pre-Shared Key wird gespeichert unter AWS Secrets Manager. Weitere Informationen zu Secrets Manager finden Sie unterVerbesserte Sicherheitsfunktionen mit Secrets Manager.
6. Wählen Sie Änderungen speichern aus.

Wenn Sie den Speichermodus von Secrets Manager auf Standard ändern:

- Der Pre-Shared Key wird aus Secrets Manager entfernt und in den Site-to-Site VPN-Dienst verschoben.
- Der Tunneleingang wurde aus dem Secrets Manager Manager-Geheimnis entfernt.

Wenn Sie den Speichermodus von Standard zu Secrets Manager ändern:

- Der Pre-Shared Key wird aus dem Site-to-Site VPN-Dienst entfernt
- Ein neues Secrets Manager Manager-Geheimnis wird erstellt, falls noch keines existiert.
- Der neue Pre-Shared Key wird im Secrets Manager gespeichert.

# Datenschutz im VPN AWS Site-to-Site

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Site-to-Site VPN. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Site-to-Site VPN oder anderen Geräten arbeiten und dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

## Richtlinie für den Datenverkehr zwischen Netzwerken

Eine Site-to-Site VPN-Verbindung verbindet Ihre VPC privat mit Ihrem lokalen Netzwerk. Daten, die zwischen Ihrer VPC und Ihrem Netzwerk übertragen werden, werden über eine verschlüsselte VPN-Verbindung geroutet, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten. Amazon unterstützt Internet Protocol Security (IPsec) VPN-Verbindungen. IPsec ist

eine Protokollsuite zur Sicherung der IP-Kommunikation durch Authentifizierung und Verschlüsselung jedes IP-Pakets in einem Datenstrom.

Jede Site-to-Site VPN-Verbindung besteht aus zwei verschlüsselten IPsec VPN-Tunneln, die Ihr Netzwerk miteinander verbinden AWS . Der Verkehr in jedem Tunnel kann mit AES128 oder verschlüsselt werden AES256 und Diffie-Hellman-Gruppen für den Schlüsselaustausch verwenden, wodurch Perfect Forward Secrecy gewährleistet wird. AWS authentifiziert sich mit unseren Hashing-Funktionen. SHA1 SHA2

Instances in Ihrer VPC benötigen keine öffentliche IP-Adresse, um eine Verbindung zu Ressourcen auf der anderen Seite Ihrer Site-to-Site VPN-Verbindung herzustellen. Instances können ihren Internetverkehr über die Site-to-Site VPN-Verbindung zu Ihrem lokalen Netzwerk weiterleiten. Sie können dann über Ihre bestehenden ausgehenden Datenverkehrspunkte und Ihre Netzwerksicherheits- und Überwachungsgeräte auf das Internet zugreifen.

Weitere Informationen finden Sie im folgenden Thema:

- Tunneloptionen für Ihre AWS Site-to-Site VPN Verbindung: Enthält Informationen zu den Optionen IPsec und Internet Key Exchange (IKE), die für jeden Tunnel verfügbar sind.
- AWS Site-to-Site VPN Optionen für die Tunnelauthentifizierung: Enthält Informationen zu den Authentifizierungsoptionen für Ihre VPN-Tunnelendpunkte.
- Anforderungen für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät: Enthält Informationen über die Anforderungen an das Kunden-Gateway-Gerät auf Ihrer Seite der VPN-Verbindung.
- Sichere Kommunikation zwischen AWS Site-to-Site VPN Verbindungen mithilfe von VPN CloudHub: Wenn Sie über mehrere Site-to-Site VPN-Verbindungen verfügen, können Sie mithilfe des AWS VPN CloudHub eine sichere Kommunikation zwischen Ihren lokalen Standorten bereitstellen.

# Identitäts- und Zugriffsmanagement für VPN AWS Site-to-Site

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um VPN-Ressourcen zu nutzen Site-to-Site. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen


- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie funktioniert AWS Site-to-Site VPN mit IAM
- Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site
- Fehlerbehebung bei AWS Site-to-Site VPN-Identität und VPN-Zugriff
- AWS verwaltete Richtlinien für VPN Site-to-Site
- Verwenden von dienstverknüpften Rollen für VPN Site-to-Site


## Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie im Site-to-Site VPN ausführen.

Dienstbenutzer — Wenn Sie den Site-to-Site VPN-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr Site-to-Site VPN-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Site-to-Site VPN nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei AWS Site-to-Site VPN-Identität und VPN-Zugriff.

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für Site-to-Site VPN-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Site-to-Site VPN. Es ist Ihre Aufgabe, zu bestimmen, auf welche Site-to-Site VPN-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Site-to-Site VPN nutzen kann, finden Sie unterWie funktioniert AWS Site-to-Site VPN mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des VPN-Zugriffs schreiben können. Site-to-Site Beispiele für identitätsbasierte Site-to-Site VPN-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

# Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

## AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-

Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

## Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

# Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

## Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto.

Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

## Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

## Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der

identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

## Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

# Wie funktioniert AWS Site-to-Site VPN mit IAM

Bevor Sie IAM zur Verwaltung des Site-to-Site VPN-Zugriffs verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen mit VPN verwendet werden können. Site-to-Site

IAM-Funktionen, die Sie mit VPN verwenden können AWS Site-to-Site

| IAM-Feature | Site-to-Site VPN-Unterstützung |
| --- | --- |
| Identitätsbasierte Richtlinien | Ja |
| Ressourcenbasierte Richtlinien | Nein |
| Richtlinienaktionen | Ja |
| Richtlinienressourcen | Ja |
| Richtlinienbedingungsschlüssel (services pezifisch) | Ja |
| ACLs | Nein |
| ABAC (Tags in Richtlinien) | Nein |
| Temporäre Anmeldeinformationen | Ja |
| Prinzipalberechtigungen | Ja |
| Servicerollen | Ja |
| Service-verknüpfte Rollen | Ja |

Einen allgemeinen Überblick darüber, wie Site-to-Site VPN und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

## Identitätsbasierte Richtlinien für VPN Site-to-Site

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für VPN Site-to-Site

Beispiele für identitätsbasierte Site-to-Site VPN-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

## Ressourcenbasierte Richtlinien innerhalb von VPN Site-to-Site

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen.

Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

## Richtlinienaktionen für VPN Site-to-Site

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Site-to-Site VPN-Aktionen finden Sie unter Von AWS Site-to-Site VPN definierte Aktionen in der Serviceautorisierungsreferenz.

Richtlinienaktionen in Site-to-Site VPN verwenden vor der Aktion das folgende Präfix:

```
ec2
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Beispiele für identitätsbasierte Site-to-Site VPN-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

## Richtlinienressourcen für VPN Site-to-Site

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der Site-to-Site VPN-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von AWS Site-to-Site VPN definierte Ressourcen in der Service Authorization Reference. Informationen dazu, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Site-to-Site VPN definierte Aktionen.

Beispiele für identitätsbasierte Site-to-Site VPN-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

## Bedingungsschlüssel für Richtlinien für VPN Site-to-Site

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Site-to-Site VPN-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Site-to-Site VPN in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Site-to-Site VPN definierte Aktionen.

Beispiele für identitätsbasierte Site-to-Site VPN-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

## ACLs im VPN Site-to-Site

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

## ABAC mit VPN Site-to-Site

Unterstützt ABAC (Tags in Richtlinien): Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

## Verwenden temporärer Anmeldeinformationen mit VPN Site-to-Site

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

## Serviceübergreifende Prinzipalberechtigungen für VPN Site-to-Site

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

## Servicerollen für VPN Site-to-Site

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Site-to-Site VPN-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Site-to-Site VPN Sie dazu anleitet.

## Dienstbezogene Rollen für VPN Site-to-Site

Unterstützt dienstverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

# Beispiele für identitätsbasierte Richtlinien für VPN AWS Site-to-Site

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Site-to-Site VPN-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Site-to-Site VPN definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Site-to-Site VPN in der Service Authorization Reference.

Themen


- Bewährte Methoden für Richtlinien
- Verwenden der VPN-Konsole Site-to-Site
- Beschreiben Sie spezifische Site-to-Site VPN-Verbindungen
- Erstellen und beschreiben Sie die für eine AWS Site-to-Site VPN Verbindung benötigten Ressourcen


## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Site-to-Site VPN-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden

Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

## Verwenden der VPN-Konsole Site-to-Site

Um auf die AWS Site-to-Site VPN-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Site-to-Site VPN-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Site-to-Site VPN-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch das Site-to-Site VPN `AmazonVPCFullAccess` oder die `AmazonVPCReadOnlyAccess` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

## Beschreiben Sie spezifische Site-to-Site VPN-Verbindungen

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
      }
   ]
}
```

## Erstellen und beschreiben Sie die für eine AWS Site-to-Site VPN Verbindung benötigten Ressourcen

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
```

```
            "Action": [
            "ec2:DescribeVpnConnections",
            "ec2:DescribeVpnGateways",
            "ec2:DescribeCustomerGateways",
            "ec2:CreateCustomerGateway",
            "ec2:CreateVpnGateway",
            "ec2:CreateVpnConnection"
            ],
            "Resource": [
               "*"
            ]
         },
      {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
            "Condition": {
               "StringLike": {
                  "iam:AWSServiceName":"s2svpn.amazonaws.com"
               }
            }
         }
      ]
}
```

## Fehlerbehebung bei AWS Site-to-Site VPN-Identität und VPN-Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Site-to-Site VPN und IAM auftreten können.

Themen


- Ich bin nicht berechtigt, eine Aktion in Site-to-Site VPN durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Site-to-Site VPN-Ressourcen ermöglichen

## Ich bin nicht berechtigt, eine Aktion in Site-to-Site VPN durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `ec2:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `ec2:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Site-to-Site VPN übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Site-to-Site VPN auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

### Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Site-to-Site VPN-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Site-to-Site VPN diese Funktionen unterstützt, finden Sie unter. Wie funktioniert AWS Site-to-Site VPN mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

## AWS verwaltete Richtlinien für VPN Site-to-Site

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS

verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

## AWS verwaltete Richtlinie: AWSVPCS2 SVpn ServiceRolePolicy

Sie können die `AWSVPCS2SVpnServiceRolePolicy`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie ermöglicht es Site-to-Site VPN, ein AWS Secrets Manager Geheimnis innerhalb des Site-to-Site VPN zu verwalten. Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSVPCS2SVpnServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

## Site-to-Site VPN-Updates für AWS verwaltete Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für Site-to-Site VPN, seit dieser Dienst im Mai 2025 damit begonnen hat, diese Änderungen zu verfolgen.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| AWSVPCS2SVpnServiceRolePolicy- Aktualisierte Richtlinie. | Der Richtlinie wurden neue Berechtigungen hinzugefügt, die es Site-to-Site VPN ermöglichen, das AWS Secrets Manager `s2svpn` verwaltete Geheimnis der VPN-Verbindung zu verwalten. | 14. Mai 2025 |

# Verwenden von dienstverknüpften Rollen für VPN Site-to-Site

AWS Site-to-Site VPN verwendet AWS Identity and Access Management dienstgebundene Rollen (IAM). Eine dienstgebundene Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit VPN verknüpft ist. Site-to-Site Dienstbezogene Rollen sind von Site-to-Site VPN vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Site-to-Site VPN, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Site-to-Site VPN definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur Site-to-Site VPN seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Site-to-Site VPN-Ressourcen, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

## Mit dem Dienst verknüpfte Rollenberechtigungen für VPN Site-to-Site

Site-to-Site VPN verwendet die dienstgebundene Rolle mit dem Namen AWSServiceRoleForVPCS2SVPN — Erlaubt Site-to-Site VPN, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

Die dienstgebundene AWSService RoleFor VPCS2 SVPN-Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `s2svpn.amazonaws.com`

Diese dienstbezogene Rolle verwendet die verwaltete Richtlinie AWSVPCS2 SVpnServiceRolePolicy , um die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Wenn Sie die Zertifikatsauthentifizierung für Ihre VPN-Verbindung verwenden, werden die AWS Certificate Manager VPN-Tunnelzertifikate zur Verwendung auf den VPN-Tunnelendpunkten AWS Site-to-Site VPN exportiert.
- AWS Site-to-Site VPN Verwaltet die Erneuerung der VPN-Tunnelzertifikate, wenn Sie die AWS Certificate Manager Zertifikatsauthentifizierung für Ihre VPN-Verbindung verwenden.

- Wenn Sie SecretsManager Pre-Shared-Schlüsselspeicher für Ihre VPN-Verbindung verwenden, AWS Site-to-Site VPN verwaltet es den von AWS Secrets Manager s2svpn verwalteten geheimen Schlüssel der VPN-Verbindung.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSVPCS2SVpnServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

## Erstellen Sie eine dienstbezogene Rolle für VPN Site-to-Site

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Kunden-Gateway mit einem zugehörigen privaten ACM-Zertifikat in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt Site-to-Site VPN die dienstbezogene Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Kunden-Gateway mit einem zugehörigen privaten ACM-Zertifikat erstellen, erstellt Site-to-Site VPN die dienstbezogene Rolle erneut für Sie.

## Bearbeiten Sie eine dienstverknüpfte Rolle für VPN Site-to-Site

Site-to-Site VPN erlaubt es Ihnen nicht, die dienstverknüpfte AWSService RoleFor VPCS2 SVPN-Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer Beschreibung einer dienstbezogenen Rolle im IAM-Benutzerhandbuch.

## Löschen Sie eine dienstverknüpfte Rolle für VPN Site-to-Site

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der Site-to-Site VPN-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um vom Site-to-Site AWSService RoleFor VPCS2 SVPN verwendete VPN-Ressourcen zu löschen

Sie können diese serviceverknüpfte Rolle erst löschen, nachdem Sie alle Kunden-Gateways gelöscht haben, denen ein privates ACM-Zertifikat zugeordnet ist. Dadurch wird sichergestellt, dass Sie nicht versehentlich die Erlaubnis zum Zugriff auf Ihre ACM-Zertifikate entfernen können, die von VPN-Verbindungen verwendet werden. Site-to-Site

So löschen Sie die -servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API, um die AWS CLI mit dem SVPN-Dienst verknüpfte Rolle zu löschen. AWSService RoleFor VPCS2 Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

# Resilienz in AWS Site-to-Site VPN

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Site-to-Site VPN Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

## Zwei Tunnel pro VPN-Verbindung

Eine Site-to-Site VPN-Verbindung besteht aus zwei Tunneln, die jeweils in einer anderen Availability Zone enden, um die Verfügbarkeit Ihrer VPC zu erhöhen. Wenn innerhalb des Tunnels ein Gerät ausfällt AWS, wechselt Ihre VPN-Verbindung automatisch zum zweiten Tunnel, sodass Ihr Zugriff nicht unterbrochen wird. Führt von Zeit zu Zeit AWS auch routinemäßige Wartungsarbeiten an Ihrer VPN-Verbindung durch, wodurch einer der beiden Tunnel Ihrer VPN-Verbindung kurzzeitig deaktiviert werden kann. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Ersatz von Tunnelendpunkten. Konfigurieren Sie beim Konfigurieren Ihres Kunden-Gateways daher unbedingt beide Tunnel.

## Redundanz

Um sich vor einem Verbindungsverlust zu schützen, falls Ihr Kunden-Gateway nicht verfügbar sein sollte, können Sie eine zweite Site-to-Site VPN-Verbindung einrichten. Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Redundante AWS Site-to-Site VPN Verbindungen für Failover
- Amazon Virtual Private Cloud Connectivity Options
- Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS

# Sicherheit der Infrastruktur in VPN AWS Site-to-Site

Als verwalteter Dienst ist AWS Site-to-Site VPN durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Site-to-Site VPN zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

# Überwachen Sie eine AWS Site-to-Site VPN Verbindung

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Site-to-Site VPN Verbindung. Sie sollten von allen Teilen Ihrer Lösung Überwachungsdaten sammeln, damit Sie bei Ausfällen, die sich über mehrere Punkte erstrecken, leichter debuggen können. Bevor Sie mit der Überwachung Ihrer Site-to-Site VPN-Verbindung beginnen, sollten Sie jedoch einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Im nächsten Schritt legen Sie einen Ausgangswert für eine normale VPN-Leistung in Ihrer Umgebung fest, indem Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen messen. Speichern Sie bei der Überwachung Ihres VPN die historischen Überwachungsdaten, damit Sie diese mit aktuellen Leistungsdaten vergleichen, normale Leistungsmuster bestimmen, Leistungsprobleme erkennen und Methoden zur Fehlerbehebung ableiten können.

Zur Festlegung eines Grundwertes sollten Sie die folgenden Elemente überwachen:

- Den Zustand der VPN-Tunnel
- Eingehende Daten in den Tunnel
- Ausgehende Daten aus dem Tunnel

Themen


- Überwachungstools
- AWS Site-to-Site VPN Logs
- Überwachen Sie AWS Site-to-Site VPN Tunnel mit Amazon CloudWatch
- AWS Health und AWS Site-to-Site VPN Ereignisse

# Überwachungstools

AWS bietet verschiedene Tools, mit denen Sie eine Site-to-Site VPN-Verbindung überwachen können. Sie können einige dieser Tools so konfigurieren, dass diese die Überwachung für Sie übernehmen, während bei anderen Tools ein manuelles Eingreifen nötig ist. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

## Automatisierte Überwachungstools

Sie können die folgenden automatisierten Überwachungstools verwenden, um eine Site-to-Site VPN-Verbindung zu überwachen und zu melden, wenn etwas nicht stimmt:

- Amazon CloudWatch Alarms — Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS SNS-Thema gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter Überwachen Sie AWS Site-to-Site VPN Tunnel mit Amazon CloudWatch.
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Protokollverarbeitungsanwendungen in Java und stellen Sie sicher, dass sich Ihre Protokolldateien nach der Lieferung von CloudTrail nicht geändert haben. Weitere Informationen finden Sie unter Protokollieren von API-Aufrufen AWS CloudTrail in der Amazon EC2 API-Referenz und Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail Benutzerhandbuch.
- AWS Health Ereignisse — Erhalten Sie Warnmeldungen und Benachrichtigungen im Zusammenhang mit Änderungen im Zustand Ihrer Site-to-Site VPN-Tunnel, Empfehlungen zur Konfiguration bewährter Verfahren oder wenn Sie sich Skalierungsgrenzen nähern. Verwenden Sie Ereignisse auf dem Personal Health Dashboard, um automatisierte Failovers auszulösen, die Zeit für die Fehlerbehebung verkürzen oder Verbindungen für hohe Verfügbarkeit optimieren. Weitere Informationen finden Sie unter AWS Health und AWS Site-to-Site VPN Ereignisse.

## Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung einer Site-to-Site VPN-Verbindung besteht darin, die Elemente, die von den CloudWatch Alarmen nicht abgedeckt werden, manuell zu überwachen. Die

Amazon VPC- und CloudWatch Konsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand Ihrer AWS Umgebung.

> **Note**
>
> In der Amazon VPC-Konsole spiegeln Site-to-Site VPN-Tunnelstatusparameter wie „Status“ und „Letzte Statusänderung“ möglicherweise keine vorübergehenden Zustandsänderungen oder vorübergehende Tunnelflaps wider. Es wird empfohlen, CloudWatch Metriken und Protokolle für detaillierte Aktualisierungen von Tunnelstatusänderungen zu verwenden.

- Das Amazon VPC-Dashboard zeigt:
  - Zustand des Services nach Region
  - Site-to-Site VPN-Verbindungen
  - VPN-Tunnelstatus (Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen, wählen Sie eine Site-to-Site VPN-Verbindung und dann Tunneldetails aus)
- Auf der CloudWatch Startseite wird Folgendes angezeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

  Darüber hinaus können CloudWatch Sie Folgendes verwenden:
  - Erstellen angepasster Dashboards zur Überwachung der gewünschten Services.
  - Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen
  - Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden

# AWS Site-to-Site VPN Logs

AWS Site-to-Site VPN Protokolle bieten Ihnen einen tieferen Einblick in Ihre Site-to-Site VPN-Bereitstellungen. Mit dieser Funktion haben Sie Zugriff auf Site-to-Site VPN-Verbindungsprotokolle, die Einzelheiten zur Einrichtung eines IP-Security-Tunnels (IPsec), zu IKE-Verhandlungen (Internet Key Exchange) und zu DPD-Protokollnachrichten (Dead Peer Detection) enthalten.

Site-to-Site VPN-Protokolle können in Amazon CloudWatch Logs veröffentlicht werden. Diese Funktion bietet Kunden eine einzige konsistente Möglichkeit, auf detaillierte Protokolle für all ihre Site-to-Site VPN-Verbindungen zuzugreifen und diese zu analysieren.

Themen


- Vorteile von Site-to-Site VPN-Protokollen
- Größenbeschränkungen der Amazon CloudWatch Logs-Ressourcenrichtlinie
- Site-to-Site Inhalt des VPN-Protokolls
- IAM-Anforderungen für die Veröffentlichung in Logs CloudWatch
- Konfiguration der AWS Site-to-Site VPN Logs anzeigen
- AWS Site-to-Site VPN Logs aktivieren
- AWS Site-to-Site VPN Protokolle deaktivieren


## Vorteile von Site-to-Site VPN-Protokollen

- Vereinfachte VPN-Fehlerbehebung: Mithilfe von Site-to-Site VPN-Protokollen können Sie Konfigurationsunterschiede zwischen dem Gateway-Gerät AWS und Ihrem Kunden-Gateway-Gerät ermitteln und anfängliche Probleme mit der VPN-Konnektivität beheben. VPN-Verbindungen können im Laufe der Zeit aufgrund von falsch konfigurierten Einstellungen (z. B. schlecht abgestimmten Timeouts) zeitweise ausfallen, es kann zu Problemen in den zugrunde liegenden Transportnetzwerken kommen (z. B. Internetwetter) oder Routing-Änderungen bzw. Pfadfehler können zu einer Unterbrechung der Konnektivität über VPN führen. Mit dieser Funktion können Sie die Ursache von zeitweise auftretenden Verbindungsfehlern genau diagnostizieren und die Low-Level-Tunnelkonfiguration optimieren, um einen zuverlässigen Betrieb zu ermöglichen.
- Zentrale AWS Site-to-Site VPN Sichtbarkeit: Site-to-Site VPN-Protokolle können Tunnelaktivitätsprotokolle für all die verschiedenen Arten der Site-to-Site VPN-Verbindung bereitstellen: virtuelles Gateway, Transit Gateway und CloudHub sowohl über das Internet als auch AWS Direct Connect als Transport. Diese Funktion bietet Kunden eine einzige konsistente Möglichkeit, auf detaillierte Protokolle für all ihre Site-to-Site VPN-Verbindungen zuzugreifen und diese zu analysieren.
- Sicherheit und Compliance: Site-to-Site VPN-Protokolle können an Amazon CloudWatch Logs gesendet werden, um den Status und die Aktivität der VPN-Verbindung im Laufe der Zeit rückwirkend zu analysieren. Dies hilft Ihnen, Compliance-Anforderungen und gesetzliche Vorschriften besser einzuhalten.

## Größenbeschränkungen der Amazon CloudWatch Logs-Ressourcenrichtlinie

CloudWatch Die Ressourcenrichtlinien für Logs sind auf 5120 Zeichen begrenzt. Wenn CloudWatch Logs feststellt, dass sich eine Richtlinie dieser Größenbeschränkung nähert, werden automatisch Protokollgruppen aktiviert, die mit `/aws/vendedlogs/` beginnen. Wenn Sie die Protokollierung aktivieren, muss Site-to-Site VPN Ihre CloudWatch Logs-Ressourcenrichtlinie mit der von Ihnen angegebenen Protokollgruppe aktualisieren. Um zu verhindern, dass die Größenbeschränkung der CloudWatch Protokollressourcenrichtlinie erreicht wird, stellen Sie Ihren Protokollgruppennamen ein Präfix voran`/aws/vendedlogs/`.

## Site-to-Site Inhalt des VPN-Protokolls

Die folgenden Informationen sind im Site-to-Site VPN-Tunnel-Aktivitätsprotokoll enthalten. Der Name der Protokollstream-Datei verwendet VpnConnection ID und TunnelOutsideIPAddress.

| Feld | Beschreibung |
| --- | --- |
| VpnLogCreationTimestamp (`event_timestamp` ) | Zeitstempel für die Protokollerstellung in vom Menschen lesbarem Format. |
| Tunnel DPDEnabled (`dpd_enabled` ) | Status Dead-Peer-Detection-Protokoll aktiviert (Wahr/Falsch). |
| CGWNATTDetectionTunnelstatus (`nat_t_detected` ) | NAT-T auf dem Kunden-Gateway-Gerät erkannt (Wahr/Falsch). |
| IKEPhase1Tunnelstatus (`ike_phase1_state` ) | IKE-Phase-1-Protokollstatus (Established (Eingerichtet) \| Rekeying (Erneute Schlüssel erstellung) \| Negotiating (Aushandlung) \| Down (Ausgefallen)). |
| IKEPhase2Tunnelstaat (`ike_phase2_state` ) | IKE-Phase-2-Protokollstatus (Established (Eingerichtet) \| Rekeying (Erneute Schlüssel erstellung) \| Negotiating (Aushandlung) \| Down (Ausgefallen)). |

| Feld | Beschreibung |
| --- | --- |
| VpnLogDetail (`details`) | Ausführliche Meldungen für die Protokolle IPsec IKE und DPD. |

Inhalt


- IKEv1 Fehlermeldungen
- IKEv2 Fehlermeldungen
- IKEv2 Verhandlungsnachrichten


## IKEv1 Fehlermeldungen

| Fehlermeldung | Erklärung |
| --- | --- |
| Peer reagiert nicht – Peer wird für tot erklärt | Peer hat nicht auf DPD-Nachrichten geantwortet und damit eine DPD-Timeout-Aktion durchgesetzt. |
| AWS Die Entschlüsselung der Tunnel-Payloads war aufgrund eines ungültigen Pre-Shared Keys nicht erfolgreich | Derselbe vorinstallierte Schlüssel muss auf beiden IKE-Peers konfiguriert werden. |
| Es wurde kein passender Vorschlag gefunden von AWS | Vorgeschlagene Attribute für Phase 1 (Verschlüsselung, Hashing und DH-Gruppe) werden von AWS VPN Endpoint nicht unterstützt — zum Beispiel`3DES`. |
| Keine Übereinstimmung mit Vorschlag gefunden. Benachrichtigen mit „Kein Vorschlag ausgewählt“ | Zwischen den Peers wird die Fehlermeldung „Kein Vorschlag ausgewählt“ ausgetauscht, um mitzuteilen, dass für Phase 2 die richtigen Vorschläge/Richtlinien auf IKE-Peers konfiguriert werden müssen. |
| AWS Der Tunnel hat DELETE für Phase 2 SA mit SPI: xxxx erhalten | CGW hat die Delete_SA-Nachricht für Phase 2 gesendet. |

| Fehlermeldung | Erklärung |
| --- | --- |
| AWS Der Tunnel hat DELETE für IKE_SA von CGW erhalten | CGW hat die Delete_SA-Nachricht für Phase 1 gesendet. |

## IKEv2 Fehlermeldungen

| Fehlermeldung | Erklärung |
| --- | --- |
| AWS Tunnel-DPD-Timeout nach erneuten Übertragungen durch {retry_count} | Peer hat nicht auf DPD-Nachrichten geantwort et und damit eine DPD-Timeout-Aktion durchgesetzt. |
| AWS Der Tunnel hat DELETE für IKE_SA von CGW erhalten | Peer hat die Delete_SA-Nachricht für Parent/IK E_SA gesendet. |
| AWS Der Tunnel hat DELETE für Phase 2 SA mit SPI: xxxx empfangen | Peer hat die Delete_SA-Nachricht für CHILD_SA gesendet. |
| AWS Der Tunnel hat eine Kollision (CHILD_RE KEY) als CHILD_DELETE erkannt | CGW hat die Delete_SA-Nachricht für die Active SA gesendet, die gerade erneut eingegeben wird. |
| AWS Die redundante SA von tunnel (CHILD_SA) wurde aufgrund einer erkannten Kollision gelöscht | Wenn aufgrund einer Kollision redundante Verbindungen generiert SAs werden, schließen Peers redundante SA, nachdem sie die Nonce-Werte gemäß RFC abgeglichen haben. |
| AWS Der Tunnel von Phase 2 konnte nicht eingerichtet werden, während Phase 1 beibehalten wurde | Peer konnte CHILD_SA aufgrund eines Verhandlungsfehlers nicht einrichten, z. B. aufgrund eines falschen Vorschlags. |
| AWS: Traffic Selector: TS_INACLECT: vom Responder empfangen | Peer hat falsche Traffic Selectors/Encryption Domain vorgeschlagen. Peers sollten identisch und korrekt konfiguriert sein. CIDRs |

| Fehlermeldung | Erklärung |
| --- | --- |
| AWS Der Tunnel sendet AUTHENTIC ATION_FAILED als Antwort | Der Peer kann den Peer nicht authentifizieren, indem er den Inhalt der IKE_AUTH-Nachricht überprüft |
| AWS Der Tunnel hat festgestellt, dass der Pre-Shared-Key nicht mit cgw übereinstimmt: xxxx | Derselbe vorinstallierte Schlüssel muss auf beiden IKE-Peers konfiguriert werden. |
| AWS Tunnel-Timeout: Löschen des nicht eingerichteten Phase-1-IKE_SA mit cgw: xxxx | Beim Löschen des halb geöffneten IKE_SA als Peer wurden keine Verhandlungen geführt |
| Keine Übereinstimmung mit Vorschlag gefunden. Benachrichtigen mit „Kein Vorschlag ausgewählt“ | Zwischen den Peers wird die Fehlermeldung „Kein Vorschlag ausgewählt“ ausgetauscht, um mitzuteilen, dass die richtigen Vorschläge auf IKE-Peers konfiguriert werden müssen. |
| Es wurde kein passender Vorschlag gefunden von AWS | Vorgeschlagene Attribute für Phase 1 oder Phase 2 (Verschlüsselung, Hashing und DH-Gruppe) werden von AWS VPN Endpoint nicht unterstützt — zum Beispiel`3DES`. |

## IKEv2 Verhandlungsnachrichten

| Fehlermeldung | Erklärung |
| --- | --- |
| AWS Die Anfrage (id=xxx) für CREATE_CH ILD_SA wurde vom Tunnel verarbeitet | AWS hat die CREATE_CHILD_SA-Anfrage von CGW erhalten. |
| AWS Der Tunnel sendet eine Antwort (id=xxx) für CREATE_CHILD_SA | AWS sendet eine CREATE_CHILD_SA-Antwort an CGW. |
| AWS Der Tunnel sendet eine Anfrage (id=xxx) für CREATE_CHILD_SA | AWS sendet eine CREATE_CHILD_SA-An frage an CGW. |
| AWS Die Antwort (id=xxx) für CREATE_CH ILD_SA wurde vom Tunnel verarbeitet | AWS hat eine CREATE_CHILD_SA-Antwort von CGW erhalten. |

# IAM-Anforderungen für die Veröffentlichung in Logs CloudWatch

Damit die Protokollierungsfunktion ordnungsgemäß funktioniert, muss die an den IAM-Prinzipal angefügte IAM-Richtlinie, die zur Konfiguration der Funktion verwendet wird, mindestens die folgenden Berechtigungen enthalten. Weitere Informationen finden Sie auch im Abschnitt Aktivieren der Protokollierung für bestimmte AWS Dienste im Amazon CloudWatch Logs-Benutzerhandbuch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Konfiguration der AWS Site-to-Site VPN Logs anzeigen

Sehen Sie sich das Aktivitätsprotokoll für eine Site-to-Site VPN-Verbindung an. Hier können Sie Details zur Konfiguration einsehen, z. B. zu Verschlüsselungsalgorithmen, oder ob Tunnel-VPN-Protokolle aktiviert sind. Sie können auch den Tunnelstatus einsehen. Auf diese Weise können Sie Probleme oder Konflikte, die Sie möglicherweise mit einer VPN-Verbindung haben, besser verfolgen.

So zeigen Sie die aktuellen Tunnelprotokollierungseinstellungen an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie in der Liste VPN connections (VPN–Verbindungen) die VPN-Verbindung aus, die Sie anzeigen möchten.
4. Wählen Sie die Registerkarte Tunnel details (Tunneldetails) aus.
5. Erweitern Sie die Abschnitte Tunnel 1 options (Tunnel-1-Optionen) und Tunnel 2 options (Tunnel-2-Optionen), um alle Details der Tunnelkonfiguration anzuzeigen.
6. Sie können den aktuellen Status der Protokollierungsfunktion unter Tunnel-VPN-Protokoll und die aktuell konfigurierte CloudWatch Protokollgruppe (falls vorhanden) unter CloudWatch Protokollgruppe anzeigen.

Um die aktuellen Tunnelprotokollierungseinstellungen für eine Site-to-Site VPN-Verbindung über die AWS Befehlszeile oder API anzuzeigen

- DescribeVpnConnections(Amazon EC2 Query API)
- describe-vpn-connections (AWS CLI)

## AWS Site-to-Site VPN Logs aktivieren

Aktivieren Sie Site-to-Site VPN-Protokolle, um VPN-Aktivitäten wie den Tunnelstatus und andere Details zu protokollieren. Sie können die Protokollierung für eine neue Verbindung aktivieren oder eine bestehende Verbindung ändern, um mit der Protokollierung von Aktivitäten zu beginnen. Wenn Sie die Protokollierung für eine Verbindung deaktivieren möchten, finden Sie weitere Informationen unterDeaktivieren Sie Site-to-Site VPN-Protokolle.

> **Note**
>
> Wenn Sie Site-to-Site VPN-Protokolle für einen bestehenden VPN-Verbindungstunnel aktivieren, kann Ihre Konnektivität über diesen Tunnel für mehrere Minuten unterbrochen werden. Um hohe Verfügbarkeit zu gewährleisten, bietet jede VPN-Verbindung jedoch zwei Tunnel, sodass Sie die Protokollierung für jeweils einen Tunnel aktivieren können, während die Konnektivität über den Tunnel erhalten bleibt, der nicht geändert wird. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Ersatz von Tunnelendpunkten.

Um die VPN-Protokollierung beim Erstellen einer neuen Site-to-Site VPN-Verbindung zu aktivieren

Folgen Sie dem Verfahren unter Schritt 5: Eine VPN-Verbindung erstellen. In Schritt 9, Tunnel Options (Tunneloptionen), können Sie alle Optionen angeben, die Sie für beide Tunnel verwenden möchten, einschließlich Optionen für die VPN-Protokollierung. Weitere Informationen zu diesen Optionen finden Sie unter Tunneloptionen für Ihre AWS Site-to-Site VPN Verbindung.

Um die Tunnelprotokollierung für eine neue Site-to-Site VPN-Verbindung über die AWS Befehlszeile oder API zu aktivieren

- CreateVpnConnection(Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)

Um die Tunnelprotokollierung für eine bestehende Site-to-Site VPN-Verbindung zu aktivieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie in der Liste VPN connections (VPN-Verbindungen) die VPN-Verbindung aus, die Sie ändern möchten.
4. Wählen Sie Actions (Aktionen), Modify VPN tunnel options (VPN-Tunneloptionen ändern) aus.
5. Wählen Sie den zu ändernden Tunnel aus, indem Sie die entsprechende IP-Adresse in der Liste VPN tunnel outside IP address (Externe IP-Adresse des VPN-Tunnels) auswählen.
6. Wählen Sie unter Tunnel activity log (Tunnelaktivitätsprotokoll) die Option Enable (Aktivieren) aus.
7. Wählen Sie unter  CloudWatch Amazon-Protokollgruppe die CloudWatch Amazon-Protokollgruppe aus, an die die Protokolle gesendet werden sollen.

8. (Optional) Wählen Sie unter Output format (Ausgabeformat) das gewünschte Format für die Protokollausgabe: json oder Text.
9. Wählen Sie Save Changes (Änderungen speichern) aus.
10. (Optional) Wiederholen Sie die Schritte 4 bis 9 gegebenenfalls für den anderen Tunnel.

Um die Tunnelprotokollierung für eine bestehende Site-to-Site VPN-Verbindung über die AWS Befehlszeile oder API zu aktivieren

- ModifyVpnTunnelOptions(Amazon EC2 Query API)
- modify-vpn-tunnel-options (AWS CLI)

## AWS Site-to-Site VPN Protokolle deaktivieren

Deaktivieren Sie die VPN-Protokollierung für eine Verbindung, wenn Sie keine Aktivitäten auf dieser Verbindung mehr verfolgen möchten. Diese Aktion deaktiviert nur die Protokollierung und wirkt sich auf nichts anderes für diese Verbindung aus. Informationen zum Aktivieren oder erneuten Aktivieren der Protokollierung für eine Verbindung finden Sie unter. Site-to-SiteVPN-Protokolle aktivieren

Um die Tunnelprotokollierung für eine Site-to-Site VPN-Verbindung zu deaktivieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Connections aus.
3. Wählen Sie in der Liste VPN connections (VPN-Verbindungen) die VPN-Verbindung aus, die Sie ändern möchten.
4. Wählen Sie Actions (Aktionen), Modify VPN tunnel options (VPN-Tunneloptionen ändern) aus.
5. Wählen Sie den zu ändernden Tunnel aus, indem Sie die entsprechende IP-Adresse in der Liste VPN tunnel outside IP address (Externe IP-Adresse des VPN-Tunnels) auswählen.
6. Deaktivieren Sie unter Tunnel activity log (Tunnelaktivitätsprotokoll) die Option Enable (Aktivieren).
7. Wählen Sie Save Changes (Änderungen speichern) aus.
8. (Optional) Wiederholen Sie die Schritte 4 bis 7 gegebenenfalls für den anderen Tunnel.

Um die Tunnelprotokollierung für eine Site-to-Site VPN-Verbindung über die AWS Befehlszeile oder API zu deaktivieren

- ModifyVpnTunnelOptions(Amazon EC2 Query API)
- modify-vpn-tunnel-options (AWS CLI)

# Überwachen Sie AWS Site-to-Site VPN Tunnel mit Amazon CloudWatch

Sie können VPN-Tunnel überwachen CloudWatch, indem Rohdaten aus dem VPN-Dienst gesammelt und in lesbare Messwerte umgewandelt werden, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. VPN-Metrikdaten werden automatisch an sie gesendet, CloudWatch sobald sie verfügbar sind.

Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt


- VPN-Metriken und Dimensionen
- Amazon CloudWatch Logs-Metriken anzeigen für AWS Site-to-Site VPN
- Erstellen Sie CloudWatch Amazon-Alarme zur Überwachung von AWS Site-to-Site VPN Tunneln


## VPN-Metriken und Dimensionen

Die folgenden CloudWatch Messwerte sind für Ihre Site-to-Site VPN-Verbindungen verfügbar.

| Metrik | Beschreibung |
| --- | --- |
| `TunnelState` | Der Status des Tunnels. Bei statischen VPNs Werten steht 0 für DOWN und 1 für UP. Für BGP VPNs steht 1 für ESTABLISHED und 0 wird für alle anderen Status verwendet. Für beide Typen von bedeuten Werte zwischen 0 und 1 VPNs, dass mindestens ein Tunnel nicht AKTIV ist. |

| Metrik | Beschreibung |
| --- | --- |
| | Einheiten: Bruchwert zwischen 0 und 1 |
| `TunnelDataIn` † | Die Byte, die auf der AWS Verbindungsseite durch den VPN-Tunnel von einem Kunden-Gateway empfangen wurden. Jeder Metrikdat enpunkt stellt die Anzahl der nach dem vorangegangenen Datenpunkt empfangen en Byte dar. Verwenden Sie die Summensta tistik, um die Gesamtanzahl der während des Zeitraums empfangenen Byte anzuzeigen.<br><br>Diese Metrik zählt die Daten nach deren Entschlüsselung.<br><br>Einheiten: Byte |
| `TunnelDataOut` † | Die Byte, die von der AWS Verbindungsseite durch den VPN-Tunnel zum Kunden-Gateway gesendet werden. Jeder Metrikdatenpunkt stellt die Anzahl der nach dem vorangegangenen Datenpunkt gesendeten Byte dar. Verwenden Sie die Summenstatistik, um die Gesamtanzahl der während des Zeitraums gesendeten Byte anzuzeigen.<br><br>Diese Metrik zählt die Daten vor deren Verschlüsselung.<br><br>Einheiten: Byte |

† Diese Metriken können die Netzwerkauslastung auch dann melden, wenn der Tunnel ausgefallen ist. Dies liegt an regelmäßigen Statusprüfungen, die am Tunnel durchgeführt werden, und auf Hintergrund-ARP- und BGP-Anfragen.

Verwenden Sie die nachstehenden Dimensionen, um die Metrikdaten zu filtern.

| Dimension | Beschreibung |
| --- | --- |
| `VpnId` | Filtert die Metrikdaten nach der Site-to-Site VPN-Verbindungs-ID . |
| `TunnelIpAddress` | Filtert die Metrikdaten nach der IP-Adresse des Tunnels für das virtuelle private Gateway. |

## Amazon CloudWatch Logs-Metriken anzeigen für AWS Site-to-Site VPN

Wenn Sie eine Site-to-Site VPN-Verbindung herstellen, sendet der VPN-Dienst Metriken zu Ihrer VPN-Verbindung an CloudWatch, sobald diese verfügbar sind. Sie können -Metriken für Ihre VPN-Verbindungen wie folgt anzeigen.

So zeigen Sie Messwerte mithilfe der CloudWatch Konsole an

Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert.

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie unter All metrics den Metriknamespace VPN aus.
4. Wählen Sie die Metrikdimension aus, um die Metriken anzuzeigen, z. B. VPN-Tunnel-Metriken.

> **Note**
>
> Der VPN-Namespace wird erst in der CloudWatch Konsole angezeigt, nachdem in der angezeigten AWS Region eine Site-to-Site VPN-Verbindung hergestellt wurde.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

# Erstellen Sie CloudWatch Amazon-Alarme zur Überwachung von AWS Site-to-Site VPN Tunneln

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und sendet eine Benachrichtigung an ein Amazon SNS-Thema, die vom Wert der Metrik im Verhältnis zu einem vorgegebenen Schwellenwert in einer Reihe von Zeiträumen abhängt.

Sie können beispielsweise einen Alarm einrichten, der den Status eines einzelnen VPN-Tunnels überwacht und eine Benachrichtigung sendet, wenn der Tunnelstatus in 3 Datenpunkten innerhalb von 15 Minuten „DOWN“ lautet.

So erstellen Sie einen Alarm für einen einzelnen Tunnelstatus

1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/
2. Erweitern Sie im Navigationsbereich Alarme, dann Alle Alarme.
3. Wählen Sie Alarm erstellen und dann Metrik auswählen aus.
4. Wählen Sie VPN und dann VPN-Tunnelmetriken aus.
5. Wählen Sie die IP-Adresse des gewünschten Tunnels in derselben Zeile wie die TunnelStateMetrik aus. Wählen Sie Select metric (Metrik auswählen) aus.
6. Denn wann immer TunnelState ist... , wählen Sie Niedriger und geben Sie dann „1" in das Eingabefeld unter als... ein .
7. Legen Sie unter Zusätzliche Konfiguration die Eingaben für Zu alarmierende Datenpunkte auf „3 von 3“ fest.
8. Wählen Sie Weiter.
9. Wählen Sie unter Eine Benachrichtigung an das folgende SNS-Thema senden eine vorhandene Benachrichtigungsliste aus oder erstellen Sie eine neue.
10. Wählen Sie Weiter.
11. Geben Sie einen Namen für den Alarm ein. Wählen Sie Weiter.
12. Überprüfen Sie die Einstellungen für Ihren Alarm, und wählen Sie dann Create alarm (Alarm erstellen) aus.

Sie können einen Alarm erstellen, der den Status der Site-to-Site VPN-Verbindung überwacht. Sie können z. B. einen Alarm erstellen, der eine Benachrichtigung sendet, wenn der Status eines oder beider Tunnel für einen Zeitraum von 5 Minuten DOWN (Ausgefallen) ist.

Um einen Alarm für den Site-to-Site VPN-Verbindungsstatus zu erstellen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Alarme, dann Alle Alarme.
3. Wählen Sie Alarm erstellen und dann Metrik auswählen aus.
4. Wählen Sie VPN und anschließend VPN Connection Metrics (VPN-Verbindungsmetriken) aus.
5. Wählen Sie Ihre Site-to-Site VPN-Verbindung und die TunnelStateMetrik aus. Wählen Sie Select metric (Ausgewählte Metrik) aus.
6. Geben Sie bei Statistic (Statistik) Maximum an.

   Wenn Sie Ihre Site-to-Site VPN-Verbindung so konfiguriert haben, dass beide Tunnel aktiv sind, können Sie alternativ die Statistik Minimum angeben, um eine Benachrichtigung zu senden, wenn mindestens ein Tunnel ausgefallen ist.
7. Wählen Sie für Jedes Mal die Option Kleiner/Gleich (<=) aus. Geben Sie 0 ein (oder 0.5, falls mindestens ein Tunnel ausgefallen ist). Wählen Sie Weiter.
8. Wählen Sie unter Select an SNS topic (Ein SNS-Thema auswählen) eine vorhandene Benachrichtigungsliste oder New list (Neue Liste) aus, um eine neue zu erstellen. Wählen Sie Weiter.
9. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter.
10. Überprüfen Sie die Einstellungen für Ihren Alarm, und wählen Sie dann Create alarm (Alarm erstellen) aus.

Sie können auch Alarme einrichten, die das Datenverkehrsvolumen überwachen, das in einen bzw. aus einem VPN-Tunnel kommt. Der folgende Alarm überwacht beispielsweise das Datenverkehrsvolumen, das von Ihrem Netzwerk in den VPN-Tunnel gesendet wird, und sendet eine Benachrichtigung, wenn innerhalb von 15 Minuten mehr als 5 000 000 Byte eingehen.

So erstellen Sie einen Alarm für eingehenden Netzwerkdatenverkehr

1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/
2. Erweitern Sie im Navigationsbereich Alarme, dann Alle Alarme.
3. Wählen Sie Alarm erstellen und dann Metrik auswählen aus.

4. Wählen Sie VPN und dann VPN Tunnel Metrics (VPN-Tunnelmetriken) aus.
5. Wählen Sie die IP-Adresse des VPN-Tunnels und die TunnelDataInMetrik aus. Wählen Sie Select metric (Ausgewählte Metrik) aus.
6. Geben Sie bei Statistic (Statistik) Sum (Summe) an.
7. Wählen Sie bei Period (Zeitraum) 15 minutes (15 Minuten) aus.
8. Wählen Sie für Whenever (Jedes Mal) die Option Greater/Equal (Größer/Gleich) (>=) aus, und geben Sie 5000000 ein. Wählen Sie Weiter.
9. Wählen Sie unter Select an SNS topic (Ein SNS-Thema auswählen) eine vorhandene Benachrichtigungsliste oder New list (Neue Liste) aus, um eine neue zu erstellen. Wählen Sie Weiter.
10. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter.
11. Überprüfen Sie die Einstellungen für Ihren Alarm, und wählen Sie dann Create alarm (Alarm erstellen) aus.

Der folgende Alarm überwacht das Datenverkehrsvolumen, das von VPN-Tunnel an Ihr Netzwerk gesendet wird, und sendet eine Benachrichtigung, wenn innerhalb von 15 Minuten weniger als 1 000 000 Byte eingehen.

So erstellen Sie einen Alarm für ausgehenden Netzwerkdatenverkehr

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Alarme, dann Alle Alarme.
3. Wählen Sie Alarm erstellen und dann Metrik auswählen aus.
4. Wählen Sie VPN und dann VPN Tunnel Metrics (VPN-Tunnelmetriken) aus.
5. Wählen Sie die IP-Adresse des VPN-Tunnels und die TunnelDataOutMetrik aus. Wählen Sie Select metric (Ausgewählte Metrik) aus.
6. Geben Sie bei Statistic (Statistik) Sum (Summe) an.
7. Wählen Sie bei Period (Zeitraum) 15 minutes (15 Minuten) aus.
8. Wählen Sie für Whenever (Jedes Mal) die Option Lower/Equal (Kleiner/Gleich) (<=) aus, und geben Sie `1000000` ein. Wählen Sie Weiter.
9. Wählen Sie unter Select an SNS topic (Ein SNS-Thema auswählen) eine vorhandene Benachrichtigungsliste oder New list (Neue Liste) aus, um eine neue zu erstellen. Wählen Sie Weiter.
10. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter.

11. Überprüfen Sie die Einstellungen für Ihren Alarm, und wählen Sie dann Create alarm (Alarm erstellen) aus.

Weitere Beispiele für die Erstellung von Alarmen finden Sie unter CloudWatch Amazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

# AWS Health und AWS Site-to-Site VPN Ereignisse

AWS Site-to-Site VPN sendet automatisch Benachrichtigungen an die AWS Health Dashboard. Dieses Dashboard erfordert keine Einrichtung und ist für authentifizierte AWS Benutzer sofort einsatzbereit. Sie können mehrere Aktionen als Reaktion auf Ereignisbenachrichtigungen über das konfiguriere AWS Health Dashboard.

Das AWS Health Dashboard bietet die folgenden Arten von Benachrichtigungen für Ihre VPN-Verbindungen:

- Benachrichtigungen über den Austausch von Tunnel-Endpunkten
- VPN-Benachrichtigungen für einen einzelnen Tunnel

## Benachrichtigungen über den Austausch von Tunnel-Endpunkten

Sie erhalten eine Benachrichtigung über den Austausch von Tunnelendpunkten, AWS Health Dashboard wenn einer oder beide VPN-Tunnelendpunkte in Ihrer VPN-Verbindung ausgetauscht werden. Ein Tunnelendpunkt wird ersetzt, wenn AWS Tunnelaktualisierungen durchführt oder wenn Sie Ihre VPN-Verbindung ändern. Weitere Informationen finden Sie unter AWS Site-to-Site VPN Ersatz von Tunnelendpunkten.

Wenn der Austausch eines Tunnelendpunkts abgeschlossen ist, wird die Benachrichtigung über den Austausch des Tunnelendpunkts im Rahmen eines AWS Health Dashboard Ereignisses AWS gesendet.

## VPN-Benachrichtigungen für einen einzelnen Tunnel

Eine Site-to-Site VPN-Verbindung besteht aus Redundanzgründen aus zwei Tunneln. Wir empfehlen dringend, dass Sie beide Tunnel für hohe Verfügbarkeit konfigurieren. Wenn bei Ihrer VPN-Verbindung ein Tunnel aktiv ist, der andere jedoch für mehr als eine Stunde an einem Tag ausgefallen ist, erhalten Sie eine monatliche VPN-Einzeltunnel-Benachrichtigung über ein AWS

Health Dashboard -Ereignis. Dieses Ereignis wird täglich aktualisiert, sobald alle neuen VPN-Verbindungen als einziger Tunnel erkannt werden, wobei wöchentlich Benachrichtigungen gesendet werden. Jeden Monat wird ein neues Ereignis erstellt, das alle VPN-Verbindungen löscht, die nicht mehr als einzelner Tunnel erkannt werden.

# AWS Site-to-Site VPN Kontingente

Ihr AWS Konto hat die folgenden Kontingente, die früher als Limits bezeichnet wurden und sich auf Site-to-Site VPN beziehen. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um eine Kontingenterhöhung für ein einstellbares Kontingent zu beantragen, wählen Sie Ja in der Spalte Anpassbar. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

## Site-to-Site VPN-Ressourcen

| Name | Standard | Anpassbar |
| --- | --- | --- |
| Kunden-Gateways pro Region | 50 | Ja |
| Virtual Private Gateways pro Region | 5 | Ja |
| Site-to-Site VPN-Verbindungen pro Region | 50 | Ja |
| Site-to-Site VPN-Verbindungen pro virtuellem privaten Gateway | 10 | Ja |
| Beschleunigte Site-to-Site VPN-Verbindungen pro Region | 10 | Ja |
| Nicht verknüpfte Site-to-Site VPN-Verbi ndungen pro Region | 10 | Ja |

> **Note**
>
> Sowohl beschleunigte als auch nicht verknüpfte Verbindungen werden auf das Gesamtkontingent für Site-to-Site VPN-Verbindungen pro Region angerechnet.

Sie können jeweils ein Virtual Private Gateway an eine VPC anfügen. Um dieselbe Site-to-Site VPN-Verbindung mit mehreren zu verbinden VPCs, empfehlen wir Ihnen, stattdessen ein Transit-Gateway zu verwenden. Weitere Informationen finden Sie unter Transit-Gateways in Amazon VPC-Transit-Gateways.

Site-to-Site VPN-Verbindungen auf einem Transit-Gateway unterliegen der Gesamtanzahl von Transit-Gateway-Anhängen. Weitere Informationen finden Sie unter Transit-Gateway-Kontingente.

## Routen

Zu den angekündigten Routenquellen gehören VPC-Routen, andere VPN-Routen und Routen von virtuellen AWS Direct Connect -Schnittstellen. Die angekündigten Routen stammen aus der Routing-Tabelle für die VPN-Verbindung.

> **Note**
>
> Wenn Sie ein Virtual Private Gateway verwenden und die Route-Propagierung in Ihrer VPC-Routing-Tabelle aktiviert ist, werden automatisch sowohl dynamische als auch statische Routen für Ihre VPN-Verbindung hinzugefügt, bis das Limit der VPC-Routing-Tabelle erreicht wird. Weitere Informationen finden Sie unter Amazon-VPC-Kontingente im Amazon-VPC-Benutzerhandbuch.

| Name | Standard | Anpassbar |
| --- | --- | --- |
| Dynamische Routen, die von einem Kunden-Gateway-Gerät zu einer Site-to-Site VPN-Verbindung auf einem virtuellen privaten Gateway angekündigt werden | 100 | Nein |
| Von einer Site-to-Site VPN-Verbindung auf einem virtuellen privaten Gateway zu einem Kunden-Gateway-Gerät angekündigte Routen | 1.000 | Nein |
| Dynamische Routen, die von einem Kunden-Gateway-Gerät zu einer Site-to-Site VPN-Verbindung auf einem Transit-Gateway angekündigt werden | 1.000 | Nein |

| Name | Standard | Anpassbar |
| --- | --- | --- |
| Von einer Site-to-Site VPN-Verbindung auf einem Transit-Gateway zu einem Kunden-Gateway-Gerät angekündigte Routen | 5,000 | Nein |
| Statische Routen von einem Kunden-Gateway-Gerät zu einer Site-to-Site VPN-Verbindung auf einem virtuellen privaten Gateway | 100 | Nein |

## Bandbreite und Durchsatz

Es gibt viele Faktoren, die sich auf die durch eine Site-to-Site VPN-Verbindung realisierte Bandbreite auswirken können, unter anderem: Paketgröße, Verkehrsmix (TCP/UDP), Shaping- oder Drosselungsrichtlinien in Zwischennetzwerken, Internetwetter und spezifische Anwendungsanforderungen.

| Name | Standard | Anpassbar |
| --- | --- | --- |
| Maximale Bandbreite pro VPN-Tunnel | Bis zu 1,25 GBit/s | Nein |
| Maximale Anzahl an Paketen pro Sekunde (PPS) pro VPN-Tunnel | Bis zu 140.000 | Nein |

Für Site-to-Site VPN-Verbindungen auf einem Transit-Gateway können Sie ECMP verwenden, um eine höhere VPN-Bandbreite zu erreichen, indem Sie mehrere VPN-Tunnel aggregieren. Zur Verwendung von ECMP muss die VPN-Verbindung für dynamisches Routing konfiguriert sein. ECMP wird nicht für VPN-Verbindungen unterstützt, die statisches Routing nutzen. Weitere Informationen finden Sie unter Transit-Gateways.

> **Note**
>
> IPv6 VPNs unterstützt denselben Durchsatz (Gbit/s und PPS), dieselbe MTU und dieselben Routenlimits wie. IPv4 VPNs Es gibt keine Leistungsunterschiede zwischen IPv4 und IPv6 VPN-Verbindungen.

# Maximum Transmission Unit (MTU)

Site-to-Site VPN unterstützt eine maximale Übertragungseinheit (MTU) von 1446 Byte und eine entsprechende maximale Segmentgröße (MSS) von 1406 Byte. Bestimmte Algorithmen, die größere TCP-Header verwenden, können diesen Maximalwert jedoch effektiv reduzieren. Um eine Fragmentierung zu vermeiden, empfehlen wir Ihnen, die MTU und MSS basierend auf den ausgewählten Algorithmen einzustellen. Weitere Informationen zu MTU, MSS und den optimalen Werten finden Sie unter Bewährte Methoden für ein AWS Site-to-Site VPN Kunden-Gateway-Gerät.

Jumbo-Frames werden nicht unterstützt. Weitere Informationen finden Sie unter Jumbo Frames im EC2 Amazon-Benutzerhandbuch.

Eine Site-to-Site VPN-Verbindung unterstützt Path MTU Discovery nicht.

Die MTU-Einschränkungen gelten IPv4 sowohl für IPv6 VPN-Verbindungen.

# Zusätzliche Kontingentressourcen

Informationen zu Kontingenten im Zusammenhang mit Transit-Gateways, einschließlich der Anzahl von Verbindungen zu einem Transit-Gateway, finden Sie unter Kontingente für Ihre Transit-Gateways im Amazon VPC-Handbuch zu Transit-Gateways.

Hinweise zum Bezug zusätzlicher VPC-Kontingente finden Sie unter Amazon VPC-Kontingente im Amazon VPC-Benutzerhandbuch.

# Dokumentenverlauf für das Site-to-Site VPN-Benutzerhandbuch

In der folgenden Tabelle werden die Aktualisierungen des AWS Site-to-Site VPN Benutzerhandbuchs beschrieben.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| IPv6 Unterstützung für AWS Site-to-Site VPN für den Außentunnel IPs | Site-to-Site VPN unterstützt jetzt IPv6 Adressen für den Außentunnel IPs auf Transit Gateway- und Cloud WAN-VPN-Verbindungen. Dies ermöglicht eine vollständ ige IPv6 Migration mit IPv6 Adressen sowohl für den äußeren Tunnel IPs und das innere Paket IPs (IPv6-in-IPv6) als auch für den IPv6 äußeren Tunnel IPs mit IPv4 innerem Paket IPs (IPv4-in-IPv6). | 1. Juli 2025 |
| Die AWSVPCS2 SVpn ServiceRolePolicy AWS verwaltete Richtlinie wurde aktualisiert | Der AWS verwalteten Richtlini e wurden neue Berechtig ungen hinzugefügt, die es Site-to-Site VPN ermöglichen, das AWS Secrets Manager verwaltete Geheimnis der VPN-Verbindung zu verwalten. | 27. Mai 2025 |
| Die Speicheroptionen für vorab gemeinsam genutzte Schlüssel wurden aktualisiert | Site-to-Site VPN unterstüt zt jetzt das AWS Secrets Manager Speichern eines vorab gemeinsam genutzten Schlüssels. | 27. Mai 2025 |

| | | |
|---|---|---|
| Informationen zum klassischen VPN entfernt | Informationen zum klassischen VPN wurden aus dem Handbuch entfernt. | 19. Januar 2023 |
| Beispielmeldungen für das VPN-Protokoll | Es wurden Beispielprotokolle für Site-to-Site VPN-Verbindungen hinzugefügt. | 9. Dezember 2022 |
| Aktualisiertes Download-Konfigurationsprogramm | Site-to-Site VPN-Kunden können Konfigurationsvorlagen für kompatible Customer Gateway (CGW) -Geräte generieren, um das Herstellen von VPN-Verbindungen zu diesen Geräten zu AWS vereinfachen. Dieses Update bietet Unterstützung für Internet Key Exchange-Parameter der Version 2 (IKEv2) für viele beliebte CGW-Geräte und beinhaltet zwei neue APIs — GetVpnConnectionDeviceTypes und. GetVpnConnectionDeviceSampleConfiguration | 21. September 2021 |
| Benachrichtigungen über VPN-Verbindungen | Site-to-Site VPN sendet automatisch Benachrichtigungen über Ihre VPN-Verbindung an die AWS Health Dashboard. | 29. Oktober 2020 |
| VPN-Tunnel-Initiierung | Sie können Ihre VPN-Tunnel so konfigurieren, AWS dass die Tunnel angezeigt werden. | 27. August 2020 |

| | | |
|---|---|---|
| VPN-Verbindungsoptionen ändern | Sie können die Verbindungsoptionen für Ihre Site-to-Site VPN-Verbindung ändern. | 27. August 2020 |
| Zusätzliche Sicherheitsalgorithmen | Sie können zusätzliche Sicherheitsalgorithmen bei Ihren VPN-Tunnel anwenden. | 14. August 2020 |
| IPv6 Unterstützung | Ihre VPN-Tunnel können den IPv6 Verkehr innerhalb der Tunnel unterstützen. | 12. August 2020 |
| AWS Site-to-Site VPN Leitfäden zusammenführen | In dieser Version werden die Inhalte des AWS Site-to-Site VPN Netzwerkadministratorhandbuchs in diesem Handbuch zusammengefasst. | 31. März 2020 |
| Beschleunigte Verbindungen AWS Site-to-Site VPN | Sie können die Beschleunigung für Ihre AWS Site-to-Site VPN Verbindung aktivieren. | 3. Dezember 2019 |
| AWS Site-to-Site VPN Tunneloptionen ändern | Sie können die Optionen für einen VPN-Tunnel in einer AWS Site-to-Site VPN Verbindung ändern. Sie können auch zusätzliche Tunneloptionen konfigurieren. | 29. August 2019 |
| AWS Private Certificate Authority Unterstützung für private Zertifikate | Sie können ein privates Zertifikat von verwenden AWS Private Certificate Authority , um Ihr VPN zu authentifizieren. | 15. August 2019 |

| | | |
|---|---|---|
| Neues Site-to-Site VPN-Benutzerhandbuch | Diese Version trennt den Inhalt AWS Site-to-Site VPN (früher bekannt als AWS Managed VPN) vom Amazon VPC-Benutzerhandbuch. | 18. Dezember 2018 |
| Ändern des Ziel-Gateways | Sie können das Ziel-Gateway der AWS Site-to-Site VPN Verbindung ändern. | 18. Dezember 2018 |
| Custom ASN | Während der Erstellung eines Virtual Private Gateway können Sie die private Autonomous System Number (ASN) für die Amazon-Seite des Gateways angeben. | 10. Oktober 2017 |
| VPN-Tunneloptionen | Sie können interne CIDR-Blöcke und vorinstallierte Schlüssel für Ihr VPN-Tunnel angeben. | 3. Oktober 2017 |
| VPN-Metriken | Sie können CloudWatch Metriken für Ihre VPN-Verbindungen einsehen. | 15. Mai 2017 |

| | | |
|---|---|---|
| VPN-Erweiterungen | Eine VPN-Verbindung unterstützt nun auch die AES-256-Bit-Verschlüsselungsfunktion, die SHA-256-Hashfunktion, die NAT-Übersetzung und zusätzliche Diffie-Hellman-Gruppen während Phase 1 und Phase 2 einer Verbindung. Zusätzlich können Sie nun auch dieselbe Kunden-Gateway-IP-Adresse für jede VPN-Verbindung benutzen, die dasselbe Kunden-Gateway-Gerät verwendet. | 28. Oktober 2015 |
| VPN-Verbindungen mit statischer Routing-Konfiguration | Sie können IPsec VPN-Verbindungen zu Amazon VPC mithilfe statischer Routing-Konfigurationen erstellen. Bisher musste für VPN-Verbindungen das Border Gateway Protocol (BGP) verwendet werden. Wir unterstützen ab sofort beide Verbindungsarten. Sie können nun auch Verbindungen von Geräten aufbauen, die kein BGP unterstützen, einschließlich Cisco ASA und Microsoft Windows Server 2008 R2. | 13. September 2012 |

| | | |
|---|---|---|
| Automatische Routing-Verbreitung | Sie können jetzt die automatische Weitergabe von Routen von Ihrem VPN und AWS Direct Connect Links zu Ihren VPC-Routingtabellen konfigurieren. | 13. September 2012 |
| AWS VPN CloudHub und redundante VPN-Verbindungen | Sie können sicher zwischen Standorten mit und ohne VPCs kommunizieren. Sie können redundante VPN-Verbindungen verwenden, um eine fehlertolerante Verbindung zu Ihrer VPC zu gewährleisten. | 29. September 2011 |

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.