



User Guide

AWS Site-to-Site VPN



AWS Site-to-Site VPN: User Guide

Copyright © 2024 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 Site-zu-Site-VPN?	1
Konzepte	1
Site-to-Site-VPN-Funktionen	2
Einschränkungen bei Site-to-Site-VPN	2
Arbeiten mit Site-to-Site-VPN	3
Preise	3
Funktionsweise von AWS Site-to-Site VPN	4
Virtuelles Privates Gateway	4
Transit Gateway	5
Kunden-Gateway-Gerät	6
Kunden-Gateway	6
VPN-Tunneloptionen	7
Optionen für die VPN-Tunnelauthentifizierung	13
Pre-Shared-Key	14
Privates Zertifikat von AWS Private Certificate Authority	14
Optionen zur Initiierung des VPN-Tunnels	14
Optionen zur IKE-Initiierung des VPN-Tunnels	15
Regeln und Einschränkungen	15
Arbeiten mit Optionen zur VPN-Tunnel-Initiierung	16
Ersatz-Endpunkte	16
Kunde hat den Austausch von Endpunkten initiiert	16
Von AWS verwalteter Endpunktaustausch	17
Lebenszyklus eines Tunnelendpunkts	18
Kunden-Gateway-Optionen	23
Beschleunigte VPN-Verbindungen	26
Aktivieren der Beschleunigung	26
Regeln und Einschränkungen	26
Site-to-Site VPN-Routing-Optionen	27
Statisches und dynamisches Routing	28
Routing-Tabellen und VPN-Routenpriorität	28
Routing während VPN-Tunnelendpunkt-Updates	31
IPv4- und IPv6-Datenverkehr	31
Erste Schritte-Tutorial	33
Voraussetzungen	33

Erstellen eines Kunden-Gateways	35
Erstellen Sie ein Ziel-Gateway	36
Erstellen eines Virtual Private Gateways	36
Erstellen eines Transit-Gateways	37
Routing konfigurieren	37
(Virtual Private Gateway) Aktivieren Sie die Routenverbreitung in Ihrer Routing-Tabelle	38
(Transit-Gateway) Fügen Sie eine Route zu Ihrer Routing-Tabelle hinzu.	39
Aktualisieren Ihrer Sicherheitsgruppe	40
Eine VPN-Verbindung erstellen	40
Konfigurationsdatei herunterladen	42
Konfigurieren Sie das Kunden-Gateway-Gerät.	43
Architekturen	44
Einzel- und Mehrfach-VPN-Verbindungen	44
Einfache Site-to-Site-VPN-Verbindung	44
Einzelne Site-to-Site-VPN-Verbindung mit einem Transit-Gateway	45
Mehrere Site-zu-Site-VPN-Verbindungen	46
Mehrere Site-to-Site-VPN-Verbindungen mit einem Transit-Gateway	46
Site-to-Site VPN-Verbindung mit AWS Direct Connect	47
Private IP-Site-to-Site-VPN-Verbindung mit AWS Direct Connect	48
AWS VPN CloudHub	49
Übersicht	49
Preisgestaltung	51
Redundante VPN-Verbindungen	51
Ihr Kunden-Gateway-Gerät	54
Beispielkonfigurationsdateien	55
Anforderungen für Ihr Kunden-Gateway-Gerät	57
Bewährte Methoden für Ihr Kunden-Gateway-Gerät	61
Firewall-Regeln	63
Szenarien mit mehreren VPN-Verbindungen	65
Routing für Ihr Kunden-Gateway-Gerät	66
Beispielkonfigurationen für statisches Routing	67
Beispielkonfigurationsdateien	67
Verfahren für statisches Routing über die Benutzeroberfläche	69
Zusätzliche Informationen für Cisco-Geräte	80
Testen	81
Beispielkonfigurationen für dynamisches Routing (BGP)	81

Beispielkonfigurationsdateien	81
Verfahren für dynamisches Routing über die Benutzeroberfläche	83
Zusätzliche Informationen für Cisco-Geräte	93
Zusätzliche Informationen für Juniper-Geräte	93
Testen	94
Windows Server als Kunden-Gateway-Gerät	94
Konfigurieren der Windows-Instance	94
Schritt 1: Erstellen einer VPN-Verbindung und Konfigurieren Ihrer VPC	95
Schritt 2: Herunterladen der Konfigurationsdatei für die VPN-Verbindung	97
Schritt 3: Konfigurieren des Windows-Servers	99
Schritt 4: Einrichten des VPN-Tunnels	101
Schritt 5: Aktivieren von Dead Gateway Detection	108
Schritt 6: Testen der VPN-Verbindung	109
Fehlerbehebung	110
Gerät mit BGP	110
Gerät ohne BGP	113
Cisco ASA	116
Cisco IOS	121
Cisco IOS ohne BGP	127
Juniper JunOS	133
Juniper ScreenOS	137
Yamaha	141
Mit Site-to-Site-VPN arbeiten	146
Erstellen Sie einen VPN-Anhang für Cloud WAN AWS	146
Einen Transit-Gateway-VPN-Anhang erstellen	148
Eine VPN-Verbindung testen	150
Eine VPN-Verbindung löschen	152
Eine VPN-Verbindung löschen	152
Ein Kunden-Gateway löschen	153
Ein Virtual Private Gateway trennen und löschen	153
Das Ziel-Gateway für die VPN-Verbindung ändern	154
Schritt 1: Das neue Ziel-Gateway erstellen	155
Schritt 2: Die statischen Routen löschen (bedingt)	155
Schritt 3: Migrieren zum neuen Gateway	156
Schritt 4: Aktualisieren der VPC-Routing-Tabellen	157
Schritt 5: Ziel-Gateway-Routing aktualisieren (bedingt)	158

Schritt 6: Kunden-Gateway-ASN aktualisieren (bedingt)	159
VPN-Verbindungsoptionen ändern	159
VPN-Tunnel-Optionen ändern	160
Die statischen Routen für eine VPN-Verbindung bearbeiten	161
Das Kunden-Gateway für die VPN-Verbindung ändern	162
Kompromittierte Anmeldeinformationen ersetzen	162
VPN-Tunnelendpunkt-Zertifikate rotieren	163
Privates IP-VPN mit AWS Direct Connect	164
Vorteile von privatem IP-VPN	164
Funktionsweise von privatem IP-VPN	165
Voraussetzungen	166
Das Kunden-Gateway erstellen	166
Das Transit Gateway vorbereiten	167
Erstellen Sie das Gateway AWS Direct Connect	167
Die Zuordnung für das Transit Gateway erstellen	168
Die VPN-Verbindung erstellen	168
Sicherheit	170
Datenschutz	170
Richtlinie für den Datenverkehr zwischen Netzwerken	172
Identity and Access Management	172
Zielgruppe	173
Authentifizierung mit Identitäten	174
Verwalten des Zugriffs mit Richtlinien	178
So funktioniert AWS Site-to-Site VPN mit IAM	181
Beispiele für identitätsbasierte Richtlinien	188
Fehlerbehebung	192
Verwenden von serviceverknüpften Rollen	194
Ausfallsicherheit	196
Zwei Tunnel pro VPN-Verbindung	197
Redundanz	197
Sicherheit der Infrastruktur	197
Überwachen Ihrer Site-to-Site-VPN-Verbindung	199
Überwachungstools	200
Automatisierte Überwachungstools	200
Manuelle Überwachungstools	201
AWS Site-to-Site VPN Logs	202

Vorteile von Site-to-Site-VPN-Protokollen	202
Größenbeschränkungen der Amazon CloudWatch Logs-Ressourcenrichtlinie	203
Inhalte von Site-to-Site-VPN-Protokollen	203
IAM-Anforderungen für die Veröffentlichung in Logs CloudWatch	207
Konfiguration von Site-to-Site-VPN-Protokollen anzeigen	208
Site-to-Site-VPN-Protokolle aktivieren	209
Site-to-Site-VPN-Protokolle deaktivieren	210
Überwachung von VPN-Tunneln mit Amazon CloudWatch	211
VPN-Metriken und Dimensionen	211
CloudWatch VPN-Metriken anzeigen	213
CloudWatch Alarme zur Überwachung von VPN-Tunneln erstellen	213
Überwachung von VPN-Verbindungen mithilfe von AWS Health Ereignissen	217
Benachrichtigungen über den Austausch von Tunnel-Endpunkten	217
VPN-Benachrichtigungen für einen einzelnen Tunnel	217
Kontingente	218
Site-to-Site VPN-Ressourcen	218
Routen	219
Bandbreite und Durchsatz	220
Maximum Transmission Unit (MTU)	220
Zusätzliche Kontingentressourcen	221
Dokumentverlauf	222
.....	ccxxvii

Was ist AWS Site-to-Site VPN?

Standardmäßig können Instances, die Sie in einer Amazon VPC starten, nicht mit Ihrem eigenen (entfernten) Netzwerk kommunizieren. Sie können den Zugriff auf Ihr entferntes Netzwerk von Ihrer VPC aus ermöglichen, indem Sie eine AWS Site-to-Site VPN-Verbindung (Site-to-Site-VPN-Verbindung) herstellen und das Routing so konfigurieren, dass der Datenverkehr über die Verbindung geleitet wird.

Auch wenn es sich bei dem Begriff VPN-Verbindung um eine allgemeine Bezeichnung handelt, bezieht er sich in dieser Dokumentation auf die Verbindung zwischen Ihrer VPC und Ihrem On-Premise-Netzwerk. Site-to-Site-VPN unterstützt IPsec-VPN-Verbindungen.

Inhalt

- [Konzepte](#)
- [Site-to-Site-VPN-Funktionen](#)
- [Einschränkungen bei Site-to-Site-VPN](#)
- [Arbeiten mit Site-to-Site-VPN](#)
- [Preise](#)

Konzepte

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

- VPN-Verbindung: Eine sichere Verbindung zwischen Ihren On-Premise-Geräten und Ihren 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 über Ihr Kunden-Gateway-Gerät zur Verfügung stellt.
- Ein Kunden-Gateway-Gerät ist ein physisches Gerät oder eine Software-Anwendung auf Ihrer Seite der Site-to-Site-VPN-Verbindung.
- Ziel-Gateway: Ein Oberbegriff für den VPN-Endpunkt auf der Amazon-Seite der Site-to-Site-VPN-Verbindung.

- **Virtual Private Gateway:** Ein Virtual Private Gateway ist der VPN-Endpunkt auf der Amazon-Seite Ihrer Site-to-Site-VPN-Verbindung, der an eine einzelne VPC angefügt werden kann.
- **Transit-Gateway:** Ein Transit-Hub, mit dem Sie mehrere VPCs und On-Premise-Netzwerke miteinander verbinden können und das Sie als VPN-Endpunkt für die Amazon-Seite der Site-to-Site-VPN-Verbindung verwenden können.

Site-to-Site-VPN-Funktionen

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

- Internet Key Exchange (IKEv2) Version 2
- NAT-Traversierung
- Konfiguration der 4-Byte-ASN im Bereich von 1 bis 2147483647 für Virtual Private Gateway (VGW). Weitere Informationen finden Sie unter [Optionen für das Kunden-Gateway für Ihre Site-to-Site-VPN-Verbindung](#).
- 2-Byte-ASN für Customer Gateway (CGW) im Bereich von 1 bis 65535. Weitere Informationen finden Sie unter [Optionen für das Kunden-Gateway für Ihre Site-to-Site-VPN-Verbindung](#).
- CloudWatch-Kennzahlen
- 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 CA von AWS Private Certificate Authority
- Unterstützung für IPv6-Datenverkehr für VPN-Verbindungen auf einem Transit-Gateway

Einschränkungen bei Site-to-Site-VPN

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

- IPv6-Datenverkehr wird für VPN-Verbindungen bei einem Virtual Private Gateway nicht unterstützt.
- Eine AWS VPN-Verbindung unterstützt Path MTU Discovery nicht.

Berücksichtigen Sie außerdem Folgendes, wenn Sie Site-to-Site-VPN verwenden:

- Wenn Sie Ihre VPCs mit einem gemeinsamen Vor-Ort-Netzwerk verbinden, empfehlen wir, dass Sie nicht überlappende CIDR-Blöcke für Ihre Netzwerke verwenden.

Arbeiten mit Site-to-Site-VPN

Sie können Ihre Site-to-Site-VPN-Ressourcen über die folgenden Schnittstellen erstellen und zur Verwaltung darauf zugreifen:

- AWS Management Console – Bietet ein Webinterface, mit dem Sie auf Ihre Site-to-Site-VPN-Ressourcen zugreifen können.
- AWS Command Line Interface (AWS CLI) — Bietet Befehle für zahlreiche AWS-Services, wie z. B. Amazon VPC, und wird unter Windows, macOS und Linux unterstützt. Weitere Informationen finden Sie unter [AWS Command Line Interface](#).
- AWS SDKs – bieten sprachspezifische APIs und übernehmen viele der Verbindungsdetails, wie zum Beispiel die Berechnung der Signaturen, die Verarbeitung des erneuten Absendens von Anforderungen 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](#).

Preise

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 Beschleunigte Site-to-Site-VPN-Verbindungen – Preise](#).

Die Datenübertragung von Amazon EC2 ins Internet wird Ihnen in Rechnung gestellt. Weitere Informationen finden Sie im Abschnitt [Datenübertragung](#) (Data Transfer) auf der Seite 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](#).

Funktionsweise von AWS Site-to-Site VPN

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](#)

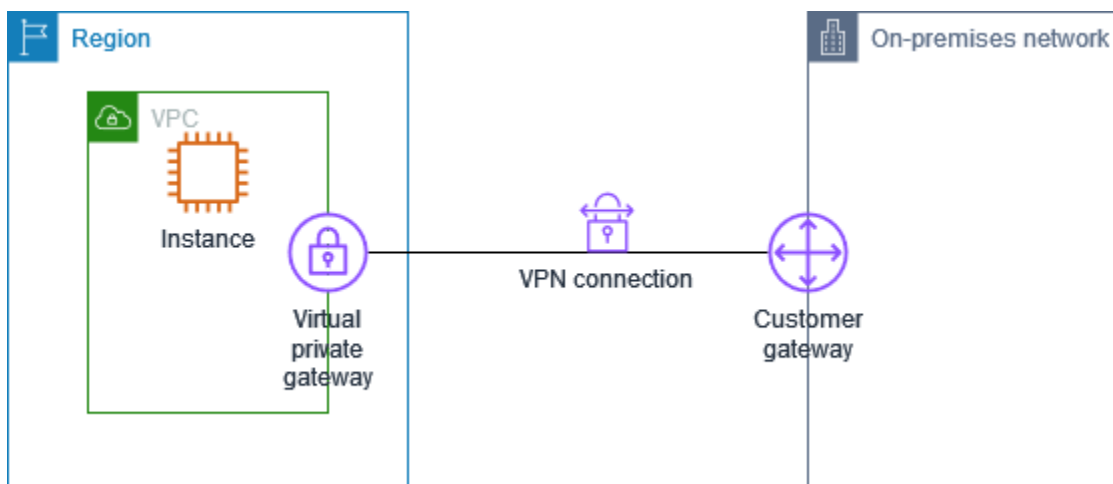
Die VPN-Verbindung bietet zwei VPN-Tunnel zwischen einem Virtual Private Gateway oder Transit-Gateway auf der AWS-Seite und einem Kunden-Gateway auf der On-Premises-Seite.

Weitere Informationen zu Site-to-Site-VPN-Kontingenten finden Sie unter [Site-to-Site VPN-Kontingente](#).

Virtuelles Privates Gateway

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



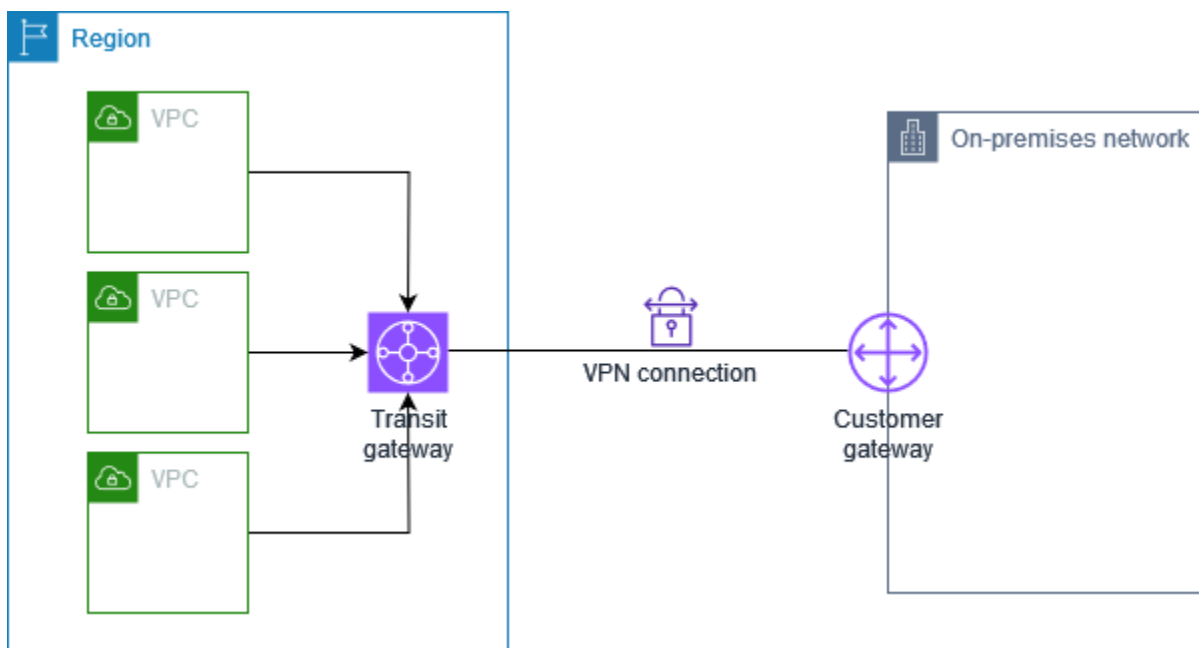
Während der Erstellung eines Virtual Private Gateway können Sie die private Autonomous System Number (ASN) für die Amazon-Seite des Gateways angeben. Wenn Sie keine ASN angeben, wird

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 die Details auf der Seite Virtual Private Gateways in der Amazon-VPC-Konsole an oder verwenden Sie den AWS CLI-Befehl [describe-vpn-gateways](#).

Transit Gateway

Ein Transit-Gateway ist ein Transit-Hub, mit dem Sie Ihre VPCs und Ihre On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie unter [Amazon VPC Transit Gateways](#). Sie können eine Site-to-Site-VPN-Verbindung als Anhang auf einem Transit-Gateway erstellen.

Das folgende Diagramm zeigt eine VPN-Verbindung zwischen mehreren VPCs und Ihrem On-Premises-Netzwerk unter Verwendung 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 innerhalb der VPN-Tunnel IPv4- oder IPv6-Datenverkehr unterstützen. Weitere Informationen finden Sie unter [IPv4- und IPv6-Datenverkehr](#).

Sie können das Ziel-Gateway einer Site-to-Site-VPN-Verbindung von einem Virtual Private Gateway zu einem Transit-Gateway ändern. Weitere Informationen finden Sie unter [the section called "Das Ziel-Gateway für die VPN-Verbindung ändern"](#).

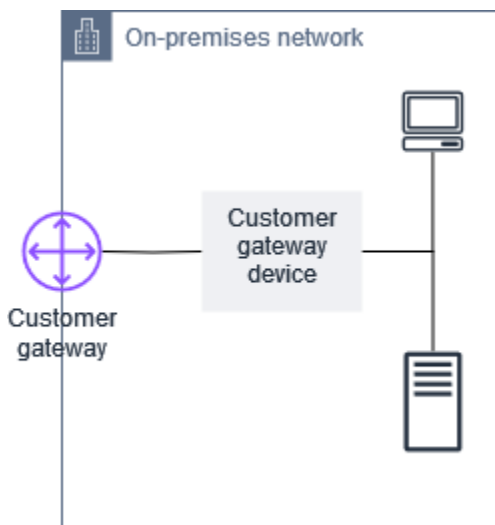
Kunden-Gateway-Gerät

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 [Ihr Kunden-Gateway-Gerät](#).

Standardmäßig muss Ihr Kunden-Gateway-Gerät die Tunnel für Ihre Site-to-Site-VPN-Verbindung aufbauen, indem Datenverkehr generiert und der IKE (Internet Key Exchange)-Aushandlungsprozess initiiert wird. Sie können Ihre Site-to-Site-VPN-Verbindung so konfigurieren, dass AWS stattdessen den IKE-Aushandlungsprozess initiieren muss. Weitere Informationen finden Sie unter [Initiierungsoptionen für Site-to-Site-VPN-Tunnel](#).

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, stellen Sie AWS Informationen zu Ihrem Gerät bereit. Weitere Informationen finden Sie unter [the section called "Kunden-Gateway-Optionen"](#).

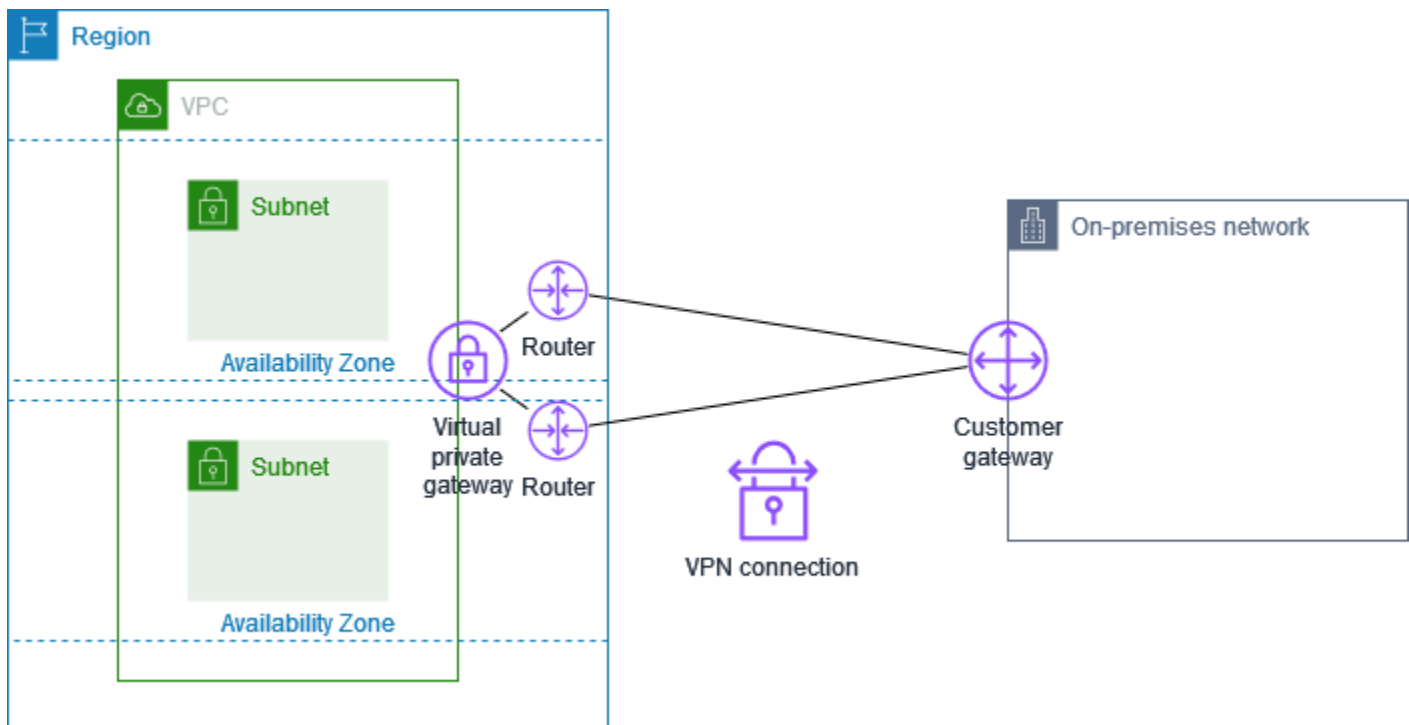


Um Amazon VPC mit einer Site-to-Site-VPN-Verbindung zu verwenden, müssen Sie oder Ihr Netzwerkadministrator auch das Kunden-Gateway-Gerät und eine Anwendung in Ihrem Remote-Netzwerk konfigurieren. Wenn Sie die Site-to-Site-VPN-Verbindung erstellen, erhalten Sie von uns die erforderlichen Konfigurationsinformationen, und in der Regel führt Ihr Netzwerkadministrator diese Konfiguration aus. Weitere Informationen über die Anforderungen und Konfiguration von Kunden-Gateways finden Sie unter [Ihr Kunden-Gateway-Gerät](#).

Tunnel-Optionen für Ihre Site-to-Site-VPN-Verbindung

Sie verwenden eine Site-to-Site-VPN-Verbindung, um Ihr Remote-Netzwerk mit einer VPC zu verknüpfen. Jede Site-to-Site-VPN-Verbindung verfügt über 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 (beispielsweise aufgrund von Wartungsarbeiten), wird der Netzwerkverkehr automatisch zu dem für diese Site-to-Site-VPN-Verbindung verfügbaren Tunnel geleitet.

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 On-Premises-Netzwerk in Richtung AWS verwendet beide Tunnel. Der Datenverkehr von AWS zum On-Premises-Netzwerk bevorzugt einen der Tunnel, kann aber automatisch auf den anderen Tunnel ausweichen, falls es auf der AWS-Seite zu einem Ausfall kommt.



Beim Erstellen einer Site-to-Site-VPN-Verbindung laden Sie eine für Ihr Kunden-Gateway-Gerät spezifische Konfigurationsdatei herunter, die Informationen zum Konfigurieren des Geräts enthält, darunter auch die Informationen zum Konfigurieren der einzelnen Tunnel. Sie können optional einige Tunnel-Optionen selbst angeben, wenn Sie die Site-to-Site-VPN-Verbindung erstellen. Andernfalls stellt AWS Standardwerte bereit.

Note

Site-to-Site-VPN-Tunnelendpunkte werten Vorschläge aus Ihrem Kunden-Gateway aus, beginnend mit dem niedrigsten konfigurierten Wert aus der folgenden Liste, unabhängig von der Angebotsbestellung des Kunden-Gateways. Sie können den `modify-vpn-connection-options`-Befehl nutzen, um die Liste der Optionen einzuschränken, die AWS-Endpunkte akzeptieren. Weitere Informationen finden Sie unter [modify-vpn-connection-options](#) in Amazon-EC2-Befehlszeilenreferenz.

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

Zeitüberschreitung bei DPD-Timeouts (Dead Peer Detection)

Die Zahl der Sekunden, nach denen eine DPD-Zeitüberschreitung auftritt. Ein DPD-Zeitlimit von 40 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 [Initiierungsoptionen für Site-to-Site-VPN-Tunnel](#).

Standard: `Clear`

VPN-Protokollierungsoptionen

Mit Site-to-Site-VPN-Protokollen erhalten Sie Zugriff auf Details zur Einrichtung von IP-Sicherheitstunneln (IPSec), Internet Key Exchange (IKE)-Aushandlungen und Dead Peer Detection (DPD)-Protokollmeldungen.

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.

Standard: `ikev1`, `ikev2`

Innentunnel IPv4-CIDR

Der Bereich der inneren (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 unter allen 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 bei mehreren 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 `169.254.0.0/16`-Bereich.

Innentunnel IPv6-CIDR

(Nur IPv6-VPN-Verbindungen) Der Bereich der inneren (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 unter allen Site-to-Site-VPN-Verbindungen, die dasselbe Transit-Gateway verwenden, eindeutig sein.

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

Lokales IPv4-Netzwerk-CIDR

(Nur IPv4-VPN-Verbindung) Der IPv4-CIDR-Bereich auf der Seite des Kunden-Gateways (On-Premise), der über die VPN-Tunnel kommunizieren darf.

Standard: 0.0.0.0/0

Remote-IPv4-Netzwerk-CIDR

(Nur IPv4-VPN-Verbindung) Der IPv4-CIDR-Bereich auf der AWS-Seite, der über den VPN-Tunnel kommunizieren darf.

Standard: 0.0.0.0/0

Lokales IPv6-Netzwerk-CIDR

(Nur IPv6-VPN-Verbindung) Der IPv6-CIDR-Bereich auf der Seite des Kunden-Gateways (On-Premise), der über die VPN-Tunnel kommunizieren darf.

Standard: ::/0

Remote-IPv6-Netzwerk-CIDR

(Nur IPv6-VPN-Verbindung) Der IPv6-CIDR-Bereich auf der AWS-Seite, der über den 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.

Standard: 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.

Standard: 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.

Standard: AES128, AES256, AES128-GCM-16, AES256-GCM-16

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.

Standard: 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.

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

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.

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

Lebensdauer für Phase 1

Note

AWS initiiert Re-Keys 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 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 initiiert Re-Keys 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 Margin-time in Sekunden vor Ablauf der Lebensdauer der Phasen 1 und 2, während der die AWS-Seite der VPN-Verbindung einen IKE-Rekey durchführt.

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 initiiert die IKE-Aushandlung, um den Tunnel aufzubauen. 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 [Initiierungsoptionen für Site-to-Site-VPN-Tunnel](#).

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 [Steuerung des Lebenszyklus von Tunnelendpunkten](#).

Standard: Off

Sie können die Tunneloptionen beim Erstellen einer Site-to-Site-VPN-Verbindung angeben oder Sie können die Tunneloptionen für eine vorhandene VPN-Verbindung ändern. Weitere Informationen finden Sie unter den folgenden Themen:

- [Schritt 5: Eine VPN-Verbindung erstellen](#)
- [Ändern von -Site-to-Site-VPN-Tunnel-Optionen](#)

Optionen für die Site-to-Site-Tunnel-Authentifizierung

Sie können Pre-Shared-Keys oder Zertifikate zur Authentifizierung Ihrer Site-to-Site-Tunnel-Endpunkte verwenden.

Pre-Shared-Key

Ein Pre-Shared-Key ist die Standardauthentifizierungsoption.

Ein Pre-Shared-Key ist eine Site-to-Site-VPN-Tunneloption, die Sie beim Erstellen eines Site-to-Site-VPN-Tunnels angeben können.

Ein Pre-Shared-Key ist eine Zeichenfolge, die Sie bei der Konfiguration Ihres Kunden-Gateway-Geräts eingeben. Wenn Sie keine Zeichenfolge angeben, generieren wir automatisch eine für Sie. Weitere Informationen finden Sie unter [Ihr Kunden-Gateway-Gerät](#).

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 serviceverknüpfte Rolle erstellen, um das Zertifikat für die AWS -Seite des Site-to-Site-Tunnelendpunkts zu generieren und zu verwenden. Weitere Informationen finden Sie unter [the section called "Service-verknüpfte Rollen"](#).

Nachdem Sie das private Zertifikat generiert haben, geben Sie das Zertifikat beim Erstellen des Kunden-Gateways an und wenden es dann auf Ihr Kunden-Gateway-Gerät an.

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.

Initiierungsoptionen für Site-to-Site-VPN-Tunnel

Standardmäßig muss Ihr Kunden-Gateway-Gerät die Tunnel für Ihre Site-to-Site-VPN-Verbindung aufbauen, indem Datenverkehr generiert und der IKE (Internet Key Exchange)-Aushandlungsprozess initiiert wird. Sie können Ihre VPN-Tunnel so konfigurieren, dass sie angeben, dass stattdessen der IKE-Verhandlungsprozess initiiert oder neu gestartet werden 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 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 werden muss, wenn ein DPD-Timeout auftritt, oder Sie können angeben, dass bei einem DPD-Timeout keine Aktion ausgeführt werden darf.

Regeln und Einschränkungen

Die folgenden Regeln und Einschränkungen gelten:

- Um die IKE-Verhandlung einzuleiten, 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, 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 Site-to-Site-VPN-Verbindung ändern](#).
- Die IKE-Initiierung (Startaktion) von der AWS Seite der VPN-Verbindung aus wird nur für IKEv2 unterstützt.
- Wenn Sie die IKE-Initiierung von der AWS Seite der VPN-Verbindung aus verwenden, enthält 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 NAT (Network Address Translation) verwendet, muss eine Identität (IDr) konfiguriert sein. Weitere Informationen zu IDr finden Sie 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: [Ändern von -Site-to-Site-VPN-Tunnel-Optionen](#)

Ersatz für Site-to-Site VPN-Tunnelendpunkte

Ihre Site-to-Site VPN-Verbindung besteht aus zwei VPN-Tunneln, um Redundanz sicherzustellen. Manchmal werden einer oder beide der VPN-Tunnel-Endpunkte ersetzt, wenn AWS Tunnel-Updates durchführt 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](#)
- [Steuerung 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 Tunnelendpunkte bereitgestellt werden,

Änderung	API-Aktion	Auswirkungen auf den Tunnel
		sind beide Tunnel nicht verfügbar
Ändern des Kunden-Gateways für die VPN-Verbindung	ModifyVpnConnection	Während neue Tunnelendpunkte bereitgestellt werden, sind beide Tunnel nicht verfügbar
Ändern der VPN-Verbindungsoptionen	ModifyVpnConnectionOptions	Während neue Tunnelendpunkte bereitgestellt werden, sind beide Tunnel nicht verfügbar
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 Service und wendet regelmäßig Updates auf Ihre VPN-Tunnel-Endpunkte an. 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 Aktualisierungen der Tunnelendpunkte bei einem Tunnel Ihrer VPN-Verbindung nacheinander 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.

Steuerung des Lebenszyklus von Tunnelendpunkten

Die Steuerung des Lebenszyklus von Tunnelendpunkten bietet Kontrolle über den Zeitplan für den Austausch von Endpunkten und kann dazu beitragen, die Verbindungsunterbrechungen beim Austausch der von AWS verwalteten Tunnelendpunkte zu minimieren. Mit dieser Funktion können Sie entscheiden, die von AWS verwalteten Updates für Tunnelendpunkte zu einem Ihr Unternehmen passenden Zeitpunkt zu akzeptieren. Verwenden Sie diese Funktion bei kurzfristigen Geschäftsanforderungen, oder wenn Sie nur einen einzigen Tunnel pro VPN-Verbindung unterstützen können.

Note

In seltenen Fällen wendet AWS wichtige Updates möglicherweise auch dann sofort auf Tunnelendpunkte an, wenn die Funktion zur Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist.

Themen

- [So funktioniert die Steuerung des Lebenszyklus von Tunnelendpunkten](#)
- [Steuerung des Lebenszyklus von Tunnelendpunkten](#)
- [Überprüfen, ob die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist](#)
- [Nach verfügbaren Updates suchen](#)
- [Wartungs-Update annehmen](#)
- [Steuerung des Lebenszyklus von Tunnelendpunkten deaktivieren](#)

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 den bevorstehenden Austausch von Tunnelendpunkten.

- Der Status der ausstehenden Wartung sowie die Zeitstempel Wartung automatisch angewendet nach und Letzte angewendete Wartung können in der AWS Management Console oder mithilfe des AWS CLI-Befehls [get-vpn-tunnel-replacement-status](#) eingesehen werden.

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 vor dem Datum Wartung automatisch angewendet nach keine Updates anwenden, führt AWS den Austausch der Tunnelendpunkte bald darauf als Teil des regulären Wartungsupdate-Zyklus automatisch durch.

Steuerung des Lebenszyklus von Tunnelendpunkten

Sie können diese Funktion mit der AWS Management Console oder der AWS CLI aktivieren.

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 Save Changes.

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

Mit dem Befehl [modify-vpn-tunnel-options](#) können Sie die Steuerung des Lebenszyklus von Tunnelendpunkten aktivieren.

New VPN connection

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

So aktivieren Sie die Steuerung des Lebenszyklus von Tunnelendpunkten-während der Erstellung einer neuen VPN-Verbindung mithilfe der 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 (Site-to-Site-VPN-Verbindungen) 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.

So aktivieren Sie die Steuerung des Lebenszyklus von Tunnelendpunkten-während der Erstellung einer neuen VPN-Verbindung mithilfe der AWS CLI

Mit dem Befehl [create-vpn-connection](#) können Sie die Steuerung des Lebenszyklus von Tunnelendpunkten aktivieren.

Überprüfen, ob die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist

Sie können mit der AWS Management Console oder der CLI überprüfen, ob die Steuerung des Lebenszyklus von Tunnelendpunkten in einem vorhandenen VPN-Tunnel aktiviert ist.

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 oder Deaktiviert ist.

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

Mit dem Befehl [describe-vpn-connections](#) können Sie überprüfen, ob die Steuerung des Lebenszyklus von Tunnelendpunkten aktiviert ist.

Nach verfügbaren Updates suchen

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.

So suchen Sie mit der AWS Management Console nach verfügbaren Updates

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.

So suchen Sie mit der AWS CLI nach verfügbaren Updates

Mit dem Befehl [get-vpn-tunnel-replacement-status](#) können Sie nach verfügbaren Updates suchen.

Wartungs-Update annehmen

Wenn ein Wartungs-Update verfügbar ist, können Sie es mit der AWS Management Console oder der CLI annehmen.

So nehmen Sie ein verfügbares Wartungs-Update mit der AWS Management Console an

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.

So nehmen Sie ein verfügbares Wartungs-Update mit der AWS CLI an

Mit dem Befehl [replace-vpn-tunnel](#) können Sie ein verfügbares Wartungs-Update annehmen.

Steuerung des Lebenszyklus von Tunnelendpunkten deaktivieren

Wenn Sie die Funktion zur Steuerung des Lebenszyklus von Tunnelendpunkten nicht mehr verwenden möchten, können Sie sie mit der AWS Management Console oder der AWS CLI deaktivieren. 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 deaktivieren, ohne die Option Tunnelaustausch überspringen zu verwenden. Die verfügbaren ausstehenden Wartungsupdates werden jedoch von AWS automatisch bereitgestellt, indem sofort ein Austausch von Tunnelendpunkten eingeleitet wird.

So deaktivieren Sie die 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. 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 Save Changes.

So deaktivieren Sie die Steuerung des Lebenszyklus von Tunnelendpunkten mithilfe der AWS CLI

Mit dem Befehl [modify-vpn-tunnel-options](#) können Sie die Steuerung des Lebenszyklus von Tunnelendpunkten deaktivieren.

Optionen für das Kunden-Gateway für Ihre Site-to-Site-VPN-Verbindung

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

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

Item	Beschreibung
	<p>Ihrem Netzwerk zugewiesene öffentliche ASN verwenden, mit Ausnahme der folgenden:</p> <ul style="list-style-type: none"> • 7224 - Reserviert in allen Regionen • 9059 - reserviert in der eu-west-1 -Region • 10124 - reserviert in der ap-northeast-1 -Region • 17943 - reserviert in der ap-southeast-1 -Region <p>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. Der Standard-ASN ist 65000. Weitere Informationen zum Routing finden Sie unter Site-to-Site VPN-Routing-Optionen.</p>
<p>(Optional) Die IP-Adresse der externen Schnittstelle des Kunden-Gateway-Geräts</p>	<p>Es muss sich um eine statische IP-Adresse handeln.</p> <p>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 Endpunkten übertragen werden dürfen. AWS Site-to-Site VPN Weitere Informationen finden Sie unter Firewall-Regeln.</p> <p>Eine IP-Adresse ist nicht erforderlich, wenn Sie ein privates Zertifikat von AWS Private Certificate Authority und ein öffentliches VPN verwenden.</p>

Item	Beschreibung
<p>(Optional) Privates Zertifikat von einer untergeordneten Zertifizierungsstelle unter Verwendung von AWS Certificate Manager (ACM).</p>	<p>Wenn Sie zertifikatsbasierte Authentifizierung verwenden möchten, geben Sie den ARN eines privaten ACM-Zertifikats an, das auf Ihrem Kunden-Gateway-Gerät verwendet werden soll.</p> <p>Beim Erstellen eines Kunden-Gateways können Sie das Kunden-Gateway so konfigurieren, dass AWS Private Certificate Authority private Zertifikate zur Authentifizierung des Site-to-Site VPN verwendet werden.</p> <p>Wenn Sie sich für diese Option entscheiden, erstellen Sie eine vollständig AWS gehostete private Zertifizierungsstelle (CA) für den internen Gebrauch in Ihrer Organisation. Sowohl das Root-CA-Zertifikat als auch die untergeordneten CA-Zertifikate werden von gespeichert und verwaltet. AWS Private CA</p> <p>Bevor Sie das Kunden-Gateway erstellen, erstellen Sie mithilfe AWS Private Certificate Authority von einer untergeordneten Zertifizierungsstelle 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 -Benutzerhandbuch.</p>
<p>(Optional) Gerät.</p>	<p>Ein Name für das Kunden-Gateway-Gerät ein, das diesem Kunden-Gateway zugeordnet ist.</p>

Beschleunigte -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) verwendet AWS Global Accelerator, um den Datenverkehr von Ihrem On-Premises-Netzwerk an einen AWS Edge-Standort weiterzuleiten, der Ihrem Kunden-Gateway-Gerät am nächsten ist. AWS Global Accelerator optimiert den Netzwerkpfad und verwendet das überlastungsfreie AWS globale Netzwerk, 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 AWS Global Accelerator Konsole oder APIs verwenden.

Informationen zu den AWS Regionen, die Accelerated VPN-Verbindungen unterstützen, finden Sie in den [AWS FAQs zu Accelerated Site-to-Site VPN](#).

Aktivieren der Beschleunigung

Wenn Sie eine Site-to-Site-VPN-Verbindung erstellen, ist die Beschleunigung standardmäßig deaktiviert. Sie können optional die Beschleunigung aktivieren, wenn Sie eine neue Site-to-Site-VPN-Verbindung auf einem Transit-Gateway erstellen. Weitere Informationen und Schritte finden Sie unter [Einen Transit-Gateway-VPN-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 mit einem Transit-Gateway verbunden 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 vorhandene Site-to-Site-VPN-Verbindung nicht aktivieren oder deaktivieren. Stattdessen können Sie eine neue Site-to-Site-VPN-Verbindung mit einer Beschleunigung erstellen, die bei Bedarf ein- oder ausgeschaltet wird. 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-Aushandlung für beschleunigte VPN-Tunnel muss vom Kunden-Gateway-Gerät 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 die zertifikatbasierte Authentifizierung verwenden AWS Global Accelerator, sind aufgrund der eingeschränkten Unterstützung für die Paketfragmentierung in Global Accelerator möglicherweise nicht mit kompatibel. 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.

Site-to-Site VPN-Routing-Optionen

Führen Sie die folgenden Schritte aus, um eine Site-to-Site VPN-Verbindung einzurichten:

- 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](#)
- [Routing-Tabellen und VPN-Routenpriorität](#)
- [Routing während VPN-Tunnelendpunkt-Updates](#)
- [IPv4- und IPv6-Datenverkehr](#)

Statisches und dynamisches Routing

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, legen Sie beim Konfigurieren Ihrer Site-to-Site VPN-Verbindung dynamisches Routing fest. Wenn Ihr Kunden-Gateway-Gerät BGP nicht unterstützt, geben Sie das statische Routing an.

Wenn Sie ein Gerät verwenden, das BGP-Advertising unterstützt, müssen Sie für die Site-to-Site VPN-Verbindung keine statischen Routen angeben, da das Gerät BGP verwendet, um seine Routen beim Virtual Private Gateway anzukündigen. 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 On-Premise-Netzwerk zur Site-to-Site VPN-Verbindung geleitet wird. Die Konfiguration hängt von der Marke und dem Modell Ihres Geräts ab. Weitere Informationen finden Sie unter [Ihr Kunden-Gateway-Gerät](#).

Routing-Tabellen und 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 verbreitete Routen von einer VPN- oder AWS Direct Connect-Verbindung mit der lokalen Route für Ihre VPC überschneiden, hat die lokale Route auch dann Priorität, wenn die verbreiteten Routen spezifischer sind.

- Wenn verbreitete Routen aus einer Site-to-Site VPN- oder einer AWS Direct Connect-Verbindung denselben Ziel-CIDR-Block wie andere bestehende statische Routen haben (die längste Präfix-Übereinstimmung kann nicht angewendet werden), priorisieren wir die statischen Routen, deren Ziele ein Internet-Gateway, ein Virtual Private Gateway, eine Netzwerkschnittstelle, eine Instance-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. Virtual Private Gateways unterstützen keinen IPv6-Datenverkehr.

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 VPNs auf virtuellen privaten Gateways und Transit-Gateways. 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-verbreitete Routen von einer AWS Direct Connect-Verbindung
- Manuell hinzugefügte statische Routen für eine Site-to-Site VPN-Verbindung
- BGP-verbreitete Routen aus einer Site-to-Site VPN-Verbindung

- Bei übereinstimmenden Präfixen, bei denen jede Site-to-Site VPN-Verbindung BGP nutzt, wird der AS PATH verglichen und das Präfix mit dem kürzesten AS PATH bevorzugt.

Note

AWS empfiehlt dringend die Verwendung von Kunden-Gateway-Geräten, 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 gleich lang sind und wenn das erste AS in der AS_SEQUENCE über mehrere Pfade hinweg gleich ist, werden multi-exit discriminators (MEDs) verglichen. Der Pfad mit dem niedrigsten MED-Wert wird bevorzugt.

Die Routenpriorität ist während [VPN-Tunnelendpunkt-Updates](#) betroffen.

Bei einer Site-to-Site VPN-Verbindung wählt AWS 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. Dieser Vorrang gilt für VPNs auf virtuellen privaten Gateways und Transit-Gateways.

Für ein Virtual Private Gateway wird ein Tunnel über alle Site-to-Site VPN-Verbindungen auf dem Gateway ausgewählt. Zur Verwendung von mehr als einem Tunnel wird Equal Cost Multipath (ECMP) empfohlen, 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 bei Site-to-Site VPN-Verbindungen auf einem Virtual Private Gateway nicht unterstützt.

Bei Site-to-Site VPN-Verbindungen, die BGP verwenden, kann der Primärtunnel durch den 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 durch 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. Von Zeit zu Zeit führt AWS eine routinemäßige Wartung an Ihrem Virtual Private Gateway durch. Dadurch kann es vorkommen, dass ein oder beide Tunnel der VPN-Verbindung kurzzeitig deaktiviert werden. 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-Datenverkehr

Ihre Site-to-Site VPN-Verbindung auf einem Transit-Gateway kann innerhalb der VPN-Tunnel IPv4- oder IPv6-Datenverkehr unterstützen. Standardmäßig unterstützen Site-to-Site VPN-Verbindungen IPv4-Datenverkehr innerhalb der VPN-Tunnel. Sie können eine neue Site-to-Site VPN-Verbindung so konfigurieren, dass IPv6-Datenverkehr innerhalb der VPN-Tunnel unterstützt wird. Wenn Ihre VPC und Ihr Netzwerk vor Ort für die IPv6-Adressierung konfiguriert sind, können Sie IPv6-Datenverkehr über die VPN-Verbindung senden.

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

Es gelten die folgenden Regeln:

- IPv6-Adressen werden nur für die internen IP-Adressen der VPN-Tunnel unterstützt. Die externen Tunnel-IP-Adressen für die AWS-Endpunkte sind IPv4-Adressen, und die öffentliche IP-Adresse Ihres Kunden-Gateways muss eine IPv4-Adresse sein.
- Site-to-Site VPN-Verbindungen auf einem Virtual Private Gateway unterstützen IPv6 nicht.
- Sie können die IPv6-Unterstützung für eine vorhandene Site-to-Site VPN-Verbindung nicht aktivieren.
- Eine Site-to-Site VPN-Verbindung kann nicht gleichzeitig sowohl den IPv4- als auch den IPv6-Datenverkehr unterstützen.

Weitere Hinweise zum Erstellen einer VPN-Verbindung finden Sie unter [Schritt 5: Eine VPN-Verbindung erstellen](#).

Erste Schritte 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 unter [Erstellen Sie einen VPN-Anhang für Cloud WAN AWS](#).
- 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	<p>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)</p>
Kunden-Gateway	<p>Um die Kunden-Gateway-Ressource in zu erstellen AWS, benötigen Sie die folgenden Informationen:</p> <ul style="list-style-type: none"> • Die über das Internet routbare IP-Adresse für die externe Schnittstelle des Geräts • Der Routing-Typ: statisch oder dynamisch • Für dynamisches Routing die Border Gateway Protocol (BGP) Autonomous System Number (ASN) • (Optional) Privates Zertifikat von AWS Private Certificate Authority zur Authentifizierung Ihres VPN <p>Weitere Informationen finden Sie unter Kunden-Gateway-Optionen.</p>
(Optional) Die ASN für die AWS Seite der BGP-Sitzung	<p>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 Virtuelles Privates Gateway.</p>
VPN-Verbindung	<p>Um die VPN-Verbindung anzulegen, benötigen Sie die folgenden Informationen:</p> <ul style="list-style-type: none"> • Für statisches Routing die IP-Präfixe für Ihr privates Netzwerk.

Item	Informationen
	<ul style="list-style-type: none">• (Optional) Tunneloptionen für jeden VPN-Tunnel. Weitere Informationen finden Sie unter Tunnel-Optionen für Ihre 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. (Optional) Geben Sie für IP adress (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.

7. (Optional) Wenn Sie ein privates Zertifikat verwenden möchten, wählen Sie für Certificate ARN (Zertifikat ARN) den Amazon-Ressourcennamen des privaten Zertifikats.
8. (Optional) Geben Sie als Gerät einen Namen für das Kunden-Gateway-Gerät ein, das diesem Kunden-Gateway zugeordnet ist.
9. Wählen Sie Kunden-Gateway erstellen aus.

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

- [CreateCustomerGateway](#) (Amazon EC2 EC2-Abfrage-API)
- [create-customer-gateway](#) (AWS CLI)
- [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 unter Verfügbare VPCs Ihre VPC und dann An VPC anfügen aus.

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

- [CreateVpnGateway](#) (Amazon EC2 EC2-Abfrage-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 EC2-Abfrage-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 Routenverbreitung für Ihre Routing-Tabelle aktivieren, um Site-to-Site VPN-Routen automatisch zu propagieren.

Für das statische 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 Virtual 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 unter 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 EC2-Abfrage-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 EC2-Abfrage-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 Edit 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 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. Geben Sie unter Static IP Prefixes (Statische IP-Präfixe) alle IP-Präfixe für das private Netzwerk Ihrer VPN-Verbindung an.
7. Wenn Ihr Ziel-Gateway vom Typ Transit-Gateway ist, geben Sie für Interne Tunnel-IP-Version an, ob die VPN-Tunnel IPv4- oder IPv6-Datenverkehr unterstützen. IPv6-Datenverkehr wird nur für VPN-Verbindungen auf einem Transit-Gateway unterstützt.
8. Wenn Sie IPv4 für die Version Tunnel inside IP 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 IPv6 für die Version Tunnel inside IP 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 $::/0$.

9. Behalten Sie für den Typ der externen IP-Adresse die Standardoption 4 bei. PublicIpv
10. (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 die IPv4-Adressen innerhalb des Tunnels.
 - Wenn Sie IPv6 bei Interne Tunnel-IP-Version angegeben haben, wird ein /126 IPv6 CIDR-Block aus dem $fd00::/8$ -Bereich für die IPv6-Adressen innerhalb des Tunnels verwendet.
 - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 und IKEv2.
 - Um die erweiterten Optionen für Ihren Tunnel zu bearbeiten, wählen Sie Tunneloptionen bearbeiten aus. Weitere Informationen finden Sie unter [VPN-Tunneloptionen](#).
11. 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

- [CreateVpnVerbindung](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)
- [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 IPv6-Datenverkehr zu nutzen.

Wir haben IKEv2-Support in den Konfigurationsdateien für viele gängige Kunden-Gateway-Geräte eingeführt und werden im Laufe der Zeit weitere Dateien hinzufügen. Unter [Ihr Kunden-Gateway-Gerät](#) finden Sie eine Liste der Konfigurationsdateien mit IKEv2-Unterstützung.

Berechtigungen

Um den Bildschirm für die Download-Konfiguration von korrekt zu laden AWS Management Console, müssen Sie sicherstellen, dass Ihre IAM-Rolle oder Ihr IAM-Benutzer über Berechtigungen für die folgenden Amazon EC2 EC2-APIs verfügt: `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

- [GetVpnConnectionDeviceTypen](#) (Amazon EC2 EC2-API)
- [GetVpnConnectionDeviceSampleConfiguration](#)(Amazon EC2 EC2-Abfrage-API)
- [get-vpn-connection-device-types](#) (AWS CLI)
- [get-vpn-connection-device-sample-configuration](#) (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 [Ihr Kunden-Gateway-Gerät](#).

Site-to-Site VPN-Architekturen

Dies sind häufig verwendete Site-to-Site VPN-Architekturen:

- [the section called “Einzel- und Mehrfach-VPN-Verbindungen”](#)
- [the section called “Redundante VPN-Verbindungen”](#)
- [the section called “AWS VPN CloudHub”](#)

Beispiele für Einzel- und Mehrfach-VPN-Verbindungen für Site-to-Site-VPN

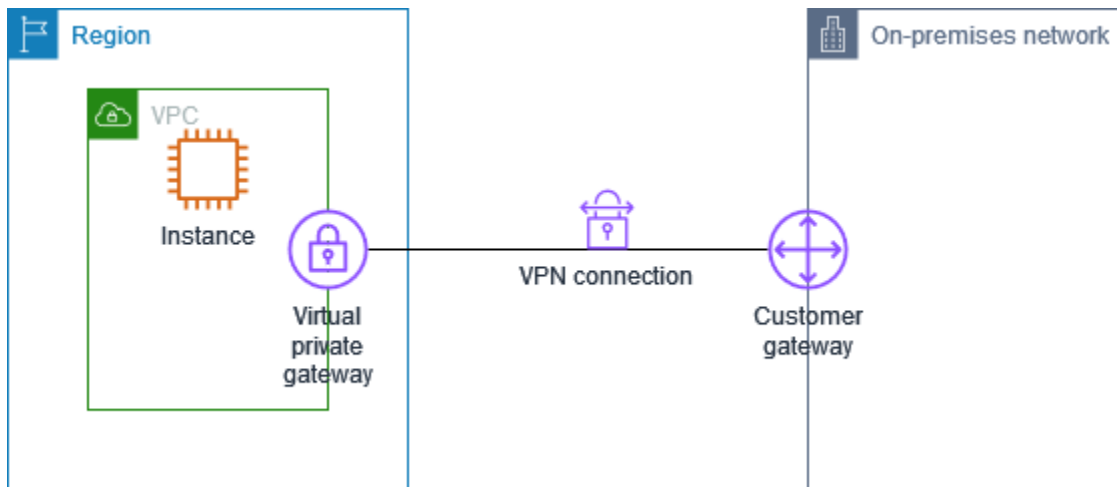
Die folgenden Diagramme illustrieren einfache und mehrfache Site-to-Site-VPN-Verbindungen.

Beispiele

- [Einfache Site-to-Site-VPN-Verbindung](#)
- [Einzelne Site-to-Site-VPN-Verbindung mit einem Transit-Gateway](#)
- [Mehrere Site-zu-Site-VPN-Verbindungen](#)
- [Mehrere Site-to-Site-VPN-Verbindungen mit einem Transit-Gateway](#)
- [Site-to-Site VPN-Verbindung mit AWS Direct Connect](#)
- [Private IP-Site-to-Site-VPN-Verbindung mit AWS Direct Connect](#)

Einfache Site-to-Site-VPN-Verbindung

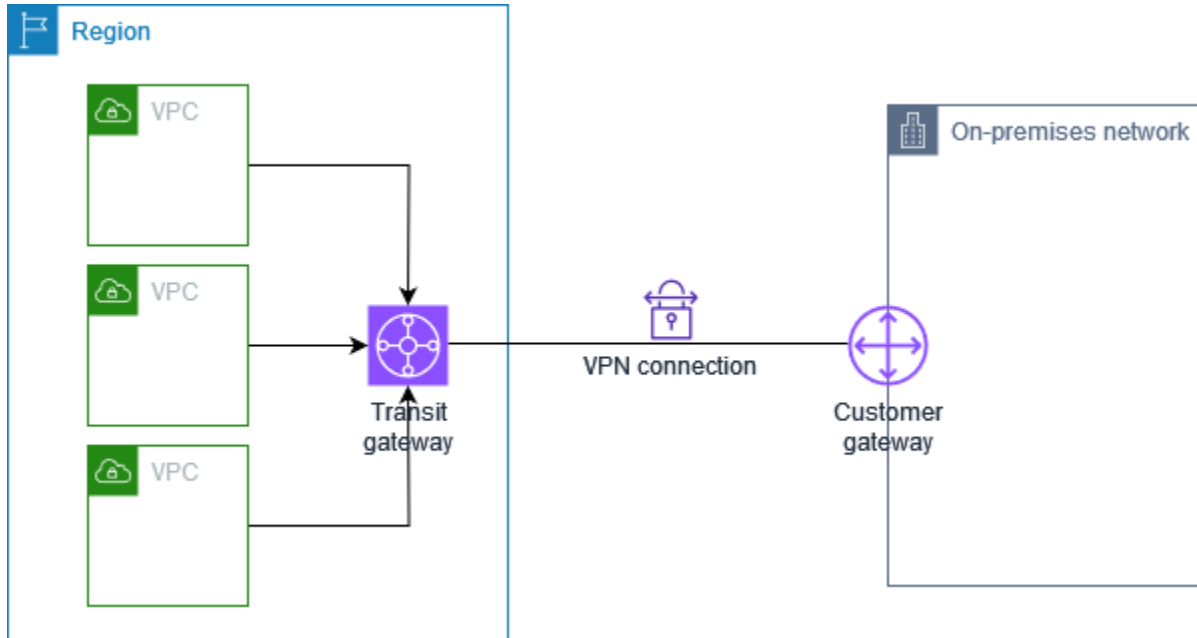
Die VPC verfügt über ein hinzugefügtes Virtual Private Gateway. Ihr On-Premises-Netzwerk (Remote) enthält ein Kunden-Gateway-Gerät, das Sie konfigurieren müssen, um die VPN-Verbindung zu aktivieren. Sie müssen die VPN-Routing-Tabellen so aktualisieren, dass jeglicher Datenverkehr von der VPC zu Ihrem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



Schritte zum Einrichten dieses Szenarios finden Sie unter [Erste Schritte mit AWS Site-to-Site VPN](#).

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

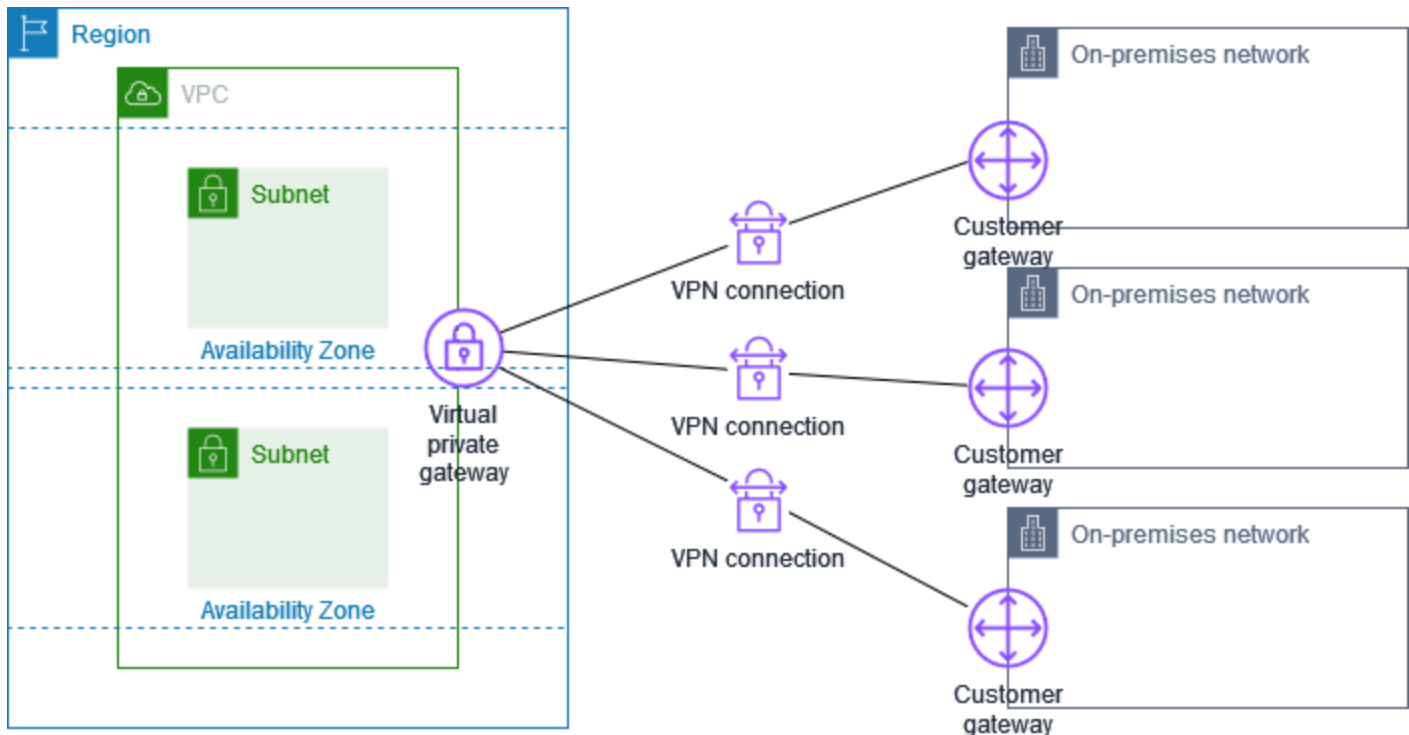
Die VPC verfügt über ein angefügtes Transit-Gateway. Ihr On-Premises-Netzwerk (Remote) enthält ein Kunden-Gateway-Gerät, das Sie konfigurieren müssen, um die VPN-Verbindung zu aktivieren. Sie müssen die VPN-Routing-Tabellen so aktualisieren, dass jeglicher Datenverkehr von der VPC zu Ihrem Netzwerk über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



Schritte zum Einrichten dieses Szenarios finden Sie unter [Erste Schritte mit AWS Site-to-Site VPN](#).

Mehrere Site-zu-Site-VPN-Verbindungen

Die VPC verfügt über ein angefügtes Virtual Private Gateway, und Sie verfügen über mehrere Site-to-Site-VPN-Verbindungen mit mehreren On-Premise-Standorten. Sie richten das Routing so ein, dass der gesamte VPC-Datenverkehr, der für Ihr Netzwerk vorgesehen ist, zum Virtual Private Gateway geleitet wird.



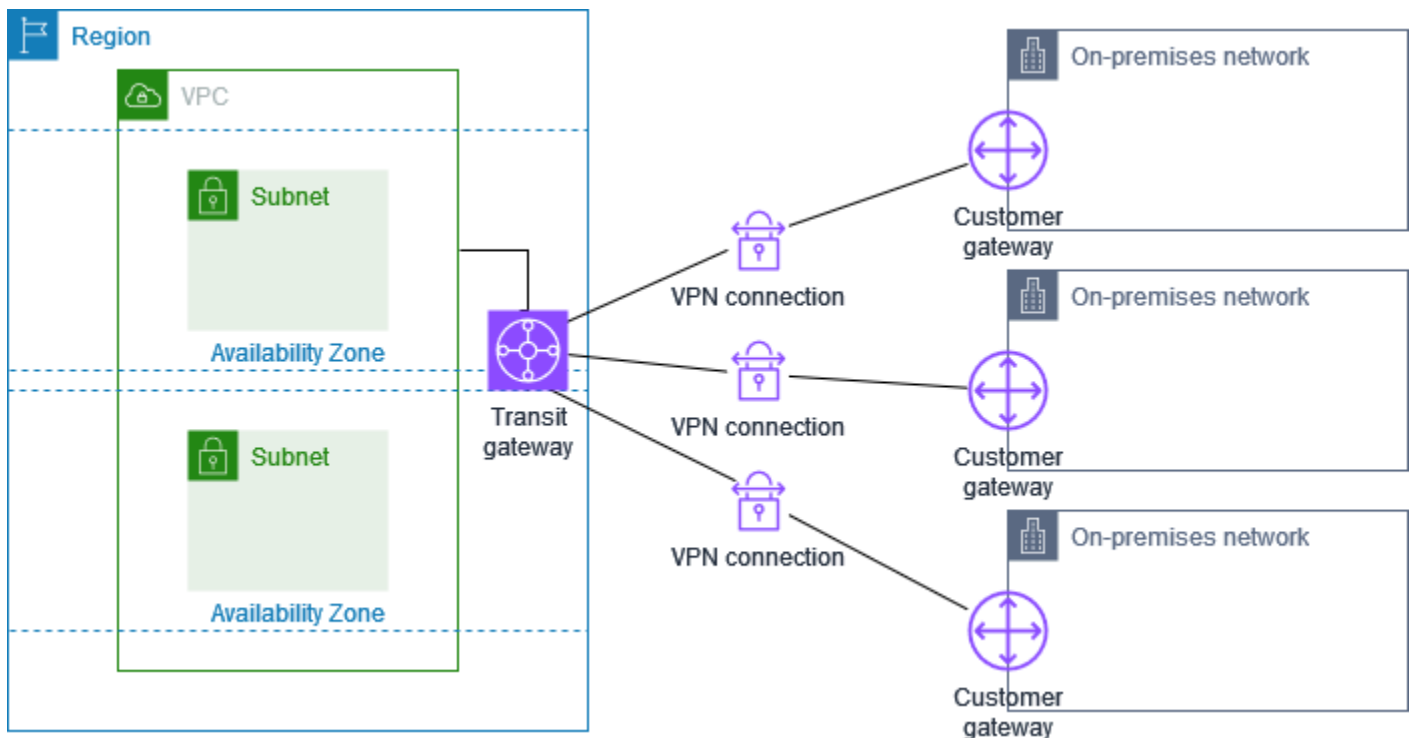
Wenn Sie mehrere Site-to-Site-VPN-Verbindungen zu einer einzelnen VPC erstellen, können Sie ein zweites Kunden-Gateway konfigurieren, um eine redundante Verbindung zu einem externen Standort zu erstellen. Weitere Informationen finden Sie unter [Verwenden redundanter Site-to-Site-VPN-Verbindungen zur Bereitstellung von Failover](#).

Sie können dieses Szenario auch verwenden, um Site-to-Site-VPN-Verbindungen zu mehreren geografischen Standorten herzustellen und eine sichere Kommunikation zwischen den Standorten bereitzustellen. Weitere Informationen finden Sie unter [Ermöglichen einer sicheren Kommunikation zwischen Standorten über VPN CloudHub](#).

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

Die VPC verfügt über ein angefügtes Transit-Gateway und Sie haben mehrere Site-to-Site-VPN-Verbindungen mit mehreren On-Premise-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.

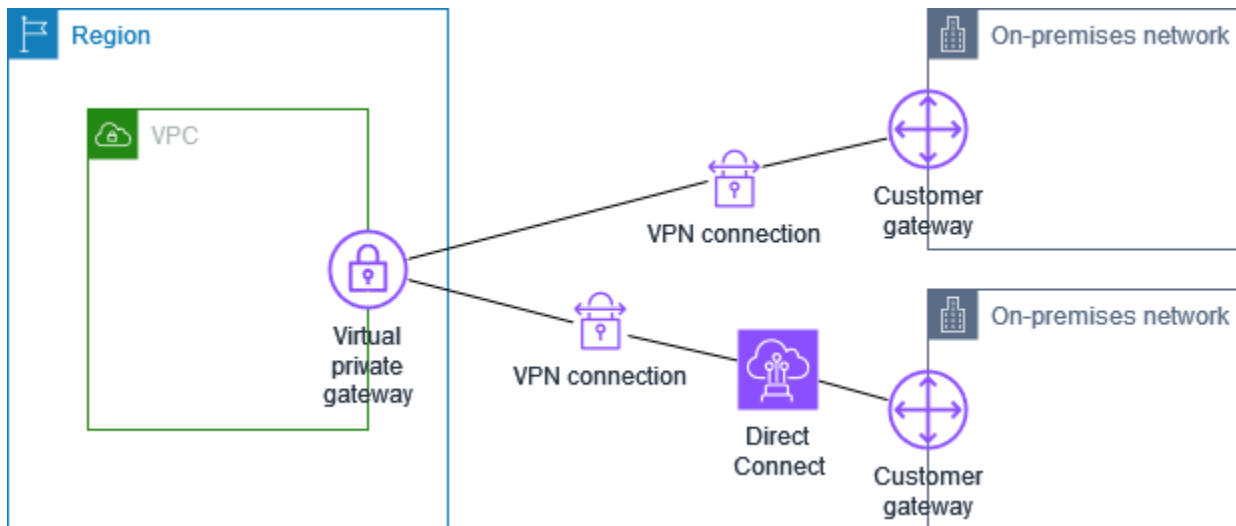


Wenn Sie mehrere Site-to-Site-VPN-Verbindungen zu einem einzelnen Transit-Gateway erstellen, können Sie ein zweites Kunden-Gateway konfigurieren, um eine redundante Verbindung zum selben externen Standort zu erstellen.

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

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

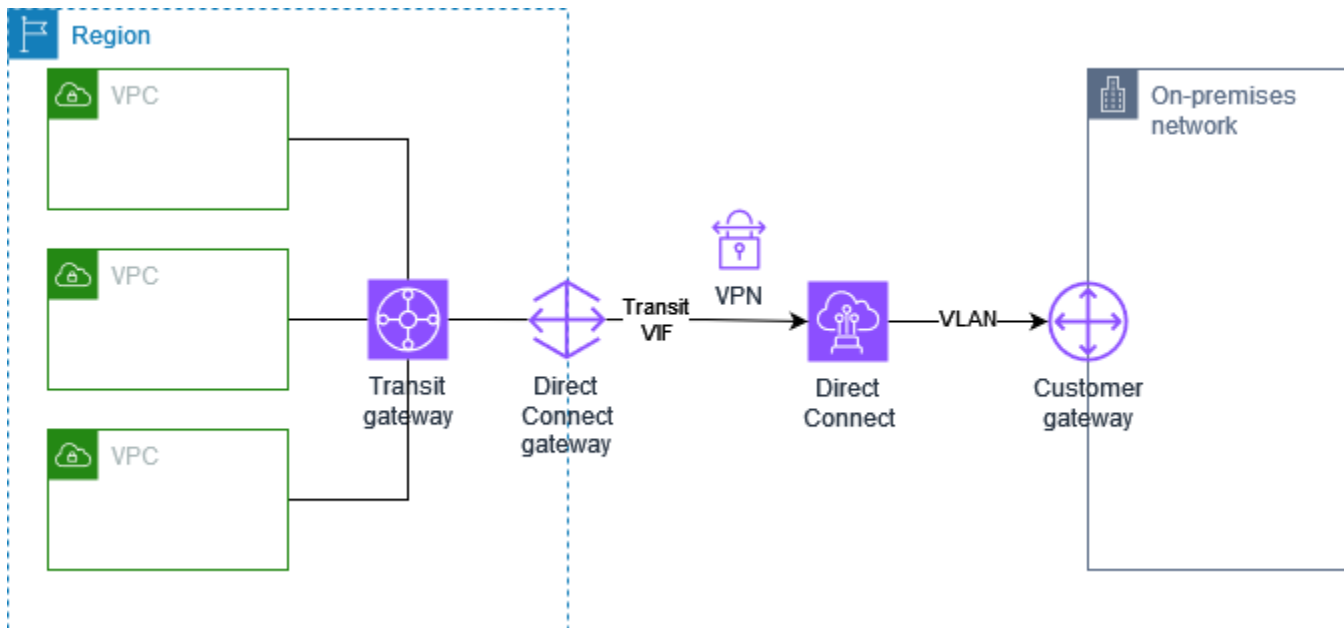
Die VPC verfügt über ein angefügtes Virtual Private Gateway und stellt über AWS Direct Connect eine Verbindung zu Ihrem lokalen (Remote-) Netzwerk her. Sie können eine öffentliche virtuelle Schnittstelle von AWS Direct Connect konfigurieren, um eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und öffentlichen AWS-Ressourcen über ein Virtual Private Gateway herzustellen. Richten Sie das Routing so ein, dass der gesamte VPC-Datenverkehr, der für Ihre Netzwerkroutrouten vorgesehen ist, zum Virtual Private Gateway und zur AWS Direct Connect-Verbindung geleitet wird.



Wenn sowohl AWS Direct Connect als auch die VPN-Verbindung auf demselben Virtual Private Gateway eingerichtet sind, kann das Hinzufügen oder Entfernen von Objekten dazu führen, dass das Virtual Private Gateway in den Status „anfügen“ 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 IP-Site-to-Site-VPN-Verbindung mit AWS Direct Connect

Mit einem privaten IP-Site-to-Site-VPN können Sie AWS Direct Connect-Datenverkehr zwischen Ihrem On-Premises-Netzwerk und AWS ohne Verwendung öffentlicher IP-Adressen verschlüsseln. Ein privates IP-VPN über AWS Direct Connect stellt sicher, dass der Datenverkehr zwischen AWS und On-Premises-Netzwerken sicher und privat ist, sodass die Kunden die gesetzlichen und sicherheitsbezogenen Vorgaben erfüllen können.



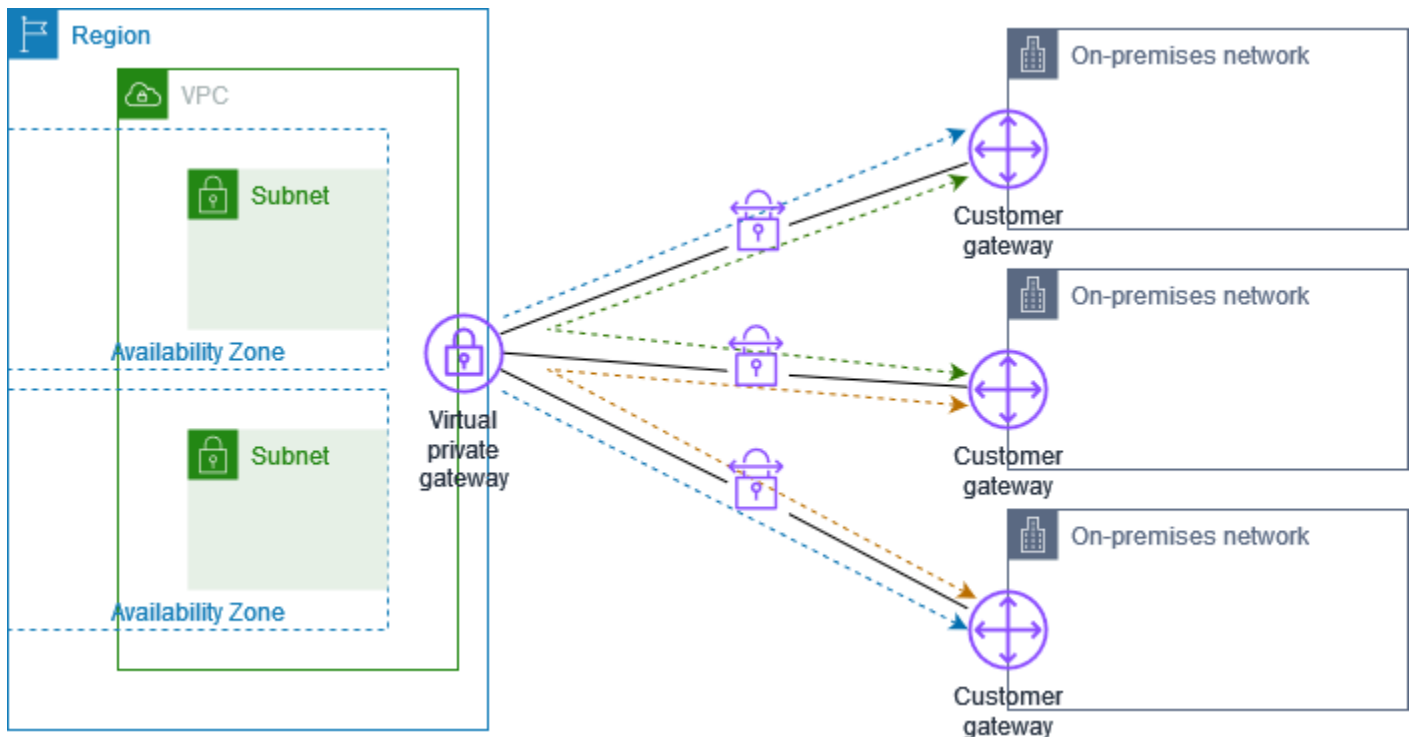
Weitere Informationen finden Sie im folgenden Blogbeitrag: [Einführung von AWS Site-to-Site VPN-VPNs mit privater IP](#).

Ermöglichen einer sicheren Kommunikation zwischen Standorten über VPN CloudHub

Wenn Sie über mehrere AWS Site-to-Site VPN-Verbindungen verfügen, können Sie eine sichere Kommunikation zwischen Standorten über den AWS VPN CloudHub ermöglichen. Dies ermöglicht den Standorten die Kommunikation untereinander und nicht nur mit den Ressourcen in Ihrer VPC. Der VPN CloudHub wird über ein einfaches Hub-and-Spoke-Modell ausgeführt, das mit oder ohne VPC verwendet werden kann. Dieses Design eignet sich für Kunden mit mehreren Niederlassungen und vorhandenen Internetverbindungen, die ein praktisches, potenziell preisgünstiges Hub-and-Spoke-Modell für die primäre oder die Backup-Konnektivität zwischen diesen Standorten implementieren möchten.

Übersicht

Das folgende Diagramm zeigt die VPN-CloudHub-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 Site-to-Site-VPN-Verbindung mit dynamischem Routing 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 über die Netzwerkanweisungen in den VPN-Konfigurationsdateien der 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.

Standorte, die AWS Direct Connect-Verbindungen zum Virtual Private Gateway verwenden, können auch Teil des AWS VPN CloudHubs werden. Beispielsweise kann der Hauptsitz Ihres Unternehmens in New York über eine AWS Direct Connect-Verbindung und Ihre Niederlassungen über Site-to-Site VPN-Verbindungen mit der VPC verbunden sein. Die Niederlassungen in Los Angeles und Miami können untereinander, aber auch mit dem Unternehmenshauptsitz Daten austauschen – alles mithilfe des AWS VPN CloudHubs.

Preisgestaltung

Um AWS VPN CloudHub zu verwenden, zahlen Sie typische Amazon VPC Site-to-Site-VPN-Verbindungsraten. 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 CloudHubs Daten von einem Standort zum anderen senden, entstehen Ihnen keine Kosten für die Übermittlung von Daten von Ihrem Standort zum Virtual Private Gateway. Sie bezahlen nur den standardmäßigen AWS-Übertragungssatz für Daten, die vom Virtual Private Gateway zu Ihrem Endpunkt übermittelt werden.

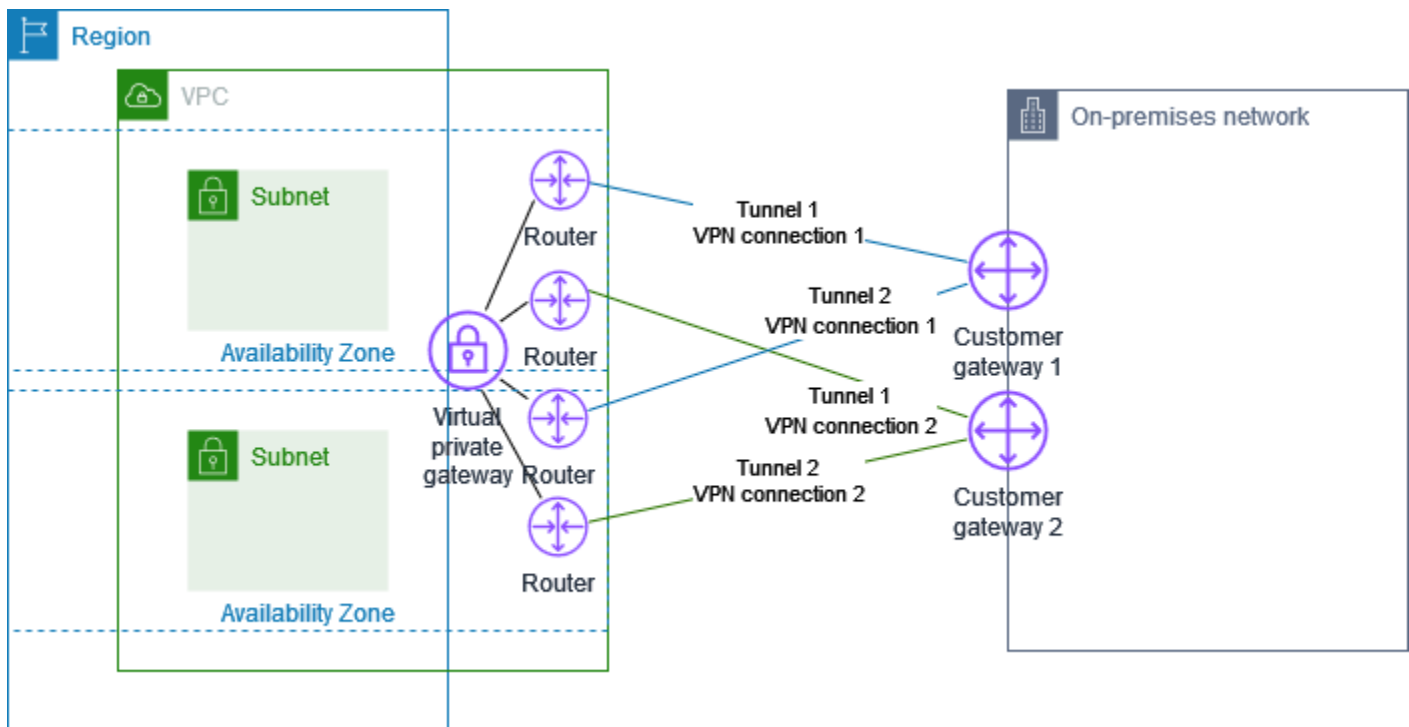
Wenn Sie z. B. einen Standort in Los Angeles und einen zweiten Standort in New York haben und beide Standorte eine Site-to-Site-VPN-Verbindung mit dem Virtual Private Gateway haben, zahlen Sie den Stundensatz für jede Site-to-Site-VPN-Verbindung (wenn der Satz beispielsweise 0,05 USD/Stunde beträgt, sind das insgesamt 0,10 USD/Stunde). Sie zahlen außerdem die Standard-AWS-Datenübertragungsraten für alle Daten, die Sie von Los Angeles nach New York (und umgekehrt) über jede Site-to-Site-VPN-Verbindung senden. Netzwerkverkehr, der über die Site-to-Site-VPN-Verbindung zum Virtual Private Gateway gesendet wird, ist kostenlos. Netzwerkverkehr, der über die Site-to-Site-VPN-Verbindung vom Virtual Private Gateway zum Endpunkt gesendet wird, wird mit der Standard-AWS-Datenübertragungsrate berechnet.

Weitere Informationen finden Sie unter [Site-to-Site-VPN-Verbindungen – Preise](#).

Verwenden redundanter Site-to-Site-VPN-Verbindungen zur Bereitstellung von Failover

Um sich vor dem Verlust der Konnektivität zu schützen, wenn Ihr Kunden-Gateway-Gerät nicht verfügbar ist, können Sie eine zweite Site-to-Site-VPN-Verbindung mit 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 IP-Adresse des Kunden-Gateways 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 weitergeleitete Site-to-Site-VPN-Verbindungen verwenden das Border Gateway Protocol (BGP), um Routing-Informationen zwischen Ihren Kunden-Gateways und den Virtual Private Gateways auszutauschen. Für statisch geroutete Site-to-Site-VPN-Verbindungen müssen Sie auf Ihrer Seite des Kunden-Gateways statische Routen für das Remote-Netzwerk 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

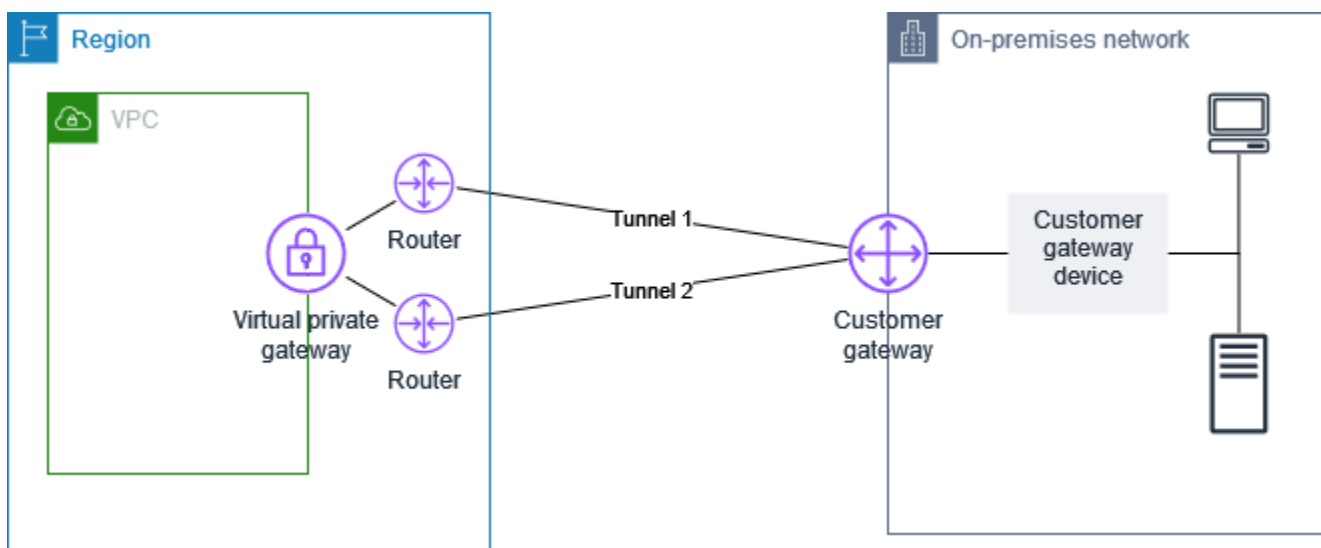
bereitgestellten Routing-Informationen verwendet (sofern verfügbar), um einen verfügbaren Pfad auszuwählen. Die genaue Konfiguration hängt von der Architektur Ihres Netzwerks ab.

Weitere Informationen zur Erstellung und Konfiguration eines Kunden-Gateways und einer Site-to-Site-VPN-Verbindung finden Sie unter [Erste Schritte mit AWS Site-to-Site VPN](#).

Ihr Kunden-Gateway-Gerät

Ein Kunden-Gateway-Gerät ist eine physische oder Software-Anwendung, die Sie in Ihrem On-Premise-Netzwerk (auf Ihrer Seite einer Site-to-Site-VPN-Verbindung) besitzen oder verwalten. 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 im Inneren 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 [Ersatz für Site-to-Site VPN-Tunnelendpunkte](#). 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 [Erste Schritte 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 [Optionen für das Kunden-Gateway für Ihre 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](#).

Themen

- [Beispielkonfigurationsdateien](#)
- [Anforderungen für Ihr Kunden-Gateway-Gerät](#)
- [Bewährte Methoden für Ihr Kunden-Gateway-Gerät](#)
- [Konfigurieren einer Firewall zwischen dem Internet und Ihrem Kunden-Gateway-Gerät](#)
- [Szenarien mit mehreren VPN-Verbindungen](#)
- [Routing für Ihr Kunden-Gateway-Gerät](#)
- [Beispiel für Kunden-Gateway-Gerätekonfigurationen für statisches Routing](#)
- [Beispiel für Kunden-Gateway-Gerätekonfigurationen für dynamisches Routing \(BGP\)](#)
- [Konfigurieren von Windows Server als Kunden-Gateway-Gerät](#)
- [Fehlerbehebung für Ihr Kunden-Gateway-Gerät](#)

Beispielkonfigurationsdateien

Nachdem Sie die VPN-Verbindung erstellt 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 herunterladen, die speziell für statisches und dynamisches Routing geeignet sind:

Zip-Dateien herunterladen

- Statische Konfiguration: [the section called “Beispielkonfigurationsdateien”](#)
- Dynamische Konfiguration: [the section called “Beispielkonfigurationsdateien”](#)

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 ist nur ein Beispiel und entspricht möglicherweise nicht vollständig den von Ihnen beabsichtigten Site-to-Site-VPN-Verbindungseinstellungen. Es 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 IPv6-Datenverkehr zu nutzen.

Note

Diese AWS gerätespezifischen Konfigurationsdateien werden nach bestem Wissen und Gewissen von 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 der Geräte, für die eine Beispielkonfigurationsdatei zum Download verfügbar ist, die aktualisiert wurde, um IKEv2 zu unterstützen. Wir haben IKEv2-Support in den Konfigurationsdateien für viele gängige 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

Hersteller	Plattform	Software
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+

Anforderungen für Ihr Kunden-Gateway-Gerät

Wenn Sie über ein Gerät verfügen, das nicht in der vorstehenden Liste von Beispielen aufgeführt ist, beschreibt dieser Abschnitt die Anforderungen, die das Gerät erfüllen muss, damit Sie es zum Aufbau einer Site-to-Site-VPN-Verbindung verwenden können.

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 erforderlich, um Schlüssel auszutauschen, die zum Aufbau der IPsec-Sicherheitszuordnung verwendet werden.
IPsec	IPsec-Sicherheitszuordnung. 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 umfasst eine IKE-Sicherheitsaushandlung, eine IPsec-Sicherheitsaushandlung und ein BGP-Peering. Sie sind auf ein Sicherheitszuordnungspaar (SA) pro Tunnel (ein eingehendes und ein ausgehendes) und somit auf zwei eindeutige SA-Paare für insgesamt zwei Tunnel (vier SAs) beschränkt. Einige Geräte nutzen eine richtlinienbasierte VPN und erstellen so viele SAs, wie ACL-Einträge vorhanden sind. 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 [Initiierungsoptionen für Site-to-Site-VPN-Tunnel](#).

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	RFC 2409 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.
IKE		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

Anforderung	RFC	Kommentare
		<p>VPN-Tunneln finden Sie unter Tunnel-Optionen für Ihre Site-to-Site-VPN-Verbindung.</p> <p>Die folgenden Versionen werden unterstützt: IKEv1 und IKEv2.</p> <p>Wir unterstützen den Hauptmodus nur mit IKEv1.</p> <p>Der Site-to-Site VPN-Service ist eine routenbasierte Lösung. Wenn Sie eine richtlinienbasierte Konfiguration verwenden, müssen Sie Ihre Konfiguration auf eine einzelne Sicherheitszuordnung beschränken.</p>
<p>Herstellen von IPsec Sicherheitsaushandlungen im Tunnel-Modus</p> 	RFC 4301	<p>Mit dem temporären IKE-Schlüssel werden Schlüssel für eine IPsec-Sicherheitsaushandlung (SA) zwischen dem Virtual Private Gateway und dem Kunden-Gateway-Gerät ausgetauscht. Der Datenverkehr zwischen den Gateways wird über diese SA ver- und entschlüsselt. Die zur Verschlüsselung des Datenverkehrs in der IPsec-SA verwendeten temporären Schlüssel werden automatisch regelmäßig von IKE rotiert. So ist die Vertraulichkeit der Kommunikation sichergestellt.</p>
Verwenden der AES 128-Bit- oder AES 256-Bit-Verschlüsselungsfunktion	RFC 3602	Die Verschlüsselungsfunktion wird zum Schutz der Daten zwischen IKE- und IPsec-Sicherheitsaushandlungen verwendet.
Verwenden Sie die SHA-1- oder SHA-2 (256)-Hash-Funktion	RFC 2404	Diese Hash-Funktion wird zur Authentifizierung der Daten zwischen IKE- und IPsec-Sicherheitsaushandlungen verwendet.

Anforderung	RFC	Kommentare
Verwenden von Diffie-Hellman Perfect Forward Secrecy.	RFC 2409	<p>IKE nutzt Diffie-Hellman zur Etablierung der temporären Schlüssel zur Absicherung der gesamten Kommunikation zwischen Kunden-Gateway-Geräten und Virtual Private Gateways.</p> <p>Folgende Gruppen werden unterstützt:</p> <ul style="list-style-type: none"> • Phase 1-Gruppen: 2, 14-24 • Phase 2-Gruppen: 2, 5, 14-24
(Dynamisch geroutete VPN-Verbindungen) Verwenden Sie IPsec Dead Peer Detection	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 Prozesses wird, wenn möglich, der alternative IPsec-Tunnel verwendet.
(Dynamisch geroutete VPN-Verbindungen) Binden Sie den Tunnel an die logische Schnittstelle (routenbasiertes VPN)	None	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	RFC 4271	BGP wird zum Austausch von Routen zwischen dem Kunden-Gateway-Gerät und dem Virtual Private Gateway verwendet. Der gesamte BGP-Datenverkehr wird über die IPsec-Sicherheitsaushandlung verschlüsselt und übertragen. Zum Austausch der über die IPsec-SA erreichbaren IP-Präfixe ist für beide Gateways BGP erforderlich.

Tunnel

BGP

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. [Konfigurieren einer Firewall zwischen dem Internet und Ihrem Kunden-Gateway-Gerät](#).

Bewährte Methoden für Ihr Kunden-Gateway-Gerät

Verwenden Sie 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 IKEv1 nur verwenden, wenn Ihr Kunden-Gateway-Gerät IKEv2 nicht unterstützt. [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 einen höheren packet-per-second Datenfluss durch das Netzwerk zu erreichen. AWS 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 für Zielnetzwerke, an die diese Pakete als Nächstes weitergeleitet werden, Überlegungen zur Paketgröße/MTU möglicherweise zu berücksichtigen sind, z. B. über AWS Direct Connect

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

TCP-Pakete sind oft der häufigste Pakettyp über IPsec-Tunnel. 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-Traversal	MTU	MSS (IPv4)	MSS (IPv6-in-IPv4)
AES-GCM-16	N/A	disabled	1446	1406	1386
AES-GCM-16	N/A	aktiviert	1438	1398	1378
AES-CBC	SHA1/SHA2-256	disabled	1438	1398	1378
AES-CBC	SHA1/SHA2-256	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 eindeutige IKE-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.

Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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 Endpunkten verbinden. AWS Site-to-Site VPN 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 mit verschlüsseltem Netzwerkverkehr.

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.

Szenarien mit mehreren VPN-Verbindungen

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 zusätzliche VPN-Verbindungen von Ihrem On-Premise-Standort zu anderen VPCs unter Verwendung desselben Kunden-Gateway-Geräts erstellen. Sie können auf dem Kunden-Gateway eine einzige IP-Adresse für alle VPN-Verbindungen verwenden.

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 [Verwenden redundanter Site-to-Site-VPN-Verbindungen zur Bereitstellung von Failover](#). Wenn Sie redundante Kunden-Gateway-Geräte an einem Standort einrichten, sollten beide Geräte dieselben IP-Bereiche ankündigen.

Mehrere Kunden-Gateway-Geräte zu einem einzigen virtuellen privaten Gateway (VPC) 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 [Ermöglichen einer sicheren Kommunikation zwischen Standorten über 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.

Routing für Ihr Kunden-Gateway-Gerät

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 [Routing-Tabellen und VPN-Routenpriorität](#).

Beispiel für Kunden-Gateway-Gerätekonfigurationen für statisches Routing

Themen

- [Beispielkonfigurationsdateien](#)
- [Verfahren für statisches Routing über die Benutzeroberfläche](#)
- [Zusätzliche Informationen für Cisco-Geräte](#)
- [Testen](#)

Beispielkonfigurationsdateien

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 Amazon EC2 EC2-API. Weitere Informationen finden Sie unter [Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen](#).

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

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

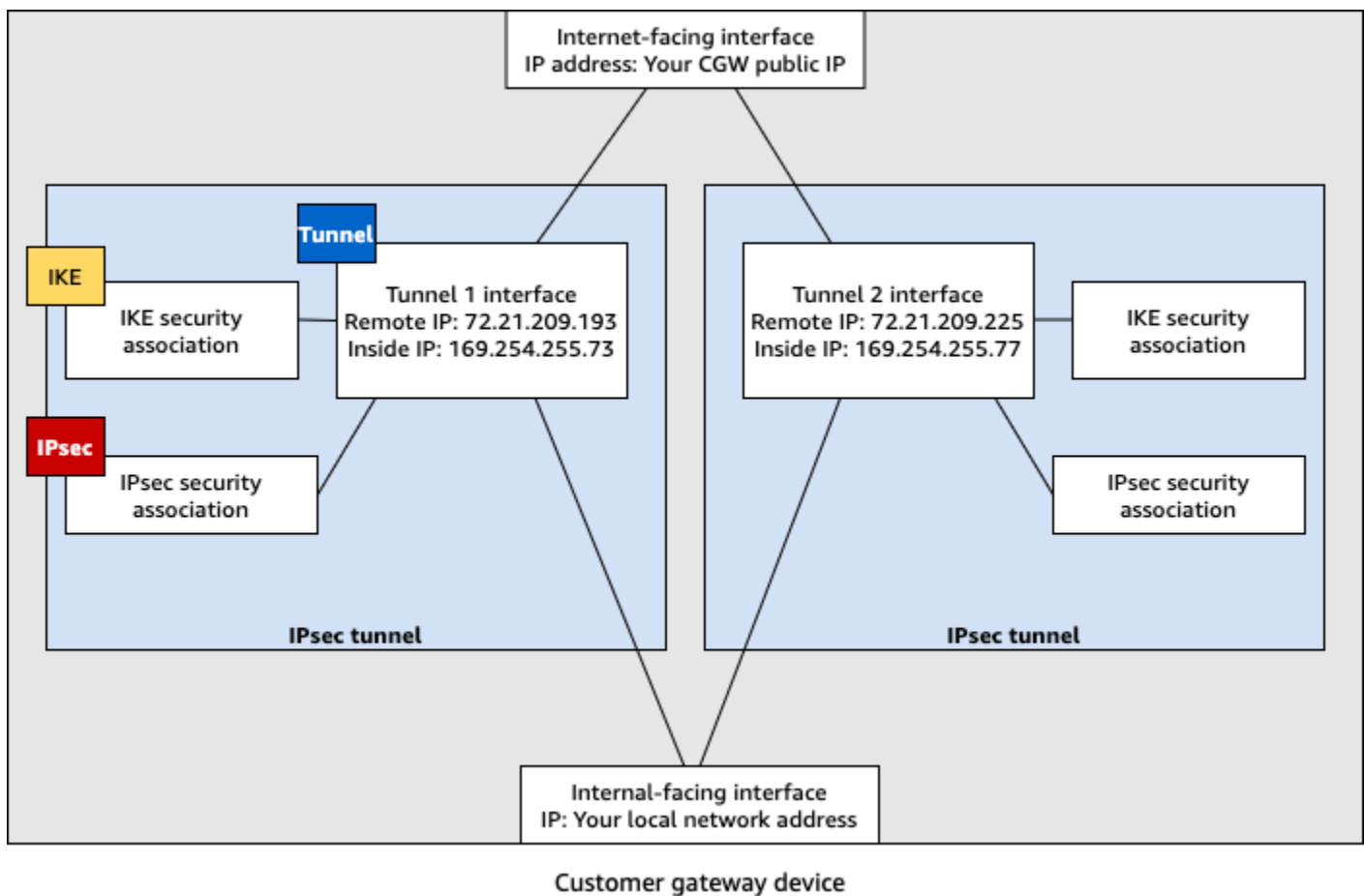
- Beispielwerte für die VPN-Verbindungs-ID, die Kunden-Gateway-ID und die ID des Virtual Private Gateways
- *Platzhalter für die (externen) AWS Remote-IP-Adressendpunkte (AWS_ENDPOINT_1 und AWS_ENDPOINT_2)*
- Ein Platzhalter für die IP-Adresse für die über das Internet routbare externe Schnittstelle auf dem Kunden-Gateway-Gerät (*your-cgw-ip-address*)
- Ein Platzhalter für den vorab freigegebenen Schlüsselwert (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 Ihr 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 und Diffie-Hellman-Gruppen sowie private Zertifikate und IPv6 zu nutzen.

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.



Verfahren für statisches Routing über die Benutzeroberfläche

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

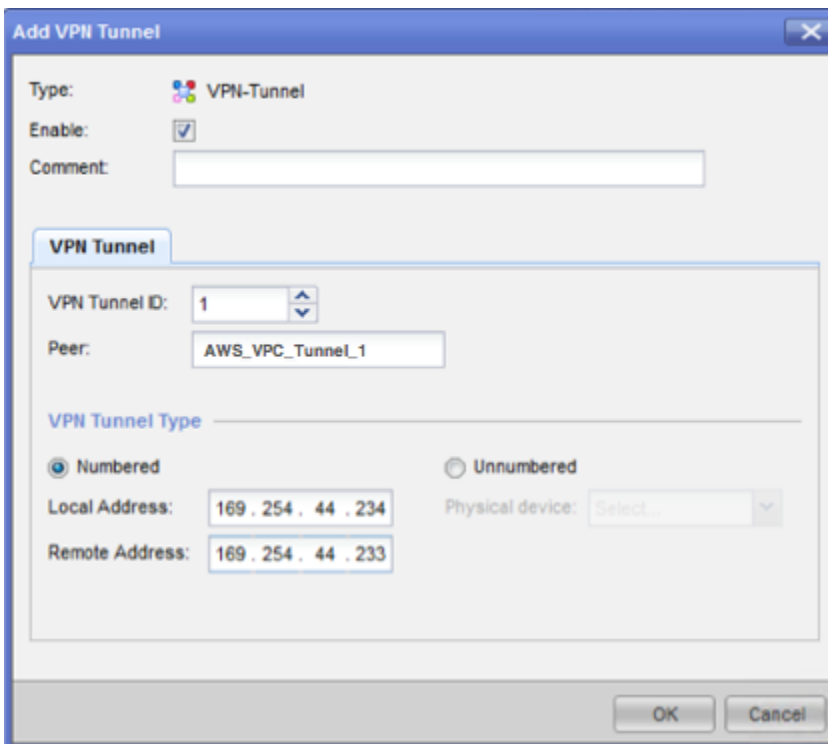
Check Point

Im Folgenden finden Sie Schritte zur Konfiguration Ihres Kunden-Gateway-Geräts, wenn 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 zu 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. Klicken Sie im Gaia-Portal auf IPv4 Static Routes und Add.
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.

Destination: 10.28.13.0/24

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

Local Scope:

Comment:

Add Gateway

Ping:

Gateway	Priority
169.254.44.233	1
169.254.44.5	2

Save Cancel

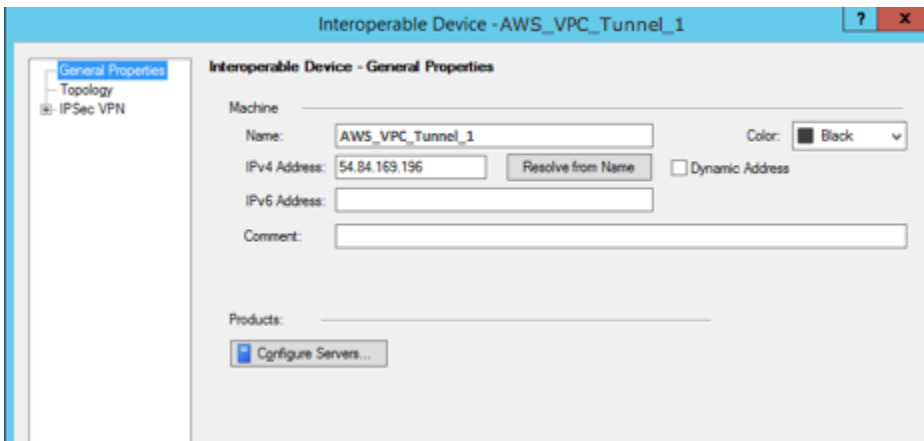
7. Wählen Sie Speichern.

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_Tunnel1_1 oder AWS_VPC_Tunnel1_2.
5. Geben Sie unter IPv4 Address die externe IP-Adresse des Virtual Private Gateways aus der Konfigurationsdatei ein, z. B. 54.84.169.196. 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

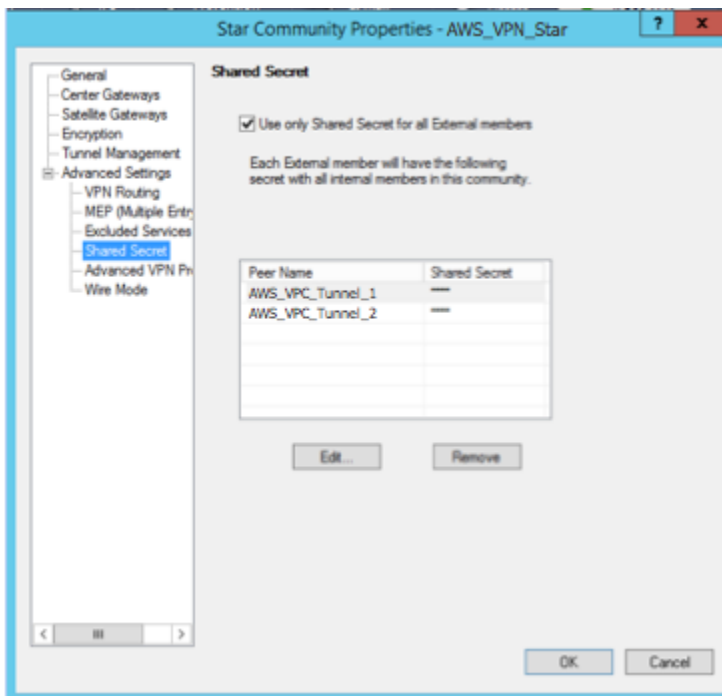
Wenn Sie Cluster verwenden, bearbeiten Sie die Topologie und legen Sie die Schnittstellen als Cluster-Schnittstellen fest. Verwenden Sie die IP-Adressen, die in der Konfigurationsdatei angegeben sind.

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. Außerdem konfigurieren Sie die IKE- und IPsec-Einstellungen.

1. Klicken Sie in den Gateway-Eigenschaften im Kategoriebereich auf `IPsec VPN`.
2. Klicken Sie auf `Communities, New and 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 Bereich `Encryption Method` `IKEv1 only` 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
 - Eigenschaften von IPsec Security Association (Phase 2):
 - Perform IPsec data encryption with: 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
 - Renegotiate IPsec security associations every 3600 seconds

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 Eigenschaft `tunnel_keepalive_method` mit dem GuiDBedit-Tool bearbeiten.

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 GuiDBedit-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 `GuiDBedit`-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 aus den angezeigten Optionen 1 aus, um die `IKE-Zuordnungen` zu überprüfen, und 2, um die `IPsec-Zuordnungen` 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		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

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): Wählen 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 Primary Gateway Name or Address: Geben Sie das Virtual Private Gateway IP aus der Konfigurationsdatei ein (z. B. 72.21.209.193).
 - IPsec Secondary Gateway Name or Address: Übernehmen Sie den Standardwert.
 - Shared Secret: Geben Sie den vorinstallierten Schlüssel aus der Konfigurationsdatei ein. Geben Sie ihn erneut in Confirm Shared Secret ein.
 - Local IKE ID: Geben Sie die IPv4-Adresse des Kunden-Gateways ein (das SonicWALL-Gerät).
 - Peer IKE ID: Geben Sie die IPv4-Adresse des Virtual Private 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.
 - Authentication: Wählen Sie SHA1 oder SHA256 aus.
 - 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.
 - Authentication: Wählen Sie SHA1 oder SHA256 aus.
 - 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 die Diffie-Hellman-Gruppe 2, AES-128 und SHA1 für beide Phasen angeben.

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.

Zusätzliche Informationen für Cisco-Geräte

Einige Cisco ASAs unterstützen nur den Aktiv-/Standby-Modus. Wenn Sie eine solche Cisco ASA verwenden, kann nur ein Tunnel gleichzeitig aktiv sein. 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 ASAs ab Version 9.7.1 und höher unterstützen den Aktiv/Aktiv-Modus. Wenn Sie diese Cisco ASAs verwenden, können beide Tunnel gleichzeitig aktiv sein. 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-Richtliniensequenz auf sonstige auf dem Gerät konfigurierte IPsec-Tunnel abgestimmt sind.

- 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.

Testen

Weitere Informationen zum Testen Ihrer Site-to-Site-VPN-Verbindung finden Sie unter [Eine Site-to-Site VPN-Verbindung testen](#).

Beispiel für Kunden-Gateway-Gerätekonfigurationen für dynamisches Routing (BGP)

Themen

- [Beispielkonfigurationsdateien](#)
- [Verfahren für dynamisches Routing über die Benutzeroberfläche](#)
- [Zusätzliche Informationen für Cisco-Geräte](#)
- [Zusätzliche Informationen für Juniper-Geräte](#)
- [Testen](#)

Beispielkonfigurationsdateien

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 Amazon EC2 EC2-API. Weitere Informationen finden Sie unter [Schritt 6: Die Endpunkt-Konfigurationsdatei herunterladen](#).

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

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

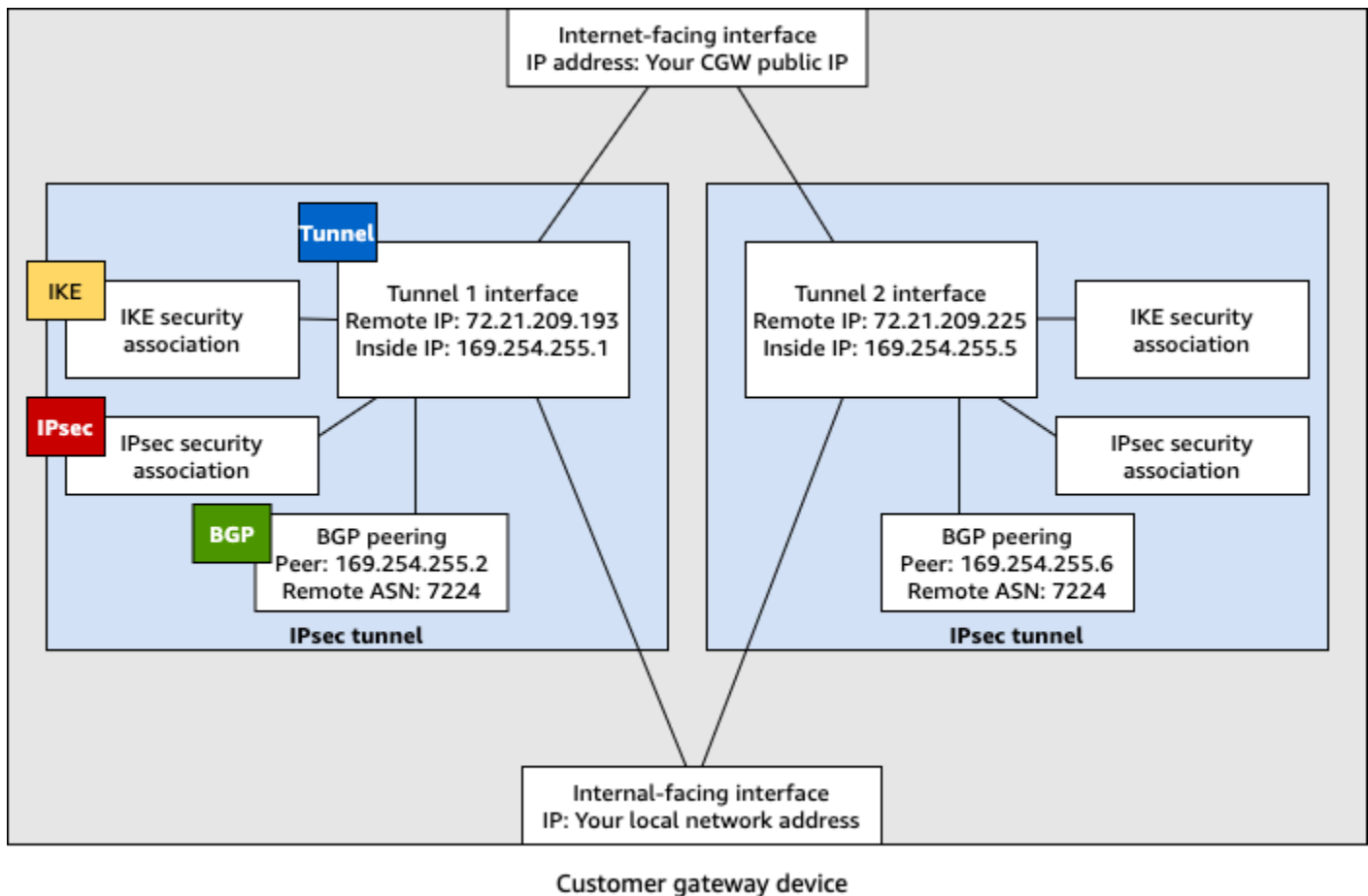
- *Platzhalter für die (externen) AWS Remote-IP-Adressendpunkte (AWS_ENDPOINT_1 und AWS_ENDPOINT_2)*
- Ein Platzhalter für die IP-Adresse für die über das Internet routbare externe Schnittstelle auf dem Kunden-Gateway-Gerät (*your-cgw-ip-address*)
- Ein Platzhalter für den vorab freigegebenen Schlüsselwert (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 Ihr 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 und Diffie-Hellman-Gruppen sowie private Zertifikate und IPv6 zu nutzen.

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.



Verfahren für dynamisches Routing über die Benutzeroberfläche

Im Folgenden finden Sie einige Beispielfahrer 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 **Speichern**.

So kündigen Sie lokale Routen an

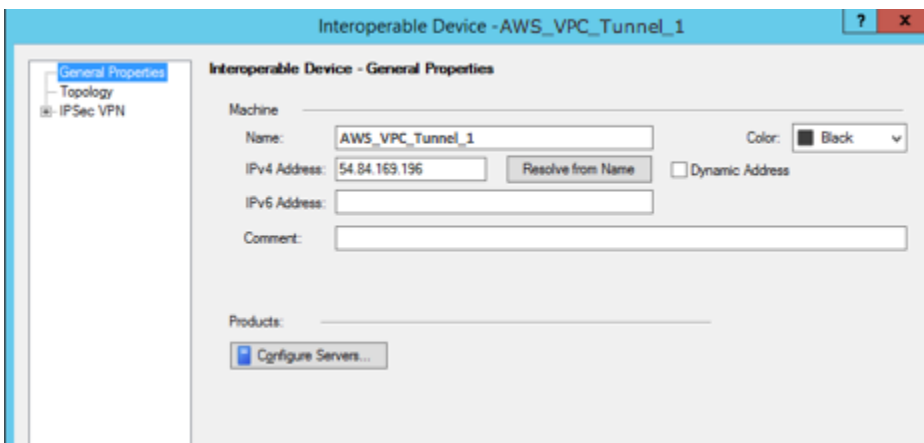
In den folgenden Schritten wird die Verteilung von lokalen Schnittstellenrouten beschrieben. Sie können Routen auch von anderen Quellen neu verteilen, z. B. statische Routen oder Routen, die Sie über dynamische Routing-Protokolle erhalten haben. Weitere Informationen finden Sie unter [Gaia Advanced Routing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

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 Address die externe IP-Adresse des Virtual Private Gateways aus der Konfigurationsdatei ein, z. B. 54.84.169.196. 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.

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

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

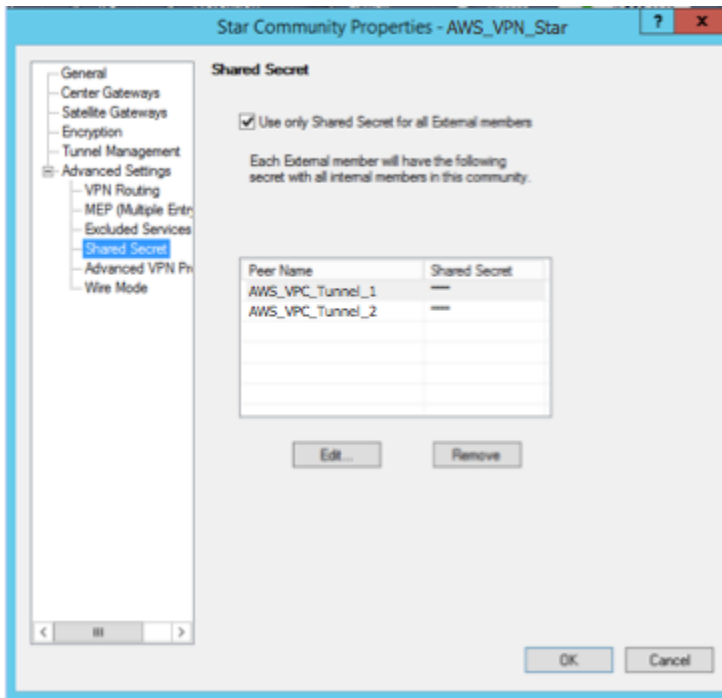
1. Klicken Sie in den Gateway-Eigenschaften im Kategoriebereich auf IPsec VPN.
2. Klicken Sie auf Communities, New und Star Community.
3. Geben Sie einen Namen für die Community ein (z. B. AWS_VPN_Star) und klicken Sie im Kategoriebereich auf Center Gateways.
4. Klicken Sie auf Add und fügen Sie Ihr 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. Klicken Sie im Bereich Encryption Method auf IKEv1 for IPv4 and IKEv2 for IPv6. Wählen Sie im Bereich Encryption Suite Custom und Custom Encryption aus.

 Note

Sie müssen die Option IKEv1 for IPv4 and IKEv2 for IPv6 (IKEv1 für IPv4 und IKEv2 für IPv6) für die IKEv1-Funktionalität 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
 - Eigenschaften von IPsec Security Association (Phase 2):
 - Perform IPsec data encryption with: 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)
 - Renegotiate IPsec security associations every 3600 seconds

So erstellen Sie Firewall-Regeln

Dann konfigurieren Sie eine Richtlinie mit Firewall-Regeln und directionalen 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 Eigenschaft `tunnel_keepalive_method` mit dem GuiDBedit-Tool bearbeiten.

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 GuiDBedit-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 GuiDBedit-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.

- 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 aus den angezeigten Optionen 1 aus, um die IKE-Zuordnungen zu überprüfen, und 2, um die IPsec-Zuordnungen 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		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

Sie können ein SonicWALL-Gerät über die SonicOS-Verwaltungsoberfläche konfigurieren. Weitere Informationen zur Konfiguration von Tunneln finden Sie unter [Verfahren für statisches Routing über die Benutzeroberfläche](#).

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.

Zusätzliche Informationen für Cisco-Geräte

Einige Cisco ASAs unterstützen nur den Aktiv-/Standby-Modus. Wenn Sie eine solche Cisco ASA verwenden, kann nur ein Tunnel gleichzeitig aktiv sein. 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 ASAs ab Version 9.7.1 und höher unterstützen den Aktiv/Aktiv-Modus. Wenn Sie diese Cisco ASAs verwenden, können beide Tunnel gleichzeitig aktiv sein. 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-Richtliniensequenz auf sonstige auf dem Gerät konfigurierte IPsec-Tunnel abgestimmt sind.
- 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.

Zusätzliche Informationen für Juniper-Geräte

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

- Die Schnittstelle nach außen wird als *ge-0/0/0/0* bezeichnet.
- Die Tunnel-Schnittstellen-IDs werden als *st0.1* und *st0.2* bezeichnet.
- 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).

Testen

Weitere Informationen zum Testen Ihrer Site-to-Site-VPN-Verbindung finden Sie unter [Eine Site-to-Site VPN-Verbindung testen](#).

Konfigurieren von Windows Server als Kunden-Gateway-Gerät

Sie können einen Server mit Windows Server als Kunden-Gateway-Gerät für Ihre VPC konfigurieren. Die folgende Anleitung kann unabhängig davon angewendet werden, ob Sie Windows Server auf einer EC2-Instance 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 von einem Windows-AMI aus gestartet haben, gehen Sie wie folgt vor:

- Deaktivieren Sie für die Instance die Quell-/Zielprüfung:
 1. Öffnen Sie die Amazon EC2-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 IPv4-Prüfsummenabladung, TCP-Prüfsummenabladung (IPv4) und UDP-Prüfsummenabladung (IPv4). Wählen Sie anschließend OK aus.
- Weisen Sie Ihrem Konto eine Elastic-IP-Adresse zu und ordnen Sie diese der Instance zu. Weitere Informationen finden Sie unter [Arbeiten mit Elastic IP-Adressen](#). Merken Sie sich diese Adresse – Sie werden sie brauchen, wenn Sie das Kunden-Gateway in Ihrer VPC erstellen.
 - Stellen Sie sicher, dass die Sicherheitsgruppenregeln der Instance 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 ausgehenden Protokollregeln für IPsec-Datenverkehr festlegen: 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 (Site-to-Site-VPN-Verbindungen) 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:              xCjNLSLoCmKsawcdoR9yX6GsEXAMPLE
```

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 vorinstallierte Schlüssel, der zum Herstellen der IPsec-VPN-Verbindung zwischen `Local Tunnel Endpoint` und `Remote Tunnel Endpoint` verwendet wird.

Wir empfehlen, dass Sie beide Tunnel als Teil der VPN-Verbindung 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 zum Internet Key Exchange (IKE) und zu IPsec-Sicherheitszuweisungen (Security Associations, SA) können Sie der heruntergeladenen Konfigurationsdatei entnehmen.

```
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, die den Standardeinstellungen für IPsec-VPN-Verbindungen für Windows Server entsprechen.

MainModeKeyLifetime

Die Lebensdauer des IKE-SA-Schlüssels. Dies sind die empfohlenen Einstellungen für die VPN-Verbindung, die den Standardeinstellungen für IPsec-VPN-Verbindungen für Windows Server entsprechen.

QuickModeSecMethods

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

QuickModePFS

Wir empfehlen, für IPsec-Sitzungen PFS-fähige (Perfect Forward Secrecy) Master Keys zu verwenden.

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 (Remotenzugriff) 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 Remotenzugriff 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 Remotenzugriff-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 Remotenzugriff) den Servernamen, dann Action (Aktion) und anschließend Configure and Enable Routing and 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 Remotenzugriff 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 IPsec-Sitzungen zu verwenden. 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=xCjNLSLoCmKsawcdOR9yX6GsEXAMPLE ^
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 ausschließen? den Standardwert Nein. Über den Tunnel sämtlichen Netzwerkdatenverkehr senden, der dieser Verbindungssicherheitsregel entspricht. ausgewählt und klicken Sie auf Weiter.
5. Wählen Sie auf der Seite mit den 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 Feld IPv4-Adresse die private IP-Adresse Ihres Windows-Servers ein und wählen Sie dann OK aus.
8. Wählen Sie unter Was ist der Remotetunnelendpunkt (am nächsten zu Computern in Endpunkt 2)? die Option Bearbeiten aus. Geben Sie in das Feld IPv4-Adresse die IP-Adresse des Virtual Private Gateways für Tunnel 1 aus der Konfigurationsdatei ein (siehe Remote Tunnel Endpoint) und wählen Sie dann OK aus.

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 aus.
16. Aktivieren Sie auf der Seite Profile (Profil) die drei Kontrollkästchen Domain (Domäne), Private (Privat) und Public (Öffentlich). Wählen Sie Weiter aus.
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 Anpassen aus. Prüfen Sie die folgende IPsec-Tunneling-Einstellungen, wählen Sie dann OK und anschließend noch einmal OK zum Schließen des Dialogfensters aus.
 - 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-Instance handelt, ist dies die private IP-Adresse der Instance.
 - 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 die Sicherheitsregeln auf dem Server eingerichtet haben, konfigurieren Sie einige grundlegende IPsec-Einstellungen für das 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. Prüfen Sie auf der Registerkarte IPsec-Einstellungen unter IPsec-Ausnahmen, ob ICMP aus IPsec ausschließen auf Nein (Standard) eingestellt ist. Überprüfen Sie, ob für IPsec-Tunnelautorisierung die Option Keine ausgewählt ist.
3. Wählen Sie unter IPsec-Standardinstellungen 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 aus, um zum Dialogfeld Customize IPsec Settings (IPsec-Einstellungen anpassen) zurückzukehren, und wählen Sie dann erneut OK aus, 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 CurrentControlSet, erweitern Sie Services, erweitern Sie Tcpip und erweitern Sie dann Parameters.
3. Wählen Sie aus dem Menü Bearbeiten die Option Neu und anschließend DWORD-Wert (32-Bit).
4. Geben EnableDeadSie den Namen GWDetect ein.
5. Wählen Sie EnableDeadGWDetect aus und wählen Sie Bearbeiten, Ändern.
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 unter [EnableDeadGWDetect](#) in 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 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-Instance handelt, stellen Sie sicher, dass die Regeln für ausgehenden Datenverkehr der Sicherheitsgruppe 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, eines der Amazon Linux-AMIs zu verwenden.
- Wenn es sich bei der Instance, an die Sie ein Ping schicken, um eine Windows-Instance handelt, stellen Sie eine Verbindung zu der Instance her und aktivieren Sie das in der Windows-Firewall eingehende ICMPv4.
- 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, überprüfen Sie, ob für die Instance die Quell-/Zielprüfung deaktiviert wurde. 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 für Ihr Kunden-Gateway-Gerät

Die folgenden Themen können Ihnen bei der Behebung von Verbindungsproblemen auf Kunden-Gateway-Geräten helfen.

Allgemeine Testanweisungen finden Sie unter [Eine Site-to-Site VPN-Verbindung testen](#).

Zusätzlich zu den Themen in diesem Abschnitt können Sie auch [AWS Site-to-Site VPN Logs](#) zur Behebung und Lösung von VPN-Verbindungsproblemen verwenden.

Themen

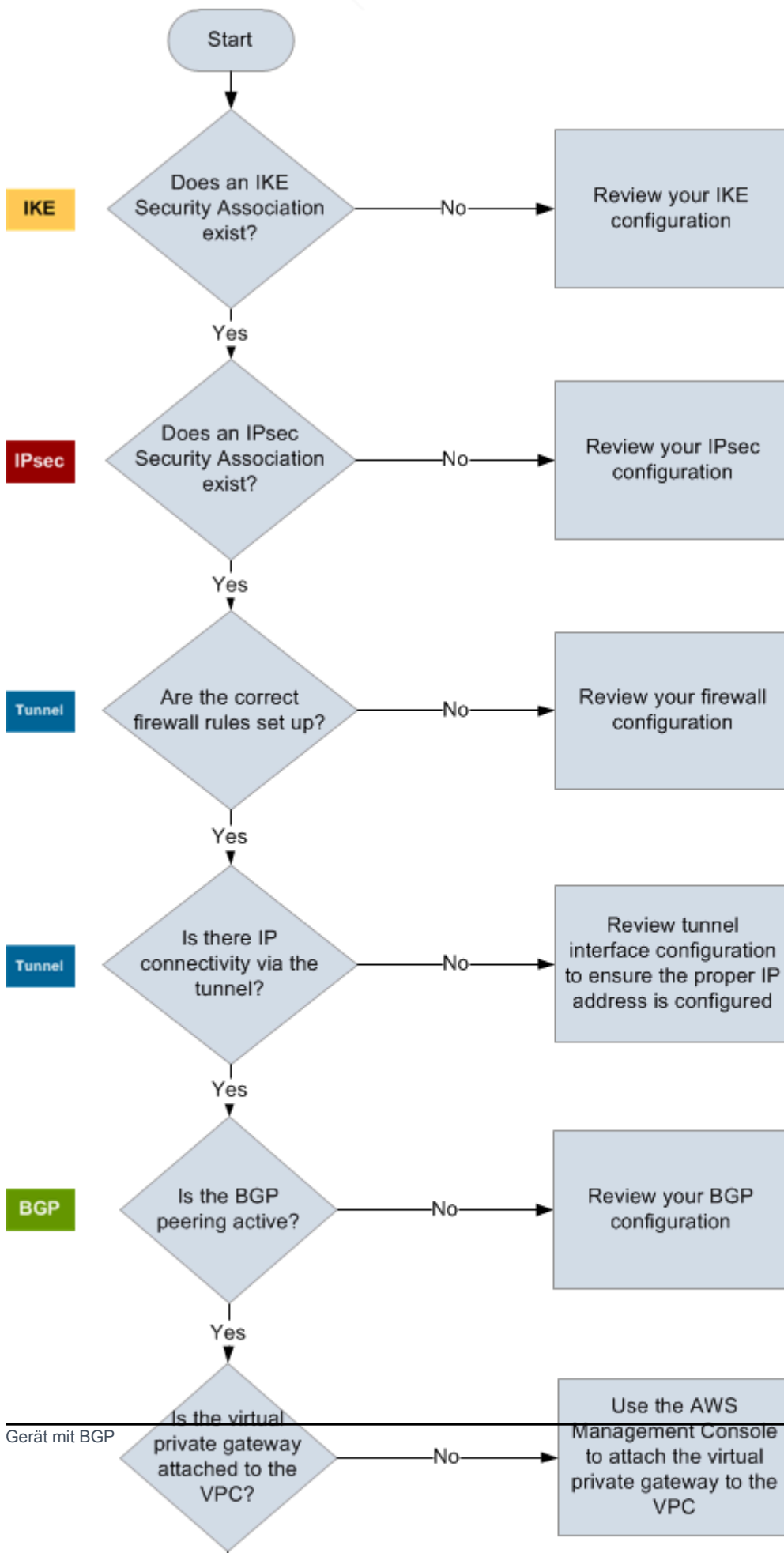
- [Fehlerbehebung bei der Konnektivität bei Verwendung des Border Gateway-Protokolls](#)
- [Fehlerbehebung bei Konnektivität ohne Border Gateway-Protokoll](#)
- [Fehlerbehebung bei der Konnektivität von Cisco ASA-Kunden-Gateway-Geräten](#)
- [Fehlerbehebung bei der Konnektivität von Cisco IOS-Kunden-Gateway-Geräten](#)
- [Fehlersuche für Cisco IOS-Kunden-Gateway-Konnektivität ohne Border Gateway-Protokoll-Konnektivität](#)
- [Fehlerbehebung bei der Konnektivität von Juniper JunOS-Kunden-Gateway-Geräten](#)
- [Fehlerbehebung bei der Konnektivität von Juniper ScreenOS-Kunden-Gateway-Geräten](#)
- [Fehlerbehebung bei der Konnektivität von Yamaha-Kunden-Gateway-Geräten](#)

Weitere Ressourcen

- [Amazon VPC-Forum](#)
- [Wie behebe ich Probleme bei der VPN-Tunnelverbindung mit meiner Amazon VPC?](#)

Fehlerbehebung bei der Konnektivität bei Verwendung des Border Gateway-Protokolls

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.



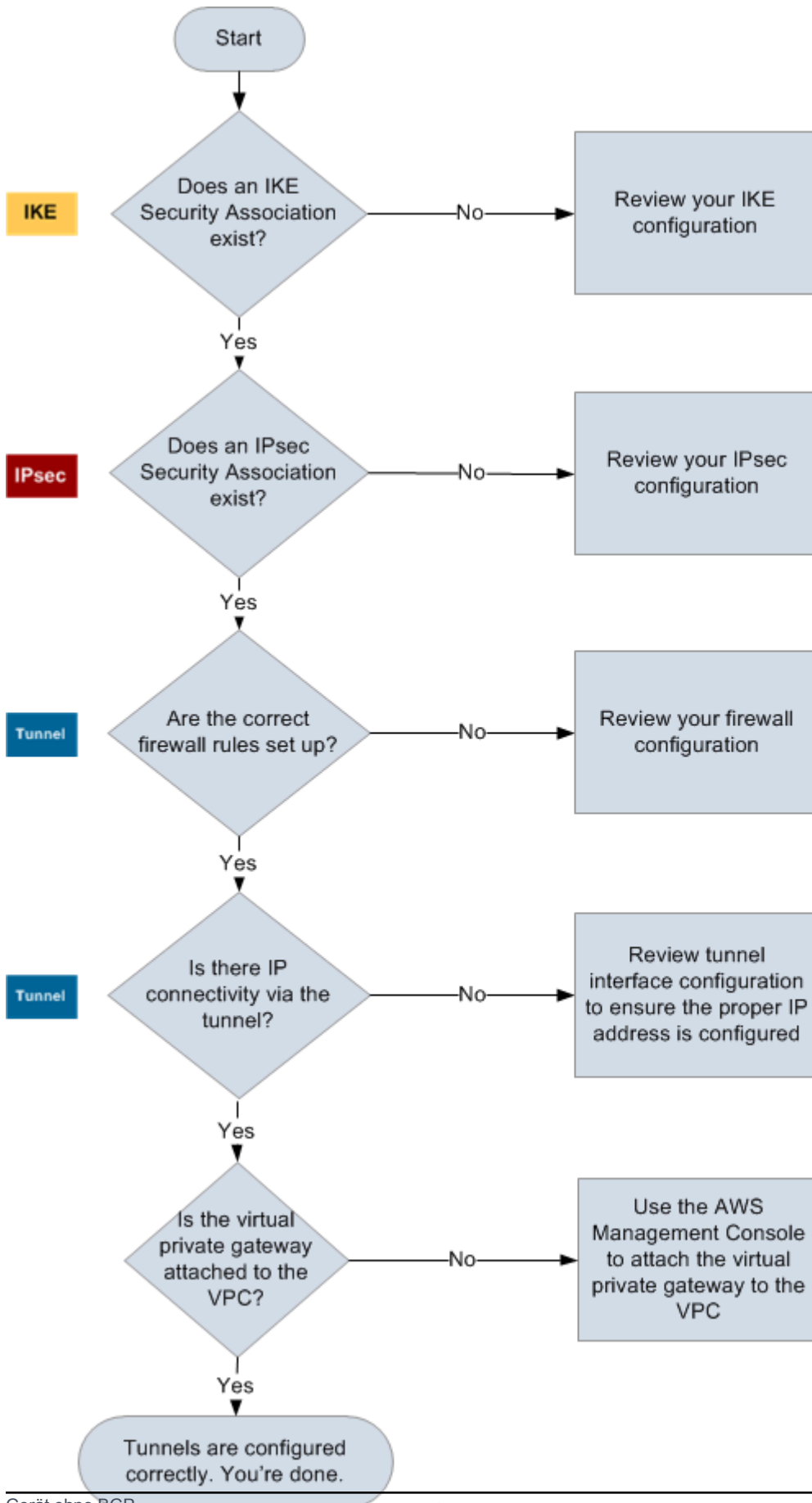
Gerät mit BGP

IKE	<p>Überprüfen Sie, ob eine IKE Sicherheitsaushandlung vorhanden ist.</p> <p>Diese ist für den Austausch von Schlüsseln erforderlich, die zur Herstellung der IPsec Sicherheitsaushandlung verwendet werden.</p> <p>Wenn keine IKE Security Association vorhanden ist, überprüfen Sie Ihre IKE-Konfigurationseinstellungen. Sie müssen die Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modusparameter entsprechend der Konfigurationsdatei konfigurieren.</p> <p>Wenn eine IKE Sicherheitsaushandlung vorhanden ist, fahren Sie mit "Ipsec" fort.</p>
IPsec	<p>Überprüfen Sie, ob eine Ipsec-Sicherheitsaushandlung (SA) vorhanden ist.</p> <p>Ein 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.</p> <p>Wenn keine IPsec-SA existiert, überprüfen Sie Ihre IPsec-Konfiguration.</p> <p>Wenn eine IPsec-SA existiert, fahren Sie mit "Tunnel" fort.</p>
Tunnel	<p>Stellen Sie sicher, dass die erforderlichen Firewall-Regeln eingerichtet sind. Eine Liste der Regeln finden Sie unter Konfigurieren einer Firewall zwischen dem Internet und Ihrem Kunden-Gateway-Gerät. Wenn die Regeln korrekt eingerichtet sind, fahren Sie fort.</p> <p>Stellen Sie fest, ob eine IP-Konnektivität durch den Tunnel besteht.</p> <p>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 entschlüsselt wird.</p> <p>Sollte dies fehlschlagen, überprüfen Sie die Konfiguration der Tunnelschnittstelle, um sicherzustellen, dass die korrekte IP-Adresse konfiguriert ist.</p>

	Wenn der Ping erfolgreich war, fahren Sie mit "BGP" fort.
BGP	<p>Bestimmen Sie, ob die BGP-Peering-Sitzung aktiv ist.</p> <p>Gehen Sie für jeden Tunnel wie folgt vor:</p> <ul style="list-style-type: none">• Überprüfen Sie auf Ihrem Kunden-Gateway-Gerät, ob der BGP-Status <code>Active</code> oder <code>Established</code> lautet. Es kann etwa 30 Sekunden dauern, bis BGP Peering aktiviert wird.• Überprüfen Sie, ob das Kunden-Gateway-Gerät die Standardroute (<code>0.0.0.0/0</code>) an das Virtual Private Gateway sendet. <p>Wenn die Tunnel einen anderen Zustand aufweisen, überprüfen Sie die BGP-Konfiguration.</p> <p>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.</p>

Fehlerbehebung bei Konnektivität ohne Border Gateway-Protokoll

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.



IKE	<p>Überprüfen Sie, ob eine IKE Sicherheitsaushandlung vorhanden ist.</p> <p>Diese ist für den Austausch von Schlüsseln erforderlich, die zur Herstellung der IPsec Sicherheitsaushandlung verwendet werden.</p> <p>Wenn keine IKE Security Association vorhanden ist, überprüfen Sie Ihre IKE-Konfigurationseinstellungen. Sie müssen die Verschlüsselung, Authentifizierung, Perfect Forward Secrecy und Modusparameter entsprechend der Konfigurationsdatei konfigurieren.</p> <p>Wenn eine IKE Sicherheitsaushandlung vorhanden ist, fahren Sie mit "Ipsec" fort.</p>
IPsec	<p>Überprüfen Sie, ob eine Ipsec-Sicherheitsaushandlung (SA) vorhanden ist.</p> <p>Ein 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.</p> <p>Wenn keine IPsec-SA existiert, überprüfen Sie Ihre IPsec-Konfiguration.</p> <p>Wenn eine IPsec-SA existiert, fahren Sie mit "Tunnel" fort.</p>
Tunnel	<p>Stellen Sie sicher, dass die erforderlichen Firewall-Regeln eingerichtet sind. Eine Liste der Regeln finden Sie unter Konfigurieren einer Firewall zwischen dem Internet und Ihrem Kunden-Gateway-Gerät. Wenn die Regeln korrekt eingerichtet sind, fahren Sie fort.</p> <p>Stellen Sie fest, ob eine IP-Konnektivität durch den Tunnel besteht.</p> <p>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 entschlüsselt wird.</p> <p>Sollte dies fehlschlagen, überprüfen Sie die Konfiguration der Tunnelschnittstelle, um sicherzustellen, dass die korrekte IP-Adresse konfiguriert ist.</p>

Wenn der Ping erfolgreich ist, fahren Sie mit "Statische Routen" fort.

Statische Routen

Gehen Sie für jeden Tunnel wie folgt vor:

- Stellen Sie sicher, dass Sie eine statische Route für das CIDR Ihrer VPC mit den Tunneln als nächstem Punkt eingerichtet haben.
- 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.

Wenn die Tunnel einen anderen Zustand aufweisen, überprüfen Sie die Gerätekonfiguration.

Stellen Sie sicher, dass beide Tunnel diesen Zustand aufweisen.

Fehlerbehebung bei der Konnektivität von Cisco ASA-Kunden-Gateway-Geräten

Wenn Sie die Konnektivität eines Cisco-Kunden-Gateway-Geräts beheben, berücksichtigen Sie IKE, IPsec und Routing. 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 ASAs unterstützen nur den Aktiv-/Standby-Modus. Wenn Sie eine solche Cisco ASA verwenden, kann nur ein Tunnel gleichzeitig aktiv sein. 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. Das Ergebnis ist ein Kunden-Gateway mit korrekt konfigurierter IPsec.

```
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, #rcv 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 aufgelistet (z. B. `spi: 0x48B456A6`) und IPsec korrekt konfiguriert ist.

Bei Cisco ASA startet IPsec erst, wenn entsprechender Datenverkehr (Datenverkehr, der verschlüsselt werden soll) gesendet wird. Um die IPsec dauerhaft zu aktivieren, sollten Sie SLA-Überwachung konfigurieren. Die SLA-Überwachung sendet dauerhaft interessanten Datenverkehr, damit die IPsec aktiv bleibt.

Sie können IPsec auch mit dem folgenden Ping-Befehl aktivieren und zu Verhandlungen zwingen.

```
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 dies funktioniert, sollte Ihr IPsec eingerichtet sein. Überprüfen Sie andernfalls Ihre Zugriffslisten und lesen Sie im vorherigen Abschnitt "IPsec" weiter.

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 einen Traceroute vom Cisco ASA-Gerät aus, um zu überprüfen, ob Sie die Amazon-Router erreichen (z. B. *AWS_ENDPOINT_1/_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.

Fehlerbehebung bei der Konnektivität von Cisco IOS-Kunden-Gateway-Geräten

Wenn Sie Konnektivitätsprobleme bei einem Cisco-Kunden-Gateway-Gerät beheben möchten, spielen dabei vier Faktoren eine Rolle: 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. Das Ergebnis ist ein Kunden-Gateway mit korrekt konfigurierter IPsec.


```
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. Dabei wird vorausgesetzt, dass ein SA (z. B. `spi: 0xF95D2F3C`) aufgeführt wird, der Status `ACTIVE` ist und IPsec korrekt konfiguriert 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 [Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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.

Fehlersuche für Cisco IOS-Kunden-Gateway-Konnektivität ohne Border Gateway-Protokoll-Konnektivität

Wenn Sie Konnektivitätsprobleme bei einem Cisco-Kunden-Gateway-Gerät beheben möchten, spielen dabei drei Faktoren eine Rolle: IKE, IPsec und Tunnel. 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. Das Ergebnis ist ein Kunden-Gateway mit korrekt konfigurierter IPsec.

```
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. Dies setzt voraus, dass eine ASN aufgeführt ist (z. B. spi: 0x48B456A6), dass der Status ACTIVE ist und dass IPsec korrekt konfiguriert 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 [Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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 Konnektivität von Juniper JunOS-Kunden-Gateway-Geräten

Wenn Sie Konnektivitätsprobleme bei einem Juniper-Kunden-Gateway-Gerät beheben möchten, spielen dabei vier Faktoren eine Rolle: 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. Das Ergebnis ist ein Kunden-Gateway mit korrekt konfigurierter IPsec.

```
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 [Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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              0      0          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    0          7224 I
```

Fehlerbehebung bei der Konnektivität von Juniper ScreenOS-Kunden-Gateway-Geräten

Wenn Sie Konnektivitätsprobleme bei einem Juniper ScreenOS-basierten Kunden-Gateway-Gerät beheben möchten, spielen dabei vier Faktoren eine Rolle: 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 [Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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.

```

s5g5-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.

```

s5g5-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	169.254.255.2	100	Enabled	ESTABLISH	10	00:01:01
7224	169.254.255.5	169.254.255.6	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
```

Fehlerbehebung bei der Konnektivität von Yamaha-Kunden-Gateway-Geräten

Wenn Sie Konnektivitätsprobleme bei einem Yamaha-Kunden-Gateway-Gerät beheben möchten, spielen dabei vier Faktoren eine Rolle: 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 Probleme bei der Herstellung einer Verbindung mit dem Site-to-Site-VPN verursachen. Wenn das auf Ihrem Router nicht konfiguriert `proxy ID` ist, sehen Sie sich bitte die AWS mitgelieferte Beispielkonfigurationsdatei an, damit Yamaha es 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. Lassen Sie die Tunnelnummer weg, um alle Sicherheitszuweisungen (Security Associations, SAs) anzuzeigen.

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. Das Ergebnis ist ein Kunden-Gateway mit korrekt konfigurierter IPsec.

```
# 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 [Konfigurieren einer Firewall zwischen dem Internet und Ihrem 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 Wert `current status online` ist und dass als `Interface type IPsec` ausgewählt ist. 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

Mit Site-to-Site-VPN arbeiten

Sie können mit Site-to-Site-VPN-Ressourcen über die Amazon VPC-Konsole oder die AWS CLI arbeiten.

Inhalt

- [Erstellen Sie einen Site-to-Site-VPN-Anhang für Cloud WAN AWS](#)
- [Einen Transit-Gateway-VPN-Anhang erstellen](#)
- [Eine Site-to-Site VPN-Verbindung testen](#)
- [Eine Site-to-Site VPN-Verbindung löschen](#)
- [Das Ziel-Gateway der -Site-to-Site VPN-Verbindung ändern](#)
- [Die Site-to-Site VPN-Verbindungsoptionen ändern](#)
- [Ändern von -Site-to-Site-VPN-Tunnel-Optionen](#)
- [Die statischen Routen für eine Site-to-Site-VPN-Verbindung bearbeiten](#)
- [Das Kunden-Gateway für eine Site-to-Site-VPN-Verbindung ändern](#)
- [Kompromittierte Anmeldeinformationen für Ihre Site-to-Site VPN-Verbindung ersetzen](#)
- [Zertifikate von Site-to-Site VPN-Tunnelendpunkten rotieren](#)
- [Privates IP-VPN mit AWS Direct Connect](#)

Erstellen Sie einen Site-to-Site-VPN-Anhang für Cloud WAN AWS

Gehen Sie wie folgt vor, um einen Site-to-Site-VPN-Anhang für AWS Cloud WAN zu erstellen.

So erstellen Sie mit 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:

- Zum Verwenden eines vorhandenen Kunden-Gateways wählen Sie Vorhanden und dann das zu verwendende Kunden-Gateway aus.
 - Um ein Kunden-Gateway zu erstellen, wählen Sie New (Neu) aus. Geben Sie für IP address (IP-Adresse) eine statische öffentliche IP-Adresse ein. Wählen Sie für Certificate ARN (Zertifikat-ARN) den ARN Ihres privaten Zertifikats aus (wenn Sie eine zertifikatsbasierte Authentifizierung verwenden). 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. Bei Routing-Optionen wählen Sie Dynamisch oder Statisch aus.
 8. Bei Interne Tunnel-IP-Version wählen Sie IPv4 oder IPv6 aus.
 9. (Optional) Aktivieren Sie bei Enable acceleration (Beschleunigung aktivieren) das Kontrollkästchen. 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.

10. (Optional) Geben Sie auf der Seite des Kunden-Gateways (lokal) bei Local IPv4 network CIDR (CIDR des lokalen IPv4-Netzwerks) den IPv4-CIDR-Bereich an, der über die VPN-Tunnel kommunizieren darf. Der Standardwert ist `0.0.0.0/0`.

Geben Sie für Remote-IPv4-Netzwerk-CIDR den IPv4-CIDR-Bereich auf der AWS Seite an, die über die VPN-Tunnel kommunizieren darf. Der Standardwert ist `0.0.0.0/0`.

Wenn Sie IPv6 für die IP-Version des Tunnels angegeben haben, geben Sie die IPv6-CIDR-Bereiche auf der Kunden-Gateway-Seite und AWS auf der Seite an, die über die VPN-Tunnel kommunizieren dürfen. Die Standardeinstellung für beide Bereiche lautet „`::/0`“.

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 die IPv4-Adressen innerhalb des Tunnels.
 - Wenn Sie IPv6 bei Interne Tunnel-IP-Version angegeben haben, wird ein /126 IPv6 CIDR-Block aus dem `fd00::/8`-Bereich für die IPv6-Adressen innerhalb des Tunnels verwendet.
 - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 und 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.

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

- [CreateVpnVerbindung](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)

Einen Transit-Gateway-VPN-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.

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:
 - Zum Verwenden eines vorhandenen Kunden-Gateways wählen Sie **Vorhanden** und dann das zu verwendende Kunden-Gateway aus.

Wenn sich Ihr Kunden-Gateway hinter einem NAT-Gerät (Network Address Translation) befindet, das für die NAT-Übersetzung (NAT-T) aktiviert ist, verwenden Sie die öffentliche IP-Adresse Ihres NAT-Geräts und ändern Sie Ihre Firewall-Regeln derart, dass die Blockierung des UDP-Ports 4500 aufgehoben wird.

- Um ein Kunden-Gateway zu erstellen, wählen Sie **New (Neu)** aus. Geben Sie für **IP Address (IP-Adresse)** eine statische öffentliche IP-Adresse ein. Wählen Sie für **Certificate ARN (Zertifikat-ARN)** den ARN Ihres privaten Zertifikats aus (wenn Sie eine zertifikatsbasierte Authentifizierung verwenden). 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. Bei Routing-Optionen wählen Sie Dynamisch oder Statisch aus.
8. Geben Sie für Interne Tunnel-IP-Version an, ob die VPN-Tunnel IPv4- oder IPv6-Datenverkehr unterstützen. IPv6-Datenverkehr wird nur für VPN-Verbindungen auf einem Transit-Gateway unterstützt.
9. (Optional) Aktivieren Sie bei Enable acceleration (Beschleunigung aktivieren) das Kontrollkästchen. 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.

10. (Optional) Geben Sie auf der Seite des Kunden-Gateways (lokal) bei Local IPv4 network CIDR (CIDR des lokalen IPv4-Netzwerks) den IPv4-CIDR-Bereich an, der über die VPN-Tunnel kommunizieren darf. Der Standardwert ist `0.0.0.0/0`.

Geben Sie auf der AWS-Seite bei Remote IPv4 network CIDR (CIDR des IPv4-Remote-Netzwerks) den IPv4-CIDR-Bereich an, der über die VPN-Tunnel kommunizieren darf. Der Standardwert ist `0.0.0.0/0`.

Wenn Sie IPv6 als Tunnel inside IP-version (Tunnel in IP-Version) angegeben haben, geben Sie auf der Kunden-Gateway-Seite und auf der AWS-Seite die IPv6-CIDR-Bereiche an, die über die VPN-Tunnel kommunizieren dürfen. Die Standardeinstellung für beide Bereiche lautet „`::/0`“.

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 die IPv4-Adressen innerhalb des Tunnels.
 - Wenn Sie IPv6 bei Interne Tunnel-IP-Version angegeben haben, wird ein /126 IPv6 CIDR-Block aus dem `fd00::/8`-Bereich für die IPv6-Adressen innerhalb des Tunnels verwendet.
 - Den vorinstallierten IKE-Schlüssel (PSK). Die folgenden Versionen werden unterstützt: IKEv1 und 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.

Erstellen einer VPN-Anfügung mithilfe der AWS CLI

Verwenden Sie den Befehl [create-vpn-connection](#) und geben Sie die Transit-Gateway-ID für die Option `--transit-gateway-id` an.

Eine 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 Instance starten und die Verbindung testen, indem Sie die Instance anpingen.

Bevor Sie anfangen, prüfen Sie Folgendes:

- Verwenden Sie ein AMI, das auf Ping-Anfragen reagiert. Wir empfehlen, eines der Amazon Linux-AMIs zu verwenden.
- 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 mit Windows Server verwenden, stellen Sie eine Verbindung mit der Instance her und aktivieren Sie auf der Windows-Firewall eingehende ICMPv4, um die Instance anzupingen.
- (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 Amazon EC2-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 Amazon EC2-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 Amazon EC2 EC2-Benutzerhandbuch. Weitere Informationen

zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter [Connect to your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

Eine Site-to-Site VPN-Verbindung 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 Virtual 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 Verbindung erstellen, müssen Sie eine neue Konfigurationsdatei herunterladen und das Kunden-Gateway-Gerät neu konfigurieren.

Aufgaben

- [Eine VPN-Verbindung löschen](#)
- [Ein Kunden-Gateway löschen](#)
- [Ein Virtual Private Gateway trennen und löschen](#)

Eine VPN-Verbindung löschen

Nachdem Sie die Site-to-Site-VPN-Verbindung gelöscht haben, bleibt sie für kurze Zeit mit dem Status „deleted“ sichtbar, und dann 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

- [DeleteVpnVerbindung](#) (Amazon EC2 Query API)
- [delete-vpn-connection](#) (AWS CLI)
- [Remove-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Ein Kunden-Gateway löschen

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 EC2-Abfrage-API)
- [delete-customer-gateway](#) (AWS CLI)
- [Remove-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Ein Virtual Private Gateway trennen und löschen

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 EC2-Abfrage-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 EC2-Abfrage-API)
- [delete-vpn-gateway](#) (AWS CLI)
- [Remove-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Das Ziel-Gateway der -Site-to-Site VPN-Verbindung ändern

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 für einen kurzen Zeitraum vorübergehend nicht verfügbar, während 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 Gateways 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 das neue Ziel-Gateway ein Transit-Gateway ist, fügen Sie die VPCs 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.

i 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.

So ändern Sie eine Site-to-Site-VPN-Verbindung mit der Befehlszeile oder der API:

- [ModifyVpnConnection](#) (Amazon EC2-Abfrage-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-Gateway.

Schritt 5: Ziel-Gateway-Routing aktualisieren (bedingt)

Wenn das neue Gateway ein Transit-Gateway ist, ändern Sie die Routing-Tabelle des Transit-Gateways, um den Datenverkehr zwischen der VPC und dem Site-to-Site-VPN zu ermöglichen. 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 [Routing-Tabellen und 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 [Optionen für das Kunden-Gateway für Ihre Site-to-Site-VPN-Verbindung](#).

Die 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 auf 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“.
- Die IPv6 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“.

Wenn Sie die VPN-Verbindungsoptionen ändern, ändern sich weder die VPN-Endpunkt-IP-Adressen auf der AWS-Seite noch die Tunneloptionen. 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 Save Changes.

So ändern Sie die VPN-Verbindungsoptionen über die Befehlszeile oder API

- [modify-vpn-connection-options](#) (AWS CLI)
- [ModifyVpnConnectionOptions](#) (Amazon EC2-Abfrage-API)

Ändern von -Site-to-Site-VPN-Tunnel-Optionen

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 anschließend Aktionen, VPN-Tunnel-Optionen 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 finden Sie unter [VPN-Tunneloptionen](#).
6. Wählen Sie Save Changes.

So ändern Sie die VPN-Tunneloptionen über die Befehlszeile oder API

- (AWS CLI) Verwenden Sie [describe-vpn-connections](#), um die aktuellen Tunneloptionen anzuzeigen, und [modify-vpn-tunnel-options](#), um die Tunneloptionen zu ändern.
- (Amazon EC2-Abfrage-API) Verwenden Sie [DescribeVPNConnections](#), um die aktuellen Tunneloptionen anzuzeigen, und [ModifyVPNTunnelOptions](#), um die Tunneloptionen zu ändern.

Die statischen Routen für eine Site-to-Site-VPN-Verbindung bearbeiten

Bei einer Site-to-Site-VPN-Verbindung auf einem Virtual Private Gateway, das für statisches Routing konfiguriert ist, können Sie statische Routen in Ihrer VPN-Konfiguration hinzufügen oder 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 aus.
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 EC2-Abfrage-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 EC2-Abfrage-API)
- [delete-vpn-connection-route](#) (AWS CLI)
- [Remove-EC2VpnConnectionRoute](#) (AWS Tools for Windows PowerShell)

Das Kunden-Gateway für eine Site-to-Site-VPN-Verbindung ändern

Sie können das Kunden-Gateway Ihrer Site-to-Site-VPN-Verbindung mithilfe der Amazon VPC-Konsole oder eines Befehlszeilen-Tools 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 Save Changes.

So ändern Sie das Kunden-Gateway über die Befehlszeile oder API

- [ModifyVpnConnection](#) (Amazon EC2-Abfrage-API)
- [modify-vpn-connection](#) (AWS CLI)

Kompromittierte Anmeldeinformationen für Ihre Site-to-Site VPN-Verbindung ersetzen

Wenn Sie glauben, dass die Tunnelanmeldeinformationen für Ihre Site-to-Site VPN-Verbindung gefährdet sind, können Sie den vorinstallierten IKE-Schlüssel ändern 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 [Optionen für die Site-to-Site-Tunnel-Authentifizierung](#).

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 [Ändern von -Site-to-Site-VPN-Tunnel-Optionen](#).

Alternativ können Sie die VPN-Verbindung löschen. Weitere Informationen finden Sie unter [Eine VPN-Verbindung löschen](#). Sie müssen die VPC oder das Virtual Private Gateway nicht löschen. Erstellen Sie mit demselben Virtual Private Gateway eine neue VPN-Verbindung und konfigurieren Sie die neuen Schlüssel auf Ihrem Kunden-Gateway. Geben Sie eigene vorinstallierte Schlüssel für die Tunnel an oder lassen Sie AWS neue vorinstallierte Schlüssel für Sie generieren. 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.

So ändern Sie das Zertifikat für die AWS-Seite des Tunnelendpunkts

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.

Zertifikate von Site-to-Site VPN-Tunnelendpunkten rotieren

Sie können die Zertifikate auf den Tunnelendpunkten auf der AWS-Seite mithilfe der Amazon VPC-Konsole rotieren. Wenn das Zertifikat eines Tunnelendpunkts kurz vor Ablauf der Gültigkeitsdauer steht, rotiert AWS das Zertifikat mithilfe der servicegebundenen Rolle automatisch. Weitere Informationen finden Sie unter [the section called "Service-verknüpfte Rollen"](#).

So rotieren Sie das Site-to-Site VPN-Tunnelendpunkt-Zertifikat 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 die Site-to-Site VPN-Verbindung und dann Aktionen, VPN-Tunnelzertifikate ändern aus.
4. Wählen Sie den Tunnelendpunkt aus.
5. Wählen Sie Save (Speichern).

So rotieren Sie das Site-to-Site VPN-Tunnelendpunkt-Zertifikat mit der AWS CLI

Verwenden Sie den Befehl [modify-vpn-tunnel-certificate](#).

Privates IP-VPN mit AWS Direct Connect

Mit einem privaten IP-VPN können Sie IPSec-VPN über bereitstellen und so den Datenverkehr zwischen Ihrem lokalen Netzwerk verschlüsseln AWS Direct Connect 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.

Inhalt

- [Vorteile von privatem IP-VPN](#)
- [Funktionsweise von privatem IP-VPN](#)
- [Voraussetzungen](#)
- [Das Kunden-Gateway erstellen](#)
- [Das Transit Gateway vorbereiten](#)
- [Erstellen Sie das Gateway AWS Direct Connect](#)
- [Die Zuordnung für das Transit Gateway erstellen](#)
- [Die VPN-Verbindung erstellen](#)

Vorteile von privatem IP-VPN

- Vereinfachtes Netzwerkmanagement und -betrieb: Ohne privates IP-VPN müssen Kunden VPNs und Router von Drittanbietern einsetzen, um private VPNs über 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.
- Verbesserte Sicherheitslage: 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 Verwendung öffentlicher IPs erhöht die Wahrscheinlichkeit externer (DOS-)Angriffe, wodurch wiederum die Kunden gezwungen sind, zusätzliche Sicherheitsausrüstung für den Netzwerkschutz einzusetzen. Außerdem 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 AWS Direct Connect Transit-VIFs (anstelle von öffentlichen VIFs) in Verbindung mit der Möglichkeit, private IPs zu konfigurieren. 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) als AWS Direct Connect reine Verbindungen, bei denen derzeit eine Obergrenze von 200 ausgehenden und 100 eingehenden Routen gilt.

Funktionsweise von privatem IP-VPN

Private IP Site-to-Site VPN funktioniert über eine virtuelle AWS Direct Connect Transitschnittstelle (VIF). Es nutzt ein AWS Direct Connect -Gateway und ein Transit Gateway zum Verbinden Ihrer On-Premises-Netzwerke mit 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-Gerät der IPsec-Tunnel private IP-Adressen zuweisen. Sie können private IP-Adressen aus den privaten IPv4-Adressbereichen RFC1918 oder RFC6598 verwenden.

Sie hängen eine private IP-VPN-Verbindung an ein Transit Gateway an. Anschließend leiten Sie den Datenverkehr zwischen dem VPN-Anhang und allen VPCs (oder anderen Netzwerken) weiter, die ebenfalls an das Transit Gateway angehängt sind. Dazu ordnen Sie dem VPN-Anhang eine Routing-Tabelle zu. In umgekehrter Richtung können Sie den Datenverkehr von Ihren VPCs an den privaten IP-VPN-Anhang weiterleiten, indem Sie den VPCs zugeordnete Routing-Tabellen verwenden.

Die Routing-Tabelle, die der VPN-Anlage zugeordnet ist, kann dieselbe oder eine andere sein als die, die der zugrunde liegenden Anlage zugeordnet ist. AWS Direct Connect Auf diese Weise können Sie verschlüsselten und unverschlüsselten Datenverkehr gleichzeitig zwischen Ihren VPCs und Ihren On-Premises-Netzwerken weiterleiten.

Weitere Informationen zum Datenverkehrspfad, der das VPN verlässt, finden Sie unter [Routing-Richtlinien für private virtuelle Schnittstellen und virtuelle AWS Direct Connect Transitschnittstellen](#) im Benutzerhandbuch.

Voraussetzungen

Die folgenden Ressourcen werden benötigt, um die Einrichtung eines privaten IP-VPN über AWS Direct Connect abzuschließen:

- Eine AWS Direct Connect Verbindung zwischen Ihrem lokalen Netzwerk und AWS
- Ein AWS Direct Connect Gateway, das mit dem entsprechenden Transit-Gateway verknüpft ist
- Ein Transit Gateway mit einem verfügbaren privaten IP-CIDR-Block
- Ein Kunden-Gateway-Gerät in Ihrem On-Premises-Netzwerk und ein entsprechendes AWS - Kunden-Gateway

Das Kunden-Gateway erstellen

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.
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.

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

- [CreateCustomerGateway](#) (Amazon EC2 EC2-Abfrage-API)
- [create-customer-gateway](#) (AWS CLI)

Das Transit Gateway vorbereiten

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-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.

Note

Wenn Sie den CIDR-Block des Transit Gateways angeben, der mit Ihrem privaten IP-VPN verknüpft werden soll, stellen Sie sicher, dass sich der CIDR-Block nicht mit IP-Adressen für andere Netzwerkanhänge auf dem Transit Gateway überschneidet. Wenn sich IP-CIDR-Blöcke überschneiden, kann dies zu Problemen bei der Konfiguration Ihres Kunden-Gateway-Geräts führen.

Spezifische AWS Konsolenschritte zum Erstellen oder Ändern eines Transit-Gateways zur Verwendung für das private IP-VPN finden Sie unter [Transit-Gateways](#) im Amazon VPC Transit Gateways Guide.

Erstellen eines Transit Gateways über die Befehlszeile oder die API

- [CreateTransitGateway](#) (Amazon EC2 EC2-Abfrage-API)
- [create-transit-gateway](#) (AWS CLI)

Erstellen Sie das Gateway AWS Direct Connect

Erstellen Sie ein AWS Direct Connect Gateway, indem Sie den Anweisungen [zum Erstellen eines Direct Connect-Gateways](#) im AWS Direct Connect Benutzerhandbuch folgen.

Um ein AWS Direct Connect Gateway über die Befehlszeile oder API zu erstellen

- [CreateDirectConnectGateway](#)(API AWS Direct Connect abfragen)
- [create-direct-connect-gateway](#) (AWS CLI)

Die Zuordnung für das Transit Gateway erstellen

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.

Weitere Informationen finden Sie unter [Transit-Gateway-Zuordnungen](#) im Benutzerhandbuch zu AWS Direct Connect .

Um eine AWS Direct Connect Gateway-Zuordnung mithilfe der Befehlszeile oder API zu erstellen

- [CreateDirectConnectGatewayAssoziation](#) (AWS Direct Connect Abfrage-API)
- [create-direct-connect-gateway-association](#) (AWS CLI)

Die VPN-Verbindung erstellen


So erstellen Sie eine VPN-Verbindung mit privaten IP-Adressen

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 unter Namens-Tag 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.
5. 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.
6. Wählen Sie für Customer gateway (Kunden-Gateway) die Option Existing (Vorhanden) aus. Wählen Sie dann das zuvor identifizierte Kunden-Gateway aus.
7. 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.
8. Geben Sie für Interne Tunnel-IP-Version an, ob die VPN-Tunnel IPv4- oder IPv6-Datenverkehr unterstützen.
 9. (Optional) Wenn Sie IPv4 für Tunnel inside IP Version 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 IPv6 für die Tunnel-Inside-IP-Version 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 die Option 4. Privatelpv
11. Wählen Sie unter Transport Attachment ID den Transit-Gateway-Anhang für das entsprechende AWS Direct Connect Gateway aus.
12. 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.

Sicherheit bei AWS Site-to-Site VPN

Cloud-Sicherheit 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](#). Informationen zu den Compliance-Programmen, die für AWS Site-to-Site VPN gelten, finden Sie unter [AWS Services in Scope by Compliance Program Compliance Program](#).
- 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 geteilten Verantwortung bei der Verwendung von Site-to-Site VPN einsetzen können. Die folgenden Themen veranschaulichen, wie Sie Site-to-Site VPN konfigurieren können, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Site-to-Site-VPN-Ressourcen überwachen und sichern können.

Inhalt

- [Datenschutz bei AWS Site-to-Site VPN](#)
- [Identitäts- und Zugriffsmanagement für AWS Site-to-Site VPN](#)
- [Resilienz in AWS Site-to-Site VPN](#)
- [Infrastruktursicherheit in AWS Site-to-Site VPN](#)

Datenschutz bei AWS Site-to-Site VPN

Das [Modell der AWS gemeinsamen 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).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- 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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

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 die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS 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 Ihren VPC privat mit Ihrem On-Premise-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 IPsec-VPN-Verbindungen (Internet Protocol Security). 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 Datenverkehr in den einzelnen Tunneln kann mit AES128 oder AES256 verschlüsselt werden und Diffie-Hellman-Gruppen für den Schlüsselaustausch verwenden, was eine perfekte Forward-Secrecy gewährleistet. AWS authentifiziert über SHA1- oder SHA2-Hashing-Funktionen.

Instances in Ihrer VPC benötigen keine öffentliche IP-Adresse, um sich mit Ressourcen auf der anderen Seite Ihrer Site-to-Site-VPN-Verbindung zu verbinden. Instances können ihren Internet-Datenverkehr über die Site-to-Site-VPN-Verbindung zu Ihrem On-Premise-Netzwerk leiten. Sie können dann über Ihre bestehenden ausgehenden Datenverkehrspunkte und Ihre Netzwerksicherheits- und Überwachungsgeräte auf das Internet zugreifen.

Weitere Informationen finden Sie im folgenden Thema:

- [Tunnel-Optionen für Ihre Site-to-Site-VPN-Verbindung](#): Enthält Informationen über die IPsec- und IKE-Optionen (Internet Key Exchange), die für jeden Tunnel verfügbar sind.
- [Optionen für die Site-to-Site-Tunnel-Authentifizierung](#): Enthält Informationen zu den Authentifizierungsoptionen für Ihre VPN-Tunnelendpunkte.
- [Anforderungen für Ihr Kunden-Gateway-Gerät](#): Enthält Informationen über die Anforderungen an das Kunden-Gateway-Gerät auf Ihrer Seite der VPN-Verbindung.
- [Ermöglichen einer sicheren Kommunikation zwischen Standorten über VPN CloudHub](#): Wenn Sie über mehrere Site-to-Site-VPN-Verbindungen verfügen, können Sie mithilfe des VPN eine sichere Kommunikation zwischen Ihren lokalen Standorten bereitstellen. AWS CloudHub

Identitäts- und Zugriffsmanagement für AWS Site-to-Site VPN

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren steuern, wer für die Nutzung von Site-to-Site-VPN-Ressourcen authentifiziert (angemeldet) und autorisiert (mit Berechtigungen ausgestattet) werden kann. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert AWS Site-to-Site VPN mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#)
- [Fehlerbehebung bei AWS Site-to-Site-VPN-Identität und -Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für Site-to-Site VPN](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie mit Site-to-Site VPN ausführen.

Service-Benutzer – Wenn Sie den Site-to-Site-VPN-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die benötigten Anmeldeinformationen und Berechtigungen bereit. Wenn Sie für Ihre Arbeit weitere 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. Beachten Sie die Informationen unter [Fehlerbehebung bei AWS Site-to-Site-VPN-Identität und -Zugriff](#), falls Sie keinen Zugriff auf eine Funktion in Site-to-Site VPN haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für Site-to-Site-VPN-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Site-to-Site VPN. Es ist Ihre Aufgabe, zu bestimmen, auf welche Site-to-Site-VPN-Funktionen und -Ressourcen Ihre Servicebenutzer Zugriff erhalten sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Site-to-Site VPN verwenden kann, finden Sie unter [So funktioniert AWS Site-to-Site VPN mit IAM](#).

IAM-Administrator – Wenn Sie IAM-Administrator sind, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Site-to-Site VPN verfassen können. Beispiele für identitätsbasierte Site-to-Site-VPN-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#).

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 Zugangportal 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, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. 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 [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, 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 und verwenden Sie diese, 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [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 [Verwenden von IAM-Rollen](#) 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](#) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch](#).
- **Serviceübergreifender Zugriff** — Einige verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. 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.
- **Anwendungen, die auf Amazon EC2 ausgeführt werden** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

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. Berechtigungen in den Richtlinien bestimmen, ob die 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 [Erstellen von IAM-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 eingebundenen Richtlinie wählen, finden Sie unter [Auswahl 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.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

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.
- **Service Control Policies (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 innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) 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](#).

So funktioniert AWS Site-to-Site VPN mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Site-to-Site VPN verwenden, erfahren Sie hier, welche IAM-Funktionen Sie mit Site-to-Site VPN verwenden können.

IAM-Funktionen, die Sie mit AWS Site-to-Site VPN verwenden können

IAM-Feature	Site-to-Site-VPN-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	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 Site-to-Site VPN

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 [Erstellen von IAM-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 Site-to-Site VPN

Beispiele für identitätsbasierte Richtlinien für Site-to-Site VPN finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#).

Ressourcenbasierte Richtlinien innerhalb von Site-to-Site VPN

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 Prinzipalentsität (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 [Kontenübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für Site-to-Site VPN

Unterstützt Richtlinienaktionen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 Service Authorization Reference](#).

Richtlinienaktionen in Site-to-Site VPN verwenden das folgende Präfix vor der Aktion:

```
ec2
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"  
]
```

Beispiele für identitätsbasierte Richtlinien für Site-to-Site VPN finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#).

Richtlinienressourcen für Site-to-Site VPN

Unterstützt Richtlinienressourcen	Ja
-----------------------------------	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen 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 finden Sie unter [Von AWS Site-to-Site VPN definierte Ressourcen](#) in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter [Von AWS Site-to-Site VPN definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien für Site-to-Site VPN finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#).

Richtlinienbedingungsschlüssel für Site-to-Site VPN

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 Richtlinien für Site-to-Site VPN finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Site-to-Site VPN](#).

ACLs in Site-to-Site VPN

Unterstützt ACLs	Nein
------------------	------

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Site-to-Site VPN

Unterstützt ABAC (Tags in Richtlinien)	Nein
--	------

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS 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 Bedingungelement 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 [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwenden von temporären Anmeldeinformationen mit Site-to-Site VPN

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 zu einer 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 Site-to-Site VPN

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 Site-to-Site VPN

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

Wenn die Berechtigungen für eine Servicerolle geändert werden, könnte dies die Site-to-Site-VPN-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Site-to-Site VPN dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Site-to-Site VPN

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer Service-Verknüpfung verbunden 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 AWS Site-to-Site VPN

Standardmäßig besitzen Benutzer und Rollen keine Berechtigungen zum Erstellen oder Ändern von Site-to-Site-VPN-Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder API ausführen. AWS 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](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Site-to-Site VPN definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, 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 Site-to-Site-VPN-Konsole](#)
- [Beschreiben Sie spezifische Site-to-Site-VPN-Verbindungen](#)
- [Erstellen und beschreiben Sie die für eine Verbindung benötigten Ressourcen AWS Site-to-Site VPN](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Site-to-Site-VPN-Ressourcen in Ihrem Konto erstellen, löschen oder darauf zugreifen kann. Dies kann zusätzliche Kosten für Ihr AWS-Konto verursachen. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. AWS ist in Ihrem Konto verfügbar. 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 [Richtlinienvvalidierung zum 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 [Konfigurieren eines MFA-geschützten API-Zugriffs](#) 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 Site-to-Site-VPN-Konsole

Um auf die AWS Site-to-Site VPN 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 anzuzeigen. 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 API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS 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 AmazonVPCReadOnlyAccess AWS die 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": [
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
      ]
    }
  ]
}
```

Erstellen und beschreiben Sie die für eine Verbindung benötigten Ressourcen AWS Site-to-Site VPN

```
{
  "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 -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Site-to-Site VPN und IAM auftreten könnten.

Themen

- [Ich bin nicht autorisiert, eine Aktion in Site-to-Site VPN auszuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Site-to-Site VPN VPN-Ressourcen ermöglichen](#)

Ich bin nicht autorisiert, eine Aktion in Site-to-Site VPN auszuführen

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 Administrator. AWS Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien so aktualisiert werden, dass 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 namens `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 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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Site-to-Site VPN diese Funktionen unterstützt, finden Sie unter [So 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 im IAM-Benutzerhandbuch unter [Kontenübergreifender Ressourcenzugriff in IAM](#).

Verwenden von serviceverknüpften Rollen für Site-to-Site VPN

AWS [Site-to-Site VPN verwendet dienstverknüpfte Rollen AWS Identity and Access Management \(IAM\)](#). Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, die direkt mit Site-to-Site VPN verknüpft ist. 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 serviceverknüpfte Rolle vereinfacht das Einrichten von Site-to-Site VPN, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Site-to-Site VPN definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Site-to-Site VPN die 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 nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rollen angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Site-to-Site VPN

Site-to-Site VPN verwendet die dienstverknüpfte Rolle mit dem Namen `AWSServiceRoleForVPC2S2VPN`— Erlaube Site-to-Site VPN, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

Die `AWSServiceRoleForVPC2S2VPN` dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- AWS Certificate Manager
- AWS Private Certificate Authority

Die genannte Rollenberechtigungsrichtlinie `AWSVPC2S2VpnServiceRolePolicy` ermöglicht es Site-to-Site VPN, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `acm:ExportCertificate` für Resource: `"*"`
- Aktion: `acm:DescribeCertificate` für Resource: `"*"`
- Aktion: `acm:ListCertificates` für Resource: `"*"`
- Aktion: `acm-pca:DescribeCertificateAuthority` für Resource: `"*"`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Site-to-Site VPN

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 serviceverknüpfte 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 serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Site-to-Site VPN

Mit Site-to-Site VPN können Sie die dienstverknüpfte Rolle nicht bearbeiten.

`AWSServiceRoleForVPCS2SVPN` Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename 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 serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Site-to-Site VPN

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-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Site-to-Site-VPN-Ressourcen zu löschen, die von der `AWSServiceRoleForVPCS2SVPN`

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 Berechtigung für den Zugriff auf Ihre ACM-Zertifikate entfernen können, die von Site-to-Site VPN-Verbindungen verwendet werden.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die serviceverknüpfte Rolle zu löschen. `AWSServiceRoleForVPCS2SVPN` 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 Datenstabilität 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 Ihrer VPC erhöhte Verfügbarkeit zu bieten. Wenn 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 [Ersatz für Site-to-Site VPN-Tunnelendpunkte](#). Konfigurieren Sie beim Konfigurieren Ihres Kunden-Gateways daher unbedingt beide Tunnel.

Redundanz

Um sich vor Verlust der Konnektivität zu schützen, wenn Ihr Kunden-Gateway nicht verfügbar ist, können Sie eine zweite Site-to-Site VPN-Verbindung aufbauen. Weitere Informationen finden Sie in der folgenden -Dokumentation:

- [Verwenden redundanter Site-to-Site-VPN-Verbindungen zur Bereitstellung von Failover](#)
- [Amazon Virtual Private Cloud Connectivity Options](#)
- [Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS](#)

Infrastruktursicherheit in AWS Site-to-Site VPN

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 Ihrer 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 jedoch mit der Überwachung Ihrer Site-to-Site-VPN-Verbindung beginnen, sollten Sie einen Überwachungsplan mit Antworten auf die folgenden Fragen erstellen:

- 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

Inhalt

- [Überwachungstools](#)
- [AWS Site-to-Site VPN Logs](#)
- [Überwachung von VPN-Tunneln mit Amazon CloudWatch](#)
- [Überwachung von VPN-Verbindungen mithilfe von AWS Health Ereignissen](#)

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 Tools zur Überwachung von Site-to-Site-VPN-Verbindungen verwenden und möglicherweise auftretende Probleme melden:

- 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 [Überwachung von VPN-Tunneln 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 mithilfe AWS CloudTrail](#) der Amazon EC2 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 für die Konfiguration bewährter Verfahren oder bei Annäherung an Skalierungsgrenzen. 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 [Überwachung von VPN-Verbindungen mithilfe von AWS Health Ereignissen](#).

Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung einer Site-to-Site-VPN-Verbindung besteht darin, die Elemente manuell zu überwachen, die von den CloudWatch Alarmen nicht abgedeckt werden. 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-Verbindung
 - VPN-Tunnel-Status (Klicken Sie im Navigationsbereich auf Site-to-Site VPN Connections (Site-to-Site-VPN-Verbindungen), wählen Sie eine Site-to-Site-VPN-Verbindung aus und klicken Sie auf Tunnel Details (Tunnel-Details)).
- Auf der CloudWatch Startseite wird Folgendes angezeigt:
 - Aktuelle Alarmer 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 erhalten Sie Zugriff auf Site-to-Site-VPN-Verbindungsprotokolle mit Details zur Einrichtung von IP-Sicherheitstunneln (IPSec), Internet Key Exchange (IKE)-Aushandlungen und Dead Peer Detection (DPD)-Protokollmeldungen.

Site-to-Site-VPN-Protokolle können in Amazon Logs veröffentlicht werden. CloudWatch Diese Funktion bietet Kunden eine einheitliche Möglichkeit, auf detaillierte Protokolle für alle ihre Site-to-Site-VPN-Verbindungen zuzugreifen und diese zu analysieren.

Inhalt

- [Vorteile von Site-to-Site-VPN-Protokollen](#)
- [Größenbeschränkungen der Amazon CloudWatch Logs-Ressourcenrichtlinie](#)
- [Inhalte von Site-to-Site-VPN-Protokollen](#)
- [IAM-Anforderungen für die Veröffentlichung in Logs CloudWatch](#)
- [Konfiguration von Site-to-Site-VPN-Protokollen anzeigen](#)
- [Site-to-Site-VPN-Protokolle aktivieren](#)
- [Site-to-Site-VPN-Protokolle deaktivieren](#)

Vorteile von Site-to-Site-VPN-Protokollen

- Vereinfachte VPN-Fehlerbehebung: Site-to-Site-VPN-Protokolle helfen Ihnen dabei, Konfigurationsunterschiede zwischen AWS und Ihrem Kunden-Gateway-Gerät zu ermitteln und anfängliche VPN-Verbindungsprobleme zu 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 Verbindungsarten von Site-to-Site VPN bereitstellen: virtuelles Gateway, Transit Gateway und CloudHub sowohl Internet als auch als Transport. AWS Direct Connect Diese Funktion bietet Kunden eine einheitliche Möglichkeit,

auf detaillierte Protokolle für alle ihre Site-to-Site-VPN-Verbindungen zuzugreifen und diese zu analysieren.

- **Sicherheit und Compliance:** Site-to-Site-VPN-Protokolle können an Amazon Logs gesendet werden, um den Status und die CloudWatch 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/`

Inhalte von Site-to-Site-VPN-Protokollen

Die folgenden Informationen sind im Site-to-Site-VPN-Tunnelaktivitätsprotokoll enthalten.

Feld	Beschreibung
VpnLogCreationTimestamp	Zeitstempel für die Protokollerstellung in vom Menschen lesbarem Format.
VpnConnectionID	Die Kennung der VPN-Verbindung.
TunnelOutsideIP-Adresse	Die externe IP des VPN-Tunnels, der den Protokolleintrag generiert hat.
TunnelDPDEnabled	Status Dead-Peer-Detection-Protokoll aktiviert (Wahr/Falsch).
Tunnel CGWNATT DetectionStatus	NAT-T auf dem Kunden-Gateway-Gerät erkannt (Wahr/Falsch).

Feld	Beschreibung
TunnelIKEPhase1State	IKE-Phase-1-Protokollstatus (Established (Eingerichtet) Rekeying (Erneute Schlüssel erstellung) Negotiating (Aushandlung) Down (Ausgefallen)).
TunnelIKEPhase2State	IKE-Phase-2-Protokollstatus (Established (Eingerichtet) Rekeying (Erneute Schlüssel erstellung) Negotiating (Aushandlung) Down (Ausgefallen)).
VpnLogEinzelheiten	Ausführliche Meldungen für IPSec-, IKE- und DPD-Protokolle.

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-Endpunkt nicht unterstützt. z. B. 3DES

Fehlermeldung	Erklärung
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
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 hat nach erneuten Übertragungen von {retry_count} eine Zeitüberschreitung erlitten	Peer hat nicht auf DPD-Nachrichten geantwortet 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/IKE_SA gesendet
AWS Der Tunnel hat DELETE für Phase 2 SA mit SPI: xxxx erhalten	Peer hat die Delete_SA-Nachricht für CHILD_SA gesendet
AWS Der Tunnel hat eine Kollision (CHILD_REKEY) 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 redundante SAs generiert werden, schließen Peers aufgrund von Kollisionen redundante SA, nachdem sie die Nonce-Werte gemäß RFC abgeglichen haben

Fehlermeldung	Erklärung
AWS Der Tunnel von Phase 2 konnte nicht eingerichtet werden, während Phase 1 beibehalten wurde	Peer konnte CHILD_SA aufgrund eines Verhandlungsfehlers, z. B. eines falschen Vorschlags, nicht einrichten.
AWS: Traffic Selector: TS_INACLECT: vom Responder empfangen	Peer hat falsche Traffic Selectors/Encryption Domain vorgeschlagen. Peers sollten mit identischen und korrekten CIDRs konfiguriert werden.
AWS Der Tunnel sendet AUTHENTICATION_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 (Verschlüsselung, Hashing und DH-Gruppe) werden von AWS VPN Endpoint nicht unterstützt, z. B. 3DES

IKEv2-Verhandlungsnachrichten

Fehlermeldung	Erklärung
AWS Die Anfrage (id=xxx) für CREATE_CHILD_SA wurde vom Tunnel verarbeitet	AWS hat die CREATE_CHILD_SA-Anfrage von CGW erhalten

Fehlermeldung	Erklärung
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-Anfrage an CGW
AWS Die Antwort (id=xxx) für CREATE_CHILD_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 von Site-to-Site-VPN-Protokollen anzeigen

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 Connections (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 einsehen.

So zeigen Sie die aktuellen Tunnelprotokollierungseinstellungen für eine Site-to-Site-VPN-Verbindung über die AWS Befehlszeile oder API an

- [DescribeVpnVerbindungen](#) (Amazon EC2 Query API)
- [describe-vpn-connections](#) (AWS CLI)

Site-to-Site-VPN-Protokolle aktivieren

Note

Wenn Sie Site-to-Site-VPN-Protokolle für einen vorhandenen VPN-Verbindungstunnel aktivieren, kann Ihre Verbindung 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 [Ersatz für Site-to-Site VPN-Tunnelendpunkte](#).

So aktivieren Sie die VPN-Protokollierung beim Erstellen einer neuen Site-to-Site-VPN-Verbindung

Folgen Sie dem Verfahren unter [Schritt 5: Eine VPN-Verbindung erstellen](#). In Schritt 9, Tunnel Options (Tunneleoptionen), 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 [Tunnel-Optionen für Ihre Site-to-Site-VPN-Verbindung](#).

So aktivieren Sie die Tunnelprotokollierung für eine neue Site-to-Site-VPN-Verbindung über die AWS Befehlszeile oder API

- [CreateVpnVerbindung](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)

So aktivieren Sie die Tunnelprotokollierung für eine vorhandene Site-to-Site-VPN-Verbindung

1. Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Connections (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-Tunneleoptionen 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.

So aktivieren Sie die Tunnelprotokollierung für eine bestehende Site-to-Site-VPN-Verbindung mithilfe der AWS Befehlszeile oder API

- [ModifyVpnTunnelOptions](#)(Amazon EC2 EC2-Abfrage-API)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Site-to-Site-VPN-Protokolle deaktivieren

So deaktivieren Sie die Tunnelprotokollierung für eine Site-to-Site-VPN-Verbindung

1. Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Connections (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. 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.

So deaktivieren Sie die Tunnelprotokollierung für eine Site-to-Site-VPN-Verbindung mithilfe der AWS Befehlszeile oder API

- [ModifyVpnTunnelOptions](#)(Amazon EC2 EC2-Abfrage-API)

- [modify-vpn-tunnel-options](#) (AWS CLI)

Überwachung von VPN-Tunneln mit Amazon CloudWatch

Sie können VPN-Tunnel mithilfe CloudWatch von VPN-Tunneln überwachen. Dabei werden Rohdaten aus dem VPN-Dienst gesammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufgezeichnet, damit Sie auf Verlaufsdaten zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. VPN-Metriken werden automatisch an Sie gesendet, CloudWatch sobald sie verfügbar sind.

Weitere Informationen finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Inhalt

- [VPN-Metriken und Dimensionen](#)
- [CloudWatch VPN-Metriken anzeigen](#)
- [CloudWatch Alarme zur Überwachung von VPN-Tunneln erstellen](#)

VPN-Metriken und Dimensionen

Die folgenden CloudWatch Messwerte sind für Ihre Site-to-Site-VPN-Verbindungen verfügbar.

Metrik	Beschreibung
TunnelState	<p>Der Status des Tunnels. Für statische VPNs gibt der Wert 0 DOWN an, während 1 UP bedeutet. Für BGP-VPNs gibt der Wert 1 ESTABLISHED an, während 0 für alle anderen Zustände verwendet wird. Für beide Arten von VPNs geben Werte zwischen 0 und 1 an, dass mindestens ein Tunnel nicht UP ist.</p> <p>Einheiten: Bruchwert zwischen 0 und 1</p>
TunnelDataIn †	Die Byte, die auf der AWS Seite der Verbindung durch den VPN-Tunnel von einem Kunden-

Metrik	Beschreibung
	<p>Gateway empfangen wurden. Jeder Metrikdatenpunkt stellt die Anzahl der nach dem vorangegangenen Datenpunkt empfangenen Byte dar. Verwenden Sie die Summenstatistik, um die Gesamtanzahl der während des Zeitraums empfangenen Byte anzuzeigen.</p> <p>Diese Metrik zählt die Daten nach deren Entschlüsselung.</p> <p>Einheiten: Byte</p>
TunnelDataOut †	<p>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.</p> <p>Diese Metrik zählt die Daten vor deren Verschlüsselung.</p> <p>Einheiten: Byte</p>

† Diese Metriken können die Netzerklastung 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.

Dimension	Beschreibung
TunnelIpAddress	Filtert die Metrikdaten nach der IP-Adresse des Tunnels für das virtuelle private Gateway.

CloudWatch VPN-Metriken anzeigen

Wenn Sie eine Site-to-Site-VPN-Verbindung herstellen, sendet der VPN-Dienst Metriken über Ihre VPN-Verbindung an CloudWatch, sobald diese verfügbar sind. Sie können -Metriken für Ihre VPN-Verbindungen wie folgt anzeigen.

So zeigen Sie Messwerte mithilfe der Konsole an CloudWatch

Metriken werden zunächst nach dem Service-Namespaces 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 zur Ansicht der Metriken die Metrikdimension aus (z. B. VPN-Tunnel-Metriken).

Note

Der VPN-Namespaces 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"
```

CloudWatch Alarme zur Überwachung von VPN-Tunneln erstellen

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 aus.
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 aus.
11. Geben Sie einen Namen für den Alarm ein. Wählen Sie Weiter aus.
12. Überprüfen Sie die Einstellungen für Ihren Alarm, und wählen Sie dann Create alarm (Alarm erstellen) aus.

Sie können einen Alarm zur Überwachung des Site-to-Site-VPN-Verbindungsstatus erstellen. 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.

So erstellen Sie einen Alarm für den Site-to-Site-VPN-Verbindungsstatus:

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 Metrik aus. TunnelState Wählen Sie Select metric (Ausgewählte Metrik) aus.
6. Geben Sie bei Statistic (Statistik) Maximum an.

Wenn Sie die Site-to-Site-VPN-Verbindung so konfiguriert haben, dass beide Tunnel aktiv sind, können Sie 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 (\leq) aus. Geben Sie 0 ein (oder 0.5, falls mindestens ein Tunnel ausgefallen ist). Wählen Sie Weiter aus.
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 aus.
9. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter aus.
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/](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 TunnelData In-Metrik 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) (\geq) aus, und geben Sie 5000000 ein. Wählen Sie Weiter aus.
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 aus.
10. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter aus.
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 Out-Metrik TunnelDataaus. 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) (\leq) aus, und geben Sie 1000000 ein. Wählen Sie Weiter aus.
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 aus.
10. Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter aus.
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.

Überwachung von VPN-Verbindungen mithilfe von AWS Health Ereignissen

AWS Site-to-Site VPN sendet automatisch Benachrichtigungen an das AWS [AWS Health Dashboard](#)(PHD), das von der AWS Health API unterstützt wird. Dieses Dashboard erfordert keine Einrichtung und ist für authentifizierte AWS Benutzer sofort einsatzbereit. Sie können mehrere Aktionen als Reaktion auf Ereignisbenachrichtigungen über das konfigurieren 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 [Ersatz für Site-to-Site VPN-Tunnelendpunkte](#).

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.

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 Virtual Private Gateway	10	Ja
Beschleunigte Site-to-Site-VPN-Verbindungen pro Region	10	Ja
Nicht zugewiesene Site-to-Site-VPN-Verbindungen pro Region	10	Ja

Note

Sowohl zugewiesene als auch nicht zugewiesene Verbindungen werden auf die Gesamtzahl der Site-to-Site-VPN-Verbindungen pro Region angerechnet.

Sie können jeweils ein Virtual Private Gateway an eine VPC anfügen. Wenn Sie eine Site-to-Site VPN-Verbindung mit mehreren VPCs verbinden möchten, 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 Gesamtbegrenzung für Transit-Gateway-Anhänge. 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 einer Site-to-Site-VPN-Verbindung auf einem Virtual Private Gateway angekündigt werden	100	Nein
Routen, die einem Kunden-Gateway-Gerät von einer Site-to-Site-VPN-Verbindung auf einem Virtual Private Gateway angekündigt werden	1.000	Nein
Dynamische Routen, die von einem Kunden-Gateway-Gerät einer Site-to-Site-VPN-Verbindung auf einem Transit Gateway angekündigt werden	1.000	Nein

Name	Standard	Anpassbar
Routen, die einem Kunden-Gateway-Gerät von einer Site-to-Site-VPN-Verbindung auf einem Transit Gateway angekündigt werden	5,000	Nein
Statische Routen von einem Kunden-Gateway-Gerät von einer Site-to-Site-VPN-Verbindung auf einem Virtual Private Gateway	100	Nein

Bandbreite und Durchsatz

Es gibt viele Faktoren, die die realisierte Bandbreite durch eine Site-to-Site-VPN-Verbindung beeinflussen können, einschließlich, aber nicht beschränkt auf: Paketgröße, Traffic-Mix (TCP/UDP), Gestaltungs- 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

Bei Site-to-Site VPN-Verbindungen auf einem Transit-Gateway können Sie ECMP verwenden, um eine höhere VPN-Bandbreite zu erhalten, 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](#).

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 Ihr Kunden-Gateway-Gerät](#).

Jumbo-Frames werden nicht unterstützt. Weitere Informationen finden Sie unter [Jumbo Frames](#) im Amazon EC2 EC2-Benutzerhandbuch.

Site-to-Site VPN-Verbindungen unterstützen Path MTU Discovery nicht.

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.

Dokumentverlauf für das Benutzerhandbuch zu Site-to-Site VPN

Die folgende Tabelle beschreibt die Überarbeitungen des AWS Site-to-Site VPN-Benutzerhandbuchs.

Änderung	Beschreibung	Datum
Informationen zum klassischen VPN entfernt	Informationen zum klassischen VPN wurden aus dem Handbuch entfernt.	19. Januar 2023
Beispielmeldungen für das VPN-Protokoll	Für Site-to-Site-VPN-Verbindungen hinzugefügte Beispielprotokolle.	9. Dezember 2022
Aktualisiertes Download-Konfigurationsprogramm	Site-to-Site-VPN-Kunden können Konfigurationsvorlagen für kompatible Kunden-Gateway-(CGW)-Geräte generieren, was das Erstellen von VPN-Verbindungen zu AWS einfacher macht. Dieses Update fügt Support für Internet Key Exchange Version 2 (IKEv2)-Parameter für viele gängige CGW-Geräte hinzu und enthält zwei neue APIs – GetVpnConnectionDeviceTypes und GetVpnConnectionDeviceSampleConfiguration.	21. September 2021
Benachrichtigungen über VPN-Verbindungen	Site-to-Site VPN sendet automatisch Benachrichtigungen über Ihre VPN-Verbi	29. Oktober 2020

	ndung an das AWS Health Dashboard.	
VPN-Tunnel-Initiierung	Sie können Ihre VPN-Tunnel so konfigurieren, dass AWS die Tunnel aufruft.	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-Support	Ihre VPN-Tunnel können IPv6-Datenverkehr innerhalb der Tunnel unterstützen.	12. August 2020
Zusammenführen von AWS Site-to-Site VPN-Leitfäden	In dieser Version wird der Inhalt des AWS Site-to-Site VPN-Netzwerkadministrator-Handbuchs in dieses Handbuch integriert.	31. März 2020
Beschleunigte AWS Site-to-Site VPN-Verbindungen	Sie können die Beschleunigung für Ihre AWS Site-to-Site VPN-Verbindung aktivieren.	3. Dezember 2019
Ändern von AWS Site-to-Site VPN-Tunnel-Optionen	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 privater Zertifikate	Sie können ein privates Zertifikat aus AWS Private Certificate Authority verwenden, um Ihr VPN zu authentifizieren.	15. August 2019
Neues Site-to-Site-VPN-Benutzerhandbuch	In dieser Version wurde der Inhalt von AWS Site-to-Site VPN (früher bekannt als AWS-verwaltetes VPN) aus dem Amazon-VPC-Benutzerhandbuch herausgetrennt.	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 anzeigen.	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 nun IPsec-VPN-Verbindungen mit Amazon VPC herstellen, indem Sie statische Routing-Konfigurationen verwenden. 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 Propagierung von Routen von Ihren VPN- und AWS Direct Connect-Links in 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.