

# Konfigurieren von ASA IPsec VTI Connection Amazon Web Services

## Inhalt

[Einführung](#)

[Konfigurieren von AWS](#)

[Konfigurieren der ASA](#)

[Verifizieren und Optimieren](#)

## Einführung

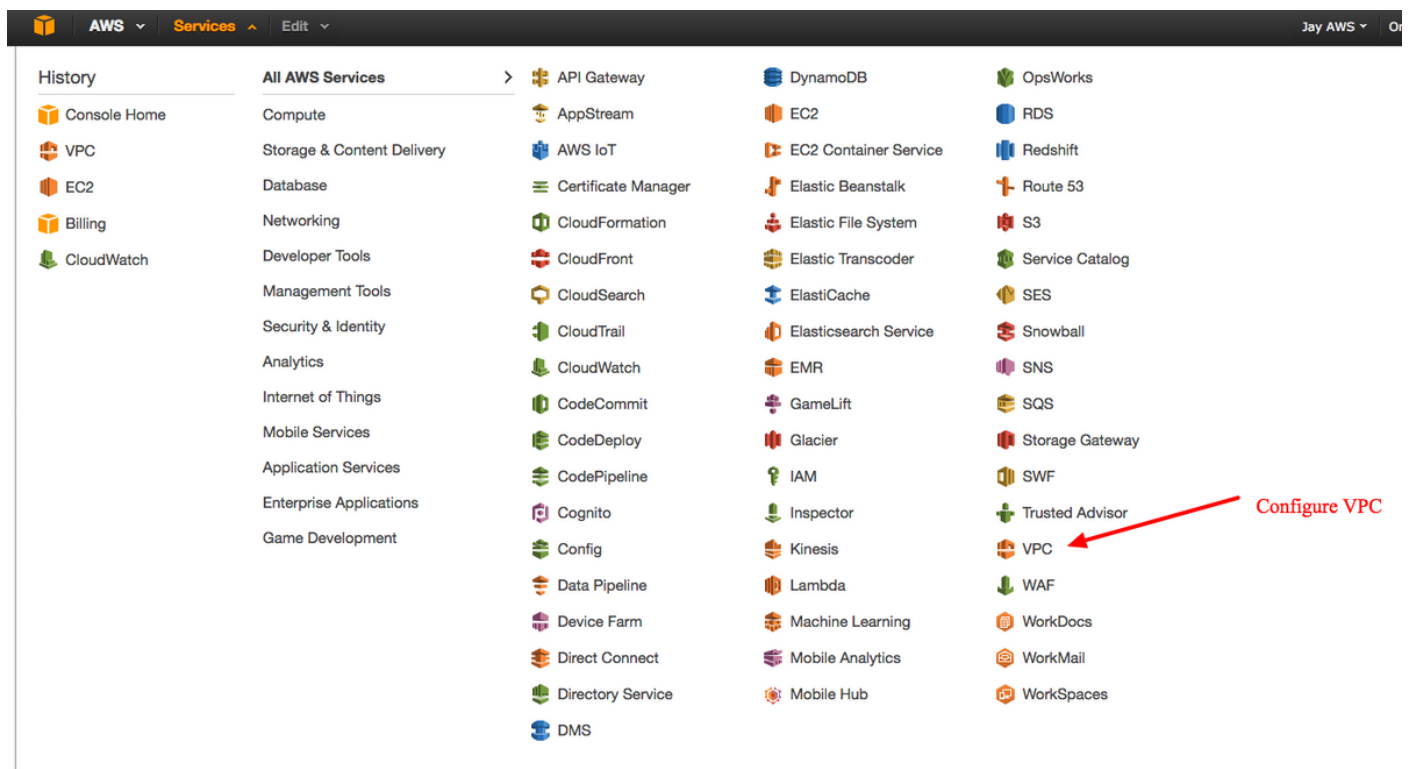
In diesem Dokument wird beschrieben, wie eine IPsec Virtual Tunnel Interface (VTI)-Verbindung (Adaptive Security Appliance) konfiguriert wird. In ASA 9.7.1 wurde IPsec VTI eingeführt. In dieser Version ist es auf sVTI IPv4 over IPv4 beschränkt, das IKEv1 verwendet. Dies ist eine Beispielfigur für die ASA für die Verbindung mit Amazon Web Services (AWS).

**Hinweis:** VTI wird derzeit nur im Single-Context-Routing-Modus unterstützt.

## Konfigurieren von AWS

### Schritt 1:

Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum VPC-Panel.



Navigieren Sie zum VPC Dashboard.

## Schritt 2:

Bestätigen Sie, dass bereits eine Virtual Private Cloud (VPC) erstellt wurde. Standardmäßig wird ein VPC mit 172.31.0.0/16 erstellt. Hier werden virtuelle Systeme (VMs) angehängt.

The screenshot shows the AWS VPC Dashboard. On the left, the 'Your VPCs' link is circled in red. The main table lists VPCs with columns: Name, VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default VPC. One VPC is listed with ID vpc-e1e00786, State available, and CIDR 172.31.0.0/16. Below the table, the details for vpc-e1e00786 (172.31.0.0/16) are shown, including VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, DNS resolution, DNS hostnames, and ClassicLink DNS Support. A red arrow points from the text 'Default VPC already created' to the VPC CIDR '172.31.0.0/16' in the table.

## Schritt 3:

Erstellen Sie ein "Kunden-Gateway". Dies ist ein Endpunkt, der die ASA darstellt.

### Feld Wert

Name-Tag Dies ist nur ein für Benutzer lesbarer Name, um die ASA zu erkennen.

Routing Dynamisch - Dies bedeutet, dass Border Gateway Protocol (BGP) zum Austausch von Routing-Informationen verwendet wird.

IP-Adresse Dies ist die öffentliche IP-Adresse der externen ASA-Schnittstelle.

BGP ASN Die AS-Nummer (Autonomous System) des BGP-Prozesses, die auf der ASA ausgeführt wird. Verwenden Sie 65000, es sei denn, Ihr Unternehmen verfügt über eine öffentliche AS-Nummer.

The screenshot displays the AWS Management Console interface for creating a Customer Gateway. The main navigation pane on the left lists various VPC services, with 'Customer Gateways' selected. The main content area shows a 'Create Customer Gateway' dialog box with the following configuration:

- Name tag: ASAVTI
- Routing: Dynamic
- IP address: 192.0.2.1
- BGP ASN: 65000

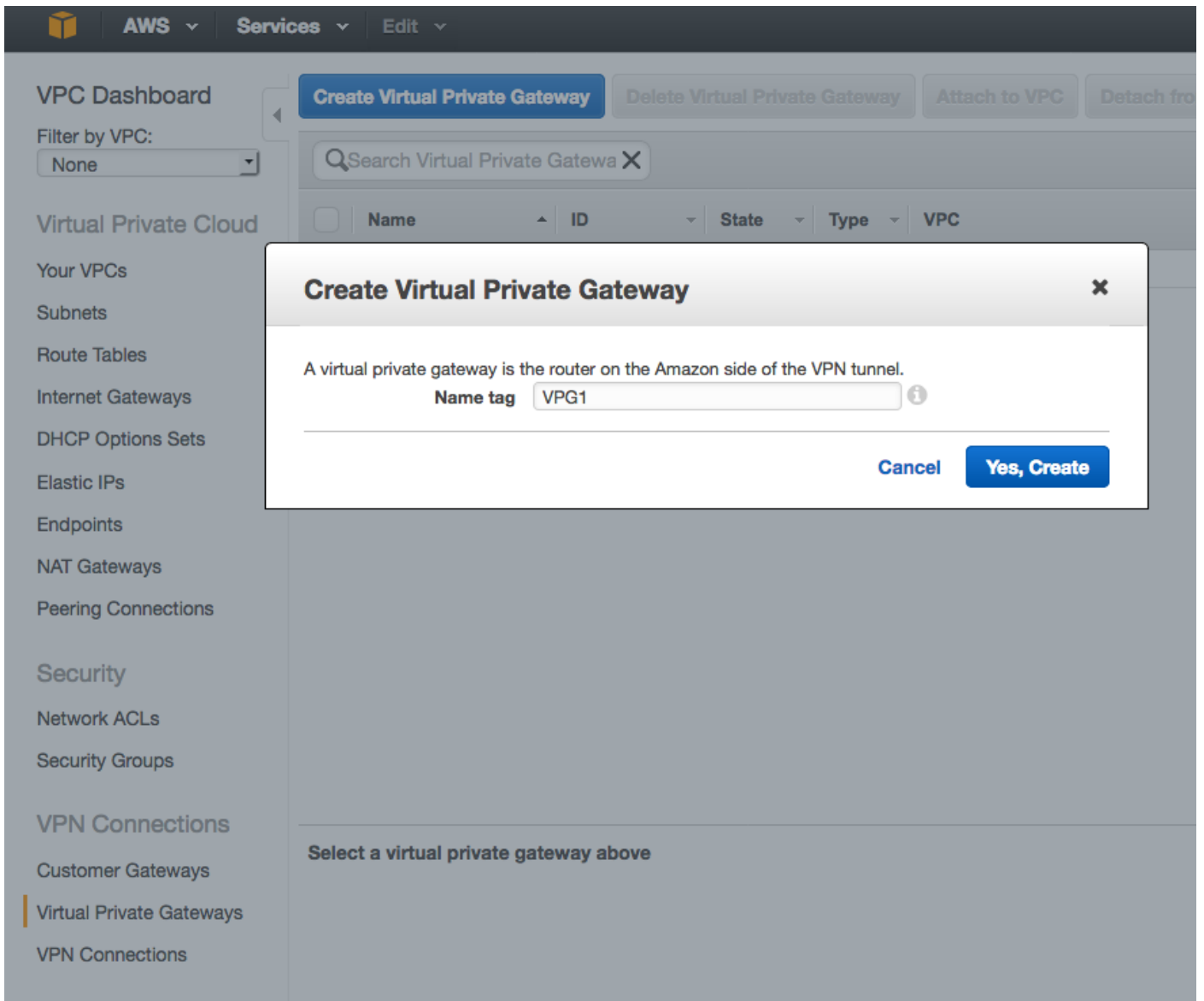
Below the dialog box, the details for a Customer Gateway (cgw-b778a1a9) are shown, including its ID, State (deleted), Type (ipsec.1), IP address (64.100.251.37), and BGP ASN (65000).

#### Schritt 4:

Erstellen Sie ein Virtual Private Gateway (VPG). Dies ist ein simulierter Router, der mit AWS gehostet wird, der den IPsec-Tunnel terminiert.

**Feld**      **Wert**

Name-Tag Ein für Benutzer lesbarer Name zur Erkennung des VPG.



## Schritt 5:

Verbinden Sie das VPG mit dem VPC.

Wählen Sie das Virtual Private Gateway aus, klicken Sie auf **An VPC anhängen**, wählen Sie in der VPC-Dropdown-Liste den VPC aus, und klicken Sie auf **Ja, Anfügen**.

The screenshot displays the AWS Management Console interface for Virtual Private Gateways. At the top, there are navigation tabs: 'Create Virtual Private Gateway', 'Delete Virtual Private Gateway', 'Attach to VPC', and 'Detach from VPC'. Below these is a search bar and a table of Virtual Private Gateways. The table has columns for Name, ID, State, Type, and VPC. One entry is visible: 'VPG1' with ID 'vgw-18954d06', State 'detached', and Type 'ipsec.1'. A red circle highlights the checkbox next to 'VPG1'. A red arrow points from this checkbox to the 'Attach to VPC' button in the top navigation bar. Another red arrow points from the 'Attach to VPC' button to the 'Yes, Attach' button in the dialog box.

**Attach to VPC**

Select the VPC to attach to the virtual private gateway

VPC: vpc-e1e00786 (172.31.0.0/16)

Cancel Yes, Attach

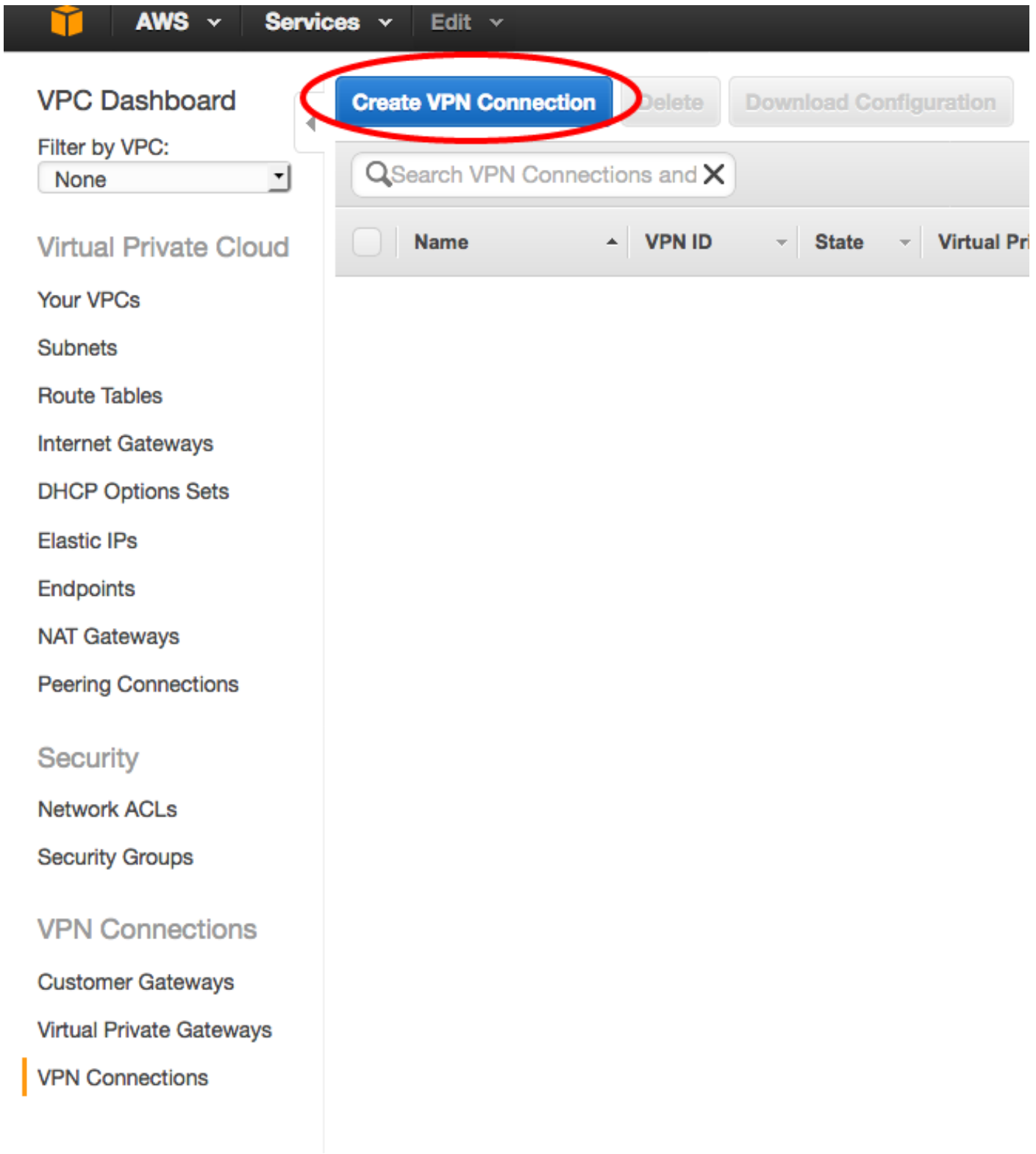
vgw-18954d06 | VPG1

Summary Tags

ID: vgw-18954d06 | VPG1  
State: detached  
Type: ipsec.1  
VPC:

## Schritt 6:

Erstellen einer VPN-Verbindung



**Feld**

- Name-Tag
- Virtuelles privates Gateway
- Kundengateway
- Routing-Optionen

**Wert**

- Ein für Benutzer lesbares Tag der VPN-Verbindung zwischen AWS und der AS
- Wählen Sie das soeben erstellte VPG aus.
- Klicken Sie auf das Optionsfeld **Vorhandenes** und wählen Sie das Gateway de
- aus.
- Klicken Sie auf das Optionsfeld **Dynamisch (BGP erforderlich)**.

The screenshot shows the AWS Management Console interface for creating a VPN connection. The left sidebar contains navigation options like 'VPC Dashboard', 'Virtual Private Cloud', and 'VPN Connections'. The main area displays a 'Create VPN Connection' dialog box with the following fields and options:

- Name tag:** VPNtoASA
- Virtual Private Gateway:** vgw-18954d06 | VPG1
- Customer Gateway:** Existing (selected) / New. Selected: cgw-837fa69d (64.100.251.37) | ASAVTI
- Routing Options:** Dynamic (requires BGP) (selected) / Static

Additional text in the dialog includes: 'Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.', 'Specify the routing for the VPN Connection (Help me choose)', and 'VPN connection charges apply once this step is complete. View Rates'. Buttons for 'Cancel' and 'Yes, Create' are at the bottom right.

## Schritt 7:

Konfigurieren Sie die Routentabelle so, dass die vom VPG (über BGP) empfangenen Routen an den VPC weitergegeben werden.

AWS Services Edit

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	rtb-3a3f9e5d	0 Subnets	Yes	vpc-e1e00786 (172.31.0.0/16)

rtb-3a3f9e5d

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Virtual Private Gate way Propagate

vgw-d19f47cf

vgw-18954d06 | VPG1

### Schritt 8:

Laden Sie die vorgeschlagene Konfiguration herunter. Wählen Sie die unten stehenden Werte aus, um eine Konfiguration im VTI-Stil zu generieren.

Feld	Wert
Anbieter	Cisco Systems, Inc.
Plattform	Router der ISR-Serie
Software	IOS 12.4+



The screenshot shows the AWS Management Console interface for VPN Connections. A modal dialog titled "Download Configuration" is open, asking the user to select configuration options for a customer gateway. The dialog includes the following fields:

- Vendor:** Cisco Systems, Inc.
- Platform:** ISR Series Routers
- Software:** IOS 12.4+

Red arrows point to these fields with the text "Pick IOS". The "Yes, Download" button is circled in red. In the background, a table lists VPN connections, with the "VPNtoASA" entry selected and circled in red. A red arrow also points from the "Download Configuration" button in the top navigation bar to the dialog.

## Konfigurieren der ASA

Nach dem Herunterladen der Konfiguration ist eine Konvertierung erforderlich.

### Schritt 1:

crypto isakmp Policy to crypto ikev1 policy. Da die Richtlinie 200 und die Richtlinie 201 identisch sind, wird nur eine Richtlinie benötigt.

#### Empfohlene Konfiguration

```
crypto isakmp-Richtlinie 200
  Verschlüsselung aes 128
  Authentifizierung Pre-Share
  Gruppe 2
  Lebensdauer 28800
  Hash-Sha
Ausgang
crypto isakmp policy 201
  Verschlüsselung aes 128
  Authentifizierung Pre-Share
  Gruppe 2
```

#### An

```
crypto ikev1-Aktivierung außerhalb
crypto ikev1-Richtlinie 10
  Authentifizierung Pre-Share
  Verschlüsselungsstufen
  Hash-Sha
  Gruppe 2
  Lebensdauer 28800
```

Lebensdauer 28800  
Hash-Sha  
Ausgang

## Schritt 2:

crypto ipsec-Transformationssatz auf crypto ipsec ikev1-Transformationssatz. Es wird nur ein Transformationssatz benötigt, da die beiden Transformationssätze identisch sind.

### Empfohlene Konfiguration

```
crypto ipsec-Transformationssatz ipsec-prop-vpn-7c79606e-0 esp-aes 128 esp-sha-hmac
  Modustunnel
Ausgang
crypto ipsec-Transformationssatz ipsec-prop-vpn-7c79606e-1 esp-aes 128 esp-sha-hmac
  Modustunnel
Ausgang
```

### An

```
crypto ipsec ikev1
transformationsset AWS esp
esp-sha-hmac
```

## Schritt 3:

crypto ipsec-Profil in crypto ipsec-Profil. Es wird nur ein Profil benötigt, da die beiden Profile identisch sind.

### Empfohlene Konfiguration

```
crypto ipsec-Profil ipsec-vpn-7c79606e-0
  Set-pfs-Gruppe2
  Einstellen der Lebensdauer der
  Sicherheitszuordnung 3600
  set transformation set ipsec-prop-vpn-7c79606e-0
Ausgang
crypto ipsec-Profil ipsec-vpn-7c79606e-1
  Set-pfs-Gruppe2
  Einstellen der Lebensdauer der
  Sicherheitszuordnung 3600
  set transformation set ipsec-prop-vpn-7c79606e-1
Ausgang
```

### An

```
crypto ipsec-Profil AWS
ikev1 transformations-set AWS
festlegen
  Set-pfs-Gruppe2
  Einstellen der Lebensdauer der
  Sicherheitszuordnung 3600
```

## Schritt 4:

crypto keyring und crypto isakmp profile müssen für jeden Tunnel in eine Tunnel-Gruppe eins konvertiert werden.

### Empfohlene Konfiguration

```
crypto keyring keyring-vpn-7c79606e-0
  local-address 64.100.251.37
  Pre-shared-key address 52.34.205.227 key QZhh90Bjf
Ausgang
!
crypto isakmp profile isakmp-vpn-7c79606e-0
  local-address 64.100.251.37
  Übereinstimmung Identitätsadresse 52.34.205.227
```

### An

```
tunnel-group
52.34.205.227, type
ipsec-l2l
tunnel-group
52.34.205.227 ipsec
attribute
ikev1 Pre-shared-k
QZhh90Bjf
```

```

keyring keyring-vpn-7c79606e-0
Ausgang
!
crypto keyring keyring-vpn-7c79606e-1
local-address 64.100.251.37
Pre-shared-key address 52.37.194.219 key JjxCWy4Ae
Ausgang
!
crypto isakmp profile isakmp-vpn-7c79606e-1
local-address 64.100.251.37
Übereinstimmung Identitätsadresse 52.37.194.219
keyring-vpn-7c79606e-1
Ausgang
isakmp keepalive-
Grenzwert 10 retry
tunnel-group
52.37.194.219 type
ipsec-l2l
tunnel-group
52.37.194.219 ipsec
attribute
ikev1 Pre-shared-k
JXCWy4Ae
isakmp keepalive-
Grenzwert 10 retry

```

### Schritt 5:

Die Tunnelkonfiguration ist fast identisch. Die ASA unterstützt nicht den Befehl `ip tcp adjust-mss` oder `ip virtual-reassembly`.

#### Empfohlene Konfiguration

```

interface Tunnell
ip address 169.254.13.190 255.255.255.252
ip virtuelle Reassemblierung
Tunnelquelle 64.100.251.37
Tunnelziel 52.34.205.227
Tunnelmodus ipsec ipv4
Tunnelschutz ipsec-Profil ipsec-vpn-7c79606e-0
ip tcp adjust-mss 1387
Kein Herunterfahren
Ausgang
!
Interface Tunnel2
ip address 169.254.12.86 255.255.255.252
ip virtuelle Reassemblierung
Tunnelquelle 64.100.251.37
Tunnelziel 52.37.194.219
Tunnelmodus ipsec ipv4
Tunnelschutz ipsec-Profil ipsec-vpn-7c79606e-1
ip tcp adjust-mss 1387
Kein Herunterfahren
Ausgang

```

#### An

```

interface Tunnell
nameif AWS1
ip address 169.254.13.190
255.255.255.252
Tunnelquellenschnittstelle
außerhalb
Tunnelziel 52.34.205.227
Tunnelmodus ipsec ipv4
Tunnel Protection IPS-Profil
!
Interface Tunnel2
nameif AWS2
ip address 169.254.12.86
255.255.255.252
Tunnelquellenschnittstelle
außerhalb
Tunnelziel 52.37.194.219
Tunnelmodus ipsec ipv4
Tunnel Protection IPS-Profil

```

### Schritt 6:

In diesem Beispiel kündigt die ASA nur das interne Subnetz (192.168.1.0/24) an und empfängt das Subnetz innerhalb von AWS (172.31.0.0/16).

#### Empfohlene Konfiguration

```

Router BGP 65000
neighbor 169.254.13.189 remote-as 7224
neighbor 169.254.13.189 aktivieren
neighbor 169.254.13.189 timers 10 30 30
address-family ipv4 Unicast
neighbor 169.254.13.189 remote-as 7224

```

#### An

```

Router BGP 65000
bgp log-neighbor-changes
timers bgp 10 30 0
address-family ipv4 Unicast
neighbor 169.254.12.85
remote-as 7224

```

```

neighbor 169.254.13.189 timers 10 30 30
neighbor 169.254.13.189 default-originate
neighbor 169.254.13.189 aktivieren
neighbor 169.254.13.189 Soft-Reconfiguration
eingehender Datenverkehr
Netzwerk 0.0.0.0
Ausgang
Ausgang
Router BGP 65000
neighbor 169.254.12.85 remote-as 7224
neighbor 169.254.12.85 aktivieren
neighbor 169.254.12.85 timers 10 30 30
address-family ipv4 Unicast
neighbor 169.254.12.85 remote-as 7224
neighbor 169.254.12.85 timers 10 30 30
neighbor 169.254.12.85 default-originate
neighbor 169.254.12.85 aktivieren
neighbor 169.254.12.85 Soft-Reconfiguration
eingehender
Netzwerk 0.0.0.0
Ausgang
Ausgang

```

```

neighbor 169.254.12.85
aktivieren
neighbor 169.254.13.189
remote-as 7224
neighbor 169.254.13.189
aktivieren
Netzwerk 192.168.1.0
keine automatische
Zusammenfassung
Keine Synchronisierung
Exitadresse-Familie

```

## Verifizieren und Optimieren

### Schritt 1:

Bestätigen Sie, dass die ASA die IKEv1-Sicherheitszuordnungen zu den beiden Endpunkten bei AWS herstellt. Der Status der SA muss "MM\_ACTIVE" lauten.

```
ASA# show crypto ikev1 sa
```

```
IKEv1 SAs:
```

```

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: 52.37.194.219
   Type      : L2L           Role      : initiator
   Rekey     : no           State     : MM_ACTIVE
2  IKE Peer: 52.34.205.227
   Type      : L2L           Role      : initiator
   Rekey     : no           State     : MM_ACTIVE

```

```
ASA#
```

### Schritt 2:

Bestätigen Sie, dass die IPsec SAs auf ASA installiert sind. Für jeden Peer sollte ein ein- und ausgehender SPI installiert sein. Es sollten inkrementelle Encaps und Decaps-Zähler vorhanden sein.

```
ASA# show crypto ipsec sa
```

interface: AWS1

Crypto map tag: \_\_vti-crypto-map-5-0-1, seq num: 65280, local addr: 64.100.251.37

access-list \_\_vti-def-acl-0 extended permit ip any any  
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: 52.34.205.227

#pkts encaps: 2234, #pkts encrypt: 2234, #pkts digest: 2234  
#pkts decaps: 1234, #pkts decrypt: 1234, #pkts verify: 1234  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 2234, #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  
#TFC rcvd: 0, #TFC sent: 0  
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0  
#send errors: 0, #recv errors: 0

local crypto endpt.: 64.100.251.37/4500, remote crypto endpt.: 52.34.205.227/4500  
path mtu 1500, ipsec overhead 82(52), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: 874FCCF3  
current inbound spi : 5E653906

inbound esp sas:

spi: 0x5E653906 (1583692038)  
transform: esp-aes esp-sha-hmac no compression  
in use settings =(L2L, Tunnel, NAT-T-Encaps, PFS Group 2, IKEv1, VTI, )  
slot: 0, conn\_id: 73728, crypto-map: \_\_vti-crypto-map-5-0-1  
sa timing: remaining key lifetime (kB/sec): (4373986/2384)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0x874FCCF3 (2270153971)  
transform: esp-aes esp-sha-hmac no compression  
in use settings =(L2L, Tunnel, NAT-T-Encaps, PFS Group 2, IKEv1, VTI, )  
slot: 0, conn\_id: 73728, crypto-map: \_\_vti-crypto-map-5-0-1  
sa timing: remaining key lifetime (kB/sec): (4373986/2384)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001

interface: AWS2

Crypto map tag: \_\_vti-crypto-map-6-0-2, seq num: 65280, local addr: 64.100.251.37

access-list \_\_vti-def-acl-0 extended permit ip any any  
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: 52.37.194.219

#pkts encaps: 1230, #pkts encrypt: 1230, #pkts digest: 1230  
#pkts decaps: 1230, #pkts decrypt: 1230, #pkts verify: 1230  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 1230, #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  
#TFC rcvd: 0, #TFC sent: 0  
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

```

#send errors: 0, #recv errors: 0

local crypto endpt.: 64.100.251.37/4500, remote crypto endpt.: 52.37.194.219/4500
path mtu 1500, ipsec overhead 82(52), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: DC5E3CA8
current inbound spi : CB6647F6

inbound esp sas:
spi: 0xCB6647F6 (3412477942)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 2, IKEv1, VTI, }
slot: 0, conn_id: 77824, crypto-map: __vti-crypto-map-6-0-2
sa timing: remaining key lifetime (kB/sec): (4373971/1044)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:
spi: 0xDC5E3CA8 (3697163432)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 2, IKEv1, VTI, }
slot: 0, conn_id: 77824, crypto-map: __vti-crypto-map-6-0-2
sa timing: remaining key lifetime (kB/sec): (4373971/1044)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

### Schritt 3:

Vergewissern Sie sich auf der ASA, dass BGP-Verbindungen mit AWS hergestellt werden. Der State/PfxRcd-Zähler sollte 1 lauten, da AWS das Subnetz 172.31.0.0/16 gegenüber der ASA ankündigt.

#### ASA# show bgp summary

```

BGP router identifier 192.168.1.55, local AS number 65000
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
3 path entries using 240 bytes of memory
3/2 BGP path/bestpath attribute entries using 624 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
BGP using 1288 total bytes of memory
BGP activity 3/1 prefixes, 4/1 paths, scan interval 60 secs

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
169.254.12.85	4	7224	1332	1161	5	0	0	03:41:31	1
169.254.13.189	4	7224	1335	1164	5	0	0	03:42:02	1

### Schritt 4:

Überprüfen Sie auf der ASA, ob die Route zu 172.31.0.0/16 über die Tunnelschnittstellen gelernt wurde. Diese Ausgabe zeigt, dass es zwei Pfade zu 172.31.0.0 von Peer 169.254.12.85 und 169.254.13.189 gibt. Der Pfad zu 169.254.13.189 Out Tunnel 2 (AWS2) wird aufgrund der niedrigeren Metrik bevorzugt.

```
ASA# show bgp
```

```
BGP table version is 5, local router ID is 192.168.1.55
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
* 172.31.0.0	169.254.12.85	200		0	7224 i
*>	169.254.13.189	100		0	7224 i
*> 192.168.1.0	0.0.0.0	0		32768	i

```
ASA# show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 64.100.251.33 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 64.100.251.33, outside
C 64.100.251.32 255.255.255.224 is directly connected, outside
L 64.100.251.37 255.255.255.255 is directly connected, outside
C 169.254.12.84 255.255.255.252 is directly connected, AWS2
L 169.254.12.86 255.255.255.255 is directly connected, AWS2
C 169.254.13.188 255.255.255.252 is directly connected, AWS1
L 169.254.13.190 255.255.255.255 is directly connected, AWS1
B 172.31.0.0 255.255.0.0 [20/100] via 169.254.13.189, 03:52:55
C 192.168.1.0 255.255.255.0 is directly connected, inside
L 192.168.1.55 255.255.255.255 is directly connected, inside
```

## Schritt 5:

Um sicherzustellen, dass Datenverkehr, der von AWS zurückgegeben wird, einem symmetrischen Pfad folgt, konfigurieren Sie eine Routenübersicht so, dass sie dem bevorzugten Pfad entspricht, und passen Sie das BGP so an, dass die angegebenen Routen geändert werden.

```
route-map toAWS1 permit 10
  set metric 100
  exit
!
route-map toAWS2 permit 10
  set metric 200
  exit
!
router bgp 65000
  address-family ipv4 unicast
    neighbor 169.254.12.85 route-map toAWS2 out
    neighbor 169.254.13.189 route-map toAWS1 out
```

## Schritt 6:

Vergewissern Sie sich auf der ASA, dass AWS 192.168.1.0/24 angekündigt wird.

```
ASA# show bgp neighbors 169.254.12.85 advertised-routes
```

BGP table version is 5, local router ID is 192.168.1.55  
 Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,  
 r RIB-failure, S Stale, m multipath  
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.31.0.0	169.254.13.189	100		0	7224 i
*> 192.168.1.0	0.0.0.0	0		32768	i

Total number of prefixes 2

ASA# **show bgp neighbors 169.254.13.189 advertised-routes**

BGP table version is 5, local router ID is 192.168.1.55  
 Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,  
 r RIB-failure, S Stale, m multipath  
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.168.1.0	0.0.0.0	0		32768	i

Total number of prefixes 1

### Schritt 7:

AWS: Vergewissern Sie sich, dass die Tunnel für die VPN-Verbindung aktiv sind, und dass Routen vom Peer erfasst werden. Überprüfen Sie außerdem, ob die Route in die Routing-Tabelle propagiert wurde.

The screenshot shows the AWS Management Console interface for VPN Connections. The left sidebar lists various services, with 'VPN Connections' selected. The main content area shows a table of VPN Connections. One connection, 'VPNtoASA', is highlighted. Below the table, the 'Tunnel Details' tab is active, showing a table of VPN Tunnels. Two tunnels are listed, both with a status of 'UP'. The 'Status' and 'Details' columns for these tunnels are circled in red.

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer Gateway Address	Type	VPC	Routing
VPNtoASA	vpn-7c79606e	available	vgw-18954d06   VPG1	cgw-837fa69d (64.100.251.37)   ASAVTI	64.100.251.37	ipsecc.1	vpc-e1e00786 (172.31.0.0/16)	Dynamic

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	52.34.205.227	UP	2016-10-18 14:23 UTC	1 BGP ROUTES
Tunnel 2	52.37.194.219	UP	2016-10-18 14:23 UTC	1 BGP ROUTES





### VPC Dashboard

Filter by VPC:

None

### Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

### Security

Network ACLs

Security Groups

### VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table

Delete Route Table

Set As Main Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>		rtb-3a3f9e5d	0 Subnets	Yes	vpc-e1e00786 (172.31.0.0/16)

#### rtb-3a3f9e5d

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	<a href="#">igw-e5ad1481</a>	Active	No
192.168.1.0/24	<a href="#">vgw-18954d06</a>	Active	Yes