

ASA IPsec VTI-verbinding configureren Web Services

Inhoud

[Inleiding](#)

[AWS configureren](#)

[De ASA configureren](#)

[Verifiëren en optimaliseren](#)

Inleiding

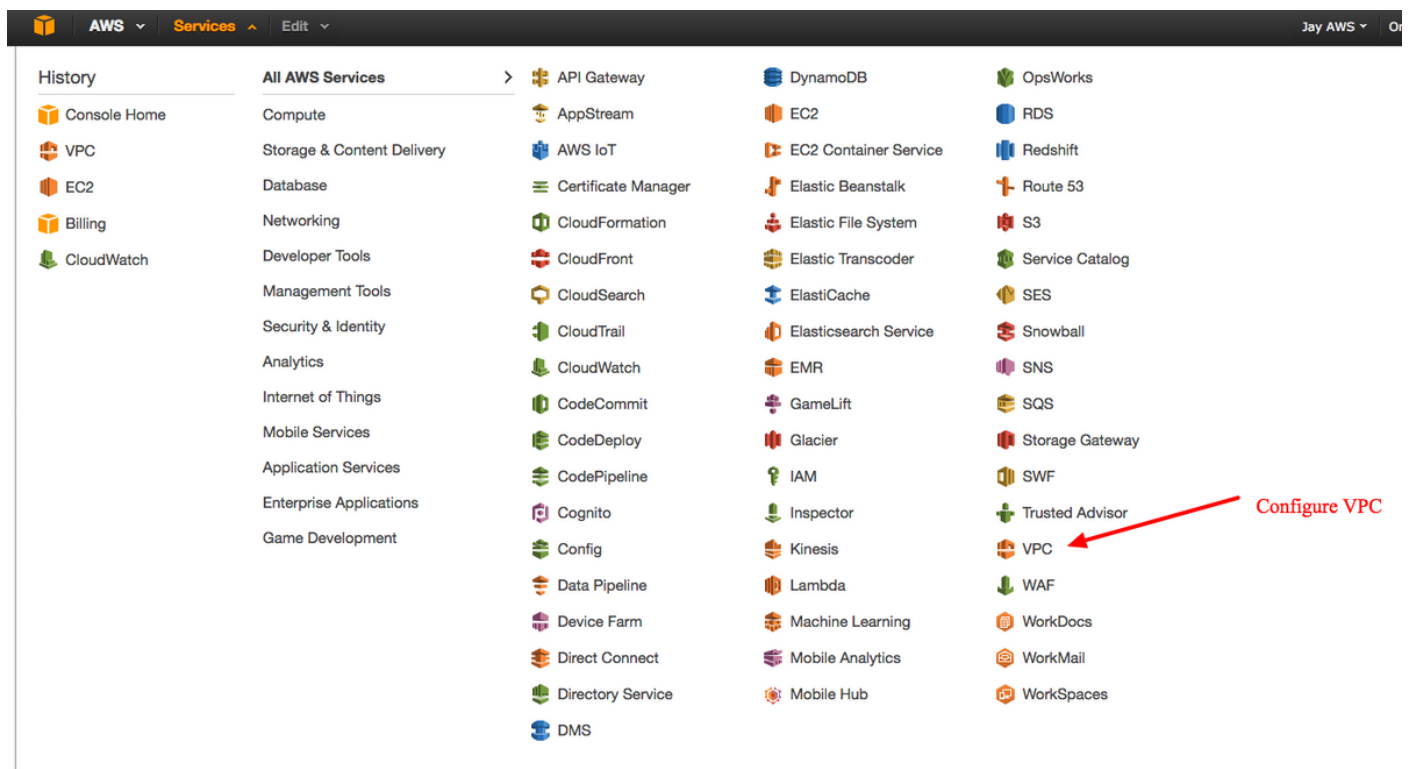
Dit document beschrijft hoe u een adaptieve security applicatie (ASA) kunt configureren en IPsec Virtual Tunnel Interface (VTI) verbinding. In ASA 9.7.1 is IPsec VTI geïntroduceerd. Het is beperkt tot sVTI IPv4 via IPv4 door IKEv1 in deze release te gebruiken. Dit is een voorbeeldconfiguratie voor de ASA om verbinding te maken met Amazon Web Services (AWS).

Opmerking: Momenteel wordt VTI alleen ondersteund in single-context, routed mode.

AWS configureren

Stap 1.

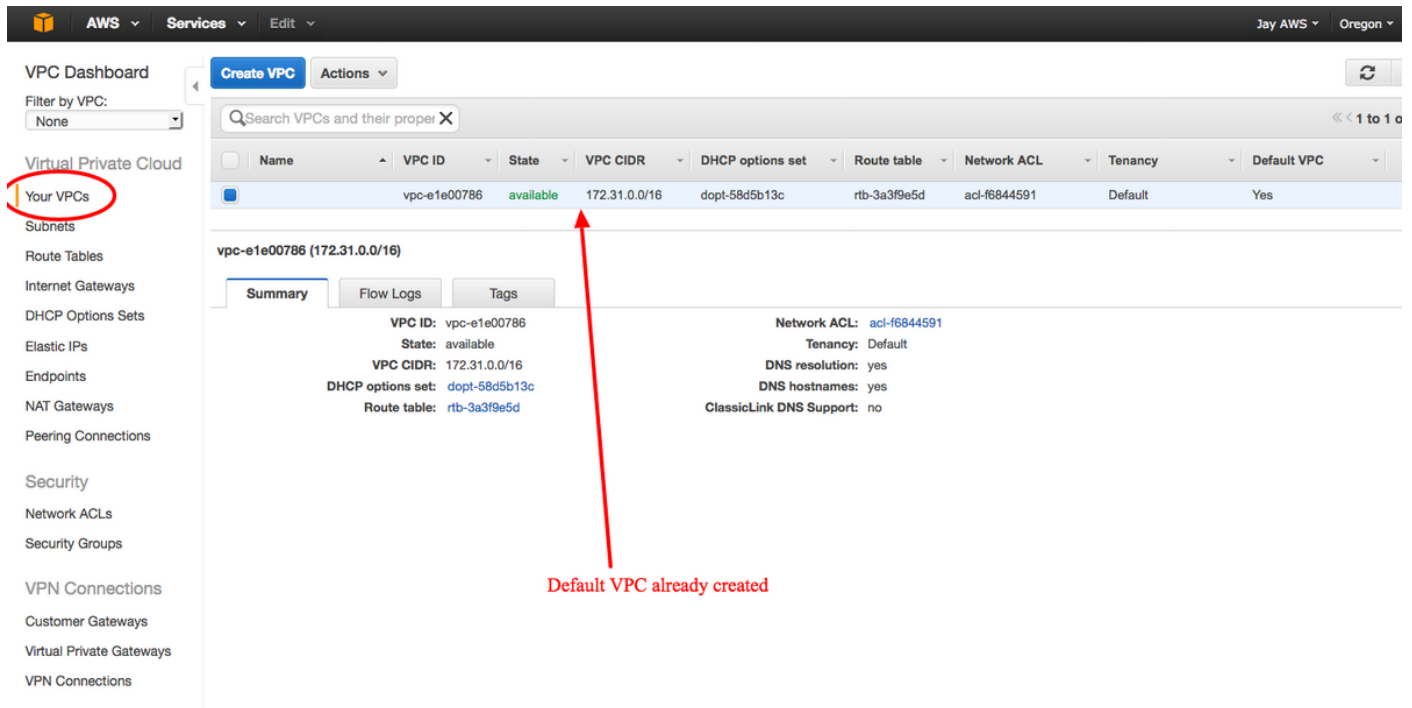
Meld u aan bij de AWS-console en navigeer naar het VPC-paneel.



Navigeren naar het VPC Dashboard

Stap 2.

Bevestig dat er al een Virtual Private Cloud (VPC) is gemaakt. Standaard wordt een VPC met 172.31.0.0/16 gemaakt. Hier worden virtuele machines (VM's) aangesloten.



The screenshot shows the AWS VPC Dashboard. On the left sidebar, 'Your VPCs' is circled in red. The main content area displays a table of VPCs with the following data:

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
	vpc-e1e00786	available	172.31.0.0/16	dopt-58d5b13c	rtb-3a3f9e5d	acl-f6844591	Default	Yes

Below the table, the details for the VPC 'vpc-e1e00786 (172.31.0.0/16)' are shown. A red arrow points from the text 'Default VPC already created' to the 'VPC CIDR' field in the details section, which is '172.31.0.0/16'.

Summary

- VPC ID: vpc-e1e00786
- State: available
- VPC CIDR: 172.31.0.0/16
- DHCP options set: dopt-58d5b13c
- Route table: rtb-3a3f9e5d
- Network ACL: acl-f6844591
- Tenancy: Default
- DNS resolution: yes
- DNS hostnames: yes
- ClassicLink DNS Support: no

Stap 3.

Maak een "klantgateway". Dit is een eindpunt dat de ASA representeert.

Veld Waarde

Naam Dit is gewoon een menselijke leesbare naam om de ASA te herkennen.

Routing Dynamisch - Dit betekent dat Border Gateway Protocol (BGP) wordt gebruikt voor het uitwisselen van routinginformatie.

IP-adres Dit is het openbare IP-adres van de externe interface van de ASA.

BGP ASN Het AS-nummer (Autonomous System) van het BGP-proces dan dat van de ASA. Gebruik 6500 tenzij uw organisatie een openbaar AS-nummer heeft.

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

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

Cancel Yes, Create

cgw-b778a1a9 (64.100.251.37)

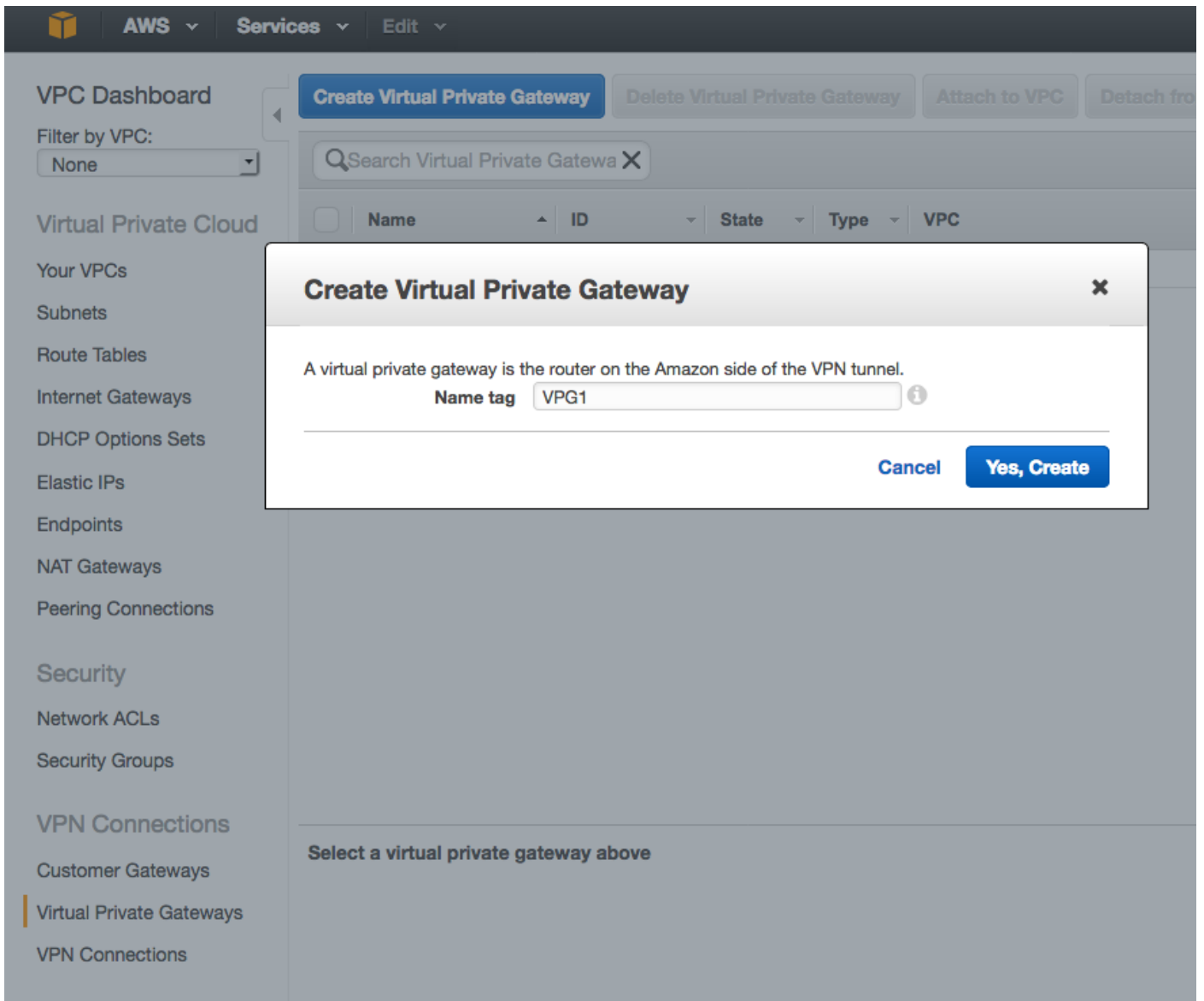
Summary	Tags
ID:	cgw-b778a1a9 (64.100.251.37)
State:	deleted
Type:	ipsec.1
IP address:	64.100.251.37
BGP ASN:	65000
VPC:	

Stap 4.

Maak een Virtual Private Gateway (VPG). Dit is een gesimuleerde router die met AWS wordt ontvangen die de IPsec-tunnel beëindigt.

Veld Waarde

Naam Een menselijke leesbare naam om de VPG te herkennen.



Stap 5.

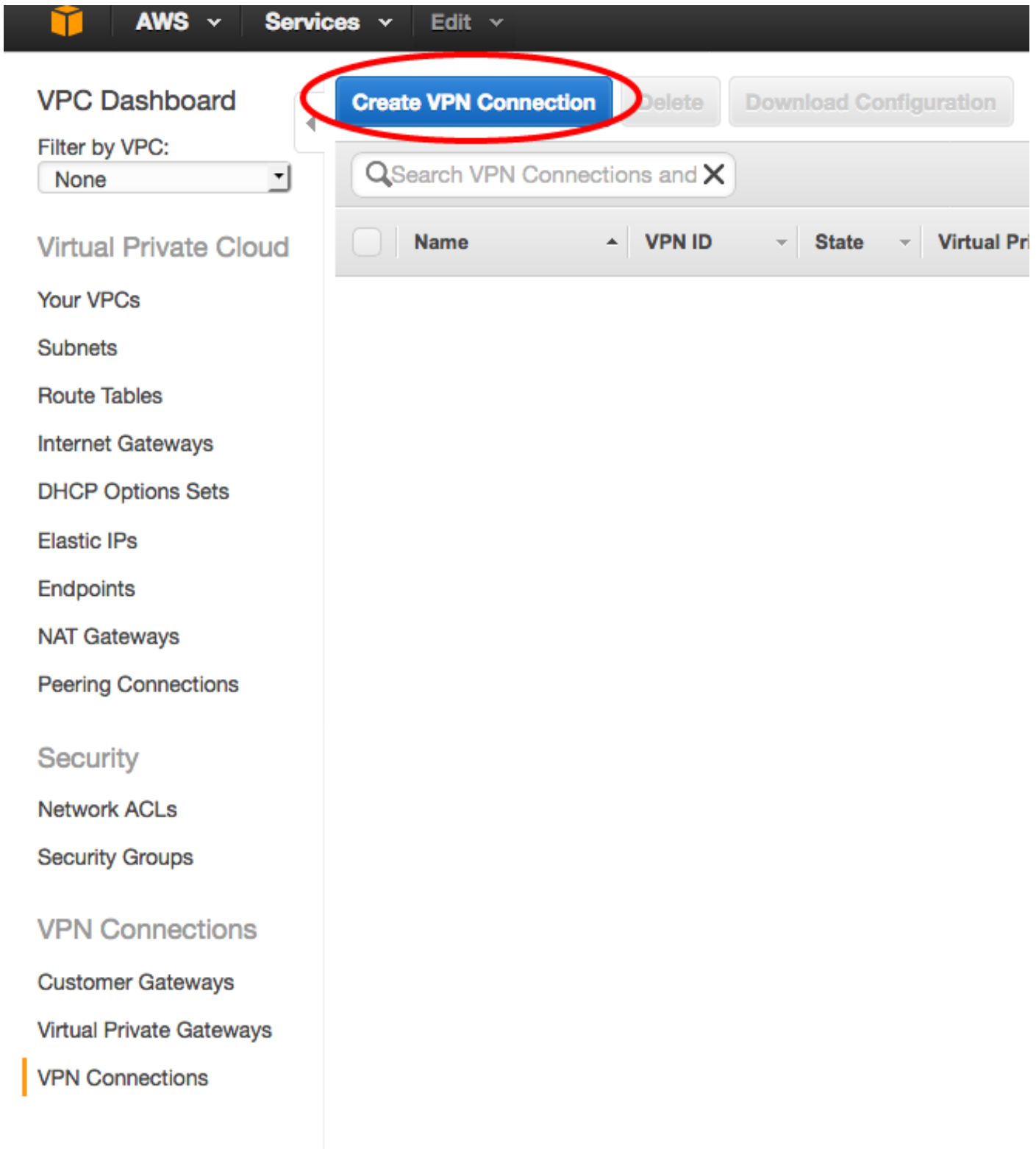
Sluit de VPG aan op de VPC.

Kies de Virtual Private Gateway, klik op **Attach to VPC**, kies de VPC in de vervolkeuzelijst VPC en klik op **Yes, Attach**.

The screenshot shows the AWS VPC Dashboard. At the top, there are buttons for '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 highlighted: 'VPG1' with ID 'vgw-18954d06', State 'detached', and Type 'ipsec.1'. A modal dialog titled 'Attach to VPC' is open, prompting the user to 'Select the VPC to attach to the virtual private gateway'. The 'VPC' dropdown menu is set to 'vpc-e1e00786 (172.31.0.0/16)'. At the bottom of the modal are 'Cancel' and 'Yes, Attach' buttons. Below the table, there is a section for 'vgw-18954d06 | VPG1' with tabs for 'Summary' and 'Tags'. The 'Summary' tab shows details: ID: vgw-18954d06 | VPG1, State: detached, Type: ipsec.1, and VPC: (empty).

Stap 6.

Een VPN-verbinding maken



Veld

- Naam
- Virtual Private Gateway
- Clientgateway
- Routing-opties

Waarde

- Een menselijk leesbaar label van de VPN-verbinding tussen AWS en de ASA.
- Kies de alleen gemaakte VPG.
- Klik op de **bestaande** radioknop en kies de gateway van de ASA.
- Klik op de radioknop **Dynamisch** (hiervoor is BGP nodig).

Step 7.

Configureer de routeswitch om de routes die zijn geleerd van de VPG (via BGP) naar de VPC te propageren.

The screenshot shows the AWS Management Console interface for configuring route propagation. The left sidebar lists various services, with 'Route Tables' selected. The main content area shows a table of route tables. The first row is selected, and the 'Route Propagation' tab is active. Below the tabs, there are buttons for 'Cancel', 'Save', 'Virtual Private Gateway', and 'Propagate'. A list of virtual private gateways is shown, with the checkbox for 'vgw-18954d06 | VPG1' checked. Red circles and arrows highlight the selection of the route table and the propagation of routes to the VPG1 virtual private gateway.

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 Gateway Propagate

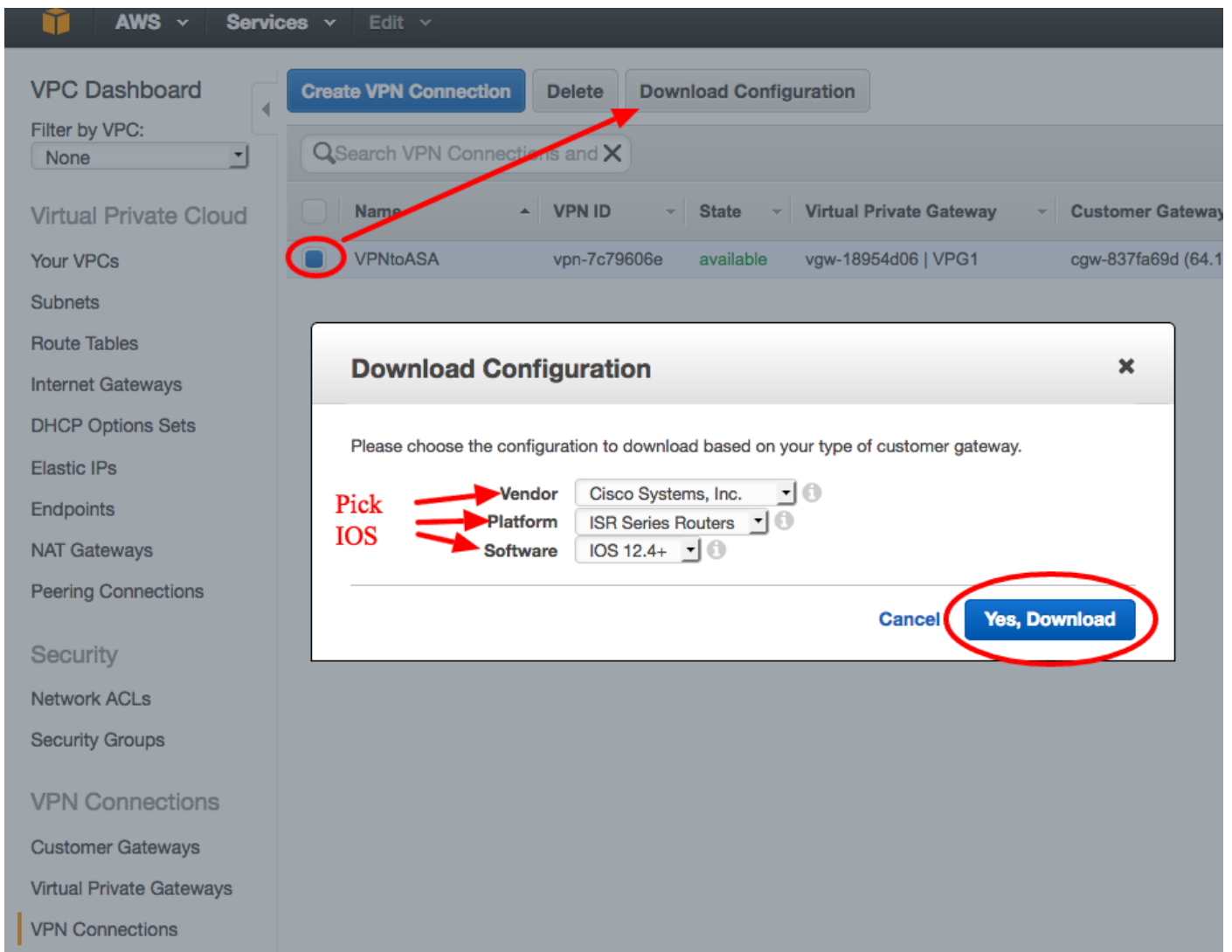
vgw-d19f47cf

vgw-18954d06 | VPG1

Stap 8.

Download de voorgestelde configuratie. Kies de onderstaande waarden om een configuratie te genereren die een VTI stijl-configuratie is.

Veld	Waarde
verkoper	Cisco Systems, Inc.
platform	ISR Series routers
Software	IOS-software-releases 12.4+



De ASA configureren

Zodra u de configuratie hebt gedownload, is er enige conversie nodig.

Stap 1.

het beleid van crypto isakmp ten aanzien van het crypto ikev1 - beleid . Er is slechts één beleid nodig omdat het beleid 2000 en het beleid 2010 identiek zijn.

Aanbevolen configuratie

```
crypto isakmp - beleid 200
  encryptie - aes 128
  controle vooraf
  groep 2
  levensduur 2800
  hash sha
  uitgang
crypto isakmp - beleid 2010
  encryptie - aes 128
  controle vooraf
  groep 2
```

Naar

```
encryptie ikev1 - mogelijkheid voor
buitengebruik
beleid inzake crypto ikev1 10
  controle vooraf
  encryptieapparaten
  hash sha
  groep 2
  levensduur 2800
```

```
levensduur 2800
hash sha
uitgang
```

Stap 2.

crypto ipsec transformatie-set voor crypto ipsec ikev1 transformatie-set. Er is slechts één transformatie-set nodig omdat de twee transformatoren identiek zijn.

Aanbevolen configuratie

```
crypto ipsec transformatie-set ipsec-prop-vpn-
7c79606e-0 esp-aes 128 esp-sha-hmac
  modemtunnel
uitgang
crypto ipsec transformatie-set ipsec-prop-vpn-
7c79606e-1 esp-aes 128 esp-sha-hmac
  modemtunnel
uitgang
```

Naar

```
crypto ipsec ikev1
transformatieset AWS esp-a
esp-sha-hmac
```

Stap 3.

crypto ipsec-profiel voor crypto ipsec-profiel . Er is slechts één profiel nodig omdat de twee profielen identiek zijn.

Aanbevolen configuratie

```
crypto ipsec-profiel ipsec-vpn-7c79606e-0
  pfs-groep2 instellen
  Stel security-associatie levensduur
seconden in 3600
  set transformatie-set ipsec-prop-vpn-
7c79606e-0
uitgang
crypto ipsec-profiel ipsec-vpn-7c79606e-1
  pfs-groep2 instellen
  Stel security-associatie levensduur
seconden in 3600
  set transformatie-set ipsec-prop-vpn-
7c7960e-1
uitgang
```

Naar

```
cryptografische IPsec-profiel AWS
ingesteld jevl transformatie-set
pfs-groep2 instellen
Stel security-associatie levensduur
seconden in 3600
```

Stap 4.

crypto sleutelring en crypto isakmp profiel moeten worden geconverteerd naar een tunnelgroep voor elke tunnel.

Aanbevolen configuratie

```
sleutelring-vpn-7c79606e-0
  plaatselijk adres 64.10.251.37
  Vooraf gedeeld adres 52.34.205.227-toets QZh90Bjf
uitgang
!
crypto-isakmp-profiel isakmp-vpn-7c79606e-0
  plaatselijk adres 64.10.251.37
  matchadres 52.34.205.227
```

Naar

```
tunnelgroep 52.34.205
type ipsec-l2l
tunnelgroep 52.34.205
ipsec-eigenschappen
ikev1 pre-gedeeld-ke
QZh90Bjf
isakmp behoudt dremp
10 opnieuw proberen 1
```

```

sleutelring-VPN-7c79606e-0
uitgang
!
sleutelring-vpn-7c79606e-1
plaatselijk adres 64.10.251.37
pre-Shared Key Address 52.37.194.219
uitgang
!
crypto-isakmp-profiel isakmp-vpn-7c79606e-1
plaatselijk adres 64.10.251.37
matchadres 52.37.194.219
sleutelring-VPN-7c79606e-1
uitgang
tunnelgroep 52.37.194
type ipsec-l2l
tunnelgroep 52.37.194
eigenschappen van ipsec
ikev1 pre-gedeeld-ke
JxCWy4Ae
isakmp behoudt drempel
10 opnieuw proberen 1

```

Stap 5.

De tunnelconfiguratie is bijna identiek. De ASA ondersteunt de IP-aangepaste mss of de IP virtuele-herassembleren opdracht niet.

Aanbevolen configuratie

```

interface-tunnelleiding1
ip-adres 169.254.13.190 255.255.255.252
IP-virtuele reassemblering
tunnelbron 64.10.251.37
tunnelbestemming 52.34.205.227
tunnelmodus ipsec ipv4
ipsec-profiel voor tunnelbescherming ipsec-vpn-
7c79606e-0
IP TCP-aanpassing-MS 1387
geen sluiting
uitgang
!
interface-tunnel2
ip-adres 169.254.12.86 255.255.255.252
IP-virtuele reassemblering
tunnelbron 64.10.251.37
tunnelbestemming 52.37.194.219
tunnelmodus ipsec ipv4
ipsec-profiel voor tunnelbescherming ipsec-vpn-
7c79606e-1
IP TCP-aanpassing-MS 1387
geen sluiting
uitgang

```

Naar

```

interface-tunnelleiding1
Naam van AWS1
ip-adres 169.254.13.190
255.255.255.252
tunnelbroninterface buiten
tunnelbestemming 52.34.205.2
tunnelmodus ipsec ipv4
tunnelbeveiligingsprofiel AW
!
interface-tunnel2
Naam van AWS2
ip-adres 169.254.12.86
255.255.255.252
tunnelbroninterface buiten
tunnelbestemming 52.37.194.2
tunnelmodus ipsec ipv4
tunnelbeveiligingsprofiel AW

```

Stap 6.

In dit voorbeeld, zal ASA slechts binnen Subnet (192.168.1.0/24) adverteren en het subnet binnen AWS (172.31.0.0/16) ontvangen.

Aanbevolen configuratie

```

router bgp 6500
buurman
169.254.13.189
afstandsbediening

```

Naar

```

router bgp 6500
bgp-logbestand-buurland-veranderingen
timers bgp 10 30 0
adresfamilie ipv4 unicast

```

```
7224
  buurman
169.254.13.189 in
werking
  buurman
169.254.13.189
timers 10 30 30
  adresfamilie ipv4
unicast
  buurman
169.254.13.189
afstandsbediening
7224
  buurman
169.254.13.189
timers 10 30 30
  buurman
169.254.13.189
standaard-originate
  buurman
169.254.13.189 in
werking
  buurman          buurman 169.254.12.85 afgelegen-as
169.254.13.189    7224
zachte configuratie buurman 169.254.12.85 actief
inwaarts          buurman 169.254.13.189
  netwerk 0.0.0.0  afstandsbediening 7224
  uitgang          buurman 169.254.13.189 in werking
uitgang           netwerk 192.168.1.0
router bgp 6500   geen auto-samenvatting
  buurman         geen synchronisatie
169.254.12.85    exit-adresfamilie
afgelegen-as 7224
  buurman
169.254.12.85
actief
  buurman
169.254.12.85
timers 10 30 30
  adresfamilie ipv4
unicast
  buurman
169.254.12.85
afgelegen-as 7224
  buurman
169.254.12.85
timers 10 30 30
  buurman
169.254.12.85
standaard-originate
  buurman
169.254.12.85
actief
```

```
buurman
169.254.12.85
zachte
reconfiguratie
binnenkomend
  netwerk 0.0.0.0
  uitgang
uitgang
```

Verifiëren en optimaliseren

Stap 1.

Bevestig de ASA de IKEv1-beveiligingsassociaties met de twee eindpunten bij AWS. De staat van de SA zou MM_ACTIVE moeten zijn.

```
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#
```

Stap 2.

Bevestig dat de IPsec SAs op ASA zijn geïnstalleerd. Er moet voor elke peer een inkomende en uitgaande SPI zijn geïnstalleerd en er moeten een aantal plafonds en decaps tellers zijn.

```
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

```

Stap 3.

Bevestig op de ASA dat BGP-verbindingen met AWS tot stand zijn gebracht. De State/PfxRCD teller moet 1 zijn aangezien AWS adverteert met 172.31.0.0/16 subster naar de ASA.

```
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

Stap 4.

Controleer op de ASA of de route naar 172.31.0.0/16 is geleerd via de tunnelinterfaces. Deze output laat zien dat er twee paden zijn naar 172.31.0.0 van peer 169.254.12.85 en 169.254.13.189. Het pad naar 169.254.13.189 out Tunnel 2 (AWS2) liever vanwege de lagere metriek.

```
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
```

Step 5.

Om ervoor te zorgen dat het verkeer dat van AWS terugkeert een symmetrisch pad volgt, moet u een route-map configureren om het voorkeurspad aan te passen en BGP aanpassen om de geadverteerde routes te wijzigen.

```
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
```

Step 6.

Bevestig op de ASA dat 192.168.1.0/24 aan AWS wordt geadverteerd.

```
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

Step 7.

In AWS, bevestig dat de tunnels voor de VPN verbinding UP zijn en de routes van de peer worden geleerd. Controleer ook dat de route in de routingtabel is verspreid.

The screenshot shows the AWS VPN Connections console. The main table lists VPN connections, with 'VPNtoASA' selected. Below, the 'Tunnel Details' tab is active, showing a table of tunnels. Two tunnels are listed, both with a status of 'UP'. Red circles highlight the 'UP' status and the '1 BGP ROUTES' detail for both tunnels.

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	52.37.194.218	UP	2016-10-18 14:23 UTC	1 BGP ROUTES

The screenshot shows the AWS Route Tables console. The main table lists route tables, with 'rtb-3a3f9e5d' selected. Below, the 'Routes' tab is active, showing a table of routes. The route for destination '192.168.1.0/24' is highlighted with a red circle, showing it is 'Active' and 'Propagated'.

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-e5ad1481	Active	No
192.168.1.0/24	vgw-18954d06	Active	Yes