Configuración de ASA IPsec VTI Connection Amazon Web Services

Contenido

Introducción

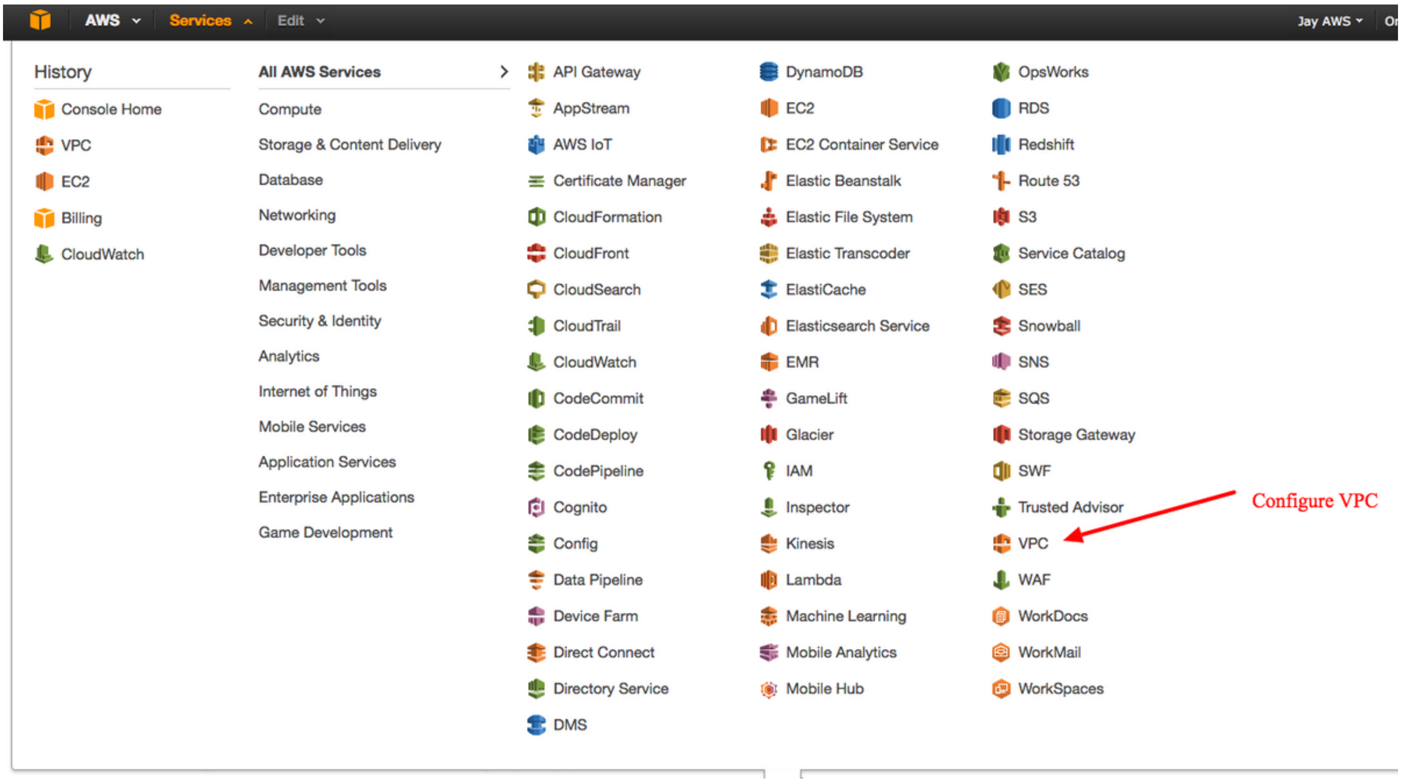
Este documento describe cómo configurar una conexión de interfaz de túnel virtual (VTI) IPsec de Adaptive Security Appliance (ASA). En ASA 9.7.1, se ha introducido IPsec VTI. Se limita a sVTI IPv4 sobre IPv4 con IKEv1 en esta versión. Este es un ejemplo de configuración para que ASA se conecte a Amazon Web Services (AWS).

> **Nota:** Actualmente, VTI sólo se admite en modo de routing de contexto único.

Configurar AWS

Paso 1.

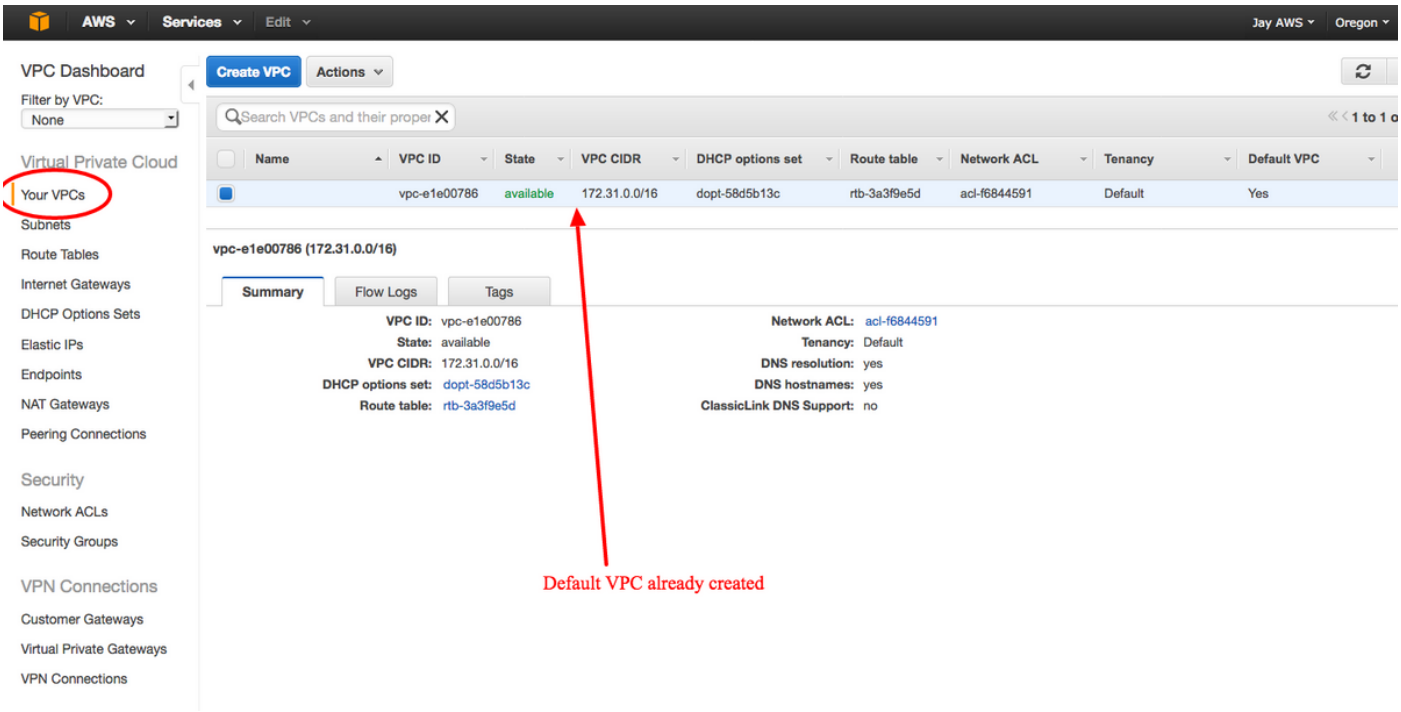
Inicie sesión en la consola AWS y navegue hasta el panel VPC.



Vaya al panel de VPC

Paso 2.

Confirme que ya se ha creado una nube privada virtual (VPC). De forma predeterminada, se crea un VPC con 172.31.0.0/16. Aquí es donde se conectarán las máquinas virtuales (VM).



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

vpc-e1e00786 (172.31.0.0/16)

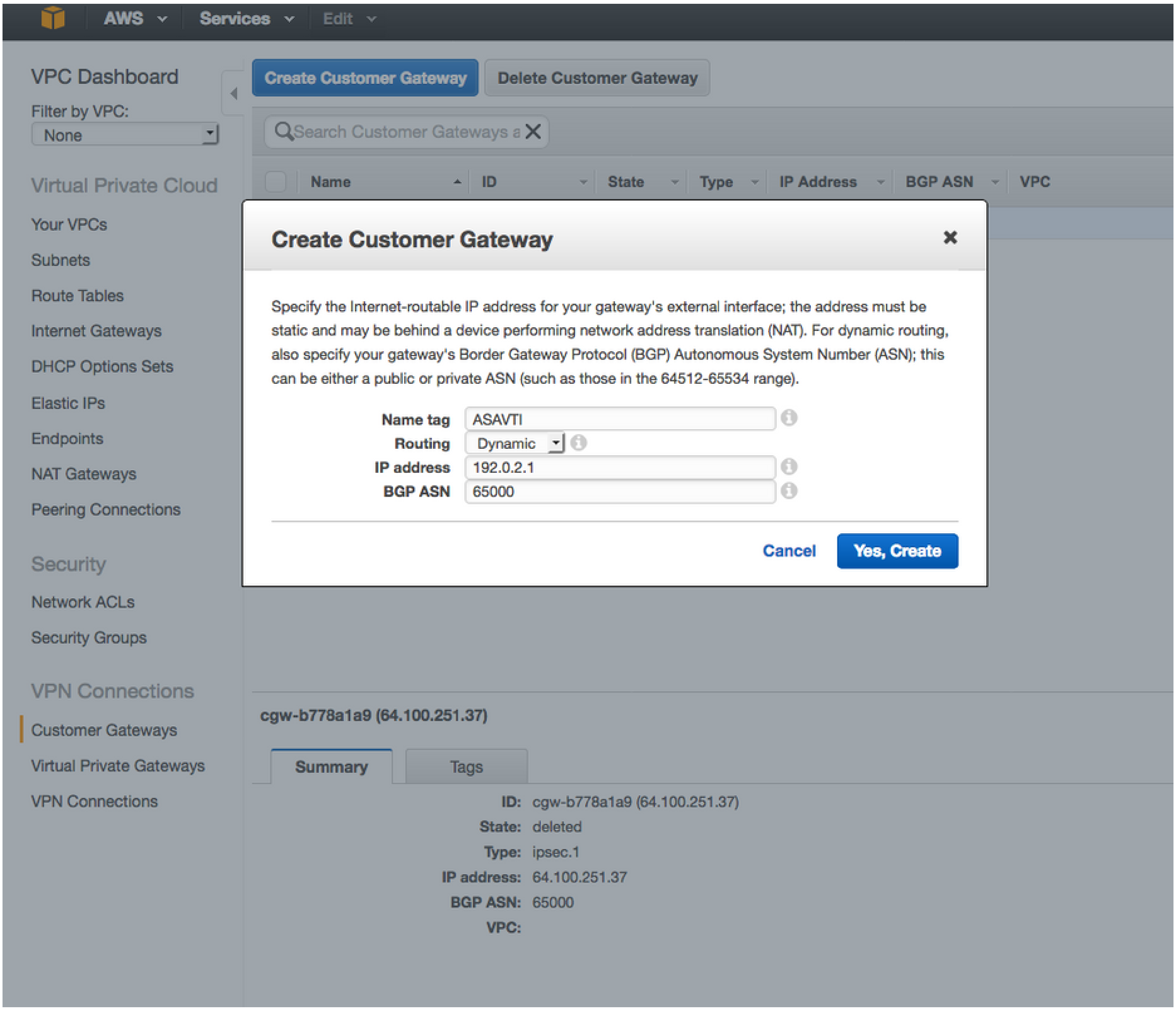
VPC ID:	vpc-e1e00786	Network ACL:	acl-f6844591
State:	available	Tenancy:	Default
VPC CIDR:	172.31.0.0/16	DNS resolution:	yes
DHCP options set:	dopt-58d5b13c	DNS hostnames:	yes
Route table:	rtb-3a3f9e5d	ClassicLink DNS Support:	no

Default VPC already created

Paso 3.

Cree una "puerta de enlace del cliente". Se trata de un terminal que representa el ASA.

Campo	Valor
Etiqueta de nombre	Este es solo un nombre legible para las personas para reconocer el ASA.
Ruteo	Dinámico: esto significa que se utilizará el protocolo de gateway fronterizo (BGP) para intercambiar información de routing.
IP Address	Ésta es la dirección IP pública de la interfaz exterior del ASA.
ASN de BGP	El número del sistema autónomo (AS) del proceso BGP que se ejecuta en el ASA. Utilice 65 menos que su organización tenga un número AS público.



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

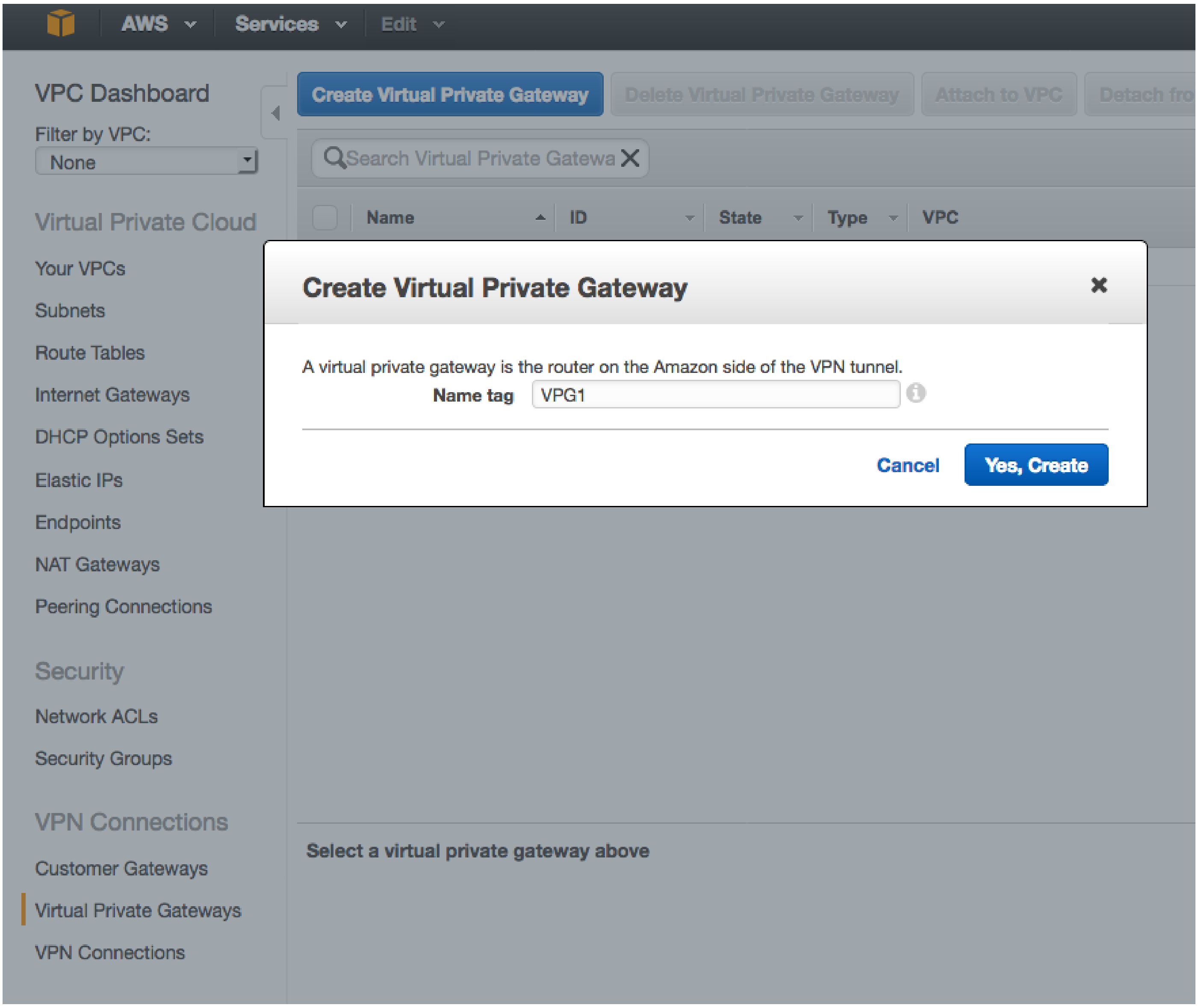
cgw-b778a1a9 (64.100.251.37)

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

Paso 4.

Cree un Virtual Private Gateway (VPG). Este es un router simulado que se aloja con AWS que termina el túnel IPsec.

Campo	**Valor**
Etiqueta de nombre	Un nombre legible por personas para reconocer el VPG.



Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

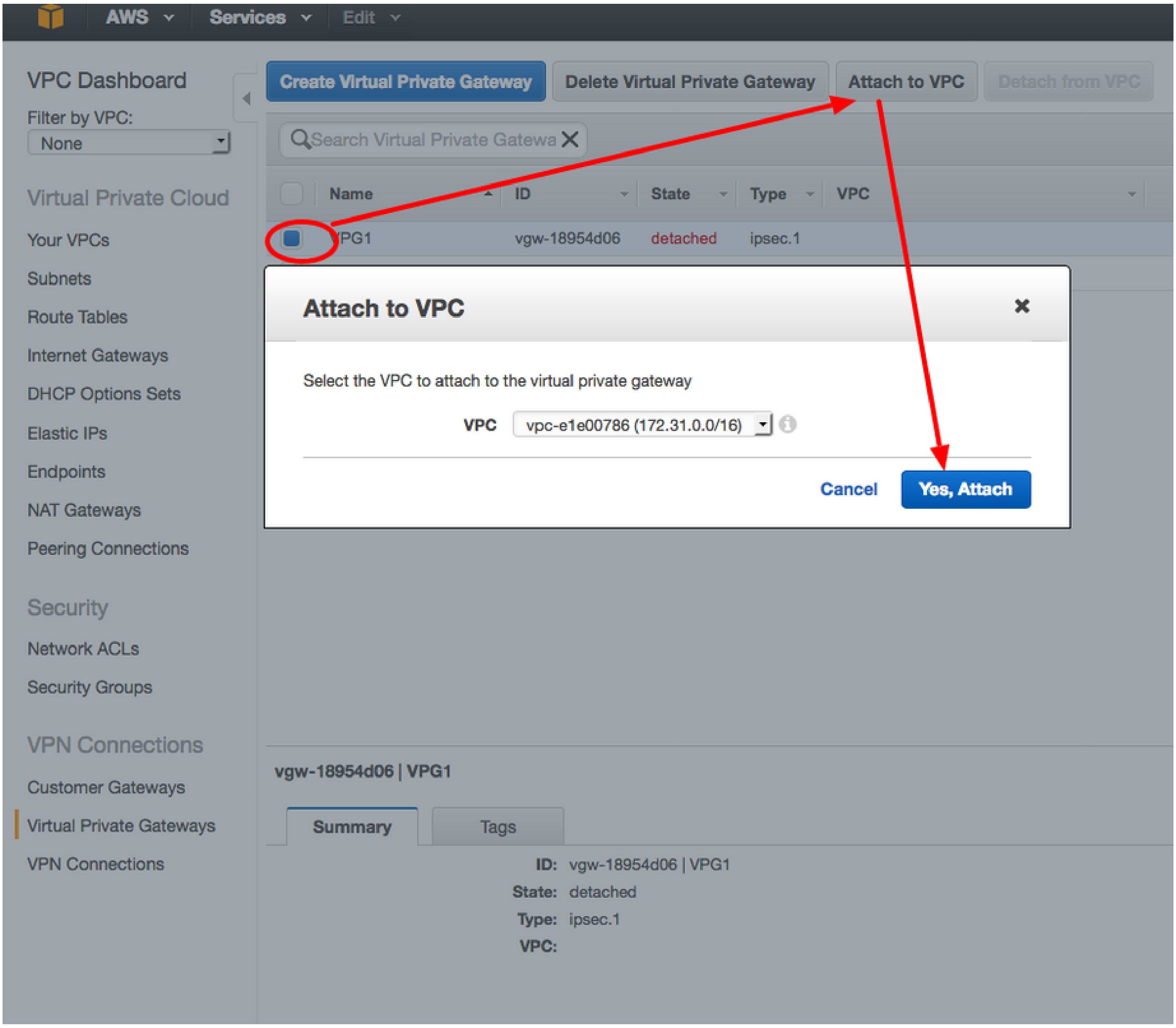
Name tag: VPG1

Select a virtual private gateway above

Paso 5.

Conecte el VPG al VPC.

Elija Virtual Private Gateway, haga clic en **Adjuntar a VPC**, elija el VPC de la lista desplegable VPC y haga clic en **Sí, Adjuntar**.



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

Attach to VPC

Select the VPC to attach to the virtual private gateway

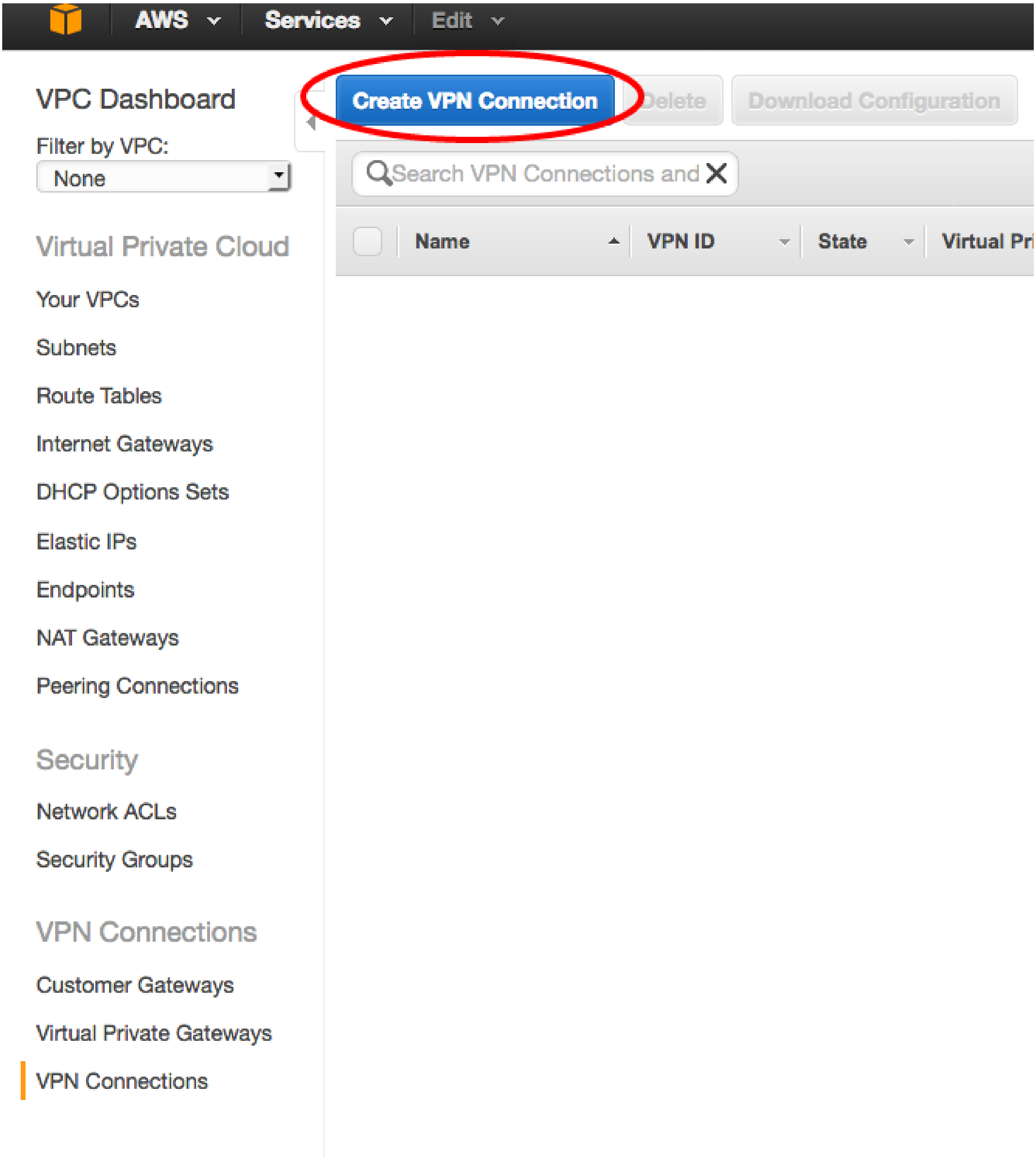
VPC: vpc-e1e00786 (172.31.0.0/16)

vgw-18954d06 | VPG1

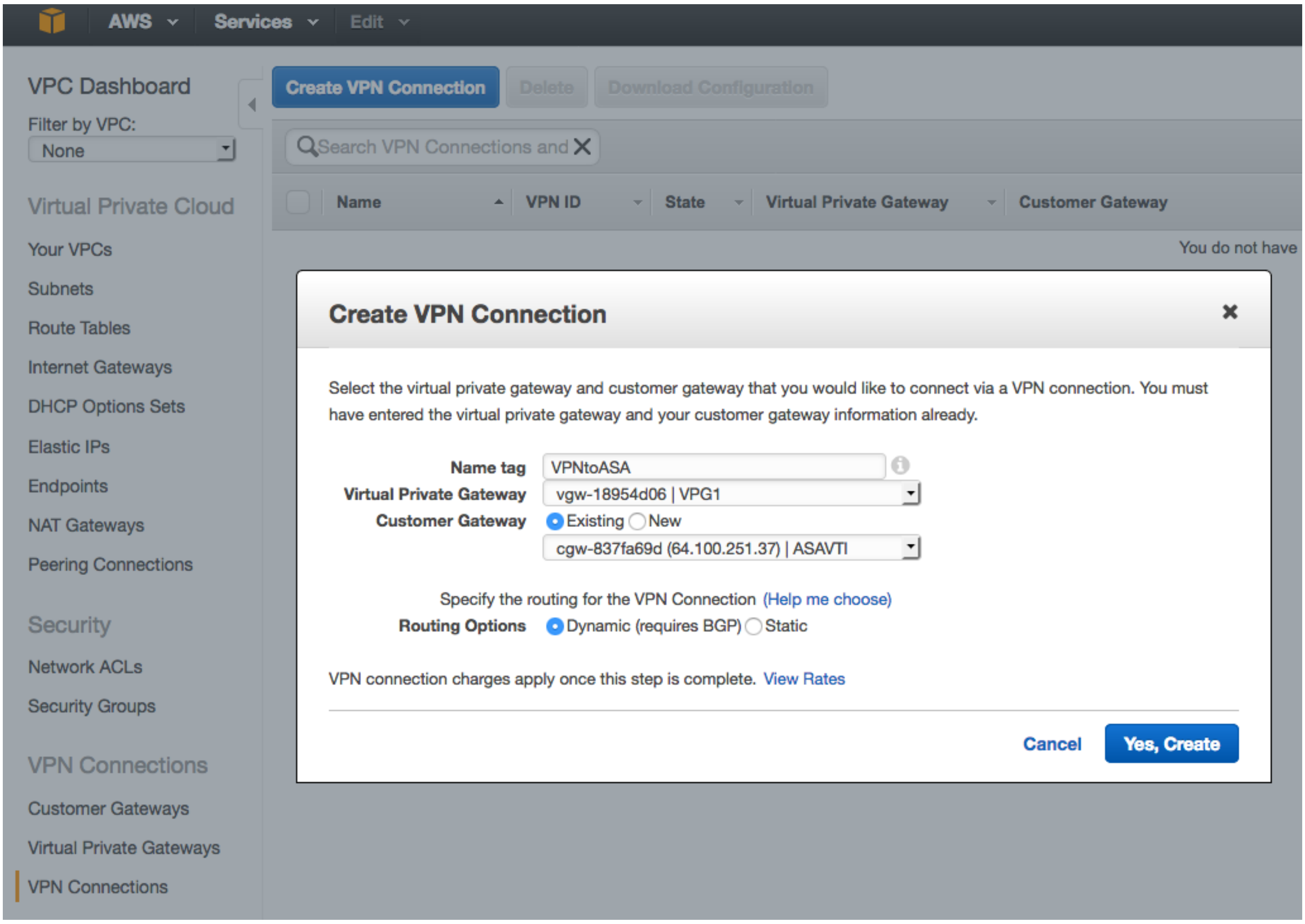
ID: vgw-18954d06 | VPG1
State: detached
Type: ipsec.1
VPC:

Paso 6.

Cree una conexión VPN.



Campo	Valor
Etiqueta de nombre	Una etiqueta legible por personas de la conexión VPN entre AWS y ASA.
Gateway privada virtual	Elija el VPG recién creado.
Gateway del cliente	Haga clic en el botón de opción **Existente** y elija el gateway del ASA.
Opciones de routing	Haga clic en el botón de opción **Dynamic (require BGP)**.



Create VPN Connection

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.

Name tag VPNtoASA

Virtual Private Gateway vgw-18954d06 | VPG1

Customer Gateway ● Existing ○ New

cgw-837fa69d (64.100.251.37) | ASAVTI

Specify the routing for the VPN Connection (Help me choose)

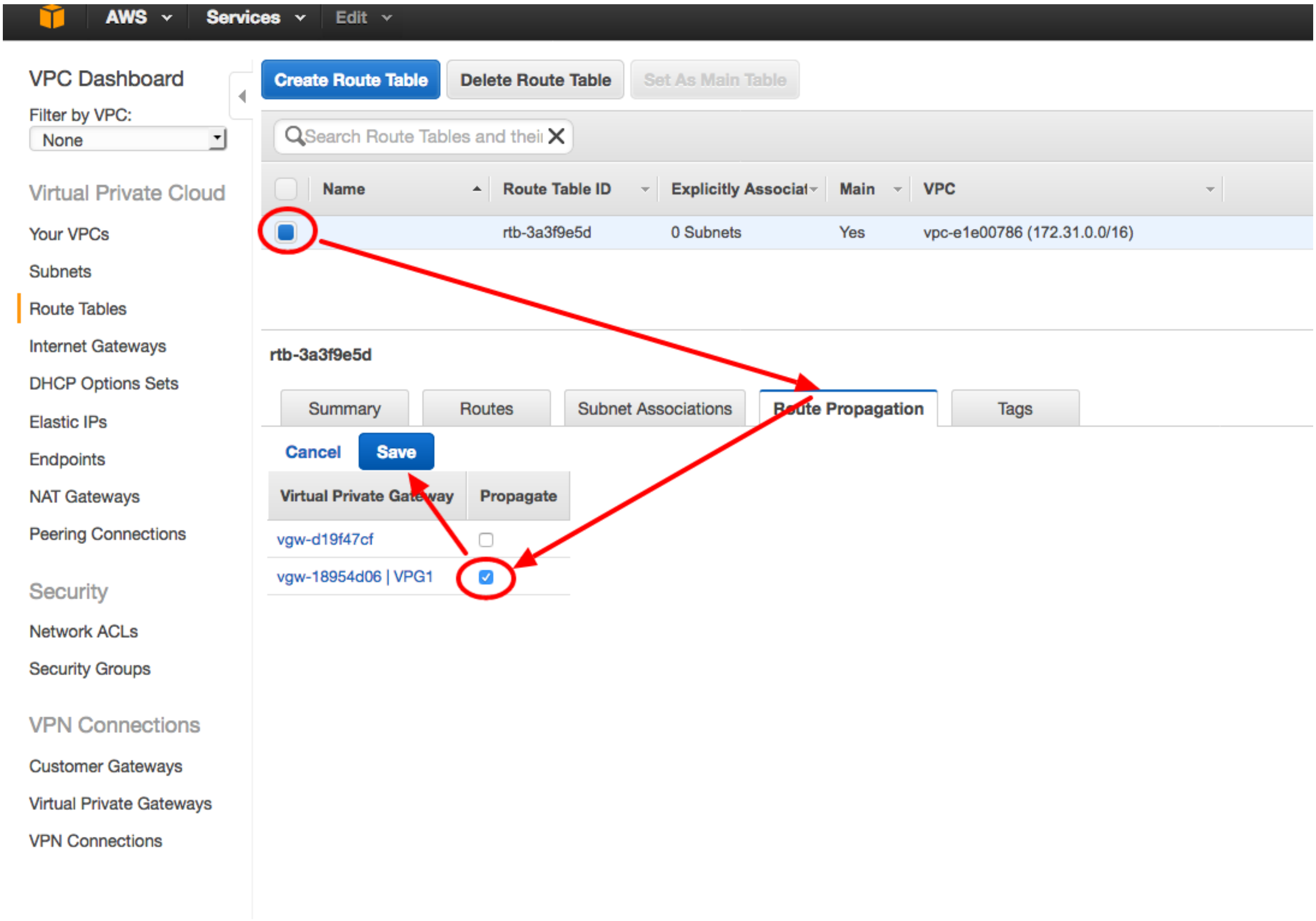
Routing Options ● Dynamic (requires BGP) ○ Static

VPN connection charges apply once this step is complete. View Rates

Cancel **Yes, Create**

Paso 7.

Configure la Tabla de Ruta para propagar las rutas aprendidas de VPG (a través de BGP) en el VPC.



	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-3a3f9e5d	0 Subnets	Yes	vpc-e1e00786 (172.31.0.0/16)

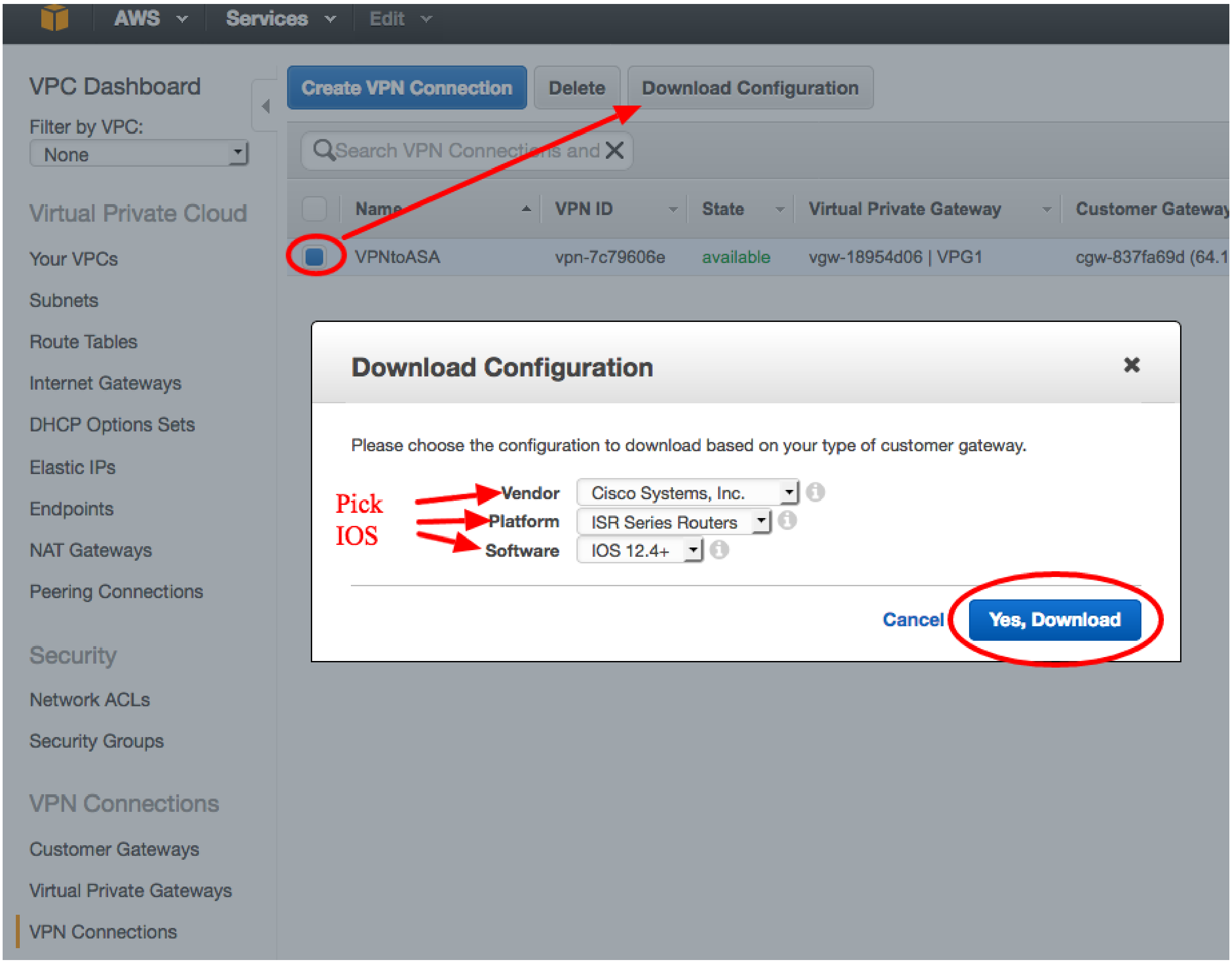
rtb-3a3f9e5d

Virtual Private Gateway	Propagate
vgw-d19f47cf	□
vgw-18954d06 | VPG1	☑

Paso 8.

Descargue la configuración sugerida. Elija los siguientes valores para generar una configuración que sea un estilo VTI.

Campo	Valor
Proveedor	Cisco Systems, Inc.
Platform	Routers de la serie ISR
Software	IOS 12.4+



Name	VPN ID	State	Virtual Private Gateway	Customer Gateway
VPNtoASA	vpn-7c79606e	available	vgw-18954d06 | VPG1	cgw-837fa69d (64.1

Download Configuration

Please choose the configuration to download based on your type of customer gateway.

Vendor: Cisco Systems, Inc.

Platform: ISR Series Routers

Software: IOS 12.4+

Configuración del ASA

Una vez descargada la configuración, es necesaria alguna conversión.

Paso 1.

crypto isakmp policy to crypto ikev1 policy. Sólo se necesita una política, ya que la política 200 y la política 201 son idénticas.

Configuración sugerida

```
crypto isakmp policy 200
 encryption aes 128
 authentication pre-share
 grupo 2
 lifetime 28800
 hash sha
salir
crypto isakmp policy 201
 encryption aes 128
 authentication pre-share
 grupo 2
```

A

```
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 grupo 2
 lifetime 28800
 lifetime 28800
 hash sha
salir
```

Paso 2.

crypto ipsec transform-set to crypto ipsec ikev1 transform-set. Sólo se necesita un conjunto de transformación, ya que los dos conjuntos de transformación son idénticos.

Configuración sugerida

```
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-
0 esp-aes 128 esp-sha-hmac
  túnel de modo
salir
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-
1 esp-aes 128 esp-sha-hmac
  túnel de modo
salir
```

A

```
crypto ipsec ikev1 transfo
set AWS esp-aes esp-sha-hm
```

Paso 3.

crypto ipsec profile to crypto ipsec profile. Sólo se necesita un perfil, ya que ambos son idénticos.

Configuración sugerida

```
crypto ipsec profile ipsec-vpn-7c79606e-0
 set pfs group2
 set security-association lifetime seconds
3600
 set transform-set ipsec-prop-vpn-7c79606e-0
salir
crypto ipsec profile ipsec-vpn-7c79606e-1
 set pfs group2
 set security-association lifetime seconds
3600
 set transform-set ipsec-prop-vpn-7c79606e-1
salir
```

A

```
crypto ipsec profile AWS
 set ikev1 transform-set AWS
 set pfs group2
 set security-association life
seconds 3600
```

Paso 4.

crypto keyring y crypto isakmp profile deben convertirse en un grupo de túnel para cada túnel.

Configuración sugerida

```
crypto keyring keyring-vpn-7c79606e-0
 local-address 64.100.251.37
 clave precompartida 52.34.205.227 clave QZhh90Bjf
salir
!
crypto isakmp profile isakmp-vpn-7c79606e-0
 local-address 64.100.251.37
 match identity address 52.34.205.227
 llavero de llenado de teclado vpn-7c79606e-0
 salir
!
crypto keyring keyring-vpn-7c79606e-1
```

A

```
tunnel-group
52.34.205.227 type ip
l2l
tunnel-group
52.34.205.227 ipsec-
atributos
 ikev1 clave previame
compartida QZhh90Bjf
 isakmp keepalive
threshold 10 retry 10
tunnel-group
52.37.194.219 type ip
```

```
 local-address 64.100.251.37
 dirección de clave previamente compartida 52.37.194.219
clave JjxCWy4Ae
 salir
!
crypto isakmp profile isakmp-vpn-7c79606e-1
 local-address 64.100.251.37
 match identity address 52.37.194.219
 llavero de llenado de teclado vpn-7c79606e-1
 salir
```

```
l2l
tunnel-group
52.37.194.219 ipsec-
atributos
 ikev1 clave previame
compartida JjxCWy4Ae
 isakmp keepalive
threshold 10 retry 10
```

Paso 5.

La configuración del túnel es casi idéntica. El ASA no soporta el comando ip tcp adjust-mss o el comando ip virtual-reassembly.

Configuración sugerida

```
interface Tunnel1
 ip address 169.254.13.190 255.255.255.252
 ip virtual-reassembly
 tunnel source 64.100.251.37
 tunnel destination 52.34.205.227
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-vpn-
7c79606e-0
 ip tcp adjust-mss 1387
 no shutdown
 salir
!
interface Tunnel2
 ip address 169.254.12.86 255.255.255.252
 ip virtual-reassembly
 tunnel source 64.100.251.37
 tunnel destination 52.37.194.219
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-vpn-
7c79606e-1
 ip tcp adjust-mss 1387
 no shutdown
 salir
```

A

```

interface Tunnel1
 nameif AWS1
 ip address 169.254.13.190
255.255.255.252
 interfaz de origen de túnel
externa
 tunnel destination 52.34.205.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profil
AWS
!
interface Tunnel2
 nameif AWS2
 ip address 169.254.12.86
255.255.255.252
 interfaz de origen de túnel
externa
 tunnel destination 52.37.194.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profil
AWS
```

Paso 6.

En este ejemplo, el ASA sólo anunciará la subred interna (192.168.1.0/24) y recibirá la subred dentro de AWS (172.31.0.0/16).

Configuración sugerida

```
router bgp 65000
 neighbor 169.254.13.189 remote-as 7224
 neighbor 169.254.13.189 active
 neighbor 169.254.13.189 timers 10 30 30
 address-family ipv4 unicast
  neighbor 169.254.13.189 remote-as 7224
  neighbor 169.254.13.189 timers 10 30 30
```

A

```
router bgp 65000
 bgp log-neighbor-changes
 timers bgp 10 30 0
 address-family ipv4 unica
  neighbor 169.254.12.85
remote-as 7224
  neighbor 169.254.12.85
  neighbor 169.254.13.189 default-originate
  neighbor 169.254.13.189 active
  neighbor 169.254.13.189 soft-reconfiguration
inbound
  network 0.0.0.0
  salir
 salir
router bgp 65000
 neighbor 169.254.12.85 remote-as 7224
 neighbor 169.254.12.85 active
 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 active
  neighbor 169.254.12.85 soft-reconfiguration
inbound
  network 0.0.0.0
  salir
 salir
```

```
active
  neighbor 169.254.13.189
remote-as 7224
  neighbor 169.254.13.189
active
  network 192.168.1.0
  no auto-summary
  sin sincronización
 exit-address-family
```

Verificar y optimizar

Paso 1.

Confirme que ASA establezca las asociaciones de seguridad IKEv1 con los dos terminales en AWS. El estado de SA debe ser MM_ACTIVE.

```
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#
```

Paso 2.

Confirme que las SA IPsec estén instaladas en ASA. Debe haber un SPI entrante y saliente instalado para cada peer y debe haber algunos contadores encaps y decaps incrementándose.

```
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
```

Paso 3.

En el ASA, confirme que las conexiones BGP se establecen con AWS. El contador State/PfxRcd debe ser 1, ya que AWS anuncia la subred 172.31.0.0/16 hacia el 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
```

Paso 4.

En el ASA, verifique que la ruta a 172.31.0.0/16 se haya aprendido a través de las interfaces de túnel. Esta salida muestra que hay dos trayectorias a 172.31.0.0 del par 169.254.12.85 y 169.254.13.189. Se prefiere la ruta hacia el túnel 169.254.13.189 de salida 2 (AWS2) debido a la métrica más baja.

```
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
```

Paso 5.

Para asegurar que el tráfico que regresa de AWS siga un trayecto simétrico, configure un route-map para que coincida con el trayecto preferido y ajuste el BGP para alterar las rutas anunciadas.

```
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
```

Paso 6.

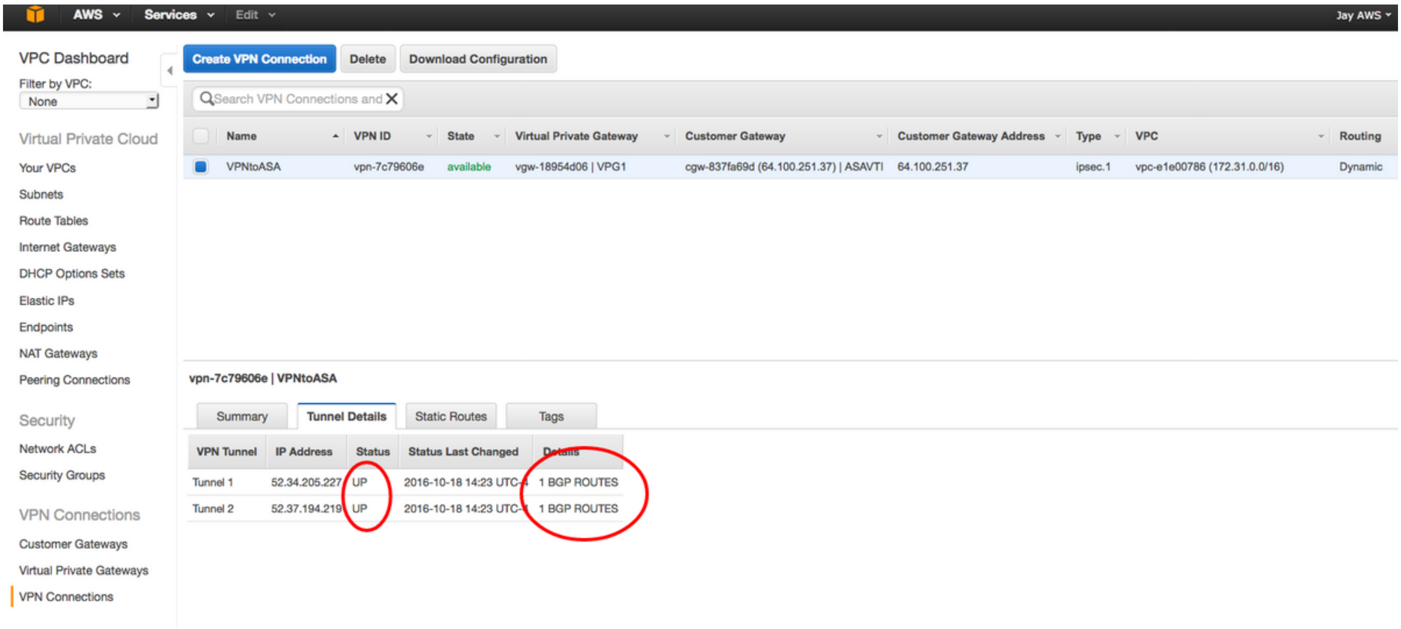
En el ASA, confirme que 192.168.1.0/24 se anuncia a AWS.

```
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
```

Paso 7.

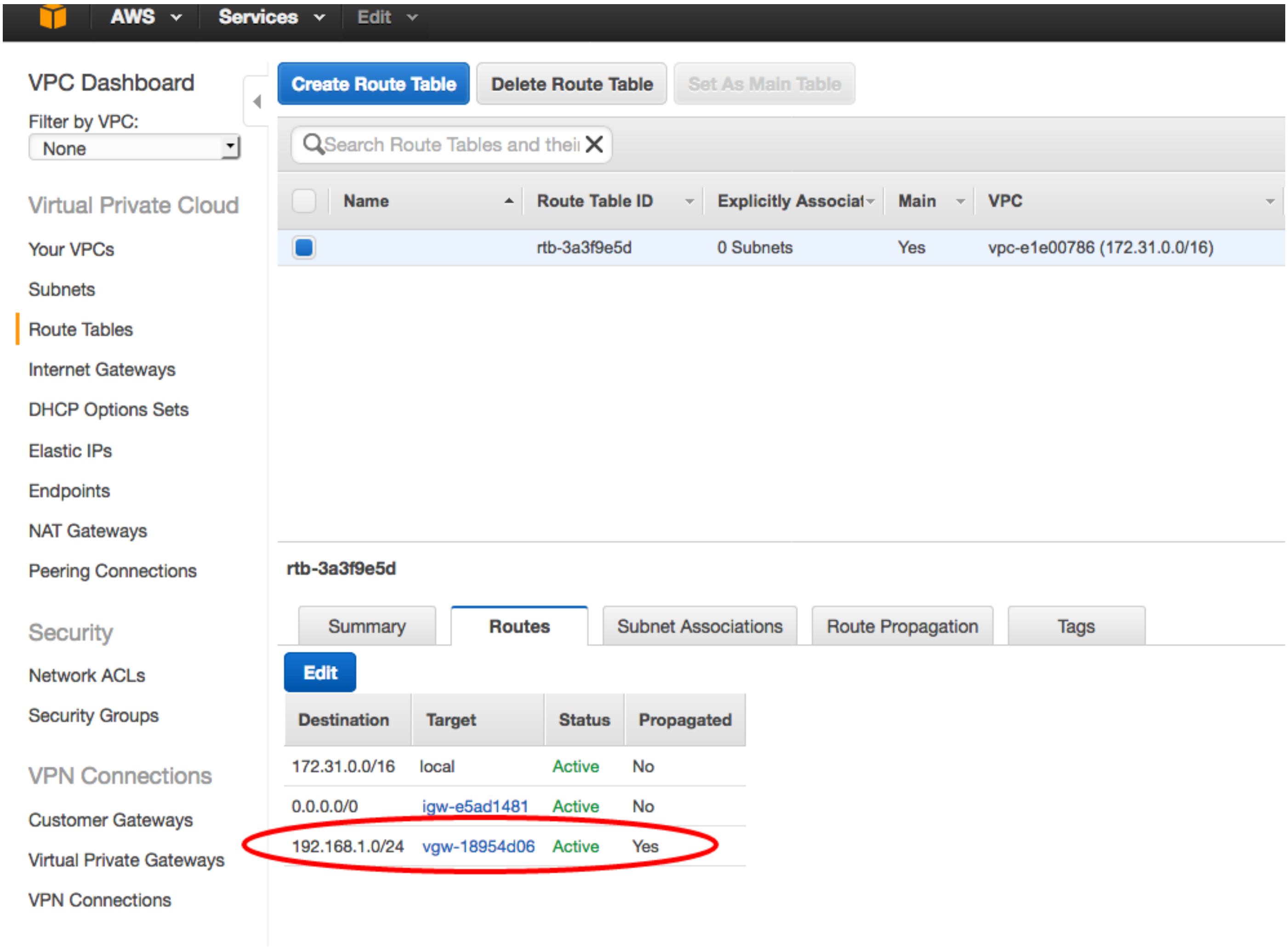
En AWS, confirme que los túneles para la conexión VPN estén ACTIVOS y que las rutas se aprendan del par. Verifique también que la ruta se haya propagado a la tabla de ruteo.



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	ipsec.1	vpc-e1e00786 (172.31.0.0/16)	Dynamic

vpn-7c79606e | VPNtoASA

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	52.34.205.227	UP	2016-10-18 14:23 UTC-4	1 BGP ROUTES
Tunnel 2	52.37.194.219	UP	2016-10-18 14:23 UTC-4	1 BGP ROUTES



Filter by VPC: None

	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-3a3f9e5d	0 Subnets	Yes	vpc-e1e00786 (172.31.0.0/16)

rtb-3a3f9e5d

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