Configurar os serviços da Web da Amazon de conexão VTI do ASA IPsec

Contents

Introduction

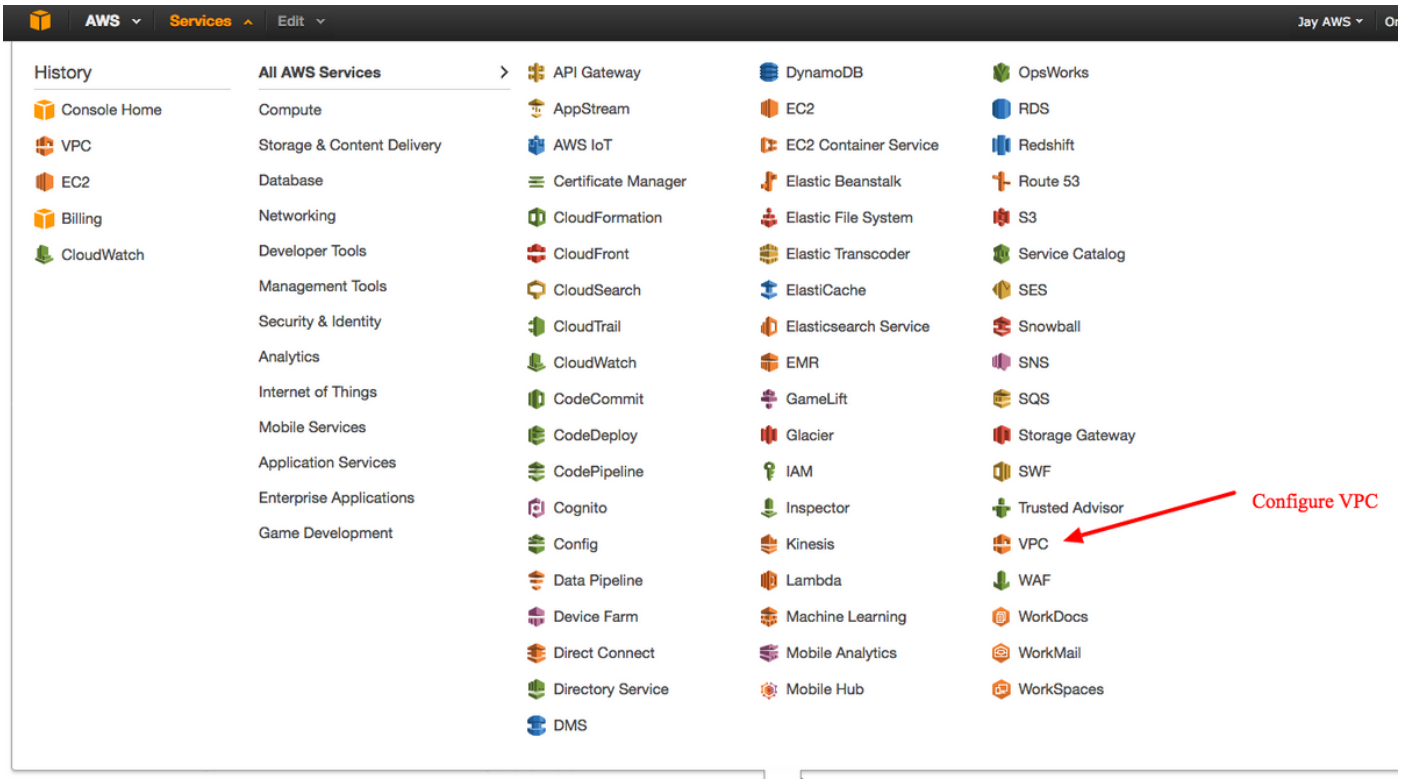
Este documento descreve como configurar uma conexão de Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) IPsec do Adaptive Security Appliance (ASA). No ASA 9.7.1, o IPsec VTI foi apresentado. Ela é limitada ao sVTI IPv4 sobre IPv4 usando IKEv1 nesta versão. Este é um exemplo de configuração para que o ASA se conecte aos Serviços Web da Amazon (AWS).

> **Note**: Atualmente, o VTI só é suportado no modo roteado e de contexto único.

Configurar AWS

Etapa 1.

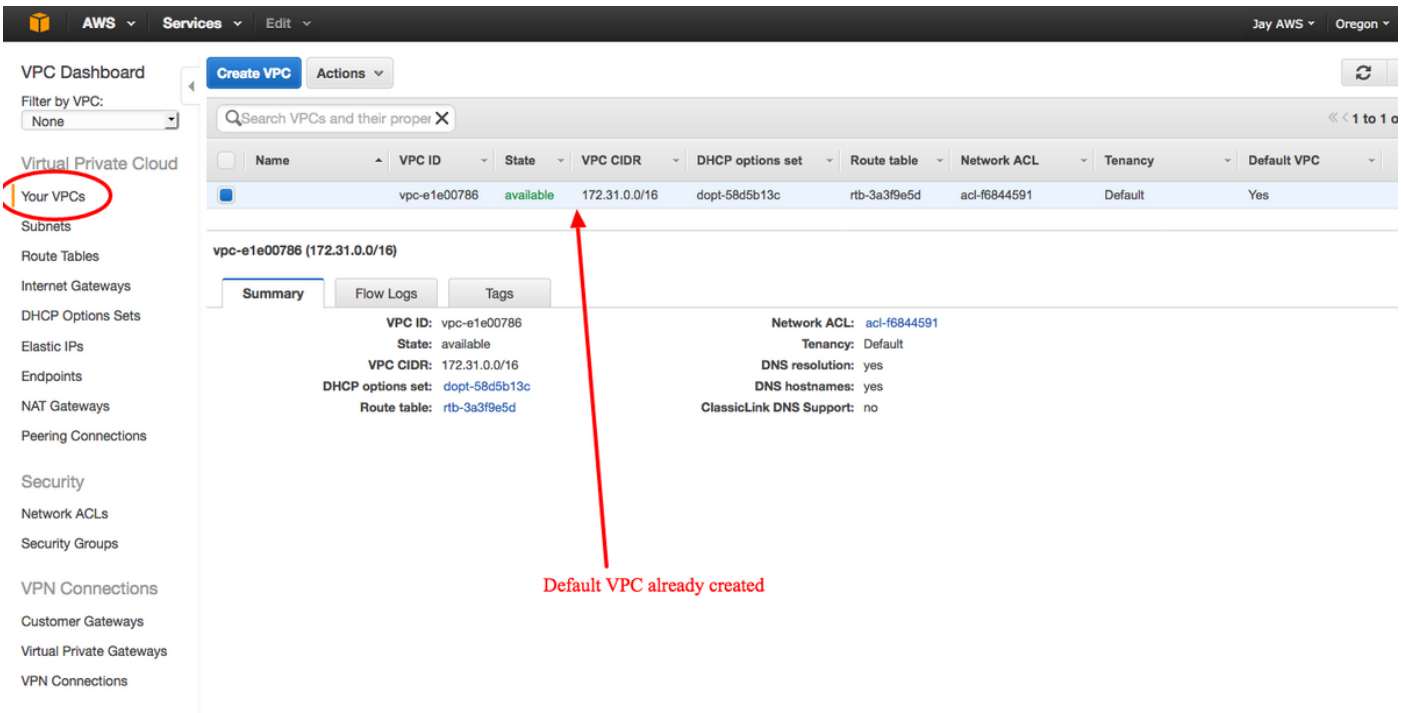
Faça login no console AWS e navegue até o painel VPC.



Navegue até o Painel do VPC

Etapa 2.

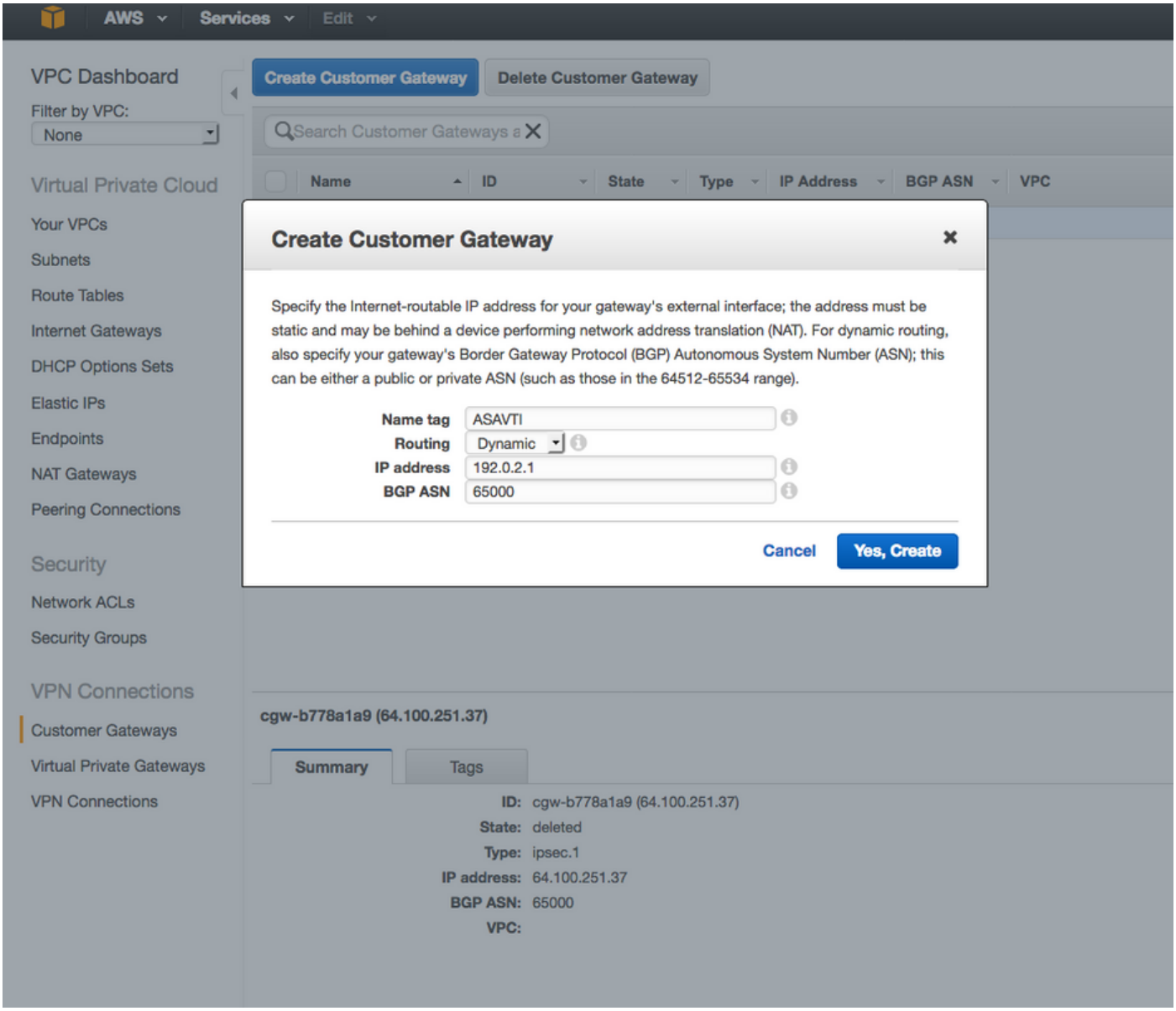
Confirme se uma nuvem privada virtual (VPC) já foi criada. Por padrão, um VPC com 172.31.0.0/16 é criado. É aqui que as máquinas virtuais (VMs) serão anexadas.



Etapa 3.

Crie um "Gateway do cliente". Este é um endpoint que representa o ASA.

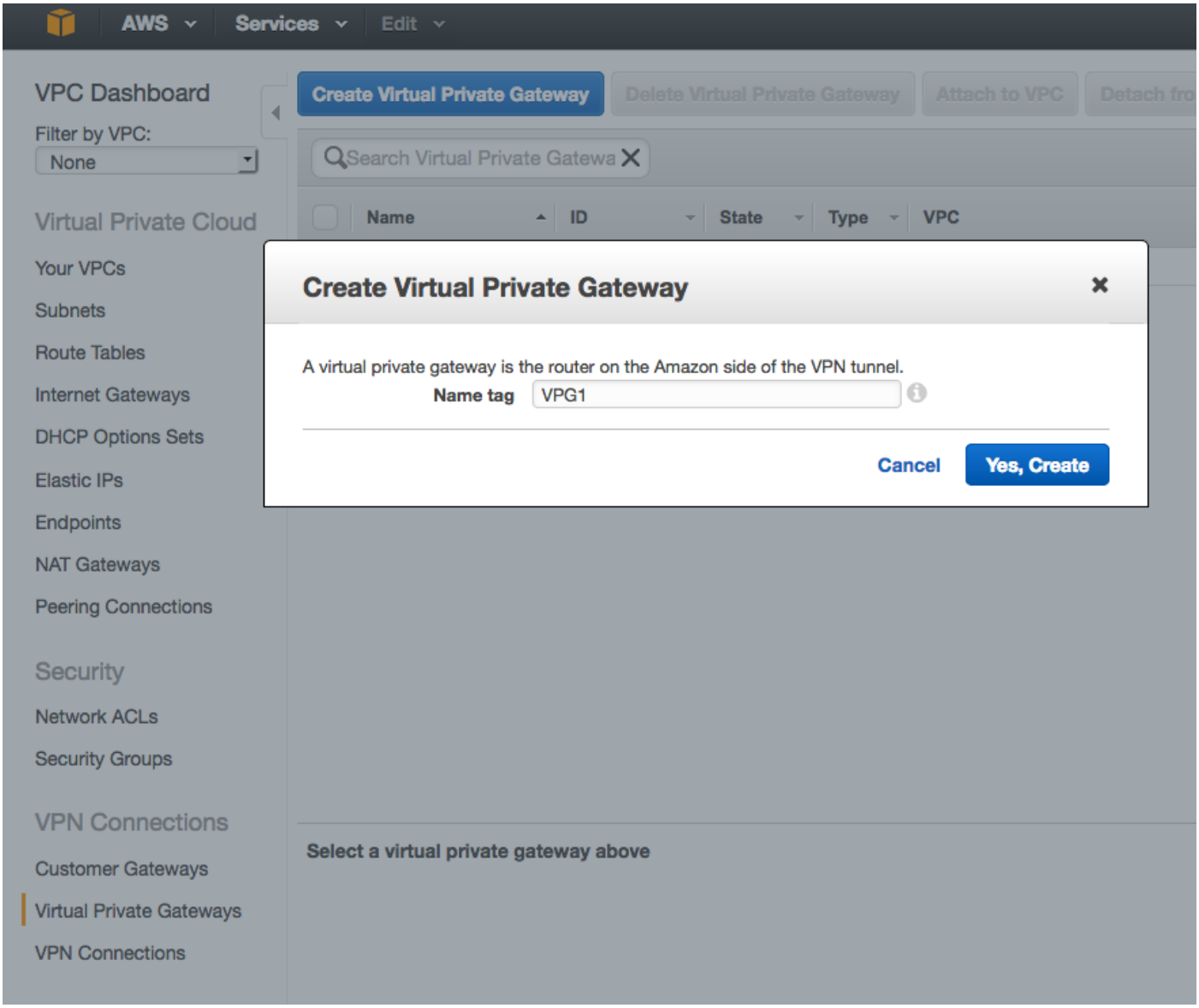
Campo	Valor
Etiqueta de nome	Este é apenas um nome legível por humanos para reconhecer o ASA.
Roteamento	Dinâmico - Isso significa que o Border Gateway Protocol (BGP) será usado para trocar informações de roteamento.
IP Address	Esse é o endereço IP público da interface externa do ASA.
BGP ASN	O número do sistema autônomo (AS) do processo BGP que é executado no ASA. Use 6500 a menos que sua empresa tenha um número AS público.



Etapa 4.

Crie um Virtual Private Gateway (VPG). Este é um roteador simulado hospedado com AWS que termina o túnel IPsec.

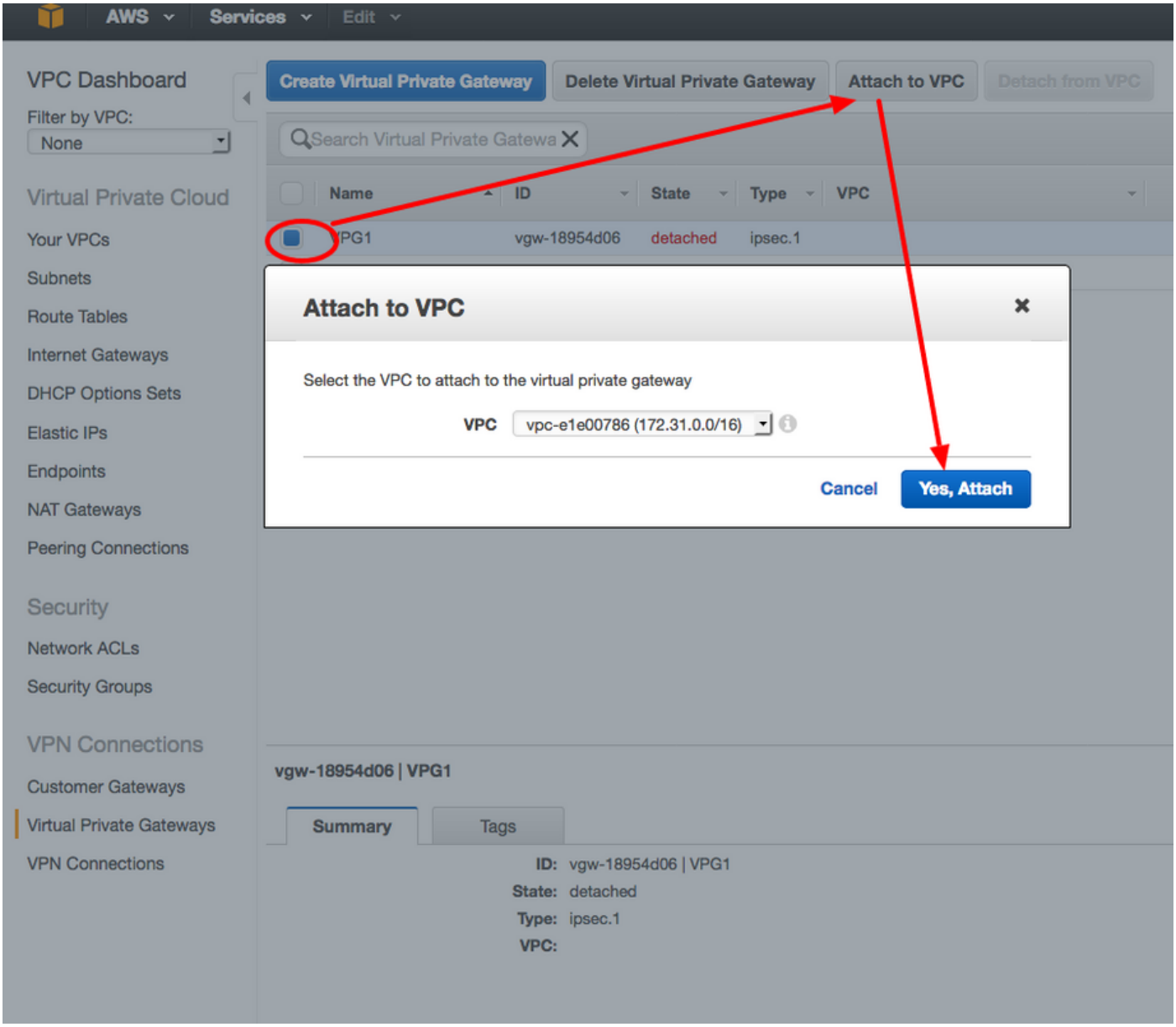
Campo	Valor
Etiqueta de nome	Um nome legível por humanos para reconhecer o VPG.



Etapa 5.

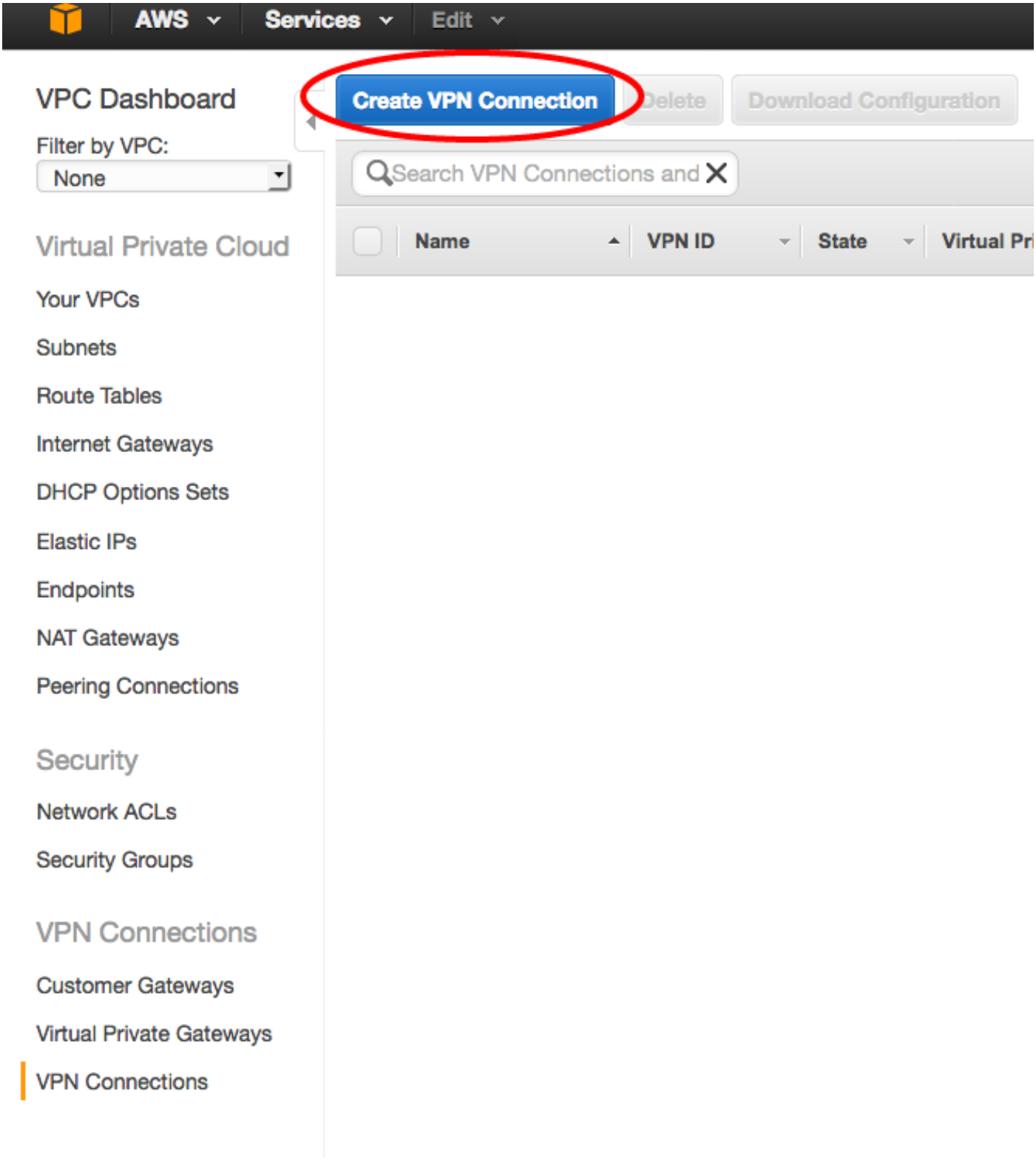
Conecte o VPG ao VPC.

Escolha o Virtual Private Gateway, clique em **Attach to VPC**, escolha o VPC na lista suspensa VPC e clique em **Yes, Attach (Sim, anexar)**.

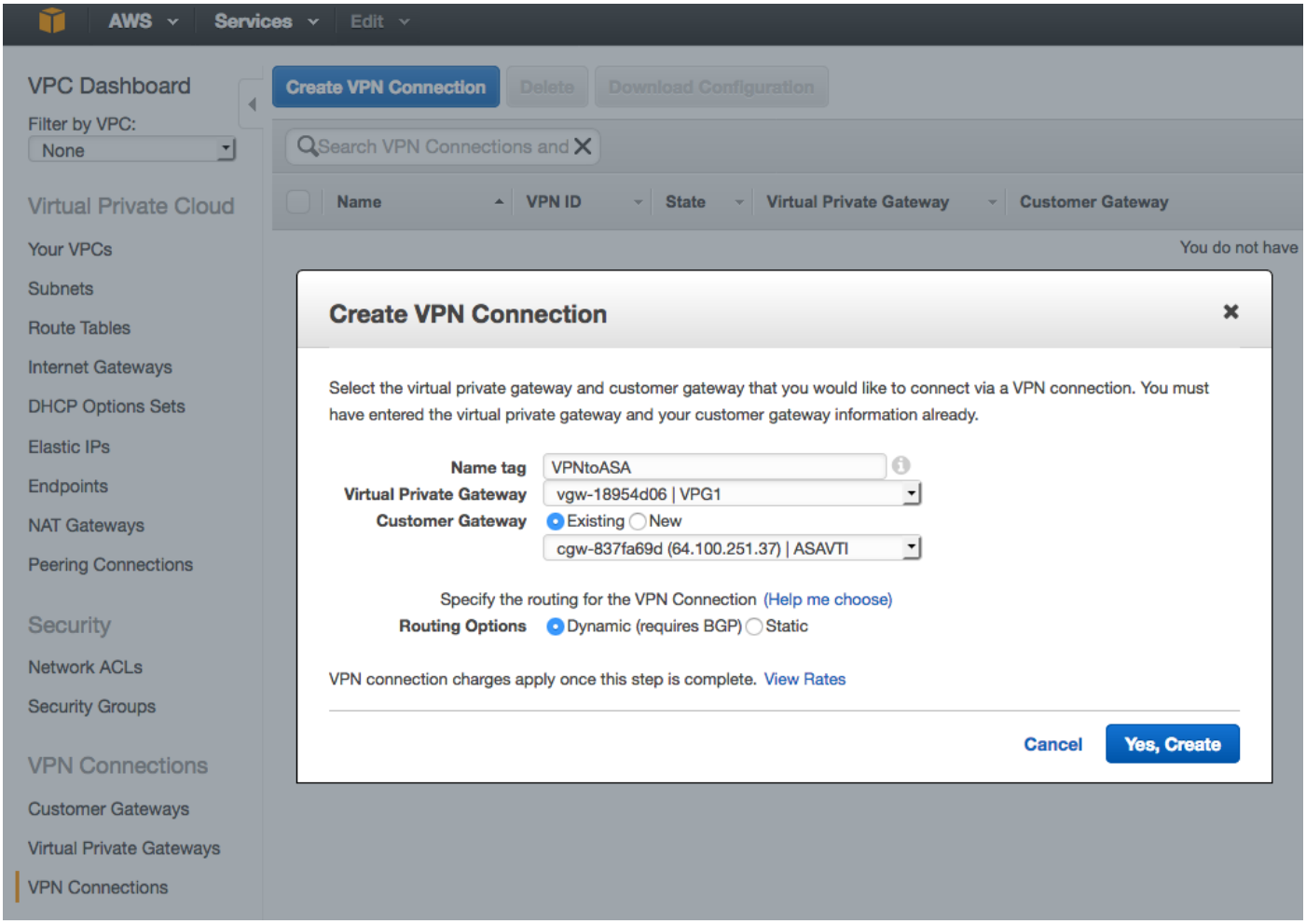


Etapa 6.

Crie uma conexão VPN.

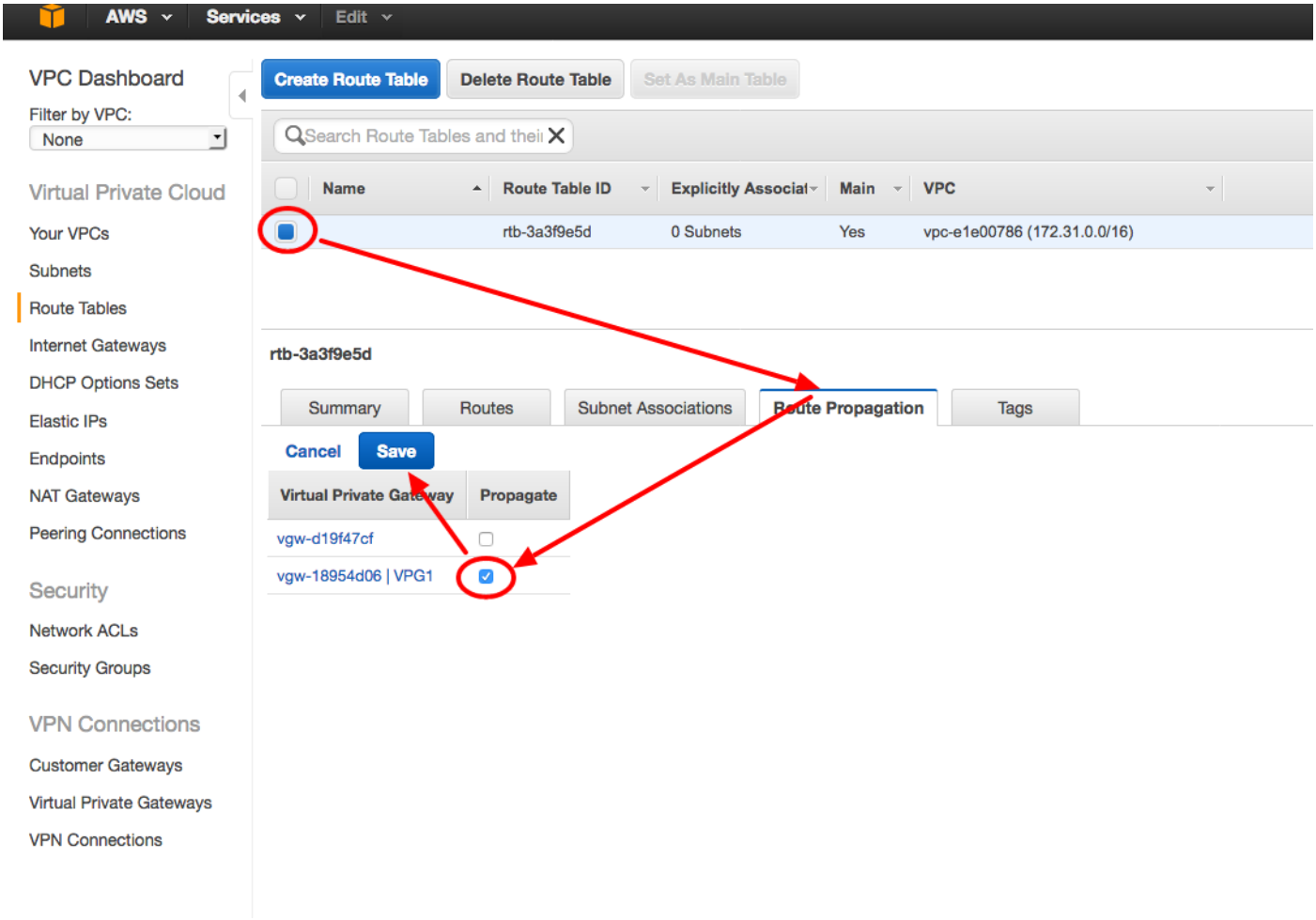


Campo	Valor
Etiqueta de nome	Uma marca legível por humanos da conexão VPN entre o AWS e o ASA.
Virtual Private Gateway	Escolha o VPG recém-criado.
Gateway do cliente	Clique no botão de opção **Existente** e escolha o gateway do ASA.
Opções de roteamento	Clique no botão de opção **Dynamic (Requer BGP)**.



Passo 7.

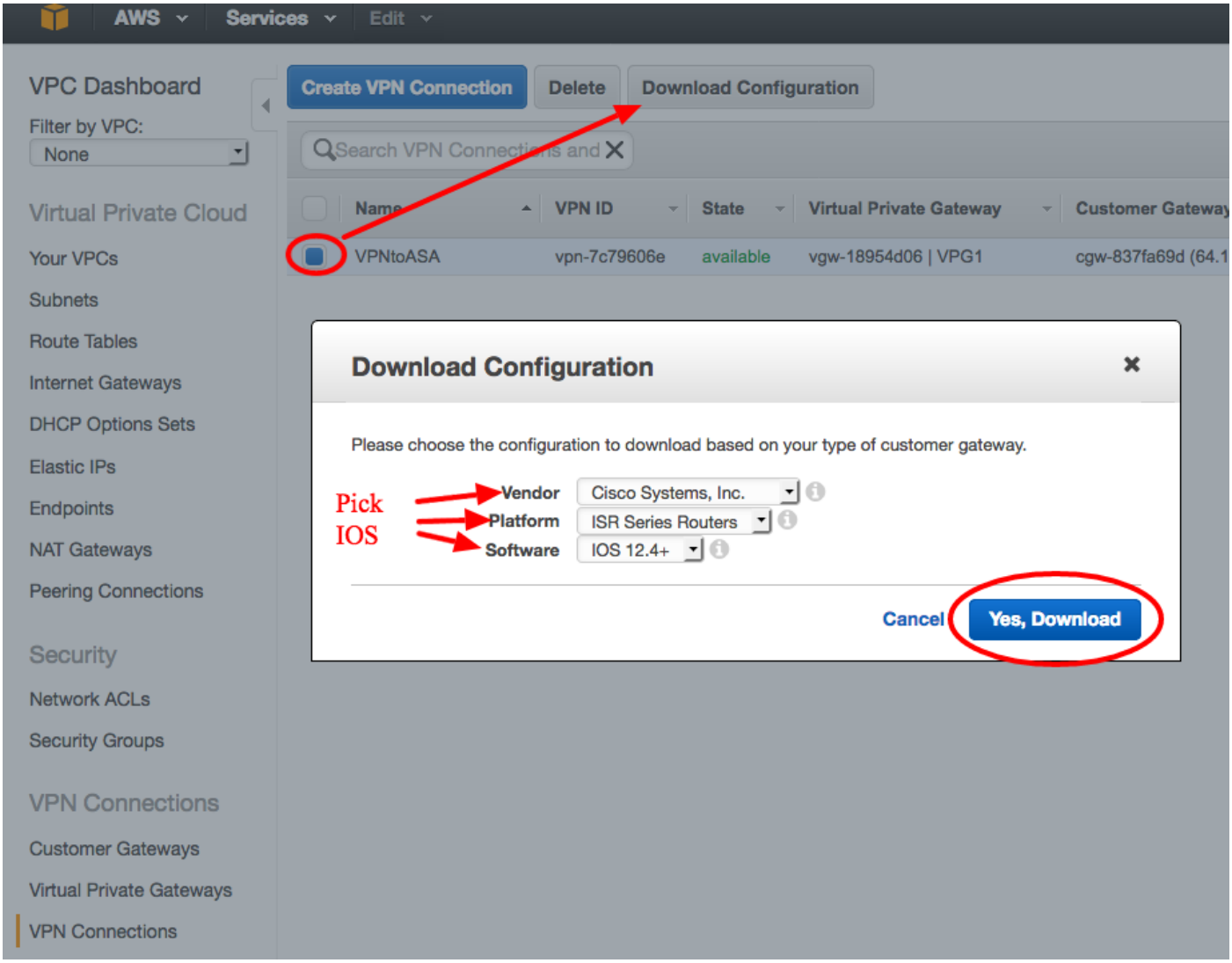
Configure a tabela de rotas para propagar as rotas aprendidas do VPG (via BGP) para o VPC.



Etapa 8.

Faça o download da configuração sugerida. Escolha os valores abaixo para gerar uma configuração que seja uma configuração de estilo VTI.

Campo	Valor
Fornecedor	Cisco Systems, Inc.
Platform	Roteadores série ISR
Software	IOS 12.4+



Configurar o ASA

Depois de fazer o download da configuração, é necessária alguma conversão.

Etapa 1.

crypto isakmp policy para crypto ikev1 policy. Só é necessária uma política, uma vez que a política 2000 e a política 2010 são idênticas.

Configuração sugerida	Para
crypto isakmp policy 200 encryption aes 128 Pré-compartilhamento de autenticação grupo 2 duração 28800 hash sha sair crypto isakmp policy 201 encryption aes 128 Pré-compartilhamento de autenticação grupo 2	crypto ikev1 enable outside crypto ikev1 policy 10 Pré-compartilhamento de autenticação aes de criptografia hash sha grupo 2 duração 28800

```
 duração 28800
 hash sha
sair
```

Etapa 2.

crypto ipsec transform-set para crypto ipsec ikev1 transform-set. Somente um conjunto de transformação é necessário, pois os dois conjuntos de transformação são idênticos.

Configuração sugerida	Para
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-0 esp-aes 128 esp-sha-hmac túnel de modo sair	crypto ipsec ikev1 transfo
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-1 esp-aes 128 esp-sha-hmac túnel de modo sair	set AWS esp-aes esp-sha-hm

Etapa 3.

crypto ipsec profile para crypto ipsec profile. Somente um perfil é necessário, pois os dois perfis são idênticos.

Configuração sugerida	Para
crypto ipsec profile ipsec-vpn-7c79606e-0 set pfs group2 set security-association lifetime seconds 3600 set transform-set ipsec-prop-vpn-7c79606e-0 sair	crypto ipsec profile AWS set ikev1 transform-set AWS set pfs group2 set security-association lifet seconds 3600
crypto ipsec profile ipsec-vpn-7c79606e-1 set pfs group2 set security-association lifetime seconds 3600 set transform-set ipsec-prop-vpn-7c79606e-1 sair	

Etapa 4.

crypto keyring e crypto isakmp profile precisam ser convertidos em um tunnel-group one para cada túnel.

Configuração sugerida	Para
crypto keyring keyring-vpn-7c79606e-0 endereço local 64.100.251.37 endereço de chave pré-compartilhada 52.34.205.227 chave QZhh90Bjf sair	tunnel-group 52.34.205.227 type ipsec-l2l tunnel-group 52.34.205.227 ipsec-attribute ikev1 chave pré-compartilhada QZhh90B
! crypto isakmp profile isakmp-vpn-7c79606e-0 endereço local 64.100.251.37 match identity address 52.34.205.227 keyring-vpn-7c79606e-0	 isakmp keepalive threshold 10 retry 10

```
 sair
!
crypto keyring keyring-vpn-7c79606e-1
 endereço local 64.100.251.37
 endereço de chave pré-compartilhada 52.37.194.219 chave
JjxCWy4Ae
 sair
!
crypto isakmp profile isakmp-vpn-7c79606e-1
 endereço local 64.100.251.37
 match identity address 52.37.194.219
 keyring-vpn-7c79606e-1
 sair
```

```
tunnel-group
52.37.194.219 type
ipsec-l2l
tunnel-group
52.37.194.219 ipsec-
attribute
 ikev1 chave pré-
compartilhada JjxCWy4
 isakmp keepalive
threshold 10 retry 10
```

Etapa 5.

A configuração do túnel é quase idêntica. O ASA não suporta o ip tcp adjust-mss ou o comando ip virtual-reassembly.

Configuração sugerida

```
interface Tunnel1
 endereço ip 169.254.13.190 255.255.255.252
 ip virtual-reassembly
 tunnel source 64.100.251.37
 tunnel destination 52.34.205.227
 ipsec ipv4 de modo de túnel
 proteção de túnel ipsec perfil ipsec-vpn-
7c79606e-0
 ip tcp adjust-mss 1387
 no shutdown
 sair
!
túnel de interface2
 endereço ip 169.254.12.86 255.255.255.252
 ip virtual-reassembly
 tunnel source 64.100.251.37
 tunnel destination 52.37.194.219
 ipsec ipv4 de modo de túnel
 proteção de túnel ipsec perfil ipsec-vpn-
7c79606e-1
 ip tcp adjust-mss 1387
 no shutdown
 sair
```

Para

```
interface Tunnel1
 nome AWS1
 endereço ip 169.254.13.190
255.255.255.252
 tunnel source interface outsid
 tunnel destination 52.34.205.2
 ipsec ipv4 de modo de túnel
 proteção de túnel IPSec perfil
AWS
!
túnel de interface2
 nome AWS2
 endereço ip 169.254.12.86
255.255.255.252
 tunnel source interface outsid
 tunnel destination 52.37.194.2
 ipsec ipv4 de modo de túnel
 proteção de túnel IPSec perfil
AWS
```

Etapa 6.

Neste exemplo, o ASA anunciará somente a sub-rede interna (192.168.1.0/24) e receberá a sub-rede no AWS (172.31.0.0/16).

Configuração sugerida

```
router bgp 65000
 neighbor 169.254.13.189 remote-as 7224
 neighbor 169.254.13.189 ativado
 neighbor 169.254.13.189 timers 10 30 30
```

Para

```
router bgp 65000
 bgp log-neighbor-changes
 timers bgp 10 30 0
 address-family ipv4 unica
```

```
 address-family ipv4 unicast
  neighbor 169.254.13.189 remote-as 7224
  neighbor 169.254.13.189 timers 10 30 30
  neighbor 169.254.13.189 default-originate
  neighbor 169.254.13.189 ativado
  neighbor 169.254.13.189 soft-reconfiguration
inbound                                          neighbor 169.254.12.85
  network 0.0.0.0                               remote-as 7224
  sair                                           neighbor 169.254.12.85
 sair                                           ativado
router bgp 65000                                 neighbor 169.254.13.189
 neighbor 169.254.12.85 remote-as 7224          remote-as 7224
 neighbor 169.254.12.85 ativado                  neighbor 169.254.13.189
 neighbor 169.254.12.85 timers 10 30 30         ativado
 address-family ipv4 unicast                     network 192.168.1.0
  neighbor 169.254.12.85 remote-as 7224          no autossummary
  neighbor 169.254.12.85 timers 10 30 30         sem sincronização
  neighbor 169.254.12.85 default-originate       exit-address-family
  neighbor 169.254.12.85 ativado
  neighbor 169.254.12.85 soft-reconfiguration
inbound
  network 0.0.0.0
  sair
 sair
```

Verificar e otimizar

Etapa 1.

Confirme se o ASA estabelece as associações de segurança IKEv1 com os dois endpoints no AWS. O estado da SA deve ser MM_ATIVE.

```
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#
```

Etapa 2.

Confirme se as SAs IPsec estão instaladas no ASA. Deve haver um SPI de entrada e saída instalado para cada peer e deve haver alguns contadores encaps e decaps incrementando.

```
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
```

Etapa 3.

No ASA, confirme se as conexões BGP estão estabelecidas com o AWS. O contador State/PfxRcd deve ser 1, pois o AWS anuncia a sub-rede 172.31.0.0/16 para o 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
```

Etapa 4.

No ASA, verifique se a rota para 172.31.0.0/16 foi aprendida através das interfaces de túnel. Essa saída mostra que há dois caminhos para 172.31.0.0 do peer 169.254.12.85 e 169.254.13.189. O caminho para 169.254.13.189 out Tunnel 2 (AWS2) é preferido devido à métrica mais baixa.

```
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
```

Etapa 5.

Para garantir que o tráfego que retorna do AWS siga um caminho simétrico, configure um mapa de rota para corresponder ao caminho preferencial e ajuste o BGP para alterar as rotas 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
```

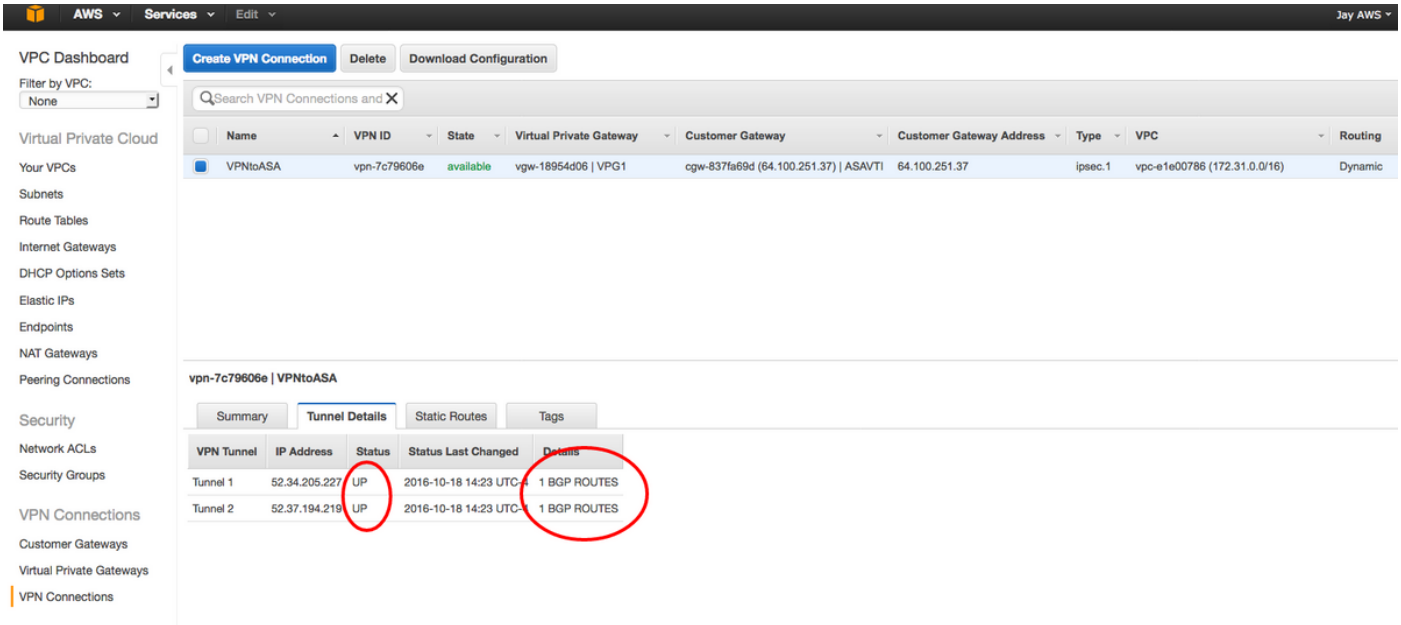
Etapa 6.

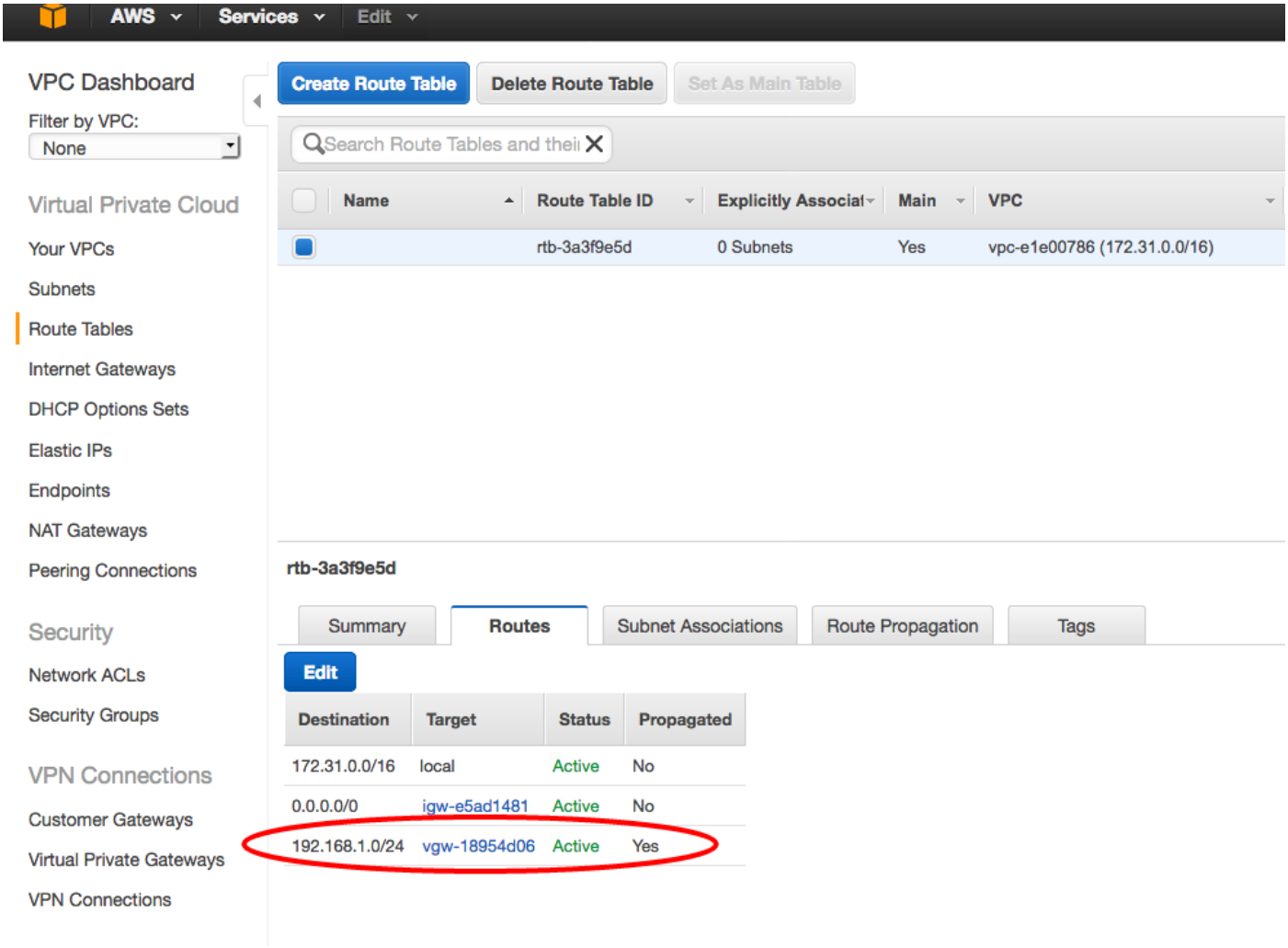
No ASA, confirme se 192.168.1.0/24 é anunciado ao AWS.

```
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
```

Passo 7.

No AWS, confirme se os túneis para a conexão VPN estão UP e se as rotas são aprendidas do peer. Verifique também se a rota foi propagada na tabela de roteamento.




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 thei
Name
Route Table ID
Explicitly Associat
Main
VPC
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
igw-e5ad1481
Active
No
192.168.1.0/24
vgw-18954d06
Active
Yes