配置ASA IPsec VTI Connection Amazon Web Services

目录

[简介](#)
[配置AWS](#)
[配置 ASA](#)
[验证和优化](#)

简介

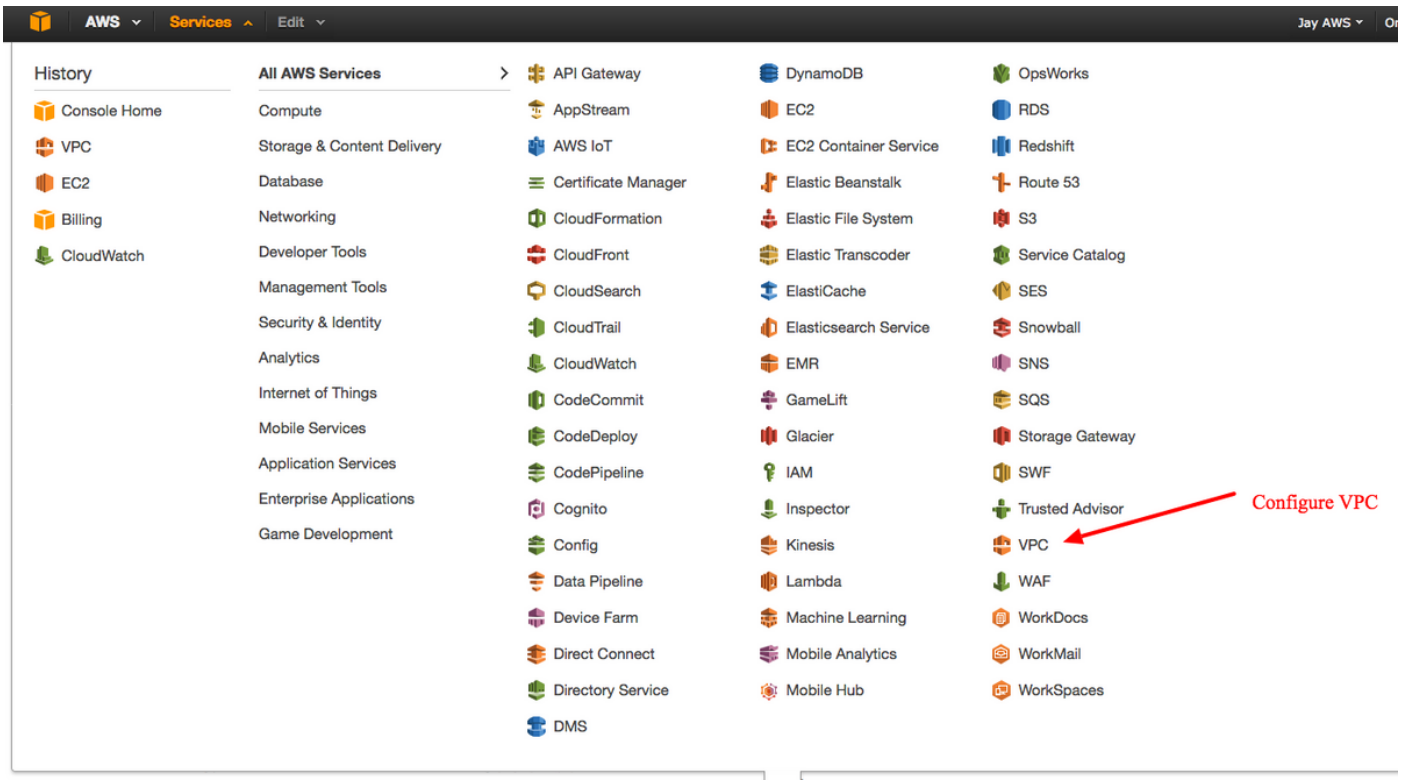
本文档介绍如何配置自适应安全设备(ASA)IPsec虚拟隧道接口(VTI)连接。在ASA 9.7.1中，引入了IPsec VTI。 此版本中仅限于使用IKEv1的sVTI IPv4 over IPv4。 这是ASA连接到Amazon Web Services(AWS)的配置示例。

> **注意**：目前，VTI仅在单情景路由模式下受支持。

配置AWS

步骤1:

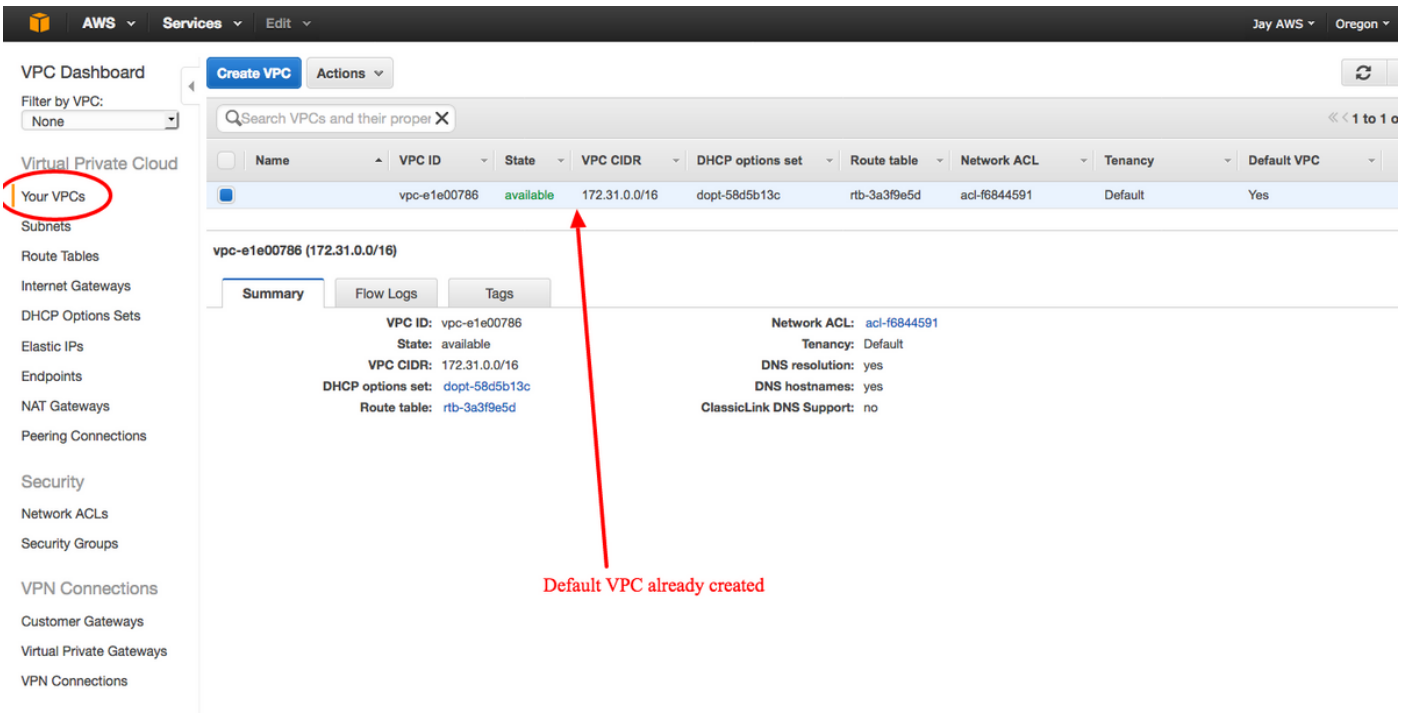
登录AWS控制台并导航至VPC面板。



导航至VPC控制面板

第二步：

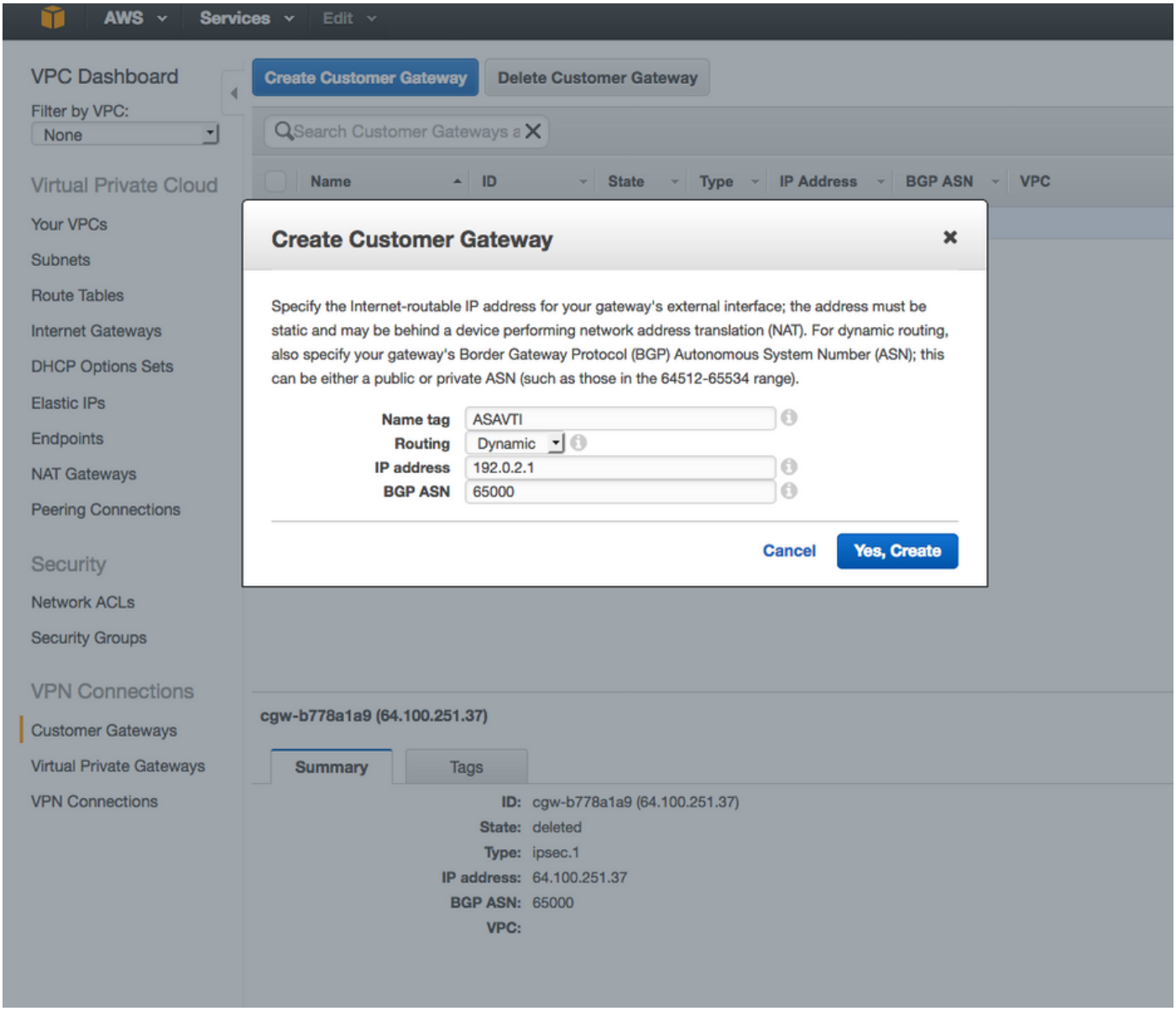
确认已创建虚拟私有云(VPC)。 默认情况下，会创建一个172.31.0.0/16的VPC。这是虚拟机(VM)的连接位置。



第三步：

创建“客户网关”。 这是代表ASA的终端。

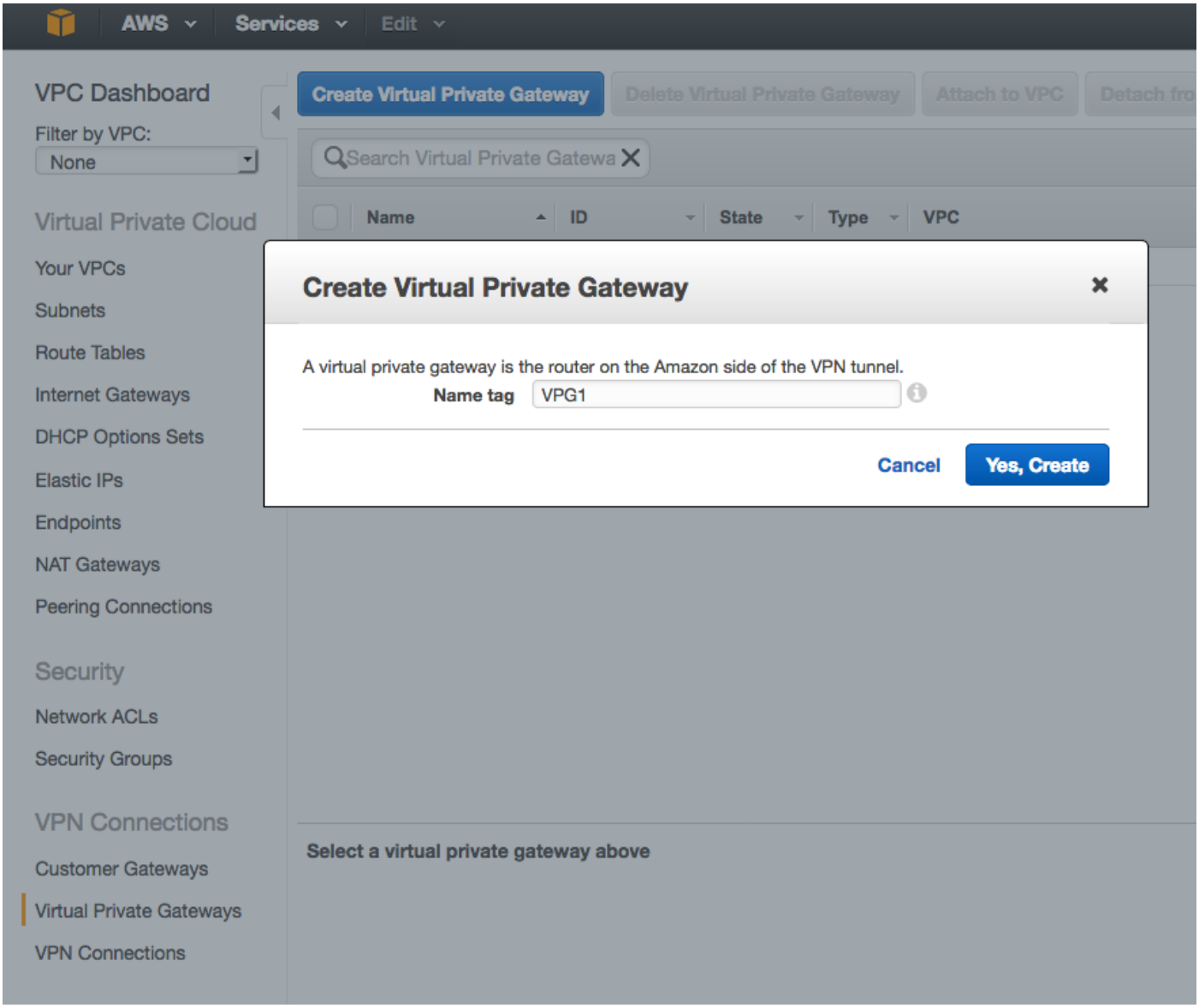
字段	**价值**
名称标记	这只是一个可识别ASA的可读名称。
路由	动态 — 这意味着将使用边界网关协议(BGP)来交换路由信息。
IP Address	这是ASA外部接口的公有IP地址。
BGP ASN	BGP进程的自治系统(AS)编号，比在ASA上运行的编号。使用65000，除非您的组织有公共AS编



第四步：

创建虚拟专用网关(VPG)。 这是一台模拟路由器，它托管于AWS，终止IPsec隧道。

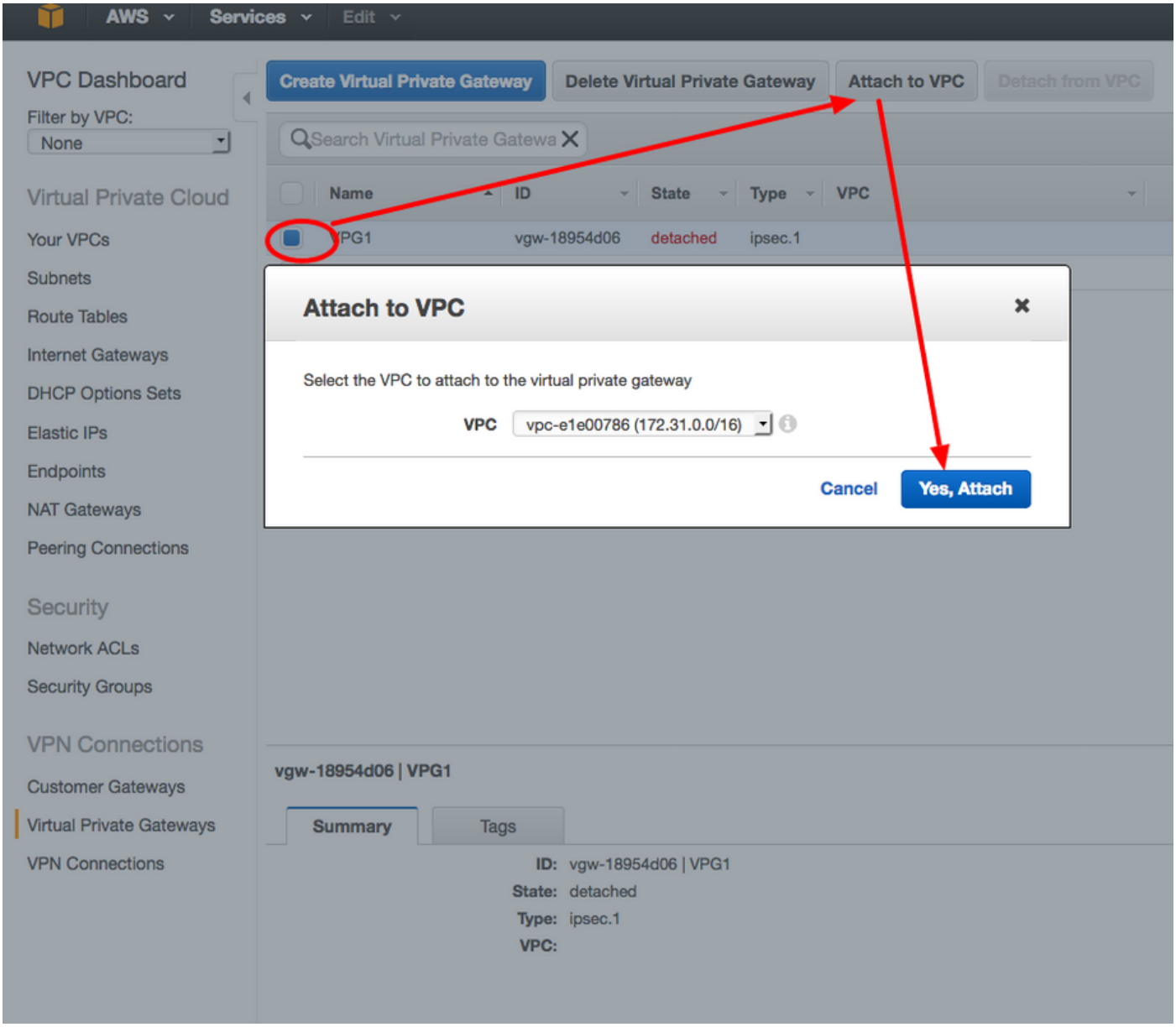
字段 价值
名称标记 识别VPG的可读名称。



第五步：

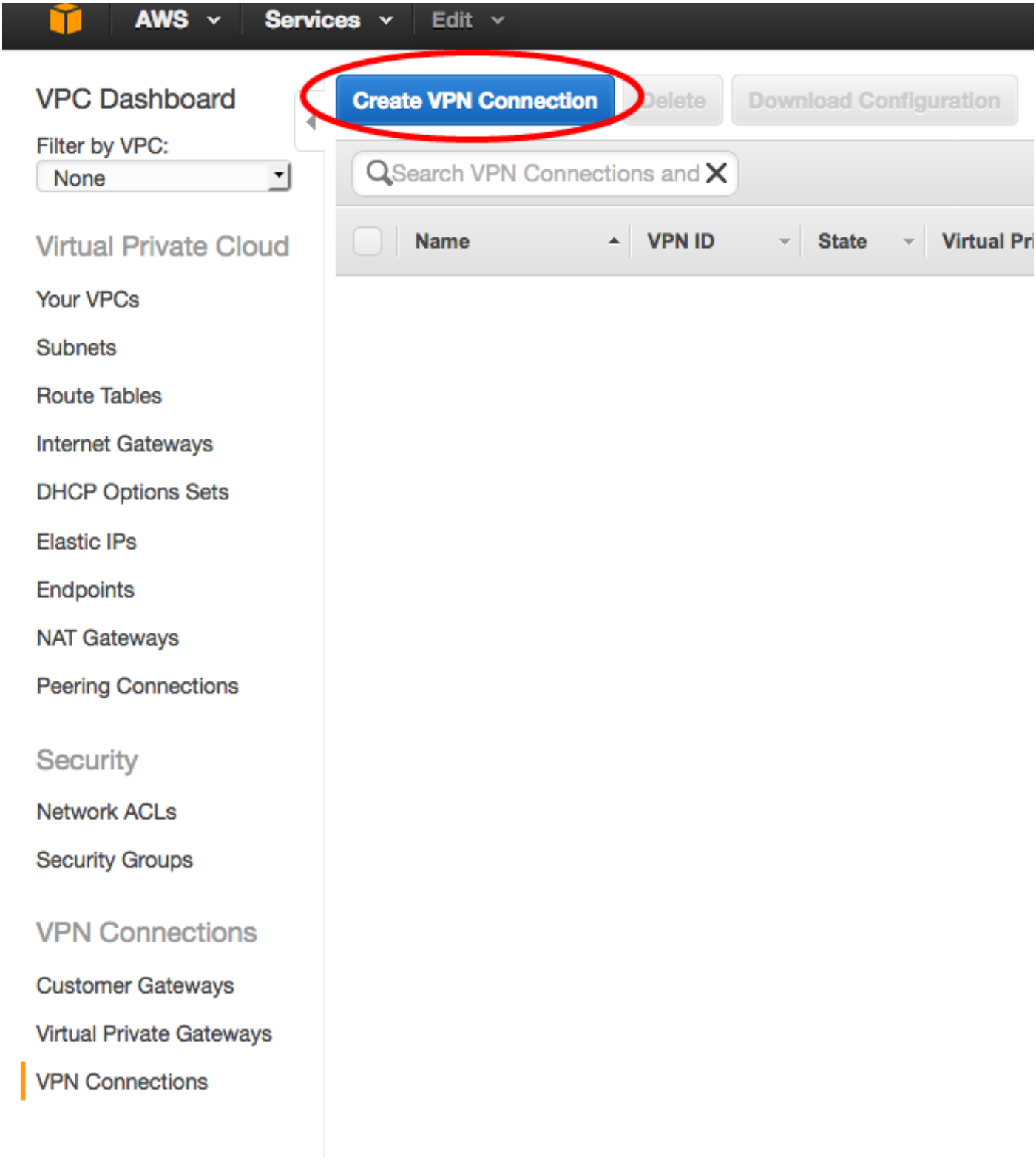
将VPG连接到VPC。

选择虚拟专用网关，点击**连接到VPC**，从VPC下拉列表中选择VPC，然**后点击是，连接**。

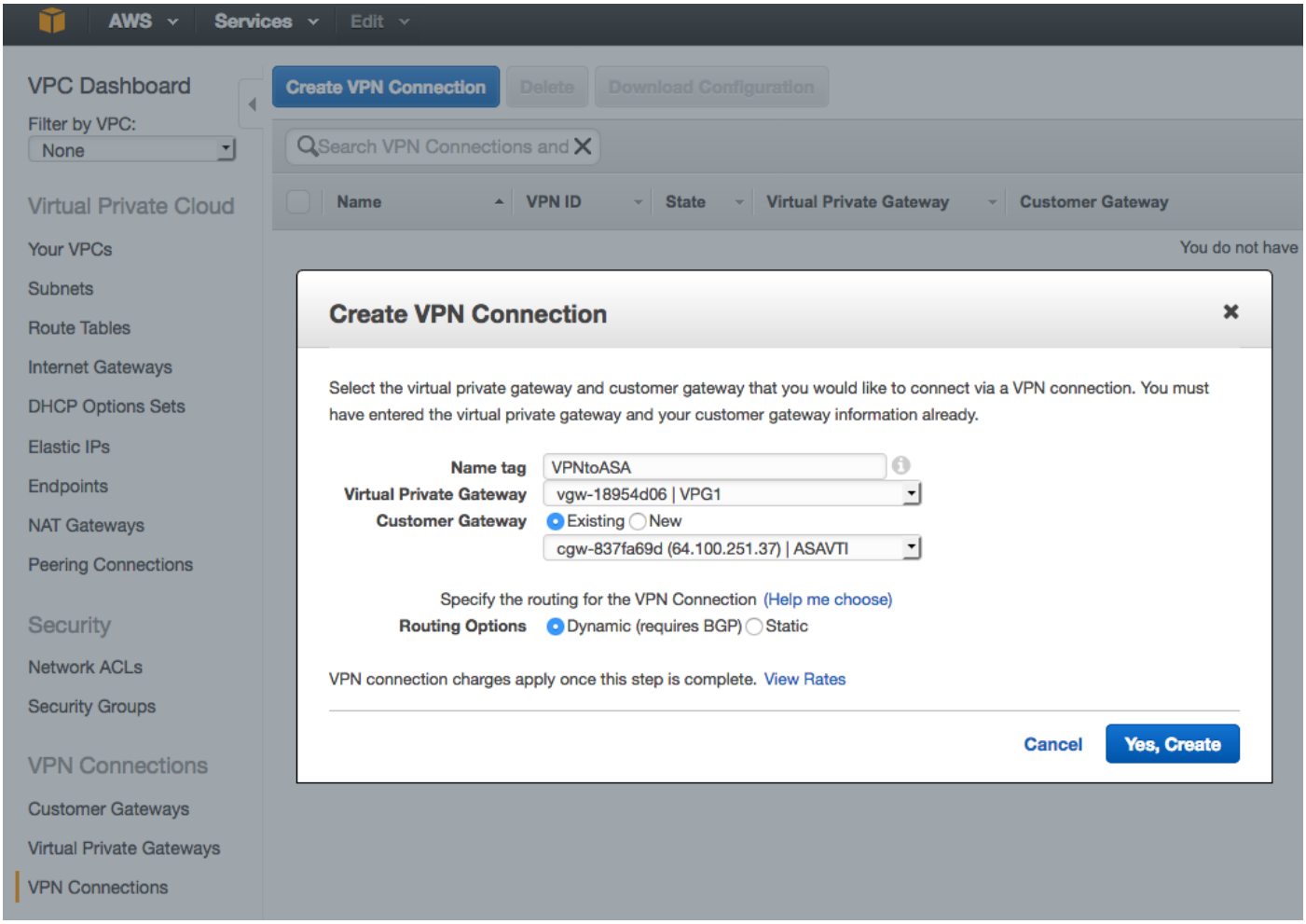

AWS
Services
Edit
VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create Virtual Private Gateway
Delete Virtual Private Gateway
Attach to VPC
Detach from VPC
Search Virtual Private Gatewa
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)
Cancel
Yes, Attach
vgw-18954d06 | VPG1
Summary
Tags
ID: vgw-18954d06 | VPG1
State: detached
Type: ipsec.1
VPC:

第六步：

创建VPN连接。

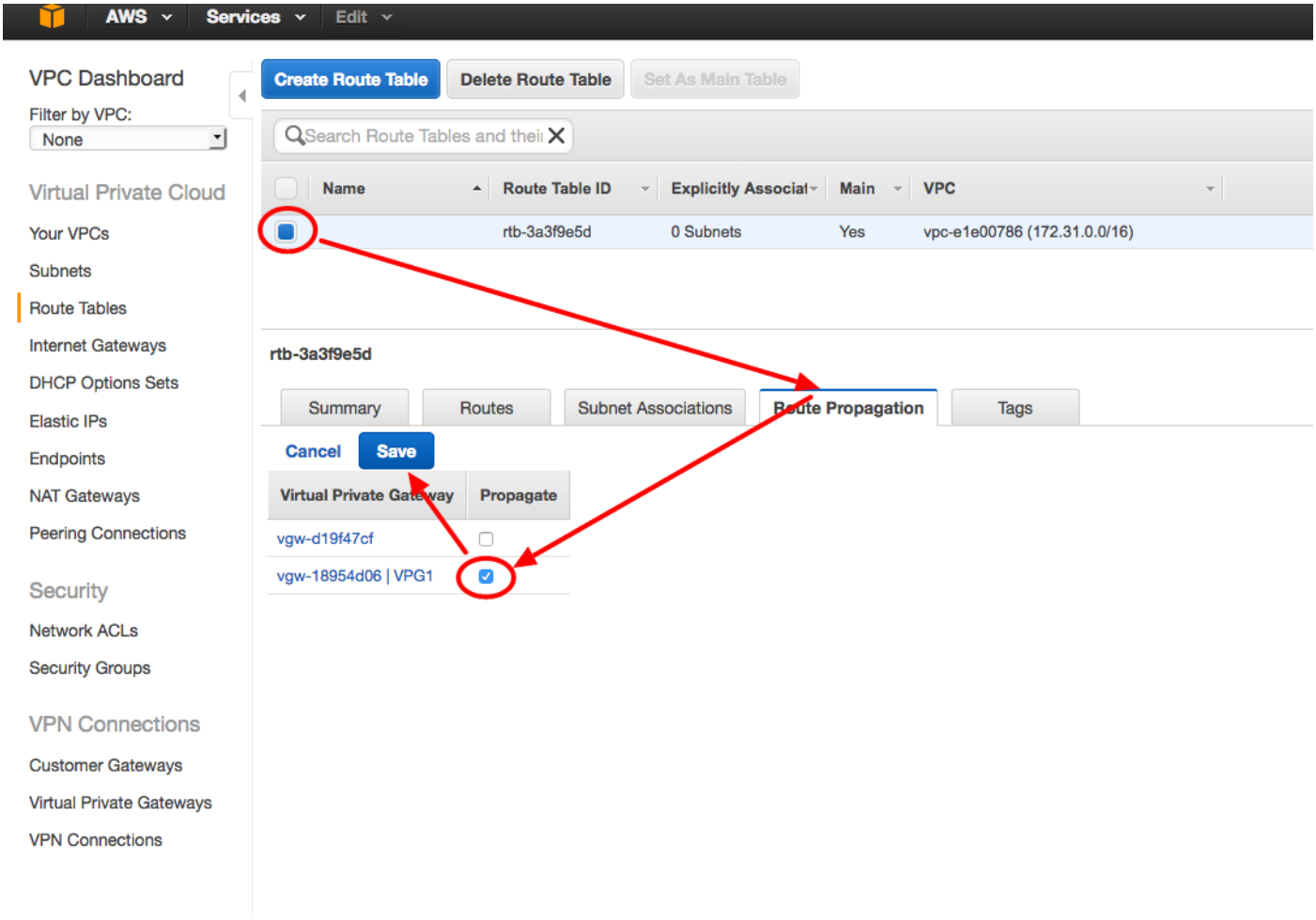


字段	价值
名称标记	AWS和ASA之间VPN连接的可读标签。
虚拟专用网关	选择刚创建的VPG。
客户网关	单击Existing单选按钮，然后选择ASA的网关。
路由选项	单击“Dynamic(requires BGP)”单选按钮。



步骤 7.

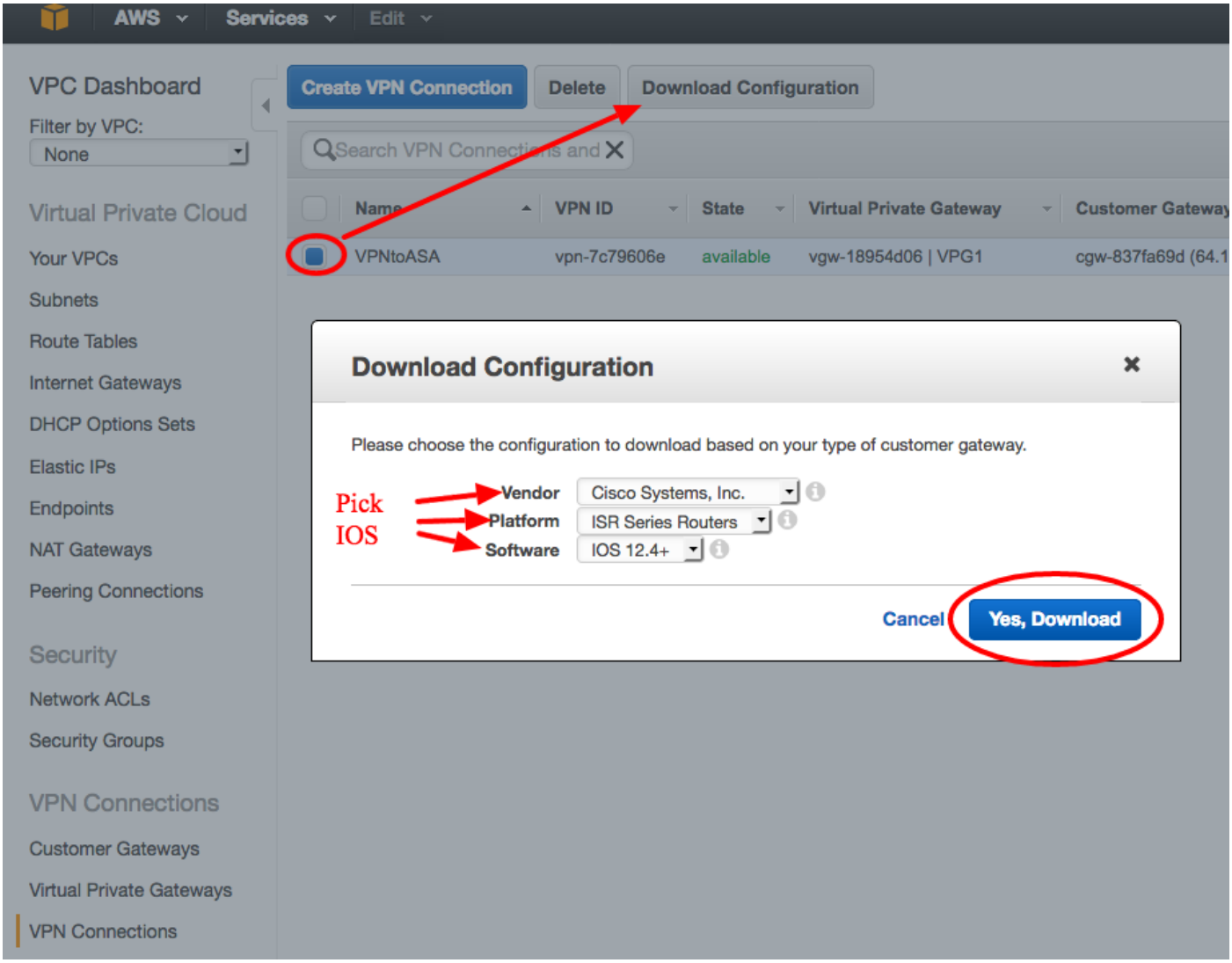
配置路由表，将从VPG（通过BGP）获知的路由传播到VPC。



步骤 8

下载建议的配置。 选择以下值以生成VTI样式配置的配置。

字段	价值
供应商	Cisco Systems, Inc.
Platform	ISR系列路由器
软件	IOS 12.4+



配置 ASA

下载配置后，需要进行一些转换。

步骤1:

crypto isakmp policy to crypto ikev1 policy。 由于策略200和策略201相同，因此只需要一个策略。

建议的配置

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

crypto isakmp policy 201
 encryption aes 128
 authentication pre-share
  2
 lifetime 28800
```

至

```
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 AES
 hash sha
  2
 lifetime 28800
```

```
 hash sha
```

第二步：

crypto ipsec transform-set到crypto ipsec ikev1 transform-set。 只需一个转换集，因为两个转换集是相同的。

建议的配置	至
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-0 esp-aes 128 esp-sha-hmac	
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-1 esp-aes 128 esp-sha-hmac	crypto ipsec ikev1 transform-s AWS esp-aes esp-sha-hmac

第三步：

crypto ipsec profile到crypto ipsec profile。 只需一个配置文件，因为两个配置文件是相同的。

建议的配置	至
crypto ipsec profile ipsec-vpn-7c79606e-0 set pfs group2 set security-association lifetime seconds 3600 set transform-set ipsec-prop-vpn-7c79606e-0	
crypto ipsec profile ipsec-vpn-7c79606e-1 set pfs group2 set security-association lifetime seconds 3600 set transform-set ipsec-prop-vpn-7c79606e-1	crypto ipsec profile AWS set ikev1 transform-set AWS set pfs group2 set security-association lifet seconds 3600

第四步：

加密密钥环和加密isakmp配置文件需要转换为每个隧道的隧道组。

建议的配置	至
crypto keyring keyring-vpn-7c79606e-0 local-address 64.100.251.37 52.34.205.227QZhh90Bjf ! crypto isakmp profile isakmp-vpn-7c79606e-0 local-address 64.100.251.37 match identity address 52.34.205.227 keyring keyring-vpn-7c79606e-0 ! crypto keyring keyring-vpn-7c79606e-1 local-address 64.100.251.37	tunnel-group 52.34.205. type ipsec-l2l tunnel-group 52.34.205. ipsec-attributes ikev1 pre-shared-key QZhh90Bjf isakmp keepalive threshold 10 retry 10 tunnel-group 52.37.194. type ipsec-l2l tunnel-group 52.37.194. ipsec-attributes ikev1JjxCWy4Ae

```
 52.37.194.219JjxCWy4Ae

!
crypto isakmp profile isakmp-vpn-7c79606e-1              isakmp keepalive
 local-address 64.100.251.37                            threshold 10 retry 10
 match identity address 52.37.194.219
 keyring keyring-vpn-7c79606e-1
```

第五步：

隧道配置几乎相同。ASA不支持ip tcp adjust-mss或ip virtual-reassembly命令。

建议的配置

```
Tunnel1
 ip address 169.254.13.190 255.255.255.252
 ip virtual-reassembly
 64.100.251.37
 52.34.205.227
 ipsec ipv4
 ipsecipsec-vpn-7c79606e-0
 ip tcp adjust-mss 1387
 no shutdown

!
Tunnel2
 ip address 169.254.12.86 255.255.255.252
 ip virtual-reassembly
 64.100.251.37
 52.37.194.219
 ipsec ipv4
 ipsecipsec-vpn-7c79606e-1
 ip tcp adjust-mss 1387
 no shutdown
```

至

```
Tunnel1
 nameif AWS1
 ip address 169.254.13.19
255.255.255.252

 52.34.205.227
 ipsec ipv4
 IPSecAWS
!
Tunnel2
 nameif AWS2
 ip address 169.254.12.86
255.255.255.252

 52.37.194.219
 ipsec ipv4
 IPSecAWS
```

第六步：

在本示例中，ASA将只通告内部子网(192.168.1.0/24)并接收AWS内的子网(172.31.0.0/16)。

建议的配置

```
router bgp 65000
 neighbor 169.254.13.189 remote-as 7224
 169.254.13.189 activate
 169.254.13.18910 30 30
 address-family ipv4 unicast
  neighbor 169.254.13.189 remote-as 7224
  169.254.13.18910 30 30
  neighbor 169.254.13.189 default-originate
  169.254.13.189 activate
  neighbor 169.254.13.189 soft-reconfiguration
inbound
  network 0.0.0.0
```

至

```
router bgp 65000
 bgp log-neighbor-changes
 timers bgp 10 30 0
 address-family ipv4 unicas
  neighbor 169.254.12.85
remote-as 7224
  169.254.12.85 activate
  neighbor 169.254.13.189
remote-as 7224
  169.254.13.189 activate
  network 192.168.1.0
  no auto-summary
```

```
router bgp 65000
 neighbor 169.254.12.85 remote-as 7224
 169.254.12.85 activate
 169.254.12.8510 30 30
 address-family ipv4 unicast
  neighbor 169.254.12.85 remote-as 7224
  169.254.12.8510 30 30                                exit-address-family
  neighbor 169.254.12.85 default-originate
  169.254.12.85 activate
  neighbor 169.254.12.85 soft-reconfiguration
inbound
  network 0.0.0.0
```

验证和优化

步骤1:

确认ASA与AWS的两个终端建立IKEv1安全关联。SA的状态应为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#
```

第二步：

确认ASA上已安装IPsec SA。每个对等设备应安装入站和出站SPI，并且应该有一些封顶和封装计数器。

```
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
```

第三步：

在ASA上，确认已与AWS建立BGP连接。 AWS向ASA通告172.31.0.0/16子网时，State/PfxRcd计数器应为1。

```
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
```

第四步：

在ASA上，验证通向172.31.0.0/16的路由已通过隧道接口获知。 此输出显示，从对等体169.254.12.85和169.254.13.189到172.31.0.0有两条路径。通向169.254.13.189的路径从隧道2(AWS)2)是首选，因为度量较低。

```
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
```

第五步：

为确保从AWS返回的流量遵循对称路径，请配置路由映射以匹配首选路径，并调整BGP以更改通告的路由。

```
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
```

第六步：

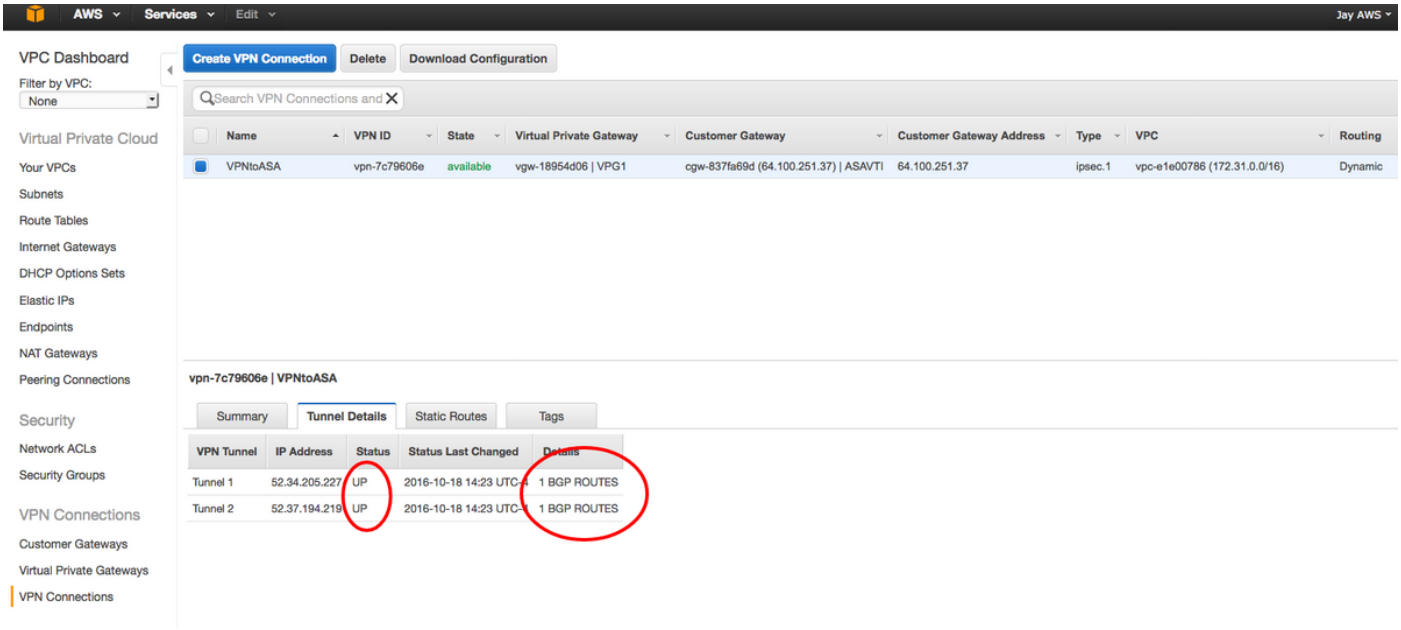
在ASA上，确认192.168.1.0/24已通告给AWS。

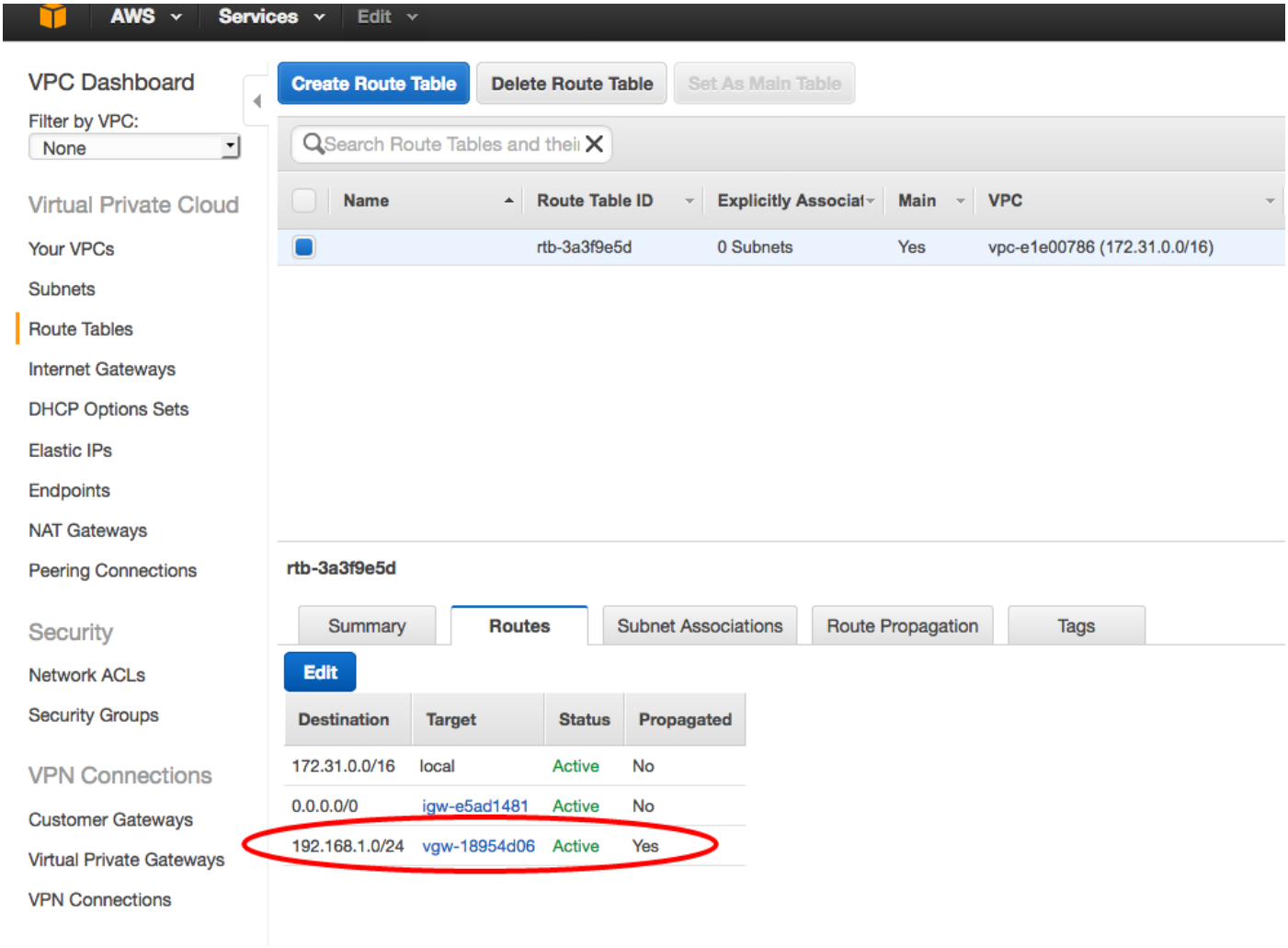
```
ASA# show bgp neighbors 169.254.12.85 advertised-routes

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
```

步骤 7.

在AWS中，确认VPN连接的隧道为UP，并从对等体获取路由。 同时检查路由是否已传播到路由表中。




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