ASA IPsec VTI 연결 Amazon Web Services 구성

목차

[소개](#)
[AWS 구성](#)
[ASA 구성](#)
[확인 및 최적화](#)

소개

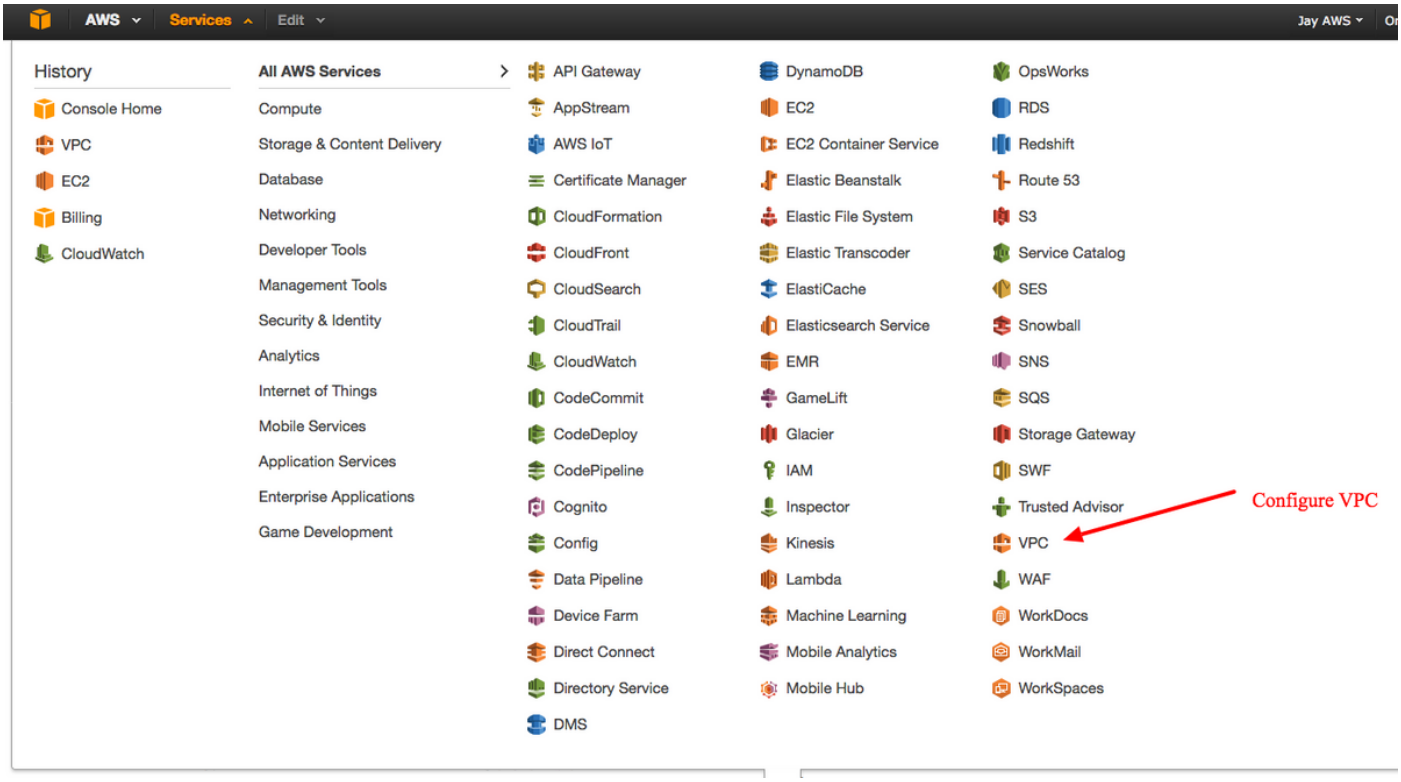
이 문서에서는 ASA(Adaptive Security Appliance) IPsec VTI(Virtual Tunnel Interface) 연결을 구성하는 방법에 대해 설명합니다.ASA 9.7.1에서 IPsec VTI가 도입되었습니다. 이 릴리스에서는 IKEv1을 사용하는 sVTI IPv4 over IPv4로 제한됩니다. 다음은 ASA가 Amazon Web Services(AWS)에 연결하기 위한 컨피그레이션의 예입니다.

> **참고:**현재 VTI는 단일 컨텍스트 라우팅 모드에서만 지원됩니다.

AWS 구성

1단계.

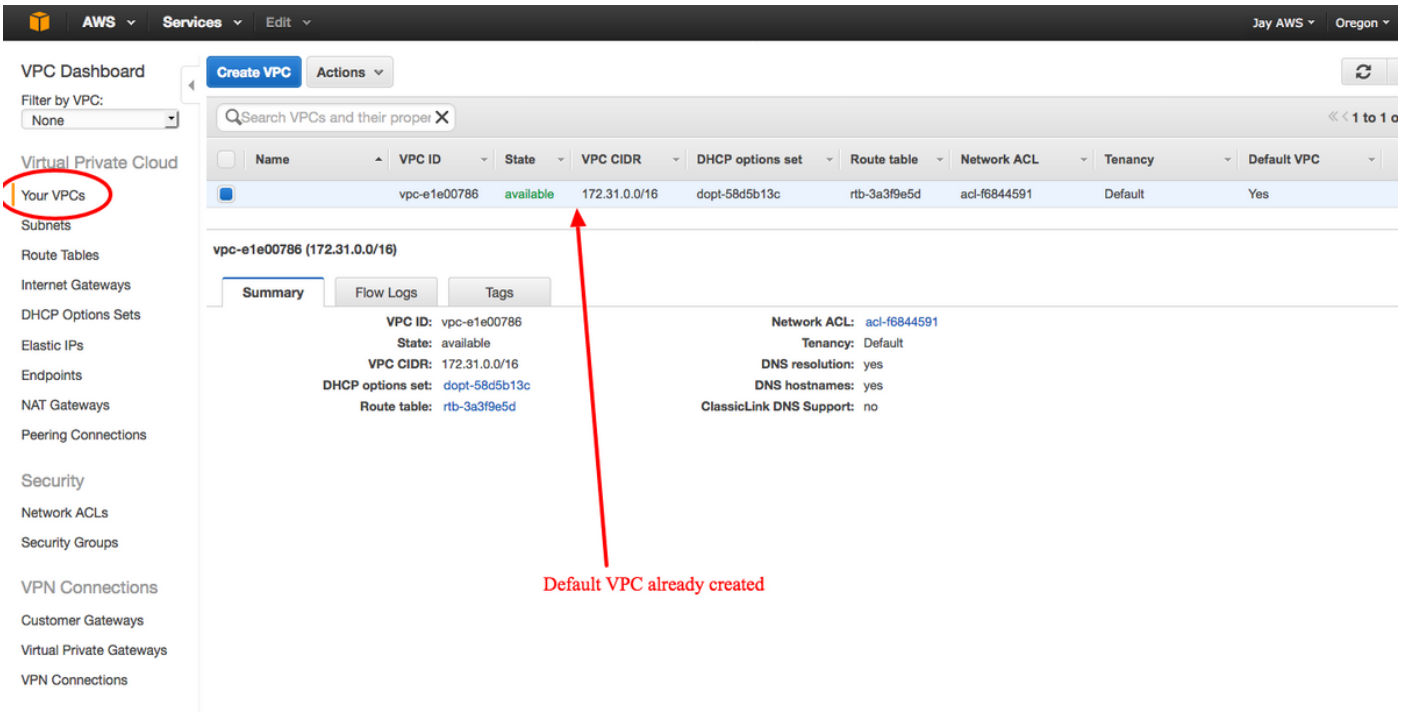
AWS 콘솔에 로그인하고 VPC 패널로 이동합니다.



VPC 대시보드로 이동합니다.

2단계.

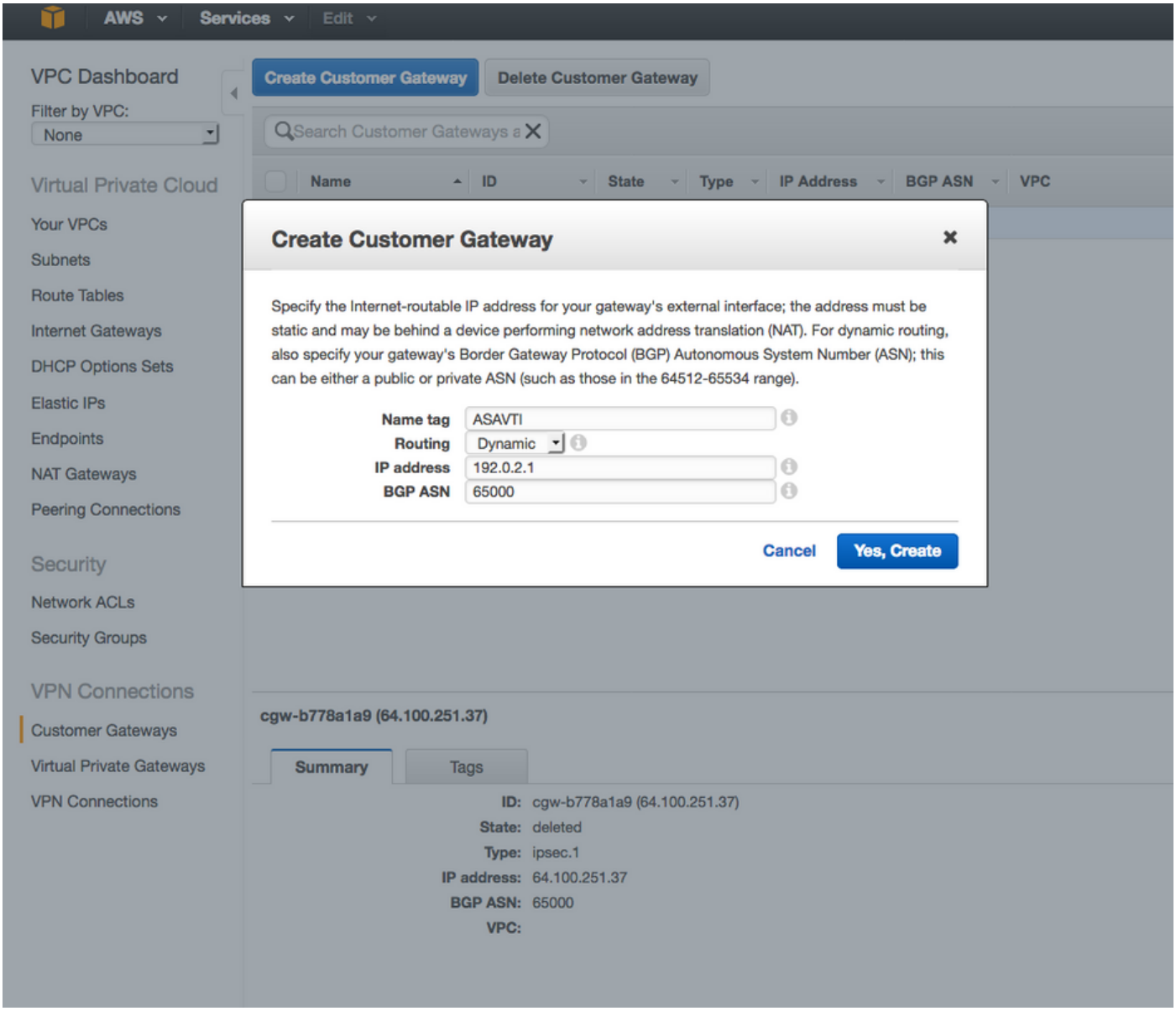
VPC(Virtual Private Cloud)가 이미 생성되었는지 확인합니다. 기본적으로 172.31.0.0/16이 있는 VPC가 생성됩니다.여기서 VM(가상 머신)이 연결됩니다.



3단계.

"Customer Gateway"를 생성합니다. ASA를 나타내는 엔드포인트입니다.

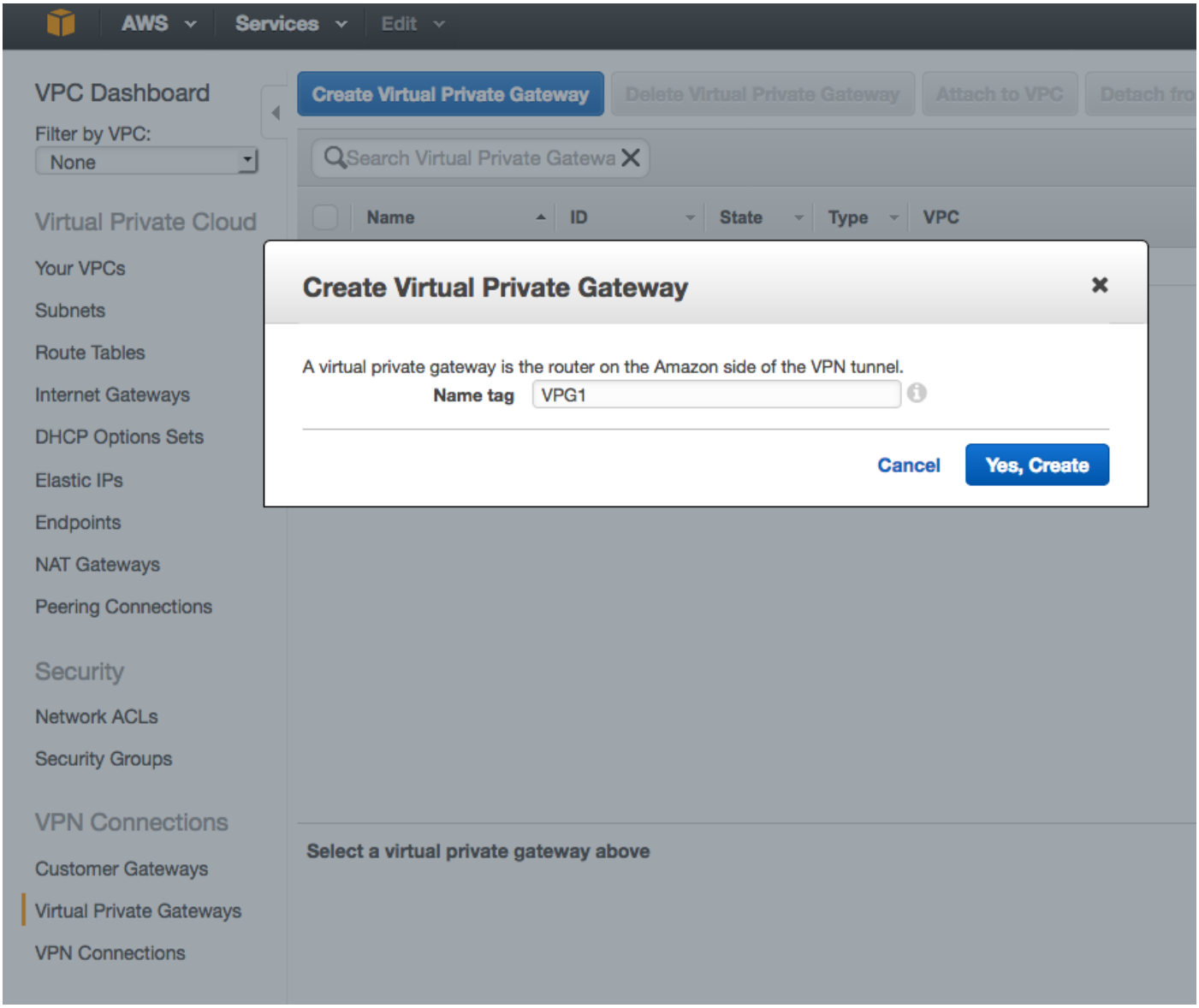
필드	가치
이름 태그	이는 ASA를 인식하기 위해 사람이 읽을 수 있는 이름입니다.
라우팅	Dynamic(동적) - 라우팅 정보를 교환하기 위해 BGP(Border Gateway Protocol)가 사용됨을 의미합
IP 주소	ASA 외부 인터페이스의 공용 IP 주소입니다.
BGP ASN	ASA에서 실행되는 BGP 프로세스의 AS(자동 시스템) 번호입니다.조직에서 공용 AS 번호를 가지고 지 않은 경우 65000을 사용합니다.



4단계.

VPG(Virtual Private Gateway)를 생성합니다. IPsec 터널을 종료하는 AWS와 함께 호스팅되는 시뮬레이션된 라우터입니다.

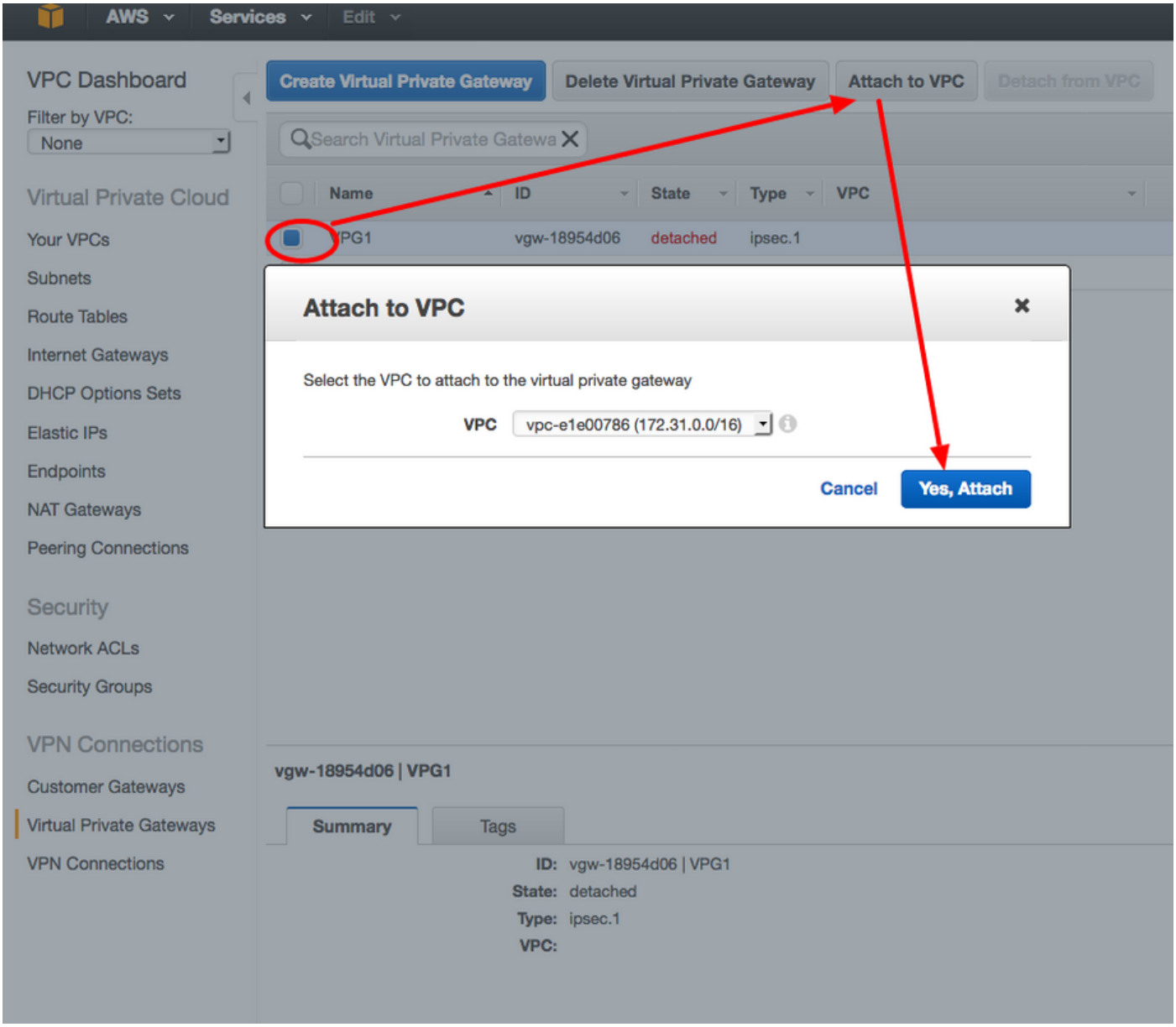
필드 가치
이름 태그 사람이 읽을 수 있는 이름으로 VPG를 인식합니다.



5단계.

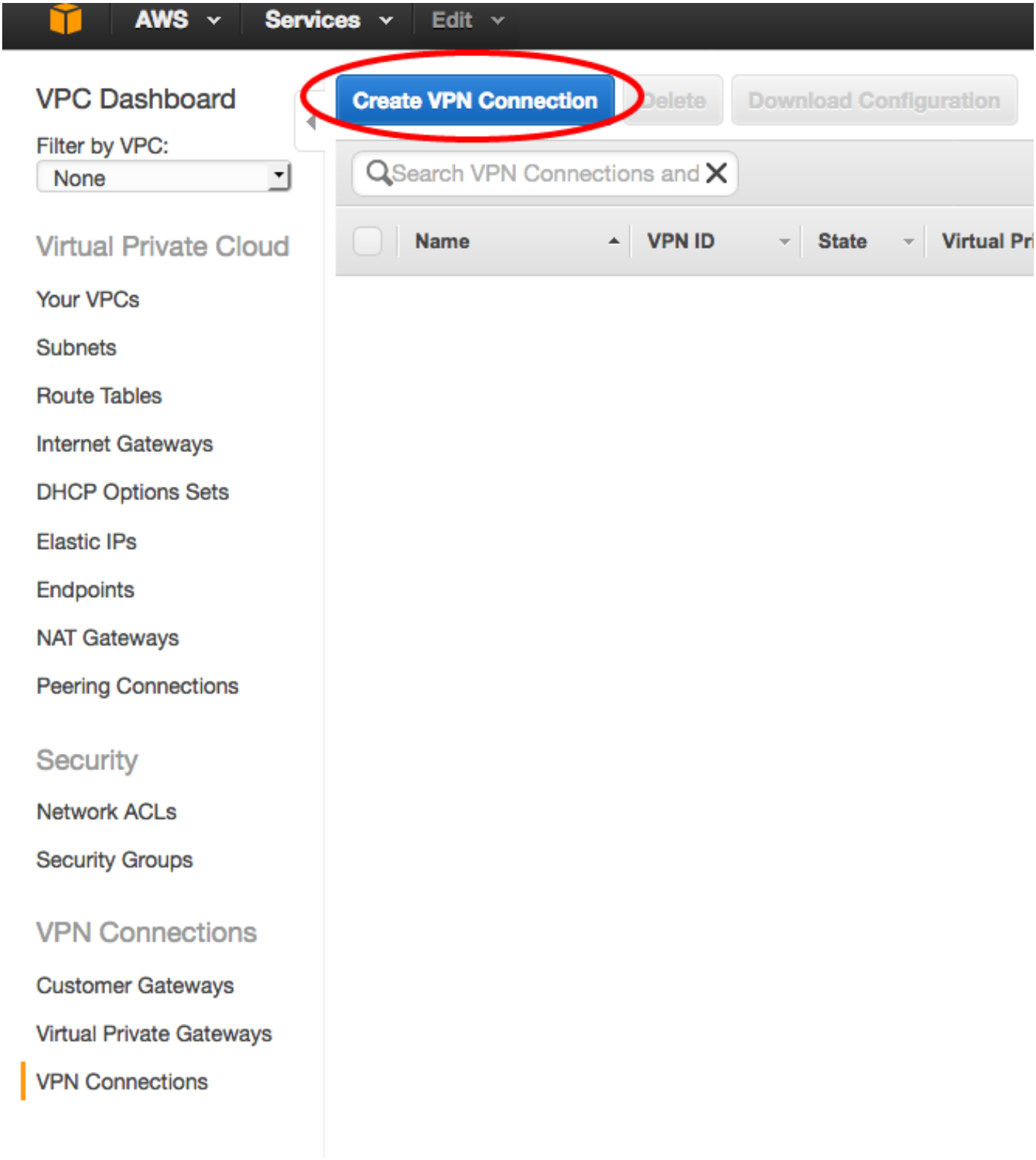
VPC에 VPG를 연결합니다.

Virtual Private Gateway를 선택하고 **Attach to VPC**를 클릭하고 VPC 드롭다운 목록에서 VPC를 선택한 다음 **Yes, Attach**를 클릭합니다.

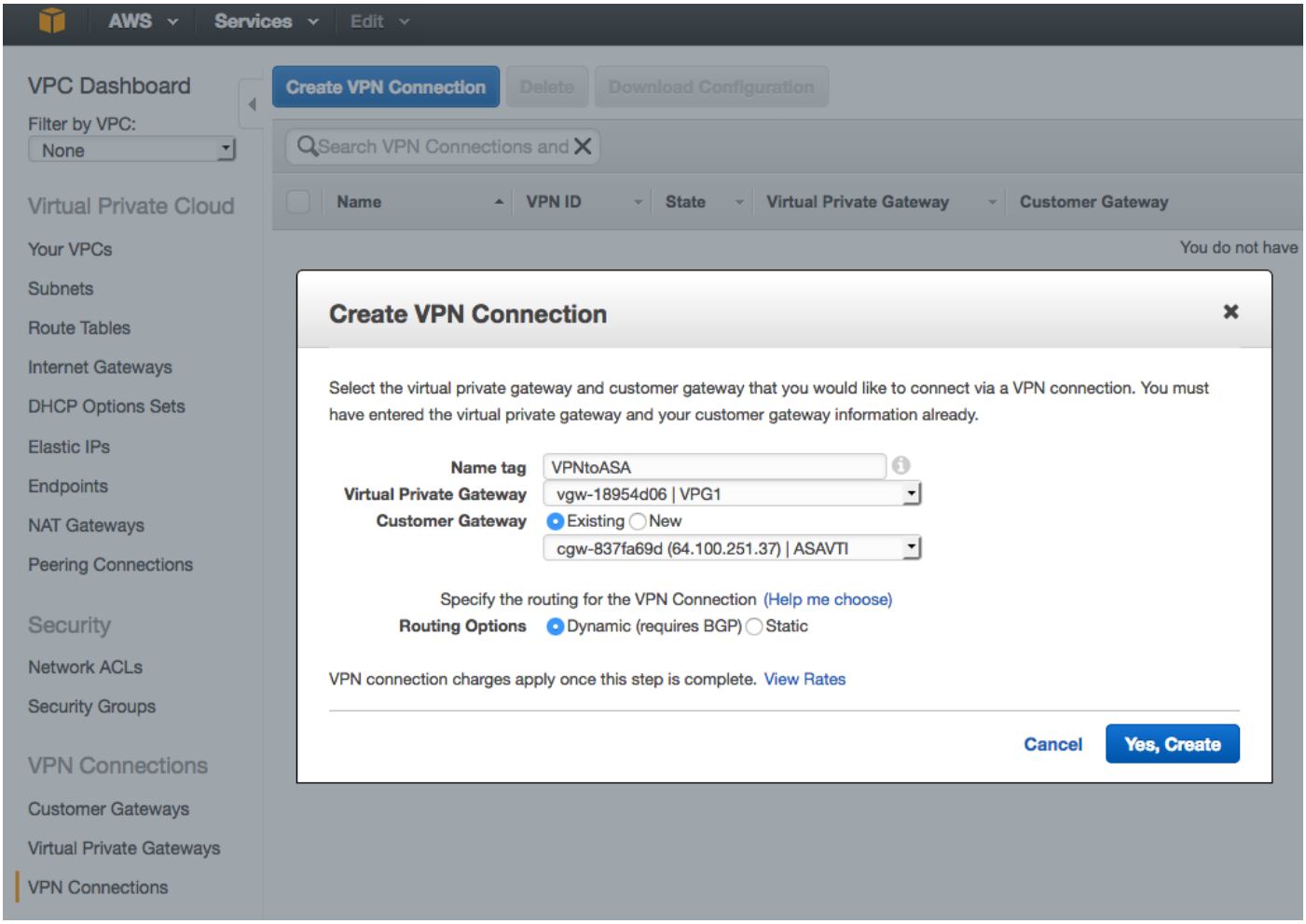


6단계.

VPN 연결을 생성합니다.

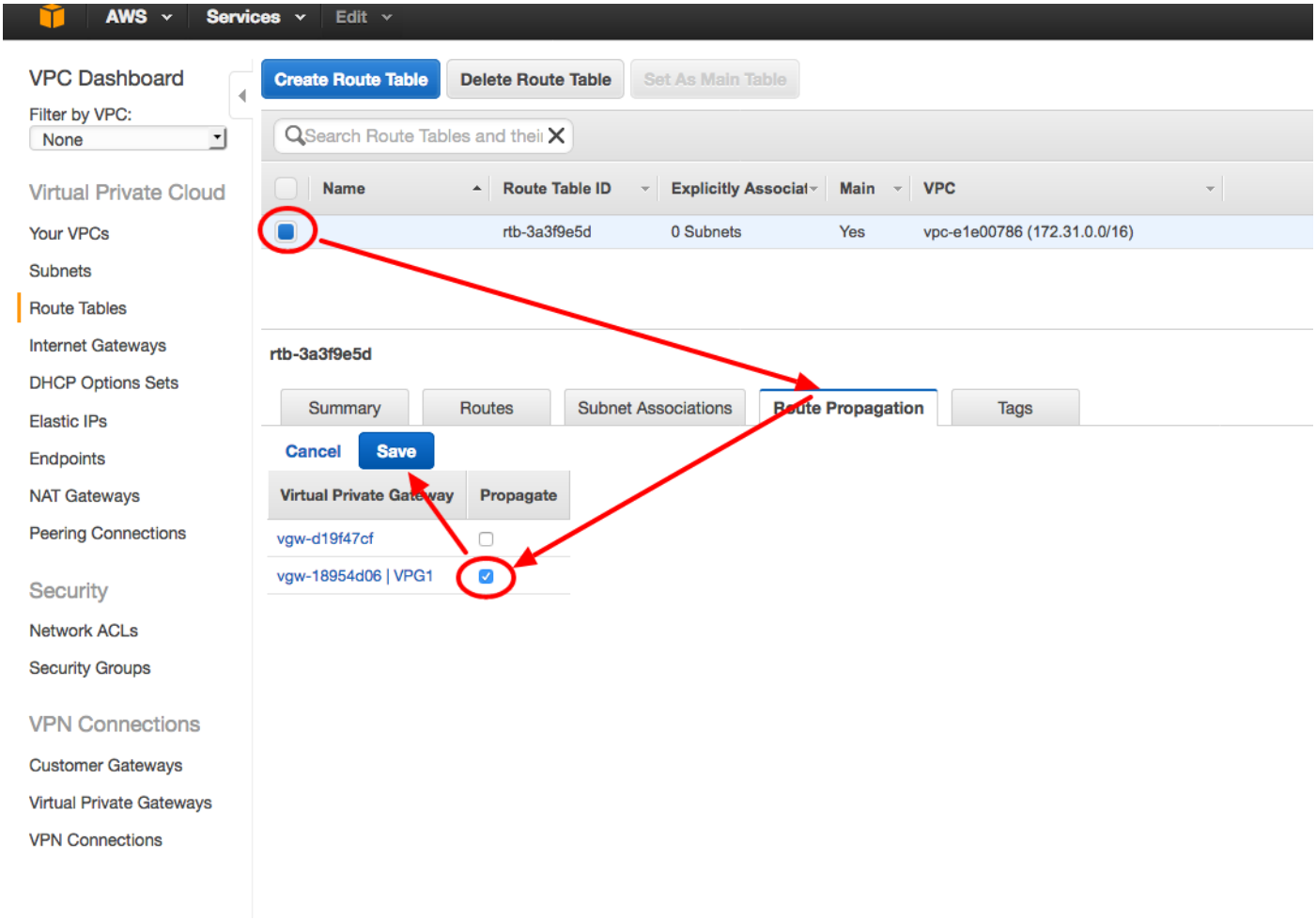


필드	**가치**
이름 태그	AWS와 ASA 간 VPN 연결의 사람이 읽을 수 있는 태그.
가상 프라이빗 게이트웨이	방금 생성한 VPG를 선택합니다.
고객 게이트웨이	Existing(**기존**) 라디오 버튼을 클릭하고 ASA의 게이트웨이를 선택합니다.
라우팅 옵션	Dynamic(**BGP 필요**) 라디오 버튼을 클릭합니다.



7단계.

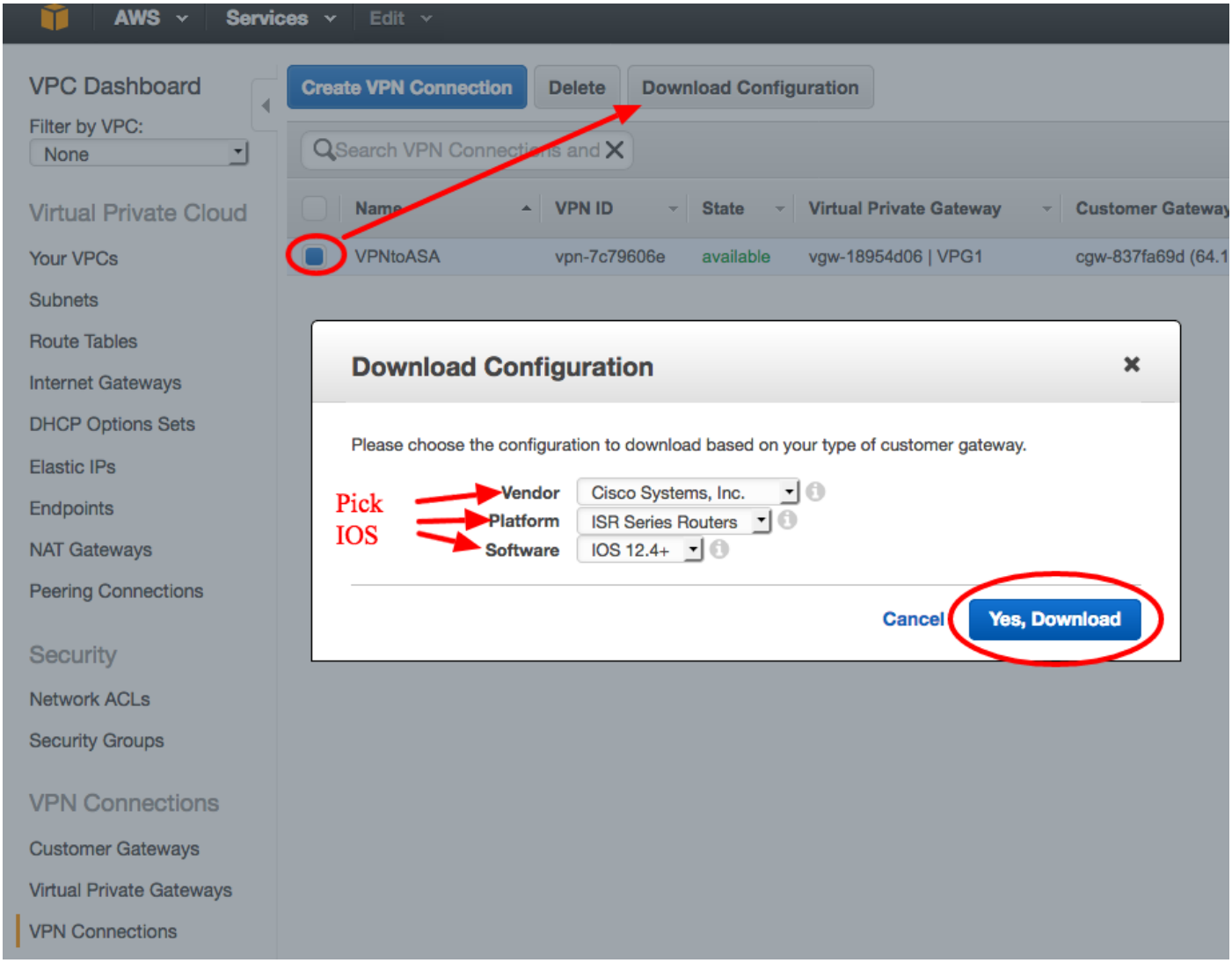
VPG(BGP를 통해)에서 학습한 경로를 VPC로 전파하도록 경로 테이블을 구성합니다.



8단계.

제안된 컨피그레이션을 다운로드합니다. VTI 스타일 컨피그레이션인 컨피그레이션을 생성하려면 아래 값을 선택합니다.

필드	**가치**
공급업체	Cisco Systems, Inc.
플랫폼	ISR Series 라우터
소프트웨어	IOS 12.4+



ASA 구성

컨피그레이션을 다운로드하면 몇 가지 변환이 필요합니다.

1단계.

crypto isakmp policy를 crypto ikev1 policy로 변환 정책 200 및 정책 201이 동일하므로 하나의 정책만 필요합니다.

권장 구성

```
crypto isakmp policy 200
  aes 128

  2
  28800
  sha

crypto isakmp policy 201
  aes 128

  2
```

받는 사람

```
crypto ikev1
crypto ikev1   10

  aes
  sha
  2
  28800
```

```
  28800
  sha
```

2단계.

crypto ipsec transform-set를 crypto ipsec ikev1 transform-set로 설정합니다. 두 변형 집합이 동일하므로 하나의 변형 집합만 필요합니다.

권장 구성	받는 사람
`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-AWS esp-aes esp-sha-hmac`

3단계.

crypto ipsec 프로필에 대한 암호화 ipsec 프로필. 두 프로파일이 동일하므로 하나의 프로파일만 필요합니다.

권장 구성	받는 사람

`crypto ipsec ipsec-vpn-7c79606e-0`
` pfs 2`
` security-association 3600`
` set transform-set ipsec-prop-vpn-7c79606e-0`
	`crypto ipsec AWS`
	` ikev1 transform-set AWS`
	` pfs 2`
	` security-association 3600`

`crypto ipsec ipsec-vpn-7c79606e-1`
` pfs 2`
` security-association 3600`
` set transform-set ipsec-prop-vpn-7c79606e-1`	

4단계.

crypto keyring 및 crypto isakmp 프로필을 각 터널에 대해 tunnel-group으로 변환해야 합니다.

권장 구성	받는 사람

`crypto keyring keyring keyring-vpn-7c79606e-0`
`  64.100.251.37`
`  52.34.205.227 QZhh90Bjf`
`!`
`crypto isakmp profile isakmp-vpn-7c79606e-0`
`  64.100.251.37`
` ID 52.34.205.227`
` keyring keyring-vpn-7c79606e-0`
`!`
`crypto keyring keyring keyring-vpn-7c79606e-1`
`  64.100.251.37`
	`  52.34.205.227`
	`ipsec-l2l`
	`  52.34.205.227`
	`ipsec`
	` ikev1 QZhh90`
	` isakmp keepaliv`
	`10 10`
	`  52.37.194.219`
	`ipsec-l2l`
	`  52.37.194.219`
	`ipsec`
	` ikev1 JjxCWy`
	` isakmp keepaliv`

```
     52.37.194.219  JjxCWy4Ae

!
crypto isakmp profile isakmp-vpn-7c79606e-1                    10  10
   64.100.251.37
 ID  52.37.194.219
 keyring keyring-vpn-7c79606e-1
```

5단계.

터널 구성이 거의 동일합니다.ASA는 ip tcp adjust-mss 또는 ip virtual-reassembly 명령을 지원하지 않습니다.

권장 구성

```
 1
 ip  169.254.13.190 255.255.255.252
 ip virtual reassembly
   64.100.251.37
   52.34.205.227
   ipsec ipv4
   ipsec  ipsec-vpn-7c79606e-0
 ip tcp adjust-mss 1387



!
 2
 ip  169.254.12.86 255.255.255.252
 ip virtual reassembly
   64.100.251.37
   52.37.194.219
   ipsec ipv4
   ipsec  ipsec-vpn-7c79606e-1
 ip tcp adjust-mss 1387
```

받는 사람

```
 1
 AWS1
 ip  169.254.13.190
255.255.255.252

   52.34.205.227
   ipsec ipv4
   ipsec  AWS
!
 2
 AWS2
 ip  169.254.12.86
255.255.255.252

   52.37.194.219
   ipsec ipv4
   ipsec  AWS
```

6단계.

이 예에서 ASA는 내부 서브넷(192.168.1.0/24)만 광고하고 AWS(172.31.0.0/16)에서 서브넷을 수신합니다.

권장 구성

```
 bgp 65000
 neighbor 169.254.13.189 remote-as 7224
   169.254.13.189
  169.254.13.189  10 30 30
  ipv4
  neighbor 169.254.13.189 remote-as 7224
   169.254.13.189  10 30 30
  neighbor 169.254.13.189 default-originate
    169.254.13.189
   169.254.13.189
   0.0.0.0
```

받는 사람

```
 bgp 65000
 bgp log-neighbor-changes
  bgp 10 30 0
  ipv4
  neighbor 169.254.12.85
remote-as 7224
    169.254.12.85
  neighbor 169.254.13.189
remote-as 7224
    169.254.13.189
   192.168.1.0
```

```
 bgp 65000
 neighbor 169.254.12.85 remote-as 7224
   169.254.12.85
  169.254.12.85  10 30 30
  ipv4
  neighbor 169.254.12.85 remote-as 7224
   169.254.12.85  10 30 30                          exit address-family
  neighbor 169.254.12.85 default-originate
    169.254.12.85
   169.254.12.85
   0.0.0.0
```

확인 및 최적화

1단계.

ASA가 AWS의 두 엔드포인트와 IKEv1 보안 연결을 설정하는지 확인합니다.SA의 상태는 MM_ACTIVE여야 합니다.

```
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#
```

2단계.

ASA에 IPsec SA가 설치되어 있는지 확인합니다.각 피어에 대해 인바운드 및 아웃바운드 SPI가 설치되어 있어야 하며 일부 캡슐화 및 decaps 카운터가 증가해야 합니다.

```
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
```

3단계.

ASA에서 BGP 연결이 AWS로 설정되었는지 확인합니다. State/PfxRcd 카운터는 1이어야 합니다. AWS가 172.31.0.0/16 서브넷을 ASA로 광고하기 때문입니다.

```
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
```

4단계.

ASA에서 172.31.0.0/16에 대한 경로가 터널 인터페이스를 통해 학습되었는지 확인합니다. 이 출력은 피어 169.254.12.85 및 169.254.13.189에서 172.31.0.0 경로가 두 개 있음을 보여 줍니다. 하위 메트릭 때문에 터널 2(AWS2)를 169.254.13.189 경로가 우선합니다.

```
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
```

5단계.

AWS에서 반환되는 트래픽이 대칭 경로를 따르도록 하려면 경로 맵을 구성하여 기본 경로와 일치시키고 BGP를 조정하여 알려진 경로를 변경합니다.

```
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
```

6단계.

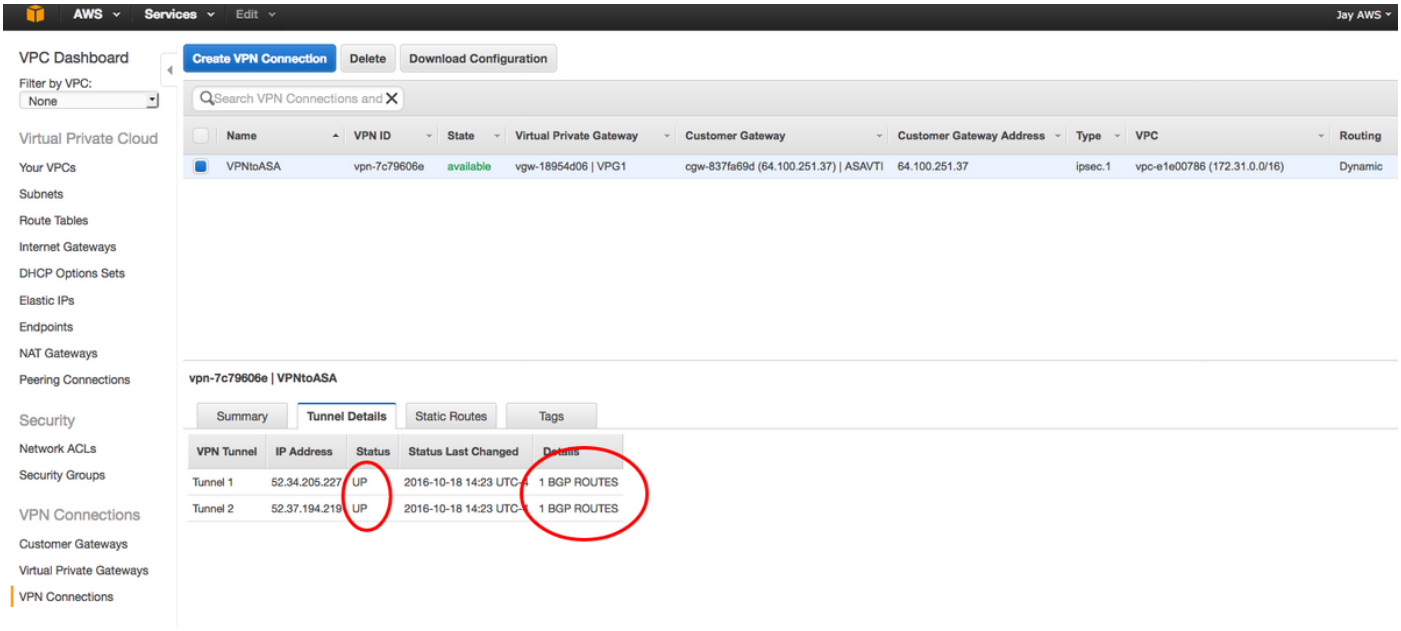
ASA에서 192.168.1.0/24이 AWS에 알려졌는지 확인합니다.

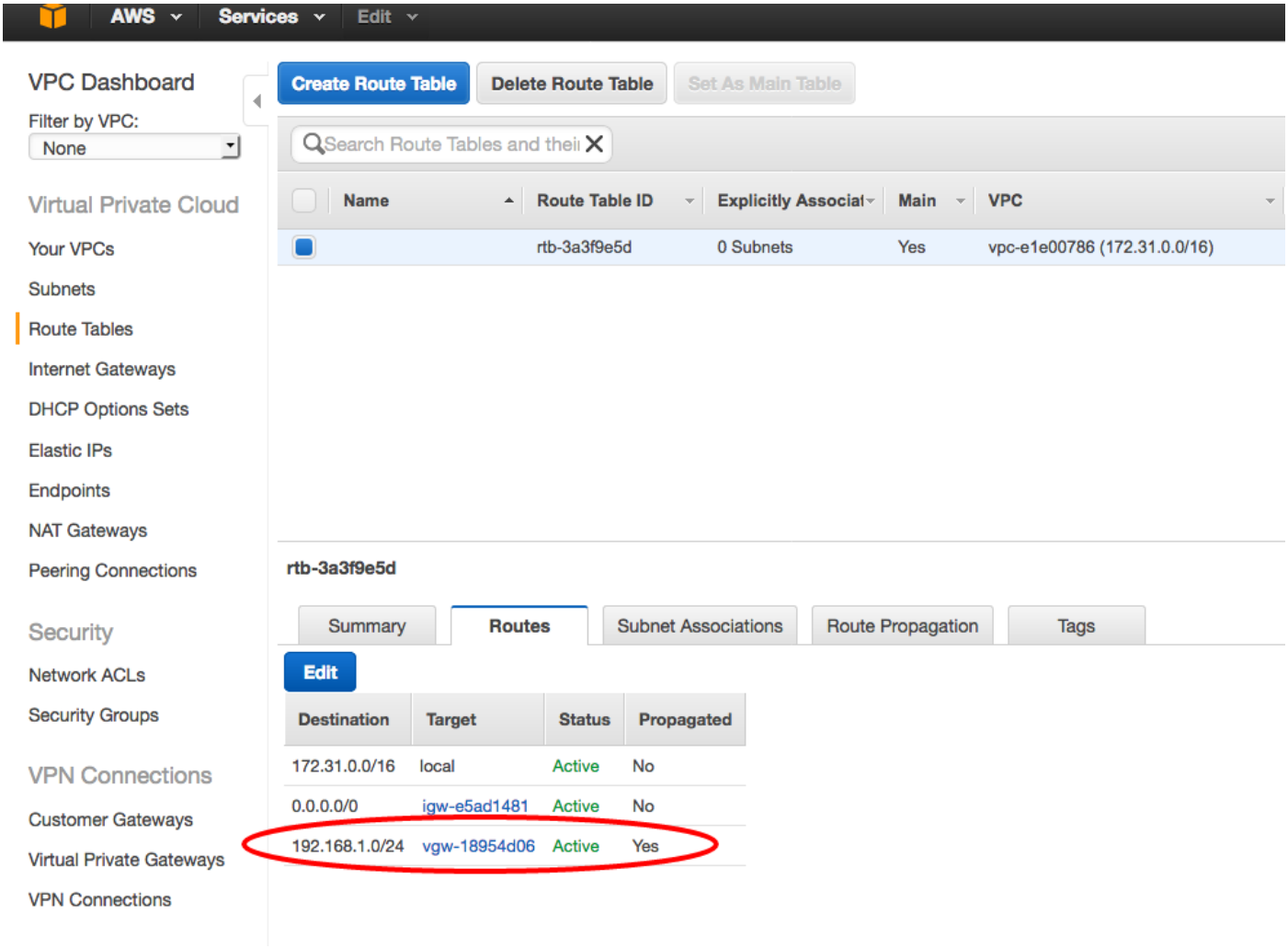
```
ASA# show bgp neighbors 169.254.12.85 advertised-routes

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
```

7단계.

AWS에서 VPN 연결에 대한 터널이 UP이고 피어에서 경로를 학습하는지 확인합니다. 또한 경로가 라우팅 테이블로 전파되었는지 확인합니다.




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