配置ASA IPsec VTI連線Amazon Web Services

目錄

簡介

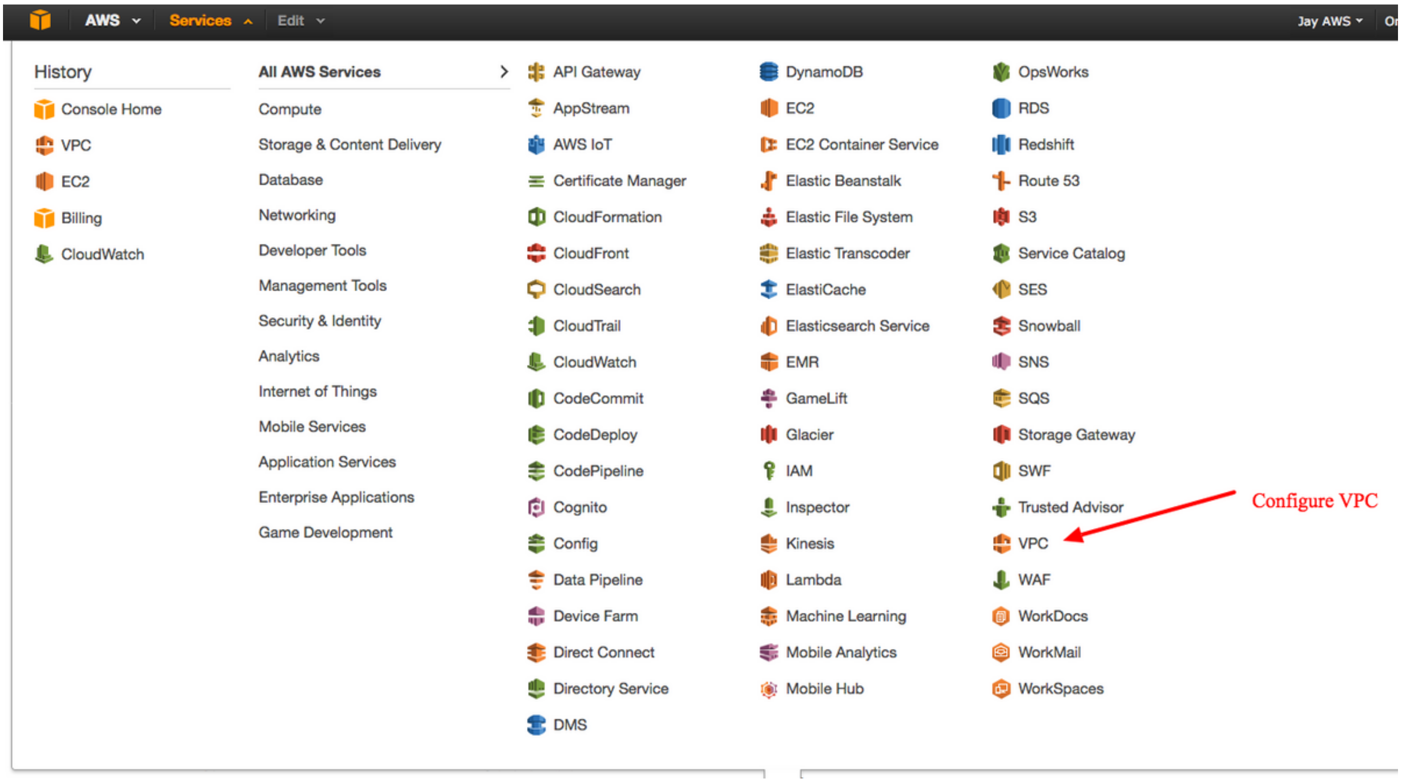
本文說明如何設定調適型安全裝置(ASA)IPsec虛擬通道介面(VTI)連線。在ASA 9.7.1中，引入了IPsec VTI。 在此版本中，它限於使用IKEv1透過IPv4進行sVTI IPv4。 這是ASA連線到Amazon Web Services(AWS)的配置示例。

> **附註**：目前，僅在單情景路由模式下支援VTI。

配置AWS

步驟1.

登入到AWS控制檯並導航到VPC面板。

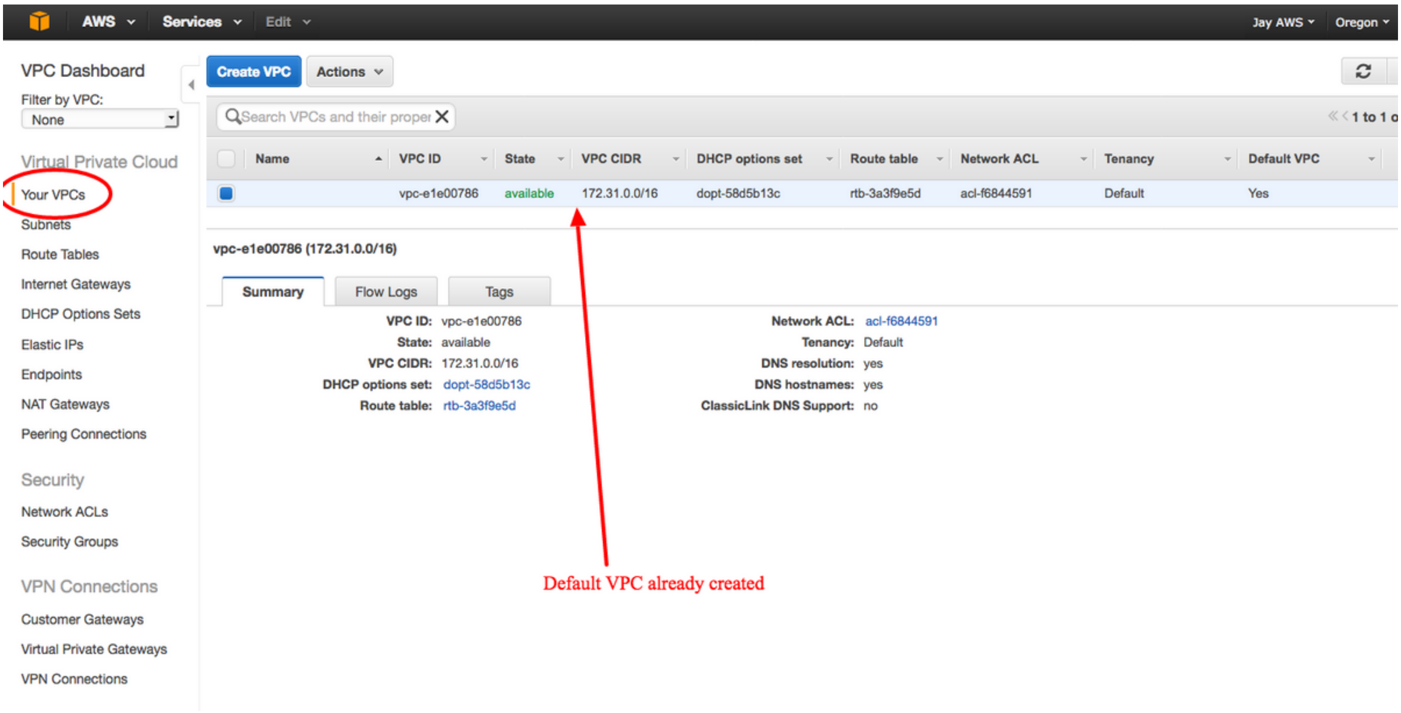


Configure VPC

導航到VPC控制面板

步驟2.

確認已建立虛擬私有雲(VPC)。 預設情況下，會建立具有172.31.0.0/16的VPC。這就是虛擬機器(VM)的附加位置。



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
State: available
VPC CIDR: 172.31.0.0/16
DHCP options set: dopt-58d5b13c
Route table: rtb-3a3f9e5d

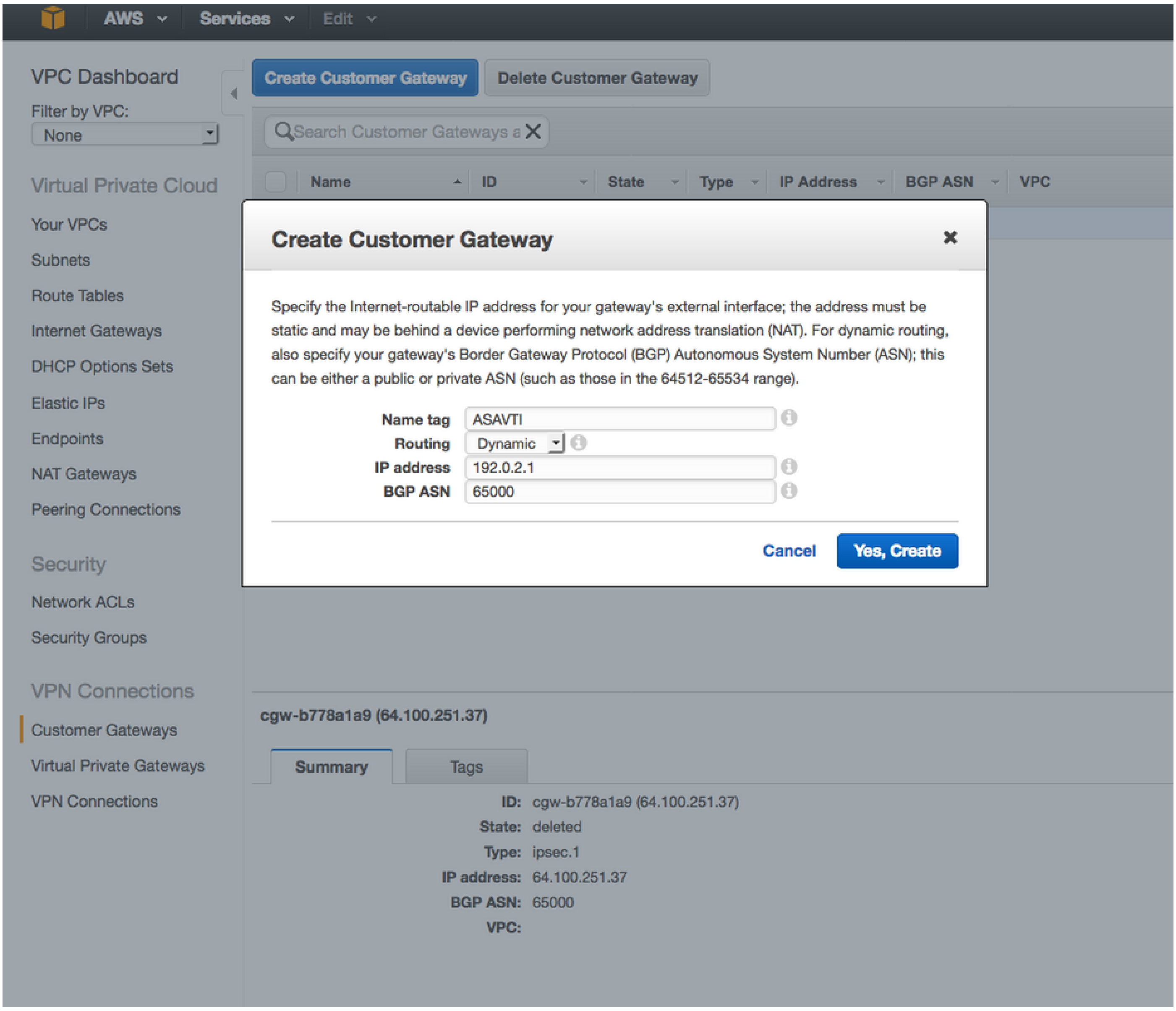
Network ACL: acl-f6844591
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

Default VPC already created

步驟3.

建立「客戶網關」。 這是一個表示ASA的端點。

欄位	**價值**
名稱標籤	這是一個用於識別ASA的可讀名稱。
路由	動態 — 這表示將使用邊界閘道通訊協定(BGP)來交換路由資訊。
IP 位址	這是ASA外部介面的公共IP地址。
BGP ASN	在ASA上運行的BGP進程的自治系統(AS)編號。除非您的組織具有公共AS編號，否則使用6500



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

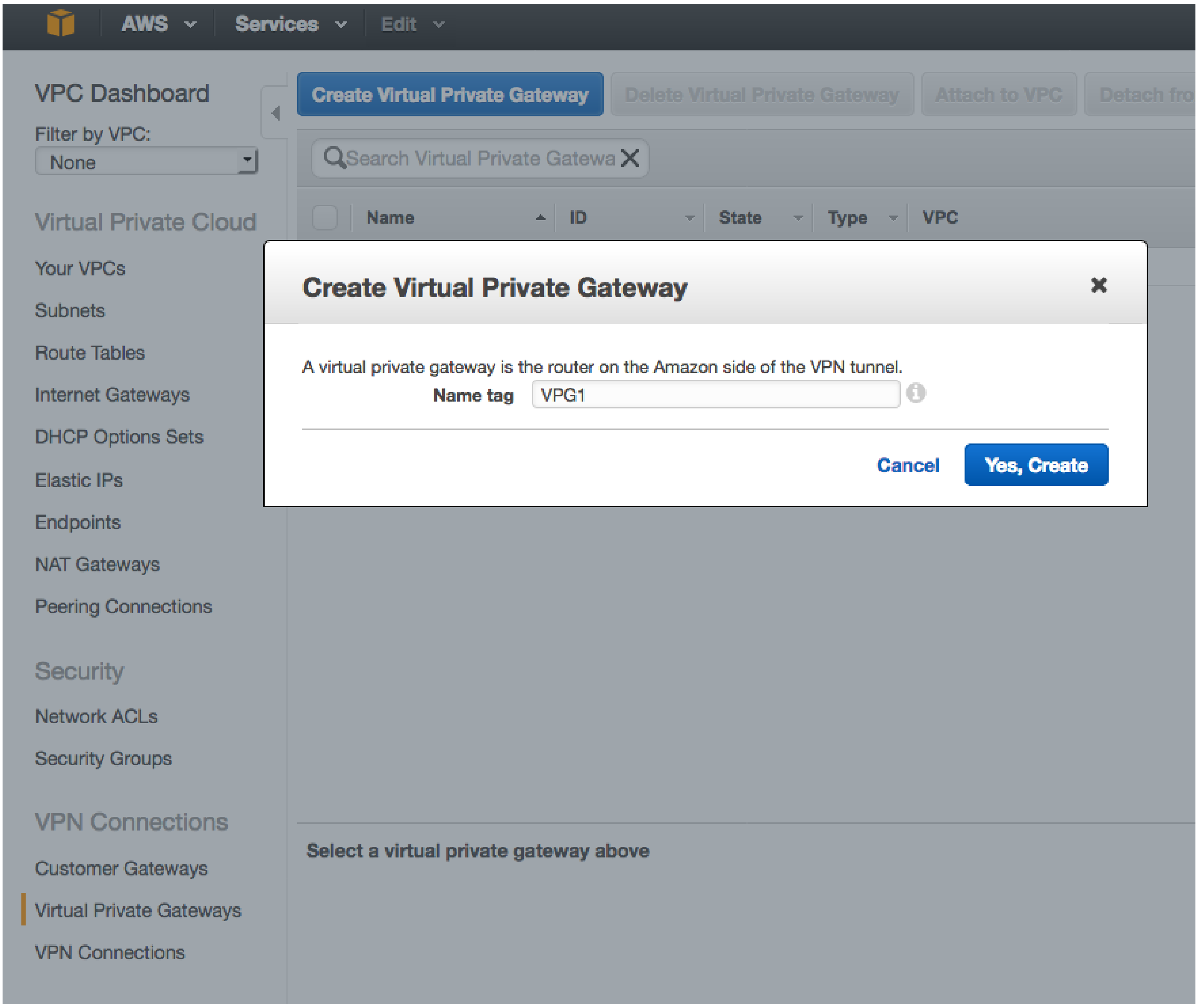
cgw-b778a1a9 (64.100.251.37)

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

步驟4.

建立虛擬私人閘道(VPG)。 這是由AWS託管的終止IPsec隧道的模擬路由器。

欄位	**價值**
名稱標籤	用於識別VPG的可讀名稱。



Create Virtual Private Gateway

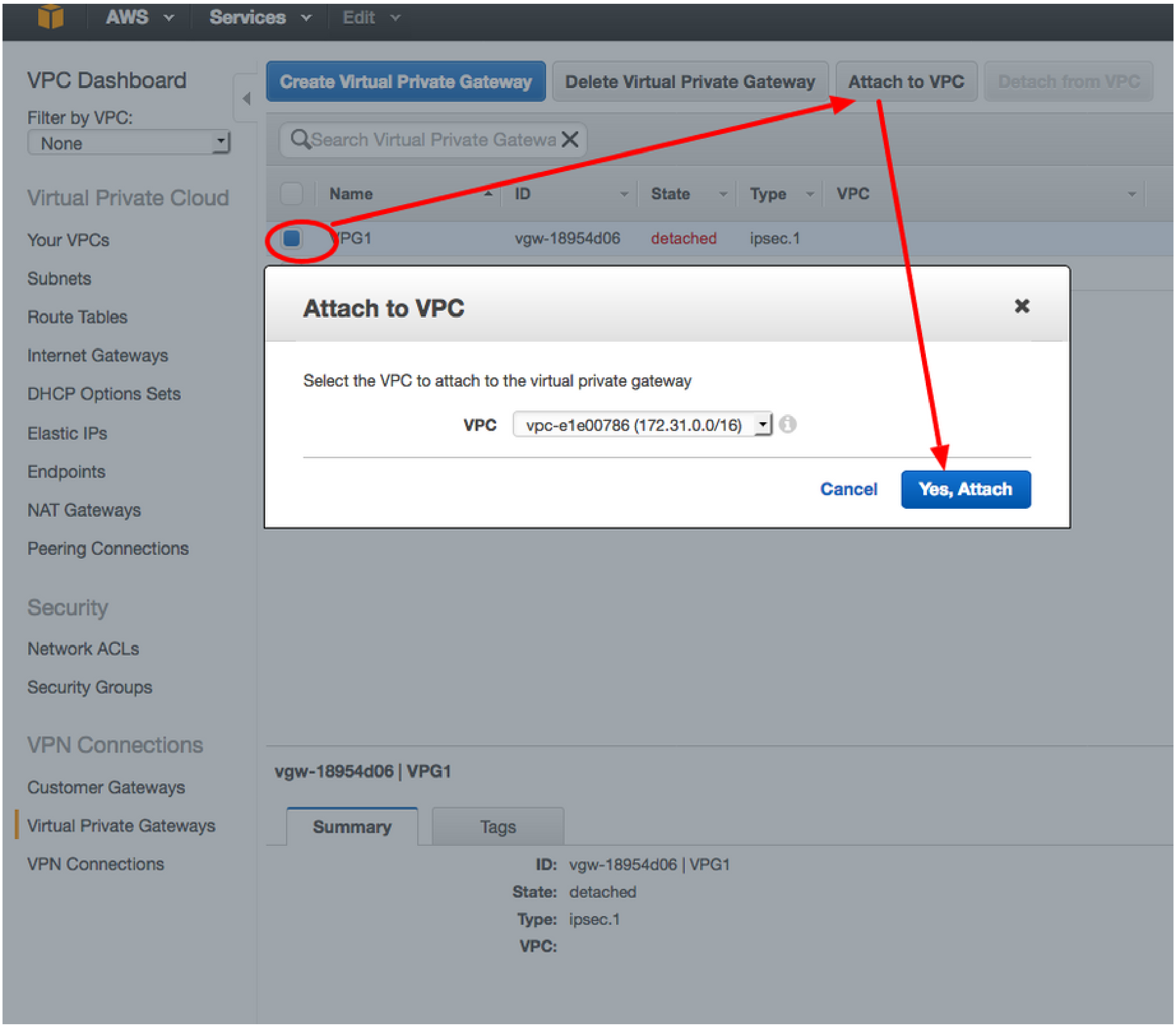
A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag: VPG1

步驟5.

將VPG連線到VPC。

選擇Virtual Private Gateway，按一下**Attach to VPC**，從VPC下拉選單中選擇VPC，然後按一下**Yes， Attach**。



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

Attach to VPC

Select the VPC to attach to the virtual private gateway

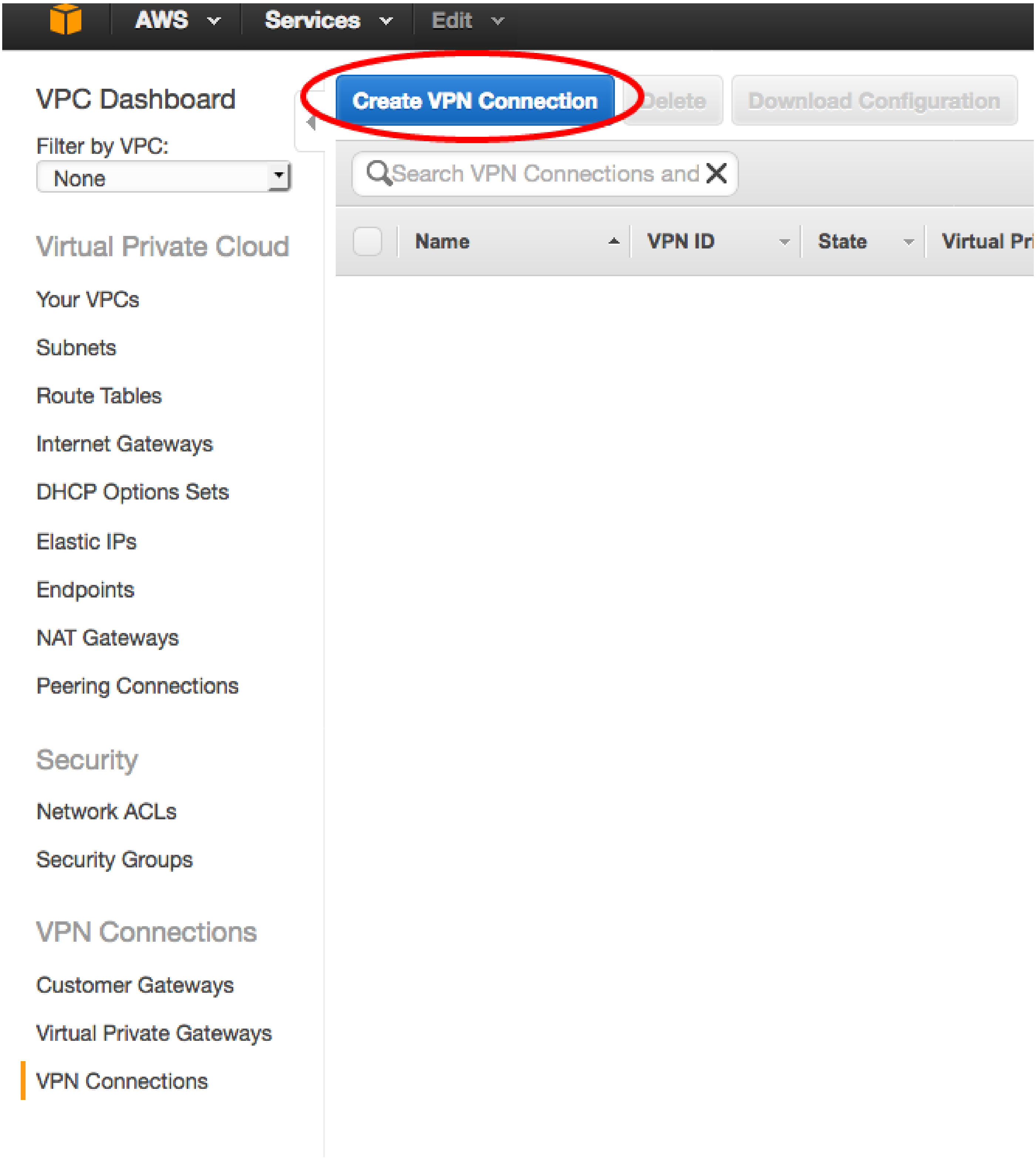
VPC vpc-e1e00786 (172.31.0.0/16)

vgw-18954d06 | VPG1

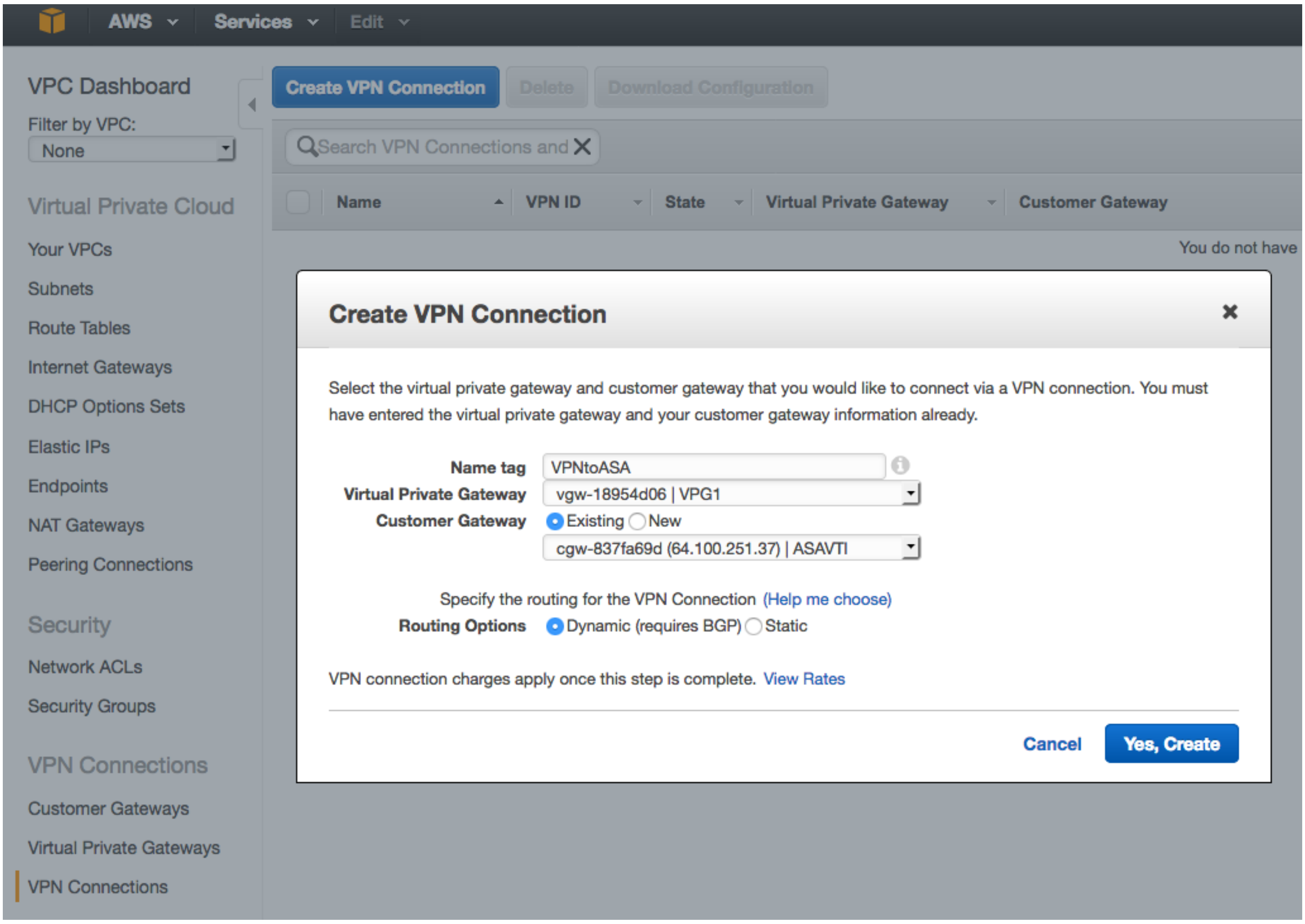
ID: vgw-18954d06 | VPG1
State: detached
Type: ipsec.1
VPC:

步驟6.

建立VPN連線。



欄位	**價值**
名稱標籤	AWS和ASA之間的VPN連線的可讀標籤。
虛擬私人閘道	選擇剛建立的VPG。
客戶閘道	按一下**Existing**單選按鈕，然後選擇ASA的網關。
路由選項	按一下「**Dynamic(requires BGP)**」單選按鈕。



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

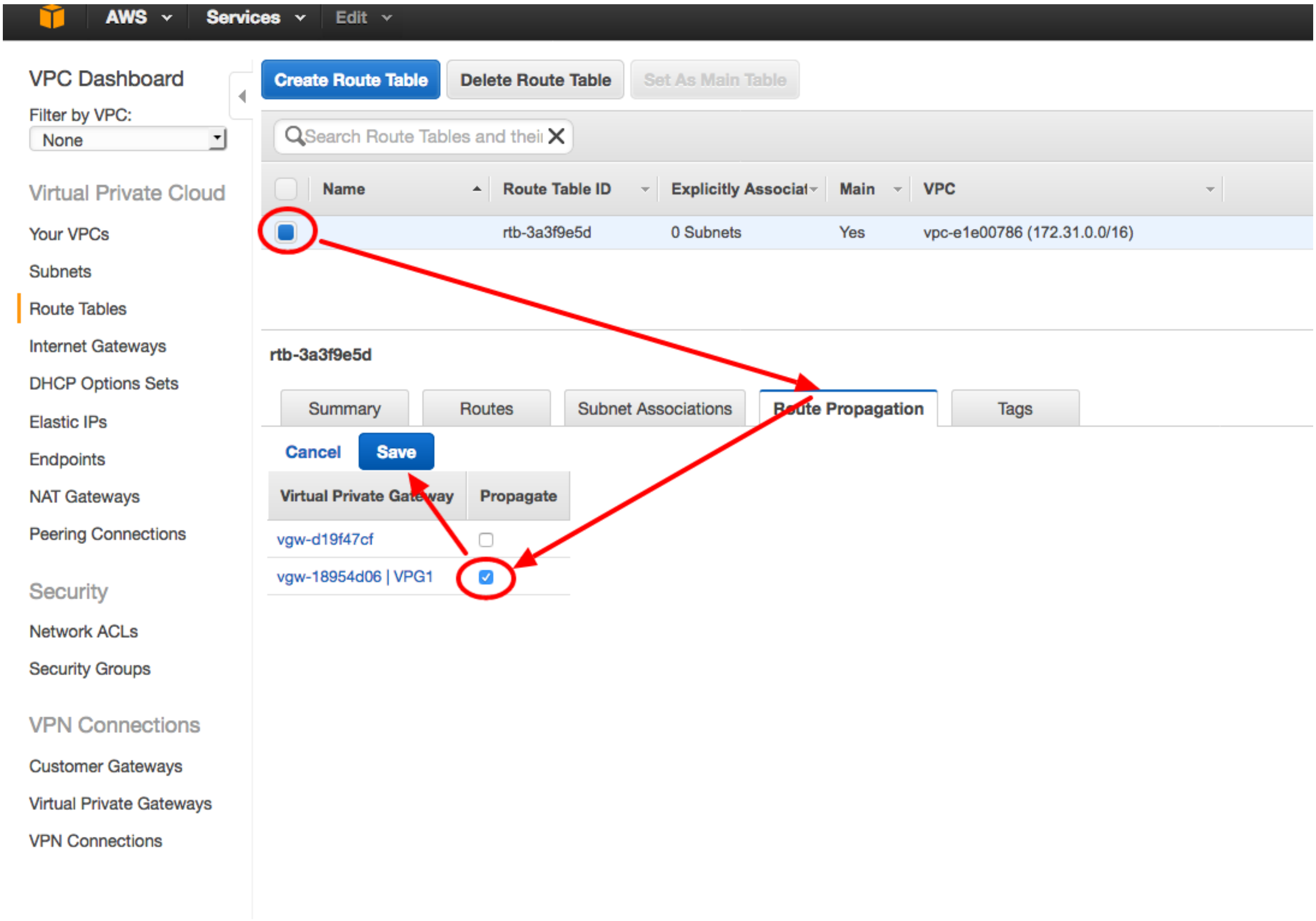
Specify the routing for the VPN Connection (Help me choose)

Routing Options: ● Dynamic (requires BGP) ○ Static

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

步驟7.

配置路由表以將從VPG（通過BGP）獲知的路由傳播到VPC。



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

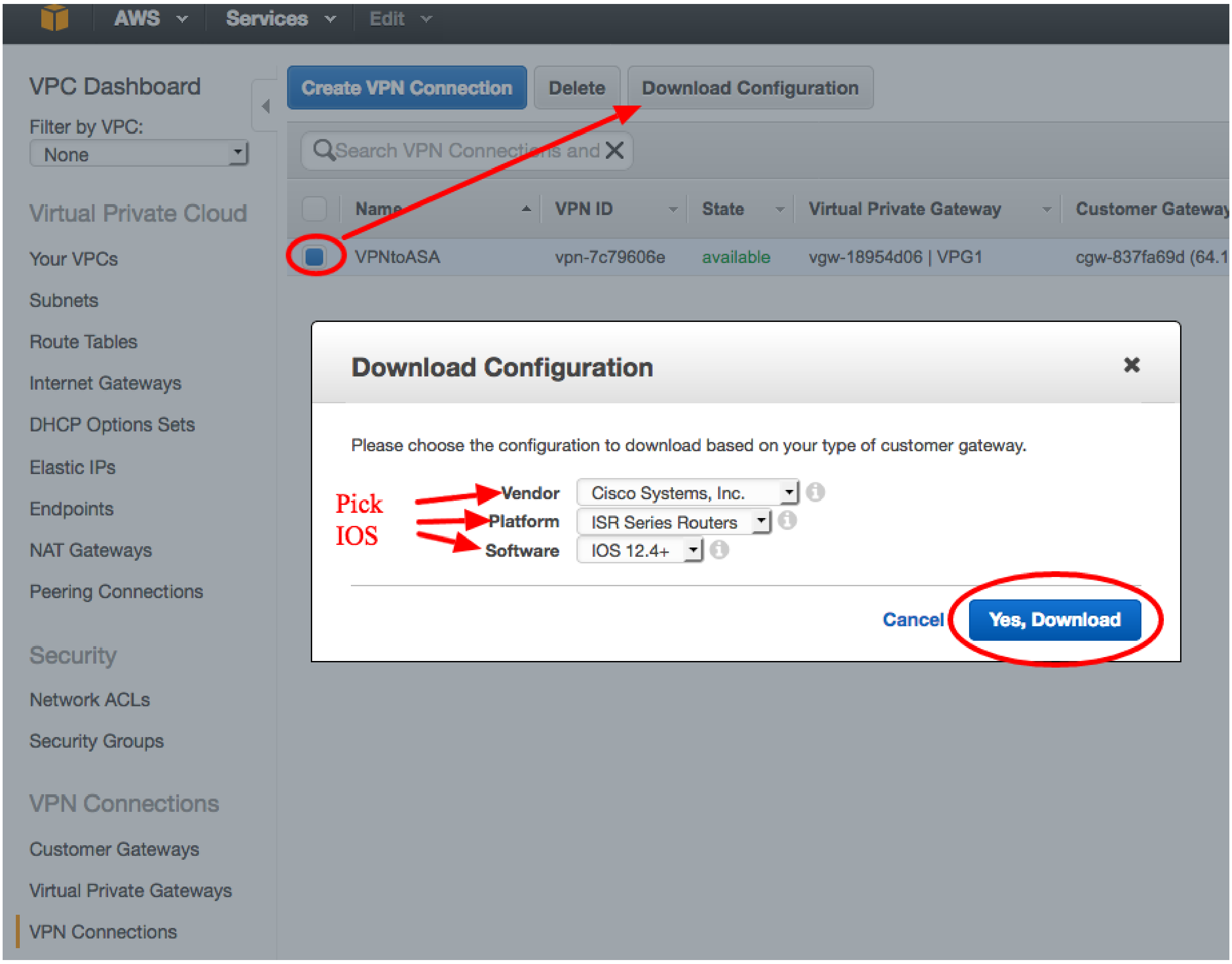
rtb-3a3f9e5d

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

步驟8.

下載建議的配置。 選擇以下值，以生成VTI樣式配置的配置。

欄位	**價值**
供應商	Cisco Systems, Inc.
平台	ISR系列路由器
軟體	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+

配置ASA

下載組態後，需要進行某些轉換。

步驟1.

crypto isakmp policy to crypto ikev1 policy。 只需要一個策略，因為策略200和策略201是相同的。

建議的配置

```
crypto isakmp policy 200
 aes 128

 2
 lifetime 28800
 hash sha
exit
crypto isakmp policy 201
 aes 128

 2
 lifetime 28800
```

成長至

```
crypto ikev1 enable outside
crypto ikev110

 aes
 hash sha
 2
 lifetime 28800
 hash sha
exit
```

步驟2.

crypto ipsec transform-set到crypto ipsec ikev1 transform-set。 只需要一個轉換集，因為兩個轉換集是相同的。

建議的配置

```
crypto ipsec transform-set ipsec-prop-vpn-
7c79606e-0 esp-aes 128 esp-sha-hmac

exit
crypto ipsec transform-set ipsec-prop-vpn-
7c79606e-1 esp-aes 128 esp-sha-hmac

exit
```

成長至

```
crypto ipsec ikev1 transform-
AWS esp-aes esp-sha-hmac
```

步驟3.

crypto ipsec profile to crypto ipsec profile。 由於兩個配置檔案相同，因此只需要一個配置檔案。

建議的配置

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

成長至

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

步驟4.

需要將每個通道的加密金鑰環和加密isakmp配置檔案轉換為隧道組配置檔案。

建議的配置

```
crypto keyring keyring-vpn-7c79606e-0
 local-address 64.100.251.37
 52.34.205.227QZhh90Bjf
exit
!
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
 exit
!
crypto keyring keyring-vpn-7c79606e-1
 local-address 64.100.251.37
```

成長至

```
tunnel-group
52.34.205.227 type
ipsec-l2l
tunnel-group
52.34.205.227 ipsec-
attributes
 ikev1QZhh90Bjf
 isakmp keepalive10
tunnel-group
52.37.194.219 type
ipsec-l2l
tunnel-group
52.37.194.219 ipsec-
```

```
 52.37.194.219JjxCWy4Ae
 exit
!
crypto isakmp profile isakmp-vpn-7c79606e-1
 local-address 64.100.251.37
 match identity address 52.37.194.219
 keyring keyring-vpn-7c79606e-1
 exit
```

```
attributes
 ikev1JjxCWy4Ae
 isakmp keepalive10
```

步驟5.

通道組態幾乎完全相同。ASA不支援ip tcp adjust-mss或ip virtual-reassembly命令。

建議的配置

```
interface 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
 exit
!
2
 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
 exit
```

成長至

```
interface Tunnel1
 nameif AWS1
 ip address 169.254.13.190
255.255.255.252

 52.34.205.227
 ipsec ipv4
 tunnel protection ipsec profi
AWS
!
2
 nameif AWS2
 ip address 169.254.12.86
255.255.255.252

 52.37.194.219
 ipsec ipv4
 tunnel protection ipsec profi
AWS
```

步驟6.

在本示例中，ASA將僅通告內部子網(192.168.1.0/24)並在AWS(172.31.0.0/16)內接收該子網。

建議的配置

```
router bgp 65000
 neighbor 169.254.13.189 remote-as 7224
 neighbor 169.254.13.189 activate
 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
  neighbor 169.254.13.189 default-originate
  neighbor 169.254.13.189 activate
  neighbor 169.254.13.189 soft-reconfiguration
inbound
  0.0.0.0
  exit
```

成長至

```
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
activate
  neighbor 169.254.13.189
remote-as 7224
  neighbor 169.254.13.189
activate
  192.168.1.0
 exit
router bgp 65000
 neighbor 169.254.12.85 remote-as 7224
 neighbor 169.254.12.85 activate
 neighbor 169.254.12.85 timers 10 30 30
 address-family ipv4 unicast
  neighbor 169.254.12.85 remote-as 7224              no auto-summary
  neighbor 169.254.12.85 timers 10 30 30
  neighbor 169.254.12.85 default-originate          exit-address-family
  neighbor 169.254.12.85 activate
  neighbor 169.254.12.85 soft-reconfiguration
inbound
  0.0.0.0
  exit
 exit
```

驗證和最佳化

步驟1.

確認ASA與AWS的兩個終端建立IKEv1安全關聯。SA的狀態應為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#
```

步驟2.

確認ASA上安裝了IPsec SA。應該為每個對等裝置安裝入站和出站SPI，並且應該會增加一些encaps和decaps計數器。

```
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
```

步驟3.

在ASA上，確認已與AWS建立BGP連線。 當AWS向ASA通告172.31.0.0/16子網時，State/PfxRcd計數器應為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
```

步驟4.

在ASA上，驗證是否已通過隧道介面獲知到172.31.0.0/16的路由。 此輸出顯示，從對等點169.254.12.85和169.254.13.189到172.31.0.0有兩條路徑。由於度量較低，通向169.254.13.189外部隧道2(AWS2)的路徑是優先使用路徑。

```
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
```

步驟5.

為確保從AWS返回的流量遵循對稱路徑，請配置route-map以匹配首選路徑，並調整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
```

步驟6.

在ASA上，確認192.168.1.0/24已通告給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
```

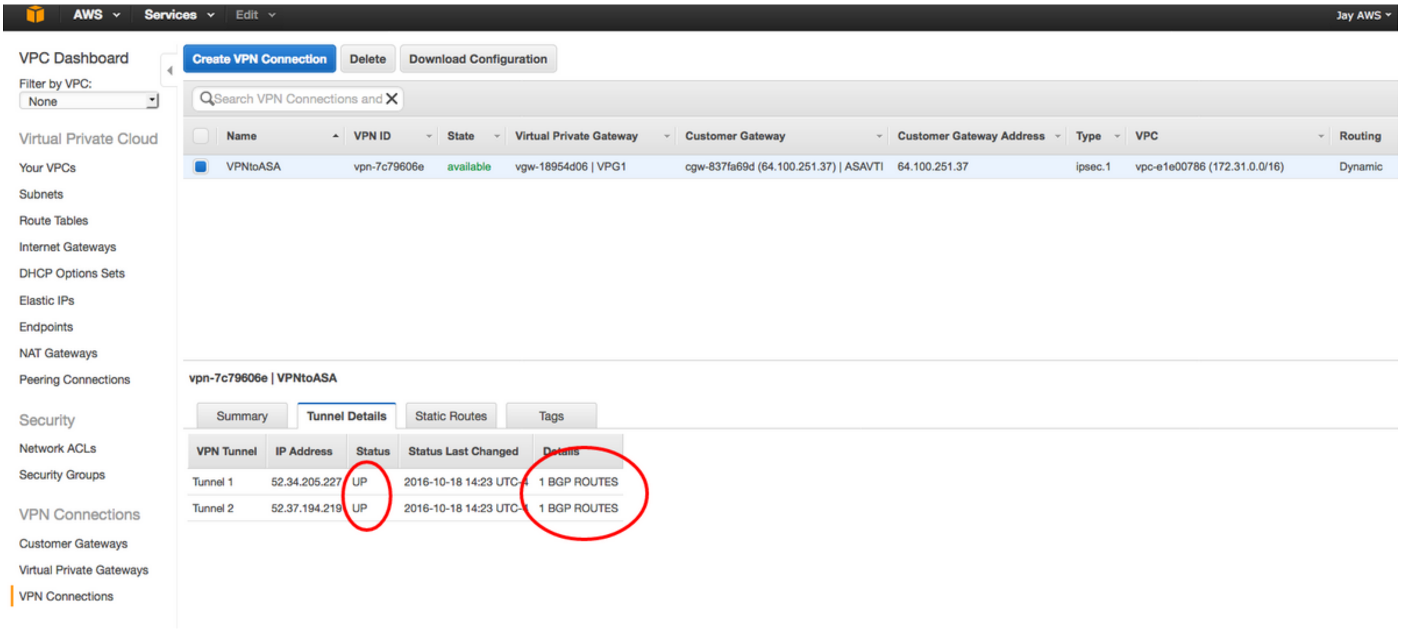
```
BGP table version is 5, local router ID is 192.168.1.55
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop         Metric LocPrf Weight  Path
*> 192.168.1.0      0.0.0.0               0         32768  i

Total number of prefixes 1
```

步驟7.

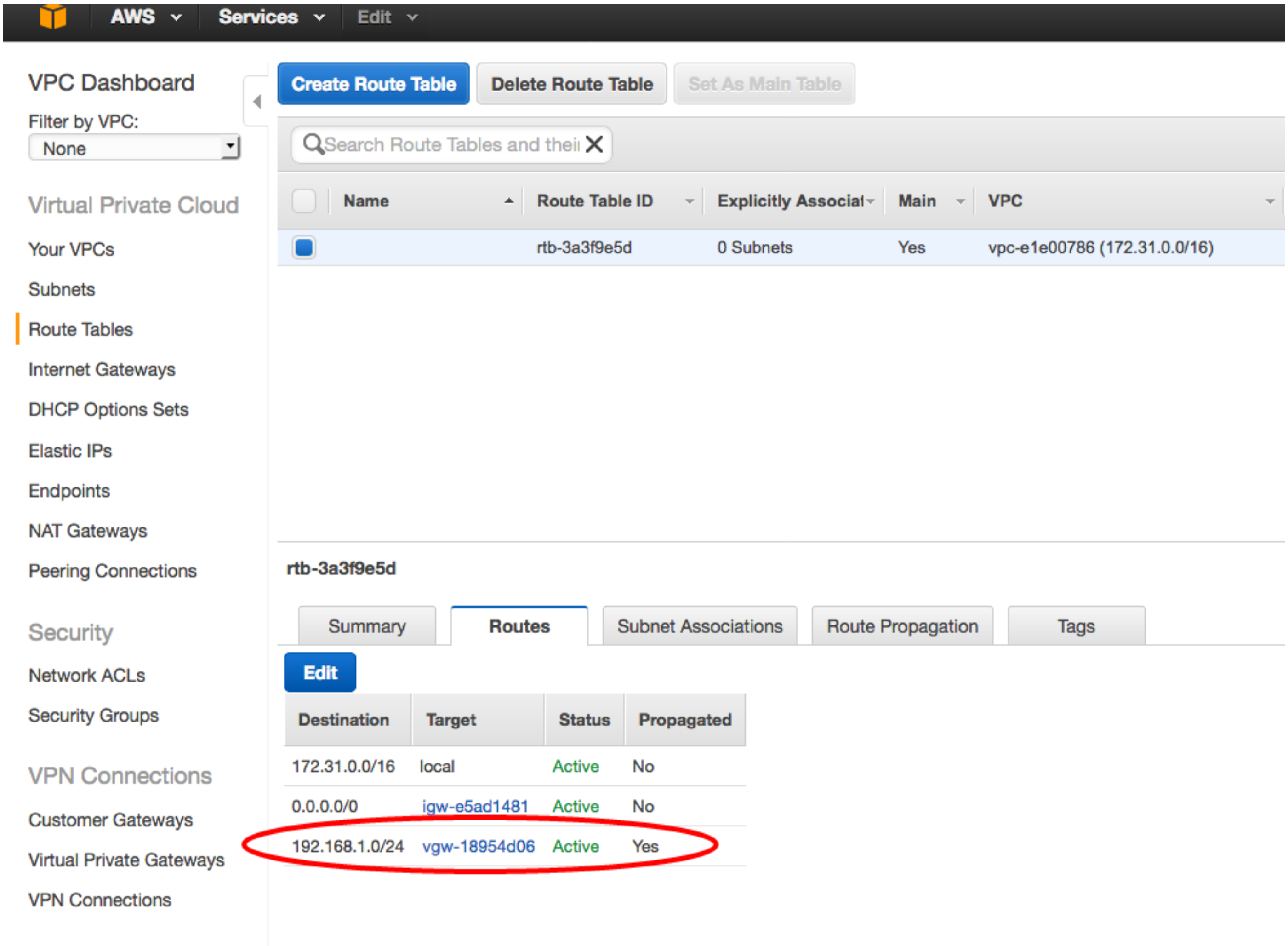
在AWS中，確認VPN連線的隧道為UP，並且路由是從對等項獲知的。 此外，檢查該路由是否已傳播到路由表中。



	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



	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