Configurazione della connessione ASA IPsec VTI Amazon Web Services

Sommario

[Introduzione](#)
[Configura AWS](#)
[Configurazione dell'ASA](#)
[Verifica e ottimizzazione](#)

Introduzione

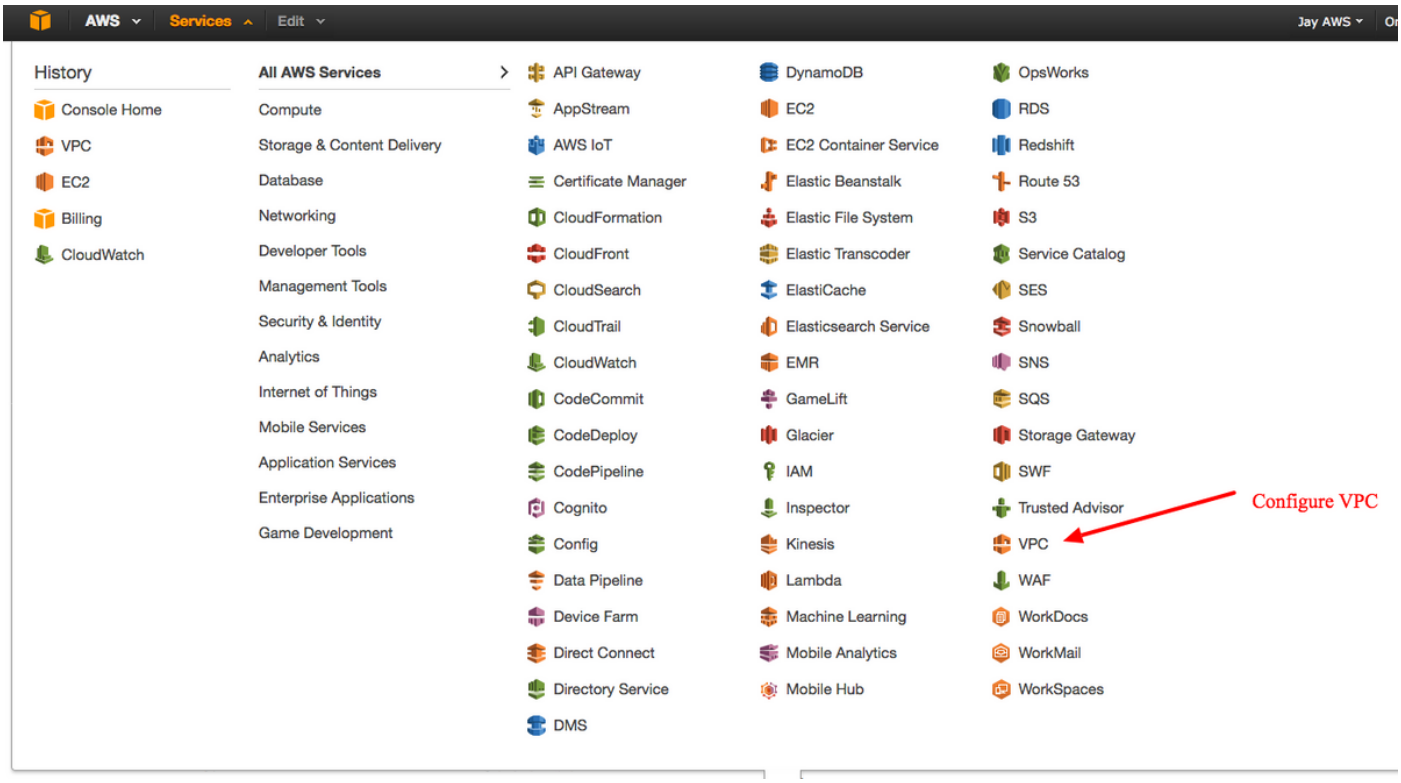
In questo documento viene descritto come configurare una connessione VTI (Virtual Tunnel Interface) IPsec di Adaptive Security Appliance (ASA). In ASA 9.7.1, è stata introdotta la VTI IPsec. In questa versione, è limitato a sVTI IPv4 su IPv4 che utilizza IKEv1. Questa è una configurazione di esempio per la connessione dell'ASA a Amazon Web Services (AWS).

> **Nota:** Attualmente VTI è supportato solo in modalità di routing a contesto singolo.

Configura AWS

Passaggio 1.

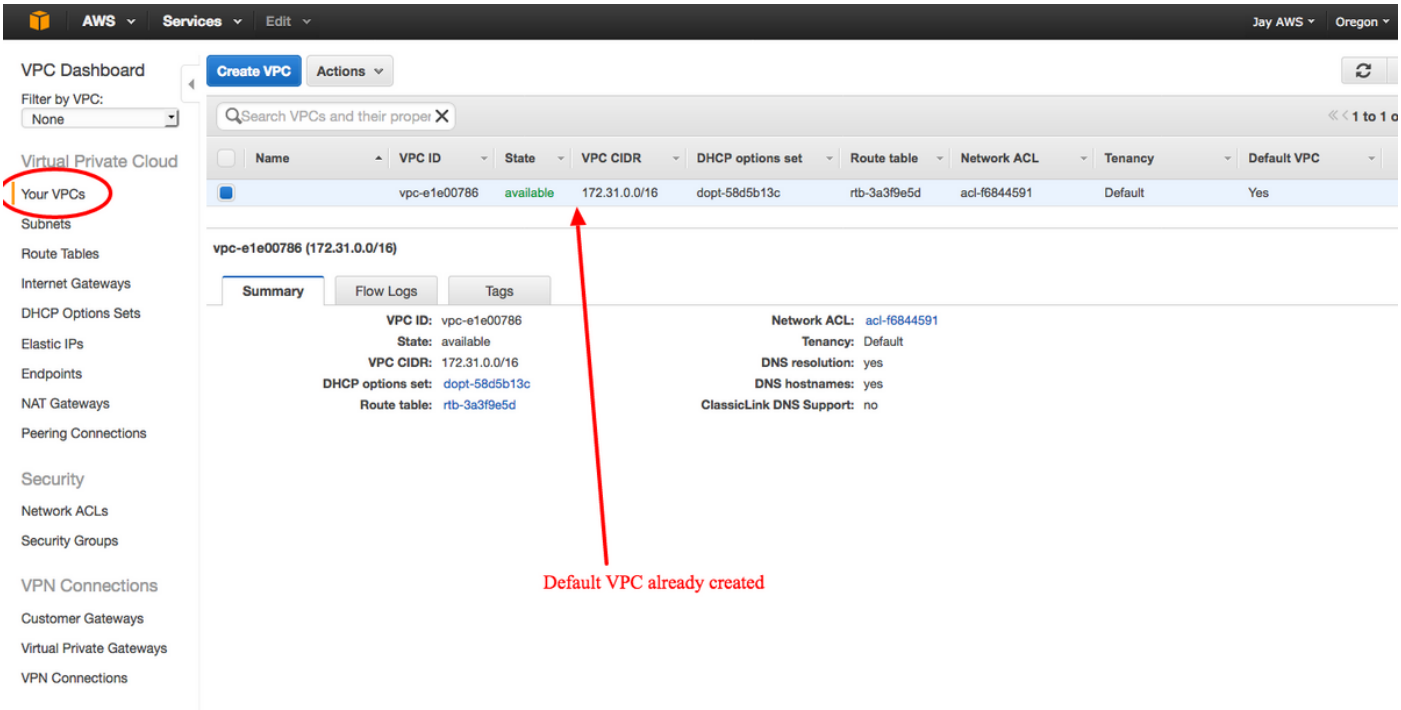
Accedere alla console AWS e selezionare il pannello VPC.



Passare al dashboard VPC

Passaggio 2.

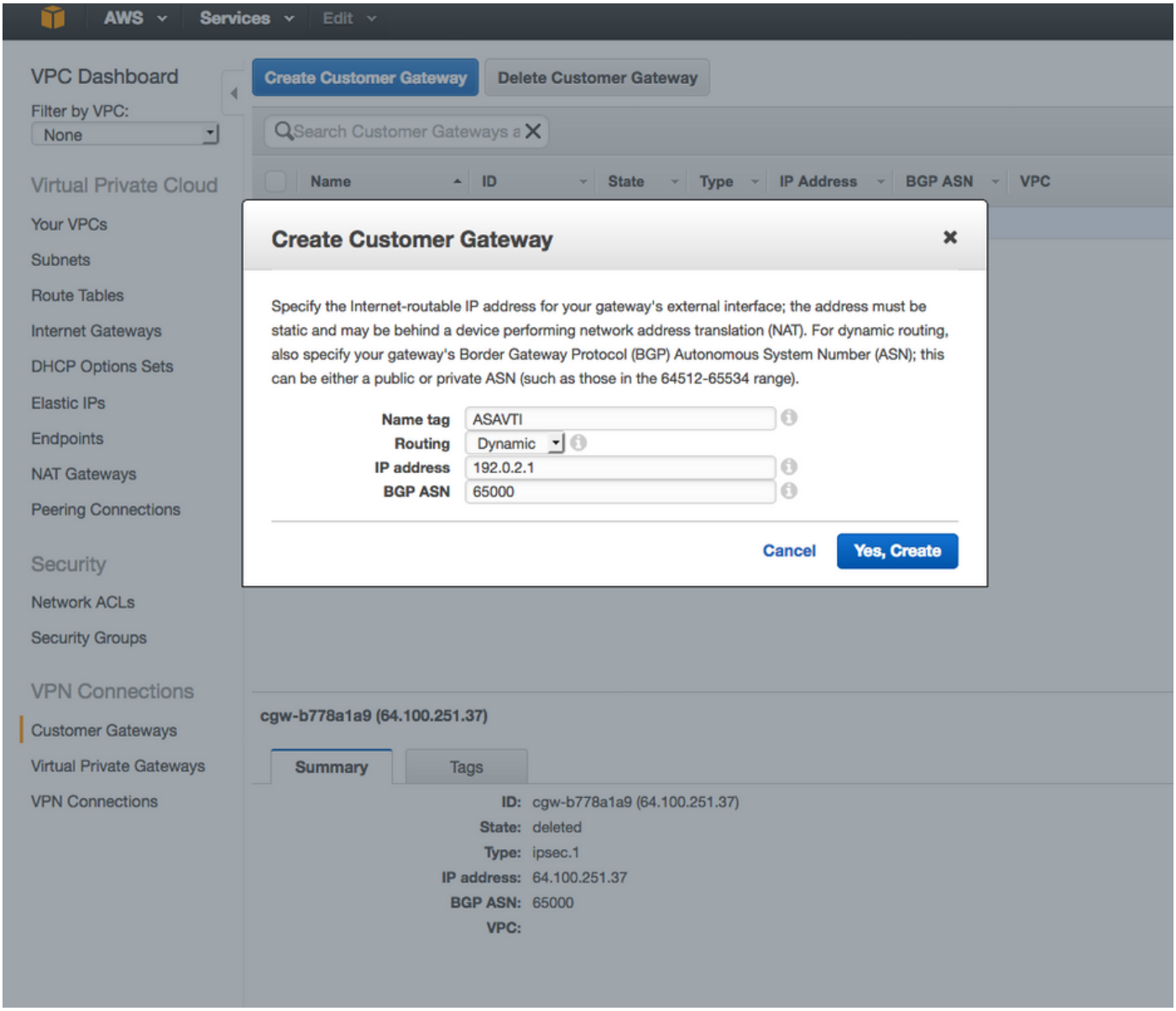
Verificare che sia già stato creato un VPC (Virtual Private Cloud). Per impostazione predefinita, viene creato un VPC con 172.31.0.0/16. In questo punto verranno collegate le macchine virtuali (VM).



Passaggio 3.

Creare un "Customer Gateway". Questo è un endpoint che rappresenta l'ASA.

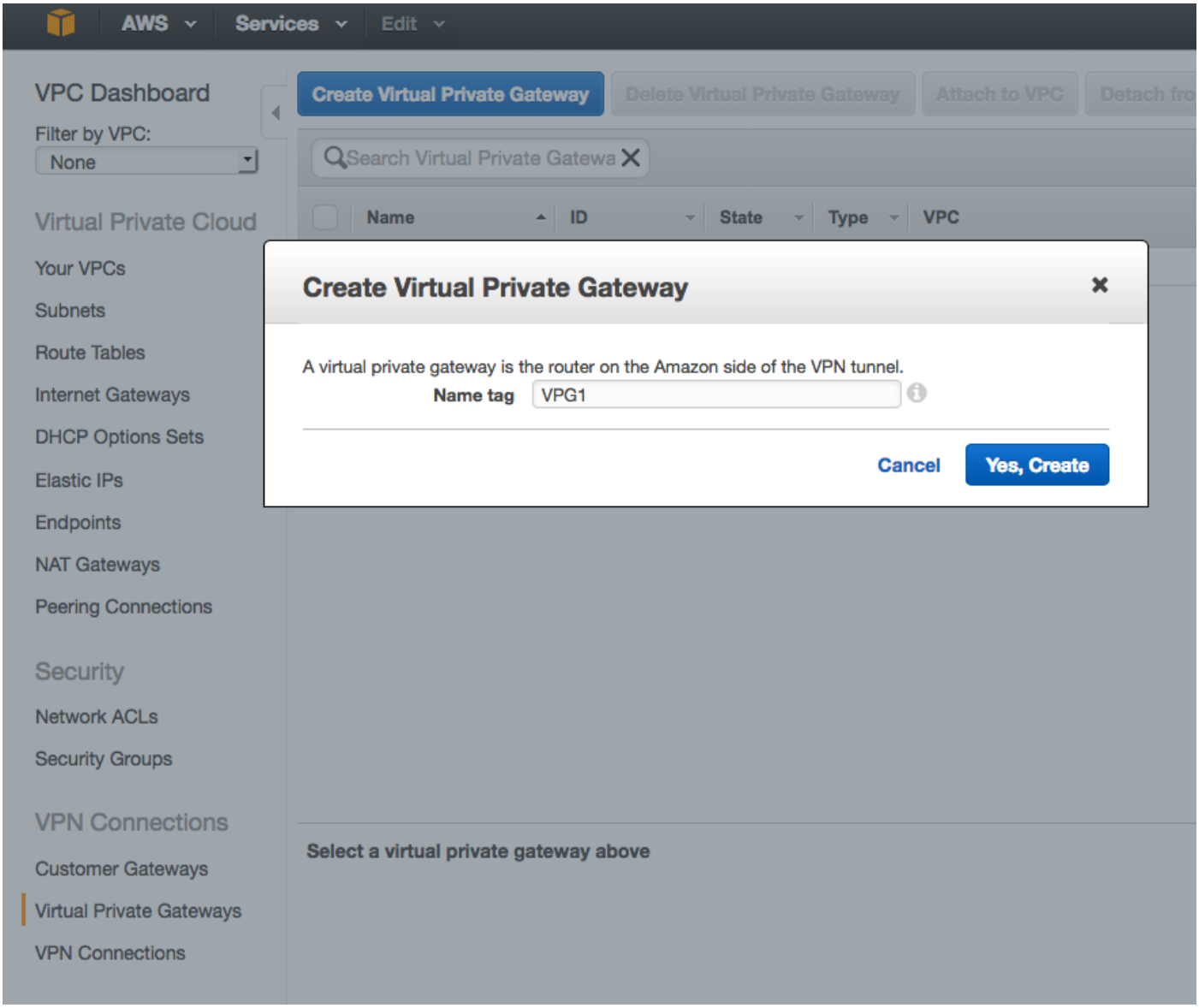
Campo	Valore
Tag Name	Questo è un nome leggibile che riconosce l'ASA.
Routing	Dinamico: significa che verrà usato il Border Gateway Protocol (BGP) per scambiare le informaz di routing.
Indirizzo IP	Questo è l'indirizzo IP pubblico dell'interfaccia esterna dell'ASA.
BGP ASN	Il numero del sistema autonomo (AS) del processo BGP rispetto a quello eseguito sull'appliance ASA. Utilizzare 65000 a meno che l'organizzazione non disponga di un numero AS pubblico.



Passaggio 4.

Creare un VPG (Virtual Private Gateway). Questo è un router simulato ospitato con AWS che termina il tunnel IPsec.

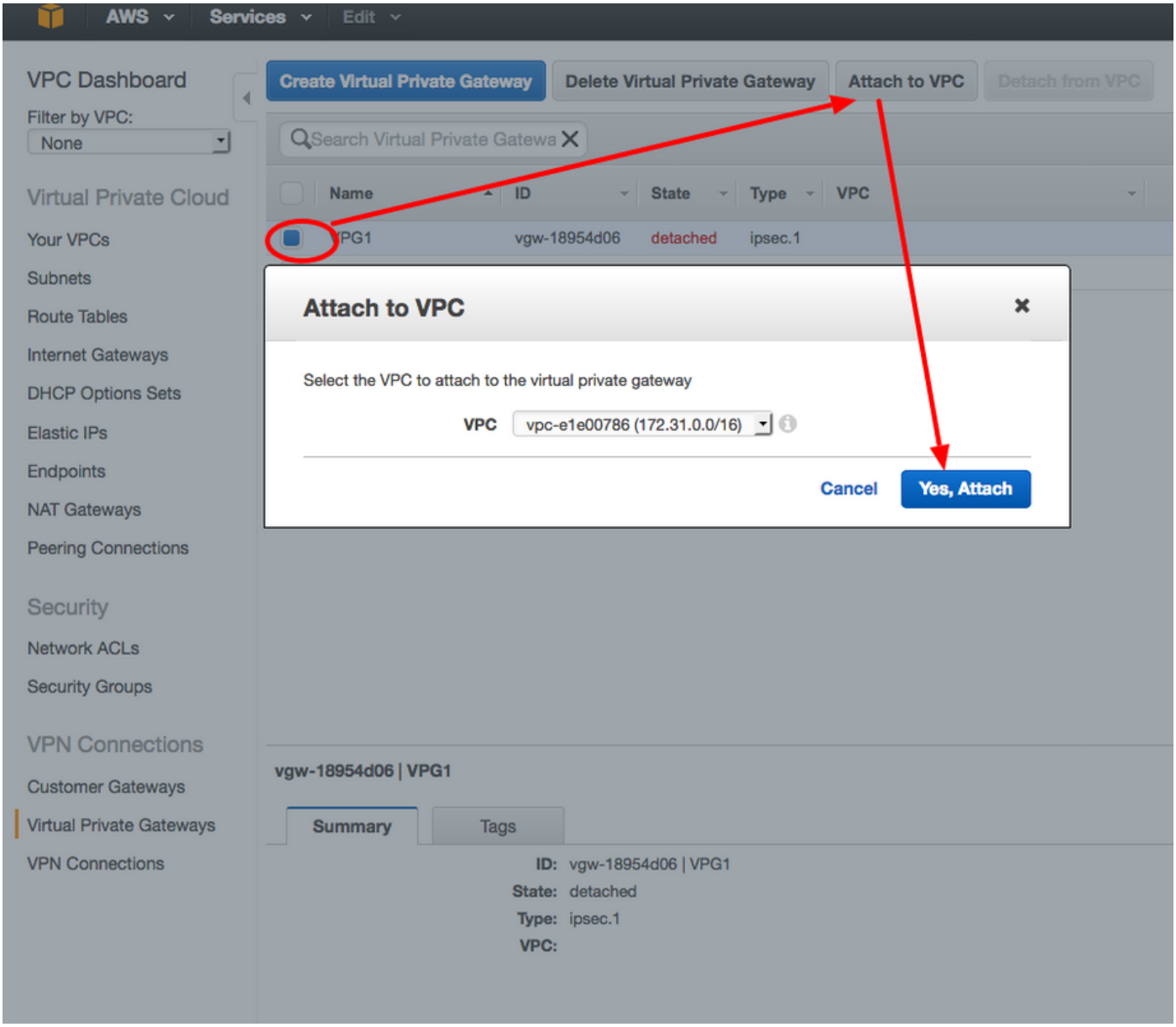
Campo	Valore
Tag Name	Un nome leggibile dall'uomo per riconoscere il VPG.



Passaggio 5.

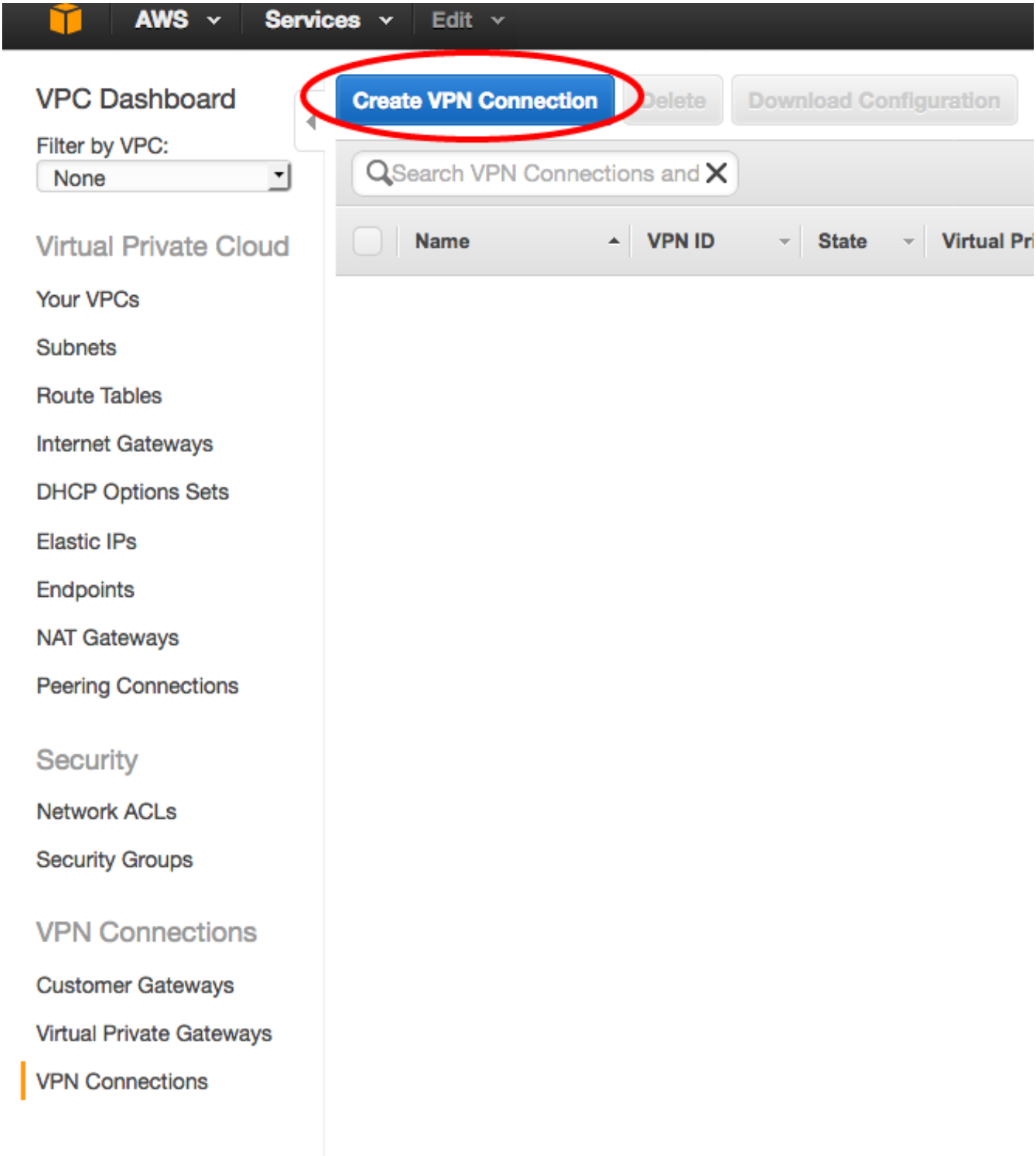
Collegare il VPG al VPC.

Scegliere il gateway privato virtuale, fare clic su **Connetti a VPC**, scegliere il VPC dall'elenco a discesa VPC e fare clic su **Sì, Connetti**.

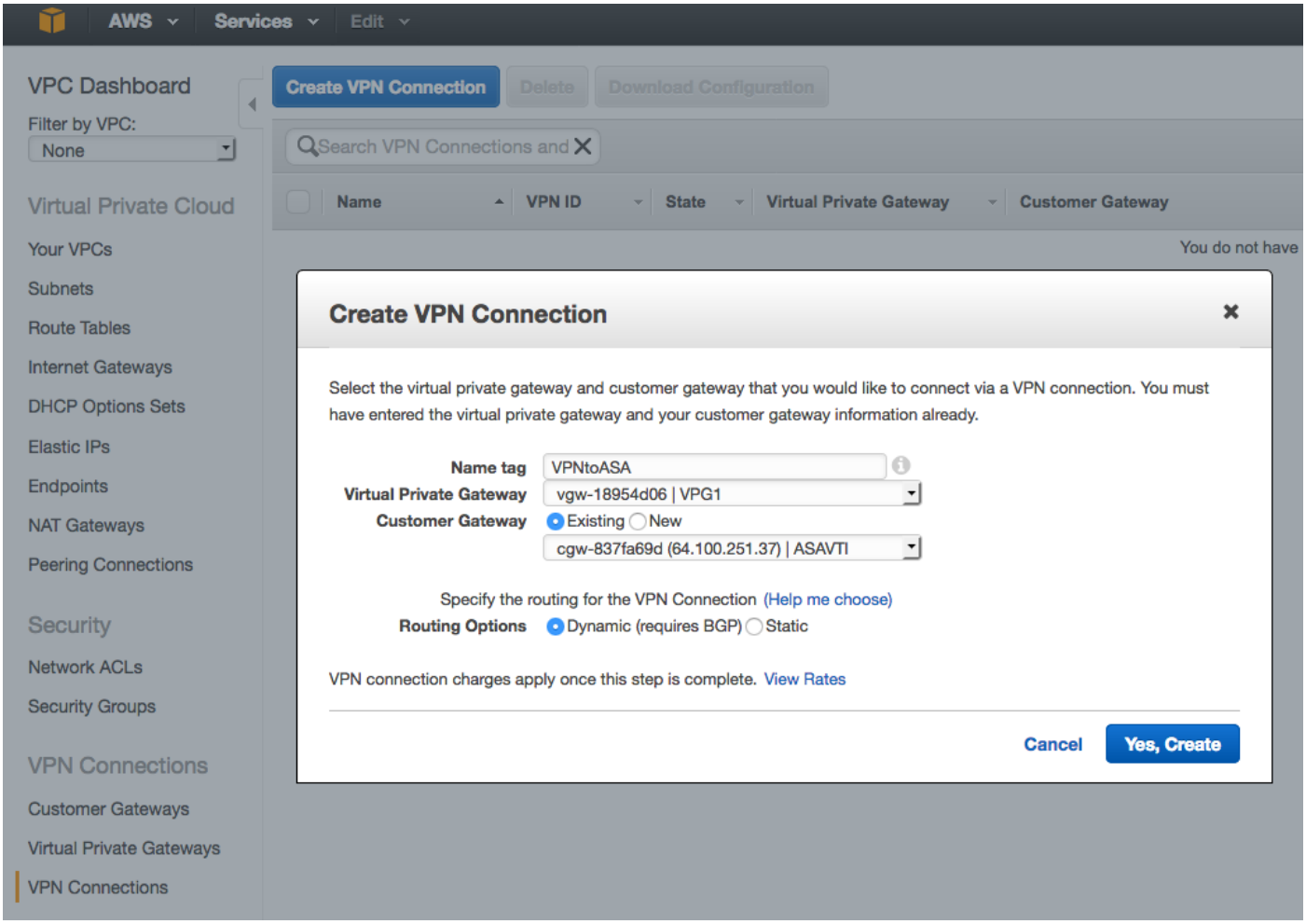


Passaggio 6.

Crea una connessione VPN.

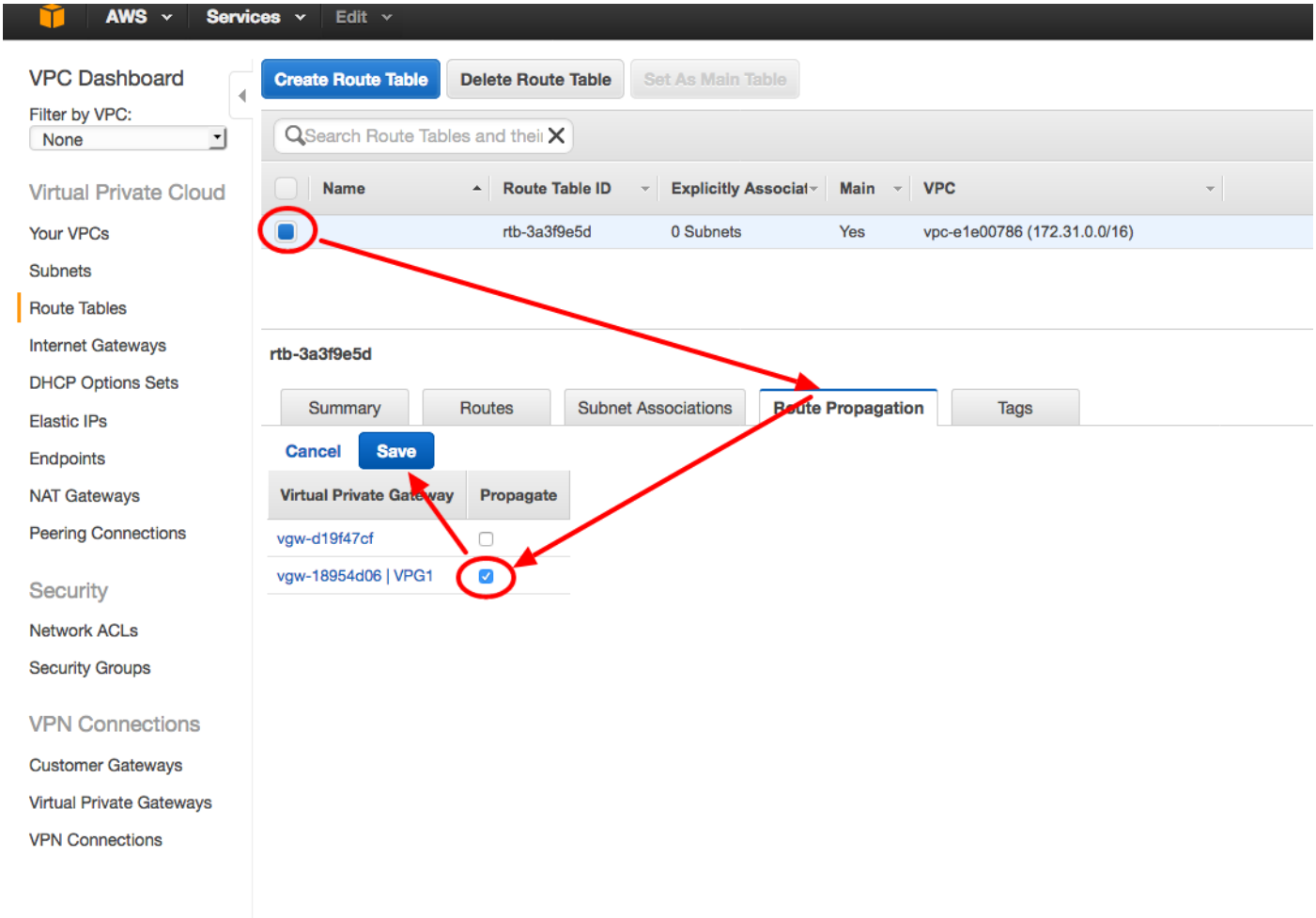


Campo	Valore
Tag Name	Tag leggibile dalla persona della connessione VPN tra AWS e ASA.
Virtual Private Gateway	Selezionate il file VPG appena creato.
Customer Gateway	Fare clic sul pulsante di opzione **Existing** (Esistente) e scegliere il gateway dell'A
Opzioni di routing	Fare clic sul pulsante di opzione **Dinamico (richiede BGP)**.



Passaggio 7.

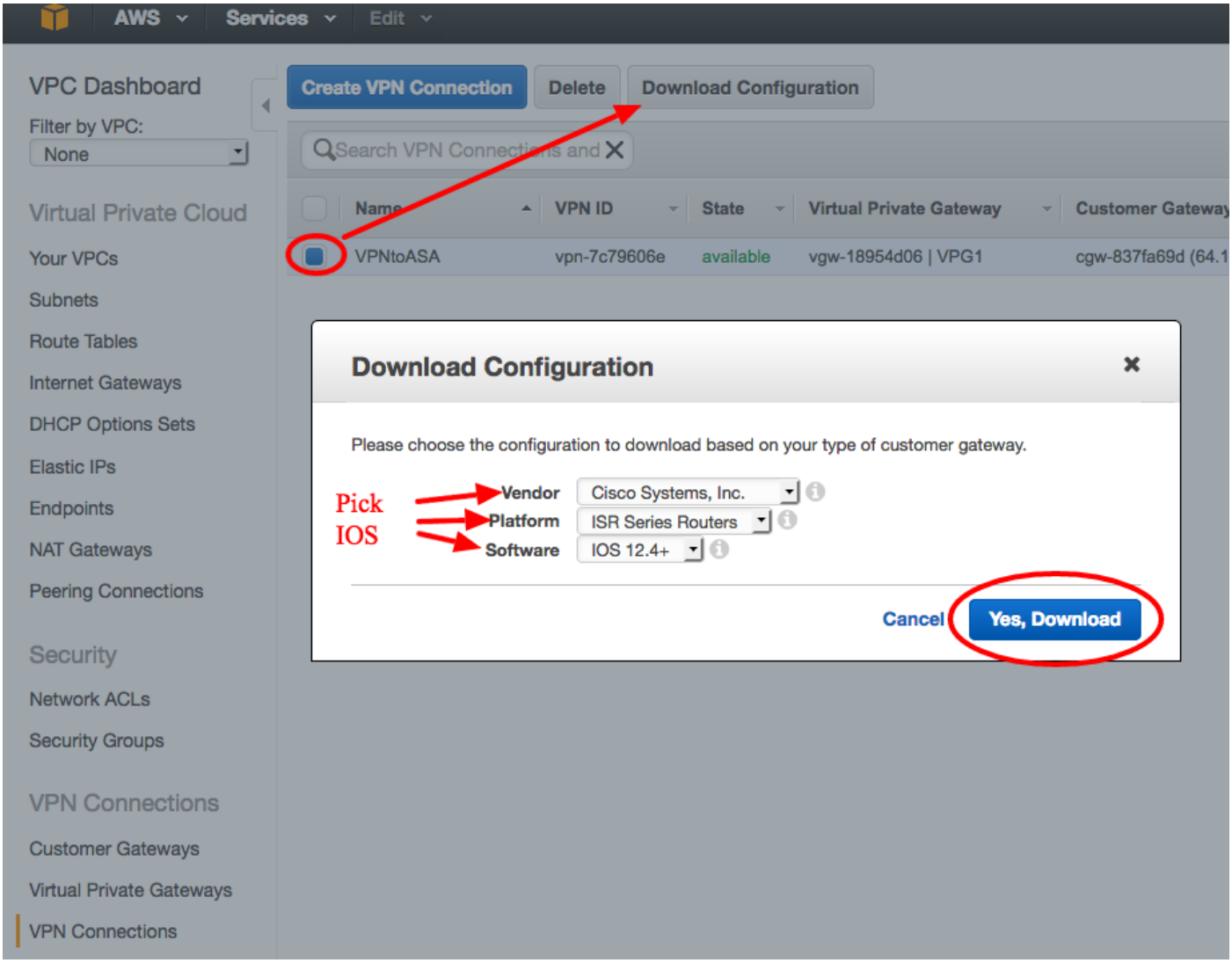
Configurare la Route Table per propagare le route apprese dal VPG (tramite BGP) al VPC.



Passaggio 8.

Scaricare la configurazione suggerita. Scegliere i valori seguenti per generare una configurazione in stile VTI.

Campo	Valore
Fornitore	Cisco Systems, Inc.
Piattaforma	Serie ISR Router
Software	IOS 12.4+



Configurazione dell'ASA

Dopo aver scaricato la configurazione, occorre procedere alla conversione.

Passaggio 1.

criterio crypto isakmp su criterio crypto ikev1. Serve un'unica politica, poiché le politiche 200 e 201 sono identiche.

Configurazione consigliata	A

`crypto isakmp policy 200`
`  crittografia aes 128`
`  pre-condivisione di autenticazione`
`  gruppo 2`
`  life 28800`
`  hash sha`
`esci`
`crypto isakmp policy 2011`
`  crittografia aes 128`
`  pre-condivisione di autenticazione`
`  gruppo 2`
	`abilitazione ikev1 crypto all'esterno`
	`criterio crypto ikev1 10`
	`  pre-condivisione di autenticazione`
	`  aes di crittografia`
	`  hash sha`
	`  gruppo 2`
	`  life 28800`

```
 life 28800
 hash sha
esci
```

Passaggio 2.

crypto ipsec transform-set su crypto ipsec ikev1 transform-set. Poiché i due insiemi di trasformazioni sono identici, è necessario un solo insieme di trasformazioni.

Configurazione consigliata	A

crypto ipsec transform-set ipsec-prop-vpn-7c79606e-0
esp-aes 128 esp-sha-hmac
  tunnel in modalità
esci
crypto ipsec transform-set ipsec-prop-vpn-7c79606e-1
esp-aes 128 esp-sha-hmac
  tunnel in modalità
esci
	crypto ipsec ikev1 transf
	set AWS esp-aes esp-sha-h

Passaggio 3.

crypto ipsec profile to crypto ipsec profile. È necessario un solo profilo poiché i due profili sono identici.

Configurazione consigliata	A

crypto ipsec profile ipsec-vpn-7c79606e-0
  imposta gruppo pfs2
  imposta durata associazione di protezione
secondi 3600
  set transform-set ipsec-prop-vpn-7c79606e-0
esci
crypto ipsec profile ipsec-vpn-7c79606e-1
  imposta gruppo pfs2
  imposta durata associazione di protezione
secondi 3600
  set transform-set ipsec-prop-vpn-7c79606e-1
esci
	AWS profilo IPSec di crittografia
	  set ikev1 transform-set AWS
	  imposta gruppo pfs2
	  imposta durata associazione di
	protezione secondi 3600

Passaggio 4.

il crypto keyring e il profilo crypto isakmp devono essere convertiti in un gruppo di tunnel per ogni tunnel.

Configurazione consigliata	A

crypto keyring-vpn-7c79606e-0
  indirizzo locale 64.100.251.37
  indirizzo chiave già condivisa 52.34.205.227 chiave
QZhh90Bjf
esci
!
crypto isakmp profile isakmp-vpn-7c79606e-0
  indirizzo locale 64.100.251.37
  corrispondenza indirizzo identità 52.34.205.227
  keyring keyring-vpn-7c79606e-0
	tunnel group
	52.34.205.227 tipo
	ipsec-l2l
	attributi ipsec tunn
	group 52.34.205.227
	  QZhh90Bjf chiave gr
	condivisa ikev1
	  soglia keepalive
	isakmp 10 tentativo
	tunnel group

```
 esci
!
crypto keyring-vpn-7c79606e-1
 indirizzo locale 64.100.251.37
 indirizzo chiave già condivisa 52.37.194.219 chiave
JjxCWy4Ae
 esci
!
crypto isakmp profile isakmp-vpn-7c79606e-1
 indirizzo locale 64.100.251.37
 corrispondenza indirizzo identità 52.37.194.219
 keyring-vpn-7c79606e-1
 esci
```

```
52.37.194.219 tipo
ipsec-l2l
attributi ipsec tunn
group 52.37.194.219
 ikev1 a chiave già
condivisa JjxCWy4Ae
 soglia keepalive
isakmp 10 tentativo
```

Passaggio 5.

La configurazione del tunnel è quasi identica. L'ASA non supporta il comando ip tcp adjust-mss o il comando ip virtual-reassembly.

Configurazione consigliata

```
interface Tunnel1
 indirizzo ip 169.254.13.190 255.255.255.252
 ip virtual-reassembly
 origine tunnel 64.100.251.37
 destinazione del tunnel 52.34.205.227
 modalità tunnel ipsec ipv4
 protezione tunnel profilo ipsec ipsec-vpn-
7c79606e-0
 ip tcp adjust-mss 1387
 nessuna chiusura
 esci
!
interface Tunnel2
 indirizzo ip 169.254.12.86.255.255.255.252
 ip virtual-reassembly
 origine tunnel 64.100.251.37
 destinazione del tunnel 52.37.194.219
 modalità tunnel ipsec ipv4
 protezione tunnel profilo ipsec ipsec-vpn-
7c79606e-1
 ip tcp adjust-mss 1387
 nessuna chiusura
 esci
```

A

```
interface Tunnel1
 nameif AWS1
 indirizzo ip 169.254.13.190
255.255.255.252
 interfaccia di origine tunnel
esterna
 destinazione del tunnel
52.34.205.227
 modalità tunnel ipsec ipv4
 AWS profilo ipsec protezione
tunnel
!
interface Tunnel2
 nameif AWS2
 indirizzo ip
169.254.12.86.255.255.255.252
 interfaccia di origine tunnel
esterna
 destinazione del tunnel
52.37.194.219
 modalità tunnel ipsec ipv4
 AWS profilo ipsec protezione
tunnel
```

Passaggio 6.

Nell'esempio, l'ASA pubblicizzerà solo la subnet interna (192.168.1.0/24) e riceverà la subnet in AWS (172.31.0.0/16).

Configurazione consigliata

```
router bgp 6500
 adiacente 169.254.13.189 remoto-as 7224
 adiacente 169.254.13.189 attivare
 adiacente 169.254.13.189 timer 10 30 30
```

A

```
router bgp 6500
 bgp log-neighbor-changes
 timer bgp 10 30 0
 unicast ipv4 famiglia di
```

```
 unicast ipv4 famiglia di indirizzi
  adiacente 169.254.13.189 remoto-as 7224
  adiacente 169.254.13.189 timer 10 30 30
  adiacente 169.254.13.189 default-originate
  adiacente 169.254.13.189 attivare
  router adiacente 169.254.13.189 soft-
reconfiguration inbound
  rete 0.0.0.0
  esci
 esci
router bgp 6500
 adiacente 169.254.12.85 remoto-as 7224
 adiacente 169.254.12.85 attivare
 adiacente 169.254.12.85 timer 10 30 30
 unicast ipv4 famiglia di indirizzi
  adiacente 169.254.12.85 remoto-as 7224
  adiacente 169.254.12.85 timer 10 30 30
  adiacente 169.254.12.85 default-originate
  adiacente 169.254.12.85 attivare
  router adiacente 169.254.12.85 soft-
reconfiguration inbound
  rete 0.0.0.0
  esci
 esci
```

```
indirizzi
  adiacente 169.254.12.85
remoto-as 7224
  adiacente 169.254.12.85
attivare
  adiacente 169.254.13.189
remoto-as 7224
  adiacente 169.254.13.189
attivare
  rete 192.168.1.0
  nessun riepilogo automat
  nessuna sincronizzazione
 exit-address-family
```

Verifica e ottimizzazione

Passaggio 1.

Verificare che l'appliance ASA stabilisca le associazioni di sicurezza IKEv1 con i due endpoint in AWS. Lo stato dell'associazione di sicurezza deve essere 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#
```

Passaggio 2.

Verificare che le SA IPsec siano installate sull'appliance ASA. Per ogni peer deve essere installata un'interfaccia SPI in entrata e in uscita, mentre alcuni contatori encaps e decaps devono essere incrementati.

```
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
```

Passaggio 3.

Sull'appliance ASA, confermare che le connessioni BGP siano stabilite con AWS. Il contatore State/PfxRcd deve essere 1 quando AWS annuncia la subnet 172.31.0.0/16 verso l'appliance 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
```

Passaggio 4.

Sull'appliance ASA, verificare che il percorso verso 172.31.0.0/16 sia stato appreso tramite le interfacce tunnel. Questo output mostra che sono disponibili due percorsi per 172.31.0.0 da peer 169.254.12.85 e 169.254.13.189. Il percorso verso 169.254.13.189 out del tunnel 2 (AWS2) è preferito a causa del valore metrico più basso.

```
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
```

Passaggio 5.

Per garantire che il traffico che ritorna da AWS segua un percorso simmetrico, configurare una route-map che corrisponda al percorso preferito e modificare il valore BGP in modo da modificare le route annunciate.

```
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
```

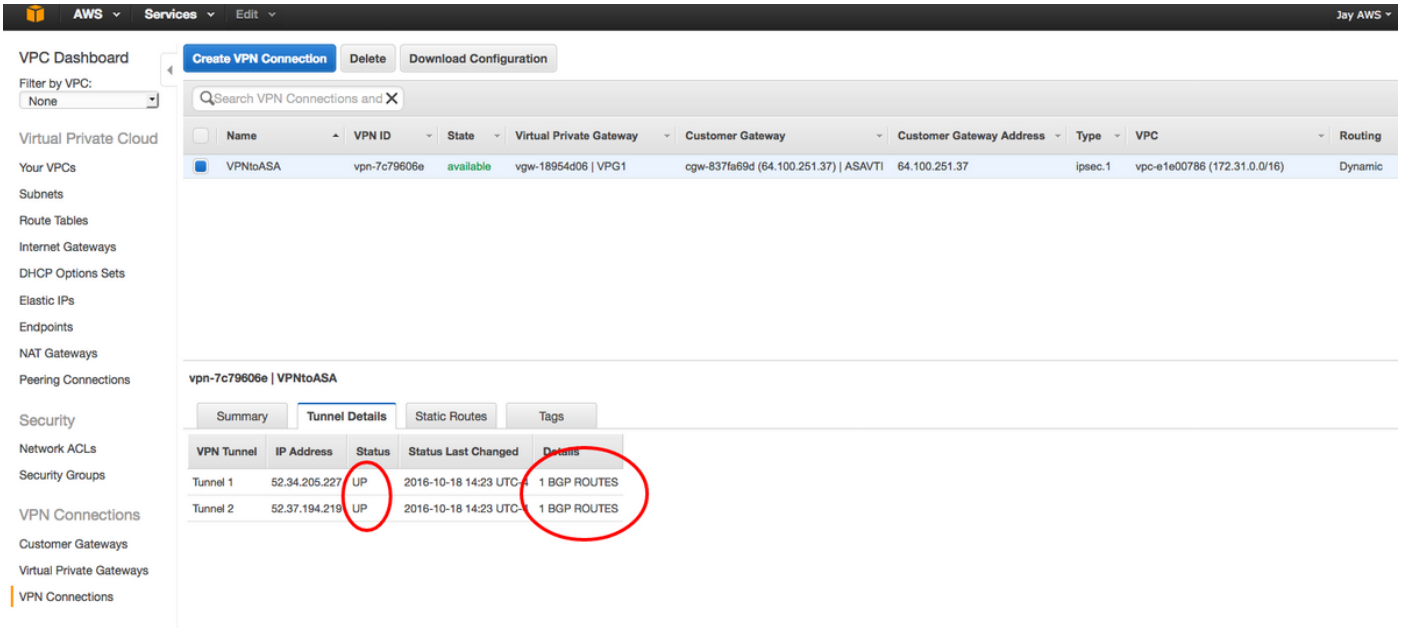
Passaggio 6.

Sull'appliance ASA, confermare che 192.168.1.0/24 sia annunciato su 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
```

Passaggio 7.

In AWS, verificare che i tunnel per la connessione VPN siano attivi e che le route vengano apprese dal peer. Verificare inoltre che la route sia stata propagata nella tabella di routing.



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