

# Configurer les services Web Amazon de connexion VTI IPsec ASA

## Contenu

[Introduction](#)

[Configurer AWS](#)

[Configuration de l'ASA](#)

[Vérifier et optimiser](#)

## Introduction

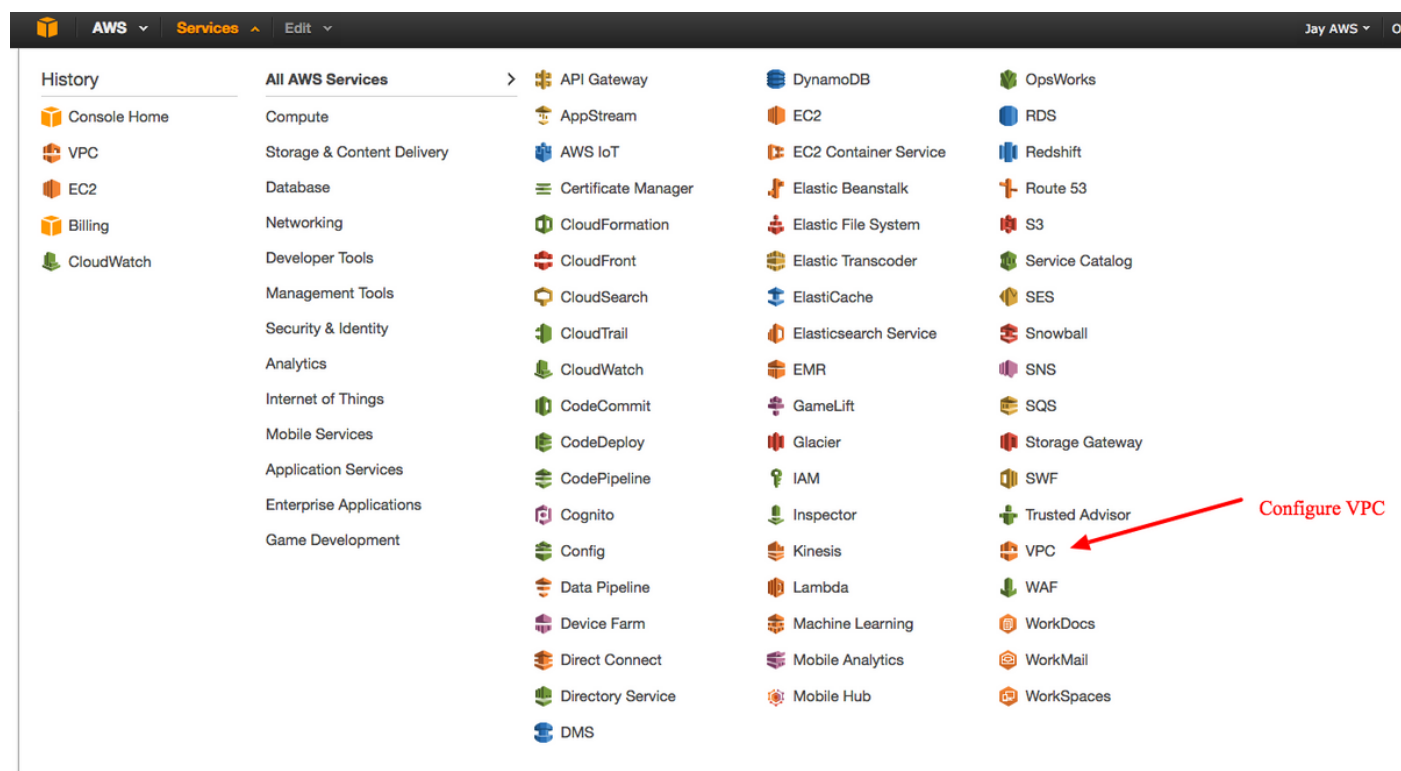
Ce document décrit comment configurer une connexion VTI (Adaptive Security Appliance) IPsec. Dans ASA 9.7.1, IPsec VTI a été introduit. Il est limité à sVTI IPv4 sur IPv4 en utilisant IKEv1 dans cette version. Ceci est un exemple de configuration pour que l'ASA se connecte à Amazon Web Services (AWS).

**Note:** Actuellement, VTI est uniquement pris en charge en mode routé à contexte unique.

## Configurer AWS

### Étape 1.

Connectez-vous à la console AWS et accédez au panneau VPC.



Accédez au tableau de bord VPC

## Étape 2.

Vérifiez qu'un cloud privé virtuel (VPC) est déjà créé. Par défaut, un VPC avec 172.31.0.0/16 est créé. C'est là que les machines virtuelles (VM) seront connectées.

The screenshot shows the AWS VPC Dashboard. On the left, a sidebar lists various services, with 'Your VPCs' circled in red. The main area displays a table of VPCs. The first row shows a VPC with ID 'vpc-e1e00786', State 'available', and CIDR '172.31.0.0/16'. Below the table, the details for this VPC are shown, including its ID, state, CIDR, DHCP options set, route table, and network ACL. A red arrow points from the text 'Default VPC already created' to the '172.31.0.0/16' CIDR value in the table.

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

**Summary**

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

## Étape 3.

Créer une passerelle client. Il s'agit d'un point de terminaison qui représente l'ASA.

### Champ Valeur

Balise de nom

C'est juste un nom lisible par l'homme pour reconnaître l'ASA.

Routage

Dynamique : cela signifie que le protocole BGP (Border Gateway Protocol) sera utilisé pour échanger des informations de routage.

Adresse IP

Il s'agit de l'adresse IP publique de l'interface externe de l'ASA.

ASN

Numéro de système autonome du processus BGP qui s'exécute sur l'ASA. Utilisez le 65000, sauf

BGP

si votre organisation possède un numéro de système autonome public.

**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 ⓘ

Cancel Yes, Create

**cgw-b778a1a9 (64.100.251.37)**

Summary Tags

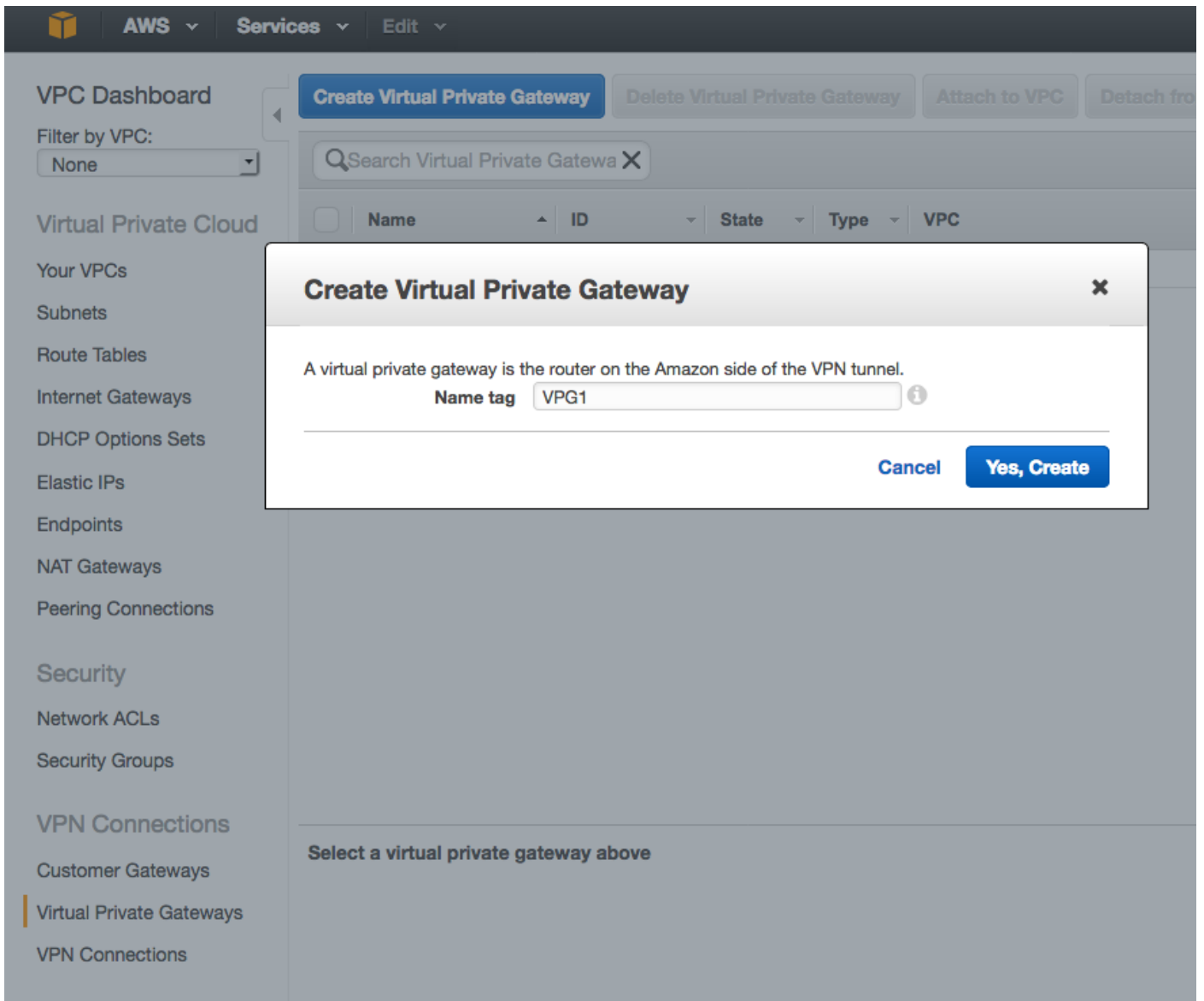
ID: cgw-b778a1a9 (64.100.251.37)  
State: deleted  
Type: ipsec.1  
IP address: 64.100.251.37  
BGP ASN: 65000  
VPC:

#### Étape 4.

Créez une passerelle privée virtuelle (VPG). Il s'agit d'un routeur simulé qui est hébergé avec AWS et qui termine le tunnel IPsec.

**Champ**      **Valeur**

Balise de nom Nom lisible par l'homme pour reconnaître le VPG.



## Étape 5.

Fixez le VPG au VPC.

Choisissez Virtual Private Gateway, cliquez sur **Attach to VPC**, choisissez le VPC dans la liste déroulante VPC, puis cliquez sur **Yes, Attach**.

The screenshot shows the AWS Management Console interface for Virtual Private Gateways. At the top, there are buttons for 'Create Virtual Private Gateway', 'Delete Virtual Private Gateway', 'Attach to VPC', and 'Detach from VPC'. Below these is a search bar and a table of Virtual Private Gateways. The table has columns for Name, ID, State, Type, and VPC. One gateway, 'VPG1' with ID 'vgw-18954d06', is in a 'detached' state and is circled in red. A red arrow points from this gateway to the 'Attach to VPC' button. Another red arrow points from the 'Attach to VPC' button to the 'Yes, Attach' button in the dialog box.

**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:

## Étape 6.

Créez une connexion VPN.

The screenshot shows the AWS Management Console interface for the VPC Dashboard. At the top, there are navigation tabs for 'AWS', 'Services', and 'Edit'. Below the navigation, the 'VPC Dashboard' is visible, with a 'Filter by VPC:' dropdown set to 'None'. A sidebar on the left lists various VPC resources, with 'VPN Connections' highlighted. In the main content area, the 'Create VPN Connection' button is circled in red. To its right are 'Delete' and 'Download Configuration' buttons. Below these buttons is a search bar labeled 'Search VPN Connections and X' and a table header with columns for 'Name', 'VPN ID', 'State', and 'Virtual Private Gateway'.

**Champ**

- Balise de nom
- Passerelle privée virtuelle
- Passerelle client
- Options de routage

**Valeur**

- Une étiquette lisible par un humain de la connexion VPN entre AWS et l'ASA.
- Sélectionnez le VPG que vous venez de créer.
- Cliquez sur la case d'option **Existant** et sélectionnez la passerelle de l'ASA.
- Cliquez sur la case d'option **Dynamique (BGP requis)**.

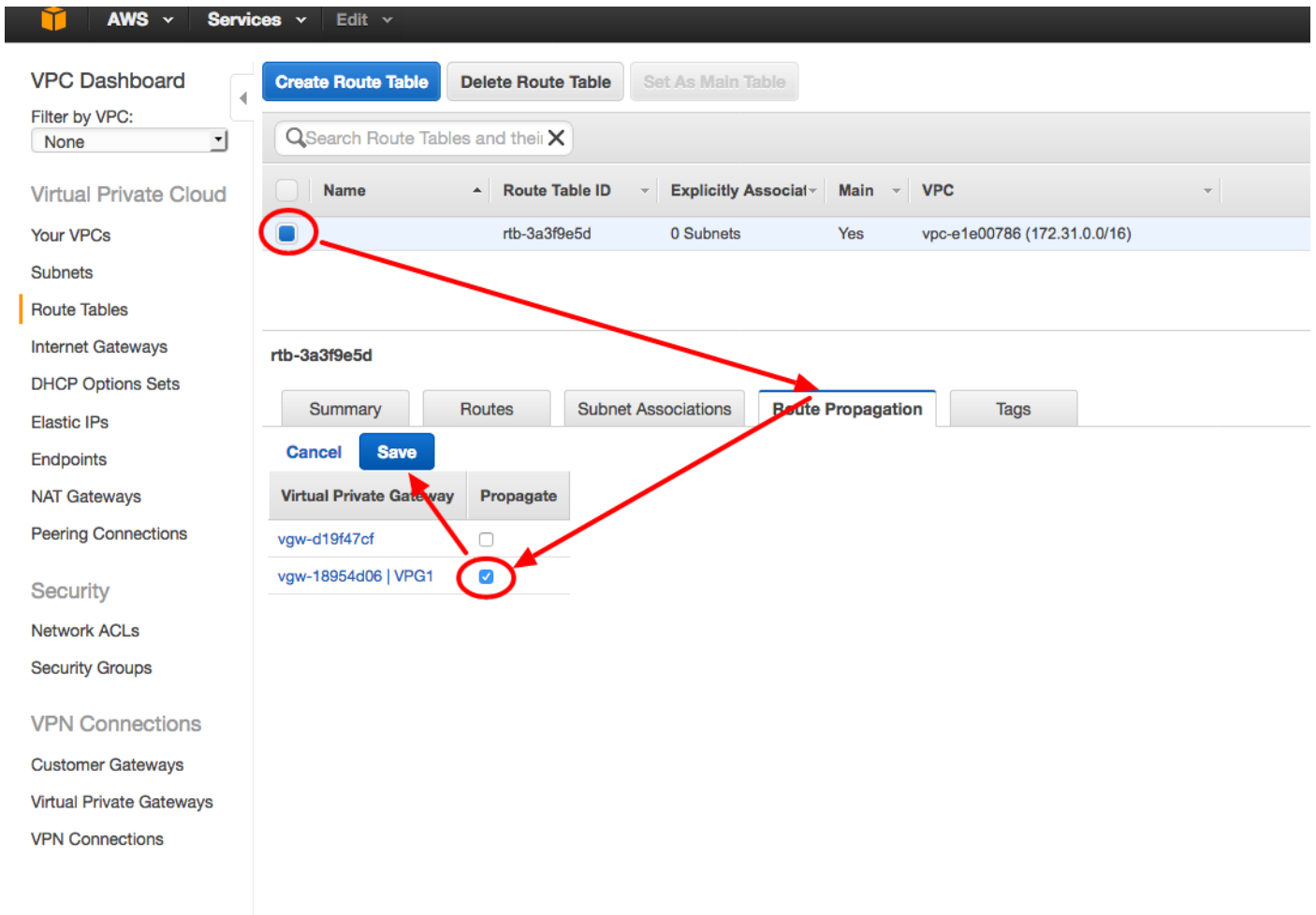
The screenshot shows the AWS Management Console interface for creating a VPN connection. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays the 'Create VPN Connection' dialog box. The dialog includes a search bar, a table header with columns for Name, VPN ID, State, Virtual Private Gateway, and Customer Gateway, and a modal window for configuration. The modal window contains the following fields and options:

- Name tag:** VPNtoASA
- Virtual Private Gateway:** vgw-18954d06 | VPG1
- Customer Gateway:** Existing (selected) / New. Selected: cgw-837fa69d (64.100.251.37) | ASAVTI
- Routing Options:** Dynamic (requires BGP) (selected) / Static

Additional text in the dialog includes: '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.', 'Specify the routing for the VPN Connection (Help me choose)', and 'VPN connection charges apply once this step is complete. View Rates'. The dialog concludes with 'Cancel' and 'Yes, Create' buttons.

## Étape 7.

Configurez la table de routage pour propager les routes apprises du VPG (via BGP) dans le VPC.

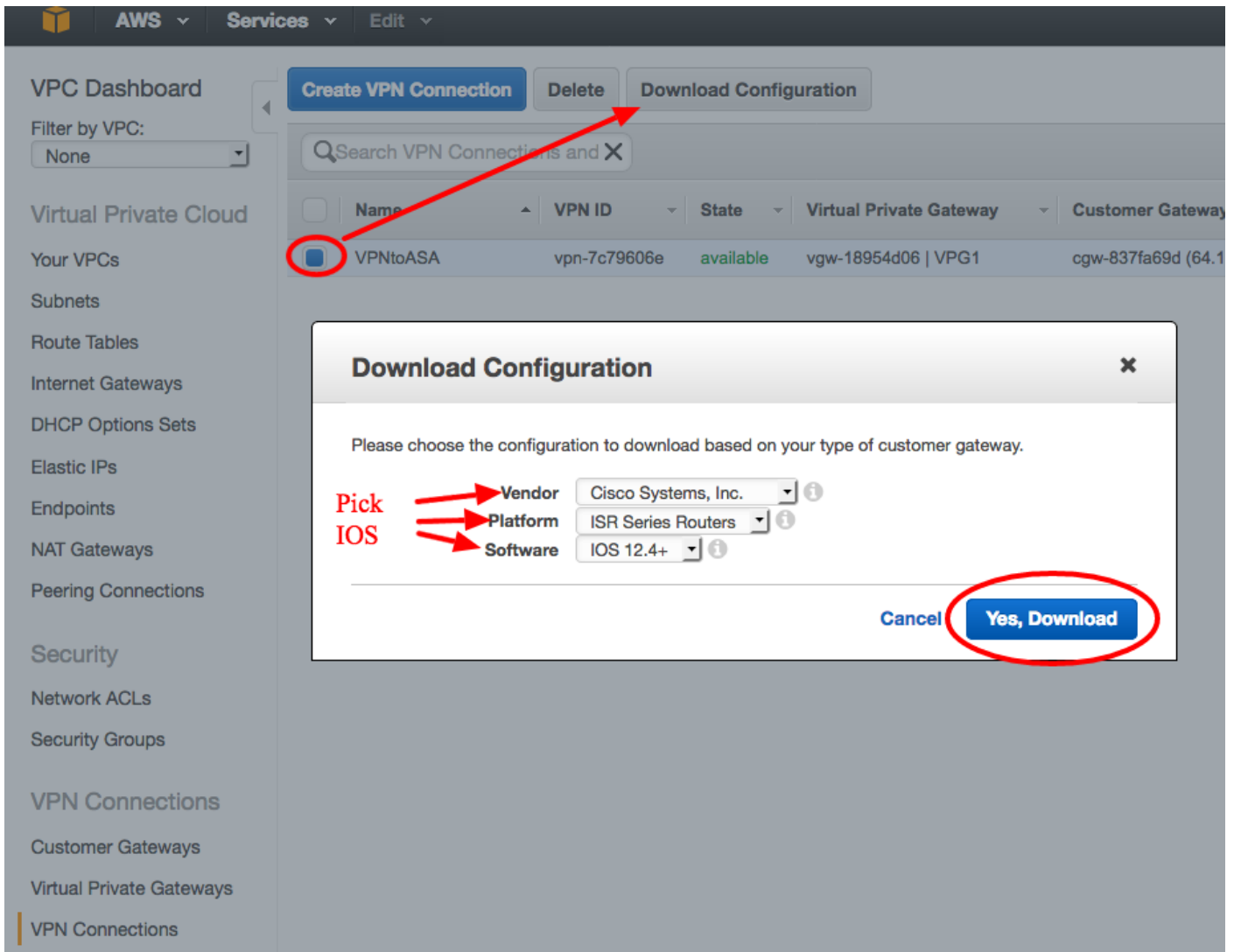


## Étape 8.

Téléchargez la configuration suggérée. Choisissez les valeurs ci-dessous afin de générer une configuration de type VTI.

Champ	Valeur
Fournisseur	Cisco Systems, Inc.
Plateforme	Routeurs de la gamme ISR
le logiciel Cisco IOS	IOS 12.4+





## Configuration de l'ASA

Une fois la configuration téléchargée, une conversion est nécessaire.

### Étape 1.

crypto isakmp policy to crypto ikev1 policy. Une seule politique est nécessaire puisque la politique 200 et la politique 201 sont identiques.

#### Configuration suggérée

```
crypto isakmp policy 200
  cryptage aes 128
  authentication pre-share
  groupe 2
  28800 à vie
  hash sha
sortir
crypto isakmp policy 201
  cryptage aes 128
  authentication pre-share
  groupe 2
```

#### Par

```
crypto ikev1 enable outside
crypto ikev1 policy 10
  authentication pre-share
  aes de chiffrement
  hash sha
  groupe 2
  28800 à vie
```

```
28800 à vie
hash sha
sortir
```

## Étape 2.

crypto ipsec transformer-set en crypto ipsec ikev1 transformer-set. Un seul jeu de transformation est nécessaire car les deux jeux de transformation sont identiques.

### Configuration suggérée

```
crypto ipsec transformer-set ipsec-prop-vpn-
7c79606e-0 esp-aes 128 esp-sha-hmac
  tunnel de mode
sortir
crypto ipsec transformer-set ipsec-prop-vpn-
7c79606e-1 esp-aes 128 esp-sha-hmac
  tunnel de mode
sortir
```

### Par

```
crypto ipsec ikev1
transformer-set AWS esp-aes
esp-sha-hmac
```

## Étape 3.

crypto ipsec profile to crypto ipsec profile. Un seul profil est nécessaire car les deux profils sont identiques.

### Configuration suggérée

```
crypto ipsec profile ipsec-vpn-7c79606e-0
  set pfs group2
  set security-association life seconds 3600
  set transformation ipsec-prop-vpn-7c79606e-0
sortir
crypto ipsec profile ipsec-vpn-7c79606e-1
  set pfs group2
  set security-association life seconds 3600
  set transformation ipsec-prop-vpn-7c79606e-1
sortir
```

### Par

```
crypto ipsec profile AWS
  set ikev1 transformer-set AWS
  set pfs group2
  set security-association life
seconds 3600
```

## Étape 4.

crypto keyring et crypto isakmp profile doivent être convertis en tunnel-group one pour chaque tunnel.

### Configuration suggérée

```
crypto keyring-vpn-7c79606e-0
  adresse locale 64.100.251.37
  adresse de clé prépartagée 52.34.205.227 clé QZhh90Bjf
sortir
!
crypto isakmp profile isakmp-vpn-7c79606e-0
  adresse locale 64.100.251.37
  match identity address 52.34.205.227
  keyring-vpn-7c79606e-0
  sortir
!
crypto keyring-vpn-7c79606e-1
```

### Par

```
tunnel-group
52.34.205.227 type ipsec
121
tunnel-group
52.34.205.227 ipsec-
attribute
  QZhh90Bjf à clé pré-
partagée ikev1
  isakmp keepalive
threshold 10 retry 10
tunnel-group
52.37.194.219 type ipsec
```

```

adresse locale 64.100.251.37
adresse de clé prépartagée 52.37.194.219 clé JjxCWy4Ae
sortir
!
crypto isakmp profile isakmp-vpn-7c79606e-1
  adresse locale 64.100.251.37
  match identity address 52.37.194.219
  keyring-vpn-7c79606e-1
  sortir
  121
  tunnel-group
  52.37.194.219 ipsec-
  attribute
  ikev1 clé pré-partag
  JjxCWy4Ae
  isakmp keepalive
  threshold 10 retry 10

```

## Étape 5.

La configuration du tunnel est presque identique. L'ASA ne prend pas en charge la commande `ip tcp adjust-mss` ou `ip virtual-reassembly`.

### Configuration suggérée

```

interface Tunnell
  adresse ip 169.254.13.190 255.255.255.252
  ip virtual-reassembly
  source du tunnel 64.100.251.37
  destination du tunnel 52.34.205.227
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-vpn-
7c79606e-0
  ip tcp adjust-mss 1387
  no shutdown
  sortir
!
interface Tunnel2
  adresse ip 169.254.12.86 255.255.255.252
  ip virtual-reassembly
  source du tunnel 64.100.251.37
  destination du tunnel 52.37.194.219
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-vpn-
7c79606e-1
  ip tcp adjust-mss 1387
  no shutdown
  sortir

```

### Par

```

interface Tunnell
  nomif AWS1
  adresse ip 169.254.13.190
255.255.255.252
  interface source du tunnel
externe
  destination du tunnel
52.34.205.227
  tunnel mode ipsec ipv4
  tunnel protection ipsec profil
AWS
!
interface Tunnel2
  nomif AWS2
  adresse ip 169.254.12.86
255.255.255.252
  interface source du tunnel
externe
  destination du tunnel
52.37.194.219
  tunnel mode ipsec ipv4
  tunnel protection ipsec profil
AWS

```

## Étape 6.

Dans cet exemple, l'ASA annonce uniquement le sous-réseau interne (192.168.1.0/24) et reçoit le sous-réseau dans AWS (172.31.0.0/16).

### Configuration suggérée

```

routeur bgp 65000
  voisin 169.254.13.189 distant-as 7224
  neighbor 169.254.13.189 activate
  voisin 169.254.13.189 temporisateurs 10 30 30
  address-family ipv4 unicast
  voisin 169.254.13.189 distant-as 7224
  voisin 169.254.13.189 temporisateurs 10 30 30
  neighbor 169.254.13.189 default-originate

```

### Par

```

routeur bgp 65000
  bgp log-neighbor-changes
  timers bgp 10 30 0
  address-family ipv4 unicast
  voisin 169.254.12.85
distant-as 7224
  neighbor 169.254.12.85
activate

```

```

neighbor 169.254.13.189 activate
neighbor 169.254.13.189 reconfiguration logicielle
entrante
réseau 0.0.0.0
sortir
sortir
routeur bgp 65000
voisin 169.254.12.85 distant-as 7224
neighbor 169.254.12.85 activate
voisin 169.254.12.85 temporisateurs 10 30 30
address-family ipv4 unicast
voisin 169.254.12.85 distant-as 7224
voisin 169.254.12.85 temporisateurs 10 30 30
neighbor 169.254.12.85 default-originate
neighbor 169.254.12.85 activate
neighbor 169.254.12.85 soft-reconfiguration
entrante
réseau 0.0.0.0
sortir
sortir
voisin 169.254.13.189
distant-as 7224
neighbor 169.254.13.189
activate
réseau 192.168.1.0
no auto-summary
aucune synchronisation
exit-address-family

```

## Vérifier et optimiser

### Étape 1.

Confirmez que l'ASA établit les associations de sécurité IKEv1 avec les deux points d'extrémité à AWS. L'état de la SA doit être 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#
```

### Étape 2.

Vérifiez que les SA IPsec sont installées sur ASA. Il doit y avoir un SPI entrant et sortant installé pour chaque homologue et il doit y avoir des compteurs de recouvrement et de décodage incrémentés.

```
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
```

### Étape 3.

Sur l'ASA, vérifiez que les connexions BGP sont établies avec AWS. Le compteur State/PfxRcd doit être 1 car AWS annonce le sous-réseau 172.31.0.0/16 vers l'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

### Étape 4.

Sur l'ASA, vérifiez que la route vers 172.31.0.0/16 a été apprise via les interfaces de tunnel. Ce résultat montre qu'il existe deux chemins vers 172.31.0.0 à partir de l'homologue 169.254.12.85 et 169.254.13.189. Le chemin vers 169.254.13.189 via le tunnel 2 (AWS2) est préféré en raison de la métrique inférieure.

```
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
```

## Étape 5.

Afin de s'assurer que le trafic qui retourne d'AWS suit un chemin symétrique, configurez une route-map pour correspondre au chemin préféré et ajustez BGP pour modifier les routes annoncées.

```
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
```

## Étape 6.

Sur l'ASA, vérifiez que 192.168.1.0/24 est annoncé à 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

## Étape 7.

Dans AWS, vérifiez que les tunnels pour la connexion VPN sont UP et que les routes sont apprises de l'homologue. Vérifiez également que la route a été propagée dans la table de routage.

The screenshot shows the AWS Management Console interface for a VPN connection named 'VPNtoASA'. The 'Tunnel Details' tab is selected, displaying a table with the following data:

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	52.34.205.227	UP	2016-10-18 14:23 UTC	1 BGP ROUTES
Tunnel 2	52.37.194.219	UP	2016-10-18 14:23 UTC	1 BGP ROUTES

Red circles highlight the 'UP' status and '1 BGP ROUTES' details for both tunnels.





### 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 their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>		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	<a href="#">igw-e5ad1481</a>	Active	No
192.168.1.0/24	<a href="#">vgw-18954d06</a>	Active	Yes