# Configure ASA IPsec VTI Connection Amazon Web Services

# Contents

Introduction Configure AWS Configure the ASA Verify and Optimize

# Introduction

This document describes how to configure an Adaptive Security Appliance (ASA) IPsec Virtual Tunnel Interface (VTI) connection. In ASA 9.7.1, IPsec VTI has been introduced. It is limited to sVTI IPv4 over IPv4 using IKEv1 in this release. This is an example configuration for the ASA to connect to Amazon Web Services (AWS).

Note: Currently VTI is only supported in single-context, routed mode.

# **Configure AWS**

### Step 1.

Log in to the AWS console and navigate to the VPC panel.



## Step 2.

Confirm that a Virtual Private Cloud (VPC) is already created. By default, a VPC with 172.31.0.0/16 is created. This is where Virtual Machines (VMs) will be attached.

| 🎁 AWS ~ Servic           | es v Edit v                       |                                    | Jay AWS 👻 0                           | regon ×   |
|--------------------------|-----------------------------------|------------------------------------|---------------------------------------|-----------|
| VPC Dashboard            | Create VPC Actions V              |                                    |                                       | C         |
| None                     | QSearch VPCs and their proper X   |                                    | ~                                     | <1 to 1 o |
| Virtual Private Cloud    | Name   VPC ID    State   VPC CIDR | ✓ DHCP options set ✓ Route table ✓ | Network ACL  v Tenancy  v Default VPC | -         |
| Your VPCs                | vpc-e1e00786 available 172.31.0.0 | /16 dopt-58d5b13c rtb-3a3f9e5d     | acl-f6844591 Default Yes              |           |
| Subnets                  | <b>†</b>                          |                                    |                                       |           |
| Route Tables             | vpc-e1e00786 (172.31.0.0/16)      |                                    |                                       |           |
| Internet Gateways        | Summary Flow Logs Tags            |                                    |                                       |           |
| DHCP Options Sets        | VPC ID: vpc-e1e00786              | Network ACL: acl-f6844591          |                                       |           |
| Elastic IPs              | State: available                  | Tenancy: Default                   |                                       |           |
| Endpoints                | VPC CIDR: 172.31.0.0/16           | DNS resolution: yes                |                                       |           |
| NAT Gateways             | Route table: rtb-3a3f9e5d         | ClassicLink DNS Support: no        |                                       |           |
| Peering Connections      |                                   |                                    |                                       |           |
|                          |                                   |                                    |                                       |           |
| Security                 |                                   |                                    |                                       |           |
| Network ACLs             |                                   |                                    |                                       |           |
| Security Groups          |                                   |                                    |                                       |           |
| VPN Connections          | Default VPC                       | already created                    |                                       |           |
| Customar Gatawaye        |                                   | -                                  |                                       |           |
| Vistual Drivate Cateways |                                   |                                    |                                       |           |
| virtual Private Gateways |                                   |                                    |                                       |           |
| VPN Connections          |                                   |                                    |                                       |           |

## Step 3.

Create a "Customer Gateway". This is a an endpoint that represents the ASA.

| Field         | Value   |  |  |  |  |
|---------------|---|--|--|--|--|
| Name<br>Tag   | This is just a human readable name to recognize the ASA.  |  |  |  |  |
| Routing       | Dynamic - This means that Border Gateway Protocol (BGP) will be used in order to exchange routing information.                        |  |  |  |  |
| IP<br>Address | This is the Public IP address of the ASA's outside interface.   |  |  |  |  |
| BGP<br>ASN    | The Autonomous System (AS) number of the BGP process than runs on the ASA. Use 65000 unless your organization has a public AS number. |  |  |  |  |
|               |   |  |  |  |  |

| 🔰 AWS 🗸 Servi   | ices v Edit v   |
|---|---|
| VPC Dashboard   | Create Customer Gateway Delete Customer Gateway   |
| Filter by VPC:     None   | QSearch Customer Gateways a X   |
| Virtual Private Cloud   | Name A ID VPC   |
| Your VPCs   | Create Customer Gateway ×   |
| Subnets<br>Route Tables<br>Internet Gateways<br>DHCP Options Sets<br>Elastic IPs<br>Endpoints<br>NAT Gateways | 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       Upnamic         IP address       192.0.2.1 |
| Peering Connections   | BGP ASN 65000<br>Cancel Yes, Create   |
| Network ACLs<br>Security Groups   |   |
| VPN Connections<br>Customer Gateways<br>Virtual Private Gateways  | cgw-b778a1a9 (64.100.251.37) Summary Tags   |
| VPN Connections   | ID:       cgw-b778a1a9 (64.100.251.37)         State:       deleted         Type:       ipsec.1         IP address:       64.100.251.37         BGP ASN:       65000         VPC:       VPC:  |

## Step 4.

Create a Virtual Private Gateway (VPG). This is a simulated router that is hosted with AWS that terminates the IPsec tunnel.

## Field Value

Name Tag A human readable name to recognize the VPG.

| 🎁 AWS 🗸 Servi                       | ces 🗸 Edit 🗸   |
|-------------------------------------|--|
| VPC Dashboard<br>Filter by VPC:     | Create Virtual Private Gateway Delete Virtual Private Gateway Attach to VPC Detach fro |
| Virtual Private Cloud               | Name ID · State · Type · VPC   |
| Your VPCs<br>Subnets                | Create Virtual Private Gateway ×   |
| Route Tables                        | A virtual private gateway is the router on the Amazon side of the VPN tunnel.          |
| Internet Gateways DHCP Options Sets | Name tag VPG1  |
| Elastic IPs                         | Cancel Yes, Create   |
| Endpoints                           |  |
| NAT Gateways                        |  |
| Peering Connections                 |  |
| Security                            |  |
| Network ACLs                        |  |
| Security Groups                     |  |
| VPN Connections                     |  |
| Customer Gateways                   | Select a virtual private gateway above   |
| Virtual Private Gateways            |  |
| VPN Connections                     |  |

## Step 5.

Attach the VPG to the VPC.

Choose the Virtual Private Gateway, click **Attach to VPC**, choose the VPC from the VPC dropdown list, and click **Yes, Attach**.

| AWS - Servic                           | es 🗸 Edit 🗸  |
|--|--|
| VPC Dashboard                          | Create Virtual Private Gateway Delete Virtual Private Gateway Attach to VPC Detach from VPC QSearch Virtual Private Gatewa X |
| Virtual Private Cloud<br>Your VPCs     | Name     ID     State     Type     VPC       PG1     vgw-18954d06     detached     ipsec.1                                   |
| Subnets<br>Route Tables                | Attach to VPC ×  |
| Internet Gateways<br>DHCP Options Sets | Select the VPC to attach to the virtual private gateway VPC vpc-e1e00786 (172.31.0.0/16)                                     |
| Endpoints<br>NAT Gateways              | Cancel Yes, Attach   |
| Peering Connections                    |  |
| Security                               |  |
| Network ACLs                           |  |
| Security Groups                        |  |
| VPN Connections                        |  |
| Customer Gateways                      | vgw-18954d06   VPG1  |
| Virtual Private Gateways               | Summary Tags   |
| VPN Connections                        | ID: vgw-18954d06   VPG1<br>State: detached<br>Type: ipsec.1<br>VPC:  |

## Step 6.

Create a VPN connection.



FieldValueName TagA human readable tag of the VPN connection between AWS and the ASA.Virtual Private GatewayChoose the VPG just created.Customer GatewayClick the Existing radio button and choose the gateway of the ASA.Routing OptionsClick the Dynamic (requires BGP) radio button.

| AWS 🗸 Service            | es 🗸 Edit 🗸   |
|--------------------------|---|
| VPC Dashboard            | Create VPN Connection Delete Download Configuration   |
| Filter by VPC:           | QSearch VPN Connections and X   |
| Virtual Private Cloud    | Name  VPN ID  Virtual Private Gateway  Customer Gateway   |
| Your VPCs                | You do not have   |
| Subnets                  |   |
| Route Tables             | Create VPN Connection ×   |
| Internet Gateways        |   |
| DHCP Options Sets        | 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. |
| Elastic IPs              |   |
| Endpoints                | Virtual Private Gateway   |
| NAT Gateways             | Customer Gateway O Existing O New   |
| Peering Connections      | cgw-837fa69d (64.100.251.37)   ASAVTI   |
| Security                 | Specify the routing for the VPN Connection (Help me choose) Routing Options Opnamic (requires BGP) Static   |
| Network ACLs             | VPN connection charges apply once this step is complete. View Rates   |
| Security Groups          |   |
| VPN Connections          | Cancel Yes, Create  |
| Customer Gateways        |   |
| Virtual Private Gateways |   |
| VPN Connections          |   |

## Step 7.

Configure the Route Table to propagate the routes learned from the VPG (via BGP) into the VPC.

| VPC Dashboard   Fitter by VPC:   None   Virtual Private Cloud   Your VPCs   Subnets   Route Tables   Note Tables   Note Tables   Note Tables   Out VPCs   Subnets   Route Tables   Note Tables   Name • Route Table ID • Explicitly Associations   Yes vpc-e1e00786 (172.31.0.016)   State Tables   Note Tables   Summary Routes   Superior  |                          |   |
|---|--------------------------|---|
| Filter by VPC:<br>None<br>Virtual Private Cloud<br>Your VPCs<br>Subnets<br>Route Tables<br>Internet Gateways<br>Peering Connections<br>Security<br>Network ACLs<br>Security<br>VPN Connections<br>Customer Gateways<br>VPN Connections<br>VPN Connections<br>VPN Connections<br>VPN Connections   | VPC Dashboard            | Create Route Table Delete Route Table Set As Main Table             |
| Virtual Private Cloud   Your VPCs   Subnets   Route Tables   Internet Gateways   DHCP Options Sets   Elastic IPs   Endpoints   Route Save   Pering Connections   Security   Network ACLs   Security Groups   VPN Connections   Virtual Private Gateways  | Filter by VPC:<br>None   | QSearch Route Tables and their X                                    |
| Your VPCs       Image: tb-3a3f9e5d       0 Subnets       Ves       vpc-e1e00786 (172.31.0.0/16)         Subnets       Route Tables       Image: tb-3a3f9e5d       Image: tb-3a3f9e5d         Internet Gateways       rtb-3a3f9e5d       Image: tb-3a3f9e5d       Image: tb-3a3f9e5d         DHCP Options Sets       Summary       Routes       Butter Propagation       Tags         Eadtic IPs       Summary       Routes       Subnet       Associations       Bedte Propagation       Tags         Endpoints       Cancel       Save       Virtual Private Cateways       Virtual Private Cateways       Vigw-18954d06   VPG1       Z         VPN Connections       Virtual Private Gateways       Virtual Private Gateways       Virtual Private Gateways       Virtual Private Gateways         VPN Connections       Ven Connections       Ven Connections       Ven Connections  | Virtual Private Cloud    | Name  A Route Table ID  Keplicitly Associat Keplicitly Associat VPC |
| Subnets   Route Tables   Internet Gateways   PtCP Options Sets   Elastic IPs   Endpoints   Cancel Save   NAT Gateways   Virtual Private Gateways   vgw-d19/47cf   vgw-d19/47   | Your VPCs                | rtb-3a3f9e5d 0 Subnets Yes vpc-e1e00786 (172.31.0.0/16)             |
| Route Tables   Internet Gateways   DHCP Options Sets   Elastic IPs   Endpoints   Cancel Save   NAT Gateways   Virtual Private Gateway   Peering Connections   vgw-d19/47cf   vgw-d19/47cf   vgw-d19/47cf   vgw-d19/47cf   VPN Connections   VPN Connections   Virtual Private Gateways   | Subnets                  |   |
| Internet Gateways rtb-3a3f9e5d   DHCP Options Sets Summary   Elastic IPs Summary   Endpoints Cancel Save   NAT Gateways Virtual Private Gateway   Peering Connections vgw-d19f47cf   Security vgw-1895dd06   VPG1 @   Network ACLs Security   VPN Connections VIRUAL Private Gateways   VIN Connections VIRUAL Private Gateways   VPN Connections VIRUAL Private Gateways   | Route Tables             |   |
| DHCP Options Sets   Elastic IPs   Endpoints   Cancel Save   NAT Gateways   Peering Connections   vgw-d19/47cf   vgw-18954d06   VPG1   Vertwork ACLs   Security   Network ACLs   Security Groups   VPN Connections   VItual Private Gateways   VPN Connections   VItual Private Gateways   VPN Connections   | Internet Gateways        | rtb-3a3f9e5d  |
| Elastic IPs Summary Routes Subnet Associations Butte Propagation Tags   Endpoints Cancel Save   NAT Gateways Virtual Private Gatewaya Propagate   Peering Connections vgw-d19f47cf   Security vgw-18954d06   VPG1   Network ACLs   Security Groups   VPN Connections   Customer Gateways   Virtual Private Gateways   VPN Connections   | DHCP Options Sets        |   |
| Endpoints Cancel Save   NAT Gateways Virtual Private Gateway   Peering Connections vgw-d19/47cf   Security vgw-18954d06   VPG1   Network ACLs Vgw-18954d06   VPG1   Security Groups VPN Connections   VPN Connections Vgw-18954d06   VPG1   Virtual Private Gateways Virtual Private Gateways   VPN Connections VIrtual Private Gateways  | Elastic IPs              | Summary Routes Subnet Associations Bottle Propagation Tags          |
| NAT Gateways Virtual Private Gateway   Peering Connections vgw-d19f47cf   vgw-18954d06   VPG1 vgw-18954d06   VPG1   Network ACLs vgw-18954d06   VPG1   Security Groups vgw-18954d06   VPG1   VPN Connections vgw-18954d06   VPG1   Virtual Private Gateways vgw-18954d06   VPG1   VPN Connections vgw-18954d06   VPG1   | Endpoints                | Cancel Save   |
| Peering Connections   vgw-d19f47cf   vgw-18954d06   VPG1   vgw-19954d06   VPG1   vgw-19954d06   Vgw-1995   vgw-19954d06   Vgw-19954d06   Vgw-1995   vgw-19954d06   Vgw- | NAT Gateways             | Virtual Private Gateway Propagate                                   |
| Security   Network ACLs   Security Groups   VPN Connections   Customer Gateways   Virtual Private Gateways   VPN Connections  | Peering Connections      | vgw-d19f47cf  |
| Network ACLs       Security Groups       VPN Connections       Customer Gateways       Virtual Private Gateways       VPN Connections   | Security                 | vgw-18954d06   VPG1   |
| Security Groups VPN Connections Customer Gateways Virtual Private Gateways VPN Connections  | Network ACLs             |   |
| VPN Connections<br>Customer Gateways<br>Virtual Private Gateways<br>VPN Connections   | Security Groups          |   |
| Customer Gateways<br>Virtual Private Gateways<br>VPN Connections  | VPN Connections          |   |
| Virtual Private Gateways VPN Connections  | Customer Gateways        |   |
| VPN Connections   | Virtual Private Gateways |   |
|   | VPN Connections          |   |
|   |                          |   |

## Step 8.

Download the suggested configuration. Choose the values below in order to generate a configuration that is a VTI style configuration.

## Field Value

Vendor Cisco Systems, Inc. Platform ISR Series Routers Software IOS 12.4+

| 🎁 AWS 🗸 Servi                           | ices 🗸 Edit 🗸   |
|---|---|
| VPC Dashboard<br>Filter by VPC:<br>None | Create VPN Connection Delete Download Configuration                                 |
| Virtual Private Cloud                   | Name - VPN ID - State - Virtual Private Gateway - Customer Gateway                  |
| Your VPCs                               | VPNtoASA vpn-7c79606e available vgw-18954d06   VPG1 cgw-837fa69d (64.1              |
| Subnets                                 |   |
| Route Tables                            |   |
| Internet Gateways                       | Download Configuration ×  |
| DHCP Options Sets                       | Disco shapes the configuration to download based on your type of systemer activupy  |
| Elastic IPs                             | Please choose the conliguration to download based on your type of customer gateway. |
| Endpoints                               | Pick Vendor Cisco Systems, Inc.  Platform ISB Series Bouters                        |
| NAT Gateways                            | IOS Software IOS 12.4+  |
| Peering Connections                     |   |
| Security                                | Cancel Yes, Download  |
| Network ACLs                            |   |
| Security Groups                         |   |
|   |   |
| VPN Connections                         |   |
| Customer Gateways                       |   |
| Virtual Private Gateways                |   |
| VPN Connections                         |   |
|   |   |

# **Configure the ASA**

Once you download the configuration there is some conversion necessary.

## Step 1.

```
crypto isakmp policy to \,\, {\rm crypto} ikev1 policy. Only one policy is needed since policy 200 and policy 201 are identical.
```

#### **Suggested Configuration**

```
crypto isakmp policy 200
encryption aes 128
authentication pre-share
group 2
lifetime 28800
hash sha
exit
crypto isakmp policy 201
encryption aes 128
authentication pre-share
group 2
```

#### То

crypto ikev1 enable outside crypto ikev1 policy 10 authentication pre-share encryption aes hash sha group 2 lifetime 28800

lifetime 28800 hash sha exit

#### Step 2.

crypto ipsec transform-set to crypto ipsec ikev1 transform-set. Only one transform-set is needed since the two transform-sets are identical.

#### **Suggested Configuration**

То

То

crypto ipsec transform-set ipsec-prop-vpn-7c79606e-0 esp-aes 128 esp-sha-hmac mode tunnel crypto ipsec ikev1 transfo exit crypto ipsec transform-set ipsec-prop-vpnset AWS esp-aes esp-sha-hm 7c79606e-1 esp-aes 128 esp-sha-hmac mode tunnel exit

#### Step 3.

| crypto  | ipsec   | profile <b>to</b> | crypto | ipsec   | profile. | Only | one | profile | is | needed |
|---------|---------|-------------------|--------|---------|----------|------|-----|---------|----|--------|
| since t | the two | profiles          | are id | lentica | 1.       |      |     |         |    |        |

```
То
crypto ipsec profile ipsec-vpn-7c79606e-0
 set pfs group2
set security-association lifetime seconds
3600
                                                crypto ipsec profile AWS
 set transform-set ipsec-prop-vpn-7c79606e-0
                                                 set ikev1 transform-set AWS
exit
                                                 set pfs group2
crypto ipsec profile ipsec-vpn-7c79606e-1
                                                 set security-association life
 set pfs group2
                                                seconds 3600
set security-association lifetime seconds
3600
 set transform-set ipsec-prop-vpn-7c79606e-1
exit
```

#### Step 4.

crypto keyring and crypto isakmp profile need to be converted to a tunnel-group one for each tunnel.

#### Suggested Configuration

```
crypto keyring keyring-vpn-7c79606e-0
                                                           tunnel-group
 local-address 64.100.251.37
                                                           52.34.205.227 type
pre-shared-key address 52.34.205.227 key QZhh90Bjf
                                                           ipsec-121
exit
                                                           tunnel-group
                                                           52.34.205.227 ipsec-
I
crypto isakmp profile isakmp-vpn-7c79606e-0
                                                           attributes
 local-address 64.100.251.37
                                                            ikev1 pre-shared-ke
                                                           QZhh90Bjf
match identity address 52.34.205.227
keyring keyring-vpn-7c79606e-0
                                                            isakmp keepalive
 exit
                                                           threshold 10 retry 1
```

```
!
                                                           tunnel-group
crypto keyring keyring-vpn-7c79606e-1
                                                           52.37.194.219 type
 local-address 64.100.251.37
                                                           ipsec-121
pre-shared-key address 52.37.194.219 key JjxCWy4Ae
                                                           tunnel-group
exit
                                                           52.37.194.219 ipsec-
1
                                                           attributes
crypto isakmp profile isakmp-vpn-7c79606e-1
                                                            ikev1 pre-shared-ke
 local-address 64.100.251.37
                                                           JjxCWy4Ae
match identity address 52.37.194.219
                                                            isakmp keepalive
keyring keyring-vpn-7c79606e-1
                                                           threshold 10 retry 1
exit
```

#### Step 5.

The tunnel configuration is almost identical. The ASA does not support the ip tcp adjust-mss or the ip virtual-reassembly command.

#### **Suggested Configuration**

#### То

| interface Tunnel1                          |                                |
|--|--------------------------------|
| ip address 169.254.13.190 255.255.255.252  |                                |
| ip virtual-reassembly                      | interface Tunnel1              |
| tunnel source 64.100.251.37                | nameif AWS1                    |
| tunnel destination 52.34.205.227           | ip address 169.254.13.190      |
| tunnel mode ipsec ipv4                     | 255.255.255.252                |
| tunnel protection ipsec profile ipsec-vpn- | tunnel source interface outsid |
| 7c79606e-0                                 | tunnel destination 52.34.205.  |
| ip tcp adjust-mss 1387                     | tunnel mode ipsec ipv4         |
| no shutdown                                | tunnel protection ipsec profi  |
| exit                                       | AWS                            |
| !  | !                              |
| interface Tunnel2                          | interface Tunnel2              |
| ip address 169.254.12.86 255.255.255.252   | nameif AWS2                    |
| ip virtual-reassembly                      | ip address 169.254.12.86       |
| tunnel source 64.100.251.37                | 255.255.255.252                |
| tunnel destination 52.37.194.219           | tunnel source interface outsid |
| tunnel mode ipsec ipv4                     | tunnel destination 52.37.194.  |
| tunnel protection ipsec profile ipsec-vpn- | tunnel mode ipsec ipv4         |
| 7c79606e-1                                 | tunnel protection ipsec profi  |
| ip tcp adjust-mss 1387                     | AWS                            |
| no shutdown                                |                                |
| exit                                       |                                |

### Step 6.

In this example, the ASA will only advertise up the inside subnet (192.168.1.0/24) and receive the subnet within AWS (172.31.0.0/16).

#### Suggested Configuration

```
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
```

To 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 169.254.13.189 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
  network 0.0.0.0
  exit
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
  neighbor 169.254.12.85 timers 10 30 30
  neighbor 169.254.12.85 default-originate
  neighbor 169.254.12.85 activate
  neighbor 169.254.12.85 soft-reconfiguration
inbound
  network 0.0.0.0
  exit
exit
```

```
neighbor 169.254.12.85
activate
  neighbor 169.254.13.189
remote-as 7224
  neighbor 169.254.13.189
activate
  network 192.168.1.0
  no auto-summary
  no synchronization
  exit-address-family
```

# Verify and Optimize

#### Step 1.

Confirm the ASA establishes the IKEv1 security associations with the two endpoints at AWS. The state of the SA should be 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#

Step 2.
```

```
Confirm the IPsec SAs are installed on ASA. There should be an inbound and outbound SPI installed for each peer and there should be some encaps and decaps counters incrementing.
```

```
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 0xfffffff 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: 0x0000000 0x0000001 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:
     0xfffffff 0xfffffff
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:
      0x0000000 0x0000001
```

#### Step 3.

On the ASA, confirm that BGP connections are established with AWS. The State/PfxRcd counter should be 1 as AWS advertises the 172.31.0.0/16 subnet towards the 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

#### Step 4.

On the ASA, verify that the route to 172.31.0.0/16 has been learned via the tunnel interfaces. This output shows that there are two paths to 172.31.0.0 from peer 169.254.12.85 and 169.254.13.189. The path towards 169.254.13.189 out Tunnel 2 (AWS2) is preferred because of the lower metric.

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 169.254.12.84 255.255.255.255.252 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 169.254.13.190 255.255.255.255.255 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

In order to ensure that traffic which returns from AWS follows a symmetric path, configure a route-map to match the preferred path and adjust BGP to alter the advertised routes.

```
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
Step 6.
```

#### On the ASA, confirm that 192.168.1.0/24 is advertised to 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

#### Step 7.

In AWS, confirm that the tunnels for the VPN connection are UP and routes are learned from the peer. Also check that the route has been propagated into the routing table.

| 🎁 AWS 🗸 Servi            | Des V Edit V  | Jay AWS 👻 |
|--------------------------|---|-----------|
| VPC Dashboard            | Create VPN Connection Delete Download Configuration   |           |
| None                     | QSearch VPN Connections and X   |           |
| Virtual Private Cloud    | Name  VPN ID  Virtual Private Gateway  Customer Gateway  VPC  VPC   | Routing   |
| Your VPCs                | VPNtoASA vpn-7c76606e available vgw-18954d06   VPG1 cgw-837/te89d (64.100.251.37)   ASAVTI 64.100.251.37 ipsec.1 vpc-e1e00786 (172.31.0.0/16) | Dynamic   |
| Subnets                  |   |           |
| Route Tables             |   |           |
| Internet Gateways        |   |           |
| DHCP Options Sets        |   |           |
| Elastic IPs              |   |           |
| Endpoints                |   |           |
| NAT Gateways             |   |           |
| Peering Connections      | vpn-7c79606e   VPNtoASA   |           |
| Security                 | Summary Tunnel Details Static Routes Tags   |           |
| Network ACLs             | VPN Tunnel IP Address Status Status Last Changed Deams  |           |
| Security Groups          | Tunnel 1 52.34.205.227 UP 2016-10-18 14:23 UTC 4 1 BGP ROUTES   |           |
| VPN Connections          | Tunnel 2 52.37.194.219 UP 2016-10-18 14:23 UTC- 1 BGP ROUTES  |           |
| Customer Gateways        |   |           |
| Virtual Private Gateways |   |           |
| VPN Connections          |   |           |

| T AWS V Services V Edit V |   |              |            |             |               |         |            |                    |             |   |
|---------------------------|---|--------------|------------|-------------|---------------|---------|------------|--------------------|-------------|---|
| VPC Dashboard             | Create Route Table Delete Route Table Set As Main Table |              |            |             |               |         |            |                    |             |   |
| None                      | QSearch Route Tables and their X                        |              |            |             |               |         |            |                    |             |   |
| Virtual Private Cloud     | Name  | <b>▲</b>     | Route Ta   | ible ID 🚽 I | Explicitly As | ssocial | Main 👻     | VPC                |             | - |
| Your VPCs                 |   | 1            | rtb-3a3f9e | e5d (       | 0 Subnets     |         | Yes        | vpc-e1e00786 (172. | .31.0.0/16) |   |
| Subnets                   |   |              |            |             |               |         |            |                    |             |   |
| Route Tables              |   |              |            |             |               |         |            |                    |             |   |
| Internet Gateways         |   |              |            |             |               |         |            |                    |             |   |
| DHCP Options Sets         |   |              |            |             |               |         |            |                    |             |   |
| Elastic IPs               |   |              |            |             |               |         |            |                    |             |   |
| Endpoints                 |   |              |            |             |               |         |            |                    |             |   |
| NAT Gateways              |   |              |            |             |               |         |            |                    |             |   |
| Peering Connections       | rtb-3a3f9e5d  |              |            |             |               |         |            |                    |             |   |
| Security                  | Summary   | Route        | s          | Subnet Asso | ciations      | Route P | ropagation | Tags               |             |   |
| Network ACLs              | Edit  |              |            |             |               |         |            |                    |             |   |
| Security Groups           | Destination   | Target       | Status     | Propagate   | d             |         |            |                    |             |   |
| VPN Connections           | 172.31.0.0/16   | local        | Active     | No          |               |         |            |                    |             |   |
| Customer Gateways         | 0.0.0/0   | igw-e5ad1481 | Active     | No          |               |         |            |                    |             |   |
| Virtual Private Gateways  | 192.168.1.0/24  | vgw-18954d06 | Active     | Yes         |               |         |            |                    |             |   |
| VPN Connections           |   |              |            |             |               |         |            |                    |             |   |