

ASA IPsec لاصتال Amazon بي و تام دخ ني وكت VTI

المحتويات

[المقدمة](#)

[تكوين AWS](#)

[تكوين ASA](#)

[التحقق من الصحة وتحسينها](#)

المقدمة

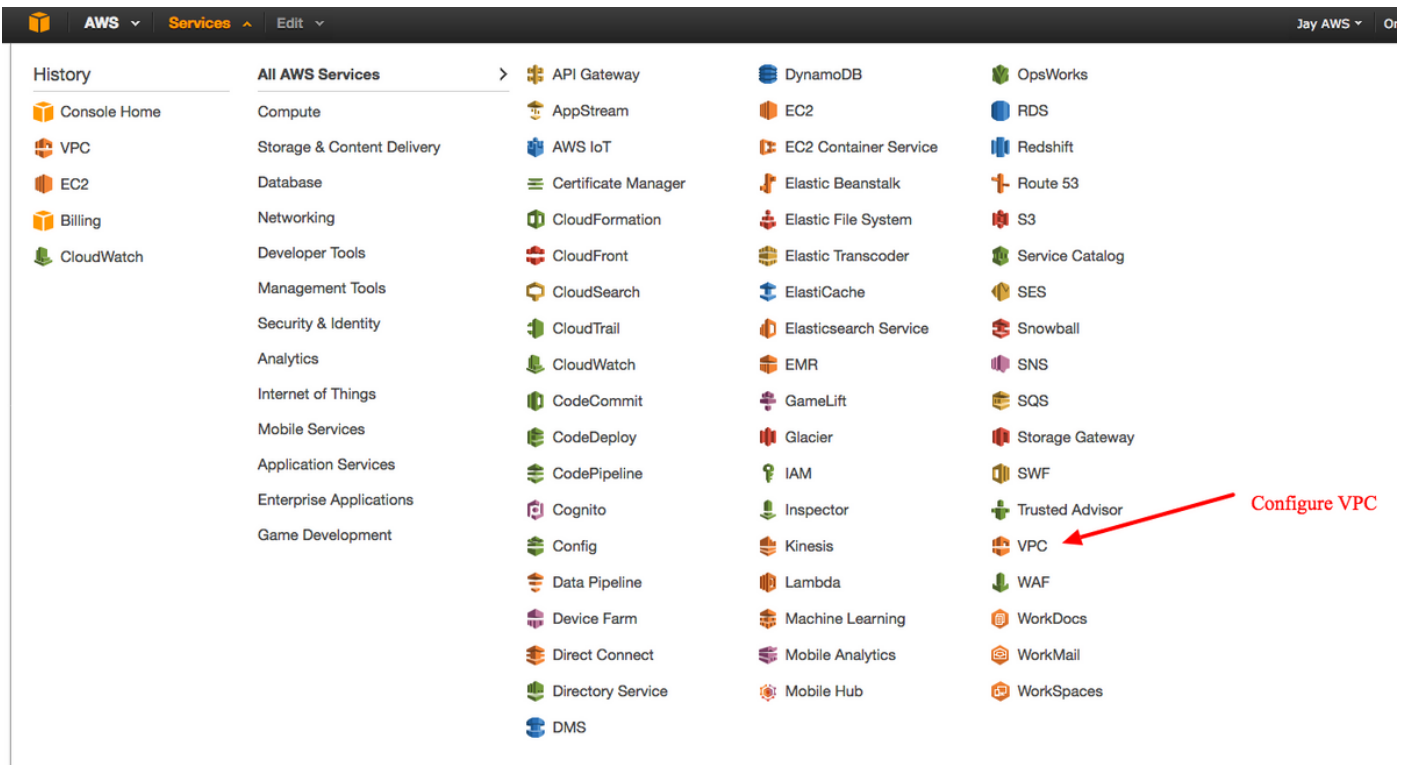
يوضح هذا المستند كيفية تكوين اتصال واجهة النفق الظاهرية (VTI) لتطبيق الأمان القابل للتكيف (ASA) عبر بروتوكول IPsec. في ASA 9.7.1، تم إدخال VTI لبروتوكول IPsec. وهو مقصور على sVTI IPv4 عبر IPv4 باستخدام IKEv1 في هذا الإصدار. هذا مثال لتكوين ASA للاتصال بخدمات ويب (AWS) (Amazon).

ملاحظة: يتم دعم VTI حاليا في وضع موجه أحادي السياق فقط.

تكوين AWS

الخطوة 1.

سجل الدخول إلى وحدة تحكم AWS وانتقل إلى لوحة VPC.



انتقل إلى لوحة معلومات VPC

الخطوة 2.

تأكد من إنشاء سحابة خاصة ظاهرية (VPC) بالفعل. افتراضيا، يتم إنشاء VPC مع 16/172.31.0.0. هذا هو المكان الذي سيتم فيه توصيل الأجهزة الظاهرية (VM).

The screenshot shows the AWS VPC Dashboard. On the left, there is a navigation menu with 'Your VPCs' circled in red. The main area displays a table of VPCs with the following columns: Name, VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default VPC. A single VPC is listed with ID vpc-e1e00786, State available, and CIDR 172.31.0.0/16. Below the table, the details for this VPC are shown, including VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, DNS resolution, DNS hostnames, and ClassicLink DNS Support. A red arrow points from the text 'Default VPC already created' to the VPC ID in the table.

الخطوة 3.

إنشاء "بوابة عميل". هذه نقطة نهاية تمثل ASA.

الحقل

علامة الاسم

توجيه

عنوان IP

BGP ASN

القيمة
هذا
اسم
يمكن
قراءت
للتعرف
ASA
دينامي
هذا
أنه س
إستخ
بروتو
العبار
الحدو
(BGP)
لتبادل
معلو
التوج
هذا
عنوان
العام
لواجه
ASA
الخارج
رقم

الذاتي
لعملية
BGP
التشغيل
على
أستخدام
5000
لم يكن
للمؤسسة
رقم
عام.

The screenshot shows the AWS Management Console interface for creating a Customer Gateway. The 'Create Customer Gateway' dialog box is open, showing the following configuration:

- Name tag: ASAVTI
- Routing: Dynamic
- IP address: 192.0.2.1
- BGP ASN: 65000

The dialog box also includes a 'Cancel' button and a 'Yes, Create' button. Below the dialog box, the details for the Customer Gateway 'cgw-b778a1a9 (64.100.251.37)' are displayed, including its ID, State (deleted), Type (ipsec.1), IP address (64.100.251.37), and BGP ASN (65000).

الخطوة 4.

إنشاء بوابة خاصة ظاهرية (VPG). هذا موجه محاكي يتم إستضافته مع AWS الذي ينهي نفق IPsec.

الحقل

القيمة
اسم يمكن
قراءته من قبل
الإنسان
للتعرف على

علامة الاسم

.VPG

The screenshot displays the AWS Management Console interface. At the top, there are navigation tabs for 'AWS', 'Services', and 'Edit'. The main content area is titled 'VPC Dashboard' and includes a 'Filter by VPC:' dropdown set to 'None'. Below this, there are several buttons: 'Create Virtual Private Gateway' (highlighted in blue), 'Delete Virtual Private Gateway', 'Attach to VPC', and 'Detach from VPC'. A search bar for 'Virtual Private Gateway' is visible. A modal dialog box titled 'Create Virtual Private Gateway' is open in the foreground. It contains the following text: 'A virtual private gateway is the router on the Amazon side of the VPN tunnel.' Below this, there is a 'Name tag' input field with the value 'VPG1' and an information icon. At the bottom right of the dialog are 'Cancel' and 'Yes, Create' buttons. The background shows a sidebar with navigation options: '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' (highlighted), and 'VPN Connections'. Below the dialog, the text 'Select a virtual private gateway above' is visible.

الخطوة 5.

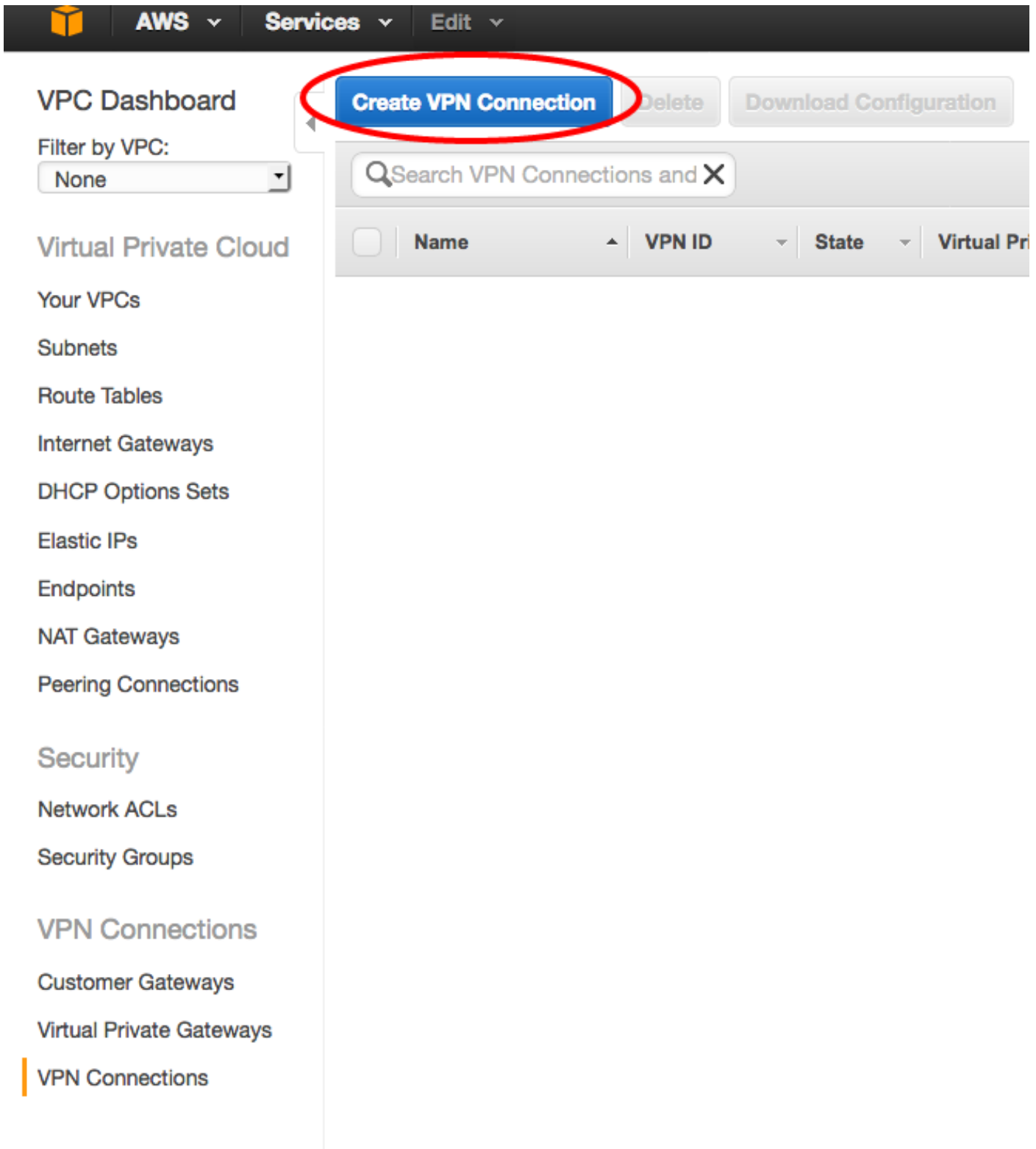
إرفاق ال VPG إلى ال VPC.

أخترت الفعلي خاص مدخل، طقطقت يربط إلى VPC، يختار ال VPC من ال VPC منسدل قائمة، وطققة نعم، يربط.

The screenshot displays 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'. A table lists the virtual private gateways, with 'VPG1' (ID: vgw-18954d06, State: detached, Type: ipsec.1) selected. A modal dialog titled 'Attach to VPC' is open, showing a dropdown menu for selecting a VPC. The selected VPC is 'vpc-e1e00786 (172.31.0.0/16)'. The dialog includes 'Cancel' and 'Yes, Attach' buttons. A red arrow points from the 'Attach to VPC' button in the top navigation bar to the 'Yes, Attach' button in the dialog. Below the dialog, the details for 'vgw-18954d06 | VPG1' are shown, including its ID, state (detached), and type (ipsec.1).

الخطوة 6.

إنشاء اتصال VPN.



القيمة
علامة قابلة للقراءة بشرية
لاتصال VPN بين AWS و
.ASA
أخترت ال VPG فقط يخلق.
طقطقت **الحالي** لاسلكي زر
واخترت البوابة من ال .ASA.
انقر زر الخيار ديناميكي (يتطلب
.BGP)

الحقل
علامة الاسم
البوابة الخاصة الظاهرية
بوابة العميل
خيارات التوجيه

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 VPN Connection Delete Download Configuration

Search VPN Connections and X

Name VPN ID State Virtual Private Gateway Customer Gateway

You do not have

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)

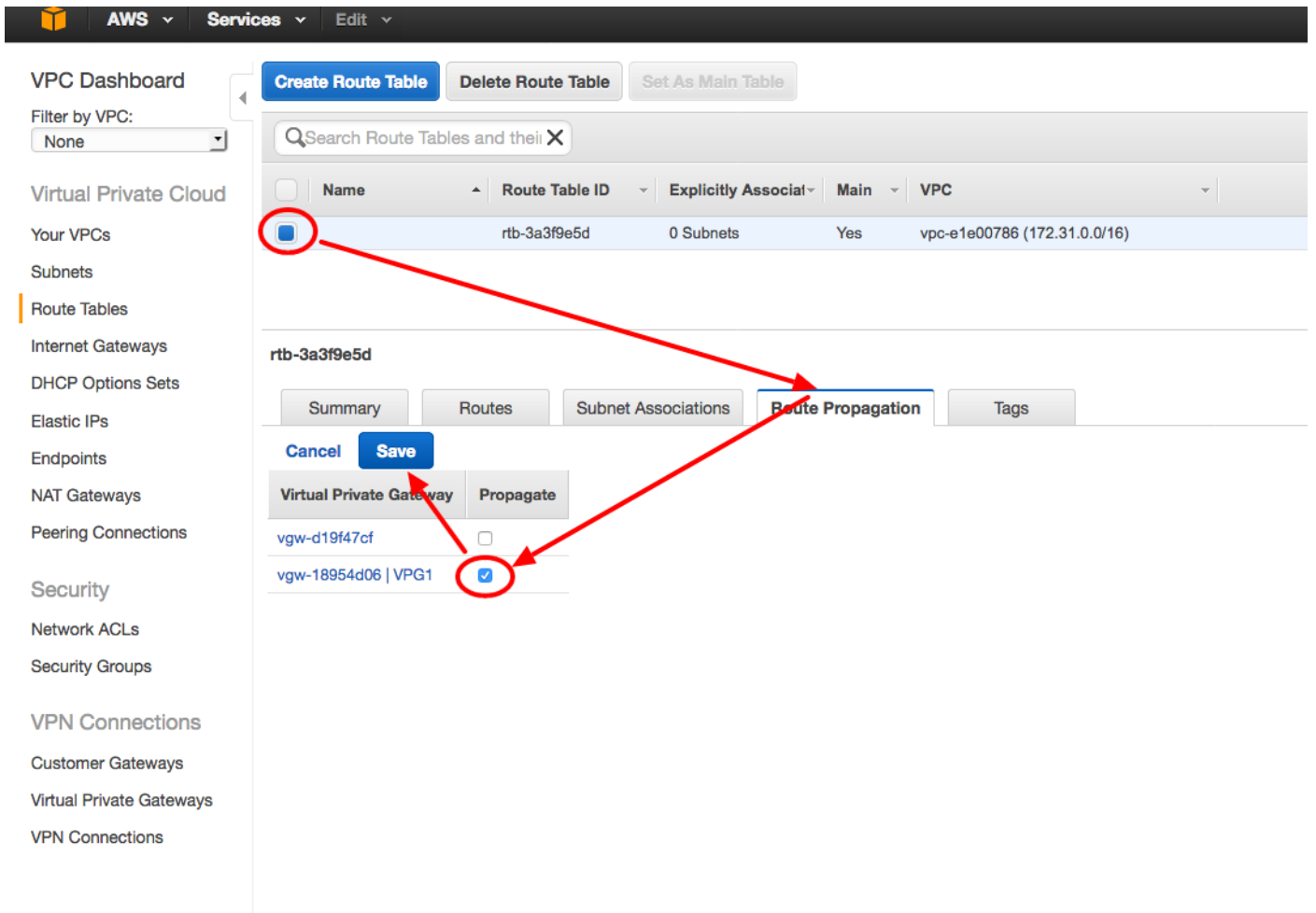
Routing Options Dynamic (requires BGP) Static

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

Cancel Yes, Create

الخطوة 7.

قم بتكوين جدول المسار لنشر المسارات التي تم التعرف عليها من VPG (عبر BGP) إلى جهاز الكمبيوتر الشخصي (VPC).



الخطوة 8.

قم بتنزيل التكوين المقترح. اخترت القيمة أدناه in order to خلقت تشكيل أن يكون VTI أسلوب تشكيل.

القيمة
Cisco Systems,
.Inc
سلسلة موجهات
IOS 12.4+

الحقل
البائع
النظام الأساسي
البرنامج

The screenshot shows the AWS Management Console interface for VPN Connections. A modal dialog titled 'Download Configuration' is open, asking the user to select configuration options. The 'Vendor' is set to 'Cisco Systems, Inc.', 'Platform' is 'ISR Series Routers', and 'Software' is 'IOS 12.4+'. The 'Yes, Download' button is circled in red. A red arrow points from the 'Download Configuration' button in the top navigation bar to the dialog box.

تكوين ASA

بمجرد تنزيل التكوين، يلزم إجراء بعض عمليات التحويل.

الخطوة 1.

سياسة crypto isakmp إلى سياسة crypto ikev1. هناك حاجة إلى سياسة واحدة فقط لأن السياسة 200 والسياسة 201 متطابقتان.

إلى

تمكين crypto ikev1 خارج
 سياسة crypto ikev1 10
 مشاركة مسبقة للمصادقة
 تشفير AES
 تجزئة
 المجموعة الثانية
 مدى الحياة 28800

التكوين المقترح

سياسة Crypto ISAKMP 200
 التشفير AES 128
 مشاركة مسبقة للمصادقة
 المجموعة الثانية
 مدى الحياة 28800
 تجزئة
 مخرج
 سياسة Crypto ISAKMP 201
 التشفير AES 128
 مشاركة مسبقة للمصادقة
 المجموعة الثانية

الخطوة 2.

مجموعة تحويل IPsec crypto ikev1 إلى مجموعة تحويل. هناك حاجة إلى مجموعة تحويل واحدة فقط لأن مجموعتي التحويل متطابقتان.

إلى

التكوين المقترح

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

مخرج

```
crypto ipSec ikev1 transform-set AWS esp-aes esp-  
sha-hmac
```

```
crypto ipSec transform-set  
ipsec-prop-vpn-7c79606e-1 esp-  
aes 128 esp-sha-hmac  
نفق النمط
```

مخرج

الخطوة 3.

ملف تعريف IPsec المشفر إلى ملف تعريف IPsec. يحتاج الأمر إلى ملف تعريف واحد فقط لأن النصفين متطابقان.

إلى

التكوين المقترح

```
crypto ipSec profile ipSec-vpn-  
7c79606e-0
```

مجموعة ملفات 2 PFS

تعيين ثواني العمر لاقتران الأمان
3600

```
set transform-set ipSec-prop-vpn-  
7c79606e-0
```

مخرج

```
AWS لملف تعريف IPsec للتشفير  
set ikev1 transform-set AWS
```

مجموعة ملفات 2 PFS

تعيين ثواني العمر لاقتران الأمان 3600

```
crypto ipSec profile ipSec-vpn-  
7c79606e-1
```

مجموعة ملفات 2 PFS

تعيين ثواني العمر لاقتران الأمان
3600

```
set transform-set ipSec-prop-vpn-  
7c79606e-1
```

مخرج

الخطوة 4.

يلزم تحويل حلقة مفاتيح التشفير وتوصيف ISAKMP إلى واحد لمجموعة النفق لكل نفق.

إلى

التكوين المقترح

```
ipSEC-121 نوع tunnel-group 52.34.205.227  
سمات بروتوكول IPsec لمجموعة النفق 52.34.205.227
```

ikev1 مفتاح مشترك مسبقا QZhh90Bjf

إعادة المحاولة لعتبة رسائل تنشيط الاتصال 10 من ISAKMP
10

```
ipSEC-121 نوع tunnel-group 52.37.194.219
```

```
crypto keyRing-vpn-  
7c79606e-0
```

العنوان المحلي

64.100.251.37

عنوان مفتاح مشترك مسبقا

52.34.205.227 مفتاح

QZhh90Bjf

مخرج

!

crypto isakmp profile

isakmp-vpn-7c79606e-0

العنوان المحلي

64.100.251.37

مطابقة عنوان الهوية

52.34.205.227

keyRing-vpn-7c79606e-0

مخرج

!

crypto keyRing-vpn-

7c79606e-1

العنوان المحلي

64.100.251.37

عنوان مفتاح مشترك مسبقا

52.37.194.219 مفتاح

JjxCWy4Ae

مخرج

!

crypto isakmp profile

isakmp-vpn-7c79606e-1

العنوان المحلي

64.100.251.37

مطابقة عنوان الهوية

52.37.194.219

keyRing-vpn-7c79606e-1

مخرج

الخطوة 5.

تكوين النفق متطابق تقريبا. لا يدعم ASA الأمر ip tcp adjust-mss أو الأمر ip virtual-reassembly.

إلى

التكوين المقترح

نفق الواجهة 1

عنوان IP 169.254.13.190

255.255.255.252

إعادة التجميع الظاهري ل IP

مصدر النفق 64.100.251.37

وجهة النفق 52.34.205.227

بروتوكول IPv4 لوضع النفق

حماية النفق لملف تعريف IPsec-vpn-

7c79606e-0

ip tcp adjust-mss 1387

عدم إيقاف التشغيل

مخرج

!

نفق الواجهة 2

عنوان IP 169.254.12.86

255.255.255.252

إعادة التجميع الظاهري ل IP

مصدر النفق 64.100.251.37

نفق الواجهة 1

اسم AWS1

عنوان IP 169.254.13.190 255.255.255.252

واجهة مصدر النفق خارج

وجهة النفق 52.34.205.227

بروتوكول IPv4 لوضع النفق

AWS لملف تعريف IPsec لحماية النفق

!

نفق الواجهة 2

ناميف AWS2

عنوان IP 169.254.12.86 255.255.255.252

واجهة مصدر النفق خارج

وجهة النفق 52.37.194.219

بروتوكول IPv4 لوضع النفق

AWS لملف تعريف IPsec لحماية النفق

وجهة النفق 52.37.194.219
بروتوكول IPv4 لوضع النفق
حماية النفق ملف تعريف IPsec-vpn-
7c79606e-1
ip tcp adjust-mss 1387
عدم إيقاف التشغيل
مخرج

الخطوة 6.

في هذا المثال، سيقوم ASA بالإعلان فقط عن الشبكة الفرعية الداخلية (24/192.168.1.0) واستلام الشبكة الفرعية داخل (AWS (172.31.0.0/16).

إلى

التكوين المقترح

```
BGP 65000 الموجه
remote- 169.254.13.189 المجاور
as 7224
يتم تنشيط المجاور
169.254.13.189
جار 169.254.13.189 وحدة توقيت
30 30 10
البث الأحادي لعائلة العنوان IPv4
remote- 169.254.13.189 المجاور
as 7224
جار 169.254.13.189 وحدة توقيت
30 30 10
جار 169.254.13.189 مصدر
افتراضي
يتم تنشيط المجاور
169.254.13.189
جار 169.254.13.189 إعادة تكوين
ناعم وارد
الشبكة 0.0.0.0
مخرج
BGP 65000 الموجه
BGP log-neighbor-changes
عدادات الوقت 0 30 10
البث الأحادي لعائلة العنوان IPv4
remote-as 7224 169.254.12.85 المجاور
169.254.12.85 المجاور
remote-as 7224 169.254.13.189 المجاور
يتم تنشيط المجاور 169.254.13.189
الشبكة 192.168.1.0
لا يوجد تلخيص تلقائي
لا توجد مزامنة
exit-address-family
BGP 65000 الموجه
remote-as 169.254.12.85 المجاور
7224
يتم تنشيط المجاور 169.254.12.85
المجاور 169.254.12.85 وحدة
توقيت 30 30 10
البث الأحادي لعائلة العنوان IPv4
remote- 169.254.12.85 المجاور
as 7224
المجاور 169.254.12.85 وحدة
توقيت 30 30 10
جار 169.254.12.85 مصدر افتراضي
يتم تنشيط المجاور
169.254.12.85
جار 169.254.12.85 إعادة تكوين
ناعم وارد
الشبكة 0.0.0.0
مخرج
```

التحقق من الصحة وتحسينها

الخطوة 1.

قم بتأكيد ASA بإنشاء اقترانات أمان IKEv1 مع نقطتي النهاية في AWS. يجب أن تكون حالة SA 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
IKE Peer: 52.37.194.219 1
Type      : L2L      Role      : initiator
Rekey     : no      State     : MM_ACTIVE
IKE Peer: 52.34.205.227 2
Type      : L2L      Role      : initiator
Rekey     : no      State     : MM_ACTIVE
#ASA
```

الخطوة 2.

تأكد من تثبيت أسماء IPsec على ASA. يجب أن يكون هناك SPI وارد ومصادر مثبت لكل نظير ويجب أن تكون هناك بعض عمليات إضافة وعدادات قطع الاتصال متزايدة.

```
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

الخطوة 3.

على ASA، تأكد من إنشاء اتصالات BGP باستخدام AWS. يجب أن يكون عداد 1 STATE/PFXrcd حيث إن AWS تعلن عن الشبكة الفرعية 16/172.31.0.0 تجاه 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
    network entries using 400 bytes of memory 2
    path entries using 240 bytes of memory 3
  BGP path/bestpath attribute entries using 624 bytes of memory 3/2
    BGP AS-PATH entries using 24 bytes of memory 1
    BGP route-map cache entries using 0 bytes of memory 0
    BGP filter-list cache entries using 0 bytes of memory 0
    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
1 03:41:31 0      0     5       1161   1332  7224      4    169.254.12.85
1 03:42:02 0      0     5       1164   1335  7224      4    169.254.13.189
```

الخطوة 4.

على ASA، تحقق من أنه قد تم تعلم المسار إلى 16/172.31.0.0 عبر واجهات النفق. يوضح هذا الإخراج أن هناك مسارين إلى 172.31.0.0 من النظير 169.254.12.85 و 169.254.13.189. يفضل المسار نحو 169.254.13.189 خارج النفق 2 (AWS2) بسبب المقياس الأدنى.

```
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
i 7224 0	200	169.254.12.85			172.31.0.0 *
i 7224 0	100	169.254.13.189			<*
i 32768	0	0.0.0.0			192.168.1.0 <*

```
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

```

الخطوة 5.

لضمان أن حركة المرور التي ترجع من AWS تتبع مسار متماثل، قم بتكوين خريطة مسار لمطابقة المسار المفضل وضبط BGP لتغيير الموجهات المعلن عنها.

```

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

```

الخطوة 6.

على ASA، تأكد من الإعلان عن 24/192.168.1.0 لـ 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
i 7224 0	100	169.254.13.189			172.31.0.0 <*
i 32768	0	0.0.0.0			192.168.1.0 <*

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
i 32768	0	0.0.0.0			192.168.1.0 <*

Total number of prefixes 1

الخطوة 7.

في AWS، تأكد من تشغيل أنفاق اتصال VPN وتعلم المسارات من النظير. تحقق أيضا من نشر المسار في جدول التوجيه.

AWS Services Edit Jay AWS

VPC Dashboard Create VPN Connection Delete Download Configuration

Filter by VPC: None

Search VPN Connections and X

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

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

vpn-7c79606e | VPNtoASA

Summary Tunnel Details Static Routes Tags

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

AWS Services Edit

VPC Dashboard Create Route Table Delete Route Table Set As Main Table

Filter by VPC: None

Search Route Tables and their X

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

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

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

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س مل ا ذه Cisco ت مچرت
م ل اع ل اء ان ا ع مچ ي ف ن م دخت س مل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ى ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س مل ا