تكوين نفق IPSec IKEv1 من موقع إلى موقع بين ASA ومُوجّه Cisco IOS

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق IKEv1 من موقع إلى موقع (LAN-to-LAN) عبر واجهة سطر الأوامر (CLI) بين Cisco ASA وموجه يعمل ببرنامج Cisco IOS®.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IOS من Cisco
- أجهزة الأمان المعدلة Cisco Adaptive Security Appliances (ASA)
- مفاهيم IPSec العامة

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 5512-X Series ASA أن يركض برمجية صيغة 9.4(1)
- موجه الخدمات المتكاملة Cisco 1941 Series Integrated Services Router (ISR) الذي يشغل برنامج Cisco IOS، الإصدار 15.4(3)M2

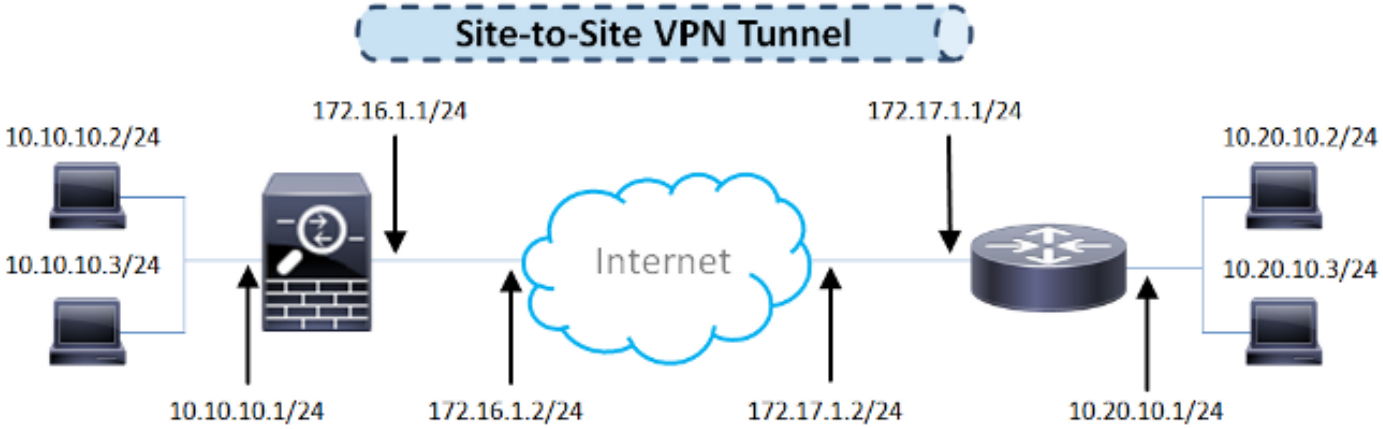
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يصف هذا القسم كيفية إكمال تكوينات ASA و CISCO IOS Router CLI.

الرسم التخطيطي للشبكة

تستخدم المعلومات الواردة في هذا المستند إعداد الشبكة التالي:



تكوين ASA

تكوين واجهات ASA

إذا لم يتم تكوين واجهات ASA، فتأكد من تكوين عناوين IP وأسماء الواجهة ومستويات الأمان على الأقل:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

ملاحظة: تأكد من وجود اتصال بالشبكات الداخلية والخارجية على حد سواء، وخاصة بالشبكات النظيرة البعيدة التي يتم إستخدامها لإنشاء نفق شبكة VPN من موقع إلى موقع. يمكنك إستخدام إختبار الاتصال للتحقق من الاتصال الأساسي.

تكوين نهج IKEv1 وتمكين IKEv1 على الواجهة الخارجية

لتكوين سياسات اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) للاتصالات الإصدار 1 (IKEv1) من مفتاح الإنترنت IPSec، أدخل crypto ikev1 policy :

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

ملاحظة: توجد مطابقة لسياسة IKEv1 عندما تحتوي كل النهج على قيم معلمات نفسها. بالنسبة لـ IKEv1، يجب أيضا أن تحدد نهج النظير البعيد فترة بقاء أقل من أو تساوي فترة البقاء في النهج الذي يرسله البادئ. وإذا كانت فترات الحياة غير متطابقة، يستخدم ASA فترة الحياة الأقصر.

ملاحظة: إذا لم تحدد قيمة لمعلمة نهج معينة، يتم تطبيق القيمة الافتراضية.

يجب أن تكون IKEv1 على الأقل على الواجهة التي تنهي VPN. بشكل نموذجي، هذه هي الواجهة الخارجية (أو العامة). لتمكين IKEv1، أدخل crypto ikev1 enable في وضع التكوين العام:

```
crypto ikev1 enable outside
```

تكوين مجموعة النفق (ملف تعريف اتصال شبكة LAN إلى شبكة LAN)

بالنسبة لنفق من شبكة LAN إلى شبكة LAN، يكون نوع ملف تعريف الاتصال ipsec-l2l . دخلت in order to شكلت الـ IKEv1 مبرم مفاتيح، الـ tunnel-group ipsec-attributes وضع التكوين:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

تكوين قائمة التحكم في الوصول لحركة مرور VPN ذات الاهتمام

يستخدم ASA قوائم التحكم في الوصول (ACLs) للتمييز بين حركة المرور التي يجب حمايتها باستخدام تشفير IPSec وحركة المرور التي لا تتطلب الحماية. وهو يحمي الحزم الصادرة التي تطابق محرك التحكم في التطبيق (ACE) المسموح به ويضمن أن الحزم الواردة التي تطابق إدخال التحكم في الوصول (ACE) المسموح به تحتوي على حماية.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

ملاحظة: تستخدم قائمة التحكم في الوصول لحركة مرور VPN عناوين IP المصدر والوجهة بعد ترجمة عنوان الشبكة (NAT).

ملاحظة: يجب نسخ قائمة التحكم في الوصول لحركة مرور VPN على كل من نظراء VPN.

ملاحظة: إذا كانت هناك حاجة إلى إضافة شبكة فرعية جديدة إلى حركة المرور المحمية، فما عليك سوى إضافة شبكة فرعية/مضيف إلى مجموعة الكائنات المعنية وإكمال تغيير معكوس على نظير VPN البعيد.

تكوين إستثناء NAT

ملاحظة: التكوين الموضح في هذا القسم إختياري.

بشكل نموذجي، يجب أن يكون هناك NAT تجنب على VPN حركة مرور. من أجل إستثناء حركة المرور تلك، يجب عليك إنشاء قاعدة NAT للهوية. عرف nat يترجم قاعدة عنوان بسبب إلى نفس عنوان.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

تكوين مجموعة تحويل IKEv1

مجموعة تحويل IKEv1 هي مجموعة من بروتوكولات الأمان والخوارزميات التي تحدد الطريقة التي تحمي بها البيانات من خلال ASA. أثناء مفاوضات "اقتران أمان IPSec (SA)"، يجب على النظراء تحديد مجموعة تحويل أو اقتراح مماثل لكل من النظراء. ثم يطبق ASA مجموعة التحويل أو الاقتراح المتطابق لإنشاء SA الذي يحمي تدفقات البيانات في قائمة الوصول الخرائطية التشفير تلك.

دخلت in order to شكلت ال IKEv1 تحويل مجموعة، crypto ipsec ikev1 transform-set :

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

تكوين خريطة تشفير وتطبيقها على واجهة

تحدد خريطة التشفير سياسة IPSec التي سيتم التفاوض عليها في IPSec SA وتتضمن:

- قائمة وصول لتحديد الحزم التي يسمح بها اتصال IPSec ويحميها
- تعريف النظير
- عنوان محلي لحركة مرور IPSec
- مجموعات تحويل IKEv1

فيما يلي مثال:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

يمكنك بعد ذلك تطبيق خريطة التشفير على الواجهة:

```
crypto map outside_map interface outside
```

التكوين النهائي ASA

فيما يلي التكوين النهائي للملحق التقني المتقدم (ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
```

```
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

تكوين واجهة سطر الأوامر لموجه Cisco IOS

تكوين الواجهات

إذا لم يتم تكوين واجهات موجه Cisco IOS بعد، فيجب تكوين واجهات LAN و WAN على الأقل. فيما يلي مثال:

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
no shutdown
```

تأكد من وجود اتصال بالشبكات الداخلية والخارجية على حد سواء، وخاصة بالشبكات التي يتم إستخدامها لإنشاء نفق شبكة VPN من موقع إلى موقع. يمكن إستخدام إختبار الاتصال للتحقق من الاتصال الأساسي.

تكوين سياسة ISAKMP (IKEv1)

دخلت in order to شكلت ال isakmp سياسة ل ال IKEv1 توصيل، ال crypto isakmp policy في وضع التكوين العام. فيما يلي مثال:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

ملاحظة: يمكن تكوين سياسات IKE متعددة على كل نظير يشارك في IPSec. عند تكوين سياسات IKE، فإن الجوار على سياسة مشتركة تم تكوينها على كل من النظراء، وتبدأ بسياسات الأولوية العليا التي تم تحديدها على النظير البعيد.

تكوين مفتاح ISAKMP تشفير

دخلت in order to شكلت ساب ق صحة هوية مفتاح، ال crypto isakmp key في وضع التكوين العام:

```
crypto isakmp key cisco123 address 172.16.1.1
```

تكوين قائمة تحكم في الوصول (ACL) لحركة مرور VPN ذات الأهمية

أستخدم قائمة الوصول الموسعة أو المسماة لتحديد حركة المرور التي يجب حمايتها بالتشفير. فيما يلي مثال:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

ملاحظة: تستخدم قائمة التحكم في الوصول لحركة مرور VPN عناوين IP للمصدر واوجهة بعد NAT.

ملاحظة: يجب نسخ قائمة التحكم في الوصول لحركة مرور VPN على كل من نظراي VPN.

تكوين إستثناء NAT

ملاحظة: التكوين الموضح في هذا القسم إختياري.

بشكل نموذجي، يجب أال يكون هناك NAT أنجزت على ال VPN حركة مرور. إن استعملت ال nat in order to أعفيت ال VPN حركة مرور، يجب ذلك مسار خريطة ينبغي كنت استعملت حمل زائد، بعد ترجمة. من مصلحة من ترجمة. الحظ أنه في قائمة الوصول التي يتم إستخدامها في خريطة المسار، يجب رفض حركة مرور بيانات شبكة VPN ذات الأهمية.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

تكوين مجموعة تحويل

لتحديد مجموعة تحويل IPSec (مجموعة مقبولة من بروتوكولات الأمان والخوارزميات)، أدخل crypto ipsec transform-set في وضع التكوين العام. فيما يلي مثال:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

تكوين خريطة تشفير وتطبيقها على واجهة

دخلت in order to خلقت وأ عدلت تشفير خريطة مدخل وأدخلت ال crypto خريطة تشكيل أسلوب، ال crypto map تشكيل أمر عام. حتى يكتمل إدخال خريطة التشفير، هناك بعض الجوانب التي يجب تعريفها كحد أدنى:

- يجب تحديد نظائر IPsec التي يمكن إعادة توجيه حركة المرور المحمية إليها. وهؤلاء هم الأقران الذين يمكن مع إنشاء مساعد خدمة. لتحديد نظير IPSec في إدخال خريطة تشفير، أدخل set peer erasecat4000_flash:.
- يجب تحديد مجموعات التحويل المقبولة للاستخدام مع حركة المرور المحمية. لتحديد مجموعات التحويل التي يمكن إستخدامها مع إدخال خريطة التشفير، أدخل set transform-set erasecat4000_flash:.
- يجب تحديد حركة المرور التي يجب حمايتها. لتحديد قائمة الوصول الموسعة لإدخال خريطة التشفير، أدخل match address erasecat4000_flash:.

فيما يلي مثال:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

تتمثل الخطوة الأخيرة في تطبيق مجموعة خريطة التشفير المحددة مسبقا على واجهة. دخلت in order to طبقت هذا، ال crypto map قارن تشكيل أمر:

```
interface GigabitEthernet0/0
crypto map outside_map
```

التكوين النهائي IOS من Cisco

وفيما يلي تكوين CLI لموجه Cisco IOS النهائي:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
```

```
 set transform-set ESP-AES-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

التحقق من الصحة

قبل التحقق مما إذا كان النفق قيد التشغيل ومن أنه يمر بحركة المرور، يجب التأكد من إرسال حركة مرور المصلحة إما إلى موجه ASA أو Cisco IOS.

> **ملاحظة:** على ASA، يمكن إستخدام أداة تتبع الحزم التي تطابق حركة مرور الاهتمام لبدء نفق IPSec (مثل packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed مثل).

التحقق من المرحلة الأولى

دخلت in order to دققت ما إذا IKEv1 مرحلة 1 يكون فوق ال ASA، **العرض crypto isakmp sa** أمر. النواتج الموقعة هو رؤية MM_ACTIVE الحالة:

```
ciscoasa# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE
```

```
There are no IKEv2 SAs
ciscoasa#
```

دخلت in order to دقق ام إذا ال IKEv1 مرحلة فوق ال cisco ios، ال show crypto isakmp sa erasecat4000_flash:. الناتج المتوقع هو رؤية ACTIVE الحالة:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

التحقق من المرحلة الثانية

للتحقق من تشغيل المرحلة 2 من IKEv1 على ASA، أدخل show crypto ipsec sa erasecat4000_flash:. الناتج المتوقع هو رؤية كل من فهرس معلمات الأمان (SPI) الوارد والصادر. إذا كانت حركة المرور تمر عبر النفق، فيجب أن ترى زيادة عدادات التضمين/قطع الاتصال.

> **ملاحظة:** لكل إدخال من إدخالات قائمة التحكم في الوصول (ACL)، يتم إنشاء وكيل دخمة إخراج show crypto ipsec sa طويلة حيث يمكن أن ينتج عنه فترة منفصل الوارد/الصادر، مما (SA) الأمر (يعتمد على عدد إدخالات ACE في قائمة التحكم في الوصول (ACL) للتشفير).

فيما يلي مثال:

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
 10.20.10.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


#pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #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.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
```

```
     current outbound spi: 8A9FE619
     current inbound spi : D8639BD0

inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

للتحقق مما إذا كانت المرحلة 2 من IKEv1 قيد التشغيل على برنامج Cisco IOS، أدخل show crypto ipsec sa erasecat4000_flash:. الناتج المتوقع هو لكل من SPI الوارد والصادر. إذا كانت حركة المرور تمر عبر النفق، فيجب أن ترى زيادة عدادات التضمين/قطع الاتصال.

فيما يلي مثال:

```
Router#show crypto ipsec sa peer 172.16.1.1

interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
```

```
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

المرحلة 1 و 2 من التحقق

يصف هذا القسم الأوامر التي يمكن إستخدامها على ASA وأ Cisco IOS للتحقق من تفاصيل كل من المرحلتين 1 و 2.

أدخل show vpn-sessiondb الأمر على ASA للتحقق:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
 Tunnel ID    : 2.1
 UDP Src Port : 500                   UDP Dst Port : 500
 IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
 Encryption   : AES128                Hashing      : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 Filter Name  :

IPsec:
 Tunnel ID    : 2.2
```

```
 Local Addr   : 10.10.10.0/255.255.255.0/0/0
 Remote Addr  : 10.20.10.0/255.255.255.0/0/0
 Encryption   : AES128                  Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds            Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes         Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes              Idle TO Left : 26 Minutes
 Bytes Tx     : 100500                  Bytes Rx     : 101400
 Pkts Tx      : 1005                    Pkts Rx      : 1014

NAC:
 Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds               EoU Age(T)   : 309 Seconds
 Hold Left (T): 0 Seconds               Posture Token:
 Redirect URL :

ciscoasa#
```

أدخل show crypto session الأمر على Cisco IOS للتحقق:

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

> **ملاحظة:** راجع المعلومات المهمة حول أوامر التصحيح وأستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء وإستخدامها مستندات Cisco قبل أن تستخدم debug أوامر.

أداة المدقق من شبكة LAN إلى شبكة IPSec

للتحقق تلقائيا من صحة تكوين شبكة LAN إلى شبكة LAN ل IPSec بين ASA و Cisco IOS، يمكنك إستخدام أداة IPSec LAN-to-LANChecker. تم تصميم الأداة بحيث تقبل show tech أو show running-config أمر من إما موجه ASA أو Cisco IOS. وهو يفحص التكوين ويحاول اكتشاف

ام إذا تم تكوين نفق IPSec مستند إلى خريطة الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN). إذا تم تكوينها، فإنها توقع بفحص متعدد النقاط للتكوين وتبرز أي أخطاء تكوين وإعدادات للنفق الذي سيتم التفاوض بشأنه.

تصحيح أخطاء ASA

لاستكشاف أخطاء تفاوض نفق IPSec IKEv1 وإصلاحها على جدار حماية ASA، يمكنك استخدام الأوامر debug التالية:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

ملاحظة: إذا كان عدد أنفاق شبكات VPN على ASA كبيرا، فإن debug crypto condition peer A.B.C.D يجب استخدام الأمر قبل تمكين تصحيح الأخطاء لتحديد مخرجات تصحيح الأخطاء لتضمين النظير المحدد فقط.

تصحيح أخطاء موجه Cisco IOS

لاستكشاف أخطاء تفاوض نفق IPSec IKEv1 وإصلاحها على موجه Cisco IOS، يمكنك استخدام أوامر تصحيح الأخطاء التالية:

```
debug crypto ipsec
debug crypto isakmp
```

ملاحظة: إذا كان عدد أنفاق شبكات VPN على برنامج Cisco IOS كبيرا، فإن debug crypto condition peer ipv4 A.B.C.D يجب استخدامه قبل تمكين تصحيح الأخطاء للحد من مخرجات تصحيح الأخطاء لتضمين النظير المحدد فقط.

تلميح: ارجع إلى حلول أستكشاف أخطاء IPSec VPN وإصلاحها الأكثر شيوعا في L2L وإلى الوصول عن بعد من Cisco للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء شبكة VPN وإصلاحها من موقع إلى موقع.

المراجع

- معلومات مهمة حول أوامر التصحيح
- أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر التصحيح واستخدامها
- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر برتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا
- دقق IPSec LAN-to-LAN
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).