تكوين نفق IKEv2 من موقع إلى موقع بين نقطتي ASAs باستخدام عمليات تبادل المفاتيح المتعددة IKEv2

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين اتصال IKEv2 VPN من موقع إلى موقع بين نظام ASAs من Cisco باستخدام عمليات تبادل المفاتيح المتعددة IKEv2.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Adaptive Security Appliance (ASA)

- مفاهيم IKEv2 العامة

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى نطاق الوصول من Cisco التي تشغل الإصدار 9.20.1.

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

القيود

يشتمل تبادل المفاتيح المتعدد ل IKEv2 على هذه القيود:

- طقم ASA مدعوم على واجهة سطر أوامر واحدة
- HA و مدعوم على الأجهزة متعددة السياقات
- غير مدعوم على الأجهزة المجمعة

الترخيص

ومتطلبات الترخيص هي نفسها كما هو الحال بالنسبة لشبكة VPN من موقع إلى موقع على ASAs.

معلومات أساسية

الحاجة إلى المزيد من عمليات تبادل المفاتيح

يشكل وصول أجهزة الكمبيوتر الكمية الكبيرة خطرا كبيرا على الأنظمة الأمنية، وخاصة تلك التي تستخدم تشفير المفاتيح العامة. الطرق المشفرة التي كان يعتقد أنها صعبة جدا على الحواسيب العادية يمكن كسرها بسهولة عن طريق الحواسيب الكمية. لذا، الحاجة تنشأ للتحول إلى طرق جديدة مقاومة للكم، تسمى أيضا خوارزميات التشفير ما بعد الكم. ويتمثل الهدف في تعزيز أمن إتصالات IPsec باستخدام عمليات تبادل متعددة للمفاتيح. وهذا يشمل الجمع بين تبادل المفاتيح التقليدي وبين تبادل ما بعد الكم. ويضمن هذا النهج أن يكون التبادل الناتج عن ذلك على الأقل بنفس قوة التبادل التقليدي للمفاتح، مما يوفر طبقة إضافية من الأمن.

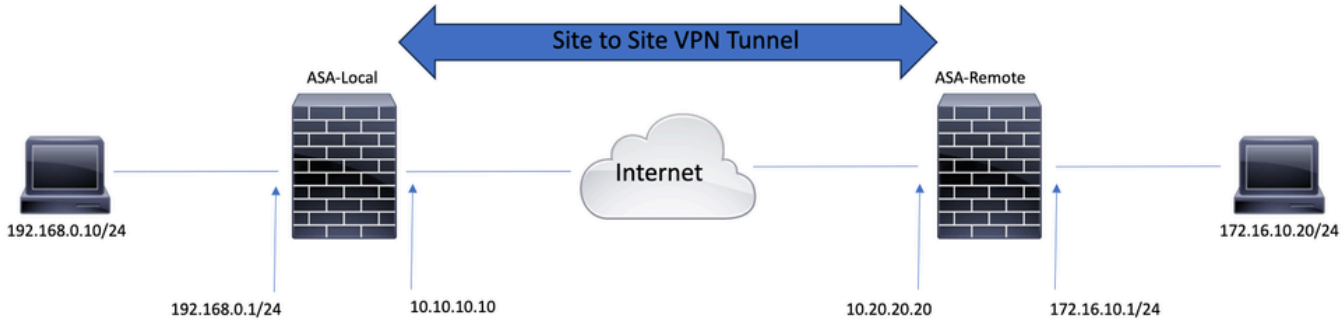
وتتمثل الخطة في تحسين الإصدار الثاني من بروتوكول الإنترنت (IKEv2) من خلال إضافة الدعم لعمليات تبادل رئيسية متعددة. هذه التبادلات الرئيسية الإضافية يمكنها التعامل مع الخوارزميات الآمنة من تهديدات الكم. لتبادل المعلومات حول هذه المفاتيح الإضافية، يتم تقديم نوع رسالة جديد يسمى Intermediate Exchange. ويتم التفاوض بشأن هذه المبادلات الرئيسية باستخدام طريقة IKEv2 العادية، من خلال حمولة SA.

التكوين

يصف هذا القسم تكوينات ASA.

الرسم التخطيطي للشبكة

تستخدم المعلومات الواردة في هذا المستند إعداد الشبكة التالي:

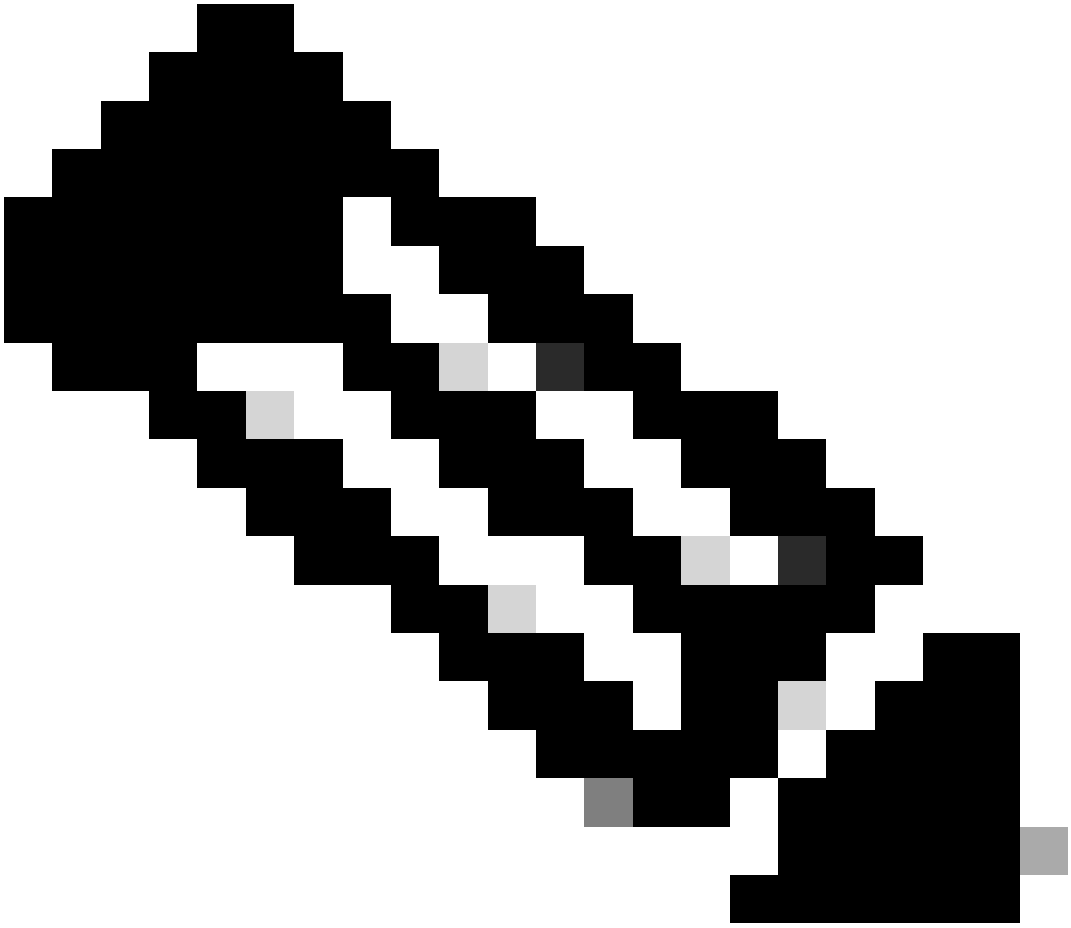


تكوين ASA

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 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```



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 استخدام الأمر ping للتحقق من الاتصال الأساسي.

تكوين سياسة IKEv2 باستخدام تبادل متعدد المفاتيح وتمكين IKEv2 على الواجهة الخارجية

دخلت in order to شكلت ال IKEv2 سياسة ل هذا توصيل، هذا أمر:

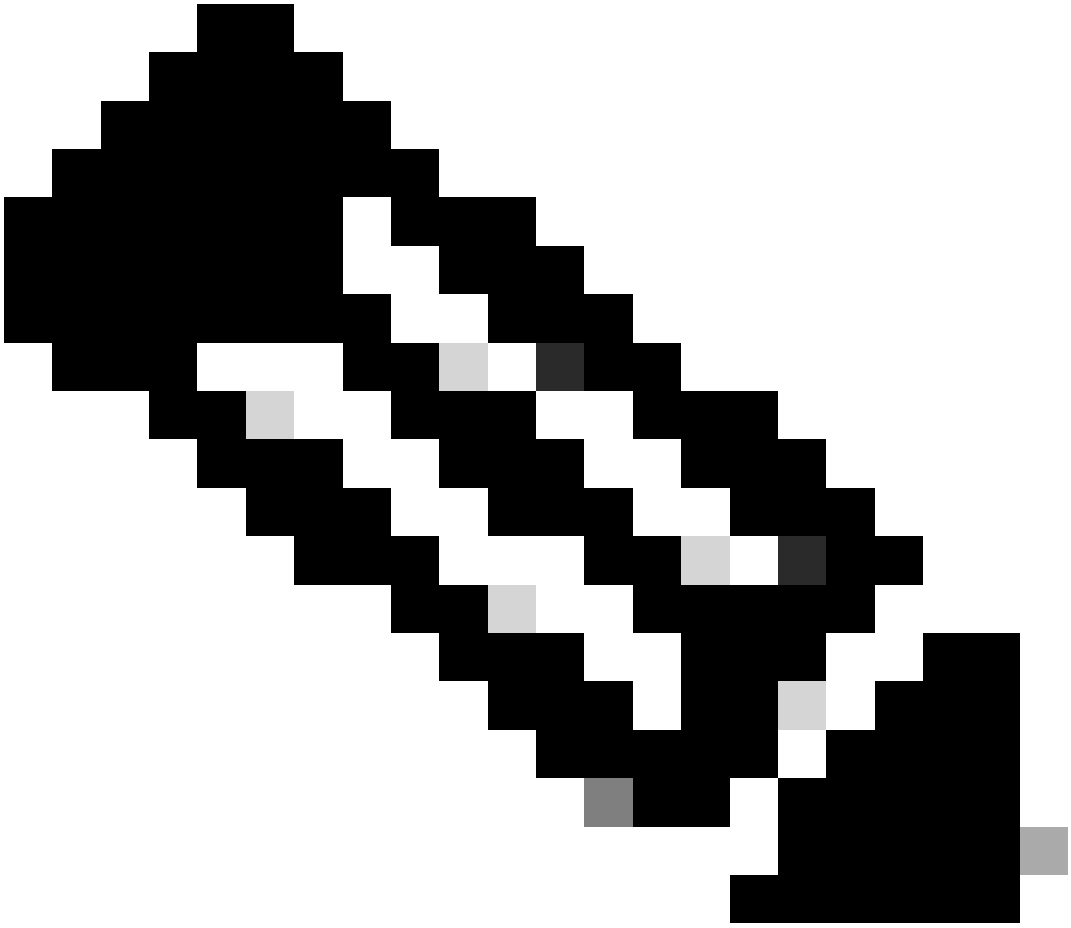
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

يمكن تكوين تحويلات تبادل المفاتيح الإضافية تحت crypto ikev2 policy إستخدام الأمرadditional-key-exchange. يمكن تكوين إجمالي سبعة تحويلات إضافية للتبادل. في هذا المثال، تم تكوين محولين Exchange إضافيين (باستخدام مجموعتي DH 21 و 31).

additional-key-exchange 1 key-exchange-method 21 additional-key-exchange 2 key-exchange-method 31

سياسة IKEv2 النهائية تبدو كما يلي:

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



ملاحظة: توجد مطابقة لسياسة IKEv2 عندما تحتوي كل النهجين على نفس قيم معلمات المصادقة والتشفير والتجزئة والمعلمة Diffie-Hellman وقيم معلمات تبادل المفاتيح الإضافية.

أنت ينبغي مكنت IKEv2 على القارن أن ينهي ال VPN نفق. بشكل نموذجي، هذه هي الواجهة الخارجية (أو الإنترنت). لتمكين IKEv2، أدخل الأمرcrypto ikev2 enable outside في وضع التكوين العام.

تكوين مجموعة النفق

بالنسبة لنفق من موقع إلى موقع، يكون نوع ملف تعريف الاتصال هو IPSec-l2l. دخلت in order to شكلت ال IKEv2 مبرد

مفتاح، هذا أمر:

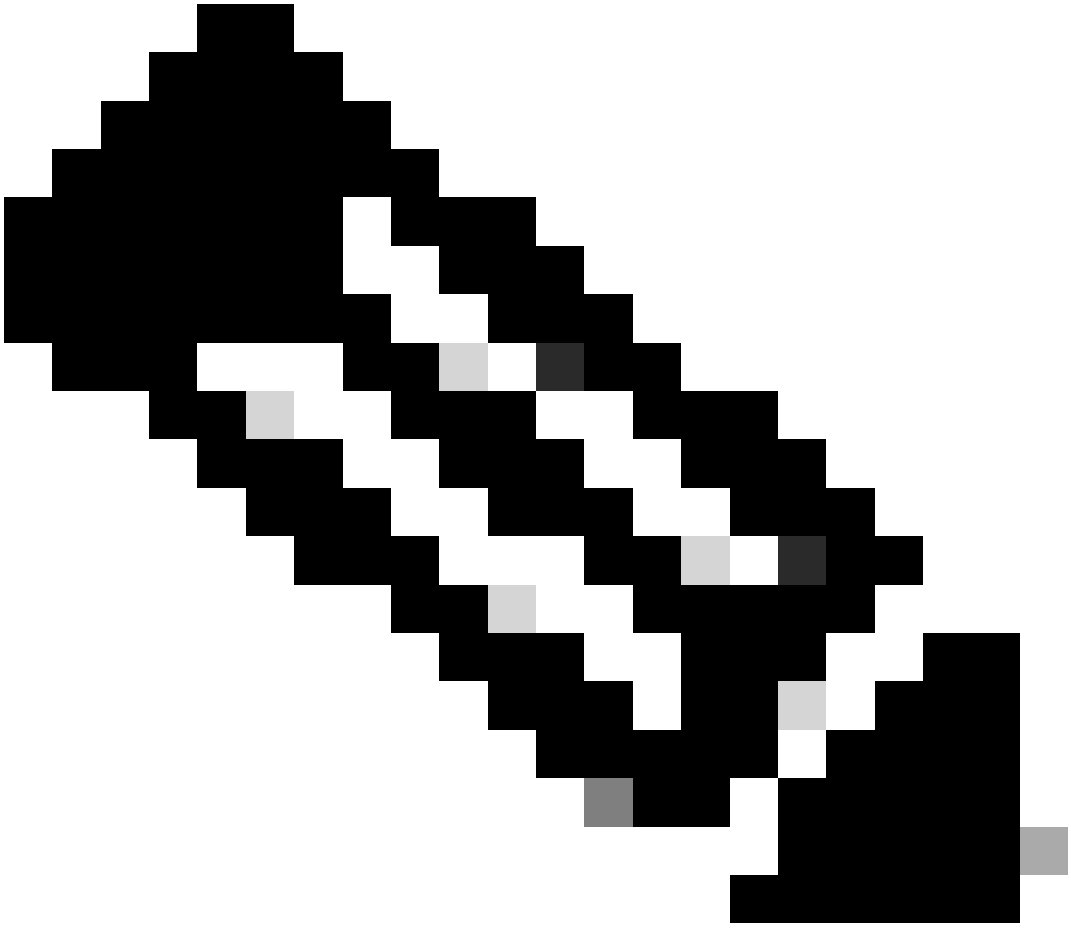
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

تكوين حركة المرور المثيرة للاهتمام وقوائم التحكم في الوصول (ACL) المشفرة

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

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
```

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



ملاحظة: يجب أن يكون لنظير VPN نفس قائمة التحكم في الوصول (ACL) في تنسيق مكرر.

تشكيل هوية NAT (إختياري)

عادة، يحتاج هوية nat in order to منع حركة المرور مثيرة من ضرب ديناميكي nat. ال هوية nat أن يكون شكلت في هذه الحالة:

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

تكوين مقترح IKEv2 IPSec

يستخدم اقتراح IKEv2 IPSec لتحديد مجموعة من خوارزميات التشفير والتكامل لحماية حركة مرور البيانات. يجب أن يطابق اذه الاقتراح كل من نظامي VPN لإنشاء IPSec SA بنجاح. الأوامر المستخدمة في هذه الحالة هي:

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

تكوين خريطة تشفير وربطها بالواجهة

تجمع خريطة التشفير بين جميع التكوينات المطلوبة ويجب أن تحتوي بالضرورة على:

- قائمة وصول لمطابقة حركة المرور التي يجب تشفيرها (يشار إليها عادة باسم قائمة التحكم في الوصول (ACL) للتشفير)
- تعريف النظير
- مقترح IKEv2 IPSec واحد على الأقل

التكوين المستخدم هنا هو:

```
crypto map outside_map 1 match address asa-vpn crypto map outside_map 1 set peer 10.20.20.20 crypto map outside_map 1 set ikev2 ipsec-proposal IKEV
```

يتم تطبيق الجزء الأخير من خريطة التشفير هذه على الواجهة الخارجية (العامة) باستخدام crypto map outside_map interface outside الأمر.

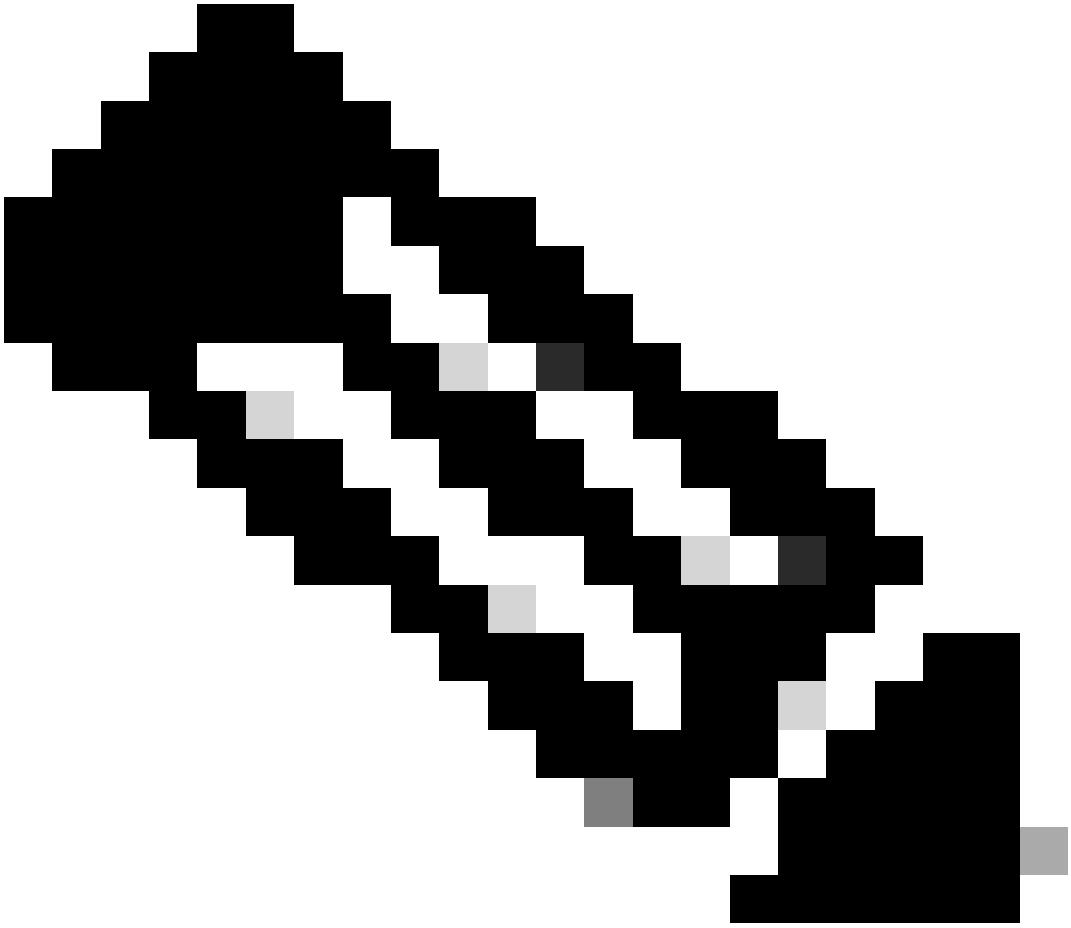
التكوين النهائي ASA المحلي

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
```

```
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
!
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
!
access-list asa-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 ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

التكوين النهائي ASA البعيد

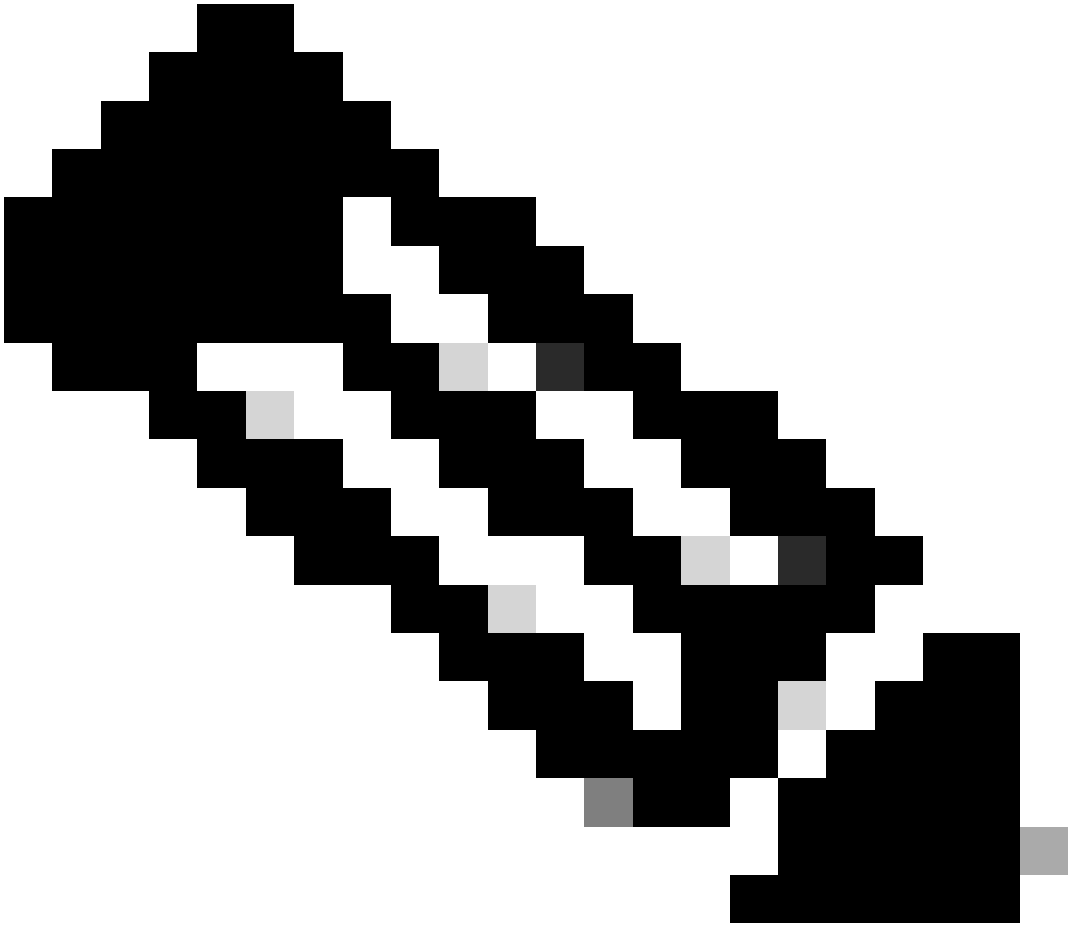
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



ملاحظة: قائمة التحكم في الوصول (ACL) بالتنسيق المنعكس والمفاتيح المشتركة مسبقا هي نفسها في كلا النهايتين.

التحقق من الصحة

قبل التحقق من أن النفق يكون فوق وأنه يمر الحركة مرور، أنت ينبغي ضمنت أن حركة مرور مهم يكون أرسلت إلى ال ASAs.



ةظحلام: استعملت الربط tracer in order to حاكت الحركة مرور flow. يمكن القيام بذلك باستخدام الأمر packet-tracer: packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 بالتفصيل على ال ASA المحلي.

للتحقق من صحة عمليات تبادل المفاتيح الإضافية، يمكنك إستخدام show crypto ikev2 sa الأمر. كما هو موضح في الإخراج، يمكنك التحقق من معلمات AKE للتحقق من خوارزميات التبادل المحددة.

<#root>

Local-ASA# show crypto ikev2 sa IKEv2 SAs: Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status R

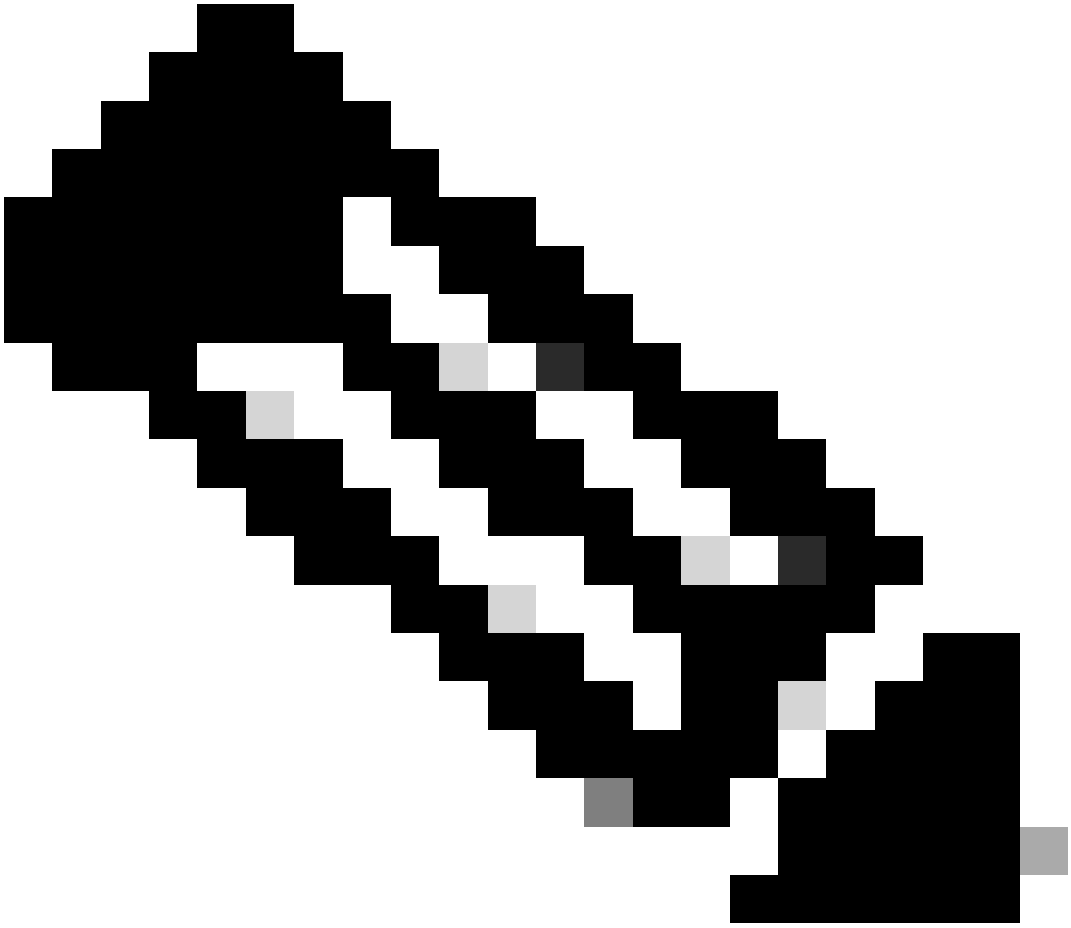
AKE1: 21 AKE2: 31

```
Life/Active Time: 86400/7 sec Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535 remote sele
```

استكشاف الأخطاء وإصلاحها

يمكن استخدام تصحيح الأخطاء المذكورة لاستكشاف أخطاء وقف IKEv2 وإصلاحها:

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```



ملاحظة: إذا كنت ترغب في أستكشاف أخطاء نفق واحد فقط وإصلاحه (والذي يجب أن يكون الحالة إذا كان الجهاز قيد الإنتاج)، فيجب تمكين تصحيح الأخطاء بشكل مشروط باستخدام أمر تصحيح أخطاء التشفير النظير x.x.x.x.

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).